Universidade de Aveiro
2009
Departamento de Electrónica, Telecomunicações e Informática

Nuno Martins de Sousa Gil

Integração de uma Access Gateway Control Function num cenário TISPAN


Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática
2009

Nuno Martins de Sousa Gil

Integração de uma Access Gateway Control Function num cenário TISPAN

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 do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro e co-orientação do Doutor Victor Marques.

o júri

presidente

Prof. Doutor Rui Valadas
professor associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

arguente

Doutor Paulo Mendes
Lider do Grupo de *Internet Architectures and Networking* (IAN) do Instituto de Engenharia de Sistemas e Computadores (INESC) do Porto

orientadora

Prof. Doutora Susana Sargento
professora auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

co-orientador

Doutor Victor Marques
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

Á professora Susana Sargento e Doutor Victor Marques pela oportunidade que me deram e pela disponibilidade e ideias durante a dissertação.

Ao Doutor Victor Marques da PT Inovação S.A. pela sua disponibilidade e ajuda ao longo do trabalho realizado no âmbito desta dissertação.

A toda a comunidade da PT Inovação S.A. pelo ambiente de integração, ajuda e apoio.

Á equipa envolvida neste projecto nomeadamente Eng. António Gamelas, Eng. Tiago Campos e em especial ao Eng. André Silva, pela sua disponibilidade e troca de conhecimentos ao longo da realização deste trabalho.

Aos meus pais, Marta e amigos por todo o seu apoio.

palavras-chave

NGN, IMS, TISPAN, SIP, MEGACO/H.248, POTS, *Acess Gateway Control Function*, *Access Media Gateway*.

resumo

Longe vão os tempos em que as comunicações se encontravam quase exclusivamente limitadas a soluções disponibilizadas pela rede telefónica tradicional (também designada de PSTN – *Public Switched Telephone Network*).
A enorme popularização da Internet levou ao aparecimento de um novo conceito denominado de "tudo-sobre-ip" permitindo na mesma plataforma transportar voz, dados e vídeo. Surgem então as NGN (*Next Generation Networks*), que apresentam uma arquitectura baseada em IP e estruturada de uma forma revolucionária isto é, em camadas horizontais. Um dos serviços que mais interesse tem despertado é o Voice over IP (VoIP). No entanto, tendo em conta o enorme número de utilizadores da rede telefónica tradicional e todas as infra-estruturas dos operadores que sustentam esta rede de comutação de circuitos não é de todo recomendável que a migração para as NGN seja realizada de modo repentino. Esta deve ser efectuada de uma forma faseada, sendo necessário dar continuidade ao serviço PSTN e a outras redes de acesso, criando-se uma rede comum e aberta, visando a convergência fixo-móvel.

Uma das soluções propostas para a arquitectura deste tipo de rede proveio do TISPAN. Esta, por sua vez, baseia-se na solução IMS do 3GPP, mas diferencia-se especialmente através do seu subsistema PES que permite a emulação da rede telefónica PSTN/ISDN de forma transparente.
Para que seja possível a interligação dos elementos POTS, que utilizam protocolos específicos como o SS7, ao core NGN, é necessária a existência de um elemento intermédio – *Access Media Gateway (A-MGW)* – e outro que efectue o seu controlo. No caso do subsistema PES, esta entidade designa-se de *Access Gateway Control Function* (AGCF).

O presente trabalho propõe-se divulgar as características da arquitectura NGN apresentada pelo TISPAN, dando especial ênfase ao subsistema PES e à AGCF que foi desenvolvida no âmbito desta dissertação.
A pretensão de introduzir este elemento num demonstrador de arquitectura NGN específico, designado de *Service Handling on ip NETworks* (SHipNET®) levou a que fossem efectuados diversos testes com o intuito de averiguar o bom funcionamento da solução implementada referente às seguintes capacidades: configuração inicial, registo/desregisto, chamada.

keywords

NGN, IMS, TISPAN, SIP, MEGACO/H.248, POTS, ***Acess Gateway Control Function*****,** ***Access Media Gateway*****.**

Abstract

The traditional standard of telephone network (known as PSTN) is nowadays no longer exclusive for communication.
The enormous spread of the Internet led to a new concept known as "all over IP", allowing voice, data and video to be transmitted on the same level of platform. The NGN come from this purpose and present an architecture based on IP and is structured from an advanced way: horizontal levels. One of the services that has most success is the Voice over IP (VOIP).
However, as the number of the traditional telephone network customers is still significant, it is obviously quite impossible a sudden transition to the new model. Instead, it should be done step by step and not negleting the PSTN service and the other types of access. This way, a common network will be implemented with the purpose of creating a convergence in both of them, which means, fixed-mobile.

One of the proposed answers viewing the implementation of this type of net, came from the TISPAN, which is based on the IMS solution from the 3GPP. Nevertheless, it differs from it on its PES subsystem, which allows the emulation of the telephone network PSTN/ISDN in a simple way.
In order to make it possible the access of the POTS (using protocol demands, such as SS7) to the core NGN, it is necessary an intermediate element - Access Media Gateway (A-MGW) - and another one to do its control. In relation to the PES subsystem, this element is called Access Gateway Control Function (AGCF).

This research aims to make it possible the knowledge of the NGN architecture proposed by TISPAN, placing special emphasis on the PES subsystem and also on the AGCF, being developed in this dissertation.
The purpose of including this element in a demonstration of NGN architecture, known as Service Handling on ip Networks (SHipNET®), was to examine - through several tests, such as initial configuration, registry/desregistry, call - how the solution runned.

Índice

Índice de Figuras

Lista de Tabelas

Acrónimos

3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AC	Authentication Center
ANACOM	Autoridade Nacional de Telecomunicações
ARF	Access Relay Function
AS	Application Servers
ASF	Application Server Function
AVP	Attribute-Value-Pairs
A-MGW	Access Media Gateway
A-MGF	Access Media Gateway Function
BGCF	Breakout Gateway Control Functions
BGF	Breakout Gateway Functions
BICC	Bearer Independent Call Control
CAGR	Compounded Average Growth Rate
CAMEL	Customized Applications for Mobile network Enhanced Logic
CAP	CAMEL Application Part
CEPT	European Conference of Postal and Telecommunications Administrations
CSCF	Call Session Control Function
DTMF	Dual-Tone Multi-Frequency
DVB	Digital Vídeo Broadcasting
ETSI	European Telecommunications Standards Institute
EU	User Equipment
FM	Feature Manager
GSM	Global System for Mobile communications
gsmSCF	GSM Service Control
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating-CSCF
IETF	Internet Engineering Task Force
IMS	IP Multimédia Subsystem
IP	Internet Protocol
IPTV	Internet Protocol Television
ISUP	ISDN User Part
ITU	International Telecommunications Union
IWF	Interworking Function
LBCD	Line based Configuration Data

LDAP	Lightweight Directory Access Protocol
MAP	Mobile Application Part
MDCP	Media Protocol Device Control
MEGACO	Media Gateway Control
MGW	Media Gateway
MGIF	Mobile Games Interoperability Forum
MGC	Media Gateway Controller
MGCF	Media Gateway Controller Function
MGCP	Media Gateway Control Protocol
MMUSIC	Multiparty Multimedia Session Control
MRF	Media Resource Functions
MRFC	MRF Controllers
MRFP	MRF Processor
MTP	Message Transfer Part
NASS	Network Attachment Subsystem
NGN	Next Generation Network
NAPT	Network Address Port Translation
NAPT-PT	NAPT Protocol Translator
OSA-SCS	Open Service Access Service Capability Server
P-CSCF	Proxy-CSCF
PCM	Pulse Code Modulation
PDF	Policy Decision Function
PES	PSTN/ISDN Emulation subsystem
PSTN	Public Switched Telephone Network
POTS	Plain Old telephone service
PSS	IMS-based PSTN Simulation Subsystem
PTT	Push To Talk
QoS	Quality of Service
RACS	Resource and Admission Control Subsystem
RADIUS	Remote authentication Dial-In User Service
RCEF	Resource Control Enforcement Function
RFC	Request for Comments
ROI	Retorno sobre os Investimentos
RTCP	Real Time Control Protocol
RTP	Real-time Transport Protocol
R-MGW	Residential Media Gateway
R-MGF	Residential Media Gateway Function
S-CSCF	Serving-CSCF
SAP	Announcement Protocol
SBLP	Service-Based Local Policy
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol

SGF	Signalling Gatyeway Function
SGW	Signaling Gateway
SIP	Session Initiation Protocol
SLF	Subscriber Location Funcion
SMTP	Simple Mail Transfer Protocol
SPAN	Services and Protocols for Advanced Networks
SPDF	Service Policy Decision Function
SS7	Signalling System #7
STD	Serviço de Transmissão de Dados
STF	Serviço Telefónico Fixo
STM	Serviço Telefónico Móvel
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
THIPON	Telecommunications and Internet Protocol Harmonization Over Networks
TISPAN	Telecoms & Internet coverged Services & Protocols for Advanced Network
TLS	Transport Layer Security
TR	Technical Reports
TS	Technical Specifications
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UPSF	User Profile Server Function
VGW	Voice Gateway
XML	Extensible Markup Language
XPCAP	Configuration Access Protocol
WCDMA	Wideband Code Division Multiple Access

Capítulo 1

Introdução

Desde sempre que a humanidade necessita de comunicar. Nos dias que correm, em que a facilidade de aceder, absorver e partilhar informação é encarada como um dado adquirido, a comunicação existe no centro da vida quotidiana e ninguém prescinde disso, e é mesmo difícil imaginar um Mundo onde tal não aconteça. Mas nem sempre foi assim, longa foi a evolução que nos trouxe até aos dias de hoje.

As primeiras formas de comunicação presencial do Homem consistiam em sons e gestos, e terão sido com estes que surgiram também os primeiros actos de telecomunicação (comunicação à distância - *tele*, prefixo grego que significa distante). Com a acústica vocal, a mensagem era transmitida através de sons, como o grito, e com as mãos e os braços transmitiam-se mensagens gestuais. Tendo o Homem aprendido a utilizar o fumo e o fogo para transmitir as suas mensagens nos casos em que as distancias eram um pouco maiores.

Com o desenvolvimento da linguagem e da escrita, tornou-se possível comunicar cada vez a maiores distâncias e surge o sistema de correio, vindo mais tarde a invenção da imprensa a reforçar o poder da comunicação.

O grande passo no sentido da rapidez e fiabilidade da telecomunicação em rede foi dado com a descoberta da energia eléctrica e das suas utilizações. Surgem os primeiros Telégrafos Eléctricos, em 1833 com Carl Gauss (1777-1855) e em 1837 com Samuel Morse (1791 – 1872), o qual criou igualmente o Código Morse. O Telégrafo de Morse começou a ser comercializado nos Estados Unidos da América tendo-se dado então inicio às comunicações entre diversos estados e cidades deste país – através de cabos terrestres – e, posteriormente, foi possível a comunicação entre diferentes Continentes por meio de cabos submarinos. Contudo, aquele que constitui possivelmente o maior acontecimento na história das telecomunicações deu-se no ano de 1876 [1] com a invenção do telefone, atribuída a Alexander Graham Bell (1847-1922), que veio possibilitar finalmente a transmissão de som.

Actualmente, de uma maneira geral, aspectos como o bem-estar, lazer e entretenimento são algo cada vez mais valorizados pelas pessoas. No entanto, para que o homem possa desfrutar desses momentos necessita de tempo, pelo que, cada vez mais, têm vindo a ser procuradas soluções e serviços a elas associados, que sejam acima de tudo fiáveis, rápidos e de fácil aprendizagem, de modo a que de forma simples as pessoas realizem as suas tarefas, acedam a informação e a partilhem.

Hoje em dia, muitos negócios são feitos entre empresas de diferentes continentes, e não seria possível que eles se desenvolvessem sem um meio de comunicação com as características acima referidas.

Uma crescente massificação e aumento de rapidez dos transportes permite que as pessoas se desloquem com facilidade para vários pontos do mundo, levando a que elas nunca abdiquem de estarem contactáveis, receberem e partilharem informação, isto é estarem como usualmente se diz "ligadas ao Mundo".

A necessidade de comunicar tem vindo a crescer de uma forma bastante acentuada mas durante anos as empresas de telecomunicações limitaram-se a oferecer apenas o telefone e o fax, suportados pela rede telefónica tradicional (também designada de PSTN) e por uma rede comutada de pacotes, no caso de transporte de dados. O alto custo das tarifas telefónicas e o número limitado de serviços obrigou muitos utilizadores a procurarem formas alternativas de comunicação visando um ambiente aberto que forneça a redução dos custos dos equipamentos/serviços e acesso a um maior número de soluções.

A popularização da Internet na década de 90 acelerou a corrida a novas tecnologias, as quais vieram impulsionar o processo de convergência de serviços ao encontro do protocolo IP. Criou-se desta forma um novo conceito denominado de "tudo sobre IP": voz sobre IP, vídeo sobre IP e dados sobre IP. Surge assim aquilo a que passou a designar-se conceito de Redes de Nova Geração (*Next Generation Network* – NGN) onde se observa uma concentração de voz, dados e vídeo na mesma infra-estrutura (rede).

O VoIP, um dos serviços que mais interesse tem despertado é já muito comum no transporte de chamadas que têm como origem e destino a rede PSTN (por exemplo em ligações internacionais), sendo totalmente desconhecido por parte dos utilizadores que a chamada é encaminhada, em grande parte, através de uma infra-estrutura IP.

Associado ao conceito de NGN existe uma arquitectura de rede que vem pôr fim a um sistema de camadas verticais onde usualmente, a cada serviço corresponde uma plataforma independente, criando-se por vezes uma enorme sobreposição de redes. O novo conceito horizontal, onde independentemente do tipo de tecnologia de acesso a informação é transportada sobre IP, apresenta-se como a solução para muitos dos problemas que os operadores enfrentam, nomeadamente o alto custo associado a diferentes plataformas e uma forte dependência das aplicações disponibilizadas por parte dos fabricantes de equipamentos.

Surge também a necessidade da existência de normas bem definidas relativamente a este tipo de rede existindo diversas organizações a trabalhar em conjunto, cada uma com uma função específica, para que este conceito seja viável e exista o menor número de incompatibilidades possíveis.

Inicialmente é através do 3GPP, na *release* 5 do *IP Multimédia Susbsystem* (IMS), que é apresentada uma solução com elementos de um *core* bem definido onde o principal objectivo era possibilitar que os utilizadores da rede móvel tivessem acesso a serviços usualmente característicos da Internet tentando assim oferecer-lhes uma experiência mais rica.

Por outro lado, é fácil de compreender que esta migração para as NGNs não deve ser efectuada abruptamente, mas sim de forma faseada devido a diversos factores como por exemplo o preço dos terminais IP, que não são apelativos para um cliente convencional, e ao elevado custo

da substituição imediata de todo o sistema actualmente implementado por parte de muitos operadores.

Assim, é necessário dar continuidade à funcionalidade da rede tradicional e seria de esperar que esta interagisse com o *core* das NGNs não de uma forma simulada, tal como o sistema de *Trunking* apresentado pelo IMS possibilita, mas permitir que utilizadores de terminais convencionais (POTS) se pudessem registar e tirar partido da rede como se de um cliente com um terminal IP/IMS se tratasse. Este pressuposto visa a criação não de um sistema isolado mas sim de um sistema aberto a qualquer tipo de redes de acesso incluindo a rede tradicional, segundo um conceito de convergência fixo-móvel.

Surge então, apresentada pelo TISPAN, uma arquitectura baseada em vários subsistemas sendo que um deles, o que atraiu mais atenções, designado de PES (PSTN/ISDN *Emulation Subsystem*) possibilita que as redes tradicionais acedam ao *core* de determinada NGN de forma transparente. Para possibilitar o interfuncionamento de POTS das redes de acesso baseadas em comutação de circuitos onde são utilizados protocolos exclusivos, com a rede de comutação de pacotes também ela com os seus protocolos específicos, é necessário recorrer a um elemento intermédio designado de *Access Media Gateway*. Este não é mais do que uma entidade passiva (*slave*) à qual um número variável de POTS são ligados, encontrando-se a ser controlados por outra entidade (master) à qual usualmente se chama de elemento de controlo da *Media Gateway*. Para o caso específico do subsistema PES IMS *based* da arquitectura apresentada pelo TISPAN este controlo é efectuado por um elemento designado de *Access Gateway Control Function* (AGCF).

1.1 Objectivos

Um dos objectivos desta dissertação é dar a conhecer a arquitectura proposta pelo TISPAN para as redes NGN efectuando uma descrição detalhada de todos os seus elementos constituintes e suas potencialidades. De entre estes, no decorrer deste trabalho, a atenção será centrada na AGCF e em todos os seus módulos internos e funcionalidades a serem desempenhadas por este elemento.

No âmbito da parte prática o objectivo é o de implementar algumas das funcionalidades da AGCF bem como que seja inserida num demonstrador de testes de uma NGN com o intuito de verificar e provar o bom funcionamento da mesma.

1.2 Estrutura

Esta dissertação encontra-se estruturada da seguinte forma:

- Capítulo 2: A arquitectura de referência do TISPAN para as NGNs é o objecto de estudo deste capítulo. Aspectos como os diferentes subsistemas e novos elementos introduzidos em comparação com o core IMS serão abordados. No entanto, é dado especial ênfase ao subsistema PES IMS *based* uma vez que é este que possibilita a emulação PSTN/ISDN.

- Capítulo 3: Inicialmente é efectuado um estudo detalhado das funcionalidades da AGCF e dos módulos da sua arquitectura interna. De seguida são enumerados os requisitos que devem ser verificados aquando da implementação deste módulo de acordo com todas as normas a serem respeitadas e as especificações do *core* de testes onde será inserida.

- Capítulo 4: Este capítulo é referente a toda a parte de implementação e testes efectuados no âmbito desta dissertação. Inicialmente é descrito o cenário prático utilizado e de seguida são apresentadas as soluções adoptadas bem como todos os resultados obtidos referentes a: configuração inicial, registo e chamada.

- Capítulo 5: Conclusões gerais sobre todo o trabalho realizado e uma perspectiva sobre a sua continuidade.

1.3 Notação e Terminologia

Este trabalho teve por base a Língua Portuguesa, mas no entanto o seu uso não pode ser generalizado a todo o documento uma vez que determinados termos técnicos não são passíveis de ser traduzidos para Português ou por vezes não existe consenso para o fazer. Desta forma, alguns termos e acrónimos aparecem em Inglês sendo o mais comum em toda a literatura.

A notação utilizada ao longo desta dissertação segue a seguinte convenção:

- texto a negrito: serve para realçar uma palavra ou expressão
- texto em itálico: utilizado para expressões ou palavras em língua estrangeira
- texto numerado: aquando a indicação de uma referência bibliográfica
- letras maiúsculas: utilizadas para referenciar acrónimos

Capítulo 2

TISPAN

Inicialmente, a solução apresentada pelo 3GPP [2] para as NGNs focava-se sobre as redes móveis, estendeu-se depois às redes fixas PSTN (sistema de *trunking*) ficando desse modo por satisfazer a necessidade de interoperabilidade e convergência também com algumas redes fixas de acesso como por exemplo o XDSL . Surge, assim, uma nova abordagem de arquitectura para as NGNs proposta pelo TISPAN que é um grupo de trabalho do *European Telecommunications Standards Institute* (ETSI) [3].

O TISPAN apresenta-se como uma resposta à necessidade de tornar mais apelativos os serviços baseados em redes de dados, e possibilitar a convergência de um leque alargado de redes de acesso com especial destaque para as xDSL. A realização conjunta destes dois objectivos, permitirá, entre outras coisas, aumentar e melhorar o número de serviços disponibilizados pelo operador, tornando-os mais atractivos. Para que esta fusão seja possível de ser implementada numa plataforma comum, de forma eficiente e apelativa existe um conjunto de requisitos que têm de ser cumpridos, os quais são descritos no início deste Capítulo.

No que diz respeito aos protocolos utilizados na arquitectura proposta pelo TISPAN, estes serão apresentados separadamente, consoante o tipo de interligação para que são utilizados e a funcionalidade associada.

A primeira versão, a *Release* 1, foi concluída em Dezembro de 2005 e apresentava o primeiro conjunto de especificações para a arquitectura NGN do referido grupo de trabalho.

As principais características desta arquitectura envolvem duas camadas distintas, contendo um conjunto de subsistemas e duas novas entidades o NASS e o RACS. Uma vez que a gestão da qualidade de serviço é um aspecto que mereceu grande atenção na norma TISPAN, foram nesta implementados fortes mecanismos que respondessem a essa preocupação.

Baseado em elementos da arquitectura IMS do 3GPP, nomeadamente os de controlo, surge um subsistema denominado de IMS *core*. Para além deste, o TISPAN definiu outro, que se veio a revelar o grande trunfo desta arquitectura – PSTN/ISDN Emulation subsystem – o que veio permitir a emulação dos serviços telefónicos tradicionais em terminais analógicos, alargando a si a rede de determinado operador a este tipo de clientes. Actualmente, são já vários os elementos de *core* NGN que estão a ser desenvolvidos com base nesta Release.

É apresentada neste Capítulo, de forma detalhada, a arquitectura global proposta pelo TISPAN, começando por se fazer referencia à camada de transporte, nomeadamente aos dois subsistemas *Network Attachment Subsystem* (NASS) e *Resource and Admission Control* Subsystem (RACS) encarregados de controlar a gestão dos recursos para determinada sessão.

De seguida, apresenta-se a Camada de Serviço, onde os subsistemas IMS *core* e PSTN/ISDN *Emulation subsystem* serão objecto de um estudo detalhado.

Os terminais na rede IP são tidos como dispositivos inteligentes possuindo total controlo sobre o estado de cada chamada, ao contrário dos telefones tradicionais que apenas reagem a comandos de uma central controladora, reflectindo uma arquitectura *master-slave*.
Para que estes últimos possam ser ligados directamente ao *core* da NGN, é necessário que se encontrem ligados a *Media Gateways* especificas para o efeito denominadas de *Acceess* ou *Residential Media Gateways* (A/R-MGF) consoante a sua capacidade de suporte de POTS e localização. Ora, sendo estas encaradas como um elemento passivo (*slave*), que necessita de estar sobre a alçada de um elemento de controlo, levou a que tenha surgido o conceito de *Access Gateway Control Function* (AGCF) de bastante importância no âmbito desta tese.

Será efectuada uma descrição dos elementos que são comuns a todos os subsistemas definidos pelo TISPAN. Isto é, são entidades com as quais todos os subsistemas da camada de serviço interagem. Esta partilha, bem como a que pode ser verificada ao nível de determinadas aplicações para emulação e simulação PSTN/ISDN, permitem que as operadoras consigam baixar os custos associados aos serviços disponibilizados e ao número de elementos que necessitam de manutenção periódica.

O facto de a arquitectura se basear num pressuposto de duas camadas e vários subsistemas possibilita que sejam suportadas novas funcionalidades sem interferir com todo o sistema já implementado.

No final de 2006 foi dada como terminada a *Release 2*, designada de TISPAN NGN Rel-2, onde novas capacidades foram acrescentadas à arquitectura base apresentada na *Release* anterior, através da inserção de novos subsistemas. Um exemplo, é a pretensão de dotar a NGN com funções de suporte de serviços IPTV (IP *Television*) com ATIS IIF (*Automatic Terminal Information Service* – IPTV *Interoperability Forum*) e DVB (*Digital Vídeo Broadcasting*). Exemplos de outros subsistemas igualmente suportados são também apresentados neste Capítulo.

O objectivo é que o 3GPP e o TISPAN trabalhem em conjunto, com o intuito de criarem uma solução comum bem definida na normalização de uma arquitectura global para as NGNs. A colaboração entre estas duas organizações iniciou-se logo após o fim da TISPAN NGN Release 1, a qual foi sendo sujeita a alterações até Maio de 2007, ou seja dois meses depois de sair a *Release* 7 apresentada pelo 3GPP. Já a *Release* 2 do TISPAN encontra-se a ser alinhada com a *Release* 8 do 3GPP.

Actualmente, são já vários os elementos de core NGN que estão a ser desenvolvidos com base nesta *Release*, a qual tem vindo a ganhar grande credibilidade. Aliás, o próprio grupo TISPAN tenta passar a imagem de que a sua arquitectura é a mais eficiente e sólida, utilizando o slogan apelativo “NGN *means* TISPAN”.

Para o futuro já existem alguns temas a serem abordados pela *Release* 3 do TISPAN, onde por exemplo dar ao utilizador a possibilidade de controlar o *roaming* ou o acesso com elevada largura de banda (VDSL, Wi-Max, etc.).

2.1 Conceitos Gerais do TISPAN

A solução apresentada pelo TISPAN baseia-se nos conceitos gerais que caracterizam as NGN. Estas possuem características específicas que as tornam inovadoras relativamente às soluções convencionais. De seguida, são apresentados os principais factores que levaram ao aparecimento deste conceito e a forma como deve ser implementado no cenário actual, tendo em conta os operadores e os respectivos clientes.

2.1.1 A Filosofia TISPAN

Longe vão os tempos em que a rede telefónica tradicional era responsável pela quase totalidade dos lucros das operadoras e a grande maioria dos Portugueses não dispunha de formas alternativas a esse meio de comunicação. Contudo, nos últimos anos, o sector das telecomunicações tem sofrido grandes transformações, estando na sua origem o aparecimento da Internet e as redes móveis, às quais tem havido grande adesão, uma vez que apresentam serviços com características que respondem melhor às exigências, cada vez maiores, do cliente actual, que valoriza muito a fácil acessibilidade, inovação e custo. De facto, as operadoras têm vindo a assistir de ano para ano a uma crescente diminuição do número de chamadas e assinantes na rede PSTN. A figura 5 apresenta dados de um estudo divulgado pela Autoridade Nacional de Telecomunicações (ANACOM) em Junho de 2008 [4], no qual é possível verificar uma redução no volume de receitas obtidas com o Serviço Telefónico Fixo (STF), onde em apenas um ano, entre 2005 e 2006, os dados apresentados indicam um crescimento médio anual composto (*Compounded Average Growth Rate* – CAGR) de -4.6%, o que representa uma perda bastante significativa.

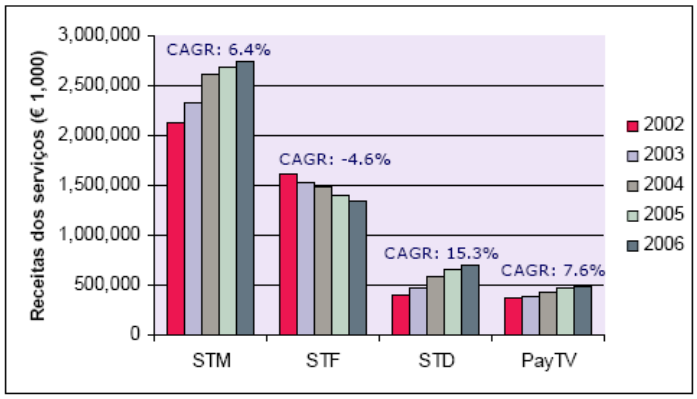


Figura 1 – Volume de receitas por serviço

A utilização cada vez maior do telefone móvel ou por cabo, em detrimento do fixo, deve-se a um maior custo de acesso deste último que chega a ser superior em cerca de 44.4%. Os operadores móveis, ao aperceberem-se desta discrepância, viram nela uma oportunidade de cativar novos clientes, oferecendo soluções vantajosas como o GSM fixo, onde o cliente pode

usufruir dos serviços móveis a preços bastante competitivos, estando este apenas limitado a determinada área residencial. Nos dados apresentados, é bem visível este aumento do número de clientes do serviço telefónico móvel (STM) e do serviço de transmissão de dados (STD), ao qual se pode dever em parte o decréscimo das receitas da rede fixa.

Assim, nem sempre é fácil às operadoras conseguirem o tão desejado retorno sobre os investimentos (ROI) e aumentarem os seus lucros [5]. É de salientar que a filosofia adoptada era a de que a cada novo serviço está associada uma nova plataforma independente, criando-se um panorama de redes sobrepostas. Por exemplo, a rede fixa encontrava-se separada da rede de dados, correspondendo cada uma a um sistema diferente, com meios distintos, quer ao nível de cablagem quer ao nível de equipamentos de rede. Por exemplo, a *British Telecommunications* PLC chegou a ter 17 redes paralelas, cada uma com necessidades exclusivas [6]. Ora a manutenção de diferentes plataformas torna-se bastante dispendiosa em diversos aspectos, como por exemplo a necessidade de profissionais com conhecimentos específicos. Outro factor a ter em conta é o de que se estava perante uma arquitectura monolítica onde os operadores se encontravam totalmente sujeitos aos fabricantes para efectuarem qualquer actualização de software/hardware ou para adquirirem novas aplicações. Tal dependência verifica-se porque os equipamentos utilizados na rede são desenvolvidos segundo um princípio onde as funções de controlo e de encaminhamento não são separáveis. Para os operadores esta grande sujeição aos fabricantes para obtenção de novas aplicações e o seu elevado custo não é de todo algo que lhes agrade. Assim, tornava-se apetecível um ambiente aberto onde cada operador fosse livre de escolher o seu equipamento e respectivo software, obtendo-se com isso a redução de custos dos equipamentos e dos serviços.

Muitas operadoras têm visto os seus lucros descerem, devido à estagnação do mercado de voz e à forte concorrência que se faz sentir, pelo que necessitam de oferecer novos e melhores serviços, com perspectivas de crescimento, com o intuito de se diferenciarem dos seus concorrentes, de forma a conservarem e até cativarem novos clientes. Era portanto bem vinda uma solução que pusesse fim a algumas lacunas existentes, de modo a que esses operadores passassem a ver aumentada a sua facturação, os seu lucros e o ROI.

Foi assim que na década de noventa, com a enorme popularização da Internet, surge como solução possível a ideia de adoptar uma estratégia de convergência de serviços sobre IP a qual vai permitir que na mesma infraestrutura de rede toda a informação seja transportada em pacotes digitais que utilizam o protocolo IP (*Internet Protocol*). Estes pacotes, utilizando o mesmo equipamento, transportariam voz, dados e vídeo. Surge, assim, o conceito de Redes de Nova Geração (*Next Generation Network*, NGN) e associado a este é apresentada pelo TISPAN uma solução bem definida para uma arquitectura deste tipo de rede.

2.1.2 Benefícios da arquitectura TISPAN

Um aspecto tido em conta foi a pretensão da separação do hardware do software pelos motivos descritos anteriormente. Na arquitectura TISPAN observa-se uma separação formal em

diferentes camadas e o uso de interfaces abertas para que se crie um ambiente multifornecedor para hardware e software. Este tipo de arquitectura é usualmente designado de horizontal, ao contrário do conceito vertical até então usado, permitindo criar uma abstracção entre camadas e tecnologias usadas. A horizontalidade encontra-se associada à possibilidade de funcionalidades comuns de diferentes serviços poderem ser partilhadas, como ilustra a Figura 2.

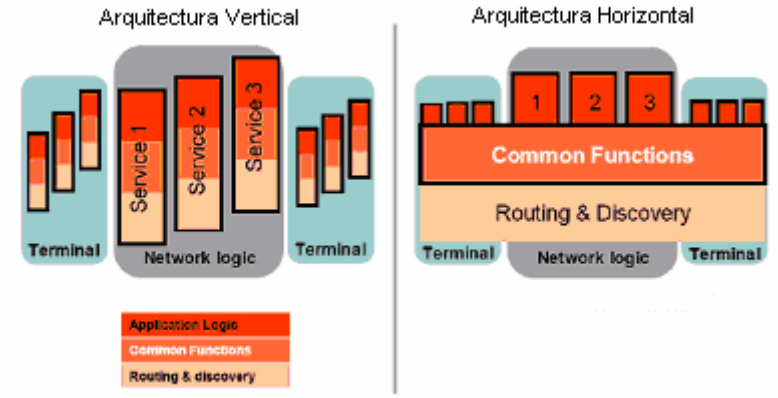


Figura 2 – Arquitectura vertical e a horizontal da NGN (adapatada de [71])

O desenvolvimento de novos serviços fica assim facilitado, bem como a integração de serviços de entidades exteriores à operadora, continuando esta, no entanto, com o controlo total da sua rede. Por ser uma arquitectura totalmente normalizada de forma transparente, é garantida interoperabilidade entre equipamentos da rede e entre operadoras diferentes, sendo portanto facilitado o processo de *roaming*. Uma descrição detalhada da arquitectura e respectivas camadas será efectuada nos capítulos seguintes.

Estamos perante uma agregação de infra-estruturas de rede, que antes eram separadas, o que possibilitam uma enorme redução (cerca de 80%) dos elementos de rede de comutação de circuitos. Assim, as operadoras conseguem reduzir bastante os custos de manutenção da rede que, até então, eram bastante elevados.

Outro factor benéfico para os operadores prende-se com a possibilidade de gerarem novas fontes de receita através da criação de novos serviços apelativos para os clientes, nomeadamente serviços multimédia, como por exemplo tele-trabalho, e-learning, ou web-conference.

Ao ser utilizado o protocolo SIP (*Session Initiation Protocol*), que será alvo de descrição detalhada adiante, é possível associar todos os dispositivos de um utilizador com apenas uma identidade pública, independente do acesso.

Assim, as NGN e consequentemente a proposta apresentada pelo TISPAN surge como a possibilidade de realizar um velho sonho por parte dos operadores, conseguindo pôr fim a algumas falhas na operacionalidade e rentabilidade das redes dos mesmos. Já para os utilizadores, é vista como impulsionadora de mais e melhores serviços, aos quais terão acesso de uma maneira fácil e possivelmente com custos acessíveis.

2.1.3 Transição

O modelo tradicional de redes de telecomunicações separadas encontra-se próximo do fim, devido ao aparecimento das NGNs que concentram tudo na mesma rede sob IP. No âmbito desta dissertação, interessa aprofundar mais especificamente como deverá ser dado o salto de transição para as NGN ao nível da rede PSTN tradicional. Tal explica-se, como referido no Capítulo 1, pelo facto de o módulo a ser desenvolvido (AGCF) efectuar o controlo da interligação dos terminais analógicos ao núcleo de determinada NGN.

No caso particular da rede PSTN, é sabido que a convergência é inevitável, uma vez que as receitas que os terminais analógicos oferecem às operadoras tem vindo a diminuir e os custos a aumentar. Tal é devido a diversos factores, alguns já referenciados anteriormente, como por exemplo, a diminuição crescente do número de clientes e das chamadas efectuadas pelos mesmos. Em muitos casos as cablagens e equipamentos da rede PSTN já se encontram bastante degradados e obsoletos, sendo os custos de manutenção de tal rede bastante elevados, tendo em conta as receitas que os mesmos proporcionam. A redução do custo das chamadas imposta pelas entidades reguladoras e pelo aparecimento de operadoras concorrentes também poderá ser apontado como um ponto forte na diminuição dos lucros obtidos com a rede PSTN tradicional. No entanto o aparecimento das NGN não pressupõe a eliminação súbita dos serviços das redes já implementados no mercado.

Alguns dos utilizadores da rede PSTN encontram-se apegados ao sistema actual telefónico e podem encarar esta mudança com alguma relutância. Alguns poderão não estar interessados em aderir a serviços avançados que estarão disponíveis ou não quererão abdicar das linhas analógicas de forma a assegurar uma continuidade do funcionamento do serviço telefónico aquando de falha de electricidade. Não se pode obrigar um utilizador de uma forma repentina a aceitar a instalação de adaptadores residenciais que se ligam aos telefones convencionais, ainda mais tendo em conta que os mesmos consomem energia. Outro entrave que pode ser colocado por parte dos utilizadores prende-se com o custo elevado dos terminais IP. Um terminal telefónico convencional possui um preço que usualmente varia entre os €5 e os €35 e possui o benefício económico, no caso de ser fixo, de não consumir energia. Por seu lado um terminal telefónico que possibilite uma ligação directa à NGN possui um preço que pode variar entre os €70 e os €300 e, salvo casos de equipamentos que vão aparecendo no mercado que se auto-alimentam através da porta *Ethernet* (PoE), necessitam de uma alimentação externa [7].

Assim, é necessário continuar a disponibilizar o funcionamento dos terminais da rede PSTN aquando do salto para as redes NGNs. A transição deverá então ser efectuada não abruptamente, mas de uma forma faseada. A solução que é mais plausível e que se encontra a ser colocada em prática por diferentes operadores, baseia-se num modelo onde a transição é feita de dentro para fora. Isto é, segundo este princípio as mudanças necessárias serão realizadas inicialmente no seio da rede e só numa fase avançada ao nível residencial.

Surge assim a necessidade de encontrar soluções que possibilitem uma correcta e transparente interligação dos terminais analógicos à NGN.

2.2 Requisitos do TISPAN

Tendo em conta as necessidades e pretensões dos operadores e a sua expectativa perante este novo conceito de negócio, é importante especificar os requisitos que a arquitectura NGN, mais especificamente uma baseada no conceito TISPAN, deve satisfazer. É inevitável referir que na sua maioria são requisitos comuns aos da arquitectura do IMS como seria de esperar uma vez que o conceito TISPAN surgiu e baseia-se na proposta apresentada pelo 3GPP. Estes são descritos, de seguida, de forma sucinta, sendo que muitos poderiam ser subdivididos em função do detalhe que se pretenda dar [8].

2.2.1 Sessões IP Multimédia

Facilmente se compreende que o serviço mais importante na rede de comutação de circuitos é a comunicação áudio, serviço esse que terá de continuar a existir com a mudança para as redes de comutação de pacotes. Como forma de aumentar o grau de satisfação do cliente, a arquitectura TISPAN deve possibilitar o estabelecimento de diferentes tipos de sessões multimédia, independentemente do terminal de acesso. Um dos pontos fortes que as tornam mais atractivas será, por exemplo, juntar vídeo durante uma simples sessão voz e permitir efectuar o *download* de conteúdos multimédia durante a chamada. Para que um cliente possa utilizar este tipo de sessões, bem como as suas funcionalidades, é necessário que se encontre com permissão para aceder a tal serviço no *core* do operador. Todas as inúmeras possibilidades de aplicações multimédia colocadas à disposição dos utilizadores devem ser disponibilizadas pelo IMS de forma transparente e sem incompatibilidades não descurando nunca aspectos como a privacidade e segurança comparativamente aos sistemas tradicionais.

2.2.2 Segurança

Em qualquer rede, um dos requisitos fulcrais prende-se com a sua segurança pelo que é indispensável que quer os operadores, quer os clientes sintam que a mesma é sólida e inviolável. O TISPAN não deve ser excepção pelo que as sessões multimédia estabelecidas nunca devem descurar aspectos como a autenticação, segurança e privacidade, tal como os sistemas tradicionais.

De forma a efectuar a autenticação e autorização dos clientes no *core* TISPAN, este dispõe de mecanismos próprios de comunicação entre o equipamento de utilizador (User Equipment – UE) e o *core* - que garantem que as mesmas são efectuadas de forma eficiente - bem como de mecanismos de segurança da própria rede de acesso. A integridade das mensagens trocadas entre a rede TISPAN e o UE é também garantida, além de serem oferecidos mecanismos opcionais de confidencialidade. A fasquia mínima de segurança que o TISPAN deve garantir tem como patamar de comparação a oferecida pela rede de comutação de circuitos e pelo GPRS (*General Packet Radio Service*).

No entanto, para os clientes, a Internet e aplicações associadas ao uso das suas tecnologias, ainda possuem alguma reputação de serem sistemas inseguros. Ainda assim é, provavelmente, mais fácil efectuar operações com intuito maldoso nas redes tradicionais do que na NGN tendo em conta a segurança que os protocolos escolhidos proporcionam. Estes serão abordados mais adiante.

2.2.3 Qualidade de Serviço (QoS)

Sendo a qualidade dos serviços oferecidos pelas operadoras um factor bastante valorizado pelos seus utilizadores, o TISPAN, pretende distinguir-se de outras soluções num dos seus pontos fortes que é a possibilidade de oferecer QoS.

Um dos grandes problemas que surgiram aquando do aparecimento dos primeiros serviços multimédia baseados em IP, nomeadamente os em tempo-real como o VoIP, prende-se com a falta de QoS. Para que esses serviços multimédia sejam oferecidos com qualidade suficiente, é necessário estabelecer mecanismos que controlem aspectos como a perda de pacotes na rede, atrasos que podem sofrer, e garantir uma largura de banda suficiente.

O TISPAN oferece mecanismos de negociação de QoS entre o UE e a rede do operador. Aquela é realizada antes do início da sessão e pode mesmo ocorrer durante a mesma. Com base nesta negociação são reservados recursos na rede de acesso que garantem as condições acordadas entre o UE e a rede. O nível de QoS disponibilizada para determinado cliente varia consoante diversos factores, podendo depender do serviço contratado, da largura de banda disponível, localização do utilizador na rede ou ainda de outro parâmetro de diferenciação que o operador queira implementar.

A arquitectura global TISPAN oferece desta forma ao operador total controlo sobre a QoS disponibilizada, permitindo assim que o mesmo possa diferenciar diferentes tipos de clientes.

2.2.4 Mecanismos de *charging*

As operadoras pretendem ter ao seu alcance mecanismos de taxação (*charging*) adequados a cada novo serviço disponibilizado, de forma a poderem implementar vários modelos de negócio e a utilização de mais do que um modelo em simultâneo, de acordo com o serviço subscrito pelo cliente. A operadora tem a possibilidade de efectuar o *charging offline* ou *online*, pelo que este pode ser posto em prática automaticamente, em tempo real sobre a sessão, ou requerer uma cobrança efectuada após a utilização do serviço. Ao implementar diferentes taxas, a operadora pode gerir de forma mais eficaz o seu modelo de negócio.

