UNIVERSIDADE FEDERAL FLUMINENSE
CENTRO TECNOLÓGICO
MESTRADO EM ENGENHARIA DE TELECOMUNICAÇÕES

ROGÉRIO BAPTISTA LOURENÇO

PROTOCOLOS VOIP PARA REDES CONVERGENTES

NITERÓI
2007

ROGÉRIO BAPTISTA LOURENÇO

Protocolos VoIP para Redes Convergentes.

Dissertação apresentada ao Curso de Pós-Graduação em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre.

Orientador: Prof. Dr. LUIZ PINTO DE CARVALHO

Niterói
2007

L892 Lourenço, Rogério Baptista.

Protocolos VoIP para Redes Convergentes / Rogério Baptista Lourenço. – Niterói, RJ : [s.n.], 2007.

150 f.

Orientador: Luiz Pinto de Carvalho.

Dissertação (Mestrado em Engenharia de Telecomunicações) - Universidade Federal Fluminense, 2007.

1. Telefonia. 2. Protocolo de comunicação. 3. Comunicação. 4. Engenharia de telecomunicações. I.Título.

CDD 621.38

ROGÉRIO BAPTISTA LOURENÇO

Protocolos VoIP para Redes Convergentes.

Dissertação apresentada ao Curso de Pós-Graduação em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre.

Aprovada em 24 de julho de 2007

BANCA EXAMINADORA

_____

Prof. Dr. Luiz Pinto de Carvalho – Orientador
Universidade Federal Fluminense

_____

Prof. Dr. Carlos Ribeiro da Cunha
Universidade Estácio de Sá

_____

Prof. Dr. Eduardo Rodrigues Vale
Universidade Federal Fluminense

_____

Prof. Dr. Pedro Henrique Gouvêa Coelho
Universidade do Estado do Rio de Janeiro

Niterói
2007

AGRADECIMENTOS

Desculpem por me estender demasiadamente nos agradecimentos, mas foi impossível desenvolver esta Dissertação sem a ajuda de tantos amigos.

Em primeiro lugar, reconheço e agradeço todo o apoio, amor e respeito da minha família. Especialmente a minha mãe, Eliane, pela minha formação e caráter, por todo incentivo aos estudos e dedicação incansável; ao meu pai, Ney, irmão, Rodrigo e "madrasta", Ana, pela compreensão dos momentos que deixamos de estar juntos e por toda a união nos momentos mais importantes, sem contar toda admiração e exemplo mútuo. Meus agradecimentos também muito especiais para minha querida noiva, Simone, por estar ao meu lado todo o tempo e por todo amor, respeito e compreensão.

Agradeço toda minha formação acadêmica à UFF e principalmente aos mestres que tive a oportunidade de ser aluno desde a graduação. Especial agradecimento ao orientador desta Dissertação, professor Luiz, por todos os ensinamentos e toda a paciência, por quem tenho grande respeito e admiração. Espero ter absorvido uma parcela de seu conhecimento e experiência. Aos amigos estudantes da UFF que tiveram participação neste trabalho, também dedico os meus agradecimentos.

Aos amigos da Star One, principalmente aos chefes imediatos, pela valorização e investimento na formação de seus funcionários e dispensa durante os horários do expediente, sem os quais não seria possível iniciar este trabalho. Aos amigos da Embratel e do CRT, especialmente na figura do amigo professor Silvério, pelas orientações profissionais e acadêmicas e por me abrir tantas portas; também sou grato aos responsáveis pelo CRT, José Silva e Walderson, por todo o apoio, presteza e comprometimento durante todo o desenvolvimento do trabalho; e aos camaradas Bernardo e Chicão, pela paciência, competência e simplicidade.

Deixo registrado o meu muito OBRIGADO a todos e agradeço a Deus por colocar tantas pessoas excepcionais na minha caminhada, pela boa saúde, coragem e perseverança em todos os momentos.

RESUMO

Este trabalho tem como objetivo avaliar os principais protocolos de sinalização desenvolvidos para o tráfego de voz sobre o protocolo IP (VoIP – "Voice over IP"), a partir da análise de um cenário atual e muito abrangente, como aquele empregado pela Empresa Brasileira de Telecomunicações (Embratel). Como preliminar, buscou-se revisar os primeiros sistemas de sinalização telefônica, até o primeiro sistema de sinalização para comunicações "on-line" desenvolvido para redes locais com base no protocolo IP, conhecido como H.323. Em seguida, são analisados protocolos relevantes na sinalização em comunicações VoIP, tendo em vista o desenvolvimento de métodos de teste de equipamentos e sistemas que devam utilizar-se desses protocolos.

Pelo lado da Empresa que implementa sistemas que utilizam esses protocolos, as decisões de adoção ou não de novas tecnologias e equipamentos não são simples e quase sempre é necessário desenvolver métodos de teste que possibilitem uma avaliação técnica apurada, de forma que os resultados sejam homogêneos e permitam a correta tomada de decisão. Neste sentido, o desafio é avaliar um sistema de sinalização telefônica a partir de um cenário real, e a proposta deste trabalho é desenvolver uma metodologia de testes que seja capaz de avaliar tecnicamente qualquer equipamento ou solução VoIP, em relação às normas internacionais aplicáveis, bem como a interligação com a rede STFC. Os protocolos em destaque são o SIP e o MGCP; a metodologia proposta por este estudo conduzirá a pelo menos dois cadernos de práticas com uma série de sugestões de testes, que serão úteis na avaliação de redes VoIP, bem como na aceitação dos equipamentos, e também para o conhecimento mais detalhado dos protocolos. O protocolo MEGACO/H.248 é apresentado como tecnologia sucessora, porém apenas os aspectos que contribuem para a evolução das redes de sinalização VoIP serão destacados. Os cadernos de testes desenvolvidos para a Embratel como resultado deste estudo não são incluídos nesta dissertação.

Palavras-chave: RTPC; VoIP; H.323; SIP; MGCP; MEGACO.

ABSTRACT

It is the purpose of this work to evaluate the main signalling protocols developed for voice over IP traffic, proceeding from the analysis of a contemporary and comprehensive scenario such as the one employed by Empresa Brasileira de Telecomunicações (Embratel).

As a preliminary, the initial telephone signalling systems are revised, up to the first signalling system for on-line communications developed for local networks based on the IP protocol, known as H.323. Next, some relevant signalling protocols used for VoIP are analyzed, in view of the development of methods of test for equipments and systems that must use these protocols.

For the company that implements systems using these protocols, the decision to adopt or not new technologies and equipments are not simple and it is almost always necessary to develop test procedures to produce a precise technical evaluation, so that the results are homogeneous and allow a correct decision.

In view of this, the challenge is to evaluate a telephone signalling system based on a real scenario, and it is this work's proposition to develop a test methodology capable of technically evaluating any VoIP equipment or solution, considering its adequacy to the international standards, as well as its connection to the STFC.

The protocols to be considered are SIP and MGCP; the methodology proposed in this study will lead to at least two practices that contain a number of suggestions of tests, which will be useful in evaluating VoIP networks, as well as in equipment acceptance and also for a more detailed knowledge of the protocols.

MEGACO/H.248 protocol is presented as a succeeding technology, however only the aspects that contribute to the evolution of VoIP networks signalling will be shown. The test procedures developed for Embratel as a result of this work are not included in this dissertation.

Key words: PSTN; VoIP; H.323; SIP; MGCP; MEGACO.

Sumário

Lista de tabelas, figuras e gráficos

Lista de abreviaturas, siglas e símbolos.

CAS	Channel Associating Signalling
CCS	Common Channel Signalling
DSS-1	Digital Subscriber Signalling System Number 1
DTMF	Dual Tone Multi Frequential
ETSI	European Telecommunications Standards Institute
IAD	Integrated Access Device
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol.
INAP	Intelligent Network Application Protocol
ISDN	Integrated Services Digital Network.
ISUP	ISDN User Part
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
MAP	Mobile Application Part
MFC-5C	Multi-Frequencial Compelida – Variante 5C
MFC-R2	Multi-Frequencial Compelida – Sistema de Sinalização R2
MGCP	Media Gateway Control Protocol
MPLS	Multi Protocol Label Switching
MTP	Message Transfer Part
NGN	Next Generation Network
OMAP	Operations and Maintenance Part
POTS	Plan Old Telephone Systems
PSTN	Public Switched Telephone Network.
QoS	Quality of Service.
PABX	Private Automatic Branch eXchange
POTS	Plain Old Telephone Service
R2D	Digital R2 Signalling System
RAS	Registration, Admission and Status.
RFC	Request For Comment.
RSVP	Resource Reservation Protocol.

RTP	Real-time Transport Protocol.
RTCP	Real-time Control Protocol.
RTPC	Rede de Telefonia Pública Comutada
SCCP	Signalling Connection Control Part
SDP	Session Description Protocol.
SDT	Sistema de Documentação Telebrás
SG	Signalling Gateway.
SIP	Session Initiation Protocol.
SIP-T	SIP for Telephone.
SS7	Signalling System No. 7.
STFC	Serviço de Telefonia Fixa Comutada
TCAP	Transaction Capability Application Part
TCP	Transmission Control Protocol.
TDM	Time-Division Multiplexing.
TUP	Telephone User Part
URI	Uniform Resource Identifier.
URL	Uniform Resource Locator.
UDP	User Datagram Protocol.
VAD	Voice Activity Detection.
VoIP	Voice over Internet Protocol.

1. Introdução

O setor de telecomunicações no Brasil passa por um período de grande desenvolvimento desde a quebra do monopólio da TELEBRÁS e sua privatização. Desde então, os investimentos de diversas empresas ou grupos econômicos proporcionam um constante surgimento de novas tecnologias consideradas emergentes e que detêm o potencial de criar um novo setor ou de transformar um já existente, tornando obsoletas estratégias, práticas e modelos de negócios já estabelecidos.

Considerando o rápido crescimento e avanço tecnológico da telefonia nos últimos anos, a área de voz sobre IP (VoIP – "Voice over IP") tem sido a maior revolução nestes tempos e surge como tema de diversos estudos e artigos, propiciando a elaboração do presente trabalho como um estudo aprofundado sobre um dos múltiplos aspectos dessa área. O assunto da pesquisa foi sugerido pela Embratel, a partir da necessidade de padronizar a avaliação técnica de soluções VoIP e garantir que os elementos da rede estejam operando em conformidade com as normas internacionais. A proposta para atender tais necessidades foi a de desenvolver um documento com uma série de testes elaborados a partir do padrão internacional de cada protocolo. A Empresa, de posse do Roteiro de Testes, será capaz de avaliar o grau de conformidade que determinado equipamento possui com a norma, terá mecanismos de comparação entre soluções VoIP e também poderá diagnosticar o grau de interoperabilidade entre equipamentos, lembrando que os equipamentos devem evitar implementações proprietárias e garantir um funcionamento padronizado, de forma que a rede possa conviver com a presença de elementos de diversos fabricantes.

Este trabalho inicialmente apresenta uma análise técnica das redes de telefonia fixa comutada, indo até o primeiro sistema de sinalização aplicável a VoIP, embora desenvolvido tendo em vista o controle da transmissão de comunicações "on-line" em redes locais, em particular teleconferências, que foi o H.323, como base para desenvolver um estudo teórico sobre os protocolos SIP e MGCP. A escolha destes dois protocolos não advém apenas das necessidades da Embratel, mas principalmente de sua grande aplicação em redes corporativas e também em ambientes de menor escala, considerando o fato de que os dois podem ser utilizados em conjunto, de forma complementar, como será esclarecido adiante.

Em seguida, procura-se identificar os pontos fundamentais destes dois protocolos e destacar os aspectos cruciais, objetivando formar uma metodologia de análise crítica para gerar testes de aceitação em equipamentos.

Por fim, para cada protocolo é apresentada uma descrição sumária dos métodos utilizados no desenvolvimento de testes para verificar a conformidade com as normas internacionais de equipamentos ou sistemas que utilizem esses protocolos. Apenas fragmentos do Roteiro de Testes gerado são apresentados como ilustração do resultado obtido.

No desenvolvimento deste trabalho, as informações referentes aos protocolos analisados estão sendo utilizadas para gerar um Roteiro de Testes para cada protocolo, roteiros estes que poderão ser utilizados na prática para avaliar a conformidade de sistemas em implantação na rede da Embratel que se encontra em operação. O motivo para que apenas fragmentos dos cadernos de testes sejam apresentados neste trabalho é que os mesmos têm seus direitos reservados pela Embratel, de acordo com o Plano de Trabalho firmado entre a Escola de Engenharia da UFF e o Centro de Referencia Tecnológica (CRT) da Empresa. A omissão de um maior detalhamento dos cadernos de teste não prejudica a dissertação visto que os mesmos contêm apenas uma série de testes práticos aos quais os equipamentos devem ser submetidos para avaliação correta de seu funcionamento. É mais relevante tecnicamente compreendermos o método de obtenção dos testes em vista das características técnicas dos protocolos.

1.1 Um Breve Histórico

A partir do surgimento do telégrafo em 1837 passando pela criação do telefone em 1876, iniciava-se o primeiro grande ciclo do universo das telecomunicações, que durante cerca de um século foi marcado por grandes descobertas e invenções. O segundo grande ciclo teve início em 1960 com a digitalização dos meios de transmissão, posteriormente das centrais e, por fim, da rede de acesso de assinantes. Em 40 anos a comunicação de dados passou, gradativamente, a ocupar mais espaço nas telecomunicações. A comunicação dos sinais de

voz e vídeo através da internet também despertou maior interesse, devido aos baixos custos, quando comparados com os sistemas tradicionais [1]. O terceiro grande ciclo surge a partir do ano 2000 e será abordado apenas no Capítulo 4, pois se refere à convergência das redes de telecomunicações.

Diante deste processo tão rico de desenvolvimento, este capítulo se restringe a resgatar as informações que serão úteis ao longo do trabalho, visto que os serviços baseados em VoIP têm tido, em sua grande maioria, integração com o sistema tradicional de telefonia. Para tanto, os tópicos subseqüentes apresentam uma descrição das sinalizações telefônicas tradicionalmente utilizadas no Brasil, para integração futura com protocolos de sinalização VoIP. O capítulo se encerra já no mundo IP através da apresentação do protocolo H.323.

O estudo tem início com a Figura 1, que busca identificar duas etapas distintas no processo de sinalização de uma chamada telefônica. A primeira se refere às redes de acesso de assinante, localizada nas bordas da rede, no trecho Terminal – Central Local, denominada Sinalização de Usuário. A outra fase do processo de encaminhamento de chamada ocorre no trecho entre Centrais; a Figura 1 apresenta apenas um nível hierárquico entre Centrais da rede pública, representado pela Central Tandem. Na realidade, as centrais públicas são classificadas em até quatro níveis hierárquicos, de acordo com a abrangência e os tipos de interligações [2].

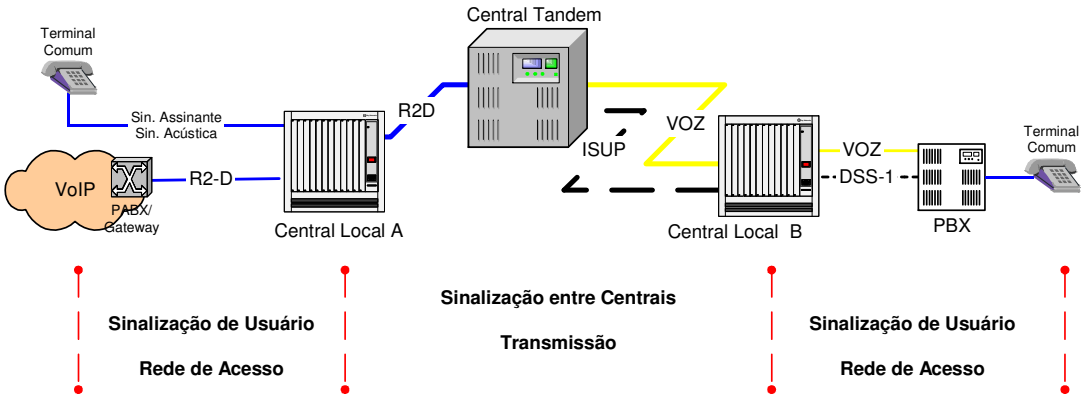


Figura 1: Exemplo de Configuração e Sinalização de uma Rede de Telefonia Tradicional incluindo uma conexão de VoIP através de Gateway.

A proposta deste trabalho é estudar protocolos VoIP em uso em conjunto com redes tradicionais; para isso, é útil mapear o funcionamento de uma rede telefônica fim-a-fim, o que permite identificar e recuperar falhas em qualquer trecho no processo de sinalização de uma chamada real. Desta forma, a Figura 1 apresenta uma proposta de uma espécie de rede híbrida de telefonia que vem se tornando cada vez mais comum, isto é, a coexistência da voz sobre IP com o legado da STFC, solução de transição válida até o momento em que a telefonia seja toda baseada na comutação de pacotes.

1.2 Aspectos da Rede Telefônica

Sinalização Telefônica no Trecho Terminal-Central

Neste trecho, toda e qualquer comunicação que parte do assinante com destino à Central Local é denominada Sinalização de Assinante e, no sentido inverso, ou seja, da Central Local até o assinante, é conhecida como Sinalização Acústica.

A Sinalização de Assinante é a mais primitiva entre todas elas, pois se refere aos números digitados pelo assinante e enviados à Central Local, ou seja, é um conjunto de pulsos ou de freqüências pré-programadas de acordo com cada tipo de Terminal, como num Terminal decádico, multifrequencial (DTMF) ou ISDN, respectivamente. [2]

Os tons enviados pela Central Local ao assinante caracterizam a Sinalização Acústica, isto é, a central envia sinais aos Terminais, onde são traduzidos acusticamente, com o objetivo de informar ao assinante sobre a fase da chamada, estado na rede ou do Terminal de destino [3]. Exemplos desta sinalização: tom de discar, corrente de toque, tom de ocupado, etc.

Quando a Rede de Acesso apresenta a configuração Terminal-PABX-Central Local, de acordo com a configuração da Figura 1, os protocolos R2-Digital e DSS-1 são utilizados no Brasil no trecho PABX-Central e serão considerados nos próximos tópicos deste capítulo. Este tipo de configuração é muito comum em redes corporativas de telefonia e

muito importante também, pois o Gateway responsável pela saída do tráfego de uma rede VoIP para a RTPC será interpretado como um PABX pela rede telefônica e, portanto, será fundamental entender o processo de sinalização no trecho PABX-Central ou Gateway VoIP-Central. Neste caso, as Sinalizações de Usuário e Acústica atuarão no trecho Terminal-PABX.

Sinalização Telefônica no Trecho Central-Central

O processo de sinalização entre Centrais permite o encaminhamento de uma chamada desde a Central Local de origem até a de destino, e fazem parte deste contexto a Sinalização por Canal Associado e a Sinalização por Canal Comum.

A Sinalização por Canal Associado (CAS) foi um sistema desenvolvido em 1960 e que ainda é usado pela China e Brasil para centrais analógicas, onde a sinalização da chamada ocorre no mesmo canal utilizado para tráfego de voz, ambos compartilhando o mesmo meio físico. [2] A Sinalização por Canal Comum (CCS) será definida mais adiante neste capítulo.

1.3 Protocolos de Sinalização

1.3.1 Sinalização R2D

A especificação R2 Digital (R2-D) foi desenvolvida pela ITU-T e está contida nas Recomendações Q.400 até Q.490. Embora exista esta faixa de recomendações para o padrão, há muitas variações no modo em que a R2-D foi implementada, isto é, vários países definiram tipos de implementações diferentes. O Brasil padronizou esta sinalização em 1968 para utilização na rede nacional de telefonia, por isso este estudo se baseia nas Práticas Telebrás.

A Sinalização R2-Digital ou Sinalização de Linha tem capacidade de sinalizar até 30 canais de áudio, operando a taxas de 2.048 Mbps (E1). A R2-D é do tipo CAS e atua em

toda a hierarquia do sistema telefônico em conjunto com a Sinalização entre Registradores (MFC-5C).

Sinalização de Linha

São sinais destinados a efetuar a ocupação, liberação e supervisão de troncos entre duas centrais; opcionalmente, permite o envio de sinais de tarifação [4]. A Sinalização de Linha é bastante antiga e vem sendo desativada devido a sua lentidão. As sinalizações exclusivamente de linha são as seguintes: E & M Pulsada, E & M Contínua e R2-D.

A Figura 2 apresenta um quadro E1 típico da Sinalização de Linha, que é dividido em 32 *time-slots* (TS), sendo o primeiro (TS0) utilizado para alinhamento de quadro, o *time-slot* TS16 é o utilizado para sinalização das chamadas propriamente dita e os 30 *time-slots* restantes são usados para transporte de 30 canais de áudio distintos, sendo todos digitais (PCM) operando a taxas de 64 Kbps.

O *time-slot* TS16, assim como todos os demais, possui 8 bits; para sinalizar cada canal de áudio, são necessários apenas 4 bits, sendo dois para controle da chamada no sentido origem-destino, chamados canais "para frente" ($a_{forward}$ e $b_{forward}$), e os outros dois para o sentido inverso, chamados canais "para trás" ($a_{backward}$ $b_{backward}$). Portanto, este sistema é capaz de sinalizar até dois canais de áudio por cada quadro E1 simultaneamente, sendo que os quatro primeiros bits referem-se à sinalização dos canais TS1 à TS15 e os quatros últimos sinalizam os canais de voz TS17 até TS31.

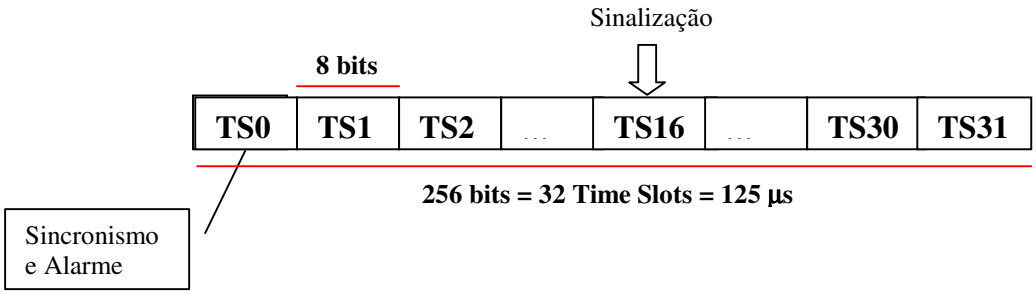


Figura 2: Quadro E1 com Sinalização de Linha

Para os sistemas digitais do Brasil e Europa, o quadro E1, representado na Figura 2, foi formado pela multiplexação de 30 canais de áudio; o sinal multiplexado resultante pode, por sua vez, ser novamente multiplexado com mais três quadros E1, resultando no quadro E2, e assim sucessivamente, com o objetivo de permitir o agrupamento de maiores quantidades de canais e mais altas taxas de transmissão.

De forma geral, a função de cada um dos quatro bits da sinalização de um canal de áudio é a seguinte:

a_f: indica as condições da linha do assinante chamador e também as condições de operação do tronco de origem.
b_f: indica ao tronco de destino a ocorrência de falhas no tronco de origem.
a_b: indica as condições da linha do assinante chamado.
b_b: reflete as condições de ocupação do tronco de destino.

A Tabela 1 apresenta um resumo das codificações das mensagens da Sinalização de Linha R2 Digital [4]. As mensagens estão divididas em dois grupos: o primeiro é referente à transição da codificação das mensagens de sinalização mais comumente utilizadas durante uma chamada normal. O segundo grupo é relativo às falhas e suas variações. A coluna A←→B indica o sentido da mensagem e representa a origem e o destino da chamada, respectivamente.

STATUS	***A←→B***	a_f	b_f	a_b	b_b	***OBSERVAÇÕES***
Circuito livre	→	1	0	1	0	
Ocupação do canal	→	1/0	0	1	0	Mensagem SEIZING (SZ)
Confirmação de ocupação	←	0	0	1	0/1	Mensagem PTS (Proceeding To Send)
Atendimento lado B	←	0	0	1/0	1	Mensagem Answer (ANS)
Conversação	←→	0	0	0	1	
Tarifação	←	0	0	0/1	1	Canal a_b = 1 durante 150 ms
Conversação	←→	0	0	0	1	
Desligar para frente	→	0/1	0	X	1	X = 0; Clear Forward (CLF)
Desligar para trás	←	0	0	X	1	X = 1; Clear Back (CLB)
Confirmação de	←	0/1	0	1	0	Mensagem em resposta a um sinal de

desconexão						desligar para frente. Release Guard (RLG)
Desconexão forçada	←	0	0	0	1/0	É um sinal que substitui o sinal de desligar para trás a partir da Central de tarifação para a Central de Origem, depois de ocorrida a temporização.
Bloqueio	←	1	0	1	1	Circuito bloqueado na condição de livre
Bloqueio	←	1	1	1	1	Bloqueio na condição de conversação
Retirada do Bloqueio	→	1	0	1	1/0	
Falha	→	1	1	1	0	Falha na condição de livre
Retirada da falha	→	1	0	1	1	

Tabela 1: Tabela representativa da codificação digital do campo 16 da Sinalização de Linha do sistema R-2 Digital.

Sinalização entre Registradores

A Sinalização entre Registradores é responsável pela troca de informação entre centrais, referindo-se às informações de numeração dos assinantes, bem como a seus tipos e estados [5]. Esta sinalização pode ser entendida como complementar à Sinalização de Linha, que por sua vez atua nos próprios *time-slots* dos canais de voz (TS1–TS15; TS17–TS31).
O sistema de Sinalização entre Registradores aqui considerado é chamado de Multifrequencial Compelida (MFC), porque ao se enviar um sinal para frente, é necessário aguardar a recepção do sinal para trás para poder enviar um novo sinal para frente. Durante este período, o sinal é enviado de forma permanente, ou seja, a mesma informação é enviada ininterruptamente até que uma resposta seja recebida.

Portanto, nesse sistema de sinalização, os sinais são divididos em “Sinais para Frente” e “Sinais para Trás” e possuem doze freqüências básicas divididas em dois grupos de seis, denominados de grupo de freqüências altas e grupo de freqüências baixas. Cada sinal é composto por duas freqüências dentro de um grupo. As freqüências altas são transmitidas para frente e, em resposta, as freqüências baixas são transmitidas para trás.

Os Sinais para Frente são divididos em: **Grupo I** (Informações Numéricas e Controle)
Grupo II (Categoria do Chamador)

Os Sinais para Trás são divididos em: **Grupo A** (Solicitação da Central de destino)

Grupo B (Condições do Assinante)

De acordo com o interesse deste estudo, as Tabelas 2 à 5 apresentam as mensagens mais importantes de cada grupo [5].

Sinais do Grupo I

SINAIS	SENTIDO	OBSERVAÇÃO
I-1 à I-10	→	Envia os dígitos espontaneamente ou em resposta aos sinais para trás. Exemplo: I1 = dígito 1; I2 = dígito 2; I10 = dígito 0
I-12	→	Pedido A-5 recusado ou indicação de trânsito internacional *
I-15	→	Fim do envio dos dígitos do chamador (resposta ao A-5) ou enlace via satélite *

Tabela 2: Sinalização entre Registradores: Sinais do Grupo I

* não será considerado

Outros:

I-11 e I-14 → Inserção de supressão de eco na origem e no destino, respectivamente.

Sinais do Grupo II

Este grupo de sinais tem a finalidade de enviar ao destino a categoria ou características dos equipamentos originadores da chamada.

SINAIS	SENTIDO	OBSERVAÇÃO
II-1	→	Terminal não possui características especiais (Terminal comum) e sem prioridade.
II-2	→	Tarifação Especial
II-4	→	Chamada originada de telefone público local.
II-6	→	Terminal ligado à equipamento de comunicação de dados.
II-8	→	Chamada a cobrar

Tabela 3: Sinalização entre Registradores: Sinais do Grupo II

Outros:

II-7 → telefone público interurbano

Sinais do Grupo A

As mensagens não indicadas nestas tabelas não foram citadas por serem reservadas para uso posterior ou para uso em centrais internacionais ou, simplesmente, não são pertinentes ao trabalho.

SINAIS	SENTIDO	OBSERVAÇÃO
A-1	←	Solicita o próximo algarismo
A-3	←	Endereço completo e preparação para recepção de sinais do grupo B (resposta da origem com sinal do grupo II obrigatoriamente)
A-5	←	Solicitar categoria do assinante chamador
A-5 *	←	Solicitar o envio do próximo algarismo do número de assinante chamador.
A-7, A-8, A-9	←	Solicitar o reenvio do algarismo (N-2), (N-3), (N-1), respectivamente.

Tabela 4: Sinalização entre Registradores: Sinais do Grupo A

* a mensagem também assume esta função somente após já ter sido encaminhada para trás uma vez.

Outros:

A-2 → Cancelador de eco

A-4 → Congestionamento

Sinais do Grupo B

Estes sinais têm a função de *acknowledge* para os sinais para frente do Grupo II ou prover tarifação da chamada e informação do usuário de destino.

SINAIS	SENTIDO	OBSERVAÇÃO
B-1	←	Linha de assinante livre com tarifação.
B-2	←	Linha de assinante ocupada.
B-3, B-7 e B-8	←	Assinante com número mudado, vago, inacessível, inexistente, fora de serviço ou com defeito.
B-6	←	Linha de assinante livre com tarifação e colocar retenção sob controle do destino.
B-5	←	Linha de assinante livre sem tarifação.

Tabela 5: Sinalização entre Registradores: Sinais do Grupo B

Outros:

B-4 → Congestionamento

A mudança do Grupo I para o Grupo II ocorre quando o registrador de origem recebe o sinal para trás A3. A passagem do Grupo A para o Grupo B é determinada pela Central Destino. A Figura A.1 do Apêndice A apresenta um exemplo de uma chamada básica bem sucedida, de forma a exemplificar a utilização das principais mensagens de sinalização do protocolo R2-D.

Os problemas da sinalização CAS não são poucos, dentre os quais pode-se citar a sua baixa velocidade por ser compelida, seu fraco desempenho, pois usa bits para sinalização que poderiam ser utilizados para transportar mais canais de voz, por isso também é conhecida como *robbed-bit signalling*. Por fim, é uma sinalização muito antiga e impossibilitada de atender a novos serviços, devido à restrição quanto ao número de mensagens de sinalização que pode suportar, por isso vem sendo descontinuada e substituída pela Sinalização por Canal Comum.
Tendo em vista os fatos apresentados, uma forma de sinalização alternativa, desenvolvida pela AT&T, surge na década de 70 ao se utilizar, no suporte de transmissão, um canal específico para troca de sinalização, ou seja, o canal de voz não é mais usado para sinalização, definindo-se para este fim um canal exclusivo capaz de transportar toda a sinalização referente a várias chamadas, razão pela qual o mesmo é denominado canal comum. [2]

A Figura 3 ilustra a rede telefônica comutada exclusiva para transporte de voz, sobreposta à rede de pacotes exclusiva para sinalização. A arquitetura desta é composta por Pontos de Sinalização (PS) e Pontos de Transferência de Sinalização (PTS). O Ponto de Sinalização, normalmente associado a uma central local, constitui a porta de entrada e saída na rede de sinalização, onde os pacotes são criados (empacotados) ou recebidos (desempacotados). O Ponto de Transferência de Sinalização (PTS) é mais um elemento da rede e somente roteia mensagens de sinalização, operando como um simples comutador de pacotes, podendo ou não pertencer a uma central de comutação. [2]

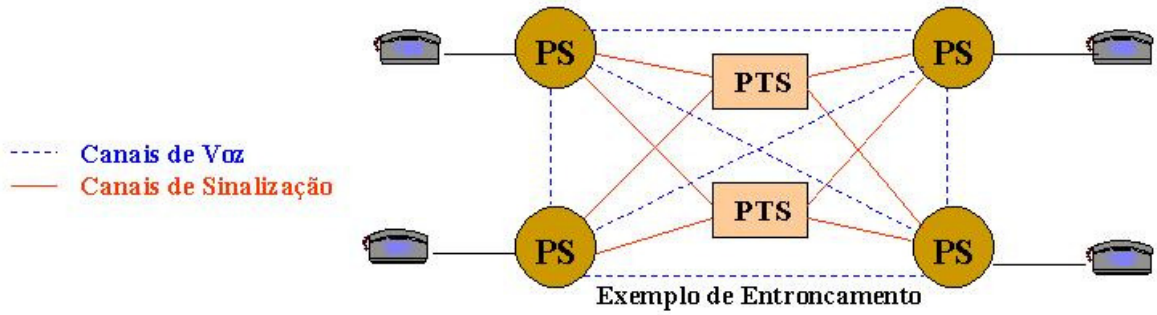


Figura 3: Topologia da Rede de Sinalização por Canal Comum

A partir desta nova proposta de sinalização, o sistema telefônico se tornou mais veloz no estabelecimento e liberação das chamadas, houve um aumento do rendimento dos circuitos de conversação e diminuição dos tempos de retenção. Outro aspecto foi a simplificação dos equipamentos de sinalização e, conseqüentemente, dos seus custos, além da possibilidade de inclusão de novos sinais de sinalização e controle, oferta de novos serviços, como os de Rede Inteligente (RI) e dados. Portanto, a proposta é realizar transferências de informações de modo confiável e na seqüência correta, sem perda ou duplicidade, tornando o sistema telefônico com elevado grau de interconectividade.

Quando comparado com a sinalização anterior, baseado no canal 16 dos sistemas de 2Mbps PCM, um canal CCS de 64Kbps é capaz de sinalizar, na prática, em torno de 1500 chamadas simultâneas. Uma desvantagem a se considerar no novo modelo é o preço das interfaces com suporte a esses tipos de sinalização em relação ao valor de placas R2-D.

Sistema de Sinalização por Canal Comum Nº 7

O Sistema de Sinalização por Canal Comum **Nº 7 (SS7)**, padronizado pelo ITU-T a partir de 1980, representou sensível evolução no processo de sinalização entre centrais telefônicas, tornando-se um sistema utilizado mundialmente, inclusive no Brasil. Deve-se observar, entretanto, que o sistema CCS N^0 7 americano (ANSI) não é compatível com o modelo nacional aqui apresentado.

Na verdade, o SS7 é um conjunto de protocolos de comunicação de dados pertencente a uma rede de pacotes, suas funções de hardware e software são divididas em níveis e

seguem o modelo de 7 camadas do Open Systems Interconnection (OSI), definido pelo International Organization for Standardization (ISO), de acordo com a Figura 4 [6].

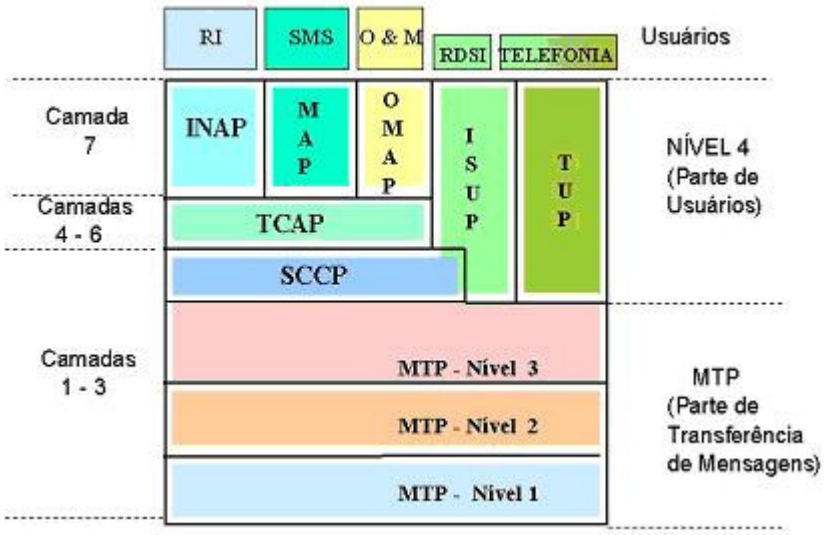


Figura 4: O Modelo de Referência OSI e a Pilha de Protocolos SS7

Consideram-se os seguintes blocos funcionais referentes às camadas de 1 à 7:

- ✓ Subsistema de Transferência de Mensagens (Message Transfer Part - MTP);
- ✓ Subsistema de Controle de Conexões de Sinalização (Signalling Connections Control Part - SCCP);
- ✓ Subsistema de Usuário Telefônico (Telephone User Part - TUP);
- ✓ Subsistema de Usuário para a RDSI (ISDN User Part - ISDN UP ou ISUP);
- ✓ Subsistema de Aplicação da Capacidade de Transações (Transaction Capabilities Application Part - TCAP);
- ✓ Protocolo de Aplicação para a Rede Inteligente (Intelligent Network Application Protocol - INAP);
- ✓ Subsistema de Aplicação para Serviço Móvel (Mobile Application Part - MAP);
- ✓ Subsistema de Aplicação de Operação e Manutenção (Operations, Maintenance Administration Part - OMAP);

O princípio fundamental da estrutura do SS7 é a divisão em funções, de um lado um Subsistema de Transferência de Mensagens (Message Transfer Part - MTP), responsável por servir como um sistema de transporte confiável para as mensagens de sinalização e, de outro lado, para os diferentes tipos de usuários, diferentes Subsistemas de Usuário (User Parts – UP ou Parte do Usuário).

