Instituto Politécnico de Setúbal

Escola Superior de Ciências Empresariais

Protocolo de Gestão Remota TR-069
CPE WAN Management Protocol

Relatório de Estágio

Alfredo Rigoberto Francisco da Conceição

Relatório de estágio apresentado para cumprimento dos requisitos necessários à obtenção do grau de

MESTRE EM SISTEMAS DE INFORMAÇÃO ORGANIZACIONAIS

Orientadora: Professora Doutora Leonilde Reis

Altran: Eng. Hélder Pinheiro

Setúbal, 2015

Dedicatória

Dedico este trabalho e todo o esforço despendido, primeiramente a Deus pela dádiva de me conceder o presente mais precioso, o dom da vida, ao meu amado pai Conceição Alfredo Hebo, e a todos que sempre me apoiaram desde o início e acreditaram que este dia seria uma realidade. Simultaneamente quero colocar uma frase que se enquadra neste Mestrado em Sistemas de Informação Organizacionais, enfatizando o valor da gestão da informação.

*How you gather, manage and use information will determine whether you win or lose. (*Bill Gates*)*

Agradecimentos

O presente relatório de estágio, só foi possível de realizar graças o apoio incondicional de várias pessoas, de um modo geral aproveito para expressar profundamente a minha gratidão pela contribuição incomensurável que tiveram para a realização deste relatório de estágio, aproveito no entanto para agradecer particularmente a algumas pessoas, cuja contribuição foi decisiva para a concretização do referida relatório de estágio.

À minha orientadora de Mestrado, Professora Doutora Leonilde Reis, o Engenheiro Hélder Pinheiro e o João Feitas da Altran Portugal, pela motivação, disponibilidade, apoio prestado, pela confiança demonstrada ao longo deste ciclo de estudos e pela sábia orientação ministrada na elaboração deste relatório de estágio.

Ao professor e coordenador do curso Doutor José Manuel Gaivéo, pelo convívio, apoio, compreensão e amizade.

A todos os Professores, pela disponibilidade e paciência ao longo do período curricular.

Aos meus colegas de Mestrado, pela paciência e por todo o apoio prestado ao longo desta caminhada, onde juntos sempre fomos superando cada obstáculo.

Ao casal de pastores Hélio e Givanilde Silveira pelos conselhos e incentivos que foram decisivos no meu desenvolvimento a nível pessoal e académico.

Ao meu pai, irmãos e família no geral especialmente a minha tia Suzana Pedro Guinê, pelos momentos que ficaram privados de estar comigo, e pelo apoio dado, espero poder compensá-los no futuro próximo.

Índice Geral

Lista de Figuras

Lista de Gráficos

Lista de Tabelas

Siglas/Acrónimos

ACS – *Auto Configuration Server*

ADSL – *Asymmetric Digital Subscriber Line*

BEEP – *Blocks Extensible Exchange Protocol*

CLI – *Command Line Interface*

CPE – *Customer Premises Equipment*

CWMP – *CPE WAN Management Protocol*

DRP – *Disaster Recovery Plan*

DSL – *Digital Subscriber Line*

DSLAM – *Digital Subscriber Line Access Multiplexer*

EPON – *Ethernet Passive Optical Network*

HTTP – *HyperText Transfer Protocol*

HTTPS – *HyperText Transfer Protocol Secure*

IETF – *Internet Engineering Task Force*

IoT – *Internet of Things*

IP – *Internet Protocol*

ISP – *Internet Service Provider*

MIB – *Management Information base*

MPLS – *Multiprotocol Label Switching*

NGN – *Next Generation Networking*

NETCONF – *Network Configuration*

PON – *Passive Optical Network*

POST – *Power On Self Test*

OSI – *Open Systems Interconnection*

QoS – *Quality of Service*

PDU – *Protocol Data Units*

RPC – *Remote Procedure Calls*

SOAP – *Simple Object Access Protocol*

SHDSL – *Symmetric high-speed digital subscriber line*

SMI – *Structure of Management Information*

SNMP – *Simple Network Management Protocol*

SOAP – *Simple Object Access Protocol*

SSH – *Secure Shell*

SSID - *Service Set Identifier*

STB – *Set-Top Box*

TCP – *Transmission Control Protocol*

TLS – *Transport Layer Security*

TR-069 – *Technical Report 69*

UDP – *User Datagram Protocol*

UPnP – *Universal Plug and Play*

URL– *Uniform Resource Locator*

VDSL – *Very-high-bit-rate Digital Subscriber Line*

VoIP – *Voice over Internet Protocol*

VPN – *Virtual Private Network*

WAN – *Wide Area Network*

XML – *eXtensible Markup Language*

Glossário

ACS – Sigla universalmente aceite que deriva de *Auto Configuration Server*, servidor responsável pela auto configuração de CPE (Broadband-Forum, 2013a).

CLI – Sigla universalmente aceite que deriva de *Command Line Interface*, mecanismo que permite interagir com um software através da digitação de comandos para realizar determinadas tarefas (winehq, 2013).

CPE – Sigla universalmente aceite que deriva de *Customer-Premises Equipment*, equipamento localizado nas instalações do cliente e ligado a um canal de uma operadora de telecomunicações (Broadband-Forum, 2013a).

CWMP – Sigla universalmente aceite que deriva de *CPE WAN Management Protocol*, também bem conhecido por TR-069, trata-se de um protocolo da camada de aplicação que permite gestão remota de CPE (Broadband-Forum, 2013a).

QoS – Sigla universalmente aceite que deriva de *Quality of Service*, refere-se a capacidade de fornecer um serviço conforme as exigências (techopedia, 2015).

RPC – Sigla universalmente aceite que deriva de *Remote Procedure Call*, trata-se de um processo de comunicação que permite que um programa local invoque remotamente a execução de um outro programa (Broadband-Forum, 2013a).

STB – Sigla universalmente aceite que deriva de *Set-Top Box* ou conversor, é um termo que descreve um equipamento que se liga a um televisor e a uma fonte externa de sinal, e transforma este sinal em conteúdo no formato que possa ser apresentado em uma tela (Broadband-Forum, 2013a).

TR-069 – Sigla universalmente aceite que deriva de *Technical Report 69*, desenvolvido pelo atual *BroadBand Forum*, corresponde à norma de especificação do protocolo CWMP (Broadband-Forum, 2013a).

UPnP – Sigla universalmente aceite que deriva de *Universal Plug and Play*, é um conjunto de protocolos de redes de computadores que permite conexões diretas e simplificadas para implementação de redes em casas e escritórios (UPnP-Forum, 2008).

Resumo

No contexto atual, de um mundo de negócios cada vez mais competitivo, responder rapidamente às condições de mudança, ser inovador no atendimento face às necessidades dos clientes e no modo de atuar perante o mercado, torna-se um fator crítico de sucesso.

A evolução da banda larga e a entrada no mercado de equipamentos terminais com funções específicas por tipo de serviço (Internet, VoIP, IPTV…), implicam a adoção de soluções inovadoras que permitam uma gestão, configuração rápida e flexível de acordo com a especificidade de cada cliente.

A convergência de diversos serviços (Internet, VoIP, IPTV…) num único canal de acesso (*Triple Play e Quadruple Play*) e a diversidade de aplicações têm dificultado a gestão, segurança e garantia do QoS (*Quality of Service*) nas redes de comunicação, incitando assim a busca de novas soluções.

O objetivo deste relatório de estágio, consiste em: *i)* Estudo do protocolo de gestão remota TR-069 CPE WAN Management Protocol; *ii)* Estudo e instalação de um ACS; *iii)* Testar a conformidade de implementação do protocolo TR069 - CWMP em CPE´s, no intuito de prevenir eventuais problemas relacionados com o protocolo.

Para se atingir estes objetivos utilizou-se como metodologia a revisão da literatura, análise de relatórios técnicos, ferramentas de *troubleshooting*, automação de testes e criação de *scripts*.

Foi possível concluir que a atividade de execução de testes é crucial porque é a forma de garantir que o processo de execução de testes decorre de acordo com os *steps* inicialmente estipulados, no sentido de garantir a conformidade do protocolo TR069 - CWMP nos CPE.

O processo de execução de testes permitiu concluir a viabilidade de submeter os dispositivos (CPE) ao processo de *Acceptance Testing* e/ou fase de aceitação, pelo que, constatou-se que apenas uma pequena percentagem de testes falharam e que estão tipificados no sentido de ser possível prevenir a ocorrência de problemas dos CPE´s.

Palavras-chave: CWMP, TR-069, CPE, ACS, testes.

Abstract

In the current context, in a world of increasingly competitive business, respond quickly to changing conditions, be innovative in service to the needs of customers and in order to act before the market becomes a critical success factor. The evolution of broadband and entry into the equipment market terminals with specific functions by service type (Internet, VoIP, IPTV ...), involve the adoption of innovative solutions that enable management, fast and flexible configuration according to specific character each client.

The convergence of different services (Internet, VoIP, IPTV...) a single access channel (Triple Play and Quadruple Play) and the diversity of applications have hampered the management, security and guarantee of QoS (Quality of Service) in communication networks, thus prompting the search for new solutions.

The purpose of this internship report consists of: i) remote management protocol TR-069 Study CPE WAN Management Protocol; ii) Study and installation of ACS; iii) test the compliance of implementing the CWMP protocol terminal equipment CPE, in order to prevent any problems with the protocol in CPE's.

To achieve these goals we used as methodology the literature review, technical reports analysis, troubleshooting tools, test automation and scripting.

It was concluded that the test execution activity is crucial because it is the way to ensure that the test execution process proceeds according to the steps set out initially, to ensure compliance of the CWMP protocol in CPE's.

The process of running tests led us to conclude the feasibility of subjecting the devices (CPE) to the Acceptance Testing process and / or acceptance phase, whereby it was found that only a small percentage of failed tests and are typified in the sense be possible to prevent the occurrence of problems CPE's.

Keywords: CWMP, TR-069, CPE, ACS tests.

1. Introdução

Atualmente as redes de comunicação têm convergido para um modelo de redes de multisserviço fundamentadas em tecnologias integradas, denominadas de *Next Generation Networking* (NGN). Segundo ITU, (2004) *Next Generation Networks*, é uma rede baseada em pacotes capaz de fornecer serviços de telecomunicações aos utilizadores e capaz de fazer uso múltiplo da banda larga, *QoS-enabled* tecnologias de transporte em que as funções relacionadas com o serviço são independentes do transporte relacionadas com as tecnologias subjacentes. Permite o acesso irrestrito aos utilizadores de redes e provedores de serviços concorrentes e serviços da sua escolha. Suporta a mobilidade generalizada, que permitirá prestação consistente e onipresente de serviços aos utilizadores.

Para os *Internet Service Providers* (ISPs), as atuais redes de acesso à banda larga evidenciam claramente um elevado risco de segurança nas redes dos clientes bem como uma maior dificuldade em garantir a respetiva QoS (*Quality of Service*). Estas dificuldades estão diretamente relacionadas aos seguintes fatores:

- Elevados débitos disponíveis para cada um dos clientes;
- Elevado número de clientes servidos por cada ISP;
- Constantes solicitações das ligações (xDSL, cabo, fibra, 3G/4G);
- Falta de conhecimentos técnicos dos clientes que proporcionam o funcionamento correto de suas redes.

Apesar de que grande parte das dificuldades atuais já existirem antes, a tendência ininterrupta das ligações *dial-up* clássicas e os reduzidos débitos disponíveis, tornavam mais simples aos ISP a resolução de tarefas tais como, detetar e controlar situações de risco para as suas redes, para os seus clientes e terceiros.

A convergência de diversos serviços (Internet, VoIP, IPTV) num único canal de acesso (*Triple Play e Quadruple Play*) e a diversidade de aplicações têm dificultado a gestão, segurança e garantia do *QoS* nas redes de comunicação, incitando assim a busca de novas soluções.

Os ISP costumam estimar que a gestão e segurança da rede dos clientes estão fora da sua esfera de influência, e que devem ser administradas pelos mesmos.

Geralmente, os provedores tendem à considerar que a sua esfera de influência termina no seu equipamento de fronteira, constituindo responsabilidade do cliente a gestão dos seus próprios equipamentos de *home gateway* e de tudo o que esteja para lá desses equipamentos.

Com o surgimento das redes *Triple e Quadruple Play* alterou-se substancialmente esta visão, começando a ser imprescindíveis e admitidas algumas intervenções dos provedores na rede do cliente, especialmente para administrar remotamente *Set-Top Box* (STB) e *gateways* de serviço telefónico.

Com o acesso dos provedores nas redes dos clientes tem influenciado que entidades tais como BroadBand-Forum, (2004) e HGI, (2004), trabalhem na padronização das tecnologias que possibilitam administrar e supervisionar remotamente os equipamentos de fronteira *home gateway* e outros equipamentos CPE (*Customer Premises Equipment*) circunscrevidos na rede do cliente.

1.1. Contextualização do Tema

Os primeiros instrumentos usados pelos administradores das redes de computador para gerir os seus dispositivos foram as *Command Line Interface* (CLI), embutidas nos equipamentos e o SNMP desenvolvido pelo IETF. Hoje em dia tem-se escolhido o padrão *CPE WAN Management Protocol* (CWMP), também conhecido como TR-069.

Technical Report 069 (TR-069) pertence ao conjunto das *Broadband Suites* do mesmo fórum, e que faz parte do conjunto de normas e protocolos extensíveis orientados para a gestão em ambientes de banda larga.

Esta norma tem tido grande aceitação globalmente pelos maiores fabricantes de dispositivos e fornecedores de serviço, e espera-se que seja gradativamente integrada em todos os dispositivos e aplicações de administração, do lado dos provedores, e por todos os dispositivos, no lado dos fabricantes de CPE (routers/modems xDSL e STB).

Optar pela utilização do protocolo CWMP possibilita aos operadores que seja mais simples difundir novas regras e configurações para grandes grupos de utilizadores, em função dos próprios perfis e dispositivos instalados. A gestão de configurações é feita mediante um *Auto Configuration Server* (ACS), capaz de fornecer atualizações de software, alteração de configurações e recolha de dados para prevenir problemas dos CPE.

Tecnologias mais novas como UPnP e NetConf foram também por sua vez estandardizadas com o objetivo de ajudar e responder as necessidades atuais de gestão de redes.

O nosso objetivo principal foi, com base numa solução *Open Source* de gestão de equipamentos utilizando o protocolo CWMP, que se comporta como servidor ACS, realizar um conjunto de testes em CPE que suportam o mesmo protocolo a fim de verificar a

conformidade de implementação do protocolo CWMP, e em caso de não conformidade a elaboração de um conjunto de linhas de orientação como proposta de melhoria, permitindo assim aumentar o nível de qualidade de serviço bem como o cumprimento de requisitos de dispositivos que suportam o protocolo CWMP. A figura 1 ilustra a arquitetura de funcionamento do protocolo CWMP.

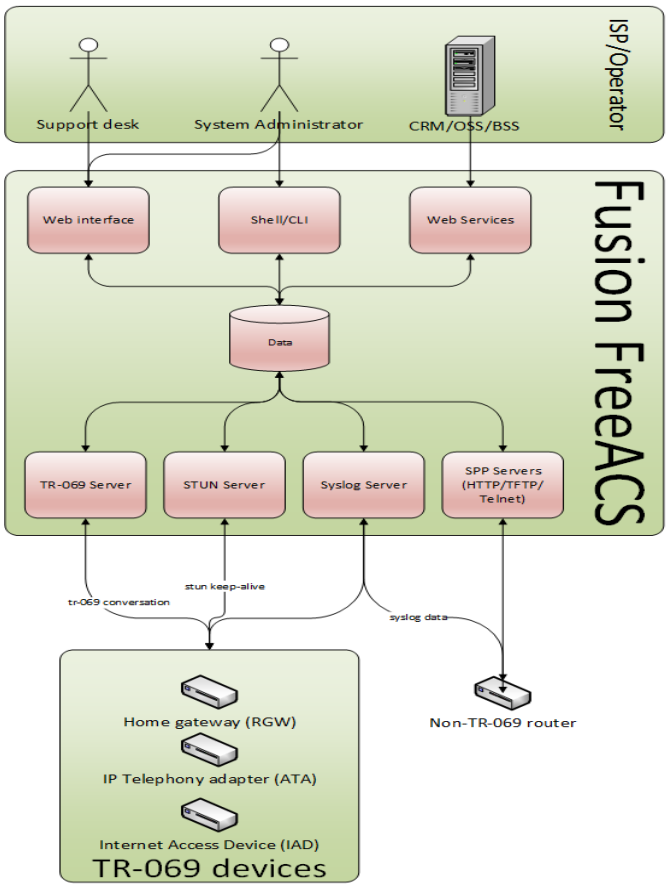

Figura 1- Arquitetura de funcionamento do protocolo CWMP

Fonte: *Free TR-069 ACS* (FreeACS, 2015)

A Figura 1 apresenta-nos de forma bastante clara e simples a arquitetura de funcionamento do protocolo CWMP incluindo os 3 principais componentes que o definem, nomeadamente:

1) ISP, agente responsável pelo fornecimento de serviço.
2) ACS e seus componentes, servidor responsável pela gestão de equipamento.
3) Cliente, representado por todos os *home gateway*.

1.2. Problemática

Segundo o diretor executivo da *Broadband Forum* Mersh, (2012) no artigo *simplifying remote management of billions of devices*, afirma que com o surgimento de novos paradigmas tais como *Connected Home* e *Internet of Things*, estamos a desenvolver um mundo com bilhões de dispositivos ligados a novos serviços e aplicações. Diante deste cenário em que se constata um crescimento vertiginoso de dispositivos ligados à internet, surge por parte dos fornecedores de serviços questões como:

Como gerir estes ambientes complexos?

Como garantir a qualidade de serviço?

Um dos problemas que os clientes da Altran pretendem que seja resolvido ao solicitar os serviços da mesma prende-se essencialmente na garantia da qualidade de funcionamento do protocolo CWMP em CPE. Uma vez garantida a qualidade de serviço do protocolo CWMP estes clientes terão os seguintes benefícios:

- Redução de custos de intervenção de técnicos no local;
- Redução de custos operacionais;
- Eficiência no atendimento e consequente resolução de problemas na rede do cliente;

E poderão evitar problemas como:

- Envio de técnicos nas instalações do cliente para resolver problemas que podiam ser resolvidos mediante a utilização do protocolo CWMP;
- Elevados custos operacionais;
- Ineficiência na resolução de problemas;

Espera-se no final deste relatório de estágio, poder mostrar como prevenir problemas dos CPE, com intuito de garantir a qualidade de serviços relacionados com protocolo CWMP.

1.3. Âmbito e Objetivos

No âmbito do protocolo de estágio realizado entre o IPS (Instituto Politécnico de Setúbal), através da ESCE (Escola Superior de Ciências Empresariais) e a empresa Altran Portugal, relativo à unidade curricular de dissertação, relatório de projeto ou relatório de estágio. Desenvolveu-se o presente relatório de estágio com o intuito de atingir os seguintes objetivos:

- Estudo do protocolo de gestão remota CWMP de modo a compreender o seu funcionamento;

- Definir a arquitetura das plataformas de gestão remota (Servidores ACS);
- Fornecer infraestrutura e plataformas para garantir o funcionamento de um laboratório de testes de equipamentos terminais CPE;
- Testar a conformidade de implementação do protocolo CWMP em equipamentos terminais CPE, no intuito de prevenir eventuais problemas relacionados com o protocolo nos CPE;

1.4. Metodologia

A metodologia adotada para a realização deste relatório de estágio, foi o método qualitativo, cujo procedimento metodológico é o estudo empírico, baseado na investigação da literatura referente ao standard, protocolo de gestão remota TR-069 *CPE WAN Management Protocol*, tecnologias similares, suas funcionalidades e arquitetura.

Paralelamente utilizou-se os seguintes métodos: revisão da literatura, formação, análise de relatórios técnicos, interação em fóruns da internet, ferramentas de automação de testes, ferramentas de *troubleshooting* e desenvolvimento de *scripts* em *JavaScript*.

1.5. Estrutura do Relatório de Estágio

No que respeita à estrutura deste documento, o mesmo encontra-se dividido em 5 capítulos. O primeiro capítulo **Introdução,** visa enquadrar o trabalho, contextualizar o tema, definir a problemática, apresentar o âmbito e os objetivos traçados e sua metodologia.

O capítulo 2 destina-se ao **Enquadramento Teórico** relacionado com o trabalho de estágio desenvolvido, ou seja, será descrito o que já se encontra produzido por outros, e o que serviu de base para o desenvolvimento deste relatório.

Pretende-se com o terceiro capítulo apresentar a organização que acolheu o estagiário para a realização do estágio curricular, Altran Portugal, referindo essencialmente à **Caracterização da Organização**, às atividades da organização, e uma breve caracterização dos ativos, SI/ TIC.

O quarto capítulo refere-se à **Descrição e Análise das Atividades Desenvolvidas** durante o estágio curricular, no qual é descrito o âmbito do projeto e seus componentes, configurações do ambiente de teste, preparação das ferramentas de automação de teste e finaliza com execução de testes.

Para finalizar no quinto capítulo serão apresentadas as principais **Conclusões** e **Perspetivas de Trabalho Futuro.**

2. Enquadramento Teórico

Neste capítulo procura-se dar uma visão da temática em questão, bem como dos principais protocolos de gestão remota.

2.1. Protocolos de Gestão

Desde a mais remota antiguidade que o ser humano procura e desenvolve meios e máquinas para realizar cálculos, do mais simples ao mais complexo, com o mínimo de tempo e o máximo de eficiência e tem-se verificado que tecnologia tem gerado tecnologia a uma velocidade estonteante.

Vale recordar duas áreas que tem registado uma crescente evolução tecnológica, são elas, as redes de telecomunicações e as redes de computadores, pelo que, encontram-se ambas atualmente em sentido de convergência. Esta convergência alinhada aos novos avanços tecnológicos das redes tem conduzido a que estas duas áreas atuem numa dimensão comum, que é o fornecimento de múltiplos serviços sustentados em uma única infraestrutura.

De acordo com Deutsche-Bank, (2006) define convergência como um processo de mudança qualitativa que liga dois ou mais mercados existentes e anteriormente distintos.

De acordo com Rouse, (2015) convergência tecnológica é a combinação de duas ou mais diferentes tecnologias em um único dispositivo.

Partindo destas definições o conceito de convergência tecnológica, corresponde a um conjunto de dispositivos e procedimentos que permitem a interconexão de redes individuais, formando redes de maiores dimensões e capacidades. Estas redes são baseadas na aplicação de computadores e seus recursos de controlo, aliadas à utilização de técnicas de comutação de pacotes e transmissão de dados dos sistemas de telecomunicações, sendo assim, uma combinação de ambas as tecnologias. É de salientar que a grande representação desta convergência é a Internet.