2.2.5 Roaming

Nos dias que correm é importante que um utilizador se possa movimentar em termos geográficos sem restrições continuando a usufruir sempre, de forma transparente, dos serviços na sua rede "mãe", como se nunca tivesse deixado de estar dentro da mesma. O conceito de *roaming*

começou a ter forte impacto com o aparecimento das redes móveis de segunda e terceira geração, e o TISPAN deve garantir que este conceito se mantém disponível na sua arquitectura.

Para que o cliente possa gozar da transparência atrás referida, torna-se necessário que os operadores de diferentes países e regiões estabeleçam entre si protocolos de parcerias, de forma a trocarem informação relativa aos clientes. Uma vez que esta funcionalidade se encontra sempre dependente de acordos celebrados entre diferentes operadoras, essa transparência acaba muitas vezes por não existir ou ser bastante reduzida. A proposta apresentada pelo TISPAN propõe um modelo de roaming onde a rede visitada se limita a oferecer o ponto de entrada, sendo a própria rede do utilizador a disponibilizar os serviços.

2.2.6 Rápida instalação e desenvolvimento de serviços

O TISPAN pretende alterar o modelo de desenvolvimento de serviços, uma vez que, normalmente, nas plataformas tradicionais de telecomunicações, estes não poderiam ser desenvolvidos livremente e não era assegurado que eles funcionassem quando o utilizador se deslocasse para outra zona geográfica.

O TISPAN, tal como o 3GPP, pôs de parte esse modelo adoptando um novo onde apenas as *capabilities* são normalizadas. Pretende-se, assim, abrir as portas a entidades independentes ao desenvolvimento de serviços, conseguindo-se desta forma que as operadores deixem de depender exclusivamente de determinados fornecedores, dando lugar a um mercado de aplicações em que teoricamente o preço de compra destas é mais baixo. É também acelerado o processo de desenvolvimento de novos serviços e facilitada a sua instalação, garantindo a sua operacionalidade na rede onde são criados, dispensando os longos testes que eram por vezes necessários para averiguar a sua operacionalidade.

2.2.7 Controlo dos Serviços disponibilizados

As operadoras de telecomunicações fazem questão de ter o máximo controlo sobre os serviços que disponibilizam aos seus clientes, o qual é ainda mais apertado quando o leque desses serviços é grande e muitos deles são desenvolvidos por entidades exteriores.

O TISPAN teve em conta esta pretensão básica dos operadores e, por isso, suporta políticas de controlo que podem ser divididas em duas categorias distintas: Políticas Gerais, aplicáveis a toda a rede, abrangendo todos os clientes. Por exemplo um operador que pretenda bloquear a utilização de determinadas aplicações por parte dos clientes que possam prejudicar o seu negócio;

Por outro lado, existem as Políticas Individuais, que se aplicam de forma independente a cada utilizador ou a um grupo específico de utilizadores. Nesta situação, pretende-se caso a caso - consoante o tipo de contrato estabelecido entre o cliente e o operador – restringir o acesso a determinadas aplicações que o utilizador não subscreveu. O utilizador até pode possuir equipamento que as suportem, só que o operador não permite que as utilize.

Relativamente ao roaming, existem dois tipos distintos de controlo: o da rede nativa e o da rede visitada. No segundo caso, é essa rede que fornece os serviços e controla o tráfego, o que

muitas vezes provoca alguns problemas no relacionamento entre os operadores, já que é exigido que ambos implementassem serviços semelhantes, de forma a evitar uma degradação dos serviços prestados. Assim, é pretendido pelo TISPAN que se adopte um sistema de controlo efectuado na rede nativa.

2.2.8 Interoperabilidade

Este requisito é bastante importante, uma vez que impõe que o TISPAN deve ser inter operável com redes de diferentes tipos. Esta interoperabilidade possui maior ênfase com a Internet, redes móveis (como o GSM), e as redes de comutação de circuitos (PSTN e ISDN). A implementação e adesão à arquitectura NGN será efectuada de uma forma faseada e os utilizadores TISPAN não devem ficar isolados das restantes redes. Não é de mais referir que o conceito associado à proposta apresentada pelo grupo TISPAN do ETSI é a convergência fixo-móvel e que o módulo dessa arquitectura a ser estudado e implementado (AGCF) possui precisamente a funcionalidade específica de efectuar o controlo de *Gateways*, possibilitando a interoperabilidade entre duas redes distintas.

2.3 Protocolos

Para que seja possível o estabelecimento de sessões numa arquitectura TISPAN, dois caminhos devem ser estabelecidos, destinando-se um deles à troca de mensagens de sinalização, responsáveis pelo controlo do outro, aquele onde vai fluir a informação propriamente dita. Esta sinalização e informação têm de ser enviadas respeitando protocolos específicos, muitos dos quais, provêm do IETF [9] e da interligação que possui com o 3GPP e o ETSI.

Estes protocolos possibilitam que a interligação do core NGN com o exterior e entre os vários elementos internos se processe de uma forma bem definida e explícita.

São cinco os principais protocolos usados no TISPAN, sendo bastante usual a sua separação em três níveis, consoante a função ou tipo de informação que é transportada. Tem-se, assim, Protocolos de sinalização, Protocolos de autenticação, autorização e accounting (*Authentication, Authorization and Accounting - AAA*) e Protocolos de media [10].

No caso de sinalização, os protocolos são responsáreis pelo estabelecimento e características do caminho multimédia entre os utilizadores, bem como pela negociação sobre quais os protocolos de media a serem usados. O protocolo SIP (Session Initiation Protocol), que tira partido do SDP (Session Description Protocol), assim como o protocolo MEGACO/H.248 (*Media Gateway Control*), fazem parte da família protocolar de sinalização.

Já o protocolo RTP (*Real-Time Transport Protocol*), utilizado em conjunto com o RTCP (*Real Time Control Protocol*), encontra-se no grupo de protocolos de media. São estes que decidem como a informação é codificada e enviada pelo caminho previamente estabelecido, permitindo que a troca de fluxos multimédia entre utilizadores seja efectuada de uma forma íntegra com QoS. Por fim, é ao Diameter [59] que cabe a responsabilidade de assegurar o tão importante AAA (Authentication, Authorization, Accounting) nas NGNs.

2.3.1 Session Initiation Protocol (SIP)

O protocolo SIP, tal como o nome indica, é utilizado para iniciar, modificar ou terminar sessões ou chamadas multimédia entre utilizadores. O seu propósito é tornar a sessão possível, não sendo a comunicação em si da sua responsabilidade, mas sim de outros como o protocolo RTP.

Foi em meados de 1995 que começou a ser desenvolvido pelo grupo de trabalho MMUSIC (*Multiparty Multimedia Session Control*) do IETF e em 2 de Fevereiro de 1999 foi proposto como standard, tendo sido publicado no RFC 2543 a 17 de Março. Este protocolo foi desenvolvido pelas mesmas pessoas que criaram o RTP e o RTCP, tendo a segunda versão, SIPv2 presente no RFC 3261 [11], aprovado em Junho de 2002 ano em que no mês de Novembro foi aceite como protocolo utilizado pelo 3GPP.

Cada vez mais fabricantes estão a adoptar este protocolo tornando-o uma aposta forte, tendo o IETF decidido criar o SIP *Working Group* para o seu desenvolvimento e que é

independente do grupo inicial MMUSIC. Uma das suas funcionalidades em voga, designada de "forking", possibilita que um utilizador se encontre registado em vários telefones simultaneamente, o que significa que ao receber uma chamada os vários telefones tocam, permitindo-lhe escolher qual deles atender. Deixa assim de ser necessário encaminhar as chamadas de uns telefones para ou outros, existindo deste modo uma maior mobilidade.

O SIP pode correr sobre *Transmission Control Protocol* (TCP) e *Stream Control Transmission Protocol* (SCTP), mas o mais utilizado é o User Datagram Protocol (UDP). Foi projectado para ser simples e extensível, pertencendo à família de protocolos Internet como o HTTP (*Hyper Text Transfer Protocol*) e SMTP (*Simple Mail Transfer Protocol*) seguindo um modelo cliente-servidor tal como ilustrado na figura 7.

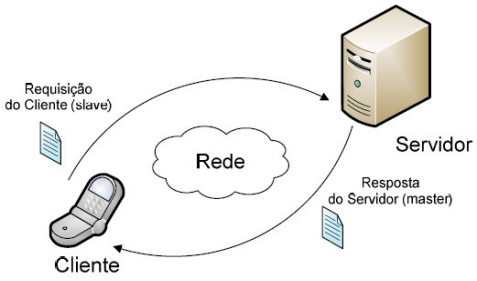


Figura 3 – Filosofia master-slave

É um protocolo de texto bastante flexível uma vez que sendo as suas mensagens em texto, permitem, de forma bastante fácil, adicionar-lhe funcionalidades. O facto de as suas mensagens serem em texto também faz com que estas sejam de fácil compreensão.

Os principais elementos presentes no SIP são espelho do modelo cliente-servidor, isto é, o cliente realiza chamadas que são atendidas pelo servidor. O cliente é visto como o terminal que pretende efectuar uma sessão multimédia e designa-se de UAC (*User Agent Client*). O servidor designa-se de UAS (User Agent Server) e é o terminal do destinatário da sessão. A troca de mensagens SIP entre o UAC e o UAS é efectuada com a ajuda de SIP *proxies,* sendo que, dentro da camada de controlo, todos os elementos da arquitectura IMS estão habilitados para tal.

2.3.1.1 Endereços SIP

Usualmente, o modelo cliente-servidor caracteriza-se por um diálogo, troca de mensagens, onde o cliente pede algo ao servidor, são acertados os pormenores e o pedido é atendido. Durante este processo o cliente é informado sobre o que se passa e responde a perguntas feitas pelo servidor. O SIP define a comunicação, utilizando dois tipos de mensagens: os pedidos e as respostas.

Tal como no processo de envio de uma carta por correio, uma mensagem possui sempre um destinatário e convém que este saiba qual o autor da mesma. No protocolo SIP, a forma de identificar um utilizador é bastante simples de compreender e análoga a um endereço de correio electrónico ou a um número (de telefone) associado a um telefone. Assim, existem duas formas de identificar um cliente, através do SIP URI (ex. sip:Alice.Smith@domain.com) ou o TEL URI (ex. tel: +351123456789) [11]. A primeira parte de um identificador SIP encontra-se associada ao

utilizador, serviço ou número de telefone. A segunda parte pode variar consoante se pretenda ou não que o endereço seja dependente da localização do utilizador. Em caso negativo, normalmente na segunda parte é especificado o nome de um domínio (ex. sip:Alice@domain.pt). No caso inverso, a segunda parte, geralmente, é um endereço IP (ex. sip:Alice@192.168.30.30:5060) ou o nome do computador no domínio (ex. sip:Alice@comp2.domain.pt).

O SIP permite ainda recorrer a identificadores especiais, denominados SIPS URI, para utilizadores que se encontrem associados a comunicações seguras. Desta forma, o utilizador é encarado como um recurso seguro de ser acedido.

2.3.1.2 Mensagens SIP

Uma mensagem SIP respeita sempre um formato, é codificada e apresenta-se em forma de texto, cujas linhas são sempre finalizadas com a sequência <CR><LF>. Ela pode ser dividida em três partes, assim ordenadas: a linha inicial, com instruções; um ou mais cabeçalhos (*headers*), seguidos de uma linha vazia que indica o fim do cabeçalho e, por último um corpo, que é opcional. Este corpo é usualmente encapsulado na mensagem, usando o protocolo SDP – objecto de exposição no sub capítulo 2.3.2 Session Description Protocol - e contém uma descrição detalhada das pretensões para a sessão.

Um pedido SIP distingue-se através da linha inicial presente em todas as mensagens, apelidada de *Request-Line* [12]. Esta linha descreve o tipo de informação que a mensagem transporta, existindo 6 métodos diferentes na actual versão SIP (versão 2) para efectuar a diferenciação.

De forma a aumentar as funcionalidades do protocolo SIP, foram-lhe sendo adicionados métodos, sem bem que os mesmos ainda se encontrem como extensões e espalhados por RFCs do IETF [9]. Existe no entanto um documento onde pode ser encontrado um índice das RFCs associadas ao SIP, o qual pode ser utilizado como guia [13]. A tabela 1 apresenta uma descrição dos seis métodos básicos do protocolo SIP e a tabela 2 algumas das suas extensões.

Método	Descrição
REGISTER	Regista a informação de contacto
INVITE	Pedido de estabelecimento ou alteração de parâmetros numa sessão
ACK	Confirma o estabelecimento de uma sessão
BYE	Termina uma sessão
CANCEL	Usado para cancelar um pedido pendente
OPTIONS	Solicita informação sobre as capacidades suportadas

Tabela 1 – Métodos básicos SIP

Método	Descrição
SUBSCRIBE	Informa o UAS que um UAC pretende ser informado sobre um evento específico (RFC 3265)
PUBLISH	Para enviar informação para o servidor que irá gerar eventos para os utilizadores (RFC3903)
NOTIFY	Notifica o utilizador de um novo evento (RFC 3265)
PING	Confirma se o UAS está receptivo
UPDATE	Utilizado para mudar o estado de uma sessão sem mudar o estado do diálogo

Tabela 2 – Algumas extensões ao método SIP

As respostas SIP são semelhantes aos pedidos, diferindo na linha inicial, denominada *Status-Line*. Esta linha contém uma referência à versão do protocolo utilizado, um código da resposta e uma frase descritiva do mesmo. O código da SIP *Response* é composto por 3 dígitos permitindo diferenciar e classificar os diferentes tipos existentes. O primeiro digito é indicador da classe da resposta, variando entre 1 e 6 inclusive, enquanto que para os últimos dois não existe qualquer regra definida. Desta forma, quando é feita uma referência a uma resposta, por exemplo, compreendida na gama entre 400 e 499, a mesma é tida como uma resposta do tipo "4XX". As respostas na gama do 1 são conhecidas como respostas provisórias, uma vez que correspondem a informação intercalar sobre o progresso do pedido. As respostas da restante gama, entre 2 e 6, são conhecidas como respostas finais e, tal como o próprio nome indica, referem-se à finalização de transacções SIP. A tabela 2 apresenta uma divisão das respostas SIP e respectivo significado tendo em conta a gama a que pertencem.

Código	Classe	Categoria	Exemplo
1XX	Informal	Provisória	180 Ringing
2XX	Sucesso	Final	200 OK
3XX	Redireccional	Final	302 Moved Temporarily
4XX	Erro no Cliente	Final	404 Not Found
5XX	Erro no Servidor	Final	501 Not Implemented
6XX	Falha Global	Final	600 Busy Everywhere

Tabela 3 – SIP *Responses*

Os cabeçalhos (*headers*) SIP, que se encontram a seguir à linha inicial, separados da mesma por uma ou mais linhas em branco, possuem vários campos e são semelhantes aos cabeçalhos HTTP. Alguns, usualmente seis, são de carácter obrigatório, tendo de se encontrar presentes em todas as mensagens SIP, por exemplo o *To* ou o *From*. Por sua vez, alguns só fazem sentido em casos específicos de determinados pedidos ou respostas. O SIP disponibiliza um mecanismo que permite transmitir os cabeçalhos mais comuns de forma abreviada. Tal poderá ser útil quando, por algum motivo, as mensagens se tornem mais extensas.

No caso da recepção de uma mensagem com um cabeçalho não obrigatório - que não faz parte da categoria da mensagem em causa – este deve ser simplesmente ignorado. A tabela 4 apresenta uma breve descrição de alguns dos cabeçalhos mais comuns presentes nas mensagens SIP [11].

Cabeçalho	Descrição	Exemplo
Via	Indica os endereços dos SIP *proxies* percorridos pela mensagem, de forma a ser possível efectuar o mesmo caminho inverso	Via: SIP/2.0/UDP 192.168.15.100:5060 ;branch=z9hG4bka7c6
From	Indica a identidade da origem, o seu SIP URI ou TEL URI	From: Alice <sip:alice@telia.com>
To	Indica a identidade do destinatário, o seu SIP URI ou TEL URI	To: Bob <sip:bob@kth.se>
Call-ID	Contém um identificador global único da sessão, à qual a mensagem pertence. É igual para todas as mensagens da mesma sessão	Call-ID: ffae7de11do@host.com
Cseq	Permite identificar e ordenar o fluxo de mensagens de forma a sincronizar o SIP *Request* e a respectiva SIP *Response*	CSeq: 1 INVITE
Max-Forwards	Possui o número de vezes que uma mensagem deve ser reencaminhada até ao destino, sendo decrementada uma unidade em cada reencaminhamento. Serve para evitar *loops* infinitos	Max-Forwards: 70 (default initial value)
Contact (opcional)	Contém uma ou mais identificações que podem ser utilizadas para contactar o utilizador	Contact: “Alice” <sip:alice@kth.se>
Require (opcional)	Indica as extensões SIP que o EU necessita	Require: 100rel
Supported (opcional)	Indica as extensões SIP que o EU entende	Supported: 100rel

Tabela 4 – Cabeçalhos SIP mais comuns

A figura 4 mostra um exemplo de uma mensagem SIP onde é perfeitamente visível a *Start Line* com um pedido de registo, o method é REGISTER, sendo utilizando a versão 2 deste protocolo.

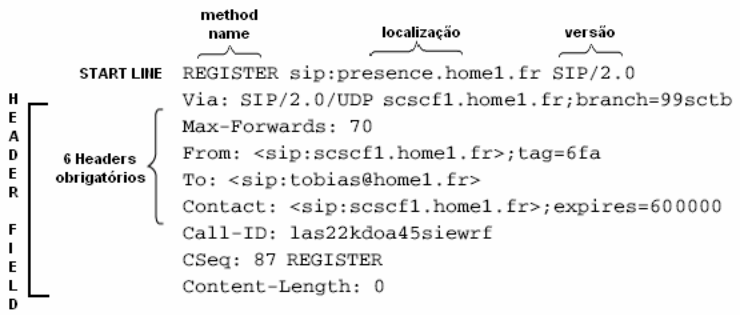


Figura 4 – Exemplo de mensagem SIP

De seguida, surgem os seis cabeçalhos obrigatórios como por exemplo, o *To* onde se constata que o destinatário da mensagem é o Tobias. Estes são precedidos de alguns opcionais que, juntamente com os primeiros, formam a totalidade de cabeçalhos da mensagem.

2.3.1.3 Segurança

Em termos de segurança, o SIP utiliza diversos mecanismos adequados a cada situação. Pretende-se que exista confidencialidade e integridade das mensagens, bem como evitar que as mesmas possam ser desviadas ou ser alvo de ataques que ponham em causa toda a estabilidade dos serviços. O melhor meio de se conseguir segurança é cifrar todas as mensagens. No entanto, uma vez que estas, no seu trajecto até ao destino, podem passar através de *proxy servers* - os quais precisam de as analisar para efectuarem o seu correcto encaminhamento, podendo necessitar igualmente de alterar informação em alguns cabeçalhos, como por exemplo o Via - este tipo de implementação não é viável.

É então utilizado um mecanismo de segurança a um nível mais baixo, onde as mensagens são cifradas entre entidades SIP. Para tal, tira-se partido do protocolo *Transport Layer Security* (TLS), que fornece segurança ao nível da camada de transporte, e do protocolo *Internet Protocol Security* (IPsec) [14] ao nível da camada de controlo.

Os identificadores seguros referidos anteriormente, os SIPS URI, garantem que a sessão irá decorrer em segurança e que é utilizado transporte criptográfico, usando TLS, para entregar a mensagem.

Ao nível da autenticação dos utilizadores, é utilizado o método *Digest* [11], baseado no esquema HTTP *Digest*. Os utilizadores autenticam-se na rede através do nome de utilizador e de uma *password*, sendo esta informação enviada pelas respostas SIP 401 ou 407. Este mecanismo de segurança evita que utilizadores mal intencionados se possam fazer passar por outros.

Exemplo de como este protocolo funciona, ao nível de troca de mensagens, será apresentado no Capítulo 4, onde serão abordados casos como Registo/Desregisto e Estabelecimento e Finalização de Sessão.

2.3.2 Session Description Protocol (SDP)

O protocolo SDP [15], definido pelo IETF, é utilizado pelo protocolo SIP para efectuar a descrição das sessões multimédia. A primeira versão saiu em Abril de 1998 e, após ser alvo de várias revisões, em Julho de 2006 sai o RFC 4566 [16]. Inicialmente o SDP surgiu como componente do *Session Announcement Protocol* (SAP), vindo mais tarde a conjugar-se com protocolos como RTP e SIP, sendo em alguns casos, utilizado de forma independente.

Os campos deste protocolo são inseridos no corpo da mensagem SIP e expressam, entre outras coisas, uma lista das capacidades áudio e vídeo suportadas ou pretendidas, e é neles que é referido para onde os meios devem ser enviados.

Tal como anteriormente foi dito, o SIP baseia-se num modelo de cliente-servidor, e recorre ao SDP para acordar, entre a origem e o destino, quais as características da sessão a ser estabelecida. A origem informa o destino sobre quais as condições que deseja e pode suportar para determinada sessão; o servidor, por sua vez, responde com as características que pretende.

Quando chegam a acordo, é enviada uma SIP *Response* com os campos iguais à SIP *Request* indicando desta forma que estão em concordância [17].

2.3.2.1 Mensagens SDP

Uma mensagem SDP é composta por algumas linhas separadas pelo *carriage-return* e cada linha é inicializada com uma letra, representativa de um parâmetro, seguida do sinal de igual que, por sua vez, é seguido da atribuição para esse parâmetro.

Nas tabelas 5,6 e 7 são apresentados alguns dos campos permitidos no protocolo SDP, estando divididos consoante a informação que comportam.

Tipo	Descrição
v	Versão do protocolo utilizado
o	Identificação do criador e da sessão
s	Nome da sessão
i (opcional)	Informação da sessão
u (opcional)	Descrição do URI
p (opcional)	Numero de telefone
c (opcional)	Informação da conexão
b (opcional)	Informação da largura de banda
z (opcional)	Ajuste do fuso horário
k (opcional)	Chave para a cifra
a (opcional)	Zero, uma ou mais linhas de atributos da sessão

Tabela 5 – Descrição da sessão

Tipo	Descrição
t	Duração temporal da sessão
r (opcional)	Zero ou mais vezes de repetição

Tabela 6 – Descrição temporal

Tipo	Descrição
m	Descrição do *stream*
i (opcional)	Titulo do meio
c (opcional)	Informação da conexão
b (opcional)	Informação da largura de banda
k (opcional)	Chave de encriptação
a (opcional)	Zero, ou mais linhas de atributos da sessão

Tabela 7 – Descrição do meio

Uma mensagem SDP pode ser dividida em duas partes. A primeira, responsável pela descrição do emissor, é seguida de zero ou mais secções que descrevem cada um dos streams. Este conjunto de secções dá origem à segunda parte da mensagem. O parâmetro 'v' é indicador do início da primeira parte e é finalizada pelo indicador de um stream, o parâmetro 'm'. Por sua vez, dentro da segunda parte, cada stream é finalizado pela próxima secção que descreve um

stream. Os nomes mais comuns utilizados são os de *session-level information* e *media-level information* para a primeira e segunda parte, respectivamente. Na figura 5 encontra-se um exemplo de uma mensagem típica, utilizando o formato SDP.

```
v=0
o=Alice 2790844676 2867892807 IN IP4 192.0.0.1
s=Let's talk about swimming techniques
c=IN IP4 192.0.0.1
t=0 0
m=audio 20000 RTP/AVP 0
a=sendrecv
m=video 20002 RTP/AVP 31
a=sendrecv
```

Figura 5 – Exemplo de mensagem SDP

A mensagem pode ser descrita de uma forma simples. O utilizador Alice, disponível no IP 192.0.0.1, pretende estabelecer uma sessão multimédia com o intuito de conversar sobre técnicas de natação. Deseja que a sessão utilize o porto 20000, com o *codec* G.711, corresponde ao 0, para a parte de áudio, com um stream bidireccional. O porto 20002 será utilizado para a parte de vídeo, também com um *stream* bidireccional, com o *codec* H.261, corresponde ao 31.

Constata-se que a mensagem SDP possui duas partes distintas. Neste caso, a primeira, a *session-level information* corresponde às cinco primeiras linhas, enquanto que a segunda possui a descrição de dois *streams*.

2.3.3 Media Gateway Control (MEGACO) / H.248

As *Gateways* são o elemento fronteiriço que permite a interligação de diferentes redes de acesso com o *core* NGN apresentado pelo TISPAN. Para efectuar o controlo destas *Gateways*, foram desenvolvidos vários protocolos como o *Media Gateway Control Protocol* (MGCP), apresentado pelo IETF, e o *Media Protocol Device Control* (MDCP) pelo ITU-T. No entanto, esses protocolos não conseguiram singrar no mercado por serem concorrentes directos entre si. Nasce assim a necessidade de criar um protocolo *standard*, cuja resposta surgiu de uma parceria entre o IETF e o grupo de estudo 16 do ITU-T (*ITU-T Study Group 16*), para esse mesmo protocolo são utilizados dois nomes distintos dependendo da organização que o menciona. A designação *Media Gateway Control* (MEGACO) apresentada na RFC 3525 [18] é utilizada pelo IETF, enquanto que o ITU-T o refere como H.248, apresentado na *Recommendation* H.248.

Este protocolo separa fisicamente duas camadas, a de transporte e a de controlo. Ao contrário do SIP, que segue um princípio de igualdade ponto-a-ponto entre todos os elementos, o MEGACO/H.248 segue um modelo de controlo conhecido por *master-slave*. A interacção é estabelecida entre elementos “inteligentes”, os *masters*, e elementos sem inteligência, *slaves*, que executam exclusivamente as regras recebidas tal como o caso de comunicação entre o MGC e a MGW (Media Gateway).

Segundo este protocolo, são definidos dois elementos designados de contextos e terminações. As terminações são os elementos que se encontram em contacto com o *slave*, por

exemplo uma ligação física entre este e um terminal analógico. A cada terminação encontra-se associada uma identificação única dentro do *slave*. Quando se pretende aglomerar todas as terminações presentes em determinado *slave*, a identificação dada ao conjunto é conhecida como *root*. Por sua vez, os contextos são um conjunto restrito de terminações em determinado *slave*.

2.2.3.1 Mensagens Megaco/H.248

Uma mensagem que utilize o protocolo MEGACO tira partido de um conjunto de comandos, na sua maioria com o intuito de efectuar o controlo dos *slaves*. A tabela 8 possui uma breve descrição dos mesmos.

Comando	Descrição
ADD	Adiciona uma terminação a um contexto. Se este comando for usado na primeira terminação no contexto, é usado para criar o contexto (enviado pelo *master*)
MODIFY	Modifica as propriedades,eventos e sinais de uma terminação (enviado pelo *master*)
SUBTRACT	Retira uma terminação de determinado contexto. Caso seja utilizado na última terminação do contexto, então o contexto é removido. (enviado pelo *master*)
MOVE	Move a terminação de um contexto para outro (enviado pelo *master*)
AUDITVALUE	Solicita o valor actual do estado das propriedades, eventos,sinais e estatísticas de uma terminação específica. (enviado pelo *master*)
AUDITCAPABILITIES	Solicita todos os valores possíveis de propriedades, eventos e sinais nas terminações do *slave*. (enviado pelo *master*)
NOTIFY	Permite que o *slave* informe o *master* dos sinais recebidos que estão a ocorrer. (enviado pelo *slave*)
SERVICECHANGE	Permite que o *slave* notifique o *master* que uma terminação ou conjunto de terminações estão ou vão estar fora de serviço ou que entraram em serviço para efeitos de registo. Pode ser utilizado pelo *master* para informar um slave, que se encontre sob o seu controlo, que vai passar para outro *master* ou informar o *slave* para tirar de serviço uma terminação ou um grupo de terminações. (enviado pelo *master* e pelo *slave*)

Tabela 8 – Comandos MEGACO/H.248

Estes comandos são utilizados de forma bem definida, seguindo a seguinte estrutura:

Comando = Terminação Por exemplo: ADD = termC a terminação C é adicionada

Usualmente, a cada comando enviado encontra-se implícita uma resposta de confirmação de recepção utilizando um REPLY. Associados aos comandos atrás descritos, existem parâmetros que são designados por descritores. Cada tipo de descritor possui informação específica para determinada função do protocolo. Alguns exemplos de descritores encontram-se na tabela 9.

Descritor	Comando
Media	Descreve a transformação a ser aplicada no fluxo multimédia através da terminação
Events, EventBuffer e Observedevents	Selecciona e reporta o evento, por exemplo *off-hook* ou *on-hook*, corrente ao *master*.
Signals	O *master* indica qual o sinal que deseja que o slave monitorize. Por exemplo sinal de ocupado ou de chamada.
Local and Remote	Carrega informações, descrevendo o tipo de fluxo multimédia no *stream*.
LocalControl	Determina a direcção do fluxo do stream
ServiceChange	É utilizado com o comando ServiceChange e notificando uma alteração que pode ser do tipo: - Graceful: remover terminações esperando finalização da ligação - Forced: remover abruptamente terminações - Restart: após ocorrer um atraso - Disconnected: aplicado sobre o *slave* - Handoff: utilizado entre um master antigo e um novo master
Error	Retorna a indicação de falha como resposta a determinado comando que não foi executado com sucesso.

Tabela 9 – Descritores MEGACO/H.248

O uso de descritores segue o seguinte padrão:

Comando = <someID>{parâmetro = valor, parâmetro = valor,.....}

No exemplo seguinte o descritor modifica a terminação C para verificar a ocorrência do evento de *off-hook*.

MODIFY = TermC{Events = 111 {al/of} }

O MEGACO/H.248 segue uma filosofia onde os comandos são agrupados dentro de acções e estas, por sua vez, dentro de transacções, tal como ilustrado na figura 6. A cada transacção encontra-se associado um identificador único – *Transaction* ID. Os comandos agrupados dentro de cada transacção são executados de forma sequencial, mas as transacções podem sê-lo fora de ordem e, simultaneamente, de forma concorrente. No final de cada transacção executada com sucesso pelo *slave*, surge uma resposta para o *master*, a *Transaction Reply* associada ao respectivo *Transaction* ID. Caso o *master* não receba a esperada *Transaction Reply*, então envia ao *slave* uma *Transaction Pending* informando que existe uma transacção pendente em espera.

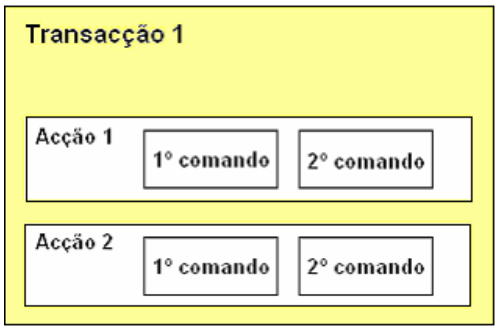


Figura 6 – Filosofia Megaco

De uma forma geral, este protocolo oferece uma abordagem simples de controlo de *Gateways* englobando todas as suas aplicações: *Gateways* de tipo *trunking* da PSTN, interfaces ATM, linhas analógicas, telefones IP e muito mais. O facto de apresentar alguns pontos-fortes como a simplicidade, flexibilidade e baixo custo efectivo contribuiu fortemente para que tivesse surgido como um dos protocolos *standard* utilizado no IMS.

2.3.4 DIAMETER

Este protocolo [59] pode ser encarado, numa perspectiva geral, como sendo o gestor da operação de autenticação, autorização e *accounting* (AAA) no IMS. Antigamente, quando um utilizador tentava por exemplo ligar-se ao seu fornecedor de Internet (*Internet Service Provider* – ISP), enviava a sua identificação (ID) e a *password* para um servidor de acesso, que posteriormente verificava a sua validade. Na maioria dos casos, as credenciais do utilizador não se encontravam guardadas directamente no servidor de acesso mas num local mais salvaguardado como um servidor LDAP (*Lightweight Directory Access Protocol*), protegido por uma *firewall*. Ora era necessário um protocolo seguro para a troca de informações entre o servidor de acesso e o servidor de credenciais, e daí ter surgido o RADIUS (*Remote authentication Dial-In User Service*) [19] para efectuar o AAA necessário.

Com o passar do tempo, verificou-se um crescimento no número de novas tecnologias e de aplicações, por exemplo o *Wireless*, aumentando a necessidade de requisitos para autenticação e autorização, os quais se encontram de uma forma sucinta na RFC 2989. O protocolo até então adoptado, o RADIUS, começou a sofrer algumas extensões com o objectivo de acomodar os, novos requisitos, ao mesmo tempo que algumas lacunas - como não suportar *roaming* de forma eficiente ou admitir que vários clientes pudessem ter a mesma *password* - passaram a ser intoleráveis, o que levou a que este protocolo deixasse de ser desenvolvido em 1998. O Diameter surge desta evolução, apresentando bastantes melhorias relativamente ao seu antecessor. Um dos trunfos deste protocolo, ilustrado na figura 7, foi o facto de aproveitar algumas características do AAA do RADIUS e definir um conjunto de mensagens que são suficientes para criar uma base protocolar independente intitulada *Diameter base protocol* [20]. O formato da mensagem, a forma como é transportada e erros são alguns dos parâmetros constituintes desta base protocolar, devendo os mesmos ser suportados por todas as implementações que utilizem

Diameter. Cada aplicação que necessite de mecanismos de AAA pode tirar partido dessa base e definir extensões da forma mais conveniente para o seu caso específico.

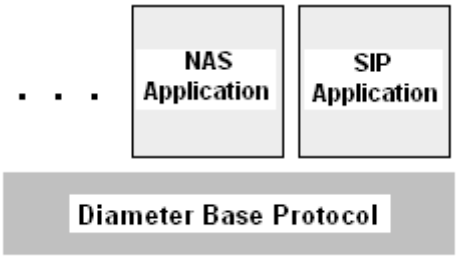


Figura 7 – Base Diameter

2.2.4.1 Mensagens Diameter

O protocolo Diameter possui um conjunto de mensagens disponíveis para a base, diferenciáveis através do seu nome e respectivo código. Por exemplo, uma base que possua um *Accounting-Request* é imediatamente associada ao transporte de informação de taxação. A cada tipo de mensagem corresponde um código de 24 *bits* – *command code* - o qual é comum ao pedido e respectiva resposta. A tabela 10 apresenta algumas das mensagens base que o protocolo Diameter suporta, com a respectiva abreviatura e *command code*.

Mensagem	Abreviatura	Command code
Abort-Session-Request	ASR	274
Abort-Session-Answer	ASA	274
Accounting-Request	ACR	271
Accounting-Answer	ACA	271
Capabilites-Exchanging-Request	CER	257
Capabilities-Exchanging-Answer	CEA	257
AA-Request	AAR	265
AA-Answer	AAA	265
Disconnect-Peer-Request	DPR	282
Disconnect-Peer-Answer	DPA	282
Re-Auth-Request	RAR	258
Re-Auth_Answer	RAA	258
Session-Terminatiom-Request	STR	275
Session-Termination-Answer	STA	275

Tabela 10 – Mensagens Diameter

O *command code* é utilizado apenas para identificar qual o intuito da mensagem, já que o suco da informação é carregada num conjunto de *Attribute-Value-Pairs* (AVPs), tal como ilustrado na figura 8, podendo estes suportar informação de AAA, encaminhamento ou segurança entre dois nós *Diameter*. O formato em que cada AVP é apresentado designa-se por *AVP Data Format* e pode, ser por exemplo, do tipo *Unsigned32* ou *OctetString*.

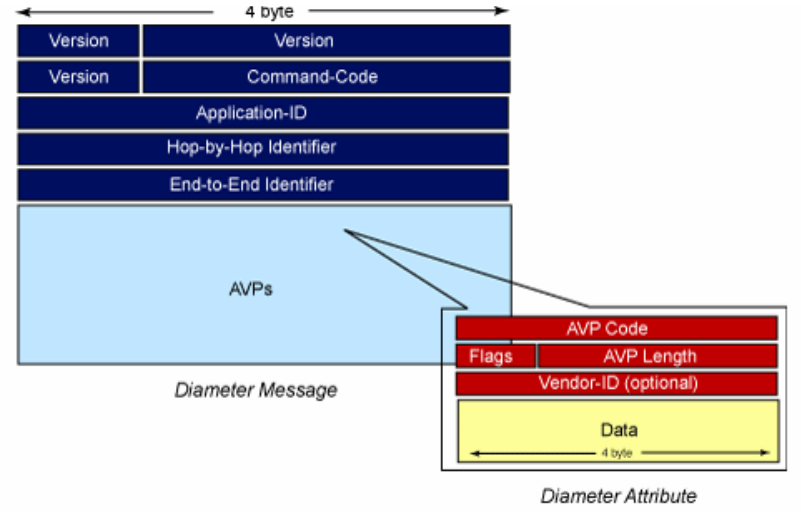


Figura 8 – Componentes de uma mensagem Diameter

Cada AVP possui um código associado, o AVP *Code*, consoante a informação transportada e o formato em que se encontra. Na tabela 11 são apresentados, apenas a título de exemplo, alguns dos inúmeros AVP *Codes* disponíveis.

Nome do Atributo	Código	Formatação
Accounting-Record-Number	485	Unsigned32
Error-Message	281	UTF8String
Authorization-Lifetime	291	Unsigned32
Accounting-Session-Id	44	OctetString

Tabela 11 – AVPs *Codecs*

Neste protocolo os erros são divididos em duas categorias: os erros de protocolo e de aplicação. Nos primeiros, englobam-se aqueles cuja origem provem do protocolo sob o qual o Diameter assenta, por exemplo um encaminhamento incorrecto da informação ou uma falha na rede. Já os segundos são devidos a falhas do próprio Diameter. Quando determinado nó detecta uma mensagem de erro, encaminha todas as mensagens semi-pendentes para um nó que suporte Diameter alternativo, designando-se esta reacção por *FailOver*. Cada nó que utiliza este protocolo tem de guardar temporariamente as mensagens enviadas, porque as que são semi-pendentes, embora já tenham sido encaminhadas, delas ainda não foi recebida a respectiva resposta. Se tal cópia de segurança não existisse, o risco de perder informação era grande.

A semântica utilizada nas mensagens de erro é a mesma do protocolo SIP, onde o tipo de erro pode ser facilmente identificado através do primeiro dígito dos três que são recebidos. Desta forma, a tabela 4 apresentada no sub capítulo 2.3.1.2 aquando da descrição das respostas nas mensagens SIP, serve de igual modo para consultar os erros disponíveis no protocolo Diameter.

2.3.5 Real-Time Transport Protocol (RTP)

O RTP [21] é um protocolo definido pelo IETF, que permite funções de transporte, ponto a ponto, na rede, sendo normalmente utilizado para o transporte de dados em tempo real, como áudio e vídeo. De uma forma geral, o RTP corre em UDP (*User Datagram Protocol*), mas pode correr em TCP ou mesmo sobre outros sistemas de transporte. A escolha recai sobre UDP, pois é um protocolo rápido, simples e sem conexão. Este protocolo suporta a multiplexagem de diversos fluxos multimédia sobre um único fluxo de pacotes UDP, o qual não garante por si só quer a entrega dos pacotes, quer, no caso de esta se verificar, a informação sobre o tempo que demora. Numa rede de dados é frequente surgir latência, atrasos (*jitter*) ou mesmo perda de pacotes.

A Latência é descrita como sendo o tempo total que um pacote demora a chegar do emissor ao receptor. De acordo com a recomendação G.114 da ITU-T [22], este tempo não deve exceder os 150ms em cada sentido. Para valores superiores, poderá existir uma grande sobreposição das vozes dos interlocutores, podendo ficar a comunicação bastante degradada, quase imperceptível. Na caso de redes que transportam dados, o tempo total é a soma das várias latências ao longo do trajecto dos pacotes por entre os elementos que a constituem.

O *Jitter* mede a variação da latência entre pacotes sucessivos de dados, e o ideal é que o ritmo a que os pacotes são recebidos fosse igual àquele a que são gerados no emissor. A um jitter elevado corresponde uma variação brusca na recepção, o que pode ser prejudicial em aplicações em tempo real, por estas necessitarem de receber pacotes a um ritmo constante, como por exemplo chamadas de voz.

Uma forma de minimizar o jitter é utilizar um *buffer*, que procede ao armazenamento dos pacotes de dados à medida que eles chegam, enviando-os posteriormente para o receptor a uma cadência fixa, podendo também efectuar o reordenamento dos pacotes. O *buffer* implica uma latência suplementar que não deve ser negligenciada.

A perda de pacotes na rede pode ser originada, quer por erros do próprio meio físico onde são transportados, quer por políticas de eliminação de pacotes por excesso de tráfego ficando, em qualquer dos casos, a prestação da rede prejudicada.

Assim, é através da utilização paralela do RTP com o RTCP que aplica mecanismos capazes de detectar perda de pacotes e efectuar monitorização de entrega. A figura 9 ilustra a informação específica que cada pacote RTP deve transportar para o seu correcto funcionamento.

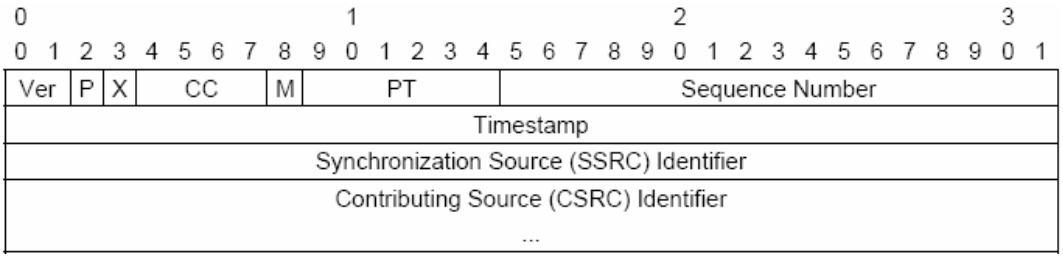


Figura 9 – Cabeçalho do Pacote RTP

Apresenta-se a seguir uma breve descrição dos campos presentes no cabeçalho do pacote RTP.