O objetivo da Figura 4 é que o leitor tenha uma noção mínima do que se processa em uma rede de Sinalização de Canal Comum e suas adaptações em relação ao modelo OSI, desenvolvido originalmente para redes de computadores.

Rede Digital de Serviços Integrados

O uso da Sinalização por Canal Comum permitiu a introdução de serviços na rede telefônica como a Rede Inteligente e a Rede Digital de Serviços Integrados (RDSI). Em 1984, o grupo de estudos XVIII do antigo CCITT, hoje ITU-T, definiu a Rede Digital de Serviços Integrados (RDSI) como: “Uma rede, em geral, evoluída de uma Rede Digital Integrada Telefônica, que provê conectividade digital fim-a-fim para suportar uma gama grande de serviços, incluindo serviços de voz e de dados, na qual os usuários têm acesso através de um conjunto limitado de interfaces usuário-rede...”. [7]

A Figura 5 é derivada da Série I de Recomendações que define a RDSI; nela pode ser observada a quantidade de normas que especificam cada detalhe do padrão. [8]

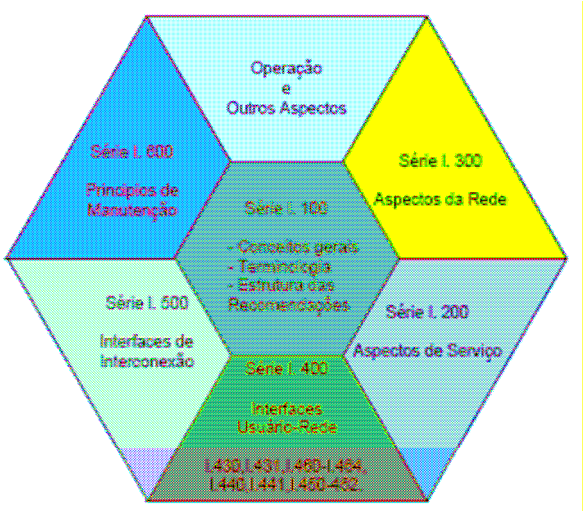


Figura 5: Mosaico da Estrutura das Recomendações RDSI

Esta tecnologia permite que centrais digitais sejam equipadas com linhas de assinantes com capacidade de transmissão de 2 canais de 64 kbps, mais um canal de sinalização de 16kbps. Esta nova configuração é chamada de BRI (Basic Rate Interface) ou 2B+D. Desta forma, o usuário dispõe de até 144 kbps, caso o canal de sinalização esteja inativo, para trafegar dados, voz e vídeo. A única restrição é que todo o tráfego em um canal D de sinalização deve ser no formato de pacotes, isto é, não pode ser utilizado para telefonia. A interface do tipo PRI (Primary Rate Interface) ou 30B+D possui trinta canais de voz de 64kbps e um canal de sinalização também do tipo D, porém este com 64kbps [6]. Essa interface é encontrada entre centrais e na ligação entre central e PABXs.

Embora o modelo OSI não sirva para representar todas as funções de protocolos necessárias em uma RDSI, o ITU-T desenvolveu um modelo de referência para a pilha de protocolos atuante em cada camada RDSI. Basicamente, o modelo é dividido em camada física, camada de enlace, seguida da camada de rede e camada de aplicação. [9] Neste estudo temos especial interesse pela camada de rede, que utiliza o protocolo definido na Recomendação Q.931, responsável pela sinalização RDSI e utilizado para estabelecer, manter e encerrar conexões nos canais de voz do tipo B.

Um dos princípios básicos das normas da RDSI tem sido a interoperabilidade. Para garantir que produtos e serviços desenvolvidos para a RDSI possam interfuncionar, a ITU-T (International Telecommunications Union – Telecommunications Services Sector) incorporou o modelo de referência OSI – Open System Interconnection da ISO, assegurando que a evolução dos protocolos se desenvolva de uma forma estruturada, sem riscos da chamada "destruição criativa", que são elevados quando falamos de um padrão mundial de uma rede de telecomunicações.

1.3.2 Sinalização DSS-1

O conjunto de recursos necessários para prover sinalização numa RDSI é chamado pelo ITU-T de Sistema de Sinalização de Assinante Digital Número 1 (DSS-1). A sinalização de controle de chamadas na interface usuário-rede da RDSI difere bastante da sinalização utilizada na operação dos sistemas telefônicos estudados anteriormente. Dentre as muitas

diferenças entre a sinalização nos dois sistemas, talvez a principal seja que a RDSI utiliza pacotes para implementar a sinalização entre os usuários e a rede.

Os conceitos da sinalização DSS-1 serão aqui apresentados devido a sua grande importância na interconexão com sistemas VoIP, pois atua no trecho Terminal ISDN - Central Local ou ainda PABX – Central Local, no caso de redes corporativas digitais. O protocolo aplica-se a interfaces PRI e tráfego assimétrico, substituindo, portanto, a Sinalização R2-D e a Sinalização entre Registradores (MFC-5C) ou, simplesmente, MFC-R2.

Este sistema de sinalização é extremamente extenso e detalhista, visto que seu conjunto de especificações tem início na norma Q.850, indo até a Q.999. O que é de real interesse para sistemas VoIP são as mensagens de sinalização definidas na Recomendação Q.931E da ITU-T, e, por conta disso, seu entendimento será mais aprofundado a seguir. Para melhor entendimento, as mensagens podem ser agrupadas de acordo com a Tabela 6.

***Mensagens para o estabelecimento da chamada*:**	***Mensagens de liberação do canal*:**
ALERTING CALL PROCEEDING CONNECT CONNECT ACKNOWLEDGE PROGRESS SETUP SETUP ACKNOWLEDGE	DISCONNECT RELEASE RELEASE COMPLETE RESTART RESTART ACKNOWLEDGE
***Mensagens para a fase de informação da chamada*:**	***Mensagens miscelâneas*:**
USER INFORMATION RESUME RESUME ACKNOWLEDGE RESUME REJECT HOLD HOLD ACKNOWLEDGE HOLD REJECT RETRIEVE RETRIEVE ACKNOWLEDGE SUSPEND SUSPEND ACKNOWLEDGE SUSPEND REJECT	INFORMATION NOTIFY SEGMENT FACILITY REGISTER NOTIFY CONGESTION CONTROL STATUS STATUS ENQUIRY

Tabela 6: Resumo das Mensagens de Sinalização do Protocolo DSS-1

A Tabela 7 apresenta o sentido e a descrição das mensagens DSS-1. [10]

MENSAGENS	*A ←→B*	*OBSERVAÇÕES*
ALERTING	←	Aviso de tom de campainha no destino. (Toque)
CALL PROCEEDING	←	Indica que a requisição de estabelecimento da chamada foi iniciada e nenhuma informação adicional de pedido de conexão será aceita. Terminal de origem deve aguardar.
CONNECT	←	Aceitação da chamada pelo destino.
CONNECT ACK	→	
DISCONNECT	←→	Esta mensagem é enviada pelo usuário para requisitar à rede o desligamento de uma conexão extremo-a-extremo.
INFORMATION	←→	Esta mensagem é enviada pelo usuário ou pela central para fornecer informações adicionais.
NOTIFY	←→	Esta mensagem é enviada pelo usuário ou pela central para indicar informação pertencente a uma chamada
PROGRESS	←	Esta mensagem é enviada pelo usuário ou pela central para indicar chamada em progresso. Mais utilizado quando na interconexão de redes com diferentes protocolos.
RELEASE	← →	Liberação do canal
RELEASE COMPLETE	→←	Término da liberação do canal.
RESUME	←	Esta mensagem é enviada pelo usuário para requisitar à rede que reassuma uma chamada suspensa.
RESUME ACK	→	
RESUME REJECT	→	Rejeição do pedido por parte da central.
RESTART	→	Retornar à posição de ocioso.
RESTART ACK	←	
SETUP	→	Esta mensagem é enviada para iniciar o estabelecimento da chamada
SETUP ACK	←	
STATUS ENQUIRY	← →	Mensagem enviada para solicitação de um status.
STATUS	← →	Esta mensagem é enviada pelo usuário ou pela central em resposta a uma mensagem de STATUS ENQUIRY ou a qualquer momento durante uma chamada para relatar certas condições de erro.
SUSPEND	← →	Esta mensagem é enviada pelo usuário para solicitar à rede a suspensão de uma chamada
SUSPEND ACK	→←	
SUSPEND REJECT	→←	
USER INFORMATION	← →	Esta mensagem é enviada pelo usuário à rede para transferir informação ao usuário remoto

Tabela 7: Mensagens da Sinalização DSS-1

A Figura A.2 do Apêndice A apresenta um exemplo de uma chamada básica bem sucedida, de forma a exemplificar a utilização das principais mensagens de sinalização do protocolo DSS-1.

1.3.3 Sinalização ISUP

A sinalização ISUP (*ISDN User Part)* define as etapas de *setup*, gerencia e liberação dos circuitos de voz e de dados fim-a-fim na rede RDSI, além de serviços suplementares em linhas RDSI e não RDSI. [11] Esta sinalização atua nos trechos entre centrais de quaisquer classes e, obviamente, chamadas originadas e terminadas na mesma central não utilizam sinalização ISUP.

A sinalização faz parte da pilha de protocolos de Nível 4 da SS7 e padronizada pelas normas Q.760–Q.769 da ITU-T. A Tabela 8 apresenta as principais mensagens e suas respectivas funções. [12], [13]

MENSAGENS	***A ←→B***	***SIGLA***	***OBSERVAÇÃO***
INITIAL ADDR. MESSAGE	→	IAM	Primeira mensagem enviada contendo dados e endereço (dígitos) de origem e destino.
SUBSEQUENT ADDR. MESSAGE	→	SAM	Mensagem enviada após o recebimento de uma IAM com endereço de destino incompleto.
ADDRESS COMPLETE MESSAGE	←	ACM	Mensagem enviada para trás indicando que todos os dados do endereço de destino foram recebidos e os recursos requisitados foram reservados. Neste momento o sinal de *ring* é enviado para a origem e para o destino.
CALL PROGRESS	←	CPG	Enviada após o recebimento da ACM, indicando a ocorrência de algum evento que deva ser informado.
CONNECT MESSAGE	←	CON	Circuito conectado
ANSWER MESSAGE	←	ANM	Mensagem de atendimento e inicio de tarifação.
RELEASE MESSAGE	←→	REL	Mensagem de liberação do canal.
RELEASE COMPLETE	←→	RLC	Mensagem de liberação completa.
SUSPEND MESSAGE	←→	SUS	Mensagem de desconexão temporária.

RESUME MESSAGE	←→	RES	Reassumir a chamada, informando que houve a reconexão por parte de quem desconectou antes a chamada.

Tabela 8: Mensagens da Sinalização ISUP

A Figura A.3 do Apêndice A apresenta um exemplo de uma chamada básica bem sucedida, de forma a exemplificar a utilização das principais mensagens de sinalização do protocolo ISUP.

Neste ponto, se encerra a avaliação dos principais protocolos de sinalização da rede telefônica tradicional de interesse para este estudo, podendo ser considerada desde então uma rede de ótima qualidade, altamente confiável, segura e que agrega vários tipos de dados a altas taxas. A Figura 6 ilustra um resumo das sinalizações abordadas, identificando o contexto de aplicação de cada protocolo neste trabalho. Essa rede, tradicional, está sendo usada para veicular VoIP, usando-se, para a interconexão, um Gateway.

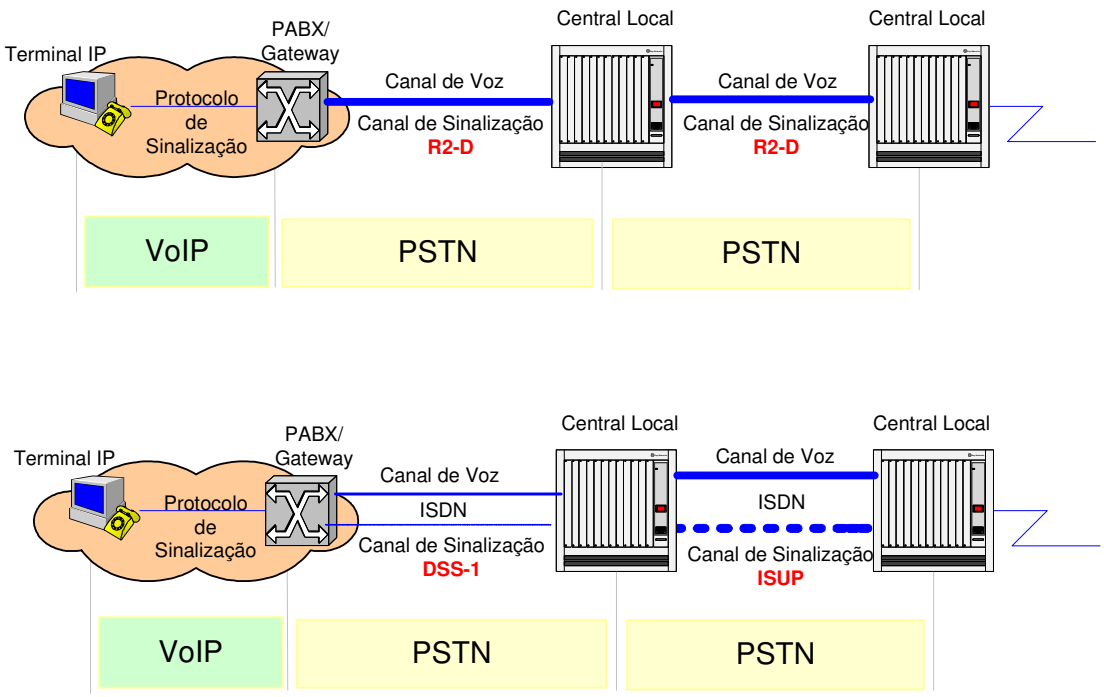


Figura 6: Integração VoIP com Rede Telefônica

1.3.4 Protocolo H.323

O padrão H.323, criado em 1996 pela ITU-T, surge no momento em que seu grupo de estudos adquiriu grande experiência durante o desenvolvimento do seu protocolo precursor, o H.320, cujo objetivo era permitir conferências multimídia para redes RDSI. Em 1998 e 1999, o ITU-T aprova as versões 2 e 3 do padrão H.323 e com elas surgem o *H.245 Tunneling* e *Fast Connect*, buscando maior agilidade e leveza do protocolo. A versão 4, lançada em 2000, trouxe melhorias nos aspectos de confiabilidade, escalabilidade e flexibilidade. A experiência do grupo no protocolo H.320 explica o alto grau de interoperabilidade do H.323 com os protocolos de sinalização RDSI [14].

O conjunto de recomendações que fazem parte do padrão H.323 descreve Terminais, equipamentos, serviços e procedimentos para comunicações multimídia sobre redes LAN e IP em tempo real [15]. A Figura 7 apresenta os protocolos de sinalização para dados, voz e vídeo que fazem parte do padrão.

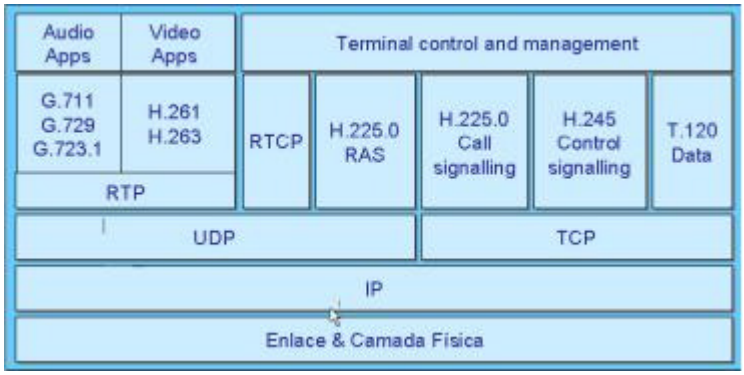


Figura 7: Stack de protocolos do padrão H.323

Analisando somente a porção referente à telefonia IP da Figura 7, o padrão consiste basicamente de três protocolos para sinalização de chamadas, além das especificações de CODECs de áudio, que não serão analisados neste trabalho.

O protocolo RTP (Real Time Protocol) é utilizado para o encapsulamento das mídias de áudio e vídeo adequados para operação em conjunto com protocolos e aplicações de tempo real, como H.323. A utilização deste protocolo se torna importante na medida em que

substitui o controle do TCP por uma solução mais simples, fornecendo informações importantes para os elementos de rede referentes à chamada, como informações de seqüência de pacotes, *timestamp* e tipo de mídia, proporcionando aos dispositivos a realização do controle de fluxo e de congestionamento. Entretanto, o padrão não efetua reserva de recurso, nem mesmo garante a qualidade de serviços. [16] Um protocolo suplementar foi desenvolvido para controle de entrega dos dados e perda de pacotes, denominado RTCP (Real Time Control Protocol). Tanto o RTP quanto o RTCP utilizam o protocolo UDP para o envio das informações pela rede.

O protocolo RTCP se baseia na transmissão periódica de pacotes para todos os participantes de uma sessão RTP, usando o mesmo mecanismo de distribuição dos pacotes de dados. Através da abertura de portas UDP, o RTCP provê um retorno da qualidade da distribuição de dados que pode ser utilizado para controle ou codificação adaptativa durante uma sessão RTP. [16]

Protocolo H.225 (RAS)

Protocolo responsável pela sinalização dos eventos de Registro, Admissão e Status (RAS). Este protocolo é independente de qualquer outro e estabelece o primeiro canal de sinalização, antes que qualquer outro canal tenha sido estabelecido previamente. Atua sobre conexões não confiáveis (UDP) e utiliza a porta *default* 1719 [17]. Todas as portas utilizadas pelo padrão são registradas no Internet Assigned Numbers Authority (IANA).

Protocolo H.225 *Call Signalling*

Protocolo responsável pela sinalização da chamada propriamente dita, utilizada para conectar, manter e desconectar chamadas entre Terminais. [17] Suas mensagens são provenientes do protocolo Q.931, camada 3 do protocolo de sinalização para interfaces de rede RDSI, que foram ambientadas e evoluídas para a arquitetura H.323.

As mensagens de sinalização de chamada podem utilizar tanto o protocolo TCP quanto o UDP e porta de destino *default* 1720. A partir da segunda versão do protocolo, a norma recomenda o uso de TCP para este canal de sinalização. [17]

Protocolo H.245 *Control Signalling*

Protocolo responsável pela abertura do canal confiável de áudio. Utiliza o protocolo TCP e portas alocadas dinamicamente, geralmente 1731, para cada canal lógico responsável pelo tráfego de sinalização da chamada. Os canais lógicos são unidirecionais, sendo necessário, portanto, a abertura de dois canais para uma conversação. [18]

O protocolo H.245 também é responsável pelo controle de fluxo da comunicação, visto que a taxa de transmissão é variável em função do controle realizado pelo RTCP. A troca de capacidades entre Terminais também ocorre neste canal de controle.

A arquitetura H.323 é composta por Terminais inteligentes que provêem a codificação da voz e interface de rede, sendo suficientes para realizar uma chamada. Os Gateways de Mídia são utilizados para os casos de interconexão H.323 – STFC ou H.323 – SIP, por exemplo. A Unidade de Controle Multiponto (MCU) é outro equipamento da rede utilizado para suporte e gerência de conferências multiponto. O Gatekeeper completa a arquitetura H.323, sendo responsável pela tradução de endereços e resolução de nomes, controle de admissão, controle de uso de banda, gerenciamento de zonas geográficas e criptografia. Este elemento não é de uso obrigatório na rede H.323, porém é muito útil no controle e roteamento de chamadas de redes corporativas e para segurança e autenticação de usuários.

A Figura 8 apresenta uma arquitetura H.323 bem abrangente, pois ilustra a interconexão de Terminais através da internet e a interligação com a rede pública de telefonia.

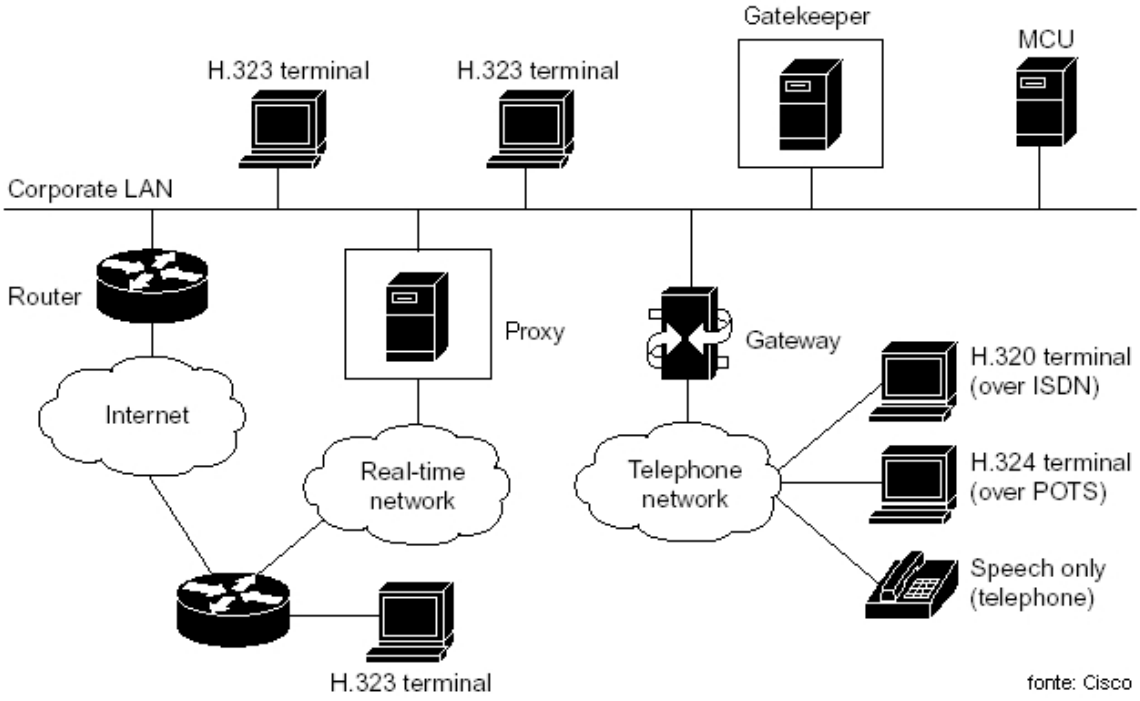


Figura 8: Arquitetura H.323

A quantidade de mensagens de sinalização para o tráfego de voz do protocolo H.323 é muito grande e por isso não serão abordadas neste trabalho. A Figura A.4 do Apêndice A apresenta um exemplo de uma chamada básica bem sucedida, de forma a exemplificar a utilização das principais mensagens de sinalização do protocolo. As mensagens utilizadas no exemplo foram comentadas, e apesar da existência de várias outras mensagens não citadas, o objetivo é mostrar a complexidade para estabelecer e encerrar um único canal de áudio bidirecional. Ainda que o padrão H.323 tenha evoluído e reduzido o número de mensagens necessárias para uma chamada, através principalmente dos métodos *Fast Connect* e *H.245 Tunneling*, resumidos no Apêndice A, o protocolo se apresenta desde o seu inicio como uma estrutura complexa e desnecessária para redes locais.

Tendo em vista os fatos apresentados acima, o protocolo H.323 é um sistema híbrido construído a partir de elementos inteligentes, como Gatekeepers e MCUs e Terminais. Apesar de estar em sua quinta versão, ainda há questões que surgem como problemas no protocolo, como seu longo tempo para estabelecer canais de mídia, muitas funções requeridas e centralizadas pelo Gatekeeper e pouca escalabilidade. A ausência de um padrão para aplicações VoIP nas primeiras versões do protocolo contribuiu para a

incompatibilidade dos equipamentos entre os diversos fornecedores. Por fim, o protocolo H.323 será útil como base de comparação com sistemas mais modernos, como o protocolo SIP, tema do próximo capítulo.

Este capítulo apresentou os principais protocolos de sinalização da rede de telefonia fixa comutada, com objetivo de realizar a integração futura com os protocolos de sinalização da telefonia IP. Também apresentou o protocolo H.323 como base para a evolução e desenvolvimento da tecnologia das redes VoIP.

A composição do restante deste trabalho é a seguinte: os Capítulos 2 e 3 são referentes à sinalização de chamadas SIP e MGCP, respectivamente. Ambos apresentam um estudo essencialmente baseado nas normas internacionais, onde são identificados pontos importantes para a avaliação de funcionamento de equipamentos e soluções VoIP. Cada capítulo apresenta uma descrição sumária do método desenvolvido para elaboração dos testes de conformidade, baseada não apenas nos estudos teóricos, mas também levando em conta os resultados práticos a serem obtidos.

O Capítulo 4 busca identificar alguns cenários para a sinalização em redes VoIP e apresenta uma conclusão geral sobre os protocolos abordados nos capítulos anteriores.

2. Protocolo SIP

O *Session Initiation Protocol* (SIP) ou Protocolo de Iniciação de Sessão é um dos mais recentes protocolos de controle de sinalização da camada de aplicação do modelo OSI, desenvolvido pela Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group como uma alternativa à especificação ITU-T H.323. O SIP se originou em meados dos anos 90 e foi primeiramente especificado em março de 1999, através da RFC 2543 e concebido para estabelecer, manter e terminar sessões multimídia em redes IP e, especialmente, sobre a Internet. [19]. Este trabalho já se baseia nas melhorias publicadas na nova recomendação, a RFC 3261, vigente desde maio de 2002.

Ao longo do texto o leitor poderá entender os padrões e as restrições de operação do protocolo, identificando as dificuldades encontradas para elaboração do Roteiro de Testes. A descrição da elaboração dos testes, dificuldades e soluções é uma contribuição original deste trabalho. Além dos limites teóricos impostos pelas normas, o capítulo também considera os aspectos práticos relevantes. Alguns testes foram selecionados como exemplo e foram transcritos neste capítulo.

O protocolo é relativamente simples, em seu funcionamento, implementação e configuração, quando comparado aos do capítulo anterior, especialmente o H.323. Estes fatores já seriam suficientes para explicar sua importância e a rápida penetração em qualquer mercado, tanto do ponto de vista do fabricante, como da operadora ou do usuário final. Por isso, o capítulo também aborda os procedimentos de testes relativos ao protocolo SDP (*Session Description Protocol*), já que atua em conjunto com o SIP e será responsável por especificar e compatibilizar as características de áudio das partes de uma chamada.

A flexibilidade oferecida pelo SIP vem do fato de que o protocolo não se importa com o tipo de mídia transportada durante uma sessão, podendo ser áudio, vídeo, texto, figura, etc; nem com o tipo de protocolo da camada de transporte usado para transferência da mídia, se TCP ou UDP. O SIP pode executar ainda sobre ATM, AAL5, IPX, X.25, sem mudanças para o protocolo. O H.323 requer o uso de um protocolo de transporte confiável.

Estas características são muito úteis no desenvolvimento de soluções customizadas e que devem ser avaliadas sempre que impactarem no interfuncionamento de equipamentos entre diferentes fabricantes, visto que quase sempre estas facilidades são perdidas nos casos de interfuncionamento.

2.1 Arquitetura

A Figura 9 apresenta uma rede SIP, que será utilizada como referência ao longo do capítulo e também para todas as simulações. O cenário é composto por dois domínios SIP, caracterizados por Servidores Proxy. O Domínio 1 é composto por dois Terminais SIP, além do Servidor Proxy, enquanto que o Domínio 2 é composto apenas por um Terminal SIP e também pelo seu Servidor Proxy. O Servidor de Registro e o Servidor de Redirecionamento pertencem a uma zona de intersessão, visto que podem ser requisitados por ambos os domínios. A interligação com a rede PSTN através de um Gateway é apenas ilustrativa e será mais bem esclarecida quando mencionados os aspectos de regulamentação do protocolo no Brasil.

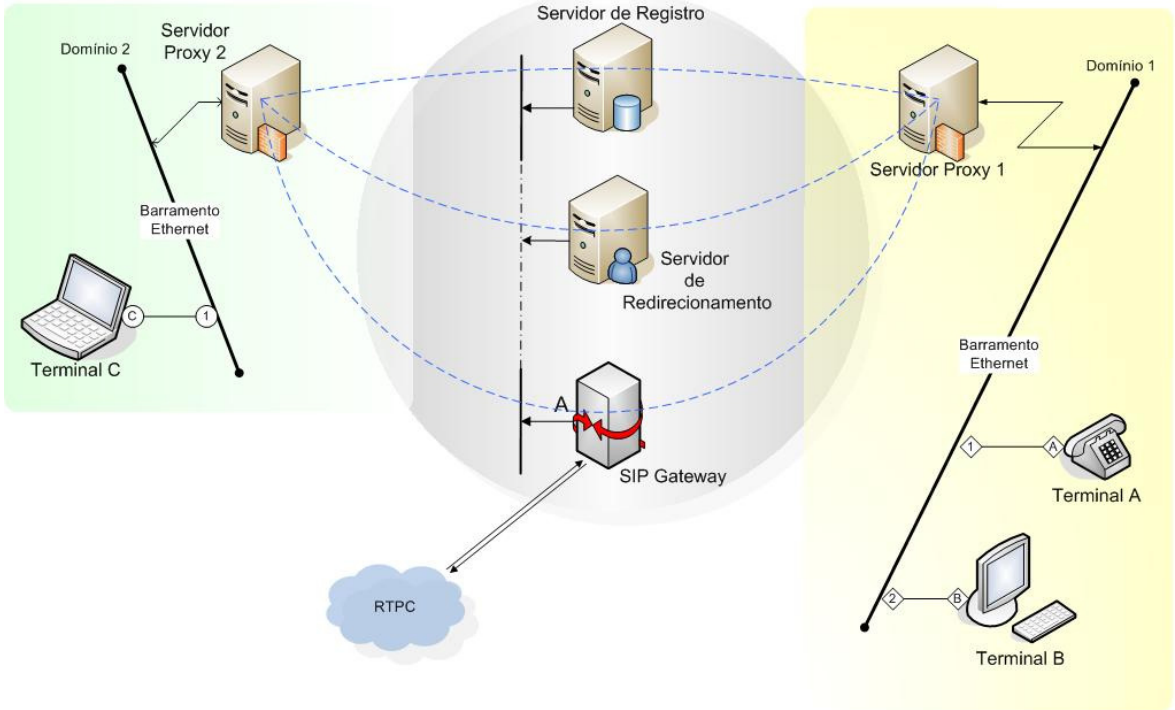


Figura 9: Arquitetura de Referência SIP

A seguir, os principais elementos da topologia da Figura 9 serão analisados:

Servidor de Registro

A atuação do Servidor de Registro abrange a criação, manutenção, finalização e alteração de um registro SIP. Na arquitetura da Figura 9, o Servidor de Registro é responsável pelo registro de terminais e por manter a informação de localização atualizada de cada usuário, isto é, possui o mapeamento entre endereços SIP e endereços IP de cada *host*. Para isso, o terminal envia uma mensagem de sinalização REGISTER, ainda não definida no capítulo, com valor de Time To Live (TTL) igual a 1 obrigatoriamente, limitando, dessa forma, o método de descoberta do Servidor de Registro à sub-rede local à qual o Terminal pertence [19]. Esta característica é equivalente ao método de descoberta do Gatekeeper que é usado nas redes H.323.

Cada terminal pode ser configurado manualmente com o endereço do Servidor de Registro, ou se registrar através de uma mensagem *broadcast*, cujo endereço *default* é 224.0.1.175, recebendo seu endereço na mensagem de resposta. Além disso, cada cliente pode ter seu registro em múltiplos servidores e um dado cliente pode ter múltiplos registros num único servidor. Neste último caso, se o usuário tiver múltiplos registros ativos e receber uma chamada, todos os destinos registrados receberão sinais de campainha simultaneamente.

O estado registrado não é permanente e deve ser atualizado em um período de tempo configurado na rede SIP. O valor *default* é de uma hora, como especificado no campo de cabeçalho *EXPIRES*, que será visto a seguir. Por outro lado, o registro também pode ser cancelado e é importante notar como o Servidor se comporta e interpreta tal pedido, que também é feito através da mensagem REGISTER, com parâmetros adequados. O Servidor de Registro também pode acumular a função de Servidor Proxy.

Portanto, a verificação dos parâmetros definidos nestas considerações é o mais importante e essencial para operação de um Servidor de Registro, conforme recomendação do padrão. Alguns aspectos de obsolescência relativos à antiga recomendação, RFC 2543, também devem ser criticados durante a avaliação deste tipo de servidor.

Servidor Proxy

O protocolo SIP faz uso de elementos chamados Servidores Proxy para auxiliar no roteamento de pedidos para a atual localização do usuário, autenticação e autorização de serviços. Os servidores implementam políticas de roteamento de chamadas e provêem recursos para os usuários, apesar de serem elementos opcionais na rede [20].

O Servidor Proxy age como servidor por um lado, recebendo e tratando requisições, e como cliente por outro, encaminhando pedidos para outros Servidores ou até mesmo diretamente para os terminais. Por isso, apesar de o SIP ser um protocolo do paradigma cliente/servidor, todo elemento assume ora funções de cliente, ora de servidor.

A entidade atua como roteador na rede determinando qual será o próximo *hop*, podendo ser o próprio usuário final, outro Servidor Proxy ou um Servidor de Redirecionamento, ou seja, este elemento de rede tem a autonomia de rotear apenas mensagens sem modificá-las, ou pode modificar alguns parâmetros antes de reencaminhá-las, ou ainda enviar uma resposta gerada localmente, como 100 TRYING, que será abordada mais adiante.

O Servidor Proxy pode rotear toda a sinalização da chamada ou simplesmente rotear a fase inicial de abertura de canal, caracterizada pelo conjunto de mensagens que faz parte da mensagem INVITE e, após, deixar que os terminais troquem outras mensagens de sinalização e a mídia diretamente. Este último procedimento é o ideal para a redução da alocação de recursos no servidor, na rede e para a redução do tempo de retenção de mensagens de sinalização durante a chamada; no entanto, a figura do Servidor Proxy é importante no roteamento de toda a sinalização quando atuando na implementação de serviços avançados.

O padrão requer que o Servidor Proxy seja capaz de realizar determinadas decisões de roteamento de mensagens e roteamento programável em função do serviço, processo conhecido como *forking*. Importante observar que o Proxy também determina o endereço, porta e protocolo de transporte quando encaminha qualquer pedido, dependendo de sua configuração.

Outra característica importante de operação deste tipo de Servidor é que pode operar em dois modos de comunicação diferentes, o modo *stateful* e/ou o modo *stateless*. A mesma funcionalidade é encontrada no Gatekeeper em redes H.323.

O servidor SIP *stateless* é uma entidade lógica que não mantém o estado de transação do cliente ou servidor quando processa pedidos, ou seja, o Proxy recebe as chamadas, realiza qualquer que seja a translação da mensagem e a encaminha convenientemente, não armazenando qualquer registro deste evento. Neste caso, a mensagem retransmitida pelo Proxy *stateless* tem que ser encaminhada exatamente da mesma forma que o pedido original. Portanto, quando *stateless*, um Proxy age como um simples elemento de encaminhamento de pedidos, descartando informações sobre as mensagens, uma vez que elas tenham sido retransmitidas. Desta forma, não é capaz de gerar suas próprias respostas, ainda que temporárias, isto é, do tipo 1xx, como será visto no tópico relacionado às mensagens SIP [19].

O Proxy *stateful* é uma entidade lógica que mantém o estado de clientes e servidores durante o processamento de um pedido, armazenando a informação de chegada da mensagem e o respectivo encaminhamento e, desta forma, é mais inteligente em pedidos subseqüentes e respostas relacionadas a uma mesma sessão, podendo modificar o processamento de futuras mensagens associadas àquele pedido. Qualquer pedido que seja encaminhado para mais de uma localidade tem que ser tratado por esse servidor; isto pode acontecer se um terminal está registrado em mais de um Servidor de Registro, por exemplo [20]. O armazenamento de informações de roteamento de mensagens de sinalização também pode ser bastante útil na retenção de informações com a finalidade de contabilidade / faturamento para tarifação, por exemplo.