Atualmente já se vive o então conhecido *Internet of Things* (IoT) que é um paradigma que tem como objetivo criar uma ponte entre acontecimentos do mundo real e as suas representações no mundo digital, integrando o estado das coisas que constituem o nosso mundo em aplicações de software, beneficiando do contexto onde estão instaladas, Valente, (2011). Ou seja é cada vez mais visível a implementação de interfaces de rede em dispositivos pessoais e domésticos tais como, (telemóveis, televisão, consolas, tablet, ipad, etc.) que outrora não era possível, esta tendência será cada vez mais crescente e num futuro próximo todos os nossos equipamentos domésticos (fogão,

micro-ondas, lâmpadas, etc.) serão implementados com interfaces de rede, possibilitando a sua ligação à internet. Tudo poderá ser equipado com tais aparelhos de rede, possibilitando uma forma de vida cada vez mais conveniente, indo ao encontro da célebre frase citada por Max Frisch "Tecnologia é a habilidade de organizar o mundo de forma que não tenhamos que senti-lo" (Frisch, 1990).

A criação do modelo de referência OSI, modelo de referência que tinha como principal objetivo ser um modelo standard, para protocolos de comunicação entre os mais diversos sistemas, e assim garantir a comunicação *end-to-end*, Pinto, (2013). Corresponde a um dos maiores passos dados na gestão de redes. Este modelo promoveu a coordenação e estruturação das comunicações de dados, permitindo redução da complexidade de desenvolvimento de normas; maior flexibilidade e simplicidade de implementação de alterações e funcionalidades nas camadas; incorporação de novas tecnologias e compatibilidade entre fabricantes.

Por um longo período à existência de um único protocolo padrão SNMP e as *Command Line Interface* (CLI) embutidas nos dispositivos, mostravam-se suficientes para a execução de tarefas de gestão e monitorização de dispositivos e serviços na rede. No entanto, o SNMP jamais se destacou como uma solução credível e segura no que concerne a configuração e a CLI permanentemente se mostrou como ferramenta pouco credível, pelo facto de certos aspetos funcionais dependerem diretamente do fabricante do dispositivo.

Se por um lado acrescentarmos a estes fatores o crescimento das redes IP, conclui-se facilmente que estas ferramentas não atendem às necessidades de gestão e configuração das redes atuais, por esta razão surge a grande necessidade de desenvolvimento de soluções de gestão automáticas e aptas de configurar sistemas através de protocolos estandardizados e extensíveis, apesar de pouco divulgada existem variadíssimas razões que fazem do CWMP tecnologia de referência na gestão de dispositivos terminais e/ou dos clientes que se encontram para la dos ISP.

O desenvolvimento do protocolo de gestão remota CWMP, apresenta a possibilidade, de que os ISP sejam capazes de aceder remotamente a distintos dispositivos de distintos fabricantes, por meio de uma tecnologia totalmente estandardizada e através da mesma infraestrutura.

Independentemente do âmbito de aplicação do protocolo CWMP ser de configuração ponto a ponto numa rede WAN, o mesmo foi projetado para ser compatível com outras tecnologias, tornando-o assim um protocolo extensível e capaz de chegar também as nossas LAN.

Uma outra característica deste protocolo é a sua flexibilidade, baseia-se em protocolos completamente normalizados e de utilização aberta SOAP, Incognito, (2013), XML, Broadband-

Forum, (2013a), HTTP/HTTPS, Broadband-Forum, (2013a) e TCP, permitindo assim que os próprios ISP desenvolvam as suas próprias ferramentas de gestão.

Fornece todo um conjunto de possibilidades que permitem adicionar serviços e instalar software nos dispositivos terminais, permitem ainda efetuar update e *downgrade* do *firmware* dos dispositivos. Proporciona uma comunicação muito segura e confiável entre o servidor e o dispositivo terminal CWMP.

Tendo em conta as limitações de gestão e configuração, mostradas pelo protocolo SNMP, o IETF criou o *Network Configuration* (NetConf), como um protocolo de gestão e configuração remota baseado em tecnologias abertas e estandardizadas. Comparativamente ao CWMP, o NetConf tem como única grande diferença o facto de permitir ser encapsulado e transportado por meio de diferentes tecnologias (SOAP, BEEP, SSH). É também muito seguro no conjunto das suas implementações.

Neste capítulo iremos falar um pouco de todas estas soluções de gestão, no entanto será dedicado especial atenção ao protocolo de gestão remota CWMP.

2.2. Interface de Linha de Comando

A interface de linha de comando, do inglês *Command Line Interface* (CLI), é um meio que permite o envio de comandos para realizar tarefas em determinado computador ou sistema, onde o utilizador emite comandos para o programa sob a forma de sucessivas linhas de texto, possibilitando assim uma interação com o mesmo, Techopedia, (2013).

Esta interface é largamente utilizada para a gestão de equipamentos, constituindo uma prática muito utilizada no mundo informático.

Segundo Andrews et al. (2015), em geral, uma interface de linha de comando é utilizada para gerir os dispositivos numa rede. Cada dispositivo pode ser controlado e configurado através da utilização do CLI de um dispositivo específico.

Esta prática de gestão de equipamentos para a execução de uma determinada função, baseia-se na escrita de um comando na linha de comandos seguidamente do envio do mesmo, o envio deste comando é feito depois de teclar a tecla *Enter* no teclado. Nesse momento o interpretador da linha de comandos recebe, analisa e executa o referido comando, Stephenson (1999).

O interpretador de linha de comando deve correr num terminal de texto localmente, ou em uma janela *Shell* remotamente, a título de exemplo podemos citar um cliente *Tera Term*, *Mobaxterm*, *Putty* e as linhas de comando do windows.

Depois de concluído o processo de introdução de comando, o interpretador devolve ao utilizador o resultado do comando introduzido em forma de texto no CLI.

Os fabricantes de equipamentos de rede especificamente *hub*, *switch*, router, repetidor, *bridge*, incorporam nos seus equipamentos um conjunto de instruções que possibilitam a configuração dos mesmos através da utilização do CLI, concedendo aos administradores de redes, técnicas inteligíveis de configuração. Vale realçar que estes instrumentos variam de fabricante para fabricante. O uso dos mesmos revela elevados custos operacionais, articulado a conceção de *scripts* e da sua manutenção. Sem esquecer o facto de que o administrador e/ou operador do equipamento necessitar de conhecer convenientemente o equipamento, bem como os comandos que introduz.

A figura 2 ilustra, a utilização do comando *get_params* seguido de um parâmetro para obter informação relativo ao *Service Set Identifier* **(SSID),** posteriormente utiliza o comando *set_params* seguido do mesmo parâmetro e o novo SSID para modificar o SSID anteriormente definido no router. Sendo esta uma prática constante e necessária para a execução de determinados testes ao longo do estágio curricular em que o objetivo consiste em, alterar o SSID do router através do CLI, pensamos que constitui um bom exemplo de gestão de equipamentos utilizando o CLI.

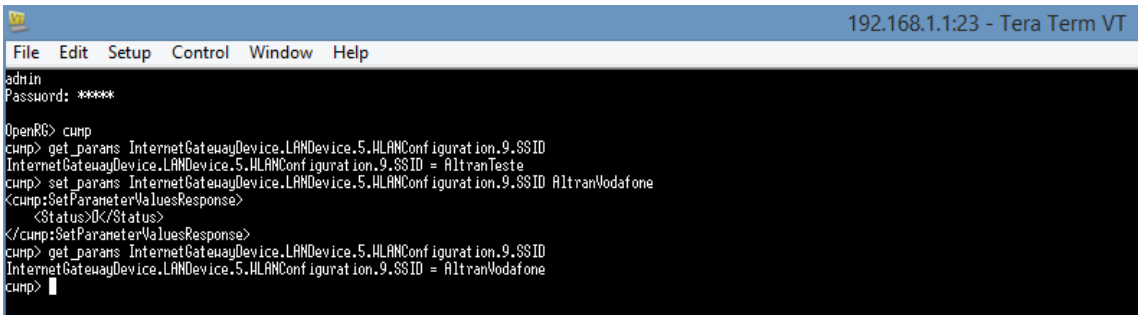

Figura 2- Exemplo de utilização da CLI, para gestão de equipamentos

Fonte: Laboratório de media Altran (Altran, 2015)

Na figura 2 podemos observar que através do CLI é possível executarmos uma infinidade de operações, neste caso em particular utilizou-se os métodos *get e set* e parâmetros CWMP para visualizar e alterar o SSID.

2.3. *Simple Network Management Protocol*

O SNMP é um protocolo de gestão que faz parte da camada de aplicação do modelo OSI, e é amplamente utilizado para obter (*GET*) dados dos dispositivos geridos e alterar (*SET*) as configurações dos dispositivos SNMP que se encontram instalados na rede baseada na pilha de protocolos TCP/IP.

De acordo com, Mauro et al. (2005) "o SNMP é um simples conjunto de operações (e a união das informações dessas operações) dão aos administradores a capacidade de alterar o estado do dispositivo baseado em SNMP. Por exemplo, pode se utilizar o SNMP para desligar a interface do router ou verificar a velocidade de ligação da interface *ethernet*''.

"O SNMP pode ser utilizado para gerir sistemas *unix*, windows, impressoras, *racks* de modem, routers, fontes de alimentação e muito mais. Pode gerir qualquer dispositivo que suporta um software que permite a recuperação de informações SNMP. Isso não inclui apenas os dispositivos físicos, mas também software, tais como servidores web e bases de dados'' Mauro et al. (2005a).

Ao passo que, segundo o IETF, (2002), SNMP é um componente do conjunto de protocolos da internet que consiste de um conjunto de padrões de gestão de redes, incluindo um protocolo da camada de aplicação, um esquema de base de dados, e um conjunto de objetos de dados.

O *Internet Standard Management Framework* identifica 7 componentes que constituem o SNMP, Boavida at al. (2011).

- Uma ou mais entidades de gestão (*management station ou manager*), onde uma aplicação disponibiliza uma interface de gestão que permite ao administrador de rede, recolher informação e controlar os dispositivos de rede;
- Agente de gestão (*management agent*), ou simplesmente agentes, que consistem em componentes de software, residentes nos dispositivos geridos, e que comunicam com a entidade de gestão para dar resposta aos seus pedidos ou enviando-lhes notificações sobre situações anómalas;
- *Management Information Base* (MIB) que resumem toda a informação relativa aos objetos geridos nos dispositivos de rede;

As especificações do *Internet Standard Management Framework* são baseadas numa arquitetura modular, que compreende quatro áreas:

- Uma linguagem de definição de dados, designada por SMI (*Structure of Management Information*) para definir os tipos de dados, os modelos dos MIB *objects* e as regras para escrever e atualizar a informação de gestão;
- Definições da informação relativa aos objetos geridos (*network management objects*) ou MIB *objects*. Concretamente, um objeto gerido pode consistir num controlador do número de pacotes que entram numa interface, uma descrição de um dispositivo, informação sobre o seu estado, etc. A informação relativa a um conjunto de objetos relacionados é resumida num módulo MIB;
- Definição do protocolo SNMP e respetivas operações, utilizado na comunicação entre a entidade de gestão e agentes;
- Funcionalidades de segurança e administração, que vão desde a simples autenticação baseada em comunidade do SNMPv1, até aos mecanismos mais elaborados de segurança especificados no SNMPv3.

O SNMP define sete tipo de mensagens PDU (*Protocol Data Units*), Boavida at al, (2011a).

- *GetRequest, GetNextRequest, GetBulkRequest*: enviadas pela entidade gestora para o agente, para obter um conjunto de valores, o valor seguinte de uma lista ou tabela ou um bloco de valores, respetivamente.
- *SetRequest:* usada pela entidade gestora para modificar um (ou mais) objetos num dispositivo gerido;
- *InformRequest:* gerada e transmitida por uma entidade gestora para notificar outra entidade gestora;
- *Trap:* gerada e transmitida pelo agente, para informar a entidade gestora sobre a ocorrência de um evento anormal;
- *ResponsePDU*: enviadas pelo agente como resposta às mensagens da entidade gestora.

Apesar do SNMP ser um protocolo muito bom em termos de monitorização, o mesmo não se reflete nas ações de configuração. O facto de utilizar data-gramas UDP para transporte da sua informação de gestão, faz dele um protocolo muito pouco fiável e seguro. Devido a estas deficiências, o IETF tem vindo a desenvolver novas versões deste protocolo (SNMPv2 e SNMPv3). O SNMPv3 por sua vez apesar de apresentar um forte mecanismos de segurança, não é ainda suportado por muitos agentes. É, assim, recomendável controlar o tráfego SNMP através de firewall.

Se adicionarmos a estas lacunas o facto do acesso aos agentes não ser controlado nem registado, e ainda o facto da arquitetura das MIBs variarem entre alguns fabricantes, faz com que o SNMP muito dificilmente se torne um protocolo convencional para a configuração de equipamentos.

2.4. *Network Configuration*

De acordo com, IETF, (2011a), NETCONF é um protocolo de gestão de rede desenvolvido e padronizado pelo IETF. Foi desenvolvido pelo grupo de trabalho NETCONF e publicado em dezembro de 2006 como RFC 4741 e posteriormente revisto em Junho de 2011 e publicado como RFC 6241.

O NETCONF permite criar, alterar e apagar configurações dos equipamentos e fornece um conjunto de funcionalidades para a execução de tarefas de monitorização de dispositivos em rede. Vale realçar que, na criação do protocolo NETCONF pretendeu-se conceber uma solução com as seguintes características:

- Capaz de distinguir dados configuráveis e de estado;
- Que seja suficientemente extensível e programável para que os fabricantes de equipamento consigam dar acesso aos dados de configuração através de um único protocolo;
- Que utilize uma representação de dados baseada em XML;
- Que proporcione a integração, instrumentos de segurança e bases de dados;
- Que suporte vários repositórios de dados;
- Que integre mecanismos para transações das configurações;
- Que suporte distintos protocolos seguros de transporte e que suporte notificações assíncronas de eventos.

O seu desenvolvimento foi independente da linguagem de modelação de dados, mas o IETF recomenda o YANG, que é uma linguagem desenvolvida especificamente para a gestão de configurações.

A arquitetura do NETCONF consiste num cliente-servidor, conceptualmente dividido em quatro camadas como se pode observar na figura 3.

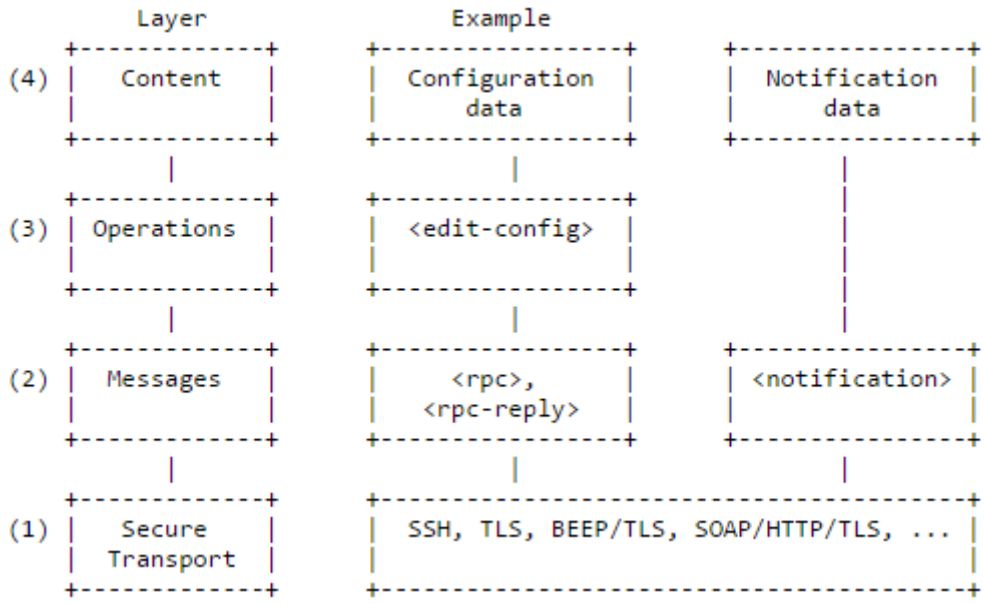

Figura 3- Camadas de protocolo NETCONF

Fonte: RFC: *Network Configuration Protocol* (RFC 624, 2011)

Na figura 3 observa-se o princípio de funcionamento do protocolo NETCONF que consiste na seguinte forma, o cliente requisita operações sobre as configurações que se encontram no servidor e pode subscrever notificações de eventos do servidor. O servidor efetua operações requisitadas pelos clientes e envia notificações de eventos se houver subscrições.

Utiliza-se a linguagem YANG para descrever as configurações dos equipamentos de rede, e as mensagens do protocolo. Na comunicação entre o cliente e o servidor utiliza-se mensagens *Remote Procedure Calls* (RPC), encapsuladas num protocolo de transporte.

A camada de transporte é responsável pela autenticação, integridade e confidencialidade da ligação entre o cliente e o servidor, assim sendo definiu-se, quatro opções para o transporte de informação: o SSH na RFC 4742, IETF, (2006b), o BEEP na RFC 4744, IETF, (2006c), o SOAP na RFC 4743, IETF, (2006d) e o TLS na RFC 5539, IETF, (2009e).

Na camada de operações são definidas operações que podem ser requisitadas pelo cliente ao servidor, estas operações permitem criar, alterar, copiar, eliminar configurações e observar o estado de um equipamento. As operações do NETCONF definidas na RFC 4741 e na RFC 5277 podem ser observadas na tabela 1.

Operações	Descrição
get	Esta operação devolve a "*running config*" e a informação de estado do servidor.
get-config	Devolve a "*running config*" e a informação de estado do servidor.
edit-config	Permite editar ou criar, caso não exista, uma configuração. Esta alteração pode ser definida nó a nó, mediante a especificação de um atributo "*operation*" diferente em cada nó, a operação por omissão é sempre a "*merge*".
copy-config	Copia uma configuração inteira para outra. Caso o objeto de destino não exista, ele é criado.
delete-config	Apaga uma configuração. A configuração "*running*" não pode ser apagada.
lock	Permite que um cliente bloqueie o acesso a uma configuração. Durante este bloqueio a configuração pode ser livremente alterada sem influenciar ou ser influenciada pela interação de outros clientes. O bloqueio termina quando explicitado pelo cliente ou terminar a sessão com o mesmo.
unlock	Desbloqueia o acesso a uma configuração.
close-session	Pede para terminar a sessão com um servidor. O servidor liberta todos os *locks* e recursos alocados nesta sessão e termina a ligação.
kill-session	É forçado o fim de uma sessão NETCONF com o servidor. As operações desta sessão são abortadas e todos os recursos são desbloqueados.

Tabela 1 – Operações do NETCONF

Adaptado de: *NETCONF Configuration Protocol* (RFC 4741, 2006)

2.5. *CPE WAN Management Protocol (CWMP)*

TR-069 abreviatura de *Technical Report 0-69* é uma especificação técnica de fórum DSL que posteriormente foi renomeado como *Broadband Forum* intitulada como CPE WAN *Management Protocol* (CWMP). Definido pelo Broadband-Forum, (2013a), é um protocolo da camada de aplicação para gestão remota de dispositivos terminais do cliente.

O mesmo protocolo tem como objetivo fornecer uma infraestrutura para uma correta e segura gestão remota de CPE compatível com o protocolo CWMP, através de um ACS. Portanto, é detalhado neste relatório técnico todos os parâmetros a fim de proporcionar interoperabilidade entre qualquer ACS e CPE independentemente do fabricante.

Por meio deste protocolo, os ISP tem a capacidade de gerir todos os equipamentos terminais do cliente através da internet. Como um protocolo da camada de aplicação e que permite comunicação bidirecional entre um determinado equipamento e a entidade gestora. Essa comunicação é feita de uma forma segura e é baseada em mensagens SOAP (*Simple Object Access Protocol*) W3C, (2007), sobre o protocolo HTTP (*HyperText Transfer Protocol*) na RFC 7230 IETF, (2014).

O CWMP foi publicado em Maio de 2004 no relatório técnico 69 do *DSL Forum*, atual *BroadBand Forum*, com alterações em 2006, 2007, 2010, julho de 2011 para a versão 1.3 e Novembro de 2013 para a versão 1.4 (AM5).

2.5.1. *BroadBand Forum*

O *BroadBand Forum* é um consórcio composto por mais de 200 empresas que atuam na indústria das telecomunicações, computação, redes e empresas provedoras de serviço. Foi fundada em 1994 com o nome de *ADSL Forum* e mais tarde *DSL Forum*, Em 17 de junho de 2008, mudou-se o nome para o então " *BroadBand Forum*".

Em 18 de maio de 2009 conseguiu uma parceria com o *IP/MPLS Forum*, organização internacional do qual são membros organizações como, provedores de serviços, fabricantes de equipamentos, centro de testes e utilizadores empresariais. A partir dessa união o *BroadBand Forum* tornou-se o órgão central para especificações da próxima geração de redes IP.

Desde 1994 o *BroadBand Forum* desenvolveu mais de 100 especificações baseadas na definição da tecnologia DSL (*Digital Subscriber Line*) para prover mais eficiência de gestão da banda larga. Vale realçar que o nome de todas as formas da tecnologia DSL foi alterado para *DSL Forum* em 1999.

Nos últimos anos, o *BroadBand Forum* teve como foco de trabalho o desenvolvimento da arquitetura da fibra ótica e em garantir que as organizações provedoras de serviço fossem capazes de gerir as suas próprias redes através de uma plataforma de endereçamento de IP.

Em 2005, criou-se o *BroadBand Suite*, que por sua vez ordenou em grupo um conjunto de soluções técnicas de transporte, gestão da rede digital e apoio ao cliente. Algumas especificações de rede desenvolvidas consiste em: solução para tecnologia ADSL, SHDSL e ADSL2/2*plus* e VDSL2. Independentemente dos trabalhos desenvolvidos sobre a tecnologia DSL, tem igualmente desenvolvido trabalhos envolvendo outras tecnologias como, PON, EPON e desenvolvimento de normas *Ethernet* ponto a ponto.

Também Faz parte das preocupações do *BroadBand Forum* a eficiência energética, tencionando propor medidas que permitam a adesão de indústrias aos acordos mundiais de redução de energia.

