Universidade do Minho
Escola de Engenharia

Departamento de Informática

Controlo de Tráfego Baseado em Políticas

Raul Graciano Oliveira Rodrigues

Dissertação apresentada à Universidade do Minho para obtenção do grau de Mestre de Informática, elaborada sob orientação do Professor Doutor Pedro Nuno Miranda de Sousa e do Engenheiro Jorge Miguel Marques Dias e Sousa

2007-2008

Agradecimentos

Os meus agradecimentos vão para as pessoas que contribuíram directa ou indirectamente para a realização deste trabalho. No contexto académico queria agradecer ao Professor Pedro Nuno a disponibilidade e empenho na ajuda do desenvolvimento deste documento, ao Professor um grande obrigado. No contexto profissional queria agradecer ao Engenheiro Jorge Sousa pelo apoio dado ao longo de todo o trabalho, ajudando na sua concretização, ao Jorge um grande obrigado. Queria também agradecer ao Engenheiro José Fernandes, como membro da equipa responsável por desenvolver a solução apresentada, o seu contributo para a realização da mesma, para ele, um grande obrigado também.

Não poderia deixar de agradecer a toda equipa que constitui a unidade de Redes de Dados do Departamento de Redes e Protocolos da PT Inovação, a disponibilidade e a ajuda dada para a realização deste trabalho. A todos eles os meus sinceros agradecimentos.

Resumo

O fornecimento dos serviços de dados por parte dos operadores de telecomunicações tem vindo a deparar-se com um crescimento exponencial, o que leva estes a adaptar as suas regras de negócio. A massificação dos acessos a preços acessíveis e competitivos, conjugada com aparecimento de serviços com velocidades cada vez maiores, tem vindo a revolucionar o perfil de tráfego, bem como a ocupação da largura de banda utilizada pelos clientes. Esta massificação tem originado a que os operadores procurem fornecer serviços distintos e inovadores, bem como desenvolver mecanismos que permitam o controlo do serviço contratualizado com o cliente.

O acesso a serviços de rede sem controlo, por parte dos clientes, tem vindo a traduzir-se num uso desmedido da largura de banda, muitas das vezes involuntário através de *spyware* ou da utilização de aplicações de P2P[1] entre outras, acabando por degradar o acesso, o que se traduz num descontentamento e numa má imagem do operador.

Baseado nesta problemática, este trabalho a ser realizado na PT Inovação propõe uma solução de controlo de tráfego baseado em políticas, permitindo atenuar os problemas anteriormente descritos e introduzir novas formas de controlo de tráfego, podendo resultar em possíveis fontes de negócio para os operadores.

Neste contexto, este trabalho será centrado na análise dos requisitos, no desenho e na implementação da solução de controlo de tráfego proposta, tendo em consideração o enquadramento normativo proposto pelo 3GPP[2]. Serão também estudadas soluções actualmente disponíveis para a implementação da funcionalidade de *Policy Enforcement* ao nível do controlo do tráfego, como fornecedores de tal tecnologia, bem como equipamentos disponíveis e a sua forma de interacção. Finalmente serão efectuados testes em ambiente real.

Palavras-chave: Controlo de Tráfego Baseado em Políticas, Redes de Comunicação, Internet, Tarifação, Redes Inteligentes, JAVA, Linux.

1 Peer to Peer
2 3rd Generation Partnership Project

Abstract

The provision of data services by telecommunications operators has been growing exponentially, leading them to adjust their business rules. The proliferation of accesses at reasonable and competitive prices, combined with emergence of advanced networking services, has been revolutionizing the traffic profile and the bandwidth required by the customers. In this way, the operators are faced with the challenge of finding new and innovators services, along with the development of mechanisms to effectively control the service subscribed by the customer.

The access to network services without control by the customers has lead to a disproportionate use of the bandwidth, many times involuntary through the use of spyware, P2P[3] applications, among others, that could degrade access. As consequence, telecommunication operators could suffer noticeable service degradation, customer dissatisfaction, and possible financial penalties.

In this context, this work, which was developed at PT Inovação, proposes a solution to control traffic based on policies, which shall allow the attenuation of the above described problems, introducing new ways to control traffic that may result in new sources of business for operators.

This work will be focused on the analysis of the problem and on the design and implementation of the devised solution, taking into account the legal framework proposed by 3GPP[4] . Also, a study of currently available solutions for the implementation of the Policy Enforcement functionality at the traffic control level is also presented, including technology suppliers, available equipment and its form of interaction. Finally, tests will be carried out in real environment.

Keywords: Policy Based Traffic Control, Communication Networks, Internet, Charging, Intelligent Network, JAVA, Linux.

3 Peer to Peer
4 3rd Generation Partnership Project

Índice de Conteúdos

Índice de Figuras

Índice de Tabelas

Acrónimos

3G	Third Generation Network
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ADSL	Asymmetric Digital Subscriber Line
AF	Application Function
API	Application Programming Interface
COPS	Common Open Policy Service
CSG	Content Services Gateway
DiffServ	Differentiated Services
DSC	Data Session Controller
DSCF	Data Service Control Function
DSCP	Data Service Control Point
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
EPM	Enterprise Policy Manager
ETSI	European Telecommunication Standards Institute
FCCN	Fundação para a Computação Científica Nacional
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service

GSM	Global System for Mobile communications
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IntServ	Integrated Services
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet service provider
LAN	Local Area Network
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
NGN	New Generation Network
OCS	Online Charging System
OFCS	Offline Charging System
OOP	Object Oriented Programming
P2P	Peer to Peer
PBMN	Policy Based Management Network
PCC	Policy Control and Charging
PCEF	Policy and Charging Enforcement Function
PCRF	Policy Control and Charging Rules Function
PDF	Policy Decision Function
PDP	Packet Data Protocol
PDP	Policy Decision Point
PDRS	Policy Decision Rules Server

PEE	Policy Enforcement Equipment
PEP	Policy enforcement Point
PRPC	Proprietary Remote Procedure Call
PS	Policy Server
PTIN	Portugal Telecom Inovação
QoS	Qualidade de Serviço
RADIUS	Remote Authentication Dial In User Service
RDIS	Rede Digital com Integração de Serviços
RP	Real Protocol
RSVP	Resource ReSerVation Protocol
RTDAP	Real Time Data Application Part
SCE	Service Control Engine
SDP	Service Data Point
SLR	Subscriber Locate Register
SM	Subscriber Manager
SPR	Subscrpition Profile Repository
TCP/IP	Transmission Control Protocol /Internet Protocol
UML	Unified Modeling Language
VLAN	Virtual Local Area Network

1 Introdução

A escassez dos recursos naturais entre outros tem vindo a ser um dos maiores problemas que a humanidade enfrenta actualmente, sendo por isso necessário reinventar formas de gerir esses mesmos recursos o mais eficientemente possível. Este paradigma tem vindo a estar cada vez mais presente nos sistemas de informação, uma vez que, embora a grande evolução que se tem sentido ao longo dos tempos nesta área, há necessidade de optimizar e gerir os recursos existentes, de forma a rentabilizar investimentos e garantir padrões de qualidade.

Tendo isto como base, actualmente vão surgindo novos métodos e mecanismos para controlar diversos recursos em áreas distintas, como seja a área das telecomunicações. Estes mecanismos, para além de condicionarem o acesso às infra-estruturas de comunicações, tornam esse mesmo acesso mais justo e mais eficiente, isto é, não só permitem ter o controlo do meio, como possibilitam a distinção entre os diversos consumidores.

Baseado neste contexto, a presente dissertação tem como principal objectivo documentar os vários passos do desenvolvimento de uma solução capaz de controlar o tráfego que flui nas redes de operadores de telecomunicações. Desta forma, será possível garantir padrões de qualidade bem como oferecer novos serviços.

Assim sendo, nos próximos capítulos serão abordadas as diversas fases da concepção de um modelo de controlo de tráfego baseado em políticas, desde o desenho da arquitectura passando pela implementação até aos testes em ambiente real. A descrição das diversas fases será a mais objectiva possível, embora que por vezes possa ser mais restrita, devido a certos conteúdos serem confidenciais ou em certos casos não fazer sentido fazer uma descrição mais alongada de conceitos que se tornam mais secundários para o problema em questão.

1.1 Enquadramento Temático

O forte crescimento das redes IP [1] [2], o aumento da sua complexidade e a diversidade de sistemas ligados a estas, têm levantado vários problemas de controlo e gestão do tráfego. Uma forma visível do uso desmedido da rede é a ocupação da largura de banda [3] [4] de alguns programas, como P2P, *spyware*, *trojans* entre outros [5] [6]. Porém, para contornar estes problemas surgem cada vez mais modelos que permitem efectuar o controlo de diversos parâmetros de funcionamento da rede. Entre estes modelos encontram-se aplicações baseadas em políticas, capazes de fazer o respectivo controlo do tráfego, garantido assim melhor Qualidade do Serviço (QoS) [7] [8] [9] bem como originar possíveis fontes de negócio.

O uso de aplicações baseadas em políticas pode ser expresso num mecanismo de controlo e acesso a um determinado sistema de informação [10], permitindo assim assegurar que o comportamento deste siga um conjunto de políticas pré-definidas. Sendo estes sistemas de uma natureza complexa e dinâmica, é necessário estruturar componentes auxiliares encarregues de aplicar e gerir as diferentes políticas inerentes ao sistema que se pretende controlar.

Estes mecanismos podem ser integrados em diversos contextos, tais como: estabelecimento de prioridades na atribuição de privilégios no acesso a um sistema, gestão de recursos, a garantia da integridade do mesmo, entre outros. A finalidade do mecanismo a ser alvo de estudo neste trabalho será controlar a utilização da largura de banda e o acesso aos recursos de rede de alguns operadores de telecomunicações.

Para a concretização deste pressuposto será necessário arquitectar um sistema capaz de controlar a largura de banda de cada cliente, baseado na política atribuída para este pelo operador. O sistema a ser implementado para esse efeito será enquadrado no modelo de *Policy Based Management Network* (PBMN) [13] proposto pelo IETF[5] e referenciado exaustivamente no livro "*Policy*

5 Internet Engineering Task Force

–Based Network Management: Solution for the Next Generation" [20]. O sistema implementado terá a capacidade de interpretação das políticas, levando à consequente afectação da largura de banda. Assim, a complexidade do sistema poderá ser diferente, dependendo do cenário de aplicação, da rede e de toda envolvente do serviço prestado.

1.2 Enquadramento Normativo

A elaboração da solução será baseada na arquitectura incluída na norma 3GPP Release 7 [14]. Esta arquitectura especifica vários componentes que no seu todo permitem fazer o controlo da qualidade de serviço de um cliente baseado em políticas e paralelamente fazer a tarifação do tráfego associado a este. A designação dada à arquitectura pelo 3GPP é de *Policy Control and Charging* (PCC), sendo que a funcionalidade a ser desenvolvida neste projecto é de *Policy Control* [15], uma vez que o próprio operador já tem implementado a função de *Charging* [16].

A arquitectura PCC é constituída por vários componentes. Uns são responsáveis pela tarifação do tráfego, sendo eles o *Online Charging System* (OCS) e o *Offline Charging System* (OFS), outros são responsáveis pelo controlo do tráfego. Entre eles encontra-se um elemento que se comporta como um repositório de políticas tendo a designação de *Subscription Profile Repository* (SPR). O elemento responsável por indicar a informação necessária para a aplicação da política, é referenciado na arquitectura por *Application Server* (AS). Um dos componentes mais importantes na arquitectura PCC tem a nomenclatura de *Policy Control and Charging Rules Function* (PCRF), tendo a função de aplicar as políticas num componente habilitado para controlar o tráfego. Este último componente também é alvo de especificação na arquitectura, tendo o nome de *Policy and Charging Enforcement Function* (PCEF).

Alguns dos componentes anteriormente referidos não vão ser implementados directamente, somente serão criadas interfaces para os

mesmos, pertencendo a sua implementação a terceiros. Dos componentes directamente implementados destaca-se o *Policy Control and Charging Rules Function* (PCRF), sendo este um componente fulcral na solução.

A arquitectura PCC e os vários componentes que a compõem serão alvo de uma descrição mais detalhada nos próximos capítulos deste trabalho.

1.3 Objectivos

O objectivo deste trabalho, como já foi referido anteriormente, será desenvolver uma solução de controlo de tráfego baseado em políticas. A solução será realizada pela unidade de Redes de Dados incluída no Departamento de Redes e Protocolos da PT Inovação. Para a concretização deste objectivo será imperativo fazer o levantamento dos requisitos do problema em questão, para posteriormente ser realizado o desenho da arquitectura e consequentemente a sua implementação. Na realização de todo o processo será adoptada a norma proposta pelo 3GPP [web1] para esta temática.

Sabendo à partida que a solução vai ser integrada num operador de telecomunicações, será preciso analisar a integração do componente na arquitectura global do mesmo. Para isso será necessário definir interfaces de interligação dos componentes já existentes (e.g. componentes do IP-Raft [17]) com o novo módulo responsável por controlar o tráfego dos clientes. Para a concretização dos objectivos será necessário recorrer a equipamentos de rede com a funcionalidade de controlar a largura de banda do tráfego que flui na rede, fazendo a distinção entre os diversos protocolos de rede e entre os respectivos clientes.

Por fim, serão realizados testes em ambiente real, onde será demonstrado efectivamente a afectação da largura de banda que um cliente irá ter, com base na política a que foi associado.

Desta forma podemos enumerar os seguintes objectivos parcelares para a realização deste trabalho:

- Análise dos requisitos do problema em questão;
- Enquadramento normativo, onde será estudada a norma proposta para o tema pelo organismo 3GPP;
- Tendo em conta o enquadramento normativo realizado, proceder ao estudo da integração da solução de controlo de tráfego no contexto do operador;
- Estudo de soluções actualmente disponíveis para a implementação da funcionalidade de *Policy Enforcement* ao nível do controlo da rede e dos seus respectivos utilizadores;
- Desenho da implementação da solução, bem como estudo da sua integração na infra-estrutura do operador;
- Desenvolvimento de software que permita controlar os elementos de rede em questão, recorrendo a APIs e/ou protocolos abertos do respectivo fornecedor;
- Teste da solução desenvolvida em contexto real de utilização;

1.4 Organização da Dissertação

A presente dissertação está dividida em cinco capítulos principais, sendo organizados da seguinte forma:

1. **Introdução:** Pretende fazer o enquadramento do trabalho, apresentando a temática de controlo de tráfego baseado em políticas, sendo por isso contextualizada a base normativa em que este vai assentar. Neste capítulo serão também apresentados os vários objectivos do trabalho a desenvolver.

2. **Controlo de Tráfego Baseado em Políticas:** Descreve a temática do controlo de tráfego baseado em políticas e os diversos componentes que lhe dizem respeito. Será feita uma especificação dos modelos referentes ao tema, com especial atenção ao modelo *Policy Control and Charging* (PCC) uma vez que será nesta arquitectura onde o trabalho se centrará. No final do capítulo serão apresentadas propostas de três fabricantes para a concretização deste tema.

3. **Desenvolvimento da Solução:** Neste capítulo serão descritos os vários passos de desenvolvimento da solução, para tal, será apresentada a análise dos requisitos, o desenho da arquitectura, o enquadramento geral da solução na arquitectura do operador e por fim serão descritos os detalhes da implementação.

4. **Cenários de Utilização e Testes:** Neste capítulo serão apresentados vários cenários de utilização da solução assim como testes, alguns em contexto real. Será possível verificar a interacção dos vários componentes presentes na solução e os respectivos resultados obtidos.

5. **Conclusões:** Descreve as principais conclusões do trabalho acerca do tema abordado, do desenvolvimento da solução, dos testes realizados e das novas funcionalidades e aplicações que a solução possa vir a desempenhar.

O trabalho completa-se com variados anexos onde serão acrescentados documentos referentes a informação complementar de algumas secções deste trabalho.

2 Controlo de Tráfego Baseado em Políticas

Este segundo capítulo visa essencialmente a contextualização de toda a temática envolvida neste trabalho. Serão apresentados modelos de controlo baseado em políticas bem como a sua evolução e estado actual. O conceito de *Policy Decision Point* (PDP) [11] [12] e *Policy Enforcement Point* (PEP) [11] [12] é apresentado fazendo o respectivo enquadramento no modelo especificado na arquitectura *Policy Control and Charging* (PCC). Esta arquitectura será analisada aprofundadamente, uma vez que será nela onde a solução proposta se baseará, fazendo desde já a devida referência aos componentes desenvolvidos neste trabalho.

Serão apresentadas igualmente as vantagens inerentes a estes modelos, tanto no controle do tráfego propriamente dito, assim como nas novas lógicas de negócio que poderão ser introduzidas por parte dos operadores. Por fim serão descritas algumas soluções existentes para a implementação destes modelos, dando evidentemente mais ênfase à solução adoptada.

2.1 Introdução

De seguida serão apresentados os princípios gerais do conceito *Policy Based Management Network* (PBMN) [19], fazendo a respectiva introdução ao tema e a sua evolução até ao estado actual, dando importância ao aspecto de controlo de QoS que os modelos baseados em PBMN permitem.

2.1.1 Especificação geral

O conceito de PBMN introduziu um novo paradigma na gestão de redes, permitindo ter um controlo centralizado de vários parâmetros de utilização da mesma. Assim é possível gerir vários nós a partir de um ponto, facilitando as tarefas de gestão e monitorização da rede. A Figura 2.1 apresenta uma visão simplicista da temática.

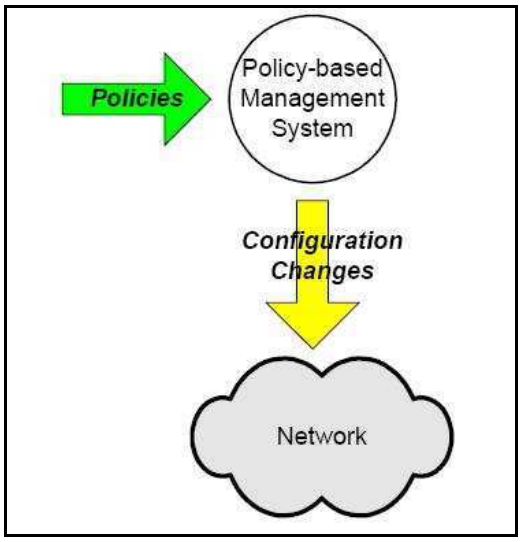

Figura 2. 1 The essence of policy-based management [23].

Através da Figura 2.1 podemos constatar que existe uma unidade central responsável por configurar/gerir os vários elementos da rede. A gestão é feita com base em políticas enviadas por agentes externos ao mecanismo de aplicação de políticas. O *Policy-based Management System* que é representado na Figura 2.1 pode ser visto como uma "caixa negra" onde são processadas as políticas recebidas, enviando as respectivas alterações para os componentes de rede. O dito sistema pode ser composto por várias entidades seguindo determinadas arquitecturas e modelos. As próximas secções serão centradas nestes aspectos.

2.1.2 Evolução dos modelos de controlo baseados em políticas

O início do desenvolvimento e estudo de modelos baseado em PBMN verificou-se a partir de 1990, surgindo com o intuito de controlar a Qualidade de Serviço (QoS) [7] [8] [9] de aplicações Internet bem como o acesso dos utilizadores. Assim pretendia-se que o controlo de QoS não fosse simplesmente traduzido num aumento e diminuição de largura de banda, mas sim num controlo de diferentes métricas, baseado no tipo de aplicações que se está usar.

As primeiras soluções baseadas em PBMN que foram aparecendo no início não tiveram uma boa aceitação por parte da Indústria, uma vez que as estruturas das redes são complexas, suportando serviços distintos com requisitos diferentes. Alguns dos entraves que aparecem no início do desenvolvimento dos modelos baseados no PBMN são os seguintes [20]:

- As primeiras soluções eram demasiado orientadas a determinados dispositivos de rede, e não encarando a rede como um todo, dificultando a integração com o resto dos outros componentes.
- As soluções eram focadas exclusivamente na perspectiva do fornecedor e restringida à sua tecnologia e dispositivos, permitindo somente o controlo da QoS por ele definido.
- As soluções eram demasiado orientadas a redes IP, dificultando a integração em organizações com outras tecnologias.
- Por fim, a existência de problemas genéricos quando se tenta introduzir um novo conceito, como seja o caso do modelo não ser percebido ou não se chegar a um consenso na normalização.

Estes factos levaram a que muito cedo se percebesse que a implementação seria complicada, dispendiosa e morosa, implicando investimento em tecnologia e recursos por parte dos operadores que

quisessem adoptar estes modelos. Facto este levou a não se sentir evolução dos modelos durante vários anos.

2.1.3 Estado actual

A forte penetração do acesso internet, quer através de acesso fixo por cabo/DSL quer por acesso por sistemas móveis, têm levado vários grupos a intensificar o estudo de formas de controlar o tráfego gerado por estes acessos. Um desses grupos é o IETF[6], definindo um protocolo para esse efeito designado por *Common Open Policy Service* (COPS) [21]. O COPS especifica um modelo cliente/servidor em que a comunicação é feita através de um protocolo de sinalização de qualidade de Serviço (e. g. *Resource ReSerVation Protocol* (RSVP) [22]).

O COPS foi estruturado de forma a ter dois modos de funcionamento, o *Outsourcing Model* [21] e o *Provisioning Model* [24]. A descrição dos modos é a seguinte:

- **Outsourcing Model:** Este é modo mais simples de implementação do modelo COPS. Todas as políticas estão armazenadas no *Policy Decision Point* (PDP), sendo que, quando o *Policy Enforcement Point* (PEP) tem de tomar uma decisão envia a informação necessária ao PDP, este analisa e toma a decisão retornando a informação necessária ao PEP para este aplicar a política.

- **Provisioning Model:** Neste modo o PEP informa o PDP das capacidades de decisão que este pode tomar. O PDP carrega as políticas no PEP, tornando este autónomo de tomar as decisões baseado nas políticas recebidas.

Outro grupo que contribui para a especificação de uma arquitectura com as funcionalidades de controlo de (QoS) é o 3GPP[7], sendo dada a designação de *Policy Control and Charging* (PCC) a essa arquitectura. Nesta existem

6 Internet Engineering Task Force
7 3rd Generation Partnership Project

componentes com funcionalidades de controlo de tráfego bem com tarifação do tráfego, vocacionadas para redes 3G (*Third Generation Networks*).

Estes modelos serviram de base para muitas soluções que aparecem no mercado, orientadas para operadores ou instituições que possam ter problemas de controlo de tráfego entre outros recursos, ou então somente para fazer distinção de utilizadores numa determinada rede.

2.2 Especificação do Modelo PBMN

Para mais fácil percepção e introdução dos elementos que constituem um modelo *Policy Based Management Network* (PBMN) [19] é apresentada a Figura 2.2.

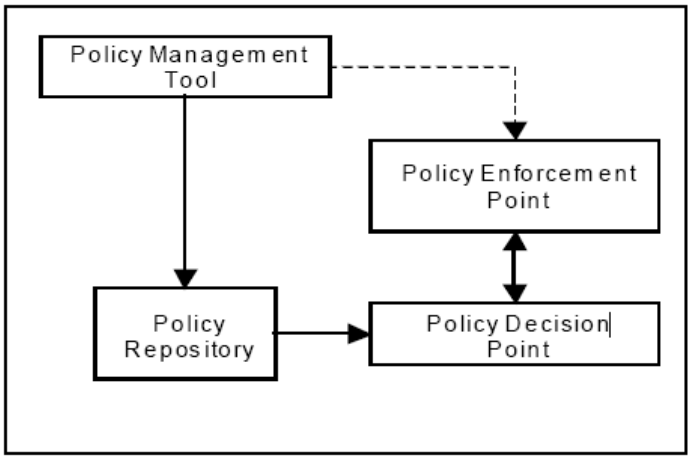

Figura 2. 2 Elementos típicos de uma arquitectura PBMN definido pelo IETF [11].

O modelo apresentado na Figura 2.2 pode ser visto como um sistema constituído por várias entidades, em que o propósito é estimular um componente que desempenhará a função de controlar um ou vários parâmetros da rede, sendo ele representado pelo *Policy Enforcement Point* (PEP). O elemento que tem um papel fundamental na interligação dos vários componentes é o *Policy Decision Point* (PDP), nele estão incluídos mecanismos de decisão baseado em políticas. As políticas estão armazenadas

no *Policy Repository*. Para interagir com os elementos *Policy Repository* e *Policy Enforcement Point* (PEP) existe uma entidade que inclui um conjunto de ferramentas que possibilitam a definição e estruturação das políticas bem como as decisões associadas a estas, na arquitectura apresentada este elemento é designado por *Policy Management Tool*. As setas com o formato sólido demonstram o fluxo normal da interacção dos componentes e a seta a tracejado ilustram uma comunicação opcional.

As soluções propostas por fabricantes especializados em desenvolver soluções de gestão de rede seguem este modelo, embora cada um faça a sua própria abordagem ao tema. Por exemplo, podem concentrar diversas funções num único componente ou adicionar outras funcionalidades que possam ser úteis para os clientes (operadores de comunicações, empresas, etc.).

As entidades do modelo mais importantes para o contexto deste trabalho são o PDP e o PEP. Desta forma serão estudadas formas de implementação de componentes com funções similares, bem como a sua relação. Serão também estudadas as interacções com outros componentes que fazem parte do modelo. A descrição destas entidades será feita nas próximas secções.

2.2.1 Policy Decision Point (PDP)

Um *Policy Decision Point* (PDP) [11] [12] pode ser considerado um administrador de recursos, capaz de providenciar o acesso de um determinado utilizador, consoante determinados eventos ou definições associadas a este. Para esse fim, o PDP insere ou actualiza as regras associadas a uma determinada política no *Policy Enforcement Point* (PEP). O PDP é responsável por tomar as decisões baseado nas políticas definidas no próprio componente ou em entidades externas (e.g. *Policy Repository*), que por sua vez vão ser inseridas em vários nós da rede de um domínio específico [25]. O PDP pode

ser expresso na forma de *software*, desde que implemente as funções anteriormente descritas, bem como interfaces de comunicação com o PEP.

No contexto deste trabalho, o componente que desempenhará a função de PDP terá a função de interagir com o PEP, traduzindo as políticas associadas a determinados eventos de um cliente em acções configuradas no PEP. Para a concretização deste objectivo, o PDP terá de comunicar com as entidades do operador responsáveis por efectuar a relação entre os eventos e política a aplicar.

2.2.2 Policy Enforcement Point (PEP)

O *Policy Enforcement Point* (PEP) [11] [12] é responsável por diversas tarefas tais como controlar a autenticação, parâmetros de QoS entre outros, bem como a autorização do acesso a serviços de rede por parte dos utilizadores. Como foi referido anteriormente, o controlo é feito baseado na política providenciada pelo PDP. O PEP pode situar-se em diversos pontos físicos da rede, como *routers*, *firewalls,* entre outros nós na rede, podendo desta forma actuar sobre o fluxo de dados que se pretende controlar.

O PEP, na maior parte das soluções existentes, é implementando na forma de um equipamento físico capaz de executar as diversas funcionalidades anteriormente descritas podendo em alguns casos ter outras funcionalidades (e.g. gerir relatórios de acesso dos utilizadores), assim como incluir funcionalidades de outros componentes presentes no modelo PBMN (e.g. armazenar as políticas a aplicar).

Neste trabalho será utilizado um equipamento proprietário responsável por assumir a função de PEP, sendo que na secção 3.2.2 do capítulo 3 será analisado em pormenor o equipamento adoptado.

