Infra-Estrutura do Projecto SEMCABO-WIFI

Armando de Jesus Ventura

Orientador: Professor Luís Rato

Tese para o Grau de Mestre

Universidade de Évora
Portugal
Outubro de 2009

Esta dissertação não inclui as críticas e sugestões feitas pelo júri.

Infra-Estrutura do Projecto SEMCABO-WIFI

Armando de Jesus Ventura

Orientador: Professor Luís Rato

Tese para o Grau de Mestre

Universidade de Évora
Portugal
Outubro de 2009

Esta dissertação não inclui as críticas e sugestões feitas pelo júri.

Dedicado

ao meu filho.

Infra-Estrutura do Projecto SEMCABO-WIFI

Armando de Jesus Ventura

Mestrado em Engenharia Informática
Outubro 2009

Resumo

Esta tese consiste no estudo, implementação e desenvolvimento da infra-estrutura para o projecto SEMCABO-WIFI. Este projecto está inserido na empresa SemCabo, com o objectivo de levar a Internet aos clientes sob a forma de *hotspots* ou no acesso à ultima milha (*Last Mile Access*) à casa dos residentes. O projecto também deu origem à própria empresa, levando esta a ISP desde Setembro de 2007. Numa primeira fase, é feita abordagem a Sistemas de *Authentication*, *Authorization* e *Accounting* para ISPs, na vertente WI-FI e apresentadas possíveis soluções comercias e *open source*. Em seguida, é apresentado a empresa SemCabo, vertente comercial e tecnológica. O sistema base da SemCabo é referido, contemplando a tecnologia de suporte, rede, equipamentos activos, módulos de emissão de sinal WI-FI, segurança, monitorização e portal de autenticação. Os servidores base são indicados posteriormente, sendo efectuado a apresentação de todos os servidores com suporte ao projecto, incluindo alguns pormenores de configuração. São apresentados equipamentos e sistemas utilizados para controlo de acesso à rede (NAS), sendo igualmente descritos pormenores de configuração.

Infrastructure of the SEMCABO-WIFI Project

Armando de Jesus Ventura

Master in Informatics Engineering
October 2009

Abstract

This thesis is about the study, implementation and development of the infrastructure created for the SEMCABO-WIFI project. This project is inserted in the company SemCabo, with the objective to bring the Internet to costumers in the form of hotspots or access in last mile to the house of residents. The project also originated the company and led the company to ISP since September 2007. In the first fase, the approach is about Systems Authentication, Authorization and Accounting for WISPs and presented possible commercial and open source solutions. In next, the SemCabo company is presented and described their technological and commercial aspects. The base system of the SemCabo is refered, considering the support technology, network equipment, modules emission signal WI-FI, security, monitoring and portal authentication module. Base servers of the SemCabo project are shown, A presentation of all the servers that support the project is made, including some details of the configuration. The equipment and systems used to control network access (NAS) are presented, details of configuration are also described.

Agradecimentos

Para que tudo terminasse da melhor forma, todo o trabalho de investigação, de desenvolvimento que só foi possível, não só apenas pelo esforço pessoal, mas também de uma série de pessoas que me apoiaram e suportaram de certa forma esse esforço. Assim, aqui fica uma pequena lista de pessoas a quem gostaria de expressar o meu sincero agradecimento.

As primeiras pessoas que gostaria de agradecer, são sem dúvida a minha família, filho, esposa, pais, irmãs e sobrinhos, sem eles não haveria motivação para nada.

Um agradecimento especial ao meu filhote.

Aos meus colegas da empresa, de aturarem os bons e maus momentos que passamos juntos.

Ao Professor Luís Rato, orientador da Tese, pela sua boa vontade e disponibilidade demonstrada.

A todos os que de alguma forma contribuíram para a realização deste trabalho, o meu obrigado.

Conteúdo

Lista de Figuras

Lista de Tabelas

Acrónimos e Abreviaturas

TCP Transport Control Protocol

FTP File Transport Protocol

RADIUS Remote Authentication Dial-In User Service

EAP Extensible Authentication Protocol

PEAP Protected Extensible Authentication Protocol

LEAP Lightweight Extensible Authentication Protocol

UAM Universal Access Method

PAP Password Authentication Protocol

CHAP Challenge Handshake Authentication Protocol

SSL Secure Socket Layer

AAA Authentication, Authorization and Accounting

ISP Internet Service Provider

DNS Domain Name System

SSH Secure Shell

SSL Secure Socket Layer

HTTP Hypertext Transfer Protocol

HTTPS HyperText Transfer Protocol Secure

WI-FI Wireless Fidelity

WDS Wireless Distribution System

LAN Local Area Network

WLAN Wireless Local Area Network

PHP Hypertext Preprocessor

XML eXtensible Markup Language

HTML HyperText Markup Language

NAS Network Access Server

NAT Network Address Translation

PPPOE Point-to-Point Protocol over Ethernet

PPTP Point-to-Point Tunneling Protocol

L2TP Layer 2 Tunneling Protocol

IPSec Internet Protocol Security

ADSL Asymmetric Digital Subscriber Line

XDSL Digital Subscriber Line

VOIP Voice Over Internet Protocol

WIMAX Worldwide Interoperability for Microwave Access

LDAP Lightweight Directory Access Protocol

NAT Network Address Translation

SPI Stateful Packet Inspection

IPS Intrusion Prevention System

DoS Denial of Service

QoS Quality of Service

VLAN Virtual Local Area Network

SMTP Simple Mail Transfer Protocol

POP3 Post Office Protocol

IMAP Internet Message Access Protocol

IMAPS Internet Message Access Protocol Secure

SQL Structured Query Language

Capítulo 1

Introdução

As tecnologias sem fios como o WI-FI, têm vindo a desencadear novos modelos de negócio, e novas formas de comunicação. O surgimento de *hotspots* públicos e privados, o acesso na última milha (*Last Mile*) à casa dos residentes, são um exemplo real da aplicação destas tecnologias.

A Empresa SemCabo, é um ISP/WISP (ICP-ANACOM N.º17/2007) recente, desenvolvendo projectos com recurso a tecnologias sem fios. Um dos principais projectos desta empresa é o projecto SEMCABO-WIFI, o qual proporciona o acesso à Internet de forma gratuita e paga, em diversas regiões.

Esta tese, composta por sete capítulos, visa descrever o trabalho efectuado, no estudo, decisão, implementação e desenvolvimento de toda a Infra-Estrutura do Projecto SEMCABO-WIFI.

O capítulo segundo, tem como objectivo, abordar o Estado da Arte, respeitante a sistemas utilizadas por ISPs com vertente WI-FI. São referidas algumas soluções existentes no mercado, incluindo sistemas comerciais e *open source.*

No capítulo terceiro, é apresentado a empresa SemCabo. É descrito o seu surgimento, as políticas de desenvolvimento, a preferência em soluções *Open Source*, os serviços disponibilizados e os projectos principais, nomeadamente, os relacionados com o projecto SEMCABO-WIFI. É apresentado o organograma, referindo os seus recursos humanos, as parcerias tecnológicas no fornecimento de Internet e de equipamentos, bem como os clientes actuais com algum peso para a empresa. Por fim, uma abordagem ao NOC (*Network Operator Center*), enumerando os servidores

existentes actualmente.

Sistema Base da Semcabo, é descrito no capítulo quarto: descrição da rede; apresentação dos equipamentos activos utilizados e as suas funcionalidades; exposição dos servidores implementados para suporte ao projecto; estrutura dos módulos de emissão de sinal WI-FI; abordado a segurança no NOC e nos módulos de emissão; incluí os sistemas de acesso à rede (NAS); o sistema de monitorização criado para controlo e *status* dos equipamentos, e ainda o portal de autenticação para validação de utilizadores através do *browser*.

O suporte do projecto SEMCABO-WIFI, é assegurado pelos servidores base, descritos no capítulo quinto: os servidores de nomes de domínio, utilizados para resolução dentro e fora da rede; o servidor WEB, alojamento do portal da SemCabo e de autenticação; o servidor de Mail, utilizado para as contas dos assinantes de acesso à Internet e funcionários de empresas cliente; o servidor RADIUS, sistema de AAA[1] utilizado para controlo dos acessos à rede; e ainda outros servidores como, Projects (gestão documental e de projectos), VPN (*Virtual Private Network*) e Backups.

Equipamentos intermédios no controlo de Acesso à Rede (NAS[2]) são descritos no capítulo sexto. Incluindo soluções de NAS diferenciadas consoante a área abrangente, o tipo de autenticação utilizada e o número de utilizadores em simultâneo.

Por fim, é apresentado no capitulo sétimo, as considerações finais e trabalhos futuros.

A princípal contribuição deste trabalho, é o estudo e implementação de um sistema completo e funcional de autenticação para um Provedor de Acesso à Internet (ISP).

[1] Authentication, Authorization and Accounting
[2] Network Access Server

Capítulo 2

Sistemas de Authentication, Authorization e Accounting para ISPs

2.1 Introdução

Neste capítulo, é feito uma abordagem ao Estado da Arte. Sistemas e tecnologias utilizados por ISPs com vertente WI-FI. São referidas soluções comerciais e *open source.*

2.2 Tecnologias e Protocolos utilizados por ISPs

No que respeita a ISPs[1] com funcionalidades de autenticação para WI-FI, ou outro tipo de tecnologia para transferência de dados, mas dando ênfase em autenticação para sistemas sem fios, enumeram-se alguns conceitos importantes a ter em conta actualmente.

- RADIUS[2]
  - O RADIUS teve surgimento em Junho de 2000, é um protocolo AAA[3]

[1] Internet Service Providers
[2] Remote Authentication Dial-In User Service
[3] Authentication, Authorization and Accounting

para controlo de acessos à rede [1]. É um Sistema *standard* de autenticação remoto presente na maioria de todos os sistemas operativos e equipamentos de rede sendo imprescindivel o seu uso por ISPs.

- NAS[4]
  - Tendo como data de início Julho de 2000, este foi desenvolvido para promover acesso a recursos remotos [2], sendo usado em equipamento intermédio entre o equipamento *client* e o servidor RADIUS. Tem a funcionalidade de permitir o acesso à Internet ou a outros recursos através de vários tipos de autenticação. O seu uso é imprescindível por ISPs.
- UAM[5]
  - Este método consiste em interceptar a ligação TCP[6] e redireccionar para um portal de autenticação, onde é pedido ao utilizador que introduza um *username* e *password* para aceder à Internet. É normalmente utilizado através de *Captive Portal*[7] na implementação de hotspots, sendo um método bastante adoptado por ISPs.
- 802.1X
  - O 802.1X com início em Junho de 2001, é um protocolo utilizado para controle de acesso à rede [3]. O qual suporta acessos, sendo por utilizador e por máquina. Tem a possibilidade de centralização de utilizadores, bem como, suporte a RADIUS e *roaming*. É utilizado por empresas, Campus universitários e adoptado por alguns ISPs.
- PPPOE[8]

[4]Authentication, Authorization and Accounting
[5]Universal Access Method
[6]Transport Control Protocol
[7]Portal Cativo, utilizado para autenticação através da web
[8]Point-to-Point Protocol over Ethernet

- O PPPOE desenvolvido em Fevereiro de 1999, é um protocolo de conexão e autenticação mais utilizado em redes *ethernet* e presente na maioria dos equipamentos *client* existentes no mercado. É utilizado quer em redes com e sem fios, torna possível o controlo de várias funcionalidades como a definição de largura de banda por utilizador, a identificação de utilizador, a contabilização em tempo de sessão *online*, entre outras [4]. Neste protocolo o *username* e *password* podem ser encriptados entre o equipamento *client* e o NAS, sendo o outro tráfego não encriptado, salvo o uso de protocolos de encriptação. Este protocolo é muito utilizado por ISPs.

- PPTP[9]

  - Foi desenvolvido para implementação de redes privadas virtuais [5], tendo surgido em Julho de 1999. Este permite privacidade no tráfego gerado, sendo uma opção utilizada por alguns ISPs para autenticação de utilizadores quer em rede com e sem fios.

- L2TP/IPSec[10]

  - O L2TP/IPSec tendo surgido em Novembro de 2001, é uma junção de dois protocolos, sendo eles L2TP e IPSec. O IPSec é usado para dar segurança aos pacotes L2TP. São utilizados para a criação de VPNs e também, utilizados por ISPs para conexão à rede. Têm a possibilidade de oferecer confidencialidade e autenticação segura [6].

- EAP[11]

  - O EAP criado em Março de 1998, é um mecanismo seguro para troca de mensagens de autenticação, o qual permite que as mensagens entre os equipamentos *client*, NAS e RADIUS sejam efectuadas de forma segura

[9]Point-to-Point Tunneling Protocol
[10]Layer 2 Tunneling Protocol/Internet Protocol Security
[11]Extensible Authentication Protocol

[7]. Não é um mecanismo de autenticação específico, o EAP fornece algumas funções comuns de negociação de mecanismo de autenticação.

Os ISPs usualmente utilizam RADIUS para *Authentication, Authorization* de utilizadores e *Accounting* para *status* ou contabilização do serviço, utilizam ainda os equipamentos NAS e equipamentos *client.* Em cenário de funcionamento, o equipamento *client* solicita acesso aos recursos do NAS, este por sua vez autentica o *client* no servidor RADIUS, se for válido o NAS decide o nível de autorização apropriado consoante os privilégios e cede acesso à rede.

Este sistema é relativamente seguro devido à partilha de uma chave secreta entre ambos os sistemas, o servidor RADIUS e NAS. Todas as mensagens são trocadas de forma segura utilizando o protocolo EAP[12] ou suas variantes (PEAP[13], LEAP[14], etc).

A Fig. 2.1 apresenta o funcionamento usual de autenticação num ISP.

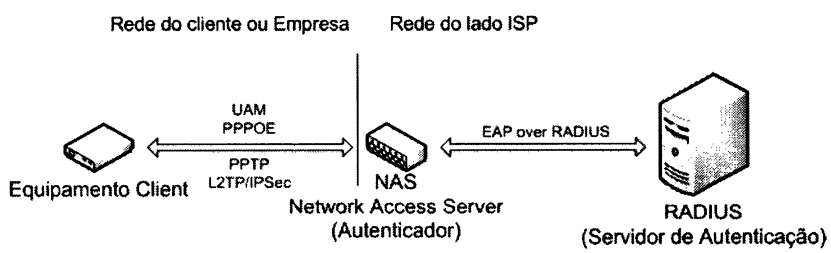

Figura 2.1: Funcionamento usual de Autenticação num ISP

No que consiste ao método de autenticação do lado do equipamento *client*, podemos salientar o método UAM[15]. Este método consiste em o utilizador introduzir *username* e *password* no *browser* enquanto tenta aceder à Internet sem ter as devidas credenciais inseridas. Dentro deste método temos a possibilidade de utilizar os protocolos PAP[16], CHAP[17] e SSL[18] para transferência de dados entre o equipa-

[12]Extensible Authentication Protocol
[13]Protected Extensible Authentication Protocol
[14]Lightweight Extensible Authentication Protocol
[15]Universal Access Method
[16]Password Authentication Protocol
[17]Challenge Handshake Authentication Protocol
[18]Secure Socket Layer

mento *client* e o NAS. Tanto os protocolos CHAP e SSL encriptam a informação introduzida pelo utilizador, já o mesmo não acontece com o protocolo PAP, sendo os dados enviados em texto simples.

Existe também, a variante de autenticação pelo endereço de MAC do equipamento *client* dentro do método UAM, sendo o próprio endereço de MAC o *username*, ficando a *password* definida no NAS.

Outra possibilidade de autenticação é através do protocolo 802.1x, este tipo de autenticação é mais utilizado para redes empresariais, não propriamente por ISPs. Este é um método que permite eliminar o chamado NAS, pois o próprio *Access Point* faz de autenticador, fazendo apenas a passagem das credenciais até ao servidor RADIUS, permitindo, ou não, o acesso à rede por parte do equipamento *client*. Ver Fig. 2.1 para topologia de rede para 802.1x.

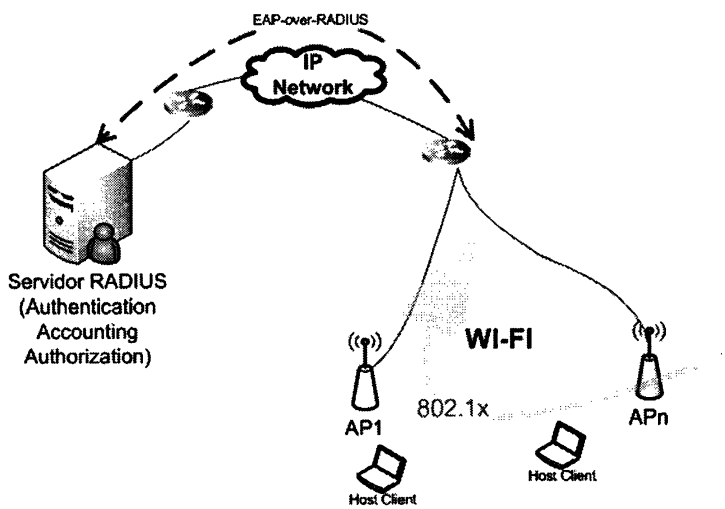

Figura 2.2: Topologia de rede para 802.1x

Da perspectiva de autenticação os protocolos mais utilizados, são PPPOE, PPTP e L2TP/IPSec [4][5][6]. Em sistemas com acessos à Internet com a ADSL[19] ou suas variantes, temos o PPPOE como sistema principal de autenticação, igualmente podemos considerar este como o protocolo de eleição utilizado pelos ISPs de vertente

[19] Asymmetric Digital Subscriber Line

WI-FI. Este protocolo está presente em quase todos os equipamentos *client*, o mesmo já não acontece com os outros dois métodos referenciados. Permitindo a encriptação dos dados de autenticação, o PPPOE torna-se seguro quanto à salvaguarda das credenciais de cada utilizador, no entanto, já não acontece o mesmo quanto ao tráfego do equipamento *client* até à *gateway* (o mesmo equipamento que o NAS).

Os outros dois protocolos, mais seguros, conhecidos por criarem túneis encriptados, tanto as credenciais dos utilizadores como o tráfego entre o equipamento *client* e a *gateway* são encriptados. Assim, evitam-se ataques como *man-in-the-middle*, visualização da informação, modificação da informação e controlo de sessão. Deve-se salientar que apenas são encriptados os dados desde o equipamento *client* até à *gateway* (NAS), como se pode observar na Fig. 2.2. O tráfego depois do NAS à Internet não é encriptado, salvo com a utilização de protocolos próprios de encriptação.

A Fig. 2.2 ilustra os protocolos de autenticação mais utilizados.

