FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO


FEUP

# Difusão Eficiente de Tráfego Multicast em Redes Emalhadas 802.11 com Suporte de Mobilidade

**Carlos Miguel Gouveia Oliveira**

Dissertação realizada no âmbito do Mestrado Integrado em Engenharia Electrotécnica e de Computadores Major Telecomunicações

Orientador: Prof. Dr. José Ruela

Co-orientador: Eng. Rui Campos

Julho de 2010

U.PORTO

FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

**MIEEC - MESTRADO INTEGRADO EM ENGENHARIA ELECTROTÉCNICA E DE COMPUTADORES** 2009/20010

A Dissertação intitulada

"SOLUÇÃO PARA DIFUSÃO DE TRÁFEGO MULTICAST EM REDES EMALHADAS 802.11 COM SUPORTE DE MOBILIDADE"


foi aprovada em provas realizadas em 19/Julho/2010

o júri

Presidente Professor Doutor Mário Jorge Moreira Leitão
Professor Associado do Departamento de Engenharia Electrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto

Professora Doutora Susana Isabel Barreto de Miranda Sargento
Professora Auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

Professor Doutor José António Ruela Simões Fernandes
Professor Associado do Departamento de Engenharia Electrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto

Licenciado Rui Campos
Investigador do INESC-Porto

O autor declara que a presente dissertação (ou relatório de projecto) é da sua exclusiva autoria e foi escrita sem qualquer apoio externo não explicitamente autorizado. Os resultados, ideias, parágrafos, ou outros extractos tomados de ou inspirados em trabalhos de outros autores, e demais referências bibliográficas usadas, são correctamente citados.

Autor - Carlos Miguel Gouveia Oliveira

Faculdade de Engenharia da Universidade do Porto

# Resumo

A tecnologia 802.11 é, actualmente, uma das principais tecnologias sem fios utilizadas no acesso ubíquo à Internet, em banda larga. As redes emalhadas 802.11 são encaradas como uma solução para aumentar a cobertura, de forma flexível e economicamente eficiente, permitindo responder à crescente procura de acessos 802.11 e ultrapassar as limitações de cobertura associadas a esta tecnologia. Várias soluções têm sido propostas para a criação automática de redes emalhadas 802.11. No entanto, estas tratam o tráfego *multicast* de forma ineficiente, visto que se focam, principalmente, no tráfego *unicast*. A crescente utilização de aplicações com necessidades de difusão de tráfego *multicast* nestas redes torna fundamental o desenvolvimento de soluções mais eficientes no tratamento deste tipo de tráfego.

Nesta dissertação é proposta uma nova solução, simples e eficiente, para a difusão de tráfego *multicast* sobre redes emalhadas 802.11, com suporte de mobilidade, designada WiFIX 2.0 (Wi-Fi Network Infrastructure eXtension, versão 2.0), que tem como ponto de partida a solução WiFIX 1.0. Os resultados experimentais obtidos, recorrendo à implementação da solução proposta e a um *test-bed* laboratorial, comprovam o seu superior desempenho relativamente à solução de referência no contexto das redes emalhadas 802.11, a solução IEEE 802.11s.

# Abstract

Nowadays, 802.11 is a leading tecnology concerning broadband ubiquitous Internet access. With the growing demand for wireless Internet access and the limited 802.11 radio range, 802.11-based Wireless Mesh Networks have been proposed as a flexible and cost-effective solution to extend the radio coverage of existing network infrastrutures. Many solutions have been proposed to create Wireless Mesh Networks automatically. However, these solutions do not deal with multicast traffic efficiently and they are mostly focused on unicast traffic. The development of more efficient solutions for multicast forwarding becomes crucial, namely with the increasing deployment of multicast applications.

We propose a simple and efficient solution to forward multicast traffic over 802.11-based Wireless Mesh Networks, with mobility support, called WiFIX 2.0 (Wi-Fi Network Infrastructure eXtension, version 2.0), which is based on WiFIX 1.0. WiFIX 2.0 was implemented and tested in a laboratorial test-bed. The experimental results obtained show that WiFIX 2.0 outperforms the reference solution for 802.11-based Wireless Mesh Networks, the IEEE 802.11s solution.

# Agradecimentos

Gostaria de agradecer aos meus orientadores, Prof. Dr. José Ruela e Eng. Rui Campos, pela ajuda na realização desta Tese de Mestrado Integrado, no que diz respeito à revisão deste documento. Gostaria, também, de agradecer, em especial, ao Eng. Rui Campos pela constante disponibilidade para o esclarecimento de dúvidas.

O Autor

# Conteúdo

# Lista de Figuras

# Lista de Tabelas

# Abreviaturas e Símbolos

| | |
|---|---|
| ACK | *Acknowledgement* |
| ADMR | *Adaptive Demand-driven Multicast Routing* |
| AP | *Access Point* |
| AR | *Access Router* |
| ATCM | *Active Topology Creation and Maintenance* |
| CAMP | *Core-assisted Mesh Protocol* |
| DHCP | *Dinamic Host Configuration Protocol* |
| DNS | *Domain Name System* |
| Eo11 | *Ethernet-over-802.11* |
| GARP | *Generic Attribute Registration Protocol* |
| GMRP | *GARP Multicast Registration Protocol* |
| HWMP | *Hybrid Wireless Mesh Protocol* |
| ICMPv6 | *Internet Control Message Protocol version 6* |
| IEEE | *Institute of Electrical and Electronics Engineers* |
| IGMP | *Internet Group Management Protocol* |
| INESC | Instituto de Engenharia de Sistemas e Computadores |
| IPTV | *Internet Protocol Television* |
| IPv4 | *Internet Protocol version 4* |
| IPv6 | *Internet Protocol version 6* |
| LAN | *Local Area Network* |
| MAC | *Medium Access Control* |
| MAP | *Mesh Access Point* |
| McB | *Multicast* como *Broadcast* |
| MCT | *Minimum Cost Tree* |
| MLD | *Multicast Listener Discovery* |
| MS | *Multicast* Selectivo |
| MSMob | *Multicast* Selectivo com Suporte de Mobilidade |
| MTU | *Maximu Transmission Unit* |
| ODMRP | *On-demand Multicast Routing Protocol* |
| OSI | *Open Systems Interconnection* |
| QoS | *Quality of Service* |
| RSTP | *Rapid Spanning Tree Protocol* |
| SPT | *Shortest Path Tree* |
| SRMP | *Source Routing-based Multicast Protocol* |
| TR | *Topology Refresh* |
| WiFIX | *Wi-Fi Network Infrastructure Extension* |
| WMN | *Wireless Mesh Network* |

# Capítulo 1

# Introdução

## 1.1 Contextualização

A Internet tornou-se na infra-estrutura de comunicação mais utilizada à escala global, sobre a qual uma miríade de aplicações e serviços estão disponíveis actualmente. Por outro lado, para aceder a essas aplicações e serviços cada vez mais os utilizadores necessitam de acessos de banda larga a qualquer momento e em qualquer lugar. Neste contexto, as redes IEEE 802.11 têm vindo a desempenhar um papel fundamental, permitindo o acesso à Internet sem fios, em banda larga. No entanto, a cobertura de grandes áreas geográficas através da tecnologia IEEE 802.11, sobretudo devido à sua cobertura rádio limitada, poderá implicar a instalação de diversos *Access Points* (APs) ligados através de uma infra-estrutura de rede por cabo. Esta abordagem poderá acarretar custos económicos elevados e força a que a instalação dos APs seja efectuada apenas em locais onde estão disponíveis acessos por cabo a essa mesma infra-estrutura.

Para resolver este problema, foi proposto o conceito de redes emalhadas sem fios, em inglês, Wireless Mesh Networks (WMNs). Numa WMN, os nós de rede cooperam entre si através de um meio de comunicação sem fios, com o objectivo de encaminhar pacotes entre nós de origem e nós de destino, que, em geral, não estão ao alcance rádio. As WMNs permitem, desde logo, uma maior flexibilidade, menor complexidade e uma diminuição dos custos de instalação, visto que os APs estão ligados via rádio. Com base no conceito de redes emalhadas sem fios, foi proposta em [1] uma nova solução denominada WiFIX (*Wi-Fi Network Infrastructure eXtension*), daqui por diante designada WiFIX 1.0. A solução WiFIX 1.0 assenta numa rede constituída por *Mesh Access Points* (MAPs) estáticos (os termos MAP e nó serão usados indistintamente) que têm como função o encaminhamento do tráfego entre os terminais ligados directamente a uma das suas interfaces e a rede infra-estruturada, e vice-versa. Desta forma, considera-se este cenário como sendo uma extensão à infra-estrutura de rede comum.

O crescimento da utilização de aplicações e serviços com perfil *multicast*, como por exemplo IPTV e áudio/vídeo conferência, levou à necessidade, também em redes emalhadas sem fios, de se

definirem mecanismos eficientes para difusão deste tipo de tráfego. Deste modo, propõe-se nesta dissertação, uma solução designada WiFIX 2.0, que consiste numa evolução da solução WiFIX 1.0, introduzindo novos mecanismos para o tratamento do tráfego *multicast*.

## 1.2 Problema

Aplicações e serviços com perfil *multicast* necessitam de mecanismos específicos para difusão deste tipo de tráfego. Com a utilização das redes emalhadas 802.11 como extensão das infra-estruturas, por cabo, existentes, surge a necessidade de difundir tráfego *multicast* entre a rede cablada e os terminais ligados à rede emalhada. Assumindo que os fluxos *multicast* são entregues ao nó directamente ligado à rede infra-estruturada, através de mecanismos existentes, o problema a resolver consiste na entrega desses fluxos, sobre a rede emalhada 802.11, aos terminais móveis que a ela se ligam, independentemente da sua localização em cada momento.

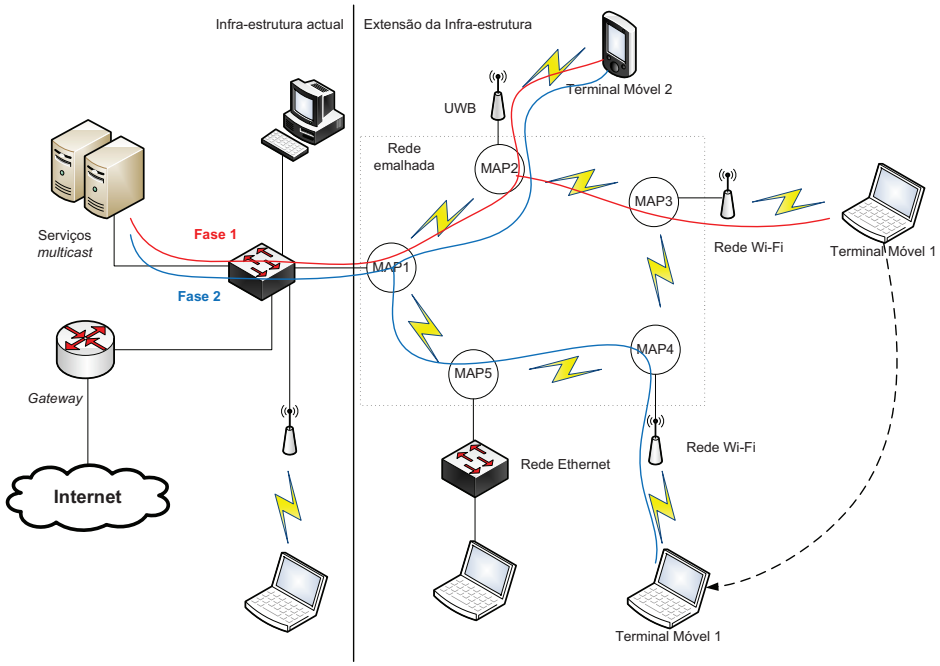



Figura 1.1: Cenário ilustrativo do problema a resolver

A Figura 1.1 pode ser usada como um exemplo concreto para ilustrar o problema a resolver na sua forma mais simples. Neste caso temos um fluxo *multicast* proveniente da infra-estrutura, que deve ser entregue aos terminais móveis (TMs) 1 e 2, tendo em conta a sua localização actual. Na Fase 1, o TM 1 está ligado ao MAP 3 e o TM 2 está ligado ao MAP 2. Portanto, dentro da rede emalhada 802.11 o fluxo *multicast* deverá ser entregue aos MAPs 2 e 3. No cenário apresentado, assume-se que, na Fase 2, o TM 1 se move para outra localização, associando-se ao MAP 4. Nessa altura é necessário redireccionar o fluxo *multicast* para a nova localização do TM 1.

## 1.3 Motivação

Considerando as redes emalhadas sem fios como um meio de acesso à Internet, a necessidade de suporte de aplicações e serviços com perfil *multicast*, implica o desenvolvimento de mecanismos de difusão deste tipo de tráfego. Além disso, a existência de terminais portáteis cada vez mais pequenos e mais facilmente transportáveis promoveu uma tendência dos utilizadores se moverem enquanto acedem à rede, aumentando a necessidade das soluções suportarem mobilidade. Por outro lado, as várias soluções até agora propostas, como por exemplo, a solução IEEE 802.11s, evidenciam algumas deficiências na forma como enfrentaram o problema da difusão do tráfego *multicast* e/ou não suportam mobilidade de terminais.

Os aspectos referidos, a relevância da tecnologia IEEE 802.11 no contexto das tecnologias de acesso sem fios e a existência da solução WiFIX 1.0 como ponto de partida, representaram as principais motivações para este trabalho.

## 1.4 Objectivos

Com o propósito de alargar a solução WiFIX 1.0 proposta em [1], que se foca, especialmente no encaminhamento de tráfego *unicast*, o objectivo desta dissertação é especificar e implementar uma solução para difusão de tráfego *multicast*, em redes emalhados 802.11, com suporte de mobilidade, de forma a garantir melhores níveis de eficiência, quando comparada com as soluções existentes e não implicar alterações nos terminais, permitindo a sua rápida implantação.

## 1.5 Contribuições

Nesta secção são apresentadas as principais contribuições deste trabalho.

### 1.5.1 Especificação da Solução WiFIX 2.0

Uma contribuição importante desta dissertação é a especificação de uma nova solução, simples e eficiente, para difusão de tráfego *multicast* em redes emalhadas 802.11, com o objectivo de permitir a utilização de aplicações e serviços com perfil *multicast* sobre este tipo de redes. As soluções existentes optam por enviar o tráfego *multicast* como *broadcast*, sendo recebido por nós que não o solicitaram. A solução proposta nesta dissertação define um mecanismo de encaminhamento selectivo do tráfego *multicast* e suporta mobilidade de terminais.

### 1.5.2 Implementação da Solução WiFIX 2.0

A implemetação da solução especificada representa uma outra contribuição deste trabalho, o que permite a realização de testes, num cenário real, com o objectivo de se obterem resultados experimentais que a validem. Além disso, poderá servir de base para futuros trabalhos de investigação no âmbito da solução WiFIX 2.0.

### 1.5.3 DHCP *snooping* para Gestão de Mobilidade

A utilização da técnica DHCP *snooping* era, até agora, realizada como meio de controlo de acesso à rede. Neste trabalho, utiliza-se esta técnica no âmbito da gestão de mobilidade de terminais, o que representa, desde logo, uma contribuição inovadora.

## 1.6 Estrutura da Dissertação

Este documento está organizado em seis capítulos. O Capítulo 1 apresenta uma introdução ao trabalho realizado. O Capítulo 2 expõe o estado da arte. o Capítulo 3 especifica a solução WiFIX 2.0. O Capítulo 4 descreve a implementação da solução WiFIX 2.0. O Capítulo 5 apresenta os resultados experimentais obtidos e a correspondente avaliação. No Capítulo 6 são apresentadas as principais conclusões e são apontadas algumas linhas de investigação futura.

# Capítulo 2

# Estado da Arte

Neste capítulo são apresentadas as soluções existentes para resolver parcial ou totalmente o problema da difusão de tráfego *multicast* sobre redes emalhadas sem fios, com suporte de mobilidade de terminais. Será dado especial relevo às soluções IEEE 802.11s e WiFIX 1.0. A primeira é, actualmente, a principal solução para o problema enunciado. A segunda é usada como ponto de partida para a solução proposta nesta dissertação. Em primeiro lugar, são abordados outros conceitos importantes para a compreensão da solução proposta nesta dissertação, nomeadamente o funcionamento das bridges IEEE 802.1D e das técnicas IGMP *snooping* e DHCP *snooping*.