2.2.3 Especificação de Políticas

A designação de Políticas pode, de uma forma genérica, ser referenciada como o processo de definir decisões importantes num determinado contexto, incluindo a identificação das várias alternativas para um caso de estudo, assim como a medição do impacto que estas irão ter no sistema global. Assim, as políticas podem ser expressas em mecanismos de controlo para atingir um determinado fim. No contexto deste trabalho, a definição de políticas pode ser expressa em regras de afectação de tráfego de um determinado utilizador. Alguns exemplos dessas regras podem ser as seguintes:

- Condicionar o acesso de um determinado utilizador a um recurso de rede, por exemplo a um certo conteúdo ou serviço;
- Condicionar o acesso consoante a hora em que este é solicitado;
- Permitir alterar o perfil de tráfego do utilizador baseado no seu consumo;
- Permitir diferenciar o acesso consoante o grupo em que o utilizador está associado;
- Definir uma certa percentagem de largura de banda a um determinado serviço que se pretende utilizar, por exemplo VOIP, P2P entre outros;
- Permitir fazer algum controlo de aplicações mal comportadas que possam degradar a qualidade do acesso, por exemplo vírus, spyware, entre outras;
- Definir perfil de tráfego baseado em diversos factores, definidos pelo administrador de rede, por exemplo definir maior largura de banda a clientes que tenham pago por ter melhor qualidade no serviço.

As regras de afectação do tráfego neste caso serão definidas no componente que desempenhará a função de PEP, cabendo ao PDP indicar qual a política aplicar para um determinado contexto.

2.3 Enquadramento do modelo PBMN nas RNGs

De forma a assegurar o correcto funcionamento das aplicações existem diversas soluções de fornecimento de Qualidade de Serviço. Por exemplo, o controlo de QoS poderá recorrer a mecanismos como a reserva dos recursos de rede (IntServ) [26] [27] e/ou marcação dos pacotes por classes de tráfego (DiffServ) [28]. Contudo, com o crescimento e especificações das arquitecturas das Redes de Nova Geração (RNG) [29], foi preciso adaptar o controlo de QoS às diferentes necessidades de utilização, bem como à integração com outros componentes presentes na arquitectura. Um dos aspectos mais importantes nas RNG é a lógica de sinalização das aplicações necessária para negociar as condições da transferência de dados operar a um nível independente do nível do fluxo de dados. Desta forma, será necessário inserir uma entidade capaz de relacionar a lógica de sinalização da camada do serviço com o fluxo de dados na camada de transporte, permitindo assim controlar a QoS do tráfego correspondente.

A entidade em questão, pode ser vista como uma entidade capaz de decidir o tipo de QoS a aplicar para uma determinada situação. Para além desta funcionalidade que caracteriza a entidade, esta poderá ter funcionalidades de autenticação, tarifação entre outras. Baseado neste pressuposto, várias organizações responsáveis por desenvolver standards nas arquitecturas RNG propõem vários papéis e funcionalidades para a identidade.

Algumas organizações são enumeradas de seguida:

- 3GPP;
- 3GPP2;
- ITU-T;
- ETSI TISPAN;
- CableLabs;
- MSF;

A descrição da entidade proposta pelo 3GPP será detalhadamente descrita nas secções seguintes, uma vez que a solução a ser desenvolvida baseia-se na norma proposta por esta organização. As descrições das entidades propostas pelas outras organizações saem do âmbito deste trabalho, sendo feita somente uma breve referência à entidade presente em cada organização.

2.3.1 Entidade de Policy no 3GPP

O grupo *Third Generation Partnership Project* (3GPP) tem a função de desenvolver especificações e relatórios técnicos no campo das redes GSM [30]. Tendo isto como base, e relembrando o paradigma do que esta dissertação trata, o grupo 3GPP apresenta uma entidade com a funcionalidade de *Policy Decision Point* (PDP) designada de *Policy Control and Charging Rules Function* (PCRF).

O PCRF é a entidade que faz a interligação entre a camada de serviço e a camada de transporte [32]. O PCRF relaciona o utilizador com o seu tráfego, aloca recursos de QoS, define a forma como a camada de transporte deve lidar com tráfego não autorizado, entre outras regras. Para esse efeito o PCRF tem de comunicar com uma entidade situada na camada de transporte, com a designação de *Policy Charging Enforcement Function* (PCEF).

2.3.2 Designação das entidades de Policy nas redes RNGs

Nas várias redes RNG o conceito de *Policy entity* está presente em várias formas, tendo a mesma funcionalidade e, em alguns casos, a abordagem da implementação é bastante semelhante. Um quadro que ilustra a relação é o apresentado na Figura 2.3.

	ITU-T NGN-GSI Rel 1	3GPP Rel 6 & 7	3GPP2 Rev B	ETSI TISPAN Rel 1	PCMM	MSF Rel 3
Policy Decision Function	PD-FE - Policy Decision Functional Entity	PCRF - Policy & Charging Rules Function	PCRF - Policy & Charging Rules Function	SPDF - Service-Based Policy Decision Function A-RACF - Access Resources & Admission Control Function (Partial)	PS – Policy Server	BM – Bandwidth Manager (Partial) P-CSC – Proxy Call and Session Controller (Partial) S-SBG – Signalling Path Session Border Gateway (Partial)
Transport Resource Control Function	TRC-FE - Transport Resource Control FE	GGSN/SGSN/ RNC/Node-B (Embedded, GPRS only)	PDSN/PCF/ BSC (Embedded, CDMA only)	A-RACF – (Partial)	CMTS – (Partial)	BM – Bandwidth Manager (Partial)
Policy Enforcement Function	PE-FE – Policy Enforcement FE residing in network devices (e.g. DSLAM/BRAS GGSN/PDSN, border gateway)	PCEF - Policy & Charging Enforcement Function (e.g. GGSN, TrGW)	AGW – Access Gateway (e.g. PDSN)	BGF - Border Gateway Function (e.g. core Border node) RCEF - Resource Control Enforcement Function (e.g. IP Edge)	CMTS – Cable Model Termination Service	D-SBG – Data Session border Gateway (e.g. core Border node) GGSN

Figura 2. 3 Entidades de *Policy* presente nas RNGs [32].

Na figura 2.3 podemos observar para cada arquitectura a correspondência da funcionalidade de *Policy Decision Point* (PDP) e do *Policy Enforcement Point* (PEP) nas respectivas entidades. Consoante o contexto de cada arquitecta RNG, as entidades têm designações e abordagens diferentes, mas ambas partilham a mesma finalidade no contexto dos modelos baseados em PBMN.

2.4 Especificação da arquitectura PCC na norma 3GGP Release 7

Como foi referido nas secções anteriores a norma 3GPP Release 7 vai servir de base no desenvolvimento deste trabalho. Portanto, será necessário estudar os componentes da arquitectura *Policy Control and Charging* (PCC)[8]

8 Neste documento, em alguns contextos, optou-se por não usar a tradução dos termos *Policy* e *Charging*, devido ao facto de representarem funcionalidades bastantes específicas do contexto da arquitectura PCC.

bem como as suas funcionalidades e formas de interacção. Nas próximas secções serão descritos os referidos componentes.

2.4.1 Introdução

A arquitectura PCC foi desenhada com intuito de englobar as funcionalidades de *Policy Control and Charging* [14] nas redes IP, permitindo controlar a QoS e o acesso por parte dos utilizadores, assim como a tarifação do fluxo de dados. A arquitectura especifica funcionalidades capazes de providenciar serviços de inspecção de pacotes, permitindo aos operadores fazer um controlo de QoS baseado em políticas para um determinado serviço, assim como a sua respectiva tarifação.

2.4.2 Funcionalidades da arquitectura PCC

A norma 3GPP release 7 [14] define vários requisitos para a arquitectura PCC, sendo apresentado de seguida os mais importantes para o contexto deste trabalho. Para uma informação mais detalhada recomenda-se a consulta da norma. Os requisitos mais importantes são os seguintes:

- Decisão da política a aplicar baseada na informação do utilizador;
- Decisão da política e tarifa a aplicar dependendo do tipo de acesso (e. g. GSM, DSL, etc.);
- Permitir descartar pacotes que não cumpram as regras definidas para uma certa política;
- A tarifação pode ser independente da política a aplicar;
- As regras de uma determinada política podem ser predefinidas ou ser definidas dinamicamente no decorrer de uma sessão de dados;

- Poderá ser feito o controlo do tráfego, a sua tarifação ou ambos em qualquer tipo de acesso fornecido por um operador de comunicações.

Para melhor percepção das funcionalidades de *charging* [33] *e* de *policy* [34] será feita uma descrição mais detalhes nos próximos parágrafos.

- **Funcionalidades de *Policy*:**

As funcionalidades de *policy* presentes na arquitectura PCC serão bastante importantes na realização deste trabalho, uma vez que vão servir de base para o enquadramento prático onde esta dissertação se baseia. As duas principais funcionalidades são a de controlo de acesso e de QoS.

A funcionalidade de controlo de acesso permite autorizar o fluxo de dados de um determinado serviço por parte de um utilizador. A funcionalidade de controlo de QoS permite controlar várias propriedades para um fluxo de dados de um determinado serviço/acesso.

- **Funcionalidades de *Charging*:**

A arquitectura PCC especifica as seguintes funcionalidades:

- Tarifação baseada no volume de tráfego;
- Tarifação baseada no tempo;
- Tarifação baseada no volume e no tempo;
- Tarifação baseada em eventos;
- Optar por não fazer tarifação;

As funcionalidades anteriormente descritas, não vão ser implementadas neste projecto, uma vez que operador onde a solução vai ser integrada já possui os seus próprios mecanismos para esse efeito, por este motivo não faz sentido aprofundar mais a descrição.

2.4.3 Arquitectura PCC

A arquitectura *Policy Control and Charging* (PCC) permite dar uma maior granularidade no serviço de tarifação de dados, bem como no controlo do tráfego nas redes de comutação de pacotes sobre o protocolo IP por parte dos operadores de comunicações [35]. Os componentes que integram a arquitectura bem com a sua interligação segundo a norma *Release* 7 do 3GPP são representados na seguinte Figura 2.4.

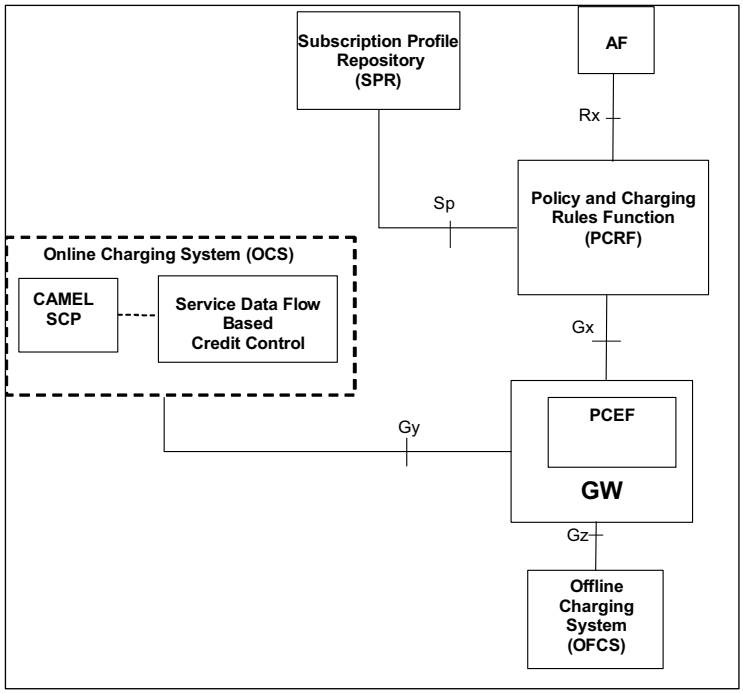

Figura 2. 4 Arquitectura lógica PCC [34].

Os vários componentes presentes na arquitectura serão descritos ao pormenor de seguida:

- **Application Function (AF):**

A entidade *Application Function* (AF) é a entidade que permite o controlo dinâmico das políticas e/ou da tarifação do fluxo de dados. Para isso a AF, baseada nos parâmetros da sessão, envia para o PCRF a informação

necessária para este tomar a decisão de alterar a política e/ou a tarifa da sessão em questão.

- **Subscription Profile Repository (SPR):**

A entidade lógica *Subscrpition Profile Repository* (SPR) é responsável por conter a informação dos subscritores, necessárias para o PCRF tomar a decisão de qual a política a aplicar. O SPR pode ser definido na camada de serviço do operador, contendo a seguinte a informação:

- Serviços permitidos;
- A prioridade para cada serviço;
- Informação de QoS para os serviços, tais como a largura de banda;
- Informação referente a tarifação;
- Tipo de subscritor.

No contexto deste trabalho, esta informação estará incluída na plataforma de serviço do operador, saindo pois do âmbito deste trabalho a sua descrição.

- **Policy Control and Charging Rules Function (PCRF):**

O *Policy Control and Charging Rules Function* (PCRF) engloba as funções de controlo de tráfego baseado em políticas e a tarifação do fluxo de dados. O PCRF providencia para o PCEF o controlo da rede, nas tarefas de controlo do fluxo de dados de um serviço, no seu respectivo acesso, QoS e tarifação.

O PCRF deve indicar ao PCEF como um fluxo de dados de um determinado serviço prestado a um subscritor deve ser tratado, mediante o perfil associado a este. O PCRF autoriza a alocação de recursos para a obtenção de um determinado nível de QoS. Baseado na informação do subscritor proveniente da camada de serviço (e.g. *Session Description Protocol* SDP ou outra informação do serviço) e/ou da informação de políticas definidas, esta entidade decide o perfil de QoS a aplicar para um determinado cenário. O

PCRF pode também ter em conta na alocação de recursos QoS pedidos provenientes do PCEF para esse efeito.

A norma 3GPP release 7 define mais funcionalidades e informação com que o PCRF deve lidar, mas para a realização deste trabalho não faz sentido menciona-las. O componente PCRF é um dos componentes da arquitectura PCC que será directamente implementado neste trabalho. Os detalhes da implementação encontram-se no capítulo 3 mais concretamente na secção 3.5.

- **Policy and Charging Enforcement Function (PCEF):**

O *Policy and Charging Enforcement Function* (PCEF) engloba na função de detecção de fluxo de dados, a função de *Policy Enforcement* [18] e funcionalidades de *charging* [33]. O PCEF deve-se situar na linha do fluxo dos dados, de forma a aplicar as regras associadas às políticas e o controlo e tarifação do tráfego associado a um subscritor. O PCEF efectua o controlo do tráfego de duas maneiras diferentes:

- Controlo no acesso: O PCEF só deve permitir o tráfego dos serviços definidos na política, rejeitando o restante.
- Controlo de QoS: O PCEF deve permitir definir a largura de banda máxima para o fluxo de dados de um determinado serviço, bem como definir prioridades no tráfego, entre outras características de QoS.

A descrição das funcionalidades relativas ao procedimento de *Charging* não será apresentada uma vez que não foram implementadas neste projecto. Os detalhes do componente que executará a função de PCEF podem ser encontrados na secção 3.2.2. do capítulo 3.

- **Online Charging System (OCS) e Offline Charging System (OFCS):**

A entidade *Online Charging System* (OCS) é composta por dois componentes responsáveis por implementar a funcionalidade de tarifação do tráfego online. A entidade *offline charging System* (OFCS) é responsável por gerir a tarifação do tráfego offline. Para mais detalhe acerca destas funcionalidades deverá ser consultada a especificação no TS 32.240 [36].

Como referido anteriormente estas funcionalidades não vão ser implementadas neste projecto.

2.5 Estudo de Soluções Existentes

Neste subcapítulo serão estudadas três soluções que permitem o controlo de tráfego baseado em políticas. As soluções pertencem a empresas especializadas em desenvolvimento de produtos vocacionados para operadores de telecomunicações. Serão abordadas as arquitecturas alvo em que as soluções se podem enquadrar, bem como apresentados alguns componentes que vão ter um papel importante no objectivo pretendido.

2.5.1 Proposta Nortel

A Nortel é uma empresa conceituada no desenvolvimento de aplicações no domínio das comunicações. No contexto do controlo de tráfego baseado em políticas a Nortel oferece uma solução designada de *Enterprise Policy Manager* (EPM) [37].

O EPM é um sistema aplicacional desenhado para gerir a prioritização de tráfego, bem como o controlo de acesso dos serviços em redes empresariais. Desta forma, é possível controlar a largura de banda, garantindo segurança nos acessos e gerindo os fluxos de dados críticos para a rede. O EPM disponibiliza um controlo centralizado do sistema, possibilitando controlar as políticas a aplicar aos elementos de rede. O EPM controla a largura de banda, definindo a prioridade do tráfego através de regras ou políticas pré-definidas. A solução identifica o fluxo do tráfego de várias aplicações e serviços, marcando os pacotes de forma a permitir o seu respectivo controlo, baseado em identificadores tais como: IP origem ou destino, porta origem ou destino, VLAN ID, VLAN tag, Identificação 802.1p entre outros.

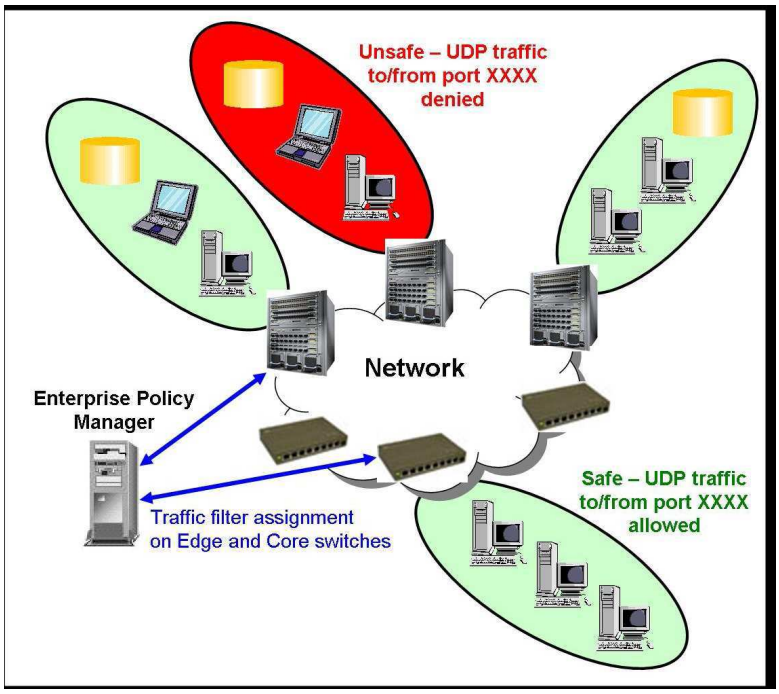

Figura 2. 5 Arquitectura da solução de EPM da Nortel [37].

Na Figura 2.5 está ilustrada a situação em que se nega o acesso a um determinado grupo com base na porta origem/destino. O Sistema EPM permite uma identificação individual de cada utilizador, permitindo assim a aplicação de políticas distintas para cada um deles. O modelo que caracteriza essa situação é o ilustrado na Figura 2.6.

O sistema EPM providencia o controlo de QoS, sendo o controlo de acesso implementado através do *Extensible Authentication Protocol* (EAP) [38] e a autenticação através de RADIUS [39]. Para mais detalhes do modo de funcionamento da solução, consultar a descrição do produto [37].

Esta solução de controlo de QoS e de acesso oferecido pela Nortel é bastante interessante. No entanto, não é uma solução válida para o trabalho em questão, uma vez que seria necessário adquirir *router(s)* e *switcher(s)* compatíveis com o EPM. A integração com a lógica de negócio do operador, infra-estruturas, entre outros componentes, seria deveras complicadas.

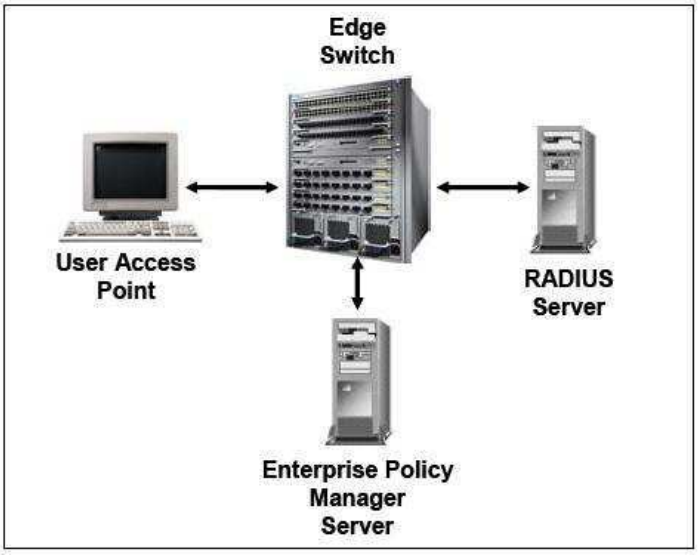

Figura 2. 6 Arquitectura de autenticação no sistema EPM usando EAP [37].

Assim, esta solução parece ser mais adequada para empresas, escolas, hospitais outras organizações, que possam ter problemas de controlo de QoS e que a dimensão da rede permitia uma fácil integração com o EPM.

2.5.2 Proposta Redknee

A Redknee é uma empresa especializada em desenvolver produtos no ramo das comunicações, oferecendo soluções de facturação, classificação, tarifação e controlo de tráfego para serviços de voz, mensagens e nova geração de serviços.

No campo de controlo de tráfego a Redknee oferece uma solução designada de *Policy Decision Rules Server* (PDRS) [40]. O PDRS permite aplicar regras de controlo de tráfego assim como aplicar modelos de tarifação as sessões, inseridas no contexto das redes IMS [31]. A solução permite as seguintes funcionalidades:

- Disponibilizar modelos flexíveis de tarifação;
- Manipulação de QoS por serviço e por utilizador;

- Providenciar acessos a serviços multimédia sujeito a subscrição;

Os componentes da solução, bem como o seu enquadramento na arquitectura IMS podem ser vistos na Figura 2.7.

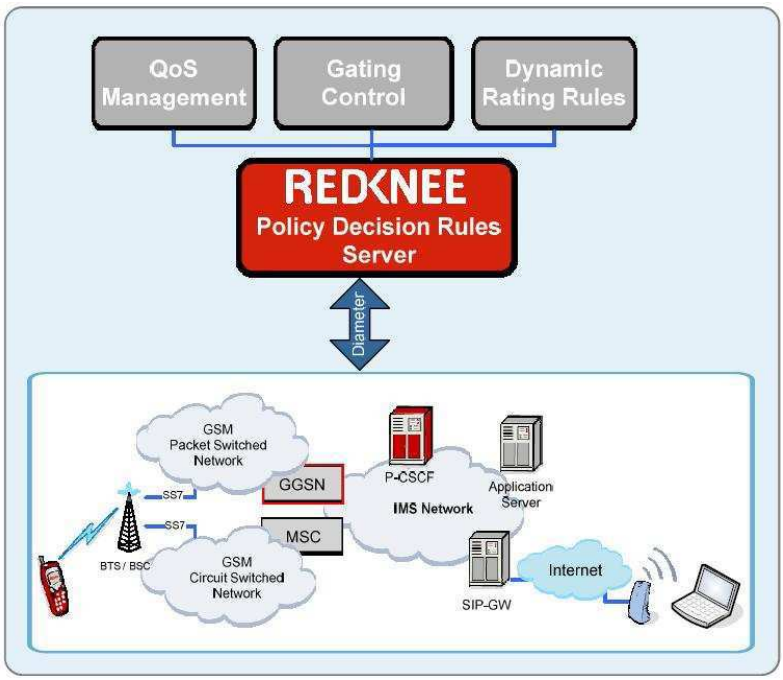

Figura 2. 7 Solução PDRS no contexto IMS [40].

Como se pode observar na Figura 2.7 a solução PDRS é orientada para o contexto IMS. O PDRS interage com o *Gateway GPRS Support Node* (GGSN) [41] através de uma interface Diameter [42], permitindo assim definir o controlo de QoS para uma determinada sessão de um utilizador.

A solução proposta situa-se numa perspectiva de alto nível da arquitectura IMS, adequando-se a operadores que queiram fazer o controlo de QoS logo no inicio de uma sessão IMS. Para o contexto deste trabalho a solução não é a melhor uma vez que é proposto fazer o controlo de QoS ao nível do fluxo de dados no *core* do operador.

2.5.3 Proposta Cisco

A CISCO é uma empresa com larga experiência em desenvolver soluções para operadores de telecomunicações, e o campo do controlo de tráfego baseado em políticas não é excepção. A solução que a CISCO propõe para esta área é composta por um pacote aplicacional onde é feita a gestão dos utilizadores e das políticas associadas, entre outras funcionalidades. Este pacote é capaz de manipular um dispositivo de rede responsável por aplicar regras ao tráfego que flui sobre este. O pacote aplicacional é composto por dois componentes principais:

- Subscriber Manager [43]: Este componente é responsável por indicar à plataforma CISCO SCE a relação perfil/subscritor. Assim, o Subscriber Manager (SM) lida com o controlo dos utilizadores presentes no sistema bem como a política a aplicar para cada um deles.

- Collection Manager [43]: Este componente recebe registos da plataforma CISCO *Service Sontrol Engine* (SCE), processando-os, dando origem a estatísticas, informação dos utilizadores, utilização da rede entre outros dados.

O componente de rede que desempenha a função de *Policy Enforcement* é designado como CISCO *Service Sontrol Engine* (SCE) [44]. O CICSO SCE é um elemento de rede altamente escalável, permitindo uma classificação das sessões dos utilizadores assim como o seu respectivo controlo do tráfego. Este é o núcleo da solução, oferecendo múltiplas formas de configuração e possibilidades de programação. A solução pretende ser escalável para os operadores, no campo do controlo de tráfego, permitindo usar as infra-estruturas já existentes.

Um exemplo de um diagrama de rede com a inclusão do CISCO SCE encontra-se ilustrado na figura 2.8.

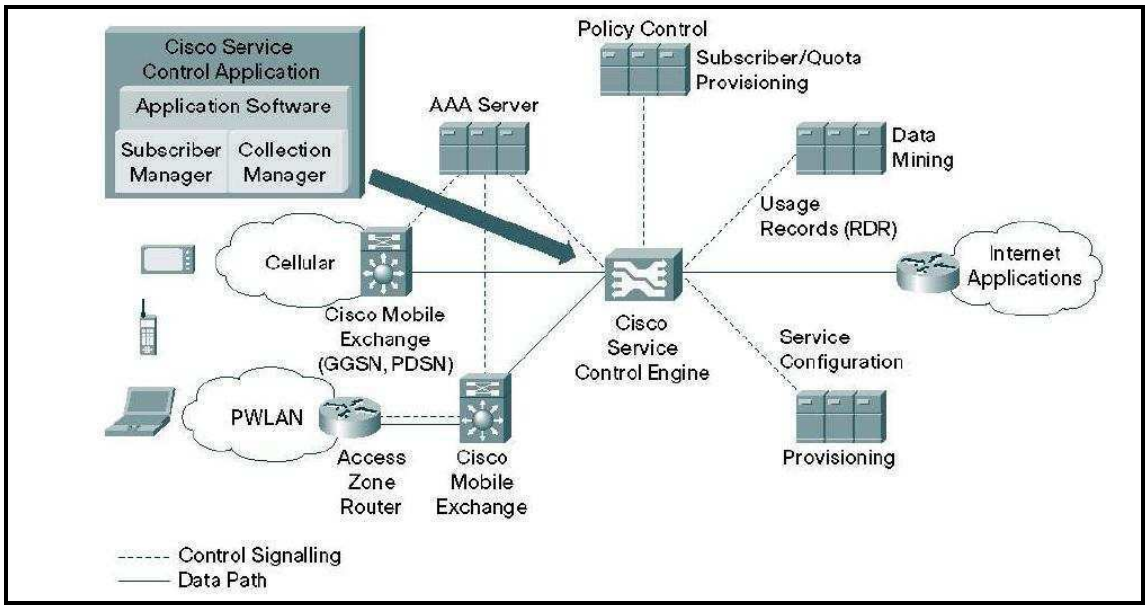

Figura 2. 8 Diagrama para redes móveis com inclusão do SCE [45].

