FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

FEUP

Projecto de um Hotspot, com uso controlado, para uma rede de empresa

António Cunha Barbosa

Relatório de Projecto/Dissertação

Mestrado Integrado em Engenharia Informática e Computação

Orientador: João Manuel Couto das Neves (Professor Auxiliar Convidado)

29 de Junho de 2009

Projecto de um Hotspot, com uso controlado, para uma rede de empresa

António Cunha Barbosa

Relatório de Projecto/Dissertação

Mestrado Integrado em Engenharia Informática e Computação

Aprovado em provas públicas pelo júri:

Presidente: João António Correia Lopes (Professor Auxiliar da FEUP)

Arguente: José Gerardo Vieira Rocha (Professor Auxiliar da Universidade do Minho)

Vogal: João Manuel Couto das Neves (Professor Auxiliar Convidado da FEUP)

17 de Julho de 2009

Resumo

O presente relatório vem descrever as acções que foram tomadas no desenvolvimento do projecto intitulado "Projecto de um Hotspot, com uso controlado, para uma rede de empresa". Este projecto consiste em desenvolver serviços para uma rede wireless que permita gerir acessos a utilizadores temporários, contemplando soluções existentes no mercado.

Neste estágio pretendia-se a criação de um sistema simples, robusto e seguro de gerir utilizadores temporários, permitindo definir os serviços que cada um tinha direito e limitar o tempo de acesso aos recursos. A solução a ser desenvolvida deveria ser o mais genérica possível, de forma a conseguir adaptá-la, tendo em conta as necessidades da empresa onde se pretende implementar. Para uma melhor compreensão do problema, foi realizado um pequeno estudo das redes wireless implementadas em locais conhecidos da cidade do Porto. Após este estudo, foi elaborado um plano sobre qual a melhor abordagem para solucionar esta questão. Ao longo do estágio, os objectivos e requisitos mais importantes foram-se tornando mais claros, o que contribuiu para a solução final. Esta solução é construída através da autenticação do protocolo RADIUS e os dados dos utilizadores serem guardados através do protocolo LDAP. A distinção de serviços, é realizada através da implementação de VLANs que é atribuída de forma dinâmica ao utilizador.

O estágio teve a duração de quatro meses e decorreu no INESC Porto, local que permitiu ter acesso a todos os equipamentos necessários para a criação da rede, e realizar todos os testes necessários. A escolha do local possibilitou também ter um conhecimento mais apurado sobre um ambiente empresarial.

O projecto foi bem sucedido, o que prova que a FEUP consegue formar indivíduos capazes de actuar nas mais diversas áreas, tendo em conta as necessidades das empresas, preparando-os para enfrentar qualquer desafio proposto.

Abstract

This report describe the actions that were taken in developing the project entitled "Project of a Hotspot, with controlled use, for a corporate network". This project pretends to develop services for a wireless network that allows manage users access temporary, reminding solutions on the market.

The stage was realized in order to create a simple, robust and safe to handle temporary users, allowing to define the services that each had a right and limiting the time of access to resources. The solution to be developed should be as generic as possible in order to adapt it to achieve, taking into account the needs of the company where you want to implement. For a better understanding of the problem, there was a small study of wireless networks implemented in known locations in the city of Oporto. After this study, it has been developed a plan on the best approach to resolve this issue. Over time, the objectives and the most important requirements were becoming more clear, which contributed to the final solution. This solution is built through the authentication of the RADIUS protocol and user data are saved through the LDAP protocol. The separation of services is done through the implementation of VLANs that are assigned dynamically to the user.

The stage had a duration of four months and ran at INESC Porto, allowing local access to all equipment necessary for establishing the network, and perform all tests required. The choice of the site also have enabled a more accurate about a business environment.

The project was successful, evidence that FEUP to train individuals capable of acting in several areas, taking into account the needs of businesses, preparing them to face any challenge proposed.

Agradecimentos

Quero agradecer a todos aqueles que contribuíram para o sucesso do projecto, através de todo o incentivo, apoio e disponibilidade demonstrado, nomeadamente o Professor João Neves, meu orientador de estágio

Gostaria também de agradecer à equipa do SCI do INESC Porto, local onde realizei o estágio, pois demonstraram serem pessoas bastante colaboradoras e competentes na área em que se inserem.

Por fim, gostaria de agradecer aos meus pais e à minha namorada pelo apoio e persistência, pois sem eles não teria realizado o estágio.

António Barbosa

Conteúdo

Lista de Figuras

Lista de Tabelas

Abreviaturas e Símbolos

AAA	Authentication, Authorization, Accounting
ACL	Access Control List
AD	Active Directory
AP	Access Point
CHAP	Challenge-Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitared Zone
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EAP-GTC	Extensible Authentication Protocol - Generic Token Card
EAP-MD5	EAP - Message-Digest algorithm 5
EAP-MSCHAP	Microsoft PPP CHAP Extensions
EAP-PSK	EAP - Pre-Shared Key
EAP-TLS	EAP - Transport Layer Security
EAP-TTLS	EAP - Tunneled Transport Layer Security
eduroam	Education Roaming
FCCN	Fundação para a Computação Científica Nacional
FEUP	Faculdade de Engenharia da Universidade do Porto
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IAX	Inter Asterisk eXchange
IEEE	Institute of Eelctrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IMAPS	Internet Message Access Protocol-SSL
INESC Porto	Instituto de Engenharia de Sistemas e Computadores do Porto
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
MAC address	Media Access Control address

MAN	Metropolitan Area Network
MD5	Message-Digest algorithm 5
MGCP	Media Gateway Control Protocol
MIEIC	Mestrado Integrado de Engenharia Informática e Computação
MPLS	MultiProtocol Label Switching
NAT	Network Address Translation
P2P	Peer-to-Peer
PEAP	Protected Extensible Authentication Protocol
PHP	PHP: Hypertext Preprocessor
PKI	Public Key Infrastructure
POP3	Post Office Protocol 3
POP3S	Post Office Protocol 3-SSL
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
SCI	Serviço de Comunicações e Informática
SFTP	Secure File Transfer Protocol
SGBD	Sistemas de Gestão de Bases de Dados
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol Secured
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell Protocol
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
VPN	Virtual Private Network
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WCCP	Web Cache Coordination Protocol
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

Capítulo 1

Introdução

Neste projecto procura-se obter uma solução capaz e robusta de gerir o acesso à rede wireless por parte dos utilizadores que não fazem parte da instituição. Estes caracterizam-se por serem utilizadores temporários, pois o seu período de permanência nas instalações é reduzido e como tal, o acesso à rede deverá ser apenas por um período restrito. Outro ponto importante a desenvolver no projecto, é o controlo de serviços disponíveis ao utilizador, de forma a permitir que apenas tenha acesso aos serviços de rede que necessita.

O projecto assentou em duas fases. A primeira fase consistiu em procurar soluções que satisfizessem os objectivos ou que de alguma forma permitissem atingir os mesmos resultados através da integração de várias soluções. A segunda fase concentrou-se numa vertente mais prática do projecto que consistia na sua implementação, permitindo verificar se as escolhas efectuadas satisfaziam ou não o pretendido.

Desde o início que existiam algumas ideias pré-concebidas, quer na escolha da plataforma operacional a utilizar, como também de algumas aplicações, na sua maioria programas de software livre, que permitiam atingir os objectivos propostos, assim como baixar o valor de implementação. De certa forma, é proposto que a implementação tivesse um custo zero, excluindo naturalmente os equipamentos de rede.

Durante todo o projecto, a fonte de informação mais requisitada foi a Internet, desde a procura de soluções, até à obtenção dos manuais de instalação dos diversos programas. Considero esta fonte de informação uma mais valia, pois permitiu resolver muitos dos diversos problemas que foram ocorrendo ao longo do projecto. Contudo, o conjunto de referências apresentado não representa a quantidade de páginas que foram consultadas, mas sim a qualidade e quantidade da informação apresentada. Outras páginas consultadas, principalmente fóruns, foram as responsáveis pela resolução de pequenos problemas, mas que não serão referenciadas.

A consulta de livros foi outra das fontes de informação utilizada. A sua procura ocorreu principalmente durante a instalação de certos programas, pois reuniam, em detalhe, informação que não era apresentada nas páginas consultadas na Internet, ou que de alguma forma se encontrava dispersa.

Por último, a fonte de informação mais importante consistiu na verificação em terreno de como se encontram implementados os acesso wireless existentes nos locais mais conhecidos da cidade do Porto. Esta fonte de informação, para além de permitir obter um perfil médio de utilizador, permitiu também saber como essas redes se encontram a ser geridas, e observar que consoante os requisitos pretendidos, varia a forma como foram implementadas.

Os objectivos deste projecto foram atingidos com sucesso, embora pense que alguns pontos poderiam ser melhorados. Considero os conhecimentos adquiridos, através da informação recolhida, da utilização das diferentes tecnologias, das diversas horas necessárias para a resolução de dúvidas, bem como a implementação da rede propriamente dita, determinantes para mim enquanto estudante e futuro profissional. O apoio das diversas pessoas que trabalham na área e que me acompanharam ao longo destas semanas, foi também importante para o desenvolvimento e conclusão do meu projecto.

1.1 Contexto/Enquadramento

Este trabalho insere-se na área de redes de computadores e é um projecto oferecido pela FEUP. Contudo, o seu desenvolvimento teve lugar no INESC Porto (Instituto de Engenharia de Sistemas e Computadores do Porto), na unidade SCI (Serviço de Comunicações e Informática), no sentido de proporcionar melhores condições de trabalho, nomeadamente acesso à Internet, bem como a diversos equipamentos de rede que foram necessários e que existem nesta unidade.

1.2 Projecto

Este projecto tem como intuito criar um hotspot numa empresa com uso controlado. Nasce da necessidade de corrigir situações de vulnerabilidade que ocorrem frequentemente numa rede empresarial, que apesar de não constituírem uma ameaça constante, ou colocarem a informação sensível em risco, merecem atenção.

O problema actual consiste em não ser possível definir para cada utilizador um conjunto de serviços que poderá utilizar e por um período de tempo estritamente necessário. Actualmente, os utilizadores usufruem de serviços que não necessitam ou, no caso em que a rede seja mais restritiva, poderá não ser possível aceder a serviços que se tornam indispensáveis para uma navegação correcta (como por exemplo a bloqueio das portas de e-mail).

O projecto traduz-se em duas fases. A primeira terá como propósito procurar informação sobre ferramentas já existentes no mercado. A segunda fase será utilizada para implementar a solução escolhida, de forma a verificar que a mesma corresponde aos objectivos propostos.

A solução final deverá permitir ao administrador da rede criar o utilizador, definir quais os serviços que o mesmo deverá ter acesso e o tempo pelo qual poderá aceder à rede, não sendo necessário qualquer acção posterior, no sentido de dar ou retirar permissões ao utilizador.

A solução a implementar deverá ser genérica, isto é, deverá permitir que a mesma solução se adapte a diversos tipos de empresa, e diversos tipos de utilizadores, não tendo como objectivo principal a correcção de uma infraestrutura de rede de uma empresa em particular.

1.3 Motivação e Objectivos

Ao longo do curso fui adquirindo um especial gosto pela área de redes de computadores, no qual obtive diversos conhecimentos, nomeadamente através das disciplinas optativas que frequentei sobre esta temática. A realização do projecto nesta área vem permitir reunir ainda mais conhecimentos e experiência sobre as diversas tecnologias com que contactei ao longo do curso. Por outro lado, possibilita o acesso a tecnologias completamente desconhecidas.

O objectivo deste projecto traduz-se na adaptação de uma ou mais ferramentas já existentes no mercado de forma a solucionar um problema existente nas redes empresariais. Este problema consiste, mais concretamente, na possibilidade de os diversos utilizadores que acedem à rede wireless apresentarem necessidades diferentes. Como exemplo de uma situação destas, temos a possibilidade de alguém se deslocar a uma instituição no intuito de realizar um estágio (normalmente com uma duração de meses), quando em simultâneo outra pessoa se desloca à mesma instituição mas com o intuito de uma reunião (onde a duração se expressa em horas). Verifica-se que, as necessidades de serviços são diferentes para cada indivíduo, o que torna necessário diferenciá-los, enquanto utilizadores da rede.

O sistema deverá também ser capaz de possibilitar ao utilizador o acesso a equipamentos que se encontram dentro da própria rede como é o caso de um auditor de contas, que necessita de ter acesso aos servidores de contabilidade, mas não necessita de estar na mesma rede que o departamento de contabilidade.

A cada administrador da rede apenas se torna necessário que o mesmo defina a cada utilizador os acessos a que tem direito e qual o tempo necessário, isto é, após criar o utilizador não deverá ser necessário mais nenhum passo para retirar permissões ou bloquear a conta do utilizador.

A solução deverá, como já foi referido, ser genérica, ou seja, adaptar-se à rede já existente numa empresa, e não se prender a um caso particular. Outro factor importante é a possibilidade de mesma poder ser extensível a outros requisitos, como também integrar-se com o software já existente (como por exemplo o repositório de autenticação).

A plataforma do sistema operativo deverá ser o Linux, não havendo qualquer restrição específica a distribuição usada. Os programas a serem usados deverão ser *open-source* ou *freeware* no intuito de manter o custo da solução nulo (excluindo naturalmente o hardware necessário).

1.4 Estrutura da Dissertação

O presente relatório encontra-se dividido em sete capítulos, acrescido dos anexos. O capítulo um corresponde à introdução, onde é apresentada uma breve explicação sobre o que é o projecto e o que se pretende do mesmo.

Para uma melhor compreensão do projecto e de alguns aspectos do relatório será, no capítulo dois, efectuada uma pequena explicação sobre redes de computadores e a evolução que estas foram tendo ao longo dos últimos anos. Neste capítulo é também incluída a forma como as redes wireless se integram nas redes físicas já criadas.

O capítulo três pretende demonstrar qual o problema existente a nível das redes wireless e o porquê da necessidade deste projecto ser aplicado numa rede empresarial, quer através de uma explicação detalhada, como também de exemplos de redes que se encontram a funcionar.

Os dois capítulos seguintes, têm como objectivo explicar como foi proposto resolver o problema mencionado no capítulo três, e como efectivamente resolvido. Esta separação de dados deve-se ao facto de inicialmente a forma de resolução do problema não se apresentar adequada e conter diversas falhas que não permitiam atingir os objectivos propostos. Após a explicação de como o projecto foi implementado, serão também discutidas as vantagens e desvantagens da solução encontrada para a resolução do problema.

Caso este projecto seja para implementação prática, é necessária a instalação de algum software adicional para garantir maior segurança à rede e melhor experiência de utilização por parte dos utilizadores. Sendo um projecto bastante genérico, é possível expandir as s4as funcionalidades, aproveitando recursos já disponíveis e criando novas soluções. Assim, o capítulo sobre trabalho futuro encontra-se dividido em software adicional e outras funcionalidades, para uma melhor percepção das ideias.

Por fim, o último capítulo pretende dar uma visão geral sobre o que foi o projecto para mim, enquanto estudante, e quais as conclusões que tirei do mesmo, oferecendo uma perspectiva pessoal sobre a temática abordada.

Capítulo 2

Apresentação de Redes

Neste capítulo será realizada uma breve introdução sobre alguns conceitos que existem na rede por cabo e na rede wireless. Será também apresentado como genericamente a topologia das empresas tem vindo a aumentar (e evoluir), no sentido de demonstrar em que medida este projecto se integra numa rede empresarial bem como a sua importância.

Para completar esta informação será também apresentado um conjunto de serviços que o utilizador tem actualmente ao seu dispor, necessários para uma melhor utilização na rede empresarial

Por fim, serão demonstrados alguns exemplos de redes wireless já existentes nas empresas, a forma como os utilizadores interagem com a rede e quais os serviços a que os mesmos tem acesso.

2.1 Rede LAN

Com o desenvolvimento dos computadores, cada vez mais se tornou necessário interligar os equipamentos, de forma a aumentar a versatilidade e a troca de informação. Uma das formas utilizadas é a rede cabo que ao longo dos anos tem aumentado em muito a sua capacidade de débito e de fiabilidade. Este conjunto de equipamentos que se encontram ligados entre si proximamente designa-se por LAN (*Local Area Network*). A designação desta interligação de rede de computadores poderá ser diferente consoante a distância a que os computadores se encontram entre si, podendo ser MAN (*Metropolitan Area Network*) ou WAN (*Wide Area Network*).

Cada vez mais as empresas apoiam a sua estrutura e funcionamento em sistemas de informação. Os sistemas de informação tendem a reunir a diversa informação que se encontra nos diversos departamentos da empresa e faz uso das capacidades das redes de computadores para distribuir e conseguir disseminar essa mesma informação já tratada

por outros departamentos. Contudo, esses departamento poderão ser locais como podem encontrar-se em diferentes cidades, e dessa forma necessitam da Internet para transmitir a informação.

Uma das arquitecturas mais usadas em redes é a arquitectura cliente-servidor, onde a informação se centra em um ou mais servidores (conhecido por *server farm* ou *server cluster*), e os utilizadores acedem a essa informação através dos seus computadores de trabalho (tipicamente através de browsers ou aplicações especificas). A utilização da Internet permite centrar a informação toda na sede, ao mesmo tempo que é utilizada nas diversas filiais.

2.2 Rede wireless

A rede wireless é parte integrante da rede LAN, sendo os seus requisitos e capacidades ligeiramente diferentes da rede por cabo. A principal diferença reside na forma como os dados são transmitidos (através de onda rádio) e nas potencialidades propostas (a mobilidade do utilizador sem perder conectividade).

Para fazer uso destas vantagens é necessário que os diversos equipamentos wireless estejam ligados entre si por cabo, permitindo que esta rede se integre perfeitamente na rede por cabo já implementada e até aumentar as capacidades da mesma. Dessa forma, um utilizador pode estar ligado por cabo no seu local de trabalho, mas quando se pretende deslocar para outra parte do mesmo, faz uso das capacidades do wireless para não perder a conectividade.

Outra das vantagens das redes wireless é a possibilidade de expandir a rede empresarial sem a necessidade de efectuar grandes investimentos de infra-estruturas, pois deixa de ser necessário a criação de um ponto de acesso para cada utilizador e passa a ser apenas preciso um ponto de acesso para cada AP (*Access Point*). Em média, cada AP permite ligar cerca de 32 utilizadores, sendo que os mesmos necessitam de estar próximos fisicamente.

Contudo, as redes wireless apresentam algumas desvantagens. Uma das principais desvantagens traduz-se na típica baixa velocidade de transmissão, em relação à rede por cabo; por outro lado encontra-se mais susceptível de interferências. Estas podem dever-se ao excessivo número de clientes centrados numa só zona, no entanto podem ocorrer por factores externos, como por exemplo um micro-ondas (que emite onda electromagnéticas na mesma frequência).

Outra desvantagem consiste na transmissão dos dados ser efectuada emitindo o sinal para diversos sentidos, transmissão essa que pode se interceptada por outra pessoa que esteja entre o cliente e o AP. Para evitar esta situação, é necessário que os dados sejam transmitidos encriptados, o que de certa forma aumenta a segurança mas diminui o débito

de transmissão. Em relação aos tipos de encriptação mais usados em redes wireless, irei desenvolver em parágrafos próximos.

Num mesmo local é possível ter diversas redes wireless, sendo distinguidas entre si pelos nomes que lhe são atribuídos. A forma de atribuição de nome a uma rede é realizado através do SSID (*Service Set Identifier*), que pode ser visível ou não para o utilizador.

Os utilizadores, para acederem a uma rede wireless, necessitam que o seu equipamento disponha de uma placa de rede wireless que costuma ser bastante usual nos computadores portáteis. Também é necessário que o AP tenha definido pelo menos um SSID (*Service Set Indentifier*). Um SSID é um identificador de rede que permite ao utilizador ligar-se a rede correcta.

2.3 Topologia usada nas empresas

Nesta secção vão ser apresentados de forma genérica alguns exemplos ilustrativos de topologias de redes de computadores, nos quais é possível verificar qual a evolução que foram tendo nos últimos anos (sem entrar em grandes detalhes).

2.3.1 Topologia inicial

Existem diversos tipos de topologias, mas a mais comum numa rede empresarial é a topologia hierárquica onde todos os computadores da empresas são ligados seguindo uma estrutura do tipo árvore (semelhante à da figura seguinte). Os ramos que estão mais próximos da raíz são normalmente usados para fazer a interligação de diferentes redes (denominados de *backbound*), e tem largura de banda superior aos ramos que se encontram mais próximos das folhas e que apenas interligam equipamentos da mesma rede.

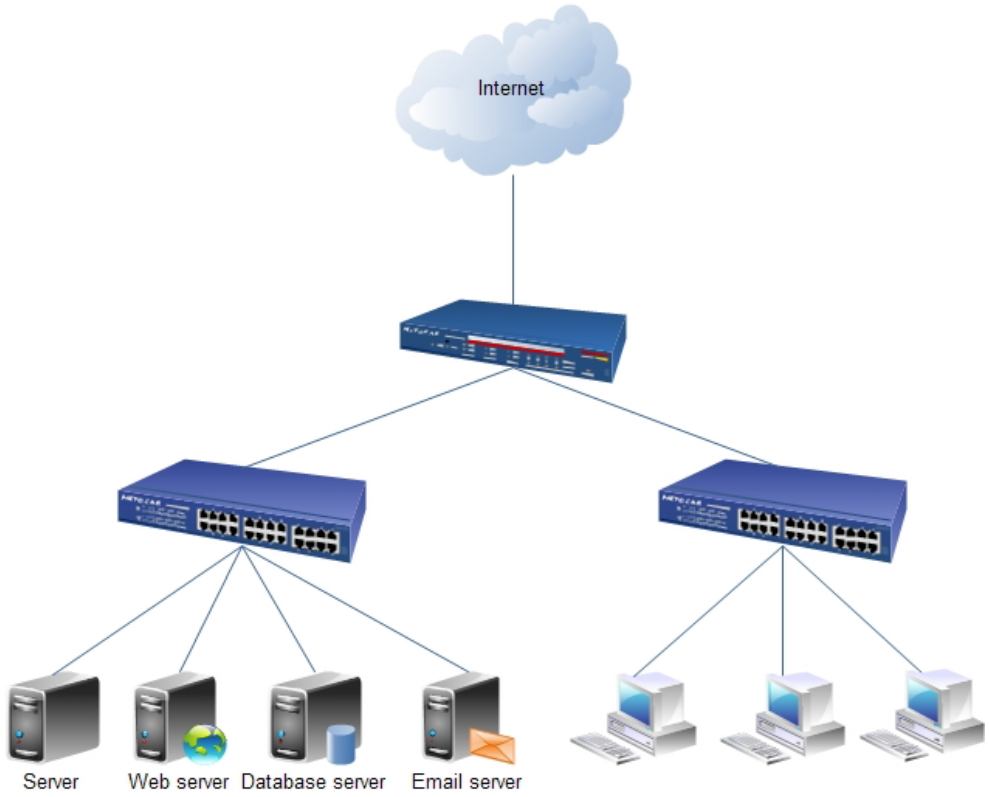

Figura 2.1: Topologia hierárquica de uma empresa

A figura 2.1 representa uma topologia onde são utilizadas várias redes no sentido de separar os equipamentos mais importantes (servidores) dos equipamentos que estão mais sujeitos a erros por parte dos utilizadores. Assim, para interligar equipamentos da mesma rede, apenas é necessário que o equipamento esteja preparado para nível 2 (switch). Para efectuar troca de pacotes entre as diferentes redes, é necessário equipamento de nível 3 (router).

Esta topologia tem a vantagem de permitir adicionar ou remover nós, sem a necessidade de serem efectuadas grandes alterações físicas, bastando que a nova estrutura que se pretende ligar apresente uma tipologia semelhante.

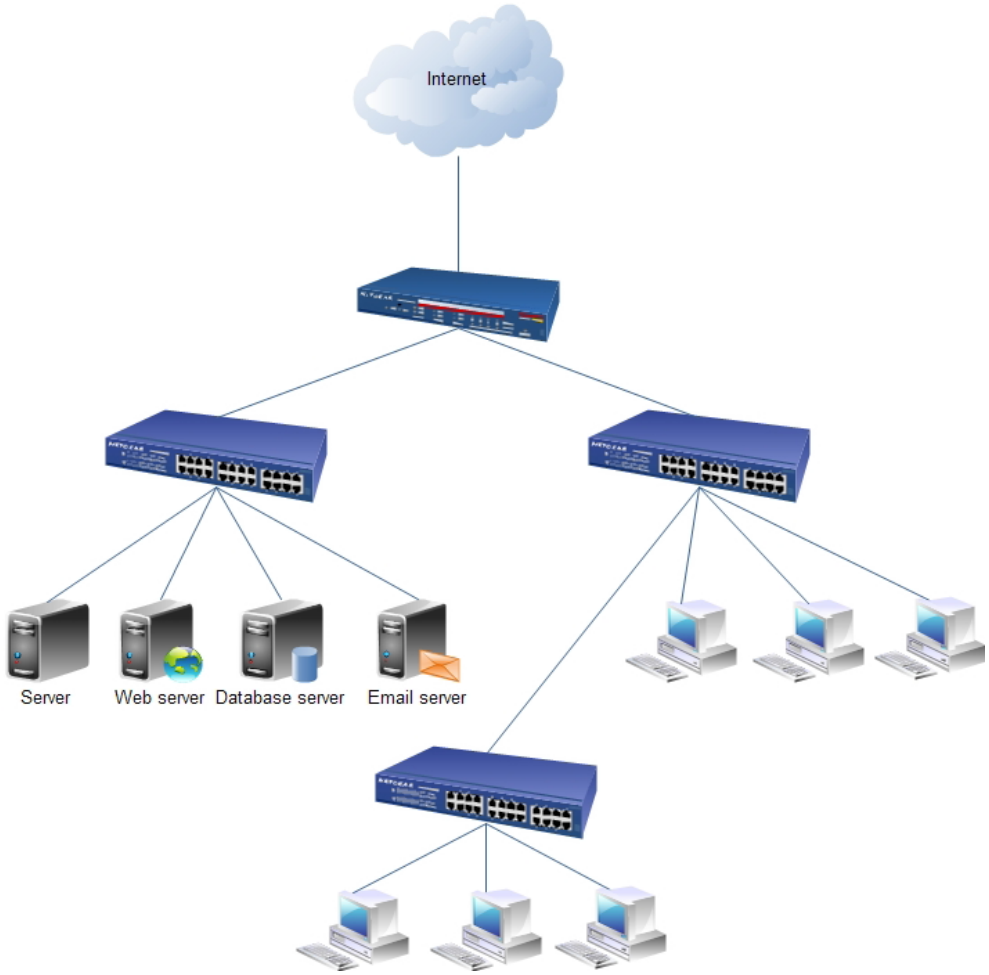

Figura 2.2: Topologia hierárquica de uma empresa com adição de mais um ramo

Neste caso, foi adicionada uma sub-árvore com apenas um nível de nós de rede.

