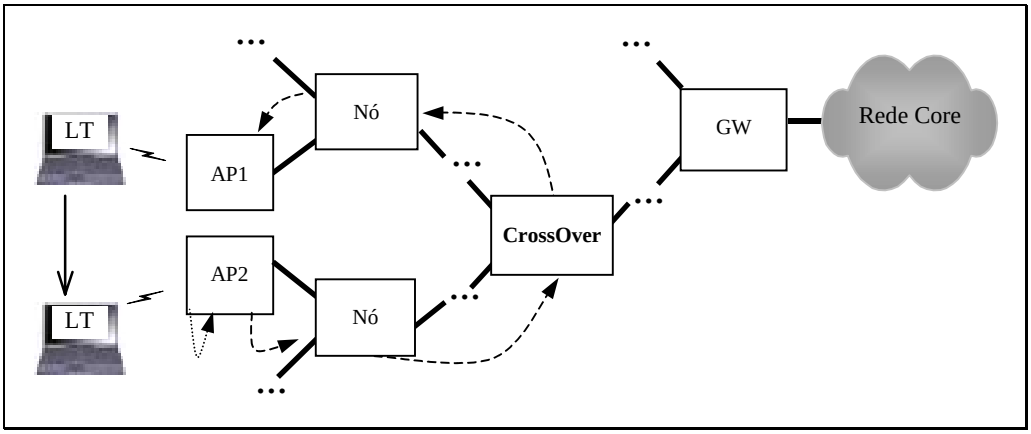
UNIVERSIDADE TÉCNICA DE LISBOA

INSTITUTO SUPERIOR TÉCNICO



Protocolos de Mobilidade para Terminais IP

Pedro Miguel Santos Reis Vale Estrela
(Licenciado)

Dissertação para obtenção do Grau de Mestre em
Engenharia Informática e de Computadores

Jurí:

Presidente:	Doutor Mário Serafim Nunes, Professor Associado do Instituto Superior Técnico, da Universidade Técnica de Lisboa. (Orientador Científico)
1º Vogal:	Doutor Manuel Alberto Pereira Ricardo, Professor Auxiliar da Faculdade de Engenharia da Universidade do Porto.
2º Vogal:	Doutora Teresa Maria Sá Ferreira Vazão Vasques, Professora Auxiliar do Instituto Superior Técnico, da Universidade Técnica de Lisboa.

Prova concluída em:

Janeiro de 2003

Tese realizada sob a orientação do

Prof. Doutor Mário Serafim dos Santos Nunes

Professor Associado do Departamento de Engenharia Electrotécnica e de Computadores

INSTITUTO SUPERIOR TÉCNICO

TÍTULO:	Protocolos de Mobilidade para Terminais IP
NOME:	Pedro Miguel Santos Reis Vale Estrela
CURSO DE MESTRADO EM:	Engenharia Informática e de Computadores
ORIENTADOR:	Prof. Dr. Mário Serafim dos Santos Nunes
PROVAS CONCLUÍDAS EM:	

Resumo

Todos os protocolos de mobilidade IP existentes até à data no IETF assumem a premissa que os terminais móveis têm sempre uma pilha de protocolos com o suporte ao próprio protocolo de mobilidade, o que ainda é um cenário pouco comum actualmente. Este desenho significa que os terminais puramente IP, sem extensões de mobilidade, apenas se podem movimentar no interior da sua subrede IP, podendo a necessidade de alteração dos terminais ser um factor que esteja a contribuir para a falta de generalização do serviço de mobilidade.

Esta Tese de Mestrado vai desenvolver uma arquitectura completa para o suporte de mobilidade Global e Eficiente para todos os possíveis terminais IP existentes. A solução proconizada é composta por uma componente de micro-mobilidade, uma nova proposta (TIMIP) fruto de um trabalho de I&D do autor com ênfase nos aspectos ainda não solucionados em propostas anteriores, e absorve algumas das melhores características que estas já detêm, combinado com uma componente de macro-mobilidade (sMIP) baseada no standard MIP.

Palavras chave: TIMIP, mobilidade IP, micro-mobilidade IP, sMIP, MOICANE, 802.11

TITLE: MOBILITY PROTOCOLS FOR IP TERMINALS

Abstract

All IP mobility protocols currently proposed on the IETF assume that the mobile nodes always have a mobility-aware IP stack, which is still a scenario that can seldom be found nowadays. Most terminals, including the laptops and PDAs which most would benefit of the mobility support, still use legacy IP stacks, limiting their use to layer-2 mobility within a single IP subnet. Currently, there exists evidence that the need of special mobile stacks for the terminals may be holding the generalization of this service.

This document will study and develop a complete arquitecture for global and efficient mobility support for all possible existing legacy IP terminals. This solution will be based on a new micro-mobility proposal – Terminal Independent Mobile IP (TIMIP) – the result of an R&D work by the author that includes both novel and similar features of previous proposals, coupled with a custom macro-mobility proposal – sMIP – based on standard MIP.

Keywords: TIMIP, IP mobility, IP micro-mobility, sMIP, MOICANE, 802.11

Agradecimentos

Em primeiro lugar, desejo agradecer com destaque especial, ao Prof. Mário Serafim Nunes pela sua orientação e conhecimentos que sempre me transmitiu, os quais foram essenciais no desenvolvimento do presente trabalho, bem como pelo facto de sempre me ter assegurado as condições operativas para o desenvolvimento do mesmo. Neste nível de agradecimentos desejo ainda englobar o apoio precioso da Prof. Teresa Vazão, a qual desempenhou efectivamente um papel de co-orientação do trabalho, em todos os seus aspectos.

São ainda devidos um reconhecimento de agradecimentos aos meus colegas do projecto MOICANE, nomeadamente António Grilo, José Calhariz, Pedro Catelas, e o líder da ilha de Lisboa, prof. Augusto Casaca, por terem, em conjunto, participado directa ou indirectamente em componentes desta Tese.

Este projecto foi ainda possível, pela atribuição da bolsa de Mestrado financiada pelo INOV durante toda a duração do mesmo, facto este que agradeço.

Por último expresso a minha gratidão aos meus pais pelo apoio e incentivo que sempre me transmitiram, e a todos os meus amigos, em especial os de longa data Bruno Espadinha, Vitor Cristina, Pedro Virote, Nuno Baptista, Joana Pimentel e Cristina Ribeiro, pelo interesse e incentivo.

Índice

Lista de Apêndices

Lista de Figuras

Lista de Tabelas

1. Introdução

1.1 Enquadramento

Presentemente, evolui-se no sentido de unificar todas as redes sob o denominador comum do protocolo IP, tornando a Internet cada vez mais importante e complexa. Quando este objectivo for atingido, haverá grandes benefícios decorrentes da possibilidade de todos os equipamentos poderem estar ligados entre si, utilizando a mesma rede para usufruir de diferentes tipos de serviço.

No cenário actual, o único serviço existente - transporte genérico de dados - permite-nos utilizar um conjunto de aplicações que fazem parte integrante da Internet actual, como o correio electrónico, a transferência de ficheiros, ou o comércio electrónico, aplicações estas que são em grande parte as grandes responsáveis pelo sucesso objectivo que actualmente já é dominante nas redes de dados.

No entanto, a sua viabilidade como **a** rede única vai depender da sua capacidade de expansão para outros tipos de mercados, com características substancialmente mais exigentes que os actuais e fortemente condicionado pela possibilidade de introdução de novos serviços – como o transporte de voz, áudio e vídeo – através dos quais se ganhe acesso a novos tipos de aplicações, como sejam a voz sobre IP, videoconferência, ensino à distância ou aplicações de entretenimento, entre outras, que se podem revelar bastante atractivas, e essenciais para fidelizar novos utilizadores.

Contudo, tais aplicações necessitam também de requisitos de qualidade de serviço, que a Internet actual através do seu paradigma *Best-Effort* não está preparada para oferecer, por genericamente não oferecer garantias no serviço do transporte de informação.

Existe ainda uma outra situação que vai ter um enorme impacto no futuro da Internet, que é despoletada pela expansão do mercado das redes locais sem fios. Neste tipo de redes, onde os utilizadores não têm necessidade de terem um suporte de conectividade física fixa, podendo movimentar-se livremente, capacidade esta bastante apelativa sobretudo no contexto das novas aplicações.

No entanto, de uma forma semelhante, a Internet actual também não está preparada para este fenómeno de mobilidade dos terminais, devido ao tipo de encaminhamento que aplica à informação que nela circula.

Desta forma, as novas aplicações conjugadas com a mobilidade abrem novas perspectivas para os utilizadores da Internet, mas do ponto de vista tecnológico, representam um desafio significativo, não existindo ainda os mecanismos de suporte necessários generalizados na Internet.

Contudo, o desenho modular desta rede, que permite que sejam criados novos protocolos IP para fornecer os requisitos desejados, vai possibilitar a extensão gradual da Internet inicial para a do Futuro, de forma a responder a estas novas funcionalidades, mas mantendo a compatibilidade com toda a estrutura e protocolos já existentes.

Relativamente aos problemas descritos – ausência de mecanismos de suporte de qualidade de serviço e de suporte de mobilidade – ambos identificados há vários anos, foram criados grupos de trabalho específicos no Internet Engineering Task Force (IETF) [1], organização responsável pela normalização das tecnologias IP, com a finalidade de estudar e resolver cada um deles, definindo propostas para tal.

O suporte de qualidade de serviço foi estudado sobre diversas vertentes, nomeadamente para redes de acesso e core, em que os aspectos de qualidade *vs* escalabilidade são totalmente diferentes, dando origem a diferentes propostas de solução que se podem utilizar de forma integrada.

O suporte da mobilidade foi também estudado em diversas vertentes, nomeadamente na mobilidade em larga e pequena escala, as quais diferem bastante nos aspectos de desempenho, escalabilidade e velocidade das movimentações. Como inicialmente o suporte de micro-mobilidade podia ser realizado de uma forma limitada com a tecnologia sub-IP já existente, então foi dada prioridade à mobilidade em grande escala, que não tinha qualquer suporte, sendo só posteriormente dada atenção à micro-mobilidade.

Evolução do suporte de mobilidade na Internet:

Durante a evolução da Internet o suporte da mobilidade teve que ser adicionado ao protocolo IP, uma vez que este incluí na sua arquitectura um aspecto de desenho que inviabiliza a mobilidade nativa dos terminais na rede, tendo esta característica sido herdada desde os primórdios da Internet, e continuamente mantida por forma a respeitar a compatibilidade

anterior com os terminais que não tenham estas extensões de mobilidade – os terminais legados (*legacy terminals*) – que têm apenas a pilha de protocolos IP básica.

Esta opção de desenho foi essencial para que, com a tecnologia da altura, se pudesse concretizar protocolos de encaminhamento suficientemente escaláveis para realizar o encaminhamento dos pacotes dos potenciais biliões de destinos possibilitados pelo endereçamento de 32 bits.

Para isto, verificou-se que a Internet como um todo seria substancialmente mais fácil de encaminhar os pacotes no seu interior se esta tivesse uma estrutura hierárquica, na qual os nós fossem agrupados em domínios, redes e subredes IP. Neste sentido, o endereço IP de um qualquer nó da Internet contém intrinsecamente em si uma parte da informação da sua localização, estando este identificador associado à sua subrede.

Usando esta opção de desenho, possibilita que os protocolos de encaminhamento considerem apenas redes inteiras, ao invés dos nós individualizados, o que reduz em várias ordens de grandeza o número de diferentes localizações a considerar, dado que assim apenas terão a complexidade de descobrir as localizações das redes como um todo.

Depois desta decisão estrutural da Internet, esta sofreu algumas evoluções, que nunca alteraram esta premissa inicial de forma a não quebrar a compatibilidade com a estrutura já existente, e resultando na Internet actual.

No entanto, é exactamente este premissa que invalida a mobilidade dos terminais móveis IP, porque não lhes vai permitir saírem do interior da sua rede de origem, uma vez que aí o seu endereço IP já não reflecte correctamente a sua localização física.

Nesta situação, o terminal poderia mudar de endereço para um da sua nova rede, mas isso implicava que todas as comunicações já estabelecidas seriam necessariamente perdidas, e a actualização de todos os interlocutores do terminal com o seu novo endereço.

Tal como já foi referenciado, para resolver este problema foram estudados mecanismos que pudessem adicionar esta funcionalidade desejada, mas com a característica de serem transparentes, por forma a não alterarem o aspecto básico do encaminhamento seguido pelos nós ao longo da Internet, mantendo assim a compatibilidade anterior.

Para isto, o protocolo MIP consegue criar mecanismos que permitem a comunicação entre os terminais fixos e móveis, sem que os primeiros se apercebam da mobilidade dos segundos, mas no entanto, a arquitectura deste protocolo considera que é necessário alterar tanto a rede

para adicionar estas funcionalidades, como também os próprios terminais móveis que beneficiam do serviço de mobilidade.

Esta situação deve-se ao facto de ser o terminal móvel a entidade natural onde as funções *activas* do mecanismo de mobilidade deverão residir, uma vez que é este que se movimenta fisicamente. Neste sentido, esta solução reflecte perfeitamente a forma como está distribuída a inteligência na Internet no que respeita ao nível de rede, pois concretamente, esta está tanto presente no interior da rede (encaminhadores) como nos extremos (terminais), de tal forma que alterações de novas funcionalidade terão que ser propagadas em ambos, o que como é sabido, implica a alteração de um muito maior número de nós nos extremos em comparação com o interior da rede.

No entanto, e como comparação, este modelo *não* foi seguido nas comunicações de voz tradicionais, em que os terminais são relativamente simples, e têm apenas as funcionalidades mais básicas necessárias apenas para suportarem os aspectos básicos da comunicação, e para receberem ordens simples enviadas pela rede. Neste sentido, e como exemplo, a introdução da mobilidade dos clientes de telemóveis entre operadoras distintas (serviço de *roaming*) é um dos serviços que teve uma aceitação imediata, uma vez que foi implementado apenas com suporte do lado da rede, sem exigir alterações nos milhões de terminais móveis GSM existentes que beneficiam deste serviço.

Por outro lado, o serviço também não exigiu qualquer alteração nos restantes terminais, tanto entre fixos como móveis, pois vão continuar a comunicar da mesma forma com estes, usando o mesmo número (endereço) tal e qual como se estivessem localizados no interior da sua operadora normal.[1]

Ao contrário das redes públicas de voz, a Internet seguiu um caminho diferente, distribuindo a inteligência no nível IP (nível 3) em toda a sua extensão, característica esta derivada dos seus primórdios de desenho de uma rede altamente robusta e redundante, em que todos os seus nós podiam à partida ser utilizados para encaminhar pacotes IP pelas suas ligações, e também porque os terminais podiam ser utilizados num conjunto muito mais alargado de tarefas do que a simples comunicação.

[1] Este serviço das redes GSM é um bom paralelo para comparação com o suporte de mobilidade IP, com a excepção das extensão típica maior das redes dos operadores comparativamente às subredes IP.

No entanto, o grande salto da Internet ocorreu quando a grande maioria dos nós da Internet se definiram como *terminais*, que executavam principalmente aplicações dos utilizadores e acediam à rede, o que lhes permitiu passarem a ser encarados explicitamente como um fim, e não um meio. Com esta mudança estes terminais tornaram-se inteligentes ao nível das aplicações, mas também no nível 3 de forma a manterem a compatibilidade anterior que sempre guiou o progresso nas tecnologias de informação.

Estas circunstâncias explicam as dificuldades da introdução de novos serviços *ao nível de rede*, que por exigirem normalmente alterações na pilha de protocolos dos terminais, vão ser bastante difíceis de generalizar, devido à multiplicidade de terminais existentes na Internet, e nos quais variam as suas arquitecturas, modelos, sistema operativos, etc.

Esta orientação é patente na evolução do suporte de mobilidade IP na Internet; de início concentrou-se em fazer uma arquitectura básica apenas com a transparência e escalabilidade suficientes para possibilitar a mobilidade entre redes, que resolvesse os problemas mais prementes relativos à concretização do serviço, como a transparência, complexidade do sistema e segurança, tendo posteriormente esta arquitectura sido estendida com outras propostas que visaram os aspectos em falta, como sejam as opções adicionais de integração, a eficiência do encaminhamento, optimização das transições, etc. Foi nesta altura que estes desenvolvimentos introduziram a divisão mais relevante da mobilidade IP, em micro e macro mobilidade, sendo esta essencial para aplicar estas optimizações de uma forma separada do protocolo MIP clássico.

No entanto, em toda esta evolução, a inteligência continuou sempre distribuída da forma inicial, uma vez que *todas* as propostas apresentadas exigiram que os terminais móveis fossem sempre alterados relativamente aos terminais iniciais (***legacy***) para deterem das funcionalidades normalizadas MIP, e/ou de outras funcionalidades proprietárias, o que invalida a aplicabilidade da tecnologia a *qualquer* terminal.

Mesmo depois da tecnologia estar suficientemente estudada e demonstrada a sua execuibilidade (fruto da experiência dos últimos anos), esta continua a pertencer praticamente apenas ao domínio de investigação académica, e a alguns poucos produtos empresariais isolados e sem expressividade relativamente a uma utilização generalizada[2].

[2] Como exemplo o produto Skamania da Intel

Nestas circunstancias pode acontecer que esta tecnologia não tenha impulso nesta linha de orientação, enquanto não existir uma oportunidade chave que possibilite a substituição de todos os clientes da rede, e que incorpore as novas funcionalidades em falta. Uma oportunidade destas será a nova versão do protocolo IP – IPv6 – mas que poderá nem chegar "realmente" a acontecer, a curto ou mesmo a médio prazo, devido ao custo implícito da substituição dos terminais já existentes.

De referir contudo que as aplicações da tecnologia móvel IP para entidades IP que detêm de mobilidade natural só são limitadas pela imaginação, mas por outro lado por esta tecnologia tardar em se generalizar, levando a que as aplicações móveis verdadeiramente inovadoras não apareçam. Como todos os ciclos de interdependências, a evolução implica a sua quebra.

No entanto, comparando com a panóplia de novas funcionalidades e serviços desenvolvidos continuamente para os telemóveis das várias gerações, fica claro que uma das principais razões para esta falta de generalização passa pela necessidade de alteração da pilha de protocolos dos terminais móveis, dado que esta tem características substancialmente mais complexas da alteração das aplicações dos terminais.

Torna-se claro, que o suporte de mobilidade só teria a ganhar se, à semelhança das redes públicas de voz, se reconcentrasse a inteligência das entidades IP apenas no interior da rede, de forma a que o mecanismo de mobilidade fosse transparente para *todos* os terminais, num modelo em que os terminais móveis fossem seriam considerados legados (*legacy*), não tendo mais qualquer funcionalidade que as já existentes (nomeadamente as definidas no documento [27]), sendo neste caso a rede a efectuar todas as acções necessárias para este suporte de mobilidade.

Definição da Hipótese:

Com base nas circunstâncias supra referenciadas, esta Tese de Mestrado concentra-se no contexto do suporte da mobilidade IP, focando a questão concreta da procura de uma solução que suporte explicitamente a mobilidade de *qualquer* terminal IP ao longo de toda a Internet, solução esta que deverá seguir as linhas gerais já estudadas e normalizadas no IETF, por forma a criar um mecanismo altamente eficiente e optimizado, procurando-se diminuir ao máximo os períodos de tempo que interrompem a conectividade dos terminais móveis que são causados pelas acções do mecanismo de mobilidade.

1.2 Objectivos

O objectivo base desta Tese de Mestrado é o de definir e propor uma Solução IP de Mobilidade Global, que suporte qualquer terminal e que seja altamente eficiente, reduzindo ao mínimo os períodos de falta de conectividade dos terminais nas suas movimentações.

Esta solução terá duas componentes, a saber: a componente de micro-mobilidade, o resultado de um trabalho de I&D com o objectivo de criar uma nova proposta, com ênfase nos aspectos de micro-mobilidade que, em propostas anteriores, ainda não tenham sido resolvidos, bem como nas melhores características destas; e a componente de macro-mobilidade, compatível com o MIP e incluindo as características desejadas.

Um segundo objectivo, complementar do acima formulado consiste na especificação, implementação, teste e integração desta solução de mobilidade numa rede de acesso móvel, por forma a demonstrar na prática estes conceitos. Dado que este trabalho se desenvolveu no âmbito do projecto MOICANE, foi escolhida a rede de acesso *wireless* baseada em 802.11 para esta implementação prática, e na medida em que estes tipos de redes têm requisitos de mobilidade que se identificam totalmente para os objectivos desta tese.

Por último, lidou-se também com aspectos motivados pela utilização desta ilha no projecto europeu, como a integração da rede com as outras componentes da ilha do INESC, da integração com as ilhas dos restantes parceiros, e com o teste e avaliação da rede com aplicações *E-learning* e Multimédia, pelo que houve a necessidade adicional de se proceder à implementação e teste de mecanismos de suporte de QoS na rede de acesso, respeitando assim o âmbito do projecto Europeu em que se insere, pese embora o seu carácter complementar dos objectivos base desta tese.

1.3 Convenções de Redacção

Referências e Numeração

Ao longo do texto serão efectuados diversos tipos de referências, nomeadamente as referências bibliográficas que serão indicadas entre parêntesis rectos, por exemplo [25]. Referências a outros capítulos ou secções serão indicados entre parêntesis curvos, como por exemplo (4.2). Outras referências presentes no texto utilizarão o formato "**ver tipo-referência número"**, por exemplo "ver Figura 28", "ver Tabela 3" ou "ver Anexo 2".

Utilização de Termos e Siglas em Inglês

Afim de se manter a coerência com artigos e trabalhos previamente editados em publicações internacionais, optou-se por utilizar abreviaturas a partir do termo em Inglês, quer no que diz respeito ao trabalho original, quer em trabalhos de outros autores. Por exemplo, para Pontos de Acesso, utiliza-se a sigla AP, correspondente a *Access Point*, e LT, utiliza-se para Terminal Legado, *Legacy Terminal*. O glossário apresentado no fim do texto permitirá a consulta rápida do significado de cada sigla.

Além destas siglas, o texto usa também alguns estrangeirismos de palavras inglesas que são comuns no vocabulário técnico da área, de que são exemplos as palavras *Handover* (transição) ou *Overhead* (ineficiência). Sempre que é introduzido um novo estrangeirismo, acrescenta-se a sua tradução portuguesa entre parêntesis, sendo todos estes indicados ao longo do texto marcados com o formato *itálico*, sendo as suas traduções portuguesas presentes no glossário apresentado no fim do texto.

Por fim, no caso de algumas palavras totalmente comuns em Português corrente, optou-se não fazer esta distinção, como por exemplo para a palavra Internet.

1.4 Estrutura da Tese

Esta tese está estruturada em 6 capítulos e complementada com 22 anexos.

No primeiro foi efectuado o enquadramento e a motivação do problema, enunciados os objectivos do trabalho e definida a sua estrutura.

No capítulo seguinte, analisam-se os mecanismos genéricos utilizados para realizar a mobilidade IP, e quais destes podem ser utilizados para criar o suporte de terminais legados, bem como serem optimizados de forma a aumentar a sua eficiência, o que pode implicar uma diminuição da escalabilidade ou cobertura atingida. Depois deste estudo, são analisadas as propostas já existentes de mobilidade IP, de forma a verificar quais destas poderão responder aos objectivos desta tese, desenhando-se por fim as características da solução escolhida para tal.

O capítulo 3 descreve teoricamente esta solução global de mobilidade para terminais legados, sendo constituída por duas partes complementares. O suporte de micro-mobilidade é baseado num novo protocolo (TIMIP) criado explicitamente para a necessidade em questão, e que inclui optimizações estudadas no capítulo anterior, e o suporte da macro-mobilidade realizado com uma adaptação do protocolo standard MIP, sendo compatível com este, e com a inclusão

do suporte de terminais legados. Um resumo desta descrição teórica originou um *draft* RFC, submetido para apreciação no organismo IETF [89].

No capítulo 4 deste trabalho analisa-se a rede de acesso *wireless* do MOICANE, que foi utilizada para a demonstração prática da solução de mobilidade estudada nesta Tese. Assim, vai ser descrito o demonstrador internacional do MOICANE, a ilha do INESC e a rede de acesso 802.11, esta última em relação à sua arquitectura, constituintes, e interacções internas e externas. Este capítulo é complementado com a descrição sumária das tecnologias que foram utilizadas nesta rede de acesso, dividindo-se entre tecnologias de rede, suporte de QoS e uma descrição dos principais componentes do Sistema Operativo utilizado (Linux).

O capítulo seguinte continua o anterior, detalhando o trabalho de Engenharia efectuado na implementação da rede, analisando-se as entidades, protocolos e mecanismos que foram desenvolvidos, e as suas relações internas. Estas funcionalidades foram implementadas em exclusivo nos nós da rede, com base no sistema operativo Linux, que foi estendido com mecanismos adicionais programados em linguagem C. Por outro lado, certos mecanismos já existentes foram reaproveitados, sendo integrados ou costumizados para utilização em módulos das entidades da rede, nomeadamente as interacções com o *driver* 802.11, módulos de IP, encaminhamento, *forwarding*, NAT e *firewalling*. Neste capítulo também estão presentes os planos de teste, que se dividem em testes funcionais e de desempenho, com os quais se avalia a qualidade da solução proposta.

No último capítulo, apresenta-se as conclusões a respeito da arquitectura apresentada, dos resultados e das perspectivas de trabalho futuro.

Como complemento ao trabalho, são apresentados numerosos Apêndices, que tanto sistematizam informação já abordada ao longo da dissertação, como apresentam outros pormenores que apenas a complementam contêm pormenores de assuntos abordados ao longo da dissertação, relativamente ao estudo genérico de mobilidade (Anexos 1 a 3), detalhes da solução de mobilidade apresentada (Anexos 4 a 9), da implementação dos conceitos na rede de acesso utilizada (Anexos 10 a 15) e dos Testes efectuados (Anexos 16 a 22).

O trabalho termina com uma lista de referências bibliográficas, e com um Glossário dos termos e abreviaturas utilizadas.

2. Estudo de Soluções de Mobilidade IP

No capítulo anterior equacionou-se a motivação e o enquadramento desta Tese de Mestrado, que levaram à procura da solução de mobilidade IP com as características específicas já definidas, pelo que se justifica no capítulo actual a apresentação de um estudo teórico relativo aos protocolos de mobilidade IP, constituindo este a base inicial de trabalho para a posterior procura da solução final encontrada.

Este estudo teórico está dividido em três secções: de início, analisam-se as acções genéricas dos protocolos de mobilidade IP, e como estes se relacionam com a mobilidade dos níveis mais baixos. Para as acções essenciais do modelo genérico apresentado, a secção seguinte vai estudar exaustivamente as optimizações possíveis que aumentam a eficiência da mobilidade IP, ao diminuírem ao mínimo os períodos sem conectividade dos terminais móveis enquanto se movimentam, procurando pistas sobre a possibilidade de instanciar a mobilidade apenas do lado da rede, de forma a suportar os terminais legados.

O estudo teórico termina com a análise das propostas já existentes de mobilidade IP de forma a verificar se alguma se enquadra e cobre as especificidades da motivação desta Tese. Assim, são verificados os principais protocolos de mobilidade IP propostos no IETF, o organismo próprio para esta normalização.

2.1 Arquitectura global de um protocolo de mobilidade IP

Os protocolos de mobilidade IP são mecanismos transparentes que permitem que os terminais possam movimentar-se fisicamente *entre entidades de nível 3*, como diferentes redes IP ou entre encaminhadores, mantendo a sua conectividade total, sem obrigar a que os terminais tenham de mudar os seus endereços, e/ou reestabelecerem as suas comunicações enquanto se movimentam.

Tais protocolos são necessários porque o encaminhamento IPv4 assume a premissa de que os terminais estão sempre localizados no interior da sua rede de origem, o que possibilita aos protocolos de encaminhamento serem escaláveis por só considerarem redes inteiras, mas que invalida a mobilidade nativa dos terminais.

Para isto, os protocolos IP de mobilidade vão utilizar mecanismos de encaminhamento, de forma a que resulte num suporte transparente, não requerendo modificações substanciais para

além das entidades directamente relacionadas com a mobilidade, e sendo também transparente para as várias tecnologias de rede (nível 2), e aos protocolos de transporte (nível 4).

Ao longo da vida do terminal móvel, o protocolo de mobilidade IP está em permanente execução, verificando se as movimentações físicas dos terminais móveis implicam uma perda de conectividade IP, dado que só as movimentações físicas dos terminais que envolvam mudança na entidade IP de acesso do terminal é que obrigam à acção do protocolo de mobilidade.

Quando tal acontece, então o protocolo vai verificar a nova situação do terminal, activando-se para alterar os seus mecanismos de encaminhamento para reflectirem a nova localização do terminal. Posteriormente, estes só voltam a ser modificados na próxima mudança da entidade actual de acesso do terminal.

Por outro lado, nos instantes em que o encaminhamento estiver estável, então os mecanismos de encaminhamento estabelecidos são utilizados para encaminhar da forma especial *todos* os pacotes dos terminais móveis, quer sejam destinados ou emitidos por estes, da forma transparente já descrita, e de modo a que os interlocutores destes não tenham que sofrer alterações. Estes mecanismos podem também complementar os mecanismos de encaminhamento já existentes, tendo também que ser transparentes a estes, ou se tal for possível, podendo substituí-los.

Um problema da mobilidade ao nível IP consiste no facto dos protocolos de mobilidade não garantirem uma conectividade constante, dado que à medida que os terminais se movimentam torna-se necessário alterar dinamicamente os mecanismos de encaminhamento para as novas localizações. Normalmente, este re-estabelecimento só vai ocorrer depois que o terminal se movimente fisicamente para a sua nova localização, e que o próprio protocolo depreenda que o terminal deixou de estar contactável pela sua localização anterior.

Durante estas operações o terminal vai estar incontactável, uma vez que os mecanismos de encaminhamento tornaram-se inconsistentes por ainda considerarem a localização anterior do terminal, o que resulta na falta de conectividade deste por não poder emitir/receber os seus pacotes de dados.

Assim, vai-se considerar como perdas incorridas pelos protocolos de mobilidade apenas as duas componentes que são directamente relacionadas com o protocolo de mobilidade, o que concretamente se traduz pela: a) operação de descoberta do movimento e b) operação de actualização dos mecanismos de encaminhamento.

De fora, ficam as perdas naturais que não são directamente atribuíveis à acção de manutenção da mobilidade IP, que podem ocorrer quando os mecanismos de encaminhamento estão estáveis, como o enchimento de filas dos encaminhadores, o descarte de pacotes de baixa prioridade, erros de transmissão/*checksum*, etc., bem como as perdas introduzidas pelo nível 2 na operação de mudança física do terminal, nomeadamente a mudança de frequência, ou outras quebras de conectividade do meio físico.

Desta forma, os protocolos de mobilidade podem ser comparados entre si verificando a arquitectura do protocolo, a complexidade e acções de nível 3 que têm que ser efectuadas até que se restabeleça a conectividade IP, quando um terminal se movimenta entre dois pontos, ou seja, para comparar protocolos de mobilidade IP verifica-se em condições semelhantes de distância, topologia, etc., a latência necessária para completar o *handover* de nível 3.

2.2 Análise e optimização do tempo de transição dos terminais

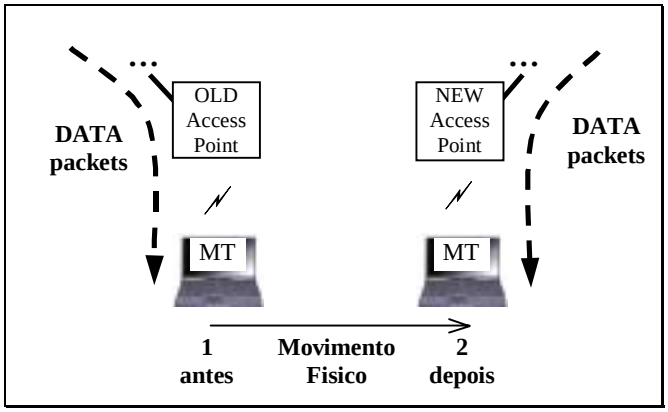


Figura 1: Visão global do handover

A situação genérica que origina perdas devidas à mobilidade IP está ilustrada na Figura 1, sendo esta secção dedicada à sua optimização até valores marginais. De início (**ponto 1**) o terminal está acessível por um dado ponto de acesso "**OLD**", enviando e recebendo pacotes de dados normalmente, pelos mecanismos de encaminhamento estáveis da mobilidade IP para a sua localização actual.

No entanto, pela movimentação física do terminal, o terminal vai transitar fisicamente para um novo ponto de acesso "**NEW**" correspondente a uma nova entidade de nível 3 distinta da

anterior[3], pelo que o fluxo de dados (seta a tracejado) é interrompido. Nesta situação, vai ocorrer o *handover* dos dois níveis, de forma que os fluxos de dados sejam reestabelecidos (**passo 2**); durante esta transição dos dois níveis, vai haver um período de tempo (ilustrado na Figura 2) no qual os pacotes de dados vão ser perdidos. Este tempo total de perda de conectividade deverá ser tão pequeno quanto possível (preferencialmente da ordem de milisegundos), para que cada movimentação física não obrigue à perda de demasiada informação do terminal.

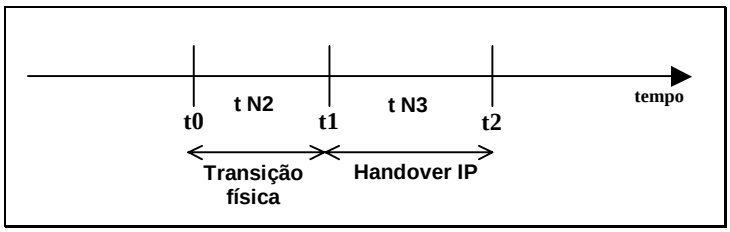


Figura 2: Handover de nível 2 e 3

Esta duração é constituída por duas componentes relativas aos dois níveis envolvidos, e que na aproximação mais simples, ocorrem de forma subsequente, sendo a primeira componente tN2 da exclusiva responsabilidade do nível 2, e compreende todas as acções necessárias para que o terminal transite de ponto de acesso, e volte a ter a conectividade física necessária para enviar e receber pacotes de dados.

Neste modelo, este tempo do nível 2 inicia-se no instante **t0**, quando a ligação é interrompida, e termina no tempo **t1** em que a ligação física é reestabelecida.

Dependendo das tecnologias específicas, o tN2 pode variar bastante de transição para transição, embora teoricamente possa ser minimizado para um valor marginal, como por exemplo se a tecnologia suportar a recepção de dados por várias formas em simultâneo, como se tivessem múltiplos canais ou interfaces de comunicação física disponíveis.

No entanto, para as tecnologias *wireless* (tecnologias sem fios) mais habituais em que o acesso ao meio físico é concretizado por uma única interface, existirá sempre um tempo apreciável tN2 nas transições dos terminais, podendo este ser variável consoante as frequências utilizadas, a latência da sinalização de nível 2, a distância e o tráfego dos pontos

[3] Sem perda de generalidade, neste estudo de mobilidade representa-se que a nova entidade de nível 2 é também coincidente com uma nova entidade de nível 3, de forma a que cada movimentação física origine um *handover* de nível 3.

de acesso, entre outros factores. Relativamente a esta latência, normalmente será apresentado um valor máximo, do qual se pode derivar a velocidade máxima do terminal a que ainda se consegue manter um serviço de qualidade.

Neste sentido, vai-se considerar que o nível 2 incorre numa latência mínima, da ordem dos milisegundos, de modo a que vão existir sempre pacotes de dados perdidos em cada transição, pelo que, o objectivo dos mecanismos de mobilidade de nível 3 será o de minimizar a perda *adicional* de pacotes directamente relacionados com o facto de a ligação de nível 3 ter que ser restabelecida (simbolizado na Figura 2 pela componente tN3).

Se este tempo de nível 3 também for minimizado para valores da mesma ordem de grandeza do tempo da movimentação física, ou inferiores, então a utilização da mobilidade IP não introduz nenhuma perda significativa da conectividade do terminal, mas este nível de desempenho do tN3 só é possível se o *handover* IP for explicitamente optimizado, para na maioria dos casos ser de rápido reestabelecimento.

Para isto, deve-se verificar que acções concretas é que têm que ser realizadas, de forma a deduzir as situações em que estas partes distintas têm o maior peso na latência do *handover*, sendo depois minimizadas com optimizações específicas para cada caso.

Os protocolos de mobilidade executam a operação crítica de *handover* dos terminais em duas fases subsequentes - localização e registo[4].

A primeira fase consiste nas acções do protocolo que são necessárias para este descobrir que a configuração de encaminhamento está inconsistente, estando o terminal inacessível devido ao seu movimento.

Para esta fase, os protocolos de mobilidade IP vão normalmente definir os seus próprios mecanismos *autónomos* de inferência da necessidade do *handover*, que embora sejam independentes de todas as tecnologias, conduzem a detecções tardias, por não saberem à partida o instante exacto que o *handover* passou a ser necessário.

Este fase é optimizada quando o nível 2 vai cooperar no processo de detecção, por via de *indicações* que oferecem uma noção bastante mais precisa dos movimentos físicos dos

[4] Existem denominações alternativas utilizadas na Literatura para os mesmos conceitos como *fase1 / detecção* para a fase de Localização, e *fase2* para o Registo.

terminais e os instantes que estes acontecem, e que permitem baixar substancialmente a latência desta fase em comparação com o método normal.

A segunda fase vai agrupar todas as restantes acções necessárias para que a configuração do encaminhamento móvel seja actualizada relativamente à nova localização do terminal, pelo que, certos elementos de rede dispersos pela Internet terão que ser informados a respeito da nova localização do terminal móvel, por via de sinalização específica dos protocolos de mobilidade IP. Para cada transição, a arquitectura do protocolo de mobilidade e a amplitude do movimento físico efectuado vão definir o número e a distância dos elementos de rede do terminal que têm que ser avisados para instanciar o *handover*, por via da alteração do seu encaminhamento móvel.

Nesta conformidade e grosso modo, a latência final desta fase corresponde ao tempo necessário para avisar *todos* estes nós, o que favorece as arquitecturas com características locais em que os elementos de rede a avisar estejam sempre perto do terminal e/ou sejam poucos em número.

A Figura 3 expande a figura anterior com os detalhes das componentes que participam em cada *handover* dos terminais, e as secções seguintes vão analisar em detalhe as possíveis optimizações para cada uma das fases em questão.

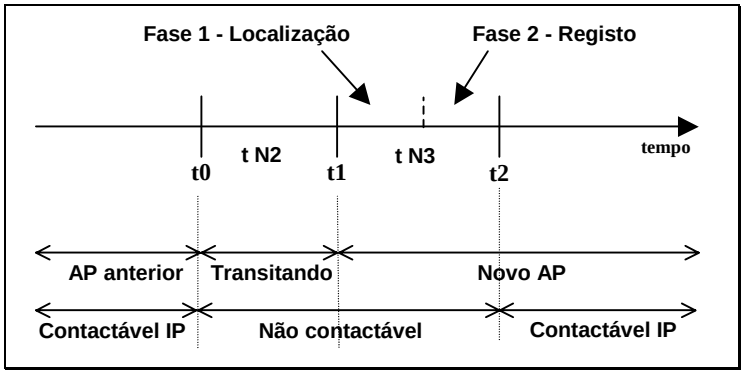


Figura 3: Componentes completos do handover

2.2.1 Optimização da fase de detecção

Relativamente à fase de detecção, existem vários modelos possíveis de integração da mobilidade IP com o nível 2, variando com as interacções/dependências existentes entre os dois níveis, a complexidade dos níveis relativamente ao caso normal, e o nível de desempenho atingido na acção de detecção, pelo que importa analisar com mais detalhe cada um destes modelos.

2.2.1.1 Acção Passiva

O modelo de integração mais simples possível, da acção de detecção, é aquele em que não existe nenhuma interacção entre os dois níveis, não existindo assim *qualquer* ponto de contacto entre os níveis. Apenas considerando esta premissa é que o mecanismo de mobilidade de nível 3 fica totalmente independente de todas as tecnologias, dado que esta é uma característica necessária nos protocolos de nível 3.

Esta situação implica que todos os protocolos de mobilidade IP terão necessariamente que possuir um modelo de detecção passiva, podendo este ser *complementado* com outras formas de detecção mais avançadas e eficientes.

A forma mais típica de concretizar esta acção é pela utilização de *beacons* (sondas), que são pacotes de dados periódicos que são emitidos em difusão com o objectivo de identificar o emissor junto dos receptores que lhe estejam no alcance.

À medida que os terminais se movimentam pela Internet, estes vão contabilizar os *beacons* recebidos dos elementos de rede, de forma a deduzirem os seus próprios movimentos físicos, detectando assim em que momentos é necessário realizar um *handover* IP, se perderam a ligação com o seu ponto de acesso actual. Isto acontece quando um terminal deixa de receber os *beacons* periódicos do seu ponto de acesso actual, conjugado com o aparecimento de *beacons* de novos pontos de acesso, que passaram a estar no alcance do terminal.

Este tipo de algoritmos são bastante simples, e completamente independentes das tecnologias, mas no entanto, estas funções de detecção do movimento requerem obrigatoriamente que o terminal detenha uma dose mínima de inteligência relacionada com o suporte de mobilidade, necessária para executar estes algoritmos passivos.

Uma característica inerente a esta classe de algoritmos é que conduzem a latências muito elevadas na fase de detecção, dado que o algoritmo não tem nenhuma indicação para inferir o momento exacto em que o terminal deixou de estar acessível pelo mesmo ponto de acesso, pelo que pode apenas questionar periodicamente o seu ponto de acesso actual para saber se este ainda está contactável (com um pedido de *beacon*).

Contudo, caso este não responda ao pedido de *beacon*, então o terminal não pode logo partir do princípio que este já não está contactável, uma vez que o pacote pode apenas ter sido perdido, pelo que, o terminal vai usualmente esperar que *vários beacons* não sejam recebidos até que tome uma acção.

De forma semelhante, o aparecimento de *beacons* de novos pontos de acesso não pode significar que o terminal decida imediatamente transitar para estes, uma vez que o seu ponto de acesso actual pode ser uma melhor escolha que os novos (nomeadamente por estes ainda estarem fisicamente longe, e proporcionarem uma conectividade inferior à do seu ponto de acesso actual).

Por último, refira-se que com esta forma de detecção o terminal só consegue detectar a necessidade do *handover* numa escala de tempo da ordem do *grão* do período dos *beacons*, que são enviadas pelos pontos de acesso (e sujeito às condicionantes atrás descritas). Este poderá ser diminuído, conduzindo a detecções mais rápidas, mas que também obrigam a uma ocupação excessiva dos recursos limitados, nomeadamente a largura de banda da rede *wireless*.

Todas estas interacções conduzem a que o terminal procure tomar decisões de uma forma lenta, e que lhe pareçam a cada instante as melhores possíveis, porque uma decisão precipitada poderá significar uma pior conectividade, além do peso do *handover* em si, significando isto que este modelo de detecção vai normalmente constituir a maior fatia do tempo total do *handover*.

2.2.1.2 Acção Reactiva

A forma mais simples de optimizar o modelo de detecção anteriormente descrito, será pela criação de um modelo *reactivo*, onde passam a existir pontos de contacto bem definidos entre o nível 2 e o nível 3, pela utilização de primitivas[5], dado que o primeiro tem uma noção muito mais precisa do momento em que a ligação física do terminal se alterou, o que possibilita ao nível 3 despoletar o seu *handover* em alturas mais antecipadas.

No entanto, este modelo quebra a independência do protocolo para todas as tecnologias, pois apenas naquelas onde existir este suporte especial é que vão suportar este modelo optimizado.

Para resolver este problema, os protocolos de mobilidade IP apresentam sempre como base um modelo de detecção passivo, igual para todas as tecnologias, e que pode ser optimizado com este modelo quando disponível, o que permite manter o estatuto de independência das tecnologias dos protocolos de mobilidade IP.

[5] Estas primitivas são equivalentes em funcionalidade aos *triggers* referidos em [18].

Dependendo de cada tecnologia específica, podem existir varias formas de o nível 2 ajudar o nível 3 a minimizar ou mesmo eliminar a fase de detecção, consistindo uma das mais simples consiste em o nível 2 associar informações relativas ao nível físico aos pacotes de dados que recebe quando os entrega ao nível acima. Desta forma, o nível 3 passa a ter informações que eram exclusivas do nível 2, como a potência do sinal dos *beacons* de nível 3 que vão sendo recebidos, o que ajuda de forma substancial a dedução dos melhores pontos de acesso para manter a conectividade de nível 3, e reduzindo-se assim, a fase de detecção do *handover* de nível 3.

Por outro lado, existem outras tecnologias que podem ajudar ainda mais a fase de detecção do nível 3, podendo mesmo reduzi-la para valores marginais, como acontece nas que definem um mecanismo próprio para a localização dos terminais no seu movimento, dado que aí o nível 2 terá a informação inequívoca da localização actual do terminal, bem como de todas as movimentações posteriores de uma forma completamente determinada, permitindo-lhe avisar o nível 3 imediatamente após a transição física. Na recepção deste aviso, o nível 3 do terminal pode começar directamente a sua fase de registo no seu novo ponto de ligação, o que significa que a grande latência incorrida pelos mecanismos lentos de detecção genéricos são eliminados.

Nestas condições, a repartição do tempo total do *handover* com esta optimização está esquematizada na Figura 4.

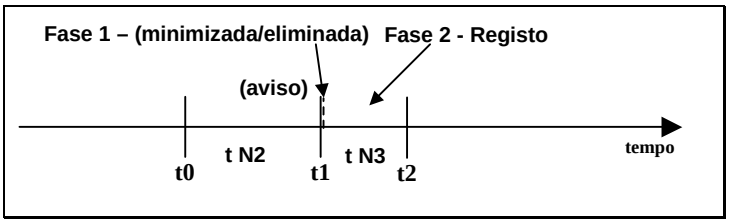


Figura 4: Protocolos reactivos

A principal dificuldade nestes mecanismos é que a adição da mobilidade IP às redes implica tanto a alteração do nível 3 dos elementos de rede, mas também do nível 2 de cada tecnologia específica, de modo a que ter-se-á que definir a alteração para cada uma delas em separado, potencialmente obrigando à costumização de partes do nível 3 para cada nível 2 particular[6].

[6] No entanto, este aspecto é minimizado definindo-se primitivas genéricas relativas às capacidades do nível 2, que o nível 3 usa apenas quando estiverem disponíveis.

No entanto, esta alteração do nível 2 é relativamente simples de implementar porque apenas *adiciona* funções de transferência de informações para o nível acima, deixando os mecanismos internos do nível 2 inalterados, como nomeadamente os algoritmos internos de escolha de pontos de acesso.

2.2.1.3 Acção Preditiva

Considerando o anterior modelo reactivo, então a latência do nível 3 poderá ficar reduzida apenas à necessária na fase de registo (fase 2), que não poderá ser completamente eliminada, porque cada *handover* obriga sempre ao aviso de um mínimo de elementos de rede.

Neste sentido, considerando que ambas as componentes restantes (tN2 e fase 2 de tN3) já são da mesma ordem de grandeza, e optimizadas até não poderem ser mais reduzidas, então a forma de minimizar ainda mais o tempo total do *handover* será o de executar ambas as fases em paralelo, o que só é possível se o *handover* de nível 3 começar *antes* do *handover* físico, aproveitando a conectividade física ainda existente, o que permite executar as duas componentes em simultâneo.

Para tal, a tecnologia de nível 2 terá que ter um comportamento mais complexo que no caso anterior, pois terá que *prever* com antecedência o movimento que o terminal vai executar, de forma a avisar o nível acima da nova localização do terminal *antes* de este começar a mudar. Quando receber esta previsão, o nível 3 vai tomar a iniciativa de começar o seu próprio *handover*, usando a conectividade que ainda detém pelo ponto de acesso anterior para informar a rede do seu próximo ponto de ligação. Pela característica de o nível 2 prever os movimentos dos terminais, então este modelo de detecção designa-se de modelo *preditivo*.

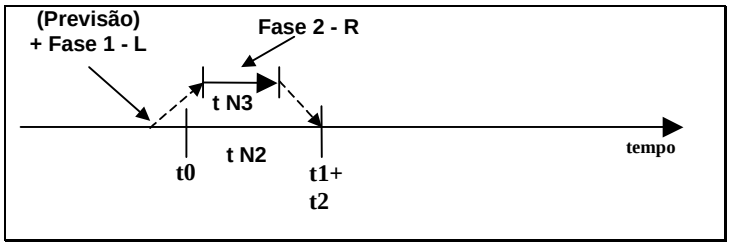


Figura 5: Protocolos preditivos

Usando este modelo, então o tN3 vai deixar de começar imediatamente a seguir a tN2, para começar sensivelmente ao mesmo tempo, o que pode tornar o tempo total do *handover* apenas

no maior dos dois (ver Figura 5), e como normalmente o tN3 será menor que tN2[7], isso significa que o tempo total do *handover* resulta apenas em tN2.

Este facto leva muitas vezes ao abuso de linguagem de se considerar que os protocolos de mobilidade IP com este suporte preditivo tenham uma latência de *handover* de "zero", o que não se verifica na realidade; uma descrição mais rigorosa será a de que este mecanismo poderá eliminar os pacotes que são perdidos *além* da latência do nível 2.

No entanto, este modelo preditivo introduz novas dificuldades à tecnologia de rede em utilização, o que limita as tecnologias a que se poderá aplicar este método, pois embora os *handovers* físicos de nível 2 continuem a ser da exclusiva responsabilidade do próprio nível 2, estes já não podem ocorrer a qualquer instante; pelo contrário, terão que ser previamente preparados pelo nível 2, de forma a este avisar o nível 3 e dar-lhe oportunidade para, enquanto há conectividade, iniciar o seu (Nível 3) *handover*.

Por outro lado, a utilização destas acções preditivas vão normalmente exigir ainda mais inteligência do nível 3 do terminal, para este ter possibilidade de reagir convenientemente no tempo correcto à predição indicada pelo nível 2, pelo que essencialmente, os dois níveis terão que ser bem sincronizados entre si, de tal forma a que os dois *handovers* ocorram preferencialmente em simultâneo[8].

Isto significa que a complexidade deste mecanismo pode ser motivo para originar piores resultados que os modelos anteriores, pois, se o nível 3 reagir com demasiada antecipação à previsão do nível 2, então poderá acontecer que os dois *handovers* deixem de ser simultâneos, de forma a que o nível 3 acabe antes do nível 2 sequer começar. Nesta condições, o terminal ficaria incontactável por um período alargado de tempo (ver Figura 6), dado que o *handover* antecipado do nível 3 cancela a localização anterior do terminal enquanto ainda está valida.

Tal situação pode ser resolvida por uma alteração no processo de registo denominada de *bicasting*, que ocorre durante um certo período de tempo depois de cada *handover* acontecer, nos quais os pacotes destinados ao terminal sejam enviados em simultâneo para *ambas* as localizações do terminal, possibilitando-lhe receber os seus pacotes em ambas as localizações

[7] Considerando as optimizações do registo, a descrever na secção seguinte

8 Em comparação, no modelo anterior, ao nível 2 bastava-lhe avisar o nível 3 "*à posteriori*", depois de o movimento físico ter sido completamente executado.

indiferentemente. No entanto, esta optimização vai aumentar a utilização dos recursos limitados do *wireless* em cada *handover*, mesmo nas situações em que tal não seja necessário.

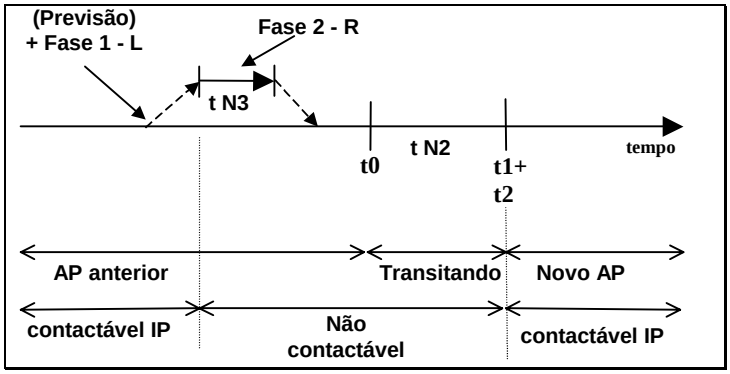


Figura 6: Protocolos preditivos (predição antecipada)

2.2.1.4 Acção Activa

O último modelo denominado de *activo*, e é o que apresenta o maior grau de interacção entre os dois níveis. Neste modelo, o nível 2 vai delegar no nível 3 todas as decisões relativas à sua própria transição física, o que só é possível pela exposição de um conjunto completo de todas as primitivas e informações, que naturalmente lhe seriam exclusivos, de modo ao nível 3 poder controlar todos os aspectos únicos de cada tecnologia particular.

Estes factores significam que não vai haver separação entre os níveis, e que algumas partes chave do nível 3 serão bastante complexas, e completamente customizadas para cada tecnologia de rede particular, o que vai totalmente no sentido oposto do modelo OSI clássico.

No entanto, a vantagem destes mecanismos é que assim o nível 3 poderá escolher com precisão o melhor momento para realizar a transição física do terminal, tornando trivial a combinação dos *handovers* referida anteriormente no modelo preditivo (Figura 5) sem os problemas que obrigavam à sincronização da acção previsão entre os níveis.

Outra função possibilitada por este modelo será o de o terminal iniciar o seu *handover* IP pelo seu novo ponto de ligação, e manter a sua conectividade pelo ponto anterior enquanto este se conclui, o que é possível porque o terminal pode transitar de frequências a pedido, ou a de escolher alturas mais propicias à execução do *handover*, quando por exemplo existam poucos pacotes prioritários a receber pelo terminal.

2.2.1.5 Comparação das optimizações da detecção

A tabela seguinte resume as opções existentes de optimização da fase de detecção do *handover* IP.

	Passivo	Reactivo	Preditivo	Activo
Independente das Tecnologias?	Sim	Sim (com primitivas genéricas)	Sim (com primitivas genéricas)	Não
Complexidade N2 + N3	Simples	Médio	Muito Complexo	Muito Complexo
Latência Total N3	Alta	Baixa	"0"	"0"

Tabela 1: Comparação das características dos vários tipos de mobilidade

2.2.2 Optimização da fase de registo

Tal como já foi referido, o modelo clássico da Internet define que os pacotes destinados a qualquer terminal são encaminhados para a respectiva rede de origem, onde por definição o terminal estará fisicamente.

Para proporcionar mobilidade aos terminais, os protocolos de mobilidade vão aplicar um encaminhamento especial aos pacotes dos terminais móveis, usando mecanismos genéricos de encaminhamento que são dispersos pela Internet desde a rede de origem até a localização actual do terminal.

São estes os mecanismos que terão que ser actualizados dinamicamente à medida que o terminal se movimenta, para manterem a conectividade ao terminal, pelo que, a fase de registo do processo de *handover* IP tem a função de contactar as entidades que participam no encaminhamento móvel do terminal, para que actualizem os seus mecanismos de encaminhamento com a localização actual do terminal.

Por via das optimizações descritas para a fase de localização, é esta fase que passa a constituir a maior fatia da latência necessária na transição dos terminais, o que resulta na perda de pacotes de dados. Esta latência é dominada pelo tempo necessário para contactar *todos* os elementos de rede envolvidos no encaminhamento móvel do terminal, que tal como já foi exposto, se estendem até à rede de origem do terminal[9] (ver Figura 7).

[9] A outra componente relevante da latência da fase de registo será o tempo necessário para o processamento das mensagens e as próprias alterações dos mecanismos de encaminhamento, sendo ambas desprezadas por dependerem da implementação.

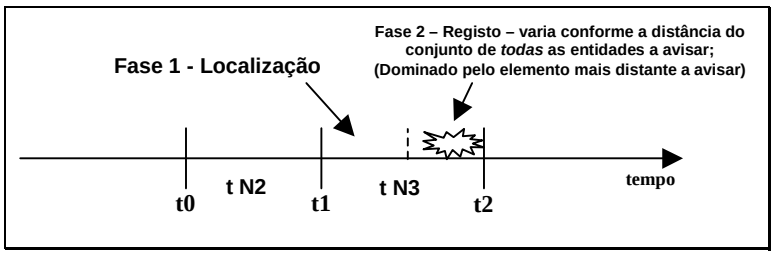


Figura 7: Variação da fase de registo

Isto significa que a fase de registo apenas terá latências baixas quando o terminal estiver perto da sua rede de origem; no caso genérico em que o terminal se movimenta numa parte da Internet distante da sua rede de origem, então as transições tornam-se pesadas constantemente, sem distinção relativamente ao tipo de movimentos executado pelos terminais (nomeadamente pequenos movimentos entre subredes ou grandes movimentos entre domínios IP).