O trabalho desenvolvido abrange igualmente especificações relativas à configuração de redes, sistemas de controlo de acesso e sistemas de suporte a operações. Estas configurações correspondem ao conjunto de práticas corretas para resolver problemas em banda larga,

envolvendo mecanismos de controlo de *frames* e fornecendo mecanismos de controlo direcionados a provedores remotos de linhas fixas.

O crescimento do protocolo de gestão remota CWMP, destaca-se como um feito histórico do *BroadBand Forum* e principalmente pelo facto de se tornar o protocolo standard para a gestão remota de dispositivos. A capacidade que o mesmo ostenta para adicionar modelos de objetos a novos dispositivos contribui de forma significativa para que os provedores de serviço sejam capazes de manter permanentemente atualizados serviços e aplicações nos dispositivos.

2.5.2. Descrição CWMP (TR-069)

O propósito de desenvolvimento do protocolo CWMP consistiu em conceber um standard de gestão de equipamentos. Por meio desta plataforma de gestão provedores de serviço são capazes de gerir todos os dispositivos com suporte ao protocolo CWMP através da internet, independentemente do fabricante do dispositivo. Até antes da existência do protocolo CWMP nunca tinha existido uma plataforma de gestão de equipamentos igual, pelo simples facto dos fabricantes de dispositivos desenvolverem formas próprias de configuração e não partilharem com os concorrentes.

Conforme descrito anteriormente o CWMP é um o protocolo da camada de aplicação que proporciona comunicação bidirecional entre determinado equipamento que se pretenda configurar e a respetiva entidade de gestão, Broadband-Forum, (2013a). A comunicação é baseada em mensagens SOAP sobre HTTPS, que por sua vez, proporciona comunicação e configuração de equipamentos de forma segura. A concessão deste standard aparece como solução às dificuldades outrora registadas na configuração dos equipamentos do cliente.

O CWMP é utilizado para gestão remota e configuração de dispositivos terminais do cliente tais como, modems, routers, *gateways*, STB, telefones VoIP etc. vale recordar que maior parte destes dispositivos são *gateways* residenciais, em certas ocasiões pode ser utilizado para a gestão de equipamentos que não o suportam, pelo facto de ser capaz de integrar com a tecnologia UPnP, constituindo-se capaz de alcançar uma infinidade de dispositivos na rede do cliente.

Quando se utiliza o protocolo CWMP, o elemento responsável pela gestão dos equipamentos CPE é o ACS que terá duas interfaces de comunicação distintas conforme ilustra a figura 4.

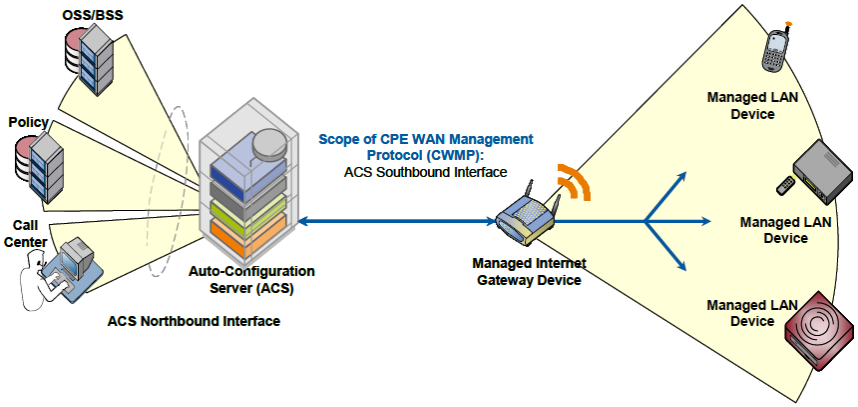

Figura 4- Posicionando na arquitetura *End-to-End*

Fonte: *TR-069 CPE WAN Management Protocol, Version: 1.4* (Broadband-Forum, 2013a)

A figura 4 ilustra duas principais interfaces em que uma refere-se a informação trocada com o fornecedor de serviço, e a outra interface diz respeito à comunicação deste servidor com os dispositivos CWMP.

O protocolo CWMP apresenta inúmeras vantagens em relação aos outros protocolos de gestão remota, tais como SNMP ou NETCONF, pelo que, utiliza o TCP como protocolo de transporte em vez de UDP usados no SNMP, aumentando assim a fiabilidade que constitui uma particularidade muito importante num protocolo de configuração. Outro atributo relevante do CWMP é o facto de não utilizar ligações TCP persistentes entre a aplicação gestora e o equipamento, permitindo assim que o ACS seja capaz de gerir um grande número de CPE em simultâneo, diferentemente de algumas implementações de NetConf, que precisam manter a sua ligação de gestão sempre aberta com o dispositivo que está a operar.

Se comparado ao NetConf verifica-se que o CWMP é muito mais flexível pelo facto de existir extensões que o fazem compatível com tecnologias modernas tais como UPnP, podendo assim alcançar dispositivos das LAN e dispositivos que não suportam o mesmo protocolo. No que concerne a flexibilidade e operacionalidade o CWMP agrega instrumentos que permitem ao ACS e ao CPE que sejam capazes de iniciarem o estabelecimento de sessões CWMP.

O CWMP foi igualmente concebido a fim de prover elevado grau de segurança e impossibilitar o manuseio não autorizado das operações realizadas entre um CPE e o ACS, bem como oferece mecanismos que garantem confidencialidade para essas operações e permite igualmente diversos níveis de autenticação.

2.5.3. Funcionalidades e Componentes

De acordo com, Broadband-Forum, (2013a) O CWMP tem como finalidade dar suporte a um vasto conjunto de funcionalidades de gestão de CPE, bem como o seguinte conjunto de recursos primários:

- Autoconfiguração e provisionamento dinâmico de serviço;
- Atualização de Software / *firmware*;
- Gestão de módulos de software;
- Monitoramento de *status* e desempenho;
- Diagnóstico;

2.5.3.1. Auto-Configuração e Provisionamento Dinâmico de Serviço.

O CWMP permite a um ACS provisionar um CPE ou a um conjunto de CPE baseando-se em uma variedade de critérios.

O mecanismo de provisionamento permite provisionar o CPE no instante da ligação à rede de acesso à banda larga, e a capacidade de reconfigurar-se em qualquer ocasião posterior.

Os mecanismos de identificação incluídos no protocolo permite provisionar o CPE com base nos requisitos específicos de cada CPE, ou em atributos coletivos, tais como o fornecedor do CPE, modelo, versão do software, etc.

O protocolo também fornece ferramentas opcionais de gestão de componentes específicos do CPE de aplicativos ou serviços opcionais para o qual é exigido um nível adicional de segurança, tais como os que envolvem pagamentos, Broadband-Forum, (2011a).

2.5.3.2. Software / *Firmware* de Gestão de Imagem

Fornece ferramentas de gestão de download do software do CPE bem como a atualização de ficheiros de *firmware*. Coloca ainda ao nosso dispor mecanismos para identificação da versão, iniciação do download, e notificação acerca do sucesso ou falha de download.

Quando o Download é iniciado pelo ACS, o ACS fornece ao CPE a localização do arquivo a ser transferido. O CPE, em seguida, efetua a transferência, e notifica o ACS.

No entanto estas transferências podem ser opcionalmente iniciadas pelo próprio CPE.

Nesse caso, o CPE envia um pedido de download de um determinado tipo de arquivo ao ACS. O ACS responde iniciando o download seguindo os mesmos passos como se fosse o ACS a fazer o download.

2.5.3.3. Gestão de Módulos de Software

Permite que o ACS seja capaz de gerir ambientes de software e executar módulos do CPE. Recursos fornecidos incluem, a possibilidade de instalar, atualizar e desinstalar módulos de software, bem como notificação para o ACS de sucesso ou falha de cada ação. Fornece igualmente suporte para os módulos de software disponíveis no dispositivo afim de, iniciar e parar aplicações no CPE, ativar e desativar ambientes de execução.

2.5.3.4. Monitoramento de *Status* e Desempenho

Proporciona suporte ao CPE de forma a tornar disponível informação com a qual o ACS poderá usar para monitorar o estado e performance do CPE. Também define um conjunto de mecanismos que permite que o CPE notifique o ACS de alterações no seu estado.

2.5.3.5. Diagnóstico

Promove suporte ao CPE de forma a tornar disponível informação com a qual o ACS poderá usar para diagnosticar e resolver problemas de ligação ou serviços, bem como a habilidade de executar definidos testes de diagnóstico.

2.5.4. Arquitetura

O protocolo CWMP contém componentes exclusivos, no entanto o seu funcionamento baseia-se no uso de diversos protocolos padrão. A pilha de protocolo definido pelo CWMP é ilustrada na Figura 5, seguido de uma breve descrição de cada camada na Tabela 2.

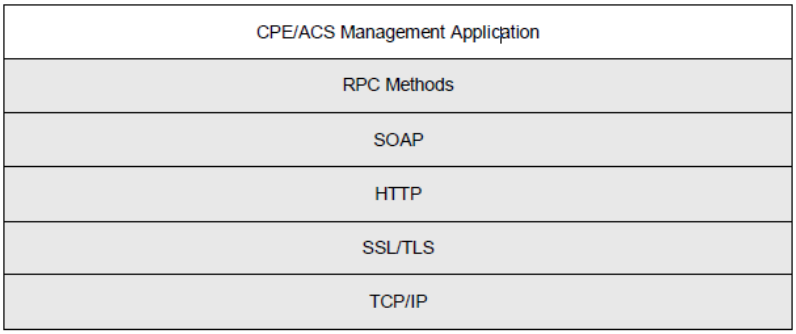

Figura 5- A pilha de protocolo CWMP

Fonte: *TR-069 CPE WAN Management Protocol, Version: 1.4* (Broadband-Forum, 2013a)

Camada	Descrição
CPE/ACS *Application*	Aplicações CWMP usadas nas entidades CPE e ACS. A aplicação é localmente definida e não faz parte do CPE WAN *Management Protocol.*
RPC *Methods*	Métodos RPC especificados na norma do CPE WAN *Management Protocol.*
SOAP	Uma norma baseada em sintaxe XML utilizada para codificar RPC *Methods*. Especificamente SOAP 1.1.
HTTP	HTTP 1.1.
TLS	Padrão do *Internet Transport Layer Security Protocols*. Especificamente, SSL 3.0 (Secure Socket Layer) ou TLS 1.0 (*Transport Layer Security*).
TCP/IP	Padrão TCP/IP.

Tabela 2 – Camadas de protocolo do protocolo CWMP

Adaptado de: *TR-069 CPE WAN Management Protocol, Version: 1.4*. (Broadband-Forum, 2013a)

2.5.4.1.Mecanismos de segurança

O uso de TLS para transporte do CWMP é recomendado, embora o protocolo pode ser utilizado diretamente sobre uma ligação TCP. Se o TLS não for utilizado, alguns aspetos da segurança serão sacrificados. TLS fornece confidencialidade e integridade dos dados e permite autenticação em ambos os terminais.

Determinadas restrições sobre a utilização de TLS e TCP são definidas na norma do CWMP. O funcionamento básico deste protocolo de configuração baseia-se em troca de mensagens SOAP transacionadas entre o CPE e o ACS através de HTTP 1.1, onde o CPE se comporta como cliente HTTP e o ACS como servidor HTTP. No entanto o protocolo contém também um mecanismo de pedidos de ligação que permite ao ACS comportar-se como cliente e o CPE por sua vez como servidor.

As operações e informações CWMP enviadas nas mensagens SOAP são emitidas em formato textual e codificadas na linguagem de transporte XML. Um ACS é capaz de configurar e monitorar um CPE através de uma série de métodos RPC (*Get, Set, Inform*, Download, Upload, *Reboot* entre outros) disponibilizados pelo protocolo.

Este protocolo possibilita que programadores com base em ferramentas de desenvolvimento, construam de uma forma aberta aplicações de configuração seguras, dinâmicas e escaláveis.

2.5.4.2.*Technical Reports*

O CWMP define o modelo de dados e comunicação através dos quais um ACS é capaz de ler, alterar ou mesmo excluir parâmetros internos dos equipamentos, atribuindo-lhe assim capacidades tais como configuração, monitorização, edição e adição fácil de novos serviços aos equipamentos. Parâmetros de diferentes tipos de CPE são definidos em documentos separados.

- TR-098: Modelo de dados para dispositivos TR-069;
- TR-104: Parâmetro de provisionamento para VoIP CPE;
- TR-135: Modelo de dados para TR-069 STB ativo;
- TR-140: TR-069 modelo de dados para o serviço de armazenamento de dispositivos ativos;
- TR-143: Rede de testes de desempenho *throughput* e monitoramento estatístico;
- TR-157: Componente de objetos CWMP;
- TR-181: Modelo de dados para dispositivo TR-069;
- TR-196: Modelo de dados para serviço de pontos de acesso;

Cada parâmetro consiste num par nome/valor. O nome identifica um determinado parâmetro, e possui uma estrutura hierárquica semelhante há arquivos num diretório, com cada nível separados por um ponto (.). O valor de um parâmetro pode ser uma definição de diversos tipos de dados. Os parâmetros podem ser definidos como de leitura ou leitura e escrita. Parâmetros só de leitura podem ser utilizados pelo ACS para determinar características específicas do funcionamento de determinado CPE, observar o seu estado atual ou reunir dados estatísticos.

Parâmetros que possibilitem leitura e escrita permitem que um ACS seja capaz de personalizar vários aspetos do funcionamento do CPE de forma a melhorar e corrigir o seu desempenho.

Apesar de certos parâmetros serem passíveis a alteração, contém informação confidencial (por exemplo passwords de determinado utilizador); nessas situações, caso seja pretendida a leitura desses valores, será retornado um valor vazio.

2.5.4.3.Sessões Iniciadas Pelo CPE

O CWMP tem definido mecanismos que permitem que o CPE se conecte ao ACS em diversas condições, garantindo assim que a comunicação CPE–ACS ocorra com alguma frequência mínima.

Conhecendo previamente o endereço do ACS, o CPE poderá a qualquer momento estabelecer sessão com o ACS, essa sessão entre os dois terminais é iniciada após o CPE enviar

ao ACS uma mensagem *Inform* num POST HTTP. Este *Inform* trata-se de um método RPC invocado pelo CPE e executado no ACS, e é utilizado para estabelecer as sessões de transação entre CPE e ACS. A invocação deste método contém informação relevante acerca do equipamento e informa o ACS das razões pela qual ele pretende estabelecer sessão.

O CPE inicia a comunicação com o ACS em diversas situações tais como o momento em que é ligado à rede após a sua instalação inicial, sempre que seja ligado ou reiniciado ou mesmo quando ocorrem eventos que devam ser comunicados ao ACS (como por exemplo quando o endereço IP do CPE é alterado). Além destas condições é ainda definido no CPE um período de tempo no qual estabelece comunicação periódica com o ACS sobre uma base de tempo contínua. Caso a mensagem de *Inform* se trate de uma invocação periódica deste método, a mensagem SOAP deverá indicar na estrutura de eventos a ocorrência do evento PERIODIC.

Este protocolo contém, no entanto, um mecanismo que permite estabelecimento assíncrono de sessões. Cada CPE CWMP possui um serviço HTTP suportando autenticação do tipo *digest* no qual o ACS poderá atuar como cliente HTTP, podendo assim informar o CPE de que se pretende comunicar com ele. Uma vez que o CPE receba um pedido de ligação enviado pelo ACS, irá responder nos próximos 30 segundos com a invocação do método *Inform*, indicando a ocorrência do evento de *Connection Request*.

Em cada caso, quando a comunicação é estabelecida o CPE identifica-se exclusivamente através da informação de fabrico (*serial number*), de modo ao ACS conhecer o CPE com quem se esta a comunicar e possa responder de forma correta.

2.5.4.4.Modelo de Comunicação

A comunicação estabelecida pelo protocolo CWMP corresponde a uma troca bidirecional de pedidos e respostas RPC. Esta transação é concluída quando ambos os terminais não tem mais mensagens para enviar. O CPE é responsável por estabelecer e terminar as sessões CWMP.

De modo a possibilitar uma troca sequencial de operações numa única sessão, o CPE deverá manter a ligação TCP durante toda sessão.

A figura 6 contém um exemplo de uma transação entre CPE e o ACS e demonstra o fluxo da comunicação e como a mesma ocorre em ambos os sentidos. Neste exemplo o ACS invoca no CPE os métodos *GetParameterValues e SetParameterValues*, e recebe do CPE as respostas das invocações desses métodos.

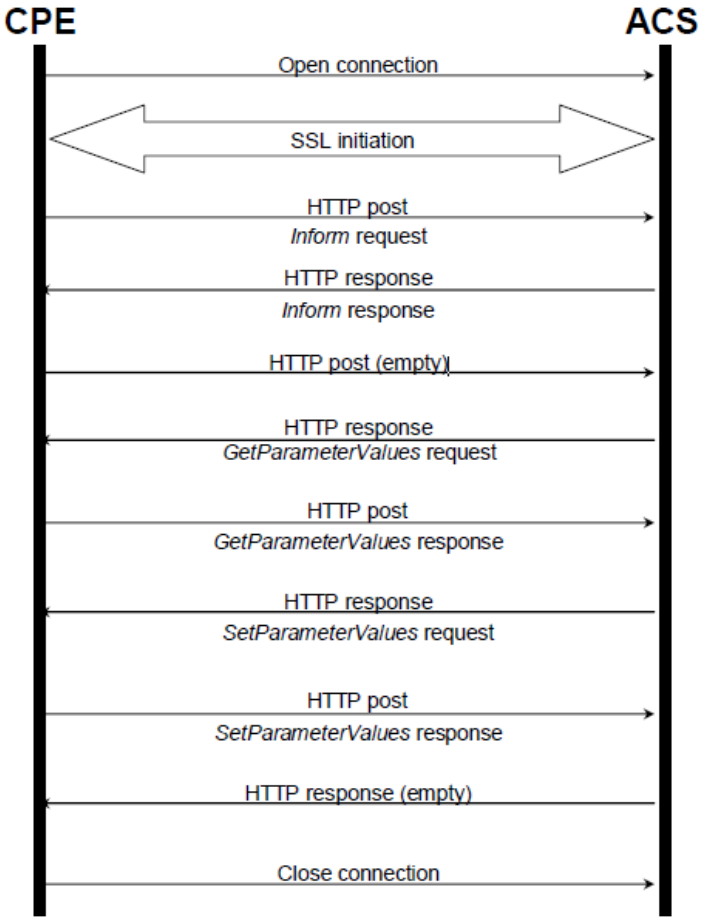

Figura 6- Modelo de comunicação do protocolo CWMP

Fonte: *TR-069 CPE WAN Management Protocol, Version: 1.4* (Broadband-Forum, 2013a)

Pode-se tirar a seguinte interpretação da figura 6:

- A sessão inicia com o estabelecimento da ligação TCP;
- Estabelecimento e ativação de SSL e respetiva ativação do mecanismo de segurança;
- Neste momento o CPE envia um POST HTTP invocando o método *Inform* para inicializar a transação de operações com o ACS;
- O ACS responde com *InformResponse*, indicando ao CPE de que o *Inform* enviado foi recebido com sucesso e que o CPE foi autenticado com sucesso;
- No seguimento da chegada do *InformResponse* o CPE entrega ao ACS um POST HTTP vazio indicando que a sessão foi estabelecida com sucesso e que esta pronto a receber pedidos de invocação de métodos RPC;

- Em resposta ao POST vazio, o ACS responde invocando no CPE uma operação, sendo neste caso do exemplo apresentado na imagem, um *GetParameterValues*;
- O CPE responde num novo POST com o *GetParameterValuesResponse* retornando o resultado à invocação do referido método;
- O ACS opta por invocar nova operação, desta feita um *SetParameterValues*;
- O CPE retorna o resultado dessa operação no *SetParameterValuesResponse*;
- O ACS envia uma mensagem vazia ao equipamento informando que não pretende invocar mais operações;
- O CPE termina a sessão e de seguida irá iniciar uma ligação do tipo *standby* podendo vir a ser aproveitada novamente pelo ACS assim que pretenda.

2.5.5. Métodos RPC

O CWMP utiliza um mecanismo bidirecional de chamada de procedimentos remotos (RPC) que permite que uma aplicação utilize serviços de uma outra aplicação a correr numa máquina remota. A aplicação que invoca a execução dos procedimentos envia mensagens contendo indicação do procedimento a executar e os dados necessários para a execução remota do programa. Uma vez executados, os respetivos resultados serão enviados à aplicação que fez a chamada dos procedimentos.

O equipamento CPE deverá suportar uma série de métodos RPC, que poderão ser invocados pelo ACS, por outro lado o próprio CPE poderá invocar chamadas de procedimentos no ACS.

Na tabela 3 estão listados os métodos requeridos e opcionais existentes em ambos os lados, conforme é especificado na norma TR-069.

Method name	CPE requirement	ACS requirement
CPE methods	Responding	Calling
GetRPCMethods	REQUIRED	OPTIONAL
SetParameterValues	REQUIRED	REQUIRED
GetParameterValues	REQUIRED	REQUIRED
GetParameterNames	REQUIRED	REQUIRED
SetParameterAttributes	REQUIRED	OPTIONAL
GetParameterAttributes	REQUIRED	OPTIONAL
AddObject	REQUIRED	OPTIONAL
DeleteObject	REQUIRED	OPTIONAL
Reboot	REQUIRED	OPTIONAL
Download	REQUIRED[7]	REQUIRED[7]
ScheduleDownload	OPTIONAL	OPTIONAL
Upload	OPTIONAL	OPTIONAL
FactoryReset	OPTIONAL	OPTIONAL
GetQueuedTransfers **(DEPRECATED)**	OPTIONAL[8]	OPTIONAL
GetAllQueuedTransfers	OPTIONAL	OPTIONAL
CancelTransfer	OPTIONAL	OPTIONAL
ScheduleInform	OPTIONAL	OPTIONAL
ChangeDUState	OPTIONAL	OPTIONAL
SetVouchers **(DEPRECATED)**	OPTIONAL[9]	OPTIONAL
GetOptions **(DEPRECATED)**	OPTIONAL[9]	OPTIONAL
ACS methods	Calling	Responding
GetRPCMethods	OPTIONAL	REQUIRED
Inform	REQUIRED	REQUIRED
TransferComplete	REQUIRED[10]	REQUIRED[11]
AutonomousTransferComplete	OPTIONAL	REQUIRED
DUStateChangeComplete	OPTIONAL[12]	OPTIONAL[13]
AutonomousDUStateChangeComplete	OPTIONAL	OPTIONAL
RequestDownload	OPTIONAL	OPTIONAL
Kicked **(DEPRECATED)**	OPTIONAL	OPTIONAL[14]

Tabela 3 – Métodos RPC

Fonte: *TR-069 CPE WAN Management Protocol, Version: 1.4.* (Broadband-Forum, 2013a)

A tabela 3 mostra o conjunto de métodos RPC que o CPE deverá suportar e que poderão ser invocados pelo ACS, por outro lado o CPE deve ter a capacidade de invocar as chamadas de procedimentos no ACS.