## 2.1 *Bridges* IEEE 802.1D

As *bridges* 802.1D [2] estão actualmente presentes nas *Ethernet* LANs (*Local Area Networks*) e dispõem de um algoritmo de aprendizagem que permite a construção de tabelas de encaminhamento de forma transparente para as estações. Esta tabela associa endereços a portas e cada entrada possui um *lifetime*. Todavia, este mecanismo implica a existência de uma topologia em árvore. Para tal, a norma IEEE 802.1D define o RSTP (*Rapid Spanning Tree Protocol*) [2], que garante o estabelecimento de uma topologia sem *loops*.

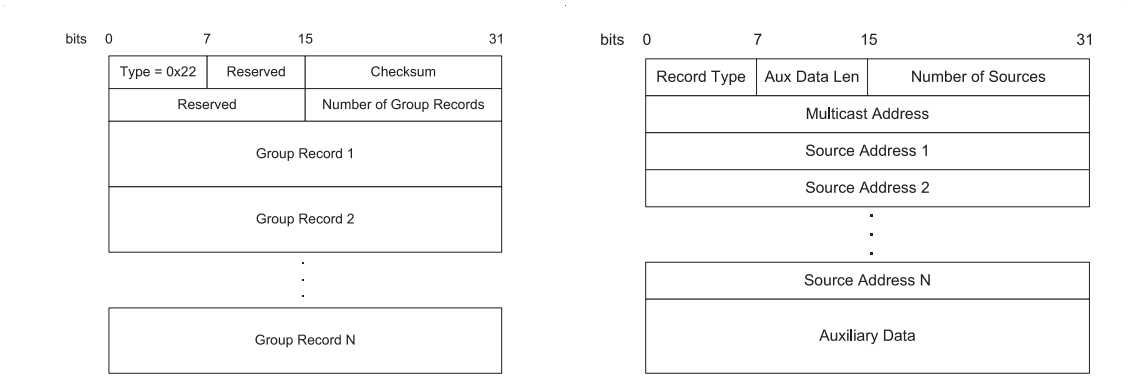
O algoritmo de aprendizagem baseia-se na análise dos endereços de origem das tramas recebidas em cada porta, de modo a aprender a porta associada a cada estação ligada à rede. Aquando da chegada de uma trama numa porta da *bridge*, será consultada a tabela de encaminhamento. Se o endereço de origem da trama não for encontrado, será adicionada uma nova entrada na tabela associando este endereço à porta na qual a trama foi recebida. Se o endereço existir na tabela, mas estiver associado a outra porta, a entrada é actualizada, substituindo a porta antiga pela nova e reinicializado o *lifetime*. Se a informação for igual apenas se actualiza o *lifetime*. Se o *lifetime* de uma entrada da tabela expirar, esta será removida.

O algoritmo de encaminhamento baseia-se na análise dos endereços de destino das tramas recebidas. Aquando da chegada de uma trama numa porta da *bridge*, será consultada a tabela de encaminhamento. Se o endereço de destino não for encontrado, será enviada uma cópia para cada uma das restantes portas. Caso contrário, se existir uma entrada correspondente ao endereço de destino, a trama é encaminhada apenas para a porta especificada. Com este mecanismo, a *bridge* é capaz de saber a localização das várias estações na rede.

Apesar da norma IEEE 802.1D definir protocolos que permitam um tratamento eficiente do tráfego *multicast*, GARP (*Generic Attribute Registration Protocol*) e GMRP (*GARP Multicast Registration Protocol*), na prática estes não são usados. Portanto, na sua forma mais simples, as *bridges* IEEE 802.1D [2], ao receberem uma trama com endereço de destino *multicast*, numa das suas portas, encaminham uma cópia da trama para as portas restantes, como fariam para uma trama com endereço de destino *broadcast*. Contudo, esta abordagem não é a mais eficiente no que diz respeito ao aproveitamento da largura de banda, principalmente quando a trama é pretendida por um pequeno grupo de nós.

## 2.2 IGMP *Snooping*

O protocolo IGMP (*Internet Group Management Protocol*) é usado, em redes IPv4, pelos sistemas para informarem os *routers multicast* sobre associações ou desassociações a grupos. Na versão 3, existem dois tipos de mensagens: IGMP *Query* e IGMP *Report*. As mensagens do tipo IGMP *Query* são enviadas por *routers multicast* de forma a inquirir os sistemas que implementam este protocolo sobre o estado de associação a um ou mais grupos. As mensagens do tipo IGMP *Report* são enviadas pelos sistemas pertencentes a grupos, com o objectivo de informar os *routers multicast* que pretendem receber tráfego relativo a esses mesmos grupos. A Figura 2.1 exemplifica a constituição de uma mensagem IGMP *Report*, assim como a constituição de cada *Group Record* existente na mensagem. Uma mensagem IGMP *Report* pode conter *n Group Records*.




(a) IGMP *Report* (b) *Group Record*

Figura 2.1: Constituição da mensagem IGMP *Report*

Como consequência do funcionamento comum das *bridges* IEEE 802.1D, relativamente ao encaminhamento de tráfego *multicast*, referido na Secção 2.1, surgiu uma nova técnica, designada IGMP *snooping*, para o caso do protocolo da camada de rede usado ser o IPv4; a técnica MLD (*Multicast Listener Discovery*) *snooping* é usada para o IPv6. Os *switches* que implementam este mecanismo servem-se da violação da pilha protocolar do modelo OSI (*Open Systems Interconnection*), inspeccionando cabeçalhos dos níveis superiores, de forma a identificar as mensagens IGMP *Report* enviadas pelas estações. Através destas mensagens, os *switches* conseguem saber em que segmentos da rede estão localizados os elementos pertencentes a cada grupo. Assim, os *switches* têm a possibilidade de construir uma tabela que associe um determinado grupo a um conjunto de portas. Através da consulta desta tabela, aquando da chegada de uma trama com endereço de destino *multicast*, o *switch* realiza o encaminhamento apenas para as portas associadas ao grupo. Esta é a funcionalidade principal da técnica IGMP *snooping* no que concerne ao plano de dados.

Usando o protocolo IGMPv3 [3] como exemplo, o mecanismo de construção das tabelas [4] funciona, de forma resumida, da seguinte maneira:

- Cada *switch* tem que manter uma tabela que associe endereços IP de grupos a portas;
- Quando o *switch* recebe uma mensagem IGMP *Report* de associação numa determinada porta, adiciona ou actualiza (caso já exista) uma entrada na tabela, associando o grupo à porta em questão;
- Cada entrada da tabela tem que possuir um parâmetro *lifetime*, não ficando dependente da recepção de mensagens IGMP *Report* de desassociação para retirar entradas da tabela.

O mecanismo de encaminhamento pode ser, resumidamente, explicado da seguinte forma:

- Um pacote de dados com endereço de destino do tipo 224.0.0.X tem que ser encaminhado para todas as portas;
- Um pacote de dados com endereço de destino *multicast* diferente de 224.0.0.X deve ser encaminhado de acordo com a tabela;
- Caso o endereço de destino do pacote de dados não conste na tabela, o pacote deve ser encaminhado para todas as portas.

Para o caso do protocolo da camada de rede usado ser o IPv6, seria usada a técnica MLD *snooping*, dado que nesse caso é usado o protocolo MLD para associação/desassociação a grupos *multicast*. O funcionamento da técnica MLD *snooping* é semelhante e, assim como o mecanismo explicado acima, pode se consultado no RFC 4541 [4].

## 2.3 DHCP *Snooping*

Quando um terminal chega a uma rede e pretende adquirir configurações de forma dinâmica, começa por difundir uma mensagem DHCP *Discover*. Consoante o número de mensagens

DHCP *Offer* que obtiver como resposta, apercebe-se do número de servidores existentes na rede. A mensagem DHCP *Offer* contém a proposta de cada servidor em termos de parâmetros de configuração. Com base no conjunto de parâmetro definidos nesta mensagem, o terminal selecciona um dos servidores [5]. De seguida, envia um DHCP *Request*, em *broadcast*, indicando o servidor escolhido. Esta mensagem serve, também, para notificar os outros servidores que as suas ofertas foram declinadas. Por fim, o servidor escolhido envia uma mensagem DHCP *ACK* com os parâmetros de configuração efectivos, incluindo o endereço IP atribuído ao terminal, finalizando, assim, a troca de mensagens.

O DHCP *snooping* é uma técnica utilizada por alguns *switches* para inspeccionar as mensagens DHCP, que é, normalmente, utilizada para fins de controlo de acesso à rede. Esta técnica permite aos *switches* facultar/negar o acesso à rede a uma determinada estação com um determinado endereço IP e um determidado endereço MAC numa determinada porta. Esta filtragem é realizada com base numa tabela, presente em cada *switch* que associa endereços IP e MAC a portas, funcionando como uma *whitelist*.

Para uma descrição completa do funcionamento do protocolo DHCP, sugere-se a consulta das respectivas normas [5] [6].

## 2.4 IEEE 802.11s

O *draft* IEEE 802.11s define uma solução para encaminhamento de tráfego em redes emalhadas 802.11, como extensão à rede infra-estruturada (Figura 1.1). Para este cenário, o *draft* IEEE 802.11s define um protocolo de *routing*, utilizado por omissão, designado HWMP (*Hybrid Wireless Mesh Protocol*), que é usado para construção de uma topologia em árvore. Este protocolo permite a construção de tabelas de encaminhamento em cada MAP. É definido um nó com funções especiais (*root* MAP) que se encontra directamente ligado à rede infra-estruturada. Esta solução também endereça o problema referido nesta dissertação (Secção 1.2). A forma como é transmitido o tráfego *multicast* baseia-se no mecanismo de *flooding* puro. Deste modo a mobilidade de terminais é suportada intrinsecamente, uma vez que todos os nós da rede recebem o tráfego destinado a um determinado grupo. Apesar deste mecanismo possuir alguma fiabilidade e simplicidade, em termos de eficiência não é a melhor solução, visto que cada nó da rede, após receber uma trama com o endereço de *broadcast* no campo de destino, vai retransmiti-la para o meio sem fios, o que fará com que os nós a possam receber mais do que uma vez. Isto provoca uma ocupação desnecessária do meio.

A solução IEEE 802.11s é usada como referência, nesta dissertação, uma vez que a respectiva norma se encontra em fase de pré-ratificação, sendo, neste momento a solução mais relevante no contexto das redes emalhadas 802.11.

## 2.5 WiFIX 1.0

Em [1], Rui Campos et al. propõem uma solução (WiFIX 1.0) para redes emalhadas sem fios, como extensão à rede infra-estruturada, baseada nas *bridges* IEEE 802.1D e num mecanismo de auto-organização da rede assente num protocolo de mensagem única. Um dos objectivos desta solução é a reutilização de princípios e ferramentas usados nas redes cabladas, aplicando-os agora às redes emalhadas 802.11.

Esta solução foi desenvolvida a pensar, principalmente, no encaminhamento de tráfego *unicast*, apesar de também especificar um mecanismo de difusão de tráfego *broadcast*. Este mecanismo introduz uma melhoria em relação ao da solução IEEE 802.11s. Apenas os nós com mais do que um vizinho reencaminham tramas *broadcast*. Desta forma, há uma redução do número total de tramas na rede para transmitir a mesma informação. No entanto, a solução WiFIX 1.0 não especifica qualquer solução para o tratamento do tráfego *multicast*. Este é, simplesmente, tratado como tráfego *broadcast*.

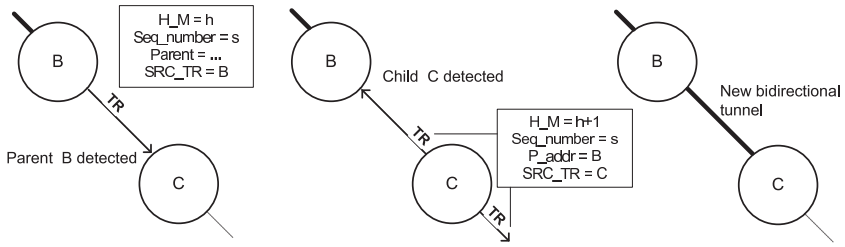



Figura 2.2: Estabelecimento de *links* virtuais no WiFIX 1.0 [1]

O WiFIX 1.0 introduz dois processos fundamentais: o mecanismo de criação de uma árvore com raiz no *master* MAP (nó directamente ligado à rede de infra-estrutura), que representa a topologia activa da rede emalhada sem fios, e a definição de um novo tipo de encapsulamento designado *Ethernet-over-802.11* (Eo11), que permite a criação de *links* virtuais (ou túneis Eo11) sobre o meio 802.11, usados no encaminhamento dos tramas *unicast*. Do ponto de vista das *bridges*, as entradas e saídas dos túneis Eo11 criados são portas lógicas, permitindo a utilização do mecanismo de aprendizagem referido na Secção 2.1. Nas subsecções seguintes, são apresentados, com mais detalhe, os dois processos referidos.

### 2.5.1 *Active Topology Creation and Maintenance*

O mecanismo usado para criar uma árvore com raiz no *master* MAP designa-se *Active Topology Creation and Maintenance* (ATCM) e baseia-se num protocolo de mensagem única (*Topology Refresh*, TR). Esta mensagem é enviada periodicamente pelo *master* MAP e encaminhada por todos os outros MAPs, após actualização dos parâmetros necessários (número de *hops*, endereço do nó pai, *time-to-live* e endereço de origem da própria trama). O mecanismo ATCM permite não só o anúncio do *master* MAP mas também informar um determinado nó que foi escolhido como pai por um nó vizinho. Além disso, permite, desde logo, o estabelecimento de túneis Eo11, que, conceptualmente, são *links* virtuais, entre um pai e os respectivos filhos (Figura 2.2). O critério pelo qual cada nó escolhe o seu pai na árvore topológica é o número mínimo de *hops* até ao *master* MAP.

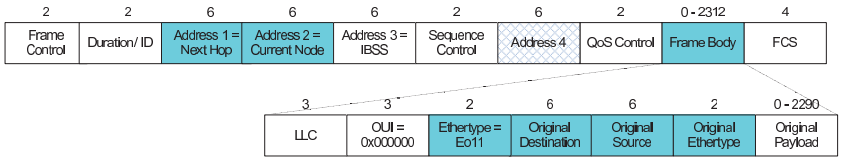



Figura 2.3: Encapsulamento das tramas de dados usado no WiFIX 1.0 [1]

### 2.5.2 Encapsulamento Eo11

Na solução WiFIX 1.0 foi adoptado um mecanismo de encapsulamento que permite a introdução de quatro endereços MAC nas tramas (endereço de origem, endereço de destino, endereço de origem intermédio e endereço de destino intermédio), de forma a permitir o encaminhamento *multi-hop* (Figura 2.3). Para isso, foi criado um novo cabeçalho constituído por dois endereços MAC e um novo *Ethertype*. Deste modo, o cabeçalho interior é preenchido com os endereços MAC e o *Ethertype* originais e o cabeçalho exterior com os endereços MAC do *next hop* (endereço de destino intermédio) e do *current node* (endereço de origem intermédio), assim como o *Ethertype* correspondente ao encapsulamento Eo11. Os MAPs intermédios processam e

alteram o cabeçalho exterior, possibilitando o encaminhamento das tramas de dados através da árvore criada, sem nunca alterar os endereços de origem e destino.

Para uma descrição mais detalhada sugere-se a consulta do artigo referenciado em [1].

## 2.6 Protocolos de *Routing Multicast*

Existem várias propostas de protocolos de *routing* que privilegiam diferentes aspectos a considerar aquando do planeamento de uma rede emalhada sem fios. Em [7] [8] [9] são propostos protocolos de *routing* para *multicast mesh-based* ao contrário de outras soluções que são *tree-based*, como por exemplo o protocolo proposto em [10]. Os protocolos *mesh-based* são mais robustos, visto que existe maior número de caminhos possíveis e suportam mobilidade entre nós, que no caso do WiFIX são os MAPs.

Em [7], Sung-Ju Lee et al. propõem o protocolo ODMRP (*On-demand Multicast Routing Protocol*), desenvolvido para redes móveis sem fios, que tem como objectivos principais, diminuir o *overhead* e melhorar a escalabilidade. O protocolo ODMRP introduz o conceito de *forwarding group* que é o conjunto de nós responsável por encaminhar tráfego *multicast* pelos caminhos de custo mínimo entre todos os elementos de um determinado grupo. O facto de ser *mesh-based* torna-o robusto a falhas nas ligações, não sendo necessário enviar pacotes de controlo aquando dessas falhas, uma vez que existe mais do que um caminho entre dois nós.

Em [9], os mesmos autores propõem melhorias ao ODMRP, nomeadamente em questões relacionadas com alterações na topologia da rede, referindo um mecanismo de previsão de mobilidade dos nós. Propõem, ainda, formas de diminuir a latência e aumentar a fiabilidade das transmissões, mais concretamente o uso de *acknowledgements* e retransmissões.

