

UNIVERSIDADE DE TRÁS-OS-MONTES E ALTO DOURO

Modelo de Gestão para Redes Wireless Banda Larga

DISSERTAÇÃO DE MESTRADO EM
Informática

NUNO FILIPE PEREIRA SALVADOR



Modelo de Gestão para Redes Wireless

Banda Larga

Dissertação de Mestrado apresentada por

Nuno Filipe Pereira Salvador

Sob orientação de Prof. Doutor Vítor Manuel de Jesus Filipe e

Prof. Doutor António Manuel de Jesus Pereira

Universidade de Trás-os-Montes e Alto Douro



Vila Real, 2008

Departamento de Engenharias

2008

AGRADECIMENTOS

Quero expressar os meus agradecimentos a todas as pessoas e instituições que, directa e indirectamente, contribuíram para a realização deste trabalho.

Começo com o meu profundo agradecimento aos meus incansáveis orientadores, Professor Doutor António Manuel de Jesus Pereira, Professor Coordenador do Departamento de Engenharia Informática do Instituto Politécnico de Leiria da Escola Superior de Tecnologia e Gestão, e ao Professor Doutor Vítor Manuel de Jesus Filipe, Professor Auxiliar do Departamento de Engenharias da Universidade de Trás-os-Montes e Alto Douro. Sem os seus incentivos e todo o apoio prestado ao longo do processo de desenvolvimento deste trabalho, não seria possível concluí-lo com sucesso.

Agradeço ainda ao Instituto Politécnico de Leiria (IPL), Escola Superior de Tecnologia e Gestão (ESTG) de Leiria e ainda à Universidade de Trás-os-Montes e Alto Douro (UTAD) pelos meios e condições que colocou ao meu dispor para a realização deste trabalho.

À minha família e aos meus amigos, um enorme obrigado pela presença e apoio nos momentos mais complicados ao longo deste percurso.

Aos meus pais, o meu sincero e sentido agradecimento, por me terem proporcionado todas as condições para chegar até aqui, sem o seu esforço, a realização deste trabalho não teria sido possível.

Por fim, nunca conseguirei expressar todo o meu agradecimento pelo apoio, paciência e compreensão que recebi da minha esposa Virgínia ao longo de toda esta difícil jornada. As horas a que foi privada da minha companhia ao longo deste ano e meio, constituem um enorme esforço, e por isso agradeço-lhe do fundo do coração, e dedico-lhe também esta dissertação.

RESUMO

Actualmente, devido a questões de índole financeiras, as operadoras de acesso à Internet não investem em zonas rurais porque não existe compensação financeira adequada ao investimento, nem uma solução tecnicamente válida. Este facto origina cada vez mais o aparecimento das designadas redes WBL (Wireless Banda Larga), que permitem fornecer acesso à Internet às populações discriminadas por esta circunstância. Os aspectos relacionados com a gestão destas redes são normalmente esquecidos e actualmente existe uma carência de soluções economicamente viáveis que possam auxiliar com eficiência esta função.

Após uma pesquisa intensiva de soluções comerciais e *opensource*, de gestão de redes WBL, verificou-se a inexistência de uma solução economicamente viável, assim como, a ausência de um modelo de gestão para as zonas rurais. Este trabalho contribui para a definição de um modelo de gestão, assim como para parte da sua implementação.

A proposta do modelo assenta numa solução centralizada, que congrega vários módulos de software *opensource*, capazes de responder ao conjunto de funcionalidades identificadas como essenciais ao modelo.

Os testes efectuados mostram que o modelo apresentado representa uma solução completa, capaz de abranger as várias áreas do processo de gestão de redes WBL em zonas rurais.

Palavras chave: wireless Banda Larga, gestão wifi, gestão de redes wireless, opensource na gestão de redes wireless, modelo de gestão de redes wireless banda larga, ferramentas de gestão de redes wireless banda larga.

ABSTRACT

Currently, due to questions of financial order, the Internet Service Providers do not invest in rural zones, because the investment is not profitable, and technologically doesn't exist a model definition. This fact originates more and more the appearance of the calls WBN (Wireless Broadband Networks), that are going to supply access to the Internet to populations discriminated by this circumstance. The aspects related with the management of these networks are normally forgetful and currently exists a lack of economically and technical viable solutions, that be able to help with efficiency this function.

After an intensive research of commercial and opensource solutions to management the wireless networks, it was verified the absence of an economically viable solution as well as the absence of a model of management for the WBN in rural zones. This article contributes to the definition of a management model of these networks.

The proposal model settles in a centralized solution, that congregates several modules of opensource software, able to respond to the range of essential features identified in the model. The tests show that the model presented, represents a complete solution, able to cover several areas of the process of WBL management.

Keywords: wireless broadband, wifi network management, wireless network management, opensource for wireless management, model for wireless broadband networks, management tools for wireless broadband networks.

ÍNDICE

LISTA DE ABREVIATURAS	10
LISTA DE TABELAS	12
LISTA DE FIGURAS	13
1. INTRODUÇÃO	16
1.1 Contexto da temática	16
1.2 Objectivos	18
1.3 Organização do documento	19
2. REDES WIRELESS BANDA LARGA	20
2.1 Conceito Wireless Banda Larga	20
2.1.1 Normas IEEE 802.11	20
2.1.2 REDES WLAN	27
2.1.3 REDES WMAN	28
2.1.4 REDES WRAN	29
2.1.5 REDES WBL	30
2.2 Arquitecturas de redes WLAN	31
2.2.1 Point-to-Point	32
2.2.2 Peer-to-Peer/Ad-hoc	32
2.2.3 Point-to-MultiPoint, APs Autónomos	33
2.2.4 WLAN Gateways	34
2.2.5 Controladores WLAN	35
2.2.6 Arquitectura Distribuída	38
2.2.7 WLAN Arrays	40
2.2.8 Arquitecturas unificadas	41
2.3 Tendência de Implementação das redes WBL	42
2.3.1 MuniWireless	43

2.3.2	Projectos de Investigação.....	44
2.3.3	Desafios na Gestão de Redes WBL	50
2.4	Resumo.....	53
3.	Levantamento de Funcionalidades e de soluções de gestão de redes WBL.....	56
3.1	Funcionalidades de gestão de redes WBL.....	56
3.2	Soluções Opensource	61
3.2.1	Sistemas Operativos Wireless (<i>firmwares wireless</i>).....	61
3.2.2	Portais Captativos (<i>hotspot's gateways</i>)	63
3.2.3	Ferramentas de Auditoria de segurança.....	64
3.2.4	Inventário, Monitorização e Diagnóstico.....	65
3.2.5	Serviços Baseados em Localização	69
3.2.6	Live CD's.....	72
3.3	Soluções Comerciais	73
3.3.1	AirWave Wireless Management Suite.....	73
3.3.2	Colubris Network Management System	74
3.3.3	AirMagnet Enterprise.....	74
3.3.4	Wavelink Avalanche MC.....	74
3.3.5	Cisco Wireless Control System	74
3.3.6	WiFi Manager	75
3.3.7	HP ProCurve Manager Plus	75
3.4	Comparação de Soluções	75
3.4.1	RESUMO.....	81
4.	MODELO DE GESTÃO DE REDES WBL	84
4.1	Metodologia para Implementação de Gestão de redes WBL.....	84
4.2	Princípios Técnicos e Ferramentas.....	87
4.3	Objectivos e Funcionalidades.....	90
4.3.1	Características Globais.....	93

4.3.2	Função Infra-estrutura.....	94
4.3.3	Função Segurança	96
4.3.4	Função Monitorização	97
4.3.5	RESUMO.....	101
5.	TESTES E RESULTADOS.....	102
5.1	Cenário	102
5.2	Infra-estrutura - Serviços de rede e Controlo de Acessos	104
5.3	Infra-estrutura - Inventário	113
5.4	Análise de Resultados	120
6.	CONCLUSÃO.....	122
6.1	Principais contribuições	123
6.2	Trabalho Futuro.....	124
7.	Referências e Bibliografia	126

LISTA DE ABREVIATURAS

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AoA	Angle of Arrival
APs	Access Point(s)
BS	Base Stations
CAPWAP	Control and Provisioning of Wireless Access Points
CDMA	Code Division Multiple Access
CPU	Central Process Unit
CWIND	Center for Wireless Network Design
DAS	Dynamic Spectrum Access
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EHAS	Enlace Hispano Americano de Salud
ESSID	Extended Service Set Identifier
GPL	General Public License
GPS	Global Position System
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HF	High Frequency
HNPS	Heterogeneous Network for European Public Safety
HSPDA	High-Speed Downlink Packet Access
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Eletronics Engineers
IETF	Internet Engineering Task Force
IT	Information Technology
IP	Internet Protocol
LAN	Local Area Network
LBS	Location-Based Services
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
LWAPP	Lightweight Access Point Protocol
MAC	Medium Access Control
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MP	Mesh Point
MRTG	Multi Router Traffic Grapher
NMS	Network Management System

OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
P2P	Peer-to-Peer
PC	Personal Computer
PDA	Personal digital assistants
PHP	Hypertext Preprocessor
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RDDTools	Round Robin Database
RF	Rádio Frequência
RFMON	Radio Frequency Monitoring
RSSI	Received Signal Strength Indicator
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SVG	Scalable Vectorial Graphics
TETRA	Terrestrial Trunked Radio
TCP	Transmit Power Protocol
TKIP	Temporal Key Integrity Protocol
UAM	Universal Access Method
UHF	Ultra High Frequency
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VHF	Very High Frequency
VLANs	Virtual Local Area Networks
VOIP	Voice over Internet Protocol
VoWLAN	Voice over WLAN
VPN	Virtual Private Network
WAVE	Wireless Access in Vehicular Environments
WCS	Cisco Wireless Control System
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Networks
WPAN	Wireless Personal Area Network
WMM	Wireless Multimedia
WOL	Wake On Lan
WPA	Wireless Protected Access
WRAN	Wireless Regional Area Networks
WTPs	WLAN Termination Points
WWAN	Wireless Wide Area Network
XML	eXtensible Markup Language

LISTA DE TABELAS

Tabela 1: Características das normas IEEE 802.11	21
Tabela 2: Arquitectura Centralizada vs Distribuída.....	39
Tabela 3: Funcionalidades de gestão de redes WBL	60
Tabela 4: Soluções <i>opensource</i> de segurança	65
Tabela 5: Soluções <i>opensource</i> de inventário, monitorização e diagnóstico.....	68
Tabela 6: Projectos <i>opensource</i> relacionados com serviços de localização wireless	71
Tabela 7: Comparação de funcionalidades entre soluções <i>Opensource</i> e soluções Comerciais	80
Tabela 8: Princípios técnicos e a sua correspondência com as o modelo OSI.....	86
Tabela 9: Princípios técnicos e a sua correspondência com o modelo OSI	86

LISTA DE FIGURAS

Figura 1: Mecanismo de funcionamento da norma IEEE 802.11s.....	26
Figura 2 : Exemplo de Redes WLAN.....	28
Figura 3: Tecnologias Wireless.....	31
Figura 4: Arquitectura <i>point-to-point</i>.....	32
Figura 5: Arquitectura <i>Peer-to-Peer/Ad-hoc</i>	33
Figura 6: Arquitectura Point-to-Multipoint.....	34
Figura 7: Arquitectura WLAN Gateway.....	35
Figura 8:<i>Thin aps</i> numa arquitectura de gestão de WLAN centralizada.....	36
Figura 9 : Arquitectura distribuída	39
Figura 10: Arquitectura WLAN array vs tradicional e controladores.....	41
Figura 11: Arquitecturas unificadas	42
Figura 12: Redes MuniWireless	44
Figura 13: Arquitectura da rede IEEE 802.22 (WRAN).....	48
Figura 14: Arquitectura do projecto HNPS	49
Figura 15: Implementação do projecto HNPS	49
Figura 16: Ciclo de inovação da tecnologia Wireless	51
Figura 17: Estimativa de posição de um transmissor a partir da medição do ângulo de chegada do sinal de duas posições distintas.....	70
Figura 18: Distribuição das funcionalidades de acordo com o tipo de software.....	81
Figura 19: Soluções com mais ocorrências na Tabela 7	81
Figura 20: Metodologia de monitorização de redes wireless	85
Figura 21: Arquitectura de gestão de redes WBL (visão de alto nível)	92
Figura 22: Funções da gestão de rede WBL.....	93
Figura 23: Modelo de gestão para as redes WBL	101
Figura 24: Cenário de testes.....	103
Figura 25: Interface do Webmin	105
Figura 26: Página de entrada Daloradius.....	106
Figura 27: Informações sobre o tráfego dos utilizadores	107
Figura 28: Localização de um <i>hotspot</i> no GoogleMaps através do Daloradius.....	108
Figura 29: Gráfico do nº de autenticações gerado pelo Daloradius	108

Figura 30: Exemplo de um vírus bloqueado com o HAVP	109
Figura 31: Termos e condições de acesso à rede	110
Figura 32: Menu de Opções	111
Figura 33: Mensagens mostradas ao utilizador de acordo com o perfil	111
Figura 34: Exemplo de um relatório criado pelo SARG	112
Figura 35: Exemplo de um relatório detalhado de um utilizador gerado pelo SARG..	112
Figura 36: Exemplo de um relatório detalhado de um utilizador, gerado pelo Squint.	113
Figura 37: Arquitectura do Openview	114
Figura 38: Arquitectura da solução implementada no Openview.....	115
Figura 39: Exemplo das redes encontradas pelo OpenView.....	116
Figura 40: Exemplo dos dispositivos de rede descobertos pelo OpenView.	116
Figura 41: Exemplo da descoberta automática de dispositivos com o Openview.....	117
Figura 42: Monitorização de um AP através do Nagios/Centreon.....	118
Figura 43: Relatório de disponibilidade de um AP e dos serviços a ele associados	118
Figura 44: Monitorização do servidor OpenView	119
Figura 45: Monitorização do interface Ethernet 4 do servidor OpenView	119

1. INTRODUÇÃO

Neste capítulo pretende-se efectuar o enquadramento do tema da tese, identificando-se os objectivos propostos e a organização do documento.

1.1 CONTEXTO DA TEMÁTICA

Com o aparecimento das redes Banda Larga, as exigências dos utilizadores no uso da Internet aumentaram significativamente, não só relativamente ao desempenho e velocidade, mas também pelo aparecimento de novas aplicações como a voz, vídeo, P2P (*Peer-to-Peer*), etc. A Largura de Banda é hoje considerada um bem essencial como o são outros bens como a água, a luz, o saneamento, entre outros. Infelizmente, por razões meramente economicistas, algumas regiões de cariz mais rural não são contempladas com o acesso à Internet de Banda Larga. As limitações do ADSL (*Asymmetric Digital Subscriber Line*) relacionados com as distâncias, obrigam os operadores a fazer investimentos, que raramente acontecem porque segundo a sua óptica, o retorno do investimento não é alcançado [Hudson,2003]. As pessoas que vivem nestas regiões sofrem por isso uma discriminação tecnológica apenas e só, porque vivem onde vivem.

É por isso importante encontrar uma alternativa tecnológica ao ADSL, fornecendo Banda Larga a estas regiões. As redes WBL (*Wireless Banda Larga*) surgem como primeira alternativa, pois permitem o fornecimento de Banda Larga em grande escala com custos relativamente baixos. Sendo assim, o primeiro desafio é encontrar uma solução de rede WBL, que permita a estas regiões a mitigação desta infoexclusão. Esta rede deve ser implementada segundo normas de segurança rigorosas, uma vez que será implementada no domínio público, sendo por isso o segundo desafio. O último desafio, mas não menos importante, é a criação de um sistema de gestão centralizado, que para além de uma solução eficaz, poderá também ser eficiente, ou seja, gerir bem ao melhor custo.

As tecnologias de Banda Larga, também designadas por *wireless broadband*, incluem todas as tecnologias que permitem transferência de dados multimédia e dados com elevada largura de banda. A Banda Larga pode ser definida como: o conjunto de serviços de alta velocidade

quer sejam voz, dados ou vídeo, assim como a infra-estrutura subjacente, clientes e tecnologias que permitem estes serviços. Especificamente o conteúdo da Banda Larga é digital e a taxa de transmissão é de pelo menos 384Kbps [Papacharissi et al,2006].

Como nas zonas rurais a Banda Larga através do cabo nem sempre chega, a WBL assume-se como a melhor solução, para fornecer o acesso à Internet nestas zonas.

A proposta de um modelo de gestão contribui para uma clara definição do que deve ser uma solução eficaz e económica, uma vez que nesta área os grandes fabricantes de equipamentos já oferecem soluções de elevada maturidade. No entanto, a proliferação das redes wireless rurais é um facto consumado, pelo que se manifesta essencial este contributo.

São vários os desafios que se colocam à gestão de redes WBL, uma vez que as arquitecturas evoluíram no sentido da centralização e da unificação. Hoje em dia a função de gestão de redes, tem tendência a não distinguir a tecnologia em uso. O mesmo equipamento tem a capacidade para suportar os dois tipos de redes, logo, a gestão da rede, quer wireless quer cablada, será facilitada porque a questão da centralização será cada vez mais abrangente [Synergy,2006]. À medida que as tecnologias wireless permitem maior cobertura e maior velocidade, a proliferação do uso destas tecnologias ocorrerá. A instalação de mais equipamentos em diversos locais da rede é por isso uma realidade. A preocupação da gestão deve agora contemplar novos factores e condições. O planeamento é extremamente importante para uma boa implementação, os *site surveys* devem ser mais completos, com informação relativa aos constrangimentos de espaços (paredes, objectos metálicos, árvores, edifícios, etc.). A gestão de redes wireless deverá suportar a monitorização da RF (rádio frequência) integrando serviços de localização. As organizações têm hoje uma heterogeneidade de equipamentos de vários fabricantes, além disso prestam serviços de redes wireless, quer aos seus colaboradores, quer ao público (*hotspots*), sendo por isso de ter em conta a possibilidade de gerir equipamentos de fabricantes diferentes e de dar suporte a uma variedade de aplicações de acordo com o perfil de utilizador.

A complexidade da gestão aumenta, obrigando os administradores de sistemas a um esforço cada vez maior para gerir as redes wireless. A simplificação de processos de administração de rede wireless são agora mais importantes que nunca, suscitando a necessidade de centralizar todos os aspectos da gestão. Configurar equipamentos num cenário com vários fabricantes e políticas de segurança pode ser um pesadelo. A gestão de redes wireless *indoor*, é por si já

um processo complexo, mitigado pela utilização de *switchs* WLAN (*Wireless Local Area Network*) agregadores de APs (*Access Points*). A gestão de redes WBL em zonas rurais torna-se um desafio ainda muito maior. O ambiente e as necessidades diferem, impelindo à identificação de requisitos que possam facilitar e diminuir custos com a gestão deste tipo de redes.

As questões relativas à segurança deverão ser contempladas nos sistemas de gestão de redes wireless. É vital controlar os acessos à rede, assim como evitar associações de APs não autorizados. As soluções deverão fornecer relatórios detalhados com informação bastante rica de forma a ajudar a equipa de suporte a solucionar e identificar problemas na rede, ponderar também a possibilidade de efectuar controlo de tráfego, quer para incrementar a performance quer para permitir *biling* (facturação) [Balachandran et al, 2005]. Uma boa solução de gestão de wireless deve, para além das capacidades de inventário, monitorização e configuração, ter capacidades de planeamento, integração de ferramenta de *helpdesk* e diagnóstico e correlação de eventos [Halton,2007].

Todos estes aspectos estão hoje mais do que nunca na ordem do dia, preocupando os administradores de redes. As organizações estão a esforçar-se para responder a este novo desafio, não obstante o longo caminho que ainda têm para percorrer. Nas zonas rurais, onde os recursos são muito menores, o caminho é ainda muito mais longo.

A proposta do modelo apresentado, nesta dissertação, converge para este interesse, na medida em que soluciona e simplifica de uma forma económica e técnica, a complexidade da gestão de redes WBL em zonas rurais. Contribui ainda para a identificação de uma panóplia de funcionalidades que uma solução deste tipo deverá contemplar.

1.2 OBJECTIVOS

O trabalho que aqui se apresenta faz parte de um projecto global na ESTG (Escola Superior de Tecnologias e Gestão de Leiria), que inclui três aspectos fundamentais:

- Definição de uma infra-estrutura de rede Wireless Banda Larga;
- Segurança em Redes Wireless Banda Larga;
- Gestão Centralizada de Redes Wireless Banda Larga - sendo este, o tema objecto da presente dissertação.

Pretende-se com este trabalho clarificar o conceito da gestão centralizada de redes Wireless Banda Larga, apresentando uma proposta de modelo para a gestão das mesmas. Será descrito o estado da arte, fazendo-se uma retrospectiva da gestão de redes wireless. Levar-se-á a cabo um levantamento das soluções comerciais e *opensource*, existentes no mercado. Após esta análise serão identificados os requisitos e funcionalidades que uma a solução de gestão de redes wireless deverá contemplar, contribuindo para a definição do modelo definido.

A proposta de modelo contribuirá para uma definição e identificação que ajudará a simplificar o processo de gestão das redes wireless das zonas rurais, assim como aumentar a qualidade da mesma.

Procura-se ainda demonstrar através dos testes, o caminho para a prossecução de uma solução *opensource*, considerando sempre um aspecto fundamental, que é a centralização da gestão de redes WBL, para as zonas rurais.

1.3 ORGANIZAÇÃO DO DOCUMENTO

O presente documento além da introdução está organizado em mais cinco capítulos:

- Capítulo 2: Redes Wireless Banda Larga – Este capítulo consiste num levantamento sumário sobre a evolução das arquitecturas de redes wireless ao longo dos anos, assim como o ponto de situação actual da gestão das mesmas. Neste capítulo serão ainda abordados alguns conceitos e definições sobre as redes wireless.
- Capítulo 3: Funcionalidades e Soluções de gestão de redes Wireless - Principais soluções existentes (comerciais e *opensource*) para a gestão das redes wireless. Neste capítulo faz-se num levantamento das principais ferramentas existentes para a gestão de redes wireless, quer comerciais, quer *opensource*.
- Capítulo 4: Proposta de modelo para a gestão de Redes WBL – Neste capítulo apresenta-se uma proposta para um modelo de gestão de redes WBL centralizada, levando em conta os estudos nos capítulos anteriores e as funcionalidades pretendidas.
- Capítulo 5: Implementação e resultados – Neste capítulo são descritas as implementações de algumas funcionalidades do modelo.
- Capítulo 6: Conclusões e trabalhos futuros – Neste capítulo apresentam-se as conclusões do estudo efectuado, as principais contribuições e algumas propostas para trabalhos futuros.

2. REDES WIRELESS BANDA LARGA

Neste capítulo pretende fazer-se uma clarificação dos conceitos que são objecto deste trabalho, assim como uma revisão das questões relacionadas com a gestão das redes WBL. Serão afloradas questões relativas às diversas tecnologias wireless, e às tendências que foram ocorrendo ao longo dos anos, nomeadamente na evolução da gestão destas redes. Será ainda efectuado um ponto de situação do estado actual da gestão de redes wireless.

Antes de se entrar em detalhe no objecto de estudo deste trabalho, importa clarificar a definição de alguns conceitos das tecnologias wireless. Após este esclarecimento, serão abordados os aspectos relacionados com a evolução das redes wireless, nomeadamente no estudo da evolução da arquitectura das mesmas. Será por isso efectuado uma pequena definição/explicação das normas IEEE 802.11.

Serão ainda descritos os desafios que a gestão das redes wireless têm actualmente, assim como as soluções futuras que se perspectivam para simplificar a mesma.

Identificaram-se também alguns projectos de investigação que estão a decorrer nesta área, nomeadamente na Europa e na América Latina.

2.1 CONCEITO WIRELESS BANDA LARGA

O propósito deste trabalho incide sobre as redes WBL, cujo conceito, devido à evolução rápida das tecnologias e à panóplia de termos, é muitas vezes impreciso, originando alguma confusão na utilização da terminologia. Este ponto tentará definir e clarificar este conceito, fazendo referência a algumas tecnologias que têm enquadramento nas redes WBL.

2.1.1 NORMAS IEEE 802.11

Antes de entrar numa descrição mais detalhada sobre as normas, importa fazer um périplo histórico das mesmas. A especificação básica de redes IEEE 802.11 foi finalizada pelo IEEE¹

¹ <http://www.ieee.org>

em 1997. Esta norma especificava na altura a operação na frequência de ondas de rádio livre 2.4 GHz, com taxa de dados de 1 Mbps e 2 Mbps. Em 1999, o IEEE publicou os acréscimos 802.11a e 802.11b, que ampliam a taxa de transmissão para 54Mbps e 11 Mbps, respectivamente. O IEEE 802.11b mantém a operação na frequência 2.4 GHz, enquanto que o IEEE 802.11a passa a operar na frequência 5GHz. O IEEE 802.11a suporta taxas variando de 6 a 54Mbps, sendo obrigatória a implementação das taxas de 6, 12 e 24 Mbps [Geier,2002].

Em 2003, o IEEE publicou a norma IEEE 802.11g que alcança taxas de transmissão de 54 Mbps. Como o IEEE 802.11b, o IEEE 802.11g opera na frequência de 2.4GHz, o que torna as duas normas compatíveis. O padrão é definido de forma que IEEE 802.11b e IEEE 802.11g trabalhem em conjunto, sem a necessidade de mudança de pontos de acesso, ou seja, é possível ligar dispositivos IEEE 802.11g em pontos de acesso IEEE 802.11b e vice-versa.

Em 2004 surgiu a norma IEEE 802.11i, que aumentou consideravelmente a segurança, definindo melhores procedimentos para autenticação, autorização e criptografia. Em 2005 foi aprovada a especificação IEEE 802.11e, agregando qualidade de serviço (QoS) às redes IEEE 802.11. Foram lançados comercialmente os primeiros pontos de acesso trazendo pré-implementações da especificação IEEE 802.11e.

Em 2006 começaram as primeiras implementações da norma IEEE 802.11n, que utiliza várias antenas para transmissão e recepção, tecnologias denominada por MIMO (*Multiple-Input Multiple-Output*), atingindo taxas de transmissão perto dos 300Mbps. Apesar desta norma ainda não estar ratificada, a sua utilização vai começar a ser uma realidade nos tempos mais próximos. Espera-se a sua ratificação no primeiro quadrimestre de 2009 [DeBeasi,2007a].

A Tabela 1 estabelece uma comparação entre as diversas normas, relativamente a aspectos como a frequência, o alcance e a taxa de transmissão:

-	1997	2.4	2	~20	~100
a	1999	5	54	~35	~120
b	1999	2.4	11	~38	~140
g	2003	2.4	54	~38	~140
n	2009	2.4,5	248	~70	~250

Tabela 1: Características das normas IEEE 802.11

Após este resumo histórico, apresenta-se nos parágrafos seguintes uma descrição sumária de cada norma IEEE 802.

2.1.1.1 Norma IEEE 802.11a

A norma IEEE 802.11a encontra-se ratificada e utiliza a banda de frequência não licenciada 5GHz. Esta frequência é menos lotada que a frequência 2.4GHz da norma 802.11b e 802.11g. A norma IEEE 802.11a apresenta boas taxas de transferência (*throughput*), que teoricamente vão até 54Mbps, mas na realidade não ultrapassam os 20Mbps. Uma vez que existem mais canais disponíveis na frequência 5GHz, a norma IEEE 802.11a apresenta menos interferências de sobreposição (*overlapping*) na atribuição de canais. Contudo, os sinais em 5GHz não atravessam tão bem alguns materiais como os sinais em 2.4 GHz, tendo por isso menos capacidade de cobertura. Infelizmente a norma 802.11a não é compatível com as 802.11b/g, significando que um utilizador que esteja a utilizar 802.11b/g não consegue ligar-se a um AP IEEE 802.11a.

2.1.1.2 Norma IEEE 802.11b

A norma IEEE 802.11b está ratificada e existem inúmeros equipamentos disponíveis no mercado. Foi a primeira actualização a nível de protocolos para produtos wireless no espectro 2.4GHz, com o aumento da velocidade máxima de 2Mbps para 11Mbps. As RF desta norma fornecem tipicamente cobertura para ambientes *indoor* num raio entre os 27,4m e os 53,34m. Hoje em dia, praticamente todos os dispositivos suportam a norma IEEE 802.11b. A maioria das organizações utilizam apenas três dos 14 canais (o canal 1, 6 e o 11), porque devem estar espaçados de pelo menos 5 de forma a minimizar a sobreposição de canais (reduzindo a interferência da RF). Apenas com três canais disponíveis, é particularmente importante otimizar a atribuição dos canais, para evitar interferências quando múltiplos APs estiverem instalados com alguma proximidade entre si. Por consequência, os vários equipamentos não wireless mas que utilizam a frequência dos 2.4GHz, podem criar interferências adicionais.

2.1.1.3 Norma IEEE 802.11g

Esta norma também se encontra ratificada sendo bastante utilizada no mercado empresarial e doméstico. Foi o protocolo que permitiu a utilização da frequência 2.4GHz, tal como a norma IEEE 802.11b e atingir velocidades (até 54Mbps), tal como a norma IEEE 802.11a. Ao

contrário dos dispositivos IEEE 802.11a, os dispositivos com a norma IEEE 802.11g são compatíveis com os IEEE 802.11b. Esta possibilidade é extremamente importante, pois ainda existem vários equipamentos IEEE 802.11b, logo permitindo uma solução híbrida, onde a migração dos equipamentos se torna mais suave pelo que o impacto financeiro é menos sentido.

2.1.1.4 Norma IEEE 802.11e (Qualidade de Serviço)

A norma IEEE 802.11e é uma norma recentemente ratificada que permite aos administradores de rede diferenciar e atribuir prioridade a classes de tráfego. Permite à infraestrutura de rede wireless a entrega com uma performance aceitável a uma série de aplicações, suportando também um maior número simultâneo de utilizadores. Com a utilização desta norma é possível para dar prioridade ao tráfego de voz e vídeo, desde que obviamente, essas aplicações sejam consideradas prioritárias. A norma IEEE 802.11e torna-se de elevada importância para as organizações que pretendem utilizar VoWLAN (voz sobre Wireless). Dado à sua natureza esta norma é muitas vezes referida como WMM (Wireless Multimédia).

2.1.1.5 Norma IEEE 802.11i (Segurança)

Existem várias normas de segurança que hoje são utilizados nas redes wireless. A mais comum é o WEP (*Wired Equivalent Privacy*), que é a norma de segurança original para autenticação e encriptação do tráfego gerado entre os clientes e os APs. O WEP fornece uma chave que é partilhada por todos os utilizadores. É uma norma de segurança manifestamente fraca e já foi demonstrado diversas vezes que é facilmente quebrável. O WPA (*Wi-Fi Protected Access*) veio rectificar as vulnerabilidades do WEP, também designado por muitos como o WEP2. A vantagem do WPA relativamente ao WEP é que os dados são encriptados utilizando um protocolo de chave temporária (TKIP), possibilitando a criação de chaves por pacotes. Assim, as chaves de segurança são construídas no decorrer da sessão, sendo trocadas de forma periódica e automática. O processo de autenticação dos utilizadores está também melhorado, uma vez que é utilizado o protocolo 802.11x e o EAP (*Extensible Authentication Protocol*), que através de um servidor de autenticação central faz a autenticação de cada utilizador.

Posteriormente ao WPA surgiu o WPA2 que é uma norma de aprimoramento de segurança que substitui os algoritmos de encriptação anteriores pelo AES (*Advanced Encryption Standard*).

2.1.1.6 Norma IEEE 802.11k

A norma IEEE 802.11k² está em fase final de ratificação, não existindo ainda produtos disponíveis no mercado com esta norma. Esta norma vai facilitar a gestão e a manutenção das redes wireless. As normas IEEE 802.11 permitem a interoperabilidade entre APs e controladores wireless de vários fabricantes, no entanto não permitem aceder aos recursos de rádio frequência dos clientes. Consequentemente limita a capacidade dos administradores para gerir eficientemente a sua rede [Dan,2004]. Como proposta para avaliar os recursos rádio, a norma IEEE 802.11k visa fornecer informação dos clientes. A proposta para a criação desta nova norma define pedidos de medição e reporta em detalhe estatísticas e dados dos clientes quer ao nível da camada 1 quer a nível da camada 2. Na maior parte dos casos, os APs ou controladores wireless pedem aos clientes para reportar dados, mas noutros casos, os clientes podem pedir dados aos APs. Esta informação permite ao cliente escolher a melhor qualidade para a sua ligação, inclusivamente a possibilidade de mudar o AP a que está associado. As medições podem ser ao nível de decisões de *roaming*, carga do canal RF, nós escondidos, estatísticas dos clientes, TCP (*Transmit Power Protocol*), ruído, detecção do meio, histograma cronológico, etc.

