**Universidade de Aveiro**
**2010**
Departamento de Electrónica, Telecomunicações e Informática

**Veridiano António Fernandes de Carvalho e Silva**

# Soluções Wireless / VoIP para Redes Comunitárias.

**Universidade de Aveiro**
**2010**
Departamento de Electrónica, Telecomunicações e Informática

**Veridiano António Fernandes de Carvalho e Silva**

# Soluções Wireless / VoIP para Redes Comunitárias.

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Computadores e Telemática, realizada sob a orientação científica do Dr. A. Manuel de Oliveira Duarte, Professor Catedrático do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.

Em primeiro lugar, dedico este trabalho aos meus pais Francisco e Sílvia pelo amor, educação, credibilidade e carinho que me deram durante toda minha vida, pois sem eles não me tornaria na pessoa que hoje sou.

Em segundo lugar, dedico-o às minhas queridas irmãs Helena, Íris e Cybélle, pelo apoio sistemático e incentivo à elaboração deste trabalho.

Por último, agradeço aos meus demais amigos (as) e restantes familiares que de uma forma directa ou indirecta me deram o total apoio na elaboração deste projecto.

**o júri**

| | |
|---|---|
| Presidente | Professor Doutor Atílio Manuel da Silva Gameiro<br>Professor Associado da Universidade de Aveiro |
| Arguente externo | Professor Doutor Adriano Moreira<br>Professor Associado da Universidade do Minho |
| Arguente interno | Professor Doutor Aníbal Manuel de Oliveira Duarte<br>Professor Catedrático da Universidade de Aveiro |

**agradecimentos**

Ao Prof. Doutor Manuel de Oliveira Duarte pelo entusiasmo constante que transmitiu, pela inspiração que incutiu e pela indispensável orientação ao longo de toda elaboração do projecto. Agradeço, também, a preciosa contribuição na forma de sugestões, críticas e reparos durante a concepção deste trabalho.

Aos colegas do GSBL – Grupo de Sistemas de Banda Larga, que estiveram envolvidos no projecto, pela colaboração e espírito de camaradagem.

**palavras-chave**

VoIP – Voz sobre IP, Protocolo Internet, SIP, H.323, IAX, SDP, RTP, SIP Proxing, IP PBX - Asterisk, PTSN, *Softphones*, Voip nas Redes Comunitárias, VoIP em *Mesh Network*, *Wireless Mesh Networks*.

**resumo**

Nas últimas décadas, a evolução das novas Tecnologias de Informação e Comunicação (TIC), contribuiu em larga escala para o crescimento da Internet e da utilização massificada das tecnologias de banda larga. Com essa evolução, surgiram novas formas de comunicar recorrendo a tecnologias inovadoras, baseadas no protocolo IP (*Internet Protocol*). Contudo, surgiram assim os softphones, que são as primeiras aplicações da tecnologia VoIP, que vieram revolucionar a forma de comunicar, com custos substancialmente reduzidos, que causaram um enorme impacto nas pessoas e nas organizações.

Com o presente trabalho, pretende-se elaborar um estudo minucioso das tecnologias VoIP, apresentando algumas soluções de implementação de um sistema de comunicações VoIP para uma rede comunitária de banda larga.

Por último, será apresentada uma proposta de arquitectura, descrevendo os possíveis cenários de implementação de um fornecedor de comunicações VoIP numa *Mesh network* de rede comunitária.

**keywords**

VoIP – Voice over IP, Internet Protocol, SIP, H.323, IAX, SDP, RTP, SIP Proxing, IP PBX - Asterisk, PTSN, Softphones, VoIP in Communitary networks VoIP in Mesh Network, Wireless Mesh Networks.

**abstract**

In latest decades, the evolution of new Information and Communication Technologies (ICT) has contributed a large scale for the growth of the Internet and use mass of broadband technologies. With these developments, there were new ways to communicate using innovative technologies, based on the protocol IP (Internet Protocol). However, emerged as the softphone, which are the first applications of the technology VoIP, who came to revolutionize the way of communicating, with costs substantially reduced, which caused a huge impact on people and organizations. With this work, it is intended to prepare a detailed study of the technology VoIP, providing some solutions for implementing a communication system to a VoIP network of community broadband. Finally, will be a proposal for architecture, describing the possible scenarios for implementing a VoIP provider of communications network in a mesh network community.

# ÍNDICE

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABELAS

# LISTA DE ABREVIATURAS E ACRÓNIMOS

| | |
|---|---|
| **AAA** | Autentication, Authorization and Accounting |
| **ACELP** | Algebraic Code Excited Linear Prediction |
| **ADPCM** | Adaptive Differential Pulse-Code Modulation |
| **ADSL** | Asymmetric Digital Subscriber Line |
| **AES** | Advanced Encryption Standard |
| **ANACOM** | Autoridade Nacional de Comunicações. |
| **AP** | Access Point |
| **API** | Application Programming Interface |
| **AS** | Application Server |
| **ASCII** | American Standard Code for Information Interchange |
| **ATA** | Analogue Telephone Adapter |
| **BSA** | Basic Service Area |
| **BSS** | Basic Service Set |
| **BSSID** | Basic Service Set Identifier |
| **CDMA** | Code Division Multiple Access |
| **CDMA/CA** | Code Division Multiple Access with Collision Avoidance |
| **CDMA/CD** | Carrier Sense Multiple Access with Collision Detection |
| **CDR** | Call Detail Records |
| **CNAME** | Canonical Name |
| **CRC** | Cyclic Redundancy Check |
| **CSMA** | *Carrier Sense Multiple Access* |
| **DA** | Destination Address |
| **DCF** | Distributed Coordination Function |
| **DECT** | Digital Enhanced Cordless Telecommunications |
| **DETI** | Departamento de Electrónica, Telecomunicações e Informática. |
| **DHCP** | Dynamic Host Configuration Protcol |
| **DNS** | Domain Name System |
| **DS** | Distribution System |
| **DSSS** | Direct Sequence Spread Spectrum |
| **DTMF** | Dual Tone Multi Frequency |
| **DVC** | Desktop Video Conferencing |
| **ESS** | Extended Service Set |
| **FAQs** | Frequently Asked Questions. |
| **FCS** | Frame Check Sequence |
| **FDDI** | Fiber Distributed Data Interface |
| **FHSS** | Frequency Hopping Spread Spectrum |
| **FOP** | Flash Operator Panel |
| **FWA** | Fixed Wireless Access |
| **FXO** | Foreign eXchange Office |
| **FXS** | Foreign eXchange Subscriber |
| **GK** | Gatekeeper |
| **GPL** | Gnu Public License |
| **GSBL** | Grupo de Sistemas de Banda Larga. |
| **GW** | Gateway |
| **H.323** | Rec. da UIT-T "Packet-based multimedia communications systems" |
| **HTML** | HyperText Markup Language |
| **HTTP** | Hyper Text Transfer Protocol |
| **IAX** | Inter Asterisk eXchange |

| | |
|---|---|
| **IBSS** | Independent Basic Service Set |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **IEETA** | Instituto de Engenharia Electrónica e Telemática de Aveiro. |
| **IETF** | Internet Engineering Task Force |
| **IFS** | Inter Frame Spacing |
| **IM** | Instant Messaging |
| **IP** | Internet Protocol. |
| **IPS** | Internet Service Provider |
| **IPX** | Internet Packet eXchange |
| **ISDN** | Integrated Services Digital Network |
| **ISM** | Industrial, Scientific and Medical |
| **ITU-T** | International Telecommunication Union Telecommunication |
| **IVR** | Interactive Voice Response |
| **LAN** | Local Area Network. |
| **LLC** | Logical Link Control |
| **LWMP** | Light Weight MP |
| **MAC** | *Media Access Control* |
| **MANET** | Mobile Ad-Hoc NETwork |
| **MAP** | Mesh Access Point |
| **MBone** | Multicast Backboneon the Internet |
| **MCU** | Multi Control Unit |
| **MGCP** | Media Gateway Control Protocol |
| **MIECT** | Mestrado Integrado em Eng.ª Computadores e Telemática. |
| **MIME** | Multipurpose Internet Mail Extension |
| **MIME** | Multipurpose Internet Mail Extensions |
| **MIMO** | Multiple Input Multiple Output |
| **MIT** | Massachusetts Institute of Technology |
| **MMUSIC** | Multiparty Multimédia Session Control |
| **MP** | Mesh Point |
| **MPEG** | Moving Picture Experts Group |
| **MPP** | Mesh Portal |
| **NAT** | Network Address Translation |
| **NIC** | Network Interface Card |
| **OFDM** | Orthogonal Frequency Division Multiplexing |
| **OLC** | Open Logical Channel |
| **OSI** | Open Systems Interconnection |
| **PBX** | Private Branch Exchange |
| **PCF** | Point Coordination Function |
| **PCI** | Peripheral Component Interconnect |
| **PCM** | Pulse-code Modulation |
| **PDA** | Personal Digital Assistant |
| **PHP** | Hypertext Preprocessor |
| **PHY** | Physical Layer of the OSI Model |
| **PNN** | Plano Nacional de Numeração |
| **PNN** | Plano Nacional de Numeração |
| **POTS** | Plain Old Telephone Service |
| **PPP** | Point-to-Point Protocol |
| **PRI** | Primary Rate Interface |
| **PSTN** | Public Switched Telefone Network |
| **PT** | Portugal Telecom |
| **PVP** | Packet Video Protocol |
| **QoS** | Qualidade de Serviço |

| | |
|---|---|
| **QSIG** | Q Signaling |
| **RA** | Receiver Address |
| **RADIUS** | Remote Authentication Dial In User Service |
| **RAS** | Registration, Admission and Status |
| **RC** | Release Candidate |
| **RDIS** | Rede Digital de Serviços Integrados |
| **RFC** | Request For Comment |
| **RSVP** | Resource ReSerVation Protocol |
| **RTCP** | Real-Time Transport Protocol |
| **RTP** | Real Time Protocol |
| **RTPC** | RTP Control Protocol |
| **RTS/ CTS** | Request to Send / Clear to Send |
| **RTSP** | Real Time Streaming Protocol |
| **SA** | Source Address |
| **SAP** | Session Announcement Protocol |
| **SCCP** | Skinny Call Control Protocol |
| **SCTP** | Stream Control Transmission Protocol |
| **SDP** | Session Description Protocol |
| **SER** | SIP Express Router |
| **SIP** | Session Initiation Protocol |
| **SMS** | Short Message Service |
| **SMTP** | Simple Mail Transfer Protocol |
| **SOHO** | Small Office Home Office |
| **SSL** | Secure Sockets Layer |
| **STA** | Station |
| **STUN** | Simple Traversal of UDP through NAT. |
| **TA** | Transmitter Address |
| **TCP** | Transmission Control Protocol. |
| **TCS** | Terminal Capability Set |
| **TG** | Task Group |
| **TIC** | Tecnologias de Informação e Comunicação |
| **TKIP** | Temporal Key Integrity Protocol |
| **TLS** | Transport Layer Security |
| **UA** | Universidade de Aveiro. |
| **UAC** | User Agent Client |
| **UAS** | User Agent Server |
| **UDP** | User Datagram Protocol. |
| **URI** | Universal Resource Identifier |
| **USC/ISI** | University of Southern California/Information Sciences Institute |
| **VOIP** | Voice Over Internet Protocol. |
| **VPN** | Virtual Private Network |
| **WAN** | Wide Area Network. |
| **WAP** | Wi-Fi Protected Access |
| **WAP2** | Wi-Fi Protected Access 2 |
| **WEP** | Wired Equivalent Privacy |
| **Wi-Fi** | Wireless Fidelity. |
| **WiMax** | Worldwide Interoperability for Microwave Access. |
| **WMN** | Wireless Mesh Network |
| **XMPP** | Extensible Messaging and Presence Protocol |

# 1

# 1. Introdução

## *1.1. Enquadramento*

O mundo das telecomunicações tem sofrido um desenvolvimento constante nas últimas décadas devido à evolução tecnológica, não só por causa da rápida proliferação da banda larga, como também ao crescimento do uso da tecnologia de redes sem fios e do surgimento de várias soluções no mercado de VoIP.

Actualmente, as redes de telecomunicações têm vindo a assumir um papel preponderante na nossa sociedade, visto que, durante as últimas décadas a necessidade de comunicação com base nestas tecnologias tem se tornado essencial quer ao nível empresarial, institucional ou pessoal.

Importa salientar que devido ao crescente fluxo de informação resultante da massificação da utilização de ferramentas como o e-mail, troca de mensagens escritas via SMS, *instant messaging* (*Windows Live Messenger, ICQ, AIM, Skype*), redes sociais (*Facebook, Orkut, MySpace*), *microblogging* (*Twitter, Identi.ca, Tumblr*), *blogging* (*Blogger, WordPress, TypePad*), ferramentas colaborativas (*Zoho, Microsoft SharePoint, Yugma*) e o *download* sistemático de conteúdos multimédia, têm vindo a criar uma forte dependência produtiva pela Internet.

Relativamente ao nível pessoal, nos últimos anos a utilização dos computadores pessoais para estabelecimento de comunicações tem vindo a aumentar de uma forma gradual e muito significativo, visto que, o consumidor está cada vez mais exigente, procurando sempre adquirir uma maior largura de banda, uma conectividade e sincronização total entre vários equipamentos (tais como: o PC, na consola de jogos, no *smartphone, netbook, iPad, iPhone*, etc.) mostrando-se ávido de novos serviços, nas áreas do entretenimento, utilidades, ensino e trabalho.

No que diz respeito ao nível empresarial, devido à necessidade de satisfazer não só todas as necessidades e exigências dos potenciais clientes, como também, aumentar a competitividade e produtividade dos colaboradores, as empresas estão a dispersar as infra-estruturas de uma forma global. Contudo, as empresas estão

sujeitas a estabelecer comunicações com recurso às novas tecnologias de informação, como por exemplo, o sistema de vídeo-conferência, de modo a minimizar os custos de deslocação dos funcionários para as eventuais reuniões presenciais.

Face a este cenário, a indústria das telecomunicações tem vindo a demonstrar uma forte capacidade de inovação de modo a dar resposta às necessidades das populações, sobretudo às regiões desfavorecidas ou onde haja falhas de mercado de telecomunicações. Com provas dadas podemos citar algumas tais como, a massificação da Internet, a constante evolução das redes WLAN e o crescimento das redes celulares. De notar que, hoje em dia já se pode encontrar em vários locais públicos ou privados, muitas infra-estruturas de redes contendo a tecnologia *Wi-Fi*. Contudo, actualmente existe uma forte tendência e necessidade destas redes aumentarem em tamanho e complexidade, de modo a oferecer uma melhor qualidade de serviço aos potenciais utilizadores quer ao nível pessoal, quer ao nível empresarial.

Devido à evolução das novas Tecnologias de Informação e Comunicação (TIC), e da utilização massificada da internet e das tecnologias de banda larga, decorrem actualmente, quer ao nível nacional quer ao nível internacional, diversas iniciativas destinadas a promover a adopção dessas inovações e introduzi-las na Sociedade de Informação e do Conhecimento. Entretanto, devido a esta necessidade de expandir essa complexidade e aos vários trabalhos de investigação científica a nível mundial nesta área, está a emergir uma nova tecnologia, denominada por *Wi-Fi Mesh* ou Redes *Mesh* Sem Fios (*Wireless Mesh Network, WMN*), que irá permitir ao utilizador final um acesso sem fios contínuo às aplicações de banda larga, virtualmente em qualquer momento e em qualquer lugar, garantindo assim uma melhor qualidade de serviço aos mesmos.

Em Portugal, essas iniciativas são consideradas como sendo uma prioridade nacional, e como exemplo, passo a citar o projecto “Cidades e Regiões Digitais”, que está inserido na iniciativa “Redes Comunitárias de Banda Larga”. Importa salientar que, o referido projecto visa dar um contributo para a concretização do Plano de Acção para a Sociedade de Informação [97] e tem como objectivos principais:

1. Massificação do acesso e utilização da Internet em banda larga em todo o país e para todos os portugueses e cidadãos residentes em Portugal;

2. Promoção de uma cultura digital, da habilitação e do conhecimento dos Portugueses para a sociedade da informação;

3. Garantia de serviços públicos de qualidade, apoio à modernização da Administração Pública, racionalização dos custos e promoção da transparência;

4. Melhoria da qualidade da democracia através do aumento da qualidade da participação cívica dos cidadãos;

5. Orientação do sistema de saúde para o cidadão, melhorando a eficiência do sistema;

6. Aumento da produtividade e competitividade das empresas através dos negócios electrónicos;

7. Promoção dos conteúdos, aplicações e serviços com valor para a sociedade, incluindo o património cultural.

É evidente que esta dissertação surge no âmbito dessas iniciativas e pretende-se com este trabalho dar mais um contributo significativo para o Plano de Acção para a Sociedade de Informação, de modo a atingir os objectivos previamente estabelecidos no respectivo plano.

## *1.2. Metodologia*

A metodologia utilizada neste trabalho partiu de um estudo minucioso, baseando-se em pesquisa bibliográfica e da análise dos conceitos e aspectos relacionados com VoIP para Redes Comunitárias. Foram também estudadas experiências de utilização de soluções *wireless* em diversas zonas do globo procurando daí extrair ensinamentos para este trabalho. Por fim as soluções propostas foram testadas e validadas em laboratório.

## *1.3. Objectivos*

Este trabalho tem como objectivo principal realizar um levantamento de soluções VoIP *Open Source* com base em tecnologias *wireless* de banda larga emergentes (tais como, as redes *Mesh*), que estão presentemente disponíveis e podem ser utilizadas no combate à infoexclusão e na promoção da igualdade de oportunidades e de acesso à banda larga nas zonas rurais e periféricas.
Em suma, pode-se afirmar que os objectivos principais deste trabalho são:

- Compreender a especificidade do contexto sócio-territorial das redes comunitárias, nomeadamente das que utilizam tecnologias *wireless*. Identificar

soluções VoIP adequadas ao contexto das redes comunitárias *wireless*, nomeadamente das soluções *Open Source* disponíveis no mercado.

- Estudar e seleccionar o(s) protocolos da tecnologia VoIP a utilizar nos vários clientes e servidores do sistema;
- Estudar a interligação com a rede telefónica – PSTN;
- Estudar, analisar e propor possíveis cenários de implementação de uma arquitectura VoIP numa *"Mesh network"* para as redes comunitárias de banda larga.
- Avaliar o impacto técnico e financeiro da migração para VoIP, indicando os custos e método de implementação;
- Disponibilizar documentação que possa servir de apoio no projecto e implementação de soluções VoIP/*Wireless* em redes comunitárias.

### *1.4. Estrutura da dissertação*

Nesta alínea, será apresentado a organização estrutural deste trabalho. O presente projecto está dividido nos seguintes capítulos:

1. **Introdução:** neste capítulo, em primeiro lugar, é feita uma breve introdução relativamente à tecnologia VoIP para as redes comunitárias, indicando alguns conceitos importantes sobre o tema em causa. Seguidamente, são apresentados os objectivos pretendidos referente a este trabalho bem como um enquadramento do mesmo. Por último, é feita uma breve descrição da organização deste relatório.

2. **Soluções VoIP para Redes Comunitárias:** neste capítulo, primeiramente será feita uma breve descrição sobre a evolução histórica da tecnologia VoIP. A seguir, serão abordados alguns conceitos básicos sobre a referida tecnologia, tais como, a sua definição e o seu funcionamento básico, as suas vantagens e desvantagens no uso dessa tecnologia. De seguida, serão descritos ainda alguns exemplos de cenários de implementação possíveis e os aspectos de segurança relacionados com essa tecnologia. Seguidamente, será apresentado um estudo detalhado sobre os principais protocolos da tecnologia VoIP. Por último, serão apresentados alguns exemplos de equipamentos da tecnologia VoIP presentes no mercado empresarial.

3. **Soluções Wireless para Redes Comunitárias:** neste capítulo, são introduzidos alguns conceitos relacionados com *Mesh netwok*. Seguidamente

será apresentada uma descrição detalhada sobre as tecnologias das redes *Wi-Fi* e *Mesh*, abordando conceitos básicos dessas duas tecnologias tais como, a sua definição, o funcionamento básico e a arquitectura, descrevendo todo os seus principais componentes. Seguidamente, será apresentado um estudo detalhado sobre os principais protocolos usados nessas tecnologias e alguns aspectos de segurança. De seguida, serão descritas as suas vantagens e desvantagens no uso dessas referidas tecnologias. Serão ainda, apresentados alguns exemplos de projectos existentes no mercado e que usam a tecnologia *Mesh*. Por último, será apresentado um estudo detalhado sobre alguns de equipamentos não só, ao nível de *hardware*, como também, de *software* gratuito (*Open Source*) e/ou proprietários presentes no mercado empresarial que poderão ser utilizados nessa tecnologia.

4. **Concepção de uma solução VoIP para Redes Comunitárias:** Neste capítulo, serão apresentadas algumas informações que são consideradas relevantes para a concepção de um sistema VoIP capaz de satisfazer todas as necessidades dos utilizadores em diferentes cenários de utilização.

5. **Implementação do protótipo VoIP para Redes Comunitárias:** este capítulo faz uma referência ao protótipo VoIP desenvolvido para as Redes Comunitárias, apresentando os aspectos mais importantes da implementação da respectiva arquitectura. Este protótipo irá permitir efectuar todos os testes necessários de forma a avaliar as capacidades dos serviços disponibilizados aos utilizadores pelo fornecedor VoIP da rede comunitária *Mesh*. Será ainda, apresentada alguma informação sobre os procedimentos de instalação dos componentes presentes na respectiva arquitectura do protótipo VoIP.

6. **Casos de Estudo sobre as Redes Mesh:** neste capítulo, é apresentado um estudo sobre alguns casos de sucesso que poderão servir de exemplos práticos na implementação de uma rede *Mesh* baseada em soluções *Open Source*, aonde poderá ser implementada uma solução VoIP para uma rede comunitária.

7. **Impacto e custos da migração para um sistema VOIP:** neste capítulo, será apresentado um estudo sobre o impacto e os custos da migração de um

sistema VoIP em Redes Comunitárias, indicando as suas vantagens e desvantagens.

8. **Conclusões e Trabalho Futuro:** aqui serão apresentadas as conclusões referente a este trabalho e são apresentadas algumas sugestões para que futuramente sejam efectuados alguns melhoramentos relativamente a implementação de uma solução Wireless/VoIP para Redes Comunitárias.

9. **Bibliografia e Sites Consultados:** neste capítulo, é feita uma referência às bibliografias e aos sites utilizados para a realização deste trabalho.

10. **Anexos:** este capítulo apresenta alguns documentos que tiveram suma importância na realização deste trabalho. Também apresenta um conjunto de manuais de instalação dos principais componentes que correspondem ao diagrama de blocos do protótipo VoIP implementado. Dentre os anexos está mencionado um manual de configuração e instalação dos *firmware Freifunk* e *DD-WRT* nos equipamentos da *Linkys,* de modo a facilitar ao gestor e/ou administrador do sistema a configurar um nó *Mesh*.

# 2

# 2. Soluções VoIP para Redes Comunitárias

Neste capítulo, será apresentada uma breve evolução histórica sobre a tecnologia VoIP. A seguir, serão abordados alguns conceitos básicos sobre a referida tecnologia, tais como, a sua definição e o seu funcionamento básico, as suas vantagens e desvantagens no uso dessa tecnologia. De seguida, serão apresentados alguns exemplos de cenários de implementação possíveis e os aspectos de segurança relacionados com essa tecnologia. Seguidamente, será apresentado um estudo detalhado sobre os principais protocolos usados na tecnologia VoIP. Por último, serão apresentados alguns exemplos de equipamentos dessa tecnologia e algumas soluções *Open Source* presentes no mercado empresarial.

## *2.1. Evolução Histórica do VoIP*

Na década de 70, *Danny Cohen*, iniciava as primeiras tentativas de transportar áudio em redes de pacotes, elaborando uma série de experiências de transmissão de voz em pacotes e em tempo real entre o USC/ISI *(University of Southern California/Information Sciences Institute)* e o *MIT's Lincoln Lab*. Em 1977, *Cohen* apresenta formalmente primeiro protocolo de Internet para transportar voz em pacotes.

Em meados da década de 80, R. Cole propõe o protocolo *Packet Video Protocol (PVP)* para o transporte de vídeo em pacotes.

Na década de 90, mais concretamente em 1992, foi realizada a primeira *audiocast* através da *Multicast Backboneon the Internet (MBone)*, pela *Internet Engineering Task Force (IETF)* a partir de *San Diego*. Em seguida no mesmo ano, *Henning Schulzrinne* começava a desenvolver o *Real-Time Transport Protocol (RTP)*, de modo a normalizar uma camada de transporte para meios em tempo real. Após a primeira realização da difusão de áudio em 1992, foi realizada através da *Mbone* a primeira difusão de áudio e vídeo em simultâneo pela IETF, a partir da cidade de Boston, utilizando as aplicações *Vat* e DVC respectivamente.

Em 1995, o protocolo RTP foi publicado como *IETF Proposed Standard*. Neste mesmo ano, surgiu uma nova aplicação que utiliza o codificador normalizado H.261, nomeadamente a Vic, que foi desenvolvido por *Steve McCanne* e *Van Jacobson*. Mais tarde foi desenvolvida uma outra aplicação, o *CU-SeeMe*, que foi um dos primeiros protótipos de videoconferência disponíveis na Internet. Inicialmente, o *CU-SeeMe* foi implementado para ser integrado em *MacOs* e depois para Windows. Esta aplicação utilizava um processo responsável pela distribuição de sinais pelos vários intervenientes da conferência.

No ano de 1996, foi publicada pela *International Telecommunications Union (ITU)*, a primeira versão da recomendação H.323 [H.323, 1996]. O protocolo H.323 foi inicialmente projectado para as redes LANs, e é uma recomendação para a comunicação multimédia. No mesmo ano foi prestado o primeiro serviço comercial de Telefonia sobre IP ao *Delta Three*, seguindo-se a *Net2phone, iBasis* e *Telematrix*. Seguidamente, a Microsoft lança o seu primeiro sistema de conferência sobre redes de pacotes, nomeadamente o *Microsoft NetMeeting v1.0*. Em 1999, o protocolo *Session Internet Protocol* (SIP) foi aceite como norma, pelo IETF como sendo um protocolo de sinalização para a criação, modificação e finalização de sessões com um ou mais participantes.

Nas últimas décadas, com a evolução das novas tecnologias de informação, o crescimento da Internet e da banda larga, fizeram com que as primeiras conferências empresariais marcassem a transição da utilização de redes de pacotes para o tráfego de voz como experiências de laboratório, para o mundo dos serviços empresariais em determinadas áreas do negócio, e que consequentemente contribuíram para o aparecimento de soluções inovadoras dessa nova tecnologia VoIP. A telefonia sobre IP é também designada como Voz sobre IP (*VoIP – Voice over IP*) ou ainda Telefonia sobre Internet (*Internet Telephony*).

## 2.2. *Conceitos básicos sobre VoIP*

### *2.2.1. Definição: O que é VoIP?*

A voz sobre Internet (*Voice over Internet Protocol - VoIP*) é uma tecnologia que permite ao utilizador estabelecer chamadas telefónicas através de uma rede de dados, convertendo um sinal de voz analógico num conjunto de sinais digitais, posteriormente enviados através de uma ligação à Internet sob a forma de pacotes com endereçamento IP. Não sendo nova, esta tecnologia atinge agora um estado de maturidade e qualidade, que permite a sua aplicação em ambientes de produção através da interligação com os sistemas telefónicos convencionais. De igual forma, a

oferta de equipamentos e serviços de operadoras, tem vindo a crescer exponencialmente.

As empresas que fornecem o serviço de VoIP são geralmente chamadas provedoras, e os protocolos usados para transportar os sinais de voz em uma rede IP são geralmente chamados protocolos VoIP. Existe uma redução de custo devido ao uso de uma única rede para carregar dados e voz, especialmente no qual os utilizadores já possuem uma rede com capacidade subutilizada, que pode transportar dados VoIP sem custo adicional. As chamadas de VoIP para VoIP no geral são gratuitas, enquanto chamadas VoIP para redes públicas (PSTN) podem ter um custo adicional para o utilizador VoIP. Considera-se, a telefonia IP, à agregação do VoIP com outros serviços agregados para a telefonia.

### *2.2.2. Funcionamento básico de um sistema VoIP*

A tecnologia VoIP promete inovar na área das telecomunicações, com a transmissão de dados multimédia, tais como, a voz e o áudio através da rede IP. O modo de funcionamento de um telefone IP é igual ao de um telefone convencional, sendo que a única diferença está na maneira como a voz é transmitida.

O procedimento é simples: baseia-se em digitalizar a voz em pacotes de dados para serem enviados pela rede internet (preferencialmente em banda larga) e serem convertidos, no destino, novamente em voz conforme ilustra a seguinte figura:

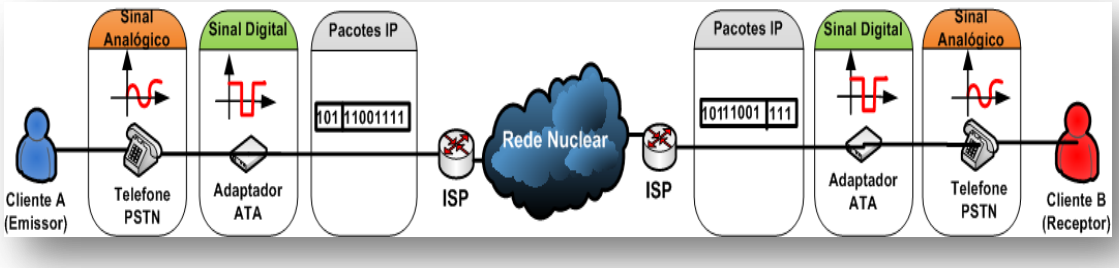



**Figura 1 – Exemplo de um processo de conversão dos dados num sistema VoIP.**

Para isso, será necessário de ter um computador pessoal (PC) ou um portátil equipado com microfone e auscultadores, um telefone IP ou um telefone tradicional ligado a um adaptador IP (*Analogue Telephone Adapter* - ATA), conforme esta ilustrada na seguinte figura:

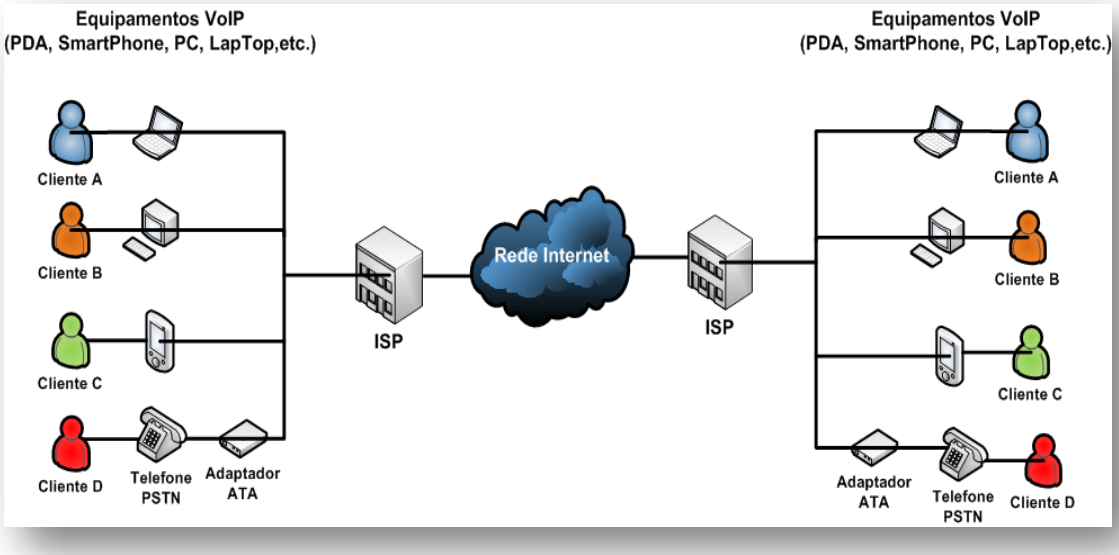



**Figura 2 – Exemplo de funcionamento básico de um sistema VoIP.**

### *2.2.3. Vantagens e Desvantagens da tecnologia VoIP*

Nesta secção serão descritas as vantagens e desvantagens no uso da tecnologia VoIP em relação ao telefone convencional (PSTN).

#### *2.2.3.1. Vantagens*

As vantagens apresentadas pelo serviço VoIP em relação á linha telefónica PSTN devem ser analisadas não só em função da redução do custo de equipamentos de comunicações, mas também, pela facilidade e mobilidade da nova forma de comunicação que o utilizador dispõe.

A seguir, passo a mencionar as potenciais vantagens:

- Redução de custos nas comunicações: esta é uma das suas maiores vantagens, visto que, uma vez implantado o sistema VoIP numa determinada empresa, será constatada de imediato uma redução de aproximadamente 70% com serviços de telefonia. Para implementar uma solução VoIP numa empresa será necessário elaborar um projecto detalhado, identificando quais são as necessidades reais da empresa, isto é, será preciso ter em conta os seguintes aspectos: qual a solução a utilizar, verificar se a empresa possui IP fixo ou IP dinâmico, qual o tamanho da banda ADSL e o qual o seu tráfego pela rede de dados.

| Países | Operadores Fixos | | Operadores VoIP | |
|---|---|---|---|---|
| | PT | NOVIS | VOIPJET | NETCALL |
| **Plano 100** | ¤ 0,045 | --- | ¤ 0,0164 | ¤ 0.017 |
| **RIDS PT UNO** | ¤ 0,067 | --- | ¤ 0,0164 | ¤ 0.017 |
| **Plano Nacional** | ¤ 0,079 | --- | ¤ 0,0164 | ¤ 0.017 |
| **Mais económico (*)** | ¤ 0,018/0,047 | ¤ 0,036/¤0,058 | ¤ 0,0164 | ¤ 0.017 |
| **Espanha** | ¤ 0,06 | ¤ 0,081 | ¤ 0,012 | ¤ 0.017 |
| **França, Alemanha e UK** | ¤ 0,10 | ¤ 0,108 | ¤ 0,011 | ¤ 0.017 |
| **UE Zona 1, Suíça e Noruega** | ¤ 0,11 | ¤ 0,108 | ¤ 0,014 | ¤ 0.017 |
| **UE Zona 2** | ¤ 0,30 | ¤ 0,108 | ¤ 0,015 | --- |
| **Rest Europa** | ¤ 0,32 | ¤ 0,342 | ¤ 0,015 | --- |
| **Brasil** | ¤ 0,20 | ¤ 0,243 | ¤ 0,022 | ¤ 0,044 |
| **USA, Canada** | ¤ 0,11 | ¤ 0,243 | ¤ 0,011 | ¤ 0,017 |
| **México** | ¤ 0,60 | ¤ 0,585 | ¤ 0,025 | ¤ 0,080 |
| **Angola** | ¤ 0,31 | ¤ 0,243 | ¤ 0,119 | ¤ 0,142 |
| **Moçambique** | ¤ 0,35 | ¤ 0,243 | ¤ 0,133 | ¤ 0,099 |
| **Macau** | ¤ 0,40 | ¤ 0,450 | ¤ 0,039 | ¤ 0,042 |
| **Japão** | ¤ 0,40 | ¤ 0,450 | ¤ 0,029 | ¤ 0,025 |
| **China** | ¤ 0,75 | ¤ 0,450 | ¤ 0,014 | ¤ 0,017 |
| **Austrália** | --- | ¤ 0,450 | ¤ 0,010 | ¤ 0,017 |
| **NOTA:** (*) A estes produtos/taxas acresce uma mensalidade fixa. Valor por minuto em chamadas locais e nacionais respectivamente. | | | | |

**Tabela 1 – Exemplo de tarifários de chamadas VoIP em Portugal.**

- Protecção do investimento: Os PBX IP são baseados em *Software*, denominados por *softphones*, permitindo assim a actualização sistemática com novos protocolos e funcionalidades ao longo do tempo;

- Sistema integrado de comunicação numa infra-estrutura simplificada: todos os telefones IP são interligados na rede Informática tradicional dos computadores não sendo assim necessário qualquer tipo de instalação de cablagem, dispensando assim a complexidade de cabos para cada uma das extensões até hoje utilizada nas centrais convencionais (PBX). Todos os equipamentos de comunicações, tais como o telefone, o fax e internet, estão centralizados numa única infra-estrutura. A voz corre na infra-estrutura de dados, na rede IP.

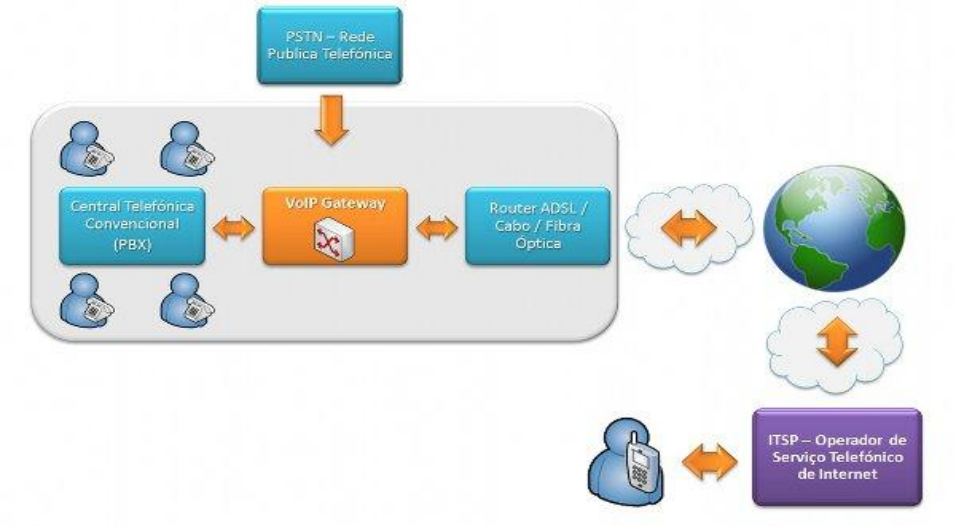



**Figura 3 – Exemplo de integração da tecnologia VoIP com a rede PSTN [121].**

- Funcionalidades acrescidas: A VoIP irá permitir ao utilizador tornar possíveis as funcionalidades que seriam difíceis ou quase impossíveis nas redes tradicionais de telefone, tais como: extensões remotas e/ou móveis, atendimentos interactivos, *voicemail, follow-me*, serviços partilhados, integração com o *Outlook* e outras mais que através de uma analise exaustiva poderão ser optimizados à medida das necessidades do cliente;

- Escalabilidade e complexidade: a tecnologia VoIP irá possibilitar às empresas que contenham um conjunto de filiais geograficamente afastadas umas das outras, a utilização de extensões da central IP PBX sem terem necessidade de adquirir uma nova central. Será necessário apenas os telefones IP que duma forma automática se interligam à una sede da empresa e estabeleçam uma comunicação como se de uma extensão local se tratasse. Este tipo de arquitectura permite implementar um número indeterminado de extensões, sendo escalável em crescimento ao longo do tempo para investimentos graduais.

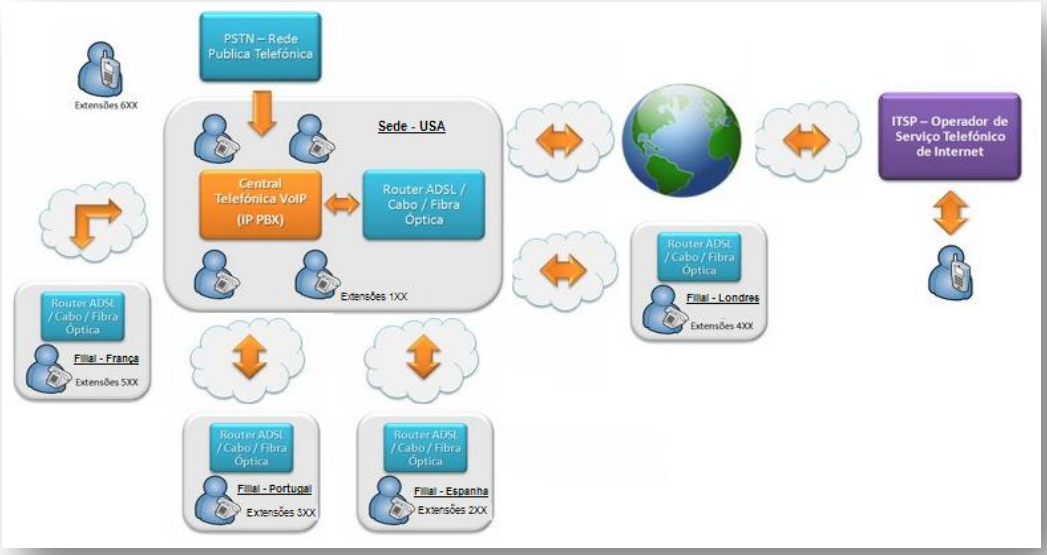



**Figura 4 – Exemplo de arquitectura expansível e flexível de uma central IP PBX [121].**

#### *2.2.3.2.Desvantagens*

As desvantagens apresentadas pelo serviço VoIP em relação á linha telefónica PSTN devem ser analisadas em função dos equipamentos de comunicações que o utilizador dispõe. Assim sendo, passo a mencionar as potenciais desvantagens:

- Se a estrutura de rede e os equipamentos forem antigos, a mudança pode ficar cara, por causa da necessidade de adquirir equipamentos novos como a cablagem, *Hubs*, *Switches*, *Router*, Telefones IP e a mão-de-obra especializada;
- Apesar de o encaminhamento das chamadas para os serviços de emergência dever ser assegurado pelos prestadores de serviços VoIP, existem dificuldades técnicas na determinação da localização precisa do terminal VoIP em uso nómada;
- O serviço VoIP não funciona quando falha a energia eléctrica e o prestador do serviço não fornece energia de socorro (a este respeito, convém certificar-se consultando a informação disponibilizada pelo prestador). No entanto, esta desvantagem pode ser ultrapassada se dispuser de uma fonte ininterrupta de alimentação convenientemente dimensionada;
- Certos prestadores VoIP não oferecem serviço de listas telefónicas e serviço informativo.

- Necessidade de ambos os utilizadores terem um acesso à internet de banda larga, sempre disponível e de estarem simultaneamente conectados à mesma hora;
- Baixa qualidade do som, que poderá ser causado por perdas de pacotes a serem transmitidos na rede.

### *2.2.4. Arquitectura básica de um sistema VoIP*

Na figura seguir está ilustrada um exemplo de uma arquitectura básica da tecnologia VoIP, apresentando algumas componentes principais da mesma.

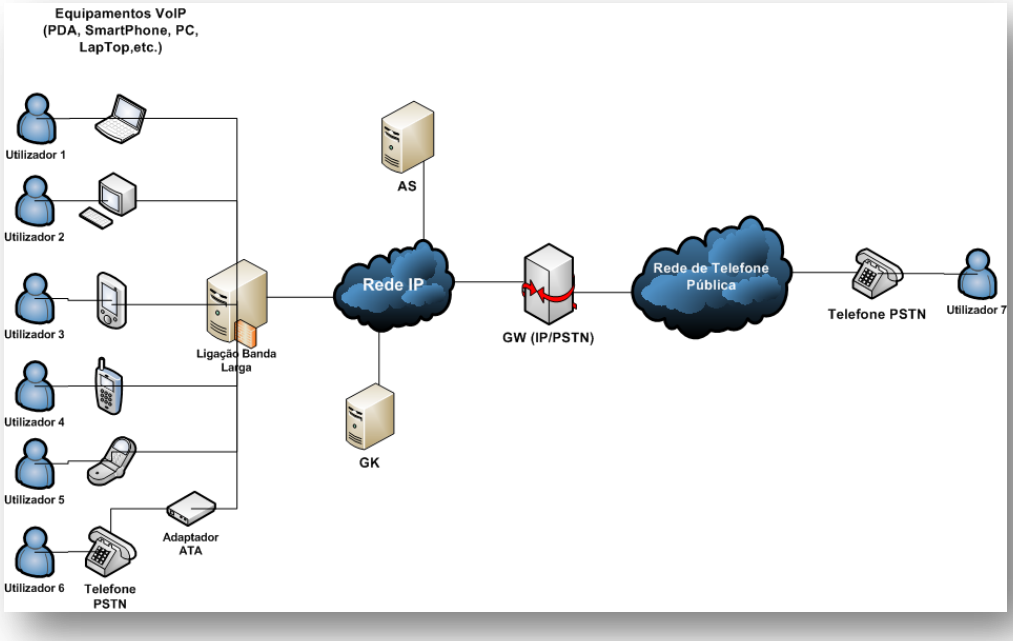



**Figura 5 – Exemplo de uma arquitectura básica da tecnologia VoIP.**

**Principais componentes da tecnologia VoIP:**

- *IP Phone*: corresponde ao sistema completo de terminais de telefonia VoIP, que são: telefone IP, VoIP adaptador telefone analógico (ATA) e PC's com *softphone*.
- *Gateway* (GW): é o responsável pela interoperabilidade entre a rede VoIP e rede telefónica pública. O *Gateway* faz uma conversão média e em tempo real da voz analógica e a digital comprimida simultaneamente. O GW efectua ainda a conversão de sinalização para as chamadas telefónicas para dentro e fora da rede VoIP.
- *Gatekeeper* (GK): tem como função a gestão de telefones IP. Tem ainda, como funções não só a execução da tradução de direccionamento dos vários

terminais, como também, controlar o acesso e as chamadas dos terminais da rede, e ainda a largura de banda utilizada.

- *Application Server* (AS): fornece os serviços adicionais à rede VoIP. Entre esses serviços pode destacar: caixa postal unidade interactiva resposta audível (IVR) serviços, lista telefónica, entre outros.

### *2.2.5. Cenários de Implementação*

Neste ponto, serão apresentados os possíveis cenários de implementação da tecnologia VoIP, numa internet pública, rede privada, no *Backbone IP* e por último num serviço de comunicações electrónicas acessível ao público.

#### *2.2.5.1.VoIP na internet pública*

Actualmente, a rede de Internet pública, no que diz respeito ao transporte de voz em pacotes IP, utilizando a tecnologia VoIP, é a mais popular. Este serviço VoIP, normalmente, não apresenta quaisquer custos adicionais aos utilizadores e geralmente em ligações são sempre estabelecidas entre dois utilizadores que contêm equipamentos VoIP.

Na figura a seguir está ilustrada um exemplo de ligação típica de VoIP na Internet pública:

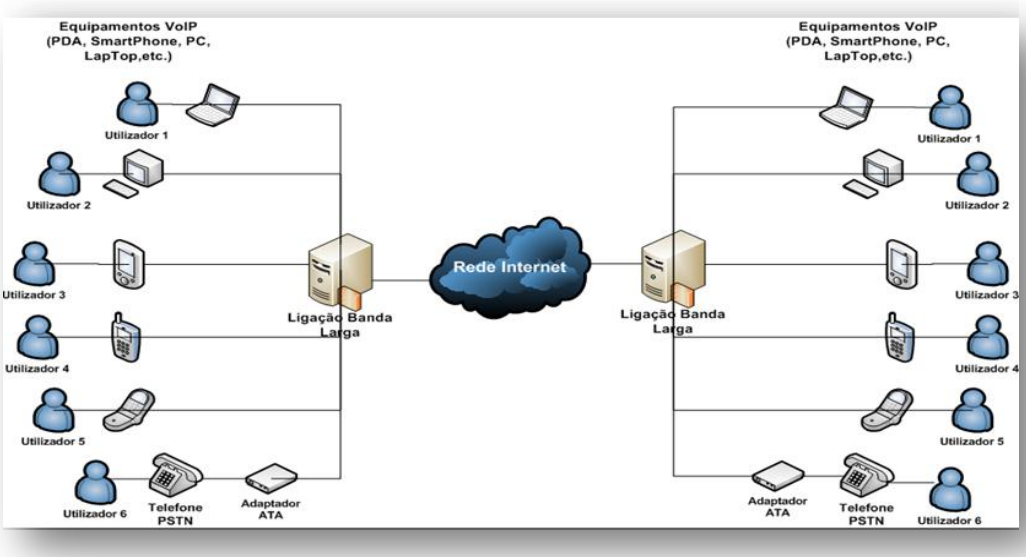



**Figura 6 – Exemplo de uma ligação típica de VoIP na Internet pública.**

Dado ao facto do que, esta tecnologia utiliza a rede de internet pública para a transmissão de dados em pacotes com endereços IP e de que actualmente, é pouco viável distinguir os serviços VoIP dos restantes serviços, não será possível garantir ou assegurar uma melhor qualidade de transmissão de dados. Contudo, essa qualidade

de transmissão poderá ser melhorada com a utilização de uma maior larga de banda da rede de modo a garantir que haja um menor congestionamento de tráfego existente numa determinada rede. Importa salientar que, o serviço VoIP na rede pública oferece aos utilizadores uma qualidade de "*best effort*".

De entre os exemplos comerciais deste tipo de serviços os que mais se destacam no mercado empresarial são: o *Skype* (que usa um protocolo proprietário), *Microsoft Messenger*, *GTalk*, *Sapo Messenger*, *VoipBuster*, etc.

#### *2.2.5.2.VoIP em redes privativas*

O serviço de VoIP em redes privadas é utilizado em ambiente privado, normalmente empresarial e não uma oferta comercial de serviços - e.g. redes corporativas com tecnologias IP e integração de voz e dados. Este serviço permitirá às empresas ou instituições substituir todo o sistema de PBX analógico para um sistema de PBX IP, permitindo-lhes assim uma revolução e inovação na nova forma de comunicarem entre si, com custos substancialmente reduzidos, causando um enorme impacto nas pessoas e nas organizações. Na seguinte figura está ilustrada um esquema que descreve um exemplo de configuração típica de utilização de VoIP em redes privadas:

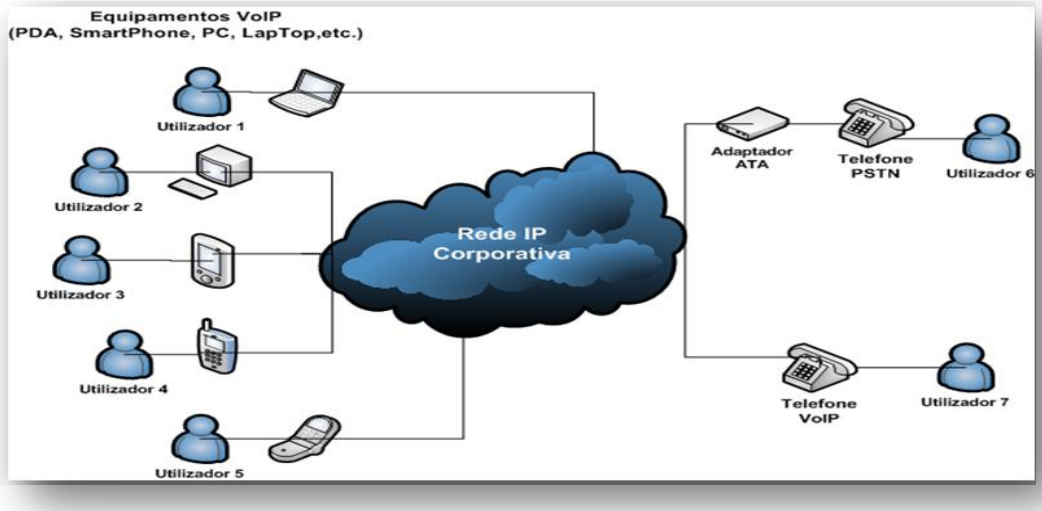



**Figura 7 – Exemplo de uma ligação típica de utilização de VoIP em redes privativas.**

Este serviço de VoIP tem como vantagens principais:

- Uma maior flexibilidade nas ligações, isto é, poderá ser efectuada uma interligação dos sistemas de PSTN com outros sistemas de telefones móveis;

- Possibilidade de integração de novos serviços aos utilizadores, nomeadamente o serviço de *Voicemail*, *Waiting Ring*, menus de resposta áudio (IVR), etc;

- Possibilidade de efectuar um encaminhamento eficiente das chamadas, serviços criados à medida da empresa, como por exemplo, a implementação de um serviço de despertar num hotel de modo a satisfazer todas as necessidades dos seus clientes.

#### *2.2.5.3. VoIP no backbone IP*

O serviço de VoIP no *backbone IP* é utilizado para suportar às comunicações de voz de um operador internacional ou de um operador de rede pública de comunicações que apenas utilizam tecnologias VoIP internamente à sua própria rede (*backbone IP*). Como exemplo deste serviço pode-se mencionar o caso dos prestadores do serviço telefónico "tradicional" através de redes de cabo, nomeadamente com ofertas "*triple play*" - serviço de voz, de acesso à Internet e de televisão -.

Na figura a seguir é apresentado um exemplo de configuração de rede típica de utilização de VoIP no *backbone IP*:

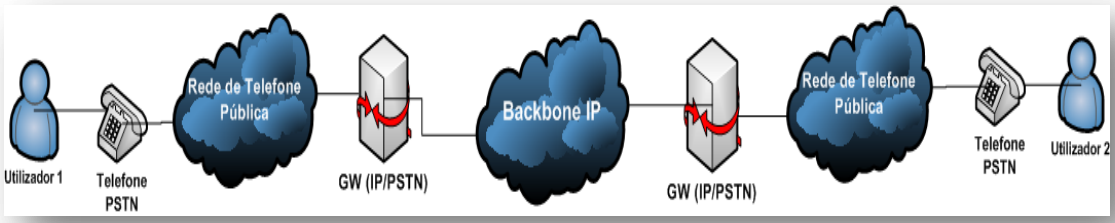



**Figura 8 – Exemplo de uma ligação típica de utilização de VoIP no backbone IP.**

#### *2.2.5.4. VoIP como serviço de comunicações electrónicas acessível ao público*

Estes serviços VoIP caracterizam-se por permitirem receber e fazer chamadas de, e para, números do plano nacional de numeração (PNN). Contudo para efectuar ou receber uma chamada será necessário utilizar um *gateway* de modo estabelecer uma ligação entre a rede IP e a RTPC, como se pode observar a seguinte figura:

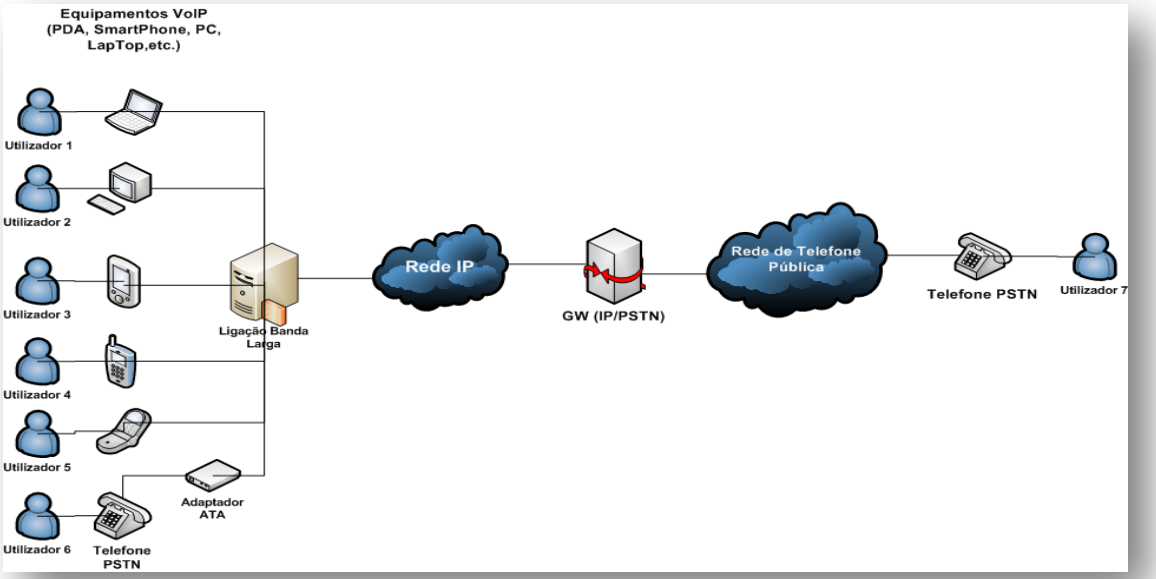



**Figura 9 – Exemplo de tecnologia VoIP como serviço acessível ao público.**

Importa salientar que, os serviços VoIP acessíveis ao público são regulados no âmbito da Lei n.º 5/2004. Segundo o referido decreto-lei existem duas formas aplicadas a este tipo de serviço que passo a citar:

1. Serviço oferecido por um prestador de acesso, designadamente de banda larga, num único local fixo e em condições percepcionadas pelo utilizador como equivalentes às do serviço telefónico fixo tradicional.
2. Serviço de uso tipicamente nómada, isto é, susceptível de utilização em vários locais que se suporte no acesso de terceiros, i.e. não controlando a rede de acesso. Como exemplo prático deste serviço temos o *Skype-OUT/IN, VoipBuster, etc.*

## 2.3. *Aspectos de Segurança*

Actualmente com a evolução das tecnologias de informação e comunicação é fundamental que as empresas adoptem políticas de segurança adequadas para proteger as suas redes convergentes, tanto para a comunicação de dados, como para a voz devido os possíveis ataques que possam prejudicar a transmissão de dados via internet.

No que se refere ao uso dessa tecnologia nas redes *wireless*, actualmente os utilizadores poderão estar mais tranquilo em relação aos aspectos de segurança, do que quando a comunicação é efectuada através de redes fixas, graças ao

desenvolvimento de novos protocolos de segurança como por exemplo a encriptação WPA, que garante a segurança para os standards 802.11b, 802.11a e 802.11g.

Importa salientar que, é fundamental que os utilizadores dessa tecnologia têm sempre consideração a configuração das funcionalidades de segurança quando adquirem qualquer dispositivo *wireless*.

Hoje em dia, com a evolução tecnológica a maioria dos produtos de segurança VoIP incluem uma série de funcionalidades tais como: a *firewall*, sistemas de prevenção de intrusão, controladores de limites de sessão e outros equipamentos desenhados para proteger a rede de comunicações de voz que transportam tráfego IP das organizações empresariais.

Estes equipamentos têm como objectivo principal disponibilizar segurança nas ligações estabelecidas entre dois utilizadores, quando os protocolos VoIP não têm condições.

À semelhança do ambiente de dados, um conjunto de equipamentos de segurança, preocupações e boas práticas são essenciais para implementar com segurança tecnologias VoIP.

Estes produtos possibilitam ao utilizador defender a sua rede de voz contra eventuais ameaças que podem ser vírus, *spam* ou outro *malware* até ataques de negação de serviço (DoS), intrusão, fraude e roubo.

Nas últimas décadas, face a evolução das tecnologias de informação e da necessidade de ampliação da utilização de telefonia IP para lá dos limites de uma rede de comunicações das organizações empresariais, a segurança do tráfego VoIP, tornou-se num assunto que está cada vez mais em voga.

Pode-se afirmar então que, a cada dia que aumenta o tráfego de voz pela Internet, as precauções como encriptação e autenticação, tornaram-se essências para uma boa prestação de serviços VoIP aos utilizadores.

## 2.4. *Protocolos*

Neste ponto, será apresentado um estudo sobre os protocolos da tecnologia VoIP com o intuito em transmitir alguns conhecimentos gerais acerca das características e funcionalidades de cada um dos protocolos associados à essa tecnologia.

Na seguinte figura está ilustrada uma breve descrição sobre todos os protocolos VoIP contidos nas diferentes camadas da rede IP.

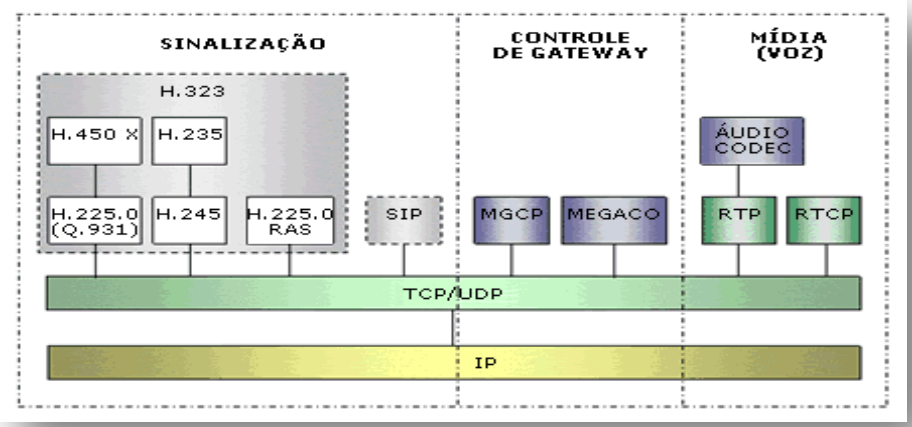



**Figura 10 – Protocolos da tecnologia VoIP [24].**

**NOTA:** Os protocolos VoIP ilustrados na figura anterior foram desenvolvidos a partir da década de 90, sendo que eles são actualizados constantemente consoante as necessidades dos utilizadores de modo garantir uma melhor qualidade de serviço entre os mesmos.

Importa salientar que neste subcapítulo, será elaborado um estudo mais detalhado sobre alguns protocolos que irão dar mais ênfase na elaboração deste projecto. São eles: SIP, H.323, IAX, SDP e o RTP.

### *2.4.1. SIP – Session Internet Protocol*

O SIP (*Session Initiation Protocol*) é um protocolo de sinalização da telefonia VoIP que foi desenvolvido pela IETF (*Internet Engineering Task Force*), nomeadamente pelo grupo MMUSIC (*Multiparty Multimédia Session Control*), com o intuito de munir um conjunto de funcionalidades avançadas de sinalização e controlo para um conjunto variado de serviços multimédia ao utilizador final.

**Arquitectura Protocolar SIP**

Foi publicado em 1996 com o RFC 2543 e publicado como uma proposta de standard em Março de 1999.Tem como objectivo principal o estabelecimento de uma comunicação entre dois utilizadores que possuem dispositivos multimédia, identificados por e-mails ou números de telefone, podendo também utilizar qualquer identificador sob a forma de um *hostname*.

Este protocolo permite ao utilizador inicializar, modificar e terminar uma sessão interactiva que envolva alguns elementos multimédia, tais como, a telefonia sobre Internet ou vídeo-conferência, a *instant messaging*, notificação de eventos ou controlo de dispositivos em rede (exemplo jogos online).

O protocolo SIP poderá localizar todos os recursos disponíveis para estabelecer uma chamada e conferências através de redes via IP, de uma forma eficiente baseados num nome (Ex: e-mail, número de telefone, etc.) independentemente da sua localização e posteriormente poderá negociar as características de sessão.

Importa salientar que, a referida comunicação tornou-se possível graças à integração e implementação de dois protocolos no protocolo SIP: RTP/RTCP e o SDP. O RTP é usado no transporte de voz em tempo real, enquanto o protocolo SDP é usado para a negociação entre ambas as partes das características da comunicação, como por exemplo, no tipo de codificação, taxa de amostragem, etc.

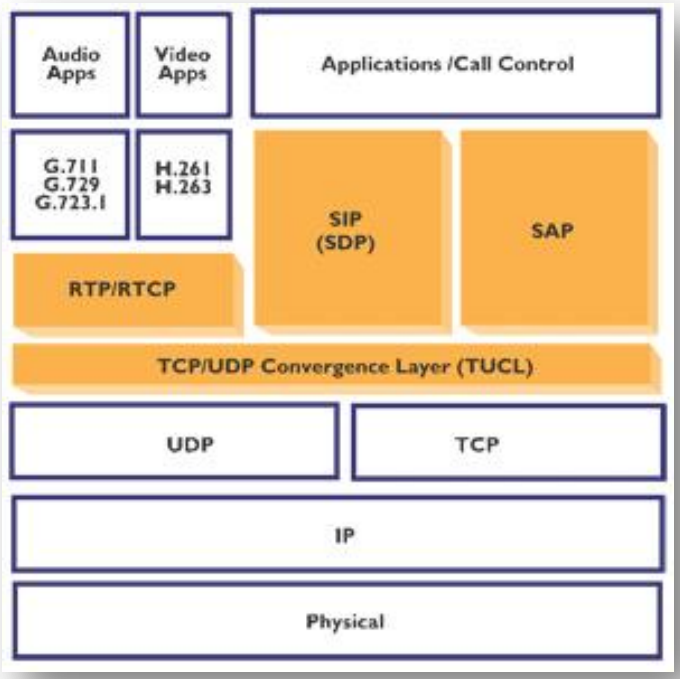



**Figura 11 – Arquitectura protocolar SIP [118].**

**Componentes do protocolo SIP**

O protocolo SIP suporta funcionalidades para estabelecer e terminar sessões multimédia: localização, disponibilidade, utilização de recursos e características de negociação.

A arquitectura do protocolo SIP é constituída pelas seguintes componentes lógicas: o *User Agent* (UA) que corresponde a parte do cliente e pelos servidores SIP, tais como, *Proxy Server, Registrar Server* e o *Redirect Server,* conforme esta ilustrada na seguinte figura:

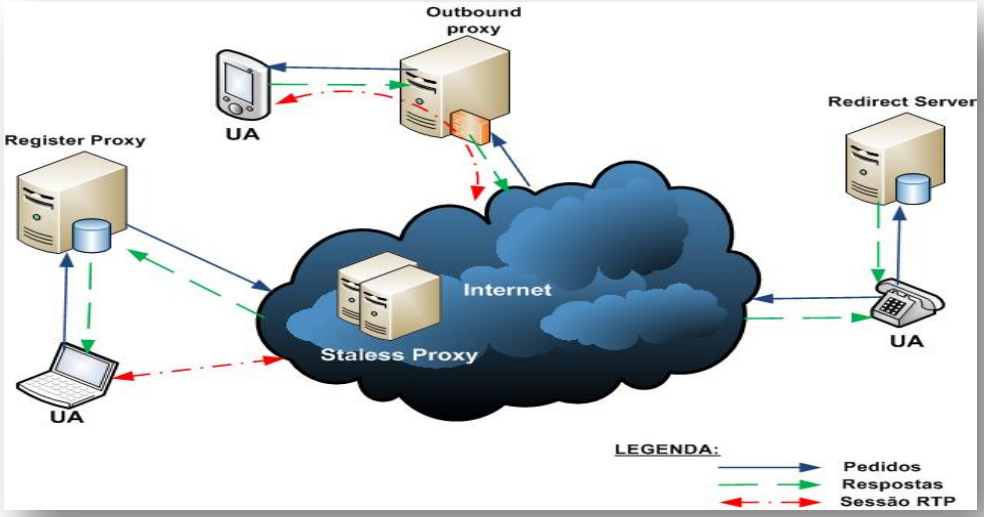



**Figura 12 – Exemplo de um cenário da arquitectura do protocolo SIP.**

Seguidamente, serão descritos todos os elementos que compõem a arquitectura do SIP, definindo os seus objectivos e as suas funcionalidades acrescidas durante as comunicações entre os *User Agent*.

1. ***User Agent***: é composto por duas partes distintas: o cliente (*User Agent Client* – UAC) e o servidor (*User Agent Server* - UAS), respectivamente. O UAC é a entidade lógica que envia os pedidos e recebe as respostas correspondentes. O UAS é a entidade lógica que responde aos pedidos SIP. O UA permite normalmente a interface com o utilizador, mas pode também ser um sistema automático que não envolva interacção como um sistema de voice mail ou um sistema de redireccionamento de chamadas.

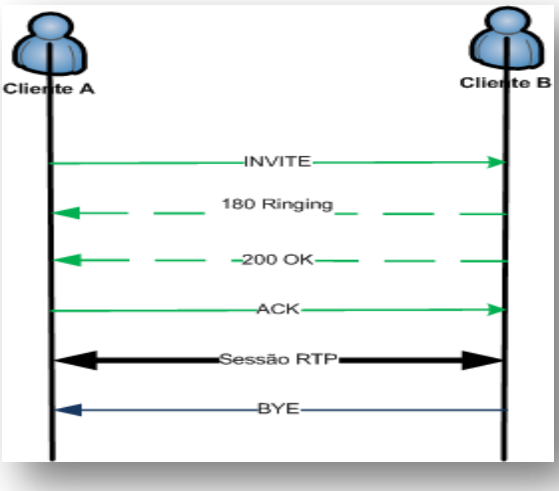



**Figura 13 – Sessão estabelecida entre dois UA.**

2. ***Proxy Server*:** É uma entidade intermediária que actua como cliente e como servidor de forma a estabelecer a ligação entre os utilizadores. Este servidor tem uma funcionalidade similar à de um *proxy http*. Sobre ele recai a tarefa de efectuar o reencaminhamento dos pedidos que recebe das outras entidades. Existem dois tipos de *Proxy Server*: *Stateful Proxy* e *Stateless Proxy*.
    - ***Stateful Proxy –*** este tipo de *proxy* mantém o estado das transacções durante o processamento dos pedidos (*request*). Isto permite a dividir uma mensagem de pedido em vários (propriedade de *forking*), tendo como finalidade a tentativa de encontrar em paralelo múltiplas localizações do chamado e apenas enviar as melhores respostas ao utilizador que fez a chamada;
    - ***Stateless Proxy –*** este tipo de *proxy* não guarda qualquer tipo de informação de estado da transacção na memória. Limita-se simplesmente a reenviar as mensagens que lhe chegam. São mais adequados quando existem requisitos de velocidade como numa *backbone* de uma infra-estrutura SIP;
    - ***Outbound Proxy –*** é um *proxy* que recebe pedidos de um utilizador, mesmo que não seja ele o destinatário do pedido. Esta configuração é muito utilizada e adequada quando existem *firewall*, em que o UA é configurado para enviar pedidos e receber pedidos através deste tipo de servidor.

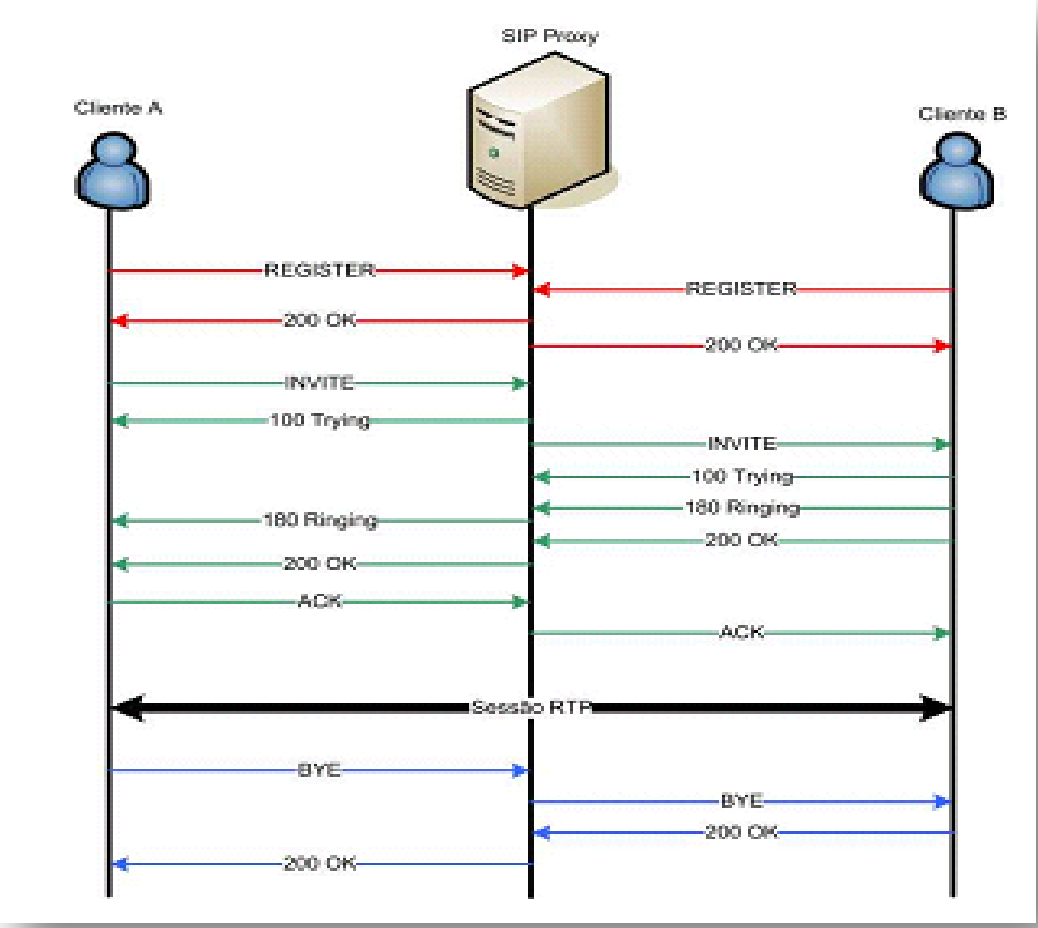



**Figura 14 – Sessão estabelecida entre dois UA com o Proxy Server.**

3. ***Registrar Server*:** é um servidor que aceita pedidos de registo dos utilizadores e mantém toda a informação proveniente desses pedidos, fornecendo serviços de localização e tradução de endereços no seu domínio que controla.
4. ***Redirect Server*:** é o servidor que gera respostas de redireccionamento aos pedidos a ele efectuados. Este servidores reencaminham os pedidos para o servidor seguinte.