Quando um ambiente real é levado em consideração, o Servidor Proxy é sempre do tipo *stateful*, pois atuam como roteadores das mensagens de sinalização e possivelmente do canal de mídia, além de realizar a função de tarifação, armazenador do estado da chamada e dos terminais, e praticam todas as mensagens de sinalização que serão enunciadas a seguir. Em contrapartida, um ambiente com uma grande quantidade de chamadas simultâneas, pode implicar em um sério problema de performance. Por isso, um servidor Proxy do tipo s*tateless* pode ser usado se não em toda a rede SIP, em pelo menos alguns

setores da rede, que, ao contrário do servidor s*tateful*, não é capaz de gerar nenhuma decisão própria e não altera qualquer cabeçalho nas mensagens, com exceção do cabeçalho *VIA*, já que este é necessário para o encaminhamento das mensagens de sinalização, como veremos adiante. O Gatekeeper H.323 é sempre *stateful*, mantendo controle do estado da chamada durante toda a sua duração.

Alguns testes foram propostos com o objetivo de analisar o comportamento de funcionamento do servidor *stateful* numa rede SIP, pois não deve ser ignorada a sua utilidade em casos de encaminhamento de chamadas não autenticadas e redução de processamento a bordo, por exemplo.

Um servidor Proxy pode chavear para operação em modo *stateless* a qualquer tempo durante o processamento de um pedido, desde que não tenha realizado nenhuma função prévia como servidor *stateful*.

A avaliação de conformidade de uma determinada solução SIP com o padrão do protocolo não foi desenvolvida levando-se em conta exclusivamente as funcionalidades dos Servidores ou Terminais pertencentes à rede, mas a proposta é avaliar a implementação das mensagens de sinalização do protocolo como um todo, sendo estas iniciadas ou destinadas a um terminal ou a qualquer um dos Servidores.

Servidor de Redirecionamento

A principal função do Servidor de Redirecionamento é a resolução de nomes e localização de terminais, proporcionando grande flexibilidade e mobilidade à rede SIP. A partir dessa entidade, qualquer usuário é capaz de realizar ou receber uma chamada de qualquer localidade, desde que origem e destino estejam devidamente registrados na rede, ainda que fora de seu domínio original.

O Servidor de Redirecionamento realiza papel semelhante ao do Gatekeeper em redes H.323 e se caracteriza por não aceitar chamadas, nem mesmo processar ou encaminhar pedidos SIP, mas apenas retornam informação de localização do terminal de destino ou Servidor Proxy competente, baseado em sua tabela de rotas. O terminal de origem, de

posse dessa informação, é capaz de contatar diretamente a entidade requerida. A Figura A.6 do Apêndice A ilustra um exemplo de traçado de uma chamada redirecionada, que será mais bem interpretada após a introdução das mensagens de sinalização do protocolo.

Em algumas arquiteturas, pode ser desejável contar com Servidores de Redirecionamento para reduzir o processamento de carga nos Servidores Proxy, com o objetivo de aumentar a robustez da rede de sinalização. Isto é realizado transferindo os Servidores de Redirecionamento para a borda da rede SIP, enquanto que os Servidores Proxy se encontram no núcleo. A cada pedido entrante na rede, o Redirecionamento é responsável por identificar o Proxy adequado por tratar aquele pedido e informar ao originador da chamada o endereço do Servidor Proxy com o qual todas as mensagens futuras serão trocadas diretamente, permitindo, portanto, considerável escalabilidade na rede.

Para efeitos de análise desse Servidor, é importante observar se o funcionamento acima descrito é verdadeiro. Este modo de operação é bastante particular do protocolo SIP e muitas vezes pode ser entendido como um modelo teórico de funcionamento ou um modelo didático de apresentação do sistema, pois as implementações dessa funcionalidade costumam ser um pouco diferentes do especificado no padrão.

Terminais

O Terminal do protocolo SIP é inteligente, pois é capaz de armazenar e gerenciar situações de chamada. O terminal do usuário pode aceitar e receber chamadas de outro terminal sem a necessidade de nenhum outro elemento da arquitetura SIP. Os terminais podem ser aparelhos DTMF comuns; neste caso é necessária a utilização de uma Gateway (ATA) ou até um PABX IP para interface entre a Sinalização SIP e Sinalização de Usuário, vista no capítulo anterior. O telefone IP é outro tipo de terminal; e ainda há a possibilidade de utilização de um *softphone*, que é um software capaz de emular um aparelho telefônico IP. Os testes em SIP utilizam s*oftphones* e telefones IP/SIP, de acordo com a disponibilidade do laboratório e necessidade para avaliar o protocolo.

Gateway

O Gateway atua como uma interface de mídia em que eventuais diferenças, como a versão do protocolo SIP em funcionamento em cada terminal, interface com outros protocolos de voz, ou demais características físicas do aparelho, podem ser corrigidas ou contornadas. Outros serviços, como secretária eletrônica, mensagens remotas em resposta a requisições do usuário e possíveis erros do sistema podem ser providos por este elemento.

2.2 Endereçamento

Conhecido como SIP *Universal Resource Indicators* (URIs), o endereçamento SIP é composto por nomes e fazem referência a uma entidade abstrata, podendo ser um terminal ou um Servidor. O formato geral da URI é sip:user@host ou sips:user@host, similar ao endereço de e-mail, porém com uma sutil diferença de sintaxe, isto é, o e-mail é da forma mailto:user@host e é baseado na *Uniform Resource Locator* (URL), mas a idéia dos dois é a mesma. [20]

O campo *user* pode representar o *username* do cliente, o próprio número de telefone na rede IP, ou até mesmo um número válido no sistema telefônico atual, visto que pode endereçar números telefônicos através de um Gateway PSTN [21]. O campo *hos*t pode referir-se tanto ao nome do domínio quanto ao endereço numérico Ipv4 ou Ipv6.

A avaliação de uma URI SIP deve ser feita por completo, visto que possibilita especificar um número de porta, protocolo de transporte, endereço *multicast*, assunto da mensagem, tipo de mídia e também sessões de emergência [19]. A forma completa é apresentada a seguir:

sip: user:password@host:port;uri-parameters?headers

Todos os parâmetros adicionais diferentes dos necessários para o endereçamento básico (user@host) são considerados opcionais pela norma. Apesar de o uso do campo *password*

ser permitido pela sintaxe URI, seu uso não é recomendado porque a passagem da informação de autenticação em texto tem provado ser um risco de segurança em quase todos os casos onde tem sido utilizado.

O campo *uri-parameters* assume a sintaxe: "nome_parâmetro = valor_parâmetro" e inclui os parâmetros*: transport, maddr, ttl, user, method,* e *lr*. Com destaque para o parâmetro *maddr*, que indica o endereço do servidor que precisa ser contatado para se alcançar o destinatário, sendo desprezado qualquer endereço derivado do campo do *host*. Quando um parâmetro *maddr* está presente, os valores de porta aplicam-se ao endereço indicado no campo *maddr*. Isto permite que a URI especifique um Servidor Proxy que precisa ser utilizado para o roteamento da mensagem até o destino final. O parâmetro *transport* determina o mecanismo de transporte a ser utilizado para envio de mensagens. SIP pode utilizar qualquer protocolo da camada de transporte, como UDP (User Datagram Protocol), RFC 768, TCP (Transmission Control Protocol), RFC 761 ou SCTP (Stream Control Transmission Protocol), RFC 2960. O protocolo SIP possui um valor padrão para a porta de comunicação de sinalização (campo *port*), estabelecido como sendo 5060, independente do protocolo de transporte configurado. Os demais parâmetros *ttl, user, method,* e *lr* serão abordados convenientemente ao longo deste capítulo.

O campo *headers,* também presente na string de endereço e separada pelo caractere "?" dos demais campos, permite a inclusão de cabeçalhos em qualquer requisição construída numa estrutura URI. Os campos de cabeçalho SIP são similares aos campos de cabeçalho HTTP (Hypertext Transfer Protocol), RFC 2616, tanto na sintaxe quanto na semântica. [19]

Tendo em vista os fatos apresentados acima, é necessário verificar se o equipamento SIP tem suporte a todos os campos de uma URI apresentados acima e como definidos pelo padrão. Neste caso, também se torna necessário verificar a resposta da rede caso determinado equipamento apresente um esquema não entendido pelo restante dos seus elementos, devendo rejeitar a requisição com o código de resposta de erro do tipo *416 Unsupported URI Scheme*, por exemplo.

2.3 Sinalização SIP

Toda a comunicação SIP se baseia em apenas dois grandes grupos de mensagens de sinalização, os pedidos e as respectivas respostas. A sintaxe das mensagens é baseada em texto e idêntica ao HTTP, isto é, ambos são protocolos da camada de aplicação do modelo OSI e possuem objetividade e rapidez necessárias para suportar sistemas de informação distribuídos cooperativos de hipermídia [19]. Já as mensagens H.323 possuem representação binária para cada campo, dificultando muito o entendimento visual rápido do protocolo. A estrutura textual dos campos SIP permite que novas características sejam incluídas de forma fácil e compatível com as versões anteriores. Os novos campos ou parâmetros podem ser colocados em qualquer parte da mensagem. Já no H.323, existem alguns locais predefinidos para inclusões futuras. Um exemplo de teste que pode ser praticado para avaliação da sintaxe das mensagens do protocolo SIP pode ser observado no Teste 1 do Apêndice B.

As mensagens SIP podem incluir campos opcionais com conteúdos não padronizados, de forma a conter as especificações e características de cada terminal da rede. Este recurso possibilita aos usuários a troca de informações configuradas de forma muito particular, como, por exemplo, quando um terminal recebe uma chamada e encontra-se indisponível, ele é capaz de informar ao originador da chamada o seu horário de retorno. Isto permite que o próprio terminal de destino retorne a ligação de forma automática na hora programada, informando que o usuário para quem ligou está disponível. Neste sentido, deve-se observar e entender estas facilidades customizadas, com objetivo de avaliar o impacto na rede e o grau de interoperabilidade com os demais equipamentos que operam de acordo com o padrão do protocolo, ou seja, sem funcionalidades proprietárias.

A Recomendação não menciona todos os serviços suportados pelo protocolo, uma vez que se torna impossível tal análise e isto vai de encontro às premissas de criação do protocolo, pois o SIP não provê serviços, mas provê primitivas que podem ser usadas para implementar diferentes serviços.

A Figura A.5 do Apêndice A tem a intenção de exemplificar um fluxo de sinalização típico do protocolo SIP, basicamente para comparação direta com o mesmo fluxo de

comunicação do protocolo H.323 necessário para a criação e encerramento de uma chamada básica bem sucedida. Esse tipo de comparação torna clara a simplicidade da sinalização SIP para abertura de canais de áudio e sua fácil adaptação aos padrões Internet, visto que é um ambiente não totalmente controlado, principalmente em relação à variação do caminho percorrido durante uma transmissão, assim como a características de tráfego desconhecidas e variáveis, apesar de ambos os padrões precisarem de outros protocolos de reserva de recurso ou políticas de prioridades para garantir a qualidade de serviço. Mesmo em ambientes controlados como no caso de uma LAN, o padrão SIP ainda apresenta maior escalabilidade.

2.3.1 Mensagens SIP

Neste momento, o objetivo é apresentar de forma sucinta todas as mensagens de sinalização previstas no protocolo SIP [19], considerando a elaboração dos procedimentos de teste. A literatura também adota os termos “pedido”, “requisição” e “método” quando fazem referência às mensagens SIP. Portanto, a mensagem INVITE pode ser referenciada tanto como pedido INVITE, requisição INVITE quanto método INVITE, por exemplo. Todas estas nomenclaturas são adequadas e também serão utilizadas neste capítulo.

I. INVITE

O método INVITE é uma parte crítica do padrão SIP e talvez represente a mensagem mais importante do protocolo. A mensagem indica que um usuário ou um serviço está sendo convidado a participar de uma sessão de chamada. A mensagem é responsável não apenas pela iniciação de uma sessão, mas também é responsável por modificá-la depois ou mesmo antes de estabelecida.

II. ACK

Esta mensagem é um pedido enviado pelo originador da chamada confirmando o recebimento de uma resposta final a um pedido INVITE. Requisições ACK são usadas para assegurar que todas as mensagens SIP foram apropriadamente recebidas pelos

elementos SIP envolvidos. A partir deste momento, as partes da chamada podem trocar mídia. Importante notar, nos testes, o comportamento da rede quando ocorre um *timeout* da requisição ACK, em relação às mensagens subseqüentes e os tempos de espera.

III. BYE

O pedido BYE é usado para terminar sessões SIP. Além dos Terminais participantes de uma sessão de áudio, o Servidor Proxy também tem a autonomia de terminar uma chamada através desta mensagem. Desde que uma sessão contenha um ou mais diálogos, um pedido BYE é sempre enviado e deve ser seguido por uma resposta *200 OK*, porém, se o Servidor não responde ou responde com um erro à requisição BYE, a sessão deve ainda ser considerada terminada.

Importante observar, nos testes, se a mensagem BYE referencia corretamente o diálogo que pretende encerrar dentre outros que existam em uma mesma sessão e analisar os casos de referência errada. Não menos importante é observar as modificações de implementação em relação à recomendação anterior à vigente.

IV. CANCEL

Habilita o cancelamento de qualquer mensagem em progresso ou que não tenha tido resposta. Assim como o método BYE, este comando pode ser originado tanto de um terminal quanto de um Servidor. Nos testes, é importante adotar a premissa de que a mensagem CANCEL fará referência apenas aos pedidos INVITE, visto que estes são os únicos utilizados para estabelecer uma sessão.

O comando é eficaz quando se deseja cancelar uma chamada antes de ser completada e quando há processos concorrentes na rede e um deles foi bem sucedido. Nos testes, é importante observar que requisições CANCEL disparam duas respostas quando enviadas a um Servidor: uma resposta do tipo *487 Request Terminated* para o INVITE original e uma resposta *200 OK* para o próprio pedido CANCEL. Notar a coerência dos cabeçalhos do pedido CANCEL aos do INVITE ao qual faz referência.

V. OPTIONS

Esta mensagem possibilita a qualquer usuário pesquisar e coletar capacidades dos Servidores ou de outros terminais SIP, que poderão ser convidados a participar de uma sessão. O pedido é feito para coletar informações de suas capacidades, como CODEC e banda disponível, serviços e extensões a que dá suporte, implementar um recurso de *traceroute*, permitindo a um cliente ver que caminho suas mensagens SIP podem percorrer para um determinado destino, etc. A mensagem não é usada para estabelecer uma sessão e é particularmente útil em relação à troca de capacidades. Deve-se observar o fato de que todos os elementos de rede são obrigados a suportar o método OPTIONS.

O teste de recebimento de mensagens OPTIONS é simples, mas freqüentemente a geração destas requisições iniciada pelo usuário não é permitida pelos Servidores e alguns outros tipos de terminais. A resposta gerada pelo Servidor Proxy deve ser do tipo *200 OK* e deve conter uma listagem de capacidades do servidor.

VI. REGISTER

Mensagem utilizada para autenticação dos terminais, estando intimamente ligada às funções do Servidor de Registro.

VII. INFO

A mensagem INFO realiza a transferência de qualquer informação durante uma chamada em progresso. O pedido INFO é flexível e não define o tipo de dado que pode ou não ser transmitido; fundamentalmente, tem o propósito de transportar informações de nível de aplicação ao longo do caminho de sinalização SIP, não sendo utilizado para modificar o estado de uma chamada ou os parâmetros iniciados na sessão [22].

O sentido desta mensagem está associado à transferência de dígitos DTMF *in band*, à transferência de mensagens de sinalização geradas por outras redes de telefonia, casos em que o assinante possui uma conta pré-paga e deseja receber informações sobre seus créditos restantes simultaneamente enquanto conversa, ao transporte de dados como

imagens, ou a qualquer outra informação diferente de *streaming* de voz entre participantes de uma sessão. Também poderá ser usado em aplicações diferentes de telefonia, como em uma conversação de texto, onde essas informações serão transportadas geralmente no corpo da mensagem, embora possam ser transportadas em cabeçalhos da mensagem INFO, que serão introduzidos na seção "3.5 Cabeçalhos SIP".

VIII. SUBSCRIBE

A mensagem SUBSCRIBE proporciona expansão na estrutura de comunicação entre terminais. O conceito geral é que entidades na rede possam solicitar recursos ou estado de uma chamada e também possam enviar notificações a partir de qualquer mudança de estado [23].

A cada solicitação submetida a um Terminal ou Servidor da rede, a mensagem SUBSCRIBE tem um período de validade que deve ser atualizado através do reenvio de uma nova mensagem do mesmo tipo a qualquer momento dentro desse intervalo de tempo. O Terminal do usuário é o responsável por incluir o cabeçalho *EVENT* na mensagem, informando qual evento ou classe de eventos está solicitando.

Um exemplo típico de fluxo de comunicação deste método pode ser visualizado através da Figura 10.

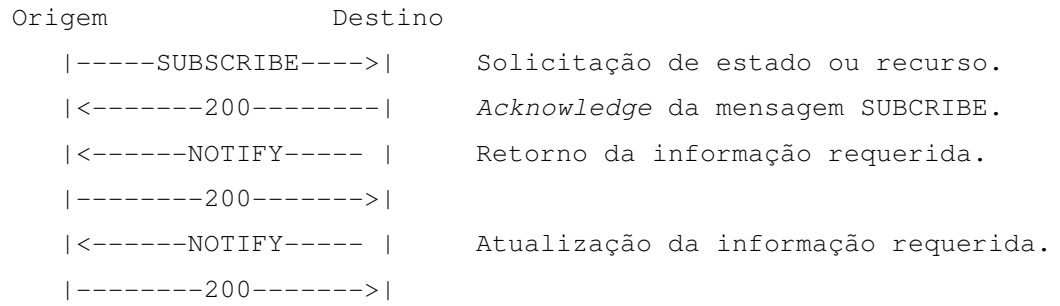


Figura 10: Fluxo de Comunicação do Método SUBSCRIBE

IX. NOTIFY

Como pode ter sido notado anteriormente, a mensagem NOTIFY é sempre enviada imediatamente após a confirmação de chegada da mensagem SUBCRIBE. O método NOTIFY é utilizado em resposta a solicitação do usuário e contêm as informações requisitadas.[23]

Importante notar o comportamento de um elemento de rede quando recebe uma requisição SUBSCRIBE referente a um evento desconhecido. Neste caso, o elemento deve responder imediatamente com a mensagem de erro do tipo *489 Bad Event* para indicar que o evento não foi compreendido.

X. UPDATE

O método UPDATE permite que os terminais atualizem os parâmetros da sessão, tais como o conjunto de *streaming* de mídia e seus CODECs, mas não tem impacto no estado do dialogo, isto é, na conexão fim-a-fim. [24]

Esta característica também pode ser assumida por um novo pedido INVITE, também conhecido como re-INVITE, com objetivo de modificar algum parâmetro de sessão uma vez que esta já tenha sido estabelecida. Porém, diferentemente do re-INVITE, a mensagem UPDATE permite tanto à origem como ao destino enviarem seus pedidos de atualização de sessão antes que o pedido INVITE inicial tenha sido completado.

A operação da mensagem UPDATE é simples e direta, como pode ser observado pela Figura 11, que apresenta um exemplo de fluxo de comunicação da mensagem. O terminal de origem inicia a requisição da chamada através da mensagem INVITE, contendo as suas características no corpo da mensagem SIP. Estas características são definidas e tratadas pelo protocolo SDP, que ainda será formalmente apresentado, mas que é responsável pela descrição dos parâmetros de configuração do terminal, como CODECs a que tem suporte, tipo de Terminal, informação de disponibilidade de banda, tipo de mídia que deseja transmitir, etc. Logo, ao convidar o terminal de destino a estabelecer uma sessão, a origem encaminha suas características de modo que o destino possa reconhecê-las e negociá-las,

visto que o processo é válido também para o terminal de destino, ou seja, ele também deve enviar seus parâmetros de configuração para a origem, de forma que ambos possam estabelecer uma sessão em comum.

Pode-se verificar que a cada mensagem UPDATE corresponde uma mensagem de confirmação, que é aproveitada para transportar a resposta do pedido. A Figura 11 também reitera o fato de que o método UPDATE pode ser enviado a qualquer momento da sessão, mesmo antes de esta ter sido criada e por qualquer uma das partes da chamada.

Importante notar também que qualquer dispositivo de uma rede SIP deve ser capaz de gerar e processar a mensagem UPDATE e que deve ser avaliado o tratamento de erros referentes a esta mensagem, como erros de sequenciamento no fluxo das mensagens, *491 Request Pending, 504 Server Timeout, 488 Not Acceptable Here, 481 Call/Transaction Does Not Exists e 408 Request Timeout*, por exemplo.

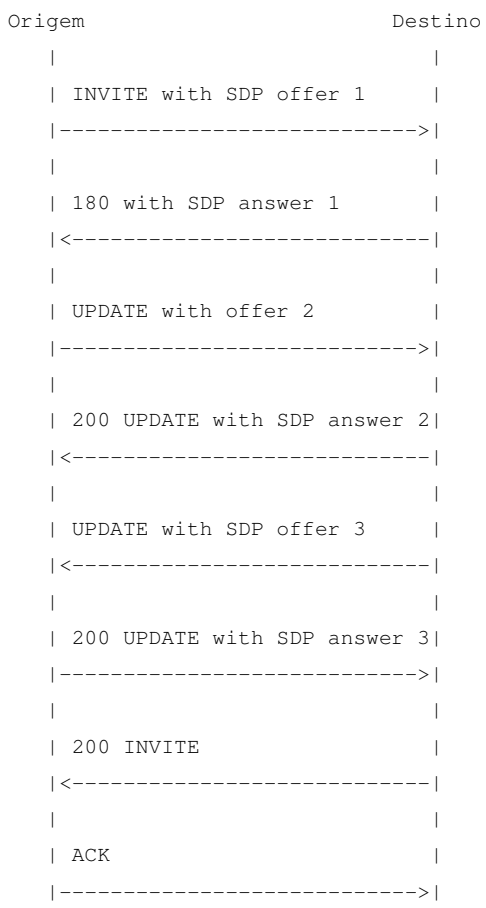


Figura 11: Fluxo de Comunicação do Método UPDATE

XI. REFER

O método REFER é utilizado para os serviços de transferência de chamada e conferência; o receptor desta mensagem deve contatar uma terceira parte definida pelas informações de endereço do cabeçalho *REQUEST-URI*.[25] Portanto, a mensagem geralmente faz referência à criação de outro diálogo ou sessão; entretanto não será objetivo deste trabalho avaliar o comportamento de equipamentos em serviços de conferência.

Conferências com H.323 obrigatoriamente necessitam da MCU, que centraliza toda sinalização, por menor que seja o número de participantes. O protocolo SIP trabalha com o controle da conferência de forma distribuída pelos participantes, sem a necessidade de um equipamento centralizador, eliminando o risco de congestionamento.

Importante, nos testes, observar o comportamento dos elementos SIP em relação ao tratamento dado aos pedidos recebidos e que não oferecem suporte. Deve-se verificar o grau de interoperabilidade entre os equipamentos, de modo que consigam realizar a negociação de capacidades, mesmo que não tenham suporte a todos os métodos SIP em comum.

2.3.2 Respostas às Mensagens SIP

As respostas SIP podem ser de duas categorias básicas, a primeira pertence à classe 1xx, que são as de caráter provisório na sinalização da chamada e que sempre serão seguidas de respostas da segunda classe, que, por sua vez, são respostas definitivas e finalizam uma requisição SIP [19].

A Tabela 9 apresenta apenas a descrição das repostas mais comumente usadas na operação de redes SIP, enquanto que outras não são apresentadas ou são simplesmente mencionadas, por serem desnecessárias neste nível de estudo ou por serem de dedução direta a partir do seu nome. Neste momento, é importante mais uma vez destacar que este trabalho tem o objetivo de apresentar aspectos da elaboração de procedimentos de teste capazes de fazer uma avaliação crítica da implementação de plataformas SIP de diversos fabricantes, que

quase sempre declaram estar coerentes com as normas e possuírem soluções customizadas do protocolo. Deve-se considerar que um dos limitantes deste estudo é a realidade prática dos testes a que devem ser submetidos os equipamentos, que não podem ser complexos demais, pois isto inviabilizaria sua aplicação em laboratório, principalmente por questões de tempo e disponibilidade de pessoal e equipamentos e, por outro lado, não podem ser simples demais, pois não faria sentido uma avaliação superficial. Portanto, o desafio é realizar um estudo ótimo das características fundamentais do protocolo para gerar uma ferramenta verdadeiramente útil e eficaz de avaliação. Como veremos neste tópico e em outros, a norma vai além destas limitações e se mostra bastante detalhada na descrição do protocolo.

Grupo	Ação	Descrição
1xx – *Informational Responses (Provisional)*	*Se o servidor não é capaz de responder a um convite imediatamente e definitivamente, ele pode escolher indicar algum tipo de progresso para o cliente, por exemplo, uma indicação de telefone tocando. Isto é realizado através da resposta provisória do tipo 100 a 199. Dessa forma, se consegue estabelecer diálogos de status antes da conexão de mídia ter sido iniciada e evita-se um período longo sem comunicação.* *Um servidor ou mesmo um terminal pode enviar tantas respostas provisórias quanto quiser, sendo que todas elas pertencem a mesma sessão. Não há confirmação de entrega destas classes de respostas, isto é, operam no modo não confiável.*	
	100 Trying	A resposta *100 Trying* indica que o pedido INVITE foi recebido e que alguma ação, tal como uma consulta ao banco de dados, está ocorrendo. O pedido é opcional durante a implementação da rede
	180 Ringing	Destino emula o som de toque/alerta para frente e para trás através desta mensagem.
	182 Queued	O pedido foi recebido, mas o terminal está ocupado e o pedido será processado de acordo com sua posição na fila.
	181 Call is Being Forward	Indica que o receptor re-roteou o pedido para o destino.

	183 Session in progress	Chamada está sendo processada e aguardando resposta do destino.
2xx – *Successful Responses*	*Esta classe de respostas indica que o pedido foi recebido, entendido e aceito satisfatoriamente.*	
	200 OK	Indica, de modo geral, a aceitação de um pedido e, entre outras coisas, pode sinalizar o atendimento da chamada por parte do destino. Adicionalmente, a maior parte dos valores dos cabeçalhos do pedido é copiado nesta mensagem de resposta e o corpo da mensagem contém a descrição do tipo de mídia que o destino pretende utilizar. Todas estas características serão apresentadas a seguir.
3xx – *Redirection Responses*	*Este conjunto de mensagens é utilizado pelo Servidor de Redirecionamento, que responde a um pedido INVITE sempre com uma resposta de classe 3xx, contendo o endereço do próximo Servidor Proxy, ou uma mensagem de erro gerado no lado do destino ou até mesmo do lado do Servidor.*	
	300 Multiple Choice	O servidor de Redirecionamento retorna possíveis endereços de registro do destino, após constatar um Servidor de Registro com todo ou uma parte do SIP URI do usuário.
	301 Moved Permanently	O servidor de Redirecionamento retorna o endereço da nova localização do terminal de destino.
	302 Moved Temporarily	O servidor de Redirecionamento retorna o endereço da localização temporária do terminal de destino.
	305 Use Proxy	Esta resposta indica que o usuário tem que usar um servidor Proxy para contatar o destino.
	380 Alternative Service	O Servidor de Redirecionamento retorna o endereço da nova localização com o cabeçalho *EXPIRES* e também pode conter uma descrição da sessão no corpo da mensagem que representa as capacidades de envio do novo endereço de destino.

4xx - *Client Failure Responses*	*Se o destino emitir uma resposta de falha da classe 4xx, ou seja, uma resposta definitiva de falha que seja um erro do cliente, uma nova requisição não será reenviada sem modificação.*	
	482 Loop Detected	Caso em que o Proxy reencaminharia a mesma mensagem já encaminhada novamente, desde que esta mensagem seja exatamente a mesma da anterior.
	486 Busy Here	Indica que o telefone do destino foi contatado com sucesso, mas não estava disponível ou estava impossibilitado de receber outra chamada.
	400 Bad request *401 Unauthorized* *402 Payment REQUIRE* *403 Forbidden* *404 Not Found* *405 Method not Allowed* *407 Proxy Authentication REQUIRE* *408 Request Timeout* *413 Request entity too large* *414 Request URI too long* *415 Unsupported media TYPE* *416 Unsupported URI scheme* *423 Interval too brief* *480 Temporarily not available* *483 Too many hops* *484 Address incomplete*	
5xx - *Server Failure Responses*	*Se a resposta de falha da classe 5xx existir, ou seja, uma falha indefinida que seja um erro do servidor, o pedido não será terminado e outras localidades possíveis são tentadas.*	
	503 Service Unavailable	O servidor de destino determina que não tem mais nenhum canal disponível e recusa a conexão através desta mensagem.

	502 Bad Gateway *500 Internal Server Error* *504 Gateway Timeout* *513 Message Too Large*	
6xx - *Global Failure Responses*	*Se o servidor emitir uma resposta de falha da classe 6xx, isto é, um erro global, o terminal não deve mais enviar nenhum pedido ao servidor.*	
	606 Not Aceptable	A mensagem é disparada toda vez que o destino não possui o CODEC que a origem espera receber a mídia. Adicionalmente, a mensagem possui os CODECs que o destino suporta. Neste caso, a origem pode reenviar um novo pedido INVITE ou utilizar um PROXY que fará o papel de Gateway para viabilizar a comunicação.
	603 Decline	Esta mensagem de resposta indica que o destino foi contatado, mas não pode ou não deseja participar da chamada. Ao receber esta resposta, o telefone codifica esta mensagem como sinal de ocupado e desconecta a chamada.
	600 Busy Everywhere *604 Does not exist anywhere*	

Tabela 9: Respostas às Mensagens de Pedido do Protocolo SIP

Como verificado através da Tabela 9, seria muito difícil testar todas as possibilidades de respostas para cada tipo de requisição; por isso os testes foram organizados baseados nos métodos SIP, que são em menor número; através destes se consegue forçar determinadas respostas de erro do sistema e, conseqüentemente, observar a resiliência a erros das entidades da rede.

Método PRACK

Como visto, as mensagens de respostas do protocolo SIP são classificadas como respostas provisórias e respostas finais. Estas últimas transportam o resultado do processamento da mensagem de requisição e são enviadas de forma confiável, isto é, o receptor destas respostas envia uma mensagem de confirmação de recebimento que, geralmente, é

processada através da mensagem ACK. Já as respostas provisórias provêem informação sobre o progresso do processamento da mensagem requisição e não são enviadas de forma confiável, de acordo com a Recomendação padrão do SIP [19].

Algum tempo após a elaboração original da norma foi observado que a confiabilidade dessas respostas era importante em muitos casos, como em cenários de interoperabilidade com PSTN. Então, uma capacidade opcional era necessária para suportar transmissões confiáveis de respostas provisórias. Dessa forma, criou-se mais um novo método chamado PRACK, no qual a técnica é a mesma do mecanismo de confiabilidade existente para respostas finais do tipo 2xx, por exemplo [26].

Resumidamente, o pedido PRACK realiza o mesmo papel do ACK, porém para respostas provisórias. Para cada resposta provisória é dado um número seqüencial, carregado no campo de cabeçalho *Rseq* da resposta. As mensagens PRACK contêm um campo de cabeçalho *Rack*, que indica o número seqüencial da resposta provisória que está sendo reconhecida. A Figura 12 exemplifica o método:

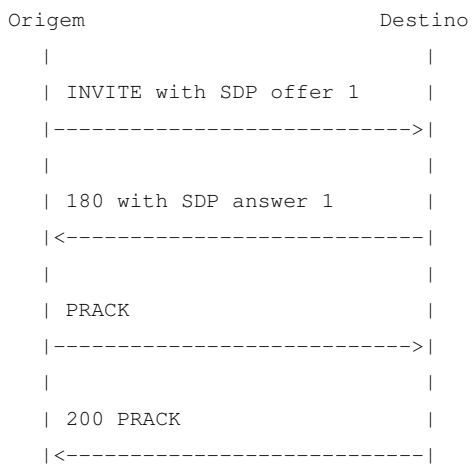


Figura 12: Fluxo de Comunicação do Método PRACK

Importante nos testes observar a capacidade dos equipamentos em formatar e gerar corretamente as respostas provisórias confiáveis, devido à necessidade de inclusão de cabeçalhos extras e informações de estado das mensagens.

2.4 Cabeçalhos SIP

O quadro de uma mensagem SIP é basicamente formado por dois campos distintos. O primeiro é portador dos cabeçalhos, cuja responsabilidade é tornar possível a comunicação multimídia na rede e descrever os detalhes da transação. O segundo campo contém a descrição da mídia propriamente dita, sendo controlado pelo protocolo SDP, que será visto no próximo tópico.

Os cabeçalhos das mensagens SIP são informações incluídas nos pedidos e respostas, para prover desde as informações mais básicas às mais avançadas e habilitar tratamento apropriado a cada mensagem. Cada cabeçalho faz sentido apenas para certos pedidos e respostas e, em alguns casos, a presença de um dado cabeçalho na resposta é conseqüência de um determinado pedido. Por isso, o objetivo aqui é apresentar os cabeçalhos e sua utilização de forma resumida e didática, visto que a descrição completa de todos os cabeçalhos é definida na recomendação do protocolo [19].

A Tabela 10 apresenta um mapeamento entre cabeçalhos, pedidos e respostas SIP. Observa-se que a inclusão de um cabeçalho em particular numa dada resposta depende do tipo de classe de código da resposta e do pedido que conduziu àquela resposta.

Um aspecto de análise importante pode ser observado através da Tabela 10, onde todos os métodos definidos no item 3.3.1 possuem cabeçalhos obrigatórios próprios, tornando-se, portanto, item obrigatório de avaliação. O Teste 2 do Apêndice B apresenta a forma como esta análise foi desenvolvida.

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
ACCEPT	R		-	o	-	o	m*	o
ACCEPT	2xx		-	-	-	o	m*	o
ACCEPT	415		-	c	-	c	c	c
ACCEPT-ENCODING	R		-	o	-	o	o	o
ACCEPT-ENCODING	2xx		-	-	-	o	m*	o
ACCEPT-ENCODING	415		-	c	-	c	c	c
ACCEPT-Language	R		-	o	-	o	o	o
ACCEPT-Language	2xx		-	-	-	o	m*	o
ACCEPT-Language	415		-	c	-	c	c	c
Alert-Info	R	ar	-	-	-	o	-	-
Alert-Info	180	ar	-	-	-	o	-	-
Allow	R		-	o	-	o	o	o
Allow	2xx		-	o	-	m*	m*	o
Allow	r		-	o	-	o	o	o
Allow	405		-	m	-	m	m	m
Authentication-Info	2xx		-	o	-	o	o	o
Authorization	R		o	o	o	o	o	o
Call-ID	c	r	m	m	m	m	m	m
Call-Info		ar	-	-	-	o	o	o
Contact	R		o	-	-	m	o	o
Contact	1xx		-	-	-	o	-	-
Contact	2xx		-	-	-	m	o	o
Contact	3xx	d	-	o	-	o	o	o
Contact	485		-	o	-	o	o	o
CONTENT-DISPOSITION			o	o	-	o	o	o
CONTENT-ENCODING			o	o	-	o	o	o
CONTENT-Language			o	o	-	o	o	o
CONTENT-LENGTH		ar	t	t	t	t	t	t
CONTENT-TYPE			*	*	_	*	*	*
CSeq	c	r	m	m	m	m	m	m
Date		a	o	o	o	o	o	o
Error-Info	300-699	a	-	o	o	o	o	o
Expires			-	-	-	o	-	o
From	c	r	m	m	m	m	m	m
In-Reply-To	R		-	-	-	o	-	-
Max-Forwards	R	amr	m	m	m	m	m	m
Min-*Expires*	423		-	-	-	-	-	m
MIME-Version			o	o	-	o	o	o

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
Priority	R	ar	-	-	-	o	-	-
Proxy-Authenticate	407	ar	-	m	-	m	m	m
Proxy-Authenticate	401	ar	-	o	o	o	o	o
Proxy-Authorization	R	dr	o	o	-	o	o	o
Proxy-Require	R	ar	-	o	-	o	o	o
Record-Route	R	ar	o	o	o	o	o	-
Record-Route	2xx,18x	mr	-	o	o	o	o	-
Reply-To			-	-	-	o	-	-
Require		ar	-	c	-	c	c	c
Retry-After	404,413,480,486		-	o	o	o	o	o
	500,503		-	o	o	o	o	o
	600,603		-	o	o	o	o	o
Route	R	adr	c	c	c	c	c	c
Server	r		-	o	o	o	o	o
Subject	R		-	-	-	o	-	-
Supported	R		-	o	o	m*	o	o
Supported	2xx		-	o	o	m*	m*	o
Timestamp			o	o	o	o	o	o
To	c(1)	r	m	m	m	m	m	m
Unsupported	420		-	m	-	m	m	m
User-Agent			o	o	o	o	o	o
Via	R	amr	m	m	m	m	m	m
Via	rc	dr	m	m	m	m	m	m
Warning	r		-	o	o	o	o	o
WWW-Authenticate	401	ar	-	m	-	m	m	m
WWW-Authenticate	407	ar	-	o	-	o	o	o

Tabela 10: Relacionamento entre cabeçalhos, pedidos e respostas SIP

Na tabela,

R: o cabeçalho pode estar presente apenas nos pedidos;

r: o cabeçalho pode estar presente apenas nas respostas;

2xx, 4xx, etc: Representam uma determinada classe de códigos de respostas, no qual o cabeçalho pode ser usado;

c: Indica que o valor do cabeçalho é copiado do pedido para a resposta.

