**Universidade de Aveiro**
**2008**
Departamento de Electrónica, Telecomunicações e Informática

**André Marques e Silva**

# Sinalização de Media Gateways em Redes de Próxima Geração

**Universidade de Aveiro**
**2008**
Departamento de Electrónica, Telecomunicações e Informática

**André Marques e Silva**

# Sinalização de Media Gateways em Redes de Próxima Geração

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações, realizada sob a orientação científica da Professora Doutora Susana Sargento, Professora auxiliar convidada do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro e co-orientação do Doutor Victor Marques.

**o júri**

| | |
|---|---|
| **presidente** | Professor Doutor José Luis Guimarães Oliveira<br>professor associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro |
| **arguente** | Professor Doutor Rui Prior<br>professor auxiliar do Departamento de Ciências de Computadores da Faculdade de Ciências da Universidade do Porto |
| **orientadora** | Professora Doutora Susana Sargento<br>professora auxiliar convidada do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro |
| **co-orientador** | Doutor Victor Marques<br>Gestor de Divisão de Desempenho de Rede e Plataformas de Acesso em Rádio e Cobre do Departamento de Desenvolvimento de Sistemas de Rede da Portugal Telecom Inovação, S.A. |

**agradecimentos**

À Professora Susana Sargento, pela sua disponibilidade, interesse e partilha de conhecimentos. Foi bastante importante a sua ajuda na concretização desta Dissertação e, também, durante o meu percurso pelo Instituto de Telecomunicações de Aveiro.

Ao Doutor Victor Marques da PT Inovação S.A. pela sua disponibilidade, preocupação e ajuda durante o trabalho realizado no âmbito desta Dissertação e, também, durante a presente colaboração com a PT Inovação S.A.

A toda comunidade *SHipNET* que sempre se mostraram disponíveis para discutir os resultados obtidos no decorrer desta Dissertação.

A todos os amigos e colegas do DSR-4 pelo apoio necessário para o desenvolvimento desta Dissertação.

Aos meus pais António e Isabel, e amigos, Marília, Miguel, Bruno, Luís Soares, Luís Silva e todos aqueles que me deram incansável apoio, motivação, e mostraram preocupação durante os períodos mais difíceis desta Dissertação.

**palavras-chave**

3GPP, TISPAN, RPG, IMS, SIP, RTP, MEGACO/H.248, VoIP, SS7, PSTN, AGCF, *Media Gateway* de *Trunking*, *Media Gateway* de Acesso.

**resumo**

Com o grande crescimento das comunicações móveis e fixas, o acesso à *Internet* tornou-se cada vez mais numa exigência, colocando à industria das Telecomunicações, especialmente aos operadores, grandes desafios. Serviços comuns como chamadas de voz, podem agora ser oferecidos pelos *Internet Service Providers* (ISPs) aos seus clientes sobre a forma de serviço *Voice over* IP (VoIP). Este serviço deixou de ser exclusivo das redes *Public Switched Telephone Network*/*Integrated Services Digital Network* (PSTN/ISDN) e passou a ser fornecido também na *Internet*. Mas devido à necessidade de manter as tradicionais redes PSTN/ISDN, houve a necessidade de criar um ambiente de convergência, não só para estas redes mas também para outros tipos de redes de acesso, independentemente da tecnologia. É neste campo que os organismos de normalização e os operadores têm dado os seus contributos, criando uma rede de controlo e de transporte comum baseada em IP para a convergência de serviços.

Inicialmente o 3rd *Generation Partnership Project* (3GPP) definiu uma arquitectura de convergência móvel com a rede IP, constituída por elementos de controlo, transporte e serviço, de nome IP *Multimedia Subsystem* (IMS). Mais tarde, esta arquitectura serviu de base (*core*) para o grupo TISPAN do *European Telecommunications Standard Institute* (ETSI) na normalização das Redes de Próxima Geração.

Esta Dissertação pretende dar uma resposta à convergência fixo-móvel no âmbito da arquitectura PSTN/ISDN *Emulation Subsystem* (PES) do TISPAN. Este sistema permite que todos os clientes de uma Rede de Próxima Geração de um operador acedam a serviços das redes PSTN/ISDN e *Digital Subscriber Line* (DSL) de uma forma simples e imperceptível. Com este intuito foram desenvolvidos cenários de testes para os sistemas *Trunking* e de Acesso da arquitectura PES, tendo como objectivo final a sua integração na plataforma de próxima geração *Service Handling on ip NETworks* (SHipNET). Esta Dissertação experimenta várias situações reais de chamadas de voz sobre os cenários de testes, e inicia a implementação de um novo elemento definido para a arquitectura PES, *Access Gateway Control Function* (AGCF), para o controlo de *Media Gateways* nas redes de Acesso.

**keywords**

3GPP, TISPAN, RPG, IMS, SIP, RTP, MEGACO/H.248, VoIP, *Trunking Media Gateway*, *Access Media Gateway*.

**Abstract**

With the big growth of mobile and fixed communications, Internet access has become a requirement, putting the telecommunication industry, and especially the operators, in front of a major challenge. Services such as voice calls can now be offered by Internet Service Providers (ISPs) to their customers. This service is no longer exclusive of Public Switched Telephone Network/Integrated Services Digital Network (PSTN/ISDN) and is now provided also through the Internet. But, because of the need to maintain the traditional PSTN/ISDN networks, there was a need to create a convergence, not only for these networks but also for other types of access networks, regardless of technology. The standards bodies and operators have made their contributions to create a network of control and transport policy, based on IP, for the services convergence.

In the beginning the 3rd Generation Partnership Project (3GPP) defined an architecture for mobile convergence with IP network, made up of control, transport and service elements, called IP Multimedia Subsystem (IMS). Later, the core IMS served the ETSI TISPAN group in standardization of Next Generation Networks.

This thesis aims to give an answer for fixed-mobile convergence within the architecture defined by TISPAN PSTN/ISDN Emulation Subsystem (PES). This system, formed by a Trunking, originally defined by the 3GPP IMS, and Access part, allows all customers of a Next Generation Network operator, access to PSTN/ISDN and Digital Subscriber Line (DSL) network services in a simple way. With this purpose, scenarios were developed for Trunking and Access systems of PES arquitecture, with the goal to integrate into the next generation platform *Service Handling on ip NETworks* (SHipNET). This thesis tests several real situations of voice calls on testing scenarios, and begins the implementation of a new element defined for PES arquitecture, *Access Gateway Control Function* (AGCF), for Media Gateways control purpose in access networks.

# Índice

# Índice de Figuras

# Índice de Tabelas

# Acrónimos

| | |
|---|---|
| 3GPP | *3rd Generation Partnership Project* |
| 3GPP2 | *3rd Generation Partnership Project 2* |
| AAA | *Authentication, Authorization, Accounting* |
| ACM | *Address Complete Message* |
| AGCF | *Access Gateway Control Function* |
| AIRP | *Analyse Information Routing Plan* |
| AKAv1 | *Authentication and Key Agreement version 1* |
| AMF | *Access Management Function* |
| A-MGF | *Access-Media Gateway Function* |
| AMI | *Alternate Mark Inversion* |
| AMR | *Adaptive Multi-Rate* |
| AMR-WB | *Adaptive Multi-Rate-Wideband* |
| ANM | *Answer Network Message* |
| ANSI | *American National Standards Institute* |
| API | *Application Programming Interface* |
| ARF | *Access Relay Function* |
| ARIB | *Association of Radio Industries and Businesses* |
| AS | *Application Server* |
| ASF | *Application Server Function* |
| ATIS | *Alliance for Telecommunications Industry Solutions* |
| AUC | *Authentication Center* |
| A-VGF | *Access-VoIP Gateway Function* |
| B2BUA | *Back-to-Back User Agent* |
| BGCF | *Breakout Gateway Control Function* |
| BGF | *Border Gateway Function* |
| BICC | *Bearer Independent Call Control* |
| BRI | *Basic Rate Interface* |

| | |
|---|---|
| BTF | *Basic Transport Function* |
| CAMEL | *Customized Applications for Mobile network Enhanced Logic* |
| CAP | *CAMEL Application Part* |
| CAS | *Channel Associated Signaling* |
| C-BGF | *Core-Border Gateway Function* |
| CCBS | *Call Control on Busy Subscriber* |
| CCSA | *China Communications Standards Association* |
| CDPN | *Called Party Number* |
| CDR | *Charging Data Record* |
| CF | *Charging Functions* |
| CGPN | *Calling Party Number* |
| CIC | *Circuit Identification Code* |
| CIDP | *Collect Information Dial Plan* |
| CLIP | *Calling Line Identification Public* |
| CLIR | *Calling Line Identification Restriction* |
| CMS | *Converged Multimedia System* |
| CODEC | *COder/DECoder* |
| CPC | *Calling Party Category* |
| CRCX | *CreateConnection* |
| CRG | *Charging Information* |
| DLCX | *DeleteConnection* |
| DND | *Do Not Disturb* |
| DNS | *Domain Name System* |
| DPC | *Destination Point Code* |
| DSL | *Digital Subscriber Line* |
| DSLAM | *Digital Subscriber Line Access Multiplexer* |
| DSP | *Digital Signal Processor* |
| DTMF | *Dual Tone Multi-Frequency* |
| DVB | *Digital Video Broadcast* |
| EMAC | *Ethernet Media Access Controller* |
| ESF | *Extended Super Frame* |
| ETSI | *European Telecommunications Standard Institute* |
| EVRC | *Enhanced Variable Rate CODEC* |

| | |
|---|---|
| FoIP | *FAX over IP* |
| FXS | *Foreign eXchange Subscriber* |
| GGSN | *Gateway GPRS Support Node* |
| GPRS | *General Packet Radio Service* |
| GSM | *Global System for Mobile communications* |
| gsmSCF | *gsm Service Control Function* |
| HDB3 | *High-Density Bipolar* 3 |
| HLR | *Home Location Register* |
| HSS | *Home Subscriber Server* |
| HTTP | *Hypertext Transfer Protocol* |
| IAM | *Initial Address Message* |
| IBCF | *Interconnection Border Control Function* |
| I-BGF | *Interconnection-Border Gateway Function* |
| I-CSCF | *Interrogating-Call Session Control Function* |
| IESG | *Internet Engineering Steering Group* |
| IETF | *Internet Engineering Task Force* |
| iLBC | *Internet Low Bit rate Codec* |
| IMS | *IP Multimedia Subsystem* |
| IMS-ALG | *IMS-Application Level Gateway* |
| IMS-MGW | *IMS-Media Gateway* |
| IM-SSF | *IP Multimedia-Service Switching Function* |
| IP | *Internet Protocol* |
| IP-CAN | *IP-Connectivity Access Network* |
| IPsec | *IP security* |
| ISDN | *Integrated Services Digital Network* |
| ISP | *Internet Services Provider* |
| ISUP | *ISDN User Part* |
| IT | *Instituto de Telecomunicações* |
| ITU | *International Telecommunication Union* |
| ITU-T | *International Telecommunication Union – Telecommunications* |
| IUA | *ISDN Q.921-User Adaptation* |
| IWF | *Interworking Function* |
| LAN | *Local Area Network* |

| | |
|---|---|
| M2UA | *Message Transfer Part* 2 *User Adaptation layer* |
| M3UA | *Message Transfer Part* 3 *User Adaptation layer* |
| MAP | *Mobile Application Part* |
| MBMS | *Multimedia Broadcast Multicast Service* |
| MD5 | *Message-Digest algorithm 5* |
| MDCX | *ModifyConnection* |
| MEGACO | *MEdia GAteway COntrol* |
| MGC | *Media Gateway Controller* |
| MGCF | *Media Gateway Control Function* |
| MGCP | *Media Gateway Control Protocol* |
| MGF | *Media Gateway Function* |
| MRFC | *Multimedia Resource Function Controller* |
| MRFP | *Multimedia Resource Function Processor* |
| MS | *Media Server* |
| MTP | *Message Transfer Part* |
| NAI | *Nature of Address Indicator* |
| NAPT | *Network Address and Port Translation* |
| NAS | *Network Access Server* |
| NASS | *Network Attachment Subsystem* |
| NAT-PT | *Network Address Translation - Protocol Translation* |
| NC | *Naming Convention* |
| NI | *Network Indicator* |
| NOA | *Nature Of Address* |
| NPI | *Numbering Plan Indicator* |
| OPC | *Originating Point Code* |
| OSA API | *Open Service Access Application Programming Interface* |
| OSA AS | *Open Service Access Application Server* |
| OSA-SCS | *Open Service Access – Service Capability Server* |
| PBX | *Private Branch eXchange* |
| PCG | *Project Coordination Group* |
| PCI | *Peripheral Component Interconnect* |
| PCM | *Pulse Code Modulation* |
| P-CSCF | *Proxy-Call Session Control Function* |

| | |
|---|---|
| PDF | *Policy Decision Function* |
| PES | *PSTN/ISDN Emulation Subsystem* |
| PLMN | *Public Land Mobile Network* |
| PoC | *Push-to-talk over Cellular* |
| POTS | *Plain Old Telephone Service* |
| PPP | *Point-to-Point Protocol* |
| PRACK | *SIP Provisional Response ACKnowledgement* |
| PRI | *Primary Rate Interface* |
| PSTN | *Public Switched Telephone Network* |
| PTT | *Push To Talk* |
| QoS | *Quality of Service* |
| RACS | *Resource and Admission Control Subsystem* |
| RCEF | *Resource Control Enforcement Function* |
| REL | *Release* |
| RFC | *Request For Comment* |
| RLC | *Release Complete* |
| R-MGF | *Residential Media Gateway Function* |
| RPG | *Rede de Próxima Geração* |
| RQNT | *NotificationRequest* |
| RTCP | *Real-time Transport Control Protocol* |
| RTP | *Real-time Transport Protocol* |
| R-URI | *Request-URI* |
| R-VGF | *Residential-VoIP Gateway Function* |
| SCCP | *Signaling Connection and Control Part* |
| SCF | *Service Control Function* |
| S-CSCF | *Serving-Call Session Control Function* |
| SCTP | *Stream Control Transmission Protocol* |
| SDP | *Session Description Protocol* |
| SER | *SIP Express Router* |
| SG | *Signalling Gateway* |
| SGF | *Signalling Gateway Function* |
| SGW | *Signalling Gateway* |
| SHipNET | *Service Handling on ip NETworks* |

| | |
|---|---|
| SIGTRAN | *Signalling Transport* |
| SIP | *Session Initiation Protocol* |
| SLF | *Subscription Locator Function* |
| SMS | *Short Message Service* |
| SMTP | *Simple Mail Transfer Protocol* |
| SN | *Signalling Node* |
| SPAN | *Services and Protocols for Advanced Networks* |
| SS7 | *Signalling System #7* |
| SSP | *Service Switching Point* |
| TC | *Technical Committes* |
| TCAP | *Transaction Capabilities Application Part* |
| TCP | *Transmission Control Protocol* |
| TDM | *Time Division Multiplexing* |
| THIG | *Topology Hiding Inter-network Gateway* |
| TIPHON | *Telecommunications and Internet Protocol Harmonisation Over Networks* |
| TISPAN | *Telecommuncations and Internet converged Services and Protocols for Advanced Networking* |
| T-MGF | *Trunking-Media Gateway Function* |
| TSG | *Technical Specification Group* |
| TTA | *Telecommunications Technology Association* |
| TTC | *Telecommunication Technology Committee* |
| UA | *User Agent* |
| UAC | *User Agent Client* |
| UAL | *User Adaptation Layer* |
| UAS | *User Agent Server* |
| UDP | *User Datagrama Protocol* |
| UE | *User Equipment* |
| UMTS | *Universal Mobile Telecommunications System* |
| UPSF | *User Proxy Server Function* |
| URI | *Uniform Resource Identifiers* |
| URL | *Uniform Resource Locators* |
| UTP | *Unshielded Twisted Pair* |

| | |
|---|---|
| VAD | *Voice Activity Detection* |
| VCC | *Voice Call Continuity* |
| VDSL | *Very-high-bit-rate Digital Subscriber Line* |
| VGF | *VoIP Gateway Function* |
| VoIP | *Voice over IP* |
| WAN | *Wide Area Network* |
| WiMax | *Worldwide Interoperability Access* |
| WLAN | *Wireless Local Area Network* |
| XCAP | *Extensible Markup Language Configuration Access Protocol* |

# Capítulo 1: Introdução

## 1.1. Motivação

Durante a última década, as redes de telecomunicações têm vindo a sofrer grandes alterações. No início dos anos 70 houve uma grande alteração nas redes de telecomunicações de voz devido à migração do formato analógico para o formato digital. Com esta alteração de tecnologia começaram a aparecer as tão utilizadas redes fixas inteligentes com o Sistema de Sinalização #7 (SS7) normalizado pelo organismo *International Telecommunication Union – Telecommunications* (ITU-T). Hoje, este tipo de tecnologia é vulgarmente utilizado nas redes convencionais *Public Switched Telephone Network* (PSTN) em muitos países para a realização, principalmente, de serviços de voz.

Paralelamente a esta tecnologia, outro tipo de redes tem vindo a crescer, desde a década 80, de uma forma espantosa e a ganhar cada vez mais protagonismo entre as diferentes tecnologias das redes de telecomunicações são as redes de comutação de pacotes, nomeadamente a *Internet*.

Este tipo de redes sempre teve um crescimento independente, devido à existência do domínio móvel e fixo, em que os serviços oferecidos pelos operadores eram dependentes do tipo de tecnologia de transporte, ou seja, cada rede com diferente tecnologia de transporte tinha os seus próprios serviços normalizados por organizações separadas. Este é o caso actual no domínio das telecomunicações, obedecendo ao conceito de integração vertical, ilustrado na Figura 1. Mas com o crescimento corrente das tecnologias de acesso fixas e móveis, houve a necessidade de convergir estes dois domínios, onde serviços multimédia como voz, rádio e televisão poderão ser oferecidos aos clientes sobre uma mesma tecnologia de transporte comum IP, independentemente da tecnologia de acesso, segundo o conceito de integração horizontal (Figura 1).

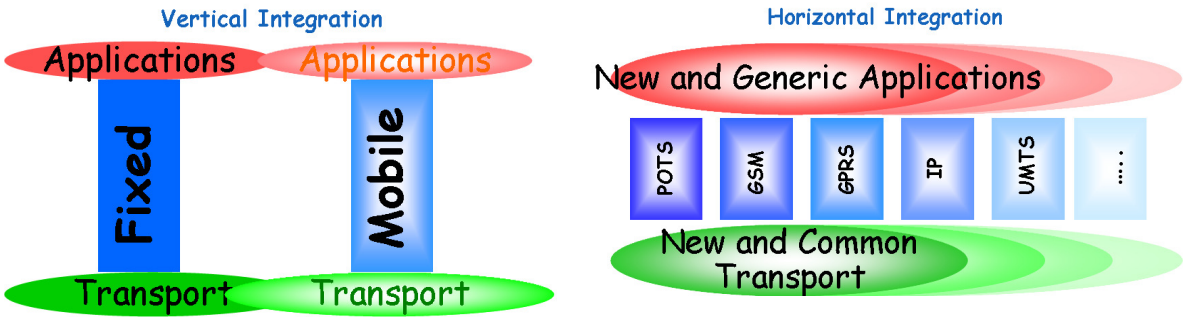



Figura 1- Modelo de camadas para o conceito de integração [1].

Este conceito alterou drasticamente a visão do mercado das telecomunicações, principalmente dos operadores. Estes podem agora oferecer serviços multimédia que anteriormente eram dependentes da tecnologia de acesso e do transporte móvel ou fixo, aos seus clientes através do domínio *Internet*. Para esta concretização, os operadores terão que dar resposta aos seguintes desafios resultantes da convergência [1]:

- Satisfazer os requisitos dos operadores de rede e de fornecedores de serviços:
  - Permitir a criação de serviços atractivos e ao mesmo tempo rentáveis, sem que os clientes finais se apercebam da interferência dos operadores;
  - Assegurar interoperabilidade entre diferentes domínios de redes de operadores, em que as regras vigentes podem ser distintas;
  - Assegurar gestão de redes *peer-to-peer*;
  - Permitir migração faseada.
- Satisfazer os requisitos dos clientes em termos de:
  - Mobilidade, incluindo facilidade de endereçamento;
  - Qualidade de Serviço (QoS);
  - Segurança.

Naturalmente, este novo conceito de convergência despertou o interesse de toda a indústria de telecomunicações, o que levou à necessidade da existência de uma cooperação mútua entre as organizações de normalização, que até aqui tinham papéis diferentes. O organismo 3rd *Generation Partnership Project* (3GPP) foi criado inicialmente com o intuito de normalizar as redes de comunicações móveis, e o *European Telecommunications Standard Institute* (ETSI) e o *International Telecommunication Union* (ITU) as redes fixas.

Como resultado desta cooperação, uma nova solução, referida como Rede de Próxima Geração (RPG), foi proposta pelos organismos de normalização como uma arquitectura

futura de convergência "*all*-IP" focada no fornecimento de serviços multimédia independentemente da tecnologia de acesso.

Aproveitando já o trabalho da *release* 5 e 6 do 3GPP na definição de uma arquitectura de controlo, designada por IP *Multimedia Subsystem* (IMS), para a migração móvel com o mundo IP, o grupo *Telecommuncations and Internet converged Services and Protocols for Advanced Networking* (TISPAN) do ETSI está neste momento a trabalhar na *release* 1 e 2, em conjunto com o 3GPP (*release* 7), para a normalização de uma arquitectura em que utiliza o *core* IMS do 3GPP como elemento central para a convergência móvel-fixo no âmbito das RPGs (Figura 2).

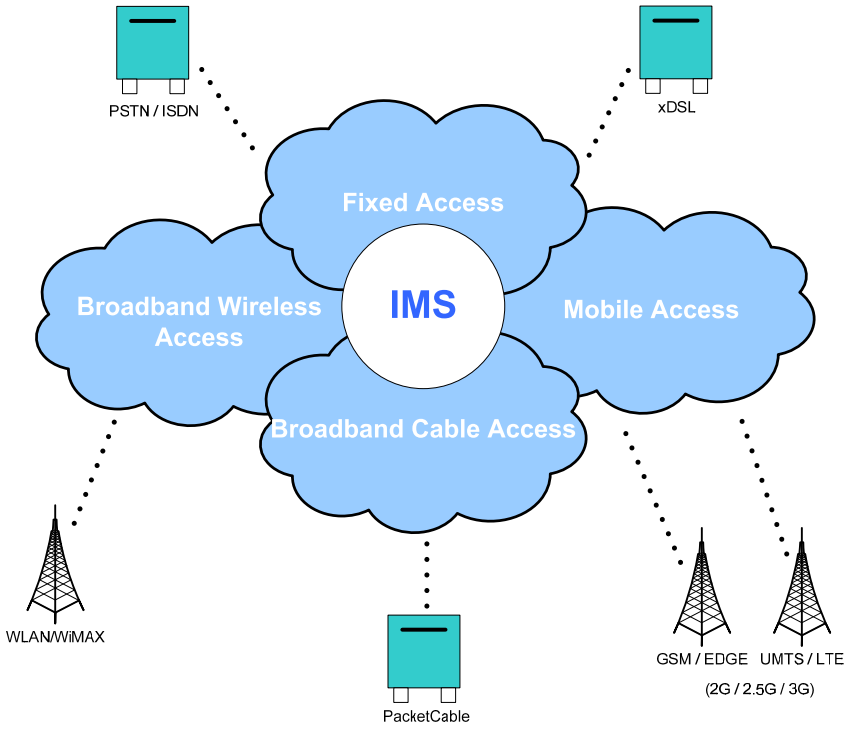



Figura 2- Modelo básico para arquitectura de convergência RPG [20].

O subsistema central IMS do 3GPP surgiu na arquitectura das RPGs devido aos seguintes motivos [2]:

- Necessidade de conectividade IP com QoS para serviços em tempo real;
- Grandes vantagens no fornecimento de serviços sobre IP:
  - Permite interacção directa com a *Internet* (explorando assim os serviços aí disponíveis);
  - Permite o fornecimento de novos serviços sem alterar a infra-estrutura;
  - Todos os dados (voz, vídeo, texto) usam o mesmo formato de transmissão.
- Previsões de aumento do mercado para Voz sobre IP (VoIP);

- Usa plataformas de serviço multimédia baseadas em protocolos da *Internet* normalizados pelo *Internet Engineering Task Force* (IETF):
  - *Session Initiation Protocol* (SIP)/*Session Description Protocol* (SDP);
  - *Real-time Transport Protocol* (RTP)/*Real-time Transport Control Protocol* (RTCP);
  - Diameter;
  - IPv6.
- Independente da tecnologia de acesso rádio;
- Independente da tecnologia de transporte IP.

A *release* 1 do TISPAN definiu uma arquitectura base de convergência móvel-fixo, designada por PSTN/*Integrated Services Digital Network* (ISDN) *Emulation Subsystem* (PES), onde foram adicionadas novas funcionalidades aos elementos IMS-*Media Gateway* (IMS-MGW), *Signalling Gateway* (SGW) e *Media Gateway Control Function* (MGCF) do sistema *Trunking* IMS do 3GPP e novos elementos, como o *Access Gateway Control Function* (AGCF), *Residential/Access-Media Gateway Function* (R/A-MGF) e VoIP *Gateway Function* (VGF) para permitir o acesso das redes fixas *Digital Subscriber Line* (DSL) aos serviços das RPGs. Esta convergência da redes fixas xDSL permite integrar sistemas de *Media Gateway* de Acesso com portos VoIP nos *Digital Subscriber Line Access Multiplexers* (DSLAMs), removendo o componente que faz a comutação dos canais de voz das linhas xDSL para a rede PSTN/ISDN.

A arquitectura orientada para as RPGs é baseada na junção de subsistemas que permitem maior flexibilidade no ajuste da arquitectura, através da adição suave de novos subsistemas ao longo do tempo, de forma a contemplar novas solicitações e classes de serviço exigidas pelo mercado, e fácil importação de subsistemas de outros organismos internacionais de normalização.

O subsistema PES é um desses exemplos para a convergência das redes fixas. Este subsistema do TISPAN está perante um processo evolutivo, presentemente na *release* 2, e será um dos principais focos do trabalho realizado para esta Dissertação.

## 1.2. Objectivos

O principal objectivo desta Dissertação é dar a conhecer as potencialidades dos elementos da arquitectura PES TISPAN através da implementação de um sistema que permitirá aos clientes o acesso, a partir das RPGs, aos mesmos serviços que acediam previamente de

uma implementação PSTN/ISDN, baseada em tecnologia *Time Division Multiplexing* (TDM). Este sistema será utilizado para a realização de alguns testes VoIP. Os elementos deverão basear-se nas funcionalidades normalizadas pelo TISPAN/IMS para os sistemas de *Media Gateway* de *Trunking* e de Acesso segundo a arquitectura PES.

Para o sistema *Media Gateway* de Acesso será implementado um AGCF para o controlo de *Media Gateways* de acesso e residenciais através do protocolo *MEdia GAteway Control* (MEGACO)/H.248, baseando-se na norma ETSI TS 182 012 [3] do TISPAN.

## 1.3. Estrutura do Documento

A presente Dissertação está organizada da seguinte forma:

- Capítulo 2: Breve descrição sobre a estrutura e funcionamento das principais organizações envolvidas na normalização das RPGs: ITU, IETF, 3GPP, ETSI; e suas contribuições para estas redes;
- Capítulo 3: Descrição da arquitectura de referência IMS do 3GPP para as RPGs. Principais requisitos apontados para o IMS, funcionalidades lógicas dos elementos constituintes para o controlo/sinalização de serviços e para o fluxo de dados multimédia, descrição dos principais protocolos adoptados para a troca de sinalização (SIP), de dados multimédia (RTP e RTCP) e para Autenticação, Autorização e *Accouting* (Diameter);
- Capítulo 4: Descrição da arquitectura de referência do TISPAN para as RPGs, tendo como base o IMS normalizado pelo 3GPP. Descrição da arquitectura PES do TISPAN para a emulação de serviços das redes PSTN/ISDN com as RPGs. Comparação e alterações efectuadas pelo TISPAN aos elementos do *core* IMS do 3GPP no âmbito do PES;
- Capítulo 5: Descrição dos produtos adoptados para a solução ip-*Keel*® *Trunking*. Realização de pequenos testes para familiarização com esses produtos. Descrição dos vários passos/cenários implementados até chegar ao demonstrador final RPG *Service Handling on ip NETworks* (*SHipNET*®), testes realizados e discussão dos resultados obtidos para a solução ip-*Keel*®. Grau de congruência entre os elementos do ip-*Keel*® com os requisitos indicados pelo PES;
- Capítulo 6: Conclusão do trabalho realizado, bem como uma visão do trabalho futuro para a solução ip-*Keel*®.

# Capítulo 2: Organizações de Normalização

As Redes de Próxima Geração (RPGs) devem ser especificadas em diferentes níveis de implementação. Estes níveis remetem para a definição de uma arquitectura global através da especificação das funções e procedimentos a desempenhar pelos vários elementos constituintes das RPGs e dos protocolos a utilizar na interacção entre estes elementos. Este trabalho é efectuado por diferentes organizações de normalização, com diferentes responsabilidades, que, em conjunto, contribuem para o desenvolvimento e evolução global destas redes para uso comercial por parte dos operadores de telecomunicações.
Antes de uma descrição detalhada dos elementos e protocolos utilizados nas RPGs, irá ser feita uma breve descrição das organizações envolvidas no desenvolvimento das RPGs e as suas contribuições para evolução destas mesmas redes.

## 2.1. International Telecommunication Union

O *International Telecommunication Union* (ITU) [4] foi fundado em 1865 com o intuito de resolver problemas no âmbito do tráfego primórdio das telecomunicações. Hoje o ITU é uma organização de cooperação internacional, onde membros de vários países e várias entidades comerciais se juntam para criar normas na área das telecomunicações. Dentro do ITU existe um sector responsável pela elaboração de recomendações e normas de acordo com as necessidades do sector das telecomunicações designado por *International Telecommunication Union – Telecommunications* (ITU-T) [5]. Neste momento o ITU-T está concentrado na normalização das RPGs dando contribuições importantes através das suas recomendações (ITU-T *Recommendations*).

## 2.2. Internet Engeneering Task Force

O *Internet Engineering Task Force* (IETF) [6] é uma organização aberta ao público, criada por operadores de telecomunicações, investigadores e prestadores de serviços, cujo

objectivo é contribuir para a evolução e melhoramento da *Internet* através da especificação de protocolos a utilizar nestas redes. A maior parte dos protocolos utilizados hoje na *Internet* foram especificados por esta organização e estão documentados em *Request For Comments* (RFCs) de acesso livre ao público. A sua missão está documentada no RFC 3935 [7].

O IETF está organizado em diferentes grupos de trabalho, formado por voluntários que contribuem para a elaboração e publicação de um conjunto de documentos técnicos. O número de grupos de trabalho não é fixo. Uma vez revistos e publicados os documentos da responsabilidade de um grupo de trabalho, este é dissolvido da organização. Os grupos de trabalho são agrupados em áreas dentro do mesmo contexto de investigação e cada uma destas áreas é gerida por uma entidade especifica. Estas áreas que agrupam um determinado número de grupos de trabalho são membros do *Internet Engineering Steering Group* (IESG). Esta entidade é responsável pela gestão técnica do IETF e decide as áreas, e consequentemente os grupos de trabalho a formar.

Os documentos produzidos pelos grupos de trabalho são designados por *Internet-Drafts*. Quando terminados, são submetidos a uma revisão pelo IESG que decide posteriormente se o *Internet-Draft* deve ser publicado num novo RFC. Este processo está documentado no RFC 2026 [8].

O IETF especificou muitos protocolos utilizados nas RPGs, e neste momento está concentrado no desenvolvimento de extensões a estes protocolos, com especial atenção para o *Session Initiation Protocol* (SIP) muito utilizado nestas redes.

## 2.3. 3rd Generation Partnership Project

O 3rd *Generation Partnership Project* (3GPP) [9] foi fundado em 1998 por várias organizações de normalização de diferentes países: *Association of Radio Industries and Businesses* (ARIB) (Japão) [10], *China Communications Standards Association* (CCSA) (China) [11], *European Telecommunications Standard Institute* (ETSI) (Europa) [12], *Alliance for Telecommunications Industry Solutions* (ATIS) (Estados Unidos da América) [13], *Telecommunications Technology Association* (TTA) (Coreia) [14] e *Telecommunication Technology Committee* (TTC) (Japão) [15], com a finalidade de especificar as redes móveis de terceira geração baseando-se nas já existentes de segunda geração.

O 3GPP está organizado em grupos designados por *Technical Specification Group* (TSG) e estes grupos são geridos e supervisionados pela entidade *Project Coordination Group* (PCG) dentro do 3GPP. Esta organização está ilustrada em [16]. Actualmente o 3GPP está estruturado em quatro TSGs que aprovam as normas desenvolvidas, resultando documentos finais designados por *Technical Specificiations* (TS) e *Technical Reports* (TR). Todas estas especificações resultantes do trabalho de cada uma das TSGs são agrupadas pelo 3GPP em *releases*.

A primeira versão do IP *Multimedia Subsystem* (IMS), utilizada nas RPGs, foi introduzida pelo 3GPP na *release* 5 [17] em 2002, que deu a conhecer uma arquitectura base deste sistema para a convergência de serviços multimédia baseados em IP com as redes móveis. Mais tarde, em 2005, surgiu a *release* 6 [18] que introduziu a este sistema algumas melhorias como suporte de serviços *Push-to-talk over Cellular* (PoC), *Multimedia Broadcast Multicast Service* (MBMS), etc., bem como a operação com as redes de acesso *Wireless Local Area Network* (WLAN). Neste momento em fase de finalização está a *release* 7 do 3GPP que engloba já o trabalho desenvolvido pelo grupo *Telecommuncations and Internet converged Services and Protocols for Advanced Networking* (TISPAN) do ETSI na convergência com as redes de acesso fixas, nomeadamente a *Digital Subscriber Line* (DSL), para os serviços multimédia.

A Figura 3 ilustra a evolução temporal das *releases* do 3GPP para o IMS.

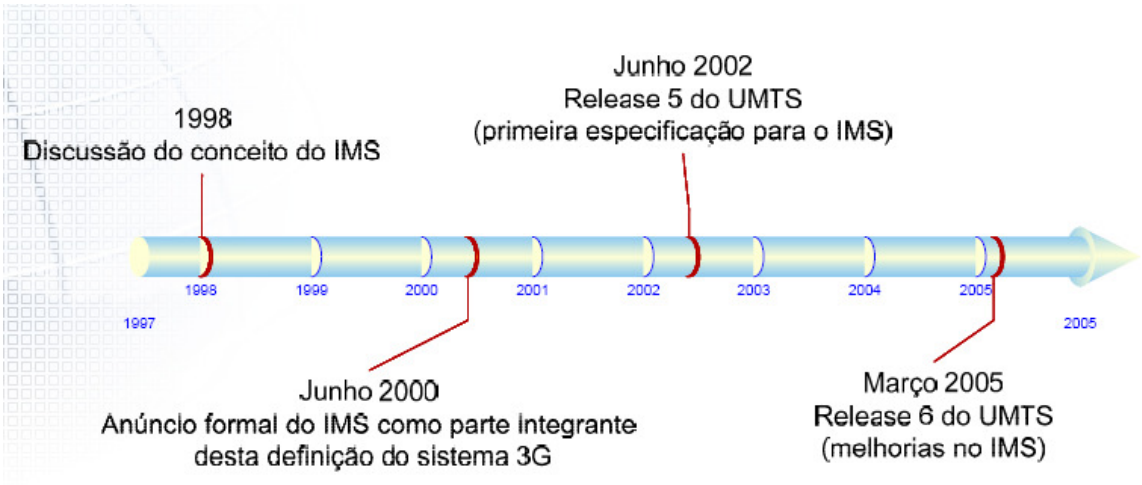



Figura 3- Evolução temporal das releases do 3GPP para o IMS [2].

Desde que o 3GPP foi criado para a especificação técnica das redes de terceira geração baseando-se no sistema móvel europeu *Global System for Mobile communications* (GSM), nasceu a necessidade de criar uma organização com a mesma missão que o 3GPP para os

sistemas móveis da América do Norte e Ásia, baseado na normalização do *American National Standards Institute* (ANSI). Este foi o motivo que deu origem à organização 3rd *Generation Partnership Project* 2 (3GPP2) [19].

## 2.4. European Telecommunications Standard Institute

O ETSI é uma organização fundada em 1988 com a responsabilidade de normalizar o sector informativo e das tecnologias da comunicação dentro da Europa. Formado por membros de operadores de telecomunicações, vendedores e prestadores de serviços, juntos participam e contribuem para a normalização das redes de telecomunicações. O trabalho nesta organização está divido em *Technical Committes* (TC) com determinadas tarefas e responsabilidades.

Em Setembro de 2003, o ETSI juntou dois TCs: o *Telecommunications and Internet Protocol Harmonisation Over Networks* (TIPHON) e o *Services and Protocols for Advanced Networks* (SPAN), dando origem a um único TC designado por TISPAN [20] com o principal papel na convergência entre as redes móveis e fixas, utilizando o IMS do 3GPP como o sistema central no acesso a aplicações multimédia baseadas em IP pelos utilizadores destas redes. Este TC está organizado em oito grupos de trabalho com diferentes responsabilidades, como se pode constatar em [21].

Em Dezembro de 2005 o TISPAN publicou a sua primeira *release* com a arquitectura global das RPGs; presentemente em fase de finalização está a *release* 2 com principal foco na integração de novas redes de acesso e serviços (IPTV, etc.), e agendada está a *release* 3 como ilustrado na Figura 4.

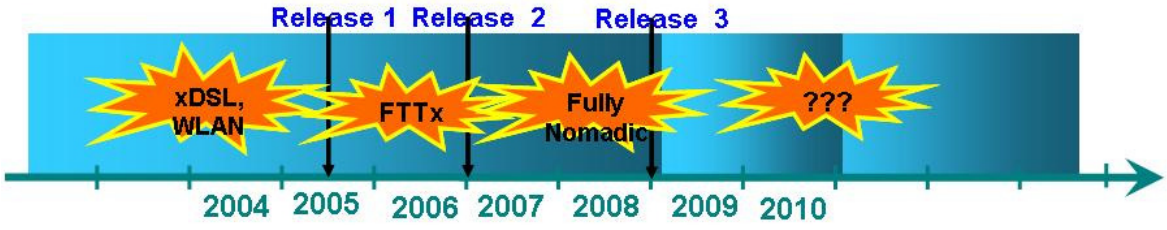



Figura 4- Evolução temporal das *releases* do TISPAN para as RPGs .

## 2.5. Relação entre as Organizações

As RPGs definidas pelo TISPAN são baseadas no IMS especificado na *release* 6 do 3GPP. Existe, portanto, um trabalho em conjunto entre estas organizações com o objectivo de criar uma solução comum. É neste pressuposto que a *release* 7 do 3GPP e a *release* 2 do

TISPAN têm dado maior ênfase, ou seja, na convergência entre diferentes redes de acesso com o IMS, dando origem a uma solução comum que são as RPGs.

As organizações TISPAN e 3GPP/3GPP2 têm especial interesse no trabalho desenvolvido pelo IETF, pois muitos protocolos utilizados no IMS foram desenvolvidos por esta organização, que por sua vez tem dado o seu contributo na realização de novos protocolos e extensões aos protocolos já existentes no âmbito das RPGs do TISPAN. O protocolo SIP e as suas extensões para as RPGs evidenciam a importância da colaboração desta organização com as restantes. A colaboração ente o 3GPP e o IETF está especificada no RFC 3113 [22] e entre o 3GPP2 e o IETF no RFC 3131 [23].

O ITU-T também tem um papel fundamental nesta colaboração. As normas desenvolvidas pelo ITU-T são recomendações para a evolução das RPGs: um exemplo são os *codecs* de áudio e vídeo, e o protocolo *MEdia GAteway COntrol* (MEGACO)/H.248 utilizado nestas redes. Este protocolo foi desenvolvido em trabalho conjunto entre as organizações IETF (MEGACO) e ITU-T (H.248 *Recommendation*).

## 2.6. Sumário

O trabalho de normalização e especificação de uma arquitectura comum para as RPGs é efectuado por diferentes organizações de normalização, com diferentes responsabilidades, que, em conjunto, contribuem para o desenvolvimento e evolução global destas redes para uso comercial por parte dos operadores de telecomunicações.

Inicialmente o ITU foi fundado com o intuito de resolver problemas no âmbito do tráfego primórdio das telecomunicações. Hoje, com o grupo ITU-T, está concentrado na normalização das RPGs dando contribuições importantes através das suas recomendações (ITU-T *Recommendations*).

O IETF especificou muitos protocolos, documentados em RFCs, que são utilizados nas arquitecturas para as RPGs, e neste momento está concentrado no desenvolvimento de extensões para estes protocolos, com especial atenção para o protocolo SIP muito utilizado nestas redes.

O 3GPP foi fundado por várias organizações de normalização de diferentes países com a finalidade de especificar uma arquitectura para as redes móveis de terceira geração baseando-se nas já existentes redes GSM. Neste momento em fase de finalização está a *release* 7 que engloba já o trabalho desenvolvido pelo grupo TISPAN do ETSI na

convergência com as redes de acesso fixas, nomeadamente xDSL, para os serviços multimédia.

Em Setembro de 2003, o ETSI formou o grupo TISPAN com o principal papel na convergência entre as redes móveis e fixas, utilizando o IMS do 3GPP como o sistema central no acesso a aplicações multimédia baseadas em IP aos utilizadores destas redes. Em Dezembro de 2005 o TISPAN publicou a sua primeira *release* com a arquitectura global das RPGs.

As organizações TISPAN e 3GPP/3GPP2 têm especial interesse no trabalho desenvolvido pelo IETF, pois muitos protocolos utilizados no IMS foram desenvolvidos por esta organização, que por sua vez tem dado o seu contributo na realização de novos protocolos e extensões aos protocolos já existentes no âmbito das RPGs do TISPAN. O protocolo SIP e as suas extensões para as RPGs evidenciam a importância da colaboração desta organização com as restantes.

# Capítulo 3: 3GPP IP Multimedia Subsystem

A ideia inicial do 3rd *Generation Partnership Project* (3GPP) [9] para o IP *Multimedia Subsystem* (IMS) era definir uma arquitectura baseada em IP que possibilitava o acesso a aplicações multimédia, disponíveis na *Internet*, pelas redes móveis. Este sistema, composto por um conjunto de elementos de controlo, seria utilizado pelos operadores de telecomunicações para fornecer serviços multimédia em tempo-real (voz, vídeo, videoconferência, etc.), e também outros tipos de serviços (pesquisa WEB, acesso ao *e-mail*, *download* de conteúdos, etc.) aos seus clientes móveis, obedecendo a determinados requisitos.

Actualmente o IMS é especificado como uma arquitectura que permite o estabelecimento de sessões multimédia entre utilizadores de redes com diferentes tipos de tecnologia: pacotes: *Wireless Local Area Network* (WLAN), *Digital Subscriber Line* (DSL), *Worldwide Interoperability Access* (WiMax), etc; e circuitos: *Public Switched Telephone Network* (PSTN), *Integrated Services Digital Network* (ISDN), etc., para além das redes móveis. A *release* 7 do 3GPP especifica o *core* IMS como um sistema independente da tecnologia de acesso, permitindo a outras organizações normalizar uma arquitectura de convergência de várias redes de acesso utilizando o *core* IMS como elemento central.

Neste capítulo serão definidos os requisitos mais importantes para esta arquitectura, será feita uma descrição de cada um dos elementos constituintes, com especial detalhe nos elementos que possibilitam a integração com as redes fixas PSTN/ISDN, bem como dos protocolos utilizados na interacção entre eles.

## 3.1. Requisitos

Nesta secção estão descritos os requisitos básicos para esta arquitectura, necessários ao suporte de aplicações multimédia baseadas em IP. Estes requisitos estão especificados na norma 3GPP TS 22.228 [24].

### 3.1.1. Sessões Multimédia

Um dos principais requisitos do IMS é possibilitar o estabelecimento de diferentes tipos de sessões multimédia entre utilizadores, independentemente do tipo de terminal ou da tecnologia da rede de acesso onde se encontra.

Para que os utilizadores possam ter acesso a estas aplicações multimédia e estabelecer novas sessões, é necessário que estes estejam registados e autenticados para essas aplicações dentro do IMS.

Dentro de cada sessão estabelecida podem ser suportadas várias aplicações multimédia concorrentes, e cada utilizador pode estabelecer diferentes sessões simultaneamente. Considere-se o seguinte exemplo: durante uma sessão de voz entre dois utilizadores, um deles pode enviar um ficheiro para o outro e estabelecer uma nova sessão com um servidor multimédia para fazer um *download* de um filme. Os terminais dos utilizadores deverão suportar diferentes tipos de *codecs* de áudio e/ou vídeo para que não ocorra nenhuma falha no estabelecimento da sessão por incompatibilidade. As aplicações devem ser fornecidas pelo IMS sem qualquer redução de privacidade, segurança, ou autenticação comparado com os sistemas tradicionais.

### 3.1.2. Qualidade de Serviço

Um dos principais requisitos da arquitectura IMS é utilizar mecanismos de Qualidade de Serviço (QoS) que garantam serviços multimédia de qualidade entre os utilizadores. Um dos maiores problemas dos serviços baseados em IP é o serviço ser realizado em modo *best-effort*[1], sem suporte de mecanismos de QoS. Os serviços em tempo-real são os mais afectados por este problema, pois são os mais sensíveis a certas condições da rede como atrasos, variações de atraso, perdas de pacotes, e necessitam de uma largura de banda mínima para que o serviço seja realizado em boas condições.

O IMS permite a negociação de QoS para as sessões multimédia, entre o utilizador e o operador, no momento em que as sessões são estabelecidas e mesmo durante o decorrer das sessões. O mesmo se aplica para a negociação de QoS de determinados componentes *media* individuais. Este requisito deve então permitir que para uma sessão de voz entre utilizadores do domínio IP se faça com igual qualidade em relação ao domínio de

[1] Modo geralmente utilizado no fornecimento de serviços sobre as redes IP.

comutação de circuitos. Isto permitiria que a qualidade de uma sessão multimédia fosse igual e independente da tecnologia da rede onde se encontra o utilizador.

O QoS negociado para uma determinada sessão depende do tipo de aplicação utilizada nessa sessão e de outros factores, como o máximo de largura de banda que pode ser alocada para esse utilizador, dependendo da sua subscrição, e do estado da rede. O IMS deve permitir que os operadores controlem os parâmetros de QoS dos seus utilizadores para que possam diferenciar certos grupos de clientes.

### 3.1.3. Acesso Independente

É obvio que um dos requisitos básicos do IMS é a interligação com o domínio *Internet*, devido a este domínio possuir um vasto número de potenciais destinatários para as sessões multimédia iniciadas pelos utilizadores IMS.

Para além das redes de comutação de pacotes, como a *Internet*, é necessário que o IMS permita o acesso às suas aplicações pelos utilizadores das redes fixas de comutação de circuitos, como o PSTN/ISDN, das redes móveis normalizadas pelo 3GPP, como o *Global System for Mobile communications* (GSM) e o *Universal Mobile Telecommunications System* (UMTS), e de outro tipo de redes já mencionadas anteriormente.

### 3.1.4. Roaming

O *Roaming* é um requisito necessário das redes móveis de segunda e terceira geração. O IMS não foge à regra para este requisito devido à mobilidade de utilizadores de um determinado operador IMS para redes de operadores diferentes, por exemplo quando se deslocam para um país estrangeiro. Um determinado operador IMS deve garantir aos seus clientes o acesso aos serviços multimédia aos quais estão subscritos independentemente da sua localização geográfica. Para isso são estabelecidos protocolos e procedimentos entre operadores IMS de diferentes regiões, para que estes possam trocar informação dos seus clientes em caso de *roaming* de uma forma segura.

### 3.1.5. Controlo de Serviços

Os operadores IMS querem ter controlo e impor políticas sobre todos os serviços multimédia fornecidos aos seus clientes. Estas políticas de controlo de serviços podem ser divididas em duas categorias:

- Políticas Gerais: Estas políticas são aplicáveis a todos os clientes de um operador IMS. Por exemplo, a restrição de determinados *codecs* de vídeo e áudio que necessitem de uma grande largura de banda;
- Políticas individuais: Este tipo de políticas são aplicadas a um cliente particular ou grupo de clientes. São configuradas especificamente para cada utilizador e dependem da sua subscrição para com o seu operador IMS. Por exemplo, existem clientes que podem ter uma subscrição de serviços multimédia com um operador IMS que não inclua a utilização de vídeo. Nesta situação, como o cliente não está autorizado a utilizar vídeo mesmo que o seu terminal o suporte, o operador IMS não deve permitir o estabelecimento da sessão de vídeo.

### *3.1.6. Implementação de Serviços*

Este requisito tem influenciado bastante a normalização da arquitectura IMS. Ele indica que os serviços multimédia disponibilizados pelo IMS não são normalizados, e que deve ser o sistema de suporte a estes serviços que deve ser normalizado de forma a permitir o desenvolvimento de novos serviços por outras entidades independentes do IMS. Este requisito é o oposto aos modelos antigos de operação das redes móveis, em que os serviços eram normalizados para um determinado operador. Nesta situação não havia garantias que um determinado serviço iria funcionar em caso de *roaming*. A arquitectura IMS deve permitir que entidades independentes possam desenvolver e fornecer rapidamente aplicações e serviços multimédia que funcionem de igual forma em diferentes redes de operadores IMS.

## 3.2. Arquitectura

Antes de descrever a arquitectura interna do IMS, é importante reter que o 3GPP não normaliza os elementos físicos constituintes, mas sim as funcionalidades e interfaces de comunicação destes elementos. Os construtores são livres de decidir sobre a implementação física dos elementos; dois ou mais elementos funcionais podem ser combinados fisicamente num mesmo dispositivo se for necessário [25]. Os elementos funcionais que compõem a arquitectura lógica IMS do 3GPP estão indicados na Figura 5.

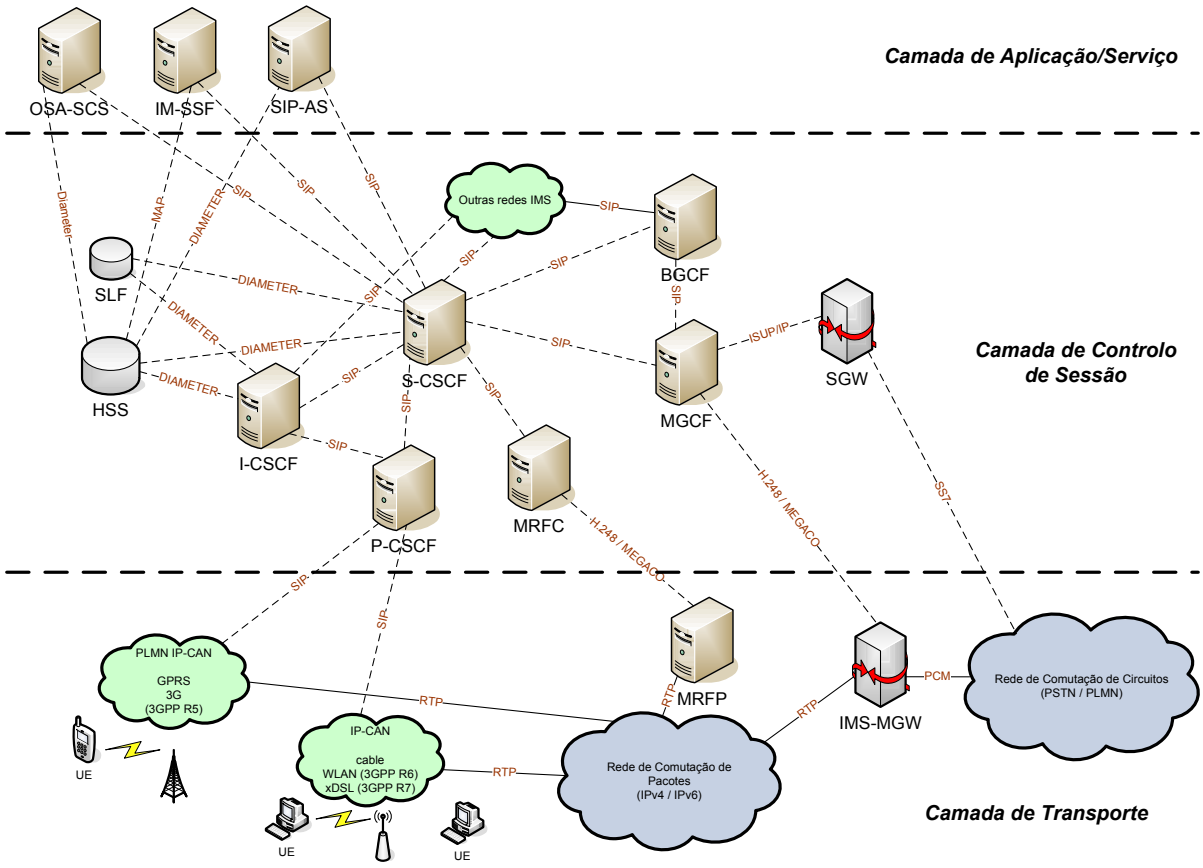



Figura 5- Arquitectura IMS do 3GPP.