2.3.2 Topologia entre sede e filiais

Com a utilização da Internet foi possível criar novas estruturas empresariais. Como mencionado anteriormente, as empresas decidiram centrar a informação toda num só distante e possibilitar, à que está longe, o acesso a esta informação. A decisão de guardar os dados num só local permite rentabilizar melhor os equipamentos e diminuir os custos de aquisição e manutenção.

Os locais remotos normalmente são filias da empresa, onde habitualmente a sua estrutura informática não é elevada, pois o número de utilizadores não requer muitos níveis na topologia de rede.

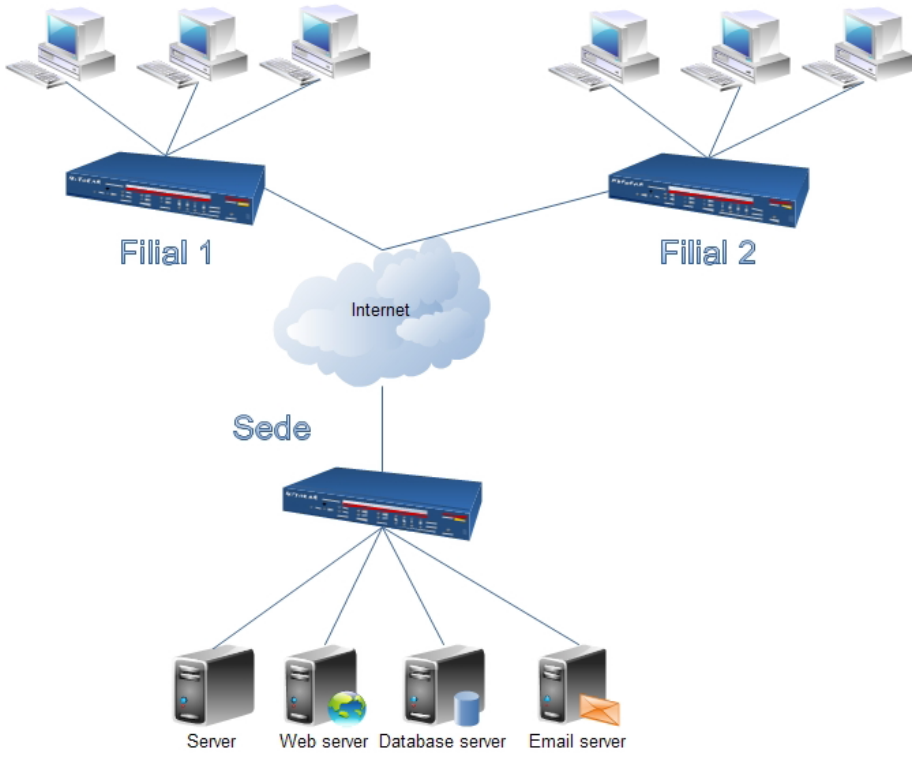

Figura 2.3: Topologia que liga a sede as filiais

No exemplo apenas é demonstrado que a sede contém servidores, contudo é possível haver máquinas cliente, mas apenas não foram representados. Há várias formas de ligar as filiais à sede, sendo a mais comum a VPN (*Virtual Private Network*).

2.3.3 Rede wireless

Como explicado anteriormente, as redes wireless não são mais do que redes normais, apenas sem a utilização de fios. Um exemplo muito simples de uma rede é o seguinte:

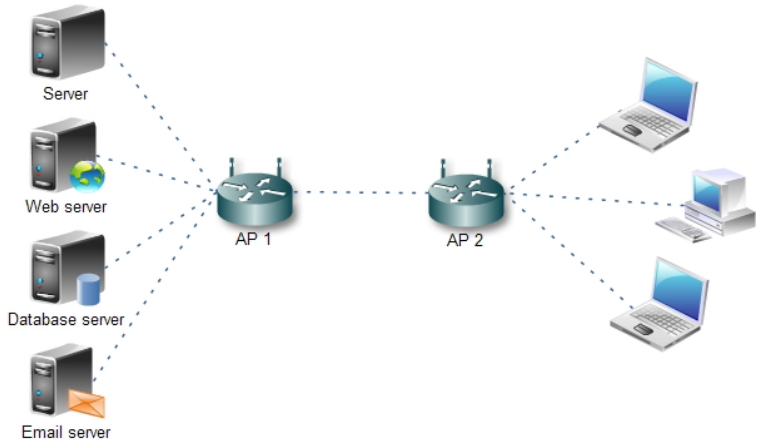

Figura 2.4: Exemplo de uma rede totalmente wireless

Neste exemplo é possível verificar que os computadores se encontram ligados aos APs e que estes se interligam entre si. Esta topologia não pode ser usada em empresas de alguma dimensão, pois não permite uma maior expansão (devido à necessidade que os AP têm de estarem próximos uns dos outros), como também não garante uma velocidade elevada e constante (com existência de interferências).

Outra das limitações trata-se de não permitir a mobilidade dos utilizadores sem perder a conectividade, pois cada equipamento portátil se encontra autenticado apenas num AP (sendo totalmente desconhecido por outros AP's). Contudo, em certos equipamentos que disponibilizam o protocolo RADIUS (*Remote Authentication Dial In User Service*) é possível definir que um deles seja o autenticador e que os outros APs não autentiquem, mas reencaminhem os pedidos para esse AP, permitindo ao utilizador mover-se sem perder a conectividade.

Normalmente a rede wireless é adicionada à rede física já existente, permitindo criar uma maior liberdade de escolha ao utilizador. Por exemplo, quando o utilizador se encontra no seu posto de trabalho, pode estar ligado através do cabo para obter uma maior qualidade de serviço, mas quando o utilizador se pretende mover dentro da empresa, pode utilizar a rede wireless para não perder a conectividade, como também pode aceder à rede no novo local onde se encontra (durante uma reunião).

Nesta topologia, os AP's passam a estar interligados entre si através do cabo, o que permite aumentar a velocidade de transferência de dados (comparativamente com o exemplo anterior), bem como colocá-los a uma distância superior para permitir uma maior cobertura, com o mesmo número de equipamentos.

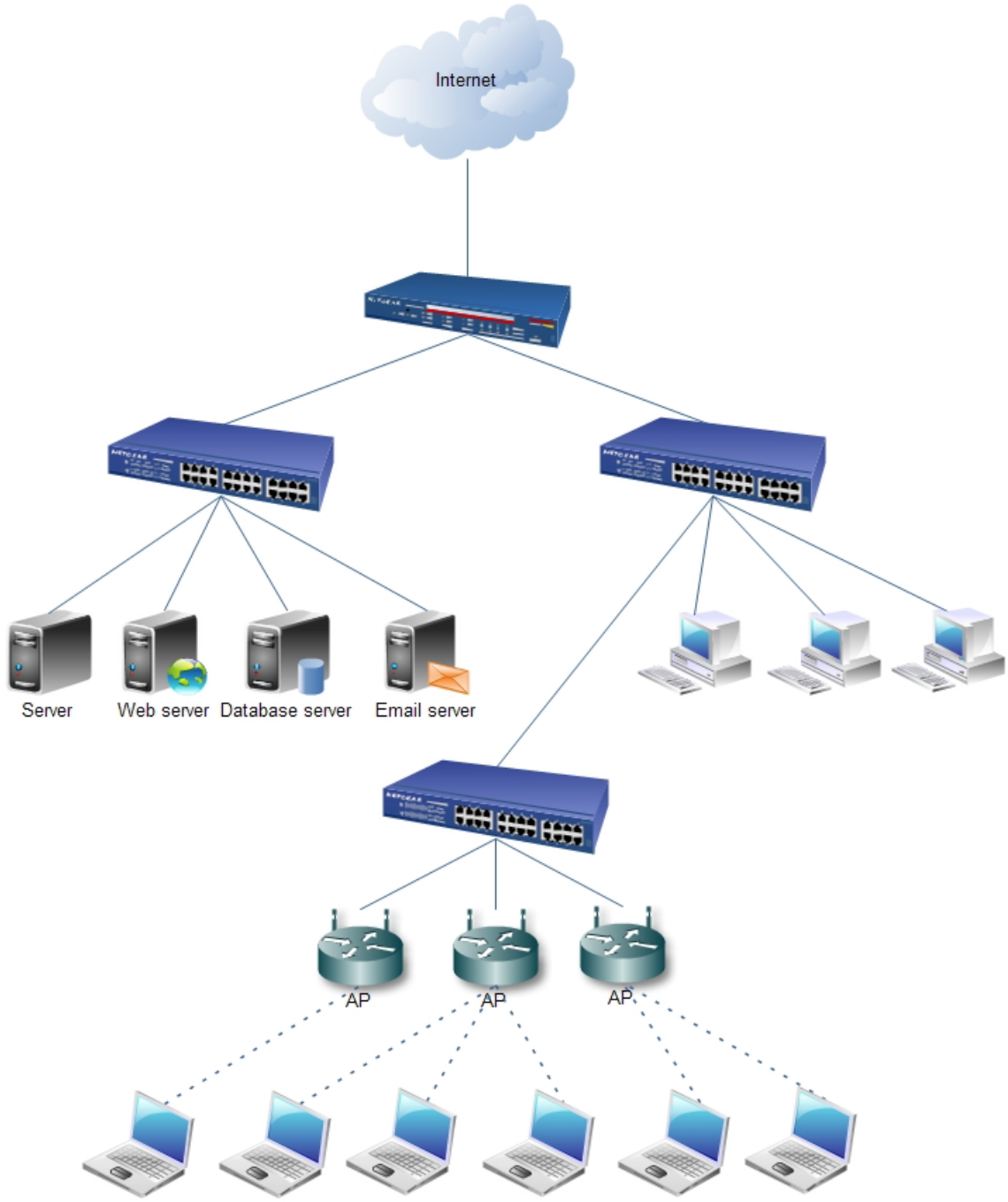

Figura 2.5: Exemplo de uma rede de cabo conjugada com uma rede wireless

Apesar de no exemplo os AP's estarem ligados ao mesmo switch, em termos funcionais não existe qualquer norma ou imperativo que assim obriga, isto é, é possível ligar um AP ao switch mais próximo fisicamente (desde que o mesmo esteja ligado correctamente a rede).

Tipicamente, o sistema de autenticação deixa de ser um AP passando a ser um servidor que executa essa função. Esse computador, poderá fazer a autenticação dos computadores que se ligam por cabo, como também a autenticação dos utilizadores nas aplicações com o

recurso, por exemplo, ao LDAP (*Lightweight Directory Access Protocol*). É indispensável que todos os AP's tenham o mesmo SSID, pois só assim será possível um utilizador estar ligado à mesma rede, passando por diversos AP's.

2.4 Aspectos de segurança

Um dos aspectos mais importantes na área de redes é a segurança dos dados que circulam entre os servidores e os clientes. Como tal, foram desenvolvidas algumas tecnologias e técnicas para minorar falhas de segurança, de forma a tornar transparente este processo para o utilizador normal.

2.4.1 Firewall

A firewall é a tecnologia mais comum e usada nas redes. A firewall consiste num programa que analisa todos os pacotes de dados que entram e saem da rede e, através de um conjunto de regras previamente criado, permite ou inibe a passagem desses pacotes. Essas regras podem ser alteradas de acordo com as necessidades da empresa, devendo contudo permitir o tráfego que é estritamente necessário para o funcionamento dos sistemas da empresa.

Inicialmente a firewall era implementada na fronteira (gateway) da rede privada com a rede pública, como o exemplo a seguir o demonstra.

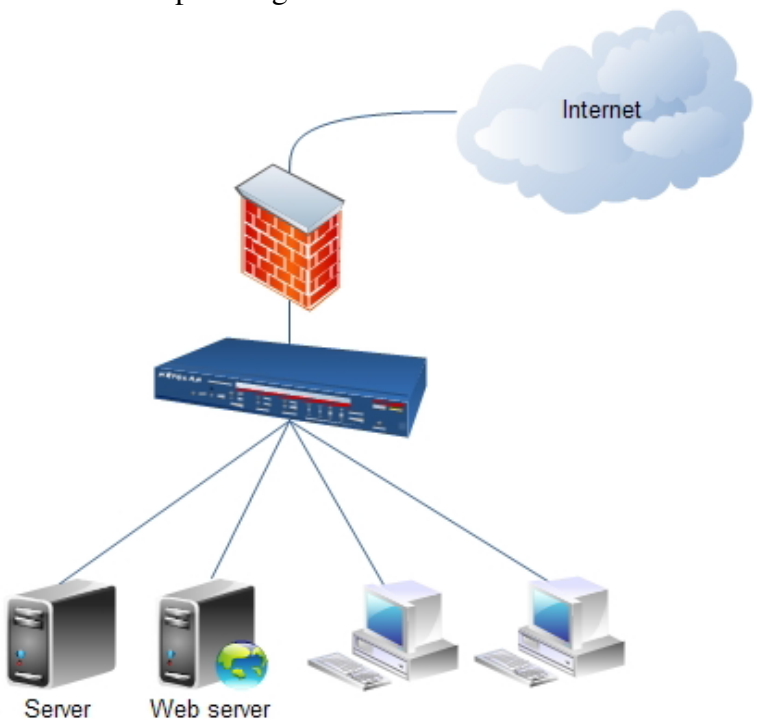

Figura 2.6: Exemplo de uma rede de com firewall

Ao longo dos anos as empresas têm apostado cada vez mais em implementar firewall entre as diversas redes e até nos próprios computadores, no sentido de aumentar a segurança da rede, permitindo criar um filtro ainda mais restrito para cada computador.

2.4.2 NAT

A tecnologia NAT (*Network Address Translation*) nasceu para colmatar a limitação da gama de endereços da rede IPv4 (*Internet Protocol version 4*) que com o crescente número de computadores, se tornava cada vez mais próximo do limite máximo de computadores que se podia ligar à Internet. Assim, em cada rede privada apenas é necessário um IP (designado por IP Público).

Quando um computador (da rede privada) tenta aceder à Internet, este deverá encaminhar o tráfego pela gateway da rede. A gateway (que tem a tecnologia NAT) irá substituir o endereço privado pelo seu endereço público e por um porto atribuído arbitrariamente. Depois, a informação do IP privado será guardada com o respectivo porto, no sentido de fazer a correspondência dos pacotes que entram na gateway vindo da rede externa, fazendo a respectiva correspondência com a máquina da rede interna.

Assim, com esta tecnologia é possível ligar cerca de 65536 (2^{16}) computadores de uma rede privada, apenas com um endereço público, o que permite retardar o esgotamento total de endereços (que se prevê que ocorra no fim de 2011)

Esta tecnologia pode ser vista como uma segurança extra, uma vez que esconde para o exterior qual o IP que realizou o pedido, pois a tabela que permite fazer a correspondência entre o IP e o porto, apenas é visível para o equipamento de NAT.

A limitação desta tecnologia, para além do limite máximo, é de apenas reconhecer protocolos TCP e UDP, que permite correr a maior parte dos serviços que os utilizadores fazem uso, mas limita ou impossibilita a execução de outros.

2.4.3 Proxy

Um proxy é um servidor que atende a pedidos efectuados pelos clientes e reencaminha os pedidos, agindo por interposta pessoa. Um cliente liga-se ao servidor proxy e requisita um determinado serviço e caso este se encontre em cache, irá entregar imediatamente ao cliente. Caso não se encontre, o proxy irá buscar os dados (pela vez do cliente) e irá entregar os mesmos ao cliente, guardando uma cópia desses dados em cache.

Uma das principais vantagens é aumentar a velocidade de navegação dos utilizadores, pois caso um segundo cliente pretenda obter os dados que anteriormente já foram requisitos, apenas será necessário realizar a transferência do proxy para o cliente. Outra vantagem é a redução do uso da banda de acesso à Internet e de reduzir o tráfego gerado, permitindo uma maior gestão.

Como os pedidos dos cliente são efectuados pelo proxy, na prática, quem se encontra fora da rede desconhece qual o equipamento que está a realizar o pedido, podendo ser considerado uma medida de segurança.

Outra funcionalidade importante do proxy, é de limitar o acesso dos utilizadores a determinados sites que podem consumir demasiada largura de banda a rede, como também a sites onde o conteúdo presente nos mesmos pode ser considerado malicioso. Neste tipo de software, é também possível verificar e gerar relatórios sobre o tráfego que cada computador utiliza. Para além disso, permite implementar filtros para limitar o acesso a determinados utilizadores, caso não vá de encontro com a política da empresa (como por exemplo o YouTube).

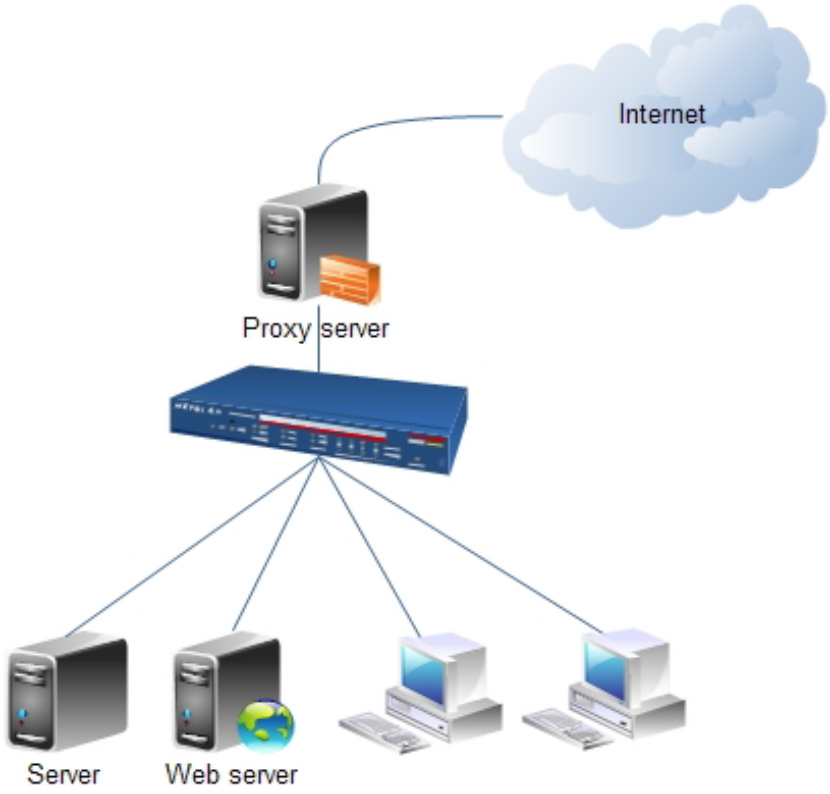

Figura 2.7: Exemplo de uma rede de com proxy server

2.4.4 DMZ

A DMZ (*DeMilitared Zone*) é um termo de origem militar que significa "zona desmilitarizada". Esta região representa uma área (sem limite definido) que separa dois territórios inimigos.

Partindo desta ideia e com o objectivo de aumentar a segurança, desenvolveu-se uma técnica bastante semelhante, isto é, entre a rede confiável (rede local) e a rede não confiável (rede Internet), cria-se uma zona onde apenas estejam equipamentos que necessitam de comunicar com a rede interna e com a rede externa.

Desta forma, todas as máquinas da rede interna que queiram aceder ao exterior, terão que encaminhar o seu pedido para uma das máquinas que se encontram na DMZ, e este é que fará o pedido ao exterior, tornando assim a rede local menos exposta a ataques.

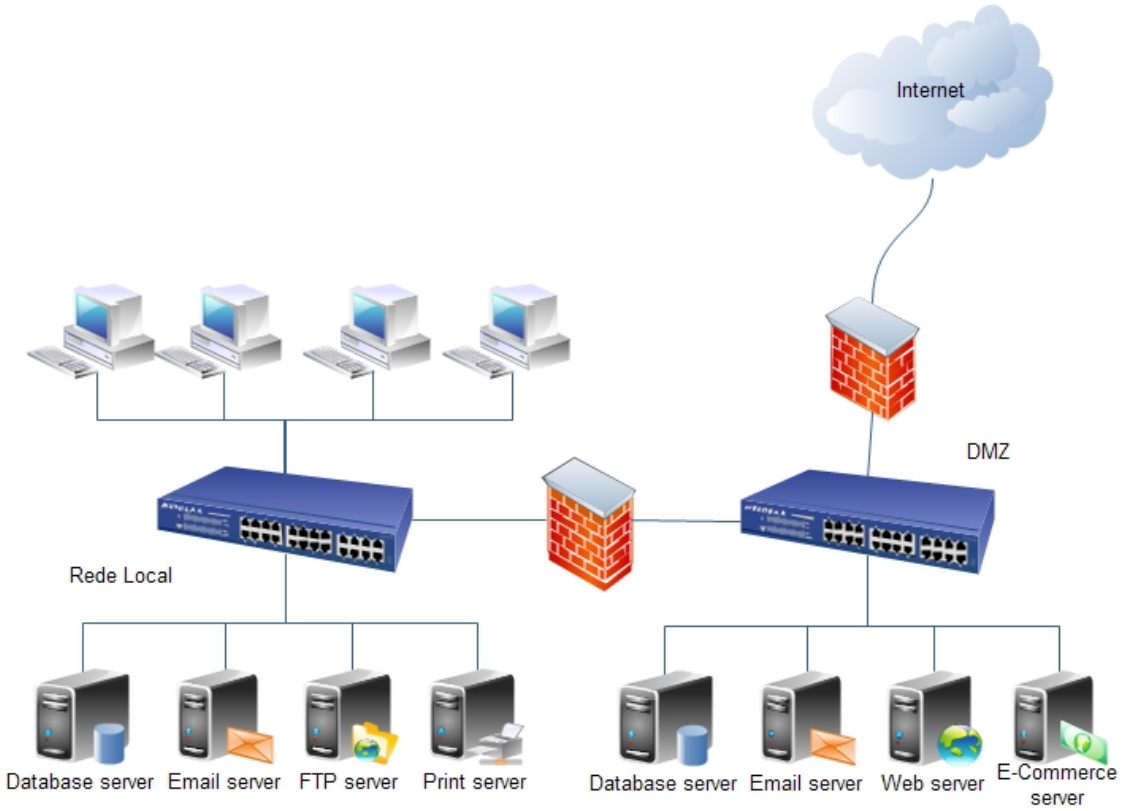

Figura 2.8: Exemplo de uma rede de com uma DMZ

Normalmente, os equipamentos que se encontram na DMZ não substituem os equipamentos da rede local, isto é, caso seja implementado um servidor de e-mail na DMZ, terá que haver um servidor de e-mail na rede local. Isto ocorre devido aos computadores das redes locais não comunicarem directamente com os equipamentos da DMZ; estes fazem o pedido ao servidor que se encontra na sua rede local e este é que fará o reencaminhamento para o computador na DMZ.

Desta forma deixa de haver a necessidade de controlar várias ligações da rede local para a rede DMZ, passam apenas a haver tantas quantos equipamentos existam na DMZ [Git09].

2.4.5 VLAN

As VLANs (*Virtual Local Area Network*) permitem criar redes virtuais. Esta tecnologia nasceu há vários anos, mas só recentemente é que começou a ser mais utilizada, devido ao aumento do tamanho das redes LAN e também pela necessidade de manter os

custos de implementação mais baixos, sem a necessidade de sacrificar a segurança ou a performance da rede.

Antes da existência das VLANs, e sempre que se pretendia ligar duas redes diferentes, era necessário que os equipamentos da mesma rede tivessem ligados a switches diferentes, como a figura seguinte o demonstra

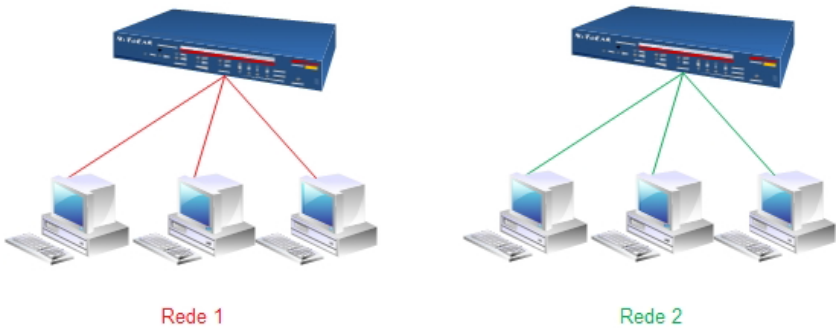

Figura 2.9: Topologia de duas redes sem VLANs

Como é normal nestas redes, não existe comunicação entre os equipamentos de redes diferentes, pois teoricamente não existe conectividade entre os switches, mas mesmo que existisse seria necessário um equipamento de nível 3 para poder fazer o encaminhamento dos pacotes de uma rede para outra.

Com a criação das VLANs, esta topologia de rede pode ser desempenhada apenas com um equipamento.