Para resolver este problema, os protocolos IP de mobilidade incluem também optimizações específicas para a fase de registo, criando condições para que a maioria dos movimentos possa ser instanciada com uma fase de registo rápida, de modo a minimizar a latência total necessária nas transições. Pelo que foi exposto, isto só é possível se estes movimentos poderem ser instanciados sem que *todos* os elementos de rede tenham que ser avisados, limitando-se aos que estejam próximos do terminal.

Para isto, vai-se considerar separadamente os diferentes tipos de movimentos que os terminais podem efectuar em escalas diferentes, o que segue a divisão natural existente da Internet, onde os domínios administrativos são constituídos por redes IP, que por sua vez são divididos internamente em subredes IP, que contém os pontos de acesso por onde os terminais se ligam à rede. Neste sentido, vai-se considerar os movimentos *lógicos* que os terminais podem realizar nestas escalas, que normalmente correspondem em igual distância aos movimentos *físicos* dos mesmos (ver Figura 8).

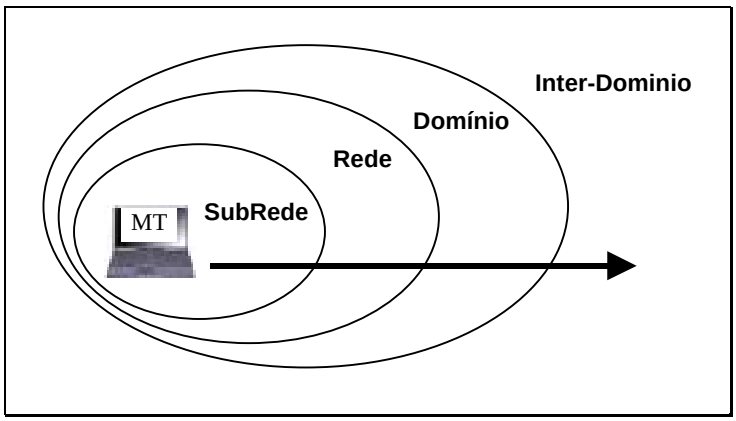


Figura 8: Escalas dos movimentos *LÓGICOS* dos terminais

Estas escalas consideradas têm características bastante diferentes entre si, nomeadamente em relação à distância física que o terminal irá percorrer, à frequência esperada do número de transições, e ao número de nós que têm que ser informados da sua nova localização.

Nestas circunstâncias, são os pequenos movimentos dos terminais entre subredes IP que deverão ser mais optimizados, por constituírem a maioria do total dos movimentos, procurando-se que só seja necessário avisar elementos de rede no interior da mesma rede;

No outro extremo da escala considera-se os movimentos lógicos longos dos terminais que envolvem transições de domínio administrativo. Normalmente, estas movimentações já têm por si só um tempo de nível 2 considerável, porque o terminal terá que se movimentar fisicamente de uma longa distância, podendo não existir uma cobertura física da tecnologia contínua.

Nestas condições, então a fase de registo vai ter condições para acompanhar esta latência elevada, permitindo-lhe contactar nós bastantes distantes do terminal, nomeadamente na sua rede de origem.

Para concretizar tais optimizações, os protocolos de encaminhamento são desenhados com arquitecturas hierárquicas que respeitam a divisão atrás delineada, tendo a característica que os elementos de rede têm apenas a informação da localização *aproximada* do terminal, ao invés da localização exacta do mesmo.

Desta forma, o encaminhamento dos pacotes dos terminais móveis é constituído por múltiplas partes, a serem aplicados em sucessão até chegarem ao seu destino (ver Figura 9). Esta aproximação tem a vantagem de que enquanto o terminal se movimentar no interior da sua área actual, a sua informação de localização continua válida nos níveis superiores, o que evita a sua actualização.

Neste sentido, apenas têm que ser actualizadas as escalas mais internas, que por estarem próximas do terminal apenas vão requerer um tempo de registo reduzido (ver exemplo na Figura 10).

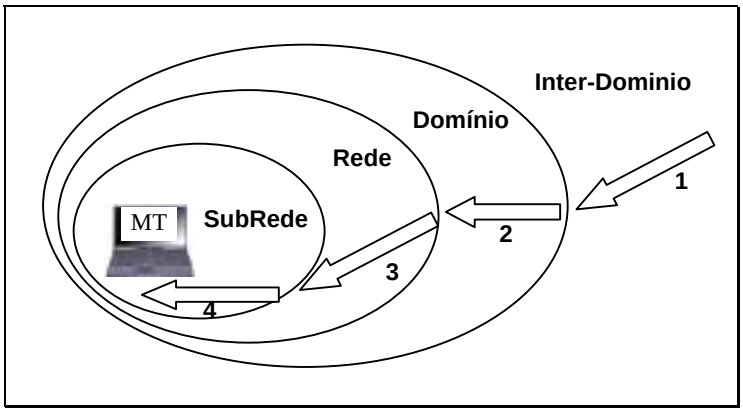


Figura 9: Mecanismos de encaminhamento móvel hierárquicos aplicados em sucessão

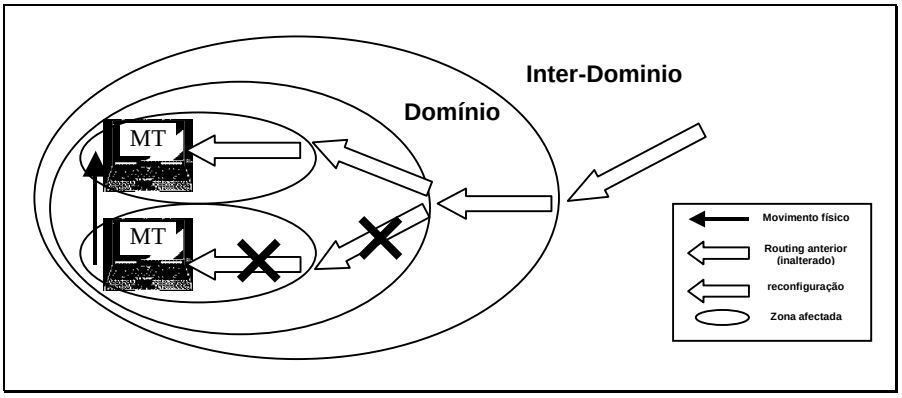


Figura 10: Mecanismos de encaminhamento móvel hierárquicos (acção local)

No entanto, dado o desenho da Internet, desde cedo se notou que a divisão mais importante e necessária seria a de distinguir o suporte da mobilidade em *dois* níveis distintos, consoante os terminais se movimentam dentro e fora dos domínios inteiros IP, o que permitiu de imediato o desacoplamento da maioria dos registos junto da rede de origem do terminal, que como foi descrito era o factor mais crítico no aumento da latência do registo.

Esta escala intermédia foi escolhida principalmente porque marca o limite máximo até onde se podem aplicar um certo tipo de mecanismos não-escaláveis para zonas mais extensas da Internet, e porque (tipicamente) marca também até onde é que a rede é gerida por uma entidade única, o que é essencial para a adopção de mecanismos uniformes que impliquem alterações mais substanciais à infra-estrutura já existente.

Assim, estes dois níveis denominam-se de **macro** e **micro mobilidade**, que vão conciliar de forma simples o melhor desempenho da maioria dos movimentos curtos, com melhor

escalabilidade para a minoria dos movimentos longos. No entanto, esta divisão não é totalmente rígida, podendo os protocolos desenhados para o suporte de macro-mobilidade poderão também ser aplicados a escalas mais típicas de micro-mobilidade e vice-versa.

Por outro lado, esta divisão conduziu ao aparecimento de um único protocolo de macro-mobilidade (MIP), que é uma condição necessária para o suporte global de mobilidade, sendo complementada por uma panóplia de protocolos de micro-mobilidade complementares e/ou alternativos entre si.

2.2.2.1 Análise da Macro-Mobilidade

Neste modelo, a macro-mobilidade, que será única ao longo de toda a Internet, vai suportar a mobilidade a uma escala *global* que permite a movimentação dos terminais para qualquer zona da Internet sem limitações.

Nesta escala, o grão do protocolo será os domínios IP como um todo, pelo que este gere apenas as movimentações dos terminais *entre* os domínios IP, que são bastante mais raras que as correspondentes do tipo complementar de micro-mobilidade. Por outro lado, nesta escala permite que o protocolo seja instanciado com um único elemento de macro-mobilidade por domínio, o que é uma característica importante para protocolos que pretendem ser implementados ao longo de toda a Internet.

Neste sentido, o desempenho típico da macro-mobilidade está ilustrada na figura seguinte (Figura 11), sendo a latência total a soma das três componentes já descritas, sendo esperado que a fase de registo seja elevada, dado que obriga ao contacto de elementos de rede fora do domínio actual do terminal (nomeadamente a rede de origem), mas isso não terá um impacto excessivo nas transições dos terminais, dado que será um acontecimento raro, e porque na prática estes movimentos estão normalmente associados a um tempo elevado de nível 2, motivado por mudança de tecnologia física ou por falta de continuidade da cobertura do *wireless* (embora teoricamente também se possam considerar condições perfeitas de cobertura do nível 2 neste tipo de movimentações de grandes distâncias).

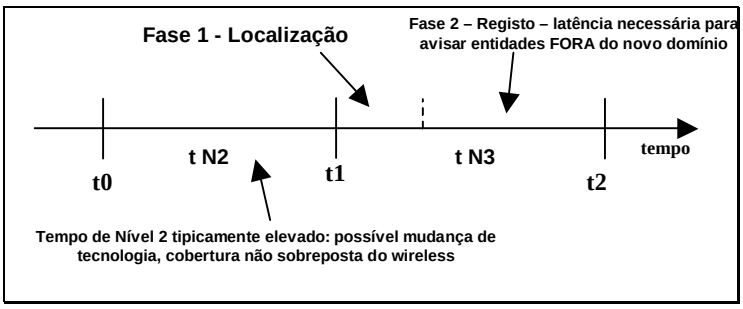


Figura 11: Macro-Mobilidade com fase de registo optimizada

2.2.2.2 Análise da Micro-Mobilidade

O complementar do modelo anterior é a micro-mobilidade, onde se considera o suporte de mobilidade apenas no interior de um único domínio IP, o que permite a existência de múltiplos protocolos de micro-mobilidade alternativos, com características distintas mais apropriadas para cada domínio particular.

Assim, no interior do domínio, o protocolo vai operar a uma escala *local*, sendo o seu grão os constituintes básicos de nível 3 mais próximos do terminal, de forma a que esta característica permite um controlo muito mais preciso do movimentos dos terminais, e possibilita a utilização de mecanismos mais complexos e eficientes, que só escaláveis para extensões limitadas da Internet como os domínios IP.

Dado que estes elementos estão bastante próximos dos terminais, criam-se as condições para que as fases de registo sejam muito rápidas, com contactos locais que são realizados rapidamente, dado que nunca envolvem contactos no exterior do domínio como nomeadamente o domínio de origem do terminal.

Nesta conformidade, o desempenho típico da micro-mobilidade está ilustrada na figura seguinte (Figura 12), onde tanto o tempo de nível 3 será baixo, fruto das optimizações locais descritas, bem como o tempo de nível 2, dado que existirá sempre uma continuidade na cobertura física do *wireless*.

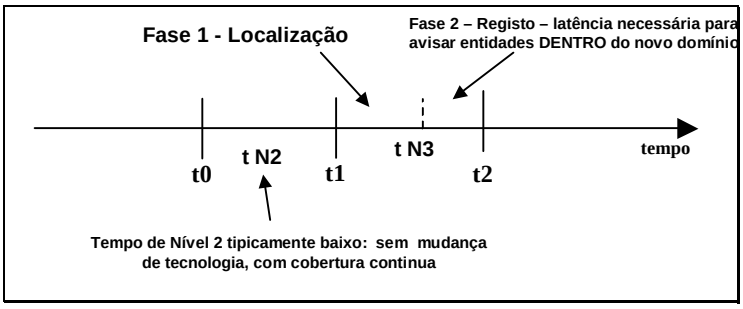


Figura 12: Micro-Mobilidade com fase de registo optimizada

2.2.3 Conclusões da optimização da mobilidade IP

As versões iniciais dos protocolos de mobilidade foram criados para resolver o problema do suporte de mobilidade na Internet, em que o objectivo inicial era apenas o de fornecer a conectividade aos terminais móveis nas alturas em que estão localizados nas redes.

Com estes protocolos, o utilizador tem a opção de gozar de uma conectividade constante, mas não permanente, dado que esta é interrompida temporariamente em certos instantes quando se movimenta (especialmente quando o terminal estiver localizado longe da sua rede de origem), de tal forma que o utilizador consegue notar esta quebra como motivada pelo suporte da mobilidade IP.

A geração seguinte de protocolos já considera explicitamente este problema, pelo que inclui as optimizações descritas especificamente para as transições dos terminais. Com a utilização da detecção optimizada e do registo local, passa a ser concretizável que os terminais detenham mobilidade permanente à escala global, incorrendo apenas num ligeiro aumento dos períodos de falta de conectividade já existentes motivados pelo nível 2, de forma a que o utilizador não consiga notar a existência da mobilidade IP. Esta nível de conectividade IP praticamente ininterrupta do nível 3 é denominado por "*seamless handoff*".

2.3 Resumo e Análise da Soluções IETF já propostas

Pelo que foi considerado no capítulo Introdutório deste trabalho, o objectivo deste Tese será o de desenvolver uma solução global de mobilidade IP para terminais legados, optimizada para diminuir os períodos sem conectividade nas transições.

Após terem sido verificadas nas secções anteriores tanto a arquitectura genérica do suporte de mobilidade, como as optimizações que diminuem a fase de transição, esta secção vai analisar a evolução do suporte de mobilidade IP no IETF, sendo estudados os protocolos propostos neste organismo.

Cada um destes será analisado numa perspectiva crítica, procurando-se verificar as suas melhores características e defeitos que sejam relevantes para a concretização do Objectivo formulado nesta Tese de Mestrado.

Durante os últimos anos, foi desenvolvido um esforço contínuo no IETF para o estudo do suporte da mobilidade IP, pois como referido anteriormente, o protocolo IP inicial não tinha suporte necessário para a mobilidade dos terminais, mas o seu desenho modular sempre

permitiu que se criassem, à medida das necessidades, novos protocolos que forneçam os requisitos desejados.

Isto permitiu ao IP ser estendido gradualmente com as novas funcionalidades, enquanto se mantêm a compatibilidade com toda a estrutura e protocolos já existentes. No caso da mobilidade, este esforço foi centralizado no grupo de trabalho "mobile IP" [3], que tem a responsabilidade de desenvolver e normalizar os mecanismos necessários para o suporte da mobilidade dos terminais na Internet, bem como de os integrar com as outras tecnologias IP emergentes, como o suporte de QoS ou a mobilidade em zonas NAT da Internet. Até ao presente, esta evolução seguiu um processo faseado por etapas, de que se salientam:

A primeira etapa em que foi criado um protocolo que resolvesse a necessidade mais pertinente que existia no suporte de mobilidade: o suporte de mobilidade a uma escala global, com o mínimo de alterações e com a escalabilidade necessária. Tal aconteceu porque o suporte da mobilidade no interior das redes IP já podia ser realizada do uma forma limitada pela tecnologia sub-IP já existente. Assim, desenvolveu-se um protocolo simples e escalável – o Mobile IP (MIP), para responder a esta necessidade.

A extensão, qualidade, e oportunidade temporal da solução encontrada, significaram que este protocolo se tornou a arquitectura de referência da mobilidade IP, possibilitando que a versão inicial do protocolo tenha sido posteriormente complementada com novas funcionalidades e com optimizações, mas sempre concentradas no aspecto fundamental da Macro-Mobilidade.

A segunda etapa consistiu na criação de protocolos de Micro-Mobilidade, que complementam o MIP na acção do suporte de mobilidade limitada no interior de domínios e redes IP.

Embora o MIP também possa ser utilizado neste contexto, os novos protocolos, tendo sido desenhados para esse objectivo específico, são mais eficientes, levando a tempos de sem conectividade menores, e por não operarem ao longo de toda a Internet, tiveram condições para introduzir outras optimizações e características especiais que o MIP não possuía, particularmente úteis quando se pretende que a mobilidade se realize com os terminais permanentemente ligados, tais com *handovers* locais e suporte de *paging* (consumo de baixa energia).

Só muito recentemente, surgiu uma nova proposta que tenta unificar as duas linhas de mobilidade IP existentes numa só, ao integrar o suporte optimizado de micro-mobilidade transformando a arquitectura base do MIP numa estrutura hierárquica. No entanto, este novo tipo de propostas só puderam aparecer como o resultado da experiência alcançada nos

protocolos de micro-mobilidade propostos, que mesmo assim não têm ainda o suporte de todas as características que estes suportam, como o *paging*, e as optimizações da fase de detecção.

Por outro lado, até ao presente, nenhuma das propostas de micro-mobilidade chegou a prevalecer, tendo permanecido todas em fase de *draft_WG*, sem progredirem para RFC.

Nesta situação e no presente, a solução mais flexível e eficiente que é escolhida para efeitos de investigação será a combinação dos dois tipos de protocolos: o MIP para a componente de mobilidade global de forma a respeitar a arquitectura normalizada, e uma componente de micro-mobilidade que optimiza a maioria das movimentações físicas dos terminais, podendo esta ser realizada com um dos protocolos já existentes, ou com uma nova proposta, dado que não existe nenhum standard aceite neste domínio.

2.3.1 MIP

O primeiro passo apresentado no IETF para o problema do suporte da mobilidade na Internet foi o protocolo MIP, para a versão 4 do IP [5], seguido da versão para IPV6 [6], com numerosas extensões e propostas adicionais, como as referenciadas de [7] a [12], tendo se tornado na solução standard de macro-mobilidade para IP. Além das referências originais, este protocolo já foi amplamente estudado, tanto no plano teórico como em implementação, noutros trabalhos [90] e [91].

Em ambas as versões, o MIP estende o protocolo IP com a capacidade de mobilidade para os terminais, que podem assim movimentar-se livremente para toda a Internet estando sempre acessíveis pelo seu endereço IP fixo, sendo este suporte vocacionado principalmente para a macro-mobilidade, e sendo concretizado de uma forma completamente transparente e automática, usando mecanismos escaláveis de encaminhamento, pelo que, o MIP vai ser transparente relativamente a todas as tecnologias, estruturas e tipos de topologia de rede, e mantém a compatibilidade com toda a estrutura da Internet já existente.

Para realizar o suporte da mobilidade, cada rede terá que possuir um novo nó fixo especial, denominado de Agente de Mobilidade, que vai gerir todas as operações de mobilidade, para os terminais que estão a visitar esta rede (papel de Foreign Agent), bem como aos terminais móveis pertencentes a esta, mas que estão a visitar outra rede (papel de Home Agent).

Além dos agentes de mobilidade, o MIP também terá que ser suportado nos próprios terminais móveis, tendo a responsabilidade de iniciarem e manterem todo o processo de

manutenção da sua conectividade, contactando caso a caso os agentes de mobilidade apropriados nas redes por que passam.

A arquitectura do MIP, incluindo as movimentações dos terminais móveis entre as redes e a diferença entre os agentes de mobilidade está ilustrada na Figura 13.

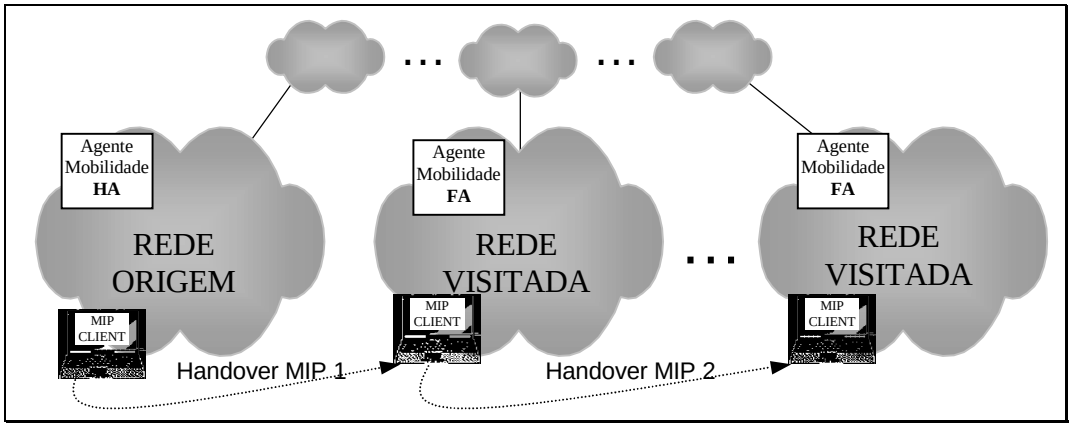


Figura 13: Arquitectura MIP

Para as redes sem suporte à Mobilidade por não terem o agente de mobilidade FA, foram posteriormente introduzidos mecanismos alternativos que permitem a mobilidade do terminal mesmo nestas redes, mas contudo no contexto MIP, o suporte de mobilidade terá no mínimo que ser *sempre* instanciado no próprio terminal, e no agente HA na sua rede de origem.

Quando o terminal estiver numa qualquer rede visitada, então este já criou em conjunção com o seu HA as condições para que possa receber o seu tráfego nessa localização e para isto, o HA reencaminha o tráfego destinado ao terminal móvel por um túnel IP para a sua localização actual. Dado os pacotes destinados ao terminal móvel serem transparentemente capturados e reenviados para a localização do terminal, isto torna o protocolo transparente para os outros nós da Internet, pois não terão que suportar o MIP para comunicarem com os terminais móveis.

Quando o terminal transitar fisicamente de rede, este vai perder a sua conectividade estabelecida, dado que o túnel estabelecido ainda aponta para a localização anterior. Para reestabelecer a conectividade na sua nova rede visitada, o terminal vai efectuar um *handover* MIP, para redireccionar o túnel para a localização actual.

Para isto, o terminal vai de início detectar a sua nova localização usando *beacons* MIP [25], e quando se der conta que já não está no mesmo lugar, vai informar o HA da sua nova localização, de forma a que este altere o destino do túnel para o novo FA.

Este aviso é suportado por sinalização MIP gerada pelo terminal, propagado desde a rede visitada do terminal até à sua rede de origem, de forma que, todos os movimentos entre redes do terminal só são efectivados depois de o HA do terminal ser avisado da sua nova localização.

AVALIAÇÃO: Contribuição do MIP para os objectivos desta Tese

Pelo que foi visto acima, o protocolo MIP é actualmente a referência standard no suporte escalável de macro-mobilidade, sendo essencial a característica de requerer poucas alterações nas redes IP para lhes adicionar o suporte de mobilidade.

No entanto, esta transparência não chega ao próprio terminal móvel, pois no MIP este é a entidade activa em todo o processo, não podendo desta forma ser legado, e acresce ainda não ter o MIP também nenhuma das optimizações do *handover* estudadas para qualquer das duas fases.

Concretamente, o MIP tem o seu próprio mecanismo de detecção do movimento do tipo acção passiva, que lhe confere a independência para todas as tecnologias de rede, mas que leva a detecções do movimento tardias, facto especialmente importante porque existem limites, da ordem dos *segundos*, para o período máximo de *beacons* trocados entre os clientes e os agentes de mobilidade, e que podem elevar a fase de detecção para esta ordem de grandeza.

Por outro lado, o MIP só está adaptado para suporte de macro-mobilidade, porque todos os movimentos dos terminais entre redes, quer sejam curtos ou longos, envolvem *sempre* um aviso ao HA do terminal, localizado potencialmente longe do terminal. Isto significa que nas transições MIP levam sempre a uma reconfiguração total, sem que se aproveitem os mecanismos anteriores já estabelecidos.

Assim, para responder aos objectivos desta Tese, o MIP poderá ser utilizado com a adição do suporte de terminais legados, mas terá que ser complementado por um protocolo específico de micro-mobilidade, uma vez que a sua utilização num contexto de micro-mobilidade implicava uma latência excessiva por cada *handover* dos terminais, que seriam claramente identificados pelo utilizador como da responsabilidade do nível IP, e não do nível 2, por simples comparação com as soluções clássicas com mobilidade baseada totalmente em nível 2.

2.3.2 CIP

O protocolo Cellular IP [14] (CIP) foi um dos primeiros de novos protocolos criados explicitamente para **complementar** o MIP com a adição de micro-mobilidade, detecção

optimizada, e outras funcionalidades não–escaláveis avançadas, que só foram possíveis de serem consideradas porque foi desenhado explicitamente para apenas fornecer mobilidade dentro de um domínio IP. Este protocolo está descrito em detalhe nas referências originais, bem como em [91].

Neste sentido, quando se integra o CIP com o MIP, vão existir simultaneamente os dois protocolos a operar, preocupando-se o CIP apenas com os movimentos no interior do domínio IP, e o MIP apenas com os movimentos entre estes domínios.

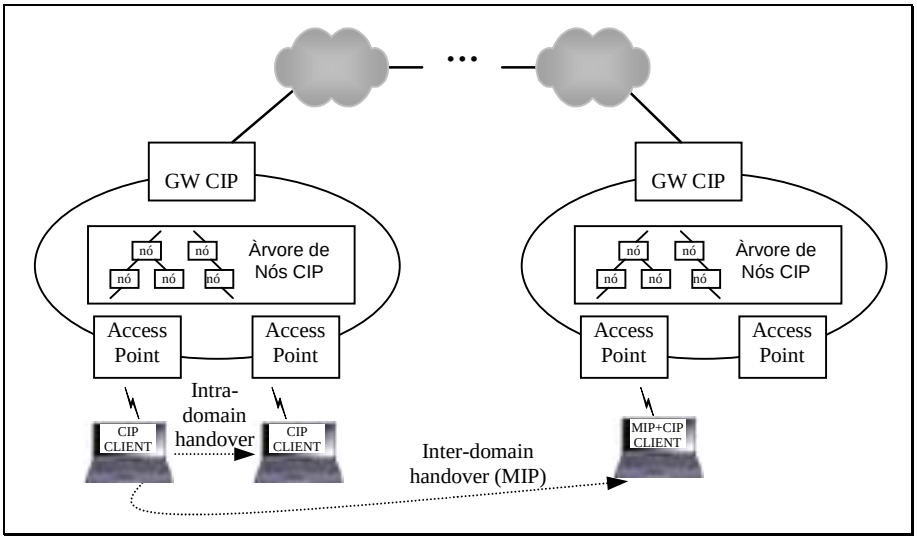


Figura 14: Visão geral da Arquitectura CIP

Na arquitectura do CIP, ilustrada na Figura 14, cada domínio CIP é constituído por uma árvore de nós CIP, contendo uma Gateway no topo, e pontos de acesso nas folhas. A GW CIP serve de ponto de controlo para as acções centralizadas, e é o único nó que tem o acesso ao exterior; por outro lado os pontos de acesso permitem que os terminais CIP acedam à rede.

Nesta conformidade, tal como no MIP, os terminais móveis também terão que ter o suporte do protocolo por via de clientes CIP, que lhes permitem participar num domínio CIP tanto na conectividade básica como na micro-mobilidade. Por esta razão, o CIP não permite o suporte de terminais legados nem mesmo na conectividade fixa.

O encaminhamento dos pacotes também é realizado de uma forma bastante diferente do MIP, pois em vez da utilização de túneis IP entre os agentes de mobilidade, no CIP cada terminal presente no domínio CIP vai ter um conjunto de entradas directas de encaminhamento criadas na árvore de nós CIP, desde o AP do terminal até à GW, em que cada uma indica apenas o próximo nó por onde o terminal está acessível, obrigando assim os pacotes a descer pela árvore sempre em sequência, mesmo para o tráfego gerado no interior da rede, desde a GW até ao AP actual do terminal.

Neste sentido, quando este transitar de AP, a sua conectividade é interrompida, uma vez que a parte final da cadeia de encaminhamento tornou-se incorrecta. Para concretizar a transição ao nível IP, o terminal vai iniciar o *handover* local CIP entre os dois APs envolvidos, começando por detectar a sua nova localização usando *beacons* específicos CIP, que troca com os APs CIP localizados na rede (modo de detecção passivo).

Por via deste método, o terminal vai-se dar conta que já não está no mesmo lugar, pelo que vai informar a rede acerca da sua nova localização, gerando sinalização específica CIP a ser propagada pela rede, desde o novo AP até à GW da rede. Cada nó que recebe a mensagem de localização altera a sua tabela de encaminhamento para indicar que o próximo nó para o terminal é quem lhe entregou a mensagem.

Desta forma, todos os movimentos entre redes do terminal só são efectivados depois do primeiro nó comum dos dois caminhos de encaminhamento (anterior e novo) ser informado – nó crossover - porque a partir deste a cadeia de encaminhamento mantém-se inalterada (ao contrário do MIP, que tinha um túnel único que não podia ser reaproveitado).

Tal como as outras soluções de micro-mobilidade, os movimentos dos terminais entre os domínios CIP terão que ser realizados com o protocolo de macro-mobilidade MIP (ou outro alternativo), tendo neste caso os terminais que suportar ambos os protocolos.

Além do suporte de micro-mobilidade, que reduz drasticamente o tempo de registo, o CIP também introduz teoricamente uma optimização para a fase de detecção, pois, além do mecanismo normal passivo, que lhe permite ser independente das tecnologias, o CIP também prevê um modo activo extremamente dependente da tecnologia, pelo qual o nível 3 controla completamente a mudança das frequências e a escolha dos pontos de acesso do nível 2.

Nesta optimização, o CIP define que quando vai acontecer um *handover*, o terminal muda para a nova frequência do novo AP, para lhe entregar apenas a sua sinalização CIP, voltando imediatamente para a frequência anterior, onde volta a receber pacotes. Depois de um tempo de espera, o terminal muda de novo em definitivo para a nova frequência, porque nessa altura o novo caminho já estará totalmente criado, o que lhe permite receber imediatamente pacotes de dados.

Este cenário só poderá ser utilizado quando a tecnologia de rede suportar estas funcionalidades avançadas, e mesmo assim quando o tempo de tN2 for pequeno, devido às várias mudanças de ligação física envolvidas; no entanto, se este modo for viável, então o tempo do nível 3 será praticamente marginal.

Por fim, o CIP introduz também novas características avançadas, como o conceito de suporte de *paging*, utilizado para aumentar a escalabilidade do protocolo e a autonomia dos terminais, e a função avançada ao conseguir manter o estado dos terminais activos apenas com os seus pacotes normais IP, evitando assim que estes tenham que explicitamente gerar sinalização para manter o estado.

AVALIAÇÃO: Contribuição do CIP para os objectivos desta Tese

Pela sua descrição, o protocolo CIP é uma escolha bastante boa para o suporte optimizado de micro-mobilidade que se pretende nesta Tese, dado que este protocolo optimiza convenientemente a fase de registo por garantir *handovers* locais à rede.

No entanto, tal como os outros protocolos, o CIP baseia todas as suas funcionalidades na assumpção de que o terminal móvel é uma entidade com inteligência relativamente à mobilidade, o que vai invalidar a utilização dos terminais legados. Em comparação com o MIP, este requisito ainda é mais pertinente, porque o CIP não suporta os terminais legados nem mesmo como terminais fixos, sem lhes fornecer conectividade mínima.

Por outro lado, a única optimização oferecida para a fase de detecção é baseada num mecanismo activo, difícil de implementar nas tecnologias de rede, o qual ainda dá mais importância ao papel do terminal no processo de mobilidade, quando o que se pretende é exactamente o oposto. Nestas circunstâncias, a forma de detecção padrão passiva que restava, apresenta uma latência tardia da mesma ordem que o MIP.

Acresce ainda que as outras características introduzidas pelo CIP não são relevantes para os objectivos principais a concretizar, pelo que o CIP não é a escolha ideal para a componente de micro-mobilidade que se procura, embora forneça pistas importantes de componentes de uma possível solução.

2.3.3 HAWAII

O protocolo HAWAII [15] foi proposto no IETF praticamente ao mesmo tempo que o CIP, para complementar o standard MIP com a adição da micro-mobilidade optimizada no interior de um domínio IP, de modo a que as movimentações efectuadas pelos terminais sejam sempre locais ao terminal, e no máximo apenas envolvendo entidades no interior do domínio (tal como o CIP).

No entanto, enquanto que o CIP se preocupa em adicionar micro-mobilidade e outras características novas, o HAWAII apenas (numa primeira fase) se preocupa com a adição de

micro-mobilidade que seja ***transparente*** aos clientes MIP já existentes, dado que estes deverão seguir a arquitectura standard MIP.

Desta forma, o HAWAII só vai alterar os nós da rede com o novo protocolo e os seus novos mecanismos associados, e por outro lado, por este ser compatível com o MIP, então os clientes MIP vão-se poder manter inalterados, transitando de FA em FA como no MIP clássico.

A diferença substancial neste cenário, é que quando o terminal mudar entre dois FAs pertencentes no mesmo domínio HAWAII, o *handover* é automaticamente local, limitado apenas à área destes FAs, sem envolver a rede de origem do terminal. Tal como no CIP, só quando o terminal necessitar de transitar de domínio é que ocorre um registo MIP normal.

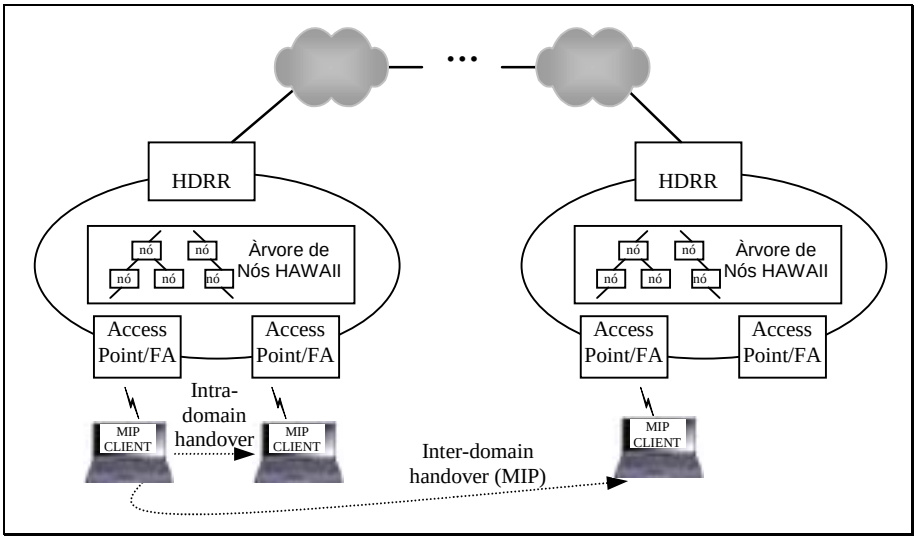


Figura 15: Visão geral da Arquitectura HAWAII

Para tal, o HAWAII considera uma arquitectura muito semelhante à do CIP, no sentido em que cada domínio é constituído por uma árvore de nós HAWAII, com um DHRR (*Domain Home Root Router*) no topo e pontos de acesso nas folhas, todos estes com funções semelhantes na arquitectura do CIP.

A grande diferença é que o terminal só terá que suportar um único protocolo de mobilidade, o MIP, que será utilizado para o suporte dos dois tipos de mobilidade. Neste sentido, tal como o MIP não suporta terminais legados, no caso do HAWAII esse problema vai-se manter.

Assim, quando o terminal estiver num domínio HAWAII, então já estão criadas nos nós da árvore desde o AP do terminal até ao DHRR uma cadeia de entradas directas de encaminhamento, em que cada uma indica apenas o próximo nó por onde o terminal está acessível.

Tal como no CIP, é esta cadeia de encaminhamento que permite que os pacotes destinados ao terminal móvel sejam encaminhados correctamente pela rede até chegarem ao AP onde está o terminal, mas com uma diferença substancial, que os pacote seguem *sempre* o caminho mais curto pela rede, beneficiando o tráfego local (ao contrário do CIP, que obrigava todo o tráfego a passar pela GW da rede).

Quando este se movimentar fisicamente e transitar de AP, então o terminal fica com a sua conectividade interrompida, e inicia um *handover* normal MIP para a reestabelecer. Para isto, o terminal vai de início detectar a sua nova localização, que será o FA presente no novo AP, usando o mecanismo genérico de detecção do MIP (passivo, baseado em *beacons*). Quando se der conta que já não está no mesmo lugar, então vai informar normalmente o HA da sua nova localização, entregando a sua sinalização MIP ao FA. No entanto o AP/FA verifica que este registo pode ser efectuado apenas com micro-mobilidade, pelo que em vez de o entregar HA, vai usá-lo para alterar as entradas de encaminhamento na zona da árvore entre os dois APs envolvidos, de forma a reestabelecer rapidamente a conectividade do terminal.

Desta forma, todos os movimentos entre redes do terminal são efectivados assim que os nós entre os dois APs tenham sido informados, dado que desde o nó crossover a cadeia de encaminhamento vai-se manter inalterada. No final do *handover*, o AP inicial do processo vai responder ao terminal móvel com a resposta standard MIP, o que finaliza de forma transparente o *handover* local do terminal, e tal como no CIP, este vai ser local porque os nós a alterar vão estar normalmente muito perto do próprio terminal, e mesmo no pior caso, nunca além do interior do domínio.

No entanto, por ser apenas um mecanismo transparente de micro-mobilidade para a arquitectura standard MIP, então o HAWAII não introduziu outras funcionalidades avançadas, como o *paging* (embora tenha sido posteriormente proposto em forma de extensão [16], mas que obriga a novas funcionalidades nos clientes, pelo que passam cada vez mais a serem clientes HAWAII ao invés de MIP), nem o refrescamento automático pelos pacotes de dados; no entanto, o encaminhamento dos pacotes internos ao domínio é mais optimizado que em comparação com o CIP, pois estes podem ir sempre pelo caminho mais curto pela árvore de nós.

AVALIAÇÃO: Contribuição do HAWAII para os objectivos desta Tese

Pelo que foi visto acima, o protocolo HAWAII é também uma escolha bastante boa para o suporte optimizado de micro-mobilidade, com a importante vantagem que estende a arquitectura standard MIP, não necessitando de novas alterações aos terminais se se

considerar que estes já são MIP. No entanto, mesmo usando a sinalização MIP, o HAWAII continua a basear todas as operações na base de que o terminal é inteligente e terá o suporte de mobilidade, o que novamente invalida o suporte de terminais legados; de igual forma ao CIP, o HAWAII nem sequer suporta os terminais legados como terminais fixos.

Além disto, por usar os clientes MIP, o HAWAII usa exactamente o mesmo mecanismo de detecção passiva que o MIP; como já foi descrito, esta forma de detecção revela-se bastante ineficiente, conduzindo a latências altas. Neste sentido, tal como o CIP, o HAWAII não responde satisfatoriamente às necessidades da micro-mobilidade desta Tese.

2.3.4 hMIP

O hierarquical MIP [17] é a mais recente proposta apresentada no IETF para o suporte optimizado de mobilidade, sendo no presente a única proposta com características de micro-mobilidade que está em processo de melhoramento[10]. O hMIP é uma proposta de extensão do MIP clássico para o tornar um mecanismo totalmente hierárquico no suporte da mobilidade dos terminais, que possibilita tanto *handovers* locais de micro-mobilidade, mas também *handovers* optimizados do tipo de macro-mobilidade. Neste sentido, o foco do hMIP será na mobilidade entre a micro e a macro mobilidade, sendo o MIP clássico um caso particular do hMIP.

Tal como o HAWAII, o hMIP só adiciona as optimizações do registo, sem adicionar outras opções mais recentes que o CIP introduz. No entanto, uma diferença essencial do hMIP para estes dois protocolos de micro-mobilidade é que este não é um protocolo novo, não introduzindo novas entidades arquitecturais. Pelo contrario, o hMIP só redefine as características e capacidades dos agentes de mobilidade já introduzidos no MIP, acrescentando novas funções aos clientes MIP.

Para isto, o hMIP vai dividir o suporte do MIP da mobilidade em N níveis hierárquicos, criando uma árvore de FAs, que encaminham os pacotes entre si **exclusivamente** por túneis IPIP [23]. Utilizando esta cadeia, quando o terminal se movimentar entre dois FAs que estejam debaixo do mesmo FA de nível superior, então o registo só se vai efectuar na zona da árvore afectada, porque os túneis anteriores mantêm-se inalterados.

[10] Actualmente, o documento *draft* de definição do HMIP está na sua 6ª versão (de Março de 2002)

Esta optimização do registo é que permite que só tenham que ser avisadas as entidades na vizinhança do terminal, diminuindo a latência da fase de registo.

Uma vez que o hMIP encaminha os pacotes exclusivamente usando túneis IP estabelecidos entre os diversos FAs, então este protocolo pode operar em qualquer topologia de rede, característica esta que já era a base do protocolo MIP, e que tanto implica a sua aplicabilidade imediata, como também que não poderá chegar tão próximo dos terminais quanto os protocolos de micro-mobilidade, uma vez que o encaminhamento no último troço continua a ser realizado pela forma clássica usando o par (rede/netmask).

Estas características significam que o hMIP tem o seu foco na mobilidade num nível intermédio entre micro e macro mobilidade, pois basicamente, o hMIP usa os métodos semelhantes aos protocolos de micro-mobilidade, mas mais escaláveis e distantes dos terminais, e por não necessitar que todas as entidades IP sejam hMIP, permite separar o suporte dos terminais móveis dos fixos. Em comparação, nos protocolos exclusivos de micro-mobilidade **todos** os terminais são móveis CIP/HAWAII, mesmo que estejam fixos, mas oferecem uma maior eficiência por não utilizarem túneis para o encaminhamento dos pacotes, mas à custa da sua menor escalabilidade.

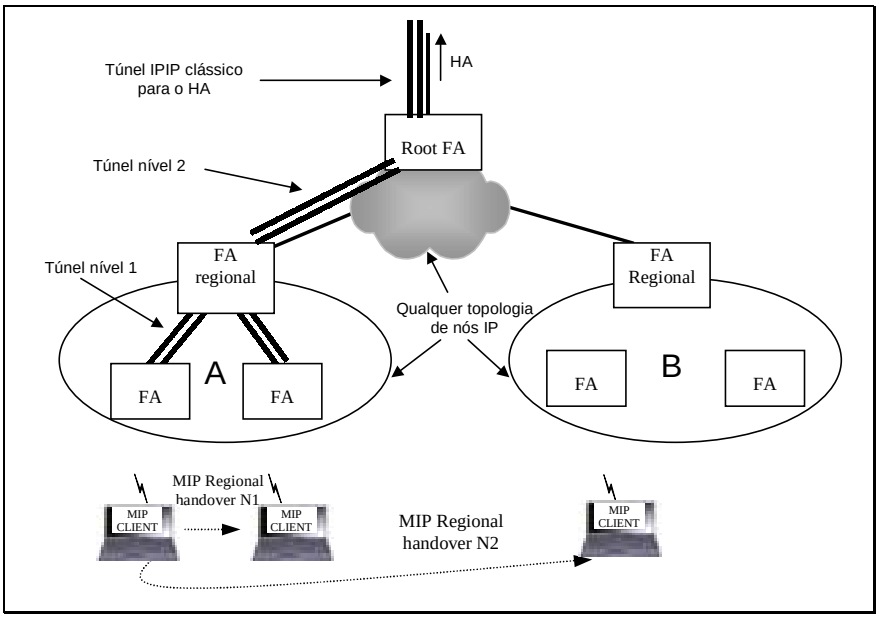


Figura 16: Arquitectura do hierarquical MIP

A arquitectura do hMIP está ilustrada na Figura 16, com um exemplo de uma cadeia de 3 níveis, suportando dois domínios IP. Aqui, os pacotes destinados aos terminais móveis são encaminhados até ao HA do terminal, que está algures na Internet, que os envia para o primeiro "root FA" dentro de um túnel IPIP. Aqui, os pacotes seguem depois num novo túnel

para o domínio correcto (A ou B), onde são recebidos pelo FA responsável pelo domínio; seguidamente seguem para o FA final, responsável pela subrede IP actual do terminal.

Enquanto o terminal se movimentar na mesma subrede, a conectividade IP manter-se-á[11], e apenas quando transitar de rede, ou de domínio, é que é despoletado o *handover* regional. Para isto, o terminal vai ter que suportar tanto o protocolo MIP, com as extensões das movimentações regionais, começando por iniciar o processo clássico de detecção MIP baseada em *beacons*. Depois de verificar o seu novo FA, vai então avisar por via deste a hierarquia de FAs necessários a respeito da sua nova localização, consoante o nível de *handover* que for necessário.

Concretamente, enquanto o terminal se mantiver no mesmo domínio IP, então só os FAs no seu interior é que têm que ser avisados, o que limita os contactos até à rede de origem do terminal de uma forma semelhante à executada pelos protocolos de micro-mobilidade.

Tal como o HAWAII, o hMIP não introduz mais nenhuma característica à mobilidade IP, simplificando-se de forma a apenas adicionar o suporte hierárquico ao MIP.

AVALIAÇÃO: Contribuição do hMIP para os objectivos desta Tese

Pelo que foi visto acima, o protocolo hMIP é uma solução bastante interessante para a "meso-mobilidade", mas que não se adapta bem às necessidades da micro-mobilidade, uma vez que os constituintes da rede continuam longe dos terminais, não tendo assim latências de registo tão baixas quanto os protocolos especificamente desenhados para este efeito. Por outro lado, tal como o MIP, este protocolo apenas consegue dar uma conectividade básica aos terminais legados, pelo que estes só podem movimentar-se no interior da sua rede local, o que tem o efeito indesejado de afastar as entidades IP dos terminais. Por fim, mesmo o uso de terminais MIP, com as extensões adequadas da mobilidade regional, continua a não optimizar a detecção passiva do movimento, obrigando a altas latências na transição.

[11] De igual forma que no IP clássico, uma vez que o hMIP usa na parte final do endereçamento o mecanismo normal (endereço rede/netmask), o que lhe permite operar em qualquer topologia IP.

2.4 Conclusões do Estudo de Mobilidade IP

Movimentação Topológica	**TIPO mobilidade IP**	Entre APs	Dentro da Rede	Dentro do Domínio	Entre Domínios	Global
MIP	Macro				+	✓
hMIP	"Meso"			✓	✓	+
HAWAII	Micro	+	✓	+		
CIP	Micro	+	✓	+		
IAPP	Nível 2	✓	*			
CIP+MIP	Micro+ Macro	+	✓	+	+	✓

Legenda:

✓	Melhor aplicação do protocolo
+	Boa aplicação do protocolo
	Má aplicação do protocolo

Na tabela acima está resumido o âmbito de cada protocolo analisado, considerando o tipo de mobilidade mais típica a que melhor se aplicam, o que varia conforme os seus aspectos de escalabilidade e desempenho; adicionalmente, esta tabela é complementada com a informação comparativa de um protocolo de nível 2, o IAPP do 802.11 [43], e das soluções conjuntas IP mais comuns que podem ser utilizadas (consultar o Anexo 1 para mais detalhes).

Da análise destes protocolos descritos, verifica-se que nenhum suporta a mobilidade IP dos terminais legados a qualquer nível entre entidades IP, uma vez que todos os protocolos consideram que o terminal é inteligente e que tanto este como a rede terão ambos que ter o suporte do mecanismo de mobilidade para se movimentar. Em particular, os protocolos optimizados de micro-mobilidade até nem asseguram uma conectividade básica aos terminais fixos que não tenham o suporte da mobilidade IP.

Por outro lado, todos os protocolos apresentados definem como mecanismo de detecção do movimento dos terminais a troca passiva de *beacons* de localização, que permitem a dedução do movimento pela falta de recepção dos *beacons* periódicos, o que conduz a latências inaceitáveis nas pequenas movimentações dos terminais. A única excepção é o mecanismo

activo do CIP, mas que requer um suporte extremamente elevado da tecnologia *no lado do terminal*, o que vai na direcção oposta ao suporte de terminais legados.

Por fim, das soluções propostas, o MIP clássico é o único que é considerado standard, tendo assim que ser obrigatoriamente seguido no seu segmento, a menos que razões mais fortes que o impeçam.

Por outro lado, os protocolos de micro-mobilidade mostraram claramente o caminho a seguir relativamente à optimização da fase de registo, mas encontram-se actualmente numa fase "estacionária": quando foram propostos, foram na altura devidamente apreciados, discutidos e melhorados, mas não tiveram aceitação generalizada, embora também não tenham sido rejeitados.

Esta situação deveu-se porque, na altura, havia a necessidade mais premente da macro-mobilidade, motivado pelos problemas que o MIP ainda detinha, e porque a micro-mobilidade IP era um problema que se resolvia de uma forma limitada pela tecnologia sub-IP existente.

Mais tarde, a mobilidade eficiente não-global voltou de novo a ser considerada, de tal forma que foi proposto o hMIP, que é ainda bastante recente e não-standard. Este protocolo é perfeitamente vocacionado para a meso-mobilidade, mas não tanto para a micro-mobilidade como os protocolos iniciais exclusivos (novamente pela mesma razão, considerando que a tecnologia sub-IP realiza esta tarefa).

A comparação dos protocolos já propostos serve para clarificar a estrutura da melhor solução, e das novas capacidades a desenvolver que terão que estar presentes, para concretizar os objectivos desta Tese.

Assim, ter-se-á que definir um novo modelo, distinto de todas as soluções de mobilidade já existentes, que permita que as acções relacionadas com a mobilidade possam ser totalmente realizadas em exclusivo pela rede, sem que os terminais tenham qualquer intervenção. Se esta característica se verificar, então este novo modelo irá suportar os terminais legados.

Para isto, pode-se verificar que nas várias arquitecturas de mobilidade examinadas, os terminais móveis apenas têm duas acções essenciais que são sempre estes a executar, por terem as melhores condições para o fazerem: a detecção do seu movimento, e a criação/manutenção do seu registo nos elementos de rede.

Assim, nesta Tese, passará a ser a rede a efectuar estas funcionalidades chave, da seguinte forma:

Relativamente à primeira, a detecção dos movimentos dos terminais será feita exclusivamente do lado da rede, nos elementos de rede IP que comunicam directamente com os terminais (Acesss Points IP). Para maximizar o desempenho, e ao contrário dos outros protocolos IP, os APs vão usar primariamente como base o modelo *reactivo* de detecção dos movimentos dos terminais, devidamente adaptado para operar apenas no lado da rede. Esta detecção será secundada por um modelo passivo não-optimizado, sem garantias de desempenho, que também opera exclusivamente do lado da rede, apenas para as tecnologias que não têm este suporte. Desta forma, o mecanismo tem o seu foco quando se consegue realizar a acção reactiva[12].

Relativamente à segunda característica, ao qual é indiferente o modelo de detecção utilizado, o processo de registo que era despoletado e mantido pelo terminal passa a ser da responsabilidade do elemento de rede que detectou a movimentação do terminal. Para isto, este elemento vai agir como se fosse o próprio terminal, tomando as acções necessárias como suas, e gerando por si só toda a sinalização necessária para interagir com os restantes elementos da arquitectura de mobilidade. Além destes aspectos necessários para o suporte dos terminais legados, as restantes opções arquitectónicas poderão ser semelhantes aos protocolos já existentes, de forma a aproveitar as suas melhores características. Neste sentido, dado que se pretende aproximar o mais possível as entidades IP dos terminais, então dever-se-á escolher um suporte de mobilidade baseado em micro-mobilidade, com especializações que maximizem o seu desempenho, o«podendo estas resultarem numa escalabilidade mais reduzida.

Este mecanismo principal deverá ser complementado com o suporte de macro-mobilidade baseado em MIP, de forma a concretizar a mobilidade global. Assim, a solução final terá estas duas componentes com suporte de terminais legados:

A componente de micro-mobilidade será a parte principal deste trabalho, por ser utilizada para a grande maioria das movimentações que os terminais vão realizar.

Uma vez que nenhum dos protocolos de micro-mobilidade existentes ter sido aceite como standard, e de todos terem diversas vantagens e desvantagens complementares, mas nenhum

[12] Note-se que os modelos mais avançados *preditivo* e *activo* não se podem aplicar para os terminais legados, por estarem intimamente ligados à tecnologia de rede *do lado do terminal.*

ter o suporte explícito à característica essencial que se procura, então existe a liberdade da criação de um ***protocolo novo***.

Este protocolo vai procurar combinar o suporte de terminais legados, com as características mais avançadas possíveis nas acções de detecção e registo que não envolvem os terminais, de forma a diminuir ao máximo os períodos sem conectividade nas transições. Desta forma, esta componente da solução final terá como fio condutor a máxima ***eficiência*** possível.

Uma segunda componente de macro-moblidade, que forneça o suporte complementar de mobilidade global, considerando os seus requisitos de escalabilidade distintos do caso anterior. Esta componente será baseada no standard MIP, com uma extensão apropriada para o suporte dos terminais legados. Neste sentido, esta componente da solução final terá como fio condutor a máxima ***escalabilidade*** possível.

Estas características conjuntas vão significar que qualquer terminal legado terá um suporte transparente, automático e eficiente de mobilidade IP enquanto se movimenta no interior e entre domínios IP.

3. Proposta de Mobilidade Global para Terminais Legados

Este capítulo vai apresentar a solução de mobilidade global proposta nesta Tese de Mestrado, desenhada explicitamente para suportar a mobilidade IP de terminais legados, e com a característica de ser altamente eficiente, reduzindo ao mínimo os períodos sem conectividade para a maioria das movimentações dos terminais.

Para responder à primeira característica, a solução proposta assegura que todos os seus mecanismos são executados em exclusivo pelos elementos do segmento administrativo da rede, em particular as acções de detecção do movimento e de reconfiguração do encaminhamento, o que possibilita o suporte dos terminais legados, uma vez que estes deixam de ter interacções com o processo da mobilidade. Neste sentido, será a rede quem vai tornar a mobilidade transparente para *todos* os elementos da Internet, em particular para os próprios terminais móveis que se movimentam, ao criar a ilusão que o terminal móvel está fixo na sua localização inicial em permanência.

Para a segunda característica, a solução foi desenhada de forma a que a reconfiguração da rede necessária em cada movimentação física do terminal seja activada da forma mais rápida possível, minimizando os períodos sem conectividade, pelo que a proposta tenha sido desenhada considerando explicitamente optimizações que vão melhorar a eficiência da mobilidade, tanto para a detecção das movimentações, mas também para acção de reconfiguração da rede, por forma a ser *local* para a maioria das movimentações.

Tal como foi analisado no fim do capítulo anterior, esta solução é constituída por duas componentes complementares de micro e macro mobilidade, de forma a considerar separadamente as diferentes aplicabilidades geográficas, e sendo as duas integradas entre si de uma forma hierárquica.

Neste sentido, este capítulo contém duas secções principais, onde é descrito cada protocolo que se aplica a cada domínio geográfico, sendo focado para cada um a sua arquitectura, opções de desenho, mecanismos e optimizações usadas para o suporte da mobilidade.

Assim, a primeira secção vai considerar o novo protocolo de micro-mobilidade IP para terminais legados proposto nesta Tese, e que constitui, quanto a nós, o seu mais importante contributo – o protocolo TIMIP. Esta secção é a referência base de desenho deste protocolo,

tendo um resumo (*draft*) do mesmo sido **submetido no IETF,** contribuindo para o processo de normalização [89]. Este novo protocolo vai procurar combinar o suporte dos terminais legados com as melhores características de outras propostas anteriores, procurando a máxima eficiência possível do mesmo.[13]

A secção seguinte completa a inicial, propondo um protocolo de macro-mobilidade que vai complementar o TIMIP na mobilidade *entre* domínios IP. Ao contrário deste último, esta vertente do problema foi resolvida com uma adaptação do protocolo standard já existente, o MIP, para terminais legados, resultando o sMIP (surrogate MIP). Neste sentido, esta adaptação vai ser totalmente compatível com o standard MIP, incluindo o referido suporte especial dos terminais legados, bem como de uma acção de detecção substancialmente optimizada relativamente ao MIP clássico.

Por fim, a descrição dos protocolos é complementada com a descrição do suporte do TIMIP para o protocolo clássico MIP, e com uma avaliação crítica da solução de mobilidade global apresentada.