Em [8] é introduzido o primeiro protocolo de *routing multicast mesh-based* desenvolvido para redes ad-hoc, CAMP (*Core-assisted Mesh Protocol*). Desta forma, possui algumas das características referidas no artigo anterior. No entanto, não prevê o suporte de mobilidade dos nós. O objectivo de [8] é mostrar que é possível criar estruturas de *routing* para comunicações multiponto mais resilientes que as árvores, ou seja, pretende mostrar que uma estrutura *mesh-based* é melhor que uma *tree-based*.

Outro protocolo de *routing multicast* é proposto em [11], SRMP (*Source Routing-based Multicast Protocol*). É mais um protocolo *mesh-based* e providencia novos mecanismos para reduzir a complexidade das tarefas de *routing* e melhorar a performance em termos de atraso. Em relação aos protocolos referidos em [7] e [10], o esquema proposto neste artigo produz melhores resultados ao nível do *overhead*, visto que evita o envio periódico de mensagens de controlo. Para o cenário assumido para este trabalho, em que os MAPs são nós estáticos, estas soluções introduzem apenas complexidade desnecessária.

Em [10], é proposto mais um protocolo de *routing multicast*, ADMR (*Adaptive Demand-driven Multicast Routing*). O objectivo principal é reduzir as componentes de sinalização proactivas, algo que está presente na maioria dos protocolos, até à altura propostos. Desta forma, não possui mecanismos de inundação periódica da rede e possibilita o estabelecimento e

manutenção de rotas de forma dinâmica. O protocolo foi desenhado para redes ad-hoc e torna-se necessário introduzir alterações em todos os nós, o que contraria um dos princípios fundamentais deste trabalho que é o facto de não ser necessário efectuar alterações nas estações mas apenas nos MAPs.

Em [12] é proposta uma solução para *routing multicast* com suporte de QoS (*Quality of Service*), em redes emalhadas sem fios. Esta solução tem como base a existência de um protocolo *mesh-based* nos *routers* do *backbone* e um protocolo *tree-based* entre os *routers* da periferia e as estações. O objectivo é eliminar o atraso no estabelecimento de rotas no *backbone* e minimizar o *overhead*, fazendo com que as rotas entre as estações e os *routers* da periferia sejam estabelecidas *on-demand*. De qualquer forma, esta solução afasta-se do nosso cenário, uma vez que explicita uma topologia com *backbone* e periferia.

Pedro M. Ruiz et al. propõem em [13] um esquema *tree-based*, baseado no conceito de *prefix continuity*, introduzido por Jelger et al. em [14]. Esta solução visa a obtenção de uma redução do *overhead* em comparação com protocolos de *routing* tradicionais. Tal como na solução proposta neste trabalho, um dos objectivos da solução descrita em [13] é evitar a necessidade de alterações nos terminais. No entanto, o facto de ser uma abordagem ao nível da camada de rede, requer a definição de um mecanismo de auto-configuração de endereços IP.

Em [15] é apresentada uma comparação entre duas diferentes abordagens ao *routing multicast* em redes emalhadas sem fios: SPTs (*Shortest Path Trees*) e MCTs (*Minimum Cost Trees*). As métricas usadas para avaliar estes dois tipos de árvores de *routing* foram: a taxa de pacotes entregues, o atraso, o *jitter*, o *overhead* e o *throughput*. Em [15] conclui-se que uma abordagem do tipo SPT traz mais vantagens relativamente às MCTs, visto que a rede apresenta melhor performance ao nível da maioria das métricas acima referidas, embora as SPTs introduzam maior *overhead*. A desvantagem mais significativa das SPTs tem a ver com a existência de grupos *multicast* muito grandes. Por exemplo, se numa rede com 300 nós existirem grupos com mais de 100 membros, a perda de pacotes de fluxos concorrentes é maior do que no caso das MCTs. Contudo, de uma forma geral, as SPTs são a abordagem mais apropriada para o *routing multicast* em redes emalhadas sem fios.

## 2.7 Mobilidade

Considerando o conceito de redes ad-hoc sem fios, é descrito em [16] um mecanismo de previsão de mobilidade de nós. O objectivo pretendido é antecipar mudanças de topologia da rede, estabelecendo novas rotas antes da quebra de conectividade. Esta é mais uma solução que assenta num cenário diferente daquele que serve de base ao WiFIX. Da mesma forma que acontece em casos anteriores, traria complexidade desnecessária, visto que os MAPs da solução WiFIX são estáticos. A mobilidade dos nós da rede é uma questão que não se coloca no âmbito desta dissertação.

Em [17] é proposto um esquema de gestão de mobilidade para redes emalhadas sem fios baseado num protocolo de *routing* híbrido. Além de prever mobilidade intra-domínio e inter-domínio, a solução proposta usa um protocolo que funciona ao nível da camada de ligação de dados e da camada de rede para encaminhar pacotes e facilitar o *handover*. O cenário de funcionamento considera que os nós da rede são dispositivos de nível três, chamados *Access Routers* (ARs). O esquema baseia-se no seguinte princípio: quando se inicia o *handover*, o terminal envia para o novo AR um pedido de associação, no qual são transmitidos o seu endereço MAC e o seu endereço IP. Após a recepção desta mensagem o AR associa estes endereços na sua tabela de ARP e envia como resposta uma mensagem de confirmação do pedido. Se existir alguma ligação entre a estação em causa e uma outra durante o *handover*, esta envia uma mensagem de ARP gratuita indicando o endereço MAC do novo AR. De seguida, a estação envia um pedido de desassociação para o antigo AR, com o endereço MAC do novo. Desta forma, pode ser criado um túnel temporário entre os dois ARs para o envio de pacotes que entretanto cheguem ao antigo AR. Esta solução prevê um período em que a estação comunica com os dois ARs em simultâneo.

## 2.8 Conclusão

Em suma, existem várias soluções para difusão de tráfego *multicast* em redes sem fios. No entanto, todas elas apresentam algumas lacunas. A solução proposta pelo IEEE 802.11s [18] propõe um mecanismo pouco eficiente, as soluções [7] [8] [9] [11] [12] [13] [16] introduzem demasiada complexidade para o cenário que estamos a abordar, a solução [10] implica realizar alterações nas estações e a solução [17] é direccionada para tráfego *unicast*. Assim, verifica-se a necessidade de uma nova solução como a que é proposta neste trabalho.

# Capítulo 3

# Especificação da Solução WiFIX 2.0

A utilização de redes emalhadas sem fios tem-se revelado um recurso para estender a rede cablada comum, de forma a abranger uma área geográfica maior, facultando o acesso à Internet, em banda larga, a um maior número de utilizadores. Tal como discutido no Capítulo 2, surgiram, neste contexto, várias soluções com o objectivo de permitir o encaminhamento de tráfego em redes emalhadas sem fios, entre as quais a WiFIX 1.0 proposta em [1]. No entanto, a grande maioria destas soluções apenas se focou na eficiência do transporte de tráfego *unicast*, incluindo a solução WiFIX 1.0.

A partir deste pressuposto, surge, neste trabalho, uma solução, designada WiFIX 2.0, que visa garantir maior eficiência no transporte de tráfego *multicast* que as soluções até agora desenvolvidas, suportando a mobilidade de terminais. O WiFIX 2.0 representa uma evolução da solução WiFIX 1.0.

Herdando os princípios de funcionamento do WiFIX 1.0, a solução aqui proposta usa conceitos sólidos e bem conhecidos das redes por cabo, como as *bridges* IEEE 802.1D para encaminhamento das tramas e um protocolo de mensagem única que permite a auto-configuração da rede. Além disso, reutiliza, também, o mecanismo de *tunnelling* definido no WiFIX 1.0, designado *Ethernet-over-802.11* (Eo11), para o encapsulamento das tramas transportadas dentro da rede emalhada 802.11.

O desenvolvimento da solução WiFIX 2.0 foi dividido em três grandes fases. Na primeira fase, propôs-se tratar todo o tráfego *multicast* como tráfego *broadcast*, embora de uma forma diferente do que acontece na solução IEEE 802.11s. No WiFIX 2.0 são utilizados os túneis Eo11 também para o transporte do tráfego *multicast/broadcast*, criados no WiFIX 1.0 exclusivamente para o encaminhamento do tráfego *unicast*. Desta forma, o tráfego *multicast* chega a todos os nós da rede, independentemente de pertenceram, ou não, ao grupo de destino. Embora este mecanismo já evidencie, desde logo, algumas vantagens, como se verá mais a frente, nesta dissertação, caminhou-se para uma solução ainda mais eficiente. Assim, numa segunda fase do trabalho, desenvolveu-se um novo mecanismo em que o tráfego *multicast* para um determinado

grupo apenas é enviado para nós pertencentes a esse mesmo grupo[1]. Por fim, na terceira fase, pretendeu-se suportar a mobilidade de terminais, que na primeira solução estava intrinsecamente presente, mas na segunda não inerentemente suportada. Com isto, um terminal é capaz de se associar a um novo MAP e readquirir o fluxo *multicast*, minimizando a perda de tramas.

A Figura 1.1 ilustra o cenário para o qual a solução WiFIX 2.0 está optimizada, ou seja, a fonte *multicast* encontra-se na Internet e todo o tráfego entra na rede emalhada através do *master* MAP.

Ao longo deste capítulo é realizada uma descrição pormenorizada do funcionamento da solução WiFIX 2.0. O capítulo está dividido em três secções, de acordo com as fases do trabalho, acima referidas. Em cada uma das fases considerou-se a especificação de um mecanismo que assenta no mecanismo proposto na fase anterior, segundo uma abordagem modular. A Figura 3.1 apresenta os três modulos desenvolvidos, que são descritos nas secções que se seguem.

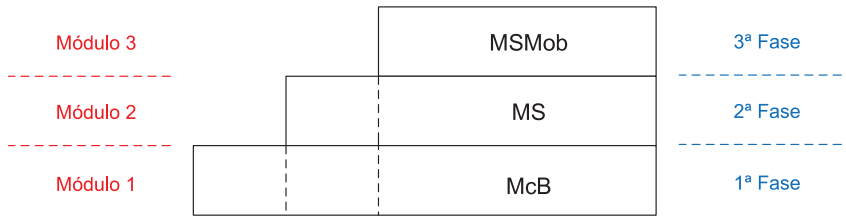



Figura 3.1: Módulos desenvolvidos nas diferentes fases do trabalho

## 3.1 *Multicast* como *Broadcast*

Uma vez que a solução WiFIX 1.0 definia túneis entre MAPs vizinhos para o envio de tramas *unicast*, considerou-se numa primeira fase a possibilidade do envio de tramas *broadcast* através desses mesmos túneis. Este mecanismo foi designado *Multicast* como *Broadcast* (McB). Após uma análise desta hipótese, verificou-se que este método traria algumas vantagens relativamente à solução proposta pelo IEEE 802.11s. Em primeiro lugar, o envio de tramas *broadcast* está

[1]Considera-se que um nó da rede emalhada pertence a um grupo quando tem terminais a si directamente ligados que pertençam a esse mesmo grupo.

especificado, nas redes IEEE 802.11, como sendo realizado ao débito mínimo para a respectiva norma (802.11a/b/g). Ora, ao encapsulá-las em tramas *unicast* (Figura 3.2), existe, desde logo, a possibilidade de envio ao débito máximo permitido pelas condições de utilização, no melhor caso 54 Mbit/s para as variantes IEEE 802.11a e IEEE 802.11g e 11 Mbit/s para a variante IEEE 802.11b. Em segundo lugar, para a solução IEEE 802.11s, a difusão de tráfego *broadcast* é realizada através dum mecanismo em que todos os nós da rede reenviam, uma vez, uma trama recebida, o que faz com que um nó ao alcance rádio de *n* nós, receba *n* tramas iguais. Esta redundância torna a solução mais robusta, mas implica o aumento de tráfego na rede. Contudo, na solução WiFIX 2.0, ao enviar as tramas encapsuladas em *unicast*, tira-se proveito do mecanismo de confirmação de recepção, oferecido pela camada MAC do IEEE 802.11, para garantir fiabilidade.

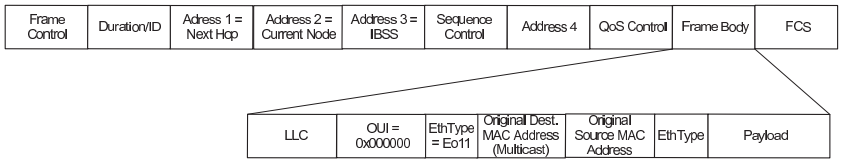



Figura 3.2: Exemplo do encapsulamento usado no WiFIX 2.0

Como foi referido, anteriormente, pretende-se, nesta primeira fase, enviar as tramas *multicast* em *broadcast*. A diferença para a solução 802.11s está na forma como é enviado o tráfego *broadcast*. O encaminhamento de tramas *broadcast* é realizado de forma simples e baseado no mecanismo de difusão das *bridges* 802.1D. Um nó recebe um trama *broadcast* na interface de rede 802.11, retira-lhe o cabeçalho correspondente ao encapsulamento Eo11 e entrega-a na porta da *bridge* correspondente ao respectivo vizinho. A *bridge* vai enviar a trama para todas as portas, que neste caso são as entradas/saídas dos túneis Eo11, excepto aquela onde recebeu. Cada uma destas tramas será encapsulada em *unicast* (Figura 3.2) e enviada para cada um dos vizinhos desse nó. Desta forma, não existe um *flooding* puro da rede, mas uma difusão sobre a árvore criada através do mecanismo ATCM definido na solução WiFIX 1.0, como ilustra a Figura 3.3.

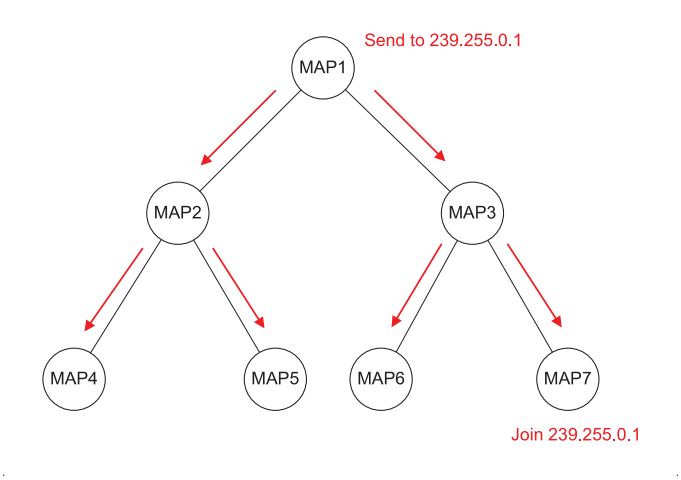



Figura 3.3: *Multicast* como *broadcast*

## 3.2 *Multicast* Selectivo

Com o objectivo de tornar a solução WiFIX 2.0 mais eficiente e mais vantajosa, desenvolveu-se um mecanismo de criação de uma árvore de grupos *multicast*, possibilitando o encaminhamento selectivo das tramas com destino aos elementos de um determinado grupo (Figura 3.4). Este mecanismo é designado *Multicast* Selectivo (MS) e representa uma evolução do mecanismo McB. Esta designação advém do facto de cada nó seleccionar os vizinhos para os quais pretende enviar as tramas *multicast*. O mecanismo MS permite libertar alguns ramos da árvore para transportarem tráfego relativo a outros fluxos, que também competem pelos recursos da rede. Numa rede cablada significaria não enviar tráfego *multicast* para determinados segmentos da rede mas, no cenário em que assenta este trabalho, isto significa enviar um menor número de tramas, ocupando o meio sem fios durante um menor período de tempo e poupando, dessa forma, largura de banda. O mecanismo desenvolvido divide-se em duas etapas: uma etapa de construção das tabelas de grupos *multicast* e uma etapa de encaminhamento de tramas *multicast*. A técnica utilizada para a primeira fase é conhecida como IGMP *snooping* para o caso do uso do protocolo IPv4 ou MLD *snooping* para o IPv6. Cada nó examina as mensagens IGMP *Report* trocadas entre os terminais e os *routers multicast*, com o objectivo de saber através de que vizinhos é que são alcançáveis terminais pertencentes a um determinado grupo. Considerando que o protocolo usado é o IGMP na versão 3, o procedimento de aprendizagem funciona da seguinte forma:

- Quando um terminal deseja receber tráfego pertencente a um determinado grupo, envia uma mensagem IGMP *Report*, com destino aos *routers multicast* demonstrando essa intenção;

- Aquando da passagem de uma trama contendo um IGMP *Report* referente a uma associação a um determinado grupo, cada MAP cria uma nova entrada na tabela de grupos com os seguintes parâmetros: endereço IP do grupo, o endereço MAC do vizinho do qual recebeu a trama e um *lifetime* que indica o tempo de vida da entrada. Caso essa entrada já exista, o

MAP apenas actualiza a lista de endereços MAC dos vizinhos. O parâmetro *lifetime* deve ser superior ao intervalo de envio de mensagens IGMP *Query* e deve ser refrescado cada vez que um IGMP *Report* de associação ao grupo seja encaminhado pelo MAP;

- Aquando da passagem de uma trama contendo um IGMP *Report* referente a uma desassociação a um determinado grupo, o MAP remove o endereço MAC do vizinho do qual recebeu a trama na entrada da tabela correspondente ao grupo em questão e, caso seja único, remove a entrada da tabela;
- Após a actualização da tabela, o MAP encaminha a trama de acordo com o mecanismo adequado para tramas com endereço de destino *multicast*, que será descrito em seguida.