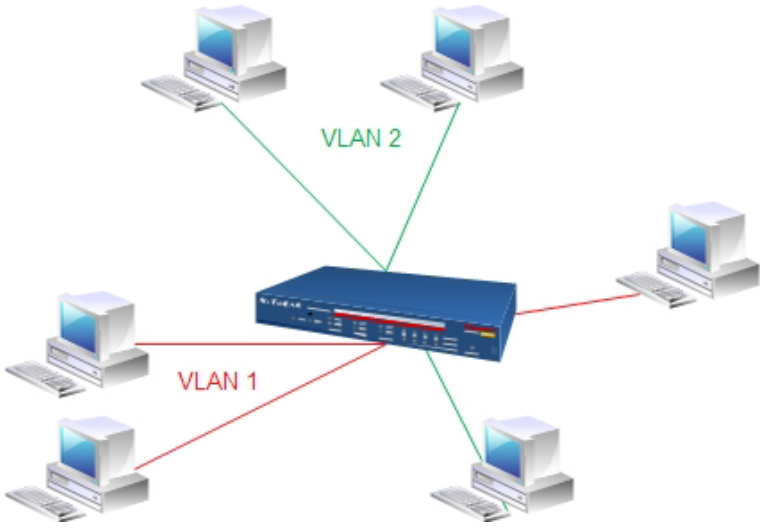

Figura 2.10: Topologia de duas redes com VLANs

As VLANs apresentam as mesmas características das redes normais, pois os pacotes com destino a rede VLAN1 não transitam para a VLAN2. Esta tecnologia apresenta a vantagem de diminuição de custos de implementação de uma rede (quer em equipamentos, quer em cabos) como também permite criar redes mais pequenas, diminuindo o domínio de colisões. Apesar de o equipamento ser o mesmo, é necessário

que tenha implementada a camada lógica de nível 3, pois só esta permite realizar troca de pacotes entre redes diferentes.

Normalmente, a rede nas empresas encontra-se dividida conforme os departamentos da mesma. Desta forma é garantido que o domínio de colisão é mais pequeno. Para além disso, os dados de um departamento não circulam por outros departamentos, evitando colocar a informação em risco.

Se pensarmos numa empresa que possui três departamentos, dispersos por três andares, seria possível atribuir um andar para cada departamento e assim só seria necessário criar uma rede para cada andar, para poder isolar as diferentes redes. Contudo, esta situação não acontece com frequência pois podem existir elementos de departamentos diferentes que precisam de trabalhar proximamente, como também podem existir restrições de espaço (como por exemplo um departamento ter a necessidade de ocupar um andar e meio).

Partindo então do principio que os três departamentos tem elementos nos três andares, torna-se necessário que existam três redes por andar. As empresas também possuem um *data center*, local esse que centra a informação da empresa e que no exemplo seguinte se encontra no rés-do-chão. [Fir09a]

A imagem seguinte, pretende resumir um pouco a descrição do problema.

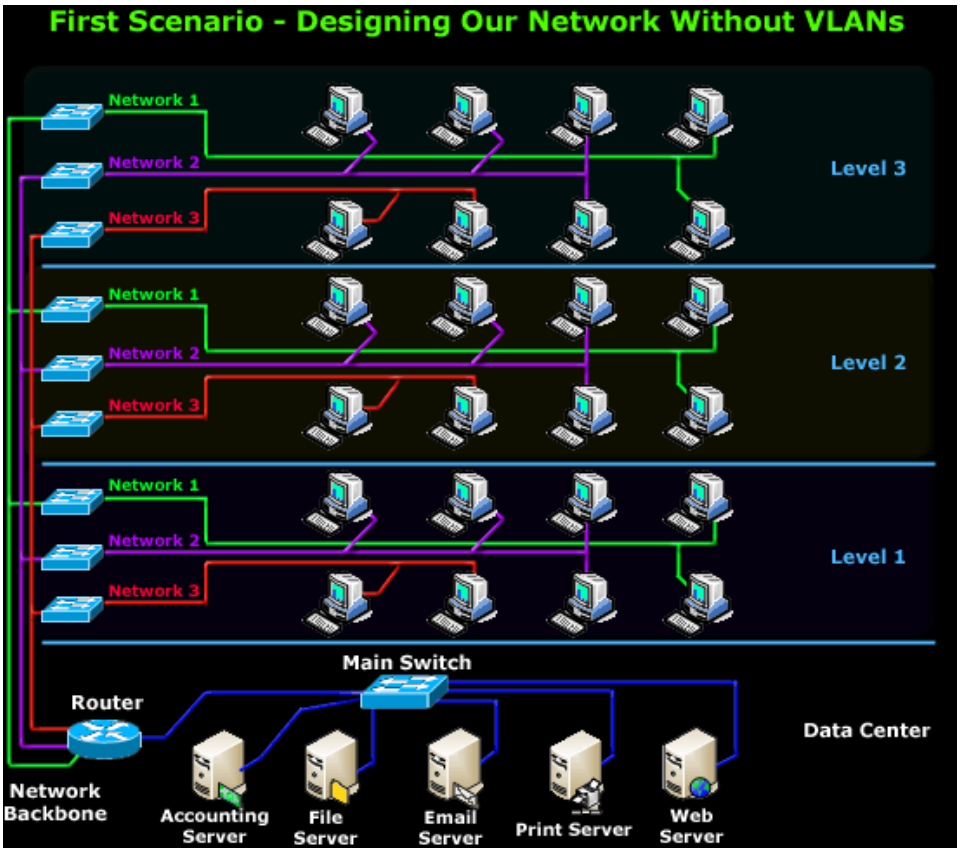

Figura 2.11: Topologia empresarial sem VLANs

Como é possível verificar, para implementar esta rede é necessário que existam três switches por andar (para ligar cada rede), e um switch para ligar a rede dos servidores (*data center*). Como as redes para comunicar entre si necessitam de um equipamento de nível 3, é necessária a implementação de um router, que no exemplo vai ficar instalado no mesmo andar dos servidores.

Com o desenvolvimento da VLAN, deixaria de ser necessário 10 switches para criar toda a rede, passando a serem necessários apenas 3 switches (um por andar), mantendo na mesma o router para interligação das redes. Desta solução, surgiriam algumas vantagens, tais como deixar de ser necessário comprar equipamento com tanta frequência, e passar a ser preciso apenas um cabo por cada andar (e não três como a solução inicial apresentava).

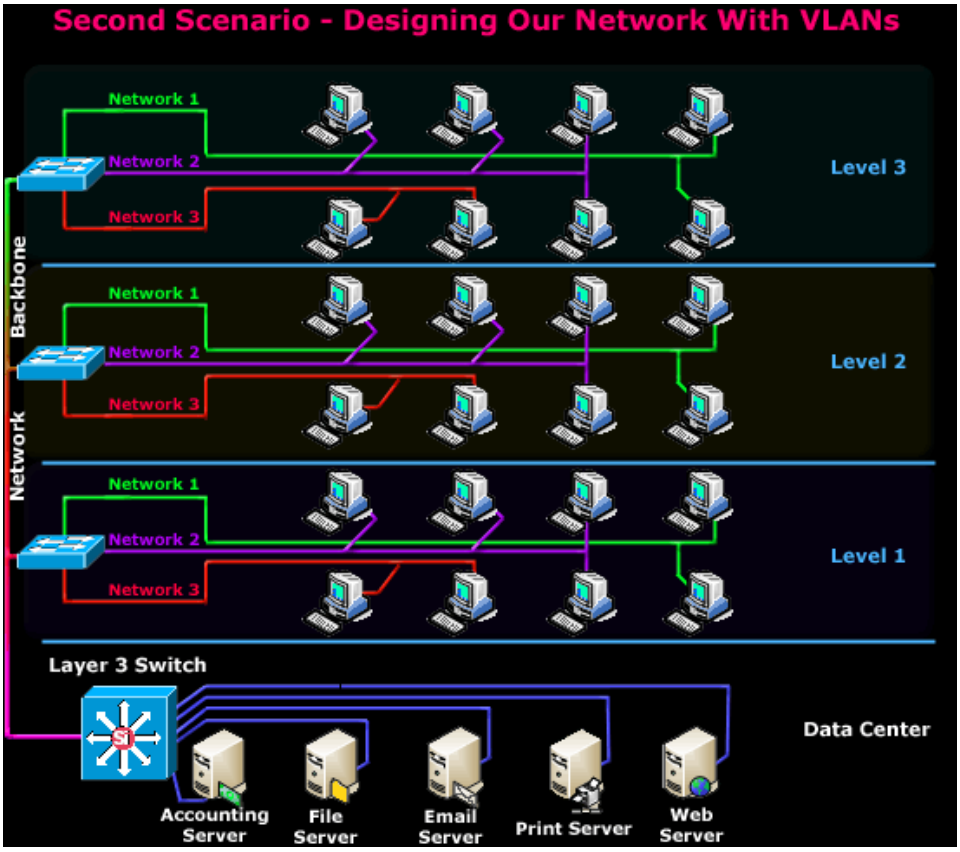

Figura 2.12: Topologia empresarial sem VLANs

A imagem anterior pretende resumir de forma esquemática a simplificação da rede. Existem também outras características que se podem associar à rede, como por exemplo a redução de calor gerado pelos diversos equipamentos, que não só contribui para a diminuição da factura energética, como também diminui a necessidade de criar sistemas de refrigeração. Outra vantagem da nova topologia em relação à anterior, consiste na possibilidade de haver orçamento para a implementação de serviços redundantes, que se torna bastante importante nos dias de hoje, numa empresa.

A implementação de VLAN na rede pode ser realizada através de VLAN estáticas ou

VLAN dinâmicas. Ambas as possibilidades tem as suas vantagens e desvantagens, tendo em conta a flexibilidade.

A VLAN estática defini-se por atribuir a cada porta do switch uma VLAN. Qualquer computador que se liga a essa porta, passa a pertencer a essa VLAN, independentemente do IP que tenha atribuído (IP de outra rede). Esta VLAN tem como principal vantagem a facilidade de implementação. Por outro lado, limita o utilizador que está em constante mudança dentro de um edifício, pois apenas se pode ligar a tomadas da sua rede (que podem não existir para o ponto a que se desloca).

A VLAN dinâmica caracteriza-se por permitir uma maior flexibilidade, bem como uma maior complexidade. Neste caso, não é atribuida uma VLAN a cada porta, mas passa a existir um servidor central que terá que guardar a informação sobre cada computador. Um servidor deste género denomina-se por VMPS (*VLAN Management Policy Server*) que guarda numa tabela a informação de cada MAC Address (*Media Access Control address*) e a VLAN associada. Assim, sempre que um cliente se ligue a uma tomada, o switch que gere a tomada pergunta ao servidor VMPS qual a VLAN que deve atribuir. Se a entrada existir, o servidor informa o switch e este atribui a VLAN ao cliente. A complexidade reside na necessidade de o servidor ter conhecimento prévio de todos os MAC address da empresa, o que a ser implementado numa rede de grande dimensão requer muito trabalho e esforço. Outro facto, é que cada vez que um computador se liga a uma porta, o switch vai interrogar o servidor, gerando tráfego na rede. Se os clientes trocarem frequentemente de lugar, produz tráfego a ponto de degradar a qualidade da rede.

Entrada	VLAN	MAC address
1	2	5D:FF:68:DE:22:0A
2	4	5A:09:DF:FF:41:12
3	4	1A:B4:4F:CC:35:32
4	12	8E:E3:FA:C8:B2:63
5	4	F2:3D:A9:00:37:42
6	4	C4:72:36:FF:A2:61
7	12	5B:90:03:BB:BC:25
8	12	B9:42:27:A3:7F:1F
9	2	DD:0D:26:52:78:35
10	2	C4:42:25:1F:DA:94

Tabela 2.1: Exemplo de entradas num servidor VMPS

Nesta tabela pretende-se ilustrar a informação que é guardada num servidor VMPS, no qual terão de existir tantas entradas, quantas placas de rede existam na empresa.

2.4.6 Tipos de autenticação wireless

O padrão IEEE 802.1x é um padrão do IEEE (*Institute of Eelctrical and Electronics Engineers*) que define mecanismos para autenticação na segunda camada de rede através do RADIUS [Sch09]. O 802.1x permite que seja utilizado o protocolo EAP (*Extensible Authentication Protocol*), o qual permite que possam ser usados os seguintes métodos de autenticação:

- **EAP-TLS**: A segurança do protocolo TLS (*Transport Layer Security*) acenta sobre o SSL (*Secure Sockets Layer*). Este utiliza a criptografia PKI (*Public Key Infrastructure*) para proteger a comunicação entre o autenticador e o servidor de autenticação. A autenticação é assente sobre a forma de certificados (previamente instalado no lado do cliente), podendo o certificado do cliente ser substituído por um *smart cards*, permitindo aumentar a segurança da rede (pois torna-se necessário retirar o cartão do utilizador para conseguir aceder a rede).

- **EAP-TTLS**: O TTLS (*Tunneled Transport Layer Security*) é uma extensão do protocolo TLS que é amplamente usado e suporta todos os sistemas operativos. Contudo, no Windows ainda não existe um suporte de raíz, sendo necessária a instalação do programa SecureW2. Apenas é preciso que exista um certificado por parte do servidor (deixando de ser necessário no cliente) deforma a criar um túnel encriptado para permitir a autenticação do cliente. O cliente para se autenticar, necessita de possuir um username e password.

- **EAP-PSK**: Este protocolo utiliza uma chave de sessão com uma chave pré-partilhada (*Pre-Shared Key*), e fornece um canal de comunicação protegido quando a autenticação é realizada com sucesso por ambas as partes. O protocolo encontra-se documentado em RFC (*Request for Comments*) experimental e exige que no mínimo sejam realizadas quatro trocas de mensagens (*four-way handshake*).

- **EAP-MD5**: Este é um protocolo que oferece uma segurança mínima, pois a função de hash MD5 (*Message-Digest algorithm 5*) é extremamente vulnerável a ataques de dicionário e não suporta a geração de uma chave, o que torna inadequado para ser usado como WEP (*Wired Equivalent Privacy*) dinâmico ou WPA (*Wi-Fi Protected Access*). Diferencia-se dos outros métodos EAP fornecendo apenas autenticação do ponto EAP para o servidor EAP, mas não com autenticação mútua.

- **PEAP**: O padrão PEAP (*Protected Extensible Authentication Protocol*) foi criado pela Microsoft, Cisco e RSA Security como um padrão aberto. Encontra-se amplamente divulgado e disponível em diversos produtos. É semelhante ao EAP-TTLS requerendo apenas um certificado PKI do lado do servidor para criar um túnel TLS seguro para proteger a autenticação do usuário. A partir de Maio de 2005

passa a existir 2 sub-tipos de PEAP que foram actualizados para o padrões do WPA e WPA2, passando a designar-se EAP-MSCHAPv2 e EAP-GTC, respectivamente.

- **EAP-MSCHAPv2**: Este protocolo é amplamente usado existindo diversas implementações em produtos da Microsoft, Cisco, Apple e Linux. O processo de autenticação é realizado em 2 fases. Numa primeira fase é criado um canal seguro (TLS) entre o autenticador e o servidor, e numa segunda fase é criado uma autenticação EAP entre o cliente EAP e o autenticador. A autenticação deste protocolo é baseada em username e password.
- **EAP-GTC**: Protocolo criado pela Cisco como alternativa ao EAP-MSCHAPv2 que realiza um desafio de texto ao servidor de autenticação, e uma resposta que se assume ser gerada por um *token* de segurança. Este método não protege os dados de autenticação.

2.5 Exemplos de redes wireless

Nesta secção são apresentados alguns exemplos de redes wireless existentes na cidade do Porto. Estes exemplos têm como base demonstrar o que já existe implementado, tendo em conta os serviços que oferecem e o tipo de utilizadores a que se destina.

2.5.1 FEUP

Na rede da FEUP é possível observar duas redes diferentes.

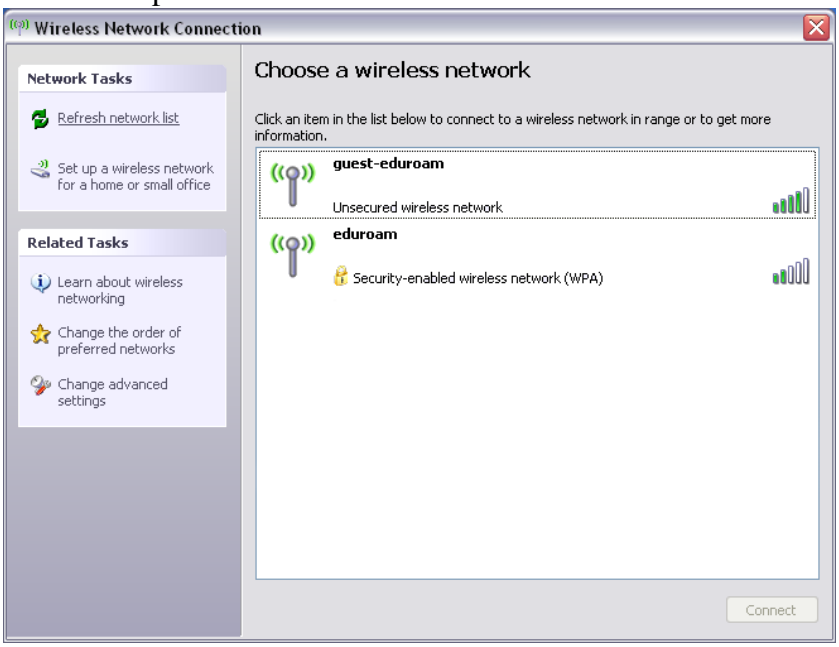

Figura 2.13: Redes wireless disponíveis na FEUP

A rede "eduroam" (*Education Roaming*) é uma rede europeia criada entre diversas universidades e centros de investigação para disponibilizar um serviço de mobilidade entre os diversos campus universitários. Assim, passa a ser possível que um membro de uma dada instituição possa utilizar a infra-estrutura de outra instituição sem a necessidade de obter novas credenciais.

Esta rede encontra-se encriptada, sendo a sua autenticação realizada através do protocolo de RADIUS. Os tipos de autenticação podem diferenciar de instituição para instituição, mas normalmente é usado o EAP-MSCHAPv2 ou o TTLS. As credenciais usadas são,geralmente, o username e a password da instituição de origem. Durante o processo de autenticação é necessário indicar qual o realm do utilizador, isto é, é preciso que o utilizador indique qual a instituição a que pertence, para além do seu nome de utilizador. Normalmente o login apresenta-se na forma de *teste@fe.up.pt*.

Esta informação tem como objectivo identificar a que servidor de RADIUS deverá ser encaminhado o pedido de autenticação. No caso Português, quando um utilizador tenta autenticar-se na rede eduroam sem qualquer realm, será tratado pelo próprio servidor. Quando o utilizador indica qual o realm (e este não for da sua rede) o processo de autenticação para o servidor de RADIUS da FCCN (Fundação para a Computação Científica Nacional), que fará o encaminhamento para a instituição correcta.

A maioria dos utilizadores desta rede pertencem a esta instituição e como tal, têm acesso a um conjunto de serviços que a faculdade lhes proporciona. A cada utilizador é atribuído um endereço privado que lhe permite efectuar a larga maioria das suas actividades. Existe ainda um conjunto de utilizadores que pertencem a outras faculdades e que se ligam à rede "eduroam" no sentido de ter acesso à Internet. Estes utilizadores são externos (também designado por utilizadores em roaming), e a eles é atribuído um endereço público. A questão da diferença de tipos de endereços, prende-se com a necessidade de facilitar ao utilizador a ligação VPN à sua instituição de origem. Esta questão será abordada no momento em que explicarei as diferenças entre endereços privado e público.

A outra rede é a "eduroam-guest" que é uma rede aberta que apenas tem como finalidade permitir que os utilizadores acedam a informação importante sobre como configurar a sua máquina para aceder a rede "eduroam". No caso da FEUP, o manual de instruções é bastante explicativo, cobrindo um conjunto diverso de equipamentos que podem aceder à rede e permitindo também que os seus utilizadores façam download do certificado digital (caso o pretendam usar).

2.5.2 UPtec

A UPtec - Parque de Ciência e Tecnologia da Universidade do Porto é a incubadora tecnológica da Universidade do Porto, a qual disponibiliza um espaço de valorização

mútua de competências entre os universitários e o meio empresarial.

Neste espaço, um dos serviços disponíveis é o acesso à Internet através da rede wireless. Assim é possível encontrar a rede "eduroam" e a rede "UPTec". Contudo, são visualizadas outras redes neste local, que não fazem parte da instituição em causa, encontrando-se em entidades vizinhas.

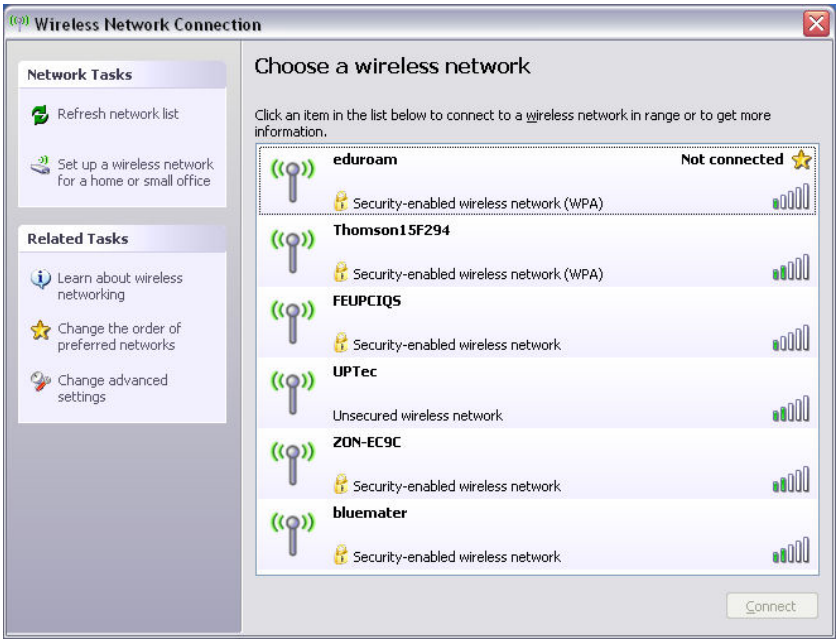

Figura 2.14: Redes wireless disponíveis na UPTec

A rede "UPTec" não se encontra encriptada, permitindo que qualquer utilizador se ligue a esta rede. Todavia, nenhum serviço se encontra disponível até o cliente tentar aceder a uma página web. Como o sistema detecta que o cliente não está autenticado, a página pretendida será redireccionada para a página de login, como o exemplo a seguir.

Figura 2.15: Página de autenticação do hotspot da UPTec

Nesta página é necessário inserir as credenciais válidas para poder aceder à Internet. Neste caso em específico, as credenciais são as mesmas para todos os utilizadores da UPTec, contudo, era possível criar credenciais para cada um dos utilizadores.

Esta característica de autenticação é normalmente usada para hotspots, pois simplifica do lado do cliente as configurações necessárias para aceder à rede. Outra das vantagens é possibilitar que o cliente possa aceder a outras páginas importantes sem estar autenticado (como a página de compra de créditos ou na obtenção de um username e password válidos).

Nesta rede não existe qualquer restrição de serviço, havendo, contudo, uma limitação ao nível da velocidade de acesso, pois o padrão de redes utilizado é norma 802.11b, limitando a velocidade máxima de acesso a 11 Mbit/s, razão a qual desconheço se é realizada propositadamente ou se é devido a limitações de hardware (baixo custo de implementação).

Observando a barra de endereços da página de login é possível evidenciar que o acesso é controlado por um software de hotspot como por exemplo o ChilliSpot. Após realizar-se login, o resultado é o seguinte:

Figura 2.16: Página de após ter realizado o login na rede

Nesta página é indicado que foi efectuado login com sucesso e passa a ser possível navegar na Internet. Para além disso, é também aberto um *pop-up* onde é apresentado um link para a pessoa poder realizar logout (quando pretender), sendo o link o que se apresenta no canto inferior esquerdo. Esta mesma página indica que caso a pessoa não faça logout, o mesmo será realizado pelo sistema de forma a garantir a segurança de acesso à rede.

2.5.3 Cidade do Porto

Com o intuito de atrair pessoas, a cidade do Porto passou a disponibilizar gratuitamente o acesso à Internet em diversos pontos da cidade. A rede que se encontra disponível ao público denomina-se "Wifi Porto Digital" e caracteriza-se por ser uma rede aberta. O ponto de captura desta rede foi a Avenida dos Aliados. Nessa mesma altura era possível obter mais três redes wireless, mas não estavam relacionadas com o projecto Porto Digital.

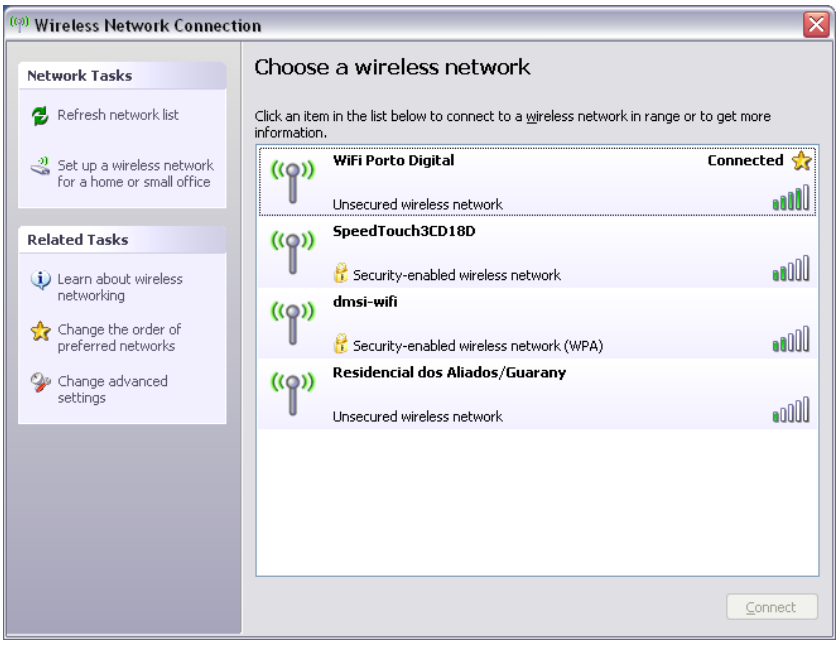

Figura 2.17: Redes wireless disponíveis na Avenida dos Aliados

Após realizar a ligação a rede e abrir um browser, o mesmo é redireccionado para uma página de entrada, tal como acontece na rede UPtec. Nesta página é pedido que o cliente efectue login, e são apresentadas as instruções de acesso. Caso o utilizador clique no botão "login" passa a dispor do tempo de uma hora, no qual pode aceder a qualquer tipo de serviço. Finda essa hora, o utilizador terá que esperar uma hora para poder aceder novamente à rede. Esta medida é utilizada para diminuir o abuso da rede wireless por parte dos utilizadores.