Uma característica importante da arquitectura IMS é a utilização exclusiva de IPv6 nas suas redes. Para integrar com as redes tradicionais de IPv4 são necessários elementos, como o *Network Address Translation - Protocol Translation* (NAT-PT) e o IMS-*Application Level Gateway* (IMS-ALG).

A arquitectura IMS está dividida logicamente em três camadas funcionais de acordo com os elementos que a compõe e as suas funções para com a arquitectura. Estas camadas são: camada de controlo de sessão, camada de transporte e camada de aplicação/serviço (Figura 5).

De seguida é feita uma descrição, de acordo com a norma 3GPP TS 23.002 [26], das funções desempenhadas por cada um dos elementos das camadas lógicas do IMS.

### 3.2.1. Camada de Controlo de Sessão

A camada de controlo de sessão é a área funcional dentro do IMS que fornece todo o controlo para as sessões multimedia e é responsável pela independência entre as aplicações e o tipo de tecnologia utilizada nas redes de acesso. Os elementos que constituem esta

camada possuem funcionalidades de encaminhamento da sinalização para o estabelecimento, modificação ou terminação das sessões multimedia e de armazenamento da informação respeitante á subscrição dos clientes.

De seguida é feita uma descrição individual dos elementos desta camada lógica.

#### 3.2.1.1. Bases de Dados: Subscription Locator Function e Home Subscriber Server

O *Home Subscriber Server* (HSS) é a base de dados central do IMS onde são guardados os dados dos clientes necessários para o estabelecimento de sessões multimédia. Estes dados incluem: identificação do cliente, informação da sua localização, parâmetros de segurança para a sua autenticação e autorização na rede, informação dos serviços para o qual está subscrito e o endereço do elemento *Serving-Call Session Control Function* (S-CSCF) alocado para esse cliente.

O IMS pode conter mais do que um HSS para efeitos de redundância: no caso de falha de um elemento HSS o processo de autenticação e autorização dos clientes pode ser realizado devido à existência de outro HSS com a mesma informação, e para o caso de ser necessário mais do que um HSS devido ao elevado número de clientes.

O *Subscription Locator Function* (SLF) é uma base de dados necessária quando existe mais do que um HSS na rede. Esta base de dados contém informação para o mapeamento entre os utilizadores e o HSS onde estão guardados os respectivos dados. Assim, quando o *Interrogating*/*Serving*-CSCF (I/S-CSCF) envia um pedido ao SLF com o endereço de um cliente, este retorna o endereço do HSS que contém a informação desse cliente. O HSS é acedido através do protocolo Diameter, normalizado pelo *Internet Engineering Task Force* (IETF) no *Request For Comment* (RFC) 3588 [27], pelas redes móveis[2] e pelos elementos I/S-CSCF para efectuar autenticação e autorização dos clientes das redes móveis e fixas (Figura 5).

#### 3.2.1.2. Proxy-Call Session Control Function

Como se pode constatar pela Figura 5, o *Proxy*-CSCF (P-CSCF) é o primeiro ponto de contacto entre os utilizadores das redes de acesso e o IMS.

Este elemento pode estar localizado na rede IMS do operador do cliente ou na rede IMS de outro operador visitado por esse cliente no caso de *roaming*. Para os acessos móveis

baseados em *General Packet Radio Service* (GPRS), o P-CSCF está sempre localizado na mesma rede do *Gateway* GPRS *Support Node* (GGSN).

A aquisição do endereço de um P-CSCF e a sua alocação para um determinado utilizador é realizada durante o processo de registo desse utilizador na rede IMS. Depois de alocado, toda a sinalização trocada entre esse utilizador e o IMS passa por este elemento durante o período de tempo em que o utilizador se encontra registado. O processo de aquisição do endereço de um P-CSCF está descrito na norma 3GPP TS 23.228 [28].

O P-CSCF funciona como um *Session Initiation Protocol* (SIP) *proxy* com as seguintes funcionalidades:

- Autentica o utilizador e estabelece uma ligação segura utilizando o protocolo IP *security* (IPsec) [29], com o seu terminal. Esta ligação permite assegurar a integridade dos dados trocados entre o utilizador e o seu P-CSCF. Os outros elementos do IMS não necessitam de autenticar o utilizador, pois esta tarefa é desempenhada pelo P-CSCF e todos os outros elementos confiam nele. Mais detalhes sobre os mecanismos e procedimentos de segurança entre o utilizador e o P-CSCF encontram-se na norma 3GPP TS 33.203 [30];
- Encaminha o registo (SIP *Register*) do utilizador para o respectivo *Interrogating-Call Session Control Function* (I-CSCF) determinado a partir do domínio do operador no qual o utilizador está subscrito;
- Encaminha as mensagens SIP, provenientes do terminal do utilizador no processo de estabelecimento de sessões, directamente para o S-CSCF, ou para um I-CSCF que depois encaminhará para o S-CSCF. O endereço do S-CSCF é obtido pelo P-CSCF como resultado do processo de registo do utilizador;
- Comprime as mensagens SIP para reduzir o tempo de transmissão e de estabelecimento da sessão, pois o protocolo SIP é um protocolo baseado em texto e as suas mensagem podem ter grandes dimensões;
- Pode conter um elemento externo ou interno designado por *Policy Decision Function* (PDF). Este elemento é responsável pela gestão de recursos e de QoS, no plano de dados[3], para o utilizador. Mais detalhes sobre o PDF encontram-se na norma 3GPP TS 23.203 [31];

---

[2] Redes móveis de tecnologia baseada em pacotes e circuitos.
[3] Plano responsável pelo tráfego da informação multimédia (áudio, video, etc.).

- Gera *Charging Data Records* (CDRs) com informação relativa às sessões e registos dos seus utilizadores para taxação;
- Permite o estabelecimento de sessões para serviços de emergência[4] mesmo na presença de falhas dos outros elementos do IMS.

A rede IMS pode conter vários P-CSCFs para efeitos de redundância ou para o caso de ter de servir um elevado número de utilizadores.

### 3.2.1.3. Interrogating-Call Session Control Function

O elemento I-CSCF é o ponto inicial do IMS para as sessões multimédia destinadas aos clientes dessa rede, ou aos clientes de outros operadores que estão registados nessa rede IMS (*roaming*).

O endereço deste elemento está presente num servidor designado por *Domain Name System* (DNS) do seu domínio IMS, para que elementos remotos de outras redes IMS lhe possam aceder e utilizá-lo para encaminhar mensagens SIP para essa rede.

O I-CSCF funciona como um SIP *proxy* com as seguintes funcionalidades de acordo com a norma 3GPP TS 22.228 [24]:

- Aloca um S-CSCF para um determinado utilizador durante o seu processo de registo. Para isso, quando recebe um registo do utilizador (SIP *Register*) proveniente do P-CSCF, o I-CSCF comunica com o HSS e com o SLF, se existir mais que um HSS, para saber se o utilizador é cliente dessa rede e para obter informações sobre a sua subscrição. Em caso afirmativo, encaminha o registo para um determinado S-CSCF com fim de registar este utilizador nesse elemento, caso o utilizador ainda não esteja registado;
- Cifra certas partes da mensagem SIP contendo informação confidencial do operador IMS. Esta funcionalidade, designada por *Topology Hiding Inter-network Gateway* (THIG), é opcional e está documentada na *release* 6 do 3GPP. A partir da *release* 7 esta função passa a ser desempenhada pelo elemento *Interconnection Border Control Function* (IBCF) da arquitectura *Telecommuncations and Internet converged Services and Protocols for Advanced Networking* (TISPAN) [20];
- Encaminha as mensagens SIP de sessões multimédia de outros operadores IMS para o S-CSCF do utilizador destinatário. O endereço do S-CSCF alocado para esse utilizador é obtido do HSS antes do encaminhamento da mensagem;

- Gera CDRs com informação relativa às sessões e registos dos utilizadores para efeitos de taxação.

A rede IMS pode conter vários I-CSCFs para efeitos de redundância ou para o caso de ter de servir um elevado número de sessões multimédia simultaneamente. Este elemento geralmente está localizado na rede do operador do cliente, mas em casos especiais, no caso da opção THIG, este elemento pode estar localizado na rede de um operador visitado por um cliente de outro operador (*roaming*).

### 3.2.1.4. Serving-Call Session Control Function

O S-CSCF é o elemento central do IMS no processamento de sinalização SIP e controlo das sessões multimédia dos utilizadores. Um operador IMS pode conter vários S-CSCFs na sua rede com diferentes funcionalidades e finalidades.

O S-CSCF funciona como um SIP *proxy* com as principais funcionalidades de acordo com a norma 3GPP TS 23.228 [28]:

- Funciona como um SIP *Registrar* de acordo com o RFC 3261 [32]. Isto significa que estabelece uma associação entre o endereço IP do terminal do utilizador com o endereço público SIP desse utilizador que se pretende registar. Para isso, este elemento aceita as mensagens de registo (SIP *Registers*) dos utilizadores e verifica a sua validade através dos vectores de autenticação obtidos do HSS;
- Acede ao HSS para obter informações sobre a subscrição de um determinado cliente IMS. Estas informações incluem os serviços aos quais o utilizador está autorizado a aceder e os *Application Servers* (ASs) que devem ser incluídos;
- Disponibiliza a informação de um determinado cliente aos outros elementos da sua rede durante o período de tempo em que esse cliente se encontra registado neste elemento;
- Controla as sessões multimédia dos utilizadores registados neste elemento e pode impedir o estabelecimento de determinadas sessões para um utilizador com base em determinados critérios subjacentes ao tipo de subscrição ou que podem prejudicar o cliente;
- Funciona como um SIP *proxy* de acordo com o RFC 3261 [32]. Pode aceitar e processar as mensagens SIP ou encaminhá-las para outro elemento;

---

[4] Exemplo: chamadas para o 112.

- Interage com diferentes ASs para fornecer serviços multimédia aos seus utilizadores;
- Gera CDRs com informação relativa às sessões e registos dos utilizadores para efeitos de taxação.

Procedimentos desempenhados pelo S-CSCF no processamento de sessões:

- O S-CSCF recebe uma mensagem SIP pertencente ao estabelecimento de uma sessão, proveniente de um AS ou de um terminal do utilizador registado nesse S-CSCF. Após análise da mensagem, se o destinatário for um cliente de outro operador IMS, o S-CSCF obtém o endereço do I-CSCF dessa rede a partir do domínio do destinatário e encaminha essa mensagem para esse elemento. Caso o destinatário seja um cliente do mesmo operador IMS, essa mensagem é enviada para o I-CSCF alocado nessa rede pelo S-CSCF;
- Se o destinatário da mensagem for um utilizador da rede PSTN ou de outro domínio do tipo comutação de circuitos, o S-CSCF encaminha essa mensagem para o elemento *Breakout Gateway Control Function* (BGCF);
- O S-CSCF encaminha as mensagens SIP para o P-CSCF do utilizador destinatário, esteja este na rede IMS do seu operador ou em situação de *roaming*. O S-CSCF também pode encaminhar as mensagens SIP para um I-CSCF de outro operador IMS no caso do destinatário ser um utilizador em *roaming* nessa rede.

A rede IMS pode conter vários S-CSCFs para efeitos de redundância ou para o caso de ter de servir um elevado número de sessões multimédia simultaneamente. Este elemento está sempre localizado na rede IMS do seu operador.

#### 3.2.1.5. Breakout Gateway Control Function

O BGCF é um dos elementos do IMS que permite a integração entre o domínio IMS e o domínio de comutação de circuitos (rede PSTN/ISDN e *Public Land Mobile Network*-PLMN). Basicamente este elemento é um SIP *server* com funcionalidades de encaminhamento das sessões multimédia para as redes de comutação de circuitos, baseando-se no número telefónico do utilizador destino. O BGCF é utilizado exclusivamente para sessões iniciadas por utilizadores de um operador IMS destinadas a utilizadores das redes PSTN/ISDN ou PLMN, ou entre utilizadores que se encontram em redes PSTN ou PLMN diferentes e que utilizam a rede IMS como intermediária. As

principais funcionalidades e procedimentos do BGCF, de acordo com a norma 3GPP TS 23.228 [28], são:

- Decide em que rede IMS será realizada a interacção com a rede PSTN/PLMN. Se esta interacção for feita na mesma rede IMS, então o BGCF encaminha a mensagem SIP para o *Media Gateway Control Function* (MGCF) apropriado dessa rede, baseado no número telefónico do destinatário. Se for realizada noutra rede IMS, o BGCF encaminha a mensagem SIP para o BGCF da outra rede;
- Gera CDRs com informação relativa às sessões dos utilizadores para efeitos de taxação.

A decisão de qual a rede IMS escolhida para a realização da integração entre os domínios IMS e de comutação de circuitos depende de questões políticas e dos próprios recursos de gestão do operador IMS. Estas decisões não fazem parte do sistema de normalização das redes IMS.

#### 3.2.1.6. Media Gateway Control Function

Como já indicado anteriormente, uma das funções do IMS é permitir o estabelecimento de sessões de voz entre utilizadores do domínio IMS e utilizadores do domínio de comutação de circuitos, como as redes PSTN/ISDN e PLMN. O IMS define um conjunto de elementos que formam o chamado sistema *Media Gateway* de *Trunking*, que em conjunto e com funções específicas permitem esta interacção e a troca de sessões entre utilizadores destes domínios. Os elementos que compõem este sistema são: o MGCF, o IMS-*Media Gateway* (IMS-MGW) e o *Signalling Gateway* (SGW). A Figura 6 ilustra a composição do sistema *Media Gateway* de *Trunking* nos seus elementos, sendo um dos pontos altos do trabalho realizado no âmbito desta Dissertação.

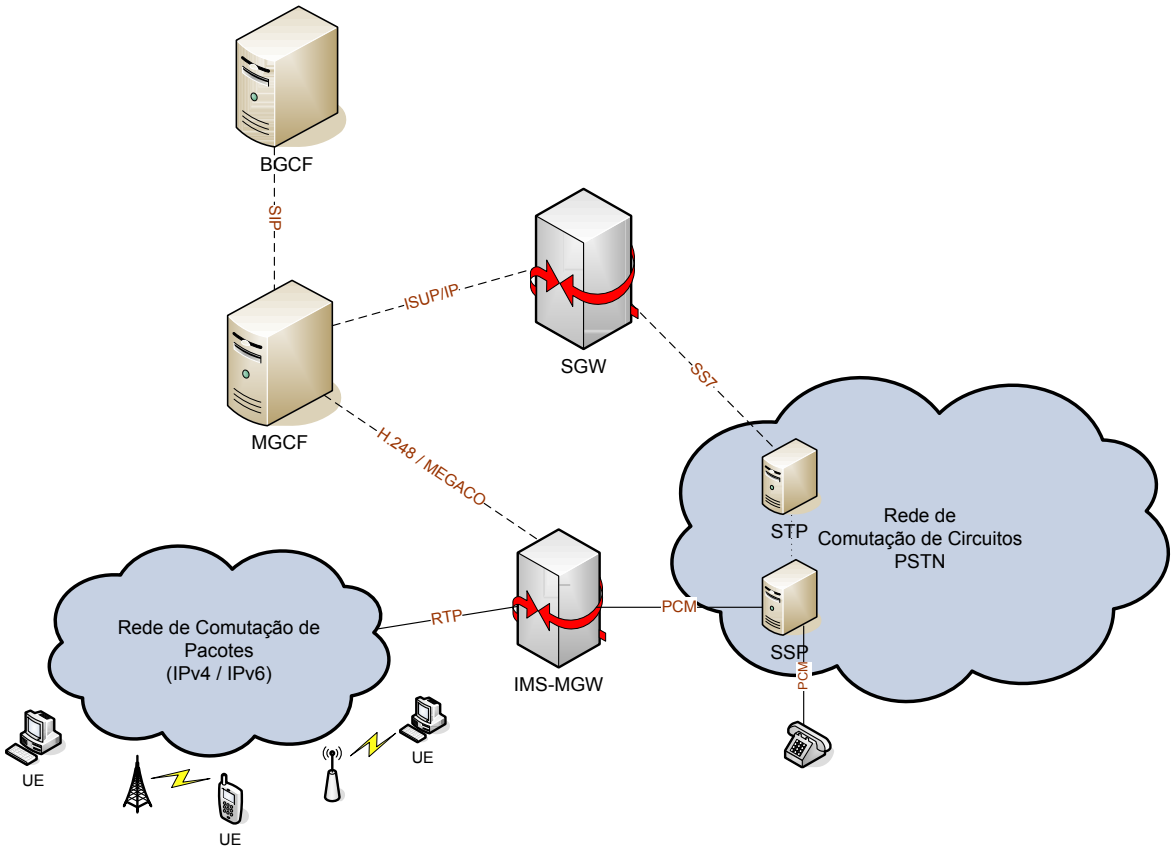



Figura 6- Sistema *Media Gateway* de *Trunking* da arquitectura IMS.

O MGCF é o elemento central do sistema *Media Gateway* de *Trunking*. Este elemento tem um papel fundamental no plano de sinalização e no plano de dados.

Algumas das funcionalidades e procedimentos do MGCF no plano de sinalização são:

- Converter e mapear a sinalização SIP, proveniente do elemento BGCF, em sinalização ISDN *User Part* (ISUP), definido no *International Telecommunication Union – Telecommunications* (ITU-T) *Recommendation* Q.761 [33], ou em *Bearer Independent Call Control* (BICC), definido no ITU-T *Recommendation* Q.1901 [34] e enviá-la sobre IP para o elemento SGW (Figura 6). O ISUP é o mais utilizado para as sessões de voz devido à preferência hoje em dia do Sistema de Sinalização #7 (SS7), definida no ITU-T *Recommendation* Q.700 [35], nas redes PSTN;
- Converter e mapear a sinalização ISUP sobre IP, proveniente do elemento SGW em sinalização SIP e enviá-la para o elemento S-CSCF do IMS.

A Figura 7 ilustra a conversão protocolar desempenhada pelo elemento MGCF.

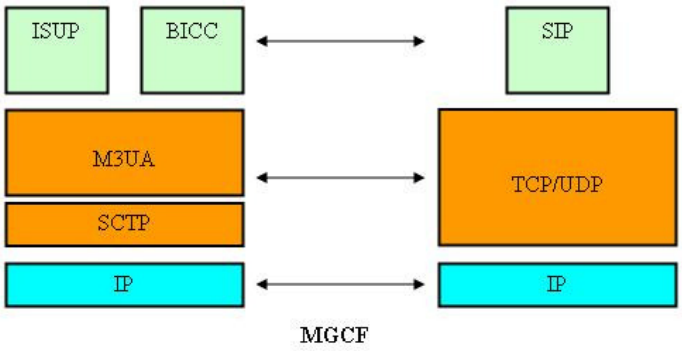



Figura 7- Conversão de sinalização no elemento MGCF.

O grupo de trabalho *Signalling Transport* (SIGTRAN) [36] do IETF definiu um conjunto de protocolos para o transporte da informação ISUP sobre IP, sendo um desses protocolos o *Stream Control Transmission Protocol* (SCTP), documentado no RFC 2960 [37], e o *Message Transfer Part* 3 *User Adaptation layer* (M3UA), documentado no RFC 3332 [38]. Algumas das funcionalidades e procedimentos do MGCF no plano de dados são:

- Controlar os recursos de vários elementos IMS-MGWs da camada lógica de transporte da arquitectura IMS, através do protocolo H.248 especificado no ITU-T *Recommendation* H.248 [39];
- Reservar canais de áudio no IMS-MGW para uma sessão de voz entre utilizadores IMS e PSTN;
- Escolher o *codec* de áudio apropriado no IMS-MGW para uma sessão de voz;
- Rejeitar a componente de vídeo de uma sessão e controlar os recursos do IMS-MGW somente para a componente de áudio;
- Gerar CDRs com informação relativa às sessões dos utilizadores para efeitos de taxação.

#### 3.2.1.7. Signalling Gateway

O elemento SGW, juntamente com o elemento MGCF descrito anteriormente, permite a troca de sinalização necessária ao estabelecimento de sessões de voz entre utilizadores da rede PSTN, onde é utilizada sinalização SS7, e utilizadores da rede IMS, onde é utilizada sinalização SIP. A principal função deste elemento passa pela conversão protocolar da sinalização ao nível do transporte, de forma a que a informação das camadas superiores (ISUP, BICC) possa ser transferida entre domínios IP e PSTN sem sofrer qualquer alteração. Mais precisamente, este elemento converte a camada protocolar *Message Transfer Part* (MTP) 1, especificada no ITU-T *Recommendation* Q.701 [40], da

sinalização SS7 no protocolo SCTP, e as camadas protocolares MTP2 e MTP3, também especificadas no ITU-T *Recommendation* Q.701 [40], no protocolo M3UA [38] com destino ao elemento MGCF. Ou seja, o ISUP ou BICC sobre M3UA/SCTP/IP proveniente do MGCF é transformado no SGW em ISUP ou BICC sobre MTP 3/MTP 2/MTP 1 e vice-versa, como se pode constatar pela Figura 8.

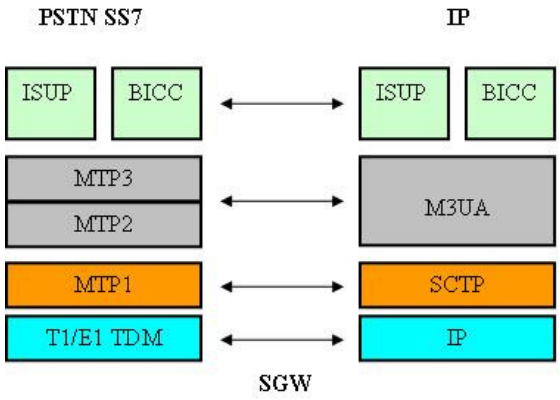



Figura 8- Conversão de sinalização no elemento SGW.

### 3.2.1.8. Multimedia Resource Function Controller

O elemento *Multimedia Resource Function Controller* (MRFC) no plano de sinalização, juntamente com o elemento *Multimedia Resource Function Processor* (MRFP) no plano de dados, permite enviar aos clientes de um operador IMS anúncios provenientes de um servidor multimédia, estabelecer sessões de vídeo e/ou áudio conferência entre vários clientes, reproduzir conteúdos multimédia em tempo-real, etc. Algumas das funcionalidades e procedimentos do elemento MRFC, de acordo com a norma 3GPP TS 23.228 [28], são:

- Controlar os recursos multimédia do elemento MRFP através do protocolo H.248 especificado no ITU-T *Recommendation* H.248 [39];
- Processar as mensagens SIP provenientes dos elementos S-CSCF e AS de forma a controlar convenientemente o MRFP;
- Gerar mensagens SIP e enviá-las para o S-CSCF e para o AS, de acordo com os recursos do elemento MRFP;
- Gerar CDRs com informação relativa às sessões dos utilizadores para efeitos de taxação.

Este elemento está sempre localizado na rede IMS do operador.

### *3.2.2. Camada de Transporte*

A camada de transporte apresenta as diferentes tecnologias de acesso, algumas ilustradas na Figura 5. Os elementos desta camada actuam no plano de dados e possuem diferentes funcionalidades para estes fluxos multimédia trocados entre os utilizadores após o estabelecimento de uma determinada sessão. Entre várias funcionalidades destacam-se a possibilidade de alteração do *codec* em tempo-real do fluxo de áudio e/ou vídeo, caso os utilizadores não possuam um *codec* em comum na comunicação, permitem a transferência de fluxo de dados de áudio e/ou vídeo entre domínios diferentes, através de *Media Gateways*, e controlam os fluxos de conteúdos multimédia fornecidos a determinados clientes IMS.

De seguida é feita uma descrição individual dos elementos que compõem esta camada lógica.

#### 3.2.2.1. Multimedia Resource Function Processor

O elemento MRFP, controlado pelo elemento MRFC já descrito, possui as seguintes funcionalidades e procedimentos de acordo com a norma 3GPP TS 23.228 [28]:

- Juntar os diferentes fluxos de dados provenientes de diferentes utilizadores de uma sessão de áudio/videoconferência;
- Fornecer anúncios multimédia e outros conteúdos semelhantes aos clientes IMS;
- Gerir estes conteúdos multimédia.

#### 3.2.2.2. IP Multimedia Subsystem – Media Gateway

Nos capítulos 3.2.1.6 e 3.2.1.7 foram descritos os elementos MGCF e SGW como peças fundamentais na convergência da sinalização entre os domínios IP e PSTN/PLMN. Estes elementos pertencem ao sistema *Media Gateway* de *Trunking*, ilustrado na Figura 6, juntamente com o elemento IMS-MGW da camada de transporte da arquitectura IMS. De seguida é feita uma descrição deste elemento, o qual representa uma parte do trabalho realizado no âmbito desta Dissertação.

O elemento IMS-MGW situa-se na "fronteira" entre o domínio IP e o domínio PSTN/PLMN e possui as seguintes funcionalidades e procedimentos no plano de dados:

- Conversão entre os dados *Real-time Transport Protocol* (RTP) [41] do domínio IP e os dados *Pulse Code Modulation* (PCM) do domínio PSTN/PLMN;

- Interacção com o elemento MGCF da camada de controlo de sessão para controlo de recursos através do protocolo H.248 especificado em ITU-T *Recommendation* H.248 [39];
- Processamento do áudio (codificação/descodificação, cancelamento do eco, etc.);
- *Transcoding* em situações em que o terminal do utilizador do lado IP não suporta o *codec* utilizado do lado PSTN/PLMN;
- Passagem de eventos (como anúncios, *Dual Tone Multi-Frequency* - DTMF) para o lado PSTN/PLMN e vice-versa;
- Detecção e processamento de sinalização DTMF de acordo com o RFC 2833 [42].

As funcionalidades de conversão e codificação aplicam-se a dados de voz (áudio), dados provenientes de *modems* e de FAX.

#### 3.2.2.3. Camada de Aplicação/Serviço

A camada de aplicação/serviço ilustrada na Figura 5 e na Figura 9 é composta por um conjunto de elementos servidores responsáveis pelo armazenamento, processamento e entrega de serviços aos clientes de um operador IMS. O estabelecimento de uma sessão simples de voz, vídeo, etc. entre dois clientes de um mesmo operador IMS não necessita de recorrer forçosamente aos elementos da camada de aplicação da arquitectura IMS, a não ser que seja necessária a aplicação de um tipo de serviço específico na sessão estabelecida. Entre vários tipos de serviços e aplicações oferecidos por estes elementos destacam-se [43]:

- *Caller ID, Call Waiting, Call Forwarding, Call Transfer, Call hold, Call pickup;*
- *Conference Call;*
- *Voice mail;*
- *Text-to-speech, Speech-to-text;*
- *Push-to-talk (PTT);*
- *Location based services;*
- *Presence, Instant Messaging;*
- *Voice Call Continuity (VCC).*

A Figura 9 mostra que esta camada é composta por três tipos de AS que comunicam directamente com o elemento S-CSCF da camada de controlo de sessão através da interface ISC baseada no protocolo SIP documentado no RFC 3261 [32].

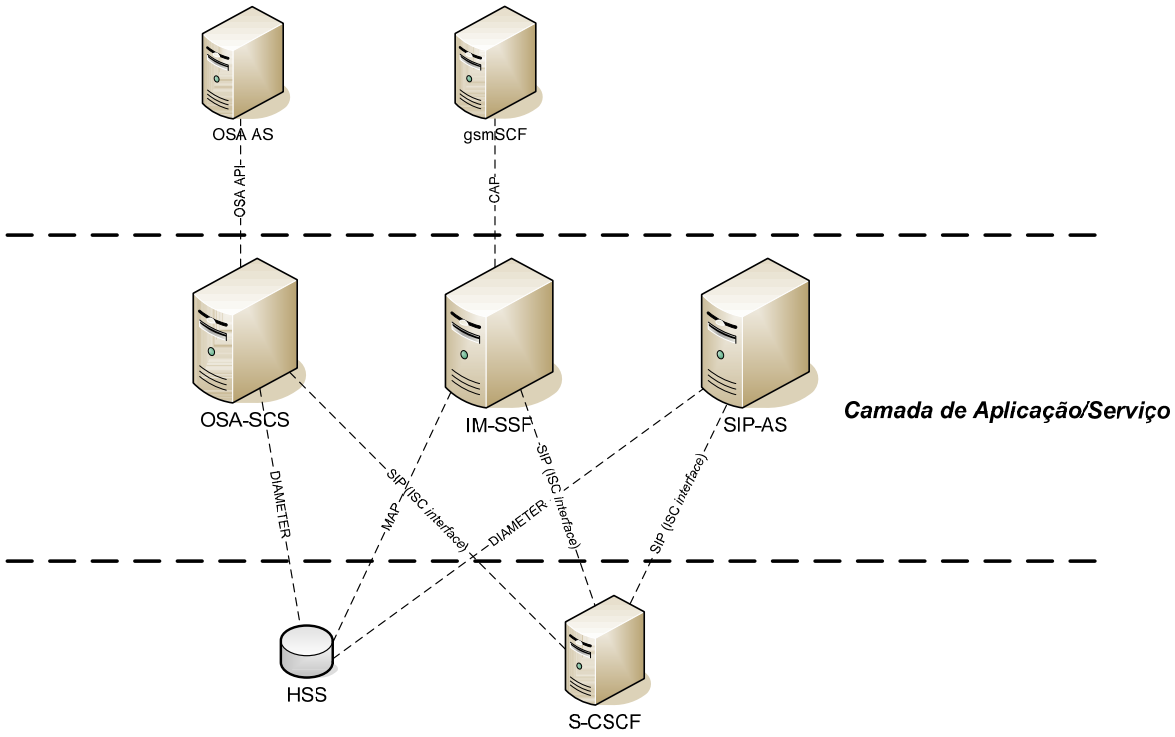



Figura 9- Camada de aplicação/serviço.

Os três AS de um operador IMS, descritos de seguida, podem estar localizados na rede do próprio operador ou na rede de um operador IMS diferente no qual existe um acordo de serviços entre ambos. Caso estejam na rede do próprio operador IMS, estes elementos possuem uma interface opcional com o elemento HSS do operador.

Os três AS possuem funcionalidades diferentes do ponto de vista da camada de serviço ou aplicação, mas para a camada de controlo de sessão são vistos da mesma forma, com o mesmo modo de funcionamento que pode ser de um SIP *Proxy Server*, de um SIP *User Agent*, de um SIP *Redirect* ou de um SIP *Back-to-Back User Agent* (B2BUA), dependendo do tipo de serviço.

### 3.2.2.4. Session Initiation Protocol Application Server

O SIP AS é o *Application Server* nativo ao IMS que armazena e executa serviços multimédia baseados em SIP. Todos os serviços futuros que estão a ser desenvolvidos para o IMS serão implementados usando este tipo de AS. Para além da interface SIP com o elemento S-CSCF do plano de controlo, este elemento pode comunicar, também, com o HSS através do protocolo Diameter [27], caso se encontre na rede IMS do seu operador,

para consultar ou actualizar a informação respeitante à subscrição de serviços de um determinado cliente [25].

#### 3.2.2.5. Open Service Access – Service Capability Server

O *Open Service Access – Service Capability Server* (OSA-SCS) é o elemento da camada de aplicação que funciona como uma interface de segurança entre as aplicações do OSA AS e os elementos da camada de controlo do IMS (Figura 9). O uso deste elemento permite criar níveis de segurança aos operadores IMS, permitindo que AS externos (OSA AS) pertencentes a entidades independentes possam utilizar a rede IMS de um determinado operador para fornecer os seus serviços aos clientes dessa rede, sem que a segurança interna seja comprometida, ou seja, este elemento permite esconder toda a sinalização SIP trocada entre os elementos da camada de controlo do IMS, dos servidores de aplicações externos (OSA AS). O OSA-SCS possui uma interface SIP baseada no RFC 3261 [32] com o elemento S-CSCF e uma interface OSA API (*Application Programming Interface*), especificada em 3GPP TS 29.198 [44], com o servidor de aplicações OSA AS. Este elemento também possui uma interface com o HSS através do protocolo Diameter [27] para consultar ou actualizar a informação respeitante à subscrição de serviços de um determinado cliente.

Mais detalhe sobre as funcionalidades deste elemento encontram-se na norma do 3GPP TS 23.198 [126].

#### 3.2.2.6. IP Multimedia – Service Switching Function

O IP *Multimedia – Service Switching Function* (IM-SSF) é um *Application Server* especializado para a integração e reutilização de aplicações tradicionais, desenvolvidas para a arquitectura GSM, nas redes dos operadores IMS. Estas aplicações designam-se por *Customized Applications for Mobile network Enhanced Logic* (CAMEL). O IM-SSF também permite a um elemento designado por GSM *Service Control Function* (gsmSCF) exterior controlar as sessões multimédia no IMS [25].

Por um lado este elemento funciona como um AS do ponto de vista da interface SIP [32] com o elemento da camada de controlo de sessão S-CSCF; por outro lado funciona como um SCF através da interface com o elemento gsmSCF baseado no protocolo CAMEL *Application Part* (CAP) definido em 3GPP TS 29.278 [45]. Este elemento também possui uma interface com o HSS através do protocolo baseado em *Mobile Application Part* (MAP) especificado pelo 3GPP em 3GPP TS 29.002 [46].

## 3.3. Protocolos

Como já foi referido, os protocolos definidos para a comunicação entre os elementos da arquitectura IMS são derivados dos desenvolvidos para o domínio *Internet*, pela organização IETF, e para o domínio GSM/GPRS, pelas organizações *European Telecommunications Standard Institute* (ETSI) e ITU-T. O 3GPP, no âmbito da normalização de uma arquitectura para o IMS, tirou partido da experiência destas organizações no desenvolvimento de protocolos, para a implementação de extensões e funcionalidades extras aos protocolos, específicas ao IMS [47].

O IMS utiliza uma grande variedade de protocolos com funcionalidades diferentes. Na Figura 10 estão ilustrados os protocolos mais importantes no âmbito desta Dissertação, através do modelo lógico de camadas TCP/IP.

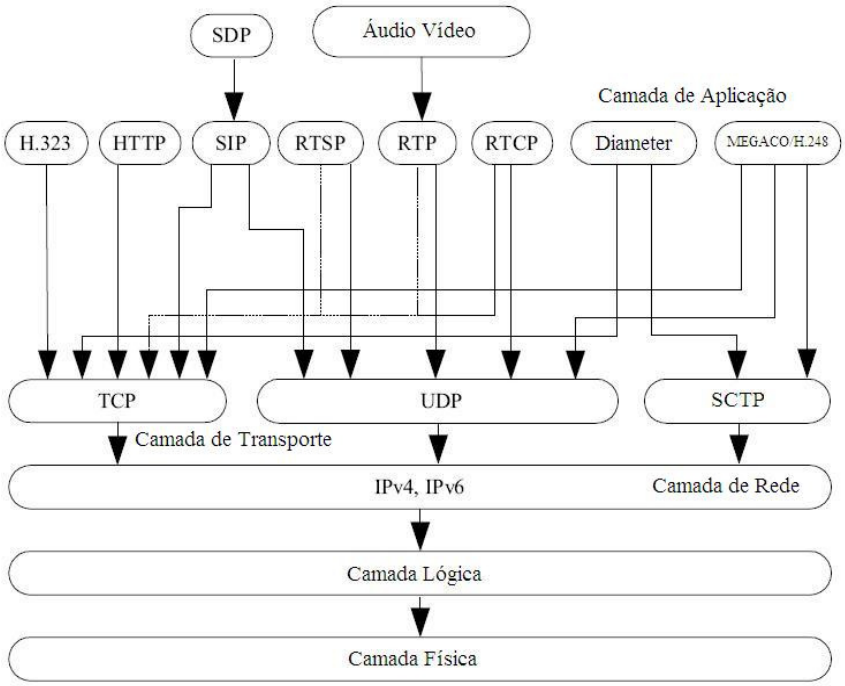



Figura 10- Protocolos da arquitectura IMS.

Estes protocolos podem ser classificados em três categorias diferentes [48]:

- Protocolos do plano de sinalização;
- Protocolos do plano de *Authentication, Authorization* e *Accounting* (AAA);
- Protocolos do plano de dados.

### *3.3.1. Plano de Sinalização*

Um dos protocolos utilizados no plano de sinalização para o controlo de sessões é o SIP especificado pelo IETF no RFC 3261 [32]. SIP é um protocolo baseado em texto (ao contrário dos protocolos BICC [34] e H.323 [49] utilizados também para o controlo de sessões). As principais razões que levaram à escolha do protocolo SIP foram as facilidades de detecção e correcção de erros no protocolo (pois é um protocolo baseado em texto), a sua extensibilidade e as facilidades de criação de novos serviços, sendo um dos requisitos do IMS [47].

Outro protocolo também utilizado no plano de sinalização para o controlo de alguns elementos da camada de transporte da arquitectura IMS (MRFP e IMS-MGW) é o *MEdia GAteway COntrol* (MEGACO)/H.248. Este protocolo foi desenvolvido em conjunto pelas organizações ITU-T, dando a designação ao protocolo de ITU-T *Recommendation* H.248 [39], e IETF, dando a designação de MEGACO [50].

#### 3.3.1.1. Session Initiation Protocol

O SIP é um protocolo da camada de aplicação, segundo o modelo TCP/IP (Figura 10), utilizado para criar, modificar e terminar sessões multimédia com um ou mais participantes em redes baseadas em IP. Este protocolo pode utilizar o *User Datagrama Protocol* (UDP) ou o *Transmission Control Protocol* (TCP) para o seu transporte nas redes IP. Normalmente é utilizado o UDP para evitar o *overhead* associado ao TCP no estabelecimento e terminação da ligação [48].

O SIP é baseado nos protocolos com grande sucesso na *Internet*, como o *Hypertext Transfer Protocol* (HTTP) e *Simple Mail Transfer Protocol* (SMTP), e tal como estes, segue o modelo cliente-servidor. Com o protocolo SIP é possível convidar novos participantes em sessões previamente estabelecidas, modificar alguns parâmetros de uma sessão e finalizar as respectivas sessões [51]. Uma das grandes vantagens deste protocolo é a sua extensibilidade, uma das razões pela sua escolha na arquitectura IMS, que permite aos utilizadores executarem outros tipos de serviços, como *instant messages* e subscrição de eventos, com este protocolo [25]. A base do protocolo SIP está definida pelo IETF no RFC 3261 [32]; as suas extensões estão definidas em outros RFCs que serão indicados quando mencionadas as extensões.

O protocolo SIP define as seguintes entidades elementares necessárias ao estabelecimento das sessões multimédia [52]:

- *User Agent Client* (UAC): terminal do utilizador que pretende iniciar uma sessão;
- *User Agent Server* (UAS): terminal do utilizador destinatário de uma sessão;
- *Registrar*: entidade responsável pelo armazenamento da informação respeitante à localização de um determinado utilizador. Na arquitectura IMS os elemento P-CSCF e S-CSCF possuem esta funcionalidade incorporada;
- *Proxy Server*: entidade responsável pelo encaminhamento das mensagens SIP para o respectivo destinatário. Todos os elementos da camada de controlo da arquitectura IMS possuem esta funcionalidade incorporada;
- *SIP Redirect*: entidade que recebe mensagens SIP para estabelecimento de sessões, mapeia o endereço do destinatário em outros endereços e envia-os para o cliente. Este elemento não funciona como um SIP *proxy*, ou seja, não encaminha as mensagens SIP até ao destinatário.

Para estabelecer e terminar uma sessão entre dois utilizadores UAC e UAS é necessário trocar várias mensagens SIP entre eles. Estas mensagens podem ser agrupadas formando transacções. Uma sessão entre dois utilizadores é geralmente caracterizada por duas transacções, uma que contém a mensagem SIP *Request Invite*, várias SIP *Responses* provisórias e a mensagem SIP *Response* final 200 OK, e outra que contém a mensagem SIP *Request Bye* e a mensagem SIP *Response* 200 OK. Isto significa que uma sessão é caracterizada por uma transacção de estabelecimento e outra de terminação da sessão.

Cada mensagem SIP é composta por uma linha inicial, vários campos e um corpo, seja ela de *Request* ou *Response*. A linha inicial das mensagens SIP *Requests*, também designada por *Resquest line*, contém o nome do método SIP, o SIP *Uniform Resource Identifiers* (URI) do destinatário da mensagem (também designado por *Request*-URI (R-URI)), e a versão do protocolo (SIP/2.0). Em (1) está um exemplo de um *Request line* [25].

*INVITE sip: Alice.Smith@domain.com SIP/2.0* (1)

Neste exemplo o nome do método é *Invite*, ou seja, indica que esta mensagem é utilizada pelo UAC para convidar um utilizador UAS para uma sessão, o R-URI do UAS é *sip: Alice.Smith@domain.com* e indica que o utilizador a que se destina a mensagem é a Alice *Smith*.

O R-URI das mensagens SIP *Request* pode estar no formato SIP URI, como no exemplo anterior, em que o utilizador é identificado por um endereço idêntico ao do *e-mail* ou no formato TEL URI em que o utilizador é identificado com um número telefónico de acordo

com o ITU-T *Recommendation* E.164 [53]. Este tipo de URI é muito utilizado no IMS para sessões com terminais telefónicos convencionais. Em (2) estão indicados alguns exemplos de SIP e TEL URIs.

*sip: Alice.Smith@domain.com*
*sip: bob@domain.pt; transport=tcp*
*sip: Charlie@192.168.15.100:5060* (2)
*tel: +351432332238*

Na Tabela I estão indicados os seis métodos inicialmente definidos para o protocolo SIP.

| Método | Funcionalidade |
|---|---|
| *INVITE* | Pedido de estabelecimento de uma sessão |
| *ACK* | Confirmação que a sessão foi estabelecida |
| *BYE* | Terminação da sessão |
| *CANCEL* | Cancelamento de um pedido de estabelecimento de sessão pendente |
| *OPTIONS* | Pedido sobre as capacidades de um determinado servidor |
| *REGISTER* | Registo de um SIP ou TEL URI no IMS |

Tabela I- Métodos base do protocolo SIP.

Na Tabela II estão indicadas as extensões dos métodos SIP utilizados no IMS.

| Método | Funcionalidade |
|---|---|
| *NOTIFY* | Envia uma notificação ao UA sobre um determinado evento |
| *PRACK* | Confirmação que um SIP *Response* provisório foi recebido |
| *PUBLISH* | Envia informação para um servidor |
| *SUBSCRIBE* | Pedido para ser notificado sobre um determinado evento particular |
| *UPDATE* | Alteração de algumas características da sessão |
| *MESSAGE* | Envio de um *instant message* |
| *REFER* | Pedido a um UA para aceder a um URI ou URL com fim a estabelecer uma sessão |
| *INFO* | Usado para o transporte de sinalização PSTN/ISDN |

Tabela II- Métodos adicionais (extensões) ao protocolo SIP.

De igual modo às mensagens SIP *Request*, as mensagens SIP *Response* também possuem uma linha inicial designada por *Status Line*. Esta linha é composta por uma indicação da versão do protocolo (SIP/2.0), e por um *Status* da transacção indicado através de um código numérico e do seu significado para o utilizador. Em (3) está um exemplo de um *Status Line* [25].

*SIP/2.0 180 Ringing* (3)

Neste exemplo o *Status* da transacção é dado através do código numérico 180 que corresponde a *Ringing*, ou seja, isto significa que o utilizador UAS é alertado para o estabelecimento de uma sessão iniciada pelo UAC.

A Tabela III mostra como estas mensagens são divididas em classes de acordo com o *Status* da mensagem.

| Gama do *Status* | Nome da classe | Descrição |
|---|---|---|
| 100 – 199 | *Provisional* | SIP *Request* recebido pelo UAS, continuação do processo de estabelecimento da sessão |
| 200 – 299 | *Success* | SIP *Request* aceite e processado |
| 300 – 399 | *Redirection* | Retorno de outros endereços de localização do destinatário após a recepção de um SIP *Request* |
| 400 – 499 | *Client Error* | Erro na mensagem SIP *Request* |
| 500 – 599 | *Server Error* | Erro no servidor ao tentar processar uma mensagem SIP *Request* aparentemente correcta |
| 600 – 699 | *Global Failure* | SIP *Request* não processado devido a uma falha não especificada |

Tabela III- Classes de mensagens SIP *Response*.

Todas as mensagens SIP, a seguir à linha inicial, possuem vários campos. Estes campos são formados por um nome, seguido de dois pontos e um valor referente ao campo. Alguns destes campos são de carácter obrigatório em todas as mensagens SIP para o correcto funcionamento do processo de estabelecimento e terminação da sessão [52]. Alguns campos das mensagens SIP estão indicados na Tabela IV.

| Campo | Conteúdo (valor) |
|---|---|
| *To* (obrigatório) | SIP ou TEL URI do destinatário (UAS) |
| *From* (obrigatório) | SIP ou TEL URI do emissor (UAC) |
| *Cseq* (obrigatório) | Número de sequência para sincronização entre os SIP *Request* e os respectivos SIP *Response* |
| *Call-ID* (obrigatório) | Identificação da sessão ao qual a mensagem pertence |
| *Max-Forwards* (obrigatório) | Número máximo de saltos até ao destino para evitar *loops* eternos |
| *Via* (obrigatório) | Endereço dos SIP *proxies* atravessados por uma mensagem SIP *Request*. Utilizado para que as respectivas mensagens SIP *Response* façam o mesmo percurso no sentido inverso |

| | |
|---|---|
| *Contact* (opcional) | SIP ou TEL URI do emissor da mensagem |
| *Record-Route* (opcional) | Endereço dos SIP *proxies* atravessados por uma mensagem SIP *Request* que devem ser atravessados pelas mensagens SIP de sessões futuras. Assegura que certos SIP *proxies* pertencem sempre ao percurso da sinalização para qualquer sessão |
| *Route* (opcional) | Endereço dos SIP *proxies* indicados no campo *Record-Route*. Utilizado para encaminhar as mensagens SIP pelos SIP *proxies* correctos |
| *Supported* (opcional) | Extensões SIP suportadas pelo emissor da mensagem que não estão no campo *Require*. Utilizado na negociação de extensões SIP numa sessão IMS |
| *Require* (opcional) | Extensões SIP pretendidas pelo emissor da mensagem para uma determinada sessão. Utilizado na negociação de extensões SIP numa sessão IMS |
| *Unsupported* (opcional) | Extensões SIP não suportadas pelo emissor da mensagem mas que foram pedidas pelo receptor. Utilizado na negociação de extensões SIP numa sessão IMS |
| *Allow* (opcional) | Nome dos métodos SIP que o emissor da mensagem suporta |
| *Content-Type* (opcional) | Natureza do conteúdo existente no corpo da mensagem (SDP, etc.) |
| *Content-Length* (opcional) | Comprimento da corpo da mensagem |

Tabela IV- Campos das mensagens SIP.

Geralmente o corpo da mensagem SIP é composto por uma descrição dos parâmetros multimédia a utilizar na sessão em questão, num formato de acordo com o *Session Description Protocol* (SDP) definido pelo IETF no RFC 2327 [54]. Este protocolo define um conjunto de campos, alguns indicados na Tabela V, utilizados para a descrição dos parâmetros multimédia que o emissor da mensagem, onde se encontra o SDP, pretende negociar para esta sessão.

| **Campo** | **Conteúdo (valor)** |
|---|---|
| *v* | Versão do protocolo |
| *o* | Identificação do criador da sessão e identificação da sessão |
| *s* | Nome da sessão |
| *t* | Tempo que a sessão está activa |
| *m* | Descrição do *stream* (tipo de *stream*, *codec*, porto de escuta, etc.) |
| *c* | Informação de comunicação (endereço IP, etc.) |
| *a* | Linha de atributos (*sendrecv*, *sendonly*) |

Tabela V- Campos do protocolo SDP.

A descrição SDP pode ser dividida em duas partes. A primeira parte corresponde à informação do emissor do SDP necessária para a sessão. Desta informação destaca-se um nome para a sessão (s = *line*), a identificação do emissor do SDP (o = *line*), a versão do protocolo SDP (v = *line*), o endereço IP do emissor (c = *line*) e o tempo da sessão pretendido (t = *line*). A segunda parte corresponde à informação multimédia, ou seja, é indicado o tipo de sessão (áudio, vídeo, etc.), o *codec* utilizado para cada um, o protocolo de transporte utilizado (RTP) e o porto onde o emissor receberá o *stream* multimédia enviado pela outra entidade no qual pretende estabelecer a sessão. Esta informação é inserida no campo m = *line*.

Para que o UAC e o UAS estejam de acordo no plano multimédia para uma determinada sessão, estes enviam e negoceiam os parâmetros indicados nos seus SDPs de acordo com o modelo oferta/resposta especificado no RFC 3264 [55]. Basicamente, o UAC envia o seu SDP (oferta) para o UAS, e este por sua vez, baseando-se no SDP do UAC, envia um SDP (resposta) para o UAC [52].

Em (4) está um exemplo de uma mensagem SIP *Request*.

```
INVITE sip:bob@domain.pt SIP/2.0
To: "Bob" <sip:bob@domain.pt>
From: "Alice" <sip:alice@domain1.pt>
Via: SIP/2.0/UDP pc123@domain1.pt:5060;branch=z9hG4bj54d
Max-Forwards: 70
Call-ID: adj3n4324jndfkw3@192.168.15.100
CSeq: 1 INVITE
Contact: <sip:alice@192.168.15.100>                    (4)
Content-Type: application/sdp
Content-Length: 153
v=0
o=alice 2554124111 2554523214 IN IP4 192.168.15.100
s=This is a SIP session.
c=IN IP4 192.168.15.100
t=0 0
m=audio 10000 RTP/AVP 0
a=sendrecv
```

Esta mensagem SIP *Request* é um *Invite* do utilizador (UAC) *Alice* para o utilizador (UAS) *Bob*. A linha inicial e os campos seguintes fornecem informação necessária aos SIP *proxies*

para o encaminhamento da mensagem até ao UAS e informação adicional para a identificação do diálogo SIP ao qual a mensagem pertence. O corpo da mensagem possui um SDP para informar ao *Bob* que a *Alice* está disponível no endereço IP 192.168.15.100 e que pretende estabelecer uma sessão de áudio com ele no porto RTP 10000, utilizando para isso o *codec* 0 (corresponde ao *codec* G.711 *μ-law*). A linha de atributo (a = *line*) indica que o *stream* de áudio deve ser bidireccional.

Se o *Bob* estiver de acordo com esta descrição multimédia enviada pela *Alice* para esta sessão, então este envia um SIP *Response* com um SDP idêntico [52].

#### 3.3.1.2. Media Gateway Control Protocol/H.248

O protocolo de controlo MEGACO/H.248 pertencente à camada lógica de aplicação segundo o modelo TCP/IP da Figura 10, e possui uma arquitectura de controlo diferente do adoptado pelo SIP. O SIP segue o modelo de controlo ponto-a-ponto, em que todas as entidades são tratadas ao mesmo nível em termos de funcionalidades. O MEGACO/H.248 segue o modelo de controlo *master-slave* baseado numa arquitectura composta por um elemento *master*, designado por *Media Gateway Controler* (MGC) ou *Call Agent*, que possui as principais funcionalidades, ou seja possui a "inteligência", e que envia comandos de controlo para outro elemento (*slave*). Na arquitectura IMS, ilustrada na Figura 5, os elementos *master* são o MGCF e o MRFC da camada de controlo de sessão que enviam comandos de controlo MEGACO/H.248 para os elementos IMS-MGW e MRFP respectivamente (*slaves*).

Este protocolo define dois elementos necessários para o controlo de ligações subjacentes a sessões multimédia que se pretendam criar, modificar ou terminar. Estes dois elementos definidos pela arquitectura do protocolo são designados por Terminações e Contextos.

As Terminações são elementos do *slave* responsáveis pelo envio e recepção de fluxos de dados multimédia. Estas Terminações podem ser físicas, tomando o exemplo de uma interface física analógica de um IMS-MGW ligado a um telefone convencional, ou efémeras, tomando o exemplo de uma interface IP do IMS-MGW responsável pelo envio e recepção de fluxo multimédia RTP. Cada Terminação possui uma identificação única dentro do *slave*. Existe um tipo de Terminação que não corresponde a nenhuma interface específica do slave. Esta Terminação é identificada por *Root* e é utilizada quando se pretende englobar todo o *slave* numa única Terminação.

Os Contextos são associações de Terminações dentro um *slave*. À semelhança das Terminações, cada Contexto possui uma identificação única dentro do *slave*. Tomando o exemplo de um IMS-MGW que possui Terminações físicas analógicas, quando um utilizador IP pretende estabelecer uma sessão/ligação com um terminal analógico do IMS-MGW é criado neste elemento um Contexto novo que associa a Terminação física desse terminal analógico a uma nova Terminação efémera do IMS-MGW para a troca de dados multimédia com o utilizador IP. Todas as Terminações isoladas, ou seja, que não estão associadas a nenhuma outra Terminação, pertencem a um Contexto específico identificado por *Null Context*.

Vários comandos de controlo MEGACO/H.248 enviados do *master* para o *slave* podem ser agrupados e executados em sequência por este último, dando origem a uma Transacção no âmbito da arquitectura definida para este protocolo. Estas Transacções também podem ser agregadas em Mensagens.