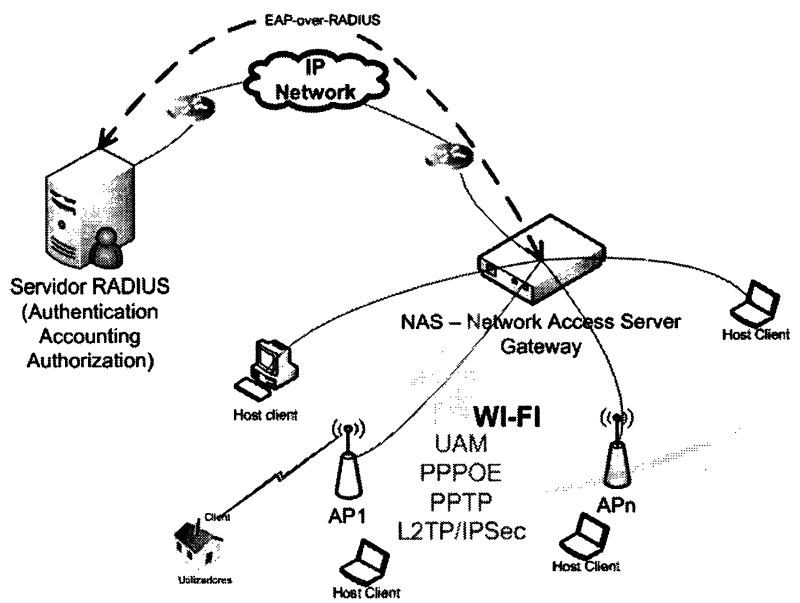

Figura 2.3: Métodos de Autenticação mais utilizados

2.3 Sistemas Comerciais / Open Source

Numa perspectiva de sistema completo, podemos considerar uma junção de várias tecnologias e equipamentos com funções específicas. Actualmente são poucos os pro-

dutos que possam oferecer uma completa funcionalidade para as necessidades totais de um ISP. Assim, existe normalmente a necessidade de agrupar várias tecnologias como bases de dados, RADIUS, NAS, sistemas de *Billing* e *Ordering*, software para gestão de utilizadores e *software* de monitorização. São poucos os produtos considerados sistemas "chave-na-mão".

Abaixo indicam-se alguns sistemas comerciais e *open source* mais conhecidos e utilizados actualmente.

2.3.1 Comerciais

2.3.1.1 Aradial Radius Server

Com início em 1997 [8], este sistema oferece várias possibilidades desde pequenos a grandes ISPs nas áreas de DSL, VOIP[20], Mobile, WI-FI, WIMAX[21]. É um sistema proprietário onde incorpora RADIUS, sistema de *billing* e *ordering*, gestão de utilizadores e monitorização. Tem a possibilidade de conectividade a várias bases de dados, como MySQL, MS SQL Server, Oracle e LDAP. Está disponível nas plataformas Microsoft, Linux e Unix. Possibilidade de interoperabilidade com vários NAS: cisco, Nomadix, Colubris, Handlink, ValuePoint, Linksys, Zyxel entre outros.

2.3.1.2 Internet Authentication Service (IAS)

RADIUS Sever da Microsoft [9], desenvolvido em Janeiro de 2003, está disponível nas versões server da Microsoft, quer em 2003 Server e 2008 Server, é uma possibilidade de implementação para ISPs. Este sistema funciona directamente com o *Active Directory* impossibilitando a consulta directa através de SQL, sendo necessário a replicação da base de dados para o *Active Directory* ou vice-versa. O IAS é compatível com alguns NAS, salientam-se o NAS da Proxim, Cisco, Interasys, 3com, Linksys, Nomadiz, Colubris e ainda Zyxel.

[20] Voice Over Internet Protocol
[21] Worldwide Interoperability for Microwave Access

2.3.1.3 Cisco ACS

RADIUS da cisco, é utilizado por várias empresas de pequena, média e grande dimensão, para autenticações dial-up, DSL ou WI-FI [10]. Neste sistema, é necessário a versão correcta de IOS[22] para activação e funcionalidade de RADIUS. No entanto, para a funcionalidade de NAS, a Cisco incorpora no seu *software* o Cisco VPDN Server, o qual poderá observar na Tabela 2.1 as respectivas funcionalidades.

2.3.1.4 RouterOS

O RouterOS teve início em 1999, é um sistema em grande crescimento e desenvolvimento. Actualmente, está com grande aceitação no mercado pelas inúmeras funcionalidades, sendo adoptado em alguns casos em vez de sistemas com grande presença no mercado como a cisco. É baseado em Linux, oferece a possibilidade de integrar RADIUS, NAS e gestão de utilizadores [11]. O sistema NAS, suporta mais funcionalidades que qualquer outro concorrente directo, como pode ser observar na Tabela 2.1. Tem ainda, a possibilidade de funcionar como NAS e *Access Point* em simultâneo.

2.3.1.5 StarOS

O StarOS começou a ser desenvolvido a partir de 2006, este teve como objectivo de ser uma solução simples e de baixo custo para WISPs[23] [12]. Contempla algumas funcionalidades importantes como o método de autenticação PPPOE. É utilizado apenas como solução NAS e em sistemas embutidos para *Access Points.*

[22]Internetwork Operating System
[23]Wireless Internet Service Providers

	RouterOS	Cisco	Chillispot	StarOS
Hotspot authentication / accounting	✓		✓	
Hotspot auto disconnect	✓		✓	
Hotspot bandwidth management	✓		✓	
Hotspot static IP address	✓			
PPPoE authentication / accounting	✓	✓		✓
PPPoE auto disconnect	✓	✓		✓
PPPoE bandwidth management	✓	✓		✓
PPPoE static IP address	✓	✓		✓
PPtP authentication / accounting	✓	✓		
PPtP auto disconnect	✓	✓		
PPtP bandwidth management	✓	✓		
L2tP authentication / accounting	✓	✓		
L2tP auto disconnect	✓	✓		
L2tP bandwidth management	✓	✓		
Wireless access list support	✓			
Hotspot MAC authentication	✓			

Tabela 2.1: Funcionalidades NAS - RouterOS / Cisco / Chillispot / StarOS

2.3.2 Open Source

2.3.2.1 Freeradius

Desenvolvido em Junho de 1999, é onsiderado o servidor RADIUS *open source* mais popular em todo o mundo, este autentica mais de 100 milhões de utilizadores diariamente e utiliza os protocolos de autenticação mais comuns. O Freeradius pode ser instalado em praticamente todas as distribuições Linux, Unix e também em Windows. Várias estimativas definem que o servidor Freeradius ronda 1/3 de todos os utilizadores que se autenticam na Internet, ficando os restantes em igual parte pelo radius da Microsoft (IAS) e da Cisco (ACS). Este suporta pedidos em *proxying* com tolerância a falhas, balanceamento de pedidos, bem como a possibilidade de acesso a vários tipos de bases de dados como *back-end* [13].

O Freeradius contempla ainda uma aplicação desenvolvida para administração e gestão de utilizadores denominada *dial-up admin,* esta suporta as seguintes características:

- Utilizadores em LDAP

- Utilizadores e grupos em base de dados SQL (MySQL, PostgreSQL e Oracle)
- Relatórios de acessos
- Testes para o correcto funcionamento do servidor
- Estatísticas de utilização dos utilizadores

Outras aplicações *open source* podem ser utilizadas para gestão, como o *phpMyPrepaid* [14] e *DaloRadius* [15].

2.3.2.2 ChilliSpot

Utilizado apenas como NAS, o ChilliSpot controla acessos de utilizadores com ou sem fios [16]. Este suporta UAM que actualmente é o *standard* para hotspots públicos e também suporta o protocolo 802.1x. O ChilliSpot está disponível para as plataformas Linux (Redhat, Febora, Debian, Mandrake) e para dispositivos embutidos com o sistema Linux OpenWRT, DD-WRT e Coova.

Capítulo 3

A Empresa Semcabo

3.1 Introdução

Este capítulo apresenta a empresa SemCabo, o seu surgimento, as políticas de desenvolvimento, a preferência em soluções *Open Source*, os serviços disponibilizados e os projectos principais. É apresentado o organograma, referindo os seus recursos humanos. São indicadas algumas parcerias tecnológicas no fornecimento de Internet e de equipamentos. Ainda é referido os clientes actuais e efectuado uma abordagem ao actual NOC (*Network Operator Center*).

3.2 Apresentação

A SemCabo é uma empresa criada em 2004 e opera dentro do ramo das novas tecnologias. Sediada em Sines, com Licença de ISP/WISP N.º17/2007, atribuída pela ICP-ANACOM para comunicações electrónicas, a SemCabo quer ter uma palavra activa no desenvolvimento deste país, através da investigação, desenvolvimento e implementação de projectos inovadores, não querendo de forma alguma ser considerada mais uma empresa dentro das novas tecnologias.

A empresa nasceu com a ideia de um projecto, sendo ele posteriormente designado SEMCABO-WIFI, resultante da experiência dos seus criadores e das necessidades que sentiram ao visitarem outras localidades/países em obterem informações de várias ordens. O projecto, pretende ser a porta de entrada para todos aqueles que

visitam uma determinada região, com objectivo de ser o ponto central na divulgação local, através das promoções do que nela existem e funcionando como uma ferramenta eficaz para o desenvolvimento da região. O projecto assenta na utilização da Internet a custos reduzidos e/ou mesmo gratuitos através da utilização da tecnologia WI-FI.

3.3 Serviços

Actualmente a Semcabo oferece os serviços apresentados abaixo:

- SEMCABO-WIFI
- Semcabo ADSL / XDSL / SDSL
- Condomínio Digital
- Hosting (Plataforma Linux)
- Serviço de Mail
- Revenda Hosting
- Registo de Domínios
- Serviço de DNS
- Aluguer de Servidores Dedicados/Virtualizados
- Criação de Websites
- Configuração e Instalação de Servidores (Linux e Windows Server)
- Cablagem Estruturada (UTP e Fibra)
- Ligações Wireless Ponto-a-Ponto ou Multi-ponto
- Redes Wireless Publicas e/ou Privadas (Realização de Projectos / Análise de Espectro)
- Configuração de VPNs (PPTP, L2TP/IPSec)

- Multimédia (Spots Publicitários, Video Streaming)

3.4 Projectos

Projectos em desenvolvimento a SemCabo salienta alguns dos seus principais projectos.

- CMS[1] SemCabo, desenvolvido sob a tecnologia LAMP[2]. Este projecto é utilizado para a maioria dos sites desenvolvidos pela SemCabo, contempla imensas funcionalidades, favorece a simplicidade de utilização para os utilizadores na actualização de conteúdos. Este CMS pode ser consultado através do seguinte URL `http://www.semcabo.pt/?lv1=mnpri&lv2=32`

- Condomínio Digital, consiste em partilhar o acesso à Internet para todos os condóminos, sinal WI-FI distribuído dentro e fora do condomínio.

- SEMCABO-WIFI, projecto principal da empresa, contempla conceitos como *hotspot*[3] e *Last Mile Access* (Acesso na Última Milha). Este consiste na utilização da Internet a custos reduzidos e/ou mesmo gratuitos através da utilização da tecnologia WI-FI.

  - Em relação aos *hotspots*, existe a "net à pala", consiste no acesso gratuito à Internet com velocidades e tempos limitados de acesso, sessões de 10 em 10 minutos onde os utilizadores são redireccionados ao portal de publicidade para nova autenticação. Existe também o Voucher, este consiste num acesso pago, é utilizado por tempos de acesso e por limites de download.

  - No que consiste ao *Last Mile Access*, é instalado na casa dos clientes um equipamento que se conecta automaticamente a um dos emissores da SemCabo. Este tipo de acesso só está disponível para assinantes do serviço em causa.

[1] Content Management System
[2] Arquitectura Linux, Apache, Mysql, PHP
[3] pontos de acesso sem fios à Internet

- Portal de Publicidade, este consiste na divulgação de informação local onde o utilizador se conecta à rede SEMCABO-WIFI, quer seja numa localidade, numa marina, parque de campismo, hotel, etc. Neste Portal é ainda apresentado ao utilizador, informação relevante sob a forma de hipertexto ou multimédia.

3.5 Organograma

A SemCabo é composta por 6 elementos permanentes. Constituída por uma equipa jovem e dinâmica, com idades compreendidas entre os 25 e os 34 anos. A organização assenta em departamentos como pode ser observado na Fig. 3.1 abaixo.

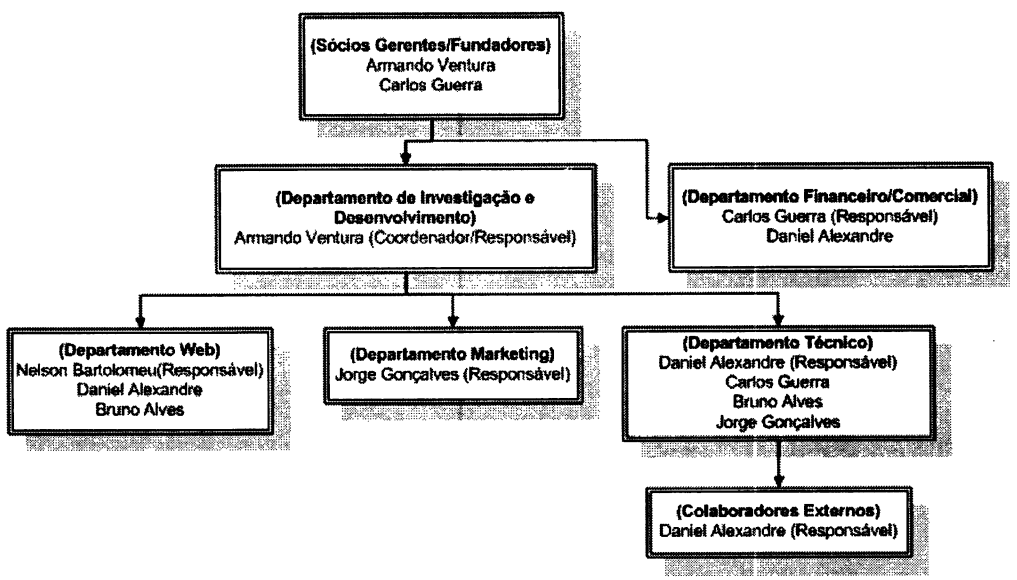

Figura 3.1: Organograma

3.6 Parcerias Tecnológicas

A SemCabo desde o seu início valoriza o conceito de parceria. Está aberta a novos desafios e projectos em conjunto com outras entidades, promove a partilha de esforços e não o isolamento empresarial. Na tabela 3.1 abaixo são apresentadas algumas empresas parceiras.

Parceiro	Breve Apresentação
Senao	Actualmente uma das maiores e prestigiadas empresas a nível global de soluções wireless. Empresa fornece uma grande variedade de equipamentos wireless.
ClaraNet	Criada no início de 1995 tendo sido o primeiro ISP privado em Portugal, a ESOTÉRICA S.A, foi adquirida em Maio de 1999 pela multinacional norte-americana Via Net Works, Inc. e em Julho de 2005, pelo grupo europeu CLARANET.
OpenCode	A openCode é uma empresa moderna de projecto e criação de aplicações informáticas que aplica alguns dos mais actuais paradigmas de desenvolvimento de software.
Engenius	Fundada em 1999, a ENGENIUS Tecnologies, Inc, fornece produtos Wireless de excelente qualidade e performance.
cerbyte	Empresa parceira para revenda e instalação de equipamentos para acesso à Internet do projecto SEMCABO-WIFI.
techsolutions	Empresa parceira para design e revenda de serviços Semcabo.
SemVirus	Empresa parceira para revenda de serviços Semcabo e instalação de equipamentos para acesso à Internet do projecto SEMCABO-WIFI.
atinovation	Empresa parceira para revenda de serviços Semcabo e instalação de equipamentos para acesso à Internet do projecto SEMCABO-WIFI.

Tabela 3.1: Parceiros Tecnológicos

3.7 Clientes actuais

A empresa contabiliza 1971 utilizadores do projecto SEMCABO-WIFI (Consulta efectuada dia 27 de Outubro de 2009).

Abaixo é apresentado alguns clientes com relevância em serviços diversos:

- Centros de Formação de Santiago do Cacém, Aljustrel e Beja
- Câmara de Santiago do Cacém
- Santa Casa da Misericórdia de Santiago do Cacém
- Câmara de Castro Verde
- Câmara de Beja
- Câmara de Grândola

- Hotel Dom Vasco
- Ambilital
- etc...

Outros clientes, não com menos relevância, mas não mencionados.

3.8 NOC - Network Operator Center

Representado sob a forma de esquema, observar Fig. 3.2, o actual centro de operações da rede SemCabo, contempla servidores para diversos serviços. Uma VPN para acesso remoto, duas *gateways* com *firewall* e VLAN, e ainda dois routers com NAT e *Intrusion Prevention System*. A LAN dos funcionários tem acesso directo aos servidores em algumas portas, e acesso à Internet através do balanceamento de duas ligações.

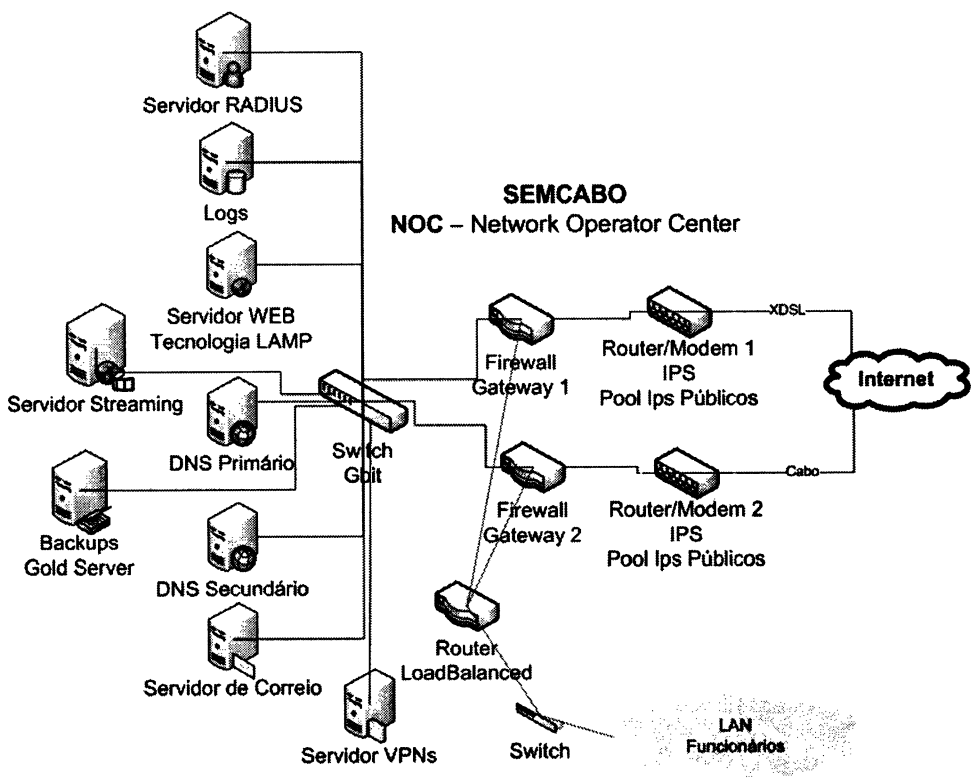

Figura 3.2: NOC - Network Operator Center

Capítulo 4

Sistema Base da SemCabo

4.1 Introdução

Para o correcto funcionamento do projecto SEMCABO-WIFI foi necessário proceder ao estudo, decisão, desenvolvimento, instalação, configuração e realização de testes para entrada em produção de diversos serviços. Este capítulo referencia as actividades consideradas principais na criação e implementação do projecto.

4.2 Estudo da Rede

A actividade inícial ou considerada base para o projecto, salienta-se o estudo da rede implementada. Devido à complexidade e grandeza esperada pelo projecto em causa, foram realizados vários contactos com operadores nacionais para possíveis parcerias/ajudas.

Tomando como negociação final, havendo outras desistências da nossa parte por motivos de garantias na estabilidade das ligações à Internet, foi escolhido como nosso parceiro principal a Claranet, antiga ViaNetworks, considerada o melhor ISP Europeu e detentora de uma das maiores redes mundiais.

Em relação à ligação de Internet foi escolhido uma XDSL[1], gama de 8 IPs públicos, necessária à instalação de servidores cruciais para o projecto dar os primeiros

[1]Digital Subscriber Line, Contenção 1:20

passos. Os routers adoptados da marca *Draytek*, são considerados dos mais fiáveis routers/modem para conexões sobre XDSL. Este tipo de ligação foi também escolhido para interligação de outras áreas de acesso à Internet onde a partilha seja efectuado por WI-FI, sendo utilizado uma ou mais linhas para balanceamento de tráfego consoante o número de utilizadores.