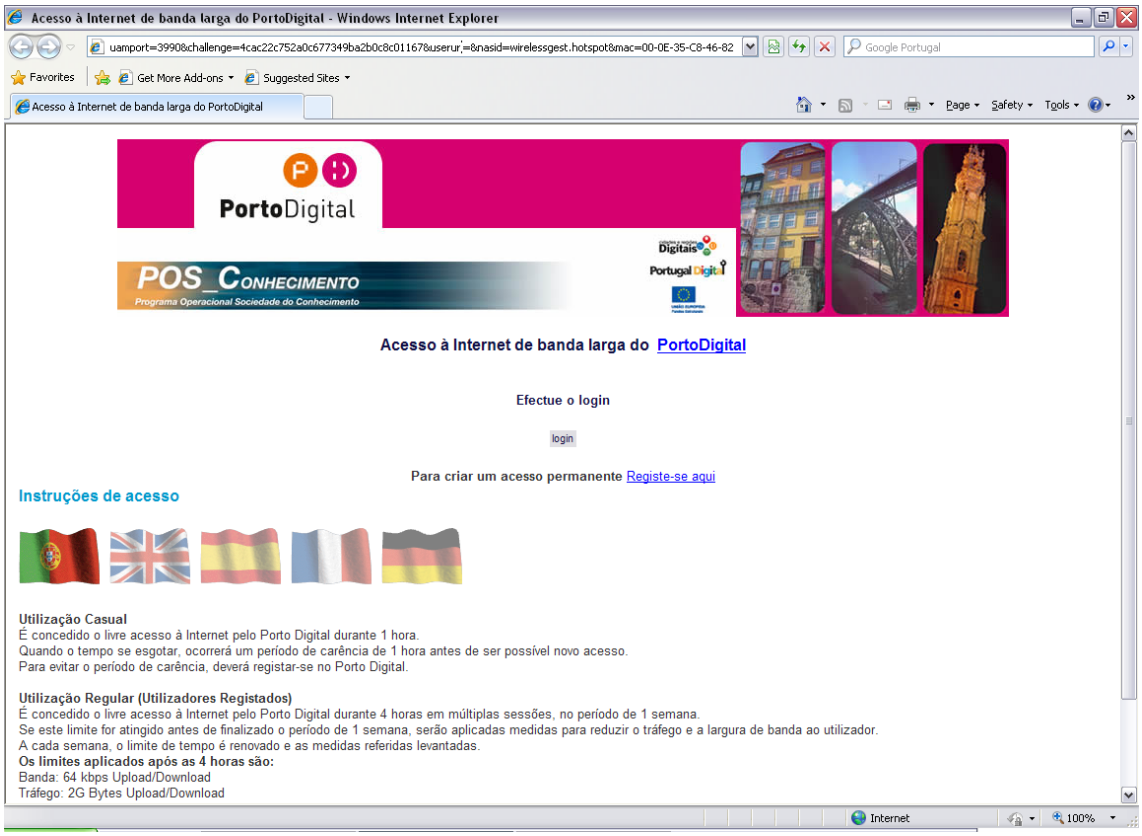

Figura 2.18: Página de autenticação do hotspot da UPTec

No entando, é possível ao utilizador ter um acesso mais prolongado, bastando para isso que se registe no site. O utilizador passa a dispor de quatro horas semanais em sessões múltiplas. Quer isto dizer, que desde que o cliente se registe até uma semana, o cliente pode aceder à Internet por diversas sessões, desde que o somatório do tempo não ultrapasse as quatro horas. Ao ultrapassar este limite, passa a ser imposta uma medida de contenção que se traduz numa redução da largura de banda e a contabilização do tráfego gerado (upload e download). Após uma semana de registo, o utilizador pode registar-se novamente, passando a usufruir das mesmas quatro horas.

A página de registo é bastante simples (figura 2.19) e são poucos os dados pedidos ao utilizador. Apesar de ser pedido o e-mail, nada é enviado para o mesmo a indicar que o registo foi efectuado com sucesso. Entretanto, se o mesmo utilizador tentar registar-se novamente com o mesmo endereço de e-mail num espaço de tempo inferior a uma semana, o sistema indica que esse mesmo utilizador já se encontra registado e que não é possível novo registo.

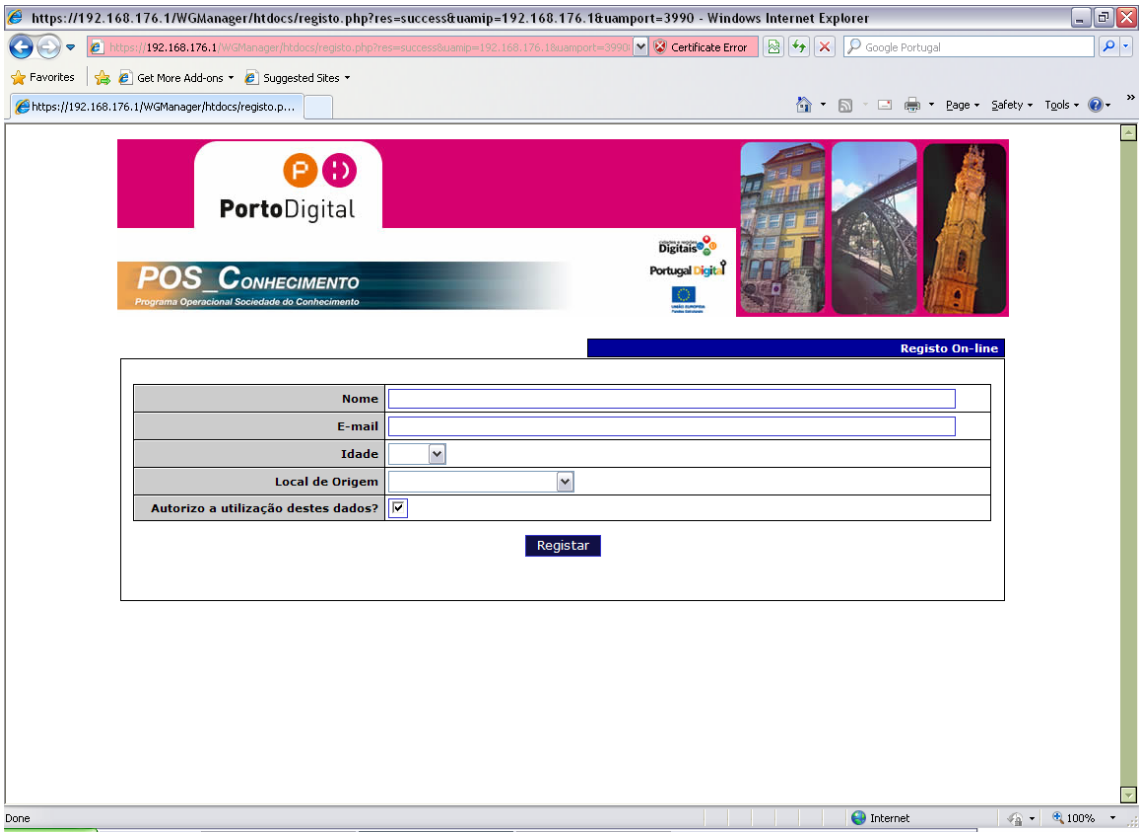

Figura 2.19: Página de registo do hotspot

Após a conclusão do registo, somos redireccionados para uma página final a indicar que foi realizado com sucesso o login na rede. Para além disso, é apresentado o link necessário para efectuar o logout (e parar a contagem), e também é aberta uma *pop-up* a indicar o tempo restante de utilização. Na imagem seguinte é possível ver as informações sobre o link e o tempo restante em falta.

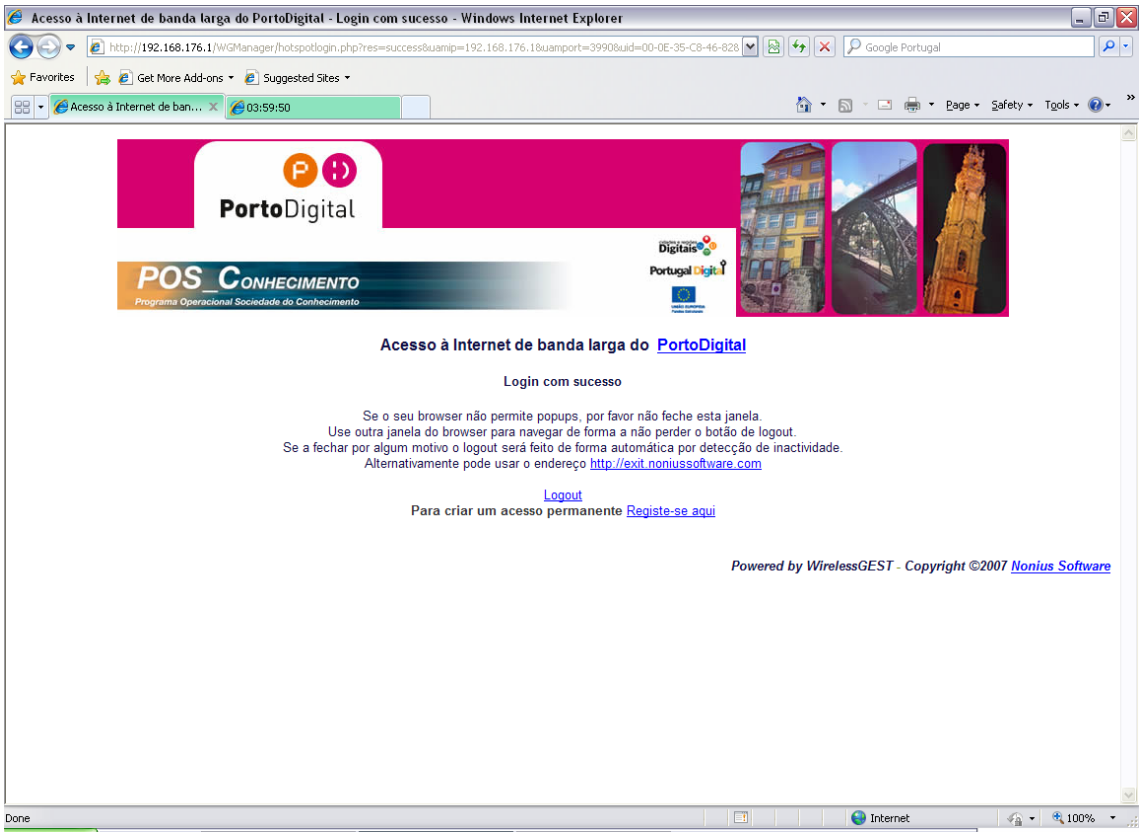

Figura 2.20: Página de autenticação do hotspot da UPTec

Nesta última imagem é possível verificar que a empresa que desenvolveu este sistema é a mesma que desenvolveu o sistema de hotspot para a rede UPtec. A Nonius Software é uma empresa fabricante de equipamentos de telecomunicações e criação de soluções para gestão de acesso à Internet. Trata-se de uma empresa portuguesa sediada na UPtec, e que criou o produto WirelessGEST [Sof09].

2.5.4 NorteShopping

No centro comercial NorteShopping é possível aceder a rede wireless na zona da restauração. Nesta área, apesar de surgirem diversas redes, os utilizadores apenas têm acesso a duas delas, sendo as restantes de lojas que se encontram nas imediações e naturalmente são privadas.

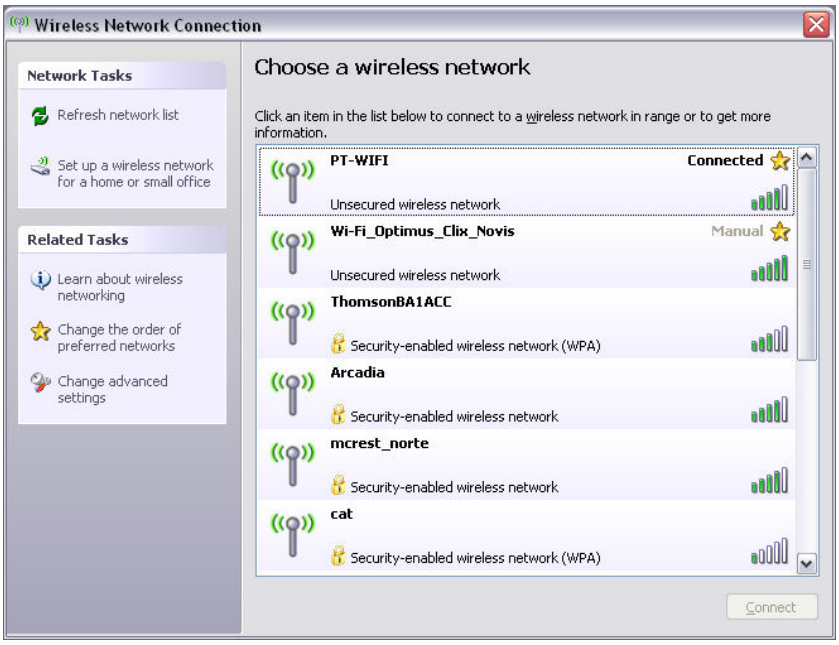

Figura 2.21: Redes wireless disponíveis no NorteShopping

As redes "PT-WIFI" e "Wi-Fi_Optimus_Clix_Novis" são redes que tem como finalidade permitir que o utilizador aceda à Internet através do seu computador pessoal, mediante uma quantia monetária. O primeiro acesso pertence ao Grupo Portugal Telecom e o segundo pertence à Novis.

Em ambos os casos o acesso é similar. As redes encontram-se desprotegidas permitindo que o cliente se ligue, contudo não é possível aceder à Internet sem antes o cliente se autenticar. Este é um caso similar ao da UPtec, ou seja, o sistema detecta que o cliente não está autenticado e reencaminha para a página de login.

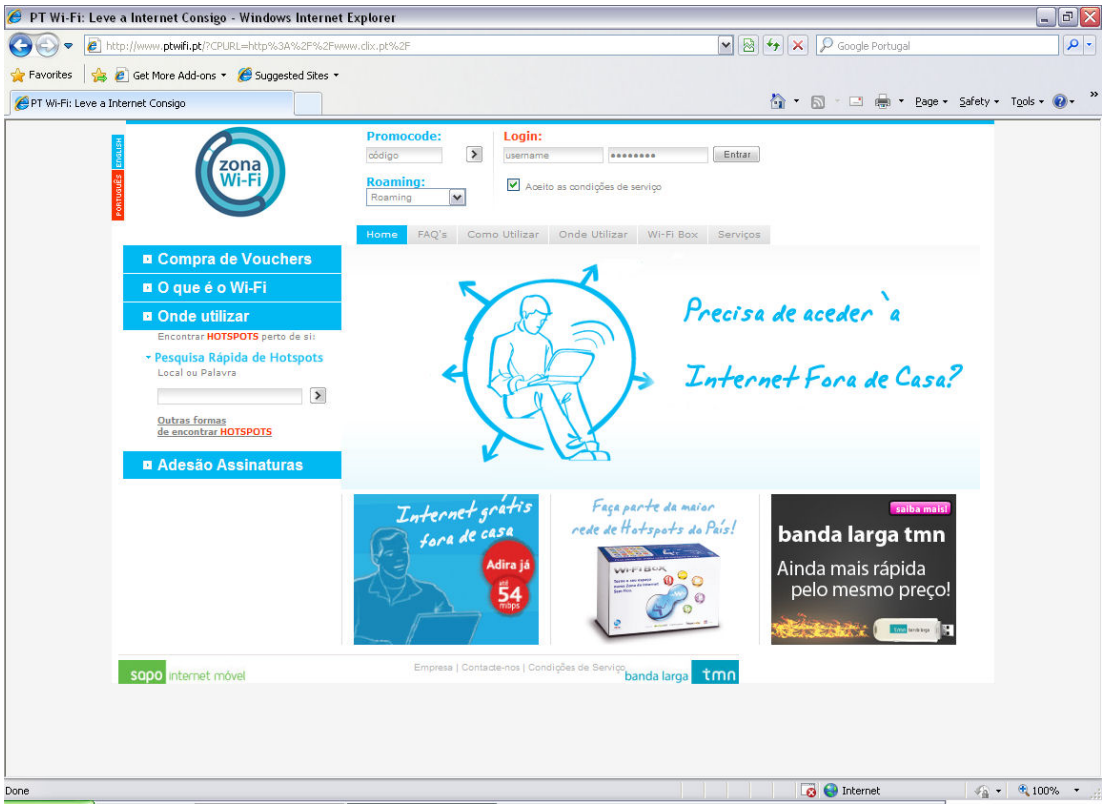

Figura 2.22: Página de autenticação do hotspot da PT-WIFI

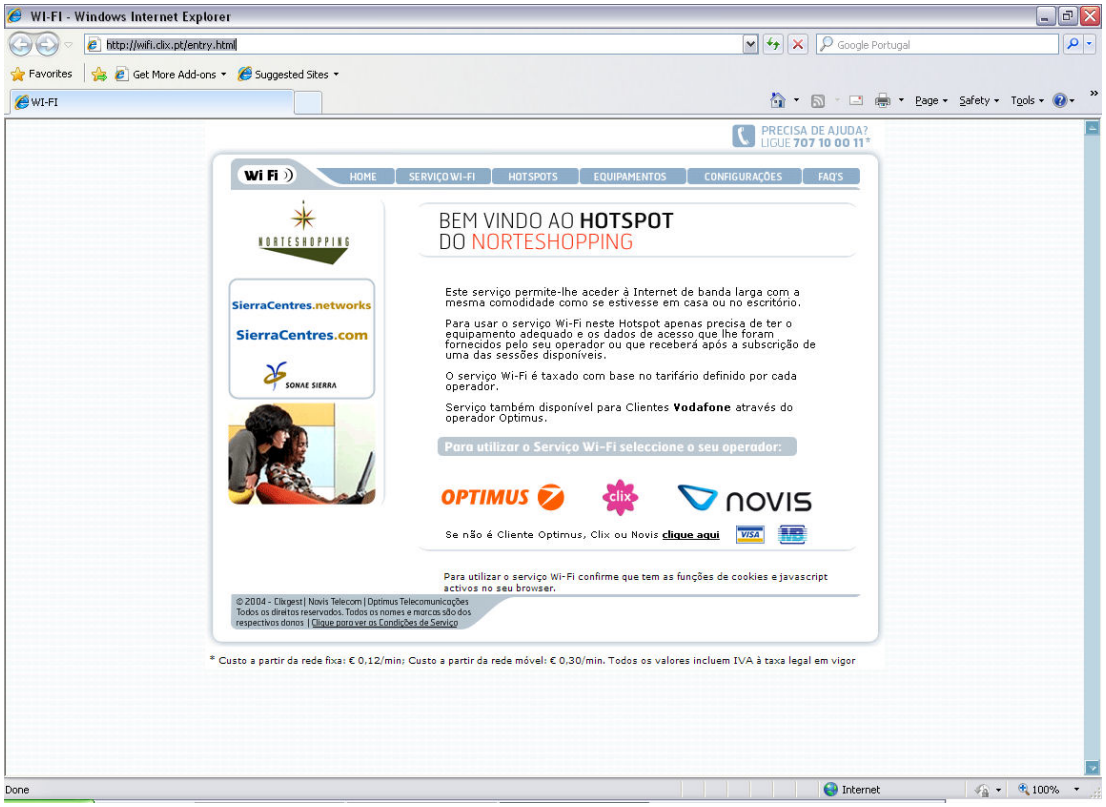

Figura 2.23: Página de autenticação do hotspot da Wi-Fi_Optimus_Clix_Novis

Apesar de não ter sido possível realizar login em ambas as redes (pois em nenhuma delas tinha conta), foi possível verificar que na rede "PT-WIFI" era possível aceder a todas as páginas que pertençam ao domínio *sapo.pt*, domínio este que pertence ao mesmo grupo.

Neste capítulo foi possível apresentar alguns dos conceitos e ideias gerais sobre as redes de computadores, assim como a recente evolução que tiveram, e em que medida a rede wireless se insere no âmbito das redes.

Os aspectos de segurança apresentados são fundamentais, e cada vez mais é importante tê-los em consideração. As redes wireless, ao integrarem as redes de cabo, vem aumentar as potencialidades dos utilizadores, aumentando também a probabilidade de ocorrerem falhas de segurança.

Por último, a apresentação de algumas redes wireless vem demonstrar que esta tecnologia já se encontra bastante difundida, e que pode ter diversos tipos de funcionamentos, de acordo com as necessidades dos utilizadores, e a política da empresa em questão.

Capítulo 3

Problema existente e Estado da Arte

Neste capítulo serão explicados em detalhe os problemas associados à gestão de utilizadores temporários na rede wireless, como também os serviços que se encontram disponíveis para os utilizadores. Para uma melhor compreensão do problema a eliminar, será realizada referência às redes wireless descritas no capítulo anterior.

3.1 Descrição

Uma das principais falhas encontradas nas rede wireless é a falta de moldagem do tipo de acesso à rede de acordo com cada utilizador, isto é, permitir ou negar serviços de rede tendo em conta a pessoa que se autentica. Actualmente, é criado um perfil médio de utilizador, onde se tenta preencher as necessidades dos utilizadores, salvaguardando a política da empresa garantindo a segurança da rede. Com esta medida, encontra-se disponível para certos utilizadores, um conjunto de serviços que estes não necessitam, como existe para outros utilizadores serviços que se encontram barrados e são importantes para a sua actividade.

Na rede da UPtec existe uma grande heterogeneidade de utilizadores, desde pessoal administrativo até funcionários das empresas incubadas. Como tal, não existe uma restrição de serviços nem uma restrição de utilização, o que pode conduzir a um abuso por parte dos utilizadores, causando instabilidade de acesso aos outros utilizadores, saturando a própria rede. Como a autenticação da rede wireless é igual para todos os utilizadores, não é possível distinguir a quem é que pertence determinado computador, o que permite a um utilizador navegar na Internet de forma anónima.

Este facto também não possibilita distinguir os serviços, dependendo do utilizador. Neste caso seria necessário atribuir um conjunto de credenciais a todos os utilizadores da

rede. Algumas empresas, impõem ainda que o utilizador indique qual é a MAC address do computador que vai aceder à rede.

Com o nascimento das credenciais, surge a necessidade de garantir que os utilizadores têm acesso à rede apenas durante o período de tempo necessário. Este facto, sendo tratado de forma manual, implica um esforço muito grande por parte do administrador da rede, de forma a garantir que é retirado o acesso aos utilizadores que já não se encontram na empresa. Uma situação que pode ocorrer, consiste no esquecimento do utilizador e este passar a ter acesso à rede durante bastante tempo.

Nas empresas, é normal haver só uma rede wireless que permite acesso apenas aos seus funcionários. Contudo, caso pretendam convidar alguém para uma reunião, torna-se necessário que essas pessoas tenham um conjunto de credenciais válidas para poderem aceder. O que se pode suceder, é o administrador criar acessos para todas as pessoas e posteriormente, retirar o acesso das mesmas. Isto implica que o administrador perca grande parte do tempo a gerir estes utilizadores. Outro facto é que estes mesmos utilizadores passariam a ter acesso a serviços que não deveriam.

Como tal, para limitar estes casos, a empresa poderia criar uma rede alternativa, onde houvesse uma chave única para todos os utilizadores temporários, mantendo-se na mesma a rede atrás indicada. Esta poderia ter um conjunto enorme de restrições, pois o seu objectivo é fornecer Internet a um utilizador por um conjunto de horas. Contudo, esta solução não se revela a mais eficaz pois pode dar-se o caso de o utilizador necessitar de aceder à rede da sua empresa de origem através de VPN (e a mesma estar bloqueada). Outro caso importante que pode ocorrer, é dois utilizadores diferentes tentarem aceder a mesma rede VPN, o que implica que apenas o primeiro iria ter acesso. Para contornar esta situação, seria necessário que os utilizadores tivessem um IP público.

Assim torna-se importante para uma empresa, possuir uma rede onde seja possível gerir os utilizadores temporários atribuindo serviços diferentes. Os utilizadores apenas devem ter acesso dentro do período especificado, desde o dia X até ao dia Y, e aos serviços que necessita, isto é, dois utilizadores diferentes acederem à mesma rede, apresentarem períodos diferentes de acesso, e ser possível definir um utilizador com capacidade para aceder à rede da sua empresa por VPN ao passo que o outro não tenha essa possibilidade. Mais importante ainda, o acesso ser efectuado de forma automática, isto é, o administrador tenha apenas de definir as credenciais do utilizador mas o bloqueio do mesmo ser efectuado pelo sistema na data indicada.

3.2 Estado da Arte

Como se pretendia criar um hotspot, foi necessário realizar a pesquisa de soluções existentes no mercado e quais as funcionalidades que ofereciam. Apesar de um dos aspectos mais importantes ser o custo do software, foram analisadas algumas aplicações

pagas, pois o seu valor poderia compensar as vantagens que trazia para a rede empresarial. Alguns destes sistemas não foram possíveis de testar, mas serão salientadas as vantagens dos mesmos.