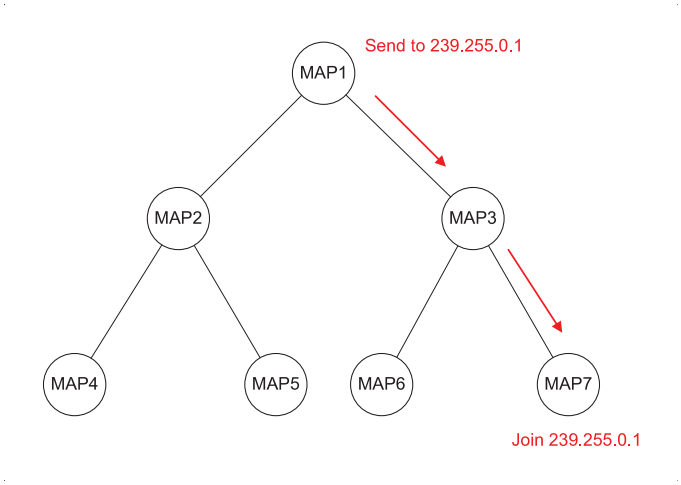



Figura 3.4: *Multicast* selectivo

Desta forma, com a aprendizagem de todos os nós da rede emalhada, é construída uma sub-árvore por cada grupo, sobre a árvore anteriormente criada pelo mecanismo ATCM. Note-se que, no caso limite, em que todos os MAPs têm associados terminais pertencentes a um determinado grupo, esta árvore coincidirá com a árvore criada pelo mecanismo ATCM.

No que diz respeito à fase de encaminhamento, aquando da recepção de uma trama com endereço de destino *multicast*, cada MAP procede da seguinte forma:

- Caso o endereço MAC de destino seja o correspondente a um endereço IPv4 *multicast* do tipo 224.0.0.X, a trama *multicast* é encaminhada para todos os vizinhos menos para aquele do qual a recebeu, tal como se tratasse de uma trama *broadcast*;
- Para todos os outros endereços, cada MAP consulta a tabela de grupos e, caso exista uma entrada correspondente ao grupo, encaminha a trama apenas para os vizinhos cujos endereços MAC estejam associados a essa entrada da tabela;
- Caso não exista a entrada na tabela de grupos correspondente ao endereço de destino do pacote IPv4, a trama correspondente é descartada.

Para o caso do IPv6, tanto o mecanismo de aprendizagem como o de encaminhamento são semelhantes aos do IPv4. As diferenças que se podem encontrar têm a ver com o facto dos MAPs terem que inspeccionar as mensagens de MLD [19] que estão definidas no âmbito do protocolo ICMPv6 (*Internet Control Message Protocol, version 6*) [20] e com o facto da estrutura dos endereços ser diferente, o que leva a que, por exemplo, uma trama que transporte um pacote com o endereço de destino FF02::1 deva ser difundida para todos os vizinhos menos para aquele do qual a recebeu.

## 3.3 *Multicast* Selectivo com Suporte de Mobilidade

A solução WiFIX 2.0 tem, também, como objectivo suportar a mobilidade de terminais. O mecanismo McB, desenvolvido na primeira fase, suporta intrinsecamente a mobilidade de terminais, uma vez que o tráfego *multicast* destinado a um determinado grupo chega a todos os nós, independentemente do MAP ter ou não associados terminais pertencentes a esse mesmo grupo. Assim, o terminal ao deslocar-se de um MAP para outro, readquiriria o fluxo *multicast*, sem quaisquer mecanismos adicionais. No caso do mecanismo MS, quando o terminal muda de MAP, o tempo de reaquisição do fluxo fica dependente do intervalo de tempo entre mensagens IGMP *Query*, uma vez que, apenas aquando da recepção desta mensagem, o terminal enviaria uma mensagem IGMP *Report* que permitiria o refrescamento das tabelas de grupos dos MAPs. O aumento deste intervalo de tempo provoca um consequente aumento do número de tramas perdidas, por parte do terminal, relativas a um fluxo *multicast* que esteja a receber no momento em que muda de MAP. Esta situação implica a necessidade de se desenvolver uma forma de acelerar o processo de reaquisição do fluxo *multicast*. Desta forma, na terceira fase do trabalho, desenvolveu-se um novo mecanismo, designado *Multicast* Selectivo com Suporte de Mobilidade (MSMob), assente no mecanismo MS. No mecanismo MSMob, assim que um terminal, pertencente a um ou mais grupos, se associa a um novo MAP, é forçado a enviar uma nova mensagem IGMP *Report* de associação a esses mesmos grupos, com o objectivo de refrescar imediatamente as tabelas de grupos dos MAPs. A técnica subjacente a este mecanismo designa-se DHCP *snooping* e, até agora, a sua utilização mais comum prende-se com questões de segurança, nomeadamente no controlo de acesso à rede.

Numa rede sem fios, principalmente com suporte de mobilidade, a configuração manual dos terminais, no que respeita por exemplo, ao endereço IP, *default gateway* e endereço(s) de servidor(es) DNS (*Domain Name System*) [21] [22], não faz sentido. Assim, é fundamental a existência de soluções que permitam a configuração automática deste parâmetros. A solução de configuração automática mais utilizada actualmente é o protocolo DHCP.

Quando um terminal se associa a um novo MAP, corre um cliente DHCP, para obter do servidor DHCP, disponível na rede, os parâmetros de configuração necessários. Tendo em conta que um dos objectivos deste trabalho é evitar alterações nos terminais, o mecanismo de suporte de mobilidade na solução MSMob funciona da seguinte forma:

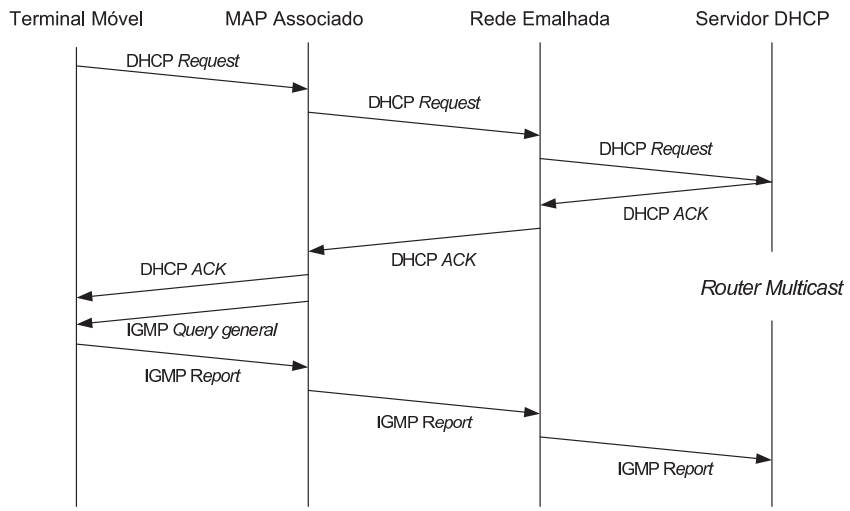



Figura 3.5: Troca de mensagens para o mecanismo MSMob

- Aquando da passagem de uma trama que transporte uma mensagem DHCP *Request*, o MAP ao qual o terminal se encontra associado cria uma entrada numa tabela de mobilidade com os seguintes parâmetros: endereço MAC do terminal, *transaction ID* relativo ao pedido DHCP e um *lifetime*;

- Aquando da passagem de uma trama que transporte uma mensagem DHCP *ACK*, o MAP ao qual o terminal se encontra associado faz uma pesquisa na tabela de mobilidade, usando como chave primária o parâmetro *transaction ID*. Caso exista uma entrada correspondente, envia uma mensagem IGMP *Query general* para o terminal, de forma a forçá-lo a enviar uma mensagem IGMP *Report* de reassociação aos grupos aos quais pertence. A mensagem IGMP *Query general* é enviada em *unicast* ao nível MAC, para que apenas seja recebida pelo terminal que acabou de se associar ao MAP. Além disso, a entrada da tabela é removida. Caso não exista na tabela uma entrada correspondente, a mensagem IGMP *Query general* não é enviada;

- As tramas contendo mensagens DHCP são encaminhadas de acordo com o funcionamento da solução WiFIX 2.0 para os respectivos endereços MAC de destino.

A troca de mensagens decorrente do mecanismo referido nesta secção está representada na Figura 3.5.

Embora algumas aplicações, ao se aperceberem do estabelecimento de uma nova ligação IP, despoletem o envio automático de uma mensagem IGMP *Report*, isto não é um procedimento generalizado, uma vez que nem sequer está definido na norma IGMP [3]. A solução apresentada nesta secção permite a reaquisição do fluxo *multicast*, após mobilidade, para todas as aplicações.

# Capítulo 4

# Implementação da Solução WiFIX 2.0

Neste capítulo descreve-se a implementação da solução WiFIX 2.0, dando especial relevo a aspectos críticos para o seu funcionamento.

A solução WiFIX 2.0 foi desenvolvida para o sistema operativo Linux, sobretudo porque a implemetação da solução WiFIX 1.0 existente também tinha sido realizada para este sistema operativo. Além disso, existe, para Linux, *software* que permite a implementação de uma *bridge* IEEE 802.1D, assim como ferramentas para criação de interfaces virtuais, que são necessárias para o funcionamento da solução. O *daemon* WiFIX2[1] situa-se, conceptualmente, entre as interfaces virtuais (*taps*) e a interface de rede IEEE 802.11, como se ilustra na Figura 4.1. Numa abordagem mais generalizada, o funcionamento do *daemon* WiFIX2 baseia-se na leitura de tramas que chegam a uma interface virtual, processamento e escrita na interface de rede 802.11, ou utilizando o mesmo procedimento em sentido contrário. Neste capítulo, será explicado o processamento das tramas *multicast* e *broadcast* realizado pelo *daemon* WiFIX2.

Uma *tap*, em termos de implementação, actua como sendo uma entrada ou saída de um túnel Eo11 estabelecido entre MAPs vizinhos e, do ponto de vista das camadas superiores, funciona como um dispositivo *Ethernet* de nível 2.

Uma trama que chega ao *daemon* WiFIX2, através de uma *tap*, possui um cabeçalho *Ethernet* com os endereços MAC de origem e destino. Consoante o tipo de endereço MAC de destino, o WiFIX2 irá processá-la, em conformidade, encapsulá-la com o cabeçalho Eo11 e enviá-la para a interface de rede 802.11. No sentido contrário, ou seja, quando uma trama de dados é recebida na interface de rede 802.11, o WiFIX2 começa por verificar se o endereço MAC de origem do cabeçalho Eo11 (*current node*) corresponde a um vizinho. Se esta condição se verificar, será retirado, à trama, o cabeçalho Eo11, e será entregue na *tap* associada ao vizinho do qual a recebeu. Caso contrário, a trama será descartada. Após a entrega numa das *taps*, o encaminhamento será realizado de acordo com o funcionamento das *bridges* IEEE 802.1D. Além das *taps*, a *bridge* pode conter outras interfaces, fazendo com que, por exemplo, uma trama que chegue a uma *tap*

[1] Este termo será utilizado ao longo deste capítulo para distinguir relativamente à solução WiFIX 1.0

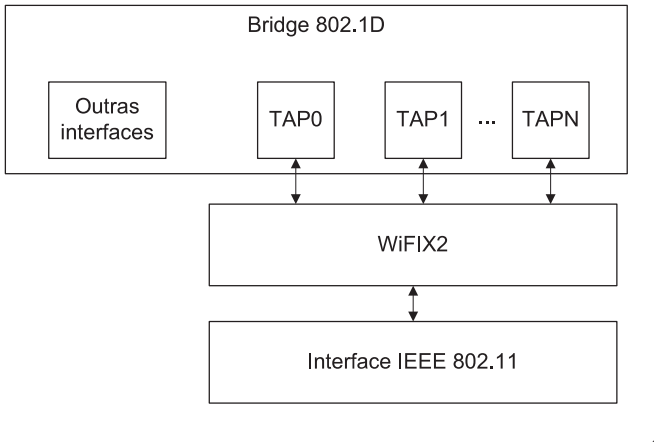



Figura 4.1: Modelo conceptual da implementação da solução WiFIX 2.0

com endereço MAC de destino *broadcast* seja encaminhada para todas as interfaces pertencentes à *bridge*. Se a trama recebida na interface de rede contiver uma mensagem *Topology Refresh* (TR), não haverá encaminhamento para as *taps*, uma vez que este tipo de tramas apenas deve ser processado pelo *daemon* WiFIX2. Para possibilitar o envio das tramas com encapsulamento Eo11, aumentou-se 14 bytes ao valor da MTU da carta de rede.

O processamento das tramas de controlo (TR) e das tramas de dados realizado pelo WiFIX2 será descrito nas secções que se seguem. No que concerne às tramas de dados, este capítulo dividir-se-á em três secções, de acordo com os três mecanismos considerados no Capítulo 3.

## 4.1 *Active Topology Creation and Maintenance*

A auto-configuração da rede emalhada sem fios depende da troca de mensagens TR entre MAPs. Desta forma, o processamento das tramas que contêm estas mensagens é um aspecto crítico e será descrito nesta secção.

Uma mensagem TR é, inicialmente, enviada pelo *master* MAP e reencaminhada pelo restantes MAPs, após alteração dos parâmetros necessários. Durante um período de decisão (na implementação igual a 5 segundos), os MAPs acumulam as tramas TR recebidas dos vários nós ao seu alcance. No fim deste período, cada MAP escolhe o pai que lhe proporcionar um caminho até ao *master* MAP com um menor número de *hops*. Os parâmetros mais importantes presentes nas mensagens TR são: o número de *hops* para o *master*, o número de sequência, o endereço do pai e o *time-to-live*. Quando um MAP escolhe o seu pai, o *daemon* WiFIX2 cria uma nova *tap* e adiciona-a à *bridge*, actualizando a tabela de associação entre as *taps* e os endereços MAC dos respectivos vizinhos. Um MAP apercebe-se que foi escolhido como pai de outro MAP, quando recebe uma mensagem TR, com o campo *parent address* preenchido com o seu próprio endereço MAC. Nesta situação, o *daemon* WiFIX2 do nó pai executa os mesmos procedimentos, ou seja, cria e adiciona uma nova *tap* à *bridge* e actualiza a respectiva tabela. Neste altura fica estabelecido

um túnel entre o nó pai e o nó filho. O conjunto de túneis estabelecidos permite criar uma árvore com raiz no *master* MAP. Desta forma, o protocolo RSTP, que pode ser usado pelas *bridges* IEEE 802.1D para eliminar *loops*, é desactivado, uma vez que o mecanismo do próprio WiFIX2 já cumpre esse objectivo.

O mecanismo ATCM não foi implementado no âmbito deste trabalho, tendo sido herdado da solução WiFIX 1.0. A existência desta secção deve-se à relevância deste mecanismo para o funcionamento da solução WiFIX 2.0.

## 4.2 *Multicast* como *Broadcast*

Como foi referido anteriormente, o trabalho desenvolvido no âmbito desta dissertação foi dividido em três fases. Nesta secção será abordada a forma como foi realizada a implementação do mecanismo McB, que trata o tráfego *multicast* da mesma forma que o *broadcast*. Nesta fase, a grande diferença desta solução relativamente às outras referidas no Capítulo 2 reside no facto das tramas de dados com endereço MAC de destino *broadcast* serem encapsuladas em tramas *unicast*. Desta forma, também as tramas de dados com endereço MAC de destino *multicast* recebem o mesmo tratamento. Portanto, todas as tramas de dados são transmitidas em *unicast* ao nível MAC 802.11. Quando uma trama de dados é recebida na interface de rede 802.11, o *daemon* WiFIX2 desencapsula-a e envia-a para a *tap* correspondente ao endereço MAC do vizinho de onde a trama foi recebida (*current node*). Se o endereço MAC de destino for *broadcast* ou *multicast*, a *bridge* coloca uma cópia da trama em cada interface, menos naquela onde a recebeu. O *daemon* verifica as interfaces, uma a uma. Cada trama é encapsulada em *unicast* e enviada para o vizinho correspondente à *tap* actual, através da interface de rede 802.11. Com este mecanismo, cada MAP com *n* vizinhos, envia *n-1* tramas. Os nós folha não efectuam encaminhamento, uma vez que têm apenas um vizinho. Nas tramas *multicast/broadcast* enviadas em *unicast*, o cabeçalho exterior contém no campo endereço MAC de origem, o endereço MAC do próprio nó e no campo endereço MAC de destino, o endereço MAC de cada nó vizinho. O valor do campo *Ethertype* corresponde ao encapsulamento Eo11.