4.2.1 Equipamentos Activos

Como mencionado em 4.2, os routers escolhidos para conexão XDSL foram da marca *Draytek*, modelo *Vigor 2700* Analógico. Configuração e características principais:

- NAT[2]
- SPI[3], IPS[4]
- DoS[5]
- QoS[6]

A nível de *switching,* foi instalado um *Switch HP Procurve* com gestão a Gbit. Foi igualmente criada uma VLAN[7] para separação dos servidores da rede de trabalho dos funcionários da empresa.

4.2.2 Servidores Implementados

Para a base do sistema foi necessário efectuar a instalação e configuração de diversos servidores. Sem eles não seria possível os clientes efectuarem autenticação, resolverem endereços e até mesmo o acesso ao portal da SemCabo. Salienta-se ainda, o serviço de mail aos clientes, e a segurança da informação de cada servidor.

- Servidores de DNS[8] (DNS Primário e DNS Secundário)

[2]Network Address Translation
[3]Stateful Packet Inspection
[4]Intrusion Prevention System
[5]Denial of Service
[6]Quality of Service
[7]Virtual Local Area Network
[8]Domain Name System

- Servidor WEB (Tecnologia LAMP)
- Servidor RADIUS[9] (Freeradius)
- Servidor de Mail (Qmail)
- Servidor VPN[10] (RouterOS)
- Servidor Streaming (Red5)
- Servidor de BACKUPS (Gold Server)

4.2.3 Módulos Standard de Emissão de Sinal WIFI

Para distribuição de sinal WI-FI para cada localidade e/ou cidade onde o serviço seja disponibilizado, foi definido módulos de emissão standard, isto é, foi definido uma estrutura composta por vários *Access Points*[11] estruturados de forma a permitir uma cobertura apropriada para o local. Cada módulo normalmente emite sinal nas normas standard 802.11 bg, sendo efectuado os *backbones*[12] na norma 802.11a. Cada módulo pode conter até 6 *Access Points* para efectuar uma emissão de 360º. Cada *Access Point* é configurado com canais diferentes e varrimentos horizontais alternados com verticais, eliminando assim, interferência entre equipamentos.

O módulo é ainda composto por um ou mais NAS consoante a área geográfica de cada instalação.

A ligação de acesso à Internet pode variar consoante o número de utilizadores, podendo ser efectuado a instalação de uma única linha ou balanceamento entre várias linhas.

A Fig. 4.1 ilustra o topologia *standard* utilizada em cada localidade. Notar ainda, que o número de células emissoras dependem da área a abranger em cada local.

[9]Remote Authentication Dial In User Service
[10]Virtual Private Network
[11]ponto de acesso WI-FI
[12]Ligação de maior capacidade entre dois módulos de emissão WI-FI

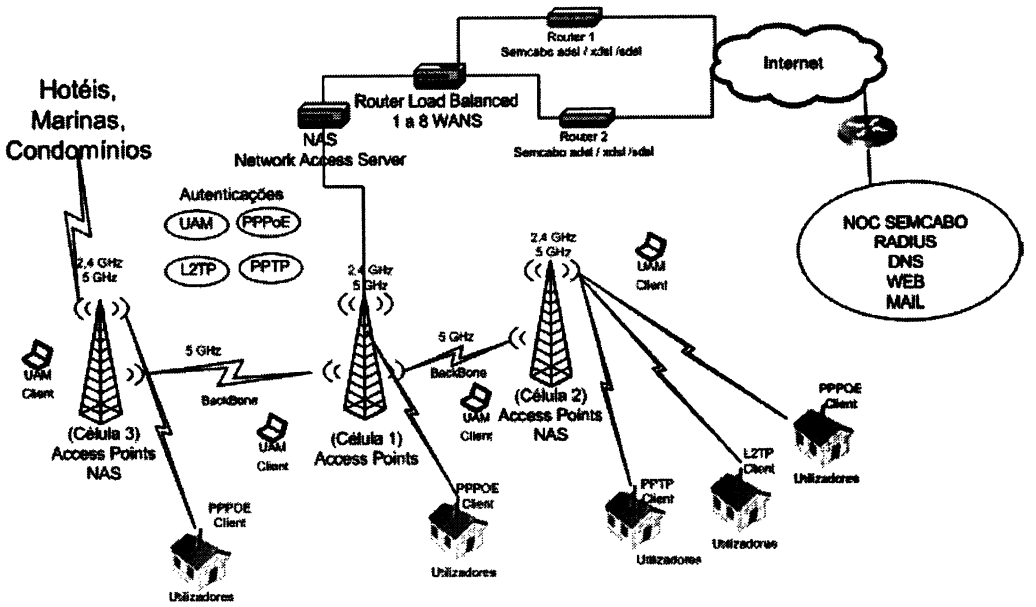

Figura 4.1: Módulo Standard de Emissão Sinal WI-FI em Localidades

Acima foi mencionado uma estrutura *standard* para localidades. Outros cenários como marinas, hotéis, parques de campismo e escolas a topologia adoptada é mais simples. Existe um NAS com autenticação UAM para os utilizadores e *Access Points* isolados a emitir sinal, podendo estes, utilizar *roaming* através do protocolo WDS[13] estático ou dinâmico (Mesh). A Fig. 4.2 abaixo mostra a estrutura utilizada.

[13]Wireless Distribution System

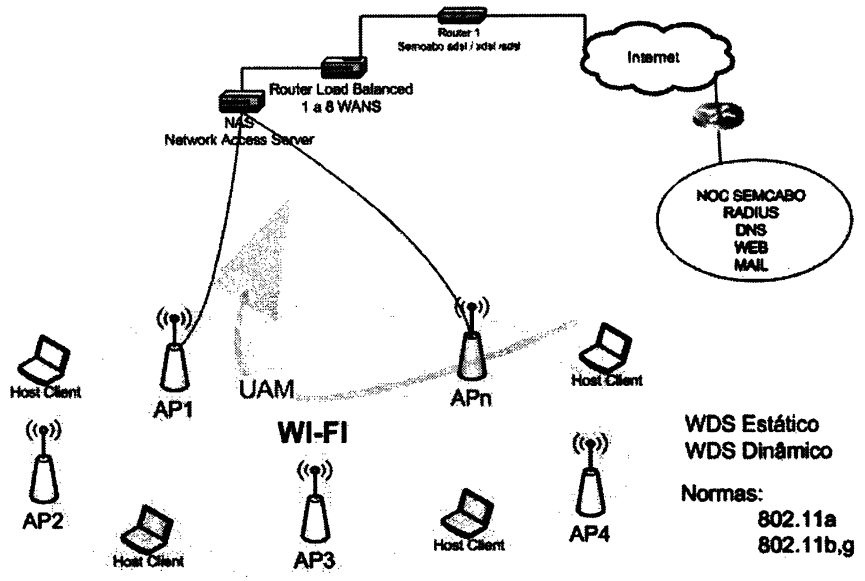

Figura 4.2: Módulo Standard de Emissão Sinal WI-FI, Hotéis, Marinas, Etc.

Em alguns casos é necessário a configuração de 2 VLANs para separação da rede dos utilizadores com a rede interna dos locais instalados.

4.2.4 Access Points

Os equipamentos instalados nos módulos *standard* de emissão de sinal, passaram por longos testes em cenários reais. Vários modelos e fabricantes diferentes foram excluídos por não terem o comportamento desejado. Abaixo fica uma lista das marcas e modelos utilizados actualmente.

- Senao Engenius
  - EOC-3220 EXT 802.11b,g
  - EOC-8610S EXT 802.11a,b,g
  - EOC-1650 802.11b,g
  - EOC-2610 802.11b,g
- Browan
  - P520 Operator Access Point
  - BW2220 Dual Radio 2,4Ghz e 5Ghz Outdoor Access Point

4.3 Segurança

Em relação à rede principal (NOC[14]), onde se encontram os servidores principais do sistema, são utilizados mecanismos de detecção e prevenção de intrusão (IDS, IPS) e mecanismo de DoS. Algo importante de salientar em segurança, todos os servidores da SemCabo consultados através da Internet têm IPs privados, o que torna impossível o encaminhamento do lado externo para o lado interno, evitando assim, qualquer tipo de ataque directo aos servidores da SemCabo. Apenas são redireccionadas as portas de cada serviço para o servidor correspondente.

Todos os colaboradores da empresa trabalham sobre uma VLAN distinta à dos servidores.

O acesso remoto ao NOC é efectuado através de uma VPN em L2TP/IPSec ou PPTP.

Nos módulos *standard* WI-FI em localidades, todos os equipamentos *client* de utilizadores assinantes conectam-se a uma SSID[15] encriptada, com WPA2/AES ou WPA2/PSK e com ACL[16]s no *Access Point* emissor. As credenciais de utilizador são inseridas posteriormente para autenticação em PPPOE, PPTP ou L2TP/IPSec. Os utilizadores "Net à Pala", conectam-se a uma SSID sem encriptação onde se autenticam por UAM.

Em hotspots públicos como marinas, hotéis, parques de campismo a SSID é sempre sem encriptação e autenticação por UAM.

No que respeita à salvaguarda dos dados, todos os servidores têm 2 discos em RAID 1 por software, todos os dias são efectuados backups diferenciais baseados em *full backups*. Existe uma margem de 24 horas para recuperação de qualquer informação eliminada por parte de clientes da empresa. Os backups são efectuados através de RSYNC[17]. Ainda de referir, cada servidor tem uma UPS dedicada.

[14]Network Operator Center
[15]Service Set Identifier
[16]Access Control List
[17]a fast, versatile, remote (and local) file-copying tool

4.4 Sistemas NAS

Aplicando o mais apropriado consoante critérios como, número de utilizadores em simultâneo, tipo de autenticação e o modelo de negócio.

Os NAS utilizados são:

- *Firmware OpenWRT* com ChilliSpot incorporado [16], instalado em equipamento Linksys modelo WRT54GL
- *Firmware DD-WRT* com ChilliSpot incorporado [17], instalado em equipamento Linksys modelo WRT54GL
- *ChilliSpot* em Linux Fedora Core [16], em *boards Mini-ITX* com 2 placas de rede
- *RouterOS* [19] em *boards Mini-ITX* e *routerboards*

4.5 Sistema de Monitorização

Após análise e testes de alguns sistemas de monitorização, salienta-se o mais testado (SolarWinds). Concluiu-se que nenhum preenchia as necessidades da monitorização em causa. Notar que muitos dos equipamentos a monitorizar encontram-se por detrás de *firewals* e NATs, equipamentos estes também com IPs privados.

A solução desenvolvida e ainda em melhoria, utiliza um servidor de VPN situado no NOC, cada NAS é um cliente VPN e servidor VPN. Cada vez que é instalado um novo NAS é criado um utilizador quer na VPN situada no NOC quer no servidor VPN do próprio NAS. As VPNs criadas são do tipo PPTP e L2TP/IPSec. Assim, quando um NAS é instalado, automaticamente se conecta e é possível aceder remotamente a ele e a todos os equipamentos por detrás dele.

É utilizado em cada NAS um *cron*[18] *job* que executa em cada 5 minutos o envio do *ip*, *nome* e *id* uma base de dados MySQL situada no NOC da SemCabo.

[18]Relógio que permite a execução de uma ou mais tarefas em intervalos de tempo

Do lado da base de dados, existe outro *cron job* onde este executa em cada 10 minutos a existência ou não de actualização de registos, no caso de algo não ter sido actualizado é enviado um mail ou um SMS[19]para o telemóvel.

Para acesso remoto a qualquer NAS, é efectuado a conexão ao servidor VPN no NOC, ficando assim, o acesso disponível a qualquer equipamento.

A tecnologia utilizada para os *scripts* de monitorização é PHP, para envio de mails o MTA *sendmail* e para SMS o serviço *voipbuster*[20] com recurso a um script em *shell.*

A Fig. 4.3 mostra o exemplo das VPNs criadas pelos NAS em 3 locais em monitorização.

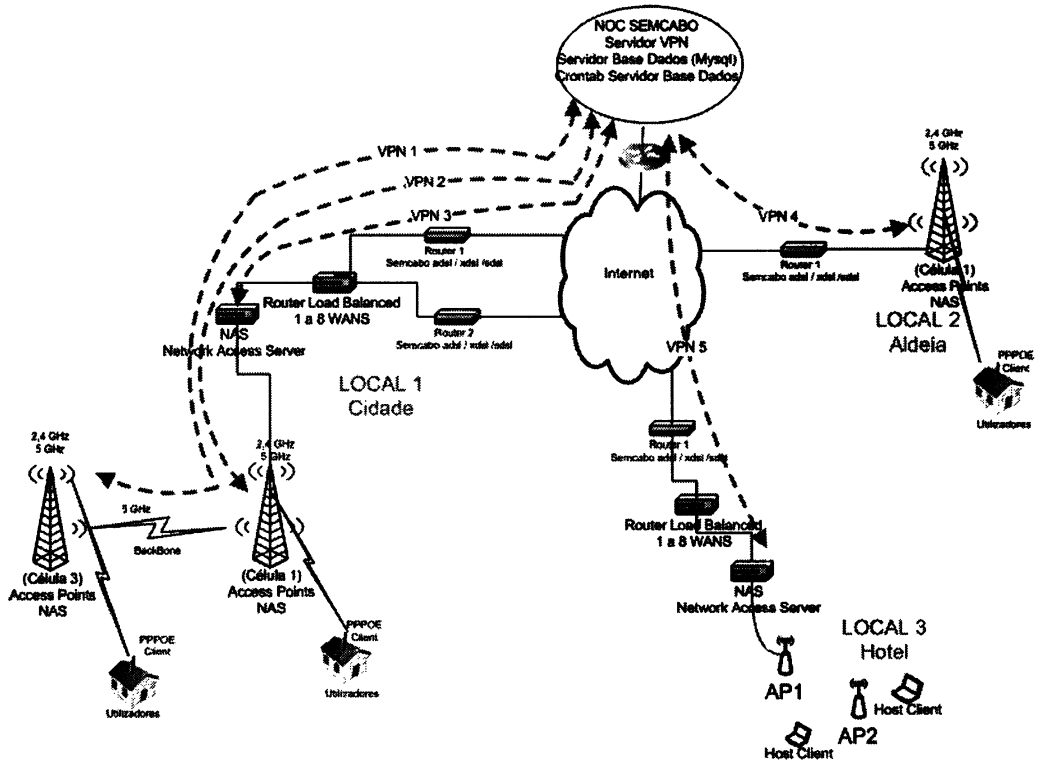

Figura 4.3: Esquema de Monitorização

A criação de VPNs é utilizado com o NAS em RouterOS, para ChilliSpot em DD-WRT, OpenWRT e Linux apenas são enviados o *ip*, *nome* e *id*. Ainda para

[19]Short Message Service

[20]*Empresa Provedora de Voz Sobre IP (VOIP) - www.voipbuster.com*

acesso remoto em ChilliSpot, são redireccionados os portos 22 e 443 para conexão segura por SSH[21] e HTTPS[22] respectivamente.

4.6 Portal de Autenticação

Uma das vertentes de negócio do projecto é a publicidade na própria rede. Assim, foi desenvolvido um módulo no portal para utilização na autenticação por UAM. Os utilizadores que se conectam à rede, são redireccionados para uma área do portal correspondente ao local que estão a navegar, mostrando informação direccionada. Como o método referido apenas permite a navegação em *sites* pré-definidos, o utilizador para navegar livremente pela Internet será obrigado a utilizar o módulo de autenticação. Caso não seja utilizador registado, poderá efectuar um registo online para posterior navegação introduzindo o *username* e *password*, cedido no momento do registo. O registo online apenas é possível em locais que exista "Net à Pala".

Foram desenvolvidos e implementados dois tipos de módulos, um para ChilliSpot e outro para RouterOS. O primeiro desenvolvido em PHP[23] e com autenticação por SSL[24], o segundo apenas alteração de layout em XML[25], HTML[26] e *javascript* com autenticação em CHAP[27]. Código parcial do módulo, consultar Apêndice A.1.

Em ambos os casos houve a necessidade da criação de um domínio não publicado (apenas resolução dentro da própria rede) com nome *wifi*, sendo agregado 4 registos de endereço *sair.wifi*, *quit.wifi*, *network.wifi* e *status.wifi*. Estes registos são utilizados para os utilizadores terem a possibilidade de terminarem a sessão e/ou verem relatório de acessos.

A Fig. 4.4 mostra o portal de entrada para os utilizadores que se conectam na

[21] Secure Shell
[22] Hypertext Transfer Protocol Secure
[23] Hypertext Preprocessor
[24] Secure Socket Layer
[25] eXtensible Markup Language
[26] HyperText Markup Language
[27] Challenge Handshake Authentication Protocol

localidade de Alvalade. A Fig. 4.5 a janela do módulo de autenticação.

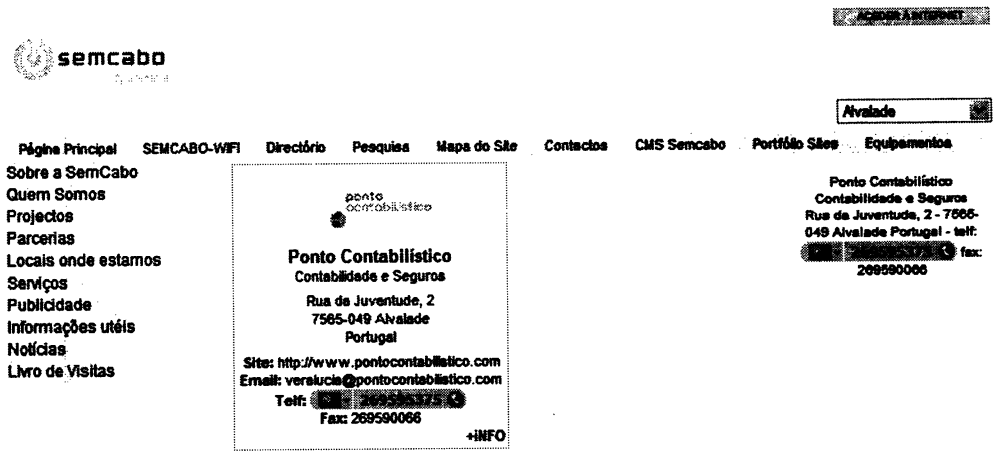

Figura 4.4: Layout Portal de Entrada - Localidade Alvalade

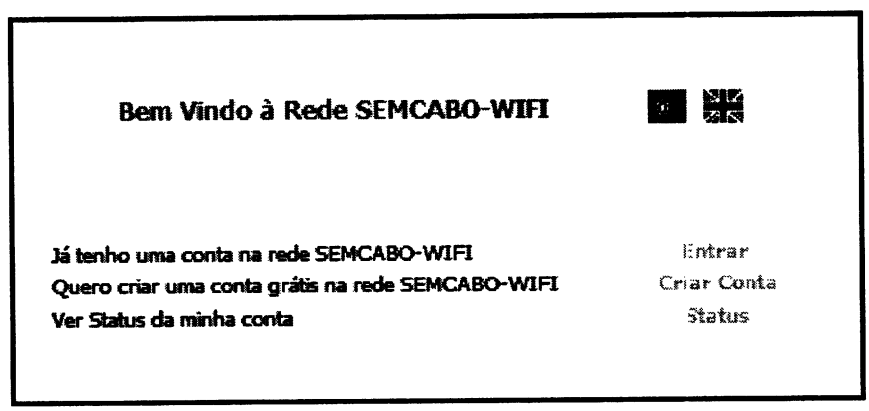

Figura 4.5: Layout módulo de autenticação

Actualmente todas as implementações com autenticação UAM são em RouterOS, esta opção prende-se pelo facto de não haver necessidade de certificado SSL, gerando por vezes, desconfiança do lado dos utilizadores. Como em RouterOS a encriptação dos dados é efectuada através de CHAP, assim, o utilizador não recebe avisos de segurança no browser. Outra razão, é a possibilidade de configuração de outros tipos de autenticação.