Na Tabela VI [56] apresentam-se os comandos existentes para o protocolo MEGACO/H.248, bem como uma breve descrição para cada um deles.

| Comando | Descrição |
|---|---|
| *Add* | Associa/adiciona uma Terminação a um Contexto para o estabelecimento de uma sessão. Se for a primeira Terminação a ser adicionada a um Contexto, então este comando é usado para criar o Contexto |
| *Modify* | Altera certas propriedades, eventos e sinais subjacentes a uma determinada Terminação |
| *Subtract* | Remove uma Terminação de um determinado Contexto. Usado quando se pretende terminar uma sessão em que a Terminação está envolvida. Se for a última Terminação do Contexto, então o Contexto é removido |
| *Move* | Move uma Terminação de um determinado Contexto para outro |
| *AuditValue* | Retorna os valores actuais das propriedades, dos eventos, das sinalizações e de estatísticas associados a uma determinada Terminação |
| *AuditCapabilities* | Retorna todos os valores possíveis para as propriedades, eventos e sinalizações de uma determinada Terminação |
| *Notify* | Usado pelo *slave* para notificar o *master* da ocorrência de algum evento |
| *ServiceChange* | Usado pelo *slave* para notificar o *master* que uma Terminação ou conjunto de Terminações vai ou vão estar fora de serviço ou que voltaram ao estado operacional. Usado para notificar o *master* que o *slave* se encontra em estado operacional e pronto para processar comandos |

Tabela VI- Comandos MEGACO/H.248.

Todos este comandos são enviados do *master* para o *slave*, à excepção do *ServiceChange* que pode ser enviado também pelo *slave* e do *Notify* que é sempre enviado do *slave* para o *master* [56].

Os comandos indicados, bem como as respostas enviadas a estes comandos, são acompanhadas por parâmetros contendo informação adicional acerca de algumas propriedades das Terminações ou das sessões. Estes parâmetros são designados por Descritores. Na Tabela VII [57] estão indicados alguns Descritores mais comuns dos comandos e respostas MEGACO/H.248.

| **Descritores** | | | **Descrição** |
|---|---|---|---|
| *Multiplex Descriptor* | | | Especifica as associações existentes entre fluxos multimédia |
| *Media Descriptor* | *Termination State Descriptor* | | Reporta o estado de uma determinada Terminação (em serviço, fora de serviço) |
| | *Stream Descriptor* | *Local Control Descriptor* | Tem as seguintes propriedades:<br>*Mode: sendonly, receiveonly, sendreceive, incative, loopback*<br>*ReserveGroup* e *ReserveValue* – indicam os recursos a serem reservados |
| | | *Local Descriptor* | Parâmetros multimédia da Terminação local e remota a utilizar para o estabelecimento de uma sessão. Estrutura idêntica ao SDP indicado para o SIP (Tabela V) |
| | | *Remote Descriptor* | |
| *Events Descriptor* | | | Lista de eventos que um *slave* deve detectar e reportar para o *master*: *off-hook, on-hook, fax tone, DTMF tones*, etc |
| *Signals Descriptor* | | | Lista de sinais que uma Terminação deve aplicar: sinal/som de chamada, sinal/som de ocupado, sinal/som de alerta, etc |
| *ServiceChange Descriptor* | | | Usado juntamente com o comando *ServiceChange*. Indica o tipo de alteração:<br>*Graceful* – remoção de Terminações sem interromper as ligações<br>*Forced* – remoção abrupta<br>*Restart* – após um atraso<br>*Disconnected* – aplicado ao *slave*<br>*Handoff* – do *master* antigo para um novo *master* |
| *DigitMap Descriptor* | | | Indica um plano de marcação (*dial plan*) válido para o *slave*. No caso do *slave* ser um IMS-MGW, permite que este consiga detectar se um determinado número marcado está completo e se possui digítos válidos |
| *Statistics Descriptor* | | | Informação estatística acerca de uma Terminação. Usado na resposta a um comando *Subtract* e *AuditValue* |
| *Topology Descriptor* | | | Indica como funcionam os fluxos multimédia dentro de um |

| | |
|---|---|
| | Contexto. Usado para a implementação de serviços como por exemplo chamadas em espera |
| *Error Descriptor* | Indicação erro/falha. Retornado na resposta a um comando que não foi bem executado |

Tabela VII- Descritores dos comandos MEGACO/H.248.

As propriedades, sinais, eventos e estatísticas a aplicar a diferentes Terminações podem ser agrupados em pacotes específicos, designados por *Packages*. O IETF e o ITU-T definiram inicialmente para o MEGACO/H.248 um conjunto de *Packages* essenciais que possuem um conjunto de características a aplicar às Terminações que servem de base para o estabelecimento de sessões multimédia. Recentemente o ETSI, no âmbito da normalização das Redes de Próxima Geração (RPGs), tem definido com o ITU-T um conjunto de *Packages* opcionais (extensões) para a execução de certos serviços específicos nestas redes.

## 3.3.2. Plano de Autenticação, Autorização e Accounting

A operação de *Authentication, Authorization* e *Accounting* (AAA) realizada pelos operadores de telecomunicações é fundamental, especialmente em ambientes IMS. É muito importante para os operadores de telecomunicações possuírem mecanismos que efectuem a autenticação de utilizadores, possíveis clientes, nas suas redes, que autorizem, aos seus clientes, o acesso a determinados recursos e serviços no qual estão subscritos (autorizados) e que estes serviços e recursos sejam taxados de forma correcta.

A arquitectura IMS utiliza o protocolo Diameter, definido no RFC 3588 [27], para executar estas tarefas.

### 3.3.2.1. Diameter

O protocolo Diameter é uma evolução do antigo protocolo Radius definido no RFC 2865 [58]. Consiste numa base protocolar para o desenvolvimento de diferentes aplicações Diameter, customizadas para uma tarefa particular. O IMS utiliza estas aplicações para o acesso ou modificação da informação relativa aos seus clientes, através da interface com os elementos SLF e HSS (Figura 5). Estas interfaces não utilizam a mesma aplicação Diameter para a operação de AAA. Geralmente, a aplicação para o *Accouting* é diferente da aplicação para realizar a autorização de clientes [47].

### 3.3.3. Plano de dados

Os protocolos do plano de dados permitem o fluxo de dados multimédia (áudio e vídeo) entre utilizadores IMS.

Os sinais de áudio e vídeo antes de serem enviados para o destinatário são codificados, e posteriormente descodificados, através de algoritmos específicos de codificação/descodificação usualmente designados por *codecs*. O IMS lista um conjunto abrangente de *codecs*, sendo a maior parte deles normalizados pelo ITU-T, que podem ser utilizados na codificação/descodificação de áudio e vídeo nas suas redes. Alguns destes *codecs* são de carácter obrigatório na normalização do IMS.

Após codificados os dados, estes são encapsulados em pacotes RTP e enviados para o destinatário que irá descodificá-los utilizando o mesmo *codec*.

O RTP, definido pelo IETF e descrito no RFC 3550 [41], é o protocolo utilizado para o transporte de dados multimédia entre clientes IMS. Este protocolo juntamente com o *Real-time Transport Control Protocol* (RTCP), também definido no RFC 3550 [41], permite criar fluxos multimédia entre utilizadores com funcionalidades de QoS.

De seguida é feita uma descrição do protocolo RTP e dos *codecs* utilizados nas redes IMS para o áudio e vídeo.

#### 3.3.3.1. Real-time Transport Protocol

O protocolo RTP é um protocolo da camada de aplicação, segundo o modelo lógico de camadas TCP/IP da Figura 10, utilizado para o transporte de informação multimédia em tempo real (áudio e vídeo) entre utilizadores do domínio IP. Os pacotes RTP podem ser enviados sobre UDP ou TCP (Figura 10), sendo o protocolo UDP preferível e mais utilizado pelas aplicações multimédia que utilizam o RTP, pois este protocolo é menos sensível a perdas de pacotes relativamente aos atrasos sentidos nas redes. Inicialmente foi especificado pelo IETF como um protocolo para serviços *multicast*, mas actualmente tem sido utilizado em *unicast*. É utilizado em vários serviços de *streaming* de áudio e/ou vídeo, na arquitectura IMS.

Como os pacotes RTP são enviados sobre o domínio IP, poderão existir situações em que os pacotes cheguem ao utilizador destino com atrasos constantes, mas também poderão existir situações frequentes em que dois pacotes enviados consecutivamente, o segundo poderá chegar antes ou ao mesmo tempo que o primeiro pacote enviado, ou seja, existe variações de atraso na rede (*jitter*), o que torna impossível de prever se os pacotes chegam

na mesma ordem que foram enviados. Para resolver este problema e para que o receptor consiga reproduzir a informação multimédia sequencialmente, o emissor coloca nos pacotes RTP indicadores temporais (*timestamps*). O receptor ao receber estes pacotes coloca-os numa fila de espera por ordem de *timestamps* e começa a reproduzir a informação multimédia [48]. Se um pacote RTP com um determinado *timestamp* precisa de ser reproduzido e ainda não chegou ao destino, então são utilizadas técnicas de interpolação para preencher a falha[5].

Os pacotes RTP também são marcados com identificações numéricas em sequências para determinar no receptor quantos pacotes foram perdidos na rede durante a sua transmissão. Se o número de pacotes perdidos durante um período de tempo for muito grande de forma a comprometer a qualidade do serviço, então os utilizadores intervenientes podem decidir utilizar outro *codec* que forneça melhor qualidade em ambientes com grande perda de pacotes (*codecs* com maior redundância) [25].

Os pacotes RTP possuem também uma identificação do utilizador que enviou o pacote e uma identificação do tipo de conteúdo que transportam (*payload type*). A identificação do utilizador é útil em serviços multimédia de vídeo e/ou áudio conferência para identificar o utilizador que de momento está em conversação. A identificação do tipo de conteúdo transportado no pacote RTP (*payload type*) é feita através de códigos numéricos que identificam os *codecs* utilizados para o transporte dos dados e que geralmente são negociados no momento de estabelecimento de uma sessão multimédia através do protocolo SDP [25], já abordado no capítulo 3.3.1.1. A Tabela VIII e a Tabela IX indicam alguns *codecs* de áudio e vídeo respectivamente que podem ser utilizados em sessões entre clientes IMS. O 3GPP, no âmbito da normalização do IMS, alega que alguns destes *codecs* devem ser suportados obrigatoriamente pelos terminais dos utilizadores para comunicarem entre si. Nas tabelas também estão indicadas algumas características específicas dos *codecs*, importantes para a sua escolha consoante as condições do cenário de aplicação.

| ***Codec*** | ***Payload Type Code*** | **Largura de banda (kbps)** | **Descrição** |
|---|---|---|---|
| *G.711 A-law e μ-law* [59] | 8 (*A-law*)<br>0 (*μ-law*) | 64 | Excelente qualidade de voz. Equiparado aos sistemas PSTN/ISDN. Utilizado em redes com grande largura de banda ou com pouco tráfego. |
| *AMR* [60] | | 12,2; 10,2; 7,95; | *Codec* desenvolvido pelo 3GPP para os terminais |

[5] No caso de áudio, o último pacote é reproduzido durante mais tempo.

| | | | |
|---|---|---|---|
| | | 7,40; 6,70; 5,90; 5,15; 7,75 | IMS. Qualidade de voz razoável. Grande complexidade de codificação. |
| *AMR-WB* [61] | | 23,85; 23,05; 19,85; 18,25; 15,85; 14,25; 12,65; 8,85; 6,60 | Utilizado em serviços de voz que requerem grande largura de banda. |
| *G.726* [62] | 99, 2, 98, 97 | 40; 32; 24; 16 | Muito boa qualidade de voz. |
| *GSM-FR* [63] | 3 | 13 | *Codec* utilizado pelos terminais móveis GSM. Aplicado em sessões entre utilizadores GSM e IP. |
| *G.723.1* [64] | 4, 80 | 6,3; 5,3 | Boa qualidade de voz, mas implica técnicas de codificação mais complexas. Óptimo em cenários de pouca largura de banda ou com elevado tráfego. |
| *G.729* [65] | 18 | 8 | Boa qualidade de voz, mas implica técnicas de codificação mais complexas. |

Tabela VIII- *Codecs* de áudio utilizados em sessões IMS.

| *Codec* | Largura de banda (kbps) | Descrição |
|---|---|---|
| *H.261* [66] | 64 – 1984 (em múltiplos de 64) | Utilizado em videoconferência em redes PSTN/ISDN. |
| *H.263* [67] | | Boa qualidade de vídeo em redes com baixa largura de banda ou com elevado tráfego. |

Tabela IX- *Codecs* de vídeo utilizados em sessões IMS.

#### 3.3.3.2. Real-time Transport Control Protocol

O protocolo de controlo RTCP é sempre utilizado em conjunto com o protocolo RTP. Os seus pacotes são enviados periodicamente entre os intervenientes de uma sessão para efeitos de monitoria dos parâmetros de QoS e sincronização dos fluxos multimédia.

A perda de pacotes, para a estatística de QoS, pode ser determinada através do número de pacotes RTP enviados pelo emissor e reportado por este através do protocolo RTCP, e pelo número de pacotes RTP recebidos pelo receptor, reportado por este através do RTCP. Outros parâmetros de QoS, como o *jitter* e atraso na rede, podem ser determinados através da informação transportada nos pacotes RTCP.

Para o sincronismo de fluxos multimédia, os emissores de fluxos RTP utilizam o RTCP para o envio de informação de mapeamento entre os *timestamps* dos seus pacotes RTP com um relógio global de referência. Com esta informação os receptores podem sincronizar diferentes fluxos multimédia do mesmo emissor para que possam ser reproduzidos

simultaneamente e de forma coerente, como por exemplo, os fluxo de áudio e vídeo de uma sessão de videoconferência.

## 3.4. Sumário

Actualmente o IMS é especificado como uma arquitectura de controlo central das RPGs que permite o estabelecimento de sessões multimédia entre utilizadores de redes com diferentes tipos de tecnologia: pacotes (WLAN, xDSL, WiMax, etc.) e circuitos (PSTN, ISDN, etc.), para além das redes móveis. A *release* 7 do 3GPP especifica o *core* IMS como um sistema independente da tecnologia de acesso, permitindo a outras organizações normalizar uma arquitectura de convergência de várias redes de acesso utilizando o *core* IMS como elemento central.

Os principais requisitos impostos pelo 3GPP para arquitectura IMS são:

- Estabelecimento de diferentes tipos de sessões multimédia entre os utilizadores;
- Sessões e serviços com garantia QoS;
- Acesso independente da tecnologia da rede;
- *Roaming*;
- Controlo e imposição de políticas por parte dos operadores sobre os serviços fornecidos aos clientes IMS;
- Possibilidade de implementação de serviços por entidades externas e independentes à arquitectura IMS.

A arquitectura IMS está dividida logicamente em três camadas funcionais de acordo com os elementos que a compõe e as suas funções para com a arquitectura. Estas camadas são de controlo de sessão, de transporte e de aplicação/serviço.

O SIP é um protocolo da camada de aplicação utilizado para criar, modificar e terminar sessões multimédia com um ou mais participantes em redes baseadas em IP. O corpo da mensagem SIP é composto por uma descrição dos parâmetros multimédia a utilizar na sessão em questão, num formato de acordo com o protocolo SDP. O SIP segue o modelo de controlo ponto-a-ponto, em que todas as entidades são tratadas ao mesmo nível em termos de funcionalidades. O MEGACO/H.248 segue o modelo de controlo *master-slave*. O *slave* possui Terminações e Contextos, recursos que são controlados pelo *master*. Os Contextos são associações de Terminações dentro um *slave*.

A arquitectura IMS utiliza o protocolo Diameter para a operação de Autenticação, Autorização e Taxação.

O RTP, definido pelo IETF, é o protocolo utilizado para o transporte de dados multimédia entre clientes IMS. Este protocolo juntamente com o RTCP, permite criar fluxos multimédia entre utilizadores com garantias de QoS.

# Capitulo 4: TISPAN Redes de Próxima Geração

O *Telecommuncations and Internet converged Services and Protocols for Advanced Networking* (TISPAN) [20] é o grupo de trabalho do *European Telecommunications Standard Institute* (ETSI) [12] responsável pela normalização de uma rede futura que permite a convergência de diferentes serviços e tecnologias de acesso no mesmo domínio IP. Estas redes são designadas por Redes de Próxima Geração (RPGs) e o papel do TISPAN é normalizar um conjunto de aspectos subjacentes a estas redes que permitem a integração de serviços de diferentes tecnologias de suporte de uma forma homogénea, utilizando o domínio IP como o suporte de convergência. Entre vários aspectos destacam-se a normalização de uma arquitectura funcional de referência para os operadores, definição dos protocolos a utilizar entre os diferentes elementos da arquitectura, definição dos parâmetros de Qualidade de Serviço (QoS) e definição de níveis de segurança e mobilidade. Esta arquitectura global utiliza o *core* IP *Multimedia Subsystem* (IMS) normalizado pelo 3rd *Generation Partnership Project* (3GPP) [9] como a arquitectura base para a convergência. Apesar das primeiras *releases*[6] do 3GPP definirem a arquitectura IMS só para a convergência das redes móveis, um dos requisitos indicado por esta organização para o IMS é o acesso independente, e é neste campo que o TISPAN entra juntamente com o 3GPP em normalizações futuras[7] para a criação de uma arquitectura global que permite, também, o acesso das redes fixas, para além das redes móveis, ao *core* IMS do 3GPP.

A *release* 1 definiu uma arquitectura extensível para as RPGs com principal foco na convergência das redes fixas de acesso *Digital Subscriber Line* (DSL) ao *core* IMS, que permite aos operadores e fabricantes a implementação da primeira geração de RPGs como base para futuros desenvolvimentos e serviços.

---

[6] *release* 5 e 6.
[7] *release* 7 e 8 do 3GPP e *release* 1 e 2 do TISPAN.

A *release* 2 pretende normalizar a rede inicial para o suporte de novos serviços, como por exemplo o IPTV, e a sua entrega de forma segura ao cliente.

A *release* 3 introduzirá o conceito de nomadismo total entre diferentes domínios e o acesso de redes de grande largura de banda[8].

A arquitectura para as RPGs definida na *release* 1 do TISPAN está de acordo com o modelo de referência conceptual indicado pelo *International Telecommunication Union – Telecommunications* (ITU-T) para estas redes [68]. A estrutura desta arquitectura é composta por duas camadas, uma de serviço e outra de transporte IP, como se pode constatar pela Figura 11.

A camada de serviço é composta por vários subsistemas, sendo o IMS um dos mais importantes desta camada e a base para a evolução desta arquitectura. Para além do *core* IMS, outros subsistemas podem fazer parte desta camada lógica:

- Subsistema para emulação de serviços *Integrated Services Digital Network*/*Public Switched Telephone Network* (ISDN/PSTN);
- Subsistema para *streaming*;
- Subsistema para *broadcast*.

Outros elementos funcionais foram adicionados a esta arquitectura pelo TISPAN e são comuns a todos os subsistemas da camada de serviço, pois permitem desempenhar funções gerais na rede como o acesso a aplicações multimédia, taxação de serviços e gestão da informação dos clientes para todos os subsistemas. Esta arquitectura baseada em subsistemas possibilita, em normalizações futuras, a adição de novos subsistemas ao longo do tempo de forma a contemplar novas solicitações e classes de serviço exigidas pelo mercado.

A ligação IP entre o terminal do utilizador/cliente com as RPGs para a troca de dados multimedia é feita pela camada lógica de transporte sob o controlo dos elementos funcionais normalizados pelo TISPAN nesta arquitectura que são o *Network Attachment Subsystem* (NASS) e o *Resource and Admission Control Subsystem* (RACS), como se pode constatar pela Figura 11. A principal função destes elementos é esconder a tecnologia de transporte das redes de acesso aos elementos da camada de serviço, para que estes possam processar os serviços de forma homogénea independentemente do tipo de rede de acesso [69].

---

[8] Exemplo: *Very-high-bit-rate Digital Subscriber Line* (VDSL), *Worldwide Interoperability Access* (WiMax), etc.

De seguida é feita uma descrição dos principais elementos pertencentes a cada uma das camadas lógicas definidas para esta arquitectura.

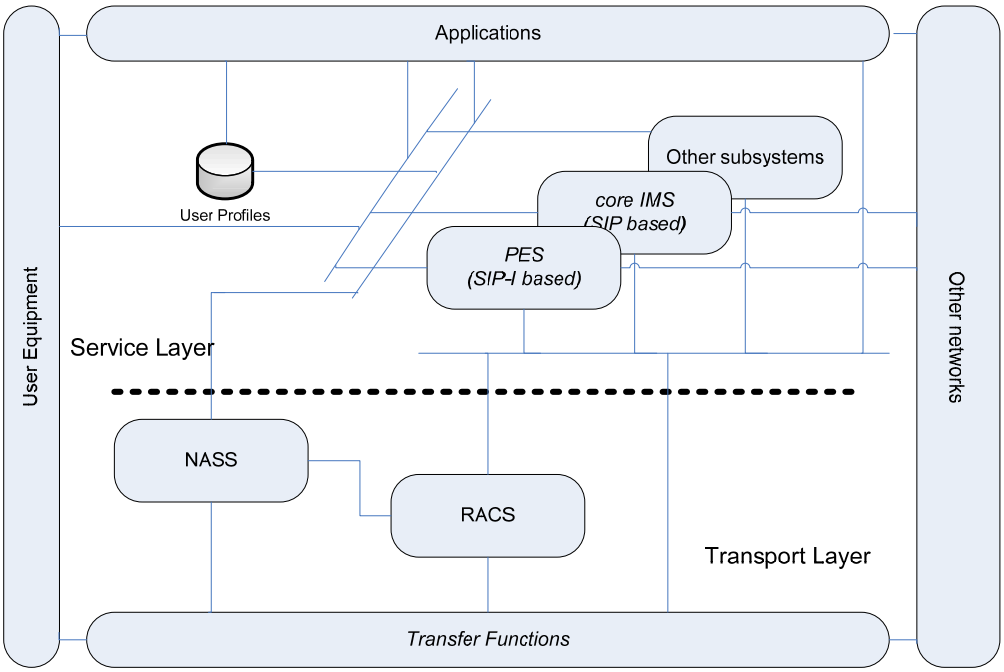



Figura 11- Arquitectura geral para as RPGs TISPAN [69].

## 4.1. Camada de Transporte

A camada lógica de transporte, responsável pela conectividade IP e transporte de informação multimédia entre os utilizadores, é formada por duas sub-camadas lógicas, nomeadamente, a sub-camada de Controlo de Transporte e a sub-camada *Transfer Functions*.

De seguida é feita uma descrição das funcionalidades dos elementos que compõem estas sub-camadas da arquitectura TISPAN.

### *4.1.1. Sub-camada de Controlo de Transporte*

Sendo a arquitectura TISPAN para as RPGs baseada em subsistemas funcionais, a sub-camada de Controlo de Transporte possui dois subsistemas ou elementos distintos que garantem o controlo e gestão de todos os recursos envolvidos no transporte de dados na sub-camada *Transfer Functions*. Estes dois subsistemas são o NASS e o RACS.

#### 4.1.1.1. Network Attachment Subsystem

O subsistema NASS da sub-camada de controlo de transporte é responsável por um conjunto de funcionalidades subjacentes à conectividade IP entre os terminais dos clientes

de uma rede de acesso e a rede RPG do operador. Mais concretamente, as principais funcionalidades deste subsistema são [69]:

- Alocação dinâmica de endereços IP aos terminais dos clientes das redes de acesso para que estes possam ter conectividade com os outros elementos definidos na arquitectura;
- Autenticação e autorização das redes de acesso baseada na subscrição dos clientes/utilizadores no domínio RPG;
- Gestão da localização dos clientes nas diferentes redes de acesso.

O NASS especificado na *release* 1 do TISPAN está normalizado tendo em conta a tecnologia de acesso xDSL.

Para mais detalhes sobre as funcionalidades e arquitectura interna do NASS, consultar a norma ETSI ES 282 004 [70].

#### 4.1.1.2. Resource and Admission Control Subsystem

O subsistema RACS da sub-camada de controlo de transporte possui um conjunto de funcionalidades que garantem determinados níveis de QoS aos clientes das redes de acesso consoante os seus perfis de serviço no operador RPG. Para isso este elemento controla o acesso a certos serviços requisitados pelos clientes através da informação de subscrição, que indica os serviços para o qual um cliente está autorizado aceder, através dos recursos disponíveis na rede e das políticas impostas pelo operador para a reserva de recursos e acesso a serviços.

Para mais detalhes sobre as funcionalidades e arquitectura interna do RACS consultar a norma ETSI ES 282 003 [71].

### *4.1.2. Transfer Functions*

A sub-camada *Transfer Functions* possui as funcionalidades necessárias para o transporte de tráfico multimédia IP entre terminais de utilizadores situados na mesma rede RPG ou em outra rede distinta, como a rede PSTN/ISDN, a rede *Public Land Mobile Network* (PLMN), a rede de acesso xDSL ou mesmo outra rede RPG. Existe um conjunto de elementos funcionais responsáveis pelo transporte de informação e integração de serviços entre a rede RPG e as diferentes redes e tecnologias de acesso. A Figura 12 mostra os principais elementos que compõem esta sub-camada de acordo com a *release* 1 do

TISPAN [69], e as suas ligações com os elementos da sub-camada de controlo de transporte.

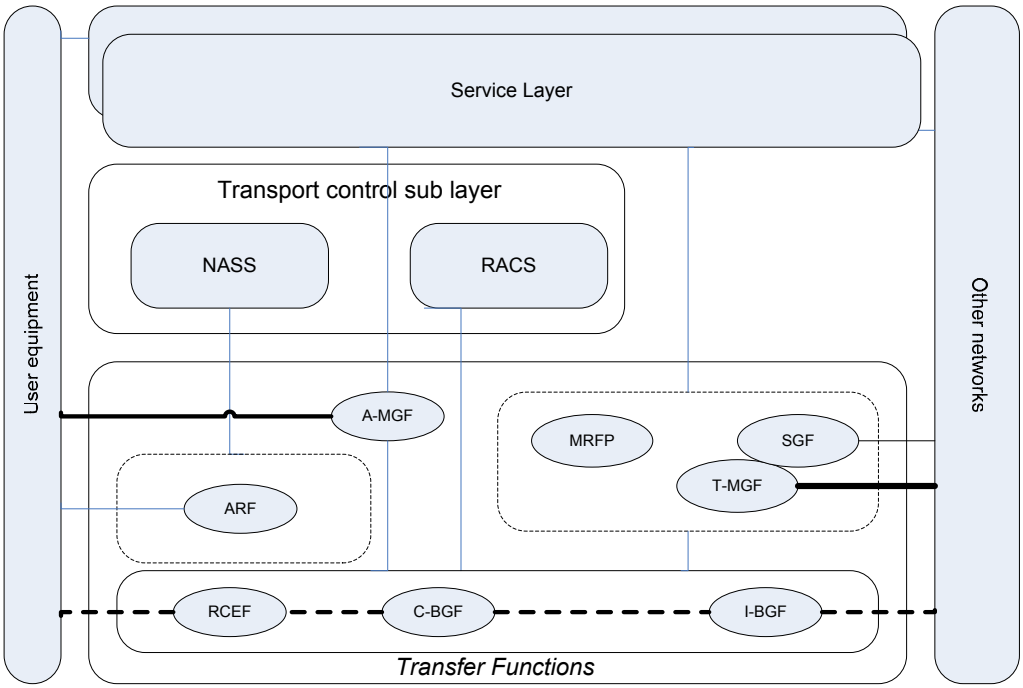



Figura 12- Sub-camada *Transfer Functions* da arquitectura TISPAN[9].

### 4.1.2.1. Border Gateway Function

O elemento *Border Gateway Function* (BGF) é a interface, no domínio do tráfego de dados multimédia, entre duas redes IP de transporte. Este elemento reside na fronteira entre a rede de acesso e a rede RPG e possui as seguintes funcionalidades, de acordo com a normalização TISPAN [69]:

- Filtragem de pacotes;
- Tradução de endereços IP e portos (NAPT);
- Interligação entre redes IPv4 e IPv6;
- *Transcoding* de áudio e vídeo entre as duas redes;
- Outras funcionalidades impostas por políticas da operadora.

O RACS, da sub-camada de controlo, interage com o BGF para controlar estas funcionalidades.

A TISPAN definiu dois tipos de BGF, ambos com as mesmas funcionalidades, mas com interfaces diferentes:

[9] Elemento *Basic Transport Function* (BTF) não está presente na ilustração. Vêr norma ETSI ES 282 001 [69].

- *Core-Border Gateway Function* (C-BGF): Localizado entre a rede de acesso e a RPG, é a interface entre estas duas redes (Figura 12);
- *Interconnection-Border Gateway Function* (I-BGF): Localizado entre duas RPG distintas, é a interface entre estas duas redes (Figura 12).

O C-BGF e o I-BGF possuem as mesmas funcionalidades que os elementos IMS-*Access Gateway* e *Translation Gateway,* respectivamente, definidos na norma ETSI TS 123 228 [72].

#### 4.1.2.2. Resource Control Enforcement Function

O elemento *Resource Control Enforcement Function* RCEF da sub-camada de transporte *Transfer Functions* possui as seguintes funcionalidades sob o controlo do elementos RACS [69]:

- Filtragem dos pacotes de dados tendo em conta o endereço IP e o porto;
- Indexagem dos pacotes do tráfego multimédia de saída da RPG;
- Policiamento do tráfego multimédia de entrada na RPG;
- Alocação dos recursos necessários para o tráfego de entrada e saída.

#### 4.1.2.3. Access Relay Function

O elemento *Access Relay Function* (ARF) traduz os pedidos de acesso dos utilizadores para um formato que seja entendido pelo NASS. No caso da utilização do *Point-to-Point Protocol* (PPP) para o acesso, o elemento *Access Management Function* (AMF) termina a ligação PPP com o utilizador, e comunica com NASS através de Diameter ou Radius tendo em conta a informação recebida no PPP [69].

#### 4.1.2.4. Media Gateway Function

O elemento *Media Gateway Function* (MGF) é responsável pelo mapeamento e/ou *transcoding* dos dados multimédia entre as redes IP e as redes de comutação de circuitos. Também possui outras funcionalidades como passagem de anúncios, envio de *Dual Tone Multi-Frequency* (DTMF) e audioconferência.

A *release* 1 do TISPAN define dois tipos de MGFs [69]:

- *Access-Media Gateway Function* (A-MGF): localizado na RPG do operador, permite a conectividade entre equipamentos com acessos analógicos e ISDN[10] das redes de acesso, e a rede RPG;
- *Trunking-Media Gateway Function* (T-MGF): localizado na rede do operador, permite a conectividade entre as redes RPG e as redes de comutação de circuitos PSTN/ISDN.

Outro MGF idêntico ao A-MGF mas de menor capacidade e situada no lado do cliente, é definido pelo TISPAN como *Residential-Media Gateway Function* (R-MGF). Este MGF é visto pela RPG como um simples equipamento do utilizador situado numa rede de acesso baseada em IP.

Os MGFs são controlados por elementos da camada de serviço, descritos nos capítulos seguintes, tendo por base o protocolo *MEdia GAteway COntrol* (MEGACO)/H.248 definido para o IMS. No âmbito das RPGs, o TISPAN definiu novas extensões a este protocolo através da adição de *packages* para o suporte de novas funcionalidades para o controlo de cada um dos tipos de MGFs. A especificação do protocolo MEGACO/H.248 para o A-MGF e R-MGF está documentada na norma ETSI ES 283 002 [73], e para o T-MGF na norma ETSI ES 283 049 [74].

Os principais requisitos para o A-MGF e R-MGF normalizados pelo TISPAN, ao qual os fabricantes destes elementos de transporte devem obedecer, estão indicados na norma ETSI ES 283 002 [73]. O T-MGF é funcionalmente idêntico ao IMS-*Media Gateway* (IMS-MGW) definido para o IMS. Os principais requisitos especificados pelo TISPAN em parceria com o 3GPP para este elemento, no âmbito da normalização das RPGs, estão documentados na norma ETSI TS 123 002 [75].

#### 4.1.2.5. Multimedia Resource Function Processor

Este elemento é idêntico em termos funcionais ao *Multimedia Resource Function Processor* (MRFP) descrito para o IMS na secção 3.2.2.1. O TISPAN adicionou novas propriedades e extensões ao protocolo MEGACO/H.248, que leva a uma nova especificação no controlo do MRFP através do elemento *Multimedia Resource Function Controller* (MRFC) localizado na camada lógica de serviço.

[10] Terminais ou *Private Branch eXchange* (PBX) com acessos básicos (BRI) e primários (PRI). Vêr norma ETSI ES 283 002 [73].

#### 4.1.2.6. Signalling Gateway Function

O elemento *Signalling Gateway Function* (SGF) possui as mesmas funcionalidades básicas que o elemento *Signalling Gateway* (SGW) descrito na secção 3.2.1.7. Os requisitos funcionais adicionados a este elemento estão normalizados pelo TISPAN, em conjunto com o 3GPP, na norma ESTI TS 123 002 [75].

## 4.2. Camada de Serviço

A camada lógica de serviço da arquitectura RPG do TISPAN, ilustrada na Figura 11, contém todas as funcionalidades de controlo e fornecimento dos serviços multimédia existentes na RPG aos terminais dos clientes. Basicamente, esta camada consiste num conjunto de subsistemas com funcionalidades específicas para cada serviço, e um conjunto de elementos com funcionalidades comuns aos subsistemas.

### *4.2.1. Subsistemas*

Existe um conjunto de subsistemas já definidos pelo TISPAN com funcionalidades específicas para as aplicações multimédia. Estes subsistemas definidos na *release* 1 do TISPAN são: o *core* IMS para o controlo e execução de serviços multimédia baseados no *Session Initiation Protocol* (SIP) das RPGs, e o PSTN/ISDN *Emulation Subsystem* (PES) para a emulação de serviços das redes PSTN/ISDN nas RPGs.

A arquitectura RPG do TISPAN foi concebida tendo em conta normalizações futuras e a adição de novas funcionalidades para a implementação de novos serviços nas RPGs através de subsistemas. No entanto, outros subsistemas foram propostos para *releases* posteriores como o subsistema com funcionalidades para serviços de *streaming* de música e vídeo e o subsistema para o *broadcasting* de conteúdos[11].

De seguida será feita uma breve descrição aos subsistemas definidos na *release* 1 do TISPAN.

#### 4.2.1.1. Core IP Multimedia Subsystem

O *core* IMS é o subsistema da arquitectura TISPAN para as RPGs responsável pelo controlo e disponibilização de serviços multimédia baseados em SIP aos utilizadores das RPGs. O TISPAN definiu este subsistema através da reutilização de alguns elementos funcionais da arquitectura IMS definida pelo 3GPP. O *core* IMS, definido na norma ETSI

TS 123 002 [75], não é mais que um subconjunto do IMS do 3GPP restrito às funcionalidades de controlo das sessões multimédia. Portanto, elementos como o *Application Server* (AS), MRFP, *Subscription Locator Function* (SLF), *Home Subscriber Server* (HSS) e IMS-MGW, pertencentes à arquitectura IMS do 3GPP, estão fora do *core* IMS do TISPAN. A Figura 13 ilustra a composição do subsistema *core* IMS definido pelo TISPAN, bem como as ligações existentes com os outros elementos da arquitectura.

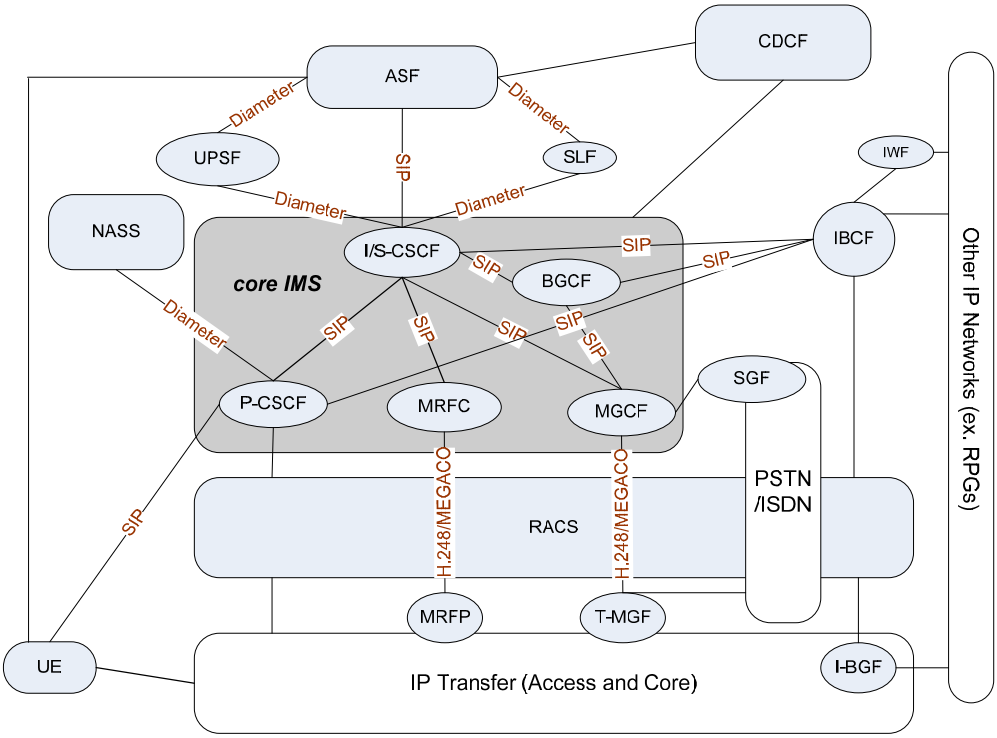



Figura 13- Subsistema *core* IMS da arquitectura TISPAN [76].

Os elementos da arquitectura IMS pertencentes a este subsistema do TISPAN foram devidamente adaptados, em cooperação com a *release* 7 do 3GPP, para o acesso a partir das redes fixas xDSL aos serviços multimédia baseados em SIP e aos serviços PSTN/ISDN *Simulation*. O conceito PSTN/ISDN *Simulation* remete para a capacidade do sistema oferecer aos terminais IP serviços semelhantes aos da rede PSTN/ISDN, através de uma infra-estrutura de controlo sobre IP.

Os elementos pertencentes ao subsistema *core* IMS apresentados na Figura 13, apesar de serem reaproveitados da arquitectura IMS definida na *release* 6 do 3GPP, possuem algumas diferenças funcionais impostas pelo TISPAN em colaboração com o 3GPP. Das diferenças indicadas na norma ETSI ES 282 007 [76], destacam-se as seguintes:

---

[11] Serviço *Digital Video Broadcast* (DVB).

- Ao elemento *Proxy-Call Session Control Function* (P-CSCF) foi adicionada a funcionalidade de *Network Address and Port Translation* (NAPT), conseguida através da interface baseada no protocolo Diameter com o RACS (Figura 13), e a possibilidade de obtenção de informação relativa à localização do terminal do utilizador na rede de acesso através da interface, também baseada no protocolo Diameter, com o NASS (Figura 13) [76];
- Ao elemento *Media Gateway Control Function* (MGCF) foi adicionado o suporte de sinalização *Transaction Capabilities Application Part* (TCAP) [77] para serviços suplementares como *Call Completion on Busy Subscriber* (CCBS) [76].

Mais informação sobre a arquitectura do subsistema *core* IMS e as diferenças face ao IMS do 3GPP pode ser encontrada na norma ETSI ES 282 007 [76].

### 4.2.1.2. PSTN/ISDN Emulation Subsystem

O subsistema PES da arquitectura TISPAN permite a emulação de serviços das redes PSTN/ISDN a clientes das RPGs. Esta emulação é conseguida através de um conjunto de elementos funcionais que compõem uma infra-estrutura de acesso dos clientes das RPGs aos serviços das redes PSTN/ISDN de uma forma transparente, e a possibilidade de terminais convencionais[12] das redes PSTN/ISDN acederem a estes mesmos serviços através de *Media Gateways* de Acesso e Residências conectadas às RPGs. O PES permite que estes terminais das redes PSTN/ISDN sejam vistos pela RPG como terminais comuns com o seu próprio registo e autenticação no domínio do operador RPG [69]. A Figura 14 ilustra os vários tipos de acesso, baseados em *Time Division Multiplexing* (TDM), suportados pelo PES do TISPAN.


Figura 14- Acessos TDM suportados pelo PES do TISPAN [78].

[12] Telefones analógicos (POTS), terminais FAX, terminais BRI e terminais PRI.

O papel do TISPAN é definir uma arquitectura lógica para o PES de forma a permitir a emulação de serviços PSTN/ISDN em cada um dos acessos TDM definidos pelo TISPAN e ilustrados na Figura 14. Baseando-se nos elementos do subsistema *core* IMS [76], o TISPAN especificou uma das possíveis estruturas internas para o subsistema PES, com as mesmas interfaces externas e com igual nível de operação que o *core* IMS relativamente à arquitectura global das RPGs. A Figura 15 mostra os elementos funcionais que compõem esta solução para a arquitectura do subsistema PES e a suas interfaces com as entidades comuns da arquitectura global RPG [3].

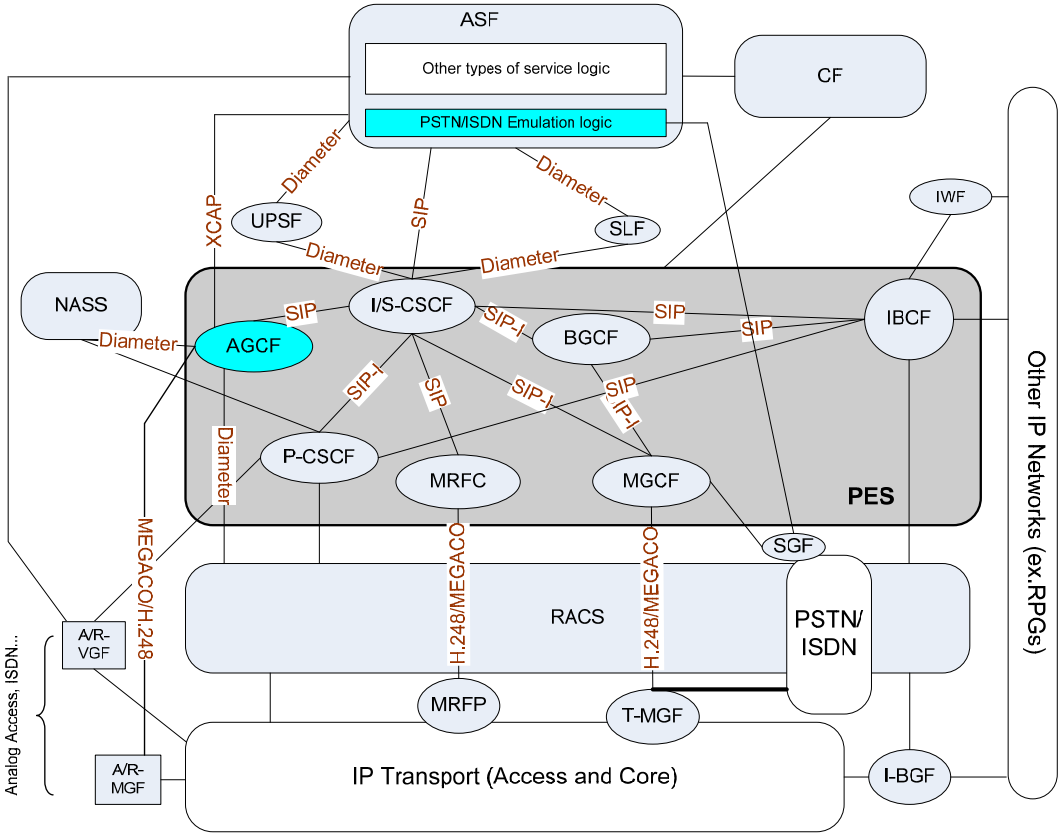



Figura 15- Arquitectura do PES baseada no IMS [3].

Apesar de muitas das funcionalidades dos elementos do subsistema PES da Figura 15 serem idênticos ou derivados da norma ETSI ES 282 007 [76], o TISPAN introduziu funcionalidades especificas a estes elementos, reflectindo-se principalmente nos protocolos das interfaces de comunicação. Como exemplo, são definidos novos perfis para o MEGACO/H.248 no controlo de A/R-MGFs [73] e T-MGFs [74], e utilizada uma nova extensão ao protocolo SIP definida pelo ITU-T, designada por SIP-I, para encapsular a sinalização ISDN *User Part* (ISUP) directamente na mensagem SIP. As vantagens desta nova extensão são: transferir a informação ISUP retirada do Sistema de Sinalização #7

(SS7), resultante da interligação com a rede PSTN/ISDN, e enviá-la para as redes de acesso baseadas em TDM das RPGs para a emulação de serviços específicos das redes PSTN/ISDN, sem que para isso seja necessário efectuar qualquer tipo de alteração aos terminais dessas redes; e estabelecer sessões de voz entre terminais de redes PSTN/ISDN distintas, utilizando a rede RPG como intermediária ("túnel" de ISUP sobre a RPG). O SIP-I é definido na ITU-T *Recommendation* Q.1912.5 [79].

Os elementos *Interrogating/Serving-Call Session Control Function* (I/S-CSCF), P-CSCF, *Breakout Gateway Control Function* (BGCF) e *Multimedia Resource Function Controller* (MRFC) da arquitectura PES da Figura 15 são idênticos em termos funcionais aos definidos pelo TISPAN para o subsistema *core* IMS na norma ETSI ES 282 007 [76]. Apenas ao MGCF foi adicionada a possibilidade de encapsular a sinalização ISUP proveniente da interligação com a rede PSTN/ISDN numa mensagem SIP, assim como retirar essa informação que chega de uma mensagem SIP-I [79] e enviá-la para a rede PSTN/ISDN via SGF. Para além destes elementos já conhecidos, o TISPAN definiu um novo elemento na arquitectura PES indicado a azul na Figura 15, designado por *Access Gateway Control Function* (AGCF). Este elemento será descrito detalhadamente de seguida segundo a normalização do TISPAN, pois é um dos pontos de destaque no âmbito do trabalho prático deste mestrado. O AGCF é responsável pelo controlo de *Access-Media Gateway Functions* (A-MGFs) e *Residential-Media Gateway Functions* (R-MGFs) [78]. Sendo o primeiro ponto de contacto para estes elementos, as principais funcionalidades do AGCF, segundo a norma ETSI TS 182 012 [3], são:

- Controlar os recursos dos A/R-MGFs para o estabelecimento de sessões, através do perfil MEGACO/H.248 definido na norma ETSI ES 283 002 [73] (Figura 15);
- Controlar os recursos na rede subjacentes ao transporte da informação multimédia e gerir os recursos QoS para as sessões através da interacção, baseada no protocolo Diameter especificado na norma ETSI TS 183 062 [80], com o subsistema RACS (Figura 15);
- Registar e autenticar no subsistema NASS os clientes ligados nos A/R-MGFs, através do protocolo Diameter especificado na norma ETSI ES 283 035 [81], de forma a permitir o acesso aos recursos da rede no transporte de informação multimédia;

- Interligar/mapear a sinalização entre o perfil SIP, definido pelo PES na norma ETSI ES 283 003 [82] para a interface com o I/S-CSCF (Figura 15), e o perfil para o protocolo MEGACO/H.248 definido na norma ETSI ES 283 002 [73];
- Actuar como um SIP *User Agent* ligado a um P-CSCF, relativamente às restantes entidades funcionais da arquitectura PES.

O TISPAN assume que os serviços PSTN/ISDN a serem emulados pelos utilizadores usando a arquitectura PES do TISPAN, devem residir em um ou mais ASs. Portanto, é definida uma unidade lógica no AS para a emulação de serviços PSTN/ISDN nesta arquitectura (a azul na Figura 15).

Para a execução de serviços suplementares[13] é necessário que pelo menos um AS com esta unidade lógica seja inserido no percurso da sinalização SIP. Mas para isso é necessário que o utilizador que requer o serviço esteja autorizado para tal. No caso dos utilizadores ligados aos A/R-MGFs controlados por um AGCF, este possui uma interface baseada no *Extensible Markup Language Configuration Access Protocol* (XCAP), para o controlo destes serviços suplementares. Para além do controlo, esta interface com a unidade lógica PSTN/ISDN do AS permite ao AGCF adquirir e enviar o *dialtone* apropriado para o terminal do cliente ligado ao A/R-MGF, caso ocorram os eventos *off-hook* ou *flash-hook* do terminal.

Os *Access*/*Residential*-VoIP *Gateway Functions* (A/R-VGFs) (Figura 15) são *Media Gateways* baseados em SIP e, como tal, não necessitam de um AGCF para o seu controlo. Neste caso, o A/R-VGF é ligado a um P-CSCF como se fosse um terminal IP ligado a um P-CSCF numa arquitectura IMS [78].

#### 4.2.1.3. Outros Subsistemas

A *release* 1 do TISPAN definiu uma arquitectura geral para as RPGs de forma a permitir a adição suave de novos subsistemas ao longo do tempo, contemplando novas solicitações e classes de serviço exigidas pelo mercado, e a importação de subsistemas de outras organizações de normalização.

Para além dos subsistemas *core* IMS e PES introduzidos na *release* 1 do TISPAN, esta define na *release* 2 um novo subsistema para o suporte de serviços IPTV, como *video-on-*

[13] *Short Message Service* (SMS), *Calling Line Identification Public* (CLIP), *Calling Line Identification Restriction* (CLIR), *call waiting*, *call forwarding*, etc.

*demand* e *broadcasting* de conteúdos multimedia, através de uma arquitectura de controlo descrita na norma ETSI TS 182 028 [83].

## *4.2.2. Entidades Comuns*

As entidades comuns da arquitectura TISPAN são elementos funcionais acedidos por todos os subsistemas da arquitectura. De seguida é feita uma breve descrição de cada um destes elementos.

### 4.2.2.1. User Proxy Server Function

O elemento *User Proxy Server Function* (UPSF) da arquitectura TISPAN é uma base de dados de armazenamento de informação relacionada com os clientes da RPG. Tal como o elemento HSS definido para a arquitectura IMS pelo 3GPP e descrito na secção 3.2.1.1, este elemento pode armazenar a seguinte informação [69]:

- Identificação do cliente na RPG;
- Parâmetros de segurança definidos para o cliente na rede;
- Localização/endereçamento do terminal do cliente na rede RPG;
- Perfil de serviços para o qual o cliente está autorizado a aceder.

O comportamento do UPSF na arquitectura TISPAN é idêntico ao HSS para as redes móveis definido na norma ETSI TS 123 002 [75], à excepção da funcionalidade de *Home Location Register/Authentication Center* (HLR/AUC). Este elemento pode ser acedido através da interface baseada no protocolo Diameter por qualquer subsistema e AS, como indicado na Figura 13 e Figura 15.

### 4.2.2.2. Server Local Function

Este elemento é idêntico ao definido na secção 3.2.1.1 para a arquitectura IMS do 3GPP. Faz a correspondência do UPSF onde está armazenada a informação de cada um dos clientes, em cenários onde existe mais do que um UPSF. Este elemento é acedido, através de uma interface baseada no protocolo Diameter, por qualquer subsistema e pelo AS, como está indicado na Figura 13 e Figura 15.

### 4.2.2.3. Application Server Function

O *Application Server Function* (ASF) é a entidade responsável pelo fornecimento de serviços e aplicações multimédia aos clientes finais das redes RPGs. Possui um conjunto de unidades lógicas com regras específicas para o fornecimento e execução dos diferentes

serviços, as quais são acedidas pelos diferentes subsistemas consoante o tipo de serviço pretendido e suportado. Para o caso do subsistema *core* IMS ilustrado na Figura 13, o ASF funciona como um AS definido na norma ETSI TS 123 002 [75]. Este subsistema suporta serviços armazenados em três tipos de ASs definidos na secção 3.2.2.3 para a arquitectura IMS. No entanto, esta entidade funcional, no âmbito da arquitectura TISPAN para as RPGs, pode ser diferente da definida pelo 3GPP para arquitectura IMS em termos de serviços suportados [69].

#### 4.2.2.4. Charging Functions

Este elemento é usado por todos os subsistemas da camada de aplicação e de transporte da arquitectura TISPAN para o registo de informação necessária à taxação de serviços executados pelos clientes de uma RPG. A especificação para esta funcionalidade está fora do âmbito da *release* 2 do TISPAN.

#### 4.2.2.5. Interworking Function

Este elemento é responsável pelo mapeamento entre os protocolos de sinalização utilizados nos subsistemas da camada de serviço e os protocolos de sinalização utilizados em outras redes baseadas em IP. Um exemplo desta funcionalidade é o mapeamento entre o perfil do protocolo SIP definido para um dos subsistemas indicados na Figura 13 e Figura 15, e o protocolo H.323 ou outro perfil SIP utilizado num subsistema de outro domínio RPG.

#### 4.2.2.6. Interconnection Border Control Function

Este elemento possui as funcionalidades necessárias para a interacção protocolar entre subsistemas *core* IMS (Figura 13) ou PES (Figura 15) de diferentes domínios RPG. Caso a interacção ocorra entre duas arquitecturas RPG do TISPAN, os protocolos de sinalização inerentes às sessões estabelecidas entre estes dois domínios TISPAN são enviados para o *Interconnection Border Control Function* (IBCF) da sua rede e, posteriormente, enviados para o IBCF do outro domínio. Se os dois domínios IP utilizarem protocolos de sinalização distintos para o estabelecimento de sessões, esta sinalização deverá ser enviada para o elemento *Interworking Function* (IWF), descrito no ponto anterior, para fazer a conversão de sinalização para posteriormente enviar para o outro domínio IP.