A norma IEEE 802.11k fornece um mecanismo para monitorizar os dispositivos de clientes wireless, não para configurar esses clientes. A norma IEEE 802.11v construída baseada na IEEE 802.11k torna isso possível.

2.1.1.7 Norma IEEE 802.11n

Norma não ratificada requerendo actualização de *firmware* dos equipamentos e nova actualização dos clientes, já existindo produtos no mercado. Esta norma está em fase final de homologação, estimada para Novembro 2008. Permite maiores taxas de transferência (entre 100Mbps a 600 Mbps). A norma IEEE 802.11n³ irá permitir o “salto” para as aplicações multimédia, pois será baseada na tecnologia MIMO, que permite o aumento da velocidade de

² http://grouper.ieee.org/groups/802/11/Reports/tgk_update.htm

³ http://www.ieee802.org/11/Reports/tgn_update.htm

transmissão de dados, a melhoria da fiabilidade e ampliação do espectro de acção das redes wireless, através de múltiplas antenas inteligentes que transmitem e recebem múltiplos fluxos de dados de forma simultânea [Demirkol et al,2004]. Portanto, para além do incremento da velocidade, permitirá maior eficiência na propagação do sinal e terá compatibilidade total com as normas anteriores (802.11a, 802.11b e 802.11g).

2.1.1.8 Norma IEEE 802.11p

Norma não ratificada esperando-se a ratificação para Abril de 2009. A norma IEEE 802.11p⁴ foi desenhada para permitir operações wireless utilizando estações (APs) que fornecem comunicação a dispositivos com mobilidade, como por exemplo veículos automóveis. Esta norma, também designada por WAVE (*Wireless Access in Vehicular Environments*), opera comunicações em ambientes em que as propriedades da camada física se alteram rapidamente e as trocas de comunicações de curta duração são requeridas com frequência.

2.1.1.9 Norma IEEE 802.11r

Esta norma não se encontra ratificada. A norma IEEE 802.11r⁵ está a ser definida para minimizar o tempo de transição de *roaming* entre APs, garantindo a conectividade ao utilizador sem descontinuidade. Os dispositivos clientes estão “pré-autenticados” no AP vizinho, que irá garantir o *roaming* minimizando o tempo de transição.

Esta funcionalidade é especialmente importante para VoWLAN e outras aplicações onde a latência é crítica para a performance. A norma IEEE 802.11r está desenhada para permitir aos clientes manter o estado de ligação relativo à segurança e QoS no novo AP.

2.1.1.10 Norma IEEE 802.11s – Mesh Networking

Esta norma ainda não se encontra ratificada. O elemento básico da norma é o MP (*Mesh Point*). Ao invés de outros protocolos IEEE 802.11, os MP têm capacidade de trocar pacotes entre vários nós da rede wireless. Estes MPs podem comunicar não só com outros MPs internos, mas também com outros externos. Semelhantes a um AP ou *portal* (como é designado nesta arquitectura), o MP tem capacidades de afinação. Por outro lado, o MP pode operar como sendo uma estação/nó que pode actuar como uma aplicação terminal. Pode ainda

⁴ http://www.ieee802.org/11/Reports/tgp_update.htm

⁵ http://www.ieee802.org/11/Reports/tgr_update.htm

reencaminhar pacotes para comunicação que não o envolva. O mecanismo de funcionamento desta norma pode ser observado na Figura 1. Contudo, o MP por si só, não fornece serviços de AP. Enquanto que o AP/portal faz a ponte de IEEE 802.11 para redes não IEEE 802.11, o MP apenas reencaminha pacotes entre as redes IEEE 802.11 [Guido et al,2007]. Tem o potencial de reduzir custos de instalação e acelerar a adopção das redes municipais também designadas por “MuniWireless”. O MP actua como repetidor do sinal RF, formando uma malha de rede.

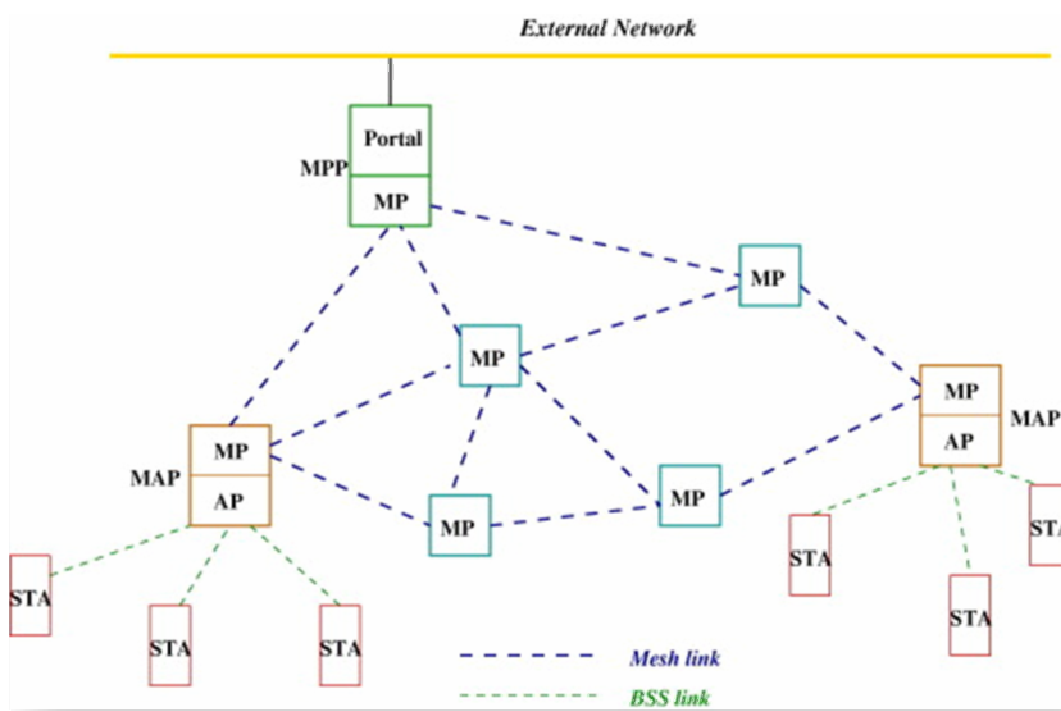


Figura 1: Mecanismo de funcionamento da norma IEEE 802.11s

2.1.1.11 Norma IEEE 802.11u “Wireless Interworking with External Networks”

Actualmente esta norma não se encontra ratificada. A proposta para a especificação IEEE 802.11u⁶ tem como objectivo a inter-conectividade com redes não IEEE 802.11, como por exemplo o GSM (*Global System for Mobile Communications*), GPRS (*General Packet Radio Service*), UMTS (*Universal Mobile Telecommunications System*), HSPDA (*High-Speed Downlink Packet Access*) etc. A ratificação desta norma é muito esperada porque permitirá

⁶ http://www.ieee802.org/11/Reports/tgu_update.htm

acelerar a adopção e implementação de aplicações VoWLAN, uma vez que permitirá, por exemplo, ter mais do que uma tecnologia disponível num equipamento como um telemóvel.

2.1.1.12 Norma IEEE 802.11v

Norma ratificada recentemente que irá permitir gestão centralizada (monitorização e configuração) dos APs, através de um mecanismo ao nível da camada 2 (modelo OSI). Como esta norma é muito recente, ainda não existem muitos equipamentos a implementá-la.

A norma IEEE 802.11k tem como objectivo obter informação dos dispositivos clientes, mas não fornece a possibilidade de os configurar. Esta norma vai criar um AP MIB (*Management Information Base*) para ser usada para configurar os clientes remotamente nos seguintes aspectos: gestão de RF; escolha dinâmica de canais; coordenação entre APs; coexistência de frequências; balanceamento de carga; gestão baseada na localização; actualização de *firmware* nos clientes; diagnósticos aos clientes; interface MIB para permitir gestão centralizada; detecção de Aps/SSIDs não autorizados;

2.1.1.13 Norma IEEE 802.11w

Esta norma não se encontra ratificada. A norma IEEE 802.11w tem como objectivo fornecer mecanismos para proteger a gestão de pacotes IEEE 802.11 (incluindo acções de gestão de pacotes, “desautenticação” e dissociação de pacotes). É essencial por razões de segurança (especialmente na dissociação e “desautenticação” de pacotes) podendo ajudar a prevenir alguns ataques de negação de serviços, mais conhecidos por *denial of service* (ataques que não têm por objectivo a invasão, mas a colocação do serviço indisponível). Em suma, esta norma foi criada para aumentar a segurança das redes wireless, através da protecção dos pacotes de gestão.

2.1.2 REDES WLAN

As redes WLAN são bastante comuns actualmente. São também muito conhecidas pelo termo Wi-Fi⁷, que é por muitos considerado o acrónimo de “Wireless Fidelity”, mas na realidade o Wi-Fi é um consórcio de diversas empresas independentes, que promovem a

⁷ Wi-Fi Alliance, www.wi-fi.org/

interoperabilidade entre vários produtos baseados na família da norma IEEE 802.11. Este consórcio atribui uma certificação que garante que o produto passou os seus testes de interoperabilidade.

Estas redes são capazes de oferecer diversas funcionalidades que facilitam o dia-a-dia dos seus utilizadores. São flexíveis e podem ser configuradas numa variedade de topologias dependendo do cenário de aplicação. São usadas basicamente por utilizadores que precisam de ter acesso a serviços de rede em qualquer altura e em qualquer lugar como por exemplo: acesso a Internet, e-mail, chats, em áreas públicas, como centros comerciais, aeroportos, hotéis, centros de conferências, entre outros.

Além disso, as redes WLAN são uma boa solução para locais, onde redes LAN (*Local Area Network*) são mais difíceis de implementar, como por exemplo prédios históricos. Na Figura 2, pode ser observado um exemplo típico das redes WLAN, onde a comunicação entre os diversos postos de trabalho é assegurada por um equipamento de rede wireless, designado por AP, já referido em pontos anteriores.

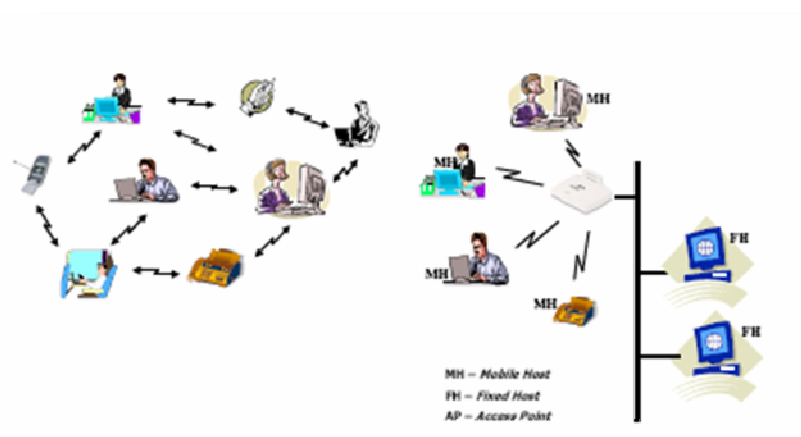


Figura 2 : Exemplo de Redes WLAN

De acordo com o sítio da Internet das normas IEEE 802.11⁸, podemos designar por WLAN todas as redes IEEE 802.11.

2.1.3 REDES WMAN

⁸ <http://ieee802.org/11/>

O termo WMAN (*Wireless Metropolitan Area Networks*) está associado à norma IEEE 802.16⁹, que é definida pelo IEEE da seguinte forma: “*IEEE 802.16 WirelessMAN® Standard for Wireless Metropolitan Area Networks*”.

Esta norma está na base da tecnologia WiMax¹⁰ (*Worldwide Interoperability for Microwave Access*), muito semelhante ao WLAN, mas com melhores desempenhos na comunicação. O funcionamento do WiMax opera de forma similar aos sistemas móveis GSM, onde existem estações base (*BS – Base Stations*) que transmitem os sinais captados por estruturas como TV's via satélite, localizados próximos do cliente. A partir daí, o encaminhamento para o cliente ocorre através de uma ligação Ethernet LAN.

As principais características do WiMax são:

- Frequências de operação entre 2 GHz e 11GHz (802.16a);
- Alcances superiores a 50 Km;
- Taxas de transmissão a partir de 70 Mbps;
- Eficiência de espectro acima dos 5 bits/segundo/Hz;
- Qualidade de serviço incorporado;
- Suporte para voz e vídeo;

Outra característica desta norma, é a possibilidade de acesso à rede *non-line-of-sight*, ou seja, sem linha de vista directa, o que significa que mesmo que haja obstáculos entre a antena do emissor e do receptor, a transmissão ocorre normalmente [Ono,2004].

É importante referir que quando se menciona a norma IEEE 802.16, o tipo de tecnologia em causa é WMAN [Cherry,2004], que é diferente dos padrões IEEE 802.11, destinados à WLAN.

2.1.4 REDES WRAN

O termo WRAN (*Wireless Regional Area Networks*) está associado à norma IEEE 802.22¹¹, e que está a cargo de mais um grupo de trabalho do IEEE criado em 2004. Este grupo de trabalho propõe-se a estudar e a definir como utilizar canais livres de TV em VHF (*Very High*

⁹ <http://grouper.ieee.org/groups/802/16>

¹⁰ <http://www.wimaxforum.org>

¹¹ <http://www.ieee802.org/22>

Frequency) e UHF (*Ultra High Frequency*) (entre 54 MHz e 862 MHz) para acesso à Internet em áreas rurais, normalmente com baixa densidade populacional.

Actualmente esta norma ainda não está ratificada, mas já se conhecem algumas características. Deverá ter a possibilidade de atingir distâncias de 33 Km, para cobertura de uma densidade populacional de 1,25 pessoas por Km². É uma tecnologia que privilegiará o acesso fixo, ou seja, os utilizadores domésticos, numa lógica de “ponto-para-multiponto”, ou seja de uma estação base para diversos clientes. A estação base determinará as características da rede, em função do número de clientes ligados a cada instante. As antenas dos clientes deverão estar instaladas a 10m do solo. A largura de banda mínima nas especificações é de 4,8Mbps e a máxima de 72,6 Mbps, apesar de terem sido observados 23Mbps em 6MHz.

Esta tecnologia ainda apresenta alguns problemas, que estão a tentar ser superados através da utilização de mecanismos de rádio cognitivo. Os dispositivos baseados na tecnologia de rádio cognitivo usam processadores comuns que correm aplicações, podendo alterar as frequências de rádio, os parâmetros de recepção de sinal, a energia de transmissão e outras características dependendo do objectivo da sua utilização. O objectivo é evitar interferências na comunicação com utilizadores legítimos ou ilegítimos. A alteração é baseada na monitorização activa de diversos factores no ambiente interno e externo de rádio, como o espectro de rádio frequência, o comportamento do utilizador e o estado da rede. De um modo geral, a flexibilidade dos sistemas de rádio cognitivo é tida como uma possível solução face à saturação de alguns espectros de rádio, porque conseguem funcionar com o espectro disponível, ou seja, detecta os 'buracos' no espectro e a explorá-lo imediatamente. Esta estratégia impõe que se equipe a rede de comunicação com scanners. Isto implica, também, uma grande reactividade dos sistemas de comunicação, já que os proprietários de espectro devem poder, imediatamente, recuperar as suas frequências.

2.1.5 REDES WBL

O termo WBL (Wireless Banda Larga) é utilizado nesta dissertação, para descrever o conjunto de tecnologias wireless que podem contribuir para o objectivo principal do trabalho que é o de fornecer cobertura sem fios, a zonas rurais que não tenham acesso à Banda Larga. É portanto o termo encontrado, para melhor caracterizar o conjunto de tecnologias possíveis para fornecer acesso wireless às zonas rurais.

Em conclusão, pode-se observar na Figura 3 o universo das tecnologias wireless: WPAN (*Wireless Personal Area Network*) onde se incluem tecnologias como o Bluetooth; depois as normas 802.11 na figura designadas por WLAN descritas no sub-capítulo 2.1.2; o WMAN (normas 802.16) também descrito no ponto 2.1.3; o WWAN (*Wireless Wide Area Network*) onde se incluem tecnologias como o GSM, UMTS e CDMA (*Code Division Multiple Access*); e por último a WRAN, que é uma tecnologia ainda em investigação, que terá como objectivo fornecer internet a zonas rurais, utilizando o mesmo mecanismo que a distribuição de sinal de TV, conforme referido no ponto 2.1.4 – Redes WRAN.

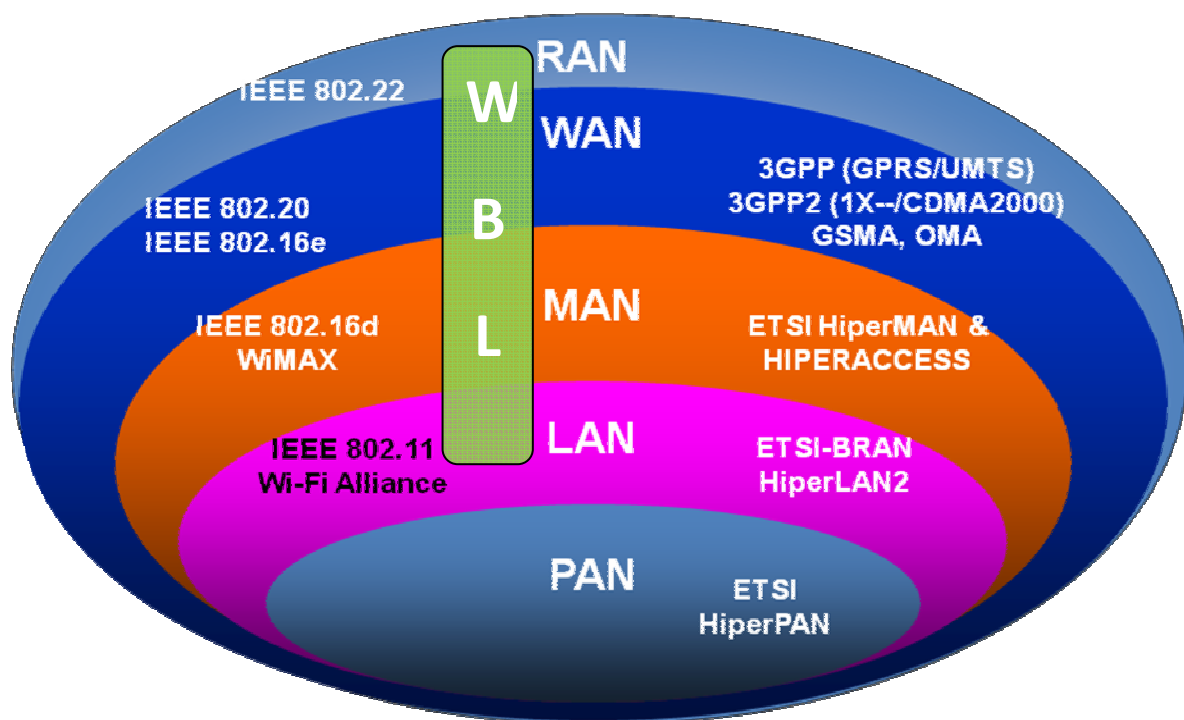


Figura 3: Tecnologias Wireless

Assim, a WBL representa o conjunto das tecnologias WLAN, WMAN, WIMAX e WRAN.

2.2 ARQUITECTURAS DE REDES WLAN

Este ponto descreve o estado da arte da gestão de redes WLAN, onde se expõe as diferentes arquitecturas e a forma como evoluíram. São também abordados alguns pontos fortes e pontos fracos de cada arquitectura.

A primeira arquitectura a surgir nas redes WLAN foi a *Point-to-Point*. Nesta arquitectura existe apenas transmissão de dados de um ponto para o outro. Existem várias organizações que utilizam esta arquitectura com sucesso para interligar edifícios, como se exemplifica na Figura 4. Num cenário em que existam poucas implementações desta arquitectura, a gestão é simples se o número de dispositivos for pequeno [Mathias,2006a]. As vantagens da arquitectura *point-to-point* residem na facilidade de instalação.



Após a arquitetura *Point-to-Point*, a evolução seguiu para arquitetura *Peer-to-Peer/Ad-Hoc*, que pressupõe a existência de vários nós na rede para comunicar entre si. Uma característica é a inexistência de APs, sendo os próprios clientes os responsáveis por suportar a comunicação [Mathias,2006a], fazendo com que a conectividade seja conseguida sem a existência de um concentrador central. Esta descrição pode ser observada na Figura 5, onde três clientes comunicam entre si, sem a existência de nenhum concentrador.

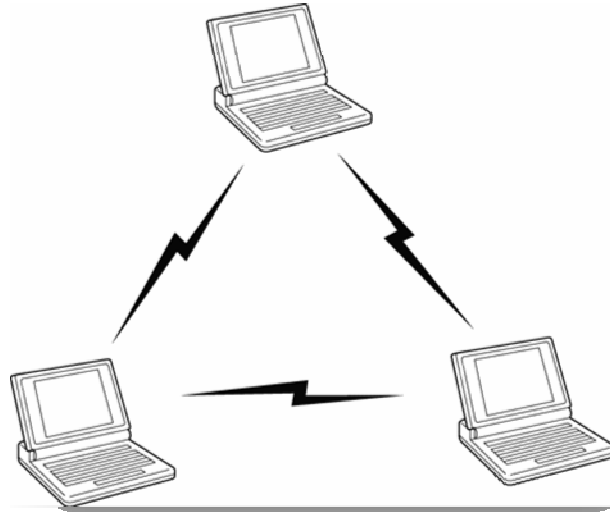


Figura 5: Arquitectura *Peer-to-Peer/Ad-hoc*

Nesta arquitectura não existe a possibilidade de efectuar operações de gestão, a menos que os clientes tenham essas capacidades, logo esta arquitectura não favorece a função gestão de redes WLAN.

2.2.3 POINT-TO-MULTIPOINT, APS AUTÓNOMOS

As arquitecturas *Peer-to-Peer* e *Point-to-Point* experimentaram a sua evolução na arquitectura *Point-to-Multipoint*, possibilitando a extensão da rede wireless com mais flexibilidade. Nesta topologia existe um ponto de convergência, resultando num controlo centralizado. Tem um ponto de interligação com a rede LAN, possibilitando uma extensão da rede. A desvantagem assenta no facto da existência de um ponto único de falha, possibilitando aparecimento de estrangulamento da rede também designado por *bottleneck*.

Os APs implementam completamente e terminam todas as funções das normas IEEE 802.11, logo todos os pacotes da rede LAN comunicam sob a norma IEEE 802.3. Cada AP pode ser gerido independentemente como uma entidade na rede.

Anteriormente ao ano 2001, a maior parte das redes WLAN eram implementadas com recurso a APs autónomos. Estes APs forneciam gestão e controlo, tudo numa mesma aplicação [Mathias,2006a]. Na Figura 6 pode-se observar este facto, ou seja, a existência de APs autónomos geridos por uma consola de gestão.

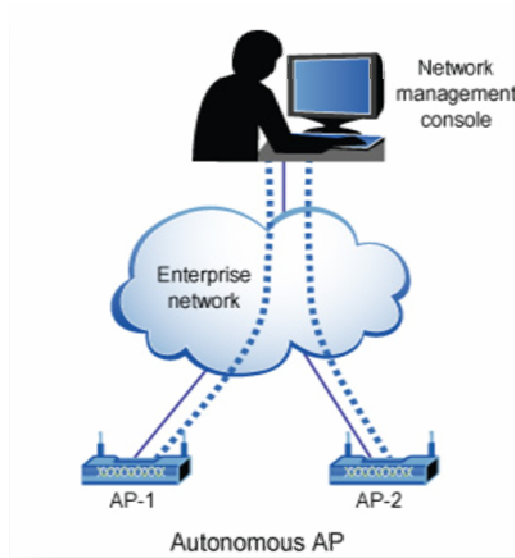


Figura 6: Arquitectura Point-to-Multipoint

Os APs autónomos são simples de instalar e de gerir, podem inclusivé ser configurados através de uma consola de gestão, acedida via protocolo HTTPS (*Hypertext Transfer Protocol Secure*) ou então SNMP (*Simple Network Management Protocol*). Os administradores de rede configuram os APs autónomos tal como um *switch* ou um *router*. Em organizações com poucos APs, esta abordagem faz todo o sentido. Ainda hoje, muitos administradores de sistema utilizam esta forma para gerir a sua rede WLAN.

Esta arquitectura também é designada pela Xirrus¹² por arquitectura de 1ª geração (anterior a 2002) [Xirrus,2005].

2.2.4 WLAN GATEWAYS

Como a distribuição dos APs começaram a proliferar pelas organizações, os administradores de rede começaram a ter preocupações de flexibilidade e de segurança. Uma das formas encontradas para resolver e controlar os problemas de segurança foi a criação de uma *gateway* comum à rede wireless. As *gateways* WLAN das empresas Bluesocket e Vernier foram as primeiras a surgir no ano 2001, permitindo um perímetro de segurança entre a rede LAN da empresa e a rede “insegura” WLAN [DeBeasi,2007b]. Na Figura 7 pode observar-se o modo de funcionamento desta arquitectura, onde se verifica a existência de um

¹² www.xirrus.com

equipamento que converge todo o tráfego da rede wireless, ou seja a *gateway*, assim como da consola para a gestão da rede WLAN.

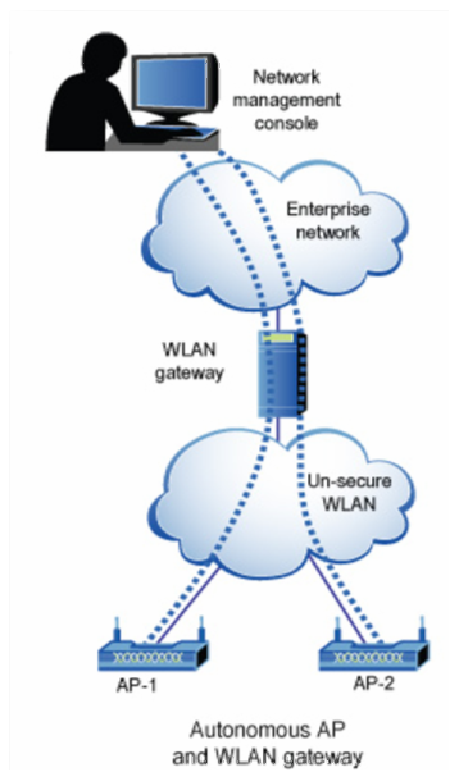


Figura 7: Arquitectura WLAN Gateway

As WLAN *gateways* proporcionam uma forma de administração centralizada da rede, pelo menos obrigando a que todo o tráfego passe num ponto único, que poderá ter controlo de acesso e aplicar políticas de segurança.

Aparentemente este seria o caminho certo, no entanto esta arquitectura não foi suficientemente eficaz, porque o administrador de rede ainda tinha de configurar e controlar os APs de forma autónoma, ou seja, individualmente. Os problemas de sobreposição de atribuição dos canais começaram a surgir. Logo se percebeu que esta abordagem não tinha qualquer escalabilidade, à medida que os APs eram instalados na rede [DeBeasi,2007b].

2.2.5 CONTROLADORES WLAN

Após a arquitectura WLAN *Gateways*, surgem as redes wireless cuja arquitectura utiliza equipamentos de rede, designados por controladores, também conhecidos por WLAN *Switch*.

Esta arquitectura é designada de 2ª geração (2002-2004) [Xirrus,2005]. A utilização tradicional de APs nas empresas começou a não fazer sentido e a gerar grandes esforços na sua gestão. Quando se tem uma rede distribuída com APs inteligentes e se decide alterar para uma arquitectura *thin-AP* ou *lightweight*, os aspectos relacionados com a gestão e segurança, têm propensão a melhorar [Wexler,2006]. De notar que os *thin-APs* são antenas inteligentes cuja função principal é receber e transmitir sinal rádio. Os dados antes de entrarem na rede LAN, passam por um controlador, como pode ser observado na Figura 8.

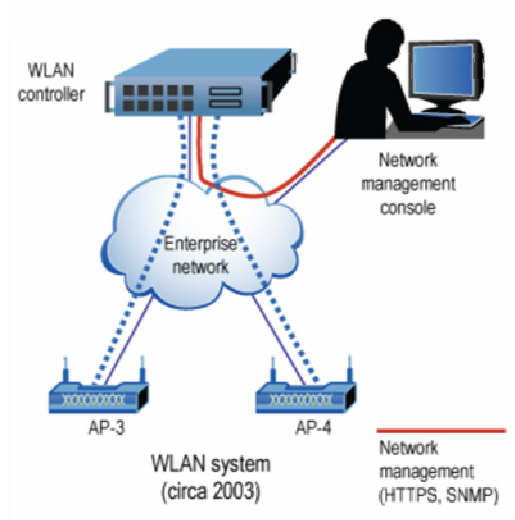


Figura 8: *Thin aps* numa arquitectura de gestão de WLAN centralizada

Como o próprio nome indica, os *thin-APs* foram criados para reduzir a complexidade dos APs. Uma das motivações para o seu aparecimento, foi a localização dos APs, pois a sua localização fixa-se em locais muito complicados em termos de ambiente, ou seja, com vários factores de interferência de RF.

Esta arquitectura contempla a utilização de um controlador WLAN que é responsável pela configuração, controlo e gestão de vários *thin-APs*. As funções das normas IEEE 802.11 são divididas entre os *thin-APs* e o controlador WLAN.

Segundo [Sridhar,2006], uma das vantagens desta arquitectura para os administradores é o facto de se instalar apenas uma vez o AP, não tendo uma manutenção complexa. Em 2002 a

Symbol Technologies¹³, actualmente uma subsidiária da Motorola¹⁴, introduziu no mercado um *switch* (*Mobius Axon Wireless Switch*) e criou o termo *wireless LAN switch* para definir um controlador centralizado capaz de administrar múltiplos APs *lightweight*. Os APs possuem funcionalidades muito reduzidas, uma vez que muitas funções foram transferidas para o controlador centralizado.

Nesta arquitectura o gestor de rede configura o controlador, e este configura individualmente os APs. O primeiro benefício verificado foi a flexibilidade, porque em vez de se configurar individualmente centenas de APs, o administrador de rede só tinha de administrar um ou mais controladores. Esta abordagem ajudou a resolver o problema da escalabilidade e as redes WLAN proliferaram.

No entanto, este processo não era linear entre os vários fabricantes, resultando numa dificuldade, que se baseava no facto de cada fabricante ter o seu próprio método de controlar os APs *lightweight* e de aplicar alterações no ambiente RF. Num esforço para estabelecer uma norma para controladores AP, a Airspace (entretanto adquirida pela Cisco¹⁵) e a NTT DoCoMo¹⁶, peticionaram a constituição de um grupo de trabalho ao IETF (*Internet Engineering Task Force*), que seria responsável por desenvolver um protocolo para uniformizar os APs *lightweight*. No entanto, este grupo de trabalho, “largou” o LWAPP (*Lightweight Access Point Protocol*) e encarregou outro grupo de desenvolver o CAPWAP¹⁷ (*Control and Provisioning of Wireless Access Points*) [DeBeasi,2007b]. O objectivo do CAPWAP é facilitar o controlo da gestão de das redes WLAN, especificando os serviços, as funções e os recursos dos APs, em consonância para permitir a interoperabilidade com os controladores. O CAPWAP¹⁸ está a ser definido por um grupo de trabalho do IETF, integrado por várias empresas, tendo como objectivo a definição de uma arquitectura de interoperabilidade de várias tecnologias wireless, onde exista uma arquitectura baseada em controladores WLAN, que este grupo denomina por ACs (*Access Controllers*). Este protocolo procura facilitar o controlo, a gestão e o aprovisionamento de WTPs (*WLAN Termination Points*), especificando serviços, funções e fontes relacionadas com as normas IEEE 802.11, no sentido de permitir a interoperabilidade entre os ACs e os WTPs.

¹³ <http://business.motorola.com/us/enterprise/index.html>

¹⁴ <http://www.motorola.com>

¹⁵ <http://www.cisco.com>

¹⁶ <http://www.nttdocomo.com>

¹⁷ <http://www.ietf.org/html.charters/capwap-charter.html>

¹⁸ <http://www.ietf.org/html.charters/capwap-charter.html>

Esta arquitectura prevê um controlo de acesso muito forte e permite efectuar *roaming* seguro, além de reduzir a carga de configuração e gestão das operações em curso. No entanto, também apresenta algumas desvantagens, por exemplo, o WLAN *Switch* central é um ponto único de falha de todos os APs que lhes estão associadas. Além disso, uma vez que todo o tráfego dos APs transita no *switch* central, pode levar a um estrangulamento da rede. Outra limitação pode ser a pouca flexibilidade para interagir com outras tecnologias e serviços.