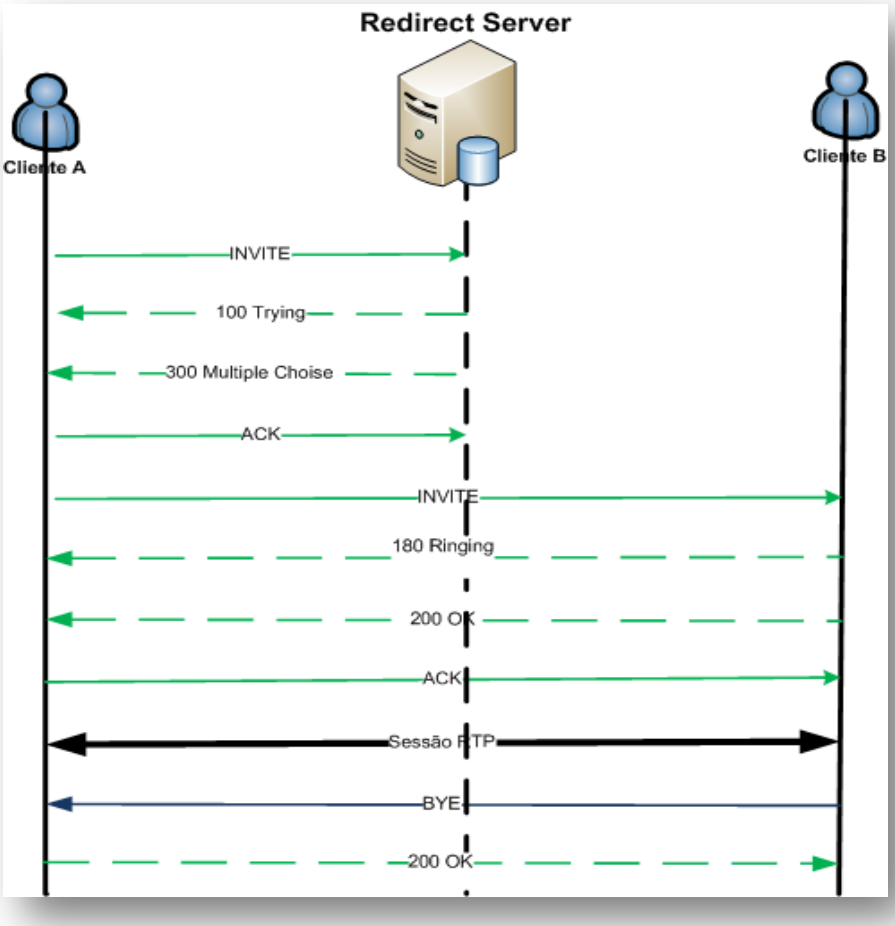



**Figura 15 – Sessão estabelecida entre dois UA usando o Redirect Server.**

### Mensagens SIP

O SIP é um protocolo de texto com uma semântica semelhante à do protocolo HTTP. Esta propriedade permitiu a reutilização de código e uma integração mais simples dos servidores SIP com servidores de Web e de e-mail. Tal como o HTTP, o SIP define a comunicação através de dois tipos de mensagens: os pedidos e as respostas. Os UACs fazem os pedidos e os UASs retornam respostas aos pedidos dos clientes. Uma mensagem SIP consiste numa linha inicial seguida de um ou mais cabeçalhos (*headers*), uma linha vazia que indica o fim dos cabeçalhos e, por fim, o corpo da mensagem que é opcional.

Os cabeçalhos são usados para transportar informação necessária às entidades SIP para processarem os pedidos ou respostas. Caso exista o corpo da mensagem, este é usado para descrever a sessão, contendo normalmente o protocolo *Session Description Protocol* (SDP); no entanto pode ter outro tipo de conteúdo, como ASCII ou HTML.

**Métodos SIP**

Na seguinte tabela, estão apresentados os seis métodos de operação, definidos pelo RFC 2543 e que podem ser utilizados em pedidos: *INVITE*, *ACK*, *OPTIONS*, *BYE, CANCEL* e *REGISTER*.

| Mensagem SIP | Descrição |
|---|---|
| INVITE | Convida um utilizador para uma chamada. |
| ACK | Confirmação do estabelecimento da comunicação. |
| OPTIONS | Solicita informação sobre as capacidades de um servidor. |
| BYE | Termina a conexão entre utilizadores e rejeita uma chamada. |
| CANCEL | Termina um pedido ou pesquisa por um utilizador. |
| REGISTER | Utilizado para sinalização em plena sessão. |

**Tabela 2 – Métodos do protocolo SIP.**

Importa salientar que, para além destes seis métodos do referido protocolo poderão sempre ser utilizados alguns métodos adicionais, como por exemplo, *INFO*, *SUBSCRIBER*, etc. (sendo estes são publicados noutros RFCs).

Como não existe nenhum mecanismo de características gerais para transportar informação de controlo de sessão, a IETF adicionou um método INFO para solucionar este problema (RFC 2976).

**Respostas SIP (State Codes)**

Depois de ser efectuado o pedido SIP, o receptor irá responder com uma mensagem contendo um código da resposta constituído por três dígitos que permitem a classificação dos diferentes tipos de resposta.

Na seguinte tabela estão descritos os respectivos códigos, sendo que o primeiro dígito define sempre a classe da resposta:

| Classe | Descrição | Exemplo |
|---|---|---|
| 1XX | Mensagem de informação | 100 Trying, 180 Ringing |
| 2XX | Resposta de sucesso | 200 OK |
| 3XX | Resposta de redireccionamento | 302 Moved Temporarily |
| 4XX | Erro no cliente | 404 Not Found |
| 5XX | Erro no servidor | 501 Not Implemented |
| 6XX | Erro global | 603 Decline |

**Tabela 3 – Exemplo de respostas do protocolo SIP (State Codes).**

### Mensagens de Erros SIP

Na seguinte tabela, estão apresentados os erros mais comuns que poderão surgir nas mensagens durante uma determinada sessão de comunicação multimédia usando o protocolo SIP. Esta tabela faz uma referência não só à classe, como também ao código dessas mensagens contendo uma breve descrição do conteúdo da mensagem de erro.

| Classe | Designação | | |
|---|---|---|---|
| 4XX | Erro no cliente: O pedido contém sintaxe inválida | | |
| Código | Descrição | Código | Descrição |
| 400 | Bad request | 421 | Extension Required |
| 401 | Unauthorized | 422 | Session Timer Interval Too Small |
| 402 | Payment Required | 423 | Interval Too Brief |
| 403 | Forbidden | 428 | Use Authentication Token |
| 404 | Not Found | 429 | Provide Referror Identity |
| 405 | Method Not Allowed | 480 | Temporarily Unavailable |
| 406 | Not Acceptable | 482 | Loop Detected |
| 407 | Proxy Authentication Required | 483 | Too Many Hops |
| 408 | Request Timeout | 484 | Address Incomplete |
| 409 | Conflict | 485 | Ambiguous |
| 410 | Gone | 486 | Busy Here |
| 411 | Length Required | 487 | Request Terminated |
| 413 | Request Entity Too Large | 488 | Not Acceptable Here |
| 414 | Requet-URI Too Long | 489 | Bad Event |
| 415 | Unsupported Media Type | 491 | Request Pending |
| 416 | Unsupported URI Scheme | 493 | Request Undecipherable |
| 420 | Bad Extension | | |
| Classe | Designação | | |
| 5XX | Erro no servidor | | |
| Código | Descrição | Código | Descrição |
| 500 | Server Internal Error | 504 | Gateway Timeout |
| 501 | Not Implemented | 505 | Version Not Supported |
| 502 | Bad Gateway | 513 | Message Too Large |
| 503 | Service Unavailable | | |
| Classe | Designação | | |
| 6XX | Erro Global | | |
| Código | Descrição | Código | Descrição |
| 600 | Busy Everywhere | 604 | Does Not Exist Anywhere |
| 603 | Decline | 606 | Not Acceptable |

**Tabela 4 – Mensagens de erros SIP.**

### Cabeçalhos SIP

Os cabeçalhos SIP são usados para transportar a informação até às entidades SIP. Estes cabeçalhos são similares aos do HTTP não só quanto à semântica como também na sintaxe. Alguns dos referidos cabeçalhos são usados em todas as mensagens enquanto outros só fazem sentido em determinados pedidos ou em respostas.

Quando um cabeçalho aparecer numa mensagem e não fizer parte da categoria dessa mensagem é simplesmente ignorado.

Os principais campos são:

| Cabeçalho SIP | Descrição |
|---|---|
| Via | Indica qual o protocolo de transporte usado e a rota de pedido (*request route*), cada proxy adiciona uma linha a este campo. |
| From | Indica o remetente da mensagem |
| To | Indica o endereço do destinatário a ser enviado a mensagem |
| Call-Id | Identifica cada chamada e o endereço da *host*. Deverá ser o mesmo para todas as mensagens dentro da mesma transacção |
| Cseq | Indica a sequência de cada mensagem e é iniciado de uma forma aleatória. |
| Contact | Indica os contactos do utilizador |
| User Agent | Indica o nome do agente que está associado à chamada. |

**Tabela 5 – Cabeçalhos SIP.**

**Endereços SIP**

O protocolo SIP identifica o utilizador através de um tipo de *Universal Resource Identifier* (URI) chamado SIP URI que está definido no RFC 2396.

O SIP URI utiliza a forma mais comum de endereçamento de utilizadores na Internet, o formato do endereço de e-mail, conforme ilustra a seguinte tabela:

| Endereços SIP | Descrição |
|---|---|
| sip:utilizador@dominio | O domínio indica o nome completo do domínio. |
| sip:utilizador@host | O *host* indica o nome da máquina. |
| sip:utilizador@IP-address | O *IP-address* indica o endereço IP da máquina. |
| sip:numero-telefone@gateway | O *gateway* indica o nome do servidor que permite o acesso ao utilizador através da PSTN. |

**Tabela 6 – Endereços SIP.**

A solução de identificação SIP, também poderá ser baseada em entidades existente na rede IP como o DNS, que foi recentemente publicada no RFC 3263. Na referida norma estão descritos todos os procedimentos DNS utilizados pelos clientes para traduzir o endereço SIP URI num endereço IP, porto e protocolo de transporte, ou pelos servidores para retornar uma resposta ao cliente caso o pedido falhe.

**Exemplo de Comunicação SIP**

Na seguinte figura, está ilustrada um exemplo de uma comunicação SIP onde será feita uma breve descrição sobre as diversas transacções efectuadas ao longo da sessão estabelecida. Uma transacção SIP consiste em vários pedidos e respectivas respostas e a forma de os agrupar é recorrendo ao parâmetro CSeq, como foi anteriormente citado.

Descrição:

1. Registo de clientes: Os clientes devem efectuar o registo de modo a que possam estabelecer o contacto entre ambos. Neste caso, os terminais enviam um pedido de registo (*REGISTER*), onde os campos "*FROM*" e "*TO*" correspondem ao utilizador a ser registado. O servidor de *Proxy*, que actua como "*Registar*", irá efectuar uma consulta de toda a informação sobre o respectivo cliente na base de dados, de modo a verificar se ele estará ou não autenticado, e seguidamente irá enviar uma mensagem OK, se não houver problema.

2. Estabelecimento de sessão: Para estabelecer uma sessão será enviado um pedido *INVITE* do cliente A ao *proxy*. A seguir, o SIP *Proxy* envia uma mensagem de informação 100 *Trying* de modo a acabar com as possíveis repetições de *INVITE* por parte do cliente e reenvia o pedido para o cliente B. Seguidamente, o cliente B enviará uma mensagem 180 *Ringing* de modo a informar o utilizador que tem uma chamada. De imediato o *proxy* reenvia a mensagem 180 *Ringing* para o cliente A. Por ultimo, a mensagem 200 OK corresponde à aceitação do processo, isto é, o utilizador B atende a chamada. Logo será estabelecida a chamada entre os respectivos clientes. O protocolo RTP inicia com os parâmetros (portos, endereços, codecs, etc.) previamente definidos através do protocolo SDP.

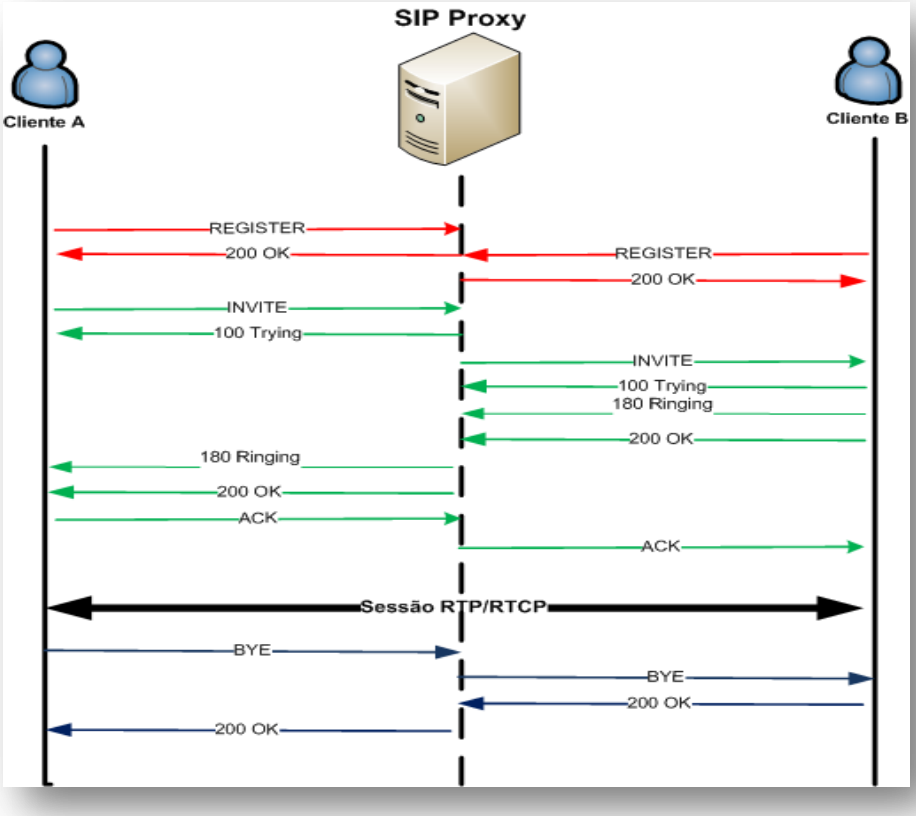



**Figura 16 – Exemplo de uma chamada SIP.**

3. Finalização da sessão: Para finalizar uma sessão pré-estabelecida poderá ser enviado um pedido *BYE* ao *proxy* por parte do cliente A que será reencaminhado para o cliente B, ou vice-versa. O cliente B ao receber este pedido, termina o envio dos meios e retorna uma resposta 200 OK, concluindo a chamada e o diálogo entre os dois utilizadores.

### *2.4.2. SDP – Session Description Protocol*

O protocolo SDP (*Session Description Protocol*) foi desenvolvido e definido no RTC 2327, pela IETF (*Internet Engineering Task Force*), nomeadamente pelo grupo MMUSIC (*Multiparty Multimédia Session Control*, com o intuito de descrever a sintaxe a usar na negociação das capacidades técnicas dos clientes.

O seu objectivo inicial era a descrição de sessões *multicast* estabelecidas no *backbone* da Internet, o *MBONE*. Embora, este protocolo ter sido criado para ser usado em sessões de teleconferências de multimédia, ele poderá ser incorporado em diferentes protocolos, como o SIP, SAP (*Session Announcement Protocol*), RTSP (*Real Time Streaming Protocol*), HTTP (*Hypertext Transport Protocol*), correio electrónico (com extensões MIME), etc.

A descrição de uma sessão presente no protocolo SDP poderá conter as seguintes informações:

- O tipo de dados de multimédia (vídeo, áudio, etc.);
- O tipo do protocolo de transporte (RTP/UDP/IP, H.320, etc.);
- O formato do tipo de dados utilizado (vídeo H.261, vídeo MPEG, etc.);
- O endereço IP de destino (*unicast* ou *multicast*) e as portas usadas pelos protocolos de transportes UDP ou TCP para o envio e/ou recepção;
- A duração de início e fim da sessão.

O SDP usa uma sintaxe textual idêntica ao do protocolo SIP. O conteúdo de uma mensagem SDP é constituído por um conjunto de linhas de texto, denominados por campos, cujo nome é identificado por uma única letra.

Na seguinte tabela está apresentado os diversos nomes que poderão facilitar a sua interpretação:

| Parâmetros | Descrição |
|---|---|
| V = | Versão do protocolo utilizado (Mandatário). |
| o = | Responsável ou criador da sessão (Mandatário). |
| S = | Nome da sessão estabelecida (Mandatário). |
| I = | Informação da sessão (Opcional). |
| U = | Descrição da URI (Uniform Resource Identifier) (Opcional). |
| e = | Endereço de E-mail (Opcional). |
| p = | Número de telefone (Opcional). |
| C = | Informação da conexão (Mandatário). |
| b = | Informação de largura de banda (Opcional). |
| Z = | Correcção do fuso horário (Opcional). |
| K = | Chave de encriptação da mensagem (Opcional). |
| a = | Linhas de atributos do parâmetro (Opcional). |
| T = | Tempo de duração da sessão (Opcional). |
| R = | Número de repetição efectuada. (Opcional). |
| m = | Informação de media (Opcional). |

**Tabela 7 – Campos existentes na mensagem do protocolo SDP.**

### *2.4.3. RTP – Real Time Protocol*

O protocolo RTP é utilizado para o suporte de serviços de transporte em aplicações de tempo real, como por exemplo *streaming* a pedido e serviços interactivos, tais como uma sessão de videoconferência entre dois utilizadores com equipamentos VoIP.

Este protocolo foi publicado pela IETF com o RFC 3550 e permite funções de transporte ponto a ponto na rede e é apropriado para aplicações que transmitem dados em tempo real como áudio, vídeo, sobre serviços de redes *unicast* ou *multicast*. O RTP tem por base o protocolo UDP (*User Datagram Protocol*) onde não existe uma conexão direccionada, o que impossibilita a verificação da recepção correcta de pacotes de dados.

Numa sessão de RTP, pressupõe-se que os utilizadores ao estabelecerem uma conexão se comuniquem através de endereços IP em conjunto com duas portas UDP, não só a de controlo como a de transporte de dados. Em cada sessão é apenas transmitido um pacote de identificação de conteúdo e a sua informação de controlo.

A estrutura de cada pacote de RTP tem um cabeçalho fixo com um mínimo de 12 bytes, seguido de uma lista variável de fontes que contém uma serie de informação que permitem identificar os dados contidos no pacote sendo ainda necessário passar informação de controlo através dos cabeçalhos dos protocolos utilizados para transportar o pacote RTP.

O cabeçalho é composto pelo carimbo temporal, o seu número de sequência de pacotes e por um identificador de sincronização. Neste protocolo não existe a possibilidade de recuperar pacotes perdidos. Este protocolo foi desenhado para ser escalável, flexível e existe separação entre os mecanismos de dados e controlo.

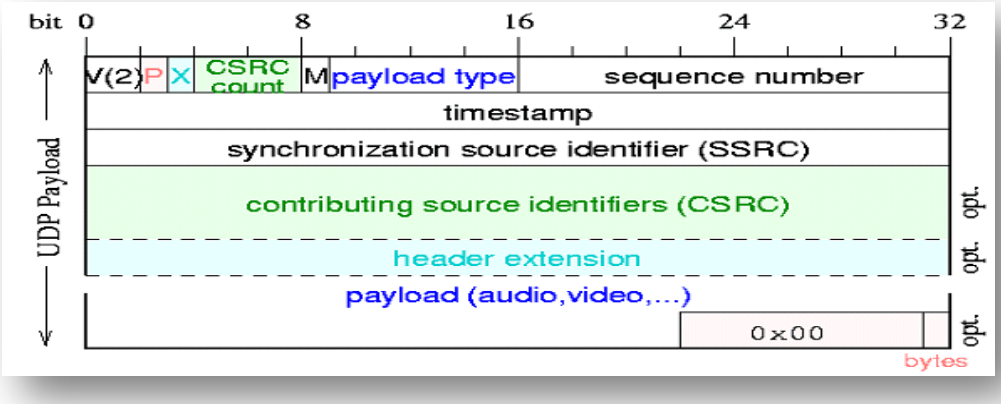



**Figura 17 – Exemplo de cabeçalho de um pacote RTP [119].**

Descrição dos campos:

| Parâmetros | Tamanho (bits) | Descrição |
|---|---|---|
| V (Version) | 2 | Indica a versão de RTP (tem 2 bits) |
| P (Padding) | 1 | Indica o *Padding* e tem 1 bit. Caso este bit estiver activado, serão adicionados octetos no final do pacote, de modo a que este tenha um tamanho pré-definido. Este método é usado quando o fluxo de média é encriptado; |
| X (Extension) | 1 | Indica a extensão e ocupa 1 bit. Se estiver activo, será adicionada uma extensão de modo a que o cabeçalho fique com 14 octetos. As extensões são definidas para certos tipos de dados; |
| CC (CSRC Count) | 4 | Este campo indica o número de identificadores de origem e ocupa 4 bits. Este campo é usado somente com misturadores que recebem diversos fluxos RTP e enviam somente um; |
| M (Marker) | 1 | Este campo corresponde ao *Marker* e é usado para indicar o início de uma frame em vídeo ou o início de uma conversação do tipo intermitente com supressão de silêncio. |
| PT (Payload Type) | 7 | Identifica o formato do *payload* do pacote RTP, determinando a interpretação necessária à aplicação. Define o codec usado. Este valor coincide com o número de perfil associado nas informações SDP; |
| SN (Sequence Number) | 16 | Permite a identificação do pacote, permitindo a aplicação destino detectar se houve a não perda de pacotes. O valor inicial é aleatório, o que dificulta ataques sobre o código encriptado. |

**Tabela 8 – Campos existentes na mensagem do protocolo RTP.**

### *2.4.4. RTCP – Real Time Control Protocol*

O protocolo RTCP (*Real Time Control Protocol*) foi publicado pela IETF com o RFC 3550 e está relacionado com RTP. O RTCP tem por base a periodicidade da transmissão de pacotes de controlo entre os utilizadores numa sessão de RTP.

O objectivo principal do protocolo RTCP é fornecer um *feedback* da qualidade dos dados distribuídos. Este protocolo é baseado na transmissão periódica de pacotes de controlo a todos os participantes na sessão, usando o mesmo mecanismo de distribuição que o de pacotes de dados.

Os pacotes RTCP podem conter informação sobre:

- A qualidade do serviço para os participantes da sessão: os receptores indicam a qualidade da recepção relativa a cada emissor (número de pacotes perdidos, *jitter e round-tripdelay*). Os emissores podem usar esta informação (no caso de aplicações adaptativas) para ajustar os débitos de codificação e outros parâmetros;
- Sincronização entre meios: por razões de flexibilidade, pacotes de áudio e vídeo são muitas vezes transportados em *streams* separados, que necessitam de ser sincronizados no receptor (por exemplo para garantir *lip synch*); a informação de sincronização entre fontes (mesmo se em servidores diferentes) é fornecida pelo RTCP;
- Identificação dos participantes na sessão: nome, endereço electrónico, úmero de telefone;
- Controlo da sessão: devido ao número de participantes numa sessão ser variável e eventualmente muito elevado, torna-se necessário evitar que o número de pacotes RTCP cresça linearmente com a dimensão do grupo *multicast*. O período entre pacotes RTCP deve ser ajustado dinamicamente à dimensão do grupo, procurando-se que o tráfego RTCP consuma uma percentagem sensivelmente constante do tráfego total.

Para garantir um funcionamento correcto, o RTCP insere uma característica fundamental nos pacotes, um identificador de fim de pacote designado CNAME (nome canónico). Na recepção, o CNAME é utilizado na associação de *substreams* garantindo a sua sincronização, sendo também importante para reportar alguns dados estatísticos para a aplicação. Estes dados estatísticos incluem o número de pacotes enviados, perdidos e o jitter.

Na comunicação via RTCP, cada utilizador envia pacotes de controlo para os outros utilizadores, o que permite a particularidade de identificar o número de

utilizadores que estão a partilhar a mesma rede na sessão. O uso desta informação permite ainda definir a banda disponível para a comunicação, podendo o utilizador limitar o fluxo de dados que partilha.

A seguir será apresentada uma tabela contendo os vários tipos de pacotes existentes no protocolo RTCP:

| Tipo de Pacotes | Nome | Descrição |
|---|---|---|
| SR | Sender report | Enviado por um participante que envia e recebe pacotes. |
| RR | Receiver report | Enviado por um participante que só recebe pacotes RTP. |
| SDES | Source description | Contém informação acerca do participante na sessão incluindo endereço de correio electrónico, número de telefone e máquina. |
| BYE | Bye | Enviado para terminar uma sessão RTP. |
| APP | Application specific | Definido por um determinado perfil. |
| XR | Extended report | Relatório e sumário. |

**Tabela 9 – Exemplo de pacotes existentes no protocolo RTCP.**

### *2.4.5. H.323*

O protocolo H.323 pertence à família das recomendações *standard* da ITU-T (*International Telecommunication Union Telecommunication Standardization sector*), nomeadamente o H.32x, pertencente à série H da ITU-T, e que trata de "Sistemas Audiovisuais e Multimédia".

Foi aprovado em 1996 pelo Grupo de estudos 16 do ITU e sua versão 2 foi aprovada em Janeiro de 1998. O H.323 tem como objectivo principal especificar os sistemas de comunicação multimédia em redes baseadas em pacotes e que não provêem uma Qualidade de Serviço (QoS) garantida.

Este protocolo estabelece ainda, uma série de padrões para codificação e descodificação de fluxos de dados de áudio e vídeo, garantindo que todos os produtos baseados no padrão H.323 de um determinando fabricante possam ser integrados com produtos H.323 de outros fabricantes.

Uma das principais características do protocolo H.323 é a sua flexibilidade, pois poderá ser aplicada tanto à voz, quanto à vídeo-conferência ou multimédia.

Actualmente devido à essa flexibilidade de utilização, os equipamentos H.323, estão-se a tornar populares no mercado corporativo e empresarial pelas seguintes razões:

- A especificação H.323 define padrões de voz para uma infra-estrutura existente, além de ser projectada para compensar o efeito de latência em LANs, permitindo que os clientes possam usar aplicações de voz sem mudar a infra-estrutura de rede;
- As redes baseadas em IP estão a ficar mais rápidas, com velocidades de 100 Mbps ou Gigabit;
- Este protocolo fornece padrões de interoperabilidade entre LANs e outras redes;
- Com o protocolo H.323 o gestor de rede poderá não só administrar o fluxo dos pacotes de dados existentes na rede poderá ser administrado, como também, poderá restringir a quantidade de largura de banda disponível para conferências e voz. O suporte à comunicação *Multicast* também reduz exigências de largura de banda;
- O protocolo H.323 tem um elevado apoio financeiro por parte de muitas empresas de comunicação e organizações multinacionais, tais como, a Intel, a Microsoft, Cisco e a IBM. Actualmente, graças ao investimento sistemático destas multinacionais, estão a gerar um nível mais alto de consciência no mercado.

**Componentes do protocolo H.323**

Para que se possa utilizar e perceber correctamente o protocolo H.323, é fundamental perceber a importância e as funcionalidades dos seus diversos componentes.

Apesar do protocolo H.323 ser usado em várias aplicações, (como por exemplo, VoIP, videoconferência e outras), o processamento H.323 é distribuído por vários componentes:

- Terminais: são equipamentos que permitem ao utilizador estabelecer uma comunicação bidireccional em tempo real com outro terminal H.323, *Gateway* ou MCU (*Multipoint Control Unit*). Esta comunicação poderá suportar trocas de elementos de multimédia, tais como, ficheiros áudio, vídeo e/ou dados em qualquer combinação entre dois terminais. Um terminal poderá ser um telefone IP, um computador pessoal (PC) com microfone, altifalantes e câmara de vídeo. Todos os terminais H.323 têm que suportar o H.245, Q.931, RAS

(*Registration, Admission and Status*) e RTP *(Real-Time Transport Protocol)*. Estes terminais poderão também suportar o protocolo de conferência de dados T.120, codificadores de vídeo e suporte para MCU;

- *Gateways* (GW): são dispositivos que permitem estabelecer a interligação entre duas redes IP distintas, de modo a possibilitar uma comunicação entre os sistemas telefónicos convencionais (PSTN) e os sistemas telefónicos VoIP.

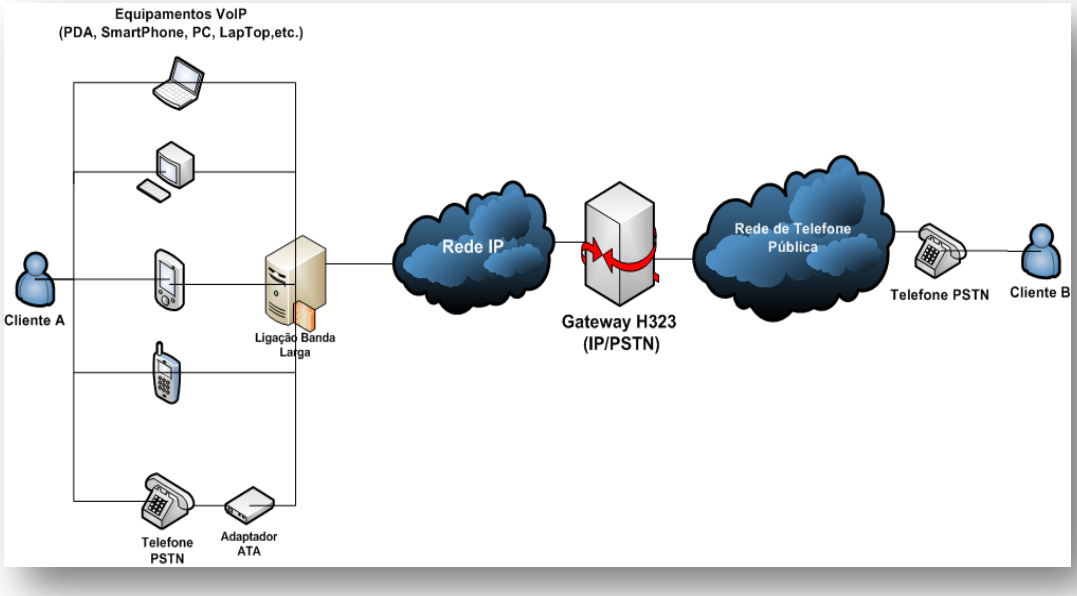



**Figura 18 – Exemplo de um Gateway H.323.**

- *Gatekeepers* (GK): O *gatekeeper* constitui um dos componentes mais importantes de uma rede H.323, visto que, possui uma série de funcionalidades especiais que permitem efectuar as seguintes operações: tradução de identificadores H.323 e números E.164 (números de telefone) em endereços IP, a autenticação de terminais H.323 (de acesso à Zona), a autorização de terminais H.323 (na utilização de Recursos), o registo de terminais H.323 (serviço de directoria), o controlo da largura de banda e a administração de zonas H.323. Uma zona é constituída por todos os equipamentos H.323 (terminais, MCU e *gateways*) que se encontram registados no *gatekeeper*. Este dispositivo controla apenas as ligações H.323 efectuadas na vizinhança da sua rede.

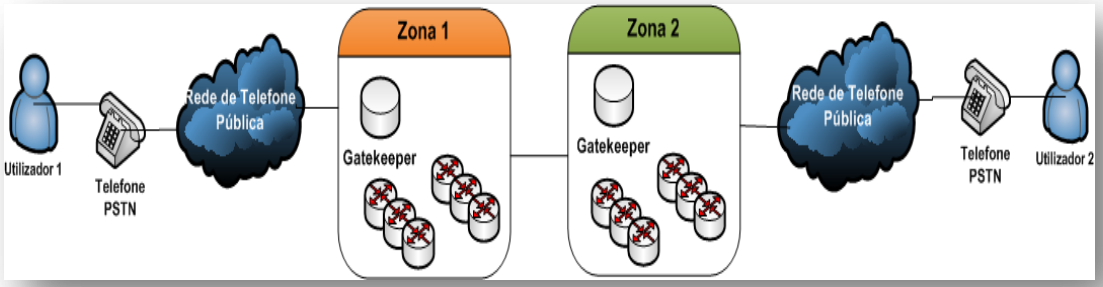



**Figura 19 – Exemplo de um Gatekeeper H.323.**

- *Mutipoint Control Units* (MCU's): Este dispositivo permite estabelecer comunicações com sessões de multiconferências entre determinados equipamentos VoiP. Uma MCU tem não só a função de gerir todos os recursos usados na conferência, como também, negociar com os terminais de forma a determinar os codecs a utilizar e ainda poderá manipular o fluxo de média. Os terminais IP efectuam uma chamada para a MCU, e seguidamente escolhem a sessão em que pretendem participar. De seguida, a MCU recebe os sinais de áudio e vídeo de todos os participantes, mistura-os e envia o resultado para todos, conforme ilustra a seguinte figura:

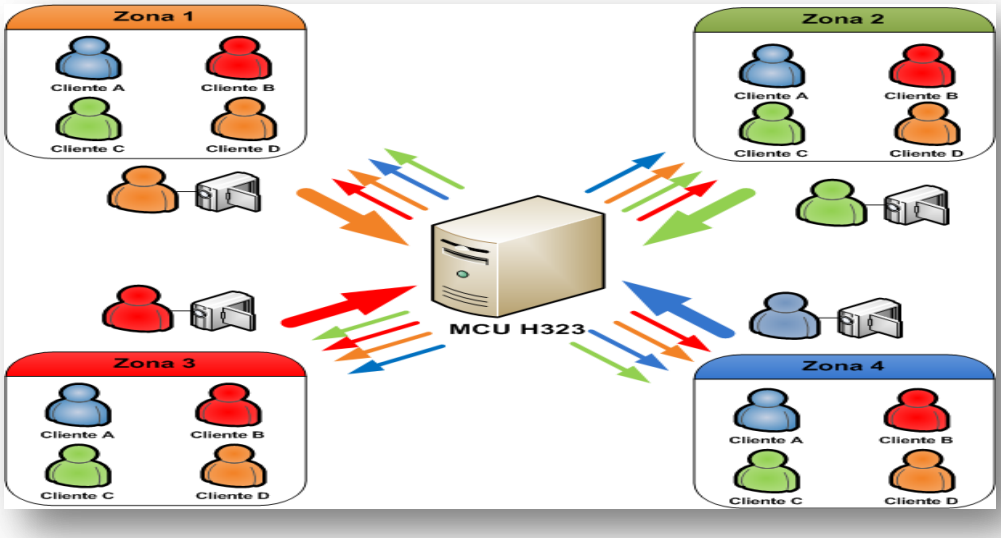



**Figura 20 – Exemplo de uma sessão de multiconferências com MCU H.323.**

- Proxy: Um servidor *proxy* H.323 tem não só, a capacidade de examinar todos os pacotes trocados na rede durante uma comunicação entre duas aplicações VoIP, como também, ter a possibilidade de determinar o destino de uma

chamada e estabelecer a conectividade desta chamada, executando todos os procedimentos necessários para o efeito.

**Arquitectura Protocolar H.323**

Na seguinte figura está ilustrada, a arquitectura do protocolo H.323, contendo a descrição dos principais protocolos que são utilizados simultaneamente com a referida especificação.

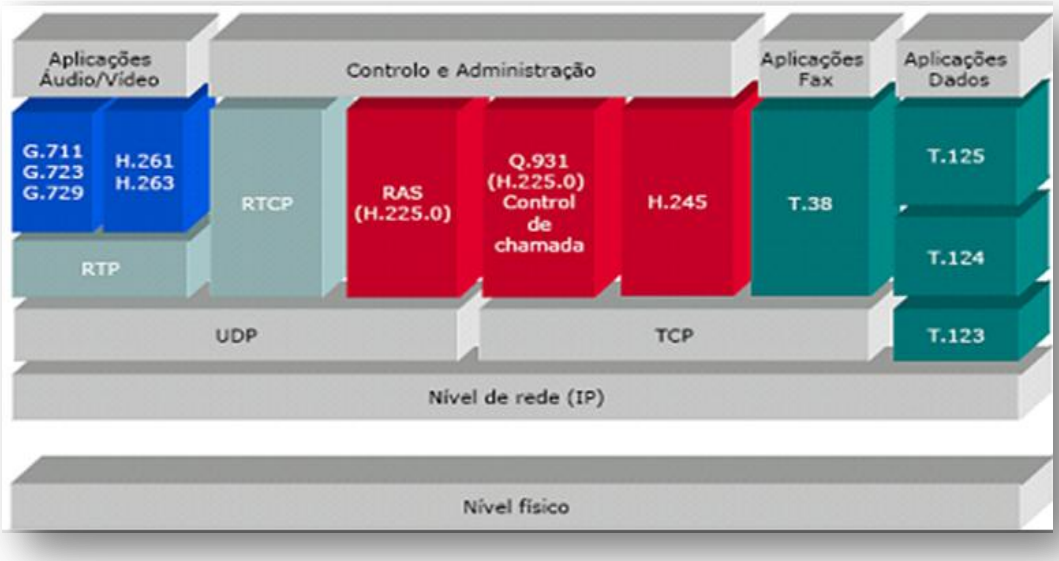



**Figura 21 – Arquitectura protocolar H.323 [120].**

Descrição:

1. RTP/RTCP (*Real-Time Transport Protocol / Real-Time Transport Control Protocol*): ambos os protocolos são utilizados para efectuar o transporte de dados de multimédia em tempo real, tais como, áudio, vídeo e dados. O protocolo RTP é praticamente usado em todas as arquitecturas VoIP, não só de vídeo-conferência, como também, de *media-on-demand*, entre outras aplicações.
2. RAS (*Registration, Admission and Status*): O RAS é um protocolo de Registo, Admissão e Estado. Este protocolo é o responsável pelo envio de mensagens de sinalização num sistema áudio ou vídeo baseado em H.323.
3. H225.0: este protocolo permite não só descrever a sinalização de uma chamada, como também, os elementos de multimédia, o fluxo de pacotes, fluxo de média e controlo dos formatos das mensagens.

4. H.245: o protocolo H.245 é utilizado no controlo de comunicações multimédia. O H.245 serve também para descrever as mensagens e determinados procedimentos que poderão ser utilizados na abertura e no fecho de canais lógicos de áudio, vídeo e dados, troca de capacidades, controlo e indicações.
5. Q.931: este protocolo é utilizado para sinalização de chamadas. Está incluído na recomendação H.225.0.
6. RSVP (*Resource ReSerVation Protocol*): permite efectuar reservas de recursos existentes numa determinada rede de forma a garantir uma melhor qualidade de serviço (QoS).
7. T.120: este protocolo é utilizado para conferência de dados e controlo de conferência em comunicações multimédia interactivas – multiponto e ponto-a-ponto.

**Codecs H.323**

Os codificadores ou *"Codecs" s*ão dispositivos que permitem efectuar uma redução da largura de banda para a transmissão de dados, utilizando técnicas de compressão de dados que operaram em tempo real devido a características do próprio serviço, como por exemplo, a comunicação interactiva.

Para a codificação do sinal áudio em tempo real são recomendados pelo protocolo H.323 os seguintes *codecs*:

1. G.711: este protocolo é uma recomendação da ITU – Modulação por impulsos codificados (PCM) de voz. O protocolo G.711 é um padrão de áudio e a sua presença é de uso obrigatório em todos os sistemas de videoconferência. O G.711 requer uma taxa de transmissão de dados entre os 56 e os 64Kbit/s.
2. H.261 e H.263: Estes codificadores são utilizados para a transmissão de vídeos do protocolo H.323, mas contudo, poderão ser utilizados outros codecs adicionais para a mesma finalidade.

**Sinalização H.323**

Todas as funcionalidades de sinalização utilizadas no protocolo H.323 são baseadas na recomendação H.225. Esta referida recomendação especificarão o uso e suporte de mensagens do tipo Q.931/Q.932. Essas mensagens serão enviadas pelo protocolo TCP (*Transmission Control Protocol*) no porto 1720. Neste porto, as

mensagens de controlo de chamadas Q.931 serão enviadas para a configuração, manutenção e desconexão.

Na seguinte tabela será apresentada alguns exemplos de mensagens que poderão ser encontradas nas especificações Q.931/Q.932.

| Tipos de Mensagem | Descrição |
|---|---|
| **Setup** | Esta mensagem será enviada com o intuito de inicializar uma chamada H.323 ou para estabelecer uma conexão com um determinado equipamento H.323. Ela irá conter não só o endereço IP, como também, o porto e alias do destinatário. |
| **Call Proceeding** | Esta mensagem será enviada pelo Gatekeeper a um determinado terminal, avisando-o da tentativa de estabelecimento da chamada após o número do destinatário ser analisado. |
| **Alerting** | Esta mensagem irá indicar o início da fase de geração do tom. |
| **Connect** | Este mensagem indica o início de uma sessão |
| **Release Complete** | Enviada pelo terminal para iniciar a desconexão. |
| **Facility** | É uma mensagem do standard Q.932 usado como pedido para um serviço adicional. |

**Tabela 10 – Exemplo de mensagens de sinalização H.323.**

**Exemplo de Comunicação H.323**

Na seguinte figura, está ilustrada um exemplo de uma comunicação H.323 onde será feita uma breve descrição sobre as diversas transacções efectuadas ao longo da sessão estabelecida.

Podemos ainda observar que, numa transacção H.323, existem quatro fases importantes que consistem em várias trocas de mensagens, utilizando os vários tipos de protocolos existentes na referida comunicação.

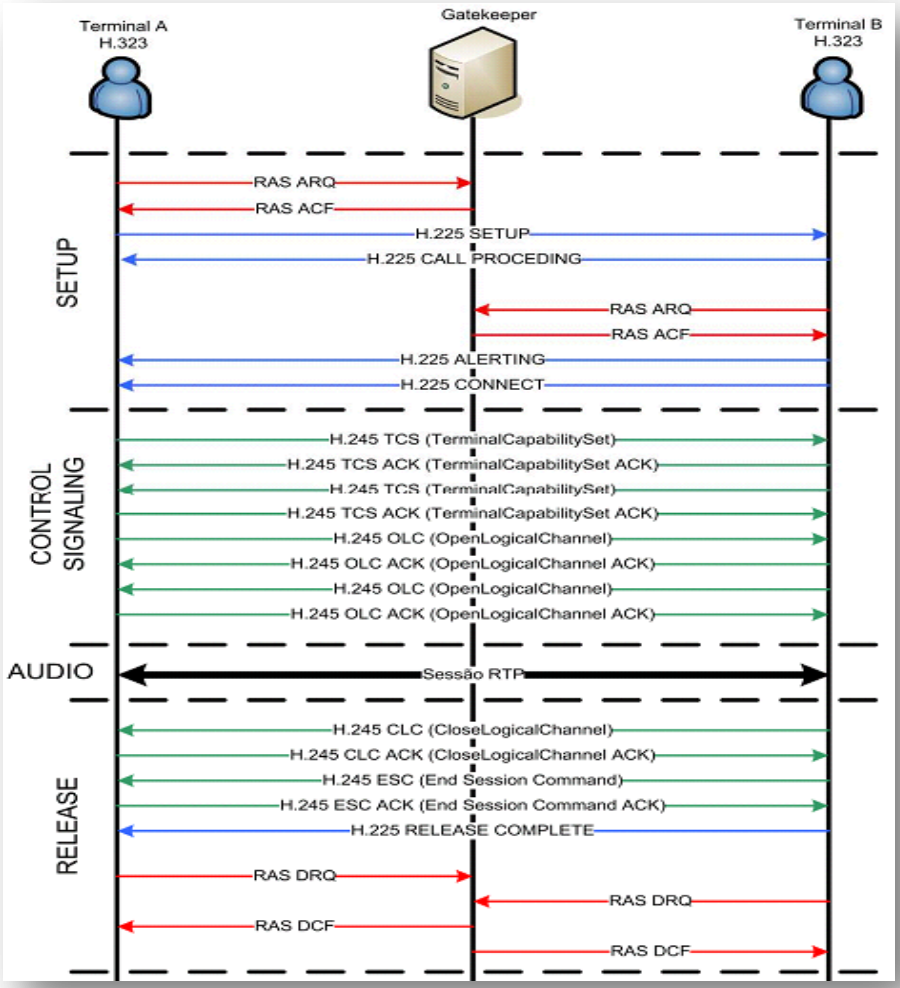



**Figura 22 – Exemplo de uma chamada H.323 [1].**

Descrição: Aqui será feita uma breve descrição das diferentes fases correspondentes à comunicação H.323:

1. *Setup*: Nesta primeira fase o terminal A irá enviar uma mensagem ARQ ao *gatekeeper* para efectuar o seu registo, usando o protocolo RAS. Em seguida, será enviando uma mensagem ACF pelo *gatekeeper* informando se o seu pedido foi aceite ou não. Seguidamente, o terminal A enviará uma mensagem de SETUP ao terminal B através do protocolo H.225, requisitando a conexão entre os respectivos terminais. Importa salientar que, nesta mensagem irá estar um conjunto de informações importantes sobre o endereço IP, porto e alias do remetente e o endereço IP, porto do destinatário. De seguida, o terminal B irá enviar uma mensagem *CALL PROCEEDING* ao terminal A, informando-o da tentativa de estabelecimento de uma chamada. A seguir, o terminal B irá efectuar o seu registo no *gatekeeper*. Depois será despoletado uma mensagem alertando o início da fase da geração do toque de aviso. Por último, será

enviada uma mensagem *CONNECT* que irá indicar que a ligação foi estabelecida.

2. *CONTROL SIGNALLING*: Esta fase, corresponde à fase da negociação efectuada através do protocolo H.245. Nesta fase, haverá muita troca de mensagens entre os respectivos terminais H.323, estabelecendo não só, quem será o *master* e quem será o *slave*, como também, gerir as capacidades dos participantes e os codecs de áudio e/ou vídeo que poderão ser eventualmente utilizados durante a sessão. Assim que terminar o processo de negociação será aberto um canal de comunicação atribuindo um endereço IP e o respectivo porto. Nesta etapa serão utilizadas as seguintes mensagens H.245:
    - TCS (*TerminalCapabilitySet*): esta mensagem indica a capacidade suportada pelos equipamentos H.323 que participam nas chamadas.
    - OLC (*OpenLogicalChannel*): esta mensagem será utilizada para efectuar a abertura do canal lógico que contém toda a informação necessária para facilitar a recepção e codificação dos dados. Nela está contida, algumas informações acerca do tipo de dados que irão ser enviados durante a comunicação.
3. AUDIO: Nesta fase ambos terminais H.323 poderão estabelecer uma comunicação usando o protocolo RTP/RTCP.
4. *CALL RELEASE*: Esta fase permite, quer o terminal A ou B inicializar o processo de finalização da chamada estabelecida, enviando as mensagens *CloseLogicalChannel* e *EndSessionComand,* respectivamente, para terminar a respectiva chamada, utilizando novamente o protocolo H.245. Seguidamente, usando a H.225, a ligação será encerada com o envio da mensagem *RELEASE COMPLETE*. Por último, será apagado todos os registos dos terminais existentes no *gatekeeper*, usando o protocolo RAS.

### *2.4.6. IAX – Inter Asterisk Exchange*

O protocolo IAX (*Inter-Asterisk Exchange*) é um protocolo que foi desenvolvido pela *Digium,* com o intuito de permitir o controlo e a transmissão de dados VoIP numa comunicação estabelecida entre servidores *Asterisk* (aplicação de IP-PBX).

O IAX é um protocolo de transporte tal como o SIP, mas apenas usa um único porto UDP, nomeadamente o 4569, para a sinalização e para o tráfego dos *streams* RTP. Devido à utilização desse único porto isto constitui uma grande vantagem em

relação aos restantes protocolos, visto que, tornará uma interoperação transparente entre o *Firewall* e a NAT (*Network Address Translation*). Actualmente, devido aos avanços tecnológicos, já se encontra disponível uma nova versão deste modelo no mercado, denominado por IAX2. Este novo modelo já está sendo utilizado, não só na comunicação entre servidores *Asterisk*, como também em telefones VoIP. Assim como existem telefones SIP existem também telefones IAX2.

Este protocolo tem como objectivos principais:

- A minimização da largura de banda usada no controlo e na transmissão de média, tendo em conta uma especial atenção nas chamadas de voz;
- A resolução de problemas relacionados com NAT, nomeadamente a transposição de redes LAN com NAT, bastante usuais no protocolo SIP;
- Permitir uma melhor capacidade de transmissão de informações relacionadas com planos de numeração (*dialplan*);

**Exemplo de Comunicação IAX**

Na seguinte figura, está ilustrada um exemplo de uma comunicação do protocolo IAX onde será feita uma breve descrição sobre as diversas transacções efectuadas ao longo da sessão estabelecida.

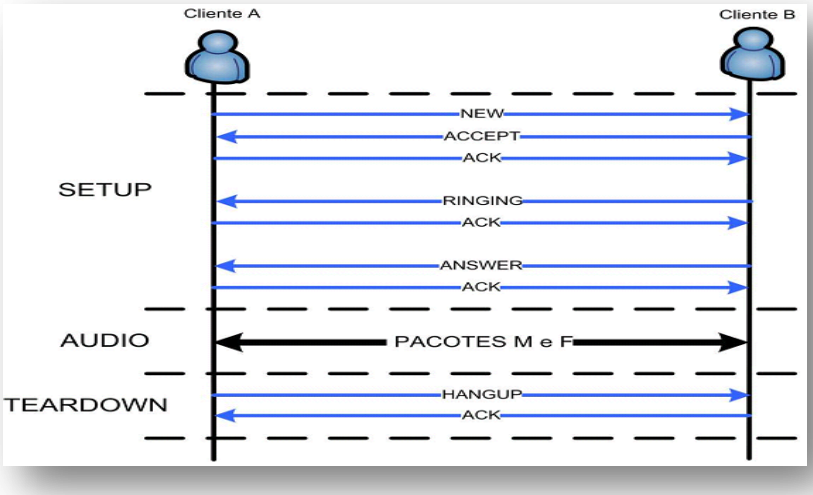



**Figura 23 – Exemplo de uma chamada IAX [1].**

Descrição: Aqui será feita uma breve descrição das diferentes fases correspondentes à comunicação do protocolo IAX:

1. *Setup*: Nesta primeira fase o cliente A irá enviar uma mensagem *NEW* ao cliente B para tentar estabelecer a conexão. Em seguida, o cliente B irá enviar

uma mensagem *ACCEPT*, indicando que aceitou o seu pedido. Seguidamente, o emissor enviará uma mensagem de resposta *ACK* ao destinatário. O cliente B por sua vez envia uma mensagem do tipo *RINGING* emitindo um sinal sonoro. A seguir, o cliente A irá enviar uma mensagem *ACK* para confirmar a recepção da referida mensagem. Por último, o cliente B enviará uma mensagem *ANSWER*, anunciando que aceita a chamada, obtendo de imediato uma resposta *ACK* do cliente A para que a ligação possa ser estabelecida.

2. Áudio: Esta fase é dedicada ao envio e trocas de pacotes do tipo M (*Mini-Frame*) e F (*Full-Frame*) respectivamente, contendo informação áudio. Cada fluxo de pacotes será composto por pacotes IAX do tipo M, contendo um cabeçalho de apenas 4 bytes o que irá permitir um aumento da eficiência na largura de banda.

3. *Teardown*: Nesta fase, quer o Cliente A ou B, poderá inicializar o processo de finalização da chamada estabelecida, enviando uma mensagem *HANGUP*, para terminar a respectiva chamada. Seguidamente, será enviada uma mensagem ACK para finalizar a ligação.

### *2.4.7. H.323 vs SIP*

Neste ponto, será apresentado um quadro comparativo contendo algumas semelhanças e as diferenças entre os protocolos SIP e H.323. Importa salientar que, embora haja um conjunto de características semelhantes entre os dois protocolos, eles diferem muito na filosofia.

| Assunto | H.323 | SIP |
|---|---|---|
| **Filosofia** | O H323 é um protocolo desenvolvido pela ITU-T que define um conjunto de protocolos para o fornecimento de comunicação de áudio e vídeo numa rede de computadores. O H.323 é um standard pesado, típico da indústria dos telefones, especificando a pilha de protocolos completa e definindo com precisão o que é permitido e o que é proibido. O H323 é um protocolo relativamente antigo que está actualmente sendo substituído pelo SIP. | O SIP é um protocolo de sinalização de telefonia IP, desenvolvido pela IETF que permite ao utilizador final estabelecer, modificar e finalizar chamadas telefónicas VoIP. O SIP se assemelha ao HTTP, é baseado em texto, e é bastante aberto e flexível em relação ao padrão H323. |
| **Arquitectura** | Monolítica | Modular |

| Componentes | Terminal/Gateway | UA |
|---|---|---|
| | Gatekeeper | Servidores |
| Protocolos | RAS/Q.931 | SIP |
| | H.245 | SDP |
| **Controlo de funcionalidades das chamadas** | | |
| Transferência de chamadas | Sim | Sim |
| Encaminhamento de chamadas | Sim | Sim |
| Chamadas em espera | Sim | Sim |
| Call Parking/Pickup | Sim | Sim |
| Sinalização de mensagens | Sim | Não |
| Identificação de Nome | Sim | Não |
| Oferta de chamadas | Sim | Não |
| Chamadas inesperadas | Sim | Não |
| **Funcionalidades Avançadas** | | |
| Sinalização *Multicast* | Sim, através de LRQ (*location requests*) e GRQ (*auto gatekeeper discovery*). | Sim, através de *group INVITEs*. |
| Controlo de 3 chamadas. | Sim | Sim |
| Negociação de parâmetros | Sim | Sim |
| **Escalabilidade** | | |
| Uso de grandes quantidades de servidores. | Sim | Sim |
| Manipulação de grandes quantidades de chamadas. | Sim | Sim |
| Modo de conexão | *Stateful* ou *Stateless*. | *Stateful* ou *Stateless*. |
| Internacionalização | Sim, usa *Unicode* (*BMPString* dentro ASN.1) para algumas informações textuais (h323-id), mas geralmente tem alguns parâmetros textuais. | Sim, usa *Unicode* (ISO 10646-1), codificados como UTF-8, para todos caracteres. |
| **Segurança** | | |
| Autenticação/ Encriptação | Sim, via H.235 (SRTP, TLS, IPSec, etc.). | Sim, via HTTP (*Digest and Basic*), SSL, PGP, S/MIME. |
| Interoperabilidade | Alargada | Alargada |
| **Protocolo de transporte** | UDP ou TCP | UDP ou TCP |
| Codificação de mensagens | Binário | ASCII |
| **Modo de endereçamento** | Endereço URL e números E.164. | Endereço URL. |
| **Conferências Multimédia** | Sim | Não |
| **Nº de portos usados numa videoconferência** | 3 (Sinalização de chamadas, RTP, e RTCP.) | 3 (SIP, RTP, e RTCP.) |

**Tabela 11 – Quadro resumo contendo uma análise comparativa entre H.323 e SIP.**

## 2.5. *Codecs utilizados na tecnologia VoIP*

Neste ponto será apresentado um quadro resumo contendo os principais codificadores utilizados na tecnologia VoIP.

| Codecs | Algoritmo | Frequência de Amostragem (KHZ) | Ritmo Binário (Kb/s) | Atraso Algorítmico (ms) | Mean Opinion Score | Processamento (MIPS) |
|---|---|---|---|---|---|---|
| G.711 | PCM | 8 | 64 | 0.125 | 4.3 | 0.01 |
| G.722 | ADPCM | 16 | 48/56/64 | 0.125 | 4.1 | 5 |
| G.722.1 | Siren7 | 16 | 24/32 | 40 | -- | -- |
| G.723.1 | ACELP | 16 | 5.3/6.3 | 37.5 | 3.8 | 16 |
| G.726 | ADPCM | 8 | 16/24/32/40 | 0.125 | 4.0 (a 32 kbit/s) | 10 |
| G.728 | LD_CELP | 8 | 16 | 0.625 | 3.9 | 30 |
| G.729A | ACELP | 8 | 8 | 15 | 4.0 | 20 |
| GSM-FR | RPE-LTP | 8 | 13 | 20 | 3.5-3.9 | 5-6 |
| GSM-EFR | ACELP | 8 | 12.2 | 20 | 3.8 | -- |
| GSM-AMR | ACELP e outras | 8 | 4.75-12.2 | 20-25 | 4 (a 12.2 kbit/s) | -- |
| iLBC | LPC | 8 | 13.33/15.2 | 20-30 | 4.14 | 20 |
| Speex | CELP | 8/16/32 | 2.15-24.6 | 30 | -- | -- |

**Tabela 12 – Principais codecs utilizados na tecnologia VoIP.**

## 2.6. *Exemplos de equipamentos da tecnologia VoIP*

Neste ponto será apresentado não só um conjunto de equipamentos da tecnologia VoIP existentes no mercado empresarial, como também, algumas soluções *Open Source* de aplicações VoIP, que futuramente poderão minimizar o custo de implementação da referida tecnologia nas empresas e/ou instituições públicas.

De entre esses equipamentos destacam-se os seguintes: os terminais (*hardphones, softphones*, a placa de ligação à rede PSTN, etc.), os *gateways* e as aplicações de gestão de serviços de telefonia VoIP (servidores SIP e de IP-PBX, etc.).

### *2.6.1. Terminais VoiP*

Os terminais VoIP são equipamentos que permitem estabelecer uma interligação de infra-estruturas necessárias ao transporte do tráfego de dados e voz dentro de uma determinada rede e num ambiente convergente, integrado e seguro.

Após essa conexão de infra-estruturas o utilizador poderá estabelecer uma comunicação bidireccional em tempo real com outro terminal VoIP, permitindo assim uma maior produtividade e disponibilização de ferramentas de colaboração entre várias empresas e/ou instituições públicas.

A seguir será apresentado um conjunto de exemplos de terminais utilizados no processo de comunicação VoIP.

#### *2.6.1.1.Telefones IP – Hardphones*

Os telefones IP têm algumas semelhanças e diferenças relativamente aos telefones vulgares. Essa diferença deve-se ao facto que, invés de possuir cabos e ligações telefónicos num formato padrão RJ-11 (RITA) ou RDIS, os telefones IP possuem cabos de ligações em formato *RJ-45 Ethernet*.

Estes equipamentos permitem ao utilizador final estabelecer uma conexão directa não só a partir da sua rede pessoal, como também, nas instituições públicas e/ou empresa.

Os telefones IP possuem um conjunto de *hardware* e *software* integrados, que permitem efectuar chamadas de videoconferências entre vários utilizadores. Actualmente graças ao avanço tecnológico já estão disponíveis no mercado empresarial, alguns modelos avançados dos telefones IP, tais como, o telefone IP *Wi-Fi* ou DECT.

No que diz respeito ao mundo empresarial, estes equipamentos estão interligados num servidor VoIP, desempenhando assim o papel de uma central telefónica munida com um conjunto de funcionalidades avançadas que permitem uma melhor comunicação entre as empresas.

Seguidamente, serão apresentadas algumas funcionalidades extras dos *Hardphones* durante uma comunicação VoIP. Os *Hardphones* permitem:

- Chamadas de videoconferência: esta funcionalidade permite efectuar chamadas de vídeo entre dois terminais VoIP. Actualmente, está funcionalidade está sendo muito utilizada em sessões de videoconferência nas instituições judiciais, de ensino e de saúde.
- Encaminhamento de chamadas: permite ao utilizador encaminhar uma determinada chamada, mesmo estando com uma outra chamada previamente estabelecida, através de teclas especiais para o efeito.
- Atendimento de uma 2ª chamada: tendo uma chamada em curso, pode atender uma nova chamada seleccionando a respectiva tecla de linha. Pode voltar à anterior seleccionando a sua respectiva tecla de linha e ir comutando entre elas.
- Colocar chamadas em espera: permite ao utilizador colocar um ou mais chamadas, mesmo estando com uma outra chamada previamente estabelecida, através de teclas especiais para o efeito.
- Sinalização de mensagens: esta funcionalidade permite visualizar uma mensagem de *voice mail* através de um sinal sonoro ou visual.

- Identificação de Nome: esta funcionalidade permite não só identificar as chamadas recebidas ou efectuadas, como também, indicar alguma informação sobre a data, a hora e pessoa que realizou a respectiva chamada.

A seguir será apresentado um quadro comparativo contendo alguns modelos de telefones IP presentes no mercado quer ao nível básico, empresarial e/ou executivo.

| Modelos de telefones IP | |
|---|---|
| **Modelo Básico** | **Funcionalidades** |
|  **Cisco IP Phone 524G** | – O telefone IP 524G da Cisco é um modelo inicial e de baixo custo. – É um telefone que possui quatro linhas com acesso para até oito chamadas. – Utiliza o *Power-over-Ethernet* ou um adaptador de força opcional, em modo *sleep* para economizar a energia quando não estiver em uso. – Única porta 10/100 PoE (802.3af). – Possui visores monocromáticos com luz de fundo e toques ajustáveis pelo usuário. |
|  **Cisco IP Phone 7931G** | – O telefone IP 7931G possui um conjunto de teclas especiais que permitem colocar uma chamada em espera, efectuar a remarcação e transferência de chamadas para simplificar e acelerar o processamento de chamadas. – Este modelo não requer qualquer cabo de alimentação. – Possui ainda, LEDs a cores que permitem indicar o estado da chamada em linha e teclas de colocação de chamada em espera, transferência de chamadas e remarcação dedicadas. – O referido modelo permite ainda uma integração com o Cisco *Unified Communications Manager* e o *Cisco Unified Communications Manager Express.* |
|  **Cisco IP Phone 7921G** | – O telefone IP 7921G é um telefone *wireless* que permite uma maior mobilidade aos utilizadores finais. – Este modelo possui uma qualidade de voz excepcional, uma elevada durabilidade e um ecrã a cores de grandes dimensões contendo 2 polegadas. – Este telefone suporta um carregamento com alta-voz e possui um conjunto de teclas especiais para controlo de volume podendo deste modo o utilizador aumentar ou diminuir o volume durante a ligação. – Possui ainda uma autonomia de 12 horas de tempo de conversação e 100 horas de tempo de espera. – Este modelo oferece funções de segurança de voz integradas. |

**Tabela 13 – Modelos básicos de telefones IP existentes no mercado VoIP [31].**

| Modelos de telefones IP | |
|---|---|
| **Modelo Empresarial** | **Funcionalidades** |
|  **Polycom SoundPoint IP650** | – O modelo SoundPoint IP650 da Polycom, possui um conjunto de 6 linhas que poderão ser expandido com o módulo de expansão para 12 linhas permitindo deste modo efectuar várias chamadas em simultâneo. – Possui um LCD grayscale 320 x 160 pixel, um sistema de voz em alta definição (HD Voice). – O referido modelo contém outras funcionalidades avançadas, tais como, a gestão avançada de chamadas, segurança e presença. – O SoundPoint IP650 possui dois portos *Ethernet switched* 10/100 Mbps, um POE IEEE 802.3af incorporado e suporte ao protocolo SIP. |
|  **Cisco IP Phone 7941G-GE** | – O telefone IP 7941G-GE da Cisco possui um ecrã de alta resolução para aplicações avançadas. – Este modelo foi concebido para acomodar aplicações de alto desempenho e não requer qualquer tipo de ligação por cabo de alimentação. – Possui ainda, o acesso a duas linhas telefónicas (ou combinação de acesso a linha telefónica e funcionalidades de telefonia) |

**Tabela 14 – Modelos empresarial de telefones IP existentes no mercado VoIP [31].**

| Modelos de telefones IP | |
|---|---|
| **Modelo Executivo** | **Funcionalidades** |
|  **Cisco IP Phone 7970G** | – O telefone IP 7970G da Cisco possui um ecrã *touch-screen* de alta resolução para aplicações avançadas. – Contém sistema de alta-voz incorporada e ligações para auscultadores. – Este modelo não requer qualquer cabo de alimentação e tem acesso a oito linhas telefónicas (ou combinação de acesso a linha telefónica e funcionalidades de telefonia). |
|  **Cisco IP Phone 7985G** | – O modelo 7985G da Cisco possibilita uma integração de todos os componentes necessários para efectuar chamadas de vídeo-conferência, tais como, ecrã LCD, altifalante, teclado e auscultadores, numa única unidade. – Este telefone IP contém um conjunto de teclas especiais que controlam funções de vídeo, tais como *"picture-in-picture"*; vista dos funcionários; controlo do silêncio, ecrã e luminosidade. – Este modelo foi concebido para acomodar aplicações de alto desempenho. |

**Tabela 15 – Modelos executivos de telefones IP existentes no mercado VoIP [31].**

#### *2.6.1.2.Telefones IP – Softphones*

Um *softphone* é uma aplicação que poderá não só ser instalado num computador pessoal, como também, configurado de modo a permitir estabelecer chamadas entre dois terminais VoIP através da internet e a custo zero. Estes programas são geralmente de uso gratuito e poderão ser utilizados para simular um adaptador analógico ATA ou Telefone IP.

Contudo, esses equipamentos possuem algumas limitações relativamente à qualidade das chamadas, visto que, é muitas vezes insuficiente. A instabilidade do sistema também constitui uma das principais desvantagens na utilização dessas aplicações e consequentemente provoca uma redução no seu uso para o mercado caseiro.

Mas contudo, devido ao facto de que essas aplicações são produto de *Open Source*, actualmente está aparecendo um conjunto de bibliotecas avançadas que estão associadas a diversas linguagens de programação, permitindo assim deste modo uma rápida implementação desses programas.

Entretanto importar salientar que, existem também versões profissionais de *softphones* que são muito competentes, mas claro, dispendiosas em termos de custos.


**Figura 24 – *Softphones X-Lite*.**

A seguir será apresentado um quadro comparativo contendo alguns modelos de *sotfphones* presentes no mercado quer ao nível básico, empresarial e/ou executivo.

| Modelos de Softphones | | | | |
|---|---|---|---|---|
| **Modelos** | **Sistemas Operativos** | | | **Funcionalidades** |
| | **Windows** | **Linux** | **MacOS X** | |
|  **X-Lite** | Sim | Sim | Sim | – *Open Standards* cliente com a próxima geração de telefonia. – Usa o SIP com sinalização em todas as sessões de multimédia. – Possui uma boa qualidade de serviço (QoS) para chamadas de voz e vídeo. – Contém uma lista personalizada de endereços e um historial detalhado chamadas. – Contém uma configuração *Zero-Touch* dos dispositivos de áudio ou vídeo. – Integração com o Microsoft Outlook, permitindo aos utilizadores importar todos os seus contactos pessoais. – IM e gestão de presença. – Permite efectuar ligações de voz em modo *Ad-Hoc e* vídeo-conferência [IP & PSTN]. – Permite gravação de chamadas de Voz e Vídeo. |
|  **Zoiper** | Sim | Sim | Sim | – Usa os protocolos SIP, IAX / IAX 2. – Integração com o Microsoft Outlook. – Permite dar respostas automática, encaminhar e transferir chamadas de uma forma intuitiva. – Estabelecer chamadas de videoconferência entre vários utilizadores. – Integra programas para imprimir e enviar fax de qualquer aplicação de Windows. – Escalabilidade e flexibilidade na utilização e criação de contas de utilizadores. – Permite efectuar chamadas de vídeo com alta definição. – Possui alta qualidade de codecs áudio, permitindo obter uma alta qualidade de transmissão com uma menor largura de banda. |
|  **Skype** | Sim | Sim | Sim | – Usa o protocolo SIP. – Integração com o Microsoft Outlook. – Possui uma boa qualidade de serviço (QoS) para chamadas de voz e vídeo. – Contém uma lista personalizada de endereços e um historial detalhado chamadas. – Permite dar respostas automática, encaminhar e transferir chamadas de uma forma intuitiva. – Estabelecer chamadas de videoconferência entre vários utilizadores. – Envio de mensagens instantâneas. |

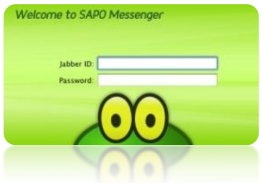
| | | | | |
|---|---|---|---|---|
|  **SJPhone** | Sim | Sim | Sim | – SJphone permite efectuar ligações com qualquer terminal VoIP, usando o seu *gateway* de VOIP ou provedores de serviços de internet. – Suporta os protocolos SIP e os padrões H.323. – É totalmente interoperável com os mais importantes fornecedores de telefonia IP e ITSP. |
|  **SIP Communicator** | Sim | Sim | Sim | – Usa os protocolos *SIP*, *SIMPLE*, *XMPP*, *Jabber*, *AIM/ICQ*, *MSN*, *Yahoo! Messenger*, *Bonjour, IRC, RSS.* – Permite estabelecer chamadas de videoconferência entre vários utilizadores. – Envio e recepção de mensagens instantâneas. – Possui o endereço básico de IPv6. |
|  **Gtalk** | Sim | Não | Não | – Usa os protocolos XMPP. – Permite estabelecer chamadas de videoconferência, chats entre vários utilizadores. – Permite transferências de ficheiros e integra serviços de *voicemail*, E-mail via *GMail.* – Interoperabilidade entre equipamentos móveis, tais como, PDA's, *smartphones*, etc. |
|  **Windows Live Messenger** | Sim | Não | Não | – Usa os protocolos MSNP, TCP e HTTP. – Permite estabelecer chamadas de videoconferência, chats entre vários utilizadores. – Permite transferências de ficheiros e integra serviços de *voicemail*, E-mail via *Hotmail.* – Interoperabilidade entre determinados equipamentos móveis. – Envio de mensagens instantâneas para terminais VoiP. |
|  **Yahoo Messenger** | Sim | Sim | Sim | – Usa os protocolos SIP (através de TLS) e RTP (média). – Permite transferências de ficheiros e integra serviços de *voicemail*, E-mail via *Yahoo Mail.* – Interoperabilidade entre vários equipamentos móveis. – Envio e recepção de mensagens instantâneas para terminais VoiP. |
|  **Sapo Messenger** | Sim | Não | Não | – Usa os protocolos *XMPP*, *Jabber*, *AIM/ICQ*, etc. – Permite estabelecer chamadas de videoconferência entre vários utilizadores. – Envio e recepção de mensagens instantâneas. – Permite transferências de ficheiros e integra serviços de *voicemail*, E-mail via *Sapo Mail.* |

**Tabela 16 – Exemplo de *softphones* existentes no mercado da telefonia VoIP.**

### *2.6.2. Placas de ligação à rede PSTN*

Este equipamento é um *hardware* específico que permite estabelecer uma ligação entre duas redes, nomeadamente a rede IP e uma rede PSTN, respectivamente. De entre este equipamento destacam-se três tipos de placas tais como: a de ligação entre a rede IP e PSTN, a de ligação entre a rede IP e PRI, e por ultimo a de ligação da rede IP para ISDN (RDIS).

Relativamente à conexão entre a rede IP à rede PSTN, é feita através das placas de ligação, FXS e FXO, respectivamente. Estas placas são as portas usadas por linhas de telefonia analógica (também conhecidas por POTS – Sistema de Telefonia Tradicional). A porta FXS (*Foreign eXchange Subscriber*) corresponde à interface que fornece a linha analógica ao assinante, enquanto, a FXO (*Foreign eXchange Office*) é a interface que recebe a linha analógica.