3.1 Suporte de Micro-mobilidade para terminais legados usando o TIMIP

3.1.1 Conceitos Fundamentais

O **TIMIP** é uma solução de micro-mobilidade que possibilita a mobilidade a *todos* os possíveis terminais IP no interior de um domínio administrativo, apenas por mecanismos de encaminhamento IP.

No interior do domínio, os terminais ligam-se à rede por meio de elementos de rede especiais denominados de pontos de acesso (AP), ficando automaticamente com conectividade independentemente da sua localização física. Para isto, os terminais não terão explicitamente que realizar qualquer acção, uma vez que é apenas da rede a responsabilidade de detectar a

[13] No entanto, deve-se notar que, uma vez que se tratou de um protocolo novo, criado e desenhado de raiz, então este não tem (ainda) alguns aspectos que os outros protocolos semelhantes suportam. Entre estes, salienta-se a falta de suporte do *paging*, e uma robustez reduzida, sendo estes aspectos áreas de trabalho futuro.

chegada do terminal, e de pôr em curso todos os mecanismos internos necessários para manter a conectividade do terminal.

Depois de se ligarem à rede pela primeira vez, os terminais podem-se movimentar sem limitações no interior desta, transitando sucessivamente de AP em AP para manterem a sua ligação física activa; nestas operações, o protocolo TIMIP garante que os terminais mantêm sempre a sua conectividade inalterada, quaisquer que sejam as suas novas localizações, por um processo automático denominado de *handover*. Este processo tem uma latência mínima, durante o qual o terminal estará incontactável momentaneamente, tendo o TIMIP sido desenhado com optimizações destinadas a tornar este processo o mais curto possível, de forma a minimizar a perda de pacotes devido à mobilidade IP.

Por fim, quando os terminais se movimentam para fora do domínio actual, o TIMIP suporta o sMIP ou o MIP como protocolo de macro-mobilidade, que se encarrega apenas das movimentações raras nesse nível hierárquico superior.

3.1.2 Arquitectura do TIMIP

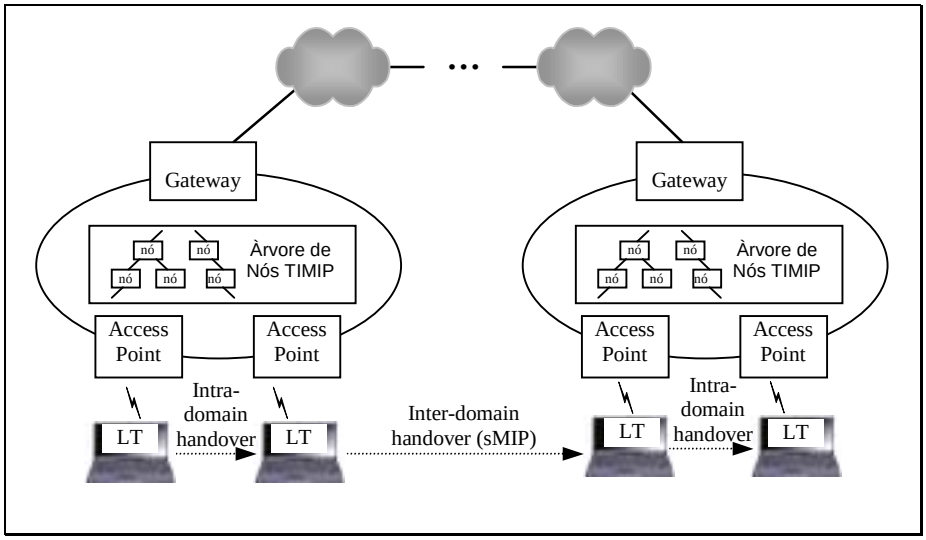


Figura 17: Visão geral da Arquitectura TIMIP

Na Figura 17 está esquematizada a arquitectura global do TIMIP. Neste exemplo, existem dois domínios TIMIP interligados por um conjunto de redes IP com qualquer topologia, e em cada domínio existem vários elementos de rede que constituem o segmento administrativo da rede, sendo estes baseados em encaminhadores IP fixos, que estão organizados numa árvore lógica de nós, com uma única ligação ao exterior. Além da parte administrativa, cada domínio contém os seus terminais móveis legados, que vão gozar do suporte de mobilidade que a rede vai fornecer enquanto se movimentam.

Descrição do segmento Administrativo:

Cada domínio TIMIP tem um único encaminhador especial denominado de *Gateway* (GW) que serve de ponto centralizador de certas operações da rede, e que detém a única porta de acesso ao exterior. Do ponto de vista das redes externas e dos seus protocolos de encaminhamento, um domínio TIMIP corresponde a uma subrede IP clássica caracterizada apenas pelo par *(Endereço de Rede*/*Máscara de Rede).*

Desta forma, o TIMIP é um protocolo transparente relativamente ao encaminhamento das outras redes, sendo indistinguível de outras subredes IP.

No interior de cada domínio existem elementos de rede denominados de *Pontos de Acesso* (AP) que permitem aos terminais móveis a sua ligação à rede. Estes APs podem ser baseados numa qualquer tecnologia de rede, e também em qualquer topologia de nível 2, bastando que os terminais possam estabelecer ligações directas nível 2 com o AP para ser possível a troca de pacotes de *dados* entre estes dois elementos. Normalmente, são as tecnologias de rede do tipo *wireless* que melhor se adequam, por possibilitarem a mobilidade física dos terminais.[14]

Dado que cada terminal móvel só se pode ligar à rede por via de um AP, então os terminais terão que estar permanentemente no alcance físico de um destes elementos para terem conectividade. Como muitas vezes é desejável que os terminais móveis possam movimentar-se ao longo de zonas extensas, isso leva a que o domínio TIMIP seja composto de vários APs dispersos geograficamente, por forma a cobrir essa região maior. Neste tipo de configuração de rede, a rede poderá crescer geograficamente acrescentando mais AP nas novas zonas a cobrir.

Por outro lado, noutras situações pretende-se não uma rede que cubra áreas extensas, mas sim que suporte um número elevado de clientes. Como cada AP terá necessariamente recursos limitados relativamente à largura de banda disponível e capacidade de processamento, este requisito conduz a concentrar vários APs perto uns dos outros, de forma a balancear o tráfego entre os vários APs.

Assim, nesta configuração, à medida que o número de clientes aumente, bastará acrescentar mais APs para manter a qualidade global da rede.

[14] Sem perda de generalidade, nesta descrição do protocolo representa-se e refere-se a tecnologia de rede dos terminais e APs como sendo *wireless*, e as ligações dos nós da rede como *wired*.

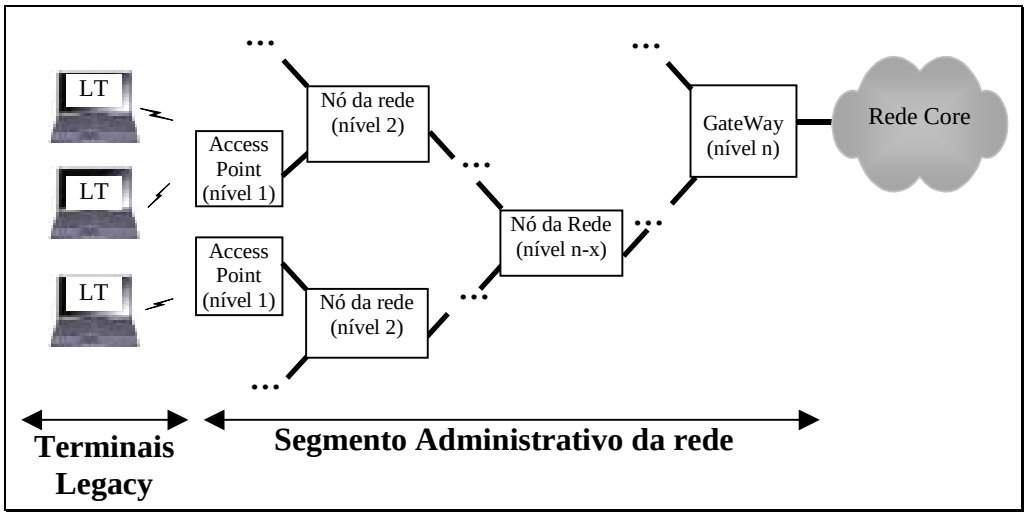


Figura 18: Organização lógica de um domínio TIMIP

Internamente, um domínio TIMIP é constituído por uma árvore de nós genéricos TIMIP, que são usados para interligar a GW, no topo da árvore e os APs existentes (ver Figura 18). No entanto, não é necessário que os APs estejam localizados nas folhas da árvore, podendo estar em qualquer posição, bastando que tenha a interface apropriada para contactar com os clientes. O único requisito que a estrutura de nós terá que respeitar é que, para cada nó, a GW seja sempre apenas acessível por *um único* caminho, o seu nó ascendente.

De modo semelhante à ligação com os terminais móveis, as ligações entre os nós também podem ser concretizadas por uma qualquer tecnologia de rede, dando normalmente preferência a tecnologias *wired*, que têm uma maior capacidade e fiabilidade, dado que os nós da rede não se movimentam fisicamente como os terminais móveis.

Desta forma, os nós da rede são encaminhadores IP que executam um novo protocolo de encaminhamento especial para mobilidade, ao invés de outro protocolo de encaminhamento IP alternativo, e uma vez que apenas o encaminhamento é diferente, as outras componentes do nível IP podem-se manter inalteradas, nomeadamente o *forwarding*, o controlo de tráfego ou a resolução de endereços.

Além dos nós acima descritos, os restantes elementos de rede que pertencem a um domínio TIMIP são os *Terminais Móveis*, que são os clientes da mobilidade TIMIP, a qual lhes vai ser proporcionada de uma forma transparente, tanto dentro como fora da sua rede de origem.

A característica fundamental no desenho do TIMIP – independência dos terminais – reflecte-se directamente nos requisitos dos terminais móveis, pois estes apenas terão que possuir um *stack* de protocolos genérico IP, sem incluir nenhum módulo relacionado com mobilidade, bastando apenas que este *stack seja* configurado de uma forma especial, e que estajam

registados na rede. Ambos estes requisitos podem ser efectuados por mecanismos manuais, ou de forma automatica se o terminal suportar o mecanismo DHCP de configuração.

Neste sentido, a única interacção de nível 3 entre os terminais e os APs é a troca normal de pacotes de dados, e dado que não existe qualquer sinalização de/para o terminal móvel, então a detecção por parte dos APs dos movimentos dos terminais é inferida preferencialmente com base nos mecanismos de nível 2 que cada tecnologia particular oferecer (modelo reactivo), ou em alternativa, de uma detecção genérica exclusiva do nível 3 (modelo passivo).

Relativamente às camadas existentes acima do nível IP, estas não terão que sofrer nenhuma alteração, porque a mobilidade está restringida ao nível 3 exclusivamente, o que significa que o protocolo TIMIP é transparente para os níveis superiores (nomeadamente o TCP e o UDP), e que significa que todas as aplicações IP beneficiam automaticamente de mobilidade sem quaisquer modificações.

Por outro lado, o TIMIP também é transparente a todos os interlocutores que estão a comunicar com o terminal móvel, e aos encaminhadores que interligam uns e outros, dado que o suporte de mobilidade é exclusivo dos elementos de rede do domínio administrativo. Todos os outros nós da Internet não estão envolvidos nas acções e acontecimentos de mobilidade, não tendo assim a noção se estão a comunicar com um nó fixo ou móvel.

Este princípio do desenho do TIMIP é comum a outros protocolos que estendem o IP de várias formas, porque esta é uma condição fundamental para manter a compatibilidade anterior com os nós que executam o protocolo IP “clássico”, com a extensão adicional de ser também compatível com o IP clássico dos terminais que se movimentam.

3.1.3 Concretização da Mobilidade TIMIP

O protocolo TIMIP fornece mobilidade no interior da rede por um conjunto de mecanismos que se assemelham aos outros protocolos de mobilidade, estando divididos em três fases - localização, registo e execução - que contêm as acções necessárias para garantir a conectividade dos terminais no interior do domínio.

Para isto, as duas primeiras fases são activadas em sequência apenas quando o terminal se movimenta e transita fisicamente de AP. Da primeira vez que o terminal chega a um domínio TIMIP, a rede vai iniciar um processo denominado de *Power-up* para *criar* a conectividade inicial ao terminal; após esta operação, as movimentações subsequentes entre os APs do mesmo domínio dão origem a *Handovers*, utilizados apenas para *restaurar* esta conectividade.

Por outro lado, a fase final do processo de mobilidade (*Execução*) vai ser executada em permanência para cada pacote destinado e originado no terminal móvel, de forma a ser encaminhado para a localização correcta, pelo que esta fase final do mecanismo opera de forma independente das duas primeiras, seguindo apenas as configurações de encaminhamento geradas por estas, e que se instanciam numa cadeia de entradas directas de encaminhamento presentes na arvores de nós para o terminal legado.

Relativamente ao processo de registo do protocolo, são os elementos de rede que vão tomar acções passivas e reactivas, de forma semelhante aos outros protocolos de mobilidade. No entanto, devido ao suporte dos terminais legados, a entidade activa do protocolo deixa de ser o terminal móvel para ser o AP onde este está localizado, passando este a ter a responsabilidade de iniciar e manter o processo de mobilidade do terminal (ver comparação dos tipos de elementos de rede entre o TIMIP e os outros protocolos no Anexo 3).

3.1.3.1 Fase 1 - Localização

A primeira fase do protocolo consiste no conjunto de acções necessárias para a descoberta *por parte da rede* que um terminal necessita de algum tipo de reconfiguração de encaminhamento IP para manter a sua conectividade. Tal como foi focado anteriormente, isto acontece quando o terminal se movimenta fisicamente de tal forma a que deixa de estar acessível pelo seu ponto de contacto anterior, despoletando o *power-up* ou *handover* TIMIP (consoante a origem do terminal).

Para isto, vai ser apenas o AP onde o terminal se liga que terá esta responsabilidade de detectar a chegada do terminal, por um de dois modelos de detecção do terminal – o modelo reactivo, utilizável quando a tecnologia poder fornecer um mínimo de ajuda ao nível 3, e o modelo passivo para o caso contrário.

Devido o primeiro conduzir a uma melhoria substancial do desempenho na detecção, então este será considerada sempre como a forma de detecção primária, sendo o modelo passivo utilizado apenas em último caso.

Para a execução desta detecção, é utilizada uma primitiva de notificação ascendente genérica de detecção que será recebida da mesma forma em ambos os casos pelo TIMIP, e que contém a informação dos terminais que são dinamicamente detectados pelo AP, identificados pelo seus endereços MAC (o único parâmetro desta primitiva). Em ambos os modelos de detecção, as acções despoletadas pelo TIMIP são exactamente as mesmas, sem distinção na origem da primitiva.

Detecção Reactiva:

No modelo de detecção reactivo (representado na Figura 19), o nível 2 vai agir de forma totalmente independente do nível 3, mas expõe a este último as suas decisões internas, o que lhe permite despoletar o processo de mobilidade assim que estas são necessárias. Neste sentido, o nível 3 beneficia apenas da ajuda do nível 2, por via de um mecanismo genérico, e sem interacções no nível abaixo que o tornariam dependente das tecnologias.

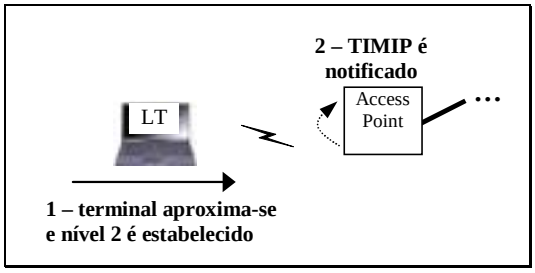


Figura 19: Fase de Localização – Detecção Reactiva

Para isto, cada tecnologia particular vai implementar a primitiva de detecção consoante os seus próprios mecanismos internos de gestão das estações móveis, os quais podem ser mais ou menos eficientes ou precisos. Concretamente, em tecnologias nas quais existe um mecanismo explícito de associação bem definido dos terminais a pontos centrais, então esta primitiva é passível de ser derivada directamente de uma forma muito eficiente e rigorosa.

Detecção Passiva:

No caso em que a tecnologia não oferecer nenhuma facilidade deste tipo, então a detecção dos terminais terá que ser efectuada por um mecanismo alternativo independente, passível de ser utilizado em todas as tecnologias, a ser operado apenas do lado da rede.

Para tal, o nível 3 de cada AP vai utilizar um *algoritmo genérico de detecção*, que é igual ao *MAC-Learning* usado pelos elementos de rede de nível 2 como as *bridges* e *switches*, na aprendizagem das localizações dos terminais.

Neste mecanismo passivo, o AP vai poder aprender a identidade das estações MAC que estão acessíveis na sua interface *wireless* através dos pacotes normais de dados que estes emitem; todo o tráfego emitido pelos terminais é continuamente analisado, de forma a verificar quais os endereços MAC de origem de todos os pacotes recebidos.

O AP tem uma *cache* dos endereços MAC já conhecidos, e verifica para todos os pacotes que vai recebendo pela sua interface *wireless* se algum veio de uma estação que não estava na *cache*, mas quando isto acontece, então o AP vai assumir que este foi originado por um terminal que acabou de chegar, o que o leva a gerar a primitiva de notificação do nível 3 neste MAC, e adiciona este endereço à *cache* (ver Figura 20).

Cada entrada nesta *cache* tem um *timeout* associado, ao fim do qual as entradas são removidas; por outro lado, mas só nesta utilização especial, existe uma segunda primitiva interna do nível 3 do tipo *pedido*, no qual o nível 3 pode invalidar entradas da *cache* a qualquer momento.[15]

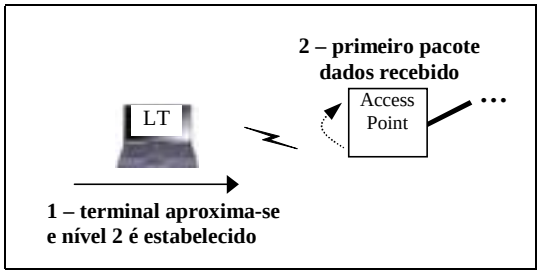


Figura 20: Fase de Localização – Detecção Passiva

Utilizando este mecanismo alternativo, o AP vai poder detectar a chegada do terminal quando este emitir o seu primeiro pacote de dados, o que poderá não acontecer de imediato, conduzindo a latências mais elevadas que o modelo reactivo. Nestas circunstâncias, esta forma de detecção terá um desempenho semelhante à utilizada na mobilidade simples de nível 2 no mecanismo *MAC-learning*.

3.1.3.2 Fase 2 - Registo

Depois de o terminal ser detectado por um dos meios descritos, o AP que o detectou vai iniciar a segunda fase do protocolo, que tem o objectivo de criar (ou recriar, consoante o movimento) as condições necessárias para o estabelecimento da conectividade IP do terminal, sendo necessário que a rede como um todo seja informada da nova localização actual do terminal; no entanto, o desenho do protocolo prevê que este objectivo possa ser atingido sem que necessariamente *todos* os elementos da rede sejam informados, sendo neste caso apenas informados os elementos de rede a que, do seu ponto de vista, o terminal já não esteja acessível pela mesma localização, pelo que além destes, os outros elementos não serão contactados, o que torna o *handover* do terminal local e optimizado.

Nesta conformidade, o mecanismo de registo aplicado aos terminais quando chegam pela primeira vez à rede está ilustrado na Figura 21.

[15] Esta funcionalidade é utilizada no processo de *handover* para possibilitar ao AP anterior do terminal a invalidação das entradas da cache do terminal, o que acelera a sua re-detecção quando o terminal volta a este AP.

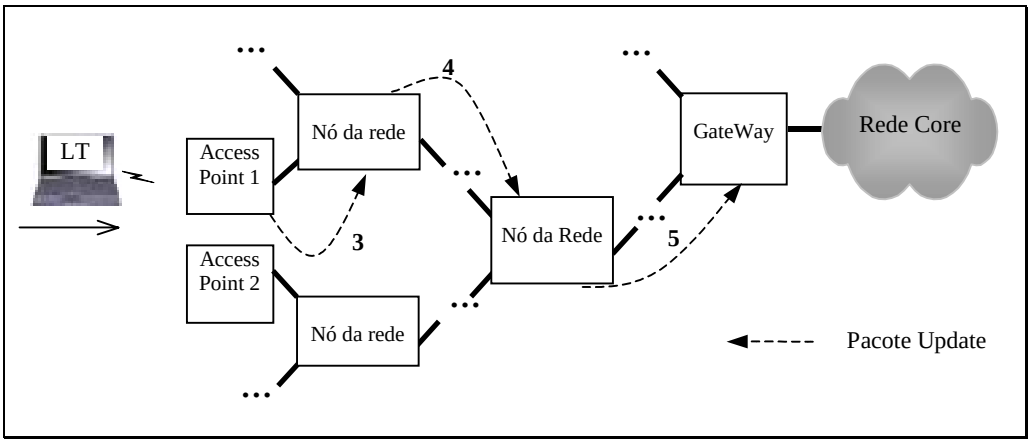


Figura 21: Registo no Power Up

O *Power-up* tem início no AP do terminal logo depois de este ser avisado da chegada deste por via da primitiva de detecção, e usando o endereço MAC contido na primitiva, o AP vai usar a sua tabela de registo dos terminais autorizados nesta rede (uma cópia da tabela central localizada na GW, conforme a secção 3.1.4.4) para consultar os dados relativos a este terminal, nomeadamente o seu endereço IP. Se este endereço MAC não corresponder a nenhum terminal registado, então o processo é cancelado, o que lhe nega a conectividade, até o terminal ser conhecido.

De posse do endereço IP do terminal móvel, então o AP vai verificar a sua tabela de encaminhamento, que não contém nenhuma entrada relativa a este terminal, e acrescenta-lhe uma nova entrada para este terminal, com a informação de encaminhamento que está acessível pela sua interface *wireless,* por via de uma entrada directa de encaminhamento IP.[16]

Depois desta alteração na tabela de encaminhamento, o AP vai tomar a iniciativa de, em nome do terminal móvel, avisar toda a restante rede que este terminal móvel chegou à rede, e a sua localização actual. Para este aviso, e todas as outras operações que envolvam comunicações TIMIP entre os nós da rede, são instanciadas pela utilização de pacotes especiais de controlo. Estes pacotes têm um formato e utilização próprios, e são encapsulados em pacotes de controlo ICMP [26], distinguidos por um código ICMP exclusivo do TIMIP no interior da rede (consultar o Anexo 4 para os formatos e detalhes específicos das mensagens de sinalização).

[16] Esta entrada é do tipo ponto-a-ponto entre o AP e o terminal, por ter uma máscara de rede do tipo fechada (255.255.255.255).

Todos estes pacotes de sinalização são encaminhados e processados nó-a-nó no interior da rede, entre os nós da rede adjacentes entre si; além disto, por serem encapsuladas em ICMP. estas mensagens não têm garantias de entrega, podendo não chegar ao destinatário.

Assim, para continuar a reconfiguração da rede, o AP vai gerar um pacote de sinalização TIMIP do tipo *update* (distinguido pelo campo apropriado*)*, contendo dados específicos do protocolo relativos à operação pretendida, nomeadamente a identificação do terminal móvel, a identificação do nó emissor e receptor, e o valor do tempo NTP em que o terminal foi detectado pelo AP. Este tipo de mensagens é utilizado para informar os nós da rede apenas da localização *aproximada* do terminal móvel – o próximo nó mais perto do terminal - ao invés de incluírem a localização exacta do terminal.

Nestas condições, esta mensagem vai ser entregue pelo AP ao seu nó ascendente na árvore de nós (**passo 3** na Figura 21), e este último, quando a receber, aprende que o terminal móvel está acessível pelo nó que entregou a mensagem, sendo esta informação apenas aproximada nas consições definidas acima.

Seguidamente, à semelhança do AP, este verifica que não tinha nenhuma entrada de encaminhamento para este terminal, pelo que também irá criar uma nova entrada para o terminal, do mesmo tipo da anterior, com a informação que este destino (o terminal móvel) está acessível pelo nó que lhe entregou a mensagem (neste caso, o AP).

Posteriormente, o ciclo de processamento da mensagem pela rede repete-se (**passos 4 e 5**), no qual cada nó da rede que recebe a mensagem por um seu descendente altera a tabela de encaminhamento para reflectir que o terminal móvel está acessível pelo nó descendente, e passa a mensagem para o seu ascendente.

Este processo é finalizado quando a mensagem é recebida na GW da rede, pois finaliza a cadeia de entradas de encaminhamento para este terminal, desde a GW da rede até ao AP do terminal, que são utilizadas pela fase 3 para encaminhar os pacotes destinados ao terminal móvel (ver Figura 22).

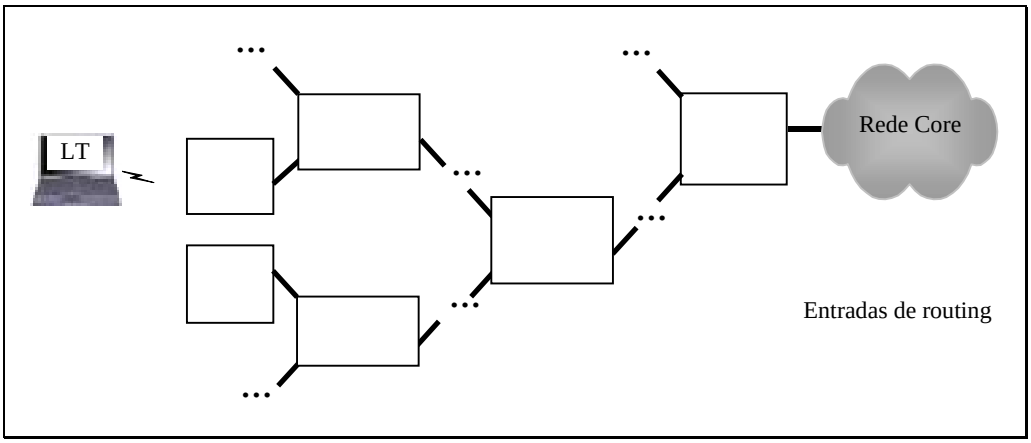


Figura 22: Cadeia inicial de entradas de encaminhamento

Depois do *power-up* inicial do terminal na rede, as suas movimentações subsequentes no interior da rede passam a ser concretizadas por *Handovers* locais na rede, que fazem basicamente as mesmas operações delineadas no *power-up*, mas com a diferença que vão apenas *restaurar* a conectividade do terminal, em vez de a *criar* de novo, por forma a suportar um *handover* local e optimizado.

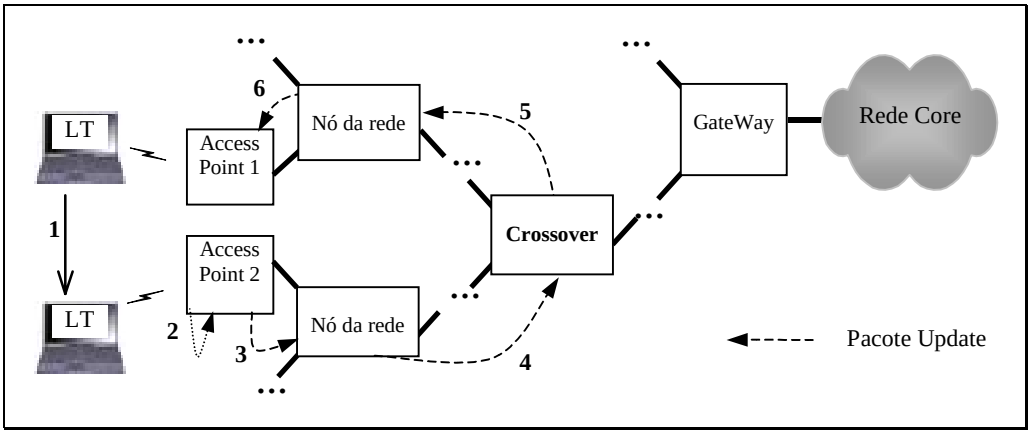


Figura 23: Handover entre APs

Assim, o processo de *handover* vai ser iniciado quando o terminal se movimenta entre dois APs da mesma rede (ver Figura 23), e quando sucede a transição física, vão ser efectuados exactamente os mesmos passos descritos no *power-up* nos primeiros nós da árvore para onde o terminal se moveu (**passos 1 a 4**), até que a mensagem de registo chega ao primeiro nó que já tinha uma entrada de encaminhamento anterior relativa ao terminal.

Este nó, denominado de *crossover*, tem um papel especial no processo de *handover*, dado que após este, o caminho que liga o terminal à GW vai ser o mesmo, não necessitando assim de ser alterado. Por esta razão, assim que este nó alterar a sua entrada de encaminhamento com a informação mais actualizada do próximo nó do terminal, a maior parte da rede volta a ter a

informação do caminho correcto para o terminal móvel, o que é suficiente para lhe restabelecer a conectividade para a maioria dos destinos.

A única excepção são os elementos de rede que estão localizados na parte da árvore desde o *crossover* pelo caminho anterior, dado que estes ainda têm a informação da localização anterior do terminal, que implicam que, para concluir o *handover*, é necessário continuar o processo em curso de registo, para se remover o caminho anterior entre o *crossover* até ao AP anterior do terminal.

Para isto, o *crossover* vai continuar por enviar a mensagem *update* para o nó seguinte que terá que ter a localização mais actualizada do terminal, sendo localizado no caminho antigo do terminal (i.e., o *antigo* próximo nó do terminal) (**passo 5**). Quando este a recebe, vai notar que foi o seu ascendente que lhe entregou a mensagem, significando isto que o terminal já não está localizado na sua zona da árvore, pelo que elimina a sua entrada de encaminhamento existente deste terminal[17]; depois, continua o processo entregando o pacote de *update* ao seu próximo nó descendente que necessita de ser informado, no caminho antigo que levava ao terminal.

Depois, o ciclo de processamento da mensagem pela rede repete-se (**passos 5 e 6**), no qual cada nó da rede que recebe a mensagem por um seu ascendente, elimina a entrada do terminal na sua tabela de encaminhamento, reflectindo que o terminal móvel não está acessível pela localização anterior, e passa a mensagem para o descendente anterior do terminal.

O processo é finalizado quando a mensagem é recebida no AP anterior, porque aí a cadeia de entradas de encaminhamento para este terminal (a utilizar na fase 3) voltou a estar consistente com a localização actual do terminal (ver Figura 24).

[17] Uma vez que o encaminhamento TIMIP define que os pacotes destinados a terminais móveis sem registo na tabela de encaminhamento são enviados para o nó ascendente (ver secção 3.1.3.3)

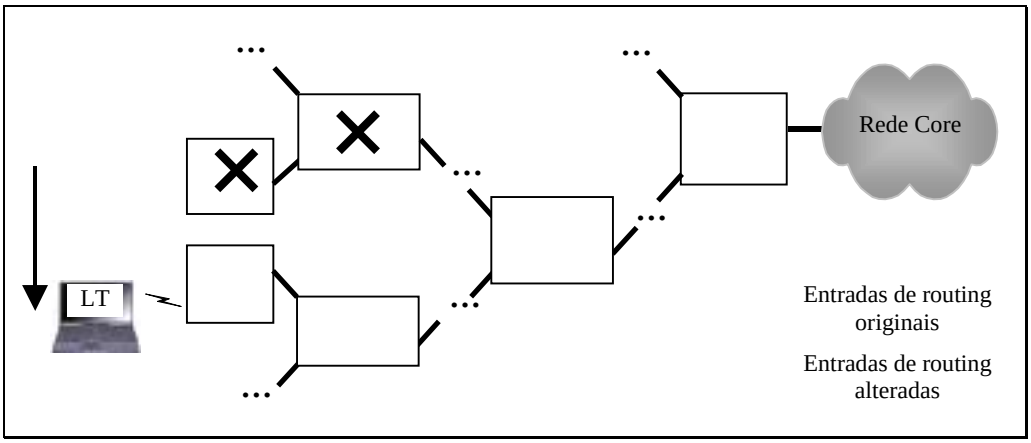


Figura 24: Nova cadeia de entradas de encaminhamento

Desta forma, à medida que o terminal móvel se movimenta livremente no interior da rede, o processo de registo garante que todos os nós *relevantes* são informados de forma a saberem sempre a direcção por onde terminal móvel está localizado, embora esta informação não revela a localização exacta (isto é, qual o AP) do terminal, mas apenas a indicação do próximo nó que está mais próximo deste.

Esta característica é fulcral para realizar um mecanismo de *handover local* que só actua na zona da árvore de nós dos dois APs envolvidos e o nó *crossover*, pois fora dessa zona as entradas de encaminhamento mantêm-se inalteradas, pelo que desta forma, mesmo em redes TIMIP extensas, o *handover* mantém-se eficiente, porque normalmente os dois APs envolvidos estarão próximos um do outro, tanto geograficamente como na árvore lógica de nós; só no pior caso é que o *handover* envolve a GW da rede.

3.1.3.3 Fase 3 - Execução

A fase final do processo de mobilidade vai ser executada à parte das fases anteriores, para o encaminhamento dos pacotes de dados IP destinados aos terminais móveis (*tráfego downlink*) e, no sentido oposto, aos que são emitidos por este (*tráfego uplink*), podendo ambos os tipos de tráfego limitar-se apenas ao interior da rede (*tráfego intra-domain*), ou além desta (*tráfego inter-domain*). Em todos os casos, os pacotes são sempre encaminhados utilizando a cadeia de entradas de encaminhamento, que a fase de registo mantém consistente com a localização dos terminais.

3.1.3.3.1 Encaminhamento *downlink*

O **encaminhamento *downlink*** é utilizado para encaminhar os pacotes que são destinados ao terminal móvel, podendo estes serem provenientes do exterior da rede, ou terem sido gerados

por outros terminais móveis. A primeira situação está ilustrada na Figura 25, em que um pacote gerado algures na Internet é encaminhado para o terminal móvel.

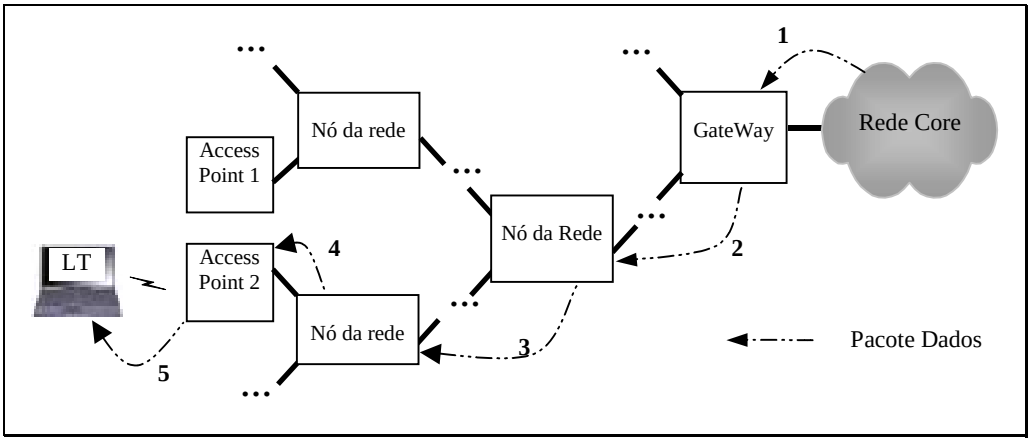


Figura 25: Encaminhamento downlink (inter-domain)

A primeira fase do encaminhamento, enquanto o pacote está fora do domínio, é realizada por outros protocolos que não o TIMIP[18], até o pacote ser entregue à GW da rede (**passo 1**).

Quando o recebe, a GW consulta a sua tabela de encaminhamento para verificar se o destino do pacote está no interior da rede, e no caso afirmativo, pode extrair daí o *próximo nó* para este terminal, e entregar-lhe o pacote (**passo 2**)[19], procedendo este próximo nó de maneira semelhante, de forma a que os pacotes sejam encaminhados ponto-a-ponto pela árvore de nós, e percorrendo a hierarquia de encaminhadores pelo caminho mais curto desde a GW até ao AP do terminal, de forma a aproximar-se sucessivamente do seu destino em cada passo (**passos 3 e 4**).

Por fim, quando o pacote chega ao AP onde está localizado o terminal, então vai ser entregue directamente para o endereço MAC do terminal móvel que está presente no registo do terminal (**passo 5**). Nesta conformidade, esta última operação não vai envolver a habitual operação da resolução do nome de nível 3 com o recurso ao protocolo ARP [32], uma vez que a resposta – o endereço de nível 2 do terminal – já é conhecida, pois está presente na base de dados do terminal nos APs.

[18] Nomeadamente o OSFP ou o RIP

[19] No caso de o terminal não se encontrar de momento presente na rede TIMIP (não tendo assim entrada na tabela da GW), então esta inicia o processo normal de tratamento de erros IP, respondendo ao emissor com um pacote de diagnóstico ICMP Host Unreachable.

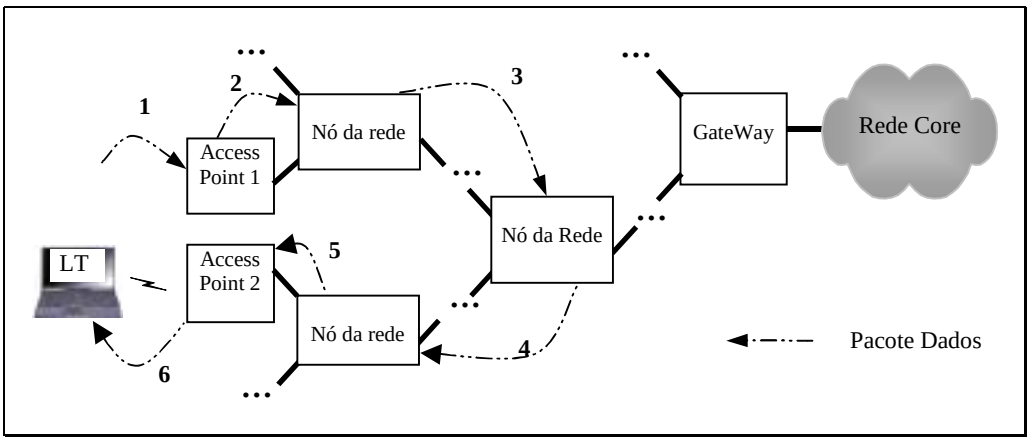


Figura 26: Encaminhamento downlink (intra-domain)

Alternativamente, o pacote destinado ao terminal também pode ser gerado no interior da rede por um outro terminal (ver Figura 26), e nesta situação, o encaminhamento tem início quando o pacote é recebido por um dos APs da rede (**passo 1**), que (neste exemplo) não tem nenhuma entrada na sua tabela de encaminhamento para este terminal.

Esta situação, em que o destino não está acessível por um descendente, então os nós da rede seguem a regra de encaminhar os pacotes para o respectivo ascendente, de tal forma a que o pacote vai subir na árvore de nós até chegar a ser encaminhado, por um dos nós que já tenha a informação da localização do terminal (**passos 2 e 3**).

Uma vez aqui, esse nó vai usar a informação da sua tabela de encaminhamento para fazer o pacote descer pela árvore de nós, da mesma forma já descrita no exemplo anterior (**passos 4 a 6**), sendo o encaminhamento dos pacotes no interior da rede local e optimizado, uma vez que estes seguem sempre pelo caminho mais curto no interior da árvore de nós, só chegando em último caso até à GW da rede, e nunca além desta.

3.1.3.3.2 Encaminhamento *Uplink*

O **encaminhamento *uplink*** vai ser aplicado no sentido oposto, para encaminhar os pacotes emitidos pelos terminais móveis tanto para o interior do domínio, como para o seu exterior. Uma característica do encaminhamento TIMIP é que *todos* os pacotes emitidos pelos terminais são *sempre* entregues ao seu AP actual, qualquer que seja o seu destino, para que este inicie o encaminhamento.

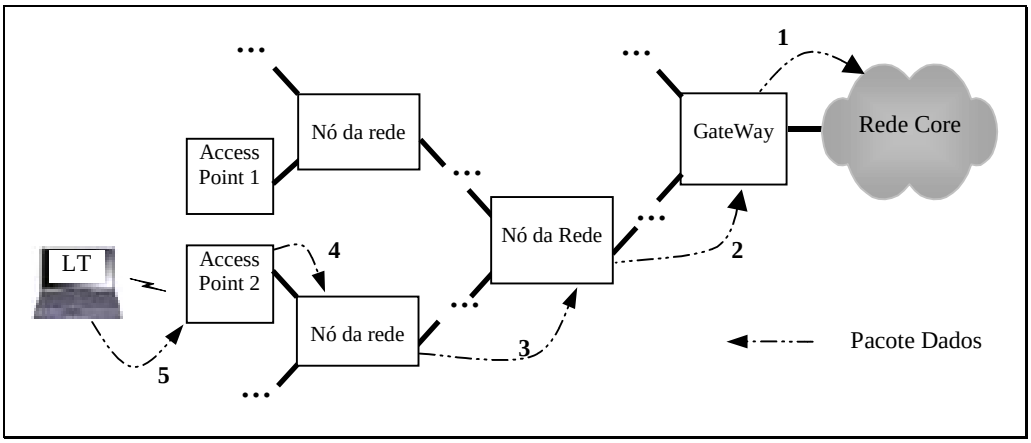


Figura 27: Encaminhamento uplink (inter-domain)

Assim, para os pacotes destinados ao exterior da rede (Figura 27), o AP inicial do terminal móvel vai encaminhar estes pacotes pela árvore de nós desde o AP até à GW da rede, na medida em que todos estes nós intermédios não irão ter entradas relativas ao destino dos pacotes (**passos 2 a 4)**.

Uma vez na GW, esta vai verificar que o destino não se encontra no interior da rede, pelo que entrega o pacote à sua rede externa a que tem ligação[20], sendo aí encaminhado por outro(s) protocolo(s) de encaminhamento IP que façam chegar o pacote ao seu destino final (**passo 5**).

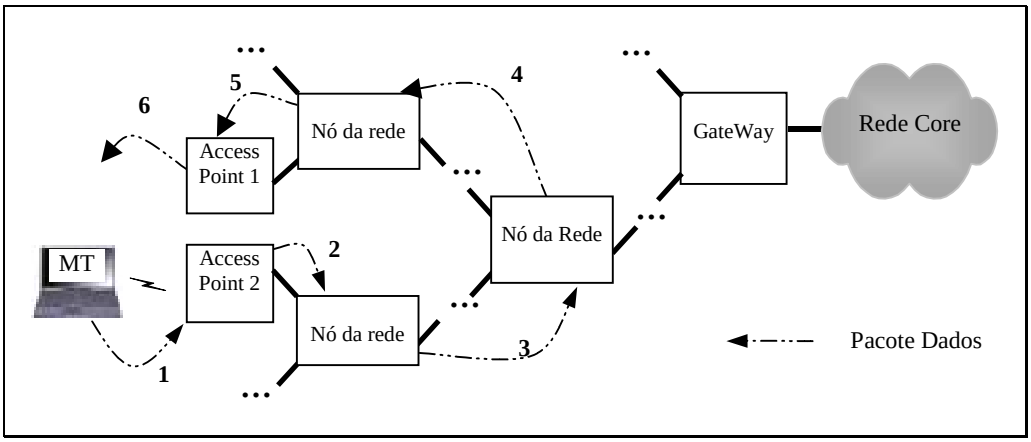


Figura 28: Encaminhamento uplink (intra-domain)

A outra possibilidade é a de o tráfego se destinar a outros terminais não localizados na mesma rede, vai ser exactamente igual ao encaminhamento *downlink intra-domain* já descrito. Neste tipo de encaminhamento, vão seguir-se os mesmos processos já descritos, nomeadamente

[20] Eventualmente, o domínio TIMIP poderá estar ligado a mais que uma rede de core, desde que internamente se mantenha uma arvore de nós com apenas 1 GW.

fazendo o pacote subir na rede até ao primeiro nó com informação do destino (**passos 2 e 3** da Figura 28), para seguidamente descer na árvore usando a cadeia de encaminhamento do destino (**passos 4 a 6**).

3.1.3.3.3 Configuração do terminal móvel para as redes TIMIP

O encaminhamento *uplink* tem uma dificuldade adicional relativamente à entrega dos pacotes aos APs pelos terminais legados (Figura 29), pois estes foram desenhados para operarem nas redes IP clássicas, que são substancialmente distintas das redes TIMIP. Neste modelo clássico, considera-se que os terminais vão comunicar entre si directamente por nível 2 quando pertencem à mesma rede, e por encaminhamento de nível 3 no caso contrário, recorrendo a encaminhadores que transmitem os pacotes pela Internet até chegarem à rede do destino (ver Figura 30).

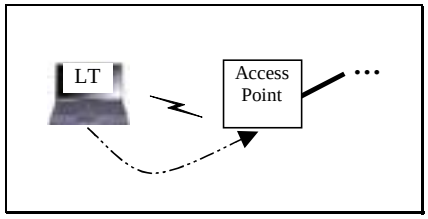


Figura 29: Encaminhamento uplink – entrega de pacotes dados ao AP

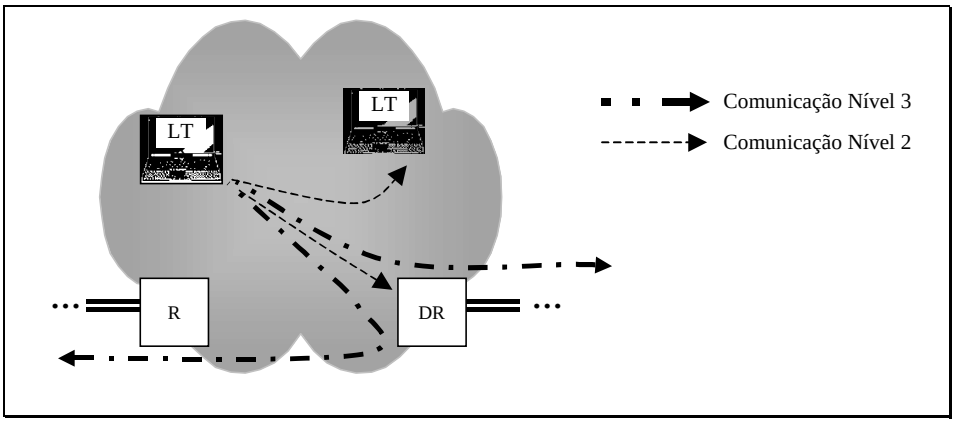


Figura 30: Modelo Clássico do ponto de vista do Terminal

Desta forma, as acções complexas de encaminhamento são relegadas apenas nos encaminhadores, que executam entre si protocolos específicos que encontram os caminhos na Internet, de forma a que os terminais são configurados de uma forma simples, com a informação da sua rede (endereço IP do terminal/máscara de rede) e de um dos seus encaminhadores de acesso, o *default router*, que lhe permite comunicar para o exterior.

Nesta situação, embora um domínio TIMIP se pareça para o exterior como uma subrede IP clássica, no seu interior este mecanismo não se pode utilizar, porque (regra geral) os constituintes da rede *não* se encontram acessíveis entre si directamente por nível 2 da forma que é esperada no modelo clássico, mas pelo contrário, e tal como foi definido anteriormente, os terminais só vão ter garantidamente a sua ligação de nível 2 ao seu AP actual, o que significa que têm que utilizar este elemento de rede para comunicarem com todos os destinos.

Como os terminais legados não podem ser alterados, o mecanismo clássico dos terminais tem que ser reconfigurado de uma forma especial, que o torne compatível com as redes TIMIP, e que terá que ser única. Para isto, o terminal é configurado com uma máscara de rede especial (máscara fechada, constituída por ter todos os bits a 1[21]), e pela GW da rede como o seu *default router*. Usando este caso particular do modelo clássico, o terminal considera que a sua rede é nula, e entrega *todo* o seu tráfego à GW da rede, para que esta o encaminhe convenientemente.

No entanto, esta configuração só funcionaria se os terminais tivessem uma ligação constante de nível 2 para a GW da rede, dado que os terminais vão tentar resolver o endereço IP da GW no seu correspondente endereço MAC para lhe entregarem directamente os pacotes IP, mas, dado que os terminais têm uma ligação permanente para o seu AP actual, então estes vão alterar a mecânica de resolução de nomes de nível 3 pelo mecanismo *proxy arp*, pelo qual vão tomar a identidade da GW da rede, bastando que os APs respondam com seu próprio endereço MAC aos pedidos de resolução do endereço IP da GW por parte dos terminais.

Usando este processo, então os APs vão criar esta ilusão necessária ao terminal para que este tenha uma configuração constante (máscara de rede/*default router*) no interior do domínio TIMIP, e que lhes entreguem sempre os seus pacotes[22].

Este mecanismo é conjugado com a acção complementar de *gratuitous arp*, com o qual o AP força o terminal a actualizar a sua *cache* de endereços MAC com o valor do seu próprio endereço MAC para o endereço IP da GW, sendo utilizado assim que o terminal é detectado pelo AP, consistindo na emissão não-solicitada de um pacote ARP *reply* ao terminal com a nova correspondência endereço IP da GW/endereço MAC do AP, de forma a que este passe imediatamente a entregar os seus pacotes para o endereço MAC do seu novo AP.

Assim, as figuras seguintes comparam, para o encaminhamento uplink, o ponto de vista do terminal legado, e da rede de acesso.

[21] 255.255.255.255

[22] O mecanismo de *proxy* ARP é utilizado no standard MIP, para a captura de pacotes pelo HA em nome do terminal move, e na concretização de *bridging* por meio de mecanismos de *routing*.

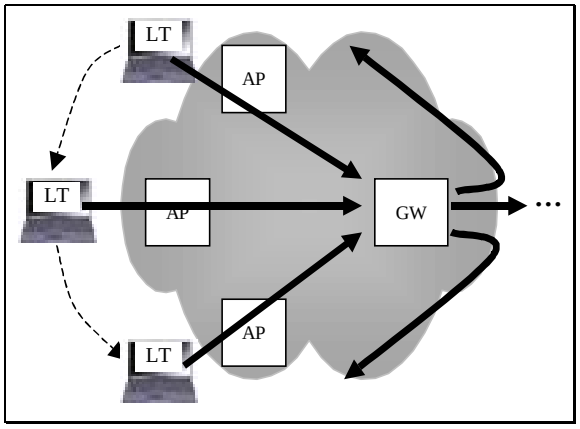


Figura 31: Modelo Clássico aplicado às redes TIMIP, do ponto de vista do Terminal

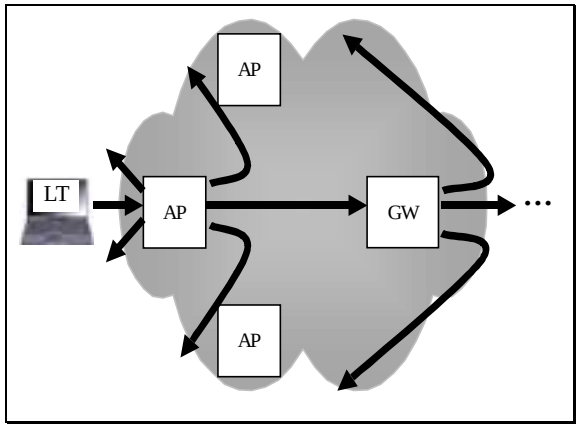


Figura 32: Correspondência do encaminhamento TIMIP na Rede

3.1.4 Acções adicionais da Mobilidade TIMIP

A secção anterior detalhou as acções básicas que são utilizadas para fornecer o suporte da mobilidade aos terminais legados, mas sem quaisquer preocupações relativamente à robustez do mesmo, situações de erros, situações transitórias e outros acontecimentos menos prováveis, que poderão no entanto acontecer e que produzem estados em que o encaminhamento da rede fica inconsistente relativamente às verdadeiras localizações dos terminais, pelo que, esta secção vai detalhar as acções adicionais que garantem que tanto a criação como a manutenção das decisões de encaminhamento se processa de uma forma garantida e consistente.

3.1.4.1 Garantia de entrega

Tal como foi analisado, os elementos da rede comunicam internamente com mensagens de sinalização proprietárias, encapsuladas em ICMP, de forma a propagar as localizações dos terminais móveis na árvore de nós.

Por usarem este protocolo, estas mensagens não têm garantias de entrega, pelo que podem ser perdidas e não chegarem ao seu destino, o que pode acontecer por diversos motivos, sendo os mais frequentes a ocorrencia de um erro de transmissão, ou se a mensagem for descartada no interior do encaminhador devido às filas internas estarem cheias.

Nesta situação, se uma destas mensagens de *update* fosse perdida, o processo de actualização da localização do terminal descrito anteriormente não seria concluído, porque os encaminhadores que não chegassem a ser avisados ficavam com a localização anterior do terminal, e não a mais actualizada, ficando a rede ficar num estado inconsistente, e o terminal deixaria de estar contactável para alguns destinos.

Para resolver este problema, as mensagens de *update* do TIMIP têm um mecanismo de entrega que garante que todos os encaminhadores envolvidos no processo vão receber a mensagem correctamente, por via de um mecanismo totalmente flexível que pode ser costumizado à medida das necessidades.

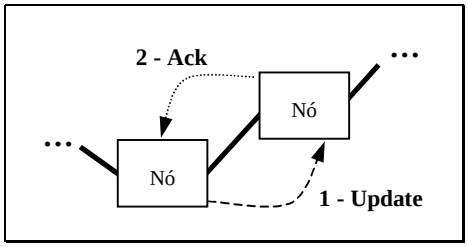


Figura 33: Garantia de entrega

Para tal, quando um nó recebe uma mensagem, este vai responder de imediato ao emissor com uma mensagem complementar do tipo *acknowledge*, utilizada para lhe indicar que a mensagem foi bem recebida (ver Figura 33), e por sua vez, depois de emitir uma mensagem, o emissor vai esperar que o seu nó adjacente lhe responda com o respectivo ack, porque quando isso acontecer, significa que este recebeu a mensagem com sucesso.

No entanto, se passar um determinado tempo limite[23] sem que a resposta apareça, então o emissor pode deduzir que a mensagem original foi perdida, pelo que recomeça o processo, reemitindo a mensagem original e recomeçando a espera.

Pode também acontecer que tenha sido a resposta, e não a mensagem original, que tenha sido perdida, não tendo neste caso o emissor nenhuma maneira de detectar esta diferença; nesta situação, o emissor vai de igual forma repetir a mensagem, pelo que o receptor pode recebe-la duas, ou mais vezes, não se originando neste caso concreto nenhuma inconsistência no estado da rede, uma vez que as acções despoletadas pelas mensagens de *update* são sempre idempotentes[24].

3.1.4.2 Sincronização dos APs

Os mecanismos anteriores que realizam a reconfiguração dos encaminhadores na rede de acesso só seriam suficientes se o processo fosse instantâneo, e em que o terminal nunca se poderia movimentar mais rapidamente que o próprio processo de registo, de modo a que a rede nunca ficava num estado inconsistente.

Efectivamente, esta condição nem sempre se verifica, dado as mensagens terem um tempo mínimo de transmissão e processamento, mas principalmente porque a perda das mensagens

[23] Este parâmetro timeout_ack é configurável no protocolo TIMIP (ver Anexo 8).

[24] Se tal não acontecesse, então seria necessário que as mensagens fossem numeradas sequencialmente de forma a detectar duplicações.

(e a sua consequente retransmissão) podem aumentar tempo total do *handover* várias ordens de grandeza do caso normal, de tal forma a que a rede ficará inconsistente durante esta actualização.

É durante este período que o terminal pode continuar a movimentar-se pela rede, de tal forma a que transite fisicamente para um outro AP, iniciando um segundo handover, de forma a que este poderá ficar concluído, enquanto o anterior ainda está em curso. Assim, em certas situações, a rede poderá ficar num estado inconsistente, se o terminal se mover mais rapidamente que o restabelecimento do estado na rede (ver exemplo detalhado no Anexo 7).

Para resolver este problema, tanto as mensagens de *update* como os seus *acknowlegdes* são marcadas com uma marca temporal (*timestamp*) única, relativa ao instante em que o *handover* foi iniciado, e que possibilita a resolução deste tipo de situações inconsistentes que acontecem na rede, pelo que para tal, cada nó vai associar ao registo do terminal o instante de tempo a que esta localização se refere, de forma poder-se distinguir de entre dois *handovers* em curso qual o mais recente.