2.2.6 ARQUITECTURA DISTRIBUÍDA

A evolução das arquitecturas de redes wireless progrediu para a arquitectura distribuída, onde os APs formam uma rede distribuída com outros APs através de ligações de rede LAN ou wireless. Esta arquitectura cria uma malha de APs e o termo mais comum para designar este tipo de arquitectura é rede *mesh* ou wireless *mesh*. Os APs numa rede *mesh* podem ser interligados quer através de ligações IEEE 802.11, quer através de ligações IEEE 802.3. Esta arquitectura é muito utilizada para redes Municipais e outras implementações em ambientes *outdoor*.

Existe um componente central que controla os controladores (*switchs*) “tradicionais” de WLAN, sendo as funcionalidades distribuídas pelos restantes controladores. Cada AP da rede comunica com outro AP utilizando *wireless backbone trunks*, em vez da rede *ethernet*. Este tipo de topologia é descentralizado, onde cada AP é ligado a muitos outros numa malha (*mesh*) e onde cada AP encaminha os pacotes de outros APs para o seu destino. Este tipo de topologia mitiga falhas porque um AP pode encaminhar tráfego de todos os APs que lhe estão próximos. Apenas as comunicações de *backbone*, podem ter necessidade de utilizar rede LAN.

Um exemplo desta arquitectura é o conceito que a Colubris¹⁹ está a desenvolver, designando-a como arquitectura “TriPlane” ou como a arquitectura da terceira geração, que consiste na distribuição de inteligência em determinados locais da rede [Metzler,2005].

Na verdade esta arquitectura resolve os problemas enunciados na arquitectura mencionada no subcapítulo anterior. Na Tabela 2 podem ser observadas as diferenças:

¹⁹ <http://www.colubris.com>

Problemas da arquitectura centralizada	Arquitectura Distribuída
O controlador pode ser um <i>bottleneck</i>	Não existe controlador
Ponto único de controlo gestão e dados	Controlo separado, gestão e dados
Processamento de dados é centralizado	O processamento de dados é distribuído
Interfaces proprietários	Interfaces abertos

Tabela 2: Arquitectura Centralizada vs Distribuída

Como o próprio nome indica, a arquitectura “TriPlane” atribui à gestão, o controlo e transmissão de dados em “planos” separados, cada um com recursos de processamento dedicados. Combina a eficiência operacional da gestão e controlo centralizados, com a escalabilidade, versatilidade e QoS aprimorado que advém do facto de existir inteligência distribuída [Colubris,2005]. Na Figura 9 pode ser observado um esquema de funcionamento desta arquitectura, onde a inteligência da gestão da rede, está repartida pelos controladores WLAN e pelos APs *Multiservice* distribuídos por diversos locais da rede.

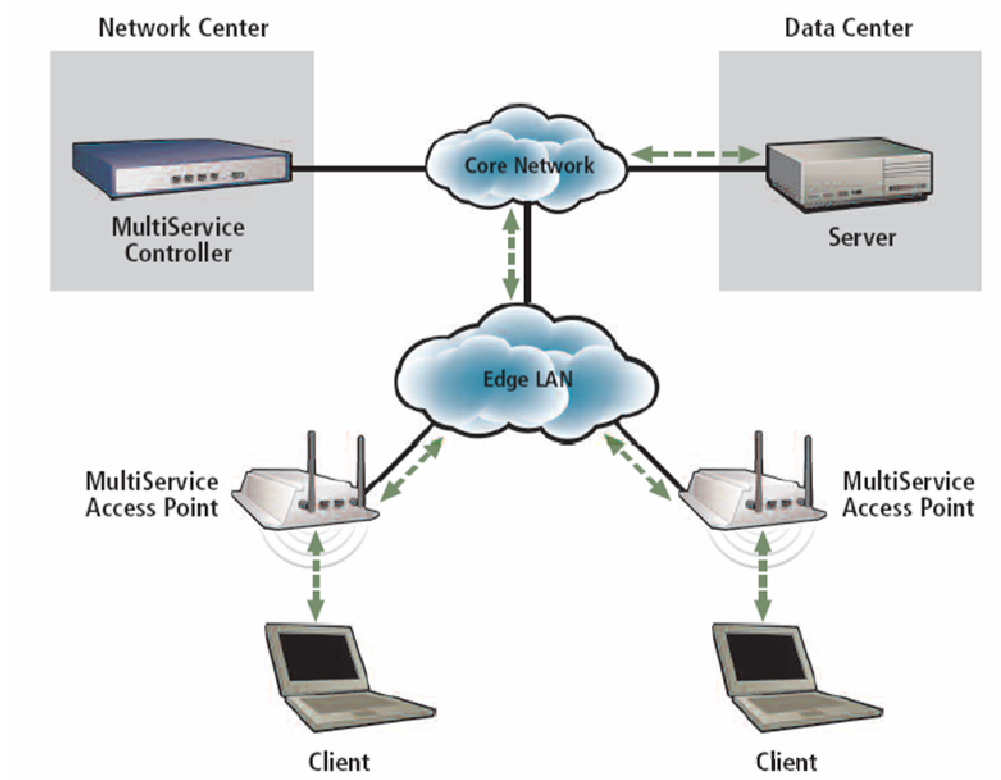


Figura 9 : Arquitectura distribuída

2.2.7 WLAN ARRAYS

Alguns fabricantes estão a desenvolver produtos baseados na arquitectura WLAN Array, como a Xirrus ou a Meru²⁰. É também designada por arquitectura de 4ª geração (2005-?) [Xirrus,2005]. Esta abordagem contempla uma combinação de vários *switchs* com múltiplos APs. A ideia é concentrar um grande potencial de *throughput* num único dispositivo (no caso da Xirrus) [Mhathias,2006a], descrito como “*super access point*” integrando mais de 16 APs IEEE 802.11a/b/g.

Esta abordagem maximiza a capacidade de cobertura, assim como acelera o retorno do investimento. Está desenhado para superar as limitações inerentes às arquitecturas anteriores, e para suportar as necessidades dos utilizadores, assim como aplicações mais avançadas [Xirrus,2005]. A arquitectura WLAN Array reduz a necessidade de equipamentos, simplificando a arquitectura de rede introduzindo poderosas e novas métricas de custo/performance em áreas como:

- Capacidade: Largura de banda;
- Cobertura: 4 vezes maior por dispositivo;
- Custo: menos dispositivos;

Contém quatro tipos de rádio distintos ou pelo menos a possibilidade de operar com quatro ou mais rádios distintos em simultâneo. A Figura 10 demonstra as diferenças entre os APs tradicionais, os WLAN *Switchs* e o WLAN Array, que apenas com dois APs consegue a mesma cobertura que as outras arquitecturas. Tem a capacidade de efectuar balanceamento de carga, ou por outro lado, priorizar o tráfego através de todos os canais de rádio simultaneamente [Fairpoint,2005].

²⁰ <http://www.merunetworks.com/>

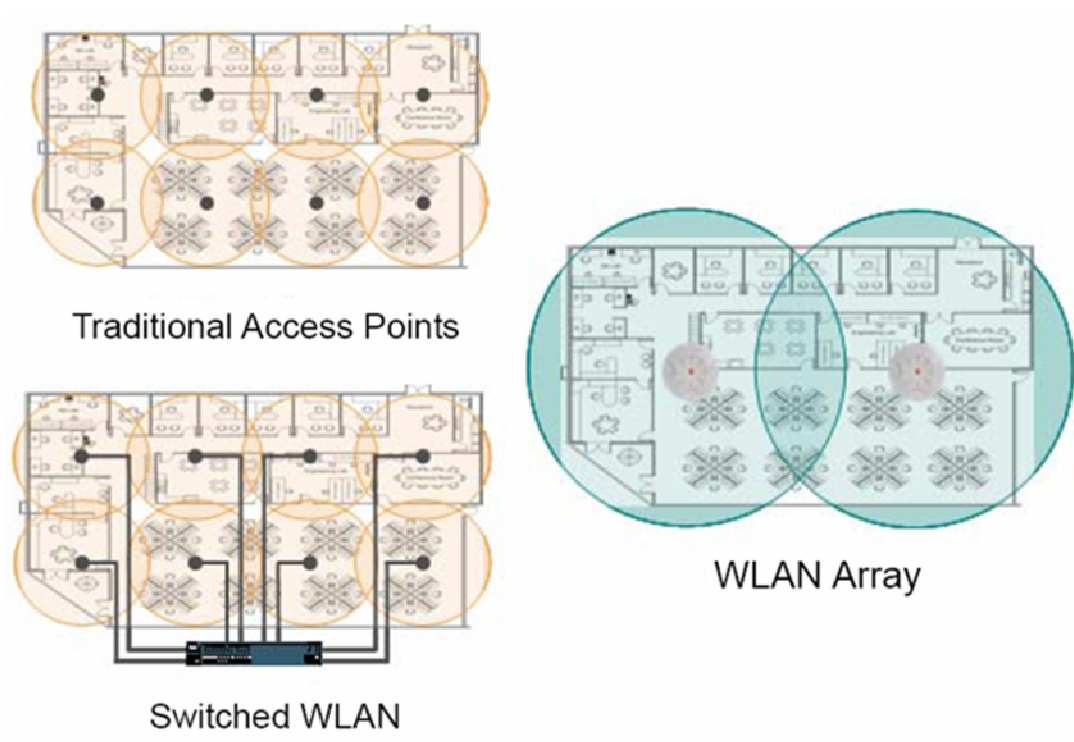


Figura 10: Arquitectura WLAN array vs tradicional e controladores

2.2.8 ARQUITECTURAS UNIFICADAS

As arquitecturas unificadas são actualmente a tendência que será seguida pela maioria dos fabricantes. Consiste na eliminação do perímetro entre a rede LAN e a WLAN. Será o fim do modelo de sobreposição, onde a convergência com outras tecnologias será uma realidade. Com as novas implementações do WIMAX, será importante a coexistência das diversas tecnologias. Na rede da organização irá ser possível por exemplo, existirem equipamentos WLAN, WIMAX, GSM, GPRS, UMTS, HSPDA, assim como outros, onde todos possam interagir. Um exemplo desta tendência passa pela utilização dos telemóveis como mais uma extensão da central telefónica.

Esta arquitectura, não faz distinção entre redes WLAN e LAN. O mesmo equipamento (*switch*) terá capacidade para suportar os dois tipos de redes, logo a gestão da rede da organização, quer WLAN quer LAN será mais facilitada pois a questão da centralização é mais abrangente [Synergy,2006]. A Figura 11 ilustra bem as diferenças das duas arquitecturas: enquanto nas arquitecturas centralizadas existe um servidor dedicado (*appliance*) para gerir os equipamentos WLAN, na arquitectura unificada o mesmo

equipamento de rede assegura a comunicação e a manutenção quer, dos equipamentos LAN, quer dos WLAN.

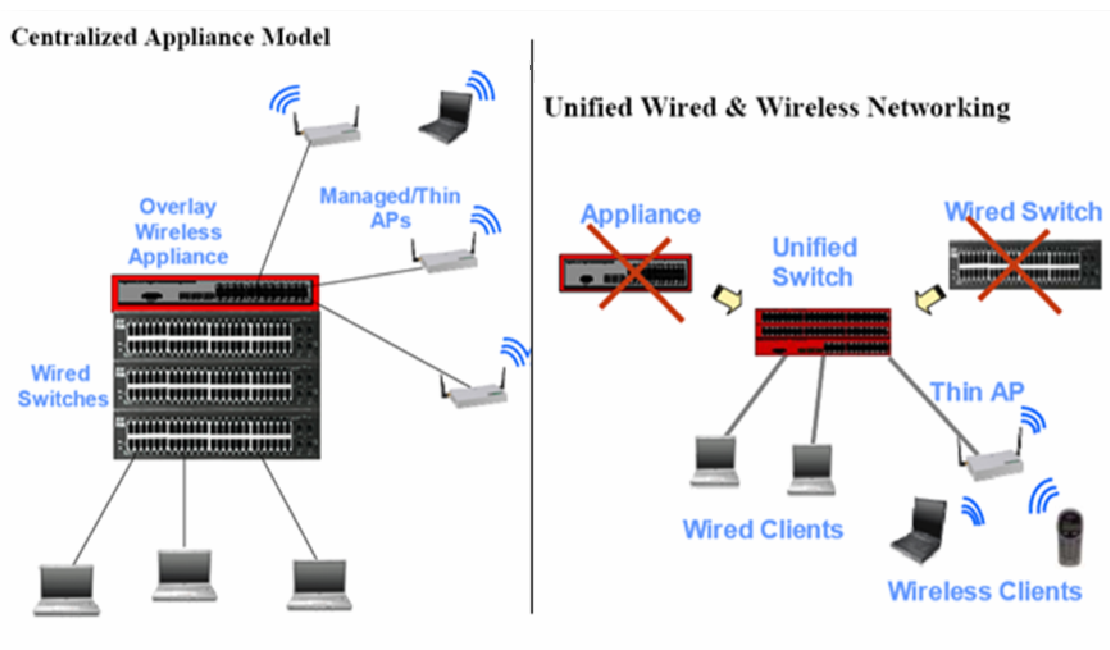


Figura 11: Arquitecturas unificadas

2.3 TENDÊNCIA DE IMPLEMENTAÇÃO DAS REDES WBL

As redes WBL não são apenas úteis para as áreas rurais ou para áreas que não tenham acesso à Banda Larga, estando a proliferar e sendo muito utilizadas como factor de desenvolvimento e diferenciador. O acesso à internet é já hoje considerado um elemento vital como o é por exemplo a água, o saneamento ou a electricidade. Existem várias cidades a optar por fornecer serviços de acesso à Internet gratuitos, constituindo este aspecto, um indicador de qualidade de vida das mesmas.

A nível empresarial o sucesso das redes WLAN é sobejamente conhecido, pois hoje em dia qualquer organização tem o seu router com capacidades wireless para fornecer cobertura nas suas instalações. Ao nível doméstico, vários estudos indicam o crescimento na utilização desta tecnologia.

Neste ponto aborda-se a tendência de implementação que as redes WBL estão a tomar actualmente assim como num futuro próximo.

2.3.1 MUNIWIRELESS

As redes WBL são consideradas por muitos, a terceira revolução das redes Wireless, depois dos telemóveis (1990s) e do Wi-Fi (2000s). A natureza do meio de transmissão destas redes oferece o acesso imediato a utilizadores móveis e fixos, que é claramente um elemento vital para o suporte de vários serviços como a voz, vídeo, dados e mobilidade.

Este tipo de redes estão muitas vezes associadas às redes municipais, que têm vindo a evoluir bastante nos últimos tempos. Normalmente são também conhecidas por MuniWireless. O MuniWireless é o termo utilizado para definir as redes Wi-Fi metropolitanas implementadas nas cidades. Estas redes sem fio permitem, entre outras coisas, o acesso público à Internet em qualquer ponto da cidade, assim como a possibilidade de criar redes privadas de uso específico. Dado que o domínio público das cidades é gerido pelos Municípios, o MuniWireless é uma rede com propensão para ser proprietária dos mesmos, daí o termo “Muni” [Cisco,2007].

Estas redes subentendem a criação de uma rede em malha, normalmente também designadas por *wireless mesh*, que pressupõem a instalação de vários pontos de acesso na cidade tendo linha de vista para, pelo menos, outro ponto. O ideal será que possam estar em linha de vista com mais do que um ponto de forma a criar redundância e balanceamento de carga na comunicação, como se ilustra na Figura 12. O seu funcionamento assenta nas tecnologias IEEE 802.11a/b/g, mas o aparecimento do WiMax (IEEE 802.16) e do IEEE 802.11n poderá alterar determinantemente esta situação.

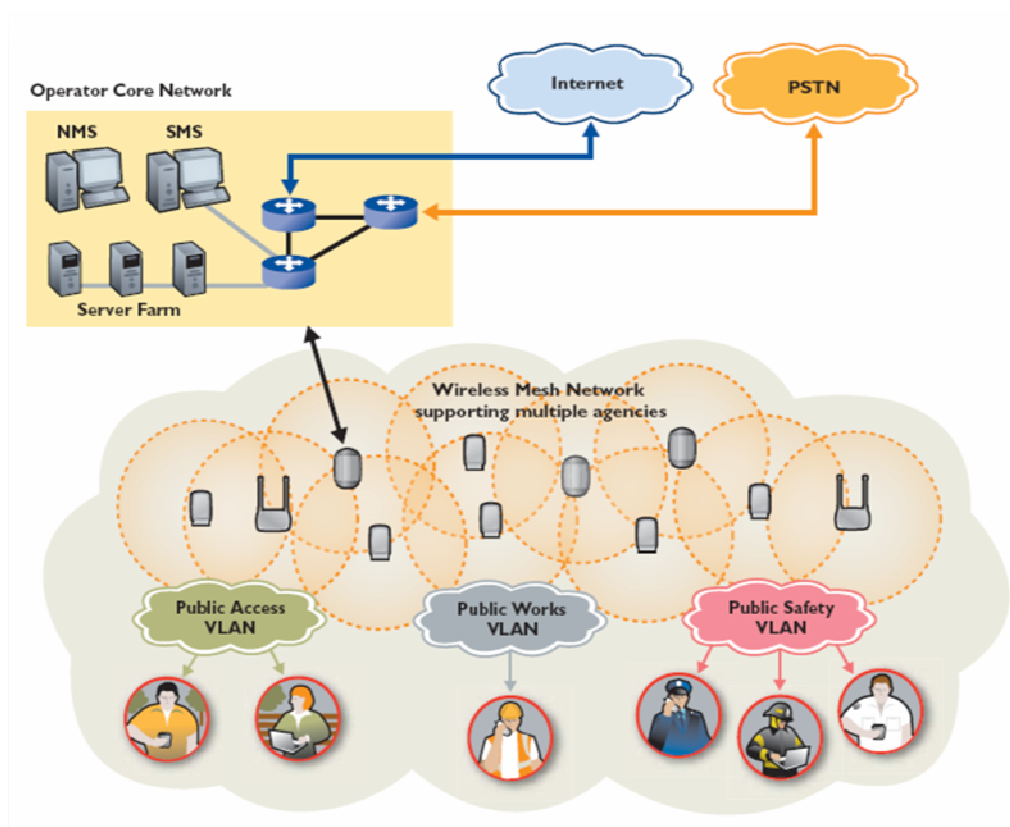


Figura 12: Redes MuniWireless

Este tipo de implementação de redes WBL, está a originar ainda um tipo de mercado até então inexistente, tendo até vários modelos de negócio. Alguns Municípios optam por construir a infra-estrutura para depois a concessionar em troca de um benefício financeiro.

2.3.2 PROJECTOS DE INVESTIGAÇÃO

Quase findo o Capítulo 2, importa aflorar os projectos de investigação que estão a ser realizados por parte de várias equipas quer na Europa quer na América Latina. Escolheram-se estas duas localizações geográficas, por uma questão de enquadramento com o nosso país. Estes projectos de investigação são indicativos sobre o futuro das tecnologias wireless.

A constante tentativa de melhorar a cobertura e o desempenho das redes wireless, impulsiona a existência de uma investigação cada vez mais acentuada na tentativa de descobrir novas tecnologias e fazer emergir outras. Subsiste também a tentativa de fazer um melhor aproveitamento das frequências já existentes [Galvis et al,2007].

Um dos projectos de investigação que ocorreu (2005-2007), onde já foram utilizadas as bandas HF (*High Frequency*) e VHF/UHF para disponibilizar voz, internet e e-mail a zonas rurais é o projecto de “Telemedicina Rural”, em que participam grupos de investigação da Argentina, Brasil, Perú, Equador, Colombia, Venezuela, Cuba, República Dominicana e México. Estes países integram um consócio chamado EHAS²¹ (*Enlace Hispano Americano de Salud*), integrado num programa EHAS-@LIS, financiado pela Comissão Europeia no programa CYTED²². No Peru, foi implementado um projecto para melhorar a saúde materno-infantil, que consistiu em fornecer dados e voz em zonas rurais, através das frequências de TV com recurso a software livre, constituindo por isso uma solução de baixo custo [Sala et al,2006].

O Grupo de Investigação de Redes de Computadores²³ da Universidade Politécnica de Valência, está neste momento a desenvolver um projecto denominado de RURALNET²⁴, cujo objectivo é desenvolver uma arquitectura de rede wireless, baseada em portais captativos, para proporcionar serviços de acesso à internet em áreas rurais da comunidade valenciana.

A Universidade Nacional de Engenharia²⁵ no Peru, está a investigar entre outros, a possibilidade de fornecer acesso à internet em zonas rurais e urbanas que estejam discriminadas, utilizando tecnologias *mesh* e WiMax, permitindo ainda a sua aplicação em comunicações de emergência.

No Equador, uma fundação de investigação chamada CITIC²⁶ (*Fundación Centro Internacional de Investigación Científica en Telecomunicaciones, Tecnologías de la Información y las Comunicaciones*), define nas suas principais áreas de trabalho para as redes wireless, entre outros, a investigação e desenvolvimento de aplicações de gestão e administração de redes móveis (móveis, WIFI, WIMAX).

O grupo de redes wireless do Departamento de Engenharia Telemática da Universidade Politécnica da Catalunha (Espanha) desenvolve entre outros, investigações nas seguintes áreas:

²¹ <http://www.ehas.org>

²² <http://www.cytcd.org>

²³ <http://www.grc.upv.es>

²⁴ http://www.grc.upv.es/prog_desc/ruralnet.htm

²⁵ <http://inictel.uni.edu.pe>

²⁶ <http://www.citic.org.ec>

- Estudo das possibilidades de utilização de uma interface rádio IEEE802.11, IEEE802.15.4, IEEE802.16 e TETRA²⁷ (*Terrestrial Trunked Radio*) na construção redes mesh;
- Desenvolvimento de projectos para conectividade de redes heterogéneas que prevêem mecanismos para fazer face a problemas de perda de benefícios e de interoperabilidade.

Na Universidade Pontifica Boliviana²⁸, as áreas de investigação das redes wireless são diversas, a saber:

- Modelagem conjunta da camada física e camada MAC (*Media Access Control*) para a análise de sistemas através de acesso de redes Banda Larga de malha sob o padrão IEEE 802.16;
- Sistema de antenas adaptativas para redes IEEE 802.11 em ambientes reais;
- Convergência de redes de Banda Larga;
- Implementação de técnicas para DAS (*Dynamic Spectrum Access*) e DFS (*Dynamic Frequency Selection*) mediante rádio cognitivo;
- Interoperabilidade em camadas inferiores de sistemas wireless;
- Modelagem de canais wireless para a norma IEEE 802.16.

Na Escola Técnica Superior de Engenheiros de Telecomunicações²⁹, da Universidade Politécnica de Madrid, investiga-se entre outros:

- Acesso de serviços Internet móvel em Banda Larga: WLAN, UMTS;
- Integração de redes fixas com redes móveis;
- Gestão de redes, serviços e aplicações;
- Segurança de redes wireless.

O Centro Experimental de Comunicações Wireless³⁰, da Universidade Rey Juan Carlos, Espanha, definiu como linhas de orientação de redes wireless que oferecem acesso simples, e barato a serviços e redes de comunicações, quer com tecnologias de última geração (UMTS), WPA (Bluetooth, ZigBee), Wi-Fi e WiMax. Dois dos projectos mais emblemáticos são: o

²⁷ <http://www.tetra-association.com>

²⁸ <http://convena.upb.edu.co/gidati/proyectos.html>

²⁹ <http://www.etsit.upm.es/investigacion/grupos-de-investigacion-en-la-etsit/redes-y-servicios-de-telecomunicacion-e-internet-rsti.html>

³⁰ <http://www.tsc.urjc.es/investigacion/ceci/>

serviço de localização baseados em redes Wi-Fi e interoperabilidade entre as redes Wi-Fi e WiMax.

Na Universidade de Vigo o grupo de Processamento de Sinal e Comunicações, do Departamento de Teorias de Sinal e Comunicações³¹, estão neste momento focados entre outros, em investigar o processamento de sinal com técnicas avançadas para rádio cognitivas (conceito já abordado no ponto 2.1.4 – Redes WRAN), cuja necessidade advém da possibilidade de fazer coexistirem várias tecnologias wireless. O surgimento do grupo de trabalho da norma IEEE 802.22 (WRAN), releva a importância da investigação na área dos rádios cognitivos, uma vez que se espera a coexistência desta norma com outras normas IEEE, como a 802.11 e a 802.16.

As tecnologias baseadas em MIMO estão também a ser alvo de diversas investigações na Europa, por exemplo o Instituto Eurecom³² (Escola de Engenheiros e Centro de Investigação) em Franca, tem diversas publicações onde esta tecnologia está muito presente. Este Instituto em parceria com outros³³, está também a trabalhar em projectos de investigação de rádio cognitiva³⁴, onde o fornecimento de Internet Banda Larga em zonas rurais merece a atenção, na medida em que o recurso às tecnologias wireless são vistas como uma inevitabilidade. Investiga-se inclusivamente a possibilidade da norma IEEE 802.22, ser uma norma que no futuro possa permitir o fornecimento de Banda Larga através das bandas de TV UHF e VHF. Na Figura 13 pode ser observado a implementação de uma rede com recurso a esta norma, onde existem as WRAN BS (Base Station), que transmitem o sinal para os WRAN *Repeater*, que o distribuem através da WLAN para os edifícios.

³¹ <http://www.gts.tsc.uvigo.es/gpsc/projects.html>

³² <http://www.eurecom.fr>

³³ <http://www.sendora.eu/node/2>

³⁴ <http://www.sendora.eu>

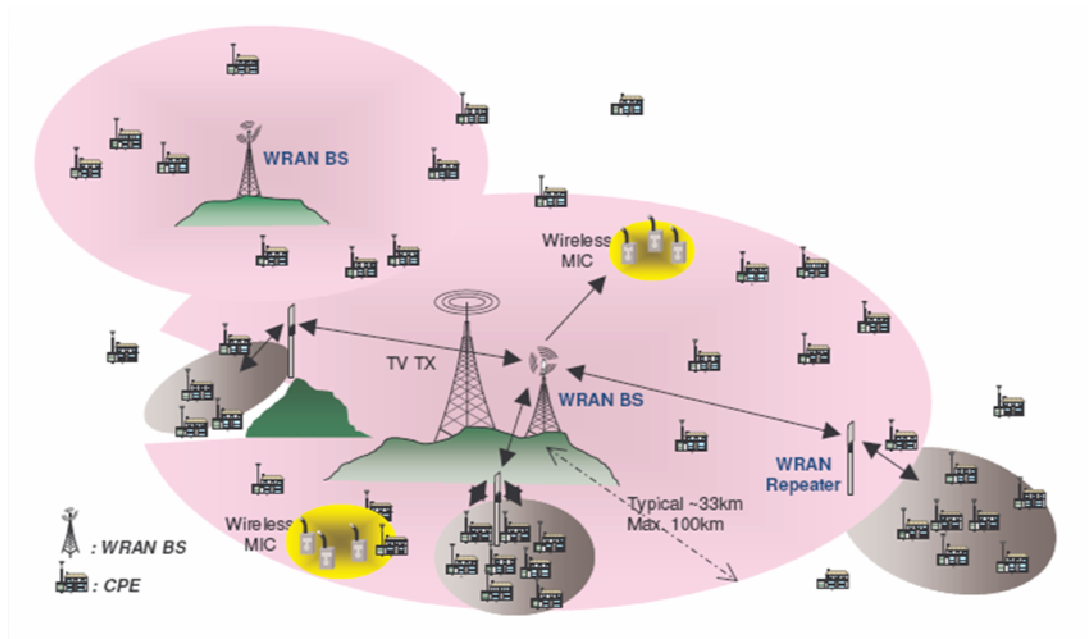


Figura 13: Arquitectura da rede IEEE 802.22 (WRAN)

O projecto HNPS (*Heterogeneous Network for European Public Safety*), é um projecto de investigação, que consiste no desenvolvimento de um conceito de redes heterogéneas, para futuras comunicações Europeias de protecção civil. Na Figura 14, pode observar-se a arquitectura deste projecto de investigação. Este é um projecto apoiado pela Comissão Europeia, desenvolvido pelo *Forum for Public Safety Communication Europe*³⁵, estando previsto a sua conclusão em 2011.

³⁵ <http://www.publicsafetycommunication.eu>

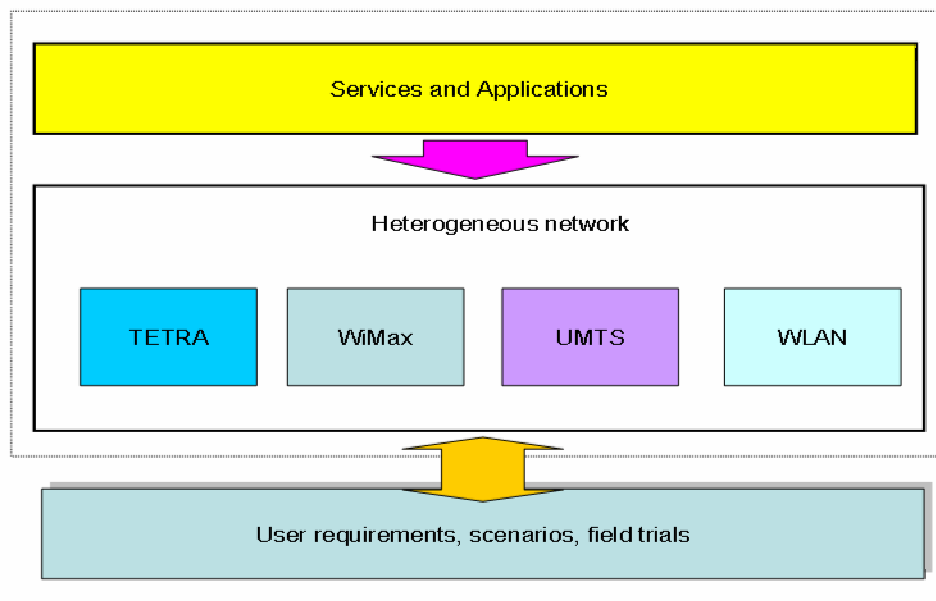


Figura 14: Arquitectura do projecto HNPS

Na Figura 15, pode ser observado uma implementação prática deste projecto, onde diversas tecnologias coexistem na mesma rede.

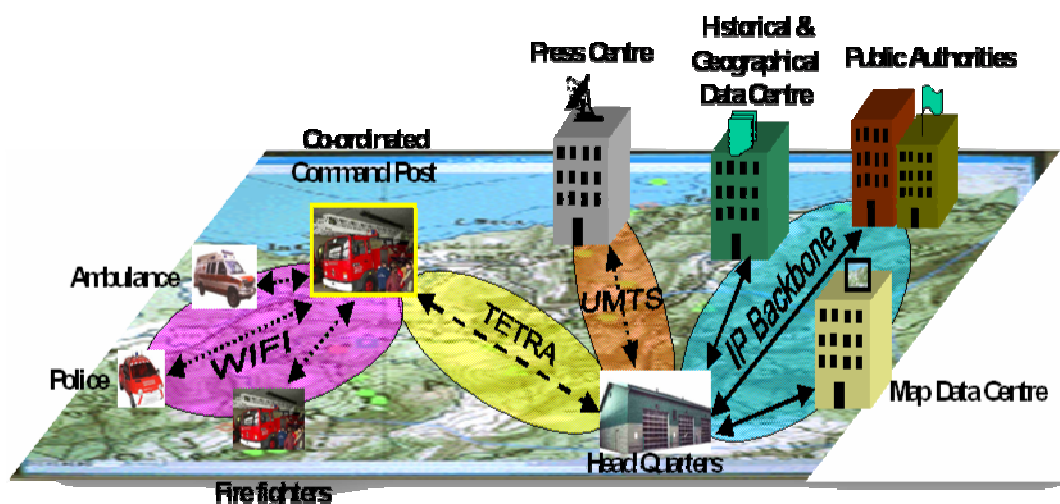


Figura 15: Implementação do projecto HNPS

No Reino Unido as áreas de investigação das redes wireless também estão muito focadas nos rádios cognitivos, como é o exemplo do Grupo de Investigação de Comunicações do Departamento de Electrónica³⁶, da Universidade de York³⁷.

Também no Reino Unido, o CWIND (*Center for Wireless Network Design*)³⁸, da Universidade de Bedfordshire³⁹, faz actualmente investigação nas seguintes áreas:

- Abordagens e ferramentas automáticas para planeamento e optimização das redes de rádio 3G/4G/WiFi/WiMAX;
- Planeamento de rede, optimização e avaliação de desempenho de redes wireless heterogéneas;
- Propagação determinística de rádio para a modelação WiFi, UMTS e WiMAX;
- O uso de medições no planeamento da rede;
- Processamento e análise de dados medidos na rede;
- Análise de performance e simulação de redes WLAN;
- Comunicação em tempo real e QoS nas redes wireless;
- Protocolos MAC e estudos de desempenho de redes wireless *mesh* e redes de sensores wireless.