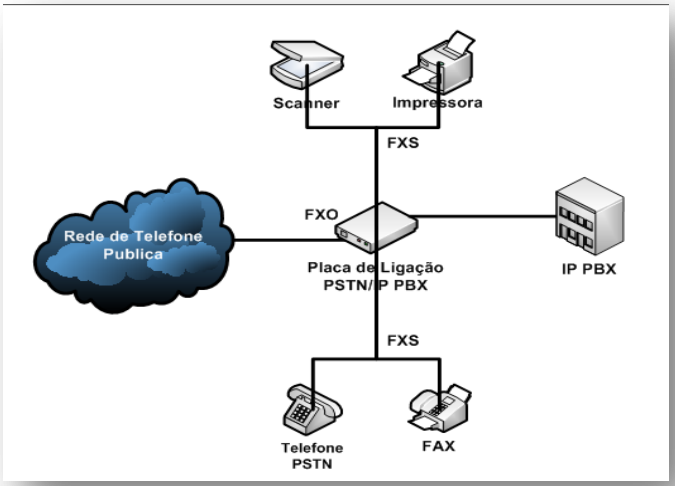



**Figura 25 – Placas de Ligação à rede PSTN.**

### *2.6.3. Gateway/Gatekeepers VoIP*

Um *gateway* VoIP tem como objectivo principal efectuar a tradução entre as redes de VoIP e PSTN. Obtenção de um gateway VoIP é necessário para se juntar e traduzir híbrido de redes de telefonia sem problemas. Um *gateway* VoIP converte o tráfego TDM de *Public Switched Telephone Network* (PSTN) ou em H.323 ou *Session Initiation Protocol* (SIP) com base no tráfego de VoIP. Considerado como sendo terminais inteligentes, os gateways podem fornecer facturação, alarmante, built-in de resposta de voz interactiva (IVR), encaminhamento de pacotes, manipulação de dígitos, e segurança.

Um *gateway* VoIP poderá ser designado não só como sendo um Media *Gateway*, como também, um *SoftSwitch*, *Media Gateway Controller*, *SIP Server* ou qualquer outro dispositivo que processa dados de VoIP e sinalização de tráfego.

Os *gateways* VoIP permitem que sejam efectuadas chamadas entre terminais que normalmente não poderiam inter-operar (SIP/ISDN, IPv4/IPv6, diferentes sistemas de codificação de voz). Os *gateways* mais utilizados são os que ligam telefones IP aos telefones tradicionais (comutação de circuitos). *Gatekeepers* são responsáveis pela admissão de chamadas e controlo de largura de banda.

### *2.6.4. Aplicações de gestão de serviços de telefonia VoIP*

Neste ponto, serão apresentados alguns exemplos de aplicações *Open Source* de gestão de serviços de telefonia VoIP existentes no mercado que são elementos considerados fundamentais numa solução VoIP, tais como, servidores SIP, servidores IP- PBX, *media relays*, portal de interacção, ferramenta AAA e ferramenta de contabilização e facturação de chamadas.

#### *2.6.4.1.IP PBX*

Um sistema IP-PBX é um sistema de transferência de chamadas telefónicas, que redireccionam as chamadas numa rede de comunicações IP para utilizadores internos e disponibilizam acesso a linhas exteriores. Tipicamente, um IP-PBX permite ainda a transferência de chamadas telefónicas entre utilizadores VoIP e indivíduos que utilizam os sistemas telefónicos tradicionais. Estes produtos são normalmente aplicações de *software* que são executadas num servidor ou em equipamentos dedicados.

Os sistemas IP-PBX eliminam a necessidade de uma rede de comunicações de voz separada, permitindo o tráfego de dados e de voz na mesma rede de comunicações. Estes produtos disponibilizam uma variedade de funcionalidades de chamadas telefónicas, tais como sistemas de menu de voz, conferência de chamadas, '*click-to-call*', registo de chamadas e localização, caixas de correio de voz e reencaminhamento.

Através dos seus sistemas de IP-PBX, as organizações podem escolher utilizar *softphones* – aplicações de telefones IP que funcionam nos computadores pessoais dos utilizadores – ou telefones tradicionais desenhados para funcionar em redes IP. As principais funcionalidades de um IP PBX são semelhantes às de um vulgar PABX (*Private Automatic Branch eXchange*). No entanto, além das funcionalidades básicas de PABX, o IP PBX apresenta inúmeras funcionalidades só

exequíveis devido à enorme flexibilidade proporcionada pelo facto de este ser desenvolvido em *software*.

A seguir estão apresentadas algumas dessas funcionalidades básicas relativamente ao PABX:

- A possibilidade de interligação vários telefones de uma organização;
- A capacidade de efectuar uma série de ligação dos telefones da organização ao exterior (outras redes);

Entretanto, importa salientar que, para além das referidas funcionalidades, a maior parte dos serviços de IP PBX apresentam também as seguintes funcionalidades extras:

- Um conjunto de menus interactivos, que permitem ao utilizador final escolher de opções pretendidas através da digitação de números;
- O serviço de V*oice Mail* que permite-lhe receber mensagens de voz sempre que o seu equipamento móvel ou fixo se encontrar sem cobertura, quando estiver desligado ou quando não puder atender uma chamada. Permite ainda efectuar a gravação das mensagens de voz;
- O reencaminhamento e a gravação de chamadas: este serviço de permite-lhe reencaminhar as chamadas dirigidas ao seu equipamento fixo ou móvel para outro equipamento de outras redes (como por exemplo em Portugal ou no Estrangeiro). Saliento que, sempre que não é possível atender, ou não deseja ser incomodado, o utilizador poderá a qualquer momento reencaminhar as chamadas para o *Voice Mail* e consultá-las mais tarde.
- *Waiting ring:* este serviço permite ao utilizador personalizar o seu equipamento com uma música em espera (*music-on-hold*) caso estiver ocupado e não puder atender uma chamada no exacto momento;
- A definição de rotas para as chamadas, isto é, caso uma chamada não for atendida em determinado telefone, a chamada deverá passar para o telefone seguinte pré-definido e assim sucessivamente;
- A possibilidade de efectuar um registo em base de dados de todos os detalhes das chamadas efectuadas e/ou recebidas entre dois equipamentos (data/hora, duração, nº destino, etc);
- O serviço de vídeo-conferência, que permite ao utilizador final estabelecer uma chamada vídeo entre um ou vários telefones;

- Apresenta ainda uma funcionalidade de envio das mensagens recebidas directamente para a caixa de correio;

Importa salientar ainda que, caso for necessário utilizador, poderá ainda personalizar o seu sistema de IP PBX, com um conjunto de funcionalidades extras, mediante uma implementação personalizada através da utilização de várias linguagens de programação.

Actualmente existem vários equipamentos que oferecem ao utilizador final vários sistemas *Open Source* ou de distribuição gratuita de IP PBX, sendo que, a maior parte deles são financiadas pelas empresas multinacionais ligadas ao ramo das telecomunicações, cuja base do seu negócio é a implementação, a instalação e manutenção destes sistemas. A seguir será apresentado um quadro comparativo contendo alguns exemplos de sistemas *Open Source* de IP PBX tais como:

| Modelos de sistemas IP PBX | | | | | |
|---|---|---|---|---|---|
| **Modelos** | **Sistemas Operativos** | **Licença** | **Protocolos** | **Encriptação** | **Outros recursos** |
| **3CX Phone System** | Windows XP, 2000, 2003. | Freeware / Software Proprietary | SIP | | IP PBX |
| **Asterisk** | Linux for PPC, OpenBSD, FreeBSD, Mac OS X Jaguar. | GPL free software / Proprietary | SIP, H.323, Inter-Asterisk eXchange | | |
| **sipX ECS** | Linux | Open Source LGPL | Native SIP Call Control | HTTPS, TLS | Full redundancy (HA), plug & play management including phones and gateways, fully featured, 100% SIP standards based |
| **OpenSER** | Linux, BSD, Solaris | GPL free software, Open Source | SIP | TLS | ENUM, IM, XMPP IM gateway, SMS gateway |
| **GNU Gatekeeper** | Linux, Mac OS X, Windows XP/2000, | GPL Free software | H.323 | | Routing, Accounting, |

| | | | | | |
|---|---|---|---|---|---|
| | FreeBSD | | | | AUthorization |

**Tabela 17 – Alguns exemplos de modelos de sistemas IP PBX existentes no mercado.**

A seguir, será feito uma breve descrição sobre dois sistemas *Open Source* de IP PBX, tais como, o *Asterisk*, *Tribox* e o *Elastix*, abordando os seguintes aspectos: as suas características e funcionalidades básicas, a arquitectura e os requisitos mínimos de implementação de ambos os sistemas.

#### *2.6.4.1.1. Asterisk*

O *Asterisk*, que é um *software Open Source* e gratuito para Linux, desenvolvido em 1999 por *Mark Spencer*. Este *software* é licenciado através de uma licença do tipo GPL - *GNU Public License*.

Inicialmente, este sistema IP PBX foi implementado para funcionar apenas no sistema operativo Linux, mas actualmente, existem várias versões desenvolvidas que permitem funcionar no *OpenBSD, FreeBSD, Mac OS X, e Sun Solaris*.

Contudo, a empresa multinacional designada por *Will Voice*, desenvolveu uma versão do *software* para Windows, mas porém, não faz parte do programa criado pela *Digium*, sendo que a referida empresa apenas criou uma versão para Windows e a distribui gratuitamente, oferecendo também um conjunto de suportes de actualizações para as respectivas versões.

Entretanto, devido à natureza do *software* livre e ao facto de que vários programadores têm contribuído para o seu desenvolvimento sistemático e de uma forma eficaz, este sistema de IP PBX está recentemente na versão 1.6.2.

Actualmente, a empresa que promove o *Asterisk*, nomeadamente a *Digium*, está a efectuar uma série de investimentos não só, ao nível do desenvolvimento tecnológico de *software* baseado na filosofia *Open Source*, como também, ao nível de *hardware* de telefonia de baixo custo que permitem a integração e a migração gradual entre os sistemas já existentes e vários equipamentos da tecnologia VoIP com o *Asterisk*. Este *software* apresenta não só, todas as funcionalidades de um PBX (*Private Branch eXchange*) tradicional, bem como, outras funcionalidades adicionais como o IVR (*Interactive Voice Response*).

Este *software* é um sistema de PBX VoIP que permite suportar um conjunto de protocolos utilizados em VoIP, tais como, o SIP, SCCP, H.323, IAX2, etc. Este programa irá permitir ao utilizador a possibilidade de utilizar telefones em *software* como dispositivos telefónicos VoIP, sendo também possível inter-operar com os

sistemas de telefonia tradicionais, sendo neste caso necessário *hardware* adicional. Neste projecto, o referido sistema de IP PBX, irá funcionar não só, como um *gateway* entre o sistema VoIP e a rede PSTN, como também um servidor de correio de voz e de reencaminhamento de chamadas.

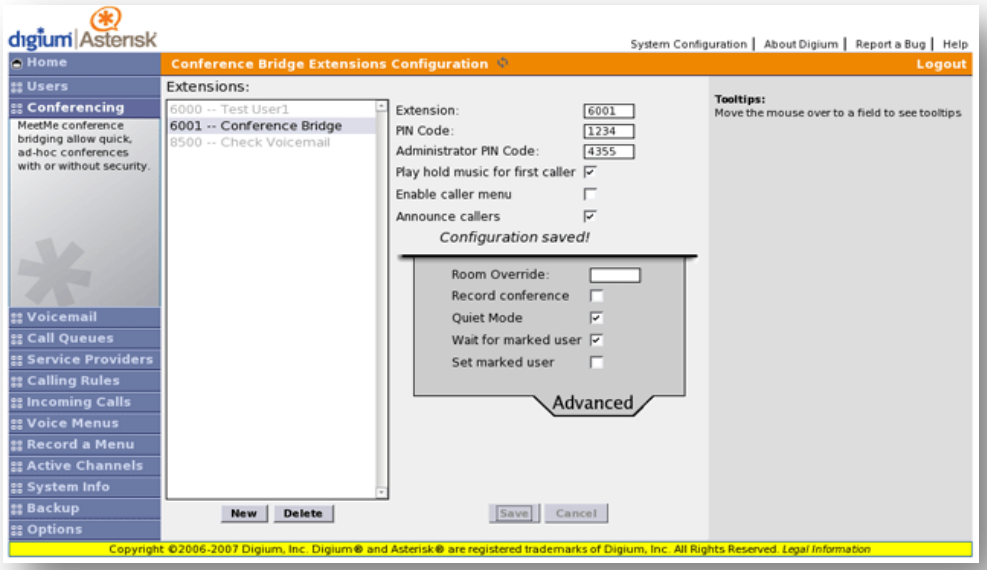



**Figura 26 – Plataforma Web Asterisk [52].**

### Funcionalidades e características do sistema PBX *Asterisk*

- Sistema de telefonia IP-PBX: esta funcionalidade permite efectuar a transferência de chamadas telefónicas entre utilizadores VoIP e indivíduos que utilizam os sistemas telefónicos PTSN;
- Serviços de encaminhamento automático de chamadas: este sistema permite ao utilizador final, não só receber uma chamada telefónica e verificar os atributos da mesma, como também, tomar decisões sobre o seu respectivo encaminhamento com base no seu conteúdo. Importa salientar que, existem vários exemplos de encaminhamento de uma chamada, visto que, podem ser enviadas para uma extensão única ou um grupo de extensões, para o sistema de gravação de chamadas, entre outros;
- Sistemas IVR (*Interactive Voice Response*): esta funcionalidade permite que o atendimento de chamadas seja programado de forma flexível, de modo a dar algum tipo de resposta às mesmas sem interacção humana, sendo que será o emissor da chamada a escolher uma das opções que lhe são expostas. Este sistema reproduz ficheiros áudio e em formato texto permitindo ao utilizador verificar toda a informação a partir de uma base de

dados. Esta funcionalidade permite ainda, seleccionar teclas do telefone para interagir com sistema, por exemplo, um sistema de votação electrónica via telefone, ou aceder a uma conta no banco, inserindo o número de conta e palavra secreta através do teclado, seguindo todas as instruções do sistema telefónico;

- Sistema de correio de voz com integração com o correio electrónico: Esta funcionalidade suporta vários contextos que permitem hospedar múltiplas entidades no mesmo servidor. Suporta ainda, diferentes fusos horários permitindo aos utilizadores perceber quando as chamadas chegaram ao *voice mail*. Através a integração com o correio electrónico, existe também, uma possibilidade de notificar o destinatário sobre uma nova mensagem de voz por e-mail, com a possibilidade de anexar a mensagem áudio gravada;
- Serviço de relatório e estatísticas das chamadas: esta funcionalidade permite ao sistema *PBX Asterisk* manter o registo completo e detalhado de todas as chamadas, sendo que esta informação poderá ser guardada num ficheiro em formato flat, ou em base de dados permitindo uma apresentação mais formatada e com maior facilidade de análise. Saliento que, a partir desta informação poderá ser monitorizado a utilização do *Asterisk*, podendo por vezes ter a possibilidade de detectar padrões ou anomalias;
- Facilidade de administração e gestão através de portais *Web*: com esta funcionalidade o utilizador poderá ter não só, uma melhor capacidade de gestão e organização de todas informações relativamente às chamadas recebidas e/ou efectuadas através deste sistema de PBX, como também, um melhor desempenho nas suas funções face ao seu ambiente profissional;
- *SIP Proxy* limitado: o sistema *PBX Asterisk* permite efectuar e receber chamadas SIP. Com já foi citado anteriormente no capítulo 2.4.1, no protocolo SIP, os dispositivos são registados num servidor SIP, permitindo deste modo aos dispositivos de localizarem-se mutuamente para estabelecer comunicações. Contudo, quando um número elevado de dispositivos SIP é utilizado, será implementado de imediato um *proxy SIP* de forma a permitir uma melhor gestão e manipulação dos registos e conexões de forma eficiente. Importa salientar que, o sistema *PBX Asterisk*, não actua como *SIP Proxy*. Entretanto, os dispositivos SIP poderão ser

registados com o *Asterisk*, mas contudo, caso houver um aumento do número de dispositivos SIP, o referido sistema não escalará os respectivos dispositivos de uma forma conveniente. Por exemplo, para um sistema com cerca de 100 dispositivos SIP, o *Asterisk* não será apropriado. O *Asterisk* pode ser configurado para utilizar um proxy para registos. Para solucionar esta limitação poderá ser utilizado o SER (*SIP Express Router*) que é um *proxy* SIP *Open Source* e gratuito, que permite ao utilizador configurar o sistema *PBX Asterisk* conforme as suas necessidades, escalando-o modo a poder suportar instalações de larga escala.

- Possibilidade de integração de sistemas PBX's analógicos com sistemas contendo novas tecnologias VoIP;
- Possibilidade de migração dos sistemas PBX's analógicos para os sistemas de IP PBX;
- Sistema voltado para pequenas e médias empresas.

**Arquitectura do sistema PBX *Asterisk***

O *Asterisk* foi implementado de uma forma cautelosa de modo a suportar uma máxima flexibilidade. O sistema PBX *Asterisk* é constituído por um conjunto de APIs específicos que constituem um avançado sistema de núcleo central PBX. O referido núcleo suporta a interligação interna da PBX, de uma forma distinta e abstracta dos protocolos específicos, codecs, e interfaces de *hardware* das aplicações de telefonia. Contudo, isto permite o *Asterisk* a usar qualquer *hardware* adequado e da tecnologia disponível agora ou no futuro para realizar suas funções essenciais – a conexão entre o *hardware* e aplicativos.

Na figura a seguir, está ilustrada um exemplo de uma arquitectura básica do sistema *PBX Asterisk*, apresentando os componentes principais da mesma.

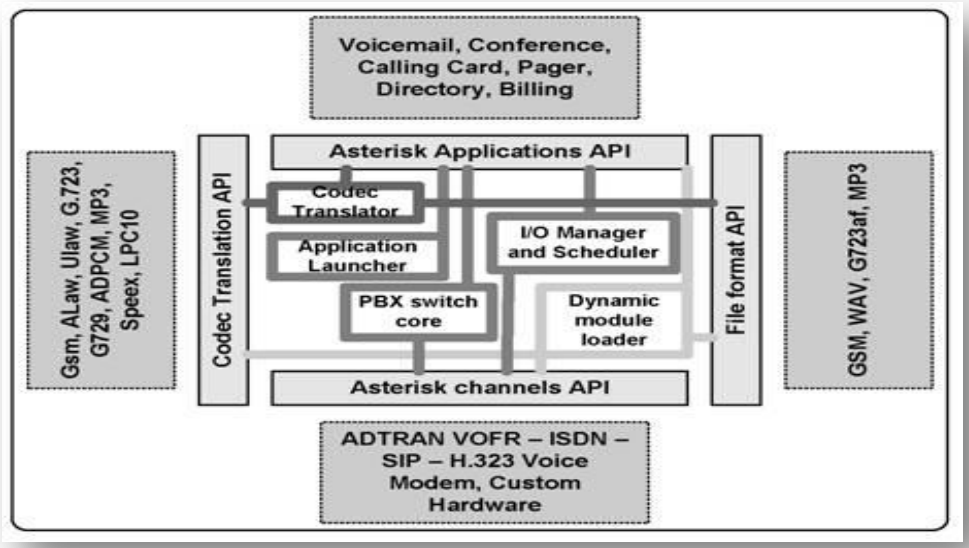



**Figura 27 – Arquitectura básica do Asterisk [122].**

O núcleo central do *Asterisk* manipula os seguintes componentes internamente:

- *PBX Switching*: este componente constitui a essência do sistema PBX *Asterisk*, visto que, permite efectuar a interconexão de chamadas para os vários utilizadores e automação de tarefas. O *Switching Core* permite efectuar uma interligação transparente das chamadas efectuadas em várias interfaces *hardware* e *software*.
- *Application Launcher*: este componente será o responsável para o lançamento de aplicações que executam serviços, como por exemplo, o *voice mail* e *playback* de ficheiros.
- *Codec Translator*: utiliza o módulo codec para codificar e descodificar vários formatos de compressão existente na indústria telefónica.
- *Scheduler and I/O Manager*: Este componente permite não só calendarizar os ficheiros de input e/ou output, como também, manipular as tarefas de baixo nível agendadas e pela gestão do sistema de forma a optimizar o desempenho para todas as condições de carga.

Importa salientar que, dentro da arquitectura do *Asterisk*, estão ainda definidas quatro APIs extremamente importantes para os módulos carregáveis, que irão facilitar a abstracção ao nível de protocolos e *hardware*. Entretanto, com os

referidos módulos carregáveis, o núcleo *Asterisk* não terá de se "preocupar" com os detalhes sobre como o emissor de uma determinada chamada (se o utilizador estará ou não a conectar, que codec estará a utilizar, etc.).

A seguir estão descritos os quatro principais módulos recarregáveis de API's, dentro dos quais passo a citar:

- *Channel API*: este componente manipula o tipo de conexões que o emissor de uma chamada efectua, seja esta uma conexão VoIP, ISDN, PRI, ou através de outra tecnologia. Contudo, serão carregados os módulos dinâmicos para manipular os detalhes da camada inferior destas conexões. Cada chamada em *Asterisk* é feita sobre uma interface num canal distinto.

- *Application API*: esta aplicação permite que várias aplicações como voice mail, chamada em conferência, transmissão de dados, chamada em espera, entre outras, sejam carregadas a partir de módulos específicos consoante a aplicação.

- *Codec Translator API*: este API será responsável por efectuar o carregamento dos módulos de codecs, tornando possível traduzir o sinal de voz a processar para outro formato desejado. Existem vários formatos de codificação áudio como o GSM, G.711, G.722, MP3,Speex, LPC10, etc.

- *File Format API*: esta aplicação permite manipular, não só vários ficheiros em determinados formatos para leitura e escrita, como também, ficheiros para armazenamento de dados fisicamente no sistema. Por exemplo, ficheiros áudio podem ser utilizados como toques de chamada, para música em espera ou para utilizar no *voice mail*. O sistema PBX *Asterisk* permite ler e reproduzir sons em diferentes formatos entre os quais, GSM, WAV, AU, G723af e MP3.

**Funcionamento do sistema PBX *Asterisk***

O sistema *PBX Asterisk* efectua uma interligação com a rede de dados através de uma porta *Ethernet* de 100Mbps, contendo uma possibilidade de activar um *firewall* de modo a garantir uma melhor gestão e segurança da largura banda para os telefones IPs, caso seja necessário.

A interligação do sistema *PBX Asterisk* com uma rede PSTN é efectuada através de vários módulos de *hardware* disponíveis no mercado a preços bastante acessíveis. Estes módulos são tipicamente baseados em placas PCI (FXS, FXO, E1, T1 e PRI), com interfaces de saída para acessos básicos RDIS (2, 4, 8 canais) ou para acessos primários RDIS. A sua conexão poderá ser efectuada directamente, não só

com as linhas do operador de comunicações tradicional, como também, com o PBX da rede telefónica de uma determinada instituição, desde que, este tenha um interface do mesmo tipo livre. No que se refere, ao nível protocolar, a interligação do *Askterisk* com o sistema PBX, será utilizado o protocolo QSIG (*Q Signaling*), que terá de ser suportado de ambos os lados da comunicação.

Na figura a seguir, está ilustrado um exemplo de uma empresa utilizando o sistema *PBX Asterisk*, onde todos os equipamentos da tecnologia VoIP quer localizados localmente ou nos portais web remotos, conectam-se ao servidor VoIP localizado na matriz através da Internet.

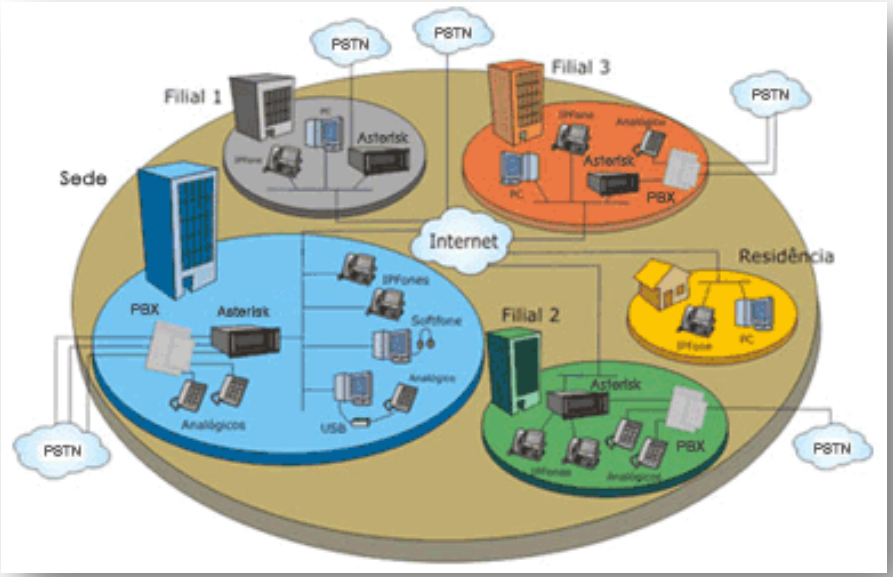



**Figura 28 – Cenário de uma empresa contendo o sistema Asterisk [51].**

### Requisitos mínimos para implementar um sistema PBX *Asterisk*

O *Asterisk* é um *software Open Source,* gratuito e bastante flexível que foi desenvolvido, não só para ser implementado na maioria das distribuições do sistema operativo Linux, bem como em grande parte de plataformas do sistema não Linux.

Contudo, os recursos mínimos necessários para a implementação do sistema *PBX Asterisk* são similares aos consumidos por uma aplicação embebida de tempo

real, e isto deve-se à necessidade de acesso prioritário ao processador e ao bus do sistema.

Importa salientar que, será também necessário que todas as tarefas a correr no sistema que não estão relacionadas com o processamento de chamadas do *Asterisk*, tenham prioridade baixa.

È de referir que, quanto maior a carga do sistema, maior será a dificuldade em manter um determinado número de conexões, sendo que esta situação para um PBX seria desastrosa e desvantajosa. Assim sendo, há que ter sempre em consideração, os requisitos mínimos de desempenho, visto que, são factores críticos no processo de escolha de uma plataforma.

Na tabela a seguir, está apresentada um conjunto de informação ao nível de *hardware*, referente aos requisitos mínimos para a implementação de um sistema PBX *Asterisk*, de forma a se obter um sistema fiável, robusto e eficiente consoante as necessidades do seu potencial utilizador.

| **Requisitos mínimos para implementar um sistema PBX Asterisk** | | |
|---|---|---|
| **Finalidade** | **Número de canais** | **Sistema mínimo recomendado** |
| Hobby system | Até 5 | 400-MHz x86, 256 MB RAM |
| SOHO (Small Office/Home Office) system | De 5 a 10 | 1-GHz x86, 512 MB RAM |
| Small business system | De 10 a 15 | 3-GHz x86, 1 GB RAM |
| Medium to large system | Mais de 15 | Dual CPUs, possibly also multiple |

**Tabela 18 – Requisitos mínimos para implementar um sistema PBX Asterisk.**

### Vantagens e Desvantagens da utilização do sistema PBX *Asterisk*

A seguir serão descritas algumas vantagens e desvantagens no uso da do sistema *PBX Asterik*.

- Vantagens:
  - Rápida e fácil implementação (através do *AsteriskNOW*);
  - Configuração relativamente simples (dependendo dos serviços desejados);
  - Inúmeros serviços disponíveis (*voicemail, call-on-wait*, etc…)

- Desvantagens:
    - Dificuldade de implementação em ambiente WAN sobretudo devido a problemas de escalabilidade (servidor *stateful*) e de *NAT Traversal* (utilização dos serviços por parte de clientes que estejam atrás de redes LAN com NAT).

#### *2.6.4.1.2. TrixBox*

*TrixBox* é uma plataforma *Open Source* e gratuito de *software* IP-PBX, que foi concebido para implementar um sistema de PBX com características tipicamente reservado para os negócios das pequenas e médias empresas. Actualmente, existem duas versões, sendo que uma edição é uma distribuição *Open Source* (CE) e a outra é uma versão comercial *hybrid-hosted*.

O projecto era anteriormente denominado de *Asterisk@Home* e após a aquisição do produto pela *Fonality* passou a ter o nome de *TrixBox*.

O *TrixBox* possui uma série de versões, sendo que a versão *TrixBox CE*, é completamente gratuita e muito simples de instalar. Possui uma interface gráfica que permite ao utilizador efectuar não só uma configuração de uma forma fácil e intuitiva, como também, uma gestão de todo o servidor *Asterisk*, incluindo todos os utilizadores/telefones e respectivos recursos através de uma interface web muito eficiente (com *Apache*, *MySQL* e *PHP*).

O sistema *PBX TrixBox* permite um utilizador final ou organização, criar não só um sistema de telefonia com as redes PSTN, bem como de telefonia através da internet ou VoIP ao custo zero.

**Figura 29 – Sistema PBX TrixBox [39].**

**Funcionalidades e características do sistema *PBX TrixBox***

O sistema *PBX TriBox* tem as mesmas funcionalidades e características relativamente ao *Asterisk*. Contudo, o *TrixBox* contém a versão completa do sistema *Asterisk* e outros programas pré-configurados no CD que fazem a auto-instalação/configuração de um PABX altamente funcional. Importa salientar que, depois de instalado o referido *software* permite-nos obter um PABX IP altamente funcional e que poderá ser configurado, consoante com as nossas necessidades.

A seguir será apresentado um conjunto de componentes que fazem parte deste novo sistema de auto-configuração do referido *software*. São eles:

- *CentOS 5.2*: corresponde ao Sistema Operacional Linux;
- *Asterisk 1.4*: corresponde ao sistema PABX IP *Open Source* e *freeware*;
- *freePBX 2.5*: esta funcionalidade corresponde ao interface *Web* que permite configurar o sistema PBX *Asterisk*;
- *SugarCRM*: esta funcionalidade permite ao administrador do sistema efectuar uma melhor gestão de contactos e dos seus potenciais clientes;
- *A2Billing*: corresponde ao sistema de tarifação que permite ao administrador do sistema obter o tarifário das chamadas em tempo real;

- *Flash Operator Panel* (FOP): esta funcionalidade corresponde ao painel que permite ao utilizador efectuar uma gestão das chamadas efectuadas;
- *Web Meet Me Control*: esta funcionalidade permite gerir as conferências;
- *Asterisk-Stat*: permite ao utilizador efectuar uma gestão dos relatórios das chamadas efectuadas (CDR);
- Possui um conjunto de bibliotecas, tais como, *mySQL*, *Apache*, PHP, etc;
- Contém diversas ferramentas que permitem uma melhor administração do servidor.

**Arquitectura do sistema *PBX TrixBox***

A administração do sistema *PBX TrixBox* é efectuada através de uma interface Web, onde será possível por um lado efectuar uma gestão de todas as chamadas efectuadas e/ou recebidas pelo utilizador, e por outro lado, configurar novos extensões de distribuição, gravar conversas, redireccionar chamadas, adicionar novas linhas, configurar e optimizar serviço de *voice-mail*, etc.

O *Trixbox* contém uma capacidade para suportar várias linguagens de programação o que garante uma maior estabilidade, permitindo assim o suporte a diversos fabricantes de *hardware*.

Como já foi anteriormente citado, o *TrixBox* contém um conjunto de pacotes e aplicações tais como: *Apache, Asterisk, FreePBX, Flash Operator Panel, MySQL, phpMyAdmin* e *SugarCRM*.

Este sistema de PBX possui ainda uma aplicação que permite ao administrador do sistema ter acesso a toda informação das chamadas efectuadas pelo utilizador, através de um ficheiro contido na base de dados, de modo a garantir uma melhor gestão do sistema em causa.

Contudo, devido à integração da aplicação com inúmeras aplicações tais como o *SugarCRM*, os drivers para as placas *Sangoma* e *Rhino*, isso proporcionou o desenvolvimento de vários suportes em diversos idiomas incluindo o Inglês, Alemão, Português e Espanhol, entre outros.

O sistema *PBX Trixbox* suporta diversos codecs de áudio, como por exemplo, o ADPCM, G.711, G.722, G.723.1, G.726, G.729, etc.

Este sistema suporta ainda um conjunto de protocolos tais como: o IAX, H.323, SIP, MGCP (*Media Gateway Control Protocol*), FXS, FXO, DTMF, PRI, etc.

**Requisitos mínimos para implementar um sistema PBX TrixBox**

Na tabela a seguir, está apresentada um quadro resumo contendo um conjunto de informação ao nível de *hardware*, referente aos requisitos mínimos para a implementação de um sistema *PBX TrixBox*, de forma a se obter um sistema fiável, robusto e eficiente consoante as necessidades do seu potencial utilizador.

| Requisitos mínimos para implementar um sistema PBX Asterisk | | |
|---|---|---|
| **Finalidade** | **Nº de canais** | **Sistema mínimo recomendado** |
| Hobby system | Até 2 | 500-MHz, 128 a 384 MB RAM |
| SOHO (Small Office/Home Office) system | De 2 a 10 | 500-MHz, 512 MB RAM e HD com 20GB |
| Small business system | De 10 a 15 | 2-GHz, 1 GB RAM e HD com 80GB |
| Medium to large system | Mais de 15 | Dual CPUs (Dual-Core), possibly also multiple |

**Tabela 19 – Requisitos mínimos para implementar um sistema PBX TrixBox.**

Importa salientar que, no processo de implementação de um sistema *PBX TrixBox*, há que ter sempre em consideração a selecção de um processador capaz de para garantir um melhor funcionamento do sistema. Contudo, é sempre aconselhado o uso de vários processadores ou processadores *dual-core,* em vez dos processadores com *Hyperthreading*, visto que, os referidos processadores não funcionam bem com o *Asterisk*.

#### *2.6.4.1.3. Elastix*

*Elastix* é actualmente uma das melhores plataformas *Open Source* presentes no mercado, e foi concebido para implementar um sistema de PBX, de modo a facilitar uma melhor a instalação e a configuração do servidor *Asterisk*.

Esta aplicação possui uma interface gráfica intuitiva e fácil de utilizar e a instalação do referido produto poderá ser feito em poucos minutos, incluindo o sistema operativo Linux, nomeadamente o *Asterisk*, contendo todas as bibliotecas necessárias, além de uma interface *Web* para configurar, gerir e administrar o referido servidor. Na figura a seguir, está ilustrada a interface *Web* da aplicação *Elastix*, apresentando as principais funcionalidades da mesma.

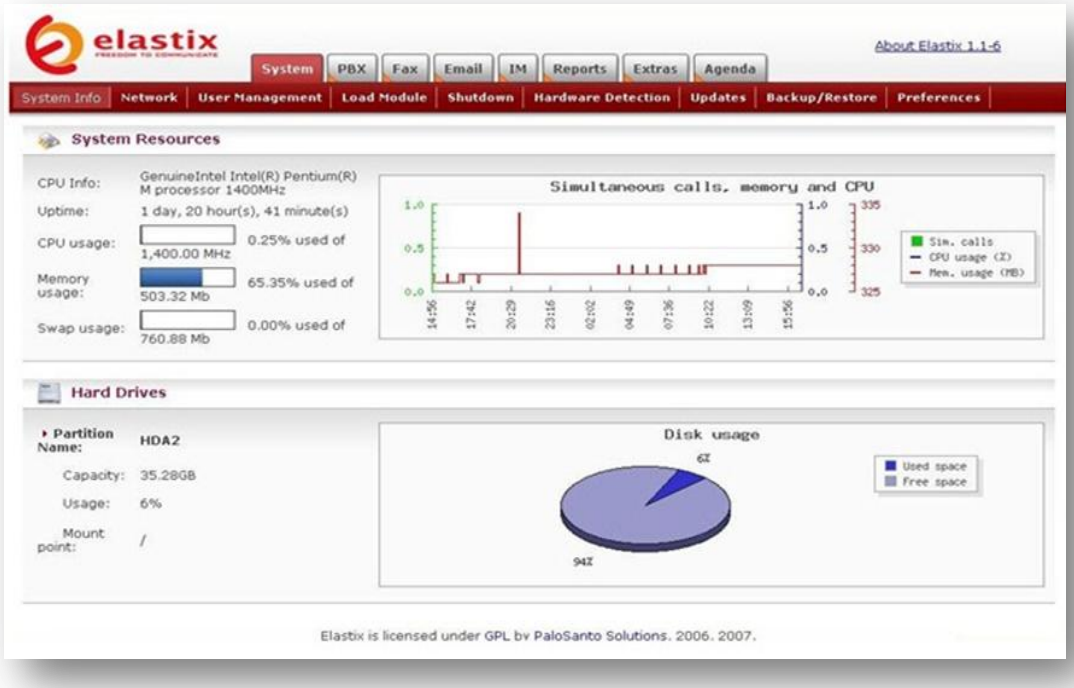



**Figura 30 – Sistema PBX Elastix [103].**

### Funcionalidades e características do sistema *PBX Elastix*

O sistema de *PBX Elastix* possui um conjunto de funcionalidades que permitem a criação de módulos para melhorar os pacotes *software* de código aberto disponíveis para o serviço de telefonia VoIP. A seguir está apresentada algumas das funcionalidades básicas da referida aplicação:

- Possui componentes que suportam sistemas de vídeo chamadas;
- Permite a utilização de múltiplas máquinas virtuais sobre a mesma máquina;
- Possui uma interface *Web* muito fácil e intuitiva para o utilizador;
- Permite enviar fax e e-mail. Permite ainda, enviar algum documento digital a um número de fax através de una impressora virtual;
- Possui uma aplicação que permite definir o tarifário das chamadas;
- Configuração gráfica de parâmetros da rede;
- Relatórios de utilização dos recursos;
- Opções para reiniciar/desligar remotamente;
- Relatórios de chamadas de entrada/saída e utilização dos canais;
- Serviço de *voice mail* integrado;

- Interface *Web* para *voice mail* e e-mail;
- Módulo integrado com painel de operador;
- Módulos incluídos *SugarCRM* e *Calling Card*;
- Secção de *download* e acessórios mais utilizados;
- Interface de ajuda integrado;
- Possui uma integração do servidor de mensagens instantâneas (*Openfire*);
- Suporte multi-linguístico.
- Servidor de correio electrónico integrado incluindo suporte multi-domínio.

**Requisitos mínimos para implementar um sistema *PBX Elastix***

A seguir, está apresentada um resumo contendo um conjunto de informação ao nível de *hardware*, referente aos requisitos mínimos para a implementação de um sistema *PBX Elastix*, de forma a se obter um sistema fiável, robusto e eficiente consoante as necessidades do seu potencial utilizador.

São eles:

- 800Mhz PC Pentium III ou superior (se for um P4 vai dar um conforto extra).
- 312MB de memória RAM, mas contudo, quanto mais melhor;
- 8 GB de espaço em disco rígido mínimo;
- 10/100 NIC (*Network Interface Card*);
- Drive de CD-ROM;
- 10/100 de 4 ou 8 portas *Ethernet hub* ou *switch* (não é necessário se o seu router tem de reposição portos. Isso depende de quantas extensões forem necessárias).

#### *2.6.4.2.SIP Server*

Como já tinha sido referido anteriormente no capítulo 2.4.1, um servidor SIP é o componente principal de um IP PBX e possibilita ao administrador do sistema, obter uma melhor capacidade de gestão e organização de todas as chamadas SIP na rede.

O referido servidor é constituído por três servidores: o *Proxy Server*, o *Registrar Server* e o *Redirect Server*. Estes componentes constituem elementos lógicos e em conjunto compõem um servidor SIP, contendo todas as funcionalidades desses respectivos servidores.

No ano de 2002, surgiu um dos primeiros projectos de servidores SIP, nomeadamente o SER (*SIP express Router*) com filosofia *Open Source.* O SER é um projecto que está a ser implementado desde 1995, por um grupo de investigadores na Alemanha.

Em 2004, o referido servidor foi adoptado por várias empresas multinacionais, nomeadamente a *freenet* e a *sipgate*, que são operadoras da tecnologia VoIP no mercado Alemão. Importa salientar que, actualmente o projecto SER está na versão 2.0 e trata de uma versão RC (*release candidate*), datada de Maio de 2007. Contudo, nos últimos anos não têm surgido novas actualizações desta distribuição.

No ano de 2005, surgiu uma nova divisão do projecto, nomeadamente o *fork*, onde esteve envolvido alguns dos co-fundadores do projecto SER.

Contudo, foi desenvolvido um novo projecto tendo baseado no SER, denominado por OpenSER e tinha como objectivo não só, melhorar o projecto já anteriormente iniciado, como também dar um novo rumo nas novas e futuras actualizações e no desenvolvimento das mesmas. O projecto *OpenSER* era patrocinado pela empresa multinacional *Voice System*, cuja sede oficial está situada na Roménia. Em Agosto de 2008, o referido projecto sofreu uma nova alteração, surgindo dois novos projectos, o *Kamailio* e o *OpenSIPS*, respectivamente.

Actualmente, ambos os projectos lançaram uma nova versão 1.4, contendo muita semelhança entre eles, sendo que qualquer apreciação final acerca da qualidade, fiabilidade e rapidez de desenvolvimento é ainda muito prematuro.

Importa salientar que, todos estes projectos anteriormente citados foram implementados utilizando a linguagem de programação C de *Unix/Linux*, sendo que a sua portabilidade para qualquer sistema operativo deste género será perfeitamente executável.

A seguir será apresentada uma breve descrição sobre o projecto *OpenSER*, abordando alguns aspectos principais deste projecto.

#### *2.6.4.2.1. OpenSER*

O *OpenSER* é um servidor proxy do protocolo SIP baseado na filosofia *Open Source*. Este *software* é licenciado através de uma licença do tipo GPL - *Gnu Public License*.

Permite, além de outras funções, o registo e estabelecimento de comunicação entre vários clientes SIP. Pode funcionar como *Registar*, *ProxyServer*, em dois diferentes modos de operação – *statefull* e *stateless*. Não tem funcionalidades de PBX.

Este projecto poderá ser usado não só em pequenos sistemas, como por exemplo, em sistemas embebidos como router DSL, mas também, em sistemas com grande escalabilidade contendo vários milhões de clientes de ISP (*Internet Service Providers*). O *software* é distribuído principalmente em código fonte, mas alguns fabricantes como Cisco, também vendem alguns produtos contendo o *OpenSER* incorporado.

Como já foi anteriormente citado este projecto, foi desenvolvido em 14 de Junho de 2005, por dois co-fundadores do *SIP Express Router* (SER), nomeadamente, o *Bogdan Andrei Iancu* e *Daniel Constantin Mierla*, juntamente com a colaboradora *Elena-Ramona Modroiu*.

O projecto *OpenSER* foi maioritariamente implementado na linguagem de programação C e executado principalmente em sistemas operacionais *Unix/Linux*. Contudo este projecto possui uma grande flexibilidade, permitindo assim implementar novas funcionalidades através do seu módulo de interface, conforme as necessidades dos seus utilizadores.

**Arquitectura do sistema *OpenSER***

Na figura a seguir, está ilustrada um exemplo de uma arquitectura da aplicação *OpenSER*, apresentando os componentes principais da mesma. Esta aplicação apresenta uma arquitectura modular constituída por duas partes:

- O núcleo principal (*OpenSER Core*): que contém as funcionalidades de mais baixo nível;
- Os módulos (*OpenSER Modules*): estes módulos correspondem a um conjunto de componentes que disponibilizam ao utilizador uma série de funcionalidades que permitem efectuar muitas tarefas tais como: ligação a bases de dados, implementação de presença, estatísticas, etc.

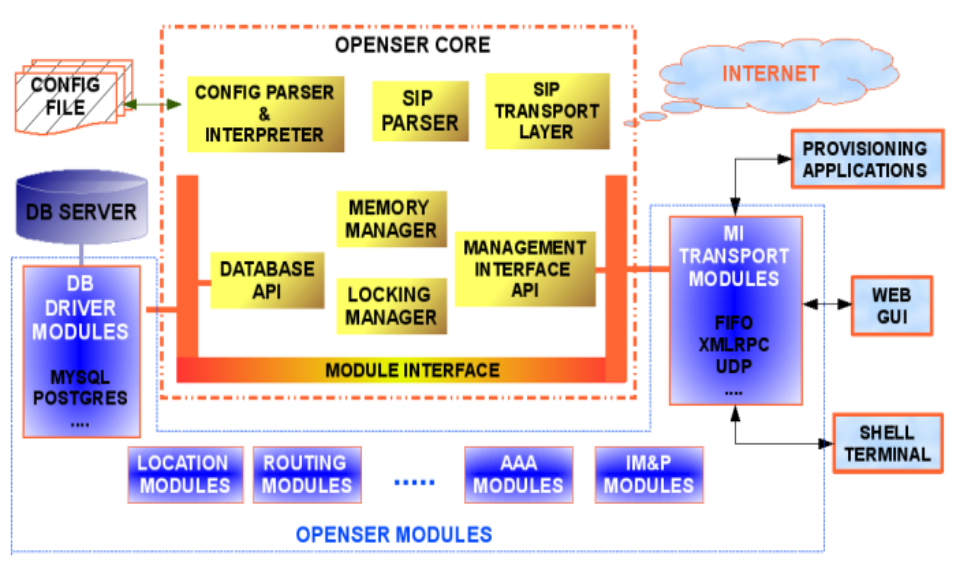



**Figura 31 – Arquitectura modular da aplicação OpenSER [104].**

### Funcionalidades do servidor *OpenSER*

Relativamente às funcionalidades o servidor *OpenSER* deve-se ter em conta o papel desempenhado pelas duas componentes que fazem parte da arquitectura principal do referido servidor, nomeadamente, o núcleo e os módulos.

O núcleo principal contém diferentes funcionalidades tais como:

- Gestão de memória;
- Sistema de bloqueio;
- Gestão de DNS e camada de transporte (UDP, TCP, TLS, SCTP);
- Configuração do leitor e interpretador de comandos;
- Camada de abstracção da Base de Dados (DB API);
- Interface de gestão (MI API);
- Encaminhamento em modo;
- Pseudo-variáveis;
- Motor de estatísticas;
- API do temporizador.

No que diz respeito aos módulos, será sempre possível configurá-los e adicionar novas funcionalidades conforme a necessidade do utilizador. São elas:

- Gestão da localização dos utilizadores;

- Autenticação, Autorização e Contabilização;
- Operações com expressões regulares e textos;
- Resposta *stateless*;
- Processamento *statefull*;
- Mensagens instantâneas e extensões de presença;
- Suporte de *RADIUS*;
- Conectores a Bases de Dados (MySQL, ODBC, etc.);
- Transporte MI;
- Interpretador CPL;
- Gateways SMS e XMPP;
- Transposição de NAT;
- Extensões para linguagem Perl e *Java SIP Servlet*.

**Vantagens e Desvantagens da utilização do *OpenSER***

A seguir serão descritas algumas vantagens e desvantagens no uso da do servidor *OpenSER*.

- Vantagens:
    - Implementação relativamente simples;
    - Boa escalabilidade (servidor *stateless* – só gere a comunicação SIP, deixando a troca de pacotes de áudio/vídeo à responsabilidade dos clientes);
    - Resolve os problemas relacionados com a sinalização SIP através de redes que utilizem NAT.
- Desvantagens:
    - Configuração elaborada e ainda pouco difundida - dificuldade na obtenção de conhecimentos;
    - Devido ao facto de não gerir os pacotes multimédia leva a problemas de *accounting* das chamadas (que poderá ser necessário em serviços que se desejem pagos);

- Não resolve, *per si*, os problemas de NAT relacionados com os pacotes multimédia (sessões RTP) – necessita de uma outra aplicação a correr em paralelo (RTP proxy);
- Não disponibiliza os serviços vulgares de PBX (*voicemail, call-on-wait,* etc.).

#### *2.6.4.3.Media Relay*

*Media Relay* é uma aplicação baseado na filosofia *Open Source* que funciona em paralelo com um servidor SIP Proxy, permitindo aos clientes do protocolo SIP que usem NAT, trocar pacotes do tipo RTP/RTCP transportados em UDP. Com esta aplicação torna-se possível a transposição de *firewalls* e/ou *router* por clientes NAT. Este *software* é licenciado através de uma licença do tipo GPL - *GNU Public License*.

Um exemplo prático de uma aplicação *media relay* é o *MediaProxy*, que foi desenvolvido pela empresa *Ag-projects*, cujo fundador foi um dos co-fundadores do projecto *OpenSER*.

A aplicação *MediaProxy* já está recentemente na versão 2.0, possuindo um novo design que permite melhorias muito significativas em áreas como a escalabilidade (uma ordem de magnitude mais escalável do que a versão anterior) e a segurança nas comunicações entre os equipamentos.

Na figura a seguir, está apresentada um diagrama contendo algumas informações sobre o funcionamento básico de uma aplicação *MediaProxy*.

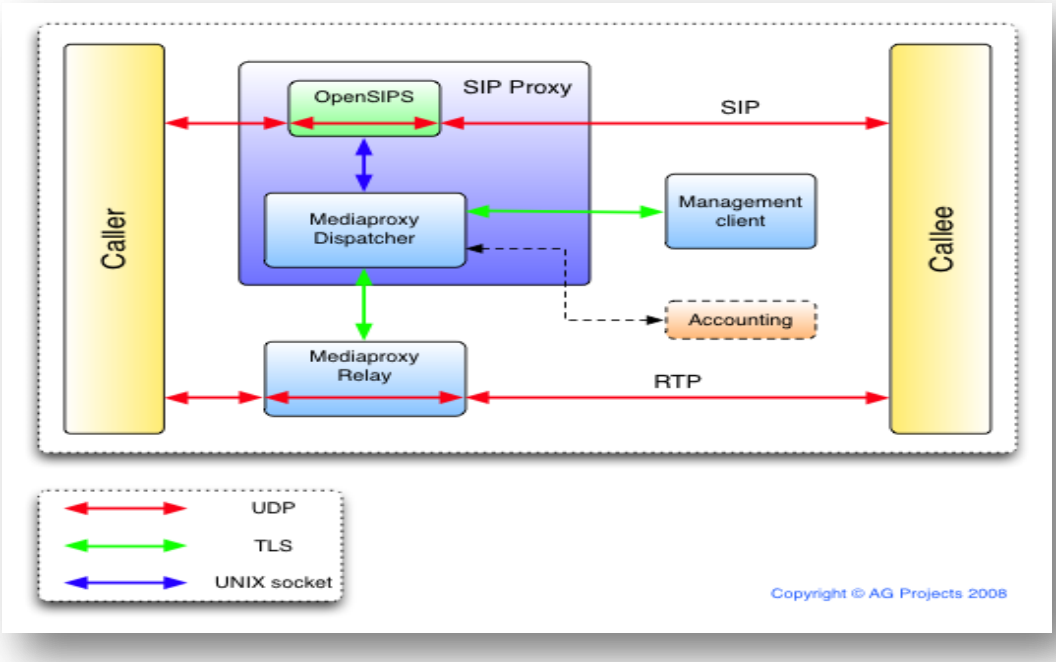



**Figura 32 – Diagrama de funcionamento básico da aplicação MediaProxy [53].**

#### *2.6.4.4.Sistemas de administração através de uma plataforma Web*

Neste ponto, será apresentado um exemplo de sistema de administração IP PBX baseado na filosofia *Open Source.*

Este sistema será administrado através de uma plataforma WEB e terá como objectivo fundamental ajudar ao administrador do sistema, a ter uma melhor capacidade de gestão de todas as questões relacionadas não só, com os utilizadores (permissões, definição de grupos, instalação de domínios, etc.), como também, com a interface gráfica para os potenciais utilizadores que pretendam utilizar o serviço VoIP (registo de utilizador, definições pessoais, consulta do crédito, consulta do histórico das chamadas efectuadas, etc.).

È de referir que, embora haja algumas aplicações de administração de sistemas IP PBX já desenvolvidas, todas elas apresentem um baixo grau de desenvolvimento e maturidade.

Contudo, isso deve-se ao facto de que, estas aplicações serem normalmente personalizadas em função das necessidades encontradas pelo operador VoIP para satisfazer todas as exigências dos seus clientes de modo a garantir uma melhor prestação de serviços nesta área.

Um exemplo prático de um sistema de administração IP PBX através de uma plataforma Web, é a aplicação *SerMyAdmin* que é um projecto *Open Source* e gratuito desenvolvido em *Grails*, e que pretende ser uma plataforma de acesso não só ao administrador do sistema, como também, aos potenciais utilizadores do serviço VoIP.

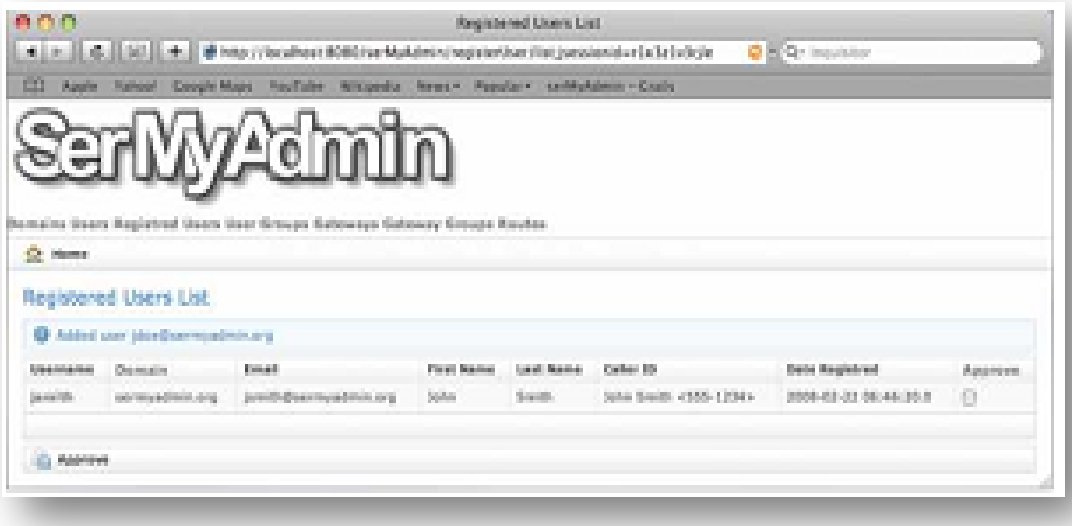



**Figura 33 – SerMyAdmin: Sistema de administração IP PBX via Web [102].**

#### *2.6.4.5.Sistema de gestão AAA - RADIUS*

Neste ponto, será apresentado um exemplo de sistema *Open Source* de gestão de autenticação, autorização e contabilização para pessoas ou computadores que se ligam e usam serviços na rede.

Um exemplo prático do referido sistema é a aplicação FreeRadius que utiliza o protocolo de rede *RADIUS*, que permite fornecer ao administrador do sistema uma melhor capacidade de gestão de autenticação, autorização e contabilização das pessoas ou computadores que se ligam e usam serviços na rede.

Importa salientar que, estes três serviços disponibilizados ao administrador do sistema pelo protocolo *RADIUS* são conhecidos pela sigla AAA (*Authentication, Authorization, Accounting)*:

- *Authentication*: este serviço obriga a um determinado utilizador ou computador que se deseja efectuar uma conexão à rede, a autenticar no sistema;
- *Authorization*: após o registo de autenticação, o protocolo RADIUS, irá determinar quais as permissões de acesso do respectivo utilizador e/ou computador, através do serviço de autorização;
- *Accounting*: uma vez autorizado, será efectuado um registo de toda a informação relativamente aos utilizadores e computadores disponíveis na rede, no serviço de contabilização;

De salientar que, actualmente o protocolo *RADIUS* está a ser utilizado pela maioria dos fornecedores de serviços VoIP, sendo que este protocolo permite atribuir credenciais de login aos clientes SIP (como por exemplo um telefone VoIP) para o servidor *SIP Registrar* usando a autenticação *digest*. Seguidamente, será atribuído uma outra credencial para o servidor *RADIUS* e este por sua vez irá efectuar o registo de toda a informação necessária relativamente às chamadas efectuadas.
Esta informação detalhada é designada por CDR (*Call Detail Records*) e poderá ser usada posteriormente para cálculo da facturação das chamadas.

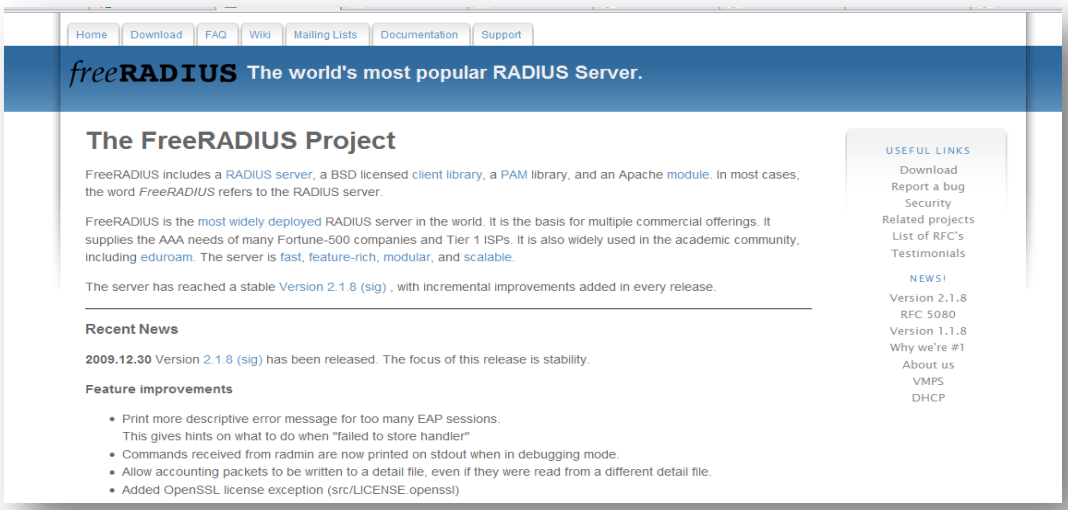



**Figura 34 – Página oficial do projecto freeRADIUS: Sistema de gestão AAA [100].**

### *2.6.4.6.Sistemas de facturação e contabilização de chamadas*

Neste ponto, será apresentado um exemplo de sistema de facturação e contabilização das chamadas efectuadas pelo utilizador, baseado na filosofia *Open Source.* Esta aplicação permite ao administrador do sistema, efectuar um controlo de facturação e contabilização de chamadas em paralelo com o servidor RADIUS, registando todos os dados das chamadas e calculando o custo das mesmas, em função das configurações previamente estabelecidas.

Um exemplo prático do referido sistema é a aplicação *CDRTool* que é uma solução *Open Source* desenvolvida pela *Ag-Projects*, que permite ao administrador do sistema obter em tempo real todas as informações acerca da utilização do serviço VoIP, tais como: CDRs das chamadas efectuadas, estatísticas baseadas em critérios configuráveis, como por exemplo, o destino das chamadas, motivos de falha, etc.

Dado ao facto de que, esta aplicação foi desenvolvida simultaneamente com o projecto *MediaProxy*, isso possibilita que a referida aplicação tenha um melhor desempenho, sobretudo na detecção de chamadas que terminam sem recorrer a mensagens do tipo BYE, como por exemplo, quando ocorre alguma falha imprevisível no sistema computacional.

A aplicação *CDRToll* possui ainda algumas funcionalidades adicionais que permitem efectuar um pagamento pós-pago, isto é, caso um utilizador desejar efectuar um determinado telefonema, poderá sempre pagar depois o custo da respectiva chamada. Contudo, este pagamento será efectuado em conjunto com outras aplicações de pagamento pré-pago, isto é, mediante uma aquisição prévia de crédito telefónico. Este tipo de funcionalidades encontra-se disponível por TCP/IP.

A seguir está apresentada de uma forma resumida algumas das funcionalidades básicas da aplicação *CDRTool*:

- Permite definir previamente o custo das chamadas a serem efectuadas;
- Permite ao administrador do sistema ter um controlo de acesso baseado em utilizador/domínio/proxy;
- Permite efectuar o cálculo das chamadas efectuadas em tempo real;
- Possui alguns mecanismos anti-fraude que permitem evitar o uso indevido do serviço a utilizadores que excederam o crédito;
- Permite ao utilizador e/ou administrador do sistema efectuar Importação/Exportação dos dados para outros formatos para posterior análise;

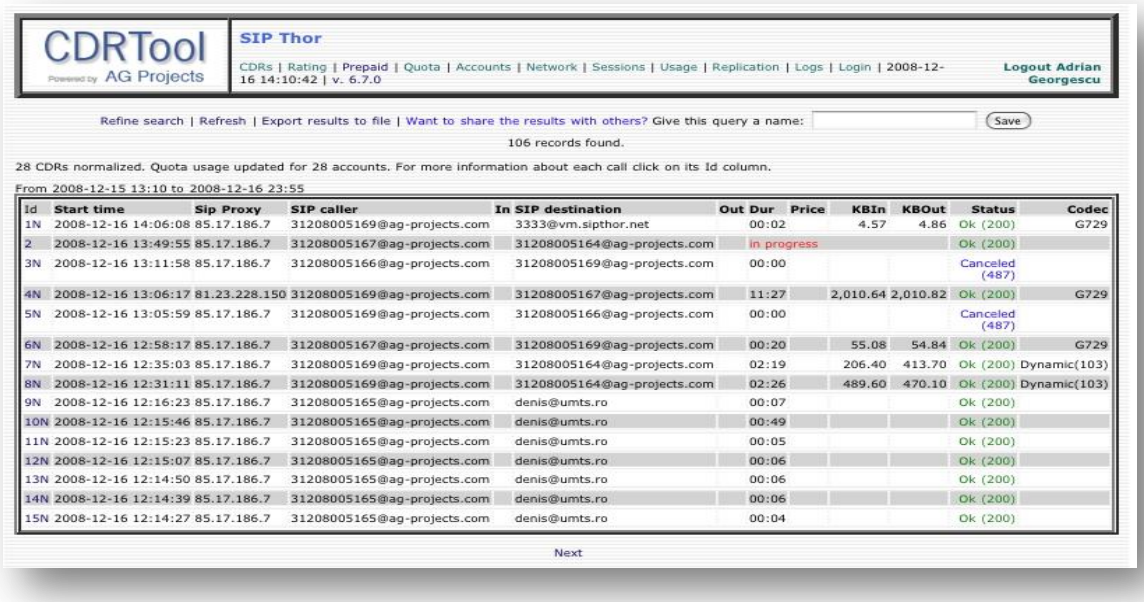



**Figura 35 – CDRTool: Sistema de facturação e contabilização das chamadas [101].**

# 3

# 3. Soluções Wireless para Redes Comunitárias

Neste capítulo, será apresentada uma breve introdução sobre a tecnologia das redes *Wi-Fi* e das *Mesh Network*, abordando alguns conceitos básicos dessas duas tecnologias, tais como, a sua definição e o seu funcionamento básico. A seguir, será feita uma descrição detalhada sobre a sua arquitectura, descrevendo os seus principais componentes. Seguidamente, será apresentado um estudo detalhado sobre os principais protocolos usados nessas tecnologias e alguns aspectos de segurança.

De seguida, serão apresentadas suas vantagens e desvantagens no uso dessa tecnologia. Será ainda, apresentado alguns exemplos de projectos existentes no mercado e que usam esta tecnologia. Por último, serão apresentados alguns exemplos de equipamentos dessa tecnologia e algumas soluções *Open Source* presentes no mercado empresarial.

## *3.1. Introdução*

Nas últimas décadas com o desenvolvimento tecnológico, o mundo das telecomunicações tem sofrido uma constante evolução, não só devido à rápida proliferação da implementação da banda larga, como também, com um crescimento do uso da tecnologia de redes sem fios.

Hoje em dia, já se pode encontrar em vários locais não só ao nível público e/ou privado, muitas infra-estruturas de redes contendo a tecnologia *Wi-Fi*. Esta norma foi criada pelo IEEE (*Institute of Electrical and Electronics Engineers*) [133] na década de 90, mais concretamente em 1997, e suportava na primeira versão, um débito máximo de 2Mbps nos 2.4GHz. Esta zona do espectro, tem como vantagem não necessitar de qualquer licenciamento, o que significa que uma rede 802.11 poderá ser mantida sem custos adicionais, mas tem como desvantagem a saturação do espectro devido a um número crescente de utilizadores. Contudo, actualmente existe uma forte tendência e necessidade destas redes se aumentarem em tamanho e complexidade, de modo a oferecer uma melhor qualidade de serviço aos potenciais utilizadores quer ao nível pessoal e/ou empresarial.

Entretanto, face à esta necessidade de expandir essa complexidade e devido há vários trabalhos de investigação científica a nível mundial nesta área, está a emergir uma nova tecnologia, denominada por *Wi-Fi Mesh* ou Redes *Mesh* Sem Fios (*Wireless Mesh Network, WMN*), que irá permitir ao utilizador final um acesso sem fios contínuo às aplicações de banda larga, virtualmente em qualquer momento e em qualquer lugar, garantindo assim uma melhor qualidade de serviço aos mesmos.

## *3.2. Redes Wi-Fi*

O padrão IEEE 802.11 é uma norma desenvolvida para descrever as redes *Wi-Fi* e fornece algumas especificações que permitem efectuar uma conectividade entre duas estações, nomeadamente, a sem fios e infra-estruturas de redes cabladas. O referido padrão tal como as restantes normas da família IEEE 802, também definem as especificações da camada física (PHY) que corresponde ao nível 1 do modelo de referência OSI, e as especificações da camada de controlo de acesso ao meio (MAC).

O nível 2 do modelo OSI corresponde à camada de ligação de dados, que é a combinação da camada de controlo de acesso ao meio e a camada de controlo da ligação lógica (*LLC – Logical Link Control*), que está especificada na norma IEEE 802.2. Na figura a seguir, está ilustrada no modelo de referência OSI, a localização da norma IEEE 802.11, conforme podemos observar.

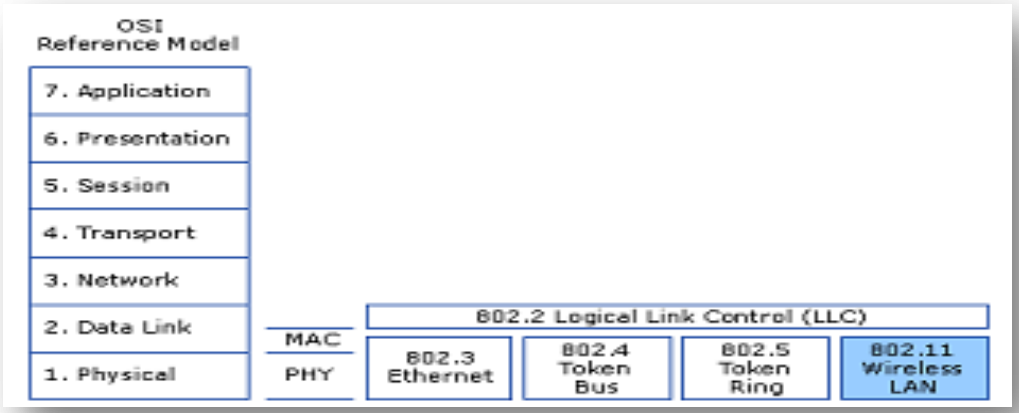



**Figura 36 – Modelo OSI [106].**

### *3.2.1. Arquitectura das Redes Wi-Fi*

A arquitectura básica da norma IEEE 802.11 é constituída por um conjunto de componentes que interagem de forma a que seja possível a formação de uma rede local sem fios, contendo um suporte capaz de permitir uma rápida e eficaz mobilidade de estações e de uma forma transparente para as camadas superiores.

A seguir será apresentada uma breve descrição dos principais componentes da referida arquitectura:

- AP (*Access Point*): estes componentes são estações análogas às estações base das redes de comunicação móveis, que permitem efectuar uma operação da rede no modo de infra-estrutura;
- STA (*Station*): este componente poderá ser qualquer dispositivo que permite implementar as camadas física e de acesso ao meio da norma IEEE 802.11, como por exemplo, uma placa de rede *Wi-Fi* de um determinado computador;
- BSS (*Basic Service Set*): este elemento representa um grupo de estações que estão sob o controlo de um *Acess Point*, utilizando o modo de operação designado de Infra-estrutura;
- IBSS (*Independent Basic Service Set*): este componente tem como função representar um grupo de estações que não utilizam a estrutura de comunicação fornecida pelo AP. As estações comunicam directamente umas com as outras, sendo que este modo de operação é denominado de *Ad-Hoc*;
- DS (*Distribution System*): corresponde ao meio pelo qual os APs comunicam entre si. A norma IEEE 802.11 não especifica a tecnologia deste sistema, podendo ser baseado em qualquer tecnologia de rede, sendo a mais comum a tecnologia *Ethernet*;
- ESS (*Extended Service Set*): este componente representa um conjunto de BSSs interligados entre si através de um sistema de distribuição (DS). A possibilidade de interligar vários BSSs permite aumentar a área de cobertura, levando a que seja possível uma maior mobilidade das estações;
- Portal: corresponderá à entidade que efectua a interligação do sistema de distribuição com outros tipos de redes, isto é, se no caso existir uma a outra rede da família IEEE 802.X, a função desta entidade será semelhante de a uma *bridge*.

#### *3.2.1.1. Redes Wi-Fi em modo Ad-Hoc*

As redes *Wi-Fi* em modo *Ad-Hoc* constituem numa cooperação entre um conjunto de nós móveis que não necessitam da intervenção de um AP centralizado ou de uma infra-estrutura já existente, visto que, podem estabelecer uma ligação directa entre eles. Este serviço é chamado de IBSS (*Independent Basic Service Set*) e pode utilizar um AP mas apenas exercendo a função de repetidor para estender o alcance da rede.

A topologia de uma rede *Ad-Hoc* poderá mudar de uma forma dinâmica devido à mobilidade dos nós. Uma rede *Ad-Hoc* móvel, também designada por MANET (*Mobile Ad-Hoc NETwork*), poderá ser definida como sendo um grupo autónomo de nós móveis que comunicam através de ligações sem fios. As MANETs possuem um conjunto de aplicações não só ao nível das redes militares, como também, ao nível das redes de emergência entre mais.

As redes *Ad-Hoc* utilizam os protocolos de *routing IP Ad-Hoc* para encaminharem os pacotes para o nível da camada do modelo OSI. Estas redes possuem outras características tais como:

- A capacidade de auto-configuração na rede;
- Possibilidade de serem utilizadas como sendo uma rede intranet ou internet;
- Utilizam várias técnicas de protocolo *routing*, tais como, o reactivo e o pró-activo.

Na seguinte figura, está ilustrada um exemplo de uma rede *Wi-Fi* em modo *Ad-Hoc*, constituída por varias estações (STA), estabelecendo uma comunicação directa umas com as outras sem o uso de um ponto de acesso para efectuar a respectiva conexão.

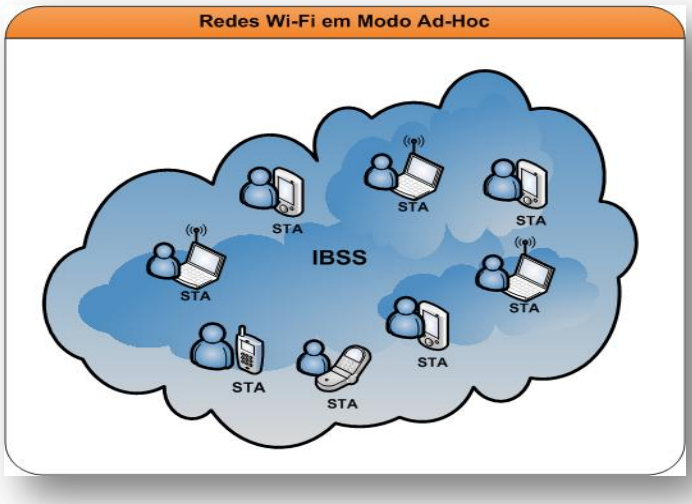



**Figura 37 – Rede Wi-Fi em modo Ad-Hoc.**

### *3.2.1.2. Redes Wi-Fi em modo Infra-estrutura*

As redes de infra-estrutura distinguem-se das redes *Ad-Hoc* pela utilização obrigatória de um AP. O AP funciona como sendo uma ponte entre a rede fixa e a rede sem fios, gerindo todo o tráfego da comunicação entre todos terminais.

O AP é um ponto de passagem obrigatório na comunicação entre todos os dispositivos. A *Basic Service Area* de uma rede infra-estrutura é definida pelos pontos alcançados pelo AP. Este tipo de arquitectura tem duas vantagens:

- Uma rede de infra-estrutura BSS é definida pela distância ao AP. Todos os terminais são obrigados a localizarem-se dentro da área de cobertura do AP mas, nenhuma restrição é imposta relativamente à distância entre terminais. A comunicação directa entre terminais salvaguardava a capacidade de transmissão mas aumentaria a complexidade do sistema já que tem de monitorizar possíveis interferências vindas de terminais vizinhos.
- O AP é normalmente um dispositivo de complexidade superior ao terminal e por isso consome uma maior quantidade de potência. Como se sabe, para um terminal móvel, a autonomia é um dos aspectos principais. Um AP apercebe-se de quando um terminal entra em modo *power saving* e guarda as suas tramas num *buffer*. Um terminal que opera com auxílio a uma bateria, podem ligar/desligar o receptor apenas para transmitir e receber a tramas contidas no *buffer* do AP.