2.5.6. Métodos CPE

A invocação destes métodos será unicamente da responsabilidade do ACS. Contudo existe a exceção do método de *Reboot*, no qual, o próprio equipamento poderá em situações pontuais decidir iniciar a execução própria desse método. Os seguintes métodos correspondem as principais operações que podem ser executadas em equipamentos CWMP.

***GetRPCMethods*:** Este método será utilizado para conhecer o conjunto de métodos suportados pelo CPE. A invocação deste método não terá qualquer tipo de argumentos e a resposta à sua invocação será uma lista dos nomes dos métodos que o CPE incorpora.

***SetParameterValues*:** Este método deverá ser chamado pelo ACS de modo a modificar o valor de um ou mais parâmetros do CPE. A invocação deste método necessita ter como parâmetros de entrada uma lista de pares nome – valor, onde o nome corresponderá ao nome do parâmetro e o valor será o valor que se pretende atribuir ao parâmetro. A resposta a invocação deste método informa se todos os parâmetros foram validados e aplicados com sucesso ou todos os parâmetros foram validados mas alguns ainda não aplicados.

***GetParameterValues*:** Este método deverá ser chamado pelo ACS de modo a obter o valor de um ou mais parâmetros do CPE. A invocação deste método necessita ter como parâmetros de entrada uma lista com os nomes dos parâmetros que pretendemos conhecer. A resposta à sua invocação será uma lista de pares nome – valor contendo o nome e o respetivo valor do parâmetro**.**

***GetParameterNames*:** Este método deverá ser chamado pelo ACS de modo a obter os parâmetros acessíveis em determinado CPE. A invocação deste método necessita ter como parâmetros de entrada um apontador e um booleano. O apontador apontará para um nó da hierarquia de parâmetros, correspondendo assim ao diretório completo de um parâmetro ou uma parte parcial desse diretório.

***SetParameterAttributes*:** Este método pode ser utilizado por um ACS para modificar os atributos associados com um ou mais Parâmetro do CPE.

***GetParameterAttributes*:** Este método pode ser utilizado por um ACS para ler os atributos associados com um ou mais Parâmetros do CPE.

***AddObject*:** Este método pode ser usado pelo ACS para criar uma nova instância de um objeto de multi-instância. A chamada do método toma como argumento o nome do caminho da coleção de objetos para os quais uma nova instância será criada.

***DeleteObject*:** Este método é usado para remover uma instância específica de um objeto. Esta chamada de método toma como argumento o nome de caminho da instância do objeto, incluindo o identificador de instância.

***Reboot*:** Este método faz com que o CPE se reinicie. A invocação deste método é mais destinada a ser feita do lado do CPE do que ACS, visto ser rara a situação em que após uma alteração da configuração do CPE, seja necessário efetuar um *reboot* ao equipamento, e quando isso acontece o próprio CPE deverá executar o seu próprio *reboot*. Contudo opcionalmente poderá também ser implementado do lado do ACS.

O uso do método no entanto é bastante simples, unicamente é usado um parâmetro vazio na sua invocação, sendo a resposta também vazia.

Download: Este método deverá ser usado pelo ACS para fazer com que o CPE inicie determinado download a partir de um URL designado pelo ACS. Para a invocação deste método são necessários bastantes mais parâmetros comparativamente aos outros métodos ate aqui falados, fazendo dele, um dos métodos mais complexos do CWMP. De entre todos esses parâmetros convêm salientar os mais importantes, tais como uma indicação do tipo de download que pretendemos que o CPE efetue (*Firmware Upgrade Image, Web Content ou Vendor Configuration File*). Uma indicação do URL onde se encontra localizado o ficheiro. Dados de utilizador e palavra-chave, necessários para autenticação no servidor onde se encontra o ficheiro (caso não seja necessária autenticação, estes dados deverão ser vazios). Deverá ser ainda especificado o nome e tamanho do ficheiro em bytes.

***FactoryReset*:** Este método repõe a configuração do equipamento no estado em que foi definido pelo fabricante.

2.5.7. Métodos ACS

A invocação destes métodos será unicamente da responsabilidade dos CPE. Os seguintes métodos correspondem as principais operações que podem ser invocadas num ACS.

GetRPCMethods: Este método será utilizado para conhecer o conjunto de métodos suportados pelo ACS. A invocação deste método não terá qualquer tipo de argumentos e a resposta à sua invocação será uma lista dos nomes dos métodos que o ACS incorpora.

Inform: O CPE deverá chamar este método para iniciar a sequência de transação sempre que seja necessário estabelecer sessão com o ACS.

A mensagem de *inform* deverá conter diversa informação tal como: Identificação do equipamento (*Organizationally Unique Identifier, Serial Number, Manufacturer, ProductClass*), listagem dos eventos ocorridos no equipamento durante o período de tempo compreendido entre o último *inform* e este. A data e hora atual, e ainda alguma informação de configuração do equipamento.

TransferComplete: O CPE invoca este método de forma a informar o ACS que foi concluída uma transferência de um download ou upload anteriormente inicializado após a invocação do método de Download ou Upload.

A mensagem de *TransferComplete* conterá no seu conteúdo, indicação de sucesso ou falha de determinada ação e respetivos instantes de início e finalização da ação.

3. Caracterização da Organização

Com mais de 800 colaboradores, a Altran Portugal, é hoje um dos principais *players* na consultoria de inovação tecnológica em Portugal. Está presente nos vários setores de atividade como o financeiro, telecomunicações e media, administração pública, indústria e *utilities* a atividade da Altran estrutura-se na venda de soluções inovadoras.

Com um modelo de negócio diferenciado, a oferta da Altran está estruturada em quatro linhas de negócio:

- *Intelligent Systems.*
- *Information Systems.*
- *Lifecycle Experience.*
- *Mechanical Engineering.*

A Figura 7 ilustra a localização geográfica da sede da empresa Altran Portugal em Lisboa, sendo circundado pelos municípios do Oeiras, Amadora e Loures.

Figura 7- Localização geográfica da sede da empresa Altran Portugal

3.1. Morada

As instalações dos serviços estão divididas por cerca de 4 edifícios, nas seguintes moradas:

- Antiga sede, morada: Av. das Forças Armadas, 125 - 3º (Edifício Open) 1600-079 Lisboa.
- Morada Fundão: Centro de Negócios e Serviços, Praça Amália Rodrigues 6230-350 Fundão.
- Morada Porto: UPTECH, Edifício Central, Rua Alfredo Allen, n.º455/4614200-135 Porto.

Com o objetivo de permitir expandir o negócio integrado num empreendimento empresarial, como claras vantagens em termos de custos, de acessibilidades, de conforto, de comodidade e de proximidade com todo o tipo de serviços, a fim de representar para todos uma mais-valia e uma melhoria das condições de trabalho, no dia 01 de junho de 2015, a sede da Altran mudou de instalações para um novo espaço com a seguinte morada:

Atual sede, morada: Edifício Expo 98, Av. D. João II Lote 1.07.2.1 – 1998-014 Lisboa.

Na figura 8 pode ser vista a parte exterior do edifício das novas instalações da Altran Portugal.

Figura 8- Localização da atual sede da Altran Portugal

3.2. Localização das Instalações

Nas imagens seguintes pode ser vista a localização do edifício da Altran Portugal, com destaque para a Figura 9, onde se pode ver a localização do edifício sede.

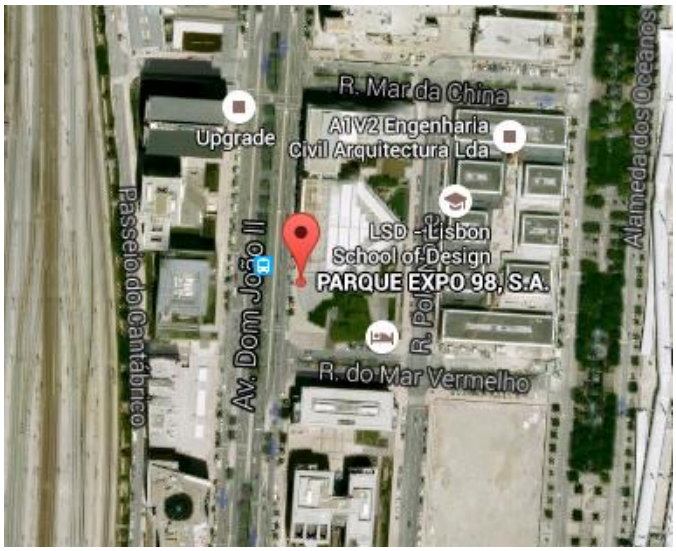

Figura 9- Localização do edifício sede

A figura anterior mostra o edifício localizado numa zona urbana e consolidada, sendo que na Figura 10 estão assinaladas as localizações geográficas dos restantes edifícios, onde para uma melhor sistematização do conhecimento produziu-se o mapa respetivo.

Figura 10- Localização das instalações da Altran em Portugal

Adaptado de: Site da Altran Portugal (Altran, 2015)

Na Figura 10 podemos ver que existem dois edifícios localizados em Lisboa, um no Fundão e o último no Porto, de acordo a história da Altram Portugal podemos afirmar que a mesma encontra-se em expansão.

3.3. Missão

A missão da Altran é trabalhar lado a lado com aqueles que mobilizam a sua criatividade todos os dias para criar soluções inovadoras a nível mundial.

Este compromisso dá à Altran o seu propósito tal como aos seus colaboradores, que desenvolvam os seus talentos e potencialidades ao máximo.

A ambição da Altran é ser líder mundial na área de inovação e desenvolvimento de tecnologia, capaz de fornecer aos seus clientes as melhores soluções face aos desafios e problemas mais complexos no seu setor de atividade.

Através da sua organização geográfica e setorial apoiam os seus clientes de qualquer parte do mundo com os seus melhores consultores nos seus projetos através do ciclo de inovação.

3.4. História

O grupo Altran, multinacional francesa já atua no mercado dedicado à inovação há 30 anos. Com mais de 20.000 colaboradores, 500 contas-chave a nível mundial e operacional em mais de 20 países.

Em Portugal o grupo está presente desde 1998, tendo-se consolidado a marca Altran em 2009. Há 14 anos que trabalham com os seus clientes concretizando projetos e respondendo aos desafios do mercado. Na figura 11 observa-se de forma resumida o trajeto da Altran Portugal.

Figura 11- História do grupo Altran em Portugal

Adaptado de: Site da Altran Portugal (Altran, 2015)

3.5. Atividades da Organização

A Altran está presente no mercado nacional há mais de 15 anos. De acordo com a Altran a sua equipa incorpora os melhores talentos e um vasto portfólio de soluções que suportam toda a cadeia de valor dos seus clientes de forma a ser um verdadeiro acelerador da inovação.

Como já referido anteriormente as atividades da Altran estão estruturadas em quatro linhas de negócio: *Intelligent Systems, Information Systems, Lifecycle Experience e Mechanical Engineering.*

3.5.1. Plataforma *Nearshore*

Nearshore é um tema ouvido cada vez mais no mundo empresarial, que se explica como sendo a transferência de processos de negócio e de projetos para empresas de países próximos. Os princípios desta abordagem passam pelo local de entrega comum, pela reutilização, pelos

processos padronizados e certificados, e sempre, pelo desenvolvimento de um plano de melhoria contínua.

Portugal, dada a sua localização estratégica, é um dos maiores centros de *nearshore* da Europa. Comparativamente com o resto da Europa, apresenta condições extremamente competitivas, que fazem de Portugal uma boa escolha para alocar determinados projetos, tais como:

- Melhoria de tempo de resposta (*time-to-market*);
- Redução de custos;
- Maior flexibilidade na gestão de capacidade;
- Serviços uniformizados;
- Capacidades linguísticas;
- Proximidade Europeia;

A Altran Portugal é o centro de competências *nearshore* para sistemas de informação do grupo Altran. Os objetivos desta plataforma Europeia de *Nearshore* passam por servir o mercado nacional e internacional. A Altran Portugal é capaz de fornecer um serviço uniforme de alta qualidade para garantir o sucesso do projeto. A Altran Portugal é a plataforma *nearshore* do grupo Altran, a figura 12 ilustra as principais atividades desenvolvidas na Plataforma *nearshore*.

Figura 12- Principais atividades da Altran

Fonte: Recursos Humanos (Altran, 2015)

3.6. Organograma

A figura 13 mostra a estrutura organizacional da Altran Portugal, que é composta por 3 unidades de negócio e 5 unidades do centro corporativo.

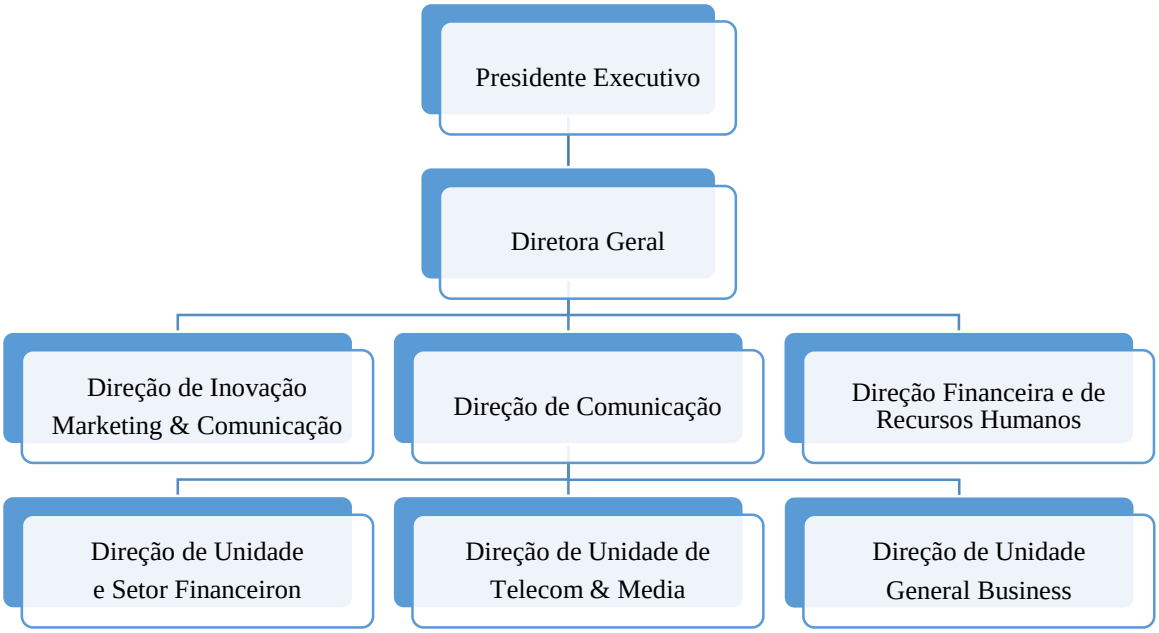

Figura 13- Organograma da Altran Portugal

Fonte: Recursos humanos (Altran, 2015)

3.7. Recursos Humanos

As mulheres e os homens da Altran são o mais rico recurso e fonte de orgulho. Por este motivo a empresa presta especial atenção ao recrutamento, à formação interna e ao desenvolvimento dos planos de carreira dos seus colaboradores.

A Altran terminou 2014 com cerca de 800 colaboradores ao seu serviço, distribuídos geograficamente pelos locais onde esta exerce a sua atividade, A Altran acordou com o governo de Portugal um novo investimento, de 12 milhões de euros, que vai permitir criar 200 novos postos de trabalho. Os novos empregos, diretos e qualificados, vão ser criados maioritariamente na região do Fundão, no âmbito do alargamento das atividades de *nearshore*.

O novo investimento foi anunciado dia 15 de Junho na inauguração oficial da nova sede, em Lisboa – no parque das nações, numa cerimónia que contou com a participação do Vice-Primeiro-Ministro, Paulo Portas.

3.7.1. Planos de Formação

Como já foi frisado acima a Altran investe continuamente na formação interna e ao desenvolvimento dos planos de carreira dos seus colaboradores, assim sendo sengue-se a estratégia do processo da formação:

- Capitalização do conhecimento e *know-how*.
    - Equipa formadores internos.
- Desenvolvimento de competências transversais -> *Impulse Program.*
    - Metodologias de trabalho, competências comportamentais (*soft skills*), e integração na organização.
- Desenvolvimento de competências técnicas específicas.
    - Carácter vertical focado em certa área técnica/funcional.
- Identificação antecipada de áreas estratégicas de formação para a empresa.
    - Constituem uma aposta em potenciais necessidades de negócio.

3.8. Caracterização dos Ativos, SI/ TIC

Neste subcapítulo procura-se fornecer uma perspetiva sucinta do ambiente empresarial interno ao nível das TIC, no sentido de percebermos a infraestrutura tecnológica da organização no seu todo que por sua vez é parte integrante no processo de execução de testes do protocolo CWMP em CPE.

3.8.1. Sistemas de Informação

Com o intuito de agilizar e tornar mais eficiente o processo tradicional de comunicação interna a estratégia da organização tem sido o desenvolvimento de aplicações Altran Portugal.

Estas aplicações permitem encontrar informações tais como: documentos, software, informação departamental, calendários de eventos, manuais de procedimentos, políticas internas, informações gerais e outras funcionalidades, nomeadamente acessos a links internos.

Assim sendo o conjunto de aplicações denominadas Altran Portugal são as seguintes:

- Portal do Colaborador Altran: este portal serve para consulta do recibo de vencimento e atualização do registo (Portal-Colaborador, 2015);

- Portal Hermes: este portal serve para registo de férias, despesas, registo de horas de trabalho e ainda acompanhar todo o processo de análise e aprovação dos teus registos (Hermes, 2015);
- E-mail Altran: plataforma de gestão de e-mails corporativo do grupo Altran Portugal, E-mail, (2015);
- DirectV2 (intranet): plataforma internacional do grupo, nela pode se consultar todos os protocolos disponíveis a nível mundial (Directv2, 2015);
- Portal da qualidade: acesso ao repositório de toda a documentação inerente ao SGI da Altran Portugal (Qualidade, 2015);
- MyCampus: esta plataforma é destinada para ajudar a componente de formação e-learning (Elearning, 2015);
- GCA: esta plataforma é destinada para a gestão de competências de consultores do grupo Altran Portugal (GCA, 2015).

3.8.2. Tecnologia de Informação e Comunicação

A organização dispõe de um *Data Center* em que a partir do mesmo derivam as ligações de distribuição das sub-redes, que ligam os vários departamentos, suportadas por *switch*, com PPPoE, PoE e o *Digital Subscriber Line Access Multiplexer* (DSLAM), com VDSL e ADSL. Também dispõe de um *Disaster Recovery Plan (DRP)* integrado no plano de continuidade de negócio da organização.

A comunicação no edifício é feita através das infraestruturas de rede local: *Local Area Network* (LAN), por cabo e sem fios, utilizada pelos diversos postos de trabalho do edifício. A comunicação com o exterior encontra-se protegida com Firewall e na comunicação das diferentes redes internas estão, naturalmente, os equipamentos de *switch* e routers, repetidores etc.

Os equipamentos especialmente portáteis podem ser configurados para acesso à organização pelo exterior, em qualquer local com ligação internet, através da infraestrutura de *Virtual Private Network* (VPN).

4. Descrição e Análise das Atividades Desenvolvidas

Este capítulo descreve os projetos que foram desenvolvidos na organização de acolhimento ao longo dos 9 meses de estágio curricular.

4.1. Descrição e Âmbito do Projeto

O projeto denominado teste CPE_Teste é um projeto de âmbito internacional que consiste na execução de testes em dispositivos de banda larga xDSL designadamente: modems/routers xDSL, mas também routers 3G/4G/LTE, assim como também software de banda larga para uso doméstico e de escritório e lançamentos de software para manutenção.

4.1.1. Âmbito do projeto

As atividades de testes devem ser geridas *on-site* por uma equipa de gestão de teste da Altran que irá combinar o desenho de testes, planeamento, execução, comunicação e coordenação global do projeto.

Os resultados que se esperam deste projeto são:

- Definição da estratégia de execução e requisitos de teste.
- Definição do plano de teste (casos de teste e cenários).
- A execução de teste deve ser feita usando a ferramenta *HP Quality Center*.
- O *Reporting* de teste deve ser feito usando a ferramenta *HP Quality Center*.

4.1.2. Áreas de Teste

O âmbito da área de teste descrita nesta seção foi definido tendo em conta:

- A experiência da Altran no fornecimento com sucesso deste tipo de serviço.

A tabela abaixo resume o âmbito da área de teste agrupados por tecnologia que Altran é capaz de executar.

Gestão CWMP	Boot Up; Políticas de upgrade, download, *provisioning*, verificação do modelo de dados, *Syslog*, NTP / SNTP, obtenção de dados etc.

Tabela 4 – Área de teste e tecnologia

Fonte: Laboratório de media (Altran, 2015)

4.2. Recursos Humanos

A equipa responsável pela execução do projeto é constituída por 5 elementos como se pode constatar na tabela 5.

Recursos				
Nome	Iniciais	Início	Fim	Função
		15-12-2014	31-12-2015	
Bernardo Costa	BS	15-12-2014	31-12-2015	Diretor do projeto
Paulo Marco	PM	15-12-2014	31-12-2015	Gestor de Projeto
Hernâni Pedro	HP	15-12-2014	31-12-2015	*Test Expert*
Alfredo Conceição	AC	15-12-2014	31-12-2015	*Tester*
Nando Braulio	NB	15-12-2014	31-12-2015	*Tester*

Tabela 5 – Recursos humanos do projeto

Fonte: Laboratório de media (Altran, 2015)

4.3. Planeamento

A execução do projeto teve início no dia 2 de março e terminou no dia 14 de setembro de 2015, mas de acordo com as necessidades do cliente em termos de âmbito de serviço o prazo poderá se alargar até dezembro de 2015.

	Março	Abril	Maio	Junho	Agosto	Setembro
	W1 -- W4	W1 -- W4	W1 -- W4	W1 -- W4	W1 -- W4	W1 -- W4
Gestão Operacional						
Gestão de Serviços						

Tabela 6 – Plano de execução do projeto

Fonte: Laboratório de media (Altran, 2015)

Na tabela 6 observa-se o plano de execução de teste de forma resumida que vai de março a setembro.

4.4. Gestão de Defeitos

Durante a fase de execução de testes podem ser detetadas falhas entre o requisito baseado no atual caso de teste e o resultado do caso de teste. A análise de defeito deve ser realizada mediante a utilização do processo denominado *Kepner-Tregoe*, que está representado na figura 14.