Como já referido no ponto 2.3.1 - Muniwireless, a Administração Pública está cada vez mais sensível para a importância da utilização da Internet como forma de desenvolvimento das suas populações, pelo que começam a interessar-se por implementar cada vez mais redes wireless. Supõe-se que as tecnologias emergentes a curto prazo serão o IEEE 802.11n⁴⁰ e o IEEE 802.16⁴¹ (WiMax), a longo prazo prevê-se o aparecimento das redes IEEE 802.22⁴² (WRAN).

2.3.3 DESAFIOS NA GESTÃO DE REDES WBL

Nesta altura será então interessante levantar a seguinte questão: quais são os desafios para a gestão das redes WBL? Tentaremos resumir a resposta nos parágrafos seguintes.

³⁶ <http://www.elec.york.ac.uk/comms/cognitive.html>

³⁷ <http://www.york.ac.uk>

³⁸ <http://www.beds.ac.uk/research/irac/cwind>

³⁹ <http://www.beds.ac.uk>

⁴⁰ http://www.ieee802.org/11/Reports/tgn_update.htm

⁴¹ <http://wirelessman.org>

⁴² <http://ieee802.org/22>

As arquitecturas WBL vão continuar a evoluir e destas dependerá a facilidade de gestão das mesmas. É fundamental assegurar que novas aplicações como a voz e vídeo possam ter desempenho sem comprometimento das restantes. Segundo [Halton,2007], o grande desafio é saber como fazer uma gestão eficiente/adequada das várias arquitecturas.

Na Figura 16 observa-se o ciclo de inovação das tecnologias wireless, de onde se podem depreender os requisitos que a gestão das redes WBL deve assimilar. As arquitecturas unificadas e *mesh* representam um grande desafio, no entanto os sistemas de gestão, não podem descurar as várias arquitecturas já implementadas e em funcionamento no mercado.

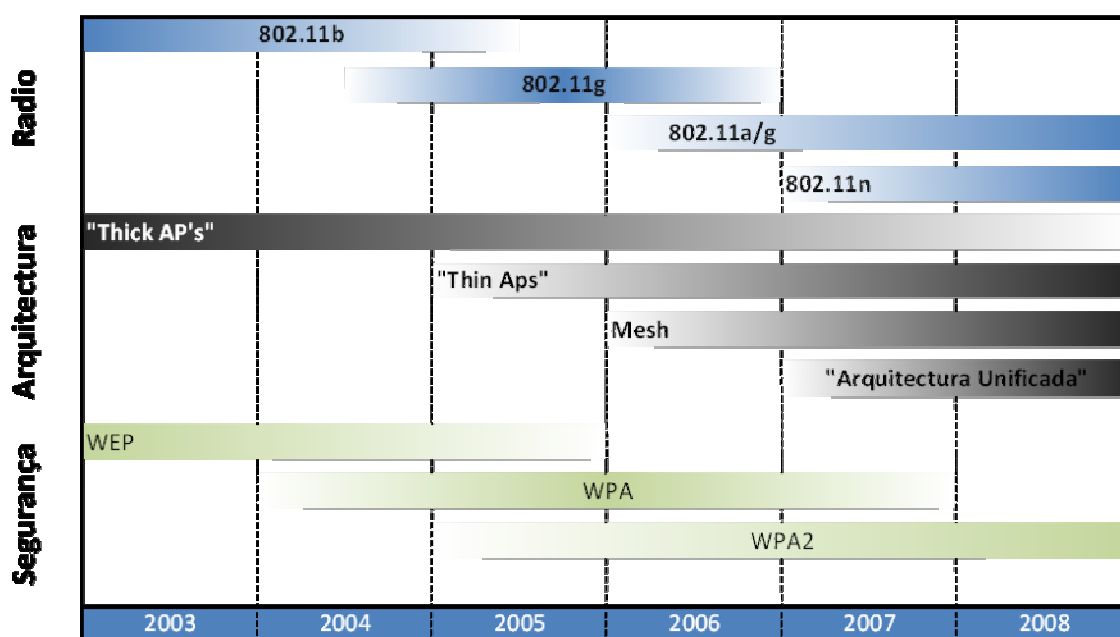


Figura 16: Ciclo de inovação da tecnologia Wireless

Surgirão as seguintes questões:

- Como gerir todas as variáveis da rede WBL: múltiplas arquitecturas, múltiplos fabricantes de hardware, múltiplas tecnologias rádio?
- Como integrar com o resto da infra-estrutura?
- Como se deve migrar a rede WBL? Migrar todos os equipamentos não será com toda a certeza a melhor solução em termos financeiros. É importante avaliar os custos da migração e tentar fazer uma migração gradual.

As arquitecturas dos sistemas de gestão de redes WBL são diferentes de fabricante para fabricante. Estas diferenças podem ter um impacto significativo na rede LAN, nos equipamentos WBL e na qualidade dos serviços prestados.

A cobertura era a grande preocupação entre os anos 2003 e 2006. Hoje em dia a preocupação está na capacidade para gerir o tráfego gerado, quer com vídeo quer com a voz [Halton,2007].

A rápida adopção das redes WBL faz com que deixe de ser uma tecnologia emergente, tornando-se numa ferramenta fundamental para as organizações, que coloca novas exigências sobre estas redes [Colubris,2005], que se enumeram a seguir:

- **Mobilidade:** inicialmente os fabricantes de produtos WBL, conceberam produtos de forma a suportar uma utilização nómada. Os trabalhadores da organização poderiam aceder à rede WBL em gabinetes ou salas de conferências, mas não nos corredores, por exemplo. Neste momento, está a surgir uma nova geração de aplicações, com a voz na primeira linha, que exige redes WBL com suporte contínuo de mobilidade em tempo real. Uma WBL deverá conseguir garantir ligações de alta performance para utilizadores com dispositivos de rede sem fio, mesmo quando estes se movem. Este aspecto requer que o sistema de gestão monitorize a mobilidade dos utilizadores em tempo real;
- **Diversidade de utilizadores:** para aumentar a produtividade e comodidade, as empresas estão a abrir as suas redes wireless a vários tipos de utilizadores. Além de dar acesso às aplicações internas aos seus colaboradores, as empresas fornecem acesso às redes wireless a pessoas que a visitam e em muitos dos casos, fornecem mesmo o acesso gratuito à internet. As questões relativas à qualidade do serviço e à segurança são agora uma preocupação mais relevante;
- **Mais dispositivos:** não são apenas mais computadores pessoais, mas vários tipos de dispositivos wireless que estão a aparecer em ambientes corporativos. Por exemplo, telemóveis, PDAs (*Personal digital assistants*), scanners de código de barras, impressoras, etc;
- **Implementação massiva:** o objectivo das organizações é fornecer o máximo de cobertura possível, dar acesso para todos os utilizadores em todas as localizações. A rede WBL deverá ser escalável para suportar aumentos de utilizadores e dispositivos;
- **Integração:** integração com dispositivos de outras redes;

Com o surgimento do IEEE 802.11n e do IEEE 802.16, o tráfego WBL irá aumentar. A voz sobre redes wireless será uma realidade e as redes terão de ter mais capacidade para a suportar.

Apesar do mercado empresarial crescer mais rápido que o mercado dos consumidores, uma quota-parte das empresas ainda continua a ser metade do conjunto de todo o mercado. Os problemas iniciais de segurança (WEP) e de QoS estão agora resolvidos. A indústria foca-se agora no desenvolvimento de novas normas para melhorar a performance (802.11n e 802.11r), segurança (802.11w), gestão (802.11k e 802.11v), facilidade de uso (802.11u) e flexibilidade de implementação (802.11s, 802.11y e 802.11p). Resumindo, as novas normas ajudarão a tornar as redes WBL mais parecidas com as redes LANs [DeBeasi,2007b].

Devido ao aparecimento das arquitecturas unificadas, a tendência da gestão de redes, caminha a passos largos para uma gestão híbrida, ou seja, para a gestão, não haverá distinção entre as redes LAN e wireless.

É ainda previsível e espectável que a função de gestão de redes wireless possa ser mais simplificada com o aparecimento dos protocolos CAPWAP, IEEE 802.11k e IEEE 802.11v.

2.4 RESUMO

É espectável que o futuro das redes wireless, seja um conjunto de diferentes tecnologias, com diferentes larguras de banda e áreas de cobertura. As redes WLAN podem conseguir velocidades rápidas de acesso à internet em espaços limitados, enquanto as redes WMAN oferecem um amplo acesso à rede, mas com taxas mais limitadas. A tendência natural é antes de mais, utilizar a elevada largura de banda fornecida pelas redes WLAN e grande cobertura com as redes WMAN [Nie et all, 2005].

Outra tecnologia que poderá emergir nos tempos mais próximos é a WRAN, definida na norma IEEE 802.22⁴³. O grupo de trabalho IEEE 802.22 está a trabalhar para definir a primeira norma de rádios cognitivas para operar no mesmo espectro de sinal utilizado para transmitir TV.

⁴³ <http://grouper.ieee.org/groups/802/22/>

Relativamente às áreas de investigação, pode aferir-se que os centros de investigação na área das tecnologias wireless estão a centrar os seus esforços para os sistemas de rádio cognitivo. Obviamente que a questão do rádio cognitivo não pode ser dissociado das investigações que estão a ser efectuadas para facilitar a interoperabilidade das redes heterogenias.

Neste capítulo foram identificados e definidos diversos termos das tecnologias wireless. Apresentaram-se de forma muito sumária as variantes da norma IEEE 802.11, que se consideram importante devido à sua abrangência. O contributo desta identificação, permite ainda perceber o estado da arte das diferentes normas IEEE 802.11, facultando uma melhor percepção de ratificações e datas para as mesmas.

Optou-se ainda por utilizar um termo próprio, para identificar o conjunto de tecnologias, que este tema pode albergar. Assim o WBL é o termo mais adequado para representar as diversas tecnologias wireless Banda Larga.

3. LEVANTAMENTO DE FUNCIONALIDADES E DE SOLUÇÕES DE GESTÃO DE REDES WBL

Um dos objectivos deste trabalho pressupõe a definição de um conjunto de funcionalidades, de forma a tornar uma solução de gestão de redes WBL eficiente e completa. Outro dos objectivos é estudar as diversas soluções existentes, para conseguir alcançar uma gestão centralizada das redes WBL.

Neste capítulo é efectuada uma identificação das diversas funcionalidades que se consideram importantes para uma boa solução de gestão WBL. De seguida são analisadas as soluções *opensource* e soluções comerciais existentes, identificando quais as funcionalidades de que dispõem.

Esta identificação será o input necessário para a definição de um modelo para a gestão das redes WBL (Capítulo 4 – Modelo de gestão de redes WBL).

3.1 FUNCIONALIDADES DE GESTÃO DE REDES WBL

Neste ponto são apresentadas as funcionalidades consideradas fundamentais numa solução de gestão de redes WBL. Este levantamento resulta de uma investigação de soluções comerciais existentes no mercado, assim como de soluções *opensource*.

Para melhor apresentar a panóplia de funcionalidades existentes, será elaborada a Tabela 3 onde se detalha sumariamente cada uma das funcionalidades.

Acesso baseado por perfil de utilizador	Acesso à solução baseado em perfis. Exemplo: Administrador, Técnico, Helpdesk, cliente.
Actualizações de firmware	Actualização automática do <i>firmware</i> dos equipamentos de rede.
Ajuste de transmissão de potência e selecção de canais	Possibilidade de ajustar a potência de transmissão e a escolha das Antenas.
Agendamento para instalação de firmware	Possibilidade de agendar instalações e actualizações nos equipamentos de rede.
Alarmes	Possibilidade de definir alarmes para a ocorrência de determinados eventos.
Alerta de configurações obsoletas	Alerta para o facto de determinadas configurações estarem obsoletas, de acordo com as políticas definidas.
Antivírus	Existência de anti-vírus.
Auditoria	Realização de diversas auditorias na rede, como por exemplo: segurança, utilização, erros de configuração, testes de carga, entre outros.
Balanceamento de carga	Possibilidade de identificar problemas e prover balanceamento de carga.
Billing/Accounting	Possibilidade para fazer a contabilização do acesso do utilizador em termos de tempo, de largura de banda utilizada, dados transferidos, etc.
Captura de pacotes na rede	Possibilidade de capturar pacotes de tráfego na rede para análise.
Command Shell	Possibilidade de operar a solução via linha de comandos.
Configurações modelo	Definição de configurações modelo, para poderem ser aplicadas a qualquer momento.
Configurações remotas	Funcionalidade para permitir efectuar configurações remotas em larga escala, ou seja por grupo.
Descoberta automática	Possibilidade de descobrir automaticamente os equipamentos da rede.
Detecção de ataques DoS	Detecção de ataques de negação de serviço.
Detecção de configurações erradas	Detecção de configurações erradas nos equipamentos da rede.
Detecção de intrusão	Detecção de intrusão na rede, por parte de acessos não autorizados.
Detecção de Rogue APs	Detecção de APs que se ligam à rede sem autorização.
Diagnóstico e correlação de erros	Correlacionar e diagnosticar erros e corrigi-los automaticamente.

EAP	O EAP (Extensible Authentication Protocol) é um protocolo de autenticação de redes wireless, definido no RFC 3748 ⁴⁴ , e permite passar a autenticação de dados, entre um servidor de Radius, o AP e o cliente wireless.
Envio de relatórios por mail	Possibilidade de agendar envio de relatórios por correio electrónico.
Filtragem de tráfego P2P	Identificação e bloqueio de tráfego P2P.
Firewall	Qualquer conjunto de esquemas de segurança que evitam que utilizadores não autorizados acessem a uma rede informática ou monitorizem transferências de informações de e para a rede.
Forçar a aplicação de políticas de segurança	Esta funcionalidade significa que a aplicação de gestão da rede WBL, permite forçar a aplicação de políticas de segurança a qualquer momento, em todos os dispositivos.
Gestão baseada em grupos	Suporte para gestão por grupos para permitir implementar facilmente novas políticas de segurança nos vários segmentos da rede (equipamentos, VLANs, SSID's, utilizadores, departamentos, localizações, etc.)
Gestão centralizada de configurações	Possibilidade de centralmente configurar diversos parâmetros nos equipamentos de rede.
Gestão de largura de banda	Conjunto de mecanismos que controla a taxa de alocação de dados, variações de atraso, tempos de entrega, fiabilidade da entrega.
Gestão de utilizadores	Possibilidade de efectuar uma gestão eficaz dos utilizadores e perfis de grupo.
Informação Gráfica	Informação gráfica da mais variada ordem, como por exemplo a utilização da largura de banda por utilizar, ou por determinada porta da rede.
Helpdesk	Módulo para registar e encaminhar pedidos de Helpdesk por parte dos utilizadores da rede.
Autenticação com LDAP	O IEEE 802.1x faz parte do conjunto de protocolos do IEEE 802. Este protocolo garante que a autenticação para a utilização da rede wireless, possa ser efectuada recorrendo a sistemas de autenticação com o LDAP (<i>Lightweight Directory Access Protocol</i>), pertencente a uma rede LAN.
Informação sobre as vulnerabilidades	Informa o administrador de eventuais vulnerabilidades existentes na rede.
Interface Web	Possibilidade de gerir o software através de um interface Web.
Listas de acessos MAC	Possibilidade de controlar os acessos através do MAC Address dos equipamentos.
Log's dos eventos na rede	Faz log's de todos os eventos na rede, e permite a sua consulta com facilidade e clarividência.
Mapa da rede	Desenhar o mapa da rede e colocá-lo graficamente visível.
Medição de interferências (ruído)	Possibilidade de medir interferências no RF, e detectar as suas fontes e otimizar as configurações para mitigar essas interferências.

⁴⁴ <http://tools.ietf.org/html/rfc3748>

Monitorização da potência e qualidade de sinal RF	Funcionalidade que permite medir a potência e a qualidade do sinal RF.
Monitorização de eventos de roaming	Para os casos onde exista roaming, é importante monitorizar como é que este é garantido, e ainda detectar prováveis falhas.
Monitorização do tipo de tráfego	Possibilidade de identificar quais são as aplicações que o cliente está a utilizar na rede.
Monitorização em tempo real (Dashboard)	Possibilidade de verificar em tempo real, o que está a acontecer na rede WBL.
Optimização das configurações RF	Possibilidade de efectuar uma análise das configurações e otimizar as mesmas para se conseguir uma melhor cobertura e utilização do espectro.
Pesquisa de dispositivos	Possibilidade de efectuar pesquisas de dispositivos de forma simples e rápida.
Pesquisa de informação	Motor de pesquisa englobando todo o tipo de informação possível.
Planeamento	Permitir efectuar um planeamento da infra-estrutura a ser utilizada, identificando inclusive restrições de protocolos e frequências dependentes da localização geográfica.
Portal Captativo/Hotspot Gateway	Uma forma de controlar o acesso dos utilizadores à rede, fornecendo ao utilizado um interface Web, para que este se possa autenticar. Muito utilizado para <i>hotspots</i> públicos de acesso à Internet.
Promove a rotação automática de chaves privadas	Possibilidade de trocar automaticamente chaves dos protocolos de segurança. Esta funcionalidade permite aumentar a segurança.
Proxy	Para além de permitir fazer cache das páginas mais visitadas, aumentando a velocidade de navegação na Internet, permite filtrar conteúdos e permitir ou negar o acesso.
Quality of Service (QoS)	Possibilidade para priorizar e moldar o tráfego da rede. O objectivo é fornecer qualidade ao serviço.
Relatórios de Erros de utilização	Fornecimento de relatórios de erros de utilização.
Relatórios de utilização da rede	Fornecimento de relatórios de utilização da rede, por exemplo a nível de protocolos, aplicações e acções indevidas.
Relatórios de utilização de canais	Extracção e identificação da utilização dos canais na rede.
Relatórios por elemento	Fornecimento de relatórios de actividades por elemento da rede (APs, cliente, administrador, entre outros).
Relatórios por períodos de tempo	Possibilidade de fornecer relatórios por períodos de tempo.
Serviços de localização	Possibilidade de localizar geograficamente os equipamentos dos clientes, assim como gravar em histórico o trajecto percorrido.
Servidor de RADIUS	O RADIUS (<i>Remote Authentication Dial-In User Service</i>), é um protocolo que utiliza um servidor de autenticação para controlar o acesso à rede.
Servidor DHCP	Servidor que permite atribuir definições de IP ao cliente para operar na rede.
Site Survey	Funcionalidade para efectuar uma pesquisa do espectro disponível e concluir as possibilidades de sucesso na implementação de um equipamento.

SNMP	O SNMP (<i>Simple Network Management Protocol</i>) é o protocolo de monitorização e controlo de rede. A utilização deste protocolo para a gestão da rede WBL é essencial.
SSH	Acesso remoto à solução via SSH.
Suporte a equipamentos de diferentes fabricantes	Possibilidade de suportar equipamentos de fabricantes diferentes.
Suporte para VLAN	Suporte para operar várias VLAN's.
Visualização em mapa de área coberta RF	Visualizar num mapa a área de cobertura RF, qualidade do sinal, zonas de sombra, entre outros.
Visualização em mapa do AP intruso	Possibilidade de visualizar a localização em mapa, do AP que se ligou à rede indevidamente.
VoWLAN	Suporte para VoWLAN, ou seja, voz sobre rede wireless.
VPN	VPN (<i>Virtual Private Network</i>) Medida de segurança para proteger os dados à medida que saem de uma rede e se dirigem para outra através da Internet.
WBL Performance	Análise de performance global da rede.
WDS	O WDS (<i>Wireless Distribution System</i>) permite estender a cobertura da rede wireless com facilidade, ou seja, sem efectuar demasiadas configurações.
WEP	O WEP (<i>Wired Equivalency Protocol</i>) é um protocolo de segurança para redes wireless e destina-se a fornecer segurança ao encriptar os dados através de ondas de rádio, de forma a ficarem protegidos à medida que forem transmitidos de um ponto para outro. É utilizada uma chave partilhada (semelhante a uma palavra-passe) para permitir a comunicação entre os computadores e o AP.
WPA	O WPA (<i>Wi-Fi Protected Access</i>) é o protocolo de segurança para redes wireless baseado no protocolo WEP. Protege a transmissão de dados sem fios utilizando uma chave semelhante ao WEP, mas a eficácia acrescida do WPA resulta na alteração dinâmica da chave.
WPA2	WPA2 (<i>Wi-Fi Protected Access 2</i>) é a segunda geração de segurança WPA e proporciona um mecanismo de encriptação mais forte através de AES (<i>Advanced Encryption Standard</i>).

Tabela 3: Funcionalidades de gestão de redes WBL

Após a identificação das funcionalidades, procurou-se investigar algumas soluções *opensource*, que pudessem satisfazer estes requisitos. É esse trabalho que se aflora nos capítulos seguintes.

3.2 SOLUÇÕES OPENSOURCE

Após uma pesquisa aprofundada de ferramentas *opensource* de gestão de redes wireless, identificou-se a existência de uma distribuição de tipos de ferramentas por categoria. Entendeu-se dividir as várias soluções de software em várias categorias, que se enumeram a seguir:

- Sistemas operativos (*firmware's wireless*);
- Portais captativos (*hotspot gateway*);
- Auditoria e Segurança;
- Diagnóstico, Monitorização e Inventário;
- Serviços de localização;
- Suites de software;
- Live CD's;

3.2.1 SISTEMAS OPERATIVOS WIRELESS (*FIRMWARES WIRELESS*)

Os sistemas operativos wireless são sistemas embebidos, que segundo [Kumar et al,1996] constituem um sistema de aplicações específicas, que contêm hardware e software para realizar uma determinada tarefa. No mercado existem alguns equipamentos que permitem a actualização do seu *firmware*, baseados em *firmware* wireless. Esta capacidade permite que o equipamento possa ser configurado à medida do que se deseja. Alguns equipamentos conseguem dar ao utilizador um elevado controlo na configuração e na utilização do mesmo [Innes,2005]. Para que tal possa acontecer é necessário utilizar um software desenvolvido especificamente para esse fim. As funcionalidades de gestão da rede wireless ganham flexibilidade e funcionalidade, pois é possível escolher e parametrizar os módulos necessários.

Encontram-se várias soluções de *firmware* em *opensource*, baseados em distribuições Linux, que se elencam a seguir:

- Sveasoft⁴⁵;
- OpenWrt⁴⁶;
- DD-Wrt⁴⁷;
- HyperWRT⁴⁸;
- m0n0wall⁴⁹;
- Mikrotik⁵⁰;

A versão de *firmware* mais actual da SveaSoft é denominada por Talisman, suportando diversas funcionalidades de gestão de redes wireless. O *firmware* Talisman pode ser instalado em routers wireless da ASUS, Belkin, Buffalo, Linksys e Netgear.

O OpenWrt oferece características semelhantes às de um pacote de base de distribuição Linux. Entre as diversas funcionalidades que serão apresentadas a seguir, destaca-se uma ferramenta de gestão de pacotes denominado por Ipkg⁵¹.

Existem duas versões principais:

- *whiterussian* – esta versão é mais antiga, mais estável e com mais documentação disponível. O desenvolvimento terminou em 2007.
- *kamikaze* - é a nova versão, baseada numa arquitectura diferente e por isso pode ser instalado num número mais alargado de equipamentos.

O *firmware* DD-WRT foi um projecto que inicialmente era baseado no Sveasoft, mas depois passou a ser uma variante do OpenWrt. É desenvolvido com base na licença GPL (*General Public License*).

O HyperWRT é um projecto GPL com o objectivo de desenvolver um *firmware* para routers wireless da marca Linksys WRT54G/WRT54GL/WRT54GS e WRTSL54GS com base em *firmwares* da Linksys. O objectivo inicial do projecto do HyperWRT consistia em adicionar um conjunto de características com a flexibilidade que os *firmwares* baseados em distribuições Linux permitem, estendendo as funcionalidades, mas sempre muito próximo do

⁴⁵ <http://www.sveasoft.com>

⁴⁶ <http://openwrt.org>

⁴⁷ www.dd-wrt.com

⁴⁸ <http://www.linksysinfo.co.uk/thibor>

⁴⁹ <http://m0n0.ch/wall>

⁵⁰ <http://www.mikrotik.com>

⁵¹ <http://www.handhelds.org/moin/moin.cgi/Ipkg>

firmware da Linksys. Ao longo do tempo, tem vindo a ser actualizado em conjunto com o *firmware* oficial da Linksys, incorporando várias funcionalidades que tipicamente se encontram em equipamentos deste género.

O *mOnOwall* é um projecto que pretende fornecer aos seus utilizadores um sistema embebido com todas as funcionalidades mais importantes que um sistema de *firewall* disponibiliza actualmente. É baseado no FreeBSD e contém um servidor Web e outras ferramentas auxiliares.

A Mikrotik é uma empresa sediada na Letónia, que fornece um software chamado “MikroTik RouterOS”, capaz de tornar um simples PC (*Personal Computer*) num router, com suporte a Wireless, Proxy, encaminhamento estático e dinâmico, entre outras funcionalidades. Apesar deste software poder ser instalado num PC, a Mikrotik também vende hardware específico para fornecimento de wireless. Apesar de ser desenvolvido em tecnologias *opensource* (Linux), requer licenciamento, ainda que a preços muito competitivos.

3.2.2 PORTAIS CAPTATIVOS (*HOTSPOT'S GATEWAYS*)

No cenário em questão, a disponibilização do serviço wireless de acesso à internet, pressupõe que os utilizadores tenham necessidades diferentes e estejam dispersos por uma vasta área geográfica. Este facto pressupõe a existência de um software que faça a gestão dos acessos dos utilizadores, mormente designado por “portais captativos” ou *hotspot's gateways*.

Como já foi mencionado, um portal captativo é um sistema que redirecciona o utilizador de uma rede de acesso público, para uma página Web que é “obrigado” a visualizar e interagir antes de garantir o acesso. Este tipo de software, força o *browser* do utilizador a visualizar uma página web, que pode ser usada para autenticar o utilizador antes de lhe fornecer acesso à internet. Depois de estar autenticado, o seu endereço IP e MAC (Media Access Control) tem permissão para passar a *gateway* [Lunde et al, 2006].

Existem algumas soluções *opensource* disponíveis, que incluem diversos aspectos relacionados com a gestão das redes wireless:

- Chillispot⁵²;
- Nocat⁵³;

⁵² <http://www.chillispot.info>

- Wifidog⁵⁴;
- Coova⁵⁵;

O ChilliSpot é um software *opensource* para controlar o acesso a redes wireless. É utilizado para autenticar os utilizadores da rede wireless, com funcionalidades *web based login*, muito utilizado para *hotspots* públicos. Pode ser instalado nas seguintes distribuições: Fedora, Debian, Mandrake, OpenWRT, FreeBSD, Gentoo entre outras.

O projecto NoCat transforma uma *gateway* numa ferramenta de portal captativo. Esta tecnologia baseia-se numa *firewall (iptables)* que bloqueia todas as ligações TCP/UDP a partir da rede local, capturando as sessões *http* e redireccionando-as para um portal de login.

O projecto Wifidog é uma solução *opensource* de portal captativo completo e embebido para operar um *hotspot* aberto ou redes de *hotspots*, prevenindo abusos no acesso à internet. Foi inicialmente desenhado para grupos de comunidades wireless, mas adapta-se a outros modelos de fornecimento de serviço wireless. Este sistema permite consultar a cada momento quem está a utilizar o *hotspot*, analisar o tráfego e o tempo de utilização por utilizador, criar um portal personalizado e interagir com os utilizadores, entre outras funcionalidades. Pode ser instalado como módulo no *firmware* OpenWRT.

Baseado no *firmware* OpenWrt, o Coova é um projecto que utiliza o Chillispot para fornecer um portal captativo com várias configurações diferentes, dividindo-se em três módulos: CoovaChilli, CoovaAP e CoovaAAA. O módulo CoovaChilli é o que contempla funções de gestão de redes wireless, nomeadamente com funcionalidades de portal captativo Coova.

3.2.3 FERRAMENTAS DE AUDITORIA DE SEGURANÇA

A segurança é um dos aspectos a ter em conta na gestão de redes WBL. Segundo [Loo,2008], a segurança nunca será perfeita enquanto os *hackers* encontrarem novos métodos de quebrar os sistemas. É por isso importante monitorizar a rede, auditar e encontrar prováveis pontos de falhas e vulnerabilidades, minimizando as possíveis quebras do sistema.

Existem várias ferramentas de segurança *opensource* que podem ser utilizadas para ajudar a tornar as redes wireless mais seguras. Como o objecto deste trabalho é a gestão, importa

⁵³ <http://nocat.net>

⁵⁴ <http://dev.wifidog.org>

⁵⁵ <http://coova.org>

referir aquelas que contenham aspectos de gestão da segurança. Na tabela 4 pode observar-se alguns exemplos.

Aircrack	http://www.wirelessdefence.org/Contents/Aircrack_aircrack.htm	Contem uma série de ferramentas que permite entre outros, fazer auditorias na rede wireless e testes de intrusão.
AirSnare	http://home.comcast.net/~jay.deboer/airsnare/	Permite detectar a intrusão de AP's na rede.
Airsnarf	http://airsnarf.shmoo.com/	Software de AP com um utilitário para demonstrar como é que se consegue captar informação de contas de acesso (username e password) de hotspot's públicos.
Karma	http://theta44.org/karma/	Conjunto de ferramentas para avaliar a segurança em várias camadas de clientes wireless.
LEAF	http://leaf.sourceforge.net/	Sistema Linux embebido, personalizável, podendo ser utilizado em diversas topologias de rede. Tem funcionalidades de hotspot gateway, router, firewall, e ainda wireless access point.
Mognet	http://node99.org/projects/mognet/	Sniffer baseado em Java distribuído segundo a licença GPL. Permite capturar em tempo real todo o tráfego 802.11.
Sentry Firewall CD-ROM	http://www.sentryfirewall.com/	CD de arranque baseado em Linux com um sistema de firewall e IDS (<i>Intrusion Detection System</i>)
Snort-Wireless	http://snort-wireless.org/	Software IDS para detecção de APs intrusos.

Tabela 4: Soluções *opensource* de segurança

3.2.4 INVENTÁRIO, MONITORIZAÇÃO E DIAGNÓSTICO

Comparado com a rede LAN, a gestão e monitorização de redes wireless, experimentam desafios adicionais, pois o desempenho é fortemente dependente de características físicas variáveis e imprevisível do meio físico (i.e. do ar) [Paquereau et al,2005]. É por isso de importância vital que exista na rede um sistema que permita ter conhecimento dos eventos

ocorridos na rede, que possam ser avaliados e produzir informações para a uma gestão mais eficiente.

Existem várias ferramentas *opensource* que fornecem serviços como o inventário, monitorização e diagnóstico, que podem ser utilizadas quer para as redes LAN quer para as redes wireless. Na tabela 5 pode-se observar as mais comuns.

Airfart	http://airfart.sourceforge.net	Ferramenta wireless para detecção de rede wireless, calculando a força do sinal e mostrando-a em informação de modo a permitir uma interpretação fácil.
Airodump	http://wirelessdefence.org/Contents/Aircrack_airodump.htm	Ferramenta para capturar tráfego wireless 802.11.
Airtraf	http://airtraf.sourceforge.net	Captura tráfego wireless e organiza-o para que a leitura do mesmo seja simples.
AP Radar	http://apradar.sourceforge.net	É uma ferramenta para Linux, que graficamente monitoriza a rede e a disponibiliza ao utilizador.
Bsd-airtools	http://www.freshports.org/net-mgmt/bsd-airtools	Pacote de ferramentas que permite obter várias informações para uma auditoria completa à rede.
Cacti	http://www.cacti.net	É uma solução de rede concebida para aproveitar as potencialidades dos dados armazenados pelo RRDTool, colocando-os graficamente legíveis.
Centreon	http://www.centreon.com	<i>Front-end</i> do Nagios, que lhe adiciona funcionalidades de gestão.
CUWiN	http://www.cuwin.net	É um software desenvolvido por uma comunidade nos EUA chamada Champaign-Urbana, onde os próprios utilizadores instalam e fazem a gestão dos AP's.
GroundWork	http://www.groundworkopensource.com	Ferramenta constituída por uma componente <i>opensource</i> capaz de integrar outras ferramentas (Cacti, Nagios, MRTG, RRDTools, Nedi, Ganglia).
Hyperic HQ	http://www.hyperic.com	Suite de ferramentas de monitorização, inventário e gestão de equipamentos e serviços.