Quando cada nó recebe uma mensagem de *update* que contém um *timestamp* mais antigo que o último deste terminal, então pode deduzir que quem lhe enviou a mensagem não tem a informação mais actualizada a respeito do terminal móvel (embora *pense* que tem, dado que lhe está a enviar um *update*), e este nó não vai responder como normalmente com o *acknowledge*, mas toma a iniciativa de informar este nó adjacente da localização mais actualizada do terminal, despoletando assim o processo de correcção do estado da rede nos nós que o necessitam (ver Figura 86 do exemplo detalhado no Anexo 7).

Neste sentido, será necessário incluir a informação temporal no processo de *handover*, de forma a garantir a consistência do estado da rede, sendo a fonte ideal para a recolha do tempo seria o relógio do próprio terminal, pois é único ao longo dos seus *handovers*, e poderia fornecer o valor de tempo exacto das transições, fornecendo valores sempre diferentes e crescentes.

No entanto, devido à característica de os terminais serem legados, isso significa que estes não vão ter necessariamente a capacidade de informar o seu AP do seu relógio, dado que esta é uma opção prevista em [27], embora opcional.

Assim, ter-se-á que excluir o terminal móvel de todas as acções de mobilidade, passando a ser o próprio AP que, quando detecta o terminal pela primeira vez, usa o seu próprio relógio como a base de tempo para o *timestamp* do terminal, obrigando a que os relógios de todos os

APs tenham que estar sincronizados entre si, de forma a possibilitar as comparações posteriores entre diferentes *handovers* concorrentes.

A acção de sincronização dos relógios dos APs entre si terá que ser efectuada por um mecanismo complementar ao TIMIP, como o protocolo de sincronização de tempo NTP [33], que resolve este problema de uma forma altamente satisfatória para esta função.

Como alternativa a esta funcionalidade, a recolha do valor do tempo também pode ser questionada directamente ao terminal por via de mensagens ICMP Timestamp Request/ Timestamp Reply (ver 3.2.2.8 de [27]), mas apenas quando a configuração do terminal indicar que este implementa esta funcionalidade. Por fim, uma outra hipótese para a recolha do *timestamp* está relacionada com o suporte de segurança, a descrever na secção 3.1.4.5).

3.1.4.3 Manutenção do estado

Depois das entradas de encaminhamento serem criadas pelos processos anteriores, estas são utilizadas no encaminhamento para os terminais móveis enquanto se mantiverem localizados no mesmo AP, sendo alteradas quando este se movimentar entre APs. Entretanto, os terminais podem ser desligados, ou movimentarem-se para fora do domínio, o que teria o resultado de manter indefinidamente as respectivas entradas, tornando o estado da rede inconsistente.

Para isto, as entradas de encaminhamento são definidas como sendo do tipo *soft-state*, tendo que serem periodicamente utilizadas sob pena de serem removidas automaticamente ao fim de um certo tempo limite (denominado de *timeout_remove*[25]), o que remove o estado dos terminais na rede de uma forma distribuída, quando estes forem desligados ou saírem do domínio, por as suas entradas deixam de ser utilizadas, repondo o estado da rede.[26]

Quando o terminal está parado num dado AP, então as suas entradas terão que ser periodicamente refrescadas pelo terminal, porque caso contrário seriam removidas, e com refrescamento, pretende-se que o terminal dê uma prova de vida à rede de forma a confirmar que ainda está localizado no mesmo AP, sendo para isto utilizados os pacotes normais de dados emitidos pelos terminais (encaminhamento *uplink*).

[25] Este parâmetro timeout_remove é configurável no protocolo TIMIP (ver Anexo 8).

[26] Note-se que o mecanismo do *timeout não* é usado para remover o caminho anterior num handover (como no caso do CIP); pelo contrário, é utilizada sinalização explícita para este efeito.

Neste tipo de encaminhamento, quando os nós da rede recebem pacotes IP de dados por uma das suas interfaces descendentes, então vão confirmar que o pacote foi entregue pelo nó onde o terminal tem registada a sua localização (i.e., é o *próximo nó* do terminal, conforme a tabela de encaminhamento). Quando isto se verifica, então essa é uma prova de que o terminal continua acessível pela mesma localização, sendo assim refrescada e adiado o *timeout* (**Situação A** da Figura 34).

Pode também acontecer a **situação B**, na qual um pacote IP aparece por uma interface que não é a mesma por onde o terminal está localizado; como os pacotes normais IP não vão criar ou alterar as entradas de encaminhamento, então as entradas de encaminhamento não vão ser refrescadas neste caso. Este situação é típica apenas durante a duração do processo de *handover*, na qual as entradas de encaminhamento ainda estão em estabilização.

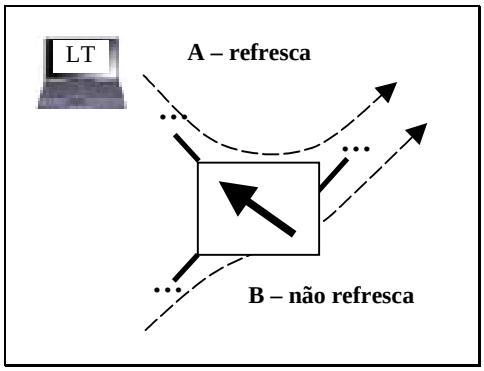


Figura 34: Refrescamento das entradas pelos pacotes IP

Este mecanismo significa que a manutenção do estado na rede dos terminais que estão activos é totalmente transparente e automática à medida que estes comunicam normalmente, não incorrendo em nenhum *overhead*, nem características especiais que não sejam suportadas pelos terminais legados.

No entanto, esta optimização só se pode aplicar aos terminais que estão activos a emitir pacotes de dados; para os receptores ou inactivos, a rede vai ter que forçá-los a dar uma prova de vida que refresque o registo do terminal com um mecanismo que todos os terminais IP suportem, sob pena de eliminar as suas entradas. Para isto, antes do *timeout* expirar[27], cada nó da rede vai gerar um pacote ICMP **EchoRequest** destinado ao terminal móvel, e com o valor

27 Parâmetro timeout_start da configuração do TIMIP (ver Anexo 8).

da GW no campo do emissor do pacote, encaminhando-o para o terminal da mesma forma que os outros pacotes de dados.

Quando o receber, o terminal vai ser obrigado[28] a responder à GW da rede[29] um correspondente ICMP **EchoReply**, o que tem o efeito de percorrer toda a rede precisamente nos nós que têm as entradas referentes ao terminal, refrescando-as de uma só passagem (ver Figura 35).

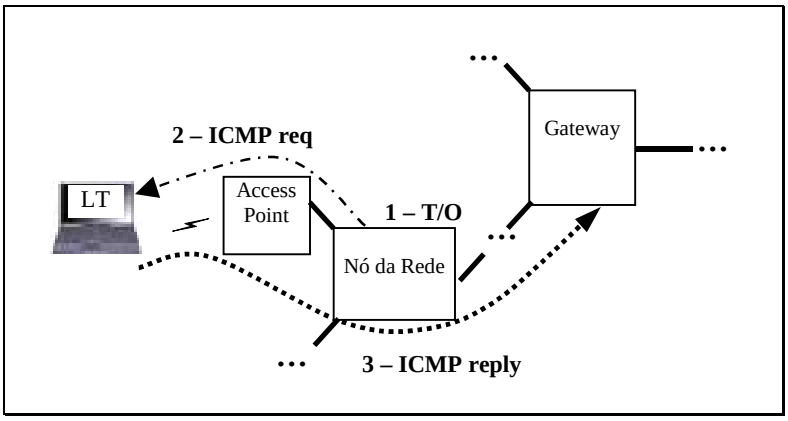


Figura 35: Refrescamento das entradas para terminais inactivos

Este mecanismo básico vai manter o estado dos terminais inactivos na rede ao forçá-los a activarem-se momentaneamente para responderem ao pedido de refrescamento, mas este processo de refrescamento pode gerar uma grande quantidade de tráfego, em especial se a rede contiver um grande número de terminais inactivos.

Para tal, o valor do *timeout* do envio do ICMP aos terminais vai ser dinâmico, sendo inicializado com o valor inicial na configuração, e variando depois conforme as respostas do terminal aos pedidos de refrescamento. Quando o nó pedir o refrescamento ao terminal, se este responder prontamente ao pedido então o nó vai duplicar o valor do *timeout* actual (até um valor máximo).

De uma forma complementar, se o nó não obtiver a resposta do terminal, quer seja porque esta se perdeu, ou o terminal já não se encontrar na rede, então o valor do *timeout* vai passar

28 De acordo com os requisitos dos *legacy hosts* "Every host MUST implement an ICMP Echo server function that receives Echo Requests and sends corresponding Echo Replies" (secção 3.2.2.6 de [27]).

29 Uma vez que o nó da rede em que expirou o *timeout* enviou o pacote como se fosse a GW

para metade, sendo o terminal removido quando este valor chegar a um mínimo pré-configurado.

Neste sentido, os pedidos de refrescamento vão variar de forma exponencial entre os dois extremos, da forma ilustrada na Figura seguinte, de forma a que a manutenção do estado ocupe significativamente menos recursos que no caso anterior, mas que ainda permita detecções rápidas da saída dos terminais da rede.

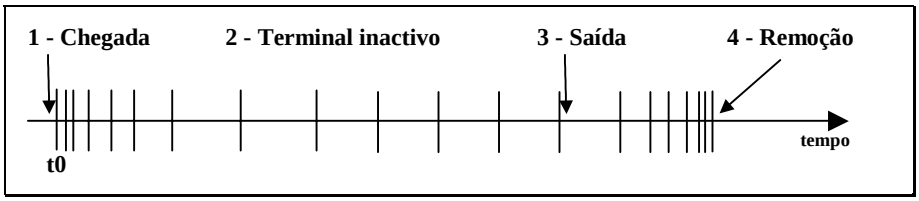


Figura 36: Frequência dos refrescamentos para um terminal inactivo

3.1.4.4 Registo TIMIP

Os mecanismos anteriormente descritos acima considerados assumem que os elementos da rede já conhecem os pormenores dos terminais móveis necessárias no processo de mobilidade, pelo que os terminais têm que efectuar um pré-registo na rede antes de terem conectividade, com os valores nos campos necessários relativamente às opções do protocolo que vão utilizar.

Este pré-registo pode ser efectuado de uma forma manual, mas também automaticamente quando o terminal suportar o mecanismo DHCP de configuração. Em ambos os casos, são guardadas na GW as seguintes informações por cada terminal da rede, das quais nem todas as opções são mandatórias, ou podendo ser descobertas por processos automáticos.

Tipo Opções	Dado	Utilização
Básicas	Endereço MAC	Fixo, ou obtido por DHCP
	Endereço IP	Fixo, ou alocado por DHCP
Protocolo	Opção Segurança TIMIP	none / secure_TIMIP
	Opção Timestamp	none / ICMP_TimeStamp_REQ / Secure_TIMIP
	Opção Macro-Mobilidade	none / surrogate_MIP / MIP
	Endereço Home Agent	Só usado para na opção sMIP
Segurança TIMIP	Chave FA<->MH	Chave de codificação secure_TIMIP para micro-mobilidade segura; Chave de codificação entre FA e MH, usada para autenticação MIP entre estas duas entidades
	Chave HA<->MH	Chave de codificação entre HA e MH, (apenas utilizada quando não houver segurança no terminal legado)
	Identificador NAI	Identificador DHCP opaco do terminal

Tabela 2: Dados de registo existente para cada Terminal

Esta tabela dos terminais é centralizada na GW, que a distribui periodicamente para elementos de rede, o que lhes permite terem a sua cópia actualizada destes dados, aumentando o desempenho dos *handovers*. O acesso a esta tabela é indexado pelo endereço IP do terminal móvel, dado que o protocolo opera no nível 3, mas também pode ser por outros campos em situações bem definidas: pelo endereço MAC quando for recebida a primitiva de detecção da fase 1 do protocolo; e pelo identificador NAI [30] quando se está a efectuar o pré-registo automático por DHCP com esta opção.

3.1.4.4.1 Suporte de registo DHCP

Relativamente à configuração automática do terminal, os parâmetros dos endereços de nível 2 e nível 3 podem ser configurados sem intervenção manual bastando que os terminais legados incluam o suporte do protocolo de auto-configuração DHCP[30] [29], que possibilita-lhes a

[30] Embora os terminais sejam *legacy* no sentido da mobilidade IP, é muito comum os sistemas operativos terem o suporte do DHCP.

alteração automática do seu endereço MAC[31], bem como a alocação de um endereço IP desta rede ao terminal.

Para isto, o processo do DHCP aplicado à rede TIMIP está resumido na Figura 37, no qual a GW da rede contém um servidor DHCP, e os terminais legados têm clientes DHCP. Para ligar uns e outros, todos os encaminhadores intermédios da rede têm as entidades DHCP relay agent, que permitem encaminhar devidamente os pedidos/respostas DHCP[32].

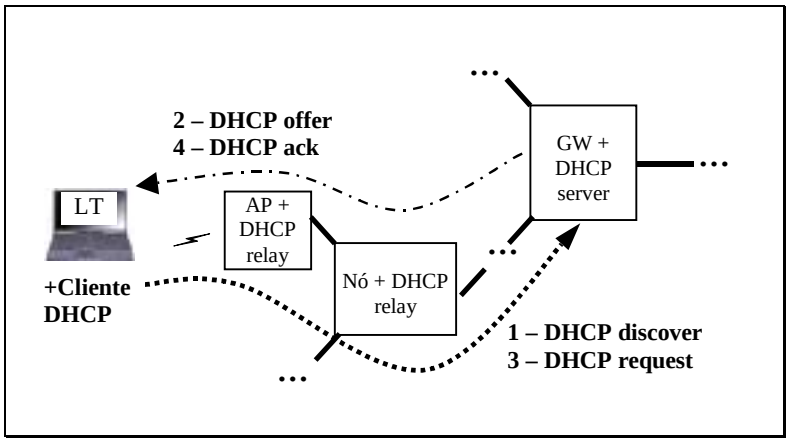


Figura 37: Auto-configuração do terminal por DHCP

Nesta arquitectura, o processo DHCP vai começar quando o terminal se activar pela primeira vez numa rede (ou quando a interface física de ligação *wireless* for alterada), emitindo uma mensagem DHCPdiscover em difusão para a sua interface *wireless*, com o objectivo de pedir à rede a atribuição de um endereço IP livre (**passo 1**). Neste pedido, o terminal identifica-se num campo próprio na mensagem[33] com um valor que ajude o servidor DHCP a distingui-lo dos outros terminais, o que pode ser pelo parâmetro NAI[34], ou pelo endereço MAC do terminal.

Esta mensagem é recebida pelo *relay agent* do AP, sendo encaminhada até ao servidor DHCP localizado na GW TIMIP, e em resposta, esta gera uma mensagem DHCPoffer que contém os

[31] Nomeadamente, o endereço MAC varia *sempre* que se troca a interface *wireless*.

[32] Este desenho é necessário porque o DHCP foi desenhado num modelo em que os clientes conseguem comunicar directamente por difusão com o servidor DHCP, o que não se verifica nas redes TIMIP.

[33] Campo CLIENT_ID do cabeçalho DHCP

[34] O NAI (Network Access Identifier) é um identificador único para cada utilizar num domínio, do tipo ("username@realm") e que é tratado como um *token* pelos processos de DHCP e mobilidade) [30].

valores para o terminal a utilizar nesta rede (**passo 2**), a qual percorre os nós da rede de forma semelhante ao anterior, sendo entregue ao terminal, que continua o processo emitindo um pedido formal DHCPrequest (**passo 3**) para o endereço IP que lhe foi proposto, sendo este confirmado pela GW com uma mensagem final DHCPack (**passo 4**).

Depois da recepção desta última mensagem, o terminal vai poder configurar-se automaticamente para utilizar a rede TIMIP, relativamente ao seu endereço IP alocado da rede, mas também com a máscara e o endereço IP da GW especiais, da forma definida na da secção 3.1.3.3.3 (e eventualmente com outras configurações como o DNS *server* da rede), ficando *do seu ponto de vista* apto a entrar na rede TIMIP.

Neste processo, o servidor DHCP da GW deverá estar em comunicação com a componente TIMIP, para que esta última possa ter as configurações mais actualizadas dos parâmetros de configuração do terminal móvel, sendo estas difundidas pelos elementos de rede pela GW.

Por outro lado, quando um terminal não tiver qualquer configuração na rede em relação ao seus endereços MAC e chegar pela primeira vez à rede, o AP que o receber não vai ter condições para o reconhecer.

Nesta situação, o processo de *power-up* inicial TIMIP fica temporariamente pendente até que o AP seja informado do par de endereços IP/MAC deste terminal (processo descrito acima), prosseguindo depois normalmente. Posteriormente, quando o terminal se movimentar no interior da rede, esta latência adicional já não vai acontecer porque os outros APs já receberam entretanto os dados mais actualizados do terminal.

3.1.4.5 Segurança no TIMIP

Esta última opção do TIMIP vai permitir o suporte de micro-mobilidade para os terminais legados de uma forma *segura*. Esta segurança é instanciada num mecanismo de autenticação de nível 3, suficiente e autónomo, que por si só garanta à rede a verificação da identidade dos terminais móveis, embora possam no futuro ser definidos novos mecanismos de utilização de soluções standard de autenicação já existentes.

A segurança do TIMIP consiste apenas na componente da autenticação – a verificação da identidade dos terminais – sem que as outras componentes normalmente associadas sejam contempladas, como a cifra dos dados emitidos, ou a contabilização dos recursos utilizados (*accounting*). Isto deve-se porque o TIMIP, ao prestar o serviço de conectividade móvel, deve ter a garantia de que o serviço só é prestado aos terminais que o têm direito, pelo que os

terminais, depois de serem detectados e identificados pela rede, terão de *provar* a sua identidade para concretizar o serviço.

Esta necessidade da autenticação dos terminais surge porque, sem a extensão de segurança, o serviço é prestado imediatamente, sem quaisquer reservas, aos terminais móveis que já estejam pré-registados na rede. Assim, quando o terminal é detectado pela rede através da primitiva de detecção, o AP onde o terminal se localizou vai converter o endereço MAC no correspondente endereço IP, e vai iniciar o processo de criação do encaminhamento na rede para este terminal, acontecendo isto com todos os possíveis terminais conhecidos pela rede e detectados pelo nível 2.

Por esta razão, isto significa que toda a segurança do protocolo em si iria residir na segurança e fiabilidade de cada tecnologia de rede particular. Em algumas tecnologias, estas já incluem mecanismos explícitos de segurança (tipicamente as tecnologias *wireless*), que visam controlar o acesso à rede física por meio de mecanismos de autenticação.

Neste cenário, só os terminais autorizados é que teriam acesso à rede, pelo que a primitiva de detecção só ia apresentar os endereços dos terminais autorizados, que o TIMIP seguiria cegamente.

Contudo, existem outras tecnologias mais simples que não vão ter qualquer segurança, o que significa que, para todos os terminais detectados no nível 2, o nível 3 irá construir os mecanismos de encaminhamento. Para este caso, um terminal atacante poderia forjar pacotes com o endereço MAC de um outro terminal autorizado, o que significaria que este iria, do ponto de vista do TIMIP, tomar a identidade do terminal atacado, de tal forma a que todos as comunicações destinadas ao terminal móvel atacado fossem entregues ao atacante.

Para realizar as suas operações de uma forma segura, o TIMIP possui o seu próprio mecanismo de autenticação de nível 3 baseado num mecanismo de *challenge*/*response* com assinaturas digitais que são geradas e confirmadas por chaves secretas partilhadas, garantindo a identidade dos terminais com um margem de erro que é praticamente tão baixa quanto se quiser.

Neste mecanismo de autenticação, a segurança vai-se basear na existência de uma informação secreta exclusiva – a chave – que terá partilhada apenas pelas duas partes envolvidas no processo de autenticação, e que são, necessariamente o próprio terminal, que é quem se vai autenticar, e um servidor de autenticação, que é quem verifica a identidade do terminal.

As chaves terão que ser geradas e entregues aos dois intervenientes de uma forma segura por outros meios que não o próprio TIMIP.

Cada terminal terá a sua própria chave única, e se esta se mantiver secreta para estes dois intervenientes, então a autenticação será segura, dado que o terminal pode provar que é ele mesmo, por apresentar uma assinatura que só ele é que pode gerar. Aqui um atacante que tentasse tomar a identidade do terminal já não poderia fazer esta prova, por não ter acesso à chave secreta, o que implicaria a suspensão do serviço de mobilidade.

Como o terminal é uma das partes envolvidas no processo de segurança, isto significa que os terminais legados para terem segurança vão ter necessariamente que suportar a autenticação do seu serviço de mobilidade, *mas* não o próprio serviço de mobilidade. Daqui resulta que os terminais legados seguros vão passar a ter um mínimo de inteligência própria relacionado apenas com este suporte de autenticação, de forma a que possa assinar, a pedido, mensagens de sinalização.

Assim, esta autenticação do serviço de mobilidade vai ser concretizada por um servidor muito simples de autenticação presente em cada terminal, utilizado para assinar mensagens que lhe são entregues, e que pertence ao nível de aplicação do terminal, o que mantém a sua pilha de protocolos TCP/IP inalterada.

Para os terminais móveis seguros, as operações de segurança são concretizadas sempre que um terminal chegue a um AP, decorrendo entre os pontos 2 e 3 da Figura 23 (página 58). Aqui, depois de o terminal ser detectado pelo AP e o TIMIP ser informado da sua presença, vai existir uma verificação da identidade do terminal, na qual se pede ao terminal que assine uma dada mensagem com a sua chave secreta.

Unicamente quando se obtiver uma resposta positiva para esta verificação é que o processo continua da forma que foi definida, pelo passo 3 que inicia a reconfiguração do encaminhamento na rede para este terminal, mas se a resposta não chegar, ou o teste der negativo, o AP vai tentar de novo um certo número de vezes até que desiste, o que bloqueando o processo de conectividade para este terminal.

Para concretizar este teste, vai existir uma sinalização muito simples entre o AP e o terminal. Estas mensagens são trocadas usando o encapsulamento UDP entre o cliente (presente no AP) e o servidor (presente no terminal), para um porto constante e conhecido deste.

Assim, o mecanismo TIMIP vai ter as seguintes acções adicionais que decorrem antes da reconfiguração do encaminhamento, e que estão ilustradas na Figura 38:

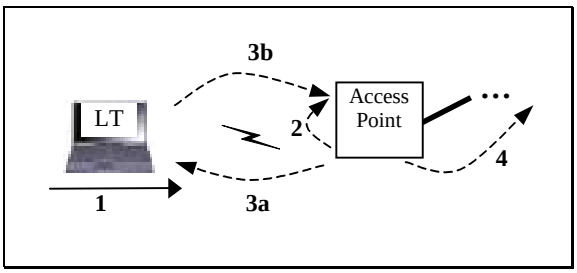


Figura 38: Autenticação dos terminais legados (TIMIP)

Depois de o terminal ser detectado pelo TIMIP (**passo 2**), o AP vai iniciar o processo de autenticação, gerando um valor aleatório, diferente de todos os anteriores para este terminal, e entrega o conjunto (IP, GW, Valor aleatório, *TimeStamp*) ao servidor de autenticação presente no terminal (**passo 3a**). Esta mensagem é passada por UDP para o porto conhecido do servidor, e é entregue ao terminal de uma forma directa, por nível 2 e sem encaminhamento[35].

O terminal, quando receber este conjunto, usa a sua chave secreta referente a esta rede (identificada pela GW) para assinar a mensagem, gerando uma resposta que contenha o conjunto (IP, GW, Valor', Time'). Aqui o Valor' vai ser o resultado de aplicação do algoritmo MD5 à mensagem original, o que produz uma assinatura específica (denominada por "*digest*") que é diferente de todas as outras anteriores (devido à utilização de um *timestamp* diferente de mensagem para mensagem). A mensagem final também inclui o *timestamp* do próprio terminal móvel, e a totalidade da resposta vai ser entregue ao AP (**passo 3b**).

Quando o AP receber esta resposta, este vai aplicar a mesma operação à mensagem original com uma cópia da chave secreta que a GW previamente lhe forneceum significando isto que a chave secreta passa a ser partilhada pelo terminal, pela GW e por todos os APs desta rede (que entre si podem trocar as chaves de uma forma segura). Deste modo, o AP vai gerar também uma assinatura MD5 da mensagem original, de forma a verificar se este é igual ao que o terminal lhe apresentou.

No caso negativo, que significa que o terminal não tem o acesso à sua chave secreta, pelo que do ponto de vista do TIMIP, este terminal não é quem diz ser, sendo nesta situação o processo TIMIP bloqueado, devendo o terminal ser desconectado usando um mecanismo apropriado de nível 2, de forma a tentar prevenir um ataque de *"denial-of-service"*.

[35] Directamente ao MAC, IP e Porto UDP do terminal. Esta entrega é igual aos processos MIP standard de entrega de pacotes entre Terminais e Agentes

No entanto, a regra geral será o caso em que a assinatura confere exactamente com a esperada, o que significa que o terminal provou com sucesso a sua identidade, uma vez que tem a sua cópia da chave secreta que lhe permitiu assinar a mensagem correctamente num curto espaço de tempo. O AP vai ficar com uma garantia extremamente elevada a respeito da identidade do terminal, porque o sistema MD5 garante que um outro terminal atacante necessitava de despender um esforço extremamente grande para gerar a assinatura que o AP está à espera.

Na situação em que o terminal provou a sua identidade, então o processo de micro-mobilidade vai prosseguir da maneira que já foi descrita anteriormente, na qual os nós apropriados da rede vão reconfigurar-se e comunicar entre si da forma apropriada (**passo 4**). Esta comunicação interna da rede é baseada em mensagens ICMP especiais, que não são autenticadas, e que qualquer terminal poderia facilmente gerar, que poderia dar lugar a outros ataques.

No entanto, os nós fronteira da parte administrativa da rede vão bloquear todas as mensagens de sinalização TIMIP que não tenham sido recebidas pelas interfaces internas da árvore de nós, porque só essas é que estão ligadas aos outros nós da rede (Figura 39). Se a parte administrativa da rede não oferecesse garantias relativamente à segurança física das ligações wired, então as mensagens de sinalização poderiam ser autenticadas com facilidade usando uma chave comum a todos os nós da rede, usando também assinaturas digitais semelhantes às descritas acima.

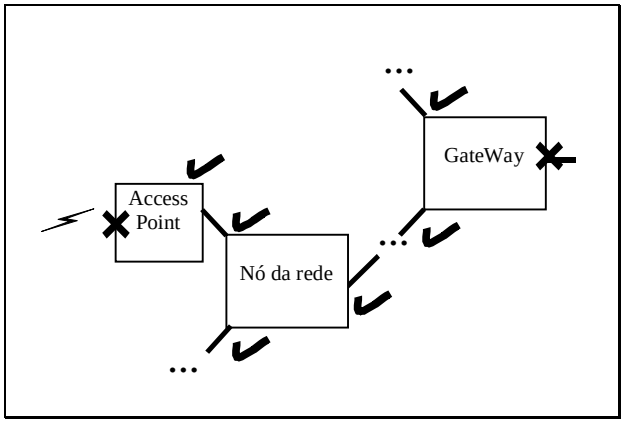


Figura 39: Interfaces que trocam sinalização TIMIP

Por ultimo, se alguma destas mensagens se perder, e nenhuma resposta for recebida, então todo o processo de autenticação vai recomeçar do início, gerando com um *novo* valor aleatório e um *novo timestamp*.

Uma optimização adicional possibilitada pela utilização do mecanismo de autenticação local dos terminais, é que neste caso o *timestamp* da detecção não vai ser o próprio relógio local do AP, mas sim o *timestamp* que está presente na resposta do terminal móvel. Isto permite que a resolução de situações ambíguas passe a utilizar *timestamps* gerados na mesma fonte (o terminal móvel), deixando de ser necessário (para estes terminais) a sincronização dos relógios entre os diversos pontos de acesso.

O mecanismo completo da segurança do TIMIP está esquematizado na seguinte tabela:

AP	gera (IP, GW, VALOR, TIME) e gera a assinatura MD5 com a chave apropriada
AP -> LH	Entrega (IP, GW, VALOR, TIME)
LH -> AP	Entrega (IP, GW, assinatura MD5, TIME')
AP	Verifica se as assinaturas MD5 são iguais

Tabela 3: Mecanismo de segurança TIMIP

3.2 Suporte de Macro-mobilidade para terminais legados usando o sMIP

3.2.1 Conceitos fundamentais

O **sMIP** é uma solução de macro-mobilidade que possibilita a mobilidade a *todos* os possíveis terminais IP ao longo de domínios TIMIP espalhados por qualquer localização da Internet. Para isto, o protocolo vai actuar de uma forma totalmente transparente para o terminal que goza desta mobilidade, criando as condições necessárias para que o seu tráfego seja correctamente encaminhado para todas as suas possíveis localizações.

Assim, vai ser a rede a executar em permanência o processo de mobilidade, que é activado quando o terminal transitar de domínio TIMIP (e *apenas* nesta situação), o que despoleta um processo automático denominado de *handover*, que altera o encaminhamento necessário de forma a manter a conectividade do terminal no seu domínio actual de acesso à Internet.

Este protocolo é uma extensão do standard de macro-mobilidade existente na Internet, o MIP, uma solução completa de suporte de mobilidade IP especialmente vocacionada para a mobilidade em larga escala, pelo que, o sMIP vai adicionar ao MIP clássico o suporte dos terminais legados, e também uma acção de detecção dos movimentos dos terminais que pode ser substancialmente mais optimizada que a detecção normal MIP.

Para isto, as acções chave do sMIP que permitem suportar terminais legados são análogas às efectuadas pelo TIMIP, embora adaptadas à diferente escala, na medida em que, são apenas os agentes de mobilidade que detectam os movimentos dos terminais, e têm a responsabilidade de gerar a sinalização necessária MIP para avisarem os outros agentes a respeito das novas localizações do terminal, o que terá o resultado de lhes manter a conectividade de uma forma totalmente transparente sem qualquer pedido por parte do terminal.

Por esta razão, este mecanismo é denominado de *surrogate* MIP, dado que essa é a palavra inglesa (técnica*)* que melhor descreve este comportamento especial dos agentes de mobilidade[36].

Por fim, note-se que actualmente este mecanismo só está definido para ser utilizado como complemento do protocolo TIMIP, de forma a criar uma solução de mobilidade *global* altamente eficiente, mas contudo, os dois protocolos são completamente separados entre si, e existindo um único ponto de contacto bem definido entre os dois na acção de detecção dos movimentos dos terminais[37].

3.2.2 Arquitectura do sMIP

A arquitectura do sMIP está presente na Figura 40. Tal como no MIP, o suporte da macro-mobilidade é efectuado por meio de entidades especiais fixas de mobilidade – agentes sMIP – que gerem as operações de macro-mobilidade, e que vão interagir entre si para criar e manter a mobilidade dos terminais móveis, embora, para aplicação nas redes TIMIP, os agentes estão limitados a serem únicos, e co-localizados na GW da rede TIMIP (ao contrário do MIP clássico em que os agentes podiam ser em qualquer número e lugar no interior da rede).

Por outro lado, por ser o único agente no interior do domínio, este vai desempenhar ambas as funções complementares de *surrogate* Home Agent, para os terminais móveis que pertencem a este domínio, e de *surrogate* Foreign Agent para os que estão a visitar.

---

36 Este termo tem exactamente o mesmo sentido que está descrito em [19], secção 4 “Registration requests generated on behalf of a mobile node”: “For reasons of backward compatibility with existing systems, it must be possible to implement Mobile IP without introducing Mobile IP signalling in the terminal. Registration requests/binding updates generated on behalf of a mobile node provide such a solution.”

37 Este ponto de contacto é semelhante ao ponto de contacto existente entre o TIMIP e o nível 2, no modelo reactivo de detecção (ver secção 3.1.3.1 na página 53)

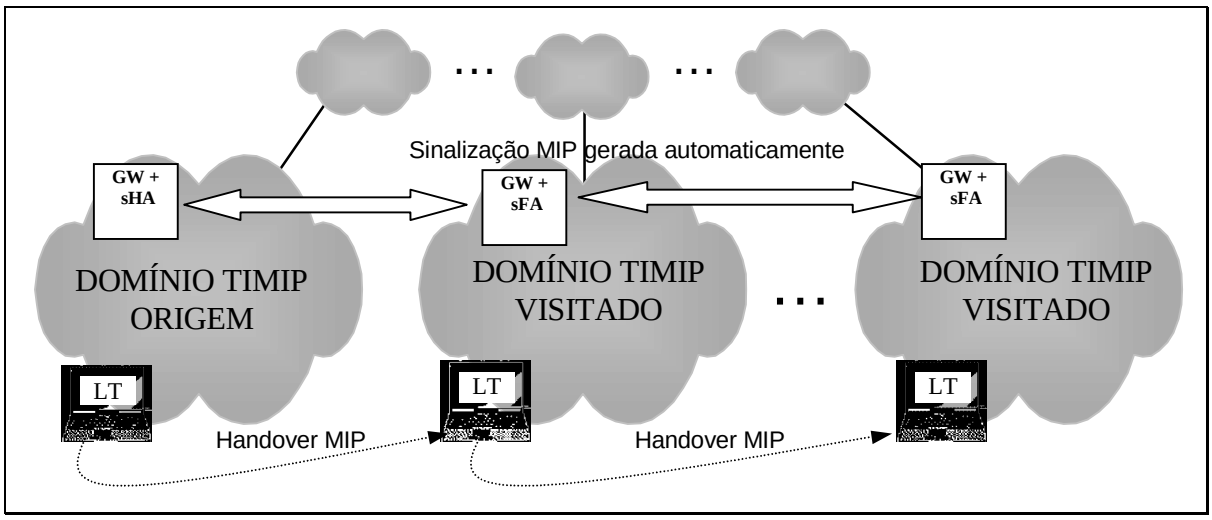


Figura 40: Arquitectura sMIP

Uma vez que estes agentes têm as condições para operarem sem interacções com os terminais, por executarem as operações de mobilidade em nome destes, então permite que arquitectura sMIP não os inclua. Assim, do ponto de vista do terminal, todas as operações que são efectuadas em seu nome pelos agentes vão decorrer automaticamente sem a sua intervenção, porque algum tempo depois de transitar fisicamente de domínio, este volta a ter condições para emitir e receber pacotes normalmente, como se estivesse localizado no seu domínio de origem.

Refira-se contudo, que devido à separação entre os dois tipos de mobilidade, os movimentos no interior do domínio, são da responsabilidade exclusiva do protocolo de micro-mobilidade TIMIP, e nunca sendo visíveis para a mobilidade sMIP.

3.2.3 Concretização da Mobilidade sMIP

Para o suporte da mobilidade entre domínios TIMIP, o sMIP vai usar o mesmo conjunto de mecanismos que o MIP e os outros protocolos de mobilidade, divididos em três fases - localização, registo e execução - que garantem a conectividade dos terminais na Internet.

Para isto, as duas primeiras fases são activadas em sequência apenas quando o terminal se movimenta e transita fisicamente de domínio, podendo ter chegado ao seu domínio de origem, ou a um outro domínio visitado, e que quando tal acontece, o agente do domínio actual detecta a chegada do terminal móvel, e inicia um *Handover sMIP* para que a conectividade do terminal se mantenha na sua nova localização.

Por outro lado, a fase final do processo de mobilidade (*Execução*) vai ser executada em permanência para cada pacote destinado e originado no terminal móvel, de forma a ser encaminhado para a localização correcta. Esta fase final do mecanismo opera de forma

independente das duas primeiras, seguindo apenas as configurações de encaminhamento geradas por estas.

3.2.3.1 Fase 1 sMIP - Localização

Esta fase do sMIP tem como objectivo a determinação da localização dos terminais, servindo esta para inferir a respeito da necessidade dos mecanismos de macro-mobilidade para os terminais. Enquanto que no MIP clássico são estes que têm a responsabilidade de se localizarem, recebendo os *beacons* de localização MIP que os agentes MIP emitem, neste protocolo esta fase é bastante simplificada, uma vez que os terminais não tomam parte do processo; como alternativa, dado que o sMIP opera em domínios TIMIP, então os agentes sMIP aproveitam as funções de detecção avançadas de micro-mobilidade do TIMIP, para as correspondentes da macro-mobilidade, uma vez que o TIMIP têm exactamente a noção da chegada do terminal.

Nesta conformidade, quando um terminal chega pela primeira vez à rede, vai ocorrer sempre um *power-up* inicial TIMIP, e no final deste, quando a GW for avisada da localização inicial do terminal (conforme a Figura 21 na página 56), então o TIMIP vai ter a oportunidade de avisar o sMIP da chegada deste terminal à rede, para este tomar as acções que entender necessárias. Este aviso é concretizado com uma primitiva de indicação do TIMIP para o sMIP, sendo este um exemplo de uma detecção reactiva.

Esta primitiva apenas indica o endereço IP do novo terminal móvel legado, porque é apenas esta a informação que a macro-mobilidade necessita; devido à separação dos dois tipos de mobilidade, o TIMIP vai esconder do sMIP outras informações que lhe são exclusivas, como a localização exacta do terminal no interior do domínio, dado que o sMIP apenas terá que criar as condições necessárias para que os pacotes destinados ao terminal sejam entregues ao seu domínio actual, e não no seu interior.

Pelas mesmas razões da separação entre os dois tipos de mobilidade, o TIMIP só vai gerar a primitiva de chegada da *primeira* vez que o terminal é detectado na rede, de forma a esconder as movimentações internas do terminal na rede.

3.2.3.2 Fase 2 sMIP - Registo

Quando o agente sMIP é avisado da chegada do terminal, este vai verificar a sua identidade, de forma a executar diferentes papeis consoante o terminal pertencer a este domínio, ou não.

No primeiro caso, então o agente sMIP faz o papel de *surrogate* Home Agent, e o mecanismo de macro-mobilidade não vai ser necessário, dado que neste caso o endereço IP do terminal

reflecte correctamente a sua localização física actual (ie, o seu domínio), pelo que os mecanismos anteriores de macro-mobilidade, se existentes, são cancelados.

Contrariamente, quando o terminal não pertencer ao domínio em que foi detectado, então a macro-mobilidade é necessária porque o endereço IP do terminal legado leva a que todos os nós da Internet infiram que este está fisicamente localizado no interior do seu domínio de origem, o que não se verifica.

Nesta última situação, o agente sMIP vai tomar o papel de *Surrogate* Foreign Agent para este terminal, e vai tomar a iniciativa de ele próprio gerar a sinalização standard MIP como se fosse o terminal, sinalização esta, que tem por objectivo contactar o Home Agent deste terminal particular, localizado na rede de origem do terminal, para este participar na macro-mobilidade.

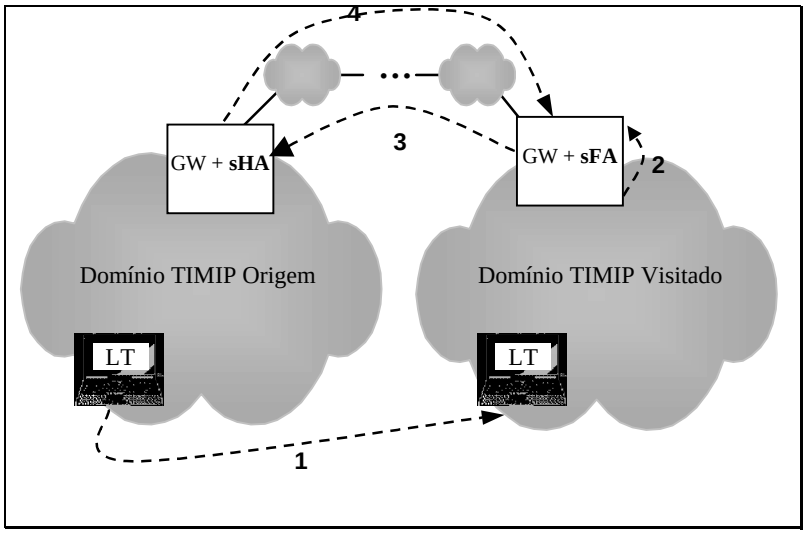


Figura 41: Fase de registo sMIP

Todo este processo está ilustrado na Figura 41, em que um terminal legado se movimenta de forma a transitar de domínio TIMIP (**passo 1**). Quando chega ao novo domínio, vai ser criada a micro-mobilidade TIMIP da forma já descrita anteriormente, e no final deste processo, o TIMIP na GW vai avisar o sFA da chegada do terminal por meio da primitiva de indicação (**passo 2**).

Esta primitiva contém apenas o endereço IP do terminal que chegou à rede, o que vai permitir ao Agente MIP aceder às outras informações relativas a este terminal, uma vez que o agente vai ter uma base de dados que relaciona os terminais que são aceites nesta rede. Entre outras informações, esta tabela terá a identificação do Home Agent deste terminal, que está localizado no seu domínio de origem.

De posse destas características, o sFA vai poder dar início ao processo sMIP, efectuando um *handover* MIP para o terminal entre os dois domínios envolvidos. Num cenário clássico de MIP, o terminal gerava um pacote *register MIP* pelo qual indica ao HA a sua localização actual – o seu FA – sendo este pacote este entregue ao HA pelo seu FA.

Pelo contrário, no mecanismo sMIP, vai ser o sFA que vai começar directamente neste último passo, entregando ao HA o pedido de registo, no qual se indica ele próprio o endereço de care-of (i.e., a localização actual do terminal móvel), e no qual indica a identidade do terminal móvel pelo seu endereço IP no campo específico. Os outros campos são preenchidos com os valores típicos que o terminal escolheria (*lifetime*, *flags*, etc.). No final, este pacote é enviado pela Internet desde o sFA para o HA do terminal móvel como normalmente (**passo 3**).

Quando o Home Agent receber este pedido de registo, este vai agir como normalmente no MIP clássico, aceitando o registo gerado pelo sFA como se tratasse do terminal móvel, e por via deste, o HA vai ficar a conhecer a localização física do Terminal Móvel, e vai criar os mecanismos de Macro-Mobilidade que vão possibilitar, na última fase do processo, que os pacotes destinados ao Terminal Móvel sejam entregues no domínio actual.

Por fim, o HA vai responder com um pacote MIP de resposta ao registo original, sendo entregue ao FA (**passo 4**). Nesta situação, o sFA então irá também criar os mecanismos necessários de Macro-Mobilidade para suportar este Terminal Móvel, finalizando assim o processo de registo da macro-mobilidade.

Além desta fase ser utilizada para criar, alterar e remover os mecanismos de macro-mobilidade MIP, quando o terminal transitar de domínio em domínio, esta fase também vai ser utilizada para manter o registo MIP, dado que este é criado no modelo *soft-state*.

Assim, é o sFA que tem a responsabilidade de periodicamente renovar o registo do terminal móvel, reemitindo o registo MIP, tal como o terminal móvel o faria.

No entanto esta operação de refrescamento não vai ter nenhuma relação com os movimentos internos do terminal no interior da rede, uma vez que se referem a tipos de mobilidade distintos, não sendo visíveis entre si. Assim, este refrescamento vai continuadamente ser efectuado pelo sFA da forma normal definida pelo MIP, até que o terminal sai da rede, quer por ser desligado, ou por transitar para outra rede qualquer.

Quando isto acontece, o TIMIP vai detectar esta situação e remover o suporte de micro-mobilidade para este terminal, o que leva a GW TIMIP a avisar o sFA, por meio de outra

primitiva, a respeito da saída do terminal. Quando a receber, o FA vai também remover o suporte do terminal, o que cancela o refrescamento do registo MIP.

3.2.3.3 Fase 3 sMIP - Execução

A fase anterior vai criar e manter os mecanismos necessários de encaminhamento para o terminal móvel, sendo o próprio encaminhamento o objecto da fase 3 do protocolo MIP, pois vai ser efectuado continuamente para cada pacote para/de o terminal móvel legado, em que o primeiro é o objectivo do encaminhamento *downlink*, e o outro o encaminhamento *uplink*.

Nesta fase de execução, o MIP vai-se encaixar perfeitamente na correspondente fase de execução do TIMIP. Todo este processo está ilustrado na Figura 42, que documenta o caminho que um pacote toma desde um emissor até a um terminal móvel legado no interior de uma rede TIMIP/sMIP.

3.2.3.3.1 Encaminhamento *downink*

De início (**passo 1**) um pacote destinado ao terminal móvel é emitido pelo emissor e será encaminhado pela Internet pelos mecanismos de encaminhamento normais até à rede de origem deste terminal móvel. Nesta situação, o HA da rede vai capturar o pacote, verificar que se destina a um terminal móvel que está neste momento localizado por este FA específico, pelo que vai encapsular o pacote num túnel IPIP destinado a este FA e envia-lhe o pacote encapsulado (**passo 2**).

Quando este pacote encapsulado é recebido pela GW da rede TIMIP, a sua componente de sFA vai verificar que o pacote original é destinado a um terminal que está neste momento localizado no interior desta rede TIMIP, e assim, o FA vai desencapsular o pacote original destinado ao terminal móvel, e expor o pacote original, o que termina a sua parte no encaminhamento *downlink*, pois o pacote já está no domínio certo.

Seguidamente, o pacote vai continuar a ser encaminhado no interior da rede até ser finalmente entregue ao terminal, sendo estas operações da responsabilidade exclusiva da micro-mobilidade TIMIP, da forma já descrita anteriormente.

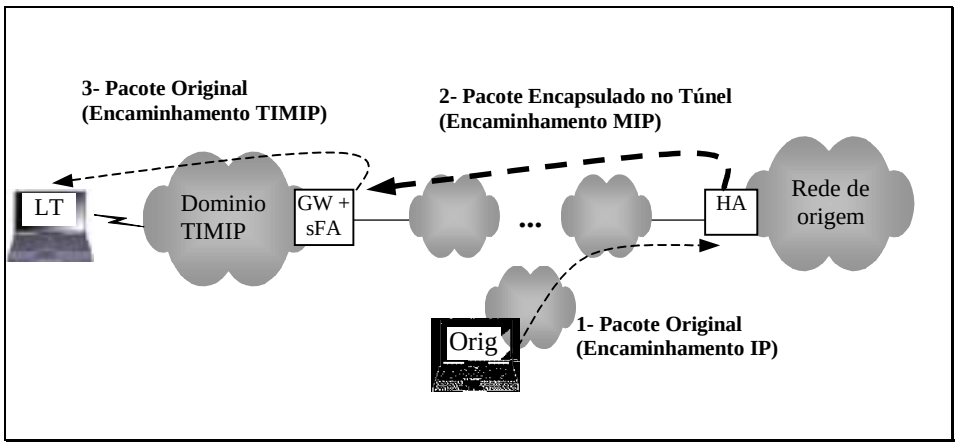


Figura 42: Encaminhamento downlink MIP para uma rede TIMIP

3.2.3.3.2 Encaminhamento *uplink*

O segundo caso de encaminhamento é mais simples que o anterior. Os pacotes emitidos pelos terminais móveis (*tráfego uplink*) são inicialmente encaminhados até à GW da rede TIMIP (encaminhamento *uplink TIMIP*), pelos processos TIMIP. Uma vez na GW, estes pacotes são enviados pelos processos normais IP para os seus destinos finais (encaminhamento *uplink MIP*), que podem eventualmente serem destinos móveis MIP e/ou TIMIP.

No entanto, vai existir o mesmo problema para o encaminhamento *uplink* sMIP, que já existia relativamente ao *uplink* TIMIP, e que consiste na entrega à rede dos pacotes dos terminais móveis. Recorde-se que este problema é resolvido no TIMIP considerando que o terminal estará configurado com o valor da GW da sua rede, e com uma máscara que o obriga a entregar todos os seus pacotes a esta gateway, fazendo cada AP *proxy* ARP para endereço IP com o seu próprio endereço MAC.

Numa situação de macro-mobilidade para terminais móveis, este problema vai voltar a aparecer, uma vez que os terminais só vão entregar correctamente o seu tráfego *uplink* aos APs no interior da sua rede de origem TIMIP. Para resolver este problema, os terminais móveis que se movimentam entre redes distintas vão ser configurados com gateway especial, comum em todos os domínios TIMIP – uma gateway "*dummy*" – que todos os APs de todos os domínios TIMIP reconhecem, com o valor "1.1.1.1".

Desta forma, o terminal vai poder sempre entregar transparentemente os seus pacotes a todos os APs de todas as redes TIMIP, que estas irão encarregar de encaminhar os pacotes para os seus destinos finais automaticamente.

3.2.4 Segurança no sMIP

Tal como o TIMIP, o sMIP também requer mecanismos de autenticação dos terminais, pelas mesmas razões já apresentadas anteriormente, e que lhe permitem limitar a utilização do serviço de macro-mobilidade apenas aos terminais legados autorizados.

Para isto, o sMIP vai usar o mesmo mecanismo de segurança que o MIP, baseado em assinaturas digitais, no qual cada terminal partilha com o seu Home Agent uma chave única com a qual ambos assinam e podem verificar a autoria das mensagens de sinalização trocadas. Adicionalmente, também pode existir autenticação entre os terminais e os Foreign Agents, e entre os agentes entre si (opcionais no MIP, dado que a chave HA<->terminal é obrigatória e suficiente para autenticar o serviço na componente crítica do HA). Assim, a sinalização sMIP gerada pela GW do terminal terá que ser assinada pela chave secreta do terminal móvel, por forma a ser aceite pela seu HA.

Para esta operação, o sMIP utiliza o mesmo servidor de segurança TIMIP já referenciado, que terá assim mais funcionalidades relativas à autenticação sMIP. Neste cenário, o terminal continua a ser legado por ter a sua pilha TCP/IP inalterada, incluí o servidor de autenticação ao nível da aplicação, que apenas assina mensagens que são geradas pela GW para si, sendo esta operação executada de uma forma segura.

Por outro lado, a chave utilizada na micro-mobilidade TIMIP passa a ser a chave MIP partilhada entre o terminal e cada Foreign Agent particular, existindo tantas chaves quantos os domínios TIMIP/FAs diferentes. No caso particular de o terminal móvel legado estar localizado na sua rede de origem, então a sua chave TIMIP de micro-mobilidade seria a mesma com que o terminal comunicaria o seu HA (a chave MH/HA).

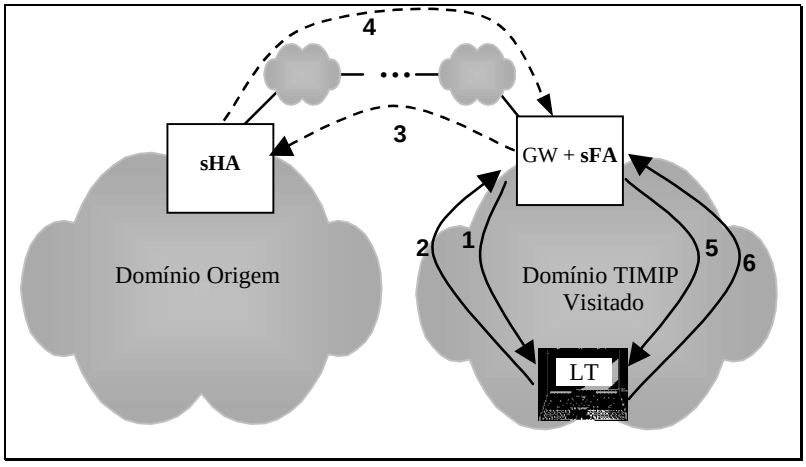


Figura 43: Segurança no sMIP

Na Figura 43 estão presentes os passos adicionais da mobilidade sMIP quando é utilizada a opção de segurança. Esta figura é igual à que descreve o registo sMIP sem segurança (Figura 41), com a diferença dos passos adicionais locais no interior da rede (marcados com as setas contínuas 1, 2, 5 e 6).

Após o processo de micro-mobilidade estar concluído, o sMIP vai gerar periodicamente a sinalização MIP que vai permitir a este terminal legado estar localizado neste domínio. Para isto, o agente presente na GW vai gerar um pedido "register MIP" que inclui a extensão de autenticação obrigatória MH/HA, a qual apenas falta a assinatura em falta.

Esta mensagem é entregue ao servidor de autenticação presente no terminal, usando o caminho que foi entretanto estabelecido na micro-mobilidade, para que este a assine com a chave MIP (**passo 1**), mas contudo, para evitar ataques, este pedido é assinado pelo sFA com a mesma chave FA/MH usada na autenticação TIMIP.

Quando o terminal recebe esta mensagem, este confirma se a mensagem foi realmente enviada pela GW desta rede, pela verificação da assinatura, e em caso afirmativo, então o terminal vai poder acrescentar a sua própria assinatura ao pedido MIP (do qual desconhece o seu interior, por não saber a sinalização MIP), e assinando o resultado com sua chave TIMIP para este domínio, entregando tudo de volta à GW (**passo 2**).

Esta, quando a recebe, vai poder verificar que o pedido MIP foi assinado pelo terminal correcto, verificando a assinatura exterior, e fica em condições de enviar o registo MIP para o HA do terminal. Aqui, o processo segue os passos já descritos anteriormente (**passos 3 e 4**), nos quais o HA vai receber uma mensagem com a assinatura correcta, como se tivesse sido originada no terminal móvel como está definido no MIP clássico, e respondendo com uma mensagem de sucesso.

No final, a mensagem de resposta também terá que ser confirmada a respeito da sua proveniência, de forma à GW o poder aceitar, pelo que, são executados os passos adicionais **5 e 6**: a resposta MIP, assinada pela GW, é entregue ao terminal, que vai verificar se ambas as assinaturas são validas, tanto a assinatura exterior da GW, como a assinatura interior do seu HA.

Quando isto acontece, então o terminal vai responder com uma resposta final de aceitação do pacote, sendo este assinado com a sua chave local. No final o sFAa vai poder confirmar a assinatura final do terminal, de forma a aceitar a resposta MIP e concluir o processo de *surrogate* macro-mobilidade.

O mecanismo completo da segurança do sMIP está esquematizado na seguinte tabela:

Entidade	Passo	Acção
GW	0	Gera (registo MIP)
GW -> MH	1	Entrega MD5(chave FA/MH, GW, (registo MIP))
MH -> GW	2	Entrega MD5(chave FA/MH, MD5(HA/MH, (registo MIP)))
GW -> HA	3	Entrega MD5(chave HA/MH, (registo MIP))
HA -> GW	4	Entrega MD5(chave HA/MH, (resposta MIP))
GW -> MH	5	Entrega MD5(chave FA/MH, GW, MD5(chave HA/MH, (resposta MIP)))
MH -> GW	6	Entrega MD5(chave FA/MH, “OK”)
GW	7	Processa (resposta MIP)

Tabela 4: Mecanismo de segurança TIMIP

3.3 Suporte de Macro-mobilidade para terminais MIP usando o MIP

Esta secção vai descrever as características que o TIMIP detém para suportar o MIP como protocolo de macro-mobilidade. Embora o protocolo sMIP já apresentada seja uma solução que suporta os terminais legados, a divisão actual em micro e macro mobilidade obriga a que todos os protocolos de micro-mobilidade suportem o standard MIP.

Para isto, é a GW TIMIP que terá o suporte MIP, contendo o Agente MIP que realiza ambas as funções de Home e Foreign Agent. No entanto, relativamente ao suporte do MIP, existe uma diferença em relação ao caso anterior, porque aqui os outros nós da rede também têm adicionalmente de ter um suporte mínimo especial relativamente aos pacotes de localização MIP, dado que terão que ser passados ponto-a-ponto desde a GW aos terminais móveis e vice-versa.

Do ponto de vista de uma rede TIMIP, o seu suporte do MIP é dividido em dois casos distintos, quer esta rede TIMIP seja a rede visitada por um terminal móvel, ou a rede de origem de um terminal que está neste momento a visitar uma outra rede qualquer.

Na primeira situação, o processo tem início quando o terminal chega pela primeira vez à rede, começando por realizar as acções normais de micro-mobilidade, por via de um *Power-Up* TIMIP, ficando nesta altura finalizada toda a conectividade da responsabilidade da micro-mobilidade, a qual consiste no caminho criado entre o terminal móvel e a GW.

Depois da micro-mobilidade TIMIP estar completa, o processo vai ser finalizado com uma operação de *handover* MIP para esta rede, executando tanto o terminal móvel, como a GW no papel de FA e o HA (localizado algures na Internet), os seus papéis nas operações MIP. No entanto, estas fases têm algumas alterações que são realizadas no lado dos nós administrativos da rede TIMIP, por forma a que os clientes possam usar os seus clientes MIP tal como foram definidos no contexto das subredes IP clássicas[38].