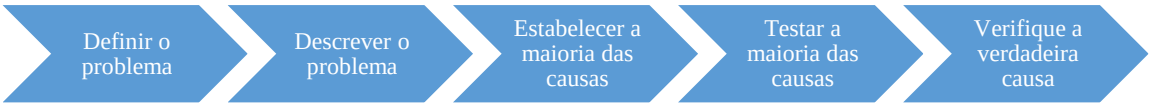

Figura 14- Gestão de defeito *Kepner Tregoe process*

Fonte: Laboratório de media (Altran, 2015)

A gestão de defeito será realizada através da ferramenta de gestão de defeito, *HP Quality Center*. Todas as questões identificadas na figura 15 devem ser preenchidas durante o registro de defeito.

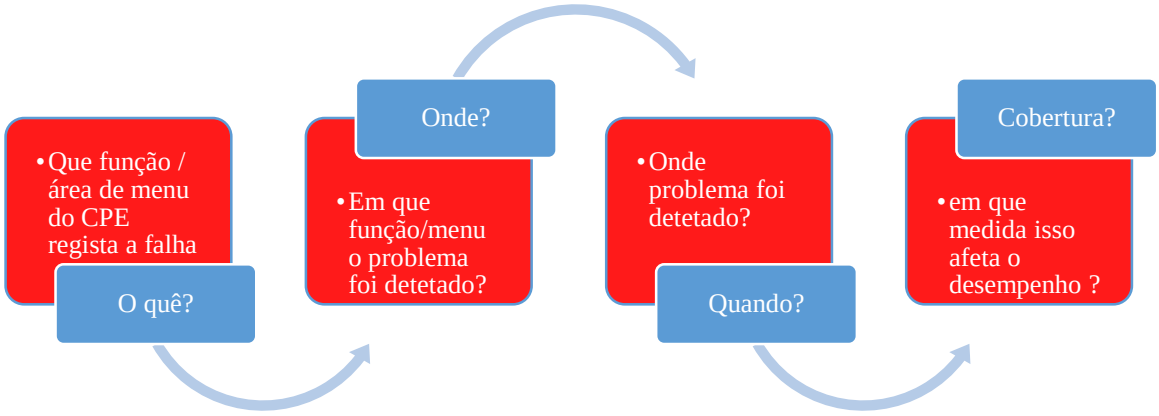

Figura 15- Registo de defeito

Fonte: Laboratório de media (Altran, 2015)

Todos os defeitos devem ser atribuídos um grau de severidade, conforme ilustra a Figura 16.

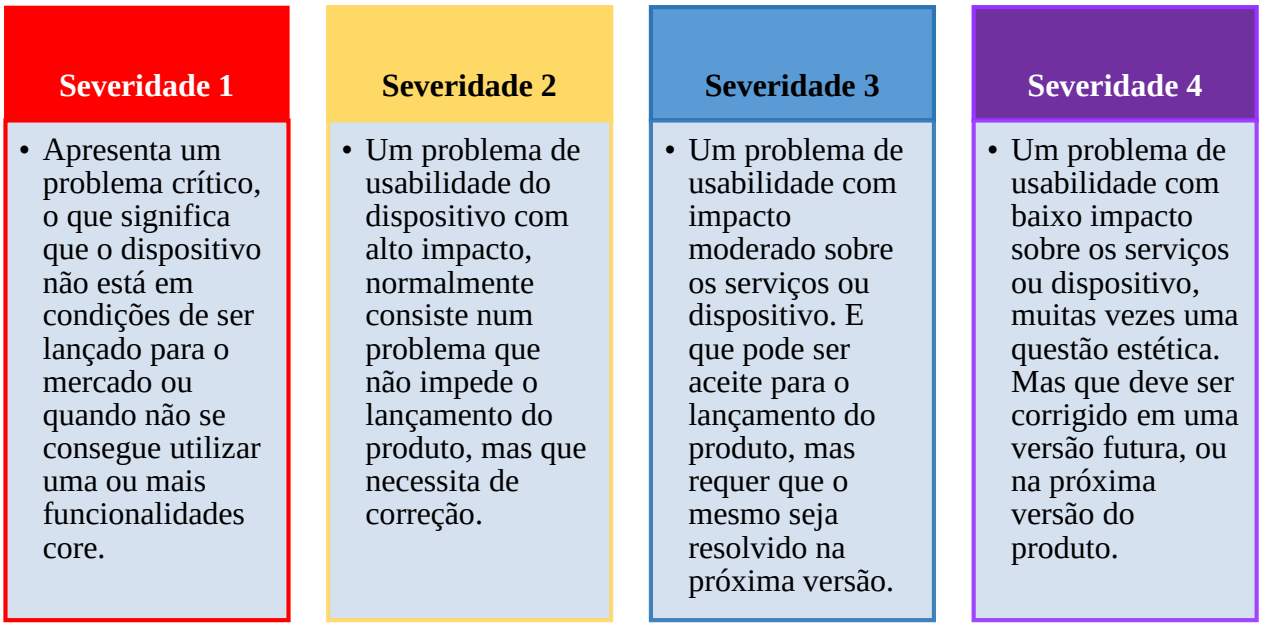

Figura 16- Grau de severidade

Fonte: Laboratório de media (Altran, 2015)

Obs: vale recordar que de acordo com os requisitos definidos para cada dispositivo a ser testado o resultado final de cada caso de teste pode ser: passou, falhou, limitação do design ou não aplicável, de acordo com estas especificações considera-se que um determinado caso de teste:

- Passou quando a execução de todos os passos definidos no caso de teste for de acordo com a espectativa definida no mesmo;
- Falhou: quando pelo menos um passo do caso de teste não corresponde a espectativa definida;
- Limitação do design: quando existem limitações de design do dispositivo que impossibilitam a execução de pelo menos um passo de um caso de teste;
- Não aplicável: quando o caso de teste não faz parte dos requisitos definidos para o dispositivo em questão;

Caso o resultado final for "falhou" é considerado um defeito e deve ser adicionado ao mesmo um defeito respeitando os passos para gestão de defeito acima descrito.

4.5. Metodologia

A Altran utiliza uma metodologia interna para a execução de testes constituída por 4 fases fundamentais, em que os órgãos de gestão tem um conhecimento profundo da mesma e constitui

responsabilidade do gestor de projeto a gestão e condução de todas as fases da metodologia. No âmbito da metodologia o estagiário esteve enquadrado mais concretamente na terceira fase (execução). Na figura 17 pode-se observar as fases que constituem a metodologia bem como os processos que constituem cada uma destas fases.

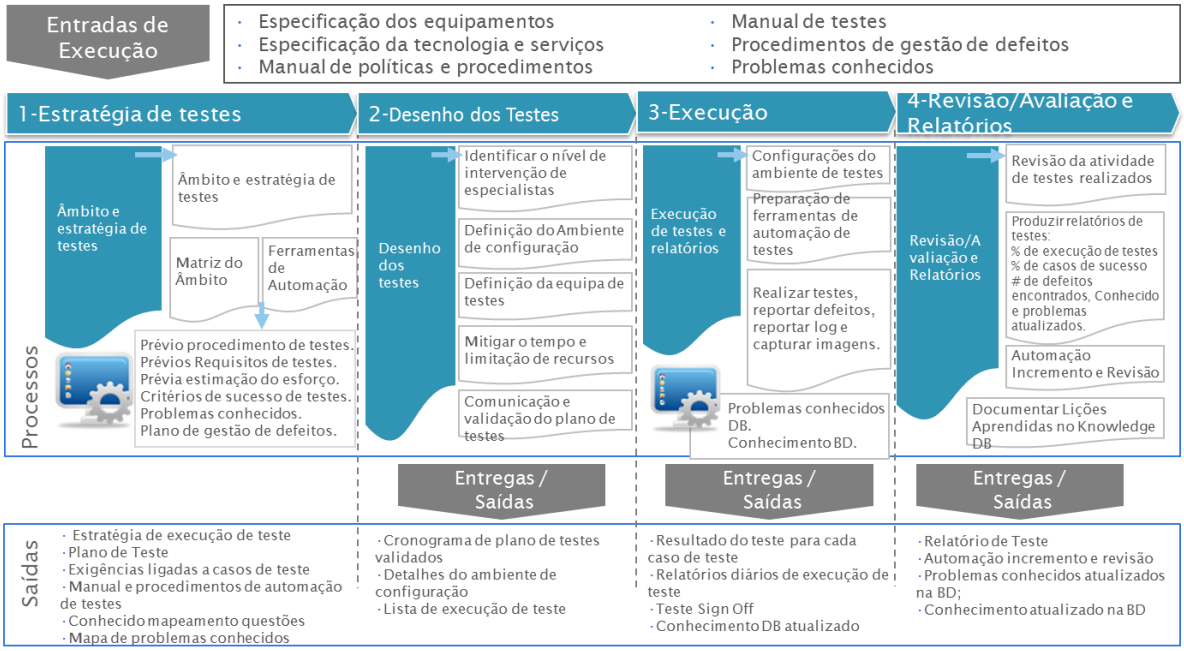

Figura 17- Metodologia interna para execução de testes

Fonte: Laboratório de media (Altran, 2015)

A figura 17 ilustra as fases que constituem a metodologia bem como os processos de cada fase, assim sendo segue-se uma breve descrição dos principais objetivos de cada fase da metodologia:

1- Estratégia de testes: o principal objetivo desta fase é a prévia definição da estratégia de execução de testes.
2- Desenho de testes: o principal objetivo desta fase consiste na definição dos testes bem como todos os recursos necessários para a devida efetivação do mesmo.
3- Execução: o principal objetivo desta fase consiste na preparação de toda a infraestrutura tecnológica necessária para a execução de teste.
4- Revisão avaliação e relatórios: o principal objetivo desta fase consiste na revisão de testes e entrega dos relatórios finais.

Tendo em conta que no âmbito da metodologia o estagiário esteve enquadrado na fase de execução, seguidamente serão descritos minuciosamente todos os processos que constituem esta fase.

4.6. Configurações do Ambiente de Testes

Este subcapítulo descreve detalhadamente a configuração da infraestrutura necessária para se dar início a execução de testes CWMP em CPE.

Para se realizar testes do protocolo CWMP a nível do laboratório de acordo com as especificações do mesmo foi necessário criar-se uma infraestrutura e plataformas para garantir a execução de testes de equipamentos terminais CPE simulando um provedor de serviço bem como um cliente final, a figura 18 ilustra a infraestrutura tecnológica em uso para a execução dos testes.

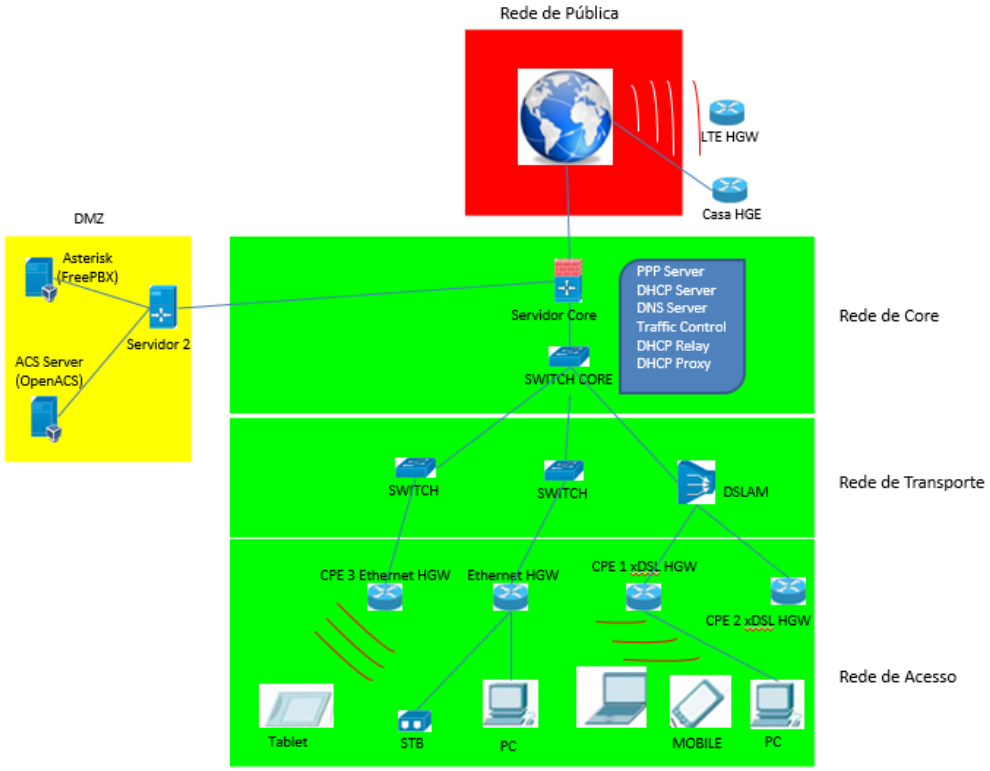

Figura 18- Infraestrutura de suporte aos testes

Fonte: Laboratório de media (Altran, 2015)

Na figura 18 observa-se toda a infraestrutura de suporte as diversas áreas de teste incluindo testes CWMP caraterizada da seguinte forma:

- Rede *Core*: é constituída por *switches*, routers e firewalls que interligam toda a infraestrutura, assim como vários serviços *core* que asseguram a conectividade básica: *dhcp server, dns, QoS, traffic shaping*;
- Rede de Transporte: faz a ponte entre os serviços *core* e a rede do cliente;
- Rede de Acesso: constituída pelo *home-gateway* assim como todos os equipamentos instalados em casa do cliente: *set-top box, tablet*;

A mesma rede encontra-se subdividida em 3 zonas designadamente:

- Rede Privada: zona de acesso controlado com nível de segurança elevado;
- DMZ: zona de acesso controlado com serviços que devem estar disponíveis tanto na rede privada como na pública;
- Pública: rede partilhada por diferentes utilizadores, pelo que, é necessária firewall para garantir acesso ao exterior.

4.6.1. Instalação das Plataformas

Na figura 18, o equipamento denominado servidor *core* consiste num servidor com o sistema operativo debian que por sua vez suporta um conjunto de servidores virtuais e serviços, de acordo com a debian, (2015), debian é um sistema operativo livre, que consiste num conjunto de programas básicos e utilitários que permitem o funcionamento do computador, com mais de 43000 pacotes de softwares pré-compilados e distribuídos em excelente formato, faz com que a instalação do mesmo seja efetuado de forma relativamente simples.

4.6.1.1. Instalação e Configuração do Debian

Para a instalação do debian basta obter a imagem de CD ou DVD através do site oficial, tão logo que o *bios* inicia é apresentado o menu responsável pelo arranque denominado *boot Isolinux*. Neste ponto, o *kernel* do Linux ainda não é carregado, este menu permite-nos escolher o *kernel* bem como iniciá-lo e de seguida passar os parâmetros a serem transferidos.

Cada opção do menu fornece linhas de comando específicas, que devem ser acedidas em função da necessidade e objetivo de cada cliente. A opção "*Help*" do menu mostra a antiga interface de linha de comando, onde as teclas F1 a F10 exibem diversos painéis de ajuda detalhando as demais opções disponíveis no terminal.

A opção "*advanced option*" fornece-nos todas as opções possíveis para o processo de instalação, e possibilita a navegação entre os vários passos sem que eles aconteçam automaticamente. A figura 19 ilustra as opções de instalação depois do arranque do CD-DVD, bem como algumas opções acima descritas.

Figura 19- Interface de instalação do debian

Fonte: Laboratório de media (Altran, 2015)

Conforme ilustra a figura 19 e em função das necessidades do laboratório escolheu-se a opção *64 bit graphical install*, depois de escolhido o tipo de instalação, o programa de instalação guia-nos passo a passo até ao final da instalação.

4.6.1.2.*ISC-DHCP Server*

Depois da instalação do debian o passo a seguir foi a instalação e configuração do *isc-dhcp server*. O *dhcp* é extremamente importante devido a sua função que consiste em gerir endereços IP e informações relacionadas de forma centralizada e fornecem-nos automaticamente aos clientes. Isto permite-nos configurar definições da rede cliente no servidor, em vez de configurá-las em cada computador cliente.

isc-dhcp consiste num conjunto de pacotes de software que implementa todos os aspetos do *dhcp*, estes pacotes são:

- Um servidor *dhcp*, que recebe as solicitações;
- Um cliente *dhcp*, que envia as solicitações ao servidor;
- Um agente de retransmissão *dhcp*, que passa solicitações *dhcp* de uma LAN para outra, de modo que não haja necessidades de ter um servidor *dhcp* em cada LAN.

O servidor *isc-dhcp* irá responder as solicitações de qualquer cliente que esteja em conformidade com as normas do protocolo, e o cliente *isc-dhcp* pode interagir com qualquer servidor que esteja em conformidade com essas normas. Assim sendo proceder-se-á sua instalação mediante os comandos descritos abaixo.

1- Aceda à consola e entre como root.

* su

-> Introduza a palavra-passe.

2- Introduza o comando: apt-get install isc-dhcp-server

A figura 20 ilustra o ambiente e/ou interface em que se escreve o comando acima descrito bem como o resultado de execução do mesmo.

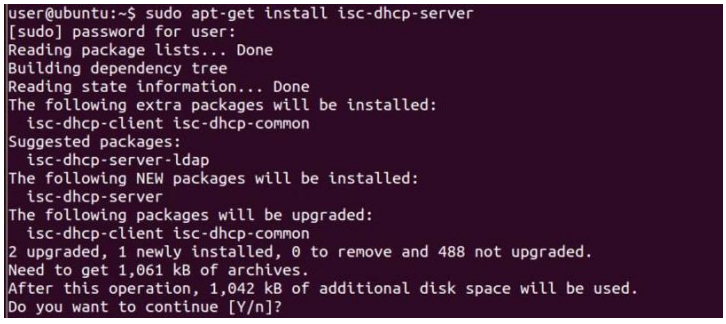

Figura 20- Instalação do *isc-dhcp server*

Fonte: Laboratório de media (Altran, 2015)

4.6.1.3. Configuração do Servidor DHCP

Depois de instalado o conjunto serviços *isc-dhcp server*, o passo a seguir consiste na configuração do mesmo de acordo com as reais necessidades do laboratório.

Aceda como utilizador root e digite o seguinte comando:

sudo nano /etc/dhcp/dhcpd.conf

Introduza a opção global "ddns-update-style none;"

Altera:

- option domain-name "introduza domínio";
- option domain-name-servers endereço ip, endereço ip;
- default-lease-time 86400;
- max-lease-time 604800;
- subnet 20.20.20.0 netmask 255.255.255.0 {
- range 20.20.20.100 20.20.20.150;
- option subnet-mask 255.255.255.0;
- option broadcast-address 20.20.20.255;
- option routers 20.20.20.254;
    - }

Verifique se não há erros na sintaxe:

* dhcpd –t

Comando para manipular o servidor:

service isc-dhcp-server start

service isc-dhcp-server stop

service isc-dhcp-server restart

service isc-dhcp-server status

CTRL+O (Salvar)

Enter (Guardar)

CTRL+X (Sair)

4.6.2. Instalação da VMs e Seus Componentes

Depois de instalado o servidor *dhcp* o passo a seguir foi a instalação da máquina virtual denominada *VirtualBox* que por sua vez suportará o servidor ACS. Os principais aspetos positivos que foram decisivos na adoção de máquina virtual neste projetos são: a redução significativa da quantidade de servidores; a redução do espaço físico para os servidores; a redução significativa de consumos energéticos, assim como a redução de impactos ambientais, aumentando a facilidade de gestão, a facilidade na reposição de um servidor e essencialmente a redução de custos.

Para a instalação do mesmo basta seguir os seguintes passos:

1- Aceda como utilizador root e digite o seguinte comando:

sudo su

echo "deb http://download.virtualbox.org/virtualbox/debian $(lsb_release -cs) contrib non-free #Virtualbox" > /etc/apt/sources.list.d/virtualbox.list

wget -q http://download.virtualbox.org/virtualbox/debian/oracle_vbox.asc -O- | apt-key add - apt-get update

apt-get install virtualbox-4.3

if ["`grep vboxusers /etc/group|grep $USER`" == ""] ; then sudo usermod -G vboxusers -a $USER ; fi

4.6.2.1. Instalação e Configuração do Ubuntu *Server*

Com a *VirtualBox* instalada o passo a seguir consiste na instalação do sistema operativo Linux, Ubuntu *Server* na versão 14.04, 64 bit que por sua vez suportará o servidor de auto configuração.

Aproveitando os recursos da tecnologia de virtualização, usando para o efeito à aplicação *VirtualBox*. Nesse sentido, criou-se um perfil da máquina virtual com as seguintes características:

- Memória RAM – 2048 MB;
- Disco: 20 GB.

Na figura 21 observa-se que para além das configurações acima descritas ativamos também a opção, 3D *Acceleration* que se encontra nas opções da máquina virtual, no separador *display* (Esta opção é importante para que o *Unity* tenha uma performance melhorada).

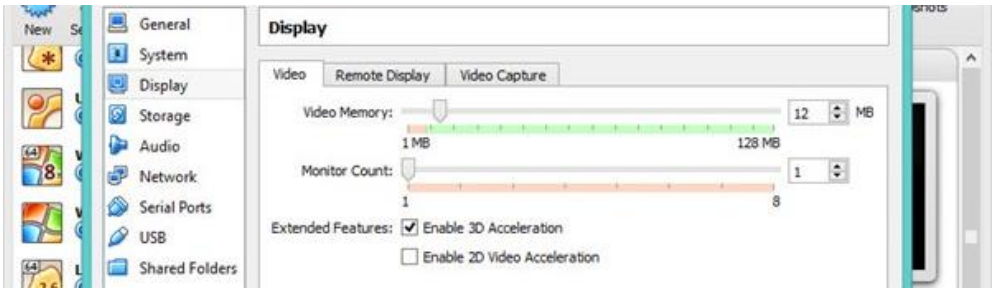

Figura 21- Configuração do ubuntu *server*

Fonte: Laboratório de media (Altran, 2015)

Depois de serem carregados alguns componentes, é apresentada a primeira janela de configuração que nos oferece um conjunto de idiomas. De acordo com as necessidades específicas do laboratório o idioma escolhido foi o inglês, conforme ilustra a figura 22.