A Figura 2.8 mostra um possível enquadramento do CISCO SCE com vários elementos presentes num operador de comunicações, observando-se os possíveis pontos de acesso à rede do operador, assim como, os elementos responsáveis pela tarefa de controlo de tráfego baseado em políticas.

Uma visão mais pormenorizada da solução oferecida pela CISCO, onde se podem ver os elementos que permitem manipular e configurar o componente CISCO SCE é apresentada na Figura 2.9. Na Figura 2.9 destaca-se a possibilidade de programação dos componentes como o *Subscriber Manager* e do Cisco SCE através de API(s) [web2] disponibilizadas pela CISCO. Esta solução é bastante robusta e flexível, permitindo a fácil integração com os componentes de rede dos operadores, oferecendo métodos de operacionalidade em tempo real.

A proposta da CISCO, devido a todo o seu potencial, foi escolhida pela PT Inovação para ser incluída na solução de controlo de tráfego baseado em políticas, sendo o próximo capítulo deste trabalho centrado na descrição do desenvolvimento da solução.

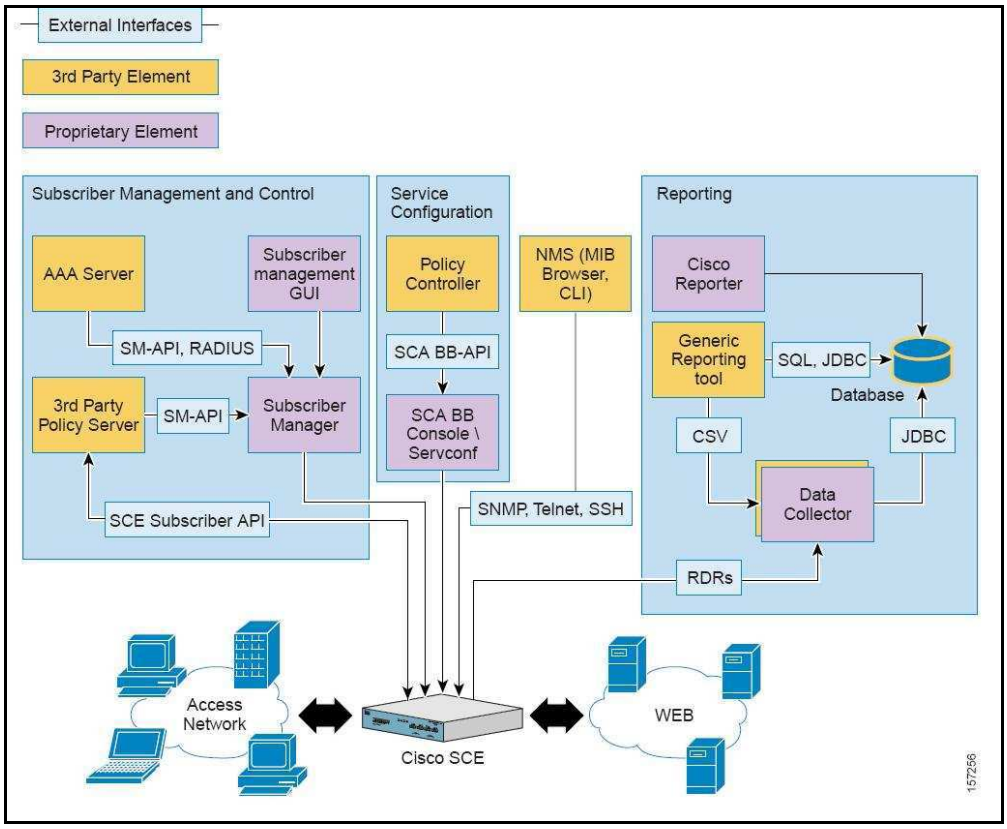

Figura 2. 9 Arquitectura da solução da CISCO mais detalhada [46].

2.6 Notas finais

Este capítulo assume elevada importância para o enquadramento do trabalho desenvolvido e documentado nesta dissertação. Desta forma, foi realizada a contextualização do tema, o seu enquadramento geral, assim como a apresentação do modelo de PBMN e das arquitecturas que o seguem. Neste contexto, foi dado destaque à arquitectura PCC, aos seus componentes e funcionalidades, sendo a solução desenvolvida baseada nesta arquitectura.

Neste capítulo foram igualmente apresentados os estudos efectuados na procura de soluções de fabricantes no campo do controlo de tráfego baseado em políticas, incluindo a solução adoptada neste trabalho. O próximo capítulo será centrado no desenvolvimento da solução propriamente dita, tendo como base sempre a temática discutida neste capítulo.

3 Desenvolvimento da Solução

Finalizada a primeira abordagem e contextualização ao tema, serão agora descritos todos os passos da elaboração da solução. No inicio deste capítulo serão apresentados os requisitos que a solução terá necessariamente de cumprir, tendo como base a arquitectura *Policy Control and Charging* (PCC) e as suas funcionalidades. Concluída a analise dos requisitos, serão descritos os passos da elaboração da solução, sendo apresentadas a arquitectura alto nível do operador, em que a solução de controlo de tráfego vai estar inserida. Posto isto será feita a apresentação em concreto da arquitectura da solução com os seus componentes e interfaces, sendo que esta arquitectura servirá de base para especificação e implementação do módulo que sustentará toda a solução, o *Policy Control and Charging Rules Function* (PCRF).

Este capítulo assumirá um cariz mais prático, uma vez que serão descritos os componentes da solução, bem como os detalhes da sua implementação.

3.1 Análise dos Requisitos

A solução desenvolvida terá de cumprir uma série de requisitos, uns genéricos, implícitos em componentes PCC, outros formulados especificamente para o operador em questão, assim como a arquitectura onde vai estar inserida. De seguida serão descritos os requisitos mais importantes que a solução deverá implementar:

- **Aplicação de políticas consoante o tipo de cliente:**

Um dos requisitos mais importantes do ponto de vista do operador, é permitir aplicar diferentes políticas consoante o tipo de cliente. Isto vai

permitir fazer diferenciação da qualidade de serviço oferecida entre os diferentes clientes.

- **Controlo da largura de banda do acesso:**

A solução terá a capacidade de controlar a largura de banda atribuída a um determinado acesso. Pretende-se fazer por exemplo o controlo baseado no cliente, protocolos ou destino.

- **Definir estaticamente a largura de banda de um protocolo:**

Pretende-se que a solução possa atribuir uma largura de banda fixa para um determinado protocolo, implicando que em qualquer situação a largura de banda não exceda o valor definido.

- **Bloquear o acesso a um serviço:**

Pretende-se implementar a funcionalidade de bloquear o acesso a um dado serviço, baseado por exemplo no protocolo usado, IP do servidor, entre outras características do serviço.

- **Integração da solução na arquitectura IP-Raft:**

Deverão ser implementados interfaces de ligação do componente PCRF com os outros componentes presentes na arquitectura IP-Raft (*online/offline Charging System*) [47].

- **Implementação de Interface PEE:**

Deverá ser implementado o interface de comunicação com o Policy *Enforcement Equipment* (PEE), possibilitando injectar as respectivas políticas no componente de rede obtendo o controlo desejado.

3.2 Desenho da arquitectura

Nesta secção serão apresentadas as várias arquitecturas em que a solução se vai enquadrar, sendo referida a arquitectura IP-Raft como uma

abstracção a alto nível. Posteriormente será feita a apresentação da arquitectura da solução e os seus componentes.

3.2.1 Enquadramento Alto Nível

Nesta secção será apresentado o enquadramento da solução de controlo de tráfego baseado em políticas no contexto IP-Raft, sendo feita a descrição de alguns componentes da arquitectura.

A arquitectura IP-Raft está contida na plataforma Shipnet (*Service Handling on IP Networks*) [48], os componentes desta têm a função de oferecer aos operadores diversas formas de tarifação dos serviços oferecidos. Esta solução oferecida pela PT Inovação oferece a possibilidade de tarifação com base na sessão (*Session Charging Function* [49] [50]) e com base nos eventos ou conteúdos (*Event Charging Function* [49] [50]). Para além desta forma de tarifação a solução também disponibiliza um sistema *offline* de tarifação.

Os vários componentes que compõem a arquitectura IP-Raft podem ser visualizados na Figura 3.1.

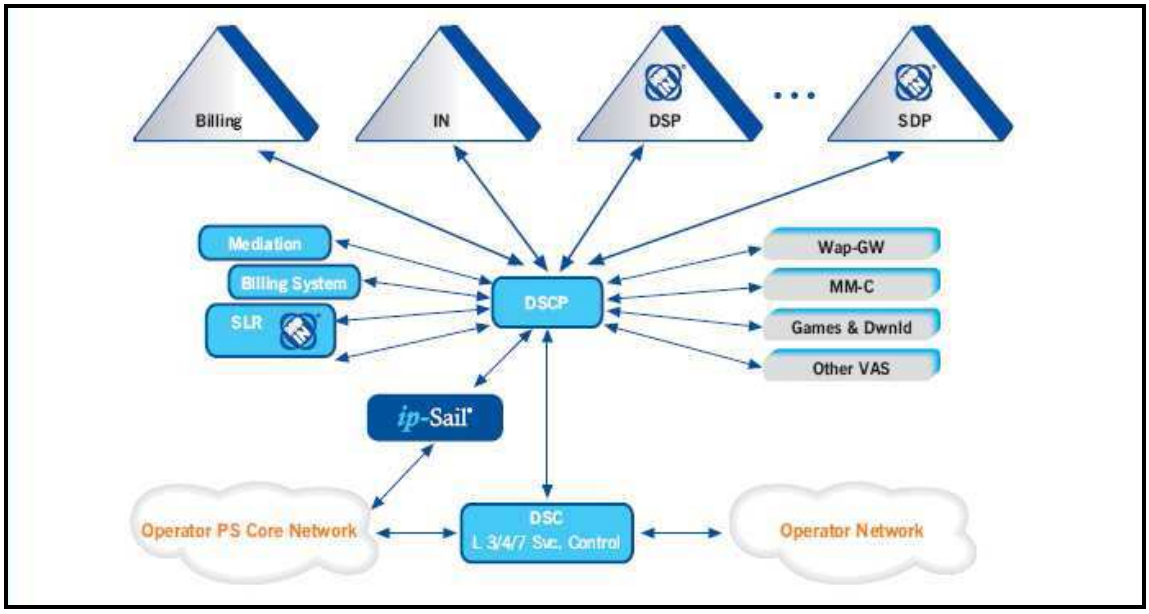

Figura 3. 1 Arquitectura IP-Raft [47].

Para melhor compreensão do enquadramento da solução na arquitectura, serão descritos os componentes que tem envolvência directa com a solução:

- **Data Service Control Point (DSCP):**

O *Data Service Control Point* (DSCP) [47] pode ser visto como o nó central da arquitectura IP-Raft, funcionando com todo o tipo de lógica no controlo de sinalização dos serviços oferecidos pelo o operador. O DSCP garante conectividade com várias plataformas de serviço de valor acrescentado, *value-added service* (VAS) [51], assim como com diversos elementos de rede.

O módulo desenvolvido neste trabalho estará contido no DSCP, uma vez que será necessário ter conectividade com elementos de rede tais como o *Policy Enforcement equipment* (PEE), assim como com os componentes do serviço do operador.

- **Subscriber Location Register (SLR):**

O *Subscriber Location Register* (SLR) é responsável por indicar a localização da informação do cliente nas plataformas de facturação do operador. No contexto IP-Raft o SLR disponibiliza a informação necessária para execução da lógica de negócio para um dado serviço.

- **Data Session Controller (DSC):**

O *Data Session Controller* (DSC) tem a função de tarifação de transporte contida no IP-Raft. É neste componente onde é feita a inspecção dos pacotes da rede, fazendo a distinção dos fluxos de dados das sessões dos clientes. A base de funcionamento do DSC tem como princípio o conceito de *triggering* [52], distinguindo padrões de tráfego e accionando acções definidas no DSCP.

- **Service data Point (SDP)**

O *Service Data Point* (SDP) [53] é um sistema que permite o acesso à plataforma de base de dados do operador, permitindo efectuar operações referentes aos dados de um cliente. O SDP providencia a informação do cliente

a componentes que necessitem dessa informação para aplicação da lógica de sinalização.

3.2.2 Enquadramento Específico

Finalizado a apresentação da arquitectura alto nível onde a solução vai estar incluída, será apresentada a arquitectura da solução, assim como a descrição dos seus componentes. A Figura 3.2 representa a arquitectura da solução.

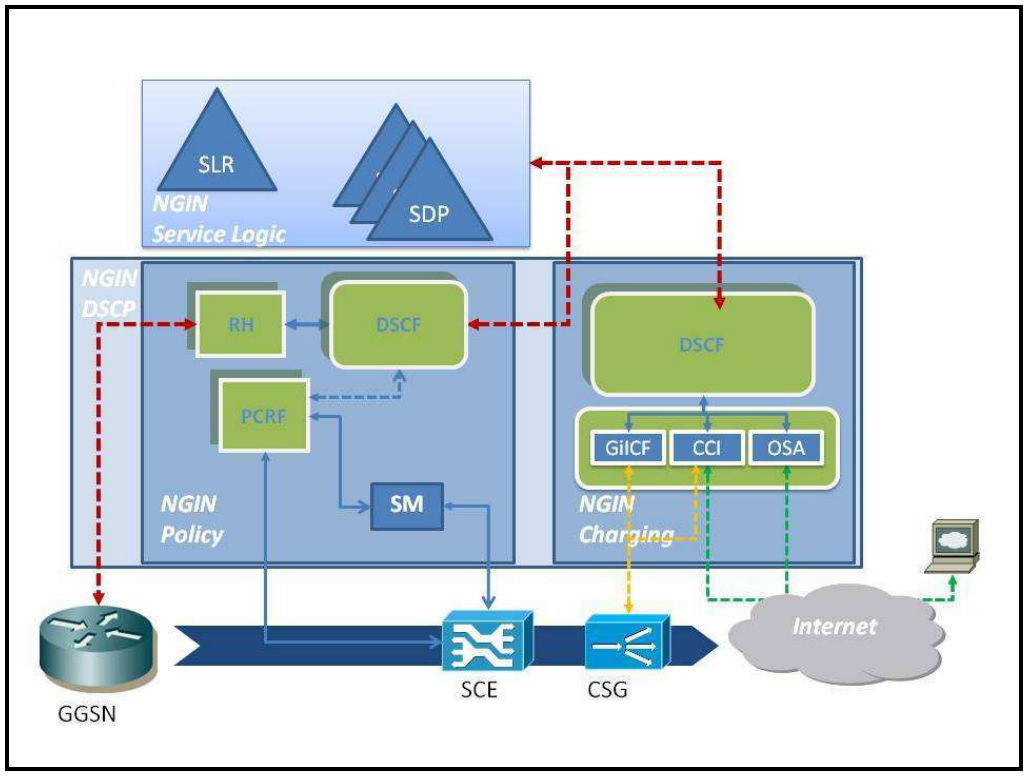

Figura 3. 2 Arquitectura da solução *Policy Enforcement*.

Na arquitectura ilustrada na Figura 3.2 podemos identificar duas secções com funcionalidades distintas, ambas pertencentes ao sistema DSCP, uma com funcionalidades de *Policy* (identificada por NGIN *Policy*), e outra com funcionalidades de *charging* (identificada por NGIN *Charging*). Como foi referido anteriormente, apesar de o componente PCRF especificado na arquitectura PCC possibilitar as funções de *charging*, neste trabalho elas não

serão implementadas. Desta forma, os componentes de grupo NGIN *Policy* vão ser descritos sucintamente nas próximas secções. No entanto, dada a sua importância, serão também brevemente descritos alguns componentes do sistema NGIN *Charging* e a sua importância no contexto da implementação da solução.

- **Policy Control and Charging Rules Function (PCRF)**:

O PCRF pode ser visto como a materialização da temática onde esta dissertação assenta, o controlo de tráfego baseado em políticas. As características do PCRF de uma forma geral foram apresentadas na secção 2.4.3. do capítulo 2. Baseado nessa descrição, o módulo aqui descrito irá implementar algumas dessas funções, daí ter a designação PCRF no contexto do sistema DSCP.

O módulo desenvolvido terá dois tipos de interfaces, uma com a parte do serviço do operador, sendo a comunicação feita via o DSCF através da interface RTDAP, e outra com o equipamento ou componentes responsáveis por aplicar as políticas, via a interface PCEF. A descrição dos dois tipos de interfaces será feita na secção 3.3.

O PCRF pode ser visto como um intermediário entre a lógica de negócio do operador, com o equipamento de rede responsável por controlar o tráfego. A implementação deste módulo será centrada nestes dois aspectos. Este, baseado na informação passada pelo DSCF, deve indicar ao componente que desempenhará a função de PCEF a política a aplicar para um determinado utilizador, tendo a capacidade de alterar em qualquer momento da sessão a política associado ao utilizador.

- **Radius Handler (RH):**

O componente *Radius Handler* é responsável por receber pedidos RADIUS [39], contendo a informação de autenticação e *accounting* de um determinado cliente. No contexto deste trabalho a informação mais relevante proveniente dos pedidos RADIUS é o *Mobile Subscriber Integrated Services*

Digital Network Number (MSISDN) e o IP. Com base nesta informação o DSCF consulta a plataforma de serviço do operador, que contem a informação do cliente. Neste trabalho a informação mais relevante será o identificador da política correspondente.

Os pedidos de RADIUS também serão interceptados pelo DSCF responsável pela função de *Charging*, permitindo assim a autenticação do utilizador na plataforma de Serviço. Com isto será possível fazer a tarifação e autorização de uma sessão de dados de um cliente.

- **Data Service Control Function (DSCF):**

O *Data Service Control Function* (DSCF) é o elemento central do sistema DSCP da arquitectura IP-Raft. Aqui é feito o processamento das soluções *Online e Offline* de *Charging* da PT Inovação.

No contexto deste trabalho o DSCF terá duas funções distintas. Uma será processar as mensagens de autenticação e alteração das políticas/perfil do cliente, sendo posteriormente envidas para o PCRF. Estas características estão incluídas no grupo de NGIN *Policy* da Figura 3.2. A outra funcionalidade será processar as mensagens de iniciação de sessão e autorização de conteúdos, referentes ao grupo NGIN *Charging* da mesma figura.

- **Subscriber Manager (SM):**

O *Subscriber Manager* (SM) é um componente disponibilizado pela CISCO, de forma a dar suporte à solução deste fabricante, para o controlo de tráfego baseado em políticas. O SM permite gerir a relação do cliente (*subscriber*) com a política (*policy*). Este componente permite gerir vários CISCO SCE, indicando para cada um deles a política a aplicar para um dado cliente. O uso do SM permitirá facilitar a manipulação e integração da solução da CISCO no ambiente do operador.

O SM pode ser visto como um *Middleware* [60] entre o PCRF e o(s) CISCO SCE. O SM baseado na informação passada pelo o PCRF faz a gestão dos utilizadores no(s) SCE(s). Esta gestão é feita com base no conceito de

domínios, assim o SM agrupa o(s) SCE(s) por domínios facilitando as operações de gestão dos utilizadores.

No contexto deste trabalho o PCRF irá interagir com o SM através da utilização de uma API disponibilizada pela CISCO, permitindo assim uma grande modularidade e abstracção das operações de controlo dos utilizadores presentes na plataforma, assim como na respectiva política associada a estes.

- **Service Control Engine (SCE):**

O Service Control Engine (SCE), disponibilizado pela CISCO irá neste trabalho executar a função de *Policy and Charging Enforcement Function* (PCEF). A função de PCEF foi descrita anteriormente no capítulo 2.

A forma de interacção com este equipamento no que diz respeito à autenticação e associação das políticas dos utilizadores é providenciada por duas formas: *i*) Através do *Subscriber Manager* (SM); *ii*) Directamente via PCRF.

Será no SCE onde serão definidas as políticas a aplicar num determinado cenário, sendo estas identificadas por um identificador numérico. Muitos dos requisitos analisados na secção 3.1., serão expressos em políticas definidas no SCE. A definição das políticas no SCE sai do âmbito deste trabalho, sendo somente importante garantir, que a política para um determinando cenário seja correctamente indicada ao SCE.

O Cisco SCE permite dois modos de funcionamento, respeitantes à autenticação dos clientes (*Subscribers*) e consequentemente na aplicação das políticas, permitindo aos operadores optarem pela melhor forma da integração com a sua arquitectura e nos cenários de utilização pretendidos. Os dois modos de funcionamento serão apresentados de seguida, sendo que o PCRF desenvolvido neste trabalho estará apto em interagir com o SCE nos dois modos de funcionamento:

  - **Modo Push:** No modo *push*, o componente que dialoga com o CISCO SCE é responsável por indicar, para um dado cliente, o seu identificador, o IP que este terá na rede, assim como o

identificador da política que lhe ficará associado. O SCE baseado nesta informação aplica as respectivas regras associadas à política ao tráfego do utilizador. Neste trabalho, no modo de configuração *Push,* o PCRF será responsável por injectar a respectiva informação no SCE.

- **Modo Pull:** No modo *Pull*, o processo de autenticação é iniciado pelo CISCO SCE. Este, baseado no IP do cliente, questiona o componente responsável por indicar a política a aplicar, podendo ser o PCRF ou o SM. No caso de ser o PCRF, este baseado no IP interage com outros componentes que lhe darão a informação da política e o respectivo identificador do cliente. Tendo a informação necessária o PCRF injecta a respectiva informação do utilizador no SCE.

- **Gateway GPRS Support Node (GGSN):**

O componente Gateway GPRS Support Node (GGSN) [54] presente na Figura 3.2 não fazendo parte directamente da solução de *Policy Enforcement*, é um elemento importante para o enquadramento da solução no ambiente de rede do operador. O GGSN é um elemento de rede que se comporta com uma *gateway* entre as redes de acesso e a redes de dados públicas ou privadas (e. g. Internet ou redes empresariais) [55]. Neste ponto de rede é feita a sinalização para as redes de acesso e rede de dados, sinalização para sistemas de *charging,* controlo da subscrição, autenticação e controlo da sessão.

Como pode ser visto na arquitectura da solução apresentada na Figura 3.2, o CISCO SCE vai ser atravessado pelo fluxo de tráfego proveniente do GGSN. Portanto as operações anteriormente descritas já ocorreram, passando simplesmente a função de controlo de largura de banda para o SCE.

- **Content Services Gateway (CSG):**

Apesar do trabalho se centrar numa solução de controlo de tráfego baseado em políticas, será necessário usar componentes de *charging* para complementar a solução. O componente principal nesta área é o CISCO *Content Services Gateway* (CSG) [56]. O CISCO CSG é uma solução vocacionada para fornecedores de serviço em redes IP, oferecendo capacidades de tarifação que podem variar por serviço ou evento. Este equipamento possibilita a análise do fluxo de dados, efectuando a examinação do seu conteúdo, a contabilização do tráfego utilizado e o controlo do acesso.

Na arquitectura da solução este elemento irá interagir com o DSCF, possibilitando o controlo do acesso e a utilização de serviços definidos na lógica de negócio do operador. Este componente irá contabilizar a quantidade de tráfego utilizado de um serviço requisitado por um cliente. Com base nessa informação serão aplicadas regras de tarifação, e o mais importante no contexto deste trabalho, permitirá alterar a política a aplicar para um cliente, mediante o tráfego consumido.

3.3 Especificação de Interfaces

Nesta secção vão ser descritos os dois tipos de interfaces que o componente PCRF irá implementar para comunicar com o módulo DSCF e com o componente que desempenhará a função de PCEF, ou seja o CISCO SCE.

3.3.1 Interface RTDAP

A interface RTDAP permite efectuar a comunicação entre o PCRF e o DSCF, permitindo assim, a comunicação com as lógicas de serviço do operador. A comunicação é feita através do protocolo *Real Time Data Application Part* (RTDAP). O protocolo RTDAP é um protocolo proprietário da

PT Inovação, este pode ser visto como um protocolo aplicacional, usando como camada de transporte o protocolo TCP [57].

No contexto deste trabalho, a interface RTDAP irá suportar mensagens contendo informação relevante para a solução, tais como o identificador do cliente (*subscriber Id*), o IP, e a política a aplicar (perfil). A Tabela 3.1 descreve as mensagens RTDAP mais relevantes para este projecto.

Nome da mensagem	Descrição
LoginReq	Esta mensagem contém a informação para o PCEF aplicar a respectiva política para um dado cliente. O conteúdo da mensagem mais importante é o identificador do cliente (subscriber Id), IP e a política aplicar, expressa na forma de um identificador.
LoginRes	Esta mensagem contem o resultado da operação login, isto é, indica se a informação do cliente foi correctamente inserida no PCEF.
LogoutReq	Esta mensagem tem como finalidade de indicar ao PCEF, que o cliente com um dado IP, não vai ser mais controlado.
LogoutRes	Esta mensagem indica se associação IP/ cliente foi removida do PCEF
ProfileUpdateReq	Esta mensagem permite alterar em tempo real a política/perfil associado a um cliente no PCEF.
ProfileUpdateRes	Esta mensagem confirma se a política/perfil foi alteado com sucesso.

Tabela 3. 1 Mensagens mais importantes que fluem na interface RTDAP.

3.3.2 Interface PCEF

Como já foi referido anteriormente o equipamento que terá a função de PCEF será o CISCO SCE. A comunicação com este será feita directamente usando uma API (SCE API [58]) ou recorrendo ao *Subscriber Manager* (SM), capaz de gerir vários CISCO SCE. A comunicação com o SM também será feita através de uma API (SM API [59]).

As API's usam um protocolo proprietário desenvolvido pela CISCO, designado de *Proprietary Remote Procedure* Call (PRPC), com base neste protocolo é feita a comunicação entre o PCRF e o SCE/SM. O PCRF, por

configuração, define ligações a um ou vários SCE(s) ou em alternativa define uma ou mais ligações a vários SM(s).

De seguida serão descritas, as mensagens que fluem nas duas interfaces, de forma análoga como foi feito na interface RTDAP.

- **Interface com Subscriber Manager (SM):**

Na Tabela 3.2 são descritas as principais mensagens desta interface.

Método	Descrição
Login	Adiciona ou altera a informação (IP, Política) de um utilizador (*subscriber*) no SM.
LogoutByName	Remove o registo de um utilizador (*subscriber*) da base de dados do SM, baseado num identificador (subscriber Id).
LogoutByNameFromDomain	Remove o registo de um utilizador (*subscriber*) da base de dados do SM, baseado no identificador (subscriber Id) e no domínio (*domain*) dos SCE(s) em que o utilizador se encontra.
LogoutByMapping	Remove o registo de um utilizador (*subscriber*) da base de dados do SM, baseado unicamente no IP do utilizador.

Tabela 3. 2 Mensagens mais importantes que fluem na interface com o SM.

A existência de várias mensagens de *Logout* deve-se somente a questões de desempenho da operação. Ou seja, se usarmos o método *Logout* com mais informação do utilizador, a operação torna-se mais eficiente, no entanto pode haver situações onde não será possível ter acesso a toda informação.

- **Interface com o Service Control Engine (SCE):**

Na Tabela 3.3 serão descritas as principais mensagens desta interface.

Método	Descrição
Login	Adiciona ou altera a informação (IP, Política) de um utilizador (*subscriber*) no SCE.
Logout	Remove a informação de um utilizador (*subscriber*) do SCE
ProfileUpdate	Altera a política/perfil de um utilizador (*subscriber*) já existente no SCE

Tabela 3. 3 Mensagens mais importantes que fluem na interface com o SCE.