Numa rede de infra-estrutura, as estações devem efectuar a função de associação ao AP de modo a obter os serviços de rede. Esta função é semelhante à de ligar o cabo *Ethernet*. Um terminal inicia-se na rede sempre com esta função mas o AP é que decide se permite ou não o seu registo. A função de associação é exclusiva do terminal que só pode estar associado a um AP.

O *standard* 802.11 não impõe nenhuma limitação ao número de terminais que podem estar associados a um AP. Esta limitação é normalmente efectuada pelos requisitos mínimos a nível de taxas de transmissão necessitadas.

Na figura a seguir, está ilustrada uma rede *Wi-Fi* em modo de infra-estrutura com dois BSS interligados por um sistema de distribuição permitindo assim uma formação de um ESS.

Por sua vez o sistema de distribuição (DS) está ligado a um portal que irá permitir ao utilizador um acesso a uma rede a família IEEE 802.X.

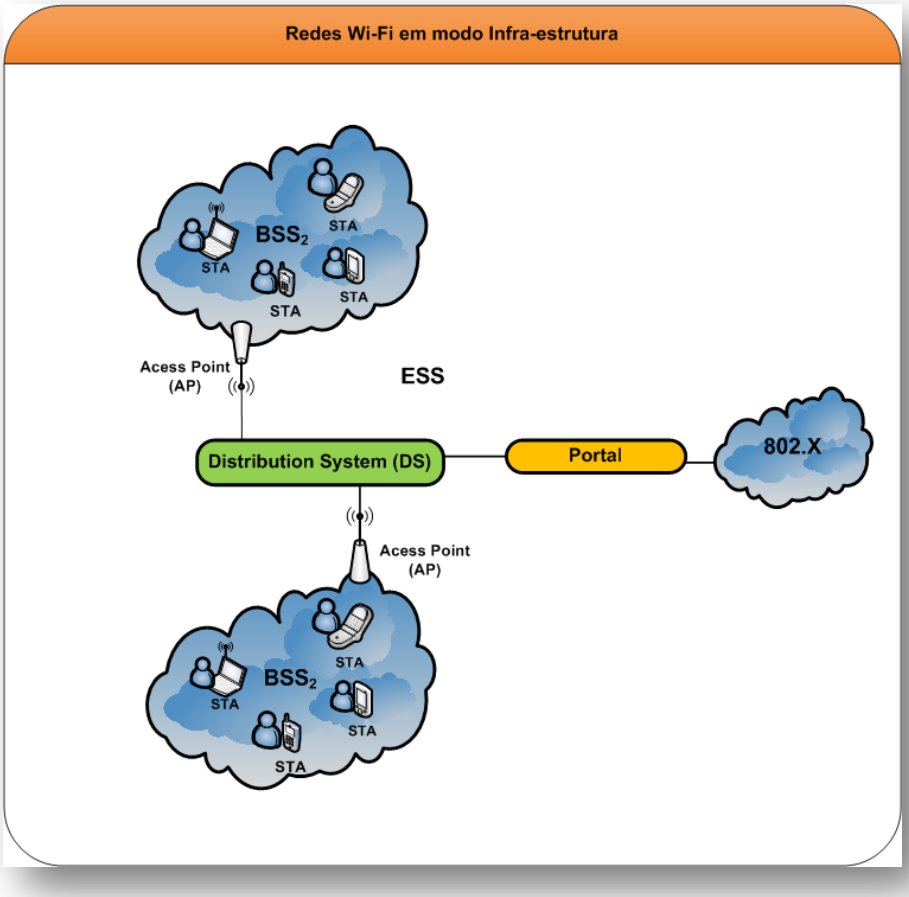



**Figura 38 – Rede Wi-Fi em modo Infra-estrutura.**

### *3.2.2. Camada física (PHY) das Redes Wi-Fi*

Nas especificações da camada física são definidas técnicas de *Spread Spectrum* que permitem a operação de várias estações em simultâneo sobre a mesma banda de frequências com o mínimo de interferência entre elas.

Na norma base é definida não só, a utilização da técnica de *Spread Spectrum* por salto em frequência (*FHSS - Frequency Hopping Spread Spectrum*), como também, a técnica de *Spread Spectrum* por sequência directa *(DSSS - Direct Sequence Spread Spectrum*), sobre uma das bandas ISM (*Industrial, Scientific and Medical*), operando entre as gamas de frequências de 2,4GHz a 2,5GHz.

A norma especifica um débito de 2Mb/s que poderá ser reduzido para 1Mb/s em condições menos ideais, sendo que, estes débitos comparados com os débitos obtidos em redes *Ethernet* são ligeiramente mais baixos.

Entretanto, o IEEE nas últimas décadas tem vindo a efectuar algumas investigações científicas e tecnológicas, para desenvolver uma série de protocolos standards que visam a aumentar esse débito. A seguir passo a citar as principais normas desta tecnologia:

- IEEE 802.11a: Esta norma permitiu o aumento do débito para 54Mb/s em condições ideais à custa do uso da técnica OFDM (*Orthogonal Frequency Division Multiplexing*), onde o espectro é divido em múltiplas portadoras (52 no total) de pequena largura de banda, permitindo uma maior resistência à interferência. Em condições menos ideais o débito pode ser reduzido para 48Mb/s, 36Mb/s, 24Mb/s, 18Mb/s, 12Mb/s, 9Mb/s ou 6Mb/s. A banda de frequências de operação é diferente das outras normas, utilizando outra das bandas ISM em 5GHz. A implementação desta norma demorou, sendo que nunca teve grande aceitação devido à larga implantação de produtos compatíveis com a norma IEEE 802.11b;

- IEEE 802.11b: Esta norma foi a principal melhoria criada para a norma base, pois permitiu um aumento do débito para 11Mb/s em condições ideais, podendo ser utilizados débitos menores de 5,5Mb/s, 2Mb/s ou 1Mb/s conforme as condições de transmissão. Utiliza a técnica de *Spread Spectrum* por sequência directa (DSSS) e funciona sob a mesma banda de frequências usadas na norma base.

- IEEE 802.11g: O standard 802.11g foi a última versão aprovada pelo IEEE que dispõe actualmente de equipamentos. Esta norma permite um alcançar débito máximo de 54Mb/s (802.11a), usando uma banda de frequências entre 2,4GHz e 2,5GHz (802.11b) em conjunto com a técnica OFDM. Em condições menos ideais o débito pode ser reduzido para 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps ou 6Mbps. Alguns fabricantes fornecem débitos até 108Mbps, o SuperG, utilizando 2 canais de 20MHz;

- IEEE 802.11n: Esta norma está recentemente a ser desenvolvida pela IEEE e permite usar a banda de entre 2,4GHz e 5GHz. Possui ainda compatibilidade com os equipamentos que usam a tecnologia 802.11g e 802.11b, sendo que, possivelmente terá o suporte para a tecnologia 802.11a.

Na figura a seguir, está ilustrada um quadro resumo sobre as normas da família IEEE 802.11, apresentando todos os principais protocolos dessa mesma, conforme podemos observar.

| | 802.11a | 802.11b | 802.11g | | 802.11n |
|---|---|---|---|---|---|
| Band | 5.7 GHz | 2.4 GHz | 2.4 GHz | | Unconfirmed<br>Possibly 2.4 and 5 GHz bands |
| Channels* | Up to 23 | 3 | 3 | | |
| Modulation | OFDM | DSSS | DSSS | OFDM | MIMO-OFDM |
| Data Rates | Up to 54 Mbps | Up to 11 Mbps | Up to 11 Mbps | Up to 54 Mbps | Speculated to be 248 Mbps for two MIMO streams |
| Pros | ~150 feet or 35 meters | ~150 feet or 35 meters | ~150 feet or 35 meters | | ~230 feet or 70 meters |
| Cons | October 1999 | October 1999 | June 2003 | | Expected in 2008 |
| Pros | Fast, less prone to interference | Low cost, good range | Fast, good range, not easily obstructed | | Very good data rates, improved range |
| Cons | Higher cost, shorter range | Slow, prone to interference | Prone to interference from appliances operating on 2.4 GHz band | | |

**Figura 39 – Normas IEEE 802.11 para a camada física [31].**

**NOTA:** Importa salientar que, a norma IEEE 802.11n está actualmente a ser desenvolvida pelo IEEE e esta tecnologia irá tirar o partido da tecnologia MIMO (*Multiple Input Multiple Output*) para aumentar o débito.

### *3.2.3. Camada de acesso ao meio (MAC) das Redes Wi-Fi*

A camada de acesso ao meio (MAC) tem como objectivo principal controlar as transmissões, de modo a evitar colisão entre pacotes (CDMA/CA).

È de referir que, todas as versões da tecnologia 802.11 (802.11a/b/g) utilizam a mesma sub-camada MAC. O protocolo 802.11 é muito semelhante ao protocolo *Ethernet*. Os interfaces cards 802.11 possuem um endereço MAC de 48-bit que são incluídos nas tabelas ARP juntamente com os endereços *Ethernet*. Entretanto, importa salientar que é quase impossível distinguir a diferença entre os dois endereços MAC.

A camada MAC original foi desenhada utilizando um mecanismo de acesso ao canal semelhante à *Ethernet* (CSMA). No entanto a *Ethernet* (com uma taxa de entrega de pacotes contendo uma eficiência na ordem de 99%) baseia o seu mecanismo na detecção de possíveis colisões de pacotes (*Colision Detection*) (CDMA-CD).

Num cenário de redes sem fios, em que 20% dos pacotes necessitam de retransmissão, é quase impossível utilizar a mesma técnica. Assim sendo, de modo a superar esta necessidade de retransmissão, poderá ser utilizada uma técnica

denominada de *Collision Avoidance* (CDMA-CA) que embora seja semelhante ao anterior mas contem algumas diferenças em relação à outra.

Para evitar uma colisão durante a transmissão de pacotes, será preciso obrigar uma determinada estação, a aguardar durante um certo intervalo de tempo de um modo aleatório antes da transmissão (IFS - *Inter Frame Spacing*).

#### *3.2.3.1. Métodos da camada MAC*

A seguir estão apresentados os principais métodos utilizados pela camada MAC:

- DCF (*Distributed Coordination Function*) com CSMA/CA: este método de acesso é utilizado para suportar transferências de dados assíncronos baseados numa topologia de *best-effort*. O referido método é apenas compatível com o modo *Ad-Hoc* onde cada terminal compete pelo tempo de antena (não existe a função de AP);
- DCF (*Distributed Coordination Function*) com RTS/CTS: este método é muito semelhante ao primeiro método, mas contudo, são utilizadas tramas de reserva de recursos RTS/CTS (*Request to Send* / *Clear to Send*). Este modo provoca um ligeiro atraso ao sistema mas torna-o mais eficiente;
- PCF (*Point Coordination Function*): este método poderá ser implementado no AP, permitindo-o ter um controlo absoluto de toda a actividade na sua célula. O PCF é apenas compatível para o modo infra-estrutura. Neste método, a ordem de transmissão é controlada a partir do AP via *polling*. A intenção inicial de se incluir PCF era com o objectivo de proporcionar um mecanismo de reserva de recursos e prioridades para voz ou outro tipo de tráfego sensível ao atraso.

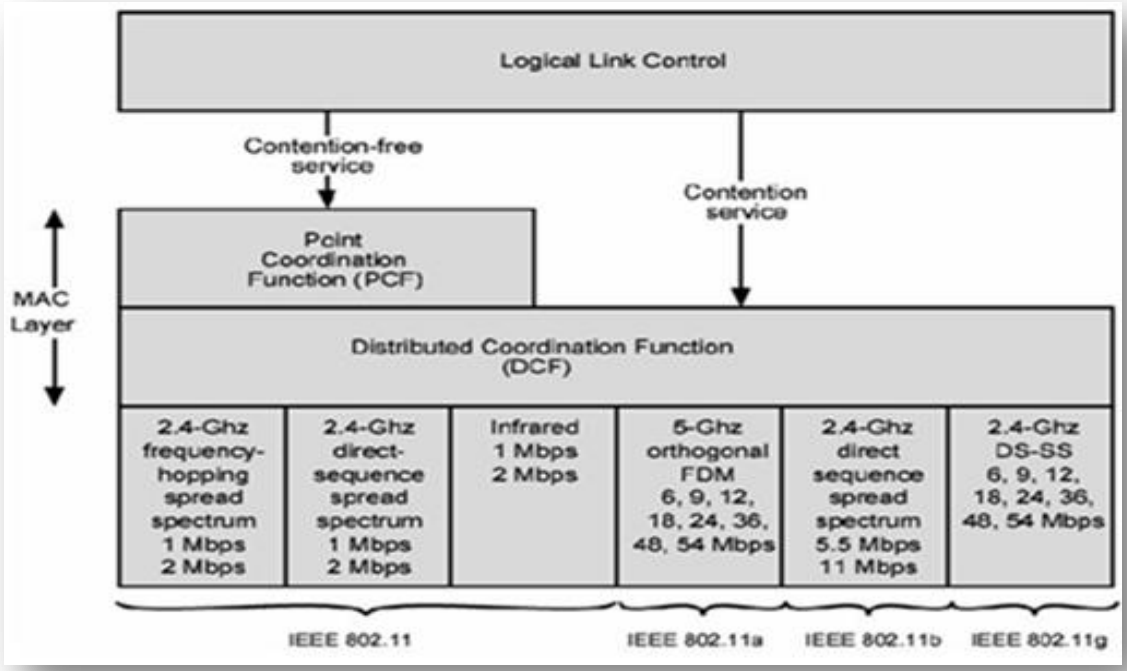



**Figura 40 – Normas IEEE 802.11 ilustrando a camada MAC e os seus métodos [70].**

#### *3.2.3.2. Tramas da camada MAC*

A camada MAC é constituída por três tipos de tramas que são os seguintes:

- Tramas de Dados: que são usadas para a transmissão de dados;
- Tramas de Controlo: estas tramas permitem efectuar um controlo de acesso ao meio (RTS, CTS, e ACK);
- Tramas de Gestão: esta corresponde à trama que são utilizadas para efectuar trocas de informação de gestão.

Na seguinte figura, está ilustrada o formato de uma trama MAC, contendo os seus principais campos. A camada MAC é composta por um cabeçalho (*MAC Header*), pelo conteúdo (*Frame Body*) e por um campo utilizado para verificação de redundância cíclica (*Frame Check Sequence*), conforme podemos observar na seguinte figura.

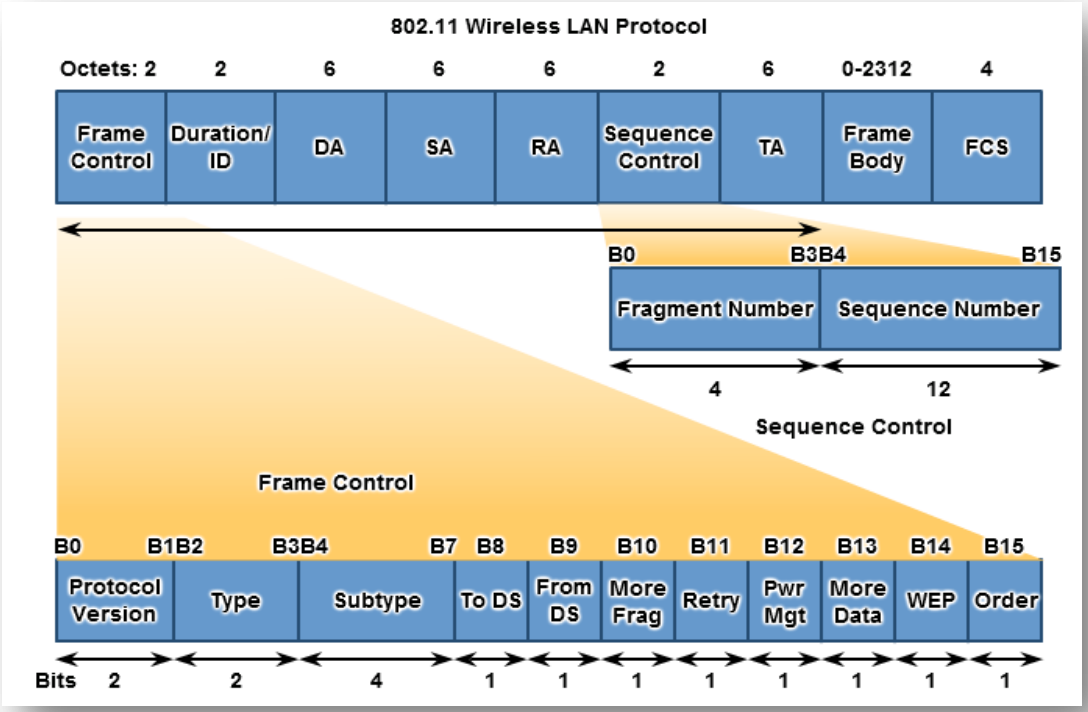



**Figura 41 – Exemplo de uma trama MAC das normas IEEE 802.11 [31].**

### Descrição dos campos do cabeçalho MAC

- *Duration/ID*: Nas tramas do tipo *Power Save Poll* o campo contém a identidade da associação da estação emissora. Nos outros tipos de tramas indica a duração até à transmissão da próxima trama.
- Campos de Endereço (DA, SA, RA, TA): Combinação dos seguintes tipos de endereços:
  - BSSID: No caso de uma rede em modo de Infra-estrutura é o endereço MAC do AP. No caso de uma rede em modo *Ad-Hoc* é o endereço MAC alocado pela estação que cria a rede;
  - DA (*Destination Address*): este campo corresponde ao endereço MAC da estação de destino final da trama;
  - SA (*Source Address*): corresponde ao endereço MAC da estação que criou a trama;
  - RA (*Receiver Address*): este campo permite identificar o endereço MAC da próxima estação a receber a trama;

  - TA (*Transmitter Address*): corresponderá ao endereço MAC da estação que emitiu a trama;

- *Sequence Control*: Este campo corresponde à área de controlo de sequências de números e é composto pelos seguintes campos:
  - *Sequence Number* (12 bit): este campo permite identificar o número de sequência de cada trama, sendo igual em todas as tramas fragmentadas. É incrementado até ao seu valor máximo (4095);
  - *Fragment Number* (4 bit): permite identificar o número do fragmento no caso das tramas fragmentadas, iniciando no valor zero.
- FCS (*Frame Check Sequence*): este campo é um CRC (*Cyclic Redundancy Check*) calculado sobre todos os campos do cabeçalho e conteúdo da trama. É utilizado para a estação receptora verificar a integridade da trama.
- *Frame Control*: este campo é composto pelos seguintes campos ou *flags*:
  - *Protocol Version*: Identifica a versão do protocolo usada. As estações usam este campo para determinar se deverão ou não descartar a trama.
  - *Type*: Indica o tipo de trama: Trama de Dados, Trama de Controlo ou Trama de Gestão.
  - *Subtype*: Indica o subtipo da trama.
  - *To DS*: Toma o valor 1 em tramas que são destinadas ao sistema de distribuição.
  - *From DS*: Toma o valor 1 em tramas com origem no sistema de distribuição.
  - *More Frag*: Indica que irão chegar mais fragmentos pertencentes a esta trama.
  - *Retry*: Indica que a trama é de uma retransmissão.
  - *Pwr Mgt*: Indica se a estação que enviou a trama está no modo de baixo consumo (*Power Save*).
  - *More Data*: Indica a uma estação que se encontra em modo de baixo consumo (*Power Save*) que virão mais tramas.
  - *WEP (Wired Equivalent Privacy)*: Indica que o conteúdo da trama está encriptado.

- *Order*: Indica que as tramas recebidas terão que ser processadas pelo seu número de sequência.

### *3.2.4. Segurança nas Redes Wi-Fi*

Conforme já tinha sido abordado no capitulo 2, o aspecto da segurança nas redes de tecnologia 802.11, é um assunto de extrema importância que não poderá ser em modo algum ignorado e/ou desprezado, devido ao facto da existência de um canal de comunicação partilhado pelas redes *Wi-Fi*.

São três os principais protocolos de segurança utilizados nesta tecnologia:

- WEP (*Wired Equivalent Privacy*);
- WPA (*Wi-Fi Protected Access*);
- WPA2 (*Wi-Fi Protected Access 2*).

Entretanto, importa salientar que, poderão existir outras medidas alternativas e/ou adicionais que podem garantir uma melhor segurança das redes *wireless*, tais como: o uso do *firewall*, VPN, *MAC Address Filtering*, etc.

#### *3.2.4.1. WEP (Wired Equivalent Privacy)*

O protocolo WEP (*Wired Equivalent Privacy*) foi inicialmente desenvolvido pelo IEEE, como sendo um algoritmo de encriptação com o intuito de dar uma maior segurança na comunicação entre os dispositivos que utilizam a tecnologia IEEE 802.11, durante o processo de autenticação, protecção e fiabilidade.

O WEP destina-se a fornecer segurança ao encriptar os dados através de ondas de rádio de forma a ficarem protegidos à medida que forem transmitidos de um ponto para outro. É utilizada uma chave partilhada (semelhante a uma palavra-chave) para permitir a comunicação entre os computadores e o router. O protocolo WEP proporciona um nível de segurança básico, mas satisfatório, para transmissão de dados sem fios.

#### *3.2.4.2. WPA (Wi-Fi Protected Access)*

O protocolo WPA (*Wi-Fi Protected Access*) é um protocolo de segurança para redes sem fios baseado no protocolo WEP. Este protocolo garante uma protecção da transmissão de dados nas redes sem fios, utilizando uma chave semelhante ao WEP, mas a eficácia acrescida do WPA resulta na alteração dinâmica da chave. Devido a essa alteração da chave, este processo torna muito mais difícil o trabalho para um pirata informático na tentativa de obter uma determinada chave e ter acesso à uma respectiva rede.

Este protocolo permite ainda, a utilização do algoritmo de encriptação TKIP (*Temporal Key Integrity Protocol*), que alterar periodicamente a chave de encriptação, tornando-a mais difícil de descodificar.

O WEP permite também utilizar de uma forma opcional o algoritmo AES (*Advanced Encryption Standard*) que é um método de encriptação que utiliza um conjunto de chaves encriptadas até 256 bits para proteger os dados ou encriptação de dados em blocos de 128 bits.

O protocolo WEP é constituído pelos seguintes modos de operação:

- *WPA-Enterprise*: este modo corresponde a uma versão do protocolo WPA que utiliza as mesmas chaves dinâmicas que o *WPA-Personal* e requer que cada dispositivo sem fios seja autorizado em conformidade com uma lista existente num servidor de autenticação específico;
- *WPA-Personal*: este modo corresponde à versão do WPA que utiliza chaves de encriptação longas e constantemente alteradas para dificultar a respectiva descodificação.

#### *3.2.4.3. WPA2 (Wi-Fi Protected Access 2)*

O protocolo WPA2 (*Wi-Fi Protected Access 2*) é a segunda geração de segurança WPA e proporciona um mecanismo de encriptação mais forte através de AES (*Advanced Encryption Standard*), requisito para alguns utilizadores governamentais.

#### *3.2.4.4. Firewalls*

O *Firewall* corresponde a conjunto de esquemas de segurança que permitem aplicar uma política de segurança a um determinado ponto de controlo da rede. Este equipamento tem como objectivo principal regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.

È de salientar que, o nível de complexidade de instalação dessa aplicação depende não só do tamanho da rede, como também, da política de segurança, da quantidade de regras que autorizam o fluxo de entrada e saída de informações, e do grau de segurança desejado pelos potenciais utilizadores dessa tecnologia.

#### *3.2.4.5. VPN*

VPN (Rede privada virtual) corresponde à uma medida de segurança, que permite efectuar uma protecção de dados à medida que saem de uma rede e se dirigem para outra através da Internet.

Uma VPN é uma rede de computadores em que algumas das ligações entre *peers,* são efectuadas através de ligações abertas ou circuitos virtuais em redes, como por exemplo a Internet, em vez de usarem circuitos dedicados.

Uma aplicação comum permite estabelecer comunicações seguras através da Internet pública, mas uma VPN não necessita de possuir funcionalidades explícitas de segurança, como a autenticação ou cifragem dos conteúdos.

Esta rede poderá ser usada para separar o tráfego de diferentes comunidades de utilizadores através de uma rede subjacente com elevadas características de segurança.

Uma VPN permite assim deste modo aos utilizadores de uma determinada rede comunitária, um acesso remoto à rede para aceder ao seu computador de casa e fazer um *download* de um determinado ficheiro contido nessa rede.

Um outro exemplo prático da utilização do VPN, é por exemplo, se por acaso a rede comunitária possuir um sistema de vigilância IP, o utilizador poderá aceder às páginas internas das câmaras para visualizar o conteúdo vídeo em directo, através da utilização de uma VPN.

A seguir estão apresentados alguns cenários de utilização de VPN nas redes comunitárias, ilustrando os vários tipos de ligação entre os equipamentos disponíveis numa determinada rede.

- Ligação estabelecida através de um acesso remoto:

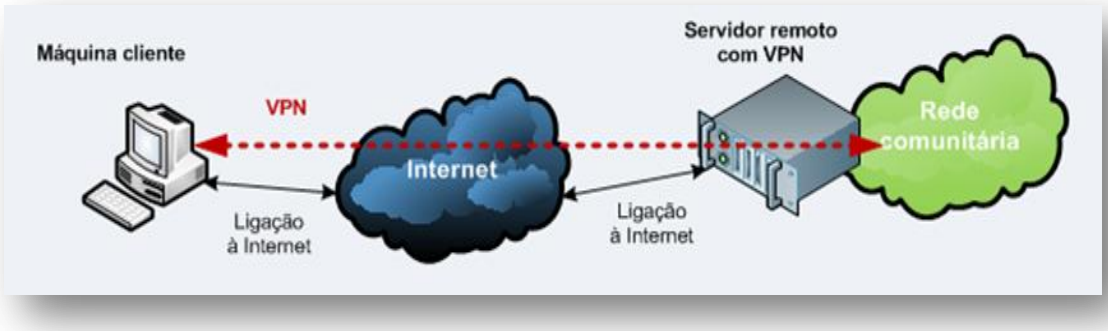



**Figura 42 – Ligação à rede VPN usando um acesso remoto [48].**

- Ligação de redes locais remotas pela rede internet:

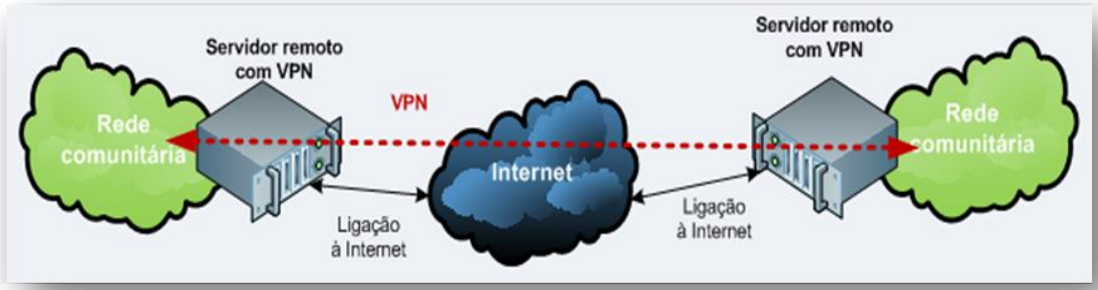



**Figura 43 – Ligação de redes locais remotas pela internet [48].**

- Ligação de um computador numa rede internet:

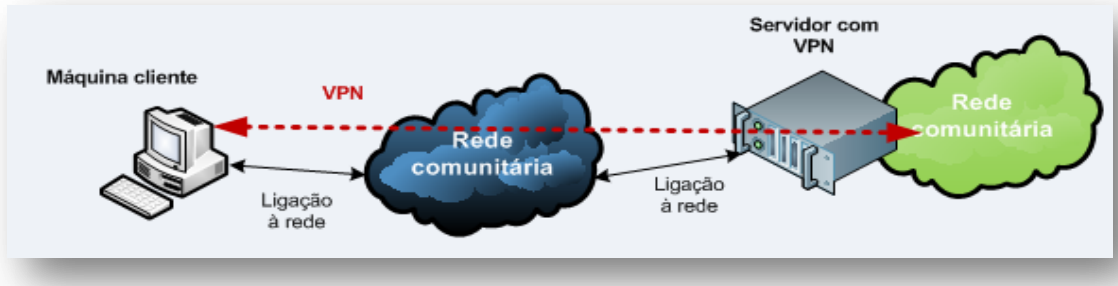



**Figura 44 – Ligação de um computador numa rede internet [48].**

#### *3.2.4.6. MAC Address Filtering*

O processo *MAC Address Filtering* permite efectuar uma fazer filtragem de endereços físicos, no AP (*Access Point*) para placas de rede autorizadas.

### *3.2.5. Vantagens e Desvantagens da utilização de uma Rede Wi-Fi*

Neste ponto, serão descritas algumas vantagens e desvantagens no uso de uma rede baseada na tecnologia *Wi-Fi*.

#### *3.2.5.1. Vantagens*

Relativamente ao uso das redes baseadas em tecnologias *Wi-Fi*, podem ser apresentadas as seguintes as vantagens:

- Redução de custos: Menor custo de instalação e exploração dos equipamentos;

- Produtividade: permite ao utilizador aceder toda a informação crítica para o seu negócio com uma maior rapidez e eficácia;
- Flexibilidade e Mobilidade total: permite ao utilizador ter um acesso flexível e com uma mobilidade total aos seus equipamentos em determinadas áreas que contenham a cobertura da rede *Wi-Fi*;
- Rapidez e Acessibilidade: permite ao utilizador estar sempre online onde quer que esteja;
- Internet de banda larga: débitos até 54 Mbps.
- Maior rapidez de instalação e distribuição;
- Convergência tecnológica num futuro próximo.

#### *3.2.5.2. Desvantagens*

A seguir estão descritas algumas das desvantagens de uma rede que usa a tecnologia *Wi-Fi*:

- Menor imunidade a interferências e escutas,
- Aumento da energia electromagnética com consequências para a saúde ainda desconhecidas;
- Menores larguras de banda actualmente disponíveis.

### *3.3. Redes Mesh*

As redes *Wi-Fi Mesh* ou redes *Mesh* Sem Fios (*Wireless Mesh Network, WMN*) são redes de comunicações compostas por vários nós rádio que se comportam como uma única e grande rede. Cada um deles pode encaminhar tramas e cada nó está ligado a um ou mais nós, possibilitando a transmissão de tramas por caminhos diferentes, oferecendo uma certa redundância à rede. Contudo, a área de cobertura desses nós torna-se uma nuvem, denominada por *Mesh Cloud* e o seu acesso torna-se possível porque, os respectivos nós, trabalham em harmonia uns com os outros, tornando possível a criação de uma rede muito fiável e que oferece uma certa redundância.

Esta nova tecnologia futuramente poderá não só mudar a nossa vida, como também, o nosso quotidiano. A tecnologia *Mesh* sem fios, apesar de existir já há algum tempo, nunca teve um papel tão importante como recentemente. Com o aumento da popularidade das redes *Mesh* sem fios, os utilizadores finais passaram a solicitar uma maior largura de banda, uma melhor cobertura e uma melhor fiabilidade de modo a satisfazer todas as suas necessidades.

As redes *Wireless Mesh* têm se tornado um novo estímulo económico para as pequenas e médias empresas a nível mundial e em determinados ramos empresariais.

Actualmente, muitos países estão anunciando grandes iniciativas baseadas na tecnologia *Wi-Fi* não só ao nível das cidades metropolitanas, como também ao nível municipal, fornecendo à população um acesso grátis à internet de banda larga. Importa salientar que, essas iniciativas visam combater à infoexclusão, promovendo a igualdade de oportunidades e de acesso público à banda larga na região, corrigir assimetrias de acessibilidade a telecomunicações, e desenvolver a iniciativa empresarial de base tecnológica e científica na região. Em geral ligam as sedes dos concelhos abrangidos, edifícios públicos e de interesse público, instituições do ensino superior, centros tecnológicos, e zonas e parques industriais.

Em *Bangladesh*, mais concretamente em *Chittagong* por exemplo, uma rede *wireless Mesh* fornecerá a todas as pessoas da referida cidade um acesso grátis à internet usando tecnologias VoIP.

Em Portugal, essas iniciativas são consideradas como sendo uma prioridade nacional, e como exemplo, passo a citar o projecto “Programa Cidades Digitais”, que está inserido na iniciativa “Redes Comunitárias de Banda Larga”. Como um exemplo prático do uso desta nova tecnologia ao nível do território nacional é o projecto-piloto uma rede *Wi-Fi* na cidade de Mirandela [133] que já foi testada e vai na 2ª fase de implementação. Importa salientar que, este projecto é uma parceria entre a Câmara Municipal de Mirandela e a empresa *NuanceView*, cujos responsáveis máximos são alguns jovens da respectiva cidade. Actualmente já existem 14 pontos de acesso (AP), localizados no centro da referida cidade, sendo que qualquer munícipe, turista ou visitante poderá aceder à Internet, enviar/receber e-mail, na rua, na esplanada ou mesmo num banco de um jardim, de uma forma gratuita.

É de referir que, mesmo sendo as WMNs tão populares, ainda não existe actualmente um *standard* oficial definido e aprovado. Mas contudo, devido à forte procura desta tecnologia no mercado empresarial e não só, o IEEE (*Institute of Electrical and Electronics Engineers*) em colaboração com uma vasta equipa de investigadores, têm vindo a desenvolver um standard especificamente para as WMNs. Saliento ainda que, essa equipa de investigadores foi denominada por *Task Group* (TG) “S”, cujo nome de código é 802.11s para reformular a norma IEEE 802.11.

As redes *Mesh* têm algumas semelhanças em relação às redes móveis *Ad-Hoc* (*Mobile Ad-Hoc NETworks, ou MANETs*), visto que, possuem os mesmos princípios de funcionamento, porém, funcionam no nível 2 da camada OSI (*Open Systems Interconnection*), usando endereços MAC. Para a descoberta de caminhos

entre os nós, o 802.11s recorre a adaptações de protocolos de *routing*. Estas redes suportam também a interligação com redes estruturadas através de *gateways*.

### *3.3.1. Arquitectura das Redes Mesh*

A arquitectura de uma rede *Mesh* é baseada integralmente na tecnologia IEEE 802.11. Mas contudo, usa comunicações do tipo *multi-hop* para efectuar o encaminhamento de todo o tráfego de pacotes contidos na rede, não só para diferentes pontos de Internet com fio, como também, para todos nós existentes e diferentes redes *Mesh*. A rede *Mesh* sem fios usa a camada física e o acesso ao meio (MAC) do protocolo 802.11 para fornecer funcionalidades de uma rede *Mesh*.

Na figura a seguir, está ilustrada um exemplo de uma arquitectura básica da rede *Mesh*, apresentando os componentes principais da mesma.

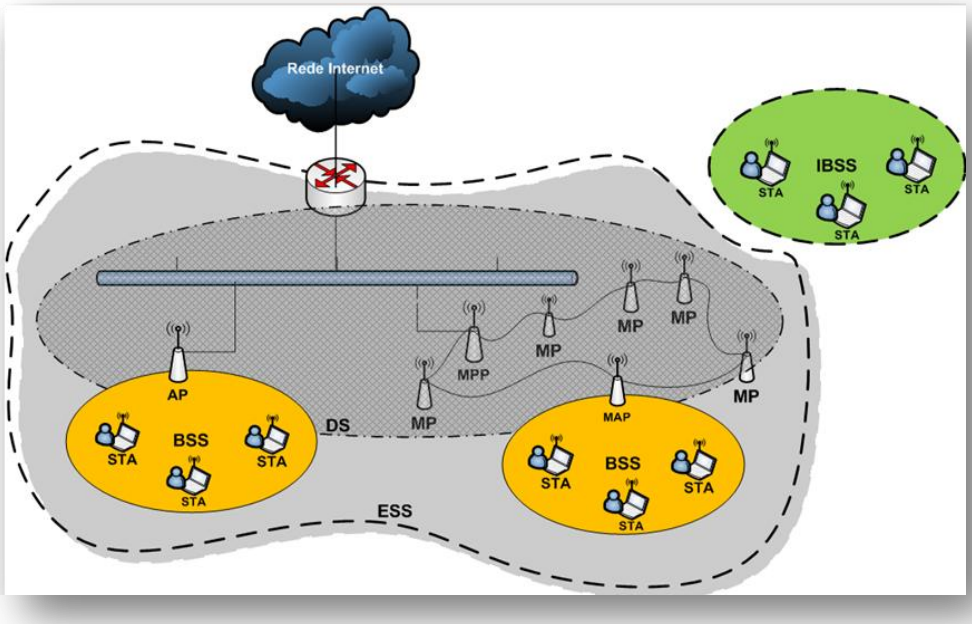



**Figura 45 – Arquitectura de uma Rede Mesh. Adaptado de [106].**

**Funcionamento básico**

Como podemos observar na figura anterior o modo de funcionamento básico de uma arquitectura de uma rede *Mesh* é feita do seguinte modo:

- Todas as estações que estão localizadas na mesma frequência de rádio partilham um *Basic Service Set* (BSS) IEEE 802.11, que consiste em ter um AP (*Access Point*) imóvel e nas STAs (*Stations*). Entretanto para garantir uma maior cobertura da área, será necessário um *Extended Service Set* (ESS), que é formado por vários APs interligados por um *Distribution Service* (DS), sendo

que normalmente é uma rede cablada. A norma IEEE 802.11s permite introduzir novos elementos ao ESS, tais como, o *Mesh Point* (MP), o *Mesh Access Point* (MAP) e *Mesh Portal* (MPP).

- O *Access Point 802.11*, conhecido como *Mesh Point* (MP), irá estabelecer ligações sem fios uns com os outros, de modo a permitir não só uma aprendizagem automática da topologia da respectiva rede, como também, uma configuração dinâmica dos caminhos para trocarem dados entre si. As ligações entre cada um dos MPs criam um *backbone* sem fios, que irão fornecer aos utilizadores, um custo bastante reduzido e económico, uma largura de banda elevada e serviços de interligação multi-salto sem falhas com um número limitado de pontos de entrada de Internet e interligação com outros utilizadores dentro da rede. Cada MP poderá, de uma forma opcional, fornecer serviços que permitam estabelecer uma comunicação com as estações 802.11, denominadas por *legacy mobile stations* (STAs). Estes dispositivos são denominados por *Mesh Access Points* (MAPs). Os MAPs têm, portanto, exactamente a mesma funcionalidade de um MP, mas contudo, fornecem serviços BSS que irá permitir um suporte, à comunicação com os STAs. Os *Mesh Access Points* desempenham um papel fundamental no protocolo IEEE 802.11s, visto que, estes dispositivos permitem a retro-compatibilidade.
- Os MPPs são MPs que permitem um *bridging* entre a rede *Mesh* e a rede cablada. Entretanto, existe um dispositivo extra e de inferior relevo, denominado por *Light Weight MP* (LWMP), que participa principalmente na comunicação dos serviços de ligação entre vizinhos.

Na seguinte figura está ilustrada um exemplo de uma possível relação entre os diferentes tipos de nós *Mesh*.

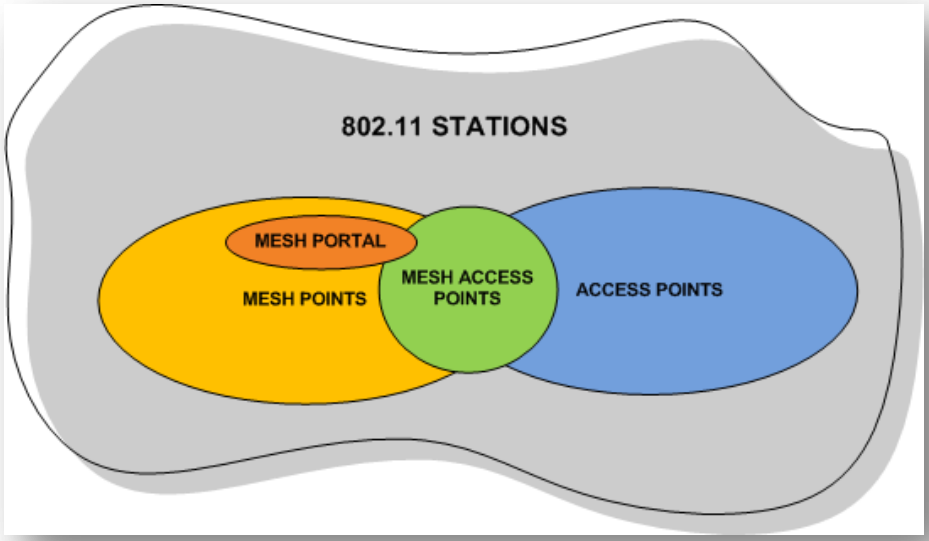



**Figura 46 – Exemplo de relação entre diferentes tipos de nós da Rede Mesh.**

O *Mesh Point* poderá ser configurado como sendo um *root* MP. Um *root* MP irá estabelecer uma política de manutenção de rotas, enviando um *Root Announcement* de uma forma periódica, informando aos restantes MPs.

Estes por sua vez, poderão responder-lhe permitindo assim ao *root* MP ter uma visão global de todos os componentes existentes na rede. O protocolo IEEE 802.11s foi desenvolvido para permitir um tamanho de 32 MPs.

### *3.3.2. Camada MAC das Redes Mesh*

Dado ao facto de que, o protocolo IEEE 802.11s corresponde à uma extensão do IEEE 802.11, a sua estrutura dos 3 tipos de tramas da sua camada MAC (tramas de dados, tramas de controlo e tramas de gestão) usadas são iguais, conforme foi citado no capítulo 3.2.3.2. O protocolo IEEE 802.11s possui novas tramas que são diferenciadas através de um campo pré-anexado no *Body* que em conjunto com o *Frame Control* (campos *Type* e *Subtype*) retiram qualquer tipo de ambiguidade ao tipo de trama que representa.

#### *3.3.2.1. Tipo de tramas das Redes Mesh*

Como já foi anteriormente citado a camada MAC de uma rede *Mesh* é constituída por três tipos de tramas que são os seguintes:

#### 3.3.2.1.1. Trama de Dados

A trama de dados do protocolo IEEE 802.11s possui uma estrutura idêntica à trama do mesmo tipo IEEE 802.11, permitindo assim uma compatibilidade com o protocolo IEEE 802.11.

Contudo possui alguma diferença no campo *Body* que é ligeiramente modificado, visto que, foi adicionado mais um campo denominado por *Mesh Header*, que irá permitir, o uso de até 6 endereços MAC entre outras coisas.

Existem também algumas alterações relativamente ao campo *Frame Control*, os subcampos *Type* e *Subtype*, visto que, foram alterados para definir as tramas de dados relacionados com a rede *Mesh*.

Na seguinte figura, está ilustrada o formato de uma trama de dados de uma rede *Mesh* contendo os seus principais campos.

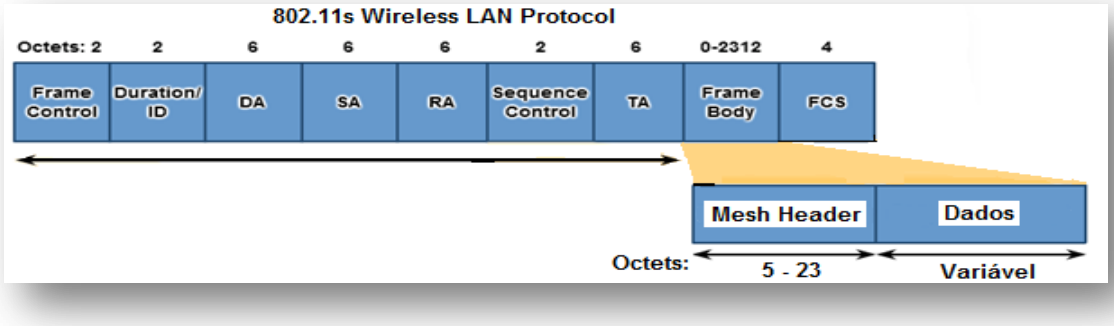



**Figura 47 – Trama MAC de dados da norma IEEE 802.11s. Adaptado de [31].**

#### 3.3.2.1.2. Trama de Controlo

Relativamente às tramas MAC de controlo da norma IEEE 802.11s, elas são utilizadas para o controlo de acesso ao meio, e não sofreram nenhum tipo de alteração.

#### 3.3.2.1.3. Trama de Gestão

No que diz respeito à trama MAC de gestão da norma IEEE 802.11s possui uma estrutura idêntica à trama do mesmo tipo IEEE 802.11, permitindo assim uma compatibilidade entre protocolo IEEE 802.11.

Contudo possui alguma diferença no campo *Body* que é ligeiramente modificado, visto que, foi adicionado mais um campo denominado por *Mesh Header*, que irá permitir, o uso de até 6 endereços MAC entre outras coisas.

Existem também algumas alterações relativamente ao campo *Frame Control*, os subcampos *Type* e *Subtype*, visto que, variam conforme o tipo de trama. Assim sendo, quando a trama é do subtipo *Action* será sempre necessário adicionar o campo

*Action Field,* depois do campo *Mesh Header* de modo a que se possa ser efectuada uma distinção e utilização das diversas tramas do tipo *Action*.

Na seguinte figura, está ilustrada o formato de uma trama MAC de gestão de uma rede *Mesh* contendo os seus principais campos.

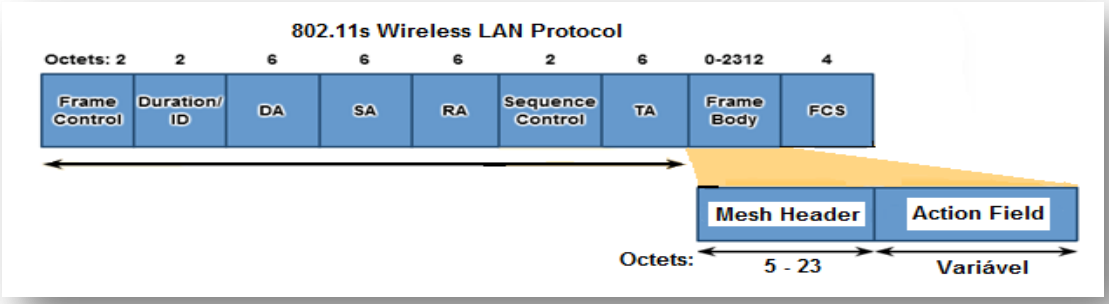



**Figura 48 – Trama MAC de gestão da norma IEEE 802.11s. Adaptado de [31].**

### *3.3.3. Protocolos de encaminhamento*

Neste ponto, será apresentado um breve estudo sobre os protocolos da tecnologia *Mesh* com o intuito em transmitir alguns conhecimentos gerais acerca das características e funcionalidades de cada um dos protocolos associados à essa tecnologia.

Importa salientar que, os protocolos da tecnologia *Mesh*, podem ser divididos em duas categorias relativamente ao nível de protocolos de encaminhamento: *Unicast* e *Multicast.*

#### *3.3.3.1. Protocolo Unicast*

O protocolo de encaminhamento *Unicast* poderá ser dividido em três subcategorias, de acordo com a forma com que o algoritmo faz a construção de uma determinada rota:

- **Pró-activos**: neste tipo de protocolo, os próprios nós mantém informações sobre a topologia da rede e trocam estas informações regularmente, por difusão para toda a rede. Estas informações serão utilizadas, por um algoritmo apropriado para construir e determinar a melhor rota entre destino e origem. Neste caso, não haverá nenhuma perda de tempo realizando uma busca para a rota. Contudo, é de salientar que, este método é pouco eficiente nos casos em que há um número elevado de nós ou uma taxa alta de mobilidade. Os principais protocolos de encaminhamento *unicast* pró-activos são: WRP

(*Wireless Routing Protocol*), DSDV (*Destination-Sequenced Distance-Vector*), OLSR (*Optimized Link State Routing*).

- **Reactivos:** os protocolos de encaminhamento que pertencem a esta subcategoria, não trocam informações optando por obter o caminho entre os nós somente quando necessário. O algoritmo define o processo de descoberta da rota. Neste caso há um *overhead* menor comparado ao anterior, porém introduz um atraso sempre que for necessário descobrir uma rota. Os principais protocolos de encaminhamento *unicast* reactivos são: DSR (*Dynamic Source Routing*), AODV (*Ad-Hoc On-Demand Distance Vector*).
- **Híbridos:** visa combinar as melhores qualidades dos anteriores. Existem zonas de encaminhamento delimitadas por certas distâncias de um determinado nó. São então aplicadas metodologias entre as características dos protocolos reactivos ou pró-activos dependendo se o nó está dentro ou fora da região. Os principais protocolos de encaminhamento *unicast* híbridos são: ZRP (*Zone Routing Protocol*), CEDAR (*Core Extraction Distributed Ad-Hoc Routing*) [63].

#### *3.3.3.2. Protocolo Multicast*

O protocolo de encaminhamento *Multicast* está dividido em duas subcategorias:

- ***Tree-based*:** neste caso só existe um caminho entre um nó origem e um nó destino e, portanto, protocolos deste tipo são muito eficientes no quesito vazão dos dados. A característica principal deste tipo de protocolo é a formação de uma pseudo-árvore de *Multicast*, composta dos membros do grupo de *multicast* com a possibilidade de haver alguns não membros também. Quando um nó da rede transmite um pacote, cada nó da árvore o encaminha por um nó, conhecido como nó *downstream*, e o recebe por outro nó, conhecido como nó *upstream* [63]. Representantes desta categoria são: MAODV (*Multicast Ad-Hoc On-Demand Distance Vector*), uma extensão do protocolo *unicast* AODV, AMRoute (*Ad-Hoc Multicast Routing Protocol*), MOLSR (*Multicast Optimized Link State Routing*), uma extensão do protocolo *unicast* OLSR, e MZRP (*Multicast Zone Routing Protocol*), uma extensão do protocolo *unicast* ZRP [63].
- ***Mesh-based*:** neste caso existem múltiplos caminhos entre um nó origem e um nó destino e, por este motivo, esse tipo de protocolo apresenta grande robustez. É usada uma trama *Multicast*, que é mais capaz de se adaptar ao dinamismo de uma rede *Ad-Hoc*. Em contrapartida, apresentam um consumo

mais elevado de recursos. Representantes dessa categoria são: ODMRP (*On-Demand Multicast Routing Protocol*), DCMP (*Dynamic Core-Based Multicast Routing Protocol*).

### *3.3.4. Vantagens e Desvantagens da utilização de uma Rede Mesh*

Neste ponto, serão descritas algumas vantagens e desvantagens no uso de uma rede baseada na tecnologia *Mesh*.

#### *3.3.4.1. Vantagens*

Relativamente ao uso das redes baseadas em tecnologias *Mesh*, podem ser apresentadas as seguintes as vantagens:

- Formação automática: São capazes de se formarem automaticamente, pois uma vez um nó configurado e activado ele gere-se autonomamente;
- Tolerância a falha: Se no caso existirem rotas redundantes numa deteminada rede, a informação flui de forma ininterrupta caso um nó falhe. Sempre que tal ocorra, será recalculada de uma forma dinâmica a rota dos dados através do próximo nó disponível;
- Auto-reconstrutora: Se um nó volta ao activo, integra-se de forma automática e transparente na rede;
- Comunitária: A rede pertence à comunidade, pois não tem um ponto central de gestão do qual possa depender;
- Baixo custo: Os nós de uma rede *Mesh* têm um baixo custo. Normalmente são baseados em produtos comerciais *off-the-shelf* adaptados. Caso seja necessário efectuar alguma modificação nesses nós, não o administrador da rede não terá nenhum custo associado à esta alteração, visto que, os respectivos nós são manipulados por um *software* adquado para o efeito.
- Custo incremental da expansão é baixo: Um novo nó na rede tem um custo marginal quando comparado com o valor acrescentado que traz à mesma.
- Fácil implementação: Uma rede *Wi-Fi Mesh* é simples de planear, implementar e manter.

#### *3.3.4.2. Desvantagens*

Uma das desvantagens da utilização das redes *Mesh* é porque cada fabricante tem o seu protocolo de *Mesh*;

### *3.3.5. Cenários de Implementação*

A seguir estão descritos os possíveis cenários de implementação de uma rede *Mesh*:

#### *3.3.5.1. Rede doméstica com acesso a banda larga*

As redes *Mesh* substituiriam as tradicionais redes 802.11, onde os *router Mesh* entrariam no lugar dos tradicionais APs (pontos de acesso). As vantagens são várias, sendo que não haverá a necessidade interligação de cabos entre os equipamentos e o que possibilitará uma melhor cobertura de rede nas zonas onde não haja uma melhor propagação dos sinais, visto que, apenas será necessário trocar os *router* de lugar ou auto-configurar a potência deles.

Além disso, como os nós estarão se comunicando directamente via rede sem fio, não há sobrecarga de *Hubs* no caso da comunicação entre pontos de acesso.


**Figura 49 – Exemplo de uma Rede Mesh Domiciliária [63].**

#### *3.3.5.2. Rede de acesso comunitário*

O acesso comunitário ou entre vizinhos utilizando redes *Mesh* é a melhor solução, pois permite sistemas de arquivo distribuídos, partilha de arquivos e *streaming* de vídeo. Com as soluções existentes todo tráfego teria que passar pela internet através de linhas ADSL, por exemplo. Ou ainda, a utilização de redes sem fio tradicionais teria que ser configurada manualmente em cada nó, além de depender de suas contribuições individuais para o encaminhamento e diversas vezes de caminhos únicos.

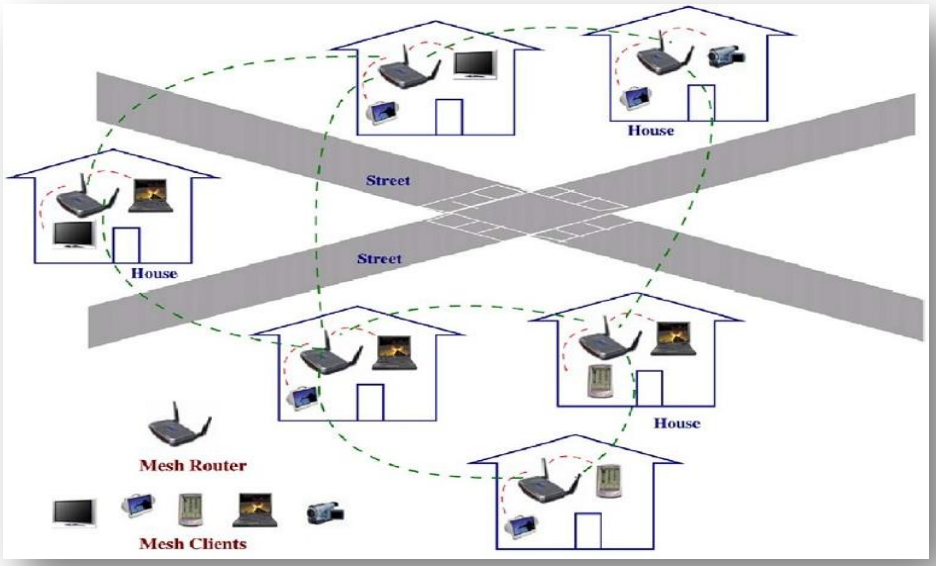



**Figura 50 – Exemplo de uma Rede Mesh Comunitária [63].**

#### *3.3.5.3. Redes empresariais*

No contexto das pequenas e médias empresas, onde a conexão poderá ser efectuada dentro de um ou vários edifícios ou, a utilização das redes *Mesh* irá possibilitar uma diminuição de custos financeiros, visto que, com a implementação desta tecnologia nas empresas a utilização das redes com conexões *Ethernet* torna-se desnecessária perante as redes *wireless* isoladas que encarecem a rede, além de aumentar a tolerância da rede a falhas na rede, sem prejudicar toda a rede da empresa em questão.

Além disso, conforme a empresa expandir e houver a necessidade da inclusão de novos equipamentos na rede, não haverá problemas para manter a rede funcionando sem a necessidade de uma reconfiguração.

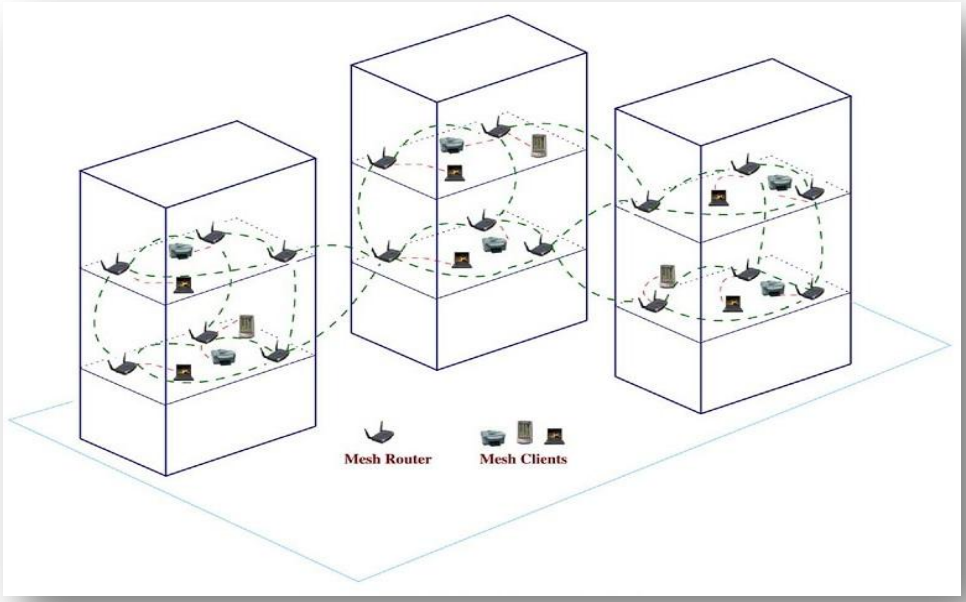



**Figura 51 – Exemplo de uma Rede Mesh Empresarial [63].**

#### *3.3.5.4. Redes metropolitanas*

Actualmente existe um número cada vez maior de *hotspots* em diversos locais, tais como, restaurantes, centro comerciais, livrarias, locais públicos, etc. Uma rede *Mesh*, como foi dito anteriormente, poderia efectuar uma interligação entre todos esses *hotspots*, e incluir novos *router Mesh*, a fim de criar uma rede para todo o município.

Esse tipo de rede é uma alternativa de baixo custo para redes metropolitanas pois não há a necessidade de utilização de redes cabladas para interligar toda a rede.

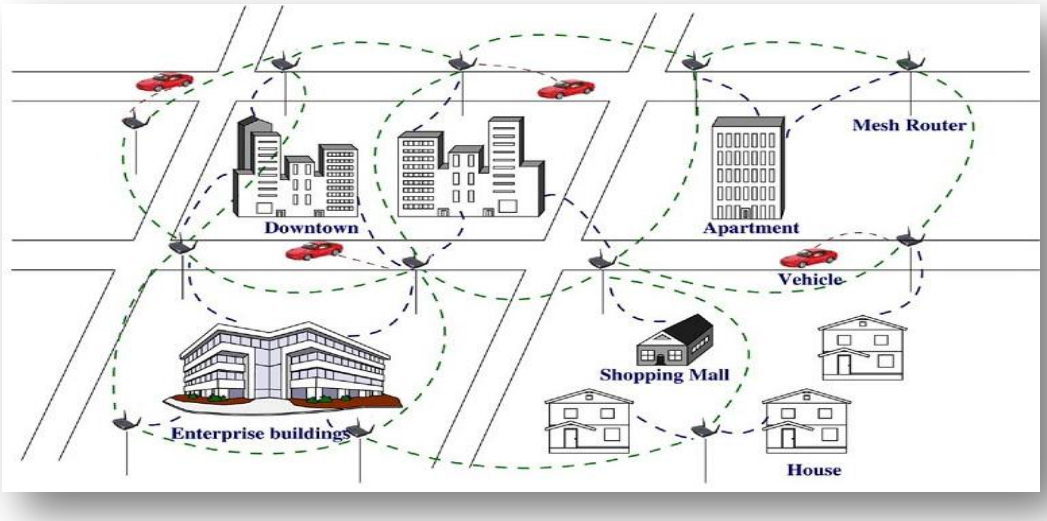



**Figura 52 – Exemplo de uma Rede Mesh Metropolitana [63].**

### *3.3.6. Projectos-piloto que usam a tecnologia VoIP em Redes Mesh*

Neste ponto será apresentado alguns exemplos de projectos-piloto que usam a tecnologia VoIP para as redes comunitárias baseando na tecnologia *Mesh*, quanto ao nível académico, comercial e empresarial.

#### *3.3.6.1. Nível Académico*

Relativamente aos projectos académicos podem-se destacar os seguintes:

##### *3.3.6.1.1. ReMesh*

O projecto *ReMesh* foi desenvolvido e implementado na Universidade Federal Fluminense como um Grupo de Trabalho da RNP (Rede Nacional de Ensino e Pesquisa ). O referido projecto tinha como objectivo principal, estudar as questões envolvidas em redes sem fio de larga escala, e viabilizar o acesso banda larga de baixo custo aos seus potenciais utilizadores.

O *ReMesh* foi o primeiro projecto-piloto desenvolvido pela comunidade universitária brasileira com sucesso na construção de redes *Mesh* [127].

##### *3.3.6.1.2. VMesh*

O projecto *VMesh* foi desenvolvido na Universidade de *Thessaly* na Grécia, com o intuito de implementar uma rede *Mesh* de baixo custo, de modo a permitir aos estudantes, funcionários e professores não só um acesso remoto e directo aos servidores da referida instituição, como também, um acesso à internet permitindo-lhes criar plataforma de testes para pesquisa e avaliação de algoritmos e programas na área de redes e sistemas distribuídos. Foram utilizados vários pontos de acesso com o auxílio dos equipamentos da *Linksys,* nomeadamente os *router WRT54G* com sistema operacional *OpenWRT*, adaptando-lhes às antenas omnidireccionais [128].

##### *3.3.6.1.3. Roofnet*

O projecto Roofnet foi implementado pelo Laboratório de Ciência da Computação e Inteligência Artificial do MIT (Instituto de Tecnologia de *Massachusetts*), tendo como objectivo principal o estudo das características do padrão IEEE 802.11, tais como, perdas de pacotes, rotas de maior *throughput* para ambientes de altas perdas [129].

#### *3.3.6.1.4. Meshnet*

Este projecto foi desenvolvido no campus universitário da Universidade da Califórnia, nomeadamente, na *"Santa Bárbara Mesh Testbed"*. Foram utilizados os *router Linksys WRT54G*, para efectuar uma interligação com a rede universitária, utilizando um gateway *Mesh* da Intel.

O projecto *Meshnet* tinha como objectivo principal o desenvolvimento de protocolos para aplicações robustas em redes sem fio *multpath* [130].

### *3.3.6.2. Nível Comercial e Empresarial*

Nas últimas décadas face ao desenvolvimento tecnológico, vários centros de pesquisa e universidades ao nível mundial vêm desenvolvendo e implementando redes sem fio com o intuito de fornecer uma comunicação ubíqua dentro de um determinado raio de cobertura das redes comunitárias.

Assim sendo, várias empresas multinacionais já efectuaram muitos investimentos em pesquisas para o desenvolvimento da tecnologia *Mesh*.

No que diz respeito à implementação de redes *Mesh*, destacam-se as seguintes empresas: a *CISCO*, a *Microsoft*, a *Nortel* e a *Planet* que já desenvolveram alguns projectos-piloto.

Actualmente, no que refere ao nível comercial, já existem várias iniciativas comerciais de projectos em redes *Mesh* e que já foram implementados um pouco por toda do mundo. Como por exemplo: Filadélfia e *Taipei* (*Nortel Wmesh*); Canadá e Tiradentes (*Cisco Mesh Network*).

## *3.3.7. Equipamentos necessários para a implementação de uma Rede Mesh*

Neste ponto será feita uma breve descrição sobre alguns exemplos de equipamentos que usam a tecnologia *Mesh* e que são necessários para a implementação de uma rede *Mesh* para as redes comunitárias.

#### *3.3.7.1. Hardware*

A seguir serão descritos alguns exemplos de equipamentos de *Hardware* que poderão ser utilizados durante a implementação de uma rede *Mesh* para as redes comunitárias.

##### *3.3.7.1.1. Antenas*

As antenas desempenham um papel muito importante nos sistemas de telecomunicações. Estes equipamentos são responsáveis pela conversão do sinal eléctrico proveniente do transmissor para o meio onde se propagará a onda electromagnética e, posteriormente, desse meio para o receptor.

A eficiência de um sistema de comunicação depende dos sistemas irradiantes e de recepção utilizados. Por este motivo existem diversos modelos de antenas, sendo os mais comuns neste tipo de utilização a antena vertical, dipolo, *Yagi* e parabólica.

A seguir será apresentado uma breve descrição dos tipos de antenas mais utilizados na implementação de uma rede *Mesh*:

###### *3.3.7.1.1.1. Antenas omnidireccionais*

As antenas omnidireccionais são do tipo vertical e as suas ondas electromagnéticas propagam-se em quase todas as direcções. Estes equipamentos possuem um ganho, que situa-se entre os valores típicos de 8 e 13 dBi, com um correspondente ângulo de abertura vertical entre os 6 e os 24 graus.

**Figura 53 – Exemplo de uma Antena Omnidireccional [105].**

Importa salientar que, com este limite na abertura vertical implica que se tenha de ter cuidado na escolha da sua localização, sendo que esta não deverá estar a uma altitude muito elevada em relação à área a servir sob pena dos utilizadores não apanharem sinal. Esta característica agrava-se à medida que o ganho aumenta, pois para aumentar o ganho no plano horizontal diminui-se o ganho no plano vertical.

É de referir que, o ganho nas antenas omnidireccionais tem um efeito semelhante ao de achatar o padrão de irradiação 3D, conforme está ilustrada na seguinte figura.

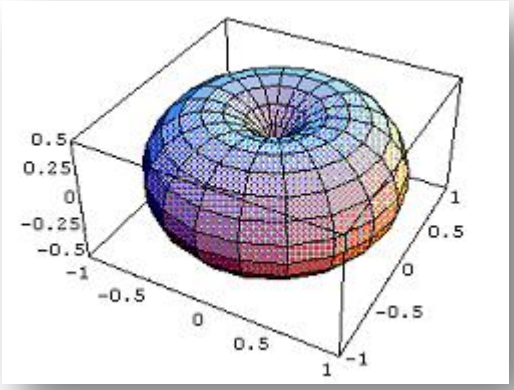



**Figura 54 – Diagrama de irradiação 3D de uma Antena Omnidireccional [105].**

#### *3.3.7.1.1.2. Antenas direccionais de alto ganho*

Estas antenas são do tipo unidireccional e servem para efectuar coberturas em áreas precisas, visto que, possuem um alto ganho que está situado normalmente no intervalo de 10 e os 18 dBi.

Estes equipamentos têm uma abertura vertical e horizontal relativamente baixa, o que permitirá a concentração do sinal numa determinada direcção e são por isso utilizadas para cobrir de forma mais localizada áreas extensas em comprimento e até interligar edifícios ou outros pontos distantes. Como exemplos principais de antenas semi-direccionais temos: as *Yagi* e Painel (*Patch Panel*), sendo que ambas são utilizadas normalmente para efectuar interligação de edifícios em distâncias curtas e médias.

As antenas direccionais *Yagi* têm a típica estrutura das antenas de TV com inúmeros elementos de metal em paralelo a um determinado ângulo desde a base ao extremo. Contudo, importa salientar que, para a norma IEEE 802.11 não se verá este tipo de arquitectura em antenas *Yagi*, visto que, as suas versões comerciais encontram-se fechadas numa redoma de plástico para as proteger dos elementos exteriores.

Na figura a seguir está ilustrada um exemplo de uma antena direccional *Yagi* de alto ganho:

**Figura 55 – Exemplo de uma Antena Direccional Yagi de 16dbi de ganho [105].**

As antenas direccionais em painel têm a vantagem de serem mais discretas, tendo por isso uma maior aceitação dos utilizadores por não causarem grande impacto visual nos edifícios.

Estes tipos de antena recebem muito ruído proveniente de todos os lados, sendo esta característica mais acentuada nas antenas *Yagi*, pelo que não constituem as soluções desejáveis para ligações ponto-a-ponto de grande distância ou com os equipamentos activos próximos de fontes de ruído electromagnético.

Na figura a seguir está ilustrada um exemplo de uma antena direccional em painel contendo um de ganho 18dBi:

**Figura 56 – Exemplo de uma Antena Direccional Patch Panel de 18 dBi de ganho [105].**

#### *3.3.7.1.1.3. Antenas direccionais de ganho muito alto*

Relativamente a estes modelos de antenas as mais eficientes são as parabólicas, visto que, elas possuem alcances muito superiores por direccionarem a maioria da radiação de energia num feixe muito estreito.

O valor típico do seu ângulo de irradiação horizontal costuma situar no intervalo de 7 e 20º, enquanto o vertical entre 3 e 10º. O seu ganho no contexto da tecnologia IEEE 802.11 encontra-se normalmente entre os 18 e os 33 dBi.

Na figura a seguir está ilustrada um exemplo de uma antena direccional de ganho muito alto:

**Figura 57 – Exemplo de uma Antena Direccional exterior de 21 dBi de ganho [105].**

#### *3.3.7.1.2. Computadores*

Estes equipamentos são necessários para que estabelecer a conectividade aos dispositivos clientes da rede, pelo que será necessário haver alguns equipamentos adicionais que serão responsáveis pelo envio e recebimento do sinal/dados.

Estes dispositivos poderão ser um computador pessoal ou um portátil contendo algum tipo de adaptador de rede sem fio, nomeadamente uma Placa *Wireless PCI* ou *Wireless USB* para conectar à internet ou na rede interna de um determinado escritório.

**Figura 58 – Exemplo de um Adaptador Wireless PCI D-Link DWL-G510 [107].**

**Figura 59 – Exemplo de um Adaptador Wireless USB 2.0 D-Link DWL-G122 [107].**

#### *3.3.7.1.3. Cabos*

Os cabos usados para efectuar a interligação entre os pontos de acesso às antenas externas devem ser de baixa perda e de grande robustez para suportar as referidas adversidades do ambiente exterior. Relativamente aos preços dos cabos há uma variação do preço de acordo com as suas características e as suas qualidades. Mas contudo, deverá ser escolhido o cabo de maior qualidade e com menor perdas de comunicação. Importa salientar que, para manter as perdas ao mínimo deve-se utilizar o mais curto possível, sendo que para este efeito poderá ser estendido o cabo *Ethernet* para se aproximar o AP da antena.

É de referir que, deverá ter-se cuidado com as frequências em que operam, pois, por exemplo, uma comunicação de 2.4 GHz deverá ter um cabo que suporte pelo menos 2.5 GHz. Existem cabos denominados de *Pigtail* que são usados para ligar dispositivos com conectores proprietários a dispositivos com conectores padrão.

Na figura a seguir está ilustrada um exemplo do cabo *Pigtail* com uma ponta de cada tipo de conector, N e SMA.

**Figura 60 – Exemplo de um Cabo Pigtail RG316-SNM-30 [105].**

Preferencialmente um cabo deverá vir cravado de origem, pois a cravagem manual pode permitir não só a fuga de potência de sinal, como a entrada de interferências. Este aspecto é particularmente importante em cabos expostos a ambientes externos onde podem ficar com água. Poderá ainda ser utilizado o cabo *standard CAT5 LAN,* para efectuar ligações entre os equipamentos existentes na rede, conforme podemos observar na seguinte figura:

**Figura 61 – Exemplo de um Cabo standard CAT5 LAN.**

#### *3.3.7.1.4. Protectores contra relâmpagos (lightning protectors)*

Estes equipamentos são utilizados para proteger o equipamento eléctrico das descargas de relâmpagos. Eles são normalmente denominados por *lightning arrestors ou lightning protectors,* e são utilizados para efectuar um desvio na corrente proveniente de relâmpagos para a terra. O relâmpago ao atingir objectos próximos da antena induz na antena picos de corrente. O *lightning protectors*, ao detectar a corrente elevada ioniza imediatamente os gases internos formando um curto-circuito com a terra, permitindo a assim a sua descarga salvaguardando o equipamento.

È de salientar que, nenhum destes dispositivos salva totalmente todo o equipamento da estação em caso do mastro ou antena ser atingido por um relâmpago. O *lightning protectors* consegue redireccionar picos de corrente até 5000 amperes e 50 volts.