3.3.1 Concretização da Mobilidade MIP

3.3.1.1 Fase 1 MIP - Localização

Na fase de localização do MIP clássico, os Agentes de mobilidade MIP emitem periodicamente *beacons* MIP para anunciar o seu serviço. Estes *beacons* são emitidos directamente por nível 2 e em difusão para a interface de rede, porque numa rede clássica IP este procedimento é suficiente para atingir todos os terminais móveis que se encontram no interior da rede, mesmo que não tenham conectividade de nível 3.

No entanto, uma vez que os nós da rede estão dispostos em árvore, este comportamento significaria que os *beacons* MIP só iam chegar ao primeiro nível (a contar da GW) da árvore de nós, uma vez que os nós TIMIP não encaminham pacotes de difusão. Para resolver este problema, cada nó TIMIP está preparado para, sempre que recebe *beacons* MIP, os encaminhar explicitamente por todos os seus descendentes; desta forma, estes *beacons* MIP são gerados pela GW e são difundidos por toda a rede até aos APs, chegando desta forma a todos os terminais móveis MIP que estejam neste domínio TIMIP.

No sentido oposto, o terminal móvel também pode requisitar o anúncio da existência de Agentes de mobilidade MIP. No entanto, estes pacotes também têm considerações semelhantes aos *beacons* MIP: os pedidos são enviados pelo cliente MIP em difusão, de forma a todos os Agentes de mobilidade presentes nesta rede o receberem e agirem em conformidade. No contexto TIMIP, como apenas existe um único agente MIP localizado na GW TIMIP, os pedidos de *beacons* MIP são capturados pelo AP onde o terminal móvel está, e este é encaminhado da mesma forma (ponto-a-ponto), desde o AP até à GW pela árvore de nós. Quando o pacote chegar à GW da rede, o agente MIP vai receber o pedido de *beacon* tal e qual como numa subrede IP clássica.

[38] Isto é, é o TIMIP que tem que criar as condições para o MIP correr tal como está definido, e não o oposto

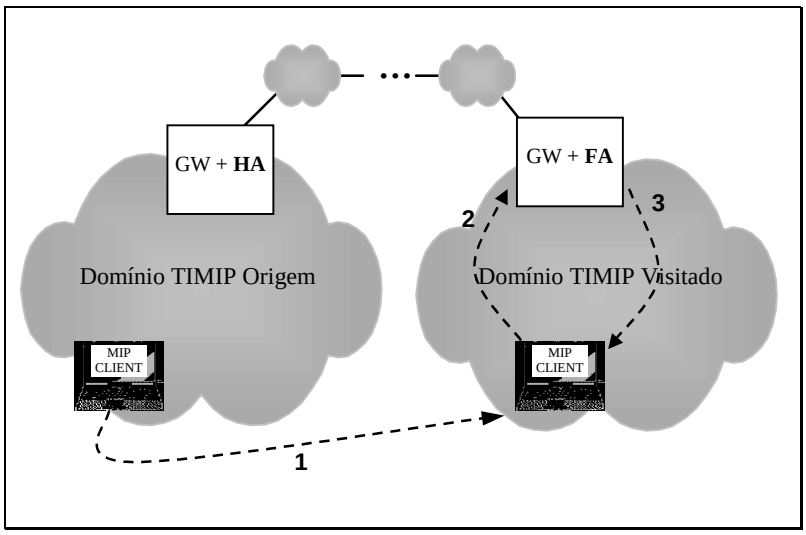


Figura 44: Fase de localização MIP

Note-se que neste modelo ambos os protocolos de micro e macro mobilidade são completamente independentes um do outro, não podendo o MIP beneficiar das informações do TIMIP como no caso do sMIP.

Desta forma, o MIP faz pelos seus próprios meios a detecção da necessidade de transição, o que faz que esta fase demore *sempre* mais tempo num cenário MIP do que num cenário sMIP, pois neste a fase de localização termina assim que o processo obrigatório de micro-mobilidade se concluir.

3.3.1.2 Fase 2 MIP - Registo

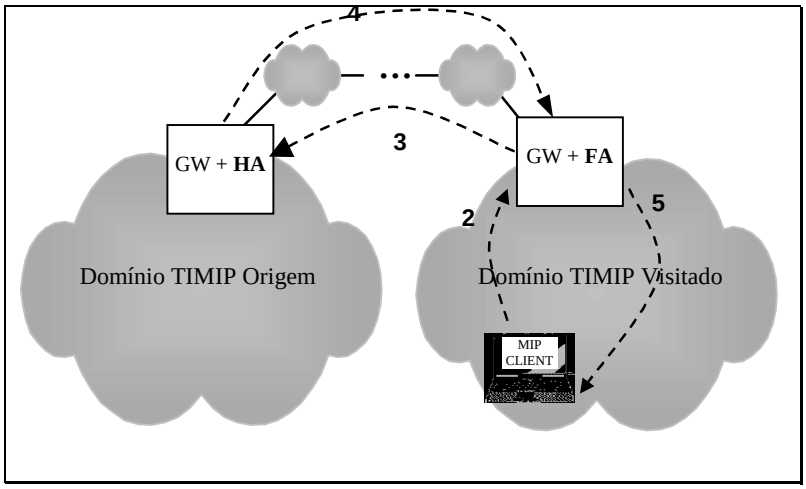


Figura 45: Fase de registo MIP

A fase de registo vai ser activada pela fase anterior no terminal, quando este transita de rede, e periodicamente para manter o seu registo; estas acções não vão ter nenhuma relação com os movimentos internos do terminal no interior da rede, pois estes são da exclusiva

responsabilidade do TIMIP. Assim, o terminal vai-se registar no seu HA por via do seu FA, que é sempre o mesmo ao longo do domínio TIMIP.

Para isto o terminal vai gerar ele próprio um pedido *Register* MIP normalmente, sendo este entregue ao AP, que o encaminha para o FA da rede (**passo 2** da Figura 45)[39], o que é possível usando o caminho normal criado pela micro-mobilidade. Quando o recebe, o FA vai agir como normalmente, e vai processar e entregar o pacote ao HA do terminal, localizado na sua rede de origem (**passo 3**).

Este, após processar o registo e criar os mecanismos apropriados, vai responder com um *acknowledge* ao terminal, por via do FA (**passo 4**), sendo este por fim entregue ao terminal no final do processo (**passo 5**).

Note-se que estas operações são protegidas de eventuais ataques pelos mesmos mecanismos de segurança do MIP clássico, nomeadamente pela utilização da chave MH<->HA partilhada entre o terminal e o seu Home Agent.

3.3.1.3 Fase 3 MIP - Execução

A fase anterior vai criar e manter os mecanismos necessários de encaminhamento para o terminal móvel. O próprio encaminhamento é o objecto da fase 3 do protocolo MIP, sendo continuamente efectuado para cada pacote para/de o terminal móvel.

Na fase de execução, o MIP vai-se encaixar perfeitamente na correspondente fase de execução do TIMIP, onde todo o processo é exactamente igual quando o terminal é legado, e o FA faz sMIP, pelo que, a descrição do processo usa a mesma Figura 41 (ver página 84), que documenta o caminho que um pacote toma desde um emissor até a um terminal móvel no interior de uma rede TIMIP/MIP (encaminhamento *downlink*).

3.3.1.3.1 Encaminhamento *Downlink*

De início (**passo 1**) o pacote destinado ao terminal móvel é gerado pelo emissor e é encaminhado pela Internet pelos mecanismos de encaminhamento normais até que chega à rede de origem deste terminal móvel. Nesta situação, o HA da rede vai capturar o pacote, verificar que se destina a um terminal móvel que está neste momento localizado por este FA

[39] o terminal vai entregar o pacote *register* MIP directamente ao AP, porque é daqui que este vê os *beacons* MIP a aparecerem, e este usa o seu endereço MAC para entregar o registo MIP.

específico, pelo que vai encapsular o pacote num túnel destinado a este FA e envia-lhe o mesmo (**passo 2**).

Quando este pacote encapsulado é recebido pela GW da rede TIMIP, a sua componente de FA vai verificar que o pacote original é destinado a um terminal que está neste momento localizado no interior desta rede TIMIP. Assim, para finalizar o encaminhamento, basta à GW da rede expor o pacote original, desencapsulando-o do túnel, e proceder aos mecanismos da fase 3 da micro-mobilidade TIMIP que entregará o pacote ao seu destino final, da forma que já foi descrita anteriormente.

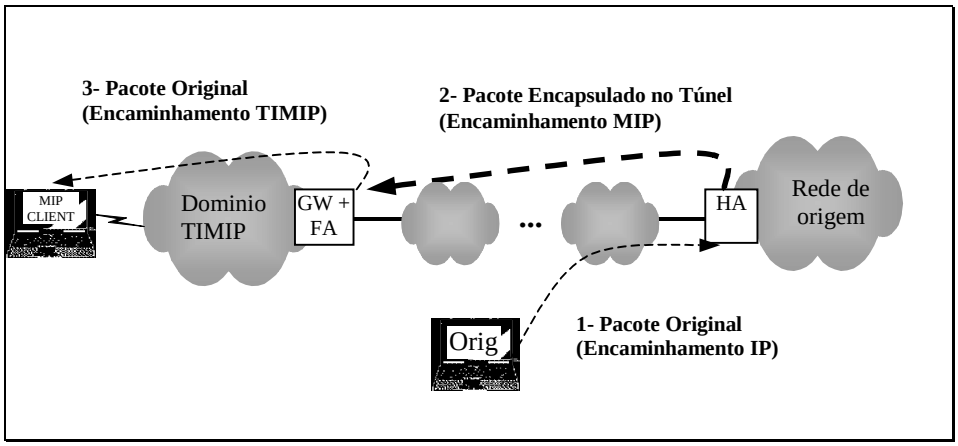


Figura 46: Encaminhamento downlink MIP para uma rede TIMIP

3.3.1.3.2 Encaminhamento *Uplink*

O segundo caso, do ponto do vista da rede TIMIP, é mais simples. Os pacotes emitidos pelos terminais móveis (*tráfego uplink*) são inicialmente encaminhados até à GW da rede TIMIP (encaminhamento *uplink TIMIP*), sendo depois enviados pelos processos normais IP para os seus destinos finais (encaminhamento *uplink MIP*), que podem eventualmente serem destinos móveis MIP e/ou TIMIP.

3.4 Avaliação da solução de Mobilidade Global (TIMIP + MIP/sMIP)

3.4.1 Avaliação do protocolo TIMIP

Esta secção vai avaliar o protocolo TIMIP no contexto isolado da micro-mobilidade, relativamente às suas características específicas de arquitectura, desempenho dos *handovers* e encaminhamento, escalabilidade e robustez.

Arquitectura:

O protocolo TIMIP apresenta uma arquitectura semelhante aos outros protocolos de micro-mobilidade, mas detém no seu desenho duas diferenças principais (entre outras menores) comparativamente com as outras propostas existentes.A primeira diferença fundamental é que o TIMIP define com rigor que as componentes activas do protocolo são *sempre* os elementos da rede no segmento administrativo, ao invés do próprios terminais móveis, tendo os encaminhadores da rede todas as funções necessárias autónomas para gerir todo o processo de mobilidade dos terminais, relativamente à detecção, criação, manutenção e cancelamento do serviço de mobilidade.

É esta abordagem radicalmente diferente de *todos* os protocolos já apresentados no IETF que confere a principal originalidade e interesse do TIMIP como uma proposta séria para um *novo* protocolo de micro-mobilidade a ser utilizado na Internet, permitindo assim a mobilidade IP de *todos* os possíveis terminais IP existentes. Para tal, o TIMIP define como activos os encaminhadores mais próximos dos terminais (APs), que depois de os detectarem vão tomar as acções activas do protocolo como suas, contactando a restante rede da forma necessária para criar ou manter a mobilidade já existente.

A segunda diferença principal do protocolo refere-se à assumpção explícita que o mecanismo primário de detecção dos movimentos dos terminais é um mecanismo reactivo, pelo qual o nível 2 avisa a chegada dos terminais por via de uma primitiva simples normalizada.

Esta característica do desenho do TIMIP é também original em comparação com os protocolos de micro-mobilidade IP já propostos, dado que os mecanismos de detecção destes são limitados ao nível IP, sendo substancialmente mais lentos que os proporcionados pelo nível 2. Neste sentido, o TIMIP é original por não seguir o modelo clássico OSI de separação dos protocolos apenas para a acção de detecção dos movimentos, dado que esta será a melhor forma de atingir o nível de desempenho pretendido.

Por outro lado, apenas para as tecnologias que não tenham possibilidades de suportar o modelo reactivo, o TIMIP também fornece a possibilidade de uma forma de detecção passiva, na qual terá (na maioria dos casos) um desempenho da ordem de grandeza dos modelos passivos propostas nos outros protocolos de micro-mobilidade.

Além da detecção, o TIMIP também dá grande importância à optimização da alteração do estado nos encaminhadores da rede, que é o objecto da fase de registo do protocolo, sendo

esta efectuada por mecanismos comparáveis aos dos outros protocolos de mobilidade, dado que o TIMIP segue essencialmente as mesmas bases da optimização do registo.

Neste sentido, o TIMIP também organiza os encaminhadores numa arquitectura hierárquica em árvore, dado que está será a topologia que permite as alterações do estado mais rápidas e próximas do terminal, sendo este alterado com uma única mensagem de *update* que é processada por todos os nós entre os APs envolvidos na transição do terminal.

Por fim, o TIMIP também se distingue dos outros protocolos de micro-mobilidade por concentrar optimizações no domínio do encaminhamento dos pacotes de dados dentro do domínio, e relativamente à manutenção do estado, que será sem *overhead* na rede para os terminais activos, e com um peso reduzido para os não-activos[40].

Desempenho dos Handovers

De acordo com o que foi descrito anteriormente, as movimentações dos terminais são executadas em duas fases consecutivas, que têm optimizações específicas.

Relativamente à fase de localização, o TIMIP assume como base o caso óptimo em que a tecnologia oferece um suporte mínimo necessário para o acção reactiva, e apenas a acção passiva no caso contrário. Neste sentido, o caso de maior desempenho do TIMIP acontece quando a localização seja for do tipo reactivo, em que a detecção da necessidade da mobilidade IP ocorre imediatamente após a finalização da transição física do terminal.

Nestas condições, como na maioria das tecnologias o terminal está fisicamente incontactável durante todo este período de transição física, então a fase de detecção incorre apenas numa latência marginal da responsabilidade do nível IP no processo de *handover* dos terminais.

Além desta acção reactiva, o protocolo também inclui a facilidade de um mecanismo passivo, independente da tecnologia, que permite ao protocolo funcionar nas tecnologias que não sejam capazes de suportar o suporte mínimo que o mecanismo reactivo necessita. Este mecanismo passivo já não tem o mesmo desempenho cuidado do mecanismo reactivo, tendo (na maioria dos casos) um desempenho da ordem de grandeza dos outros modelos passivos já propostos anteriormente.

[40] No entanto, este peso não é nulo por o TIMIP não possuir (ainda) suporte da função de *paging*

Relativamente à acção de registo, esta será exactamente igual para ambos os tipos de detecção, beneficiando assim ambas das optimizações desta fase, e que têm genericamente o objectivo de envolver o número mínimo de interacções necessárias no interior a rede, considerando tanto o número e a distância dos nós que vão comunicar.

Assim, depois da detecção automática, o AP pode identificar o terminal e começar imediatamente o seu processo de registo, dado que este já terá todas as informações que necessita usando a sua cópia da informação (centralizada na GW da rede), o que lhe permite começar imediatamente o processo de aviso dos nós adjacentes, exceptuando-se o caso em que o terminal tenha que ser previamente questionado a respeito da sua identidade, sendo esta uma opção da política de segurança. Nesse caso particular, então é necessário ainda a troca rápida do par *challenge/response* entre o AP e o terminal (adjacentes entre si), o que é também suficiente dado que o AP já tem a cópia da chave deste terminal relativa a esta rede.

A alteração do encaminhamento na rede processa-se de uma forma completamente local, sendo apenas envolvidos os nós da rede que ligam, pelo caminho mais curto na árvore, os dois APs envolvidos no *handover*, privilegiando as acção que aceleram a alteração do conjunto de nós a notificar. Para isto, cada nó quando recebe a mensagem de sinalização, vai imediatamente passar esta ao próximo nó, de forma a informár-lo da movimentação do terminal, para só depois alterar a sua própria tabela de encaminhamento e enviar o *acknowledge* da mensagem que recebeu ao nó anterior.

Do ponto de vista da velocidade do *handover*, a maioria das comunicações vai ser reestabelecida assim que seja criado o novo caminho desde o novo AP até ao nó *crossover*. Para isto, a latência máxima até o restabelecimento da ligação será limitada, dado que este nó em questão estará tão próximo do terminal na àrvore de nós como em distância geográfica.

A única excepção a esta regra é relativa aos emissores que estão localizados na parte da árvore anterior, (por baixo do *crossover*), uma vez que estes nós ainda estão a utilizar a localização anterior do terminal, pelo que a mensagem de *update* continua a ser propagada até ao AP final, por forma a finalizar a reconfiguração da rede.

Conclui-se assim que em condições óptimas, o TIMIP vai começar directamente após o *handover* de nível 2, e apenas terá que informar alguns (poucos) nós a respeito da nova localização do terminal, que estarão sempre proximos do terminal. Como apenas se terá que informar alguns nós pelo backbone da rede, e que vão realizar alterações locais de encaminhamento, então pode-se considerar que a latência introduzida pelo nível 3 é pequena comparativamente com a latência do nível 2, que vai desta forma dominar a latência total.

Por outro lado, mesmo no pior caso, a latência introduzida pelo nível 3 continua na maioria dos casos a ser menor que a sua correspondente no nível 2, desde que o protocolo for reactivo; esta situação acontece quando o terminal, depois de ser detectado, ter que ser questionado a respeito da sua identidade (introduzindo 2 mensagens locais AP<-->MH), e que se tenha que percorrer toda a rede desde o AP actual, até ao AP anterior (passando pela GW da rede).[41]

Desempenho do Encaminhamento

Além da atenção especial que o TIMIP dá ao desempenho dos *handovers* locais (fases 1 e 2), este também cria as condições necessárias para que os pacotes sejam encaminhados da forma mais rápida e directa possível, por forma a melhorar a latência total para as comunicações entre os utilizadores, e minimizar a ocupação dos recursos no interior da rede.

Assim, depois de o *handover* se ter processado, cada nó da rede no caminho directo desde o AP até à GW passa a ter uma entrada directa de encaminhamento para o terminal com a indicação do próximo nó para o terminal, o que significa que quando existe um pacote que lhe é destinado, este vai ser encaminhado rapidamente pela rede, sem nenhum encapsulamento ou outra qualquer acção em cada nó que não seja a simples consulta por parte do módulo de *forwarding* da tabela de encaminhamento, por forma a colocar o pacote na interface ligada ao próximo nó.

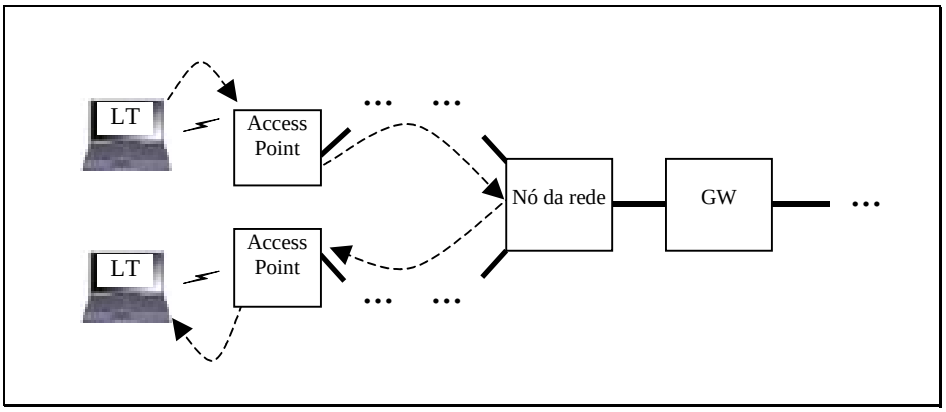


Figura 47: Encaminhamento intra-domain optimizado

[41] Esta característica da velocidade de alteração do encaminhamento é semelhante ao protocolo HAWAII; no entanto, do ponto de vista do tráfego *intra-domain*, no protocolo CIP o *handover* acaba sempre mais cedo, bastando que o *update* chegue ao crosshover. No entanto, esta optimização é minimizada por o CIP obrigar a *todo* o tráfego passar pela GW da rede.

Por outro lado, esta forma de encaminhamento também garante que os pacotes seguem sempre pelo caminho mais curto no *interior da rede*, o que permite optimizar em grande escala as comunicações *intra-domain* (ver Figura 47), porque desta forma só no pior caso é que envolvem a GW[42]. Nas redes do tipo empresarial, em que os terminais têm grande tendência para comunicar entre si, e especialmente com os que lhes estão próximos, esta optimização vai melhorar a utilização dos recursos da rede como um todo.

Escalabilidade:

Devido às suas características, o TIMIP só vai ter uma escalabilidade suficiente para o tipo de mobilidade para que foi desenhado – micro-mobilidade, concluindo-se que esta escalabilidade vai ser menor que as outras propostas, mas mesmo assim ainda na mesma ordem de grandeza, por o seu desenho se apoiar nos mesmos princípios básicos dos outros protocolos.

Este facto deve-se por duas opções principais de desenho, que privilegiam o desempenho do protocolo tanto nas vertentes dos *handovers* como no encaminhamento, em detrimento da escalabilidade.

Por um lado, o TIMIP organiza os nós da rede numa estrutura hierárquica em árvore, que tem o objectivo de aumentar o desempenho das movimentações, por possibilitar os *handovers* locais. No entanto, o TIMIP também define que cada nó da rede terá entradas directas de encaminhamento para os terminais que estão acessíveis por si, o que privilegia o desempenho do encaminhamento dos pacotes, por estes o serem da forma mais directa possível sem recurso a encapsulamento.[43]

Conjugando estas duas opções de desenho básicas, comuns aos outros protocolos de micro-mobilidade CIP e HAWAII, então verifica-se que a principal incapacidade de escalabilidade para além de domínios IP reside em que a GW da rede ter necessariamente a informação

[42] Tal como o HAWAII, e ao contrário do CIP e o HMIP.

[43] Esta situação pode ser comparada com os encaminhadores das redes de core, que têm uma entrada para cada rede na tabela de encaminhamento, e tendo esta tabela que ser consultada para cada pacote a encaminhar; no entanto, existe a diferença essencial que as rede de core conseguem manter o número de entradas de *routing* sempre na mesma ordem de grandeza, aproveitando a estrutura hierárquica do endereçamento IP para a grupar as redes a encaminhar de uma forma hierárquica.

completa da localização de *todos* os terminais presentes na rede na sua tabela de encaminhamento.[44]

Sabendo-se que para cada pacote que venha do exterior da rede, e também do interior provenientes de outra parte da árvore, esta tabela tenha que ser consultada, isso vai limitar o número máximo de terminais activos aos quais se pode fornecer um serviço satisfatório; esta situação é minimizada por a maioria do tráfego interno da rede não chegar a passar necessariamente pela GW, por acção da optimização do encaminhamento.

Num nível mais secundário, o TIMIP tem outras características que também limitam a escalabilidade do protocolo, como a utilização do mecanismo de manutenção do estado (ver secção 3.1.4.3). Esta necessidade também está presente nos outros protocolos de encaminhamento, mas no TIMIP prevê-se explicitamente que as entradas de encaminhamento sejam refrescadas pelos pacotes normais gerados pelos terminais, o que efectivamente elimina a necessidade do refrescamento dos terminais activos[45].

Por outro lado, quando o terminal passa a estar inactivo, então a rede vai começar a gerar *beacons* para a manutenção do estado, mas os quais são sujeitos ao controle ("backoff") já descrito, de forma a não ocuparem em demasia os recursos da rede (que tanto o CIP e ou HAWAII não possuem).

Além disto, tanto o CIP como o HAWAII definem mecanismos de *paging* que permitem reduzir a sinalização trocada dos terminais com a rede, e no caso do CIP, de adicionalmente manter apenas os terminais activos na tabela de encaminhamento principal dos encaminhadores (e os inactivos numa tabela secundária).

Contudo, embora o TIMIP não detenha desta funcionalidade, note-se que os terminais não trocam qualquer sinalização com a rede, por serem legados (exceptuando as acções de segurança), e que a segunda vantagem do CIP pode ser facilmente emulada como opção de implementação por mecanismos hierárquicos de *caches* a aplicar na relativas à na tabela de encaminhamento dos *routers*.

Por fim, a última limitação da escalabilidade do TIMIP reside no facto de os APs da rede terem que estar sincronizados entre si, para utilização apenas para os terminais que não têm a

[44] E, num nível secundário, os outros nós dos níveis mais elevados da árvore.

[45] Da mesma forma que o protocolo CIP

opção de segurança, e que garantem a resolução correcta das inconsistências do estado dos terminais na rede.

Neste sentido, o protocolo TIMIP apenas é escalável para utilização em estruturas limitadas IP. No entanto, devido à divisão do suporte da mobilidade nos dois tipos, esta situação não incorre em dificuldades, dado que os movimentos mais amplos seram comportados pelo protocolo complementar de macro-mobilidade.

Robustez

Relativamente ao seu desenho, o TIMIP também não tem na sua forma actual uma robustez total, sendo identificados dois problemas importantes:

Por um lado, a sua arquitectura (partilhada por todos os outros protocolos de micro-mobilidade) assume um único nó GW na árvore de nós em cada domínio, que se revela num ponto único de falha da rede, no caso de esta ficar indisponível por qualquer motivo. No entanto, note-se que mesmo nesta situação os terminais no interior da rede ainda podem comunicar (o que não se verifica no CIP), podendo-se melhorar a robustez dos nós por medidas de redundância física.

Por outro lado, o TIMIP ainda não tem mecanismos de recuperação de falhas como a reinicialização dos nós, baseando-se actualmente a robustez apenas no mecanismo de *soft-state*, podendo tal situação ser solucionada pela adição de novos mecanismos e mensagens para considerar esta situação particular, sendo um dos tópicos a considerar como trabalho futuro.

Conclusão

Como conclusão, o protocolo TIMIP responde com muito bom desempenho ao suporte da micro-mobilidade dos terminais legados, mas terá que ser limitado apenas a domínios IP de dimensões limitadas, por não ser escalável extensões maiores, tendo todos os nós da rede que suportarem o protocolo TIMIP e estarem organizados numa estrutura obrigatória de árvore. Para a mobilidade em distâncias maiores, terá que ser utilizado um mecanismo de macro-mobilidade, que já detém esta escalabilidade necessária, possibilitado pelo detrimento do desempenho final atingido.

3.4.2 Avaliação da Solução de Mobilidade Global (TIMIP + sMIP/MIP)

Considerando a solução global de mobilidade apresentada, a componente de macro-mobilidade é baseada completamente no MIP clássico, ao qual são apenas aplicadas as

diferenças necessárias para o suporte dos terminais legados. Desta forma, as considerações que se aplicam ao sMIP são as mesmas do MIP, com algumas diferenças pontuais.

Assim, o protocolo sMIP é usado como complementar do TIMIP pela sua escalabilidade que lhe permite ser estendido ao longo de toda a Internet, dado que fornece a transparência na localização para ambos os extremos da comunicação do terminal móvel, bem como aos encaminhadores genéricos que ligam as redes entre si.

Esta transparência e estabilidade nestes vários níveis é atingida pela criação dinâmica de túneis entre os domínios de origem e visitado do terminal móvel, que são utilizados para redireccionar os pacotes destinados ao terminal na sua localização actual.

Desempenho dos Handovers:

Todos os protocolos baseados no MIP têm problemas de velocidade no *handover*, dado que as mudanças físicas do terminal obrigam sempre que o Home Agent seja informado acerca da nova localização do terminal, por forma a restabelecer o túnel IPIP para o novo local. Isto significa que, para trocar de rede visitada, o *handover* do terminal requer a propagação da sinalização de registo entre o domínio visitado e o domínio de origem, por forma a restabelecer a conectividade.

No entanto, quando se usa o sMIP/MIP em redes TIMIP, o número de *handovers* que se vão realizar do tipo MIP vai decrescer de forma acentuada, porque agora só vai haver um único registo por cada transição física do terminal entre os domínios TIMIP. Como comparação, um domínio TIMIP poderá equivaler a várias redes IP, o que é o suficiente para transformar os *handovers* MIP entre as redes adjacentes do mesmo domínio em *handovers* optimizados TIMIP.

Esta optimização é possibilitada pela divisão da mobilidade, em que os movimentos no interior da rede são da responsabilidade exclusiva do protocolo de micro-mobilidade, sendo assim transparentes na macro-mobilidade.

Por outro lado, o sMIP tem um comportamento semelhante, dado que este só é activado no *power-up* inicial TIMIP, e não nos subsequentes *handovers* TIMIP; na opção MIP, o mesmo é concretizado dado que apenas existe um único agente FA na GW, que é único para a totalidade do domínio TIMIP, o que leva o MIP a considerar que o terminal está imóvel no interior da rede, não necessitando de acções de mobilidade.

Desta forma (ver Figura 48) as duas formas de mobilidade não têm interferência uma com a outra, o que mantém o grande grau de independência entre as duas, tendo como resultado final

que o terminal vai gozar, na maioria das vezes, de *handovers* rápidos TIMIP, conjugados com *handovers* MIP lentos, utilizados em exclusivo para as transições de domínio, e o resultado final o aproveitamento total do modelo de divisão da mobilidade em macro e micro-mobilidade.

Este duplo suporte de mobilidade é passível de ser aplicado aos terminais móveis legados de uma forma totalmente transparente e automática, o que significa que estes nunca vão ter a noção que se estão a movimentar, tanto dentro como entre domínios.

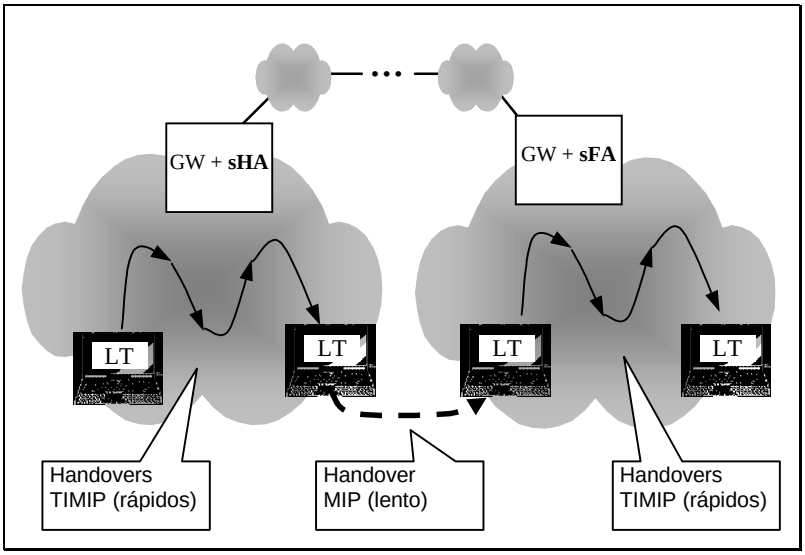


Figura 48: Integração do TIMIP com o MIP (handovers)

Além disto, mesmo os *handovers* sMIP que restam também são acelerados, na medida em que a detecção dos movimentos do sMIP se baseia num modelo reactivo, sendo este automaticamente despoletado quando o *power-up* do TIMIP terminar, o que significa que não existe a fase de localização MIP, na qual se recorrem a *beacons* MIP para os terminais se localizarem.

Nestas condições, quando o próprio TIMIP for também baseado numa tecnologia de rede reactiva, então ambas as fases de detecção do TIMIP e sMIP terão latências marginais, reduzindo-se desta forma apenas à sinalização desde o AP até ao agente, seguido do agente até ao HA.[46]

[46] Com a opção de segurança sMIP, esta vai acrescer mais dois pacotes locais no interior da rede, que não são significativos em comparação com o tempo necessário para avisar o HA.

No entanto, quando se usa o MIP clássico, este já não vai poder beneficiar desta optimização, mesmo quando sejam utilizadas redes TIMIP. Isto acontece porque por o MIP ser totalmente independente do TIMIP, este terá que detectar, pelos seus próprios meios, os movimentos do terminal, o que como já foi descrito, é um processo lento.

Desempenho do Encaminhamento:

Relativamente à forma como os pacotes são encaminhados, estes vão seguir exactamente os mesmos processos que o MIP clássico, nomeadamente os pacotes destinados ao terminal móvel serem todos encaminhados primeiramente pela rede de origem do terminal, parta depois serem encapsulados num túnel para o FA actual do terminal, para serem por fim desencapsulados e encaminhados no interior do domínio. Desta forma, existe o mesmo problema da triangulação, e do consumo de recursos adicional devido a este encapsulamento que no MIP clássico.

Relativamente a estes problemas de desempenho do domínio da macro-mobilidade, o sMIP poderia adoptar sem dificuldades as mesmas optimizações de desempenho e outras capacidades que estão a ser definidas pelo grupo de trabalho do MIP, nomeadamente as descritas em [6], [7], [8] e [9].

Escalabilidade:

De igual forma que o MIP, o sMIP tem características semelhantes de escalabilidade, o que lhe permite sem dificuldade concretizar a mobilidade à escala mundial, nomeadamente por não requerer modificações além dos agentes de mobilidade, e no caso único do sMIP, pela primeira vez também nos clientes móveis.

No entanto, o suporte ao MIP/sMIP nos domínios TIMIP terá uma escalabilidade inferior que o MIP clássico, uma vez que só suporta um único agente MIP por domínio TIMIP, que terá que estar co-localizado na GW do domínio. Pelo contrário, no MIP clássico previa-se possibilidade da existência de vários agentes dos dois tipos em cada rede, utilizável tanto para o aumento da robustez a falhas como da distribuição do serviço.

4. Descrição da Rede de Acesso Wireless e Tecnologias associadas

Este capítulo descreve em detalhe a rede *wireless* do projecto MOICANE que contribuiu para a motivação desta tese de Mestrado, e para a demonstração pratica das tecnologias descritas. Assim, na primeira secção vão ser descritas as necessidades específicas desta rede, a sua integração com as outras redes e ilhas, e a descrição dos componentes que a constituem.

Esta descrição é complementada na secção seguinte por um resumo das tecnologias recentes utilizadas na rede de acesso, e que foram recentemente normalizadas pelos organismos competentes - o 802.11 pelo IEEE, e o Diffserv pelo IETF.

4.1 Rede de acesso

4.1.1 Enquadramento da rede de acesso no MOICANE

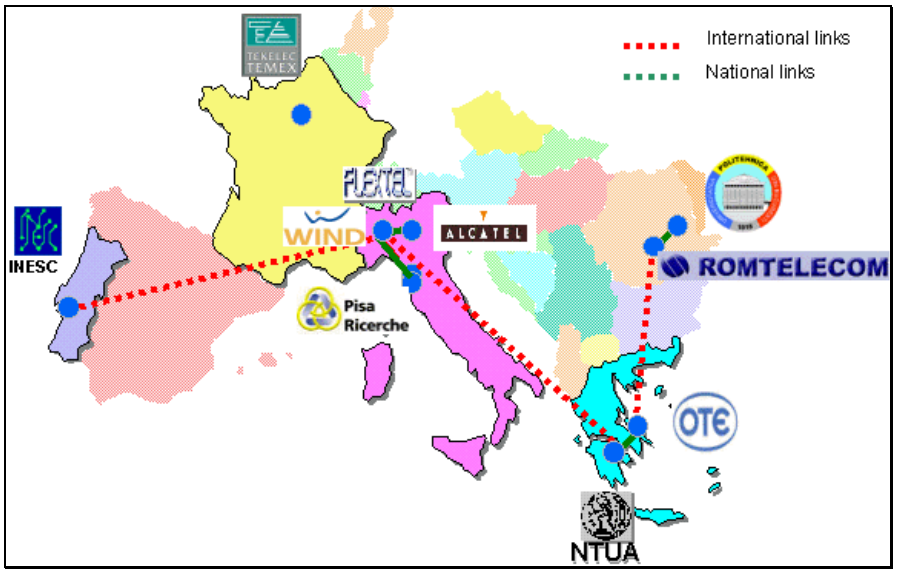


Figura 49: Arquitectura global do MOICANE

A rede internacional de demonstração criada para o projecto MOICANE está delineada na Figura 49, onde várias ilhas pertencentes a cada parceiro estão interligadas entre si por ligações internacionais. O objectivo principal deste projecto será o de analisar as novas tecnologias IP de suporte de qualidade de serviço, nomeadamente o Diffserv e o Intserv, com a análise destas tecnologias verificada tanto num contexto local, onde se considera apenas o interior de cada ilha por si, mas também numa perspectiva global ao longo de todas as ilhas e

ligações internacionais, por forma a existir durante todo o caminho dos fluxos de dados um suporte de qualidade de serviço permanente extremo-a-extremo.

Desta forma, cada participante no projecto tem a responsabilidade de criar uma ilha, constituída por um conjunto de redes de acesso e uma rede de suporte (*core*), sendo as primeiras mais vocacionadas para o teste e demonstração de novas tecnologias de rede, e as segundas para o estudo do suporte de QoS, usando mecanismos escaláveis e integrados ao longo dos vários domínios, recriando as necessidades das redes de core da Internet.

O demonstrador internacional final vai ser testado através da utilização de aplicações com diferentes requisitos de qualidade, como sejam aplicações de laboratório virtual e ensino à distância, o que leva a passar pela rede diferentes fluxos de dados prioritários, nomeadamente Voz, Áudio, Vídeo e Dados, que terão que coexistir com tráfego sem requisitos de QoS, como transferências de ficheiros ou simples tráfego de carga da rede.

Assim, será possível demonstrar o suporte de QoS extremo-a-extremo, tanto no interior como ao longo das várias ilhas, pelo que, tanto as ilhas como as ligações internacionais vão ter mecanismos de suporte de QoS, sendo as primeiras escaláveis, flexíveis e da responsabilidade de cada parceiro, e as segundas fixas e da responsabilidade dos vários provedores de serviço que oferecem as ligações ponto-a-ponto entre as ilhas[47].

De um modo global, o suporte do QoS foi realizado principalmente com base no modelo de Serviços Diferenciados, sendo este complementado ou substituído por outros mecanismos complementares caso-a-caso para algumas redes específicas, como a integração do modelo de serviços integrados no Diffserv por conversão.

Neste modelo, cada rede vai constituir um domínio DiffServ, formando a rede do MOICANE uma região DiffServ, e o suporte de QoS entre domínios assegurado através de Níveis de Serviço Contratados (SLAs - *Service Level Agreements*) que, para além dos aspectos contratuais, definem as características do serviço que a rede cliente espera receber e que a rede fornecedora se compromete a assegurar.

[47] No entanto, devido a dificuldades fora do controlo do projecto, nem todas as ligações internacionais tiveram efectivamente garantias de QoS.

4.1.2 Ilha do INESC

Pela sua localização geográfica (sediada em Lisboa), a ilha do INESC está localizada num extremo do demonstrador internacional, estando ligada a este por via de uma ligação internacional para a ilha CPR (Pisa), com uma capacidade garantida de 1.5 Mbit/s (bidireccionais), e é disponibilizada pelas redes RCCN, GEANT, e GARR usando um túnel "IP dentro de IP" que encapsula os pacotes de dados que passam entre os dois extremos do túnel[48].

A ilha do INESC está resumida na Figura 50, e em grande detalhe no Anexo 10. Esta ilha, de igual forma das dos restantes parceiros, é dividida em duas componentes: várias redes de acesso, referentes às diversas tecnologias a demonstrar, e uma rede de *core* que as interliga, contendo o acesso internacional já referido.

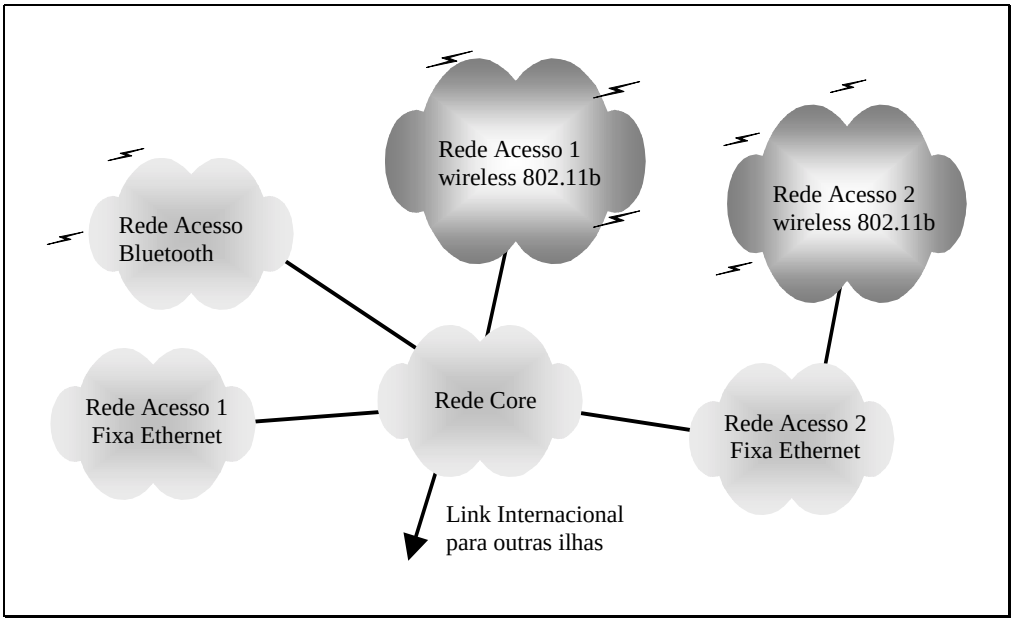


Figura 50: Arquitectura da ilha do INESC

Relativamente às primeiras, as redes de acesso são baseadas nas tecnologias *wireless* 802.11, *wireless* bluetooth e *wired* em ethernet simples, de tal forma a que cada rede é especializada nos diferentes problemas e soluções de cada tecnologia diferente, nomeadamente nas diferenças de suporte de QoS e na mobilidade (este último só no caso das redes 802.11). A

[48] Este modelo vai ser o mais simples para os provedores dos serviços, por simplificar o encaminhamento nas suas redes de core por apenas terem que ligar entre si pontos específicos das suas redes, e possibilita a máxima flexibilidade às ilhas, que podem acordar entre si livremente as redes IP a usar no demonstrador.

rede de core é baseada em tecnologia Ethernet com ligações de 10 Mbits entre os encaminhadores de core; este débito é suficientemente alto para suportar as aplicações de teste da rede, mas ainda é suficientemente baixo para ser possível saturar com tráfego, forçando a ocorrência da congestão necessária para o teste dos mecanismos de QoS.

Tem-se ainda que cada rede de acesso das presentes na ilha corresponde a uma subrede IP integrada na rede IP da ilha do INESC, utilizando o mecanismo CIDR[49], adequado para criar pequenas redes que comunicam entre si usando encaminhamento *estático*. Em particular, as redes de acesso *wireless* 802.11 são vistas do exterior como subredes IP, com um único router de acesso à sua rede de adjacente.

4.1.3 Rede de acesso wireless 802.11

Relativamente ao acesso *wireless* 802.11, existem duas redes de acesso independentes para demonstração dos mecanismos de micro-mobilidade, macro-mobilidade e QoS na tecnologia *wireless*. A primeira rede de acesso é a principal, onde serão efectuadas a maioria das experiências; a segunda é apenas uma cópia da anterior, para ser utilizada apenas nas experiências de macro-mobilidade, possibilitado por as duas redes corresponderem a dois domínios TIMIP distintos separados por várias redes IP.

Assim, a rede *wireless* 802.11 principal é a rede de acesso mais complexa da ilha INESC, tendo um nível de complexidade comparável à rede de core, e distinguindo-se de todas as outras no projecto MOICANE por apresentar um ambiente móvel sem fios, onde os terminais se podem mover livremente no interior da rede.

A rede está dividida em duas componentes distintas (ver Figura 51): uma *wireless* móvel que contém os terminais móveis, e uma componente fixa *wired* constituída por encaminhadores (fixos) que formam o *backbone* da rede. Nesta rede de suporte, alguns encaminhadores têm interfaces *wireless* 802.11 para os terminais se ligarem à rede durante o seu movimento, servindo assim de concentradores sem fios, e um destes detém a ligação à rede de core.

Internamente, os encaminhadores fixos estão ligados entre si por ligações dedicadas baseadas em ethernet, de forma que esta rede de suporte só é utilizada para encaminhar pacotes de/para

[49] Classless Inter Domain Routing, um mecanismo que permite dividir redes IP em subredes de várias dimensões.

os terminais móveis, restringidos ao interior da rede *wireless* para as comunicações locais entre terminais, e passando pela rede de core INESC no caso contrário.

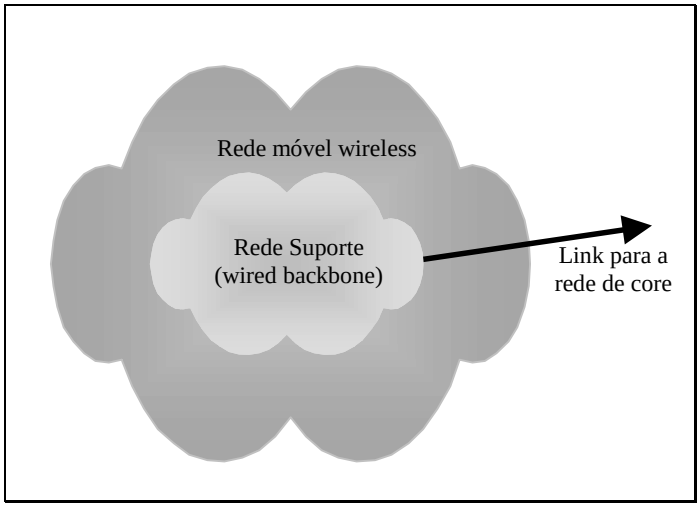


Figura 51: Componentes da rede de acesso *wireless* 802.1

Foi sobre esta rede de suporte que se centrou o trabalho desenvolvido, tendo sido as novas tecnologias IP de QoS e Mobilidade implementadas em exclusivo neste troço da rede, de forma transparente e de modo a que os terminais não participem nestes processos. Para tal, considerou-se que os terminais seriam legados, sem extensões ou alterações no seu *stack* IP, por forma a garantir a compatibilidade com o maior número possível de terminais.

Concretamente, a rede de demonstração está ilustrada na Figura 52, sendo constituída por 3 terminais móveis (C1, C2 e C3) e 3 encaminhadores fixos, dos quais 2 são pontos de acesso 802.11 (AP1 e AP2) e o restante é a GW desta rede.

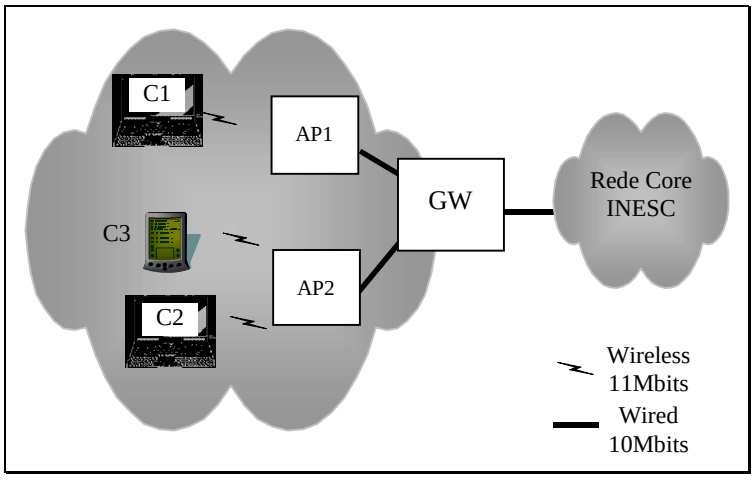


Figura 52: Rede *wireless* 802.11 de demonstração do inesc

Clientes da rede

Relativamente aos clientes da rede, procurou-se ter a maior variedade possível de terminais IP com interface 802.11 existentes, com diferentes opções de hardware e software, de forma a demonstrar o suporte de terminais legados da rede.

Desta forma, a rede conta com 2 PCs portáteis Toshiba com ambos os sistemas operativos Windows 2000 e Linux, e com interfaces PCMCIA 802.11 Lucent[50]; o terceiro cliente da rede é um PDA Siemens com Windows CE e interface 802.11 Linksys.

Estes clientes vão ser utilizados para testar a rede, o que permite verificar o suporte do QoS e da mobilidade que a rede oferece, sendo estas componentes testadas nos níveis *Funcional* e de *Desempenho*, pelo que os clientes vão usar aplicações com requisitos de QoS, como aplicações de "e-learning" e Laboratório Virtual, além de aplicações multimédia remotas, como Voz sobre IP (VoIP), ou "video a pedido" (Vídeo on demand - VoD).

Usando estas aplicações, os clientes podem estabelecer comunicações entre si, ou para o exterior da rede de acesso, onde se localizam os servidores e outros clientes fixos.

Além destas aplicações destinadas aos utilizadores finais, também são utilizadas aplicações avançadas de teste administrativo da rede, de forma a efectuar medições rigorosas da rede.

Rede de Suporte

Em relação aos encaminhadores que constituem a rede de suporte, estes já não têm a mesma variedade que caracteriza os clientes, sendo todos PCs Desktops fixos com o Sistema Operativo Linux, com extensões apropriadas para os requisitos concretos da rede.

Os encaminhadores estão dispostos numa árvore lógica em que a GW está localizada na raiz da árvore e os dois APs nas folhas, sendo todos ligados entre si por ligações Ethernet de 10 Mbit/s dedicadas.

Os dois APs têm interfaces *wireless* 802.11, as quais estão a operar no modo estruturado como Pontos de Acesso 802.11, de forma a que os terminais se possam associar explicitamente a estes. Para esta rede *wireless* é definido um *nome*[51] da rede, que a identifica e

[50] No entanto, para teste de compatibilidade, a rede também foi testada com outros sistemas operativos, e outras interfaces *wireless* de outros fabricantes.

[51] parâmetro ESSID do 802.11

separa de outras redes 802.11 que possam existir, sendo assim comum aos APs e aos clientes desta rede.

Note-se que esta pequena estrutura é suficiente para testar as funcionalidades da rede e das aplicações, mas poderá crescer a qualquer altura, acrescentando mais APs ou nós na árvore lógica existente. Os dois APs estão separados geograficamente o suficiente, para tornar possível a transição controlada dos terminais móveis entre os Pontos de Acesso, e, com vista a maximizar o débito e evitar as interferências, cada AP vai estar separado nas frequências, ocupando assim uma célula inteira, com um débito máximo de 11Mbit/s.

Ao contrário dos outros encaminhadores existentes na ilha do INESC com encaminhamento estático, nestes o encaminhamento é efectuado de uma forma totalmente automática pelo mecanismo TIMIP de suporte de mobilidade dos terminais móveis da rede, o qual apenas necessita saber a posição do encaminhador na árvore lógica da rede, de forma a automaticamente criar, manter e reconfigurar todo o encaminhamento necessário para suportar os terminais móveis no interior da rede durante os seus movimentos.

Por se usar um mecanismo de mobilidade ao nível IP, então a mudança dos terminais entre os APs incorre, além da latência inerente do 802.11, numa latência adicional necessária para a execução completa das alterações de encaminhamento para cada terminal particular; mas no entanto, este mecanismo foi desenhado explicitamente para assegurar transições de nível 3 muito rápidas, o que torna este peso adicional completamente despercebido, especialmente quando comparado com a latência inerente do nível 2.

Note-se que este encaminhamento de suporte de mobilidade só está presente no interior da rede, sendo transparente para fora desta, o que significa que a rede do exterior é apenas uma subrede IP, acessível pela sua GW, e lhe permite ser integrada no encaminhamento estático CIDR da rede de core da ilha do INESC sem qualquer dificuldade.

Por fim, a GW desta rede de acesso também inclui o suporte dos protocolos sMIP e MIP, que são utilizados para garantir o suporte de macro-mobilidade dos clientes da rede, de tal forma que estes podem transitar para outras redes com suporte MIP, como a segunda rede de acesso *wireless* da ilha do INESC.

Suporte de QoS

Por fim, para o suporte de QoS, a rede de suporte vai constituir um domínio Diffserv limitado, independente das outras redes da ilha do INESC. Cada encaminhador tem os mecanismos de

suporte de QoS presentes em todas as interfaces de rede, sendo estas classificadas em interfaces *edge* (Fronteira) ou *core* (Núcleo).

As primeiras (edge) são aquelas por onde os pacotes de dados entram na rede de suporte, sendo aí classificados pela primeira e única vez neste domínio DiffServ; as segundas (core) são as interfaces que trocam entre si pacotes de dados já marcados na classe agregada correcta, evitando a repetição da classificação já efectuada na interface *edge*.

Devido à topologia da rede em árvore, isto significa que são do tipo *edge* as interfaces *wireless* 802.11 dos APs, por estarem em contacto com os terminais móveis, e a interface Ethernet de ligação à rede de core, e todas as restantes interfaces que fazem as ligações dedicadas entre os encaminhadores são do tipo core (ver Figura 53).

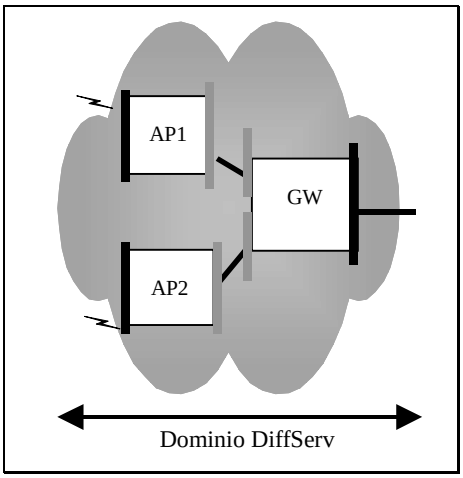


Figura 53: Rede de suporte wired como um domínio DiffServ

Assim, quando um pacote entra na rede de suporte, este é inicialmente classificado e policiado no primeiro encaminhador, sendo-lhe atribuída uma classe de serviço agregada, que é marcada no próprio pacote para futura referência[52]. Se o pacote for aceite pela decisão de policiamento, então vai ser colocado na interface de saída do encaminhador que o encaminhamento TIMIP indicar, para sofrer um tratamento de saída que depende da sua classe de serviço, e das condições actuais desta e das outras classes existentes (por exemplo, se o pacote pertencer a uma classe que excedeu o seu ritmo de saída, então o pacote será atrasado propositadamente até poder ser enviado). Estas operações de saída vão-se repetir ao longo dos encaminhadores seguintes, até que o pacote saia da rede de suporte.

No entanto, note-se que este mecanismo de QoS não garante o pretendido suporte de QoS extremo-a-extremo (embora esteja próximo); Concretamente, quando os pacotes chegam vindos da rede de core no sentido do *wireless* (*Downlink*), então vai existir QoS ao longo de toda a rede, porque o pacote é sempre emitido por interfaces pertencentes aos encaminhadores da rede, até que chegam à interface *wireless* e são processados com QoS.

[52] concretamente no campo DSCP do cabeçalho IP

Por outro lado, no sentido oposto (*UpLink*), só vai existir QoS *desde* o primeiro encaminhador do caminho - o AP, devendo-se isto, porque na emissão do pacote, o terminal vai usar o mecanismo distribuído DCF de acesso ao meio, que dá a todas as estações uma igual oportunidade de transmissão, não distinguindo assim as prioridades relativas dos vários pacotes dos terminais entre si, significando isto que os pacotes prioritários *uplink* podem ser perdidos no *wireless*, por concorrerem em igualdade de circunstâncias com os pacotes não prioritários. No entanto, assim que o pacote chega ao AP, então passa automaticamente a ter QoS, qualquer que seja o seu destino[53].

Para resolver completamente este problema, seria necessária a utilização de um mecanismo de suporte de QoS de nível 2 específico do 802.11, comum a todas as estações e APs desta rede, que controlasse o acesso ao nível físico pelas estações. Um exemplo de um mecanismo com estas características seria o modo PCF do 802.11, embora sem suporte no hardware utilizado.