3.5 Implementação

Esta secção descreve a implementação do módulo PCRF. Na descrição da sua concepção serão apresentadas as várias perspectivas da sua elaboração:

i) A perspectiva lógica onde será visível a interacção das várias entidades;

ii) A perspectiva funcional dos componentes que compõem o PCRF

iii) A perspectiva física.

Alguns pormenores específicos da implementação serão omitidos, uns por motivos de confidencialidade, outros por serem bastante específicos e de baixo nível, não se adequando ao contexto deste documento.

3.5.1 Perspectiva Lógica

A perspectiva lógica da solução pode ser vista como a interacção entre 3 entidades lógicas, como é apresentado na Figura 3.3.

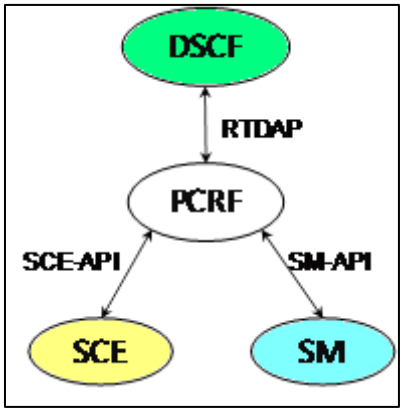

Figura 3. 3 Diagrama lógico das entidades.

A interface RTDAP, que foi descrita na secção 3.3.1. será usada para comunicar com o DSCF, nesta interface será transportada toda a informação necessária para a aplicação das políticas aos utilizadores.

A interface com o SCE é feita através da SCE API, permitindo a comunicação entre o PCRF com um ou vários CISCO SCE. Os métodos e os parâmetros da API são transpostos para mensagens específicas do interface RTDAP. De forma análoga, as mensagens RTDAP são transpostas para os métodos da API.

A interface com o SM é feita igualmente usando uma API fornecida pela CISCO, neste caso a SM API. Com esta podemos enviar mensagens de gestão dos utilizadores para o SM, permitindo assim, abstrairmos das conexões e gestão dos vários SCE(s), ficando estas a cargo do SM. Da mesma forma como no interface SCE, as mensagens RTDAP serão transpostas para métodos da SM API e vice-versa. A definição de cores nas entidades que irão interagir como o PCRF assumirá importância nos próximos diagramas, visto que os elementos definidos e implementados por lidar com as interfaces terão a mesma cor.

3.5.2 Perspectiva Funcional

Nesta secção serão apresentadas a forma como as entidades externas, interagem com o PCRF, assim como os componentes internos que lidam com as interfaces. Serão também mencionados alguns componentes incluídos no PCRF necessários para o seu enquadramento no sistema DSCP.

A perspectiva funcional pode ser vista como um diagrama de *uses cases* especificado em UML [61], existindo actores externos ao sistema PCRF. Os três actores que irão interagir com o PCRF são:

- DSCF: Sendo este um componente dentro do sistema DSCP, terá a função de actor na relação com o sistema PCRF. A interacção deste com o PCRF será feita recorrendo ao interface RTDAP, descrita na secção 3.3.1;

- OAM: Este actor tem a designação de *Operation and Management,* tendo a função de operar e configurar o PCRF;
- SM: É o actor que representa o *Subscriber Manager* da CISCO, este irá interagir com o sistema PCRF usando a interface descrita na secção 3.3.2;
- SCE: É o actor que representa o CISCO SCE, este comunica com o sistema PCRF usando a interface descrita na secção 3.3.2.

O diagrama de *uses cases* do sistema PCRF é apresentado na Figura 3.4. Da análise da Figura 3.4 concluímos que o PCRF irá implementar três *handlers* responsáveis por lidar com as ligações com as respectivas interfaces, sendo eles expressos na forma de *uses cases,* tendo a designação de *RPConnectionHandler* identificado na figura com a cor verde, o *SMConnectionHandler* com a cor azul e *SCEConnectionHandler* com a cor amarela respectivamente. Existe um *use case* com funcionalidade de configuração e operação do modulo PCRF, sendo representado por *Config Operation*.

As funcionalidades que o sistema PCRF terá de suportar para se enquadrar no sistema DSCP são:

- A geração e gestão de alarmes: funcionalidade reapresentada no diagrama pelo *uses case Alarms*;
- Monitorização do estado do módulo: funcionalidade representada pelo *use case StatsHandler*;
- Utilização de temporizadores: funcionalidade reapresentada pelo *use case TimersHandler*.

O *use case* que pode ser visto como nó central de todo o sistema PCRF, tem a designação de *Main*, este terá a função de permitir conectividade com todos actores no diagrama.

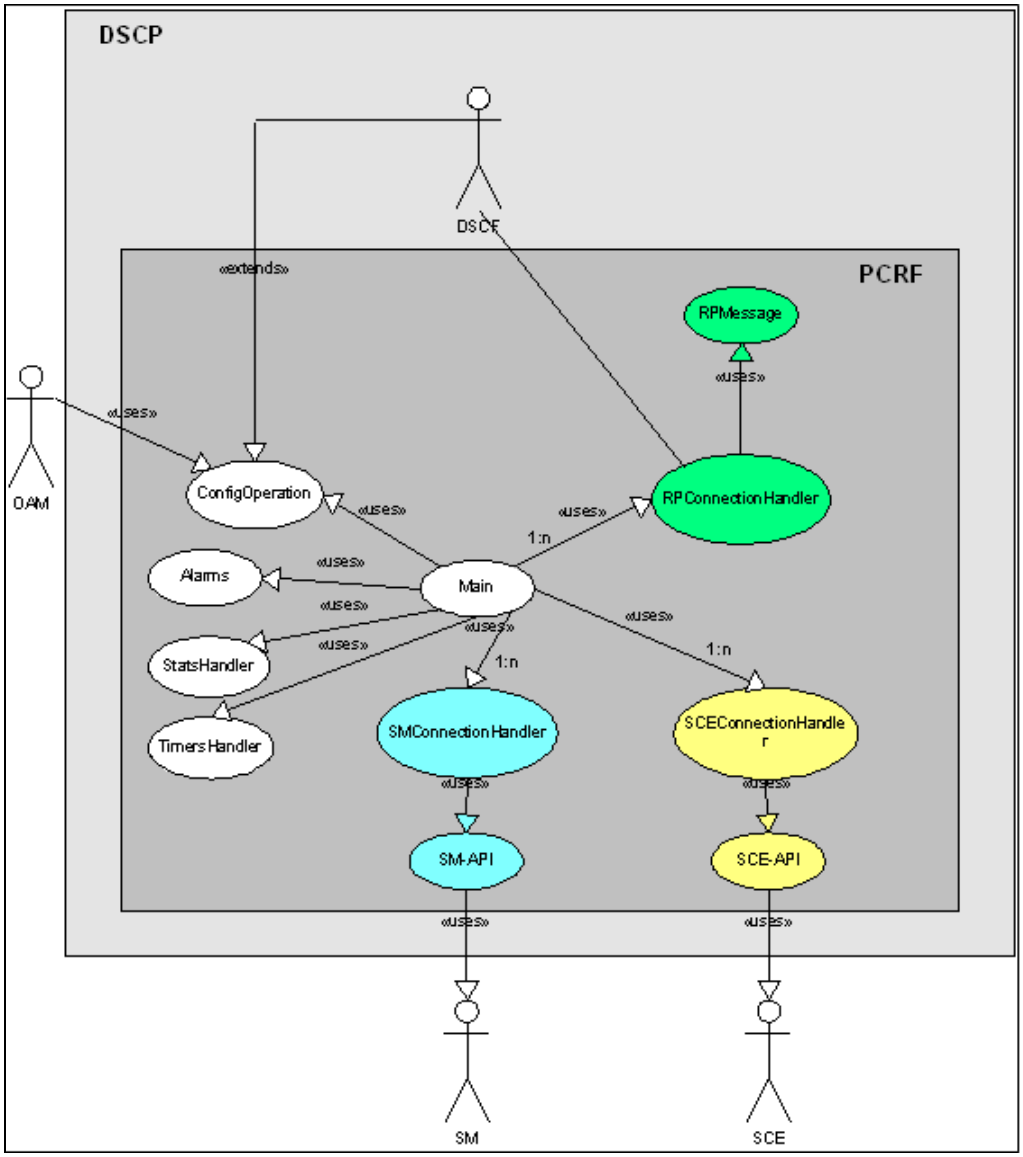

Figura 3. 4 Diagrama de *uses cases* do sistema PCRF.

3.5.3 Perspectiva Física

Depois da exposição das duas perspectivas de mais alto nível da implementação da solução, serão agora descritos os componentes que compõem o módulo PCRF assim como os elementos que interagem com este. A título de exemplo também se apresentarão em secção posterior, pequenos extractos de pseudo-código referentes à implementação de determinados objectos desenvolvidos. A Figura 3.5 ilustra o diagrama de componentes e a sua tipologia, que dá suporte à solução desenvolvida.

A implementação do módulo PCRF desenvolvido será baseada no paradigma de programação orientada a objectos *Object Oriented Programming* (OOP) [62]. Portanto, diversos dos componentes do PCRF podem ser expressos em entidades presentes em OOP. Os objectos e componentes referentes à interface descrita na secção 3.3.1. estão identificados na Figura 3.5 com a cor verde. Os objectos e componentes referentes as interface descritas em 3.3.2. estão identificados, no caso da interface com o SM com a cor azul, no caso do interface com o SCE com a cor amarela.

Os objectos presentes no PCRF são:

- *SM*: Objecto interno que irá lidar com a manipulação da SM-API;
- *SCE*: Objecto interno que irá lidar com a manipulação da SCE-API;
- *RPConInt*: Objecto responsável em lidar com as ligações RTDAP;
- *ProcessRPMsg*: Objecto responsável em processar as mensagens RTDAP;
- *Main*: Objecto principal responsável por gerir a ligação com os restantes objectos;
- *SigRecvServer*: Objecto responsável por gerir os sinais recebidos pelo módulo;
- *FileReader*: Objecto responsável por ler de um ficheiro a configuração do módulo;
- *Trace*: Objecto que gere o *trace* das sessões;
- *ReportManager*: Objecto que tem a função de controlar a monitorização do módulo e das suas acções;
- *Alarm*: Objecto responsável por gerar alarmes;

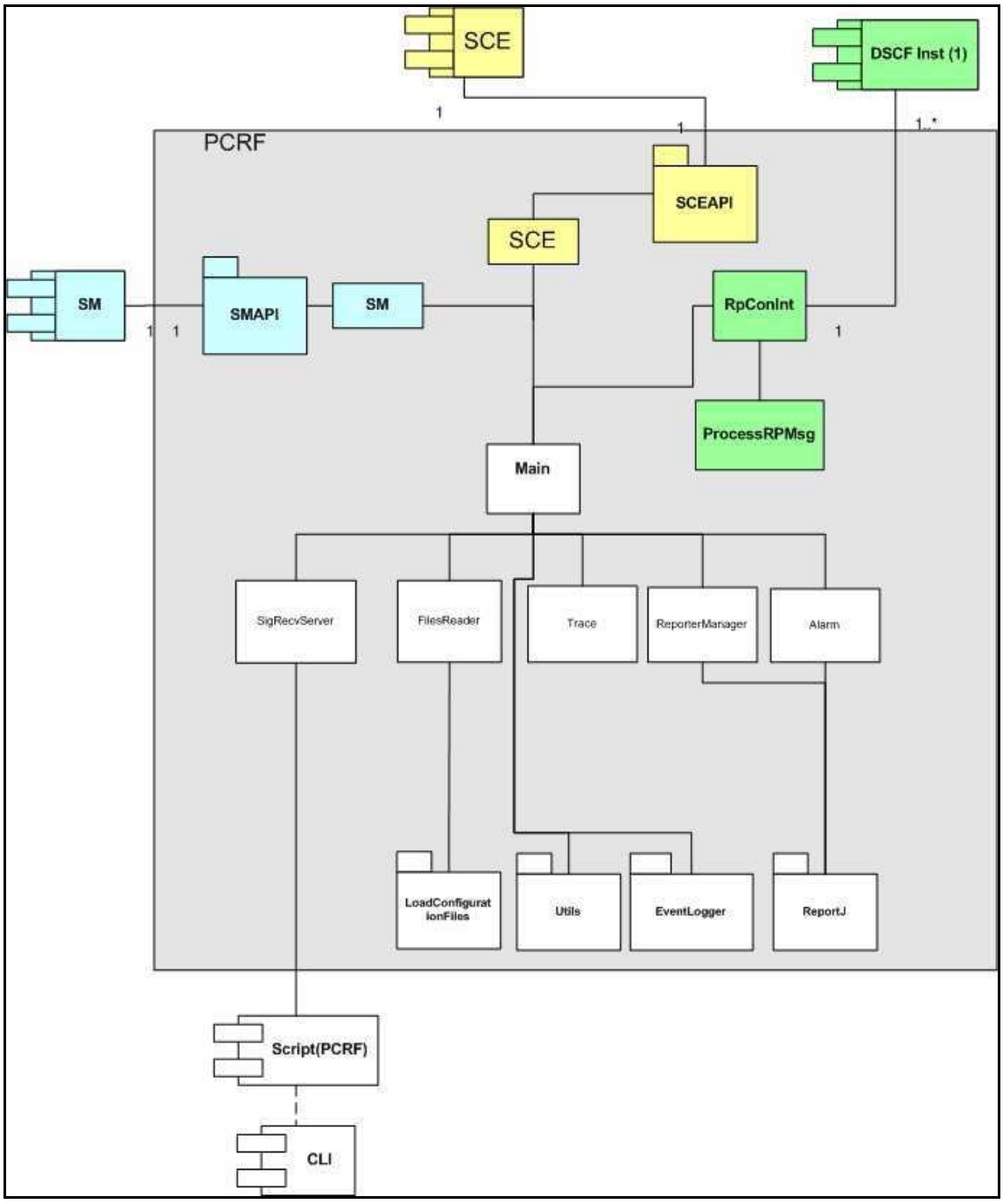

Figura 3. 5 Diagrama de componentes e objectos do PCRF desenvolvido.

Os pacotes presentes no PCRF desenvolvido são:

- *SM API*: Este pacote contém a API da CISCO disponibilizando todos os métodos necessários para a manipulação do SM;
- *SCE API*: Este pacote contém a API da CISCO disponibilizando todos os métodos necessários para a manipulação do SCE;

- *LoadConfigurationFile*: Este pacote contém métodos e estruturas de dados que dão suporte à leitura do ficheiro de configuração;
- *Utils*: Este pacote contém métodos e estruturas de dados que irão dar suporte ao desenvolvimento dos vários objectos do PCRF;
- *EventLogger*: Pacote necessário para a implementação do sistema de *loggers,* seguindo a norma dos módulos do sistema DSCP;
- *RerportJ*: Pacote necessário para a implementação da funcionalidade de *Report*, seguindo a norma dos módulos do DSCP.

Os componentes externos do PCRF são:

- *SM*: *Subscriber Manager*
- *SCE*: CISCO *Service Control Engine*
- *DSCF*: *Data Service Control Function*
- *Script (PCRF)*: Script [63] responsável por receber os sinais do CLI e os enviar para o objecto interno do PCRF com a funcionalidade de os processar.
- *CLI: O Command Line Interface (CLI)*: o CLI [64] neste contexto é o componente responsável por enviar sinais de gestão ao PCRF.

3.5.4 Exemplo de implementação de alguns objectos

Analisando o diagrama presente na Figura 3.5 da secção anterior, podemos concluir que o objecto designado por *Main* é o objecto que lida com as interacções entre as interfaces, assim como os objectos mais secundários. Baseado nisto, e simplesmente a título de exemplo, será apresentado o pseudo-código do objecto *Main,* assim como um objecto que implementa a

comunicação com uma interface. Dada a analogia da implementação dos objectos que lidam com as três interfaces, será apresentado somente o pseudo-código do objecto que interage com o SM. As implementações dos objectos referentes às outras interfaces podem ser encontradas nos Anexo A1 (Pseudo-código SCE) e Anexo A2 (Pseudo-código ProcessRPMsg). As implementações dos outros objectos desenvolvidos no contexto deste projecto não se encontram neste documento.

- **Pseudo-código do objecto main:**

```
class PseudoMain {
//variables Declaration
MainConfReader mainConfObj;
InterfacesConfReader intConfObj;
Queue mainQueue;

AbstractList routeDSCFCnx;
AbstractList routeSMCnx;
AbstractList routeSCECnx;
// Methods Implementations
Object getObjectFromQueue(){
        Object obj;
        obj = this.mainQueue.dequeue();
        return obj;
        }

void addObjectToQueue(Object obj){
        this.mainQueue.enqueue(obj);
        }
// Main Implementation
void main(confFileMsg) {

mainConfObj =  MainConfReader(confFileMsg);
mainConfObj.readMainConf();
intConfObj =
InterfacesConfReader(mainConfObj.mainConfigurationFile.getCfgFiles().getInterfac
esFile());
intConfObj.readInterfaceFile();
//Going to read and start DSCF cnX
for(int i = 0; intConfObj.interfacesConfigurationFile.getDscfCount() > i; i++){
RPConInt dscfCnxP = new RPConInt();
dscfCnxP.setApplicationName(intConfObj.interfacesConfigurationFile.getDscf(i).ge
tPrimary().getApplicationName());
dscfCnxP.setHost(intConfObj.interfacesConfigurationFile.getDscf(i).getPrimary().
getAddress().getIp());
dscfCnxP.setPort(intConfObj.interfacesConfigurationFile.getDscf(i).getPrimary().
getAddress().getPort());
dscfCnxP.setDomain(intConfObj.interfacesConfigurationFile.getDscf(i).getDomain()
);
routeDSCFCnx.addObject(i,dscfCnxP);
}
//Going to read and start SM cnX
for(int i = 0; intConfObj.interfacesConfigurationFile.getSmCount() > i;i++){
SM smCnx = new SM();
smCnx.setDomain(intConfObj.interfacesConfigurationFile.getSm(i).getDomain());
smCnx.setHost(intConfObj.interfacesConfigurationFile.getSm(i).getSmAddress().get
Ip());
smCnx.setPort(intConfObj.interfacesConfigurationFile.getSm(j).getSmAddress().get
Port());
pcrfInst.routeSMCnx.addObject(i,smCnx);
}
```

```
//Going to read and start SCE cnX
for(int k = 0; intConfObj.interfacesConfigurationFile.getSceCount() > k;k++){
SCE sceCnxP = new SCE();
sceCnxP.setConnectionTyp(SCE_CON);
sceCnxP.setMode(intConfObj.interfacesConfigurationFile.getSce(k).getMode());
sceCnxP.setDomain(intConfObj.interfacesConfigurationFile.getSce(k).getDomain());
sceCnxP.setHost(intConfObj.interfacesConfigurationFile.getSce(k).getSce().getSce
Address().getIp());
sceCnxP.setPort(intConfObj.interfacesConfigurationFile.getSce(k).getSce().getSce
Address().getPort());
pcrfInst.routeSCECnx.addObject(k,sceCnxP);
}
        Object objRq;
        while(!this.Killed()){
        try {
                objRq = this.getObjectFromQueue();
            }
         if (objRq != null) {
        switch (objRq.session.actions){
        case SEND_TO_PCEF_INT:
        if(objRq.session.sMInterrogation == true){
        SM tmpCnx;
        tmpCnx = this.routeSMCnx.getObject(objRq.session.domain);
                if(tmpCnx != null){tmpCnx.addInputEvent(objRq.session);}
                else{this.print("Error routing Domain: "+objRq.session.domain);}
                                                        }
        }else{

        if(this.routeSCECnx.getObjectsList(objRq.session.domain).length==0){
                this.print("Error routing Domain: "+objRq.session.domain);
                }
        else{
        int sizeArray =
        this.routeSCECnx.getObjectsList(objRq.session.domain).length;
        for(int i=0;i<sizeArray;i++)
        {
 SCE TmpSCE = (SCE)this.routeSCECnx.getObjectsList(objRq.session.domain))[i];
                if(TmpSCE.getMode() == PULL)
        {
        String ipMsgSCE = objRq.session.getIPMSg;
if(ipMsgSCE.equals(TmpSCE.getIp())){ TmpSCE.addSceInputEvent(objRq.session);}
} else{ TmpSCE.addSceInputEvent(objRq.session);}

                        }
                }
        }
}
        case SEND_TO_RTDAP_INT:
        RPConInt tmpCnx;
        if(objRq.session.cnxRTDAPId > -1){
        tmpCnx = (RPConInt)this.routeDSCFCnx.getObject(objRq.session.cnxRTDAPId);
        } else{
        tmpCnx = (RPConInt)this.routeDSCFCnx.getObject(objRq.session.domain);}
        if(tmpCnx != null){
        tmpCnx.getProcessRpMsgInst().addObjectToQueue(objRq.session);}
        else{this.print("Error routing Domain: "+objRq.session.domain);
                                }
                        }
                }
        }
}
```

Figura 3. 6 Pseudo-código do objecto Main.

O pseudo-código do objecto *Main* representado na Figura 3.6 resume as funções e o comportamento que este objecto irá ter. O objecto *Main*, inicialmente lê do ficheiro de configuração toda a informação necessária para a definição do seu comportamento e instanciação de componentes. Numa fase posterior o objecto é responsável por encaminhar as mensagens para as respectivas a interfaces.

- **Pseudo-código do objecto SM:**

```
class PseudoSM {

String ip;
int port;

String  domain;
SMNonBlockingApi  smAPI;

Queue queueSMQueue;

public SM()
        {
                smAPI.init();
                smAPI.connect()
                this.start();
        }

void addInputEvent(Object session)
        {
                this.queueSMQueue.enqueue(session);
        }

        Object getInputEvent()
        {
                Object obj;
                try{
                        obj= this.queueSMQueue.dequeue();
                }
                return obj;
        }

        void loginReq(Session session)
        {
                try{
                        smAPI.login(session.subscriberId,
                                        session.ip,
                                        session.typeIP,
                                        session.property,
                                        session.propertyValues,
                                        session.domain,
                                        session.networkaAdditive,
                                        session.autoLogoutTime);
                }
        }
        void logoutReq(Session session)
        {
                try{
                        smAPI.logoutByNameFromDomain(session.subscriberId,
                                        session.ip,
                                        session.typeIP,
                                        session.domain);
                }
        }
```

```
boolean processInputOperation()
{
        Session s = (Session) this.getInputEvent();
        switch(s.operation)
        {
        case LOGINRQ:
        {
                this.loginReq(s);

        }
        case UPDATERQ:
        {
                this.loginReq(s);

        }
        case LOGOUTRQ:
        {
                this.logoutReq(s);
        }

        return true;
        }

}
void start()
{
        try{
                while(!main.Killed())
                {
                        processInputOperation();
                }
        }
        this.disConnect();
}
```

Figura 3. 7 Pseudo-código SM.

A Figura 3.7 resume o comportamento que objecto *SM* irá ter. O objecto *SM* baseado nas mensagens que recebe do objecto *Main* faz o seu respectivo processamento enviando as operações para o SM.

3.5.5 Tecnologias Utilizadas

Nesta secção serão descritas as tecnologias e especificações dos equipamentos utilizados no desenvolvimento da solução, assim como os ambientes de instalação e utilização da mesma. A descrição e as especificações serão as mais sucintas possíveis centrando-se unicamente no essencial para a implementação da solução.

- **Linguagem de Programação**

As API's disponibilizadas pela CISCO para o provisionamento dos subscritores no SM [59] e da manipulação do CISCO SCE [58] são disponibilizadas na forma de *packages* para ambientes de desenvolvimento em linguagem JAVA [web3] na versão 1.4.2. Este facto, restringiu a implementação do módulo PCRF, sendo adoptada a mesma versão do JAVA para o desenvolvimento do módulo.

- **Subscriber Manager (SM)**

O componente Subscriber Manager, como referido anteriormente, foi desenvolvido pela CISCO para dar suporte na função de subscrição dos utilizadores/clientes no *Subscriber Manager* (SM).

Para dar suporte na tarefa de armazenamento da informação dos subscritores, o SM recorre à utilização de uma base de dados em memória da ORACLE, com a designação de *Oracle TimesTen In-Memory DataBase* [web4]. Desta forma, é permitindo disponibilizar uma plataforma de tempo real, desenhada para eventos que exijam baixas latências e transferências de grande volume de informação.

O *Subscriber Manager* na solução implementada pela PT Inovação vai ser instalado em ambiente Unix [65]. A configuração do SM será feita através de um ficheiro de configuração, podendo os parâmetros ser configuráveis dependendo do cenário que operador vier a implementar.

- **CISCO Service Control Engine(SCE)**

O CISCO *Service Control Engine* (SCE) [44] a ser utilizado no projecto é um equipamento da série 2020*,* especialmente desenhado para lidar com classificação de sessões de dados, providenciando controlo ao nível IP por subscritor.

O CISCO SCE tem como base uma arquitectura baseada em processadores *high-speed Reduced Instruction Set Computer* (RISC) [66],

permitindo um alto desempenho na medição e controlo do tráfico. O CISCO SCE consegue gerir dois milhões de fluxos de aplicações sobre redes IP. Outra funcionalidade é a possibilidade de programação na perspectiva de detecção e controlo dos protocolos, nomeadamente no reconhecimento do tráfego P2P.

A descrição detalhada da configuração do CISCO SCE a utilizar na solução não se adequa neste documento, uma vez que diz respeito a políticas internas que os operadores possam vir a definir.

- **Ambiente de Funcionamento do PCRF**

O ambiente de instalação e funcionamento do PCRF dependerá do cenário que o operador irá implementar, sendo a arquitectura da solução desenhada para funcionar em arquitecturas Itanium e Xeon ambas da Intel. Estas arquitecturas terão de ter os seguintes requisitos mínimos:

Itanium:

- 2 CPU's IA 64 1.4 GHz
- 10 Mbytes espaço disponível em disco.
- 30 Mbytes de memória requerido.

Xeon:

- 4 CPU's Intel(R) Xeon (TM) 2.4 GHz
- 10 Mbytes espaço disponível em disco.
- 30 Mbytes de memória requerido.

A nível dos requisitos de software o PCRF necessita:

- Um sistema Linux: A solução foi desenhada para funcionar na distribuição Linux Red Hat AS3.
- NGIN CLI V4.4.0: Módulo desenvolvido pela PT Inovação e já descrito anteriormente.

- JRE 1.4.2 *Virtual machine* JAVA 1.4.2: sendo imperativo o ambiente ter instalado esta versão.
- Perl V5.8.0: Necessário para a utilização da *script* que lida com os sinais enviados para o PCRF.

3.6 Notas finais

Este capítulo pode ser visto como um resumo do processo de desenvolvimento da solução. Nesse sentido, foi apresentado o contexto onde a solução vai assentar, assim como todos os componentes que vão fazer parte desta. De igual forma, foi referenciada a especificação das interfaces desenvolvidas, bem como apresentados pormenores relativos à implementação realizada, nas perspectivas lógica, funcional e física.

Após a descrição do desenvolvimento, serão apresentados os cenários de utilização e evidência de resultados obtidos no próximo capítulo.

4 Cenários de Utilização e Testes

Neste capítulo serão apresentados os diferentes cenários de utilização da solução, podendo ser encontrados na secção 4.1 deste capítulo. Para além dos cenários de utilização serão apresentados testes efectuados em ambiente real, referidos na secção 4.2. O conhecimento dos componentes da solução apresentados no capítulo anterior, assim como a sua forma de interacção, serão essenciais para a percepção dos cenários de utilização apresentados. No final serão apresentadas evidências da aplicação das políticas: *i*) no tráfego de um utilizador em particular, *ii*) na limitação da largura de banda de um protocolo específico; e *iii*) na largura de banda global de um operador.