• **V** – identifica a versão RTP utilizada
• **P** – *padding* de octetos no final. Estes deverão ser ignorados pois estão ali apenas devido a certos algoritmos de encriptação necessitarem um tamanho fixo dos blocos
• **X** – bit que permite assinalar se existe ou não um cabeçalho de extensão.
• **CC** – quantos identificadores CSCR existem
• **M** – bit de marcação específico da aplicação
• **Sequence Number** - este número identifica de forma única cada pacote RTP sendo incrementado em uma unidade a cada novo pacote. É utilizado para detectar perda de pacotes ou para restaurar a sua ordem correcta.
• **Timestamp** – Indicador temporal
• **PT** – O *Payload Type* indica o tipo de *codec* que está a ser utilizada. Por exemplo o tipo 31 corresponde ao H.261 enquanto que o 33 ao MPEG2.

Alguns tipos de *Payload Type* compatíveis com o protocolo RTP, assim como as respectivas RFCs, encontram-se na tabela 12.

Formato de *Payload type* RTP	RFC
H.261 Video Streams	2032
JPEG-compressed Video	2435
RTP Payload Format for MPEG-4 Audio/Visual Streams	3016
MP3 Audio	3119
PureVoice(tm) Audio	2658
H.263 Video Streams	2190

Tabela 12 – *Payload types* para RTP

Todos os elementos que tirem partido do protocolo RTP devem possuir um buffer, como forma de precaver algumas das situações anteriormente descritas. Um receptor ao receber pacotes que vão preenchendo o buffer organiza-os segundo o seu *timestamp*. Caso seja necessário reproduzir um pacote associado a determinado *timestamp* e este não se encontre ainda disponível no buffer, então, de forma a colmatar essa falha, são utilizadas técnicas de interpolação.

Embora este protocolo não garanta qualidade de serviço, é no entanto, frequentemente utilizado em conjunto com o RTCP, permitindo que haja uma monitorização da sessão. O uso do RTP e RTPC é paralelo, mas os pacotes de cada protocolo são transmitidos de forma independente.

2.3.6 Real-Time Control Protocol (RTCP)

Com o intuito de monitorizar a qualidade de serviço, o RTP faz uso de um protocolo auxiliar de controlo denominado RTCP (*Real-Time Control Protocol*), que não é responsável pelo transporte de quaisquer dados, tendo como principal e única função fornecer *feedback* sobre o estado da rede e monitorizar determinada sessão. Esta monitorização permite que os participantes de determinada sessão multimédia se adaptem dinamicamente da melhor forma. A figura 14 apresenta uma mensagem RTCP com os respectivos campos.

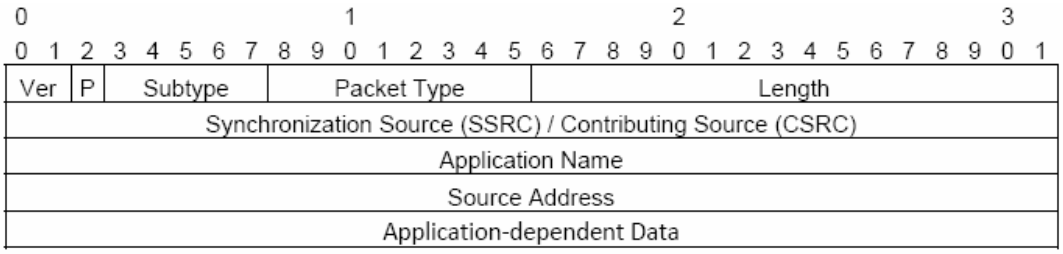


Figura 10 – Mensagem RTCP

De forma a tornar o controlo de determinada sessão mais eficiente, todos os participantes numa sessão RTP são responsáveis pelo envio de pacotes RTCP, usando o mesmo método de envio dos pacotes RTP, mas numa porta UDP diferente.

É assim possível às partes envolvidas numa sessão RTP obter informação sobre a QoS da mesma, isto é, sobre o número de pacotes recebidos, pacotes enviados, pacotes perdidos e atraso. Esta informação não fornece de forma directa QoS, mas permite que uma aplicação recolha dados sobre a transmissão e se possa adaptar ao estado da comunicação.

2.4 Arquitectura

A arquitectura global [23], tendo por base o core IMS, apresentada pelo TISPAN para as NGNs, é a que se encontra esquematizada na figura 11.

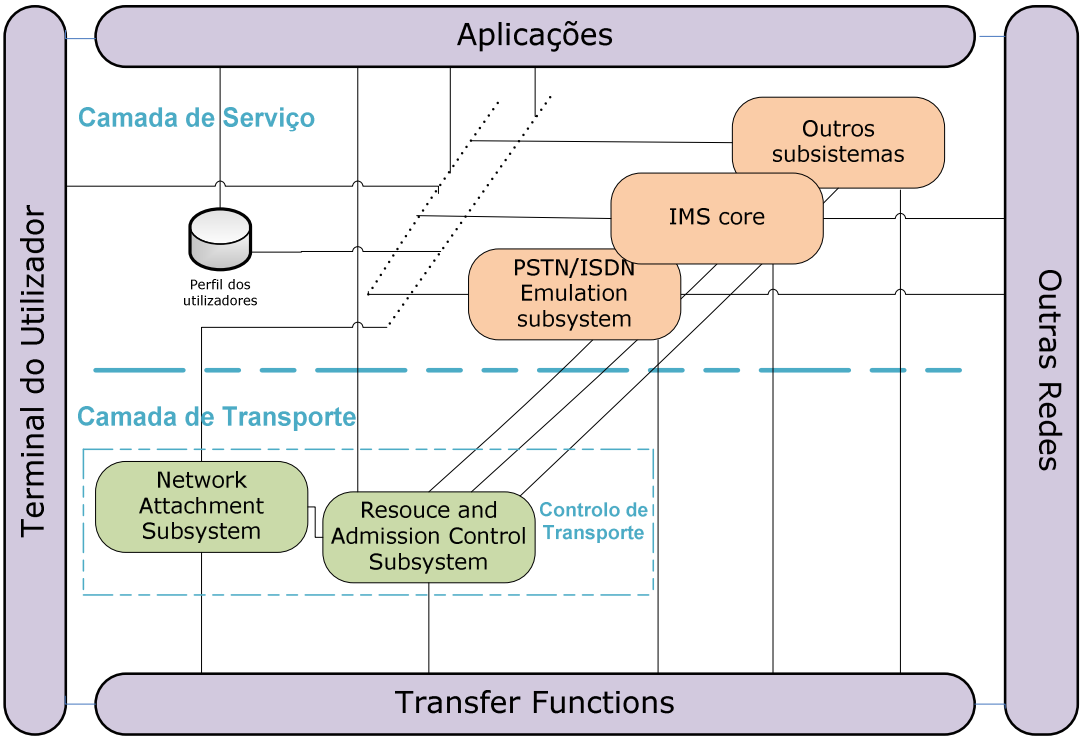


Figura 11 – Arquitectura global TISPAN

Existe uma divisão clara em duas camadas distintas com diferentes subsistemas que, no seu conjunto, formam a arquitectura global TISPAN. Este tipo de segmentação em diversos subsistemas - que intercomunicam entre si e o exterior, mas que, em termos de funcionalidades são independentes - é bastante apelativo, uma vez que permite uma evolução quer a nível global quer a nível específico de determinado subsistema sem que, de uma maneira geral, a arquitectura global sofra alterações bruscas.

A camada de serviço engloba vários subsistemas, sendo de destacar o IMS core e o subsistema para Emulação de serviços PSTN/ISDN (PSTN/ISDN Emulation Subsystem – PES). Sendo este último que permite a ligação directa de POTS, através de *Media Gateways* Residenciais/Acesso, ao core IMS definido pelo TISPAN.

A camada de Transporte inclui dois subsistemas, cuja função é controlar a gestão dos recursos envolvidos na conectividade IP, designados por *Network Attachment Subsystem* (NASS) e *Resource and Admission Control Subsystem* (RACS). Engloba também o subsistema denominado “Funções de Transferência”, responsável pela definição das funcionalidades dos elementos físicos que efectuam a interligação da rede NGN e outras redes de acesso.

Os vários subsistemas presentes na arquitectura global TISPAN encontram-se interligados, mas podem e devem ser analisados de forma independente, tendo em conta a camada onde se encontram localizados e a sua funcionalidade.

2.4.1 Camada de Transporte

O NASS e o RACS podem ser inseridos numa subcamada responsável pelo controlo de transporte, diferenciando-se mais nitidamente da subcamada Funções de Transferência, tal como ilustrado na figura 11. De seguida é efectuada uma breve descrição dos subsistemas funcionais que constituem esta camada.

2.4.1.1 Network Attachment Subsystem (NASS)

O subsistema NASS [24] fornece um contexto ao utilizador, alocando de forma dinâmica endereços IP e outros parâmetros de configuração a cada terminal na rede de acesso, o que permite que estes possam ter relação com outros elementos da arquitectura. A gestão do espaço de endereços disponíveis e a localização de cada utilizador nas diferentes redes de acesso encontra-se a cargo deste elemento. É igualmente responsável por fornecer autenticação na camada IP noutras camadas e ainda pela autorização e configuração do acesso à rede, baseada no perfil dos utilizadores. Este subsistema engloba vários elementos como por exemplo o CLF (*Connectivity session Location and repository Function*) e o UAAF (*User Access Authorization Function*).

2.4.1.2 Resource and Admission Control Subsystem (RACS)

De uma forma geral, o RACS [25] pode ser encarado como sendo o subsistema que permite a reserva de recursos e níveis específicos de qualidade para determinada sessão. Interage com as “Funções de Transporte” de forma a controlar uma ou mais funcionalidades, como por exemplo, alocação de banda, classificação de tráfego, *firewall*, filtragem de pacotes ou gestão de prioridade, actuando desta forma como um árbitro na negociação entre as aplicações e as funções de transporte. Este elemento comunica com o NASS para verificar perfis de utilizadores e, com isso, saber quais os serviços que determinado utilizador está habilitado a usufruir.

Este subsistema é composto por dois elementos, denominados A-RACF e SPDF (*Service Policy Decision Function*). O primeiro encontra-se sempre localizado na rede de acesso, e suporta a reserva de recursos, recebendo também pedidos do SPDF para tomar decisões de gestão sobre este.

O SPDF fornece um ponto de contacto aos elementos que necessitam de interagir com o RACS, como, por exemplo, o IBCF, a AGCF ou o P-CSCF, tirando partido do protocolo DIAMETER.

2.4.1.3 Transfer Functions

A camada de transporte possui esta subcamada que contém diversas identidades com funções necessárias para a realização da transferência de tráfego IP entre os terminais dos utilizadores e qualquer destino que se encontre na NGN ou noutro tipo de rede de acesso. A figura 16 ilustra as diversas entidades abrangidas por este subsistema, sendo objecto de uma breve descrição as seguintes: A *Media Resource Function Processor* (MRFP), a *Signalling Gateway Functions* (SGF), a *Media Gateway functions* (MGF), a *Access Relay Functions* (ARF), a *Border Gateway Function* (BGF) e a *Resource Control Enforcement Function* (RCEF).

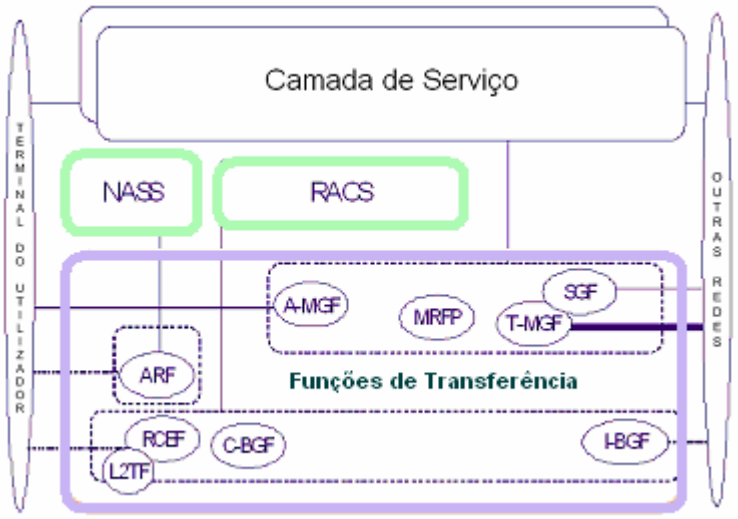


Figura 12 – Funções de Transferência

2.4.1.3.1 Media Resource Function Processor (MRFP)

A MRFP [26] disponibiliza funcionalidades adicionais, para além das oferecidas pela MGW, tais como conferências multimédia, análise do conteúdo multimédia e funcionalidades IVR (*interactive voice response*). O IVR é o acrónimo inglês para descrever a resposta interactiva de voz que possibilita a detecção de voz ou de DTMF.

O MRFC (???) é responsável pelo controlo da MRFP e encontra-se localizado na camada de serviço.

2.4.1.3.2 Signalling Gateway Function (SGF)

De uma forma geral, é este elemento [26] que tem o papel de efectuar a conversão de sinalização ao nível de transporte. A informação não é interpretada ao nível da aplicação, limitando-se este elemento a fazer a conversão de MTP (*Message Transfer Part*) da sinalização SS7 em SCTP (*Stream Control Transmission Protocol*), sendo o resultado encaminhado para a MGCF. No caso inverso, quando se recebe informação ISUP ou BICC [39] proveniente da MGCF, dá-se a conversão para MTP.

2.4.1.3.3 Media Gateway Function (MGF)

A MGF [26] é considerada um dos elementos mais importantes na integração de serviços entre a rede PSTN as NGNs. De uma forma abrangente, é encarada como o elemento responsável pelo *transcoding* entre os dados da rede IP e da rede de comutação de circuitos. Outras das suas funcionalidades são efectuar o controlo e reserva de recursos media e envio de anúncios. Existem três MGF com diferentes designações, tendo em conta a sua localização e tarefas desempenhadas: a MGF Residencial (*Residential* MGF – R-MGF), a MGW de Acesso (*Access* MGW – A-MGF) e a MGW de *Trunking* (T-MGW). As duas primeiras serão abordadas neste Capítulo na secção 2.4.2.2 .

A T-MGW definida na arquitectura TISPAN advém da IMS-MGW descrita pelo 3GPP, encontrando-se entre o domínio IP e a rede de comutação de circuitos. As suas características funcionais podem ser consultadas na norma ETSI TS 123 002 [27]. Uma das suas funções é efectuar a conversão entre o protocolo RTP, do domínio IP, e o protocolo PCM, do domínio PSTN, devendo possuir ainda capacidade de detecção e processamento de sinalização DTMF [28] e interagir com o MGCF, através do protocolo MEGACO/H.248, para controlo de recursos. No caso em que existem incompatibilidades entre o codec utilizado no terminal IP e no terminal PSTN, deve ser capaz de efectuar o transcoding. Este elemento é, assim, o intermediário entre dois tipos de redes distintas.

2.4.1.3.4 Access Relay Function (ARF)

Este elemento [26] actua como um retransmissor entre o UE e o NASS, recebendo pedidos dos UE, presentes na rede de acesso, e reencaminhando-os para o NASS. Antes de efectuar o reencaminhamento, a ARF pode também inserir na mensagem informação relevante de configuração e/ou ter necessidade de efectuar conversão protocolar, de modo a que o NASS compreenda a informação. Por exemplo, se utilizar PPP (*Point-to-Point Protocol*) [29], a ARF tem como função efectuar a sua conversão para RADIUS ou DIAMETER, podendo também efectuar conversões de PPPoA (*Point-to-Point Protocol over ATM*) [30] para PPPoE (*Point-to-Point Protocol over Ethrnet)* [31].

2.4.1.3.5 Border Gateway Function (BGF)

Tal como o próprio nome indica, a BGF [26] actua como uma *gateway* entre dois domínios IP. Podendo encontrar-se localizado na fronteira entre a rede de acesso e o UE, entre uma rede de acesso e o core da rede ou entre dois *cores* diferentes.

Muitas são as funções desempenhadas por este elemento, sendo algumas as seguintes:

- Filtragem de pacotes baseada nos endereços IP ou no controlo de portos
- Alocação de recursos
- Medidor de utilização
- Alocação e tradução de endereços IP e números de portas - *Network Address Port*

Translation (NAPT) [32]

- Esconder a topologia utilizada
- Efectuar a interligação entre as redes IPv4 e IPv6 - *Network Address Port Translator-Protocol Translator* (NAPT-PT) [33]
- Marcação de pacotes para tráfego externo

A BGF interage com entidades na subcamada de controlo de transporte com o intuito de monitorizar uma ou mais das funcionalidades que implementa. Podem ser identificadas, dois tipos distintos de BGFs - *core* BGF (C-BGF) e *Interconnection* BGF (I-BGF) – encontrando-se a primeira localizada na *Border Gateway*, na fronteira entre a rede de acesso e o *core* do lado deste último.

Entre o *core* e outra rede IP de acesso, encontra-se a I-BGF, que é também controlada pelo RACS.

.

2.4.1.3.6 Resource Control Enforcement Function (RCEF)

A RCEF pode estar na rede de acesso ou nas suas bordas sendo controlada pelo RACS. Algumas das suas tarefas são efectuar o policiamento do tráfego que entra na NGN ou a alocação de recursos utilizados pelo tráfego de entrada/saída.

2.4.2 Camada de Serviço

A subcamada de serviço da arquitectura geral TISPAN contempla um conjunto de diferentes subsistemas, com o intuito de dar resposta à interligação entre diferentes redes de acesso. O IMS, definido pelo 3GPP na *Release* 6, pode ser encarado como o subsistema base da arquitectura apresentada pelo TISPAN sendo que este tira partido da camada de controlo deste *core* e reutiliza-o na sua arquitectura, abrangendo, através de elementos de outros subsistemas, um leque mais vasto de redes de acesso.

A esta subcamada cabe-lhe também a função de englobar um arquivo com informação dos clientes e por albergar os servidores de aplicações.

O grande trunfo da arquitectura TISPAN é a chamada emulação PSTN, permitindo que determinada operadora NGN alargue a sua oferta aos clientes da rede tradicional nomeadamente acessos xDSL e que a transição para as NGNs seja efectuada suavemente.

O subsistema PES imita uma rede PSTN/ISDN, do ponto de vista dos terminas analógicos (POTS), interligando-os a uma rede IP acedida através de uma *gateway* específica. Todos os serviços base continuam disponíveis e idênticos para o utilizador, não se apercebendo este, sequer, que não se encontra ligado a uma rede convencional baseada em TDM.

Figura 13 – Evolução PSTN (adaptada de [34])

Novos operadores que estão agora a entrar no mercado acreditam que a emulação PSTN/ISDN é pobre e oferece quase a mesma experiência aos utilizadores, incluindo os terminais, e que só através do salto para a simulação PSTN, conforme se ilustra na figura 13, é possível disponibilizar uma experiência rica aos utilizadores. No entanto, para os muitos operadores actuais e para a maioria dos clientes, este tipo de salto não pode ser repentino. A emulação poderá ser encarada como o passo intermédio necessário para se alcançar a verdadeira convergência fixo-móvel, com todos os novos serviços associados.

2.4.2.1 IMS core

A arquitectura global apresentada pelo TISPAN para as NGN possui, na sua camada de serviço, um subsistema designado de IMS *core*. Face à necessidade de disponibilizar aos clientes das NGN serviços multimédia baseados em SIP e efectuar o seu controlo o TISPAN baseou-se na *Release* 6 do core IMS do 3GPP. No entanto, só alguns elementos, os de controlo, são associados como sendo parte integrante do subsistema. A figura 14 é elucidativa relativamente a esta questão, ilustrando o subsistema e os seus elementos constituintes, bem como a sua interligação com a restante arquitectura.

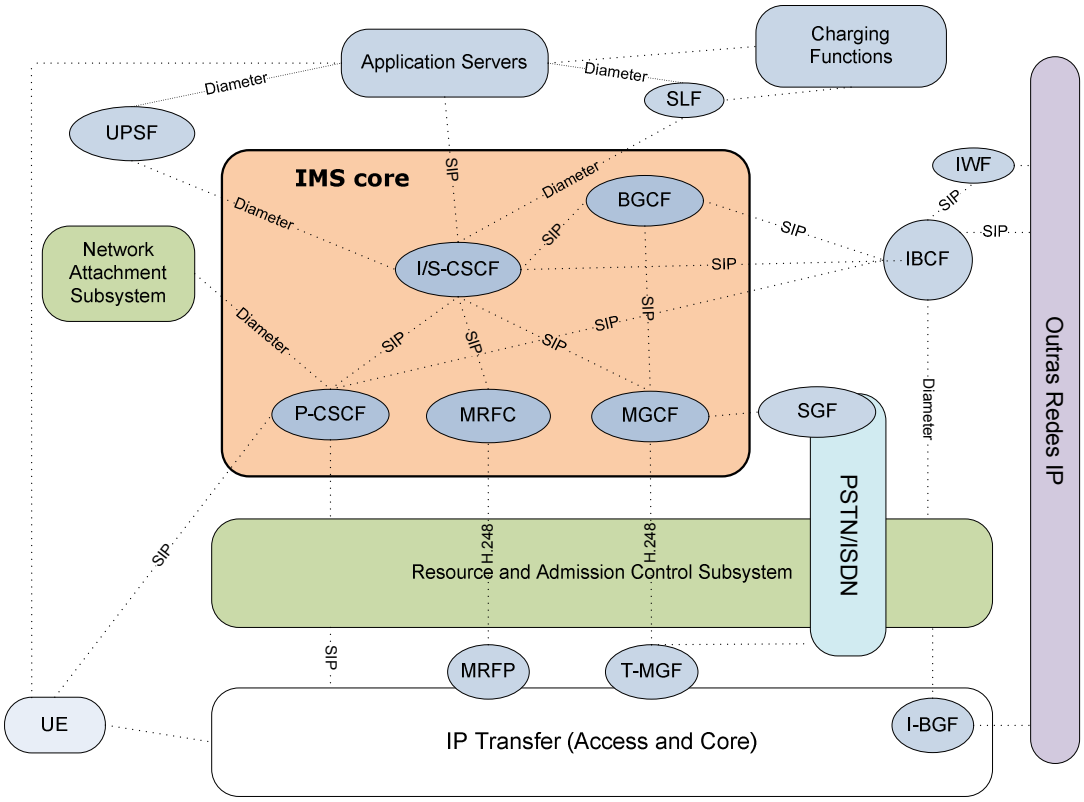


Figura 14 – Subsistema *core* IMS (adaptada de [26])

Existem elementos que até então, eram considerados pelo 3GPP como parte integrante do *core* IMS, mas que não o são da arquitectura apresentada pelo TISPAN. O SLF, elemento residente na camada de controlo do *core* IMS do 3GPP, é um bom exemplo desta situação.

Embora muitos elementos utilizados neste subsistema advenham da arquitectura do 3GPP, é de salientar que alguns sofreram pequenas adaptações. Na sua generalidade, tal deve-se ao facto de o acesso às redes xDSL, suportadas na arquitectura proposta pelo TISPAN, ser diferente do acesso às redes UMTS e ao facto da reserva de recursos ser efectuada de maneira distinta. Na maioria dos casos o reajustamento efectuado foi um *upgrade* às funcionalidades básicas dos elementos. Por exemplo, ao P-CSCF, tirando partido da sua ligação ao RACS, foi acrescentada a capacidade de obtenção de informação sobre a localização do UE na rede. Esta funcionalidade é denominada de *Network Address and Port Translation* (NAPT).

De seguida é efectuada uma descrição dos elementos que são parte integrante deste subsistema.

2.4.2.1.1 Proxy Call Session Control Function (P-CSCF)

O P-CSCF é vulgarmente descrito como sendo o primeiro ponto de contacto dentro do subsistema IMS e é visto como a sua porta de entrada. A cada utilizador encontra-se associado um P-CSCF, sendo este atribuído aquando a fase de registo. Todo o tráfego de sinalização

proveniente do UE é encaminhado para este nó, o mesmo acontecendo com todo o tráfego do *core* com destino a terminado UE, funcionando o mesmo como um *proxy*.
Mecanismos de compressão de mensagens SIP devem ser suportados por este elemento, reduzindo desta forma o tempo de transmissão e, consequentemente, o tempo de estabelecimento da sessão.

De entre as funcionalidades especificadas para o P-CSCF, uma das principais é a autenticação do utilizador [36]. É durante este processo que se estabelecem SAs (*Security Associations*) com os UEs e são aplicados mecanismos de integridade e confidencialidade necessários. Todos os outros elementos da arquitectura IMS encaram o P-CSCF como um nó de confiança e apenas ele procede à autenticação do utilizador.
Ao ser a porta de entrada para os pedidos SIP o P-CSCF, verifica previamente a validade de cada pedido antes de o encaminhar para o interior da rede, diminuindo assim o número de mensagens incorrectas, o que permite rentabilizar o funcionamento do *core* IMS.

Outra característica deste elemento é o facto de possuir uma PDF (*Policy Decision Function*) responsável por efectuar a gestão dos recursos disponíveis com o intuito de garantir Qos. As informações que o PDF do P-CSCF possui são necessárias, caso um operador deseje implementar uma SBLP (*Service-Based Local Policy*).

O P-CSCF deve ter a capacidade para detectar casos de chamadas de emergência, e de as encaminhar.

2.4.2.1.2 Interrogator Control Session Control Function (I-CSCF)

O I-CSCF quando recebe um pedido de registo vindo do P-CSCF é responsável por atribuir um S-CSCF a cada cliente. Para tal, comunica com o UPSF, tirando partido do protocolo Diameter, de forma a obter informações acerca do cliente. Depois de ter atribuído um S-CSCF durante o processo de registo, a função deste elemento é a de encaminhar pedidos para S-CSCFs de outras redes. É o caso de um utilizador que pretenda efectuar uma sessão multimédia para um destinatário que se encontra registado noutro operador, sendo o endereço do S-CSCF exterior obtido antes de efectuar o encaminhamento das mensagens SIP. O I-CSCF funciona assim como um proxy SIP entre operadores distintos.

Este elemento pode também, de forma opcional, implementar uma funcionalidade conhecida por THIG (*Topology Hiding Inter-network Gateway*) que permite cifrar os cabeçalhos das mensagens SIP que transportem informação considerada sensível, conseguindo assim, esconder a informação relativa à sua topologia.

2.4.2.1.3 Serving Control Session Control Function (S-CSCF)

Este elemento é a peça central do subsistema IMS, funcionando como um SIP *proxy* utilizado durante o processo de registo dos utilizadores. É necessário que o S-CSCF comunique, através de Diameter, com o UPSF (???), de forma a obter diversas informações de autenticação do cliente verificando a sua veracidade através de vectores de autenticação.

Após o registo, o S-CSCF acede ao UPSF com o intuito de consultar o perfil do cliente, para saber quais os serviços que este está habilitado a usufruir. Consegue desta forma decidir para que AS devem ser encaminhados os pedidos dos clientes e efectuar uma politica de controlo sobre todos eles. O S-CSCF partilha com os outros elementos da rede que a ele se encontrem ligados, caso lho solicitem, as informações que obteve do UPSF.

A este elemento cabe também a função de decidir todas as rotas de encaminhamento de mensagens que têm como destino ou origem determinado UE que se encontre associado a esse S-CSCF.

2.4.2.1.4 Media Resource Function Controller (MRFC)

Este elemento faz parte de um conjunto de dois MRFs (*Media Resource Functions*) e encontra-se no plano da camada de serviço, situando-se e o outro, o MRFP, que será objecto de estudo mais adiante, na de transporte. Estes trabalham em conjunto e, de entre as suas funções, destaca-se o fornecimento de mecanismos para efectuar o tratamento do media que a rede recebe. Deve efectuar igualmente o controlo dos streams multimédia, como áudio e vídeo, possuindo recursos para a conversão de *codecs* ou a mistura de médias. Outras funcionalidades são a capacidade de cancelamento de eco e detecção e geração de DTMF (*Dual-tone multi-frequency*).

Um aspecto a ter em conta é que, em muitos serviços disponibilizados pelo operador, estes MRFs não são utilizados, isto porque é a própria aplicação que acarreta todo o tratamento de media.

2.4.2.1.5 Breakout Gateway Control Function (BGCF)

O BGCF é um elemento, cuja funcionalidade se enquadra no grupo de elementos que permitem a interoperabilidade do *core* com diferentes domínios, como por exemplo a rede de comutação de circuitos [35]. É utilizado quando surge a necessidade de efectuar uma chamada IMS que possui como destino um domínio diferente, ou em casos em que dois utilizadores da rede de comutação de circuitos pretendem tirar partido da rede IMS como intermediária. Pode, pois, ser encarado como sendo um SIP *server*.

Este elemento tem como função decidir se o pedido de ligação entre a rede de comutação de pacotes e a rede de comutação de circuitos se efectua via o MGCF da própria rede ou se é encaminhado para o BGCF de outra rede, sendo essa decisão baseada no número de telefone do destinatário. No caso em que a rede a ser utilizada é a própria o BGCF, têm também a tarefa de escolher qual a *gateway* PSTN que vai ser usada.

2.4.2.1.6 Media Gateway Control Function (MGCF)

A MGCF é vista como o nó central da gateway de *Trunking* e é escolhida pelo BGCF, tal como descrito no ponto anterior.

Analisando o subsistema IMS *core* e as entidades que o envolvem, constatamos que este elemento interage com elementos do próprio subsistema onde se encontra inserido e com a camada de transporte. De entre as suas funcionalidades pode-se referir a capacidade de converter o protocolo de sinalização SIP em ISUP (ISDN *User Part*) [38] ou em BICC (*Bearer Independent Call Control*). Normalmente, a conversão é efectuada para ISUP, uma vez que nas redes PSTN é o ISUP o protocolo utilizado dentro da sinalização SS7. Quando a comunicação com a SGW é feita em sentido contrário, este elemento converte a sinalização ISUP recebida em SIP e encaminha-a para o S-CSCF do *core* IMS.

Na camada de transporte, a MGCF encontra-se interligada com a T-MGW, podendo no que respeita a esta existir mais do que uma. A ligação entre estes dois elementos é efectuada através do protocolo MEGACO/H.248. Uma das funcionalidades de controlo da MGCF sobre a T-MGW consiste em escolher o *codec* adequado para o estabelecimento de uma sessão de voz e reservar canais de áudio. Outro aspecto a ter e ao qual a MGCF tem de ser sensível no seu controlo da T-MGW, é descartar a componente de vídeo, se a mesma se encontrar presente na sessão, e focar-se apenas na componente de áudio.

As principais diferenças entre os elementos do subsistema IMS core relativamente aos definidos pela 3GPP encontram-se documentadas na norma ETSI ES 282 007 [40].

Estas divergências funcionais foram já tidas em conta na *release* 7 do 3GPP, devido à forte colaboração que existe entre as duas entidades e no esforço de se apresentar uma solução comum para uma arquitectura NGN.

2.4.2.2 PSTN/ISDN Emulation Subsystem IMS based – PES

Este subsistema é fulcral no âmbito desta tese, pois é nele que se disponibiliza aos clientes da NGN a capacidade de emulação de serviços da rede PSTN/ISDN. Assim, por exemplo terminais analógicos, vulgarmente denominados de POTS (*Plain Old Telephone Service*) podem aceder à NGN de forma transparente.

Duas características são desejadas quando se fala em transparência: Do lado do cliente, pretende-se que este nunca se aperceba de que não se encontra ligado à habitual rede de comutação de circuitos; do lado da NGN, o terminal POTS deve ser encarado como um terminal comum. Ora, para que isso se possa verificar e para que todo o processo de emulação funcione de forma correcta, nasce a necessidade de criar *Media Gateways* específicas para este efeito e elementos que efectuem o seu controlo, surgindo o conceito de AGCF.

A figura 15 mostra a arquitectura de referência para o subsistema PES, baseado na arquitectura IMS (*PES IMS-based*), definido pelo TISPAN.

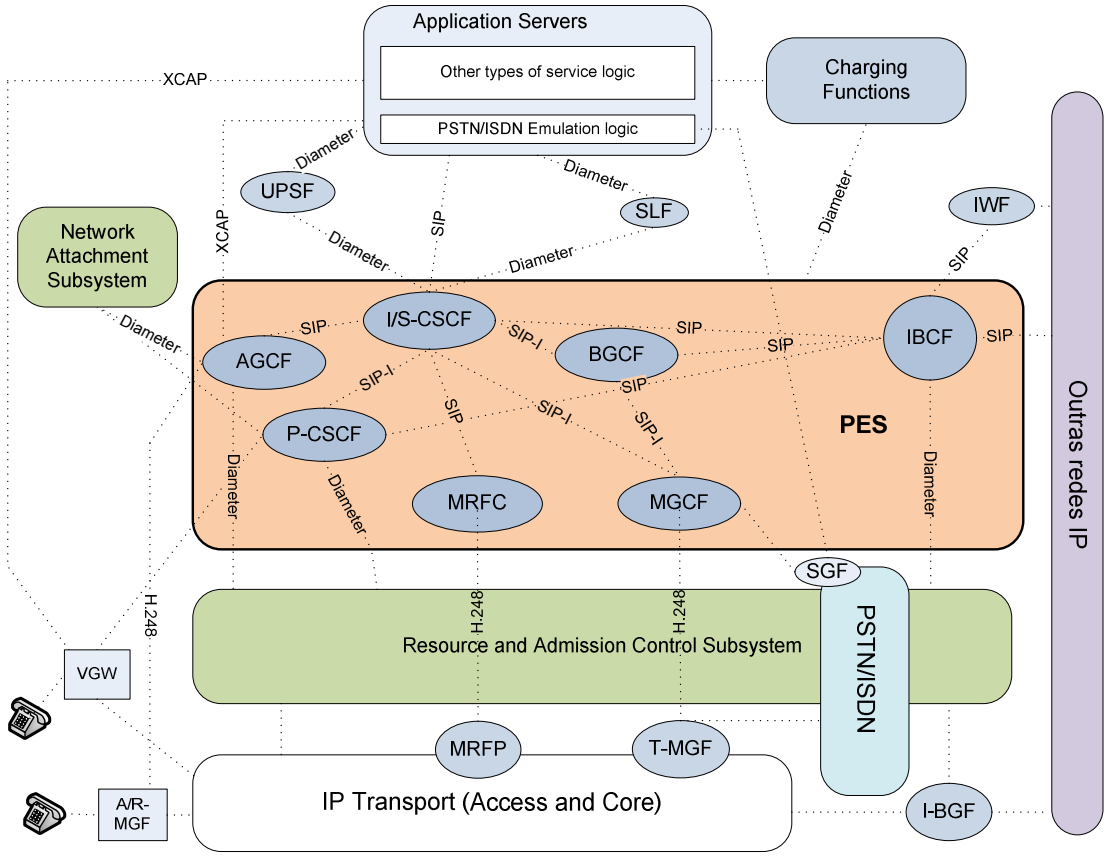


Figura 15 – Subsistema PES IMS *based* (adaptada de [26])

A arquitectura geral PES tira partido de elementos do *core* IMS definido pelo 3GPP, embora tenha acrescentado alguns ou alterado o nome de outros, mantendo, no entanto, de uma forma geral as suas funcionalidades, tendo em alguns casos havido o acréscimo de algumas. Na sua maioria, as diferenças mais significativas verificam-se não ao nível funcional, mas sim ao nível protocolar na interligação dos vários elementos.

De uma forma abrangente, os protocolos mantiveram-se, embora tenham sofrido alguns ajustes face às novas exigências. Por exemplo, ao protocolo MEGACO/H.248 foram acrescentados perfis para lidar com a ligação de controlo de A/R-MGF e T-MGF. Relativamente ao protocolo SIP, foi alvo de uma extensão, a SIP-I, definida na ITU-T *recommendation* Q.1912.5 [42], possibilitando o encapsulamento de sinalização ISDN *User Part* (ISUP) de uma forma directa na mensagem SIP [35].

Os elementos internos do PES que mantêm pelo menos as suas capacidades básicas definidas para o subsistema core IMS, são: P-CSCF, BGCF, I/S-CSCF e MRFC. Já o elemento MGCF sofreu um acréscimo, passando a possibilitar, quer o encapsulamento de sinalização proveniente da PSTN/ISDN, do tipo ISUP, numa mensagem SIP, quer, no sentido contrário, a extracção dessa informação das mensagens SIP-I e enviá-la para a rede PSN/ISDN via SGF.

Para que o trunfo deste subsistema, a emulação PSTN/ISDN, seja possível, são necessários elementos intermediários, através dos quais os POTS interagem com o *core* da NGN, denominados de *Media Gateways Functions* sendo neste caso específico aprofundadas a R-MGF,

a A-MGF e a VGW [69]. As diferenças entre estas prendem-se com aspectos como a sua localização na rede e com a capacidade de POTS suportada ou a forma como são consideradas pela rede. É de ter em conta que as mesmas não são tidas como elementos internos deste subsistema mas serão alvo, a seguir, de uma descrição mais detalhada, uma vez que são o elo de ligação para efeitos de emulação - em conjunto com a AGCF responsável pelo seu controlo - entre a rede PSTN/ISDN e o PES. Será também efectuada uma breve descrição do elemento, localizado fora do subsistema, designado de VGW.

2.4.2.2.1 Access Media Gateway Function (A-MGF)

A A-MGF caracteriza-se pelo facto de se encontrar localizada do lado do operador, cabendo-lhe as seguintes missões [43] na interligação dos terminais da rede PSTN/ISDN ao subsistema PES:

- Processamento de dados (voz, modem, etc.)
- Cancelamento de eco
- Passagem de anúncios e DTMF
- Conversão entre media RTP da rede IP e sinalização analógica dos POTS
- *Transcoding*, tirando partido de vários *codecs* de áudio
- Interacção com a AGCF, para efeitos de controlo de recursos

2.4.2.2.2 Residential Media Gateway Function (R-MGF)

Esta Media Gateway Function Residencial possui funcionalidades idênticas à A-MGF. No entanto, encontra-se localizada do lado do cliente e a sua capacidade de ligação de terminais é inferior. Para o *core* PES, esta *Gateway* é considerada como um simples equipamento baseado em IP do lado do cliente.

2.4.2.2.3 Voice Gateway (VGW)

Esta Gateway efectua a ligação de terminais, encontrando-se localizada do lado do operador. No entanto, ao contrário da A/R-MGF, não necessita de ser controlada por uma AGCF uma vez que é uma *Gateway* baseada em SIP sendo vista pelo resto da rede como um SIP User Agent estando ligada directamente ao P-CSCF da rede.

2.4.2.2.4 Access Gateway Control Function (AGCF)

Ora, de forma a efectuar toda a monitorização necessária da A-MGF ou R-MGF, vistas como um *slave* tal como descrito no início deste capítulo, surge a AGCF. Este elemento (*master*) é fulcral, possuindo todas as capacidades de controlo, e é de extrema importância no âmbito da parte prática desta tese. Uma análise exaustiva sobre este elemento será efectuada no Capítulo 3 onde, aspectos como as suas funcionalidades e blocos internos serão abordados.

2.4.2.2.5 Elementos comuns

Existem elementos definidos pelo TISPAN para a sua arquitectura de referência do subsistema PES baseado na arquitectura IMS, que são comuns a todos os subsistemas, isto é, são entidades com as quais todos os subsistemas da camada de serviço interagem. Uma breve descrição das mesmas é efectuada de seguida sendo as seguintes [44] :

- Server Local Function (SLF)
- User Profile Server Function (UPSF)
- Charging Functions
- Application Server Function (ASF)
- Interworking Function (IWF)
- Interconnection Border Control Function (IBCF)

2.4.2.2.5.1 Server Local Function (SLF)

É possível identificar dois tipos distintos de bases de dados na arquitectura TISPAN: a UPSF e a SLF. A última é apenas necessária quando existe mais do que um HSS. Tal acontece quando o operador possui muitos clientes e é necessário mais do que um UPSF ou se pretende evitar casos de redundância, isto é, quando um HSS falha existe outro de reserva. O SLF possui um registo dos HSS presentes na rede e, quando recebe um pedido de informações sobre determinado cliente, retorna o endereço do UPSF ao qual esse cliente se encontra associado. Esta informação é enviada, utilizando o protocolo Diameter, para os diferentes subsistemas da camada de serviço nomeadamente o I/S-CSCF e para os ASFs [45]

A arquitectura TISPAN pode não ter um SLF, se apenas tiver um UPSF, mas tem de ter sempre no mínimo uma base de dados UPSF.

2.4.2.2.5.2 User Profile Server Function (UPSF)

O UPSF incluiu-se numa família de elementos não definidos pelo 3GPP, tendo surgido por intermédio da arquitectura geral TISPAN. Este elemento é encarado como um grande arquivo de dados sendo que são vários os subsistemas que acedem a este elemento quando necessitam de consultar ou guardar dados relativos a determinado cliente específico. Por exemplo, alguma da informação contida no UPSF pode ser [26]:

- Localização do UE na rede
- Serviços subscritos aos quais o cliente possui permissão para utilizar
- Identificação do perfil de utilizador e respectivos dados associados
- Informações para efeitos de registo
- Qual o S-CSCF associado ao utilizador

De forma a ser possível garantir o acesso ao domínio de comutação de pacotes e da comutação de circuitos, existem ainda no HSS uma sub função HLR (*Home Location Register*) e AC (*Authentication Center*). Tal como no caso do SLF, é Diameter o protocolo escolhido para a comunicação com este elemento.