4.1.4 Rede secundária de acesso wireless 802.11

Além da rede de acesso *wireless* principal, a ilha do MOICANE conta com uma segunda rede *wireless* 802.11 de apoio, que com conjunção com a rede anterior, será utilizada para demonstrar a tecnologia desenvolvida de macro-mobilidade. Para tal, a segunda rede, representada na Figura 54, é constituída por um único AP, que acumula as funções de GW, AP, e Agente sMIP/MIP, sendo este o caso mínimo de um domínio TIMIP.

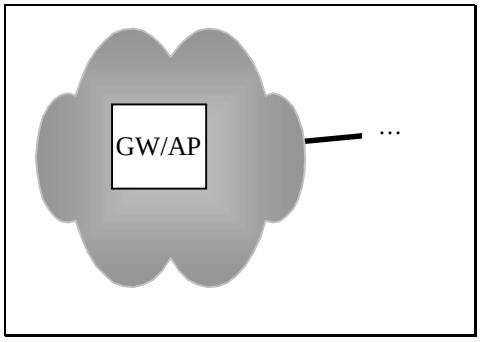


Figura 54: 2ª Rede wireless de demonstração do inesc

Relativamente ao AP da rede, a sua interface *wireless* está configurada de forma a que os terminais legados possam transitar com facilidade entre os dois domínios. Para isto, o AP vai estar configurado no modo estruturado do 802.11, e com um endereço de rede e frequência distintas da rede principal, o que separa totalmente as duas redes.

Esta configuração simples permite que os terminais transitem *controladamente* entre os dois domínios de uma forma simples, apenas escolhendo a rede de nível 2 a que se vão associar,

[53] Esta característica aplica-se mesmo às comunicações entre estações associadas ao mesmo AP, dado que o TIMIP obriga a que todo o tráfego passe pelo AP dos terminais.

que os protocolos de micro e macro mobilidade vão agir de forma automática para criar a mobilidade necessária para suportar os terminais.

4.2 Tecnologias utilizadas

Esta secção vai resumir os aspectos mais importantes das tecnologias utilizadas na rede de acesso, recentemente normalizadas pelos organismos competentes.

Esta descrição é necessariamente sumária, dando-se unicamente uma visão genérica das mesmas, mas focando os aspectos chave das tecnologias que são mais relevantes para esta rede de acesso. Descrições mais detalhadas podem ser encontradas nos documentos originais, referidos em referências bibliográficas.

4.2.1 Tecnologia de Rede 802.11

O 802.11, também denominado de *wireless* LAN, é uma tecnologia de rede sem fios normalizada pelo IEEE [2] para concretizar redes locais (LANs) de terminais móveis sem fios, com débitos elevados. Usando o standard 802.11 [4] [41], diferentes implementações da tecnologia de diferentes fabricantes têm condições para serem compatíveis entre si, de forma a operarem sem limitações.

Os terminais têm uma ligação à rede por tecnologias de alto débito sem fios, utilizando ondas de rádio-frequência para comunicar. A comunicação é tipicamente de alta velocidade quando existem condições favoráveis à transmissão, com adaptação dinamicamente a velocidades mais moderadas quando os terminais se afastarem entre si, ou por outras condições como interferência, desvanecimento, redução da potência do sinal, etc.

Esta funcionalidade vai permitir ao 802.11 melhorar a qualidade global da transmissão nestas condições adversas, uma vez que as transmissões em velocidades mais baixas são mais resistentes aos erros, e sendo assim transmitida mais informação útil do que se estes mecanismos não existissem.

Esta tecnologia pertence à mesma família 802 de outras tecnologias de rede utilizadas para concretizar LANs, como as tecnologias *wired* ethernet 802.3, token ring 802.5, etc., e também *wireless* como o 802.15 (bluetooth). Em comparação, o 802.11 é relativamente parecido com a tecnologia 802.3, dado que ambas as tecnologias têm o mesmo âmbito (redes locais), e características semelhantes, nomeadamente as suas operações internas, formatos dos pacotes, controlo de acesso ao meio, etc. Por estas razões, o 802.11 é muitas vezes denominado

(comercialmente) como a "wireless ethernet", aproveitando o nome bem sucedido da tecnologia mais comum para as LANs *wired*.

Internamente, a norma 802.11 está dividida em 2 níveis distintos: o nível físico e o nível MAC, correspondendo aos níveis 1 e 2 da pilha OSI.

4.2.1.1 Nível físico 802.11

O nível físico vai considerar os aspectos de baixo nível relativas às possíveis formas de comunicação sem fios. Neste sentido, o 802.11 prevê diversas tecnologias diferentes de comunicação, variando nestas a forma da codificação da informação, o débito binário, a robustez do sinal estabelecido, e a distância/qualidade do sinal. Para isto, existem várias alternativas de transmissão do sinal como o *infrared*, *direct sequence spread spectrum*, *frequency hopping spread spectrum*, e as mais recente *orthogonal frequency division multiplexing* (OFDM).

Para suportar as várias velocidades de transmissão, e para as outras estações saberem qual o tempo que este pacote vai demorar a ser transmitido, abstendo-se entretanto de transmitir outros pacotes para evitar colisões, o nível físico vai sempre adicionar um cabeçalho seu o qual indica a velocidade de transmissão do *payload*, e o seu comprimento, o que permite a que todas as estações presentes na frequência de verificarem com exactidão o tempo futuro em que este pacote termina a sua transmissão, acedendo ao meio apenas após esse instante.

No entanto, esta capacidade de utilização a várias velocidades significa que este cabeçalho de nível 1 tem *sempre* que ser transmitido na velocidade mínima possível[54], por forma a dar a oportunidade a todas as possíveis estações saberem que o meio está ocupado, e durante quanto tempo. Isto significa que o *overhead* do nível 1 por pacote do 802.11 vai ser substancial, porque este vai ter uma duração de transmissão mínima constante por cada pacote, sendo esta independente da velocidade actual de transmissão dos dados[55].

Esta característica do nível 1 do 802.11 vai significar que os débitos elevados só são bem aproveitados quando se transfere uma quantidade elevada de informação por cada pacote, o

[54] Que em 802.11b será de 1Mbit/s

[55] Concretamente (por pacote), o tempo de transmitir os 24 bytes do cabeçalho de nível 1 a 1 Mbits (0,192 ms) (em 802.11b)

que equivale a considerar um MTU elevado, que em 802.11 corresponde a um máximo de 2342 bytes.

No entanto, existem aplicações que, pela sua natureza, têm pouca informação para transmitir de cada vez, como o transporte de voz, e têm requisitos de tempo real que as impedem de acumularem dados para transmissão. Se o 802.11 for utilizado maioritariamente para este tipo de aplicações, então o débito líquido que efectivamente se atinge ao nível 3 é substancialmente mais baixo que o débito físico da tecnologia, porque uma parte considerável do débito é perdido nos *overheads* do 802.11. Esta ineficiência do 802.11b está estudada teoricamente na referência [44], e comparada com um estudo prático do mesmo assunto (ver Anexo 20) .

Das várias propostas normalizadas pelo IEEE, a mais difundida actualmente é o 802.11b [42] que utiliza o mecanismo DSSS (*Direct Sequence Spread Spectrum*) num conjunto de frequências de livre utilização na banda dos 2.4 GHz[56], oferece um débito binário de transferência de informação máximo de 11 Mbits por segundo para distâncias curtas, baixando progressivamente à medida que a distância aumenta. Este débito elevado associado a um baixo custo dos equipamentos significa que o 802.11b é uma solução bastante interessante para o acesso *wireless* para os ambientes empresarial como residencial.

4.2.1.2 Nível MAC 802.11

Ao contrário do nível físico, o 802.11 define um único nível de ligação MAC comum para os vários níveis físicos do 802.11, agrupando as funções de acesso ao meio, o endereçamento de estações e redes, o controlo de erros associado à velocidade de transmissão *vs* distância entre as estações, entre outras. Desta forma, é o nível MAC que vai ter os mecanismos que permitem que as estações possam comunicar entre si, de uma forma ordenada e possível, procurando utilizar eficientemente a capacidade limitada de largura de banda do *wireless*.

Por outro lado, o nível MAC também inclui outras características especiais pouco comuns nas outras tecnologias *wired*, mas que são necessárias devido à natureza aberta do acesso sem fios que não liga as estações com uma ligação física "palpável". Entre estas encontram-se um mecanismo de agrupamento das estações entre si, necessário para dividir as diferentes redes

[56] Na maioria dos países, em particular Portugal. No entanto, existem excepções como em França e Espanha, dado que algumas das frequências desta banda já estão reservadas para outras aplicações.

de estações que estejam em contacto umas com as outras, e um mecanismo de segurança (WEP) que com os serviços de autenticação e cifra, vai controlar o acesso e as comunicações dos terminais entre si, de forma a evitar ataques passivos e activos à rede que ameaçariam a sua integridade e a confidencialidade das comunicações.

Assim, o 802.11 organiza as entidades que participam na rede *wireless* em **estações**, e agrupa as estações em redes de dados. Cada estação vai ter um endereço único[57] e comunicam entre si usando pacotes de dados com um formato pré-especificado.

As redes são criadas e separadas entre si por deterem um identificador único por rede, o ESSID, que é uma cadeia de caracteres com qualquer valor, que será o nome da rede. Esta separação é feita de forma a que os terminais só recebam e enviem pacotes da sua rede actual, o que as permite separar quando estiverem no alcance umas das outras.

Quando uma estação pretender transmitir um pacote para qualquer outra, então o nível MAC vai criar um pacote de dados com os endereços de origem e destino desejados. O pacote também pode ser enviado de forma a ser recebido por múltiplas estações, nomeadamente em difusão para ser recebido por todas as estações pertencentes a esta rede 802.11, ou em *multicast* para apenas algumas destas.

Em ambos os casos, o pacote é entregue ao nível físico para transmissão na velocidade actual do nível físico, e dado que o meio sem fios é altamente propício à ocorrência de erros de transmissão, em especial nos débitos mais elevados, o 802.11 define que todos os envios de pacotes *unicast* são individualmente confirmados pelo receptor, por via de um pacote MAC de *acknowledge*[58].

Nesta conformidade, se o emissor do pacote não receber de imediato o correspondente pacote de confirmação do receptor, então este considera que o pacote original foi perdido, procedendo à sua retransmissão, operação esta automática, e repetida até um número máximo de vezes (configurável em MIB). Desta forma, o MAC do 802.11 vai apresentar ao nível 3 um meio físico mais fiável que o existente.

[57] composto por 6 bytes, tal como os endereços do 802.3

[58] Este comportamento do MAC 802.11 corresponde à utilização de uma janela de emissão de tamanho 1

4.2.1.3 Organização das redes 802.11

O 802.11 define dois métodos alternativos do modo como as estações se organizam entre si para criarem redes sem fios.

4.2.1.3.1 Modo Ad-Hoc

O modo mais simples consiste no modo **ad-hoc**, e é apenas adequado a redes muito rudimentares, constituídas por poucas estações, uma vez que terão que estar todas ao alcance umas das outras para comunicarem na mesma frequência. Isto significa que este modo só é utilizável em redes muito limitadas geograficamente e sem requisitos elevados de largura de banda, mas no entanto, com a vantagem de todas as estações serem iguais, não necessitando de mecanismos adicionais para estabelecerem uma comunicação *wireless* básica.

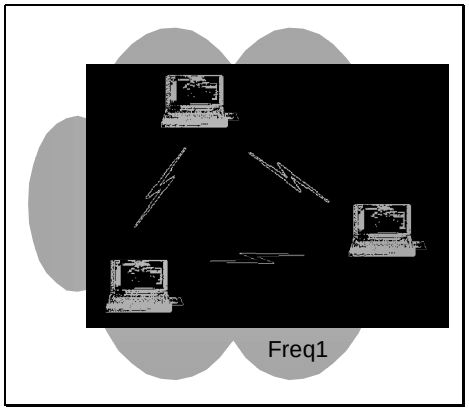


Figura 55: Modo *ad-hoc* do 802.11

Por estas razões, este modo é principalmente utilizado em redes simples e de curta duração.

4.2.1.3.2 Modo Estruturado

O segundo modo de utilização das redes *wireless* é mais complexo que o anterior, mas bastante mais flexível e escalável. Este modo, denominado de **estruturado**, é caracterizado por definir que certos elementos da rede são estações com funções adicionais relativas à gestão da rede (ver Figura 56).

Estes pontos da rede são denominados de pontos de acesso (APs), e a sua principal função é a de constituir pontos centralizadores da rede sem fios, estando as estações normais associadas a um único AP. Além desta funcionalidade, os APs também se ocupam de outras funcionalidades típicas de gestão, como as funções de poupança de energia, autenticação e ligação ao exterior da rede.

Desta forma, a rede é dividida internamente nos APs existentes, que podem operar em frequências diferentes de forma a aumentar a capacidade total de largura de banda da rede disponível para as estações.

No interior da rede, as estações móveis vão-se associar explicitamente a um único AP de cada vez, trocando mensagens especiais de gestão para concretizar a operação de associação. Sempre que tenham pacotes de informação para transmitirem, as estações podem comunicar

directamente entre si, se estiverem localizadas no mesmo AP, mas também por via do AP (podendo duplicar a distância máxima de uma célula 802.11, centrada no AP).

No entanto, a principal diferença é que os APs vão poder executar as funções de *bridges*, possibilitando a comunicação de estações localizadas em APs diferentes, ou seja, quando um AP receber um pacote de dados destinado a uma estação localizado noutro AP, então o AP recebe-a e encaminha o pacote pelas suas ligações, de forma a este chegar ao seu destino. Estas ligações dos APs entre si são normalmente dedicadas e *wired*, o que assegura um bom desempenho, mas também podem ser *wireless* e partilhadas com as estações normais.

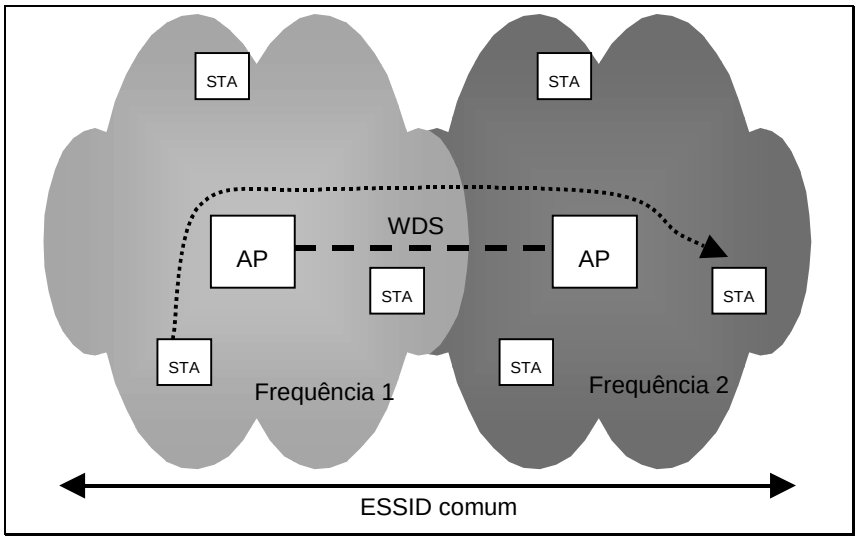


Figura 56: Modo estruturado do 802.11, incluindo transmissão de dados

Embora os terminais tenham que estar em cada momento associados a um único AP, estes têm a liberdade de transitarem de AP quando pretenderem, e para tal, o terminal vai a cada momento verificar qual a sua localização física, e quais os APs perto de si para o terminal transitar.

Nestas circunstâncias, os APs emitem periodicamente em difusão pacotes de gestão especiais denominados de *beacons*, que servem para anunciar a sua presença no interior da rede, e que os terminais recebem e usam para decidir transitar.

No entanto, o 802.11 não define propositadamente o algoritmo que cada terminal pode seguir para escolher a sua ligação à rede, optando normalmente os terminais por medir a potência do sinal dos *beacons* recebidos, e escolhendo transitar para um novo AP quando a qualidade do sinal actual baixar depois de um certo nível. Como exemplo, um algoritmo de transição das estações entre os APs é detalhado na referência [85].

Este processo de procura de novos APs não é feito de uma só vez, pois numa primeira fase o terminal vai apenas procurar os *beacons* de outros APs na sua própria frequência, o que lhe permite manter a sua conectividade, continuando a receber e enviar os seus pacotes de dados; só quando a qualidade do sinal do AP actual baixar significativamente é que começa a procurar nas outras frequências, iniciando varrimentos (*sweeps*) até encontrar um AP que esteja mais próximo que o actual.

No entanto, quando o terminal começa este processo vai perder momentaneamente a sua conectividade por ter saído da frequência do seu AP actual. Esta perda de conectividade só termina quando o terminal encontrar um novo AP, associando-se a este, provocando a alteração das tabelas de localização (*bridging tables*) dos APs e outros elementos de nível 2 envolvidos na transição do terminal.

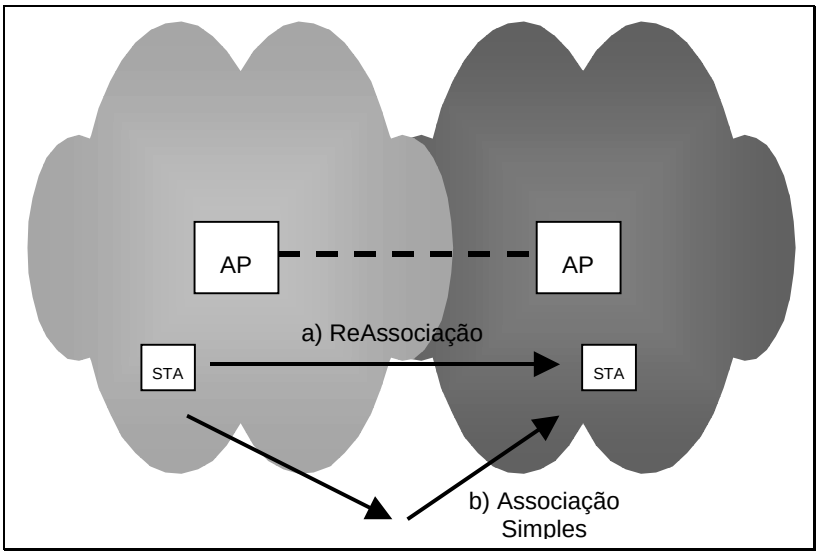


Figura 57: Movimentos dos terminais no interior da rede 802.11

Nestas condições, quando um terminal transitar directamente entre dois APs (situação A da Figura 57), apenas envia um pacote de reassociação para o seu novo AP, no qual lhe indica a sua identidade, e o endereço do seu AP anterior. Usando estes dados, existe um mecanismo adicional que se executa entre os APs envolvidos, denominado de IAPP (Inter Access Point Protocol), que vai tomar as acções necessárias para que o terminal passe a estar acessível pelo seu novo AP, efectuando um *handover* do AP anterior para o novo.

Actualmente, este protocolo ainda não está normalizado pelo IEEE, estando ainda em estudo pelo sub-grupo 802.11f, o que significa que os fabricantes não têm um mecanismo standard para suportar as movimentações dos terminais móveis em redes 802.11 heterogéneas de vários fabricantes.

Nestas circunstâncias, o *handover* dos terminais em 802.11 é efectuado actualmente da mesma forma que as movimentações dos terminais nas outras tecnologias de rede, baseando-se na capacidade de aprendizagem das *bridges* de nível 2 das localizações dos terminais. Neste mecanismo, depois de o terminal se associar ao seu novo AP, vai ser o primeiro pacote de dados emitido pelo terminal que chegue ao backbone da rede[59], que vai servir para os APs e as outras *bridges* aí existentes notarem que o terminal já não está acessível pela mesma localização, aprendendo assim a nova localização do terminal.

No caso do terminal não transmitir nenhum pacote de dados, então as entradas de localização relativas a ele são removidas ao fim de um dado *timeout*, o que força os pacotes de dados destinados ao terminal a serem difundidos por toda a rede, até que o terminal responda a um destes pacotes de dados, o que revela a sua localização actual.

4.2.1.4 Acesso ao Meio

O 802.11 define dois mecanismos alternativos para o controlo do acesso ao meio partilhado *wireless* pelas estações. Estes mecanismos são essenciais ao bom funcionamento da rede como um todo, serializando de uma forma equilibrada os acessos ao meio. Quando isto acontece, então só uma única estação de cada vez é que vai transmitir pacotes, evitando-se assim colisões que acontecem quando multiplas estação tentam aceder ao meio em simultâneo, e que resulta na perda dos pacotes.

Por outro lado, o mecanismo de acesso ao meio também é suposto dar igual oportunidade a todas as estações para transmitirem, de forma a não criar situações de "starvation" das estações entre si.

4.2.1.4.1 Modo DCF

O mecanismo base do 802.11 para controlar o acesso ao meio do 802.11 é o DCF (Distributed Coordination Function), um mecanismo distribuído semelhante ao CSMA/CD do 802.3, podendo ser utilizado nos dois modos de estrutura da rede.

Neste mecanismo, as estações que pretendem transmitir estão permanentemente à escuta no meio, para verificarem o momento é que este passa a estar livre. Quando este acontecer, a

[59] Denominado em 802.11 por WDS (Wireless Distribution System), que consiste nas ligações internas dos APs entre si, e que são utilizadas para passar pacotes de dados entre diferentes partes da rede, ou para o exterior da mesma.

estação vai esperar um pequeno tempo adicional que varia com a importância do seu próximo pacote de dados, esperando intervalos ordenados por ordem crescente, denominados de SIFS, PIFS, DIFS consoante a estação queira transmitir um fragmento do pacote actual, um pacote de gestão ou um novo pacote de dados.

Se esta estação foi a última a transmitir, e se o próximo pacote for prioritário, então começa de imediato a sua transmissão; no caso normal, então a estação vai ainda esperar um tempo adicional aleatório entre 0 até ao valor máximo da sua janela de *backoff*.

Se durante todo este período de espera o meio se manteve livre, então significa que as outras estações escolheram tempos aleatórios de espera superiores (ou iguais), pelo que a estação começa a transmissão do seu pacote. Se durante este período outra estação tiver começado a transmitir o seu pacote, então a próxima espera vai continuar no fim desta transmissão.

Nesta situação, só podem acontecer colisões quando outra estação tenha escolhido exactamente o mesmo tempo de espera, o que resulta na perda de ambos os pacotes. Nesta situação, ambas as estações podem verificar que a transmissão resultou em colisão, recomeçando o processo duplicando o tempo máximo de espera (a janela de *backoff*) e escolhendo um novo valor de espera.

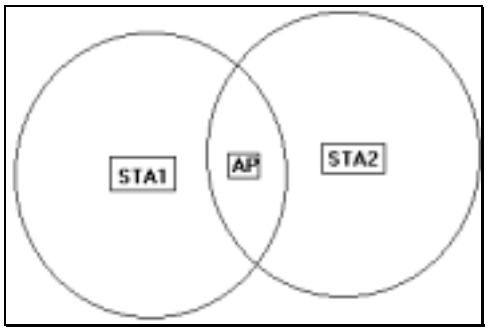


Figura 58: Problema da estação escondida

No entanto, mesmo com este mecanismo, podem acontecer colisões para além das descritas, sendo este o problema denominado da "estação escondida", sendo este solucionado pelo DCF por um mecanismo adicional de RTS/CTS (Request to Send/Clear to Send), que consiste num *handshake* inicial antes de se transmitir o pacote que se pretende, e que avisa todas as estações no alcance do emissor e do receptor para não acederem ao meio.

Nesta situação, se uma estação escondida forçar uma colisão, então esta vai acontecer no RTS ou no CTS, e não no pacote de dado. Contudo, o peso adicional de dois pacotes por mensagem pode ser significativo, pelo que este mecanismo só é normalmente utilizando quando a rede tem um grande número de estações e apenas para a transmissão dos pacotes grandes.[60]

[60] Tipicamente, apenas para os pacotes com um comprimento acima dos 1000 bytes

4.2.1.4.2 Modo PCF

O 802.11 define ainda um mecanismo alternativo de acesso ao meio, utilizado principalmente para a eliminação das colisões do mecanismo distribuído. Neste modelo, a decisão do acesso ao meio passa a ser centralizado no Access Point, que vai decidir explicitamente as estações que vão transmitir, e por que ordem.

Para isto, as estações só vão transmitir quando o AP as autorizar, pois este envia-lhes um pacote especial de controlo, *Poll*, o que elimina as colisões no acesso ao meio. No entanto, por usar esta centralização dos acessos, este modo de acesso só poderá ser utilizado no modo estruturado, onde existe a entidade AP.

Desta forma, existem dois períodos de transmissão periódicos regulados pelo AP: "com contenção" e "sem contenção". No primeiro período, de dimensão reduzida, é utilizado o DCF para as estações notificarem o AP que pretendem transmitir dados, e para outras funções de gestão como as associações, e no segundo período (normalmente maior que o anterior), as estações vão aceder ao meio da forma descrita acima, o que evita as colisões[61].

O modo PCF também tem interesse além da mera eliminação das colisões, porque possibilita a introdução de um suporte de prioridades no acesso ao meio, o que pode ser utilizado para suportar QoS de nível 2 no acesso ao *wireless* (relativamente ao controle de atrasos e débitos garantidos).

Para isso, um algoritmo de escalonamento presente no AP pode ser usado para dar preferência às estações que tenham dados prioritários a transmitir, enviando-lhes mais *polls*. Note-se que no entanto, outras funções avançadas direccionadas para o suporte de QoS ainda estão em estudo pelo subgrupo "E" do 802.11, não tendo ainda sido normalizadas, como a introdução de um suporte de prioridades no modo DCF.

Por outro lado, este modo de acesso ao meio não está a ter actualmente uma aceitação generalizada dos fabricantes, uma vez que o mecanismo de *polls* explícitos incorre num *overhead* muito elevado, que reduz ainda mais a capacidade efectiva de largura disponível para o nível 3.

[61] No entanto, note-se que isto só é possível se não houverem mais APs na mesma frequência no alcance da célula 802.11, porque nesse caso só se removem completamente as colisões se os APs estiverem sincronizados entre si, o que pode invalidar as garantias e vantagens do PCF.

4.2.2 Tecnologias de Suporte de Qualidade de Serviço

4.2.2.1 O que é o suporte de QoS

Designa-se suporte de Qualidade de Serviço (QoS) ao conjunto dos mecanismos integrados que terão que estar presentes nas redes de dados para garantirem que as características específicas dos fluxos que transportam são cumpridos, nomeadamente em relação a valores médios, mínimos e máximos de atrasos máximos, perdas e débitos médios, entre outras.

Sem este suporte, a utilização da rede pode implicar que estas características do tráfego não sejam cumpridas, dado que os recursos existentes são limitados e partilhados por todos os fluxos sem distinção. Nestas condições, as aplicações com requisitos apertados do tipo interactivas/tempo-real podem deixar de ser utilizáveis, por não receberem os fluxos de dados nas condições necessárias.

De notar que o suporte de qualidade de serviço está inerente nas redes clássicas de comutação de circuitos, porque para cada comunicação individual é criado um caminho físico exclusivo ao longo de todo o percurso, desde o emissor até ao receptor com as características desejadas, que garante que o transporte da informação detenha sempre os recursos necessários para respeitar na perfeição as características do fluxo pré-acordadas.

No entanto, este mecanismo simples tem custos associados elevados, pois não permite que os recursos atribuídos por um fluxo sejam utilizados por outro quando não estiverem a ser utilizados. Isto leva a uma má utilização de recursos, e a uma limitação no número total de comunicações que se conseguem estabelecer.

Para resolver este problema, foram criadas as redes de comutação de pacotes, que transportam a informação em pequenos pacotes individuais, podendo seguir caminhos diferentes, e que partilham os recursos disponíveis entre si. Assim, se um dado fluxo de informação parar temporariamente de transmitir dados, os recursos que estavam a ser ocupados por este poderão ser utilizados para outros fluxos que estejam a passar nos mesmos troços de rede.

Relativamente à Internet, esta seguiu este modelo de pacotes, mas aplicando o mecanismo mais simples possível para a escolha da ordem e importância dos pacotes entre si – o modelo **Best-Effort** –, em que todos os pacotes são considerados de igual importância, e apenas são encaminhados da forma o mais rápida possível, sem ter em conta as características específicas das classes a que pertencem.

Enquanto a utilização da rede for reduzida, sem os recursos da rede serem estrangulados, o modelo BE vai dar bons resultados para todos os fluxos; contudo, quando a utilização da rede

subir, certos pontos da rede vão esgotar os seus recursos limitados, o que cria atrasos e perdas de pacotes em todos os fluxos estabelecidos, levantando os problemas já referenciados para as aplicações com características tempo-real, dado que a perda, ou a entrega tardia de pacotes, podem baixar significativamente a qualidade do serviço, até ao ponto de ficar inutilizável.

Para resolver este problema, são utilizados mecanismos que adicionam o suporte de qualidade de serviço às redes de dados, reaproveitando algumas das características das redes de comutação de circuitos, mas associadas às vantagens da flexibilidade da comutação de pacotes.

Neste cenário, o suporte de QoS vai-se concentrar na separação lógica dos fluxos entre si, podendo esta separação ser a vários níveis, desde os fluxos individuais até aos conjuntos de fluxos com características semelhantes, denominados de *agregados*.

Por via desta separação, os pacotes vão passar a sofrer tratamentos distintos nos encaminhadores, de acordo com as características das aplicações finais. Como exemplo, um dos tratamentos mais simples consiste na prioridade absoluta aos pacotes das classes de serviço sem tolerância a atrasos, em que, com esta medida, os fluxos de dados prioritários vão ter condições para controlar o atraso e minimizarem/eliminarem as perdas, mesmo quando a rede está utilizada com muito tráfego.

Esta melhoria do tratamento destas classes é feita à custa das outras classes menos prioritárias, dado que as primeiras podem passar à frente dos fluxos menos prioritários, que podem admitir um serviço pior, por tolerarem uma degradação do serviço, ou por terem direito a menos recursos da rede.

4.2.2.2 Evolução do suporte de QoS na Internet

O primeiro passo para o suporte de QoS na Internet, começou pela marcação dos pacotes com diferentes identificadores simples, que identificam genericamente o pacote como proveniente de tráfego interactivo, tempo-real, *bulk*, etc. Para tal, as aplicações quando emitem pacotes IP vão utilizar o campo “type-of-service” (TOS) com bits que indicavam o tipo de pacote em questão, podendo ser do tipo *low-delay*, *low-loss*, *low-jitter*.

Quando o pacote for enviado para a rede, os encaminhadores no caminho que suportarem esta extensão podem usar esta informação para conhecerem a natureza do pacote, e proporcionar-lhes um tratamento mais prioritário que o normal. No entanto, esta acção é meramente sugestiva, dado que há garantias de que os encaminhadores no caminho tenham o suporte

desta extensão, nem que estes tenham os recursos disponíveis para este tratamento especial dos pacotes prioritários.

Mais tarde, apareceram novas extensões de QoS integradas e que fornecem garantias do tratamento que os pacotes vão sofrer na sua passagem pela Internet, sendo o primeiro passo dado com o modelo de serviços integrados – **Intserv [39]** – que define 2 classes prioritárias relativamente ao tráfego não-prioritário BE.

Estas duas classes referem-se às necessidades mais típicas das aplicações tempo-real, nomeadamente para garantias de latência e *jitter* (classe Guaranteed Service), e garantia de débitos médios (classe Controlled Load). Durante o estabelecimento do fluxo de comunicação, o emissor vai explicitamente reservar recursos nos encaminhadores ao longo do caminho para o seu tráfego, ficando cada encaminhador com a informação de estado deste fluxo.

Esta reserva é realizada usando o mecanismo de sinalização RSVP, com o qual o emissor caracteriza o seu tráfego numa destas duas classes, e por parâmetros relativos ao fluxo que está a pedir, como débitos médios, máximos, *jitter* máximo, entre outros. Este processo de reserva de recursos é sujeito a um controlo prévio de admissão, no qual os encaminhadores verificam se têm recursos disponíveis para garantir o serviço.

Depois de os recursos serem reservados, então os pacotes destes fluxos reservados vão ter um tratamento especial em relação aos pacotes normais, sendo em cada nó classificados[62] e sujeitos a políticas de encaminhamento diferentes, recebendo da rede um tratamento como se tivessem para si um circuito dedicado, mas utilizando comutação de pacotes, o que só acontece porque vai existir qualidade de serviço extremo-a-extremo.

No entanto, o mecanismo Intserv ao considerar o *grão* de cada fluxo individual, obriga à criação e manutenção de estado por cada fluxo individual em todos os encaminhadores do caminho. Esta opção de desenho ainda é aceitável nos extremos da rede, onde passam relativamente poucos fluxos, mas compromete seriamente a escalabilidade do mecanismo no núcleo da rede, onde a maioria das comunicações da Internet passa.

[62] Os fluxos são identificados pelo conjunto dos endereços IP de origem e destino, bem como dos portos UDP/TCP.

4.2.2.3 Modelo Diffserv

O modelo Diffserv [34] foi desenhado para fornecer suporte de qualidade de serviço de uma forma simples e escalável, para ser passível de ser aplicada nos encaminhadores internos das redes de core.

Neste modelo, os encaminhadores não vão tratar os fluxos individuais em particular, mas sim tratar os fluxos em grupo que precisam de um tratamento semelhante na mesma classe de serviço. O resultado vai ser que estes encaminhadores vão tratar os *agregados* dos fluxos, e não os fluxos em si, o que lhes permite apenas guardar *estado* por cada classe de serviço.

Além disto, o Diffserv distingue-se do Intserv por prever um número alargado de possíveis classes de serviço, em vez das 2 únicas existentes no modelo anterior. Estas classes podem ser normalizadas pelo grupo competente, mas também experimentais, sendo privadas no interior de um domínio Diffserv.

Até ao momento já foram normalizadas duas classes de serviço, que definem diferentes características de encaminhamento (*Per Hop Behaviour* - PHBs): o Expedited Forwarding (EF), o Assured Forwarding (AF), além do base Best Effort (BE). Estas classes normalizadas têm características semelhantes às classes GS e CL existentes do IntServ.

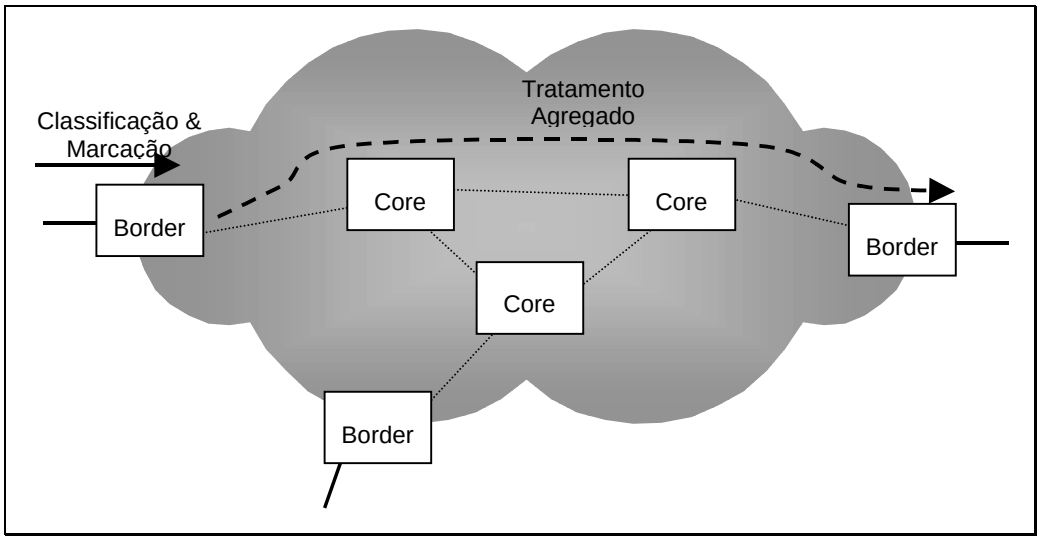


Figura 59: Arquitectura de um domínio Diffserv

A arquitectura do Diffserv está ilustrada na Figura 59, em que se observa que cada região contígua constituída exclusivamente por encaminhadores Diffserv é denominada de domínio, existindo dois tipos de encaminhadores: Borders e Core.

Os primeiros são os encaminhadores fronteira que recebem os fluxos de dados do exterior do domínio. Quando estes entram no domínio, vão ser classificados pela única vez no domínio

numa das classes de serviço existentes, de acordo com as suas características específicas, como por exemplo os valores dos campos dos cabeçalhos IP, ou por reclassificação (se o pacote tiver sido entregue por outro domínio adjacente a este).

Isto significa que depois de passarem no *border router*, do ponto de vista dos encaminhadores da rede, os pacotes vão perder a sua identidade como fluxo único, sendo agregados no tratamento da classe inteira com outros fluxos individuais que necessitam genericamente das mesmas acções de *forwarding*. Desta forma, quando os pacotes chegarem aos encaminhadores internos do núcleo do domínio Diffserv, então vão sofrer o tratamento apenas referente à sua classe de serviço, o que é essencial para a escalabilidade do mecanismo.

Esta associação dos pacotes a classes genéricas, e ao seu posterior tratamento rápido pela classe, é possível porque os pacotes são marcados no *border router* com um identificador único da sua classe, de acordo com as regras de classificação atrás descritas.

Para isto, no interior de um domínio Diffserv o campo TOS do cabeçalho IP vai ser renomeado de DSCP (Diffserv Code Point) [35], sendo utilizado para receber o identificador da classe do pacote, e dado este campo ter um comprimento de 6 bits, permite a existência de múltiplas classes de serviço possíveis.

A arquitectura DiffServ é altamente flexível, e concentra-se em colocar as funções complexas para os extremos do domínio, simplificando o interior, definindo ainda diversas componnetes base a serem utilizadas na distinção das classes de serviço, como sejam classificadores, policiadores, *meters*, *droppers*, *shapers* e *schedulers*. A cada classe agregada cabe a definição da utilização destas componentes para instanciarem as suas características particulares, como por exemplo a utilização de *policiadores* para o confirmação dos débitos médio e de pico, e a utilização de escalonadores de prioridade para respeitar os atrasos máximos permitidos pelas aplicações interactivas.

Note-se ainda, que a arquitectura Diffserv se baseia bastante nas componentes “macro” dos domínios como um todo, ao contrário do Intserv que considera os fluxos explicitamente, e que tem o controlo explícito de admissão nó-a-nó ao longo de todo o caminho usado pelos fluxos.

Desta forma, existe normalmente uma entidade central denominada de Bandwith Broker (BB) que gere os mecanismos de QoS para um domínio inteiro, instruindo dinamicamente os encaminhadores do seu domínio com configurações particulares, e recebendo e aceitando os pedidos de QoS para os agregados de fluxos (em vez dos fluxos individuais).

Para isto, o BB pode comunicar com os seus correspondentes dos outros domínios por via de protocolos que ainda estão em estudo[63], de forma a estabelecer e respeitar SLAs do seu domínio, permitindo a criação do suporte de QoS extremo-a-extremo.

4.2.2.3.1 Clase de serviço EF

A primeira classe de serviço normalizada foi a classe Expedited Forwarding [36], que teve o objectivo de criar um serviço semelhante a uma linha alugada virtual estabelecida entre os seus extremos. Neste canal privilegiado de comunicação, o EF pode garantir que as comunicações agregadas desta classe vão sofrer tanto baixas perdas, latência e *jitter*, com largura de banda garantida, tal como numa linha física real, mesmo que as outras classes pretendam ocupar recursos desmesuradamente.

Para concretizar estas características, esta classe vai ter que garantir que os fluxos agregados pertencentes a este serviço "premium" nunca encontram filas de espera, ou caso encontrem, que sejam muito pequenas em tamanho.

Isto apenas se consegue quando o ritmo de entrada do agregado EF seja inferior ao ritmo de saída pré-reservado para esta classe, tendo este último que ser independente dos outros tipos de tráfego presentes nos encaminhadores Diffserv. Por exemplo, esta premissa aceita que os recursos utilizados pelo EF possam ser utilizados pelas outras classes menos prioritárias, desde que o EF possa ocupar sem limites o outro tráfego, de modo a que sua fila não aumente.

Para garantir esta característica, esta classe é sujeita a SLAs restritivos (por exemplo, não aceitando débitos de pico elevados), impostos com rigor por mecanismos de condicionamento de tráfego presentes nos *borders routers* (shapers/droppers), que só deixam entrar no domínio diffserv valores seguros de tráfego prioritário.

4.2.2.3.2 Classe de Serviço AF

Além do EF, também foi normalizada uma segunda classe de serviço denominada de Assured Forwarding (AF) [37], que oferece um tratamento substancialmente menos rígido que o EF, mas oferecendo ainda boas garantias para a entrega dos pacotes. Relativamente ao tráfego médio pré-acordado, este será entregue com uma probabilidade de entrega muito grande.

[63] Nomeadamente o COPS

No entanto, os clientes desta classe também podem exceder este valor medio de tráfego, tendo este excedente uma probabilidade mais baixa de sucesso na sua entrega ao destino. Desta forma, por oferecer menos, mas ainda algumas garantias, o AF vai-se posicionar entre o EF e o BE.

Para tal o AF disponibiliza 4 sub-classes independentes entre si, que vão suportar diferentes tipos de agregados de fluxos, sendo distinguidas pela quantidade de recursos que estão atribuídos para cada sub-classe (como o número de *buffers* e a largura de banda). No interior de cada sub-classe AF existem 3 bandas de diferentes probabilidades de perda de pacotes, em que cada banda indica a importância relativa dos pacotes uns em relação aos outros.

Por outro lado, em caso de congestão, os pacotes não vão ser descartados da forma praticamente aleatória da classe BE, mas sim de uma forma inteligente e que favoreça o agregado como um todo, descartando primeiro os pacotes pouco importantes ou de excesso, antes de descartar pacotes conformantes, penalizando primeiro as fontes que estão a exceder o tráfego acordado.

Para que tal ocorra, a escolha do nível de perda pode ser feita de forma a indicar que tráfego é que esteve inicialmente dentro do limite pré-acordado em SLA, e qual é o excedente, no caso em que todos os pacotes são iguais entre si.

Outra utilização típica em outras aplicações mais avançadas é quando existem pacotes que são claramente mais importantes que outros, o que leva a separar as diferentes componentes do tráfego nas diferentes bandas de perda[64]. Refira-se também que o AF define explicitamente que as perdas no interior de uma sub-classe não podem levar ao reordenamento dos pacotes entre si.

[64] Um exemplo da utilização desta característica do AF será a separação das diferentes componentes de codificação de vídeo (tramas I, B e P) nas bandas de probabilidade de perda.

5. Implementação da rede de acesso wireless do MOICANE

Este Capítulo vai descrever a implementação das soluções de mobilidade que apresentadas teoricamente nos capítulos anteriores, na rede *wireless* do MOICANE. Esta implementação consistiu tanto na instanciação da tecnologia, como também no trabalho de engenharia necessário para a integração com as outras componentes da ilha do MOICANE.

Para esta rede de acesso, a sua instalação, configuração e utilização completas foram já descritas em [92]; assim, este capítulo vai detalhar apenas os pormenores que não estão presentes nesta referência, necessários para a compreensão do *software* desenvolvido, tanto para a sua avaliação e alteração/extensão.

Assim, a rede de acesso é constituída por encaminhadores IP genéricos baseados no sistema operativo LINUX, que foram customizados, alterados e configurados de acordo com as necessidades específicas da rede de acesso, sendo estes focados neste capítulo. Além dos módulos já existentes, tiveram que ser criados novos para as características novas da rede, tendo estes sido programados na linguagem C.

Este capítulo está dividido em três secções:

A primeira analisa genericamente a arquitectura dos elementos de redes, identificando os módulos existentes e as suas relações internas, e as operações efectuadas aos pacotes de dados no interior do encaminhador;

A segunda secção vai analisar os detalhes dos módulos existentes no encaminhador, com especial atenção aos que foram criados propositadamente para esta rede de acesso – tanto de mobilidade como de QoS;

Por fim, a última secção vai detalhar os testes funcionais e de desempenho efectuados na rede.

5.1 Arquitectura dos elementos de rede

Nesta secção analisa-se a arquitectura genérica dos elementos da rede de suporte, focando as características particulares que estes encaminhadores têm e que os distinguem dos encaminhadores genéricos IP, sendo descritos os módulos existentes nestes elementos, as interacções entre eles, e a vida do pacote desde a entrada até à saída do elemento de rede.

5.1.1 Módulos

Tal como já foi referido anteriormente, os elementos de rede são baseados num modelo base que detém as funções comuns a todos estes encaminhadores, e que pode ser especializado com funções e módulos adicionais para realizar as funções de APs e de GW da rede.

Para tal, a arquitectura genérica dos nós da rede está presente na próxima figura:

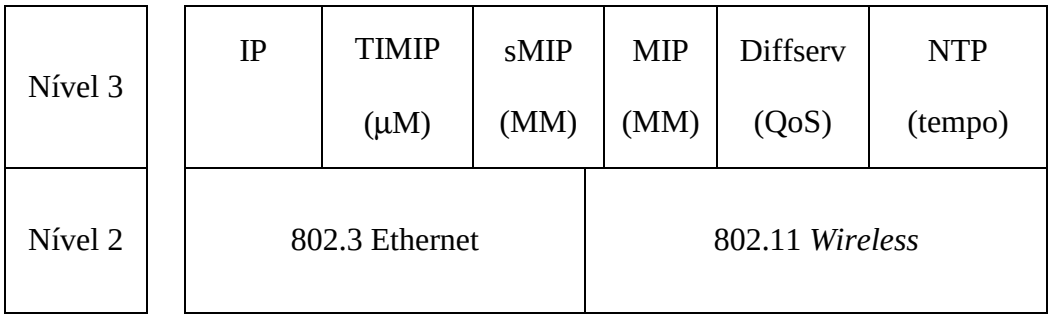


Figura 60: Arquitectura dos Elementos de rede

Os elementos de rede têm a maior parte das funcionalidades ao nível IP (nível 3), com funções que são independentes das várias tecnologias.

Neste nível, o módulo IP vai conter todas as funcionalidades dos encaminhadores genéricos que implementam o *stack* de protocolos TCP/IP versão 4, estando presentes neste módulo, para além de outras, funções como o *Forwarding*, resolução de endereços ARP, gestão de erros por ICMP, encapsulamento de pacotes em túneis IPIP, etc.

Estes mecanismos genéricos vão ser reaproveitados pelos novos módulos necessários nesta rede de acesso, sendo estes configurados dinamicamente pelos novos módulos.

Módulos de encaminhamento:

Associado ao *forwarding* está o módulo de encaminhamento, que em encaminhadores muito simples poderá ser estático, mas usualmente dinâmico para os encaminhadores mais avançados. Neste caso, o módulo de encaminhamento vai automaticamente aprender as localizações dos terminais móveis na rede de acesso, configurando a tabela de encaminhamento do sistema.

Quando existirem pacotes para encaminhar, o módulo de *forwarding* vai consultar esta tabela do sistema para encontrar o próximo nó e a interface de saída dos pacotes, e deste modo os módulos de encaminhamento vão configurar dinamicamente o módulo genérico de *forwarding*.

No caso desta rede de acesso *wireless*, todos os elementos de rede vão deter um módulo de encaminhamento dinâmico (TIMIP), responsável pelo suporte da micro-mobilidade dos

terminais móveis no **interior** da rede, de forma a que tenha a noção da localização dos terminais móveis, o que é essencial para lhe dar a conectividade.

O conjunto dos encaminhadores da rede vão estar organizados numa árvore lógica, em que cada encaminhador tem um único nó ascendente, e o encaminhador localizado na raiz é denominado de GW e tem a ligação à rede de core.

Além da comunicação pela tabela de encaminhamento, o módulo TIMIP também vai comunicar com os seus correspondentes dos encaminhadores adjacentes por via de pacotes de controlo exclusivos deste protocolo. A última característica deste módulo é que deverá receber uma cópia do cabeçalho IP de todos os pacotes de dados que são recebidos pelas interfaces do encaminhador para inspecção.

Além do TIMIP, a GW da rede vai ter um segundo módulo de encaminhamento sMIP (*surrogate* MIP), complementar ao TIMIP para o suporte da macro-mobilidade dos terminais móveis, tornando a GW num *surrogate agent* sMIP com a capacidade de localizar e suportar a conectividade dos terminais móveis entre as redes, comunicando com o HA localizado na rede de origem do terminal legado como se fosse este.

Este módulo de encaminhamento tem interacções com TIMIP, para este último lhe induzir a fase de detecção dos terminais legados ao nível da macro-mobilidade, sendo estas criadas por via de uma sinalização interna definida entre os dois.

Note-se que estes dois tipos de encaminhamento são completamente independentes um do outro; nomeadamente, o TIMIP apenas encaminha os pacotes para terminais móveis que estejam no interior da rede de acesso, tendo o sMIP a responsabilidade complementar de encaminhar pacotes para terminais móveis entre as redes.

Além do sMIP, a GW tem também um módulo clássico de suporte do MIP na sua componente de servidor (papel de HA e FA), sendo a sua execução independente dos anteriores TIMIP e sMIP.

Módulos de QoS:

O módulo de DiffServ vai ser utilizado para adicionar à rede suporte de QoS, sendo os fluxos de dados agregados em classes de serviço e tratados com serviços diferenciados de acordo com a sua classe durante toda a rede.

Este módulo vai estar presente em todos os encaminhadores da rede de acesso e é ortogonal ao módulo do encaminhamento, detendo das funcionalidades de configuração, tratamento dos pacotes à entrada e tratamento dos pacotes à saída. A primeira parte vai interagir com o

módulo IP para criar e alterar diferentes configurações estáticas de elementos de controlo de tráfego nas interfaces físicas do encaminhador, por forma a criar uma arquitectura adequada para executar as acções definidas na arquitectura DiffServ.

Quando a componente de configuração criar ou alterar uma dada configuração estática, cada interface do encaminhador vai deter de ambas as componentes genéricas DiffServ de Entrada e Saída, constituídas por elementos genéricos independentes das tecnologias, pertencentes ao módulo IP. Em cada interface a componente de Diffserv de entrada vai efectuar acções DiffServ assim que o pacote chega ao nível 3 do encaminhador.

Este módulo vai ser diferente quer se trate de uma interface fronteira ou core, uma vez que estas últimas **não** executam as acções de classificação e policiamento que são exclusivas das do tipo fronteira.

Além do Diffserv de entrada, cada interface do encaminhador também vai detém da componente de Diffserv de saída, com as funções de execução dos tratamentos agregados das varias classes (“*per hop behaviour”*) definidas nesta rede, por via de escalonadores de prioridades/“*weighted round robin”*.

A última acção que os pacotes sofrem antes de saírem do nível 3 do encaminhador é o de serem marcados com a sua classe de serviço agregado no campo apropriado do cabeçalho IP (campo DSCP).

Módulo de Tempo:

O último módulo que está ao nível IP presente em todos os encaminhadores, será o módulo de sincronização de tempo, que tem o objectivo de garantir que os relógios dos nós da rede de suporte estão o mais sincronizados possível de acordo com o relógio de referência da rede (relógio da GW), dado que este é um requisito do protocolo de encaminhamento TIMIP, e necessário para as medições a executar na rede.

Para isto, ter-se-á que usar um qualquer mecanismo que faça este acerto distribuído do relógio, como por exemplo o protocolo NTP (Network Time Protocol). Quando é usado este protocolo, a GW vai ter um servidor NTP para responder com o valor do seu relógio actual aos clientes NTP, que estão presentes nos restantes nós da rede. Este protocolo, específico para esta função de acerto dos relógios, atinge margens de erro na sincronização bastantes baixas porque executa automaticamente acções adicionais de correcção e ajuste relativos à própria acção de propagação e tratamento das mensagens NTP.

Módulos do Nível 2:

As restantes componentes dos elementos da rede já são dependentes das tecnologias de rede, fazendo parte do nível 2 do encaminhador ("*link layer*"). Estas vão estar intimamente associadas às interfaces físicas e aos detalhes de cada tecnologia específica, existindo tantos componentes quanto as interfaces físicas presentes no encaminhador.

As interfaces físicas *wireless* 802.11 vão permitir que os terminais móveis se liguem à rede e se movimentem no interior desta, podendo qualquer elemento da rede de suporte ter uma interface deste tipo, o que torna num AP (Access Point, ponto de acesso da rede. Para tal, as interfaces 802.11 vão funcionar no modo estruturado do 802.11, de forma a ocuparem uma célula inteira, e participarem na rede 802.11 comum com o mesmo nome de rede que os outros APs.

A principal acção desta interface será o de receber e enviar pacotes de dados de/para os terminais móveis, pelo que, todos os pacotes emitidos pelos terminais que sejam recolhidos por esta interface vão ser entregues ao nível acima IP para encaminhamento (e também uma cópia do cabeçalho para o TIMIP).

O outro tipo de interface que os encaminhadores possuem é respeitante às interfaces Ethernet, que vão receber e enviar pacotes de dados de forma semelhante às interfaces *wireless*. Estas interfaces são utilizadas para ligar os encaminhadores entre si, e adicionalmente para ligar a rede de acesso à rede de core, no encaminhador na raiz da árvore.

Nesta situação, o encaminhador que tiver a ligação à rede de core será a GW desta rede, e o seu endereço IP desta interface o endereço identificador desta rede como um todo para os protocolos de encaminhamento).

5.1.2 Vida do pacote

No interior da rede de acesso vão existir apenas 2 tipos de fluxos diferentes de pacotes IP: fluxos de controle e dados IP.

Os primeiros são utilizados pelos componentes dos encaminhadores nas suas comunicações internas, nomeadamente a transferência de informações de mobilidade, configuração remota de QoS e sincronização de tempo, os quais são recebidos directamente pelo módulo correspondente no interior dos encaminhadores.

Todos os restantes fluxos vão ser considerados como fluxos de dados, com um tratamento genérico simples no interior do encaminhador, ilustrado na Figura 61, que descreve o processamento dos pacotes de dados no interior do núcleo do encaminhador, tanto no nível 2

como no 3. Para referência, a mesma figura com mais detalhe, incluindo os *deamons* de controle do encaminhadores da rede, está presente no Anexo 15.

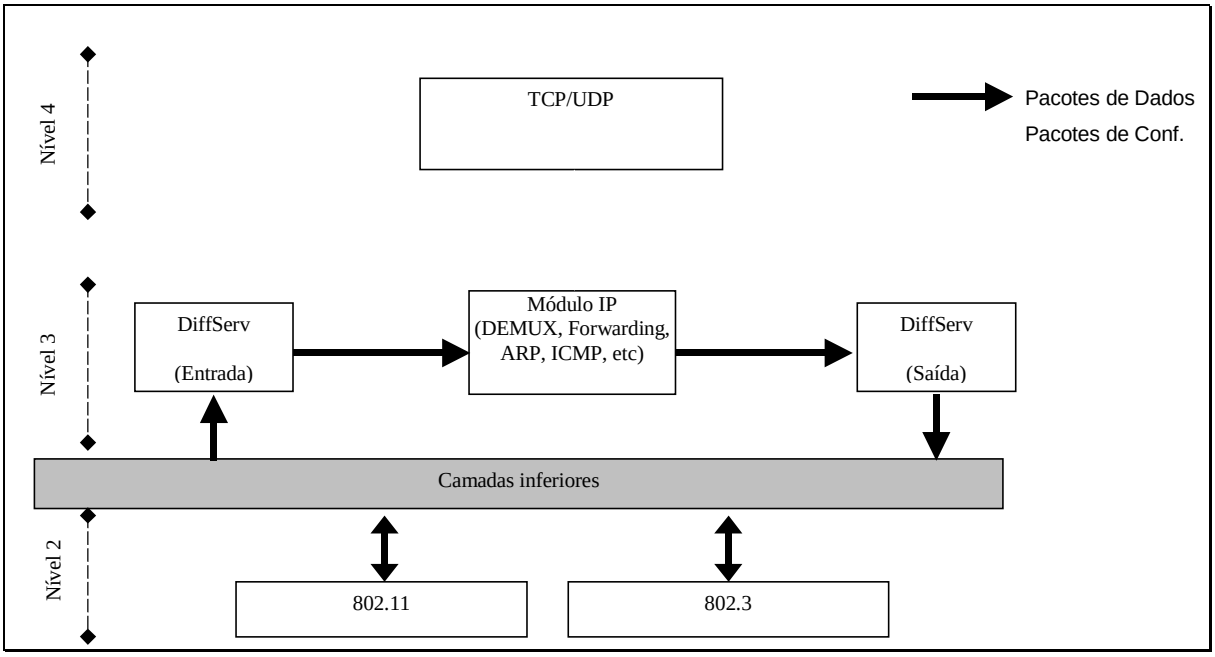


Figura 61: Vida dos pacotes de dados

Assim, quando um pacote de dados chega ao encaminhador por uma das interfaces deste, o pacote vai ser sempre entregue pelo nível 2 ao IP para processamento, e nesta operação, o pacote é entregue à componente de DiffServ de entrada da interface por onde chegou, e uma cópia do cabeçalho IP é entregue ao módulo TIMIP para análise.