## 4.3 *Multicast* Selectivo

Na segunda fase do trabalho, foi implementado o mecanismo MS para uma difusão de tráfego *multicast* mais eficiente que no caso do mecanismo McB e no caso das soluções referidas no Capítulo 2, no que diz respeito à gestão da largura de banda disponível na rede. A implementação realizada baseia-se na técnica IGMP *snooping*, uma vez que o protocolo de nível 3 considerado na implementação foi o IPv4. Além disso, está optimizada para as versões 2 e 3 do protocolo IGMP. Alguns fabricantes implementam este mecanismo nos seus *switches*, mas o *software* de implementação das *bridges* 802.1D para Linux não prevê esta possibilidade. Assim, o elemento do sistema que irá realizar esta função será o *daemon* WiFIX2, uma vez que a implicação de

alterações no *software* da *bridge* sairia do âmbito desta dissertação. O fluxograma da Figura 4.3 decreve o mecanismo implementado para a construção das tabelas de grupos.

Tabela 4.1: Exemplo de uma tabela de grupos

| Endereço IP do grupo *multicast* | Listas de *taps* | *Lifetime* (s) |
|---|---|---|
| 239.255.0.1 | *tap1* e *tap3* | 74 |
| 239.255.0.2 | *tap2*, *tap4* e *tap5* | 118 |
| 239.255.255.1 | *tap3* | 125 |

Cada vez que o *daemon* WiFIX2 lê uma trama de dados na interface de rede 802.11, após o desencapsulamento, verifica se o endereço MAC de destino (original) é *multicast*, através da análise do primeiro octeto deste campo. Se o último bit for 1, o endereço MAC é *multicast* [23]. Caso esta situação se verifique e o campo *Ethertype* da trama indique que o encapsulamento seguinte corresponde ao protocolo IP na versão 4 (0x0800), o *daemon* WiFIX2 inspecciona o cabeçalho IP, identificando o encapsulamento seguinte. Se o pacote IP transportar uma mensagem IGMP *Report*, ou seja, se o campo *protocol* for igual a 0x02 e o campo *type* do cabeçalho IGMP for igual a 0x22, o *daemon* inspecciona determinados campos da mensagem. Em primeiro lugar, lê o campo *number of group records*, uma vez que no protocolo IGMPv3 é possível enviar mensagens de associação ou desassociação a diferentes grupos, em simultâneo. Para cada *group record* lê os campos *record type* e *multicast address*, de forma a preencher a tabela de grupos (Tabela 4.1) em conformidade com o tipo de mensagem. Se o *record type* for igual a 0x02 ou 0x04 e o *number of sources* for igual a 0x00, indica que a interface da estação que enviou a mensagem se encontra no modo *EXCLUDE* ou mudou para o modo *EXCLUDE*, respectivamente, e pretende receber tráfego direccionado ao grupo correspondente ao endereço IP do campo *multicast address*, com origem em qualquer fonte. Se a estação enviar, de seguida, uma nova mensagem IGMP *Report* com um *Group Record* relativo ao mesmo grupo, com o campo *record type* igual a 0x03 e o campo *number of sources* igual a 0x00, indica que deixou de pretender receber tráfego relativo àquele grupo. Caso considere que o pacote IGMP *Report* represente uma associação a um grupo, o *daemon* WiFIX2 cria uma nova entrada na tabela de grupos com o endereço IP *multicast* do grupo, a *tap* correspondente ao endereço MAC do vizinho de onde recebeu a trama e o *lifetime* (por omissão, carregado com 125 segundos [3]). A chave primária da tabela é o endereço IP *multicast*, portanto existe uma entrada por endereço IP *multicast*. Assim, aquando da chegada de um IGMP *Report* de associação, se a respectiva entrada já existir, o *daemon* WiFIX2 adiciona-lhe a *tap* correspondente ao endereço MAC do vizinho de onde recebeu a trama e actualiza o *lifetime*. Quando é recebido um pacote IGMP *Report* de desassociação, o *daemon*, para cada *Group Record*, realiza uma pesquisa na tabela de grupos a partir do valor lido no campo *multicast address*. Caso exista uma entrada relativa a esse endereço, remove a *tap* correspondente ao vizinho de onde recebeu a mensagem IGMP *Report*. Caso não exista, o pacote é ignorado. Todas as tramas que transportam mensagens IGMP *Report* são encaminhadas de acordo com o endereço MAC de destino.

Após a criação das tabelas de grupos, o *daemon* WiFIX2 está apto a encaminhar as tramas *multicast* de forma selectiva. Aquando da recepção de uma trama *multicast*, devido ao método

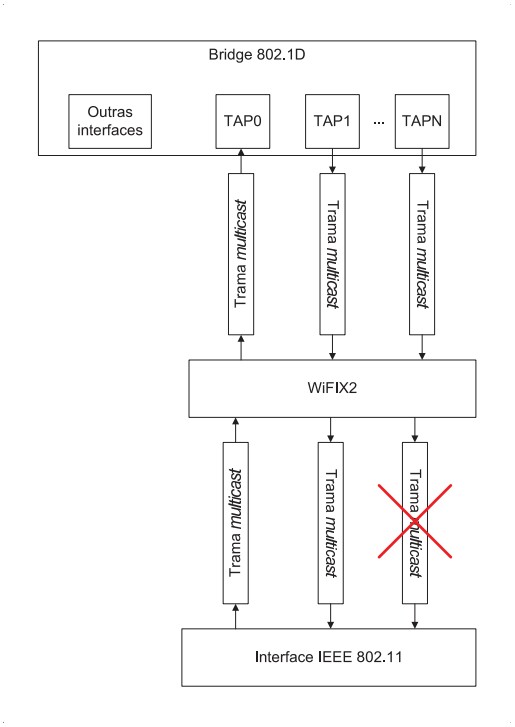



Figura 4.2: Encaminhamento selectivo de tramas *multicast*

de encaminhamento de tramas *multicast* aplicado pela *bridge*, irá aparecer uma cópia da trama em cada uma das *taps*, excepto aquela que corresponde ao vizinho do qual a recebeu. Nem todas as *taps* estarão associadas a esse endereço *multicast* e, deste modo, não se pretende enviá-la para todos os vizinhos. A função do *daemon* é verificar as *taps*, uma a uma, e por cada trama, consultar a tabela de grupos. Mais uma vez, o *daemon* WiFIX2 inspecciona o cabeçalho do protocolo IP, para obter o endereço IP *multicast* de destino. Se existir uma entrada na tabela relativa ao endereço IP *multicast* em questão e se a *tap* onde surge a trama estiver associada a esse grupo, esta é encapsulada e enviada para o vizinho correspondente, através do túnel Eo11. Se não estiver associada ao grupo, a trama é descartada. A Figura 4.2 ilustra o processamento realizado pelo *daemon* WiFIX2 relativamente às tramas *multicast*.

## 4.4 *Multicast* Selectivo com Suporte de Mobilidade

Tendo em conta que no mecanismo referido na secção anterior o tráfego já não chega, automaticamente, a todos os nós, a reaquisição dum fluxo *multicast* por parte de um terminal que muda de MAP deixa de ser garantida. Nesta secção será descrita a implementação realizada para o mecanismo MSMob.

O problema da mobilidade surge no contexto desta dissertação, numa situação em que o terminal pertence a um ou mais grupos. Como um dos objectivos deste trabalho é garantir a mobilidade de terminais evitando alterações nos mesmos, considera-se que um terminal não tem a

possibilidade de avisar a rede que vai iniciar um processo de *handover* entre MAPs. Deste modo, terá que ser a rede a descobrir onde se encontra o terminal, para que os MAPs possam actualizar as suas tabelas de grupos e encaminhar o tráfego *multicast* da forma pretendida.

Quando um terminal muda de MAP, dentro de uma mesma rede IP, tem como objectivo readquirir o endereço IP que possuía anteriormente. Assim que seja estabelecido o *link* com o novo MAP, o terminal envia uma mensagem DHCP *Request* à qual o servidor DHCP responde com uma mensagem DHCP *ACK*. O mecanismo de suporte de mobilidade tira partido desta troca de mensagens para ser capaz de actualizar as tabelas de grupos, usando a técnica DHCP *snooping*.

Quando uma trama com endereço de destino *broadcast* e *Ethertype* igual a 0x0800 é recebida numa das *taps*, o *daemon* WiFIX2 inspecciona o cabeçalho IP e caso o campo *protocol* indique que o protocolo da camada de transporte usado é o UDP, verifica, através do campo *source port number* se se trata de uma mensagem DHCP. Caso seja uma mensagem DHCP *Request*, o *daemon* lê o campo *transaction ID* e juntamente com o endereço MAC de origem da trama e um *lifetime*, cria uma entrada numa tabela, mantida para este propósito, aqui designada tabela de mobilidade. Esta entrada permanecerá na tabela de mobilidade até ser recebida na interface de rede 802.11 uma trama que transporte a mensagem DHCP *ACK* que possua o mesmo *transaction ID* ou até expirar o seu *lifetime*. No caso de ser recebida a mensagem DHCP *ACK*, o *daemon* constrói uma mensagem IGMP *Query general*, com o objectivo de forçar o terminal a enviar uma mensagem IGMP *Report*, algo que apenas ocorrerá se o terminal estiver associado a um ou mais grupos. A mensagem IGMP *Query* é encapsulada num pacote IP e posteriormente numa trama em que endereço MAC de destino será o que consta na entrada correspondente da tabela de mobilidade. Ao receber a mensagem IGMP *Query*, o terminal responderá com uma mensagem IGMP *Report* que será difundida através da rede emalhada 802.11 e permitirá a actualização das tabelas de grupos de todos os MAPs. Todas as tramas que transportam mensagens DHCP são encaminhadas de acordo com o procedimento definido para a solução WiFIX 2.0, para o seu endereço MAC de destino.

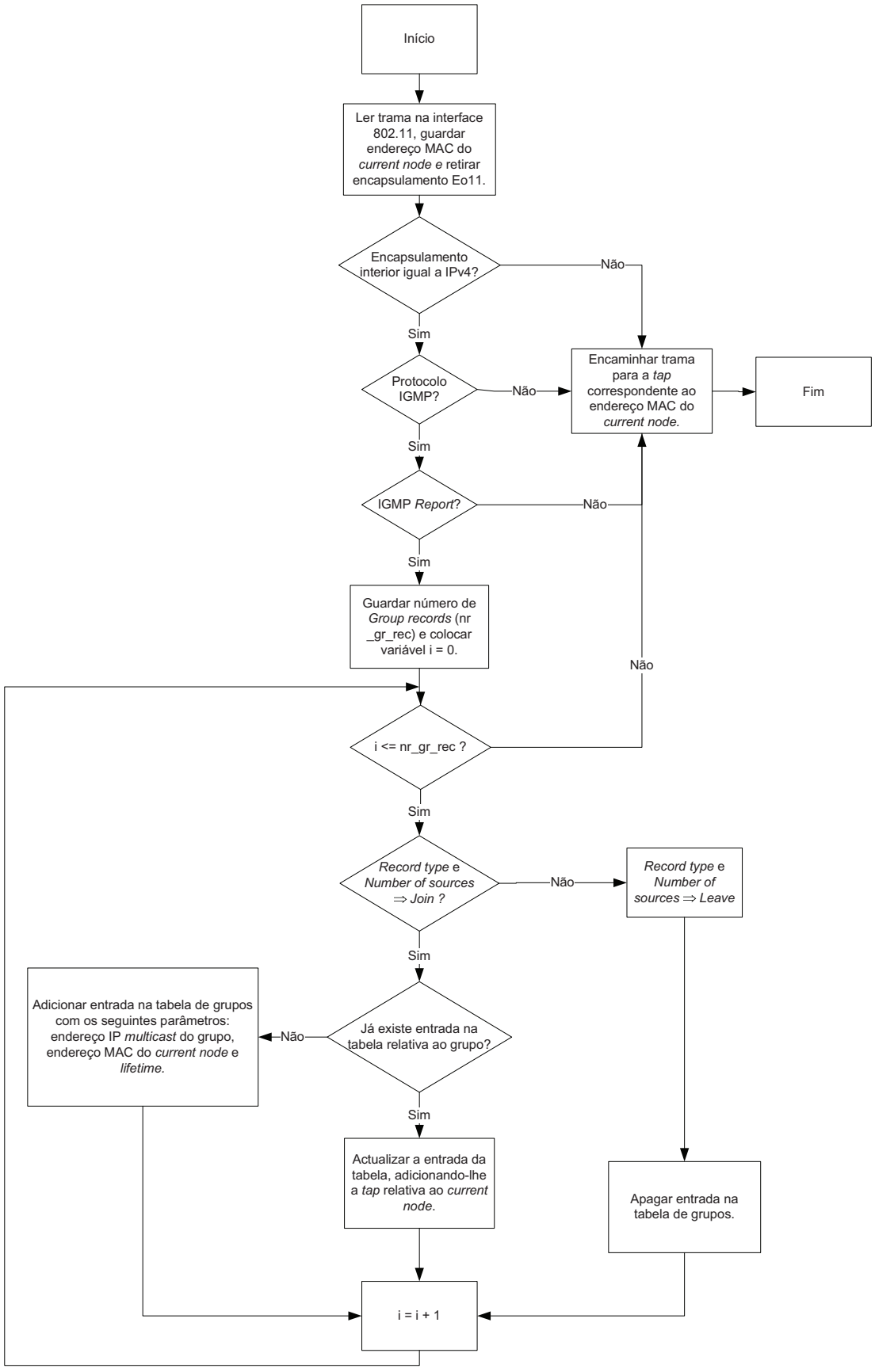



Figura 4.3: Mecanismo de construção das tabelas de grupos

# Capítulo 5

# Avaliação da Solução WiFIX 2.0

Com o objectivo de validar a solução WiFIX 2.0, utilizou-se a implementação realizada para a execução de alguns testes comparativos. Em primeiro lugar comparou-se o mecanismo McB com a principal solução referida no Capítulo 2 para resolver o problema enunciado no Capítulo 1, a solução IEEE 802.11s. De seguida, sendo, à priori, expectável o melhor desempenho do mecanismo McB comparativamente com a solução IEEE 802.11s, comparou-se o mecanismo McB com o mecanismo MS, este último representando uma evolução do primeiro. E por fim, comparou-se o mecanismo MSMob com o mecanismo McB, representando este último, a solução óptima do ponto de vista do suporte da mobilidade de terminais. As principais métricas utilizadas para quantificar o desempenho de cada solução foram: a carga transportada na rede, o atraso dos pacotes e o tempo médio de restabelecimento de um fluxo *multicast* quando há mobilidade. Foram, também, realizados testes com base noutras métricas (*jitter* e *packet loss ratio*), sendo, da mesma forma, importantes para caracterizar o comportamento da rede. A implementação *open-source* do IEEE 802.11s, designada *open802.11s*[1], foi utilizada para avaliar o desempenho desta solução.

Com os recursos disponibilizados, foi possível montar um *test-bed* de quatro máquinas com o sistema operativo Linux, que funcionavam como MAPs. Estas máquinas estavam situadas numa sala do edifício do INESC Porto e todos os MAPs estavam no mesmo alcance rádio. No caso do WiFIX 2.0, para que fosse possível criar a topologia representada na Figura 5.1, utilizou-se uma técnica de filtragem de mensagens TR, suportada pelo próprio *daemon* WiFIX2. Caso contrário, devido ao mecanismo ATCM, obter-se-ia uma árvore com um pai (*master* MAP) e com três filhos. Forçou-se esta árvore para garantir que era usada a mesma topologia activa, ao longo de todos os testes, para as duas soluções, WiFIX 2.0 e IEEE 802.11s. Uma vez que este trabalho assenta num cenário de redes sem fios e a criação de um ambiente completamente livre de interferências não é realizável, todos os testes estiveram sujeitos a factores externos. Assim, tentou-se ao máximo que a influência fosse a mais reduzida possível e afectasse da mesma forma todos eles. Para

[1] Disponível em http://open80211s.org

isso, todos os testes foram realizados aos fins-de-semana, de modo a minimizar, sobretudo, a interferência da rede 802.11 do INESC Porto. As cartas de rede 802.11 de cada um dos MAPs, usados para formar a rede emalhada sem fios, foram configuradas em modo ad-hoc e no canal 3, para minimizar adicionalmente essa interferência. Foi estabelecido um débito máximo de 11 Mbit/s, por aconselhamento da documentação relativa ao *driver* utilizado (Ath5k[2]).