2.4.2.2.5.3 Charging Functions

Este componente da arquitectura é utilizado pelos diversos subsistemas com o intuito de efectuar registos de taxação, tendo em conta a actividade de determinado cliente na rede. A funcionalidade desta entidade não se encontra normalizada pelo TISPAN, ficando a cargo das pretensões de cada operador [45]. Como é de prever, diversos operadores possuem pretensões de taxação diferentes consoante o seu plano de actividade. Por exemplo um operador pode querer cobrar consoante o nível de QoS oferecido ou consoante o número de serviços disponibilizados aos seus clientes enquanto que outro pode pretender estabelecer um preço fixo. A forma como a taxação é efectuada pode ser em tempo real no acto da utilização do serviço ou posteriormente.

2.4.2.2.5.4 Application Server Function (ASF)

Na camada de serviço podemos encontrar servidores de aplicações (*Application Servers* - AS) que são responsáveis pelo alojamento e execução das aplicações colocadas à disposição dos clientes IMS dessa operadora. É então nesta camada que se encontram os tão desejados novos serviços multimédia que irão acrescentar valor ao IMS.

Um exemplo é o *Push To Talk* (PTT) que oferece aos utilizadores a possibilidade de um grupo se encontrar a comunicar segundo o conceito conhecido de *walkie talkie*. Tal poderá ter bastante impacto em certas áreas onde a comunicação rápida e prática de um conjunto de utilizadores é uma exigência. Ao utilizar o IMS, os operadores pretendem enriquecer ainda mais o conceito de PTT adicionando-lhe algumas funções multimédia extra. Do ponto de vista de utilização de recursos, ao contrário dos mecanismos tradicionais de voz, só são reservados canais quando existe conversação, e não durante toda a sessão, sendo esta uma das características das NGNs versus Sistema tradicional.

Nem sempre é necessário aceder a esta camada, mas apenas quando determinado cliente pretende aceder a um serviço específico que se encontra guardado nos servidores de aplicações. Por exemplo, para efectuar uma chamada de voz entre dois clientes da mesma operadora não é necessário comunicar com a camada de serviços. Do ponto dos elementos de controlo dos subsistemas da arquitectura TISPAN, os AS são tidos como iguais e podem encontrar-se na própria rede do utilizador ou encontrar-se noutra rede com a qual o operador possui um contracto para o estabelecimento desse serviço. A comunicação com esse serviço é sempre efectuada através da rede do operador do utilizador, mais especificamente através do S-CSCF. Os AS, além de possuírem interface com o S-CSCF, podem também tê-lo com o UPSF no caso de pertencerem à rede do operador onde se encontra, usando para isso o protocolo Diameter É de ter em conta que numa sessão multimédia, dependendo do serviço requisitado em causa, podemos ter mais do que um AS envolvido.

A arquitectura TISPAN apresenta uma divisão interna clara consoante o subsistema, IMS *core* ou PES, que acedem a este elemento.

Caso de o subsistema ser o *core* IMS, então o ASF comporta-se como um AS definido pela 3GPP e, de entre os AS disponibilizados para este subsistema na arquitectura IMS , pode ser por exemplo, um OSA-SCS ou um SIP-AS:

Os servidores OSA-SCS [46] permitem aos utilizadores acederem a serviços baseados na OSA [47]. Este servidor tem também como principal característica o facto de esconder, entre outros, o protocolo SIP das aplicações, conseguindo desta forma garantir segurança. Assim, AS externos à rede do operador podem fornecer os seus serviços multimédia, não pondo em causa a segurança interna da rede. O maior trunfo destes servidores é a segurança que a eles se encontra associada quando funcionam como intermediários entre duas redes distintas.

Estes encontram-se interligados ao S-CSCF através de uma interface SIP e opcionalmente podem possuir uma interligação com o UPSF através do protocolo Diameter com o objectivo de permitir que os mesmos tenham acesso a informações relativas a determinado cliente no que diz respeito a serviços subscritos.

Por sua vez, os SIP AS são considerados servidores nativos na arquitectura IMS. Estes permitem o armazenamento e execução de serviços multimédia IP, específicos para o IMS, baseados em SIP. São estes os servidores que vão albergar os tão esperados novos serviços associados ao *core* IMS. Existe uma interligação baseada em SIP com o S-CSCF e poderá também estar ligado ao HSS, tirando partido do protocolo Diameter para que informações como, por exemplo, quais os serviços contratados ao operador por determinado cliente possam ser consultadas pelo SIP AS.

No caso do subsistema em questão ser o PES, o TISPAN define que os serviços a serem emulados pelos clientes devem estar presentes num AS próprio para o efeito, o qual deve suportar SIP-I e ISUP. Outra característica neste caso é a sua interacção com o RACS em comparação com o subsistema IMS *core*. Assim, o TISPAN define dois tipos distintos de aplicações: as que necessitam de aceder aos subsistemas da camada de serviço e as que interagem directamente com o RACS embora a *Release* 1 aprofunde pouco estas últimas

A tabela 13 apresenta alguns dos serviços suplementares telefónicos suportados pela arquitectura TISPAN, podendo ser consultados na norma ETSI TS 181 002 [48].

Nº do serviço	Serviço	Nome
3	ACR	Anonymous Communication rejection
4	MICD	Malicious Communication Identification
5	ICB	Incoming Call Barring
9	CFB	Communication Forwarding on Busy
11	CFNL	Communication Forwarding on Not Logged In

Tabela 13 – Serviços telefónicos suplementares

2.4.2.2.5.5 Interworking Functions (IWF)

Esta entidade [49] possui funcionalidades de conversão entre os protocolos utilizados na sinalização dos subsistemas da camada de serviço, característicos das NGNs, e os de outras redes baseadas em IP como por exemplo H.323.

2.4.2.2.5.6 Interworking Border Control Function (IBCF)

A IBCF é responsável pela interligação dos diferentes subsistemas, ao nível da camada de serviço, definidos pelo TISPAN e outras NGNs ou entre os próprios subsistemas. Algumas das suas funcionalidades são [45]:

- Interagir com o RACS para controlo de recursos de transporte entre domínios distintos
- Encaminhamento de sinalização proveniente de outras redes IP
- Colocar o IWF na rota de envio quando diferentes protocolos de sinalização são utilizados entre dois domínios para estabelecimento de uma sessão

Podem existir várias IBCFs em determinada rede, sendo que o seu uso é opcional e depende das políticas de cada operador.

No caso do subsistema PES este elemento é parte integrante do mesmo algo que já não se verifica no subsistema IMS *core* o que se verifica através da figura 15 e 14 respectivamente.

2.4.2.3 Outros Subsistemas

Devido a uma arquitectura devidamente estruturada em camadas e subsistemas independentes, o TISPAN possibilita a introdução de novas capacidades à sua abordagem de NGN de forma facilitada. Assim, face às exigências dos clientes e operadores e à evolução tecnológica, esta arquitectura encontra-se preparada para suportar diferentes subsistemas.

Inicialmente a *Release* 1 apenas contemplava o subsistema *core* IMS e PES, sendo que entretanto na *Release* 2 novas propostas de subsistemas foram surgindo como por exemplo:

- **Streaming Subsystem**: este subsistema fornece capacidades de suporte para serviços de *streaming* de vídeo baseados no protocolo *Real-Time Streaming Protocol* (RTSP).

- **Content Broadcasting Subsystem**: serviços como o IPTV definido na norma ETSI TS 182 027 [37] são oferecidos aos clientes por este subsistema criado com o intuito de suportar *broadcasting* de conteúdos multimédia

Após uma abordagem mais específica das camadas e respectivos subsistemas, segue-se na figura 16 uma descrição mais detalhada da arquitectura TISPAN para as NGNs apresentada pela TISPAN RES 282 001 [26].

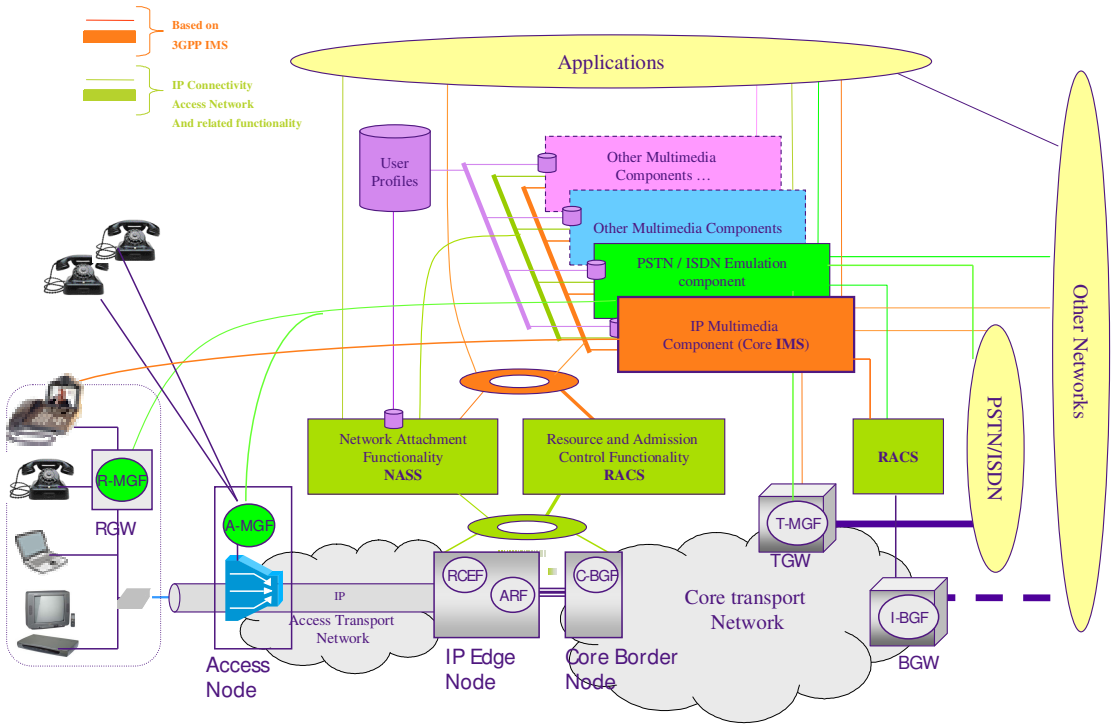


Figura 16 – Arquitectura global TISPAN detalhada (fonte: ETSI RES 282 001)

É visível a divisão em camadas e respectivos subsistemas associados bem como o elemento funcional A-MGF ou R-MGW a interagir com terminais analógicos e ligado ao subsistema PES IMS based.

Capítulo 3

Access Gateway Control Function (AGCF)

A AGCF é um elemento de controlo fulcral presente na arquitectura de referência para o subsistema PES, baseado na arquitectura IMS (PES IMS-based), definido pelo TISPAN.
Os elementos analógicos, de forma a poderem ser conectados ao *core* NGN, precisem de ser previamente ligados a *Gateways* intermédias específicas, usualmente designadas de A-MGFs ou R-MGFs. Estas são elementos passivos (*slave*) que necessitam de ser controlados por determinada entidade (*master*) que, neste caso específico da arquitectura PES, é denominado de AGCF.

A interligação com as *Gateways* é efectuada através do protocolo MEGACO/H.248, enquanto que para o core NGN é utilizado o protocolo SIP. É assim perceptível que a AGCF tem de possuir capacidade para lidar com estes dois protocolos

Esta entidade encontra-se do lado do operador na mesma localização que o P-CSCF, sendo parte integrante dos elementos pertencentes ao subsistema PES do TISPAN.

As funcionalidades gerais que este elemento deve respeitar, de forma a estar em conformidade com a norma ETSI TS 182 012 [50], são apresentadas no início deste Capítulo.

De seguida é efectuada uma dissecação da AGCF, apresentando-se todos os módulos internos e as suas características mais relevantes.

O trabalho prático desta tese é focado neste elemento, o qual deve vir a ser inserido num ambiente NGN específico. O *core* de testes onde deverá ser integrado denomina-se de *Service Handling on* IP *Networks* (*SHipNET*®), cujas características mais importantes e alguns dos seus elementos, nomeadamente a A-MGF e R-MGF da camada ip-*Keel*®, serão apresentados com algum detalhe.

Por fim, serão enumeradas todas as condições que devem ser respeitadas uma vez que, antes de se implementar a AGCF, é necessário efectuar um estudo dos requisitos a serem satisfeitos nas mais diversas áreas, aspectos funcionais, de redundância e ambientais, por exemplo, serão igualmente expostos.

3.1 Funcionalidades

Diversas são as funcionalidades que o elemento AGCF deve ser capaz de suportar para fazer face ao complexo processo de emulação disponibilizado aos clientes pelo subsistema PES da camada de serviço da arquitectura TISPAN.

Este é o primeiro ponto de contacto para as *Media Gateways* no *core* PES. sendo que esta interacção é efectuada utilizando o protocolo MEGACO/H.248, o mesmo que é usado para comunicar com o NASS e RACS. A ligação com o I/S-CSCF processa-se através do protocolo SIP. Para o controlo da execução de serviços suplementares, abordados no Capítulo 2, a AGCF possui uma ligação ao AS baseada no protocolo *Extensible Markup Language* (XML) *Configuration Access Protocol* (XPCAP) [51]. Estas interligações encontram-se ilustradas na figura 17.

Segundo a norma TISPAN TS 182 012 [50], as funcionalidades gerais que a AGCF deve disponibilizar são:

• Interagir com o subsistema RACS, com o intuito de efectuar o controlo de recursos associados ao transporte de informação multimédia. Um controlo de QoS é também efectuado através desta interacção;

• Interagir com o subsistema NASS, de forma a autenticar e registar os UE dos clientes que se encontram ligados às A-MGF ou R-MGF;

• Actuar sobre as A/R-MGFs para efectuar o controlo de recursos de estabelecimento de sessões (*codecs*, etc.);

• Enviar *dialplans* e *dialtones* para as *Media Gateways*;

• Relativamente às restantes entidades funcionais da arquitectura PES a AGCF, deve actuar como um SIP *User Agent*;

• Efectuar o mapeamento entre o protocolo SIP, aquando da comunicação com I/S-CSCF, e o protocolo MEGACO/H.248 utilizado na comunicação com as *Media Gateways*;

• Do ponto de vista do IMS a AGCF, é encarada como um P-CSCF, pelo que deve efectuar os mesmos procedimentos associados a esta entidade, como é o caso do envio de registos (SIP *Registers*) dos POTS para o core IMS;

• Efectuar o processamento de chamadas e todo um conjunto de funções associadas como, por exemplo, a análise dos dígitos telefónicos ou a selecção de circuito de acordo com o POTS destino;

• Suporte de *Calling Line Identification Presentation* (CLIP), *Calling Line Identification Restriction* (CLIR) e suporte para encaminhamento de chamadas de emergência.

3.2 Estrutura Interna

Diversas são as capacidades disponibilizadas pela AGCF através de um correcto funcionamento e interligação das entidades contidas na sua arquitectura. A estrutura interna pode ser dividida em diversos blocos os quais comunicam entre si, embora do ponto de vista funcional sejam independentes e possuam características bem definidas.

A figura 17 apresenta a arquitectura interna baseada na norma ETSI TS 183 043 [52].

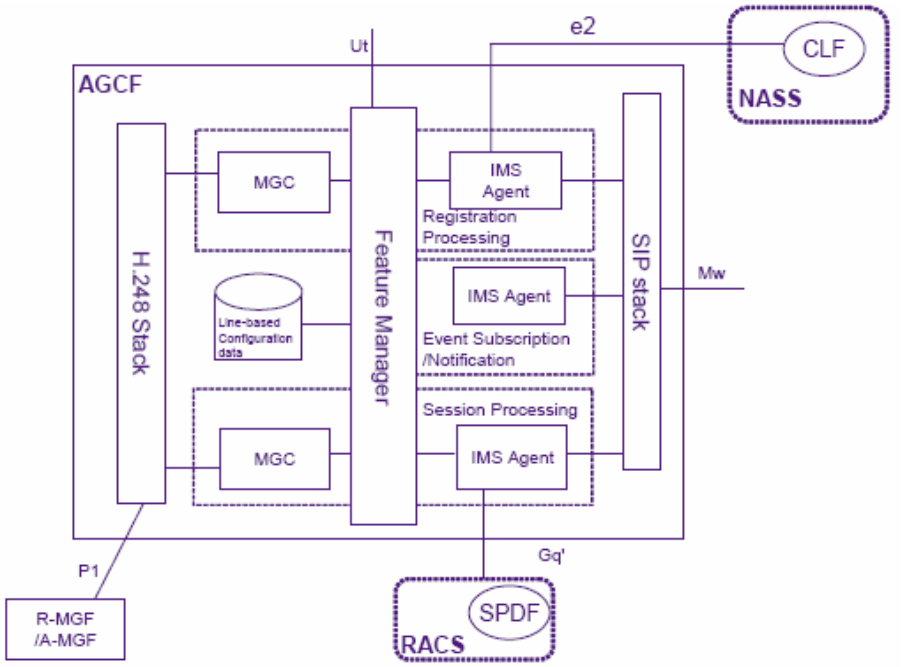


Figura 17 – Arquitectura interna AGCF

Tal como ilustrado, a arquitectura interna da AGCF pode ser dividida em três módulos lógicos:

- Media Gateway Controller (MGC)
- Feature Manager (FM)
- IP Multimedia Subsystem Agent (IMS Agent)

Além dos módulos lógicos, a arquitectura interna da AGCF apresenta ainda duas *stacks* protocolares para SIP e MEGACO/H.248 e uma entidade de armazenamento de informação denominada por *Line based Configuration data* (LBCD).

Cada módulo, embora encarado como um todo, encontra-se desdobrado em três subsistemas: *Registration Processing*, *Event Subscription/Notification* e *Session Processing*. Isso deve-se ao facto de as várias funcionalidades disponibilizadas pela AGCF requererem diferentes capacidades de cada módulo. Por exemplo, o MGC encontra-se presente em 2 subsistemas consoante a tarefa a ser desempenhada. De uma forma resumida o subsistema *Registration*

Processing encontra-se encarregado, tal como o nome indica, de todo o processo de registo/desregisto de terminais. O *Event Subscription Notification* possui funcionalidades de aviso para determinados eventos a serem tratados. Por fim, ao subsistema *Session Processing* encontra-se associada a capacidade de lidar com o processo de estabelecimento e monitorização de chamadas.

A tabela 14, tendo em conta a figura 17, apresenta uma correspondência entre o nome da interligação, as entidades envolvidas e o protocolo associado para as ligações externas entre os módulos, internos da AGCF e os elementos da arquitectura geral PES IMS *based*.

Nome	Elementos interligados	Protocolo
Ut	Ponto de referência entre o FM e o Application Server	XCAP
e2	Ligação entre IMS Agent e o NASS	Diameter
Mw	Ponto de referência entre SIP stack o I/S-CSCF	SIP
Gq'	Ligação entre IMS Agent e RACS	Diameter
P1	Ponto de referência entre MGC e A/R-MGW	H.248/MEGACO

Tabela 14 – Ligações externas da AGCF

De seguida é efectuada uma descrição de cada um dos módulos tendo em conta as funcionalidades que devem suportar.

3.2.1 Media Gateway Controller (MGC)

Este módulo é encarado como a porta de entrada para a conectividade da A/R-MGF, bem como dos respectivos POTS a ela ligados, com a AGCF. O protocolo utilizado nesta interligação é o MEGACO/H.248 [41] e, para tal, a arquitectura interna da AGCF possui uma Stack H.248. Esta, dependendo do fabricante, possui diversas funções que facilitam o envio e a escuta de mensagens enviadas ou recebidas respectivamente.

A MGC encontra-se presente em dois subsistemas, o de Registo e o de Estabelecimento de Sessão, e possuindo as seguintes funcionalidades de controlo sobre as A/R-MGFs [43]:

• Controlo de *Dial Tones* e anúncios na A-MGF/R-MGF

• Tratamento de comandos H.248 *ServiceChange* enviados pela A-MGF/R-MGF para efeitos de registo ou desregisto de terminais

• Envio de *Dial Plans* para a A-MGF

• Análise dos dígitos DTMFs enviados pela A-MGF ou R-MGF com o intuito de detectar chamadas de emergência.

• Processamento de comandos H.248 *Audit*, possibilitando a manutenção permanente do estado dos POTS pela AGCF

• Informar a A/R-MGF, através de comandos H.248 *Notify*, para o envio de eventos telefónicos e dígitos DTMF

• Recepção e processamento de eventos telefónicos e dígitos DTMF da A-MGF/R-MGF

3.2.2 Feature Manager (FM)

Este módulo pode ser considerado o "cérebro" da AGCF pois, de uma forma geral todas as decisões tomadas passam pelo FM. Encontra-se interligado com o MGC e, com o IMS Agent, efectuando a sua coordenação. A ponte que se cria através desta entidade deve ser encarada também do ponto de vista protocolar uma vez que lida com dois protocolos distintos: MEGACO, do lado da MGC, e SIP, do lado do IMS *Agent*.

De entre os três módulos que constituem a arquitectura interna da AGCF, este é o único que pode aceder ao LBCD para consultar ou guardar informações.

As funcionalidades suportadas pelo FM [43] são as seguintes:

• Sinaliza o módulo SIP *User Agent* para o envio de registos individuais ou em grupos dos terminais POTS para o core IMS

• Interage com o AS para obter informações (dial tone, etc.) dos utilizadores em causa

• Processa registos e sessões de acordo com a informação de estado da A-MGF/R-MGF e respectivos POTS

3.2.3 IP Multimédia Subsystem (IMS Agent)

O IMS Agent é, tal como o MGC, uma porta de entrada para a AGCF, mas agora do lado do *core*, enviando e recebendo primitivas deste. O protocolo utilizado nesta ligação é o SIP, tirando-se partido da SIP *stack* presente na arquitectura. Este módulo efectua os mesmos procedimentos que estão associados ao conjunto dos elementos P-CSCF, abordado no Capítulo 2 e IMS UE, cujas funcionalidades se encontram especificadas na norma 3GPP TS 23.228 [36].

De certa forma, este elemento apenas serve de porta de entrada e de saída de mensagens SIP, sendo as suas decisões tomadas pelo FM.

3.2.4 Line based Configuration data (LBCD)

Esta entidade pode ser encarada como um armazém de informações sobre as A/R-MGF e respectivos POTS que se encontram sob o controlo de determinada AGCF. A informação guardada pode ser de diferentes tipos, tais como:

• Estado actual de cada POTS, isto é, informações sobre se determinado terminal se encontra por exemplo ocupado, desligado, disponível ou on/off-hook.

• Interage com o *Application Server* para obter informações (*dial tone*, etc.) dos utilizadores em causa

• Possui informação relativa à identificação pública e privada de cada utilizador

3.2.5 Stacks protocolares

São duas as stacks apresentadas na arquitectura interna da AGCF. A presença da *stack* MEGACO e da SIP possui o mesmo pressuposto: facilitar o manuseamento destes protocolos.

No Capítulo 2 estes foram detalhados e, embora se tente que sejam o mais simples possível de compreender e lidar, nem sempre são de fácil e rápida implementação.

Para tornar os protocolos mais acessíveis, as *stacks* possuem funções pré-definidas que podem ser utilizadas, o que facilita e acelera todo o processo que envolva a utilização de determinado protocolo.

Os procedimentos detalhados para cada módulo da AGCF, tendo em conta o subsistema onde se encontram e a funcionalidade a ser disponibilizada, podem ser consultados ainda com mais pormenor na norma ETSI TS 183 043 [52].

3.3 Service Handling on IP Networks (SHipNET®)

No âmbito desta tese, pretende-se que a AGCF a ser implementada seja inserida num demonstrador de *core* NGN específico, denominado de *SHipNET*®. O objectivo deste *core* de testes é criar uma NGN que possibilite a conexão às redes tradicionais e de nova geração [53]. O SHipNET® encontra-se dividido em três camadas distintas, o que é característico de uma arquitectura horizontal, apresentando bastantes benefícios, relativamente às tradicionais arquitecturas verticais. Respeitando as camadas utilizadas nas NGNs, esta arquitectura apresenta os seguintes níveis:

• Nível de Aplicações e Serviços
• Nível de Controlo de Sessão e de Transporte
• Nível de Transporte

Em cada camada, ou partilhados entre elas, surgem diversos grupos bem delimitados, tendo em conta os elementos que os constituem e a sua função.

A figura 18 ilustra a arquitectura global deste demonstrador onde se identificam os seguintes grupos: ip-*Sail*®, ip-*Jib*®, ip-*Cockpit*®, ip-*Deck*®, ip-*Rudder*®, ip-*Tiller*®, ip-*Windless*®, ip-*Keel*®. A escolha destes nomes deve-se à analogia que foi estabelecida com um veleiro.

De uma forma sucinta, apresenta-se a seguir a função de cada um dos grupos inseridos nos respectivos níveis.

• Nível de Aplicações e Serviços

•ip-*Sail*®: possui funcionalidades para efectuar taxação em tempo real dos serviços disponibilizados

•ip-*Jib*®: é uma plataforma SIP *Application Server* que disponibiliza ambiente de execução de um conjunto alargado de serviços

• Nível de Controlo de Sessão e de Transporte

•ip-*Cockpit*®: efectua o armazenamento de informação relativa aos clientes do *core*. Possui os elementos HSS e SLF de acordo com o standard 3GPP Rel.6

•ip-*Deck*®: possui funcionalidades de controlo de sessões multimédia, implementando os três elementos: P-CSCF, S-CSCF e I-CSC

•ip-Windless®: possui as mesmas funcionalidades que o MRF da arquitectura IMS, englobando o MRFC e MRFP com capacidades de *media/dialog server*

•ip-*Rudderk*®: é responsável pela autorização dos pedidos de serviço e controlo da qualidade de serviço (QoS). Engloba as entidades internas do RACS.

•ip-*Tiller*®: possui as mesmas funcionalidades do elemento NASS da arquitectura global TISPAN.

• Nível de Transporte

•ip-*Keel*®: possibilita o inter funcionamento do *core* NGN com as redes denominadas de tradicionais.

De acordo com a divisão efectuada na arquitectura deste demonstrador e a sua analogia com um veleiro, a AGCF encontra-se na quilha do veleiro, e está inserida no grupo ip-*Keel*®. Este será objecto de uma descrição, na qual será dada especial ênfase à A-MGF e R-MGF, uma vez que são elementos com os quais a AGCF interage.

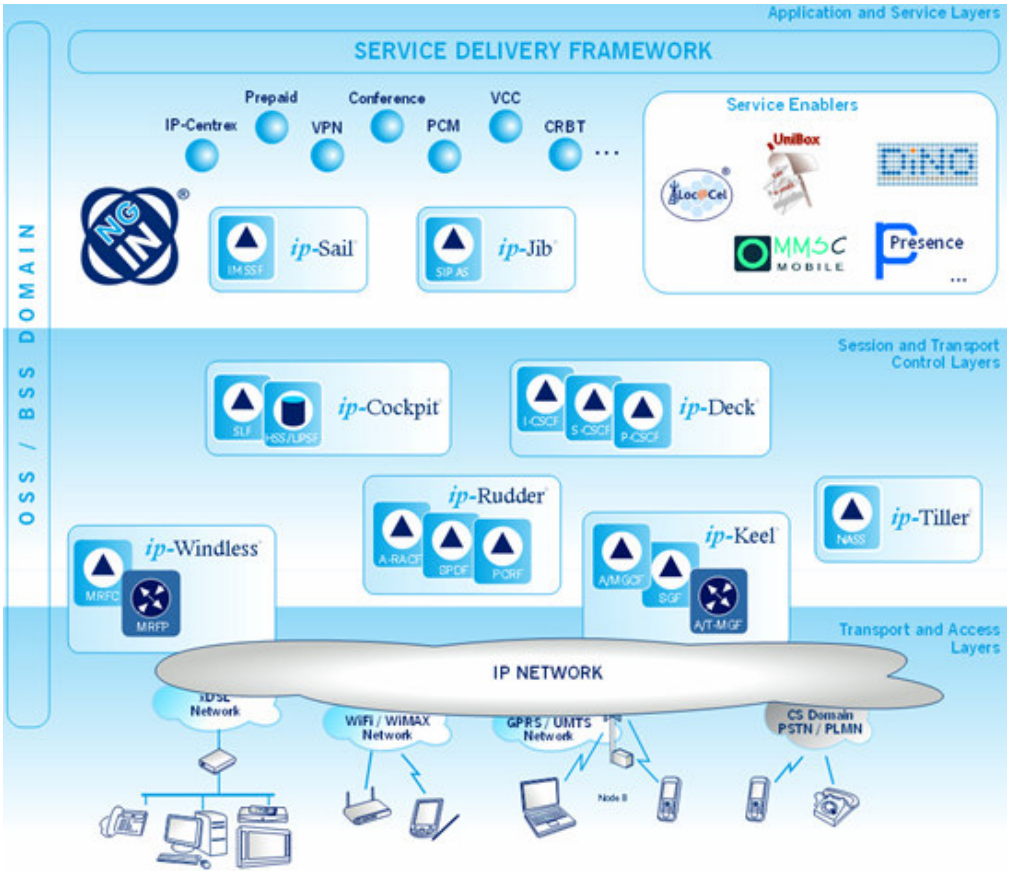


Figura 18 – Demonstrador SHipNET®

3.3.1 IP-Keel®

Este grupo do nível de transporte caracteriza-se por permitir a ligação do *core* com as redes tradicionais, fornecendo para tal dois mecanismos distintos de interligação:

•**Trunking**: interfuncionamento com outro tipo de redes (*Trunking-MGW*), quer do tipo *circuit switched* (ex.:PSTN/ISDN), quer do tipo *packet switched* (ex.:Internet)

•**Acesso**/**Residencial**: interfuncionamento directo com os terminais POTS dos clientes do *core* (Access-MGW/Residential-MGW)

Neste último mecanismo oferecido pelo SHipNET® que possibilita a emulação de serviços PSTN/ISDN aos clientes do *core*. Assim, de seguida será efectuada uma descrição dos elementos A-MGF e R-MGF a serem inseridos no ip-*Keel*® uma vez que a função base da AGCF é efectuar o controlo dos mesmos.

3.3.1.1 Access Media Gateway Function (A-MGF)

Este módulo localizado do lado do operador encontra-se de momento em fase de construção e irá ser baseado em elementos discretos da arquitectura apresentada pela AudioCodes® [54]. A base proposta para esta solução assenta nos seguintes módulos ilustrados na figura 19:

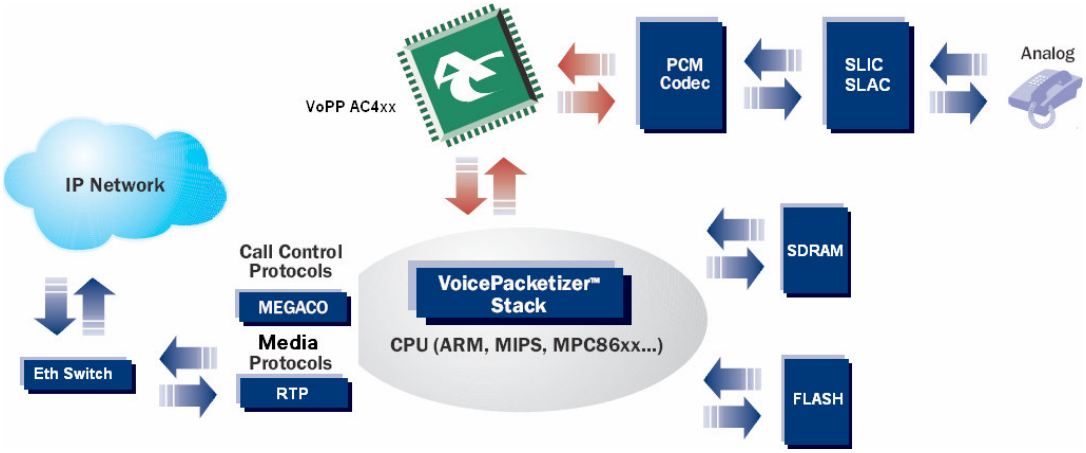


Figura 19 – Arquitectura interna de uma A-MGF

Um dos módulos mais importantes nesta arquitectura é o DSP (*Digital Signal Processor*), o qual se encontra descrito como VoPP AC4xx que possui diferentes características consoante o tipo de *Media Gateway* a ser implementada, por exemplo aspectos que se relacionem com o número de canais suportados podem variar [43]. Algumas das funcionalidades deste elemento, que se encontram de acordo com o descrito no Capítulo 2 para as funções a serem suportadas para a A-MGF, são:

- Cancelamento de eco
- Geração e detecção de DTMFs (*in-band signalling* e *out-of-band signalling*)
- Processamento de dados de sessões de voz, de Modem e FAX (T.38)
- Codificação e descodificação de áudio, tirando partido de vários *codecs*

A *stack* VoicePacketizer™ efectua a interligação entre o VoPP e o software que se encontra no CPU, tirando partido de uma biblioteca em linguagem C. Para o caso da A-MGW o protocolo de controlo suportado é o MEGACO/H.248, tal como seria de esperar, respeitando a arquitectura TISPAN.

De entre as tarefas desempenhadas pelo CPU, destacam-se o processamento dos comandos de controlo e processamento dos dados media, as quais podem ser efectuadas paralelamente, isto é, o processador pode estar a atender um comando MEGACO de pedido de estabelecimento de chamada e ao mesmo tempo estar a processar os dados media entre o DSP e o interface da rede.

A junção de vários DSPs, com o VoicePacketizer™ e um CPU, formam módulos VoP PMC que podem ser combinados com interfaces telefónicas formando *boards* PCI/cPCI de *Media Gateways* que, utilizadas em conjunto, o que permite a ligação de um elevado número de terminais.

As suas funcionalidades estarão de acordo com o descrito no Capítulo 2 e cumprirão os requisitos a que os fabricantes devem obedecer, apresentados na norma ETSI 282 002 [69].

3.3.1.2 Residential Media Gateway Function (R-MGF)

A R-MGF não é parte integrante do *core* definido pelo TISPAN, logo também não o é no demonstrador SHipNET®, nem se encontra do lado do operador, mas sim do lado do cliente. No entanto, a AGCF deve possuir capacidades para suportar este tipo de *Residential Gateway*. Este elemento suporta um menor número de terminais e será utilizado exclusivamente com fins residenciais e empresariais. A sua arquitectura será idêntica à descrita para a A-MGF no ponto anterior.

3.4 Requisitos

Antes de se iniciar a implementação da AGCF é necessário proceder a um estudo prévio dos requisitos a serem disponibilizados pela mesma. Esta pesquisa abrange as normas definidas para este elemento, a serem respeitadas, e as características do *core* SHipNET onde aquele será introduzido. Futuramente, após a sua inserção no demonstrador, este protótipo deverá evoluir para um produto comercial.

Inicialmente, são identificados os requisitos funcionais relacionados com os módulos internos e *stacks* protocolares que servem de base ao funcionamento desta entidade.

De seguida, são indicados os requisitos de interface de utilizador, isto é, os requisitos do sistema para a interacção com o utilizador, como os modos e parâmetros de configuração do sistema. São enunciados, também, os requisitos de interface da AGCF com os sistemas externos, incluindo as interfaces físicas, os protocolos utilizados nestas interfaces e mecanismos de QoS.

As exigências a serem cumpridas necessárias à instalação do software da AGCF e da plataforma física de suporte são também abordadas neste subcapítulo bem como a sua dependência das *stack*s SIP e MEGACO escolhidas para o seu desenvolvimento.

Para efeitos de demonstração em pilotos são também indicados os requisitos exigidos para a interligação da AGCF no demonstrador SHipNET® e, eventualmente, poderão ser referidos outros requisitos de interligação caso a AGCF seja introduzida noutros cenários.

Esta parte é seguida por uma identificação de exigências de implementação comuns relacionados com a Gestão da AGCF, por exemplo Geração de Alarmes ou Geração de Estatísticas.

Por último são enumerados os requisitos de desempenho e segurança que a AGCF deve respeitar.

Deve ser tido em conta que aspectos mais detalhados sobre alguns requisitos serão especificados aquando da implementação da AGCF no Capítulo 4. Tal explica-se porque consoante o módulo interno a ser desenvolvido e respectivas funcionalidades associadas existem requisitos específicos que devem ser cumpridos.

Toda esta informação será apresentada sobre a forma de uma tabela dividida por tipos de requisitos, indicando a sua prioridade de implementação e respectivas dependências.

3.4.1 Requisitos Funcionais

Nesta parte do presente documento são identificados os requisitos funcionais da AGCF de uma forma mais técnica, relacionados com as suas características técnicas, módulos internos e funcionalidades, de acordo os organismos de normalização.

- **Módulos**

A AGCF pode ser dividida internamente em três módulos lógicos funcionais: IMS Agent, Feature Manager e Media Gateway Controller e ainda as suas stacks protocolares de comunicação e a *Line based Configuration data*.

Código	Descrição	Prior.	Dependências
RF.AGCF-MDL.1	IMS Agent	1	RF.AGCF-MDL.4
RF.AGCF-MDL.2	Feature Manager	1	RI.AGCF-INST.1 RF.AGCF-MDL.1 RF.AGCF-MDL.3 RF.AGCF-MDL.6
RF.AGCF-MDL.3	MGC	1	RF.AGCF-MDL.5
RF.AGCF-MDL.4	Stack SIP	1	-
RF.AGCF-MDL.5	Stack H.248/Megaco	2	-
RF.AGCF-MDL.6	Base de dados	1	-

RF.AGCF-MDL.1: O módulo IMS Agent integra a estrutura interna da AGCF especificada na norma ETSI TS 182 012 [50], que, de uma forma geral, implementa os mesmos procedimentos associados aos elementos P-CSCF e IMS UE do IMS da 3GPP definidos na norma TISPAN ES 283 003 [55]. Este deve encontrar-se permanentemente em escuta de mensagens SIP, do lado do core, e de primitivas provenientes do FM tendo ainda de possuir capacidades para lidar com os processos associados aos diferentes tipos de pedidos que a AGCF deve suportar como por exemplo registo/desregisto. Deve possuir capacidades de distinguir os diferentes tipos de pedidos e respectivas informações associadas provenientes do FM tirando depois partido da stack interna de forma construir mensagens SIP que serão enviadas para o core.

RF.AGCF-MDL.2: O módulo *Feature Manager* é o bloco funcional da AGCF especificada na norma ETSI TS 182 012 [50] responsável pela coordenação entre o *core* IMS e as *Media Gateways* com funcionalidades diversas, como a interacção com o AS, de forma a obter informações (*dial tone*, etc.) dos utilizadores, e processamento das sessões de acordo com a informação do estado da A-MGW ou R-MGW e respectivos POTS ligados às mesmas. Desta forma, numa perspectiva interna da AGCF, é o módulo que coordena o funcionamento dos restantes módulos. Este deve assim possuir mecanismos de interacção com o MGC e IMS Agent, capacidade de reconhecimento dos diferentes pedidos e será responsável por testar a credibilidade das informações provenientes do MGC. Requisitos funcionais aprofundados para este módulo encontram-se nas normas ETSI TS 182 012 [50] e TS 183 043 [52].

RF.AGCF-MDL.3: O módulo *Media Gateway Controller* (MGC), inserido na estrutura interna da AGCF especificada na norma ETSI TS 182 012 [50], é, de uma forma geral, responsável pelo controlo da A-MGW ou R-MGW, integrando funcionalidades como monitorização do estado e controle de configuração da ligação. Este de um lado deve encontrar-se em escuta de mensagens MEGACO, tirando partido da stack interna que lhe possibilitará interpretar e construir as mensagens recebidas/enviadas, e por outro deve possuir funcionalidades de comunicação com o módulo FM com o intuito de lhe enviar ou receber primitivas com campos específicos consoante o a acção pretendida a satisfazer. Requisitos funcionais mas aprofundados para este módulo encontram-se nas normas ETSI TS 182 012 [50] e TS 183 043 [52].

RF.AGCF-MDL.4: Stack SIP com funções especificas (API) para a implementação de mensagens SIP de comunicação com elementos externos. A *stack* escolhida deve respeitar as capacidades indicados no RFC 3261 [7] e na norma TISPAN ES 283 003 [55]. Esta possui diversas funções que facilitam a construção e interpretação de pedidos e respostas SIP entre o IMs Agent e o core da rede em questão.

RF.AGCF-MDL.5: Stack H.248/MEGACO com funções especificas (API) para a implementação de comandos de controlo dos elementos A/R-MGW. Os requisitos para esta *stack* estão indicados no ITU-T *Recommendation* H.248 [56] e na norma ETSI ES 283 002 [41] cujos benefícios são iguais aos referidos anteriormente.

RF.AGCF-MDL.6:Implementação de uma base de dados com vários campos contendo diversas informações relativas aos POTS e respectivos clientes associados que se encontram ligados a determinada A-MGW controlada pela AGCF. O ponto RIU.AGCF-CFG.1 específica mais detalhadamente este requisito.

• Requisitos de Interface de Utilizador

Todos os requisitos do ponto de vista da interacção com o utilizador a serem respeitados encontram-se de seguida descritos.

Configuração (CFG)

Código	Descrição	Prior.	Dependências
RIU.AGCF-CFG.1	Parâmetros de configuração da AGCF	1	-
RIU.AGCF-CFG.2	Métodos de configuração da AGCF	1	-
RIU.AGCF-CFG.3	Configuração dos parâmetros da AGCF para o demonstrador SHipNET	2	RIU.AGCF-CFG.1 RIU.AGCF-CFG.2

RIU.AGCF-CFG.1: Diversos são os parâmetros a serem introduzidos na base de dados interna (LBCD) da AGCF aquando o seu arranque inicial de forma a que esta possua diversas informações essenciais ao seu funcionamento nomeadamente características das A-MGWs e respectivos clientes (POTS). Estas informações poderão vir a sofrer acréscimos e/ou alterações à medida que se procede a implementação das diversas funcionalidades a serem disponibilizadas pela AGCF.