3.2.1 2hotspot

Este programa funciona apenas em Windows, sendo a sua instalação bastante simples e habitual ao estilo deste sistema operativo. No entanto, o programa não funcionou correctamente na rede do INESC Porto pois requeria uma ligação ao site da empresa para validar os logins dos utilizadores. Como não havia a opção de definir o proxy, não foi possível ir mais além. Contudo, este software não cumpria os requisitos pretendidos, pois funcionava em Windows (não havendo versão em Linux) e a validação não era local, factor bastante importante para manter a segurança dos utilizadores. [2ho09]

3.2.2 ZoneCD

Este programa é indicado como uma das referências nos sistemas de hotspot, disponibiliza uma versão adaptada da distribuição linux Morphix CD, onde inclui diverso software pré-configurado para a criação de um hotspot. Existem duas versões, uma gratuita e outra paga. A versão gratuita tem como base o projecto NoCat e a autenticação é realizada através do site da empresa. A versão paga assenta num projecto mais recente denominado por wifidog, sendo que a versão mais cara permite realizar a autenticação localmente, bem como gerir diversos relatórios de utilização. Em Março de 2009, deixou de ser possível obter a versão gratuita, mantendo-se contudo a autenticação válida para os sistemas que se encontravam a funcionar por um período de tempo não definido. [Zon09]

3.2.3 Softvision Explorer

O Softvision Explorer é uma solução para a gestão de hotspots e *cyber cafés*. A autenticação é realizada através de credenciais, no caso de hotspots, como também através de *smart cards*, no caso de cyber cafés. A profissional (a única que permite criar hotspots) permite que os dados dos utilizadores sejam guardados em MySQL, como também realizar configurações ao nível da firewall ou limite de utilização por parte dos clientes wireless. Inclui também uma ferramenta própria de gestão de utilizadores, e permite a obtenção de diversas estatísticas. Esta versão também inclui a gestão de chamadas através do protocolo VoIP (*Voice over Internet Protocol*). Trata-se de um software muito centrado na implementação de hotéis e restaurantes, não sendo necessários grandes conhecimentos para a sua implementação e gestão. [Exp09]

3.2.4 MikroTik

A empresa MikroTik é um fabricante de soluções de hardware e de software. O seu principal produto é o sistema operativo designado por MikroTik RouterOS que é baseado em linux. É um sistema que possibilita a implementação em qualquer computador, que funciona como gateway da rede, permitindo a gestão de diversos pontos importantes da rede como a firewall, routing, MPLS (*MultiProtocol Label Switching*) acesso VPN ou a limitação de banda por QoS. O sistema também inclui a possibilidade de gerir rede wireless e hotspot. O sistema é pago e possui quatro variantes. Para além disso, dispõe de um módulo gratuito e de uma demonstração funcional. Em ambos os casos não foi possível testar a aplicação. Apesar de o site indicar que é compatível com a maior parte do equipamento, foram encontradas diversas queixas sobre o facto de este software só funcionar em equipamento específico da empresa. Foram também apresentados alguns erros que ainda não foram corrigidos. [Mik09]

3.2.5 CafeRadius

O software CafeRadius é um sistema aberto de gestão de hotspot, que foi desenhado para funcionar em sistemas embebidos como o WRAP/ALIX ou placas da Soekris. No entanto é possível instalar o mesmo em sistemas operativos Linux. Permite criar contas para utilizadores através de geração automática de login e password e imprimir esses dados. Permite também definir limites de tempo, de banda e restringir o login a determinadas datas, através de uma interface Web. O sistema encontra-se parado desde o dia 1 de Janeiro de 2008, sendo apenas possível encontrar suporte através de um grupo de discussão que não tem qualquer actividade recente. [Caf09]

3.2.6 FirstSpot

O software FirstSpot encontra-se na versão 6 e pertence à famosa empresa PatronSoft. Trata-se de um sistema de gestão de hotspot baseado em Windows e permite a gestão centralizada de utilizadores. Possui diversas funcionalidades tais como a criação de utilizadores de forma automática, utilizadores anónimos, múltiplos logins e também suporta o protocolo RADIUS. Para além disso, permite ao utilizador associar um MAC address após este ter-se autenticado a primeira vez, deixando de ser necessário realizar login sempre que o utilizador se liga à rede. [Fir09b]

Este software, tal como os outros, permite aplicar restrições em termos de banda utilizada, tal como o tempo que o utilizador tem acesso à rede. Também é possível configurar uma firewall para permitir negar o acesso a certos serviços ou páginas da Internet. O sistema é pago, sendo um dos mais caros, a par do MikroTik.

3.2.7 ChilliSpot

O programa ChilliSpot é um portal software livre que permite a autenticação de clientes através de uma interface Web. Os utilizadores são controlados através de um servidor RADIUS que a própria solução implementa. A adição de utilizadores é realizada através de ficheiros de configuração próprios. A cada utilizador é possível definir parâmetros como o tempo de login, limite de tráfego ou a largura de banda disponível. Implementa também alguns atributos do protocolo RADIUS. [Chi09]

A última versão deste software foi disponibilizada em Setembro de 2006, sendo actualmente continuada através da versão CoovaChilli. Este software nasceu de um entusiasta e actualmente apresenta características bastante semelhantes ao programa original, tendo sido efectuadas algumas correcções de segurança. [Coo09]

3.2.8 Antamedia Hotspot

A empresa Antamedia apresenta diversos programas de gestão de redes, sendo um deles o Antamedia Hotspot. Este é um sistema que funciona em Windows e não precisa de hardware específico. Apresenta uma interface simples para realizar a gestão da rede, como também dos utilizadores. Os utilizadores podem aceder à rede através de contas pré-pagas ou pós-pagas, sendo possível impor limites de utilização (quer tempo, tráfego ou período em que pode realizar login). Permite também criar limites de banda disponíveis através de grupo de utilizadores, deixando de ser necessário definir um a um. Uma das diferenças em relação aos outros sistemas hotspot, trata-se de ser possível adaptar as páginas de acesso diferentes, consoante o ponto de acesso em que o utilizador se autentica, isto é, se o utilizador se autentica num AP que se encontra no 1º andar, recebe uma página de autenticação diferente do utilizador que pretende autenticar-se num AP do 3º andar.

Este software também funciona como gateway, o que permite criar restrições ao nível da firewall e impedir que os utilizadores acedam a determinados sites ou serviços. Esta empresa dispõe também de uma solução RADIUS não gratuita que é a implementada neste produto. [Hot09]

O armazenamento da informação dos utilizadores pode ser realizado através de diversas formas. Uma delas é com recurso ao protocolo LDAP. Após alguma pesquisa, reuniu-se informação sobre alguns destes sistemas existentes, tendo em comum grandes empresas que os desenvolvem e o facto de funcionarem em Linux.

3.3 Servidores LDAP

3.3.1 OpenLDAP

O projecto OpenLDAP é um projecto que nasceu em 1998, sendo um clone de um projecto já iniciado pela Universidade de Michigan. Em Abril de 2006 houve uma reestruturação da equipa, que passou a contar com um grupo de três membros na equipa base e outros elementos para a implementação de funcionalidades e testes. Contudo, existe uma comunidade ainda maior que permite criar funcionalidades e efectuar testes ao software. O facto desta comunidade ser bastante grande e de o software livre, demonstra confiança aos administradores de rede e faz com que seja um dos mais usados.

Trata-se de um software com bastantes funcionalidades e recursos, sendo uma delas a forma de como os dados são guardados. Actualmente permite que estes dados sejam guardados em bases de dados relacionais, estando já optimizado para guardar em Berkeley DB. O Berkeley DB é uma ferramenta de software aberto que proporciona uma base de dados embebida para permitir que seja usada de forma rápida e sem a necessidade de configuração.

O OpenLDAP disponibiliza um grande conjunto de ferramentas, encontrando-se actualmente mais de vinte ferramentas implementadas de raíz e mais dez a ser testadas para a implementação futura. Estas ferramentas permitem que sejam implementadas políticas de palavras passe, ferramentas de log, sincronização de servidores LDAP, entre outras possibilidades.

A configuração do servidor é realizada através de ficheiros de texto, não apresentando qualquer interface gráfica. Para aceder aos dados do servidor, é possível usar diversas ferramentas que se encontram na Internet, como por exemplo o LDAP Admin ou o phpLDAPadmin.

3.3.2 389 Directory Server

O projecto 389 Directory Server é o projecto Fedora Directory Server, mas renomeado. É um programa desenvolvido pela Red Hat que actualmente todas os seus componentes são software livre. Trata-se de um projecto que implementa um servidor LDAP como também uma interface em Java.

Também apresenta diversas funcionalidades, como os dados serem guardados em Berkeley DB, permitir a sincronização de dados entre diversos servidores, como também sincronizar dados com o Active Directory. A sua interface é bastante fácil de usar e permite definir diversas opções para grupos de utilizadores ou individualmente para cada conta. Apesar de possuir bastantes requisitos, o sistema não permite ao administrador ferramentas para personalizar os dados que são inseridos para cada utilizador. Para além disso, não foi possível aceder ao servidor com outro tipo de interface. Contudo, sendo

um software livre é possível alterar o código fonte para adaptar aos requisitos de cada empresa.

3.3.3 ApacheDS

A Apache Software Foundation desenvolveu também um servidor LDAP totalmente escrito em Java. Apresenta uma ferramenta para interceder como interface com o servidor denominado por Apache Directory Studio, desenvolvido na mesma plataforma. Ambas as ferramentas são software livre.

O servidor já suporta diversas extensões para além das mencionadas do protocolo LDAP, como por exemplo o DHCP, Kerberos Authentication Service ou mesmo Samba. Tal como os anteriores, permite adicionar novas funcionalidades. Contudo, o servidor arranca com um domínio por defeito (*example.com*) e para colocar as configurações correctas, foi necessário despender algum tempo, isto é, não é tão intuitivo como os dois anteriores.

3.4 Conclusões do Estado da Arte

Para além destes sistemas de gestão de hotspot, foram vistos outros que na grande maioria eram variações de outros sistemas ou não possuíam vantagens extras sobre os apresentados. É de salientar que as versões que trabalham em Windows e possuem gestão própria, apresentam uma interface rica em funcionalidades, de forma a possibilitar a melhor ferramenta de gestão ao administrador. Contudo, estas soluções são pagas o que não vai de encontro com o pretendido no projecto.

As versões de software aberto funcionam plenamente em Linux e apresentam-se capazes de responder aos requisitos pretendidos. Apesar de algumas soluções não apresentarem interface gráfica, não deixa de ser possível configurar a rede pretendida. Contudo, fica a nota que existem diversas soluções, mas que o seu desenvolvimento já não acontece, por decisão dos seus criadores. Outro factor importante, é a qualidade da documentação ser bastante inferior a habitual noutros programas por se encontrar incompleta ou desactualizada.

De entre as soluções vistas, a decisão de escolher o CoovaChilli (sucessor do ChilliSpot) deveu-se ao facto de ser uma solução de software livre, possível de instalar em qualquer versão Linux e implementar as funcionalidades do protocolo RADIUS. Os aspectos de segurança ficariam a cargo da firewall Iptables, que iria permitir restringir o acesso a determinados serviços. Apesar de não ser um requisito do projecto, a implementação de um proxy transparente iria permitir impedir o utilizador de aceder a determinados páginas Web.

Das soluções de LDAP, o servidor OpenLDAP é aquele que reúne melhores características pois é o que se torna o mais moldável a empresa. Outro facto importante, é este ser já bastante mais conhecido e ser actualmente implementado num conjunto diverso de empresas, para armazenar a informação.

Capítulo 4

Proposta de Resolução

Este capítulo foi criado devido à necessidade de explicar qual a proposta de resolução para o problema deste projecto. Após uns testes iniciais sobre a resolução proposta, foi verificado que a mesma não correspondia aos objectivos propostos e problemas avançados. Assim, foi necessário redesenhar a solução final. No capítulo seguinte, será apresentada a proposta final como também as vantagens e desvantagens sobre a proposta inicial.

Uma das partes mais importantes do projecto assenta sobre permitir ou inibir serviços para os utilizadores. Todavia, é necessário primeiramente saber qual a importância dos mesmos para a sua navegação.

4.1 Serviços de rede

Na lista de serviços seguidamente nomeados, apenas são indicados os mais importantes, ou aqueles que os utilizadores utilizam com mais frequência. Existem outros serviços, como agentes de backup que não são abordados, mas que também podem fazer parte da configuração da rede empresarial.

Uma questão importante na utilização de certos serviços trata-se de saber se o utilizador possui um IP público ou IP privado. Ambos têm as suas vantagens e desvantagens, embora o funcionamento de certos serviços possa ficar limitado, quer na qualidade do serviço, quer na quantidade de utilizadores que pretendem usufruir do mesmo.

4.1.1 Serviços existentes

Como indicado anteriormente, a lista de serviços indicados não é fechada, podendo o administrador de rede permitir o acesso a outro tipo de serviços. No entanto, apenas

pretende reunir os mais importantes [Tec06].

- **HTTP, HTTPS**
  Genericamente, o protocolo HTTP (*Hypertext Transfer Protocol*) é utilizado para a transferência de dados na forma de hipertexto. Assume-se hipertexto qualquer página Web normalmente possível de aceder por um browser. O HTTPS (*Hypertext Transfer Protocol Secure*) é a sua versão segura, pois é implementado sobre cada SSL ou TLS. Estes serviços usam a porta 80 e 443 (HTTP e HTTPS respectivamente). Por razões de segurança ou de a porta já se encontrar ocupada, é possível usar qualquer outra porta acima da 1024, tendo-se convencionado o uso da porta 8080, mas nada obriga por utilizar outra porta.

- **FTP, SFTP**
  O FTP (*File Transfer Protocol*) é um protocolo que permite a troca de ficheiros entre um cliente e um servidor. Tal como acontece no HTTP, existe uma versão do FTP que é implementado sobre SSH (*Secure Shell Protocol*), denominado por SFTP (*Secured File Transfer Protocol*). Do lado do servidor, é utilizado a porta 21 para escutar os pedidos dos clientes, no qual o cliente indicará qual a porta por onde quer receber os dados (um valor aleatório acima do valor 1024). Após esta comunicação, o servidor começa a enviar os dados através da porta 20 para a porta especificada pelo cliente. Por sua vez, o SFTP utiliza a porta 22 para efectuar a comunicação (autenticação e transferência de ficheiros).

- **IMAP, IMAPS, POP3, POP3S, SMTP, SMTPS**
  Os protocolos mencionadas são normalmente utilizados para aceder ao e-mail através de um cliente de e-mail. Todavia, não é obrigatório utilizar todos os protocolos ao mesmo tempo para ser possível utilizar o serviço correctamente. Cada um dos três protocolos possui uma versão mais segura com o intuito de aumentar a segurança dos dados que são transferidos entre o cliente e o servidor. Em traço simples, o POP3 permite descarregar o e-mail do servidor para o cliente. Este utiliza a porta 110 na versão normal e a porta 995 na versão segura. O protocolo SMTP (*Simple Mail Transfer Protocol*) é um padrão para o envio de e-mail através da Internet, ou seja, envio de dados do cliente para o servidor e entre os servidores. Este utiliza a porta 25 para comunicar, sendo que a versão segura necessita que a porta 465 se encontre activa. Por fim, o protocolo IMAP (*Internet Message Access Protocol*) tem ganho cada vez mais popularidade pois o número de funcionalidades é superior aos outros dois. Este protocolo permite enviar e receber e-mail, necessitando apenas que esteja disponível a porta 143 na versão normal e a porta 993 na versão segura.

- **SSH**
  O protocolo SSH permite realizar a troca de informações entre dois equipamentos de rede de forma segura, fazendo com que os dados circulem na rede de forma encriptada. Actualmente, o SSH é associado a um programa que permite executar acções em computadores remotos, fazendo uso deste mesmo protocolo. Este necessita da porta 22, tal como o SFTP utiliza, pois na prática é o protocolo FTP a funcionar dentro de um túnel SSH).

- **P2P (BitTorrent, Skype)**
  Este protocolo é utilizado para partilhar informação entre computadores sem a necessidade de existir um servidor central ou uma ligação directa para um determinado computador. Para além disso, estabelece uma ligação ponto a ponto com outro computador onde é iniciada a transferência de ficheiros. Como é possível realizar mais do que uma ligação ao mesmo tempo, permite aumentar a velocidade de transferência (pois normalmente os utilizadores tem velocidades de download superiores ao upload). Programas que utilizem este protocolo podem ser usados para partilhar informação entre diversas pessoas e instituições (tipicamente de pesquisa, onde a quantidade de dados é elevada), como também pode ser usado para efectuar comunicações de voz e video como o Skype. Este protocolo pode também ser utilizado para a partilha de ficheiros com direitos de autor e que não é da sua autoria (vulgo pirataria), o que não vai de encontro às politicas das empresas e também pela Lei Portuguesa. Outro aspecto importante é que a utilização intensiva deste tipo de programas conduz a uma degradação elevada da rede, reduzindo substancialmente a largura de banda para os restantes utilizadores.

- **VoIP**
  O VoIP não é bem um protocolo, mas sim uma família de tecnologias que deriva das comunicações por voz e que permite realizar chamadas através do protocolo IP (*Internet Protocol*). Esta tecnologia tem como principal vantagem a redução de custos pois a rede de voz acenta sobre a rede de dados já criada e muitas vezes sub-aproveitada. Geralmente, as chamadas entre clientes VoIP são gratuitas, pois os dados circulam sempre na mesma rede, e são tratados como se fossem pacotes de dados. As chamadas entre VoIP e PSTN (*Public Switched Telephone Network*) são pagas, mas sendo o custo inferior a uma chamada PSTN-PSTN. Alguns dos protocolos do VoIP são o H.323, SIP (*Session Initiation Protocol*), MGCP (*Media Gateway Control Protocol*), H.248, Jingle ou IAX (*Inter Asterisk eXchange*). É possível efectuar chamadas de VoIP de duas formas diferentes: através de software (denominados *softphone*), que utilizam o equipamento de som de um computador para efectuar a chamada ou através de telefones específicos para este protocolo (denominados por *hardphones*). Estes últimos, podem integrar as

funcionalidades de VoIP e de telefonia normal, permitindo ao utilizador ou a uma central (caso a empresa possua) escolher qual a forma mais barata de efectuar essas comunicações. [tec09a] A vantagem na rede wireless prende-se com a possibilidade de o utilizador poder comunicar com a sua empresa de forma gratuita, ou de poder efectuar conferências remotas.

- **VPN**
  A VPN é uma rede de comunicações privada, normalmente para interligar empresas que é constituída sobre a Internet. Como os dados que circulam na Internet não são seguros, a VPN vem permitir a criação de túneis de comunicação e possibilitar que esses mesmos dados circulem de forma encriptada. Actualmente, a VPN permite ao cliente utilizar todos os serviços da sua rede empresarial, não estando presente na mesma, isto é, o administrador da rede apenas precisa de dispor dos serviços na sua rede, pois o utilizador pode ligar-se remotamente a essa mesma rede e usufruir desses mesmos serviços. [Tec09b]

4.1.2 IP Público vs IP Privado

A diferença entre IP's públicos e privados apenas se realiza na forma como são visíveis para a Internet. Um endereço público é visível para o exterior e normalmente é atribuído por um ISP (*Internet Service Provider*), ou caso a empresa já opere desde os princípios da Internet e tenha requisitado ao instituto IANA (*Internet Assigned Numbers Authority*) uma gama de endereços públicos. Um endereço privado apenas é visível na sua rede local sendo atribuído pela própria empresa. Quer isto dizer, que num endereço público, a empresa não tem qualquer possibilidade de alterar o IP (apenas dentro da sua gama) sendo que num endereço privado, torna-se possível realizar esta alteração. Para o utilizador que se liga a rede, estes endereços são atribuídos por um servidor DHCP (*Dynamic Host Configuration Protocol*) que informa o cliente das definições necessárias para aceder a rede.

Para um computador com endereço privado poder comunicar com a Internet necessita que na empresa esteja implementada a tecnologia NAT. Como já foi referido, apenas os serviços que usam os protocolos TCP e UDP podem comunicar com o exterior.

Para contornar este problema é necessário que o computador tenha um IP público de forma a funcionar correctamente. A VPN é um dos serviços que funciona com IP privado, mas não permite que seja para todos os utilizadores. Por exemplo, no caso de dois utilizadores que tentam aceder a redes VPN diferentes, não existe qualquer problema. No entanto, quando esses mesmos utilizadores tentam aceder à mesma rede, apenas um deles (o primeiro que efectuar a ligação) conseguirá obter conectividade, pois o servidor VPN da empresa remota interpreta que é o mesmo cliente a tentar estabelecer a comunicação. [McL09]

Outro serviço que apresenta algumas limitações é o VoIP. Este serviço, para funcionar necessita obrigatoriamente de possuir IP público, isto é, não funciona através de NAT. Uma das formas de contornar este problema é através da implementação de uma central VoIP, onde o utilizador não comunica directamente com outro cliente VoIP, mas sim através da central. A central necessita de IP público para funcionar e realizará a ponte para todos os clientes da rede privada.

4.2 Rede a criar

Para iniciar este projecto foi necessário planear qual a configuração da rede a implementar. Apenas será usada como testes, pois não poderá representar uma rede real. Esta solução pretende também representar parte da rede wireless que foi especificada em exemplos anteriores.

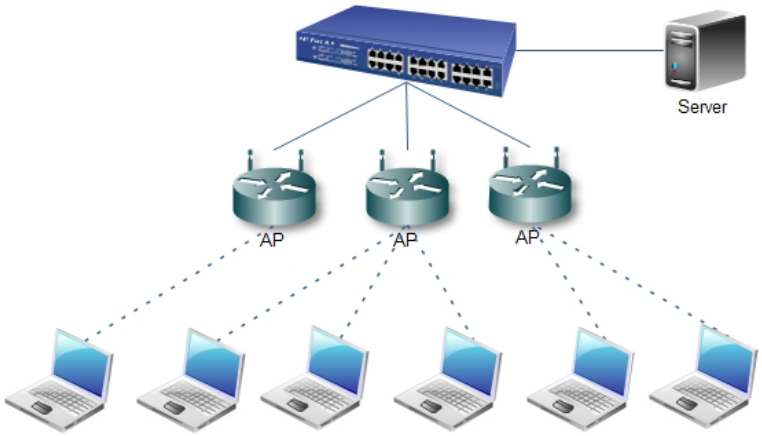

Figura 4.1: Rede a desenvolver

Para constituir esta rede, serão utilizados equipamentos da Cisco. O AP será o modelo Aironet 1130 AG Series, sendo o switch um Cisco Catalyst 2950 Series de 24 portas 10/100 Mbit/s. O servidor será um computador normal, onde será instalado todo o software necessário para poder autenticar os clientes wireless. Apenas se encontra representado um, pois o número de clientes que vai existir para testes não necessita de colocar redundância de serviço ou mecanismos de falhas.

O software a ser instalado será descrito a seguir, sendo indicado qual o programa que será instalado e as configurações gerais para o seu funcionamento.

4.3 Software necessário

Para colocar a rede em funcionamento é necessária a implementação de algum software, desde fornecer IP aos clientes até realizar a autenticação dos mesmos. É importante salientar que existem outros programas que podem ser instalados,

principalmente para garantir uma maior segurança dos dados que circulam entre os diversos sistemas. Esta informação será explicada no capítulo sobre melhoramentos do projecto.

4.3.1 DHCP

O protocolo DHCP atribui de forma dinâmica endereços IP aos computadores da rede. Estes endereços podem ser atribuídos de forma manual ou automática. O programa a utilizar chama-se DHCP *daemon* que permite de forma rápida configurar a rede. Os endereços manuais serão atribuídos aos equipamentos que constituem a rede, pois a sua MAC address não se altera e são equipamentos que têm mobilidade. Os clientes temporários, têm um endereço automática que é definido através de uma *pool*.

O serviço DHCP permite também informar os computadores qual a gateway da rede e os servidores DNS (*Domain Name System* que no caso será usado o serviço DNS do INESC Porto.

4.3.2 RADIUS

RADIUS é um protocolo AAA (*Authentication, Authorization, Accounting*) que providencia de forma central o acesso e controlo de computadores que se ligam a rede. O servidor de RADIUS permite autenticar os utilizadores ou equipamentos antes de lhe garantir o acesso à rede, definir quais os serviços que tem acesso e por fim, permite contabilizar a utilização desses serviços para fins estatísticos ou de facturação.

Neste protocolo é possível definir diversas características, quer já implementadas pelo IETF (*Internet Engineering Task Force*), como também características adicionadas e criadas pelos fabricantes de equipamentos que interagem com o RADIUS. Contudo, uma das características fundamentais são as credenciais com que é realizado o acesso à rede. Estas credenciais definem-se na forma de username e password (que é forma usada no projecto) ou através de um certificado.

As credenciais de acesso podem ser guardadas de diversas formas, sendo a mais primitiva através de ficheiros de texto. Para além da possibilidade de guardar os dados em bases de dados de modelos relacionais, mais genericamente conhecidos por SGBD (Sistemas de Gestão de Bases de Dados), os dados serão guardados em LDAP (sistema de directório).

Existem diversas empresas de desenvolvimento de software RADIUS e para escolher aquele que preenche os requisitos foi realizado um pequeno estudo que se encontra em anexo. O software escolhido é o FreeRadius. [Has02]

4.3.3 LDAP

O LDAP é um protocolo que deriva do modelo X.500 que não é mais do que um directório estruturado. Este directório é constituído por nós que formam uma sub-árvore, que por sua vez constituem a árvore final. Em cada nó é possível guardar diversa informação, não havendo a necessidade de haver uma estrutura semelhante em nós vizinhos.

Devido à forma como os dados são guardados, é possível aceder rapidamente a informação através de pesquisa. No entanto, a adição dessa mesma informação é bastante lenta, o que torna útil guardar informação que não é constantemente alterada.

Outro facto importante, trata-se da maior parte das empresas já possuir um servidor LDAP, o que possibilita guardar a informação gerada numa sub-árvore desse servidor.

O software escolhido foi o OpenLDAP que permite interligar com servidores de RADIUS. Em anexo encontra-se também uma referência sobre a pesquisa realizada. [Car03]

4.3.4 Base de dados

O LDAP necessita de um local próprio para armazenar a informação. Uma das formas primeiramente usadas recaía sobre a forma de ficheiros de texto, o qual se torna pouco eficiente à medida que a quantidade de informação aumenta.

Felizmente, o OpenLDAP já permite guardar esta informação sobre o BerkeleyDB que é uma base de dados relacional. Este forma de guardar os dados, permite obter uma eficiência superior em relação a ficheiro de texto, como também em relação a outras bases de dados relacional. [Cor09]

4.3.5 Servidor HTTP

O servidor HTTP apenas tem como funcionalidade apresentar a página web que será utilizada para os clientes efectuarem login no sistema. Como o sistema de hotspot escolhido necessita do módulo de PHP (PHP: *Hypertext Preprocessor*), torna-se importante a sua instalação.