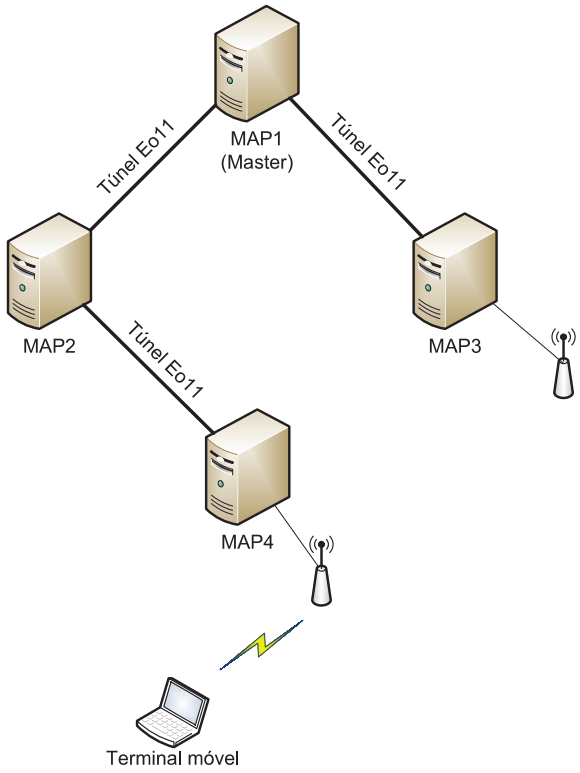



Figura 5.1: *Test-bed*

Os testes de desempenho foram realizados com as ferramentas *Iperf*[3] e *Ping*, colocando-se no *master* MAP uma fonte geradora de tráfego *multicast*, uma vez que se pretendia simular a chegada de tráfego à rede emalhada sem fios, vinda da rede infra-estruturada, através deste nó. Ao longo deste capítulo, será utilizada a designação ilustrada na Figura 5.1 para referência aos quatro MAPs.

Este capítulo está dividido em três secções: Comparação entre WiFIX 2.0 McB e IEEE 802.11s, Comparação entre WiFIX 2.0 McB e WiFIX 2.0 MS e Comparação entre Mobilidade com WiFIX 2.0 McB e com WiFIX 2.0 MSMob. Na Secção 5.1 apresentam-se os resultados obtidos para a solução WiFIX 2.0 McB e para a solução IEEE 802.11s, bem como a sua análise

[2] http://wireless.kernel.org/en/users/Drivers/ath5k
[3] Disponível em http://www.noc.ucf.edu/Tools/Iperf/

e discussão. Na Secção 5.2 apresentam-se os resultados obtidos para os mecanismos McB e MS, nomeadamente no que diz respeito ao aproveitamento da largura de banda total da rede e do efeito em fluxos concorrentes. Na Secção 5.3 apresenta-se a avaliação dos mecanismos McB e MSMob quando há mobilidade de terminais.

## 5.1 Comparação entre WiFIX 2.0 McB e IEEE 802.11s

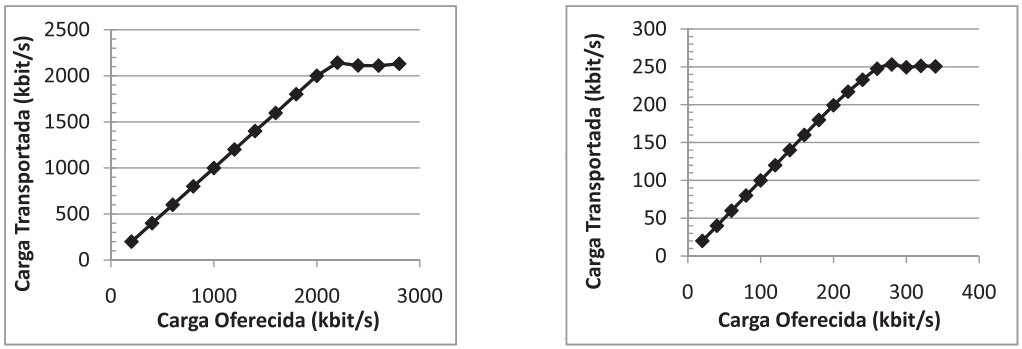
Nesta secção apresenta-se uma descrição do *setup* para a realização dos testes com as soluções WiFIX 2.0 McB e IEEE 802.11s, assim como a análise e discussão dos resultados obtidos.

Para avaliar a solução WiFIX 2.0, colocou-se a correr o *daemon* WiFIX2 em cada uma das máquinas do *test-bed* acima referido, forçou-se a topologia representada na Figura 5.1 e gerou-se tráfego UDP *multicast* no *master* MAP. Em cada um dos outros três nós, mediu-se a carga transportada, o atraso, o *jitter* e o *packet loss ratio* em função da carga oferecida à rede.

### 5.1.1 Carga Transportada

A Figura 5.2 mostra a carga transportada para um nó a um *hop* do *master* MAP para a solução WiFIX 2.0 e para a solução 802.11s. O WiFIX 2.0 McB revela resultados bastante melhores que o 802.11s no que diz respeito à carga transportada. No WiFIX 2.0 McB, a saturação da rede é atingida com uma carga oferecida de aproximadamente 2,2 Mbit/s, enquanto que, para o caso do 802.11s, esta situação acontece para um valor de cerca de 250 kbit/s. Como o WiFIX 2.0 McB usa túneis *unicast* para enviar as tramas *multicast*, é possível utilizar o débito máximo permitido pela norma, que neste cenário de testes foi restringido a 11 Mbit/s, pelas razões apontadas no início deste capítulo. Na prática, o débito máximo obtido para um fluxo UDP *multicast* a um *hop* foi 6 Mbit/s, o que está dentro dos valores expectáveis. No caso do 802.11s, o débito máximo de envio de tramas *multicast* é o mínimo permitido pela norma, que, neste caso, é, teoricamente, 1 Mbit/s. Na prática este valor desce para cerca de 800 kbit/s. Apesar da topologia criada, devido à proximidade dos nós, o meio sem fios é partilhado por todos. Considerando a Figura 5.1, no WiFIX 2.0, o MAP1 envia duas tramas *unicast* e o MAP2 retransmite uma, também em *unicast*. Desta forma, existem sempre dois nós a competir pelo meio, o *master* MAP (MAP1) e o MAP2 que reencaminha o fluxo *multicast* para o MAP4. No IEEE 802.11s, todos os nós retransmitem uma vez uma trama *multicast* recebida, portanto existem quatro nós a competir pelo mesmo meio sem fios. Para o cenário de teste analisado neste capítulo, o WiFIX 2.0 McB introduz uma redução de uma trama, no número total de tramas necessárias na rede, para transmitir a mesma informação. Os gráficos da Figura 5.2 demonstram, desde logo, uma das vantagens da solução WiFIX 2.0, em relação à solução IEEE 802.11s, ou seja, a carga máxima transportada é quase dez vezes maior.

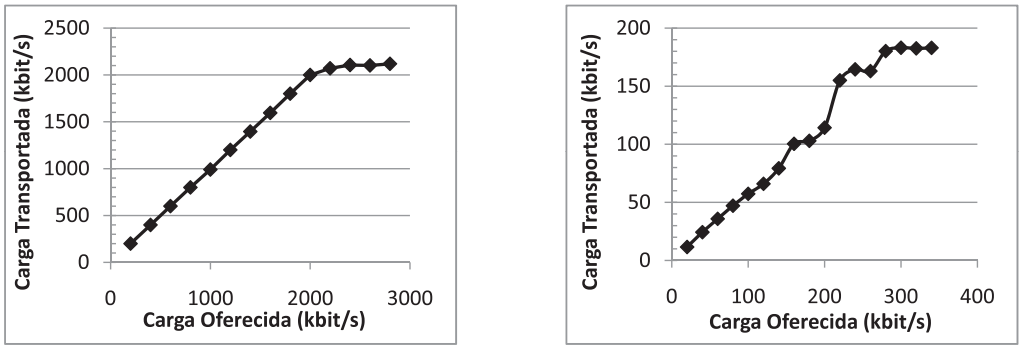
A Figura 5.3 mostra, para ambas as soluções, a carga transportada para um nó a dois *hops*. É possível verificar que para o WiFIX 2.0, a curva do gráfico é praticamente igual à anterior, enquanto que, para o IEEE 802.11s, isto já não se observa. Neste caso, a carga máxima transportada por um nó a dois *hops* é de, aproximadamente, 180 kbit/s, o que equivale a uma redução de quase 30 %. Esta situação deve-se ao facto de se observar uma grande perda de pacotes




(a) WiFIX 2.0 (b) IEEE 802.11s

Figura 5.2: Carga transportada para um nó a um *hop*

neste nó, com percentagens que rondam os 40 %, o que torna a rede completamente inutilizável. Estes dados podem ser consultados mais à frente nesta secção. Tomando em consideração a Figura 5.1, a causa deste comportamento tem a ver com o facto de existir uma sincronização no encaminhamento das tramas por parte dos MAPs 2 e 3, o que provoca colisões frequentes. No envio de tramas *broadcast* e *multicast*, o IEEE 802.11s não prevê um mecanismo de confirmação de recepção, portanto se houver uma colisão, a trama é perdida, não havendo retransmissão.



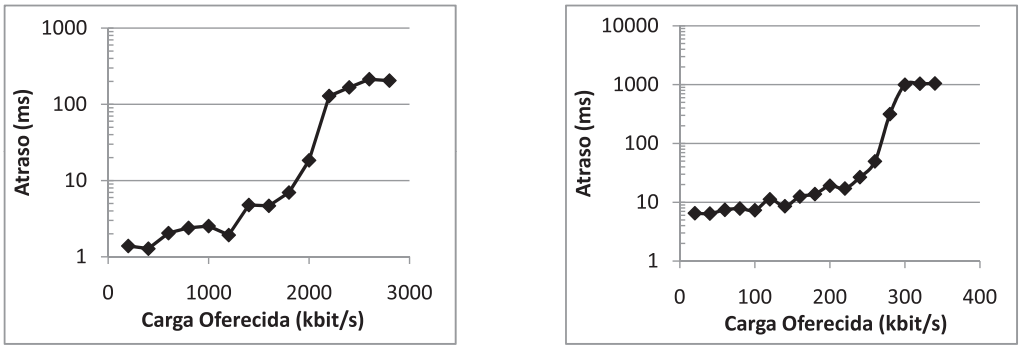

(a) WiFIX 2.0 (b) IEEE 802.11s

Figura 5.3: Carga transportada para um nó a dois *hops*

### 5.1.2 Atraso

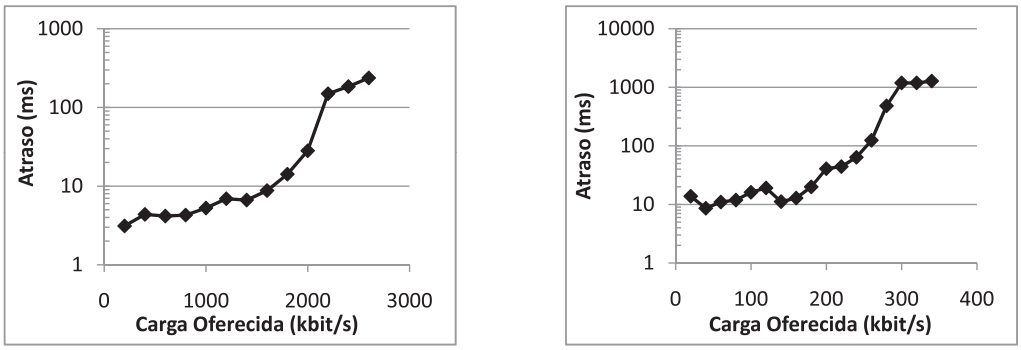
No que concerne à análise do atraso dos pacotes, as Figuras 5.4 e 5.5 mostram as diferenças existentes entre as duas soluções em causa, para um nó a um e dois *hops* do *master*, respectivamente. O WiFIX 2.0 demonstra, também, ganhos em relação ao IEEE 802.11s nesta métrica, apresentando um atraso máximo de aproximadamente 200 ms num nó a um *hop* e 300 ms num nó a dois *hops*, enquanto que o IEEE 802.11 apresenta um atraso máximo no valor de

aproximadamente 1 s, para ambos os casos, embora o atraso num nó a dois *hops* seja ligeiramente superior. A possibilidade de enviar tráfego a um débito maior, para a solução WiFIX 2.0 McB é um factor determinante para que o valor do atraso seja menor. Assim, para um dado valor de carga oferecida à rede, o WiFIX 2.0 McB introduz sempre um menor atraso nos pacotes.




(a) WiFIX 2.0 (b) IEEE 802.11s

Figura 5.4: Atraso dos pacotes num nó a um *hop*




(a) WiFIX 2.0 (b) IEEE 802.11s

Figura 5.5: Atraso dos pacotes num nó a dois *hops*

### 5.1.3 *Jitter*

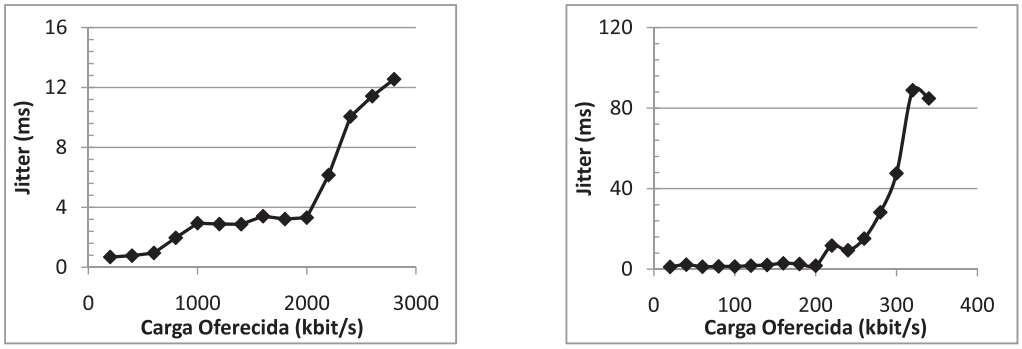
Aplicações com requisitos de tempo-real, com por exemplo, video conferência, difusão de rádio sobre IP, fazem, frequentemente, uso de mecanismos de difusão de tráfego *multicast*. Este tipo de aplicações revela sensibilidade à variação do atraso dos pacotes, tornando importante a avaliação do desempenho das redes, no que diz respeito ao *jitter*[4].

Nas Figuras 5.6 e 5.7 são apresentados os gráficos para o *jitter* obtido a um e dois *hops* do *master* MAP, respectivamente, para as soluções WiFIX 2.0 McB e IEEE 802.11s, em função da

[4]No contexto desta dissertação este termo significa a variação do atraso dos pacotes

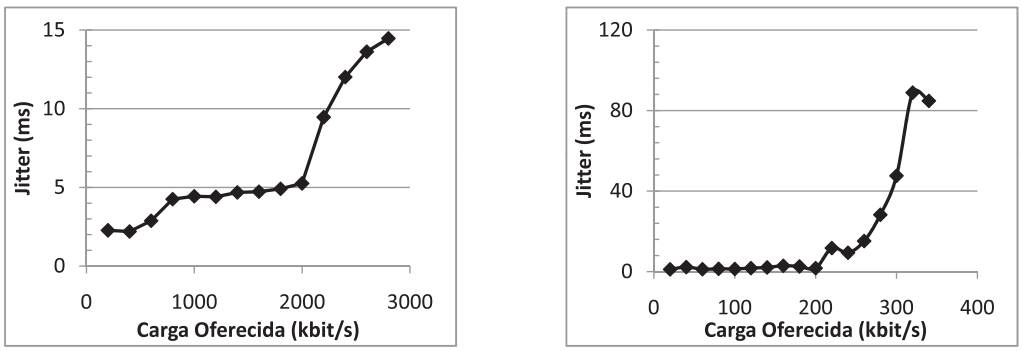
carga oferecida à rede. À medida que esta carga aumenta, em ambas as soluções, o *jitter* tende a subir de forma linear até ao limite de saturação da rede. Após este valor, tende a subir de uma forma abrupta.