RIU.AGCF-CFG.2: Deve ser possível aceder aos dados contidos na LBCD com o intuito de inserir/retirar informações dos clientes de forma a manter actualizados todos os dados associados a cada cliente. Assim, a AGCF deve ser encarada não como um módulo isolado no qual a informação necessita de ser inserida exclusivamente uma única vez mas sim que é necessário que esta se encontre permanentemente actualizada. O método possível de interagir com a LBCD por parte do operador deverá ser o mais simples e fiável possível não pondo nunca em causa o correcto e permanente funcionamento da AGCF aquando uma necessidade de actualização dos seus dados internos.

RIUAGCF-CFG.3: O módulo AGCF deverá ser inserido no demonstrador SHipNET com o intuito de ser parte integrante do *core* de uma NGN. Assim, poderão surgir alguns parâmetros específicos que necessitaram de ser tidos em conta de acordo com os requisitos a serem cumpridos pelos elementos constituintes do demonstrador SHipNET. Estes, à medida que o módulo A-MGW e AGCF são desenvolvidos, serão especificados no documento “A-MGW_concepção_v1.0” [57] e “AGCF_concepção_v1.0” [58] respectivamente.

• Requisitos de Interface com Sistemas Externos

A AGCF não pode ser idealizada como um sistema isolado tendo necessidade de possuir interfaces físicas com sistemas externos, as quais são descritas de seguida.

Interfaces físicas (IF)

Código	Descrição	Prior.	Dependências
RISE.AGCF-IF.1	Suporte de interface Ethernet	1	RI.AGCF-INST.1
RISE.AGCF-IF.2	Outras	5	-

RISE.AGCF-IF.1: Para suporte de ligação à rede *core* baseada em Eth que será assegurada pela plataforma PC/servidor de 19" Linux.

RISE.AGCF-IF.2: Todas as interfaces externas da *Access Media Gateway Function* (AGCF) são asseguradas pelas interfaces da plataforma e servirão de base para o funcionamento deste elemento. Como tal, qualquer interface externa que possa vir a ser requerida estará dependente e será assegurada pela plataforma física.

Protocolos (PR)

Código	Descrição	Prior.	Dependências
RISE.AGCF-PR.1	Suporte de protocolos de sinalização para efeitos de controlo de A-MGWs	2	RF.AGCF-MDL.3 RF.AGCF-MDL.5
RISE.AGCF-PR.2	Suporte de protocolos de comunicação com o elemento I/S-CSCF	1	RF.AGCF-MDL.1 RF.AGCF-MDL.4
RISE.AGCF-PR.3	Suporte de protocolos de comunicação com o elemento RACS	3	RF.AGCF-MDL.1
RISE.AGCF-PR.4	Suporte de protocolos de comunicação com o elemento NASS	3	RF.AGCF-MDL.1
RISE.AGCF-PR.5	Suporte de protocolos de comunicação com o elemento AS	4	RF.AGCF-MDL.2
RISE.AGCF-PR.6	Suporte de protocolos de comunicação com o elemento IBCF	3	RF.AGCF-MDL.1
RISE.AGCF-PR.7	Suporte de protocolos de encaminhamento ao longo da rede IP	4	-
RISE.AGCF-PR.8	Suporte de protocolos de transporte IP	1	-
RISE.AGCF-PR.9	Suporte de integração de novos protocolos	5	-

RISE.AGCF-PR.1: Para comunicação com a A/R-MGW através de protocolo MEGACO/H.248 especificado na norma ETSI ES 283 002 [41]. Interface P1 da arquitectura PES IMS based da norma ETSI TS 182 012 [50].

RISE.AGCF-PR.2: Possibilita a comunicação e o encaminhamento de mensagens de sinalização entre a AGCF e o módulo I/S–CSCF utilizando o protocolo SIP especificado na norma ETSI ES 283 003 [55]. Interface Mw da arquitectura PES IMS based da norma ETSI TS 182 012 [50].

RISE.AGCF-PR.3: Permite a interacção da AGCF com o RACS, através do protocolo DIAMETER de forma a possibilitar funcionalidades como a autorização de recursos com Qualidade de serviço (QoS). Interface Gq' da arquitectura PES IMS based da norma ETSI TS 182 012 [50].

RISE.AGCF-PR.4: Permite a interacção da AGCF com o NASS que é responsável, entre outras funcionalidades, pela informação relativa ao perfil do cliente para o acesso aos recursos da rede de transporte. Protocolo DIAMETER especificado na norma ETSI ES 283 035 [59] correspondendo à interface e2 da arquitectura PES IMS based da norma ETSI TS 182 012 [50].

RISE.AGCF-PR.5: Responsável pela ligação da AGCF com o módulo *Application Server* (AS) para funcionalidades de acordo com os serviços pretendidos através do Protocolo HTTP. Interface Ut da arquitectura PES IMS based da norma ETSI TS 182 012 [50].

RISE.AGCF-PR.6: Responsável pela ligação da AGCF com o módulo *Interconnect Border Control Function* (IBCF) tirando partido do protocolo SIP detalhado na norma ETSI ES 283 003 [55]. Interface Mx da arquitectura PES IMS *based* da norma ETSI TS 182 012 [50].

RISE.AGCF-PR.7: Capacidade de suporte dos protocolos OSPF, BGP, ou extensões associadas, de forma a suportar MPLS. O uso de *labels* MPLS tem algumas vantagens, nomeadamente ao nível do suporte multi-serviço, da baixa latência, do reencaminhamento de pacotes IP, da simplicidade na gestão, e do suporte de elevado QoS ainda não disponibilizado actualmente pelo IP. Neste cenário, a *Media Gateway* deve suportar LSR, i.e. , *Label Switch Routing*, como função da norma MPLS.

RISE.AGCF-PR.8: São utilizados protocolos da camada de transporte onde assentam os protocolos SIP, MEGACO/H.248, DIAMETER e HTTP utilizados pela AGCF para comunicação com os módulos da arquitectura PES IMS based da norma ETSI TS 182 012 [50]. Assim sendo, e tendo em conta o modelo geral de Camadas OSI, os protocolos são: SIP que assenta em TCP, UDP;, MEGACO/H.248 que assenta em TCP, UDP, SCTP ; DIAMETER que assenta em TCP, SCTP ; e HTTP assenta em TCP.

RISE.AGCF-PR.9: Funcionalidades futuras da AGCF poderão requerer a capacidade de integração modular de novos protocolos. Como tal, deve-se prever e evitar situações associadas a incompatibilidade e fomentar a coexistência.

Mecanismos de QoS (MQ)

Código	Descrição	Prior.	Dependências
RISE.AGCF-MQ.1	Suporte de mecanismo *IntServ*	3	RI.AGCF-INST.2
RISE.AGCF-MQ.2	Suporte de mecanismo *DiffServ*	3	RI.AGCF-INST.2

RISE.AGCF-MQ.1: Controlo de QoS (IntServ) através do protocolo MEGACO/H.248, de acordo com a norma ETSI ES 283 002 [41] uma vez que outras interfaces poderão ter funcionalidades de QoS para a AGCF. A introduzir futuramente as respectivas normas de especificação com os requisitos caso tal se venha a verificar.

RISE.AGCF-MQ.2: Controlo de QoS (DiffServ) através do protocolo MEGACO/H.248, de acordo com a norma ETSI ES 283 002 [41] tendo em conta que outras interfaces poderão ter funcionalidades de QoS para AGCF. A introduzir futuramente as respectivas normas de especificação com os requisitos caso tal se venha a verificar.

• Requisitos de Integração em Demonstradores

Nesta parte do presente documento são indicados os requisitos necessários à configuração da AGCF, de acordo com o cenário de utilização para efeitos de testes e demonstração. A integração da AGCF deve cumprir os requisitos relacionados com descrição de demonstradores, tal como se encontra definido nos documentos elaborados dentro do âmbito do projecto PR-SHipNET.

Demonstrador SHipNET (DSHIP)

Código	Descrição	Prior.	Dependências
RID.AGCF-DSHIP.1	Capacidade de integração no demonstrador SHipNET	2	RIU.AGCF-CFG.3

RID.AGCF-DSHIP.1: Tendo em conta que o módulo AGCF deve ser inserido no demonstrador de testes SHipNET que poderá não se encontrar plenamente estável e sofrer alterações durante a implementação tal como a A-MGW em desenvolvimento devem ser tidos em conta requisitos adicionais que poderão surgir e que serão enunciados futuramente.

• **Requisitos de Gestão**

Nesta parte, são indicadas as funcionalidades comuns à operação de Gestão da AGCF, isto é, em termos de Geração de Alarmes, Geração de CDRs, e Geração de Estatísticas.

Código	Descrição	Prior.	Dependências
RG.AGCF-ALR.1	Alerta de falhas do sistema físico de suporte (PC) e da AGCF em geral	4	RI.AGCF-INST.2
RG.AGCF-CDR.1	Geração de informação CDR para cada chamada/sessão	4	RI.AGCF-INST.2
RG.AGCF-EST.1	Geração de estatísticas relacionadas com o funcionamento em geral da AGCF e especifico para cada Endpoint de controlo da AGCF	4	RI.AGCF-INST.2

RG.AGCF-ALR,CDR,EST.1: Com o intuito de monitorizar falhas físicas da plataforma que serve de suporte à AGCF e falhas desta deverão, futuramente, ser criados mecanismo que alertem para este tipo de ocorrências.

• **Requisitos Gerais**

Nesta parte, são indicados vários requisitos que de uma forma geral têm de ser cumpridos pela AGCF, como o caso dos requisitos ambientais.

Vários (VAR)

Código	Descrição	Prioridade	Dependências
RGR.AGCF-VAR.1	Redundância	4	-
RGR.AGCF-VAR.2	Escalabilidade e partilha de carga	4	-
RGR.AGCF-VAR.3	Disponibilidade	4	-
RGR.AGCF-VAR.4	Ambientais	2	-

RGR.AGCF-VAR.1,2,3: Estes requisitos são assegurados pela plataforma PC/servidor de 19" Linux, que futuramente servirá de base ao funcionamento deste elemento.

RGR.AGCF-VAR.4: A AGCF cumprirá os requisitos do certificado NEBS *Level* 3.

Capítulo 4

Implementação e Testes

A AGCF é o elemento fulcral de controlo presente na arquitectura de referência para o subsistema PES, baseado na arquitectura IMS (PES IMS-*based*), definido pelo TISPAN para as Redes de Nova Geração.

Após o levantamento dos requisitos a serem cumpridos por este elemento, surge a necessidade de se planear a implementação do mesmo, a qual é efectuada de forma faseada, por patamares, tendo em conta as prioridades apresentadas no Capítulo 3 e a disponibilidade de certas dependências que poderão limitar o desenvolvimento.

Inicialmente é descrito todo o cenário de implementação e testes que foi utilizado no decorrer da parte prática deste trabalho.

O módulo *Line Based Configuration Data* (LBCD) - presente na arquitectura interna da AGCF é acedido pelo *Feature Manager* - deve suportar o armazenamento de diferentes tipos de informação relativa aos clientes cujo terminal está ligado a uma A-MGFs ou R-MGFs que se encontre sob a alçada dessa AGCF.

Primeiro apresenta-se a solução criada para efectuar todo este processo bem como qual a natureza da informação armazenada e todos os testes efectuados para verificar o bom funcionamento da solução implementada.

De seguida, apresenta-se todo o projecto efectuado no âmbito do processo de registo e desregisto de terminais. Foi necessário fazer um estudo sobre como se processa o registo de um terminal no *core* NGN, e ao nível prático, proceder à implementação dos módulos MGC, IMS *Agent* e FM, sendo que, para este último houve ainda a necessidade de ter em conta a sua comunicação com o LBCD. Outro aspecto a considerar foi um levantamento das diferenças entre um processo de registo e um de desregisto.

O subsistema "*Session Processing*" engloba as capacidades que a AGCF deve possuir para lidar com chamadas. Ao contrário do registo que futuramente será executado com apenas um pedido isto é, o grupo de POTS ligados à A-MGW efectuarão o registo de forma conjunta, a solução adoptada tem de ser mais complexa introduzindo o conceito de processos de forma a verificar um correcto funcionamento no que diz respeito à capacidade de efectuar e receber vários pedidos de chamadas simultâneos.

Será apresentada a solução escolhida para a implementação dos módulos referentes a esta funcionalidade e todos os testes efectuados aquando o caso de POTS ligados à AMGW pretenderem efectuar chamadas. Inicialmente apresentam-se os testes para apenas um POTS seguindo-se o caso estendido para n POTS.

Para o sentido inverso, quando um cliente pretende contactar um POTS sob a alçada da AGCF foi iniciada a implementação

4.1 Conceitos gerais

Antes de serem apresentados casos práticos de módulos e respectivas funcionalidades implementadas, bem como os testes efectuados, é descrito todo o ambiente e conceitos geras aplicáveis a qualquer situação descrita na implementação exposta nos sub capítulos seguintes.

A plataforma utilizada para implementar a AGCF foi um PC Pentium M-745, 512 RAM e monitor 15.4" com o sistema operativo Linux UBUNTU ver. 7.10 instalado [60]. Todo o código foi desenvolvido em linguagem C tirando partido do editor gVim [61] .

Na figura 20 encontra-se ilustrado o cenário implementação e testes básico onde se encontra inserida a AGCF. Uma vez que a A-MGW ainda se encontra em fase de implementação as mensagens provenientes dos POTS ligados a esta foram simuladas.

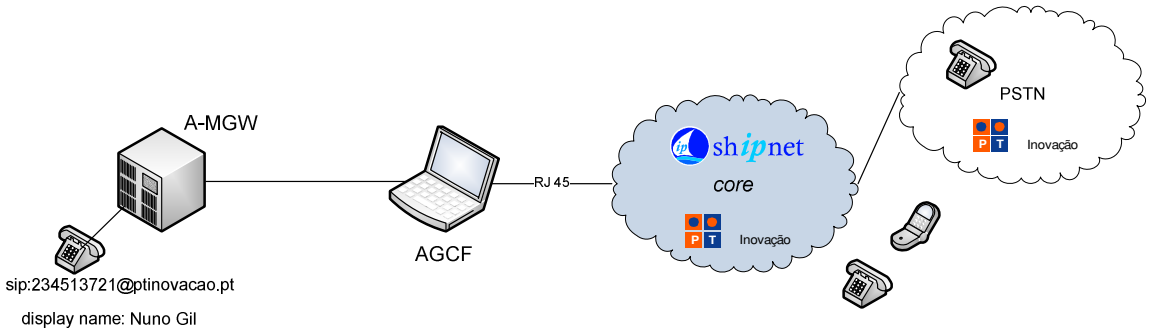


Figura 20 – Cenário de implementação e testes

A *stack* Megaco presente na arquitectura da AGCF será da *Netbricks* [62] não se encontrando ainda integrada.

4.1.1 libosip2/libeXosip2

A estrutura interna da AGCF contempla uma *stack* SIP interligada ao módulo IMS Agent e ao *core*. No decorrer do projecto oSIP [63] surge a *stack open source* denominada *liboxip2* que possui uma biblioteca utilizada em aplicações que tirem partido do protocolo SIP respeitando a norma RFC 3261 [11]. Esta *stack* encontra-se escrita em linguagem C e encontra-se constantemente em renovação.

A *libeXosip2* é uma extensão à libosip2 que possui *Application Programming Interfaces* (APIs) facilitando a implementação de aplicações que utilizem o protocolo SIP.

4.1.2 Wireshark

No decorrer dos testes efectuados surge a necessidade de captar os pacotes trocados entre a AGCF e o core com o intuito de verificar detalhadamente todos os sus campos. Para tal recorreu-se ao software de captura e análise designado de Wireshark [64].

4.2 Configuração da AGCF

Neste subcapítulo começa-se por fazer uma exposição de toda a informação relativa ao processo de configuração inicial da AGCF, apresentando-se uma descrição da solução adoptada. Por fim, é apresentada a descrição de um conjunto de testes efectuados, bem como os respectivos resultados obtidos, com o intuito de avaliar a fiabilidade do módulo implementado.

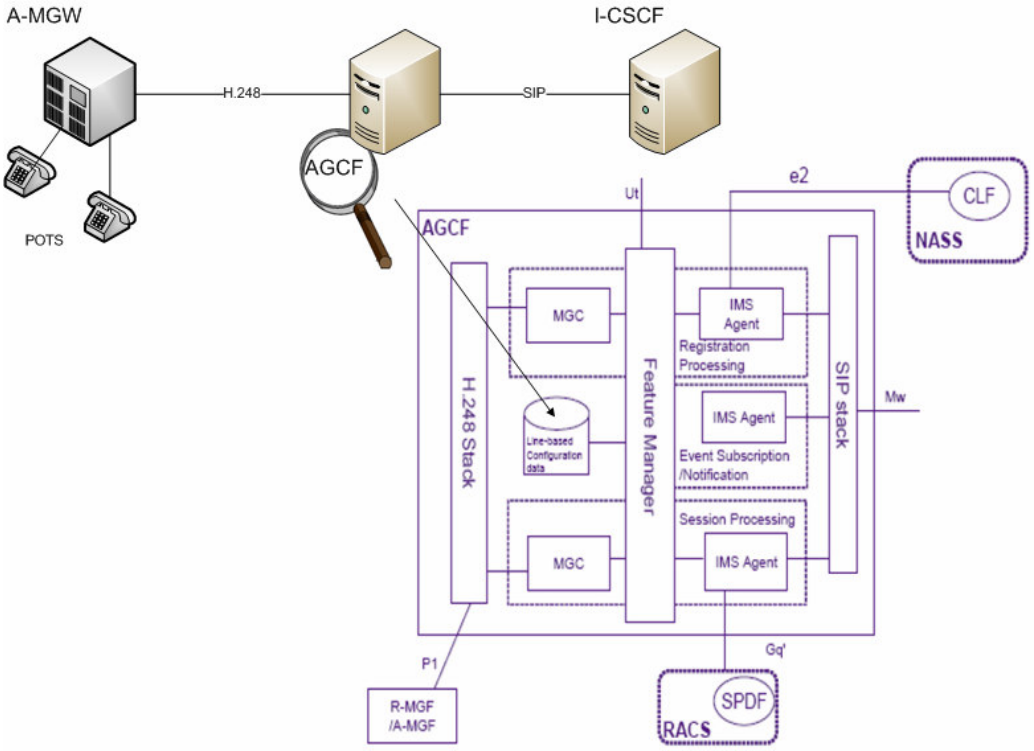


Figura 21 – Módulo LBCD

4.2.1 Objectivo geral

Com o intuito geral de efectuar a configuração inicial da AGCF, procedeu-se a um levantamento dos parâmetros que deveriam ser armazenados no seu módulo interno *Line Based Configuration Data*, de acordo com a arquitectura da norma TS 182 012 [50], tendo em conta todos os módulos com que a mesma comunica, ilustrados na figura 21. Este requisito encontra-se descrito no Capítulo 3 abrangendo os pontos: RF.AGCF-MDL.6 e RIU.AGCF-CFG.2,1e3.

Os parâmetros a serem armazenados que foram tidos em conta são:

- IP ou Host Name da máquina nativa;
- IP ou Host Name das A-MGWs (ex. xxx.xxx.xxx.xxx ou a-mgw1, a-mgw2, etc...);
- Porto H.248 de escuta das A-MGWs (ex. 2427);
- Porto H.248 da AGCF (Porto de escuta de comandos H.248 enviados pelas A-MGWs, ex. 2727);

- H.248 Termination ID dos POTS ligados às A-MGWs (ex: al/trunk0/ts0@a-mgw_address.com);
- IP ou Host Name do I/S-CSCF (ex. xxx.xxx.xxx.xxx ou iscscf);
- Porto SIP de escuta do I/S-CSCF (ex. 5060);
- Porto SIP da AGCF (Porto de escuta de mensagens SIP enviadas pela I/S-CSCF, ex:5060);
- SIP Public URI dos POTS ligados às A-MGWs (ex. sip:gil@domain.com);
- SIP Private URI dos POTS ligados às A-MGWs (ex. sip:gil@domain.com);
- TEL URI dos POTS ligados às A-MGWs (ex. tel:+351234513723);
- Display Name dos POTS ligados às A-MGWs (ex. Nuno Gil);
- User Name dos POTS ligados às A-MGWs (ex. gil);
- Password para registo dos POTS ligados às A-MGWs (ex:****);
- Authorization User Name dos POTS ligados às A-MGWs (ex: gil@domain.com) ;
- Domain IP onde se registam os POTS ligados às A-MGWs (ex: domain.com);
- Expires Register Timer dos POTS ligados às A-MGWs (ex: 3600seg);
- Digit Map para os POTS ligados às A-MGWs;
- Dial Tone Code para os POTS ligados às A-MGWs;

O módulo LBCD irá conter a informação numa estrutura geral que poderá ser acedida e alterada pelo módulo Feature Manager sendo o único, de entre os módulos que constituem a arquitectura interna da AGCF, que possui uma ligação a este módulo.

Surgiu a necessidade de decidir qual a linguagem utilizada para criar o ficheiro que irá servir de ponto de entrada para a inserção de dados dos clientes.

Foi sabido à partida, que no decorrer da implementação de outros módulos, poderia vir a ser necessário acrescentar mais alguns parâmetros a serem armazenados pela LBCD e que, de operador para operador, os campos a serem guardados podem variar. Outro aspecto tido em conta foi que seria interessante e prático poder efectuar a actualização manual do LBCD remotamente via Web e sem necessidade de se desligar a AGCF.

Assim, é necessária uma linguagem que seja flexível, tendo em vista possibilitar de forma fácil e rápida a introdução de novos campos, devendo ser o mais aberta possível para que não surjam questões de incompatibilidades entre diversas plataformas, e ainda de fácil adaptação a uma aplicação remota.

4.2.1.1 eXtended Markup Language (XML)

Foi em 1989 que surgiu a primeira forma de representação de hipertexto na Internet tendo posteriormente evoluído para a linguagem *standard*, conhecida como *Hiper Text Markup Language* (HTML) e desenvolvida no Laboratório Europeu de Física das Partículas (*European Organization for Nuclear Research* - CERN). No entanto, cedo se percebeu que era necessária uma linguagem mais flexível e extensível de forma a fazer face às novas exigências. Surge assim a linguagem XML, especificada em Fevereiro de 1998 pelo W3C (*World Wide Web Consortium*) [65] e, que desde então, rapidamente se tornou bastante popular. Nos dias que correm este tipo

de conceito já se encontra bastante enraizado nas mais diversas áreas. Um factor que foi decisivo para a rápida expansão desta linguagem é o elevado número, e com forte posição no mercado, de empresas que adoptaram o XML em algumas das suas aplicações, como por exemplo o caso da Microsoft, Oracle, IBM ou SUN [66]. Mas, a base de todo o seu sucesso, prende-se com o facto de se tratar de uma linguagem com um formato universal que permite a partilha de dados entre aplicações de forma bastante simples sendo que o XML adapta-se ao mais variado tipo de documentos: catálogos de produtos, relatórios financeiros, transacções comerciais, grafismos vectoriais, etc. .

Para que esta partilha seja possível, é necessário a existência de um *standard* universal para o XML, de modo a não se verificarem casos de incompatibilidades [67]. Antes do aparecimento deste tipo de linguagem, muitas eram as aplicações consideradas incompatíveis, já que a cada uma delas se encontrava associada uma linguagem exclusiva e unicamente suportada pela própria aplicação vindo o XML abrir novos horizontes, tal como se encontra ilustrado na figura 22.

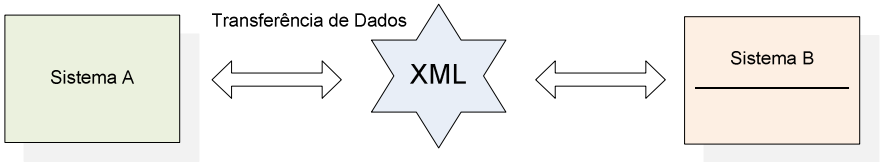


Figura 22 – Compatibilidade verificada no XML

Esta linguagem levou, em poucos anos, ao aparecimento de outras, baseadas no seu princípio de simplicidade e compatibilidades como por exemplo o MathML, ICE, SOAP e WML .

De uma forma geral, o corpo de uma mensagem XML baseia-se em vários elementos que constituem a estrutura de dados e a cada elemento encontram-se associadas tags de *markup*, seguindo sempre uma sintaxe do tipo <categoria> </categoria>, onde toda a informação que se encontra entre estes dois campos é relativa à categoria em causa. O segmento apresentado a seguir representa um exemplo simples de um excerto XML, onde se tem um elemento com o nome AGCF, cujo conteúdo é o texto Control Gateway.

<AGCF> Control Gateway </AGCF>

É através destes *tags* que se torna possível localizar todo o tipo de informação necessária num documento XML.

O facto de o XML ser flexível e extensível, permitindo descrever dados estruturados rapidamente e de fácil integração com o HTML, foram os factores determinantes na sua escolha para a inserção de informação inicial e actualização na LBCD.

4.2.2 Funcionalidades implementadas

Após o levantamento dos parâmetros que é necessário armazenar na LBCD, e escolhida a linguagem que servirá de ponte entre a forma como se possibilita a inserção e actualização de dados referentes aos clientes por parte de um operador e o modo como esta fica armazenada em linguagem C na LBCD, foi criada a estrutura base em XML, ilustrada na figura 23.

```
<?xml version="1.0" ?>
- <AGCF EQUIPNAME="PTIN_AGCF" NSERIE="100001">
  - <GLOBAL_PARAMETERS>
      <IP_AGCF>xxx.xxx.xxx.xxx</IP_AGCF>
      <IP_ISCSCF>xxx.xxx.xxx.xxx</IP_ISCSCF>
      <PORT_SIP_ISCSCF>5060</PORT_SIP_ISCSCF>
      <PORT_SIP_AGCF>5060</PORT_SIP_AGCF>
   </GLOBAL_PARAMETERS>
 - <AMGW nbr="1">
      <IP>xxx.xxx.xxx.xxx</IP>
      <PORT>2427</PORT>
      <PORT_AGCF>2727</PORT_AGCF>
   - <POTS nbr="1">
         <TERMINATION_ID>al/trunk0/ts0@a-mgw1_addr.com</TERMINATION_ID>
         <SIP_PUB_URI>sip:gil@domain.com</SIP_PUB_URI>
         <SIP_PRIV_URI>sip:gil@domain.com</SIP_PRIV_URI>
         <TEL_URI>tel:+351234513723</TEL_URI>
         <DISPLAY>Nuno Gil</DISPLAY>
         <USER>gil</USER>
         <PASS>ptinov</PASS>
         <AUTH>gil@domain.com</AUTH>
         <DOMAIN>domain.com</DOMAIN>
         <EXPIRES>3600</EXPIRES>
         <MAP>xxxxx</MAP>
         <TONE>xxxx</TONE>
      </POTS>
   </AMGW>
</AGCF>
```

Figura 23 – Ficheiro XML base

Os dados inseridos e actualizados no ficheiro XML, denominado de *bd_xml_reader.h*, têm de ser lidos para uma estrutura criada em linguagem C, surgindo a necessidade de se implementar um *parser* que leia um ficheiro XML como parâmetro de entrada e traduza toda a informação nele contida, preenchendo de seguida os campos da estrutura que se encontra no módulo LBCD.

Para a criação do parser, foi necessário efectuar a instalação de packeges específicas que permitem trabalhar com documentos XML – libxm12 e libxm12-dev. Todo o código criado para o parser encontra-se no ficheiro *bd_xml_reader.c*.

No código criado, foi inserida uma função de *debugging* de forma a apresentar na consola Linux onde se coloca a LBCD, a correr a informação recolhida pelo *parser*. A figura 28 exemplifica o resultado dos prints efectuados no seguimento dos testes no caso específico em que uma AGCF controla uma A-MGW com 1 POTS ligados.

```
Print Values BD
Equipname: PTIN_AGCF , nserie: 100001
IP_AGCF: xxx.xxx.xxx.xxx
IP_ISCSCF: xxx.xxx.xxx.xxx
PORT_SIP_ISCSCF: 5060
```

```
PORT_SIP_AGCF: 5060
        AMGW:1 -> IP_AMGW: xxx.xxx.xxx.xxx
        AMGW:1 -> PORT_AMGW: 2427
        AMGW:1 -> PORT_AGCF: 2727
                AMGW:1 -> POTS:1 -> TERM_ID: al/trunk0/ts0@a-mgw1_addr.com
                AMGW:1 -> POTS:1 -> SIP_PUB_URI: sip:gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_PRIV_URI: sip:gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_TEL_URI: tel:+351234513723
                AMGW:1 -> POTS:1 -> DISPLAY NAME: Nuno Gil
                AMGW:1 -> POTS:1 -> USER_NAME: gil
                AMGW:1 -> POTS:1 -> PASS: ptinov
                AMGW:1 -> POTS:1 -> AUTHOR: gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_DOMAIN: domain.com
                AMGW:1 -> POTS:1 -> EXPIRES: 3600
                AMGW:1 -> POTS:1 -> DIGIT_MAP: xxxxx
                AMGW:1 -> POTS:1 -> DIAL_TONE: xxxx
```

Figura 24 – Exemplo de print de *debugging*

4.2.3 Testes

Foram realizados vários testes com o intuito de se verificar o bom funcionamento do módulo LBCD criado, no que diz respeito à informação recolhida por este. Para tal foram criadas várias situações distintas. A especificação do objectivo a ser testado e o respectivo resultado concreto são enunciados de seguida de alguns dos testes realizados, a apresentação de todos tornaria o trabalho bastante extenso.

- **Situação base (1POTS)**

Documento XML com informação sobre AMGW nbr=1 e POTS nbr=1

Parâmetros bd_xml_reader.h: NUM_MAX_AMGW = 1;
NUM_MAX_POTS = 1.

Com este teste pretendeu-se verificar o correcto funcionamento do *parser* na situação base onde a AGCF controla uma AMGW com um POTS. Esperava-se que a informação na estrutura respeitasse a que está contida nos campos inseridos no documento XML. O resultado obtido através da função de debugging foi o seguinte:

```
Print Values BD
Equipname: PTIN_AGCF , nserie: 100001
IP_AGCF: xxx.xxx.xxx.xxx
IP_ISCSCF: xxx.xxx.xxx.xxx
PORT_SIP_ISCSCF: 5060
PORT_SIP_AGCF: 5060
        AMGW:1 -> IP_AMGW: xxx.xxx.xxx.xxx
        AMGW:1 -> PORT_AMGW: 2427
        AMGW:1 -> PORT_AGCF: 2727
                AMGW:1 -> POTS:1 -> TERM_ID: al/trunk0/ts0@a-mgw1_addr.com
                AMGW:1 -> POTS:1 -> SIP_PUB_URI: sip:gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_PRIV_URI: sip:gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_TEL_URI: tel:+351234513723
                AMGW:1 -> POTS:1 -> DISPLAY NAME: Nuno Gil
                AMGW:1 -> POTS:1 -> USER_NAME: gil
                AMGW:1 -> POTS:1 -> PASS: ptinov
                AMGW:1 -> POTS:1 -> AUTHOR: gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_DOMAIN: domain.com
                AMGW:1 -> POTS:1 -> EXPIRES: 3600
                AMGW:1 -> POTS:1 -> DIGIT_MAP: xxxxx
                AMGW:1 -> POTS:1 -> DIAL_TONE: xxxx
```

Confirma-se pois, que o *parser* funciona de forma perfeita, uma vez que a informação apresentada está de acordo com os parâmetros do documento XML.

- **XML com parâmetros errados**

Documento XML com informação sobre AMGW nbr=1 e POTS nbr=1,nbr=2e nbr=3.

Parâmetros bd_xml_reader.h: NUM_MAX_AMGW = 1;
NUM_MAX_POTS = 3.

Para observar o comportamento do *parser* na situação em que o documento XML possuía um índice para POTS que ultrapassa o NUM_MAX_POTS definido no ficheiro *bd_xml_reader.h* e onde a ordem dos índices não é efectuada de forma seguida. Seria de esperar que a informação do POTS número oito fosse descartada, uma vez que o seu índice ultrapassa o número máximo de POTS definido no ficheiro *bd_xml_reader.h* e que a troca de ordem não perturbe o bom funcionamento do *parser*. Obtiveram-se os seguintes resultados:

```
Print Values BD
Equipname: PTIN_AGCF , nserie: 100001
IP_AGCF: xxx.xxx.xxx.xxx
IP_ISCSCF: xxx.xxx.xxx.xxx
PORT_SIP_ISCSCF: 5060
PORT_SIP_AGCF: 5060
        AMGW:1 -> IP_AMGW: xxx.xxx.xxx.xxx
        AMGW:1 -> PORT_AMGW: 2427
        AMGW:1 -> PORT_AGCF: 2727
                AMGW:1 -> POTS:1 -> TERM_ID: al/trunk0/ts0@a-mgw1_addr.com
                AMGW:1 -> POTS:1 -> SIP_PUB_URI: sip:gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_PRIV_URI: sip:gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_TEL_URI: tel:+351234513723
                AMGW:1 -> POTS:1 -> DISPLAY NAME: Nuno Gil
                AMGW:1 -> POTS:1 -> USER_NAME: gil
                AMGW:1 -> POTS:1 -> PASS: ptinov
                AMGW:1 -> POTS:1 -> AUTHOR: gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_DOMAIN: domain.com
                AMGW:1 -> POTS:1 -> EXPIRES: 3600
                AMGW:1 -> POTS:1 -> DIGIT_MAP: xxxxx
                AMGW:1 -> POTS:1 -> DIAL_TONE: xxxx
                AMGW:1 -> POTS:2 -> TERM_ID:
                AMGW:1 -> POTS:2 -> SIP_PUB_URI:
                AMGW:1 -> POTS:2 -> SIP_PRIV_URI:
                AMGW:1 -> POTS:2 -> SIP_TEL_URI:
                AMGW:1 -> POTS:2 -> DISPLAY NAME:
                AMGW:1 -> POTS:2 -> USER_NAME:
                AMGW:1 -> POTS:2 -> PASS:
                AMGW:1 -> POTS:2 -> AUTHOR:
                AMGW:1 -> POTS:2 -> SIP_DOMAIN:
                AMGW:1 -> POTS:2 -> EXPIRES: 0
                AMGW:1 -> POTS:2 -> DIGIT_MAP:
                AMGW:1 -> POTS:2 -> DIAL_TONE:
                AMGW:1 -> POTS:3 -> TERM_ID: 3_al/trunk0/ts0@a-mgw1_addr.com_3
                AMGW:1 -> POTS:3 -> SIP_PUB_URI: 3_sip:gil@domain.com_3
                AMGW:1 -> POTS:3 -> SIP_PRIV_URI: 3_sip:gil@domain.com_3
                AMGW:1 -> POTS:3 -> SIP_TEL_URI: 3_tel:+351234513723_3
                AMGW:1 -> POTS:3 -> DISPLAY NAME: 3_Nuno Gil_3
                AMGW:1 -> POTS:3 -> USER_NAME: 3_gil_3
                AMGW:1 -> POTS:3 -> PASS: 3_ptinov_3
                AMGW:1 -> POTS:3 -> AUTHOR: 3_gil@domain.com_3
                AMGW:1 -> POTS:3 -> SIP_DOMAIN: 3_domain.com_3
                AMGW:1 -> POTS:3 -> EXPIRES: 3
                AMGW:1 -> POTS:3 -> DIGIT_MAP: 3_xxxxx_3
                AMGW:1 -> POTS:3 -> DIAL_TONE: 3_xxxx_3
```

Confirmou-se que, tal como era esperado, o índice número oito não foi tido em conta pelo *parser*, tendo este apenas considerado os POTS até ao número defendido no ficheiro *bd_xml_reader.h* .

- **XML com falta de parâmetros**

Documento XML com informação sobre AMGW nbr=1 e POTS nbr=1,nbr=2, mas com falta de campos.

Parâmetros bd_xml_reader.h: NUM_MAX_AMGW = 1;
NUM_MAX_POTS = 2.

Pretendeu-se testar o parser num cenário em que faltavam campos no documento XML, tendo-se retirado dentro do nó <AGCF> a declaração NSERIE="100001", em <GLOBAL_PARAMETERS> os campos <IP_AGCF> xxx.xxx.xxx.xxx </IP_AGCF>, <PORT_SIP_ISCSCF> 5060 </PORT_SIP_ISCSCF>, e suprimido no nó <POTS nbr="1"> os campos <SIP_PUB_URI> sip:gil@domain.com <SIP_PUB_URI>, <USER> gil </USER> e <MAP> xxxxx </MAP>.

Aguardou-se que, neste caso de falta de campos, o parser viesse a considerar valores que foram inseridos nas declarações auxiliares das estruturas efectuadas no ficheiro *bd_xml_reader.c* . O resultado foi o seguinte:

```
Print Values BD
Equipname: PTIN_AGCF , nserie:
IP_AGCF: 0
IP_ISCSCF: xxx.xxx.xxx.xxx
PORT_SIP_ISCSCF: 0
PORT_SIP_AGCF: 5060
        AMGW:1 -> IP_AMGW: xxx.xxx.xxx.xxx
        AMGW:1 -> PORT_AMGW: 2427
        AMGW:1 -> PORT_AGCF: 2727
                AMGW:1 -> POTS:1 -> TERM_ID: al/trunk0/ts0@a-mgw1_addr.com
                AMGW:1 -> POTS:1 -> SIP_PUB_URI: 0
                AMGW:1 -> POTS:1 -> SIP_PRIV_URI: sip:gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_TEL_URI: tel:+351234513723
                AMGW:1 -> POTS:1 -> DISPLAY NAME: Nuno Gil
                AMGW:1 -> POTS:1 -> USER_NAME: 0
                AMGW:1 -> POTS:1 -> PASS: ptinov
                AMGW:1 -> POTS:1 -> AUTHOR: gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_DOMAIN: domain.com
                AMGW:1 -> POTS:1 -> EXPIRES: 3600
                AMGW:1 -> POTS:1 -> DIGIT_MAP: 0
                AMGW:1 -> POTS:1 -> DIAL_TONE: xxxx
                AMGW:1 -> POTS:2 -> TERM_ID: 2_al/trunk0/ts0@a-mgw1_addr.com_2
                AMGW:1 -> POTS:2 -> SIP_PUB_URI: 2_sip:gil@domain.com_2
                AMGW:1 -> POTS:2 -> SIP_PRIV_URI: 2_sip:gil@domain.com_2
                AMGW:1 -> POTS:2 -> SIP_TEL_URI: 2_tel:+351234513723_2
                AMGW:1 -> POTS:2 -> DISPLAY NAME: 2_Nuno Gil_2
                AMGW:1 -> POTS:2 -> USER_NAME: 2_gil_2
                AMGW:1 -> POTS:2 -> PASS: 2_ptinov_2
                AMGW:1 -> POTS:2 -> AUTHOR: 2_gil@domain.com_2
                AMGW:1 -> POTS:2 -> SIP_DOMAIN: 2_domain.com_2
                AMGW:1 -> POTS:2 -> EXPIRES: 2
                AMGW:1 -> POTS:2 -> DIGIT_MAP: 2_xxxxx_2
                AMGW:1 -> POTS:2 -> DIAL_TONE: 2_xxxx_2
```

Notou-se que a estrutura nos campos em falha apresentava os valores inseridos na inicialização, assim, o resultado foi o esperado e surgiu a ideia de melhorar determinados campos da estrutura de inicialização, como, por exemplo, poder inicializar os campos <USER> e <DISPLAY NAME> com UNKNOWN em vez de 0.

- **XML com parâmetros a mais**

Documento XML com informação sobre AMGW nbr=1 e POTS nbr=1, nbr=2, mas com adição de campos.

Parâmetros bd_xml_reader.h: NUM_MAX_AMGW = 1;
NUM_MAX_POTS = 2.

Agora, pretende-se testar a situação inversa da anterior, isto é, aquela em que o documento XML possui mais campos do que os necessários para a estrutura. Para isso, acrescentaram-se os seguintes campos a esse documento : no nó <GLOBAL_PARAMETERS> acrescentou-se a linha <TESTE> 123abc </TESTE> ; no nó <POTS nbr="1"> as linhas <TESTE_2> 123456789 </TESTE_2> e <TESTE_3> abcd </TESTE_3>.

Deseja-se que o *parser* não tenha esses campos em consideração e que estes não interfiram no seu bom funcionamento. A função de *debugging* efectuou o seguinte *print*:

```
Print Values BD
Equipname: PTIN_AGCF , nserie: 100001
IP_AGCF: xxx.xxx.xxx.xxx
IP_ISCSCF: xxx.xxx.xxx.xxx
PORT_SIP_ISCSCF: 5060
PORT_SIP_AGCF: 5060
        AMGW:1 -> IP_AMGW: xxx.xxx.xxx.xxx
        AMGW:1 -> PORT_AMGW: 2427
        AMGW:1 -> PORT_AGCF: 2727
                AMGW:1 -> POTS:1 -> TERM_ID: al/trunk0/ts0@a-mgw1_addr.com
                AMGW:1 -> POTS:1 -> SIP_PUB_URI: sip:gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_PRIV_URI: sip:gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_TEL_URI: tel:+351234513723
                AMGW:1 -> POTS:1 -> DISPLAY NAME: Nuno Gil
                AMGW:1 -> POTS:1 -> USER_NAME: gil
                AMGW:1 -> POTS:1 -> PASS: ptinov
                AMGW:1 -> POTS:1 -> AUTHOR: gil@domain.com
                AMGW:1 -> POTS:1 -> SIP_DOMAIN: domain.com
                AMGW:1 -> POTS:1 -> EXPIRES: 3600
                AMGW:1 -> POTS:1 -> DIGIT_MAP: xxxxx
                AMGW:1 -> POTS:1 -> DIAL_TONE: xxxx
```

Como era de prever, a adição esses campos no documento XML não afectou o bom funcionamento do *parser*, tendo os mesmos sido descartados.