4.1 Cenários de Utilização

Os cenários de utilização da solução estudados neste trabalho podem ser divididos em dois grupos:

- Interacção directa com o componente SCE (*Service Control Engine*): nestes cenários o PCRF (*Policy Control and Charging Rules Function*) interage directamente com o SCE.
- Interacção com o componente SCE via SM (*Subscriber Manager*): nos cenários apresentados o PCRF interage directamente com o SM, sendo este o responsável por gerir a comunicação com o SCE.

A representação dos cenários será feita com base em diagramas de sequência UML [61]. Os componentes que fazem parte da arquitectura da solução serão representados através de objectos e as entidades externas como actores. As mensagens que fluem entre os objectos são indicativas da

acção a ser desempenhada. A comunicação na maior parte dos casos segue uma lógica de Pedido/Resposta.

As funcionalidades das entidades presentes no diagrama são as seguintes:

- AAA[9]: Esta entidade tem as funções de autenticação, autorização e *accouting* para um dado cliente, enviando a informação relativamente a estas funções, na forma de pedidos RADIUS [39] para o Radius Handler (RHng).
- RHng: Este componente é responsável por enviar para o DCSF a informação dos pedidos RADIUS, que por sua vez vão ser mapeados em mensagens de autenticação e subscrição. A descrição deste componente foi realizada na secção 3.2.2.
- DSCF: Componente responsável por interligar o PCRF, o RHng e a SL, processando as mensagens provenientes destas identidades. A descrição deste componente foi realizada na secção 3.2.2.
- SCE: CISCO SCE, componente físico já descrito anteriormente na secção 3.3.2.
- PCRF: Componente desenvolvido neste trabalho, descrito na secção 3.2.2.
- SL: *Service Logic:* Entidade que representa a lógica de serviço do operador.
- GGSN: Esta entidade representa o *Gateway GPRS Support Node* (GGSN), descrito na secção 3.2.2.
- Utilizador: Entidade que representa o utilizador do serviço, neste caso o cliente do operador.

9 Da terminologia inglesa: *Authentication, Authorization and Accounting*

4.1.1 Utilização Directa via SCE

Nesta secção serão apresentados os cenários de funcionamento da solução, em que a comunicação com o SCE é feita directamente via o PCRF. Os cenários apresentados são os seguintes:

- Login: o cenário *Login* representa a operação de *accounting* de um utilizador, sendo traduzido neste caso na autenticação de um cliente no SCE. Neste cenário será indicado ao SCE: *i*) o identificador (*subscriberId*) que o cliente terá na sessão; *ii*) o seu IP; *iii*) a política/perfil que vai ser associado ao controlo do tráfego gerado por este. Como foi dito anteriormente, o SCE tem dois modos de configuração no que diz respeito a forma de autenticação, o modo *push e pull*, este facto levou a dois cenários de *Login*, um para cada modo de funcionamento.

- Actualização da Política: Este cenário representa a alteração da política/ perfil associada a um utilizador.

- Logout: O cenário de *Logout* representa a remoção da informação do IP referente a um subscritor no SCE, isto é, representa que um determinado utilizador não será mais controlado. De forma análoga ao cenário *Login* também existirão os dois cenários na operação de *Logout* no SCE, mediante o modo em que o SCE este está configurado.

Login modo *Push*

O processo de *Login* de um utilizador em que o SCE é configurado em modo *Push* é ilustrado no diagrama da Figura 4.1. A interacção entre as diversas entidades presentes no diagrama da Figura 4.1 é a seguinte:

- O GGSN identifica que um utilizador pretende usar um serviço de rede, sendo iniciado o processo de autenticação, autorização e subscrição do serviço. O GGSN envia um pedido de iniciação de sessão designado de *accounting start*, este será interpretado pelo *Radius Handler* (RHng).

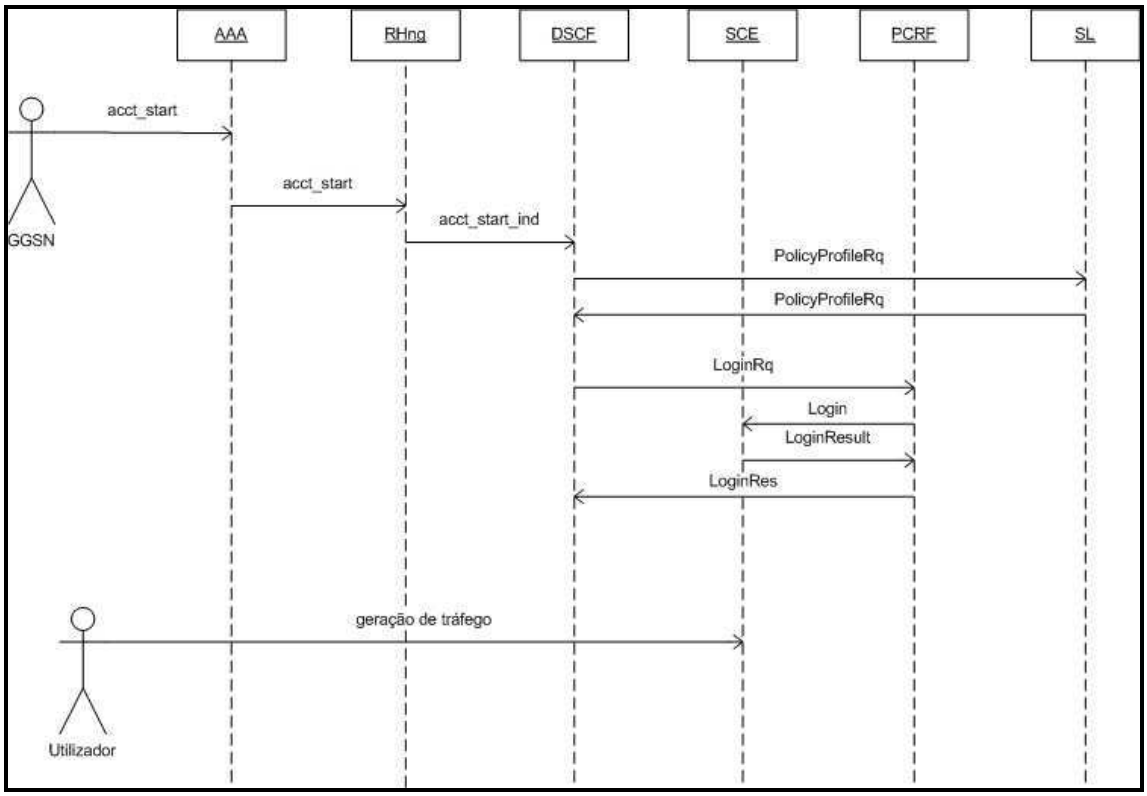

Figura 4. 1 Login de um utilizador, com o SCE em modo *Push*.

- O RHng recebe o pedido de *accounting start* e encaminha-o para o DSCF correspondente.
- O DSCF interpreta o pedido, questionando de seguida a lógica do operador (representada no diagrama por SL), para saber a respectiva política a aplicar para o cliente em questão.
- A SL com base no MSISDN e na informação associada a este, envia uma mensagem com perfil/política para o DSCF.
- O DSCF contendo já a informação necessária a fornecer ao SCE, envia para o PCRF o pedido de *Login* via a interface RTDAP já descrita anteriormente.
- O PCRF analisa o pedido de *Login,* enviando-o ao SCE correspondente, permitindo assim o SCE controlar o tráfego da sessão.
- Finalizado a fase de associação de política, o utilizador gera tráfego mediante as regras definidas na política.

Login modo *Pull*

O *Login* de um utilizador em que o SCE é configurado em modo *Pull,* tem algumas semelhanças com o *Login* em modo *Push,* sendo alterada a forma como é feita a inserção do utilizador e no instante em que é feita. A ilustração do diagrama do cenário de *Login* em modo *Pull* pode ser encontrada no Anexo B1 Login modo Pull.

Actualização da Política

O cenário de actualização da política pode ser visto como o mais interessante e o que pode originar mais serviços de valor acrescentado para os operadores. Através deste mecanismo pode-se alterar em tempo real a política associado ao utilizador, mediante diversos factores (e.g. a hora de acesso, tráfego consumido, promoções, entre outras).

O cenário de actualização da política apresentado na Figura 4.2 ilustra a situação em que o utilizador, depois de lhe ser atribuído a política, está a utilizar um determinado serviço. A SL baseada em diversas condições, envia um pedido de mudança de perfil para o DSCF, sendo obviamente o principal destinatário o SCE.

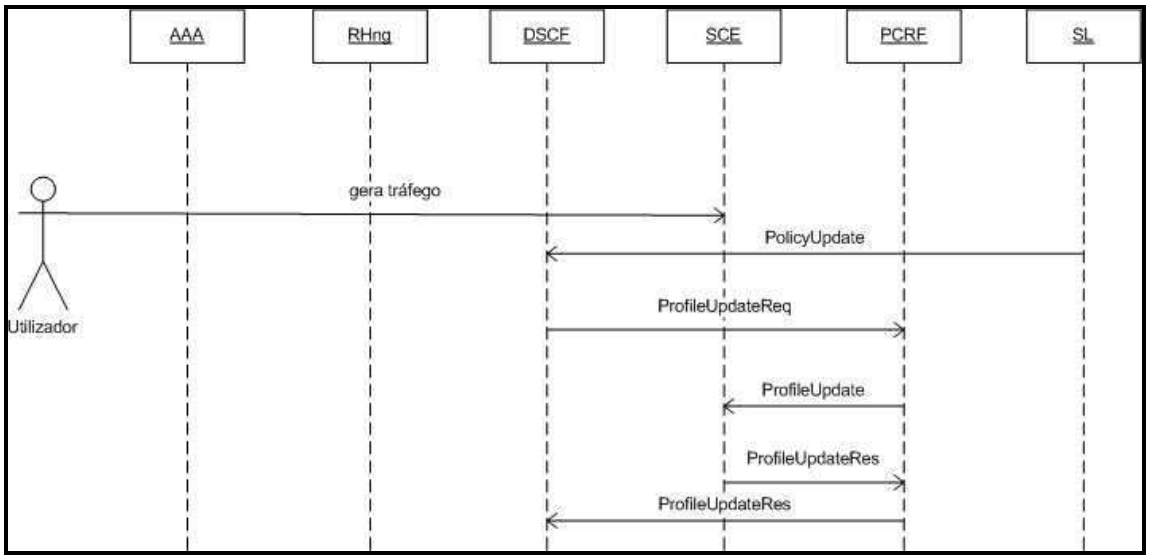

Figura 4. 2 Actualização da política directamente no SCE.

A interacção entre as diversas entidades presentes na Figura 4.2 é a seguinte:

- A SL baseado em critérios estabelecidos envia para o DSCF o pedido de alteração da política.
- O DSCF envia para o PCRF o pedido de alteração da política.
- O PCRF após receber o pedido de alteração de perfil indica ao SCE correspondente que o cliente com o MSISDN recebido terá uma nova política associada.
- O SCE com a nova relação utilizador/política altera a forma de controlo do tráfego para este utilizador.

Logout modo *Push*

Os cenários de *Logout* representam o final de uma sessão de um utilizador. O fim de sessão do ponto de vista do SCE é quando o IP associado a um dado utilizador é removido. Os cenários de *Logout*, de uma forma análoga aos cenários de *Login*, também irão depender do modo da configuração do SCE, ou seja modo *Push* ou *Pull.* O *Logout* no modo *Push* está ilustrado na Figura 4.3:

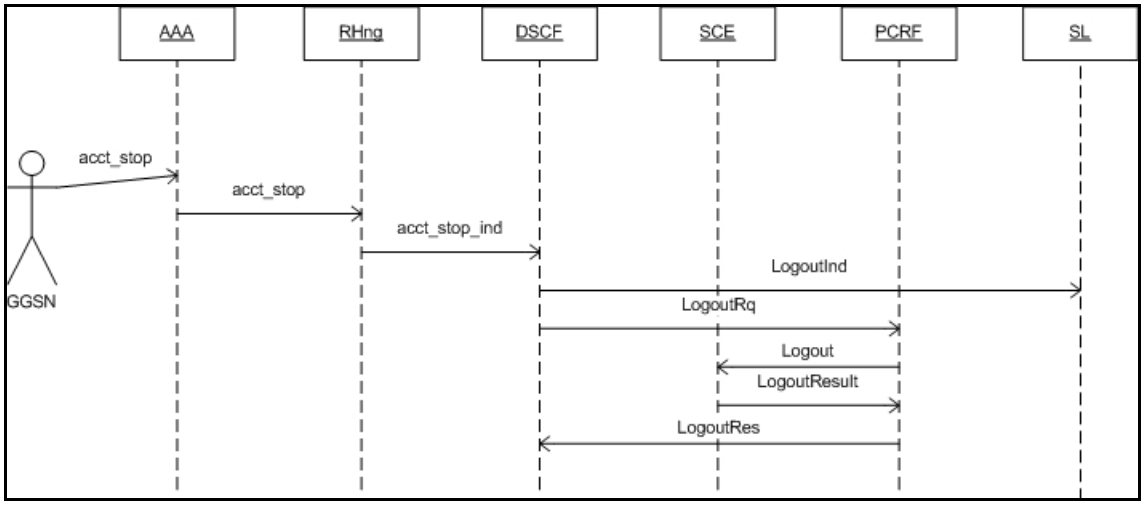

Figura 4. 3 Logout de um utilizador, com o SCE em modo *Push.*

A interacção entre as diversas entidades é a seguinte:

- O GGSN identifica que um utilizador pretende finalizar um serviço de rede. O GGSN envia a mensagem de finalização de sessão

designado de *accounting stop* que será interpretado pelo *Radius Handler* (RHng).

- O RHng recebe o pedido de *accounting stop* e encaminha o para o DSCF correspondente.
- O DSCF interpreta o pedido e indica a SL que o utilizador não irá mais utilizar o serviço, consequentemente envia o pedido de *Logout* para o PCRF.
- O PCRF baseado no pedido recebido, indica ao SCE que o utilizador não irá mais utilizar o IP da sessão.
- O SCE remove a associação utilizador/IP.

Logout modo Pull

O cenário de *Logout* em modo *Pull*, com o SCE configurado para tal, irá ocorrer quando estiver definido por um exemplo um tempo de *timeout* para as sessões. Neste caso o SCE inicia o processo de *Logout* de um utilizador. O cenário de *Logout* no modo *Pull* pode ser visto no Anexo B2 Logout modo Pull.

4.1.2 Utilização via SM

Nesta secção serão apresentados os cenários de funcionamento da solução, onde a comunicação com o SCE é feita via o SM. O PCRF terá a função de interagir com o SM nas operações de *Login,* actualização da política e *Logout.* A finalidade dos cenários será a mesma do que a dos anteriores, alterando somente a interacção dos componentes. Este facto leva a descrição dos cenários ser mais breve do que na secção anterior, feita referencia somente aos pormenores que variam.

Login modo *Push*

Como foi referido anteriormente a finalidade do cenário de *Login* é a mesma do que na secção anterior, alterando unicamente a forma como o PCRF indica a política a aplicar para um dado utilizador no SCE. A Figura 4.4

ilustra a troca das mensagens entre os componentes, sendo bastante semelhante ao cenário ilustrado na Figura 4.1, com a diferença que o *login* é feito no SM e não no SCE.

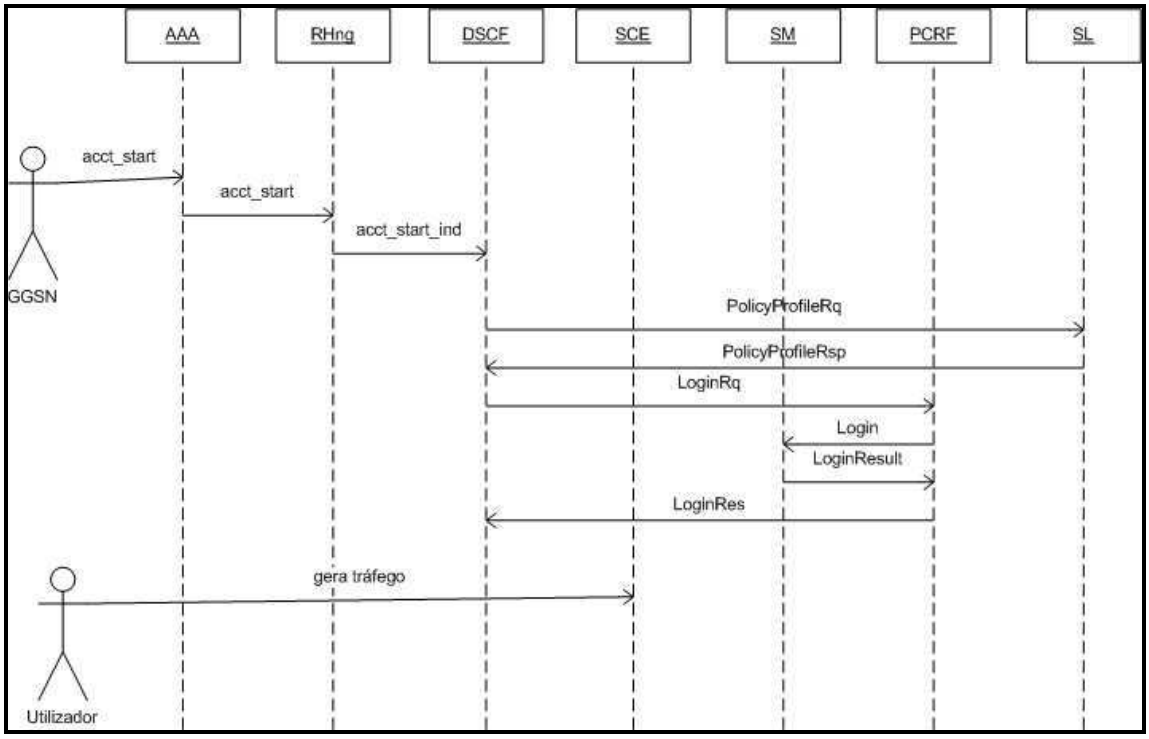

Figura 4. 4 Login de um utilizador via SM com o SCE em modo *Push.*

Login modo *Pull*

O cenário de *Login* em modo *Pull* via SM tem algumas particulares. Uma delas é derivada ao facto de SM fazer a gestão dos utilizadores, tendo a capacidade de armazenar a última política associada a estes. Este facto leva a que quando o SCE questiona o SM acerca da política a aplicar a um utilizador, se este tiver registado no SM, a política é logo atribuída. Se não houver a informação do utilizador é atribuída a política por defeito ficando o SM a espera do *Login* do PCRF. O diagrama da operação pode ser encontrado no Anexo B3 Login via SM modo Pull.

Actualização da Política

A interacção das entidades no cenário de actualização da política via SM é extremamente parecida com a do cenário onde esta actualização é feita directamente com o SCE, existindo somente duas diferenças. A primeira é não existir a operação *ProfileUpdate* para alterar a política no SM, sendo necessário efectuar novamente a operação *Login* no SM com a nova política. A segunda é a comunicação ser feita via SM e não directamente via SCE. O cenário de actualização da política via SM pode ser visto na Figura 4.5:

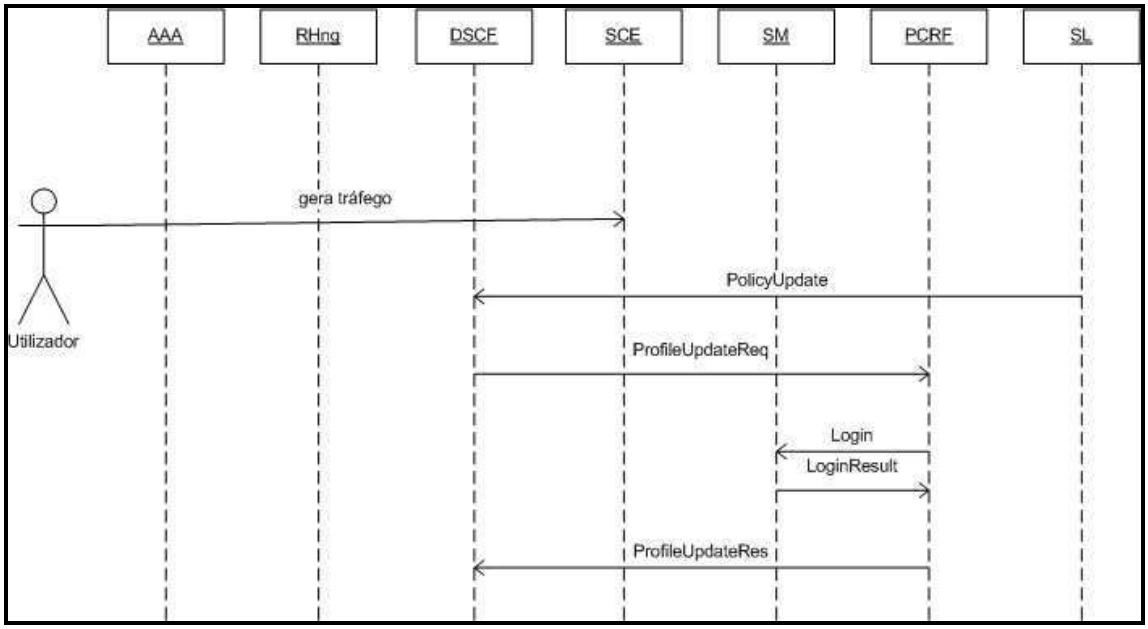

Figura 4. 5 Actualização das políticas via SM.

Logout

A utilização do SM permite uma abstracção na gestão das mensagens de *Logout Indication* vindas do SCE, deixando para o PCRF a tarefa de indicar quando um IP deixa de ser utilizado. Este facto leva a só existir um cenário de *Logout* via SM, independentemente o modo em que SCE está configurado. O cenário de *Logout* via SM pode ser visto na seguinte Figura 4.6.

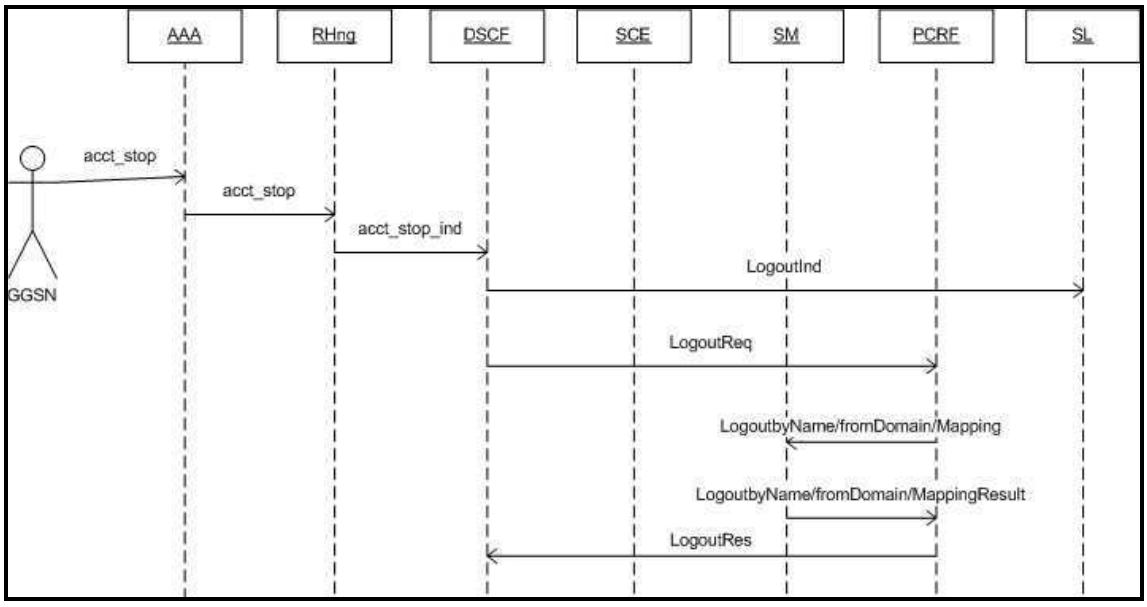

Figura 4. 6 Logout de um utilizador via SM.

A interacção das entidades é análoga à descrita na secção da operação *Logout* com o SCE configurado no modo *Push*. A operação de *Logout* no SM pode ser realizada de três formas diferentes, como descrito na secção onde é apresentada a interface com o SM (secção 3.3.2).

4.2 Testes em Ambiente Real

Após a apresentação dos cenários de utilização em que solução poderá funcionar, serão apresentados testes concretos. Na apresentação dos testes, serão apresentados três cenários em que a solução poderá funcionar:

i) Cenário de *Login*;

ii) Cenário de actualização da política;

iii) Cenário de *Logout;*

A comunicação com o SCE nestes cenários será feita via SM, estando o SCE configurado no modo *Push*. A referência à comunicação com a *Service*

Logic (SL) representada nos cenários de utilização vão ser omitidos, uma vez que fazem parte da lógica de negocio do operador e não da solução de controlo de tráfego em si.

Nos três cenários anteriormente referidos, a visualização da interacção entre os módulos será feita com base em *logs* que cada identidade irá emitir no fluxo de uma sessão, ilustrando assim resultados obtidos em cenários reais.

4.2.1 Iniciação de uma sessão com uma determina política

O primeiro teste a ser descrito é a inicialização de uma sessão por parte de um utilizador. O *Radius Handler* (RH), como primeiro componente da solução, irá receber o pedido de inicialização da sessão, fazendo o respectivo mapeamento da informação para operação *Login,* sendo interpretado pelo DSCF. O DSCF irá enviar para o PCRF toda a informação necessária para este poder fazer o *Login* do utilizador no SM. A descrição dos *Logs* de cada módulo será feita de seguida.

Inicio da sessão recebido no RHng

O *Radius handler* irá receber mensagens de *accounting start* provenientes do GSSN, sendo o RHng responsável por enviar os parâmetros RADIUS necessários para o mapeamento da operação *Login* no DSCF. A mensagem recebida no RHng e o seu respectivo mapeamento na operação Login recebida no DSCF pode ser vista na Figura 4.7.

Na Figura 4.7 está identificada com cor azul a informação mais importante da mensagem recebida no RHng e enviada para o DSCF.

```
Parâmetros Radius:
Logs no RHng:

2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: Acct-Status-Type = Start
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: Acct-Session-Id = "00000ACB"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: NAS-IP-Address = 192.168.78.97
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: Framed-IP-Address = 192.168.78.147
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: Calling-Station-Id = "069069096"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: Configuration-Token = "ME***"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: Called-Station-Id = "pcrf.med***.**"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: Connect-Info = "wap.meditel.ma"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: 3GPP-GPRS-Negotiated-QoS-profile = "98-
FFFFFF"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: 3GPP-PDP-Type = 1
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: 3GPP-IMSI = "069069096"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: 3GPP-Charging-ID = 147
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: 3GPP-Attr-18 = 0x3131313131
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: 3GPP-SGSN-Address = 41.205.207.0
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: 3GPP-GGSN-MCC-MNC = "22222"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: 3GPP-GGSN-Address = 1.1.1.1
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: 3GPP-IMSI-MCC-MNC = "33333"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: 3GPP-NSAPI = "0000"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: 3GPP-Selection-Mode = "4444"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: User-Name = "MT-ME***-147-069069096-
PCRF-GPRS"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: Client-IP-Address = 192.168.78.38
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: Acct-Unique-Session-Id =
"761a7144d5749447"
2008-07-29 15:05:11.323 RAD_LOG      INF 2 | VALUE: Realm = "NULL"

Mapeamento do acct-start em Login Request no DSCF:


2008-07-29 15:05:11.275 TRACE        INF 1 | [] | RECV: ===> RP_OPER[0] CallId[125], OpCode
= [309]
        ------------------------------------------------------------------------------
                 OperatioName[RH:LoginReq]
        ------------------------------------------------------------------------------
         RP     | IN  |    0 | $OperationCode    | 309
         RP     | IN  |    1 | $Framed-IP-Addres| 192.168.78.147
         RP     | IN  |    2 | $NAS-IP-Address   | 192.168.78.97
         RP     | IN  |    3 | $Acct-Session-Id  | 00000ACB
         RP     | IN  |    4 | $Calling-Station-| 069069096
         RP     | IN  |    5 | $rQoS             | 98-FFFFFF
         RP     | IN  |    6 | $IMSI             | 069069096
         RP     | IN  |    7 | $Called-Station-I| pcrf.med***.**
         RP     | IN  |    8 | $SGSN-IP-Address  | 41.205.207.0
         RP     | IN  |    9 | $GGSN-IP-Address  | 1.1.1.1
        ------------------------------------------------------------------------------
2008-07-29 15:05:11.275 TRACE        INF 1 | [] | CORE: CallId[125] is in state
WAITING_FOR_PROCESSING
```

Figura 4. 7 Logs do inicio da sessão, no RHng e no DSCF.