Uma entrada vazia na coluna “where” indica que o cabeçalho pode estar presente em todos os pedidos e respectivas respostas.

A coluna “Proxy” descreve as operações que o Proxy pode executar em relação aos cabeçalhos:

a: O Proxy pode adicionar ou concatenar o cabeçalho caso este não esteja presente na mensagem;

m: O Proxy pode modificar o valor existente do cabeçalho;

d: O Proxy pode deletar o valor do cabeçalho;

r: O Proxy tem que ser capaz de ler o cabeçalho e, conseqüentemente, o cabeçalho não pode ser criptografado.

As próximas seis colunas relacionam a presença dos cabeçalhos com cada método SIP:

m = mandatório;

m* = mandatório no pedido, mas o receptor deve estar preparado para receber e processar um pedido mesmo sem o campo;

o = opcional, ou seja, o terminal pode incluir o cabeçalho no pedido ou resposta, e o destino pode ignorar o cabeçalho se presente no pedido ou resposta.

t = campo deve ser incluído no pedido, mas tanto o cliente como o servidor devem estar preparados para receber mensagens sem o cabeçalho. Se o protocolo TCP for usado, o cabeçalho tem que ser enviado obrigatoriamente.

c = condicional, ou seja, a presença do cabeçalho depende do contexto em que a mensagem está inserida.

- = não aplicável, isto é, o cabeçalho não deve ser enviado no pedido. Caso o receptor da mensagem receba o cabeçalho, este deve ser descartado.

* = O cabeçalho tem que ser incluído se a mensagem contém um corpo de mensagem (SDP), caso contrário, o cabeçalho pode ser omitido.

Os cabeçalhos descritos acima podem ser classificados como globais quando contêm informações básicas necessárias para o tratamento tanto das perguntas quanto das respostas, isto é, podem ser usados nas perguntas e respostas, e estão identificados pela cor

vermelha; cabeçalhos de pedido, aplicados apenas nas mensagens de pedido SIP, estão na cor verde; cabeçalhos de resposta, análogo ao anterior, estão na cor rosa e, por fim, cabeçalhos de entidade, que indicam o tipo e o formato da informação contida no corpo da mensagem, de forma que a aplicação apropriada possa ser chamada. Os cabeçalhos deste último tipo estão em azul nas tabelas acima.

Faz-se necessário, portanto, entender o sentido e a aplicação de alguns cabeçalhos descritos anteriormente. A Tabela 11 faz algumas considerações importantes destes cabeçalhos:

Cabeçalhos	**Função**
VIA	O campo *VIA* armazena o endereço de cada *hop* no qual mensagem é processada, de forma que os *elementos* de destino conheçam o caminho completo de retorno. Para isso, cada servidor Proxy adiciona um novo campo *VIA* com seu próprio endereço na frente do endereço anterior. O campo *VIA* deve possuir informações da versão do protocolo SIP, endereço e porta que a origem deseja receber a mídia, mesmo em redes com NAT, e possui ainda o protocolo da camada de transporte utilizado. O parâmetro *maddr* do cabeçalho *VIA* informa o valor de TTL (Time To Live) e também indica que a mensagem foi transmitida em *broadcast,* dependendo do endereço contido no parâmetro. Há ainda outro parâmetro do cabeçalho *VIA*, chamado *branch*, que é um identificador único para todas os pedidos feitos pelo cliente e suas respostas respectivas, com exceção dos pedidos CANCEL e ACK, que recebem outra numeração *branch*, apesar de fazerem parte do contexto de uma mesma chamada. O objetivo é fazer o relacionamento entre perguntas e respostas correspondentes e evitar *loops*. Este parâmetro foi inicialmente especificado pela antiga RFC 2543, que era opcional e não identificava unicamente uma transação, entretanto, o campo *branch* deve possuir o valor fixo inicial z9hG4bK, para certificar que os elementos de rede estão operando de acordo

	com a mais recente RFC. Importante verificar o comportamento do Terminal de origem ao receber o cabeçalho *VIA* com erro ou duplicado. E garantir que no caso de Proxy s*tateless*, o campo *VIA* não sofre qualquer alteração na retransmissão.
CSEQ	O cabeçalho realiza a função de sequenciação de grupos de requisição e respostas. Deve ser observada a sintaxe do cabeçalho, que inicia com um numero inteiro com valor aleatório e a partir de então é seqüencial. Após o número de identificação, o cabeçalho também transporta o tipo de pedido SIP, como INVITE, ACK, etc.
FROM	Indica o endereço do remetente da mensagem. Importante notar a presença do parâmetro *tag* do cabeçalho, que assume um valor pseudo-randômico gerado pelo transmissor do pedido e é usado para propósitos de identificação e segurança.
TO	Indica a URI do destinatário. Este campo não é modificado em caso de mudança de localidade do destinatário, isto possibilita saber se a ligação foi feita para a sua localidade padrão e foi redirecionada para o seu local atual de trabalho. Os valores dos campos *FROM* e *TO* são idênticos quando inseridos no pedido REGISTER, já que esta é uma transação de registro e realizada por apenas um terminal.
CALL-ID	O campo é muito importante na comunicação, pois além de atribuir um identificador numérico único para as mensagens pertencentes a uma mesma chamada, identifica os pedidos e respostas correspondentes, e também é útil na detecção de copias duplicadas de mensagens, além de possibilitar a modificação de parâmetros dinamicamente em uma conferência.

CONTACT	O cabeçalho *CONTACT* normalmente possui a URI do próprio Terminal que está enviando a mensagem, porém possui uma diferença sutil para o campo *FROM*. A diferença é que este último contém o endereço no formato URI original do cliente, já o campo *CONTACT* também identifica na URI o *host* que o usuário está conectado e que espera ser contactado. Dessa forma, após o procedimento de um pedido INVITE e as respostas e pedidos subseqüentes, os dois terminais tem informações suficientes de endereço para comunicação direta fim-a-fim. Este cabeçalho deve ser avaliado tanto nos pedidos para estabelecimento de uma sessão, quanto pelos pedidos de registro e redirecionamento. Novamente, aqui cabe uma observação interessante e já anunciada com relação ao Servidor de Redirecionamento, pois este se torna uma opção muito útil na medida em que é capaz de realizar distribuição/balanceamento de carga quando utilizado como *frontend* a partir de um grupo de servidores Proxies secundários, e para isso utiliza-se o cabeçalho *CONTACT*, já que possui o endereço real dos *hosts* e Servidores. Importante observar que o cabeçalho *CONTACT* assume o valor "*" quando o usuário deseja cancelar todos os seus registros no Servidor. Deve ser acompanhado do valor "0" no cabeçalho *EXPIRES*. As respostas de classe 3xx podem conter mais de um valor de endereço no cabeçalho *CONTACT*, indicando os possíveis destinos de um dado terminal.
EXPIRES	Geralmente indica o tempo de validade do *login* do usuário, que na maioria das vezes é especificado pelo assinante, mas o Servidor de Registro pode diminuir esse valor em sua resposta. O valor *default* é 3600s. O cabeçalho *EXPIRES* está contido em várias mensagens SIP e até como subcampo em outros cabeçalhos, como no caso do *CONTACT*, por exemplo.

SUBJECT	Cabeçalho utilizado para fornecer uma descrição textual da natureza da sessão ou mensagem digitada pelo usuário.
PRIORITY	Indica a urgência de um pedido, que pode ser classificado como emergência, urgência, normal ou não urgente. Este cabeçalho pode ser configurado em associação ao número discado pelo usuário, como telefone de polícia, bombeiro, etc. A importância deste campo é notável seja em redes totalmente IP ou também em redes híbridas de telefonia (RTPC-VoIP).
MIN-EXPIRES	Este cabeçalho deve ser verificado, pois é incluído pelo Servidor de Registro e está sempre associado a uma resposta do tipo *423 Interval Too Brief*, ou seja, quando o usuário informa na mensagem REGISTER um tempo muito curto de expiração do seu processo de *login*.
MAX-FORWARD	Número de saltos que a mensagem pode percorrer, sendo esse valor decrementado na passagem por cada Proxy. O valor *default* é 70.
RECORD-ROUTE e *ROUTE*	Ambos os cabeçalhos são mecanismos para terminais e servidores determinarem a rota de sinalização de uma chamada. Geralmente, o cabeçalho ROUTE é preenchido pelo terminal, já o servidor Proxy utiliza o cabeçalho RECORD-ROUTE de forma a criar uma rota estática para a sinalização. Uma vez inserido um ou outro cabeçalho numa requisição INVITE transmitida ou retransmitida pelo Proxy, as respostas relacionadas são também encaminhadas contendo o mesmo cabeçalho. O resultado é a garantia de que cada pedido e resposta sigam o mesmo caminho, apesar da diminuição da escalabilidade da rede em função do aumento de processamento por parte do Proxy. Portanto, este recurso deve ser utilizado para serviços especiais e realmente necessários. Importante notar a presença do parâmetro *Loose Routing* (lr) no cabeçalho, utilizado apenas para assegurar que o sistema esteja de acordo com a nova norma, já que a recomendação antiga implementava o chamado *Strict Routing* (sr), onde o cabeçalho *ROUTE* possuía sempre o valor do endereço do Terminal de destino.

ALLOW	O cabeçalho define os métodos SIP suportados pelo terminal de origem, sendo importante para definir a compatibilidade de recursos que podem ser utilizados pelas partes da chamada.
SUPPORTED, *UNSUPPORTED*, *REQUIRE* e *PROXY-REQUIRE*	O cabeçalho *SUPPORTED* enumera todos os serviços suportados pelo Terminal ou Servidor. Quando um serviço é fundamental para uma determinada aplicação requerida, este é incluído no cabeçalho *REQUIRE* ou *PROXY-REQUIRE*, este último no caso de exigência específica de suporte ao serviço por parte do(s) Proxy (ies) ao longo do trecho de sinalização. Portanto, estes cabeçalhos permitem que o protocolo implemente a negociação de parâmetros e serviços avançados para uma chamada. Os testes referentes a estes parâmetros devem analisar o cabeçalho *SUPPORTED* em relação aos seus valores pré-definidos pela norma, evitando, portanto, a inclusão de outros valores ou parâmetros que possam acarretar numa solução proprietária e sem qualquer interoperabilidade básica entre fornecedores. O mesmo vale para os cabeçalhos *REQUIRE, PROXY-REQUIRE* e *UNSUPPORTED*, pois todos estes são igualmente responsáveis pelo suporte aos mecanismos de compatibilidade dos serviços SIP. Portanto, os valores assumidos por estes cabeçalhos são padronizados e registrados no IANA* quando publicado definitivamente na Recomendação, isto é, a partir do momento que a norma assume a categoria *Standards Track.* Logo, não é permitida a inclusão de novos valores para estes cabeçalhos mesmo que constem em Recomendações de categoria *Experimental* ou *Informational*, sendo que estas categorias são freqüentemente utilizadas em implementação customizadas ou proprietárias por parte dos fornecedores. Caso algum serviço não seja suportado em ambos dispositivos, uma resposta de erro do tipo *420 Bad Extension,* incluindo os serviços a que não tem suporte no cabeçalho *UNSUPPORTED* deve ser observada. Deve ser tratada também as exceções destes cabeçalhos referentes as mensagens CANCEL e ACK.

	* http://www.iana.org/assignments/sip-parameters
WARNING	O cabeçalho contém os motivos de erros em relação ao corpo da mensagem (SDP).

Tabela 11: Descrição dos Principais Cabeçalhos SIP (Primeira Parte)

E, por fim, o SIP ainda prevê um mecanismo para representar nomes de cabeçalhos de uma forma abreviada, visto que é um protocolo baseado em texto, diferentemente dos protocolos binários, que assumem formas mais compactas. Isso pode ser útil quando as mensagens se tornam muito grandes para serem carregadas no *frame* dos protocolos das camadas inferiores, isto é, excedendo a unidade máxima de transmissão quando o UDP é usado, por exemplo. A forma compacta pode ser substituída pela forma tradicional a qualquer momento sem que seja mudada a semântica da mensagem. O nome dos campos do cabeçalho podem aparecer em ambas as formas longa e curta.

Além da verificação de suporte aos cabeçalhos na forma simplificada, os elementos de rede SIP devem ser avaliados em relação aos cabeçalhos mal formados ou desconhecidos, que devem ser ignorados, uma vez que estes não têm impacto direto na interoperabilidade dos elementos.

2.5 Protocolo SDP

O início e o término, a configuração e a mudança de uma sessão, são responsabilidades do protocolo SIP e é independente do tipo de mídia ou aplicação que será usada na comunicação, visto que uma chamada pode utilizar diferentes tipos de dados, incluindo áudio, vídeo e muitos outros formatos. Já informações sobre o tipo de mídia são proporcionadas pelo uso do protocolo SDP (Session Description Protocol), que possui especificação própria, a RFC 2327, que vem sofrendo várias alterações desde sua publicação em 1998, apesar de ainda apresentar-se como *Category: Draft*. O padrão SIP também faz referência ao SDP em sua Recomendação, principalmente em relação a interoperação entre os dois protocolos.

O propósito do SDP é especificar informações de *streaming* de mídia, de modo a permitir ao receptor participar da sessão, isto é, descreve o conjunto de tipos de mídia (vídeo, áudio, etc), protocolos de transporte (RTP/UDP/IP, H.320, etc), formatos de mídia (H.261 vídeo, MPEG vídeo, etc), nome da sessão, há quanto tempo à sessão está ativa, informações para recebimento da mídia, como endereços e portas, de forma que as partes de uma chamada possam acordar a troca de dados. [27]

Este protocolo adicional se faz necessário porque o SIP se limita a ter certeza de que as mensagens irão ser transportadas de um local para o outro corretamente. O conteúdo do protocolo SDP é transportado pela mensagem SIP de forma análoga a um documento anexado a uma mensagem de e-mail, ou uma página *web* sendo carregada numa mensagem do protocolo HTTP. Outra analogia que pode ser feita é dizer que o SDP representa uma carta já formatada e selada, e o carteiro é representado pelo protocolo SIP, que apenas se encarrega de transportar esta carta para o lugar correto sem saber o seu conteúdo.

Portanto, o protocolo SIP faz uma parceria com o protocolo SDP para viabilizar a comunicação. Enquanto o SIP fornece um mecanismo de troca de mensagem para o estabelecimento de sessões multimídia, o SDP fornece uma linguagem estruturada que descreve estas sessões. O suporte a novos padrões de codificadores de áudio e vídeo é livre no SIP, basta que este novo CODEC seja registrado com uma identificação em órgão competente. No caso do H.323, os CODECs devem ser padronizados pelo ITU, dificultando o processo de inclusão de novos CODECs.

A sintaxe do SDP é sempre do tipo *campo*=*valor*, onde campo é exatamente um caractere; isto se deve ao fato de o protocolo ser baseado em texto e não em binário, sendo que a desvantagem é o maior consumo de banda, e para isso o *campo* é sempre a inicial de uma palavra referente a um parâmetro na língua inglesa. E *valor* é dependente do campo em questão.

Não haveria interesse em fazer uma descrição detalhada de todos os campos de um pacote SDP, por isso segue-se um breve resumo dos campos, obrigatórios e opcionais, na ordem especificada pelo padrão, visto que alguns campos podem aparecer em nível de sessão e de mídia simultaneamente. Os campos opcionais são marcados com o caractere “*”.

Informações de Sessão

v= (protocol version)

o= (owner/creator and session identifier).

s= (session name)

i=* (session information)

u=* (URI of description)

e=* (email address)

p=* (phone number)

c=* (connection information - not required if included in all media)

b=* (bandwidth information)

Informações de Tempo

z=* (time zone adjustments)

k=* (encryption key)

a=* (zero or more session attribute lines)

t= (time the session is active)

r=* (zero or more repeat times)

Informações de Mídia

m= (media name and transport address)

i=* (media title)

c=* (connection information - optional if included at session-level)

b=* (bandwidth information)

k=* (encryption key)

a=* (zero or more media attribute lines)

É importante observar a formatação correta do protocolo SDP, analisando os campos e subcampos e as respectivas abreviaturas e formatações. A descrição completa de cada subcampo se distancia do escopo deste trabalho, visto que sua Recomendação é bastante completa neste sentido.

A Tabela 12 apresenta os principais cabeçalhos SIP relacionados ao protocolo SDP.

Cabeçalhos	Função
ACCEPT	Indica, numa mensagem OPTIONS, o tipo de corpo de mensagem que o originador da chamada espera receber. Valor *default* é application/SDP. O cabeçalho *ACCEPT* é formalmente especificado pela RFC 1288.
ACCEPT-LENGUAGE e *ACCEPT-ENCODING*	Indica o idioma utilizado pelo corpo da mensagem (campo SDP) do originador da chamada. O cabeçalho *ACCEPT-LENGUAGE* é especificado na RFC 1286. O mesmo ocorre no cabeçalho *ACCEPT-ENCODING*, responsável pela especificação da codificação utilizada no corpo da mensagem.
CONTENT-LENGTH	Especifica o tamanho do corpo da mensagem (campo SDP) em octetos. O cabeçalho assume valor nulo quando incorporado no pedido REGISTER, pois esta não possui corpo de mensagem.
CONTENT-TYPE	Indica o tipo de mídia do corpo da mensagem. No caso de VoIP, este cabeçalho sempre indicará SDP ou application/sdp.
CONTENT-ENCONDING	Indica qualquer codificação adicional aplicada ao corpo da mensagem, assim como o esquema de compressão utilizado. Para isso, o *decoder* deve possuir a capacidade de decodificar o corpo da mensagem no destino, de forma a extrair o tipo de mídia definida pelo cabeçalho *CONTENT-TYPE*.
CONTENT-DISPOSITION	Descreve como o corpo da mensagem deve ser interpretado. Se o corpo da mensagem descreve as características de uma sessão, o valor associado a este cabeçalho deve ser “session”. Além das características de uma sessão, o corpo da mensagem pode transportar outros dados como parte de serviços agregados de telefonia, como é o caso de transporte de imagens, onde o valor do cabeçalho contém o valor “icon”. O cabeçalho também pode assumir o valor “render” nos casos em que o corpo da mensagem deve ser mostrado ao usuário, esse conteúdo pode ser um texto que a origem deseja exibir ao destino, por exemplo. E, por fim, há também o valor “alert” indicando que o corpo da mensagem contém informações como a de uma gravação de voz que alertaria o usuário quando na recepção de um pedido SIP, um exemplo desta aplicação é a personalização dos toques telefônicos em função da origem.

Tabela 12 – Descrição dos Principais Cabeçalhos SIP (Segunda Parte)

Todos os cabeçalhos descritos na Tabela 12 são importantes e devem ser avaliados no processo de estabelecimento da chamada, pois uma requisição INVITE típica contém um *payload* SDP no corpo de sua mensagem para negociar parâmetros RTP de áudio. Durante o processo de sinalização de uma chamada, o protocolo SDP apresenta sempre uma oferta de capacidades, conhecida como SDP *offer*, ao destino, que é obrigado a incluir outra oferta SDP de confirmação ou rejeição na mensagem de resposta ao pedido INVITE do Terminal de origem.

Variações também devem ser avaliadas, como no caso em que a mensagem INVITE inicial não contém um SDP *offer* e a oferta parte da resposta ao INVITE. O teste deve garantir que o Terminal é capaz de receber e processar uma oferta SDP numa mensagem de resposta e enviar uma oferta SDP num pedido ACK.

Qualquer modificação de parâmetros de uma comunicação pode ser realizada através de novas mensagens INVITE; essa modificação pode envolver mudança de endereços ou portas, adição ou remoção de um *streaming* de mídia, troca de CODECs, etc. Isto é realizado através do envio de um novo pedido INVITE ou um re-INVITE, referenciado a um mesmo diálogo. Tanto a origem quanto o destino de uma chamada podem modificar uma sessão existente, visto que é útil dentro de uma sessão SIP alterar os parâmetros do *streaming* de mídia. Por isso, também é importante uma análise da troca de capacidade dos dispositivos a partir de um segundo pedido INVITE dentro de um mesmo diálogo de forma a atualizar os parâmetros SDP.

Uma possibilidade que deve ser levada em consideração é o caso em que as partes não possuem tipos de mídia em comum; neste caso, a resposta a um INVITE deve conter a mensagem com o código de status *488 Not Acceptable* ou *606 Not Acceptable*. Adicionalmente, a resposta poderia conter o cabeçalho WARNING com a mensagem *304 Media TYPE Not Available* ou *305 Incompatible Media TYPE.*

Portanto, o protocolo SIP faz uma parceria com o protocolo SDP para viabilizar a comunicação. Enquanto o SIP fornece um mecanismo de troca de mensagem para o estabelecimento de sessões multimídia, o SDP fornece uma linguagem estruturada que descreve estas sessões.

2.6 Metodologia de Testes e Resultados

O Capítulo 3 apresentou uma descrição do protocolo SIP ao mesmo tempo em que procurou descrever os procedimentos para criação dos testes de conformidade, cuja elaboração é objetivo do projeto que deu origem a esta Dissertação.

Aspectos de Qualidade de Serviço e de segurança do protocolo SIP, assim como chamadas multiponto (conferências) não estão no escopo deste trabalho, por se tratar de assuntos que exigem um estudo à parte e bastante aprofundado, saindo definitivamente do objetivo da Dissertação. Esta observação também vale para o capitulo seguinte.

A metodologia de desenvolvimento do caderno de teste tem inicio com a observação de caderno de testes de outras tecnologias desenvolvidos pela própria Embratel, como ISUP, R2-D, etc. Essa realidade foi bem incorporada ao mundo de telefonia IP. A partir desta análise, o estudo da norma foi orientado à proposta do trabalho e aos modelos da Embratel.
A RFC 3261 define regras e também recomenda a implementação de outros pontos do protocolo, além de apresentação formal do padrão. Todas as regras, identificadas em sua maioria pela palavra “MUST”, foram entendidas e incorporadas ao contexto dos testes, por se tratarem de fatores críticos de funcionamento e interoperabilidade de equipamentos.

Outro foco da pesquisa foi identificar as principais características operacionais dos elementos de rede do protocolo, assim como verificar os testes necessários para garantir operação conforme a norma. Entretanto, o Roteiro de Testes não busca avaliar as facilidades ou serviços oferecidos pelos Servidores ou Terminais da rede, ao invés procura validar estes elementos através de um modelo mais genérico capaz de avaliar a implementação das mensagens de sinalização na sua essência, independentemente do serviço avaliado.

A arquitetura proposta através da Figura 9 (pág. 39) foi realmente utilizada, todavia um instrumental de testes chamado Spectra2[1] foi utilizado em substituição aos Terminais para execução, edição e criação dos testes propostos.

O Servidor de Redirecionamento foi o caso mais particular em relação à análise prática dos testes. A rede utilizada como referência para este estudo nos revela que todos os três Servidores SIP são implementados em um único equipamento físico, sendo a tabela de rotas entre os elementos implementada de forma manual, assim como o registro de cada Terminal. Portanto, as mensagens de sinalização são simplesmente roteadas entre os domínios, não havendo registro automático de Terminais nem redirecionamento automático de chamadas como previsto pelo padrão e, conseqüentemente, as mensagens de classe 3xx não puderam ser observadas, apesar de terem sido propostas.

Em relação à interconexão com os protocolos do capítulo anterior, o Gateway H.323/SIP é perfeitamente implementável e opera em redes VoIP híbridas, principalmente devido ao legado H.323. O Gateway RTCP/SIP não é regulamentado pela ANATEL, pois o SIP é extremamente simplificado e não atende a todos os requisitos para interconexão com os protocolos ISUP, DSS-1 e R2-D, utilizados pela rede Embratel. Como exemplo, os eventos de desconexão de chamadas (*release calls*) são mais ricos em detalhes nos protocolos da rede de telefonia tradicional do que no SIP, que na maioria dos casos trata estes eventos com uma única mensagem de erro; além destes, existem os casos de chamada a cobrar, não especificados pelo SIP, e informações para geração de tráfego estatístico da rede, que também não são fornecidos pelo lado da rede SIP, entre outras questões.

[1] **SPECTRA2** é um instrumental de testes da Tektronix capaz de gerar tráfego e monitorar protocolos de sinalização de telefonia IP e RTPC, através do qual podem ser realizados testes de conformidade, emulação de elementos de rede, etc.

As chamadas SIP destinadas a RTPC podem ser tratadas de duas formas gerais, a primeira é inserir na rede dois Gateways de sinalização, o primeiro referente à tradução dos protocolos SIP/H.323 e o segundo responsável pela interconexão H.323/RTPC, este último podendo ser denominado CPE (*Customer Premises Equipament*). Essa configuração é adotada em casos mais específicos e geralmente atende às redes privativas, onde internamente todo o tráfego VoIP é baseado em SIP e toda chamada destinada ou proveniente da RTPC é realizada através de H.323 e posteriormente convertida em SIP, visto que o protocolo é perfeitamente compatível com a rede telefônica legada, inclusive sob o ponto de vista regulatório.

Um outro modelo de interconexão do protocolo SIP com a rede de telefonia pública pode ser empregado através de uma abordagem mais genérica. O ambiente SIP pode ser considerado um subsistema pertencente a uma rede de nova geração mais abrangente. Portanto, no caminho de qualquer chamada SIP endereçada ou proveniente da RTPC, a NGN será a encarregada pela tradução dos protocolos e para isso deve contar com a presença de Gateways de Sinalização. Esta configuração é a mais comum e requer o entendimento da troca de sinalização SIP/MEGACO e, conseqüentemente, MEGACO/RTPC.

Como a proposta do trabalho é avaliar a sinalização dos protocolos VoIP e analisar a interconexão com a rede de telefonia pública, tendo em vista as limitações teóricas e práticas do protocolo SIP em relação à interconexão com a rede telefônica legada, a análise destas questões terá que ser adiada para o próximo capitulo, quando um cenário mais completo de sinalização telefônica será vislumbrado a partir do conceito de redes convergentes.

Enfim, o trabalho atinge alguns de seus objetivos na medida em que todos os testes propostos foram executados em laboratório, cumprindo o desejo de desenvolver um modelo de testes de conformidade no qual o operador é capaz de implementá-lo de forma inteligente e seqüencial, para que possa ter informações de análise suficientes para avaliar determinado equipamento ou um conjunto deles. Outros detalhes da metodologia de desenvolvimento do caderno de testes serão abordados no próximo item.

A última etapa foi relacionada à pesquisa de trabalhos similares, sendo os resultados abordados neste último tópico do capítulo. A partir de um convite para acompanhar os testes de conformidade do protocolo SIP, que seriam realizados pelo CPqD no próprio CRT para validação dos equipamentos da Huawei, pude acompanhar os procedimentos adotados para tal análise. Os testes realizados pelo CPqD foram todos baseados em documentos ETSI (European Telecommunications Standards Institute), que descrevem procedimentos de testes de conformidade para vários protocolos, incluindo SIP, ou seja, exatamente o mesmo trabalho desenvolvido nesta dissertação. Apesar da perplexidade nos primeiros momentos, pude perceber os desafios de confrontar o Roteiro de Testes aqui proposto com outro de maior importância e abrangência. A partir de então, vários questionamentos surgiram, pois, estando esta dissertação quase que concluída, ainda teria serventia? Quais seriam as diferenças entre os métodos de teste do CPqD e os aqui desenvolvidos? O Roteiro de Testes proposto neste trabalho estaria muito aquém do desenvolvido por especialistas dedicados? Teria alguma originalidade? Quais os pontos positivos e negativos dos dois modelos? Etc. Em vista dessas questões, a partir deste momento todo o estudo do protocolo SIP desenvolvido neste capítulo será concluído na medida em que todas estas perguntas são respondidas, com o objetivo de atender à realidade e à necessidade do corpo técnico da Embratel.

O Instituto ETSI publica seu Roteiro de Testes da seguinte forma: Methods for Testing and Specification (MTS); Conformance Test Specification for SIP (IETF RFC 3261); Part 2: Test Suite Structure and Test Purposes (TSS&TP), é um modelo desenvolvido pela ETSI Technical Committee Methods for Testing and Specification (MTS) e publicado para a sociedade científica. Na verdade, a especificação de testes de conformidade do protocolo SIP é bastante completa e composta por três partes, sendo a segunda parte de maior interesse para o estudo comparativo. A bibliografia citada pelo documento do Instituto é baseada na RFC 3261 e documentos ISO/IEC (Information technology - Open Systems Interconnection - Conformance testing methodology and framework), que devem ser adquiridos para consulta.

Além deste, o IETF desenvolveu a RFC 4475 para testes avançados de conformidade do protocolo, que avalia detalhes de sintaxe, condições atípicas de funcionamento, caracteres especiais e condições de *stress*. Há ainda pacotes comerciais de *software* para testes em

SIP relativos à conformidade com a norma, robustez do sistema, segurança e QoS, que obviamente são pagos.

Um aspecto importante do Roteiro de Testes ETSI está no fato de estar todo traduzido em *scripts*, podendo ser executado automaticamente através do instrumental de testes adequado. Tanto o CPqD quanto este estudo utilizaram o Spectra2[1] durante os testes. para execução, edição e criação dos testes propostos. Este recurso possibilita uma análise muito mais eficiente, já que centenas de testes podem ser executados automaticamente e analisados através de alarmes de aprovação ou reprovação para cada um deles.

A partir de uma análise preliminar do caderno da ETSI, foi possível verificar que os testes abordam todos os aspectos da RFC 3261, já o roteiro proposto sugere que apenas os pontos mais críticos do protocolo sejam verificados; sendo assim, a realização completa dos testes de conformidade propostos neste documento não garante que o dispositivo da rede em teste irá interoperar com outros equipamentos em todas as situações a que for submetido. Não obstante, a finalização completa dos conjuntos de testes deve prover um nível razoável de confiança de que o dispositivo testado funcionará de acordo com a norma e com outras soluções de diferentes fornecedores, desde que estes estejam também em conformidade com a norma.

O Roteiro de Testes proposto está agrupado em conjuntos de características comuns, de forma que reduza o tempo de configuração, montagem e execução do *setup* de testes. A primeira parte compreende os testes preliminares, principalmente em relação ao tratamento de determinados cabeçalhos mais importantes do protocolo. As partes subseqüentes são relativas a cada comando SIP, além disso há mais dois capítulos referentes ao protocolo SDP e aos testes considerados mais avançados, no qual são considerados os protocolos UDP e TCP, testes em Servidor *Stateless* e *Stateful*, entre outros. O Roteiro proposto pela ETSI é agrupado em relação aos elementos de rede SIP: Terminal de Origem e de Destino, Servidor de Registro, de Redirecionamento e, por fim, testes referentes ao Servidor Proxy.

Em relação à descrição dos testes, ambos os documentos, isto é, o Roteiro de Testes ETSI e o Roteiro de Testes aqui proposto, se preocuparam em descrever brevemente quase que no mesmo nível de detalhes o objetivo de cada um dos testes. Porém, o caderno aqui

proposto se preocupa em fornecer mais detalhes teóricos na maioria dos casos, como pode ser observado no Teste 3 do Apêndice B.

Apesar de mais detalhado, os testes ETSI são menos abrangentes, pois não há propostas de testes para o protocolo SDP, por exemplo. A norma também não avalia os comandos INFO, SUBSCRIBE, NOTIFY, UPDATE, REFER e o método PRACK, por possuírem recomendações próprias.

A arquitetura dos testes é a mesma nas duas propostas, certamente baseadas no entendimento da norma. O monitoramento da troca de sinalização foi feito através do *software* Ethereal e a geração do tráfego e configuração dos parâmetros do protocolo foi realizado através do Spectra2. A Tabela 13 faz um resumo das diferenças citadas entre as duas práticas.

	ETSI TS 102 027-2 V3.1.1	**ROTEIRO PROPOSTO**
Principais Referências	RFC 3261 + ISO/IEC	RFC 3261
Número de Testes	610	53
Extensões SIP	INVITE ACK BYE CANCEL OPTIONS REGISTER	INVITE ACK BYE CANCEL OPTIONS REGISTER INFO SUBSCRIBE NOTIFY UPDATE REFER
Estrutura do Documento	Terminal de Origem Terminal de Destino Servidor de Registro Servidor Proxy Servidor de Redirecionamento	Comandos Cabeçalhos Protocolo SDP Testes Avançados
Estrutura dos Testes	TPId Status Reference Purpose	Testes ID Objetivo Referências Versão Procedimentos Resultados Esperados Observações
Implementação	Automática (*Scripts* + Spectra2)	Manual

Tabela 12: Comparação entre Roteiros de Testes

A seguir, são apresentados dois exemplos de testes retirados do Roteiro proposto.

Teste 1 – Sintaxe dos Pedidos e Respostas SIP

Objetivo:

Este teste verifica a formatação das mensagens de requisição e resposta SIP, isto é, o objetivo é que a sintaxe das mensagens do protocolo seja respeitada.

Referências:

Seção 7.1 da RFC 3261

Seção 7.2 da RFC 3261

Versão:

01/10/06

Procedimentos:

1. Verificar o envio do pedido OPTIONS do Terminal 1 para o Servidor Proxy.
2. O Servidor Proxy deve retornar a mensagem de resposta *200 OK* ao Terminal 1.

Resultados Esperados:

1. Garantir que o pedido foi enviado na forma "OPTIONS sip: user@host SIP/2.0 [CRLF]", sendo que as linhas seguintes contêm os cabeçalhos.
2. Garantir que a mensagem de resposta seja da forma "SIP/2.0 200 OK [CRLF]"

Observações:

A sintaxe básica descrita no item anterior pode conter entre os campos SIP/2.0 e [CRLF] na mensagem de requisição um texto chamado *reason phrase* ou razão da mensagem indicando a razão do pedido OPTIONS, entretanto esta não representa necessariamente um erro de sintaxe. O texto que representa a razão da mensagem na resposta é [OK], que se encontra entre os campos 200 e [CRLF] na mensagem de resposta.

Teste 2 – Inclusão e Equivalência dos Cabeçalhos Obrigatórios

Objetivo:

Embora a maioria dos cabeçalhos seja opcional, alguns deles são mandatários. Para as mensagens SIP terem um significado e serem roteadas perfeitamente para todos os elementos da rede, certos cabeçalhos são realmente necessários. Portanto, este teste verifica a inclusão dos cabeçalhos baseado nas respostas do método OPTIONS.

Qualquer pedido SIP válido deve conter no mínimo seis cabeçalhos: *TO*, *FROM*, *CSEQ*, *CALL-ID*, *MAX-FORWARD*s e *VIA*.

Referências:

Seção 8.2.6.2 da RFC 3261

Versão:

01/10/06

Procedimentos:

1. Enviar um pedido OPTIONS do Terminal 1 para o Servidor Proxy.
2. O Servidor Proxy deve enviar a mensagem de resposta de sucesso de *200 OK* ao Terminal 1.

Resultados Esperados:

1. Verificar a existência dos seguintes cabeçalhos no método OPTIONS: TO, *FROM*, *CSEQ*, *CALL-ID*, *MAX-FORWARD*s e o campo *VIA*.
2. Os valores dos campos TO e *FROM* da mensagem de resposta têm que assumir os mesmos valores dos campos TO e *FROM* do pedido. (Isso é verdade especificamente para o método OPTIONS, visto que essa mensagem não é utilizada para estabelecer um canal de voz).
3. O campo *VIA* da mensagem de resposta tem que assumir o mesmo valor do campo *VIA* do pedido e ambos os valores devem estar na mesma ordem. (Isso é verdade especificamente para o método OPTIONS, visto que essa mensagem não é utilizada para estabelecer um canal de voz).

4. O valor do campo *CSEQ* da mensagem de resposta tem que assumir o mesmo valor do campo *CSEQ* do pedido.
5. Observar o formato do cabeçalho *CSEQ*, que deve ser composto por um número inteiro menor que 2**31, um espaço em branco, seguido pelo nome do método SIP da mensagem.
6. O valor do campo *CALL-ID* da mensagem de resposta tem que assumir o mesmo valor do campo *CALL-ID* do pedido.
7. O cabeçalho *MAX-FORWARD*s é utilizado apenas nas mensagens de requisição SIP e não deve assumir valor inteiro inferior a 70.