- **Capacidade (48POTS)**

Documento XML com informação sobre AMGW nbr=1, … , nbr=4 e POTS nbr=1, … , nbr=12.

Parâmetros bd_xml_reader.h: NUM_MAX_AMGW = 4;
NUM_MAX_POTS = 12.

Foi posta aprova a fiabilidade do *parser*, quando exposto a grandes quantidades de informação, tendo-se neste caso específico aumentado o número de A-MGWs para 4 cada uma com 12 POTS num total de 48 POTS. O parser deverá apresentar de uma forma correcta toda a informação das 4 A-MGWs e dos respectivos POTS. Uma vez que o *print* da função de *debugging* é bastante extenso, apenas se apresenta um excerto do mesmo:

```
AMGW:1 -> POTS:11 -> DIGIT_MAP: 2_xxxxx_2
AMGW:1 -> POTS:11 -> DIAL_TONE: 2_xxxx_2
AMGW:1 -> POTS:12 -> TERM_ID: 3_al/trunk0/ts0@a-mgw1_addr.com_3
```

```
AMGW:1 -> POTS:12 -> SIP_PUB_URI: 3_sip:gil@domain.com_3
AMGW:1 -> POTS:12 -> SIP_PRIV_URI: 3_sip:gil@domain.com_3
AMGW:1 -> POTS:12 -> SIP_TEL_URI: 3_tel:+351234513723_3
AMGW:1 -> POTS:12 -> DISPLAY NAME: 3_Nuno Gil_3
AMGW:1 -> POTS:12 -> USER_NAME: 3_gil_3
AMGW:1 -> POTS:12 -> PASS: 3_ptinov_3
AMGW:1 -> POTS:12 -> AUTHOR: 3_gil@domain.com_3
AMGW:1 -> POTS:12 -> SIP_DOMAIN: 3_domain.com_3
AMGW:1 -> POTS:12 -> EXPIRES: 3
AMGW:1 -> POTS:12 -> DIGIT_MAP: 3_xxxxx_3
AMGW:1 -> POTS:12 -> DIAL_TONE: 3_xxxx_3
AMGW:2 -> IP_AMGW: xxx.xxx.xxx.xxx
AMGW:2 -> PORT_AMGW: 2427
AMGW:2 -> PORT_AGCF: 2727
AMGW:2 -> POTS:1 -> TERM_ID: al/trunk0/ts0@a-mgw1_addr.com
AMGW:2 -> POTS:1 -> SIP_PUB_URI: sip:gil@domain.com
AMGW:2 -> POTS:1 -> SIP_PRIV_URI: sip:gil@domain.com
AMGW:2 -> POTS:1 -> SIP_TEL_URI: tel:+351234513723
AMGW:2 -> POTS:1 -> DISPLAY NAME: Nuno Gil
AMGW:2 -> POTS:1 -> USER_NAME: gil
AMGW:2 -> POTS:1 -> PASS: ptinov
AMGW:2 -> POTS:1 -> AUTHOR: gil@domain.com
AMGW:2 -> POTS:1 -> SIP_DOMAIN: domain.com
AMGW:2 -> POTS:1 -> EXPIRES: 3600
AMGW:2 -> POTS:1 -> DIGIT_MAP: xxxxx
AMGW:2 -> POTS:1 -> DIAL_TONE: xxxx
AMGW:2 -> POTS:2 -> TERM_ID: 2_al/trunk0/ts0@a-mgw1_addr.com_2
AMGW:2 -> POTS:2 -> SIP_PUB_URI: 2_sip:gil@domain.com_2
AMGW:2 -> POTS:2 -> SIP_PRIV_URI: 2_sip:gil@domain.com_2
AMGW:2 -> POTS:2 -> SIP_TEL_URI: 2_tel:+351234513723_2
AMGW:2 -> POTS:2 -> DISPLAY NAME: 2_Nuno Gil_2
AMGW:2 -> POTS:2 -> USER_NAME: 2_gil_2
AMGW:2 -> POTS:2 -> PASS: 2_ptinov_2
AMGW:2 -> POTS:2 -> AUTHOR: 2_gil@domain.com_2
AMGW:2 -> POTS:2 -> SIP_DOMAIN: 2_domain.com_2
AMGW:2 -> POTS:2 -> EXPIRES: 2
AMGW:2 -> POTS:2 -> DIGIT_MAP: 2_xxxxx_2
AMGW:2 -> POTS:2 -> DIAL_TONE: 2_xxxx_2
AMGW:2 -> POTS:3 -> TERM_ID: 3_al/trunk0/ts0@a-mgw1_addr.com_3
AMGW:2 -> POTS:3 -> SIP_PUB_URI: 3_sip:gil@domain.com_3
AMGW:2 -> POTS:3 -> SIP_PRIV_URI: 3_sip:gil@domain.com_3
AMGW:2 -> POTS:3 -> SIP_TEL_URI: 3_tel:+351234513723_3
AMGW:2 -> POTS:3 -> DISPLAY NAME: 3_Nuno Gil_3
AMGW:2 -> POTS:3 -> USER_NAME: 3_gil_3
AMGW:2 -> POTS:3 -> PASS: 3_ptinov_3
AMGW:2 -> POTS:3 -> AUTHOR: 3_gil@domain.com_3
AMGW:2 -> POTS:3 -> SIP_DOMAIN: 3_domain.com_3
AMGW:2 -> POTS:3 -> EXPIRES: 3
AMGW:2 -> POTS:3 -> DIGIT_MAP: 3_xxxxx_3
AMGW:2 -> POTS:3 -> DIAL_TONE: 3_xxxx_3
AMGW:2 -> POTS:4 -> TERM_ID: al/trunk0/ts0@a-mgw1_addr.com
AMGW:2 -> POTS:4 -> SIP_PUB_URI: sip:gil@domain.com
AMGW:2 -> POTS:4 -> SIP_PRIV_URI: sip:gil@domain.com
AMGW:2 -> POTS:4 -> SIP_TEL_URI: tel:+351234513723
AMGW:2 -> POTS:4 -> DISPLAY NAME: Nuno Gil
AMGW:2 -> POTS:4 -> USER_NAME: gil
AMGW:2 -> POTS:4 -> PASS: ptinov
AMGW:2 -> POTS:4 -> AUTHOR: gil@domain.com
AMGW:2 -> POTS:4 -> SIP_DOMAIN: domain.com
AMGW:2 -> POTS:4 -> EXPIRES: 3600
AMGW:2 -> POTS:4 -> DIGIT_MAP: xxxxx
AMGW:2 -> POTS:4 -> DIAL_TONE: xxxx
AMGW:2 -> POTS:5 -> TERM_ID: 2_al/trunk0/ts0@a-mgw1_addr.com_2
AMGW:2 -> POTS:5 -> SIP_PUB_URI: 2_sip:gil@domain.com_2
AMGW:2 -> POTS:5 -> SIP_PRIV_URI: 2_sip:gil@domain.com_2
AMGW:2 -> POTS:5 -> SIP_TEL_URI: 2_tel:+351234513723_2
AMGW:2 -> POTS:5 -> DISPLAY NAME: 2_Nuno Gil_2
AMGW:2 -> POTS:5 -> USER_NAME: 2_gil_2
AMGW:2 -> POTS:5 -> PASS: 2_ptinov_2
AMGW:2 -> POTS:5 -> AUTHOR: 2_gil@domain.com_2
AMGW:2 -> POTS:5 -> SIP_DOMAIN: 2_domain.com_2
AMGW:2 -> POTS:5 -> EXPIRES: 2
AMGW:2 -> POTS:5 -> DIGIT_MAP: 2_xxxxx_2
AMGW:2 -> POTS:5 -> DIAL_TONE: 2_xxxx_2
AMGW:2 -> POTS:6 -> TERM_ID: 3_al/trunk0/ts0@a-mgw1_addr.com_3
AMGW:2 -> POTS:6 -> SIP_PUB_URI: 3_sip:gil@domain.com_3
AMGW:2 -> POTS:6 -> SIP_PRIV_URI: 3_sip:gil@domain.com_3
AMGW:2 -> POTS:6 -> SIP_TEL_URI: 3_tel:+351234513723_3
AMGW:2 -> POTS:6 -> DISPLAY NAME: 3_Nuno Gil_3
AMGW:2 -> POTS:6 -> USER_NAME: 3_gil_3
AMGW:2 -> POTS:6 -> PASS: 3_ptinov_3
AMGW:2 -> POTS:6 -> AUTHOR: 3_gil@domain.com_3
AMGW:2 -> POTS:6 -> SIP_DOMAIN: 3_domain.com_3
```

```
AMGW:2 -> POTS:6 -> EXPIRES: 3
AMGW:2 -> POTS:6 -> DIGIT_MAP: 3_xxxxx_3
AMGW:2 -> POTS:6 -> DIAL_TONE: 3_xxxx_3
AMGW:2 -> POTS:7 -> TERM_ID: al/trunk0/ts0@a-mgw1_addr.com
AMGW:2 -> POTS:7 -> SIP_PUB_URI: sip:gil@domain.com
AMGW:2 -> POTS:7 -> SIP_PRIV_URI: sip:gil@domain.com
AMGW:2 -> POTS:7 -> SIP_TEL_URI: tel:+351234513723
AMGW:2 -> POTS:7 -> DISPLAY NAME: Nuno Gil
AMGW:2 -> POTS:7 -> USER_NAME: gil
AMGW:2 -> POTS:7 -> PASS: ptinov
AMGW:2 -> POTS:7 -> AUTHOR: gil@domain.com
AMGW:2 -> POTS:7 -> SIP_DOMAIN: domain.com
AMGW:2 -> POTS:7 -> EXPIRES: 3600
AMGW:2 -> POTS:7 -> DIGIT_MAP: xxxxx
AMGW:2 -> POTS:7 -> DIAL_TONE: xxxx
AMGW:2 -> POTS:8 -> TERM_ID: 2_al/trunk0/ts0@a-mgw1_addr.com_2
AMGW:2 -> POTS:8 -> SIP_PUB_URI: 2_sip:gil@domain.com_2
```

O *parser* efectuou de forma perfeita o preenchimento dos campos, de acordo com a informação do documento XML, como seria de esperar, provando que a LBCD está apta a armazenar grandes quantidades de informação e que esta é tratada de maneira correcta pelo parser.

4.3 Registo e Desregisto

Neste ponto serão abordadas as questões relativas ao registo e desregisto de terminais no *core* sendo inicialmente apresentada a solução adoptada, efectuando-se uma descrição detalhada das características específicas escolhidas para cada módulo e de que forma estes comunicam entre si. Posteriormente, são enunciados os testes efectuados ao módulo geral implementado, apresentando-se os resultados e uma discussão dos mesmos. A figura 25 ilustra a arquitectura geral da AGCF, onde é visível o subsistema responsável pelo processo de registo, bem como os módulos que o constituem e a serem implementados.

Este ponto abrange os seguintes requisitos referidos no Capitulo 3: RF.AGCF-MDL.1, RF.AGCF-MDL.2, RF.AGCF-MDL.3, RISE.AGCF-PR.1, RISE.AGCF-PR.2, RISE.AGCF-PR.7, RISE.AGCF-PR.8.

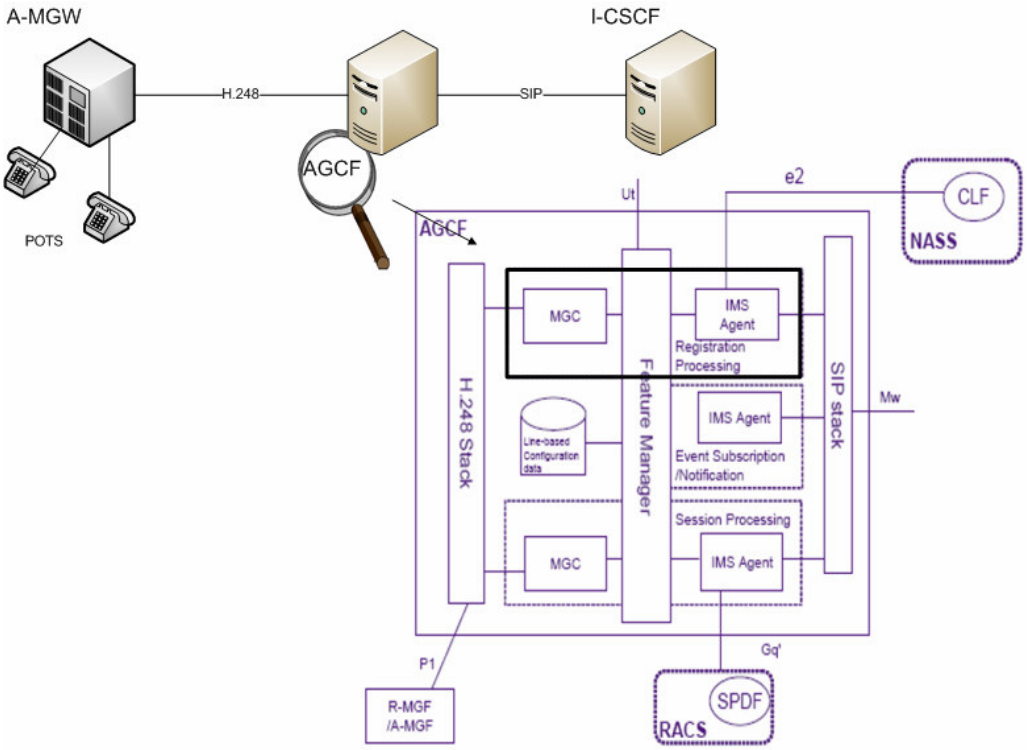


Figura 25 – Módulo Registration Processing

4.3.1 Objectivo geral

De forma a verificar como deveria ser efectuado o registo dos POTS ligados à A-MGF, que é controlada pela AGCF, foi tido em conta que esta é vista pelo *core* como um P-CSCF com vários IMS *Terminals* ligados, de acordo com a arquitectura da norma ETSI TS 182 012 [50]. Como tal, foi necessário averiguar como é processado o registo de um terminal SIP no *core* IMS, via P-CSCF [68]. Deve-se em consideração que, para a AGCF, as mensagens que devem ser suportadas pelo processo de registo, referentes ao P-CSCF e UE, estão representadas a negrito.

Apresenta-se de seguida a sequencia de todas as primitivas presentes num pedido de registo e o fluxo das mesmas, considerando o UE e os elementos do *core* que percorrem [68].

1) O terminal IMS envia o SIP REGISTER Request para o P-CSCF

2) O P-CSCF envia para o I-CSCF da home network o pedido de registo

3) De forma a descobrir qual o S-CSCF associado ao utilizador, o I-CSCF envia um Diameter User - *Authentication* – Request (UAR) ao HSS com a identificação pública e privada do utilizador e a identificação da rede .

4) O HSS responde com uma mensagem Diameter User – *Authentication* – Answer (UAA), onde indica qual o S-CSCF reservado para o utilizador

5) Depois de o I-CSCF ter determinado qual o S-CSCF associado ao utilizador, envia a esse mesmo S-CSCF o SIP REGISTER Request

6) O S-CSCF contacta o HSS.

7) O HSS guarda o S-CSCF URI associado ao cliente e responde ao S-CSCF através de uma mensagem Diameter – Multimedia - Auth - Answer *message* (MAA). Este MAA inclui um ou mais vectores de autenticação que o S-CSCF necessita para autenticar o cliente.

8) O S-CSCF cria uma resposta SIP 401 Unauthorized. Esta resposta inclui um desafio (*challenge*) no WWW - *Authenticate header field* ao qual o terminal IMS deve ser capaz de responder.

9) A mensagem SIP 401 Unauthorized é encaminhada do I-CSCF para o P-CSCF.

10) A mensagem SIP 401 Unauthorized é encaminhada do P-CSCF para o terminal IMS.

11) O terminal IMS recebe a mensagem SIP 401 Unauthorized, verifica que a mesma possui um desafio cifrado em MD5 ou AKA que deve ser resolvido e como tal resolve-o. Esta resposta usualmente é denominada usualmente de *credentials*, sendo criada uma nova mensagem SIP REGISTER Request que é enviada para o P-CSCF.

12) O P-CSCF efectua o mesmo procedimento que no primeiro SIP REGISTER Request

13) O I-CSCF envia um UAR para o HSS (de forma a descobrir qual o S-CSCF apropriado para o cliente)

14) O HSS responde com um UAA com a especificação de qual o S-CSCF determinado para o cliente

15) O I-CSCF envia para o S-CSCF determinado para o cliente a SIP REGISTER Request *message* que inclui as *credentials* (resposta do terminal IMS ao desafio que o S-CSCF havia enviado na resposta SIP 401 Unauthorized ao 1º SIP REGISTER Request)

16) O S-CSCF valida as *credentials*, baseando-se nos vectores de autenticação recebidos do HSS na MAA (7) e envia ao HSS uma Diameter SAR *message*, informando o HSS que o cliente se encontra registado e pretende fazer o *download* do *profile* deste.

17) O HSS envia ao S-CSCF o *user profile*.

18) O S-CSCF envia uma mensagem SIP response 200 (OK) para o I-CSCF que posteriormente a encaminhará até ao P-CSCF (19) e o mesmo até ao terminal IMS (20).

19) O I-CSCF encaminha a SIP response 200 (OK) para o P-CSCF

20) O P-CSCF encaminha a SIP response 200 (OK) para o terminal IMS

A figura 26 apresenta de uma forma simples como é executado o processo de um pedido de registo por parte de um cliente, ilustrando as mensagens SIP trocadas entre este e o elemento do *core* com que comunica.

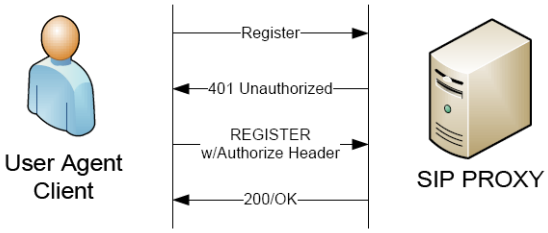


Figura 26 – Mensagens registo

Em resposta ao primeiro pedido de registo, é recebida uma mensagem de 401 *Unauthorized* mas que vem acompanhada de um desafio ao qual o cliente responde no segundo pedido de registo. Caso todos os dados se encontrem correctos, o cliente é registado e informado de que o processo foi bem sucedido através de uma primitiva de 200 OK.

Considerando o caso específico de registo, pode-se afirmar de uma forma resumida que o módulo MGC é responsável pela comunicação com a A-MGW, recebendo mensagens *H.248 ServiceChange*. Por sua vez o IMS Agent comunica com o *core* enviando e recebendo todas as mensagens que são trocadas usualmente entre um P-CSCF / IMS UE e o *core* na fase de registo. Por fim, o módulo FM efectua toda a interligação e respectiva coordenação entre os dois módulos anteriores e interage com o LBCD onde se encontra informação relativa aos POTS e respectivas A-MGWs ligadas à AGCF.

De uma forma geral, as funcionalidades que cada módulo interno da AGCF deve suportar, tendo como objectivo o registo ou o desregisto de POTS no *core*, são abaixo descritas. Deve-se ter em conta que, para o caso de desregisto, o procedimento a tomar, no que respeita à implementação, será muito parecido ao de um registo.

Media Gateway Controller

- Receber por parte da A-MGW mensagens de ServiceChange;
- Enviar para o Feature Manager primitivas de pedido de registo com os respectivos parâmetros informativos referentes à entidade que se pretende registar;
- Receber por parte do FM primitivas informando o sucesso ou não do pedido;

Feature Manager

- Receber por parte da MGC primitivas indicando que se trata de um ServiceChange;
- Interagir com o LBCD, de forma a obter dados relativos aos POTS que se pretendem registar;
- Enviar para o IMS Agent um Register Request com os dados adquiridos no ponto anterior;
- Receber do IMS Agent uma primitiva de 200 OK, caso o registo tenha sido efectuado com sucesso, ou uma mensagem de erro em caso contrário;

•Enviar para o MGC uma primitiva de OK, informando que o registo foi bem sucedido, ou de erro, caso contrário;

IMS Agent

•Receber por parte do FM pedidos de registo;

•Construir mensagens SIP REGISTER Request com base nos parâmetros recebidos, tirando partido da stack SIP;

•Enviar para o core, mais precisamente para o I-CSCF, um SIP Register Request;

•Responder ao Challange de acordo com os parâmetros recebidos do FM e enviar um SIP Register Request para o core.;

•Receber, por parte do *core*, mensagens de 200 OK, informando que o registo foi bem sucedido ou de erro em caso de falha;

•Enviar uma primitiva para o FM, informando-o do sucesso ou não do pedido de registo

Outro aspecto importante, a considerar, prende-se com a interacção dos três módulos da arquitectura interna da AGCF intervenientes no processo de registo, a qual deve ser rápida e efectuada de forma bem coordenada, sob pena de um incorrecto funcionamento da AGCF.

4.3.2 Funcionalidades implementadas

- **Funcionalidades Gerais**

A grande diferença entre um pedido de registo e um de desregisto é o facto de um dos campos do pedido enviado para o *core* variar consoante o que se pretende. Este campo é o *expires*, onde é colocado o tempo, em segundos, que se pretende que o registo fique activo no *core*. Assim, de forma a efectuar o desregisto, este deve adquirir o valor de zero segundos, sendo todo o processo igual ao de um registo convencional. A troca de primitivas para efectuar o registo desde o POTS até ao *core* encontra-se exemplificada na figura 27.

Para efectuar a comunicação entre os três módulos internos da AGCF a solução adoptada foi baseada em *sockets* segundo um modelo de clientes servidores sendo que o IMS Agent é servidor do FM que por sua vez é servidor do MGC.

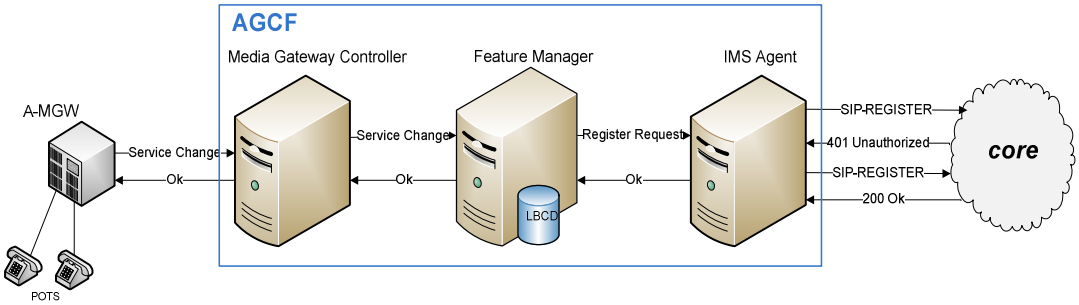


Figura 27 – Processo completo de registo

- **Funcionalidades Específicas**

- Media Gateway Controller

O módulo MGC é, de uma forma geral, aquele que interage com a A-MGW através do protocolo MEGACO/H.248 [41]. No bloco funcional da AGCF encontra-se uma H.248 *stack*, tal como ilustrado na figura 29, a qual é utilizada para a construção e leitura de mensagens que utilizem este protocolo (nesta fase inicial esta stack ainda não se encontra presente sendo que os comandos H.248 são emulados através de mensagens específicas para efeitos de teste).

Registo e Desregisto dos terminais (POTS)

A abordagem tida em conta para a implementação do módulo Media Gateway Controller - no caso da recepção por parte da sua *stack* MEGACO (simulada) de uma mensagem de pedido de registo - foi a apresentada no diagrama da figura 28.

Do ponto de vista de implementação, considerou-se que o módulo MGC apenas iria querer saber se o *type* da mensagem recebida é *ServiceChange*, não estando interessado no seu *method*, onde se encontra indicado se se trata de um pedido de registo ou desregisto sendo tal informação tratada posteriormente pelo FM.

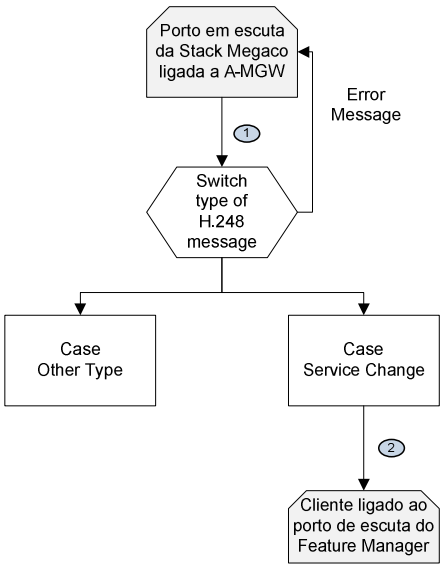


Figura 28 – Mensagem recebida no MGC de ServiceChange

1) O *Media Gateway Controller* recebe no seu porto de escuta uma mensagem H.248 e verifica qual o seu *type*. Caso este não seja reconhecido, é enviada uma primitiva de erro para a A-MGW emissora do pedido.

2) Comprovou-se que o *type* da mensagem recebida era do tipo *Service Change*. Agora - de acordo com os parâmetros recebidos relativamente ao POTS que se pretende registar/desregistar, isto é, qual a A-MGW que controla esse POTS e qual o endereço do

mesmo - é enviada uma primitiva para o Feature Manager, indicando o pedido que se pretende efectuar.

Primitivas entre Media Gateway Controller de registo e Feature Manager

Atendendo a que nesta fase inicial ainda não se dispõe de uma *stack* MEGACO, as primitivas deste módulo serão forçadas, de forma a simular a recepção de mensagens H.248 no porto de escuta da MGC. Os parâmetros de entrada serão inseridos na linha de comandos associada a este módulo.

O formato das primitivas enviadas pelo módulo Media Gateway Controller para o Feature Manager encontra-se declarado no ficheiro *bd_mensagens.h* e possui na sua estrutura os seguintes campos:

```
struct message_mgc_to_fm
{
      char type [20];
      char reason[20];
      char mgw_adress[20];
      char terminationid[50];
      char method [10];
}
```

type – indica o tipo de primitiva que está a ser enviada. No caso de registo/desregisto a primitiva em causa terá um *type* contendo um *ServiceChange*;

reason – permite, caso necessário, indicar qual o motivo específico do pedido em causa;

mgw_adress – indica o endereço da A-MGW à qual se encontra ligado o POTS que pretende efectuar o registo;

terminationid – indica o índice do POTS na A-MGW;

method – para o caso específico do *type* ser *ServiceChange* pode ser um *Restart* quando se pretende efectuar um novo registo. Para o caso de desregisto o *method* pode ser *Forced* ou Gracefu,l onde na primeira hipótesse todas as conexões activas serão forçosamente desligadas e os terminais desregistados, enquanto na segunda se terá de aguardar que as comunicações que se encontrarem activas terminem antes de efectuar o desregisto;

Feature Manager

O módulo Feature Manager é um módulo fulcral em todos os processos, incluindo o de registo, uma vez que, é responsável por toda a intercomunicação entre os módulos que interagem com a A-MGW e o *core*. De um lado, encontra-se em escuta de primitivas enviadas pela MGC, verificando se são referentes a um pedido de registo ou desregisto, isto é, se possuem um *type* declarado como *ServiceChange*, e tem ainda de comunicar ao MGC o sucesso, ou não, da tentativa de registo. Já no lado oposto, comunica com o IMS Agent, enviando-lhe parâmetros necessários à construção de uma mensagem *SIP Register*, tirando partido da SIP *stack* recebendo

da parte desta, a notificação de sucesso ou não do pedido.

É de referir que o FM acede e altera o módulo LBCD com o intuito de consultar dados relativos ao POTS que se pretende registar ou alterar esses mesmos dados.

Na planificação da abordagem a ser tida em conta para o funcionamento do FM - no caso de recepção de uma mensagem H.248 por parte do MGC, mais especificamente quando o *type* dessa mensagem é um *ServiceChange* - alguns aspectos tiveram de ser tidos em conta. Por exemplo, situações como receber um pedido de registo do MGC e o POTS em questão já se encontrar registado então este pedido não se efectua novamente. No caso de a primitiva recebida ser um *ServiceChange,* mas o seu *method* ser *Graceful* ou *Forced* - indicando que se pretende efectuar um desregisto de determinado terminal - não faz sentido tentar efectuá-lo se o terminal não se encontrar registado. Este tipo de situações foram tidas em conta de forma a minimizar o desperdício de recursos.

Será necessário acrescentar um campo à estrutura já implementada na LBCD o que será uma variável booleana *register* que permite indicar se o POTS se encontra ou não registado.

Assim, antes de interagir com os restantes módulos, o FM tem de verificar o tipo e validade das informações recebidas de maneira a limitar todos os casos indesejáveis possíveis.

- Registo dos terminais (POTS)

A abordagem considerada para a implementação do módulo Feature Manager Register, no caso da recepção por parte do MGC de uma mensagem de pedido de registo, foi a que está representada no diagrama da figura 29 e os seus pontos descritos em baixo.

1) O Feature Manager recebe no seu porto de escuta do MGC uma primitiva e verifica qual o seu *type*. No caso específico de registo, este deve ser *ServiceChange*. Se este não for um *type* válido, é enviada para o MGC uma primitiva de erro.

2) Comprovou-se que o *type* da mensagem recebida era do tipo *Service Change*. Agora, de acordo com os parâmetros recebidos relativamente ao POTS que se pretende registar, isto é, qual a A-MGW que controla esse POTS e qual o endereço do mesmo, o Feature Manager interage com o LBCD. Esta interacção tem como objectivo verificar se os dados contidos no LBCD possuem informação relativa à A-MGW e POTS que se pretende registar. Se tal se verificar pode-se afirmar que os parâmetros recebidos são válidos para prosseguir; caso contrário, é enviada para o MGC uma primitiva de erro.

3) Neste ponto já se sabe que a base de dados possui informação válida relativa ao POTS, mas tem de se verificar qual o *method* do *ServiceChange* que se pretende efectuar, podendo este ser de três tipos distintos: *Restart*, *Forced*, *Graceful*.

4) O *method* é *Restart*, mas, não faz sentido desperdiçar recursos a efectuar o registo de um POTS que já foi previamente registado. Assim, consulta-se a informação relativa ao mesmo e testa-se o estado de uma variável booleana, verificando se esta se encontra a TRUE ou FALSE. No caso de TRUE, é enviada uma primitiva de erro para o MGC.

5) Caso contrário, prossegue-se enviando uma primitiva para o IMS Agent de Registo com os parâmetros que este necessita para proceder à construção de um SIP *Register Request*.

- Desregisto dos terminais (POTS)

No caso de se pretender efectuar o desregisto de terminais ligados a determinada A-MGW a abordagem tida em conta para a implantação do módulo Feature Manager Register é idêntica à anterior considerando apenas a seguinte alteração no ponto 4:

6) O method é *Forced ou Graceful* e será enviada uma mensagem de erro, caso o terminal não se encontre registado.

Primitivas entre Feature Manager e Media Gateway Controller de registo

As primitivas possíveis de serem enviadas para o MGC por parte do FM, no âmbito do registo ou desregisto, encontram-se no ficheiro *bd_mensagens.h* . Estas possuem um código inicativo do tipo de acção que foi desencadeada e quais as suas consequências. De seguida, apresentam-se quatro das dez primitivas criadas:

- 200 OK Desregistado com sucesso

Esta primitiva é enviada quando um pedido de registo/desregisto é efectuado com sucesso no core IMS.

- Erro vindo do FM - type de mensagem enviada pelo MGC não reconhecido

Ocorre quando a informação que é enviada no campo *type* pelo MGC não é reconhecido pelo Feature Manager. Para o caso de registo, o mesmo deve ser do tipo ServiceChange.

- Erro vindo do FM - MGW ou POTS not valid in LBCD (bd_xml_reader.h)

Verifica-se quando os dados carregados da *Line Based Configuration Data* no arranque do FM não possuem referência a determinada A-MGW ou POTS que se pretende registar.

- 200 OK Registado com sucesso

Tal código é enviado na primitiva quando um pedido de registo é efectuado com êxito no *core*.

O FM encontra-se permanentemente à espera de registos/desregistos do módulo MGC, assim, os parâmetros contidos na LBCD são lidos e carregados no FM aquando do seu arranque, sendo apenas alterados - por exemplo a variável booleana que indica se determinado POTS se encontra registado - no caso de determinado registo/desregisto ser efectuado com sucesso.

Primitivas de registo entre Feature Manager e IMS Agent

Os campos da primitiva de registo trocada entre o FM e o IMS Agent são os seguintes:

```
struct message_fm_to_imsagent
{
      char type [20];
      char method [20];
      char sip_pub_uri[50];
      char sip_priv_uri[50];
      char display_name[50];
      char user_name[50];
      char auth[50];
      char ip_agcf[20];
      char pass [50];
      char domain[20];
}
```

type – indica o tipo de primitiva que está a ser enviada. No caso de registo, a primitiva em causa terá um *type* contendo um *ServiceChange*;

method – para o caso específico do *type* de *ServiceChange*, pode ser um *Restart* se se pretender efectuar um novo registo. Para desregisto, o *method* pode ser *Forced* ou *Graceful*, onde na primeira hipótese todas as conexões activas serão forçosamente desligadas e os terminais desregistados, enquanto na segunda se aguarda que as comunicações que se encontrarem activas terminem antes de efectuar o desregisto;

sip_pub_uri – indica o sip public uri do cliente (ex. sip:nunogil@ptinovacao.pt);

sip_priv_uri – indica o sip private uri do cliente (ex. sip:nunogil@ptinovacao.pt);

display_name – este campo possui o nome de utilizador do cliente (ex. Nuno Gil);

auth – authorization user name do POTS ligado à A-MGW (ex. nunogil@ptinovacao.pt);

ip_agcf – possui o endereço IP da máquina nativa onde se encontra a AGCF;

pass – possui a password necessária para o processo de registo;

domain – contém o domínio onde os terminais vão ser registados (ex. ptinocao.pt) ;

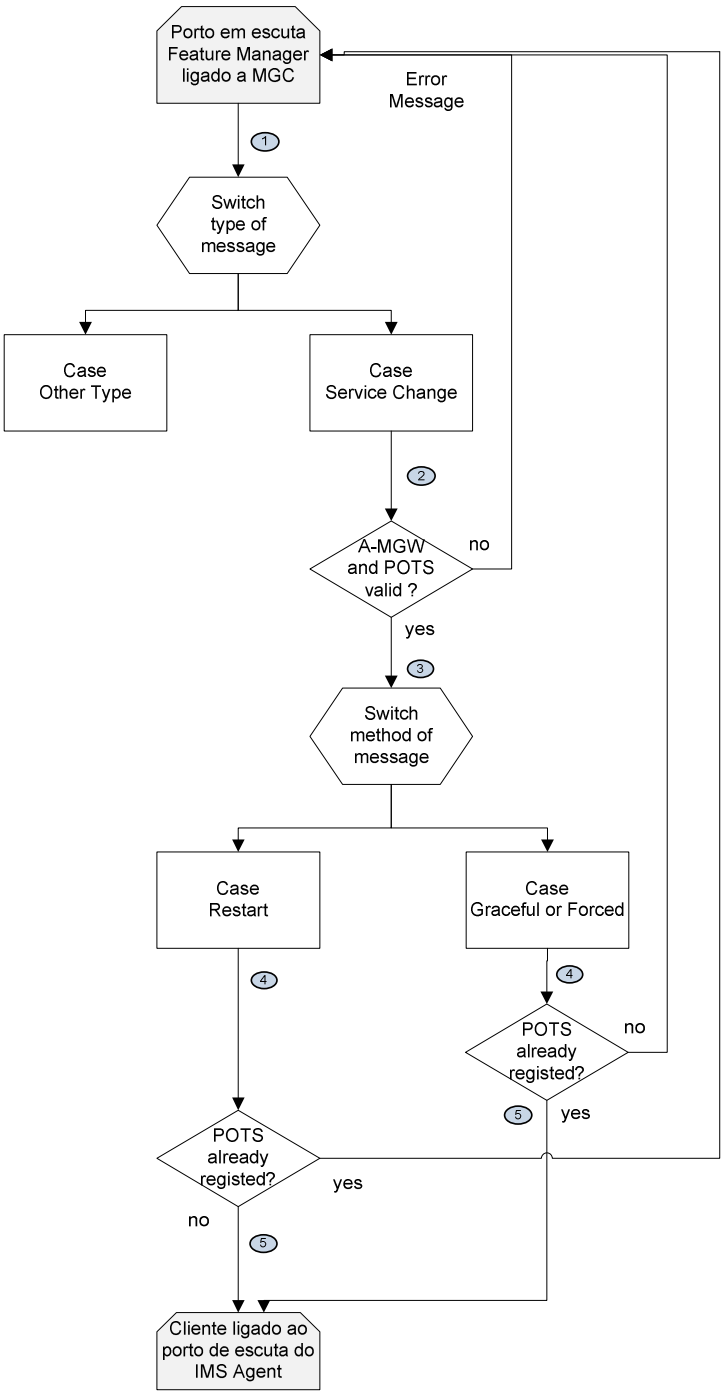


Figura 29 – Mensagem enviada no FM de ServiceChange

IMS Agent

O módulo IMS Agent pode ser descrito de uma forma prática como sendo a porta de comunicação com o *core*, enviando e recebendo mensagens do mesmo, utilizando o protocolo SIP, presente na *stack* interna da AGCF para efectuar esta intercomunicação.

Numa fase inicial, o registo será efectuado colocando o módulo IMS Agent a interagir com o P-CSCF do *core*.

A abordagem adoptada para a implementação do módulo IMS Agent, no caso da recepção de uma primitiva de registo, encontra-se apresentada no diagrama da figura 30 e os seus pontos a seguir apresentados:

1) O IMS Agent recebe do FM uma primitiva e verifica qual o conteúdo do campo *method*. No caso específico do processo de registo, pretende-se verificar se tal corresponde a um pedido de registo ou desregisto.

2) Se o type recebido for do tipo *Restart*, então o IMS Agent constata que se trata de um pedido de registo e coloca a variável *expires* com o valor de 3600 (*default value*). No caso deste ser do tipo *Graceful* ou *Forced*, esta variável adquire o valor 0, uma vez que se trata de um desregisto. De ter em conta que o campo *expires* representa, em segundos, o tempo que se pretende que o registo fique activo no core IMS. Através da *stack* SIP, são construídas as mensagens necessárias ao processo de registo/desregisto. Este módulo aguarda mensagens do core e é ele que é responsável por responder ao desafio e reportar ao FM o sucesso ou não do pedido efectuado.

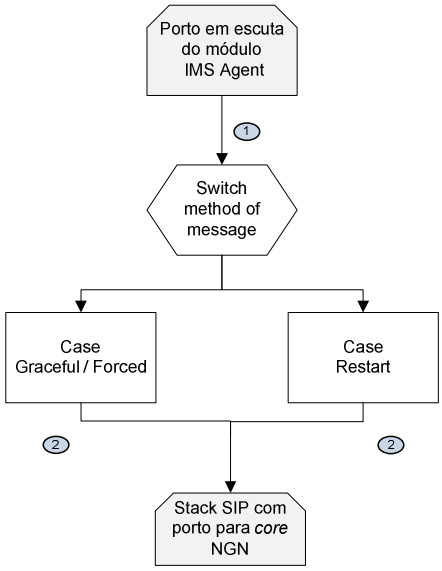


Figura 30 – Pedido de registo/desregisto no módulo IMS Agent

Mensagens entre IMS Agent e Core IMS

As mensagens possíveis de serem enviadas para o P-CSCF por parte do IMS Agent, no âmbito do registo ou desregisto, são:

- Enviar para o *core*, mais precisamente para o P-CSCF um SIP REGISTER*;*
- Receber mensagem SIP do tipo *401 Unauthorized – Challenging the UE*;

- Responder ao *Challange*, de acordo com os parâmetros recebidos do Feature Manager, e enviar um novo *SIP Register Request* para o Core IMS;

- Receber, por parte do *core*, mensagens de *200 OK*, informando que o registo foi efectuado com sucesso ou de erro, em caso de falha;

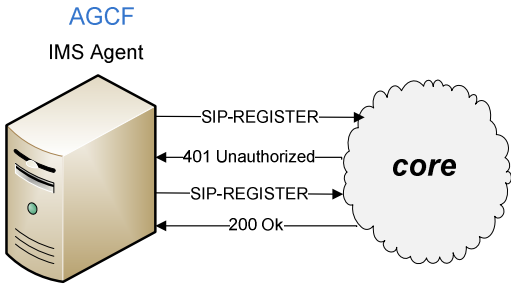


Figura 31 – Mensagens entre IMS Agent e *core* para efeito de registo

4.3.3 Testes

Para verificar o bom funcionamento dos três módulos implementados, foram criados vários cenários distintos de testes, onde aspectos como a existência de uma correcta interacção e a sua capacidade de processar correctamente todos os pedidos de registo, foram tidos em conta.

Os vários testes realizados e respectivos resultados encontram-se divididos em cinco grupos, consoante o aspecto específico a ser avaliado. Para tal, inicializaram-se os três módulos, cada um numa consola Linux, podendo-se, com recurso a vários *prints* de *debugging* e ao programa de captura de pacotes WireShark, averiguar o seu funcionamento.

Parâmetros não válidos por parte do Media Gateway Controller

Neste grupo de testes, pretende-se verificar a fiabilidade de comunicação entre os módulos internos da AGCF e mais especificamente a capacidade do módulo central FM de "filtrar" pedidos considerados como inválidos por parte do MGC. É de ter em conta que é esperado que o FM detecte todos os erros, de modo a evitar o envio desnecessário de primitivas para o módulo IMS Agent, e o consequente desperdício de recursos..

- Method não válido

Na consola do MGC forçou-se um comando com um parâmetro de entrada correspondente ao *method* a ser enviado na primitiva para o FM incorrecto, sendo este xxRestartxx.

Pretende-se que seja criado um canal de comunicação entre o MGC e o FM e que os parâmetros sejam enviados de forma correcta, sendo de prever que o FM verifique a invalidade do *method* recebido, enviando uma primitiva de erro de retorno para o MGC e nenhuma primitiva para o IMS Agent.