O IBCF deve determinar para que elemento seguinte do seu domínio deve enviar a sinalização proveniente de outras redes IP, tendo em conta a informação da sinalização recebida e as políticas internas da rede. Os próximos elementos podem ser o I/S-CSCF, P-

CSCF e BGCF como está evidenciado nas arquitecturas da Figura 13 e Figura 15. O IBCF também interage com o elemento RACS da camada de transporte para o controlo dos elementos responsáveis pela interacção entre os dois domínios ao nível do transporte de dados da sessão.

## 4.3. Sumário

Este capítulo descreveu a arquitectura TISPAN definida pelo ETSI responsável pela normalização de uma rede futura que permite a convergência de diferentes serviços e tecnologias de acesso no mesmo domínio IP. Encontram-se também definidos os dois subsistemas normalizados na *release* 1 do TISPAN.

- *Core* IMS: O TISPAN definiu este subsistema através da reutilização de alguns elementos funcionais da arquitectura IMS definida pelo 3GPP (Figura 13);
- PES: Permite a emulação de serviços das redes PSTN/ISDN a clientes das RPGs. Define novos perfis para o MEGACO/H.248 no controlo de A/R-MGFs e T-MGFs, e utiliza uma nova extensão ao protocolo SIP definida pelo ITU-T, designada por SIP-I. O PES introduziu também o elemento AGCF para o controlo de A/R-MGFs.

Neste capítulo também foi analisada a camada lógica de transporte, responsável pela conectividade IP e transporte de informação multimédia, e as suas sub-camadas lógicas, nomeadamente, a sub-camada de Controlo de Transporte e a sub-camada *Transfer Functions*. Os elementos da sub-camada de Controlo de Transporte: o NASS e o RACS, e os elementos da sub-camada *Transfer Functions*: C-BGF, I-BGF, RCEF, ARF, A-MGF, T-MGF, R-MGF, MRFP e SGF.

Finalmente, foram descritas entidades comuns que são acedidas por todos os subsistemas da arquitectura.

# Capítulo 5: Realizações Práticas de Testes *Standalone*

A implementação de um sistema para o acesso a serviços sobre IP por todos os tipos de tecnologias de acesso implica a instalação e configuração de um conjunto de entidades físicas que implementem as funcionalidades impostas pelos organismos de normalização para as Redes de Próxima Geração (RPGs) já descritas nos capítulos anteriores.

O principal objectivo deste capítulo é dar a conhecer as potencialidades e características mais relevantes de alguns produtos adquiridos, que implementam fisicamente os elementos funcionais da arquitectura *PSTN/ISDN Emulation Subsystem* (PES) do *Telecommuncations and Internet converged Services and Protocols for Advanced Networking* (TISPAN). Com este intuito, foram feitos vários testes a estes equipamentos através de um cenário simples designado por cenário de testes *standalone*.

Neste capítulo será feita inicialmente uma pequena abordagem às principais características físicas e funcionais (interfaces, protocolos, capacidade, *codecs*, etc.) dos produtos adquiridos tendo em conta os cenários a implementar. De seguida será feita uma descrição da montagem dos cenários para os testes *standalone*, indicando as principais configurações para a ligação e comunicação dos elementos entre si. Por último serão indicados os vários testes realizados, bem como os resultados obtidos.

## 5.1. Testes Standalone

Antes de ligar os vários equipamentos que compõem os elementos da RPG para os sistemas de *Trunking* e Acesso, é necessário uma familiarização com as funcionalidades e principais parâmetros de configuração destes equipamentos. Para isso foi adquirida inicialmente, após uma pesquisa de mercado, uma Mediant™ 2000 do fabricante AudioCodes® [85] para a implementação futura do elemento funcional *Trunking-Media*

*Gateway Function* (T-MGF) e *Signalling Gateway Function* (SGF) da Figura 15, e um *kit* de testes designado por *Mombasa* que pretende demonstrar as potencialidades do micro-controlador *Chagall* M82530 SiPBX™ da Mindspeed® [86] para a implementação de *Media Gateways*. Este protótipo foi muito importante na construção de um cenário para testes ao equipamento Mediant™ 2000.

Antes de passar à descrição do cenário utilizado para os testes *standalone* composto pelos equipamentos Mediant™ 2000 e *kit Mombasa*, é feita uma breve descrição, após um estudo aprofundado, das características físicas, protocolos suportados, principais módulos internos, etc. destes equipamentos. O cenário posteriormente será utilizado para domínio do equipamento, familiarização com os principais parâmetros de configuração e conhecimento das potencialidades da Mediant™ 2000.

## 5.2. Mediant™ 2000

Neste capítulo será feita uma breve descrição, após um estudo da Mediant™ 2000, dos principais módulos internos que compõem fisicamente este sistema, bem como das características mas relevantes e dos principais parâmetros de configuração imprescindíveis para o bom funcionamento deste produto da AudioCodes®.

A AudioCodes® apresenta a Mediant™ 2000 como uma solução completa para a implementação dos elementos T-MGF, SGF, *Access-VoIP Gateway Function* (A-VGF[14]) e *Access-Media Gateway Function* (A-MGF[15]) de acordo com os principais requisitos da arquitectura PES do TISPAN, apresentada na Figura 15, para estes elementos. Este produto está ilustrado na Figura 16.


Figura 16- Mediant™ 2000.

Internamente a Mediant™ 2000 é composta por vários módulos físicos, comuns a todos os fabricantes de *Media Gateways*, que em conjunto implementam as principais funcionalidades pretendidas para uma *Media Gateway*. A Figura 17 mostra os principais

[14,15] A-MGF e A-VGF só para acessos ISDN PRI.

módulos constituintes da Mediant™ 2000 de uma forma simplificada para melhor compreensão.

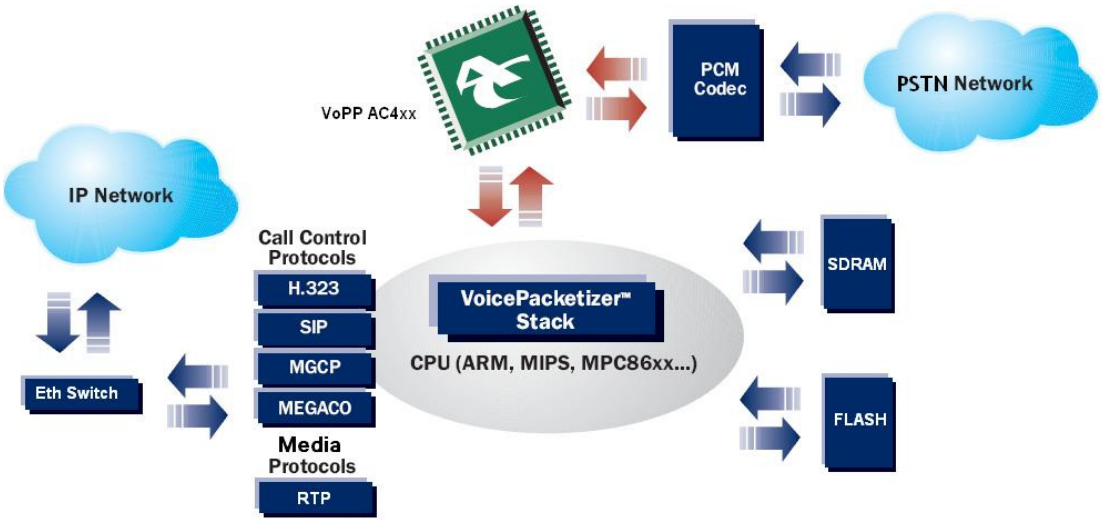



Figura 17- Arquitectura interna da Mediant™ 2000 [87].

Um dos módulos principais de uma *Media Gateway* é o *Digital Signal Processor* (DSP). Este módulo possui várias funcionalidades, sendo as mais importantes:

- Codificação e descodificação de áudio utilizando *codecs* de compressão;
- Cancelamento de eco para as sessões de voz em tempo-real;
- Geração e detecção de *Dual Tone Multi-Frequency* (DTMF);
- Processamento dos dados das sessões de voz, dos dados de Modem e de FAX.

O VoicePacketizer™ *Stack* da Figura 17 é uma biblioteca em linguagem C da AudioCodes® com funções para o encapsulamento dos dados em pacotes *Real-time Transport Protocol* (RTP) de acordo com os *Request For Comments* (RFCs): 3550 [41], 3551 [88], 2198 [89] e 2833 [42].

A Mediant™ 2000 da AudioCodes® possui um conjunto de *stacks* protocolares de controlo definidas pelas organizações *European Telecommunications Standard Institute* (ETSI), *International Telecommunication Union – Telecommunications* (ITU-T) e *Internet Engineering Task Force* (IETF). Este elemento pode conter, de acordo com o tipo de *firmware* e licença instalada no sistema, os seguintes protocolos para o controlo de sessões: *Session Initiation Protocol* (SIP) [32], *Media Gateway Control Protocol* (MGCP) definido pelo IETF no RFC 3435 [91], H.323 [49] e *MEdia GAteway COntrol* (MEGACO)/H.248 [39], sendo o MEGACO/H.248 o indicado pelo TISPAN para os elementos T-MGF e A-MGF, e o SIP para o A-VGF.

Após uma descrição dos principais módulos internos da Mediant™ 2000, será feita uma listagem das principais características e funcionalidades deste produto tendo em conta a sua aplicação neste trabalho. Para mais informação pode ser consultado o manual do utilizador [90].

Fisicamente, a Mediant™ 2000 possui 2 portas RJ-45 de *ethernet* 10/100 Base-TX a funcionarem em modo de redundância para ligação a *Local Area Networks* (LANs) ou *Wide Area Networks* (WANs), e 4 portas RJ-48c para ligações físicas E1/T1/J1 a *Private Branch eXchange* (PBX) ou a redes *Public Switched Telephone Network/Integrated Services Digital Network* (PSTN/ISDN). Nesta configuração a Mediant™ 2000 suporta até 120 canais de voz, FAX e Modem em simultâneo através das 4 interfaces E1/T1/J1. Mas este produto pode ser escalável até 16 interfaces E1/T1/J1, permitindo assim uma configuração máxima de 480 canais para esses serviços.

No que respeita à Voz sobre IP (VoIP) os protocolos utilizados para o transporte de dados é o RTP e o *Real-time Transport Control Protocol* (RTCP) de acordo com os RFCs 3550 [41] e 3551 [88]. Estes protocolos foram descritos nos capítulos 3.3.3.1 e 3.3.3.2 respectivamente. Para a codificação de voz a ser transportada pelo RTP, a Mediant™ 2000 suporta os seguintes *codecs* com diferentes *bit rates*[16]:

- G.711 *A-law* e *μ-law* [59];
- G.723.1 [64];
- G.726 [62];
- G.727 [93];
- G.728 [94];
- G.729A [65];
- *Global System for Mobile communications* (GSM) [63];
- *Enhanced Variable Rate CODEC* (EVRC) [95];
- *Internet Low Bit Rate Codec* (iLBC) [96].

No que respeita à sinalização do lado PSTN/ISDN, que será traduzida pela Mediant™ 2000 em SIP, MGCP ou MEGACO/H.248 do lado IP, este produto consegue gerar e interpretar um conjunto diversificado de sinalizações, através das interfaces E1/T1/J1, normalizadas pelas principais organizações de normalização:

[16] Para mais informação sobre as caracteristicas destes *codecs* consultar o manual de utilizador da Mediant™ 2000 [90] ou as próprias normas dos *codecs*.

- ISDN *Primary Rate Interface* (PRI): ETSI EURO ISDN, *American National Standards Institute* (ANSI) NI2M, Nortel DMS, Lucent 5ESS, Lucent 4ESS, Japan NTT, Australian Telecom, New Zealand Telecom, Korean Operator e Hong Kong *variant*;
- *Channel Associated Signaling* (CAS): MF-R1 e MFC/R2.

Tendo em conta o indicado pelo TISPAN para os acessos/interfaces a suportar pelos *Access/Residential-Media Gateway Functions* (A/R-MGFs) e *Access/Residential-VoIP Gateway Functions* (A/R-VGFs) da arquitectura PES e ilustrados na Figura 14, a Mediant™ 2000 não pode ser utilizada pontualmente como A-MGF e A-VGF para acessos básicos (BRI), pois esta só suporta sinalização do tipo ISDN e CAS para acessos primários (PRI). Também não pode ser utilizada como R-MGF e R-VGF para acessos básicos e analógicos.

A Mediant™ 2000 possui, também, a funcionalidade de SGF incorporada de acordo com arquitectura PES da Figura 15. Qualquer *time-slot* de um E1/T1/J1 deste elemento pode ser configurado para a troca de sinalização com a rede PSTN/ISDN que utilize o Sistema de Sinalização #7. Esta sinalização é por sua vez transportada para o lado IP através dos protocolos de transporte ISDN Q.921-*User Adaptation* (IUA) [97], *Message Transfer Part* 2 *User Adaptation layer* (M2UA) [98], *Message Transfer Part* 3 *User Adaptation layer* (M3UA) [38], via *Stream Control Transmission Protocol* (SCTP) [37] sobre IP. Este mecanismo de transporte da informação das camadas superiores do *Sistema de Sinalização #7* (SS7) sobre IP é definido pelo grupo *Signalling Transport* (SIGTRAN) do IETF e está descrito no capítulo 3.2.1.7.

Outras funcionalidades serão descritas ao longo da Dissertação, quando a utilização da Mediant™ 2000 em determinados cenários. Também será feita uma comparação dessas funcionalidades com os requisitos indicados pelo TISPAN.

## 5.3. kit Mombasa

O *kit Mombasa*, ilustrado na Figura 18, é uma plataforma simples de testes que pretende demonstrar as potencialidades do micro-controlador *Chagall* M82530 SiPBX™ da Mindspeed® e ajudar os fabricantes no desenvolvimento dos seus próprios sistemas de A/R-MGFs com acessos analógicos e ISDN PRI, de acordo com a normalização TISPAN, e no desenvolvimento de sistemas IP PBX.

A Figura 18 identifica as interfaces de ligação ao exterior mais importantes que integram esta plataforma, destacando-se a interface de ligação ao barramento *Peripheral Component Interconnect* (PCI) de um computador para alimentação, os conectores RJ11 para ligação e estabelecimento de sessões de voz com *Plain Old Telephone Service* (POTS), os conectores RJ45 para ligação IP e estabelecimento de sessões VoIP, e para ligação E1/T1 a dispositivos baseados em sinalização PRI ISDN [99].

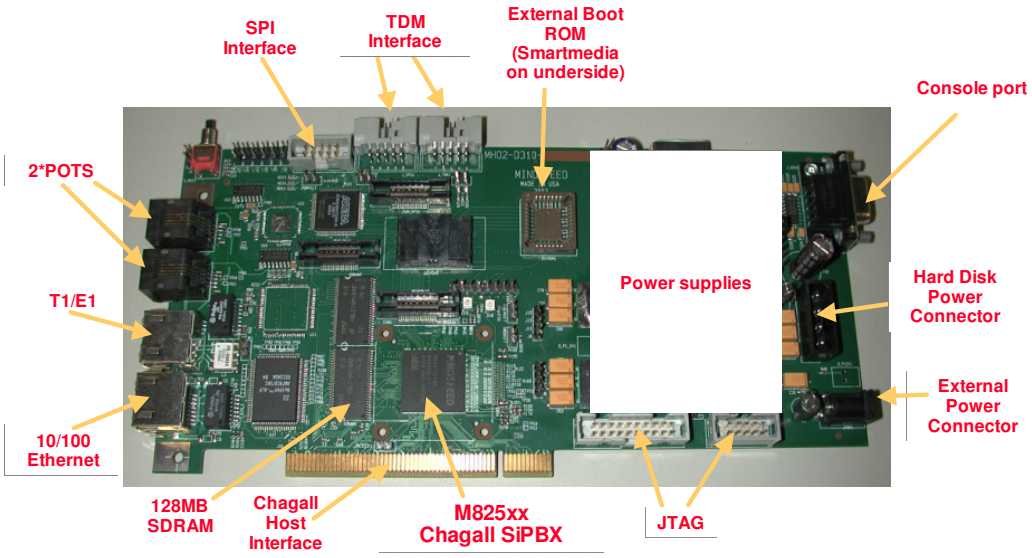



Figura 18- *kit Mombasa* da Mindspeed® [99].

A Figura 19 ilustra a arquitectura interna do micro-controlador em questão. Segundo esta, o M82530 é formado por um controlador programável ARM920T a 250 MHz, um *Packet Processor*, um DSP, um *Soft Encryption Core* e um conjunto de controladores de acesso para *hardware* externo.

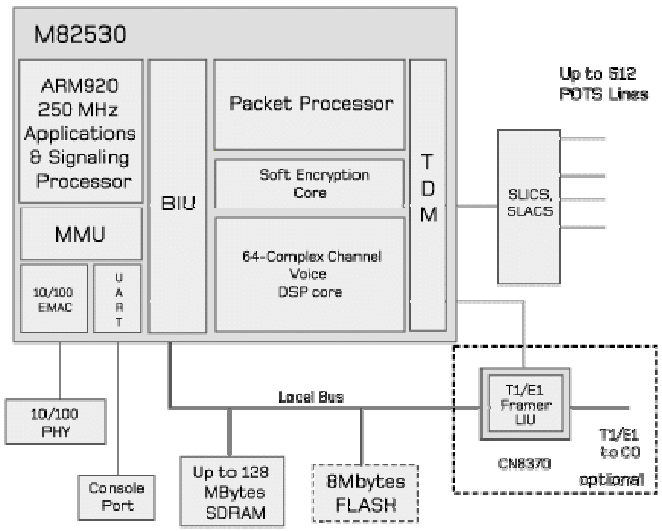



Figura 19- Arquitectura do micro-controlador *Chagall* M82530 SiPBX™ da *Mindspeed*® [100].

Segue-se uma descrição de cada um dos blocos do micro-controlador de acordo com a documentação [100].

O bloco *Applications & Signalling Processor* é implementado fisicamente através de um processador incorporado ARM920T a 250MHz. Este processador possui o *software* necessário para o controlo e processamento de sinalização das sessões de voz quer da parte ISDN e analógica, quer da parte IP. Para a parte ISDN, a única sinalização testada na plataforma *Mombasa* foi a ISDN PRI Lucent 5ESS [101]. Embora a plataforma seja bastante rudimentar para o tipo de sinalização ISDN relativamente à especificação do TISPAN, é o suficiente para a realização dos testes *standalone* com a Mediant™ 2000. Para a parte IP, este processador suporta os seguintes protocolos de sinalização: SIP [32], H.323 [49] e MEGACO/H.248 [39].

O bloco *Packet Processor* é necessário para a construção e gestão dos pacotes *ethernet* a serem transmitidos de ou para a rede IP. Este segue um conjunto de protocolos na construção dos pacotes, de acordo com a arquitectura TISPAN, para o transporte de sinalização SIP, H.232 ou MEGACO/H.248, e para o transporte de voz através do protocolo RTP definido no RFC 3550 [41]. Portanto para o transporte de sinalização é utilizado o *User Datagrama Protocol* (UDP) sobre IP e para o transporte de voz é utilizado o protocolo RTP.

O bloco DSP é responsável pelo processamento em tempo real do sinal de voz. Suporta vários *codecs* de acordo com as especificações do TISPAN:

- G.711 $\mu$*-law* e *A-law* [59];
- G.723.1 e G.723.1A [64];
- G.726 [62];
- G.729A e G.729B [65].

Embora o DSP deste micro-controlador não suporte os *codecs* de voz *Adaptive Multi-Rate* (AMR) [60] e *Adaptive Multi-Rate-Wideband* (AMR-WB) [61] exigidos pelo *3rd Generation Partnership Project* (3GPP) e pelo TISPAN, estes são suficientes para os testes pretendidos com esta plataforma. Dependendo do *codec* utilizado, a capacidade em número de sessões simultâneas entre terminais IP e POTS, e entre POTS, é limitada.

O bloco *Soft Encryption Core* é responsável pela segurança e cifragem dos dados a transmitir.

## 5.4. Cenários de Testes

Para os testes *standalone* em questão foram criados dois cenários com a Mediant™ 2000 da AudioCodes® e o *kit Mombasa* da Mindspeed®.

O primeiro cenário está ilustrado na Figura 20. Este cenário, para além dos equipamentos já mencionados, também possui um terminal SIP emulado pelo *softphone X-Lite* 3.0 [102] num computador e dois POTS.

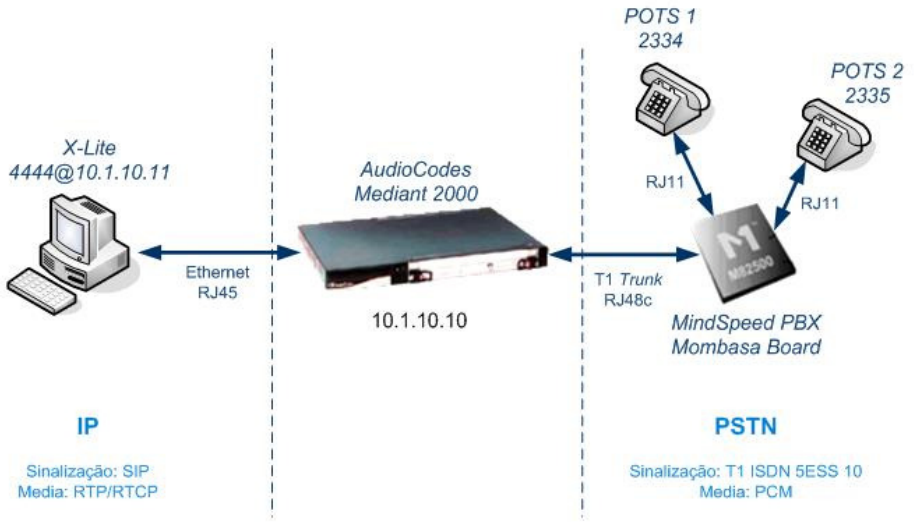



Figura 20- Cenário I dos testes *standalone*.

Para proceder à montagem do cenário foi necessário configurar vários parâmetros internos de cada um dos equipamentos. Antes da configuração ligaram-se os equipamentos directamente entre si, como ilustra a Figura 20, ficando o *kit Mombasa* a funcionar como um PBX com dois POTS ligados nos conectores RJ11 e com uma ligação do conector RJ48c E1/T1 ao conector #1 RJ48c E1/T1/J1 da Mediant™ 2000. Para a ligação IP, o computador foi ligado directamente pela interface RJ45 à Mediant™ 2000.

As ligações E1/T1 RJ48c e IP RJ45 utilizam o mesmo cabo físico *Unshielded Twisted Pair* (UTP) cat.5e com uma pequena diferença na troca dos pares nas fichas de ligação, como está explicado no manual de utilizador da Mediant™ 2000 [90].

Após a ligação física dos equipamentos entre si procedeu-se à configuração de cada um destes começando pelo *kit Mombasa*. Para configurar os parâmetros de acordo com o cenário da Figura 20, ligou-se esta plataforma a um computador através de um cabo série de 9 pinos. No computador, através da aplicação *Hyper-terminal*, configurou-se uma ligação série com os parâmetros indicados no Anexo I. De seguida foi feito o arranque do *kit* e, antes de executar a aplicação *Sipbx* responsável pelo controlo e estabelecimento de

sessões no micro-controlador, foram configurados alguns parâmetros do ficheiro de entrada "*gateway.conf*". Os parâmetros dizem respeito à ligação ISDN PRI com a Mediant™ 2000, sendo configurada uma ligação com as seguintes características:

- Sinalização: T1 5ESS 10 ISDN [101];
- Código de Linha: *Alternate Mark Inversion* (AMI) [103];
- Estrutura da trama: *Extended Super Frame* (ESF) [104].

Este ficheiro de configuração pode ser consultado no Anexo I. Só os parâmetros da secção *[BT8370_CFG]* foram configurados, os restantes foram deixados com a definição de fábrica.

De seguida, através da ligação série foi executada a aplicação *Sipbx*, responsável pela iniciação de todos os módulos e *stacks* protocolares no micro-controlador para o estabelecimento de sessões, de acordo com os passos indicados no manual [99]. Neste momento, o *kit* está preparado para estabelecer sessões de voz simples entre os dois POTS, POTS e IP, IP e ISDN, e ISDN e POTS. Antes da configuração da Mediant™ 2000 foram realizados pequenos testes com o *kit*, testes estes que passam pelo estabelecimento de chamadas entre os dois POTS e entre um terminal IP ligado directamente à porta RJ45 e um dos POTS. Para o teste entre POTS, marcou-se no POTS 1, com o número "2334", o número "2335" do POTS 2 e vice-versa, para estabelecer uma chamada a fim de aferir a configuração da plataforma ao nível da ligação com os POTS. Estes números já estão definidos por defeito para cada um dos POTS, podendo o utilizador alterá-los através do ficheiro "*sipbx_linux.conf*" apresentado no Anexo I.

Para os testes entre terminal IP e POTS, configurou-se o computador com o *softphone X-Lite* 3.0 com o endereço 192.168.9.50 estático, dado que na configuração do *kit* para chamadas de POTS para IP, este endereço estar definido por defeito para um terminal IP ligado ao *kit*, como se pode constatar através da tabela "*SIP_TABLES*" do ficheiro "*sipbx_linux.conf*", apresentado no Anexo I. Por análise desta tabela, todas as chamadas originadas dos POTS com o número de destino "9335" são mapeadas internamente para o número IP "4444" e encaminhadas para o terminal IP com o endereço 192.168.9.50. Portanto, configurou-se o *softphone X-Lite* 3.0 no computador com a seguinte conta ilustrada na Figura 21.

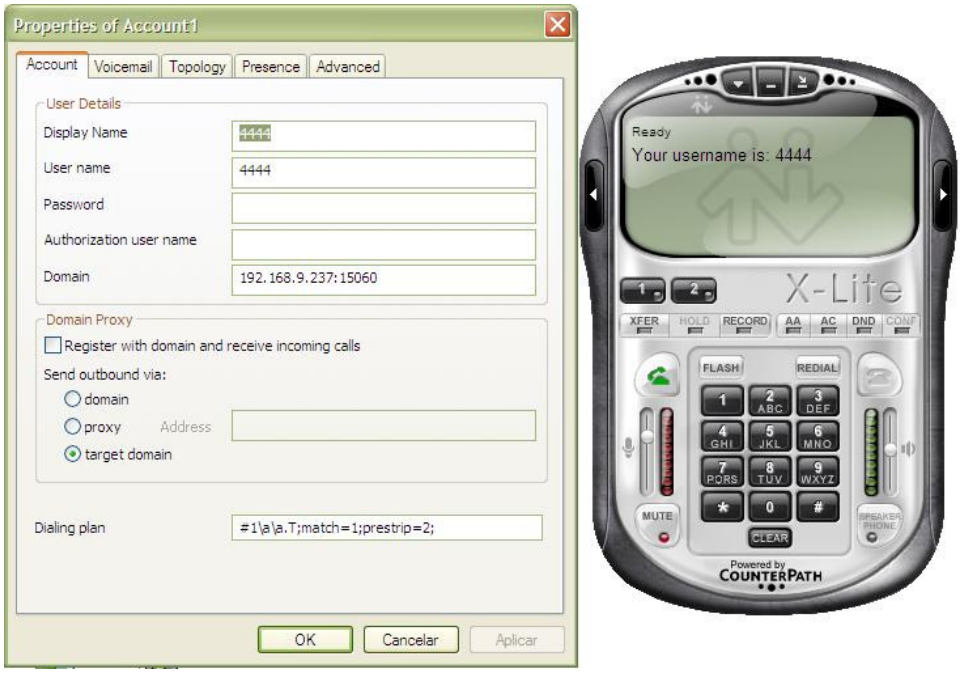



Figura 21- Configuração do *softphone X-Lite* 3.0 ligado directamente ao *kit Mombasa*.

O *Display Name* e *User Name* têm o número "4444", obedecendo à configuração do *kit*, e o *Domain* tem o endereço/porto IP 192.168.9.237:15060, correspondendo ao endereço IP do *kit Mombasa*, utilizado para encaminhar as chamadas do lado IP para os POTS ligados ao *kit*. Após esta configuração efectuaram-se chamadas do POTS 1 para o *X-Lite* 3.0. Através da marcação do número "9335" no POTS 1 é tocado sinal *ring tone* de alerta no *X-Lite* 3.0 e o sinal de chamada no POTS 1. Após o atendimento do lado IP a chamada é estabelecida como pretendido. Também se efectuou uma chamada do *X-Lite* 3.0 para o POTS 1, através da marcação do número "2334" no *softphone*. O processo de estabelecimento da chamada, bem como a parte de conversação correu dentro da normalidade como seria de esperar.

Para maior facilidade e familiarização com os vários parâmetros da Mediant™ 2000, esta configuração foi realizada via *web server* através de um computador com um *web browser*, ligado directamente à porta RJ45 (Figura 22).

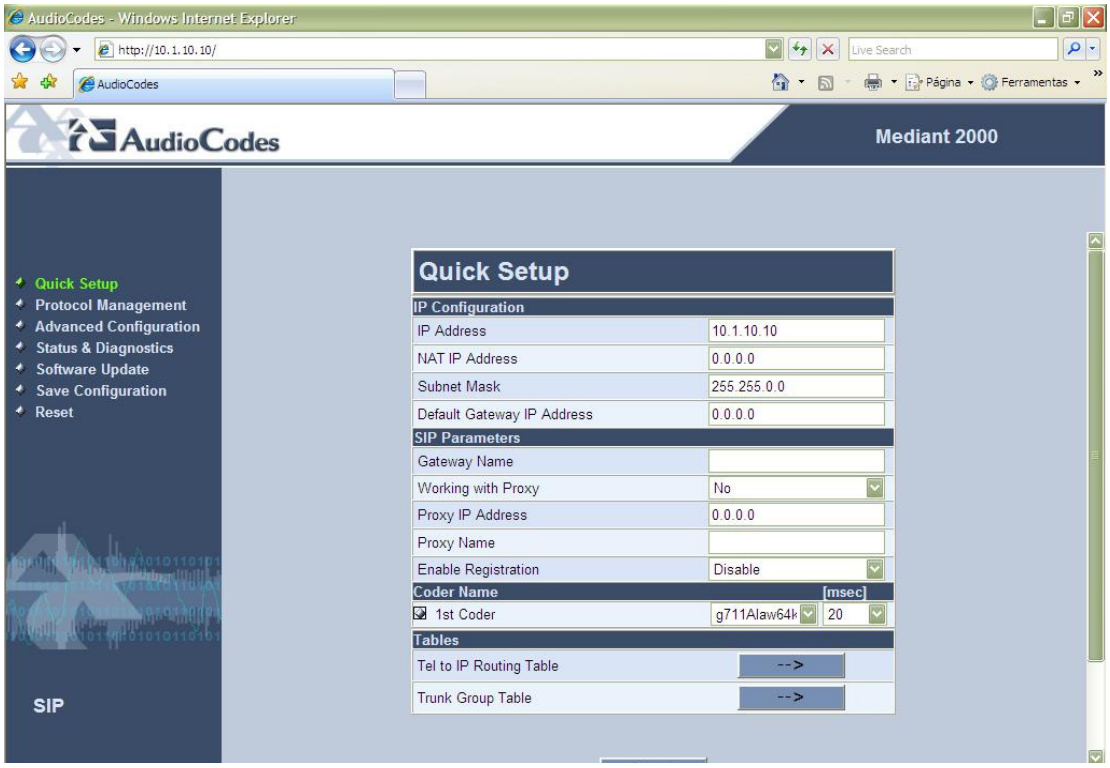



Figura 22- Página *web* inicial da Mediant™ 2000 versão 4.6 SIP.

Após o acesso ao *web server* da Mediant™ 2000, foi necessário configurar vários parâmetros para o cenário de testes da Figura 20. No entanto, antes deste processo foi carregado um ficheiro "*.ini*" de configuração que contém vários parâmetros pré-definidos de fábrica para o suporte a ligações T1. Este ficheiro, designado por "*Mediant_SIP_T1.ini*", encontra-se no Anexo II já com a configuração final pretendida. Para carregar este ficheiro na Mediant™ 2000 seguiram-se os passos indicados no manual de utilizador [105].

Após o ficheiro ter sido carregado no dispositivo, foi configurada a ligação T1 ISDN com o *kit Mombasa* como ilustra a Figura 23. Como é evidente as características da ligação são iguais às configuradas no *kit Mombasa* para o tipo de protocolo, código de linha e estrutura da trama. Depois de efectuados alguns ajustes na configuração da ligação, que serão indicados mais adiante, foi obtido o sincronismo com o *kit Mombasa* que pode ser provado na Figura 23 através da sinalização verde no *trunk* #1 correspondente ao conector #1 RJ48c da Mediant™ 2000.

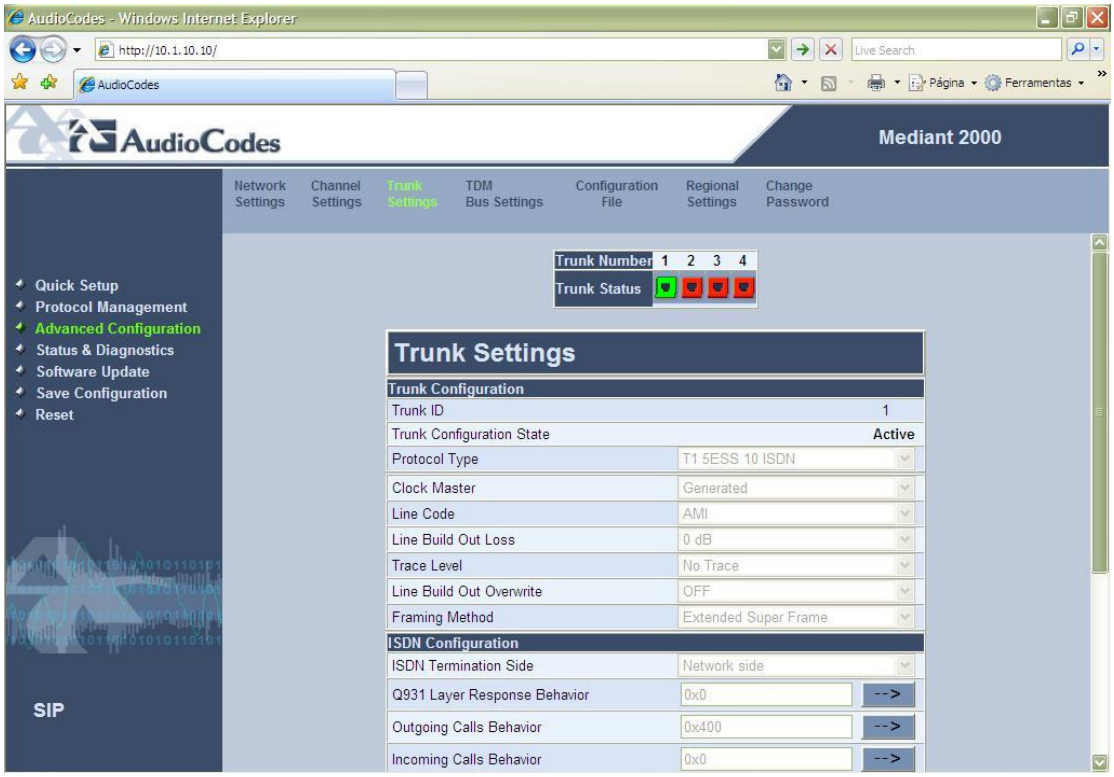



Figura 23- Configuração da ligação T1 ISDN com o *kit Mombasa*.

Para realizar chamadas entre o *softphone X-Lite* 3.0 e os POTS tendo em conta o cenário da Figura 20, foi necessário configurar as tabelas de *routing* internas da Mediant™ 2000. Estas tabelas são muito importantes, pois permitem atribuir políticas e decisões no encaminhamento da chamada até ao destino correcto tendo em conta o número ou gama de números do originário e do destinatário, e ainda atribuir perfis de parâmetros comuns a cada encaminhamento, como por exemplo, o tipo de *codec* a utilizar para todas as chamadas originadas por um determinado utilizador ou conjunto de utilizadores para um determinado destino. Desta forma, foram configuradas as tabelas de *routing* de ISDN para IP e IP para ISDN de acordo com a Figura 24 e Figura 25 respectivamente.

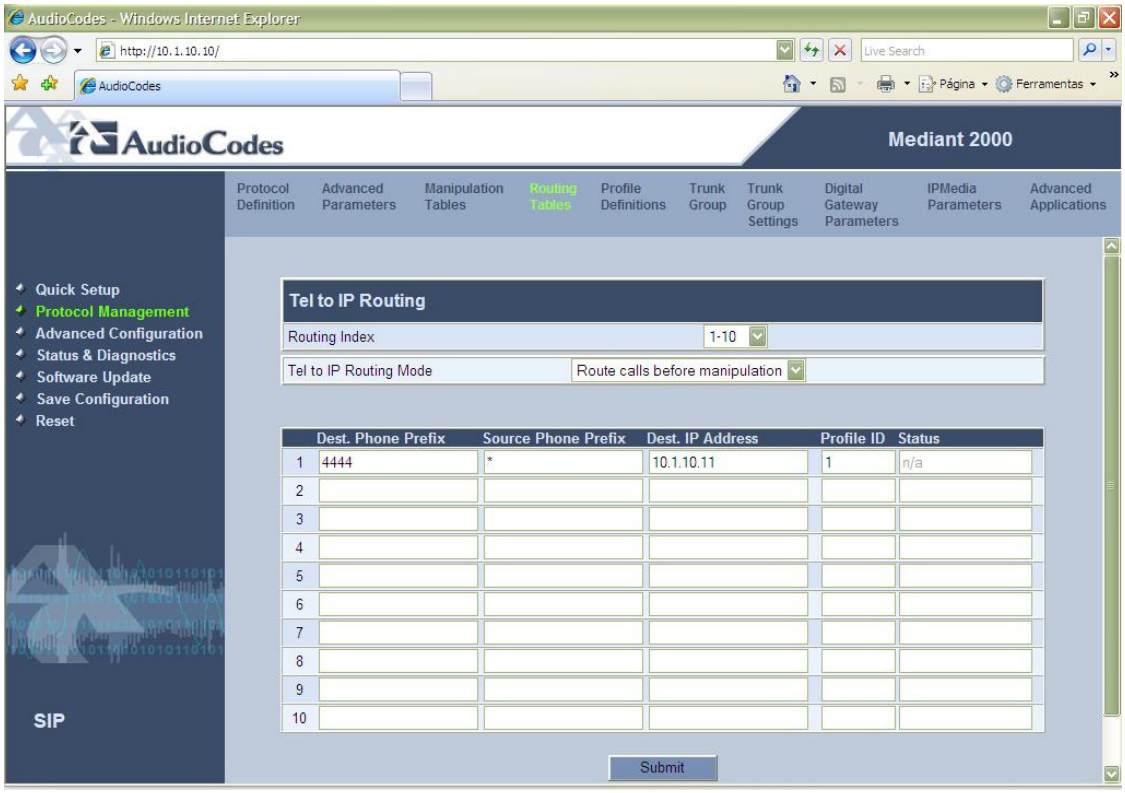



Figura 24- Tel *to* IP *Routing* para o Cenário I dos testes *standalone*.

A Figura 24 mostra que todas as chamadas de ISDN para IP cujo o número do destinatário comece por "4444", são encaminhadas para o terminal IP de endereço 10.1.10.11, independentemente do número de quem originou a chamada[17]. Neste caso o terminal IP é um computador com o *softphone X-Lite* 3.0 configurado com o número "4444" de acordo com o cenário da Figura 20. Todas as chamadas de ISDN para IP que validam este *routing*, utilizam, preferencialmente, o *codec* de voz G.711 *μ-law* [59] de 64 kbps e como secundário o *codec* G.723.1 [64], ambos configurados para o *Profile* ID 1 como indicado no Anexo II.

[17] O "*" na Figura 24 significa que pode ser qualquer número.

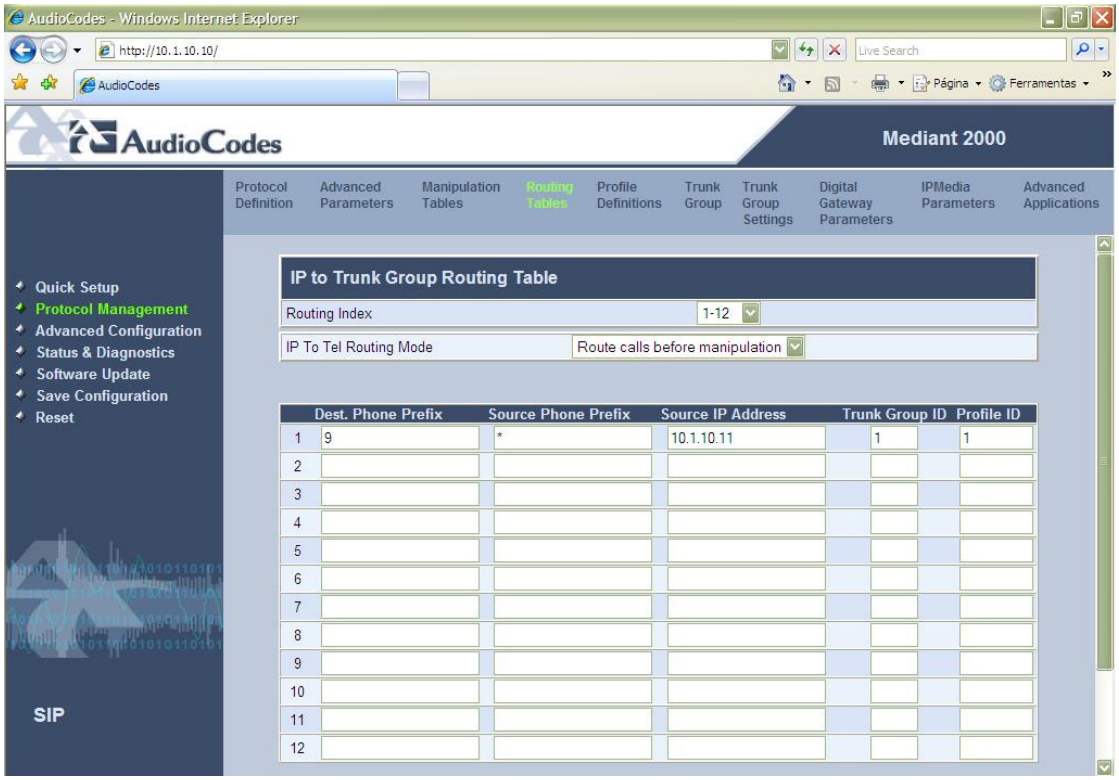



Figura 25- IP *to* Tel *Routing* da para o Cenário I dos testes *standalone*.

Na Figura 25 a tabela de *routing* está configurada para que todas as chamadas de IP para ISDN, cujo o número do destinatário comece por "9" e o terminal IP de origem possua o endereço 10.1.10.11, sejam encaminhadas para o *trunk* ID 1 ISDN, independentemente do número de quem originou a chamada do lado IP. O prefixo "9" corresponde ao número PRI do *kit Mombasa* PBX. Sendo assim, sempre que se pretenda efectuar uma chamada de ISDN para um dos POTS, por exemplo, utilizando o *kit* como PBX, deve-se marcar inicialmente o número do PBX, neste caso o "9", seguido do número "2334" ou "2335" consoante o POTS. Tal como na Figura 24, também foi definido para este *routing* o *Profile* ID 1, ou seja, todas as chamadas de IP para ISDN que obedeçam a esta configuração de *routing*, utilizam, preferencialmente, o *codec* de voz G.711 *μ-law* [59] de 64 kbps e como secundário o *codec* G.723.1 [64].

Embora não estejam indicados no Anexo II, há outros parâmetros importantes que foram deixados com a definição de fábrica, o porto SIP e RTP, e o protocolo de transporte utilizado:

- SIP UDP *port*: 5060 (*default*);
- RTP UDP *port*: 6000 (*default*).

Os parâmetros *ProtocolType_0* = 13 e *LineCode_0* = 1 indicados no Anexo II, são códigos correspondentes à sinalização T1 5ESS 10 ISDN para o tipo de protocolo e ao *Alternate Mark Inversion* (AMI) para o código de linha, respectivamente, configurados para o *trunk* #1 da Mediant™ 2000, segundo o manual de utilizador [105].

De seguida, foi configurado o terminal IP da mesma forma que a Figura 21 ilustra, só que neste caso, para o cenário da Figura 20, nas definições de rede do computador foi alterado o endereço IP para 10.1.10.11 e no *sofphone X-Lite* 3.0 foi alterado o *domain* para o IP 10.1.10.10 da Mediant™ 2000.

Com o cenário de testes da Figura 20 montado, foram realizados alguns testes simples de chamadas IP para ISDN e ISDN para IP a fim de averiguar se a configuração de cada um dos dispositivos e a comunicação entre cada um deles estava de acordo com o pretendido. Para os testes IP para ISDN foram efectuadas: chamadas para um número de destino válido, ou seja, para os números "9 2334" e "9 2335"; uma chamada para ISDN sem marcar inicialmente o dígito "9" para efectuar a ligação ISDN com o *kit*, ou seja, marcação dos números "2334" e "2335" sem marcar o dígito "9" primeiro; e uma chamada para um número de destino inválido, ou seja, marcação de um número diferente de "2334" ou "2335", sempre com a marcação inicial do dígito "9". Para os testes ISDN para IP, foi efectuada uma chamada para um número IP válido, ou seja, do POTS 1 "2334" e do POTS 2 "2335" para o número do *X-Lite* "4444", e uma chamada para um número IP inválido, diferente de "4444".

O segundo cenário, no âmbito dos testes *standalone*, está ilustrado na Figura 26. A diferença deste cenário para o da Figura 20, é a ligação de três computadores, em que cada um tem configurado uma conta no *X-Lite* 3.0, à Mediant™ 2000 através da rede IP 193.136.93.0. As configurações para a ligação ISDN entre o *kit Mombasa* e a Mediant™ 2000 permaneceram inalteradas, só mudou a configuração dos computadores com o *X-Lite* e da Mediant™ 2000 para o lado IP. A finalidade deste cenário foi configurar a Mediant™ 2000 para a realização de chamadas de audioconferência entre os três *softphones* e os POTS ligados ao *kit* e analisar, de uma forma perceptível, a qualidade de alguns *codecs* de voz num cenário de maior tráfego IP.

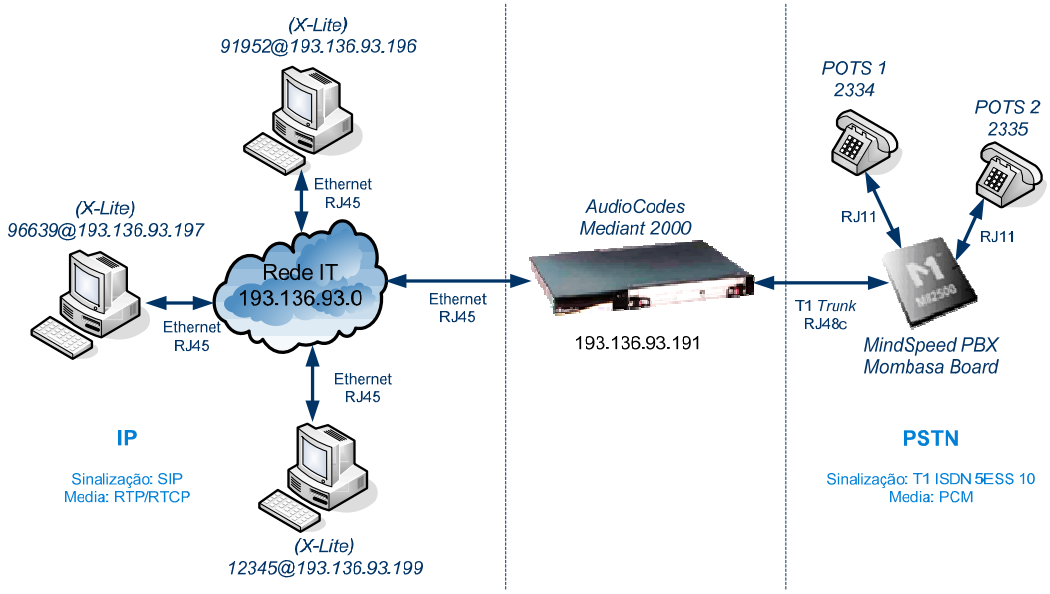



Figura 26- Cenário II dos testes *standalone*.

Neste sentido alterou-se a configuração de rede para o endereço IP estático 193.136.93.191 e *default gateway* 193.136.93.1 para ligar este elemento à rede pretendida.

De seguida configuraram-se também as tabelas de *routing* ISDN para IP e IP para ISDN da mesma forma que para o cenário I, tendo em conta, neste caso, o cenário II da Figura 26 para a realização de chamadas entre os POTS e os *softphones X-Lite* 3.0. Esta configuração está ilustrada nas Figura 27 e Figura 28.

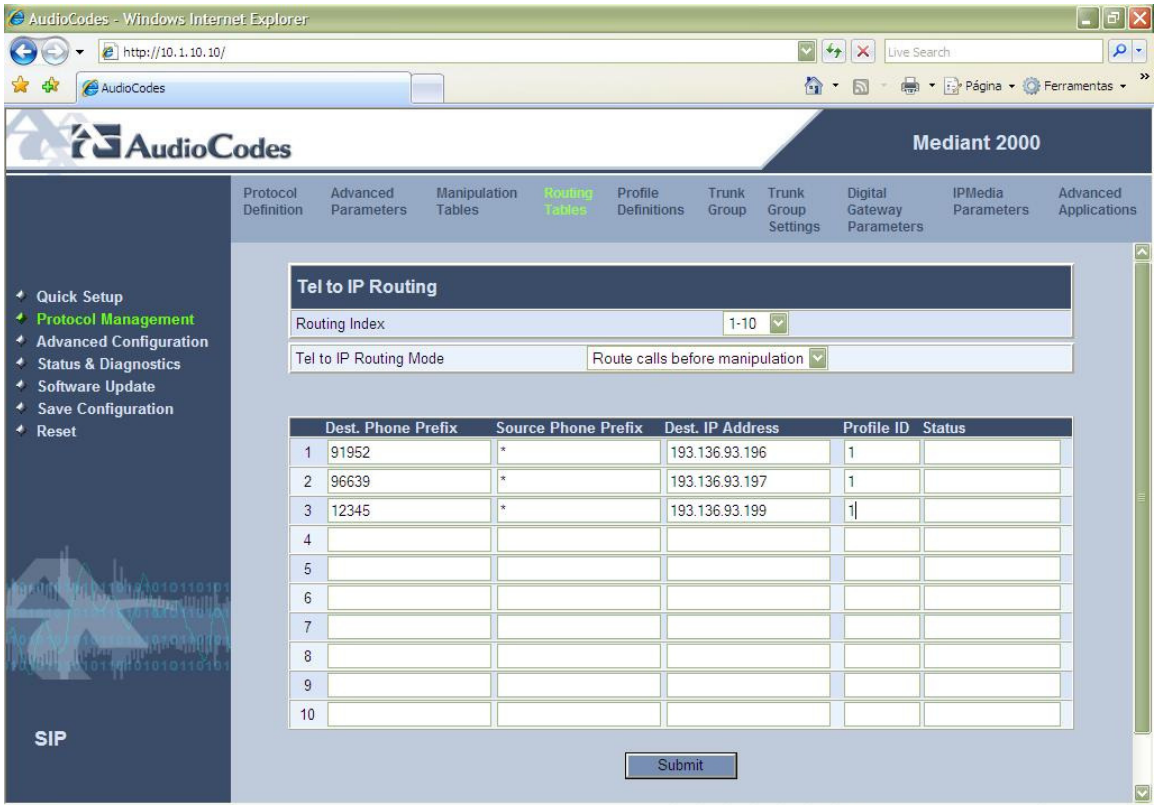



Figura 27- *Tel* to IP *Routing* para o Cenário II dos testes *standalone*.

A configuração da Figura 27 pretende demonstrar o cenário em que uma chamada de qualquer POTS do *kit Mombasa* é encaminhada para: o computador com o endereço 193.136.93.196 se o destinatário for o *X-Lite* 3.0 como o número "91952"; ou para o computador com o endereço 193.136.93.197 se o destinatário for o *X-Lite* 3.0 com o número "96639"; ou para o computador 193.136.93.199 se o destinatário for o *X-Lite* 3.0 com o número "12345", de acordo com os requisitos ilustrados na Figura 26.