Capítulo 5

Servidores Base

5.1 Introdução

O suporte do projecto SEMCABO-WIFI, é assegurado por um conjunto de servidores base, descritos neste capítulo: servidores de nomes de domínio, utilizados para resolução dentro e fora da rede; servidor WEB, onde é efectuado o alojamento do módulo de autenticação e do portal da SemCabo; servidor de Mail, envio e recepção de mails para as contas dos assinantes de acesso à Internet e funcionários de empresas; servidor RADIUS, é o sistema de AAA utilizado para autenticação no controlo dos acessos à rede. Existem ainda outros servidores, como Projects (gestão documental e de projectos), *video streaming*, VPN (*Virtual Private Network*) e de Backups.

5.2 Servidor DNS Primário / Secundário

Para registo e controlo dos domínios principais como semcabo.pt, semcabo.com e semcabo.net, foram configurados dois servidores de DNS[1], um primário e outro secundário. Os *registrars*[2] de registo e delegação dos domínios são, *flesk* (semcabo.pt e semcabo.com) e *godaddy* (semcabo.net).

Ambos os servidores estão em *Linux Fedora Core* versão 10, o pacote do serviço

[1]Domain Name System
[2]Entidade acreditada para gestão e registo de nomes de Internet

de DNS é a versão *bind 9.5.1.* O modelo dos servidores que albergam o serviço são *HP Proliant ML 110*, estes servidores são compostos por dois discos em RAID 1 por software.

Actualmente o serviço de DNS serve aproximadamente 60 domínios. É política da SemCabo vir a ser um registrar, sendo necessário um número de 100 domínios, nomeadamente para domínios *.pt.*

Abaixo, nas tabelas 5.1, 5.2 e 5.3 são apresentadas as configurações dos domínios semcabo.pt, semcabo.com e semcabo.net respectivamente.

semcabo.pt	$ttl 38400			
	semcabo.pt.	IN	SOA	dns1.semcabo.pt. mail.semcabo.pt. (
			1161100277	
			10800	
			3600	
			604800	
			38400)	
	semcabo.pt.	IN	NS	dns1.semcabo.pt.
	semcabo.pt.	IN	NS	ns3.zoneedit.com.
	semcabo.pt.	MX	10	mail.semcabo.pt.
	www.semcabo.pt.	IN	A	80.172.48.226
	dns1.semcabo.pt.		IN	A 80.172.48.225
	dns2.semcabo.pt.		IN	A 80.172.48.229
	armando.semcabo.pt.		IN	A 80.172.48.225
	ftp.semcabo.pt.	IN	A	80.172.48.226
	mail.semcabo.pt.		IN	A 80.172.48.225
	semcabo.pt.	IN	A	80.172.48.225
	isp.semcabo.pt.	IN	A	213.228.144.25
	semcabo.pt.	IN	TXT	"v=spf1 ip4:80.172.48.224/29
				ip4:80.172.48.225 ip4:80.172.48.226
				ip4:80.172.48.227 mx ~all"
	mail.semcabo.pt.		IN	TXT "v=spf1 a -all"
	isp.semcabo.pt.		IN	TXT "v=spf1 a -all"
	hosting.semcabo.pt.		IN	TXT "v=spf1 a -all"
	email.semcabo.pt.		IN	TXT "v=spf1 a -all"
	semcabo.pt.	IN	NS	ns8.zoneedit.com.
	semcabo.pt.	IN	NS	dns2.semcabo.pt.

Tabela 5.1: Zona Forward semcabo.pt

semcabo.com	$ttl 38400 semcabo.com. IN SOA dns1.semcabo.pt. mail.semcabo.com. (1163576245 10800 3600 604800 38400) semcabo.com. IN NS dns1.semcabo.net. semcabo.com. MX 10 mail.semcabo.pt. www.semcabo.com. IN A 80.172.48.226 dns1.semcabo.com. IN A 80.172.48.225 dns2.semcabo.com. IN A 80.172.48.225 wifi1.semcabo.com. IN A 80.172.48.226 wifi2.semcabo.com. IN A 80.172.48.226 projects.semcabo.com. IN A 80.172.48.231 radius1.semcabo.com. IN A 80.172.48.226 radius2.semcabo.com. IN A 80.172.48.226 cmsdemo.semcabo.com. IN A 80.172.48.225 webmail.semcabo.com. IN A 80.172.48.224 carlos.semcabo.com. IN A 80.172.48.225 isp.semcabo.com. IN A 80.172.48.225 hosting.semcabo.com. IN A 80.172.48.225 semcabo.com. IN A 80.172.48.226 iris.semcabo.com. IN A 80.172.48.225 rsync.semcabo.com. IN A 80.172.48.227 wifigrandola.semcabo.com. IN A 80.172.48.225

Tabela 5.2: Zona Forward semcabo.com

semcabo.net	$ttl 38400 semcabo.net. IN SOA dns1.semcabo.pt. mail.semcabo.net. (1208382822 10800 3600 604800 38400) semcabo.net. IN NS dns1.semcabo.pt. semcabo.net. IN A 80.172.48.225 www.semcabo.net. IN A 80.172.48.226 dns1.semcabo.net. IN A 80.172.48.225 dns2.semcabo.net. IN A 80.172.48.225 semcabo.net. IN MX 10 mail.semcabo.pt. mail.semcabo.net. IN A 213.228.144.25 hosting.semcabo.net. IN A 213.228.144.25

Tabela 5.3: Zona Forward semcabo.net

Outra situação implementada foram os SPFs[3] [24] no domínio semcabo.pt, como pode ser observado na tabela 5.1 com registos do tipo TXT. Estes são necessários na verificação da veracidade do emissor de email, utilizado pela comparação do nome do servidor de mail com o IP correspondente. É necessário uma zona reverse para resposta de IP em nome.

[3]Sender Policy Framework

5.3 Servidor WEB

Nos serviços WEB, foi escolhido o servidor Apache (versão 2.2.0) em *Linux Fedora Core 5*. O modelo do servidor utilizado é *HP Proliant ML110* com 2 discos em RAID1 por *software*.

Actualmente este servidor suporta cerca de 160 portais, com tecnologia PHP e MySQL.

A configuração deste servidor para diferenciação dos pedidos de vários domínios foi baseada em *name-based Virtual Hosts* [20]. Foi utilizado um DNS, este configurado no mesmo servidor físico para suporte no mapeamento de cada nome para IP, sendo o IP do próprio servidor. Desta forma, o Apache consegue responder do directório correcto através do nome previamente pedido.

Abaixo na tabela 5.4, pode ser observado o excerto do ficheiro de configuração "httpd.conf", onde é criado os *Virtual Hosts* dos domínios semcabo. É apresentado na tabela 5.5 a configuração do DNS para auxílio na resolução de nomes.

APACHE Virtual Hosts Name-Based semcabo.pt semcabo.com semcabo.net	<VirtualHost 10.2.0.30:80> DocumentRoot "/home/semcabopagina" ServerName www.semcabo.pt ServerAlias semcabo.pt <Directory "/home/semcabopagina"> Options Indexes FollowSymLinks AllowOverride None Order allow,deny Allow from all </Directory> </VirtualHost> <VirtualHost 10.2.0.30:80> DocumentRoot "/home/semcabopagina" ServerName www.semcabo.com ServerAlias semcabo.com <Directory "/home/semcabopagina"> Options Indexes FollowSymLinks AllowOverride None Order allow,deny Allow from all </Directory> </VirtualHost> <VirtualHost 10.2.0.30:80> DocumentRoot "/home/semcabopagina" ServerName www.semcabo.net ServerAlias semcabo.net <Directory "/home/semcabopagina"> Options Indexes FollowSymLinks AllowOverride None Order allow,deny Allow from all </Directory> </VirtualHost>

Tabela 5.4: Virtual Hosts domínios semcabo.net, .com, .pt

DNS Zonas para resolução por name-based virtual hosts

```
#Domínio semcabo.pt
$ttl 38400
semcabo.pt.      IN      SOA     web1.semcabo.com. mail.semcabo.pt. (
                                 1161426382
                                 10800
                                 3600
                                 604800
                                 38400 )
semcabo.pt.      IN      NS      web1.semcabo.com.
www.semcabo.pt.  IN      A       10.2.0.30
armando.semcabo.pt.      IN      A       10.2.0.30

#Domínio semcabo.com
$ttl 38400
semcabo.com.     IN      SOA     web1.semcabo.com. mail.semcabo.com. (
                                 1163575833
                                 10800
                                 3600
                                 604800
                                 38400 )
semcabo.com.     IN      NS      web1.semcabo.com.
www.semcabo.com.         IN      A       10.2.0.30
cmsdemo.semcabo.com.     IN      A       10.2.0.30
carlos.semcabo.com.      IN      A       10.2.0.30
webmail.semcabo.com.     IN      A       10.2.0.30
iris.semcabo.com.        IN      A       10.2.0.30
wifigrandola.semcabo.com.        IN      A       10.2.0.30

#Domínio semcabo.net
$ttl 38400
semcabo.net.     IN      SOA     web1.semcabo.com. mail.semcabo.net. (
                                 1208432078
                                 10800
                                 3600
                                 604800
                                 38400 )
semcabo.net.     IN      NS      web1.semcabo.com.
semcabo.net.     IN      A       10.2.0.30
www.semcabo.net.         IN      A       10.2.0.30
```

Tabela 5.5: Zonas Internas para name-based Virtual Hosts

5.4 Servidor de Mail

No servidor de correio electrónico, foi utilizado um *HP Proliant ML110* com 2 discos em RAID1 por software. O sistema operativo adoptado foi o *Linux Fedora Core 5*, o *Qmail* foi o MTA[4] instalado para o protocolo SMTP[5] e *courier-imap* para os protocolos POP3[6], IMAP[7] e IMAPS[8] [21].

Para gestão do servidor foram instalados pacotes com interligação ao *Qmail*,

[4]Mail Transfer Agent
[5]Simple Mail Transfer Protocol
[6]Post Office Protocol
[7]Internet Message Access Protocol
[8]Internet Message Access Protocol Secure

sendo eles:

- *autoresponder*, possibilidade de auto-resposta
- *Vpopmail*, permite a virtualização de mail para vários domínios
- *Vqadmin*, ferramenta web para manipulação de domínios virtuais (vpopmail)
- *SpamAssassin*, ferramenta de *SPAM filter*

Actualmente todos os clientes do projecto SEMCABO-WIFI e/ou clientes de *hosting*, são detentores de pelo menos uma conta de correio electrónico. Estes podem aceder através de qualquer cliente de mail, dando como exemplo o *outlook express, mozilla thunderbird*, entre outros. Existe também, a possibilidade de aceder ao *webmail* da semcabo, disponibilizado através da configuração do *squirrelmail*[9] no próprio servidor de correio.

5.5 Servidor RADIUS

O sistema de AAA[10] escolhido foi o Freeradius [13], este foi instalado no sistema operativo *Linux Fedora Core 5*. O modelo do servidor utilizado foi o *HP Proliant ML110* com 2 discos em RAID1 por *software*.

Alguns aspectos importantes da instalação são descritos abaixo:

1. Pacotes Instalados
   - Freeradius1.0.5.tar.gz
   - php-radius5.0.4-10.1.i386.rpm
   - phpMyadmin2.7.0-pl2.zip

   Compilação e instalação:

[9] Webmail open source desenvolvido em PHP
[10] Authentication, Authorization, and Accounting

- Após descompactação, *tar zxvf freeradius-1.0.5.tar.gz,* procedeu-se à compilação do Freeradius, *./configure -prefix=/usr -with-logdir=/var/log -with-radacctdir=/var/log/radacct -with-raddbdir=/etc/raddb,* em seguida à instalação, *./make install.*

A instalação do pacote *php-radius-5.0.4-10.1.i386.rpm*, deveu-se ao script de autenticação utilizar a tecnologia PHP para o método de autenticação UAM através de *ChilliSpot.*

2. O código presente na Fig. 5.1, foi adicionado ao ficheiro de configuração */etc/-raddb/clients.conf* devido à necessidade do sistema autenticar NAS com IPs públicos dinâmicos.

```
client 0.0.0.0/0 {
        secret      = XXXXXXXXXXXX
        shortname = network-semcabowifi
        nastype = other
}
```

Figura 5.1: Autenticar NAS com IPs públicos dinâmicos, máscara global

3. A base de dados utilizada com o Freeradius é o MySQL, a configuração da conexão foi efectuada através do ficheiro */etc/raddb/sql.conf*, a Fig. 5.2 apresenta um pequeno excerto das directivas principais de configuração.

```
sql {
        driver = "rlm_sql_mysql"
        server = "localhost"
        login = "xxxxx"
        password = "xxxxx"
        radius_db = "radius"
        ...
      }
```

Figura 5.2: Directivas principais para conexão MySQL

4. No ficheiro */etc/raddb/sql.conf* foi desabilitado a autenticação de acessos em simultâneo, eliminando assim, a possibilidade que um *login* seja utilizado por mais do que uma pessoa em simultâneo. Observar Fig. 5.3.

```
simul_count_query = "SELECT COUNT(*) FROM ${acct_table1} WHERE
UserName='%{SQL-User-Name}' AND AcctStopTime = 0"

simul_verify_query = "SELECT RadAcctId, AcctSessionId, UserName,
NASIPAddress, NASPortId, FramedIPAddress, CallingStationId, FramedProtocol
FROM ${acct_table1} WHERE UserName='%{SQL-User-Name}' AND AcctStopTime = 0"
```

Figura 5.3: Desabilitar Acessos Simultâneos

5. Indicação no ficheiro */etc/raddb/radiusd.conf,* nas secções de *"authorize"* e *"accounting"* a directiva *sql.* Desta forma o Freeradius utiliza a configuração definida acima no ponto 3, os pedidos de *"authorization"* são consultados na base de dados SQL e armazenados os dados de *"accounting"*.

   Ainda na secção *"accounting"*, foi retirado algumas directivas de *logging* por defeito como: *detail, unix, radutmp* para prevenir situações de ocupação de disco por *logs* gerados pelo sistema.

   Para completar o ponto 4 acima, foi necessário activar a directiva *sql* na secção *"session"*, sendo esta necessária para consulta e verificação de acessos em simultâneo na base de dados.

   Na secção *"authentication"* foi indicado os tipos de autenticação utilizado pelos NAS, sendo estes CHAP e MSCHAP.

   A Fig. 5.4 abaixo, mostra a configuração no Freeradius nas secções de AAA.

```
#secção authorize
authorize {...
        preprocess
        chap
        mschap
        suffix
        eap
        files
        sql     # Configuração em sql.conf
}

#secção authentication
authenticate {
        Auth-Type PAP {
                pap
        }
        Auth-Type CHAP {  #UAM por CHAP
                chap
        }
        Auth-Type MS-CHAP {  #PPPOE #PPTP #L2TP
                mschap
        }
        eap  #Entre NAS e RADIUS
}

#Secção accounting Log the accounting data
accounting {
        detail
        radutmp
        sql # Configuração em sql.conf, Log data in sql database
}

#Secção de sessão
session {
        #  Acessos em simultâneo através de sql.conf, data in sql database
        sql
}
```

Figura 5.4: Secções de AAA

6. Para o Freeradius ter suporte a atributos específicos respeitantes aos NAS *chillispot* e *RouterOS*, foram adicionados dois novos *dictionary*[11] em */etc/raddb/dictionary*. A Fig. 5.5 mostra os dois *dictionary* adicionados.

```
# ChilliSpot dictionary.

VENDOR          ChilliSpot                      14559

#
#       ChilliSpot Vendor Specific Extensions
#
#
ATTRIBUTE       ChilliSpot-Max-Input-Octets         1       integer ChilliSpot
ATTRIBUTE       ChilliSpot-Max-Output-Octets        2       integer ChilliSpot
ATTRIBUTE       ChilliSpot-Max-Total-Octets         3       integer ChilliSpot
ATTRIBUTE       ChilliSpot-Bandwidth-Max-Up         4       integer ChilliSpot
ATTRIBUTE       ChilliSpot-Bandwidth-Max-Down       5       integer ChilliSpot
ATTRIBUTE       ChilliSpot-Config                   6       string  ChilliSpot
ATTRIBUTE       ChilliSpot-Lang                     7       string  ChilliSpot
ATTRIBUTE       ChilliSpot-Version                  8       string  ChilliSpot

# MikroTik Attributes

VENDOR          Mikrotik        14988

ATTRIBUTE       Mikrotik-Recv-Limit             1       integer         Mikrotik
ATTRIBUTE       Mikrotik-Xmit-Limit             2       integer         Mikrotik
ATTRIBUTE       Mikrotik-Group                  3       string          Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Forward       4       integer         Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Skip-Dot1x    5       integer         Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Enc-Algo      6       integer         Mikrotik
ATTRIBUTE       Mikrotik-Wireless-Enc-Key       7       string          Mikrotik
ATTRIBUTE       Mikrotik-Rate-Limit             8       string          Mikrotik
ATTRIBUTE       Mikrotik-Realm                  9       string          Mikrotik
ATTRIBUTE       Mikrotik-Host-IP                10      ipaddr          Mikrotik
ATTRIBUTE       Mikrotik-Mark-Id                11      string          Mikrotik
ATTRIBUTE       Mikrotik-Advertise-URL          12      string          Mikrotik
ATTRIBUTE       Mikrotik-Advertise-Interval     13      integer         Mikrotik
ATTRIBUTE       Mikrotik-Recv-Limit-Gigawords   14      integer         Mikrotik
ATTRIBUTE       Mikrotik-Xmit-Limit-Gigawords   15      integer         Mikrotik
```

Figura 5.5: Dictionary ChilliSpot e RouterOS

5.5.1 Base dados

Actualmente a base de dados MySQL de suporte ao Freeradius é composta por 21 tabelas (Apêndice B.1), cada uma com funcionalidades diferentes, as mais relevantes são as seguintes:

- *usergroup*: associa um nome de utilizador a um grupo
- *radcheck*: possui o registo de cada utilizador com o valor da sua palavra-passe
- *radreply*: cria para cada utilizador respostas específicas

[11] Atributos utilizados para suporte aos NAS utilizados

- *radgroupreply*: cria atributos que são retornados para todos os utilizadores de um grupo
- *radacct*: contém toda a informação de *status* e de contabilidade das ligações

5.5.2 Gestão de Utilizadores

Existe uma aplicação com recurso à tecnologia LAMP ainda em desenvolvimento, sendo esta para criação de Acessos/Vouchers. Esta gera automaticamente acessos na base de dados consultada pelo RADIUS. As etapas de criação dos acessos podem ser observadas na Fig. 5.6.

Há ainda necessidade de recurso a outra aplicação, o *PhpMyAdmin*[12], o qual é utilizado na passagem de utilizadores registados autonomamente no portal (tipo grátis) para assinantes. Este é ainda usado na construção das estatísticas retiradas para o ICP-ANACOM dos tráfegos gerados pelos utilizadores, onde são utilizados scripts em SQL[13].