Para a solução WiFIX 2.0 McB, ao aumentar a carga oferecida, a probabilidade de um trama sofrer uma colisão aumenta, o que leva a um aumento do número de retransmissões. Desta forma, a diferença entre o atraso de pacotes consecutivos sofre uma variação de maior amplitude. Além disso, o mecanismo de acesso ao meio em redes 802.11 introduz desde logo variações no atraso, que têm tendência a intensificar-se com o aumento do congestionamento da rede. Antes de um nó iniciar uma transmissão, escuta o meio, e caso esteja livre durante um dado período de tempo (DIFS, *Distributed Inter Frame Space*), envia a trama, caso contrário terá que esperar tempo aleatório determinado pelo *random backoff algorithm* do 802.11. Este tempo contribui também para o valor do *jitter*. Na zona de saturação, o congestionamento da rede e o aumento do número de perdas são os responsáveis pela rápida subida do *jitter*. Além disso, irá aumentar ainda o número de vezes em que um nó necessitará de executar o *random backoff algorithm*.




(a) WiFIX 2.0 (b) IEEE 802.11s

Figura 5.6: *Jitter* para um nó a um *hop*




(a) WiFIX 2.0 (b) IEEE 802.11s

Figura 5.7: *Jitter* para um nó a dois *hops*

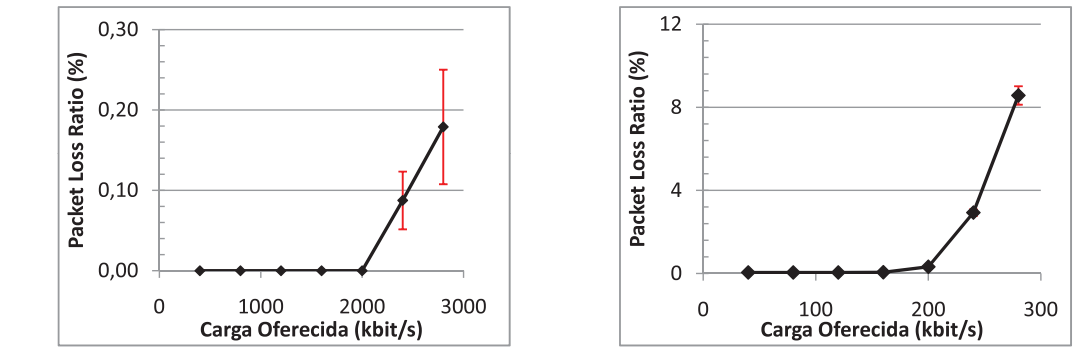
No caso da solução IEEE 802.11s, o comportamento é semelhante ao da solução anterior. Nesta solução, por cada trama enviada pelo *master* são reenviadas três tramas, no total de quatro tramas para transmitir a mesma informação, o que leva a que haja uma maior competição pelo meio. Em termos globais, o *jitter* verificado na solução WiFIX 2.0 é bastante mais baixo que o da solução IEEE 802.11s, mesmo considerando intervalos de carga oferecida diferentes.

A tendência de crescimento das curvas dos gráficos relativos aos dois nós é semelhante. A diferença está no valor do *jitter* para cada ponto. Para o nó a dois *hops* o valor do *jitter* é superior, uma vez que as tramas têm que ser enviadas duas vezes, passando por duas filas e competindo duas vezes pelo meio.

### 5.1.4 *Packet Loss Ratio*

A avaliação do *packet loss ratio* é importante, sobretudo porque, muitas vezes, as aplicações que difundem tráfego *multicast* usam o protocolo UDP da camada de transporte. Este protocolo não suporta qualquer tipo de mecanismo de garantia de entrega, portanto o número de pacotes perdidos é um aspecto importante a considerar.

As Figuras 5.8 e 5.9 apresentam os gráficos da variação do *packet loss ratio* em nós a um e dois *hops* do *master*, respectivamente, para as soluções WiFIX 2.0 McB e IEEE 802.11s.

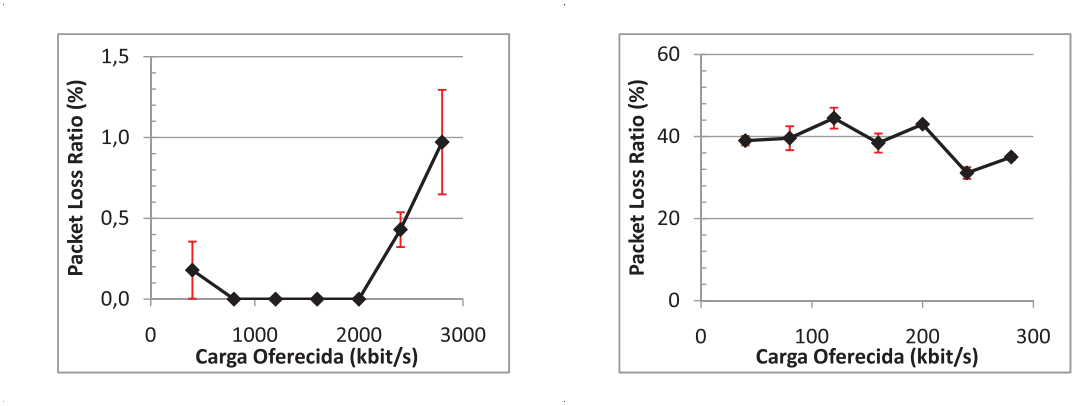



(a) WiFIX 2.0 (b) IEEE 802.11s

Figura 5.8: *Packet loss ratio* para um nó a um *hop*

Comparando com os resultados apresentados anteriormente, nesta secção, é de salientar o facto de estarem representados, nestes gráficos, os intervalos de confiança, uma vez que estes testes foram realizados na fase final do trabalho, não havendo tempo para serem repetidos vezes suficientes para a obtenção de intervalos de confiança de menor amplitude. Pela mesma razão, as curvas representadas são constituídas por um menor número de pontos. De qualquer forma, é possível obter-se uma aproximação do comportamento da rede, ao nível do *packet loss ratio* observado em dois nós.

A situação mais crítica é a verificada para um nó a dois *hops*, com a solução 802.11s. O *packet loss ratio* apresenta um comportamento oscilatório e mesmo para valores baixos de carga




(a) WiFIX 2.0 (b) IEEE 802.11s

Figura 5.9: *Packet loss ratio* para um nó a dois *hops*

oferecida, é da ordem dos 40 %. No Apêndice A, é descrita uma experiência auxiliar que foi realizada tendo em conta este comportamento e é apresentada uma explicação para o mesmo.

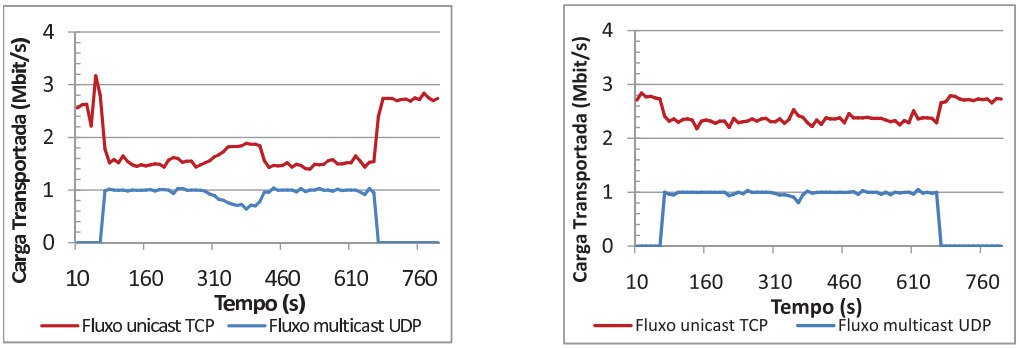
De uma forma geral, os valores do *packet loss ratio* para a solução WiFIX 2.0 McB são menores do que para a solução IEEE 802.11s, mesmo para valores de carga oferecida maiores. No que diz respeito ao impacto do número de *hops* para o *master* MAP nesta métrica, observa-se que, para ambas as soluções, o nó a dois *hops* apresenta um *packet loss ratio* máximo maior do que o nó a um *hop*. Considerando a Figura 5.1, como o MAP2 reencaminha as tramas para o MAP4, o valor do *packet loss ratio* para o nó a dois *hops* (MAP4) reflecte as tramas perdidas na transmissão entre o MAP1 e o MAP2 e na transmissão entre o MAP2 e o MAP4, logo faz sentido que seja maior do que o observado para o nó a um *hop*.

## 5.2 Comparação entre WiFIX 2.0 McB e WiFIX 2.0 MS

Nesta secção comparam-se os mecanismo McB e MS propostos no contexto do WiFIX 2.0, no que diz respeito à influência de um fluxo *multicast* num fluxo *unicast* que concorra pelos mesmos recursos da rede. Consideraram-se dois cenários. No Cenário 1, colocou-se uma fonte geradora de tráfego *multicast* UDP relativo a um grupo a que apenas o MAP3 pertencia e uma fonte de tráfego *unicast* TCP com destino ao MAP4 no *master* MAP. No Cenário 2, inverteu-se a situação, introduzindo um fluxo *unicast* TCP para o MAP3 e um fluxo *multicast* UDP que apenas seria recebido pelo MAP4. Para estes dois cenários, testaram-se os dois mecanismos de difusão de tráfego *multicast*. O fluxo *multicast* é gerado com um débito fixo de 1 Mbit/s.

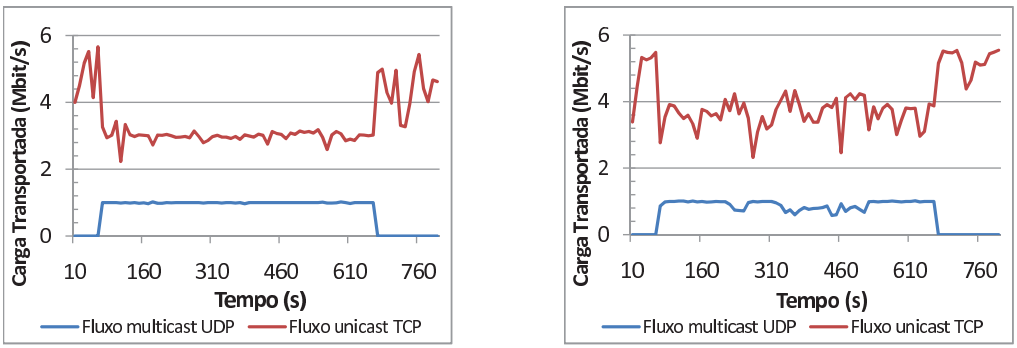
Os gráficos da Figura 5.10 mostram, para o Cenário 1, a influência do fluxo *multicast* no débito efectivo do fluxo *unicast* já existente na rede. Quando a difusão do tráfego *multicast* é realizada usando o mecanismo McB, em cada instante, o MAP1 envia duas tramas a um débito igual a 1 Mbit/s cada e o MAP2 envia uma, também a um débito igual a 1 Mbit/s. Deste modo, o fluxo *unicast* TCP toma posse da restante largura de banda. É, portanto, fácil de concluir que, quanto menos tramas *multicast* forem enviadas, em cada instante, maior é a largura de banda disponível

para o fluxo *unicast* usar. Sendo assim, pode, desde logo, deduzir-se que a influência do fluxo *multicast* quando é usado o mecanismo MS será menor. O factor mais importante em jogo é, então, o facto das tramas *multicast* que chegam aos MAPs 2 e 3 serem descartadas, uma vez que estes nós não pretendem receber tráfego relativo ao grupo em questão. Há, portanto, uma ocupação desnecessária da rede. Com a difusão do tráfego *multicast* usando o mecanismo McB, aquando da entrada do fluxo *multicast*, o débito do fluxo *unicast* diminui, aproximadamente 1,3 Mbit/s, o que representa um decréscimo de cerca de 46 % e o atraso médio dos pacotes é igual a 543 ms. Com o uso do mecanismo MS, a diminuição é de, aproximadamente 400 kbit/s, representando um decréscimo de, apenas, 14 % e o atraso médio dos pacotes é igual a 243 ms. Estes dados reflectem, simplesmente, as vantagens de usar encaminhamento selectivo.




(a) *Multicast* como *broadcast* (b) *Multicast* selectivo

Figura 5.10: Cenário 1: Influência do fluxo *multicast* UDP no fluxo *unicast* TCP




(a) *Multicast* como *broadcast* (b) *Multicast* selectivo

Figura 5.11: Cenário 2: Influência do fluxo *multicast* UDP no fluxo *unicast* TCP

Os gráficos da Figura 5.11 indicam os resultados obtidos, com o Cenário 2, para os dois mecanismos de difusão de tráfego *multicast*. Usando o mecanismo McB, a diminuição do débito do fluxo *unicast* TCP é, aproximadamente, igual a 48 %, enquanto que, com o mecanismo MS é,

aproximadamente, igual a 36 %. A diferença dos atrasos médios dos pacotes é de 144 ms. Neste cenário, a melhoria introduzida pela utilização de encaminhamento selectivo não é tão significativa como no cenário anterior. No entanto, em termos absolutos, o débito do fluxo *unicast* TCP é sempre maior, no segundo cenário.

## 5.3 Mobilidade com WiFIX 2.0 McB e com WiFIX 2.0 MSMob

Nesta secção apresentam-se os resultados obtidos para os mecanismos McB e MSMob no que concerne ao tempo de reaquisição de um fluxo *multicast*, quando um terminal muda de MAP. A Figura 5.12 ilustra o cenário de mobilidade do terminal nos testes efectuados. O objectivo é analisar o impacto do tempo necessário para actualizar as tabelas de grupos dos MAPs e redireccionar um determinado fluxo *multicast*, no tempo total de reaquisição desse mesmo fluxo, por parte do terminal, quando se usa o mecanismo MSMob. Por outro lado, importa comparar esse tempo com o tempo de reaquisição óptimo, obtido com o mecanismo McB. No terminal, iniciou-se uma aplicação que permitisse a associação a um determinado grupo, invocando o protocolo IGMP para o envio de mensagens de IGMP *Report*. No MAP1, iniciou-se a ferramenta *Ping* de forma a enviar pacotes de 64 bytes com endereço de destino *multicast*, com intervalos de 10 ms.

Com a ferramenta *Wireshark*[5], foi possível obter, no terminal, o instante de tempo em que chegou o último pacote *multicast* através do MAP4 e o instante de tempo em que chegou o primeiro pacote através do MAP3, sendo possível dessa forma calcular o tempo de reaquisição do fluxo *multicast*.

Tabela 5.1: Tempo médio de reaquisição de um fluxo *multicast*

| Mecanismo | Tempo (ms) |
|---|---|
| McB | 207 |
| MSMob | 384 |

A implementação do cliente DHCP, em Linux, *dhclient*, que é invocada quando o terminal chega ao MAP3, introduz um tempo aleatório antes de enviar uma mensagem DHCP *Request*. Este tempo irá influenciar o tempo total de reaquisição do fluxo *multicast*. Visto que o objectivo era avaliar o efeito da solução MSMob no tempo total de reaquisição do fluxo *multicast*, este tempo aleatório foi subtraído nos cálculos efectuados.

A solução MSMob introduz um tempo de reaquisição de um fluxo *multicast* superior ao obtido para solução McB, como seria de esperar. Este aumento deve-se, essencialmente, a dois factores: o atraso das mensagens DHCP *Request* e DHCP *ACK* e o tempo de resposta do terminal à mensagem IGMP *Query* enviada pelo MAP3. Embora menos significativo, existe ainda outro factor, o tempo de actualização das tabelas. A solução McB não depende destes factores, uma vez que, quando o terminal chega ao MAP3, adquire logo o fluxo, que já estava a ser enviado para este MAP.

[5] http://www.wireshark.org/

A Tabela 5.1 apresenta os valores para o tempo médio de reaquisição de um fluxo *multicast*, para ambas as soluções, resultante da média dos tempos de reaquisição de fluxo *multicast* medidos para dez experiências distintas. Os valores observados para os dois mecanismos são da mesma ordem de grandeza. Assim, globalmente, o mecanismo MSMob é mais vantajoso, visto que é mais eficiente na difusão do tráfego *multicast*, e não compromete de forma significativa o tempo de reaquisição de fluxos *multicast*, quando comparado com o mecanismo McB, menos eficiente mas óptimo do ponto de vista da gestão da mobilidade de terminais.