- *Acct Status-Type*: Neste teste o valor deste parâmetro é igual a *start,* identificado o inicio de sessão.
- *Framed-IP-Address*: Este parâmetro contém o IP do utilizador, neste caso é o IP: 192.168.78.147.
- *Calling-Station ID*: Este parâmetro contém o MSIDN do utilizador, sendo o identificador do utilizador na sessão, nesta caso é o número 069069096.

Login processado no DSCF

O DSCF após receber a pedido de *Login* vindo do RHng faz o respectivo processamento de forma a identificar a política a aplicar para o utilizador em questão, assim como a forma de envio (directamente/via SM) da informação para o SCE. Este processo pode ser observado na Figura 4.8.

```
Login Request vindo do RHng processado no DSCF:

        ------------------------------------------------------------------------------
                 OperationName[RH:LoginReq]
        ------------------------------------------------------------------------------
         RP     | IN  |   0 | $OperationCode    | 309
         RP     | IN  |   1 | $Framed-IP-Addres| 192.168.78.147
         RP     | IN  |   2 | $NAS-IP-Address   | 192.168.78.97
         RP     | IN  |   3 | $Acct-Session-Id  | 00000AD7
         RP     | IN  |   4 | $Calling-Station-| 069069096
         RP     | IN  |   5 | $rQoS             | 98-FFFFFF
         RP     | IN  |   6 | $IMSI             | 069069096
         RP     | IN  |   7 | $Called-Station-I| pcrf.med***.**
         RP     | IN  |   8 | $SGSN-IP-Address  | 41.205.207.0
         RP     | IN  |   9 | $GGSN-IP-Address  | 1.1.1.1
        ------------------------------------------------------------------------------

Login Request enviado para o PCRF:

2008-07-29 17:23:16.354 TRACE        INF 1 | [] | SEND: <=== RP_OPER[2] CallId[7], OpCode =
[701]
        ------------------------------------------------------------------------------
                 OperationName[PCRF:LoginReq]
        ------------------------------------------------------------------------------
         RP     | OUT |   0 |                   | 701
         RP     | OUT |   1 | $Acct-Session-Id  | 00000AD9
         RP     | OUT |   2 |   SusbscriberId   | 069069096
         RP     | OUT |   3 |         IP        | 192.168.78.147
         RP     | OUT |   4 |                   | 0
         RP     | OUT |   5 |                   | 0
         RP     | OUT |   6 |      PCEF         | SM
         RP     | OUT |   7 |  PolicyProfile    | 1
         RP     | OUT |   8 |                   | 0
         RP     | OUT |   9 | SM Interrogation  | 1
         RP     | OUT |  10 |                   | 3600
         RP     | OUT |  11 |                   | 0
         RP     | OUT |  12 |                   | 0
        ------------------------------------------------------------------------------
2008-07-29 17:23:16.354 TRACE        INF 1 | [] | CORE_RP: <== AppId[11], Vers.[1],
ReqId[0], ProvId[7], IvkId[0], Op[701]
```

Figura 4. 8 Processamento da operação Login no DSCF.

Na Figura 4.8 está identificada a informação que será enviada para o PCRF, sendo as informações mais importantes as seguintes:

- *SusbscriberId*: Identificador que o utilizador terá no SCE, sendo no contexto deste trabalho igual ao MSISDN.
- *IP*: Parâmetro que contém o IP do utilizador.

- *PolicyProfile*: Informação com a identificação da política a aplicar, neste caso será aplicado a política com identificador 1.

- *SM Interrogation*: Parâmetro que define se a comunicação com o SCE será feita via SM ou directamente via SCE, neste caso o valor é 1 significará que o SM será utilizado.

Login processado no PCRF

O PCRF após receber a informação de *Login* através do interface RTDAP analisa a informação recebida, verificando que terá de enviar a informação através da interface com o SM. Finalizado o envio da mensagem de *Login* ao SM, o PCRF enviará o sucesso da operação para o DSCF para análise posterior. O fluxo da operação através do PCRF pode ser visto na Figura 4.9. A informação mais importante no processamento do *Login* no PCRF é a seguinte:

- *SusbscriberId*: Identificador que utilizador terá no SCE, sendo no contexto deste trabalho igual ao MSISDN.

- NetworkId: Parâmetro que no ponto de vista do SCE contém o IP do utilizador.

- *SM Interrogation*: Parâmetro que define se a comunicação com o SCE vai ser feita via SM.

- *PolicyProfile*: Informação com a identificação da política a aplicar.

- *Domain*: É o domínio em que o SCE está associado no SM, neste caso a identificação de domínio é DRP1.

- *PCEFId*: parâmetro informativo contendo a informação técnica do SM, sendo esta: o IP da máquina (10.112.64.242) onde o SM está a correr; a porta (14374) que está a escuta de pedidos; e o domínio (DRP1) a que o SM está associado.

```
Processamento do login no PCRF:

008-07-29 17:23:16,367 TRACE         INFO  1 | [069069096] RECV: ===> LOGIN RQ CallId = [7]
OpCode = [701]
                ---------------------------------------------------------------------
                         Operation - LOGIN RQ
                ---------------------------------------------------------------------
                 RP      | IN    | OpCode           | 701
                 RP      | IN    | SessionId        | 00000AD9
                 RP      | IN    | SubscriberId     | 069069096
                 RP      | IN    | NetworkId        | 192.168.78.147
                 RP      | IN    | NetworkIdType    | 0
                 RP      | IN    | NetworkIdAdditi  | 0
                 RP      | IN    | PCEFid           | SM
                 RP      | IN    | PolicyProfile    | 1
                 RP      | IN    | SMInterrogation  | 1
                 RP      | IN    | AutoLogoutTime   | 3600
                 RP      | IN    | QuotaOperationI  | 0
                ---------------------------------------------------------------------

                ---------------------------------------------------------------------
                         Operation - LOGIN
                ---------------------------------------------------------------------
                 SM      | OUT   | OpCode           | 701
                 SM      | OUT   | SessionId        | 00000AD9
                 SM      | OUT   | SubscriberId     | 069069096
                 SM      | OUT   | NetworkId        | 192.168.78.147
                 SM      | OUT   | NetworkIdType    | 0
                 SM      | OUT   | NetworkIdAdditi  | 0
                 SM      | OUT   | Domain           | DRP1
                 SM      | OUT   | AutoLogoutTime   | 3600
                ---------------------------------------------------------------------


                ---------------------------------------------------------------------
                         Operation - LOGIN SUCESS
                ---------------------------------------------------------------------
                 SM      | IN    | SessionId        | 00000AD9
                 SM      | IN    | SubscriberId     | 069069096
                 SM      | IN    | NetworkId        | 192.168.78.147
                 SM      | IN    | NetworkIdType    | 0
                 SM      | IN    | NetworkIdAdditi  | 0
                 SM      | IN    | PCEFid           | 10.112.64.242:14374@DRP1
                 SM      | IN    | AutoLogoutTime   | 3600
                ---------------------------------------------------------------------


                ---------------------------------------------------------------------
                         Operation - LOGIN Res
                ---------------------------------------------------------------------
                 RP      | OUT   | SessionId        | 00000AD9
                 RP      | OUT   | Result           | 0
                 RP      | OUT   | SubscriberId     | 069069096
                 RP      | OUT   | NetwordId        | 192.168.78.147
                 RP      | OUT   | NetwordIdType    | 0
                 RP      | OUT   | PCEFid           | 10.112.64.242:14374@DRP1
                ---------------------------------------------------------------------
2008-07-29 17:23:16,374 TRACE         INFO  1 | [069069096] [RTDAP] Login Res Sent to DSCF
```

Figura 4. 9 Processamento do Login no PCRF.

- Result: Indica o resultado da operação, neste caso como a operação foi bem sucedida o valor é 0

Informação do Login no SM

Para a confirmação de que a informação foi correctamente introduzida pelo PCRF é necessário executar um comando disponibilizado pela CISCO na máquina onde o SM está a correr. Essa informação pode ser visualizada na Figura 4.10.

```
Visualização no SM do Policy Profile / ip Adress / Subscriber ID

 p3subs --show --subscriber=069069096
Name:           069069096
Domain:         DRP1
Mappings:
        IP: 192.168.78.147/32
Properties:
        packageId=1
```

Figura 4. 10 Informação do utilizador visualizada no SM.

Da análise da Figura 4.10 podemos ver toda a informação necessária para aplicação da política. O conteúdo do campo *Name* faz correspondência ao *subscriberId*, neste contexto é o MSISDN, o conteúdo do campo *Mappings* faz correspondência ao *NetworkId* (IP) e por fim o campo *packageId* contido na secção *Properties* faz referência ao identificador da política.

4.2.2 Alteração de uma política durante uma sessão

Como foi referido anteriormente o cenário de actualização da política é visto como um dos cenários mais interessantes que a solução possibilita. A secção seguinte descreve os passos mais importantes da operação de actualização da política. A entidade que despoleta esta operação é a *Service Logic* (SL) do operador, mas como foi referido anteriormente, os detalhes da interacção com esta entidade não serão descritos sendo só apresentada a mensagem à saída do componente DSCF.

Actualização da política recebida pelo DSCF e processado no PCRF

Na operação de actualização o DSCF envia para o PCRF toda a informação como se de uma mensagem de autenticação (*Login*) se tratasse. A principal diferença do teste de *Login* é o facto de a política ser diferente. Neste caso o identificador da política tem o valor 2, enquanto todos os outros parâmetros são iguais e podem ser vistos na Figura 4.11.

```
Pedido de Update enviado do DSCF para o PCRF:

2008-07-31 13:20:58.572 TRACE        INF 1 | [] | SEND: <=== RP_OPER[12] CallId[10], OpCode
= [703]
        ------------------------------------------------------------------------------
                 OperatioName[PCRF:UpdateReq]
        ------------------------------------------------------------------------------
         RP     | OUT |   0 |                  | 703
         RP     | OUT |   1 | $Acct-Session-Id | 2003a090
         RP     | OUT |   2 |   SubscriberId   | 069069096
         RP     | OUT |   3 |       IP         | 192.168.78.147
         RP     | OUT |   4 |                  | 0
         RP     | OUT |   5 |                  | 0
         RP     | OUT |   6 |                  | SM
         RP     | OUT |   7 |   PolicyProfile  | 2
         RP     | OUT |   8 |                  | 0
         RP     | OUT |   9 |  SMInterrogation | 1
         RP     | OUT |  10 |                  | 3600
        ------------------------------------------------------------------------------

Update processado no PCRF:

2008-07-31 13:20:58,578 TRACE         INFO  1 | [069069096] RECV: ===> UPDATE RQ CallId =
[10]  OpCode = [703]
                 ------------------------------------------------------------------
                          Operation - UPDATE RQ
                 ------------------------------------------------------------------
                  RP     | IN    | OpCode           | 703
                  RP     | IN    | SessionId        | 2003a090
                  RP     | IN    | SubscriberId     | 069069096
                  RP     | IN    | NetworkId        | 192.168.78.147
                  RP     | IN    | NetworkIdType    | 0
                  RP     | IN    | NetworkIdAdditi  | 0
                  RP     | IN    | PCEFid           | SM
                  RP     | IN    | PolicyProfile    | 2
                  RP     | IN    | SMInterrogation  | 1
                  RP     | IN    | AutoLogoutTime   | 3600
                 ------------------------------------------------------------------

                 ------------------------------------------------------------------
                          Operation - UPDATE
                 ------------------------------------------------------------------
                  SM     | OUT   | SessionId        | 2003a090
                  SM     | OUT   | SubscriberId     | 069069096
                  SM     | OUT   | NetworkId        | 192.168.78.147
                  SM     | OUT   | NetworkIdType    | 0
                  SM     | OUT   | NetworkIdAdditi  | 0
                  SM     | OUT   | Domain           | DRP1
                  SM     | OUT   | AutoLogoutTime   | 3600
                 ------------------------------------------------------------------
2008-07-31 13:20:58,583 TRACE         INFO  1 | [069069096] [SM] Login Req Sent to SM
```

```
2008-07-31 13:20:58,583 TRACE         INFO  1 | [069069096] [SM] Login Req Sent to SM

                ---------------------------------------------------------------
                         Operation - UPDATE SUCESS
                ---------------------------------------------------------------
                 SM     | IN    | SessionId        | 2003a090
                 SM     | IN    | SubscriberId     | 069069096
                 SM     | IN    | NetworkId        | 192.168.78.147
                 SM     | IN    | NetworkIdType    | 0
                 SM     | IN    | NetworkIdAdditi  | 0
                 SM     | IN    | PCEFid           | 10.112.64.242:14374@DRP1
                 SM     | IN    | AutoLogoutTime   | 3600
                ---------------------------------------------------------------

Resultado do Update enviada para o DSCF:

                ---------------------------------------------------------------
                         Operation - UPDATE Res
                ---------------------------------------------------------------
                 RP     | OUT   | OpCode           | 704
                 RP     | OUT   | SessionId        | 2003a090
                 RP     | OUT   | Result           | 0
                 RP     | OUT   | SubscriberId     | 069069096
                ---------------------------------------------------------------
2008-07-31 13:20:58,593 TRACE         INFO  1 | [069069096] [RTDAP] Update Res Sent to DSCF
```

Figura 4. 11 Actualização da política enviada do DSCF e processado no PCRF.

Informação da actualização da Política no SM

A confirmação da actualização da política no SM pode ser feita da mesma maneira apresentada no teste de *Login*, isto é, através da execução do mesmo comando. A informação resultante da aplicação da actualização da política pode ser vista na seguinte na Figura 4.12.

```
Visualização no SM do Policy Profile / IP Adress / Subscriber ID

 p3subs --show --subscriber=069069096
Name:           069069096
Domain:         DRP1
Mappings:
        IP: 192.168.78.147/32
Properties:
        packageId=2
```

Figura 4. 12 Informação do utilizador após a actualização da política visualizada no SM.

Destaca-se na Figura 4.12 o valor do campo *packageId,* tendo neste caso o valor 2.

4.2.3 Finalização de uma sessão

O último teste de utilização a ser descrito é o de finalização de uma sessão, sendo representado pela operação *Logout*. A interacção dos componentes é parecida com a do cenário de *Login,* alterando claro o valor de alguns parâmetros, bem como a exclusão de outros que não são necessários.

Logout recebido no RHng

À semelhança do cenário de *Login,* o RHng recebe um pedido RADIUS proveniente do GGSN enviando-o de seguida para o DSCF, sendo a principal diferença neste caso o valor do parâmetro *Acct.Status-Type*, tendo neste caso o valor de *Stop.* A informação recebida no RHng pode ser vista na Figura 4.13.

```
Parametros Radius:
Logs no RH:

2008-07-29 15:30:13.593 RAD_LOG      INF 1 | rad_recv: ==> Accounting-Request packet from
host 192.168.78.38:4989, id=104, length=296
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: Acct-Status-Type = Stop
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: Acct-Session-Id = "00000ACD"
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: NAS-IP-Address = 192.168.78.97
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: Framed-IP-Address = 192.168.78.147
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: Calling-Station-Id = "069069096"
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: Configuration-Token = "MED***"
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: Called-Station-Id = "pcrf.med***.**"
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: 3GPP-GPRS-Negotiated-QoS-profile = "98-
FFFFFF"
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: 3GPP-PDP-Type = 1
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: 3GPP-IMSI = "069069096"
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: 3GPP-Charging-ID = 147
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: 3GPP-Attr-18 = 0x3131313131
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: 3GPP-SGSN-Address = 41.205.207.0
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: 3GPP-GGSN-MCC-MNC = "22222"
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: 3GPP-GGSN-Address = 1.1.1.1
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: 3GPP-IMSI-MCC-MNC = "33333"
2008-07-29 15:30:13.595 RAD_LOG      INF 2 | VALUE: 3GPP-NSAPI = "0000"
2008-07-29 15:30:13.596 RAD_LOG      INF 2 | VALUE: User-Name = "MT-ME***-147-069069096-
PCRF-GPRS"
2008-07-29 15:30:13.596 RAD_LOG      INF 2 | VALUE: User-Password = "\rI\271\304"

Mapeamento do acct-stop em Logout Request no DSCF:

        ------------------------------------------------------------------------
                 OperatioName[RH:LogoutReq]
        ------------------------------------------------------------------------
         RP     | IN  |   0 | $OperationCode     | 313
         RP     | IN  |   1 | $Framed-IP-Addres  | 192.168.78.147
         RP     | IN  |   2 | $NAS-IP-Address    | 192.168.78.97
         RP     | IN  |   3 | $Acct-Session-Id   | 00000AD3
         RP     | IN  |   4 | $Calling-Station-  | 069069096
         RP     | IN  |   5 | $IMSI              | 069069096
         RP     | IN  |   6 | $Called-Station-I  | pcrf.med***.**
```

Figura 4. 13 Logs da finalização da sessão, no RHng.

Logout processado no DSCF

O DSCF após receber o pedido de *Logout* do RHng informa a SL desse facto e de seguida envia o pedido para o PCRF. As informações do processamento da operação no DSCF podem ser visualizadas na Figura 4.14.

```
Logout Request vindo do RH processado no DSCF:

2008-07-29 17:06:12.874 TRACE        INF 1 | [] | RECV: ===> RP_OPER[20] CallId[2], OpCode =
[313]
        ------------------------------------------------------------------------------
                 OperatioName[RH:LogoutReq]
        ------------------------------------------------------------------------------
         RP     | IN  |    0 | $OperationCode     | 313
         RP     | IN  |    1 | $Framed-IP-Addres  | 192.168.78.147
         RP     | IN  |    2 | $NAS-IP-Address    | 192.168.78.97
         RP     | IN  |    3 | $Acct-Session-Id   | 00000AD3
         RP     | IN  |    4 | $Calling-Station-  | 069069096
         RP     | IN  |    5 | $IMSI              | 069069096
         RP     | IN  |    6 | $Called-Station-I  | pcrf.med***.**
         RP     | IN  |    7 | $SGSN-IP-Address   | 41.205.207.0
         RP     | IN  |    8 | $GGSN-IP-Address   | 1.1.1.1
        ------------------------------------------------------------------------------
        ------------------------------------------------------------------------------

logout enviado para o PCRF:

2008-07-29 17:06:12.908 TRACE        INF 1 | [] | SEND: <=== RP_OPER[22] CallId[2], OpCode =
[705]
        ------------------------------------------------------------------------------
                 OperatioName[PCRF:LogoutReq]
        ------------------------------------------------------------------------------
         RP     | OUT |    0 |                    | 705
         RP     | OUT |    1 | $Acct-Session-Id   | 00000AD3
         RP     | OUT |    2 |   SubscriberId     | 069069096
         RP     | OUT |    3 | $Framed-IP-Addres  | 192.168.78.147
         RP     | OUT |    4 |                    | 0
         RP     | OUT |    5 |                    | SM
         RP     | OUT |    6 | SM Interrogation   | 1
        ------------------------------------------------------------------------------
```

Figura 4. 14 Processamento da operação Logout no DSCF.

Logout processado no PCRF

O processamento do *Logout* no PCRF é realizado de uma forma análoga à da operação *Login*, exceptuando o envio da identificação da política. Uma vez que esta operação é para indicar ao SCE que um determinado utilizador não será controlado, o envio da política é desnecessário. As informações do processamento da operação no componente PCRF podem ser visualizadas na Figura 4.15.

```
Logout processado no PCRF:

008-07-29 17:06:12,917 TRACE         INFO  1 | [069069096] RECV: ===> LOGOUT RQ CallId = [2]
OpCode = [705]
                  ------------------------------------------------------------------
                           Operation - LOGOUT RQ
                  ------------------------------------------------------------------
                   RP      | IN    | OpCode           | 705
                   RP      | IN    | SessionId        | 00000AD3
                   RP      | IN    | SubscriberId     | 069069096
                   RP      | IN    | NetworkId        | 192.168.78.147
                   RP      | IN    | NetworkIdType    | 0
                   RP      | IN    | PCEFid           | SM
                   RP      | IN    | SMInterrogation  | 1
                  ------------------------------------------------------------------

                  ------------------------------------------------------------------
                           Operation - LOGOUT BY NAME FROM DOMAIN
                  ------------------------------------------------------------------
                   SM      | OUT   | OpCode           | 705
                   SM      | OUT   | SessionId        | 00000AD3
                   SM      | OUT   | SubscriberId     | 069069096
                   SM      | OUT   | NetworkId        | 192.168.78.147
                   SM      | OUT   | NetworkIdType    | 0
                   SM      | OUT   | Domain           | DRP1
                  ------------------------------------------------------------------

                  ------------------------------------------------------------------
                           Operation - LOGOUT SUCESS
                  ------------------------------------------------------------------
                   SM      | IN    | OpCode           | 706
                   SM      | IN    | SessionId        | 00000AD3
                   SM      | IN    | SubscriberId     | 069069096
                   SM      | IN    | NetworkId        | 192.168.78.147
                   SM      | IN    | PCEFid           | 10.112.64.242:14374@
                  ------------------------------------------------------------------

                  ------------------------------------------------------------------
                           Operation - LOGOUT Res
                  ------------------------------------------------------------------
                   RP      | OUT   | OpCode           | 706
                   RP      | OUT   | SessionId        | 00000AD3
                   RP      | OUT   | Result           | 0
                   RP      | OUT   | SubscriberId     | 069069096
                  ------------------------------------------------------------------
2008-07-29 17:06:12,923 TRACE         INFO  1 | [069069096] [RTDAP] Logout Res Sent to DSCF
```

Figura 4. 15 Processamento do Logout no PCRF.

Informação do Logout no SM

A confirmação que o tráfego de um utilizador não será mais controlado pela solução, pode ser vista na informação que o SM guarda acerca do utilizador. A informação pode ser vista na Figura 4.16.

```
Visualização no SM com o utilizador offline

p3subs --show --subscriber=069069096

Name:           069069096
Domain:         DRP1
Properties:
        packageId=2
```

Figura 4. 16 Informação do utilizador visualizada no SM após o Logout.

Analisando a Figura 4.16 constatamos que não existe *NetworkId* (IP) associado ao utilizador, o que permite concluir que não existe a relação IP/utilizador no(s) SCE(s).

4.2.4 Verificação da Afectação do Tráfego

Finalizada a descrição dos testes envolvendo vários cenários de utilização que ilustram com dados reais a forma como os diversos componentes comunicam, serão agora apresentados alguns resultados práticos do que o controlo de tráfego baseado em políticas pode originar.

Serão descritos três casos práticos onde se poderá verificar o controlo do tráfego. Os casos práticos são os seguintes: *i*) verificação que a largura de banda do acesso Internet de um utilizador é alterada mediante a política associada a este; *ii*) verificação que a solução pode limitar a largura de banda de um protocolo específico; *iii*) demonstração como a solução pode controlar a largura de banda de vários acessos e serviços.

Nos testes, a demonstração que a solução desenvolvida permite fazer o respectivo controlo de tráfego, será feita com base na noção de *traffic shaping* [68]. Baseado nesta noção, o SCE limita o valor da largura de banda do tráfego de acordo com o que está definido nas políticas, levando a que este não ultrapasse um valor definido. O gráfico que ilustra o conceito de *traffic shaping* pode ser visto na Figura 4.17. O mecanismo de *traffic shaping* possibilita o armazenamento temporário de algum tráfego em excesso, sendo este posteriormente transmitido de forma a serem obedecidos os limites de largura de banda impostos.

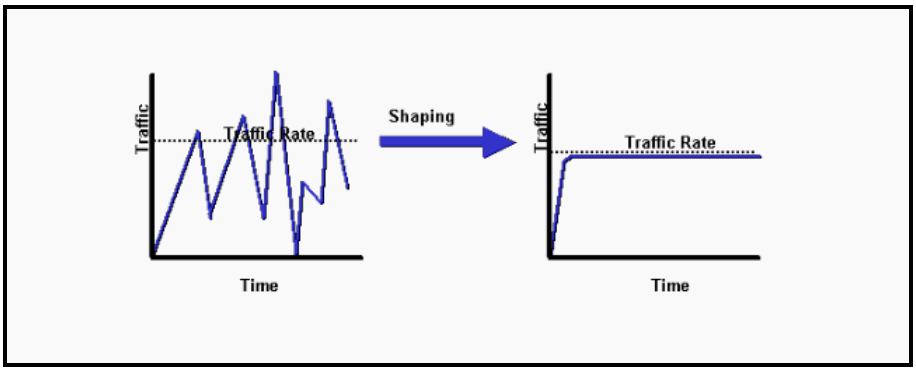

Figura 4. 17 Conceito de *Traffic Shaping* [67].

4.2.4.1 Controlo de largura de banda de um utilizador

Este caso prático consistirá na verificação da afectação da largura de banda do acesso à Internet por parte de um utilizador, em que este será afectado por duas políticas diferentes. As políticas estão associadas a valores de largura de banda diferentes, sendo a largura de banda expressa em Kbps (Kilobit por segundo). A verificação do que a política está a ser aplicada correctamente, será confirmada com base num medidor de largura de banda, neste trabalho será usado o *speedmeter* [web5] da FCCN[10]. Os pormenores do primeiro caso prático serão apresentados de seguida:

Diagrama físico do teste:

Na realização deste caso prático, o SCE será introduzido entre o ponto de acesso ao núcleo do operador em causa e o ponto de saída para a Internet, permitindo assim fazer o controlo desejado. A Figura 4.18 dá uma visão alto nível da disposição dos elementos envolvidos no teste.

10 Faculdade para a Computação Cientifica Nacional

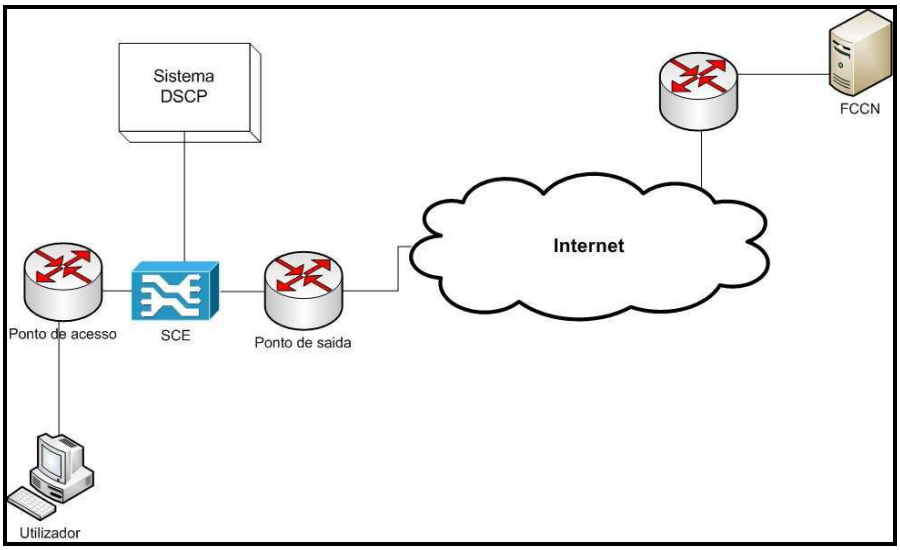

Figura 4. 18 Diagrama alto nível do primeiro caso prático.