Observações:
É útil observar as Tabelas 2 e 3 na Seção 20.1 da RFC 3261, copiadas neste documento na Tabela 10.
Este tipo de teste deve ser extrapolado para todos os demais pedidos do protocolo SIP.

Os testes a seguir foram copiados na íntegra do caderno de práticas ETSI para serem comparados ao Teste 2 anterior do caderno de práticas proposto. Foram selecionados testes do tópico 5.4 referentes à troca de capacidades através do método OPTIONS, onde o equipamento em teste é um terminal que origina a chamada. Este é um caso típico que ilustra bem as diferentes metodologias, enquanto que o Teste 2 agrupa vários eventos em comum para serem analisados, os mesmos tópicos são abordados em sete testes diferentes no documento ETSI, como pode ser verificado.

TPId: SIP_QC_OE_ V_001
Status: Mandatory
Ref: RFC 3261 [1] sections 11 and 8.1.1.
Purpose: Ensure that the IUT, to query for capabilities sends an OPTIONS request including at least To, From, CSeq, Call-ID, Max-Forwards and Via headers.

TPId: SIP_QC_OE _V_002
Status: Recommended
Ref: RFC 3261 [1] sections 11 and 8.1.1.

Purpose: Ensure that the IUT, to query for capabilities sends an OPTIONS request with a Request-URI set to the same URI value of the To header.

TPId: SIP_QC_OE _V_003

Status: Mandatory

Ref: RFC 3261 [1] sections 11 and 8.1.1.3.

Purpose: Ensure that the IUT, to query for capabilities sends an OPTIONS request including a From header with a TAG parameter.

TPId: SIP_QC_OE _V _004

Status: Mandatory

Ref: RFC 3261 [1] sections 11 and 8.1.1.5.

Purpose: Ensure that the IUT, to query for capabilities sends an OPTIONS request including a CSeq header with a method that matches "OPTIONS".

TPId: SIP_QC_OE _V _005

Status: Recommended

Ref: RFC 3261 [1] sections 11 and 8.1.1.6.

Purpose: Ensure that the IUT, to query for capabilities sends an OPTIONS request including a Max-Forward header set to 70.

TPId: SIP_QC_OE _V _007

Status: Mandatory

Ref: RFC 3261 [1] sections 11 and 8.1.1.7.

Purpose: Ensure that the IUT, to query for capabilities sends an OPTIONS request including a Via header with a protocol name set to SIP, a protocol version set to 2.0 and a branch parameter set to a value beginning with "z9hG4bK".

Neste sentido, foi criada uma grande tabela com o propósito de mapear a equivalência entre todos os testes dos dois cadernos, mas que não está disponibilizada neste estudo. A confecção da tabela foi um instrumento importante para análise mais precisa das diferenças entre os dois modelos. Conseqüentemente, a tabela pode proporcionar ao operador uma ajuda na identificação de um determinado teste no padrão ETSI com o mesmo teste no

Roteiro proposto e vice-versa. Dessa forma, pode-se esclarecer eventuais dúvidas e, principalmente, identificar quais testes existem em apenas um dos documentos e poder avaliar a importância de sua execução.

No caso em que um teste se equivale exatamente ao mesmo teste em outro documento, casos menos comuns em relação ao anterior, pode-se observar um menor grau de detalhamento dos testes ETSI, visto que apresentam apenas suas Referencias (**Ref**) e Proposta (**Purpose**), ao contrário dos testes aqui desenvolvidos, que possuem **Referencias**, **Objetivo**/Proposta, além dos **Procedimentos de Testes** e **Resultados Esperados**, o que garante maior entendimento por parte do operador.

Apesar da tabela comparativa dos Roteiros de Testes não estar presente neste estudo, segue abaixo o Gráfico 1 com a síntese de todos os seus dados, com o propósito de resumir as diferenças e equivalências entre os testes propostos pelos dois modelos.

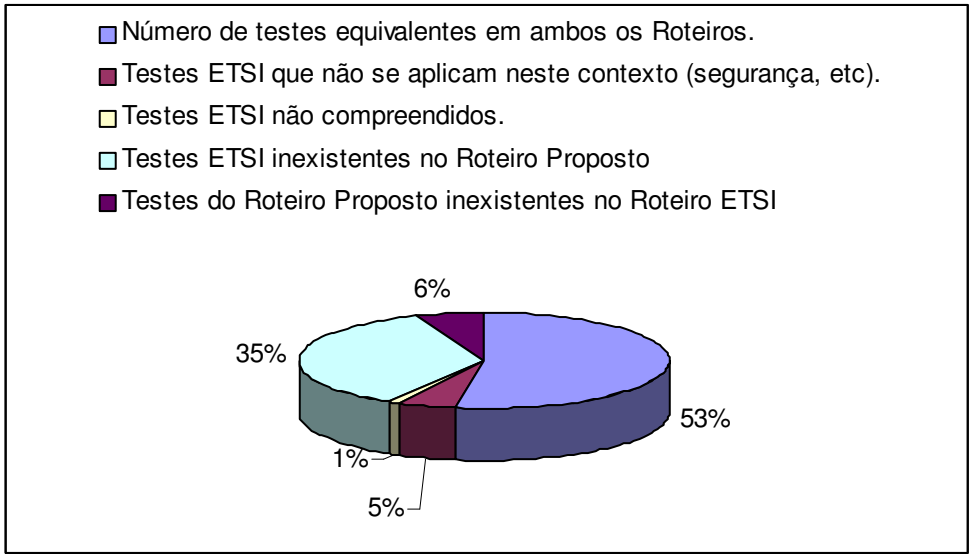


Gráfico 1 - Comparação entre os testes do Roteiro Proposto e do Roteiro ETSI.

3. Media Gateway Control Protocol

Este capítulo é motivado a partir da observação contínua e detalhada do cenário tecnológico mundial, que, devido a sua grande abrangência e complexidade, é capaz de incorporar diversos setores das Telecomunicações, onde não são poucos nem discretos os resultados a serem obtidos quando sua aplicação é inserida em um contexto adequado.

As chamadas redes de nova geração começam a se tornar realidade para os usuários domésticos e bem mais conhecidas pelo segmento corporativo, que deverá ser responsável pela popularização da tecnologia, devido ao cenário competitivo em que está inserido. Por isso, este capítulo inicia-se com uma breve descrição do conceito de redes convergentes, pois o conhecimento de suas aplicações e topologia se torna imprescindível quando o objetivo é compreender o protocolo MGCP (Media Gateway Control Protocol).

O conjunto de testes desenvolvidos que deram origem a este capítulo tem o mesmo objetivo do capítulo anterior, ou seja, avaliar a funcionalidade de equipamentos e soluções VoIP, segundo normas internacionais aplicáveis, porém este capítulo aborda o protocolo MGCP e por isso tem o compromisso de fornecer uma idéia muito mais ampla da relação do protocolo com as demais tecnologias de voz que fazem parte de um contexto muito mais amplo.

A RFC 3435 foi a principal fonte para a elaboração do Roteiro de Testes relativo ao MGCP, além de suas referências. O Tópico 5 da referida recomendação não será objeto de estudo, pois trata das questões de segurança do protocolo. Assim como no capítulo anterior, os testes aqui propostos não serão baseados em eventos comuns de telefonia, como a recepção do sinal de atendimento (chamada bem sucedida), recepção do sinal de desligar para trás ou para frente, envio do sinal de atendimento, envio do sinal de ocupado, entre vários outros, mas todo o conjunto de testes estará moldado pelas normas do protocolo e, portanto, se referem ao correto tratamento e formatação de suas mensagens e da própria funcionalidade do protocolo como um todo.

Redes de Nova Geração

A convergência, atualmente um dos temas mais discutidos na indústria de telecomunicações, nos apresenta uma nova visão sobre o futuro da próxima geração das redes, denominada por Next Generation Network (NGN). A convergência se refere à existência de uma única plataforma de transporte comum para vídeo, voz, dados e aplicações móveis, compondo o chamado *quad-play*.

A NGN apresenta-se como integrador e tradutor de infra-estruturas de diversos meios de transmissão, incluindo xDSL, Cable Modems, fibra óptica, WLANs e a própria rede telefônica tradicional. A essa nova filosofia, adiciona-se não apenas o sonho tecnológico da engenharia em desenvolver uma infra-estrutura centralizada, porém o maior estímulo para a mudança das redes é a redução de custos e um aumento da receita gerada pela integração de recursos e a convergência de tráfego, reduzindo os custos totais da rede, permitindo o compartilhamento da operação, da administração, da manutenção e aprovisionamento de equipamentos, além de criar um ambiente propício para aplicações multimídia.

Para todo novo conceito, faz-se necessária uma definição formal; no entanto, a NGN não possui uma descrição única oficial; a ITU-T, através do grupo NGN Global Standardization Initiative (NGN-GSI), apresenta sua definição e o IETF, assim como o ETSI, também têm, cada qual, sua definição particular. Portanto, seu conceito será definido neste trabalho como sendo um termo genérico para certo tipo de rede convergente, cujo papel central é transportar qualquer fluxo de comunicação multimídia através do protocolo IP, que está inserido em outra camada de rede responsável pela qualidade de serviço, geralmente do tipo MPLS (Multi Protocol Label Switching). A Figura 13 apresenta a NGN como um modelo de 4 camadas; a mais inferior é composta pelos diversos tipos de redes de acesso, a seguinte é referente ao Backbone IP/MPLS, seguida pela camada de controle de comutação de chamadas, realizada através do Softswitch e Signalling Gateway (SGW), finalizada pela camada de mais alto nível referente aos Servidores de aplicação. Cada componente da rede referente à telefonia será discutido em detalhes no decorrer do capítulo, assim como o enquadramento do sub sistema SIP neste contexto.

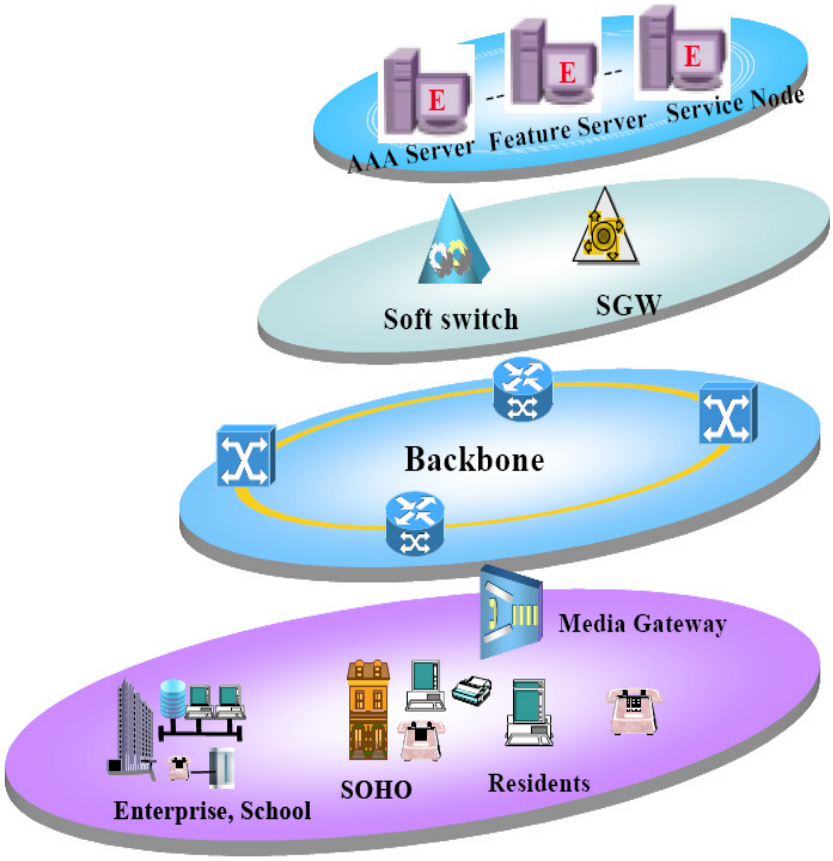


Figura 13: Modelo em Camadas para uma Rede de Nova Geração

Nos primórdios da telefonia IP, o mercado VoIP foi criado usando o estímulo da comunicação internacional de longa distância e a empolgação da nova tecnologia. A partir daí, a credibilidade técnica de se transportar dados em tempo real foi reconhecido pelas operadoras e provedores de serviços, e o envolvimento dos grandes fabricantes de equipamentos na definição de protocolos de telefonia IP mudou bastante e essa tendência foi apoiada por companhias interessadas no mercado de computadores, como a Intel e a Microsoft.

Em meados de 1998, quando se iniciaram os pedidos para construção de grandes redes VoIP, aquelas companhias que não tinham nenhum produto com base no H.323 foram pegas de surpresa. Elas não poderiam deixar a oportunidade passar e, por outro lado, alguns departamentos de P&D perceberam que o H.323v1 não era satisfatório para atender a alguns requisitos importantes das operadoras, ao passo que o SIP ainda estava em

processo de padronização. A partir de então as companhias começaram a propor protocolos alternativos proprietários para atender as necessidades dos negócios em larga escala.

A primeira versão do MGCP foi baseada na união de dois protocolos, o Simple Gateway Control Protocol (SGCP), criado em 1998, que tratava das necessidades das operadoras de cabo a se tornarem CLECs (Competitive Local Exchange Carrier) usando IP no topo de suas infra-estruturas HFC, e a segunda parcela proveniente de um conjunto de protocolos Internet Protocol Device Control (IPDC). As empresas BellCore e Level3 desempenharam um papel central na união destas duas propostas criando o MGCP, cuja premissa era que sua arquitetura fosse projetada para facilitar a interoperabilidade entre uma rede IP transportando dados em tempo real e uma RTPC.

O MGCP, definido inicialmente pela RFC 2705 e atualmente através da RFC 3435, baseia-se na premissa mestre-escravo. Sua principal característica é estabelecer um modelo de chamada centralizado, atuando entre o Controlador de Gateway de Mídia ou Media Gateway Controller (MGC) e o Gateway de Mídia ou Media Gateway (MG), que fará a tradução dos protocolos da rede de acesso para a Rede de Nova Geração IP. Os canais de sinalização são dissociados fisicamente ou logicamente das conexões de mídia.

3.1 Arquitetura

O protocolo MGCP está inserido em uma arquitetura distribuída, conhecida como Arquitetura Softswitch, que se baseia em quatro camadas bem definidas como comentado anteriormente. A Figura 14 apresenta em mais detalhes a arquitetura, onde os elementos de cada camada independem de fabricantes para interoperar.[29]

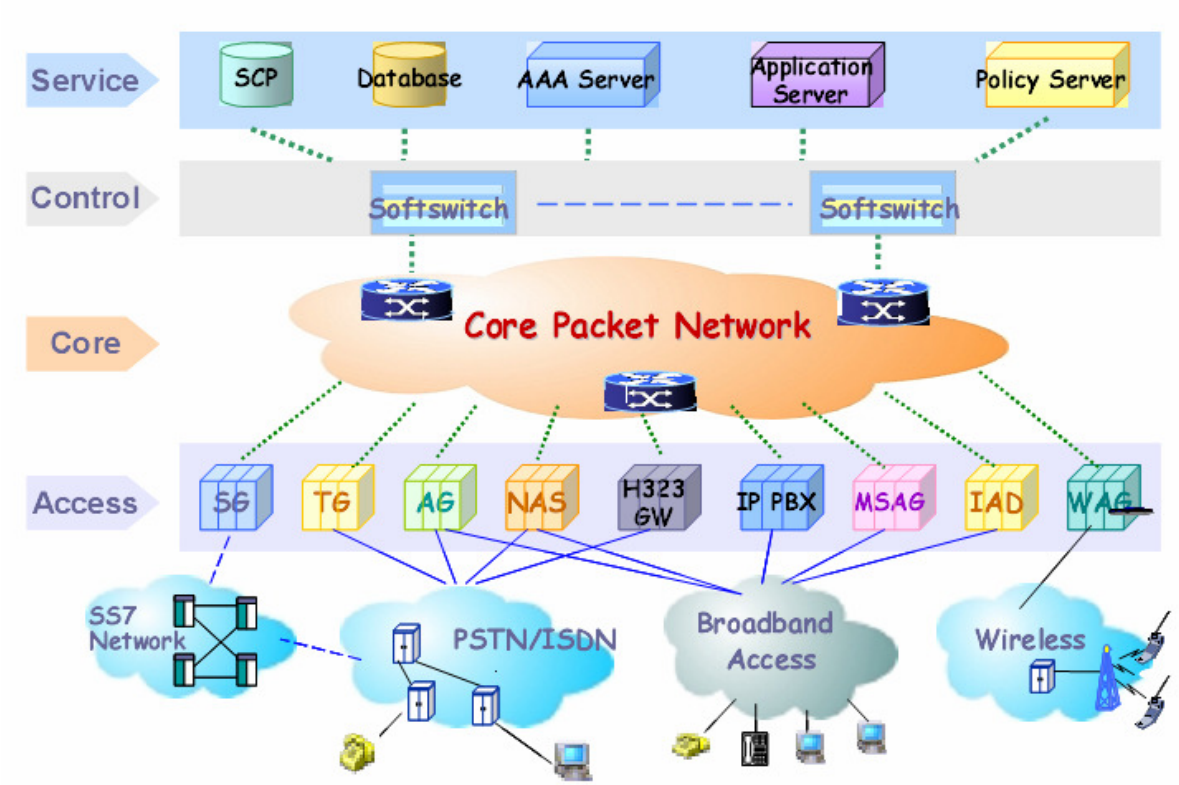


Figura 14: Arquitetura MGCP

Na camada de controle (*Control*) da Figura 14, os Media Gateway Controllers (MGCs), também chamados de Call Agents, tratam do controle e comutação das chamadas e também são chamados de Agentes de Chamada ou simplesmente Softswitch, cujo nome quer dizer comutação através de software. Estes elementos contêm toda a inteligência do controle de chamadas e são responsáveis pela inicialização, encaminhamento, transferência e finalização de chamadas, conferência, roteamento, autenticação, autorização, contabilização e supervisão dos Media Gateways. Esta camada também implementa qualquer protocolo ponto-a-ponto para comunicação entre os MGCs, como H.323, SIP ou SIP-T (SIP for Telephone), por exemplo. Estes protocolos também irão atuar em questões relacionadas à sincronia da chamada quando na criação de uma conexão entre Terminais gerenciados por MGCs distintos. Portanto, a inteligência do controle de chamada não está contida no Gateway, mas é tratada por elementos de controles externos, como sugerido na camada *Control* da Figura 14.[20]

A camada composta pelos Media Gateways (MGs), ou Gateways de Mídia, é identificada na Figura 14 como *Access*, que basicamente recebe instruções e executam os comandos provenientes do Softswitch por meio do protocolo de sinalização MGCP. A função básica destes elementos é a adaptação da mídia entre redes, ou seja, perfaz a tradução de sinais ou a conversão de protocolos entre uma determinada rede de acesso e a rede IP/MGCP. Os MGs são, portanto, equipamentos escravos na hierarquia e podem ser caracterizados pelo seu número de portas, capacidade de compressão, grau de interoperabilidade com diferentes tipos de Softswitches e suporte a múltiplas interfaces de rede.[20]

Como sugerido pela Figura 14, existem vários tipos de Gateways de Mídia, cada qual realiza a tradução de um tipo de serviço para o *Core* IP da rede NGN. Dentre eles, tem-se especial interesse pelo Access Gateway, chamado comercialmente de IAD (Integrated Access Device), que possui várias interfaces de telefonia analógica tradicional (RJ11-telefone DTMF analógico comum) ou uma interface de PABX digital e realiza a tradução de áudio e sinalização básica de assinante para a interface com a rede de voz sobre IP.

Além deste, a proposta dos testes e, conseqüentemente, desta Dissertação é abordar outro tipo de Gateway que realiza a interface com a SS7, chamado de Signalling Gateway (SG). Em todos os casos, a regra do SG é estabelecer e encerrar uma ou mais conexões IP-SS7 e manter o estado de conexão entre as duas redes, mantendo a seqüência de números, confirmações de conexões e retransmissões. O controle de congestionamento, a detecção de falhas nas sessões e segurança são outras funções importantes executadas pelo Signalling Gateway [20]. Importante notar que este tipo de Gateway não realiza a tradução de áudio entre as redes de circuitos e de pacotes, ficando a cargo dos Gateways de Mídia realizarem esse papel, conhecido como Trunking Media Gateways (TMG). Detalhes deste cenário serão visualizados gradualmente com a apresentação da arquitetura utilizada para os testes.

Os Servidores de aplicação fazem parte da camada *Service* na Figura 14, que está conectado ao Softswitch por meio de APIs (Application Programming Interfaces) e protocolos abertos de sinalização. Esta camada possibilita o aprovisionamento de serviços de valor adicionado à rede, que podem contribuir de forma decisiva para a geração de um volume maior de receitas, especialmente em relação ao cenário atual no âmbito da RTPC.

A plataforma aberta permite que terceiros também usem as APIs para criar aplicativos customizados em períodos curtos de tempo e garantir às operadoras oportunidades de diferenciação competitiva.

E, por fim, a camada *Core* representa os roteadores da rede IP propriamente dito, cuja abrangência é determinada pela operadora de telecomunicações e geralmente é dotada de QoS e recursos se segurança, visto que a rede é multiserviços.

Este estudo tem especial interesse pelas camadas *Control* e *Access*, nas quais o protocolo MGCP atua. A arquitetura preliminar utilizada para os testes é apresentada na Figura 15 e será construída na medida em que novos conceitos forem sendo introduzidos.

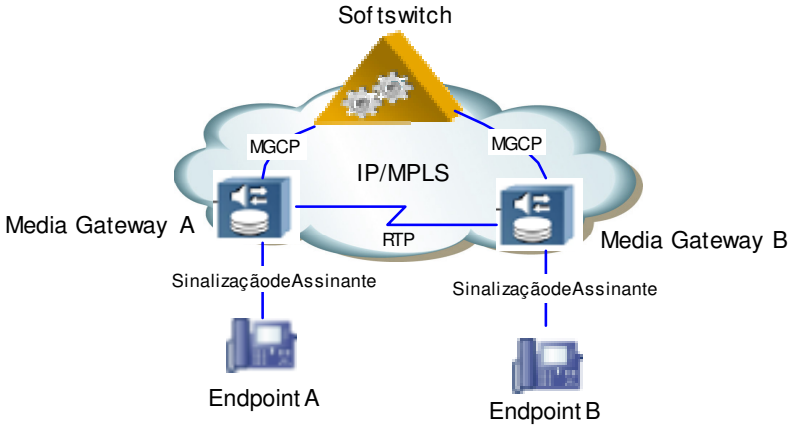


Figura 15: Arquitetura de Testes - Parte I

A Figura 15 sugere uma arquitetura do protocolo MGCP baseada em uma NGN sob o ponto de vista das aplicações de voz. O padrão mais básico da rede física para execução dos testes será composto por um *Softswitch*, dois Media Gateways ligados a um *Endpoint* cada um. O *Softswitch* realiza a função de controle de comutação de chamada e possui todo o controle sobre os Gateways de Mídia através do protocolo MGCP. Os Endpoints se comunicam com os respectivos Media Gateways através da Sinalização de Assinante, conforme visto no capítulo 2. Importante notar que o Endpoint utilizado neste exemplo se refere à um telefone analógico comum, apesar da norma do protocolo MGCP definir Endpoint como um conceito mais amplo. Um Endpoint é definido como sendo fonte ou receptor de dados, podendo ser físico ou virtual. Exemplos: Telefone IP, linhas analógicas, linhas tronco (T1, E1, etc.), etc.

3.2 Endereçamento

Antes da análise direta do endereçamento do protocolo, é necessário acrescentar que cada Gateway possui uma ou várias interfaces de conexão para os Terminais, também chamados de *Endpoints* neste trabalho. Um Gateway pode ter várias interfaces para redundância, lembrando que, ao invés de apenas Terminais, o Gateway pode conter interfaces para linhas tronco do tipo E1, por exemplo.

Assim como no protocolo SIP, o endereçamento MGCP é codificado seguindo a mesma sintaxe do e-mail, ou seja, é composto por duas entidades separadas pelo caractere "@". Desse modo, cada Terminal é especificado na rede pelo domínio do Gateway a que pertence e pelo nome local dentro do Gateway, assumindo a forma: local-terminal-name@gateway-name.gateway-domain-name:port_number. Todos estas referências podem ser feitas diretamente através de endereço IP (IPv4 ou IPv6). O endereço do Agente de Chamada (Softswitch) também segue o mesmo padrão: local-call_agent-name@call_agent-domain-name:port_number. [30]

O conceito geral de endereçamento é o mesmo do protocolo SIP, embora a arquitetura e a referência aos elementos de rede sejam consideravelmente diferentes. Em termos práticos, pode-se observar numa primeira análise que o endereço do Softswitch não está contido em nenhuma mensagem MGCP, visto que seu endereço é conhecido pelos terminais a partir da configuração realizada a priori no Media Gateway. Portanto, o endereço do Softswitch pode ser verificado apenas no nível da camada IP ou através da configuração do próprio Media Gateway. Em relação ao endereço dos terminais, é importante notar que existem vários tipos de terminais e cada um é identificado diferentemente pelo protocolo. A arquitetura proposta para realização dos testes sugere a seguinte nomenclatura:

Terminal 1 : aaln/1@iad07.com
Terminal 2: aaln/2@iad07.com

A *string* "aaln" deve sempre ser utilizada como o primeiro termo de um Terminal do tipo analógico controlado por um Media Gateway. O número da porta na qual o Terminal está conectado vem em seguida, separado por uma barra do campo anterior. Uma vez

determinado o tipo de Terminal e sua respectiva porta de acesso no Gateway, a segunda parte do endereço é composta pelo domínio ou nome do Media Gateway, que no exemplo é “iad07.com”. O Softswitch possui um endereço IP, que deve ser configurado no Gateway.

É importante verificar, portanto, as regras de formação do endereço de cada terminal, que, independe da representação em caixa-alta ou caixa-baixa, é dependente do tipo de terminal e possui certa hierarquia em sua sintaxe de acordo com a localização física no Gateway. O MGCP ainda especifica caracteres coringas para os casos em que se deseja referenciar um ou mais tipo de Terminal ou porta simultaneamente e, conseqüentemente, são caracteres reservados pelo protocolo, incluindo “@”, ”/”, ”*” e ”$”; todos os outros caracteres podem ser utilizados para nomear um Terminal. Daí surge o interesse em verificar o comportamento do protocolo quando induzido ao processamento de endereço desconhecido ou inválido, como retornado pela mensagem: *500 The transaction could not be executed, because the endpoint is unknown*, por exemplo.

Casos em que o número da porta é omitido devem ser testados, visto que a porta padrão do Agente de Chamada é 2727 e do Gateway é 2427. O MGCP trabalha tanto com IPV4 quanto IPV6 para endereçamento, sendo que este último foi inserido mais recentemente pela nova recomendação do protocolo, item que também sugere análise.

As questões de mobilidade e redirecionamento de chamadas são tratadas no MGCP de forma semelhante ao protocolo SIP. Portanto, toda vez que um endpoint pertence a um novo domínio caracterizado por outro Softswitch, diz-se que o endpoint foi redirecionado, pois recebe a mensagem *521 Endpoint Redirected to Another Call Agent*. Esta mensagem de resposta tem que incluir o parâmetro NotifiedEntity com o nome do novo Softswitch ao qual o endpoint pertence. Após este processo, o endpoint deve reinicializar novamente com o novo endereço do Softswitch.

Já é possível notar várias semelhanças deste protocolo com o SIP, apesar das particularidades inerentes a um protocolo mestre-escravo como o MGCP. Importante notar que a recomendação do MGCP chama os cabeçalhos das mensagens de sinalização de parâmetros, diferentemente do protocolo SIP. Portanto, chamaremos de parâmetros os cabeçalhos das mensagens MGCP. Um recurso não permitido pelo protocolo e que existe

no H.323v2 é a capacidade de um MGC fornecer os endereços de outros MGCs para servir de redundância ou como *backup* para os casos de falhas. Essa tarefa é realizada pelo Gatekeeper no H.323.

3.3 Sinalização MGCP

O protocolo MGCP é usado para estabelecer, manter e desconectar chamadas através de redes IP e permite a interconexão com diversos tipos de redes, como ATM, Celular e RTPC, por exemplo [29]. De forma bastante genérica, a Figura 16 apresenta um cenário de aplicação de voz para o protocolo MGCP, onde a rede NGN surge como complementar/substituta das Centrais Tandem de telefonia fixa. A realização de chamadas de longa distância é perfeitamente possível utilizando-se apenas a rede IP e as Centrais Locais de origem e de destino, através do percurso em vermelho na Figura 16, em substituição às tradicionais Centrais Trânsito de qualquer Classe ou hierarquia.

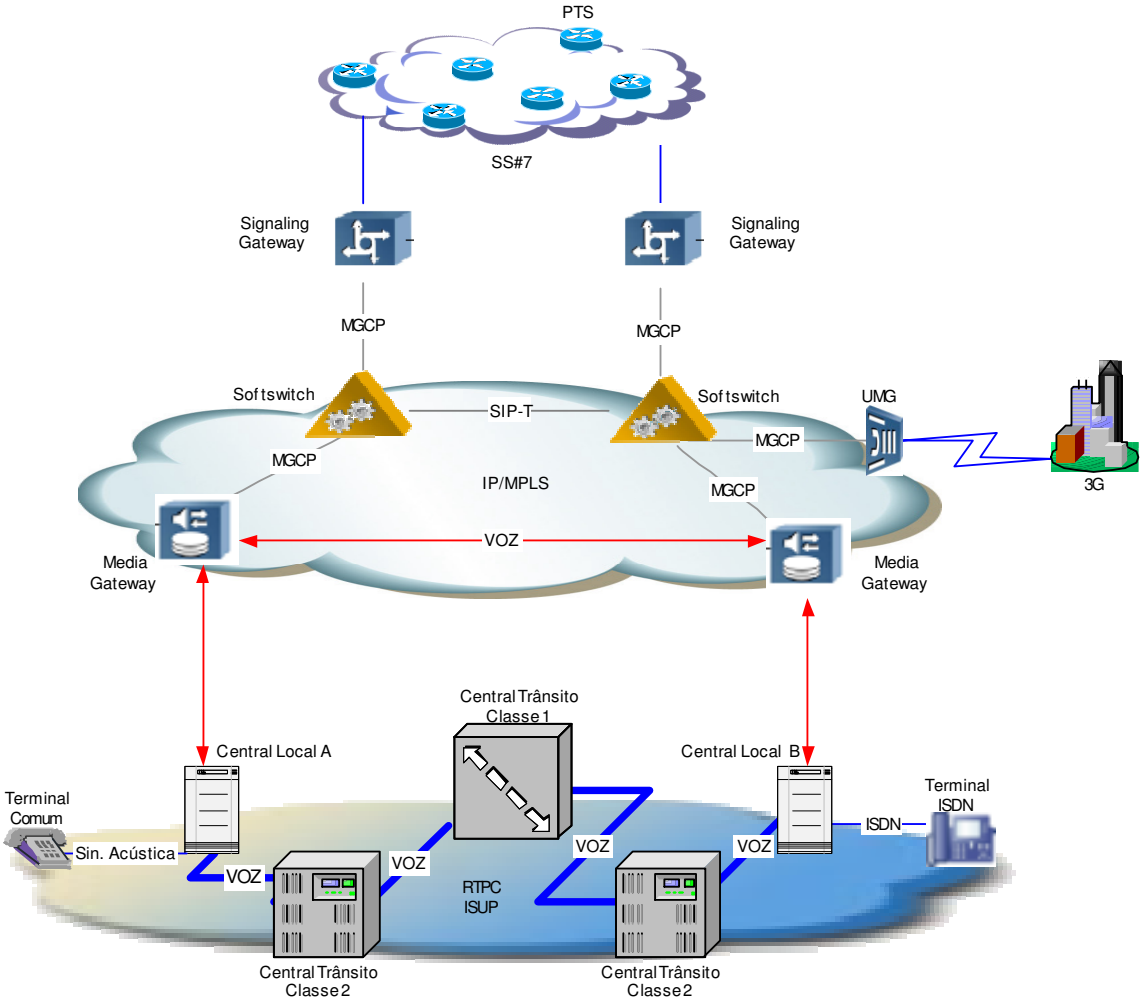


Figura 16: Cenário de Aplicação de Voz para o Protocolo MGCP

A Figura 16 vai um pouco além na arquitetura proposta e ilustra a interligação de dois MGCs com diversos tipos de *Gateways*. Os Gateways de Mídia fornecem funções de tradução de áudio e os Signalling Gateways (SG) são as interfaces da NGN com a rede de telefonia pública tradicional. A interface com a rede celular realizada através do UMG (*Universal Media Gateway*) é apenas ilustrativa, visto que não foi contemplada nos testes.

3.3.1 Comandos MGCP

O protocolo de controle de mídia é composto por comandos e respostas, trocados entre os *Gateways* e seus controladores, compondo um total de 10 comandos primitivos e que serão detalhados a partir de agora. Cada mensagem é representada aqui pelo seu nome completo, abreviação entre parênteses, seguida pelo seu sentido de fluxo.

I. NotificationRequest (NTRQ) MG ← MGC

O comando NotificationRequest é enviado pelo MGC com determinadas instruções para que o MG envie uma notificação na ocorrência de EVENTOS específicos no endpoint, como reportar informações de fone fora do gancho, enviar números discados, etc. O MGC também faz uso desta mensagem para enviar SINAIS de controle ao Media Gateway, como enviar sinal de toque, tom de ocupado, etc. Testes destes e outros eventos certamente devem ser realizados, observando a redução drástica dos números de idas e vindas necessárias para estabelecer uma conexão entre dois terminais, já que o protocolo permite o envio de vários SINAIS e o recebimento de vários EVENTOS simultâneos em uma única mensagem, aumentando, portanto, a escalabilidade do protocolo. Os EVENTOS e SINAIS estão neste parágrafo em caixa alta porque são extensões definidas pela norma, ou seja, EVENTOS são todas as informações reportadas pelo Gateway ao MGC, geralmente enviadas através do comando Notify, e SINAIS são sinalizações, geralmente audíveis, enviados ao Gateway pelo MGC através da mensagem NTRQ.

Esta mensagem ocupa papel central na implementação do protocolo, juntamente com o comando Notify que vem a seguir, já que fazem parte da fase inicial de troca de informações de sinalização telefônica, similar a Sinalização de Assinante, apresentada no Capítulo 2.

Nessa fase, o Gateway tem três opções para notificar ao MGC a existência de algum evento. O mais comum é o Endpoint receber a mensagem NTRQ com o parâmetro *RequstedEvents* contendo a informação dos eventos que deve detectar e reportar ao MGC.
O parâmetro opcional *DetectEvents* é utilizado pelo comando NTRQ e especifica uma lista de eventos que o Gateway é solicitado a detectar durante o período de quarentena. Este

período é iniciado logo após o Gateway ter enviado a resposta ao NTRQ e a recepção de outra mensagem NTRQ. Neste caso, o parâmetro *QuarantineHandling* é utilizado pelo MGC através da mensagem NTRQ para especificar o tratamento destes eventos definidos como em quarentena. Em termos práticos, o protocolo MGCP prevê ainda a notificação de um conjunto de eventos chamados de persistentes, em que o Gateway pode informar ao MGC a sua existência antes mesmo de receber qualquer comando NotificationRequest, independentemente de mensagens ou parâmetros anteriores. Resumindo, qualquer evento que ocorra no Endpoint antes que o Gateway receba a mensagem NTRQ e que seja reportada ao MGC através do comando Notify pode ser considerado persistente. Portanto, o Gateway é capaz de detectar estas três condições iniciais de operação, que devem ser induzidas e analisadas através dos testes, de acordo com o padrão do protocolo.

Certamente que condições de erro também são avaliadas, como a de telefone "no gancho" ou "fora do gancho". O primeiro caso proporciona a observação das mensagens de erro do tipo *401 phone off hook*, quando o Gateway é requisitado a notificar o evento "fora do gancho" ao Agente de Chamada, porém o usuário já está previamente com o telefone fora do gancho. O outro caso é análogo ao anterior e se refere à notificação do evento "no gancho" quando o telefone já está no gancho. Neste caso, a mensagem retornada deve ser do tipo *402 phone on hook*.

Em relação à análise de conformidade desta mensagem de sinalização, a primeira medida é verificar a inclusão e a equivalência dos parâmetros obrigatórios do comando e observar a possibilidade de inserção dos parâmetros na forma abreviada, isto é, com no máximo dois caracteres. Aliás, essa medida vale para todos os comandos subseqüentes do protocolo.