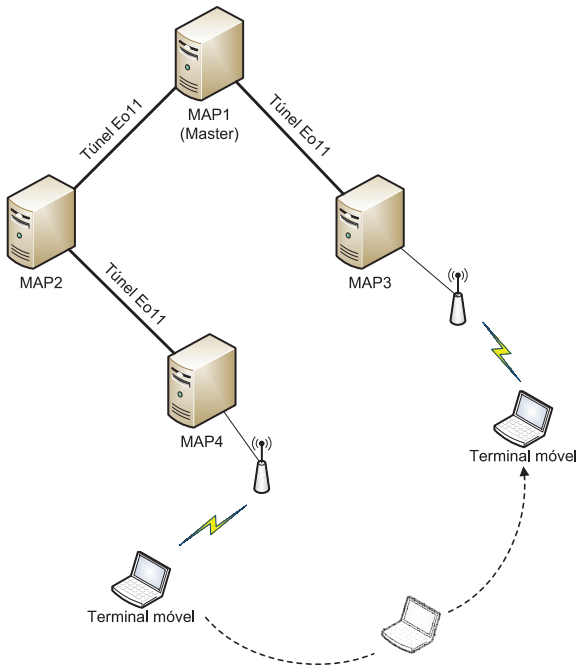



Figura 5.12: Cenário de mobilidade

## 5.4 Discussão

Nesta secção são discutidos alguns aspectos relevantes relativos aos resultados experimentais obtidos. Na Secção 4.3 é referido que o *lifetime* de cada entrada da tabela de grupos é carregado com 125 s. Este foi o valor escolhido, uma vez que corresponde ao intervalo, por omissão, especificado em [3], entre o envio de mensagens IGMP *Query* por parte dos *routers multicast*. No entanto, este valor poderá ser demasiado elevado, comprometendo a eficiência da solução WiFIX 2.0 MSMob. Uma solução para este problema seria diminuir o valor do intervalo entre o

envio de mensagem IGMP *Query* pelos *routers multicast* e, por consequência, diminuir o valor inicial do *lifetime* das tabelas de grupos. Outra solução seria manter para cada *tap* de cada entrada da tabela de grupos, uma lista de endereços MAC dos terminais pertencentes ao respectivo grupo. Essa informação seria adicionada à tabela, aquando da passagem de uma mensagem IGMP *Report* por cada MAP. Assim, um MAP, ao receber uma trama contendo uma mensagem IGMP *Report*, leria o endereço MAC de origem e verificaria na tabela se este endereço já estaria associado uma *tap* que, por sua vez, estaria associada ao grupo correspondente à mensagem IGMP *Report*. Caso isto acontecesse, quereria dizer que o terminal que enviou a mensagem, já teria estado associado a outro MAP, o que é o mesmo que dizer que teria havido mobilidade. Caso o endereço MAC referido fosse o único associado à respectiva *tap* do respectivo grupo, essa *tap* poderia ser eliminada da entrada da tabela, deixando de ser encaminhado, por ela, o tráfego para esse grupo.

Na Secção 5.1 foram utilizadas diferentes gamas de valores de carga oferecida à rede para as duas soluções comparadas. Esta opção deveu-se ao facto da solução WiFIX 2.0 possuir um limite máximo para a carga transportada na rede cerca de uma ordem de grandeza acima do valor obtido para a solução IEEE 802.11s. Nesta primeira fase do desenvolvimento da solução WiFIX 2.0, verificou-se fundamentalmente a vantagem de usar encapsulamento da tramas *multicast* em *unicast*.

Na secção 5.2, o objectivo era, desde logo, demonstrar a poupança de largura de banda que se poderia obter usando o mecanismo MS do WiFIX 2.0. Uma forma de o conseguir foi introduzir um fluxo concorrente na rede que ocupasse a largura de banda restante. Deste modo, os testes foram realizados no sentido de quantificar a influência do uso dos dois mecanismos (McB e MS) nesse fluxo concorrente. Foram utilizados dois cenários diferentes, visto que o facto do fluxo *unicast* TCP ser dirigido a um nó a um ou dois *hops* influencia o valor da largura de banda, por ele, utilizada.

Na secção 5.3, o objectivo fundamental era demonstrar que o mecanismo de suporte de mobilidade permitia, efectivamente, a reaquisição de um fluxo *multicast* por parte do terminal que mudava de MAP. No entanto, era também importante mostrar que o tempo de reaquisição de um fluxo não aumentaria consideravelmente, o que foi conseguido.

Uma vantagem importante da solução WiFIX 2.0 é o facto de ter sido desenvolvida por módulos. Desta forma, é possível utilizar-se apenas o mecanismo que se pretender (McB, MS ou MSMob).

# Capítulo 6

# Conclusões

Neste capítulo são expostas as conclusões relativas à concretização dos objectivos definidos para esta dissertação e apresentam-se novamente as contribuições inovadoras deste trabalho. No final, apontam-se algumas propostas para trabalho futuro no âmbito da solução aqui apresentada.

## 6.1 Concretização dos Objectivos

Os objectivos propostos no início deste trabalho foram alcançados. Uma solução para difusão eficiente de tráfego *multicast* com suporte de mobilidade de terminais, designada WiFIX 2.0, foi especificada, implementada e testada. A avaliação de resultados demonstrou que a solução desenvolvida é mais eficiente que a principal solução concorrente - a solução IEEE 802.11s, não só porque permite o envio de tráfego *multicast* com um débito maior, mas também porque realiza um encaminhamento selectivo, aumentando a eficiência. Além disso, e como consequência, a solução proposta tem também a vantagem de introduzir um menor atraso nos pacotes. Provou-se, ainda, a viabilidade do mecanismo de suporte de mobilidade de terminais. O aumento verificado no tempo de reaquisição de um fluxo *multicast* permite considerar a solução WiFIX 2.0 MSMob mais vantajosa que as soluções WiFIX 2.0 McB e IEEE 802.11s.

## 6.2 Contribuições

Analisando as contribuições previstas no início deste trabalho, é possível dizer que todas foram concretizadas.

### 6.2.1 Especificação da Solução WiFIX 2.0

A especificação de uma solução para difusão de tráfego multicast em redes emalhadas 802.11 com suporte de mobilidade, foi realizada, descrevendo o conjunto de princípios utilizados para conceber o sistema. O aumento da carga transportada e a diminuição do atraso dos pacotes

são algumas das vantagens da solução WiFIX 2.0 em relação à solução IEEE 802.11s. Uma desvantagem desta solução tem a ver com o facto de não estar optimizada para difusão de tráfego *multicast* a partir de fontes localizadas dentro da rede emalhada 802.11, uma vez que as árvores *multicast* para cada grupo têm todas a raíz no *master* MAP.

### 6.2.2 Implementação da Solução WiFIX 2.0

A implemetação da solução especificada representa uma outra contribuição concretizada neste trabalho, o que permitiu a realização de testes, num cenário real, de forma a validar a solução proposta. Esta implementação poderá ser utilizada como base para trabalhos futuros relacionados com a solução WiFIX 2.0. Uma desvantagem da implementação da solução WiFIX 2.0 com os mecanismo MS eMSMob tem a ver como o facto de funcionar apenas para redes IPv4.

### 6.2.3 DHCP *snooping* para Gestão de Mobilidade

A utilização da técnica DHCP *snooping* para gestão de mobilidade de terminais foi uma contribuição inovadora deste trabalho, uma vez que, até ao momento, foi apenas utilizada para controlo de acesso à rede.

## 6.3 Trabalho Futuro

Um aspecto a melhorar em relação à solução desenvolvida seria o alargamento da implementação, de forma a suportar MLD *snooping* e DHCPv6 *snooping*, possibilitando a aplicação da solução em redes IPv6. A adição dos endereços MAC dos terminais à tabela de grupos, de acordo com o que é referido na Secção 5.4, seria, também, uma hipótese como trabalho futuro a desenvolver, pois permitiria melhorar o mecanismo MSMob da solução WiFIX 2.0. No que diz respeito aos testes realizados, poderá utilizar-se um *test-bed* composto por um maior número de máquinas, com o objectivo de avaliar a escalabilidade da solução proposta. Outro aspecto a ter em conta como trabalho futuro seria a realização de testes com a solução WiFIX 2.0, utilizando cartas de rede configuradas para as normas IEEE 802.11a, 802.11g e 802.11n. Recorrendo a estas variantes da tecnologia IEEE 802.11 prevê-se que os ganhos da solução WiFIX 2.0 sejam ainda superiores aos apresentados nesta dissertação. Finalmente, no sentido de melhorar o desempenho do mecanismo MSMob, poderá no futuro considerar-se a especificação de um mecanismo de suporte de mobilidade envolvendo alterações nos terminais móveis. Com esta solução, será expectável a obtenção de tempos de reestabelecimento do(s) fluxo(s) *multicast* menores dos que os obtidos com o mecanismo MSMob.

# Apêndice A

# Testes Com um Cenário de Três Nós

Na Secção 5.1 refere-se a existência de um grande número de colisões entre as tramas enviadas pelo MAP2 e pelo MAP3, nos testes realizados com a solução IEEE 802.11s, o que provoca um grande número de pacotes perdidos no MAP4. Para se confirmar esta hipótese, foram realizados testes com apenas três máquinas e foi avaliado o *packet loss ratio* observado no MAP4. A Figura A.1 mostra o novo *test-bed* montado.

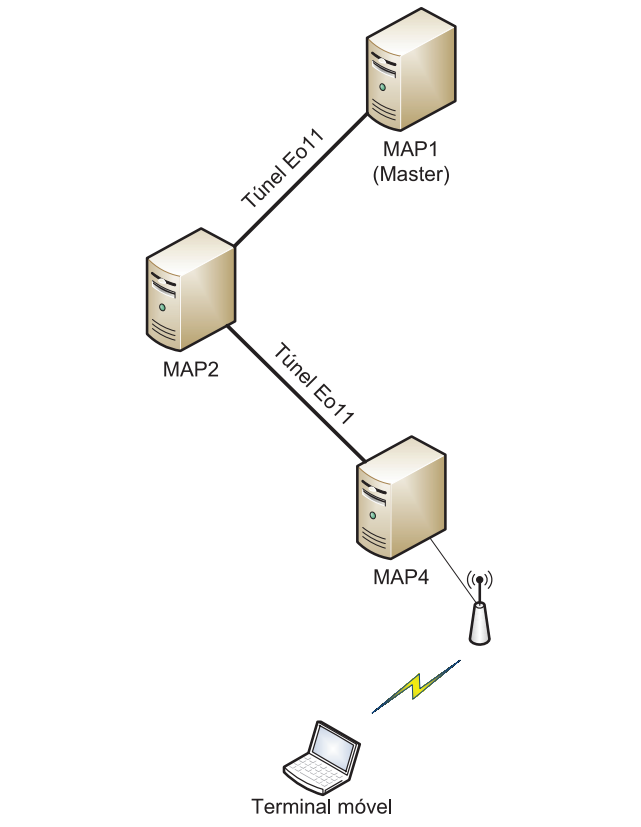



Figura A.1: *Test-bed* de três máquinas

O gráfico da Figura A.2 mostra a variação do *packet loss ratio* no MAP4. O facto mais importante verificado nos testes referidos na Secção 5.1 estava relacionado com os valores obtidos para o *packet loss ratio* para baixos valores de carga oferecida. Nessa situação, obtiveram-se valores acima de 40 %, o que revelava um péssimo desempenho da rede. Neste novo cenário de teste, para valores de carga oferecida em que a rede não se encontra saturada, obtêm-se valores abaixo dos 3 %. Mesmo na zona em que a rede está saturada, por exemplo, para uma carga oferecida de 320 kbit/s, obtém um *packet loss ratio* de aproximadamente 14 %. Para este valor de carga, nos testes referidos na Secção 5.1, obteve-se um valor de 33 %.

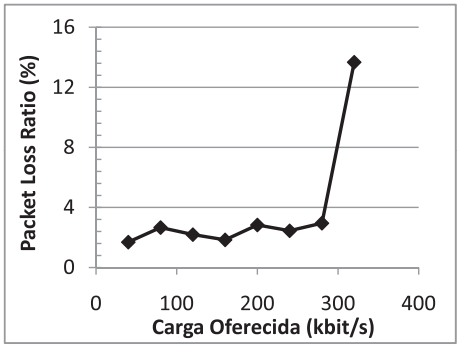



Figura A.2: *Packet loss ratio* no MAP4

Esta experiência auxiliar mostra, ainda que de forma indirecta, que a retransmissão do pacote recebido do MAP1 por parte do MAP3 vai muitas vezes ocorrer num instante temporal muito próximo do instante em que o MAP2 efectua também a sua retransmissão. Este facto aumenta a probabilidade de colisão entre os dois pacotes retransmitidos e provoca o grande aumento do *packet loss ratio* verificado na prática para o MAP4, no cenário com os quatro MAPs. Este é aliás um problema já identificado no âmbito das redes ad-hoc móveis (em inglês *Mobile Ad-hoc Networks* – MANETs), conhecido por *broadcast storm problem* [24].

# Referências


[1] Rui Campos, Ricardo Duarte, Filipe Sousa, Manuel Ricardo, and José Ruela. Network infrastructure extension using 802.1D-based wireless mesh networks. *Wireless Communications And Mobile Computing*, 2009.

[2] IEEE 802.1D. *IEEE Standard for local and metropolitan area networks*. IEEE, June 2004.

[3] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan. *Internet Group Management Protocol, Version 3, RFC3376*. IETF, October 2002.

[4] M. Christensen, K. Kimball, and F. Solensky. *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches, RFC4541*. IETF, May 2006.

[5] R. Droms. *Dynamic Host Configuration Protocol, RFC2131*. IETF, March 1997.

[6] S. Alexander and R. Droms. *DHCP Options and BOOTP Vendor Extensions, RFC2132*. IETF, March 1997.

[7] Sung-Ju Lee, William Su, and Mario Gerla. On-demand multicast routing protocol in multihop wireless mobile networks. *Mobile Networks and Applications 7*, 2002.

[8] J. J. Garcia-Luna-Aceves and Ewerton L. Madruga. A multicast routing protocol for ad-hoc networks. In *IEEE INFOCOM*, 1999.

[9] Sung-Ju Lee, William Su, and Mario Gerla. Ad hoc wireless multicast with mobility prediction. In *Proceedings of IEEE ICCCN'99*, 1999.

[10] Jorjeta G. Jetcheva and David B. Johnson. Adaptive demand-driven multicast routing in multi-hop wireless ad hoc networks. In *MobiHoc '01: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, October 2001.

[11] Hasnaa Moustafa and Houda Labiod. A multicast on-demand mesh-based routing protocol in multihop mobile wireless networks. In *Proceedings of IEEE 58th Vehicular Technology Conference, VTC*, 2003.

[12] W. A. Shittu, Aisha-Hassan A. Hashim F. Anwar, and W. Al-Khateeb. A proposed qos multicast routing framework for next-generation wireless mesh network. *IJCSNS*, 8 No.9, September 2008.

[13] Pedro M. Ruiz, Franciso J. Galera, Christophe Jelger, and Thomas Noel. Efficient multicast routing in wireless mesh networks connected to internet. In *Proceedings of the First International Conference on Integrated Internet Ad Hoc and Sensor Networks*, Nice, France, May 2006.

[14] C. Jelger and T. Noel. Proactive address autoconfiguration and prefix continuity in IPv6 hybrid ad hoc networks. In *Proceedings of IEEESECON'05*, Santa Clara, CA, USA, September 2005.

[15] Uyen Trang Nguyen. On multicast routing in wireless mesh metworks. *Computer Communications 31*, 2008.

[16] William Su, Sung-Ju Lee, and Mario Gerla. Mobility prediction in wireless networks. In *Proceedings of IEEE MILCOM*, 2000.

[17] Zhenxia Zhang, Richard W. Pazzi, and Azzedine Boukerche. A mobility management scheme for wireless mesh networks based on hybrid routing protocol. *Computer Networks*, 2009.

[18] IEEE P802.11s/D2.0. draft amendment to standard IEEE 802.11: Mesh networking. March 2008. work in progress.

[19] R. Vida and L. Costa. *Multicast Listener Discovery Version 2 (MLDv2) for IPv6, RFC3810*. IETF, June 2004.

[20] A. Conta, S. Deering, and M. Gupta. *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, RFC4443*. IETF, March 2006.

[21] P. Mockapetris. *Domain Names - Concepts and Facilities, RFC1034*. IETF, November 1987.

[22] P. Mockapetris. *Domain Names - Implementation and Specification, RFC1035*. IETF, November 1987.

[23] IEEE-SA. Standard group MAC addresses a tutorial guide, 2009. http://standards.ieee.org/regauth/groupmac/tutorial.html.

[24] S. Ni, Y. Tseng, Y. Chen, and J. Sheu. The broadcast storm problem in a mobile ad hoc network. In *Proceedings of the ACM Mobicom'99*, Seattle, USA, August 1999.