[12]Software Open Source escrito em PHP para administração de Base de Dados MySQL
[13]Structured Query Language

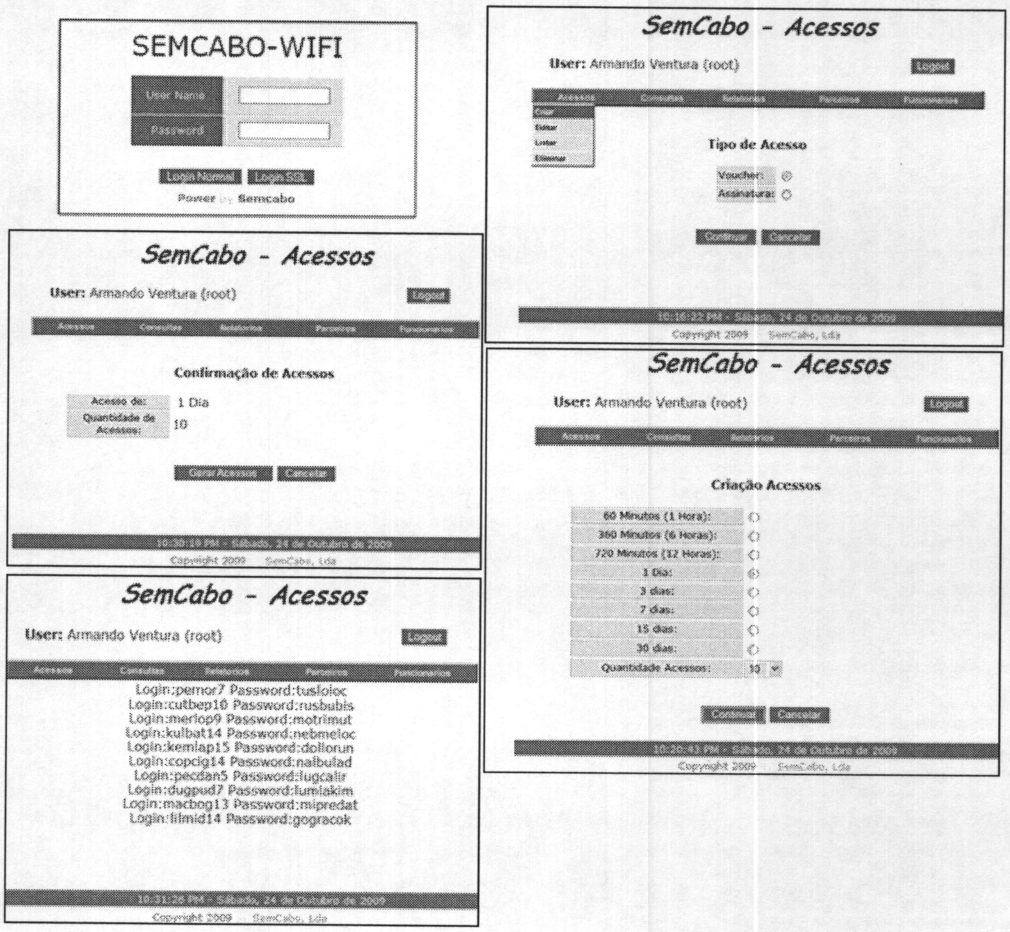

Figura 5.6: Etapas para criação de Acessos/Vouchers

5.6 Servidor Projects

Este servidor funciona num *HP Proliant ML110* com discos em RAID1 por *software*, utiliza o sistema operativo *Fedora Core 5*. Ainda neste servidor encontra-se o serviço WEB instalado e base de dados MySQL necessário ao funcionamento do *Software Open Source DotProject* [22]. O *software DotProject* é utilizado para gestão de projectos, para arquivamento de backups da configuração de equipamentos de rede, no armazenamento do resultado de investigação e ainda para organização de documentação diversa.

5.7 Servidor Streaming

Este servidor é utilizado para *spots* publicitários com recurso a *video streaming* no portal da SemCabo. O serviço de *streaming* está implementado através do *software Red5* (*Open Source Flash Server*) [25], estando a funcionar sob o sistema operativo *Linux Fedora Core 5*. Este serviço funciona sobre um *HP Proliant ML110* com 2 discos em RAID1 por *software*.

5.8 Servidor VPN

O servidor VPN[14] configurado e presente no NOC da SemCabo utiliza o sistema operativo RouterOS. Este servidor é configurado com dois tipos de VPNs, em PPTP e L2TP/IPSec. Uma das finalidades deste servidor é permitir o acesso a todos os NAS RouterOS e aos equipamentos ligados a eles, nomeadamente a *Access Points*. É ainda, utilizado na autenticação do NAS ao RADIUS pelos túneis criados, sendo o restante tráfego encaminhado por fora do túnel. Os túneis criados, permitem ainda que cada NAS ligado a qualquer tipo de acesso à Internet com IP dinâmico, seja tratado através de IP fixo na autenticação ao RADIUS.

O acesso aos *Access Points* por detrás dos NAS, é efectuado através da criação de duas VPNs. É estabelecida uma VPN directa ao servidor VPN no NOC da SemCabo, de seguida, utilizando o mesmo túnel, é criado outra VPN no sentido do próprio NAS.

Nota: Cada NAS RouterOS é configurado como cliente VPN e também com possibilidade de servidor VPN.

5.9 Servidor de Backups

Como mencionado atrás nos pontos 5.2 a 5.7, todos os servidores funcionam em Linux com RAID 1 por *software*, o servidor de backups não é diferente, apenas

[14]Virtual Private Network

contempla discos com capacidades superiores.

Este servidor comporta-se como *Gold Server*[15], e ainda contém todos os *full backups* dos servidores e *backups* diferenciais.

Todos os servidores configurados, testados e prontos para produção, são sujeitos a *full backup* ou *full image* com a ferramenta G4U[16]. Diariamente são efectuados *backups diferenciais* de todos os dados relevantes de cada servidor, é utilizado a ferramenta RSYNC[17] após mapeamento em NFS[18]. O tipo de *backups*, não pode ser considerado *diferencial standard*, apenas são copiados ou eliminados ficheiros modificados sobre a primeira cópia efectuada. Assim, por este método podemos repor a informação sempre pelo último backup efectuado.

- Abaixo são apresentados os scripts/comandos utilizados para o backup diário dos servidores do ponto 5.2 a 5.6.

  - Servidor de Backups

    Configuração do serviço NFS através do ficheiro */etc/export*, indicação da directoria a guardar as cópias de backups de cada servidor:

    /backups/mail1 x.x.x.x(rw,sync)

    /backups/controladorwifi1 x.x.x.x(rw,sync)

    /backups/web1 x.x.x.x(rw,sync)

    /backups/dns1 x.x.x.x(rw,sync)

    /backups/documentos1 x.x.x.x(rw,sync)

  - Servidor DNS Primário

    #mount -t nfs y.y.y.y:/backups/dns1 /backups

    #rsync -av -delete /etc/named.conf /var/named/chroot/var/named /root /backups

[15]Servidor que guarda backups, scripts, configurações
[16]Harddisk Image Cloning
[17]a fast, versatile, remote (and local) file-copying tool
[18]Network File System

#umount /backups

* Execução crontab

  *1 3 * * * sh /root/backup_dns1.sh* #Execução shell script backups_dns1.sh

- Servidor WEB

  #mount -t nfs y.y.y.y:/backups/web1 /backups

  #mysqldump -opt -user root -password=aaaaaa -all-databases > /backups/web1_databases.dump

  #rsync -av -delete /home /etc/named.conf /etc/httpd /var/www /var/named/chroot/var/named /root /etc/passwd /etc/group* /etc/shadow* /etc/gshadow /aquota.user /aquota.group /etc/vsftpd /backups*

  #umount /backups

  * Execução crontab

    *10 4 * * * sh /root/backup_web1.sh* #Execução shell script backups_web1.sh com dns interno

- Servidor de Mail

  #mount -t nfs y.y.y.y:/backups/mail1 /backups

  #mysqldump -opt -user root -password=aaaaaa -all-databases > /backups/mail1_databases.dump

  #rsync -av -delete /home/vpopmail /home/webmail /root /backups

  #umount /backups

  * Execução crontab

    *0 4 * * * sh /root/backup_mail1.sh* #Execução shell script backup_mail1.sh

- Servidor RADIUS

  #mount -t nfs y.y.y.y:/backups/controladorwifi1 /backups

  #mysqldump -opt -user root -password=aaaaaa -all-databases >

/backups/controladorwifi1_databases.dump

#rsync -av -delete /home /etc/httpd /root /etc/passwd /etc/group* /etc/shadow* /etc/gshadow /backups*

#umount /backups

* Execução crontab

  *1 2 * * * sh /root/backups_controladorwifi1.sh* #Execução shell script backup_controladorwifi1.sh

- Servidor Projects

  #mount -t nfs y.y.y.y:/backups/documentos1 /backups

  #mysqldump -opt -user root -password=aaaaaa -all-databases > /backups/doc_databases.dump

  #rsync -av -delete /publico /home /etc/httpd /var/www /root /etc/passwd /etc/group* /etc/shadow* /etc/gshadow /backups*

  #umount /backups

  * Execução crontab

    *10 22 * * * sh /root/backup_doc.sh* #Execução shell script backup_doc.sh

Outra finalidade deste servidor é backups remotos para clientes empresariais. É utilizado em simultâneo o RSYNC e SSH, deste modo, é aplicado compressão e confidencialidade na transferência de informação através da Internet.

Na automatização dos backups remotos e para cada nova empresa é gerado um par de chaves (chave pública e privada), *ssh -keygen -t dsa -b 1024 -f certificadoN*. A chave pública é guardada no servidor de Backups da SemCabo para autorização SSH [23], sendo a chave privada guardada no servidor da empresa cliente. Ainda no servidor da empresa cliente, são agendadas execuções temporais para o backup remoto, o comando para execução do RSYNC e SSH em simultâneo é dado por *#rsync -avz -delete "directorias de backups" -e "ssh -i certificadoN userxpto@IP:/home/userxpto"*.

Capítulo 6

Sistemas NAS

6.1 Introdução

Este capítulo refere as configurações consideradas essenciais para as autenticações UAM e PPPOE, realizadas nos NAS instalados na SemCabo. Em primeiro lugar é mencionado o NAS ChilliSpot em Linux Fedora Core, seguindo-se em OpenWRT e DD-WRT. Por fim, é referido a configuração em NAS RouterOS.

6.2 Chillispot (Open Source)

Chillispot, é um *software open source*, permite o redireccionamento para uma página de autenticação para aceder à Internet, normalmente usado na criação de *hotspots*, ou em empresas para aumento de segurança em redes com e sem fios.

Este sistema permite dois tipos de autenticações, UAM[1] e WPA[2]. No primeiro método (UAM), o equipamento *client* requer um IP sendo este atribuído pelo ChilliSpot, quando o utilizador abre o browser o ChilliSpot capta a conexão TCP e redirecciona para o portal de autenticação. De seguida é verificado as credenciais do utilizador entre o ChilliSpot, o servidor WEB e RADIUS.

O segundo método, WPA utilizando o ChilliSpot, sendo neste caso também designado por 802.1x, a autenticação é assegurada directamente pelo *Access Point,*

[1]UAM-Universal Authentication Method
[2]WPA-Wireless Protected Access

ficando este, o responsável pelo encaminhando das credenciais do *client* para o ChilliSpot.

Em ambos os métodos, o ChilliSpot autentica os utilizadores no RADIUS, sendo o próprio RADIUS o responsável pelo envio de uma mensagem de *access-accept* para o *ChilliSpot* em caso de sucesso, caso contrário, será enviado um *access-reject* ficando desta forma o ChilliSpot incumbido de negar o acesso à rede ao equipamento *client.*

Foi definido a utilização do ChilliSpot em três sistemas, sendo eles em Linux Fedora Core em Mini-ITX, o firmware OpenWRT e DD-WRT em routers Linksys WRT54GL Version 1.1.

O ChilliSpot na SemCabo apenas é utilizado para autenticação UAM.

6.2.1 Chillispot em Linux Fedora Core (Mini ITX)

Em situações que a perspectiva do número de utilizadores em simultâneo seja elevada, é utilizado arquitectura PC[3], sendo configurado com o Sistema Operativo *Linux Fedora Core* para instalação do ChilliSpot.

Alguns aspectos importantes da instalação são descritos abaixo:

1. Requisitos necessários

   - 2 placas ethernet
   - chillispot-1.1.0.tar.gz
   - Compilador C/C++

2. Compilação e instalação:

   - Após descompactação, *gzip chillispot-1.1.0.tar.gz* e *tar xvf chillispot-1.1.0.tar,* procede-se à compilação do ChilliSpot, *./configure* e *./make* , de seguida à instalação, *./make install.*

[3]Personal Computer

3. Para permitir a passagem de pacotes entre duas placas de rede é necessário activar o *IP packet forwarding.*

   #echo "1" > /proc/sys/net/ipv4/ip_forward

4. A configuração do ChilliSpot é realizada através do ficheiro */etc/chilli.conf.* Abaixo é apresentado as directivas principais de configuração:

   - #Pool de IPs distribuídos aos clientes

     net 172.16.100.100/16

   - #DNS

     dns1 213.58.105.160

   - #Domínio

     domain semcabo.pt

   - #Indicação IP Radius

     radiusserver1 80.172.48.226

     radiusserver2 80.172.48.227

   - #Portas de Autenticação e Accounting

     radiusauthport 1812

     radiusacctport 1813

   - #Chave partilhada entre NAS e Radius

     radiussecret aaaaaa

   - #Identificação NAS

     radiusnasid aaaaaa

   - #DHCP activo na eth1, interface do lado dos Access Points

     dhcpif eth1

   - #URL do Script PHP para autenticação entre chillispot e Radius

     uamserver https://www.semcabo.pt/control/semcabowifi.php

   - #Página de Boas Vindas

     uamhomepage http://www.semcabo.pt/?showib=1&setlocal=3

- #Chave partilhada entre o NAS ChilliSpot e Web Server

  uamsecret aaaaaa

- #Páginas de Visita

  uamallowed www.semcabo.pt

5. Actualização da *firewall iptables*, sendo esta actualizada através da execução de um script em shell.

   Alteração da firewall para permissão de conexão por SSH ao NAS.

   Consultar Apêndice C1 para consulta do script em shell.

6. Configuração de um *cron job* para execução de 5 em 5 minutos de um script em PHP para actualização de IP e status do NAS, utilização da ferramenta WGET[4].

   # *wget http://www.semcabo.pt/control/ddns/ddns.php?localID=xxx*

6.2.2 ChilliSpot em OpenWRT (Linksys WRT54GL)

O firmware OpenWRT é baseado em Linux, é um projecto *open source* para sistemas embutidos, nomeadamente para equipamentos *wireless*. Tem compatibilidade com equipamentos de vários fabricantes.

Os *Access Points* adoptados para instalação do firmware OpenWRT com ChilliSpot são os equipamentos *Linksys WRT54GL Version 1.1*, ver Fig 6.1. Este sistema é utilizado em situações que não sejam ultrapassados os 40 utilizadores em simultâneo, sendo em cenários como, pequenos hotéis, parques de campismo, auditórios, etc. O método de autenticação utilizado é UAM.

A configuração é realizada através de linha de comandos por SSH ou telnet.

[4]command line application for file retrieval over ftp, http and https connections

Figura 6.1: Linksys WRT54GL V1.1

Alguns aspectos importantes da instalação são descritos abaixo:

1. Instalação inicial

   - O *default settings* do OpenWRT utiliza a estrutura de *bridging* representada na Fig. 6.2.

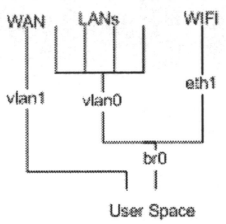

Figura 6.2: Default Settings OpenWRT

   - *vlan0*, Virtual Lan: Portas 1 a 4
   - *vlan1*, Virtual Lan: Internet
   - *eth1*, interface WIFI
   - *br0*, ponte entre vlan0(portas LAN) e WIFI

2. Requisitos necessários

   - Software ChilliSpot
     - *chillispot_1.1_mipsel.ipk*

- *firewall*

- Driver tun/tap[5]
  - *tun-modules_2.4.20-wrt1_mipsel.ipk*

3. Instalação:

   - Instalação driver tun/tap e activação
     - *ipkg install tun-modules_2.4.20-wrt1_mipsel.ipk*
     - *insmod tun*
   - Instalação software chillispot
     - *ipkg install chillispot_1.1_mipsel.ipk*

   Efectuado o passo 3, a estrutura de *bridging* no OpenWRT passa a ser representado como na Fig. 6.3.

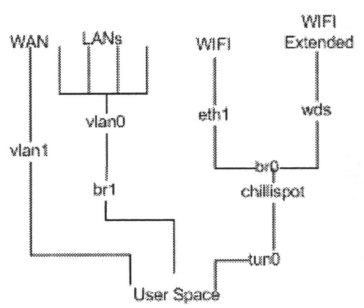

Figura 6.3: Bridging após instalação de tun/tap e chillispot

- *vlan0*, Virtual Lan: Portas 1 a 4
- *vlan1*, Virtual Lan: Internet
- *eth1*, interface WIFI
- *wds*, extended wifi, ligar a outros equipamentos por wifi utilizando o protocolo WDS[6]
- *br0*, ponte entre interfaces WDS e WIFI

[5]Virtual Network Kernel Drivers
[6]Wireless Distribution System

- *br1*, nova ponte para a interface LAN

4. Alteração de */etc/init.d/S45firewall* para a *firewall* apresentada em *Apêndice C.3.*

5. Início automático do ChilliSpot através da inclusão da linha */usr/sbin/chilli* no final do ficheiro */etc/init.d/S50services.*

6. *cron job* para execução de 5 em 5 minutos executar o script de monitorização.

   *5 * * * * wget http://www.semcabo.pt/control/ddns/ddns.php?localID=xxx*

O ficheiro de configuração */etc/chilli.conf* é apresentado na Fig. 6.4.

```
radiusserver1 radius1.semcabo.com
radiusserver2 radius2.semcabo.com
radiussecret aaaaaa
dhcpif br0
uamserver https://wifi1.semcabo.com/control/semcabowifi.php
dns1 80.172.48.225
dns2 80.172.48.229
uamsecret aaaaaa
radiusnasid c0004
domain semcabo.pt
net 172.16.100.100/16
uamhomepage http://www.semcabo.pt/?showib=1&setloc=4
uamallowed 80.172.48.224
uamallowed 80.172.48.225
uamallowed 80.172.48.226
uamallowed 80.172.48.227
uamallowed 80.172.48.228
uamallowed 80.172.48.229
uamallowed 80.172.48.230
uamallowed 80.172.48.231
```

Figura 6.4: Ficheiro configuração chillispot em OpenWRT

6.2.3 ChilliSpot em DD-WRT (Linksys WRT54GL)

O ChilliSpot em DD-WRT é instalado nos mesmos equipamentos que o OpenWRT, o firmware DD-WRT é escolhido em cenários até 20 utilizadores em simultâneo. A instalação do chillispot neste firmware passa pela escolha do nível *standard* dos 3 (*micro, mini, standard*) que a distribuição tem.

A versão utilizada do DD-WRT é *23 SP2 standard generic.* Esta permite a activação do módulo do ChilliSpot e a sua configuração.

A Fig. 6.5 mostra a janela de activação e configuração do ChilliSpot em DD-WRT.