II. Notify (NTFY) MG → MGC

Comando de resposta enviado pelo Gateway ao MGC contendo os eventos observados através do parâmetro *ObservedEvents*. Os eventos notificados podem ser entendidos como aqueles pertencentes à Sinalização de Linha, apresentada no Capítulo 2, visto que o MG é o elemento escravo na rede, assim como o telefone analógico é o elemento passivo na RTPC.

Seguindo a metodologia proposta, os dispositivos devem ser submetidos a condições de erro sempre que possível e neste caso a percepção de eventos desconhecidos pelo MGC deve ser tratada através da mensagem de erro *512 The transaction could not be executed, because the gateway is not equipped to detect one of the requested events*. Neste momento, deve ser observada as condições de equivalência dos parâmetros entre esta mensagem e a NTRQ, devido a grande dependência entre estes dois comandos.

III. CreateConnection (CRCX) MG ← MGC

O comando CreateConnection é enviado pelo Softswitch para criar uma conexão entre dois Terminais. O comando é sempre enviado para as duas pontas de uma chamada. Ao final da definição dos comandos MGCP, será apresentado um fluxo de comunicação do protocolo para ficar mais claro o entendimento das mensagens de sinalização.

O objetivo do grupo de testes relativo ao CRCX é verificar o comportamento de envio do comando e posterior recebimento da mensagem de resposta, com destaque para o surgimento do parâmetro CallId, responsável pela identificação de uma chamada, que pode conter mais de uma sessão ou conexão. A observação da formação correta deste parâmetro é importante porque será utilizado no reporte de *status* da chamada e bilhetagem.

O comando CreateConection é enviado pelo MGC aos dois Gateways, sendo as duas mensagens com características semelhantes, porém com as suas particularidades. O parâmetro Mode indica o modo de operação de cada lado da conexão, podendo assumir valores básicos como “send”, ”receive”, “send/receive”, ”conference”, “inactive”, etc. Deve ser observado que alguns Terminais não tem suporte a todos os modos definidos pela norma, neste caso sendo retornado uma mensagem de erro.

Um parâmetro importante no comando CRCX é o LocalConnectionOptions, utilizado pelo MGC para descrever as capacidades e características sugeridas ao Gateway, como requisitos de banda, CODECs, tipo de serviço, cancelador de eco, supressor de silêncio, segurança, etc. Apesar de opcional, quando presente na mensagem o parâmetro deve ser compatível com as características especificadas pelos protocolos SDP e RTP, que estarão presentes na mensagem de resposta a este comando.

Outra avaliação pertinente é em relação ao encapsulamento de comandos, importante na redução do número de mensagens trocadas entre entidades do protocolo. A mensagem CreateConnection encapsula os comandos NotificationRequest e EndpointConfiguration individualmente ou juntos, na ordem CreateConnection >> NotificationRequest >> EndpointConfiguration. Não basta configurar o elemento de rede para enviar ou interpretar estes eventos, o mais importante é notar o comportamento dos parâmetros nestes casos, visto que alguns deles são necessários apenas na mensagem de mais alto nível, enquanto outros devem constar obrigatoriamente nos dois ou três comandos encapsulados.

IV. ModifyConnection (MDCX) MG ← MGC

O comando ModifyConnection é utilizado para modificar a visão do Gateway em relação a conexão, visto que os Terminais até o momento se comunicam com o MGC, que criou a conexão com cada um através do comando CreateConnection. Através deste comando o MGC é capaz de mediar e determinar as características em comum dos dois Gateways, com o objetivo de estabelecer a comunicação direta fim-a-fim.

Deve ser observado que os parâmetros e campos em ModifyConnection são os mesmos daqueles do comando CreateConnection, apenas com a adição do parâmetro *ConnectionID*, que identifica unicamente a conexão com o Terminal. Normalmente, o valor do parâmetro Mode passa a ser “sendrec” ao invés de “reconly” como no comando CreateConnection.

Este comando permite a introdução de mais um parâmetro, o RemoteConnectionDescriptor, que, assim como o LocalConnectionDescriptor, são especificados pelo protocolo SDP; a diferença é que especifica as características do Gateway remoto.

Para este comando, os testes são praticamente análogos ao Grupo de Testes da mensagem CreateConnection; entretanto, deve-se tratar individualmente as questões de encapsulamento, formatação e respostas particulares ao comando, assim como devem ser observadas as alterações de algumas características de comunicação no campo SDP, como durante a negociação de capacidades, por exemplo.

V. DeleteConnection (DLCX) MG ←→ MGC

O Agente de Chamada utiliza o comando DeleteConnection para encerrar a conexão entre dois Terminais ou excluir todas as conexões de um dado *Gateway*, que por sua vez também se utiliza deste comando para encerrar conexões e liberar o canal se detecta que um Terminal não é mais capaz de enviar ou receber áudio. Se o Gateway exclui uma conexão, é incluída uma razão na mensagem indicando sua causa.

Em resposta ao comando DeleteConnection, o Gateway retorna uma lista de parâmetros que descrevem estatísticas relacionadas à chamada, como pacotes enviados e recebidos, pacotes perdidos, jitter e latência e pode ser observado através do parâmetro ConnectionParameters.

Além dos testes já citados como os referentes à sintaxe, respostas e encapsulamentos, é necessário observar as possíveis diferenças entre a desconexão realizada pelo Gateway e pelo Softswitch.

VI. AuditEndpoint (AUEP) MG ← MGC

O comando AuditEndpoint é utilizado pelo MGC com a finalidade de auditar parâmetros e capacidades de um determinado Terminal. Deve ser observado que todos os parâmetros auditados devem ser respondidos e nos casos em que o parâmetro auditado é desconhecido pelo Gateway, este não deve disparar uma mensagem de erro, mas apenas omitir o parâmetro requisitado na mensagem de resposta.

Muitos parâmetros e os respectivos valores passiveis de serem auditados já foram descritos ou ainda o serão ao longo deste capítulo. Entretanto, as capacidades dos Endpoints que podem ser auditadas ainda não foram apresentadas; portanto, o parâmetro Capabilities inclui as seguintes informações: lista de CODECs suportados, período de empacotamento, banda, cancelador de eco, supressão de silencio, controle de ganho, tipo de serviço, RSVP, criptografia, tipo de rede e modo de operação (Mode).

As mensagens MGCP são transmitidas através do protocolo UDP encapsulado pelo protocolo IP. O *overhead* dos protocolos UDP e IP somados é de 28 *bytes*; o tamanho máximo teórico do datagrama IP é de 65535 *bytes* e o mínimo teórico de 576 *bytes*. A norma exige que o tamanho mínimo de um datagrama MGCP seja 4000 *bytes*, pois um valor inferior diminuiria o percentual de informação útil em relação ao tamanho de *overhead* de todos os protocolos somados. Esta premissa é verdadeira tanto para Terminais quanto para o Agente de Chamada; este último pode verificar o tamanho do datagrama MGCP praticado pelos terminais com a mensagem AuditEndpoint através do parâmetro MaxMGCPDatagram. Entretanto, os terminais não têm a capacidade de auditar o Agente de Chamada.

Um teste de capacidade pode ser concretizado através do envio do comando AUEP com o caractere curinga “All of”, pois a resposta deve conter os parâmetros auditados separados de cada Terminal através do parâmetro EndpointIdList. Caso a listagem de capacidades dos Terminais auditados seja maior que o tamanho máximo do datagrama MGCP, uma resposta de erro do tipo *533 – responsse too large* deve ser retornada.

VII. AuditConnection (AUCX) MG ← MGC

O Agente de Chamada utiliza este comando para recuperar parâmetros referentes a uma determinada conexão. Em caso de sucesso no processamento do comando AuditConnection, a resposta também deve conter todas as informações dos parâmetros requisitados.

VIII. EndpointConfiguration (EPCF) MG ← MGC

O comando EndpointConfiguration enviado pelo Agente de Chamada especifica a codificação dos sinais da PSTN recebidos pelo endpoint. O parâmetro BearerInformation contém a codificação utilizada pelo lado da PSTN, que pode assumir o valor a-law ou u-law, dependendo da rede telefônica analisada. Portanto, os testes referentes a esta mensagem devem ser configurados de tal forma que o MGC tenha interconexão com a PSTN.

IX. RestartInProgress (RSIP) MG → MGC

O comando informa ao Agente de Chamada que um Terminal ou um grupo de Terminais está fora de serviço ou está reiniciando seus serviços. O comando é útil na notificação de problemas e deve ser observado em diversos momentos na rede.

A primeira observação se refere à forma de inicialização do Terminal através do parâmetro RestartMethod, que pode assumir o valor *Restart* quando o MG foi iniciado normalmente, *Graceful* indicando que nenhuma conexão foi perdida, visto que o Endpoint foi reiniciado de forma programada, *Forced* quando há perda de algumas conexões, já que o Endpoint foi abruptamente desligado e posteriormente reinicializado, etc.

A segunda análise é referente ao redirecionamento de Terminais, pois toda vez que um endpoint pertence a um novo domínio, caracterizado por outro Softswitch, diz-se que o endpoint foi redirecionado e recebe a mensagem *521 Endpoint Redirected to Another Call Agent* por parte do MGC. Esta mensagem de resposta tem que incluir o parâmetro NotifiedEntity com o nome do novo Softswitch ao qual o endpoint pertence. Após este processo, o endpoint deve reinicializar novamente com o novo endereço do Softswitch através da mensagem RestartInProgress.

Uma última análise se refere ao comportamento do Agente de Chamada quando um grande número de Gateways é inicializado simultaneamente. Para evitar perdas de mensagens e congestionamento da rede, durante o processo de (re) inicialização, os Gateways devem gerar um *timer* aleatório, cujo valor observado deve pertencer ao intervalo de zero ao valor máximo de *delay* de espera (Maximum Waiting Delay). O valor MWD *default* para um gateway residencial é de 600 segundos e um valor típico sugerido seria de 10 a 12 minutos. Portanto, deve-se evitar a sincronização do valor do *timer* dos Gateways que utilizem o mesmo algoritmo de geração de tempo.

3.3.2 Sintaxe dos Comandos MGCP

Cada mensagem de sinalização é composta por um comando de linha e seus diversos parâmetros, formando o chamado *command header* ou cabeçalho da mensagem. A descrição de sessão de áudio é especificada pelo protocolo SDP, compondo a segunda parte da mensagem, formando o chamado *message body* ou corpo da mensagem, da mesma forma que no protocolo SIP. Outra característica idêntica ao SIP é que toda mensagem é representada em formato de texto, utilizando o conjunto de caracteres ASCII. A sintaxe da linha de comando do protocolo MGCP é apresentada a seguir, onde SP é o caractere espaço [28]. Portanto, as verificações mais básicas de conformidade refererindo-se a análise e a boa formação dos comandos MGCP devem ser avaliados:

CommandVerb **SP** TransactionID **SP** TerminalID **SP** MGCP 1.0 **CRLF**

Parameter Line(s)

.

.

<linha em branco>

[SDP]

CommandVerb são os comandos descritos anteriormente e codificados seguindo a respectiva sigla entre parênteses. Os parâmetros referentes ao comando seguem em linhas subseqüentes e a descrição da sessão é separada da linha de comando e de seus parâmetros por uma única linha em branco, também de forma similar aos pacotes SIP. O campo *TransactionID* correlaciona o comando às respectivas respostas, o campo *TerminalID* representa a identificação do Terminal pertencente ao Gateway, podendo opcionalmente conter informação de porta, o comando é finalizado com a versão do protocolo. O caractere CRLF termina a linha de comando e significa *Carriage Return Line Feed.*

O campo *TransactionID* é codificado como uma string de até nove dígitos decimais. Importante notar também que uma mensagem com a versão do protocolo não suportada pelo dispositivo é responsável pela geração da seguinte mensagem de erro: *528 Incompatible Protocol Version*. Interessante observar que todos os campos do protocolo MGCP podem ser representados em caixa alta ou baixa, de acordo com RFC 2234, isto

inclui os verbos dos comandos, parâmetros e valores, mas não inclui os campos do SDP. Portanto, os dois tipos de representação, ou ainda um misto delas, devem ser tratados da mesma forma pelos dispositivos.

A Figura A.8 do Anexo A apresenta um diagrama de fluxo de comunicação comentado de uma chamada básica bem sucedida do protocolo MGCP, de forma a exemplificar a utilização das mensagens explicitadas anteriormente. Os parâmetros de cada mensagem do exemplo também são identificados, apenas para familiarizar o leitor com o esquema do protocolo, pois serão definidos a seguir.

As mensagens MGCP são sempre transportadas através do protocolo UDP, por isso os comandos são retransmitidos em caso de falha e as respostas das transações mais recentes são mantidas em memórias caso haja necessidade de retransmissão. Um teste para avaliação desta condição foi desenvolvido com objetivo de gerar uma alta quantidade de informações a partir do Terminal, de forma a superar a capacidade do *buffer* do Gateway. Neste caso, os eventos não processados devem ser descartados e o surgimento do parâmetro *Quarantine Buffer Overflow* deve ser verificado. O algoritmo de retransmissão é apresentado em detalhes através de um diagrama de estados na seção 4.3 da RFC 3435. Os testes propostos relativos a temporização das mensagens de sinalização não foram contemplados como no diagrama de estado do protocolo; outra abordagem foi feita, já que a responsabilidade de especificar o valor de *timeout* para retransmissão de uma mensagem em caso da ausência de resposta é do dispositivo que realiza a requisição. O valor de *timeout* pode variar de rede para rede e deve respeitar o recuo exponencial de tempo, sendo o código de erro associado à mensagem de *timeout 406 Transaction Time-out*.

Há casos em que o Agente de Chamada deseja enviar várias mensagens ao mesmo tempo para os gateways e vice-versa, com objetivo de garantir a entrega ordenada ou para garantir o envio das mesmas mensagens para mais de um destino. Portanto, além da facilidade de encapsulamento de comandos já abordada, o MGCP ainda permite o envio de vários comandos em um mesmo pacote UDP simultaneamente, desde que sejam respeitadas algumas regras simples. Nestes casos, o protocolo MGCP agrega todas as mensagens na capacidade de um datagrama, e para isso cada mensagem deve estar separada de uma linha

com um ponto”.”. Sendo que as mensagens devem ser processadas individualmente na recepção e na ordem em que foram inseridas.

3.3.3 Parâmetros MGCP

Assim como no protocolo SIP, as mensagens apresentadas anteriormente contêm parâmetros específicos requeridos para executarem suas funções. Neste sentido, a Tabela 13 apresenta a correlação entre as mensagens de sinalização e seus respectivos parâmetros Opcional (O), Mandatório (M) ou Forbidden (F) [28].

Parameter name	EP CF	CR CX	MD CX	DL CX	RQ NT	NT FY	AU EP	AU CX	RS IP
BearerInformation	O	O	O	O	O	F	F	F	F
CallId	F	M	M	O	F	F	F	F	F
Capabilities	F	F	F	F	F	F	F	F	F
ConnectionId	F	F	M	O	F	F	F	M	F
ConnectionMode	F	M	O	F	F	F	F	F	F
Connection-Parameters	F	F	F	O*	F	F	F	F	F
DetectEvents	F	O	O	O	O	F	F	F	F
DigitMap	F	O	O	O	O	F	F	F	F
EventStates	F	F	F	F	F	F	F	F	F
LocalConnection-Options	F	O	O	F	F	F	F	F	F
MaxMGCPDatagram	F	F	F	F	F	F	F	F	F
NotifiedEntity	F	O	O	O	O	O	F	F	F
ObservedEvents	F	F	F	F	F	M	F	F	F
PackageList	F	F	F	F	F	F	F	F	F
QuarantineHandling	F	O	O	O	O	F	F	F	F
ReasonCode	F	F	F	O	F	F	F	F	O
RequestedEvents	F	O	O	O	O	F	F	F	F
RequestIdentifier	F	O	O	O	M	M	F	F	F
RequestedInfo	F	F	F	F	F	F	O	M	F
ResponseAck	O	O	O	O	O	O	O	O	O
RestartDelay	F	F	F	F	F	F	F	F	O
RestartMethod	F	F	F	F	F	F	F	F	M
SecondConnectionId	F	F	F	F	F	F	F	F	F
SecondTerminalId	F	O	F	F	F	F	F	F	F
SignalRequests	F	O	O	O	O	F	F	F	F
SpecificTerminalId	F	F	F	F	F	F	F	F	F
RemoteConnection-Descriptor	F	O	O	F	F	F	F	F	F
LocalConnection-Descriptor	F	F	F	F	F	F	F	F	F

Tabela 13: Comandos e Parâmetros MGCP

* O parâmetro ConnectionParameters é válido apenas na mensagem **DeleteConnection** enviada pelo Gateway.

A Tabela 14 apresenta as funções dos principais parâmetros que compõem as mensagens de sinalização do protocolo MGCP. As siglas entre parênteses representam a abreviação de cada parâmetro, que é a forma compacta e utilizada na mensagem de sinalização. A descrição formal e completa de todos os parâmetros pertencentes aos comandos MGCP são encontrados na seção 3.2.2 da RFC 3435.

Além dos testes referentes a inclusão dos cabeçalhos obrigatórios nos comandos e respostas, outro objetivo é verificar o comportamento dos dispositivos em relação aos parâmetros mal formados ou desconhecidos, já que estes não têm impacto direto na interoperabilidade dos elementos.

Parâmetros	Descrição
Notified Entity (N)	Se presente na mensagem, especifica o endereço da entidade na qual a notificação deve ser enviada. Se não presente, indica que a notificação deve ser enviada ao originador da chamada.
Request Identifier (X)	O parâmetro é usado para fazer a correlação do comando inicial com a respectiva resposta disparada ou com o comando consecutivo associado ao original. Importante notar que o valor do campo é um hexadecimal de até 32 caracteres e não menos importante avaliar o comportamento quando o parâmetro assume o valor "0", pois este é reservado para reportar eventos persistentes nos casos em que um NotificationRequest ainda não tenha sido recebido após a inicialização do Gateway.
Signal Requests (S)	Especifica um conjunto de ações requisitadas pelo Gateway e enviadas para o Terminal. Na verdade estes sinais são provenientes do Agente de Chamada e enviados a cada Terminal através de seus Gateways. Inclui toque, toque para trás, ocupado, chamada em espera, tom de discar, entre outros.
Observed Events (O)	Representa uma lista de eventos detectados e acumulados pelo

	Gateway.
Call ID (C)	Identificador global para todas as conexões de uma mesma chamada.
ConnectionId (I)	Identificador de uma conexão com o MGC, geralmente criada a partir de uma resposta ao comando CRCX.
Mode (M)	Operação em duplex, simplex, inativo, conferência ou *loopback*.
Bearer Information (B)	Identifica a técnica de codificação utilizada tanto na transmissão quanto na recepção dos sinais.
Reason Code (E)	O parâmetro ReasonCode indica a causa do comando DeleteConnection e é composto por um código numérico seguido por um texto descritivo da razão da desconexão. A lista completa de códigos é encontrada na seção 2.5 da RFC 3435.
Connection Parameters (P)	Apresenta a estatística da conexão, isto é, de pacotes enviados e recebidos e medidas de perda de pacotes, latência e jitter.
Capabilities (A)	O parâmetro Capabilities é utilizado para informar ao Call Agent as capacidades quando auditadas. O parâmetro inclui as seguintes informações: lista de CODECs suportados, período de empacotamento, banda, cancelador de eco, supressão de silencio, controle de ganho, tipo de serviço, RSVP, criptografia, tipo de rede e modo de operação (Mode).

Quando o Agente de Chamada envia o comando CreateConnection ou ModifyConnection, três parâmetros devem ser analisados, pois determinam o tipo de mídia suportado pela conexão:

Local Connection Descriptor (LC)	O parâmetro é encontrado nas mensagens enviadas pelo Gateway ao Agente de Chamada para informar os parâmetros de mídia suportados para a conexão. O parâmetro LocalConnectionDescriptor deve estar codificado dentro do corpo da mensagem, isto é, seus valores estarão especificados pelo protocolo SDP.
Remote Connection Descriptor (RC)	O parâmetro é análogo ao anterior, porém se refere às características do Gateway remoto. O parâmetro SecondTerminalId pode ser utilizado em

	substituição a este para estabelecer uma conexão entre dois Terminais localizados no mesmo Gateway.
Local Connection Options (L)	Descreve os parâmetros operacionais que o Agente de Chamada fornece ao Gateway. Exemplo: método de codificação, período de empacotamento, banda, tipo de serviço, cancelamento de eco, supressão de silêncio, controle de ganho, criptografia, tipo de rede e reserva de recursos. Quando estes parâmetros são fornecidos pelo Agente de Chamada, o Gateway é obrigado a utilizá-los até que a conexão seja encerrada ou enviado um comando do tipo ModifyConnection com os novos parâmetros de comunicação.
O protocolo MGCP envia pedidos para notificação de eventos de forma que qualquer evento interpretado pelo Gateway possa ser notificado para o Agente de Chamada. Os quatro parâmetros responsáveis pelo transporte destes eventos seguem abaixo e devem ser obrigatoriamente verificados pelos dois dispositivos envolvidos na transação:	
Requested Events (R)	Contém a listagem de eventos que Gateway deve detectar e reportar ao Agente de Chamada. Possíveis eventos da lista seriam tons de fax e de modem, ramal no gancho ou não, sinais DTMF, etc. Além disto, cada evento tem uma ação associada, como a de notificar o evento imediatamente, acumular dígitos, ignorar o evento, etc.
Digit Map (D)	Mapa de dígitos é um conjunto de regras de planos de discagem (*dialplan*) enviado pelo Agente de Chamada para instruir o Gateway a coletar os dígitos inseridos pelo Terminal de forma correta. O mapa de dígitos é muito útil, pois evita o envio de mensagens de sinalização a cada digito teclado pelo usuário, visto que é preferível acumular os números digitados e depois enviá-los de uma só vez, de acordo com as regras pré-estabelecidas. Deve haver testes específicos em relação a parâmetro, devido a sua importância e complexidade, já que possui uma série de

	regras de formação e interpretação por parte dos Gateways.
Quarantine Handling (Q)	Este parâmetro especifica o tratamento das mensagens seguindo a política de filas FIFO.
Detect Events (T)	DetectEvents é um parâmetro opcional que especifica uma lista de eventos que o Gateway é requisitado a detectar durante o período de quarentena.

Tabela 14: Parâmetros das mensagens do protocolo MGCP

A partir do conhecimento mais detalhado dos parâmetros, torna-se útil observar como o CODEC de uma chamada é selecionado. A negociação de CODECs entre dois endpoints é realizada por intermédio do Agente de Chamada, e baseia-se na interseção das informações internas e das informações fornecidas pelo dispositivo, sendo este último contido nos parâmetros LocalConnectionOptions/RemoteConnectionDescriptor, dependendo do referencial da conexão. Em caso de ausência destes parâmetros nas mensagens de sinalização, apenas a lista interna de CODECs do dispositivo é considerada. A lista de CODECs é ordenada de acordo com a preferência de cada dispositivo e em caso de falha durante a negociação, um erro do tipo *534 Codec Negotiation Failure* pode ser observado.

O MGCP é um protocolo desenhado de forma modular e extensível, para isso a norma introduz o conceito de pacotes, com o objetivo de agrupar um conjunto de sinais e eventos telefônicos equivalentes. São exemplos de pacotes, segundo RFC 2705, atual RFC 3435, DTMF *package*, Trunk *package*, Line *package*, etc. Este último, por exemplo, agrupa sinais e eventos específicos relativos à linha telefônica analógica tradicional, da mesma forma que o Trunk *package* se refere aos eventos e sinais relativos aos testes de circuitos, notificação de falhas, etc. O conceito de sinais e eventos também ocupa papel central no protocolo MGCP. O Softswitch pode solicitar que seja notificado quando há a ocorrência de certos eventos no Endpoint, (fora do gancho, por exemplo) incluindo o nome do evento no parâmetro RequestedEvents. Por outro lado, o Softswitch também pode solicitar que certos sinais sejam enviados ao Endpoint (tom de discagem, por exemplo), os incluindo no parâmetro SignalRequests.

Um pacote, portanto, é uma coleção de eventos e sinais suportados por um determinado tipo de Gateway ou Endpoint em particular, que por sua vez, podem suportar mais de um pacote. Alguns testes foram propostos devido às diversas regras de formação de pacotes, sinais e eventos. Um exemplo básico desta sintaxe é L/hu, onde "L" representa o Line *package*, que possui o evento "hu" (*hang-up*/fone no gancho), entre outros. As *strings* separadas pela "/" independem de serem maiúsculas ou minúsculas, a norma ainda prevê a utilização de caracteres curingas como "*" e "all" para fazer referencia a mais de um pacote ou evento, respectivamente. Os sinais, por outro lado, são divididos em três tipos básicos, On/Off (OO), uma vez aplicados, estes sinais são extinguidos quando desligado; Time-Out(TO), que permanecem ate um determinado período de tempo; e Brief (BR), referente aos sinais de curta duração. As regras de formação dos sinais são as mesmas observadas nos eventos, isto é, a string é formada pela sigla do pacote separada por uma barra do código do sinal. Exemplo: L/rg, significa toque telefônico (*ringing*) precedido do pacote *Line* [31].

3.3.4 Respostas aos Comandos MGCP

Para todo e qualquer comando MGCP, é retornada uma resposta, seguindo a mesma idéia do protocolo SIP, onde as respostas são divididas em categorias e códigos de retorno, como segue:

0xx (000 to 099) Indica um *acknowledgement* para uma resposta.
1xx (100 to 199) Resposta temporária e em seguida, será encaminhada uma resposta final.
2xx (200 to 299) Indica que o comando foi executado com sucesso.
4xx (400 to 499) Falha devido a um erro transitório.
5xx (500 to 599) Falha devido a um erro permanente.
8xx (800 to 899) Códigos específicos de resposta referente a pacotes de eventos.

As mensagens de resposta apresentam a mesma estrutura de comando de linha apresentada anteriormente, isto é, o *Response Header* ou cabeçalho da resposta compõe o primeiro trecho da mensagem, e o *Message Body* é formado pelo SDP, como segue:

ReturnCode **SP** TransactionID **SP** Commentary **CRLF**

Parameter Line(s)

.

.

<linha em branco>

[SDP]

Os testes relacionados às mensagens de resposta foram desenhados primeiramente obedecendo à estrutura de resposta do protocolo, onde o campo *Commentary* é opcional, significando a razão da resposta e tem formato textual. O campo *ReturnCode* é representado por um valor inteiro. A lista completa dos códigos de respostas já definidos no protocolo pode ser encontrada na seção 2.4 da RFC 3435 e, obviamente, não foram todas contempladas no Roteiro de Testes.

Logicamente, uma resposta tem que estar correlacionada com o comando que a dispara. Assim, o campo *TransactionID* é o mesmo na(s) resposta(s) e no comando que gerou a(s) resposta(s). Outra característica do protocolo é que os mesmos parâmetros resumidos na Tabela 13 estão todos habilitados também para uso nas respostas, entretanto a utilização nos dois casos difere, como pode ser visualizado na Tabela 15, que correlaciona os parâmetros em cada mensagem de resposta aos comandos que geram as respostas. A Tabela 15 demonstra que as respostas geralmente possuem menos parâmetros que os comandos. As Tabelas 13 e 15 são extremamente úteis na análise prática dos testes e por isso também foram incluídas neste capítulo.

Parameter name	EP CF	CR CX	MD CX	DL CX	RQ NT	NT FY	AU EP	AU CX	RS IP
BearerInformation	F	F	F	F	F	F	O	F	F
CallId	F	F	F	F	F	F	F	O	F
Capabilities	F	F	F	F	F	F	O	F	F
ConnectionId	F	O	F	F	F	F	O	F	F
ConnectionMode	F	F	F	F	F	F	F	O	F
Connection-Parameters	F	F	F	O	F	F	F	O	F
DetectEvents	F	F	F	F	F	F	O	F	F
DigitMap	F	F	F	F	F	F	O	F	F
EventStates	F	F	F	F	F	F	O	F	F
LocalConnection-Options	F	F	F	F	F	F	F	O	F

MaxMGCPDatagram	F	F	F	F	F	F	O	F	F
NotifiedEntity	F	F	F	F	F	F	O	O	O
ObservedEvents	F	F	F	F	F	F	O	F	F
QuarantineHandling	F	F	F	F	F	F	O	F	F
PackageList	O*	O*	O*	O*	O*	O*	O	O*	O*
ReasonCode	F	F	F	F	F	F	O	F	F
RequestIdentifier	F	F	F	F	F	F	O	F	F
ResponseAck	O*	O*	O*	O*	O*	O*	O*	O*	O*
RestartDelay	F	F	F	F	F	F	O	F	F
RestartMethod	F	F	F	F	F	F	O	F	F
RequestedEvents	F	F	F	F	F	F	O	F	F
RequestedInfo	F	F	F	F	F	F	F	F	F
SecondConnectionId	F	O	F	F	F	F	F	F	F
SecondTerminalId	F	O	F	F	F	F	F	F	F
SignalRequests	F	F	F	F	F	F	O	F	F
SpecificTerminalId	F	O	F	F	F	F	O	F	F
LocalConnection-Descriptor	F	O*	O	F	F	F	F	O*	F
RemoteConnection-Descriptor	F	F	F	F	F	F	F	O	F

Tabela 15: Relacionamento entre parâmetros nas mensagens de resposta de acordo com cada comando MGCP

O protocolo MGCP também implementa respostas provisórias, pois são importantes ferramentas para manter o estado de um diálogo, principalmente quando há grande espaço de tempo entre uma mensagem e outra de sinalização, evitando, dessa forma, retransmissões por *timeout*. Quando uma destas respostas é disparada, principalmente em relação aos comandos CreateConnection e ModifyConnection, é recomendado que a descrição de sessão e a identificação da conexão estejam contidos na mensagem. Uma vez que a transação seja completada corretamente, será gerada uma resposta final e deve repetir as informações contidas na resposta provisória, caso contrário, pode-se considerar um erro do protocolo.

Assim como no SIP, os dispositivos devem ter o compromisso com mais algumas regras referentes às respostas de caráter provisório. Em relação ao comando CreateConection, por exemplo, após uma resposta provisória ser disparada, uma resposta final é enviada pelo Gateway e deve conter o parâmetro ResponseAck, de acordo com o novo padrão RFC 3435.

3.4 Protocolo SDP

O protocolo MGCP, assim como o SIP e o SGCP, utiliza SDP para realizar a alocação e a descrição dos recursos que serão utilizados pelos Gateways durante uma chamada [28]. A função primária do MGCP é habilitar o estabelecimento de conexões e garantir a troca da descrição da sessão de cada ponta da comunicação. Portanto, assim como no SIP, o SDP será responsável pelo armazenamento de endereços IP e portas de comunicação, e por realizar a descrição da mídia dos pacotes UDP/RTP. Essa característica é particularmente útil quando na integração do MGCP e SIP, isto é, para o cenário em que há mais de um Agente de Chamada comunicando-se em SIP ou SIP-T e os Gateways utilizando o protocolo MGCP. Observa-se que a comunicação entre Gateways controlados por Agentes de Chamadas diferentes ocorre de forma quase que transparente desde que utilizam SDP para descrever a sessão. Essas questões serão abordadas no próximo tópico relativo a interconexão de chamadas.

O tópico sobre SDP deve mesmo ser mais resumido neste capítulo, pois o grupo de testes desenvolvido para este protocolo engloba todos aqueles desenvolvidos e citados no capítulo de SIP (item 2.5), assim como a definição e a teoria do protocolo SDP. Obviamente as individualidades de cada protocolo devem ser tratadas, como no caso de um Terminal MGCP receber uma oferta SDP na qual não pode provisionar por qualquer que seja a razão, como um CODEC incorreto, porta protegida, etc. Neste caso, o Terminal deve responder com uma mensagem onde o campo “Media Announcements” deve conter o valor “0” no subcampo <port> do protocolo SDP.

De acordo com o modelo desenvolvido já no capítulo anterior, o Roteiro de Testes do protocolo MGCP também prevê um grupo de testes dedicado a análise mais detalhada de algumas características do protocolo, permitindo a abordagem de itens da recomendação que não se aplicam a nenhum outro grupo de testes anterior. A seguir, chamaremos a atenção de outros detalhes do protocolo que também foram mapeadas em testes de conformidade.

No item anterior foi verificada a sintaxe do comando de linha do protocolo MGCP, onde o verbo que representa o comando é codificado em quatro letras, independentemente se maiúsculas ou minúsculas e na seqüência a ID da transação é representado como dígitos decimais de até nove posições. Entretanto, a recomendação aborda os casos em que novos verbos ou comandos podem ser definidos no protocolo, importante para experimentos e implementação de novas aplicações por parte dos fabricantes. A norma obriga que novos verbos sejam identificados também por quatro letras, porém com a primeira letra sendo "X".

Além dos casos de implementação de novos comandos, a norma ainda permite que novos parâmetros sejam especificados no protocolo e a regra geral é que devem ser iniciados com os caracteres "X-" ou "X+". Os parâmetros iniciados por "X-" se referem àqueles não críticos, ou seja, o dispositivo MGCP simplesmente ignora o parâmetro caso este não seja reconhecido. Já os iniciados por "X+" formam os parâmetros críticos e caso algum elemento não o reconheça, um erro do tipo *511 Unrecognized Extension* tem que ser observado.

Os testes não devem parar por ai, pois soluções proprietárias também podem abranger os parâmetros da conexão, além daqueles valores padrão (*delay*, *jitter*, pacotes enviados e perdidos, etc) já estabelecidos pelo protocolo. A norma sugere o uso de duas letras para identificar/codificar o nome de cada parâmetro, sendo seus valores sempre decimais e precedidos pelo sinal de igual "=". A regra é que esses nomes devem ser iniciados pelo caractere "X-" seguido por duas ou mais letras representativas do nome do parâmetro. Caso o nome ou o valor do parâmetro de conexão enviado não seja reconhecido, este deve ser simplesmente ignorado pelo dispositivo.

A norma ainda aborda requisitos para reserva de recursos, que podem também ser verificados na pratica. Os Gateways podem ser instruídos a alocarem recursos, por exemplo, utilizando o protocolo RSVP (Resource ReSerVation Protocol) numa dada conexão. Para viabilizar este tipo de conexão, o Agente de Chamada faz a especificação do perfil da reserva a ser realizada, que pode ser de duas formas: a *controlled load* ou *guaranteed service*, definidas pelo RSVP. Apesar de o roteiro de testes elaborado não abordar questões de QoS, deve ser mencionado que este teste tem o objetivo apenas de

verificar a funcionalidade da reserva de recursos do protocolo MGCP e não o de analisar como a reserva de recursos é estabelecida.

Os novos itens contemplados na atual recomendação do protocolo e os itens obsoletos da antiga norma também podem ser avaliados, de forma a garantir que a plataforma em teste esteja em conformidade com estas atualizações. Algumas das principais diferenças foram abordadas ao longo do texto e são resumidas a seguir:

- Inclusão de IPv6 para nomes dos endpoints;
- O parâmetro BearerInformation passa a ser opcional e condicional quando utilizado pelo comando EndpointConfiguration.
- O valor *default* do parâmetro *Type of Service* passa a ser zero.
- Incorporado novos valores de códigos de retorno: 101, 405, 406, 407, 409, 410, 503, 504, 505, 506, 507, 508, 509, 533, 534, 535, 536, 537, 538, 539, 540, 541.
- Definição do novo range de valores de códigos de retorno 800-899.
- Adicionados os códigos de retorno 903, 904, 905.

3.5 Metodologia de Testes e Resultados

O Capítulo 4 apresentou uma descrição do protocolo MGCP, ao mesmo tempo em que procurou descrever os procedimentos para criação dos testes de conformidade, cuja elaboração é contribuição original do projeto desenvolvido pelo autor desta Dissertação. O objetivo deste capítulo foi relatar o desenvolvimento de um conjunto de testes que, baseados em normas internacionais, serão capazes de verificar a conformidade dos principais protocolos utilizados em soluções de voz sobre IP.

A partir do desenvolvimento do caderno de teste para SIP, o Roteiro de Testes MGCP procurou seguir a mesma metodologia, isto é, o estudo da norma do protocolo foi orientado à proposta do trabalho e aos modelos da Embratel. As regras de implementação do protocolo, segundo RFC 3435 e suas referências, foram seguidas e em sua maioria incorporadas à listagem de testes, de forma a garantir uma avaliação adequada de

plataformas genéricas de Redes de Nova Geração, que implementam o serviço de Voz sobre IP baseadas no protocolo MGCP, em relação às recomendações e normas internacionais pertinentes.