Os protectores de relâmpagos devem obedecer a determinadas características, como o facto de respeitarem a norma IEEE, serem reutilizáveis e possuírem o *Gas tube breakdown voltage*. Na sua aquisição deverá ter-se em conta a impedância, o tipo de conector, as perdas devido à inserção e a garantia.

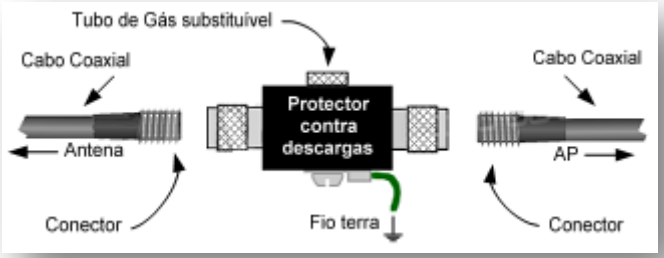



**Figura 62 – Exemplo de um dispositivo Lightning Protectors [105].**

#### *3.3.7.1.5. Conectores*

Estes componentes permitem efectuar uma ligação directa de dispositivos e de cabos a dispositivos. No ano de 1994 a FCC (*Federal Communications Commission*) e o DOC (actualmente a *Industry Canada*) determinaram que os conectores para ligações de WLAN deveriam ser proprietários, fazendo com que surgisse uma grande variedade de conectores criando, consequentemente, incompatibilidades.

Na figura a seguir estão ilustrados os tipos de conectores mais comuns, como por exemplo, o conector N, BNC, F, SMA e TNC.


**Figura 63 – Exemplo de alguns conectores [105].**

#### *3.3.7.1.6. Adaptador PoE (Power Over Ethernet)*

O adaptador PoE é um dispositivo utilizado para o transporte de energia eléctrica DC para um dispositivo *Ethernet* sobre o cabo *Ethernet* Cat5 ou superior, com o objectivo de dispensar alimentação externa ao dispositivo.

Importa salientar que, o componente PoE especificado na norma IEEE 802.3-2005 deverá ser utilizado quando uma tomada AC não está disponível onde o dispositivo está a ser instalado. Assim sendo, o cabo *Ethernet* irá fornecer alimentação e transportar dados para o AP (*Access Point*), que consequentemente provocará uma redução dos custos de instalações eléctricas.

Entretanto, é de referir que o adaptador PoE não suporta todo o tipo de equipamentos. Dispositivos com tecnologia MIMO, por exemplo, exigem muitas vezes uma voltagem superior à fornecida pela tecnologia actual. O IEEE já se encontra a especificar a nova norma IEEE 802.3at para endereçar esta limitação [IEEE 2008c].

Na figura a seguir, está ilustrada um exemplo de uma instalação de um adaptador PoE entre dois equipamentos existentes na rede.

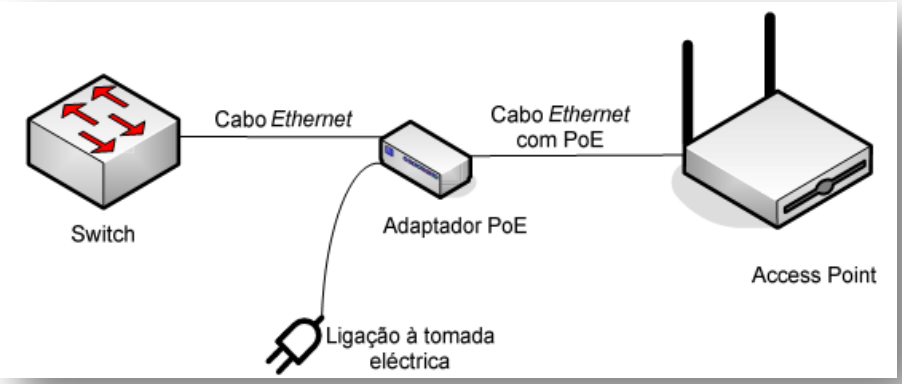



**Figura 64 – Exemplo de uma instalação de um adaptador PoE [105].**

**NOTA:** Importa salientar que, embora pode-se observar na figura anterior, um adaptador para injectar energia eléctrica no cabo *Ethernet*, existem actualmente equipamentos *switch* capazes de o fazer sem qualquer equipamento adicional.

#### *3.3.7.1.7. Equipamentos Wireless*

A seguir será apresentado uma breve descrição dos tipos de equipamentos *wireless* que poderão ser utilizados na implementação de uma rede *Mesh*:

##### *3.3.7.1.7.1. 4G AccessCube*

O *4G AccessCube* é uma nova plataforma de *hardware* dedicado a *Wireless LAN MeshRouting*, desenvolvido pela empresa *4G Systems*, em Hamburgo - Alemanha. Este equipamento possui um processador MIPS de 400MHz, 64MB RAM, 32MB de flash e extensível até 8 cartões miniPCI, é poderoso o suficiente para proporcionar uma excelente segurança e criptografia.

O *4G AccessCube* é suficientemente flexível para ser modificado e personalizado consoante as necessidades dos seus utilizadores.

O *software* do *AccessCube* é de *nylon*, uma distribuição Linux especializada para *WirelessLAN* e *MeshRouting*. Este dispositivo possui como principais características as redes em geral, *Wireless* LAN, o protocolo de encaminhamento *MeshRouting*, a auto-configuração, uma ênfase na segurança (IPSec, VPN) e um *design* compacto para caber num dispositivo flash de 32MB. É totalmente licenciado sob uma licença *Open Source* e é baseado em *OpenEmbedded*.

**Figura 65 – 4G AccessCube [108].**

##### *3.3.7.1.7.2. MeshNode*

Na figura a seguir está ilustrada uma apresentação do equipamento *MeshNode*, que é uma pequena caixa impermeável projectada para uso ao ar livre. Este dispositivo contém um sistema operacional baseado no sistema operativo *Debian / GNULinux* e duas placas de rádio com *dual-band* (2,4 GHz e 5,8 GHz). O seu preço é de aproximadamente 500 ¤ [110].

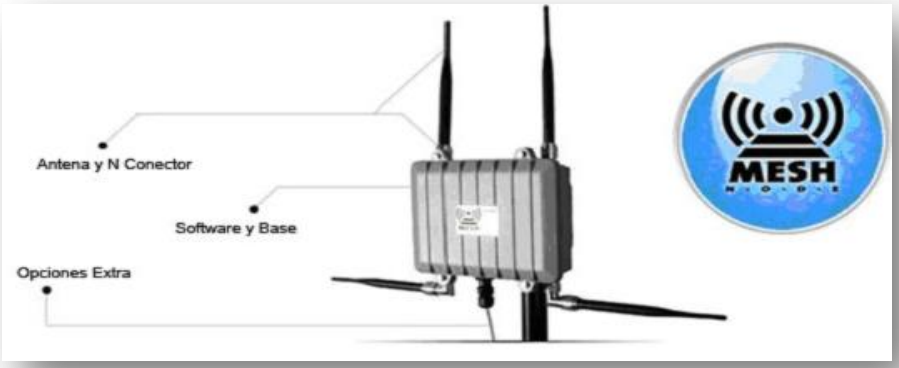



**Figura 66 – MeshNode [110].**

#### *3.3.7.1.7.3. Router Wireless Linksys - WRT54G*

O WRT54G é um dos *router wireless* mais famosos da marca *Linksys* e um dos mais utilizados no mundo na sua gama, nomeadamente em soluções para exteriores. Existe uma grande comunidade utilizadora do router, tanto para projectos residenciais como para implementações de grande dimensão. A comunidade desenvolveu inúmeros *firmware* alternativos ao de origem, permitindo uma maior flexibilidade do equipamento e o uso de novas funcionalidades originalmente suportadas pelo *hardware* mas não disponibilizadas no *front-end* do *software*.

**Figura 67 – Exemplo de um Router wireless Linksys WRT54G [109].**

Embora o referido modelo seja o mais comercializado, porém existem inúmeras variantes da família WRT54G, sendo as mais populares:

- WRT54G: este modelo é baseado em Linux até à versão 4. A partir da versão 5 o *firmware* é o *VxWorks*, baseado em Unix;
- WRT54GL: esta versão possui código aberto para implementação e variação do *firmware* custando aproximadamente apenas 70¤;
- WRT54GS: este equipamento tem a funcionalidade de *speedy booster*, designada também por *channel bonding*, permitindo a agregação de canais de

transmissão contíguos de forma a obter uma maior largura de banda. O referido dispositivo possui mais capacidade de armazenamento que o modelo WRT54G;

- WRT54GC: este é um modelo compacto tendo, por isso, um alcance inferior em 10%;
- WRTSL54GS: Possui apenas uma antena, permite funcionalidades de *firmware* alternativos e contém uma porta USB 2.0, ideal para armazenamento externo.

**NOTA:** É de referir que, o modelo WRT54GL poderá ser considerado como sendo uma reedição do WRT54G com suporte para *firmware* de terceiros baseados em Linux. Este modelo é o melhor candidato dos produtos *off-the-shelf*, pois é o dispositivo principal de muitas distribuições de *firmware* de terceiros para os vários *router* baseados em Linux comummente encontrados no mercado. O modelo WRT54GL é actualmente um dos mais populares dispositivos para as redes wireless.

#### *3.3.7.2. Software*

Neste ponto serão descritos alguns exemplos de soluções de *software* que poderão ser utilizados durante a implementação de uma rede *Mesh* para as redes comunitárias.

##### *3.3.7.2.1. Software para Sistemas Operativos de router*

Aqui serão apresentados os tipos de programas para os sistemas operativos dos *router* que poderão ser utilizados nas redes *Mesh*:

- *Firmware* proprietários: Os *firmware* proprietários pertencem normalmente a *hardware* específico do mesmo fabricante. São, frequentemente, dispositivos de comercialização doméstica, contendo diversas limitações por *software* não fazendo uso da plenitude de potencialidades do *hardware* ou dispositivos de soluções comerciais específicas para exteriores, dispendiosos e nem sempre com a flexibilidade desejada. Estes programas possuem funções de *routing* e de suporte de serviços *wireless* (como por exemplo: *CiscoOS, VxWorks, JUNOSe*, etc.) e são feitos pelos fabricantes de *hardware* ou companhias especializadas;
- Sistemas operativos: Os sistemas operativos apresentam-se como soluções de *software* viáveis, mas não são feitos a pensar no alto desempenho a baixo custo para microssistemas de *hardware* que são procurados neste tipo de projectos (como por exemplo: *Microsoft Windows, Linux, FreeBSD, OpenBSD, pfsense,* etc.);

- *Firmware* de terceiros: estes programas são soluções desenvolvidos ou adaptados por terceiros baseados em Unix para equipamentos de redes comuns no mercado e modificação de *firmware* proprietários.

A seguir será apresentada uma lista contendo apenas alguns dos *firmware* mais relevantes no mercado:

- *DD-WRT*: este *software* é baseado em Linux, com versão paga e livre, tendo ambas inúmeras funcionalidades;
- *FreeWRT*: é um *firmware* baseado no *OpenWRT* direccionado para o Mercado profissional;
- *OpenWRT*: este é um *firmware* altamente personalizável criado de raiz com o sistema de ficheiros JFFS2 para gestão de bibliotecas. É indicado maioritariamente para utilizadores avançados;
- *X-Wrt*: este modelo é uma extensão do *OpenWRT* contendo uma interface gráfica muito fácil e intuitivo para o utilizador comum;
- *Sveasoft*: esta versão corresponde à uma modificação do *firmware* do WRT54GL. As suas versões mais antigas são gratuitas;
- *Tomato*: este *firmware* é baseado no *HyperWRT* com o intuito de ser fácil de utilizar, alegadamente mais estável e rápido.

A seguir será efectuada uma descrição mais detalhada das principais soluções de programas que poderão ser utilizadas na implementação de uma rede *Mesh* para as redes comunitárias. São elas: *DD-WRT, OpenWRT, Freifunk, IkarusOS*, *pfSense*, *RouterOS* (*MikroTik*).

#### *3.3.7.2.1.1. DD-WRT*

O *firmware DD-WRT* surgiu em 2005 como uma simples modificação do *Alchemy firmware*, da *Sveasoft*, que por sua vez é uma modificação do *firmware* original da *Linksys* para suportar autenticação *RADIUS.* O respectivo *firmware* teve uma óptima aceitação no mercado e a sua rápida evolução permitiu que fosse novamente implementado e posteriormente reescrito de raiz.

Actualmente, existem um conjunto de versões desses modelos implementados por diversas empresas. A sua disseminação levou a que fosse incluindo em *wireless router* de *La Fonera* e se celebrasse um contrato com a *Buffalo Technology*, um grande vendedor de *router wireless*, para incluir o firmware na comercialização de alguns modelos.

Este *software* possui uma licença da *GNU General Public License* versão 2. Entretanto, poderá sempre ser possível obter licenças gratuitas do *DD-WRT* ou versões modificadas denominadas de *Special Edition* e *Professional Edition* por um

preço simbólico de 10 a 25¤. Na figura a seguir está ilustrada um exemplo de uma interface *Web* da *firmware DD-WRT*, contendo todas as suas funcionalidades:

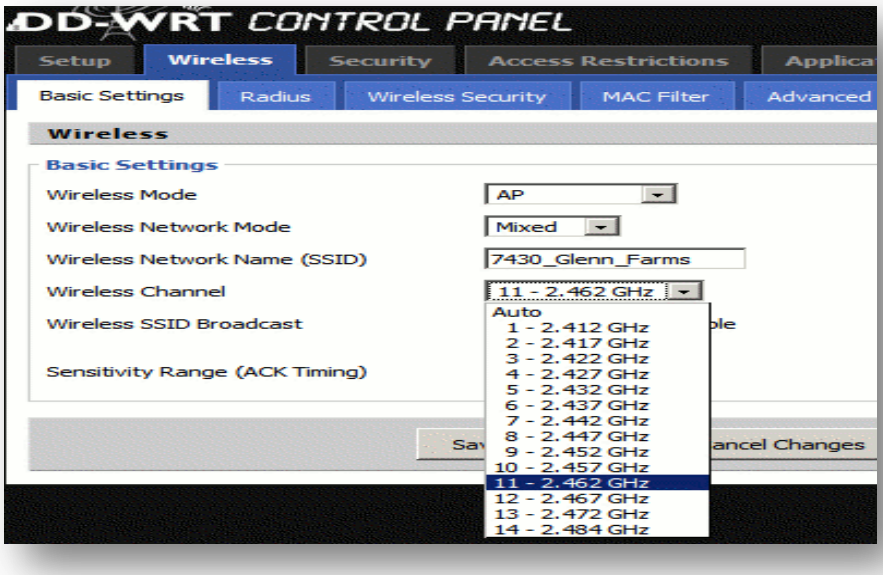



**Figura 68 – Exemplo de um painel de controlo do firmware DD-WRT [111].**

Este sistema tem como principais características:

- 802.1x *Extensible Authentication Protocol*;
- Controlo da potência de saída;
- Cliente *RADIUS*;
- Cliente e Servidor VPN (*OpenVPN* e PPTP);
- Suporte HTTPS para gestão por Web;
- *Hotspot (Sputnik Agent, Chillispot*);
- *Milkfish SIP Router;*
- *MMC/SD Card Support;*
- *Network Time Protocol* (NTP);
- QoS avançado;
- RADIUS;
- *Samba*/*CIFS client*;
- Serviços baseados em *deamons*:
- SNMP (*Simple Network Management Protocol*);
- Suporta os modos *Access Point*, Cliente e *Bridge* cliente;
- Servidor e cliente SSH;
- UPnP;
- VLAN;
- WDS;

- WPA sobre WDS;
- WPA/TKIP com AES e WPA2;

#### *3.3.7.2.1.2. OpenWRT*

O *software OpenWRT* é uma distribuição Linux gratuita desenvolvida para sistemas embebidos como *gateways* residenciais. Inicialmente foi concebido apenas para suportar apenas a família *Linksys* WRT54G, mas contudo, foi rapidamente expandido para suportar outros chipsets e fabricantes, como os *Netgear*, *D-Link*, *Asus*, *PC Engines* e *MikroTik*. Este *firmware* utiliza como interface principal a linha de comandos e secundariamente uma interface web através da instalação da extensão *X-WRT*. O suporte à sua utilização é apenas facultado através dos fóruns e canal do IRC (*Internet Relay Chat*).

Aproveitando as licenças GPL do *software* dos fabricantes dos aparelhos, este *firmware* foi desenvolvido e melhorado de forma a suportar diversas funcionalidades frequentemente inexistentes em *router* de soluções domésticas. Em vez de se ter criado um único *firmware* estático, criou-se um sistema de ficheiros com gestão de pacotes. Assim, libertou-se o utilizador da selecção de aplicações que vêm do vendedor de *hardware* e permitem a customização do dispositivo.

Na figura a seguir está ilustrada um exemplo de uma interface *Web* da *firmware OpenWRT*, contendo todas as suas funcionalidades:

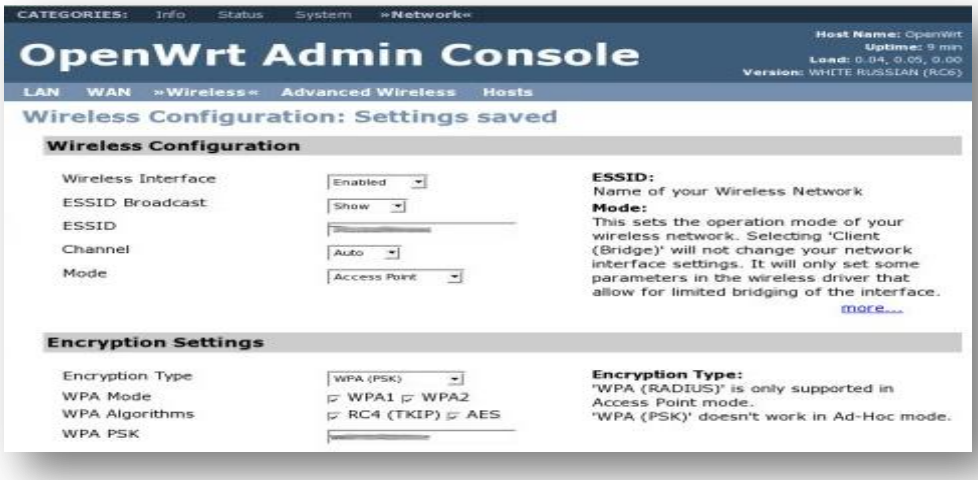



**Figura 69 – Exemplo de um painel de controlo do firmware OpenWRT [89].**

O sistema *OpenWRT* possui as mesmas características às do *firmware DD-WRT* uma vez que partilham o mesmo *kernel*. Mas contudo, o *OpenWRT* tem a vantagem de facilitar a escalabilidade através da adição de pacotes permitindo a expansão e personalização do sistema.

#### *3.3.7.2.1.3. Freifunk*

Este *firmware* foi desenvolvido por *Freifunk group*, em Berlim na Alemanha e pode ser instalado em qualquer equipamento da *Linksys* tais como: o WRT54G (contendo a versão 1.0 a 2.2), o WRT54GS (versão de 1.0 a 1.1), o WAP54G (somente para a versão 2.0) ou ainda um outro dispositivo compatível que permite um funcionamento rápido e fácil num nó OLSR.

Na figura a seguir está ilustrada um exemplo de um ecrã de uma interface Web da *firmware Freifunk*, contendo todas as suas funcionalidades:

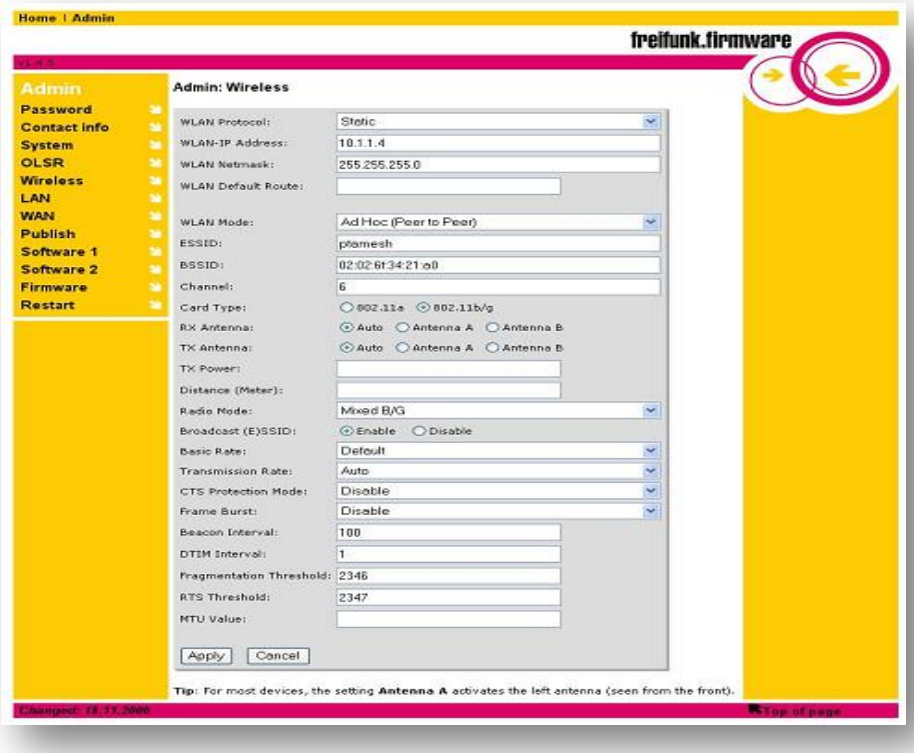



**Figura 70 – Exemplo de um painel de controlo do firmware Freifunk [93].**

#### *3.3.7.2.1.4. IkarusOS*

O sistema *IkarusOS* permite transformar sistemas embebidos em *router wireless* desde que estes possuem incorporados placas wireless *Atheros* ou *Prism*. O *IkarusOS* permite ainda aos utilizadores efectuar uma fácil configuração, monitorização e gestão do dispositivo através da aplicação *IkarusOS Manager*. Esta aplicação fornece visibilidade e controlo em tempo real dos sistemas e estado da rede a partir de qualquer plataforma que suporte Java.

A aquisição do *IkarusOS* faz-se através do pagamento de 13 e 24$ (USD) para as versões mais simples e 34$ (USD) para a versão completa. Na figura a seguir está ilustrada um exemplo de um ecrã de uma interface *Web* da referida *firmware*, contendo todas as suas funcionalidades:

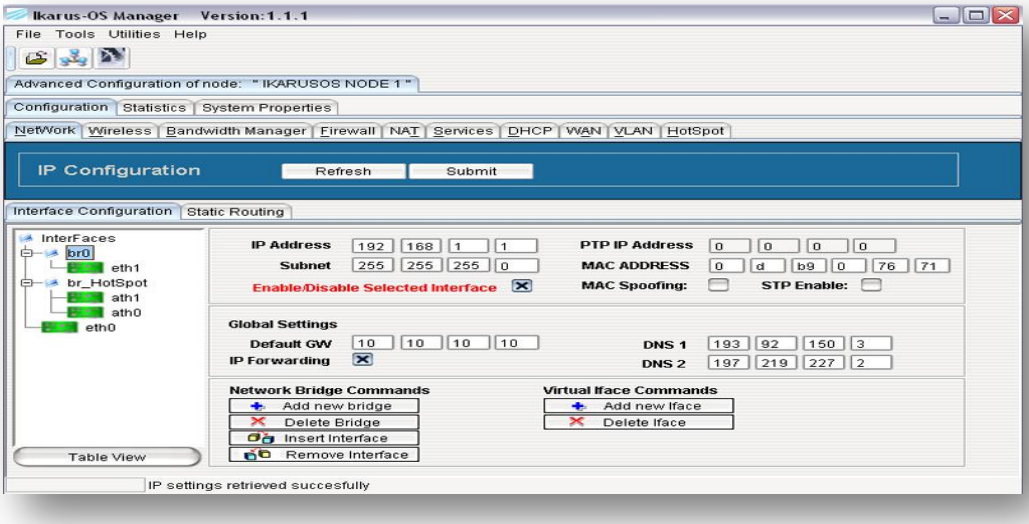



**Figura 71 – Exemplo de um painel de controlo do firmware IkarusOS [112].**

Este sistema embora seja direccionado para sistemas embebidos, suporta também computadores pessoais tais como:

- PC tradicional (x86);
- *PC Engines* (WRAP e ALIX);
- *Soekris*;
- *ADI Engeneering;*
- *Gateworks;*
- *Compex;*
- *Ubiquiti;*
- *LanReady;*
- *Senao-EnGenius*.

O sistema *IkarusOS* tem como principais características:

- ACL/WEP/WPA/WPA2;
- Suporte de AR;
- DFS e TPC (802.11h);
- *Bridging* transparente;
- *Firewall*/NAT;
- *Hotspot*;
- VLAN (802.1q);
- Gestão de largura de banda;
- Cliente *RADIUS*;
- Portal captativo;

- *Walled Garden*;
- *Wireless* super a/g;
- Turbo a/g (108 Mbit/s);
- *Bursting*;
- *Fast frames*;
- QoS (802.11e);
- Compressão.

#### *3.3.7.2.1.5. pfSense*

O sistema *pfSense* é um *software* de distribuição gratuita e *Open Source* do *FreeBSD* e foi adaptada para utilização como *firewall* e *router*. Este *firmware* surgiu a partir do famoso projecto *mOnOwall,* mas entretanto, focou-se em instalações para PC em vez de sistemas de *hardware* embebidos.

Além de ser uma plataforma poderosa de *firewall* e *routing*, inclui uma longa lista de funcionalidades disponibilizadas através de uma extensa e intuitiva interface *Web*.

Permite também a expansão do sistema através de pacotes sem colocar em causa a robustez da distribuição base. É um projecto muito popular, tanto em pequenas redes caseiras como em grandes empresas, universidades e organizações.

Na figura a seguir está ilustrada um exemplo de um ecrã de uma interface Web da referida *firmware*, contendo todas as suas funcionalidades:

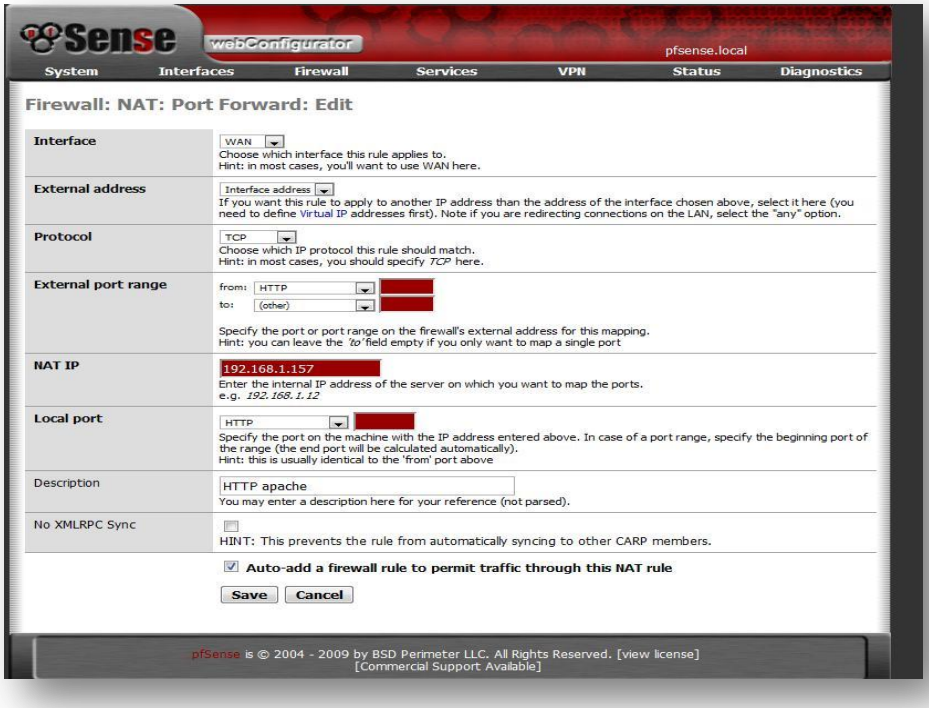


**Figura 72 – Exemplo de um painel de controlo do firmware pfSense [113].**

O sistema *pfSense* tem como principais características:

- *Firewall*;
- Balanceamento de carga;
- *VPN - IPsec, OpenVPN, PPTP*;
- Servidor *PPPoE*;
- Geração de gráficos;
- Informação em tempo real;
- Portal captativo;
- Servidor e encaminhador DHCP;
- Wireless:
    - *wpa_supplicant* com turbo;
    - WEP;
    - WPA-E/PSK;
    - WPA2 (TKIP);
    - Modo AP-host;
    - Encriptação por *hardware*.
- *Mac-filtering*;
- Suporte para múltiplas portas WAN;
- *Traffic Shapping*;
- *Proxy*:
    - FTP;
    - SIP;
    - Anti-SPAM.
- *Accounting*;
- *FreeRADIUS*.

#### *3.3.7.2.1.6. RouterOS (MikroTik)*

O *RouterOS* é o sistema operativo da *MikroTik* criado para o seu *hardware*, as *RouterBOARD*. Contudo, este sistema baseado em Linux pode ser instalado em qualquer plataforma x86 e dispor de todas as funcionalidades de um router de ponta altamente configurável.

O referido SO é licenciado em níveis escaláveis que são diferenciados pela quantidade de funcionalidades disponibilizadas à medida que se sobe de nível. Este sistema permite correr scripts e disponibiliza uma pequena API que permite, de forma limitada, a criação de aplicações para gestão e monitorização dos dispositivos e redes.

É ainda disponibilizado no website um *software* gratuito, denominado de *Winbox*, que fornece uma interface gráfica sofisticada, sendo usada em detrimento da linha de comandos.

Este sistema já deu provas da viabilidade das suas funcionalidades ao ser utilizado por WISP de média e grande dimensão. O suporte a clientes é feito através de e-mail durante os primeiros 15 a 30 dias da instalação, um fórum um *Wiki* que disponibiliza inúmeros tutoriais, exemplos de configuração e experiências de outros clientes. Adicionalmente, são realizadas sessões de treino e conferências um pouco por todo o mundo.

Curiosamente, uma empresa do Brasil planeou o primeiro curso de formação em *RouterOS* direccionado a Administradores de Redes, Gerentes de TI, Técnicos de WISP e ISP em Portugal para o início de Novembro de 2008, pelo preço de 650 ¤, acabando por ser cancelado devido ao reduzido número de inscrições.

Este sistema possui um custo de aquisição que varia entre 45 a 250$ (USD), consoante a versão. Contudo a versão mais barata poderá servir perfeitamente o âmbito deste projecto. Tal como o *IkarusOS*, o *RouterOS* suporta apenas placas wireless com chipsets *Atheros* e *Prism*.

Na figura a seguir está ilustrada um exemplo de um ecrã de uma interface da referida *firmware*, contendo algumas das suas funcionalidades:

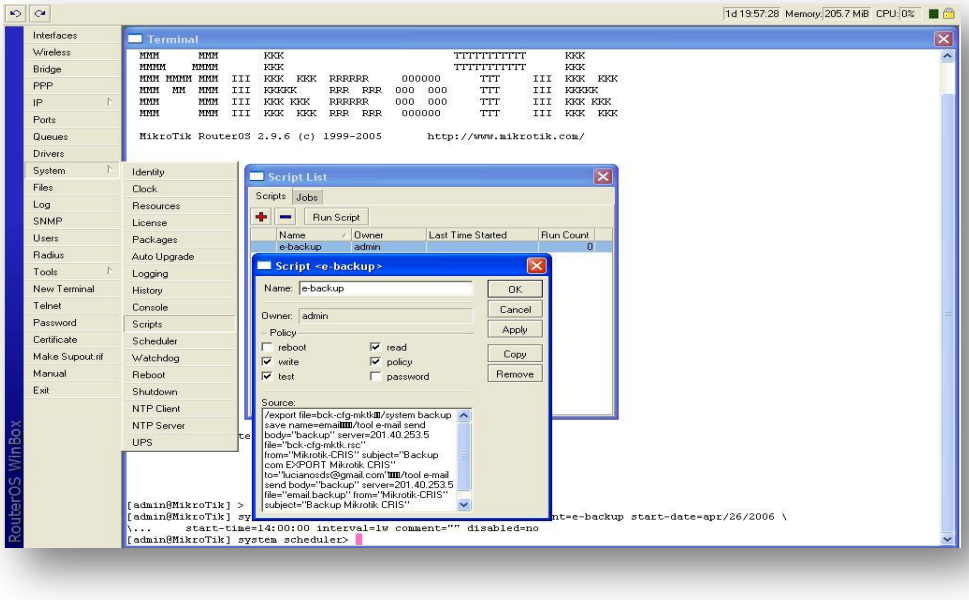



**Figura 73 – Exemplo de um painel de controlo do firmware RouterOS [114].**

O sistema *RouterOS* tem como principais características:

- Extensões proprietárias da norma IEEE 802.11 para melhoria do desempenho da ligação wireless e suporte de débitos na ordem da centena de Mbit/s;

- Comunicação *wireless* em *full-duplex*;
- Interface gráfica por *software* e por Web;
- Configuração e monitorização em tempo real;
- *Hotspot* com *Walled Garden*;
- Cliente e servidor RADIUS;
- Cliente e servidor SSH;
- Web Proxy, Servidor FTP;
- QoS avançado, filtro de tráfico P2P e controlo de largura de banda;
- Suporte dos modos *Access Point*, *AP Bridge*, Cliente, Virtual AP e WDS;
- Alta disponibilidade com VRRP (*Virtual Router Redundancy Protocol*)
- *Firewall* com estados e túneis, NAT;
- WEP/WPA;
- Telnet/mac-telnet/ssh/administração por consola;
- Diversos protocolos de encaminhamento (RIP, OSPF, BGP);
- PPPoE;
- Servidor VPN (PPTP, L2TP, OVPN e IPsec), VLAN;
- NTP, SMNP;
- *Watchdog*.

#### *3.3.7.3. Outros programas*

Aqui serão apresentados outros tipos de programas que poderão ser utilizados nas redes *Mesh*, não só ao nível de autenticação na respectiva rede, como também, ao nível da monitorização e visualização.

##### *3.3.7.3.1. FreeRADIUS*

O acesso de um determinado utilizador à uma rede *Mesh* deverá ser feito através de autenticação e para isso aconselha-se a utilizar a ferramenta *FreeRADIUS*, visto que, para além de ser um *software* gratuito e de *Open Source*, ele funciona nos sistemas operacionais do tipo Unix (*Linux, FreeBSD, OpenBSD, OSF/Unix, Solaris*).

A *FreeRADIUS* é uma aplicação que utiliza o protocolo de rede RADIUS (*Remote Authentication Dial In User Service*), para fornecer ao administrador do sistema uma melhor capacidade de gestão de autenticação, autorização e contabilização das pessoas ou computadores que se ligam e usam serviços na rede. Importa salientar que, estes três serviços disponibilizados ao administrador do sistema pelo protocolo *RADIUS* são conhecidos pela sigla AAA (*Authentication, Authorization, Accounting*):

- *Authentication*: este serviço obriga a um determinado utilizador ou computador que se deseja efectuar uma conexão à rede, a autenticar no sistema;
- *Authorization*: após o registo de autenticação, o protocolo RADIUS, irá determinar quais as permissões de acesso do respectivo utilizador e/ou computador, através do serviço de autorização;
- *Accounting*: uma vez autorizado, será efectuado um registo de toda a informação relativamente aos utilizadores e computadores disponíveis na rede, no serviço de contabilização;

Na figura a seguir está ilustrada um exemplo de um ecrã de uma interface Web do *FreeRADIUS*, contendo todas as suas funcionalidades:

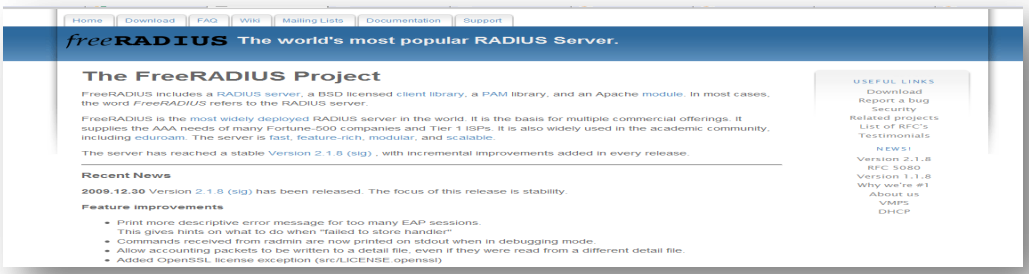



**Figura 74 – Exemplo de um painel de controlo do FreeRADIUS.**

#### *3.3.7.3.2. PUTTY*

O *PuTTy* é um cliente de SSH destinado a promover o acesso remoto a servidores via *Shell* Seguro (SSH) e a construção de "túneis" encriptados entre servidores. Este *software* também permite efectuar ligação directa (*raw*), *telnet*, *rlogin* e por porta serial.

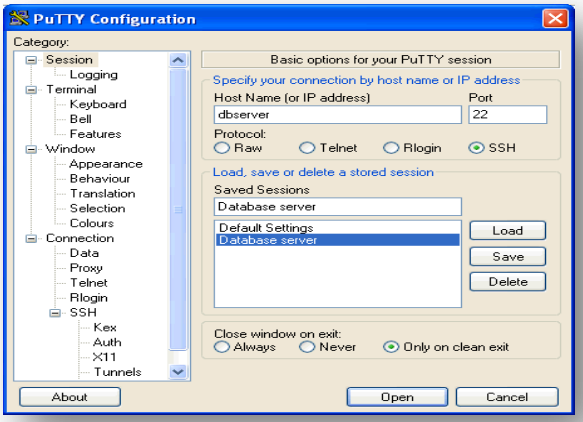


**Figura 75 – Exemplo de um painel de controlo do PUTTY [115].**

#### *3.3.7.3.3. Tcpdump*

O *tcpdump* é uma ferramenta utilizada para monitorar o tráfego dos pacotes numa determinada rede de computadores. Esta ferramenta permite ilustrar os cabeçalhos dos pacotes que passam pela interface de rede.

O *tcpdump* é um conhecido *sniffer* do mundo *GNU/Linux*, que permite configurar uma placa de rede entre em modo promíscuo e capture todos os pacotes (da rede) que cheguem até uma determinada máquina, independentemente de serem encaminhadas para ela ou não. Esta funcionalidade permite gerar um ficheiro em modo de texto, que poderá ser analisada posteriormente.

O *tcpdump* também permite o uso de filtros, como por exemplo, através de um comando *tcpdump* poderá ser verificado o tráfego de pacotes existente num determinado endereço IP na porta 80 do seu servidor: *tcpdump -ni eth0 src "numero ip" and dst port 80.*

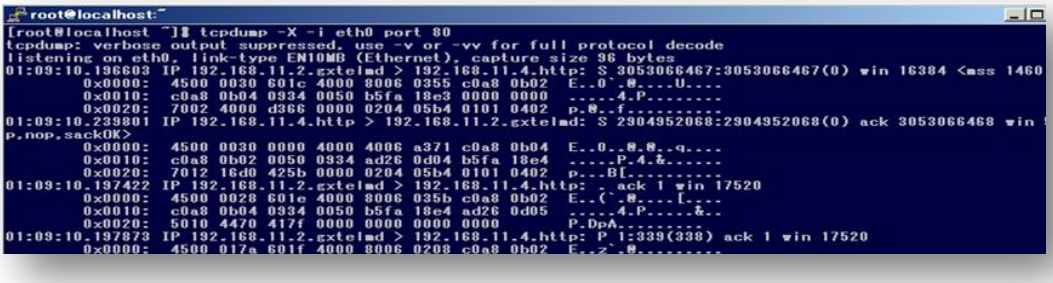



**Figura 76 – Exemplo de uma monitorização de pacotes usando o tcpdump [116].**

#### *3.3.7.3.4. WireShark*

O *Wireshark* (anteriormente conhecido como *Ethereal*) é um programa que permite ao administrador da rede analisar todo tráfego de uma determinada rede, organizando-o por protocolos. As funcionalidades do *Wireshark* são parecidas com o tcpdump, mas com uma interface *GUI*, com mais informação e com a possibilidade da utilização de filtros.

É então possível controlar o tráfego de uma rede e saber tudo o que entra e sai do computador, em diferentes protocolos, ou da rede à qual o computador está ligado. Também é possível controlar o tráfego de um determinado dispositivo de rede numa máquina que pode ter um ou mais desses dispositivos.

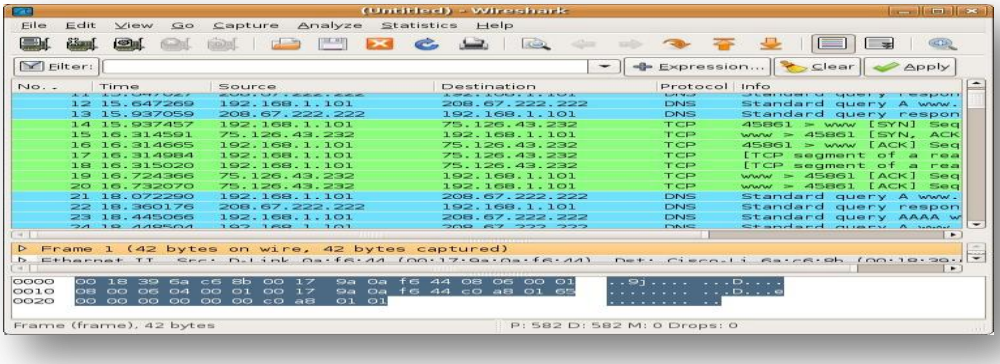



**Figura 77 – Exemplo de uma monitorização de pacotes usando o wireshark [98].**

#### *3.3.7.3.5. OLSR Dot Draw*

O *OLSR Dot Draw* é uma ferramenta que permite ao administrador da rede visualizar toda a complexidade da topologia de uma determinada rede *Mesh*. Esta ferramenta poderá ser adicionada nos equipamentos *router* WRT54G de modo a facilitar a visualização da complexidade da referida da rede *Mesh* [131].

# 4

# 4. Concepção de uma solução VoIP para Redes Comunitárias

Neste capítulo, será apresentada uma solução VoIP para as Redes Comunitárias, tendo em conta alguns cenários de implementação para os potenciais destinatários, nomeadamente, as câmaras municipais inseridas no programa Regiões Digitais, as organizações públicas e outro tipo de organizações ligadas a redes comunitárias.

## *4.1. Cenários de Implementação da solução VoIP numa Mesh Network*

Para os cenários de implementação de uma solução VoIP para uma rede *Mesh* deve-se ter em conta uma série de factores que, por sua vez, irão influenciar na escolha e distribuição do equipamento que irá servir de suporte ao serviço VoIP da referida rede.

Os principais factores são:

- O número e a localização dos utilizadores a serem abrangidos numa determinada rede;
- Os serviços específicos que se pretende disponibilizar aos utilizadores da rede;
- A tipologia de utilização da rede por parte dos utilizadores, sendo que a mesma poderá ser utilizada de um modo intensivo ou esporádico dependendo do nível de sofisticação do utilizador;
- A estimativa do número máximo de chamadas a ocorrer simultaneamente nos dispositivos VoIP existentes na rede, entre outros.

Tendo em conta o que foi anteriormente citado, serão descritas neste documento duas soluções possíveis de arquitecturas para os seguintes cenários de implementação:

- Um serviço IP PBX numa rede privada de uma organização, como por exemplo uma determinada Câmara Municipal;
- Um fornecedor de serviço VoIP numa instituição pública, como por exemplo, uma Biblioteca Municipal e/ou Universidades.

### *4.1.1. Implementação de um serviço IP PBX numa organização*

No que diz respeito a este cenário de implementação, pode-se observar na figura a seguir que existe uma utilização de um serviço IP PBX bastante vulgar de uma organização com necessidades não só ao nível de comunicação internas usando a rede privada, como também, ao nível de comunicação externas com ligações a outras redes.

Na figura a seguir, está ilustrada um exemplo de arquitectura a ser implementado contendo um serviço IP PBX numa rede privada de uma determinada organização:

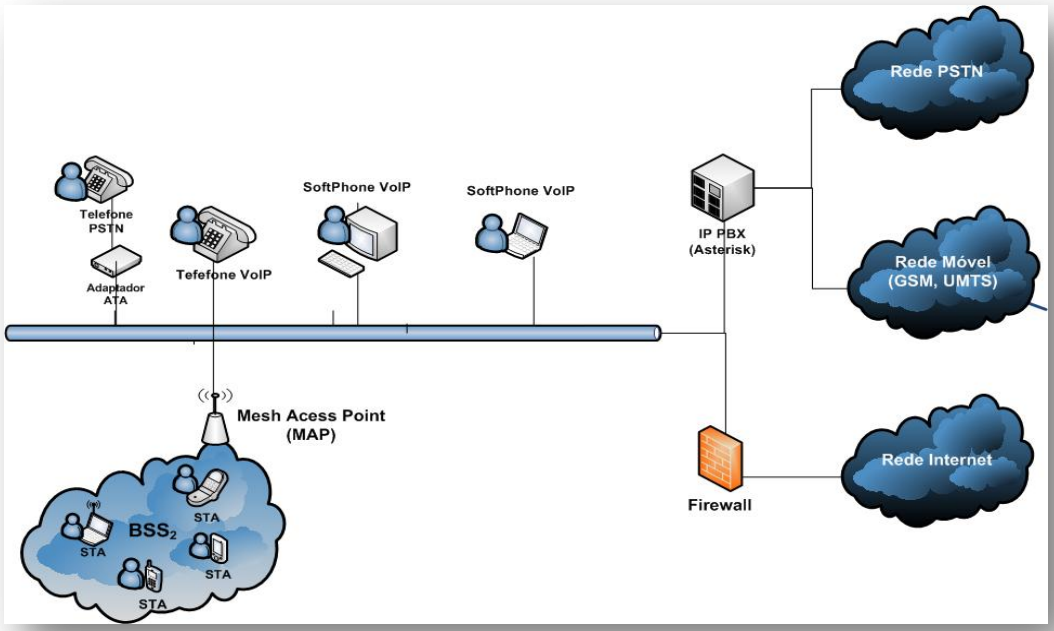



**Figura 78 – Exemplo de uma Implementação de um serviço IP PBX numa organização.**

Neste cenário de implementação todos os equipamentos da VoIP (como por exemplo os telefones, os hardphones ou os softphones) estão interligados não só, através da rede *Ethernet*, como também, através de um *Mesh Access Point* (MAP) ao servidor IP PBX.

Importa salientar que, o servidor IP PBX estará ligado às redes móveis e PSTN, estabelecendo uma ligação entre os vários equipamentos existentes na rede da respectiva organização. Este modelo de arquitectura, permitirá efectuar de um modo rápido de eficaz todas as comunicações internas e externas entre utilizadores da rede privada (e vice-versa).

Este cenário de implementação permite ao administrador da rede, configurar uma série de serviços e disponibilizá-los para todos os utilizadores, tais como:

- *Voicemail*: O serviço de *Voice Mail* que permite-lhe receber mensagens de voz sempre que o seu equipamento móvel ou fixo se encontrar sem cobertura, quando estiver desligado ou quando não puder atender uma chamada. Permite ainda efectuar a gravação das mensagens de voz;
- Reencaminhamento e gravação de chamadas: esta funcionalidade possibilita a implementação de um menu de entrada com redireccionamento automático, possibilitando a minimização das chamadas no *help desk*;
- *Waiting ring*: este serviço permite ao utilizador personalizar o seu equipamento com uma música em espera (*music-on-hold*) caso estiver ocupado e não puder atender uma chamada no exacto momento;
- Definição de rotas para as chamadas: Este serviço permite efectuar uma definição de uma rota mais económica para efectuar chamada, por exemplo, se a chamada para o exterior for para um telemóvel, o IP PBX irá usar a interface para a rede móvel, baixando os custos da chamada;
- Controlo de chamadas e custos: com esta funcionalidade o administrador da rede poderá efectuar um controlo sistemático de todas as chamadas efectuadas, contendo toda a informação da chamada efectuada, tais como: a duração, o destino, o custo, etc.
- Bloqueio de chamadas: esta funcionalidade permite bloquear chamadas para o exterior, ou a determinados utilizadores;

Importa salientar que, esta arquitectura não só fornece vantagens ao nível de serviços disponíveis, como também, vantagens em termos económicos quer ao nível da implementação, manutenção e gestão da mesma.

### *4.1.2. Implementação de um fornecedor de serviço VoIP para uma instituição pública*

Relativamente a este cenário de implementação, pode-se afirmar que o seu principal objectivo é a disponibilização de um serviço telefónico bastante semelhante ao serviço da rede telefónica PSTN, mas com, recurso à tecnologia VoIP para as redes comunitárias *Mesh*.

Na figura a seguir, está ilustrada um exemplo de uma possível implementação de um fornecedor de serviço VoIP para uma instituição pública, contendo alguns componentes necessários para garantir o fornecimento do respectivo serviço.

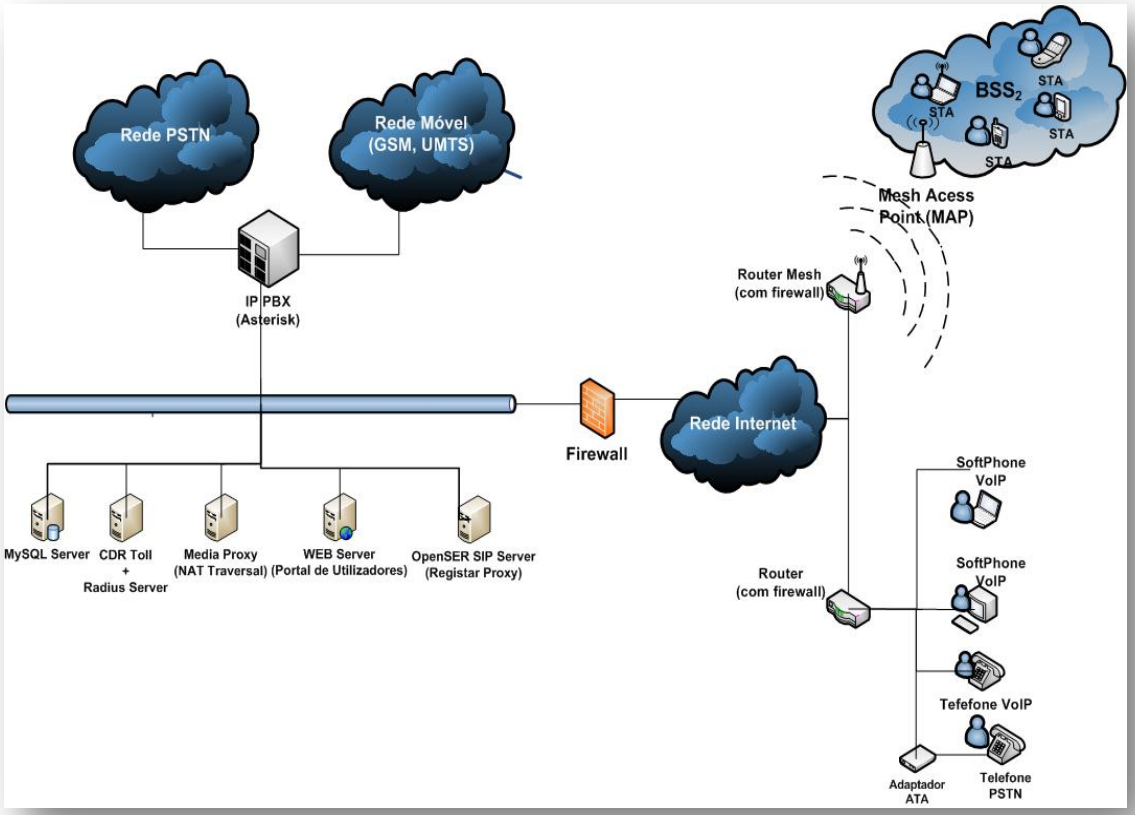



**Figura 79 – Exemplo de uma Implementação de um fornecedor de serviço VoIP.**

Importa salientar que, nesta arquitectura poderá existir um conjunto de factores que poderão influenciar as escolhas e opções ao nível de equipamento e requisitos técnicos que irão servir de suporte ao serviço VoIP da referida rede.

Como exemplo desses factores temos: o número expectável de utilizadores a serem abrangidos numa determinada rede e o número máximo de chamadas efectuadas em simultâneo entre os utilizadores da mesma rede IP e em redes diferentes (IP para PSTN, IP para GSM).

È de referir que, a referida arquitectura apresenta uma limitação quanto ao nível da recepção de chamadas na rede IP de chamadas efectuadas a partir das redes telefónicas convencionais. Isto deve-se ao facto de que, um determinado utilizador ao efectuar uma subscrição deste serviço, não poderá receber chamadas provenientes da rede PSTN ou móvel (GSM, UMTS). Mas contudo, esta limitação não se prende com aspectos técnicos, mas sim com a falta de adopção, a nível mundial de um sistema de numeração único que permita a conversão de números telefónicos (PSTN, Móveis e IP) para um endereço URL que possa ser interpretado na rede IP.

**NOTA:** Importa salientar que, actualmente foi desenvolvido um protocolo que foi lançado com o RFC 3761, nomeadamente o ENUM, que é um protocolo que permite estabelecer uma conversão de números do sistema VoIP para a norma E.164 (usada nos telefones da rede PSTN), com base no protocolo DNS. Sendo assim, será possível implementar um sistema telefónico eficiente, que irá permitir o acesso aos telefones usados pelo sistema VoIP.

### *4.2. Serviços a disponibilizar na Rede Comunitária Mesh*

Neste ponto será apresentado um conjunto de serviços que deverão ser disponibilizados por qualquer fornecedor VoIP para uma rede comunitária *Mesh*:

- Sistema de telefonia IP-PBX: esta funcionalidade permite efectuar a transferência de chamadas telefónicas entre utilizadores VoIP e indivíduos que utilizam os sistemas telefónicos PTSN e GSM (nacionais e internacionais);
- Serviços de encaminhamento automático de chamadas: este sistema permite ao utilizador final, não só receber uma chamada telefónica e verificar os atributos da mesma, como também, tomar decisões sobre o seu respectivo encaminhamento com base no seu conteúdo. Importa salientar que, existem vários exemplos de encaminhamento de uma chamada, visto que, podem ser enviadas para uma extensão única ou um grupo de extensões, para o sistema de gravação de chamadas, entre outros;
- Serviços de *voicemail*: este serviço permite receber mensagens de voz sempre que o seu equipamento móvel ou fixo se encontrar sem cobertura, quando estiver desligado ou quando não puder atender uma chamada.
- Serviço de relatório e estatísticas das chamadas: esta funcionalidade permite efectuar o registo de mensagens efectuadas, não atendidas e rejeitadas entre os utilizadores.

Importa salientar que, todas as funcionalidades que foram anteriormente citadas são disponibilizadas com recurso de um conjunto de *software* gratuito e *Open Source* que poderão ser implementados durante a concepção da solução VoIP para a rede comunitária *Mesh*.

### *4.3. Funcionalidades da plataforma Web para a solução VoIP*

Neste ponto, será apresentado um conjunto de funcionalidades que deverão ser considerados e implementadas na plataforma *Web* da solução VoIP para as Redes Comunitárias, de modo a proporcionar, não só ao administrador do sistema, como também, aos utilizadores da rede toda a informação acerca da sua conta pessoal.

A seguir estão descritas todas as funcionalidades, que se poderão ser consideradas de base na plataforma *Web* que irá servir de interface entre o provedor do serviço VoIP e os seus potenciais utilizadores. São eles:

- Serviço de criação de contas: esta funcionalidade permite criar uma conta pessoal de forma intuitiva e rápida, permitindo o acesso ao sistema VoIP a ser implementado;
- Serviço de alteração dos dados registados: este serviço permite efectuar uma determinada alteração dos dados introduzidos previamente na base de dados do sistema, tais como, alterar o nome e/ou a senha de acesso do utilizador;
- Serviço de créditos: esta funcionalidade permite ao utilizador efectuar não só, uma consulta do saldo de créditos, como também, toda a informação sobre o procedimento para compra de créditos;
- Serviços de tarifários: aqui o utilizador poderá consultar não só os pagamentos efectuados, como também, consultar toda a informação sobre tabela de tarifas correspondente às chamadas efectuadas;
- Serviços de extractos: com esta funcionalidade o utilizador do sistema poderá consultar o seu extracto on-line das ligações efectuadas, bem como, o histórico das ligações dos últimos 3 meses. Este serviço poderá ainda permitir a geração de um extracto no formato CSV e PDF;
- Serviço de plano de ligações e interconexão com as principais operadoras: através deste serviço o utilizador poderá consultar e configurar um plano de ligações e interconexão com as principais operadoras existentes no mercado empresarial;
- Serviço de ajuda: esta funcionalidade permite ao utilizador consultar um manual de configuração contendo toda a informação dos equipamentos SIP a usar, de uma forma detalhada.

Importa salientar que, para além destas funcionalidades ainda poderá ser disponibilizado, ao administrador do sistema uma plataforma *Web* permitindo-lhe não só, configurar toda a informação relativamente ao sistema operativo do router *Mesh*, como também, administrar e monotorizar todo o funcionamento da sua rede.

É de referir ainda que, embora haja aplicações com base em *software* gratuito em que disponibilizam a maioria das funcionalidades anteriormente citadas, o desenvolvimento de novas funcionalidades são da total responsabilidade do fornecedor, sendo que normalmente são solicitados serviços adicionais por parte de programadores especializados.

# 5

# 5. Implementação do protótipo VoIP para Redes Comunitárias

Neste capítulo, será descrito os aspectos mais importantes da implementação do protótipo VoIP para as Redes Comunitárias, que permita testar todos os serviços e funcionalidades que foram mencionados anteriormente. Este protótipo irá permitir efectuar todos os testes necessários de forma a avaliar as capacidades que um serviço poderá ser implementado com uma maior escalabilidade, de modo a proporcionar um potencial fornecedor VoIP da rede comunitária *Mesh*.

## *5.1. Diagrama de blocos do protótipo VoIP*

Na figura a seguir está ilustrado um diagrama de blocos do protótipo VoIP a ser implementado, contendo todos os seus principais componentes conforme pode-se observar a figura:

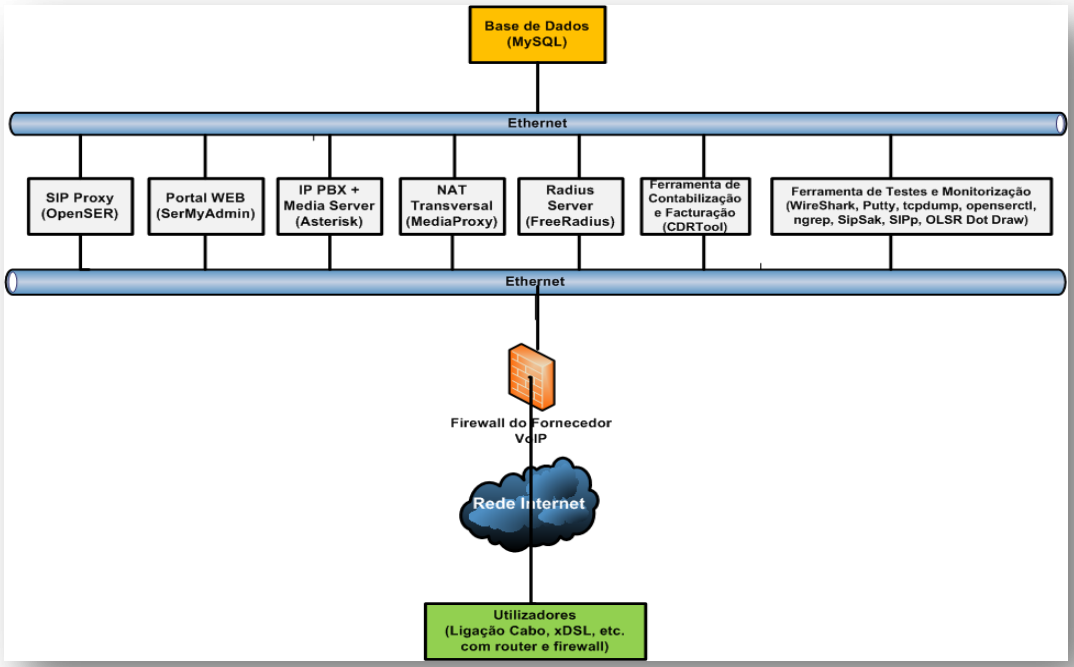



**Figura 80 – Diagrama de blocos do protótipo VoIP a ser implementado. Adaptado de [1].**

## *5.2. Equipamentos necessários para a implementação do protótipo VoIP*

Neste ponto serão apresentados os equipamentos, ao nível de *hardware* e *software*, que são necessários para a implementação de um protótipo VoIP para uma rede comunitária *Mesh*.

### *5.2.1. Hardware*

No que diz respeito, aos equipamentos de *hardware* que poderão ser utilizados durante a implementação de uma rede *Mesh* para as redes comunitárias, passo a citar os seguintes:

- *Router Wireless* da *Linksys*: o equipamento mais indicado nesta família é o modelo WRT54G (nas versões acima de 4.0) ou o WRT54GL (nas versões 1.0 e 1.1). Relativamente à versão 5.0 do modelo WRT54G, importa salientar que a memória *flash* foi reduzido de 4MB para 2MB e consequentemente a sua memória não é compatível com alguns *firmware*, como por exemplo, o *firmware Freifunk*.

  Actualmente, o modelo de router WRT54GL da *Linksys* é um dos dispositivos mais popular para as redes de comunicação *wireless*.
- PC's ou portáteis: poderá ser utilizado um conjunto de computadores pessoais ou portáteis, contendo a placa de ligação LAN para efectuar as conexões dos equipamentos na rede internet ou na rede interna de uma determinada empresa;
- Cabos de ligação: standard CAT5 LAN;
- Adaptadores PoE (*Power-over-Ethernet*): estes equipamentos serão utilizados caso seja necessário implementar um nó *Mesh* exterior;
- Antenas Direccionais de alto ganho e/ou de ganho muito alto: poderá ser utilizado as antenas direccionais *Yagi* e *Painel*, dependendo das necessidades da implementação do respectivo protótipo;
- Antenas Omnidireccionais: este equipamento será utilizado para as *hotspots*;
- Protectores de relâmpagos (*Lighting protectors*): este dispositivo só é utilizado caso houver a necessidade de implementar um equipamento no exterior, de modo a proteger o respectivo equipamento eléctrico das descargas de relâmpagos.

### 5.2.2. Software

Tendo em conta o que foi descrito nos capítulos anteriores, pode-se afirmar que existem um conjunto de equipamentos de *software* gratuito e *Open Source*, que poderão ser utilizados durante a implementação de uma rede *Mesh* para as redes comunitárias. Importa salientar que, poderão surgir algumas dificuldades relativamente a este ponto, visto que, estes programas podem sofrer constantes actualizações pelo facto de serem programas *Open Source*. É de referir o caso do servidor *SIP Proxy*, nomeadamente o *OpenSer*, que é um exemplo prático disso e que sofreu uma separação em dois novos projectos, o *Kamailio* e o *OpenSips* respectivamente.

Dado que, actualmente a tecnologia VoIP ainda está em constante desenvolvimento deve-se ter em conta a necessidade de manter um acompanhamento constante das actualizações dos respectivos programas.

A seguir, será apresentado um quadro resumo dos principais *programas* que poderão ser utilizados durante a implementação de uma rede *Mesh* para as redes comunitárias. São eles:

| Nome | Descrição | Versão |
|---|---|---|
| Sistema Operativo dos Servidores | Debian | 4.0r4 etch |
| Servidor SIP Proxy | OpenSER | 1.3.3 |
| Portal Web | SerMyAdmin | 0.7 |
| IP PBX | Asterisk | 1.4.1 |
| Transposição NAT / Media Relay | MediaProxy | 1.9.1 |
| Radius Server | FreeRadius | 1.1.3-3 |
| Ferramenta de Contabilização e Facturação | CDRTool | 6.1.10 |
| *Software* de Virtualização | VMWare Server | 1.0.8 |
| Ferramentas de monitorização | WireShark | 0.99.7 |
| | Putty | --- |
| | TCPdump | --- |
| | OLSR DotDraw | --- |
| Sistema Operativo para Router | Freifunk firmware | 1.4.5 |
| | DD-WRT firmware | 2.3 |

**Tabela 20 – Programas necessários para a implementação do protótipo VoIP.**

## 5.3. Instalação de componentes

Nesta secção será apresentada uma breve descrição sobre a instalação dos principais componentes que correspondem ao diagrama de blocos da arquitectura VoIP a ser implementada. Contudo, importa salientar que, será apresentada uma

instalação passo a passo dos diversos componentes que fazem parte deste trabalho, de uma forma detalhada e pormenorizada nos manuais de instalação anexados no final deste documento. Assim sendo, para efectuar a instalação dos respectivos componentes deverão ser executados os seguintes passos:

### *5.3.1. Sistema Operativo*

Relativamente ao sistema operativo a ser instalado deverá ser escolhido o *S.O. Linux Debian* (versão 4.0r4 etch), visto que, possui várias vantagens em relação aos restantes sistemas e dentro das quais se destacam as seguintes:

- A sua facilidade de instalação e a ampla compatibilidade com diversos *hardware* e aplicações VoIP existentes no mercado empresarial;

- Possui uma enorme comunidade aderente ao *Debian*, o que o torna um sistema bastante documentado, facilitando a resolução de erros e problemas de instalação das aplicações (consultar a secção 10.1).

### *5.3.2. OpenSer*

No que diz respeito, à instalação do Servidor *SIP Proxy*, pode-se afirmar que o manual de instalação está muito bem documentado. Mas contudo, importa salientar que, durante esta fase de instalação poder-se-ão surgir alguns problemas pontuais relacionados com a configuração do ficheiro *openser.cfg* que serão descritos também nos anexos. Ainda, durante este passo será instalada e configurada a ligação à base de dados *MySQL* (consultar a secção 10.2).

### *5.3.3. Portal WEB – SerMyAdmin*

O sistema de portal *Web*, *SerMyAdmin*, foi desenvolvido em *Ruby on Rails* sendo que poderá ser necessário efectuar uma série de instalações prévias, nomeadamente do *Java* 1.5 JDK e um servidor *Web*, o *Apache Tomcat*. Contudo, devido à alteração que esta aplicação implementa na base de dado original do *OpenSer*, será necessário ter alguns cuidados extraordinários durante a instalação do referido portal (consultar a secção 10.4).

### *5.3.4. Software de transposição de NAT – Mediaproxy*

O processo de instalação do *software Mediaproxy* é fácil e intuitivo, visto que, o manual de instalação disponibilizado no site oficial desse projecto (em http://mediaproxy-ng.org/), esta muito bem documentado e não levanta qualquer complexidade (consultar a secção 10.3).

Importa salientar que, poderá existir a possibilidade de instalar vários *Mediaproxy Relay* em diferentes máquinas de forma a equilibrar a carga imposta pelas comunicações RTP pelos diferentes servidores.

### 5.3.5. IP PBX – Asterisk – e interligação com o OpenSer

O processo de instalação do sistema *IP PBX Asterisk* é semelhante do que acontece com a instalação do servidor *OpenSer*, visto que, o manual de instalação disponibilizado no site oficial do referido projecto (http://www.asterisk.org/) está muito bem documentado. Entretanto, existe um conjunto de informações sobre a instalação do *Asterisk* em vários sítios da internet. É de referir que, poderá existir a possibilidade de surgir algumas questões de maior complexidade relativamente durante a fase de configuração para a interligação do *Asterisk* com o *OpenSer* (consultar a secção 10.5).

### 5.3.6. FreeRadius e CDRTool

Para a instalação destes programas deverão ser executados uma série de "subpassos" para a instalação de pacotes necessários à instalação do *FreeRADIUS*, tais como:

- A configuração da base de dados para uso do *FreeRADIUS*;
- A configuração do *FreeRadius*;
- A instalação do cliente *FreeRADIUS*;
- E por último a configuração do *OpenSer*.

É de referir que, após o término do processo de instalação e configuração dos elementos anteriormente citados, deverá proceder-se à instalação da ferramenta de contabilização e contabilização, nomeadamente a *CDRTool* (consultar a secção 10.6).

### 5.3.7. Ferramentas de teste e monitorização

Neste ponto, serão instaladas algumas ferramentas de teste e análise de pacotes VoIP. Entre elas, temos o *WireShark*, o *PuTTY*, o *tcpdump*, o *openserctl*, o ngrep, o *SipSak*, *SIPp* e o *OLSR Dot Draw*. Esta última ferramenta permite visualizar toda complexidade de uma rede *Mesh* (consultar a secção 10.7).

### 5.3.8. Firmware para o Sistema Operativo dos Router

Neste ponto, deverão ser considerados alguns aspectos de configuração e de segurança relativamente aos *firmware* para os sistemas operativos embutidos nos *routers wireless*, visto que, estes aplicativos podem ser configurados consoante a

necessidade de utilização e de implementação de uma determinada rede comunitária *Mesh*.

Importa salientar que, em anexo a este projecto estão presentes dois manuais de instalação de *firmware* que deverão ser instalados nos equipamentos da *Linkys*, nomeadamente, os *firmware Freifunk* e *DD-WRT*, respectivamente (consultar as secções 10.8.1.1 e 10.8.4.1).

# 6

# 6. Casos de Estudo sobre as Redes Mesh

Neste capítulo, será apresentado um estudo sobre alguns casos de sucesso sobre as redes *Mesh*, que poderão servir como sendo um exemplo prático da implementação de uma rede *Mesh* com base em soluções *Open Source*, aonde poderá ser implementada uma solução VoIP para uma determinada rede comunitária. É de referir que, o presente trabalho de investigação teve como base principal o projecto "*Freifunk OLSR Experiment"* que foi desenvolvido pelo *Freifunk group* em Berlim na Alemanha.

## *6.1. Projecto – "Freifunk OLSR Experiment" em Berlim, Alemanha*

Este projecto foi desenvolvido pelo *Freifunk group*, em Berlim na Alemanha e constitui numa rede experimental para a comunidade urbana. Actualmente, este projecto está constituído por mais de 400 nós baseados no *OLSR Firmware Freifunk*. Hoje em dia, existem muitos projectos comunitários e em vias de desenvolvimento que utilizam o referido *software* [93].

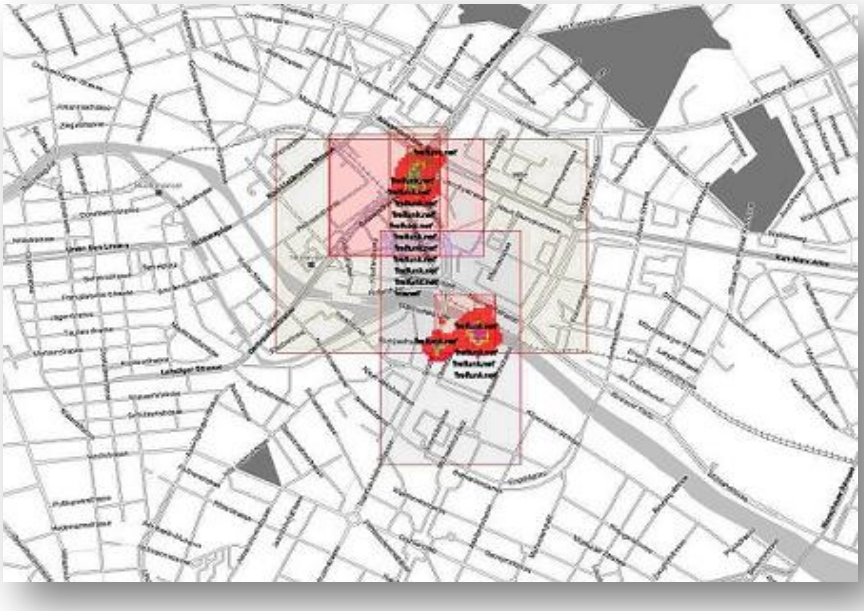


**Figura 81 – Projecto Freifunk OLSR Mesh em Berlim [93].**

Na figura a seguir, está ilustrada um exemplo de uma possível visualização da complexidade da rede *Mesh* do referido projecto, através de um *software* de monitorização, nomeadamente o *OLSR Dot Draw*.