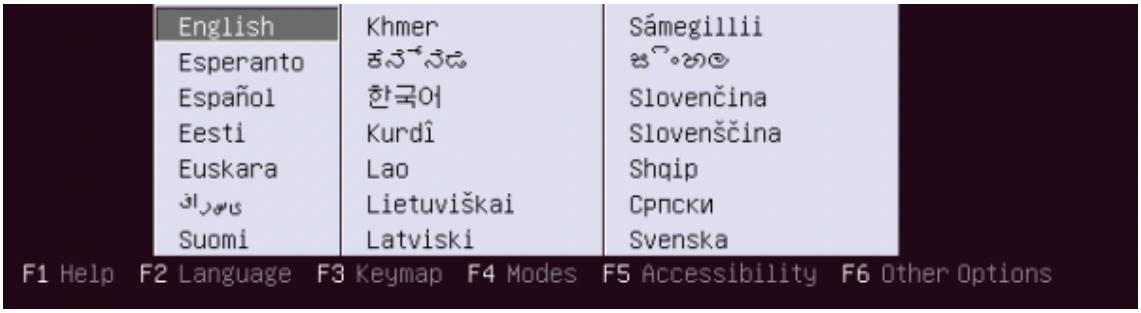

Figura 22- Fase de escolha do idioma de instalação do ubuntu *server*

Fonte: Laboratório de media (Altran, 2015)

Nesta fase seleciona-se a primeira opção *Install* Ubuntu *Server* conforme ilustra a figura 23.

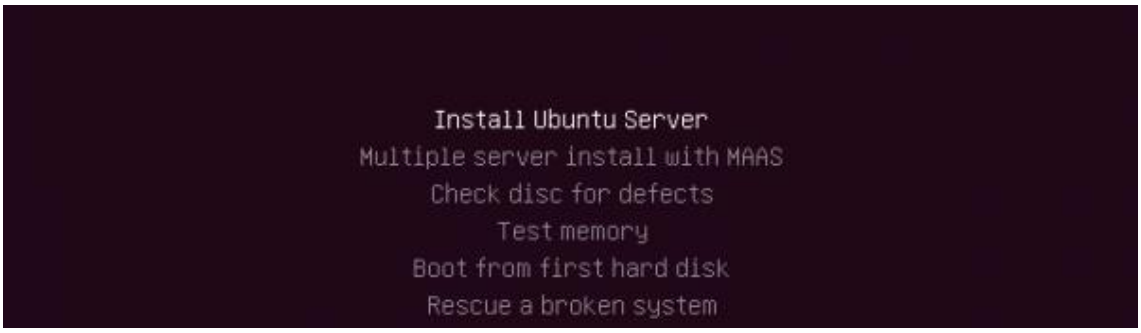

Figura 23- Instalação do ubuntu *server*

Fonte: Laboratório de media (Altran 2015)

Esta opção nos guiará a um conjunto de passos relativamente simples de se preencher tais como o idioma do teclado, gestor de pacotes, como se pretende receber atualizações etc. No final da instalação é apresentada uma mensagem de confirmação de finalização da instalação, conforme ilustra a figura 24.

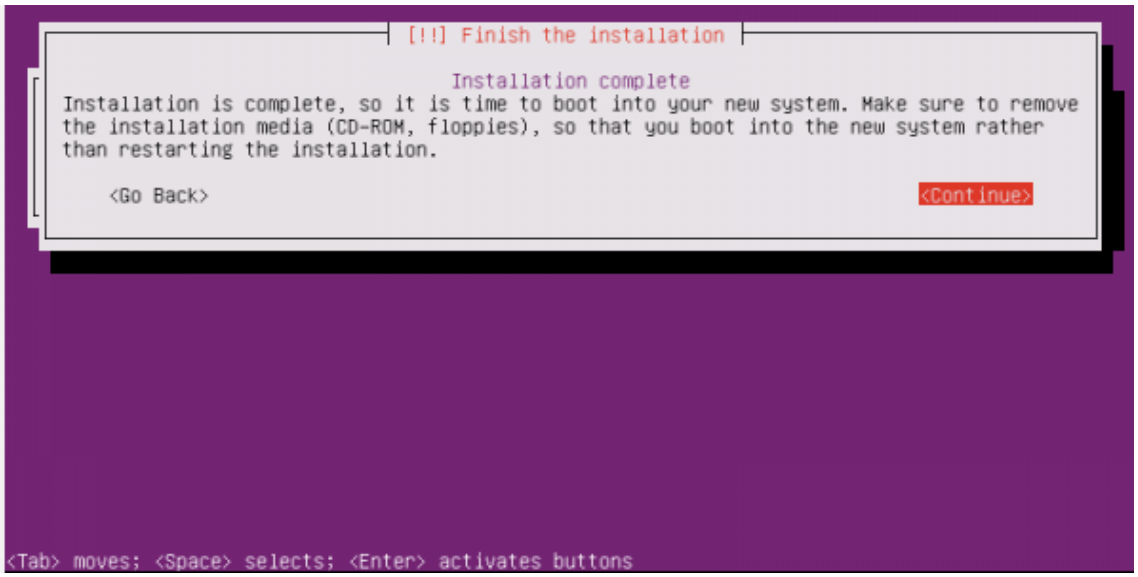

Figura 24- Mensagem de instalação concluída do ubuntu *server*.

Fonte: Laboratório de media (Altran 2015)

A figura 24 ilustra a mensagem de instalação concluída do ubunto *serve*r. Depois de concluída a instalação do ubuntu *Server*, o passo a seguir consiste na instalação do servidor de auto configuração.

4.6.2.2. Instalação do Servidor ACS

Vale realçar que existem várias aplicações de suporte ao protocolo tr-069, assim sendo as aplicações e/ou ACS que serão instaladas para a realização dos testes são: 1º*FreeACS* e 2º*OpenACS*.

FreeACS é considerado por muitos como o mais completo TR-069 ACS disponível gratuitamente no marcado sob a licença MIT.

FreeACS é uma aplicação de gestão de dispositivos também conhecida como servidor de autoconfiguração, gratuito com suporte ao protocolo tr-069 atualmente implementado na maioria dos dispositivos eletrónicos domésticos tais como: routers, *Set-top box*, telefones etc. Dentre as diversas funcionalidades que a mesma aplicação fornece vale destacar algumas que no nosso ponto de vista são bastante relevantes e que foram decisivas na escolha da mesma à fim de satisfazer as necessidades do laboratório levando em consideração o fator qualidade e redução de custos, estas funcionalidades são, a possibilidade de atualizar e instalar *firmware*, executar *scripts*, gerar relatórios relativo ao comportamento do dispositivo, verificar mensagens de erros e de

configuração de backup, fornece pesquisa avançada para dispositivo e um simples painel de controlo dos mesmos. O sistema ainda suporta um conjunto de tarefas de apoio ao protocolo HTTP / TFTP e *Telnet* para provisionamento.

Existem diversas formas de instalar o *FreeACS*, para o efeito utilizaremos a forma considerada por muitos como a mais simples, rápida e eficiente.

1º Aceder como utilizador root no ubuntu *server* e executar os comandos que se seguem:

cd && wget http://freeacs.com/download/install-or-update-freeacs-ubuntu.sh

chmod 755 install-or-update-freeacs-ubuntu.sh

sudo ./install-or-update-freeacs-ubuntu.sh

4.7. Preparação das Ferramentas de Automação de Testes

Esta fase da metodologia consiste em averiguar todos recursos tecnológicos de suporte a execução dos testes. Assim sendo proceder-se-á a um conjunto de testes de usabilidade sobre o ACS à fim de nos certificarmos se a ferramenta está operacional.

4.7.1. Explorando o *FreeACS*

1- Para acedermos ao *FreeACS*, primeiramente deve-se abrir o *browser* e digitar o endereço IP (*Internet Protocol*), seguido da porta que se definiu no ato da instalação, como se pode observar na figura 25.

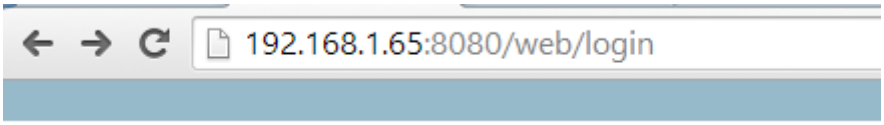

Figura 25- Endereço de acesso ao *FreeACS*

Fonte: Laboratório de media (Altran, 2015)

2- De seguida é visualizada a fronte office do *FreeACS* à solicitar o nome de utilizador e a palavra-passe, por definição o nome de utilizador é: admin e a palavra-passe é: xaps, conforme ilustra à figura 26.

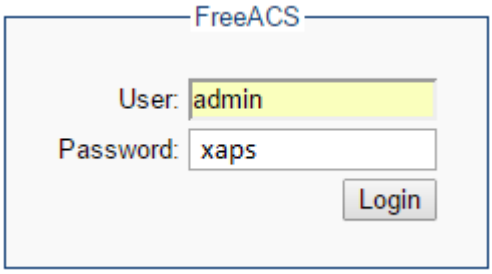

Figura 26- Autenticação *FreeACS*

Fonte: Laboratório de media (Altran, 2015)

Informações de base: Ao iniciar sessão, de seguida é apresentado o ambiente de trabalho do *FreeACS*, e se observamos na parte superior, mais para o lado esquerdo verifica-se a barra de menus, conforme ilustra figura 27.

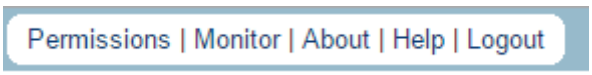

Figura 27- Lista de menus *FreeACS*

Fonte: Laboratório de media (Altran, 2015)

***Permissions* / Permissões:** Em permissões pode-se gerir utilizador e/ou criar utilizador, atribuir privilégios bem como efetuar operações *crud (create, read, update e delete)* do mesmo, conforme ilustra a figura 28.

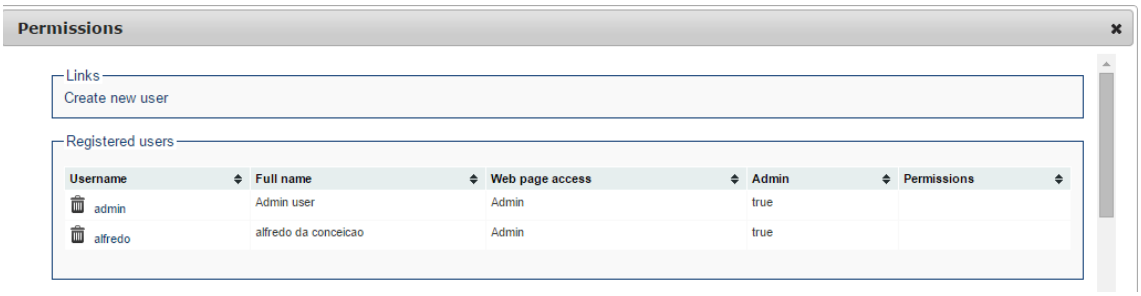

Figura 28- Conteúdo do menu permissões

Fonte: Laboratório de media (Altran, 2015)

Para se criar um utilizador basta clicar na opção "*Create new user*" e lhe será fornecido um formulário, conforme ilustra a figura 29.

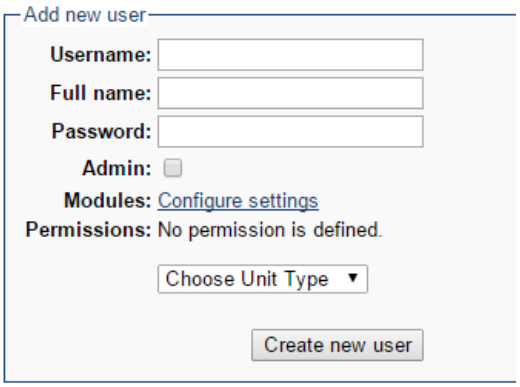

Figura 29- Campos para criação de utilizador

Fonte: Laboratório de media (Altran, 2015)

Ao se preencher o formulário primeiramente começa-se por definir o nome de utilizador e palavra-passe, de seguida seleciona-se a opção admin caso queira atribuir privilégios de administrador ao utilizador. Em **módulos** define-se e/ou atribui-se privilégios relativo aos módulos da aplicação (*FreeACS*) que o utilizador deve ter acesso, por fim devemos atribuir permissões relacionadas às unidades de perfis que o mesmo deve ter acesso, caso não se defina as unidades de perfis o utilizador terá acesso a todas as unidades de perfis.

***Monitor*:** No menu monitor nos é fornecido uma página de *status* (estado) através do qual podemos verificar o estado de funcionamento de todos os módulos da aplicação (*FreeACS*), Conforme ilustra a figura 30.

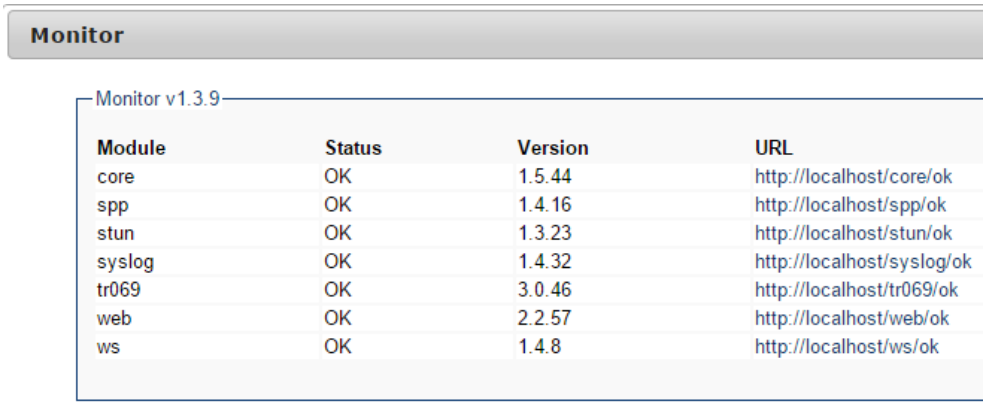

Figura 30- Estado de funcionamento dos módulos

Fonte: Laboratório de media (Altran, 2015)

About: O menu *About* fornece um conjunto de informação acerca do produto tais como, o *FreeACS* tem sido desenvolvido desde 2005 e está sendo executado em uma plataforma Java, utilizando o banco de dados MySQL, bem como um conjunto vasto de bibliotecas e/ou referências que tornaram possível o desenvolvimento da mesma.

***Help*:** Na secção e/ou menu *Help*, fornece ajuda de acordo com a página que estamos a navegar, vale realçar que encontramos ajuda a medida que navegamos nas páginas, esta ajuda é demonstrada em pequenas perguntas e/ou sinais de ponto de interrogação.

***Logout*:** Na secção e/ou menu *logout*, permite-nos terminar a sessão do utilizador.

***Global search*:** Existem diversas formas de localizar as unidades, em que a primeira consiste na busca global localizada no canto superior direito, como se pode constatar na figura 31.

Figura 31- Filtro de pesquisa *FreeACS*

Fonte: Laboratório de media (Altran, 2015)

Esta pesquisa irá procurar por um valor de parâmetro de unidade ou um ID da unidade em todos os tipos de unidade no sistema. Isto significa que, se você procurar por um número, por exemplo, "888", todos os dispositivos que tem este número como parte de uma senha, número de telefone, ID da unidade, serão listados.

Context search: Esta pesquisa funciona exatamente da mesma forma que a pesquisa global, mas apenas dentro de um dado contexto (tipo unidade e / ou perfil). O campo de pesquisa encontra-se na barra de contexto. Ao escolher-se um tipo de unidade, como resultado da pesquisa será visualizado mais informações, caso contrário, apenas uma lista de identificadores de unidade serão listados, conforme ilustra a figura 32.

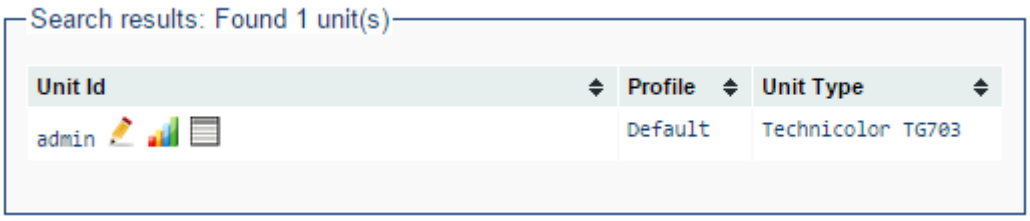

Figura 32- Pesquisa do tipo *Context search*

Fonte: Laboratório de media (Altran, 2015)

A figura 32 ilustra o CPE que foi localizado de acordo com a pesquisa efetuada. Ao clicarmos no *unit id* correspondente ao CPE, nos é visualizado o *unit dashboard* onde podemos encontrar informações básicas tais como, estado atual do dispositivo e o histórico desde que foi estabelecida a ligação até a data presente conforme se pode observar na figura 33.

Unit Dashboard: Ao clicar-se em um *unit id* da *unit listing* na página de pesquisa, visualiza-se um painel *unit*. O *painel unit Dashboard* contém o resumo do estado do dispositivo (CPE), o estado de funcionamento dos dispositivos é relativamente importante em termos de provisionamento / gestão, versão do software, serviço VoIP e *status* do hardware.

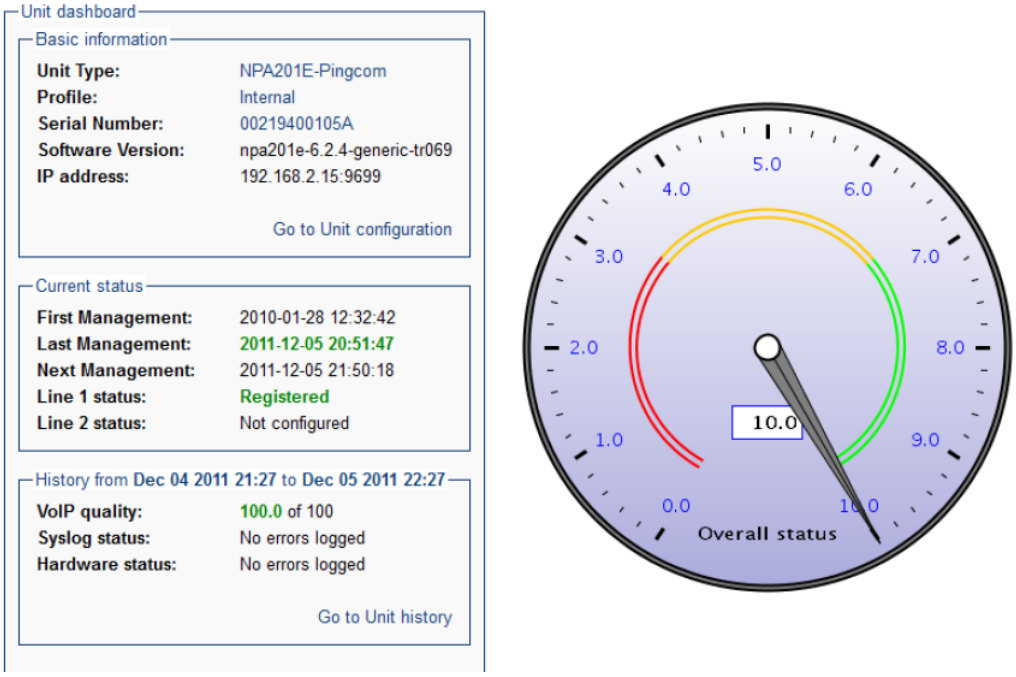

Figura 33- ***Unit Dashboard FreeACS***

Fonte: Laboratório de media (Altran, 2015)

Conforme se pode observar na figura 33 o texto a verde e pontuação máxima no velocímetro indicam bom estado de funcionamento do dispositivo (CPE). A cor amarela indica uma anomalia. De forma global o velocímetro resume o estado geral de todos os dispositivos ligados ao ACS, de maneira que o administrador e/ou utilizador do ACS tenha uma visão geral da situação.

Unit History ou Support > Syslog: A partir do painel de instrumentos é possível navegar nas configurações da unidade. O histórico fornece uma visão geral dos vários componentes de um dispositivo como, histórico de hardware e histórico VoIP. O histórico fornece ainda uma visão

geral dos vários componentes de um dispositivo, como histórico de hardware e VoIP, conforme ilustra a figura 34.

Figura 34- Log eventos CWMP do *FreeACS*

Fonte: Laboratório de media (Altran, 2015)

4.7.2. Adicionando o CPE CPE 1 xDSL HGW ao ACS *FreeACS*

Depois de constatado que o servidor de auto configuração está devidamente configurado e operacional o passo a seguir consiste em fazer com que o CPE se comunique com o ACS. Para o efeito deve-se aceder por *telnet* ao CPE e inserir os seguintes comandos:

conf set "/cwmp/acs_url" "http://20.20.20.4/tr069"

conf set "/cwmp/username" "61901U0000194"

conf set_obscure "/cwmp/password" "xaps"

conf set "cwmp/conn_req_username" "xaps"

conf set_obscure "cwmp/conn_req_password" "xaps"

conf set "/cwmp/periodic_inform/interval" "60"

conf reconf 1

Obs: vale realçar que as configurações variam de acordo o modelo do CPE e as credencias de acesso ao ACS.

4.8. Execução de Testes e *Report* CPE 1 xDSL HGW

Com o cenário de testes montado e com todas as ferramentas de apoio à execução de testes devidamente configuradas, estamos em condições de dar início ao processo de execução de testes, o 1º dispositivo a ser testado consiste num CPE denominado CPE 1 xDSL HGW, as caraterísticas do mesmo encontram-se descritas na tabela 7:

Componente	Estado	Observações
ADSL	Suporta	
VDSL	Suporta	
LAN-Ethernet	Suporta Parcialmente	Não está completamente personalizada
Wi-Fi	Suporta Parcialmente	*Guest Wi-Fi* não suporta
Layer 2, Layer 3	Suporta	
NAT, DHCP, DDNS, NTP	Suporta	
Buttons and LEDs	Suporta Parcialmente	Comportamento do LED ainda não está totalmente implementado
ACS integration	Suporta	
Remote Upgrade	Suporta	
Firewall	Suporta	
VLANs	Suporta	
Sharing (File Server, Media Server)	Suporta	
WBM	Suporta Parcialmente	Ajustes GUI são parcialmente suportados página de login não é suportada

Tabela 7 – Caraterísticas do CPE 1 xDSL HGW

Fonte: Laboratório de media (Altran, 2015)

As áreas de teste que serão executadas pela equipa são: *DSL_Usability, DSL_Stress_Tests, DSL_Router, DSL_QoS, DSL_Health_Check, DSL_ACS_Communication, DSL_Exploration, DSL_DLNA, DSL_WiFi, APP_DSL_iOS, APP_DSL_Android.*

Neste relatório será apresentada os principais processos envolvidos na área de teste DSL_ACS_Communication, pelo facto de ser a área de teste cujo objetivo consiste em testar as funcionalidades do protocolo CWMP sobre o CPE supracitado que por sua vez constitui um dos

principais objetivos de realização deste relatório e também pelo facto de ser a área de teste em que o estagiário esteve enquadrado. As demais áreas de teste não serão descritas neste relatório pelo facto de não fazerem parte do âmbito de realização deste trabalho e pelo facto de estas obrigações estarem a cargo de outros profissionais. Esta área de teste é constituída por 37 casos de teste mas devido a questões de confidencialidade, iremos mostrar em detalhe a resolução de apenas 2 casos de teste, de acordo com os critérios estabelecidos no ponto 4.4. Gestão de defeitos o resultado final de cada caso de teste pode ser, passou, falhou, limitação do design ou não aplicável.