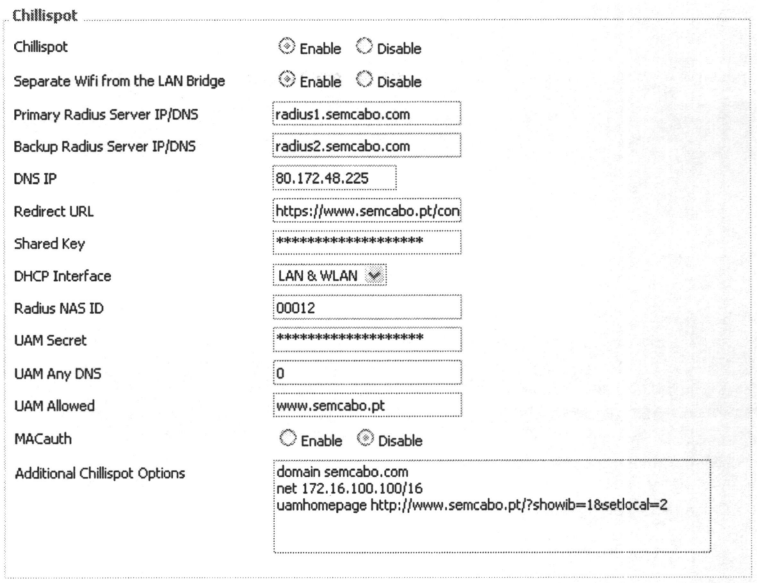

Figura 6.5: Configuração ChilliSpot em DD-WRT

6.3 RouterOS

Actualmente todas as instalações de NAS são preferencialmente em RouterOS. É instalado em duas arquitecturas, PC e *routerboard*. Utilizado PC quando o processamento é bastante exigente. A configuração é igual em ambas as arquitecturas, a instalação em PC é através de rede ou CD, na *routerboard* já vem instalado.

Será abordado as configurações essenciais numa *routerboard* com 5 portas *ethernet* (Ver Fig. 6.6), sendo utilizado a autenticação UAM e PPPOE. Terá ligação até 4 *Access Points* para distribuição de sinal WI-FI. O cenário de exemplo é apresentado na Fig. 6.7.

Configuração completa em *Apêndice D.1.*

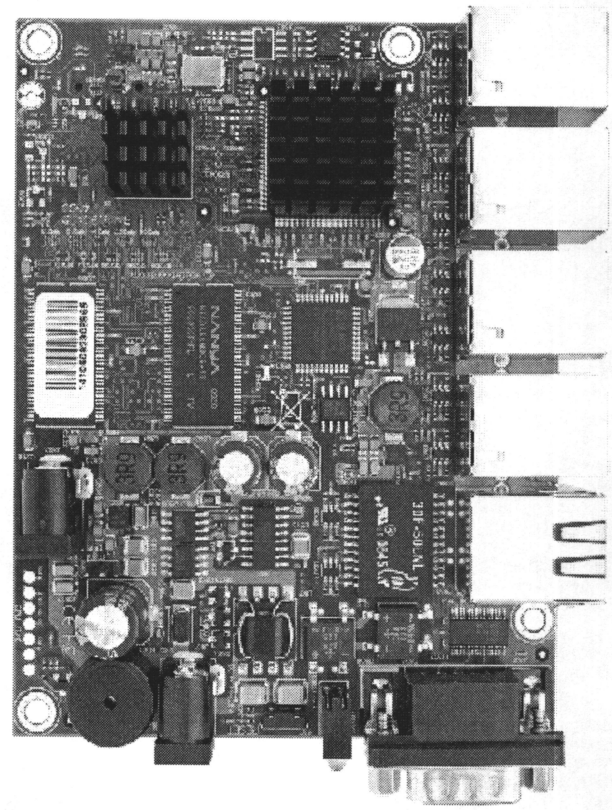

Figura 6.6: RouterBoard com 5 Portas a Gbit

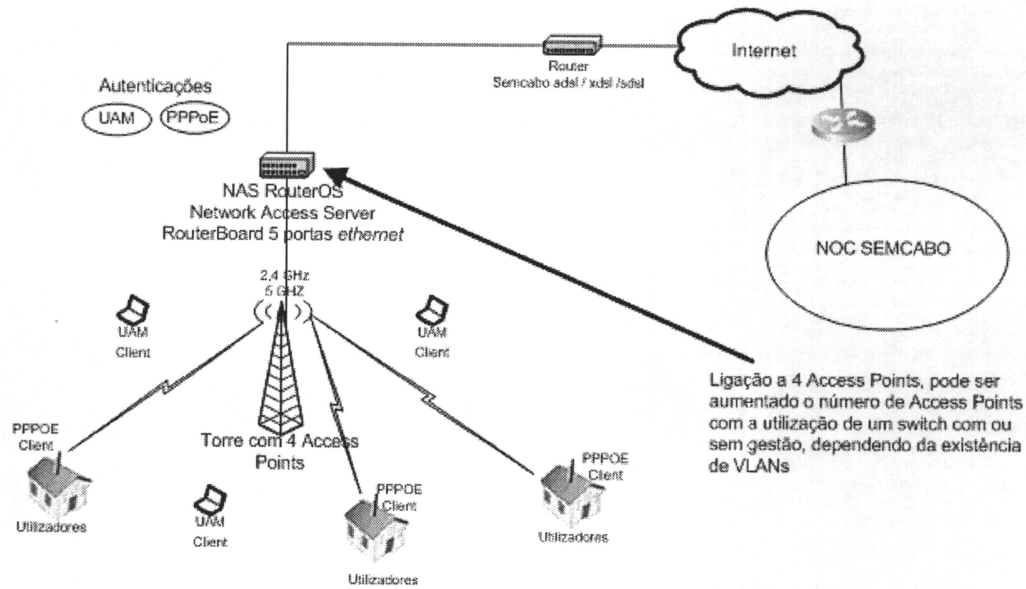

Figura 6.7: Cenário de configuração com RouterOS

1. Configuração geral do RouterOS

   - A configuração geral do RouterOS passa pela criação de *bridges*, a atribuição de IPs às *interfaces* e *bridges*, na definição de encaminhamentos, a configuração NAT, na criação de VLANs, na definição de VPN, a activação e configuração do serviço de DHCP e a configuração da *firewall*. Em seguida, são configurados os pontos 2 a 6, mencionados abaixo.

2. RADIUS *authentication* e *accounting*

   - Configuração do serviço de *authentication* e *accounting*.

```
/radius add accounting-port=1813 address=x.x.x.x authentication-port=1812
    disabled=no secret=aaaaaa service=ppp,hotspot
/radius incoming
set accept=no port=1700
```

   radius add: Adicionar novo serviço RADIUS

   accounting-port e authentication-port: Portos de comunicação com o servidor RADIUS

   address: IP do servidor RADIUS

   secret: chave NAS configurada no servidor RADIUS em */usr/raddb/clients.conf*

   service: Serviços de autenticação, hotspot(UAM) e ppp(PPPOE)

   incoming port: Porto para desconexão remota de utilizadores

3. Configuração Hotspot (UAM)

   - Criação do serviço de hotspot

```
/ip hotspot add address-pool=hs-pool-4 disabled=no idle-timeout=5m interface=
    scbridge1 name=hotspot23 profile=hsprof1
```

   ip hotspot add: novo servidor de hotspot

   address-pool: Intervalo de IPs a atribuir aos clientes (*pool* com o nome *hs-pool-4*)

   disabled: "no" significa activado

idle-timeout: Inactivo durante 5 minutos a sessão termina

interface: interface que está configurado o hotspot, *bridge* com o nome *sc-bridge1*

name: nome atribuído ao servidor hotspot (*hotspot23*)

profile: perfil utilizado pelo servidor hotspot (perfil criado abaixo)

- Criação do *profile* para utilização do servidor hotspot

```
/ip hotspot profile add dns-name=status.wifi hotspot-address=172.16.0.1 html-
    directory=hotspot login-by=mac,http-chap mac-auth-password=aaaaaa name=
    hsprof1 radius-accounting=yes radius-interim-update=5m use-radius=yes
```

dns-name: Fully Qualified Domain Name do NAS (*status.wifi*)

hotspot-address: IP do NAS (*gateway* dos equipamentos *client*)

html-directory: Directoria da página html para autenticação UAM

login-by: Tipo de autenticação (mac e chap)

mac-auth-password: Password utilizada para autenticação por mac(user=mac, pass=mac-auth-password)

name: Nome de perfil do hotspot (*hsprof1*)

radius-accounting: Utilizar accounting para o hotspot

radius-interim-update: Intervalo de tempo em que o RADIUS accounting faz update

use-radius: Utilizar RADIUS na autenticação

4. Configuração PPP

   - PPPOE Server

```
/interface pppoe-server server add authentication=chap,mschap1,mschap2
    default-profile=default-encrytion disabled=no interface=scbridge1 max-mru
    =1480 max-mtu=1480 service-name=pppoeserver
```

interface pppoe-server server: criação do servidor PPPOE

authentication: tipo de autenticação suportada pelo servidor PPPOE (chap, mschap1, mschap2)

default-profile: perfil utilizado por defeito

disabled: estado do servidor (*no*, activado)

interface: interface onde funciona o servidor (*scbridge*)

max-mru[7]*:* recebimento máximo de 1480 bytes por unidade/pacote

max-mtu[8]*:* envio máximo de 1480 bytes por unidade/pacote

service-name: nome do servidor PPPOE (*ppposerver*)

- Alteração de perfil utilizado por PPPOE

```
/ppp profile set default-encryption dns-server=172.16.0.1,80.172.48.226 local
    -address=172.16.0.1 remote-address=pppPool use-encryption=yes
```

ppp profile set default-encryption: alteração do perfil *default-encryption*

dns-server: lista de dns atribuída aos equipamentos *client*

local-address: IP do NAS ou IP do servidor PPPOE (*gateway* dos equipamentos *client*)

remote-address: pool de IPs distribuídos aos equipamentos *client* (*pppPool*)

use-encryption: utilizar encriptação na autenticação dos equipamentos *client* por PPPOE

5. Pool de IPs para hotspot

```
/ip pool add name=hs-pool-4 ranges=172.16.50.1-172.16.200.1
```

6. Pool de IPs para hotspot

```
/ip pool add name=pppPool ranges=172.16.200.10-172.16.255.254
```

[7]Maximum Receive Unit
[8]Maximum Transmission Unit

Capítulo 7

Considerações Finais e Trabalho Futuro

7.1 Considerações Finais

Este trabalho foi motivado pelo interesse em desenvolver um projecto e aplicar o seu esforço e conhecimento em algo promissor. Muitas decisões e indecisões passaram ao longo de todo este trabalho. Factores financeiros ditaram alguns aspectos na implementação, nomeadamente na escolha de equipamentos e de acessos iniciais à Internet. Salienta-se que todo o investimento deste projecto foi efectuado pelos fundadores da empresa. A fase inicial de testes ditaram alguns indicadores de sucesso na implementação do projecto, a rede WI-FI ao ser disponibilizada era detectada por pessoas que se conectavam e navegavam na Internet, sendo divulgada "boca a boca" o projecto que iria nascer. O objectivo do projecto é ser sustentável, assim, foi desde cedo obrigado e condicionado a agendamentos programados para alterações quer em equipamentos emissores ou servidores de suporte ao projecto. Estes condicionamentos deveram-se única e exclusivamente à defesa da imagem do bom funcionamento do projecto desde o seu início, junto dos clientes finais.

O projecto materializou-se numa panóplia de tecnologias conjugadas entre si com a finalidade de levar a Internet às pessoas através de hotspots ou às residências

através do acesso à última milha. É possível caracterizar o projecto em 5 grandes fases, sendo elas: o início do projecto, o qual se deu na altura do estudo da rede a implementar; a escolha das ligações no acesso à Internet e equipamentos activos de rede, *switchs*, *routers* e *Access Points*; a definição e construção de módulos standard de emissão de sinal; a implementação dos servidores de suporte ao projecto (servidor WEB, DNS, RADIUS, mail, Projects, Streaming, VPN, Backups); e por fim os sistemas intermédios de autenticação (NAS), de gestão e monitorização de utilizadores e equipamentos.

A SemCabo contabiliza 1971 utilizadores (Consulta efectuada dia 27 de Outubro de 2009). São efectuados em média cerca de 10000 acessos mês, contabilizando todos os tipos de autenticação, UAM, PPPOE, PPTP e L2TP/IPSec. São ainda, contabilizados 270 GBytes de tráfego total (dados referentes ao mês de Agosto de 2009). Actualmente as localidades onde o projecto está presente são: Santiago do Cacém, Sines, Alvalade Sado, Cercal, Porto Côvo e Vila Nova de Milfontes.

7.2 Trabalho Futuro

Como trabalho futuro, numa primeira fase: serão virtualizados todos os servidores para melhor optimização de recursos e de gestão; continuação no desenvolvimento da aplicação de criação de utilizadores; o alargamento da rede para outras áreas geográficas; testar outros tipos de autenticação, nomeadamente no acesso à última milha; melhorar e desenvolver o sistema de monitorização implementado.

Numa segunda fase: instalar e configurar outros servidores RADIUS, passando o principal a fazer de proxy RADIUS, sendo desta forma possível criar sub-domínios de autenticação, e ainda possibilitando a criação de Mini-ISPs baseados na estrutura da SemCabo; efectuar estudos e testes sobre IP TV, VoD e vídeo vigilância em cima de sistemas sem fios, nomeadamente na rede SEMCABO-WIFI.

Bibliografia

[1] *RADIUS (Consulta Julho de 2009),* http://www.ietf.org/rfc/rfc2865.txt, http://www.ietf.org/rfc/rfc2138.txt, http://www.ietf.org/rfc/rfc2139.txt, http://www.ietf.org/rfc/rfc2548.txt

[2] *NAS (Consulta Julho de 2009)*, http://www.rfc-archive.org/getrfc.php?rfc=2881

[3] *802.1x (Consulta Julho de 2009)*, http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

[4] *PPPOE (Consulta Outubro de 2009)*, http://www.ietf.org/rfc/rfc2516.txt

[5] *PPTP (Consulta Setembro de 2009)*, http://www.faqs.org/rfcs/rfc2637.html

[6] *L2TP/IPSec (Consulta Setembro de 2009)*, http://www.rfc-archive.org/getrfc.php?rfc=3193

[7] *EAP (Consulta Setembro de 2009)*, http://www.ietf.org/rfc/rfc2284.txt, http://www.ietf.org/rfc/rfc2716.txt

[8] *Aradial Server (Consulta Julho de 2009)*, http://www.aradial.com

[9] *IAS (Consulta Agosto de 2009)*, http://technet.microsoft.com/en-us/network/bb643123.aspx

[10] *Cisco ACS (Consulta Setembro de 2009)*, http://www.cisco.com/en/US/ products/sw/secursw/ps2086/index.html

[11] *RouterOS (Consulta Setembro de 2009)*, http://www.routeros.com

[12] *StarOS (Consulta Outubro de 2009)*, http://www.staros.com

[13] *Freeradius server (consulta Setembro de 2009)*, http://www.freeradius.org

[14] *PhpMyPrepaid (Consultado Outubro de 2009)*, http://sourceforge.net/projects/phpmyprepaid

[15] *DaloRadius (Consulta Outubro de 2009)*, http://sourceforge.net/ projects/daloradius

[16] *ChilliSpot (Consulta Outubro de 2009)*, http://www.chillispot.info

[17] *DD-WRT (Consulta Outubro de 2009)*, http://www.dd-wrt.com

[18] *OpenWRT (Consulta Outubro de 2009)*, http://www.openwrt.org

[19] *RouterOS (Consulta Outubro de 2009)*, http://www.routeros.com

[20] *APACHE Web Server (Consulta a Outubro de 2009)*, http://www.apache.org

[21] *Qmail (Consulta a Outubro de 2009)*, http://www.lifewithqmail.org

[22] *DotProject (Consulta a Outubro de 2009)*, http://www.dotproject.net

[23] *RSYNC (Consulta a Setembro de 2009)*, http://rsync.samba.org

[24] *Sender Policy Framework (Consulta a Setembro de 2009)*, http://www.openspf.org

[25] *Red5 Open Source Flash Server (Consulta a Setembro de 2009)*, http://osflash.org/red5