Iperf	http://dast.nlanr.net/Projects/Iperf	Permite medir diversos parâmetros da rede, mas tem um funcionamento contrário aos demais, pois injecta informação na rede, permitindo efectuar cálculos para obter, por exemplo, a latência e o débito.
Kismet	http://www.kismetwireless.net	Pacote de ferramentas que actuam ao nível da camada 2 do modelo OSI, para detectar redes wireless, com <i>sniffer</i> e detecção de intrusão. Consegue operar com todas as placas que suportem RFMON (Radio Frequency Monitoring) e consegue captar tráfego 802.11a/b/g.
Mrt	http://www.bitwizard.nl/mtr	Combina as funcionalidades dos comandos “traceroute” e “ping” num único programa de diagnóstico da rede.
MRTG	http://oss.oetiker.ch/mrtg	Ferramenta para monitorização do tráfego gerado na rede.
Nagios	http://www.nagios.org	Software de monitorização de rede, quer de equipamentos quer de serviços.
Netstumbler	http://www.netstumbler.com	Ferramenta gratuita para Windows que fornece várias informações sobre a rede wireless, tais como: canais utilizados, sinal da rede, congestionamento e interferências, verificação da existência de AP's não autorizados, entre outros.
Ntop	http://www.ntop.org	Ntop é uma ferramenta de monitorização de tráfego, que mostra a utilização da rede, similar ao comando Unix <i>top</i> .
Opennms	http://www.opennms.org	Software de gestão de rede.
RRDTool	http://oss.oetiker.ch/rrdtool	É uma biblioteca que permite recolher e guardar informações baseadas em base de dados rotativas, criado por Tobias Oetiker sob a licença GNU/GPL. Armazena séries de dados numéricos sobre o estado da rede, mas pode ser empregue noutro tipo de informação como a temperatura e utilização do CPU (<i>Central Process Unit</i>).
SmokePing	http://oss.oetiker.ch/smokeping	Ferramenta que mede a latência da rede. Envia pacotes de testes para a rede, e mede o tempo que estes precisam para atravessar de um local até ao outro e depois novamente ao ponto de partida.

Wellenreiter	http://sourceforge.net/projects/wellenreiter	Ferramenta desenvolvida em Perl, que descobre, invade e audita/monitoriza redes wireless 802.11, descobrindo vulnerabilidades. Através desta ferramenta é possível obter informações tais como: canal de comunicação, o ESSID, MAC Address, se a rede utiliza ou não algum recurso de criptografia, o fabricante do AP, entre outras informações.
Wicrawl	http://midnightresearch.com/projects/wicrawl	Permite auditar APs existentes no espectro, extraindo informação importante para a gestão da rede.
Wifi-Owl's	http://www.wifi-owl.com	Software que permite monitorizar e gerar relatórios detalhados sobre as redes wireless, maioritariamente em questões de segurança.
Wifiscanner	http://wifiscanner.sourceforge.net	Ferramenta para descobrir nós da rede wireless, isto é, AP's e clientes.
Wifizoo	http://community.corest.com/~hochoa/wifizoo/index.html	Software que recolhe informação da rede de forma passiva.
Wavemon	http://freshmeat.net/projects/wavemon	Aplicação baseada em <i>ncurses</i> , para monitorizar dispositivos wireless. Permite obter informações como a qualidade do sinal, níveis de ruído, estatísticas de pacotes, configuração dos dispositivos, e parâmetros da rede.
WiFi Hopper	http://wifihopper.com	Software que combina funcionalidades de descoberta de rede, <i>site survey</i> , e gestão de ligações. Consegue facilmente detectar congestionamento de canais da rede wireless.
Wireless Access Point Utilites for Unix	http://ap-utils.polesye.net	Conjunto de utilidades para configurar e monitorizar APs sobre Unix utilizando SNMP e o protocolo tftp.
Wireshark	http://www.wireshark.org	Programa para monitorizar o tráfego da rede, analisando e dissecando os pacotes de dados.
Zennos Community	http://www.zenoss.com	Fornecer uma suite de software, para ajudar a monitorizar a infra-estrutura de rede. Possibilita a integração de processo de inventário, configuração, disponibilidade, performance e eventos.

Tabela 5: Soluções *opensource* de inventário, monitorização e diagnóstico

De referir que a maioria destas soluções podem ser instaladas sobre a licença GNU/GPL.

3.2.5 SERVIÇOS BASEADOS EM LOCALIZAÇÃO

Os Serviços Baseados em Localização possuem características que resultam num desafio complexo do ponto de vista tecnológico.

É possível determinar a localização de um equipamento wireless de duas formas: utilizando uma infra-estrutura específica para posicionamento com por exemplo o GPS (*Global Positioning System*), ou modificando de alguma forma o sistema de comunicação utilizado. Na primeira hipótese, existem a desvantagem da necessidade de hardware e ainda o fraco desempenho do GPS no interior de edifícios.

Segundo [Lunde et al, 2006], existem duas metodologias principais para recolher medições de forma eficaz na tentativa de localizar através da rádio frequência as estações wireless: inserção de pacotes “sonda”, ou de forma passiva pela observação real de pacotes. Estas estratégias são denominadas por medidas activas e medidas passivas respectivamente. As medidas podem ser efectuadas em diferentes camadas de protocolos: dados, rede, transporte e aplicações.

Em [Prasithsangaree, et al 2002], os autores referem três métodos básicos para determinar a localização de utilizadores, através de uma infra-estrutura de wireless. O primeiro é por triangulação, que necessita de pelo menos três estimativas distintas da distância entre o dispositivo wireless e algum local fixo conhecido.

O segundo método utiliza a direcção ou ângulo de chegada do sinal AoA (*Angle of Arrival*) medidos de pelo menos dois pontos fixos distintos. Basicamente, uma antena direccionada é ligada ao receptor e a área em torno do receptor é testada para medir e marcar a partir de que direcção o sinal recebido é mais forte. Em seguida, o receptor é movido de lugar para uma segunda posição, e o mesmo procedimento de pesquisa pela direcção com melhor sinal é realizado. A localização da fonte transmissora é então descoberta através de geometria básica, onde o encontro das rectas que seguem as duas direcções medidas é a posição do transmissor. Este método pode ser observado na Figura 17.

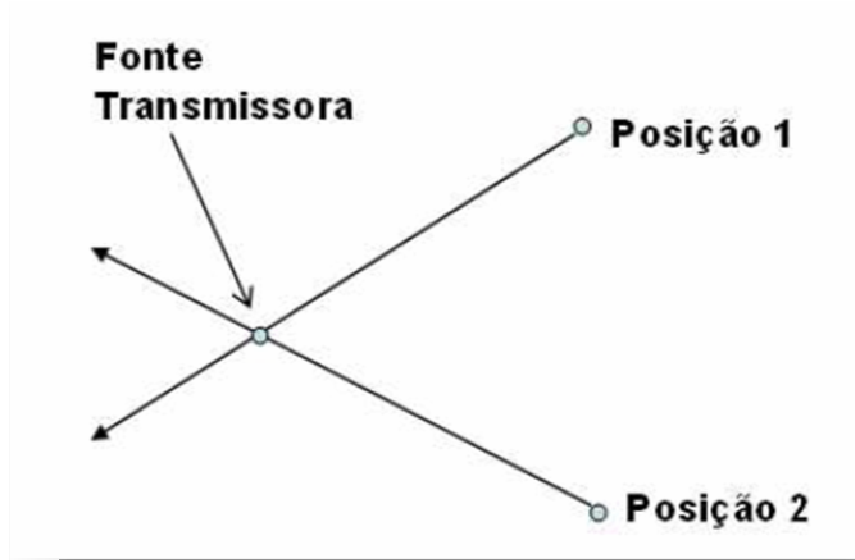


Figura 17: Estimativa de posição de um transmissor a partir da medição do ângulo de chegada do sinal de duas posições distintas.

O terceiro método é a utilização de esquemas de mapeamento, também conhecidos como esquemas de calibragem, ou *location fingerprinting*, ou ainda *site profiling*. Este método baseia-se no princípio de amostrar determinadas características do sinal de rádio, dependentes da localização do ponto onde tais características são aferidas. Estas características são diferentes para cada local medido, funcionando como uma impressão digital. Estas “impressões digitais” são armazenadas numa base de dados e comparadas posteriormente com o sinal amostrado de um dispositivo wireless que se deseja localizar.

Existem alguns projectos *opensource* que contribuem para minimizar a complexidade desta função. Na Tabela 6 apresentam-se e descrevem-se alguns desses projectos.

Wi-viz	http://devices.natetrue.com/wi-viz	Ferramenta que pode ser instalada num router wireless da Linksys WRT54G ou compatível, com um firmware Linux como o OpenWRT, permitindo visualizar via web os nós da rede wireless e alguma informação.
Knsgem	http://www.rjpi.com/knsgem.htm	Converte os <i>logs</i> resultantes dos <i>surveys</i> efectuados pelo NetSumbler, Kismet e WifiHopper, em códigos de cores e coloca-os

		em mapas 3D, mostrando o resultado no Google Earth.
Musatcha Advanced WiFi Mapping Engine	http://www5.musatcha.com/musatcha/computers/software/wifi/mapping/index.htm	Software que permite colocar num mapa os nós da rede wireless.
Gpsd	http://gpsd.berlios.de	Gpsd é um <i>daemon</i> que monitoriza equipamentos GPS colocados em computadores através da porta <i>serie</i> ou USB, possibilitando a visualização de informação como a localização, percurso e velocidade, questionando a porta TCP 2947 do computador.
CampusMapper	http://geoserver.itc.nl/campusmapper	Ferramenta interactiva de mapas. Desenvolvido pela Universidade de Twente na Suíça. Utilizando o MySQL, Tomcat and SVG, consegue mostrar em mapas a localização de dispositivos.
StumbVerter	http://www.sonar-security.com/sv.html	É uma aplicação que permite importar informações do Network Stumbler, por exemplo, para o Microsoft MapPoint 2004.
AiroMap	http://www.divideconcept.net/airosuite	Software para PocketPC, que associado a um GPS, consegue registar as localizações das detecções de wireless que faz.
Herecast	http://www.herecast.com	É uma infra-estrutura aberta para LBS utilizando dispositivos wireless. Basicamente, consegue informar a localização do dispositivo num mapa. Trabalha sobre as plataformas Windows CE e XP/Vista.
MagicMap	http://www2.informatik.hu-berlin.de/rok/MagicMap	É um sistema para determinação cooperativa de localização de dispositivos WLAN.
OpenGTS	http://www.opengts.org	OpenGTS (<i>Open GPS Tracking System</i>) foi o primeiro projecto <i>opensource</i> desenhado especificamente para fornecer um sistema <i>web-based</i> de serviços de rasto GPS para veículos.
WifiDog	http://dev.wifidog.org	Solução integrada de portal captativo (Linux), que utiliza o método da triangulação para localizar os dispositivos wireless.

Tabela 6: Projectos *opensource* relacionados com serviços de localização wireless

3.2.6 LIVE CD'S

Existem ainda alguns projectos *opensource* que disponibilizam pacotes de ferramentas para fornecer serviços wireless, na forma de Live CD's. Um Live CD é um CD que contém um sistema operativo (GNU/Linux, BSD ou outro) que não precisa ser instalado no disco do utilizador uma vez que o sistema operativo é executado directamente a partir do CD e da memória RAM. A maioria dessas distribuições também permitem que se instale o sistema operativo no disco com as mesmas configurações do sistema executado no CD, caso o utilizador o deseje.

Como exemplo de alguns projectos tem-se:

- Linux LiveCD Router⁵⁶
- Public IP Zone CD⁵⁷
- Zeroshell⁵⁸

O projecto Linux LiveCD Router permite partilhar uma ligação à internet em Banda Larga de forma segura e optimizada utilizando wireless. Não requer instalação, mas precisa de um computador dedicado onde se possa fazer *boot* através do CD.

O Public IP ZoneCD é um *LiveCD*, que por isso mesmo não é instalado no disco do computador. Contém uma colecção de software baseado na licença GNU/Linux, pré-configurado para trabalhar como um Wifi *gateway*. As funcionalidades mais interessantes são: autenticação/registo do utilizador, redireccionamento para uma *homepage*, controlo de largura de banda, estatísticas de downloads, filtragem de conteúdo, *firewall*, entre outras. Este projecto já foi descontinuado.

O projecto Zeroshell é uma pequena aplicação para servidores e dispositivos embebidos, que disponibiliza o acesso à rede através do fornecimento dos diversos serviços de rede necessários. Está disponível quer num LiveCD, quer numa imagem *Compact Flash* (*firmware*), que pode ser facilmente configurado e administrado através de um *browser*.

⁵⁶ <http://www.wifi.com.ar/english/cdrouter>

⁵⁷ <http://www.publicip.net>

⁵⁸ <http://www.publicip.net>

3.3 SOLUÇÕES COMERCIAIS

As soluções comerciais mitigam a desvantagem das ferramentas *opensource*, porque ao contrário das soluções *opensource*, existem soluções comerciais mais completas para a gestão de redes WBL.

No mercado existem várias soluções de gestão de redes wireless, normalmente mais direccionadas para as redes *indoor*. São vários fabricantes que têm a sua solução de gestão de redes wireless. Neste capítulo procura apresentar-se resumidamente as soluções mais relevantes existentes no mercado. Obviamente que existe uma panóplia de soluções, no entanto, como a lista seria interminável, optou por realizar-se o estudo recorrendo a uma amostra, até porque o objectivo, é demonstrar a diferença de funcionalidades relativamente às soluções *opensource*.

As soluções comerciais estudadas foram as seguintes:

- AirWave Wireless Management Suite⁵⁹ (Airwave);
- Colubris Network Management System⁶⁰ (Colubris);
- AirMagnet Enterprise⁶¹ (AirMagnet);
- Avalanche Mobilite Center⁶² (Wavelink);
- Cisco Wireless Control System⁶³ (Cisco);
- WifiManager⁶⁴ (ManageEngine)
- ProCurve Manager Plus⁶⁵ (HP)

Nos próximos pontos descrevem-se sumariamente estas soluções.

3.3.1 AIRWAVE WIRELESS MANAGEMENT SUITE

A solução da *AirWave*, o *Wireless Management Suite*, é uma solução abrangente de gestão de redes wireless, concebida para utilização de todo o departamento de IT (*Information Technology*) de uma organização. Reduz custos e melhora a segurança em tempo real, através

⁵⁹ <http://www.airwave.com>

⁶⁰ <http://www.colubris.com/global-wireless-network-management/network-management-system.asp>

⁶¹ <http://www.airmagnet.com/products/enterprise>

⁶² <http://www.wavelink.com/products/avmc.aspx>

⁶³ <http://www.cisco.com/en/US/products/ps6305/index.html>

⁶⁴ <http://manageengine.adventnet.com/products/wifi-manager/index.html>

⁶⁵ http://www.hp.com/rnd/products/management/ProCurve_Manager_Plus/overview.htm

de um acompanhamento ao nível do utilizador, monitorização de acções, relatórios de descoberta de rede, configuração de gestão, auditorias automáticas, detecção de APs indesejados, entre outros. O software suporta múltiplas arquitecturas de redes wireless ("*thin*" e "*fat*" APs, *mesh*, ponto a ponto, WiMax, entre outros) assim como equipamentos de vários fabricantes (Aruba, Cisco, Symbol, HP ProCurve, Meru, Trapezze, Avaya, Proxim, Tropos, Colubris, etc...).

3.3.2 COLUBRIS NETWORK MANAGEMENT SYSTEM

A Colubris tem uma solução denominada de NMS (*Network Management System*), tendo como funções principais: a centralização de todas as configurações; monitorização e performance em tempo real; diagnóstico (*troubleshooting*); descoberta automática de equipamentos; gestão do *firmware*; detecção de APs indesejados; *reporting*.

3.3.3 AIRMAGNET ENTERPRISE

A solução da AirMagnet designada de *AirMagnet Enterprise*, fornece uma solução simples e escalável que permite a qualquer organização monitorizar de forma pró-activa todo o tipo de “ameaças” wireless, forçando a aplicação de políticas de segurança, prevenindo problemas de performance e auditando com regularidade o serviço fornecido. É uma solução de gestão e monitorização WLAN, que oferece uma visão completa e um controlo total da RF, permitindo à organização na sua gestão de redes wireless, assegurar os mesmos níveis de segurança e de fiabilidade que nas redes LAN.

3.3.4 WAVELINK AVALANCHE MC

A solução de gestão de redes wireless da empresa Wavelink, denominada por *Avalanche MC*, é uma solução que fornece total visibilidade e controlo de todos os dispositivos wireless, numa consola central. Configura, instala, analisa, actualiza, planeia, de uma forma simples através dessa consola. Suporta equipamentos de diversos fabricantes: Avaya, Cisco, Dell, HP, Proxim, Symbol and Systimax.

3.3.5 CISCO WIRELESS CONTROL SYSTEM

A solução da Cisco para gestão de redes wireless denomina-se por WCS (*Cisco Wireless Control System*). O WCS é a plataforma para o planeamento, configuração e gestão de redes wireless. O Cisco WCS permite aos administradores de sistemas, desenhar, controlar e

monitorizar a redes wireless da organização, de uma forma centralizada, simplificando operações e reduzindo o *total cost of ownership* (estimativa financeira para ajudar a avaliar os custos indirectos e directos, normalmente associados a software ou hardware).

3.3.6 WIFI MANAGER

O *WiFi Manager* é uma solução de gestão centralizada de redes wireless da empresa norte americana *ManageEngine*. Permite monitorizar dispositivos wireless, efectuar configurações “one-click”, efectuar a gestão do *firmware* do AP, efectuar gestão de segurança e gerar uma variedade de relatórios que mitiga a complexidade da gestão de redes wireless. Detecta a maior parte das ameaças de segurança, tais como: intrusão, ataques indesejados, ataques DoS e vulnerabilidades.

3.3.7 HP PROCURVE MANAGER PLUS

O *ProCurve Manager Plus* é um software da HP que permite aos administradores de rede configurar, actualizar, monitorizar e resolver problemas dos dispositivos deste fabricante, centralmente e de uma forma fácil.

3.4 COMPARAÇÃO DE SOLUÇÕES

Após o levantamento dos dois grandes grupos de soluções, *opensource* e comerciais, importa efectuar um estudo comparativo sobre as funcionalidades que ambos os grupos suportam ou não. Esta comparação será efectuada a nível de aplicação. Para isso recuperamos a Tabela 7 do ponto 3.1 – Funcionalidades de Gestão de redes WBL.

Acesso baseado por perfil de utilizador	Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Actualizações de firmware	Airwave, Colubris, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Definição da potência de transmissão e escolha de canal	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Sveasoft, HyperWrt	Comercial/Opensource

Agendamento para instalação de firmware	Airwave, Colubris, AvaranceMC, WifiManager, Procurve Manager Plus	Comercial
Alarmes	Airwave, Colubris, AirMagnet, AvaranceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Alerta de configurações obsoletas	Airwave, Cisco WCS, WifiManager	Comercial
Auditorias	Airwave, Colubris, AirMagnet, AvaranceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Aircrack, Wicrawl, Bsd-airtools, Wellenreiter,	Comercial/Opensource
Balanceamento de carga	Airwave, Colubris, AirMagnet, Cisco WCS, WifiManager, Procurve Manager Plus, Mikrotik, m0n0wall	Comercial/Opensource
Billing/Accounting	Mikrotik	Comercial/Opensource
Captura de pacotes na rede	Airwave, Colubris, AirMagnet, AvaranceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Mognet, Aircrack, Airodump, Kismet, Airtf, Wifizoo	Comercial/Opensource
Consola linha de comandos	Airwave, Colubris, Procurve Manager Plus, HyperWrt, Mikrotik	Comercial/Opensource
Configurações modelo	Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Descoberta automática de equipamentos na rede	Airwave, Colubris, AirMagnet, AvaranceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Aircrack, Wifi Hopper, Nagios, Hyperic HQ, Opennms, Zennos, GroundWork	Comercial/Opensource
Detecção de ataques DoS	AirMagnet, Cisco WCS, WifiManager	Comercial
Detecção de configurações erradas	Airwave, Colubris, Procurve Manager Plus	Comercial
Detecção de intrusão	Airwave, Colubris, AirMagnet, AvaranceMC, Cisco WCS, WifiManager, Sentry Firewall CD-ROM, AirSnare, Snort-Wireless, Aircrack	Comercial/Opensource
Diagnóstico e correlação de erros	Airwave, Colubris, Procurve Manager Plus	Comercial

EAP	Airwave, Colubris, Cisco WCS, DD-WRT,	Comercial/Opensource
Envio de relatórios por mail	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Firewall	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Sveasoft, OpenWrt, DD-WRT, HyperWrt, Mikrotik	Comercial/Opensource
Força a aplicação de políticas de segurança	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Gestão baseada em grupos	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Gestão centralizada de configurações	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Gestão de largura de banda	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Mikrotik, Chillispot, Wifidog, Coova, Public IP Zone, ZeroShell	Comercial/Opensource
Gestão de utilizadores	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Sveasoft, OpenWRT, DD-WRT, HyperWRT, Mikrotik, Chillispot, Wifidog, Coova, Public IP Zone, ZeroShell, Airsnarf	Comercial/Opensource
Informação Gráfica	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Mikrotik, Chillispot, Netstumbler, MRTG, Ntop, Cacti, Nagios, Hyperic HQ, Zennos, Ap Radar, Wavemon, Kismet	Comercial/Opensource
Helpdesk	Airwave	Comercial
IEEE 802.1x	Airwave, Colubris, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Mikrotik,	Comercial/Opensource
Informação sobre as vulnerabilidades	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Weellenreiter, Kismet	Comercial
Interface Web	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Mikrotik, Sveasoft, OpenWrt, DD-WRT, HyperWRT, Chillispot, Nocat, Coova,	Comercial/Opensource

	Wifidog, Nagios, Cacti, Goundwork, Hyperic HQ, MRTG	
Listas de acessos MAC	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager	Comercial
Log's dos eventos na rede	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Mapa da rede	Airwave, Colubris, AvalanceMC, Cisco WCS, Procurve Manager Plus	Comercial
Medição de interferências (ruído)	AirMagnet ,Cisco WCS, Procurve Manager Plus, Wifi Hoper	Comercial/Opensource
Monitorização da potência e qualidade de sinal RF	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Netstumbler, Sveasoft, HyperWRT, Mikrotik, Kimet, AirFart, Wavemon, StumbVerter	Comercial/Opensource
Monitorização de eventos de roaming	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS	Comercial
Monitorização do tipo de tráfego	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Monitorização em tempo real (Dashboard)	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Optimização das configurações RF	Airwave, Cisco WCS	Comercial
Pesquisa de dispositivos	Cisco WCS, Procurve Manager Plus	Comercial
Pesquisa de informação	Airwave, Cisco WCS	Comercial
Planeamento	Cisco WCS, Procurve Manager Plus	Comercial
Portal Captativo/Hotspot Gateway	Chillispot, Nocat, Wifidog, Coova, Sveasoft, DD-WRT, Mikrotik	Opensource
Promove a rotação automática de chaves privadas	Airwave, AvalanceMC, Cisco WCS	Comercial

Proxy	HyperWrt, Mikrotik	Opensource
Quality of Service (QoS)	Sveasoft, DD-WRT, HyperWrt, Mikrotik, Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial/Opensource
Relatórios de Erros de utilização	Airwave, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Relatórios de utilização da rede	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Relatórios de utilização de canais	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Relatórios por elemento	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Relatórios por períodos de tempo	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
Serviços de localização	Airwave, Colubris, AvalanceMC, Cisco WCS, Procurve Manager Plus	Comercial
Servidor de RADIUS	Airwave, Colubris, AvalanceMC, Cisco WCS	Comercial
Servidor DHCP	OpenWrt, DD-WRT, Mikrotik	Opensource
Site Survey	DD-WRT, HyperWrt, Knsgem, Cisco WCS, Procurve Manager Plus	Comercial/Opensource
SNMP	DD-WRT, m0n0wall, Mikrotik, Nagios, Groundwork, Opennms, Zenoss, MRTG, Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial/Opensource
SSH	Sveasoft, DD-WRT, Mikrotik	Opensource
Suporta equipamentos de diferentes fabricantes	Nagios, Groundwork, Opennms, Zenoss, MRTG, Airwave, AirMagnet, Cisco WCS, WifiManager	Comercial/Opensource
Suporte para VLAN	Airwave, Colubris, AirMagnet, AvalanceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial

Visualização em mapa de área coberta RF	Airwave, Colubris, Cisco WCS, Procurve Manager Plus	Comercial
Visualização em mapa do AP intruso	Airwave, AirMagnet, Cisco WCS	Comercial
VoWLAN	Cisco WCS	Comercial
VPN	Airwave, Colubris, AirMagnet, AvaranceMC, Cisco WCS, DD-WRT, m0n0wall	Comercial/Opensource
WBL Performance	Airwave, Colubris, AirMagnet, AvaranceMC, Cisco WCS, WifiManager, Procurve Manager Plus	Comercial
WDS	Sveasoft, DD-WRT, HyperWrt, Mikrotik	Opensource
WEP	Airwave, Colubris, AirMagnet, AvaranceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Mikrotik, DD-WRT	Comercial/Opensource
WPA	Airwave, Colubris, AirMagnet, AvaranceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Mikrotik, DD-WRT	Comercial/Opensource
WPA2	Airwave, Colubris, AirMagnet, AvaranceMC, Cisco WCS, WifiManager, Procurve Manager Plus, Mikrotik, DD-WRT	Comercial/Opensource

Tabela 7: Comparação de funcionalidades entre soluções *Opensource* e soluções Comerciais

Da Tabela 7 podem extrair-se várias informações. Para poder expressá-las melhor, apresentam-se dois gráficos que ajudam a clarificar as diferenças entre as duas grandes categorias de software livre e comercial.

Na Figura 18 pode observar-se a distribuição percentual em termos ocorrências na Tabela 7 de tipo de software, ou seja, pode concluir-se que 56% do das funcionalidades identificadas, só são garantidas por soluções comerciais. Enquanto 37% são garantidas por soluções comerciais e *opensource*, apenas 7% são garantidas por soluções de software livre.

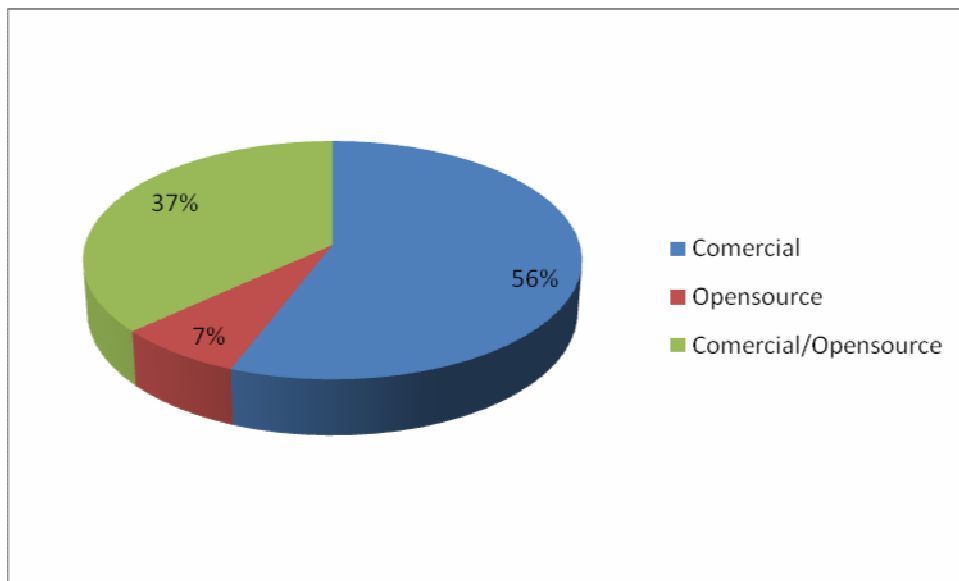


Figura 18: Distribuição das funcionalidades de acordo com o tipo de software

Analisando as dez soluções mais mencionadas na Tabela 7, observa-se na Figura 19, que as sete soluções comerciais estudadas, aparecem nas sete primeiras posições, o que evidencia a riqueza de funcionalidades destas soluções, e as lacunas das soluções *opensource*.

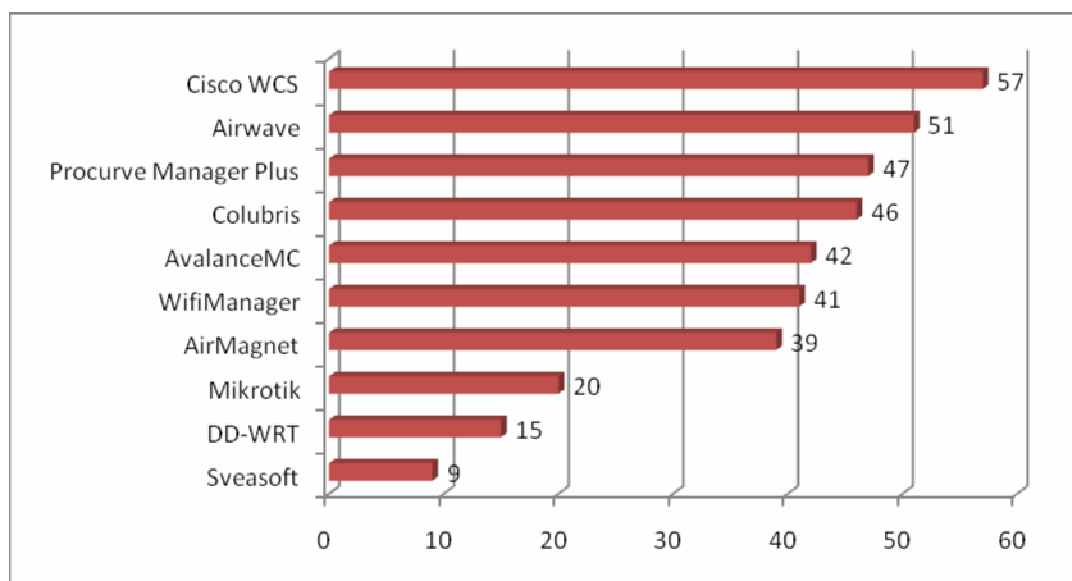


Figura 19: Soluções com mais ocorrências na Tabela 7

3.4.1 RESUMO

Existem várias soluções *opensource* capazes de responder a várias funcionalidades da gestão de redes WBL, no entanto, estão “desgarradas”, sem interligação entre si.

Já as soluções de gestão wireless comerciais exibem a função da gestão de uma forma mais abrangente, conjugando todos os aspectos da gestão numa única plataforma centralizada.

Com a definição das funcionalidades consideradas mais importantes para a obtenção de uma gestão de redes WBL completa, foi possível identificar quais as soluções que melhor respondem aos requisitos identificados. Na análise efectuada, conclui-se que as soluções comerciais já apresentam níveis bastante aceitáveis para a gestão das redes WBL, mas no que concerne às soluções *opensource*, tal já não acontece. Existem diversas soluções, mas a sua utilização cumpre apenas uma funcionalidade muito específica, sem atender ao conceito de globalidade e centralidade.

Assim, está encontrada a justificação para a necessidade de se desenvolver/implementar uma solução, que corresponda aos requisitos identificados. Para isso, é fundamental definir um modelo, que possa servir de base para se conseguir uma solução completa de gestão de redes WBL.

4. MODELO DE GESTÃO DE REDES WBL

Após a descrição e identificação das funcionalidades de gestão de redes wireless, apresenta-se neste capítulo uma proposta de arquitectura para aquilo que se considera uma gestão completa de redes WBL.

O modelo proposto baseia-se na identificação de um conjunto de características e funcionalidades, que uma possível solução deverá contemplar. Verificado que está a inexistência de uma solução economicamente vantajosa, considera-se como mais indicado o recurso às ferramentas *opensource* para a sua implementação.

Começa-se por identificar os princípios técnicos da gestão de redes WBL e a seguir define-se o modelo representado na arquitectura e funcionalidades. As funcionalidades são agrupadas por tipos de funções que a solução deve cumprir.

4.1 METODOLOGIA PARA IMPLEMENTAÇÃO DE GESTÃO DE REDES WBL

A monitorização de diferentes aspectos de um sistema de telecomunicações é um requisito básico para assegurar a prestação de um bom serviço. Entender onde está a informação valiosa e ter a capacidade de recolher a informação correcta, é meio caminho para tomar as decisões mais acertadas. No entanto, só o facto de se ser detentor dos dados, não indica que os problemas possam ser resolvidos. Os dados não significam informação e ter a informação não significa necessariamente ter conhecimento.

Uma boa gestão de redes deve ser capaz de:

- Adquirir/colher os dados necessários do sistema;
- Processar e apresentar os dados, fornecendo diferentes níveis de detalhe dos dados adquiridos;
- Tomar decisões automáticas se necessário;

Paralelamente a uma aproximação centralizada, importa implementar uma gestão de redes, tendo como base uma definição de objectivos para essa gestão. As decisões não podem ser tomadas apenas tendo em conta os princípios técnicos, mas também os objectivos e prioridades que são definidas.