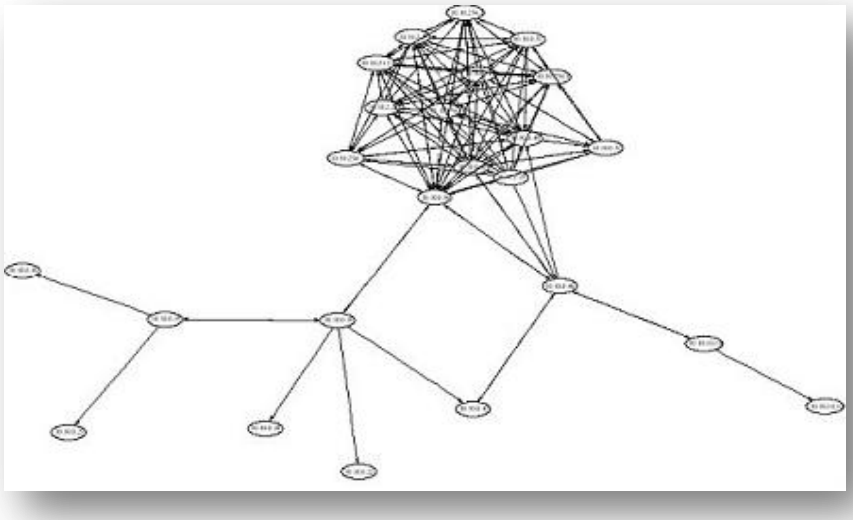


**Figura 82 – Diagrama de uma rede Mesh OLSR [93].**

## *6.2. Projecto – "CUWiN", Estados Unidos de América*

O projecto *CUWiN* (*Champaign-Urbana Community Wireless Network*) é uma iniciativa de investigação e desenvolvimento, baseado em *software* gratuito e *open source*. Este projecto utiliza o protocolo de encaminhamento HSLS (*Hazy-Sighted Link State*), e aposta numa rede *Ad-Hoc* sem fio escalável e altamente robusta [123].

**Figura 83 – Projecto CUWiN [123].**

## *6.3. Projecto – "The Dharamsala Mesh" em Dharamsala, Índia*

Este projecto foi desenvolvido em *Dharamsala* na India, pelo Grupo de Tecnologia da Informação *TibTec Dharamsala.* Foi inaugurado em Fevereiro de 2005, logo após algumas alterações no regulamento oficial sobre as redes *Wi-Fi* para o uso externo na Índia [124]. No final do referido mês, com a implementação da respectiva rede *Mesh*, já tinham sido conectados oito *campus*. Entretanto, foram efectuados vários testes durante esse mês, que permitiram demonstrar que embora a Índia seja constituída por terrenos montanhosos e de difícil acesso, é sempre mais apropriado e indicado a implementação das redes *Mesh*. Isto deve-se ao facto de que, as redes ponto-a-multiponto não conseguem ultrapassar as limitações e as interferências na propagação de sinais por causa das montanhas.

A topologia *Mesh* oferece uma área de cobertura muito maior, já que possui um protocolo de encaminhamento dinâmico o que provou ser essencial em zonas rurais que têm alguns problemas com o fornecimento da energia eléctrica. A rede *Mesh* inclui mais de 30 nós, todos compartilhando um único canal de rádio. Isto permitiu fornecer serviços de acesso à Internet de banda larga a todos os membros da rede *Mesh*. O número total de largura de banda disponível é de 6 Mbps [124].

Este projecto permitiu interligar várias organizações sem fins lucrativos. Actualmente, existem mais de 2.000 computadores conectados entre si, colocando uma grande sobrecarga na respectiva rede. O referido projecto utiliza o router WRT54G da *Linksys* contedo o *firmware OpenWRT*. Utiliza ainda o protocolo OLSR com ETX *(Expected Transmission Count)* [124].

**Figura 84 – Redes Mesh Dharamsala [124].**

### *6.4. Projecto – "Peebles Valley" em Mpumalanga, África do Sul*

Na África, a implementação de serviços de telecomunicações em zonas rurais, como por exemplo, a telefonia e o acesso à internet, é muito baixa e em algumas regiões quase inexistente. Os operadores de telecomunicações em África consideram as zonas rurais, como sendo zonas cujo desenvolvimento económico é pouco sustentável, devido à natureza dessas regiões. Isto deve-se ao facto de que, estas zonas possuirem uma localização remota e muitas vezes inacessíveis. Existe ainda a falta de infra-estrutura e são pouco povoadas, sendo que a maior parte das famílias possue um fraco rendimento económico e pouca qualificação ao nível de habilitações literárias e/ou académicos.

No entanto, o acesso confiável, acessível e fácil a serviços de telecomunicações para todos, foi identificado como sendo um aspecto principal para o desenvolvimento social e económico em África.

Actualmente, há vários projectos-piloto em Àfrica que estão a ser implementados e co-financiados em parceria com várias instituições internacionais, (tais como, o *Department of Computer Science* na Universidade da Califórnia em Santa Barbara, o *CUWiN*, etc.) com o intuito de levar a conectividade wireless de banda larga às zonas rurais de África, sendo que o primeiro país a testar o projecto será a África do Sul. Com estes projectos pretende-se estimular o desenvolvimento económico rural, através da implementação de uma tecnologia baseda em rede *Mesh* sem fios (*Wireles Mesh Network*) baseada nos *standards* IEEE 802.11 a/b/g, que permitirá a disponibilização de serviços de telecomunicações por banda larga às empresas locais.

De entre desses os referidos projectos, destaca-se projecto *"Peebles Valley"* foi desenvolvido pela *Meraka Institute*, em *Mpumalanga* na África do Sul. Esta instituição é responsável não só por todo o desenvolvimento técnico do referido projecto, como também, pela de sua própria rede de informações comunitária (COIN), que é uma iniciativa como o projecto *Wireless África*.

O projecto *"Peebles Valley"* tem demonstrado que uma comunidade, poderá estabelecer e manter uma rede *Mesh* sem fio, estabelecendo um acesso directo a um conjunto de informações actuais e serviços de comunicação. Estes serviços incluem a telefonia IP (VoIP), mensagens instantâneas, correio eletrônico, acesso à Internet, serviços de multimídia e serviço de entrega (por exemplo, tele-saúde e *e-learning*).

Este projecto constitui numa das várias iniciativas inovadoras que pretendem estimular o desenvolvimento económico rural, através da implementação de uma tecnologia baseada em rede *Mesh* sem fios, e que são financiados pelo CSIR (*Council for Scientific and Industrial Research*).

O referido projecto utiliza o router WRT54G da *Linksys* contendo o *firmware Freifunk*, e actualmente já possui mais de 10 nós Mesh que está em fase de crescimento. O primeiro nó Mesh utilizado com o intuito de auxiliar uma clínina médica no tratamento da SIDA (ACTS - *Aids Care Training and Support*) [64].

**Figura 85 – Redes Mesh Mpumalanga [64].**

De referir que, a implementação de uma arquitectura de rede para uma rede *wireless Mesh* dependerá muito da localização geográfica e da distâncias entre os *Access Point* (AP) a serem conectados. Sendo assim, de modo a criar uma rede *Mesh* confiável entre dois nós, deverá existir não só, uma combinação de ligações de longo alcance ponto-a-ponto (usando antenas direccionais), como também, de ligações locais ponto-multiponto (utilizando antenas omnidireccionais).

Nas zonas rurais de África, uma ligação via satélite (VSAT - *Very Small Aperture Terminal*) geralmente fornece uma única possibilidade de efectuar uma interligação entre uma rede *Mesh* local para um provedor de rede *upstream*, oferecendo uma conectividade global.

Na figura a seguir, está ilustrada um exemplo de arquitectura de uma rede *Mesh* sem fios, onde poderá ser efectuado uma ligação *upstream* entre os equipamentos conforme foi citado anteriormente.

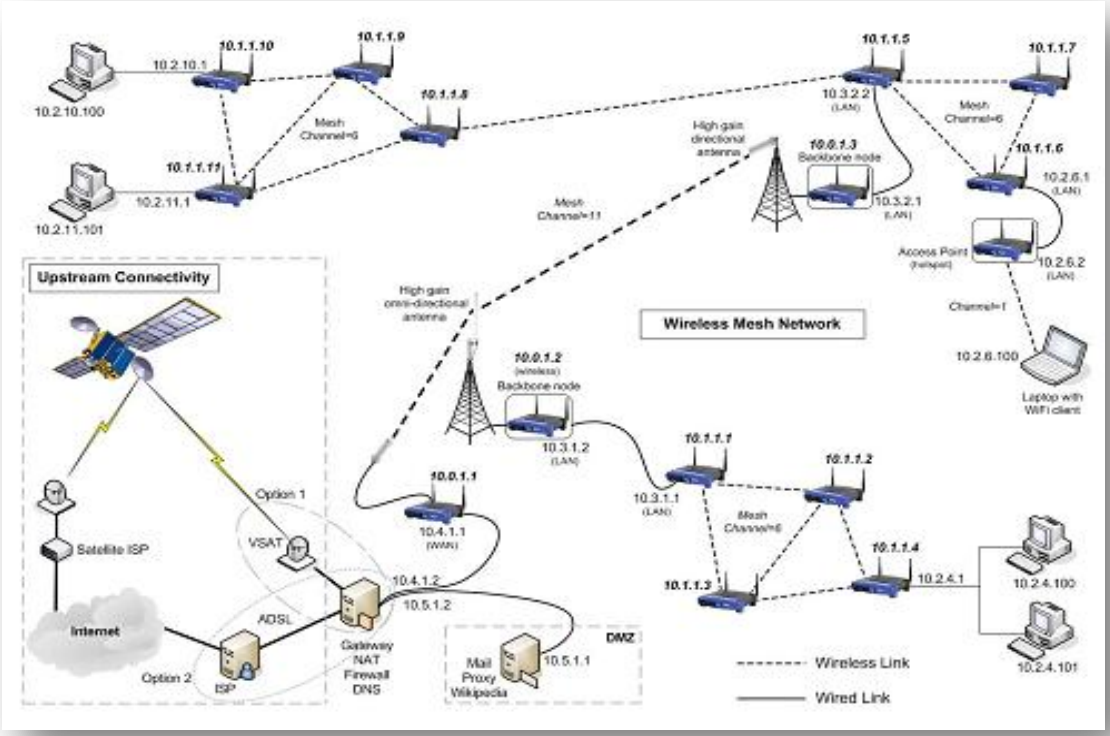



**Figura 86 – Exemplo de arquitectura de uma Rede Mesh sem fios [117].**

### *6.4.1. Benefícios*

Na África do Sul foi estabelecida uma parceria entre o Departamento de Ciência e Tecnologia e a União Europeia, com o intuito de implementar um projecto-piloto, que terá um custo de 30 milhões de euros. Importa salientar que, embora a África do Sul seja o segundo maior mercado de telecomunicações do continente africano logo a seguir à Nigéria, muitas das áreas rurais do país – e as escolas e empresas instaladas nessas regiões – ainda não possuem um acesso grátis à Internet. Contudo, com esse projecto a UE pretende atingir uma cobertura de 95 por cento nas áreas de intervenção.

Como já foi anteriormente citado, à semelhança do que se passa na África do Sul, muitas zonas rurais do continente africano ainda não contam com ligação à Internet, devido à situação económica e social das mesmas. Entretanto, tendo em consideração esses aspectos, o governo sul-africano e a União Europeia querem criar e patrocinar um conjunto de pequenas empresas que serão geridas por operadores

locais, de modo a proporcionar serviços de acesso à Internet e VoIP (*Voice Over Internet Protocol*) a mais de 450 entidades públicas, na sua maioria escolas.

Numa fase inicial do projecto, serão intervencionadas instalações comunitárias como escolas, clínicas e bibliotecas, que passarão a contar assim com infra-estruturas de banda larga, de modo a permitir o combate à infoexclusão, promovendo a igualdade de oportunidades e de acesso público à banda larga na região, corrigir assimetrias de acessibilidade a telecomunicações, e desenvolver a iniciativa empresarial de base tecnológica e científica na região.

De acordo com União Europeia, o continente africano, necessitará de uma solução híbrida que permitirá obter uma conectividade global, tais como, a combinação de tecnologias de fibra óptica e banda larga *wireless*, bem como uma abordagem profunda em termos de crescimento das infra-estruturas e aplicação de regulações [125].

### *6.4.2. Serviços disponibilizados pelo sistema aos utilizadores*

Neste ponto, será apresentado um conjunto de funcionalidades que estão disponíveis na plataforma *Web* do referido projecto, de modo a proporcionar, ao administrador da rede uma melhor administração do sistema via *Web*.

É de referir que, os serviços oferecidos vão depender de uma série de factores, tais como:

- A exigência de largura de banda dos serviços;
- Competências técnicas na comunidade;
- E a memória disponível nos nós da rede *Mesh*;

Entre estas funcionalidades as mais importantes são as seguintes:

- *Gateway/Firewall* (para definição e gestão da largura de banda): Esta funcionalidade é geralmente utilizada como sendo um servidor que permite compartilhar uma única ligação à Internet. Normalmente será conectado num terminal VSAT (*Very Small Aperture Terminal*) através de uma interface e da rede sem fio numa outra interface. A elaboração e gestão da largura de banda também são normalmente encontradas numa *gateway*, de modo a assegurar que todos os utilizadores têm a mesma largura de banda que eles pagaram para o efeito (ou para garantir que todos recebam uma parte ainda da largura de banda).
- DNS (*Domain Name System*): este funcionalidade permite definir um sistema de conversão de nomes dos hosts e domínios, em endereços IP

na Internet ou redes locais. Isso pode melhorar significativamente os tempos de resposta da rede.

- E-mail (baseado na web ou no servidor): Este serviço permite aos utilizadores da rede, estabelecer uma comunicação por intermédio de mensagens eletrônicas enviadas ou recebidas por meio de um servidor de e-mail. A opção mais fácil seria para que todos os utilizadores da respectiva rede pudessem utilizar um sistema de e-mail *web-based,* onde o servidor estará alocado em qualquer sítio na internet (como por exemplo, *GMail*, *Yahoo!Mail ou Hotmail*).
- *Chat/Instant Messaging*: esta funcionaIidade permite aos utilizadores efectuarem conversações (baseado em modo texto) em tempo real, num ambiente de rede como a Internet. Por exemplo, caso um utilizador digite uma mensagem de texto e pressione a tecla “Enter”, o respectivo texto aparecerá imediatamente nos computadores dos restantes utilizadores, permitindo deste modo efectuar conversações digitais. Estas conversações são muitas vezes mais lentas do que as conversações normais.
- VOIP (baseado em *Asterisk*): permite ter um sistema PABX (*Asterisk*, por exemplo), mas contudo, precisa de ser configurado em algum sítio na rede (como por exemplo, próximo de um *gateway*), de modo a permitir efectuar chamadas telefónicas entre os utilizadores existentes numa rede. Será necessário um telefone comum, ligado um adaptador de telefone analógico (ATA), que estará ligado ao nó *Mesh* (*router Linksys*) via *Ethernet*.
- *Web Proxy* (para acesso à web): Um *proxy* funciona como intermediário entre o seu programa (browser) de acesso à *World Wide Web* e os servidores WWW dispersos pela Internet. O servidor *proxy* armazena localmente grande parte dos documentos transferidos, de forma a optimizar as ligações que outros utilizadores venham a fazer no intuito de obter os mesmos documentos. Consegue-se, deste modo, um significativo aumento de rapidez no acesso a informação já disponível na cópia local do *proxy*, para além de se optimizar a utilização da largura de banda para o exterior.
- *Community Server*: esta funcionalidade corresponde a um servidor *Web* que poderá facilitar o intercâmbio de informações entre os membros da comunidade, tais como: eventos de publicidades previstas na comunidade, serviços oferecidos por membros da comunidade e os seus contactos. Poderá também ainda, funcionar como sendo uma biblioteca digital, onde os recursos importartes para a respectiva comunidade, como por exemplo, a informação

sobre a saúde, a agricultura e/ou educacionais (por exemplo, uma enciclopédia electrônica) poderá ser acessado via *Web*.

### *6.4.3. Estado actual dos projectos-piloto de Rede Wireless em África*

Neste ponto, será apresentado algumas figuras contendo um conjunto de informações sobre o estado actual do regime de licenciamento sobre a rede *wireless* em vigor no continente Africano, para uma taxa de transferência no intervalo de 2,4 e 5 GHz, respectivamente. Essas figuras ilustram uma diversidade significativa que existe em todo o continente Africano.

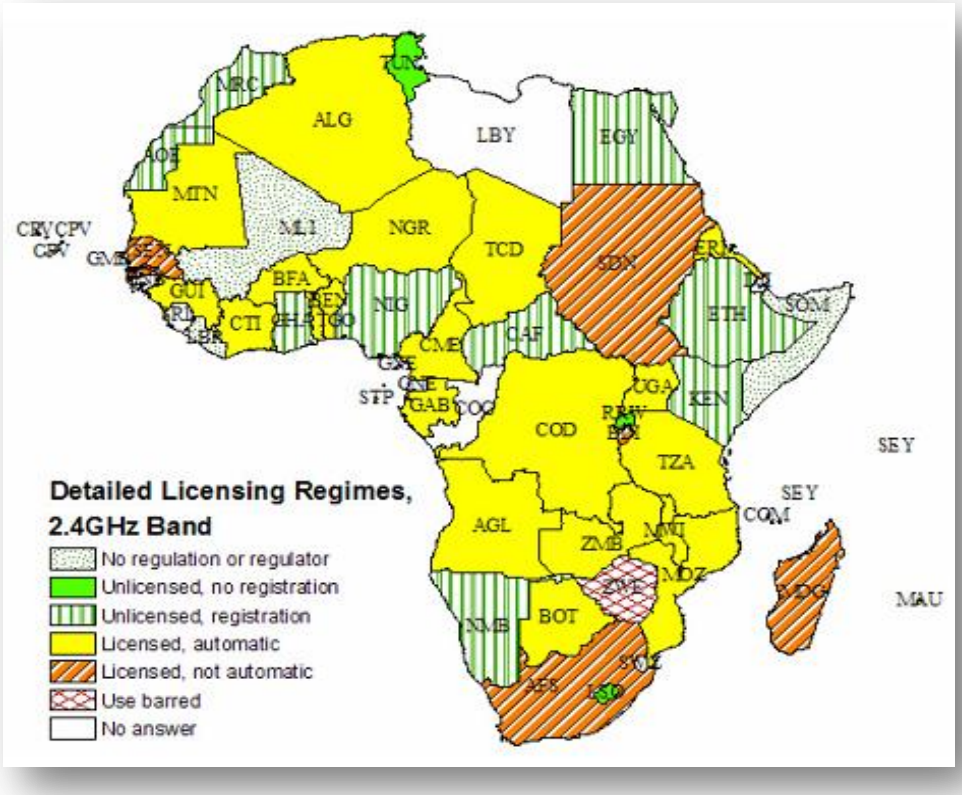



**Figura 87 – Regime de licenciamento para a largura de banda 2,4 GHz [117].**

Na figura a seguir, poderá ser observado que, na faixa de 2,4 GHz, 19% dos países permitem o uso sem licença, mas exigem um registo (15% para a faixa de 5GHz). Entretanto existe uma excepção para a banda de 2,4 GHz aos seguintes países: Ruanda, Lesoto e Tunísia.

Poderá ainda ser observado que, em África, o uso das faixas não licenciadas é muito significativo em relação aos Estados Unidos de América, visto que, apenas três países (6% da África) usam a frequência de 2,4 GHz e 2 países (4%) a faixa de 5GHz. Estes valores são extremamente baixos [117].

Relativamente ao uso licenciado da largura de banda, a atribuição de licença é normalmente efectuado automaticamente no acto de pagamento de uma determinada taxa (aproximadamente com uma percentagem de 40% do total dos países para as duas larguras de banda, 2,4 GHz e 5 GHz, respectivamente).

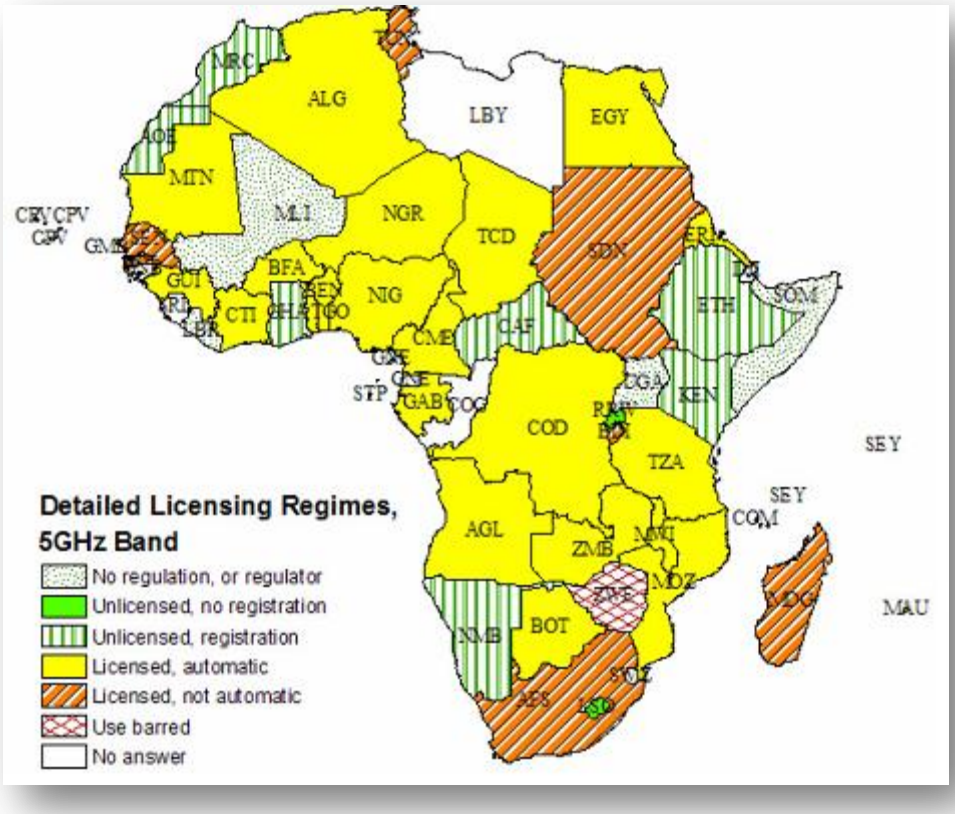



**Figura 88 – Regime de licenciamento para a largura de banda 5 GHz [117].**

Importa salientar que, em anexo a este documento está um manual de configuração e de implementação de uma rede *Mesh* sem fios, de modo a permitir um conjunto de serviços que deverão ser disponibilizados por qualquer fornecedor VoIP para uma rede comunitária (consultar a secção 10.8). È de referir que, este manual foi baseado no projecto *Wireless* África, desenvolvido pela instituição *Meraka* na África do Sul. No referido projecto, foi utilizado um *firmware Open Source* e gratuito, que foi desenvolvido pelo *Freifunk group*, em Berlim na Alemanha, e que poderá ser instalado em qualquer equipamento da *Linksys* (tais como: o WRT54G), transformando-o num nó *Mesh*.

# 7

# 7. Impacto e custos da migração para um sistema VOIP

Neste capítulo, será descrito o impacto sócio-económico sobre a migração para um sistema VoIP, apresentando as suas principais vantagens e desvantagens. Será ainda efectuado uma breve descrição dos aspectos mais importantes no dimensionamento de um fornecedor VoIP para as Redes Comunitárias.

## *7.1. Impacto da migração para um sistema VoIP em Redes Comunitárias*

Nas últimas décadas, a utilização massificada de tecnologias de banda larga constitui uma das evoluções mais marcantes no mundo das redes de telecomunicações. Contudo, devido a esta massificação, cresce o recurso a estas tecnologias para as comunicações quer ao nível empresarial, institucional ou pessoal.

Após uma profunda análise do que foi citado anteriormente, pode-se afirmar que a utilização das tecnologias com base nas redes *Wireless Mesh,* têm-se tornado num novo estímulo económico, não só para países industrializados (como por exemplo a América do Norte, Europa e Leste Asiático, como também, para os países com um fraco desenvolvimento económico (como por exemplo a África). Actualmente, existe um conjunto de iniciativas em *Wi-Fi* que estão sendo implementados quer ao nível nacional, local e regional.

É de salientar que, o impacto do uso das tecnologias baseadas em redes *Wi-Fi* e/ou *Mesh*, será ainda mais significativo nos países em desenvolvimento, onde serviços de telecomunicações são ainda muito limitados devido ao fraco poder económico. Contudo, com a invasão dos dispositivos móveis que contêm a integração de um conjunto de sistema de comunicação multimédia (tais como o *smartphone*, *netbook*, *iPad*, *iPhone*, etc.) e com a introdução dos *laptops* de baixo custo no mercado (um bom exemplo disso é o projecto OLPC - *One Laptop per Child*), poderão estimular rapidamente a economia de algumas regiões do interior de Portugal e a de países em desenvolvimento na África e na América Latina.

Hoje em dia, devido à massificação do uso das tecnologias baseadas em redes *wireless Mesh*, muitas empresas multinacionais estão constatando que existe uma nova oportunidade de investimento e de negócios no ramo das telecomunicações. É de referir que, ao implementar um provedor de serviços VoIP com base numa rede *wireless Mesh* a um custo reduzido em diversas zonas rurais, as populações terão novas oportunidades de lazer e de negócios. De notar que, num futuro próximo as redes *wireless Mesh* irão sendo instaladas de um forma global e maciça, com o intuito de promover novas oportunidades de negócios e munir as populações com novas ferramentas para criar negócios, proporcionando-lhes um aumento da produtividade e competitividade.

Cada vez mais, as redes *wireless Mesh* estão provando que as redes em larga escala e de alta confiabilidade, poderão ser implantadas de modo a fornecer um acesso sem fios contínuo às aplicações de banda larga, a um número elevado de utilizadores e em grandes regiões, com óptimo custo-benefício.

A seguir serão apresentados alguns exemplos de estudos que poderão servir de exemplos práticos ao que foi anteriormente citado.

### *7.1.1. Chittagong, em Bangladesh*

*Chittagong* é uma cidade portuária de *Bangladesh* com cerca de 3,5 milhões de habitantes. Nesta cidade existe uma rede *wireless Mesh* que proverá um serviço VoIP e acesso internet em banda larga para todos os clientes residenciais e corporativos [126].

Inicialmente, as instalações foram projectadas para servir cerca de 200.000 linhas de voz, mas contudo, pretendem ser expandidas não só por toda a parte da *Chittagong*, bem como as cidades vizinhas.

Actualmente, é de se notar que um país em desenvolvimento como *Bangladesh*, uma rede *wireless Mesh* confiável, poderá fornecer de um acesso à internet com banda larga de um modo rápido e económico aos cidadãos, de modo a estimular a economia da respectiva cidade.

Uma empresa de telecomunicações que possui uma rede de serviços baseados em endereços IP terá a vantagem de fornecer aos seus assinantes em áreas que actualmente não tem serviço telefónico, um melhor serviço de telefonia sem ter a necessidade de construir uma infra-estrutura tradicional de comunicações [126]. Contudo, para além desse serviço ser baseado completamente em tecnologias *wireless*, a instalação não irá depender de uma rede de distribuição eléctrica. Importa salientar que, de forma a assegurar que a rede irá trabalhar sob todas as condições, todos nós das redes *wireless*, irão funcionar com baterias que fornecem energia

durante um intervalo de seis dias consecutivos antes de serem recarregadas. Entretanto, poderá ainda ser utilizado um conjunto de baterias com painéis solares, de modo garantir o melhor funcionamento do sistema.

É de salientar que, embora haja um interesse global em implementar sistemas VoIP com base em redes *Mesh* em todo o mundo, existirão sempre algumas zonas remotas, cuja implementação dessas tecnologias poderão trazer alguns desafios aos fornecedores desses serviços. No entanto, enquanto há alguns países que estão procurando uma forma mais proactiva de estimular o crescimento e impulsionar as suas economias, outras poderão estar muito isoladas impossibilitando-os de ter as mesmas oportunidades de combater contra a infoexclusão. Assim sendo, uma solução viável para o combate à infoexclusão, será as redes *wireless Mesh*, que permitem prover um estímulo económico-social a um país em desenvolvimento, proporcionando-lhe uma entrada no mercado global.

Saliento ainda que, a implementação de um fornecedor VoIP com base em tecnologia *Mesh* nos países em desenvolvimento, traz consigo algumas questões que devem ser analisadas cuidadosamente antes de serem tomadas decisões relativas ao seu dimensionamento na prática. Estas decisões devem ser baseadas em alguns pré-requisitos antes de ser implantado o respectivo fornecedor VoiP para uma rede comunitária.

Em primeiro lugar, terá que haver um envolvimento entre as entidades públicas e o governo, no processo de implementação uma rede *wireless Mesh* para o país, de modo a possibilitar um melhor desenvolvimento das soluções de telecomunicações, proporcionando aos seus cidadãos uma igualdade de oportunidades e de acesso público à banda larga nas zonas rurais e semi-rurais a um custo acessível.

Em segundo lugar, deverão também existir profissionais especializados ou pessoas que possuem um certo *know-how* para entender a indústria internacional das telecomunicações, uma vez que a implementação desses serviços numa rede comunitária *Mesh*, irá permitir que o país possa desenvolver economicamente e industrialmente.

Em terceiro lugar, deverá existir um provedor de serviços VoIP para as Redes Comunitárias quer ao nível local ou internacional, que seja capaz de fornecer estes serviços para todas as zonas do país.

È de referir que, para que uma implementação de um fornecedor VoIP para uma determinada rede comunitária seja efectuada um sucesso, será sempre aconselhável ter em conta um plano ou um modelo de negócios de acordo com

situação económica do país e que a implementação do sistema seja baseada de acordo com o referido plano de negócios.

Contudo, será sempre necessário estabelecer uma relação bilateral de modo a que possam ser criadas algumas iniciativas inovadoras de programas económicos para educação e negócios que possam sustentar o crescimento da rede.

Resumindo, pode-se afirmar que com todos estes pré-requisitos um provedor de serviços poderá desenvolver um plano estratégico para a implementação de um conjunto de serviços baseados em tecnologias VoIP numa rede comunitária *Mesh*.

### *7.1.2. Países em desenvolvimento*

Para países em desenvolvimento, as tecnologias VoIP com base nas redes *Mesh* são as soluções atractivas, visto que, essas tecnologias funcionam com uma elevada taxa de sucesso, independentemente se a zona for montanhosa ou de localização remota. Como esses países possuem um certo desenvolvimento económico, será necessário apenas estabelecer um *link* – via terrestre, via satélite (*VSAT - Very Small Aperture Terminal*), ou um *link* de longa distância – para conectar a rede *Mesh* ao resto do mundo [126].

Actualmente as redes *Mesh* apresentam um largo espectro de benefícios, visto que, as suas implementações podem ser efectuadas em tempo recorde e com uma excelente relação custo-benefício relativamente à implementação das redes móveis ou qualquer outro serviço. Por exemplo, uma rede que contém um conjunto de nós cuja potência é suficiente para dar cobertura num raio de 16-24 quilómetros, permite fornecer um alcance máximo de serviço e é muito mais económico para ser implementado. Isto é, esta rede irá necessitar de menos nós de conexão (ligação *point-to-point*) para alcançar as áreas montanhosas ou de difícil acesso.

Para Nóbile Scandelari, analista de rede do *Serpro* e actual presidente da WIN em Brasil [132], uma rede *wireless Mesh* poderá fornecer aos seus potenciais utilizadores um excelente serviço, visto que, o seu *throughput* poderá alcançar até 108 Mbps próximo de um nó, e poderá variar num intervalo de 24 a 54 Mbps até cerca de 16 Mbps no limite da cobertura [126].

Feita essa análise, pode-se afirmar que um nó poderá servir muitos assinantes individuais, sendo que cada um deles obterá um serviço de banda larga de 1 Mbps a 3 Mbps, que será muito melhor e mais económico em relação ao serviço móvel. Por exemplo, o preço estipulado para 20 telemóveis, poderá aproximadamente equivaler a um serviço com cerca de 768 assinantes de voz numa rede que contém serviços baseados na tecnologia *Mesh* [126].

Nos países em desenvolvimento, como o Brasil e a África do Sul, uma rede *Mesh* implementada com base numa arquitectura multi-rádio (poderá conter três ou mais rádios), seria talvez uma óptima solução, visto que, um determinado município poderá dividir a largura de banda, de modo a fornecer aos seus cidadãos múltiplos serviços (tais como o acesso gratuito à internet com banda larga, voz, comunicações empresariais, serviços públicos, educação, saúde e segurança pública) de uma forma separada e com um *throughput* optimizado de acordo com as necessidades de cada serviço.

Importa salientar que, um dos benefícios mais importantes de uma rede *wireless Mesh* multi-rádio é a sua possibilidade de crescimento de acordo com a taxa de utilização da rede por parte da população. No entanto, a taxa de utilização poderá aumentar e novas tecnologias poderão ser adicionadas à rede, sem quaisquer necessidades de actualizações da solução ou dos serviços. De referir que, uma rede *Mesh* escalável poderá suportar múltiplos serviços, e aumentar a capacidade de retorno do investimento em relação às soluções que suportam apenas um único serviço.

Hoje em dia, a implementação de um fornecedor VoIP com base em tecnologias *Mesh* num país em desenvolvimento, poderá literalmente mudar a qualidade de vida das populações e estimular as suas economias. Importa salientar que, estes países possuem serviços de internet e telefónicos muitas vezes limitados, e o custo destes serviços são bastantes elevados. Nesses países em desenvolvimento, poderão existir algumas empresas que não possuem qualquer tipo de acesso a comunicação de dados.

Os serviços disponibilizados aos utilizadores pelas empresas fornecedoras são frequentemente limitados e dispendiosos, obrigando-os a esperar por um período indeterminado até que o serviço seja instalado. Consequentemente, os utilizadores serão excluídos automaticamente de terem o acesso gratuito de utilização da Internet em banda larga. Sendo assim, optar por implementar e/ou aderir a um serviço móvel não seria uma solução viável para a resolução deste problema, visto que, este serviço é muito caro para as pessoas com pouco poder económico.

Resumindo, a solução viável seria a adesão completa aos serviços que utilizam a tecnologia VoIP em redes *Mesh*, visto que, esta solução permite a um utilizador que possui um dispositivo com capacidade *Wi-Fi* (como por exemplo um computador portátil, PDA ou telemóvel), de se autenticar numa rede com um serviço barato e muito rápido [126].

Importa salientar que, uma aplicação VoIP como o *Skype*, funcionando numa rede *Mesh* poderá não só fornecer aos seus potenciais clientes um serviço de voz

gratuito, como também, permitir às empresas angariar uma receita no valor de R$4.000,00 (≈1.665,84¤) por ano. Naturalmente, os preços dos serviços VoIP estão ficando cada vez mais económicos e salienta-se o recém lançado Google Voice que permite chamadas internacionais a custos reduzidos, o envio gratuito de mensagens para números de telefone dentro do mesmo país e permite recorrer ao serviço enquanto aplicação nativa para o telefone, assim como as chamadas gratuitas efectuadas *Skype-to-Skype,* quer ao nível nacional ou internacional. [126].

### *7.1.3. Visão Geral*

Uma implementação de um fornecedor VoIP para uma rede comunitária *Mesh* possibilitará a criação de uma infra-estrutura de comunicação com alta qualidade, fornecendo aos seus utilizadores uma melhor qualidade de serviços e a custo zero, que consequentemente provocará um grande impacto nos negócios locais e na economia mundial.

Assim sendo, pode-se afirmar que um país em desenvolvimento poderá criar novas oportunidades de negócios, atraindo empresas multinacionais que queiram investir capital no mercado empresarial do referido país, devido aos serviços disponibilizados com base na tecnologia *Mesh*.

Essa tecnologia permite-lhes não só expandir os seus negócios, como também, facilitar a comunicação directa entre os seus potenciais clientes e os seus colaboradores em todo o mundo a um custo muito reduzido.

Saliento ainda que, as redes *Mesh* poderão também estimular o crescimento da investigação científica ao nível pessoal e empresarial, permitindo que as empresas locais desenvolvam e comercializam os seus produtos para além das fronteiras do seu estado ou país.

Futuramente, as redes *Mesh* irão provocar um impacto mais profundo e a longo prazo nas nossas sociedades, visto que, em geral irão interligar as sedes dos concelhos abrangidos, edifícios públicos e de interesse público, instituições do ensino superior, centros tecnológicos, e zonas e parques industriais.

Entretanto, apesar de existir actualmente bastantes esforços quer ao nível de investigação científica, quer ao nível de implementação e de todos os benefícios económicos que uma rede *Mesh* poderá proporcionar aos seus utilizadores, implementar uma rede *Mesh* poderá requerer mais recursos económicos do que possivelmente poderão estar disponíveis.

Resumidamente, pode-se afirmar que deverá sempre existir iniciativas inovadoras destinadas a promover a adopção dessas práticas e introduzi-las na Sociedade de Informação e do Conhecimento.

Estes projectos permitem não só estabelecer, como também, manter e reembolsar os custos de implementação da rede *Mesh*. No entanto, há que existir sempre uma cooperação por parte das entidades publicas e/ou privadas com o governo, de modo a que esses projectos possam ser financiados com o intuito de combater a infoexclusão no país [126].

## *7.2. Custos de implementação de um sistema VoIP em Rede Abertas*

Neste ponto, não será apresentado as informações sobre o custo estimativo de uma implementação de um sistema VoIP para as Redes Comunitárias, visto que, actualmente os preços dos equipamentos na área da tecnologia informática estão constantemente sujeitos a sofrer alterações no seu valor real.

Contudo, será apresentado um conjunto de informações que poderão ajudar a ter uma noção dos custos de implementação de um sistema VoIP para uma rede comunitária *Mesh*.

Tendo em conta a análise elaborada nos capítulos anteriores serão necessários os seguintes equipamentos:

- Servidores (em regime de redundância) – Duplo Processador a 3 GHz, 4GB RAM, 36 GB SCSI em RAID 1 e 4 placas de rede 10/100 [1];
- *Gateway* contendo portas de interligação à rede PSTN;
- *Switchs* contendo várias portas e com capacidade VLAN;
- Adaptadores PoE (*Power-over-Ethernet*): estes equipamentos serão utilizados caso for necessário implementar um nó *Mesh* exterior;
- Antenas Direccionais de alto ganho e/ou de ganho muito alto: poderá ser utilizado as antenas direccionais *Yagi* e *Painel*, dependendo das necessidades da implementação do respectivo protótipo;
- Antenas Omnidireccionais: este equipamento será utilizado para as *hotspots*;
- Protectores de relâmpagos (*Lighting protectors*):
- *Router Wireless* da *Linksys*;
- Infraestrutura de acolhimento do equipamento;
- Ligação à internet através de linha dedicada com IP fixos;
- Ligação à rede PSTN com pelo menos 30 linhas disponíveis;

Relativamente, ao nível de recursos humanos será também necessário:

- Um administrador ou gestor de todo o sistema num regime *fulltime,* de modo a garantir uma melhor prestação de serviços;
- Investigadores científicos de modo a acompanhar a evolução dos serviços que usam a tecnologias *Mesh*.
- Programadores para o portal *web* (fase inicial);
- Serviço de apoio ao cliente (*Helpdesk* ou *Callcenter*);

Importa salientar que, para além de toda a informação disponibilizada sobre os equipamentos técnicos e recursos humanos, será ainda necessário não só cumprir todos os artigos abordados na Lei nº 5/2004 referente ao fornecimento de redes e comunicações electrónicas (Artigo 21 da Lei 5/2004), como também, elaborar uma consulta minuciosa sobre toda a documentação disponibilizada pela ANACOM - Autoridade Nacional de Comunicações, com o intuito de cumprir todos os pré-requisitos estabelecidos perante a prestação deste serviço [1].

# 8

# 8. Conclusões e Trabalho Futuro

Neste capítulo, são apresentadas as conclusões finais deste projecto e serão apresentados algumas soluções para que futuramente possam dar um melhor contributo nos aspectos relacionados com esta tecnologia.

Naturalmente, dada a qualidade das infrastuturas existentes em diversos países desenvolvidos, o enfoque deste trabalho esteve sobretudo na produção de uma solução acessível, escalável e adaptável a espaços territoriais periféricos, nomeadamente, algumas regiões do interior de Portugal ou vastas zonas da África e da América Latina.

Após a elaboração deste projecto, onde foi efectuado com minúcia um estudo sobre os aspectos relacionados com a operacionalização das tecnologias VoIP para as redes comunitárias, pode-se concluir que o uso dessas tecnologias permite o seguinte:

- Implementar um fornecedor VoIP para as redes comunitárias, recorrendo não só à tecnologia *Mesh*, como também, ao uso de *software* gratuito e *Open Source*;
- Criação infra-estruturas de comunicação com alta qualidade, fornecendo aos seus utilizadores uma melhor qualidade de serviços e a custo zero;
- Massificação do acesso e utilização da Internet em banda larga para a população de uma determinada zona residencial dos países em desenvolvimento;
- Criação de novas oportunidades de negócios, atraindo empresas multinacionais que queiram investir capital no mercado empresarial, visto que, haverá um aumento da produtividade e competitividade das empresas através dos negócios electrónicos;
- Combater a infoexclusão;

- Garantir um conjunto de serviços públicos de qualidade, que permitem um apoio sistemático à modernização da Administração Pública, racionalização dos custos e promoção da transparência;
- Possibilidade de interligação com a rede telefónica – PSTN;
- Tolerância a falhas;
- Redução de custos de instalação e exploração dos equipamentos;
- Flexibilidade e mobilidade total, visto que, este sistema poderá ser aproveitado como base para o fornecimento de serviços diferenciados, individualizados e adaptados de acordo com a necessidade de cada utilizador.

Embora a utilização dos serviços VoIP com base na tecnologia *Mesh* possa trazer inúmeras vantagens para uma rede comunitária, a implementação desses serviços requerer não só alguma investigação científica como também, alguns recursos económicos de modo a permitir uma melhor gestão e controle da rede a ser implementada.

Em suma, pode-se afirmar que deverão sempre existir iniciativas inovadoras destinadas a promover uma melhor adopção dessas práticas e introduzi-las na Sociedade de Informação e do Conhecimento. Contudo, deverá existir também, alguma cooperação entre as entidades públicas e/ou privadas com o governo para que essas iniciativas possam ser financiadas permitindo, assim, o combate à infoexclusão nos países em desenvolvimento.

# 9

# 9. Bibliografia e Sites Consultados

Neste capítulo, é feita uma referência às bibliografias e aos sites utilizados para a realização deste trabalho.

## 9.1. *Bibliografia e Sites consultados*

[1] MARQUES, Nuno Alexandre A. – Voz sobre IP (VoIP) para redes comunitárias de Regiões Digitais, Tese Mestrado MIEET, Universidade de Aveiro, 2008.

[2] ICP. Autoridade Nacional de Comunicações – Relatório sobre a situação das comunicações em 2005 Lisboa, Portugal, 2005 p232. Disponível em versão pdf em http://www.anacom.pt/template12.jsp?categoryId=197822 [citado em Novembro de 2009].

[3] SOUSA, J. P. P., sIPtel – Um sistema de IPtel com suporte para vídeo utilizando o protocolo SIP, Tese Mestrado, FEUP, 2003.

[4] SMITH, Jared; MEGGELEN, Jim Van; MADSEN, Leif; O´Reilly – Asterisk: The Future of Telephony, 2005.

[5] GOMILLION, David; DEMPSTER, Barrie – Building Telephony Systems with Asterisk, Packt Publishing, 2006, ISBN 1-904811-15-9.

[6] WALLINGFORD, Theodore; O´Reilly – Switching to VoIP. 30/06/2005

[7] Apontamentos da disciplina de Telemática nas Organizações e na Sociedade do ano lectivo de 2006/07 gentilmente disponibilizados pelo professor Dr. Oliveira Duarte e disponíveis via URL em http://gsbl.det.ua.pt/tos/default.asp (Novembro de 2009).

[8] JOHNSTON, Alan B. – SIP: Understanding the Session Initiation Protocol, 2ª ed. Artech

House, 2004, ISBN 1-58053-655-7.

[9] GONÇALVES, E. Flávio – Building Telephony Systems with OpenSER, Packt Publishing, 2008, ISBN 978-1-847193-73-5.

[10] SIMIONOVICH, Nir – AsteriskNOW, Packt Publishing, 2008, ISBN 978-1-847192-88-2

[11] STALLINGS, William – Data and Computer Communications, 5ª ed. Prentice Hall, 1997, ISBN 0-02-415425-3.

[12] RFC971:"IP:Internet Protocol", Internet Engineering Task Force's - IETF, Network Working Group, disponível em http://www.ietf.org.html.

[13] GARRISON, Kerry – Trixbox CE 2.6: Implementing, managing, and maintaining an Asterisk-based telephony system, Packt Publishing, 2009, ISBN 978-1-847192-99-8

[14] SOUSA, Luís António Pereira – Avaliação de desempenho do PBX Asterisk, Tese Mestrado, IST, 2008.

[15] LEITÂO, Jorge André e SERRÂO, Mário – VoIP sobre wireless, Mestrado em Redes e Serviços de Comunicação, FEUP, 2003.

[16] BATES, Regis J. (Bud) - Broadband Telecommunications Handbook, 2ª ed., McGraw-Hill, 2002, ISBN 0□07□139851□1

[17] RUSSELL, Travis – SESSION INITIATION PROTOCOL (SIP) Controlling Convergent

Networks, McGraw-Hill, 2008, ISBN 0-07-148852-9

[18] ANACOM – Relatório da Consulta Pública sobre a Abordagem regulatória aos serviços de voz suportados na tecnologia IP (VoIP), Fevereiro 2006 [citado em Novembro de 2010].

Disponível em versão pdf em <http://www.anacom.pt/template12.jsp?categoryId=183042>.

[19] http://www.anacom.pt/ – Setembro de 2009
[20] http://www.anacom.pt/txt/template25.jsp?categoryId=168642 – Setembro de 2009
[21] http://en.wikipedia.org/wiki/VoIP – Novembro de 2009
[22] http://en.wikipedia.org/wiki/H323 – Novembro de 2009
[23] http://pt.wikipedia.org/wiki/SIP – Novembro de 2009
[24] http://www.teleco.com.br/es/es_tecvoip.asp – Junho de 2009
[25] http://www.cs.columbia.edu/sip/ – Agosto de 2009
[26] http://www.voip-info.org/wiki/ – Julho de 2009
[27] http://www.fccn.pt – Novembro de 2009
[28] http://www.lusosis.pt/VoIP_SIP.htm - Outubro de 2009
[29] http://www.voipthink.com/ – Novembro de 2009
[30] http://www.voip.pt/ – Novembro de 2009
[31] http://www.cisco.com/ – Julho de 2009
[32] http://en.wikipedia.org/wiki/Comparison_of_VoIP_software – Novembro de 2009
[33] http://www.mediaproxy-ng.org/ – Novembro de 2009
[34] http://mit.edu/sip/sip.edu/ – Dezembro de 2009
[35]http://www.anacom.pt/streaming/radiomovel_voip.pdf?categoryId=183122&contentId=337227&field=ATTACHED_FILE – Dezembro de 2009
[36] http://mit.edu/sip/sip.edu/ – Dezembro de 2009
[37] http://www.kamailio.org/w/ – Março de 2010
[38] http://www.asterisktutorials.com – Março de 2010
[39] http://www.trixbox.org – Março de 2010
[40] http://www.the-asterisk-book.com/ – Março de 2010
[41] http://www.asteriskguru.com/ – Março de 2010
[42] http://www.3cx.com.br/voip-sip/fxs-fxo.php – Março de 2010
[43] http://www.opensips.org/ – Abril de 2010
[44] http://en.wikipedia.org/wiki/OpenSER – Abril de 2010
[45] http://pplware.sapo.pt/networking/elastix-o-servidor-voip-para-todos/ – Abril de 2010
[46] http://sourceforge.net/projects/elastix/files/ – Abril de 2010
[47] http://www.trixbox.com/products/trixbox-pro/tech-architecture – Abril de 2010
[48] http://paginas.fe.up.pt/~ee07055/mieec/index.php – Abril de 2010
[49] http://www.kamailio.org/docs/openser-devel-guide/ – Abril de 2010
[50] http://kennedy.jimdo.com/asterisk__trixbox.php – Abril de 2010
[51] http://www.asterisk.pt/ – Abril de 2010
[52] http://www.asterisk.org – Abril de 2010
[53] http://www.asteriskonline.com.br/ – Abril de 2010
[54] http://www.computerworld.com.pt/2009/02/17/ip-pbx/ – Abril de 2010
[55] http://clevitonmendes.blogspot.com/2008/06/integrao-do-asterisk-com-openser.html – Abril de 2010
[56] http://www.voip-info.org/wiki/view/OpenSER – Abril de 2010
[57] http://www.iptel.org/ – Abril de 2010
[58] http://mediaproxy.ag-projects.com/ – Abril de 2010
[59] http://mediaproxy-ng.org/ – Abril de 2010
[60] http://wireless.com.pt/ – Abril de 2010
[61] http://www.ptwifi.pt/ – Abril de 2010
[62] http://www.locustworld.com/ – Abril de 2010
[63] http://www.gta.ufrj.br/grad/10_1/malha/index.html – Setembro de 2010
[64] http://www.moskaluk.com/voip_using_wireless_mesh_infrast.htm – Setembro de 2010
[65] http://www.wiligear.com/wiki/index.php/WILI_MESH_Installation_Guide – Setembro de 2010

[66] http://wirelessafrica.meraka.org.za/wiki/index.php/Wireless_Africa_Home_Page – Setembro de 2010
[67] http://downloads.openwrt.org/whiterussian/packages/ – Outubro de 2010
[68] http://www.oreillynet.com/pub/a/wireless/2004/01/22/wirelessmesh.html – Outubro de 2010
[69] http://pdos.csail.mit.edu/roofnet/design/ – Outubro de 2010
[70] http://paginas.fe.up.pt/~ee99207/index.html – Outubro de 2010
[71] http://paginas.fe.up.pt/~ee07055/mieec/index.php – Outubro de 2010
[72] http://paginas.fe.up.pt/~ee03172/dst_estarte.php – Outubro de 2010
[73] http://en.wikipedia.org/wiki/WRT54G – Outubro de 2010
[74] http://www.strixsystems.com/case-studies/voice.asp – Outubro de 2010
[75] http://www.gta.ufrj.br/seminarios/semin2003_1/fernandes/MAC_1.htm – Outubro de 2010
[76] http://www.ligarportugal.pt/ – Outubro de 2010
[77] http://www.hollmanenciso.com/es/category/etiquetas/mesh – Outubro de 2010
[78] http://www.umic.pt – Novembro de 2010
[79] http://www.open-mesh.org/wiki/MeshLinux – Novembro de 2010
[80] http://www.lugro-mesh.org.ar/ – Novembro de 2010
[81] http://nightwing.lugro-mesh.org.ar/ – Novembro de 2010
[82] http://www.zoociedad.org/wiki/Red_Comunitaria_Libre – Novembro de 2010
[83] http://www.debian.org/ – Novembro de 2010
[84] http://www.zoociedad.org/cogitowireless/ – Novembro de 2010
[85] http://el-directorio.org/inalambricadc – Novembro de 2010
[86] http://oldwiki.openwrt.org/Hardware%282f%29Linksys.html – Novembro de 2010
[87] http://es.wikipedia.org/wiki/Netsukuku – Novembro de 2010
[88] http://www.buenosaireslibre.org/ – Novembro de 2010
[89] http://openwrt.org/ – Novembro de 2010
[90] http://wiki.openwrt.org/oldwiki/OpenWrtDocs/IPTables – Novembro de 2010
[91] http://wiki.openwrt.org/oldwiki/OpenWrtDocs – Novembro de 2010
[92] http://pt.wikipedia.org/wiki/Freifunk – Novembro de 2010
[93] http://start.freifunk.net – Novembro de 2010
[94] http://download-master.berlin.freifunk.net/ipkg/_trx/ – Novembro de 2010
[95] http://www.openwireless.ch/ – Novembro de 2010
[96] http://olsr.org/ – Novembro de 2010
[97] http://www.anacom.pt/render.jsp?contentId=952401 – Novembro de 2010
[98] http://www.wireshark.org/ – Novembro de 2010
[99]http://www.the-asterisk-book.com/unstable/installation-1.4-debian-4.0.html – Novembro de 2010
[100] http://freeradius.org – Novembro de 2010
[101] http://cdrtool.ag-projects.com – Novembro de 2010
[102] http://www.sermyadmin.org – Novembro de 2010
[103] http://www.elastix.org/ – Novembro de 2010
[104]http://www.asipto.com/pub/openser-devel-guide – Julho de 2009 e Novembro de 2010.

[105] SELADA, Rodrigo Sastre Cordeiro – Redes Wireless de Banda Larga, Mestrado em Informática, Universidade de Trás-os-Montes e Alto Douro, 2008. – Outubro de 2010.

[106] RODRIGUES, Nuno José Pereira Farias – Redes Mesh Sem-Fios, Tese de Mestrado, FEUP, 2009. – Outubro e Novembro de 2010.

[107] www.dlink.com – Novembro de 2010.
[108] http://herbert.the-little-red-haired-girl.org/en/nylon/index.html – Outubro de 2010.
[109] http://www.linksys.com/ – Outubro de 2010.
[110] http://www.meshnode.org – Outubro de 2010.
[111] http://www.dd-wrt.com/site/index – Outubro de 2010.
[112] http://wiki.antcor.com/wiki/index.php/Main_Page – Outubro de 2010.
[113] http://www.pfsense.org/ – Outubro de 2010.
[114] http://www.mikrotik.com/ – Outubro de 2010.
[115] http://www.putty.org/ – Outubro de 2010.
[116] http://www.tcpdump.org/ – Outubro de 2010.

[117] JOHNSON, David, MATTHEE Karel, SOKOYA Dare, MBOWENI Lawrence, MAKAN Ajay, and KOTZE Henk – Building a Rural Wireless Mesh Network, Wireless África, Meraka Institute, South África, October 2007. – Outubro e Novembro de 2010.

[118] http://www.ccpu.com/trillium-protocol-software-products/voip-voice-over-ip/ – Outubro de 2010.

[119] www.fe.up.pt/~jruela/Apontamentos/Arq_IETF.pdf – Outubro de 2010.

[120] CARDOSO, Paulo e CARDOSO, Vitor – VoIP – Características e Estado da Arte, Trabalho para a disciplina de Serviços Multimédia, FEUP, 2004. – Outubro e Novembro de 2010.

[121] http://www.ipworld.pt/VoIP.aspx – Outubro de 2010.

[122] http://www.asteriskguide.com/mediawiki/index.php/Introduction_to_Asterisk – Maio e Novembro de 2010.

[123] http://cuwireless.net – Novembro de 2010.

[124] http://www.tibtec.org – Novembro de 2010.

[125] http://www.computerworld.com.pt/tag/uniao-europeia – Dezembro de 2010.

[126]http://www.momentoeditorial.com.br/index.php?option=com_content&task=view&id=6502&Itemid=43 – Novembro de 2010.

[127] http://mesh.ic.uff.br/ – Novembro de 2010.

[128] http://www.vmesh.inf.uth.gr – Novembro de 2010.

[129] http://www.pdos.csail.mit.edu/roofnet – Novembro de 2010.

[130] http://www.mesh.net – Novembro de 2010.

[131] http://wirelessafrica.meraka.org.za/wiki/index.php/OLSR_Dot_Draw – Novembro de 2010.

[132] www.wnint.com.br – Novembro de 2010.

[133] http://www.ieee.org/index.html – Novembro de 2010.

[134] http://www.asteriks.com.br/html/ – Julho e Novembro de 2010.

[135] KELLER, Alexandre – Asterisk na Pratica, 2009, ISBN 9788575221839. – Outubro e Novembro de 2010.

[136] KELLER, Alexandre – Curso de Asterisk Avançado, Ministrado pelo Grupo Galileu em Lisboa, 2010. – Julho e Novembro de 2010.

[137] IEEE 802.11s. D1.07. *Draft STANDARD for Information Technology-Telecommunications and information exchange between system-Local and metropolitan area networks-Specific requirements*. 2007. – Junho e Novembro de 2010.

[138] http://www.cm-mirandela.pt/index.php?oid=7127 – Junho e Dezembro de 2010.

# A

## 10. Anexos

Neste capítulo, estão anexos alguns documentos importantes e que tiveram um grande contributo na implementação do protótipo do VoIP para as Redes Comunitárias. Será apresentado, de uma forma detalhada um conjunto de manuais de instalação dos principais componentes que correspondem ao diagrama de blocos do referido protótipo VoIP a ser implementado.

### *10.1 Instalação do Sistema Operativo Debian*

Neste ponto, será apresentada um manual de instalação do Sistema Operativo Debian de uma forma detalhada de modo a permitir ao administrador do sistema uma melhor interacção com o sistema em causa.

#### *10.1.1 Download do ficheiro de instalação do S.O Debian*

Para efectuar *download* do ficheiro de instalação do Sistema Operativo *Debian* devem ser executados os seguintes passos:

1. Na página oficial do projecto *Debian* (*http://www.debian.org*), seleccionar a opção "***Imagens de CD ISO"*** do menu lateral esquerdo da referida página para efectuar o *download* da imagem ISO (observar a seguinte figura);


**Figura 89 – Menu Principal do site oficial do Projecto Debian [83].**

2. Seguidamente, seleccionar a opção ***"baixar imagens CD/DVD usando HTTP ou FTP"***.

3. Em seguida, seleccionar o ficheiro pretendido para efectuar uma instalação adequada à arquitectura do servidor. Neste caso em específico, deverá ser escolhido o ficheiro ***"debian-40r4a-i386-netinst.iso"*** correspondente à arquitectura i386.

   **NOTA:** Importa salientar que, a referida versão será suficiente para instalar o sistema base pretendido. É de referir que, durante a fase de instação do referido sistema operativo, será efetuado uma actualização dos restantes pacotes de uma forma automática a partir do servidor debian;

4. A seguir, deverá ser gravado o conteúdo do ficheiro ISO para um CD, usando uma aplicação adequada para a gravação de CD's, como por exemplo, *Nero Burning ROM* ou *CDBurnerXP*;

5. Após efectuar a gravação do respectivo ficheiro, o CD de instalação do sistema operativo *Debian* estará pronto a ser utilizado.

   **NOTA:** É de salientar que, caso for necessário a utilização de uma *VMware* (máquina virtual), não será necessário utilizar o referido CD, visto que, será possível utilizar directamente o ficheiro ISO para efectuar a instalação do S.O Debian.

### *10.1.2 Instalação do Sistema Operativo Debian*

Para efectuar a instalação do Sistema Operativo *Debian* devem ser executados os seguintes passos:

1. Introduzir o CD de instalação do SO *Debian* na máquina onde irá ser feito a devida instalação. Em seguida, a respectiva máquina deverá efectuar um arranque a partir do referido CD;

2. Seguidamente, será ilustrada um menu inicial de instalação (observar na figura a seguir). Em seguida, seleccionar a opção ***"Enter"***, de modo a dar início ao processo de instalação;


**Figura 90 – Menu Inicial de instalação do S.O Debian.**

3. A seguir, será despoletado um menu onde o administrador do sistema irá escolher o idioma pretendido para ser instalado na respectiva máquina. Seguidamente deverá seleccionar ***"Enter"***, para confirmar a opção pretendida.


**Figura 91 – Menu de Idiomas do S.O Debian.**

4. No menu de Idiomas, poderá ainda ser seleccionado o país, o território ou a área de localização da respectiva máquina. A seguir deverá ser escolhido o país pretendido, sendo que neste caso em concreto é ***"Portugal"*** e seleccionar ***"Enter"***, para confirmar a opção pretendida.

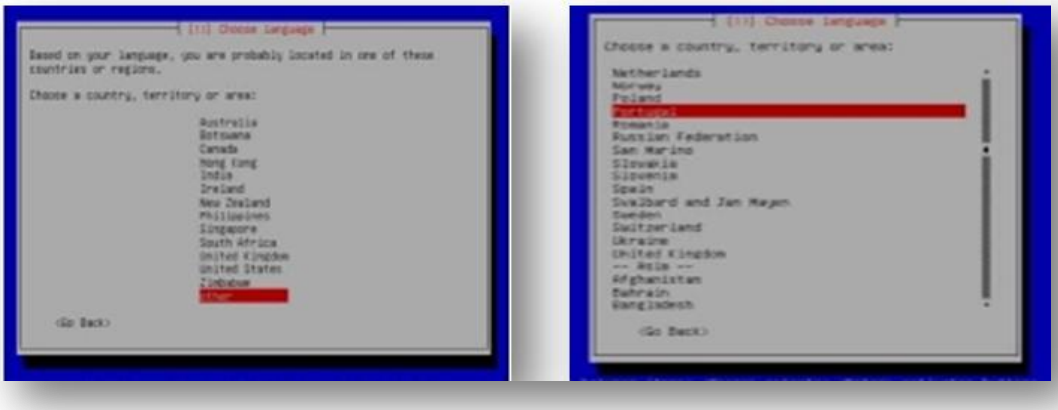


**Figura 92 – Menu de selecção do país, território ou área.**

5. Seguidamente, será apresentado um menu que corresponde à selecção e configuração do teclado a ser utilizado durante o processo de instalação do respectivo S.O. Seleccionar a opção ***"Português"***;

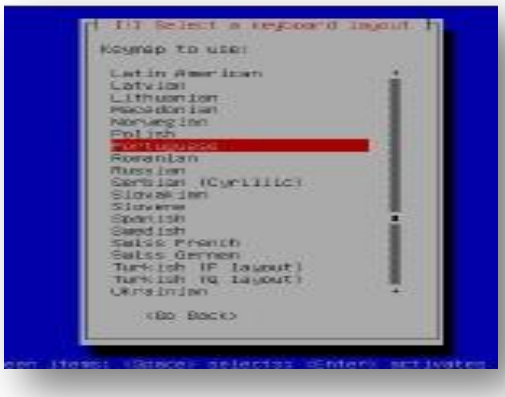


**Figura 93 – Menu de configuração do teclado.**

6. Atribuir um nome à respectiva máquina onde irá ser instalado o servidor *OpenSer*, atribuindo-lhe um determinado domínio (exemplo: labvoipua.com).

**Figura 94 – Menu de configuração do domínio *network*.**

7. No menu de partição de disco, configurar o modo de partição pretendido para a respectiva máquina e em seguida seleccionar o disco a ser efectuado o particionamento.

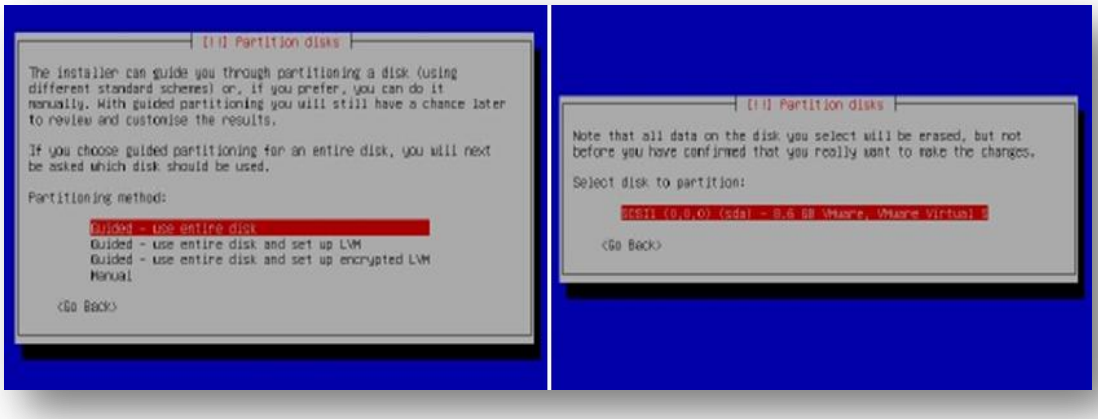



**Figura 95 – Menu de Partição de discos.**

8. No menu de partição de disco, poderá ainda ser seleccionado a opção ***"All files in one partition"***, de modo a ser utilizado apenas uma partição.

9. A seguir, deverá ser teminado o processo de partição do respectivo disco seleccionando a opção ***"Finish partitioning and write changes to disk"***, e em seguida aplicar as alterações pretendidas no disco.

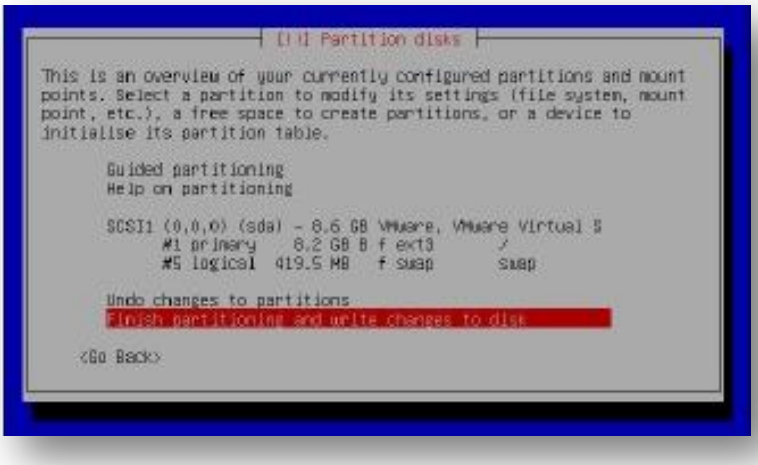



**Figura 96 – Menu de Partição de discos – Finalização do processo de criação.**

10. Em seguida, deverá seleccionar a opção ***"Yes"***, para confirmar as alterações pretendidas.

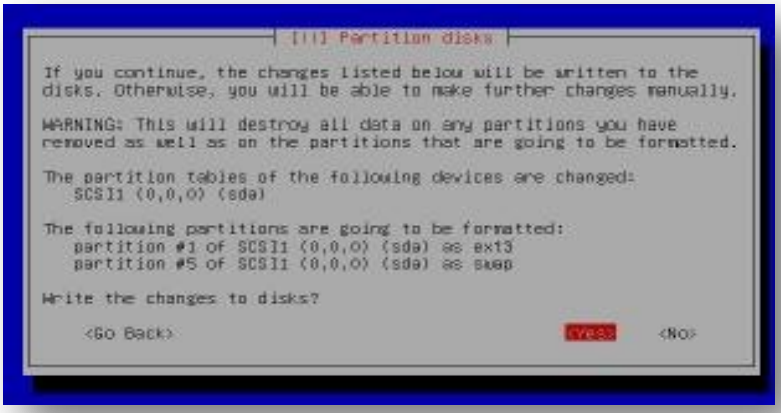



**Figura 97 – Menu de Partição de discos – Confirmação das altereções efectuadas.**

11. Em seguida, deverá escolher o local para a definição da zona horária pretendida, como por exemplo, seleccionar a opção ***"Lisbon"***.

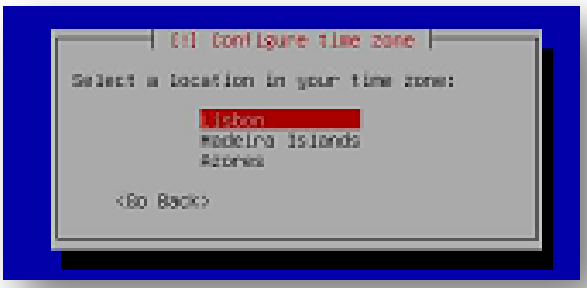



**Figura 98 – Configuração da zona horária.**

12. A seguir, deverá ser introduzido uma *password* para a conta ***root*** e seleccionar a opção ***"Continue"*** para confirmar a opção pretendida.

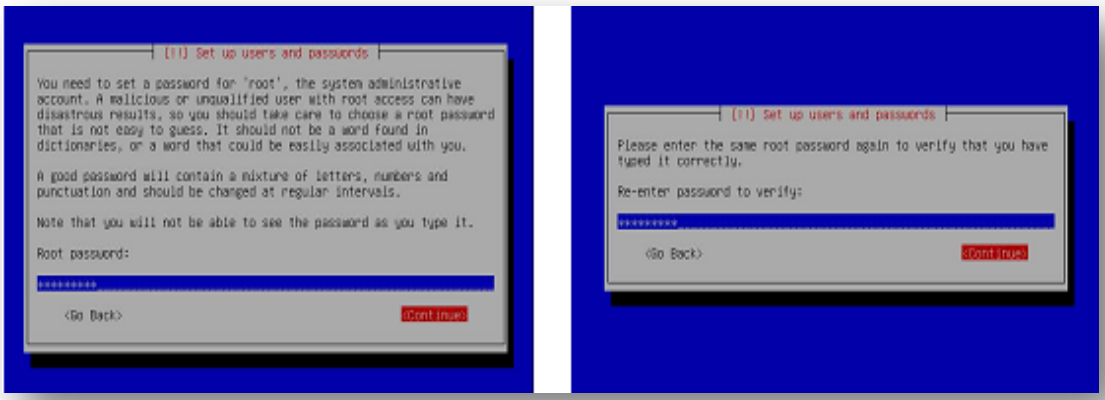



**Figura 99 – Menu de configuração do utilizador.**

13. No menu de configuração do utilizador, introduzir um nome para uma conta de utilizador (como por exemplo o ***"openser"***). A seguir, introduzir um nome de login (como por exemplo o ***"openser"***) e seleccionar a opção ***"Continue"*** para confirmar a opção pretendida.

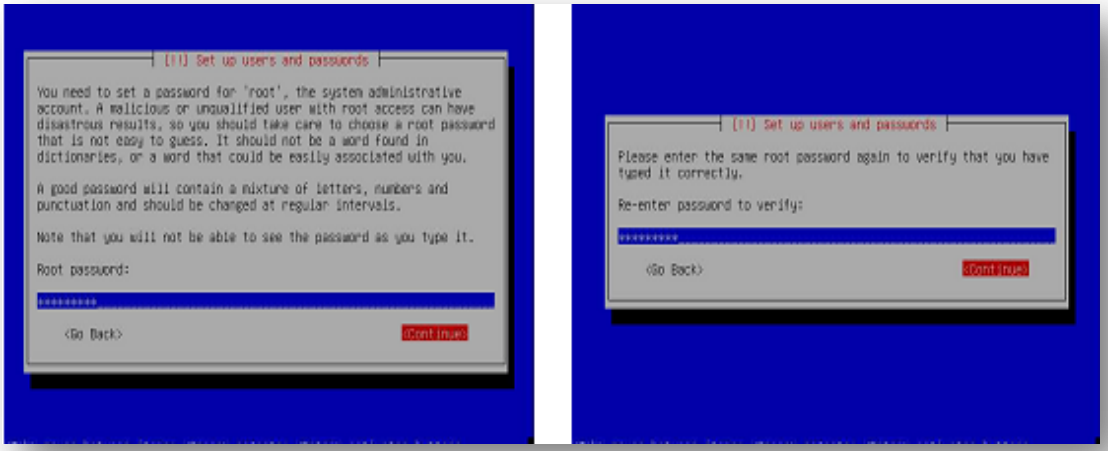



**Figura 100 – Menu de configuração do utilizador e da password.**

14. A seguir, deverá ser introduzido uma *password* e reintroduzi-lo novamente para confirmar a opção pretendida.

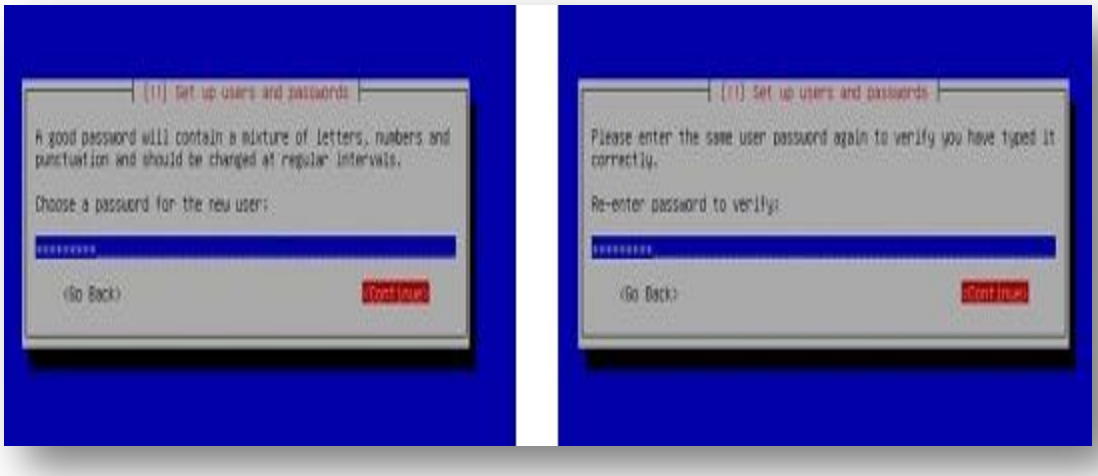



**Figura 101 – Menu de configuração do utilizador - Reintrudução da password.**

15. Seguidamente, deverá ser configurado o gestor de pacotes, seleccionando a opção ***"Yes"*** para confirmar a opção pretendida.