A tabela 8 apresenta a descrição do primeiro caso de teste, seguidamente será apresentado a resolução do mesmo passo a passo.

Nome do Projeto		
Teste_CPE		
Teste ID: 1		
Nome do Teste: *Logging*		
Área de Teste: *DSL_ACS_Communication*		
Descrição do teste:		
Não se deve notar qualquer anomalia nos serviços de voz, dados e tv do CPE enquanto estiver a decorrer este teste. O objetivo do mesmo consiste em verificar os log /ou registos enquanto forem executadas um conjunto de operações no ACS sobre o CPE.		
Passo 1	**Descrição do passo**	**Expetativa**
	Execute várias ações TR069 tais como, *ConnectionRequest, Get Parameter Value, Set Parameter Value* e falhas no ACS sobre o CPE.	Os *logs* devem ser vistos pelo CLI ou GUI do CPE.

Tabela 8 – Descrição do caso de teste, *Logging*

Adaptado de: Laboratório de media (Altran, 2015)

4.8.1. Resolução do Caso de Teste *Logging*

1º Com o ACS (*OpenACS*) clique sobre o menu ***Device profiles***, de seguida selecione o ***Device profiles* correspondente** por ex: ***default.***

2º Em ***Device profile: Default/General/Configuration script to be run*:** define o método a ser executado por ex: ***GetParameterValue***.

3º Clique em ***Save*.** Clique sobre o menu ***Find* CPE,** na opção **Hardware:** selecione o hardware correspondente ao CPE e na opção *Serial No*: digite o número de série do CPE.

5º Clique sobre a opção ***details*** e abaixo da opção ***Connection request* URL:** um clique sobre o URL, conforme ilustra a figura 35.

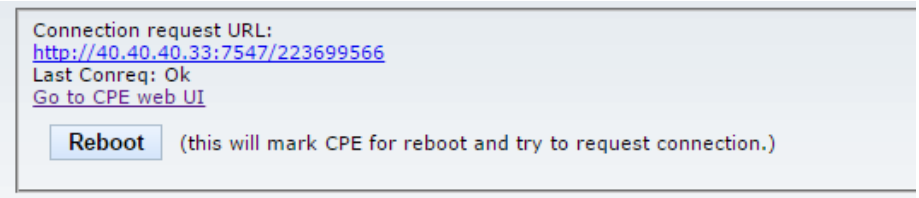

Figura 35- URL, para *Connection Request OpenACS*

Adaptado de: Laboratório de media (Altran, 2015)

6º Aceder por *telnet* ao CPE e executar o comando: *log filter set* *.* ou *log filter set cwmp_ipc*.*. Na figura 36 observa-se através do CLI os *logs* relativos a execução do método.

Figura 36- *Logs* relativo a execução de parâmetros CWMP

Fonte: Laboratório de media (Altran, 2015)

Na figura 36 pode-se observar todos os parâmetros CWMP que foram executados no ACS sobre o CPE, os *logs* são muito importante porque através deles conseguimos verificar o registo de atividades executadas sobre o CPE e que pode ajudar na resolução de determinados problemas.

O passo seguinte consiste em reportar o resultado na aplicação *HP Quality Center*, tendo em conta que o teste vai de encontro com a expetativa, considera-se que passou.

4.8.2. *Report* do Resultado do Teste *Logging*

Conforme descrito no ponto 1.1.1. Âmbito do projeto, a execução de teste bem como o *Reporting* do mesmo deve ser feita usando a ferramenta *HP Quality Center*.

Com o *HP Quality Center* aberto selecione com um clique o caso de teste, clique sobre a opção *Run*, clique sobre a opção *Bigin Run*, altere o *status* do *step* 1 para *passed*, clique sobre a opção *End Run*, duplo clique sobre o caso de teste e altere o *status* para *passed*, clique sobre ok e o resultado do caso de teste é alterado de *No Run* para ***passed*** conforme ilustra a figura 37.

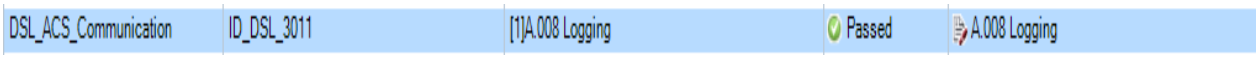

Figura 37- Estado do caso de teste depois de atualizado

Fonte: Laboratório de media (Altran, 2015)

A tabela 9 apresenta a descrição do segundo caso de teste denominado *Connection Request*, seguidamente será apresentado a resolução do mesmo passo a passo. No intuito de deixarmos o leitor não só com uma visão teórica mas também com uma abordagem prática.

Nome do Projeto		
Teste_CPE		
Teste ID: 2		
Nome do Teste: *Connection Request*		
Área de Teste: *DSL_ACS_Communication*		
Descrição do teste:		
Não se deve notar qualquer anomalia nos serviços de voz, dados e tv do CPE enquanto estiver a decorrer este teste.		
	Descrição do passo	**Expetativa**
Passo 1	Execute no ACS sobre o CPE uma ação, *ConnectionRequest*.	Verifique se a autenticação *Digest* é usado
Passo 2	Altere no ACS a senha de autenticação do CPE com o ACS e execute uma ação *ConnectionRequest*	O CPE, não deve permitir *ConnectionRequest*
Passo 3	verifique se apenas os seguintes ip são permitidos: 145.253.2.0/24 145.253.3.0/24	verificar se apenas se consegue comunicar com os ips da lista.

Tabela 9 – Descrição de caso de teste, *Connection Request*

Adaptado de: Laboratório de media (Altran, 2015)

Tendo em conta a descrição do caso de teste bem como a expetativa definida na tabela 9, proceder-se-á a devida resolução.

4.8.3. Resolução do Caso de Teste *ConnectionRequest*

1º Depois de alterada a password de autenticação do CPE com o ACS clique sobre o menu ***Device profiles***, de seguida selecione o ***Device profiles*** correspondente por ex: ***default.***

2º Em ***Device profile*****:** ***Default/General/Configuration script to be run*****:** definir o método ser executado: ***ConnectionRequest***.

3º Clique em ***Save*****.**

4º Clique sobre o menu ***Find*** **CPE,** na opção **Hardware:** selecione o hardware correspondente ao CPE e na opção *Serial No*: digite o número de série do CPE.

5º Clique sobre a opção ***details*** e abaixo da opção ***Connection request*** **URL:** um clique sobre a URL, conforme ilustra à figura 38.

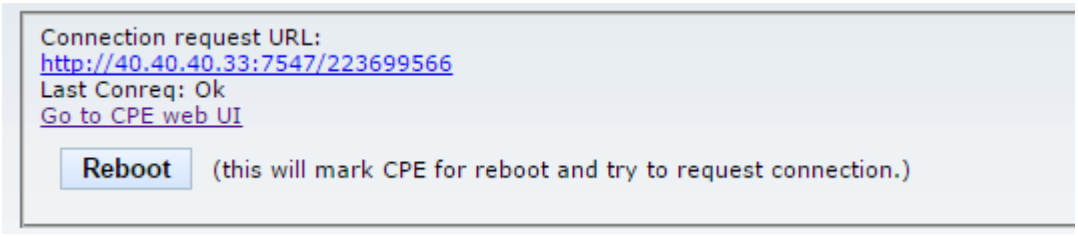

Figura 38- URL, para efetuar tentativas de ligação *ConnectionRequest*

Fonte: Laboratório de media (Altran 2015)

6º Depois de feita à captura com a ferramenta *wireshark,* constatou-se que o CPE comunicava com o ACS e com IP que não constam da lista.

O passo a seguir consiste em reportar o resultado na aplicação *HP Quality Center*, tendo em conta que o teste não vai de encontro com a expetativa, considera-se que falhou.

4.8.4. *Report* de Defeito *Connection Request*

Conforme descrito no ponto 4.4. gestão de defeitos, durante a fase de execução de teste podem ser detetadas falhas entre o requisito baseado no atual caso de teste e o resultado do caso de teste. A análise de defeito deve ser realizada mediante a utilização do processo denominado

Kepner-Tregoe, assim sendo altera-se o estado do caso de teste para *Failed* e deve-se adicionar ao mesmo um defeito conforme descrito abaixo.

1- Com o *HP Quality Center* aberto selecione com um clique o passo do caso de teste que falhou, conforme ilustra a figura 39.

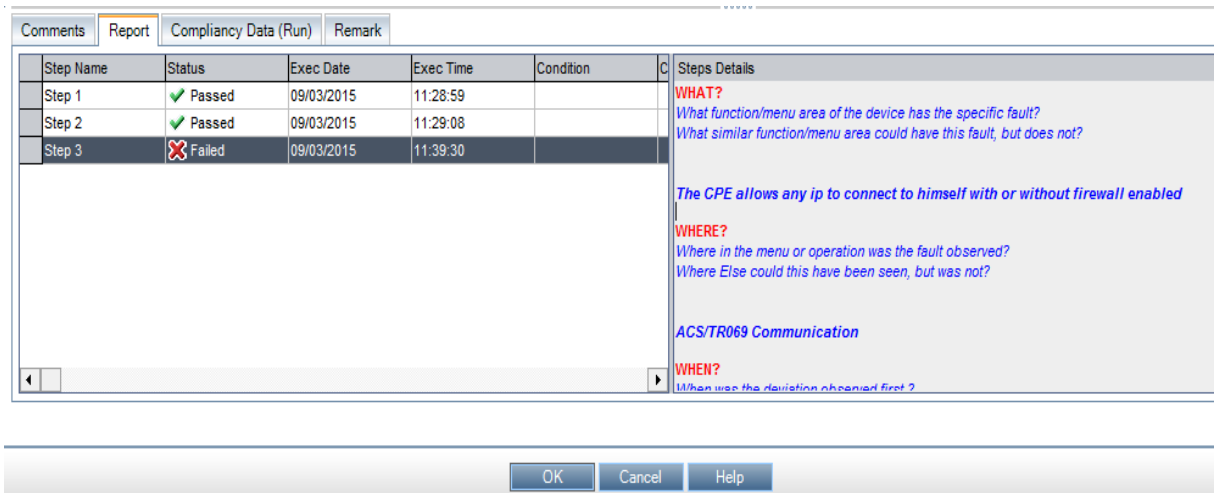

Figura 39- Criando defeito

Fonte: Laboratório de media (Altran, 2015)

2- Descrever os campos *WHAT? WHERE? WHEN? e EXTENT?*. Que o descrevemos da seguinte forma:

- *What*: O CPE permite que seja comunicado com qualquer IP com ou sem firewall ligada.
- *Where*: Comunicação ACS/CPE.
- *When*: Ao conectar o ACS com o CPE.
- *Extent*: Com este comportamento a porta de gestão remoto do CPE fica acessível para a internet, que por sua vez aumenta a exposição do CPE para hackers e ataques.

Seguidamente um clique sobre a opção ok.

3- Duplo clique sobre o caso de teste, de seguida um clique sobre a opção *linked defects*
4- Um clique sobre a opção *add and linked defects.*
5- Preencher todos os campos solicitados conforme ilustra a figura 40.

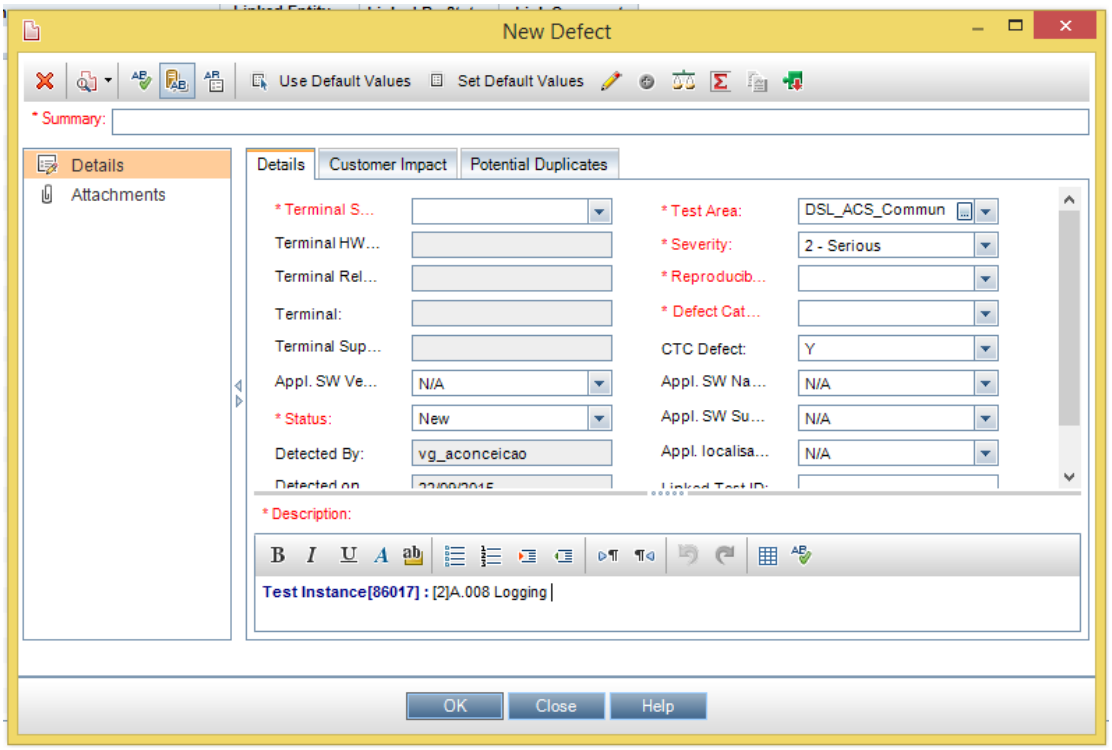

Figura 40- Campos de atualização de defeito

Fonte: Laboratório de media (Altran, 2015)

Depois de preenchido todos os campos principalmente o campo *severity*, que para este caso de teste atribui-se o grau de severidade 2, de acordo com o que está definido no ponto 4.4. gestão de defeitos deste relatório.

Cumprindo com os passos acima descritos o resultado do caso de teste é alterado de *No Run* para ***failed*** conforme ilustra a figura 41.

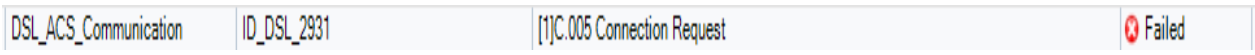

Figura 41- Estado final do caso de teste

Fonte: Laboratório de media (Altran, 2015)

4.8.5. Resultados Globais dos Testes

Na tabela 10 observa-se o resultado de execução dos 37 casos de teste dentre os quais 23 passaram, 3 falharam, 1 limitação de design e 10 não aplicável. A grande preocupação centra-se nos testes falhados e também por receberem o grau de severidade 2, de acordo com o que está estabelecido no subcapítulo 4.4. gestão de defeitos, o grau de severidade 2 consiste num problema

de usabilidade do dispositivo com alto impacto, normalmente consiste num problema que não impede o lançamento do produto, mas que necessita de correção. Assim sendo espera-se que o cliente resolva este problema junto do fabricante do dispositivo.

Id	*Nome do Teste*	Comentários	Resultado Final
1	*Logging*		Passou
2	*WAN reconnect button*		Passou
3	*Bootstrap on for all WAN Intf*		Passou
4	*Update and Rollback scenarios*		Passou
5	*NTP Servers*		Passou
6	*GetPararameterValue of all Tree*		Passou
7	*Long-term Firmware updates via ACS*		Passou
8	*Devicelog readable by ACS*		Passou
9	*Active notification*		Passou
10	*Inform Messages[PERIODIC]*		Passou
11	*ACS-Update during bootstrap message*		Passou
12	*Inform if IP address changes on WAN Interface*		Passou
13	*Connection Request*		Falhou
14	*Power off firmware*		Passou
15	*SET GET TR-098 PARAMETERS*		Passou
16	*CWMP RPCs*		Passou
17	*Retry behaviour while ACS is down*		Passou
18	*WiFi LAN Extension*		Passou
19	*Passive notification*		Passou
20	*CR port is selected randomly*		Passou
21	*Config Rollback*		Passou
22	*Remote Access*		Passou
23	*Connection Request*		Passou
24	*Passwords*		Falhou
25	*New CR port is selected if port gets occupied by user*		Passou
26	*USB Status*		Passou
27	*DMZ Host configured*	Funcionalidade não implementada	Limitação do design
28	*SIP Account(s) Provisioning*	Não suporta o SIP	Não aplicável
29	*CPE checks server certificate hostname*	O ACS não possui	Não aplicável
30	*While downloading or flashing firmware, phone is disabled*	Não suporta o SIP	Não aplicável
31	*FXS status can be read by ACS*	Não suporta o SIP	Não aplicável
32	*ACS-Firmware + Calls*	Não suporta o SIP	Não aplicável
33	*TR111*	O CPE não suporta	Não aplicável
34	*CPE checks server certificate validity period*	O ACS não possui	Não aplicável
35	*CPE checks server certificate*	O ACS não possui	Não aplicável
36	*TR143*	O CPE não suporta	Não aplicável
37	*ACS communication is encrypted*	Não suporta	Não aplicável

Tabela 10 – Resultados globais dos testes sobre CPE 1 xDSL HGW

Fonte: Laboratório de media (Altran, 2015)

Relativamente aos resultados de execução de testes referidos na tabela 10, constata-se que 62% dos testes passaram, 8% dos testes falharam, 3% limitação de design e 27% não aplicável, para o cálculo das percentagens utilizou-se a regra de três simples que se pode observar abaixo.

Passou	Falhou	Limitação do design	Não aplicável
37x = 100 * 23	37x = 100 * 3	37x = 100 * 1	37x = 100 * 10
37x = 2300	37x = 300	37x = 100	37x = 1000
x = 2300/37	x = 300/37	x = 100/37	x = 1000/37
x = 62%	x = 8%	x = 3%	x = 27%

De forma a simplificar a visualização dos resultados de execução dos testes sobre o CPE 1 xDSL HGW, elaborou-se o gráfico 1, com o objetivo de melhorar a perceção relativa ao grau de percentagem de execução dos testes.

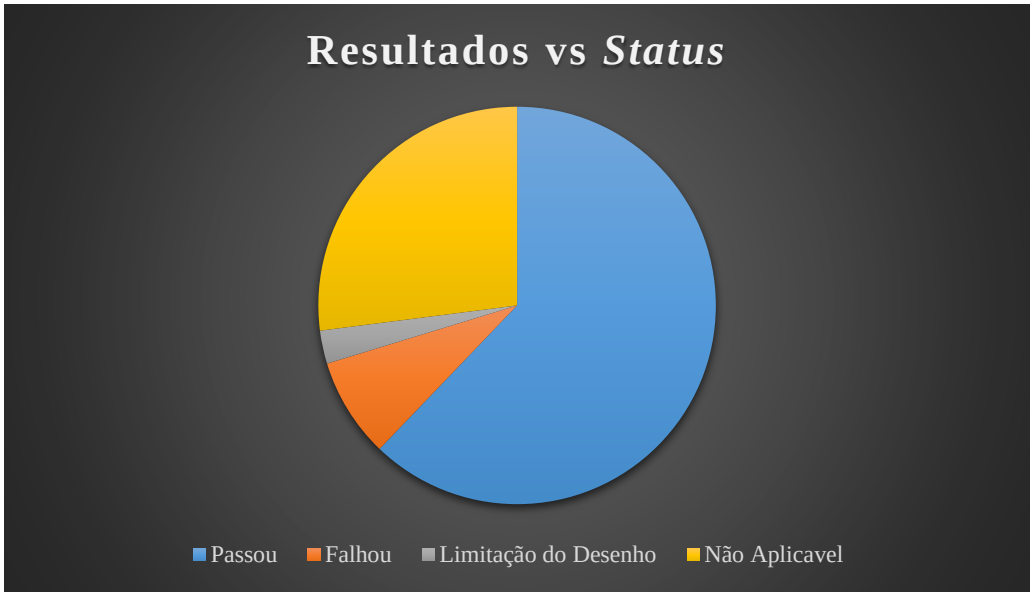

Gráfico 1- Resultados vs *status* CPE 1 xDSL HGW

Adaptado de: *HP Quality Center* (Altran, 2015)

No gráfico 1 consegue-se ter uma visão mais elucidativa relativa ao desenvolvimento dos testes, por classificação.

4.8.6. Considerações

A tabela 11 apresenta as considerações finais sobre a visão global do dispositivo, estas considerações estão organizadas por grau de gravidade onde: 1- significa crítico, 2- importante e 3- moderado.

Severidade 1-3	Nota	Descrição
1	*Connection Request*	O CPE ao permitir comunicação com qualquer ip aumenta a sua exposição para hackers e ataques
2	*Passwords*	Com as passwords desencriptadas, constitui um grave erro de segurança.
3	*DMZ Host configured*	O facto de o dispositivo não suportar DMZ pode limitar o utilizador de explorar esta funcionalidade.

Tabela 11 – Grau de gravidade dos defeitos detetados

Fonte: Laboratório de media (Altran, 2015)

A tabela 11, tem como principal objetivo informar de forma resumida o cliente acerca do grau de gravidade dos defeitos detetados no sentido de tomar a melhor providência possível.

4.9. Execução de Testes e *Report* CPE 2 xDSL HGW

É de salientar que a área de teste bem como os testes que foram submetidos para testar o CPE 1 xDSL HGW é a mesma. No que concerne as caraterísticas a única diferença centra-se no facto de que este CPE suporta VOIP e o anterior não. A figura 42 ilustra o cenário simplificado da infraestrutura necessária para execução de teste CWMP sobre o CPE 2 xDSL HGW.

Figura 42- Cenário de teste CPE 2 xDSL HGW

Adaptado de: Laboratório de media (Altran, 2015)

A figura 42 ilustra o cenário de teste real que simula uma operadora e um cliente, portanto os testes serão executados no servidor ACS que se encontra no lado da operadora sobre o CPE 2 xDSL HGW que se encontra nas instalações do cliente ligado a vários dispositivos.