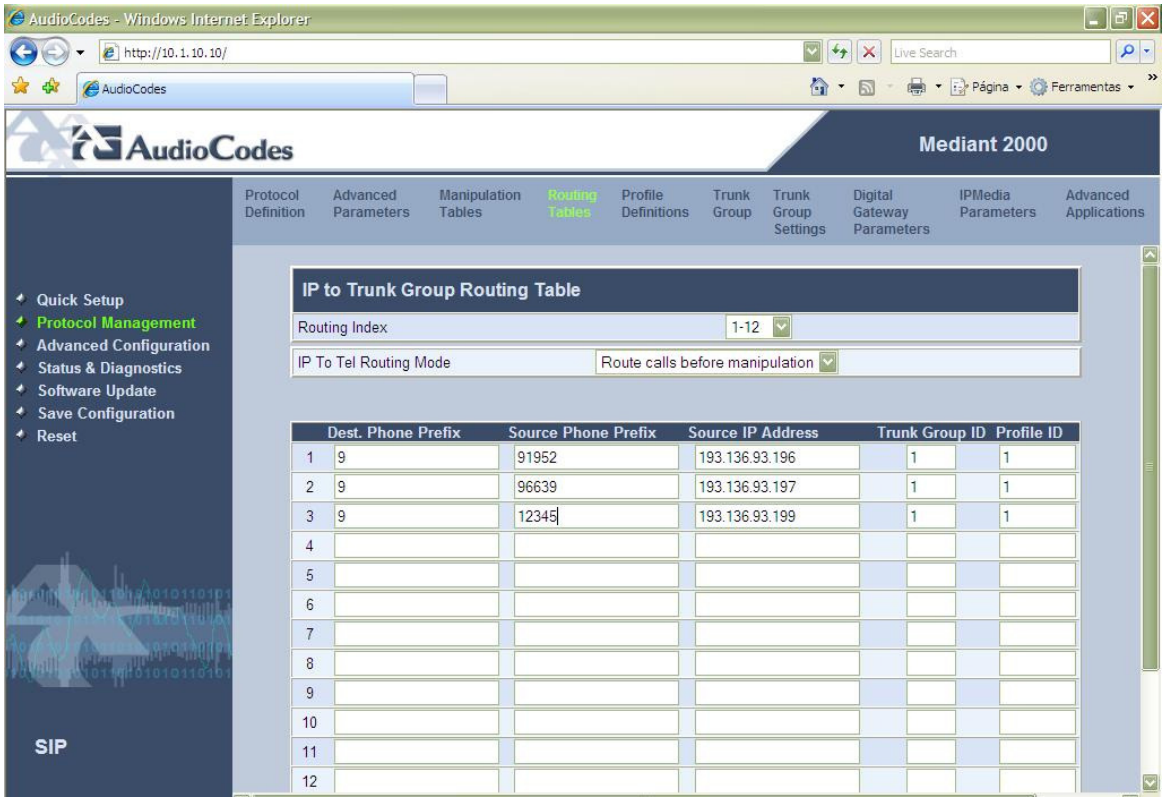



Figura 28- IP to *Tel Routing* para o Cenário II dos testes *standalone*.

A tabela de *routing* da Figura 28 indica que todas as chamadas originadas pelos *X-Lite's* 3.0 dos computadores, cujos endereços IP são 193.136.93.196, 193.136.93.197 e 193.136.93.199, e o número de destinatário comece pelo dígito "9", correspondente ao número PRI do *kit Mombasa*, são enviadas para o *kit Mombasa* através da ligação ISDN.

Os restantes parâmetros foram deixados iguais aos configurados para o cenário I, bem como os perfis dos *codecs* definidos para as chamadas que estejam de acordo com as tabelas de *routing*.

Após esta configuração da Mediant™ 2000, procedeu-se à sua ligação física directamente à rede IP. Para os terminais IP, configuraram-se três computadores com os seguintes endereços estáticos: 193.136.93.196, 193.136.93.197 e 193.136.93.199. Os *default gateway* das definições de rede de cada um deles foram configurados com o mesmo endereço do configurado para a Mediant™ 2000. Os *softphones X-Lite's* 3.0 foram configurados de igual forma que no cenário anterior com as seguintes contas: "91952" para o 193.136.93.196, "96639" para o 193.136.93.197 e "12345" para o 193.136.93.199. O *domain* é o mesmo para todos os *softphones* e igual ao endereço IP da Mediant™ 2000.

Com o cenário de testes da Figura 26 implementado, foram realizados alguns testes de audioconferência entre os participantes POTS 1 "2334" e os *softphones* "91952" e

"12345". Tendo o cenário II uma rede IP com maior tráfego em comparação com o cenário I, seria este cenário o mais indicado para efectuar testes a alguns *codecs* recomendados pelo TISPAN. Para isso realizaram-se chamadas entre o POTS 1 e o *X-Lite* 3.0 "91952" utilizando os *codecs* G.711 *μ-law*, G.711 *A-law*, G.723, G.726, G.729 e GSM, definidos na Mediant™ 2000.

Na elaboração destes cenários de testes *standalone* para familiarização com os principais parâmetros envolvidos nos sistemas VoIP, foram encontradas algumas dificuldades na configuração, destacando-se principalmente a configuração da ligação ISDN de comunicação entre a Mediant™ 2000 e o *kit Mombasa*. Foram testadas várias combinações de tipos de protocolos de sinalização, de códigos de linha e de estruturas de trama, numa tentativa de encontrar a melhor configuração ISDN para a sincronização entre estes dois dispositivos. Embora o tipo de sinalização e código de linha configurados não sejam muito utilizados hoje em dia nas redes PSTN/ISDN, foi o suficiente para possibilitar a realização de alguns testes e adquirir conhecimento na configuração de alguns parâmetros para cenários futuros. Foram também efectuados alguns ajustes na fonte do relógio de sincronismo, ficando a Mediant™ 2000 com o gerador do relógio para a rede, e o *kit Mombasa* como terminal ISDN receptor desse relógio para sincronização.

### 5.4.1. Resultados dos testes standalone

De seguida são apresentados os resultados de alguns testes mais relevantes efectuados nos cenários I e II de testes *standalone*.

Utilizando o cenário I foi feita uma chamada simples do *softphone X-Lite* 3.0 "4444" para o POTS 1 "2334" e para o POTS 2 "2335". Para isso marcou-se no *X-Lite* 3.0 o dígito "9" e efectuou-se a chamada só com este dígito para estabelecer a ligação ISDN entre o *kit Mombasa* e a Mediant™ 2000. Após estabelecida esta ligação marcou-se no *X-Lite* 3.0 o número "2334". A chamada foi estabelecida como seria de esperar, com sinal de chamada no *softphone* e sinal de alerta *Ringing* no POTS 1. Foi efectuado o *off-hook* do POTS 1 e estabelecida a conversação com boa qualidade entre os dois intervenientes. Repetiu-se o mesmo processo para o POTS 2 "2335". Relativamente à terminação da chamada também correu como seria de esperar, tanto do lado POTS como do lado *X-Lite* 3.0, ficando o utilizador que não cessou a sessão com o sinal de ocupado.

Efectuou-se este mesmo teste de IP para ISDN, só que neste caso não se marcou inicialmente o dígito "9". Como seria de esperar neste caso, a chamada não correu com

sucesso. Ao marcar no terminal *X-Lite* 3.0 o número "2334" ou o "2335", como a ligação ISDN entre o *kit* e a Mediant™ 2000 ainda não tinha sido estabelecida, ocorreu uma falha na chamada ficando o sinal de ocupado no *X-Lite* 3.0, logo após a tentativa de estabelecimento. O mesmo se sucedeu quando se marcou um número diferente do "9 2334" ou do "9 2335".

Para os testes POTS para IP, foi efectuada uma chamada com sucesso do POTS 1 "2334" e do POTS 2 "2335" para o *X-Lite* 3.0. Após a marcação do número "4444" tocou o sinal de chamada no POTS e de alerta *Ringing* no *X-Lite* 3.0. Todo este processo de estabelecimento correu dentro da normalidade. Após o atendimento por parte do *softphone*, foi estabelecida uma conversação de boa qualidade entre estas entidades. Foi efectuado também um teste de falha através da marcação no POTS 1 de um número diferente de "4444". Como seria de esperar, a chamada não foi estabelecida, ficando retida na Mediant™ 2000, pois não obedece a nenhuma entrada da tabela de *routing* da Figura 24.

O cenário II foi utilizado para a realização de um teste de audioconferência entre o POTS 1 e os *softphones X-Lite* 3.0 "91952" e "12345" da Figura 26. Para o seu estabelecimento no *kit Mombasa*, esta plataforma possui configurado um número que todas as entidades participantes devem marcar para entrar na audioconferência. Este número é o "8334", segundo a configuração do ficheiro "*sipbx_linux.conf*" do *kit*, apresentado no Anexo I. Para os testes de *codecs*, efectuou-se uma chamada entre o *softphone X-Lite* 3.0 "91952" e o POTS 1 para cada *codec* da Tabela X configurado na Mediant™ 2000. Com este conjunto de testes pretende-se analisar o impacto de cada *codec* de voz na conversação de uma forma perceptível.

| ***Codec*** | **G.711 *μ-law*** | **G.711 *A-law*** | **G.723** | **G.729** | **G.726** | **GSM** |
|---|---|---|---|---|---|---|
| **Estado** | Boa Qualidade | Perceptível mas com algumas falhas | Não disponibilizado pelo *X-Lite* 3.0 | Não disponibilizado pelo *X-Lite* 3.0 | Não disponibilizado pelo *X-Lite* 3.0 | Muito ruído |

Tabela X- Testes de *codecs* no cenário II.

Pela análise da Tabela X, comprovou-se que o *codec* G.711 *μ-law* neste cenário se revelou o melhor em termos de qualidade de conversação, pois é o que apresenta menor taxa de compressão dos dados e por conseguinte maior débito binário (64 kbps). O correspondente *A-law* revelou uma conversação perceptível mas com algumas falhas, pois utiliza um

algoritmo de compressão diferente em relação ao utilizado no lado ISDN para a ligação T1, *μ-law*. O facto de existir uma conversão destes algoritmos poderá desencadear algumas perdas de dados resultando em falhas na conversação. O *codec* GSM mostrou-se o de menor qualidade pois apresentou muito ruído e falhas durante a conversação. É o *codec* com menor débito, na ordem dos 13 kbps, e com fracos algoritmos de compressão o que envolve menos complexidade.

## 5.5. Sumário

O principal objectivo do capítulo 5 foi dar a conhecer as potencialidades e características mais relevantes de alguns produtos adquiridos, que implementam fisicamente os elementos funcionais da arquitectura PES do TISPAN, bem como a familiarização com os principais parâmetros de configuração.

Para os testes *standalone* em questão foram criados dois cenários com a Mediant™ 2000 da AudioCodes® e o *kit Mombasa* da Mindspeed®. O primeiro cenário é muito simples, composto por estes elementos ligados directamente entre si através de uma interface T1 e um *softphone* IP *X-Lite* 3.0 ligado à Mediant™ 2000. O segundo cenário difere do primeiro relativamente ao IP, pois é composto por três *softphones* IP *X-Lite* 3.0 ligados à Mediant™ 2000 através da rede IP 193.136.93.0.

Estes cenários foram configurados para a realização de alguns testes de chamadas entre os POTS ligados ao *kit Mombasa*, e entre os *softphones X-Lite* 3.0 e os POTS. O cenário II, dado a ligação a uma rede IP com algum tráfego, também foi utilizado para o estudo do comportamento de alguns *codecs* de voz que poderão ser utilizados em chamadas.

# Capítulo 6: Realizações Práticas com o Demonstrador *SHipNET*

Após a familiarização com as potencialidades de cada um dos equipamentos e as suas principais configurações físicas e funcionais, vários testes e cenários intermédios foram realizados subsequentemente para o estudo do comportamento dos elementos até chegar a uma primeira versão para os sistemas *Trunking* e de Acesso do demonstrador *Service Handling on ip NETworks* (*SHipNET*®).

Dentro do contexto das Redes de Próxima Geração (RPGs) foi criada uma nova linha de sistemas de suporte a uma plataforma aplicacional, designada por *SHipNET*® [84], com acesso universal através de interfaces abertas, que consegue servir diversos tipos de domínios de redes de acesso. Os referidos produtos de suporte a essa plataforma, responsáveis pela criação das condições necessárias para que o acesso aos domínios seja efectuada de forma transparente, são baseados nos elementos das RPGs que se encontram presentemente a serem definidos nas normas do 3rd *Generation Partnership Project* (3GPP) IP *Multimedia Subsystem* (IMS) para redes móveis, bem como no *Telecommuncations and Internet converged Services and Protocols for Advanced Networking* (TISPAN) [20] para redes fixas.

Cabe no âmbito deste projecto de Mestrado a implementação do sistema responsável pela interligação das redes *Public Switched Telephone Network/Integrated Services Digital Network* (PSTN/ISDN) (sistema *Trunking*) e das redes fixas de acesso *Digital Subscriber Line* (DSL) (sistema de Acesso) a este demonstrador *SHipNET*®, tendo por base a arquitectura PSTN/ISDN *Emulation Subsystem* (PES) ilustrada na Figura 15.

Resumidamente, o principal objectivo desta Dissertação é a implementação e configuração física e funcional dos elementos a azul da Figura 29 para o demonstrador *SHipNET*®. Mas antes de atingir o objectivo final, vários objectivos intermédios foram impostos durante o

desenvolvimento que se traduzem por vários cenários e testes intermédios até chegar ao cenário final *SHipNET*®.

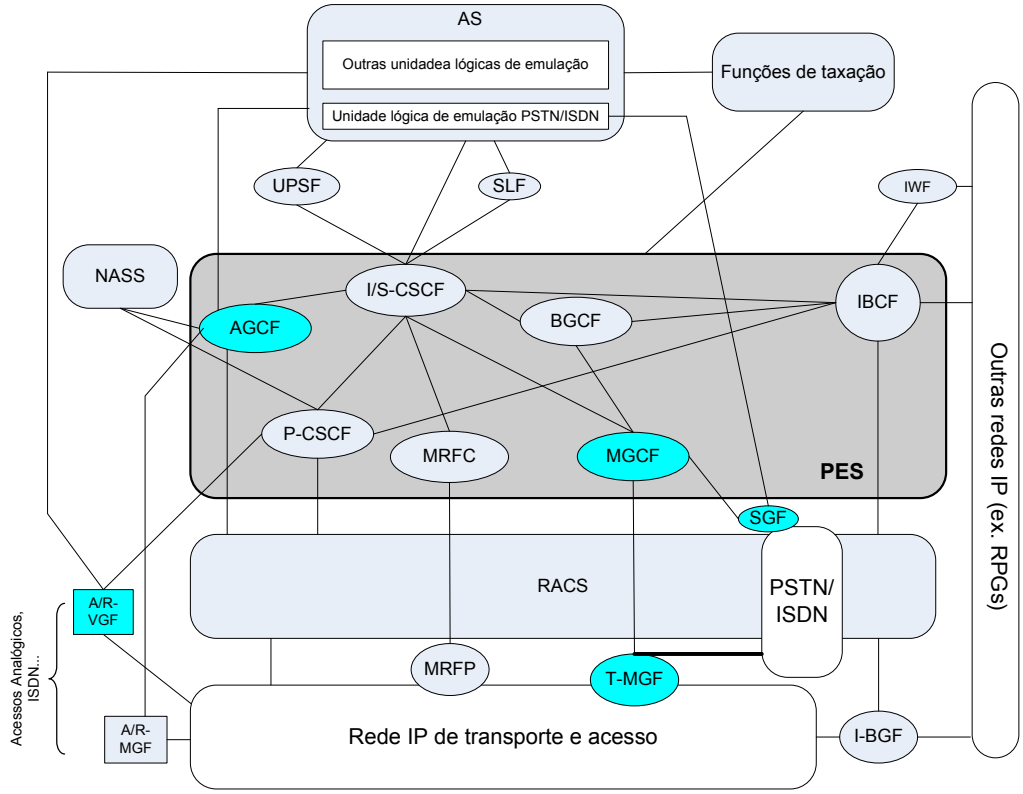



Figura 29- Elementos da arquitectura PES TISPAN a implementar.

Este capítulo pretende implementar um cenário como resposta aos principais requisitos impostos pelo organismo TISPAN para os sistemas *Trunking* e de Acesso da arquitectura PES. Este está organizado em duas secções principais, uma para o sistema *Trunking* (ip-*Keel*® *Trunking*) e outra para o sistema de Acesso (ip-*Keel*® Acesso). Na secção ip-*Keel*® *Trunking* será feita uma descrição da montagem e configuração dos dispositivos constituintes de cada um dos cenários intermédios (cenário de testes interno e Amora) até ao cenário final com o demonstrador RPG *SHipNET*®. No final de cada cenário serão indicados os testes realizados, bem como os resultados obtidos. A secção ip-*Keel*® Acesso está dividida em duas partes, uma para o sistema baseado em *Session Initiation Protocol* (SIP) e outra para o sistema baseado em *MEdia GAteway COntrol* (MEGACO)/H.248. Na secção para o sistema baseado em SIP será feita uma descrição da implementação de um *Access-VoIP Gateway Function* (A-VGF) da arquitectura PES para o cenário *SHipNET*®, e para o sistema baseado em MEGACO/H.248 a implementação do processo de registo SIP para o componente *Access Gateway Control Function* (AGCF) da arquitectura PES.

Antes da descrição de cada um destes cenários de testes será feita de seguida uma abordagem ao demonstrador *SHipNET*® dando maior ênfase ao componente ip-*Keel*®, sendo a referência para os sistemas *Trunking* e de Acesso desta Dissertação.

## 6.1. Demonstrador SHipNET

A arquitectura IMS assume um papel relevante, sendo figura central na criação e desenvolvimento global de um demonstrador RPG, designado por *SHipNET*®, actualmente em curso no âmbito do projecto *Converged Multimedia System* (CMS). Este demonstrador pretende integrar de forma evolutiva dispositivos físicos que possuem as funcionalidades dos elementos constituintes da arquitectura RPG ilustrada na Figura 11, de forma a criar uma plataforma para demonstrações das potencialidades dos componentes constituintes, de soluções e de serviços multimédia convergentes.

Os vários elementos do demonstrador *SHipNET*® foram agrupados de acordo com a Figura 30. Assim o demonstrador pode ser dividido em vários conjuntos: ip-*Keel*®, ip-*Deck*®, ip-*Cockpit*®, ip-*Compass*®, ip-*Windless*®, ip-*Deck*®, ip-*Hatch*®, ip-*Rudder*® e ip-*Tiller*® [84].

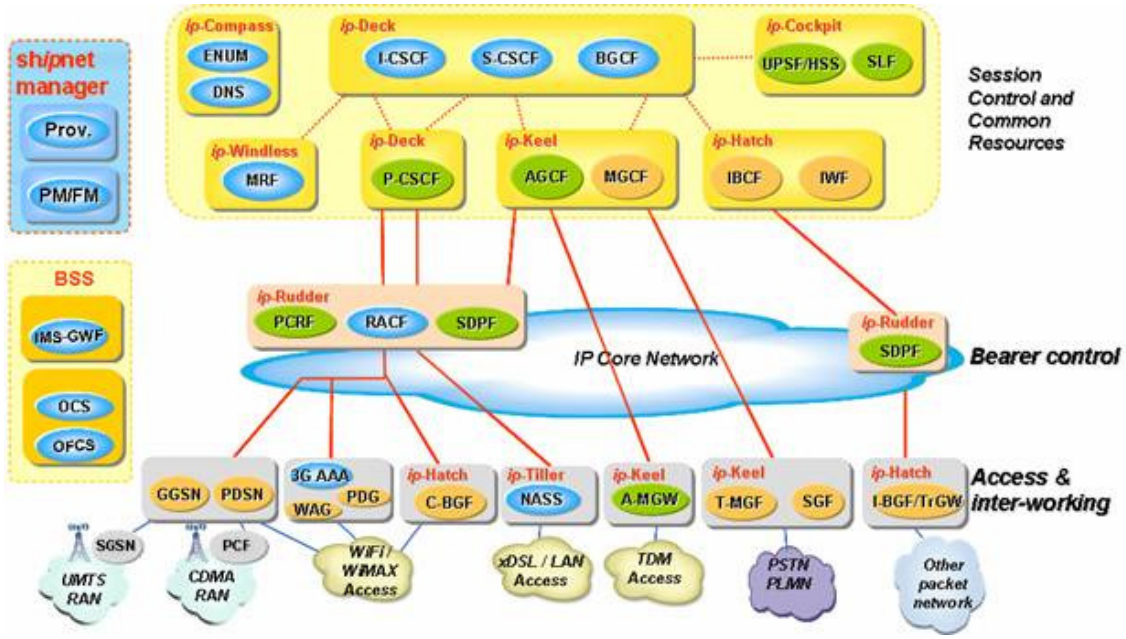



Figura 30- Demonstrador *SHipNET*® [84].

No âmbito do trabalho experimental desta Dissertação, foi implementado o ip-*Keel*® formado pelos elementos: *Media Gateway Control Function* (MGCF), *Signalling Gateway Function* (SGF), *Trunking-Media Gateway Function* (T-MGF), *Access-Media Gateway Function* (A-MGF) e AGCF da arquitecta PES do TISPAN. Para melhor compreensão do trabalho realizado, o ip-*Keel*® foi dividido em dois conjuntos: o ip-*Keel*® *Trunking* e o ip-

*Keel*® Acesso; em concordância com os sistemas *Media Gateway* de *Trunking* e de Acesso da Figura 29 [84].

## 6.2. ip-Keel Trunking

Para efeitos demonstrativos em diferentes cenários de testes da evolução desta solução até chegar ao ip-*Keel*® do *SHipNET*®, foi utilizado para o elemento T-MGF e SGF a solução Mediant™ 2000 da AudioCodes®, e para o elemento MGCF a solução openCallAgent® da OpenTelecommunications® [106].

### *6.2.1. openCallAgent*

Nesta secção será feita uma breve descrição dos principais módulos internos que compõem o openCallAgent® 3.1.12, bem como das características mais relevantes e dos principais parâmetros de configuração imprescindíveis para o bom funcionamento deste produto da OpenTelecommunications®.

A função de MGCF é realizada por este *software* openCallAgent® 3.1.12, instalado fisicamente numa plataforma *workstation blade*® 1000 da SUN® com o sistema operativo Solaris 2.8, conforme os requisitos de instalação indicados no manual de utilizador [107]. Para desempenhar essa função, este *software* possui basicamente um processo de controlo de sessões e três *stacks* elementares que implementam as interfaces de sinalização SIP, H.323, *Media Gateway Control Protocol* (MGCP) e ISDN *User Part* (ISUP) com os restantes elementos da arquitectura. O openCallAgent® interliga utilizadores SIP, H.323 e Sistema de Sinalização #7 (SS7) PSTN entre si para poderem estabelecer serviços de voz, FAX, etc. Para isso devem ser configuradas rotas para cada um dos tipos de sinalização SIP e ISUP tendo em conta a chamada ou serviço em questão. Tomando o exemplo de uma chamada de voz da rede PSTN para IP, a aplicação openCallAgent® analisa a informação contida no ISUP (destinatário, origem, tipo de chamada, variante de sinalização, etc.), e caso esteja de acordo com alguma das rotas SIP de saída configuradas, constrói a respectiva mensagem SIP e envia para o SIP *proxy*, para o SIP IP *Centrex* ou para o SIP *softswitch* correspondente. O processo é idêntico mas de forma inversa no caso de uma chamada de IP para PSTN. Nas secções seguintes referentes à configuração dos vários cenários de testes, será descrito mais detalhadamente como se configuram rotas SIP e ISUP no openCallAgent®.

De acordo com o manual de utilizador [107], esta aplicação suporta os seguintes protocolos de sinalização:

- ISUP (variantes: ANSI, ITU-T, ETSI v2, SWEDISH e G500);
- *Message Transfer Part* 3 *User Adaptation layer* (M3UA) [38]/*Stream Control Transmission Protocol* (SCTP) para o transporte da sinalização ISUP sobre IP de acordo com o especificado pelo grupo *Signalling Transport* (SIGTRAN);
- H.323 [49];
- MGCP v.1.0, especificado no *Request For Comment* (RFC) 3435 [91], para o controlo dos recursos *media* de T-MGFs, de *Network Access Servers* (NASs) e de *Media Servers* (MSs);
- SIP de acordo com o RFC 3261 [32] e extensões indicadas na Tabela XI.

| RFC | Descrição |
|---|---|
| RFC 3262 [108] | Método *PRACK* (*Provisional Response Acknowledgest*) |
| RFC 3264 [55] | Modelo oferta/resposta |
| RFC 3265 [109] | Método *Notify* |
| RFC 2327 [54] | *Session Description Protocol* (SDP) |
| RFC 3515 [110] | Método *Refer* |
| RFC 2976 [111] | Método *Info* |

Tabela XI- Extensões SIP suportadas pelo openCallAgent® 3.1.12.

Da análise da sinalização suportada pelo openCallAgent®, conclui-se que existem algumas divergências relativamente ao especificado para o elemento MGCF da arquitectura PES (Figura 15). Para a interface com a rede SS7 PSTN só é suportado o protocolo ISUP, o *Transaction Capabilities Application Part* (TCAP), para serviços suplementares como o *Call Control on Busy Subscriber* (CCBS) em cenários futuros, não é suportado por esta aplicação. Outro facto bastante importante é a utilização do protocolo MGCP v.1.0 de controlo invés ao MEGACO/H.248 especificado pelo PES do TISPAN para esta interface. Relativamente ao protocolo SIP, não são suportadas as seguintes extensões (métodos) da Tabela II: *Publish* [112], *Subscribe* [109], *Update* [113] e *Message* [114]; nem a extensão SIP-I [79] definida para arquitectura PES.

O openCallAgent® também suporta algumas funcionalidades básicas especificadas pelo 3GPP e pelo *European Telecommunications Standard Institute* (ETSI) para o elemento MGCF:

- Suporte de sessões FAX utilizando o protocolo T.38 [92];
- Passagem de anúncios no T-MGF sob o controlo MGCP;

- Geração e detecção de tons *Dual Tone Multi-Frequency* (DTMF) de acordo com o RFC 2833 [42];
- Suporte do serviço *Calling Line Identification Public* (CLIP) e *Calling Line Identification Restriction* (CLIR) de acordo com o RFC 3323 [115] e 3325 [116].

### 6.2.2. Cenário interno

A actividade de concepção do ip-*Keel*® *Trunking* como solução integrante da arquitectura RPG do TISPAN sofreu várias fases de desenvolvimento até chegar ao cenário final *SHipNET*®, que se traduzem por cenários de testes intermédios com o objectivo de dar a conhecer alguns parâmetros importantes na configuração dos dispositivos constituintes da solução ip-*Keel*® *Trunking*.

Inicialmente foi implementado o cenário de testes da Figura 31, designado por cenário interno. Este cenário é formado pelos elementos constituintes do conjunto ip-*Keel*® numa configuração simples de integração com a rede PSTN e por um terminal SIP emulado por um *softphone X-Lite* 3.0 ligado directamente. O principal objectivo deste cenário foi construir uma plataforma para a realização de testes simples de chamadas de voz entre um utilizador da rede pública PSTN e o terminal SIP. Este cenário foi muito importante para adquirir conhecimentos sobre a configuração da Mediant™ 2000 e do openCallAgent® para interligar a rede fixa PSTN com sinalização SS7.

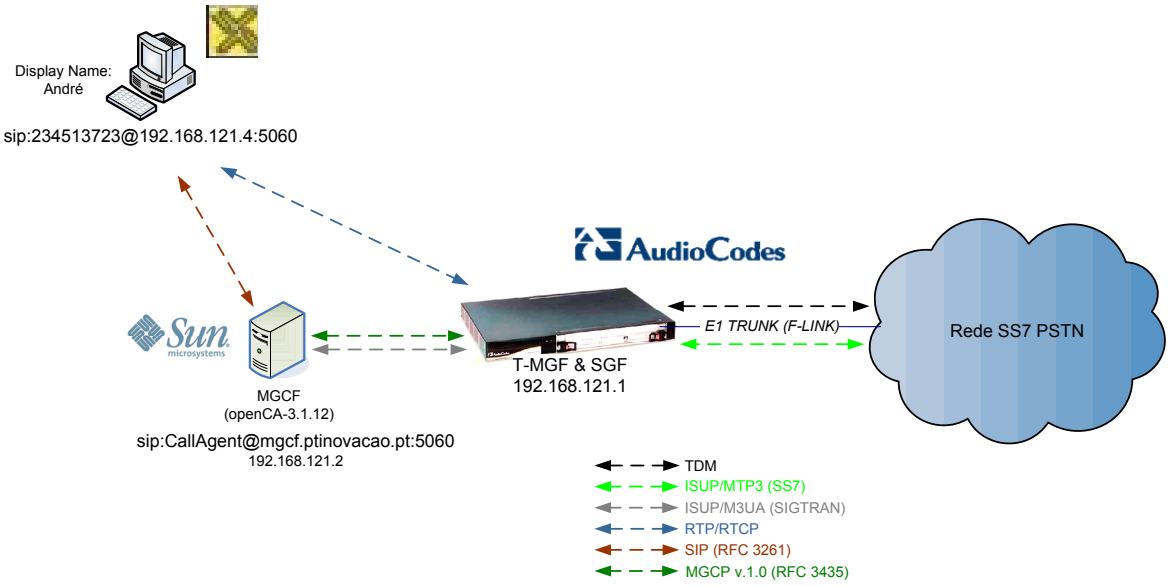



Figura 31- Cenário interno – ip-*Keel*® *Trunking*.

Fisicamente, os elementos Mediant™ 2000, *workstation* blade® 1000 com o openCallAgent®, e o computador com o *softphone X-Lite* 3.0 do cenário da Figura 31,

foram ligados directamente entre si através de um HUB para o lado IP, e para o lado PSTN, ligou-se a Mediant™ 2000, com função de SGF incorporada, a um comutador do PSTN com funcionalidades de *Service Switching Point* (SSP) da arquitectura SS7 [35], através do conector RJ48c *trunk* #1.

Após montado fisicamente o cenário da Figura 31, configuraram-se os parâmetros de cada um dos elementos, começando pelo elemento central do sistema *Trunking*, o MGCF openCallAgent®.

À *workstation* de suporte à aplicação foi atribuído o endereço IP estático 192.168.121.2, o *default gateway* 192.168.121.254 e o *Domain Name System* (DNS) 192.168.122.253. Estas definições de rede permanecerão iguais para os restantes cenários do ip-*Keel*® *Trunking*. Instalado o openCallAgent® de acordo com o manual de utilizador [107], configuraram-se os parâmetros para a ligação SIP com o *softphone X-Lite* 3.0, para a ligação ISUP, do protocolo SS7, com a rede PSTN, e para a ligação MGCP e M3UA/SCTP com a Mediant™ 2000. Relativamente ao SIP, foi configurada uma rota, através da linha de comandos do openCallAgent® [107], com o computador de suporte ao *X-Lite* 3.0 para a troca de mensagens SIP. A configuração desta rota está ilustrada na Figura 32.

```
DIS-SIP-ROUTE:ROUTE=sip_in_out;
COMMAND ACCEPTED

ROUTE         HOST            PORT    MAX-CALLS    ROUTE-OPTIONS
-------------------------------------------------------------------------------
sip_in_out    192.168.121.4   5060    30           AIRP             = sip_in_out_airp
                                                   CIDP             = first_cidp
                                                   ORNP             = NONE
                                                   TREATMENT-TABLE  =
                                                   ROUTE-GROUP      =
                                                   CPS              = DISABLED
                                                   CLIR             = NONE
                                                   CLIP             = TRUE
                                                   CLI-TRUSTED      = TRUE
                                                   PROXY            = NO
                                                   REGISTER         = NONE
                                                   ALLOW-REDIRECT   = YES
-------------------------------------------------------------------------------
```

Figura 32- Rota SIP para o cenário interno – ip-*Keel*® *Trunking*.

Esta figura mostra que a rota SIP *sip_in_out* do openCallAgent® foi configurada para a entrada e saída de mensagens SIP com o endereço:porto IP 192.168.121.4:5060, tratando-se do computador com o *softphone X-Lite* 3.0 segundo o cenário da Figura 31. Também se pode verificar que esta rota pode processar no máximo 30 chamadas em simultâneo com esse terminal (a Mediant® 2000 possui apenas o *trunk* E1 #1 activo com 30 *time-slots* ou circuitos). Os parâmetros CLIP e CLI-TRUSTED estão igual a "TRUE", e o CLIR igual a "NONE", pois, segundo o manual do utilizador [107], esta configuração implica que a

identificação do originário das chamadas que entram na rota só seja mostrada consoante os parâmetros de privacidade contidos na mensagem. Também foi adicionada a esta rota um *dial plan*, através do parâmetro *Collect Information Dial Plan* (CIDP), para todas as chamadas. Assim, caso uma chamada de entrada ou saída do openCallAgent® cujo o número do originário e/ou destinatário não obedeça a um *dial plan* configurado, esta não é processada por essa rota. Juntamente com CIDP também foi configurado um plano de *routing* para esta rota SIP através do parâmetro *Analyse Information Routing Plan* (AIRP). Este parâmetro introduz critérios que condicionam o *routing* das chamadas por essa rota através da análise e comparação de alguns valores contidos nas mensagens. A configuração do CIDP e do AIRP para esta rota SIP será descrita mais a baixo.

Para a ligação de controlo MGCP com a Mediant™ 2000, foi adicionado um "*Media Gateway*" no openCallAgent® de acordo com a Figura 33.

```
LST-MGCP-MG;
COMMAND ACCEPTED

MG                    NC          VENDOR        PREFERRED-MS    STATUS
-------------------------------------------------------------------------
m2k-ptinovacao.pt     CISCO_E1    audiocodes                    IN SERVICE
```

Figura 33- Ligação de controlo MGCP para o cenário interno – ip-*Keel® Trunking*.

Este "*Media Gateway*" tem o nome *m2k-ptinovacao.pt*. Para o openCallAgent® poder resolver este nome, ou seja, traduzir no respectivo endereço IP para a comunicação, foi introduzido uma entrada no ficheiro "*/etc/hosts*" da *workstation* contendo o nome *m2k-ptinovacao.pt* e o respectivo endereço IP 192.168.121.1. O parâmetro *Naming Convention* (NC) foi configurado com o valor "CISCO_E1" (Figura 33). Este parâmetro indica a convenção a utilizar para o nome de identificação dos *endpoints* na Mediant™ 2000.

A configuração do openCallAgent® para a ligação com o SGF da Mediant™ 2000 possui vários passos intermédios desde a configuração do protocolo M3UA até ao ISUP. Inicialmente foi configurada uma rota para o protocolo M3UA para transportar as mensagens ISUP sobre IP. Para isso adicionou-se um "*Signalling Gateway*" (SG) ao openCallAgent® conforme ilustra a Figura 34. Este SG de nome *m2k_sg* foi configurado com a variante *International Telecommunication Union* (ITU) para o protocolo *Message Transfer Part* 3 (MTP3) utilizado para a ligação SS7 entre a Mediant™ 2000 e a rede PSTN. Este passo foi necessário para posteriormente definir no openCallAgent® o *point code* associado ao sistema local (sistema *Trunking*), pois do ponto de vista da rede PSTN o sistema *Trunking* é visto como um *Signalling Node* (SN) da arquitectura SS7, e para a

definição, também, do *point code* associado ao sistema remoto, ou seja, *point code* do SN da rede PSTN ao qual liga a Mediant™ 2000.

```
LST-M3UA-SG;
COMMAND ACCEPTED

SG        M3UA-VERSION    MTP-PROTOCOL-VARIANT    STATUS
-------------------------------------------------------------
m2k_sg    RFC             ITU                     Active

DIS-M3UA-RK:ROUTING-KEY=ss7_route;
COMMAND ACCEPTED

ROUTING-KEY    NI    LOCAL-PC    REMOTE-PC-SET    STATUS
-------------------------------------------------------
ss7 route      2     3338        3328             Active

LST-M3UA-SGP;
COMMAND ACCEPTED

SGP        SG        LOCAL-ADDRESS    LOCAL-PORT    REMOTE-ADDRESSES    REMOTE-PORT    STATUS
-------------------------------------------------------------------------------------------------
m2k_sgp    m2k_sg    myASP            2905          192.168.121.1       2905           Up
```

Figura 34- Ligação SS7 para o cenário interno – ip-*Keel*® *Trunking*.

De seguida foi adicionado o *routing key* de nome *ss7_route* ao openCallAgent® que associa o *point code* do openCallAgent, configurado com 3338 (OPC – *Originating Point Code*), ao *point code* remoto, configurado com 3328 (DPC – *Destination Point Code*), para todas as mensagens. Esta configuração teve por base os requisitos SS7 da rede PSTN nacional ligada à Mediant™ 2000, indicados em anexo (Anexo III).

Ao SG *m2k_sg* configurado anteriormente, foi adicionado um processo responsável pela ligação SCTP entre o openCallAgent® (LOCAL-ADDRESS) e o SGF da Mediant™ 2000 (REMOTE-ADDRESS). Como já foi referido anteriormente, este protocolo SCTP é responsável, segundo a arquitectura SIGTRAN, pelo transporte da informação das camadas superiores do SS7 [35] sobre o protocolo M3UA.

Da mesma forma que foi criada uma rota SIP, também foi feito algo do género para o ISUP, através da rota *isup_route* da Figura 35. Esta configuração teve por base os requisitos especificados no Anexo III que serão descritos de seguida.

```
DIS-ISUP-ROUTE:ROUTE=isup_route;
COMMAND ACCEPTED

ROUTE          VARIANT       OPC     DPC     ROUTE-OPTIONS
-------------------------------------------------------------------------------
isup_route     ETSI_V2       3338    3328    AIRP              = isup_airp
                                             CIDP              = first_cidp
                                             ORNP              = NONE
                                             TREATMENT-TABLE   =
                                             ROUTE-GROUP       =
                                             CPS               = DISABLED
                                             CLIR              = NONE
                                             CLIP              = TRUE
                                             CLI-TRUSTED       = TRUE
                                             ECHO-CANCELLATION = NONE
                                             VAD               = NONE
                                             PTIME             = 0
                                             CODEC             =
                                             CODEC-CHOICE      = NONE
                                             VOICE-CALLS       = 4096
-------------------------------------------------------------------------------
```

Figura 35- Rota ISUP para o cenário interno – ip-*Keel*® *Trunking*.

A rota *isup_route* foi configurada para a troca de mensagens ISUP entre o openCallAgent® (OPC 3338) e o SN SS7 (DPC 3328).

A variante do protocolo ISUP utilizada foi o ETSI V2 [117] entre as restantes possibilidades indicadas no manual de utilizador [107]. Esta escolha vai ao encontro da variante utilizada na rede PSTN nacional (Anexo III). Os parâmetros CLIR, CLIP e CLI-TRUSTED, foram configuradas da mesma forma que na rota SIP. As opções de detecção de voz (VAD), cancelamento de eco (ECHO-CANCELLATION) e de escolha do *codec* (CODEC-CHOICE) foram configuradas com o valor "NONE", significando que estas funcionalidades foram deixadas ao critério da Mediant™ 2000 e do terminal da rede IP, que no cenário da Figura 31 é o *softphone X-Lite* 3.0, quando são submetidos à realização de chamadas. Também foi adicionada a esta rota um *dial plan*, através do parâmetro CIDP, para todas as chamadas, bem como um plano de *routing* através do parâmetro AIRP. A configuração destes parâmetros será descrita mais a baixo.

A esta rota ISUP foram associados circuitos ou *time-slots* do *trunk* #1 da Mediant™ 2000 que se traduzem por *endpoints* controlados pelo protocolo MGCP. Esta associação é necessária, pois quando se pretende estabelecer uma chamada, deve-se proceder à reserva de um circuito no lado PSTN para a passagem do áudio da conversação. Para isso foram adicionados os seguintes circuitos ou *time-slots* da Mediant™ 2000 à rota *isup_route* do openCallAgent® de acordo com a Figura 36.

```
LST-ISUP-CIRCUIT:ROUTE=isup_route;
COMMAND ACCEPTED

ROUTE      OPC  DPC  CIC   ENDPOINT                      STATUS  MT-STATUS  HW-STATUS
-------------------------------------------------------------------------------------
isup_route 3338 3328 1     s0/ds1-0/1@m2k-ptinovacao.pt  Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 2     s0/ds1-0/2@m2k-ptinovacao.pt  Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 3     s0/ds1-0/3@m2k-ptinovacao.pt  Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 4     s0/ds1-0/4@m2k-ptinovacao.pt  Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 5     s0/ds1-0/5@m2k-ptinovacao.pt  Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 6     s0/ds1-0/6@m2k-ptinovacao.pt  Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 7     s0/ds1-0/7@m2k-ptinovacao.pt  Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 8     s0/ds1-0/8@m2k-ptinovacao.pt  Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 9     s0/ds1-0/9@m2k-ptinovacao.pt  Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 10    s0/ds1-0/10@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 11    s0/ds1-0/11@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 12    s0/ds1-0/12@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 13    s0/ds1-0/13@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 14    s0/ds1-0/14@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 15    s0/ds1-0/15@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 17    s0/ds1-0/17@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 18    s0/ds1-0/18@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 19    s0/ds1-0/19@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 20    s0/ds1-0/20@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 21    s0/ds1-0/21@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 22    s0/ds1-0/22@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 23    s0/ds1-0/23@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 24    s0/ds1-0/24@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 25    s0/ds1-0/25@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 26    s0/ds1-0/26@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 27    s0/ds1-0/27@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 28    s0/ds1-0/28@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 29    s0/ds1-0/29@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 30    s0/ds1-0/30@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
isup_route 3338 3328 31    s0/ds1-0/31@m2k-ptinovacao.pt Idle    NONE&NONE  NONE&NONE
-------------------------------------------------------------------------------------
```

Figura 36- Circuitos/*endpoints* para o cenário interno – ip-*Keel*® *Trunking*.

O circuito ou *time-slot* 16 do *trunk* #1 não foi adicionado à rota para o estabelecimento de chamadas com a rede PSTN, pois este circuito foi reservado na Mediant™ 2000 para a troca de sinalização SS7.

Por último configuraram-se os parâmetros CIDP e AIRP para as rotas SIP e ISUP. A configuração CIDP analisa a informação contida na chamada e verifica se obedece aos requisitos impostos para posterior análise do AIRP. A Figura 37 mostra a configuração para este parâmetro associado às rotas SIP e ISUP da Figura 32 e Figura 35 respectivamente.

```
LST-CIDP-SCEN:CIDP=first_cidp;
COMMAND ACCEPTED

first_cidp (ACTIVE)

SCENARIO     CDPN    LENGTH
----------------------------
cidp_scen    .       1
```

Figura 37- CIDP para o cenário interno – ip-*Keel*® *Trunking*.

A Figura 37 mostra que as rotas foram configuradas para que as chamadas que as utilizam podessem utilizar qualquer número para identificação do destinatário, através da

configuração do "." para o *Called Party Number* (CDPN), e que esse número deveria ter no mínimo um dígito (LENGTH igual a 1). Como se pode constatar, para o cenário interno não foi elaborado nenhum critério especial para o CIDP, são aceites chamadas para qualquer destinatário não havendo qualquer filtragem do número desde que tenha pelo menos um dígito.

Após essa análise pelo CIDP, a chamada é filtrada consoante os parâmetros do AIRP ilustrados na Figura 38 e Figura 39 para a rota SIP e ISUP respectivamente.

```
DIS-AIRP-SCEN:AIRP=sip_in_out_airp, SCEN=sip_in_out_scen;
COMMAND ACCEPTED

sip_in_out_airp (ACTIVE)

SCENARIO          CRITERIA            MODIFICATION    OUTCOME
-------------------------------------------------------------------------------
sip_in_out_scen   CDPN=.                              RTCASE=rc_isup_route
                  CPC=ORDINARY
                  CDPN-NAI=NATIONAL
                  CDPN-NPI=ISDN
```

Figura 38- AIRP rota SIP para o cenário interno – ip-*Keel® Trunking*.

O AIRP para a rota SIP foi configurado de forma a que chamadas que entram na rota provenientes do *X-Lite* 3.0 sejam filtradas de acordo com os seguintes critérios: o número do destinatário deve conter pelo menos um dígito (CDPN=.); o *Calling Party Category* (CPC) deve ser ORDINARY, isto significa que se trata de um utilizador normal, sem qualquer informação para o destino de funcionalidades adicionais como *Do Not Disturb* (DND), chamada via satélite, cancelamento de eco activo, etc.; o *Nature of Address Indicator* (NAI) do destinatário deve ser NATIONAL, ou seja, só são aceites chamadas nacionais na rota; e o *Numbering Plan Indicator* (NPI) do destinatário deve ser ISDN, ou seja, o plano de numeração utilizado no número do destinatário deve obedecer à normalização *International Telecommunication Union – Telecommunications* (ITU-T) E.164 [53]. Todas as chamadas que entram na rota SIP e que obedecem a estes critérios são encaminhadas para a rota *isup_route* associada ao *routing case* (RTCASE) *rc_isup_route*. O CPC é utilizado para diferenciar grupos de utilizadores, como serviço de hotel, polícia, empresas, etc., que necessitam de funcionalidades específicas de *routing*, restrições de identificação, entre outros serviços.

Para a rota ISUP foram dados os mesmos critérios de filtragem que na rota SIP às chamadas que entram na rota provenientes da rede PSTN (Figura 39).

```
DIS-AIRP-SCEN:AIRP=isup_airp, SCEN=isup_scen;
COMMAND ACCEPTED

isup_airp (ACTIVE)

SCENARIO     CRITERIA              MODIFICATION    OUTCOME
-------------------------------------------------------------------------
isup_scen    CDPN=.                                RTCASE=rc_sip_in_out
             CPC=ORDINARY
             CDPN-NAI=NATIONAL
             CDPN-NPI=ISDN
```

Figura 39- AIRP rota ISUP para o cenário interno – ip-*Keel*® *Trunking*.

Todas as chamadas que entram na rota ISUP e que obedecem a estes critérios são encaminhadas para a rota SIP *sip_in_out* associada ao RTCASE *rc_sip_in_out* com destino ao terminal *X-Lite* 3.0.

Configurado o openCallAgent® para o cenário da Figura 31, procedeu-se à configuração da Mediant™ 2000 para a funcionalidade de SGF e de T-MGF. Para isso mudou-se o *firmware* SIP, utilizado nos testes *standalone*, para o *firmware* 4.8 MGCP/MEGACO fornecido pela AudioCodes®. A Figura 40 e a Figura 41 ilustram a página *web* inicial da Mediant™ 2000 na vertente MGCP/MEGACO.

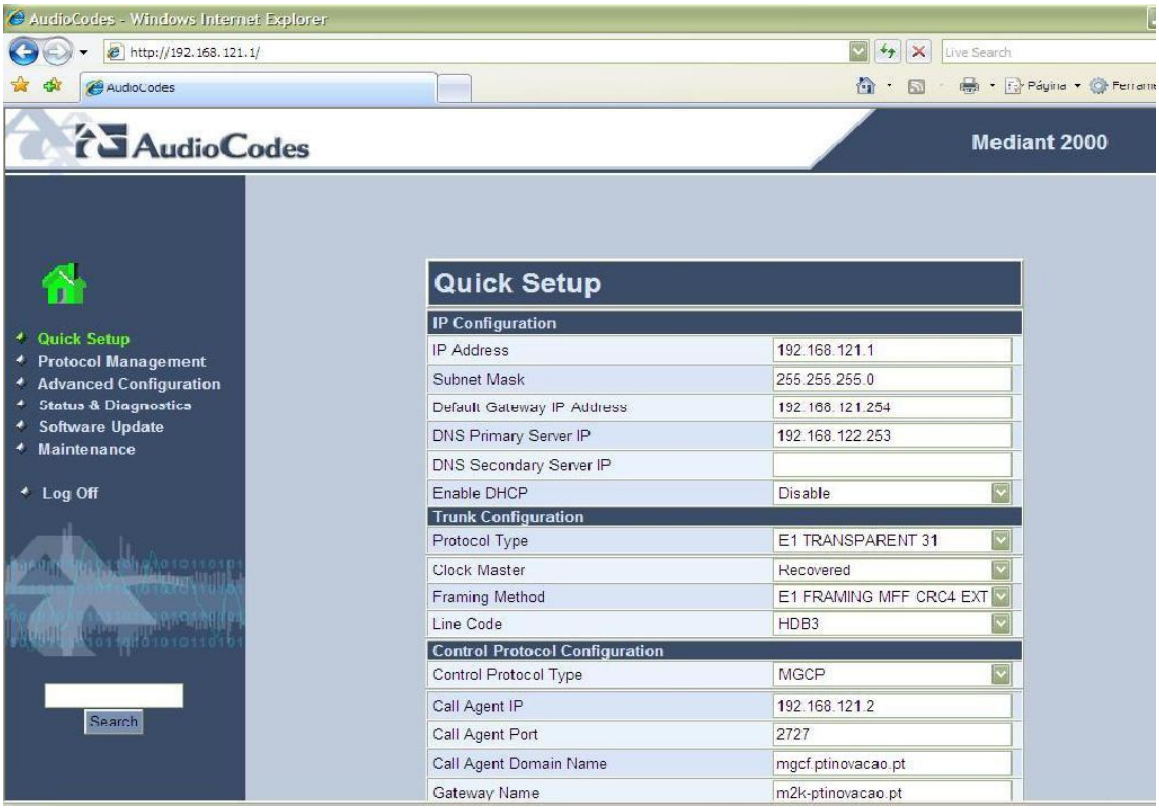



Figura 40- Página inicial da Mediant™ 2000 versão 4.8 MGCP/MEGACO – 1.

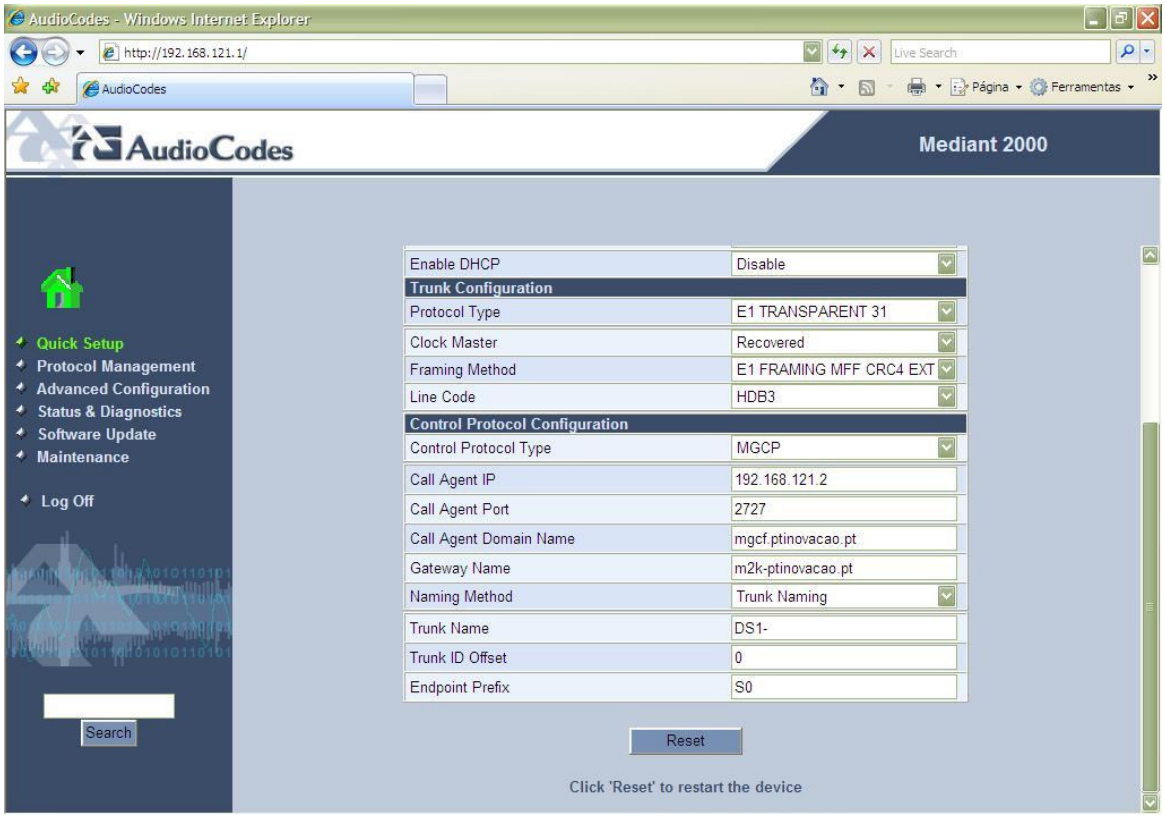



Figura 41- Página inicial da Mediant™ 2000 versão 4.8 MGCP/MEGACO – 2.

O endereço IP da Mediant™ 2000 foi alterado para o 192.168.121.1, tendo em conta o cenário da Figura 31, e os endereços para o *default gateway*, bem como para o DNS, foram configurados com os mesmos endereços relativamente ao openCallAgent® (Figura 40).

Como a Mediant™ 2000 irá funcionar em modo SGF transportando sinalização SS7 para a rede PSTN no *trunk* #1, configurou-se esta ligação em modo E1[18] transparente. No âmbito do esquema de controlo MGCP, foi aplicado à Mediant™ 2000 o nome *m2k-ptinovacao.pt* (Gateway Name), o Endpoint Prefix "S0" e o Trunk Name "DS-" para identificar os *endpoints* segundo a nomenclatura descrita durante a configuração do openCallAgent®.