Apêndice A

Módulos de Autenticação

A.1 Chillispot e RouterOS

```
###### index.php ######
######Author: Armando Ventura ######
<?php
session_start();
if(!session_is_registered("visited"))
{
echo "What you want here???";
exit();
}
//Autenticação para RouterOS
$path_login;
if(session_is_registered("auth"))
{
$path_login="http://status.wifi/login?encript=pass";
session_register("path_login");
}
else
{
$path_login="http://network.wifi:3990/prelogin";
session_register("path_login");
}
?>


###### config_db.php ######
######Author: Armando Ventura ######
<?php
//Config Access Data Base
$COMPUTER = 'localhost';
```

```
$USER = 'aaaa';
$DB_PASSWORD = 'aaaaaa';
$DB = 'radius';

$result = mysql_connect($COMPUTER,$USER,$DB_PASSWORD);
if (!$result) {
die('Could not connect - Contact Administrator of the database system...');

}
$db = mysql_select_db($DB,$result);
if (!$db)
die("Error to open database!!!!");

?>

###### register_user.php ######
######Author: Armando Ventura ######
<?php
require("functions_control_wifi.php");
//validate the necessary fields
if($name=="" || $address=="" || $email=="" || $country=="Select your Country" ||
    $phone=="" || $userName=="" || $password1=="" || $password2=="")
{
echo "<div align='center'><span class='style11'>Error:* You must write Necessary
    Fields</span></div>";
include("register_user_form.php"); // to fill the fields again
exit();  // end the script
}
//verify if passwords are different
if($password1 != $password2)
{
echo "<div align='center'><span class='style11'>Error:* you have a different
    password, write again...</span></div>";
include("register_user_form.php"); // to fill the fields again
exit();  // end the script
}
//Verify the lenght of the user name and passwords
if(strlen($userName)<5 || strlen($password1)<5)
{
echo "<div align='center'><span class='style11'>Error: UserName and Pasword must
    have 5-10 Characteres, try again...</span>        </div>";
include("register_user_form.php"); // to fill the fields again
exit();  // end the script
}
//check email
if(!ValidateMail($email)){
echo "<div align='center'><span class='style11'>Error:* your EMAIL is not valid or
```

```
    does not exist , write again... </span>                </div>";
include("register_user_form.php"); // to fill the fields again
exit();  // end the script
}
include("config_db.php");
$result_sql =  mysql_query("select count(*) from radcheck where UserName = '
    $userName'");
$numUserName = mysql_fetch_row($result_sql);

if($numUserName[0] > 0) // If exist username
{
echo "<div align='center'><span class='style11'>Error: Define other USER, the user
    <strong>$userName</strong> already exists          </span></div>";
include("register_user_form.php"); // to fill the fields again
exit();  // end the script
}
else //Create new user
{    //insert data in gratis table

mysql_query("INSERT INTO gratis( codigoSequencial , userName , dateCreation , name,
    address , contry , email , phone , obs , status , others) VALUES ('' , '$userName',
    '".date('Y-m-d')." ".date('H:i:s')."', '$name', '$address', '$country', '$email
    ', '$phone', '$comments', 'unblocked', '')");
mysql_query("insert into gratis (codigoSequencial , userName, dateTimeCreation , name
    , address , contry , email , phone , obs) values('','$userName','".date('Y-m-d')."
    ".date('H:i:s')."','$name','$address','$country','$email','$phone','$comments')
    ");
//insert data in radcheck table
mysql_query("insert into radcheck (UserName, Attribute , op, Value , complet_name)
values ('$userName','Password','==','$password1','$name')");

//insert data in usergroup table
mysql_query("insert into usergroup (UserName, GroupName)
values ('$userName','gratis')");

}
include("create_new_user_sucess.php");
?>


###### controlAccess.php ######
######Author: Armando Ventura ######
<?php
/*
Módulo que controla os vouchers de minutos
acrescentar a linha seguinte no inicio da secção de login no semcabowifi.php
controlAccess($_GET['uid'],$_GET['pwd']);
```

```
*/
//Function Control Minutes
function controlAccess($login, $password)
{
$sql = mysql_query("select UserName, Value from radcheck  where UserName='$login'
    and Value='$password'");

if( mysql_num_rows($sql) > 0) // if user and password exist
{

//verificar a que tipo de voucher o utilizador pertence, a que grupo pertence se
    voucher ou assinatura ou gratis
$groupUser = mysql_query("select GroupName from usergroup  where UserName='$login
    '");
$registerAccess = mysql_fetch_row($groupUser);

if($registerAccess[0] == "voucher") // if voucher days or minutes
{
$sql = mysql_query("select UserName, Attribute , Value from radreply  where
    UserName='$login'");
$register = mysql_fetch_row($sql);

if( mysql_num_rows($sql) > 0) //if user have register in radreply attribute Session
    -Timeout or WISPr-Session-Terminate-Time
{
if ($register[1] == "Session-Timeout") //if voucher minutes
{
$sqlSumSecondsConsumed = mysql_query("select sum(AcctSessionTime) from radacct
    where UserName='$login'");
$registerSumSecondsConsumed = mysql_fetch_row($sqlSumSecondsConsumed);

$sqlMinutesVoucher = mysql_query("select minutes from vouchers where userName='
    $login'");
$registerMinutesVoucher = mysql_fetch_row($sqlMinutesVoucher);

$actualSecondsLeft = ($registerMinutesVoucher[0]*60) - $registerSumSecondsConsumed
    [0];

mysql_query("UPDATE radreply SET Value = '".$actualSecondsLeft."' where UserName =
    '$login' and
Attribute='Session-Timeout'");
// efectuar código para quando termina o cartão dos minutos, dar mensagem ao
    utilizador
}
if ($register[1] == "WISPr-Session-Terminate-Time") //if voucher days
{
if($register[2] == "0000-00-00T00:00:00+00:00")//if is the first time that user
```

```
    connect
{
$sqlDaysVoucher = mysql_query("select days from vouchers where userName='$login'");
$registerDaysVoucher = mysql_fetch_row($sqlDaysVoucher); // time in days
$newDate = date("Y-m-d",strtotime('now')+($registerDaysVoucher[0]*24*60*60))."T".
    date('H:i:s')."+00:00";
mysql_query("UPDATE radreply SET Value = '".$newDate."' where UserName = '$login'
    and
Attribute='WISPr-Session-Terminate-Time'");
// efectuar código para quando termina o cartão dos dias, dar mensagem ao
    utilizador
}}}
}//end type of voucher - days or minutes
else
{echo "Access Control ERROR, Try Later - thanks";}
}//end function control minutes
?>


###### status.php ######
######Author: Armando Ventura ######
<?php
include("config_db.php");
$L_IP = $_SERVER["REMOTE_ADDR"];
$statement = "select value,complet_name from radcheck where UserName ='".$UserName
    ."'";
$result = mysql_query($statement);
$row = mysql_fetch_object($result);
$password = $row->value;
$complete_name = $row->complet_name;

if($UserPassword == $password && $UserPassword != '')
{
//tipo de conta ( grátis, assinatura, voucher, especial )
$statement = "select GroupName from usergroup where UserName ='".$UserName."'";
$result = mysql_query($statement );
$row = mysql_fetch_object($result);
$group_name = $row->GroupName;

if($group_name == "")
$group_name = "Especial";

$statement = "select sum(AcctSessionTime) as time_total, count(AcctSessionTime) as
    total_connections, sum(AcctInputOctets) as total_input, sum(AcctOutputOctets)
    as total_output from radacct where UserName ='".$UserName."'";
$result = mysql_query($statement );
$row = mysql_fetch_object($result);
```

```
$time_total_hours=($row->time_total / 3600);
$time_total_minutes=($row->time_total % 3600) / 60;
$time_total_seconds=($row->time_total % 3600)%60;
$total_connections=$row->total_connections;
$total_downloads = ($row->total_input / 1024) / 1024;
$total_uploads = ($row->total_output / 1024) / 1024;

echo '<p> </p>
<table width="200" border="0" align="center">
<tr>
<td><div align="center" class="text1">Status Account </div></td>
</tr>
</table>
<table width="315" height="25" border="0" align="center">
<tr>
<td width="373">';
echo '<br><br><br><b>Hello '.$complete_name.' ('.$UserName.')</b><br>';
//echo '<br> your IP address is:' . $L_IP .' <br>';
echo " <br> You use a <b>$group_name</b> account.";
echo " <br> You use a total of: <b>".round($time_total_hours,0)." Hora(s) ".round(
    $time_total_minutes,0)." Minute(s)
".round($time_total_seconds,0)." Seconds(s) </b>.";
echo ' <br> You use a total of: <b>'.round($total_downloads,2)." MBytes Uploads </b
    >.";
echo ' <br> You use a total of: <b>'.round($total_uploads,2)." Mbytes Downloads</b
    >.";
echo ' <br> You use a total of: <b>'.round($total_downloads+$total_uploads,2)."
    Mbytes </b> and a number of <b>".$total_connections." conections</b>.</center
    >";
echo '</td>
</tr>
</table>
<p> </p>
<table width="180" border="0" align="center">
<tr>
<td width="83"><div align="right" class="text1"><span class="style9">Powered by </
    span></div></td>
<td width="87"><img src="logo.jpg" width="87" height="28" border="1" /></td>
</tr>
</table>';
}
else
{
echo "<p> </p><div align='center'><span class='style11'>ERROR: username does
    not exist or password error, try again...</span>        </div>";
include ("status_form.php");
```

```
}
?>
```

Apêndice B

RADIUS

B.1 Tabelas - Dicionário de Dados

#confpag

Field	Type	Null	Default	Comments
codPag	int(11)	No		
fileName	varchar(255)	No		
top	varchar(255)	No		
center	varchar(255)	No		
bottom	varchar(255)	No		

#ddns

Field	Type	Null	Default	Comments
cod	int(11)	No		
IP	varchar(50)	No		
date	date	No	0000-00-00	
local	varchar(50)	No		

#funcionario

Field	Type	Null	Default	Comments
codFunc	int(10)		No	
login	varchar(15)	No		
password	varchar(15)	No		
nome	varchar(40)	No		
cargo	varchar(30)	No		

#gratis

Field	Type	Null	Default	Comments
codigoSequencial	bigint(20)	No		
userName	varchar(20)	No		
dateCreation	varchar(30)	No	0000-00-00	
name	varchar(50)	No		

```
address          varchar(50)      No
contry   varchar(20)      No
email    varchar(50)      No
phone    varchar(14)      No
obs      text     No
status   enum('blocked', 'unblocked')     No       blocked
others   varchar(100)     No

#nas
Field    Type     Null     Default  Comments
id       int(10)  No
nasname          varchar(128)     No
shortname        varchar(32)      Yes      NULL
type     varchar(30)      Yes      other
ports    int(5)   Yes      NULL
secret   varchar(60)      No       secret
community        varchar(50)      Yes      NULL
description      varchar(200)     Yes      RADIUS Client

#radacct
Field    Type     Null     Default  Comments
RadAcctId        bigint(21)       No
AcctSessionId    varchar(32)      No
AcctUniqueId     varchar(32)      No
UserName         varchar(64)      No
Realm    varchar(64)      Yes
NASIPAddress     varchar(15)      No
NASPortId        int(12)  Yes      NULL
NASPortType      varchar(32)      Yes      NULL
AcctStartTime    datetime         No       0000-00-00 00:00:00
AcctStopTime     datetime         No       0000-00-00 00:00:00
AcctSessionTime          int(12)  Yes      NULL
AcctAuthentic    varchar(32)      Yes      NULL
ConnectInfo_start        varchar(32)      Yes      NULL
ConnectInfo_stop         varchar(32)      Yes      NULL
AcctInputOctets          bigint(12)       Yes      NULL
AcctOutputOctets         bigint(12)       Yes      NULL
CalledStationId          varchar(50)      No
CallingStationId         varchar(50)      No
AcctTerminateCause       varchar(32)      No
ServiceType      varchar(32)      Yes      NULL
FramedProtocol   varchar(32)      Yes      NULL
FramedIPAddress          varchar(15)      No
AcctStartDelay   int(12)  Yes      NULL
AcctStopDelay    int(12)  Yes      NULL

#radcheck
```

Field	Type	Null	Default	Comments
id	int(11)		No	
UserName	varchar(64)		No	
Attribute	varchar(32)		No	
op	char(2)	No	==	
Value	varchar(253)		No	
complet_name	text		No	
address	longtext		No	
country	text		No	
email	text	No		
phone	text	No		
obs	longtext		No	
force_alt_dados	char(3)	No	OFF	
msg_force_alt_dados	longtext		No	

#radgroupcheck

Field	Type	Null	Default	Comments
id	int(11)		No	
GroupName	varchar(64)		No	
Attribute	varchar(32)		No	
op	char(2)	No	==	
Value	varchar(253)		No	

#radgroupreply

Field	Type	Null	Default	Comments
id	int(11)		No	
GroupName	varchar(64)		No	
Attribute	varchar(32)		No	
op	char(2)	No	=	
Value	varchar(253)		No	
prio	int(10)		No	0

radpostauth

Field	Type	Null	Default	Comments
id	int(11)	No		
user	varchar(64)		No	
pass	varchar(64)		No	
reply	varchar(32)		No	
date	timestamp		Yes	CURRENT_TIMESTAMP

#radreply

Field	Type	Null	Default	Comments
id	int(11)		No	
UserName	varchar(64)		No	
Attribute	varchar(32)		No	
op	char(2)	No	=	

```
Value    varchar(253)    No

#usergroup
Field    Type    Null    Default  Comments
id       int(11)         No
UserName         varchar(64)     No
GroupName        varchar(64)     No

#voucher15Dias
Field    Type    Null    Default  Comments
codidoSequencial         bigint(20)      No
userName         varchar(20)     No
estadoCartao     enum('Nao Utilizado', 'Em Uso', 'Gasto', 'Expirado', 'Bloqueado')       No
emitido          enum('SIM', 'NAO')      No      NAO
dataCriacao      date    No      0000-00-00
dataEmissao      date    No      0000-00-00
codCliente       int(11) No      0
tipoSaida        enum('Oferta', 'Pago')  No      Pago

#voucher1Dia
Field    Type    Null    Default  Comments
codidoSequencial         bigint(20)      No
userName         varchar(20)     No
estadoCartao     enum('Nao Utilizado', 'Em Uso', 'Gasto', 'Expirado', 'Bloqueado')       No
emitido          enum('SIM', 'NAO')      No      NAO
dataCriacao      date    No      0000-00-00
dataEmissao      date    No      0000-00-00
codCliente       int(11) No      0
tipoSaida        enum('Oferta', 'Pago')  No      Pago

#voucher30Dias
Field    Type    Null    Default  Comments
codidoSequencial         bigint(20)      No
userName         varchar(20)     No
estadoCartao     enum('Nao Utilizado', 'Em Uso', 'Gasto', 'Expirado', 'Bloqueado')       No
emitido          enum('SIM', 'NAO')      No      NAO
dataCriacao      date    No      0000-00-00
dataEmissao      date    No      0000-00-00
codCliente       int(11) No      0
tipoSaida        enum('Oferta', 'Pago')  No      Pago

#voucher360Minutos
Field    Type    Null    Default  Comments
codidoSequencial         bigint(20)      No
userName         varchar(20)     No
estadoCartao     enum('Nao Utilizado', 'Em Uso', 'Gasto', 'Expirado', 'Bloqueado')       No
emitido          enum('SIM', 'NAO')      No      NAO
```

dataCriacao	date	No	0000-00-00	
dataEmissao	date	No	0000-00-00	
codCliente	int(11)	No	0	
tipoSaida	enum('Oferta', 'Pago')	No		

#voucher3Dias

Field	Type	Null	Default	Comments
codidoSequencial	bigint(20)	No		
userName	varchar(20)	No		
estadoCartao	enum('Nao Utilizado', 'Em Uso', 'Gasto', 'Expirado', 'Bloqueado')	No		
emitido	enum('SIM', 'NAO')	No	NAO	
dataCriacao	date	No	0000-00-00	
dataEmissao	date	No	0000-00-00	
codCliente	int(11)	No	0	
tipoSaida	enum('Oferta', 'Pago')	No		

#voucher60Minutos

Field	Type	Null	Default	Comments
codidoSequencial	bigint(20)	No		
userName	varchar(20)	No		
estadoCartao	enum('Nao Utilizado', 'Em Uso', 'Gasto', 'Expirado', 'Bloqueado')	No		
emitido	enum('SIM', 'NAO')	No	NAO	
dataCriacao	date	No	0000-00-00	
dataEmissao	date	No	0000-00-00	
codCliente	int(11)	No	0	
tipoSaida	enum('Oferta', 'Pago')	No	Pago	

#voucher720Minutos

Field	Type	Null	Default	Comments
codidoSequencial	bigint(20)	No		
userName	varchar(20)	No		
estadoCartao	enum('Nao Utilizado', 'Em Uso', 'Gasto', 'Expirado', 'Bloqueado')	No		
emitido	enum('SIM', 'NAO')	No	NAO	
dataCriacao	date	No	0000-00-00	
dataEmissao	date	No	0000-00-00	
codCliente	int(11)	No	0	
tipoSaida	enum('Oferta', 'Pago')	No	Pago	

#voucher7Dias

Field	Type	Null	Default	Comments
codidoSequencial	bigint(20)	No		
userName	varchar(20)	No		
estadoCartao	enum('Nao Utilizado', 'Em Uso', 'Gasto', 'Expirado', 'Bloqueado')	No		
emitido	enum('SIM', 'NAO')	No	NAO	
dataCriacao	date	No	0000-00-00	
dataEmissao	date	No	0000-00-00	
codCliente	int(11)	No	0	

tipoSaida	enum('Oferta', 'Pago')	No	Pago	

#vouchers

Field	Type	Null	Default	Comments
userName	varchar(64)	No		
minutes	int(11)	Yes	NULL	
days	int(11)	Yes	NULL	
signature	enum('SIM', 'NULL')	Yes	NULL	

Apêndice C

ChilliSpot

C.1 Ficheiro semcabowifi.php

```
<?php
#File semcabowifi.php
#Autenticação UAM para ChilliSpot

session_start();
$uamsecret = "aaaaaa";
$loginpath = "semcabowifi.php";
$_GET['challenge'];
$_GET['timeleft'];
$_GET['prelogin'];
$_GET['userurl'];
$_GET['chal'];
$_GET['reply'];
$_GET['login'];
$_GET['logout'];
$_GET['prelogin'];
$_GET['nasid'];
$aplic_host="172.16.100.101";
#Login
if ($_GET['login'] == login)
        {
        if(!(session_is_registered("security")))
        {
                //echo "variavel security por registar";
                die("EN:What do you here? <br> PT:O que faz por aqui?");
        }
        else
        {
                include("config_db.php");
```

```
                include("controlAccess.php");
                controlAccess($_GET['uid'],$_GET['pwd']);
        }
        $hexchal = pack ("H32", $_GET['chal']);
        if (isset ($uamsecret))
                {
                  $newchal = pack ("H*", md5($hexchal . $uamsecret));
                }
        else
                {
                  $newchal = $hexchal;
                }
        $response = md5("\0" . $_GET['pwd'] . $newchal);
        $newpwd = pack("a32", $_GET['pwd']);
        $password = implode ("", unpack("H32", ($newpwd ^ $newchal)));
        include("wait_to_connect.html");
        if ((isset ($uamsecret)) && isset($userpassword))
                {
                  print '<meta http-equiv="refresh" content="3;url=http://' . $_GET
                      ['uamip'] . ':' . $_GET['uamport'] . '/logon?username=' .
                      $_GET['uid'] . '&password=' . $password . '&timeleft=10">';
                }
        else
                {
                  print '<meta http-equiv="refresh" content="3;url=http://' . $_GET
                      ['uamip'] . ':' . $_GET['uamport'] . '/logon?username=' .
                      $_GET['uid'] . '&response=' . $response . 'timeleft=10">';
                }
        }
#Login successful
if ($_GET['res'] == success)
        {
        include("success.php");
        }
#Login failed
if ($_GET['res'] == failed)
        {
        echo "Login Failed!!!, Sorry, try again<br>";
        include("login.html");
        }
#Logged out
if ($_GET['res'] == logoff)
        {
        include("logoff.html");
        }
#Tried to login while already logged in
if ($_GET['res'] == already)
```

```
        {
        echo "Already logged in!!!!!";
        }
#Not logged in yet
if ($_GET['res'] == logon)
        {
        include("login.html");
        }
#Notyet login
if ($_GET['res'] == notyet)
        {
        include("login.html");

        if ($_GET['reply']) {
          print '<center>' . $_GET['reply'] . '</center>';
        }
        }
?>
```

C.2 Firewall para Arquitectura PC

```
#!/bin/sh
#
# Firewall script for ChilliSpot (Linux Fedora Core XX)
# A Wireless LAN Access Point Controller
#
# Uses $EXTIF (eth0) as the external interface (Internet or intranet) and
# $INTIF (eth1) as the internal interface (access points).
#
#
# SUMMARY
# * All connections originating from chilli are allowed.
# * Only ssh is allowed in on external interface.
# * Nothing is allowed in on internal interface.
# * Forwarding is allowed to and from the external interface, but disallowed
#   to and from the internal interface.
# * NAT is enabled on the external interface.

IPTABLES="/sbin/iptables"
EXTIF="eth0"
INTIF="eth1"

$IPTABLES -P INPUT DROP
$IPTABLES -P FORWARD ACCEPT
$IPTABLES -P OUTPUT ACCEPT
```

```
#Allow related and established on all interfaces (input)
$IPTABLES -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#Allow releated, established and ssh on $EXTIF. Reject everything else.
$IPTABLES -A INPUT -i $EXTIF -p tcp -m tcp --dport 22 --syn -j ACCEPT
$IPTABLES -A INPUT -i $EXTIF -p tcp -m tcp --dport 53 --syn -j ACCEPT
$IPTABLES -A INPUT -i $EXTIF -j REJECT

#Allow related and established from $INTIF. Drop everything else.
$IPTABLES -A INPUT -i $INTIF -j DROP

#Allow http and https on other interfaces (input).
#This is only needed if authentication server is on same server as chilli
$IPTABLES -A INPUT -p tcp -m tcp --dport 80 --syn -j ACCEPT
$IPTABLES -A INPUT -p tcp -m tcp --dport 443 --syn -j ACCEPT
$IPTABLES -A INPUT -p tcp -m tcp --dport 53 --syn -j ACCEPT
$IPTABLES -A INPUT -p tcp -m tcp --dport 10000 --syn -j ACCEPT

#Allow 3990 on other interfaces (input).
$IPTABLES -A INPUT -p tcp -m tcp --dport 3990 --syn -j ACCEPT

#Allow everything on loopback interface.
$IPTABLES -A INPUT -i lo -j ACCEPT

# Drop everything to and from $INTIF (forward)
# This means that access points can only be managed from ChilliSpot
$IPTABLES -A FORWARD -i $INTIF -j DROP
$IPTABLES -A FORWARD -o $INTIF -j DROP

#Enable NAT on output device
$IPTABLES -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE
```