Como é necessário existir alguma forma de os utilizadores pedirem ao administrador da rede credenciais válidas, vai ser criado um simples formulário também em PHP. Quando o formulário é submetido pelo utilizador, este vai criar um e-mail e enviar a informação preenchida para o administrador da rede.

Como os requisitos de servidor web não eram elevados, foi escolhido o Apache por ser um software simples e robusto e por ter sido implementado durante as aulas de redes.

4.3.6 Servidor e-mail

O servidor de e-mail apenas é necessário para efectuar a troca de informação entre os utilizadores e o administrador da rede (quando o formulário é submetido e quando o administrador responde ao utilizador). Apesar de o software escolhido ter sido o sendmail (já instalado de origem do CentOS) é possível utilizar o servidor da própria empresa, bastando para tal mudar os parâmetros necessários no formulário.

4.4 Software de hotspot

Para a gestão de uma rede wireless do tipo hotspot, é necessária a existência de algum software que realize a gestão dos utilizadores. Essa gestão passa por armazenar os dados dos utilizadores, realizar a sua autenticação e a respectiva desautenticação da rede.

Entre os diversos programas procurados, aquele que reunia as melhores funcionalidades pelo custo pretendido foi o CoovaChilli sendo os seus pontos fortes o facto de ser software livre e o seu desenvolvimento ainda ocorrer, algo que não acontece com outros sistemas.

4.5 Conclusões

Após implementar esta solução, foi detectado que a mesma não correspondia as necessidades do projecto. Apesar de facilitar a ligação por parte do utilizador, pois apenas necessitava de abrir uma página web e introduzir as credencias, por parte do administrador levantava alguns problemas de segurança e performance na rede.

Um dos pontos limitativos encontrados, é a obrigatoriedade de a rede encontrar-se aberta. Isto permitia que qualquer pessoa liga-se a rede (apesar de não ter acesso aos serviços disponíveis) à procura de pontos fracos. Em certos locais, como bancos, é um factor bastante importante. Outra característica do software de hotspot é de guardar os dados dos utilizadores em ficheiros de texto. Isto permite de forma simples e rápida definir quais os utilizadores que devem ter acesso a rede, mas por outro lado não permite comportar um elevado número de utilizadores. Para além disto, estes dados são carregados em memória apenas quando o programa é iniciado, o que obriga a reiniciar sempre que forem acrescentados novos utilizadores.

Por fim, não permitia ao administrador definir quais os tipos de serviços que cada utilizador deveria ter acesso, como também não permitia a criação de VLANs. Isto iria obrigar os utilizadores a terem todos acesso ao mesmo conjunto de serviços.

O capítulo seguinte, pretende retratar qual foi realmente o sistema desenvolvido e também as mudanças necessárias pela substituição do sistema de hotspot.

Capítulo 5

Resolução efectiva

Após a implementação da rede inicialmente proposta, foi verificado que a mesma não correspondia a todos os objectivos propostos e não resolvia alguns dos problemas evidenciados. Como tal, foi necessário efectuar algumas mudanças, que naturalmente, traz vantagens e desvantagens.

Esta nova solução, permite também uma maior expansão da rede, pois o traçado original ficava muito dependente do desenvolvimento de funcionalidades de um só software. As alterações serão explicadas seguidamente.

5.1 Alterações efectuadas

O software de Hotspot escolhido apresentava diversas funcionalidades, mas mesmo assim foi necessário retirar o mesmo do projecto. Apesar de efectuar a autenticação por RADIUS, não era possível utilizar outra infraestrutura de RADIUS, pois não era compatível. Outra situação levantada foi a limitação na forma como os endereços IP eram atribuídos; não era possível definir mais do que uma gama de endereços e essa mesma gama tinha uma dimensão semelhante às classes C. Apesar de não ser restritivo em termos funcionais, não permitia atribuir um endereço público a um utilizador e a outro um endereço privado.

Existem também outros pormenores que não foram tidos em conta na solução original, que apesar de não ser uma alteração é necessário que os mesmos se encontrem especificados.

5.2 Rede criada

A rede a ser desenvolvida é em todo semelhante à rede inicial. A informação extra adicionada refere-se apenas a pormenores técnicos que não foram especificados na solução original e que são importantes para uma melhor compreensão de como o problema é resolvido.

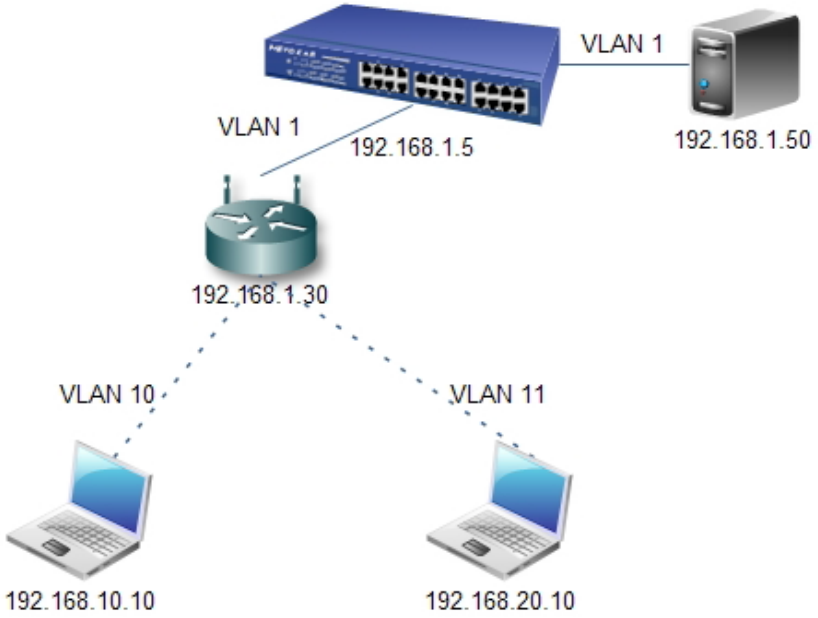

Figura 5.1: Rede desenvolvida

Para ser possível atribuir um conjunto de serviços distintos a utilizadores diferentes, foi necessário isolar os mesmos em VLANs. Neste caso, não é criado apenas um perfil médio para os utilizadores que acedem à rede, mas sim vários perfis, nos quais se tenta satisfazer a maioria dos utilizadores.

Como medida de segurança, os equipamentos ficam na VLAN1 (que normalmente é considerada a VLAN de gestão). Esta rede nunca será atribuída a nenhum utilizador, excepção feita ao administrador da rede. Ao ser criado o utilizador, é indicada qual a VLAN que possui os serviços de rede que foram requisitados. Quando o utilizador efectua login na rede, o switch atribui-lhe a respectiva VLAN. Isto permite que vários utilizadores acedam ao mesmo SSID, quando na prática se encontram em redes diferentes. Desta forma, torna também possível ao administrador atribuir VLANs que já existam implementadas na rede empresarial.

5.3 Interacção dos utilizadores

Um aspecto importante e que não foi mencionado trata-se de como vai ser efectuada a troca de informação entre os diversos actores do sistema. Nesta rede vão existir três

tipos de actores. Cada um tem um papel e responsabilidades diferentes. Para uma melhor compreensão será dada uma breve explicação sobre cada um.

5.3.1 Administrador

O "administrador" será desempenhado pelo administrador da rede ou por qualquer outra pessoa que a empresa indique para realizar a gestão. Tem como papel principal adicionar ou remover utilizadores, bem como garantir o funcionamento de toda a estrutura.

5.3.2 Responsável

O "responsável" deverá ser alguém que trabalhe na empresa ou que se encontre directamente relacionado com a mesma. Este fará a ponte entre o administrador e o utilizador, pois irá pedir as credenciais de acesso ao administrador e entregar as mesmas ao utilizador (após terem sido criadas). Este papel nasceu da necessidade de garantir que os pedidos de rede efectuados sejam legítimos.

Este elemento é aquele que convida o utilizador a deslocar-se à empresa e que também deverá estar atento às actividades do utilizador. Todas as actividades abusivas ou ilegais que o utilizador realize, serão da responsabilidade do mesmo perante a empresa.

5.3.3 Utilizador

Será a pessoa que se desloca à empresa (a convite de alguém) e que pretende aceder a rede.

5.4 Dados trocados

Esta secção pretende demonstrar quais são as informações que circulam entre os diversos actores. Primeiramente é necessário que o "responsável" efectue o pedido de ligação e para tal deverá preencher um formulário com a informação que se lá encontra.

Depois, o "administrador" indica a sua posição transmitindo as credenciais e outras informações relevantes, ou caso rejeite o pedido, deverá também indicar essa informação ao "responsável".

5.4.1 Formulário

O formulário de acesso será semelhante ao seguinte:

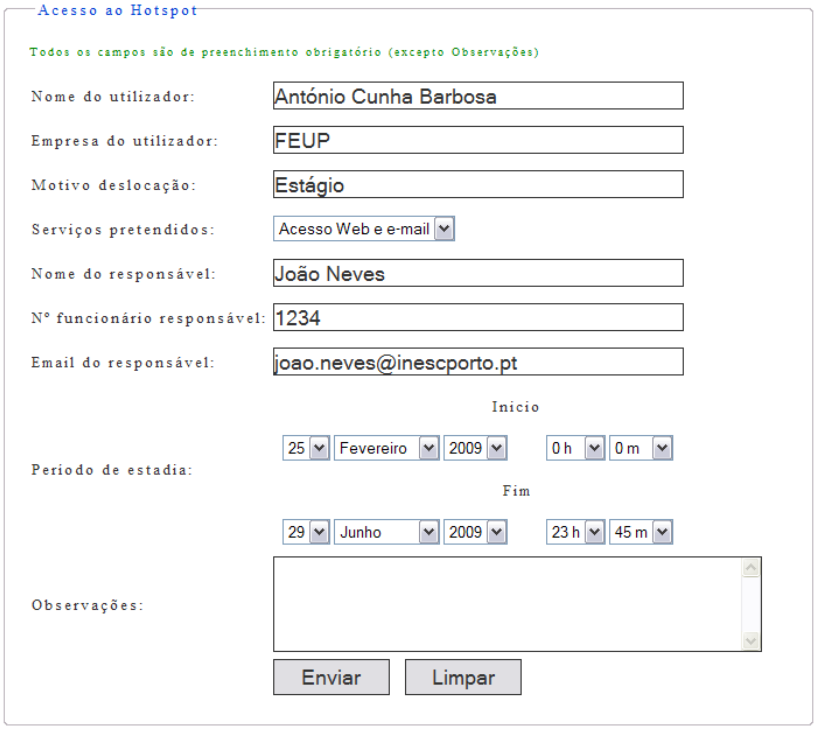

Figura 5.2: Exemplo de preenchimento de formulário de acesso ao hotspot

Quando o projecto foi lançado, não havia a indicação sobre que o tipo de informação que se pretendia guardar. A forma como este formulário está preenchido, pretende retratar a informação que se julga pertinente. No entanto, não deixa de ser possível guardar outras informações, sendo para isso necessário preencher o campo "Observações" (que não é de preenchimento obrigatório).

O campo "Serviços disponíveis" é preenchido pelo "administrador", tendo apenas o "responsável" que escolher aquele que mais se adapta às características do "utilizador". Este factor não é decisivo, pois o administrador poderá escolher outro tipo de serviços (caso verifique que aos mesmos não é possível atribuir aquele "utilizador").

Após o "responsável" clicar no botão de submeter, este irá ver um ecrã a confirmar que a operação foi bem sucedida, o que significa que o e-mail para o "administrador" foi enviado sem qualquer problema.

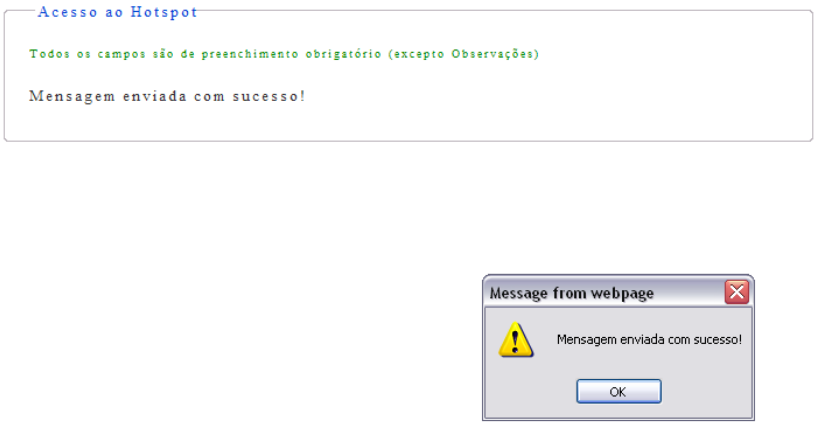

Figura 5.3: Mensagem do formulário a indicar que foi enviado com sucesso

5.4.2 E-mail recebido pelo administrador

O administrador recebe o seguinte e-mail:

Figura 5.4: Mensagem do formulário que o administrador recebe

Esta informação é necessária para o administrador criar a conta de utilizador e enviar as credenciais para o e-mail do responsável. Salienta-se ainda o facto de este e-mail apresentar uma informação que não se encontrava disponível para o "responsável". No campo de *Serviços pretendidos* foi adicionada a informação de VLAN para o administrador não ter de procurar essa informação.

5.4.3 E-mail de confirmação do acesso

Após criar a conta de "utilizador", é necessário informar o "responsável" de quais as credenciais necessárias para aceder à rede. Na resposta é fornecido um pequeno manual sobre como configurar o acesso.

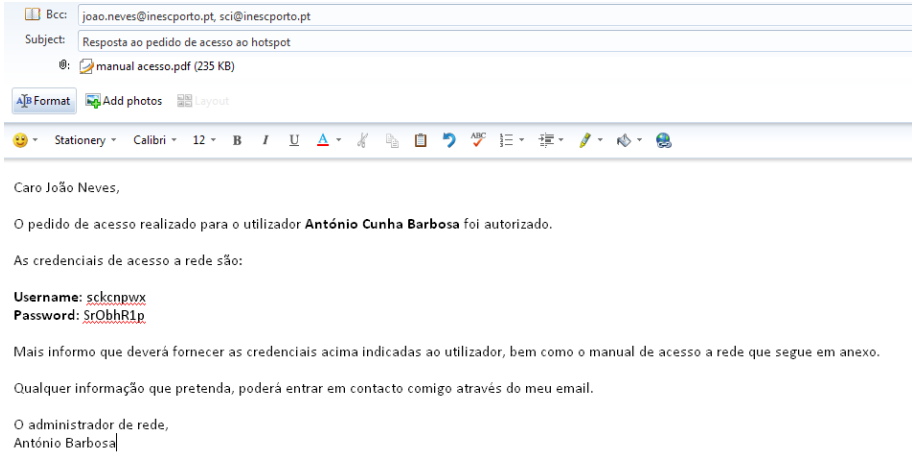

Figura 5.5: Mensagem que o responsável recebe a confirmar o pedido

Tanto as credencias como o manual, deverão ser entregues ao "utilizador" pelo "responsável" de forma a este poder aceder à rede wireless.

5.4.4 E-mail de rejeição do acesso

Como também é possível que o administrador rejeite a possibilidade de criar a conta ao utilizador (por diversos motivos), é também necessário informar o "responsável".

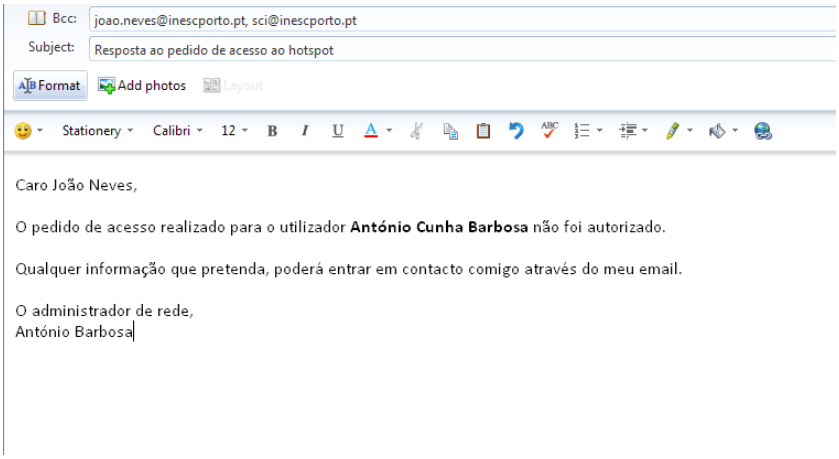

Figura 5.6: Mensagem que o responsável recebe a negar o pedido

Para o utilizador poder aceder à rede, o "responsável" deverá aceder novamente ao formulário para realizar novo pedido.

5.5 Fluxograma

Para uma melhor interpretação sobre a forma como os diversos actores interagem, foi criado um fluxograma que contempla todas as possibilidades.

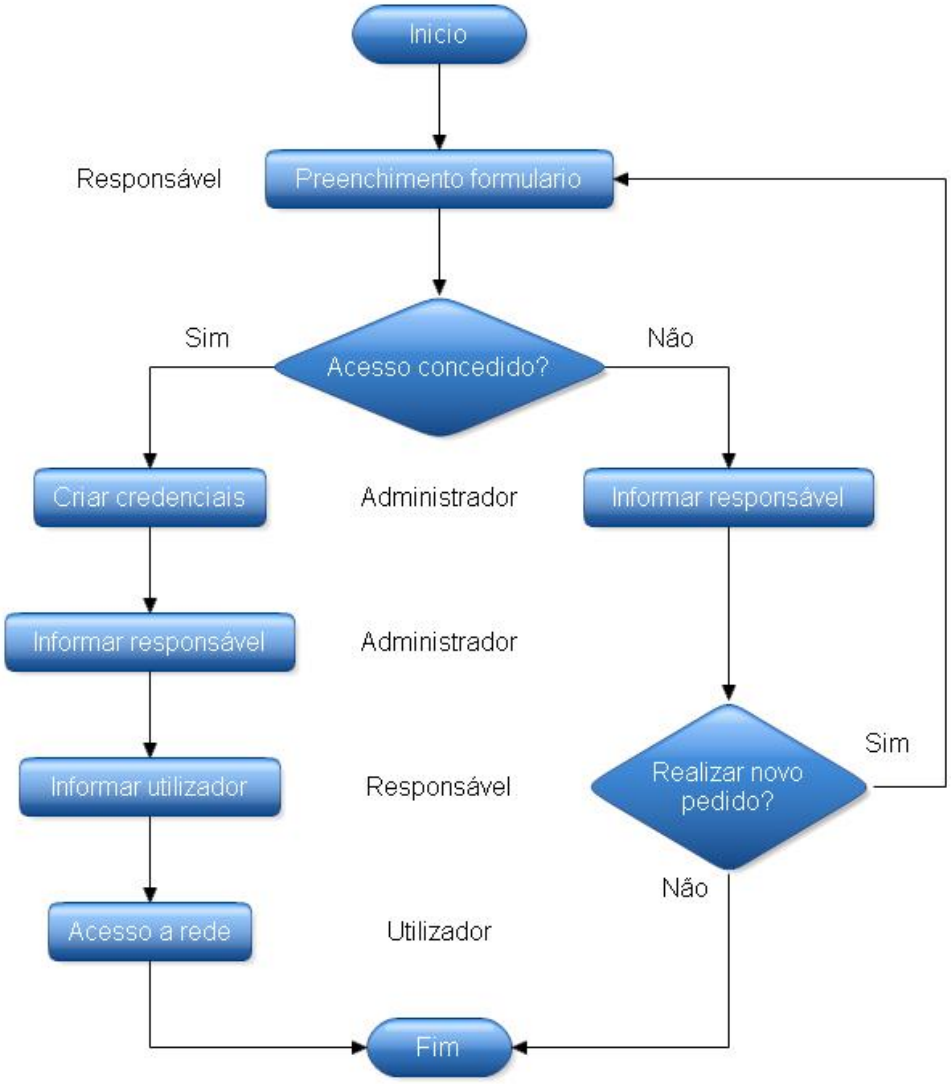

Figura 5.7: Fluxograma de como os actores interagem entre si

Como é possível ver no fluxograma, o pedido de acesso à rede é iniciado com o "responsável" a preencher e submeter o formulário atrás indicado. Caso o acesso seja negado por parte do "administrador", este deverá informar o "responsável" (que toma a liberdade de submeter novo pedido ou de não realizar qualquer acção). Quando o acesso é permitido, o "administrador" terá que criar as credenciais para o utilizador e informar o "responsável". O "responsável" informa o "utilizador" de quais as credenciais e informações necessárias para aceder à rede.

5.6 Gestão do sistema

Para a criação das credenciais do utilizador é necessário que o "administrador" insira os dados referentes ao utilizador no servidor LDAP e também que crie os scripts

necessários para automatizar o processo de bloquear e desbloquear a conta do utilizador.

5.6.1 Criação de credenciais

Para que os dados sejam guardados em LDAP é necessário que os mesmos se encontrem no formato LDIF (LDAP Data Interchange Format). O LDAP permite que os dados sejam adicionados de duas formas, através do *sldapadd* (que permite inserir dados com o servidor LDAP parado), e através do *ldapadd* (que permite inserir dados com o servidor a funcionar).

Para melhorar a interacção do "administrador" com o sistema, foi realizada pesquisa sobre a existência de ferramentas com interface gráfica. Existem diversos pacotes de software, mas só alguns foram testados, não sendo possível indicar qual o melhor, pois todos são bastante semelhantes na forma de funcionamento, tendo sido escolhida a aplicação mais intuitiva.

No Apache Directory Studio (que funciona em Windows e Linux) é necessário criar uma ligação ao servidor LDAP e estabelecer a mesma. Uma vez estabelecida a ligação, é possível visualizar todos os nós da árvore LDAP.

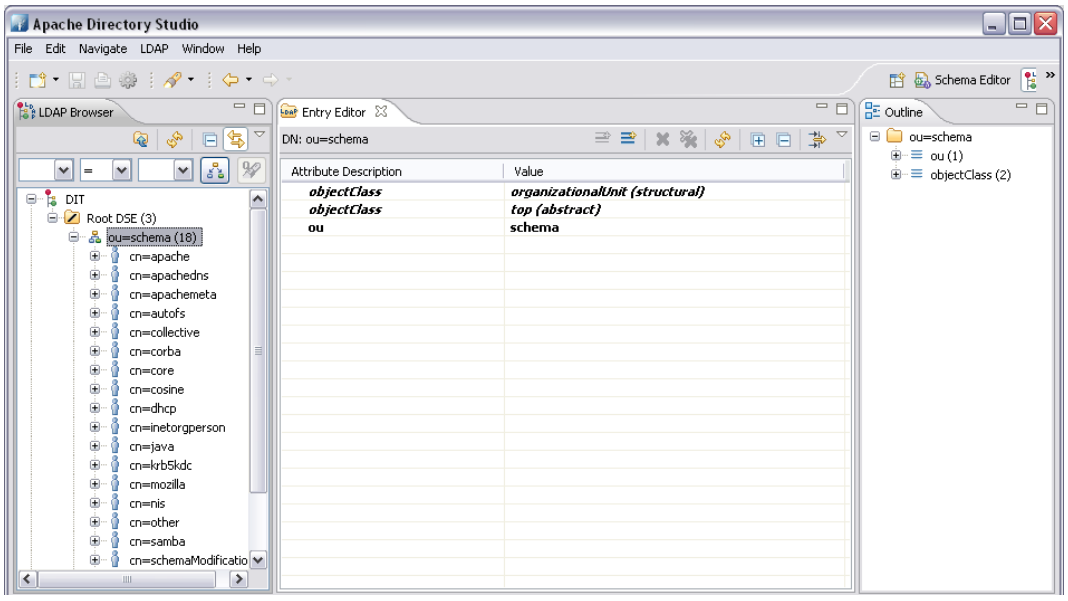

Figura 5.8: Visualização de todos os nós no servidor LDAP

Para o caso de testes foi estabelecida uma sub-árvore *organizationalUnit* com o nome de *hotspot*. Ao clicar sobre essa sub-árvore temos acesso a várias opções, sendo uma delas a *New Entry*.

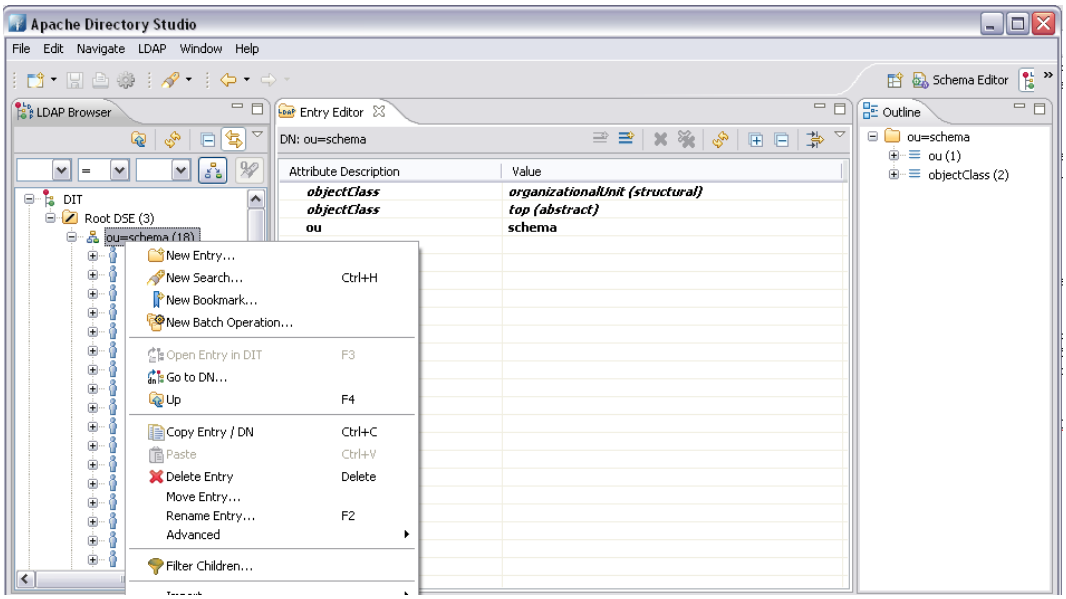

Figura 5.9: Menu para inserção de utilizadores

O programa pergunta se queremos criar um novo objecto de raíz ou através de um template. O template, neste caso, trata-se de utilizar a estrutura de uma entrada anteriormente criada, onde apenas se torna necessário alterar os dados essenciais.