Especificações das políticas a aplicar:

A identificação das políticas a aplicar para o utilizador será feita com base num valor que servirá de identificador, como foi comprovado e explicado nas secções anteriores. O exemplo do controlo do tráfego que será apresentado terá como base duas políticas, tendo estas valores máximos de largura de banda diferente. Assim sendo a definição das políticas é a seguinte:

- Política com ID 1: Esta política tem um valor máximo de largura de banda de 2500 Kbps (2.5 Mbps) para qualquer tipo de serviço.
- Política com ID 2: Esta política tem um valor máximo de largura de banda de 1500 Kbps (1.5 Mbps) para qualquer tipo de serviço.

Um cenário possível para a utilização destas duas políticas, no contexto do operador de telecomunicações, poderá ser a diferenciação dos tipos de cliente, a atribuição de diferentes limites consoante o horário de acesso, entre outras formas de negócio.

Visualização da afectação na largura de banda:

Como foi referido, a verificação que a respectiva política está a ser aplicada a largura de banda de acesso de um cliente, pode ser visto recorrendo a ferramenta *speedmeter* da FCCN. O *speedmeter* realiza os testes ao nível da aplicação, existindo portanto *overheads* introduzidos pelas diversas camadas

da pilha TCP/IP. Sendo assim os resultados dos testes do *speedmeter* representam o débito útil da ligação IP entre a máquina do utilizador e servidor WEB presente na FCCN e não o débito físico da ligação. Para mais pormenores da ferramenta consultar [web5]. Outra condicionante que pode ter influência nos testes realizados está associada ao facto do canal de comunicação entre operador e a internet estar muitas vezes congestionado. Assim sendo, baseado na largura de banda definida para cada política, podemos observar o resultado da aplicação destas.

A Figura 4.19 mostra a afectação da largura de banda condicionada pela política 1. O dado mais importante a reter da Figura 4.19 é o valor do campo "**Largura de banda útil**", neste caso com o valor de 1.81 Mbps, ou seja inferior a 2.5 Mbps da largura de banda física definida pela política. Como foi explicado anteriormente, a diferença obtida entre a largura de banda útil e o valor especificado pela política advém dos overheads e funcionalidades inerentes às camadas protocolares, assim como, de possíveis condicionantes a que estão sujeitos os canais de comunicação externos ao operador em questão.

Figura 4. 19 Largura de banda afectada pela política 1.

A Figura 4.20 mostra a afectação da largura de banda condicionada pela política 2.

Figura 4. 20 Largura de banda afectada pela política 2.

Da mesma forma como o explicado para a Figura 4.19, o campo mais importante a reter da Figura 4.20 é o de "**Largura de banda útil"**. Neste caso, como a política aplicada foi a identificada com o ID 2, o valor foi inferior a 1.5 Mbps ficando perto do valor 1 Mbps.

4.2.4.2 Controlo específico de um Protocolo

O segundo caso prático consiste em demonstrar que a solução permite fazer o controlo específico de um protocolo. No teste em causa o protocolo será o (*File Transfer Protocol*) FTP.

Diagrama físico do teste:

O cenário físico deste teste é bastante simples, uma vez que só temos um utilizador aceder a um servidor FTP, e em que no meio do canal de comunicação se encontra o SCE. A Figura 4.21 ilustra o cenário deste teste.

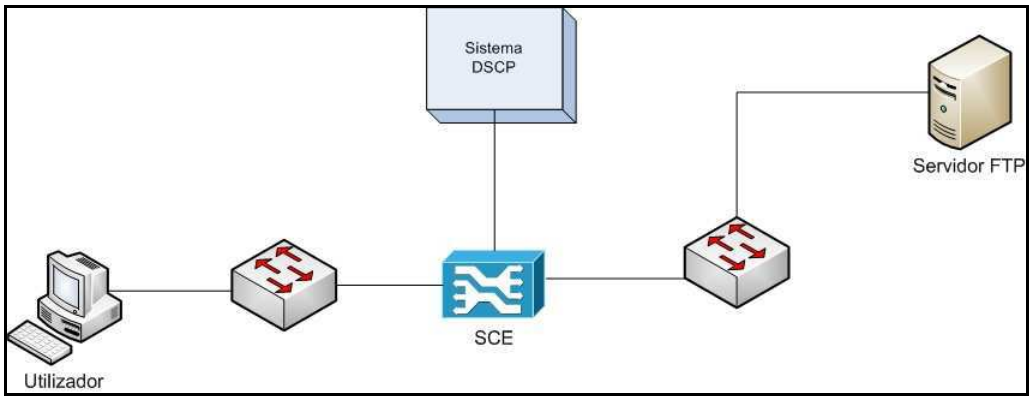

Figura 4. 21 Diagrama alto nível do segundo caso prático.

Especificações das políticas a aplicar:

A definição das políticas a aplicar neste caso também será simples, somente será aplicado no SCE uma política que limita o tráfego FTP a 10 Kbps.

Visualização da afectação na largura de banda:

A afectação que a política definida causou no tráfego FTP, pode ser visualizada na Figura 4.22. Na figura 4.22 podemos ver a largura de banda máxima que o serviço FTP atingiu antes e depois de ser aplicada a política. Podemos observar também na Figura 4.22 o instante em que a política foi aplicada, causando uma diminuição acentuada na largura de banda do serviço.

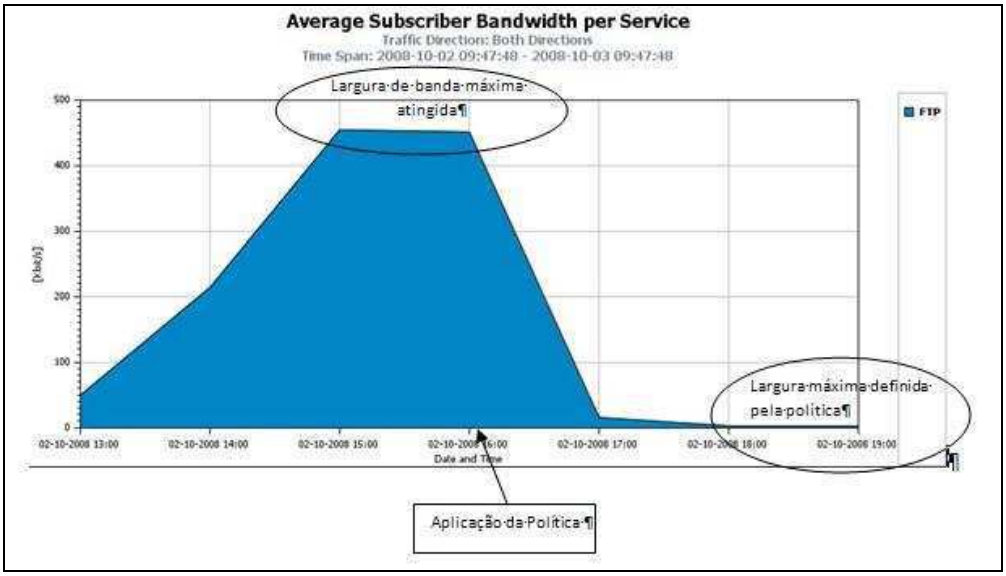

Figura 4. 22 Ilustração da afectação do protocolo FTP pelo SCE.

Na Figura 4.22 o tempo que decorre até se verificar o limite imposto pela política está relacionado com o facto da aplicação de monitoria usada no teste, estar configurada para efectuar cálculos ponderados baseado em valores médios com intervalos de 1 hora.

4.2.4.3 Controlo Diferenciado por Serviço e Acesso

O terceiro caso prático como foi referido anteriormente será baseado na verificação da afectação do tráfego de vários acessos e serviços. Neste caso em concreto, será feito o controlo de vários acessos que um operador disponibiliza, assim como a diferenciação de alguns serviços, sendo distinguidos os vários utilizadores através da atribuição de políticas específicas, bem como, serão definidas percentagens máximas de largura de banda para certos serviços/protocolos. Os pormenores do terceiro caso prático serão apresentados de seguida.

Diagrama físico do teste:

O diagrama físico deste caso prático tem várias semelhanças com o primeiro, sendo adicionada mais complexidade ao nível dos acessos dos utilizadores e nos serviços controlados pela solução. Existirão seis acessos ao núcleo do operador, cada um com velocidades de acesso diferentes mas ambos partilharão a largura de banda que o operador usufrui para aceder à Internet (12 Mbps). A ilustração do diagrama alto nível do terceiro caso prático pode ser encontrada na Figura 4.23.

Especificações das políticas a aplicar:

As descrições das políticas, neste caso prático serão divididas em duas partes: *i)* a atribuição de diferentes valores de largura de banda máxima a diferentes acessos e diferentes prioridades que o seu tráfego terá; *ii)* a atribuição de diferentes valores de largura de banda aos serviços que serão controlados. A definição dos diferentes valores da largura de banda dos acessos, das gamas dos IP atribuídos aos diversos grupos e dos serviços definidos é da responsabilidade do operador em que o teste foi realizado,

ficando a análise destes fora do âmbito deste documento. Os valores definidos para as diferentes larguras de banda podem ser consultados na Tabela 4.1.

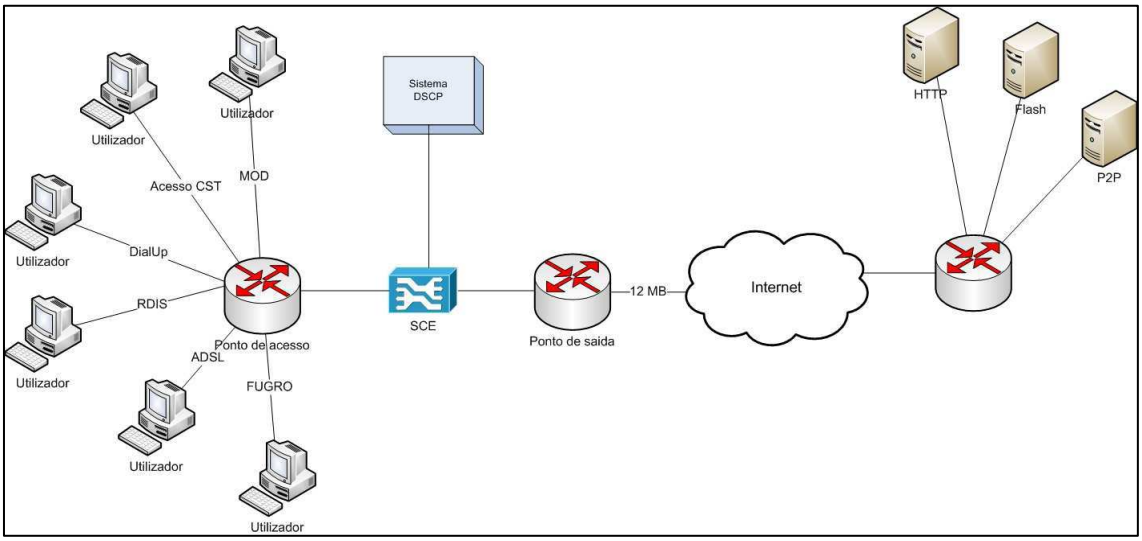

Figura 4. 23 Diagrama alto nível do terceiro caso prático.

Tipo de Acesso	Nome da Política	Prioridade	Largura de Banda máxima	Serviços	
RDIS	RDIS	1.º	33%	P2P	10%
				Flash	10%
				HTTP	50%
DialUp	DialUp	4.º	16%	P2P	10%
				Flash	10%
				HTTP	50%
ADSL	ADSL12	3.º	33%	P2P	10%
				Flash	10%
				HTTP	50%
	ADSL25	2.º	16%	Flash	10%
				P2P	10%
				HTTP	50%

Tipo de Acesso	Nome da Política	Prioridade	Largura de Banda máxima	Serviços
Acesso CST	CST	2.º	10%	Não aplicável
FUGRO	FUGRO	3.º	2%	Não aplicável
MOD	MOD	4.º	1%	Não aplicável

Tabela 4. 1 Tabela das definições da largura de banda por política.

Da análise da Tabela 4.1 podemos concluir que cada acesso vai ter uma largura de banda máxima diferente, isto é, cada acesso não pode ultrapassar a percentagem atribuída, no entanto, também existirá a noção de prioridade, ou seja, o acesso que terá a política com prioridade maior terá se possível a sua largura de banda máxima assegurada. Por exemplo, a política com prioridade 1 terá mas prioridade do que a política com prioridade 2. Esta noção de prioridades leva a ser possível definir mais políticas, nas quais, a soma das suas percentagens de largura de banda seja superior a 100%, uma vez que o SCE baseado nas prioridades faz alocação dinâmica da largura de banda total.

Nos acessos ADSL, RDIS e DialUp serão controlados três serviços de igual forma. Os serviços controlados serão: *i*) HTTP; *ii*) P2P e *iii*) Flash, para estes serão definidas percentagens de largura máxima referente à largura atribuída para os acessos em causa.

Uma possível identificação de grupos de utilizadores que utilizam um determinado acesso poderá ser o representado na Tabela 4.2. Na tabela 4.2 por exemplo, podemos analisar que vários grupos serão identificados por políticas descendentes da política do acesso RDIS, levando a que todos eles herdem as propriedades da política identifica na Tabela 4.1 como RDIS.

Política	Política descendente
BANCOCENTRAL	RDIS
ISLANDBANK	RDIS
CSTDIVMARKETTING	RDIS

Política	Política descendente
MIGRACAOFRONTEIRA	RDIS
(…)	(…)

Tabela 4. 2 Tabela que identifica grupos de utilizadores por política.

Visualização da afectação na largura de banda:

Para uma mais fácil percepção inicial da afectação do tráfego que a solução pode originar, serão apresentados gráficos de largura de banda antes e depois da aplicação das políticas. O gráfico que ilustra a ocupação da largura de banda antes da aplicação das políticas pode ser vistos na Figura 4.24. A afectação do tráfego do operador depois de se aplicar as políticas definidas nas tabelas 4.1 e 4.2 no SCE, pode ser visto no gráfico da Figura 4.25.

Para interpretar os resultados que se pretendem transmitir através das Figuras 4.24 e 4.25, o leitor não se deve centrar nas diferentes cores dos serviços presentes no canal, mas unicamente observar os valores totais da largura de banda utilizada durante o teste.

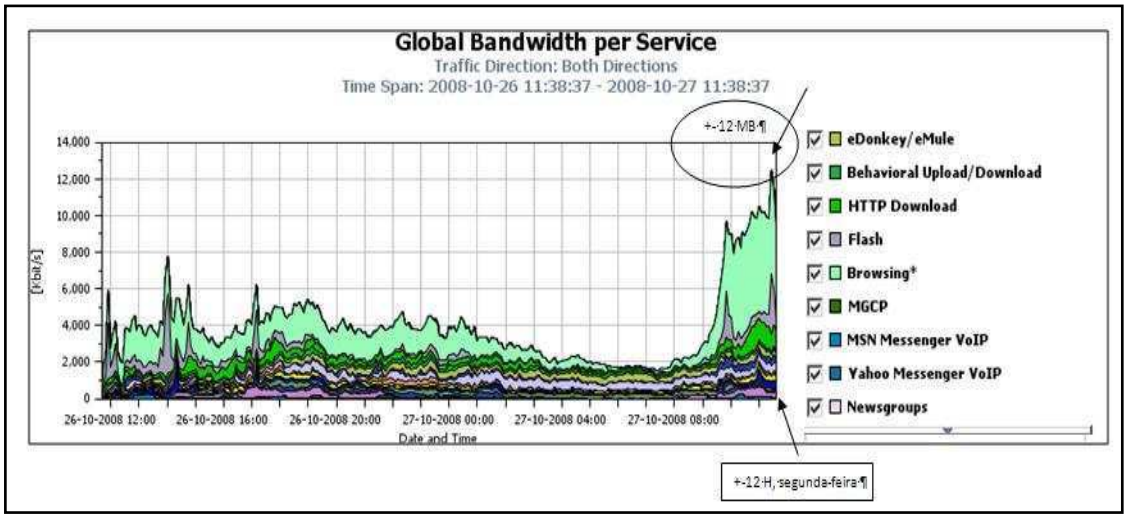

Figura 4. 24 Ilustração da largura de banda antes da aplicação das políticas.

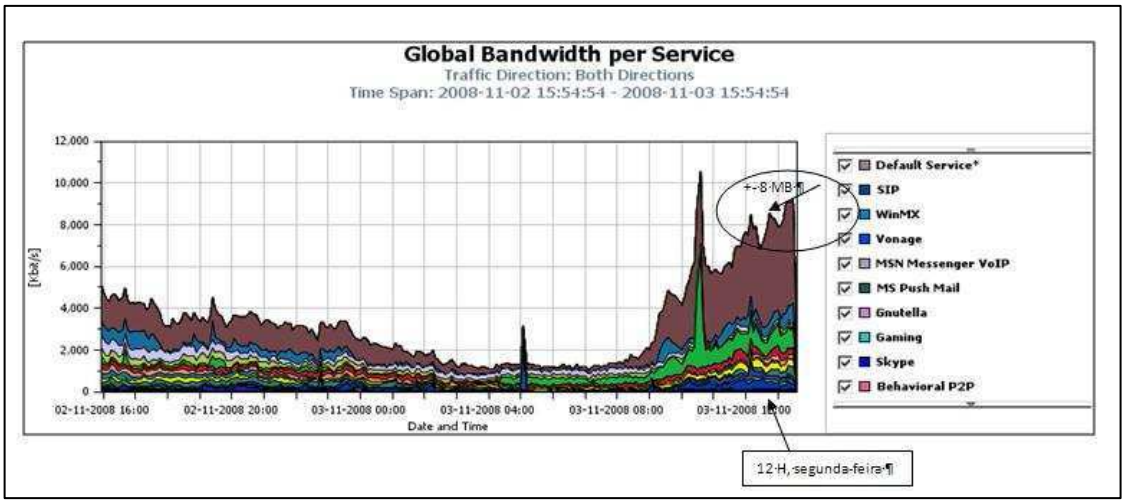

Figura 4. 25 Ilustração da largura de banda depois da aplicação das políticas.

Da análise das Figuras 4.24 e 4.25 podemos observar que para aproximadamente a mesma hora no mesmo dia da semana, a largura de banda do tráfego desceu ligeiramente, apresentando o tráfego agora valores de pico em torno dos 8 Mbps e 10 Mbps em contraste com os 12 Mbps do exemplo anterior. De igual forma, comparando as duas figuras anteriores observa-se uma ligeira diminuição da largura de banda utilizada ao longo dos períodos estudados, no caso da aplicação das políticas. Estes resultados poderão advir do facto de estar a haver alguma limitação agora imposta aos serviços e acessos definidos na Tabela 4.1. A eficácia do controlo do tráfego proporcionado pela solução nos grupos/acessos identificados pelas políticas da Tabela 4.1, e a evidência da realização de *traffic shaping* podem ser verificados nos próximos gráficos.

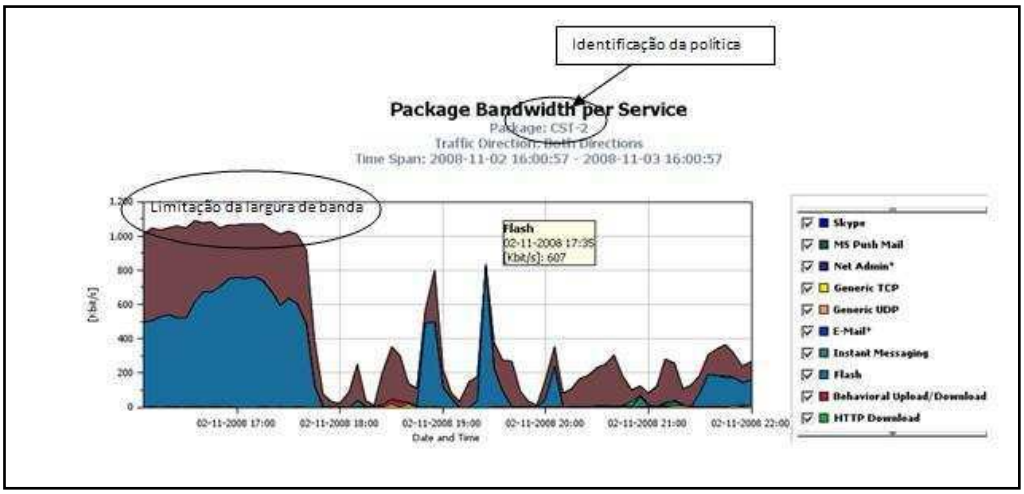

Figura 4. 26 Largura de banda dos serviços da política CST.

Na Figura 4.26 podemos observar os serviços que estão a ser monitorizados pelo acesso CST. Pela Tabela 4.1 podemos concluir que a política CST limita a largura de banda do acesso a aproximadamente 1,2 Mbps (0.10x12Mbps), esta limitação está evidenciada e identificada na Figura 4.26, em que se observa que a totalidade do tráfego do acesso nunca ultrapassa esse valor. De notar que, neste caso, o tráfego *Flash* (representado a azul) ocupa uma parcela significava do acesso, devido ao facto de não serem especificados limites por serviço (*Flash* incluído) para o acesso CST, como se pode analisar na Tabela 4.1. A evidência que a solução permite controlar um determinado serviço e fazer a respectiva herança das propriedades de uma política pode ser observado nas Figuras 4.27 e 4.28.

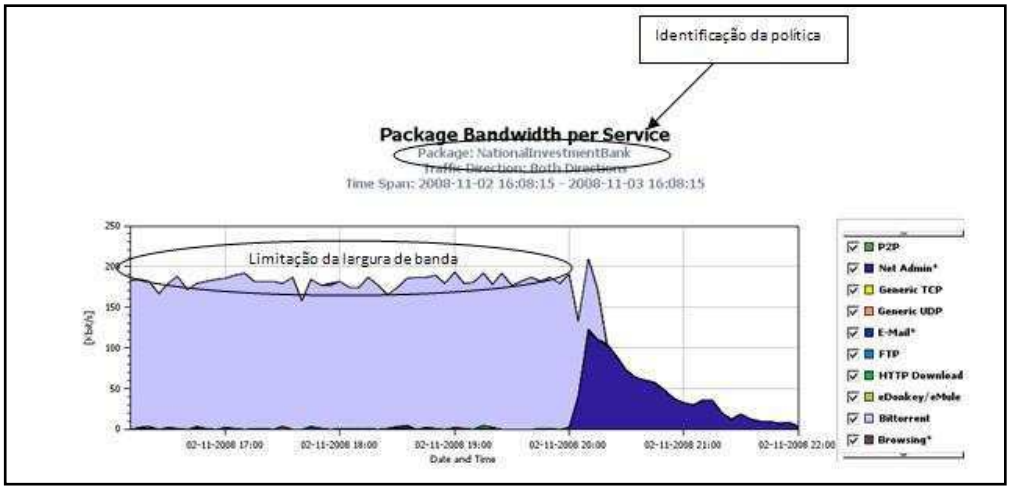

Figura 4. 27 Largura de banda dos serviços da política NationalInvestmentBank.

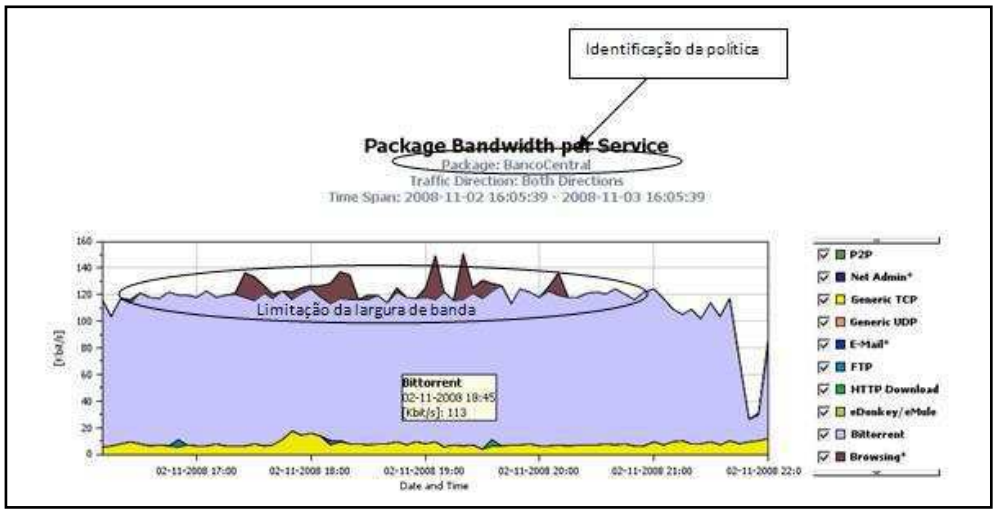

Figura 4. 28 Largura de banda dos serviços da política BancoCentral.

Analisando as Figura 4.27 e 4.28 podemos observar que o protocolo *Bittorrent* (protocolo incluído no serviço P2P) nas duas figuras não ultrapassa um certo valor, no caso da Figura 4.27 o valor é próximo dos 190 Kbps e no caso da Figura 4.28 é próximo dos 120 kbps. Recordando que as políticas *NationalInvestmentBank* e *BancoCentral* descendem da política RDIS e tendo esta um valor máximo para serviço P2P de 396 Kbps ((0.33*12 Mbps)*0.10), ambas partilham a largura de banda disponível para esse serviço, ocupando as duas (190+120=320 Kbps) quase o limite máximo para este serviço. Neste caso, a restante largura de banda do serviço deverá estar dividida por entre os outros grupos ou utilizadores, que estejam associados à política RDIS.

4.3 Notas finais

Neste capítulo foram apresentados os vários cenários em que a solução poderá funcionar, bem como a ilustração da comunicação entre os seus componentes obtida em contexto real. No final do capítulo foram apresentadas evidências do controlo do tráfego que a solução pode originar, tanto no controlo individual da largura de banda de um utilizador, como no controlo do tráfego de vários acessos e serviços oferecidos por um operador.

O primeiro e o terceiro teste foram realizados em ISP(s), mostrando assim que a solução desenvolvida tem uma grande aplicabilidade e usabilidade, permitindo materializar vários conceitos estudados no capítulo 2.

5 Conclusões

Ao longo de todo o documento foram sendo feitas pequenas observações e análises, quer na descrição dos capítulos quer na parte final dos mesmos. Este capítulo será agora exclusivamente dedicado ao relato das conclusões mais importantes do trabalho, bem como à discussão de perspectivas de trabalho futuro.

5.1 Controlo de Tráfego Baseado em Políticas

A temática do controlo de tráfego baseado em políticas foi várias vezes referida ao longo deste documento, sendo o capítulo 2 exclusivamente dedicado à descrição do tema. Uma das conclusões que se pode tirar deste tema é que o controlo de tráfego baseado em políticas terá surgido por necessidade de ter algum controlo nos recursos disponibilizados pelos operadores de comunicações, permitindo assim, oferecer padrões mínimos na qualidade do acesso oferecido aos utilizadores.

Baseadas na necessidade de controlar o tráfego, várias organizações definiram arquitecturas baseadas em normas, onde são especificados mecanismos de controlo de tráfego. O grupo 3GPP foi uma dessas organizações e na sua abordagem ao tema, concluiu que as funcionalidades de controlo de tráfego (*Policy Control*) e de tarifação (*Charging*) devem estar juntas na mesma arquitectura. Para isso especificou a arquitectura PCC (*Policy Control and Charging*), descrita sucintamente na secção 2.4.3.