C.3 Firewall OpenWRT

```
#!/bin/sh
#
# Firewall script for ChilliSpot on OpenWRT
#
# Uses $WANIF (vlan1) as the external interface (Internet or intranet) and
# $WLANIF (eth1) as the internal interface (access point).
# $LANIF is used as a trusted management interface.
#
# SUMMARY
# * All connections originating from ChilliSpot are allowed.
# * Nothing is allowed in on WAN interface.
# * Nothing is allowed in on WLAN interface.
```

```
# * Everything is allowed in on LAN interface.
# * Forwarding is allowed to and from WAN interface, but disallowed
# to and from the WLAN interface.
# * NAT is enabled on the WAN interface.

. /etc/functions.sh

WANIF=$(nvram get wan_ifname)
WLANIF=$(nvram get wifi_ifname)
LANIF=$(nvram get lan_ifname)

IPTABLES="/usr/sbin/iptables"

for T in filter nat mangle ; do
$IPTABLES -t $T -F
$IPTABLES -t $T -X
done

$IPTABLES -P INPUT DROP
$IPTABLES -P FORWARD ACCEPT
$IPTABLES -P OUTPUT ACCEPT

#Allow related and established on all interfaces (input)
$IPTABLES -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#Allow ssh from $WAN
$IPTABLES -A INPUT -i $WANIF -p tcp -m tcp --dport 22 --syn -j ACCEPT
$IPTABLES -A INPUT -i $WLANIF -p tcp -m tcp --dport 22 --syn -j ACCEPT
$IPTABLES -A INPUT -i $LANIF -p tcp -m tcp --dport 22 --syn -j ACCEPT

#Allow related and established $WANIF. Reject everything else.
$IPTABLES -A INPUT -i $WANIF -j REJECT

#Allow related and established $WLANIF. Drop everything else.
$IPTABLES -A INPUT -i $WLANIF -j DROP

#Allow 3990 on other interfaces (input).
$IPTABLES -A INPUT -p tcp -m tcp --dport 3990 --syn -j ACCEPT

#Allow everything on loopback interface.
$IPTABLES -A INPUT -i lo -j ACCEPT

#Allow everything on $LANIF
#$IPTABLES -A INPUT -i $LANIF -j ACCEPT

#Drop everything to and from $WLANIF (forward)
$IPTABLES -A FORWARD -i $WLANIF -j DROP
```

```
$IPTABLES -A FORWARD -o $WLANIF -j DROP

#Drop everything to and from $WLANIF (forward)
$IPTABLES -A FORWARD -i $LANIF -j DROP
$IPTABLES -A FORWARD -o $LANIF -j DROP

#Enable NAT on output device.
$IPTABLES -t nat -A POSTROUTING -o $WANIF -j MASQUERADE
```

Apêndice D

RouterOS

D.1 Configuração RouterOS

```
# oct/21/2009 16:46:52 by RouterOS
#
/interface bridge
add admin-mac=00:00:00:00:00:00 ageing-time=5m arp=enabled auto-mac=yes \
    comment="" disabled=no forward-delay=15s max-message-age=20s mtu=1500 \
    name=scbridge1 priority=0x8000 protocol-mode=none transmit-hold-count=6
/interface ethernet
set 0 arp=enabled auto-negotiation=yes comment="" disabled=no full-duplex=yes \
    mac-address=00:0C:42:2F:27:60 mtu=1500 name=ether1 speed=100Mbps
set 1 arp=enabled auto-negotiation=yes bandwidth=unlimited/unlimited comment=\
    "" disabled=no full-duplex=yes mac-address=00:0C:42:2F:27:61 master-port=\
    none mtu=1500 name=ether2 speed=100Mbps
set 2 arp=enabled auto-negotiation=yes bandwidth=unlimited/unlimited comment=\
    "" disabled=no full-duplex=yes mac-address=00:0C:42:2F:27:62 master-port=\
    none mtu=1500 name=ether3 speed=100Mbps
set 3 arp=enabled auto-negotiation=yes bandwidth=unlimited/unlimited comment=\
    "" disabled=no full-duplex=yes mac-address=00:0C:42:2F:27:63 master-port=\
    none mtu=1500 name=ether4 speed=100Mbps
set 4 arp=enabled auto-negotiation=yes bandwidth=unlimited/unlimited comment=\
    "" disabled=no full-duplex=yes mac-address=00:0C:42:2F:27:64 master-port=\
    none mtu=1500 name=ether5 speed=100Mbps
/interface wireless security-profiles
set default authentication-types="" eap-methods=passthrough group-ciphers="" \
    group-key-update=5m interim-update=0s mode=none name=default \
    radius-eap-accounting=no radius-mac-accounting=no \
    radius-mac-authentication=no radius-mac-caching=disabled \
    radius-mac-format=XX:XX:XX:XX:XX:XX radius-mac-mode=as-username \
    static-algo-0=none static-algo-1=none static-algo-2=none static-algo-3=\
    none static-key-0="" static-key-1="" static-key-2="" static-key-3="" \
```

```
    static-sta-private-algo=none static-sta-private-key="" \
    static-transmit-key=key-0 supplicant-identity=MikroTik tls-certificate=\
    none tls-mode=no-certificates unicast-ciphers="" wpa-pre-shared-key="" \
    wpa2-pre-shared-key=""
/ip hotspot profile
set default dns-name="" hotspot-address=0.0.0.0 html-directory=hotspot \
    http-cookie-lifetime=3d http-proxy=0.0.0.0:0 login-by=cookie,http-chap \
    name=default rate-limit="" smtp-server=0.0.0.0 split-user-domain=no \
    use-radius=no
add dns-name=status.wifi hotspot-address=172.16.0.1 html-directory=hotspot \
    http-proxy=0.0.0.0:0 login-by=mac,http-chap mac-auth-password=conf3218 \
    name=hsprof1 nas-port-type=wireless-802.11 radius-accounting=yes \
    radius-default-domain="" radius-interim-update=5m radius-location-id="" \
    radius-location-name="" rate-limit="" smtp-server=0.0.0.0 \
    split-user-domain=no use-radius=yes
/ip hotspot user profile
set default advertise=no idle-timeout=none keepalive-timeout=2m name=default \
    open-status-page=always shared-users=1 status-autorefresh=1m \
    transparent-proxy=yes
/ip ipsec proposal
set default auth-algorithms=sha1 disabled=no enc-algorithms=3des lifetime=30m \
    name=default pfs-group=modp1024
/ip pool
add name=hs-pool-4 ranges=172.16.50.1-172.16.200.1
add name=pppPool ranges=172.16.200.10-172.16.255.254
/ip dhcp-server
add address-pool=hs-pool-4 authoritative=after-2sec-delay bootp-support=\
    static disabled=no interface=scbridge1 lease-time=1h name=dhcp1
/ip hotspot
add address-pool=hs-pool-4 addresses-per-mac=2 disabled=no idle-timeout=5m \
    interface=scbridge1 keepalive-timeout=none name=hotspotescritorio \
    profile=hsprof1
/port
set 0 baud-rate=115200 data-bits=8 flow-control=none name=serial0 parity=none \
    stop-bits=1
/ppp profile
set default change-tcp-mss=yes comment="" dns-server=172.16.0.1,80.172.48.226 \
    local-address=172.16.0.1 name=default only-one=default remote-address=\
    pppPool use-compression=default use-encryption=yes use-vj-compression=\
    default
set default-encryption change-tcp-mss=yes comment="" name=default-encryption \
    only-one=default use-compression=default use-encryption=yes \
    use-vj-compression=default
/interface pptp-client
add add-default-route=no allow=pap,chap,mschap1,mschap2 comment="" \
    connect-to=213.228.144.25 disabled=no max-mru=1460 max-mtu=1460 mrru=\
    disabled name=pptp-out1 password=escri2323 profile=default-encryption \
```

```
    user=alvalade1
/queue type
set default kind=pfifo name=default pfifo-limit=50
set ethernet-default kind=pfifo name=ethernet-default pfifo-limit=50
set wireless-default kind=sfq name=wireless-default sfq-allot=1514 \
    sfq-perturb=5
set synchronous-default kind=red name=synchronous-default red-avg-packet=1000 \
    red-burst=20 red-limit=60 red-max-threshold=50 red-min-threshold=10
set hotspot-default kind=sfq name=hotspot-default sfq-allot=1514 sfq-perturb=\
    5
set default-small kind=pfifo name=default-small pfifo-limit=10
/routing bgp instance
set default as=65530 client-to-client-reflection=yes comment="" disabled=no \
    ignore-as-path-len=no name=default out-filter="" redistribute-connected=\
    no redistribute-ospf=no redistribute-other-bgp=no redistribute-rip=no \
    redistribute-static=no router-id=0.0.0.0
/routing ospf area
add area-id=0.0.0.0 authentication=none disabled=no name=backbone type=\
    default
/snmp
set contact="" enabled=no engine-boots=0 engine-id="" location="" \
    time-window=15 trap-sink=0.0.0.0 trap-version=1
/snmp community
set public address=0.0.0.0/0 authentication-password="" \
    authentication-protocol=MD5 encryption-password="" encryption-protocol=\
    DES name=public read-access=yes security=none
/system logging action
set memory memory-lines=100 memory-stop-on-full=no name=memory target=memory
set disk disk-lines=100 disk-stop-on-full=no name=disk target=disk
set echo name=echo remember=yes target=echo
set remote name=remote remote=0.0.0.0:514 target=remote
/system routerboard settings
set baud-rate=115200 boot-delay=2s boot-device=nand-if-fail-then-ethernet \
    boot-protocol=bootp cpu-frequency=300MHz enable-jumper-reset=yes \
    enter-setup-on=any-key
set baud-rate=115200 boot-delay=2s boot-device=nand-if-fail-then-ethernet \
    boot-protocol=bootp cpu-frequency=300MHz enable-jumper-reset=yes \
    enter-setup-on=any-key
/user group
add name=read policy="local,telnet,ssh,reboot,read,test,winbox,password,web,sn\
    iff,!ftp,!write,!policy"
add name=write policy="local,telnet,ssh,reboot,read,write,test,winbox,password\
    ,web,sniff,!ftp,!policy"
add name=full policy="local,telnet,ssh,ftp,reboot,read,write,policy,test,winbo\
    x,password,web,sniff"
add name=grandola policy="ssh,reboot,read,!local,!telnet,!ftp,!write,!policy,!\
    test,!winbox,!password,!web,!sniff"
```

```
/interface bridge port
add bridge=scbridge1 comment="" disabled=no edge=auto external-fdb=auto \
    horizon=none interface=ether2 path-cost=10 point-to-point=auto priority=\
    0x80
add bridge=scbridge1 comment="" disabled=no edge=auto external-fdb=auto \
    horizon=none interface=ether3 path-cost=10 point-to-point=auto priority=\
    0x80
add bridge=scbridge1 comment="" disabled=no edge=auto external-fdb=auto \
    horizon=none interface=ether4 path-cost=10 point-to-point=auto priority=\
    0x80
add bridge=scbridge1 comment="" disabled=no edge=auto external-fdb=auto \
    horizon=none interface=ether5 path-cost=10 point-to-point=auto priority=\
    0x80
/interface bridge settings
set use-ip-firewall=no use-ip-firewall-for-vlan=no
/interface ethernet mirror
set mirror-port=none source-port=none
/interface l2tp-server server
set authentication=pap,chap,mschap1,mschap2 default-profile=\
    default-encryption enabled=no max-mru=1460 max-mtu=1460 mrru=disabled
/interface ovpn-server server
set auth=sha1,md5 certificate=none cipher=blowfish128,aes128 default-profile=\
    default enabled=no keepalive-timeout=60 mac-address=FE:AD:7F:03:9F:0F \
    max-mtu=1500 mode=ip netmask=24 port=1194 require-client-certificate=no
/interface pppoe-server server
add authentication=chap,mschap1,mschap2 default-profile=default disabled=no \
    interface=scbridge1 keepalive-timeout=10 max-mru=1480 max-mtu=1480 \
    max-sessions=0 mrru=disabled one-session-per-host=no service-name=\
    pppoeserver
/interface pptp-server server
set authentication=mschap1,mschap2 default-profile=default-encryption \
    enabled=no keepalive-timeout=30 max-mru=1460 max-mtu=1460 mrru=disabled
/interface wireless align
set active-mode=yes audio-max=-20 audio-min=-100 audio-monitor=\
    00:00:00:00:00:00 filter-mac=00:00:00:00:00:00 frame-size=300 \
    frames-per-second=25 receive-all=no ssid-all=no
/interface wireless sniffer
set channel-time=200ms file-limit=10 file-name="" memory-limit=10 \
    multiple-channels=no only-headers=no receive-errors=no streaming-enabled=\
    no streaming-max-rate=0 streaming-server=0.0.0.0
/interface wireless snooper
set channel-time=200ms multiple-channels=yes receive-errors=no
/ip accounting
set account-local-traffic=no enabled=no threshold=256
/ip accounting web-access
set accessible-via-web=no address=0.0.0.0/0
/ip address
```

```
add address=192.168.2.50/24 broadcast=192.168.2.255 comment="" disabled=no \
    interface=ether1 network=192.168.2.0
add address=172.16.0.1/16 broadcast=172.16.255.255 comment="" disabled=no \
    interface=scbridge1 network=172.16.0.0
/ip dhcp-server config
set store-leases-disk=5m
/ip dhcp-server network
add address=172.16.0.0/16 comment="hotspot network" gateway=172.16.0.1
/ip dns
set allow-remote-requests=yes cache-max-ttl=1w cache-size=2048KiB \
    max-udp-packet-size=512 primary-dns=172.16.0.1 secondary-dns=\
    80.172.48.225
/ip firewall connection tracking
set enabled=yes generic-timeout=10m icmp-timeout=10s tcp-close-timeout=10s \
    tcp-close-wait-timeout=10s tcp-established-timeout=1d \
    tcp-fin-wait-timeout=10s tcp-last-ack-timeout=10s \
    tcp-syn-received-timeout=5s tcp-syn-sent-timeout=5s tcp-syncookie=no \
    tcp-time-wait-timeout=10s udp-stream-timeout=3m udp-timeout=10s
/ip firewall filter
add action=passthrough chain=unused-hs-chain comment=\
    "place hotspot rules here" disabled=yes
/ip firewall nat
add action=passthrough chain=unused-hs-chain comment=\
    "place hotspot rules here" disabled=yes
add action=masquerade chain=srcnat comment="masquerade hotspot network" \
    disabled=no src-address=172.16.0.0/16
/ip firewall service-port
set ftp disabled=no ports=21
set tftp disabled=no ports=69
set irc disabled=no ports=6667
set h323 disabled=no
set sip disabled=no
set pptp disabled=no
/ip hotspot service-port
set ftp disabled=no ports=21
/ip hotspot user
add comment="" disabled=no name=admin password=futureinovation profile=\
    default
/ip hotspot walled-garden
add action=allow comment="" disabled=no server=hotspotescritorio
add action=allow comment="" disabled=no server=hotspotescritorio
add action=allow comment="" disabled=no dst-port=22 server=hotspotescritorio
/ip neighbor discovery
set scbridge1 discover=yes
set ether1 discover=yes
set ether2 discover=yes
set ether3 discover=yes
```

```
set ether4 discover=yes
set ether5 discover=yes
set pptp-out1 discover=no
/ip proxy
set always-from-cache=no cache-administrator=webmaster cache-drive=system \
    cache-hit-dscp=4 cache-on-disk=no enabled=no max-cache-size=unlimited \
    max-client-connections=600 max-fresh-time=3d max-server-connections=600 \
    parent-proxy=0.0.0.0 parent-proxy-port=0 port=8080 serialize-connections=\
    no src-address=0.0.0.0
/ip route
add comment="" disabled=no distance=1 dst-address=0.0.0.0/0 gateway=\
    192.168.2.1 scope=30 target-scope=10
/ip service
set telnet address=0.0.0.0/0 disabled=yes port=23
set ftp address=0.0.0.0/0 disabled=yes port=21
set www address=0.0.0.0/0 disabled=yes port=809
set ssh address=0.0.0.0/0 disabled=no port=22
set www-ssl address=0.0.0.0/0 certificate=none disabled=yes port=443
set api address=0.0.0.0/0 disabled=yes port=8728
set winbox address=0.0.0.0/0 disabled=no port=8291
/ip socks
set connection-idle-timeout=2m enabled=no max-connections=200 port=1080
/ip traffic-flow
set active-flow-timeout=30m cache-entries=4k enabled=no \
    inactive-flow-timeout=15s interfaces=all
/ip upnp
set allow-disable-external-interface=yes enabled=no show-dummy-rule=yes
/ppp aaa
set accounting=yes interim-update=0s use-radius=yes
/queue interface
set scbridge1 queue=default
set ether1 queue=ethernet-default
set ether2 queue=ethernet-default
set ether3 queue=ethernet-default
set ether4 queue=ethernet-default
set ether5 queue=ethernet-default
set pptp-out1 queue=default
/radius
add accounting-backup=no accounting-port=1813 address=80.172.48.226 \
    authentication-port=1812 called-id="" comment="" disabled=no domain="" \
    realm="" secret=ajvwjfhdcoerguid239dm44jf service=ppp,hotspot timeout=\
    300ms
/radius incoming
set accept=no port=1700
/routing mme
set bidirectional-timeout=2 gateway-class=none gateway-keepalive=1m \
    gateway-selection=no-gateway origination-interval=5s preferred-gateway=\
```

```
    0.0.0.0 timeout=1m ttl=50
/routing ospf
set distribute-default=never metric-bgp=20 metric-connected=20 \
    metric-default=1 metric-rip=20 metric-static=20 mpls-te-area=unspecified \
    mpls-te-router-id=unspecified redistribute-bgp=no redistribute-connected=\
    no redistribute-rip=no redistribute-static=no router-id=0.0.0.0
/routing rip
set distribute-default=never garbage-timer=2m metric-bgp=1 metric-connected=1 \
    metric-default=1 metric-ospf=1 metric-static=1 redistribute-bgp=no \
    redistribute-connected=no redistribute-ospf=no redistribute-static=no \
    timeout-timer=3m update-timer=30s
/system clock manual
set dst-delta=+00:00 dst-end="jan/01/1970 00:00:00" dst-start=\
    "jan/01/1970 00:00:00" time-zone=+00:00
/system console
add disabled=no port=serial0 term=vt102
/system health
set fan-mode=auto use-fan=main
/system identity
set name=alv1
/system logging
add action=memory disabled=no prefix="" topics=info
add action=memory disabled=no prefix="" topics=error
add action=memory disabled=no prefix="" topics=warning
add action=echo disabled=no prefix="" topics=critical
/system note
set note="" show-at-login=yes
/system ntp client
set enabled=yes mode=unicast primary-ntp=78.46.194.188 secondary-ntp=\
    193.126.17.66
/system scheduler
add comment="" disabled=no interval=3d name=autoreboot on-event=reboot \
    start-date=jan/01/2008 start-time=06:00:00
add comment="" disabled=no interval=30m name=ddns on-event=ddns start-time=\
    startup
/system script
add name=reboot policy=\
    ftp,reboot,read,write,policy,test,winbox,password,sniff source=\
    "/system reboot"
add name=ddns policy=ftp,reboot,read,write,policy,test,winbox,password,sniff \
    source="/tool fetch address=www.semcabo.pt port=80 mode=http src-path=/con\
    trol/ddns/ddns-alvalade1.php"
/system upgrade mirror
set check-interval=1d enabled=no primary-server=0.0.0.0 secondary-server=\
    0.0.0.0 user=""
/system watchdog
set auto-send-supout=no automatic-supout=yes no-ping-delay=5m watch-address=\
```

```
    none watchdog-timer=yes
/tool bandwidth-server
set allocate-udp-ports-from=2000 authenticate=yes enabled=yes max-sessions=10
/tool e-mail
set from=<> server=0.0.0.0
/tool graphing
set store-every=5min
/tool mac-server
add disabled=no interface=all
/tool mac-server ping
set enabled=yes
/tool sniffer
set file-limit=10 file-name="" filter-address1=0.0.0.0/0:0-65535 \
    filter-address2=0.0.0.0/0:0-65535 filter-protocol=ip-only filter-stream=\
    yes interface=all memory-limit=10 only-headers=no streaming-enabled=no \
    streaming-server=0.0.0.0
/user aaa
set accounting=yes default-group=read interim-update=0s use-radius=no
```