Escolhendo criar o objecto de raíz, é necessário seleccionar o objecto *hotspot*, *radiusprofile* e o objecto *pwdPolicy*. Nenhum deles faz parte do standard do LDAP. O objecto *hotspot* foi criado por forma a permitir guardar toda a informação sobre o utilizador do hotspot (toda a informação constante no formulário). O objecto *radiusprofile* é criado e gerido pela equipa responsável pelo desenvolvimento do FreeRadius. O objecto *pwdPolicy* é uma implementação criada pela IETF (Internet Engineering Task Force) como uma política para palavras-passe.

Em LDAP é possível criar um nó com a junção de vários objectos, contudo terá de haver um (e um só) objecto que seja do tipo STRUCTURAL. Como o objecto *radiusprofile* é do tipo STRUCTURAL, foi necessário passar para o tipo AUXILIAR e colocar o objecto *hotspot* como principal. Isto deve-se à necessidade de a rede obrigatoriamente precisar de um campo *uid* e *userPassword*, e só no objecto *hotspot* existe os dois.

Os dados que se inserem no objecto *hotspot* são transcrição completa do formulário. Apenas é gerado username e password. A geração destes dados é realizada através de um programa externo. O objecto *radiusprofile* pretender guardar a informação a ser utilizada pelo RADIUS. Esta informação poderá ser, por exemplo, um endereço IP, ou quantas vezes é possível o mesmo login autenticar-se ao mesmo tempo. Por fim, o objecto *pwdPolicy* pretende ser utilizado de forma a conseguir bloquear a conta do utilizador. Para tal, é necessário indicar qual a política de passwords que é aplicada ao utilizador (se existir), ou no caso de omissão desta informação é aplicada a política por defeito.

Após a conclusão da inserção do utilizador, é possível verificar se os mesmos estão correctos e em caso de necessidade, alterar os mesmos, bastando para tal seleccionar o campo a modificar. A imagem seguinte, é um exemplo da informação guardada.

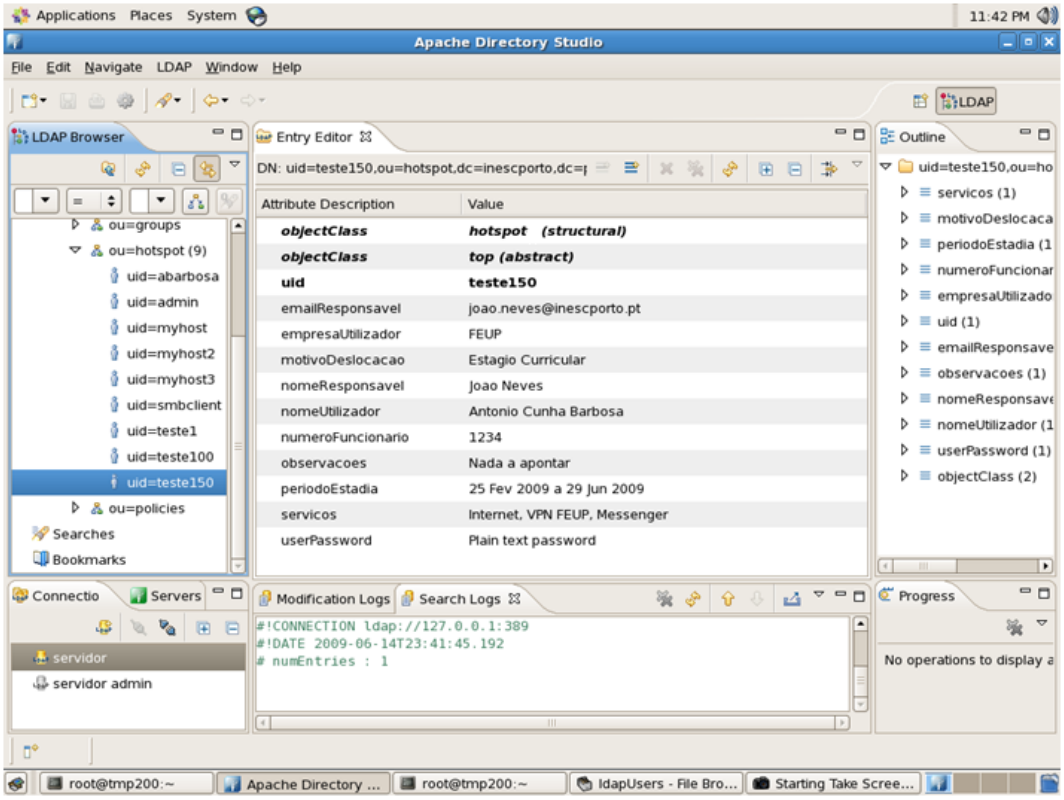

Figura 5.10: Exemplo de dados guardados em LDAP

5.6.2 Automatização de bloqueio da conta

O utilizador ao ser criado, tem a sua conta bloqueada desde o início. Este bloqueio é efectuado através da colocação de um valor no campo *pwdAccountLockedTime* para bloquear a conta. Posteriormente, é necessário criar um *script* para definir no *cronotab* a execução de duas tarefas. A primeira é executada quando se inicia o período que o utilizador pode aceder a rede, que consiste em alterar o valor do campo para a data actual. A segunda tarefa encontra-se agendada para executar no fim do período de acesso do utilizador e que deverá repor o valor inicial. No caso, as *scripts* encontrando-se em *Perl* onde se pretende que executa o comando *ldapmodify*. Após estes passos, o "administrador" deixa de estar preocupado com o desbloqueio e bloqueio da conta, podendo dar antecipadamente ao utilizador as suas credenciais.

5.7 Manual do utilizador

Apesar de o sistema de autenticação utilizado permitir que seja acedido, quer por utilizadores do Windows, quer por utilizadores do Linux, as instruções apresentadas apenas visam o sistema operativo Windows XP, pois pretende-se que sejam meramente indicativas.

O utilizador ao pesquisar as redes wireless existentes, deverá encontrar a rede temporária definida na empresa. Neste caso, a rede tem o nome de "hotspot" e para aceder a mesma, deverá o utilizador realizar duplo clique na mesma. Após isso, o sistema irá tentar aceder a rede com as credenciais do próprio sistema operativo, sendo que o mesmo irá falhar, como demonstra a imagem seguinte.

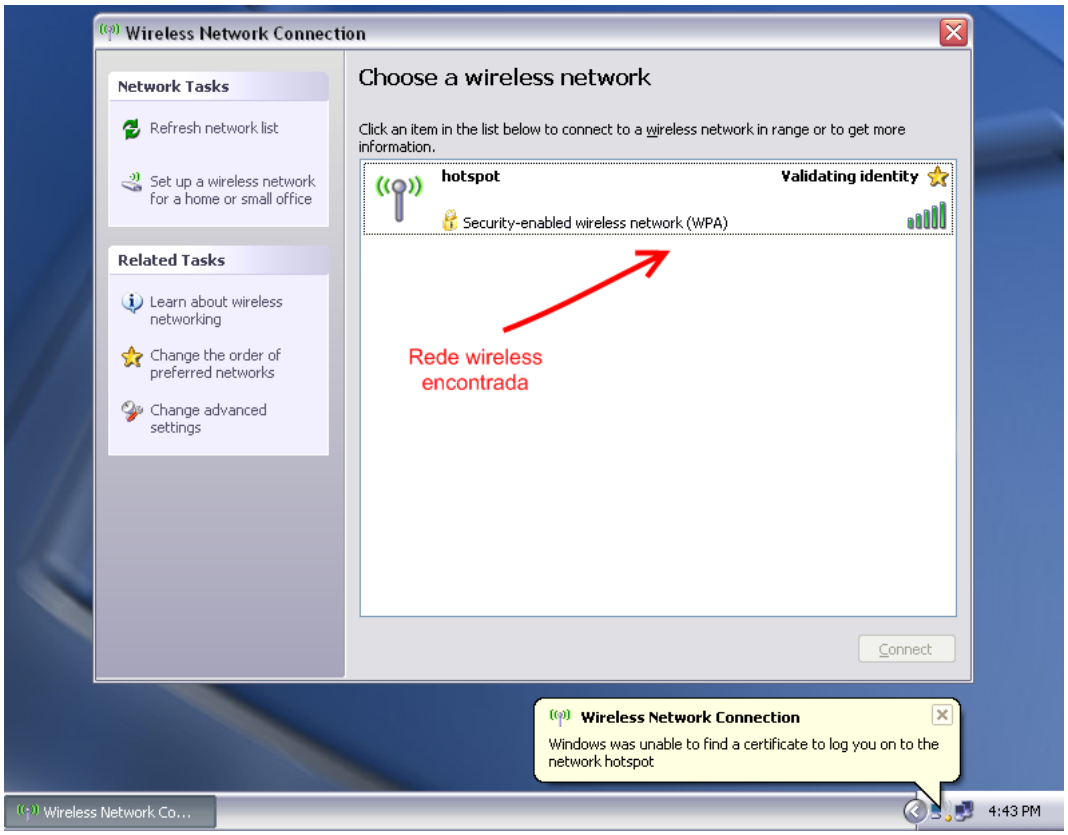

Figura 5.11: Rede "hotspot" disponível para o utilizador

Após esta fase, o "utilizador" deverá clicar no balão apresentado para aceder as propriedades da placa wireless. A imagem seguinte, apresenta as redes que o utilizador já teve acesso. Para configurar a rede, é necessário aceder a propriedades da mesma.

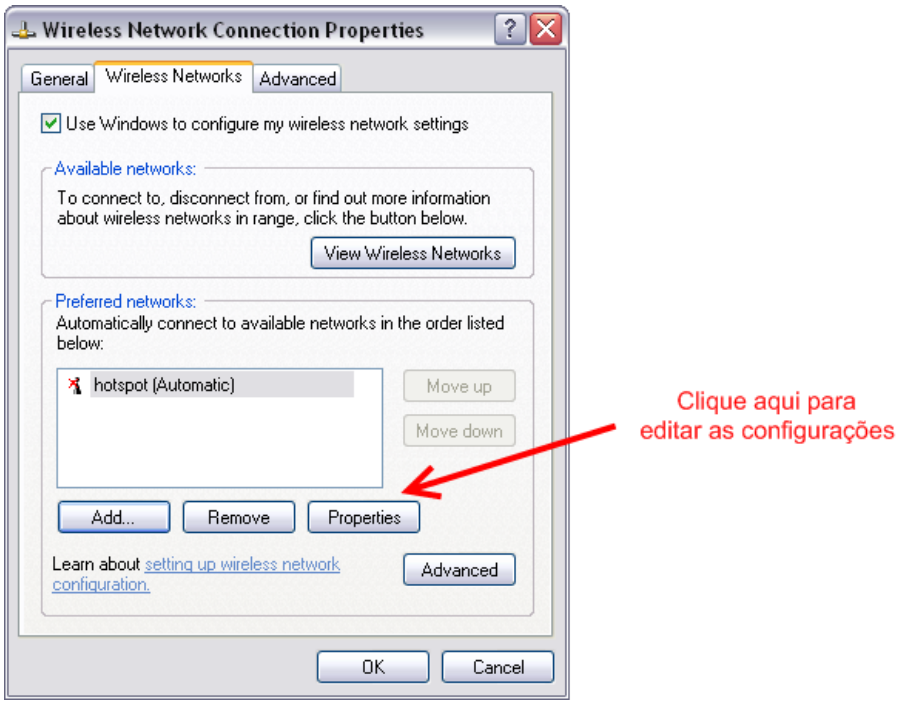

Figura 5.12: Aceder as propriedades da rede "hotspot"

Ao clicar no botão, vai surgir uma nova janela com três separadores. O primeiro separador é respeitante a encriptação usada na rede. Deverá ficar definido a autenticação da rede como WPA e a encriptação dos dados como TKIP. Em princípio não é necessário nenhuma acção do utilizador, pois o sistema operativo já define estas opções.

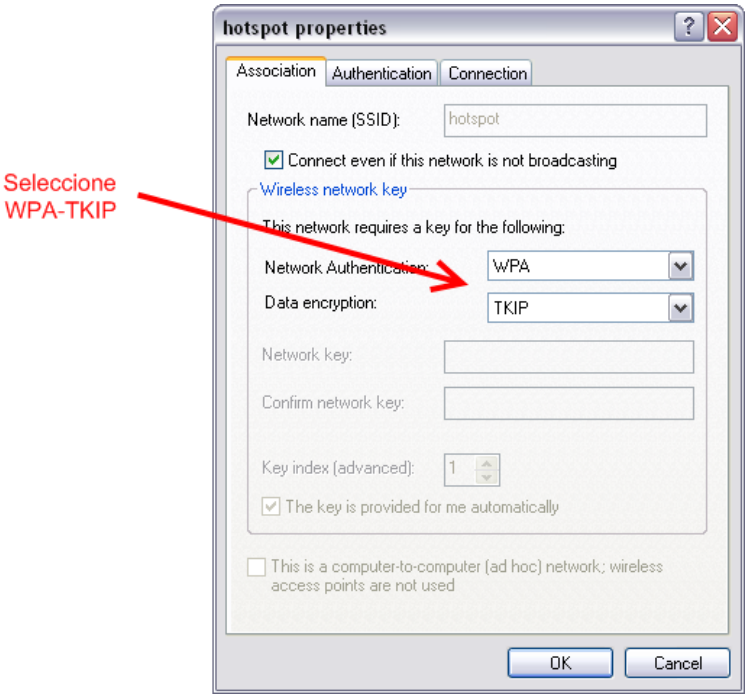

Figura 5.13: Propriedades da rede wireless "hotspot" - Separador *Association*

O separador *Authentication* já exige do utilizador que o mesmo realize algumas alterações. Como tal, deverá ser seleccionado o tipo EAP como *Protected EAP (PEAP)* e aceder as propriedades do mesmo.

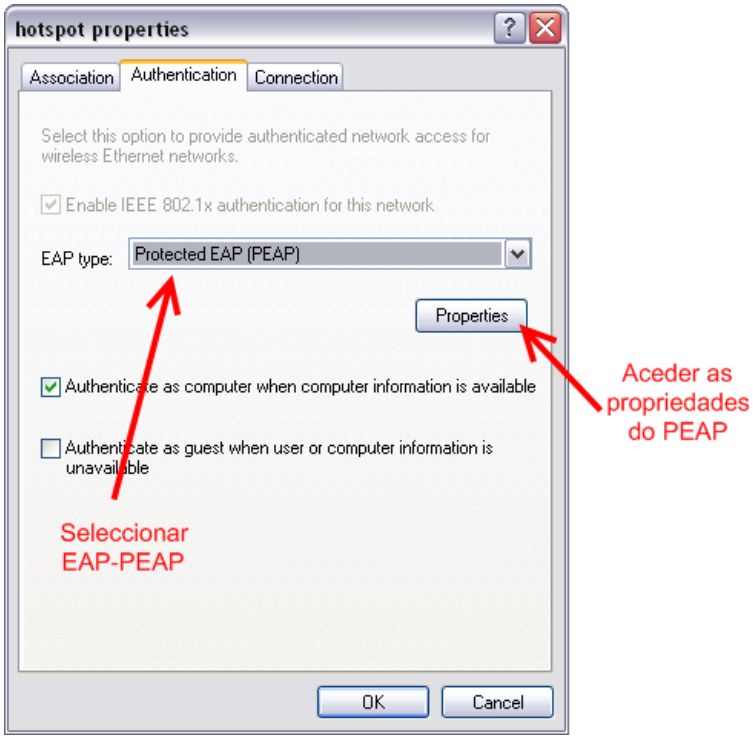

Figura 5.14: Propriedades da rede wireless "hotspot" - Separador *Authentication*

Nas propriedades do PEAP, deverá ser desmarcado a opção de *Validate server certificate* como também deverá estar seleccionado o método de autenticação *Secured password (EAP-MSCHAP v2)*. Por fim, é necessário aceder as opções de configuração do EAP-MSCHAP v2 e desmarcar a opção *Automatically use my Windows logon name and password (and domain if any)*. A imagem seguinte, pretende retratar o resumo destas alterações.

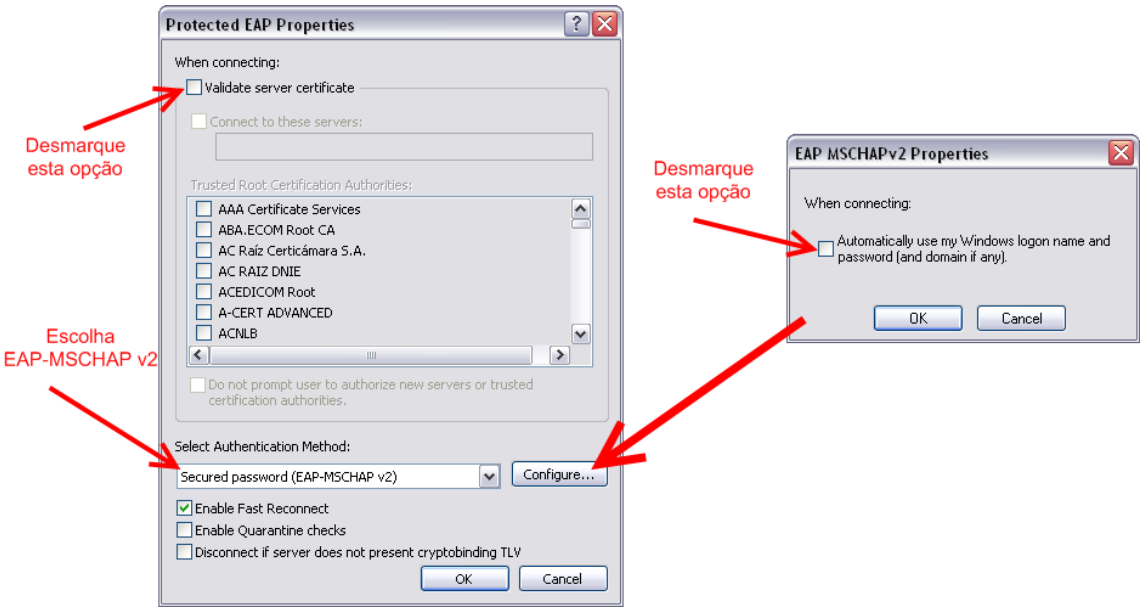

Figura 5.15: Propriedades da rede wireless "hotspot" - *Protected EAP Properties*

Após confirmar todas as janelas, o Windows irá tratar as alterações efectuadas e como tal, deverá surgir uma imagem, como a janela seguinte, onde o utilizador deverá colocar o username e password que lhe foram atribuídos.

Figura 5.16: Introdução das credenciais na rede

Após este passo, o sistema indica que o login foi realizado com sucesso e o utilizador poderá aceder a rede. Caso as credenciais estivessem erradas, ou fora do período de tempo que o utilizador poderia aceder rede, o sistema apenas indicaria que as credenciais fornecidas não eram válidas.

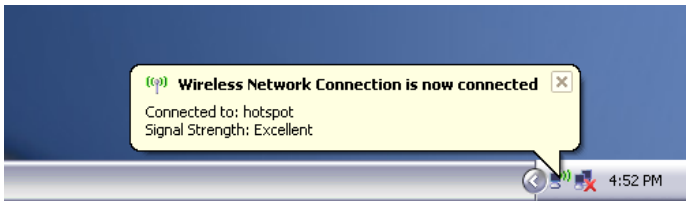

Figura 5.17: Confirmação de acesso a rede

5.8 Conclusões

A solução final difere ligeiramente da solução inicial, pois a mesma não cumpria correctamente com os objectivos propostos. Como tal, esta implementação traz vantagens e desvantagens para as partes envolvidas, sendo necessário a sua especificação.

5.8.1 Vantagens da solução escolhida

Como já foi referido, o software inicialmente proposto seria com a implementação do ChilliSpot. Contudo, após a sua implementação, foi possível verificar que não correspondia às necessidades e expectativas pretendidas.

Primeiro, esta versão já não era desenvolvida, tendo dando origem ao CoovaChilli e a outras variantes sem grande expressão. Depois, o CoovaChilli nasceu graças a um entusiasta que efectuou diversas correcções de *bugs* e implementou algumas funcionalidades que achava em falta.

Apesar de continuar a ser possível implementar em Linux, o seu desenvolvimento e apoio centra-se na implementação em OpenWRT e na criação de hotspots, sendo a sua gestão via *homepage* do CoovaChilli. Como neste projecto a gestão deveria ser local, a mesma implicava que fosse comprada.

Depois de ter sido implementado, foi detectada a existência de algumas limitações do software que não se adequavam ao projecto. A mais importante centrava-se na forma como os utilizadores eram guardados. O CoovaChilli requeria que os utilizadores fossem guardados em ficheiros de texto, o que limitava um grande número de utilizadores, como também requeria que o serviço de hotspot fosse reiniciado cada vez que um utilizador fosse adicionado, para que o *daemon* do processo lesse as alterações efectuadas.

Um dos objectivos do projecto trata-se de o administrador de rede poder indicar quando o login do utilizador é válido e quando deixa de ser válido. O CoovaChilli não implementava nenhuma destas duas características. Como tal, era necessário contornar a situação. Se por um lado era possível calcular o período de tempo em que a conta deixava de ser válida, através da diferença de tempo, a implementação de quando a conta passava a ser válida era algo mais complicado. Uma das formas possíveis seria com recurso ao *crontab*, em que o utilizador seria adicionado ao sistema no dia e hora marcados. No

entanto, como já foi indicado, cada vez que um utilizador fosse adicionado ao sistema, o *daemon* teria que ser reiniciado.

Se este sistema fosse mantido, poderia causar erros em dois cenários possíveis. O primeiro cenário é que se a empresa tivesse um grande conjunto de utilizadores, o sistema de reiniciar o processo de cada vez que é inserido um utilizador, poderia conduzir a quebras do serviço pois os utilizadores não se podem autenticar durante esse período de tempo. Outro cenário possível, seria acabar com o limite em termos de horas (contando apenas os dias) que o utilizador precisa, bastando para tal que o serviço reinicie uma vez por dia. Contudo, caso um utilizador se deslocasse a uma empresa, e só deveria ter acesso entre as 12h e as 14h, passaria a ter acesso durante o dia todo. Outro caso é o pedido para o utilizador chegar às 9h (ao administrador) para permitir que o utilizador tivesse acesso entre as 20h e as 22h, e a hora marcada para reiniciar o processo ser posterior a este horário.

Relativamente aos IP's, o CoovaChilli não permitia que fosse usado um servidor DHCP externo, apesar de ser possível atribuir endereços físicos (através da MAC Address). Para além disso, permitia limitar a gama de endereços disponíveis (ao contrário do ChilliSpot que não permitia reduzir o número de endereços disponíveis). Os endereços IP fixos também são guardados em ficheiros de texto, acarretando as mesmas limitações que a gestão dos utilizadores.

Outro problema referia-se a não ser possível efectuar uma distinção de serviços para cada tipo de utilizador, ou seja, apenas era possível definir um conjunto de serviços tipo e aplicá-lo a todos os utilizadores, algo que já acontece nas redes wireless e que não se pretendia que acontecesse neste projecto.

Um sistema de hotspot necessita que o funcionamento da rede seja efectuado de modo "aberto", pois o utilizador só é autenticado quando tenta aceder à Internet, e para tal já deverá ter IP atribuído. Este facto levanta alguns problemas de segurança, uma vez que torna possível alguém explorar alguma falha de segurança do CoovaChilli.

Por último, um passo não tão importante mas que não deixa de ser necessário numa rede empresarial, que é a redundância. Não era possível ter mais do que um servidor a correr na mesma rede e que funcionasse ao mesmo tempo ou que entrasse em funcionamento quando outro servidor deixava de responder.

Assim, tendo em contas estas limitações e o seu desenvolvimento ser realizado apenas por um grupo pequeno de pessoas, tornava-se importante procurar outra solução mesmo que fosse necessário sacrificar outros aspectos.

5.8.2 Desvantagens da solução escolhida

A grande desvantagem da solução final prende-se com o facto de o utilizador final necessitar de configurar o acesso à rede. Apesar de as instruções a realizar serem simples,

não é na forma de caixa diálogo onde é pedido username e password e já se encontra a funcionar.

É possível que este facto não tenha sido reparado agora neste projecto, visto que a solução é inspirada na rede “eduroam”, e seja desenvolvido um novo protocolo de autenticação mais seguro e sem estas limitações de configurações (mais automatizado).

Capítulo 6

Conclusões e Trabalho futuro

Este capítulo pretende apresentar algumas conclusões que foram retiradas do projecto, bem como dar uma opinião pessoal sobre a forma como decorreu o estágio e as mais valias retiradas do mesmo. Sendo este um projecto de quatro meses, onde é necessário incluir tempo para pesquisar informação e elaborar os documentos necessários do projecto, torna-se difícil não apresentar melhoramentos. Estes melhoramentos são divididos em duas partes; uma referente a um conjunto de software que melhora a segurança e qualidade da rede, e outra parte onde são apresentadas algumas ideias para permitir a expansão do projecto.

6.1 Satisfação dos objectivos

Tendo o projecto sido desenvolvido segundo os objectivos propostos, é possível afirmar que os mesmos foram atingidos. Como a proposta de trabalho implicava que o projecto fosse o mais flexível possível, foi criada uma solução facilmente expansiva a outros objectivos ou requisitos da empresa onde se implemente a solução. O facto de terem sido usados protocolos standard e aplicações de software aberto, permite que esta seja integrada na rede da empresa e seja possível adaptar os equipamentos de rede à nova solução.