Lembrando que uma avaliação adequada, neste caso, significa desenvolver uma série de testes criteriosos a partir de algumas premissas: todos os testes devem ser de natureza prática e implementável, devem ser agrupados de forma lógica e seqüencial, de forma que facilite e reduza o tempo de configuração e montagem do *setup* de testes, e a execução destes deve utilizar uma arquitetura padronizada, a menos que uma nova configuração seja especificada para um teste em particular, e deve sugerir a utilização de recursos e instrumentais disponíveis.

Assim como na recomendação do protocolo SIP, o padrão MGCP também é muito abrangente, porém apenas o Tópico 5 não foi objeto de estudo, pois trata das questões de segurança do protocolo. Esta foi uma decisão tomada levando-se em consideração fatores como objetivos do trabalho, relacionamento entre os tópicos e a relação custo (tempo) versus beneficio. Para este estudo, os tópicos relacionados a segurança, chamada em conferência e qualidade de serviço também não serão considerados, apesar de serem igualmente importantes para os itens que foram abordados.

É importante novamente dizer que os testes do protocolo MGCP propostos também não foram baseados em eventos comuns de telefonia, como chamada em espera, transferência de chamada, chamada a cobrar, entre vários outros, mas todo o conjunto de testes estará moldado pelas normas do protocolo e, portanto, referem-se ao correto tratamento e formatação de suas mensagens e da própria funcionalidade do protocolo como um todo.

A Figura 17 representa uma Rede de Nova Geração real sob o ponto de vista de serviços telefônicos e, na realidade, sua representação vai além das nossas necessidades para validação dos testes de conformidade em laboratório. Entretanto, a proposta é demonstrar como os subsistemas telefônicos, VoIP e PSTN, se interligam, destacando os protocolos e Gateways envolvidos em todo o sistema.

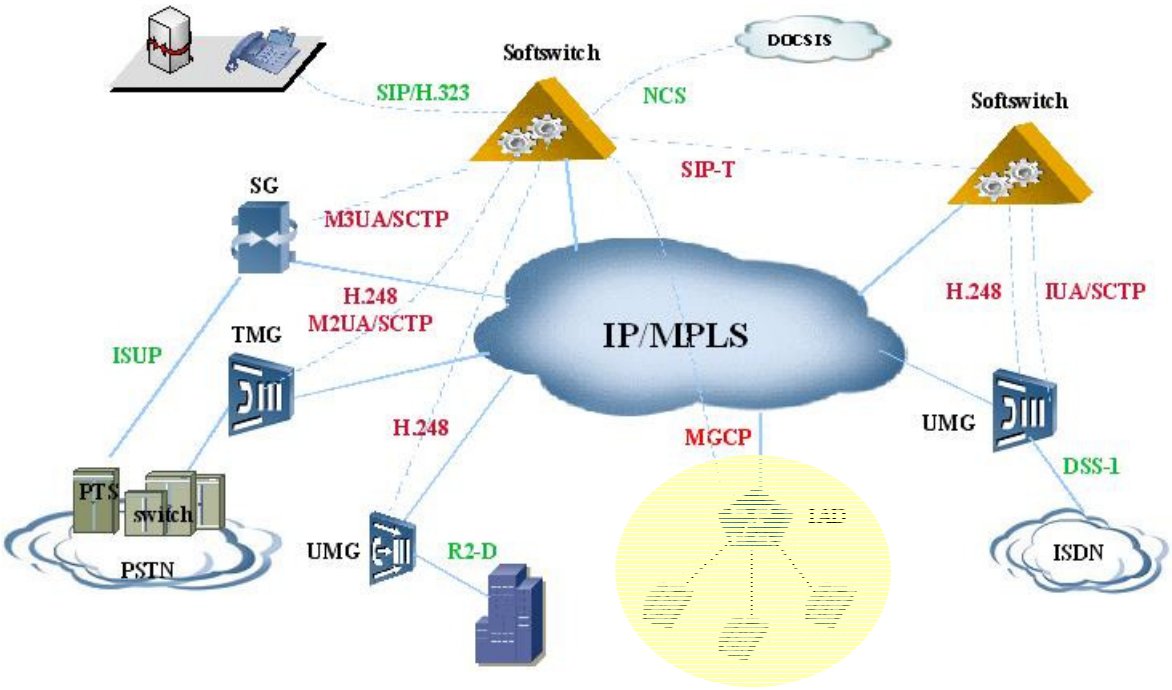


Figura 17: Arquitetura de Testes - Parte III

O núcleo da rede IP/MPLS na figura é composto por dois Softswitch (MGC) interligados pelo protocolo SIP-T[1]. A área em amarelo logo abaixo da figura, representada pela ligação do Softswitch com o IAD através do protocolo MGCP, que será a utilizada para validação do Roteiro de Testes, visto que é o único trecho da arquitetura que implementa o protocolo MGCP efetivamente. A Figura 17 ainda destaca o subsistema SIP ou H.323, tema dos capítulos anteriores, no interior da NGN.

---

[1]**SIP-T (SIP for Telephones)**

SIP for Telephones (RFC 3372) é um mecanismo que permite a integração de uma rede de telefonia IP baseada em SIP com a rede SS7 baseada em ISUP. A recomendação não especifica um novo protocolo, apenas especifica o mapeamento SIP/ISUP. A premissa é que o *payload* da mensagem ISUP seja transportado no corpo da mensagem SIP, ou seja, o protocolo SDP passa a especificar também as características da mensagem ISUP.

A Figura 17 também tem a intenção de representar a interface da NGN com redes telefônicas privadas ou redes corporativas. A interface é realizada através do UMG (Universal Media Gateway) tanto para a sinalização R2-D quanto para ISDN, o UMG também atua como Gateway de Mídia. A diferença é que o UMG da interface ISDN possui mais uma conexão com o Softswitch através do protocolo IUA[2] pela própria necessidade da sinalização ISDN. O mais importante é notar que o protocolo responsável pela sinalização entre o Gateway e o Softswitch neste trecho é o MEGACO/H.248, que foi definido com mais detalhes no Anexo B devido a sua grande importância.

Os Softswitch têm interface com a rede SS7 através do Gateway de Sinalização (SG), que atua como tradutor da sinalização ISUP para o protocolo M3UA[3] da rede IP. Vale abrir um parêntesis para dizer que o IUA e M3UA são protocolos pertencentes a um padrão chamado SIGTRAN (SIGnalling TRANsport) desenvolvido pelo IETF.

Em paralelo tem havido uma movimentação significativa de diversos grupos de estudo, em âmbito mundial, no sentido de integração das redes de circuitos comutados com as redes IP. Há dois outros grupos conhecidos como PINT (PSTN and Internet Interworking) para os serviços originados na rede IP e SPIRITS (Service in the PSTN/IN Requesting Internet Service) para os serviços originados na rede de circuitos comutados, que endereçam a questão de interfuncionamento de serviços telefônicos entre estas redes, além do próprio SIGTRAN. A plataforma NGN-Huawei disponível para os testes utiliza o padrão SIGTRAN, que define um conjunto de padrões projetado para fornecer um modelo de arquitetura para o transporte de sinalização da RTPC sobre redes IP.

---

[2] **IUA (*ISDN-User Adapter Layer*)**
Protocolo da família SIGTRAN responsável por transportar na rede IP as informações Q.921 da camada 2 ou camada de enlace da pilha de protocolos ISDN.

[3] **M3UA (*MTP3-User Adapter Layer*)**
Protocolo da família SIGTRAN responsável por fornecer serviços similares na rede IP das informações MTP3 da camada 3 da estrutura de protocolos da SS7.

O objetivo principal dos trabalhos conduzidos pelo Grupo de Trabalho SIGTRAN é permitir o transporte da sinalização DSS-1 e o Sistema de Sinalização Nº7 sobre a infra-estrutura IP. A interface de voz propriamente dita da RTPC com a NGN é realizada pelo Gateway de Voz ou de Mídia (MG), também conhecido como TMG (Trunking Media Gateway).

Finalmente, a Figura 17 também ilustra a interface com a rede HFC (Híbrida Cabo-Fibra) de TV a cabo com o Sofswitch, diretamente através do protocolo NCS[4], muito semelhante ao MGCP, porém adaptado para trabalhar sobre o protocolo DOCSIS[5] e com os próprios elementos da rede HFC, como MTAs (Multimedia Terminal Adapter), CMTS (Cable Modem Termination System), etc.

O instrumental de testes Spectra2 foi utilizado em substituição ao Softswitch desta vez, com a responsabilidade de controlar o IAD e, conseqüentemente, os Terminais a ele conectados. Portanto, o Spectra2 assumiu todas as funções de um Controlador de Gateway (MGC) na NGN, inclusive atuando na edição de testes, configuração dos parâmetros do protocolo quando necessário e também na geração e análise de tráfego. O Mídia Gateway utilizado foi o IAD208 da Huawei de 8 portas RJ11 e os Terminais utilizados foram telefones comuns (analógicos). O monitoramento do tráfego na rede foi feito através do *software* Ethereal, alocado dinamicamente em pontos estratégicos da rede para avaliação da sinalização de interesse.

---

[4] **NCS (*Network-based Call signalling*)**

Outro protocolo originado nos moldes MGCP, responsável pela configuração, gerenciamento e encerramento de sessões multimídias adaptado para redes HFC e desenvolvido pelo CableLabs como um padrão PacketCable. Obviamente, que o protocolo contem algumas modificações e adaptações para tratamento dos elementos das redes de TV a cabo, apesar da estrutura básica e o formato do protocolo MGCP serem os mesmos.

[5] **DOCSIS (*Data Over Cable Service Interface Specifications*)**

CableLabs® Certified™ Cable Modem desenvolve o projeto conhecido como DOCSIS, um padrão internacional que define requerimentos da camada 1 e camada 2 para operação e comunicação para sistemas de dados multimídia de alta capacidade sobre a infra-estrutura de redes de TV a cabo. A sua terceira versão data 2006.

Os testes foram agrupados em relação aos comandos do protocolo e questões mais genéricas foram agrupadas em testes básicos e avançados, muito semelhante a estrutura desenvolvida para o protocolo SIP. A primeira parte compreende os testes preliminares, principalmente em relação a sintaxe do protocolo, tratamento de alguns cabeçalhos, endereçamento, testes de portas, caracteres curinga, etc.

Os nove capítulos subseqüentes são relativos aos testes de cada comando MGCP, cuja descrição de como e porque foram desenvolvidos estão detalhados no tópico *4.3.1 Comandos MGCP*. Pode-se destacar a análise da inclusão e a equivalência dos parâmetros obrigatórios em cada comando, observação da possibilidade de inserção dos parâmetros na forma abreviada, condições de erro, condições de equivalência dos parâmetros entre comandos dependentes, mensagens de respostas permanentes e provisórias, análise de parâmetros pertinentes a cada comando, negociação de CODECs, *piggybacking* ou encapsulamento de comandos, regras de formação de pacotes, sinais e eventos, entre outras.

Outros três capítulos completam o Roteiro e são referentes ao protocolo SDP, aos testes considerados avançados, no qual são considerados comandos e parâmetros experimentais, reserva de recursos, filas de processos, *timeouts* de mensagens, capacidades dos Terminais, pacotes de eventos, entre outros, finalizando com o grupo de testes relativo as modificações da antiga RFC 2705.

As questões de mobilidade e redirecionamento de chamadas são tratados no MGCP de forma semelhante ao protocolo SIP, entretanto, o processo também não pode ser verificado na prática apesar de constar no Roteiro de Testes proposto, visto que a transferência de usuários não é feita de forma automática no laboratório como recomenda o protocolo, mas configurada manualmente a cada transferência de assinante.

Questões de interoperabilidade sempre foram de especial interesse neste estudo, já que cada protocolo atua sempre em um contexto maior, principalmente em relação a redes telefônicas que já existem a mais de um século. Entretanto, não foi possível uma análise mais aprofundada da relação dos protocolos VoIP abordados, com a sinalização telefônica legada, referida no Capítulo 2. Estamos chegando ao final da Dissertação e pudemos

comprovar que a interconexão é realizada por protocolos da família SIGTRAN ou pelo protocolo MEGACO/H.248, de acordo com as plataformas utilizadas pela Embratel. Neste sentido, fica aqui uma sugestão para trabalhos futuros, pela necessidade de desenvolver um caderno de práticas com mapeamento de funções entre os protocolos das duas redes, baseadas em diversas normas que já tratam da questão de interoperabilidade entre redes telefônicas. Existem vários grupos de estudos desenvolvendo método e protocolos capazes de garantir uma infra-estrutura comum de telefonia, a partir do momento que a convergência total das redes telefônicas para as redes IP não acontecerá do dia para a noite.

A especificação de testes desenvolvida a partir deste capítulo, estabelece procedimentos de ensaios e requisitos necessários para a validação de elementos MGCP, em função das recomendações internacionais do protocolo e destina-se ao uso do corpo técnico da Embratel. O Roteiro de Teste proposto foi executado em laboratório, cumprindo o desejo de desenvolver um modelo de testes de conformidade através do qual o operador é capaz de implementá-lo para que possa ter informações de análise suficientes para avaliar determinado equipamento ou solução MGCP.

Entretanto, o trabalho desenvolvido cumpre outras metas na medida em que se alinha com os critérios de qualidade do Centro de Referência Tecnológica da Embratel, já que é credenciado na norma internacional ABNT NBR ISO/IEC 17025 com requisitos específicos de comprovação de competência técnica para laboratórios de ensaios. Os Roteiros de Testes entregues a Embratel são importantes pontos de partida para a aprovação de procedimentos internos de testes da tecnologia VoIP, em relação aos protocolos SIP e MGCP. Estes procedimentos são documentos oficiais pertencentes ao Sistema de Gestão do laboratório, chamados de Especificação de Teste (EPT), cujo objetivo é descrever métodos específicos para realização de ensaios padronizados, normalmente elaborados segundo normas técnicas (ex: Normas Anatel, ITU-T), práticas Telebrás e da própria Embratel.

Os resultados finais dos experimentos deste capítulo, assim como do capítulo anterior, foram analisados e aprovados pelos responsáveis técnicos, o controle da qualidade dos documentos foi garantido através da análise comparativa dos resultados obtidos com os de

ensaios anteriores na mesma área de conhecimento e repetição do ensaio ou parte dele a partir de uma amostragem aleatória.

A metodologia para o desenvolvimento de testes de conformidade descrita nesta Dissertação proporcionou a criação de dois Roteiros de Testes práticos dos protocolos atualmente em voga na tecnologia VoIP e alcançam alguns objetivos importantes, que podem ser resumidos da seguinte forma:

1. O laboratório desenvolve o seu primeiro instrumento padronizado de avaliação de protocolos de sinalização telefônica no mundo IP, capaz de prover um nível elevado de confiança de que o dispositivo testado funcionará bem na maioria das soluções com os diferentes fornecedores de equipamentos.
2. Cada Roteiro de Teste se constitui em ferramenta capaz de fornecer um meio para o isolamento de um determinado problema em uma dada implementação. Estas informações podem ser posteriormente assinaladas para que o fabricante possa efetuar as correções necessárias.
3. O laboratório caminha na direção da padronização de processos e protocolos também na tecnologia VoIP, de acordo com os padrões de qualidade do laboratório e a certificação ISO.
4. O CRT é capaz de assegurar o desenvolvimento de competência interna e do capital intelectual da Empresa.
5. Os Roteiros de Testes desenvolvidos são de interesse geral na medida em que se constitui como um padrão de análise para determinada tecnologia.

A última etapa foi a de pesquisa de trabalhos relacionados. Existem alguns cadernos de testes, sendo em sua totalidade vendidos como produtos para avaliação de desempenho das redes, abordam testes de conformidade, de robustez do sistema, de QoS da rede VoIP, segurança, e de capacidades de servidores e gateways. Este trabalho adotou o roteiro de testes do CableLabs[7] como referência para comparação, que apesar de pago pode ser observado a partir dos seus *scripts* embarcados no Spectra2. Os testes propostos pelo PacketCable[8] foram observados um a um no próprio equipamento de teste e comparado com o modelo proposto. Este Roteiro foi o escolhido por duas razões principais: a primeira porque é o único que se constitui num padrão de fato, já que os outros são meros pacotes comerciais, o segundo motivo é que foi o único a que se teve acesso, mesmo que indiretamente.

O PacketCable publica seu Roteiro de Testes da seguinte forma: PKT-TP-TGCP-MG-CTP1.0-I02-050112, o que se consegue traduzir é PacketCable – Test Purpose – Trunking Gateway Control Protocol – Media Gateway – Cmpliance Test Plan, ou seja, são conjuntos de testes de conformidade destinados ao Media Gateway. O padrão desenvolvido pelo PacketCable é completado com testes para MGC: PKT-TP-TGCP-MGC-CF-CTP1.0-I01-041216. Todos os documentos foram avaliados através de seus *scripts* a partir do instrumental de testes.

---

[7] Cable Labs (www.cablelabs.com)

Fundado em 1988 por membros da indústria de televisão a cabo, o Cable Television Laboratories, Inc. (CableLabs®) é um consorcio de pesquisa e desenvolvimento sem fins lucrativos.

[8] Packet Cable

PacketCable é um dos vários projetos do CableLabs que tem o objetivo de desenvolver especificações de interfaces interoperáveis para fornecer serviços multimídia em tempo real avançado sobre a infra-estrutura de cabo no protocolo IP. Exemplo: Telefonia IP, conferência multimídia, jogos interativos, etc.

A partir de uma análise preliminar do caderno do PacketCable, não se pode afirmar quais foram as referências utilizadas para tal desenvolvimento; entretanto, houve grande equivalência de testes entre os dois Roteiros. O PacketCable desenvolveu dois cadernos de testes, um para MG e outro para MGC, incluindo algumas tímidas sessões de testes de interconexão com redes de cabo e PSTN.

O Roteiro do PacketCable mostrou-se bastante simples e menos abrangentes, pois não há propostas de testes para vários comandos e eventos do protocolo. Apesar do maior número de testes do Roteiro proposto pelo PacketCable, já descontando os testes referentes a interoperabilidade com outras redes, os testes são muito genéricos e superficiais, não sendo definitivamente, instrumento de avaliação e análise contundente de qualquer equipamento MGCP. A Tabela 16 faz um resumo das principais diferenças entre as duas práticas.

	PKT-TP-TGCP-MG PKT-TP-TGCP-MGC	**ROTEIRO DE TESTES PROPOSTO**
Principais Referências	Não determinado	RFC 3435
Número de Testes	115 Obs.: 27 testes de interoperabilidade.	69
Comandos MGCP	RQNT DLCX CRCX MDCX AUEP AUCX RSIP	RQNT DLCX CRCX MDCX AUEP AUCX RSIP NTFY EPCF
Estrutura do Documento	O documento é dividido em grupos genéricos de testes, como: aditamento, convenções de nomes, controle de conexão, falhas, etc.	Cabeçalhos Comandos Protocolo SDP Testes Avançados em MGCP
Estrutura dos Testes	Não determinado	Testes ID Objetivo Referências Versão Procedimentos Resultados Esperados Observações
Implementação	Automática (*Scripts* + Spectra2)	Manual

Tabela 16: Comparação entre Roteiros de Testes

4. Conclusão

Durante toda a Dissertação pouco se falou sobre os aspectos mais gerais da tecnologia VoIP; mesmo não sendo o objetivo do trabalho, vale ressaltar que o estudo aplicado dos principais protocolos da telefonia IP se refere à parte mais técnica de uma tecnologia realmente revolucionária nos negócios das operadoras, corporações e cliente final. Este último percebe seus benefícios com a redução das tarifas telefônicas e maior oferta de serviços, enquanto que as corporações se beneficiam com a redução dos custos de aquisição e manutenção de equipamentos, redução dos custos diretos com telefonia e aumento de produtividade devido, principalmente, a mobilidade permitida pela telefonia IP. As operadoras de telecomunicações, por sua vez, observam a redução dos custos de operação e manutenção da rede, têm grande potencial e agilidade de oferta de novos serviços, maior facilidade de implementação de novos serviços que virão a compensar a atual perda de receitas e, por fim, o surgimento de diversos produtos de diferentes fornecedores.

Em contrapartida, a tecnologia de transmissão de voz sobre o protocolo IP tem seus próprios gargalos e desafios técnicos, como o alto grau de qualidade e confiabilidade dos serviços, necessidade de QoS e SLA nas redes IP, a diversidade de padrões e escolha de tecnologia, falta de pessoal especializado, aspectos regulatórios, impacto cultural nas empresas, custo principalmente de terminais, questões de segurança e necessidade de interoperabilidade com a rede telefônica atual. Cada uma destas questões poderia ser tema de diversos outros estudos.

Pode-se concluir em relação ao protocolo SIP que, por ser um padrão aberto, abrange um conjunto de extensões, vários modelos de arquitetura em função de aplicações, integração com outras tecnologias IP e um *framework* para desenvolvimento de novos serviços de comunicação. Entretanto, a partir de uma definição mais rigorosa do protocolo, é sabido que o SIP não provê serviços, mas primitivas que podem ser usadas para implementar diferentes serviços.

Ao longo do Capítulo 3 várias características do protocolo foram citadas, podendo-se acrescentar ainda o fato de o SIP ser usado em conjunto com outros protocolos para

proporcionar serviços multimídia completos para os usuários, tais como RTP para transporte de dados em tempo real, protocolos de QoS e o SDP, para descrição de sessões multimídia.

O passo inicial do Capítulo 3 foi descrever resumidamente o protocolo SIP, de forma a criar uma base de conhecimento. Um segundo passo foi identificar os pontos críticos do protocolo para a elaboração de uma estrutura de testes de conformidade com as normas aplicáveis, sendo estes pontos destacados ao longo de todo texto. A partir do modelo teórico, a terceira etapa foi caracterizada pela criação do caderno de testes, seguida pela sua avaliação prática; nesta fase se pode avaliar a metodologia e os critérios utilizados para confecção dos testes. Os resultados práticos foram conclusivos para validação do modelo teórico, logo esta experiência também foi aproveitada ao longo de todo texto.

Em relação ao Capítulo 4, conclui-se que o modelo de conexão e a estrutura de comando do MGCP são simples, flexíveis e de *design* poderoso, provendo vantagens tais como redução de *overhead* das mensagens, da complexidade e dos custos, quando comparado principalmente com o protocolo H.323. Enfim, o MGCP coleciona atributos chaves como simplicidade, eficiência, flexibilidade e baixo custo efetivo, eliminando a necessidade de terminais complexos para a Telefonia IP, o que o torna um protocolo padrão para uso em redes NGN. A tecnologia SIP não concorre diretamente com o MGCP, visto que é um protocolo ponto-a-ponto e que pode ser tratado como um subsistema VoIP dentro de uma Rede de Nova Geração.

A Figura 18 fornece um resumo dos protocolos de sinalização da telefonia IP a partir de tudo que foi estudado durante a elaboração da Dissertação. Em destaque, estão os protocolo das camadas de rede (IP) e de transporte (UDP/TCP) típicos da telefonia em redes IP. Os protocolos de sinalização são apresentados de acordo com suas aplicações, pode-se notar que H.323 e SIP são concorrentes e foram agrupados por atuarem em uma arquitetura distribuída e serem protocolos ponto-a-ponto. Os protocolos tratados como sendo de Controle de Gateway pela figura, MGCP e MEGACO, atuam em redes centralizadoras, ou seja, no paradigma mestre-escravo. A Figura 18 também apresenta a hierarquia de protocolos do trafego de voz propriamente dita, visto que seu tratamento é quase sempre confundido com os protocolos de sinalização citados anteriormente.

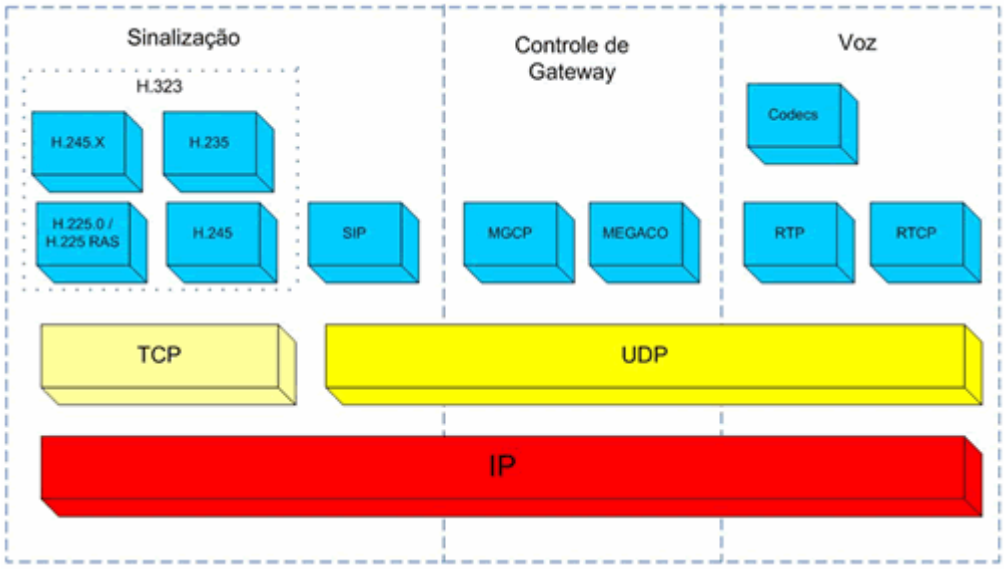


Figura 18: Estrutura dos protocolos VoIP na rede IP

A proposta do Capítulo 4 foi idêntica à do anterior, ou seja, a partir de uma simples descrição do protocolo MGCP, seus pontos críticos puderam ser bem conhecidos para a elaboração de uma estrutura de testes de conformidade com as normas aplicáveis, sendo estes pontos destacados ao longo de todo o texto. O caderno de testes também foi concretizado e submetido à prática, proporcionando uma avaliação da metodologia e dos critérios utilizados para confecção dos testes. Os resultados práticos foram conclusivos para validação do modelo teórico da mesma forma que no capítulo anterior, logo esta experiência também foi aproveitada ao longo de todo o texto.

Normalmente, todo novo equipamento é testado sob certas condições para serem avaliados e submetidos a campo. Geralmente, estes testes são disponibilizados pelo fabricante e, geralmente, o próprio operador sugere outros testes na medida em que adquire conhecimento sobre a tecnologia. A avaliação de sistemas telefônicos é quase sempre orientada a eventos e causas, principalmente em testes de protocolos da telefonia tradicional, devido ao alto grau de especificações e recomendações dos protocolos, que definem regras claras de funcionamento e seqüência do fluxo de sinalização para os diferentes serviços. Somente em casos de falhas de um determinado teste, uma análise mais apurada é realizada, como através do traçado da sinalização da chamada.

Por outro lado, as normas dos protocolos de sinalização telefônica do protocolo IP são muito mais abrangentes e menos detalhistas em relação às regras para estabelecimento de conexão ou serviços telefônicos.

A conclusão é que temos hoje dois mundos distintos em relação à avaliação de equipamentos telefônicos: a telefonia tradicional possui regras bem definidas e que devem ser seguidas em testes de conformidade, enquanto que a telefonia IP representa um universo menos rigoroso e mais flexível em relação às regras de sinalização de chamadas. A eficiência do tipo de avaliação realizada, hoje, dos protocolos de telefonia tradicionais é satisfatória, porém não pode ser sustentada pela realidade dos equipamentos IP, já que as recomendações de seus protocolos não têm o nível de detalhamento e amarrações como ocorre na RTPC.

Um Roteiro de Testes é uma ferramenta importante para a criação de procedimentos técnicos em uma Empresa. De maneira geral, tanto o Roteiro de Testes ETSI para SIP, quanto o Roteiro de Testes PacketCable para o protocolo MGCP são mecanismos mais eficientes quando utilizados para testes de aceitação ou conformidade de uma determinada solução ou equipamento, já que são utilizados de forma automática através de um instrumental de testes como o Spectra2. Por outro lado, os Roteiros de Testes dos dois protocolos cujo desenvolvimento foi descrito nesta Dissertação podem ser entendidos como complementares aos citados acima, visto que são excelentes ferramentas para conhecimento teórico e prático da tecnologia, apesar de menos detalhado no caso do protocolo SIP, e mais custosos em termos de tempo para sua execução.

Em contrapartida, essa característica é capaz de proporcionar a sedimentação do conhecimento sobre a tecnologia, o que é muito útil na realização de projetos e identificação de problemas em campo. Além disso, resulta na formação do capital intelectual da Organização, visto que o Centro de Referência Tecnológica atua como um verdadeiro laboratório de produtos e serviços de telecomunicações, estimulando o pensamento futuro, antecipando-se às realidades e assegurando mais qualidade e satisfação para os clientes.

Bibliografia

[1] Ferrari, Antonio Martins, *Telecomunicações Evolução e Revolução*, Érica, 1999.

[2] ALENCAR, Marcelo Sampaio de. *Telefonia Digital*. Ed. Érica, SP, 1998.

[3] Prática Telebrás, SDT 210-110-704, *Especificações de Sinalização Acústica para a Rede Nacional de Telefonia.* STB, 1996.

[4] Prática Telebrás, SDT 210-110-703, *Especificações de Sinalização de Linha para Rede Nacional de Telefonia VIA Terrestre.* STB, 1996.

[5] Prática Telebrás, SDT 210-110-702, *Especificações de Sinalização entre Registradores para a Rede Nacional de Telefonia VIA Terrestre.* STB, 1996.

[6] DAVIDON, Jonathan; PETERS, James, *Voice over IP Fundamentals*, Cisco Press, 2000.

[7] ITU-T, Recommendation I.210 (03/93), *Principles of Telecommunication Services SUPPORTED by an ISDN and the Means to Describe Them.*

[8] ITU-T, Recommendation I.120 (03/93), *Integrated Services Digital Networks (ISDNs).*

[9] ITU-T, Recommendation I.320 (11/93), *ISDN Protocol Reference Model*.

[10] ITU-T, Recommendation Q.931 (05/98), *ISDN User-Network Interface Layer 3 Specification for Basic Call Control.*

[11] Prática Telebrás, SDT 220-250-732, *Subsistema de Usuário RDSI – ISUP Sistema de Sinalização por Canal Comum Nº. 7*. STB, 1998

[12] ITU-T, Recommendation Q.762 (1997), *Signalling System No. 7 ISDN User Part general functions of messages and signals.*

[13] ITU-T, Recommendation Q.764 (1997), *Signalling System No. 7 ISDN User Part signalling procedures.*

[14] HERSENT, Oliver; GUIDE, David; PETIT, Jean-Pierre, *Telefonia IP: Comunicação Multimídia Baseada em Pacotes*, Makron Books, 2002.

[15] ITU-T, Recommendation H.323 (02/98), Packet-Based Multimedia Communications Systems.

[16] IETF, RFC 3550, *RTP: A Transport Protocol for Real-Time Applications*, 2003.

[17] ITU-T, Recommendation H.225 (05/06), *Call Signalling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems.*

[18] ITU-T, Recommendation H.245 (02/98), *Control Protocol for Multimedia Communication.*

[19] IETF, RFC 3261, *SIP: Session Initiation Protocol*, June 2002.

[20] COLLINS, Daniel, *Carrier Grade Voice Over IP*, Second Edition, McGraw-Hill Networking, 2003.

[21] IETF, RFC 2806, *URLs for Telephone Calls*, April 2000.

[22] IETF, RFC 2976, *The SIP INFO Method*, October 2000.

[23] IETF, RFC 3265, *Session Initiation Protocol (SIP) – Specific Event Notification*, June 2002.

[24] IETF, RFC 3311, *The Session Initiation Protocol (SIP) UPDATE Method*, September 2002.

[25] IETF, RFC 3515, The Session Initiation Protocol (SIP) Refer Method, April 2003.

[26] IETF, RFC 3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP), June 2002.

[27] IETF, RFC 2327, Session Description Protocol (SDP), April 1998.

[28] IETF, RFC 3435, *Media Gateway Control Protocol (MGCP) Version 1.0*, January 2003.

[29] IETF, RFC 2805, *Media Gateway Control Protocol Architecture and Requirements*, April 2000.

[30] IETF, RFC 1034, *Domain Names – Concepts and Facilities*, November 1987.

[31] IETF, RFC 3660, *Basic Media Gateway Control Protocol (MGCP) Packages*, December 2003.

Anexo A - Fluxos de Comunicação

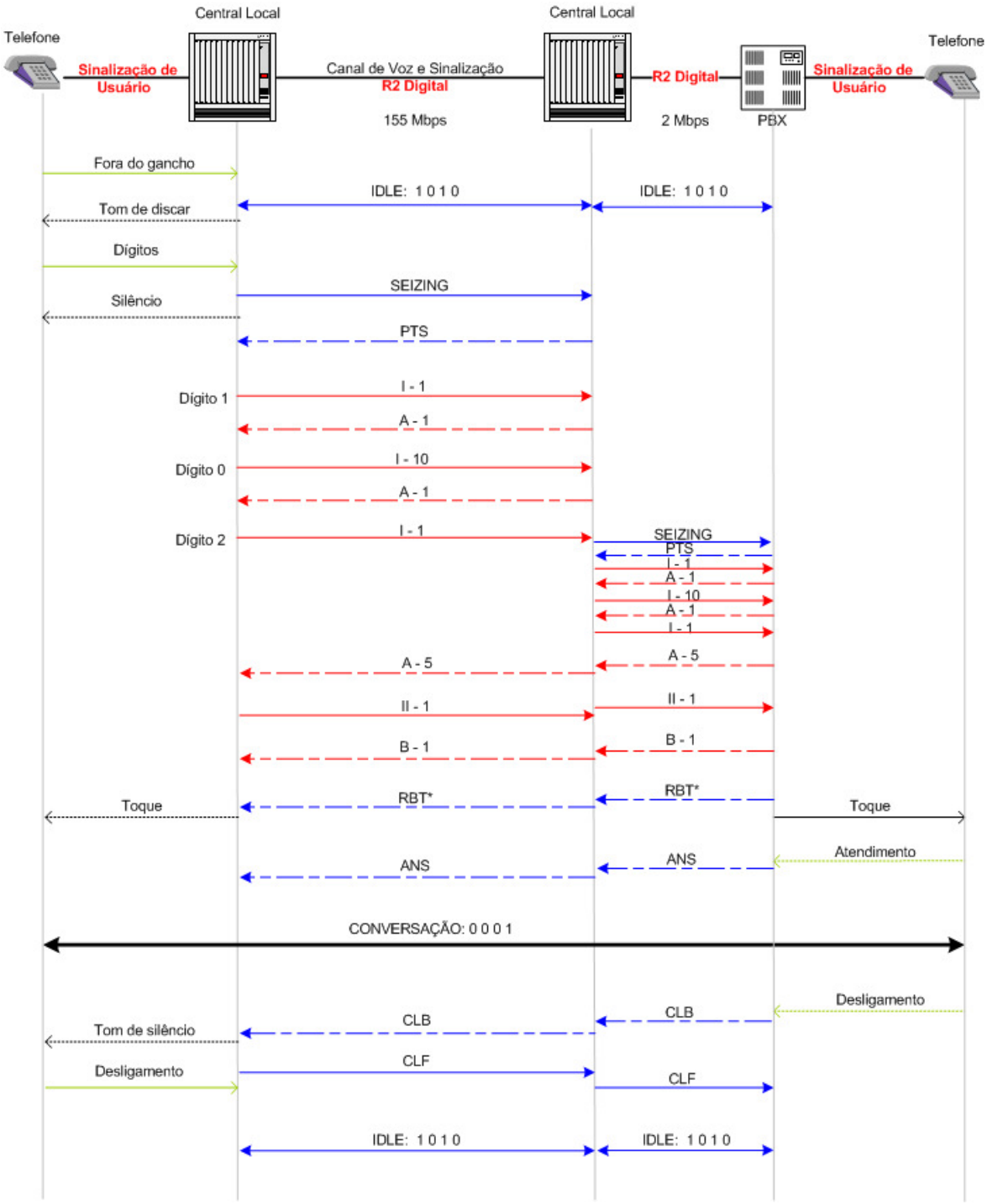


Figura A.1: Sinalização R2-Digital de uma chamada básica bem sucedida

* RBT = Ring Back Tone.

As demais siglas da Figura A.1 foram definidas na Tabela 1 do Capítulo 1.