Assim, quando se pretende implementar uma solução de gestão de redes wireless, deve primeiro definir-se um objectivo, identificar quais são os princípios técnicos a utilizar, quais as ferramentas para o alcançar, para que seja possível tomar uma decisão. Na Figura 20, pode observar-se esta metodologia num ciclo que se repete.



Figura 20: Metodologia de monitorização de redes wireless

Nesta metodologia a função de gestão de redes wireless não se focaliza inicialmente nas ferramentas, mas sim nos objectivos. Após esta definição, é necessário entender os princípios técnicos que estão por detrás das ferramentas, para que estas possam ser correctamente escolhidas para cumprir o objectivo definido, uma vez que, entendendo os princípios técnicos, consegue encontrar-se mais facilmente as melhores ferramentas.

Para demonstrar esta metodologia de monitorização, observe-se um exemplo em que se definem dois objectivos:

1. Fornecer melhor qualidade de serviços para o VoIP (*Voice over Internet Protocol*);
2. Gestão de serviços e crescimento da rede.

As próximas tabelas, mostram como estes dois objectivos utilizam princípios técnicos e como cada um destes objectivos necessita de recolher informação de cada camada do modelo OSI, da rede wireless.

Aplicação	
Transporte	Traffic shaping (Princípios de Queueing) Traffic accounting (SNMP)
Rede	Traffic shaping (Princípios de Queueing) Traffic accounting (SNMP)
Controlo de Acesso ao Meio	Recolha de Dados (SNMP) Redução de <i>wireless latency</i>

Tabela 8: Princípios técnicos e a sua correspondência com as o modelo OSI

Na tabela anterior, podem ser observados os princípios técnicos e sua correspondência com as camadas do modelo OSI, que podem ser utilizadas para alcançar uma melhor qualidade de serviço para sistemas VOIP.

Na Tabela 9 podem ser observados os princípios técnicos a ter em conta para permitir um crescimento da rede e gerir os serviços.

Aplicação	Virús/Spam, SQL
Transporte	Recolha de estatísticas TCP/UDP, balanceamento de firewall
Rede	Recolha de estatísticas da camada IP, Princípios de encaminhamento
Controlo de Acesso ao Meio	Recolha de dados camada 2 (SNMP)

Tabela 9: Princípios técnicos e a sua correspondência com o modelo OSI

A falha na optimização de alguma camada do protocolo irá afectar toda a performance da rede. Por exemplo, se existir um elevado número de pacotes corrompidos na rede wireless, irá ter impacto em toda a performance do protocolo TCP e originará uma elevada latência que o utilizador irá percepcionar, se estiver a utilizar uma aplicação em tempo real.

A complexidade não está só em entender cada camada do modelo OSI, mas sim, em inter-relacioná-las entre si.

4.2 PRINCÍPIOS TÉCNICOS E FERRAMENTAS

Importa então conhecer alguns exemplos de princípios técnicos, que se devem ter em consideração, para a escolha da ferramenta correcta, ou até em alguns casos, partir para o desenvolvimento de novas ferramentas. Para entender melhor a metodologia aqui descrita, enumeram-se os seguintes princípios técnicos para a gestão de redes wireless: *SNMP*, *Traffic Accounting*, *Traffic Shaping*, *Bayesian Filters*, Assinaturas de antivírus.

O *SNMP* (*Simple Network Protocol*) é um protocolo de gestão específico para a gestão de redes, e que permite através das suas informações, melhorar o desempenho das redes, encontrar eventuais problemas, entre outros. Existem três versões do protocolo *SNMP*, sendo que a primeira (*SNMPv1*) foi desenvolvida pelo IETF em 1993. O *SNMPv3* é a versão mais actual deste protocolo, no entanto muitos dispositivos wireless apenas suportam as versões anteriores. É um protocolo da camada de aplicação do modelo OSI, para troca de informação, onde cada dispositivo que o implementa, tem uma base de dados denominada por MIB. Esta base de dados, contem a informação que vai sendo recolhida durante a operação do dispositivo. A grande vantagem do *SNMP* é a interoperabilidade que é garantida, independentemente do equipamento.

Quando se deseja implementar o protocolo *SNMP* para efectuar a gestão de rede wireless, é importante ter em conta os seguintes aspectos:

- O *SNMP* também origina tráfego na rede;
- O *SNMPv1* não fornece encriptação;
- O *SNMP* consome recursos de CPU dos dispositivos;

O *Traffic Accounting* é um princípio técnico para monitorizar estatísticas de tráfego em redes de computadores. A informação recolhida por esta técnica é muito importante na tomada de decisões para organizar a rede, resolução de problemas e monitorização da actividade da rede em geral. A informação que o *Traffic Accounting* produz é a seguinte:

- Contagem de pacotes e bytes;
- Distribuição estatística por protocolos (tipo, tempos, %);
- Erros de *checksum* IP
- Descoberta de *hosts* activos

- Actividade dos dados trocados entre *hosts*

Existem duas formas de recolher informações com esta técnica, de forma activa e passiva. Na forma activa, consiste em activar o protocolo SNMP em todos os routers e bridges da rede. De forma passiva consiste em recolher informação em modo promíscuo, “escutando” os canais de comunicação.

Já relativamente ao *Traffic shaping*, este é um método de controlar o fluxo de tráfego de uma rede, de forma a otimizar e garantir alguma performance na rede, ou seja, é a prática de atribuir prioridades ao tráfego de dados. Saber manusear estas regras permite ajustar o comportamento da rede no que concerne:

1. Latência e gestão de congestionamento;
2. Gestão da largura de banda e equidade;

Outro princípio técnico que pode ser utilizado para a gestão de redes wireless é o designado *Bayesian Filters* (termo criado pelo matemático inglês Thomas Bayes), que consiste em criar sistemas de *anti-spam* para calcular a probabilidade de um e-mail conter *spam*. Este sistema consegue verificar todo o conteúdo de uma mensagem e classificá-la quanto à sua boa ou má proveniência. Se este tipo de tráfego for eliminado logo à entrada da rede, permitirá obter obviamente mais performance, uma vez que este tráfego é desnecessário e pode ser descartado.

Por último, a função dos sistemas de antivírus são comumente conhecidos por detectar, através de assinaturas aplicadas em algoritmos heurísticos, códigos maliciosos que possam eventualmente provocar danos na rede.

Para colocar estes princípios técnicos em prática podem enumerar-se um conjunto de ferramentas *opensource*. A título de exemplo, serão sumariamente detalhadas as seguintes ferramentas:

- Ferramentas de monitorização: Ntop⁶⁶ e MRTG⁶⁷
- Filtros Spam: SpamAssassin⁶⁸

⁶⁶ <http://www.ntop.org>

⁶⁷ <http://oss.oetiker.ch/mrtg>

⁶⁸ <http://spamassassin.apache.org>

- Software antivírus: Clam AV⁶⁹

Todos os fabricantes utilizam nos seus equipamentos, funcionalidades próprias para monitorizar a actividade dos mesmos, no entanto, se se desejar uma monitorização global e centralizada, será necessário utilizar um software específico. Uma das formas de se conseguir integrar as diferentes ferramentas de gestão de redes wireless num interface único, é utilizar o protocolo SNMP, numa ferramenta que integre todos os dados, utilizando ferramentas auxiliares, como é o exemplo do MRTG (*Multi Router Traffic Grapher*).

O MRTG é uma ferramenta *webbased* de gestão de redes, que permite monitorizar e visualizar a evolução de diversos parâmetros da rede. O MRTG utiliza o protocolo SNMP, e mostra diversas informações em forma de gráfico. Uma das funcionalidades mais utilizadas é a possibilidade para mostrar a largura de banda utilizada num equipamento, ou por um utilizador da rede, assim como mostrar em gráfico a potência e o ruído de sinal.

O Ntop é uma ferramenta multi-plataforma e *opensource*, que permite medir o tráfego e monitorizar a rede. Todas as funcionalidades do Ntop, estão acessíveis via interface Web. As funcionalidades mais comuns são:

- Medição de tráfego;
- Caracterização e monitorização do tráfego;
- Detecção de violações na rede (Exemplos: Portscan, Spoofing, Spyes, Trojan horses, Denial of Service (DoS));
- Optimização da rede e planeamento (Exemplo: desactivação de protocolos desnecessários na rede);

A detecção e bloqueio de spam numa rede pode tornar-se um pequeno pesadelo na gestão de uma rede wireless. Uma das ferramentas *opensource* mais conhecidas é o SpamAssassin, que de forma inteligente (porque utiliza diferentes métodos de filtragem), diminui as probabilidades da existência deste tipo de tráfego desnecessário.

Para exemplificar o princípio técnico antivírus, foi seleccionado o software *opensource* Clam Antivirus, capaz de detectar mais de 30000 vírus, *worms* e cavalos de tróia. Um computador com vírus pode desligar uma rede wireless numa questão de minutos. É importante

⁶⁹ <http://www.clamav.net>

implementar este tipo de ferramentas, de forma a evitar consequências nefastas para a rede e consequentemente ajudar a conseguir-se uma gestão otimizada.

Concluindo, a gestão de redes wireless, requer uma definição de objectivos como fornecedores de um serviço. Se não se souber o que se pretende no fornecimento desse serviço, dificilmente se conseguirá decidir o que se quer ou o que se precisa monitorizar. Se não se souber o que monitorizar, torna-se difícil encontrar as ferramentas que nos poderão ajudar a tomar decisões. Neste subcapítulo, há cinco noções que devem ficar registadas:

1. Recolher informação ou instalar ferramentas, pode não ser o suficiente para ter uma rede operacional. Se se tiver uma ideia clara do que se pretende, será fácil encontrar a ferramenta adequada;
2. Monitorizar o estado físico dos *links* rádio, não será suficiente, se a rede estiver cheia de actividade causada por vírus;
3. Quando se implementa um sistema de gestão de redes wireless, é importante ter em conta o aspecto da integração das diferentes ferramentas, de forma a tomar as melhores decisões;
4. Caso as ferramentas existentes não sejam suficientes para os objectivos definidos, deve considerar-se o desenvolvimento de uma ferramenta à medida;
5. Para monitorizar redes wireless, deve numa primeira fase definir-se os objectivos desejados como por exemplo, quais são as funcionalidades pretendidas. Após essa fase, devem identificar-se os princípios técnicos que possam responder a essas funcionalidades. A terceira fase é encontrar ou desenvolver as ferramentas que suportem os princípios técnicos. Findo este processo, é então possível tomar decisões para melhorar a rede wireless, se necessário.

4.3 OBJECTIVOS E FUNCIONALIDADES

No pressuposto do ponto anterior, explanam-se neste ponto os objectivos e as funcionalidades que o modelo de gestão de redes WBL para zonas rurais, deve preconizar.

A gestão de uma rede numa organização é constituída por vários intervenientes: serviço de *helpdesk*, responsável por dar suporte aos utilizadores; engenheiros de rede, com a responsabilidade de implementar e efectuar manutenção da rede; o grupo de auditoria e segurança, que terá a responsabilidade de monitorizar a rede e assegurar a segurança do

sistema; e por fim a gestão executiva, que terá a necessidade de recolher informação sobre a utilização da rede.

A solução deverá fornecer a informação completa para estes intervenientes, e deverá ter a possibilidade de gerir equipamentos de vários fabricantes.

Posto isto, observa-se na Figura 21 o cenário numa organização com alguma dimensão, onde se ilustra a existência de vários agentes do sistema e as suas necessidades. Cada agente tem a sua necessidade específica, por exemplo: o *helpdesk* de 1ª linha, não deverá ter as mesmas funcionalidades que o *helpdesk* de 2ª linha, que é normalmente desempenhado por engenheiros, por isso com necessidades mais avançadas. A gestão não necessita de ter acesso a estas ferramentas, mas deve ter a possibilidade de visualizar relatórios de utilização da rede, assim como de custos associados. Uma boa solução deve ainda ter uma política de acessos, baseados em perfis e ser independente do fabricante.

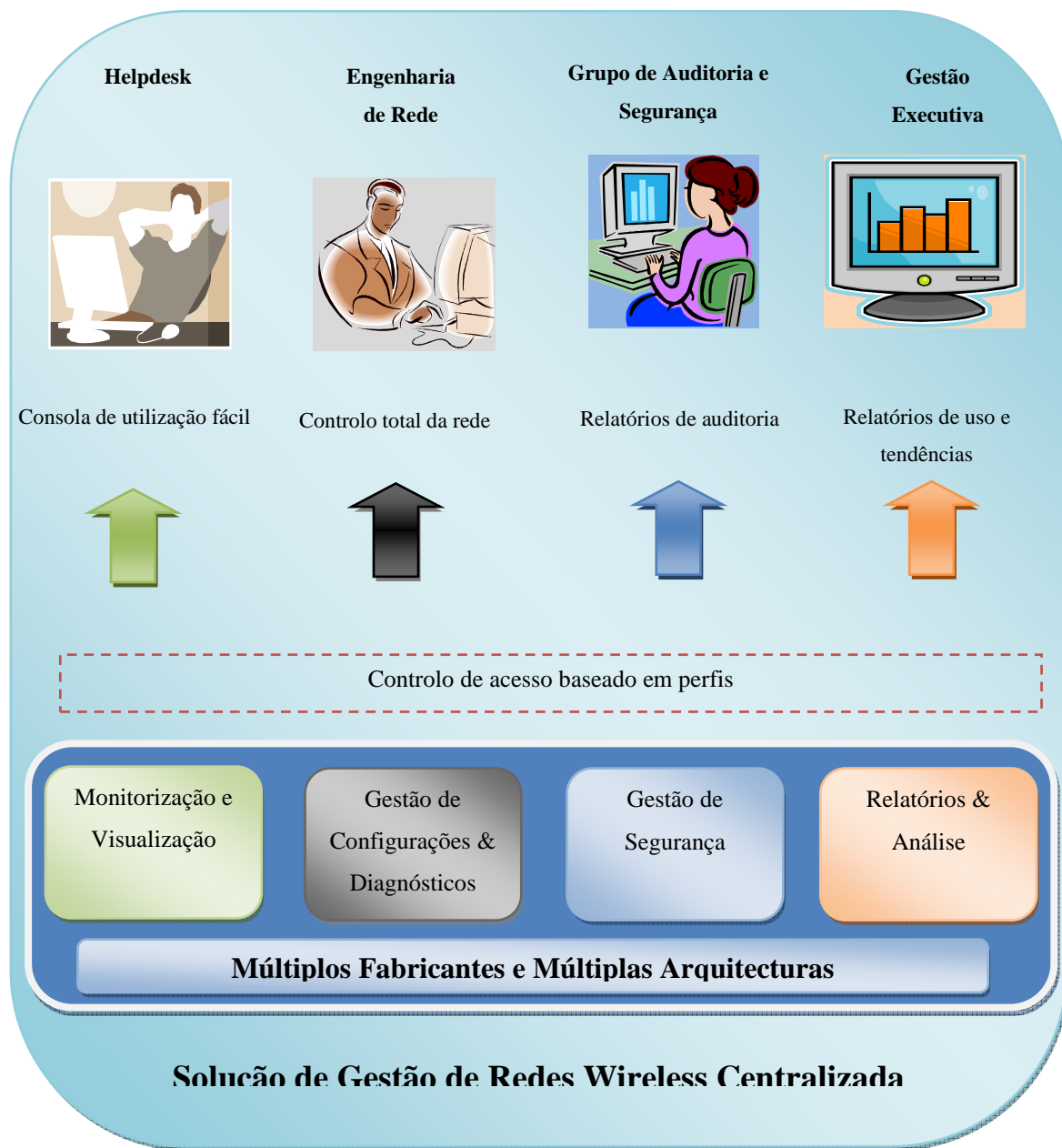


Figura 21: Arquitectura de gestão de redes WBL (visão de alto nível)

Após as pesquisas efectuadas e pelo exposto no presente documento, conclui-se que as funções da gestão de redes WBL podem dividir-se em três grandes categorias: Infra-estrutura, Segurança e Monitorização (Figura 22):



Figura 22: Funções da gestão de rede WBL

Pretende-se nos seguintes pontos, detalhar cada uma destas categorias.

4.3.1 CARACTERÍSTICAS GLOBAIS

Para além das categorias identificadas foram definidas características globais que o modelo deverá compreender. Uma boa solução deverá permitir robustez, flexibilidade e modularidade, pelo que se identificam as seguintes características:

- **Gestão Centralizada** – para as redes WBL, a existência de um ponto único de controlo afigura-se como escolha mais acertada. Note-se que nestes cenários (zonas rurais) não se espera a gestão de um grande volume de informação, nem muito complexa. Segundo [Yang et al,2001], esta é uma das principais razões para utilizar a aproximação centralizada em detrimento da aproximação distribuída. Para ambientes com grande volume de informação, a aproximação distribuída é mais vantajosa, devido à distribuição do processamento de informação. As arquitecturas de redes cuja gestão é centralizada, permitem simplificar dramaticamente a tarefa de gerir centenas de AP's individuais [DeBeasi,2007b].

- **Plataformas de gestão híbrida** - Integração da gestão de todos os elementos da rede, por exemplo a partir da mesma consola ter a possibilidade de gerir APs integrados num sistema de gestão centralizada (*lightweight APs*), assim como os APs autónomos, muito à semelhança do que acontece na arquitectura “Controladores WLAN”.
- **Planeamento** – Questões como: Quantos utilizadores utilizarão a rede? Que tecnologias serão usadas? Que tipo de aplicações? Estas questões deverão ter resposta na fase de planeamento. Estas respostas irão contribuindo para o aumento da probabilidade de sucesso de implementação.
- **Histórico de actividades na rede** – Deverá ser possível a qualquer momento obter informações sobre as actividades que estão a acontecer na rede.
- **Configurações baseadas em grupos** - Uma solução de gestão de redes WBL, deve suportar gestão por grupos para permitir implementar políticas de segurança nos vários segmentos da rede e perfis de utilização.
- **Helpdesk** - Uma solução de gestão de redes WBL deverá ajudar o *helpdesk* a identificar toda a informação relativa aos utilizadores e equipamentos. Quando ocorrer uma falha, a gestão do sistema deve ajudar o *helpdesk* a analisar onde é que a falha ocorreu e em que circunstâncias.
- **Outros** - Possibilidade para centralmente configurar parâmetros de segurança de um dispositivo cliente, para que possa coincidir com as políticas da organização; gerir a distribuição de *firmware* nos clientes; correlacionar e diagnosticar questões relacionadas com os clientes e automaticamente implementar acções correctivas, de forma a alterar as configurações dos clientes; configurar clientes e APs para melhorar a gestão de energia para aumentar a performance (questão pertinente em telefones e *palmtops*); controlo sobre as configurações dos dispositivos clientes de forma a prevenir associações de APs não autorizados;

4.3.2 FUNÇÃO INFRA-ESTRUTURA

No modelo que se apresenta, a função infra-estrutura divide-se nos seguintes módulos:

- Inventário;
- Configuração;
- Serviços de rede e controlo de acessos;
- Planeamento.

O módulo de **Inventário** terá a responsabilidade de gerir quer os equipamentos da rede quer dos seus utilizadores. Deverá ser capaz de fazer uma caracterização de todos os elementos existentes na rede WBL. As funcionalidades que este módulo deverá ter são:

- Descoberta automática de equipamentos e utilizadores na rede;
- Descoberta de novos equipamentos, recorrendo por exemplo a serviços de localização baseados na rádio frequência;
- Relatórios por AP, por controlador, por clientes;
- Permitir pesquisas por utilizador, por IP, por MACAddress, por tipo de equipamento (portátil, PC, PDA, Smartphone, telefones Voip, etc..);
- Garantir a legalidade da solução (frequências utilizadas, potências);
- Geração automática de mapas de topologia;
- Identificação do rádio 802.11 utilizado por cada AP e cliente;
- Gestão dos canais utilizados nas frequências rádio.

O módulo de **Configuração** deverá permitir a gestão de toda a configuração dos equipamentos da rede, que deverá de conter as seguintes funcionalidades:

- Configuração remota dos equipamentos, incluindo a actualização remota do *firmware*;
- Definição de configurações modelo (*templates*), para facilitar a instalação quando houver necessidade de instalar um novo AP;
- Inventariar a versão do *firmware* e verificar automaticamente se existe necessidade de o actualizar;
- Definição de vários parâmetros tais como os canais e a potência do sinal;
- Actualização de software;
- Agendamento para a configuração de parâmetros;
- Gestão de rede baseada em políticas – definição de políticas de acordo com a localização, com o perfil. Por exemplo, nos acessos *guest*, a largura de banda pode ser limitada.

O sucesso de qualquer implementação está na capacidade para efectuar um bom **Planeamento**. Um bom planeamento evitará surpresas desagradáveis. Assim, este módulo deverá ser capaz de:

- Efectuar site *surveys* (testes de RF), gerando relatórios e posterior análise;

- Identificar que norma IEEE 802 deverá ser utilizada;
- Possibilidade de efectuar testes de carga (por exemplo: previsão de distribuição de utilizadores por AP? Quantos APs são necessários para a cobertura pretendida?);
- Identificar a melhor infra-estrutura para as aplicações (voz e vídeo);
- Medição de interferências, obstáculos e ruídos;
- Demonstrar resultados em mapas (cobertura, qualidade de sinal, zonas de sombra).

Na categoria Infra-estrutura deverá ainda estar presente um módulo para disponibilizar **Serviços de rede e controlo de acessos**, que deverá proporcionar as seguintes funcionalidades:

- Gestão e administração dos utilizadores;
- LDAP, DHCP, DNS, Proxy, etc...
- Protocolo de segurança associado;
- Registar a actividade dos utilizadores;
- Atribuição de permissões baseadas em perfis de utilizador;
- Sistema de controlo de acesso, baseado num portal captativo (*web based login*).

4.3.3 FUNÇÃO SEGURANÇA

No modelo, a função Segurança integra os seguintes módulos:

- Definição e atribuição de políticas de segurança;
- Auditoria;
- Detecção de AP's não autorizados.

O módulo de **Definição e atribuição de políticas de segurança**, deverá ter as seguintes funcionalidades:

- Gestão de múltiplos SSID's/ESSID's;
- Gestão de múltiplos protocolos de segurança (WEP, WPA, WPA2, Radius, 802.11x, EAP, VPNs etc.);
- Definição de perímetros de segurança, *firewalls*, tipo de encriptação a utilizar;
- Implementação de assinaturas para ataques conhecidos, e possibilidade de criar novas, de modo a prevenir ataques conhecidos;

- Instalação de configurações de segurança (*patches*).

O módulo de **Auditoria** terá a responsabilidade de informar sobre o estado da rede, com o objectivo de garantir a detecção de falhas e corrigi-las. Este módulo deverá ter as seguintes funcionalidades:

- Detecção de erros humanos;
- Detecções de configurações que não foram bem efectuadas;
- Envio de alertas quando as anomalias são detectadas;
- Possibilidade de encontrar equipamentos roubados.

Deverá ainda existir um módulo para detectar AP's não autorizados. Esta função é muito importante, pois se não existir um controlo efectivo do consumo do serviço, o sistema pode perder performance e mais grave do que isso, permitir que a segurança do sistema seja quebrada. Deverão ser implementados mecanismos IDS.

4.3.4 FUNÇÃO MONITORIZAÇÃO

A função Monitorização deverá fornecer informações sobre o estado da rede. Uma boa solução deverá contemplar os seguintes módulos:

- Monitorização em tempo real;
- *Helpdesk e troubleshooting*;
- Implementação de QoS;
- Serviços de localização;
- *Reporting*.

O módulo de **Monitorização em tempo real** deverá considerar as seguintes funcionalidades:

- *DashBoard* que permite em tempo real verificar o que está a acontecer na rede, identificando se ela está de “boa saúde”.
- Permitir avaliar o estado dos equipamentos da rede: temperatura, humidade;
- Alertas e diagnósticos;
- Visualização do tráfego gerado na rede;
- Identificação do AP que o utilizador está utilizar ou já utilizou;

- Identificação do SSID ou VLAN que está a ser utilizado;
- Visualização da norma 802.11 que se está a utilizar na rede;
- Visualização do canal utilizado;
- Visualização da largura de banda utilizada;
- Força do sinal;
- Endereço IP;
- *Mac Address*;
- Verificação da existência de sobreposição de canais;
- Verificar se a cobertura é suficiente para o tipo de tráfego gerado;
- Identificação das aplicações na rede que estão a provocar estrangulamentos;
- Possibilidade de correlacionar os erros;
- Resolução de interferência do espectro, provocadas pelas tecnologias GSM, Bluetooth, WIMAX, entre outras;
- Possibilidade de definir alertas para quando ocorrem os picos de utilização e se se aproximam da capacidade limite.

Outrora, o administrador de redes só se tinha de preocupar com a quantidade de dispositivos a instalar e com o controlo da infra-estrutura. A tendência actual é para que as suas preocupações se focalizem em aspectos como estatísticas de aspectos técnicos:

- Quem está a causar picos de utilização?
- Que aplicações estão a exigir mais da rede?
- Em que momentos ocorrem os picos de utilização da rede?
- Onde se localizam geograficamente os utilizadores das aplicações?

A atribuição de canais e a potência da transmissão de energia RF necessita de ser ajustada para evitar interferências à medida que a utilização da rede cresce. As soluções de gestão devem fornecer algoritmos de optimização automática para controlar as configurações da RF de forma a eliminar a necessidade de repetir alterações manuais. Os sistemas de gestão devem monitorizar a qualidade de sinal do utilizador e a performance da rede, com o intuito de ajudar a equipa de *helpdesk* a diagnosticar interferências RF quando estas ocorrem.

O módulo de ***Helpdesk e Troubleshooting*** deverá ajudar a equipa de suporte a prestar *Helpdesk* aos utilizadores, fornecendo ferramentas para resolução de problemas. Deverá

ainda permitir o registo dos *ticket's*. Relativamente ao diagnóstico, a solução deverá permitir as seguintes funcionalidades:

- Detecção de interferência de canais;
- Detecção de ruído no sinal;
- Optimização da utilização dos canais RF;
- Detecção e reconfiguração de configurações erradas;
- Promover a rotação automática de chaves privadas;
- Ferramenta de *Troubleshooting* para cliente;
- Informação sobre as vulnerabilidades;
- Log's dos eventos na rede;
- A solução de gestão deve ter capacidade para mostrar o tipo de tráfego que o cliente está a gerar;
- Responder às seguintes questões: o utilizador está ligado? Está autenticado? Qual é o AP que ele está a utilizar? Este está a funcionar correctamente? Onde é que ele está localizado? Quais são as condições da área, são normais? Este utilizador tem prioridades? Terá ele um sinal forte?
- Uma solução de gestão de redes WBL deve suportar APs com *dual radio*, e devem informar com facilidade o serviço de *helpdesk*, sobre qual o rádio que o utilizador está a utilizar.

O módulo de **QoS** deverá garantir a implementação de mecanismos de qualidade de serviço na rede para as aplicações definidas como prioritárias, como a voz e o vídeo. Identificar sobrecargas de APs e efectuar balanceamento de carga;

O módulo de **Reporting** deverá fornecer a informação mais variada sobre a rede. Exemplo de alguns relatórios a gerar por este módulo:

- Relatórios de utilização da rede;
- Relatórios por AP;
- Relatórios por períodos de tempo;
- Gráficos;
- WLAN Performance;
- Relatórios de Inventário por dispositivo;

- Relatórios de auditorias;
- Relatórios de Erros de utilização;
- Relatórios de ameaças de segurança;
- Envio de relatórios por mail.

O módulo de **Serviços de localização** deverá fornecer aos administradores de rede ferramentas visuais do que está a acontecer na rede. Deverá contemplar as seguintes funcionalidades:

- Possibilidade de visualização numa planta, carta militar ou ortofotomapa (GoogleMaps) os APs e os clientes;
- Visualização da cobertura e da performance da rede; Detecção de zonas de sombra – Detecta zonas de sombra e tenta corrigi-las através do ajuste da potência de transmissão dos APs adjacentes;
- Gestão da mobilidade do utilizador (*roaming history*);
- Alertas para a capacidade de cobertura rádio – a solução deverá ter a capacidade para alertar o administrador da rede, para a capacidade de cobertura no cenário da rede.

Como resumo da explanação efectuada neste capítulo, onde se expõe uma proposta para o modelo de gestão de redes WBL para zonas rurais, ilustra-se na Figura 23, o respectivo modelo.

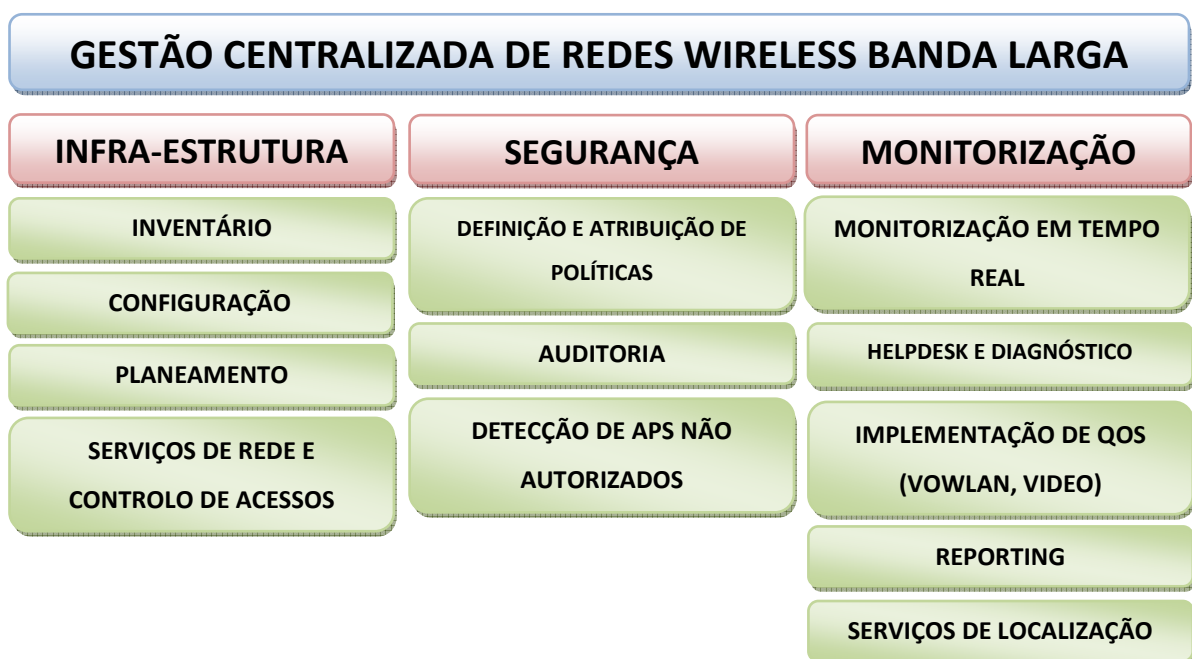


Figura 23: Modelo de gestão para as redes WBL

Este modelo pretende servir de base para uma solução de gestão, que possa ajudar a tornar as implementações de redes WBL em zonas rurais mais fáceis de gerir, onde não existe capacidade económica para adquirir soluções de gestão comerciais.

A questão da centralização é crucial para a simplificação da gestão, pois não são apenas os recursos financeiros que escasseiam, os recursos humanos nestes cenários também não abundam, por esta razão é necessário otimizar os recursos. Na Figura 23 podem ser observadas as três categorias em que se divide o modelo: Infra-Estrutura, Segurança e Monitorização. Sobre estas categorias, apresentam-se os vários módulos já descritos neste ponto.

4.3.5 RESUMO

Neste capítulo pretendeu-se apresentar o modelo de gestão para as redes WBL para cenários de zonas rurais, onde o acesso ADSL não é ainda uma realidade.

Para ajudar a definir o modelo, foi apresentada uma metodologia que poderá ser seguida na implementação de gestão de redes WBL. As categorias identificadas, os módulos definidos, e as funcionalidades desses módulos, constituem a 1ª fase da metodologia, que consiste na definição dos objectivos pretendidos para a gestão de redes WBL para zonas rurais. Os princípios técnicos e a escolha das ferramentas que permitem atingir esses objectivos, são expostas no Capítulo 5 - Testes e Resultados. Após a implementação das ferramentas e a consequente obtenção de uma solução de gestão, permitirá ao administrador de rede tomar decisões (a última fase da metodologia).

5. TESTES E RESULTADOS

Este capítulo reflecte a experimentação de algumas funcionalidades derivadas da definição do modelo da Gestão de Redes WBL em zonas rurais, descrita no capítulo anterior. Neste capítulo irão ser demonstradas algumas das funcionalidades de dois módulos da categoria Infra-Estrutura, identificados no modelo definido, a saber: módulo de Serviços de rede e Controlo de Acessos e ainda o módulo de Inventário.