Relativamente ao processo SGF da Mediant™ 2000, foi adicionado a esta uma ligação SS7 (*m2k_ss7_link*) com os parâmetros da Figura 42. Esta configuração teve em conta mais uma vez os requisitos SS7 do Anexo III e a configuração do openCallAgent®.

[18] A ligação E1 é baseada em TDM de 32 *time-slots*, em cada um tem uma capacidade de 64 kbps prefazendo um total de 2048 kbps para a ligação. É o sistema utilizado nas redes PSTN europeias.

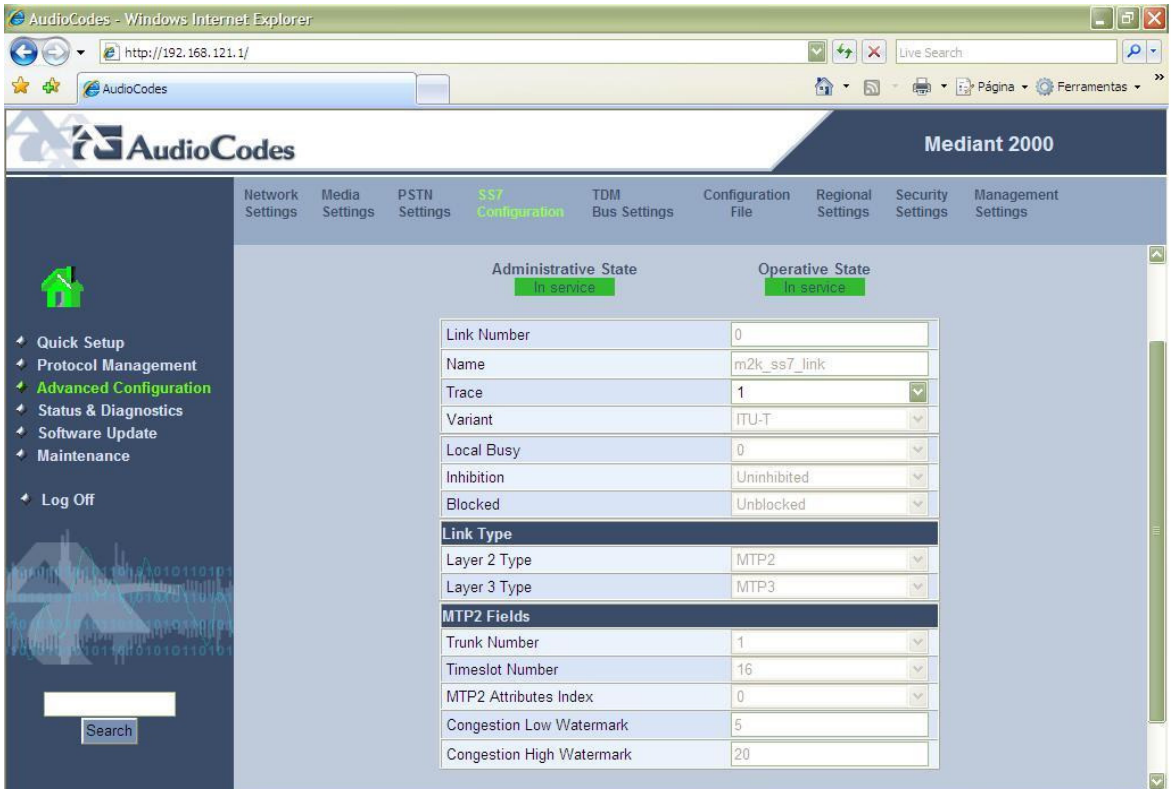



Figura 42- Ligação SS7 da Mediant™ 2000.

Para a camada dois e camada três, segundo a pilha protocolar SS7, foram configurados os protocolos MTP2 e MTP3 para esta ligação de acordo com as actuais redes PSTN. A variante aplicada para estes protocolos foi o ITU-T, pois é o utilizado pela rede PSTN nacional (Anexo III). Esta ligação SS7 para a rede PSTN é feita por intermédio do *time-slot* ou circuito 16 (Timeslot Number) do *trunk* #1 (Trunk Number), configurado já no openCallAgent® para esse propósito (Figura 36). A sinalização SS7 e os dados (áudio) são transportados no mesmo *trunk* E1 que liga a Mediant™ 2000 à rede PSTN, tratando-se portanto de uma ligação *F-link* [118]. O *trunk* E1 dispõe de 30 *time-slots* ou circuitos, nos quais um, neste caso o 16, será utilizado para o transporte de sinalização e os restantes para dados.

Como já foi referido anteriormente, o sistema *Trunking*, por intermédio da Mediant™ 2000, é visto pela rede PSTN como um SN. A configuração desse elemento SS7 está ilustrado na Figura 43.

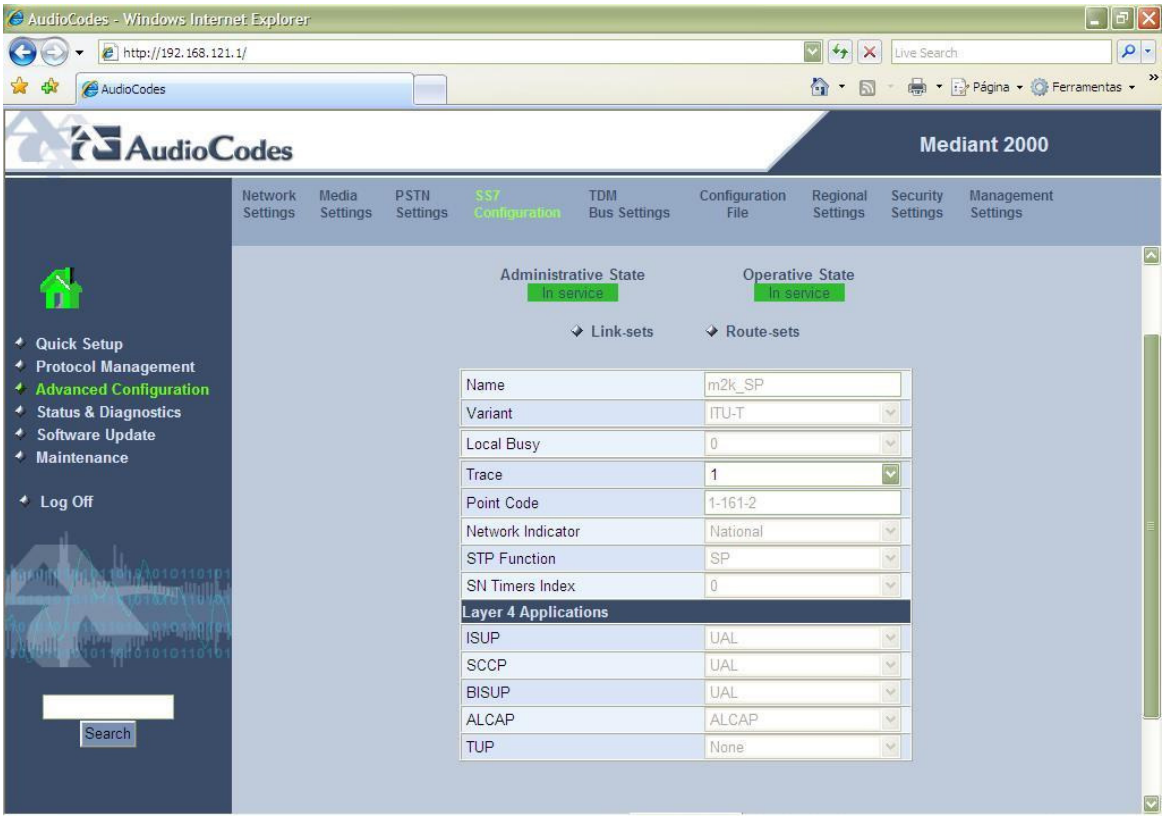



Figura 43- *Signalling Node* SS7 da Mediant™ 2000.

O SN *m2k_SP* da Mediant™ 2000 foi configurado com a variante ITU-T, NI igual a Nacional e com o OPC 1-161-2 correspondente em decimal ao 3338. Dado que a ligação com a rede PSTN é utilizada para o transporte de dados (áudio) e sinalização SS7, o SN da Mediant™ 2000 foi configurado como se tratasse de um elemento SN da arquitectura SS7 [35]. Para o transporte de sinalização das camadas superiores da pilha SS7 (ISUP, *Signaling Connection and Control Part* (SCCP), etc.), o SN foi configurado para utilizar protocolos do *User Adaptation Layers* (UAL), como o M3UA, sobre SCTP/IP.

Para a configuração da interface SIGTRAN do lado IP com o openCallAgent®, o SG da Mediant™ 2000 utiliza o protocolo M3UA para a camada protocolar de transporte, o porto de destino SCTP 2905 e a variante ITU utilizada na rede SS7, conforme ilustrado na Figura 44.

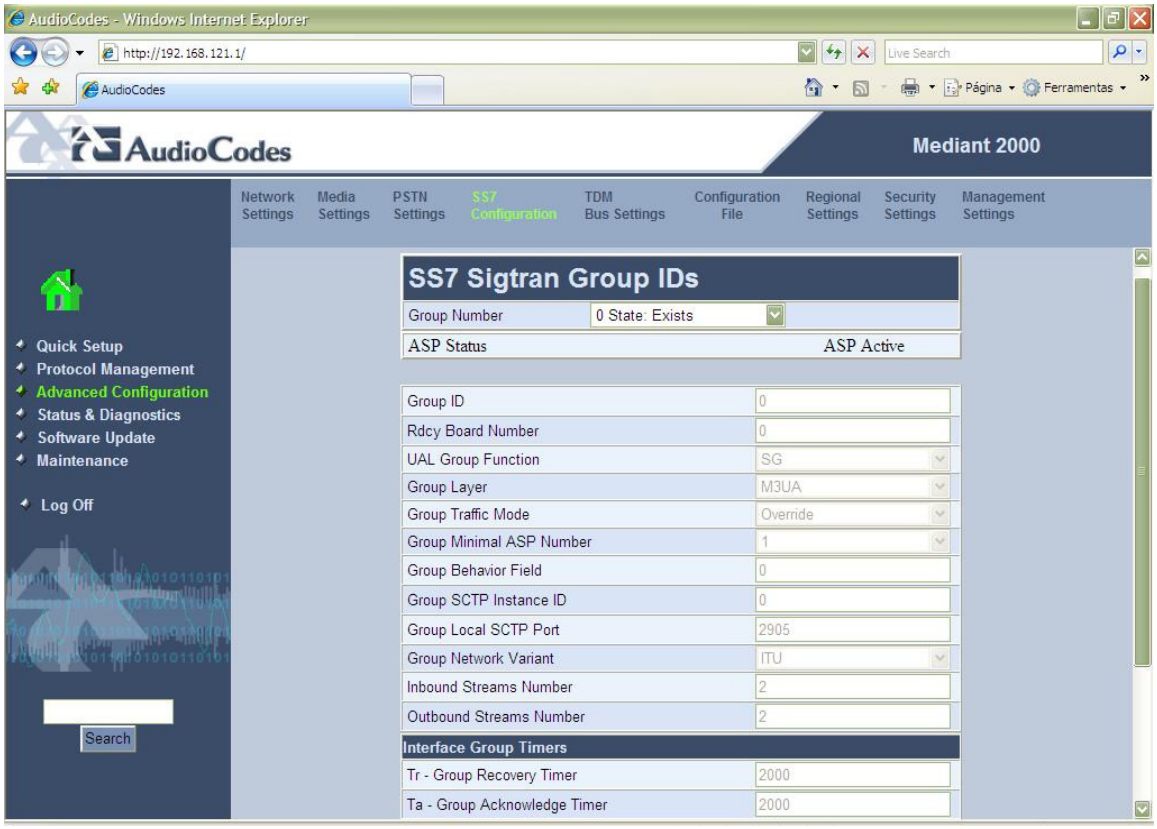



Figura 44- SS7 *Sigtran* da Mediant™ 2000.

Após configurados os elementos T-MGF & SGF (Mediant™ 2000) e MGCF (openCallAgent®) para o cenário interno da Figura 31, procedeu-se à configuração do único terminal SIP emulado pelo *softphone X-Lite* 3.0, ligado directamente aos elementos. O terminal SIP possui o SIP *Uniform Resource Identifiers* (URI) *sip:234513723@192.168.121.4:5060*, para isso configurou-se o *X-Lite* 3.0 com o *Display* e *User Name* "234513723" e *Domain* 192.168.121.2:5060 para os requisitos da conta SIP. O motivo pela escolha do número "234513723" deveu-se à configuração da gama de numeração entre "234513721" e "234513759" no comutador PSTN que liga à Mediant™ 2000 para o sistema *Media Gateway* de *Trunking*. Isto significa que quando é recebida uma chamada cujo o destinatário seja um destes números, então este comutador encaminha a chamada para este sistema.

Estando o cenário completo, efectuaram-se algumas chamadas simples entre um *Plain Old Telephone Service* (POTS) da rede fixa PSTN e o *X-Lite* 3.0 do lado IP de forma a assegurar o bom funcionamento e interligação dos elementos, bem como a conversão protocolar de sinalização realizada pelo sistema *Trunking*.

### 6.2.2.1. Testes e resultados

Através do terminal *X-Lite* 3.0 com o SIP URI *sip:234513723@192.168.121.4* realizou-se um teste simples de chamada de voz para um terminal da rede PSTN, que neste caso é um terminal móvel "96xxxxxxx". A utilização deste terminal como terminal da rede PSTN não tem qualquer influência no teste realizado. O diagrama da Figura 45 mostra a troca de mensagens de sinalização entre os elementos *Trunking* para o estabelecimento e terminação, por parte do terminal móvel, de uma chamada de voz.

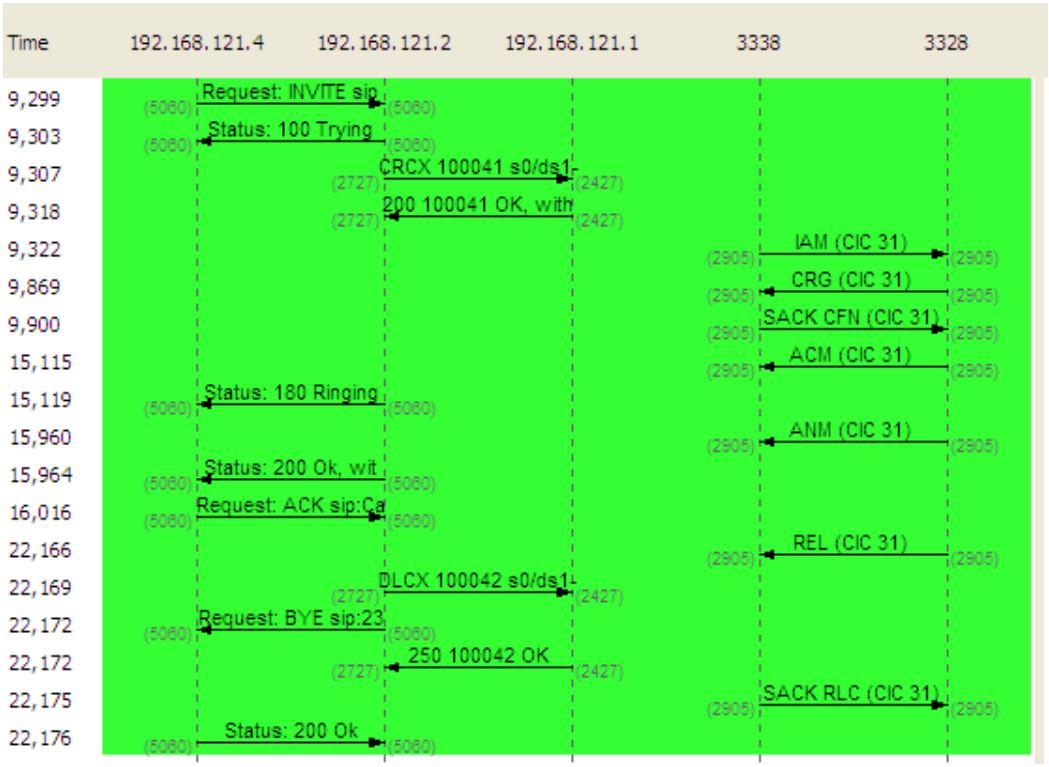



Figura 45- Diagrama de sinalização da chamada SIP para PSTN para o cenário interno.

Para estabelecer a chamada é marcado no *X-Lite* 3.0 o número "96xxxxxxx". Após a marcação, o terminal envia uma mensagem SIP/SDP *Invite* (Figura 46) para o openCallAgent®. No SDP são enviados os parâmetros *media* do *X-Lite* para esta chamada, com a lista de *codecs* de áudio que suporta, sendo o G.711 *A-law* (pcma) o preferido, e o porto *Real-time Transport Protocol* (RTP) 6000.

```
Session Initiation Protocol
    Request-Line: INVITE sip:96xxxxxxx@192.168.121.2 SIP/2.0
    Message Header
        Via: SIP/2.0/UDP 192.168.121.4:5060;rport;branch=z9hG4bK002157B563B2FBF53D84791CA64800A4
        From: Andre <sip:234513723@192.168.121.2>;tag=2023520027
        To: <sip:96xxxxxxx@192.168.121.2>
        Contact: <sip:234513723@192.168.121.4:5060>
        Call-ID: 29CE71D2-277B-6467-3A70-E3D99499488C@192.168.121.4
        CSeq: 2285 INVITE
        Max-Forwards: 70
        Content-Type: application/sdp
        User-Agent: X-Lite release 1105d
        Content-Length: 314
    Message body
        Session Description Protocol
            Session Description Protocol Version (v): 0
            Owner/Creator, Session Id (o): 234513723 791986415 791986481 IN IP4 192.168.121.4
            Session Name (s): X-Lite
            Connection Information (c): IN IP4 192.168.121.4
            Time Description, active time (t): 0 0
            Media Description, name and address (m): audio 6000 RTP/AVP 8 0 3 98 97 101
            Media Attribute (a): rtpmap:8 pcma/8000
            Media Attribute (a): rtpmap:0 pcmu/8000
            Media Attribute (a): rtpmap:3 gsm/8000
            Media Attribute (a): rtpmap:98 iLBC/8000
            Media Attribute (a): rtpmap:97 speex/8000
            Media Attribute (a): rtpmap:101 telephone-event/8000
            Media Attribute (a): fmtp:101 0-15
            Media Attribute (a): sendrecv
```

Figura 46- SIP *Invite* da chamada SIP para PSTN para o cenário interno.

Depois de receber esta mensagem, o openCallAgent® envia um comando *CreateConnection* (CRCX) MGCP [91] para a Mediant™ 2000 com fim a alocar um circuito/*endpoint* (*Circuit Identification Code* - CIC 31) e os parâmetros *media* necessários para a chamada através do envio do SDP. Caso a Mediant™ 2000 suporte algum dos *codecs* enviados no SDP e a alocação o canal ocorra com sucesso é enviado um comando MGCP de retorno 200 OK com SDP a indicar o *codec* escolhido da lista pela Mediant™ 2000 (G.711 *A-law*), e o porto RTP da Mediant™ 2000 (Figura 47).

```
User Datagram Protocol, Src Port: 2427 (2427), Dst Port: 2727 (2727)
Media Gateway Control Protocol
Session Description Protocol
    Session Description Protocol Version (v): 0
    Owner/Creator, Session Id (o): - 1928009965 0 IN IP4 192.168.121.1
    Session Name (s): -
    Connection Information (c): IN IP4 192.168.121.1
    Time Description, active time (t): 0 0
    Media Description, name and address (m): audio 6300 RTP/AVP 8 96
    Media Attribute (a): rtpmap:96 telephone-event/8000
    Media Attribute (a): fmtp:96 0-15
```

Figura 47- MGCP 200 OK da chamada SIP para PSTN para o cenário interno.

O openCallAgent® de seguida constrói a mensagem ISUP *Initial Address Message* (IAM) [35] correspondente à mensagem SIP *Invite* para enviar para a rede PSTN. O conteúdo desta mensagem está ilustrado na Figura 48.

```
Stream Control Transmission Protocol, Src Port: 2905 (2905), Dst Port: 2905 (2905)
MTP 3 User Adaptation Layer
ISDN User Part
    CIC: 31
    Message type: Initial address (1)
    Nature of Connection Indicators: 0x0
    Forward Call Indicators: 0x0
    Calling Party's category: 0xa (ordinary calling subscriber)
    Transmission medium requirement: 0 (speech)
    Called Party Number: 96xxxxxxxF
    Pointer to start of optional part: 9
    Calling Party Number: 234513723
    End of optional parameters (0)
```

Figura 48- ISUP IAM da chamada SIP para PSTN para o cenário interno.

A mensagem ISUP IAM é construída através do mapeamento do campo *Request*-URI (R-URI) da mensagem SIP *Invite* para CDPN da mensagem ISUP IAM, do sistema de numeração destes números (ISDN), do NI configurado no openCallAgent® (National) e da natureza do endereço (NOA), considerado como nacional pois os números de origem e destino não são acompanhados com o prefixo do indicativo do país. Nesta mensagem também é enviado o CIC reservado na Mediant™ 2000, para fazer a alocação do mesmo circuito no lado PSTN. A mensagem *Charging Information* (CRG) ISUP [35] enviada pela rede PSTN possui informação útil para taxação da chamada ao utilizador *X-Lite* 3.0. Esta indica que se trata de uma chamada nacional, portanto, deve ser cobrada como tal. O terminal móvel ao receber a mensagem ISUP IAM de pedido de estabelecimento de uma chamada, envia uma resposta ISUP *Address Complete Message* (ACM) [35] a indicar que recebeu toda a informação e que a sessão está a ser estabelecida no lado PSTN. É tocado o sinal de alerta *Ringing* no terminal móvel. O openCallAgent® ao receber esta mensagem ISUP mapeia-a numa mensagem SIP 180 *Ringing* com o SDP do MGCP 200 OK e envia para o *X-Lite* 3.0. Ao receber a mensagem é tocado o sinal de chamada no terminal *X-Lite* 3.0. Foi atendida a chamada no móvel (*off-hook*) e consequentemente enviada uma mensagem ISUP *Answer Network Message* (ANM) [35] a indicar que a chamada foi atendida e criado um canal de comunicação no lado PSTN para os dados (áudio) através do CIC 31. O openCallAgent® mapeia esta mensagem ISUP numa mensagem SIP 200 OK com o SDP da Mediant™ 2000 e envia para o *X-Lite* 3.0. Este terminal envia uma resposta SIP ACK ao openCallAgent® a informar que o SIP 200 OK foi recebido e que a chamada foi estabelecida. Neste momento está instaurada a conversação entre as duas entidades através da troca de dados RTP entre a Mediant™ 2000 e o *X-Lite* 3.0 e dados *Pulse Code Modulation* (PCM) entre a Mediant™ 2000 e o terminal móvel. Após concluída a conversação a chamada é terminada do lado do terminal PSTN (*on-hook*) através do envio

de uma mensagem ISUP *Release* (REL) [35] com indicação de causa de terminação (*Cause indicator*) igual a 16 [35], que significa que a chamada foi terminada em condições normais pelo utilizador. O conteúdo desta mensagem está ilustrado na Figura 49.

```
Stream Control Transmission Protocol, Src Port: 2905 (2905), Dst Port: 2905 (2905)
MTP 3 User Adaptation Layer
ISDN User Part
    CIC: 31
    Message type: Release (12)
    Cause indicators, see Q.850 (2 bytes length)
        Mandatory Parameter: 18 (Cause indicators)
        Pointer to Parameter: 2
        Parameter length: 2
        Cause indicators (-> Q.850)
        .... 0000 = Cause location: User (U) (0)
        .00. .... = Coding standard: ITU-T standardized coding (0x00)
        1... .... = Extension indicator: last octet
        .001 0000 = Cause indicator: Normal call clearing (16)
        1... .... = Extension indicator: last octet
    No optional parameter present (Pointer: 0)
```

Figura 49- ISUP REL da chamada SIP para PSTN para o cenário interno.

O openCallAgent® ao receber esta mensagem envia um comando *DeleteConnection* (DLCX) MGCP [91] para a Mediant™ 2000, com fim a libertar o canal/*endpoint* CIC 31, e mapeia a mensagem ISUP REL numa mensagem SIP *Bye* para o *X-Lite* 3.0. Após este envio, o openCallAgent® recebe uma resposta MGCP 200 OK da Mediant™ 2000 a indicar que a ligação no lado PSTN, através do CIC 31, foi cessada e que este canal/*endpoint* está livre para outras chamadas. O openCallAgent® envia de seguida uma mensagem ISUP *Release Complete* (RLC) [35] para completar a terminação da chamada no lado PSTN e recebe um SIP 200 OK do *X-Lite* 3.0 como resposta ao SIP *Bye* enviado, terminando assim a sessão também do lado IP. Nesta fase foi ouvido o sinal de interrompido no terminal *X-Lite* 3.0.

A realização do teste de chamada do terminal móvel para o *X-Lite* 3.0 é idêntico ao descrito acima para o teste SIP para PSTN, mas em sentido inverso (Figura 50).

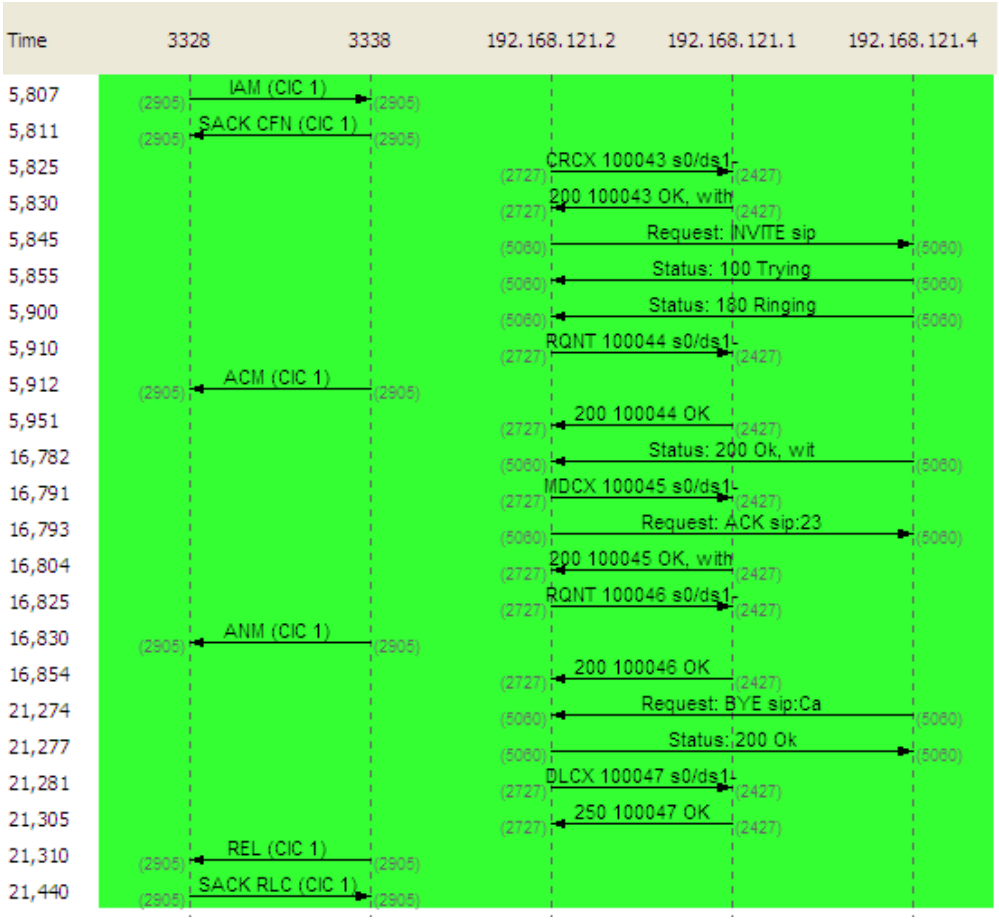



Figura 50- Diagrama de sinalização da chamada PSTN para SIP para o cenário interno.

O openCallAgent® envia um comando *NotificationRequest* (RQNT) MGCP [91] para a Mediant™ 2000 com o objectivo de aplicar o sinal de chamada no terminal móvel, através do envio da *package* G/rt [91], antes da chamada ser atendida pelo *X-Lite* 3.0. O segundo RQNT MGCP enviado pelo openCallAgent® antes da mensagem ISUP ANM serviu para que a notificação anterior (G/rt) deixasse de ter efeito, ou seja, que o sinal de chamada no terminal móvel deixasse de ser ouvido. O comando *ModifyConnection* (MDCX) MGCP [91] enviado pelo openCallAgent® para a Mediant™ 2000, após receber o SIP 200 OK com SDP do atendimento da chamada, serviu para alterar as características da ligação já criada através do comando CRCX MGCP. Uma dessas características foi o modo da ligação que inicialmente foi configurado como *recvonly* (CRCX) e depois alterado para o modo *sendrecv* (MDCX) de forma a que canal possa receber e enviar dados após o atendimento da chamada.

O processo de terminação da chamada do lado PSTN é idêntico ao do lado SIP mas em sentido inverso como se pode constatar por comparação da Figura 50 com a Figura 45.

### 6.2.3. Cenário Amora

Outro cenário intermédio utilizado para a realização de testes com os elementos do sistema ip-*Keel*® *Trunking* foi o cenário Amora. Este cenário foi construído para testes do comportamento do sistema e adquirir conhecimentos de configuração dos seus elementos para o caso de existir mais do que um terminal SIP. Partindo do cenário interno, configurou-se um SIP *proxy* (OnDO SIP *Server*) no domínio Amora (*Domain*: *amora-sip.pt*) com a função de *Registrar* para vários terminais SIP.

O Amora® é um demonstrador de serviços *triple-play* (IPTV, Voz sobre IP (VoIP), e *Internet*), *video-on-demand*, entre outros para clientes xDSL (Figura 51).

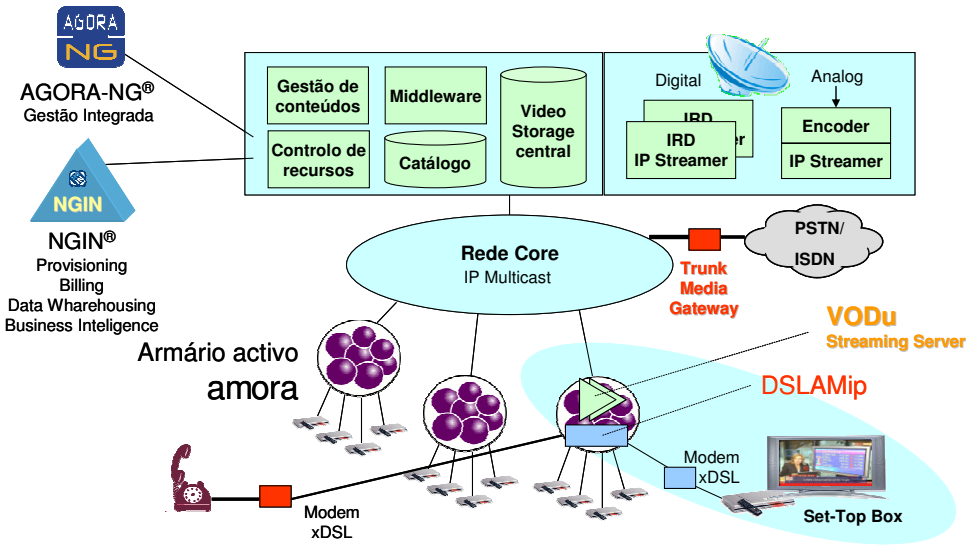



Figura 51- Piloto Amora® [127].

O sistema *Media Gateway* de *Trunking* configurado no cenário interno foi inserido no cenário Amora de forma a viabilizar uma rede piloto VoIP com utilizadores reais. Para isso, procedeu-se à montagem do cenário indicado na Figura 52. Do ponto de vista da configuração SS7 com a rede PSTN e da configuração de controlo MGCP, o cenário é igual ao do interno descrito anteriormente. A única diferença está na rota SIP, que no cenário interno (Figura 32) tinha como destino o terminal *X-Lite* 3.0, e agora foi configurado para o computador com o OnDO SIP *Server* instalado (192.168.121.3). Neste SIP *proxy*/*registrar* do domínio Amora irão ser registados 3 terminais *X-Lite* 3.0 para testes de chamada de voz para a rede PSTN.

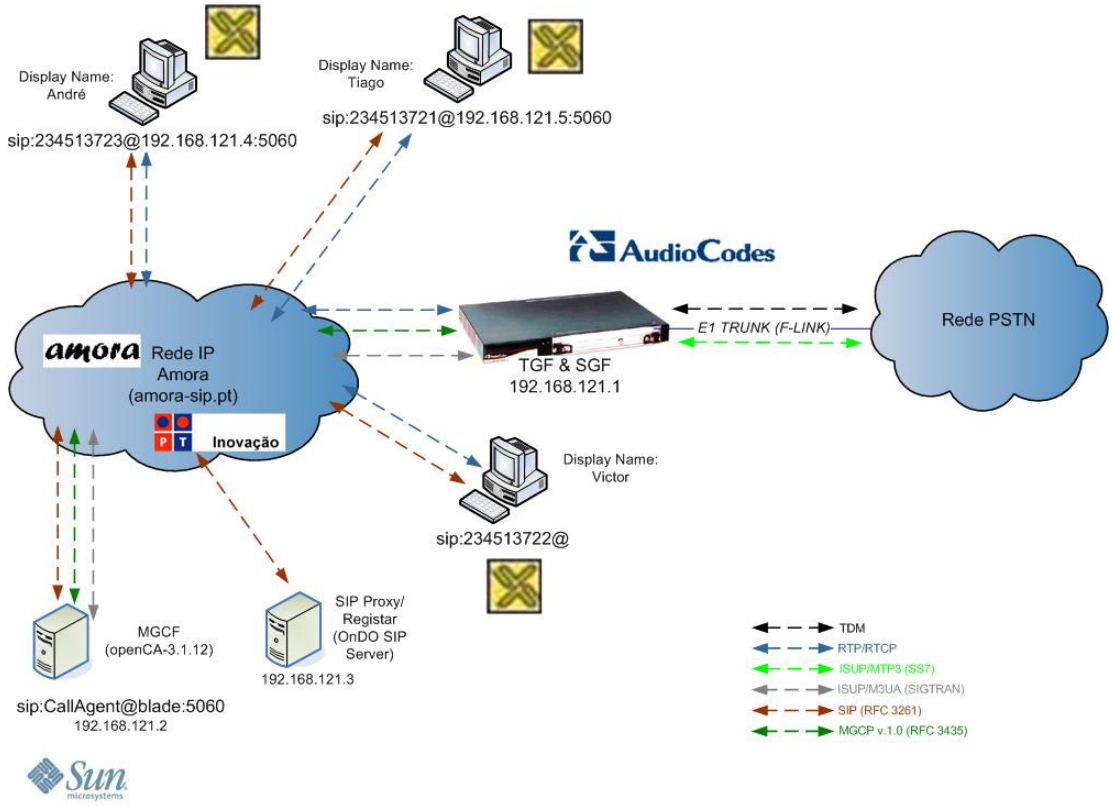



Figura 52- Cenário Amora – ip-*Keel*® *Trunking*.

#### 6.2.3.1. Testes e resultados

Os resultados obtidos dos testes efectuados entre os terminais *X-Lite* 3.0 e os terminais da rede PSTN são idênticos aos obtidos, relativamente à sinalização, no cenário interno como seria de esperar. O facto de realizar mais do que uma chamada em simultâneo com o sistema *Trunking* nada interfere no processamento na chamada de cada utilizador. O motivo desta integração no Amora passa por conhecer o comportamento do sistema *Trunking* na presença de vários utilizadores e providenciar serviço VoIP com a rede PSTN para os clientes do Amora.

### *6.2.4. Cenário SHipNET*

Os cenários intermédios foram muito importantes na aquisição de conhecimento sobre os parâmetros de configuração dos elementos que possibilitam a interligação entre os domínios IP e PSTN. Mas o grande objectivo para o sistema ip-*Keel*® *Trunking* é a sua introdução no demonstrador RPG *SHipNET*® e sua configuração de forma a dar uma resposta o mais completa possível aos requisitos impostos pela arquitectura PES do TISPAN face às várias fases evolutivas do cenário.

A Figura 53 ilustra o cenário de testes com o demonstrador RPG *SHipNET*®. A rede IP de domínio *ptinovacao.pt*, referida na figura, possui o *core* IMS/TISPAN (RPG) de acordo com a normalização indicada na Figura 15. Portanto, o ip-*Keel*® *Trunking* teve que ser ligado ao cenário de forma a existir conectividade entre o openCallAgent® e o dispositivo que faz de *Serving-Call Session Control Function* (S-CSCF), para a troca de sinalização SIP, e entre a Mediant™ 2000 e os terminais registados no domínio RPG para a troca de dados RTP. Um dos requisitos do TISPAN não considerados, sem influência nos testes pretendidos, foi a comunicação entre o openCallAgent® e o elemento que faz de *Breakout Gateway Control Function* (BGCF). Todas as mensagens SIP de entrada no sistema ip-*Keel*® *Trunking* são enviadas directamente pelo S-CSCF. As mensagens SIP de saída são enviadas para o *Interrogating-Call Session Control Function* (I-CSCF) de acordo com a normalização TISPAN [72].

Fisicamente nada foi alterado relativamente ao cenário de testes interno da Figura 31 para a ligação PSTN, matendo-se as mesmas configurações para o SGF da Mediant™ 2000 apenas foram alteradas as configurações no openCallAgent® para a ligação SIP ao demonstrador, bem como a rota ISUP.

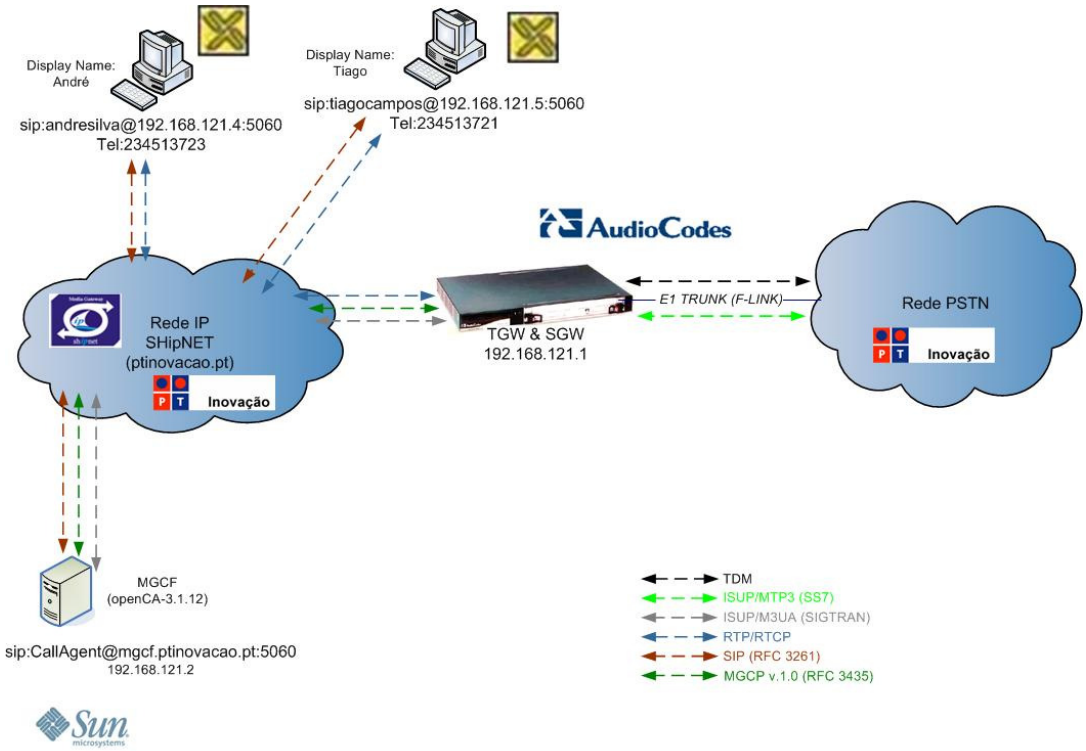



Figura 53- Cenário *SHipNET*® – ip-*Keel*® *Trunking*.

Após a configuração do cenário, foram utilizados dois terminais SIP *X-Lite* 3.0 registados no domínio *ptinovacao.pt* através do *Proxy-Call Session Control Function* (P-CSCF) *SHipNET*® para a realização de testes.

Para a ligação SIP foram criadas no openCallAgent® duas rotas SIP, uma de entrada (*sip_in*) e outra de saída (*sip_out*) de acordo com a Figura 54 e Figura 56 respectivamente.

```
DIS-SIP-ROUTE:ROUTE=sip_in;
COMMAND ACCEPTED

ROUTE     HOST             PORT    MAX-CALLS    ROUTE-OPTIONS
-------------------------------------------------------------------------------
sip_in    192.168.20.69    5060    30           AIRP              = sip_in_airp
                                                CIDP              = first_cidp
                                                ORNP              = NONE
                                                TREATMENT-TABLE   =
                                                ROUTE-GROUP       =
                                                CPS               = DISABLED
                                                CLIR              = NONE
                                                CLIP              = TRUE
                                                CLI-TRUSTED       = TRUE
                                                PROXY             = YES
                                                REGISTER          = NONE
                                                ALLOW-REDIRECT    = YES
-------------------------------------------------------------------------------
```

Figura 54- Rota SIP (*sip_in*) para o cenário *SHipNET*® – ip-*Keel*® *Trunking*.

A rota SIP *sip_in* foi configurada no openCallAgent® para ligar à máquina com endereço:porto 192.168.20.69:5060 que corresponde ao elemento S-CSCF do cenário *SHipNET*®. Os restantes parâmetros foram deixados iguais comparativamente ao cenário de testes interno, à excepção do PROXY igual YES, que significa que o HOST da rota é um elemento com funcionalidades de SIP *proxy* (S-CSCF), e do parâmetro AIRP que impõe restrições e alterações às mensagens das chamadas que passam por essa rota, conforme ilustrado na Figura 55.

```
DIS-AIRP-SCEN:AIRP=sip_in_airp;
COMMAND ACCEPTED

sip_in_airp (ACTIVE)

SCENARIO              CRITERIA          MODIFICATION              OUTCOME
-------------------------------------------------------------------------------
to_isup_int           CPC=ORDINARY                                RTCASE=rc_isup_route
                      CDPN-NPI=ISDN

to_isup_int_00        CDPN=00           REMOVE=(CDPN,1,2)         RTCASE=rc_isup_route
                      CPC=ORDINARY      CDPN-NAI=INTERNATIONAL
                      CDPN-NPI=ISDN

to_isup_intsip_nat    CDPN=351          REMOVE=(CDPN,1,3)         RTCASE=rc_isup_route
                      CPC=ORDINARY      CDPN-NAI=NATIONAL
                      CDPN-NPI=ISDN

to_isup_nat_nat       CDPN=351          REMOVE=(CDPN,1,3)         RTCASE=rc_isup_route
                      CGPN=351          REMOVE=(CGPN,1,3)
                      CPC=ORDINARY      CDPN-NAI=NATIONAL
                      CDPN-NPI=ISDN     CGPN-NAI=NATIONAL
```

Figura 55- AIRP rota *sip_in* para o cenário *SHipNET*® – ip-*Keel*® *Trunking*.

O AIRP *sip_in_airp* foi configurado para responder a quatro cenários possíveis de chamadas que entram na rota SIP *sip_in*. O primeiro cenário indicado na Figura 55 (*to_isup_int*) foi configurado para que todas as chamadas com destino internacional, ou seja, todas as chamadas em que o número do destinatário comece por "+" e os três dígitos seguintes sejam diferentes de "351"[19], sejam encaminhadas para a rota ISUP com destino à rede PSTN sem qualquer alteração. Todas as sessões provenientes do *SHipNET*® trazem o número do destinatário CDPN no R-URI da mensagem, no formato internacional E.164 [53], e o mesmo se aplica ao número do originário *Calling Party Number* (CGPN) no campo *P-Asserted-Identity* da mensagem SIP. Este é um dos requisitos impostos pela normalização TISPAN. Outro cenário do AIRP (*to_isup_intsip*) foi criado para as chamadas que entram na rota SIP em que o número do originário CGPN é internacional e diferente de "+351", e o número do destinatário CDPN possui o prefixo "+351". Neste caso, todas as chamadas que entram na rota e que acentuam nestes requisitos do AIRP, o openCallAgent® retira o "351" do CDPN, modifica o NAI deste número para nacional e encaminha a chamada para a rota ISUP. O último cenário (*to_isup_nat_nat*) foi criado para as chamadas que entram na rota SIP e cujo os números do destinatário e do originário são nacionais mas estão no formato internacional ("+351"). O openCallAgent® a estas chamadas, retira o "351" do CDPN e CGPN, e modifica o NAI destes números para nacional para retirar o "+".

A rota SIP *sip_out* (Figura 56) foi configurada no openCallAgent® para ligar à máquina com endereço:porto 192.168.121.7:5060 que corresponde a um SIP *proxy* auxiliar que apenas altera o URI de SIP para TEL do R-URI e dos campos *from* e *to*, em algumas mensagens SIP enviadas pelo openCallAgent®, consoante o número do destinatário. A utilização desta máquina deveu-se ao facto de existirem alguns terminais do *SHipNET*® que não suportam o formato TEL URI, definido pelo TISPAN. Este elemento envia de seguida as mensagens para o I-CSCF do *SHipNET*®.

[19] "+351" é o indicativo de Portugal

```
DIS-SIP-ROUTE:ROUTE=sip_out;
COMMAND ACCEPTED

ROUTE      HOST             PORT    MAX-CALLS    ROUTE-OPTIONS
-------------------------------------------------------------------------------
sip_out    192.168.121.7    5060    30           AIRP             = sip_out_airp
                                                 CIDP             = first_cidp
                                                 ORNP             = NONE
                                                 TREATMENT-TABLE  =
                                                 ROUTE-GROUP      =
                                                 CPS              = DISABLED
                                                 CLIR             = NONE
                                                 CLIP             = TRUE
                                                 CLI-TRUSTED      = TRUE
                                                 PROXY            = YES
                                                 REGISTER         = NONE
                                                 ALLOW-REDIRECT   = YES
-------------------------------------------------------------------------------
```

Figura 56- Rota SIP (*sip_out*) para o cenário *SHipNET*® – ip-*Keel*® *Trunking*.

A configuração dos parâmetros AIRP para esta rota está indicada na Figura 57.

```
LST-AIRP:AIRP=sip_out_airp;
COMMAND ACCEPTED

AIRP            DEFAULT-REASON             MODIFICATION    STATUS
-------------------------------------------------------------------
sip_out_airp    NO_ROUTE_TO_DESTINATION    DELETED         IN USE
```

Figura 57- AIRP rota *sip_out* para o cenário *SHipNET*® – ip-*Keel*® *Trunking*.

Nesta rota SIP não foi configurado nenhum cenário para a imposição de restrições e modificações ao conteúdo das mensagens de sinalização, pois é uma rota de saída.

A configuração do openCallAgent® para a ligação SS7 com a rede PSTN é igual à do cenário de testes interno. Apenas foi alterado o AIRP para a rota ISUP de acordo com a Figura 58.

```
DIS-AIRP-SCEN:AIRP=isup_airp;
COMMAND ACCEPTED

isup_airp (ACTIVE)

SCENARIO    CRITERIA          MODIFICATION              OUTCOME
-------------------------------------------------------------------------
to_sip      CPC=ORDINARY      INSERT=(CDPN,1,351)       RTCASE=rc_sip_out
            CDPN-NPI=ISDN     CDPN-NAI=INTERNATIONAL
```

Figura 58- AIRP rota *isup_route* para o cenário *SHipNET*® – ip-*Keel*® *Trunking*.

Para existir acordância entre o *ip-Keel*® *Trunking* e o plano de numeração E.164 imposto pelo *SHipNET*®, foi necessário configurar o AIRP da rota ISUP de forma a que todas as chamadas provenientes da rede PSTN seja acrescentado o prefixo "351" ao CDPN, bem como o "+" através da alteração do NAI para internacional.

Neste cenário apenas foi configurado o protocolo ISUP para o estabelecimento de sessões, o TCAP não foi configurado pois o sistema não foi utilizado inicialmente para serviços PSTN suplementares.

Comparando a lista de *codecs* suportados pela Mediant™ 2000 e pelos terminais de teste *X-Lite* 3.0, apenas os *codecs* de voz G.711 *A-law* e *μ-law*, G.729 e *Global System for Mobile communications* (GSM) da Tabela VIII, podem ser utilizados para o estabelecimento de sessões de voz com estes terminais. Uma das grandes restrições para o *SHipNET*® ao utilizar esta configuração do sistema ip-*Keel*® *Trunking* (Figura 53), é a utilização de apenas uma ligação E1 da Mediant™ 2000 ao *Service Switching Point* (SSP) da rede PSTN, o que limita o número máximo de chamadas em simultâneo para o *SHipNET*® em 30.

Cada um dos clientes de teste *X-Lite* 3.0 do cenário da Figura 53 foi configurado com as seguintes contas para se poderem registar no domínio *ptinovacao.pt* do *SHipNET*® (Figura 21):

- *Display Name*: André Silva / Tiago Campos;
- *User Name*: andresilva / tiagocampos;
- *Authorization username*: andresilva@ptinovacao.pt / tiagocampos@ptinovacao.pt;
- *Domain*: ptinovacao.pt;
- *Proxy*: 192.168.21.2:5060.

A opção "*Register with domain and receive incoming calls*" do *X-Lite* 3.0 foi activada. No UPSF ou *Home Subscriber Server* (HSS), segundo a normalização do 3GPP, existe um TEL URI: *tel*:+35123453723 e *tel*:+351234523721, implícito a cada um dos SIP URI's *sip*:*andresilva@ptinovacao.pt* e *sip*:*tiagocampos@ptinovacao.pt*, respectivamente. Portanto, a cada um destes clientes fica associado um SIP URI e TEL URI para o seu contacto, logo após o registo no domínio *SHipNET*®.

### 6.2.4.1. Testes e resultados

Para testar a configuração do sistema ip-*Keel*® como parte integrante do demonstrador RPG *SHipNET*®, foram efectuados alguns testes relacionados com sessões de voz entre o terminal *X-Lite* 3.0 com SIP URI *sip:andresilva@ptinovacao.pt* e um terminal analógico da rede PSTN. Muitos dos testes realizados são situações reais e que visam a analisar o comportamento do ip-*Keel*® num cenário RPG real, como falhas do lado PSTN e do lado SIP, cancelamento da chamada antes de ser atendida, rejeição da chamada pelo destinatário

antes de ser atendida, SIP *timeout* e PSTN *timeout*, terminal ocupado, CLIP, CLIR, número do destinatário não atribuído, etc.

Nesta Dissertação vão ser descritos apenas dois dos testes realizados que poderão ser úteis para antever o comportamento, bem como o conteúdo das mensagens de sinalização, noutros casos de teste.

No primeiro teste é realizada uma chamada do *X-Lite* 3.0 para o número "96xxxxxxx" do terminal móvel da rede PSTN e antes da chamada ser atendida, esta é cancelada pelo *X-Lite* 3.0. O diagrama da Figura 59 mostra a troca de mensagens de sinalização entre os elementos *Trunking* e o *SHipNET*® para este teste.

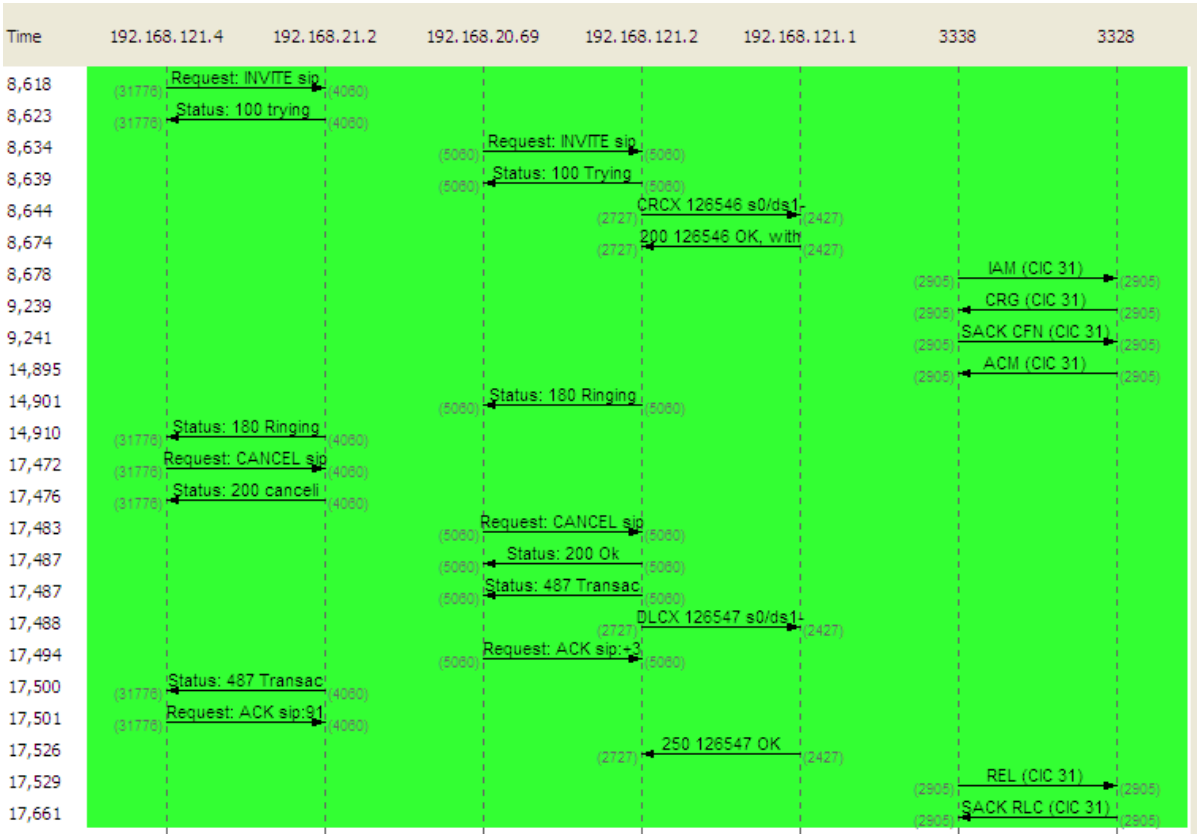



Figura 59- Diagrama de sinalização de cancelamento da chamada pelo SIP para o cenário *SHipNET*®.