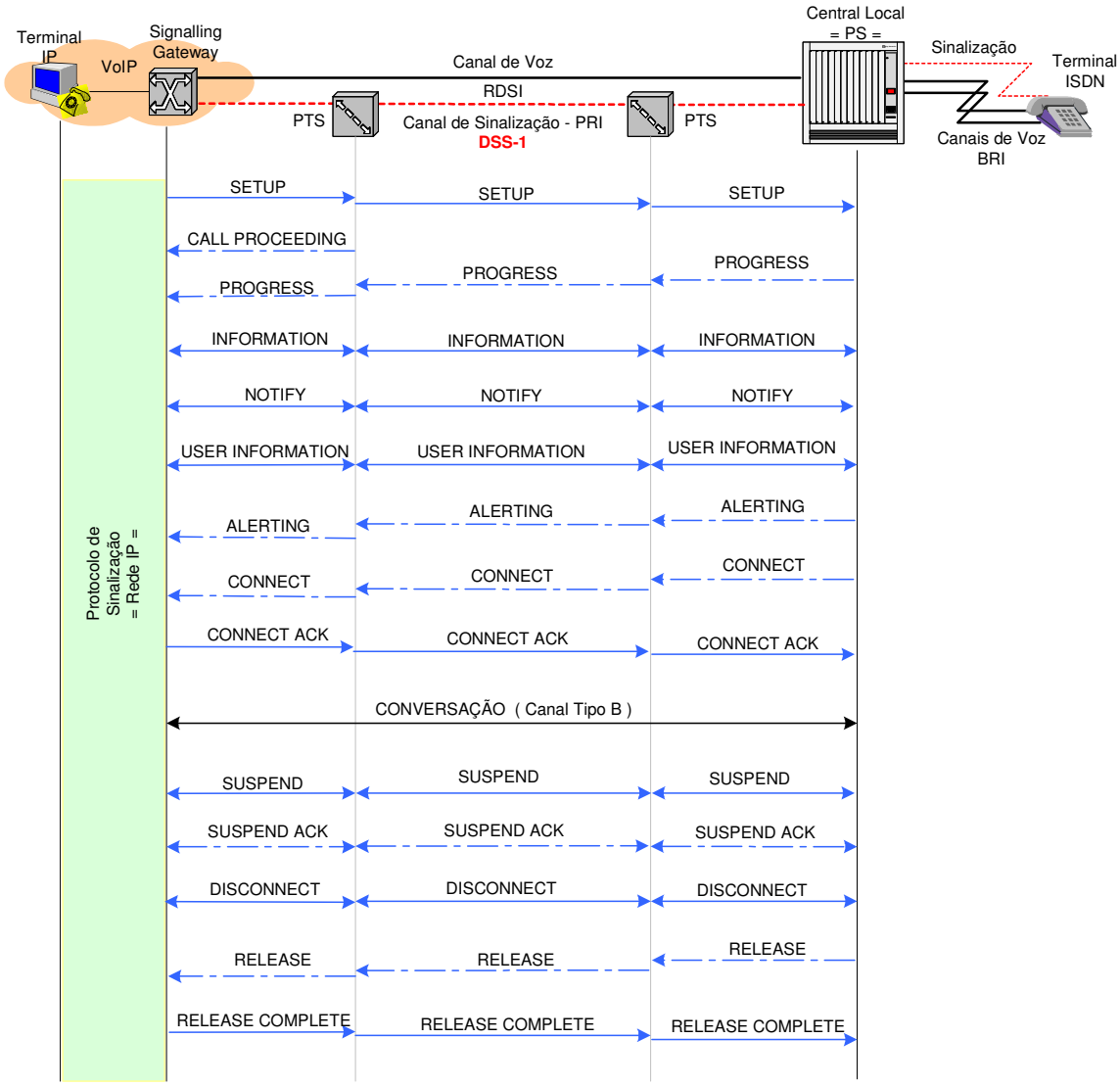


Figura A.2: Sinalização DSS-1 de uma chamada básica bem sucedida

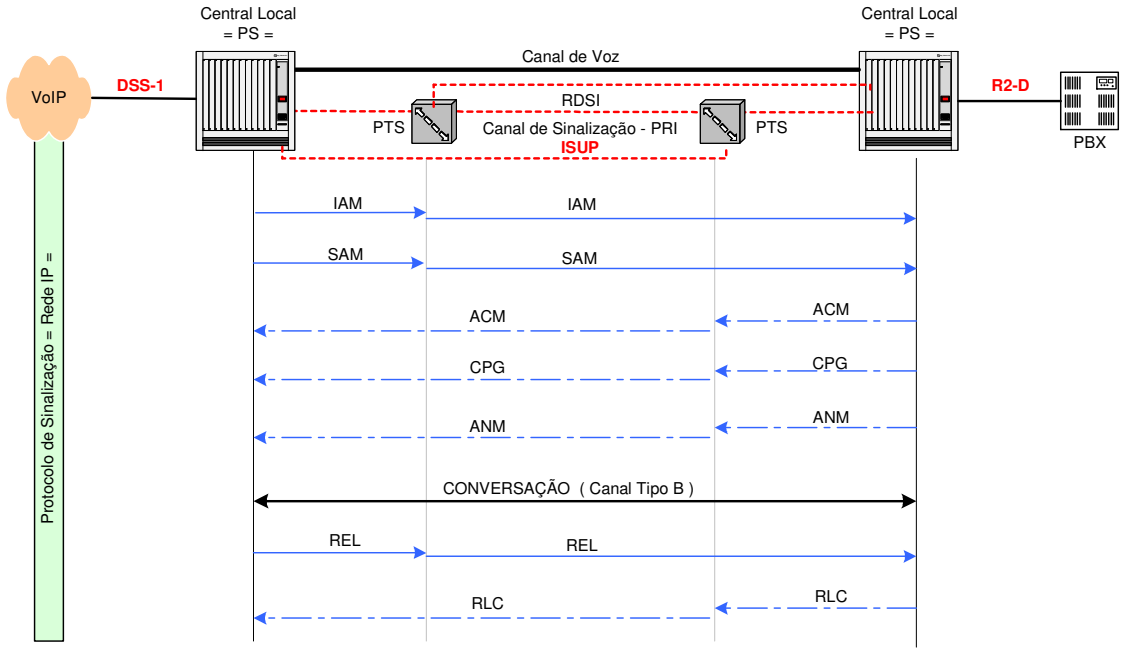


Figura A.3: Sinalização ISUP de uma chamada básica bem sucedida

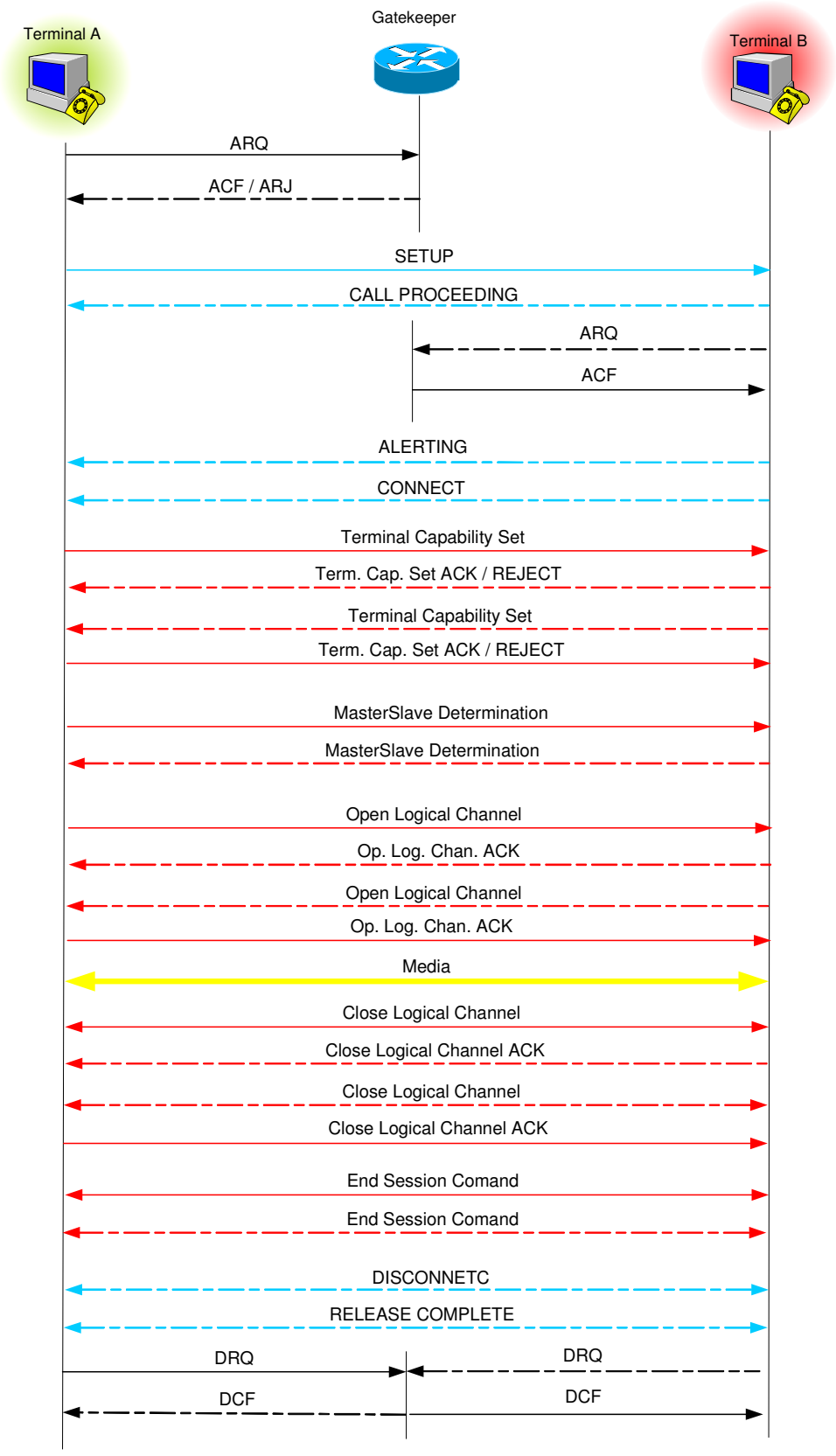


Figura A.4: Sinalização H.323 de uma chamada básica bem sucedida

As mensagens na cor preta da Figura A.4 são referentes ao protocolo H.225 (RAS) e mostra apenas o processo de Admissão por parte dos Terminais, entretanto mensagens de Registro, como *RRQ (Registration_Request)* e mensagens de Status, como *BRQ (Bandwidth_Request)* também fazem parte deste protocolo, entre outras.

ARQ *(Admission_Request)*→ Solicitação de recursos ao Gatekeeper para transmissão. Esta mensagem contém o endereço de origem e de destino (IP ou E.164), tipo de chamada (voz, vídeo, conferencia, etc) e de CODEC, entre vários outros parâmetros.

ACF *(Admission_Confirm)*→ Autorização para transmissão com os recursos requeridos pelo Terminal/Gateway ou com recursos menores. Permite que o Terminal de origem inicie o procedimento de sinalização de controle de chamada.

ARJ *(Admission_Reject)*

Em azul claro se encontram as mensagens de sinalização do protocolo H.225 *Call Signalling*, proveniente do protocolo Q.931 de redes RDSI. Estas mensagens já foram enunciadas no tópico sobre Sinalização DSS-1. O protocolo H.245 aparece na cor vermelha e cada mensagem estabelece a comunicação em apenas um sentido, como pode ser visto na figura.

TerminalCapabilitySet → Permite a troca de capacidades entre Terminais. Dessa forma, através desta mensagem cada Terminal indica o numero de seu canal lógico, o tipo de mídia que deseja transmitir e, principalmente, define o CODEC que deseja usar em sua transmissão, assim como quais suporta receber no canal lógico de retorno, de acordo com sua preferência.

TerminalCapabilitySet ACK → Cada Terminal responde com a mensagem *TerminalCapabilitySetAck*, caso aceite os parâmetros anunciados.

TerminalCapabilitySetReject → Se houver rejeição de capacidade por parte de alguns dos Terminais ou até mesmo pelo Gatekeeper, esta mensagem é enviada até que se estabeleça um acordo em relação às capacidades suportadas pelas partes Caso o

transmissor não receba resposta desta mensagem, ele envia a seguinte mensagem: *TerminalCapabilitySetRelease.*

MasterSlaveDetermination → Os Terminais trocam mensagens para a definição de quem será o Master ou Slave durante a chamada, isto é herança do protocolo H.235 e evita conflitos de interesse entre os Terminais, como em chamadas simultâneas e em conferências. Também é útil para distribuição de chaves de criptografia. Um parâmetro importante desta mensagem é o "Tipo de Terminal", a partir deste campo define-se o mestre/escravo pela ordem de prioridade. Segue a lista de prioridades: MCU > GK > GW > Telefones IP.

OpenLogicalChannel → Abertura de canais unidirecionais para tráfego de mídia. Os canais de dados (T.120) são bidirecionais. Esta mensagem contém parâmetros de endereço e porta que o destino deve enviar pacotes RTP e RTCP, se usa supressão de silêncio e código corretor de erro, etc.

De forma mais didática, a Figura A.5 apresenta outra visão do conjunto de protocolos H.323 para VoIP.

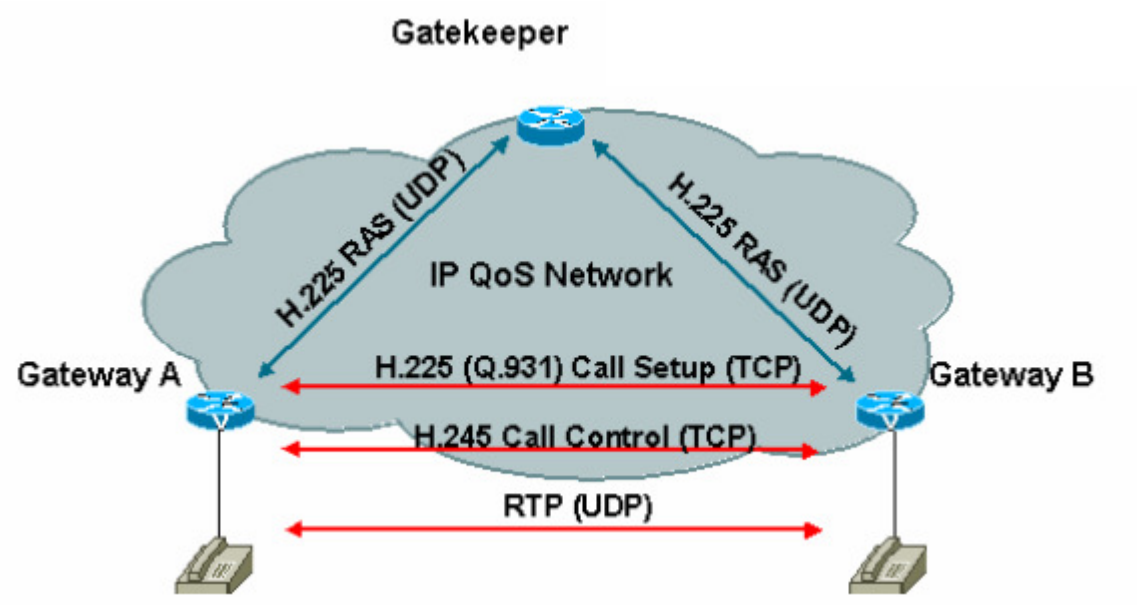


Figura A.5: Aplicação Típica dos Protocolos H.323

FAST CONNECT

Há outros mecanismos para tornar o estabelecimento de uma conexão de áudio H.323 menos custosa e mais eficiente, como o procedimento *FAST CONNECT*. Sua premissa é permitir comunicação bidirecional básica, isto é, apenas áudio, imediatamente após a mensagem *CONNECT* tenha sido recebida. A partir deste procedimento a mensagem *OpenLogicalChannel* é suprimida do fluxo de sinalização e o Terminal inclui um novo parâmetro nas mensagens *SETUP*, chamado *faststart*, que inclui os canais de mídia que o Terminal pode enviar e receber, contendo os CODECs, portas RTP e RTCP e o número do canal lógico. De maneira geral, parece ser um equívoco considerar as características descritas anteriormente como simplificações H.323. Na verdade, elas foram introduzidas principalmente para corrigir falhas na estrutura do H.323v1, existente no que diz respeito a tempos de configuração de chamada e operação com a rede de comutação de circuitos.

H.245 TUNNELING

O método *H.245 Tunneling* pode ser visto como substituto do *FAST CONNECT*, visto que as mensagens H.245 seguem encapsuladas nas mensagens Q.931, de modo que apenas uma conexão TCP seja necessária para sinalizar uma chamada. É também uma otimização que pode ser aplicada para todas as chamadas que requerem sinalização H.245 complexa, como o caso de conferências multiponto. O Terminal encapsula uma ou mais mensagens H.245 codificadas em um novo campo chamado *H.245control* de qualquer mensagem Q.931. Quando uma mensagem H.245 precisa ser enviada quando nenhuma mensagem Q.931 estiver pendente, a mensagem H.245 será encapsulada em uma mensagem Q.931 *FACILITY*. Uma vez que qualquer conexão estiver estabelecida, os Terminais devem parar de usar o túnel H.245.

SINALIZAÇÃO SIP

A Figura A.6 apresenta um exemplo de chamada de um Terminal IP para outro similar, com encerramento ao fim da conversa. Esta é a configuração mais simples de uma ligação SIP, onde um telefone liga diretamente para outro Terminal através do número IP de destino. Neste cenário, a esfera de serviços está limitada, não só pelas características individuais de cada Terminal, mas também, pela ausência de provedores de serviços dentro da rede, onde a ligação acontece sem o intermédio de Gateways ou Servidores.

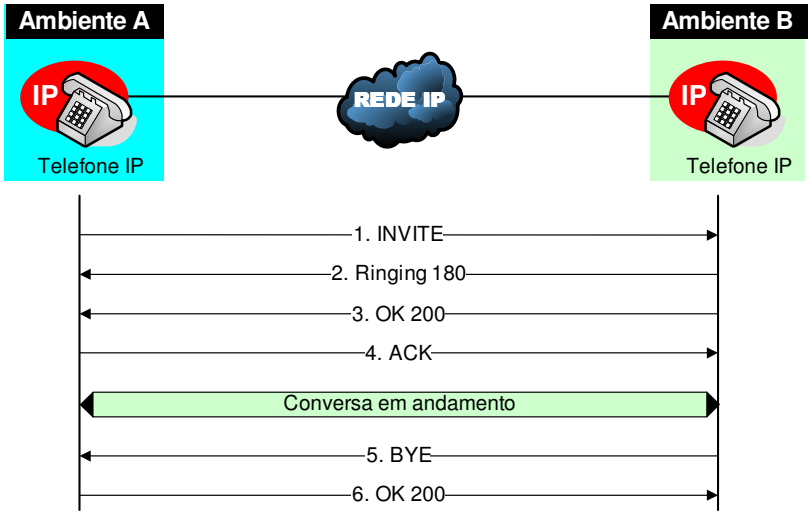


Figura A.6: Sinalização SIP de uma chamada básica bem sucedida

Descrição das Etapas

	Etapa	Descrição
1	INVITE	Convite para realização de uma chamada do telefone IP do Ambiente A para o telefone IP do Ambiente B.
2	Ringing 180	Sinalização de toque na origem e no destino. Isto indica que o Telefone IP do Ambiente B buscado foi encontrado.
3	OK 200	Terminal de destino aceita pedido de conexão. Ao fazer isto, além de abrir a conexão por sua parte, sinaliza que é capaz de tratar media no formato requisitado pelo telefone de origem.
4	ACK	Mensagem de confirmação de ocupação do canal de conversação.
5	BYE	O pedido BYE é usado quando qualquer uma das partes deseja finalizar a conversa.
6	OK 200	Aceitação do pedido BYE e encerramento da conversa.

A Figura A.7 apresenta um cenário um pouco mais complexo e dois fluxos de comunicação distintos. O primeiro fluxo é representado em vermelho e a chamada é realizada dentro dos limites de um mesmo domínio SIP. Inicialmente, o Endpoint 1 se registra no Servidor de Registro, que atualiza sua localização no Servidor de Redirecionamento. Em seguida, realiza uma chamada para o Endpoint 2 através do Servidor Proxy, que conhece o terminal de destino e encaminha a troca de sinalização até o estabelecimento do canal RTP de voz fim-a-fim. O Endpoint 2 encerra a conexão através da troca de sinalização entre os terminais com auxílio do Servidor Proxy.

A segunda etapa da Figura A.7 ilustra o processo de sinalização quando o Endpoint 1 deseja chamar o Endpoint 3, que se encontra em outro domínio SIP. Este processo está identificado em verde e tem início com uma requisição de chamada para o Servidor Proxy, que não conhece a localização do terminal de destino e por isso faz uma consulta ao Servidor de Redirecionamento, que informa o endereço real do terminal de destino ao Endpoint 1. De posse desta informação, o Endpoint 1 encaminha sua chamada diretamente ao Endpoint 3 e a sinalização para estabelecimento e encerramento da chamada dessa vez é trocada fim-a-fim. O Servidor de Redirecionamento do Domínio A conhece a localização dos terminais registrados no Domínio B, representado pela nuvem azul, pois este último também possui todos os servidores SIP, apesar de não ilustrado na Figura A.7. Portanto, os Servidores de Redirecionamento devem se comunicar entre as nuvens, de forma a possuírem as informações atualizadas de localização dos usuários.

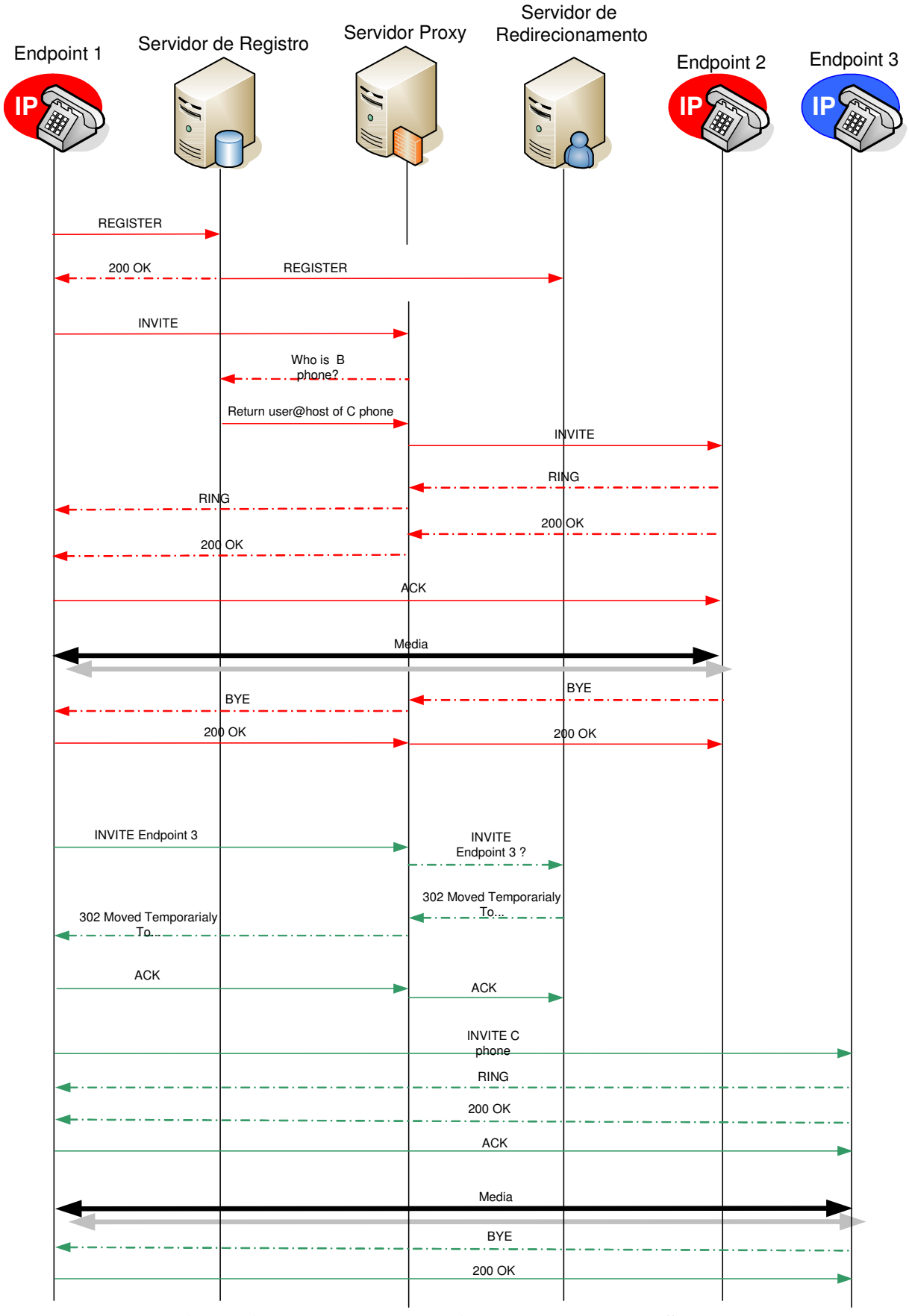
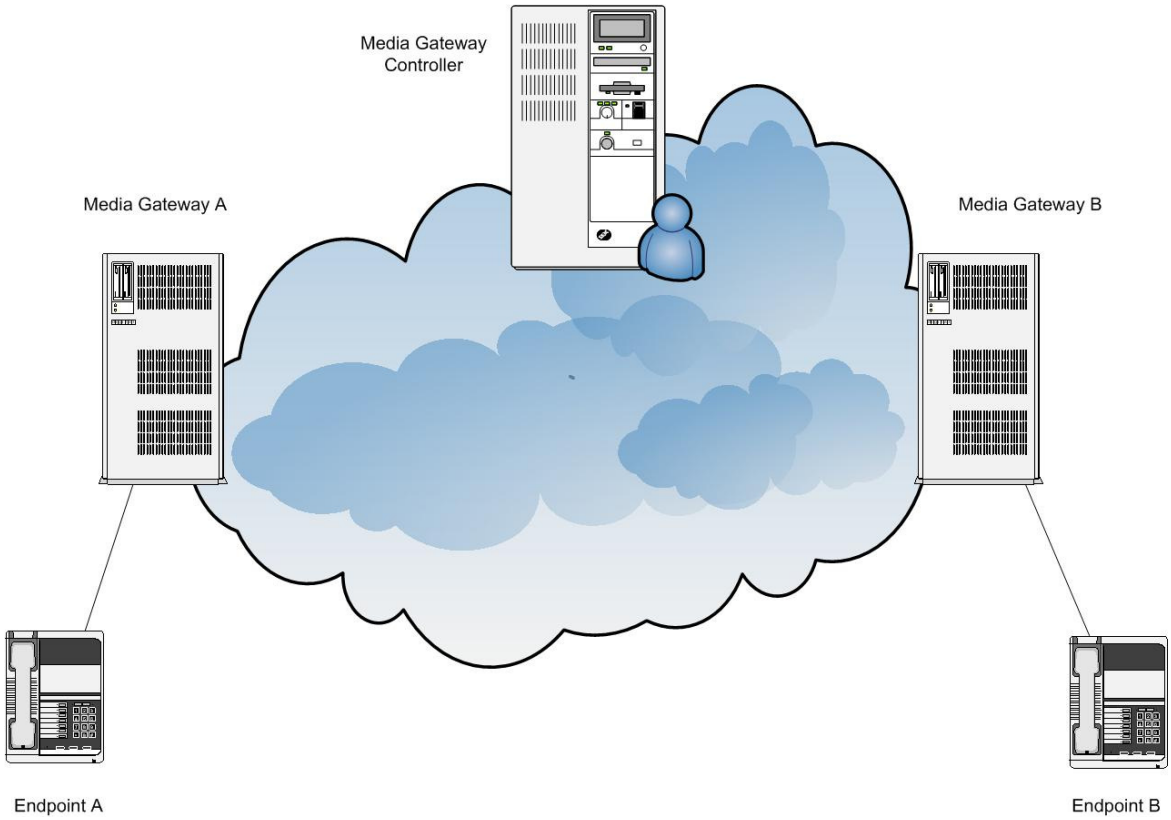


Figura A.7: Fluxo de comunicação do protocolo SIP.

SINALIZAÇÃO MGCP

Neste exemplo, o *Endpoint* A deseja realizar uma chamada para o *Endpoint* B, cada qual ligado ao seu respectivo Media Gateway, controlados pelo Media Gateway Controller de acordo com a Figura A.8 a seguir. Logo abaixo o comentário de cada mensagem pode ser acompanhado, incluindo os seus parâmetros ou cabeçalhos.



Media Gateway A	Media Gateway Controller	Media Gateway B
1 «--	RQNT	--»
2 RQNT Response	--» «--	RQNT Response
	Off Hook and Dialling	Off Hook and Dialling
3 NTFY from A	--»	
4 «--	CRCX	
5 CRCX Response	--»	
	CRCX	--»
6	«--	CRCX Response
7 «--	MDCX	--»
8 MDCX Response	--» «--	MDCX Response
	Ringing and Answer	Ringing and Answer

9	«--	RTP/RTCP		--»
	On Hook			
10	NTFY from A	--»		
11	«--	DLCX		--»
12	DLCX Response	--»	«--	DLCX Response

Figura A.8: Fluxo de comunicação do protocolo MGCP

1. Notification Request (RQNT) Command

O Media Gateway Controller usa o comando RQNT para informar ao Media Gateway que deve ser notificado na ocorrência de determinados eventos. Neste comando, o Media Gateway Controller envia parâmetros permitindo que o Media Gateway dê o tom de discagem para o Terminal quando este estiver fora do gancho, seja apto a coletar os dígitos e enviá-los em bloco ao invés de mandá-los individualmente, etc. A sintaxe da mensagem segue abaixo e os parâmetros opcionais e os comandos que podem ser encapsulados estão entre colchetes.

RQNT TransactionID TerminalID MGCP 1.0

[NotifiedEntity]

[RequestedEvents]

RequestIdentifier

[DigitMap]

[SignalRequests]

[QuarantineHandling]

[DetectEvents]

[pode encapsular o comando **TerminalConfiguration**]

2. NotificationRequest (RQNT) Response

O Media Gateway responde ao Media Gateway Controller dizendo que o comando foi recebido e entendido com sucesso.

200 TransactionID Commentary
[packageList]

3. Notify (NTFY) Command

Comando é enviado ao Media Gateway Controller para informar os eventos do Terminal A: terminal fora do gancho, enviado o tom de discagem, coleta dos dígitos. Os eventos são enviados todos juntos ao Media Gateway Controller.

3. Notify (NTFY) Response

401 TransactionID Commentary
[packageList]

4. CreateConnection (CRCX) Command

O Media Gateway Controller usa o comando CRCX para instruir o Media Gateway A a criar uma conexão com o Terminal A. Este comando especifica o modo da conexão, inicialmente *simplex*, pois o Terminal A pode receber mídia da rede, mas não pode transmitir. A razão para esta configuração é que o Terminal A ainda não possui informações suficientes do Terminal de destino para a troca de mídia.

Outro campo que compõe a mensagem de sinalização CRCX é o *LocalConnectionOptions*, que possui as informações de QoS, como RSVP, banda disponível e ToS, supressores de eco e de silêncio e questões de segurança.

CRCX TransactionID TerminalID MGCP 1.0
CallID
[NotifiedEntity]
[LocalConnectionOptions]
Mode
[RemoteConnectionDescriptor | SecondTerminalID]
[pode encapsular o comando **NotificationRequest**]
[pode encapsular o comando **TerminalConfiguration**]

5. CreateConnection (CRCX) Response

O MG A responde com sucesso, informando sua configuração através do parâmetro *LocalConnectionDescriptor*, como Endereço IP e porta para recepção, codificação de mídia, etc.

200 TransactionID Commentary
ConnectionID
[SpecificTerminalID]
[LocalConnectionDescriptor]
[SecondTerminalID]
[SecondConnectionID]
[PackageList]

5. CreateConnection (CRCX) Command

O MGC localiza o Gateway B de destino e utiliza este comando para instruir o MG B à criar uma conexão com o Terminal B. Importante observar, que diferentemente do comando CRCX anterior, este inclui as informações do Terminal A, através do parâmetro

RemoteConnectionDescriptor. De posse destas informações, o Terminal B conhece as características e o endereço do Terminal A de origem.

CRCX TransactionID TerminalID MGCP 1.0
CallID
[NotifiedEntity]
[LocalConnectionOptions]
Mode
[RemoteConnectionDescriptor | SecondTerminalID]
[pode encapsular o comando **NotificationRequest**]
[pode encapsular o comando **TerminalConfiguration**]

6. CreateConnection (CRCX) Response

O MG B por sua vez, responde ao MGC que o comando foi recebido com sucesso e inclui o parâmetro *LocalConnectionDescriptor*, com a descrição de sua configuração.

200 TransactionID Commentary
ConnectionID
[SpecificTerminalID]
[LocalConnectionDescriptor]
[SecondTerminalID]
[SecondConnectionID]
[PackageList]

7. ModifyConnection (MDCX) Command

O Media Gateway Controller manda o comando MDCX para o Media Gateway A. Este comando contêm o parâmetro RemoteConnectionDescriptor, correspondente ao session description recebido do Media Gateway B referente ao terminal B. Neste ponto, cada

terminal tem o session description do outro e sabem exatamente onde mandar o media stream e em qual formato.Agora que o session description está habilitado para o terminal, o Media Gateway A tem um endereço e a porta que deve mandar a media. Então, é com o comando MDCX que é ablactado que o terminal A passe a mandar e receber o que não acontecia até agora.

MDCX TransactionID EndpointID MGCP 1.0
CallID
ConnectionID
[NotifiedEntity]
[LocalConnectionOptions]
[Mode]
[RemoteConnectionDescriptor]
[encapsulated NotificationRequest]
[encapsulated EndpointConfiguration]

7. Notify (NTFY) Response

É nesta resposta que o Media Gateway A informa ao Media Gateway Controller que a conexão foi finalizada sem nenhum motivo aparente.

250 TransactionID Commentary
[packageList]

8. DeleteConnection (DLCX) Command

O Media Gateway Controller manda o comando DLCX para o Media Gateway B para que seja cancelada a conexão com o Media Gateway B. Esta operação é feita depois da inesperada desconexão ocorrida na outra ponta da chamada.

DLCX TransactionID TerminalID MGCP 1.0
CallID
[ConnectionID]
[encapsulated **NotificationRequest**ed]
[encapsulated **TerminalConfiguration**]

9. DeleteConnection (DLCX) Response

O Media Gateway B responde ao Media Gateway Controller que o comando foi executado com sucesso e a chamada é encerrada.

250 transactionID commentary
ConnectionParameters
[PackageList]

Anexo B – MEGACO/H.248

O protocolo Megaco é mais um protocolo para controle de Gateway. Desenvolvido pela IETF, através da RFC 3525, substituindo a antiga RFC 3015, em conjunto com a ITU-T, definido através da Recomendação H.248. Atualmente se encontra em sua primeira versão e é um protocolo de sinalização na nova arquitetura convergente, chamada de NGN como definida anteriormente. A função fundamental deste protocolo, assim como o MGCP, é permitir que os elementos da rede possam trocar informações de controle e de gerenciamento dos serviços.

Em meio aos protocolos de sistemas de comunicação atuais e emergentes, o Megaco/H.248 se fixa como uma opção compatível e complementar para o Media Gateway Control Protocol, provendo importantes vantagens em todo esse ramo de atuação. Hoje já se fala do Megaco como o protocolo de controle de Gateway do futuro e pode ser considerado o sucessor do MGCP, conforme o aumento na sua adesão já pelas novas redes.

MEGACO tem um grande número de similaridades com o MGCP. O MEGACO define oito comandos que fornecem a habilidade de controlar e manipular contextos e terminações. A maioria dos comandos é enviada do MGC para o MG. O protocolo também define o número de parâmetros disponíveis pra uso com os comandos e respostas. Dependendo do comando ou resposta em questão, um dado parâmetro será mandatório, proibido ou opcional. Para endereçar as variações entre diferentes tipos de terminações, MEGACO também incorpora o conceito de pacotes. Pacotes são grupos de propriedades, sinais, eventos e estatísticas. Num pacote, estes itens são definidos e atribuídos identificadores e os parâmetros associados a eles são especificados.

Obviamente, existem melhorias e algumas novas características no protocolo em relação ao MGCP, como o fato de poder implementar TCP em suas mensagens de sinalização; os comandos possuem nomes e algumas funções também diferentes; define um conceito mais amplo de estruturas, terminações e contextos; suporta uma gama maior de redes, como a ATM; suas mensagens também estão em formato binário, além de texto, maior eficiência na sinalização de chamadas e oferta de serviços multimídia, entre outros.

Como enunciado, o MEGACO é o padrão de evolução dos protocolos de controle de Gateways. Entretanto, não é objetivo deste trabalho abordar com mais profundidade o protocolo, ficando como sugestão para trabalhos futuros seu estudo técnico aprofundado, nos moldes dos desenvolvidos nesta Dissertação, permitindo posterior análise de suas relações com protocolos da rede de telefonia pública comutada do Capítulo 1.