Fazendo jus ao defendido no modelo, a questão da gestão centralizada da rede é um aspecto de elevada importância, conforme já detalhado no Capítulo 4 – Modelo de Gestão para as Redes WBL. As abordagens possíveis para a consecução de uma gestão de Redes Wireless Centralizada são duas, conforme referido no ponto 4.2 - Princípios Técnicos e Ferramentas:

- Desenvolvimento de uma plataforma de gestão;
- Implementação de soluções em plataformas existentes;

Decidiu-se por seguir o caminho da segunda possibilidade, ou seja, concentração das funcionalidades numa plataforma centralizadora de todas as funções de gestão de redes WBL.

Tendo em conta a constatação retirada do ponto 3.4 – Comparação de Soluções, onde se concluiu que se deveria desenvolver uma solução recorrendo a soluções *opensource*, houve necessidade de escolher um sistema operativo onde a solução se baseasse. Entre as várias distribuições de sistemas operativos *opensource*, a escolha recaiu sobre o Linux Ubuntu⁷⁰, dado tratar-se de uma distribuição com elevado desempenho e fiabilidade, não obstante ser possível implementar o modelo proposto noutras distribuições Linux.

Nas funcionalidades que não foram possíveis testar com software existente, houve necessidade de desenvolvimento.

5.1 CENÁRIO

⁷⁰ <http://www.ubuntu.com>

As zonas rurais são, conforme descrito ao longo da dissertação, o cenário para o qual se direcciona o modelo identificado. No entanto, o cenário implementado para testar as funcionalidades identificadas no modelo, consistiu na configuração de uma rede interna em laboratório, onde se simularam os vários tipos de acessos, ou seja, os vários perfis de acesso à rede.

A Figura 24 mostra o cenário implementado, onde a solução de gestão é o último componente de uma rede com vários APs, ligados através de um *Switch*. Esses APs podem ser de duas categorias, *hotspots* para fornecer Internet ao público, ou APs “fixos” para fornecer internet aos utilizadores domésticos. Neste cenário, a solução de gestão funciona como uma *gateway*, que filtra e analisa todo o tráfego para a *Internet*. Os clientes utilizados foram portáteis e *desktops* com o sistema operativo Windows XP Professional.

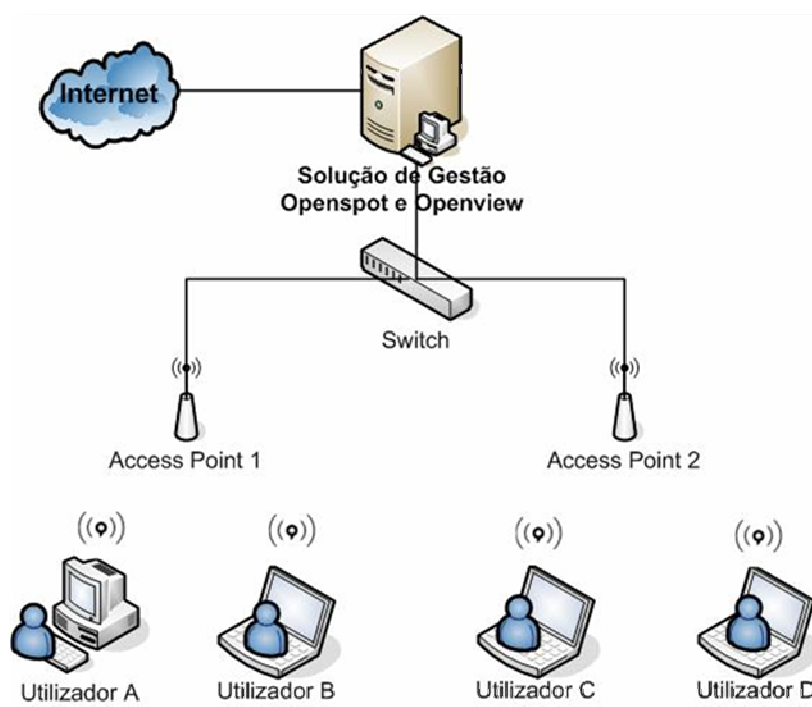


Figura 24: Cenário de testes

Os utilizadores para terem acesso à Internet podem fazê-lo a partir de *hotspots* públicos ou requisitando os equipamentos domésticos, que permitem uma maior estabilidade, no sentido em que são fixos. Num cenário de zona rural, os APs domésticos irão ligar-se aos APs de

core da Infra-Estrutura, que deverão permitir cobertura em toda a área pretendida. Nos subcapítulos seguintes descreve-se a implementação dos dois módulos da solução de gestão de redes WBL.

5.2 INFRA-ESTRUTURA - SERVIÇOS DE REDE E CONTROLO DE ACESSOS

Neste ponto serão demonstradas as funcionalidades testadas para o módulo Serviços de Rede e Controlo de Acessos da categoria Infra-Estrutura. O nome que se designou para este módulo foi “Openspot”.

O primeiro desafio na implementação dos testes foi conseguir colocar todos os módulos e suas funcionalidades num sistema centralizado. Para reunir a quantidade de módulos *opensource* num só, encontrou-se na ferramenta Webmin⁷¹ a solução mais adequada. O Webmin é uma ferramenta de administração gráfica, baseada num interface Web, escrito na linguagem Perl⁷². É um software de administração funcional, que pode ser facilmente escalável e modular. A base do Webmin funciona como um centralizador de módulos que permite configurar e administrar o sistema operativo, monitorizando todos os serviços e servidores, com uma interface muito amigável que quando configurado com um servidor Web, pode ser acedido a partir de qualquer *browser*. O Webmin permite ainda o desenvolvimento de novos módulos, para que seja possível efectuar a gestão de uma qualquer aplicação que seja instalada no sistema operativo Linux. Na Figura 25 pode ser observado um menu do interface do Webmin, contendo as diversas opções para as funcionalidades do módulo de Serviços de Rede e Controlo de Acessos.

Este teste permitiu demonstrar como é possível implementar-se na solução a característica de gestão centralizada.

⁷¹ <http://www.webmin.com>

⁷² <http://www.perl.org>

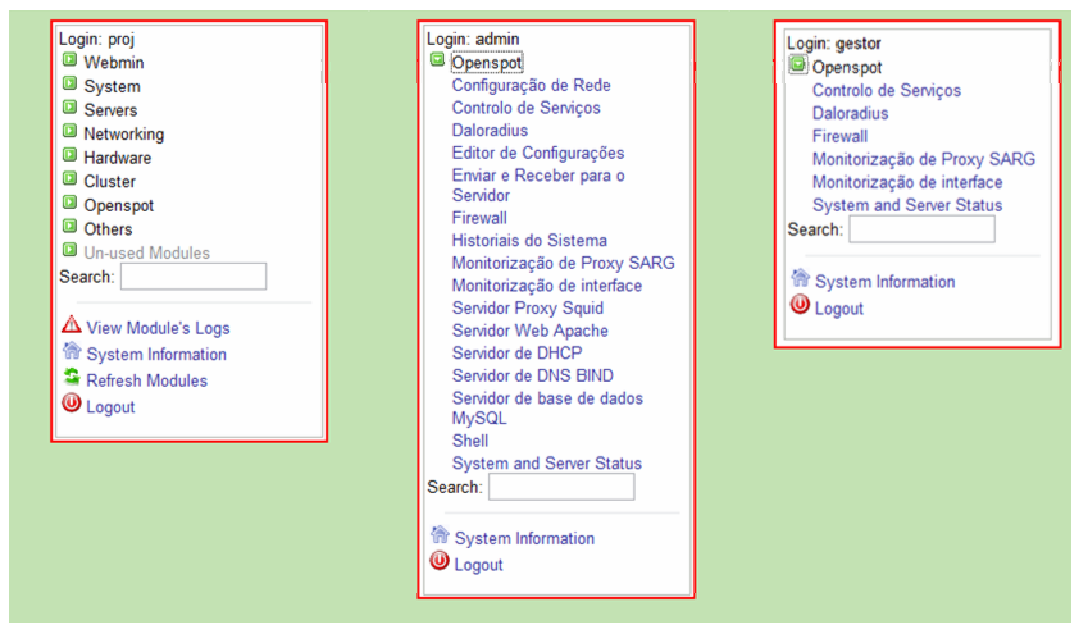


Figura 25: Interface do Webmin

Com a finalidade de gerir os utilizadores e as suas permissões para aceder aos serviços de rede, utilizou-se o seguinte software *opensource*: Feeradius⁷³, Doloradius⁷⁴, MySQL⁷⁵, Squid⁷⁶.

A solução de gestão precisa de ter pelo menos um servidor de autenticação, que será responsável pela validação das credenciais apresentadas pelos utilizadores. O software de servidor *radius* escolhido para autenticar os pedidos de acesso à rede foi o Freeradius. Para facilitar a gestão do Freeradius, optou-se pela utilização do software Doloradius, que para além de possibilitar a gestão Web do Freeradius, apresenta relatórios gráficos, *billing* e integração com o Google Maps. Para armazenar toda a informação foi necessário uma base de dados, pelo que a escolha recaiu no servidor de base de dados MySQL. O Squid é um software que para além de fazer *cache* das páginas consultadas na Internet, permite redireccionar tráfego, como se de um router se tratasse.

Depois de uma pequena definição de cada ferramenta, importa explicar como foram utilizadas. No MySQL foi armazenada toda a informação sobre os utilizadores e permissões.

⁷³ <http://freeradius.org>

⁷⁴ <http://sourceforge.net/projects/doloradius>

⁷⁵ <http://www.mysql.com>

⁷⁶ <http://www.squid-cache.org>

Através do Freeradius foi possível limitar a largura de banda por utilizador, assim como definir o tempo de sessão. O serviço proxy Squid permitiu redireccionar os utilizadores com o perfil de guest, ou seja, os utilizadores que acederem à rede através dos hotspot's. Uma vez que nestes casos, o acesso à rede será garantido através de um mecanismo de *web based login*, que será explicado em parágrafos seguintes. Através do Daloradius, foi possível através de um interface *Web*, gerir este processo.

Para se conseguir incorporar o Daloradius a partir do Webmin foi necessária uma configuração para acrescentar o menu. Esta configuração consiste em alterar um *script do Webmin*. Já o Squid faz parte das aplicações que o Webmin suportavam de origem.

Na Figura 26 é apresentada a página de entrada do Daloradius, incluída no Webmin.



Figura 26: Página de entrada Daloradius

O menu “Management” do Daloradius permite efectuar diversas acções:

- Adição de utilizadores;
- Remoção de utilizadores;
- Edição e pesquisa de utilizadores;
- Gestão de perfis de utilizadores;
- Gestão de grupos de utilizadores;

- Gestão de *hotspots*;
- Modificar atributos, domínios;

O menu “Accounting” é um dos menus mais importantes pois permite ao administrador monitorizar o tráfego dos clientes da rede, como aliás se pode observar na Figura 27.

Users Accounting +

STATISTICS									
ID	USERNAME	PASSWORD	CREDIT	USED	TIME REMAINS	% OF TIME LEFT	TOTAL SESSIONS	UPLOAD (BYTES)	DOWNLOAD (BYTES)
4	teste1	teste1	N/A	4 days, 8 hours, 20 minutes, 31 seconds	0 seconds	N/A%	61	2.1 Gb	73.29 Mb

CSV Export

1234

ID	HotSpot	Username	IP Address	Start Time	Stop Time	Total Time	Upload (Bytes)	Download (Bytes)	Termination	NAS IP Address
52	OpenSpot Guest	teste1	192.168.100.2	2008-06-23 21:10:02	2008-06-23 21:10:21	19 seconds	8.63 Kb	3.27 Kb	User-Request	192.168.100.1
53	OpenSpot Guest	teste1	192.168.100.2	2008-06-23 21:10:52	2008-06-23 21:11:22	30 seconds	4.8 Kb	5.53 Kb	User-Request	192.168.100.1
54	OpenSpot Guest	teste1	192.168.100.2	2008-06-23 21:13:43	2008-06-23 21:15:04	1 minutes, 21 seconds	9.68 Kb	9.66 Kb	User-Request	192.168.100.1
55	OpenSpot Guest	teste1	192.168.100.2	2008-06-23 21:15:12	2008-06-23 21:15:48	36 seconds	27.95 Kb	7.31 Kb	User-Request	192.168.100.1
56	OpenSpot Guest	teste1	192.168.100.2	2008-06-23 21:15:56	2008-06-23 21:16:33	37 seconds	4.96 Kb	1.92 Kb	User-Request	192.168.100.1
57	OpenSpot Guest	teste1	192.168.100.2	2008-06-23 21:16:51	2008-06-23 21:17:15	24 seconds	4.21 Kb	1.71 Kb	User-Request	192.168.100.1

Figura 27: Informações sobre o tráfego dos utilizadores

Outra funcionalidade interessante que este menu apresenta é a possibilidade de comparar *hotspots* de forma a identificar possíveis anomalias e corrigir eventuais erros de sessão.

O menu “GIS” oferece um sistema de informação geográfica que permite identificar a localização de cada hotspot através do GoogleMaps⁷⁷. A Figura 28 mostra um exemplo de uma localização geográfica de um *hotspot*.

⁷⁷ <http://maps.google.com>

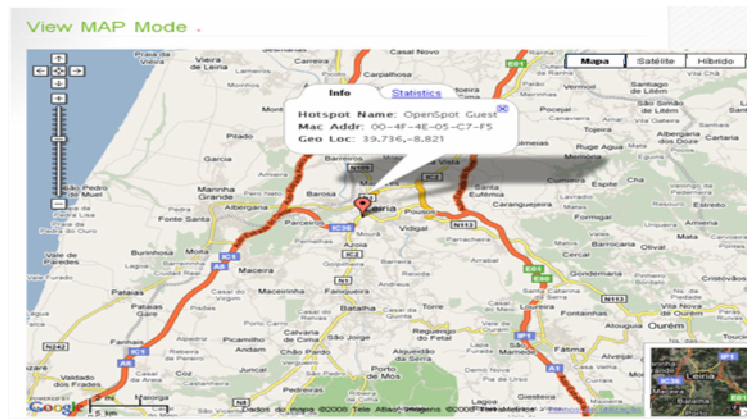


Figura 28: Localização de um *hotspot* no GoogleMaps através do Doloradius

O menu “Graphs” gera um conjunto de gráficos e estatísticas onde se pode visualizar entre outras coisas:

- Os downloads e uploads por utilizador;
- O tráfego total;
- O número de utilizadores, como se mostra na Figura 29.

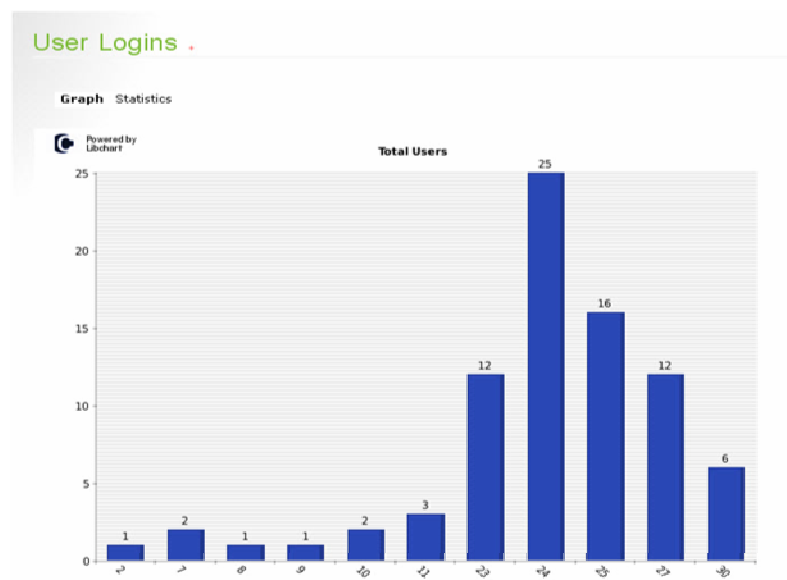


Figura 29: Gráfico do nº de autenticações gerado pelo Doloradius

Além dos menus mencionados, existem ainda mais dois para configurações gerais e ajuda.

Com a finalidade de demonstrar a funcionalidade de antivírus (Segurança), foi utilizada a ferramenta HAVP⁷⁸, que consiste num HTTP proxy antivírus, que tem como objectivo inspeccionar todo o tráfego HTTP da rede. O tráfego é verificado através de um antivírus que no caso de detectar código malicioso, irá impedir a sua entrada na rede. O HAVP utiliza o antivírus ClamAV⁷⁹, que consiste num *toolkit* antivírus para plataformas UNIX, sendo a característica mais reconhecida a capacidade para analisar e-mails. Para testar esta funcionalidade, criou-se um vírus que foi bloqueado com sucesso aquando da navegação do cliente no *browser*, conforme pode ser observado na Figura 30.

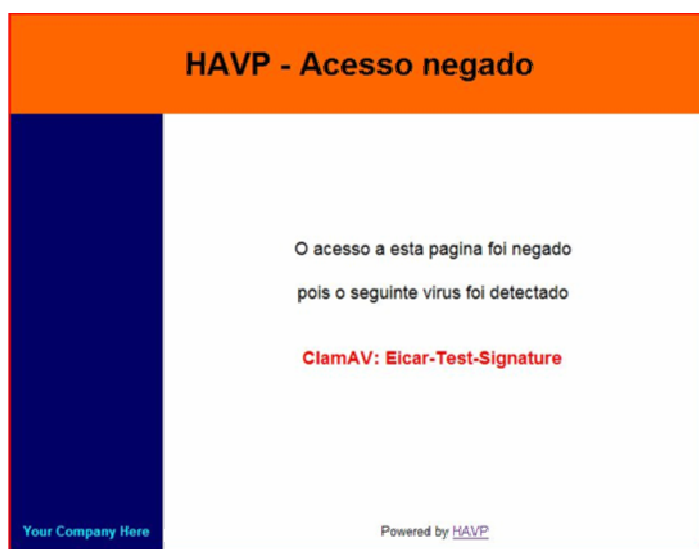


Figura 30: Exemplo de um vírus bloqueado com o HAVP

Para testar a funcionalidade de controlo de acesso à rede, foi utilizado o software CoovaChilli⁸⁰, pois apresenta um elevado conjunto de funcionalidades, nomeadamente no suporte a vários tipos de autenticação. O CoovaChilli é um software de portal captativo, utilizado em *hotspots*, para controlar acessos às redes wireless. Demonstra-se nos parágrafos seguintes, um teste efectuado para aceder à rede com controlo do CoovaChilli .

⁷⁸ <http://www.server-side.de>

⁷⁹ <http://www.clamav.net>

⁸⁰ <http://coova.org/wiki/index.php/CoovaChilli>

Logo que o utilizador encontra a rede wireless, mas não se encontre ainda autenticado, é redireccionado para uma página a informar os termos e condições de acesso à rede da rede (ver Figura 31).

openspot W-LAN

Termos e Condições de Utilização

1. Alterações e Condições e Termos Adicionais Especiais

O OpenSpot pode modificar as Condições Gerais sem qualquer aviso prévio. Recomendamos a consulta periódica desta Página na Web para verificar se está a par das Condições Gerais mais recentes, porque elas são vinculativas. O uso da Página na Web ou dos Serviços após essas alterações indica sua anuência e concordância com as mesmas.

2. Segurança da página Web

É proibido violar, ou tentar violar, a segurança da página Web ou dos Serviços. Quaisquer infracções desse tipo podem originar responsabilidades civis e criminais. Nós iremos investigar quaisquer alegadas infracções, e, se houver suspeita de uma infracção criminal, iremos colaborar nas investigações efectuadas pelos órgãos competentes com vista ao cumprimento da lei. As violações da segurança da Página da Web e dos Serviços incluem, sem restrições, o seguinte:

Envolver-se em comportamentos que possam prejudicar ou diminuir a operacionalidade desejada da Página da Web ou dos Serviços.

Representar qualquer indivíduo ou entidade, expressar erroneamente ou ainda deturpar sua identidade ou filiação de algum modo, ou forjar, apagar ou alterar qualquer parte das informações do cabeçalho do pacote de TCP/IP.

Envolver-se em marketing online enganoso;

Ajudar ou permitir que qualquer pessoa se envolva em quaisquer das actividades acima descritas.

3. Uso da página Web

A. Serviço. A página pretende disponibilizar um método de autenticação e registo com a finalidade de obter acesso à internet. É importante que o utilizador tenha conhecimento de que a segurança dos dados apenas é garantida durante o processo de autenticação e registo. Após a conclusão de qualquer um destes processos não garantimos segurança nas transacções HTTP que o utilizador efectua. Em alternativa, pode ter usado o método de autenticação 802.1x estando disponível apenas para residentes na freguesia.

B. Utilizador Não Residente. Considera-se utilizador não residente qualquer indivíduo que não possua morada na freguesia e que pretende utilizar o serviço por tempo limitado. Os privilégios de uso do serviço estão de acordo com o que o openspot definiu como sendo suficientes às suas necessidades. O processo de registo passa pelo preenchimento de um formulário existente na página Web e consequente confirmação através de email.

C. Utilizador Residente. Considera-se utilizador residente qualquer indivíduo que possua residência na freguesia. O processo de registo é semelhante ao utilizador não residente, sendo necessária uma confirmação dos dados por parte administrativa para que lhe sejam atribuídos os privilégios de uso do serviço respectivos.

4. Como nos contactar

Se tiver alguma dúvida ou pergunta sobre a declaração online referente a esta Página da Web ou a sua implementação, contacte-nos através do seguinte endereço:

webmaster@openspot.pt

Li e aceito os termos e condições de utilização

OpenSpot© 2008
Todos os direitos Reservados ©

Figura 31: Termos e condições de acesso à rede

Após aceitar as condições, o utilizador é redireccionado para outra página, que lhe mostra as várias opções: *Login*, *Registar*, *Editar Dados* e *Opengardens*, conforme pode ser observado na Figura 32.

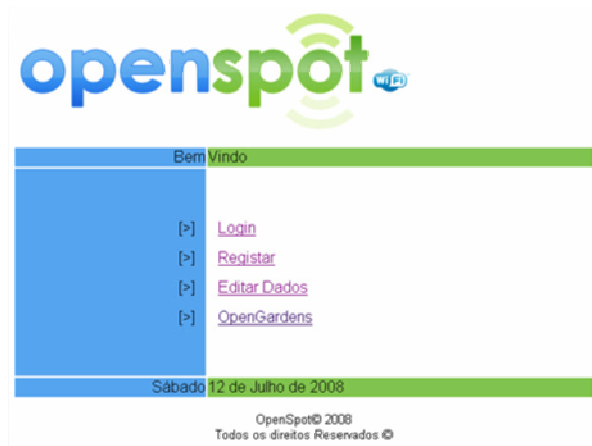


Figura 32: Menu de Opções

Aqui, o utilizador terá a oportunidade de efectuar login na rede, caso já esteja registado, registar-se na rede, editar e alterar os seus dados, ou então escolher a opção OpenGardens. Caso escolha esta última opção, estará a entrar na rede com o perfil de OpenGuest. Após seguir todas as instruções para se registar na rede, que inclui uma validação através de um *url* enviado por e-mail, o utilizador é informado do tipo de acesso que poderá usufruir na rede. Na Figura 33 é possível observar um exemplo destas mensagens.

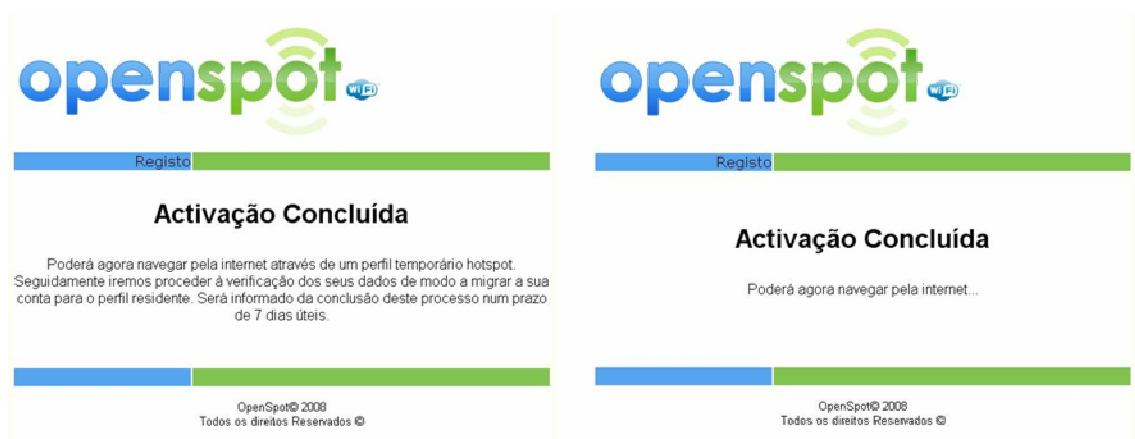
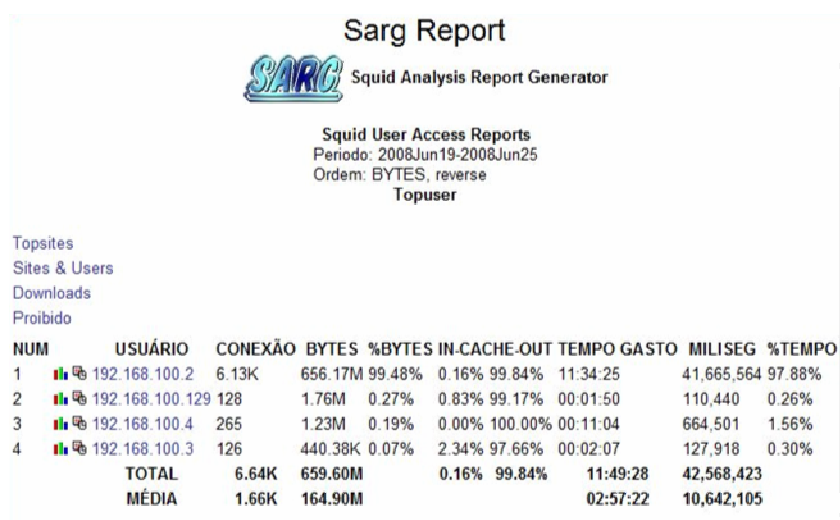


Figura 33: Mensagens mostradas ao utilizador de acordo com o perfil

Com o objectivo de testar a funcionalidade de controlar o tráfego utilizado pelos utilizadores na rede, foram utilizadas as ferramentas SARG e o Squint. O SARG é um software que utiliza o ficheiro de *log* de acessos do Squid (*access.log*), colocando-o legível e de fácil

interpretação. Na Figura 34, pode-se observar um exemplo de um relatório gerado por esta ferramenta.



Sarg Report
Squid Analysis Report Generator

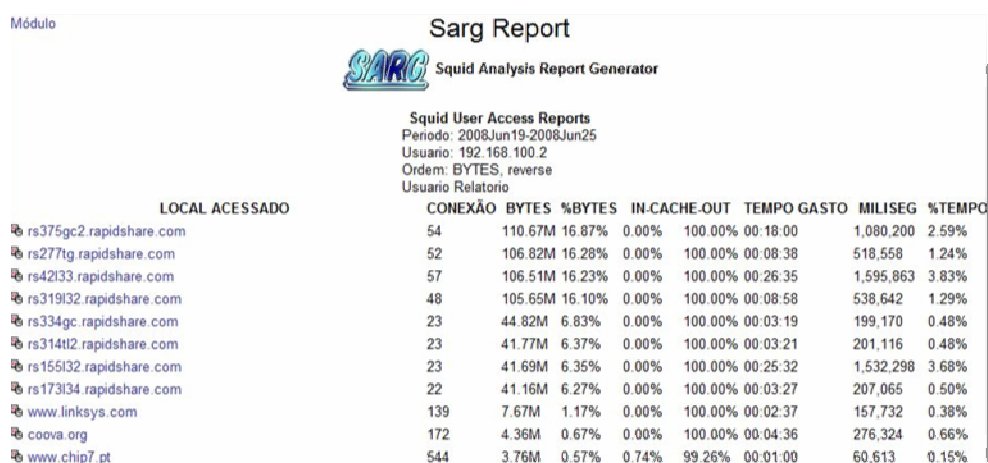
Squid User Access Reports
Período: 2008Jun19-2008Jun25
Ordem: BYTES, reverse
Topuser

Topsites
Sites & Users
Downloads
Proibido

NUM	USUÁRIO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT	TEMPO GASTO	MILISEG	%TEMPO
1	192.168.100.2	6.13K	656.17M	99.48%	0.16% 99.84%	11:34:25	41,665,564	97.88%
2	192.168.100.129	128	1.76M	0.27%	0.83% 99.17%	00:01:50	110,440	0.26%
3	192.168.100.4	265	1.23M	0.19%	0.00% 100.00%	00:11:04	664,501	1.56%
4	192.168.100.3	126	440.38K	0.07%	2.34% 97.66%	00:02:07	127,918	0.30%
	TOTAL	6.64K	659.60M	0.16%	99.84%	11:49:28	42,568,423	
	MÉDIA	1.66K	164.90M			02:57:22	10,642,105	

Figura 34: Exemplo de um relatório criado pelo SARG

É possível ainda, mostrar os detalhes por cliente, como se pode observar na Figura 35.



Sarg Report
Squid Analysis Report Generator

Squid User Access Reports
Período: 2008Jun19-2008Jun25
Usuário: 192.168.100.2
Ordem: BYTES, reverse
Usuário Relatório

LOCAL ACESSADO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT	TEMPO GASTO	MILISEG	%TEMPO
rs375gc2.rapidshare.com	54	110.67M	16.87%	0.00%	100.00% 00:18:00	1,080,200	2.59%
rs277tg.rapidshare.com	52	106.82M	16.28%	0.00%	100.00% 00:08:38	518,558	1.24%
rs42133.rapidshare.com	57	106.51M	16.23%	0.00%	100.00% 00:26:35	1,595,863	3.83%
rs319132.rapidshare.com	48	105.65M	16.10%	0.00%	100.00% 00:08:58	538,642	1.29%
rs334gc.rapidshare.com	23	44.82M	6.83%	0.00%	100.00% 00:03:19	199,170	0.48%
rs314112.rapidshare.com	23	41.77M	6.37%	0.00%	100.00% 00:03:21	201,116	0.48%
rs155132.rapidshare.com	23	41.69M	6.35%	0.00%	100.00% 00:25:32	1,532,298	3.68%
rs173134.rapidshare.com	22	41.16M	6.27%	0.00%	100.00% 00:03:27	207,065	0.50%
www.linksys.com	139	7.67M	1.17%	0.00%	100.00% 00:02:37	157,732	0.38%
coova.org	172	4.36M	0.67%	0.00%	100.00% 00:04:36	276,324	0.66%
www.chip7.pt	544	3.76M	0.57%	0.74%	99.26% 00:01:00	60,613	0.15%

Figura 35: Exemplo de um relatório detalhado de um utilizador gerado pelo SARG

Através do SARG, consegue-se ainda extrair informação como os sites mais pesquisados na rede, a quantidade de downloads efectuados, gráficos de utilização diária, páginas cujo acesso foram negadas, entre outros.

Através da ferramenta Squint consegue-se obter informações detalhadas sobre os acessos de cada utilizador. As suas funcionalidades não se apresentam ao nível do SARG, sendo a sua principal característica discriminar detalhadamente os pedidos de determinado cliente. O Squint foi utilizado para se conseguir obter informações mais detalhadas e precisas sobre o utilizador, uma vez que permite associar um cliente à respectiva sessão do utilizador. Na Figura 36 é possível identificar que o utilizador com o IP 192.168.100.2 efectuou pedidos de acesso a páginas *Web* a partir das 21 horas e 26 minutos, terminando às 22 horas. Para identificar a que utilizador pertence o endereço IP, basta ir á página de gestão de utilizadores (daloRadius) e efectuar uma pesquisa por IP entre as 21 horas e as 22 horas.