Uma vez no Diffserv de entrada, o pacote vai sofrer diferentes tratamentos se esta interface for do tipo fronteira, ou core. No primeiro caso, o pacote vai ser classificado e policiado pela única vez nesta rede, sendo-lhe atribuído uma classe de serviço consoante as suas características (dependentes da configuração estática actual que a configuração Diffserv instanciou). No outro caso, o pacote já está previamente aceite e marcado numa classe por um encaminhador anterior, pelo que a sua classe é extraída do cabeçalho IP.

Seguidamente o pacote é entregue ao módulo genérico IP, que é igual aos encaminhadores normais IP. Neste módulo, a operação de *forwarding* vai considerar o destino do pacote, e escolher o próximo nó por onde este pacote de dados vai ser encaminhado, consultando para tal a tabela de encaminhamento do sistema, que os protocolos de encaminhamento vão manter consistente com o estado actual da rede de acordo com as localizações presentes dos terminais móveis.

O pacote é então entregue à interface de saída, sendo entregues transparentemente à componente Diffserv de Saída, onde o pacote vai ser considerado juntamente com os restantes da mesma classe, formando em conjunto um *Agregado*.

Nesta componente, os agregados são processados de acordo com as suas importâncias relativas e ocupação dos recursos de saída, por via de escalonadores que serializam os pacotes por várias métricas, que estão associados a filas de espera com diferentes limites ou tratamentos, como acções de perda antecipada (*early drop).*

A última acção deste componente será o de marcar o pacote com a informação da sua classe, num campo específico do cabeçalho IP (DSCP) (com efeito apenas nos encaminhadores Fronteira da rede, já que nos *core* a marcação mantém-se inalterada).

Por fim, quando o pacote sair desta última componente, então é entregue à interface de saída do encaminhador por onde será transmitido para o próximo nó, ou para o seu destino final.

5.2 Módulos dos elementos de rede

Esta secção vai descrever em detalhe os módulos que estão presentes nos elementos de rede, que consoante o tipo de elemento de rede poderão não estar presentes na sua arquitectura.

5.2.1 Kernel Linux

Este módulo de *software* é a peça base onde todos os restantes módulos vão encaixar, estando bem documentado, como em [51], [52], [53] e [60]. Entre outros, o *kernel* inclui na sua componente de rede os protocolos base, *drivers*, controlo de tráfego, além de todas as funcionalidades necessárias para a utilização do hardware, como a gestão dos processos, memória, dispositivos, etc.

Como está descrito em grande detalhe em [92], nesta rede de acesso os nós usaram o *kernel* 2.4.18 (a versão estável mais recente, à data do início da implementação deste trabalho), com alterações específicas (*patches*) a diversas componentes, e com adições ao suporte de hardware utilizado, como as interfaces PCMCIA. Além disto, o *kernel* também foi configurado de uma forma especial, nomeadamente pela alteração do grão do sistema para um valor mais rápido, e pela medição do tempo de uma forma mais precisa.

5.2.2 Módulo IP

O módulo IP vai genericamente agrupar as funções genéricas dos encaminhadores Linux que implementam a base do protocolo IP clássico (nível 3), contendo as funções de *demultiplexing*

(DEMUX), *forwarding*, resolução de endereços por ARP, gestão de erros (ICMP), etc. Este modulo, residente no Kernel do linux, e as suas utilidades associadas, estão bem documentados nas referências [52] a [63], cobrindo estas referencias tanto a configuração, utilização, programação e alteração das componentes de rede.

No caso dos encaminhadores da rede de acesso, este módulo vai ser configurado dinamicamente pelos módulos de Encaminhamento e Diffserv, de forma a que os pacotes de dados são sempre processados por mecanismos exclusivamente residentes no núcleo do sistema, o que aumenta substancialmente o desempenho (comparando com a sua manipulação por programas do espaço do utilizador).

Um aspecto chave existente no IP é a sua configuração pela tabela de encaminhamento por parte dos módulos de encaminhamento, que será utilizada pelo módulo de *forwarding* com as vantagens referidas no parágrafo anterior. No entanto, note-se que esta tem uma latência mínima de 2 segundos, por omissão, relativamente à efectivação das alterações, mas dado que esta latência está no caminho crítico do processo de *handover* do TIMIP, a tabela de encaminhamento foi alterada por forma a retirar esta limitação.

5.2.3 Driver 802.3

Este módulo consiste num *driver* de *software* de acesso às interfaces físicas Ethernet presentes nos elementos da rede. Relativamente ao hardware, esta carta *ethernet* é descrita em [92], sendo utilizado um *driver* já existente no *kernel linux*, que não necessitou de qualquer alteração. Este acrescenta uma interface ao sistema denominada de **eth**x, sendo automaticamente utilizada pelo módulo IP, e configurada pelo suporte de mobilidade e Diffserv (pelos comandos **ifconfig** e **tc**).

5.2.4 Driver 802.11

Este módulo também consiste num *driver* de *software* para utilização do hardware 802.11 que está presente nos APs da rede, descritos em [92]. Estas cartas têm uma interface PCMCIA, e utilizam o *chipset* prism2 da Intersil [79], o qual tem um modo especial, denominado de *hostAP*[81], no qual as funções básicas de estação são complementadas por *software*, de forma a realizar um AP completo compatível com qualquer cliente 802.11, tendo este *driver* o suporte deste modo especial.

Esta solução provou ser a mais flexível para os objectivos pretendidos neste trabalho, por permitir a alteração de grande parte das características do ponto de acesso 802.11, dado serem implementadas em *software*[65].

No início da implementação da rede de acesso, este *driver* estava ainda num estado inicial com suporte ao modo especial desejado, mas ainda numa fase inicial da sua depuração. Por esta razão, ao longo da duração deste trabalho, o módulo sofreu diversas alterações, sendo algumas genéricas, e outras específicas para esta rede de acesso.

Relativamente às primeiras, no contexto da rede foram descobertos e corrigidos diversos *bugs*, *race conditions*, ineficiências, etc., bem como foi adicionado suporte para mais funcionalidades, como certas *wireless extensions* e acções de gestão. Por serem genéricas, estas alterações foram propagadas para o *driver* original, para benefício da comunidade de utilizadores deste *software* [82].

Por outro lado, houve alterações específicas para esta rede de acesso, de que se destacam:

a) Adição da notificação assíncrona das acções de gestão do 802.11 para o TIMIP, utilizando um *socket netlink* de comunicação entre o núcleo e os *deamons* que correm no espaço do utilizador. Esta funcionalidade vai instanciar no 802.11 a detecção reactiva do protocolo TIMIP de uma forma extremamente eficiente.

b) Alteração da política de *queueing* interna do hardware, de forma a limitar o número máximo de pacotes de dados que podem estar pendentes para transmissão (à saída da interface *wireless*), para o valor de 10 pacotes (abaixo deste valor o desempenho da carta sofria, deixando se ser possível transmitir o máximo da tecnologia).

   Esta alteração deveu-se ao facto de o hardware ter memória interna (*buffer*) para transmissão de pacotes, utilizada para reduzir a ocupação do processador na acção de transmissão de pacotes em rajada. No entanto, esta optimização cria um atraso substancial nos pacotes prioritários quando a saída estiver saturada, dado que nesta fila não existe distinção das classes de pacotes (i.e., esta fila afasta demasiadamente a qualidade de serviço do nível 3 da transmissão).

[65] Esta solução foi comparada com outras possibilidades, nomeadamente pela utilização de *firmware* adicional para a funcionalidade de AP (*firmware* terciário [80]), mas que não permitia customizações. No entanto, foi a opção seguida por um trabalho paralelo a este, descrito em [84], utilizando outro driver [83].

De uma forma semelhante à da interface Ethernet, o *driver* vai criar uma interface ao sistema denominada de **wlan**x, sendo esta utilizada pelo módulo IP, e configurada tanto pelo suporte de mobilidade com pelo Diffserv (pelos comandos iwconfig, ifconfig e tc).

5.2.5 Módulo TIMIP

Para a implementação do TIMIP, cada nó da rede vai ter um *deamon* que instancia este protocolo. O processo completo da sua instalação, configuração e execução está detalhado em [92], sendo aqui apenas descrita a informação que não está nesta referência, nomeadamente a relativa à arquitectura interna, interacções e algoritmos/máquinas de estado.

Dada a sua natureza, este módulo foi implementado no espaço do utilizador, não necessitando de estar no núcleo para garantir um desempenho máximo[66]. Isto acontece porque este apenas vai, em certas ocasiões periódicas, interagir com o módulo de *forwarding* do IP através da configuração da tabela de encaminhamento do sistema.

Neste sentido, a componente crítica do *forwarding* dos pacotes de dados continua a ser efectuada no interior do núcleo, sendo apenas o seu controlo no exterior, o que tanto garante o seu desempenho, como mantém a facilidade de implementação do módulo. Assim, o controlo TIMIP é instanciado em "user space", sendo os dados IP em "kernel space".

Estas interacções com as componentes do IP são efectuadas principalmente por via de comandos externos do sistema, exceptuando-se as alterações à tabela de encaminhamento, que são efectuados de forma directa por *netlink*[67], dados que estão no caminho crítico do processo de *handover* do TIMIP. Por estas razões, o *deamon* terá que ser executado com os privilégios totais do sistema (utilizador *root*).

5.2.5.1 Arquitectura do módulo TIMIP

A figura seguinte – Figura 62 – vai descrever a estrutura interna do *deamon* TIMIP, que contém grupos de acções, estruturas de dados, e interfaces.

[66] Embora seja lançado com prioridade sobre os restantes programas e *deamons que se executam no sistema*, por via do comando *nice do Unix*.

[67] Sendo esta uma opção (na compilação do *deamon*), podendo-se utilizar comandos externos em todas as situações.

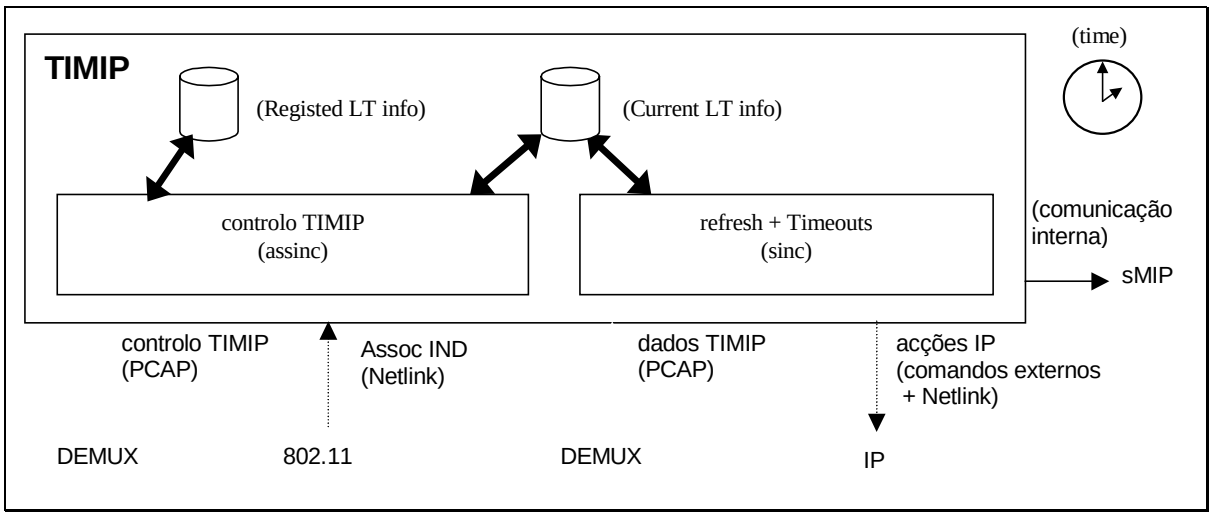


Figura 62: Interfaces do módulo TIMIP

5.2.5.1.1 Acções

O módulo TIMIP tem dois tipos de componentes de acções básicas, que vão estar relacionadas com as acções assíncronas e síncronas do *deamon*:

As primeiras estão relacionadas com o controlo TIMIP de suporte à criação e modificação da mobilidade dos terminais legados, tendo requisitos apertados de responsividade, pois entram no caminho crítico dos *handovers* TIMIP, devendo estes ser tão rápidos quanto possível para reduzir ao mínimo os períodos sem conectividade da responsabilidade da micro-mobilidade IP.

Entre estas, estão as acções despoletadas pela detecção dos terminais e pela recepção de mensagens de controlo TIMIP, utilizadas para a comunicação entre os nós da rede. Para tal, estas acções assíncronas têm o objectivo último de configurar a tabela de encaminhamento do nó, de acordo com o estado dos terminais móveis na rede.

O segundo módulo vai tratar dos algoritmos TIMIP que não têm este requisito de rapidez, nomeadamente a manutenção do estado dos terminais, envolvendo a recepção dos pacotes de dados IP, e as acções de *timeout* utilizadas para forçar os terminais a gerarem provas de vida, ou para cancelar os seus registos (ver Anexo 8)

Normalmente, esta distinção entre acções prioritárias e não prioritárias leva à utilização de mecanismos de paralelismo de *software* com suporte de preempção, o que obrigaria à existência de sincronização interna, por via de mecanismos como semáforos.

Contudo, optou-se por desenhar este modelo com base num modelo totalmente síncrono, sem paralelismo, mas com um desempenho muito semelhante relativamente à responsividade das acções de mobilidade.

Este modelo alternativo tem a vantagem de não necessitar de sincronização, por ter apenas um único fio de execução, e de possibilitar o processamento das acções do protocolo sem requisitos tempo-real periodicamente em modo "batch", o que aumenta o desempenho do módulo ao reduzir o seu peso no sistema, e, em última instância, permitindo o suporte de mais clientes ao protocolo.

O modelo está ilustrado em forma de máquina de estados na Figura 63, e consiste no tratamento periódico das acções síncronas, em modo "batch", e apenas uma vez em cada segundo (valor configurável). Durante esta operação, no final de cada acção síncrona, é sempre verificada a existência de acções assíncronas, que se existirem vão interromper o tratamento síncrono (por serem mais prioritárias).

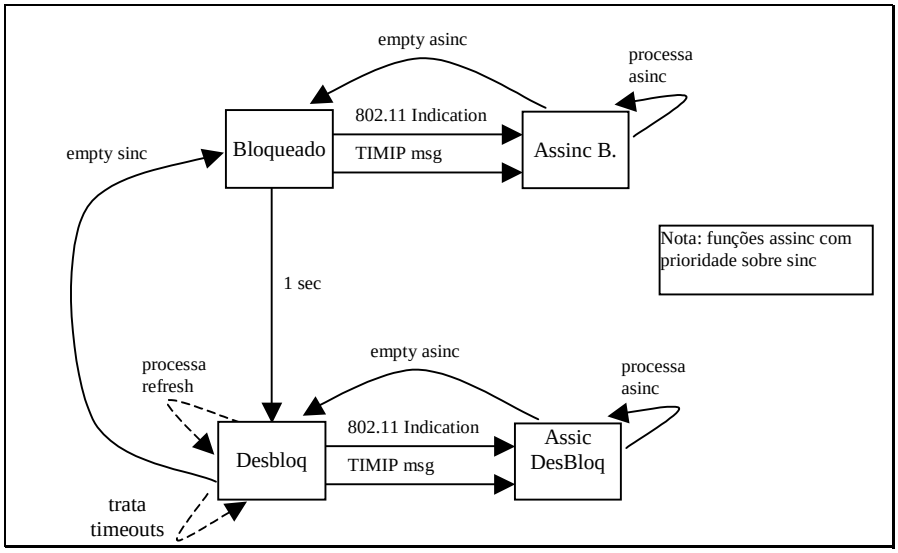


Figura 63: Máquina de estados para eventos assíncronos e síncronos

5.2.5.1.2 Estruturas de dados

As estruturas de dados vão conter as informações relativas aos terminais do ponto de vista deste nó da rede.

A primeira estrutura, BD_REGISTED, contém as informações dos terminais móveis que estão registados a operarem na rede, incluindo o seu endereço IP e MAC e outros dados (conforme a secção 3.1.4.4). Para os nós da rede normais, esta tabela é usada somente em leitura, podendo o seu conteúdo ser alterado por ordem da GW por processos de gestão.

A segunda estrutura, BD_CURRENT, vai conter a relação dos terminais que estão activos localizados por descendentes deste nó. Esta informação é alterada de acordo com os algoritmos de registo TIMIP, descritos na secção 3.1.3.1, que podem incluir a detecção dos terminais nos APs, a chegada de mensagens TIMIP dos nós adjacentes, ou pelos *timeouts*.

Note-se que a tabela de encaminhamento do sistema é sempre alterada de acordo com as alterações desta tabela interna, por forma a instanciá-las no encaminhamento dos pacotes IP.

Por último, é também de referir que esta estrutura é concretizada por uma árvore binária, por forma a optimizar a pesquisa de informação que será indexada pelo endereço IP dos terminais.

5.2.5.1.3 Interfaces

O módulo vai comunicar com o exterior por via de interfaces bem definidas, do tipo uni ou bidireccionais, e que envolvem pacotes de informação ou apenas recursos internos do Linux, como a troca de mensagens.

Relativamente às interfaces que trocam pacotes, estas são efectuadas directamente de/para o módulo DEMUX do *kernel*, por onde todos os pacotes passam no nível 3, e que são entregues ao módulo interno do Linux para processamento (nomeadamente o TCP/UDP/ICMP/ FORWARDING). Para utilizar este tipo de interfaces, o *deamon* vai na sua inicialização registar-se directamente no DEMUX estabelecendo interfaces PCAP (Packet capture) [64].

Esta interface PCAP é uma API genérica multi-plataforma utilizada para a recepção e envio de pacotes directamente de/para as interfaces físicas do encaminhador, com uma utilização integrada nos *sockets* BSD. Esta API é largamente utilizada nas aplicações de inspecção/gestão/análise da rede, como o Ethereal e o Tcpdump.

Para isto, por cada interface física do encaminhador, vão existir 2 interfaces PCAP distintas para controlo e dados, onde se indica *que* pacotes desta interface o módulo pretende receber, por via de uma "string" com uma sintaxe e semântica simples. Em Linux, o PCAP tem uma implementação muito poderosa, dado que a componente de desmultiplexagem dos pacotes à entrada no IP é pré-compilada dinamicamente no DEMUX, efectuando-se a escolha em "kernel mode" de uma maneira muito eficiente. Os detalhes destas *strings* de captura utilizadas no *deamon* estão detalhadas no Anexo 12.

Esta separação entre controlo e dados, permite a divisão anterior entre acções síncronas e assíncronas, o que leva a uma grande responsividade do módulo em relação às operações críticas do *handover*.

Assim, o PCAP do controlo vai tratar exclusivamente dos pacotes de controlo TIMIP encapsulados em ICMP, e o PCAP dos dados vai receber apenas o cabeçalho IP dos dados encaminhados pelo encaminhador, para a inspecção do endereço de origem (apenas nos instantes síncronos bem determinados, como já foi referenciado).

Por outro lado, o *deamon* também vai, em situações bem definidas, gerar pacotes do tipo controlo por via de um dos PCAP da interface de saída, o que permite assemblar o pacote desejado especificando *todos* os campos de *todos* os níveis, sendo assim substancialmente mais poderoso que *sockets* clássicos INET. Entre estes, o *deamon* vai gerar pacotes TIMIP encapsulados em ICMP para as comunicações inter-nó das acções de update e acknowledge, pacotes ICMP *echo request* para a manutenção do estado dos terminais, e pacotes *gratuitous* ARP para a alteração em cada handover das caches ARP dos terminais com o novo valor da GW.

Relativamente à comunicação com as outras componentes do sistema, todas as acções de configuração das funções IP são efectuadas pela utilização dos comandos específicos externos, que têm a grande vantagem de se manterem válidos mesmo que o *kernel* linux sofra alterações internas. Entre estes, encontram-se o comando **route** (manipulação da tabela de encaminhamento), **arp** (manipulação da tabela de arp/proxy arp), **ip** (manipulação de túneis IPIP), **ifconfig** (gestão IP das interfaces físicas), **iwconfig** (gestão L2 das interfaces *wireless*).

A única excepção a este comportamento é nas alterações da tabela de encaminhamento do sistema, que terão de ser efectuadas de uma forma extremamente eficiente por estar no caminho crítico do *handover* dos terminais. Neste caso específico, a tabela é alterada usando uma interface *netlink* directa ao módulo FORWARD do *kernel* (que detém esta tabela).

A última interface existente é referente à detecção reactiva do TIMIP, originada no *driver* 802.11. Para isto, é também usada uma interface *netlink*, unidireccional, desde o *driver* directamente para o *deamon*.

Conceptualmente, também existiria uma interface entre o módulo e o módulo sMIP, necessária para a detecção dos movimentos dos terminais, mas no entanto, tal como vai ser descrito no módulo sMIP, tal interface é meramente interna, uma vez que o *deamon* inclui o suporte para os dois protocolos em simultâneo (mas que são todavia independentes entre si).

Por fim, é da responsabilidade do TIMIP o suporte do MIP, tal como está definido em 3.3.1.1, pelo que a GW TIMIP vai gerar pacotes de *beacons* MIP, que vão ser propagados pela rede por via dos nós TIMIP, que vão agir como um *relay agent* destes *beacons* MIP, passando-os desde os terminais até à GW e vice-versa.

5.2.5.2 Implementação dos algoritmos avançados TIMIP

Esta secção vai detalhar a implementação dos algoritmos mais importantes que foram definidos teoricamente no TIMIP.

5.2.5.2.1 Detecção da chegada dos terminais

Quando a primitiva assíncrona de chegada dos terminais é despoletada pelo mecanismo netlink, o *deamon* analisar imediatamente a informação que esta contém, que será o endereço MAC do terminal detectado.

Quando isto acontece, o *deamon* vai consultar a informação de registo (BD_REGISTED), para verificar se este terminal está registado na rede. Em caso afirmativo, então o seu endereço IP é extraído desta base de dados, sendo usado exclusivamente em todas as operações subsequentes.

Assim, quando recebe a informação da detecção, o AP vai:

a) Verificar o seu próprio relógio, que terá que estar sincronizado com os dos outros APs (por NTP, ou outro protocolo de sincronização de tempo), o valor temporal desta movimentação do terminal na rede, alterando (BD_CURRENT) com a informação que o terminal se encontra localizado na sua interface *wireless* e com o tempo da sua chegada.

b) Se anteriormente o terminal já estava presente neste AP, então significa que o nó não aprendeu nada de novo, pelo que o processo termina aqui.

c) No caso contrário, então o terminal vai colocar o antigo nó mais próximo (i.e. o nó por onde anteriormente o terminal era acessível) numa lista de nós que ainda não responderam com *acknowledge*, e cria um pacote de *update* relativo a este terminal com: endereço origem/destino apropriados, endereço do terminal móvel, *timestamp* actual. Este pacote de *update* é então enviado ao anterior próximo nó, utilizando a interface PCAP apropriada. (ver Anexo 4 relativamente ao formato dos pacotes de controlo TIMIP).

d) De seguida, o nó vai instanciar a alteração que ocorreu, alterando a tabela de encaminhamento do sistema com a informação mais actualizada que aprendeu. Para isto, o *deamon* vai comunicar por *netlink* directamente para o módulo *Forward* do *kernel* Linux, com a alteração desejada.

e) Por fim, o AP vai enviar um *gratuitous* ARP do valor da GW ao terminal (gerando um pacote **ARP reply** enviado por PCAP), e adiciona o seu MAC à tabela de ARP do sistema (pelo comando externo **ARP**).

5.2.5.2.2 Tratamento do update

O processamento dos *Updates* é a parte chave do funcionamento do *deamon* TIMIP, porque é por estas mensagens que a rede fica a saber a nova localização dos terminais.

Neste processo, quando um nó recebe uma mensagem de *update* vindo de um qualquer nó adjacente a si, então no caso normal este passa a ser o novo próximo nó do terminal, isto é, o nó por onde o terminal se localiza e por onde são encaminhados os pacotes que lhe são destinados (estas acções têm excepções/opções a descrever posteriormente).

Assim, quando recebe o *update*, o nó vai:

a) Comparar o *timestamp* da associação deste terminal com o seu actual (consultando BD_CURRENT), aceitando se for igual ou mais recente que o actual para este terminal.

b) Emitir um pacote de *acknowledge* ao emissor, gerando o pacote de resposta TIMIP, usando a interface correcta de PCAP para emitir o pacote. Note-se que se este pacote de *ack* não tem garantias de recepção; se se perder, o emissor original reenvia o *update* original, e que terá um comportamento idempotente neste nó.

c) Considera o novo *timestamp* do terminal (se for mais recente), alterando o estado do terminal (BD_Current).

d) Se o *update* manteve o próximo nó do terminal, então significa que o nó não aprendeu nada de novo, pelo que o processo termina aqui.[68]

e) No caso contrário, então o terminal vai colocar o antigo nó mais próximo (o nó por onde anteriormente o terminal era acessível) numa lista de nós que ainda não responderam com *acknowledge*, e recria o pacote de *update* com: endereço origem/destino apropriados, endereço do terminal móvel, *timestamp*. Este pacote de *update* é então enviado ao anterior próximo nó, por PCAP. (ver Anexo 4 relativamente ao formato dos pacotes de controlo TIMIP)

f) Excepções: tanto o AP anterior como a GW da rede vão terminar a propagação do *update*, quando o caminho anterior não apontar para um nó da árvore.[69]

[68] Embora, do seu ponto de vista, o nó não tenha aprendido nada de novo, o terminal pode ter-se movimentado num nível mais baixo na árvore de nós.

g) De seguida, o nó vai efectuar as acções locais necessárias para instanciar a alteração que ocorreu, bastando-lhe alterar a tabela de encaminhamento do sistema com a informação mais actualizada que aprendeu, comunicando por *netlink* directamente para o módulo *Forward* do *kernel linux*.

5.2.5.2.3 Resolução das inconsistências do estado na rede

Tal como foi descrito na descrição teórica do TIMIP, existem certas situações de inconsistência da rede que são resolvidas com o recurso ao *timestamp* presente em todas as mensagens de controlo TIMIP, e permite resolver os conflitos.

Neste sentido, quando um nó receber um *update* relativo a uma movimentação mais antiga que a actual (registada em BD_CURRENT), então é sinal que o nó que está a enviar a mensagem não tem a informação mais actualizada do terminal móvel, *embora pense que tem* (porque está a enviar o *update*).

Nestas condições, o nó não vai enviar o *acknowledge* como normalmente, pois isso indicaria a aceitação do *update*, mas sim uma resposta do tipo *update* com a informação mais actualizada do terminal (incluindo o novo *timestamp*), que quando for recebida pelo nó confuso vai obrigar à recorrecção do estado inconsistente da rede (esta situação é ilustrada em detalhe no Anexo 7).

De uma forma complementar, quando um nó recebe um *acknowledge*, este vai verificar o *timestamp* a que se refere. Se for o esperado, então o nó que respondeu é retirado da lista dos nós que ainda têm que responder ao *ack*; se for mais antigo, então este nó está desactualizado, pelo que o *deamon* mantêm-no nesta lista, o que vai ter o efeito secundário de lhe transmitir o *update* mais recente (mais tarde, pelo mecanismo de *timeout*).

5.2.5.2.4 Acções síncronas

Esta secção vai descrever em detalhe as acções síncronas efectuadas pelo *deamon*, acções estas apenas processadas periodicamente (em "batch"), uma vez que as acções que despoletam não têm requisitos temporais apertados, ao contrário das mensagens de controlo e

[69] Note-se que a chegada da mensagem de update ao AP anterior do terminal pode ser utilizada para outras acções extra-mobilidade, como por exemplo a cópia do contexto anterior do terminal entre os dois APs (sendo esta funcionalidade útil para o suporte "*seamless*" de QoS na rede de acesso).

detecção dos movimentos. Basicamente, estas acções estão apenas relacionadas com a gestão dos *timers* do protocolo, que são descritos no Anexo 8.

CONTROLO (Garantia de entrega)

O primeiro *timer*, configurado pela opção Timeout_ack do TIMIP, controla a retransmissão automática dos *updates* para os nós adjacentes da rede. Da forma como foi descrita anteriormente, cada nó tem uma lista dos nós que ainda não responderam com um *acknowledge*, o que pode ter acontecido porque houve perda de pacotes (tanto do *update*, como do *ack*), mas também se este não tiver sido aceite (ver acima). Assim, para cada nó nestas condições, depois de passar este tempo (Timeout_ack) sem resposta, o *update* é reemitido de novo para cada nó em questão.

DADOS (Manutenção do estado)

O segundo *timer* controla a manutenção do estado do terminal móvel no nó, com o objectivo de verificar se o terminal ainda está no interior do domínio TIMIP.

No caso em que o terminal estiver silencioso, então este *timer* vai começar a ser disparado, com intervalos dinâmicos compreendidos entre as opções do TIMIP (Timeout_start) e (Timeout_min), com o valor inicial de Timeout_start, e com a optimização que o valor do *timeout* na GW é ligeiramente menor que os dos nós normais. De cada vez que o *timer* for disparado, o seu valor dinâmico é alterado da forma descrita na secção 3.1.4.3, (página 69), e é gerado um pacote ICMP ECHO REQUEST destinado ao terminal para o forçar a responder, sendo este identificado como emitido pela GW da rede, e que tem o efeito secundário de refrescar todo o estado da rede de uma só vez.

De forma complementar, o *deamon* vai, de tempos a tempos, verificar “em batch” os cabeçalhos dos pacotes de dados recebidos por cada interface descendente (usando a interface o PCAP de dados), para verificar se algum pacote de dados emitido pelo terminal aparece da interface esperada (a interface onde o terminal está registado). Em caso afirmativo, então o terminal é refrescado, sendo o *timer* dinâmico alterado da forma descrita na secção 3.1.4.3.

Por fim, quando o *timer* é sucessivamente disparado sem resposta do terminal, então depois do tempo limite (Timeout_remove), o nó assume que o terminal saiu da rede ou foi desligado, sendo o seu estado removido do nó, incluindo as alterações efectuadas no módulo IP (encaminhamento, arp, etc.) (no entanto, note-se que este mecanismo só é utilizado para a remoção do terminal nesta situação; para as alterações do encaminhamento, é usada a sinalização explícita em todos os casos).

5.2.6 Módulo sMIP

O módulo sMIP vai complementar o TIMIP para o suporte de macro-mobilidade dos terminais legados, em que os agentes MIP executam as funções dos terminais em nome destes. Neste sentido, *embora se localize num agente MIP*, o sMIP é mais parecido ao cliente MIP do que ao Agente MIP.

Conceptualmente, o módulo sMIP é totalmente independente do TIMIP, com a excepção da que as acções de detecção, dado que são sempre despoletadas pelo TIMIP, dividindo-se entre a detecção de chegada e partida dos terminais. Deste modo, existe um módulo bem definido sMIP que implementa este protocolo, mas que coexise no interior do mesmo *deamon* TIMIP, o que simplifica a acção de execução do *software*, e comunicação entre os dois módulos.

Para implementar o sMIP, foi adaptado o *software* anteriormente realizado de implementação do cliente MIP, sendo a sua arquitectura, acções, algoritmos, etc., descritos em grande detalhe no trabalho [90].

Nesta implementação, cada GW sMIP vai executar vários clientes MIP em simultâneo, um para cada terminal legado com necessidade de macro-mobilidade, e executando apenas a fase 2 do Cliente MIP (registo). As outras fases do cliente MIP foram *desactivadas* na implementação do sMIP, e adaptadas da forma que seguidamnete se descreve:

5.2.6.1 Fase 1 – detecção

Quando o sMIP opera em conjunção com o TIMIP, este usa uma acção reactiva de detecção dos terminais substancialmente mais optimizada do que a acção clássica passiva. Neste sentido, as acções TIMIP são convertidas em acções de detecção do cliente MIP, de acordo com a seguinte tabela, o que leva cada cliente MIP no sMIP a alterar o seu estado de acordo com as acções originadas pelo TIMIP.

ACÇÃO TIMIP	==>	ACÇÃO sMIP
Power-up TIMIP de um terminal legado visitante com opção de sMIP		Detecção por parte do cliente MIP da chegada a uma rede visitada MIP com Fa (coincidente com a GW TIMIP)
Remoção de um terminal legado visitante		Detecção por parte do cliente MIP da chegada à sua rede de origem MIP, em que a GW é o seu HA

5.2.6.2 Fase 2 – registo

Para esta fase, o TIMIP vai apenas deixar que o sMIP se execute, pois este vai-se comportar automaticamente de acordo com o seu estado actual, induzido pelo TIMIP pela fase anterior.

Desta forma, o cliente MIP vai registar-se automaticamente no seu HA quando o terminal chega ao domínio TIMIP pela primeira vez, manter este registo enquanto o terminal se mantiver no domínio, e desregistar-se no seu HA quando o terminal sair do domínio.

ACÇÃO TIMIP	==>	ACÇÃO sMIP
periodicamente, invocar o sMIP sem mudança de estado		criação/manutenção do processo de registo (fase 2) como está definido no MIP

5.2.6.3 Fase 3 – execução

Uma vez que o sMIP apenas terá que fazer chegar os pacotes ao domínio correcto, passando estes a serem encaminhados pela micro-mobilidade, a única acção do sMIP da fase de execução será a de aceitar os pacotes encapsulados enviados pelos diversos HAs, e para isto, na inicialização do *deamon*, este vai configurar o módulo IPIP com esta informação, utilizando para isto um comando externo apropriado.

5.2.7 Módulo MIP

De uma forma totalmente distinta do sMIP, o módulo MIP vai executar a componente de Agente MIP (componente servidor), sendo implementado como um *deamon* único a executar-se na GW da rede TIMIP, sendo configurado da forma apropriada para esta rede de acesso.

Tal como no caso anterior, este *software* está descrito em grande detalhe no trabalho [90], em relação à sua instalação, configuração e utilização. As únicas alterações necessária para a utilização do *deamon* MIP foram referente à desactivação tanto da fase 1 (localização) e 3 (registo), da forma semelhante ao sMIP, dado que estas funções são executadas pelo TIMIP.

5.2.8 Módulo DiffServ

5.2.8.1 Módulo DSR

Para o suporte de QoS na rede de acesso, foi utilizado o mesmo *software* desenhado para a rede de core da ilha do INESC, o DSR. Este *deamon* está detalhado no seu manual [70], e a sua instalação, configuração e utilização está descrita na referência [92].

Basicamente, DSR é um *deamon* que instancia a arquitectura Diffserv nos recursos de controle de tráfego existentes no Linux, que estão bem documentados nas referências [65] a [69], e em especial em [71], cobrindo todos os aspectos do controle de tráfego, relativamente aos filtros, filas, escalonadores, classes, etc., sendo estes elementos configuráveis no Linux por um comando externo denominado **tc**. Neste sentido, o *kernel* do Linux já tem as

componentes necessárias para criar uma arquitectura Diffserv, embora não estejam integradas entre si, o que é o objectivo do DSR.

Assim, este *deamon* vai gerar a arquitectura Diffserv completa, com encaminhadores do tipo *edge* e *core*, apenas controlando os elementos do *kernel* por via da geração de comandos **tc**. Para tal, o DSR é configurável remotamente, ou por uma linha de comandos interna, o que lhe permite uma integração facilitada com outros componentes como os Bandwith Brokers. No caso concreto da rede de acesso *wireless*, o DSR é executado na sua configuração inicial (ver [92]), sendo depois customizado com filtros específicos para o tráfego que vai passar na rede, estando estes presentes em *scripts*.

Nestas circunstancias, embora a configuração dos filtros DSR seja manual, este já está preparado para receber externamente pedidos de QoS, o que exigiria apenas a implementação de um módulo controlador para tornar este aspecto do suporte de QoS totalmente automático[70].

Relativamente à arquitectura dos dois tipos de elementos de rede – *edge* e *core routers* – o DSR vai seguir a arquitectura definida pelo Diffserv, presente no Anexo 13.

Nestas, o encaminhador vai suportadas todas as classes de serviço actualmente normalizadas – EF, AF1 a 4 com 3 "drop precedences" e BE – escalonadas por um *scheduler* HTB (Hierarquical Token Bucket), que oferece uma precisão superior ao CBQ clássico [40], conjugado com um escalonador PRIO para o tráfego EF (limitado por um *token-bucket* TBF).

Assim, as interfaces a interfaces *edge* nos encaminhadores fronteira vão incluir todas as componentes de classificadores, policiadores e marcadores, enquanto que as do tipo *core* já não as vão ter, dado que só se aplicam ao interior do domínio Diffserv, onde os pacotes já terão que estar devidamente marcados e policiados.

Para criar esta arquitectura, o DSR vai usar os já referidos elementos de controlo de tráfego do linux, da forma detalhada pelas figuras presentes no Anexo 14.

[70] O que poderá ser criado nomeadamente pela conversão Intserv=>DiffServ, com base na sinalização RSVP que descreve os fluxos de dados que passam na rede

5.2.8.2 Módulo DSR-Stats

O módulo DSR-Stats vai ser complementar ao módulo DSR descrito, por permitir a recolha periódica de estatísticas Diffserv do encaminhador, e com a possibilidade de as enviar remotamente para entidades centralizadoras da informação.

Uma destas será o sistema de monitorização desenvolvido para a análise da ilha do INESC no MOICANE, que permite a recolha, análise e comparação dos dados coleccionados dos diversos encaminhadores Diffserv da ilha do MOICANE, nomeadamente os presentes na rede de core, e na rede de acesso *wireless* principal.

Ambas estas componentes de monitorização estão descritas em grande detalhe em [70], tendo sido adaptadas para incluir o suporte da rede de acesso *wireless*.

5.3 Testes da Rede de Acesso

Nesta última secção, vão ser descritos os testes efectuados para avaliar a implementação da solução de mobilidade proposta para terminais legados nesta Tese, bem como das outras características complementares presentes na rede de acesso. Foram efectuados testes distinguidos entre funcionais e de desempenho, e para cada um, são apresentadas os objectivos, condições especificas e resultados do teste, estando estes dados resumidos na forma de *cartões de teste* no Anexo 16.

5.3.1 Aplicações utilizadas nos Testes

Para realizar os testes da rede de acesso, utilizaram-se diversas aplicações de teste, divididas entre aplicações genéricas e aplicações de ensino à distância criadas no contexto do projecto MOICANE.

Assim, as primeiras incluem os programas clássicos de teste ao protocolo IP PING e TRACEROUTE (ver [55]), com os quais é possível avaliar de uma forma normalizada em todos os sistemas a conectividade simples entre dois nós da Internet, incluindo a latência da comunicação (ping) e o caminho que os pacotes utilizam para chegar ao destino (traceroute).

Por outro lado, foi utilizado um programa (MGEN/DREC) [74] para efectuar a geração de tráfego arbitrário de teste da rede, sendo utilizado para criar diversas situações que vão testar e medir as características especiais da rede. Este programa (ver Figura 64) permite a geração de vários fluxos de dados UDP entre nós IP, com suporte para *unicast* e *multicast*,

possibilitando a emulação de padrões de tráfego de outras aplicações, ou apenas para carregar a rede.

No emissor, o tráfego pode ser gerado variando o número, tamanho, e distribuição dos pacotes; no receptor, o tráfego pode ser guardado em ficheiro, para posterior calculo de estatísticas relativamente ao débito, perdas, atraso, *jitter* da comunicação estabelecida, podendo estas serem bastante mais precisas que as possibilitadas pelo programa ping.

Figura 64: Gerador de tráfego MGEN/DREC

Este programa considera todos os seus valores ao nível UDP, de tal forma a medir as condições em que as aplicações dos utilizadores vão receber da rede, mas no entanto, em alguns testes a executar, pretende-se avaliar especificamente as características da tecnologia de rede 802.11, pelo que este programa foi alterado para efectuar as suas medições ao nível IP, de forma a que os tamanhos dos pacotes gerados sejam relativos aos entregues ao nível 2, e os débitos recebidos relativos à recepção pelo nível 3.

Além dos resultados extremo-a-extremo disponibilizados pelo MGEN/DREC, também foram efectuadas medições no interior da rede, sendo verificadas as estatísticas dos *deamons* dos *routers* (TIMIP/sMIP/DSR), e a utilização de *packet sniffers* nas interfaces de forma a verificar a estrutura dos pacotes IP gerados/recebidos, como também para efectuar medições de débitos em tempo real que são recebidos e enviados nestes elementos da rede. Para tal utilizou-se os programas Ethereal/TcpDump e o IPTraf para as funções descritas ([75], [76], [77]).

Por fim, a características da rede foram também testadas e demonstradas utilizando as aplicações dos clientes finais criadas para o ambiente Windows. Entre estas, foram utilizadas

aplicações genéricas como o acesso a servidores WWW (Internet Explorer), transferência de ficheiros (FTP), acesso remoto virtual a outros clientes (VNC), e aplicações multimedia como o programa de vídeo conferencia Netmeeting.

Além destas aplicações genéricas, foram utilizadas as aplicações desenvolvidas pelos parceiros Gregos no projecto MOICANE [78], e que criam um ambiente de *e-learning* necessário para um ensino à distância em que os intervenientes podem ser móveis. Estas são constituídas por diversas aplicações, entre o Chat (comunicação remota), VOD (Vídeo on Demand), VidConf (Audio e Vídeo Conferência remota), e Virtual Lab (ambiente de laboratório remoto que permite efectuar experiências e medições em instrumentos distantes), entre outras.

Das várias aplicações disponíveis, as mais interessantes para a demonstração da rede de acesso são as aplicações multimédia VOD e VidConf (ilustradas nas figuras seguintes), dado que têm requisitos específicos que deverão ser cumpridos por parte da rede.

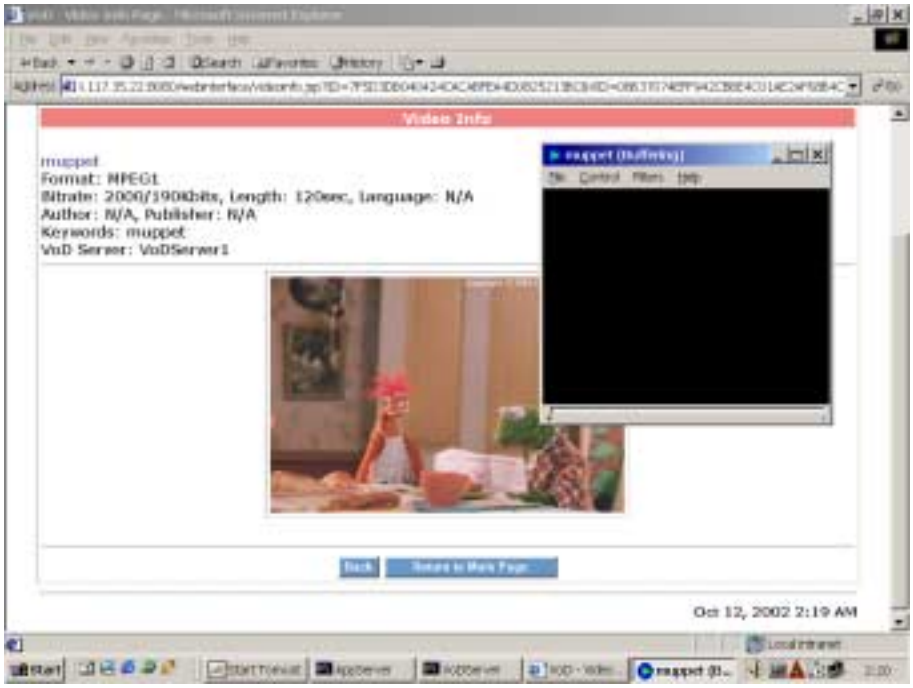


Figura 65: Cliente da Aplicação VOD desenvolvida no MOICANE

5.3.2 Testes Funcionais

Os testes funcionais vão focar os aspectos mais básicos da rede de acesso, que procuram verificar apenas se as características desejadas da rede de acesso estão presentes e correctas na rede implementada, como o TIMIP, o sMIP e o Diffserv, sem preocupações de desempenho, de tal forma a que estes testes sejam normalmente efectuados com ferramentas muito simples de teste da rede.

5.3.2.1 Conectividade IP básica

Este teste vai verificar que qualquer terminal IP fixo participante na rede de acesso, e com a configuração necessária para a rede TIMIP, vai ter conectividade proporcionada pelo TIMIP, sendo esta efectuada de acordo com as regras de encaminhamento definidas pelo TIMIP.

Para este teste vão ser utilizados dois programas simples de teste da rede: PING e TRACEROUTE, verificando o primeiro o a conectividade IP básica TIMIP, e o segundo o caminho utilizado pelo encaminhamento TIMIP. Este teste é dividido nos dois tipos de encaminhamento existentes no TIMIP: inter-domain, e intra-domain.

5.3.2.1.1 Comunicação inter-domain para um destino fixo

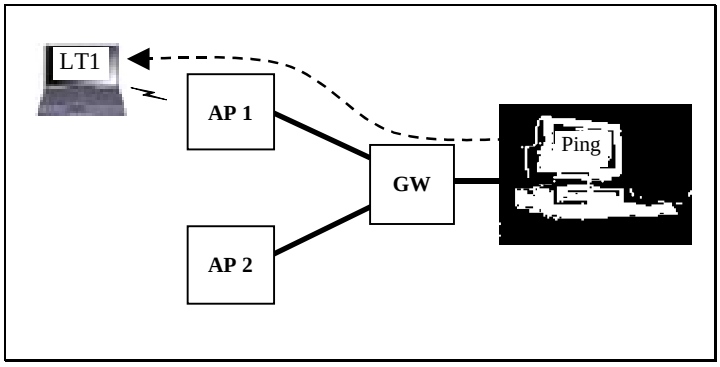


Figura 66: Teste de Comunicação inter-domain TIMIP

Este teste vai utilizar o cenário ilustrado na Figura 66, onde um terminal legado LT configurado com as características necessárias para a rede TIMIP está ligado por 802.11 ao Acess Point AP1, enquanto que um PC externo à rede está ligado à GW da rede por uma ligação ethernet de 10 Mbit/s.

Para este teste, o PC vai emitir com o programa PING pedidos de resposta ao terminal, que terão que ser respondidos correctamente por este. Adicionalmente, o PC externo vai verificar o caminho que estes pacotes levam para chegar ao terminal, usando o programa TRACEROUTE, tendo estes que seguir o caminho mais curto na árvore de nós tal como está definido no encaminhamento *downlink* do TIMIP.

Usando estes programas, verificou-se que a conectividade básica era possibilitada pelo TIMIP, por todos os pedidos ICMP ECHO REQUEST terem sido correctamente respondidos pelo terminal, verificando-se ainda que o encaminhamento *downlink* segue o caminho mais directo na árvore de nós, por terem respondido ao TRACEROUTE os nós GW, AP1 e LT (por esta ordem).

5.3.2.1.2 Comunicação intra-domain para um destino fixo

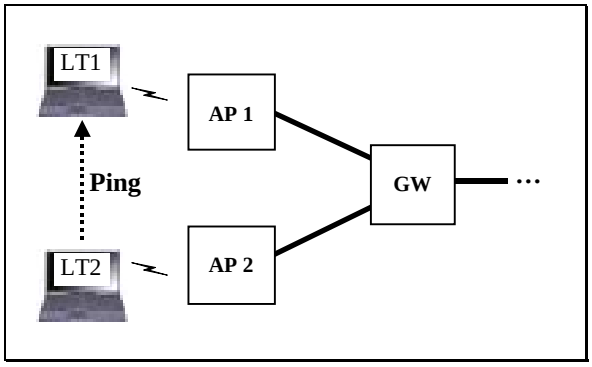


Figura 67: Teste de Comunicação intra-domain TIMIP.

Este teste vai utilizar o cenário ilustrado na Figura 67, onde agora dois terminais legados LT1 e LT2, configurados com as características necessárias para a rede TIMIP, estão ligados na rede TIMIP por 802.11 em dois Access Points separados.

Para este teste, o terminal LT2 vai comunicar com LT1, sendo esta uma situação de tráfego intra-domain TIMIP, com os mesmos objectivos de medição do teste anterior (conectividade básica com o PING e caminho utilizado com o TRACEROUTE), e espera-se neste teste que o tráfego no interior do domínio tenha as mesmas características do teste anterior.

Usando estes programas, verificou-se que a conectividade básica era possibilitada pelo TIMIP, por todos os pedidos ICMP ECHO REQUEST terem sido correctamente respondidos pelo terminal LT1; por outro lado, também se verificou que o encaminhamento intra-domain segue o caminho mais directo na árvore de nós, por em resposta ao TRACEROUTE ter respondido (por esta ordem) a o AP2, GW, AP1 e LT1.

5.3.2.2 Mobilidade TIMIP

Este teste vai verificar que qualquer terminal IP móvel participante na rede de acesso vai poder mover-se sem limitações em toda a extensão do domínio TIMIP, e ao transitar fisicamente de AP em AP, a rede sozinha vai detectar a sua movimentação e reconfigurar-se por forma a manter-lhe a conectividade de uma forma totalmente transparente.

Para este teste, à situação anterior do teste da conectividade básica, será adicionado a movimentação contínua de um dos terminais entre os dois APs da rede, medindo o outro interveniente as condições da rede depois da conclusão da operação de *handover* pelo TIMIP. De uma forma semelhante ao caso anterior, este teste foca os dois tipos de encaminhamento existentes no TIMIP, variando a localização do emissor.

5.3.2.2.1 Comunicação inter-domain para um destino móvel

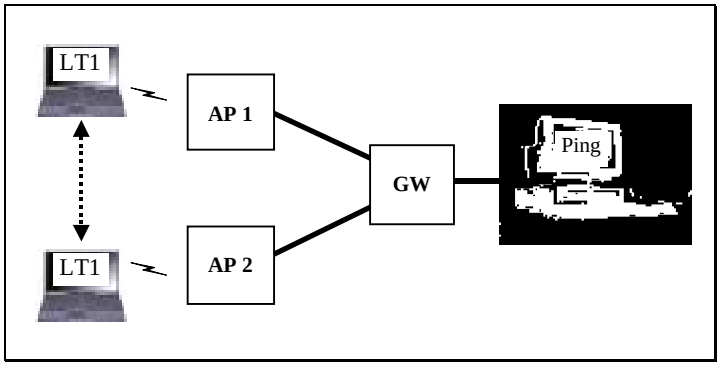


Figura 68: Teste A de mobilidade local TIMIP

Este teste vai utilizar o cenário ilustrado na Figura 68, que é a mesma situação da Figura 66 com a diferença que o terminal móvel de destino vai-se movimentar entre os dois APs, por forma a alterar a sua ligação física. Após cada transição física, o TIMIP vai efectuar um *handover* por forma a reconfigurar o encaminhamento da rede; após esta operação, o PC externo verifica as condições da rede com os programas de teste.

Usando estes programas, verificou-se que a mobilidade no interior da rede é possibilitada pelo TIMIP, por se continuarem a receber correctamente as respostas do PING após cada transição física do terminal, seguindo estas pelo caminho mais curto no interior da árvore de nós.

5.3.2.2.2 Comunicação intra-domain para um destino móvel

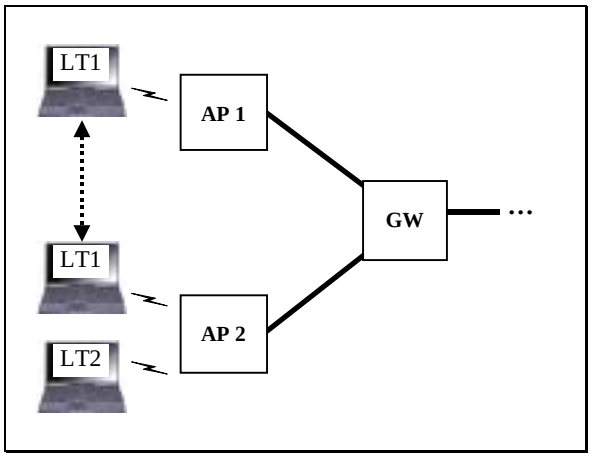


Figura 69: Teste B de mobilidade local TIMIP

Este teste vai utilizar o cenário ilustrado na Figura 67, com a diferença que o terminal móvel de destino (LT1) vai-se movimentar entre os dois APs, por forma a alterar a sua ligação física. Após cada transição física, o TIMIP vai efectuar um *handover* por forma a reconfigurar o encaminhamento da rede; após esta operação, o terminal LT1 verifica as condições da rede com os programas de teste.

Usando estes programas, verificou-se que a mobilidade no interior da rede é possibilitada pelo TIMIP, por se continuarem a receber correctamente as respostas do PING após cada transição física do terminal, seguindo estas pelo caminho mais curto no interior da árvore de nós. Note-se também que quando os dois terminais estão localizados no mesmo AP, a comunicação é efectuada pelo AP e não directamente, tal como está especificado no encaminhamento *uplink* do TIMIP.

5.3.2.3 Garantia de entrega das mensagens s de controlo TIMIP

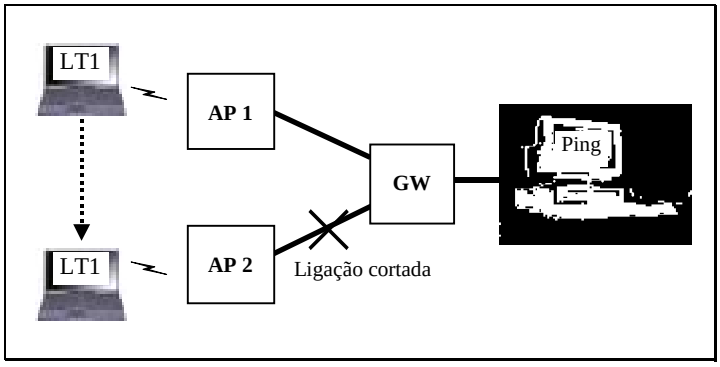


Figura 70: Teste A de mobilidade local TIMIP

Este teste vai verificar se o protocolo é robusto o suficiente para suportar a perda de mensagens de controlo TIMIP entre os nós da rede. Para tal, o terminal móvel vai-se movimentar para um AP com uma falha temporária de ligação ao backbone.

Algum tempo após o *handover* físico, a ligação será restabelecida. Durante este teste, a conectividade e encaminhamento ao terminal são avaliadas desde o exterior da rede com os programas ping e traceroute.

Usando estes programas, verificou-se que enquanto a ligação do backbone não foi reestabelecida, o terminal esteve incontactável, estando as suas entradas de encaminhamento relativas ao AP1. Depois de a ligação física ser reposta, verificou-se que a conectividade e encaminhamento foram reestabelecidas da forma correcta para a nova localização do terminal.

5.3.2.4 Conectividade/mobilidade IP em mobilidade Global

Este teste é utilizado no seguimento dos anteriores, de forma a verificar que qualquer terminal IP móvel participante de um domínio TIMIP se pode movimentar para outro distinto, mantendo a sua conectividade após esta transição, por acção do suporte sMIP. Além disso, enquanto se mantiver no domínio visitado, as suas movimentações posteriores vão ser proporcionadas pela micro-mobilidade em exclusivo, sem acções de macro-mobilidade, sendo

a conectividade efectuada de acordo com as regras de encaminhamento definidas pelo TIMIP + sMIP.