O processamento de estabelecimento da chamada até ao 180 *Ringing* é idêntico ao da Figura 45. As diferenças existentes residem no conteúdo das mensagens SIP impostas pelo cenário com o demonstrador *SHipNET*®. A Figura 60 ilustra o conteúdo da mensagem SIP *Invite* que chega ao MGCF openCallAgent® pelo S-CSCF (192.168.20.69).

```
Internet Protocol, Src: 192.168.20.69 (192.168.20.69), Dst: 192.168.121.2 (192.168.121.2)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Session Initiation Protocol
    Request-Line: INVITE sip:+35196xxxxxxx@ptinovacao.pt SIP/2.0
        Method: INVITE
        [Resent Packet: False]
    Message Header
        Record-Route: <sip:mo@scscf.ptinovacao.pt:6060;lr>
        P-Asserted-Identity: <tel:+351234513723>
        Record-Route: <sip:mo@pcscf.ptinovacao.pt:4060;lr>
        Via: SIP/2.0/UDP 192.168.20.69;branch=z9hG4bKc33c.8b7bbd5.0
        Via: SIP/2.0/UDP 192.168.20.5:6060;branch=z9hG4bKc33c.5d48c172.0
        Via: SIP/2.0/UDP 192.168.21.2:4060;branch=z9hG4bKc33c.b7c770f6.0
        Via: SIP/2.0/UDP 192.168.121.4:31776;branch=z9hG4bK-d87543-404b896c0e1b5836-1--d87543-;rport=31776
        Max-Forwards: 14
        Contact: <sip:andresilva@192.168.121.4:31776>
        To: "96xxxxxxx"<sip:96xxxxxxx@ptinovacao.pt>
        From: "Andr\303\251 Silva"<sip:andresilva@ptinovacao.pt>;tag=5d5b823f
        Call-ID: NzMxOTRjMjhkNTZjMjg4NTVkNjM5YWI4ZjgxMmU0MGE.
        CSeq: 1 INVITE
        Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
        Content-Type: application/sdp
        User-Agent: X-Lite release 1011s stamp 41150
        Content-Length: 264
        P-Asserted-Identity: <sip:andresilva@ptinovacao.pt>
        P-Charging-Vector: icid-value="P-CSCFabcd476b320500000e59"; icid-generated-at=127.0.0.1; orig-ioi="ptinovacao.pt"
    Message body
```

Figura 60- SIP *Invite* da chamada SIP para PSTN - cenário *SHipNET*®.

Um reparo importante sobre o R-URI desta mensagem é a existência de um SIP URI *sip:+35196xxxxxxx@ptinovacao.pt* sem *user=phone* definido pelo 3GPP [28]. Esta falha do demonstrador *SHipNET*® nada interfere no funcionamento do ip-*Keel*®. O TEL URI do originário *X-Lite* 3.0 presente no campo *P-Asserted-Identity* colocado pelo *SHipNET*® será mapeado sobre o formato nacional (Figura 55) no campo CGPN da mensagem ISUP para a rede PSTN, bem como o número do destinatário presente no SIP URI do R-URI que será mapeado, também no formato nacional, no campo CDPN. Outra falha do *SHipNET*® é a colocação de dois *P-Asserted-Identity* na mesma mensagem SIP *Invite* (Figura 60), um com a identificação do utilizador *X-Lite* 3.0 no formato SIP URI e outro no formato TEL URI. Deveria ser colocado apenas o do formato TEL URI, pois o openCallAgent® não consegue mapear SIP URI's com nome de utilizador alfabético. Mas neste caso como o do TEL URI aparece primeiro na mensagem, o segundo é descartado.

O openCallAgent® guarda o valor do parâmetro *orig-ioi* do campo *P-Charging-Vector* para identificar a rede onde se encontra e subsequentemente enviar este parâmetro nas restantes mensagens SIP dentro da mesma sessão.

Após o *X-Lite* 3.0 receber a mensagem SIP 180 *Ringing*, é ouvido o sinal de alerta *Ringing* no terminal móvel. Antes da chamada ser atendida (*off-hook*), esta é cancelada pelo *X-Lite* 3.0. O openCallAgent® ao receber o SIP *Request Cancel* envia uma resposta 200 OK de retorno para o *X-Lite* 3.0 a confirmar a recepção da mensagem SIP *Cancel.* Na sequência do processo de cancelamento da chamada, este envia para o *X-Lite* 3.0 uma mensagem SIP 487 *Transaction Cancelled* de resposta na sequência do SIP *Invite* inicial para terminar o

estabelecimento do lado SIP. O S-CSCF e o *X-Lite* 3.0 enviam uma mensagem SIP ACK para a entidade que lhes enviou o SIP 487 *Transaction Cancelled* para confirmar a recepção. Após a recepção do SIP ACK do S-CSCF, o openCallAgent® envia uma mensagem ISUP REL com indicação de causa de terminação (*Cause indicator*) igual a 16, que significa que a chamada foi terminada em condições normais pela rede IP ("*Network beyond interworking point*...'). Esta mensagem está ilustrada na Figura 61.

```
Internet Protocol, Src: 192.168.121.2 (192.168.121.2), Dst: 192.168.121.1 (192.168.121.1)
Stream Control Transmission Protocol, Src Port: 2905 (2905), Dst Port: 2905 (2905)
MTP 3 User Adaptation Layer
ISDN User Part
    CIC: 31
    Message type: Release (12)
    Cause indicators, see Q.850 (2 bytes length)
        Mandatory Parameter: 18 (Cause indicators)
        Pointer to Parameter: 2
        Parameter length: 2
        Cause indicators (-> Q.850)
        .... 1010 = Cause location: Network beyond interworking point (BI) (10)
        .00. .... = Coding standard: ITU-T standardized coding (0x00)
        1... .... = Extension indicator: last octet
        .001 0000 = Cause indicator: Normal call clearing (16)
        1... .... = Extension indicator: last octet
    No optional parameter present (Pointer: 0)
```

Figura 61- ISUP REL da chamada SIP para PSTN - cenário *SHipNET*®.

O teste seguinte pretende mostrar a funcionalidade CLIR configurada na rota ISUP do openCallAgent® (Figura 35), numa chamada realizada do terminal móvel da rede PSTN, sem envio da identificação, para o *X-Lite* 3.0. A Figura 62 mostra o conteúdo da mensagem ISUP IAM que chega ao sistema *Trunking* pela rede PSTN.

```
⊟ ISDN User Part
    CIC: 1
    Message type: Initial address (1)
  ⊞ Nature of Connection Indicators: 0x10
  ⊞ Forward Call Indicators: 0x6001
  ⊞ Calling Party's category: 0xa (ordinary calling subscriber)
  ⊞ Transmission medium requirement: 0 (speech)
  ⊞ Called Party Number: 234513723F
    Pointer to start of optional part: 9
  ⊟ Calling Party Number: 96xxxxxxx
      Optional Parameter: 10 (Calling party number)
      Parameter length: 7
      1... .... = Odd/even indicator: odd number of address signals
      .000 0011 = Nature of address indicator: national (significant) number (3)
      0... .... = NI indicator: complete
      .001 .... = Numbering plan indicator: ISDN (Telephony) numbering plan (1)
      .... 01.. = Address presentation restricted indicator: presentation restricted (1)
      .... ..11 = Screening indicator: network provided (3)
    ⊞ Calling Party Number: 96xxxxxxx
  ⊞ User service information, (3 bytes length)
  ⊞ Propagation delay counter = 0 ms
  ⊞ Parameter Type unknown/reserved (1 Byte)
    End of optional parameters (0)
```

Figura 62- ISUP IAM da chamada PSTN para SIP com CLIR - cenário *SHipNET*®.

Apesar de o número CGPN estar presente na mensagem, é enviado um campo ("*Address presentation restricted indicator*") a indicar que a identificação é restrita, ou seja, que não deve ser apresentada no terminal destino *X-Lite* 3.0. O openCallAgent® ao receber esta

mensagem ISUP IAM de estabelecimento, envia para o *SHipNET*® uma mensagem SIP *Invite* indicada na Figura 63.

```
Internet Protocol, Src: 192.168.121.2 (192.168.121.2), Dst: 192.168.121.7 (192.168.121.7)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Session Initiation Protocol
    Request-Line: INVITE tel:+351234513723 SIP/2.0
    Message Header
        From: <sip:anonymous@anonymous.invalid>;tag=ds-2c67-4460d128128b7
        To: <tel:+351234513723>
        Call-ID: cc8ce842-1dd1-11b2-b3ae-f3b1b8457fbf@mgcf
        CSeq: 23679 INVITE
        Content-Length: 903
        Content-Type: application/sdp
        Supported: 100rel
        Supported: timer
        P-Asserted-Identity: <tel:+35196xxxxxxx>
        Privacy: id
        Session-Expires: 1800
        Contact: <sip:CallAgent@mgcf.ptinovacao.pt;transport=udp>
        Via: SIP/2.0/UDP 192.168.121.2:5060;branch=z9hG4bKcc8d1376-1dd1-11b2-8875-b60ce1c37405
        Max-Forwards: 70
    Message body
```

Figura 63- SIP *Invite* da chamada PSTN para SIP com CLIR - cenário *SHipNET*®.

O openCallAgent® processa o CLIR na construção da mensagem SIP *Invite* de acordo com o mecanismo documentado no RFC 3325 [116]. Coloca a identificação do CGPN no campo SIP *P-Asserted-Identity*, pois a rota ISUP, *isup_route* (Figura 35), foi configurada de forma a que a rede *SHipNET*® de entrada de chamadas provenientes da rede PSTN, seja considerada como um domínio de confiança para o utilizador (CLI-TRUSTED = TRUE), e coloca o campo *Privacy* com o valor "*id*" para indicar que o utilizador quer manter a sua privacidade, relativamente ao seu número de identificação, para as entidades SIP fora do domínio de confiança *SHipNET*®. No campo *from* da mensagem é colocado o SIP URI *sip:anonymous@anonymous.invalid* de acordo com o RFC 3325 [116].

## 6.3. ip-Keel Acesso

O ip-*Keel*® Acesso representa o sistema *Media Gateway* de Acesso da arquitectura PES do TISPAN ilustrada na Figura 15. Esta solução possui duas vertentes de sinalização consoante o cenário pretendido. No caso em que o A-MGF ou *Residential-Media Gateway Function* (R-MGF) ilustrado na Figura 15 seja baseado em SIP (A/R-VGF), então este será ligado directamente a um P-CSCF. Caso seja baseado no protocolo MEGACO/H.248, terá que existir um elemento de controlo integrante na arquitectura do ip-*Keel*® Acesso para fazer a "tradução" MEGACO/H.248 para SIP e vice-versa, com as mesmas funcionalidades que um P-CSCF, do lado RPG, ligado a um I/S-CSCF (Figura 15).

Para efeitos demonstrativos do ip-*Keel*® Acesso baseado em SIP no *SHipNET*®, foi montado um cenário com um A-VGF formado pelo produto TP®-260 da AudioCodes® ligado, via E1, a uma carta designada por 30AB.

Para o ip-*Keel*® Acesso baseado em MEGACO/H.248, está em fase de construção um elemento de controlo com as mesmas funcionalidades que o AGCF da Figura 15, utilizando *stacks* SIP *opensource* e algumas funcionalidades (extensões) já implementadas por essas *stacks* para o desenvolvimento de SIP *proxies* e SIP *User Agents*.

## *6.3.1. Sistema baseado em SIP*

### 6.3.1.1. TP-260

Uma das possíveis soluções para implementar um A-VGF passa por utilizar o módulo TP®-260/SIP disponibilizado pela AudioCodes® (Figura 64).

Esta solução é idêntica em termos funcionais, protocolos suportados e arquitectura interna, ilustrada na Figura 17, ao T-MGF Mediant™ 2000. Ambos possuem os mesmos módulos principais e obedecem aos mesmos requisitos para a solução T-MGF da arquitectura PES do TISPAN.

A diferença reside ao nível físico, a TP®-260 ganha em termos de portabilidade o que permite a sua utilização na implementação de T-MGFs quando o espaço é um factor importante. Esta solução possui um barramento PCI para alimentação, permitindo a sua colocação num *slot* PCI de um computador.

Figura 64- TP®-260/SIP da AudioCodes® [105].

Fisicamente, este módulo disponibiliza uma porta RJ-45 de *ethernet* 10/100 Base-TX para ligação a LANs ou WANs, e até 8 interfaces físicas E1/T1/J1 (RJ-48c) nas quais podem ser ligadas directamente uma rede PSTN/ISDN ou uma plataforma de interface entre POTS e a

ligação E1/T1, para a implementação de A-MGFs ou A-VGFs, consoante o *firmware* de sinalização instalado, com interfaces analógicas.

### 6.3.1.2. Carta 30AB

A carta de 30AB, ilustrada na Figura 65, agrega trinta linhas analógicas telefónicas numa única ligação E1.

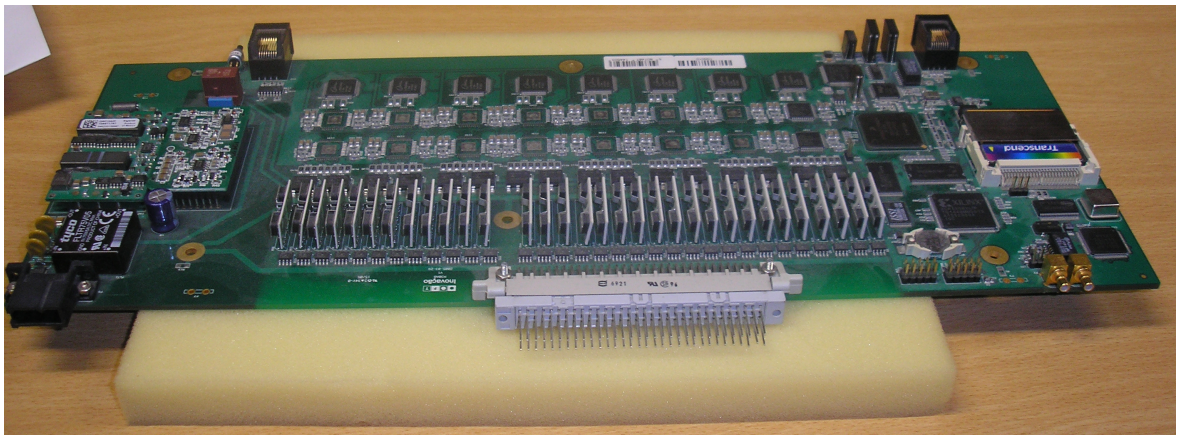


Figura 65- Carta 30AB.

Fisicamente é constituída por trinta interfaces analógicas para POTS e uma interface coaxial E1 digital. Cada *slot*/circuito E1 tem correspondência directa com cada ligação física dos POTS. Esta carta, internamente, converte a sinalização digital recebida de um *slot* E1 na respectiva sinalização analógica para o POTS e vice-versa, permitindo, assim, a realização de chamadas de voz.

### 6.3.1.3. Cenário SHipNET

Na Figura 66 está ilustrado o cenário para testes do ip-*Keel*® Acesso baseado em SIP. Este cenário utiliza o demonstrador *SHipNET*® e o sistema ip-*Keel*® *Trunking* já descrito, para a realização de testes de chamadas entre o POTS ligados à carta 30AB e os terminais da rede PSTN. Este cenário pretende demonstrar as potencialidades do A-VGF da arquitectura PES do TISPAN (Figura 15) com acessos PRI (*trunks* E1/T1/J1 da TP®-260) e analógicos (interface com 30AB).

Para os testes pretendidos, ligou-se à interface analógica #3 da carta 30AB um POTS e à interface coaxial E1, o *trunk* #1 da TP®-260 (192.168.123.118:5060) através de um conversor de impedâncias. A TP®-260 foi posteriormente ligada ao P-CSCF de endereço:porto IP 192.1168.21.2:4060 do *SHipNET*® para a troca de sinalização SIP.

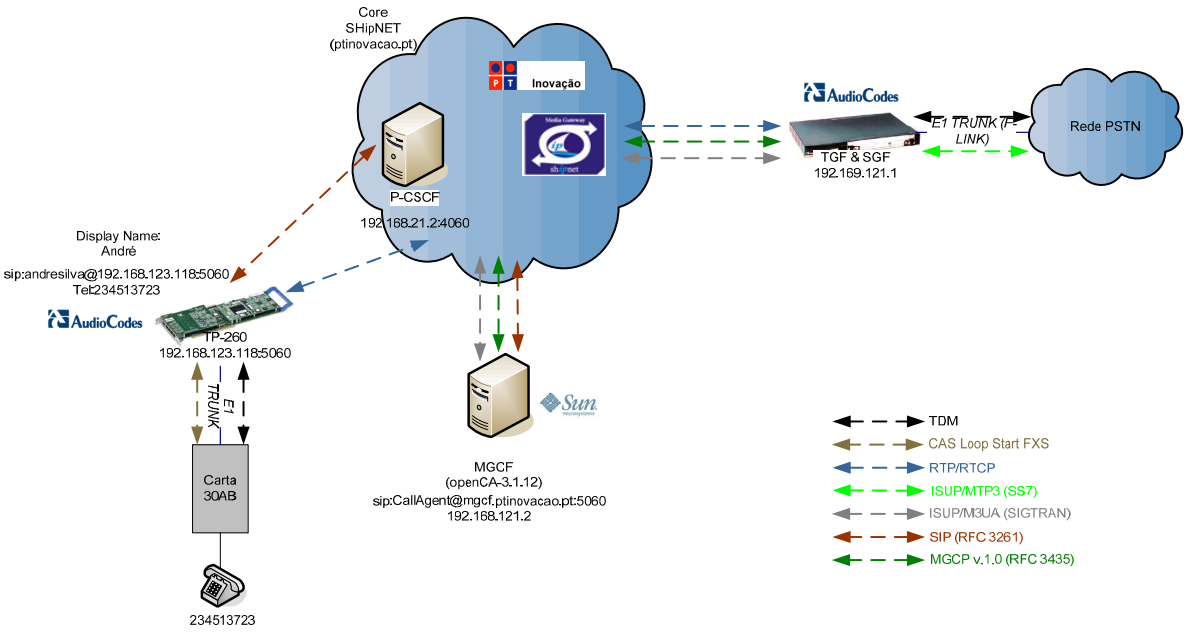



Figura 66- Cenário *SHipNET*® – ip-*Keel*® Acesso.

Nesta configuração o ip-*Keel*® de Acesso é tratado pelo P-CSCF como se vários terminais/clientes SIP estivessem ligados. Como só existe um terminal POTS "234513723", é como se estivesse ligado ao P-CSCF um terminal SIP.

Para este cenário de teste, a TP®-260 foi configurada com o número telefónico do POTS e o respectivo *slot*/circuito associado no *trunk* E1 (*slot*/circuito #3), bem como um conjunto de parâmetros de autenticação: SIP URI associado ao POTS (*sip:andresilva@ptinovacao.pt*), *username* (*andresilva*), *password*, domínio (*sip:ptinovacao.pt*), etc., de forma a permitir o envio do SIP *Register* do POTS para o *SHipNET*® e por conseguinte realizar chamadas através deste domínio.

Para o cenário da Figura 66 foi necessário alterar a versão do *firmware* SIP da TP®-260 para o 4.8, pois a versão 4.6 instalada não permitia que a TP®-260 enviasse registos (SIP *Registers*) de cada um dos terminais POTS.

Relativamente à carta 30AB foram necessárias efectuar algumas alterações para permitir a comunicação entre esta carta e a TP®-260 e para efectuar um correcto controlo dos terminais POTS.

Relativamente ao protocolo de sinalização utilizado entre esta carta e a TP®-260, o escolhido foi o E1 *Channel Associated Signaling* (CAS) *LoopStart Foreign eXchange Subscriber* (FXS). O motivo da escolha desta sinalização, deve-se ao facto do *LoopStart* FXS, transportado no CAS, ser utilizado para os acessos analógicos, da existência de um

ficheiro com a informação da sinalização *Channel Associated Signaling* (CAS) *LoopStart* FXS preparado para introduzir na TP®-260, a simplicidade de implementação e a disponibilização de uma tabela com a informação dos bits AB para cada estado, o que permitiu alterar o *software* da carta 30AB de acordo com a sinalização indicada na Tabela XII e Tabela XIII.

| **State** | **Transmit Signalling** | | **Receive Signalling** | |
|---|---|---|---|---|
| | A | B | A | B |
| *Idle State* | 0 | 1 | 0 | 1 |
| *Seizure* | 0 | 1 | 1 | 1 |
| *Completion of Dialling (Dial Tone + Collecting Digits)* | 0 | 1 | 1 | 1 |
| *Answer* | 0 | 0/1 | 1 | 1 |

Tabela XII- Bits AB do CAS para chamada de entrada (Carta 30AB para TP®-260).

| **State** | **Transmit Signalling** | | **Receive Signalling** | |
|---|---|---|---|---|
| | **A** | **B** | **A** | **B** |
| *Idle State* | 0 | 1 | 0 | 1 |
| *Ring on* | 0 | 0 | 0 | 1 |
| *Ring off* | 0 | 1 | 0 | 1 |
| *PBX Answers Call* | 0 | X | 1 | 1 |
| *Normal Talking State* | 0 | X | 1 | 1 |

Tabela XIII- Bits AB do CAS para chamada de saída (TP®-260 para carta 30AB).

Foram também corrigidas algumas falhas no *software* da carta 30AB, relativamente ao controlo dos POTS e à sua máquina de estados correspondente, que se traduzem em dificuldades encontradas durante a montagem:

- Correcção de um erro relativo ao estado de METTER que era inicializado várias vezes fazendo aumentar significativamente o estado de ocupação do processador e inviabilizando assim a utilização de vários terminais simultaneamente;
- Introdução do sinal de interrompido no terminal POTS quando a chamada é terminada pelo lado SIP;
- Correcção de um erro relativo à entrada no estado METTER quando o terminal POTS era atendido.

#### 6.3.1.3.1 Testes e resultados

No cenário indicado na Figura 66 do ip-*Keel*® Acesso baseado em SIP como parte integrante do demonstrador RPG *SHipNET*®, foram efectuados alguns testes de chamadas de voz entre o POTS, com o número "234513723" e SIP URI *sip:andresilva@ptinovacao.pt*, e o terminal móvel dos cenários anteriores por intermédio da rede PSTN.

Os testes descritos de seguida pretendem simular situações reais que podem ocorrer durante uma chamada, como por exemplo o terminal da rede PSTN encontrar-se ocupado numa chamada iniciada pelo POTS do A-VGF (TP®-260 mais carta 30AB), e uma chamada bem sucedida de um POTS da rede PSTN para o POTS do A-VGF.

Antes de efectuar estes testes, o POTS "234513723" foi registado no domínio *SHipNET*® de igual forma que um simples terminal SIP, com o SIP URI *sip:andresilva@ptinovacao.pt* e TEL URI *tel:+351234513723*. O processo de registo do terminal SIP ou POTS do A-VGF, de acordo com a normalização TISPAN/3GPP, será descrito na secção 6.3.2.1.3 da implementação do AGCF.

Após o registo do POTS, procedeu-se à realização do primeiro teste de numa chamada do POTS para PSTN com o terminal móvel ocupado. O procedimento do teste passou por colocar inicialmente este terminal no estado ocupado, através da realização de uma chamada para um determinado número antes da marcação no POTS do número do móvel. A sinalização SIP trocada entre o A-VGF (192.168.123.118) e o P-CSCF do *SHipNET*® (192.168.21.2) está ilustrada no diagrama da Figura 67. A sinalização com o ip-*Keel*® *Trunking* não está ilustrado, pois desse lado o processo é idêntico ao ilustrado na Figura 59.

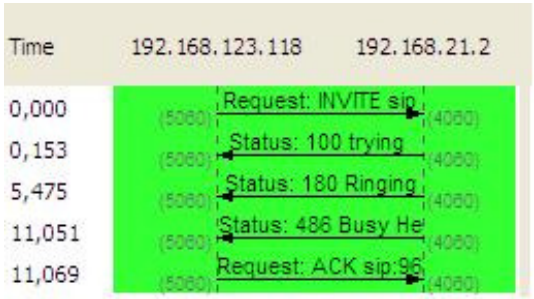



Figura 67- Diagrama de sinalização de terminal ocupado para o cenário *SHipNET*®.

Como se pode constatar pela Figura 67, o processo de estabelecimento da sessão (SIP *Invite*, 100 *Trying* e 180 *Ringing*) é igual ao dos outros testes realizados e vai de encontro

com o indicado pela normalização. Apenas a mensagem SIP 486 *Busy Here* aparece pela primeira vez devido ao estado ocupado do terminal da rede PSTN.

Inicialmente, antes da marcação do número "96xxxxxxx" no POTS, o sistema A-VGF encontra-se no estado *Idle* (Tabela XII), após o *off-hooh* do POTS para a marcação deste número, é enviada sinalização E1 CAS da carta 30AB para a TP®-260 com os *bits* AB afectados com o valor 11 (Tabela XII) com o intuito de indicar à TP®-260 que o POTS, ligado na interface analógica #3 (*slot*/circuito #3 do E1), está *off-hook* e pretende estabelecer uma chamada. De seguida foi marcado o número do móvel no POTS e no final, após um *timeout* de recepção dos dígitos, o sistema entrou no estado *Completion of Dialling* (Tabela XII). Como resultado foi enviado o SIP *Invite* com o SIP URI *sip:andresilva@ptinovacao.pt* configurado para o *slot*/circuito #3 do E1 na TP®-260. O conteúdo desta mensagem está ilustrado na Figura 68.

```
Internet Protocol, Src: 192.168.123.118 (192.168.123.118), Dst: 192.168.21.2 (192.168.21.2)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 4060 (4060)
Session Initiation Protocol
    Request-Line: INVITE sip:96xxxxxxx@ptinovacao.pt;user=phone SIP/2.0
    Message Header
        Via: SIP/2.0/UDP 192.168.123.118;branch=z9hG4bKac1906504963
        Max-Forwards: 70
        From: <sip:andresilva@ptinovacao.pt>;tag=1c1906498760
        To: <sip:96xxxxxxx@ptinovacao.pt;user=phone>
        Call-ID: 19064980971120003303 5@192.168.123.118
        CSeq: 1 INVITE
        Contact: <sip:andresilva@192.168.123.118>
        Supported: em,100rel,timer,replaces,path,early-session,resource-priority
        Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
        User-Agent: amgw_pots/v.5.00A.043
        Content-Type: application/sdp
        Content-Disposition: session
        Content-Length: 400
    Message body
        Session Description Protocol
            Session Description Protocol Version (v): 0
            Owner/Creator, Session Id (o): AudiocodesGW 1906463277 1906462962 IN IP4 192.168.123.118
            Session Name (s): Phone-Call
            Connection Information (c): IN IP4 192.168.123.118
            Time Description, active time (t): 0 0
            Media Description, name and address (m): audio 6020 RTP/AVP 8 0 2 18 3 13 101
            Media Attribute (a): rtpmap:8 PCMA/8000
            Media Attribute (a): rtpmap:0 PCMU/8000
            Media Attribute (a): rtpmap:2 G726-32/8000
            Media Attribute (a): rtpmap:18 G729/8000
            Media Attribute (a): fmtp:18 annexb=yes
            Media Attribute (a): rtpmap:3 GSM/8000
            Media Attribute (a): rtpmap:101 telephone-event/8000
            Media Attribute (a): fmtp:101 0-15
            Media Attribute (a): ptime:20
            Media Attribute (a): sendrecv
            Media Attribute (a): rtcp:6021 IN IP4 192.168.123.118
```

Figura 68- SIP *Invite* do teste terminal ocupado - cenário *SHipNET®*.

O R-URI da mensagem tem o número de telefone do terminal móvel destinatário na forma de SIP URI com o parâmetro *user=phone* de acordo com a normalização do 3GPP [28].

A TP®-260 também envia no SIP *Invite*, para além dos campos mandatários, o campo opcional *Supported* para indicar aos elementos do *core SHipNET®* as extensões e funcionalidades que o terminal pode suportar para esta sessão, destacando-se o *100rel* e o

*early-session*, e o campo *Allow* para informar o *core SHipNET®*, quais os métodos que suporta e que consegue processar. O parâmetro *100rel* no campo *Supported* informa o utilizador destino, neste caso o ip-*Keel® Trunking*, que o A-VGF aceita e processa SIP *Responses* provisórios (Tabela III) com mecanismo de fiabilidade[20]. Se uma resposta provisória for recebida, por exemplo o SIP 180 *Ringing*, com um campo *Require* contendo o parâmetro *100rel*, então o A-VGF deve enviar uma mensagem SIP *Provisional Response ACKnowledgement* (PRACK) (Tabela II) dentro do diálogo associado ao SIP 180 *Ringing* [108]. O parâmetro *early-session* do campo *Supported*, juntamente com o campo *Content-Disposition*, é utilizado para informar o utilizador destino que o A-VGF está disposto a estabelecer uma sessão *early-media* utilizando o mecanismo oferta/resposta. Para estabelecer esta sessão dentro do diálogo, foi enviado juntamente no SIP *Invite* o SDP contendo os parâmetros *media* para a chamada e para a sessão *ealy-media*. O destino ip-*Keel® Trunking* ao receber este SIP *Invite*, enviou uma resposta SIP 180 *Ringing* com o SDP contendo os seus parâmetros media para a sessão *early-media*: é enviada esta resposta, mesmo sem o terminal móvel da rede PSTN ser alertado, pois encontra-se no estado ocupado [119].

Devido ao terminal móvel se encontrar no estado ocupado, o sistema ip-*Keel® Trunking*, após receber uma mensagem ISUP REL [35] da rede PSTN com indicação de ocupado, envia para o S-CSCF do *SHipNET®* uma resposta SIP 486 *Busy Here*, que por sua vez chega ao A-VGF com o conteúdo indicado na Figura 69.

```
Internet Protocol, Src: 192.168.21.2 (192.168.21.2), Dst: 192.168.123.118 (192.168.123.118)
User Datagram Protocol, Src Port: 4060 (4060), Dst Port: 5060 (5060)
Session Initiation Protocol
    Status-Line: SIP/2.0 486 Busy Here
    Message Header
        Via: SIP/2.0/UDP 192.168.123.118;rport=5060;branch=z9hG4bKac1906504963
        From: <sip:andresilva@ptinovacao.pt>;tag=1c1906498760
        To: <sip:96xxxxxxx@ptinovacao.pt;user=phone>;tag=ds-538f-43cdbd1aab270
        Call-ID: 190649809711200033035@192.168.123.118
        CSeq: 1 INVITE
        Content-Length: 0
        Reason: Q.850 ;text="User busy CCBS indicator";cause=17
        P-Asserted-Identity: <tel:+351>
        Contact: <sip:CallAgent@mgcf.ptinovacao.pt;transport=udp>
```

Figura 69- SIP 486 *Busy Here* do teste terminal ocupado - cenário *SHipNET®*.

O campo *Reason* contém a indicação da razão da terminação da sessão, mapeada da rede PSTN pelo sistema ip-*Keel® Trunking*. Neste teste, o ISUP REL com a indicação de

[20] *Reliable Provisional Responses*.

utilizador ocupado é mapeado numa mensagem SIP 486 *Busy Here* com essa indicação (*text="User busy CCBS indicator";cause=17*).

Após receber esta mensagem SIP, a TP®-260 enviou o sinal *media* de interrompido (ocupado) para o POTS através do *slot*/canal 3 do E1.

O teste seguinte pretende demonstrar apenas o processo de sinalização de uma chamada simples do terminal fixo PSTN "234377900" (IT) para o POTS registado com o SIP URI *sip:andresilva@ptinovacao.pt*. O diagrama de sinalização SIP trocada entre o A-VGF e o P-CSCF para este teste está ilustrado na Figura 70.


Figura 70- Diagrama de sinalização da chamada PSTN para POTS - cenário *SHipNET*®.

Mais uma vez, o processo de estabelecimento da sessão (mensagens trocadas) e terminação é igual ao dos testes realizados anteriormente. Na Figura 71 está ilustrado o conteúdo da mensagem SIP *Invite* enviada pelo P-CSCF para o estabelecimento da sessão.

```
Internet Protocol, Src: 192.168.21.2 (192.168.21.2), Dst: 192.168.123.118 (192.168.123.118)
User Datagram Protocol, Src Port: 4060 (4060), Dst Port: 5060 (5060)
Session Initiation Protocol
    Request-Line: INVITE sip:andresilva@192.168.123.118 SIP/2.0
    Message Header
        Record-Route: <sip:mt@pcscf.ptinovacao.pt:4060;lr>
        Record-Route: <sip:mt@scscf.ptinovacao.pt:6060;lr>
        Record-Route: <sip:192.168.121.7;lr;ftag=ds-b7d-441beb9439b2c>
        From: 234377900 <tel:+351234377900>;tag=ds-b7d-441beb9439b2c
        To: <tel:+351234513723>
        Call-ID: 502564f8-1dd2-11b2-952f-ced3b009a08e@mgcf
        CSeq: 5240 INVITE
        Content-Length: 904
        Content-Type: application/sdp
        Supported: 100rel
        Supported: timer
        P-Asserted-Identity: <tel:+351234377900>
        Session-Expires: 1800
        Contact: <sip:CallAgent@mgcf.ptinovacao.pt;transport=udp>
        Via: SIP/2.0/UDP 192.168.21.2:4060;branch=z9hG4bK0e4a.c8a2f4f1.0
        Via: SIP/2.0/UDP 192.168.20.5:6060;rport=6060;branch=z9hG4bK0e4a.d6cc6d22.0
        Via: SIP/2.0/UDP 192.168.20.5;branch=z9hG4bK0e4a.4da77135.0
        Via: SIP/2.0/UDP 192.168.121.7;branch=z9hG4bK0e4a.8c3461d.0
        Via: SIP/2.0/UDP 192.168.121.2:5060;branch=z9hG4bK50258e10-1dd2-11b2-9895-9c9e6c0a9f29
        Max-Forwards: 14
        P-Called-Party-ID: <tel:+351234513723>
    Message body
```

Figura 71- SIP *Invite* da chamada PSTN para POTS - cenário *SHipNET*®.

Os campos *Record-Route* são colocados em modo sequencial pelos elementos IMS do *SHipNET*® atravessados pela mensagem, ou seja, o último elemento (P-CSCF) está sempre em primeiro lugar. Estes campos têm o SIP URI desses elementos do domínio *SHipNET*® e são utilizados para que futuros SIP *Requets* pertencentes à sessão atravessem os mesmos elementos que o SIP *Invite*. O campo *P-Asserted-Identity* foi adicionado para cobrir a possibilidade do POTS possuir um mostrador digital para o número do originário. Neste teste não é o caso, pois para além do POTS não possuir essa característica, a carta de 30 AB também não está preparada para receber sinalização fora de banda com a indicação do número do originário.

A TP®-260 ao receber esta mensagem envia a sinalização E1 CAS com os *bits* AB igual 00, passando o sistema do estado *idle* para *Ringing on* (Tabela XIII). Neste momento foi ouvido o sinal de alerta *Ringing* no POTS. Para este sinal ser tocado de acordo com o convencional, a TP®-260 alterna o *bit* B do conjunto AB do CAS, que envia para carta 30AB, de 0 (estado *Ring on*) para 1 (estado *Ring off*) e vice-versa com uma determinada frequência (Tabela XIII). Durante este estado, a TP®-260 envia para o P-CSCF do *SHipNET*® a resposta SIP 180 *Ringing* ao SIP *Invite* para informar a rede, mais precisamente o terminal da rede PSTN, que o POTS foi alertado. Quando é feito o *off-hook* do POTS são enviados os *bits* AB do E1 CAS com o valor 11 da carta 30AB para a TP®-260, passando o sistema do estado *Ringing* para *PBX Answers Call* e posteriormente para *Normal Talking State* (Tabela XIII). Neste estado, a TP®-260 envia para o P-CSCF a mensagem SIP 200 OK de atendimento da chamada pelo POTS.

### 6.3.2. Sistema baseado em MEGACO/H.248

Para a solução MEGACO/H.248 do ip-*Keel*® Acesso foi dado início no âmbito deste trabalho, à implementação do elemento aplicacional AGCF, descrito na secção 4.2.1.2 (Figura 15), para o controlo de acessos analógicos, básicos (BRI) e primários (PRI) dos A/R-MGFs na concretização de chamadas com utilizadores em ambiente IP.

Para este sistema apenas foi implementado o processo de registo do lado SIP para o AGCF. Funcionalidades como a interacção de controlo com o MGF, com o *Application Server Function* (ASF), e com o *Resource and Admission Control Subsystem* (RACS) e o *Network Attachment Subsystem* (NASS) não foram implementadas no final desta Dissertação, sendo trabalho para realizações futuras de médio/longo prazo.

De seguida é feita uma descrição do desenvolvimento do processo de registo SIP da solução AGCF, abordando temas como descrição de todos os passos/cenários intermédios, configuração dos elementos constituintes de acordo com o cenário usado para efeitos demonstrativos das suas potencialidades, e as dependências existentes para sistemas externos.

#### 6.3.2.1. AGCF

A Figura 72 ilustra a arquitectura interna da aplicação AGCF do ip-*Keel*® Acesso em fase de implementação.

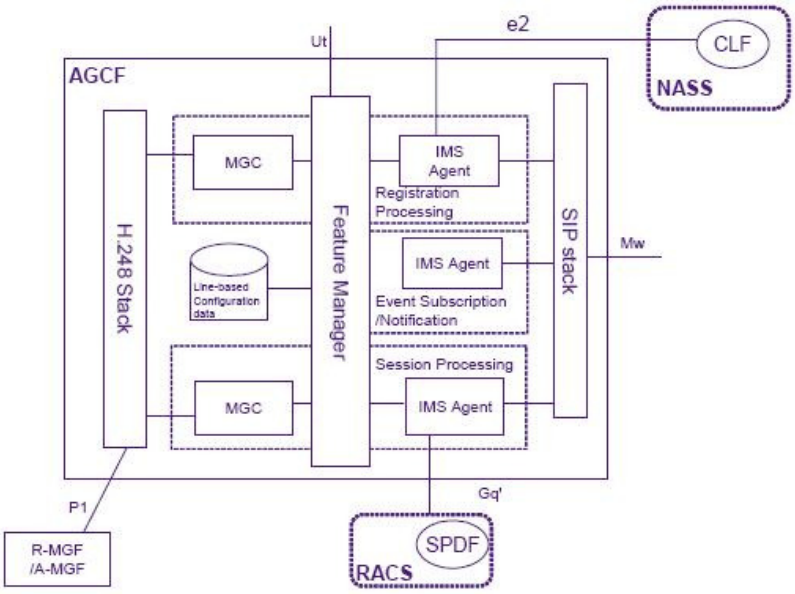



Figura 72- Arquitectura interna do AGCF [3].

O AGCF pode ser dividido internamente em três módulos lógicos de acordo com a norma ETSI TS 182 012 [3]:

- *Media Gateway Controller* (MGC);
- *Feature Manager*;
- IMS *Agent*.

O módulo MGC é responsável pelo controlo de A/R-MGFs baseados no perfil do protocolo MEGACO/H.248 definido pelo TISPAN na norma ETSI ES 283 002 [73]. Este módulo possui as seguintes funcionalidades no processamento de registos e de sessões dos terminais ligados aos A/R-MGFs:

- Processamento de comandos H.248 *ServiceChange* [39] enviados pelo A/R-MGF para o registo ou remoção de registo dos terminais;

- Envio periódico de comandos H.248 *Audit* [39] de forma a manter o estado dos terminais actualizado no AGCF;
- Controlo de *dial tones* e anúncios no A/R-MGF;
- Informa o A/R-MGF através de comandos H.248 *Notify* [39] para o envio de eventos telefónicos e dígitos DTMF;
- Recepção e processamento de eventos telefónicos e dígitos DTMF do A/R-MGF;
- Análise dos dígitos DTMFs enviados para detecção de chamadas de emergência;
- Envio de *dial plans* para o A/R-MGF.

O módulo *Feature Manager* é o responsável pela coordenação do funcionamento dos restantes módulos do AGCF. Possui as seguintes funcionalidades no processamento de registos dos terminais e no processamento das sessões:

- Processamento das sessões de acordo com a informação de estado do A/R-MGF e dos seus terminais;
- Sinaliza o módulo SIP *User Agent* para o envio de registos individuais ou em grupos dos terminais para o *core* IMS/TISPAN;
- Interage com o *Application Server* para obter informações (*dial tone*, etc.) dos utilizadores.

O módulo IMS *Agent* implementa os mesmos procedimentos associados aos elementos P-CSCF e IMS *User Equipment* (UE) do *core* IMS. Estas funcionalidades estão indicadas na norma 3GPP TS 23.228 [28]. As mensagens recebidas são enviadas para o módulo *Feature Manager* que as processa de acordo com a informação presente na mensagem de sinalização e no *Line-Based Configuration data* do destinatário.

No módulo *Line-Based Configuration data*, acedido pelo *Feature Manager*, estão guardadas as identificações públicas/privadas, os parâmetros de autenticação para o registo, o estado presente e as configurações (*dial tone*, etc.) de cada um dos terminais ligados ao A/R-MGF.

Os procedimentos subjacentes a cada um dos módulos do AGCF estão indicados na norma ETSI TS 183 043 [120].

#### 6.3.2.1.1 libosip2/libeXosip2

O *libosip2* é uma *stack* SIP *open source* criada no âmbito do projecto oSIP [121] em Setembro de 2000 que visa a contribuir para o desenvovimento contínuo de uma biblioteca utilizada em implementações baseadas no protocolo SIP. Esta *stack*, escrita em linguagem

C, possui internamente uma máquina de estados e um *parser* que permite o desenvolvimento de terminais, *proxies*, ou outro tipo de aplicações SIP de acordo com o especificado no RFC 3261 [32]. Esta *stack* serve de base a uma extensão desenvolvida também pelo oSIP com *Application Programming Interfaces* (APIs) avançadas, de forma a facilitar e optimizar as implementações SIP que utilizam as funções da biblioteca *libosip2*. A esta extensão do *libosip2* designa-se por *libeXosip2* [121].

#### 6.3.2.1.2 open IMS core (FOKUS)

O FOKUS [122] é um instituto de investigação e desenvolvimento na área das telecomunicações fundado em 1998 em Berlim. Este instituto lançou em 2004 uma aplicação designada por *open* IMS *core* que pretende dar continuidade ao desenvolvimento de uma plataforma IMS *open source*, integrando os principais elementos: P-CSCF, S-CSCF, I-CSCF e HSS, que podem ser executados e configurados de forma independente através de um *script*. Esta implementação é baseada no SIP *Proxy*/*Server* do SIP *Express Router* (SER) [123].

#### 6.3.2.1.3 IP Multimedia Subsystem Agent

Numa primeira fase foi implementado o bloco IMS *Agent* do AGCF para o processo de registo (Figura 72). Para este cenário foi instalada a *stack* SIP *libosip2-3.0.1* e a sua extensão *libeXosip2-3.0.1* [121] num computador provisório com o sistema operativo *Linux* (distribuição *Ubuntu* 7.10) configurado com o endereço IP 192.168.127.68. Também foi instalado na mesma máquina o *open* IMS *core* do FOKUS [122].

O cenário IMS *Agent* para o processo de registo foi implementado a partir da aplicação "*sip_reg.c*" do *libeXosip2-3.0.1*, que implementa o processo de registo de um terminal SIP sem autenticação, e do *script* "*pcscf.cfg*" executado com o *open* IMS *core*, que implementa as funcionalidades do elemento P-CSCF do IMS de acordo com a norma 3GPP TS 23.228 [28] para o AGCF. Estas aplicações tiveram de ser adaptadas ao ambiente IMS/TISPAN do demonstrador *SHipNET*®, para que o processo de registo para o cenário IMS *Agent* se realize segundo as normas ETSI TS 183 043 [120] e ETSI ES 283 003 [82].

A principal alteração ao ficheiro "*sip_reg.c*" foi a adição do procedimento de autenticação do utilizador exigido pelo *core SHipNET*® no processo de registo. Os parâmetros de entrada desta aplicação foram alterados para também introduzir as credenciais de autenticação do utilizador, ficando no final os seguintes parâmetros:

- SIP URI público do utilizador;

- SIP URI privado do utilizador;
- *Password* de autenticação;
- Domínio de autenticação (*Domain*);
- Tempo de expiração do registo (*Expires register time*).

Posteriormente estes parâmetros serão armazenados numa base de dados interna designada por *Line-Based Configuration data* e passados ao IMS *Agent* pelo *Feature Manager* através de primitivas internas especificadas na norma ETSI TS 183 043 [120].

A função *eXosip_add_authentication_info* [124], introduzida na aplicação, guarda os parâmetros de autenticação: *username*, SIP URI, *password* e o *domain* do utilizar que se pretende registar. A aplicação, ao receber uma reposta ao registo com pedido de autenticação, gera através da função *eXosip_automatic_action* [124] um novo registo com os parâmetros de autenticação do utilizador e uma resposta cifrada pelo protocolo MD5. À mensagem SIP *Register* inicial enviada por esta aplicação para o componente P-CSCF do AGCF, foi adicionado o campo *Supported* com o valor *path* conforme a especificação do IMS/TISPAN através da função *osip_message_set_supported*. Esta aplicação envia as mensagens SIP sobre *User Datagrama Protocol* (UDP) para o componente P-CSCF através do porto configurado 5063.

O *script* "*pcscf.cfg*" também foi alterado para colocar o parâmetro *integrity-protected* igual a *yes* no campo *Authorization*, contendo uma resposta ao desafio de autenticação, mesmo sem o estabelecimento prévio de uma ligação segura *IP security* (IPsec) entre o componente terminal SIP ("*sip_reg.c*") e o componente P-CSCF do AGCF. Para este cenário não foi implementada a ligação segura de acordo com a norma ETSI ES 283 003 [82], pois estes componentes fazem parte da mesma aplicação AGCF (Figura 73) e portanto é como se o terminal SIP fosse um elemento pertencente ao *core* IMS/TISPAN do *SHipNET*®. Os campos *Require* e *Proxy-Require* com o valor *sec-agree*, e o campo *Security-Client* contendo a lista de algoritmos de segurança do utilizador para estabelecer a ligação segura não foram colocados na mensagem SIP *Register* inicial, nem o procedimento de verificação e estabelecimento de segurança no componente P-CSCF, conforme indicado na norma ETSI ES 283 003 [82].

O P-CSCF foi configurado para enviar mensagens SIP através do porto 5060 para o I-CSCF externo do *SHipNET*® (192.168.20.5).

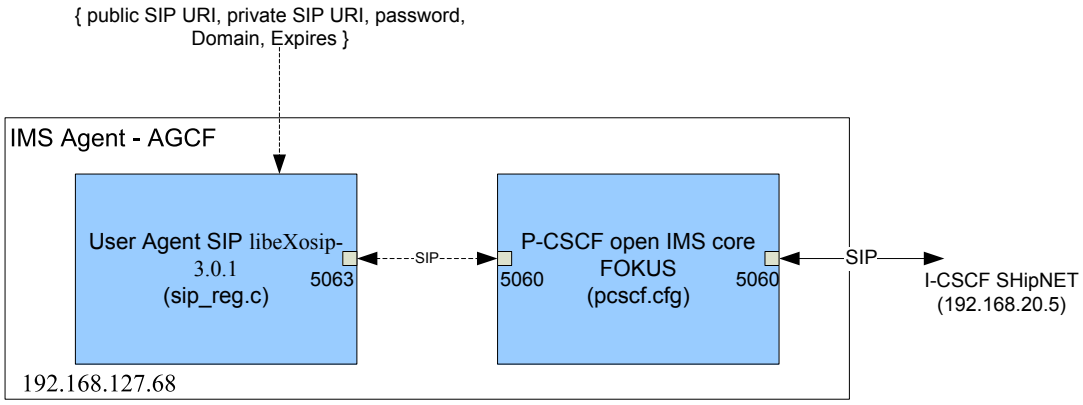



Figura 73- Protótipo IMS *Agent* para o registo do AGCF.

Os procedimentos executados pelo protótipo IMS *Agent* ilustrado na Figura 73 estão esquematizados no diagrama do Anexo IV para o processo de registo. Esta implementação (Anexo IV) será descrita na secção seguinte através do teste de registo do *sip:andresilva@ptinovacao.pt*.

#### 6.3.2.1.3.1 Testes e resultados

Para a implementação e teste do processo de registo SIP do AGCF foram utilizados os seguintes parâmetros de acordo com o indicado na secção anterior:

- SIP URI público do utilizador: *sip:andresilva@ptinovacao.pt*;
- SIP URI privado do utilizador: *sip:andresilva@ptinovacao.pt*;
- Domínio de autenticação (*Domain*): *ptinovacao.pt*;
- Tempo de expiração do registo (*Expires register time*): 3600 segundos.

Pela análise do diagrama do Anexo IV, antes de usar qualquer função do *libeXosip2* a primeira tarefa a efectuar é inicializar a *stack* SIP *libosip2* e a extensão *libeXosip2* (*parser* e máquina de estados) no arranque do IMS *Agent*.

Após esta inicialização foi criado um *socket* UDP de escuta no porto 5063 através da função *eXosip_listen_addr* [124] (Anexo IV) para a comunicação com o P-CSCF interno. As credenciais de autenticação: *username*, SIP URI, *password* e domínio de autenticação do utilizador, também foram adicionadas no início através da função *eXosip_add_authentication_info* [124] à aplicação, para o caso de receber um pedido de autenticação no processo de registo. Para este cenário foram adicionadas as credencias do utilizador com SIP URI *sip:andresilva@ptinovacao.pt*.

De seguida foi criada a mensagem inicial SIP *Register* com os campos mandatários indicados na Tabela IV, construídos a partir dos parâmetros: SIP URI público do utilizador

que se pretende registar (*sip:andresilva@ptinovacao.pt*), domínio para onde é enviado o SIP *Register* colocado no R-URI (*sip:ptinovacao.pt*[21]), tempo de duração do registo em segundos (*Expires*: 3600) e o *username* (*andresilva*) mais o IP do IMS *Agent* (*192.168.127.68*) para construir o campo *Contact* da mensagem (*sip:andresilva@192.168.127.68*).

Foi adicionado o campo *Supported* através da função *osip_message_set_supported* ao SIP *Register* inicial com o valor *path* para indicar ao *core* RPG que o AGCF suporta a funcionalidade *Path*. Este SIP *Register* foi enviado para o *ptinovacao.pt* (192.168.127.68:5060), que corresponde ao P-CSCF segundo a entrada no ficheiro "*/etc/hosts*", através da função *eXosip_register_send_register* [124] (Anexo IV).

Após o envio, o IMS *Agent* fica a aguardar uma resposta do P-CSCF interno, mais propriamente de um SIP 401 *Unauthorized* para a autenticação do utilizador.

Os procedimentos do P-CSCF do FOKUS ao receber esta mensagem estão documentados na norma ETSI ES 283 003 [82]. Este adiciona o campo *Path* com o valor <*sip:term@192.168.127.68:5060;lr*>, que inclui o endereço IP do componente P-CSCF do AGCF para informar o S-CSCF que todas as mensagens SIP *Requests* para o *sip:andresilva@ptinovacao.pt* devem terminar no AGCF. O campo *Require* com o valor *path* adicionado é utilizado para informar o *core SHipNET*® que a mensagem SIP *Register* possui o campo *path* e que este o deve suportar e processar obrigatoriamente. O campo *P-Charging-Vector* contém o parâmetro IMS *Charging Identity* (icid) utilizado para correlacionar informação de taxação de serviço e para identificar a transacção ou diálogo. Este deve ser um valor único global gerado de acordo com a especificação 3GPP TS 32.260 [125]. O campo *P-Visited-Network-ID* é adicionado com o valor *ptinovacao.pt* para identificar o nome do domínio onde é feito o registo.

Após completado o SIP *Register* com os campos indicados e ilustrados na Figura 74, este é enviado para o I-CSCF (192.168.20.5:5060) do *SHipNET*®.