Internet access by 192.168.100.2 - Qui 10 Jul 2008

Time	Site	Minutes	Pages	Downloads	Size
21:26 - 21:58	www.google.pt	6:31	11	13	38 kbytes
21:26 - 21:26	wiki.freeradius.org	0:12	6	12	47 kbytes
21:26 - 21:38	www.google-analytics.com	3:37		6	9 kbytes
21:28 - 21:28	www.freebsd.com.br	0:18	2	14	38 kbytes
21:28 - 21:28	www.telcom.com.br	0:01	1	1	296 bytes
21:28 - 21:28	freebsd.com.br	0:04		4	16 kbytes
21:28 - 21:28	www.freebsdbrasil.com.br	0:01	1	1	8 kbytes
21:29 - 21:36	asdir.com	0:55	4	7	18 kbytes
<hr/>					
21:55 - 21:55	s7.addthis.com	0:02		4	14 kbytes
21:58 - 22:03	www.mibdepot.com	5:00	13	27	414 kbytes
21:59 - 21:59	images.parcipal.com	0:00		1	997 bytes

Interpretation:

- Time: Time of day (hours:minute:second) at which this site was first visited. The time of the last visit is also shown.
- Site: The name of the site to which this user connected. The link points to the first URL which was downloaded from this site.
- Minutes: The number of minutes and seconds that were spent connected to this site. All breaks of more than 5:00 minutes are not included in this amount.
- Pages: The number of HTML pages that were downloaded from this site. If any HTML pages were downloaded from the site, the entry for the is highlighted. HTTPS connections are counted as a single page.
- Downloads: The number of objects of any type that were downloaded from this site, ie: a HTML page, a HTTPS connection, an image, a style sheet, a javascript page, etc
- Size: The volume of data downloaded over the connection to this site

Figura 36: Exemplo de um relatório detalhado de um utilizador, gerado pelo Squint

Este conjunto de testes efectuados, mostram que apesar das várias condicionantes e melhorias, é ainda possível implementar uma solução de gestão centralizada e eficaz, que permita fornecer serviços de rede e infra-estrutura aos clientes de uma rede WBL, recorrendo apenas a software *opensource*.

5.3 INFRA-ESTRUTURA - INVENTÁRIO

Neste ponto pretende-se demonstrar outro módulo da categoria Infra-estrutura definido no modelo, nomeadamente o Inventário. A designação usada para este módulo foi de Openview Network Inventory Tool, que abreviado se designa por Openview. O conjunto de testes

efectuados tem como objectivo demonstrar a possibilidade de inventariar os equipamentos existentes na rede, quer AP's, quer clientes.

A implementação deste teste baseou-se no software *opensource* Nagios⁸¹. A principal funcionalidade do Nagios é a pesquisa automática de dispositivos na rede. Apesar das potencialidades do Nagios, houve necessidade de tornar a sua gestão mais amigável, sendo por isso escolhido o software Centreon⁸², que não é mais que um interface para o Nagios, tornando a informação disponibilizada por este, numa forma mais simples para o administrador da rede. As tarefas de configuração do Nagios também são facilitadas pelo Centreon.

Para apresentação da informação em modo gráfico, foi utilizado o software Cacti⁸³ que recolhe informações da rede e permite a sua visualização sob forma de gráficos.

Na Figura 37 pode ser observado a arquitectura da implementação deste módulo.

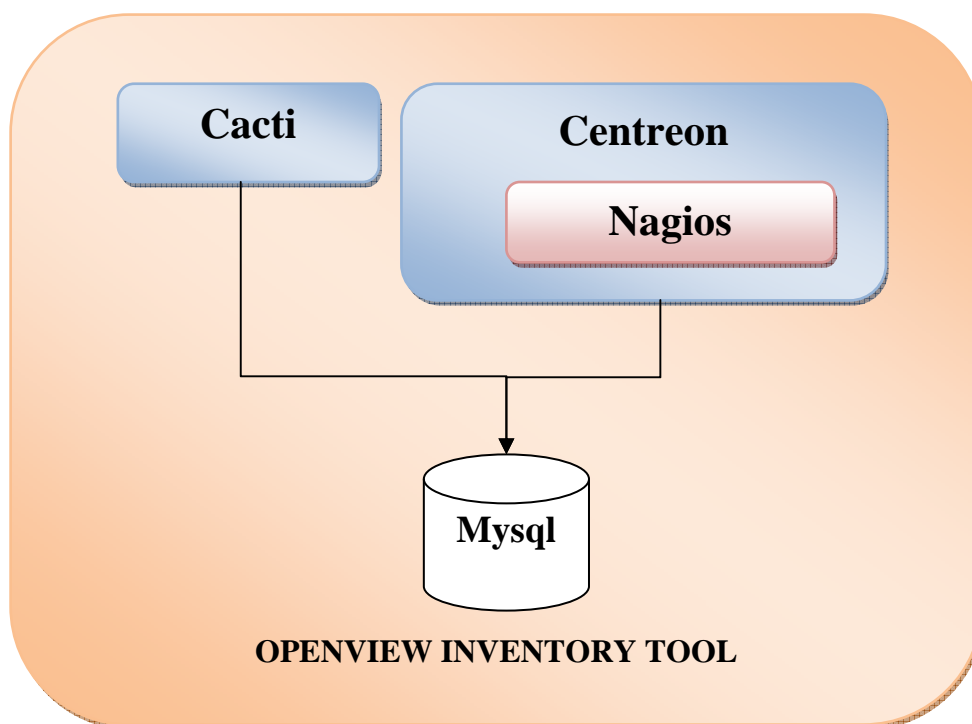


Figura 37: Arquitectura do Openview

⁸¹ <http://www.nagios.org>

⁸² <http://www.centreon.com>

⁸³ <http://www.cacti.net>

A implementação deste módulo teve em conta o módulo do ponto anterior (5.2 – Infra-estrutura – Serviços de Rede e Controlo de Acessos). Numa lógica de gestão centralizada, como refere o modelo de gestão de Redes WBL, este módulo utilizou a mesma base de dados de utilizadores que o Opensot.

O Openview foi colocado na rede onde já se encontrava o Openspot, e onde existia um AP, que permitia o acesso wireless a dois utilizadores. Na Figura 38 pode-se observar o cenário de implementação deste módulo.

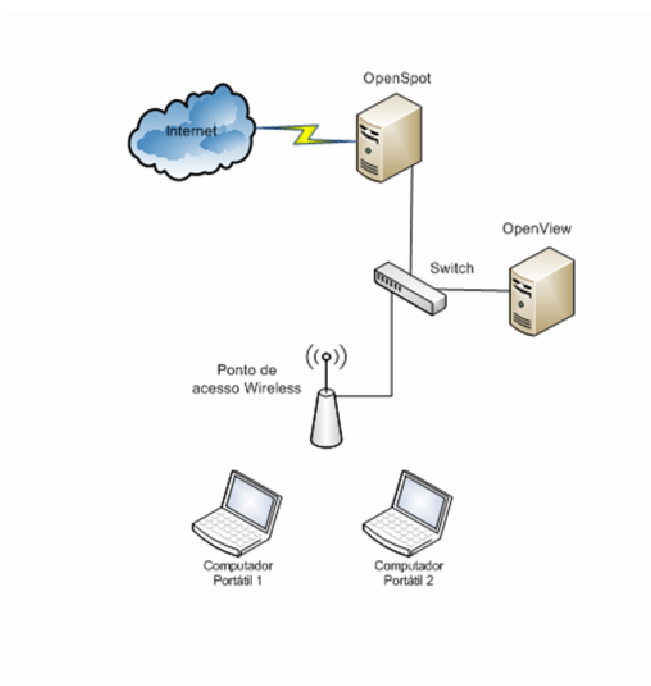


Figura 38: Arquitectura da solução implementada no Openview

Demonstram-se nos parágrafos seguintes, alguns testes realizados com as funcionalidades implementadas para este módulo de Inventário.

O primeiro teste que se descreve, tem como finalidade avaliar a capacidade de descoberta de equipamentos e utilizadores da ferramenta OpenView. O objectivo final é obter o inventário completo da rede utilizada como cenário de testes. Na Figura 39 e 40, mostram os resultados obtidos pela ferramenta OpenView na descoberta automática de redes a inventariar (Figura 39) e na descoberta de todos os dispositivos de rede presentes no cenário de testes (Figura 40).

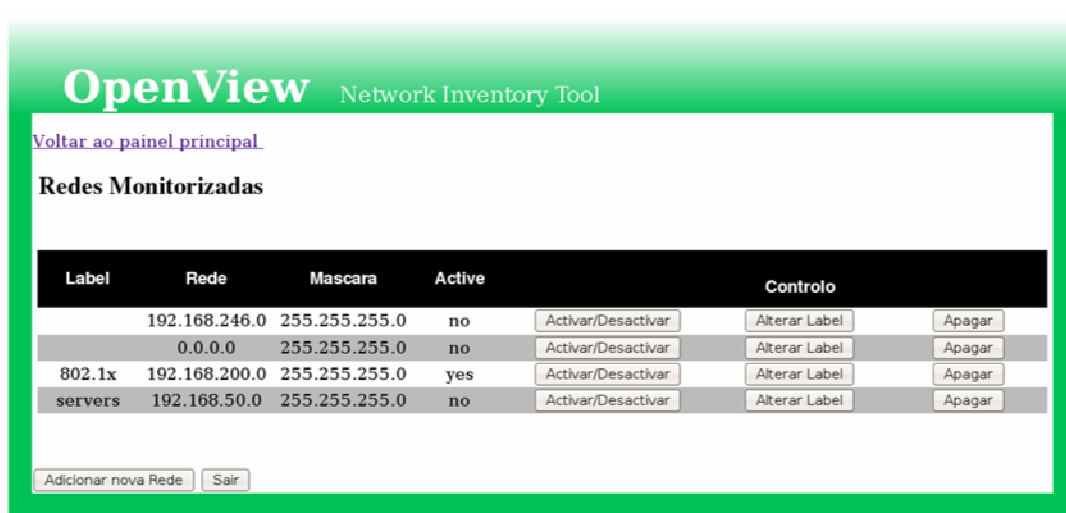


Figura 39: Exemplo das redes encontradas pelo OpenView

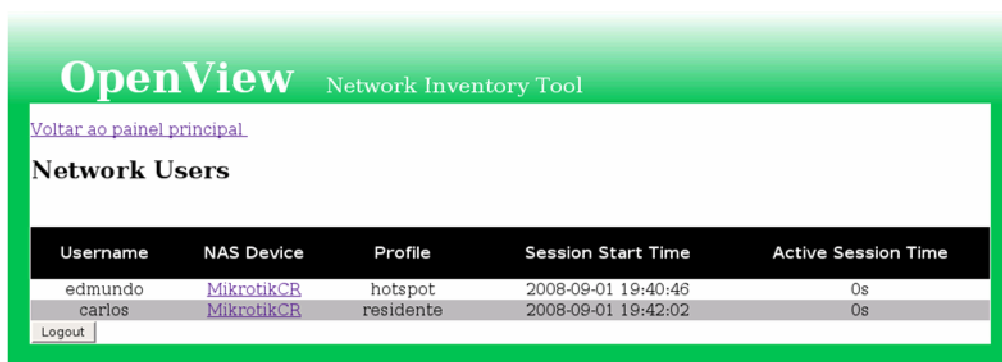


Figura 40: Exemplo dos dispositivos de rede descobertos pelo OpenView.

Com o objectivo de testar a funcionalidade de descoberta de novos equipamentos, adicionou-se um novo AP ao cenário inicial, previamente configurado com o *hostname* “cisco” e o IP estático 192.168.200.254, ligando-o à rede através do *switch*. O resultado pode ser observado na Figura 41, onde é possível verificar algum detalhe sobre o novo dispositivo descoberto.



Figura 41: Exemplo da descoberta automática de dispositivos com o Openview

Este componente do Openview, responsável pela descoberta automática de dispositivos e redes, foi desenvolvido de raiz com recurso a *scripts* em PHP⁸⁴ e PERL⁸⁵. Esta necessidade deve-se ao facto de não terem sido encontradas ferramentas *opensource*, com a eficácia desejada para satisfazer esta funcionalidade do modelo de gestão.

O teste seguinte tinha como finalidade a demonstração da inventariação e monitorização de vários parâmetros do dispositivo de rede.

Tanto o Nagios como o Centreon oferecem a capacidade de criar relatórios com base na informação de monitorização de equipamentos e serviços. Na Figura 42 pode observar-se um exemplo da monitorização de um AP com a informação relativa ao seu estado, tempos de resposta, verificação de conectividade, latência, entre outros. No Centreon a secção *Reporting* é totalmente dedicada a esta tarefa, podendo criar-se um relatório, que tenha em consideração o tipo de informação que se pretende avaliar e em que período de tempo. No interface do Nagios existe a mesma funcionalidade na secção com o mesmo nome.

⁸⁴ <http://www.php.net>

⁸⁵ <http://www.perl.org>

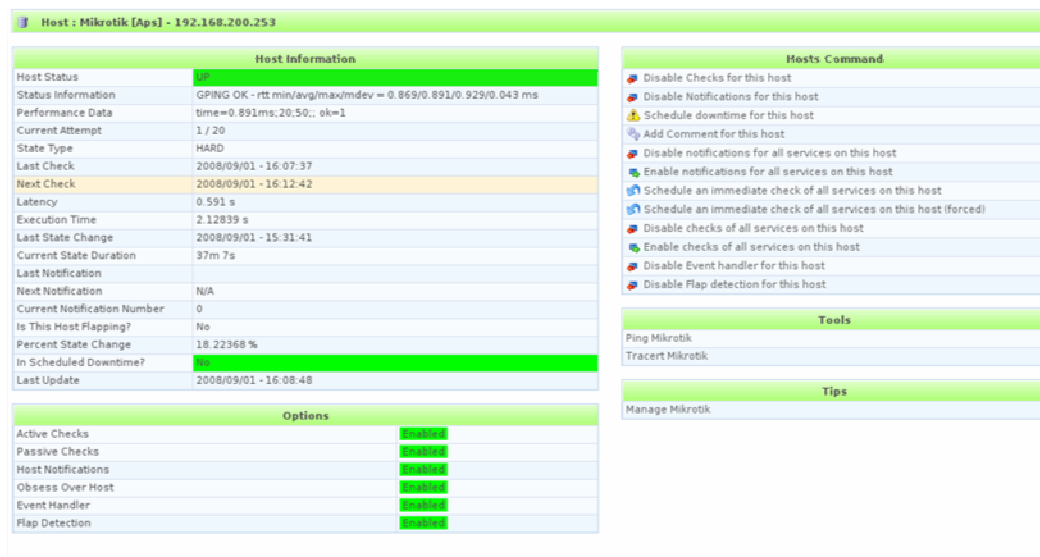


Figura 42: Monitorização de um AP através do Nagios/Centreon

Na Figura 43, é possível verificar a disponibilidade de um dos APs utilizados nos testes (Mikrotik CR).

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	5d 3h 38m 17s	73.594%	73.594%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	5d 3h 38m 17s	73.594%	73.594%
DOWN	Unscheduled	0d 2h 20m 31s	1.394%	1.394%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 2h 20m 31s	1.394%	1.394%
UNREACHABLE	Unscheduled	1d 18h 1m 12s	25.012%	25.012%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	1d 18h 1m 12s	25.012%	25.012%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	7d 0h 0m 0s	100.000%	100.000%

State Breakdowns For Host Services:					
Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
ping	73.104% (73.104%)	0.000% (0.000%)	24.828% (24.828%)	2.068% (2.068%)	0.000%
Average	73.104% (73.104%)	0.000% (0.000%)	24.828% (24.828%)	2.068% (2.068%)	0.000%

Figura 43: Relatório de disponibilidade de um AP e dos serviços a ele associados

Para testar as funcionalidades de monitorização de tráfego nos interfaces dos equipamentos, espaço em disco do servidor onde a aplicação está instalada, utilização do CPU, utilização da

memória, desempenho, entre outros, foi utilizada a ferramenta Cacti. Nas Figuras 44 e 45 podem ser observados os resultados dos exemplos referidos.

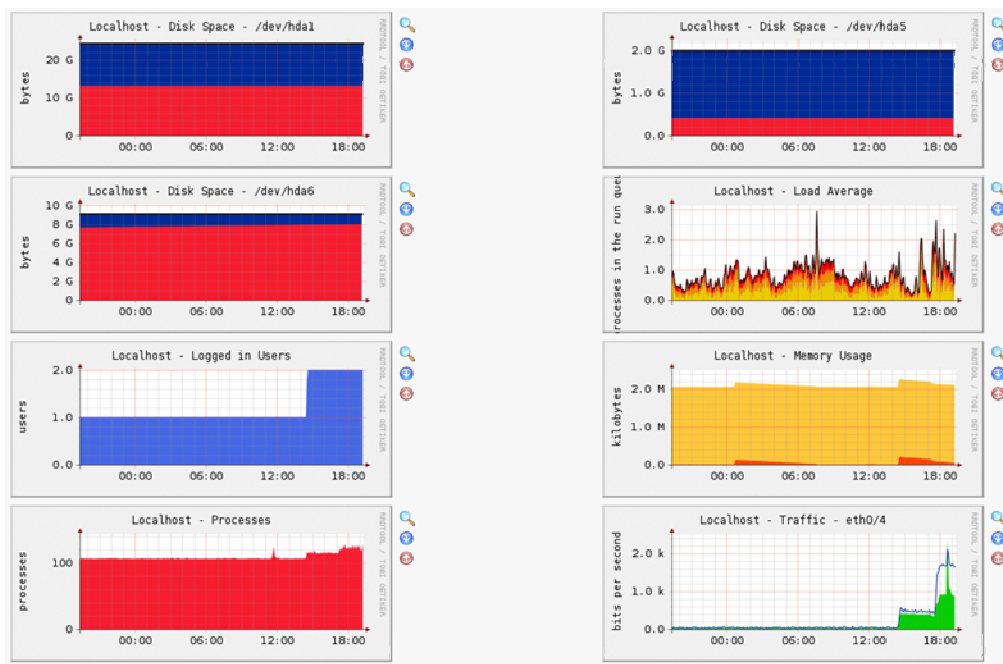


Figura 44: Monitorização do servidor OpenView

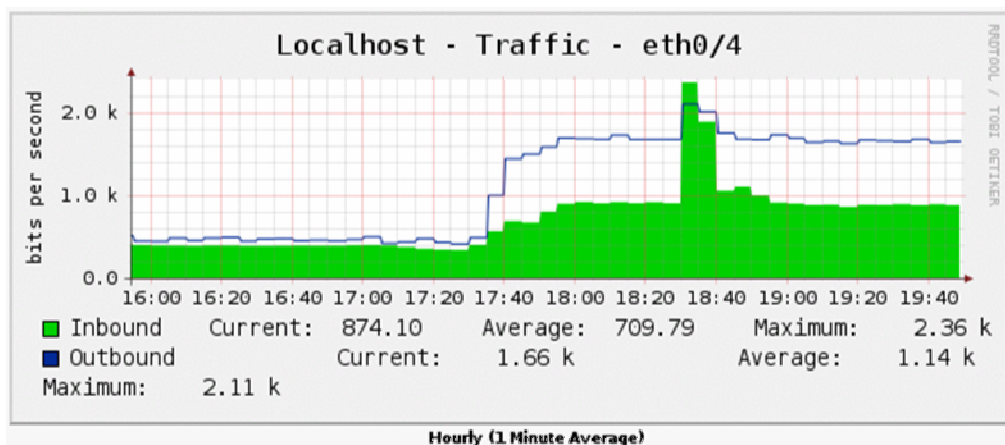


Figura 45: Monitorização do interface Ethernet 4 do servidor OpenView

5.4 ANÁLISE DE RESULTADOS

No ponto anterior foram demonstradas várias funcionalidades definidas no modelo de gestão apresentado no capítulo 4 - Modelo de Gestão de redes WBL. Naturalmente que a demonstração de resultados nem sempre comprova os modelos, pelo que se identificam nos mesmos, algumas oportunidades de melhoria.

No entanto, houve um número considerável de funcionalidades testadas, que se podem enunciar a seguir:

- Descoberta automática de equipamentos e utilizadores na rede;
- Descoberta de novos equipamentos na rede;
- Geração automática de mapas de topologia;
- Gestão e Administração dos utilizadores;
- Serviços de rede, tais como LDAP, DHCP, DNS, e outros;
- Registar a actividade dos utilizadores (Proxy);
- Atribuição de permissões baseadas em perfis de utilizador;
- Sistema de acesso *Web Based Login*;
- Possibilidade de visualização numa planta, carta militar ou ortofotomapa (GoogleMapsg) os APs e os clientes;
- Visualização do tráfego gerado na rede;
- Identificação do AP que o utilizador está a utilizar ou já utilizou;
- Visualização da largura de banda utilizada;
- Informação sobre o endereço IP;
- Informação sobre o endereço *Mac Address*;
- Relatórios de utilização da rede;
- Relatórios de Inventário por dispositivo;

Muitas funcionalidades ficaram por demonstrar, nomeadamente as que estão relacionadas com a monitorização de sinal de rádio, segurança e serviços de localização. O modelo que se definiu pressupõe a implementação de um número elevado de funcionalidades, pelo que se justifica a não demonstração de todos.

A implementação e testes realizados demonstraram que é possível implementar o modelo definido e que o mesmo pode contribuir para os objectivos enunciados que, relembre-se, consistem em obter uma gestão centralizada de gestão de redes WBL.

6. CONCLUSÃO

O domínio de investigação da presente dissertação é a da gestão de redes WBL que conforme definido no Capítulo 2 – Redes Wireless Banda Larga, consistem em redes wireless existentes em zonas onde a Banda Larga por cabo não chega.

Os principais objectivos desta dissertação foram o de especificar e conceber um modelo, que permitisse efectuar uma gestão de redes WBL de forma eficaz e eficiente. Eficaz porque se pretende obter uma boa solução para gerir bem as redes WBL, eficiente porque se pretende fazê-lo da forma mais económica.

Para auxiliar na definição do modelo, foram abordados vários temas sobre as redes wireless no Capítulo 2. Neste capítulo para além do conceito de redes WBL, objecto da presente dissertação, foram abordadas as várias normas das redes wireless, assim como a evolução da gestão das mesmas, à medida da evolução das diversas arquitecturas. No Capítulo 2 foram ainda abordadas as tendências que as redes wireless estão a tomar, e alguns projectos desenvolvidos na Europa e na América Latina. Foi possível, por exemplo, constatar que academicamente Portugal não integra qualquer destes projectos, o que é de lamentar.

Na busca de uma definição das funcionalidades que um modelo deveria contemplar, efectuou-se no Capítulo 3 – Levantamento de Funcionalidades e soluções de gestão de redes WBL, um levantamento das soluções comerciais e soluções *opensource*, para a gestão das redes wireless. Neste capítulo foi possível concluir e evidenciar a importância que o tema desta dissertação tem nos dias de hoje, isto porque, se constatou que as melhores ferramentas de gestão de redes wireless são comerciais. Sendo a natureza das implementações redes WBL mormente de carácter local, como por exemplo Juntas de Freguesia, verifica-se a inexistência de grandes recursos financeiros para investir na gestão da rede. Logo, apesar de ser possível implementar o modelo em qualquer tecnologia, licenciada ou gratuita, a conclusão, dadas as circunstâncias descritas, inclinou-nos para a utilização de ferramentas *opensource* (Capítulo 5 - Testes e Resultados).

No Capítulo 4 – Modelo de Gestão para Redes WBL, foi definido o modelo que abrange todas as áreas da gestão das redes WBL e onde são especificados todos os requisitos para

uma boa solução. O modelo apresentado sugere uma solução centralizada, que permita efectuar uma gestão das redes WBL de uma forma simples. É ainda abordada uma metodologia para a implementação de uma solução de gestão, consistindo em definir bem os objectivos pretendidos, identificar os princípios técnicos e ferramentas de forma a alcançar os objectivos definidos, para que se possam tomar decisões para melhorar a gestão das redes WBL. Esta metodologia deve estar presente quando se desejar implementar uma solução de gestão de redes WBL, como pôde ser observado no Capítulo 5 através da implementação.

Em suma, o modelo de gestão para as redes WBL apresenta como principal característica a centralização, que agrega três grandes funções: Infra-estrutura, Segurança e Monitorização. Estas áreas, por sua vez dividem-se em vários módulos, cada um cumprindo uma funcionalidade específica. O conjunto destes elementos representa o modelo enunciado.

Para comprovar o modelo, foram demonstrados no Capítulo 5 dois módulos da área de Infra-estruturas: Inventário e Serviços de rede e Controlo de Acessos. Com estas duas implementações, foi possível demonstrar alguns resultados, que permitem comprovar que o modelo definido pode ser implementado e tem boas possibilidades de constituir uma boa solução para a gestão de redes WBL em zonas rurais.

6.1 PRINCIPAIS CONTRIBUIÇÕES

Apresentam-se como principais contribuições desta dissertação as seguintes:

- Resumo de definições e conceitos de diversas normas de redes wireless;
- Conceito de redes WBL;
- Levantamento da evolução das arquitecturas de redes wireless, desde o seu início até à actualidade, nomeadamente da forma como a sua gestão era e é efectuada;
- Levantamento de soluções *opensource* e comerciais existentes no mercado, assim como das suas funcionalidades, identificando os pontos fortes e pontos fracos;
- Conclusão da inexistência de uma ferramenta *opensource*, que satisfaça os requisitos mínimos para uma gestão eficaz e eficiente de redes wireless;
- Apresentação de um modelo de gestão para as redes WBL, incluindo a identificação de funcionalidades para uma boa solução;
- Demonstração prática de dois módulos identificados no modelo, que consubstanciam a aplicabilidade do mesmo. Na demonstração de resultados, evidenciou-se que os

requisitos identificados no modelo podem ser conseguidos com recurso a ferramentas *opensource*, ou seja, de baixo custo;

- O modelo apresentado pode constituir uma base para se conseguir obter uma boa solução de gestão de redes WBL e outras. Para organizações com limitações de orçamento, este modelo representa uma solução completa, capaz de abranger as várias áreas do processo de gestão de redes WBL, na medida em que clarifica e define essas áreas. Demonstrou-se através dos módulos implementados e demonstrados, que o modelo resulta e é possível implementar;

6.2 TRABALHO FUTURO

O modelo identificado abrange todas as áreas da gestão de redes WBL, o que implica um grande volume de módulos e funcionalidades. Seria por isso impossível neste trabalho demonstrar todos os módulos identificados, logo, para além da melhoria dos módulos de Infra-estruturas demonstrados (Serviços e Controlo de Acessos e Inventário), falta ainda demonstrar os restantes módulos identificados no modelo.

Nos resultados demonstrados, foi patente a possibilidade de se conseguir uma solução de gestão centralizada através do Webmin, no entanto, esta funcionalidade ainda tem algum espaço para ser melhorada, pois alguns módulos poderão necessitar de algum desenvolvimento para se conseguir esta convergência. Existe também a oportunidade de se criar uma *framework* comum a todos os módulos, ou seja, possibilidade de se ter um directório de dados único como por exemplo, colocar todos os módulos a obter a mesma informação sobre os utilizadores, sobre os equipamentos, sobre as configurações de segurança, sobre os perfis, entre outros. Existem módulos cuja funcionalidade depende desta centralização, por exemplo, o módulo de Helpdesk e Diagnóstico, precisa de ter esta informação centralizada.

Dos módulos demonstrados, o que tem mais margem para melhoria é o módulo de inventário, pois existem aspectos que devem constar deste módulo e que não foram desenvolvidos na implementação. É necessário obter mais informação sobre o estado do sinal de rádio de cada equipamento cliente e servidor. A implementação da norma 802.11v nos equipamentos, irá facilitar em muito esta funcionalidade, mas para isso é necessário que os equipamentos a suportem.

Um desafio muito interessante será aplicar este modelo a outras tecnologias que não as IEEE 802.11, como são o exemplo das IEEE 802.16 e IEEE 802.22. Apesar de estas tecnologias ainda não proliferarem no mercado, prevê-se que sejam rapidamente adoptadas, logo, necessitarão de uma solução de gestão. Ainda no mesmo desafio, será interessante reformular o modelo, para poder abranger diversas tecnologias na mesma solução de gestão.

7. REFERÊNCIAS E BIBLIOGRAFIA

[Hudson,2003] - Hudson, H. E., “Bridging the broadband divide: Strategies for rural and developing regions”, White Paper - p. 3, 2003.

[Papacharissi et all,2006] - Zizi Papacharissi and Anna Zaks, “Is broadband the future? An analysis of broadband technology potential and diffusion”, Science Direct, 2006.

[Synergy,2006] - Synergy research group, “NextHop: The Next Step in Enterprise Wireless LANs”, Dezembro 2006.

[Balachandran et all,2005] - Anand Balachandran, Geoffrey M. Voelker, Paramvir Bah, “Wireless Hotspots: Current Challenges and Future Directions”, 2005.

[Halton,2007] – Jeremy Halton, “WLAN Best Practices, How to manage a Wireless LAN?”, Airwave Webcast, 2007.

[Geier,2002] - Geier Jim, “Wireless LANs - Sans Publishing, 2nd edition”, 2002.

[DeBeasi,2007a] - Paul DeBeasi, “802.11n: Beyond the Hype”, Burton Group, 2007.

[Dan,2004] – Simone Dan, “802.11k makes WLANs measure up”, revista Network World, Março 2004.

[Demirkol et all,2004] - Demirkol, M.F. Ingram, M.A. Zhengqing Yun, “Feasibility of closed loop operation for MIMO links with MIMO interference”, Center for Adv. Commun., Hawaii Univ., Honolulu, HI, USA , 2004.

[Guido et all,2007] - Hiertz Guido R., Max Sebastian, Zhao Rui, Denteneer Dee Berlemann Lars, “Principles of IEEE 802.11s”, artigo de revista Computer Communications and Networks, 2007.

[Ono,2004] - Edson Toshiaki Ono, “Implantação de redes Wireless de Alta Velocidade”, Tese Mestrado – Universidade Federal de Santa Catarina , 2004.

[Cherry, 2004] – Cherry Steven, “WiMax and Wi-Fi: Separate and Unequal”, Spectrum IEEE, Março 2004.

[Mathias,2006a] - Craig J. Mathias, “Which WLAN architecture wins?”, Farpoint Group, Julho 2006.

[Xirrus,2005] – Xirrus, “Enterprise Wireless Lan Evolution”, Março 2005.

[DeBeasi,2007b] – Paul DeBeasi, “Wireless LAN Systems: Ready for the Future?”, Buron Group WhitePaper, Abril 2007.

[Wexler,2006] - Joanie Wexler, “From thick to thin APs: Making the WLAN transition”, Artigo da revista Network World, Julho 2006.

[Sridhar,2006] - T. Sridhar, “Wireless LAN Switches — Functions and Deployment”, The Internet Protocol Journal - Volume 9 Number 3 Cisco, Setembro 2006.

[Metzler,2005] – Ashton, Metzler & Associates, “A Third Generation Distributed Wireless LAN Architecture”, White Paper, Agosto 2005.

[Colubris,2005] – Colubris, “Colubris TriPlane™ Architecture: Unprecedented WLAN Scalability”, Agosto 2005.

[Farpoint,2005] – Farpoint Group, “Advances in Wireless LAN Architecture: The Wireless Array”, Julho 2005.

[Synergy,2006] - Synergy research group, “NextHop: The Next Step in Enterprise Wireless LANs”, Dezembro 2006.

[Cisco,2007] – Cisco Systems, “Municipalities Adopt Successful Business Models for Outdoor Wireless Networks”, 2007.

[Galvis et al,2007] – Alexander Galvis Q., Rafael A. Márquez C., Luis A. Fletsher B., “Alternativas Tecnológicas para un mejor uso del espectro electromagnético”, White Paper, Centro de Investigacion de Las Telecomunicaciones - Columbia, 2007.

[Sala et al,2006] - Arnau Sánchez Sala, Joaquín Seoane, “Software libre para transmisión digital en enlaces radio”, Fundación EHAS - UPM, 2006.

[Nie et al, 2005] - Jing Nie, Xin He, Zheng Zhou, ChengLin Zhao, "Benefit-driven handoffs between WMAN and WLAN", Wireless Network Lab, Beijing University of Posts and Telecommunications, Beijing - China, 2005.

[Kumar et al,1996] - Sanjaya Kumar, J. Aylor, B. Johnson and W. Wulf, "The Codesign of Embedded Systems: A Unified Hardware/software Representation", Kluwer Academic Publishers, 1996.

[Innes,2005] - Simon Innes, "Turning a Linksys WRT54G into more than just a Wireless Router 2005", School of Computer and Information Science, Edith Cowan University, 2005.

[Lunde et al, 2006] - Lars Lunde, Audun Wangensteen, "Using SIM for strong end-to-end Application Authentication", Norwegian University of Science and Technology, Faculty of Information Technology, 2006.

[Loo,2008] - Alfred Loo, "The myths and truths of wireless security", Communications of the ACM, 2008.

[Paquereau et al,2005] - Laurent Paquereau, Brynjar Viken, Poul Heegaard, "Combining performance monitoring and location data in wireless networks", Universidade de Ciências e Tecnologia, Noruega, 2005.

[Prasithsangaree, et al 2002] - P. Prasithsangaree, P. Krishnamurthy, and P. K. Chrysanthis, "On indoor position location with wireless lans", IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Setembro 2002.

[Yang et al,2001] - Weishuai Yang Shanping Li Yuming Yao, "Hybrid network management paradigm", Dept. of Comput. Sci. & Eng., Zhejiang Univ., Hangzhou, 2001.