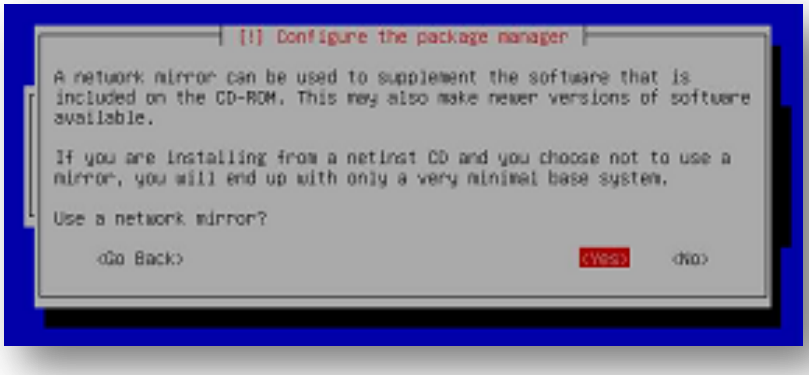



**Figura 102 – Menu de configuração do gestor de pacotes.**

16. Seguidamente, no menu da configuração do gestor de pacotes, deverá ser seleccionado o país e indicar o servidor pretendido para continuar o processo de configurador do referido gestor de pacotes.

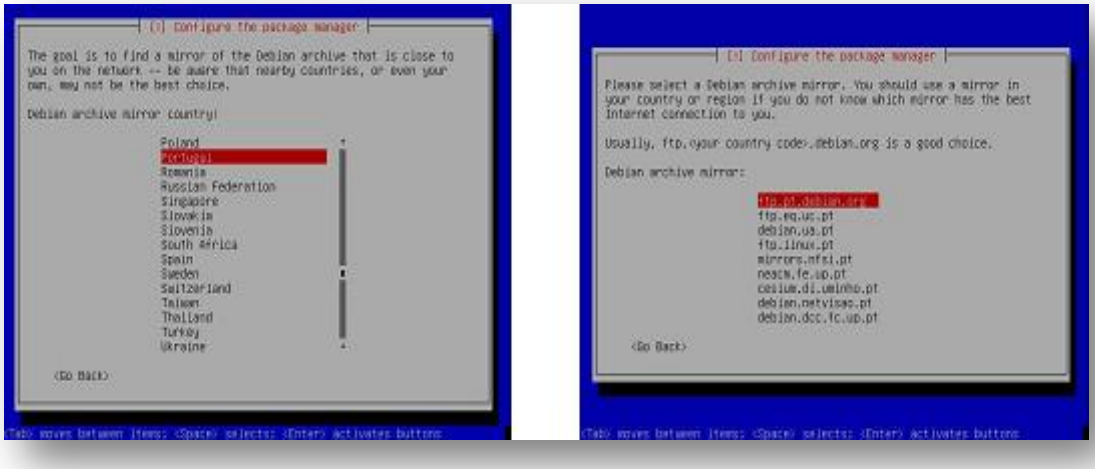



**Figura 103 – Menu de configuração do gestor de pacotes.**

17. No menu da configuração do gestor de pacotes, caso for necessário poderá ainda ser configurado o servidor *proxy*.

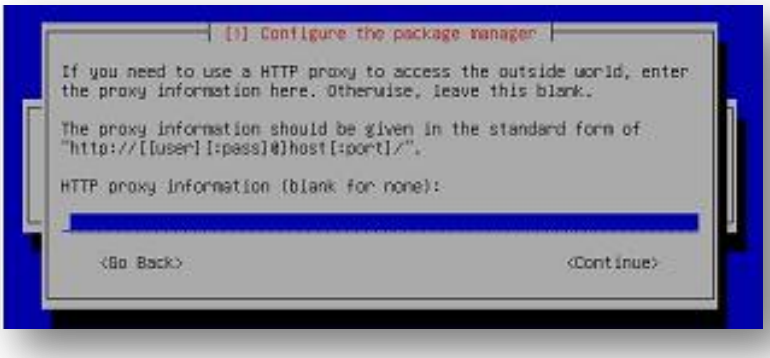



**Figura 104 – Configuração do servidor proxy.**

18. No menu da configuração do gestor de pacotes, caso for necessário participar no concurso de selecção dos pacotes mais populares, deverá ser seleccionado a opção ***"Yes"***.

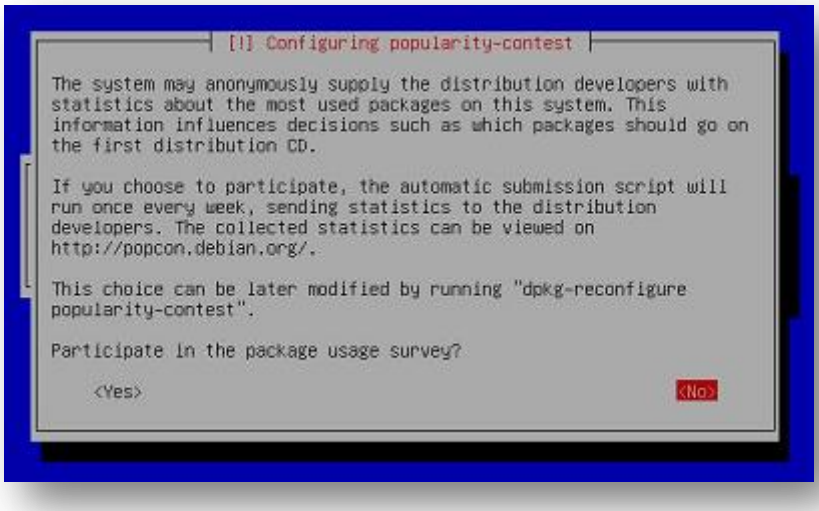



**Figura 105 – Menu de configuração dos pacotes mais populares.**

19. No menu da configuração do *software*, escolher opção pretendida, sendo neste caso em específico deverá ser escolhido a opção ***"Standard System"***.


**Figura 106 – Menu de configuração do software pretendido.**

20. No menu da instalação do GRUB *(GRand Unified Bootloader)*, seleccionar a opção ***"Yes"***, para instalar o gestor de arranque GRUB.

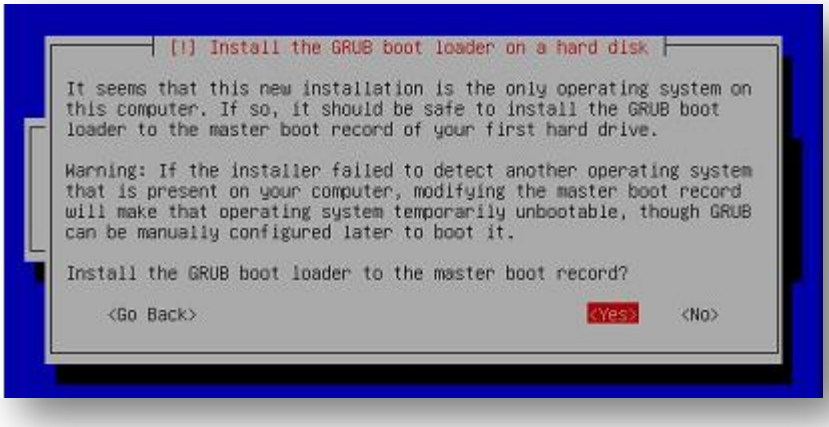



**Figura 107 – Menu de instalaçção do GRUB (GRand Unified Bootloader).**

21. No menu de finalização da instalação do SO *Debian*, seleccionar a opção ***"Continue"***, para concluir todo o processo de instação do respectivo sistema.

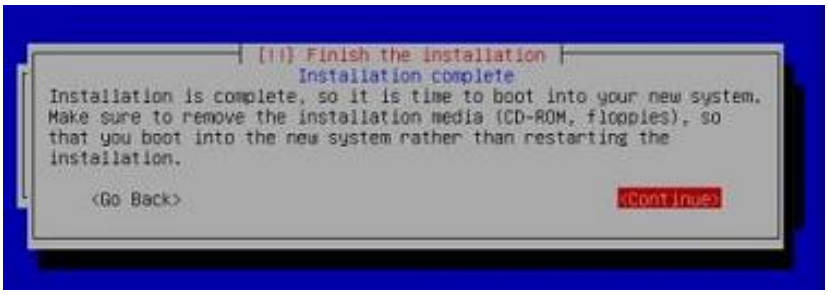



**Figura 108 – Menu de finalização da instalação do SO Debian.**

22. Após a instalação do sistema operativo *Debian*, será despoletado ao gestor do sistema, um novo aspecto visual do referido sistema, sendo que deverá ser usado em modo CLI (*Command Line Interface*), conforme ilustra a seguinte figura.

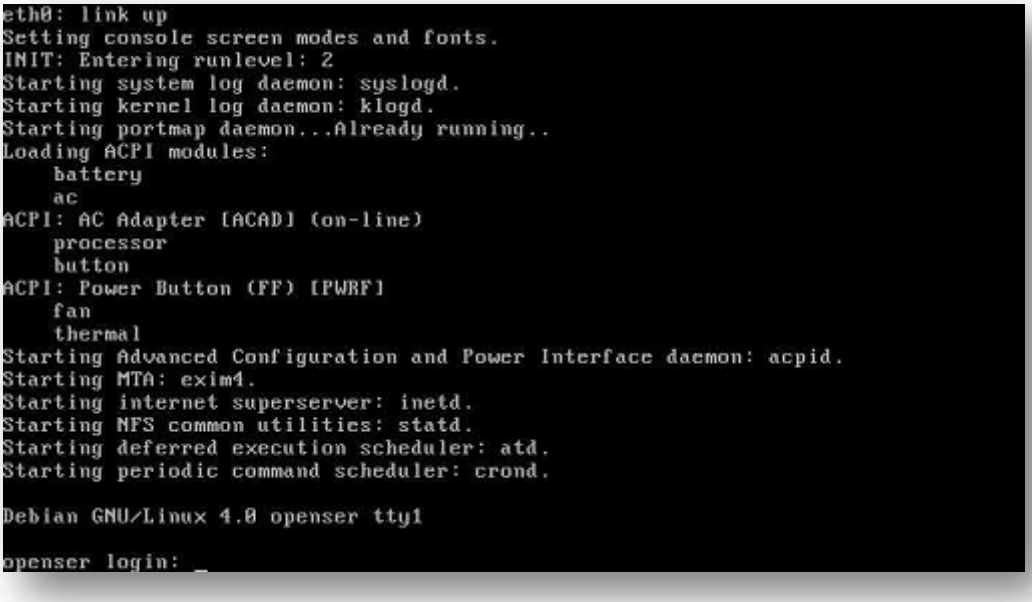



**Figura 109 – Ecrã do SO Debian em modo CLI (Command Line Interface).**

23. Importa salientar que, para usar o servidor em modo remoto deverá ser instalado o pacote ssh, executando o seguinte comando:

    - ***"apt-get install ssh".***

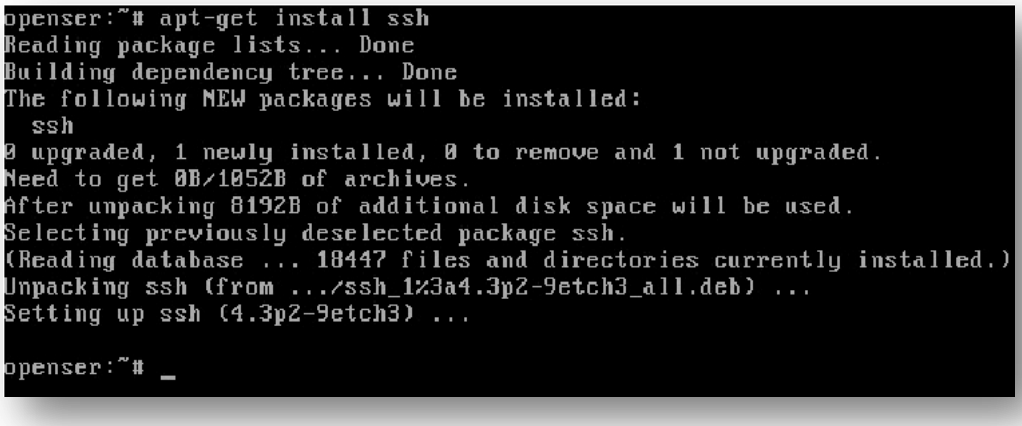



**Figura 110 – Instalação do pacote SSH.**

24. Por último, deverá ser configurado um IP fixo (estático) no referido servidor, de modo a facilitar o seu acesso remoto, bem como para facilitação de posteriores configurações. Para efectuar a configuração de um IP fixo basta editar o ficheiro interfaces que se encontra em ***/etc/network/*** com o editor preferido (vi, nano, etc.), executando o seguinte comando:

    - ***nano /etc/network/interfaces***

Em seguida, deverá ser alterado o ficheiro para os seguintes valores:

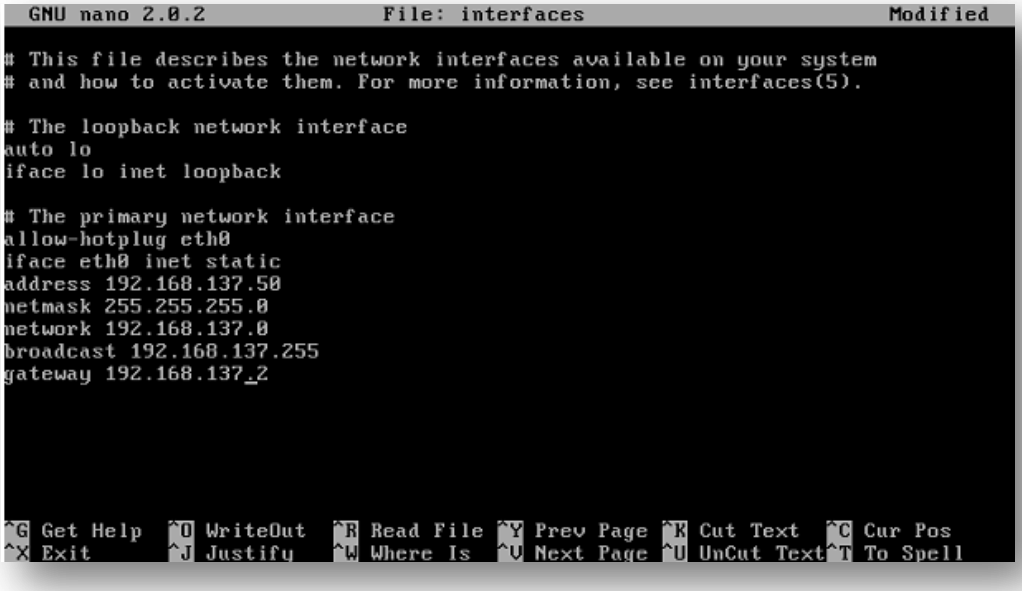



**Figura 111 – Instalação do pacote SSH.**

**NOTA:** É de referir que, o valor do endereço IP está relacionado com a rede a ser utilizada e deverá ser escolhido em conformidade com a mesma.

Terminando o processo de instalação do Debian, deverá sempre ser em conta os seguintes aspectos:

1. Reinialização do sistema: Para reiniciar as configurações da placa de rede deverá ser efectuado um reboot à máquina.
2. Actualização os pacotes do SO: Deverá ser efectuado uma actualização de novos pacotes que visam a optimizar o funcionamento do referido sistema operativo executando o seguinte comando:
    - ***apt-get install build-essential***.
3. Análise e Monitorização dos pacotes: Caso for necessário, o administrador do sistema, poderá sempre efectuar uma análise aos pacotes que entram e saem do sistema, sendo que deverá ser instalado a ferramenta *ngrep*, executando o seguinte comando:
    - ***apt-get install ngrep***

## *10.2 Instalação da aplicação OpenSer*

Neste ponto, será feita uma breve descrição sobre a instalação da aplicação *OpenSer*. Para efectuar a instalação da referida aplicação deverão ser executados os seguintes passos:

1. Instalar os pacotes necessários à compilação do *Openser*;
2. Descarregar ficheiro de instalação do *OpenSer* VX.X.X.
3. Instalar o módulo de autenticação com base de dados *MySQL* para garantir persistência de dados.

### *10.2.1 Instalação dos pacotes para compilar o OpenSer*

Para efectuar a instalação dos pacotes necessários para a compilação da referida aplicação, deverão ser executados os seguintes passos:

1. Instalar alguns pacotes cujo *OpenSer* depende para funcionar correctamente, usando a ferramenta de instalação ***apt-get***. Os pacotes necessários a instalar são:
    - ***gcc***
    - ***bison***
    - ***flex***
    - ***make***
    - ***openssl***
    - ***libmysqlclient-dev***
    - ***libradiusclient-ng2***
    - ***libradiusclient-ng-dev***
    - ***mysql-server***
2. Para os instalar basta escrever na linha de comandos:
    - ***"apt-get install gcc bison flex make openssl libmysqlclient-dev libradiusclient-ng2 libradiusclient-ng-dev mysql-server"***

### *10.2.2 Download do ficheiro de instalação do OpenSer VX.X.X*

Para efectuar o *download* dos pacotes necessários para a instalação da versão mais recente do *OpenSer*, deverão ser executados os seguintes passos:

1. Efectuar o *download* da última versão do *OpenSER*, será necessário aceder ao repositório da *Kamailio* para descarregar os ficheiros de código (*source*), executando os seguintes comandos:

   - ***cd /usr/src***
   - ***wget http://www.kamailio.org/pub/kamailio/3.3.3/src/openser-1.3.3-tls_src.tar.gz***
   - ***tar -xzvf openser-1.3.3-tls_src.tar.gz***

2. Seguidamente, será criada uma pasta com o nome ***openser-1.3.3-tls***.

3. A seguir, editar o ficheiro *Makefile* com o editor preferido (nano, vi, etc.), executando os seguintes comandos:

   - ***cd /usr/src/openser-1.3.3-tls***
   - ***nano Makefile***

   **NOTA:** Importa salientar que, na secção do ficheiro onde está contido os módulos ***"exclude_modules?="***, deverá ser retirado todos os módulos que se pretende ver instalados. Isto é, devem ser retirados da listagem os seguintes módulos:

   - ***mysql***
   - ***avp_radius***
   - ***auth_radius***
   - ***group_radius***
   - ***uri_radius***

4. Compilar o ficheiro *Makefile* com o editor preferido (nano, vi, etc.), executando os seguintes comandos:

   - ***make prefix=/ all***
   - ***make prefix=/ install***

   **NOTA:** É de salientar que, a respectiva compilação poderá demorar alguns minutos.

5. Criar uma pasta com o nome ***openser*** em ***/var/run***, executando o seguinte comando:

   - ***mkdir /var/run/openser***

6. Seguidamente, para colocar o openser a correr no arranque do Linux deverão ser executados os seguintes comandos:

   - ***cd /usr/src/openser-1.3.3-tls/packaging/debian***

- ***cp openser.default /etc/default/openser***
- ***cp openser.init /etc/init.d/openser***
- ***update-rc.d openser defaults 99***

7. A seguir, editar o ficheiro de configuração do *OpenSer*, nomeadamente em ***/etc/openser/openser.cfg*** e remover a linha ***fork=no***, mesmo que esta se encontre em modo comentário.
8. Dar permissões de execução ao ficheiro openser que se encontra em ***/etc/init.d/***.

    - ***cd /etc/init.d***
    - ***chmod 755 openser***

9. Editar o ficheiro ***/etc/default/openser*** e alterar os seguintes parâmetros:

    - ***nano /etc/default/openser***
    - ***RUN_OPENSER=no*** para ***RUN_OPENSER=yes***
    - ***MEMORY=64*** para ***MEMORY=128***

10. Editar o ficheiro ***/etc/init.d/openser*** e alterar os seguintes parâmetros:

    - ***RUN_OPENSER=no*** para ***RUN_OPENSER=yes***
    - ***DAEMON=/usr/sbin/openser*** para ***DAEMON=/sbin/openser***

11. Antes de ser reinicializado o sistema, deverá ser verificado se existe o utilizador ***openser***, que foi previamente criado no sistema e no grupo. Caso for necessário criar o grupo e utilizador, deveraão ser executados os seguintes passos:

    - ***addgroup --system openser***
    - ***adduser –system openser –ingroup openser***

12. Por fim, reiniciar o sistema operativo e verificar se o openser arrancou, executando o seguinte passo.

    - ***ps –ef | grep openser***

    **NOTA:** Importa salientar que, caso existirem processos com ***openser***, significa que o processo de instalação foi executado com sucesso.

### *10.2.3 Instalação do módulo MySQL no OpenSer*

Para efectuar a instalação do módulo *mysql* no *openser*, deverão ser executados os seguintes passos:

1. Editar o ficheiro ***/etc/openser/openserctlrc*** e retirar os comentários a alguns parâmetros.
2. Criar a base de dados, executando o seguinte comando:
   - ***openserdbctl create***

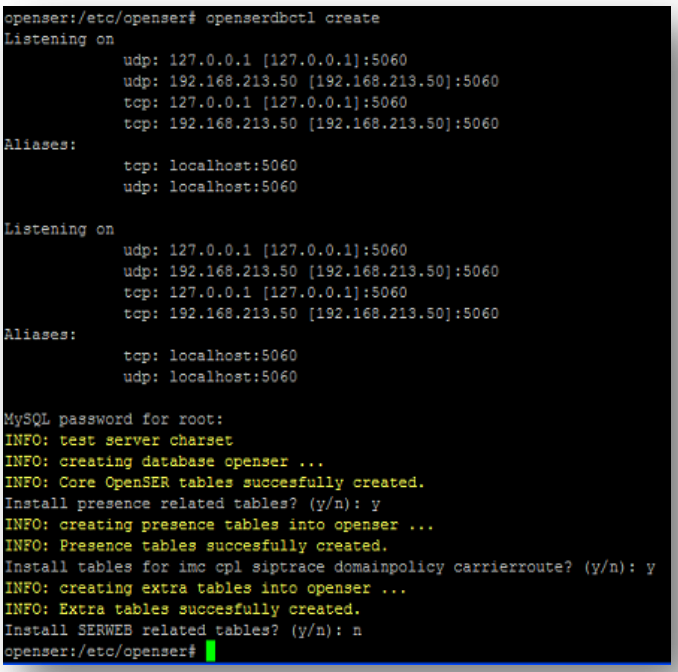



**Figura 112 – Criação da Base de Dados MySQL no OpenSer.**

3. Seguidamente, caso for solicitada a introdução de uma *password* de *root*, deverá apenas pressionar a tecla ***"Enter"***, de modo a criar uma base de dados sem password.
4. De seguida, surgirão algumas questões relacionadas com a criação de outras tabelas.

   **NOTA:** É de referir que, não deverão ser instaladas as tabelas relacionadas com ***SERWEB***, visto que, esta aplicação não se encontra em desenvolvimento. Assim sendo, não serão instaladas quaisquer tabelas para o efeito na base de dados. O *SERWEB* é uma aplicação que permite, ao administrador do sistema gerir o *OpenSER* através de um portal *Web*.

   Após a execução deste passo, o processo de instalação do módulo *mysql* no openser está finalizado. Importa salientar que, para tirar partido das funcionalidades da base de dados é necessário que a configuração do ficheiro ***openser.cfg*** faça uso desses módulos.

## *10.3 Instalação do Mediaproxy*

Neste ponto, será feita uma breve descrição sobre a instalação do *Mediaproxy*, de modo a facilitar ao gestor e/ou administrador do portal, uma melhor gestão de toda a informação disponível no respectivo site para garantir um melhor funcionamento do portal.

Para efectuar a instalação da referida aplicação deverão ser executados os seguintes passos:

1. Efectuar o *download* da última versão pretendida, executando os seguintes comandos:
   - ***cd /usr/local***
   - ***wget http://download.ag-projects.com/MediaProxy/old/ mediaproxy-1.9.1.tar.gz***
2. Descompactar o respectivo ficheiro executando o seguinte comando:
   - ***tar –xzvf mediaproxy-1.9.1.tar.gz***
3. Criar uma pasta com o nome ***mediaproxy***, executando o seguinte comando:
   - ***cd /usr/local/mediaproxy***
4. Efectuar uma cópia do ficheiro ***mediaproxy.ini.sample*** e em seguida, alterar o seu nome para ***mediaproxy.ini,*** através do seguinte comando:
   - ***cp mediaproxy.ini.sample mediaproxy.ini***
5. Editar o ficheiro ***mediaproxy.ini*** para os valores adaptados ao sistema em uso.
   - ***nano mediaproxy.ini***
6. Configurar o ficheiro de script para arrancar o mediaproxy no inicio do arranque do sistema.
   - ***cp /usr/local/mediaproxy/boot/mediaproxy.debian /etc/init.d/mediaproxy update-rc.d mediaproxy defaults 20 90***

**NOTA:** É de referir que, o *Mediaproxy* sofreu uma evolução a elaboração deste trabalho, sendo que a montagem do protótipo foi baseada na versão 1.9.1. Actualmente, foi lançada última versão a 2.4.3, baseada nos dois novos servidores *SIP*

*Proxy* existentes *Kamailio* e o *OpenSips*. Esta nova versão tem como principal vantagem um aumento substancial na capacidade de lidar com um maior número de chamadas simultâneas. É de salientar que, existem algumas imcompatibilidades entre a versão 2.4.3 e o *OpenSER*, razão pela qual deverá ser executados os passos da instalação da versão 1.9.1.

O *Mediaproxy* contem algumas ferramentas que permite efectuar um teste e verificar o estado do ***dispatcher***. A secção, ***Sessions.py*** indica quais as sessões RTP que estão em curso e dentro da pasta ***utils*** existem geradores de tráfego RTP que poderão também ser usados para testes.

Importa salientar que, para que o *OpenSER* tire partido do *mediaproxy*, este deverá ser carregado como módulo no ficheiro de configuração do ***OpenSER – openser.cfg***.

## *10.4 Instalação da aplicação SerMyAdmin*

Neste ponto, será feita uma breve descrição sobre a instalação da aplicação *SerMyAdmin*. Para efectuar a instalação da referida aplicação deverão ser executados os seguintes passos:

1. Actualizar a lista de repositórios. Introdução de novos repositórios.
   - ***nano /etc/apt/sources.list***
2. Editar o respectivo ficheiro e introduzir as seguintes linhas:
   - ***deb http://ftp.pt.debian.org/debian/ etch main contrib non-free***
   - ***deb-src http://ftp.pt.debian.org/debian etch main contrib non-free***
   - ***deb http://security.debian.org/ etch/updates main contrib non-free***
   - ***deb-src http://security.debian.org/ etch/updates main contrib non-free***
3. Seguidamente, deverá ser actualizado a funcionalidade ***apt-get***, executando o seguinte comando:
   - ***apt-get update***
4. Instalar o JDK do Java, executando o seguinte comando:
   - ***apt-get install sun-javaX-jdk***
5. Em seguida, actualizar a configuração do Java
   - ***update-java-alternatives -s java-1.X.0-sun***
6. Caso seja necessário verificar da versão java usada, deverá ser executado o seguinte comando:

- ***java -version***

7. Descarregar o ficheiro de instalação do *Tomcat*.

   - ***cd /usr/local***
   - ***wget http://neacm.fe.up.pt/pub/apache/tomcat/tomcat-6/v6.0.18/bin/apache-tomcat-6.0.18.tar.gz***

   **NOTA:** De referir que, o endereço poderá ser modificando consoante a versão e o repositório usado, pelo que, será sempre aconselhável procurar o ficheiro a partir do site oficial no seguinte endereço: *http://tomcat.apache.org/* .

8. Descompactar o respectivo ficheiro de instalação, executando o seguinte passo:

   - ***tar –xzvf apache-tomcat-6.0.18.tar.gz***

9. Seguidamente, criar uma ligação para a pasta criada, sendo que será usada posteriormente no script de arranque automático.

   - ***ln –s apache-tomcat-6.0.18 tomcat6***

10. Colocar o *Tomcat* a arrancar aquando do arranque do sistema. Colocar um ficheiro com o script necessário em ***/etc/init.d/***.

    - ***cd /etc/init.d/***
    - ***nano tomcat6***

    Para efectuar a passagem do referido *script* deverá ser executados os seguintes passos:

    - ***chmod 755 /etc/init.d/tomcat6***
    - ***update-rc.d tomcat6 defaults 99***

11. Verificar se a instalação do *Tomcat* foi efectuada com sucesso, acedendo, através de um *browser*, o seguinte endereço electrónico: ***http://<ip_da_máquina>:8080***. Seguidamente, será ilustrado uma página que apresenta o *Tomcat* apresentando a seguinte mensagem: ***"If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!"***. Se for o caso, significa que o processo de instalação foi efectuado com sucesso.

12. Em seguida, instalar o driver de *MySQL* para o *Tomcat*, de modo a que a aplicação *SerMyAdmin* possa aceder à base de dados do *OpenSER*.

- ***cd /usr/src/***
- ***wget http://mysql.nfsi.pt/Downloads/Connector-J/mysql-connector-java-5.1.6.tar.gz*** (pesquisar por mysql-connector-java em www.mysql.com).
- ***tar –xzvf mysql mysql-connector-java-5.1.6.tar.gz***
- ***cd mysql-connector-java-5.1.6***
- ***cp /mysql-connector-java-5.1.6-bin.jar /usr/local/tomcat/lib/***

13. Instalar a aplicação *Exim4* – Agente de transferência de mensagens – que permite ao *SerMyAdmin* o envio de mensagens de correio electrónico aos utilizadores.

    **NOTA**: Esta aplicação necessita de uma grande quantidade de informação específica para a sua configuração. Deverá consultar a página da aplicação para obter mais informações (www.exim.org).

    - ***apt-get install exim4***
    - ***dpkg-reconfigure exim4-config***

14. A seguir deverá ser efectuada, uma declaração dos dados necessários para que o *SerMyAdmin* possa ligar-se à base de dados do *OpenSER*. Editar o ficheiro XML que se encontra em ***/usr/local/tomcat6/conf/context.xml***. O ficheiro deverá conter os seguintes elementos:

```
<?xml version="1.0" encoding="UTF-8"?>
<Context path="/serMyAdmin">
<Resource auth="Container" driverClassName="com.mysql.jdbc.Driver"
maxActive="20" maxIdle="10" maxWait="-1" name="jdbc/openser_MySQL"
type="javax.sql.DataSource" url="jdbc:mysql://localhost:3306/openser"
username="sermyadmin" password="secret"/>
</Context>
```

    **NOTA:** É de referir que, o texto a negrito deverá ser adaptado consoante a configuração que foi anteriormente efectuada. Caso a base de dados esteja numa outra máquina (por motivos de escalabilidade e desempenho), deverá ser tido em conta que a instalação do *MySQL* do *Debian* só aceita pedidos efectuados no *localhost*, ou seja, pedidos provenientes da mesma máquina onde está alojada a BD, pelo que será necessário editar o ficheiro ***etc/mysql/my.cnf*** e alterar essas permissões de modo que os pedidos possam ser provenientes de outras máquinas.

15. Criar o utilizador (referido no ficheiro context.xml) no *MySQL* e atribuir-lhe as permissões necessárias à alteração da base de dados do *OpenSER*.

    - *mysql -u root –p mysql> grant all privileges on openser.* to **sermyadmin**@'%' identified by '**secret**';*
    - *mysql -u root –p mysql> grant all privileges on openser.* to **sermyadmin**@'localhost' identified by '**secret**';*

    **NOTA**: Os valores a negrito devem ser adaptados à configuração desejada e igual aos valores introduzidos no ficheiro ***context.xml*** do passo 13.

16. Instalar a aplicação ***SerMyAdmin.WAR***. Descarregar o ficheiro WAR e copiá-lo para a pasta ***webapps*** do *Tomcat*. Reiniciar o *Tomcat*. Para descarregar o ficheiro WAR deverá ir ao sítio sourceforge.net e pesquisar por sermyadmin – ali encontra o link para descarregar o ficheiro.

    - ***cp serMyAdmin-0.7.war/usr/local/tomcat6/webapps/serMyAdmin.war***
    - ***invoke-rc.d tomcat6 restart***

17. Aceder à página ***http://<ip_da_máquina>:8080/sermyadmin***. Desta forma, será efectuada uma alteração à base de dados do OpenSER. **NOTA:** Não deverá ser efectuado o login.

18. Editar o ficheiro ***/usr/local/tomcat6/webapps/serMyAdmin/WEB-INF/spring/resource.xml*** que contém os parâmetros do servidor de mail, executando o seguinte comando:

    - ***nano /usr/local/tomcat6/webapps/serMyAdmin/WEB-INF/spring/resource.xml***

```
<?xml version="1.0" encoding="UTF-8"?>
<beans
xmlns="http://www.springframework.org/schema/beans"xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xsi:schemaLocation="http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans-2.0.xsd">
<bean  id="mailSender"
class="org.springframework.mail.javamail.JavaMailSenderImpl">
<property name="host">
        <value>localhost</value>
</property>
</bean>
<!-- You can set default email bean properties here, eg:
from/to/subject -->
<bean  id="mailMessage
"class="org.springframework.mail.SimpleMailMessage">
<property name="from">
        <value>admin@labvoipua.com</value>
</property>
</bean>
```

**NOTA:** Importa salientar que, deverão ser alterados os valores (*tag value)* de host e de from, que estão assinalados a cor azul. Esses atributos indicam qual o servidor e qual o nome que deverá aparecer no remetente.

19. A seguir, criar um utilizador Administrador na base de dados e efectuar algumas alterações nos dados da base de dados, executando o seguinte comando:
    - ***mysql –u root openser < openser.sql***
20. Por último, dado ao facto que o processo de instalação já foi concluído, deverá introduzir os valores ***admin@setup*** e ***secret*** nos campos ***login*** e ***password.*** De referir que, estes valores são os que foram introduzidos aquando da criação do utilizador administrador e que poderão ser alterados caso for necessário.

    **NOTA:** Importa salientar que, todas estas aplicações sofrem constantes actualizações, pelo que será sempre aconselhável consultar a página oficial da referida aplicação, nomeadamente, em *http://www.sermyadmin.org/*.

### *10.5 Instalação do sistema IP PBX – Asterisk*

Neste ponto, será feita uma breve descrição sobre a instalação do sistema IP PBX - *Asterisk*. Para efectuar a instalação da referida aplicação deverão ser executados os seguintes passos:

1. Actualizar a lista de pacotes da distribuição *Debian*, utilizando o seguinte comando:
    - ***apt-get update***
2. Actualizar os pacotes instalados
    - ***apt-get –y upgrade***
3. Efectuar um reboot ao sistema
    - ***reboot***
4. Instalar os pacotes necessários à instalação do Asterisk
    - ***apt-get -y install build-essential libncurses5-dev libcurl3-dev libvorbis-dev libspeex-dev unixodbc unixodbc-dev libiksemel-dev linux-headers-`uname -r`***
5. Ir para a pasta /usr/src

- ***cd /usr/src***

6. Efectuar o *download* da última versão do Asterisk.

   - ***wget http://downloads.digium.com/pub/asterisk/asterisk-1.4-current.tar.gz***

7. Efectuar o *download* da última versão dos drivers da *Zaptel*

   - ***wget http://downloads.digium.com/pub/zaptel/zaptel-1.4-current.tar.gz***

8. Descompactar os ficheiros descarregados em pastas.

   - ***tar xvzf asterisk-1.4-current.tar.gz && tar xvzf zaptel-1.4-current.tar.gz***

9. Mudar para a pasta Zaptel-1.4.x

   - ***cd zaptel-1.4.x (NOTA: o x deverá ser substituído pelo valor correspondente da versão descarregada)***

10. Compilar e construir os drivers *Zaptel*

    - ***./configure && make && make install***

11. Activar o módulo *ztdummy* (presente no *kernel* e que será usado como fonte de temporização para o *asterisk*)

    - ***modprobe ztdummy***

12. Mover para a pasta de instalação do Asterisk

    - ***cd /usr/src/asterisk-1.4.x***

13. Alterar a estrutura ast_*vm*_user do ficheiro /apps/app_voicemail.c para corresponder ao usado no *Openser – uniqueid*.

```
/* Structure for linked list of users */
struct ast_vm_user {
	char context[AST_MAX_CONTEXT];  /* Voicemail context */
	char mailbox[AST_MAX_EXTENSION];/* Mailbox id, unique within vm context
	char password[80];            /* Secret pin code, numbers only */
	char fullname[80];            /* Full name, for directory app */
	char email[80];               /* E-mail address */
	char pager[80];               /* E-mail address to pager (no attachme
	char serveremail[80];         /* From: Mail address */
	char mailcmd[160];            /* Configurable mail command */
	char language[MAX_LANGUAGE];    /* Config: Language setting */
	char zonetag[80];             /* Time zone */
	char callback[80];
	char dialout[80];
	char uniqueid[64];            /* Unique integer identifier */
	char exit[80];
	unsigned int flags;           /* VM_ flags */
	int saydurationm;
	int maxmsg;                   /* Maximum number of msgs per folder fo
	struct ast_vm_user *next;
};
```

14. Construir e instalar o Asterisk.
    - ***./configure && make && make install***
15. Verificar a versão do Asterisk
    - ***asterisk –V***
16. Instalar scripts de arranque no inicio do SO.
    - ***make config***
    - ***echo "ztdummy" >> /etc/modules (para que o módulo ztdummy seja iniciado sempre que o sistema operativo for reiniciado)***
17. Instalação do driver UnixODBC MySQL
    - ***apt-get install libmyodbc***
18. Alterar tabela subscriber do Openser (para receber o PIN a ser usado no voicemail)
    - ***mysql –u root –p***
    - ***(introduzir password)***
    - ***ALTER TABLE subscriber ADD vmail_password varchar(32);***
19. Criar BD do Asterisk e respectivas tabelas (duas tabelas não serão mais do que simples VIEWS das tabelas originais do OpenSer)

```
create database asterisk;

use asterisk;

CREATE TABLE `voicemessages` (
  `id` int(11) NOT NULL auto_increment,
  `msgnum` int(11) NOT NULL default '0',
`dir` varchar(80) default '',
  `context` varchar(80) default '',
  `macrocontext` varchar(80) default '',
  `callerid` varchar(40) default '',
  `origtime` varchar(40) default '',
  `duration` varchar(20) default '',
  `mailboxuser` varchar(80) default '',
  `mailboxcontext` varchar(80) default '',
  `recording` longblob,
  PRIMARY KEY  (`id`),
  KEY `dir` (`dir`)
) ENGINE=InnoDB;

CREATE VIEW vmusers AS
SELECT id as uniqueid,
  username as customer_id,
  'default' as context,
  username as mailbox,
  vmail_password as password,
  CONCAT(first_name,' ',last_name) as fullname,
  email_address as email,
  NULL as pager,
  datetime_created as stamp
FROM openser.subscriber;
```

```
CREATE VIEW sipusers AS
SELECT username as name,
  username,
  'friend' as type,
  NULL as secret,
  domain as host,
  CONCAT(rpid, ' ','<',username,'>') as callerid,
  'default' as context,
  username as mailbox,
  'yes' as nat,
  'no' as qualify,
  username as fromuser,
  NULL as authuser,
  domain as fromdomain,
  NULL as insecure,
  'no' as canreinvite,
  NULL as disallow,
  NULL as allow,
  NULL as restrictcid,
  domain as defaultip,
  domain as ipaddr,
  '5060' as port,
  NULL as regseconds
FROM openser.subscriber;
```

20. Criar um utilizador do *Mysql* com permissões na BD asterisk.

    - ***GRANT ALL ON asterisk.* to asterisk@localhost IDENTIFIED BY 'password';***

21. Configurar o *UnixODBC*. Acrescentar ao ficheiro */usr/local/etc/odbcinst.ini* o seguinte:

```
 [MySQL]
Description = MySQL driver
Driver = /usr/lib/odbc/libmyodbc.so
Setup = /usr/lib/odbc/libodbcmyS.so
CPTimeout =
CPReuse =
UsageCount = 1
```

Acrescentar ao ficheiro */usr/local/etc/odbcinst.ini* o seguinte:

```
[MySQL-asterisk]
Description = MySQL Asterisk database
Trace = Off
TraceFile = stderr
Driver = MySQL
SERVER = localhost
USER = asterisk
PASSWORD = some_password
PORT = 3306
DATABASE = asterisk
```

22. Configurar o Asterisk.

    Acrescentar ao ficheiro */etc/asterisk/res_odbc.conf* o seguinte:

```
[[asterisk]
enabled => yes
dsn => MySQL-asterisk
username => asterisk
password => asterisk
pre-connect => yes
```

23. Acrescentar ao ficheiro ***/etc/asterisk/extconfig.conf*** o seguinte:

    - ***sipusers => odbc,asterisk,sipusers***
    - ***sippeers => odbc,asterisk,sipusers***
    - ***voicemail => odbc,asterisk,vmusers***

24. Configurar o ficheiro ***extensions.conf.*** Adicionar:

    - ***[default]***
    - ***exten =>_9.,1,Dial(ZAP/g1/${EXTEN})***
    - ***exten =>_9.,2,hangup()***
    - ***exten =>_u.,1,Voicemail(u${EXTEN})***
    - ***exten =>_u.,2,hangup()***
    - ***exten =>_b.,1,Voicemail(b${EXTEN})***
    - ***exten =>_b.,2,hangup()***

    **NOTA:** O que esta configuração faz é reconhecer qual o primeiro carácter do contacto – '9', 'u' ou 'b'. Em função desse carácter efectua três funções diferentes – '9': estabelece ligação para PSTN;

    **'u':** envia para o *Voicemail* indicando que a chamada não foi atendida; **'b'** envia a chamada para o *Voicemail* indicando que o destinatário se encontra ocupado (*busy*).

### *10.5.1 Instalação da interface WEB do Asterisk – a Asterisk-GUI*

O sistema de IP PBX – Asterisk, possui uma interface de configuração via *Web* bastante intuitiva e funcional, permitindo ao administrador ou gestor da rede uma melhor gestão do sistema.

Para efectuar a instalação da referida aplicação deverão ser executados os seguintes passos:

1. Instalar o pacote ***subversion*** executando o seguinte comando:

    - ***apt-get install subversion***

2. Ir para a pasta ***/usr/src***

   - ***cd /usr/src***

3. Descarregar a ultima versão do *Asterisk-GUI*

   - ***svn co http://svn.digium.com/svn/asterisk-gui/branches/2.0 asterisk-gui***

4. Ir para a pasta /usr/src/asterisk-gui

   - ***cd asterisk-gui***

5. Compilar e construir a Asterisk-GUI

   - ***sh configure && make && make install***

6. Verificar se a instalação foi correctamente efectuada

   - ***make checkconfig***

   **NOTA:** Caso surgirem algumas mensagens de erros, basta efectuar as correcções que são propostas.

   Depois da configuração estará disponível a página *Web* em:

   *http://<ip_da_máquina:8088>/asterisk/static/config/cfgbasic.html*.

   Agora a configuração do Asterisk torna-se bastante mais fácil e intuitiva.

## *10.6 Instalação de FreeRadius e CDRTool*

Neste ponto, será feita uma breve descrição sobre a instalação das aplicações *FreeRadius* e *CDRTool*. A instalação das aplicações *FreeRadius* e *CDRTool* é efectuada em simultâneo. Relembra-se neste ponto que muitas das configurações apresentadas necessitam de ser adaptadas a cada caso, sobretudo se forem utilizadas mais do que uma máquina para a implementação do protótipo (i.e. uma máquina para servidor de base de dados, outra para Radius, etc.).

### *10.6.1 Instalação de CDRTool*

Para efectuar a instalação da referida aplicação deverão ser executados os seguintes passos:

1. Descarregar o ficheiro de instalação.

   - ***cd /usr/src***
   - ***wget http://download.ag-projects.com/CDRTool/cdrtool_6.6.10.all.deb***

2. Instalar pacotes dependentes necessários para o *CDRTool*

- ***apt-get update***
- ***apt-get install apache2 libapache2-mod-php5 php5 php5-cli php5-mysql php5-curl php-pear php-soap mrtg smarty***

**NOTA:** Num determinado ponto da instalação será pedido, num ecrã azul, para responder se deseja que a ferramenta mrtg só seja utilizada pelo utilizador especifico *Mrtg*. Responda *Yes*)

3. Instalar o pacote ***cdrtool_6.x.all.deb***

   - ***dpkg –i cdrtool_6.6.10.all.deb***

4. Mudar para a pasta ***/var/www/CDRTool***

   - ***cd /var/www/CDRTool***

5. Criação da base de dados para *CDRTool*. Para efectuar este passo deverá ter permissões de *root* para criar/alterar bases de dados no *mysql*. Alterar os dados referentes às *password* a usar no acesso à base de dados do CDRTool, no ficheiro ***/var/www/CDRTool/setup/mysql/create_users.mysql***

   - ***nano /var/www/CDRTool/setup/mysql/create_users.mysql***
   - ***Substituir PASSWORD pela password desejada.***

6. Correr o script para criação da base de dados. Executar o ***ficheiro setup_mysql.sh***.

   - ***/var/www/CDRTool/setup/mysql/setup_mysql.sh <password> <máquina com mysql>***

   **NOTA:** Este script efectua as seguintes operações:

   - Adiciona um utilizador para a base de dados *cdrtool* presente no servidor *MySQL*;
   - Cria uma base de dados com o nome “cdrtool”
   - Cria um utilizador de administração da interface *Web* com o *login/password* igual a *admin/admin*;
   - Carrega para as tabelas da BD cdrtool os valores iniciais;

7. Criar ficheiro de configuração para ***cdrtool – global.inc***. Copiar o ficheiro de exemplo ***global.inc.simple.sample*** para a pasta ***/etc/cdrtool/***

   - ***cp /var/www/CDRTool/setup/global.inc.simple.sample /etc/cdrtool/global.inc***

Editar o ficheiro *global.inc* e configurar as variáveis em conformidade com o sistema usado.

**NOTA:** A configuração aqui apresentada é somente um exemplo que deverá ser adaptado a cada caso. Para cada elemento que disponibilize informação para a *CDRTool* (*openser, asterisk, mediaproxy*, etc.) deverá ser configurada uma nova entrada no ficheiro.

8. Activar o ***Rating Engine*** - usado para efectuar o cálculo dos custos de chamadas pré-pagas e/ou pós-pagas. Proporciona acesso às tabelas de preços e fica em memória (como *daemon*) para evitar o acesso às tabelas sempre que seja necessário efectuar um cálculo de pagamento. È possível alterar as tabelas de preços sem ter de reiniciar o *Rating Engine*.
9. Alterar os valores de IP e porto da máquina onde o ***Rating Engine*** vai receber os dados do *OpenSer* no ficheiro global.inc. Activar o funcionamento do *Rating Engine* em ***/etc/default/cdrtool***
    - ***nano /etc/default/cdrtool*** alterar para ***RUN_ratingEngine=yes***

### *10.6.2 Configuração do RADIUS*

Para efectuar a configuração da referida aplicação deverão ser executados os seguintes passos:

1. Instalar os pacotes *freeradius*
    - ***apt-get install freeradius freeradius-mysql***
2. Criar uma base de dados radius para o *freeradius*
    - ***mysqladmin –u root –p create radius***
3. Executar *script* de criação das tabelas necessárias na base de dados *radius*.
    - ***cp /usr/share/doc/freeradius/examples/mysql.sql.gz /usr/src***
    - ***cd /usr/src***
    - ***gunzip mysql.sql.gz***
    - ***mysql –u root –p radius < mysql.sql***
4. Aplicar o script necessário para alterar a tabela ***radacct*** de forma a receber atributos específicos do *OpenSer*.
    - ***/var/www/CDRTool/setup/radius/OpenSIPs/radacct-patch.sh***

5. Criar utilizador para a base de dados radius do *MySQL*. Criar um utilizador com o nome radius e atribuir privilégios de utilização (USAGE) da base de dados *radius* criada.

6. Configurar o freeradius para escrever a informação na tabela ***radacct***

   - ***cp /var/www/CDRTool/setup/radius/OpenSIPs/sql.conf /etc/freeradius/sql.conf***

   Editar os valores para a configuração usada pela máquina *mysql*

7. Adicionar os clientes *RADIUS* no ficheiro *clients.conf*.

   - ***nano /etc/freeradius/clients.conf***

8. Activar a contabilização através de *MySQL* para o *freeradius*

   - ***nano /etc/freeradius/radius.conf***

   Descomentar a palavra sql no parâmetro *accounting*

9. Copiar dictionary.ser para /etc/openser

   - ***cp /var/www/CDRTool/setup/radius/OpenSIPs/dictionary.ser /etc/openser***

   Descomentar a linha ***#INCLUDE /etc/radiusclient-ng/dictionary***

10. Reiniciar todo o sistema e testar a aplicação (através da interface *Web*)

    - ***reboot***

    Abrir um browser em ***http://<ip_da_máquina_cdrtool>/CDRTool***

    Deverá surgir um formulário de introdução de *login* e *password* introduzir *admin/admin*

    **NOTA:** Após conclusão da instalação base do *FreeRadius* + *CDRTool* para o *OpenSER*, será necessário relembrar que esta instalação não contempla o envio de informação por parte do *Mediaproxy* e do *Asterisk* directamente para o *freeradius*. Para implementar essa solução é necessário consultar toda a documentação presente no mediaproxy e em ***/var/www/CDRTool/setup/asterisk***. Importa salientar que, a instalação do *FreeRadius* e *CDRTool* é bastante complexa e adaptável a cada situação pretendida pelo que se aconselha à leitura do ficheiro de instalação ***INSTALL.txt*** bem como todos os documentos presentes em:

    - ***http://download.ag-projects.com/CDRTool/doc/.***

## 10.7 Instalação das aplicações de teste e monitorização

Neste ponto, será feita uma breve descrição sobre a instalação das aplicações de teste e monitorização da rede a ser implementada.

### 10.7.1 Instalação da aplicação WireShark

O *Wireshark* é um *software* bastante completo que permite ao administrador da rede capturar e análisar de tráfego de dados numa determinada rede. Esta aplicação utiliza o mesmo motor de captura da aplicação *tcpdump*, permitindo gravar os ficheiros gerados no mesmo formato. O *Wireshark* suporta dois tipos de filtros: filtros de captura, baseados no *tcpdump*; e filtros de amostragem, utilizados para controlar o que se está a observar. Este *software* possui uma interface gráfica simples e intuitiva, que permite o administrador e/ou gestor da rede, uma melhor interacção com a referida aplicação. Contudo, poderá ser também utilizado em ambiente *text-only*.

A tecnologia VoIP envolve uma série de protocolos que o *Wireshark* pode descodificar e relacionar. Como um exemplo prático, pode-se considerar o estabelecimento de uma chamada que envolve um protocolo diferente do utilizado para o tráfego de voz propriamente dito: SIP e RTP/RTCP, respectivamente.

O *Wireshark* permite utilizar a informação de sinalização referente ao estabelecimento de uma chamada para uma melhor compreensão e visualização do fluxo de voz. É de referir que, está aplicação permite actualizar a lista de pacotes capturados em tempo real de forma a verificar se o tráfego que está a ser gerado está de acordo com o esperado.

A seguir está descrito um manual de instalação e utilização da referida aplicação nos sistemas operativos Windwos e Linux.

#### 10.7.1.1 Windows

Para ser efectuado a instalação do *Wireshark* no SO Windows devem ser executados os seguintes passos:

1. Efectuar o *download* da aplicação no site oficial: *http://www.wireshark.org/download.html*
2. Instalar o Wireshark, efectuando um duplo click no ficheiro executável.
3. No menu "***Iniciar***", seleccionar a opção **"*Programas*",** e em seguida seleccionar **"*Wireshark*".**

4. Seguidamente será despoletado o ambiente de trabalho da referida aplicação, conforme ilustra a seguinte figura:

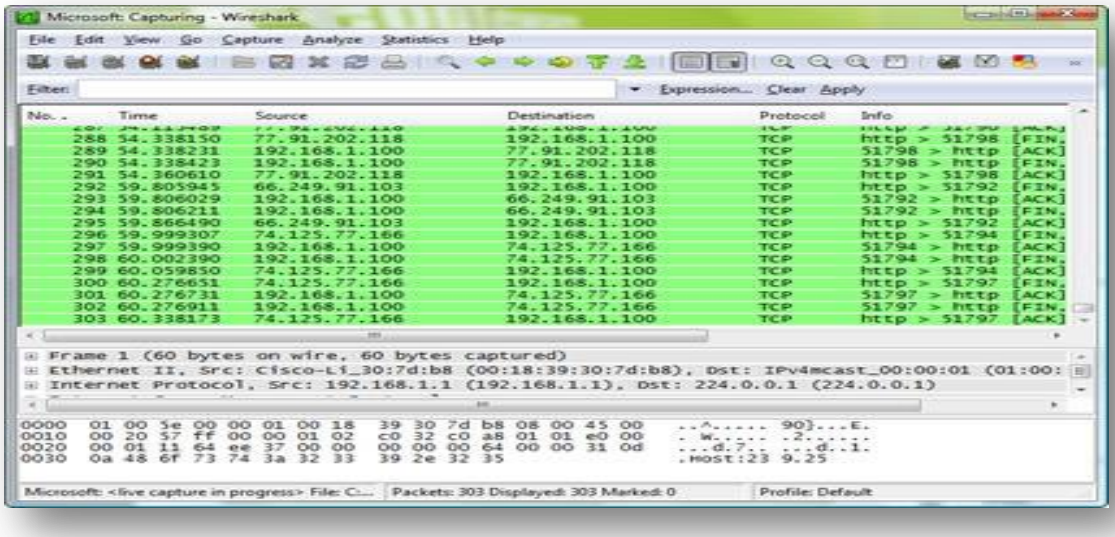



**Figura 113 – Exemplo do Menu principal do WireShark (Windows).**

5. Para começar a capturar e analizar o tráfego dos pacotes que circulam numa determinada rede, será necessário escolher qual a interface de rede que vai estar à escuta de pacotes. Para efectuar a definição das interfaces pretendidas, ir ao menu ***"Capture"*** e em seguida escolher a opção ***"Interfaces"*** (observar a seguinte figura).

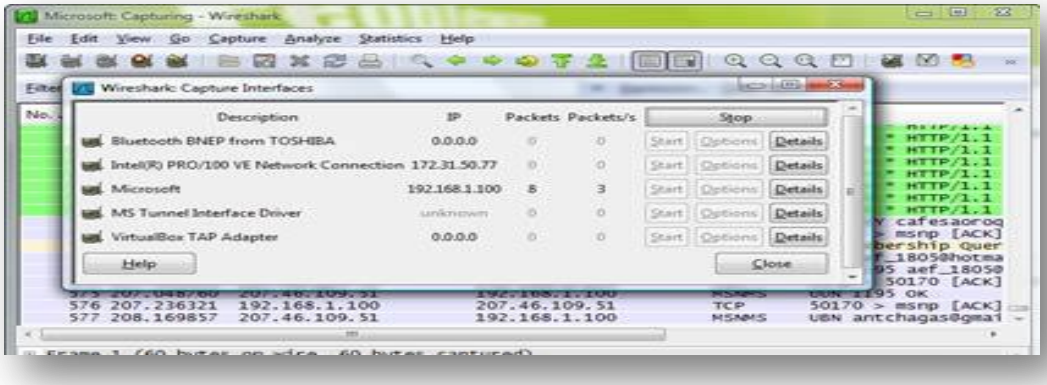



**Figura 114 – Exemplo de uma captura de pacotes no WireShark.**

**NOTA:** Importa salientar que, poderão existir algumas placas wireless que não funcionarão em modo promíscuo. Desta forma basta ir às opções dessa interface e tirar o vista da *checkbox* que diz: "***Capture packets in promiscuous mode"***.

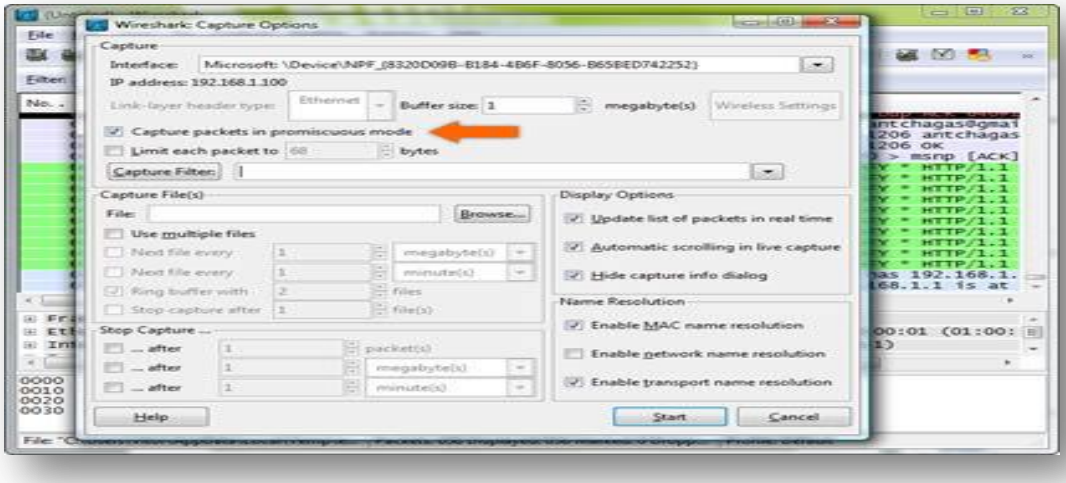



**Figura 115 – Exemplo de uma captura de pacotes sem o modo promíscuo.**

6. Para começar o processo de *sniffing*, deverá ser seleccionado a opção ***"start"*** na interface pretendida, de modo que se possa ser visualizado os pacotes a serem capturados.

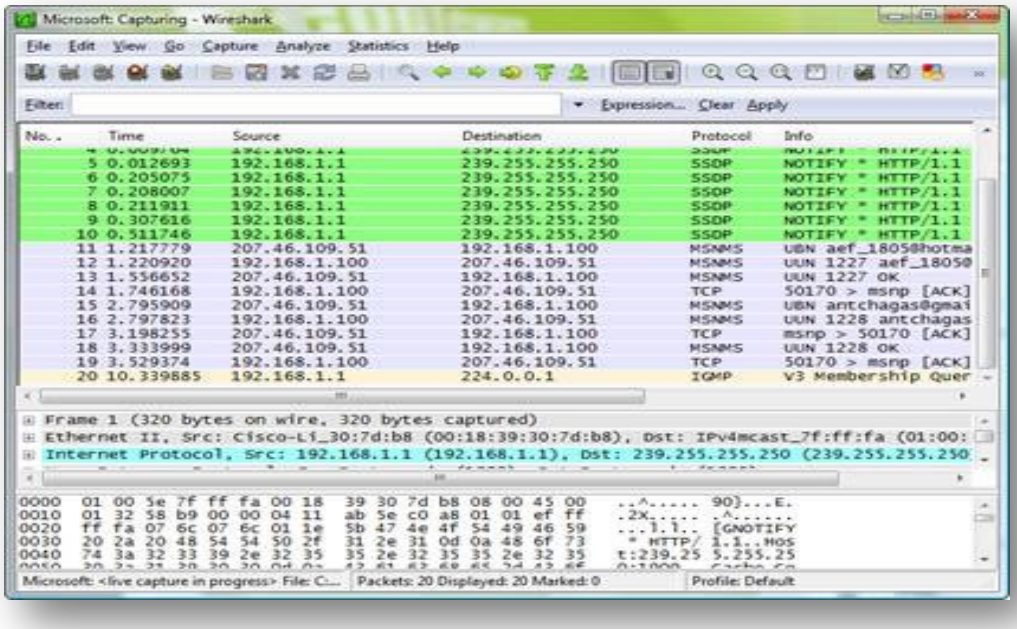



**Figura 116 – Exemplo de uma captura de pacotes com o processo sniffing.**

### *10.7.1.2 Linux*

Para ser efectuado a instalação do *Wireshark* no SO Linux devem ser executados os seguintes passos:

1. Para instalar o *Wireshark*, ir num terminal, entrar em modo de privilégios de root:

- Se for no Ubuntu: digitalizar o comando: ***"sudo apt-get -y install wireshark wireshark-common wireshark-dev".***
- Se for no Debian (a partir do repósitório): digitalizar o comando: ***" aptitude install wireshark"***

**NOTA:** Poderá ainda ser, utilizado um processo mais simples de instalação de todos os componentes necessários para a compilação, usando o comando ***"auto-apt"***, disponível através da função ***"apt-get"***. Para usá-lo, instale o pacote via apt-get e rode o comando "auto-apt update":

- ***apt-get install auto-apt***
- ***auto-apt update***

Após a execução dos passos anteriores, deverão ser executados os seguintes comandos de compilação:

- ***tar -zxvf tar zxvf wireshark-1.4-tar.gz***
- ***cd wireshark-1.4-tar.gz***
- ***auto-apt run ./configure***
- ***auto-apt run make***
- ***su <senha>***
- ***make install***

2. Depois da instalação poderá abrir o *Wireshark*, ir ao menu ***"Aplicações"***, seleccionar a opção **"*Internet"*,** e em seguida seleccionar **"*Wireshark"*.**
3. Seguidamente será despoletado o ambiente de trabalho da referida aplicação, conforme ilustra a seguinte figura:

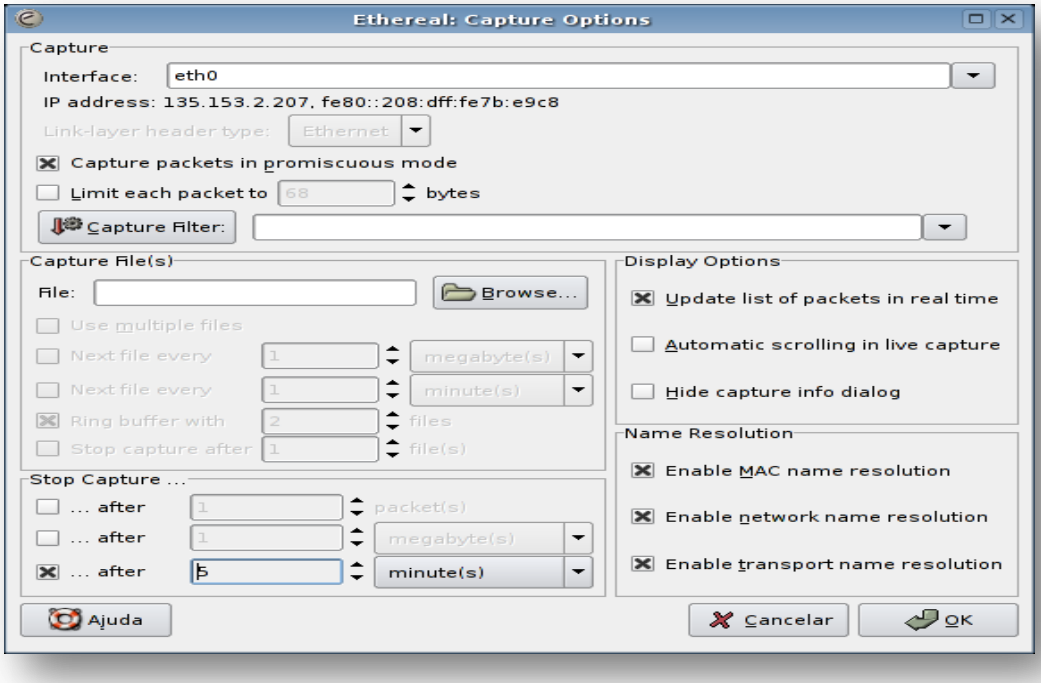



**Figura 117 – Exemplo do Menu principal do WireShark (Linux).**

**NOTA:** Importa salientar que, poderá existir algumas placas wireless que não funcionarão em modo promíscuo. Desta forma basta ir às opções dessa interface e tirar o vista da *checkbox* que diz: "***Capture packets in promiscuous mode"***.

### *10.7.2 Instalação da aplicação o tcpdump*

O *Tcpdump* é uma ferramenta que permite efectuar captura e análise de pacotes numa determinada rede. Esta fornece estatísticas sumárias e reporta o número de pacotes perdidos. Após capturar tráfego, é possível redireccionar este para um ficheiro e analisar posteriormente noutras ferramentas de análise como por exemplo o *wireshark* e o *tcptrace*.

O *Tcpdump* é uma ferramenta de *software* geralmente utilizada em computadores com ambiente *text-only* ou em computadores remotos.

Para ser efectuado a instalação do tcpdump devem ser executados os seguintes passos:

1. Para instalar o *tcpdump*, no terminal, entrar em modo de privilégios de *root*:
   - ***apt-get install tcpdump***
2. Para iniciar a utilização do *tcpdump*, será necessário de especificar a interface de rede a que se pretende ser analizada, introduzindo o parâmetro -i seguido da interface desejada. Por exemplo, se quisermos analisar todo o

tráfego que passa pela interface eth0, executaríamos a seguinte linha de comando:

- ***tcpdump -i eth0***

**NOTA:** De referir que a aplicação *tcpdump* possui uma serie de funcionalidades que poderão ajudar o gestor da rede a ter uma melhor gestão e análise de toda as informações sobre a sua rede.

A seguir estão apresentados alguns exemplos dessas funcionalidades:

a) "src host": Com esta funcionalidade poderá ser analizada o tráfego que vem de um computador com um endereço IP 192.168.0.9, para um outro computador, com o endereço IP 192.168.0.2. A linha de comando ficaria da seguinte forma:

- ***tcpdump -i eth0 src host 192.168.0.9***

b) "dst host": este parâmetro pemite monitorar as conexões especificando um host de destino.

- ***tcpdump -i eth0 dst host 192.168.0.1***

**NOTA:** No exemplo anterior foi considerado que está sendo analizado todo o tráfego do src host 192.168.0.2 para o dst hot 192.168.0.1, sendo que o este é nosso *gateway*.

c) "not host": Com tcpdump também podemos especificar exceções com o parâmetro not host. Por exemplo, caso num servidor queremos analisar todo o tráfego que se passa em sua interface, excepto o de 192.168.0.8, faríamos da seguinte forma:

- ***tcpdump -i eth0 not host 192.168.0.9***

d) "src port" e "dst port": No tcpdump podemos também especificar portas de origem e destino com os comandos src port e dst port. Caso for necessário analisar o tráfego da rede de um destinatário, no porto 80 (http), deverá ser executado o seguinte comando:

- ***tcpdump -i eth0 dst port 80***

Para verificarmos o tráfego da porta de origem 32881 por exemplo, faríamos da seguinte forma:

- ***tcpdump -i eth0 src port 32881***

e) "log": Esta funcionalidade permite filtrar e criar um log usando o tcpdump:

- ***tcpdump -v -i eth0 src host 192.168.xx..xxx | grep palavra_chave > /home/nome.txt***

### *10.7.3 Instalação da aplicação PuTTY*

*PuTTY* é uma implementação livre de *Telnet* e *SSH* para plataformas *Win32*, juntamente com um emulador de terminal *XTerm*.

Esta aplicação permite ao administrador ou gestor de uma determinada rede, aceder a servidores remotos, quer usando o protocolo telnet e/ou ssh. Com esta ferramenta podemos por exemplo aceder a um servidor, normalmente um servidor Linux, de forma segura e rápida.

Para ser efectuado a instalação do *PuTTY* devem ser executados os seguintes passos:

1. Efectuar o *download* da aplicação no site oficial: *http://www.putty.org*
2. Instalar o *PuTTY*, efectuando um duplo click no ficheiro executável.
3. No menu "***Iniciar***", seleccionar a opção **"*Programas*"**, e em seguida seleccionar **"*PuTTY*".**
4. Seguidamente será despoletado o ambiente de trabalho da referida aplicação, conforme ilustra a seguinte figura:

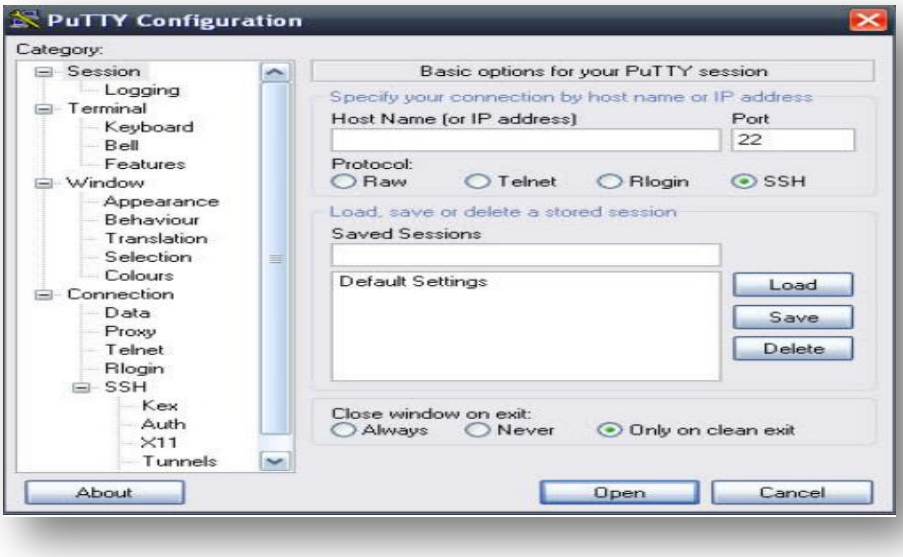



**Figura 118 – Exemplo do Menu principal do PuTTY.**

**NOTA:** É de notar que, no menu principal existe uma secção à esquerda que possui um conjunto de categorias que poderão permitir efectuar uma configuração mais avançada consoante a necessidade do utilizador. No lado direito do menu principal, pode-se observar a sessão que corresponde aos parâmetros de configuração de cada item seleccionado. Poderá ser configurado, vários protocolos tais como, o SSH, o Raw e o próprio Telnet para estabelecer a comunicação remota entre vários terminais. Para mais informações consultar: *http://www.chiark.greenend.org.uk/~sgtatham/putty*

### *10.7.4 Instalação da aplicação OLSR Dot Draw*

Para ser efectuado a instalação da aplicação *OLSR Dot Draw* devem ser executados os seguintes passos:

1. Instalar os seguintes pacotes no computador de modo a permitir a gerar as imagens que correspondem à topologia da restectiva rede:
    - ***Graphviz*** *(http://www.graphviz.org/);*
    - ***Imagemagick*** *(http://www.imagemagick.org/ );*
    - Instalar o *Dot OLSR Draw Plugin* (por exemplo num router WRT54G) executando o seguinte comando:
        - ***"ipkg instalar olsrd-libs"***
2. Em seguida, àpos a instalação do respectivo plugin deverá ser adicionado no ficheiro, ***"/olsrd.conf/etc",*** a seguinte linha de comando: "***LOAD_PLUGIN olsrd_dot_draw.so.0.1"***.
3. A seguir, deverá ser reiniciado o protocolo OSLR.
4. Seguidamente, verificar se existe alguma saída na porta TCP 2004, digitando o seguinte comando: ***"telnet localhost 2004"***
5. Por último, poderá ser verificado a actualização da topologia da rede em tempo real, executando o script através do seguinte comando: ***". /olsr-topology-mesh-lab.pl"***

    **NOTA:** É de referir que, poderá ainda ser obtido um gráfico contendo cores e informações de um nó de um determinado laboratório, executando o seguinte comando:

    - ***" ./olsr-topology-mesh-lab.pl --server meshy.dhcp --noshow --fontsize 14 --size 10,10 --port 2005 --bgcolor blue"***

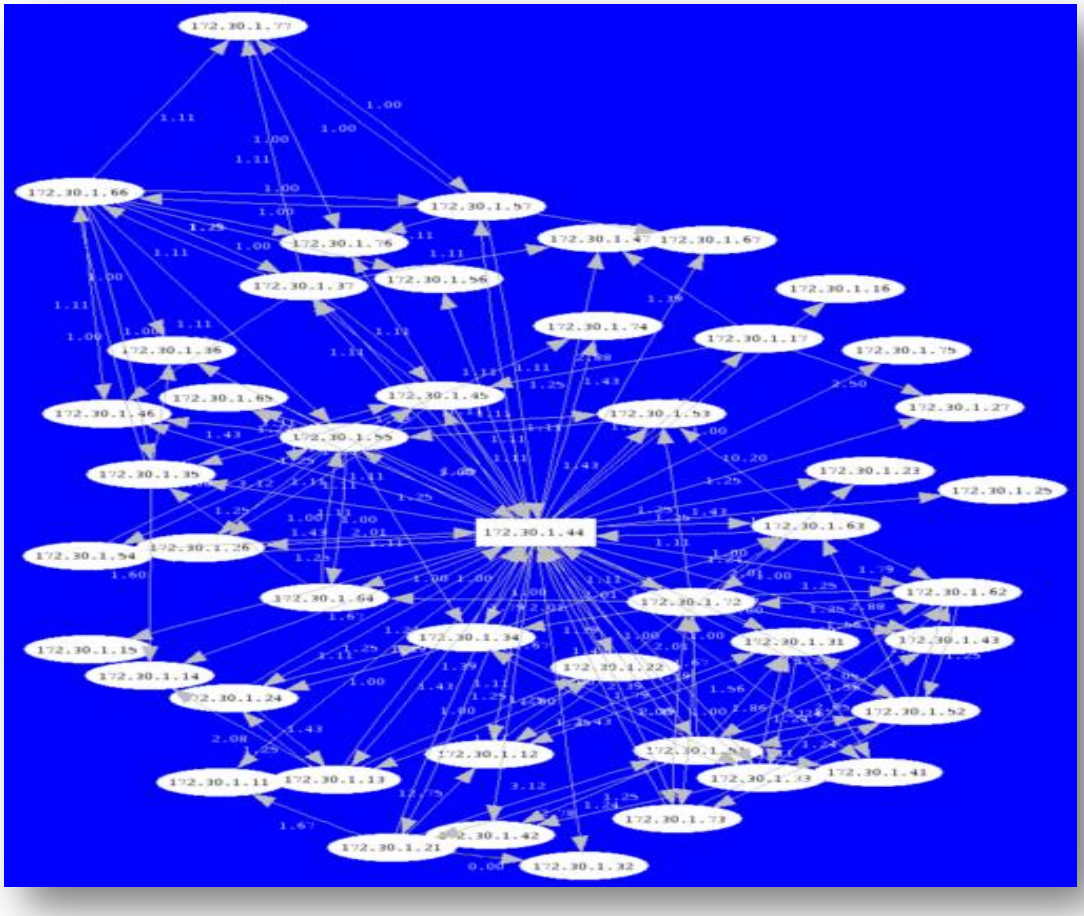



**Figura 119 – Exemplo de uma topologia de rede OLSR gerada automaticamente.**

## *10.8 Instalação do Firmware Freifunk para o SO do router WRT54G*

Neste ponto, será feita uma breve descrição sobre o manual de instalação do *firmware Freifunk*, de modo a facilitar ao gestor e/ou administrador do sistema, uma melhor gestão de toda a informação disponível no sistema operativo de um router numa determinada rede *Mesh* para garantir um melhor funcionamento da respectiva rede.