4.9.1. Resultados Globais dos Testes

Na tabela 12 observa-se o resultado de execução dos 37 casos de teste dentre os quais 31 passaram, 3 falharam, 1 limitação de design e 2 não aplicáveis.

Id	Nome do Teste	Comentários	Resultado Final
1	*Logging*		Passou
2	*WAN reconnect button*		Passou
3	*Bootstrap on for all WAN Intf*		Passou
4	*Update and Rollback scenarios*		Passou
5	*NTP Servers*		Passou
6	*GetPararameterValue of all Tree*		Passou
7	*Long-term Firmware updates via ACS*		Passou
8	*Devicelog readable by ACS*		Passou
9	*Active notification*		Passou
10	*Inform Messages[PERIODIC]*		Passou
11	*ACS-Update during bootstrap message*		Passou
12	*Inform if IP address changes on WAN Interface*		Passou
13	*Connection Request*		Passou
14	*Power off firmware*		Passou
15	*SET GET TR-098 PARAMETERS*		Passou
16	*CWMP RPCs*		Falhou
17	*Retry behaviour while ACS is down*		Passou
18	*WiFi LAN Extension*		Passou
19	*Passive notification*		Passou
20	*CR port is selected randomly*		Passou
21	*Config Rollback*		Passou
22	*Remote Access*		Falhou
23	*Connection Request*		Passou
24	*Passwords*		Passou
25	*New CR port is selected if port gets occupied by user*		Passou
26	*USB Status*		L / Desenho
27	*DMZ Host configured*	Não implementada	Passou
28	*SIP Account(s) Provisioning*	Não suporta o SIP	Passou
29	*CPE checks server certificate hostname*	O ACS não possui	Não aplicável
30	*While downloading or flashing firmware, phone is disabled*	Não suporta o SIP	Passou
31	*FXS status can be read by ACS*	Não suporta o SIP	Falhou
32	*ACS-Firmware + Calls*	Não suporta o SIP	Passou
33	*TR111*	O CPE não suporta	Passou
34	*CPE checks server certificate validity period*	O ACS não possui	Não aplicável
35	*CPE checks server certificate*	O ACS não possui	Passou
36	*TR143*	O CPE não suporta	Passou
37	*ACS communication is encrypted*	Não suporta	Passou

Tabela 12 – Resultados globais dos testes sobre CPE 1 xDSL HGW

Adaptado de: Laboratório de media (Altran, 2015)

Relativamente aos resultados de execução de testes referidos na tabela 12, constata-se que 84% dos testes passou, 8% falhou, 3% limitação de design e 5% não aplicável, para o cálculo das percentagens utilizou-se a regra de três simples que se pode observar abaixo.

Passou	Falhou	Limitação do design	Não aplicável
37x = 100 * 31	37x = 100 * 3	37x = 100 * 1	37x = 100 * 2
37x = 3100	37x = 300	37x = 100	37x = 200
x = 3100/37	x = 300/37	x = 100/37	x = 200/37
x = 84%	x = 8%	x = 3%	x = 5%

De forma a simplificar a visualização dos resultados globais de execução dos testes sobre o CPE 2 xDSL HGW, elaborou-se o gráfico 2, com o objetivo de melhorar a perceção relativa ao grau de percentagem de execução dos testes.

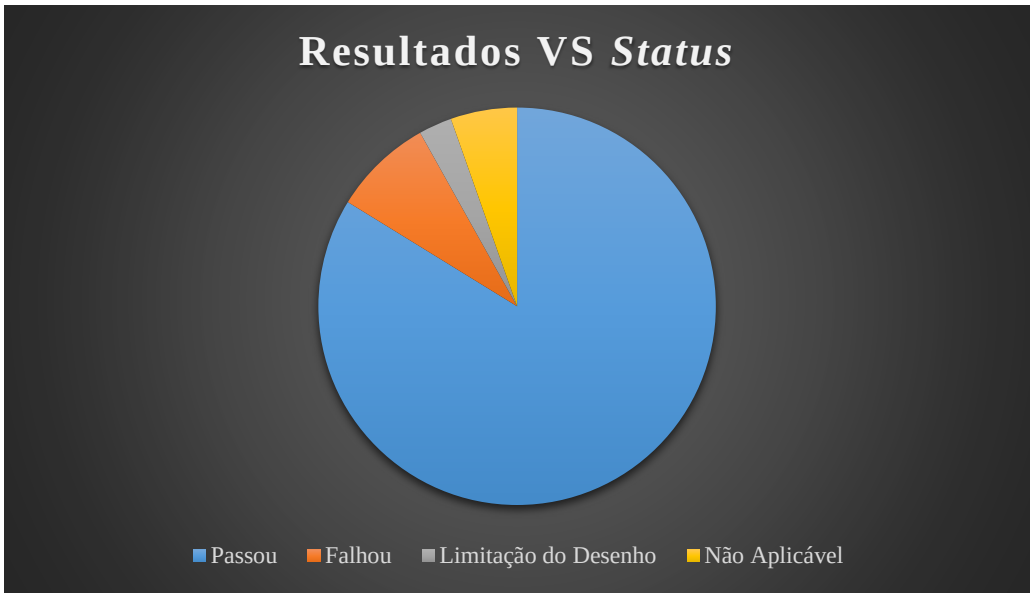

Gráfico 2- Resultados VS *status* CPE 2 xDSL HGW

Adaptado de: Laboratório de media (Altran, 2015)

No gráfico 2 consegue-se ter uma visão mais elucidativa relativa ao desenvolvimento dos testes, por classificação.

4.9.2. Considerações

A tabela 13 apresenta as considerações finais sobre a visão global do dispositivo, estas considerações estão organizadas por grau de gravidade onde: 1- significa crítico, 2- importante e 3- moderado.

Severidade 1-3	Nota	Descrição
1		
2	- FXS *status* can be read by ACS	-A impossibilidade de execução deste método pode limitar diversas funções
3	- FXS *status* can be read by ACS	- Não se consegue verificar o *status* do telefone quando ligado ou desligado do CPE

Tabela 13 – Grau de gravidade dos defeitos detetados

Adaptado de: Laboratório de media (Altran, 2015)

A tabela 13, tem como principal objetivo advertir de forma resumida o cliente acerca do grau de gravidade dos defeitos detetados no sentido de tomar a melhor providência possível.

4.10. Execução de Testes e *Report* CPE 3 xDSL HGW

É de salientar que a área de teste bem como os testes que foram submetidos aos demais dispositivos é exatamente a mesma que será utilizada para testar este dispositivo, no que concerne as caraterísticas são iguais ao dispositivo CPE 2 xDSL HGW. A figura 43 ilustra o dispositivo a ser testado denominado CPE 3 xDSL HGW bem como o cenário simplificado da infraestrutura necessária para execução de teste, dentro da nossa infraestrutura global.

Figura 43- Cenário de teste CPE 3 xDSL HGW

Adaptado de: Laboratório de media (Altran, 2015)

4.10.1. Resultados Globais dos Testes

Na tabela 14 observa-se o resultado da execução dos 37 casos de teste dentre os quais 20 passaram, 11 falharam, 0 limitação de design e 6 não aplicáveis.

Id	Nome do Teste	Comentários	Resultado Final
1	*Logging*		Passou
2	*WAN reconnect button*		Passou
3	*Bootstrap on for all WAN Intf*		Falhou
4	*Update and Rollback scenarios*		Passou
5	*NTP Servers*		Passou
6	*GetPararameterValue of all Tree*		Falhou
7	*Long-term Firmware updates via ACS*		Passou
8	*Devicelog readable by ACS*		Passou
9	*Active notification*		Falhou
10	*Inform Messages[PERIODIC]*		Passou
11	*ACS-Update during bootstrap message*		Não aplicável
12	*Inform if IP address changes on WAN Interface*		Passou
13	*Connection Request*		Passou
14	*Power off firmware*		Passou
15	*SET GET TR-098 PARAMETERS*		Falhou
16	*CWMP RPCs*		Passou
17	*Retry behaviour while ACS is down*		Falhou
18	*WiFi LAN Extension*		Passou
19	*Passive notification*		Falhou
20	*CR port is selected randomly*		Passou
21	*Config Rollback*		Passou
22	*Remote Access*		Falhou
23	*Connection Request*		Passou
24	*Passwords*		Falhou
25	*New CR port is selected if port gets occupied by user*		Passou
26	*USB Status*		Falhou
27	*DMZ Host configured*	Não implementada	Falhou
28	*SIP Account(s) Provisioning*	Não suporta o SIP	Passou
29	*CPE checks server certificate hostname*	O ACS não possui	Não aplicável
30	*While downloading or flashing firmware, phone is disabled*	Não suporta o SIP	Não aplicável
31	*FXS status can be read by ACS*	Não suporta o SIP	Falhou
32	*ACS-Firmware + Calls*	Não suporta o SIP	Passou
33	*TR111*	O CPE não suporta	Passou
34	*CPE checks server certificate validity period*	O ACS não possui	Não aplicável
35	*CPE checks server certificate*	O ACS não possui	Não aplicável
36	*TR143*	O CPE não suporta	Passou
37	*ACS communication is encrypted*	Não suporta	Não aplicável

Tabela 14 – Resultados globais dos testes sobre CPE 3 xDSL HGW

Adaptado de: Laboratório de media (Altran, 2015)

Relativamente aos resultados de execução de testes referidos na tabela 14, constata-se que 54% dos testes passaram, 30% falharam, 0% limitação de design e 16% não aplicável, para o cálculo das percentagens utilizou-se a regra de três simples que se pode observar abaixo.

Passou	Falhou	Limitação do design	Não aplicável
37x = 100 * 20	37x = 100 * 11	37x = 100 * 0	37x = 100 * 6
37x = 2000	37x = 1100	37x = 0	37x = 600
x = 2000 /37	x = 1100 /37	x = 0/37	x = 600/37
x = 54%	x = 30%	x = 0%	x = 16%

De forma simplificar a visualização dos resultados globais de execução dos testes sobre o CPE 3 xDSL HGW, elaborou-se o gráfico 3, com o objetivo de melhorar a perceção relativa ao grau de percentagem de execução dos testes.

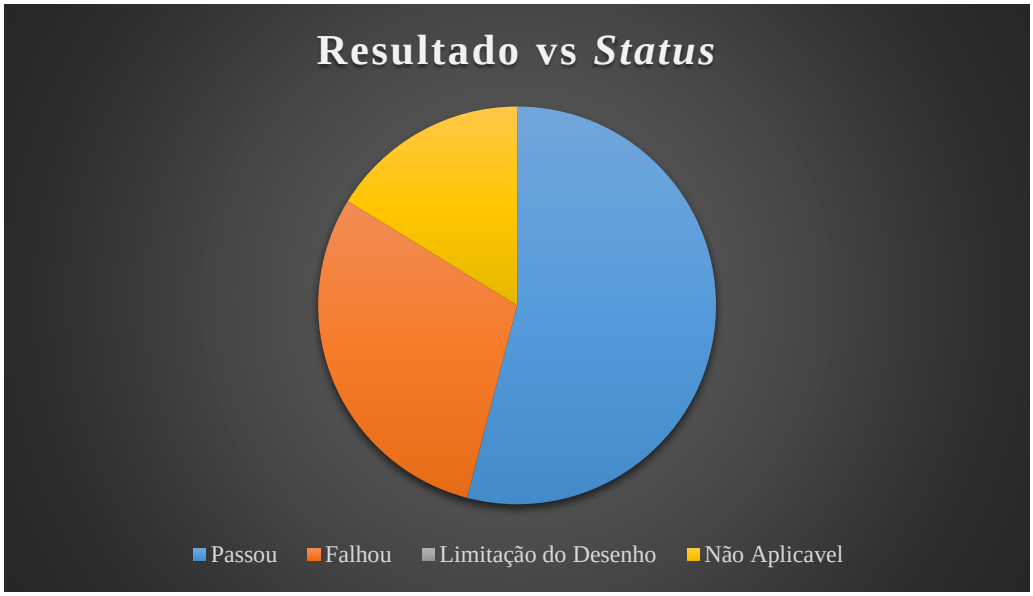

Gráfico 3- Resultados VS *status* CPE 3 xDSL HGW

Adaptado de: *HP Quality Center* (Altran, 2015)

No gráfico 3 consegue-se ter uma visão mais elucidativa relativa ao desenvolvimento dos testes, por classificação.

4.10.2. Considerações

A tabela 15 apresenta considerações finais sobre a visão global do dispositivo, estas considerações estão organizadas por grau de gravidade onde: 1- significa crítico, 2- importante e 3- moderado.

Severidade 1-3	Nota	Descrição
1	*GetPararameterValue of all Tree*	O CPE ao não permitir ao ACS ler a por completo a árvore de objeto limita a leitura de certos parâmetros.
2	*Active notification*	Não se consegue receber notificações no instante das alterações de um parâmetro.
3	*USB Status*	Não se consegue observar o estado de dispositivos usb.

Tabela 15 – grau de gravidade de defeitos detetados

Fonte: Laboratório de media (Altran, 2015)

A tabela 15, tem como principal objetivo informar de forma resumida o cliente acerca do grau de gravidade dos defeitos detetados no sentido de se tomar a melhor providência possível.

5. Conclusões e Perspetivas de Trabalho Futuro

Neste capítulo será elaborada uma breve síntese das atividades desenvolvidas ao longo do estágio e do seu contributo para o conhecimento do protocolo CWMP, assim como da execução de testes efetuados e os resultados que dele emanam, culminando com as principais conclusões, encerrando o capítulo com as perspetivas de trabalho futuro.

5.1. Conclusões

Concluídas as várias fases deste trabalho, desde a revisão da literatura, formação e aprendizagem, complementada com o trabalho prático, em que o objetivo principal foi a realização de testes CWMP em CPE de modo a garantir a conformidade de implementação do mesmo.
Pode se concluir que o protocolo CWMP tem tido grande aceitação globalmente pelos maiores fabricantes de dispositivos e fornecedores de serviços, por possibilitar que os mesmos sejam mais simples de difundir no que se refere às novas regras e configurações por grandes grupos de utilizadores, em função dos próprios perfis e dispositivos instalados. Mediante a utilização de um *Auto Configuration Server* (ACS), capaz de fornecer atualizações de software, alteração de configurações e recolha de dados para prevenir problemas dos CPE´s.

Tendo em conta que o CWMP é um protocolo da camada de aplicação para gestão remota, é possível concluir que, o conhecimento prévio de redes e tecnologias relacionadas constitui uma vantagem para o alcance dos objetivos traçados.

Foi ainda possível concluir, que face às questões levantadas na problemática no que se refere a submeter os equipamentos a testes antes de serem lançados para o mercado considera-se que deve constituir uma prática amplamente estratégica no sentido de refletir questões ao nível da garantia da qualidade de serviço, redução de custos e eficiência na resolução de problemas.

O processo de execução de testes permitiu concluir a viabilidade de submeter os dispositivos (CPE´s) ao processo de *Acceptance Testing* e/ou fase de aceitação, pelo que, constatou-se que apenas uma pequena percentagem de testes falharam e que estão tipificados no sentido de ser possível prevenir a ocorrência de problemas dos CPE´s.

Finalmente pode-se concluir que a adoção do protocolo CWMP para a gestão de dispositivos exerce um papel fundamental face à capacidade de gerir, monitorar e controlar uma grande quantidade de dispositivos ligados, para que isso ocorra o processo de testes de CPE desempenha um papel fundamental afim de permitir aos provedores de serviço manter elevados níveis de

qualidade e a experiência do utilizador final. Os resultados obtidos durante esta fase foram bastante satisfatórios no sentido de que o cliente junto do fabricante puderam evitar certos defeitos que foram corrigidos mediante o lançamento de novas versões da *firmware*.

5.2. Perspetivas de Trabalho Futuro

Como perspetiva de trabalho futuro sugere-se um maior envolvimento do cliente e de especialistas no processo de definição dos requisitos de teste bem como no processo de definição dos casos de teste, pelo facto de nalgumas situações detetar-se falta de clareza no que se refere ao processo de definição dos testes bem como o nível do detalhe dos *steps*.

Sugere-se que a Altran afira o grau de adequação do ACS atualmente em uso, pelo facto de ao longo do processo de execução de testes o mesmo ter-se revelado com nível de fiabilidade a necessitar de ser otimizado ao ponto de apresentar erros quase que impercetíveis obrigando a reiniciar, efetuar restauro e outras ações relacionadas para que o mesmo voltasse a funcionar.

Nesse sentido sugere-se que a Altran providencie ações de capacitação e/ou formação especializada para os engenheiros de teste no sentido de estes possuírem uma visão mais crítica diante dos fabricantes de dispositivos com o intuito de se atingirem maiores níveis de fiabilidade.

Referências

Altran, (2015). Historia. Disponível em 24 de setembro de 2015 em: http://www.altran.pt/sobre-nos/Altran-portugal/historia.html#.VhAr2PlViko

Andrews, K. M., Yim, P. (2015). Command Line Interface. Disponível em 24 de setembro de 2015 em: http://www.google.com/patents/US20150019199

Boavida, F., Bernardes, M., Vapi, P., (2011). Administração de Redes informáticas (2st ed.). Lisboa FCA – Editora de informática.

Broadband-Forum, (2004). About the Broadband Forum. Disponível em 24 de setembro de 2015 em: http://www.broadband-forum.org/about/forumhistory.php

Broadband-Forum, (2013a). TR-069 CPE WAN Management Protocol, Disponível em 24 de setembro de 2015 em: https://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf

Debian, (2015). debian the universal operating system . Disponível em 24 de setembro de 2015 em: https://www.debian.org/index.pt.html

Deutsche Bank, (2006). The dawn of technological convergence. Disponível em 24 de setembro de 2015 em: http://www.dbresearch.com/PROD/DBR_INTERNET_ENPROD/PROD0000000000198220.pdf

Directv2, (2015). Directv2 Altran. Disponível em 24 de setembro de 2015 em: https://directv2.altran.com

Elearning, (2015). Elearning Altran. Disponível em 24 de setembro de 2015 em: http://elearning.altran.pt/mycampusAltran

E-mail, (2015). E-mail Altran. Disponível em 24 de setembro de 2015 em: https://mail.altran.com

Freeacs, (2015). Free TR-069 ACS, Disponível em 24 de setembro de 2015 em: http://www.freeacs.com/

Frisch, M. (2015). Todas as Frases de Max Frisch. Disponível em 24 de setembro de 2015 em: http://www.frasesfamosas.com.br/frases-de/max-frisch/

GCA, (2015). GCA Altran. Disponível em 24 de setembro de 2015 em: http://gca.altran.pt/gca

Hermes, (2015). Portal Hermes. Disponível em 24 de setembro de 2015 em: https://hermes.altran.com/

HGI, (2004). About the Broadband Forum. Disponível em 24 de setembro de 2015 em: http://www.homegatewayinitiative.org/

Incognito, (2013). Auto Configuration Server, TR-069. Disponível em 24 de setembro de 2015 em: https://www.incognito.com/tips-and-tutorials/faq-tr-069/

IETF, (1990). A Simple Network Management Protocol (SNMP. Disponível em 24 de setembro de 2015 em: https://www.ietf.org/rfc/rfc1157.txt

IETF, (2011a). Network Configuration Protocol (NETCONF). Disponível em 24 de setembro de 2015 em: https://tools.ietf.org/html/rfc6241

IETF, (2006b). Using the NETCONF Configuration Protocol over Secure SHell (SSH). Disponível em 24 de setembro de 2015 em: https://tools.ietf.org/html/rfc4742

IETF, (2006c). Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP). Disponível em 24 de setembro de 2015 em: https://tools.ietf.org/html/rfc4744

IETF, (2006d). Using NETCONF over the Simple Object Access Protocol (SOAP). Disponível em 24 de setembro de 2015 em: https://tools.ietf.org/html/rfc4743

IETF, (2009e). NETCONF over Transport Layer Security (TLS). Disponível em 24 de setembro de 2015 em: https://tools.ietf.org/html/rfc5539

IETF, (2014f). Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing draft-ietf-httpbis-p1-messaging-26. Disponível em 24 de setembro de 2015 em: https://tools.ietf.org/html/draft-ietf-httpbis-p1-messaging-26

ITU, (2004). Definition of Next Generation Network. Disponível em 24 de setembro de 2015 em: http://www.itu.int/ITUT/studygroups/com13/ngn2004/working_definition.html

Mauro, D., Schmidt, K. (2005). Essential SNMP (2st ed.). E.U.A Sebastopol: O'Reilly Media.

Mauro, D., Schmidt, K. (2005a). Essential SNMP (2st ed.). E.U.A Sebastopol: O'Reilly Media.

Mersh, R. (2012), Simplifying remote management of billions of devices. Global-ICT, p. 1.

Pinto, P. (2010) Redes – Sabe o que é o modelo OSI?, Disponível em 24 de setembro de 2015 em: http://pplware.sapo.pt/tutoriais/networking/redes-sabe-o-que-e-o-modelo-osi/

Portal-Colaborador, (2015).Portal do Colaborador Altran. Disponível em 24 de setembro de 2015 em: http://portalcolaborador.altran.pt.

Qualidade, (2015). Qualidade Altran. Disponível em 24 de setembro de 2015 em: https://qualidade.Altran.pt/login.php.

RFC 6241, (2011). Network Configuration Protocol (NETCONF). Disponível em 24 de setembro de 2015 em: https://tools.ietf.org/html/rfc6241

RFC 4741, (2006). NETCONF Configuration Protocol. Disponível em 24 de setembro de 2015 em: https://tools.ietf.org/html/rfc4741

Rouse, M. (2005). Definition of convergence. Disponível em 24 de setembro de 2015 em: http://whatis.techtarget.com/definition/convergence

Stephenson, N. (1999). In the Beginning was the Command Line, Disponível em 24 de setembro de 2015 en: http://faculty.georgetown.edu/irvinem/theory/Stephenson-CommandLine-1999.pdf

Techopedia, (2015). Command Line Interface (CLI). Disponível em 24 de setembro de 2015 em: https://www.techopedia.com/definition/3337/command-line-interface-cli

UPnP-Forum, (2008). UPnP™ Device Architecture 1.1. Disponível em 24 de setembro de 2015 em: http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf

Valente, B. (2011). Um Middleware Para a Internet das Coisas. Porto: Universidade do Porto.

W3C, (2007). SOAP Version 1.2 Part 1: Messaging Framework (Second Edition). Disponível em 24 de setembro de 2015 em: http://www.w3.org/TR/soap12-part1/

Winehq, (2013). Text mode programs. Disponível em 24 de setembro de 2015 em: https://www.winehq.org/docs/wineusr-guide/cui-programs