Media Gateway Controller:

```
gil@gil-laptop:~/Desktop/AGCF_nova/mgc/src$ ./mgc ServiceChange 123.456.123.456 al/trunk0/ts0@a-mgw1_addr.com xxRestartxx

 Recebeu de retorno do FM : 5

        Erro vindo do FM - Method do ServiceChange nao reconhecido
```

Feature Manager:

```
        --------- Parametros recebidos da MGC --------
type:  ServiceChange
reason: empty
mgw_adress:  123.456.123.456
terminationid:  al/trunk0/ts0@a-mgw1_addr.com
method:  xxRestartx
                --------  //  ---------

         ServiceChange - invocar FM_Service_Change

         AMGW valida

         POTS valido
```

Constatou-se que os parâmetros inseridos na MGC foram correctamente enviados para o FM, tendo este, por sua vez, detectado de forma correcta a invalidade do *method* recebido, enviando um código na primitiva de erro para o MGC, ilustrando o sucedido.

- Type não válido

Na consola do MGC forçou-se um comando com um parâmetro de entrada correspondente ao *type* a ser enviado na primitiva para o FM incorrecto, sendo este xxServicexx.

É criado um canal de comunicação que deve efectuar de forma correcta a transferência de primitivas entre o MGC e o FM, sendo esperado que este último detecte a invalidade do parâmetro recebido e que envie uma primitiva de erro para o MGC, indicando o sucedido. No que diz respeito ao módulo IMS Agent, este deve ficar em escuta de primitivas do FM, não recebendo neste caso nenhuma.

Media Gateway Controller:

```
gil@gil-laptop:~/Desktop/AGCF_nova/mgc/src$ ./mgc xxServicexx 123.456.123.abc al/trunk0/ts0@a-mgw1_addr.com Restart

 Recebeu de retorno do FM : 2

        Erro vindo do FM- type de mensagem enviada pelo MGC nao reconhecido
```

Feature Manager:

```
        --------- Parametros recebidos da MGC --------
type:  xxServicexx
reason: empty
mgw_adress:  123.456.123.abc
terminationid:  al/trunk0/ts0@a-mgw1_addr.com
method:  Restart
                --------- //  ---------

        type não reconhecido
```

Através dos resultados obtidos, constata-se, pelos *prints* de *debugging* nas consolas correspondentes ao módulo MGC e FM, que os parâmetros foram correctamente enviados e que o *type* não válido foi detectado, sendo criada e enviada uma primitiva, como seria de esperar.

- A-MGW não válida

Pretende-se testar a capacidade de rejeição do módulo FM aquando da recepção de um IP da A-MGW, inválido, que será passado para o MGC, erradamente, como: 123.456.123.abc, estando definido como 123.456.123.456 no documento XML que é "carregado" pelo FM no seu arranque.

Espera-se que o módulo MGC envie correctamente os parâmetros para o FM que, por sua vez, receberá o seguinte IP: 123.456.123.abc, devendo ser capaz de verificar que se trata de um IP inválido de acordo com a informação que consultou da LBCD, enviando, assim, uma mensagem de erro para o MGC. Mais uma vez o módulo IMS Agent não deve receber nada, ficando em escuta.

Media Gateway Controller:

```
gil@gil-laptop:~/Desktop/AGCF_nova/mgc/src$ ./mgc ServiceChange 123.456.123.abc al/trunk0/ts0@a-mgw1_addr.com Restart
 Recebeu de retorno do FM : 3

        Erro vindo do FM - MGW ou POTS not valid in LBCD ( bd_xml_reader.h )
```

Feature Manager:

```
        --------- Parametros recebidos da MGC --------
type:  ServiceChange
reason: empty
mgw_adress:  123.456.123.abc
terminationid:  al/trunk0/ts0@a-mgw1_addr.com
method:  Restart
                --------- //  ---------

        ServiceChange - invocar FM_Service_Change
```

Verifica-se que o FM detecta a falha no campo mgw_adress recebido, comparando-o com

aos parâmetros obtidos do LBCD, e envia uma primitiva para o MGC, indicando de forma correcta o erro ocorrido.

- Terminal (POTS) não válido

O parâmetro inválido será agora o *Termination ID* do POTS que se pretende registar, estará definido como al/trunk0/ts0@a-mgw1_addr.com na LBCD e será passado ao MGC como al/trunk0/ts01@a-mxxx_addr.com.

Mais uma vez, pretende-se que os parâmetros sejam correctamente enviados para o FM e que este consiga detectar a falha, enviando uma primitiva com um código de erro para o MGC.

Media Gateway Controller:

```
gil@gil-laptop:~/Desktop/AGCF_nova/mgc/src$ ./mgc ServiceChange 123.456.123.456 al/trunk0/ts0@a-mxxx_addr.com Restart
 Recebeu de retorno do FM : 3

        Erro vindo do FM - MGW ou POTS not valid in LBCD ( bd_xml_reader.h )
```

Feature Manager:

```
        --------- Parametros recebidos da MGC --------
type:  ServiceChange
reason: empty
mgw_adress:  123.456.123.456
terminationid:  al/trunk0/ts0@a-mxxx_addr.com
method:  Restart
                --------- //  ---------

        ServiceChange - invocar FM_Service_Change

        AMGW valida
```

Comprovou-se que os parâmetros foram correctamente passados de um módulo para o outro e o erro foi detectado pelo FM enviando uma primitiva de erro para o MGC como seria de esperar.

Tentativa de registo de terminal que já fora previamente registado

Neste caso, pretende-se registar um terminal que já se encontra registado, não se devendo desperdiçar recursos desnecessariamente. De forma a indicar que o terminal já fora previamente registado, actualiza-se o valor da variável booleana responsável por tal informação no ficheiro XML (esta adquire o valor 1). O passo seguinte para efectuar o teste é enviar um pedido de registo por parte de um terminal válido na LBCD, do MGC para o FM.

Este último deve possuir informação actualizada sobre o referido terminal, isto é, saber que este já se encontra registado, enviando para o MGC uma primitiva de erro informando o sucedido. O IMS Agent não deve receber nenhuma primitiva, continuando em espera de pedidos

como se nada tivesse acontecido, conseguindo-se desta forma reduzir a número de recursos e o esforço por parte da AGCF.

De futuro este tipo de tentativa de reregisto poderá ser encarado como uma renovação do tempo que o utilizador se encontra registado. Assim, o pedido seria aceite pelo FM, desde que este validasse a informação recebida, e enviaria uma primitiva para o IMS Agent como se de um pedido de registo inicial se tratasse tendo em conta o tempo presente no campo *Expires*.

Media Gateway Controller:

```
gil@gil-laptop:~/Desktop/AGCF_nova/mgc/src$ ./mgc ServiceChange 123.456.123.456 al/trunk0/ts0@a-mgw1_addr.com Restart

 Recebeu de retorno do FM : 4

        Erro vindo do FM - POTS já registado
```

Feature Manager:

```
gil@gil-laptop:~/Desktop/AGCF_nova/feature_menager/src$ ./FM
  conteudo de newsock :  4


        --------- Parametros recebidos da MGC --------
type:  ServiceChange
reason: empty
mgw_adress:  123.456.123.456
terminationid:  al/trunk0/ts0@a-mgw1_addr.com
method:  Restart
                ---------  //  ---------

         ServiceChange - invocar FM_Service_Change

         AMGW valida

         POTS valido
```

Como seria de esperar, comprova-se que, aquando da recepção do pedido de registo, o módulo FM consulta a informação relativa ao POTS e constata que este já fora previamente registado (variável booleana a 1), não construindo a primitiva a ser enviada para o IMS Agent e informando o MGC do sucedido através de uma primitiva de erro.

Tentativa de desregisto de terminal que não se encontra registado

Agora pretende-se efectuar o oposto da situação anterior, efectuando um pedido de desregisto de um terminal que não havia sido registado. Assim, envia-se uma primitiva de desregisto para o FM, a qual possui campos correctos referentes a um terminal que se encontre presente nos dados carregados inicialmente do LBCD.

O esperado será que o FM detecte tal incoerência não permitindo que o pedido de desregisto seja enviado para o módulo IMS Agent, enviando, sim, uma primitiva de erro para o

MGC com um código identificativo do sucedido.

Media Gateway Controller:

```
gil@gil-laptop:~/Desktop/AGCF_nova/mgc/src$ ./mgc ServiceChange 123.456.123.456 al/trunk0/ts0@a-mgw1_addr.com Forced

 Recebeu de retorno do FM : 7

        Tentativa de DESregisto de POTS que não se encontra registado
```

Feature Manager:

```
gil@gil-laptop:~/Desktop/AGCF_nova/feature_menager/src$ ./FM
  conteudo de newsock :  4


        --------- Parametros recebidos da MGC --------
type:  ServiceChange
reason: empty
mgw_adress:  123.456.123.456
terminationid:  al/trunk0/ts0@a-mgw1_addr.com
method:  Forced
                 ---------  //  ---------

         ServiceChange - invocar FM_Service_Change

         AMGW valida

         POTS valido
```

Pode-se comprovar que o módulo FM testa eficazmente a variável booleana que controla o estado – registado/não registado – verificando que esta se encontra com o valor 0, enviando uma primitiva de erro para o MGC informando-o que tal POTS não se encontra registado. Mais uma vez, como esperado, o IMS Agent não recebe qualquer primitiva por parte do FM.

Tentar registo sem ligação ao core estabelecida

Neste teste, o objectivo é tentar efectuar um registo quando a AGCF se encontra na situação em que o core não está acessível. Para tal, desligou-se a ligação Eth. à rede, impossibilitando, assim, o módulo IMS Agent de comunicar com o exterior.

É esperado que o IMS Agent informe de forma eficiente o FM da falha de registo e que este, por sua vez, o comunique ao MGC.

Media Gateway Controller:

```
gil@gil-laptop:~/Desktop/AGCF_nova/mgc/src$ ./mgc ServiceChange 123.456.123.456 al/trunk0/ts0@a-mgw1_addr.com Restart

 Recebeu de retorno do FM : 8

        Registo não efectuado com sucesso no core IMS
```

Feature Manager:

```
        --------- Parametros recebidos da MGC --------
type:  ServiceChange
reason: empty
mgw_adress:  123.456.123.456
terminationid:  al/trunk0/ts0@a-mgw1_addr.com
method:  Restart
                 ---------  //  ---------

         ServiceChange - invocar FM_Service_Change

         AMGW valida

         POTS valido

         Enviou mensagem fm_ims para o socket de escuta do IMS_AGENT

 o que recebeu de retorno do IMS_AGENT: 8

        Registo não efectuado com sucesso no core IMS
```

IMS Agent:

```
         --------- Parametros recebidos do Feature Manager --------
 type:  Register-Request
 method: Restart
 sip_pub_uri:  sip:nunogil@ptinovacao.pt
 sip_priv_uri:  sip:nunogil@ptinovacao.pt
 display_name:  Nuno Gil
 user_name:  nunogil
 authorization name: nunogil@ptinovacao.pt
 ip_agcf: 192.168.127.86
 pass:  nunogil
 domain:  ptinovacao.pt

          ---------  //  ---------

          IMS_AGENT_Restart

 Campos para eXosip_add_authentication_info

  username : nunogil
  author : nunogil@ptinovacao.pt
  password : nunogil
  realm : ptinovacao.pt

  ----------------   //    --------------

 Campos para eXosip_register_build_initial_register

  fromuser : sip:nunogil@ptinovacao.pt
  proxy : sip:ptinovacao.pt
  contact : sip:nunogil@192.168.127.86
  expires : 3600

  ----------------   //    --------------

 passou....1 e 3
 registration failed
```

Tal como seria de esperar, não se obteve sucesso no processo de registo e verificou-se que o fluxo de primitivas foi devidamente efectuado entre os módulos da AGCF. Isto é, todos os parâmetros estavam correctos e válidos na LBCD e o POTS não fora previamente registado. Assim, o pedido de registo foi correctamente enviado para o módulo IMS Agent que o processou e tentou enviar para o *core*.

Registo e desregisto com parâmetros correctos

Neste grupo de testes pretende-se averiguar a fiabilidade da AGCF relativamente à capacidade de efectuar um pedido de registo e desregisto de forma eficiente. Espera-se que haja uma correcta intercomunicação entre os módulos da AGCF e que o pedido seja devidamente processado e enviado para o core. O IMS Agent deve aguardar uma resposta, primeiro um 401 e depois um 200, e processá-las de forma correcta, sendo no final de todo o processo o MGC informado do sucedido.

- Registo

Para efectuar um registo de forma correcta inserem-se parâmetros de entrada no MGC que sejam válidos, isto é, A-MGW e POTS presentes na LBCD, *type* correcto e *method* válido.

Se o registo for efectuado com sucesso no *core*, então o módulo IMS Agent, após todo o processo necessário, recebe por fim uma primitiva SIP de *200 OK* que deve ser interpretada de forma correcta e comunicada ao FM, o qual, por sua vez, actualizará a variável booleana relativa ao registo desse terminal na LBCD e comunicará o sucesso de todo o processo ao MGC.

Media Gateway Controller:

```
gil@gil-laptop:~/Desktop/AGCF_nova/mgc/src$ ./mgc ServiceChange 123.456.123.456 al/trunk0/ts0@a-mgw1_addr.com Restart
 Recebeu de retorno do FM : 9

        200 OK Novo Registo efectuado com sucesso 200 OK
```

Feature Manager:

```
gil@gil-laptop:~/Desktop/AGCF_nova/feature_menager/src$ ./FM
  conteudo de newsock :  4


        --------- Parametros recebidos da MGC --------
type:  ServiceChange
reason: empty
mgw_adress:  123.456.123.456
terminationid:  al/trunk0/ts0@a-mgw1_addr.com
method:  Restart
                 ---------  //  ---------

         ServiceChange - invocar FM_Service_Change

         AMGW valida

         POTS valido

         Enviou mensagem fm_ims para o socket de escuta do IMS_AGENT

 o que recebeu de retorno do IMS_AGENT: 9

        200 OK NOVO Registo efectuado com sucesso 200 OK

 enviou o que recebeu do IMS Agent para o MGC
```

IMS Agent:

```
        --------- Parametros recebidos do Feature Manager --------
type:  Register-Request
method: Restart
sip_pub_uri:  sip:nunogil@ptinovacao.pt
sip_priv_uri:  sip:nunogil@ptinovacao.pt
display_name:  Nuno Gil
user_name:  nunogil
authorization name: nunogil@ptinovacao.pt
ip_agcf: 192.168.127.86
pass:  nunogil
domain:  ptinovacao.pt

         ---------  //  ---------

         IMS_AGENT_Restart

Campos para eXosip_add_authentication_info

 username : nunogil
 author : nunogil@ptinovacao.pt
 password : nunogil
 realm : ptinovacao.pt

 ----------------   //    --------------

Campos para eXosip_register_build_initial_register

 fromuser : sip:nunogil@ptinovacao.pt
 proxy : sip:ptinovacao.pt
 contact : sip:nunogil@192.168.127.86
 expires : 3600

 ----------------   //    --------------

passou....1 e 3

registrered successfully
```

Pacotes capturados (wireshark):

No.	Time	Source	Destination	Protocol	Info
3	0.011565	192.168.127.86	192.168.21.61	SIP	Request: REGISTER sip:ptinovacao.pt
4	0.197320	192.168.21.61	192.168.127.86	SIP	Status: 401 Unauthorized - Challenging the UE (0 bindings)
7	0.207441	192.168.127.86	192.168.21.61	SIP	Request: REGISTER sip:ptinovacao.pt
8	0.423304	192.168.21.61	192.168.127.86	SIP	Status: 200 OK - SAR succesful and registrar saved (1 bindings)

Através dos resultados obtidos pelos *prints* de *debugging* nas consolas correspondentes ao módulo MGC, FM, IMS Agent e da análise aos pacotes capturados, verifica-se que todo o processo de registo se desenrola conforme o esperado. Confirma-se também uma correcta intercomunicação entre todos os módulos intervenientes, sendo a troca de primitivas efectuada de forma eficaz.

A figura 32 apresenta com mais detalhe os pacotes capturados, ilustrando como toda a troca de mensagens entre o IMS Agent e o *core* foi efectuada no âmbito do processo de registo.

Figura 32 - Pacotes de registo

- Desregisto

Para efectuar um desregisto, o procedimento é idêntico ao descrito no caso anterior, tendo como única diferença o facto de o campo *expires* possuir o valor 0. No entanto, do ponto de vista dos testes efectuados, tal é encarado como um registo onde o *method* é Graceful ou Forced.

Media Gateway Controller:

```
gil@gil-laptop:~/Desktop/AGCF_nova/mgc/src$ ./mgc ServiceChange 123.456.123.456 al/trunk0/ts0@a-mgw1_addr.com Forced
 Recebeu de retorno do FM : 1

        200 OK DESREGISTADO com sucesso
```

Feature Manager:

```
gil@gil-laptop:~/Desktop/AGCF_nova/feature_menager/src$ ./FM
  conteudo de newsock :  4


        --------- Parametros recebidos da MGC --------
type:  ServiceChange
reason: empty
mgw_adress:  123.456.123.456
terminationid:  al/trunk0/ts0@a-mgw1_addr.com
method:  Forced
                 ---------  //  ---------

         ServiceChange - invocar FM_Service_Change

         AMGW valida

         POTS valido

         Enviou mensagem fm_ims para o socket de escuta do IMS_AGENT

 o que recebeu de retorno do IMS_AGENT: 9

        200 OK DESREGISTADO

 enviou o que recebeu do IMS Agent para o MGC
```

IMS Agent:

```
gil@gil-laptop:~/Desktop/AGCF_nova$ sudo ims_agent_reg

        --------- Parametros recebidos do Feature Manager --------
type:  Deregister-Request
method: Forced
sip_pub_uri:  sip:nunogil@ptinovacao.pt
sip_priv_uri:  sip:nunogil@ptinovacao.pt
display_name:  Nuno Gil
user_name:  nunogil
authorization name: nunogil@ptinovacao.pt
ip_agcf: 192.168.127.86
pass:  nunogil
domain:  ptinovacao.pt

        IMS_AGENT_Graceful_or_Forced

Campos para eXosip_add_authentication_info

 username : nunogil
 author : nunogil@ptinovacao.pt
 password : nunogil
 realm : ptinovacao.pt

 ----------------   //    --------------

Campos para eXosip_register_build_initial_register

 fromuser : sip:nunogil@ptinovacao.pt
 proxy : sip:ptinovacao.pt
 contact : sip:nunogil@192.168.127.86
 expires : 0

 ----------------   //    --------------

passou....1 e 3

registrered successfully
```

Pacotes capturados:

No.	Time	Source	Destination	Protocol	Info
18	2.326606	192.168.127.86	192.168.21.61	SIP	Request: REGISTER sip:ptinovacao.pt
19	2.493230	192.168.21.61	192.168.127.86	SIP	Status: 401 Unauthorized - Challenging the UE (0 bindings)
22	2.512277	192.168.127.86	192.168.21.61	SIP	Request: REGISTER sip:ptinovacao.pt
23	2.730042	192.168.21.61	192.168.127.86	SIP	Status: 200 OK - SAR succesful and registrar saved (1 bindings)

Verifica-se mais uma vez que o pedido de desregisto, com o campo *expires* a 0, foi efectuado com sucesso, tendo em conta a análise das consolas correspondentes aos módulos envolvidos e aos pacotes capturados.

Apresenta-se na figura 33 uma descrição detalhada da troca de mensagens SIP capturada.

Figura 33 – Pacotes de desregisto

4.4 Chamada

Este ponto é referente a todo o processo de chamada, onde, inicialmente, será explicado o método escolhido para dotar a AGCF com funcionalidades de efectuar e receber pedidos de chamadas, o que corresponde a criar o subsistema denominado *Session Processing* apresentado na figura 38. Todo um conjunto de testes foi efectuado com o intuito de verificar a robustez da solução implementada, sendo os mesmos descritos e os resultados apresentados também dentro deste subcapítulo.

Este ponto abrange os seguintes requisitos referidos no Capitulo 4 - RF.AGCF-MDL.1, RF.AGCF-MDL.2, RF.AGCF-MDL.3, RISE.AGCF-PR.1, RISE.AGCF-PR.2, RISE.AGCF-PR.7, RISE.AGCF-PR.8.

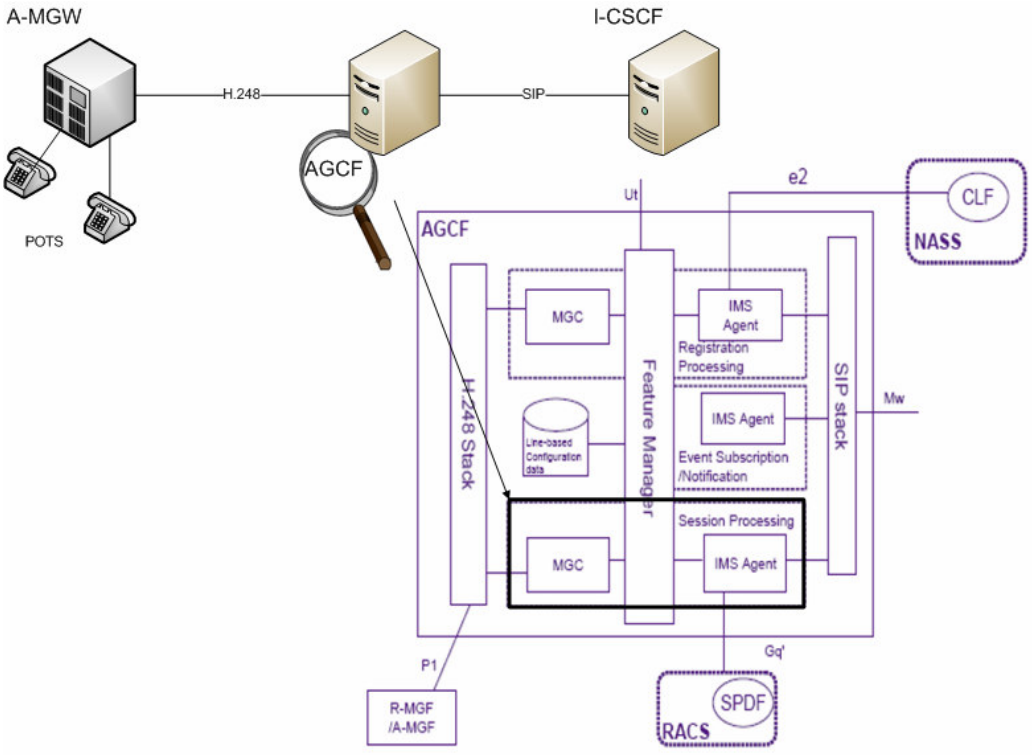


Figura 34 – Módulo Session Processing

4.4.1 Objectivo geral

Com o intuito de dotar a AGCF com capacidades que permitem aos POTS a ela associados de estabelecerem chamadas, foi efectuada uma pesquisa de como todo este processo se desenrola. Dois novos conceitos associados a termos que foram utilizados para descrever acções verificadas num terminal analógico devem ser apresentados: o *on-hook* que se verifica quando o auscultador se encontra pousado no terminal; quando este é levantado tal acção é designada de *off-hook*.

De uma forma geral, o módulo MGC recebe um aviso de que o auscultador de determinado terminal foi levantado (*off-hook*), recebendo depois um pedido de estabelecimento de chamada que é enviado para o FM. Este consulta a LBCD de forma a retirar informação relativa ao cliente associado ao POTS em questão e envia uma primitiva para o IMS Agent com os dados necessários para este proceder à construção e envio de um SIP Request. De seguida, é recebida informação sobre o estado do pedido, por exemplo uma mensagem SIP de 180 *Ringing*, e em caso de a chamada ser aceite, uma mensagem de 200 OK. Nesta fase, é trocada a informação media e quando um dos utilizadores desliga, é enviada uma mensagem ao outro utilizador que por sua vez acarreta o fecho da sessão respondendo com um 200 OK. Este processo encontra-se exemplificado na figura 35, ilustrando um pedido por parte de o utilizador A para o B.

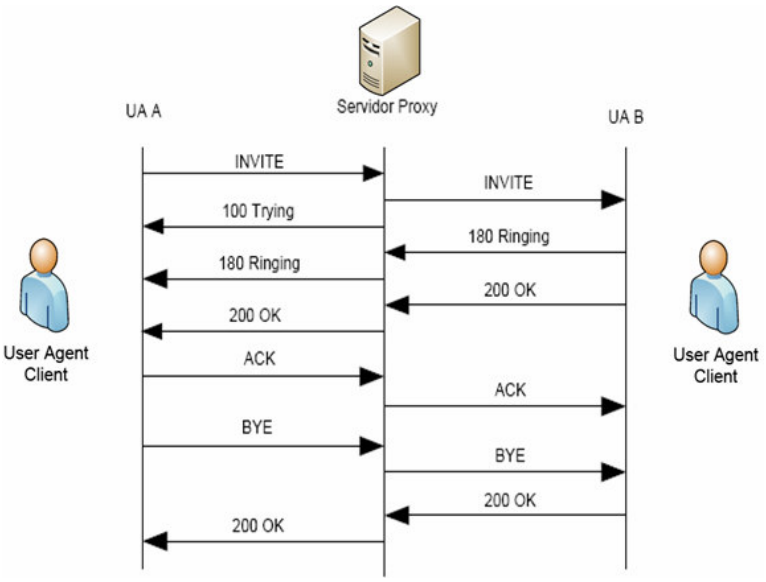


Figura 35 – Troca de mensagens chamada

De uma forma geral as funcionalidades que cada módulo interno da AGCF deve suportar, tendo como objectivo o processamento de pedidos de sessões de voz (chamadas) no *core* NGN, são as em baixo descritas.

Media Gateway Controller

- •Receber por parte da A-MGW eventos descritivos do estado dos POTS e pedidos de estabelecimento de chamada;
- •Enviar para o Feature Manager os pedidos com os respectivos parâmetros informativos referentes à identificação do POTS que pretende estabelecer uma sessão;
- •Receber por parte do FM primitivas informativas sobre o estado do pedido.

Feature Manager

•Receber por parte da MGC informações sobre o estado actual dos POTS e pedidos de estabelecimento de sessões por parte dos mesmos;

•Interagir com o LBCD, de forma a obter dados relativos ao POTS que pretende efectuar uma chamada e/ou actualizar o estado de determinado POTS;

•Enviar para o IMS Agent um Setup Request com os dados adquiridos no ponto anterior;

•Receber do IMS Agent primitivas informativas sobre o decorrer do estabelecimento da sessão, por exemplo 486 *Busy Here* ou 200 OK;

•Enviar para o MGC primitivas sobre o estado da sessão.

IMS Agent

•Receber por parte do FM pedidos de estabelecimento de chamada;

•Construir mensagens SIP INVITE com base nos parâmetros recebidos tirando partido da *stack* SIP;

•Enviar para o core, mais precisamente para o I-CSCF um SIP INVITE;

•Receber, por parte do core, mensagens informando o estado do decorrer do pedido;

•Enviar primitivas para o FM informando-o do estado do processo;

Outro aspecto importante prende-se com a interacção dos três módulos da arquitectura interna da AGCF intervenientes no processo de registo. Esta deve ser rápida e efectuada de forma bem coordenada, sob pena de um incorrecto funcionamento da AGCF.

4.4.2 Funcionalidades implementadas

- **Funcionalidades Gerais**

Tendo em conta que a AGCF é responsável por manter, na sua base de dados, informação relativa ao estado actual de cada POTS e que nesta fase surgiram os conceitos de *off-hook* e *on-hook*, foi necessário adicionar um novo campo (variável booleana) para o LBCD possui informação actualizada do estado dos POTS.

Aquando da projecção de qual a solução a ser implementada para dotar a AGCF de funcionalidades que permitissem o processamento de pedidos de chamadas bem como, no futuro, a sua recepção, foi necessário introduzir o conceito de *threads*. Isto é, a AGCF controla determinada gateway à qual se encontram ligados vários POTS e, deve ser prevista, não a situação mínima onde apenas um POTS, de cada vez estaria a ser utilizado, mas sim a situação extrema onde todos os POTS estão ocupados e pretendem efectuar ou receber chamadas. Assim, o conceito de *thread* permite que a AGCF consiga dar resposta a todos os pedidos que recebe sob um conceito de concorrência e paralelismo.

- **Funcionalidades Específicas**

É de referir que existem aspectos que não serão novamente objecto de descrição detalhada uma vez que já o foram no subcapítulo anterior – Registo/Desregisto - tais como:

- comunicação entre os módulos e primitivas trocadas entre os mesmos;
- descrições detalhadas de cada módulo

- Media Gateway Controller

Este elemento encontra-se a aguardar pedidos por parte das *Gateways* sendo lançado um processo por cada pedido recebido. O diagrama da figura 36 apresenta o seu funcionamento.

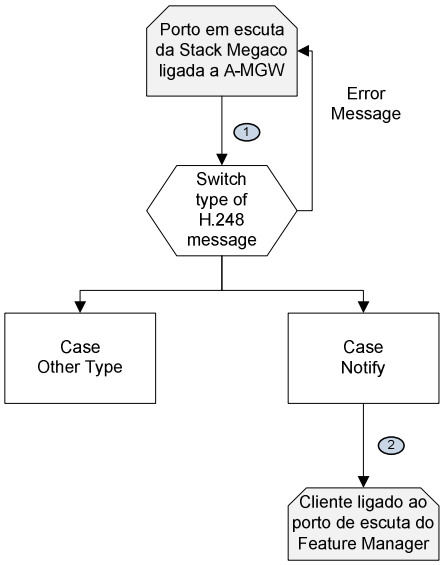


Figura 36 – Mensagem recebida no MGC de Setup Request

1) O *Media Gateway Controller* recebe no seu porto de escuta uma mensagem H.248 e verifica qual o seu tipo. Caso não seja reconhecido, é enviada uma primitiva de erro para a A-MGW emissora do pedido.

2) Comprovou-se que o tipo da mensagem recebida era *Notify*. Agora é criado um processo e - de acordo com os parâmetros recebidos relativamente ao POTS que pretende efectuar a chamada, isto é, em função da A-MGW que controla esse POTS e do endereço do mesmo - é enviada uma primitiva para o Feature Manager, indicando o pedido que se pretende efectuar.

Deve ser tido em conta que a troca de mensagens entre a *gateway* e a AGCF para efectuar uma chamada, não se resume à recepção por parte da AGCF de um comando NOTIFY. O processo engloba algumas transacções, como por exemplo a notificação da ocorrência de um off-hook, entre as duas entidades. De seguida, é efectuada uma descrição da troca de mensagens

que deveria ser tida em conta caso a *stack* MEGACO se encontrasse instalada e a AGCF ligada a uma *gateway* aquando da fase inicial de um pedido de chamada. Todos os comandos e descritores foram abordados no Capítulo 2 na altura em que foi feita a apresentação do protocolo MEGACO/H.248.

1) (AGCF →A-MGW) : AGCF envia um comando MODIFY para a terminação do cliente na A-MGW com os seguintes descritores: verificar o evento off/on-hook, *dialtone*, *digitmap*.

2) (CLIENTE →A-MGW) : O cliente tira o telefone do gancho (*off-hook*).

3) (A-MGW → AGCF) : A-MGW detecta a mudança de estado e gera o comando NOTIFY. Este possui o descritor de *Observedevents* informando a mudança de estado à AGCF.

4) (AGCF → A-MGW) : AGCF envia um NOTIFY *reply* confirmando o processamento da mensagem recebida

5) (AGCF →A-MGW) : AGCF responde ao NOTIFY enviando um comando MODIFY para a A-MGW colocar o *dialtone* e preparar-se para a recepção de dígitos pelo cliente.

6) (A-MGW → CLIENTE) O cliente recebe o *dialtone*.

7) (A-MGW → AGCF): A.-MGWresponde à AGCF com um MODIFY *reply*.

8) (CLIENTE →A-MGW): A-MGW recebe os dígitos gerados pelo cliente.

9) (A-MGW → AGCF): A-MGW envia a sequência recebida através de um comando NOTIFY.

- Feature Manager

O módulo Feature Manager é, como se sabe, responsável pela coordenação dos restantes e possui acesso à base de dados da AGCF. Para este elemento, a abordagem tida em consideração encontra-se representada no diagrama da figura 37 e os pontos descritos de seguida.

Há que ter presente que, no futuro, esta abordagem será precedida da recepção de uma primitiva *Session-Attemp*, a qual permitirá alterar o estado do POTS na LBCD de on-hook para off-hook.

1) O Feature Manager recebe no seu porto de escuta do MGC uma primitiva e lança um processo para tratar a mesma, o qual verifica o seu *type*. No caso específico de chamada este deve ser *SetupRequest*. Se este não for um *type* válido, é enviada para o MGC uma primitiva de erro.

2) Comprovou-se que o *type* da mensagem recebida era do tipo *SetupRequest*. Agora de acordo com os parâmetros recebidos relativamente ao POTS que pretende efectuar uma sessão, isto é, qual a A-MGW que controla esse POTS e qual o endereço do mesmo, o FM interage com o LBCD. Esta interacção tem como objectivo verificar se os dados contidos no LBCD possuem informação relativa à A-MGW e POTS que se pretende efectuar a chamada. Se tal se verificar, então pode-se afirmar que os parâmetros recebidos são válidos para prosseguir, caso contrário é enviada para o MGC uma primitiva de erro.

3) Neste ponto já se sabe que a base de dados possui informação válida relativa ao POTS, mas tem que se verificar se este se encontra registado e no estado *off-hook* (entretanto poderia ter ocorrido um *on-hook*).

4) O pedido recebido do MGC cumpre todos os requisitos para que o FM envie uma primitiva para o módulo IMS Agent com o pedido de chamada.

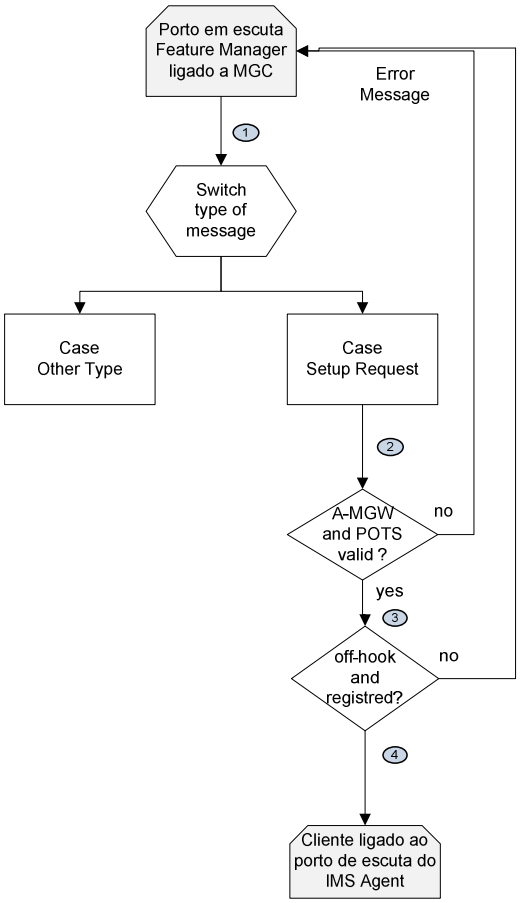


Figura 37 – Mensagem enviada no FM de SetupRequest

IMS Agent

O módulo IMS Agent pode ser descrito de uma forma prática como sendo a porta de comunicação com o *core*, enviando e recebendo mensagens do mesmo, utilizando o protocolo SIP presente na *stack* interna da AGCF para efectuar esta intercomunicação.

A abordagem adoptada para a implementação do módulo IMS Agent, no caso da recepção de uma primitiva de chamada, encontra-se apresentada no diagrama da figura 38 e os nos pontos seguintes:

1) O IMS Agent recebe do FM uma primitiva e verifica qual o conteúdo do campo *type*. No caso específico de chamada este deve ser um *SetupRequest* e é lançado um processo independente para tratar este pedido específico.

2) Através da SIP *stack* é enviado um INVITE para o *core* e este módulo fica a aguardar todas as respostas sobre este pedido encaminhando-as para o FM.

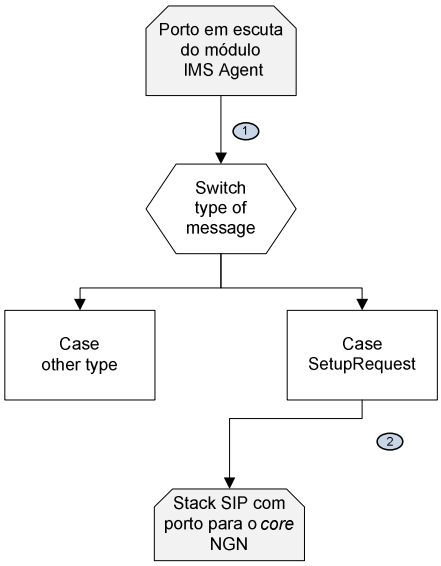


Figura 38 – Pedido de chamada no módulo IMS Agent

4.4.3 Testes

Com o intuito de verificar o correcto funcionamento do módulo Session Processing da arquitectura interna da AGCF, foram realizados vários testes. Inicialmente, estes foram efectuados na situação base em que apenas um cliente pretende realizar determinada operação. Após se ter verificado o bom funcionamento neste caso, passou-se para uma situação mais realista onde existem vários clientes a tirar partido das funcionalidades da AGCF.

Situações que pretendiam pôr à prova a fiabilidade do módulo FM, no que diz respeito a detectar parâmetros não válidos por parte do MGC, foram já testados na parte de Registo/Desregisto, pelo que não serão repetidas.

1 Cliente

Os testes que se seguem correspondem à situação em que um POTS de determinado cliente pretende efectuar uma chamada. O cenário simulado encontra-se descrito na figura 39.

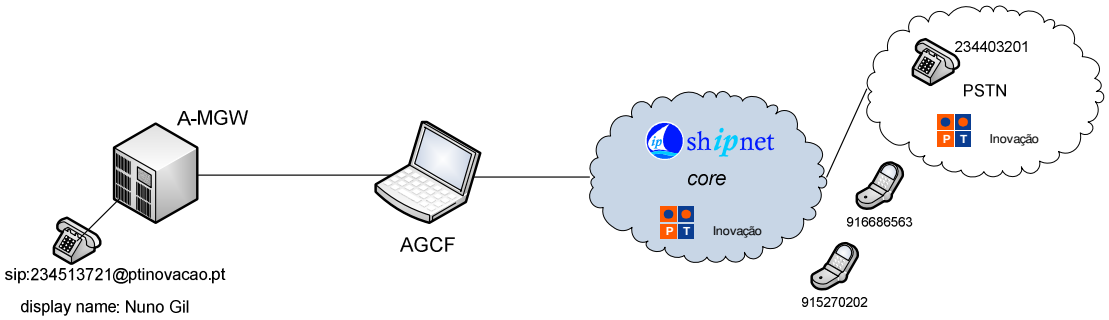


Figura 39 – Cenário para testes com 1 POTS

Os testes encontram-se divididos consoante a situação específica a ser testada. O cliente será Nuno Gil e o terminal de destino 234403201 ou 915270202.

- O destino rejeita a chamada sem atender

Neste caso pretende-se testar a situação em que o destino desliga a chamada sem chegar a atender. Inicialmente, é esperado que todo o fluxo de mensagens no sentido MGC-FM-IMS Agent seja efectuado de forma correcta. De seguida, pretende-se que todo o processo seja relatado, em tempo real e com veracidade, ao IMS Agent, e que este proceda de igual modo para com o FM e este, por sua vez, para com o MGC.

- Media Gateway Controller:

```
gil@gil-laptop:~/Desktop/AGCF_nova_testes/mgc/src$ ./mgc_sess SetupRequest 123.456.123.456 al/trunk0/ts0@a-mgw1_addr.com 915270202

        Mensagem do FM- 180 Ringing

        Mensagem do FM- Chamada foi rejeitada pelo utilizador

        Mensagem do FM- Call Released (chamada libertada)
```

- Feature Manager:

```
gil@gil-laptop:~/Desktop/AGCF_nova_testes/feature_menager/src$ ./FM_2


       --------- Parametros recebidos da MGC --------
type:  SetupRequest
reason: empty
mgw_adress:  123.456.123.456
terminationid:  al/trunk0/ts0@a-mgw1_addr.com
method:  0
to:  915270202
                ---------  //  ---------

         AMGW valid

         POTS valid

         Setup-Request - invocar FM_Setup_Request

         Entrou FM_Setup-Request

         Enviou mensagem fm_ims para o socket de escuta do IMS_AGENT

         Telefone a tocar

 enviou o que recebeu do IMS Agent para o MGC


         Boolean do toca está a: 1
         Chamada foi regeitada pelo utilizador
```

- IMS Agent:

```
gil@gil-laptop:~/Desktop/AGCF_nova_testes/ims_agent_sess/src$ ./ims_agent_sess
1
        --------- Parametros recebidos do Feature Manager --------
type:  SetupRequest
method: not aplicable
sip_pub_uri:  sip:nunogil@ptinovacao.pt
sip_priv_uri:  sip:nunogil@ptinovacao.pt
display_name:  Nuno Gil
user_name:  nunogil
authorization name: nunogil@ptinovacao.pt
ip_agcf: 192.168.127.86
pass:  nunogil
domain:  ptinovacao.pt
to:  915270202
```

Pacotes capturados (wireshark):

No.	Time	Source	Destination	Protocol	Info
145	154.3	192.168.127.86	192.168.21.61	SIP/SDP	Request: INVITE sip:+351915270202@ptinovacao.pt, with session description
146	154.3	192.168.21.61	192.168.127.86	SIP	Status: 100 Trying
213	160.4	192.168.21.61	192.168.127.86	SIP/SDP	Status: 180 Ringing, with session description
554	171.5	192.168.21.61	192.168.127.86	SIP	Status: 486 Busy Here
557	171.5	192.168.127.86	192.168.21.61	SIP	Request: ACK sip:+351915270202@ptinovacao.pt

Através dos resultados obtidos pelos *prints* de *debugging* nas consolas correspondentes ao módulo MGC, FM e IMS Agent e da observação aos pacotes capturados, verifica-se que todo o processo de chamada se processa conforme o esperado. Uma análise mais detalhada aos pacotes recebidos será efectuada mais adiante, de forma a não se repetir constantemente este estudo. Aqui, apenas deve ser retido que após a recepção da mensagem SIP 100 *Trying*, confirmando o sucesso do pedido de chamada, é recebida uma outra com o código 486 associado ao estado *Busy Here* que ilustra o estado do destino tal como seria de esperar.