A arquitectura PCC serviu de base para o desenvolvimento da solução de controlo de tráfego baseado em políticas, orientada para operadores de comunicações. Assim, os operadores poderão fazer um controlo do tráfego da rede, permitindo optimizar investimentos, garantir padrões de qualidade e oferecer novos serviços aos seus clientes.

5.2 Soluções Estudadas

Para a concepção da solução foi necessário estudar varias soluções que permitem o controlo do tráfego da rede. As descrições de algumas soluções estudadas podem ser encontradas na secção 2.5 do capítulo 2. Do estudo realizado pode-se concluir que existem várias soluções para a concretização desta temática, variando essencialmente na arquitectura da rede em que operador ou organização está inserida e no controlo oferecido.

Outra observação que se pode fazer do estudo das soluções, é a complexidade da solução variar conforme o nível do controlo que se pretende fazer. Normalmente as soluções mais simples permitem fazer um controlo reduzido do tráfego bem como controlar um número reduzido de utilizadores. No lado oposto, soluções mais robustas oferecem variadas formas de controlo, assim como um grande número de utilizadores suportados.

A solução escolhida neste trabalho apresenta grande versatilidade na interacção com o componente de rede responsável por controlar o tráfego dos utilizadores, bem como a disponibilização de métodos que permitem uma fácil integração com as infra-estruturas dos operadores.

5.3 Desenvolvimento da Solução

O desenvolvimento da solução consistiu essencialmente em construir um componente capaz de interagir com: *i)* o elemento de rede responsável por controlar o tráfego e *ii)* com os elementos da lógica de negócio dos operadores em que a solução foi integrada.

Os pormenores das diversas fases de desenvolvimento da solução podem ser encontrados no capítulo 3. Das diversas fases destaca-se o desenho da arquitectura da solução, tendo como base a arquitectura PCC, assim como a especificação da implementação dos seus diversos

componentes. Esta respectiva estruturação permitiu que o desenvolvimento fosse realizado de uma forma coerente e organizada, implementando os diversos requisitos dos operadores. As tecnologias usadas tanto no desenvolvimento do módulo PCRF (*Policy Control and Charging Rules Function*) como no equipamento responsável por controlar o tráfego, contribuíram para o sucesso deste trabalho, uma vez o que o equipamento disponibilizava ferramentas de fácil utilização, bem como métodos que permitem integração com outros sistemas.

5.4 Cenários de Testes

No capítulo 4 foram apresentados os vários cenários em que a solução pode funcionar, assim como evidências da afectação do tráfego provocadas pelo controlo efectuado pelo elemento de rede da solução.

Na descrição dos cenários procurou-se sempre resumir e simplificar a interacção dos componentes da solução. Desta forma, foi dada relevância ao controlo de tráfego baseado em políticas, deixando para segundo plano outros aspectos mais secundários da solução.

No que diz respeito à visualização da afectação do tráfego, foi apresentado um dos cenários que poderá ser o mais comum no uso destas soluções, ou seja, o controlo da largura de banda de um determinado utilizador. Neste teste foi observado como a solução pode dinamicamente alterar a política associada aos utilizadores e consequentemente a alteração da largura de banda. Outro caso prático interessante que foi estudado no capítulo 4 foi o controlo diferenciado de vários acessos que um operador dispõe para aceder à Internet, assim como o controlo de alguns serviços oferecido por este. Nestes casos práticos foi retratado como a solução é importante para garantir padrões de qualidade mínimos, em situações onde os recursos são limitados.

5.5 Trabalho Futuro

Existem inúmeras observações e ideias para trabalho futuro, de forma a tornar a solução mais modular a abrangente possível. Algumas das possibilidades de expansão da solução podem ser as seguintes:

- Funcionalidades de *Charging:* a norma 3GPP Release 7 especifica que as funcionalidades de *Policy Control* e *Charging* devem estar incluídas no mesmo componente, assim, um possível trabalho futuro é adicionar funcionalidades de *Charging* a solução.

- Suporte para mais equipamentos que desempenhem a funcionalidade PCEF (*Policy and Charging Enforcement Function*): outra possibilidade que seria interessante desenvolver é a solução suportar mais equipamentos que desempenhem a função de PCEF, para além do CISCO SCE.

- Suporte de novos interfaces de interacção com o PCRF: o PCRF desenvolvido só suporta a interface RTDAP para a manipulação das operações com o equipamento responsável pela função de PCEF. Uma funcionalidade adicional interessante seria implementar novos interfaces, de forma a que outros componentes de outras arquitecturas (e.g. IMS) e sistemas possam interagir com o PCRF.

Muitas das ideias que foram anteriormente descritas encontram-se agora em fase de estudo pela equipa de desenvolvimento da PT Inovação.

6 Referências

6.1 Referências Bibliográficas

[1] Preparing Europe’s digital future i2010 Mid-Term Review, Commision of the European Communities, April 2008.

[2] The Future of the Internet, A Compendium of European Projects on ICT Research Supported by the EU 7th Framework Programme for RTD, European Communities, 2008.

[3] Hal R. Varian, The Demand for Bandwidth, Evidence from the INDEX Project, In Crandall, R.W., and Alleman, J.H. (Eds.) Broadband: Should We Regulate High-Speed Internet Access?, Aei-Brookings Joint Center for Regulatory Studies, American Enterprise Institute, pp. 39 -56, 2003.

[4] Angele A. Gilroy, et al, Broadband Internet Access: Background and Issues, CRS Issue Brief for Congress, April 2008.

[5] Laxma Nandikonda, Users Should Be Concerned of Spyware in Free P2P Software, HUT T-110.551, seminar on Internetworkin, 2005.

[6] Karthik Lakshminarayanan et al, Network Performance of Broadband Hosts: Measurements & Implications, Technical Report, 2003.

[7] Ferguson et al, Quality of Service: Delivering QoS on the Internet and in Corporate Networks, John Wiley & Sons, January 1998.

[8] Vegesna et al. IP Quality of Service for the Internet and the Intranets, Indianapolis: Cisco Press, 2000.

[9] ITU-T Rec E.800: Terms and definitions related to quality of service and network performance including dependability, ITUT –T, 1994.

[10] Robert Popp et al, Designing Technical Systems to Support Policy: Enterprise Architecture, Policy Appliances, and Civil Liberties, Emergent Information Technologies and Enabling Policies for Counter Terrorism, 2006.

[11] Dinesh C. Verma,et al, Policy based Management of Content Distribution Networks, IEEE Network Magazine, Vol. 16, pp. 34-39, 2002.

[12] A. Westerinen et al, Terminology for Policy- Based Management, RFC 3198, November 2001.

[13] Adrian Waller et al, Policy based Management Network, INET, May 2004.

[14] 3GPP TS 23.203 V7.6.0, 3rd Generation Partnership Project; Technical Specification, Policy and charging control architecture (Release 7), 2008.

[15] Ray S. Atarashi et al, Policy Control Network Architecture using Metadata, Dublin Core Metadata Initiative, 2002.

[16] John Cushnie et al, Evolution of Charging and Billing models for GSM and Future Mobile Internet Services, Proc. of Quality of Future Internet Services, Lecture Notes on Computer Science, Vol. 1922, pp. 312-323, 2000.

[17] Sinalização e controlo de Serviços, Portugal Telecom Inovação SA.

[18] Rodney Thayer, What is Network Policy Enforcement?, InteropNet Labs Full Spectrum Security Initiative, May 2005.

[19] Radia Perlman, Interconnections: Bridges, Routers, Switches, and Internetworking Protocols, Addison-Wesley Longman Publishing Co., Inc, 2000.

[20] John Strassner, Policy-Based Network Management: Solutions for the Next Generation (The Morgan Kaufmann Series in Networking), Morgan Kaufmann Publishers Inc., 2003.

[21] D. Durham, Ed. Et al, The Common Open Policy Service Protocol (COPS), RFC 2748, January 2000.

[22] F. Baker et al,The Resource ReSerVation Protocol (RSVP), RFC 3175, September 2001.

[23] OpenView Network Management Division Hewlett-Packard Company, A Primer on Policy-based Network Management, V1.0, 1999.

[24] K. Chan et al, COPS Usage for Policy Provisioning (COPS-PR), RFC 3084, March 2001.

[25] R.Yavatkar et al, Framework for Policy-based Admission Control, RFC 2753, January 2000.

[26] R. Braden et al., Integrated Services in the Internet Architecture: an Overview, RFC 1633, June 1994.

[27] S. Shenker et al., General Characterization Parameters for Integrated Service Network Elements, RFC 2215, September 1997.

[28] S. Black et al., An Architecture for Differentiated Services, RFC2475, December 1998.

[29] ECMA TR/91, Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN), Ecma-International, 2005.

[30] Siegmund M. Redl et al, An Introduction to GSM, Artech House, 1995.

[31] Miikka Poikselka et al, The IMS: IP Multimedia Concepts and Services, Wiley, 2006

[32] Cathal MC Daid, Overview and Comparison of QoS Control in Next Generation Networks, Palowiless,3G/UMTS Resource Center,2000.

[33] 3GPP TS 23.125 V6.7.0: Overall high level functionality and architecture impacts of flow based charging, 2005.

[34] 3GPP TS 23.207V6.6.0: End-to-end Quality of Service (QoS) concept and architecture, 2005.

[35] Victor Y.H. Kueh et al, Evolution of Policy Control and Charging (PCC), Architecture for 3GPP Evolved System Architecture, Proc .of Vehicular Technology Conference,Vol.1, pp. 259-263, May 2006.

[36] 3GPP TS 32.240: Telecommunication management, Charging management; Charging architecture and principles (Release 6), March 2005.

[37] Nortel, Nortel Enterprise Policy Manager 4.3, Product Brief.

[38] B. Aboab et al., Extensible Authentication Protocol (EAP), RFC 3748, June 2004

[39] C, Rigney et al., Remote Authentication Dial In User Service (RADIUS), RFC 2865, June 2000.

[40] Redknee Synaxis Policy Decision Rules Server (PDRS), Product bulletin.

[41] C. Bettstetter et al, GSM Phase 2+; General Packet Radio Service GPRS: Architecture, Protocols and Air Interface, IEEE Communications Surveys, Vol 2, No.3, 1999.

[42] P.Calhoun et tal, Diameter Base Protocol, RFC 3588, September 2003

[43] Cisco Service Control Solution Deployment: Consulting Service Offerings from Cisco Services, Cisco Systems, Brochure, April 2007.

[44] Cisco SCE 2000 Series Service Control Engine, Cisco Systems, Data sheet, October 2006.

[45] Cisco Systems, Maximizing use of mobile data infrastructure: the importance of service control in mobile networks, White Paper, June 2005.

[46] Cisco SCA BB Introduction to Policy Integration Solution Guide, Cisco System, May 2007.

[47] IP-Raft online/offline Charging System, data sheet, PT Inovação.

[48] Shipnet – service handling on IP Networks, data sheet, PT Inovação.

[49] TIA-873-008 - IP Multimedia Subsystem; Accounting Information Flows and Protocol. December 2003.

[50] TIA-873-000 - All-IP Core Network Multimedia Domain Overview. Version 1.0, December 2003.

[51] Lars-Erik Sellin et al, SIM – The basis for Mobile Value Added Services, White Paper.

[52] DELSYS, Technical Note 301: Synchronization and Triggering.

[53] Paul W. Bayliss, Intelligent Networks: The Path to Global Networking, International Council for Computer Communication Conference, 1992.

[54] 3GPP TS 23.002, Network architecture, Release 4, 2002.

[55] Jorma Tuominen, Test process analysis of Gateway GPRS Support Node, Master Thesis, Helsinki University of technology, 2006.

[56] CISCO, Subscriber Control and Billing with the Cisco Content Services Gateway, White Paper, March 2003.

[57] W. Richard Stevens, TCP/IP Illustrated, Volume 1: The Protocols, Addison-Wesley Longman Publishing Co., Inc, 1993.

[58] Cisco SCMS SCE Subscriber API Programmer Guide, Release 3.1, May 2007

[59] Cisco SCMS SM Java API Programmer Guide, Release 3.1, May 2007

[60] P. Bernstein. Middleware: A Model for Distributed System Services, Communications of the ACM, Vol. 39, pp.89-98, 1996.

[61] M. Fowler, UML Distilled, Third Edition, Addison-Wesley, 2004.

[62] Stephen et al, Object-Oriented and Classical Software Engineering, Seventh Edition, McGraw-Hill, 2006.

[63] John K. Ousterhout, Scripting: Higher Level Programming for the 21st Century, IEEE Computer Magazine, Vol. 31, pp. 23-30, 1998

[64] Neal Stephenson, In the Beginning...Was the Command Line, William Morrow & Co., Inc. , 1999.

[65] Maurice J.BACH, The design of the Unix operating system, Prentice Hall, Inc , 1986.

[66] David A. Petterson et al, The Case for the Reduced Instruction Set Computer, SIGARCH Computer Architecture News, pp. 25-33, 1980.

[67] CISCO, Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting, Technical Support, QoS Policing, ID 19645, August 2005.

[68] Leonidas Georgiadis et al, Efficient network QoS provisioning based on per node Traffic Shaping, IEEE/ACM Transaction on Networking, Vol. 4, pp. 482-501, IEEE, 1996.

6.2 Referências WWW

[web1] http://www.3gpp.org

[web2] www.sei.cmu.edu/str/descriptions/api.html

[web3] http://java.sun.com/

[web4] http://www.oracle.com/database/timesten.html

[web5] http://speedmeter.fccn.pt/

Anexo A1 Pseudo-código SCE

```
class PseudoSCE {

String ip;
int port;
int mode;
int cnxId;
String domain;

PRPC_SCESubscriberApi sceapiP;

Queue queueSCEQueue;
public SCE()
{
    sceapiP.init();
    sceapiP.connect();
    this.start();
}
void addSceInputEvent(Object session)
{
        this.queueSCEQueue.enqueue(session);
}

Object getInputEvent()
{
        Object obj;
        try {
                obj =this.queueSCEQueue.dequeue();
                return obj;
        }

        void loginReqPush(Session session)
        {
                sceapiP.login(session.subscriberId,
                              session.network,
                              session.networkaAdditive,
                              session.policyProfile);
        }


        void logoutReq(Session session)
        {
                sceapiP.logout(session.msg.subscriberId,
                              nid,
                              resultHandler);
        }

        void loginResPull(Session session){

                sceapiP.loginPullResponse(session.subscriberId,
                              session.anonymousSubscriberId,
                              session.network,
                              session.policyProfile);
        }

        void UpdateRq(Session session)
        {
        sceapiP.policyProfileUpdate(session.subscriberId,
                                    session.policyProfile);
        }
```

```
boolean processSceInputOperation()
{
        Session s = this.getInputEvent();
        switch(s.operation)
        {
        case LOGINRQ:
        {

                if (mode == PUSH)
                {
                this.loginReqPush(s);
                }
                else if(mode == PULL)
                {
                this.print("Error Unexpected Login Rq: mode Pull!!");
                }

        }
        case LOGINRS:
        {
                if (this.mode == PUSH)
                {
                this.print("Error Unexpected Login Res: mode Push!!");
                }
                else if (this.mode == PULL)
                {
                this.loginResPull(s);
                }
        }
        case UPDATERQ:
        {
                this.UpdateRq(s);
                }
                case LOGOUTRQ:
                {
                this.logoutReq(s);
                }

        }
}
        void start()
        {
                try{
                        while(!main.killed())
                        {
                                this.processSceInputOperation();
                        }

                }
                this.disConnect()
        }

}
```

Figura A 1 Pseudo-código do objecto SCE.

Anexo A2 Pseudo-código ProcessRPMsg

```
class pseudoProcessRPMsg {

Queue rpQueue;
RPConInt rpInst;
public  pseudoProcessRPMsg(RpConInit rpInstP){
        rpInst = rpInstP;
        this.start();
}
void rpUnfold(byte RPmsg) {

        Session s = this.getSession(RPmsg);
        switch(s.operation){
        case Constants.LOGINRQ:
                main.addObjectToQueue(s);
        case Constants.LOGINRS:
                main.addObjectToQueue(s);
        case Constants.UPDATERQ:
                main.addObjectToQueue(s);
        case Constants.UPDATERS:
                this.print("Unexpected Update Response received.");
        case Constants.LOGOUTRQ:
                main.addObjectToQueue((Object) new Integer(sessionIndex));
        case Constants.LOGOUTRS:
                this.print("Unexpected Logout Response received. ");
                }
        }
}
void start()
{
while (!main.Killed()) {
        obj =null;
        try {
                obj = (Object) this.getObjectFromQueue();
                }
        switch (session.operation){
        case Constants.LOGINRS:
                foldMsg = encodeLoginResPush(session);
                try{
                        rpInst.sendMsgToActive(foldMsg);
                    }
        case Constants.UPDATERQ:
                this.print("Unexpected Update Request received.");
        case Constants.UPDATERS:
                foldMsg = encodeUpdateRes(session);
                try{
                        rpInst.sendMsgToActive(foldMsg);
                   }
        case Constants.LOGOUTRQ:
                this.print("Unexpected Logout Request received.");
                        break;
        case Constants.LOGOUTRS:
                fordMsg = encodeLogoutRes(session);
                try{
                        rpInst.sendMsgToActive(foldMsg);
                    }
        }
}
}
void addObjectToQueue(Object obj){
        this.rpQueue.enqueue(obj);
}
Object getObjectFromQueue(){
        Object obj=null;
        obj=this.rpQueue.dequeue();
return temp;
}
}
```

Figura A 2 Pseudo-código do objecto ProcessRPMsg.

Anexo B1 Login modo Pull

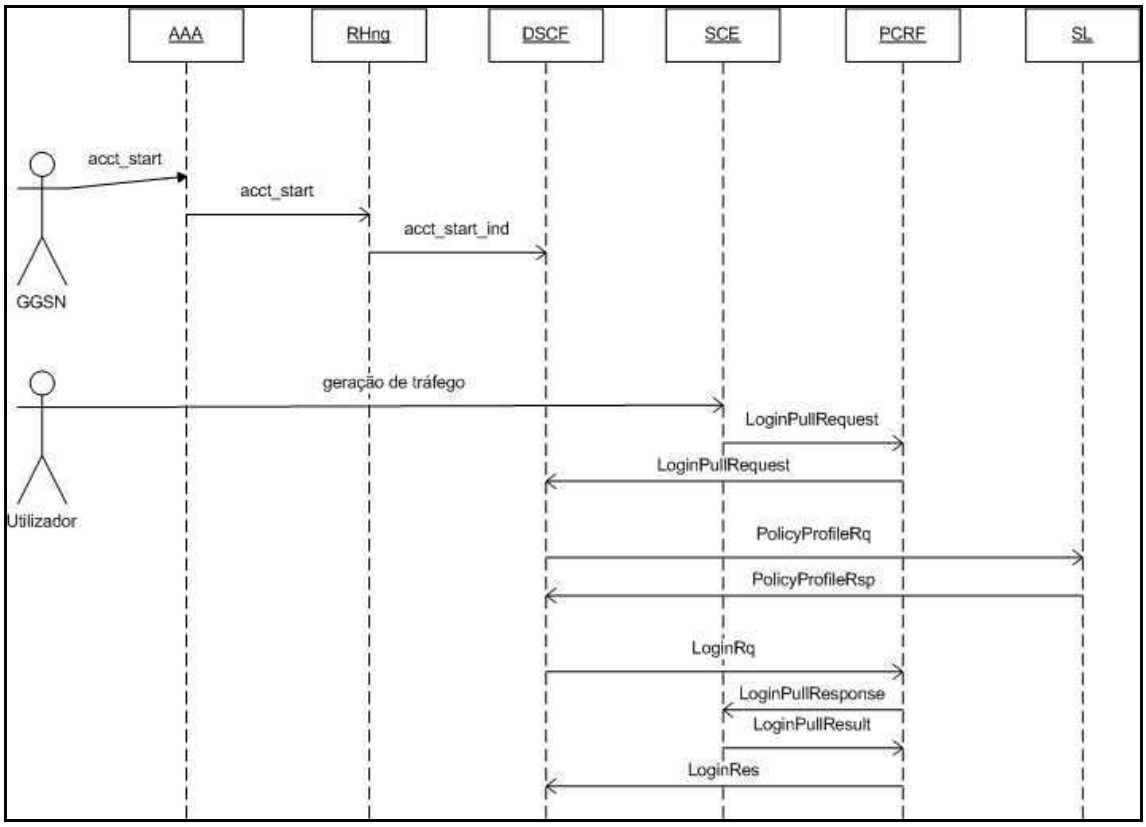

Figura B 1 Login de um utilizador com o SCE, em modo *Pull.*

A interacção entre as diversas entidades ilustradas na Figura B1 é a seguinte:

- O GGSN devido a sua localização na arquitectura da solução (pode ser vista na Figura 3. 2 Arquitectura da solução *Policy Enforcement*), é a primeira identidade da solução a lidar com pedidos de iniciação de sessão, enviando os pedidos de *accounting start* via RHng para o DSCF.
- O utilizador neste modo de funcionando pode inicialmente gerar tráfego baseado na política por defeito definida no SCE. Neste ponto é iniciado o processo de autenticação e associação da política.
- O SCE envia um pedido de autenticação para o PCRF baseado no IP do utilizador que iniciou a sessão, este processo é designado de *Login Pull Request.*
- O PCRF envia para o DSCF o pedido de autenticação juntamente com o IP do utilizador.

- O DSCF com base no MSISDN recebido no *accounting start,* e do IP, questiona a SL acerca da política à aplicar, para o utilizador em questão.
- O SL envia para o DSCF a informação necessária para o devido controlo da sessão.
- O DSCF envia para o PCRF a informação passada pela SL.
- O PCRF baseado no MSISDN, na política recebida através do DSCF e do IP em que o utilizador iniciou a sessão, indica ao SCE a política a aplicar, assim como o identificador que o utilizador irá ficar associado.
- O SCE com a nova informação faz o devido controlo do tráfego baseado na nova política, substituindo o controlo que estava a ser feito baseado na política por defeito.

Anexo B2 Logout modo Pull

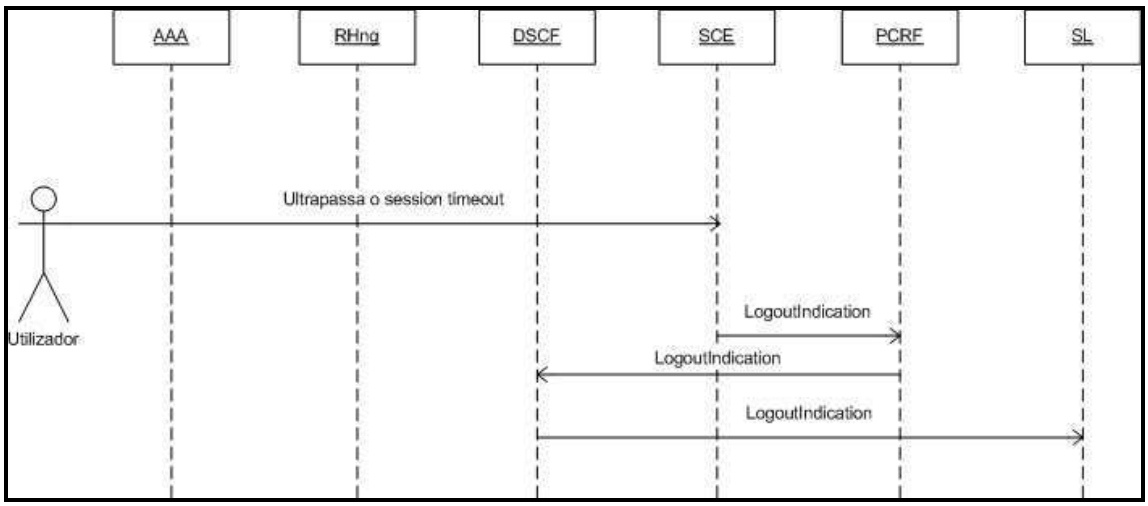

Figura B 2 Logout de um utilizador, com o SCE em modo *Pull.*

A interacção entre as diversas entidades ilustrada na Figura B2 é a seguinte:

- O SCE detecta que um utilizador ultrapassou o tempo predefino, para a duração de uma sessão, iniciando de imediato o processo de *Logout,* enviando para o PCRF a mensagem de *Logout Indication*.
- O PCRF envia para o DSCF a informação de *Logout* do utilizador.

- O DSCF informa a SL que o IP do utilizador não se encontra mais mapeado no SCE.

Anexo B3 Login via SM modo Pull

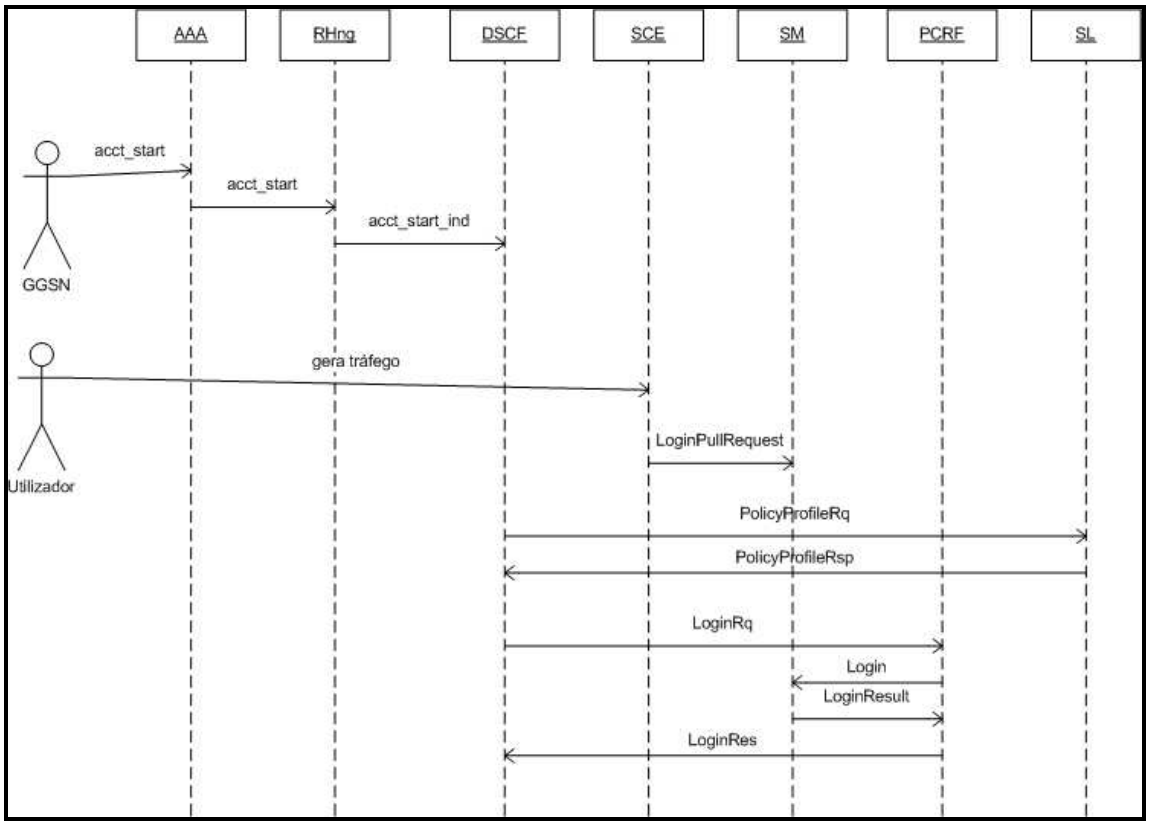

Figura B 3 Login de um utilizador, via SM com o SCE em modo *Pull.*

Na Figura B3 é apresentado o cenário em que a política a aplicar não está no SM, sendo a interacção das entidades semelhantes a operação *Login* modo *Pull,* descrita na secção 4.1.1 do capítulo 4.