Antes de ser efectuado a instalação do firmware Freifunk devem ser considerados os seguintes aspectos:

Em primeiro lugar, deve-se implementar uma rede *Mesh* sem fios, configurando todos os nós *Mesh* e os AP's numa central de acordo com a arquitectura a ser implementada. Seguidamente, deverá ser anotado e guardado toda a informação necessária relativamente ao plano de configuração de cada um dos equipamentos e se preferível deverá ser colado nos respectivos equipamentos de modo a permitir uma melhor planificação por parte de um técnico e/ou administrador da rede.

È de referir que, será sempre uma boa pratica salvaguardar um ficheiro ".log", contendo não só, todos os detalhes da configuração e a localização dos nós, como também, toda a informação do historial de cada nó.

Em segundo lugar, estando o técnico responsável pela instalação da rede na central deverá efectuar um teste exaustivo em todos os equipamentos de modo a garantir um melhor funcionamento dos equipamentos.

Seguidamente, deverá ser conectado um nódo *Mesh* com um PC usando um cabo LAN, sendo que, em seguida deverá ser verificado se na respectiva máquina está a ser solicitado um endereço IP pelo DHCP.

A seguir, verificar se existe conectividade entre os equipamentos executando o comando "ping". Caso o ping for efectuado com sucesso, isto significa que o nó *Mesh* que está interligado no PC e os restantes nós estão funcionando correctamente. Em caso contrário deverá ser verificado toda a configuração do respectivo nó *Mesh*.

O terceiro passo, será instalar os nós *Mesh* numa *gateway* que permitirá ao administrador da rede, efectuar uma interligação entre a internet e a rede *Mesh*. Sendo assim, poderá ser confirmado que a rede estará funcionando assim que for configurado um novo nó *Mesh*, conectando-o no PC com um cabo LAN.

A seguir, efectuar um ping para verificar a conexão na *gateway* e caso for executado com sucesso deverá ser efectuado um ping para um determinado site na internet de modo a verificar se o PC está a ter acesso à internet.

### *10.8.1 Configuração e instalação de um nó Mesh sem fios*

Para ser efectuado a configuração e instalação de um nó *Mesh* sem fios devem ser executados os seguintes passos:

1. Efectuar um *upgrade* do *firmware* a ser instalado no router, sendo que, deverá ser efectuado em todos os backbone e nos nódos *Mesh*;
2. Deverá ser efectuado uma configuração nos seguintes campos do respectivo firmware:
    - *System settings;*
    - *Wireless settings;*
    - *LAN settings;*
    - *OLSR (Optimized Link State Routing) settings.*


**Figura 120 – Exemplo de um router Linksys WRT54GL.**

#### *10.8.1.1 Upgrading do firmware - Freifunk*

A seguir estão descritos todos os passos para efectuar um *upgrade* do *firmware Linksys* com o *firmware Freifunk*:

1. Efectuar o *download* o *firmware Freifunk* no seguinte site: *http://download-master.berlin.freifunk.net/ipkg/_g%2bgl/*
2. Seguidamente, deverá ser conectado um cabo LAN no PC/laptop e na porta de ligação *Ethernet* 1-4 conforme está ilustrada na figura anterior. **NOTA:** Importa salientar que, não deverá ser interligado na porta correspondente à Internet. O cabo LAN não precisa ser o que provem da distribuição da *Linksys*, visto que, qualquer cabo LAN *straight through* (*not cross-over*) poderá efectuar esta ligação.
3. A seguir, deverá ser verificado se a respectiva máquina está configurada para adquirir um endereço IP address de forma automática (Consultar a secção 10.8.6).
4. Conectar o cabo de ligação do router *Linksys* e clicar no botão de *power*.
5. Dependendo da porta LAN do router a que foi seleccionado, será activado o LED (*Light Emitting Diode*) com um sinal verde, que corresponderá ao número da respectiva porta. Por exemplo, se for utilizado o porto 1 então o LED 1 será activado. Caso não estiver activado deverá ser verificado a ligação do respectivo cabo.

6. Reparar e configurar a conexão LAN de modo a atribuir um endereço IP 192.168.1.x (Consultar a secção 10.8.6). Para verificar que o PC está com o respectivo endereço deverá ser executado os seguintes passo:

    - Na janela de “Ligação de Área Local”, com o botão direito do rato → Seleccionar a opção “Status” → Seguidamente, clicar em no submenu “Suporte”. A seguir será ilustrada a gama do endereço IP 192.168.1.x, (em que terá um valor variado no seguinte intervalo $1 \leq x < 255$).

7. A seguir, deverá ser confirmado se o *Web browser* não está configiurado para aceder ligação à internet via um *proxy*. Deverá ser introduzido o seguinte endereço IP, nomeadamente o 192.168.1.1, de modo a permitir ser redireccionado para a paginá principal da configuração do router *Linksys*.

    **NOTA:** Importa salientar que, para aceder à área de administração do referido equipamento, deverá ser efectuado uma autenticação para o efeito, introduzindo os seguintes dados de acesso:

    - Login: root;
    - Password: admin.

8. Seguidamente, deverá ser seleccionado a opção ***"Administration"*** e depois ***"Firmware Upgrade".*** Em seguida, clique em no botão ***"Browse"***, e a seguir a opção ***"Choose file",*** para seleccionar o respectivo *firmware Freifunk* (*openwrt-g—Freifunk 1.4.5 en.bin*) que anteriormente foi feito o *download*. Por último, seleccionar a opção ***"Upgrade"***, para efectuar a actualização do referido *software*. É de referir que, durante o processo de actualização, o LED começará a piscar e o LED DMZ, estará activado ou com a luz a piscar. **NOTA:** Importa referir que, será despoletado uma mensagem no ecrã informando que a operação foi bem-sucedida, sendo que, é recomendado a aguardar um intervalo de 4 a 6 minutos de modo a não interromper o processo de actualização e corromper o ficheiro de instalação, tornando o equipamento imprópio para utilização. Após cerca de 4-6 minutos, o LED de energia deverá estar permanentemente ON e o LED DMZ deverá estar permanentemente desligado.

9. Por último, seleccionar a opção ***“Continue"*** de modo a finalizar o processo de actualização do respectivo *firmware*. Em seguida, será redireccionado para a página de boas vindas do referido sofware.

Após o processo de actualização do *firmware* da *Linksys* para a versão do *firmware Freifunk*, poderá ser configurado o nó da rede *Mesh*. Entretato, conforme já tinha sido referido anteriormente deverão ser efectuadas as seguintes configurações:

- *System settings;*
- *Wireless settings;*
- *LAN settings;*
- *OLSR settings.*

Deverá ser configurado um nó para a rede *Mesh* sem fio, com o seguinte, endereço IP 10.1.1.4, conforme ilustra a seguinte figura:

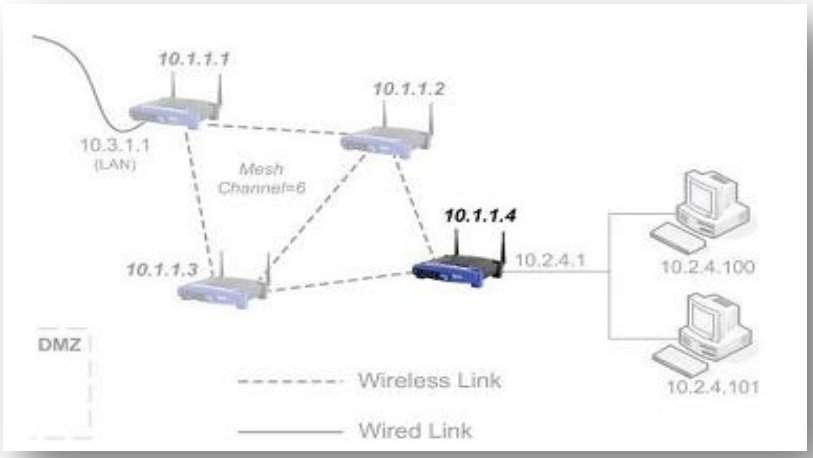



**Figura 121 – Exemplo de configuração de um nó para a rede mesh sem fio.**

### *10.8.1.2 System settings*

A seguir estão descritos todos os passos para efectuar uma alteração nas definições do sistema do *firmware Freifunk*:

1. No ecrã principal de administração, seleccionar o menu ***"Admin"*** e em seguida seleccionar a opção ***"System"***, para configurar as definições do sistema.
2. A seguir será despoletado um ecrã de configuração do sistema contendo vários campos de preenchimento, conforme poderá ser observado na figura a seguir:

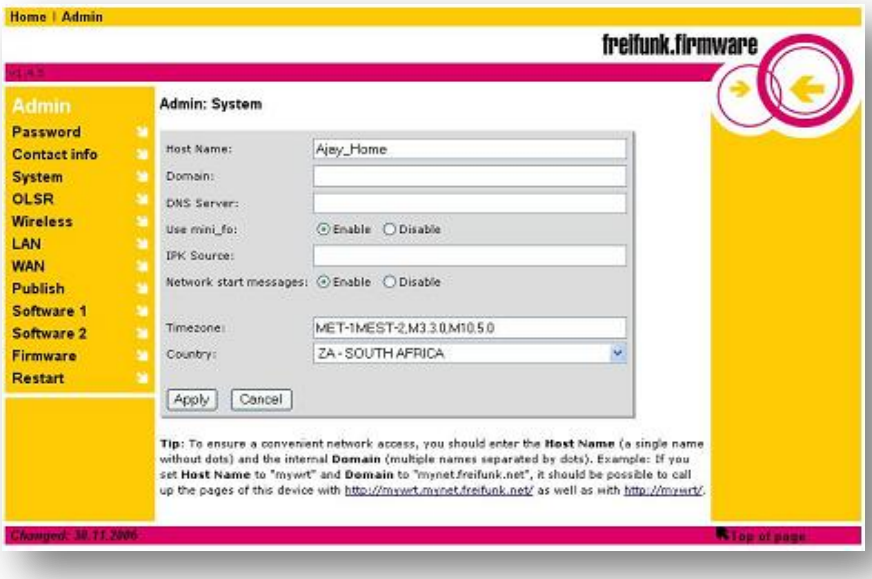



**Figura 122 – Menu de Administração do firmware Freifunk – System Settings.**

3. Seguidamente deverão ser preenchidos os seguintes campos de edição conforme ilustra a figura anterior:

    - Host Name: este campo permite atribuir um nome qualquer de modo a descrever e identificar o respectivo equipamento *Linksys*;
    - Country: deverá ser seleccionado um país aonde o equipamento *Linksys* estará sendo usado (por exemplo: Portugal), de modo que as configurações referentes a opção pretendida sejam determinadas.

    **NOTA:** Importa salientar que, os restantes campos não são de preenchimento obrigatário, sendo que poderão não ser preenchidas.

4. A seguir, seleccionar a opção ***"Apply"***, para aplicar as alterações efectuadas. Seguidamente, será ilustrada uma mensagem informando que as devidas alterações foram salvaguardadas e que serão aplicadas após o *restart* do dispositivo.


5. Na área de ***"Restart"***, seleccionar a opção ***"Restart",*** para reiniciar a máquina de modo que as respectivas alterações poderão ser aplicadas. Importa salientar que, o processo de inicialização poderá demorar alguns minutos e o

sistema do dispositivo da *Linksys* será actualizado automaticamente durante o respectivo processo. Seguidamente, será redireccionado para a página ***"Freifunk.Net - Hello!"***, sendo que será atribuído o nome do respectivo equipamento (com o seguinte formato ***"[Host Name] - Hello! "***).

#### *10.8.1.3 Wireless settings*

A seguir estão descritos todos os passos para efectuar uma alteração nas definições de *Wireless* do *firmware Freifunk*:

1. No ecrã principal de administração, seleccionar o menu ***"Admin"*** e em seguida seleccionar a opção ***"Wireless"***, para configurar as definições da interface wireless.
2. A seguir será despoletado um ecrã de configuração do sistema contendo vários campos de preenchimento, conforme poderá ser observado na figura a seguir:

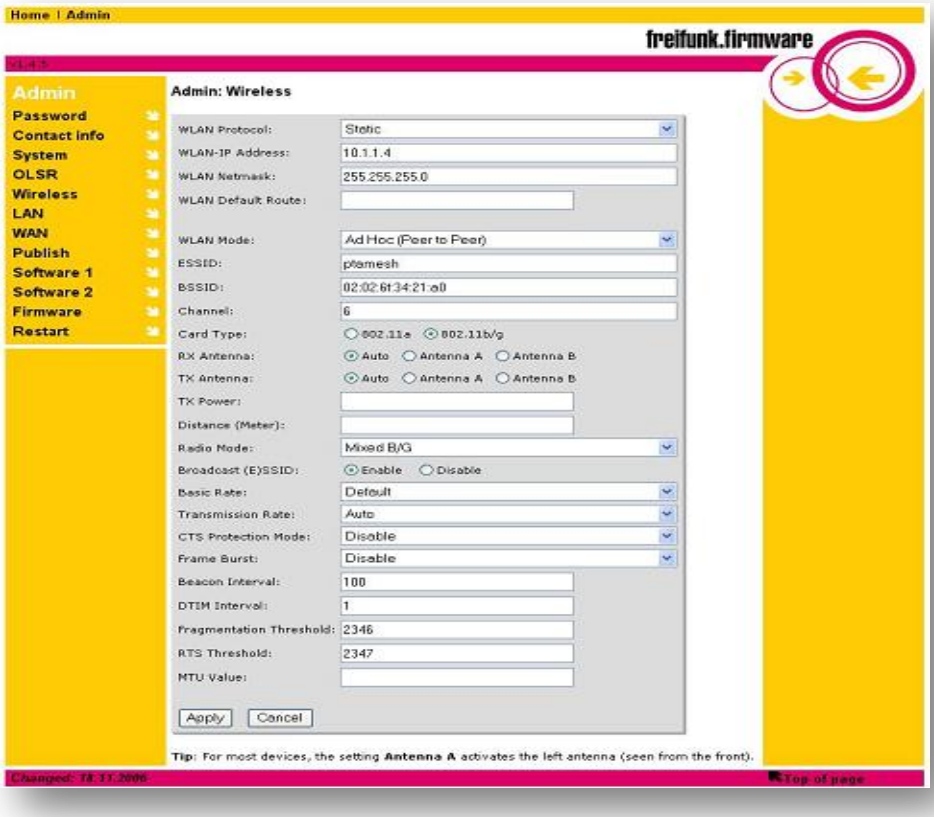



**Figura 123 – Menu de Administração do firmware Freifunk – Wireless Settings.**

3. Seguidamente deverão ser preenchidos os seguintes campos de edição conforme ilustra a figura anterior:
    - WLAN Protocol: Neste campo deverá ser escolhido na *dropdown* a opção opção ***"Static"***;

- WLAN IP Address: este campo permite introduzir o endereço IP correspondente à rede wireless (como por exemplo 10.10.1.4);
- WLAN IP Mask: este campo permite introduzir a máscara de rede sem fios (como por exemplo 255.255.255.0);
- WLAN Default Route: permite introduzir uma rota por defeito, sendo que caso for o padrão poderá permanecer em branco;
- WLAN Mode: neste campo deverá ser seleccionado a opção "*Ad-Hoc* (*Peer to Peer*);
- ESSID: esse campo permite ao administrador da rede introduzir uma descrição do ESSID à sua escolha;
- BSSID: esse campo permite ao administrador da rede introduzir uma descrição do BSSID à sua escolha;

  **NOTA:** Importa salientar que, será sempre aconselhável bloquear o BSSID. Poderá ser escolhido um determinado endereço MAC de um equipamento *Linksys* e usá-lo para todos os restantes equipamentos *Linksys* existentes na rede *Mesh*. O BSSID é muito importante, visto que, permite especificar e reunir redes *Mesh*, caso houver uma quebra entre duas redes devido a uma falha de ligação, ela será mais tarde restabelecida.

- *Channel*: este campo permite digitalizar um determinado número de canal, num intervalo de 1 a 13 canais disponíveis, mas contudo, isto dependerá muito do país escolhido sob a configuração do sistema.
- RX Antena e TX Antena: nesses campos deverão ser escolhidos a opção "Auto", tanto para o campo "RX Antena" e/ou "TX Antena". Contudo, poderá ser escolhido uma outra opção de acordo com a antena que esteja a ser utlizado.

**NOTA:** Importa salientar que, os restantes campos não são de preenchimento obrigatário sendo que poderão ser preenchidas.

4. A seguir, seleccionar a opção ***"Apply"***, para aplicar as alterações efectuadas. Seguidamente, será ilustrada uma mensagem informando que as devidas alterações foram salvaguardadas e que serão aplicadas após o *restart* do dispositivo.


5. Na área de ***"Restart"***, seleccionar a opção ***"Restart"***, para reiniciar a máquina de modo que as respectivas alterações poderão ser aplicadas. Importa salientar que, o processo de inicialização poderá demorar alguns minutos e o sistema do dispositivo da *Linksys* será actualizado automaticamente durante o respectivo processo.

   **NOTA:** Importa salientar que, o preenchimento dos campos apartir de "*WLAN Mode" até ao "RX Antena e TX Antena",* deverão ser aplicados da mesma forma para os restantes equipamentos.

### *10.8.1.4 LAN settings*

A seguir estão descritos todos os passos para efectuar uma alteração nas definições da rede LAN do *firmware Freifunk*:

1. No ecrã principal de administração, seleccionar o menu ***"Admin"*** e em seguida seleccionar a opção ***"LAN"***, para configurar as definições da interface LAN.
2. A seguir será despoletado um ecrã de configuração do sistema contendo vários campos de preenchimento, conforme poderá ser observado na figura a seguir:

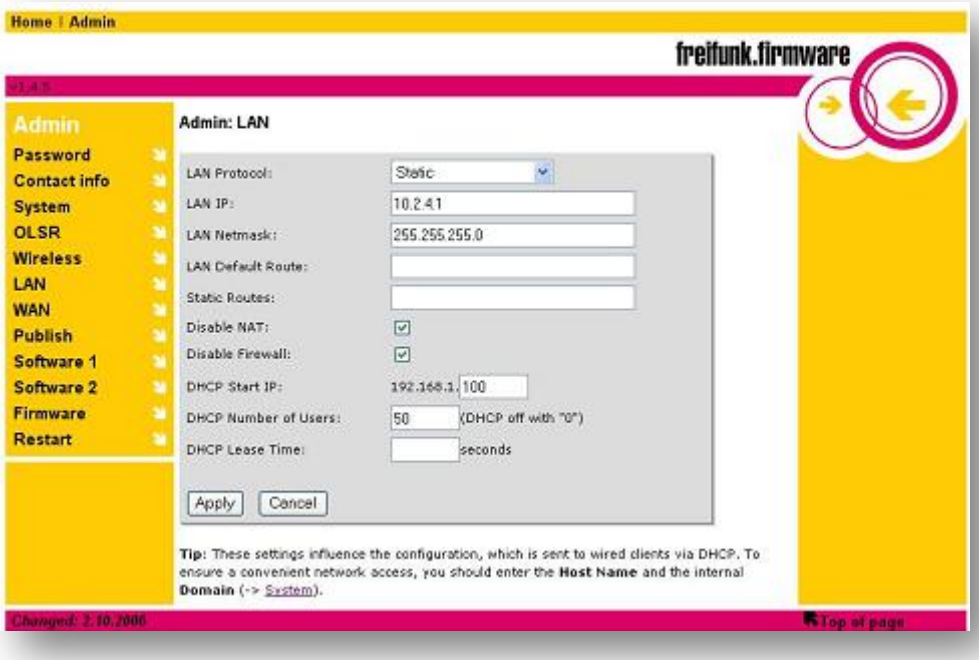



**Figura 124 – Menu de Administração do firmware Freifunk – LAN Settings.**

3. Seguidamente deverão ser preenchidos os seguintes campos de edição conforme ilustra a figura anterior:

    - LAN Protocol: Neste campo deverá ser escolhido na dropdown a opção opção ***"Static"***;
    - LAN IP: este campo permite introduzir o endereço IP correspondente à rede wireless (como por exemplo 10.2.4.1);
    - LAN NetMask: este campo permite introduzir a máscara de rede sem fios. Poderá ser utilizado a seguinte máscara 255.255.255.0, mas contudo, caso for necessário poderá ainda ser usado uma outra máscara qualquer);
    - LAN Default Route: permite introduzir uma rota por defeito, sendo que caso for o padrão poderá permanecer em branco;
    - Disable NAT: este campo deverá ser seleccionado de modo a que o NAT possa ser desactivado;
    - Disable Firewall: este campo deverá ser seleccionado de modo a que o Firewall possa ser desactivado;

4. A seguir, seleccionar a opção "*Apply*", para aplicar as alterações efectuadas. Seguidamente, será ilustrada uma mensagem informando que as devidas alterações foram salvaguardadas e que serão aplicadas após o *restart* do dispositivo.


5. Na área de ***"Restart"***, seleccionar a opção ***"Restart"***, para reiniciar a máquina de modo que as respectivas alterações poderão ser aplicadas. Importa salientar que, o processo de inicialização poderá demorar alguns minutos e o sistema do dispositivo da *Linksys* será actualizado automaticamente durante o respectivo processo.
6. Caso não for executado o passo no ponto anterior (passo 5.), deverá ser ignorado este passo (passo 6.). Importa salientar que, caso seja re-estalebecido a conexão ela não será valida, sendo que ápos um intervalo de 10 a 15 segundos deverá ser efectuada a reparação a respectiva ligação (consultar a secção 10.8.7).

7. Caso não for executado o passo no ponto anterior (passo 5.), deverá ser ignorado este passo (passo 7.). No campo de endereço do browser, deverá ser introduzido o endereço IP da rede LAN que foi anteriormente especificado no campo ***"LAN IP"*** e em seguida pressionar a tecla [Enter].

#### *10.8.1.5 OLRS settings*

A seguir estão descritos todos os passos para efectuar uma alteração nas definições de OLRS do *firmware Freifunk*:

1. No ecrã principal de administração, seleccionar o menu ***"Admin"*** e em seguida seleccionar a opção ***"OLRS"***, para configurar as definições do OLRS.
2. A seguir será despoletado um ecrã de configuração do sistema contendo vários campos de preenchimento, conforme poderá ser observado na figura a seguir:

**Figura 125 – Menu de Administração do firmware Freifunk – OLSR Settings.**

3. Seguidamente deverão ser preenchidos os seguintes campos de edição conforme ilustra a figura anterior:

    - HNA4: Neste campo deverá ser introduzido os três primeiros octetos do endereço IP da LAN seguido por 0/24 (como por exemplo: Se o endereço IP da LAN é 10.2.4.1, digite na 10.2.4.0/24);

    - DynGW: este campo permite ao administrador estabelecer uma ligação entre um router *Linksys* conectado à internet, com outros nós de modo a permitir-lhes um acesso à internet. Para isso será necessário seleccionar a opção *"Enable"* para activar o gateway para modo dinâmico.

4. A seguir, seleccionar a opção "*Apply*", para aplicar as alterações efectuadas. Seguidamente, será ilustrada uma mensagem informando que as devidas alterações foram salvaguardadas e que serão aplicadas após o restart do dispositivo.


5. Na área de ***"Restart"***, seleccionar a opção ***"Restart"***, para reiniciar a máquina de modo que as respectivas alterações poderão ser aplicadas. Importa salientar que, o processo de inicialização poderá demorar alguns minutos e o sistema do dispositivo da *Linksys* será actualizado automaticamente durante o respectivo processo.

    **NOTA:** É de salientar que, se no caso não foram efectuados os passos de inicialização do equipamento *Linksys* durante o processo de configurações nas sessões anteriores, deverá ser efectuado de imediato o processo de inicialização do respectivo equipamento *Linksys*.

### *10.8.2 Configuração de OLRS para interligar duas redes mesh*

Neste ponto, será feita uma breve descrição sobre a configuração do protocolo OLRS de modo a que possa ser estabelecida uma interligação entre duas redes *Mesh* sem fios.

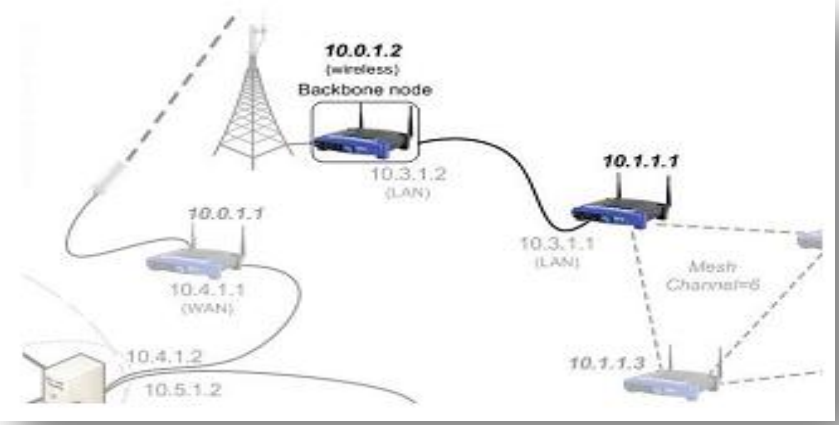



**Figura 126 – Interligação de duas redes mesh.**

Na figura anterior, está ilustrada um exemplo contendo duas redes *Mesh* separadas, sendo que em ambas as respectivas redes está configurado o protocolo OLSR. Será utilizado dois rourter da *Linksys* para juntar as duas redes, conforme poderá ser observado na figura anterior (são os nós com os seguintes endereços *Ethernet*: 10.3.1.2 e 10.3.1.1).

Importa salientar que, no exemplo anterior, foi considerado o seguinte:

- As duas redes devem ter endereços IP únicos, senão eles não podem ser unidos;
- Que no máximo uma das redes deve possuir apenas um unico gateway de internet.

Para configuração do protocolo OLRS de modo a que possa ser estabelecida uma interligação entre duas redes *Mesh* sem fios deverá ser considerado duas configurações importantes, quer ao nível do *hardware* e do *software*.

### *10.8.2.1 Configuração ao nível de Software*

A seguir estão descritos todos os passos para efectuar uma configuração ao nível de *software* para efectuar uma interligação entre duas redes *Mesh* com o auxílio do protocolo OLRS do *firmware Freifunk*:

1. Deverá ser conectado um cabo LAN no PC/laptop e na porta de ligação *Ethernet* 1-4 conforme está ilustrada na figura anterior.

   **NOTA:** Importa salientar que, não deverá ser interligado na porta correspondente à Internet.

O cabo LAN não precisa ser o que provem da distribuição da *Linksys*, visto que, qualquer cabo *LAN straight through* (*not cross-over*) LAN cable poderá efectuar esta ligação.

2. Efectuar *logon* no *Linksys* usando *ssh* ou *PuTTY* (se estiver usando Windows).
3. Editar o arquivo ***/olsrd.conf/etc***, editando o seguinte comando:
    - “***vi /olsrd.conf/etc”;***
4. Efectuar a seguinte alteração na secção das interfaces:
    - ***interface "eth1" “br0";***
5. Repitir todos os passos ateriormente citados no segundo router da *Linksys*;

#### *10.8.2.2 Configuração ao nível de Hardware*

A seguir estão descritos todos os passos para efectuar uma configuração ao nível de *hardware* para efectuar uma interligação entre duas redes *Mesh* com o auxílio do protocolo OLRS do *firmware Freifunk*:

- Deverá ser efectuado uma interligação entre os *router* da *Linksys*, através da utilização de um cabo *straight* (em vez de um cabo cruzado), nos portos de 1-4 dos respectivos equipamentos. Considerando o exemplo descrito na figura anterior, deverá ser ligado uma extremidade do cabo LAN à porta 1-4 do router com o endereço IP 10.3.1.2, com uma outra extremidade à porta 1-4 do equipamento contendo o endereço IP 10.3.1.1.

### *10.8.3 Configuração de Gateway*

Neste ponto, será feita uma breve descrição sobre a configuração do gateway de modo a que possa ser estabelecida uma interligação entre duas redes *Mesh* sem fios.

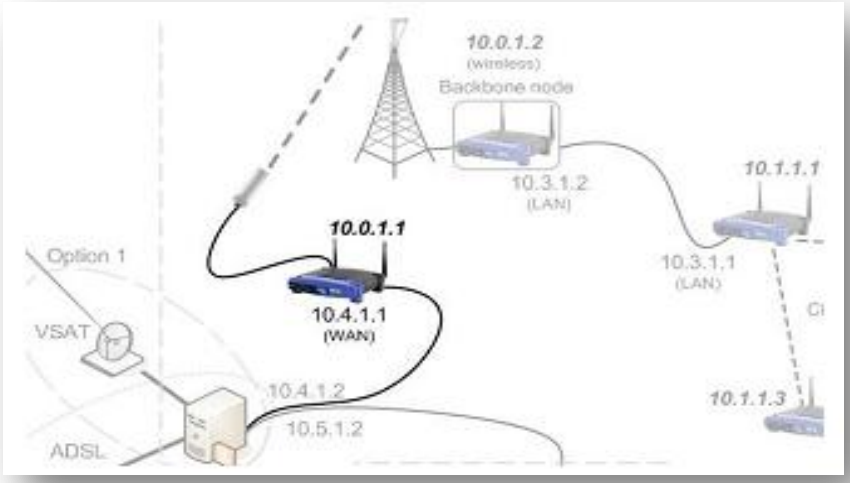



**Figura 127 – Exemplo de configuração de uma gateway para a rede mesh.**

**NOTA:** É de referir que, para a configuração do gateway para a referida rede *Mesh*, deve ser levado em consideração uma alteração na configuração da interface WAN.

### *10.8.3.1 WAN settings*

A seguir estão descritos todos os passos para efectuar uma alteração nas definições da rede LAN do firmware Freifunk:

1. No ecrã principal de administração, seleccionar o menu ***"Admin"*** e em seguida seleccionar a opção ***"WAN"***, para configurar as definições da interface WAN.
2. A seguir será despoletado um ecrã de configuração do sistema contendo vários campos de preenchimento, conforme poderá ser observado na figura a seguir:

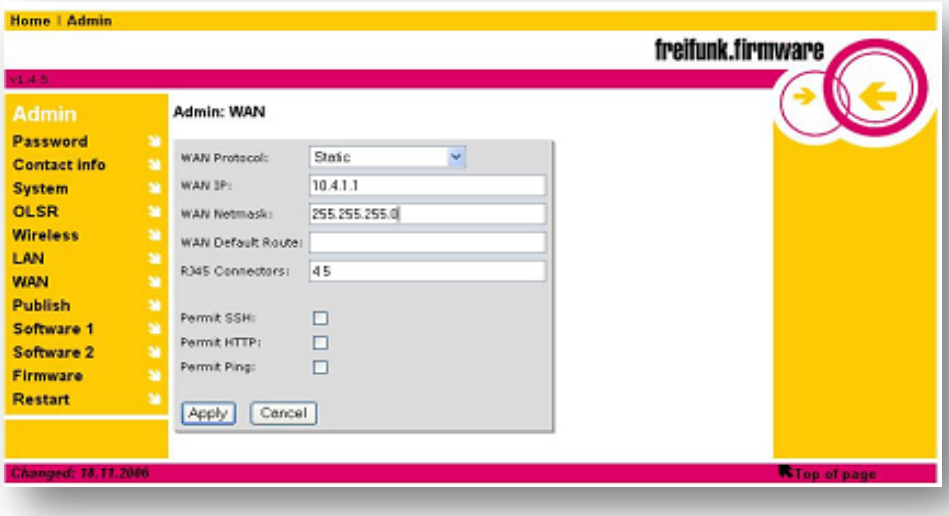



**Figura 128 – Menu de Administração do firmware Freifunk – WAN Settings.**

3. Seguidamente deverão ser preenchidos os seguintes campos de edição conforme ilustra a figura anterior:

    a) WLAN Protocol: Neste campo deverá ser escolhido na dropdown a opção opção ***"Static"***;

    b) WLAN Protocol: Neste campo deverá ser escolhido na dropdown a opção opção ***"Dynamic"***;

    c) WAN IP: neste campo deverá ser introduzido um endereço IP que esteja num intervalo pertencente ao endereço IP DHCP de um outro equipamento disponível na rede. Considerando o exemplo anterior deverá ser introduzido o seguinte endereço 10.4.1.1;

    d) WAN Netmask: este campo permite introduzir a máscara de rede sem fios (como por exemplo 255.255.255.0);

    e) WAN Default Route: dece ser introduzido o endereço IP do firewall. Considerando o exemplo anterior deverá ser introduzido o seguinte endereço 10.4.1.2;

**NOTA:** Importa salientar que, se no caso for considerado o exemplo anterior há que ter em conta os seguintes aspectos:

- Se o servidor gateway (10.4.1.2 no exemplo anterior) não correr o DHCP deverão ser executados os passos: 1, 2, 3.a), 3.a), 3.c), 3.d) e 3.e).
- Se o servidor DHCP for activado então deverão ser executados os passos: 1, 2 e 3 (b).

### *10.8.4 Configuração de uma ligação entre um nó mesh e um AP*

Neste ponto, será feita uma breve descrição sobre a configuração de uma ligação entre um nó *Mesh* e um AP (*Access Point*), permetindo criar um *hotspot*.

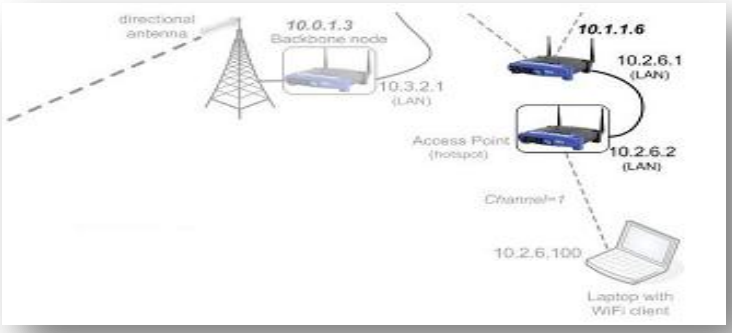



**Figura 129 – Exemplo de configuração de um AP sem fios.**

Para ser efectuado a configuração e instalação de um AP *Mesh* sem fios devem ser executados os seguintes passos:

1. Efectuar um *upgrade* do firmware (DD-WRT);
2. Deverá ser efectuado uma configuração nos seguintes campos do respectivo firmware:
    - *Setup – Basic settings;*
    - *Wireless - Basic Setup settings;*

#### *10.8.4.1 Upgrading do firmware – DD-WRT*

A seguir estão descritos todos os passos para efectuar um *upgrade* do *firmware Linksys* com o *firmware DD-WRT*:

1. Efectuar o *download* o *firmware DD-WRT* no seguinte site: *http://www.dd-wrt.com/*
2. Seguidamente, deverá ser conectado um cabo LAN no PC/laptop e na porta de ligação *Ethernet* 1-4 conforme está ilustrada na figura anterior.

    **NOTA:** Importa salientar que, não deverá ser interligado na porta correspondente à Internet. O cabo LAN não precisa ser o que provem da distribuição da *Linksys*, visto que, qualquer cabo *LAN straight through* (*not cross-over*) poderá efectuar esta ligação.
3. A seguir, deverá ser verificado se a respectiva máquina está configurada para adquirir um endereço IP address de forma automática (Consultar a secção 10.8.6).
4. Conectar o cabo de ligação do router *Linksys* e clicar no botão de power.
5. Dependendo da porta LAN do router a que foi seleccionado, será activado o LED (*Light Emitting Diode*) com um sinal verde, que corresponderá ao número da respectiva porta. Por exemplo, se for utilizado o porto 1 então o LED 1 será activado. Caso não estiver activado deverá ser verificado a ligação do respectivo cabo.
6. Reparar e configurar a conexão LAN de modo a atribuir um endereço IP 192.168.1.x (Consultar a secção 10.8.7). Para verificar que o PC está com o respectivo endereço deverá ser executado os seguintes passo:
    - Na janela de “Ligação de Área Local”, com o botão direito do rato → Seleccionar a opção “Status” → Seguidamente, clicar em no submenu

"Suporte". A seguir será ilustrada a gama do endereço IP 192.168.1.x, (em que terá um valor variado no seguinte intervalo $1 \leq x < 255$).

7. A seguir, deverá ser confirmado se o *Web browser* não está configiurado para aceder ligação à internet via um proxy. Deverá ser introduzido o seguinte endereço IP, nomeadamente o 192.168.1.1, de modo a permitir ser redireccionado para a paginá principal da configuração do router *Linksys*.

   **NOTA:** Importa salientar que, para aceder à área de administração do referido equipamento, deverá ser efectuado uma autenticação para o efeito, introduzindo os seguintes dados de acesso:

   - Login: root;
   - Password: admin.

8. Seguidamente, deverá ser seleccionado a opção ***"Administration"*** e depois ***"Firmware Upgrade".*** Em seguida, clique em no botão ***"Browse"***, e a seguir a opção ***"Choose file",*** para selecionar o respectivo firmware DD-WRT (a última versão e a mais estável) que foi anteriormente foi feito o *download*. Por último, seleccionar a opção ***"Upgrade"***, para efectuar a actualização do referido *software*. É de referir que, durante o processo de actualização, o LED começará a piscar e o LED DMZ, estará activado ou com a luz a piscar. **NOTA:** Importa referir que, será despoletado uma mensagem no ecrã informando que a operação foi bem-sucedida, sendo que, é recomendado a aguardar um intervalo de 4 a 6 minutos de modo a não interromper o processo de actualização e corromper o ficheiro de instalação, tornando o equipamento imprópio para utilização. Após cerca de 4-6 minutos, o LED de energia deverá estar permanentemente ON e o LED DMZ deverá estar permanentemente desligado.

9. Por último, seleccionar a opção ***"Continue"*** de modo a finalizar o processo de actualização do respectivo firmware. Em seguida, será redireccionado para a seguinte página de boas vindas: ***"WRT54GL – Setup";***

Após o processo de actualização do *firmware* da *Linksys* para a versão do firmware DD-WRT, poderá ser configurado o AP sem fios para a rede *Mesh*. Entretato, conforme já tinha sido referido anteriormente deverão ser efectuadas as seguintes configurações:

- *Setup – Basic settings;*
- *Wireless - Basic Setup settings.*

### *10.8.4.2 DD-WRT Wireless settings*

A seguir estão descritos todos os passos para efectuar uma alteração nas definições da interface *wireless* do *firmware DD-WRT*:

1. No ecrã principal de administração do respectivo firmware, seleccionar o menu ***"Basic Setup"*** e em seguida seleccionar a opção ***"Wireless"***, para configurar as definições da interface wireless.
2. A seguir será despoletado um ecrã de configuração do sistema contendo vários campos de preenchimento, conforme poderá ser observado na figura a seguir:

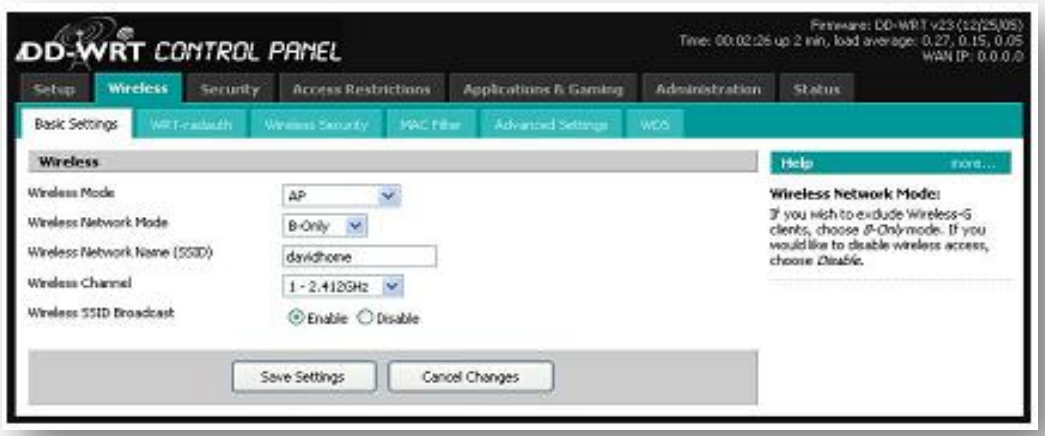



**Figura 130 – DD-WRT – AP Wireles Basic Settings.**

3. Seguidamente deverão ser preenchidos os seguintes campos de edição conforme ilustra a figura anterior:
    - Wireless Model: Neste campo deverá ser escolhido na dropdown a opção opção ***"AP"***;
    - Wireless Network Name (SSID): esse campo permite ao administrador da rede introduzir uma descrição do SSID à sua escolha;
    - Wireless Channel: este campo permite introduzir o número de canal pretendido pelo administrador da rede;

      **NOTA:** Importa salientar que, os restantes campos deverão ser deixados inalterados por defeito.
4. Por último, deverá ser seleccionado a opção ***"Save Setings",*** para salvaguardar as alterações efectuadas.

#### *10.8.4.3 DD-WRT Basic Setup settings*

A seguir estão descritos todos os passos para efectuar uma alteração nas definições da interface *wireless* do *firmware DD-WRT*:

1. No ecrã principal de administração do respectivo *firmware*, seleccionar o menu ***"Basic Setup"*** e em seguida seleccionar a opção ***"Wireless"***, para configurar as definições da interface do *AP wireless*.
2. A seguir será despoletado um ecrã de configuração do sistema contendo vários campos de preenchimento (observar a figura a seguir).
3. Seguidamente, deverão ser preenchidos os seguintes campos de edição conforme ilustra a figura anterior:
    - Internet Connection Type: Neste campo deverá ser escolhido na dropdown a opção opção ***"Disable"*** para especificar o tipo de ligação;
    - Network Address Server Settings (DHCP): esse campo permite ao administrador da rede seleccionar a opção "DHCP Forwarder" para defenir o tipo do protocolo DHCP a ser utilizado;
    - Wireless Channel: este campo permite introduzir o número de canal pretendido pelo administrador da rede;

      **NOTA:** Importa salientar que, esta funcionalidade vai reduzir automaticamente as opções de menu que será necessário para esta configuração.
    - Router IP: neste campo permite definir o endereço IP do AP da rede LAN, preenchendo o campo ***"Local IP Address"***.
    - Subnet Netmask: este campo permite introduzir a máscara de rede sem fios (como por exemplo 255.255.255.0);
    - DHCP Server: nesse campo deverá ainda ser introduzido o endereço IP do nó *Mesh* para que possa ser definido como sendo um "DHCP Server";
    - Time Setting: este campo permite definir o fuso horário

      **NOTA:** Importa salientar que, os restantes campos deverão ser deixados inalterados por defeito.
4. Por último, deverá ser seleccionado a opção ***"Save Setings",*** para salvaguardar as alterações efectuadas.

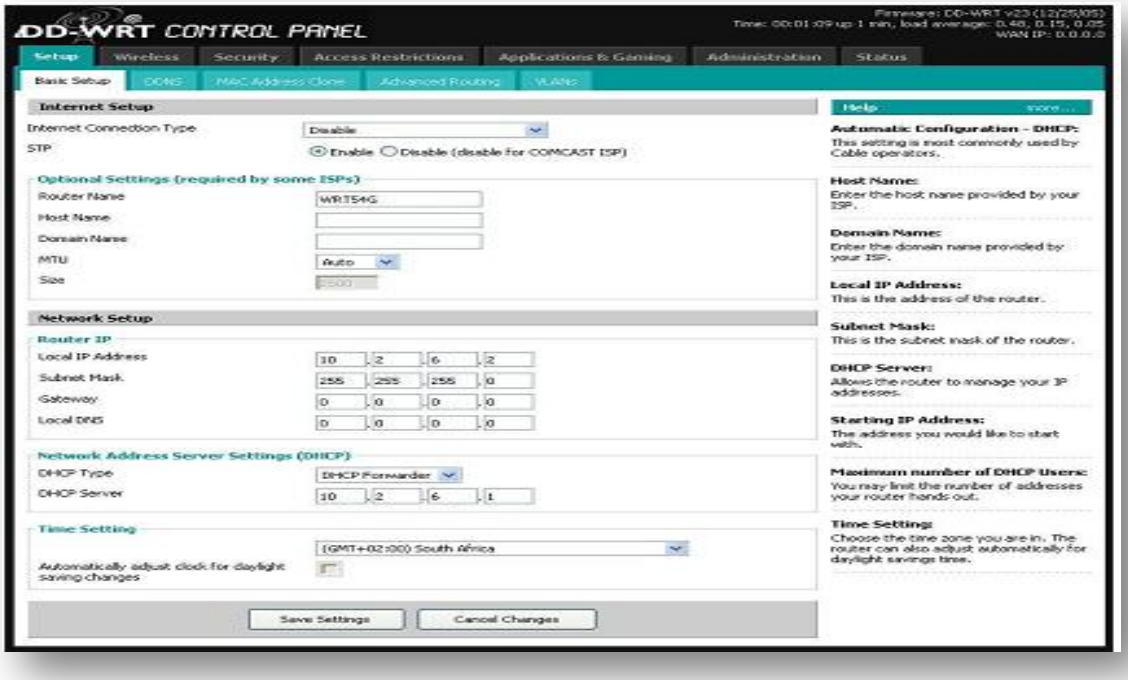



**Figura 131 – DD-WRT – AP Basic Setup Settings.**

### *10.8.5 Troubleshooting FAQs*

Neste ponto, será apresentado uma breve descrição de possíveis soluções que poderão resolver alguns problemas que possam surgir durante o processo de instalação e configuração da rede *Mesh*.

#### *10.8.5.1 Após o upload do firmware, o power LED não para de piscar. O que fazer?*

Esse problema poderá ser causado por vários factores, sendo que, o mais comum o erro humano. È de referir que, durante o processo de actualização o LED de energia deverá piscar, mas contudo, deverá parar após um intervalo de 6 minutos. Em caso contrário, deverá ser reiniciado o dispositivo da *Linksys*, desligando o cabo da tomada e ligá-lo novamente.

Caso o procedimento anterior não resultar, então deverão ser executados os passos seguintes:

1. Verificar se esta sendo utilizado correctamente o firmware apropriado durante o processo de *upload*;
2. Introduzir no seu PC ou computador portátil um endereço IP 192.168.1.x, onde 1 <x <255.

3. Abrir uma janela correspondente à inha de comando e verificar se exite conectividade entre os equipamentos, digitando o comando *ping* para o endereço IP 192.168.1.1.

4. Deverá ser feito um *reupload* do respectivo *firmware* usando o TFTP:

   a) Em Linux: No ambiente do S.O Linux deverá ser executado os seguintes procedimentos:

      - Na linha de comandos digitalizar os seguintes comandos:

        ***tftp 192.168.1.1***

        ***binary***

        ***rexmt 1***

        ***trace***

      - Em seguida, pressionar o botão [Enter] e antes de digitar o próximo comando, liga o equipamento *Linksys*. Seguidamente, deverá colocar a versão do *firmware*:

        ***put [openwrt-xxx-x.x xxx.bin];***

      - Depois será ilustrada no ecrã uma série de mensagens sendo que ao mesmo tempo, o power LED estará piscando. Entretanto, deverá aguardar por um período de 4 a 6 minutos para que o processo de *upload* possa ser terminado.

   b) Em Windows: No ambiente do S.O Windows deverá ser executado os seguintes procedimentos:

      - No menu "***Iniciar***", abrir duas linhas de comando, seleccionando a opção "***Executar"***. Em seguida, digitalizar ***"cmd"*** e, em seguidamente, pressionar o botão ***[ENTER]***;

      - Numa das janelas digitalizar o seguinte comando: ***"ping w t ping-10 192.168.1.1"*** e em seguida pressionar a tecla ***[ENTER]*** (Este endereço IP corresponde ao endereço IP do router). Deverá ser executado o comando ping de uma forma contínua para testar a interligação com o router, num tempo limite de 10 ms em vez do padrão 4000ms;

      - Na segunda janela, preparar o comando tftp, digitando:

        ***"tftp -i 192.168.1.1 put [openwrt-xxx-x.x-xxx.bin]"***

**NOTA:** Não deve ser pressionado a tecla ***[Enter]*** antes de ser efectuado o passo a seguir;

- Activar o power no dispositivo da *Linksys* (caso o cabo estiver ligado, deverá ser desligado e ligado novamente).

  Na janela de execução do comando ping deverá aparecer a seguinte mensagem ***"Hardware Error"***;

- Voltar para a janela tftp. Assim que receber uma resposta por parte do *router Linksys*, pressionar ***[Enter]*** na janela de tftp. A imagem deverá ser copiada sem serem feitas várias tentativas;

- Se o *ping* começa com ***"Hardware Error"***, em seguida, começar a responder e retornar novamente a mensagm ***"Hardware Error",*** por um breve intervalo de tempo deverá ser repetido o procedimento;

- Após cerca de seis minutos, deve ser introduzido o seguinte endereço IP 192.168.1.1 na barra de endereço de um browser, e caso tudo correr bem, deverá ser exibido a página oficial do respectivo firmware.

#### *10.8.5.2 Tenho o cabo de rede ligado ao meu PC / portátil e ao router da Linksys, mas o LED correspondente à rede LAN está inactivo. O que fazer?*

Para resolver este problema deverão ser executados os passos seguintes:

1. Verificar se o equipamento da *Linksys* está ligado;
2. Verificar se o cabo está:
   a) Conectado numa das portas de 1 a 4 da rede LAN e não das portas correspondentes à ligação de Internet.
   b) Conectado corretamente na parte de trás do router e também no PC e/ou no computador portátil.
   c) Ligado a um cabo directo e não num cabo *cross-over*.
3. Caso os procedimentos anteriores forem executados sem sucesso, será aconselhável substituir o respectivo cabo por um novo.

#### *10.8.5.3 Como poderá ser efectuado um teste num nó Mesh?*

Um único nó *Mesh* poderá ser testado de várias formas, por exemplo, usando um outro nó *known-working* ou uma outra estação sem fio (um PC ou portátil contendo uma placa wireless). De qualquer forma, deverá ser garantido que a estação ou o nó a serem testados, deverão ter a mesma configuração da rede (SSID, BSSID, channel, *Ad-Hoc* mode, wireless IP address na mesma sub-rede) como o nó que está sendo testado. Caso o comando ping for executado com sucesso, isso significará que o nó irá passar no teste.

### *10.8.6 Configuração das definições do protocolo TCP/IP*

Neste ponto, será feita uma breve descrição sobre o manual de configuração das definições do protocolo TCP/IP, de modo a facilitar ao administrador da rede consultar e configurar o estado de obtenção de um endereço IP de uma forma manual e/ou automática. Em seguida, será descrita os passos para efectuar a reparação e resolução dos possíveis problemas que eventualemente possam surgir na respectiva rede

#### *10.8.6.1 Configuração do protocolo TCP/IP em Windows XP*

Para ser efectuado a configuração do protocolo TCP/IP em Windows XP devem ser executados os seguintes passos:

1. No menu ***"Iniciar"***, escolher a opção ***"Painel de Controlo"***. A seguir, usando a vista clássica do respectivo Windows seleccionar ***"Ligações de Rede"***. Em seguida, seleccionar na lista de ligações de rede existentes a rede a que se pretende configurar com o botão direito do rato e depois clique em ***"Propriedades"***.

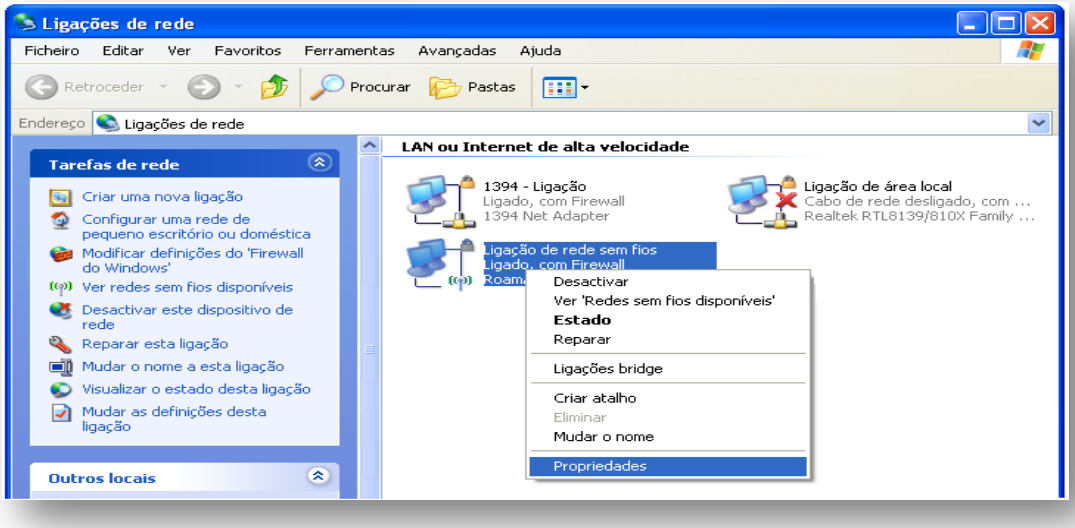



**Figura 132 – Windows XP – Ligações de Rede.**

2. No ecrã ***"Ligações de Rede"***, seleccionar o menu "***Geral"*** clique em Protocolo Internet (TCP/IP) e depois clique em Propriedades.

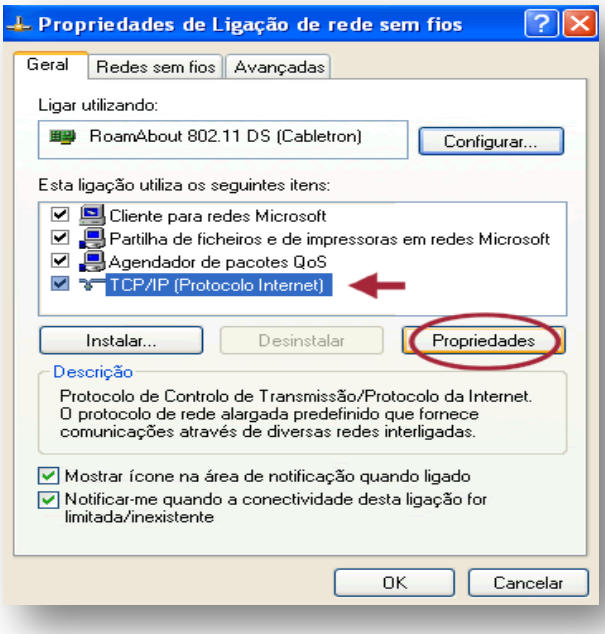



**Figura 133 – Windows XP – Ecrã de Propriedades de Ligação de Rede.**

3. Caso, se pretender obter automaticamente os endereços de servidor DNS de um servidor DHCP, deverá ser seleccionado a opção ***"Obter automaticamente o endereço dos servidores DNS"***, conforme ilustra a seguinte figura.


**Figura 134 – Windows XP – Ecrã de Propriedades de TCP/IP.**

### *10.8.6.2 Configuração do protocolo TCP/IP em Windows Vista*

Para ser efectuado a configuração do protocolo TCP/IP em Windows Vista e/ou Windows 7 devem ser executados os seguintes passos:

1. No menu "***Iniciar***", seleccionar a opção "***Painel de Controlo"***. Em seguida, no menu ***"Rede e Internet"***, seleccionar a opção ***"Centro de Rede e Partilha"*** e, em seguidamente, clicar em ***"Gerir Ligações de rede"***.

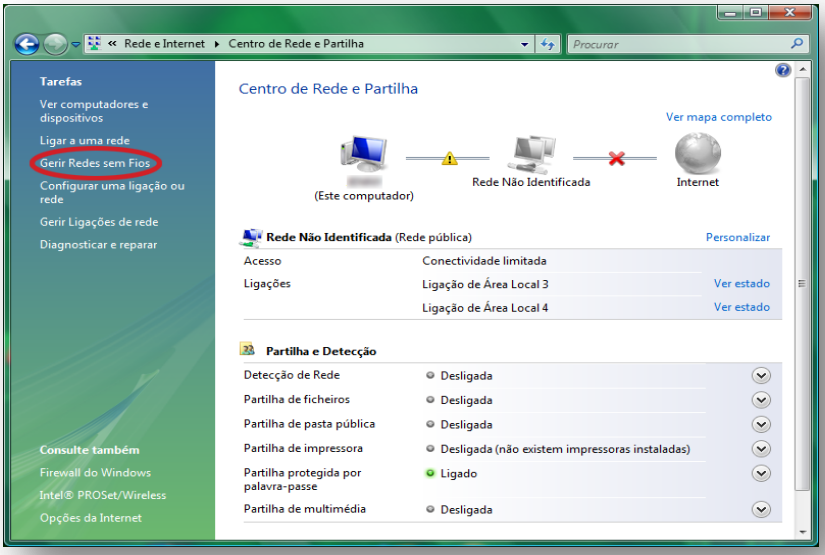



**Figura 135 – Windows Vista – Ecrã do Centro de Rede e Partilha.**

2. A seguir, seleccionar a ligação que pretende alterar e, em seguida, clique em ***"Propriedades do Adaptador"***. Caso for solicitado o preenchimento de uma palavra-passe de administrador ou uma confirmação, deverá ser introduzido a palavra-passe ou seleccionar a opção ***"OK"*** para confirmar a opção pretendida.

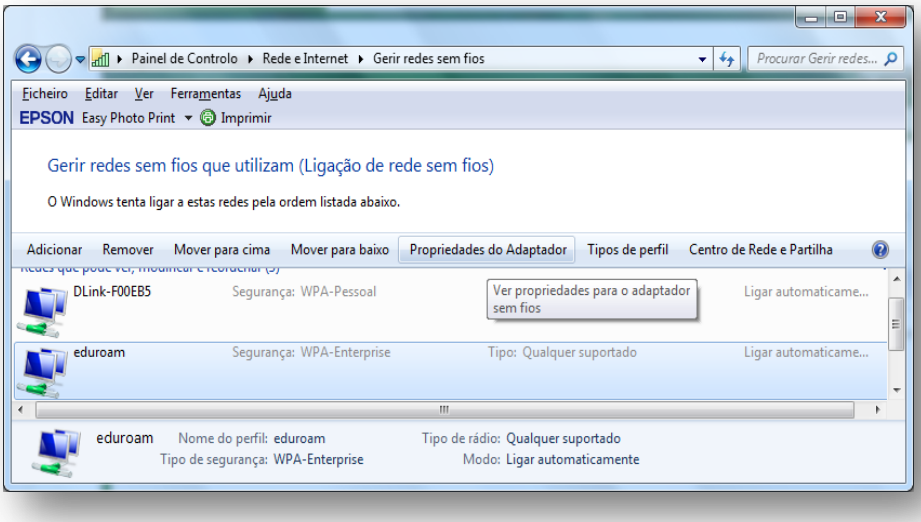



**Figura 136 – Windows Vista – Ecrã de Gestão redes sem fios.**

3. Seguidamente, seleccionar o separador ***"Funcionamento em rede"***. Na secção ***"Esta ligação utiliza os seguintes itens:"***, clique em ***"Protocolo IP versão 4 (TCP/IPv4) "*** ou em ***"Protocolo IP versão 6 (TCP/IPv6) "*** e, em seguida, clique em ***"Propriedades".***

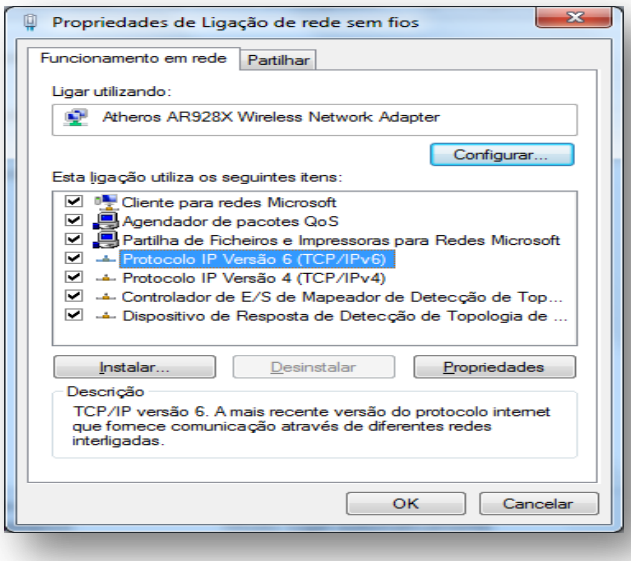



**Figura 137 – Windows Vista – Ecrã das Propriedades de Ligação de rede.**

4. Para especificar definições do endereço IP do IPv4, execute um dos seguintes procedimentos:

    - Para obter definições de IP automaticamente, clique em ***"Obter um endereço IP automaticamente"*** e, em seguida, clique em ***"OK"***.
    - Para especificar um endereço IP, clique em ***"Utilizar o seguinte endereço IP"*** e, em seguida, nas caixas Endereço IP, ***"Máscara de sub-rede e Gateway predefinido"***, introduza as definições do endereço IP.

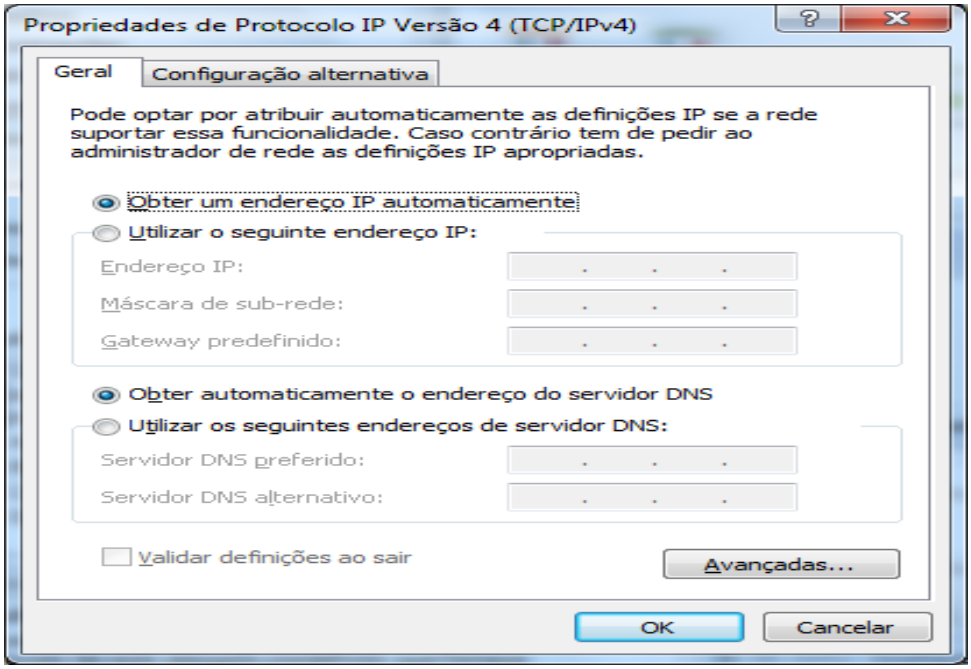



**Figura 138 – Ecrã das Propriedades de Protocolo IP Versão 4 (TCP/IPv4).**

5. Para especificar definições do endereço IP do IPv6, execute um dos seguintes procedimentos:

    - Para obter definições de IP automaticamente, clique em ***"Obter um endereço IPv6 automaticamente"*** e, em seguida, clique em OK.
    - Para especificar um endereço IP, clique em ***"Utilizar o seguinte endereço IPv6"*** e, em seguida, nas caixas Endereço IPv6, Comprimento do prefixo de sub-rede e *Gateway* predefinido, introduza as definições do endereço IP.

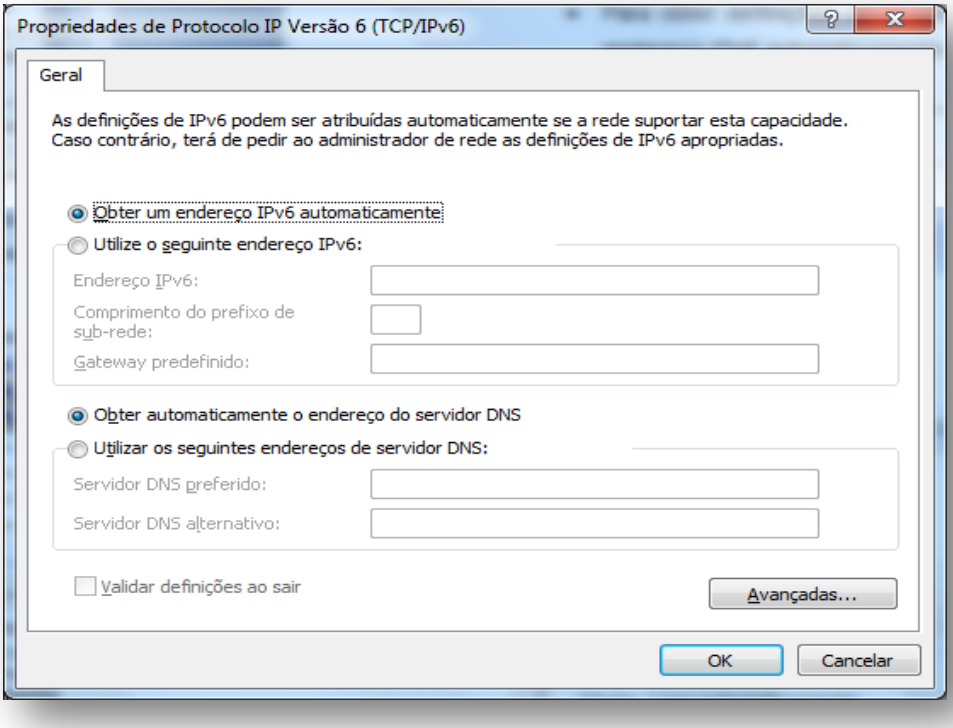



**Figura 139 – Ecrã das Propriedades de Protocolo IP Versão 6 (TCP/IPv6).**

6. Para especificar definições do endereço do servidor DNS, deverá ser executado os seguintes procedimentos:

    - Para obter um endereço do servidor DNS automaticamente, seleccionar a opção ***"Obter automaticamente o endereço do servidor DNS"*** e, em seguida, confirmar a opção pretendida em ***"OK"***.

    - Para especificar um endereço do servidor DNS, seleccionar a opção ***"Utilizar os seguintes endereços de servidor DNS"*** e, em seguida, nas caixas ***"Servidor de DNS preferido e Servidor de DNS alternativo"***, escrevendo os endereços dos servidores DNS principal e secundário.

7. Para alterar as definições de DNS, WINS e IP, clique em ***"Avançadas"***.

### *10.8.7 Reparação de problemas na rede*

Neste ponto, será feita uma breve descrição sobre o manual sobre a resolução de eventuais problemas que poderão surgir na rede quer no sistema operativo Windows e/ou em Linux.

#### *10.8.7.1 Windows*

Para ser efectuado a reparação de problemas na rede no SO Windows devem ser executados os seguintes passos:

1. No menu "***Iniciar***", seleccionar a opção "***Painel de Controlo"***.
2. Na caixa de pesquisa escrever ***"Resolução de problemas"***.
3. Em seguida, clicar em ***"Resolução de problemas"*** e seguidamente ***"Rede e Internet"***,
4. Por último, seleccionar a opção ***"Ligações de internet"*** e, em seguida a opção ***"Seguinte".***

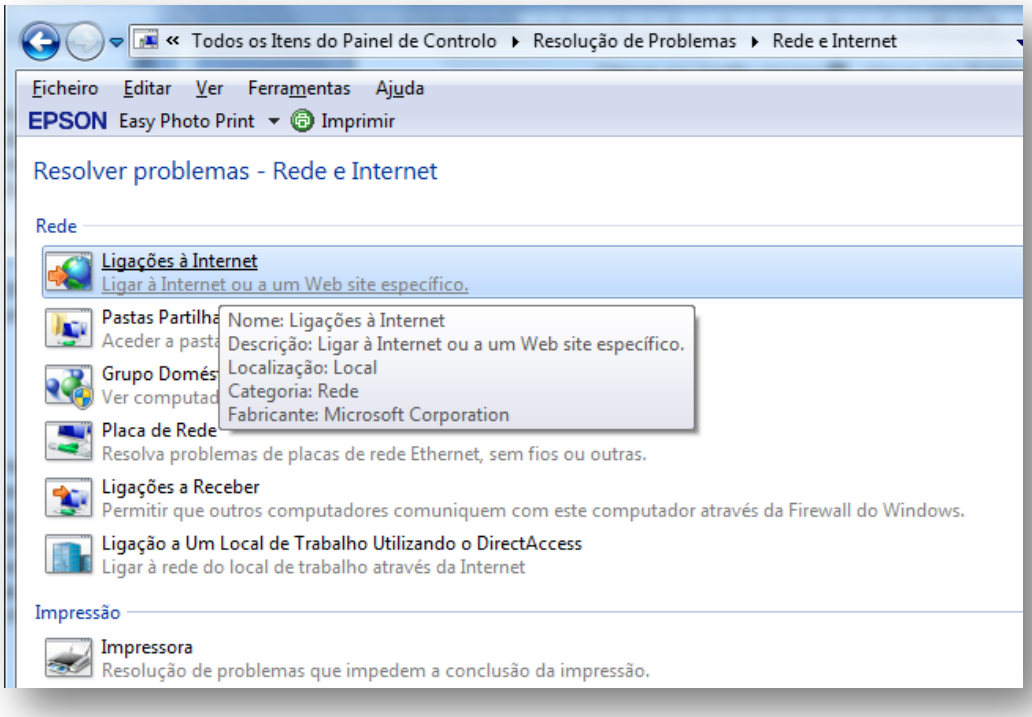



**Figura 140 – Windows Vista – Ecrã de Resolução de problemas.**

#### *10.8.7.2 Linux*

Para ser efectuado a reparação de problemas na rede no SO Linux devem ser executados os seguintes passos:

1 Num terminal, entrar em modo de privilégios de *root* (por exemplo, se for no Ubuntu, digitalizar o comando ***"sudo"*** ou simplesmente ***"sudo dhclient eth0"***) e sem seguida pressionar a tecla [Enter];

2 Seguidamente, digitalizar o comando ***"sudo dhclient eth0"***, e pressionar a tecla [Enter].

**NOTA:** É de referir que a interface eth0 corresponde ao nome da interface LAN. Poderá ser visualizado um endereço IP 192.168.1.x (onde 1 ≤ x <255), caso contrário poderá ser consultado a secção 10.8.6 deste documento.