Um dos objectivos implicava que o utilizador acedesse à rede sem a necessidade de instalação de qualquer tipo de software específico. Este facto permite não só ao utilizador aceder à rede wireless mais rapidamente, como também contribui para um maior nível de confiança dos utilizadores. Contudo, apesar de o nível de configuração ser bastante simples, requer ainda alguns passos prévios para poder aceder à rede. Este facto ocorre devido ao sistema operativo Windows colocar como opção por defeito a autenticação por smart card ou certificado. Esta situação não é, no entanto, algo incomum pois para que os

utilizadores acedam a outras redes com o mesmo tipo de autenticação, como por exemplo a rede "eduroam", necessitam de utilizar as mesmas configurações.

Com a evolução das redes wireless e o surgimento de novos protocolos, é possível que o sistema operativo Windows passe a suportar outros protocolos como o EAP-TTLS, que possibilita ao utilizador introduzir apenas as suas credenciais. Aliás, o principal factor de não ter sido usado este protocolo, deve-se mesmo à necessidade de instalação do SecureW2 por parte dos utilizadores nos seus equipamentos.

Não é demais salientar a evolução que os projectos de hotspot têm tido estes últimos anos e a quantidade de locais onde já é possível utilizar este tipo de rede. Cada vez mais, as empresas direccionam os projectos de software tendo em conta as necessidades das empresas e sempre com o intuito de criar algo que ainda não desenvolvido, não é de descurar a possibilidade de num futuro próximo a existência de um software que já permita implementar esta solução numa ferramenta integrada e que desta forma aumente a segurança das redes wireless.

6.2 Relato da minha experiência

Este trabalho permitiu para mim aumentar os conhecimentos adquiridos ao longo do curso, bem como adquirir experiência em diversas ferramentas. O facto de no curso existir algumas cadeiras de redes, não permite ao estudante obter a prática e os conhecimentos necessários para se evoluir nesta área, sendo bastante importante a realização deste tipo de estágio no decorrer do curso.

Outro facto importante, trata-se de o mesmo ter sido realizado no INESC Porto, o que permitiu estar integrado no mundo real, observando e evidenciar as dificuldades dos utilizadores e os problemas que surgem na rede. Sendo um instituto com alguma dimensão, permitiu tomar conhecimento sobre como foi planeada a rede para os utilizadores actuais e futuros, tendo em conta a chegada de novos utilizadores.

É também de salientar as diversas dificuldades que foram ocorrendo ao longo do curso, nomeadamente na instalação de diversos programas, pois a documentação existente não se encontrava completa. Uma das falhas mais encontradas em programas de desenvolvimento aberto é a documentação não acompanhar a evolução do programa e existir mudanças radicais nas várias versões do software. Este último facto torna outro tipo de documentação, criada por entusiastas, obsoleta. Estas dificuldades, apenas puderam ser superadas após a realização de muitas pesquisas e a perda de um elevado número de horas para a sua resolução.

6.3 Software suplementar

Como já referido, os melhoramentos centram-se em duas partes. Nesta primeira é apresentado um conjunto de ferramentas auxiares que permite aumentar a segurança dos dados que circulam na rede, como também proporcionar ao utilizador uma melhor experiência de acesso a rede. É importante indicar que as empresas, podem já ter algum deste software implementado, o que apenas faz sentido instalar neste projecto se o objectivo for mesmo ter uma rede "separada" da rede actual.

6.3.1 OpenSSL

O OpenSSL é um projecto de software livre que implementa protocolos criptograficos nomeadamente o SSL (v2/v3) e o TLS(v1). A implementação deste software visa a necessidade de proteger a forma como os dados circulam entre o servidor RADIUS e LDAP. Sendo o servidor o mesmo, só existe perigo quando o computador for invadido. Caso não seja o mesmo servidor, os dados vão circular na rede de forma aberta e susceptível de qualquer programa de captura de pacotes obter essa informação.

Este software estabelece um túnel seguro entre os dois programas, e a informação passa a circular encriptada na rede (apesar de manter os dados transmitidos).

6.3.2 Proxy

Já foram referidas quais as vantagens da implementação de um proxy na rede de uma empresa. No entanto, pode suceder-se o caso de o hotspot criado numa empresa ser utilizado por um conjunto elevado de pessoas e dessa forma torna-se precioso implementar um proxy separado do proxy da empresa, quer para responder mais rapidamente aos pedidos dos utilizadores, quer para a gestão de acessos.

Para minimizar o número de configurações por parte dos utilizadores, a implementação de um proxy deverá ficar de forma transparente para o utilizador. Este facto pode ser conseguido através de duas formas. A primeira é com recurso à implementação do mesmo gateway para todos os utilizadores e dessa forma ser instalado o proxy (o tráfego era redireccionado através do iptables). Uma segunda hipótese seria através do protocolo WCCP (*Web Cache Coordination Protocol*) que é propriedade da Cisco Systems e que já se encontra na segunda versão. Este protocolo é implementado em routers Cisco que analisam o tráfego da rede; quando existe algum pacote que tenha de passar pelo proxy, este é redireccionado para ele.

As principais vantagens traduzem-se no facto do utilizador não necessitar de realizar configurações no seu sistema operativo, nem precisar de saber que existe um proxy a correr dentro da empresa. Outra questão importante é a possibilidade de criação de

ACL (*Access Control List*) que permite que certos endereços que necessitam de funcionar directamente, não sejam reencaminhados para o proxy.

6.3.3 DNS

Quando um browser tenta aceder a uma determinada página, necessita primeiro de ”saber” qual o IP onde se encontra alojado o mesmo. Esta tradução é realizada com recurso a servidores DNS. Normalmente as empresas já apresentam implementado um servidor próprio, mas no caso de se pretender isolar a rede de hotspot da restante rede, é necessária a implementação de um servidor DNS próprio. Este permite acelerar o tempo de resposta, caso existe muitos utilizadores na rede.

6.3.4 SNMP

O protocolo SNMP (*Simple Network Management Protocol*) é usado para realizar a gestão e monitoramento da rede e dos equipamentos que pertencem à mesma. Este foi desenvolvido pelo IEFT e faz parte do TCP/IP. Uma das principais vantagens seria de controlar todos os equipamentos (AP, switch, servidores) que se encontram a funcionar, e em caso de erro poder alertar o administrador da rede para poder verificar a situação e prestar um melhor serviço de rede ao utilizador.

6.3.5 QoS

A implementação do QoS (*Quality of Service*) permite gerir melhor o tráfego dando uma maior prioridade a determinados serviços. Normalmente, os serviços de multimédia e VoIP necessitam de ter uma velocidade mínima para garantir o mínimo de qualidade do serviço. Esta velocidade mínima é garantida, dando preferência aos dados destes serviços em detrimento de outros (que se podem atrasar).

O QoS é um serviço que pode ser implementado no router de saída da empresa, pois tipicamente é o local de estrangulamento, visto que uma rede empresarial comunica toda no mínimo a 100 Mbit/s, embora ainda não se encontrem acessos a Internet com a mesma velocidade.

Curiosamente, um consórcio sem fins lucrativos que desenvolve e estuda mecanismos avançados para aplicações de rede, denominado por *Internet2* chegou à conclusão que aumentando a banda disponível, seriam obtidos mais resultados práticos, do que implementando o QoS. É essencial lembrar que o aumento da banda disponível não ocorre apenas com o aumento da velocidade de contratação do serviço do ISP, mas também reduzindo o tráfego desnecessário (com recurso, por exemplo, ao proxy).

6.3.6 Accounting em MySQL

O servidor de RADIUS possui mecanismos que permite efectuar o login de todos os clientes. Contudo, esta informação centra-se em ficheiros de texto. O FreeRadius cria um ficheiro novo para cada cliente (neste caso, os clientes do RADIUS são os AP's) e para cada dia. Este traz consigo ferramentas poderosas que permitem compilar essa informação no que for requerido, embora essa mesma informação continue a encontrar-se em ficheiros de texto.

A implementação de um servidor MySQL, permitia armazenar toda a informação referente ao *Accounting* do RADIUS e dessa forma torna seria possível, através de queries SQL (*Structured Query Language*), apresentar diversos tipos de relatórios. Outra das vantagens, é a quantidade de dados que podem ser armazenado num sistema SGBD ser muito maior que em ficheiros.

6.4 Outros melhoramentos

Nesta parte, pretende-se demonstrar algumas ideias que poderiam dar mais recursos aos utilizadores temporários. Contudo, não deixa de ser possível aplicar estas mesmas ideias na rede já existe para os trabalhadores das empresas poderem também usufruir das mesmas melhorias.

6.4.1 Permissões de impressão

Uma das acções que um utilizador pode realizar no computador é imprimir. Normalmente esta acção encontra-se desactivada para pessoas de fora, sendo apenas atribuída quando é requerido pelas mesmas ou por superiores (devido aos custos que comportam).

Como o actual sistema faz uso do protocolo RADIUS, é possível dar permissões a um utilizador temporário e atribuir os custos. Para tal, é necessário que as impressoras comuniquem com o RADIUS para determinar se devem ou não imprimir trabalhos de determinado utilizador. Os custos seriam reportados através do *Accounting* do RADIUS e imputados ao "responsável" do utilizador.

Desta forma surgiriam vantagens, pois deixaria de ser preciso que o utilizador trouxesse já imprimido determinado documento (pois poderia até não ser preciso) como também deixaria de ser preciso que os documentos tivessem de ser transferidos para outro computador que tem permissões de impressão.

6.4.2 Integração com Active Directory

Este projecto apenas foi pensado para permitir a atribuição de permissões de acesso a rede a utilizadores temporários através da rede wireless. Pode também dar-se o caso de a empresa possuir um espaço com computadores que são utilizados pelos seus funcionários apenas quando lá estão (como o caso de empresas de auditores ou vendedores ambulantes). Normalmente neste tipo de espaços, os utilizadores não têm um computador pré-definido ,utilizando aquele que se encontra livre, enquanto que o seu perfil se encontra guardado num computador central que permite aceder de qualquer máquina.

A implementação de um servidor com AD (*Active Directory*) permite que os utilizadores acedam aos equipamentos com o mesmo login. A integração do AD com o LDAP vem também permitir que os utilizadores temporários possam aceder a rede wireless como também a estes mesmo computadores.

6.4.3 SSID guest

O SSID guest normalmente é conhecido por uma rede aberta que apenas contém instruções de acesso à rede. Apesar de não ser uma verdadeira inovação, não deixa de ser útil uma empresa poder disponibilizar uma rede destas para permitir que o utilizador aceda às instruções dos diversos sistemas operativos, em diversas línguas, como também de certificados de acesso.

6.4.4 Integração DHCP com LDAP

Em certas empresas, onde a segurança está em primeiro lugar, pode acontecer situações de o servidor DHCP não atribuir IP's a computadores que não tenham o seu MAC address previamente registado. Como tal, o utilizador precisa que o seu MAC address esteja registado no servidor, e precisa também que essa informação apenas esteja disponível durante o tempo que o utilizador pode usufruir. Uma das formas de garantir isso é com recurso ao servidor LDAP.

Normalmente, os *daemons* DHCP guardam a informação em ficheiros de configuração. Contudo, com a utilização de sripts, é possível reconstruir esses mesmos ficheiros, mas preenchendo os mesmos com informação constante no LDAP. Assim, torna-se necessário criar uma sub-árvore apenas para objectos DHCP, mas com o campo *seeAlso* é possível indicar a quem pertence o MAC address indicado.

Com este caso, seriam necessários dois scripts adicionais; um para adicionar o MAC address ao servidor LDAP e outro para retirar o mesmo. Torna-se também necessário que o servidor DHCP reinicie para que possam correr as novas alterações.

6.4.5 Interface administrador

Apesar de não estar directamente ligado com a experiência do utilizador, o "administrador" faz parte da rede, e como tal não pode ser esquecido. Quando as credenciais são criadas no servidor LDAP, o mesmo necessita de passar por diversos passos, uma vez que as interfaces apresentam o directório como um todo. Uma das formas de minimizar esta situação, seria a criação de formulários em PHP onde bastaria clicar na opção que se pretende realizar, preencher a informação necessário e esse mesmo formulário realizaria os passos todos. No caso de adicionar um utilizador, o formulário deveria ser capaz de adicionar o mesmo ao servidor LDAP, criar o ficheiro de texto em LDIF, o ficheiro de script em *Perl* e adicionar o mesmo ao *cronotab*, tudo isto, com uma só operação.

Referências

[2ho09] 2hotspot. 2hotspot homepage, Março 2009. http://www.2hotspot.com/.

[Caf09] CafeRadius. Caferadius homepage, Março 2009. http://www.caferadius.com/.

[Car03] Gerald Carter. *LDAP System Administration*. O'Reilly Media, March 2003.

[Chi09] Chillispot. Chillispot homepage, Março 2009. http://www.chillispot.info/.

[Coo09] CoovaChilli. Coovachilli homepage, Março 2009. http://coova.org/wiki/index.php/CoovaChilli.

[Cor09] Oracle Corporation. Oracle berkeley db product family, Abril 2009. http://www.oracle.com/technology/products/berkeley-db/index.html.

[Exp09] Softvision Explorer. Softvision explorer homepage, Março 2009. http://www.cyber-cafe-software.com/.

[Fir09a] Firewall.cx. Designing vlans - a comparison with old networks, Maio 2009. http://www.firewall.cx/vlans-designing-intro.php.

[Fir09b] FirstSpot. Firstspot homepage, Março 2009. http://www.patronsoft.com/firstspot/.

[Git09] Vivek Gite. Linux demilitarized zone, Março 2009. http://www.cyberciti.biz/faq/linux-demilitarized-zone-howto/.

[Has02] Jonathan Hassell. *RADIUS*. O'Reilly Media, October 2002.

[Hot09] Antamedia Hotspot. Antamedia hotspot homepage, Março 2009. http://www.antamedia.com/.

[McL09] William McLachlan. Public/private ip numbers, Março 2009. http://www.wmld.com/tech/privateipnums.html.

[Mik09] MikroTik. Mikrotik homepage, Março 2009. http://www.mikrotik.com/.

[Sch09] Carla Schroder. Wireless authentication and encryption with zeroshell linux, Abril 2009. http://www.enterprisenetworkingplanet.com/netsecur/article.php/3744881.

[Sof09] Nonius Software. Nonius software homepage, Junho 2009. http://www.noniussoftware.com/.

[Tec06] Javvin Technologies. *Network Protocols Handbook*. Javvin Technologies, Março 2006.

[tec09a] techFAQ. What is voip?, Abril 2009. http://www.tech-faq.com/voip.shtml.

[Tec09b] Microsoft TechNet. What is vpn?, Abril 2009. http://technet.microsoft.com/en-us/library/cc739294(WS.10).aspx.

[Zon09] ZoneCD. Zonecd homepage, Março 2009. http://www.publicip.net/.

Anexo A

RADIUS

De entre os diversos fabricantes de software RADIUS, foi decidido apenas efectuar uma comparação conjunta entre o Cisco Systems Secure Access Control Server, Navis Radius, OSC Radiator, FreeRadius, Microsoft IAS e GNU Radius. De entre os seis fabricantes, apenas dois são softwares livres e como tal o seu custo é nulo.

Para uma melhor compreensão da informação recolhida, foram criadas diversas tabelas que se encontram divididas desde suporte a protocolos de informação, locais para armazenar os dados, sistemas operativos suportados, ferramentas de configuração, políticas de segurança, ferramentas de análise e por fim a possibilidade de apresentar outras ferramentas. Para simplificar a informação na tabela, os nomes dos programas foram encolhidos, mas segue a mesma ordem que foi apresentada acima. Nas tabelas é possível encontrar espaços em branco. Este facto deve-se a não se conseguir apurar se o software suporta ou não a funcionalidade.

A.1 Autenticação

	CSSA	Navis	Radiator	Free	IAS	GNU
CHAP	Sim	Sim	Sim	Sim		Sim
PEAP	Sim	Sim	Sim	Sim	Sim	Sim
EAP-TLS	Sim	Sim	Sim	Sim	Sim	Sim
EAP-TTLS	Sim	Sim	Sim	Sim		Sim
EAP-MD5-Challenge		Sim	Sim	Sim	Sim	Sim
EAP-PSK		Sim	Sim	Sim		
EAP-GTC		Sim	Sim	Sim		
MS-CHAP	Sim	Sim	Sim	Sim	Sim	Sim
MS-CHAP2	Sim	Sim	Sim	Sim	Sim	Sim
PAP	Sim	Sim	Sim	Sim		Sim

Tabela A.1: Tabela comparativa RADIUS: Autenticação

A.2 Armazenamento da informação

	CSSA	Navis	Radiator	Free	IAS	GNU
Ficheiro texto	Sim	Sim	Sim	Sim		Sim
Kerberos	Não	Não	Sim	Sim (plugin)		
LDAP	Sim	Sim	Sim	Sim	Sim	Sim
Proxy server	Sim	Sim	Sim	Sim	Sim	
SQL	Sim	Sim	Sim	Sim	SQL server	Sim
TACACS+	Sim	Não	Sim	Não		
Unix	Sim	Sim	Sim	Sim		Sim

Tabela A.2: Tabela comparativa RADIUS: Armazenamento da informação

A indicação de plugin, indica que este software não suporta, de origem, guardar os dados com o Kerberos, mas que através de uma ferramenta extra, é possível ter esta funcionalidade. Relativamente ao Microsoft IAS, apenas suporta o servidor de base de dados SQL server.

A.3 Sistema operativo

	CSSA	Navis	Radiator	Free	IAS	GNU
Linux	Sim	Sim	Sim	Sim	Não	Sim
Windows	Sim	Sim	Sim	Sim	Sim	Não

Tabela A.3: Tabela comparativa RADIUS: Sistema operativo

A.4 Gestão sistema

	CSSA	Navis	Radiator	Free	IAS	GNU
Suporte simultâneo de protocolos	Sim	Sim	Sim			
Configuração utilizadores	Sim	Sim	Sim	Sim	Sim	Sim
Detecção de inactividade	Sim	Sim	Sim	Sim	Sim	Sim
Tempo de sessão	Sim	Sim	Sim	Sim	Sim	Sim
Atribuição IP por utilizador	Sim	Sim	Sim	Sim	Sim	Sim
SSL certs para LDAP	Sim	Não	Sim	Sim		Sim

Tabela A.4: Tabela comparativa RADIUS: Gestão sistema

A.5 Gestão de segurança

	CSSA	Navis	Radiator	Free	IAS	GNU
Limite tempo	Sim	Sim	Sim	Sim	Sim	
Restrição em dias marcados	Sim	Sim	Sim	Sim	Sim	
Restrição de apenas 1 login	Sim	Sim				
Filtro de pacotes RADIUS	Sim	Sim		Sim		

Tabela A.5: Tabela comparativa RADIUS: Gestão Segurança

A.6 Ferramentas de log

	CSSA	Navis	Radiator	Free	IAS	GNU
Informação	Tabela	Gráfico	Gráfico	Sim	SQL server	Sim
Monitorização	Sim	Sim	Sim	Sim		Sim
Definições de logging	Sim	Sim	Sim	Sim	Sim	Sim
Notificação por e-mail	Não	Sim	Sim			

Tabela A.6: Tabela comparativa RADIUS: Ferramentas de log

Todos os programas permitem guardar os dados de utilização, contudo alguns deles também possuem ferramentas para mostrar os dados analiticamente. A forma de apresentação dos dados pode ser realizada em tabelas ou em gráficos. Nesta tabela, quando se indica que o programa permite mostrar a informação em gráficos, o mesmo permite que a informação seja disponível em tabelas. No caso do Microsoft IAS, os dados são guardados em SQL server e a informação pode ser tratada como uma base de dados normal.

A.7 Outras funcionalidades

	CSSA	Navis	Radiator	Free	IAS	GNU
Dicionários fabricantes	Sim	Sim	Sim	Sim		
SNMP	Não	Sim	Sim	Sim		Sim
DHCP	Não	Sim		Sim	Windows	Sim
DNS	Sim	Sim			Windows	
LDAP integrado	Não	Não	Não	Não	Windows	Não
Possui cliente teste	Sim	Sim	Sim	Sim		Sim
BD integrada	Sim	Sim	Sim	Sim		Sim
Taxação VoIP	Sim	Não	Sim			

Tabela A.7: Tabela comparativa RADIUS: Outras funcionalidades

Como o Microsoft IAS apenas funciona em Windows Server, as funcionalidades de DHCP, DNS e LDAP (Active Directory) são efectuadas pelo sistema operativo.

Anexo B

Configurações

O ponto mais importante deste projecto centra-se na informação que é guardada no servidor LDAP. Ao criar o utilizador, eram necessários vários objectos e repetir atributos para a informação ficar toda guardada. Para uma melhor gestão do ponto de vista administrativo, foi necessário criar atributos e objectos específicos para este projecto. A informação seguinte pretende apresentar o ficheiro completo que já foi mencionado no relatório.

Para uma melhor compreensão da informação que é guardada no LDAP,é também apresentado um exemplo de um utilizador temporário da rede wireless. Outras configurações, necessárias para executar os programas, foram colocadas de parte, pois não apresentam informação extra.

B.1 Ficheiro hotspot.schema

```
    # OpenLDAP hotSpot schema
# This work is part of Antonio Barbosa Project
#
# Copyright 2009 Antonio Barbosa Project.
# All rights reserved.
#
# Version: 0.5
# Date: 2009-06-01
# OID allocate to INESC Porto - 1.3.6.1.4.1.33536
# OID allocate to hotspot - 1.3.6.1.4.1.33536.1
# OID allocate to attributeTypes hotspot - 1.3.6.1.4.1.33536.1.1
# OID allocate to objectClasses hotspot - 1.3.6.1.4.1.33536.1.2
# RFC 4517

##### Attribute types ######
# Nome do utilizador
# 3.3.29. Printable String
attributetype ( 1.3.6.1.4.1.33536.1.1.101
    NAME 'nomeUtilizador'
    DESC 'Nome do utilizador'
    EQUALITY caseIgnoreMatch
```

```
    SUBSTR caseIgnoreSubstringsMatch
    ORDERING caseIgnoreOrderingMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.44200 )

# Empresa do utilizador
# 3.3.29. Printable String
attributetype ( 1.3.6.1.4.1.33536.1.1.102
    NAME 'empresaUtilizador'
    DESC 'Empresa do utilizador'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    ORDERING caseIgnoreOrderingMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.44200 )

# Motivo da deslocacao
# 3.3.29. Printable String
attributetype ( 1.3.6.1.4.1.33536.1.1.103
    NAME 'motivoDeslocacao'
    DESC 'Motivo da deslocacao'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    ORDERING caseIgnoreOrderingMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.44200 )

# Servicos pretendidos
# 3.3.29. Printable String
attributetype ( 1.3.6.1.4.1.33536.1.1.104
    NAME 'servicos'
    DESC 'Servicos pretendidos'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    ORDERING caseIgnoreOrderingMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.44200 )

# Nome do responsavel
# 3.3.29. Printable String
attributetype ( 1.3.6.1.4.1.33536.1.1.105
    NAME 'nomeResponsavel'
    DESC 'Nome do responsavel'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    ORDERING caseIgnoreOrderingMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.44200 )

# Numero funcionario responsavel
attributetype ( 1.3.6.1.4.1.33536.1.1.106
    NAME 'numeroFuncionario'
```

```
    DESC 'Numero funcionario responsavel'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 )

# E-mail do responsavel
# 3.3.29. Printable String
attributetype ( 1.3.6.1.4.1.33536.1.1.107
    NAME 'emailResponsavel'
    DESC 'E-mail do responsavel'
    EQUALITY caseIgnoreIA5Match
    SUBSTR caseIgnoreIA5SubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26200 )

# Periodo de estadia
# 3.3.29. Printable String
attributetype ( 1.3.6.1.4.1.33536.1.1.108
    NAME 'periodoEstadia'
    DESC 'Periodo de estadia'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    ORDERING caseIgnoreOrderingMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.44200 )

# Observacoes
attributetype ( 1.3.6.1.4.1.33536.1.1.109
    NAME 'observacoes'
    DESC 'Observacoes'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    ORDERING caseIgnoreOrderingMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.151024 )


#### Object classes #####

objectclass ( 1.3.6.1.4.1.33536.1.2.100
    NAME 'hotspot'
    DESC 'User from hotspot'
    SUP top
    AUXILIAR
    MUST ( uid )
    MAY (
        nomeUtilizador $ empresaUtilizador $ motivoDeslocacao $ servicos $
        nomeResponsavel $ numeroFuncionario $ emailResponsavel $
        periodoEstadia $ observacoes $ userPassword)
    )

# Nao usado. Apenas para testes
```

```
objectclass ( 1.3.6.1.4.1.33536.1.2.101
    NAME 'hotspot2'
    DESC 'User from hotspot'
    SUP organizationalPerson
    STRUCTURAL
    MUST ( sn $ cn )
    MAY (
        nomeUtilizador $ empresaUtilizador $ motivoDeslocacao $ servicos $
        nomeResponsavel $ numeroFuncionario $ emailResponsavel $
        periodoEstadia $ observacoes $ uid $ userPassword)
    )
```

B.2 Estrutura de utilizador em LDIF

```
dn: uid=teste345,ou=hotspot,dc=inescporto,dc=pt
objectClass: hotspot
objectClass: top
objectClass: radiusprofile
objectClass: pwdPolicy
uid: teste345
nomeUtilizador: Antonio Cunha Barbosa
motivoDeslocacao: Estagio Curricular
empresaUtilizador: FEUP
nomeResponsavel: Joao Neves
emailResponsavel: joao.neves@inescporto.pt
numeroFuncionario: 1234
observacoes: Nada a apontar
periodoEstadia: 25 Fev 2009 a 29 Jun 2009
servicos: Internet, VPN FEUP, Messenger
userPassword:: dGVzdGU=
radiusServiceType: Framed-User
radiusTunnelMediumType: IEEE-802
radiusTunnelType: VLAN
radiusTunnelPrivateGroupId: 10
radiusSimultaneousUse: 1
radiusExpiration: "Jul 17 2009 17:00:00 WEST"
pwdAttribute: userPassword
pwdCheckQuality: 2
pwdAccountLockedTime: 000001010000Z
```