[21] Foi colocada uma entrada no ficheiro "*/etc/hosts"* para traduzir o *ptinovacao.pt* no endereço IP do componente P-CSCF.

```
Internet Protocol, Src: 192.168.127.68 (192.168.127.68), Dst: 192.168.20.5 (192.168.20.5)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Session Initiation Protocol
    Request-Line: REGISTER sip:ptinovacao.pt SIP/2.0
    Message Header
        Via: SIP/2.0/UDP 192.168.127.68;branch=z9hG4bK106.8cd224f.0
        Via: SIP/2.0/UDP 192.168.127.68:5063;rport=5063;branch=z9hG4bK1067196795
        From: <sip:andresilva@ptinovacao.pt>;tag=707044426
        To: <sip:andresilva@ptinovacao.pt>
        Call-ID: 1521110179@192.168.127.68
        CSeq: 1 REGISTER
        Contact: <sip:andresilva@192.168.127.68>
        Max-Forwards: 16
        User-Agent: AGCFv1.0 - POTS
        Expires: 3600
        Supported: path
        Content-Length: 0
        Path: <sip:term@192.168.127.68:5060;lr>
        Require: path
        P-Charging-Vector: icid-value="AGCFabcd48209afb00000000"; icid-generated-at=127.0.0.1; orig-ioi="ptinovacao.pt"
        P-Visited-Network-ID: ptinovacao.pt
```

Figura 74- SIP *Register* inicial.

Após o envio, o P-CSCF do IMS *Agent* entra no estado de espera de uma resposta do I-CSCF do *SHipNET*®. Se a resposta recebida for uma mensagem SIP 401 *Unauthorized* com o campo *WWW-Authenticate* impondo um desafio (*Challenging*) do S-CSCF ao utilizador, então significa que esse utilizador (*sip:andresilva@ptinovacao.pt*) consta do conjunto de clientes do domínio *SHipNET*® e foi submetido a um pedido de autenticação na rede. A descrição dos parâmetros do campo *WWW-Authenticate* está documentada na norma ETSI ES 283 003 [82]. O conteúdo desta mensagem está ilustrado na Figura 75.

```
Internet Protocol, Src: 192.168.20.5 (192.168.20.5), Dst: 192.168.127.68 (192.168.127.68)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Session Initiation Protocol
    Status-Line: SIP/2.0 401 Unauthorized - Challenging the UE
    Message Header
        Via: SIP/2.0/UDP 192.168.127.68:5060;branch=z9hG4bK106.8cd224f.0
        Via: SIP/2.0/UDP 192.168.127.68:5063;rport=5063;branch=z9hG4bK1067196795
        From: <sip:andresilva@ptinovacao.pt>;tag=707044426
        To: <sip:andresilva@ptinovacao.pt>;tag=0f53b9bc5756a8bd9a5590208e75ba82-4b71
        Call-ID: 1521110179@192.168.127.68
        CSeq: 1 REGISTER
        WWW-Authenticate: Digest realm="ptinovacao.pt", nonce="71225d8373f5cdfcc487036638be82f7", algorithm=MD5
        Path: <sip:term@192.168.127.68:5060;lr>
        Service-Route: <sip:orig@scscf.ptinovacao.pt:6060;lr>
        Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, MESSAGE, INFO
        Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
        Content-Length: 0
        Warning: 392 192.168.20.5:6060 "Noisy feedback tells:  pid=24198 req_src_ip=192.168.20.5 req_src_port=5060 in_uri=sip:
```

Figura 75- Resposta SIP 401 *Unauthorized*.

Esta mensagem é enviada para a aplicação baseada no *libeXosip2* retida na função *eXoSIP_event_wait* [124] (Anexo IV) a aguardar por uma resposta do P-CSCF interno. Ao receber o SIP 401 *Unauthorized* envia novamente uma mensagem SIP *Register* com uma resposta ao desafio de autenticação. Esta mensagem contém o campo *Authorization* com os parâmetros: *Digest username* com o SIP URI privado utilizado para construir o *digest* do protocolo *Message-Digest algorithm* 5 (MD5) no momento da autenticação (*Challenging*), *realm* com o nome da rede onde o cliente pretende ser autenticado (*realm=ptinovacao.pt*), *algorithm* com o nome do protocolo utilizado para a cifra (MD5), *Authentication URI* com

o *sip:ptinovacao.pt* e o *Digest Authentication Response* com a resposta ao desafio de autenticação.

Este processo desafio-resposta através de cifragem MD5 é realizado pela função *eXosip_automatic_action* [124] (Anexo IV). Mais informação sobre este processo pode ser consultada na norma ETSI ES 283 003 [82].

Esta mensagem é enviada para o componente P-CSCF que coloca o parâmetro *integrity-protected=yes* no campo *Authorization* como requisito imposto pelo *SHipNET*® para o registo e autenticação do utilizador. Esta mensagem enviada posteriormente para o I-CSCF está ilustrada na Figura 76.

```
Internet Protocol, Src: 192.168.127.68 (192.168.127.68), Dst: 192.168.20.5 (192.168.20.5)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Session Initiation Protocol
    Request-Line: REGISTER sip:ptinovacao.pt SIP/2.0
    Message Header
        Via: SIP/2.0/UDP 192.168.127.68;branch=z9hG4bKef5.99dce6e1.0
        Via: SIP/2.0/UDP 192.168.127.68:5063;rport=5063;branch=z9hG4bK1587736439
        From: <sip:andresilva@ptinovacao.pt>;tag=707044426
            SIP from address: sip:andresilva@ptinovacao.pt
            SIP tag: 707044426
        To: <sip:andresilva@ptinovacao.pt>
            SIP to address: sip:andresilva@ptinovacao.pt
        Call-ID: 1521110179@192.168.127.68
        CSeq: 2 REGISTER
        Contact: <sip:andresilva@192.168.127.68>
            Contact Binding: <sip:andresilva@192.168.127.68>
        Max-Forwards: 16
        User-Agent: AGCFv1.0 - POTS
        Expires: 3600
        Supported: path
        Content-Length: 0
        Authorization: Digest username="andresilva@ptinovacao.pt", realm="ptinovacao.pt", nonce="bd8a3db8a3fd8a3fb8afde3", u
            Authentication Scheme: Digest
            Username: "andresilva@ptinovacao.pt"
            Realm: "ptinovacao.pt"
            Nonce Value: "bd8a3db8a3fd8a3fb8afde3"
            Authentication URI: "sip:ptinovacao.pt"
            Digest Authentication Response: "fdbe07009c411441908ea7b6f6178d12"
            Algorithm: MD5
            integrity-protected="yes"
        Path: <sip:term@192.168.127.68:5060;lr>
        Require: path
        P-Charging-Vector: icid-value="AGCFabcd48209afb00000001"; icid-generated-at=127.0.0.1; orig-ioi="ptinovacao.pt"
        P-Visited-Network-ID: ptinovacao.pt
```

Figura 76- SIP *Register* para autenticação.

O IMS *Agent* do AGCF fica aguardar uma resposta do I-CSCF, caso essa resposta seja um SIP 200 OK então significa que o cliente *sip:andresilva@ptinovacao.pt* foi autenticado no UPSF e registado no I/S-CSCF do domínio *SHipNET*®.

A Figura 77 ilustra a transição de mensagens SIP para o estabelecimento do registo do POTS *sip:andresilva@192.168.127.68* ligado ao A-MGF.


Figura 77- Diagrama de sinalização do registo POTS- cenário *SHipNET*®.

## 6.4. Sumário

Dentro do contexto das RPGs foi criada uma plataforma aplicacional, designada por *SHipNET*®.

Coube no âmbito deste projecto de Mestrado a implementação do sistema responsável pela interligação das redes PSTN/ISDN e das redes fixas xDSL a este demonstrador *SHipNET*®, tendo por base a arquitectura PES do TISPAN. O principal objectivo foi a implementação e configuração física e funcional dos elementos a azul da Figura 29 para o demonstrador *SHipNET*®.

O ip-*Keel*® *Trunking* é uma resposta para o sistema *Media Gateway* de *Trunking* da arquitectura PES do TISPAN composto pela solução da AudioCodes® Mediant™ 2000 para os elementos T-MGF e SGF, e pela solução openCallAgent® da OpenTelecommunications® para o elemento MGCF. O cenário inicial, designado por cenário interno, foi muito importante para adquirir conhecimentos sobre a configuração da Mediant™ 2000 e do openCallAgent® para interligar a rede PSTN com sinalização SS7. Outro cenário intermédio utilizado para a realização de testes com o sistema ip-*Keel*® *Trunking* foi o cenário Amora. Este cenário foi importante para a realização de testes com vários terminais SIP.

Muitos dos testes realizados são situações reais, tais como falhas do lado PSTN e do lado SIP, cancelamento da chamada antes de ser atendida, rejeição da chamada pelo destinatário antes de ser atendida, SIP *timeout* e PSTN *timeout*, terminal ocupado, CLIP, CLIR, número do destinatário não atribuído, etc. Nesta Dissertação apenas foram descritos dois dos testes realizados no cenário *SHipNET*®: processo de cancelamento da chamada pelo lado SIP e mecanismos de privacidade da chamada.

O ip-*Keel*® Acesso é uma resposta ao sistema *Media Gateway* de *Acesso* da arquitectura PES do TISPAN. Este sistema possui duas vertentes consoante a sinalização SIP ou MEGACO/H.248. Este cenário pretende demonstrar as potencialidades do A-VGF da arquitectura PES do TISPAN com acessos PRI (*trunks* E1/T1/J1 da TP®-260) e analógicos (interface com 30AB). Após o registo do POTS procedeu-se à realização de testes de uma chamada do POTS para o PSTN com o terminal PSTN ocupado e de uma chamada simples do terminal fixo PSTN "234377900" (IT) para o POTS do A-VGF.

Para o sistema baseado em MEGACO/H.248 apenas foi implementado o processo de registo do lado SIP para o AGCF. O IMS *Agent* do AGCF foi testado para o registo de um utilizador com SIP URI: *sip:andresilva@ptinovacao.pt* no ambiente IMS/TISPAN do

*SHipNET*®. Este processo foi implementado e o resultado obtido seguiu as normalizações ETSI TS 183 043 [120] e ETSI ES 283 003 [82].

# Capítulo 7: Conclusões

O trabalho desenvolvido nesta Dissertação envolve uma arquitectura de convergência entre as redes fixas baseadas em *Time Division Multiplexing* (TDM), como por exemplo o *Public Switched Telephone Network/Integrated Services Digital Network* (PSTN/ISDN) e as de acesso *Digital Subscriber Line* (DSL), com as unidades de controlo e transporte das Redes de Próxima Geração (RPGs). Estas redes são de momento o grande desafio dos operadores de telecomunicações no fornecimento de serviços independentemente da tecnologia de acesso do cliente e das organizações de normalização na especificação de uma arquitectura global para estas redes. A *release* 5 do 3rd *Generation Partnership Project* (3GPP) introduziu o IP *Multimedia Subsystem* (IMS) como uma arquitectura normalizada para as redes "*all*-IP", destacando a convergência de serviços das redes móveis 2G, 2.5G e 3G, e fixas PSTN/ISDN com as redes IP. Posteriormente esta arquitectura foi utilizada pelo grupo de trabalho *Telecommuncations and Internet converged Services and Protocols for Advanced Networking* (TISPAN) [20] do *European Telecommunications Standard Institute* (ETSI) [12] como a base para evolução de uma arquitectura de convergência para os operadores de Telecomunicações. As *releases* 1 e 2 do TISPAN especificam uma arquitectura de convergência das redes fixas PSTN/ISDN e xDSL com o domínio IP baseada nos elementos do IMS, designada por PSTN/ISDN *Emulation Subsystem* (PES). É esta arquitectura do TISPAN a referência de todo o desenvolvimento endossado nesta Dissertação: construir um protótipo como resposta à convergência das redes PSTN/ISDN (ip-*Keel*® *Trunking*) e de xDSL (ip-*Keel*® Acesso) com o demonstrador IMS/TISPAN *Service Handling on ip NETworks* (*SHipNET*®) [84].

O sistema ip-*Keel*® *Trunking* foi implementado com a Mediant™ 2000 da AudioCodes® com função de *Trunking-Media Gateway Function* (T-MGF) e *Signalling Gateway Function* (SGF) da arquitectura PES e pela aplicação *openCallAgent*® instalada numa *workstation* da SUN com função de *Media Gateway Control Function* (MGCF). Com fim de aferir do comportamento e configuração do sistema na presença de uma ou várias chamadas em simultâneo e de todos os passos da sinalização para o estabelecimento e

terminação da chamada, foram realizados vários testes. De uma forma perceptível para o utilizador, todo o processo de estabelecimento, sinal de chamada no originário, sinal de alerta *ringing* no destinatário, fase de conversação e processo de terminação correu como esperado e de acordo com o convencional. Ao nível de sinalização apesar de ser utilizado o *Media Gateway Control Protocol* (MGCP) para o controlo do T-MGF em vez do protocolo *MEdia GAteway COntrol* (MEGACO)/H.248 especificado na normalização 3GPP/TISPAN, todos os passos e mapeamento de sinalização estão de uma forma geral de acordo com a normalização 3GPP TS 23.228 [28] para entrada e saída de chamadas de um terminal IP. Após estes testes foi configurado sistema ip-*Keel*® *Trunking* tendo em conta os critérios/requisitos impostos pelo demonstrador *SHipNET*®. Neste cenário para além dos testes realizados de situações reais, como por exemplo chamada bem sucedida de *Session Initiation Protocol* (SIP) para PSTN e vice-versa com terminação na origem e no destino, destacam-se dois testes, um de cancelamento da chamada pelo originário antes ser atendida e o outro sobre mecanismos de privacidade do utilizador originário, que tiveram comportamentos de acordo com o RFC 3325 [116] e RFC 3325 [116], respectivamente. Foram também realizados alguns testes de uma forma perceptível aos *codecs* G.711 $\mu$-*law*, G.711 *A-law*, G.723, G.726, G.729 e *Global System for Mobile communications* (GSM) para uma chamada no cenário *standalone* constituído pela Mediant™ 2000 e a plataforma *Mombasa*. Apesar de algumas condicionantes/falhas já mencionadas do *SHipNET*® e pelos próprios elementos do sistema, o ip-*Keel*® mostrou-se um sistema robusto e estável em muitas situações reais que podem ocorrer vulgarmente numa chamada.

O sistema ip-*Keel*® Acesso foi desenvolvido para dar resposta às duas vertentes de sinalização da arquitectura PES para o sistema *Media Gateway* de Acesso. Para o sistema baseado em SIP foram realizados testes de casos reais que podem ocorrer durante uma chamada de voz. As situações testadas foram as mesmas que para o ip-*Keel*® *Trunking* no cenário *SHipNET*®. Dos testes realizados destacaram-se nesta Dissertação o teste de chamada de um *Plain Old Telephone Service* (POTS), ligado à carta 30AB e registado no domínio *SHipNET*®, para um terminal da rede PSTN através do sistema ip-*Keel*® *Trunking*, em que este se encontrava no estado ocupado. Apesar de alguns problemas encontrados e ultrapassados com a carta 30AB na comunicação E1 *Channel Associated Signaling* (CAS) com a TP®-260, este sistema baseado em SIP mostrou-se um sistema robusto e estável em muitas situações reais que podem ocorrer vulgarmente numa chamada.

Em fase de implementação está o elemento de controlo AGCF para o ip-*Keel*® baseado em MEGACO/H.248. No âmbito desta Dissertação, e como sendo um trabalho de médio prazo, foi desenvolvido o módulo IMS *Agent* para o processo de registo.

Como trabalho futuro no âmbito desta Dissertação será feito um esforço no acompanhamento das normalizações das organizações envolventes e na evolução do demonstrador *SHipNET*® para a actualização dos sistemas ip-*Keel*® de acordo com as funcionalidades indicadas nas últimas *releases* do 3GPP/TISPAN. Para o protótipo AGCF continuarão a ser desenvolvidos os vários módulos internos de acordo com a norma ETSI TS 182 012 [3] e a sua interligação, primeiro com o S-CSCF para o processamento da chamada do lado SIP, depois com o A/R-MGF. Serão implementadas posteriormente as ligações com os elementos externos *Application Server Function* (ASF), *Network Attachment Subsystem* (NASS) e *Resource and Admission Control Subsystem* (RACS) com todas as funcionalidades e *stacks* envolventes, depois de validados os primeiros testes reais com terminais dos A/R-MGFs.

# Anexo I

Configuração da ligação série do *kit Mombasa* de acordo com o documento [99]:

*From the Windows environment, open up an existing Hyper-terminal session or go to (Start | Programs | Accessories | Communications | Hyper-terminal) to create a new session.*
*Make sure that the Serial port is set to COM 1.*
*Bits per Second = 115200.*
*Data bits = 8.*
*Parity = None.*
*Stop Bits = 1.*
*Flow Control = None.*
*File | Save As... (Save the session as "Mombasa.ht" ).*
*Exit Hyper-Terminal.*
*Open the "Mombasa" hyper-terminal session by double-clicking on the "Mombasa.ht" file in the Hyper-Terminal folder.*

Ficheiro de configuração "*gateway.conf*" do *kit Mombasa* para os testes *standalone*:

```
[GATEWAY_CFG]
ctrl_IP_addr = 192.168.9.237
ctrl_UDP_port = 1111

csmv6s_to_use = 0
csmv12s_to_use = 0
miros_to_use = 0
chagalls_to_use = 1

[MGC_CFG]
IP = 192.168.0.2
UDPport = 1111

[CSM6_CFG]
is_channel_reset_at_hangup = 0

#  operation_mode    channel_default_type channel_management_scheme
#  --------------    --------------------  ------------------------
#  0 = VoIPoPCI      1 = Data              0 = Static channels  & CCT disabled
#  1 = VoIPoETH      2 = VoIP              1 = Static channels  & device CCT enabled
#  2 = VoAAL1oATM 7 = FoIP                 2 = Dynamic channels & CCT disabled
#  3 = VoAAL2oATM 8 = AAL2                 3 = Dynamic channels & device CCT enabled
#  4 = VoAAL2oETH 32 = CCS                 4 = Dynamic channels & host CCT enabled
```

```
#   5 = VoAAL2oPCI  64 = AAL1
#   6 = VoIPoAAL5oATM
#   7 = CDMAoAAL5
#   8 = VoIPoPOS
#   9 = VoVCIDoETH

[CSM12_CFG]
max_channels = 12
channel_default_type = 2
channel_management_scheme = 3
is_channel_reset_at_hangup = 0
is_nextport_msg_enabled = 0
is_data_pci_bus_master_enabled = 0
is_cmddat_pci_bus_master_enabled = 0
is_g711_low_delay_enabled = 0

[MIRO_CFG]
max_channels = 128
operation_mode = 1
channel_default_type = 2
channel_management_scheme = 4
is_data_pci_bus_master_enabled = 0
is_channel_reset_at_hangup = 0
is_data_vlan_enabled = 0

[CHAGALL_CFG]
max_channels = 128
operation_mode = 1
channel_default_type = 2
channel_management_scheme = 4
is_data_pci_bus_master_enabled = 0
is_channel_reset_at_hangup = 0
is_data_vlan_enabled = 0

[CSM6_0]
data_IP_addr = 192.168.6.3
tdm = 0

[CSM6_1]
data_IP_addr = 192.168.6.4
tdm = 0

[CSM6_2]
data_IP_addr = 192.168.6.5
tdm = 0

[CSM6_3]
data_IP_addr = 192.168.6.6
tdm = 0
```

*[CSM12_0]*
*data_IP_addr = 192.168.6.7*
*tdm = 0*

*[CSM12_1]*
*data_IP_addr = 192.168.6.8*
*tdm = 0*

*[MIRO_0]*
*data_IP_addr = 192.168.0.3*
*mac_addr = 00:11:22:33:44:55*
*host_mac_addr = 00:11:22:33:44:55*
*is_eth_download_by_broadcast = 0*

*latency_level = 0x0000*

*vlan_user_priority = 0*
*vlan_vid = 0*

*atm_vpi_start_value = 0*
*atm_vpi_nb = 8*
*atm_vci_start_value = 32*
*atm_vci_nb = 128*

*aal2_cps_operation_mode = 1*
*aal2_max_num_vcc = 128*
*aal2_max_num_cid = 8*
*aal2_first_cid_num = 8*
*aal2_timer_cu = 0*

*aal5_rfc_encaps = 0x00f8*
*aal5_packet_detection_options = 0x0000*

*pos_ppp_encapsulation = 0*
*pos_mpls_encapsulation = 0*
*pos_mpls_header = 0x00000000*

*tdm = 0*

*[MIRO_1]*
*data_IP_addr = 192.168.0.4*
*mac_addr = 00:11:22:33:44:56*
*host_mac_addr = 00:11:22:33:44:55*
*is_eth_download_by_broadcast = 0*

*latency_level = 0x0000*

*vlan_user_priority = 0*
*vlan_vid = 0*

*atm_vpi_start_value = 0*
*atm_vpi_nb = 8*
*atm_vci_start_value = 32*
*atm_vci_nb = 128*

*aal2_cps_operation_mode = 1*
*aal2_max_num_vcc = 128*
*aal2_max_num_cid = 8*
*aal2_first_cid_num = 8*
*aal2_timer_cu = 0*

*aal5_rfc_encaps = 0x00f8*
*aal5_packet_detection_options = 0x0000*

*pos_ppp_encapsulation = 0*
*pos_mpls_encapsulation = 0*
*pos_mpls_header = 0x00000000*

*tdm = 0*

*[CHAGALL_0]*
***data_IP_addr = 192.168.9.237***
*mac_addr = AA:BB:CC:00:00:08*
*host_mac_addr = 00:11:22:33:44:55*
*is_eth_download_by_broadcast = 0*

*latency_level = 0x0000*

*vlan_user_priority = 0*
*vlan_vid = 0*

*tdm = 0*
*#device tdm used is 1 for phase 1 and 3 for phase2*
*device_tdm = 1*

*[CHAGALL_1]*
*data_IP_addr = 192.168.0.6*
*mac_addr = 00:11:22:33:44:58*
*host_mac_addr = 00:11:22:33:44:55*
*is_eth_download_by_broadcast = 0*

*latency_level = 0x0000*

*vlan_user_priority = 0*
*vlan_vid = 0*

*tdm = 0*

*#device tdm used is 1 for phase 1 and 3 for phase2*
*device_tdm = 1*

```
[CSM12_HW_CFG]
clock_multiplier = 14
sdram_timing1 = 0

[MIRO_HW_CFG]
clock_multiplier = 20
sdram_timing1 = 0

# -------------  ---------  ---------  --------------  -----------------------------------
# tdm_clock     line_mode  line_code  framing_format  pstn_signalling
# -------------  ---------  ---------  --------------  -----------------------------------
# 0 = 1.544 MHz  0 = T1     0 = B8Z7      0 = FT        0 = CAS - ABCD (not implemented yet)
# 1 = 2.048 MHz  1 = E1     1 = B7ZS      1 = FS        1 = CCS - ISDN/PRI Lucent 5ESS
# 2 = 4.096 MHz             2 = HDB3      2 = SLC       2 = CCS - ISDN/PRI National ISDN1
# 3 = 8.192 MHz             3 = AMI       3 = ESF       3 = CCS - ISDN/PRI Nortel DMS 100
#                           4 = UMC       4 = FAS       4 = CCS - ISDN/PRI Euro ISDN
#                                         5 = FAS/CAS   5 = CCS - ISDN/PRI French VN4
#
# 3          0       0       3          1   (usual T1 settings with M60)
# 3          1       2       4          4   (usual E1 settings with M60)
# 3          1       2       0          5   (usual E1 settings with France Telecom)

[BT8370_CFG]
mainboard_id = 8
is_network_side = 0
is_hdlc_enabled = 1
tx_pulse_template = 0

tdm_clock = 0
line_mode = 0
line_code = 3
framing_format = 3
pstn_signalling = 1
```

Ficheiro de configuração "*sipbx_linux.conf*" do *kit Mombasa* para os testes *standalone*:

```
#comment
#comment

$ATOMIC$
localport=15060;
#global_contact=<sip:default@192.168.14.242:15060>;
networktype=IN;
addr_type=IP4;
SIPversion=0;
media=audio;
media_protocol=RTP/AVP;
start_time=0;
```

*stop_time=0;*
*media_attrib_name=rtpmap;*
*media_attrib_payload_1=0;*
*media_attrib_value_1=pcmu/8000;*
*media_attrib_payload_2=18;*
*media_attrib_value_2=g729/8000;*
*max_sip_sessions=50;*
*max_pots_port=2;*
*max_pots_card=1;*
*max_phone_no_length=4;*
*max_sip_entries=32;*
*max_conf_entries=5;*
*sip_starting_num=9;*
*conf_starting_num=8;*
*eth_port=eth1;*
*target_name=miro;*
*supvsr_ready_reqd=no;*
*supervisor_ch_num=65535;*
*channel_count=512;*
*min_severity_level=1;*
*max_log_size=100000;*
*eth1_mac_address=00:11:22:33:44:55;*
*#localip=192.168.9.236;*
*#eth0_mac_address=00:AA:BB:CC:DD:EE;*
*#gateway_mac_address=00:07:EB:BE:3E:1B;*
*#msp_ip=192.168.9.236;*
*#gateway_ip_address=192.168.9.2;*
*dump_path = ./fsm.dump;*
*log_path = /var/log/pbx.log;*
*fsm_dump_num = 5555;*

*#CALL PARAMETERS FOR MSP*
*frame_length = 20;*
*#For Voice Activity Detection possible values 0,1,2 or 3,Caution:Donot use 2 for G729*
*vad_enable = 1;*
*#Echo Canceler tail value possbile values 0,5 or 15*
*ec_tail = 15;*
*#Initial jitter buffer parameter for RPPH*

*rpph_lpw_initial = 0;*
*rpph_lpw_min = 20;*
*rpph_lpw_max = 200;*
*enable_thc=no;*
*#comment*

***$POTS_TABLE$***
***0\0\1\2334\5;***
***1\1\1\2335\4;***

***$SIP_TABLE$***

***5001\|9335\|<sip:4444@192.168.9.50>;***

*5002\|9336\|<sip:2334@192.168.9.238:15060>;*

*5003\|9337\|<sip:2335@192.168.9.238:15060>;*

*5004\|9338\|<sip:95793365@192.168.9.238:15060>;*

*5005\|9339\|<sip:95793364@192.168.9.238:15060>;*

*5006\|9340\|<sip:95793091@192.168.9.238:15060>;*

*$CONFERENCE_TABLE$*

***500\|8334\|5\|10;***

*501\|8335\|5\|10;*

*502\|8336\|5\|10;*

*503\|8337\|5\|10;*

*504\|8338\|5\|10;*

# Anexo II

```
;**************
;** Ini File **
;**************

;Board: Mediant 2000
;Serial Number: 589483
;Slot Number: 1
;Software Version: 4.60A.016.003
;Board IP Address: 10.1.10.10
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 0.0.0.0
;Ram size: 128M   Flash size: 8M
;Num DSPs: 24  Num DSP channels: 144
;Profile: NONE
;Key features:;Max SW Ver: 5.0;Board Type: Mediant 2000;SS7 Links: MTP2=8 MTP3=8 M2UA=8 M3UA=8 ;Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol ;Channel Type: RTP PCI DspCh=240;DSP Voice features: EC128mSec IpmDetector RTCP-XR ;Control Protocols: MGCP MEGACO H323 SIP ;IP Media: VXML ExtVoicePrompt=10 ;E1Trunks=8;T1Trunks=8;Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ;PSTN Protocols: ISDN IUA=8 CAS V5.2;Default features:;Coders: G711 G726;
;------------------------------

[SYSTEM Params]

DNSPriServerIP = 10.2.1.2
DisableRS232 = 1

[BSP Params]

[ATM Params]

[Analog Params]

CallProgressTonesFilename = 'call_progress_portugal.dat'

[ControlProtocols Params]

[MGCP Params]


[MEGACO Params]
```

*[PSTN Params]*

*TDMBusPSTNAutoClockEnable = 1*
***ProtocolType_0 = 13***
*ProtocolType_1 = 10*
*ProtocolType_2 = 10*
*ProtocolType_3 = 10*
*DisableTrunkAfterReset = 0*
*ClockMaster_0 = 1*
*ClockMaster_1 = 0*
*ClockMaster_2 = 0*
*ClockMaster_3 = 0*
*TerminationSide_0 = 1*
*TerminationSide_1 = 0*
*TerminationSide_2 = 0*
*TerminationSide_3 = 0*
***LineCode_0 = 1***
*LineCode_1 = 0*
*LineCode_2 = 0*
*LineCode_3 = 0*
*CASTablesNum = 1*
*CASFileName_0 = 'LoopStartTable_FXS.dat'*
*CASFileName_1 = ''*
*CASFileName_2 = ''*
*CASFileName_3 = ''*
*CASFileName_4 = ''*
*CASFileName_5 = ''*
*CASFileName_6 = ''*
*CASFileName_7 = ''*

*[SS7 Params]*

*[Voice Engine Params]*

*IdlePCMPattern = 255*
*VoiceVolume = 1*
*FaxRelayRedundancyDepth = 2*
*FaxRelayEnhancedRedundancyDepth = 2*
*RFC2833PayloadType = 101*

*[WEB Params]*

*LogoWidth = '339'*

*[SIP Params]*

*TIMEFORREORDERTONE = 5*
*REGISTRATIONTIME = 3600*
*ENABLEHOLD = 1*

*ENABLEFORWARD = 1*
*ENABLEEARLYMEDIA = 1*
*CNONCE = '0a123bcf'*
*PASSWORD = '787899'*
*ISFAXUSED = 1*
*ENABLETRANSFER = 1*
***CODERNAME = g711Ulaw64k,20***
***CODERNAME = g7231,30***
***CODERNAME_1 = g711Ulaw64k,20***
*PREFIX = 4444,10.1.10.11,*,1*
*PSTNPREFIX = 9,1,*,10.1.10.11,1*
*TRUNKGROUPSETTINGS = 1,1*
*TXDTMFOPTION = 4*

*[SCTP Params]*

*[VXML Params]*

*[IPsec Params]*

*[Audio Staging Params]*

*[PSTN-SDH Params]*

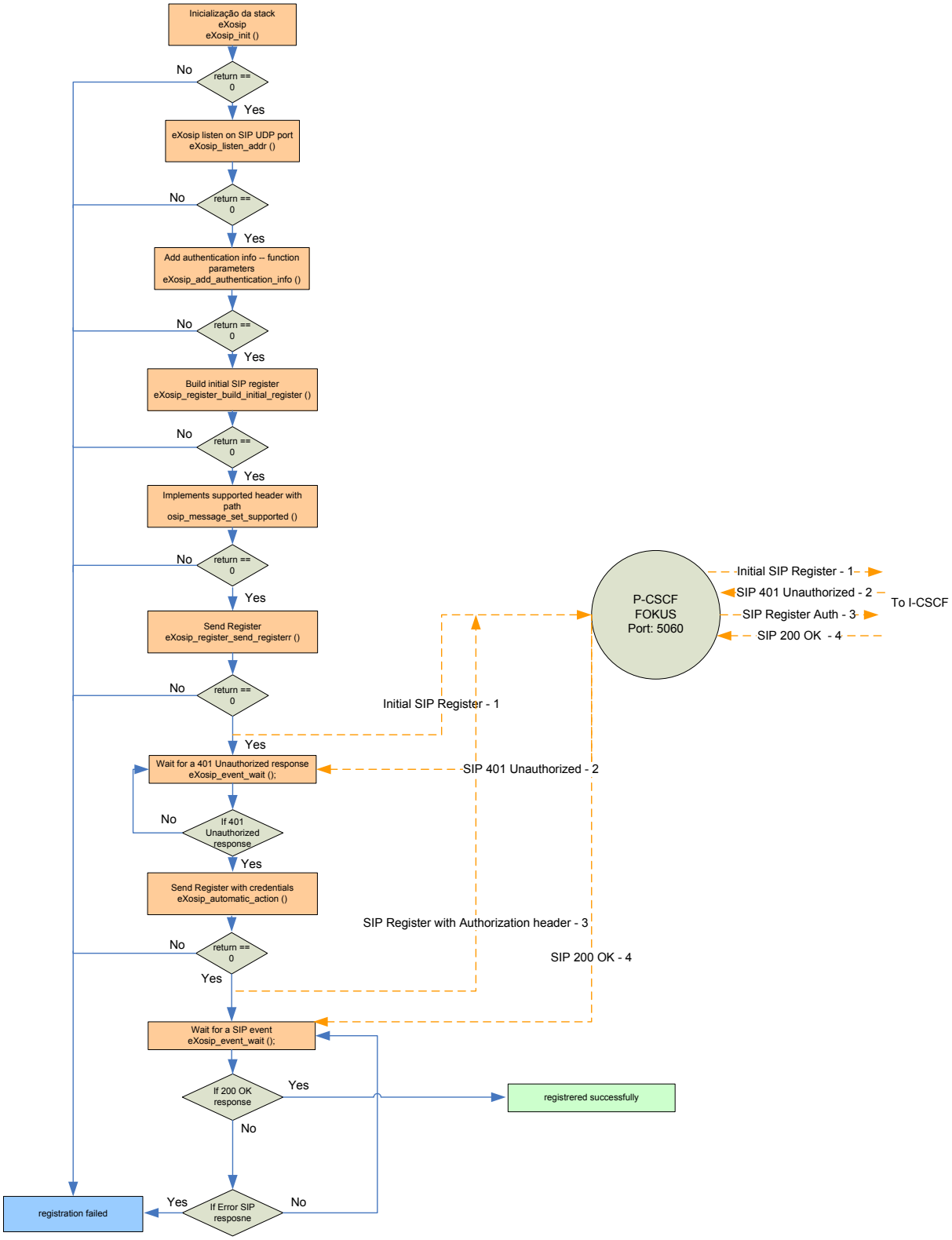
# Anexo III

Requisitos do Sistema de Sinalização #7 (SS7) da rede *Public Switched Telephone Network* (PSTN).

*Destination Point Code (DPC) = 3.4.10* (sistema *Trunking*)
*Originator Point Code (OPC) = 3.4.0* (SN da rede PSTN)
*Network Indicator (NI) = National*
*ISUP Variant = ETSI V2*
*Nature Of Address (NOA) = National*
*Numbering Plan Indicator (NPI) =ISDN*
*Calling Party's Category (CPC) = Ordinary*
*MTP Protocol Variant = ITU-T*

# Anexo IV

Diagrama funcional para o registo IP *Multimedia Subsystem* (IMS) *Agent*.



# Referências


[1] António Gamelas, "TISPAN – Visão Global", PT Inovação.

[2] Nuno Novo, "Arquitectura IMS IP Multimedia Subsystem", IT.

[3] ETSI, "IMS-based PSTN/ISDN Emulation Subsystem; Functional architecture", ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), draft ETSI TS 182 012 V2.0.1, 2007-09.

[4] *International Telecommunication Union* (ITU). [Online]
URL: http://www.itu.int

[5] *International Telecommunication Union – Telecommunications* (ITU-T). [Online]
URL: http://www.itu.int/ITU-T/

[6] *Internet Engineering Task Force* (IETF). [Online]
URL: http://www.ietf.org/

[7] H. Alvestrand, "A Mission Statement for the IETF", RFC 3935, Internet Engineering Task Force (IETF), October 2004.

[8] S. Bradner, "The Internet Standards Process - Revision 3", RFC 2026, Internet Engineering Task Force (IETF), October 1996.

[9] 3rd *Generation Partnership Project* (3GPP). [Online]
URL:http://www.3gpp.org/

[10] *Association of Radio Industries and Businesses* (ARIB). [Online]
URL: http://www.arib.or.jp/english/index.html

[11] *China Communications Standards Association* (CCSA). [Online]
URL: http://www.ccsa.org.cn/english/

[12] *European Telecommunications Standards Institute* (ETSI). [Online]
URL: http://www.etsi.org

[13] *Alliance for Telecommunications Industry Solutions* (ATIS). [Online]
URL: http://www.atis.org/

[14] *Telecommunications* Technology *Association* (TTA). [Online]

URL: http://www.tta.or.kr/English/new/main/index.htm

[15] *Telecommunication Technology Committee* (TTC). [Online]
URL: http://www.ttc.or.jp/e/index.html

[16] *Structure of* 3GPP. [Online]
URL: http://www.3gpp.org/tb/home.htm

[17] ETSI, "Overview of 3GPP Release 5", ETSI Mobile Competence Centre, 9 September 2003.

[18] ETSI, "Overview of 3GPP Release 6", Version TSG #33, ETSI Mobile Competence Centre, 2006.

[19] 3rd *Generation Partnership Project* 2 (3GPP2). [Online]
URL:http://www.3gpp2.org/

[20] *Telecoms & Internet converged Services & Protocols for Advanced Networks* (TISPAN). [Online]
URL: http://www.etsi.org/tispan/

[21] TISPAN *Structure*. [Online]
URL: http://www.etsi.org/tispan/#Structure

[22] K. Rosenbrock, R. Sanmugam, S. Bradner, J. Klensin, "3GPP-IETF Standardization Collaboration", RFC 3113, Internet Engineering Task Force (IETF), June 2001.

[23] S. Bradner, P. Calhoun, H. Cuschieri, S. Dennett, G. Flynn, "3GPP2-IETF Standardization Collaboration", RFC 3131, Internet Engineering Task Force (IETF), June 2001.

[24] 3GPP, "Service requirements for the Internet Protocol (IP) multimedia core network subsystem (Release 7)", Technical Specification Group Services and System Aspects, Stage 1, 3rd Generation Partnership Project (3GPP), TS 22.228 V7.6.0, 2007-09.

[25] Gonzalo Camarillo, Miguel A. García-Martín, "The 3G IP Multimedia Subsystem (IMS) Merging the Internet and the Cellular Worlds", Wiley, January 2005.

[26] 3GPP, "Network architecture (Release 7)", Technical Specification Group Services and System Aspects, 3rd Generation Partnership Project (3GPP), TS 23.002 V7.1.0, 2006-03.

[27] P. Calhoun, G. Zorn, J. Arkko, "Diameter Base Protocol", RFC 3588, Internet Engineering Task Force (IETF), September 2003.

[28] 3GPP, "IP Multimedia Subsystem (IMS)", Technical Specification Group Services and System Aspects, Stage 2, 3rd Generation Partnership Project (3GPP), TS 23.228 V7.6.0, 2006-12.

[29] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, Internet Engineering Task Force (IETF), November 2002.

[30] 3GPP, "3G security", Access security for IP-based services (Release 7), Technical Specification Group Services and System Aspects, 3rd Generation Partnership Project (3GPP), TS 33.203 V7.5.0, 2007-03.

[31] 3GPP, "Policy and charging control architecture (Release 7)", Technical Specification Group Services and System Aspects, 3rd Generation Partnership Project (3GPP), TS 23.203 V7.2.0, 2007-03.

[32] Rosenberg, J., et al., "SIP: Session Initiation Protocol", RFC 3261, Internet Engineering Task Force (IETF), June 2002.

[33] ITU-T, "Signalling System No. 7 – ISDN User Part functional description", ITU-T Recommendation Q.761, 09/97.

[34] ITU-T, "Bearer independent call control protocol", ITU-T Recommendation Q.1901, 06/2000.

[35] ITU-T, "Introduction to CCITT Signalling System No. 7", ITU-T Recommendation Q.700, 03/93.

[36] *Signaling Transport* (SIGTRAN). [Online]
URL: http://www.ietf.org/html.charters/sigtran-charter.html

[37] R. Stewart, K. Morneault, H. Schwarzbauer, I. Rytina, "Stream Control Transmission Protocol", RFC 2960, Internet Engineering Task Force (IETF), October 2000.

[38] G. Sidebottom, K. Morneault, J. Pastor-Balbas, "Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA)", RFC 3332, Engineering Task Force (IETF), September 2002.

[39] ITU-T, "Gateway control protocol: Version 2", ITU-T Recommendation H.248.1 v2, 03/2004.

[40] ITU-T, "Functional Description of the Message Transfer Part (MTP) of Signalling System No. 7", ITU-T Recommendation Q.701, 03/93.

[41] H. Schulzrinne, S. Casner, R. Frederick, "RTP: A Transport Protocol for Real-Time Applications", RFC 3550, Internet Engineering Task Force (IETF), July 2003.

[42] H. Schulzrinne, S. Petrack, "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals", RFC 2833, Internet Engineering Task Force (IETF), May 2000.

[43] Jun-Won Lee, "IP Multimedia Subsystem (IMS) and Its Applications", KNOM Conference, 26 April 2007.

[44] 3GPP, "Open Service Architecture (OSA) Application Programming Interface (API) - Part 1 (Release 1999)", Technical Specification Group Core Network, 3rd Generation Partnership Project (3GPP), TS 29.198 V3.4.0, 2001-06.

[45] 3GPP, "CAMEL Application Part (CAP) specification for IP Multimedia Subsystems (IMS) (Release 7)", Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 4, Technical Specification Group Core Network, 3rd Generation Partnership Project (3GPP), TS 29.278 V7.0.0, 2005-12.

[46] 3GPP, "Mobile Application Part (MAP) specification; (Release 7)", Technical Specification Group Core Network and Terminals, 3rd Generation Partnership Project (3GPP), TS 29.002 V7.8.0, 2007-06.

[47] Gaurav Paliwal, "Convergence: The Next Big Step", Thesis, Rochester Institute of Technology, 2006.

[48] Vassilios Koukoulidis, Mehul Shah, "The IP Multimedia Domain in Wireless Networks: Concepts, Architecture, Protocols and Applications", IEEE 6º International Symposium on Multimedia Software Engineering, 2004.

[49] ITU-T, "Packet-based multimedia communications systems", ITU-T Recommendation H.323, 06/2006.

[50] F. Cuervo, C. Huitema, B. Rosen, "Megaco Protocol Version 1.0", RFC 3015, Internet Engineering Task Force (IETF), November 2000.

[51] Sauli Santeri Österman, "Combining Circuit and Packet Based Services in Converging Networks", Master thesis, Helsinki University, 13 March 2006.

[52] Jonas Pettersson, "Converged Services in the Next-Generation Network", Master of Science Thesis, Royal Institute of Technology, Stockholm, Sweden, June 2006.

[53] ITU-T, "List of ITU-T Recommendation E.164 Assigned Country Codes", ITU-T Recommendation E.164, 02/2005.

[54] M. Handley, "SDP: Session Description Protocol", RFC 2327, Internet Engineering Task Force (IETF), April 1998.

[55] J. Rosenberg, H. Schulzrinne, "An Offer/Answer Model with the Session Description Protocol (SDP)", RFC 3264, Engineering Task Force (IETF), June 2002.

[56] *Megaco*/H.248: *Media Gateway Control Protocol Overview* (RFC 3525). [Online] URL: http://www.javvin.com/protocolMegaco.html

[57] "05.01 – Media Gateway Control; Redes de Serviços e Comunicações Multimédia", RSCM/ISEL-DEETC-SRC/2004.

[58] C. Rigney, A. Rubens, W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, Engineering Task Force (IETF), June 2000.

[59] ITU-T, "Pulse code modulation (PCM) of voice frequencies", ITU-T Recommendation G.711, 1993.

[60] 3GPP, "AMR speech codec", Transcoding functions (Release 4), Mandatory Speech Codec speech processing functions, Technical Specification Group Services and System Aspects, 3rd Generation Partnership Project (3GPP), TS 26.090 V4.0.0, 2001-03.

[61] 3GPP, "Adaptive Multi-Rate - Wideband (AMR-WB) speech codec", Transcoding functions (Release 7), Speech codec speech processing functions, Technical Specification Group Services and System Aspects, 3rd Generation Partnership Project (3GPP), TS 26.190 V7.0.0, 2007-06.

[62] ITU-T, "40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)", ITU-T Recommendation G.726 (1990) – Corrigendum 1, 05/2005.

[63] ITU-T, "Transmission planning for voiceband services over hybrid Internet/PSTN connections", ITU-T Recommendation G.177, 09/99.

[64] ITU-T, "Dual Rate Speech Coder For Multimedia Communications Transmitting at 5.3 and 6.3 kbit/s", ITU-T Recommendation G.723.1, 03/96.

[65] ITU-T, "G.729: Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)", ITU-T Recommendation G.729, 03/96.

[66] ITU-T, "Video Codec for Audiovisual Services at p x 64 kbits", ITU-T Recommendation H.261, 03/93.

[67] ITU-T, “Video coding for low bit rate communication”, ITU-T Recommendation H.263, 01/2005.

[68] ITU-T, "General principles and general reference model for next generation networks", ITU-T Recommendation Y.2011, 10/2004.

[69] ETSI, “NGN Functional Architecture Release 1”, ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), ETSI ES 282 001 V1.1.1, 2005-08.

[70] ETSI, “Network Attachment Sub-System (NASS)”, ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), ETSI ES 282 004 V1.1.1, 2006-06.

[71] ETSI, “NGN Release 1: Functional Architecture; Resource and Admission Control Sub-system (RACS)”, ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), ETSI ES 282 003 V1.1.1, 2006-06.

[72] ETSI, “IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228 version 7.9.0 Release 7)”, ETSI Standard, Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS), ETSI TS 123 228 V7.9.0, 2007-10.

[73] ETSI, “NGN Release 2 H.248 Profile Version 2 for controlling Access and Residential Gateways”, ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), ETSI ES 283 002 V2.1.0, 2007-11.

[74] ETSI, “H.248 Profile for controlling Trunking Media Gateways [3GPP TS 29.332 V7.7.0 modified]”, ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), Draft ETSI ES 283 049 V2.0.2, 2007-09.

[75] ETSI, “Network architecture (3GPP TS 23.002 version 7.1.0 Release 7)”, ETSI Standard, Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS), ETSI TS 123 002 V7.1.0, 2006-03.

[76] ETSI, “IP Multimedia Subsystem (IMS); Functional architecture”, ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), ETSI ES 282 007 V1.1.1, 2006-06.

[77] ITU-T, "Guidelines for using transaction capabilities", ITU-T Recommendation Q.775, 06/97.

[78] ETSI, "PSTN/ISDN Emulation Sub-system (PES); Functional architecture", ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), ETSI ES 282 002 V1.1.1, 2006-03.

[79] ITU-T, "Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part", ITU-T Recommendation Q.1912.5, 03/2004.

[80] ETSI, "Resource and Admission Control: DIAMETER protocol for domains interconnection information exchange between SPDFs", ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), ETSI TS 183 062 V2.2.0, 2008-03.

[81] ETSI, "Network Attachment Subsystem; e2 interface based on the DIAMETER protocol", ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), ETSI ES 283 035 V1.2.1, 2007-06.

[82] ETSI, "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 (Release 7), modified]", ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), ETSI ES 283 003 V1.8.0, 2007-09.

[83] ETSI, "IPTV Architecture", Dedicated subsystem for IPTV functions, ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), ETSI TS 182 028 V2.0.0, 2008-01.

[84] *Service Handling on* IP *NETworks* (SHipNET). [Online]
URL: http://www.ptinovacao.pt/produtos/P&S_PTIN.html

[85] VoIP (*Voice Over* IP) *Solutions – AudioCodes*. [Online]
URL: http://www.audiocodes.com/

[86] Mindspeed. [Online]
URL: http://www.mindspeed.com/web/home.html

[87] AudioCodes, "Audio Codes Voice over Packet Processors", LTRT-00273 08/05 V.3, 2005.

[88] H. Schulzrinne, S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control", RFC 3551, Engineering Task Force (IETF), July 2003.

[89] C. Perkins, V. Hardman, M. Handley, S. Fosse-Parisis, "RTP Payload for Redundant Audio Data", RFC 2198, Engineering Task Force (IETF), September 2003.

[90] AudioCodes, "Fast Track Installation Guide MGCP, MEGACO, H.323 & SIP", Mediant 2000, Version 4.6, LTRT-70105, 13 July 2005.

[91] F. Andreasen, B. Foster, "Media Gateway Control Protocol (MGCP) Version 1.0", RFC 3435, Engineering Task Force (IETF), January 2003.

[92] ITU-T, "Procedures for real-time Group 3 facsimile communication over IP networks", ITU-T Recommendation T.38, 04/2007.

[93] ITU-T, "5-, 4-, 3- and 2-bit/sample embedded Adaptive Differential Pulse Code Modulation (ADPCM)", ITU-T Recommendation G.727 (1990) – Corrigendum 1, 05/2005.

[94] ITU-T, "CODING OF SPEECH AT 16 kbit/s USING LOW-DELAY CODE EXCITED LINEAR PREDICTION", ITU-T Recommendation G.728, 09/92.

[95] *Enhanced Variable Rate* CODEC (EVRC CODEC), *Wikipedia, the free encyclopedia.* [Online]
URL: http://en.wikipedia.org/wiki/Enhanced_Variable_Rate_Codec

[96] S. Andersen, A. Duric, R. Hagen, J. Linden, "Internet Low Bit Rate Codec (iLBC)", RFC 3951, Engineering Task Force (IETF), December 2004.

[97] K. Morneault, S. Rengasami, G. Sidebottom, "ISDN Q.921-User Adaptation Layer", RFC 3057, Engineering Task Force (IETF), February 2001.

[98] K. Morneault, R. Dantu, G. Sidebottom, J. Heitz, "Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Adaptation Layer", RFC 3331, Engineering Task Force (IETF), September 2002.

[99] Mindspeed, "Mombasa Evaluation Kit Setup Instructions", 825XX-APP-001-Mombasa Setup Instructions, 3 September 2003.

[100] André M. Silva, Tiago M. M. P. Campos, "Projecto Media Gateway - Relatório", IT, PT Inovação, November 2005.

[101] *5ESS switch, Wikipedia, the free encyclopedia*. [Online]
URL: http://en.wikipedia.org/wiki/5ESS_switch

[102] CounterPath *Corporation | Home*. [Online]

URL: http://www.counterpath.com/

[103] AMI (*Alternate Mark Inversion*). [Online]
URL: http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/ami.html

[104] *Extended Super Frame* (ESF), *Wikipedia, the free encyclopedia*. [Online]
URL: http://en.wikipedia.org/wiki/Extended_Super_Frame

[105] AudioCodes, "Mediant 2000, Mediant 1000, TP-1610 and TP-260 SIP User's Manual Manual Version 4.6", LTRT-68803, 13 July 2005.

[106] *OpenTelecommunications* (OT). [Online]
URL: http://www.opentelecommunications.com

[107] OpenTelecommunications, "openCallAgent 3.1 User Guide", October 2005.

[108] J. Rosenberg, H. Schulzrinne, "Reliability of Provisional Responses in the Session Initiation Protocol (SIP)", RFC 3262, Internet Engineering Task Force (IETF), June 2002.

[109] A. B. Roach, "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, Internet Engineering Task Force (IETF), June 2002.

[110] R. Sparks, "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, Internet Engineering Task Force (IETF), April 2003.

[111] S. Donovan, "The SIP INFO Method", RFC 2976, Internet Engineering Task Force (IETF), October 2000.

[112] A. Niemi, Ed., "Session Initiation Protocol (SIP) Extension for Event State Publication", RFC 3903, Internet Engineering Task Force (IETF), October 2004.

[113] J. Rosenberg, "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, Internet Engineering Task Force (IETF), September 2002.

[114] B. Campbell, Ed., H. Schulzrinne, C. Huitema, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, Internet Engineering Task Force (IETF), September 2002.

[115] J. Peterson, "A Privacy Mechanism for the Session Initiation Protocol (SIP), RFC 3323, Internet Engineering Task Force (IETF), November 2002.

[116] C. Jennings, J. Peterson, M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, Internet Engineering Task Force (IETF), November 2002.

[117] ETSI, "Integrated Services Digital Network (ISDN); Signalling System No.7; ISDN User Part (ISUP) Version 2 for the International Interface; Part 1: Basic Services", ETSI Standard, ETSI ETS 300 356- 1, 1995-01.

[118] Performance Technologies, "Tutorial on Signaling System 7 (SS7)".

[119] G. Camarillo, "The Early Session Disposition Type for the Session Initiation Protocol (SIP)", RFC 3959, Internet Engineering Task Force (IETF), December 2004.

[120] ETSI, "IMS-based PSTN/ISDN Emulation Stage 3 specification", Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), ETSI TS 183 043 V1.1.1, 2006-05.

[121] *The* GNU oSIP *library* – GNU *Project* – *Free Software Foundation* (FSF). [Online]
URL: http://www.gnu.org/software/osip/

[122] OpenIMSCore.org | *The Open IMS Core Project*. [Online]
URL: http://www.openimscore.org/

[123] *About* SIP *Express Router* | iptel.org. [Online]
URL: http://www.iptel.org/ser

[124] libeXosip2: *Module Index*. [Online]
URL: http://www.antisip.com/doc/exosip2/index.html

[125] 3GPP, "IP Multimedia Subsystem (IMS) charging", Charging management, Telecommunication management, Technical Specification Group Service and System Aspects, 3rd Generation Partnership Project (3GPP), TS 32.260 V7.4.0, 2007-09.

[126] 3GPP, "Open Service Access (OSA) (Release 7)", Technical Specification Group Core Network and Terminals, Stage 2, 3rd Generation Partnership Project (3GPP), TS 23.198 V7.2.0, 2007-03.

[127] António Gamelas, "Media Gateway SHipNET – Reunião de Control", PT Inovação, 4 de Maio de 2005.