Outro aspecto a considerar é que, daqui em diante não serão mais apresentados os prints de debugging do módulo FM, uma vez que este é intermédio entre os extremos da AGCF. Assim, se tudo estiver bem no MGC e IMS Agent, tal significa que também o terá de estar com o FM.

- O terminal de destino não responde

Neste caso pretende-se testar a fiabilidade de todo o processo quando o terminal de destino toca sem que qualquer acção seja tomada. Ora, não é de todo pretendido que este fique interminavelmente a tocar, esperando-se obter uma resposta identificativa do sucedido e que esta seja transferida até ao MGC. Assim, o cliente não fica indefinidamente a ouvir o sinal de chamada.

- Media Gateway Controller:

```
gil@gil-laptop:~/Desktop/AGCF_nova_testes/mgc/src$ ./mgc_sess SetupRequest 123.456.123.456 al/trunk0/ts0@a-mgw1_addr.com 915270202

        Mensagem do FM- 180 Ringing

        Mensagem do FM - Operador nao conseguiu estabelecer chamada

        Mensagem do FM- Call Released (chamada libertada)
```

- IMS Agent:

```
gil@gil-laptop:~/Desktop/AGCF_nova_testes/ims_agent_sess/src$ ./ims_agent_sess
1
        --------- Parametros recebidos do Feature Manager --------
type:  SetupRequest
method: not aplicable
sip_pub_uri:  sip:nunogil@ptinovacao.pt
sip_priv_uri:  sip:nunogil@ptinovacao.pt
display_name:  Nuno Gil
user_name:  nunogil
authorization name: nunogil@ptinovacao.pt
ip_agcf: 192.168.127.86
pass:  nunogil
domain:  ptinovacao.pt
to:  915270202
```

Pacotes capturados (wireshark):

No.	Time	Source	Destination	Protocol	Info
3	0.0	192.168.127.86	192.168.21.61	SIP/SDP	Request: INVITE sip:+351915270202@ptinovacao.pt, with session description
4	0.0	192.168.21.61	192.168.127.86	SIP	Status: 100 Trying
79	6.2	192.168.21.61	192.168.127.86	SIP/SDP	Status: 180 Ringing, with session description
1564	66.6	192.168.21.61	192.168.127.86	SIP	Status: 408 Request Timeout
1567	66.6	192.168.127.86	192.168.21.61	SIP	Request: ACK sip:+351915270202@ptinovacao.pt

Tal como se esperava, o terminal do destinatário não fica a tocar incessantemente. Neste caso é a mensagem SIP 408 *Request Timeout* que ilustra que o tempo para efectuar o pedido expirou isto é, o destino já tocou durante o tempo limite sem se ter obtido resposta por parte deste. Através do tempo associado a cada pacote, constata-se que o número de segundos decorridos desde que começou a tocar – 180 *Ringing* – até a AGCF receber a informação de que o tempo se esgotou– *408 Request Timeout* – é de aproximadamente 60 segundos. Mais uma vez a troca de primitivas e a recepção por parte do MGC do sucedido decorreu normalmente.

- O destinatário atende e desliga

Este é o caso em que a chamada é estabelecida e posteriormente terminada. Os módulos da arquitectura interna da AGCF implementados devem ser capazes de suportar esta situação e mais uma vez pretende-se que o MGC seja informado em tempo real do que vai ocorrendo no estabelecimento da sessão.

- Media Gateway Controller:

```
gil@gil-laptop:~/Desktop/AGCF_nova_testes/mgc/src$ ./mgc_sess SetupRequest 123.456.123.456 al/trunk0/ts0@a-mgw1_addr.com 234403201

        Mensagem do FM- 180 Ringing

        Mensagem do FM- 200 OK Chamada Atendida

        Mensagem do FM- Chamada foi desligada (depois de já ter sido atendida)

        Mensagem do FM- Call Released (chamada libertada)
```

- IMS Agent:

```
gil@gil-laptop:~/Desktop/AGCF_nova_testes/ims_agent_sess/src$ ./ims_agent_sess
1
        --------- Parametros recebidos do Feature Manager --------
type:  SetupRequest
method: not aplicable
sip_pub_uri:  sip:nunogil@ptinovacao.pt
sip_priv_uri:  sip:nunogil@ptinovacao.pt
display_name:  Nuno Gil
user_name:  nunogil
authorization name: nunogil@ptinovacao.pt
ip_agcf: 192.168.127.86
pass:  nunogil
domain:  ptinovacao.pt
to:  234403201

         ---------  //  ---------

from: <sip:nunogil@ptinovacao.pt>
to: sip:+351234403201@ptinovacao.pt> EXOSIP_CALL_PROCEEDING:
EXOSIP_CALL_RINGING:
EXOSIP_CALL_ANSWERED:
EXOSIP_CALL_MESSAGE_NEW:
EXOSIP_CALL_CLOSED:
EXOSIP_CALL_RELEASED:
```

Pacotes capturados (wireshark):

No.	Time	Source	Destination	Protocol	Info
3	0.0	192.168.127.86	192.168.21.61	SIP/SDP	Request: INVITE sip:+351234403201@ptinovacao.pt, with session description
4	0.0	192.168.21.61	192.168.127.86	SIP	Status: 100 Trying
66	1.4	192.168.21.61	192.168.127.86	SIP	Status: 180 Ringing
67	1.4	192.168.21.61	192.168.127.86	SIP/SDP	Status: 183 Session Progress, with session description
258	8.5	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
280	9.0	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
333	10.0	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
376	12.1	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
525	16.1	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
642	20.1	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
741	24.1	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
800	28.1	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
853	32.1	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
899	36.1	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
1003	40.1	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
1165	44.1	192.168.21.61	192.168.127.86	SIP	Request: BYE sip:nunogil@192.168.127.86:5060
1166	44.1	192.168.127.86	192.168.21.61	SIP	Status: 200 OK

Os prints de *debugging* apresentados nas consolas do MGC e IMS Agent comprovam uma correcta interacção entre os módulos internos da AGCF e de todo o processo em causa. Através dos pacotes capturados, observa-se que inicialmente é recebida a mensagem SIP de 180 *Ringing* ilustrando que o terminal de destino se encontra a tocar, precedida de uma 183 *Session Progress*, *with session description*, informando que o destinatário, esteve a avaliar os parâmetros contidos na mensagem SDP encapsulada na SIP INVITE e suporta o pedido. De seguida a sessão é estabelecida, recebendo-se uma mensagem de 200 OK no IMS Agent. Verifica-se que todo o processo decorre normalmente, à excepção do facto que o IMS Agent não se encontra a enviar o ACK necessário em resposta ao 200 OK do destinatário, ficando este a enviar este tipo de mensagens à espera do ACK, visível nos pacotes capturados. Tal deveu-se ao facto de não se ter colocado o *thread* a enviar a resposta necessária o que pode ser efectuado futuramente, de forma simples e rápida, tirando partido das funções *eXosip_call_build_ack* e *eXosip_call_send_ack* presentes na *stack* SIP.

A figura 40 ilustra com mais detalhe a troca de pacotes efectuada onde se visualiza o conteúdo dos seus campos.

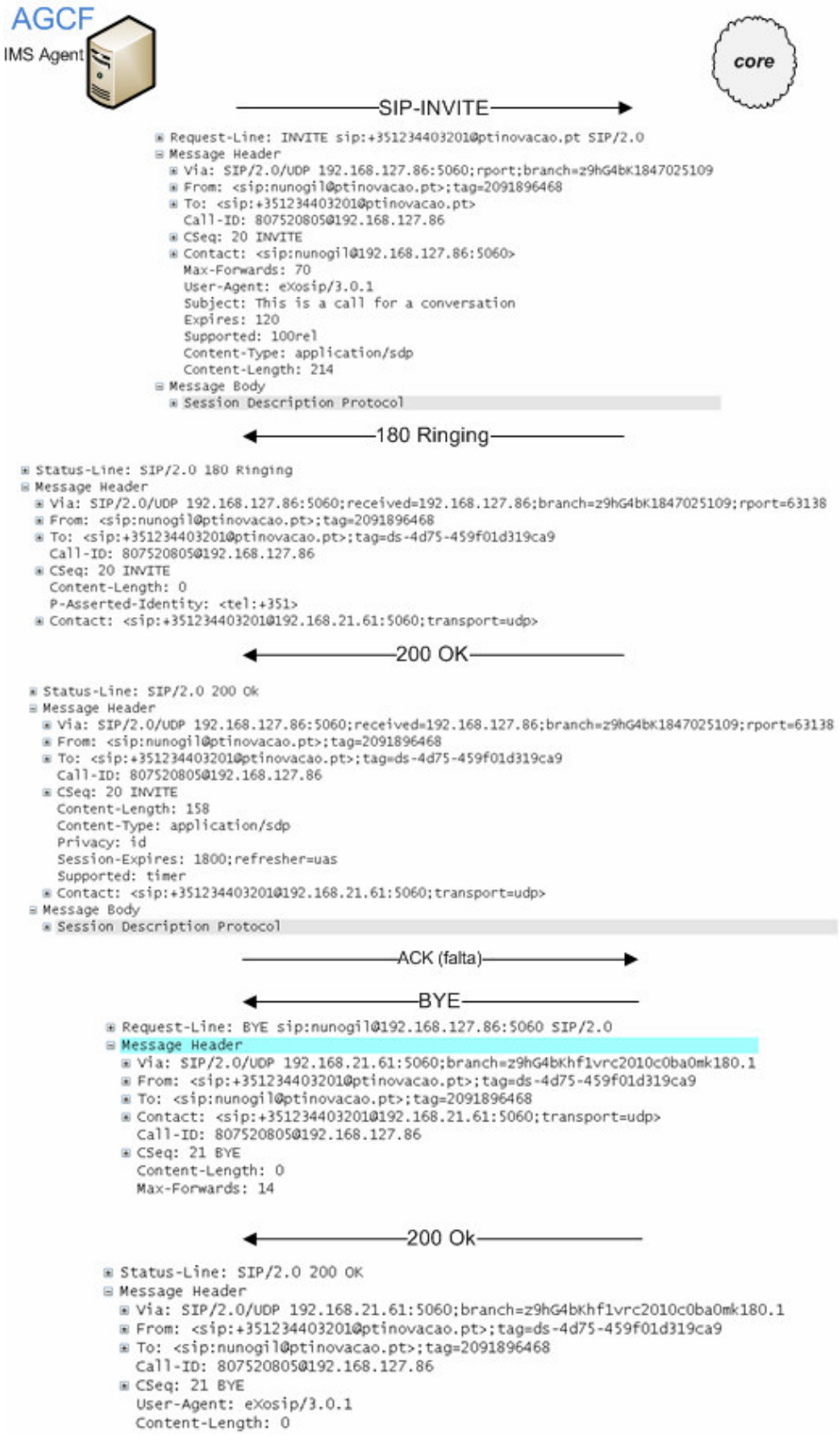


Figura 40 – Troca de pacotes chamada

Uma das formas de aferir a qualidade no tempo de resposta, poderá ser através do *post-dial delay* PDD) ou *call setup delay*. O intervalo de tempo que decorre entre, a primeira mensagem INVITE enviada pela origem e a recepção da mensagem 180 *Ringing* do destino é encarado como o PPD, tal como a figura 41 ilustra.

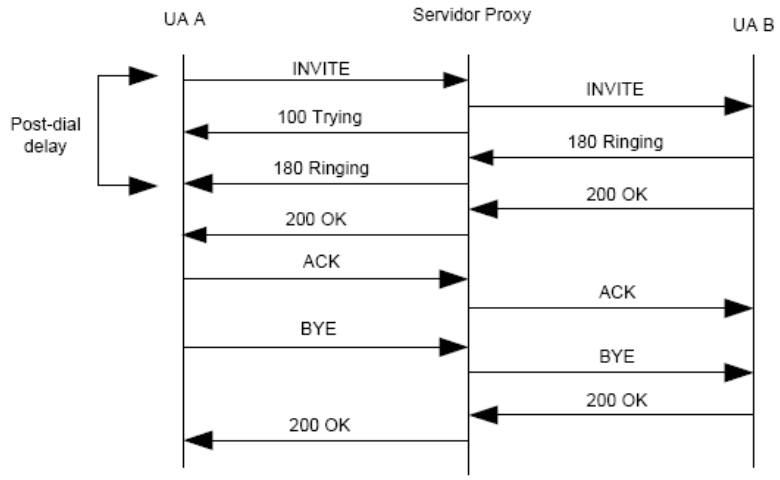


Figura 41 – Post-dial delay

Analisando os pacotes capturados, verifica-se que o PDD foi de 1.4 segundos, o que é perfeitamente aceitável, tendo em conta o sistema telefónico tradicional. Um aspecto a ter em consideração, prende-se com o facto de o *core* ser de testes, podendo, por vezes, não estar completamente estável e, com isso levar a um aumento do PDD.

Seria interessante medir mais tempos como, por exemplo, o *post-pickup delay* (PPD) e o *call release delay* (CRD), representados na figura 42. Para isso seria necessário outro computador instalado com, por exemplo, um terminal SIP como o xLite [70], condição que na altura não foi possível satisfazer.

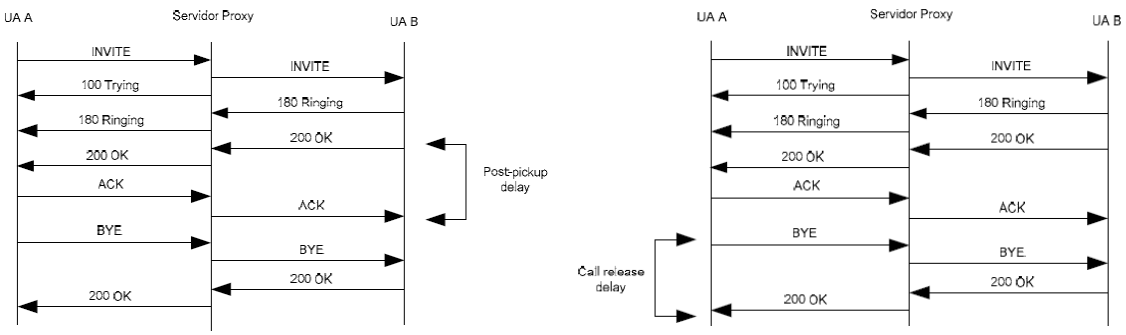


Figura 42 – PPD e CRC

2 Clientes (simultâneo)

Os testes que se seguem correspondem à situação em que dois POTS, associados a

clientes distintos, pretendem efectuar uma chamada. O cenário simulado encontra-se descrito na figura 43.

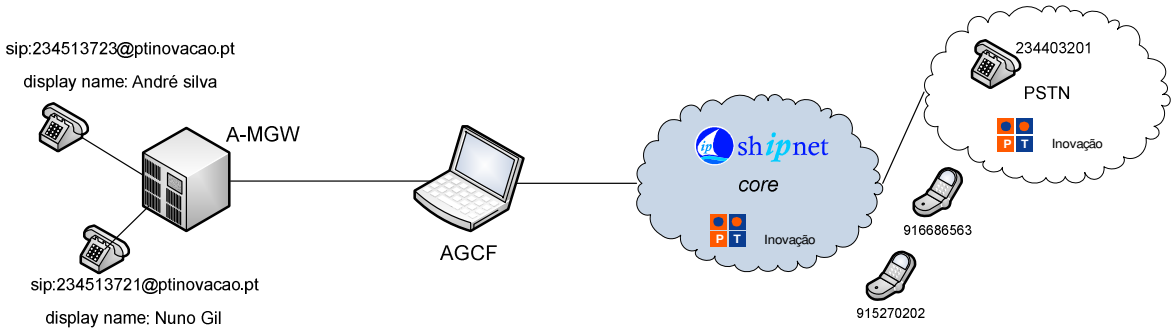


Figura 43 – Cenário para testes com 2 POTS

Os clientes serão Nuno Gil e André Silva e os terminais de destino 916686563 ou 915270202.

- Uma chamada atendida outra rejeitada

Neste teste pretende-se verificar a boa implementação dos processos associados a cada pedido e um correcto encaminhamento entre a informação dos mesmos. É necessário que quando o IMS Agent recebe uma mensagem do *core* saiba a que POTS é referente e a encaminhe para o processo associado.

Para testar tal situação foram enviados dois pedidos de chamada por dois clientes distintos, onde uma é rejeitada e a outra atendida e desligada. O cliente Nuno Gil, com o número associado de 234513721, deseja estabelecer uma chamada para o número 915270202, enquanto que o cliente André Silva, com o número associado 234513723, pretende uma ligação para o número 916686563.

- Media Gateway Controller:

CLIENTE A

```
gil@gil-laptop:~/Desktop/modulo2/mgc/src$ ./mgc_sess SetupRequest 123.456.123.45
6 al/trunk0/ts0@a-mgw1_addr.com 915270202
Thread iniciado!

 1

 Recebeu de retorno do FM : 9

         Criou thread no FM

 Recebeu de retorno do FM : c

         Mensagem do FM- 180 Ringing

 Recebeu de retorno do FM : g

         Mensagem do FM- Chamada foi rejeitada pelo utilizador

 Recebeu de retorno do FM : e

         Mensagem do FM- Call Released (chamada libertada)
Thread concluid!
```

CLIENTE B

```
gil@gil-laptop:~/Desktop/modulo2/mgc/src$ ./mgc_sess SetupReques
t 123.456.123.456 al/trunk0/ts1@a-mgw1_addr.com 916686563
Thread iniciado!

 1

 Recebeu de retorno do FM : 9

         Criou thread no FM

 Recebeu de retorno do FM : c

         Mensagem do FM- 180 Ringing

 Recebeu de retorno do FM : d

         Mensagem do FM- 200 OK Chamada Atendida

 Recebeu de retorno do FM : f

         Mensagem do FM- Chamada foi desligada (depois de já ter
sido atendida)

 Recebeu de retorno do FM : e

         Mensagem do FM- Call Released (chamada libertada)
Thread concluid!
```

- IMS Agent:

```
         IMS_AGENT_Chamada

from: <sip:nunogil@ptinovacao.pt>

to: sip:+351915270202@ptinovacao.pt>

          identificador : 1

          newsockcham : 9
        received eXosip event (type, did, cid) = (8, 0, 1)EXOSIP_CALL_PROCEEDING:
received eXosip event (type, did, cid) = (9, 2, 1)EXOSIP_CALL_RINGING:
received eXosip event (type, did, cid) = (9, 2, 1)
esta a tocar

 newsock : [10]
newSock no tratar_mensagem_recebida : 10

         IMS_AGENT_Chamada

from: <sip:andresilva@ptinovacao.pt>

to: sip:+351916686563@ptinovacao.pt>

          identificador : 3

          newsockcham : 10
        received eXosip event (type, did, cid) = (8, 0, 3)EXOSIP_CALL_PROCEEDING:
received eXosip event (type, did, cid) = (9, 4, 3)EXOSIP_CALL_RINGING:
received eXosip event (type, did, cid) = (9, 4, 3)
esta a tocar
received eXosip event (type, did, cid) = (12, 2, 1)EXOSIP_CALL_REQUESTFAILURE:
received eXosip event (type, did, cid) = (10, 4, 3)EXOSIP_CALL_ANSWERED:
received eXosip event (type, did, cid) = (18, 4, 3)EXOSIP_CALL_MESSAGE_NEW:
received eXosip event (type, did, cid) = (25, 4, 3)EXOSIP_CALL_CLOSED:
received eXosip event (type, did, cid) = (26, -1, 1)EXOSIP_CALL_RELEASED:


received eXosip event (type, did, cid) = (26, 0, 3)EXOSIP_CALL_RELEASED:
```

Descrição detalhada dos pacotes:

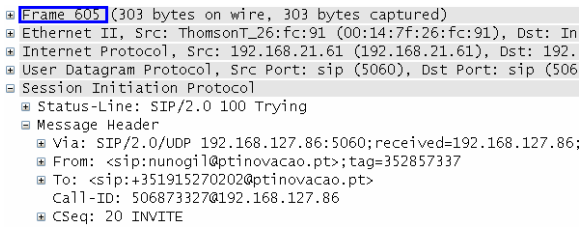
No.	Time	Source	Destination	Protocol	Info
604	174.5	192.168.127.86	192.168.21.61	SIP/SDP	Request: INVITE sip:+351915270202@ptinovacao.pt
605	174.5	192.168.21.61	192.168.127.86	SIP	Status: 100 Trying
672	181.8	192.168.21.61	192.168.127.86	SIP/SDP	Status: 180 Ringing, with session description
711	182.4	192.168.127.86	192.168.21.61	SIP/SDP	Request: INVITE sip:+351916686563@ptinovacao.pt
713	182.5	192.168.21.61	192.168.127.86	SIP	Status: 100 Trying
942	188.6	192.168.21.61	192.168.127.86	SIP/SDP	Status: 180 Ringing, with session description
1520	200.3	192.168.21.61	192.168.127.86	SIP	Status: 486 Busy Here
1523	200.3	192.168.127.86	192.168.21.61	SIP	Request: ACK sip:+351915270202@ptinovacao.pt
1722	209.4	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
1749	209.9	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
1768	210.9	192.168.21.61	192.168.127.86	SIP/SDP	Status: 200 Ok, with session description
1812	211.8	192.168.21.61	192.168.127.86	SIP	Request: BYE sip:andresilva@192.168.127.86:5060
1813	211.8	192.168.127.86	192.168.21.61	SIP	Status: 200 OK

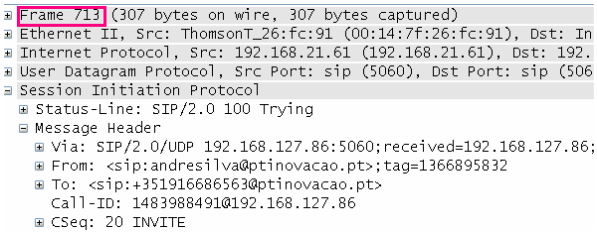
CLIENTE A

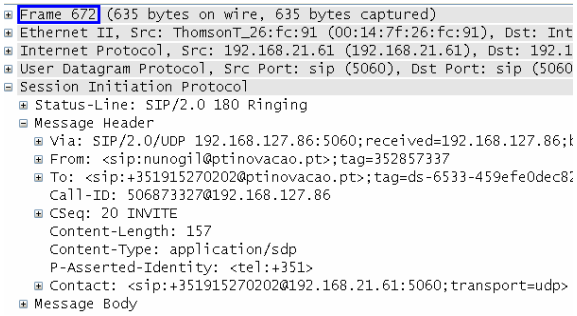
```
⊞ Frame 604 (734 bytes on wire, 734 bytes captured)
⊞ Ethernet II, Src: Intel_bd:85:1c (00:0e:35:bd:85:1c), Dst: Tho
⊞ Internet Protocol, Src: 192.168.127.86 (192.168.127.86), Dst:
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5
⊟ Session Initiation Protocol
  ⊞ Request-Line: INVITE sip:+351915270202@ptinovacao.pt SIP/2.0
  ⊟ Message Header
    ⊞ Via: SIP/2.0/UDP 192.168.127.86:5060;rport;branch=z9hG4bK1
    ⊞ From: <sip:nunogil@ptinovacao.pt>;tag=352857337
    ⊞ To: <sip:+351915270202@ptinovacao.pt>
      Call-ID: 506873327@192.168.127.86
    ⊞ CSeq: 20 INVITE
    ⊞ Contact: <sip:nunogil@192.168.127.86:5060>
      Max-Forwards: 70
      User-Agent: eXosip/3.0.1
      Subject: This is a call for a conversation
      Expires: 120
      Supported: 100rel
      Content-Type: application/sdp
      Content-Length: 214
  ⊞ Message Body
```

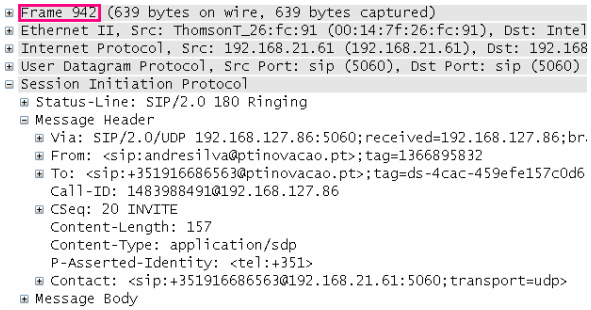
CLIENTE B

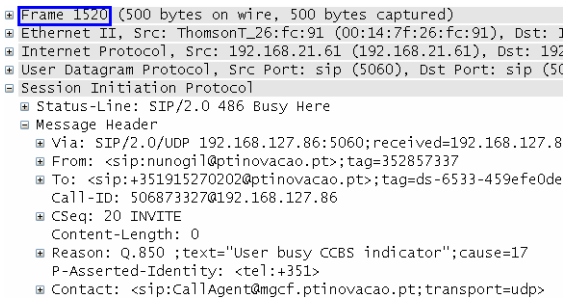
```
⊞ Frame 711 (741 bytes on wire, 741 bytes captured)
⊞ Ethernet II, Src: Intel_bd:85:1c (00:0e:35:bd:85:1c), Dst: Tho
⊞ Internet Protocol, Src: 192.168.127.86 (192.168.127.86), Dst:
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5
⊟ Session Initiation Protocol
  ⊞ Request-Line: INVITE sip:+351916686563@ptinovacao.pt SIP/2.0
  ⊟ Message Header
    ⊞ Via: SIP/2.0/UDP 192.168.127.86:5060;rport;branch=z9hG4bK21
    ⊞ From: <sip:andresilva@ptinovacao.pt>;tag=1366895832
    ⊞ To: <sip:+351916686563@ptinovacao.pt>
      Call-ID: 1483988491@192.168.127.86
    ⊞ CSeq: 20 INVITE
    ⊞ Contact: <sip:andresilva@192.168.127.86:5060>
      Max-Forwards: 70
      User-Agent: eXosip/3.0.1
      Subject: This is a call for a conversation
      Expires: 120
      Supported: 100rel
      Content-Type: application/sdp
      Content-Length: 214
  ⊞ Message Body
```

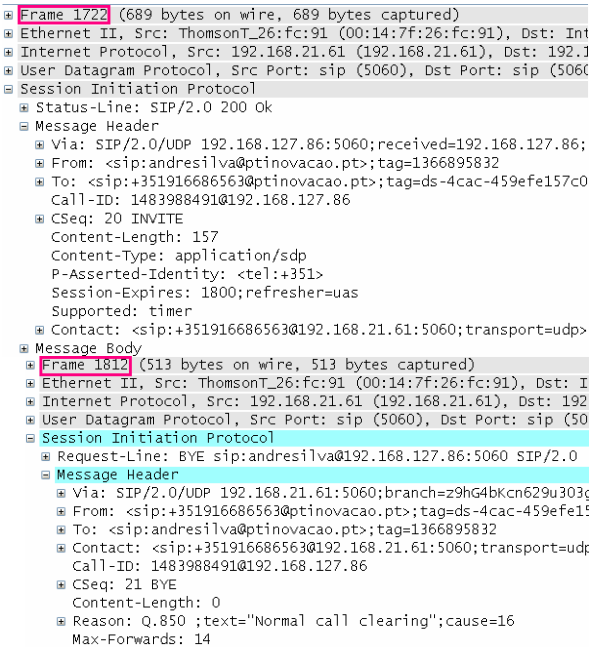


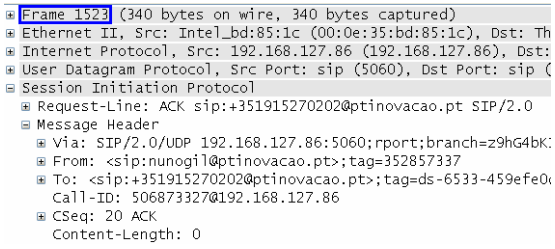


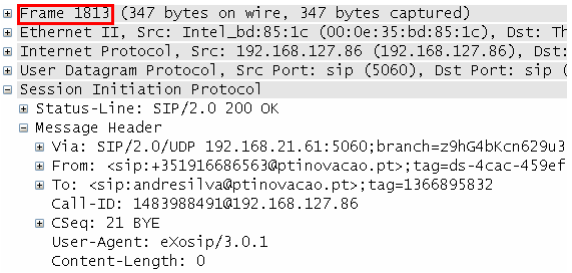












Verificou-se todo um funcionamento como seria esperado. As mensagens foram correctamente encaminhadas para MGC, com o recurso aos processos e uma correcta

implementação destes, conseguindo-se desta forma dotar a AGCF com capacidade para atender pedidos simultâneos.

Recepção de chamadas

Deu-se início a um pequeno teste onde a AGCF recebe pedidos de comunicação com POTS pela qual é responsável – recepção de chamadas.

Para este caso apenas se pretendia testar o comportamento do bloco interno IMS Agent uma vez ,que, este tipo de situação apenas foi apenas implementado para este bloco. Assim, realizou-se uma chamada de um telemóvel para o número 234513721 associado ao cliente Nuno Gil. O módulo IMS Agent foi inicializado ficando em escuta de pedidos no porto 5060,

Verificou-se que foi detectado o pedido e este foi apresentado na consola referente ao IMS Agent. O pedido foi desligado no telemóvel e esta situação foi também detectada com sucesso.

Não é possível apresentar os pacotes capturados e o *printscreen* referente à consola associada ao IMS Agent devido a perda de tal informação.

Capítulo 5

Conclusão

Pretendia-se que, após a realização desta dissertação, ficassem bem claros todos os benefícios que a filosofia NGN vem trazer, quer aos operadores, quer aos utilizadores, e que ficasse igualmente evidente que a evolução para estas redes de nova geração se torna inevitável. Aspectos característicos das NGN, como tudo sobre IP na mesma plataforma segundo uma arquitectura de camadas horizontais, não podem ser aplicados repentinamente, deixando de lado toda uma enorme infraestrutura e número de clientes das redes designadas de tradicionais. Assim, demonstrou-se a importância do conceito TISPAN derivado do IMS numa convergência fixo-móvel e no que diz respeito às redes xDSL.

A AGCF é o elemento fulcral de controlo presente na arquitectura de referência para o subsistema PES, baseado na arquitectura IMS (PES IMS-based), o que levou à sua dissecação e à apresentação de todos os requisitos da sua estrutura interna, bem como de todas as funcionalidades a desenvolver.

A implementação foi feita de forma faseada e teve como primeiro objectivo a base de dados interna (LBCD), de forma a efectuar a configuração inicial da AGCF.

De seguida, foi o subsistema *Registration Processing* sujeito a estudo para se dotar a AGCF com funcionalidades de Registo/Desregisto. Neste caso foi já necessário proceder à implementação dos 3 módulos internos – MGC, FM e IMS Agent – e toda a intercomunicação entre estes. Foram vários os testes realizados, muitos deles (os iniciais) não com o intuito de verificar a capacidade da AGCF de efectuar pedidos de registo/desregisto, mas sim de testar a fiabilidade dos módulos e a sua correcta interacção. Quanto aos pedidos de registo/desregisto, estes foram efectuados com sucesso. No entanto, para que todo o processo se encontre de acordo com o normalizado, seria necessário proceder à instalação de um *script* na máquina, onde a AGCF se encontra implementada, que tivesse as funcionalidades de um P-CSCF.

O subsistema *Session Processing* obrigou a reformular a intercomunicação entre os elementos internos e introduzir o conceito de processos para permitir que a AGCF atenda vários pedidos de estabelecer/receber chamadas simultaneamente, como é esperado.

Inicialmente, foi criada uma situação simples de teste onde apenas existe um cliente (POTS) a tirar partido da AGCF. Estes testes foram realizados de forma a verificar o correcto funcionamento do processo de estabelecimento de chamada. De seguida, utilizaram-se dois clientes em simultâneo a aceder a funcionalidades da AGCF para verificar se esta conseguia dar, de forma fiável, resposta aos pedidos.

Neste caso, poderia ser curioso realizar testes com mais de dois terminais para tirar conclusões sobre a capacidade da AGCF tolerar um número elevado de POTS ligados a determinada *Gateway*. Outro aspecto que seria interessante de testar, com o intuito de colher

dados sobre tempos de resposta, seria o de ter um *softphone*, como por exemplo o X-Lite, instalado noutra máquina a receber e captar pacotes dos pedidos de chamadas.

Ainda no que diz respeito a testes que têm como intuito verificar a capacidade de resposta da AGCF poderia ser criado um *script* para testes de carga simulando uma grande quantidade de pedidos de POTS a chegarem em simultâneo ao MGC.

De uma forma geral, a comunicação interna dos módulos da AGCF e a sua capacidade de processar pedidos para o *core* NGN encontra-se funcional.

Assim, futuramente, além de algumas questões referidas anteriormente existem pontos que deveriam ser alvo inicial de implementação.

Deve ser tido em conta que o processo de estabelecimento de chamada, para o lado SIP, se encontra operacional para todos os blocos internos da AGCF e que se começou a implementar a capacidade de recepção de chamadas.Como tal, deve ser dada continuidade à implementação desta última funcionalidade para todos os blocos internos da AGCF uma vez que apenas foi inicializada para o IMS Agent.

De seguida, a AGCF deverá ser dotada com capacidades para comunicar com A/R-MGWs. Para tal é necessário proceder à instalação da *stack* MEGACO e, tirando partido de funções da mesma, implementar a comunicação entre o MGC e a A/R-MGW.

Neste ponto obtém-se uma linha de interacção – POTS até *core* – conseguindo-se desta forma que a AGCF seja tida em conta como um elemento capaz de ser inserido no demonstrador SHipNET®.

Posteriormente, quando a AGCF se encontrar capaz de suportar o estabelecimento (recepção) de chamadas entre POTS e o *core* do demonstrador SHipNET®, deve inicializar-se a implementação de todo o processo de interacção com o NASS, RACS e AS.

Qualquer trabalho futuro deve acompanhar sempre alterações significativas que possam surgir em novas *releases* relativamente ao funcionamento da AGCF e da sua comunicação com elementos externos. A evolução do demonstrador SHipNET®, ao qual a AGCF se encontra ligada, deve também ser tida em conta.

Referências

[1] Rogério Santos, "História das Telecomunicações em Portugal", biblioteca On-line de Ciências da Comunicação, 1999.
URL:http://www.bocc.ubi.pt/pag/santos-rogerio-historia-telecomunicacoes.pdf, Julho 2008.

[2] Third Generation Partnership Project (3GPP)
URL: http://www.3gpp.org , Outubro 2008.

[3] European Telecommunications Standards Institute (ETSI).
URL: http://www.etsi.org, Setembro 2008.

[4] Ovum Consulting, "Estudo sobre o Impacto das Redes de próxima Geração no Mercado", ANACOM, Junho 2008.

[5] Huway, "Soluções IMS".
URL: http://www.huawei.com/pt/catalog.do?id=588, Agosto 2008.

[6] Vinicius Funicelli, "NGN e IMS I: Redes Legadas e Redes Convergentes", TELECO, Março 2008.
URL: http://www.teleco.com.br/tutoriais/tutorialngnims1/Default.asp, Agosto 2008.

[7] Onedirect, Venda telefones IP.
URL: http://www.onedirect.pt/fr/telefones/telefones-voip-ip, Junho 2008.

[8] 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.

[9] Internet Engineering Task Force (IETF)
URL: http://www.ietf.org/, Outubro 2008.

[10] Koukoulidis, V. Shah, M. , "The IP multimedia domain in wireless networks: concepts, architecture, protocols and applications", IEEE, 2004.

[11] Rosenberg, J., et al., "SIP: Session Initiation Protocol", RFC 3261, Internet Engineering Task Force (IETF), June 2002.

[12] Tudor Golubenco, "Application Layer Handover of VoIP Sessions in IMS Environments", Polytechnic University of Bucharest, August 2006.

[13] J. Rosenberg, "A Hitchhikers Guide to the Session Initiation Protocol (SIP)" , Cisco Systems , June 2006.

[14] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, Internet Engineering Task Force (IETF), November 2002.

[15] M. Handley, "SDP: Session Description Protocol", RFC 2327, Internet Engineering Task Force (IETF), April 1998.

[16] M. Handley, V. Jacobson, " SDP: Session Description Protocol", RFC 4566, Internet Engineering Task Force (IETF), July 2006.

[17] J. Rosenberg, H. Schulzrinne, “An Offer/Answer Model with the Session Description Protocol (SDP)”, RFC 3264, Engineering Task Force (IETF), June 2002.

[18] Megaco/H.248: Media Gateway Control Protocol Overview (RFC 3525).
URL: http://www.javvin.com/protocolMegaco.html, Outubro 2008

[19] C. Rigney, A. Rubens, W. Simpson, “Remote Authentication Dial In User Service (RADIUS)”, RFC 2865, Engineering Task Force (IETF), June 2000.

[20] P. Calhoun, G. Zorn, J. Arkko, “Diameter Base Protocol”, RFC 3588, Internet Engineering Task Force (IETF), September 2003.

[21] H. Schulzrinne, S. Casner, R. Frederick, “RTP: A Transport Protocol for Real-Time Applications”, RFC 3550, Internet Engineering Task Force (IETF), July 2003.

[22] ITU-T, “International telephone connections and circuits – General Recommendations on the transmission quality for an entire international telephone connection”, ITU-T Recommendation G.114

[23] António Gamelas, “TISPAN – Visão Global”, PT Inovação.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] H. Schulzrinne, S. Petrack, “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”, RFC 2833, Internet Engineering Task Force (IETF), May 2000.

[29] W. Simpson, “The point-to-Point-Protocol (PPP)”,RFC 1661, Internet Engineering Task Force (IETF), July 1994

[30] G. Gross, “PPP Over AAL5”, RFC 2364, Internet Engineering Task Force (IETF), July 2008.

[31] L. Mamakos, K. Lidl, J. Evarts , “A Method for Transmitting PPP Over Ethernet (PPPoE)”, RFC 2516, Internet Engineering Task Force (IETF), February 1999.

[32] W. Simpson, “PPP in HDLC-like Framing ”,RFC 1662, Internet Engineering Task Force (IETF), July 1994.

[33] G. Tsirtsis, P. Srisuresh , “Network Address Translation - Protocol Translation (NAT-PT)”, RFC 2766, Internet Engineering Task Force (IETF), February 2000.

[34] Wu Xiaochuan, “ In Search of the Future Developments of PSTN Reconstruction” , November 2006.

[35] André Silva, “Sinalização de Media Gateways em Redes de Próxima Geração”, UA, 2008.

[36] 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.

[37] 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.

[38] ITU-T, “Signalling System No. 7 – ISDN User Part functional description”, ITU-T Recommendation Q.761, 09/97.

[39] ITU-T, “Bearer independent call control protocol”, ITU-T Recommendation Q.1901, 06/2000.

[40] 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.

[41] 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.

[42] 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.

[43] PT Inovação, “ shipnet – ip Keel documento técnico”, v3.4.

[44] Rainer M., “NGN & TISPAN” , ETSI presentation.

[45] Jonas Pettersson, “Converged Services in the Next-Generation Network”, Royal Institute of Techology , 2006.

[46] 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.

[47] 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.

[48] ETSI, "Multimedia Telephony with PSTN/ISDN simulation services”, ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), ETSI TS 181 002 v1.2.10, 2007-11.

[49] Telecommunication Engineering Centre, “IMS Tispan Architecture”, Release 1

[50] 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.

[51] J. Rosenberg, “An XML Configuration Access Protocol” , October 2006.
URL : http://www.jdrosen.net/simple_acap.html, Outubro 2008

[52] 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.

[53] PT Inovação, “SHipNET”.
URL: http://www.ptinovacao.pt/produtos/P&S_PTIN.html, Novembro 2008.

[54] AudioCodes.
URL: http://www.audiocodes.com, Setembro 2008.

[55] 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.

[56] ITU-T, “Gateway control protocol: Version 2”, ITU-T Recommendation H.248.1 v2, 03/2004.

[57] PT Inovação, “A-MGW_concepção_v1.0”

[58] PT Inovação, “AGCF_concepção_v1.0”

[59] 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.

[60] Ubuntu.
URL: http://www.ubuntu.com

[61] Gvim.
URL: http://www.vim.org/

[62] NetBricks
URL: http://www.netbricks.com

[63] GNU Project
URL: http://www.gnu.org/

[64] WireShark
URL: http://www.wireshark.org

[65] World Wide Web consortium
URL: http://www.w3.org/

[66] Paulo Heitlinger, “O guia prático da XML”, Centro Atlântico, Outubro 2001

[67] Pedro L. Rui D., “XML”, Instituto Superior de Engenharia do Porto

[68] Gonzalo Camarillo, Miguel A. García-Martín, “The 3G IP Multimedia Subsystem (IMS) Merging the Internet and the Cellular Worlds”, Wiley, January 2005.

[69] 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.

[70] X-Lite
URL: http://www.counterpath.com

[71] Vladimir Borcic, “NGN Architecture for Fixed Network – Operator Perspective”, Sonaecom, 2006-9

URL:http://www.anacom.pt/streaming/1.vladimir_borcic.pdf?categoryId=212463&contentId=411440&field=ATTACHED_FILE