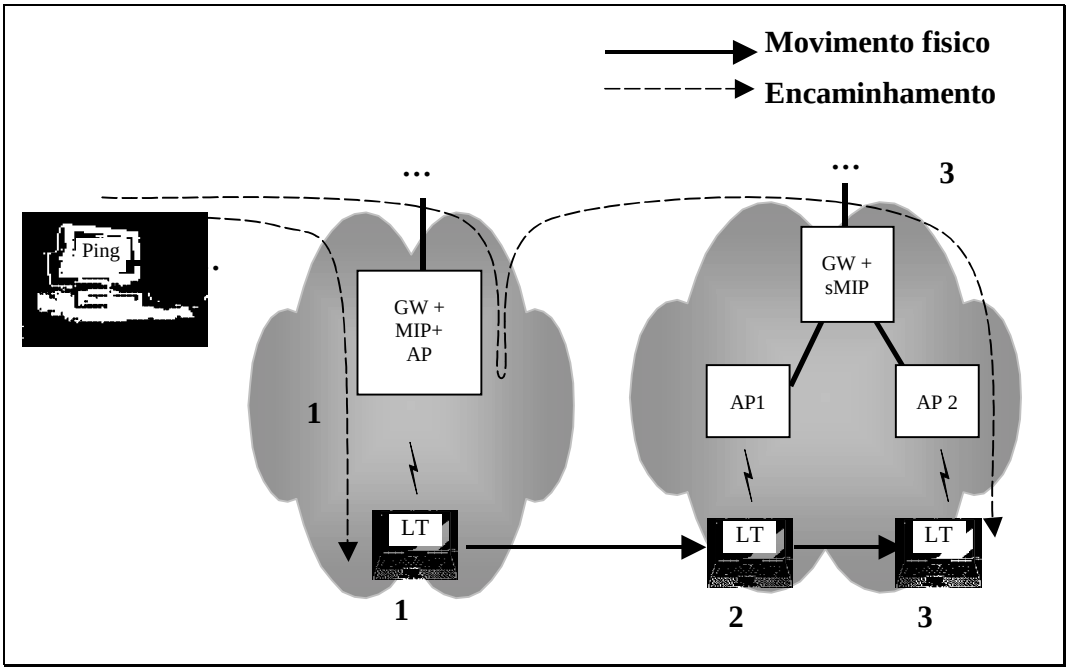


Figura 71: Teste de mobilidade global TIMIP + sMIP

Para este teste vai-se utilizar um ambiente mais complexo que os dos testes anteriores, onde o domínio TIMIP utilizado (a rede de acesso *wireless* 802.11 do MOICANE) é complementado com o segundo domínio já referido da ilha do INESC, por forma a testar a macro-mobilidade (ver Figura 71).

Para isto, o terminal legado LT vai estar de início neste domínio inicial (ponto 1), localizado no seu AP que é ao mesmo tempo GW. Nesta situação, um terminal fixo localizado fora destes domínios vai avaliar tanto a conectividade de LT, por via dos programa PING, e o encaminhamento, por via do programa TRACEROUTE.

Posteriormente, o terminal móvel vai-se movimentar para o AP1, que já pertence a outro domínio, despoletando um *power-up* TIMIP seguido de um *handover* sMIP, de forma a ficar estável na situação 2. Nesta localização, a sua conectividade será avaliada de novo.

Por último, o terminal vai-se deslocar para o AP2 do seu domínio actual (visitado), sendo apenas despoletado um *handover* TIMIP de micro-mobilidade, sem qualquer acção de macro-mobilidade envolvida, e sendo esta avaliada da forma descrita nos casos anteriores (ponto 3).

Usando estes programas, verificou-se que os dois protocolos de mobilidade vão interagir quando necessário de uma forma totalmente automática, por a conectividade ter sido reposta em todas situações.

Adicionalmente, o programa TRACEROUTE mostrou que os pacotes seguem o caminho definido para o encaminhamento TIMIP/sMIP aplicável às localizações dos terminais nas redes em questão, nomeadamente ao serem recebidos no domínio de origem, e encaminhados pelo túnel para o domínio visitado.

5.3.2.5 Testes Funcionais do Diffserv

Estes testes vão verificar as capacidades de DiffServ implementadas pela rede de acesso. Para isto, vai-se verificar as funcionalidades dos elementos constituintes da arquitectura DiffServ, nomeadamente dos filtros, marcadores, policiadores, filas e escalonadores.

A configuração utilizada para estes testes simples vai utilizar encaminhamento *inter-domain*, o que não implica nenhuma perda de generalidade (relativamente ao encaminhamento *intra-domain*). Para isto, considera-se um terminal fixo, e um PC no exterior da rede (ver Figura 72).

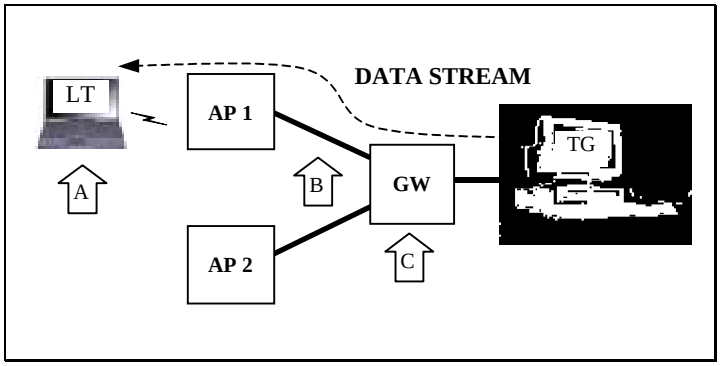


Figura 72: Testes funcionais Diffserv simples

Para cada teste, o terminal vai receber do PC externo um fluxo de dados gerado pela aplicação MGEN, composto por um *stream* contínuo UDP periódico de 2Mbit/s, constituído por 200 pacotes por segundo de 1250 *bytes* ao nível IP.

Em cada situação, a rede vai ter uma configuração estática por omissão, com valores base para os parâmetros Diffserv, conforme descrição presente [92]. Esta configuração pode ser alterada configurando os *border routers* necessários, pela manipulação dos filtros para distinguir os fluxos estabelecidos, de acordo com as características específicas do mesmo nomeadamente o seu porto UDP de destino.

Os resultados são avaliados pelas capacidades do próprio gerador de tráfego (seta A), por sondas da rede como o programa Ethereal (seta B), e por estatísticas dos encaminhadores Diffserv, utilizando o sistema de monitorização (seta C).

5.3.2.5.1 Filtragem DiffServ

Para testar o módulo de filtragem do DiffServ, a GW é programada para filtrar o trafego que é gerado, sendo este descartado propositadamente (acção *drop*), e gerados dois fluxos, um que detém das características filtradas, e outro que não. Para tal, vai-se testar variando o porto UDP, e/ou o endereço IP do destino, (ou outros campos apropriados), por forma a coincidir parcial ou totalmente com os fluxo de teste.

Aplicando esta experiência, verificou-se que quando o filtro correspondia exactamente às características do tráfego, então todos os pacotes eram bloqueados na entrada da rede, tendo como resultado por nenhum pacote ter sido recebido no receptor (seta A).

Filtragem	Inactiva	Activa
Recepção fluxo "prova"	2Mbit/s (100%)	0 Mbit/s (0%)

Tabela 5: Resultados do teste à filtragem DiffServ

5.3.2.5.2 Policiamento DiffServ

Este teste vai verificar se o tráfego individual pode ser policiado com base em SLAs estáticos pré-definidos. É usado um filtro com um débito máximo (λ) de 1Mbit/s e *burst* (b) de 10kbytes, sendo gerados fluxos de tráfego que não excedem este limite (conformantes) e que o excedem (não-conformantes). Nesta situação, é escolhida a acção de descarte para este tráfego não conformantes, sendo descartados os pacotes em excesso. Neste teste, os resultados são verificados no receptor do fluxo (seta A).

Aplicando este teste, verificou-se que acima de um dado débito de tráfego, o primeiro encaminhador só deixa passar aproximadamente os pacotes conformantes de acordo com o SLA utilizado, sendo o restante débito descartado. Estes resultados estão presentes sob a forma de gráficos na Figura 98 do Anexo 21.

Policiamento	Inactivo	Activo
Recepção fluxo "prova"	2Mbit/s (100%)	~ 1.05 Mbit/s (52%)

Tabela 6: Resultados do teste ao policiamento DiffServ

5.3.2.5.3 Marcação DiffServ

Este teste vai verificar se o tráfego classificado é correctamente marcado com o identificador da classe agregada no campo DSCP dos pacotes IP, de forma a ter o mesmo tratamento ao longo de toda a rede. Para tal, vai-se testar variando a classe em que o fluxo é classificado,

verificando a marcação no interior dos pacotes com uma sonda de tráfego imediatamente à saída da GW (seta B), e à chegada ao receptor (seta A).

Aplicando este teste, verificou-se que as marcações do Diffserv respeitaram os *codepoints* definidos nas normas (resumidas no 0), por o campo DSCP do cabeçalho IP conter os valores correctos para cada classe de serviço.

5.3.2.6 Testes Funcionais do Diffserv com Mobilidade

Estes Testes vão verificar as capacidades complementares de DiffServ que a rede detêm, relativamente aos componentes de escalonadores e filas, que necessitam de múltiplos fluxos de teste, de forma a evidenciar as capacidades de nível 3 e de nível 2 que intervém no suporte de qualidade de serviço da rede *wireless*.

Assim para estes testes, foi utilizada a configuração descrita na Figura 73, constituída por um terminal fixo LT1 que se movimenta entre os APs, um terminal fixo LT2 localizado permanentemente no AP2, e dois PCs no exterior da rede que têm ligações dedicadas independentes à GW da rede.

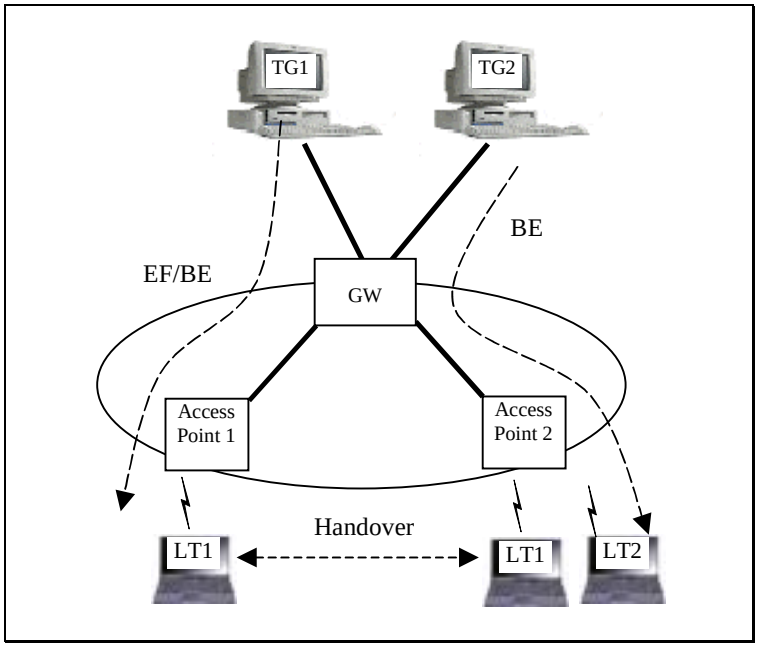


Figura 73: Testes avançados Diffserv (Prova e Carga DownStream)

Para cada teste, será estabelecido um fluxo de carga BE desde o PC fixo 2 para o terminal LT2 (ou vice versa) com o objectivo explícito de forçar a saturação da célula 802.11 do AP2. Para tal, este fluxo é composto por um *stream* contínuo UDP periódico de 2000 pacotes por segundo, sendo cada um de dimensão 48 bytes ao nível IP (o mínimo permitido pelo MGEN). Este *stream* vai constituir apenas 0.768 Mbit/s ao nível IP, pelo que será transmitido com

perdas marginais nas ligações Ethernet no backbone[71]. No entanto, por se tratar de pacotes pequenos, este fluxo será maior do que a capacidade do *wireless*, devido ao *overhead* substancial desta tecnologia de rede (conforme mostrado no teste de desempenho na secção 5.3.3.3).

Além do fluxo de carga, na rede é transmitido também um fluxo de teste destinado ao terminal móvel LT1, que emula o agregado de 3 ligações de vídeo *downstream* conformantes de ~ 4.2 Mbit/s no total[72], sendo esta constituída por pacotes 480 pacotes por segundo de 1093 bytes, e que será classificado alternadamente nas BE e EF.

A rede vai usar a sua configuração por omissão (ver [92]), à qual é aplicada uma configuração estática dos filtros necessários para classificar o fluxo de prova na classe desejada. Os resultados são avaliados nos receptores do tráfego, que podem ou não receber a totalidade do tráfego gerado no emissor.

5.3.2.6.1 Fluxos "prova" e "carga" BE downstream

O primeiro teste vai analisar a rede nas condições iniciais, sendo este semelhante à Internet clássica, em que ambos os fluxos estão em igualdade de circunstâncias por serem classificados na classe BE. O terminal que recebe o fluxo de prova movimenta-se alternadamente nos dois APs, e quando estiver localizado no AP2 vai sofrer perdas, dado que o backbone da rede de acesso está sempre saturado com o tráfego de enchimento, e o tráfego de prova não ter garantias de serviço por parte da rede.

Localização	AP1	AP2
Recepção fluxo "prova" BE	4.1979 Mbit/s	0.5821 Mbit/s

Tabela 7: Resultados fluxos "prova" e "carga" BE downstream

5.3.2.6.2 Fluxo "prova" EF downstream e "carga" BE downstream

Este teste vai ser igual ao anterior com a diferença de que agora o tráfego do fluxo de teste é marcado com a classe de serviço EF, sendo o tráfego classificado à entrada da rede na GW

[71] Dado que o *overhead* introduzido pelos níveis 1 e 2 da tecnologia Ethernet é reduzido, o valor final de utilização do fluxo no meio físico fica assim muito abaixo do máximo 10Mbit/s.

[72] o vídeo emulado será o "muppet.mpg", codificado em CBR MPEG1, e que será utilizado no teste final de QoS na secção 5.3.2.7.

para esta classe. Nestas condições, a rede vai sempre respeitar os requisitos do tráfego EF, passando este à frente do tráfego BE quando LT1 está localizado no AP2, o que significa que este tráfego prioritário é recebido na sua totalidade no receptor.

Localização	AP1	AP2
Recepção fluxo "prova" EF	4.1979 Mbit/s	4.1879 Mbit/s

Tabela 8: Resultados fluxo "prova" EF downstream e "carga" BE downstream

5.3.2.6.3 Fluxo "prova" EF downstream e fluxo "carga" BE upstream

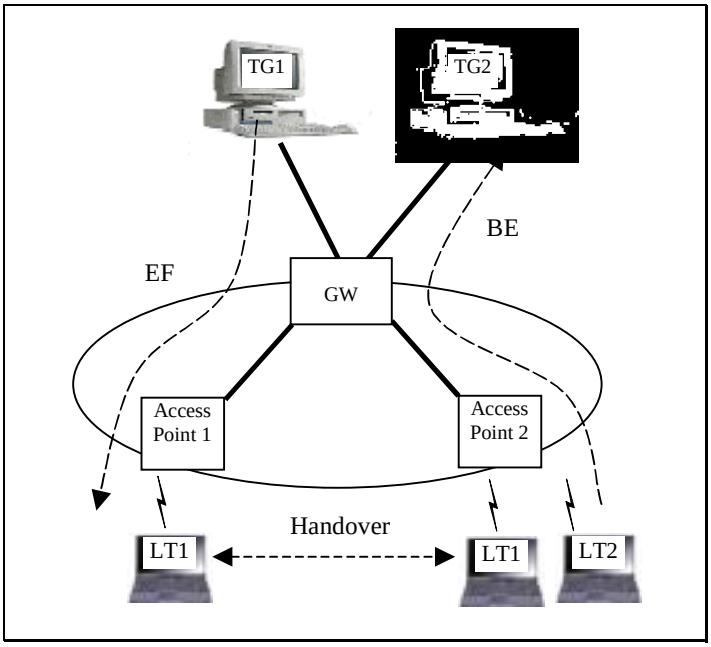


Figura 74: Testes avançados Diffserv (prova DownStream, carga Upstream)

Este teste vai ser igual ao anterior com a importante diferença que agora o tráfego de carga é gerado no sentido *uplink*, desde o terminal LT2 para o receptor TG2 (ver Figura 74).

Localização	AP1	AP2
Recepção fluxo "prova" EF	4.1979 Mbit/s	3.4079 Mbit/s

Tabela 9: Resultados fluxo "prova" EF downstream e fluxo "carga" BE upstream

Nesta situação, só vai existir tratamento de QoS *desde o primeiro* encaminhador do tráfego da carga – o AP2 – uma vez que o acesso ao meio partilhado não tem qualquer suporte de QoS de nível 2. Assim, usando apenas a tecnologia de QoS IP na rede de acesso, as diferentes classes vão competir em igualdade de circunstâncias no acesso ao meio (uma vez que com o DCF todas as estações são iguais entre si), o que resulta na garantia do tráfego EF *até* ao AP2,

e não até ao destino LT1. Esta situação é verificada pela recepção do tráfego de "prova" no nó AP2, onde está presente na sua totalidade.

No entanto, esta é uma situação que acontece *sempre* que se satura um meio partilhado sem suporte de qualidade de serviço de nível 2. Por esta mesma razão, os geradores fixos de tráfego são separados em dois meios físicos distintos Ethernet, porque se esse cuidado não existisse, então era despoletado exactamente o mesmo problema, tal como está ilustrado na Figura 75.

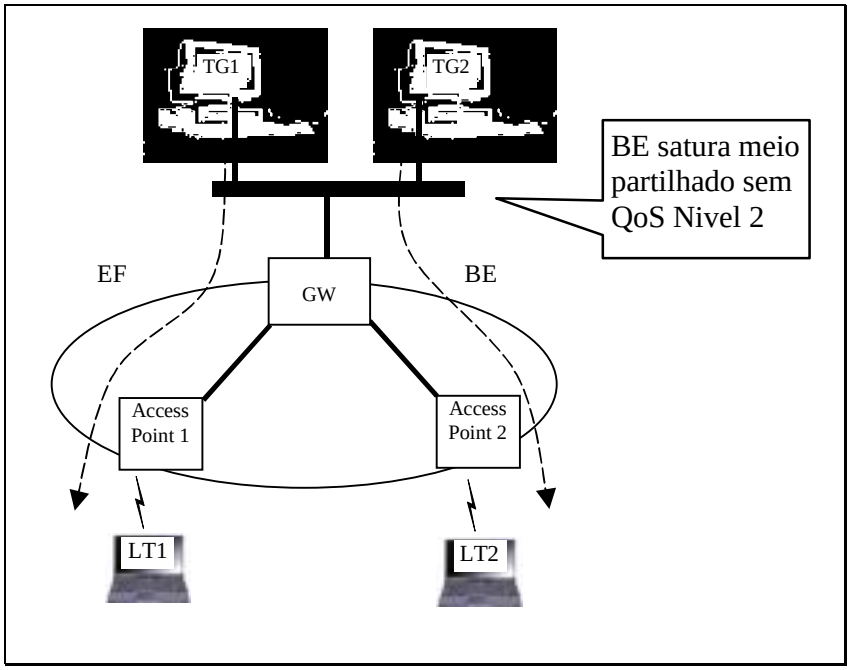


Figura 75: Meios partilhados sem suporte de QoS de Nível 2

5.3.2.7 Teste de QoS e mobilidade com aplicações multimédia

Este último teste é semelhante ao anterior, com a distinção de se utilizar a aplicação de *e-learning* desenvolvida no projecto MOICANE – a aplicação VOD – usando o vídeo (muppet.mpg) simulado na experiência anterior. Esta aplicação tem requisitos muito restritivos em relação à entregas dos pacotes de dados, exigindo da rede capacidades de resposta elevadas sob pena de má qualidade do vídeo visualizado, pelo que é a aplicação de teste ideal para avaliar as componentes de serviço de DiffServ estático da rede, conjugada com a mobilidade para terminais legados.

Aplicando este teste verifica-se cabalmente os resultados das tecnologias referidas, dado o vídeo possuir muito má qualidade quando é recebido sem reservas no AP carregado, e com qualidade perfeita nos outros casos. Por outro lado, o teste também evidencia subjectivamente a latência das acções de mobilidade, pois a perda de pacotes de dados devidos à mudança de

AP ou domínio resultar no aparecimento de artefactos visuais relacionados com o algoritmo de compressão.

Os resultados deste teste incluem gráficos recolhidos nos encaminhadores da rede, detalhados Anexo 21, e mostram uma relação directa entre os eventos efectuados (movimentação entre os APs, presença de carga, utilização de QoS) e os resultados obtidos.

5.3.3 Testes de Desempenho

Os testes de desempenho vão focar aspectos presentes na rede de acesso que os testes funcionais já provaram a sua correcta execução, mas que, por incluírem aspectos especiais na sua arquitectura e/ou optimizações concretas na sua implementação, este testes vão medir com rigor as operações despoletadas, de forma a avaliar a qualidade final da solução desenhada e implementada.

5.3.3.1 Velocidade do handover TIMIP

Este teste vai verificar qual é o peso da adição da micro-mobilidade TIMIP aos domínios IP, sendo este comparado com a utilização apenas da mobilidade proporcionada pelo nível 2.

Para isso, vai-se usar a mesma configuração da rede já testada nos testes funcionais, mas agora utilizando o gerador de tráfego MGEN ao invés do programa PING. Neste sentido, o gerador de tráfego emite um fluxo constante periódico de pacotes UDP numerados com o período de 1 milisegundo.

Estes pacotes são destinados a um terminal móvel, que recolhe e grava o fluxo para ficheiro, e que se movimenta alternadamente entre os dois APs; e por outro lado, estes verificam o tempo em que recebem o pacote de gestão de *associate* do 802.11, guardando esta informação em ficheiro[73], sendo assim possível analisar o instante de tempo em que a ligação de nível 2 é reestabelecida pelo 802.11b.

Note-se que a rede de acesso já exige que os APs da rede estejam sincronizados entre si; adicionalmente, para este teste particular, também o relógio do terminal terá que estar sincronizado com o dos APs, de forma a possibilitar as comparações das medições efectuadas.

[73] Para máxima precisão, é marcado o tempo no *driver* assim que o *interrupt* do pacote de *associate* é disparado.

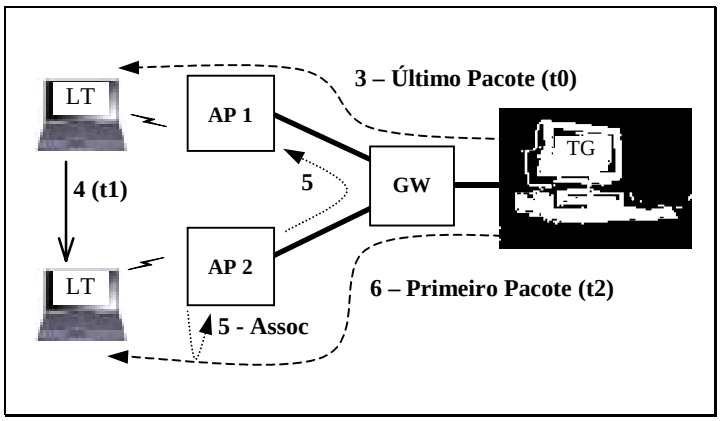


Figura 76: Detalhe do handover para teste da velocidade TIMIP

Neste sentido, a movimentação do terminal é decomposta da seguinte forma (ver Figura 76):

1. LT1 está associado ao AP1, e está a receber o tráfego gerado em TG.
2. LT1 movimenta-se de forma a aproximar-se da célula do AP2, ao mesmo tempo que se afasta do AP1
3. LT1 recebe o último pacote UDP pelo AP1, antes de perder a conectividade física **– Tempo T0**
4. LT1 executa o *handover* do nível 2, que termina assim que o pacote 802.11 de *associate* é recebido no AP2 **– Tempo T1**
5. O nível 2 do AP avisa o nível 3 da chegada do novo terminal móvel, que inicia a reconfiguração da rede, bastando que o AP2 e a GW alterem o seu encaminhamento para a nova localização do terminal.
6. LT1 recebe o primeiro pacote UDP entregue pelo AP2 **– Tempo T2**

Comparando os valores de **T0, T1** e **T2**, é possível extrair o tempo total do *handover* (T2 - T0), a componente relativa do TIMIP (T2 - T1), e a componente relativa do nível 2 (T1 - T0) (ver Anexo 17Anexo 17). Teoricamente, a parte do TIMIP deverá ser muito menor que a parte do nível 2, dado que a acção de detecção é totalmente reactiva, e a fase de registo está optimizada para efectuar *handovers* locais ao terminal, e no pior caso nunca além do interior do domínio TIMIP.

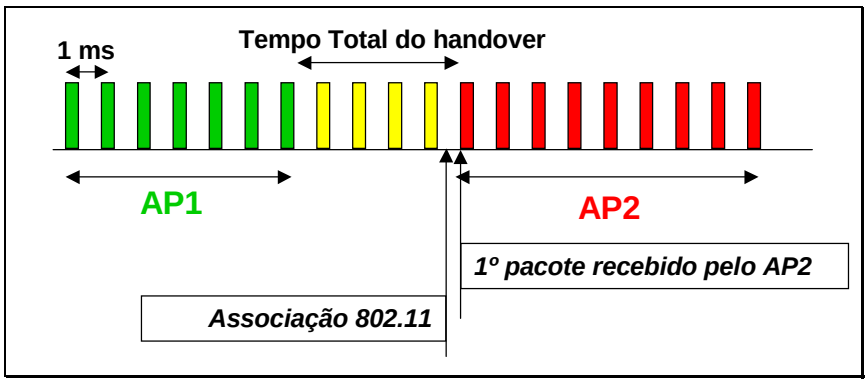


Figura 77: Detalhe do teste da velocidade do handover TIMIP

Executando o teste as vezes necessárias para um alto grau de confiança, verificou-se que o TIMIP demora em média **2ms** a transitar (0,224ms desvio padrão), enquanto que o 802.11 demora **101.06ms** a transitar (25,650ms desvio padrão). Os dados completos estão presentes no Anexo 17, incluindo um exemplo da forma de medição.

Analisando estes resultados, verifica-se então que em condições óptimas, a mobilidade TIMIP demorou em média 1ms por cada nível da árvore de nós necessário para concretizar o *handover*.

Uma vez que o TIMIP optimiza o registo (local), então os *handover*s são sempre limitados à parte da árvore dos APs envolvidos; uma vez que normalmente estes estarão localizados perto um do outro, então a parte envolvida da árvore será pequena, que se reflecte em poucos níveis da árvore (na maioria das movimentações).

Mesmo no pior caso, em que o registo tem que percorrer toda a árvore desde o AP até à GW, o peso do *handover* TIMIP será sempre (em condições óptimas) bastante menor que o tempo necessário na transição do 802.11, sendo assim totalmente despercebido em comparação com este.

Realce-se que a grande diferença é que o TIMIP permite a mobilidade optimizada ao longo de domínios inteiros, comparada com o interior de LANs no *handover* de nivel2 do 802.11, o que complementado com outras tecnologias IP mostra a sua abrangência superior.

5.3.3.2 Velocidade dos handovers em mobilidade Global

Este teste vai verificar qual é o peso da adição da micro-mobilidade TIMIP, conjugada agora com a macro-mobilidade sMIP aos domínios IP, o que permite a mobilidade global ao longo de toda a Internet. Neste sentido, este teste vai se basear no teste funcional já efectuado de mobilidade global (ver secção 5.3.2.4, na página 158), mas medido da forma rigorosa especificada no teste de desempenho da micro-mobilidade (ver teste anterior). Neste teste,

ilustrado na Figura 78, um terminal LT vai-se movimentar entre 3 APs que lhe estão acessíveis, de forma a efectuar movimentos entre o seu domínio de origem e um domínio visitado (movimentos 1 e 4), e no interior do domínio visitado entre os seus APs (movimentos 2 e 3).

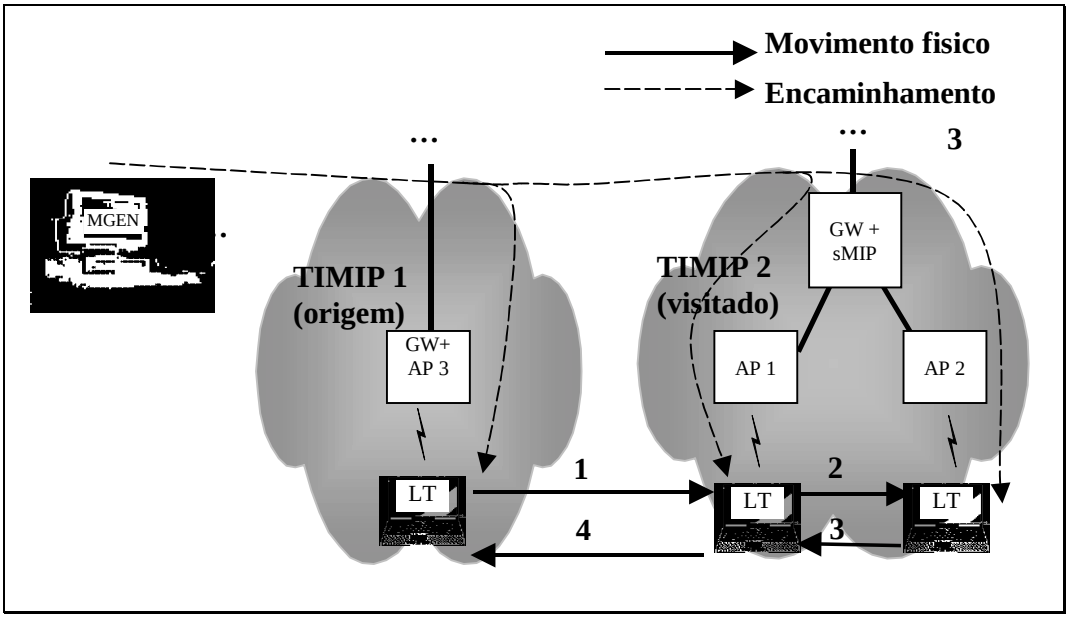


Figura 78: Teste de performance de mobilidade global TIMIP + sMIP

O ponto chave que este teste evidencia é a total independência dos dois tipos de mobilidade, dado que os movimentos 2 e 3 no domínio visitado vão ser instanciados apenas com o recurso à micro-mobilidade, independentemente da distância do terminal até ao domínio de origem, e assim com durações em tudo semelhantes às já encontradas no teste anterior, dado que as alterações a efectuar serem sempre locais limitadas ao domínio visitado.

Por outro lado, as movimentações 1 e 4 entre os domínios terão previsivelmente uma latência apreciável da ordem dos segundos, uma vez que (propositadamente) o processamento das acções de macro-mobilidade não têm qualquer optimização ou preocupação relativas ao seu desempenho (rapidez), conjugado com atrasos impostos pelo protocolo MIP.

Efectuando-se este teste, verificou-se os resultados sumariados na Tabela 10, obtidos com base em medições presentes no Anexo 18.

TIPO	de	para	Mobilidade:	Descrição	Latência
1	AP3	AP2	Macro+Micro	entrada num domínio visitado	3117 ms
2	AP2	AP1	Micro	movimentação em domínio visitado	3 ms
3	AP2	AP2	Micro	movimentação em domínio visitado	2 ms
4	AP2	AP3	Macro+Micro	retorno ao domínio de origem	5 ms

Tabela 10: resultados teste sMIP+TIMIP

Nestes, é notória a diferença substancial entre o tempo necessário para restabelecer a conectividade entre a movimentação entre domínios, e no interior do domínio. Tal como foi previsto, as movimentações do tipo 1 só são finalizadas segundos depois de terem sido iniciadas, pois envolvem macro-mobilidade; por outro lado, as movimentações do tipo 2 e 3 são totalmente semelhantes às do teste anterior, com a diferença que operam num domínio visitado, sendo suficientes para provar a independência entre os dois tipos de mobilidade.

Por fim, as movimentações do tipo 4, relativas ao retorno dos terminais aos seus domínios de origem poderá parecer surpreendente, por embora envolver acções de macro-mobilidade, está na mesma ordem de grandeza dos movimentos de micro-mobilidade (embora ligeiramente superior). Este comportamento é explicado por optimizações explicitas na implementação do sMIP, dado que a acção de retorno dos terminais apenas terá que remover o túnel criado, não necessitando de qualquer troca de sinalização entre domínios. Outro factor que contribui para este valor é a optimização do sMIP possuir uma forma de detecção reactiva (despoletada pelo TIMIP que detém também de detecção reactiva despoletada pelo 802.11), que reduz esta fase a um valor marginal.[74]

5.3.3.3 Débito oferecido pelo 802.11b

Este teste vai verificar qual é o débito máximo atingido em condições óptimas pelo 802.11b num fluxo simples *downlink*. Tal como foi analisado na descrição teórica, o 802.11b tem *overheads* muito pronunciados no nível 2 (como o *acknowledge*) e no nível 1 (*multi-rate*), que baixam significativamente o débito alcançado quando se utilizam pacotes pequenos no nível 3.

Para isto, vai ser testado com um fluxo constante de 11 Mbit/s ao nível IP, constituído por diversas combinações de tamanho do MTU do nível 2 *vs* número de pacotes por segundo

[74] ver descrição sobre a fase de detecção do sMIP, (secção 3.2.3.1, na página 83).

emitidos, por forma a gerar o débito considerado. Estes fluxos são medidos durante largos períodos de tempo, desde o emissor MGEN localizado no AP, ao receptor DREC localizado no terminal, sendo no final analisadas as estatísticas da transmissão

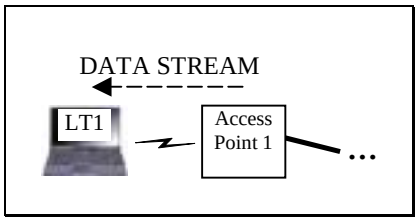


Figura 79: Teste de medição do débito máximo do 802.11b

Executando o teste, verificou-se que o débito atingido varia bastante com o tamanho dos pacotes, variando desde um máximo de **0.404 Mbit/s** para pacotes pequenos de **48 bytes IP**, e um máximo de **5.5 Mbit/s** para pacotes de **1500 bytes IP**. Os resultados estão resumidos no gráfico abaixo e os dados completos presentes no Anexo 19.

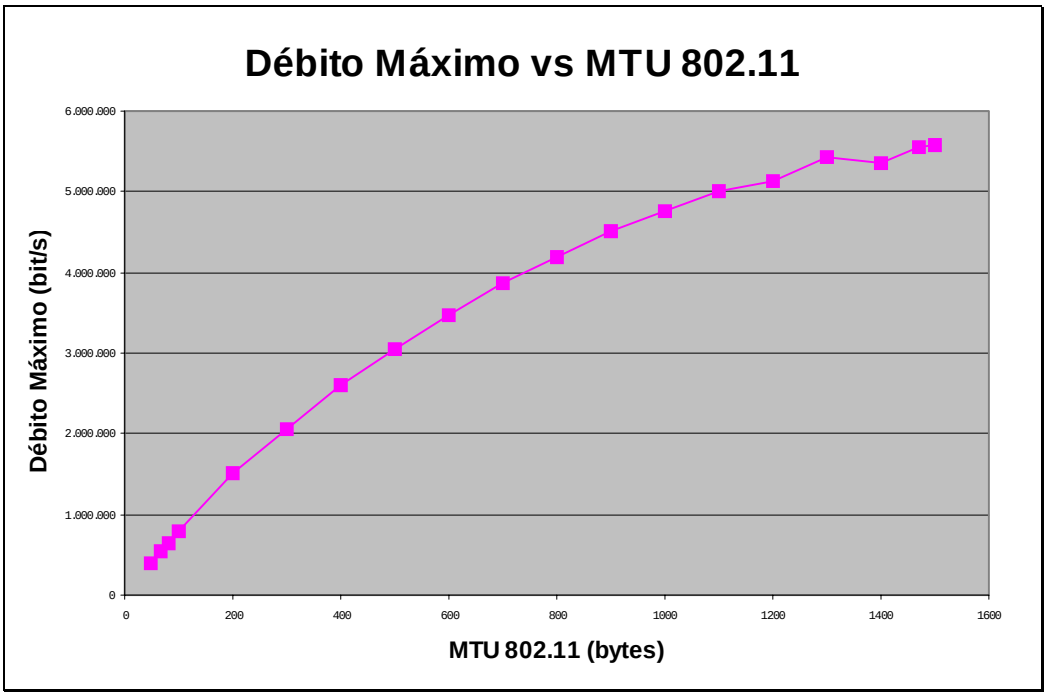


Figura 80: Resultados do Débito oferecido pelo 802.11b

Note-se que estes resultados estão em conformidade com estudos teóricos, e mostram que esta tecnologia oferece débitos bastante mais baixos que os anunciados pelos fabricantes (11 Mbit/s).

5.3.3.4 Teste de atraso da classe EF

Este teste vai avaliar o desempenho da classe EF na rede de acesso. Tal como está normalizada, esta classe define que terá que existir um limite máximo para o atraso dos

pacotes respectivos, o que terá que ser respeitado mesmo quando esta classe coexistir com outras classes de tráfego menos prioritárias. Acresce ainda que a utilização de *software* para concretizar o suporte de QoS também vai introduzir um peso, que se pode reflectir neste requisito do EF.

Deste modo, vai ser verificado o valor do atraso máximo da classe EF quando esta compete com outras classes, e o valor do mesmo quando está sozinha, medindo assim o peso mínimo desta implementação do DiffServ. Para referência, ambos os valores são comparados com o valor do atraso nominal, em que não existem mecanismos de QoS no caminho dos pacotes IP na rede.

Para isto vai ser utilizada uma configuração (ver Figura 81), constituída por dois terminais fixos LT1 e LT2, localizados permanentemente no AP2, e dois PCs no exterior da rede que têm ligações dedicadas independentes à GW da rede, estando os relógios destes elementos sincronizados entre si.

Para este teste, o terminal móvel 1 vai receber um fluxo de teste emitido pelo PC1 e classificado na rede como tráfego prioritário EF, de forma a avaliar o atraso necessário no percurso dos pacotes EF nesta rede, e o segundo PC vai gerar um fluxo de carga BE, com as mesmas características dos anteriormente utilizadas, sendo recebido pelo terminal LT2. [75]

[75] Outra forma de realizar esta experiência seria a de utilizar o programa **ping** para verificar o tempo de ida e volta entre os nós em questão, dado que aí a fonte de relógio seria a mesma (apenas o relógio do emissor). No entanto, esta experiência não pode ser testada de uma forma fiável, dado que os pacotes de respostas teriam que competir com o fluxo BE para aceder ao meio, (dado não existir suporte de QoS de nível 2 o 802.11).

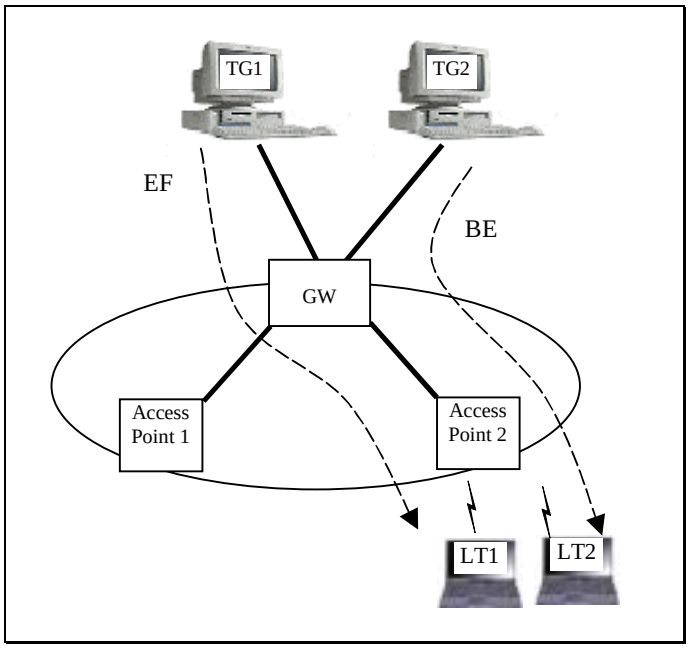


Figura 81: Testes de atraso do EF

Nestas condições vai ser medidos os seguintes atrasos na propagação dos pacotes:

a) fluxo EF sem carga BE, sem os mecanismos de DiffServ activos

b) fluxo EF sem carga BE, com os mecanismos de DiffServ activos

c) fluxo EF com carga BE, com os mecanismos de DiffServ activos

Estas medições estão resumidas na tabela seguinte:

teste	QoS Activo?	Carga BE?	Pacotes Gerados	Pacotes Recebidos	Latência Média	Latência Mínima	Latência Máxima
a)	Não	Não	1000	1000	1 ms	0 ms	10 ms
b)	Sim	Não	1000	1000	1 ms	0 ms	10 ms
c)	Sim	Sim	1000	1000	6 ms	1 ms	10 ms

Tabela 11: Teste de desempenho da classe EF

Destes resultados, pode-se verificar que todos os valores estão na mesma ordem de grandeza, sendo assim os diferentes cenários em teste interpretados como semelhantes para os utilizadores da rede de acesso.

Comparando os resultados a) e b), verifica-se que a adição do *software* de Diffserv à rede de acesso incorre um *overhead* mínimo em todas as situações, mas que é tão pequeno que não consegue ser detectado com o mecanismo criado, dado que o processo de sincronização dos

relógios apenas garante uma margem de erro de 1ms, e por o MGEN ter uma precisão limitada no acesso ao relógio (também com um erro mínimo de 1ms).

Esta medição mostra contudo, que a estrutura de controlo de tráfego DiffServ presente no caminho crítico do *forwarding* dos pacotes de dados é escalável, principalmente por estar implementada em exclusivo no interior do *kernel* do Linux.

A segunda comparação entre os resultados b) e c) mostra que o tráfego EF sofre em média um aumento na sua latência de transmissão quando existem classes menos prioritárias a competir para a transmissão pela interface. Contudo, este aumento mantém o valor médio da latência na mesma ordem de grandeza, de tal forma a que os requisitos apertados dos SLAs associadas aos fluxos EF continuam a serem cumpridos, mesmo no pior caso.

6. Conclusões

Este trabalho propôs-se a definir e propor uma solução de mobilidade IP aplicável a qualquer terminal. Este objectivo foi formulado pela constatação que, mesmo após alguns anos depois do aparecimento da tecnologia, de os seus problemas iniciais terem sido resolvidos, e de aparecerem propostas de extensões de optimizações, esta tecnologia continuar a ter uma grande resistência em se generalizar, especialmente se a compararmos com os serviços semelhantes, altamente bem sucedidos, existentes nas redes móveis públicas de voz (telemóveis).

Segundo esta Tese, esta falta de generalização não se deve a problemas da tecnologia em si, nem da falta de aplicabilidade dos novos serviços possibilitados, mas pelo facto que a introdução de novos serviços *de rede* na Internet exige tanto a alteração da *própria rede*, como a alteração dos *terminais* que beneficiam desta tecnologia, sendo este derivado da forma como a inteligência está distribuída no nível de rede na Internet.

Neste sentido, procurou-se uma solução que respondesse directamente a este problema, mas que aproveitasse o trabalho anterior já realizado. Para isto, analisou-se o enquadramento do problema e os esforços anteriores, que embora não tenham endereçado este problema específico, sugeriram pistas para a melhor alternativa a aplicar.

Daqui considerou-se que a melhor alternativa seria um mecanismo em dois níveis, para responder separadamente às várias escalas de mobilidade, nos quais se conjugasse a característica desejada com as melhores das propostas já existentes.

Este trabalho resultou no protocolo TIMIP, submetido para apreciação no organismo competente (IETF), e no seu complementar sMIP, que juntos suportam a mobilidade global de qualquer terminal IP.

O primeiro consiste num novo protocolo de micro-mobilidade alternativo aos já existentes, com a característica chave pretendida, bem como de detecção optimizada (reactiva), registo local (hierárquico), encaminhamento optimizado (*intra-domain*) e manutenção do estado optimizada (sem *overhead* para terminais activos).

O segundo consiste numa adaptação do standard de mobilidade MIP com a inclusão da característica chave pretendida, usada agora para a função exclusiva de macro-mobilidade (relegando a micro-mobilidade no protocolo especializado). Além disto, o sMIP também

herda do TIMIP as características de detecção optimizada (reactiva entre os protocolos), e manutenção do estado optimizada (sem *overhead* utilizando os pacotes de dados).

Relativamente à contribuição referida, publicada em Março de 2002 no IETF como *draft* individual, esta foi, por ter sido escrita em inglês, importante para difundir o novo protocolo de mobilidade proposto e a sua nova aproximação, colocando esta solução de mobilidade a par das já existentes.

De notar que esta versão inicial do *draft* será seguida por uma descrição mais detalhada, já incluindo correcções e outras funcionalidades não descritas na versão inicial, e que será submetido em Janeiro de 2003[76].

Além do estudo teórico da solução proposta, esta foi implementada numa rede de acesso *wireless* 802.11b, que detém de características chave para a demonstração desta tecnologia, pois proporciona um ambiente móvel sem fios e de alto débito ideal para uma *nova* classe de aplicações, que estão ainda bastante inexploradas.

Por esta rede estar integrada no contexto do projecto MOICANE, este trabalho também teve muito a ganhar, dado por este projecto de Qualidade de Serviço considerar algumas destas novas aplicações referidas, que permitiram testar e demonstrar a solução de mobilidade com situações totalmente reais. Estes testes práticos foram complementados com testes funcionais e de desempenho mais rigorosos e profundos, que confirmado totalmente a execuibilidade dos conceitos propostos, bem como da qualidade da implementação realizada.

Tal como todos os trabalhos de investigação, este não se dá por concluído, requerendo ainda o desenvolvimento de algumas características ou funcionalidades que ainda não respondem satisfatoriamente às requeridas pelas novas aplicações IP, bem como a implementação prática de algumas funcionalidades que, nesta primeira fase, apenas foram estudadas teoricamente.

Entre outras, saliente-se a introdução de novas funcionalidades já presentes noutros protocolos de mobilidade, como o *paging*, o *bicasting* ou a robustez melhorada do protocolo, bem como da implementação das extensões DHCP e da componente de segurança do TIMIP. Noutro plano, existem ainda outras funcionalidades que poderão ser adicionadas ao TIMIP

[76] Previsão

relacionadas com a *integração* desta tecnologias com outras IP, como o suporte de QoS, a transição de contexto dos terminais na rede, ou o encaminhamento Multicast, podendo a solução proposta crescer com extensões adicionais.

Contudo, pese embora estas ultimas constatações, saliente-se que o trabalho apresentado define uma arquitectura completa para o suporte de mobilidade IP de qualquer terminal, o que lhe abre substancialmente o espectro relativamente às propostas anteriores apresentadas, podendo indicar um possível caminho para a generalização e evolução do suporte de mobilidade IP na Internet.

Apêndices

Anexo 1 Comparação dos Tipos de Mobilidade

Soluções IETF

Movimentação Topológica		Entre APs	Dentro da Rede	Dentro do Domínio	Entre Domínios	Global
Exemplo Geográfico (nota1)		Andar	Edifício	Campus	Cidade	Continente
Distância Típica (nota1)		2 m	100m	1km	5 km	1000km
	TIPO mobilidade IP					
MIP	Macro				+	✓
hMIP	"Meso"			✓	✓	+
HAWAII	Micro	+	✓	+		
CIP	Micro	+	✓	+		
TIMIP+sMIP	Micro +Macro	+	✓	+	+	✓

Outras Soluções

IAPP	Nível 2	✓	+			
CIP+MIP	Micro +macro	+	✓	+	+	✓

Legenda:

✓	Melhor aplicação do protocolo
+	Boa aplicação do protocolo
	Má aplicação do protocolo

nota1: Os exemplos geográficos e as distâncias típicas apresentadas são meramente exemplificavas dos casos mais comuns de aplicação dos protocolos de mobilidade.

Anexo 2 Características da solução de mobilidade global

Acções	Características	
	Terminais Legados	Eficiente
Detecção	Automática	De tipo Reactivo
Reconfiguração	Elementos rede Activos	Local/Hierárquica

Terminais Legados => Detecção Automática; reconfiguração activa

Eficiente => Detecção Reactiva; reconfiguração Hierárquica, divida em micro e macro-mobilidade

Anexo 3 Tipos de Elementos em Protocolos de Mobilidade

	Tipo de Elemento		
	Activo	**Passivo**	**Reactivo**
MIP	MH	FA	HA
HAWAII	MH	**-**	Todos os Nós CIP
CIP	MH	**-**	Todos os Nós CIP
TIMIP	AP do Terminal Legado	**-**	Todos os Nós TIMIP
sMIP	Agente de Mobilidade Visitado	**-**	HA

	Tipo de Elemento		
	Activo	**Passivo**	**Reactivo**
MIP, CIP, etc.	**terminal**	rede	rede
TIMIP	rede	**rede**	rede
sMIP	rede	**rede**	rede

	Tipo de Elemento		
	Activo	**Passivo**	**Reactivo**
mobilidade IP actual	**terminal**	rede	rede
Hipótese da tese	**rede**	rede	rede

Anexo 4 Formatos e tipos de mensagens TIMIP

As mensagens utilizadas para a sinalização do TIMIP são encapsuladas no protocolo de controlo ICMP, e são utilizadas em exclusivo entre os nós adjacentes no interior do domínio. Actualmente, existem apenas duas mensagens definidas: Update e Update_Ack. As mensagens têm a seguinte estrutura genérica:

```
0                   1                   2                   3
01234567890123456789012345678901
```

Versão	IH Len	DSCP/Priority	Total Len
ID		Flags	
TTL		Protocol	Header Checksum
Source IP Address			
Destination IP Address			
ICMP_type		ICMP_code	ICMP_Checksum
Legacy Terminal IP			
Association Time NTP (LOW)			
Association Time NTP (HIGH)			

A descrição detalhada de cada campo está presente na seguinte tabela:

	campo	valor	descrição/notas
IP	proto	1	identificador do protocolo ICMP
	src	endereço IP do nó da rede emissor	nas mensagens de update e update ack, indicam a o próximo nó para o terminal legado IP_LT
	dest	endereço IP do nó da rede receptor	indica o endereço IP de um nó adjacente do nó emissor
ICMP	type	200	identificador do protocolo TIMIP
	code	1 ou 2	operação TIMIP a efectuar: 1 update; 2 update_ack
	checksum		operação de checksum simples no header ICMP
TIMIP	LT_IP	endereço IP do terminal legado	identificador do terminal
	Assoc_Time	Tempo da detecção do terminal	campo formatado em NTP (32 bits para segundos) + 32 bits para microsegundos) com o tempo NTP da detecção do terminal no AP

Anexo 5 Configuração especial dos terminais legados

Os terminais são configurados como se tivessem uma ligação ponto-a-ponto permanente para a GW da sua rede local, sendo este papel transparentemente realizado pelo AP actual do terminal móvel, com proxy ARP.

Os terminais são configurados com a seguinte configuração especial de rede, o que pode ser efectuado tanto manualmente, ou automaticamente por DHCP:

Item	valor	observações
Endereço IP	X.Y.Z.W	permanente, ou alocado por DHCP
Máscara de rede	255.255.255.255	Máscara Fechada
GW	GW da rede TIMIP ou 1.1.1.1	A segunda opção é a GW universal para todos os domínios TIMIP+sMIP

Tabela 12: Configuração especial dos clientes das redes TIMIP

Com esta configuração, e por via dos mecanismos proxy/gratuitous ARP efectuados pelos APs, o terminal tem a seguinte visão da sua conectividade:

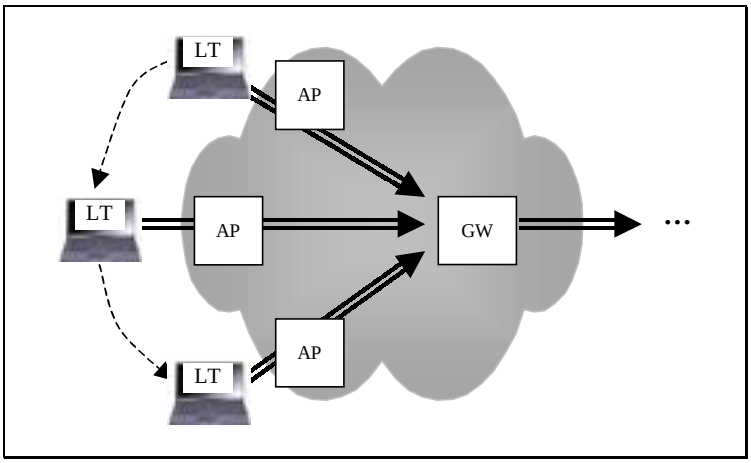


Figura 82: ligação P2P lógica para a GW da rede

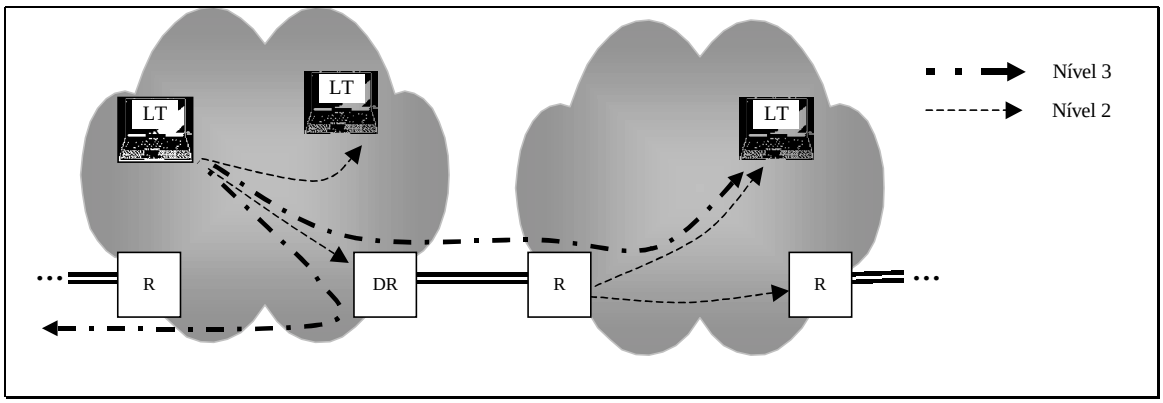


Figura 83: Detalhe encaminhamento (modelo clássico) do ponto de vista do terminal

Anexo 6 Detalhe do handover dos terminais

A figura seguinte vai detalhar as acções que são utilizadas para efectuar um handover, incluindo os acknowledges das mensagens e o update da *cache* ARP do cliente, e a ordem destas.

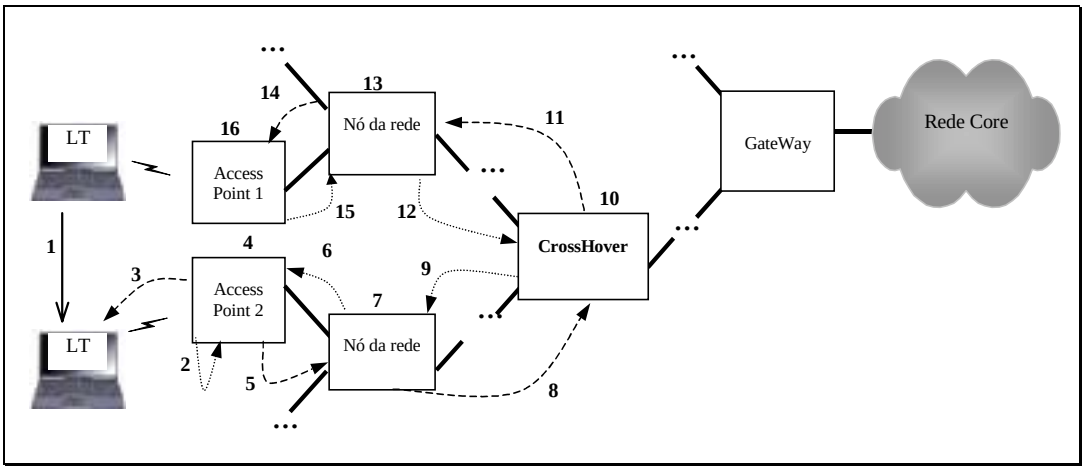


Figura 84: Handover do TIMIP (Detalhe)

Passo	Acções
1	Movimento Físico
2	Notificação Detecção (Passivo ou Reactivo)
3	Gratuitous ARP
4, 7	Cria Entrada Encaminhamento
5, 8, 11, 14	TIMIP Update
6, 9, 12, 15	TIMIP Update ACK
10	Altera Entrada Encaminhamento
13, 16	Remove Entrada Encaminhamento

Anexo 7 Detalhe do problema da inconsistência da rede

Esta nota é referente a um exemplo das potenciais inconsistência da rede que motivam a sincronização dos APs entre si (ver secção 3.1.4.2). A figura seguinte mostra a inconsistência, e a figura seguinte as acções adicionais que corrigem esta situação, quando o existe sincronização dos relógios.

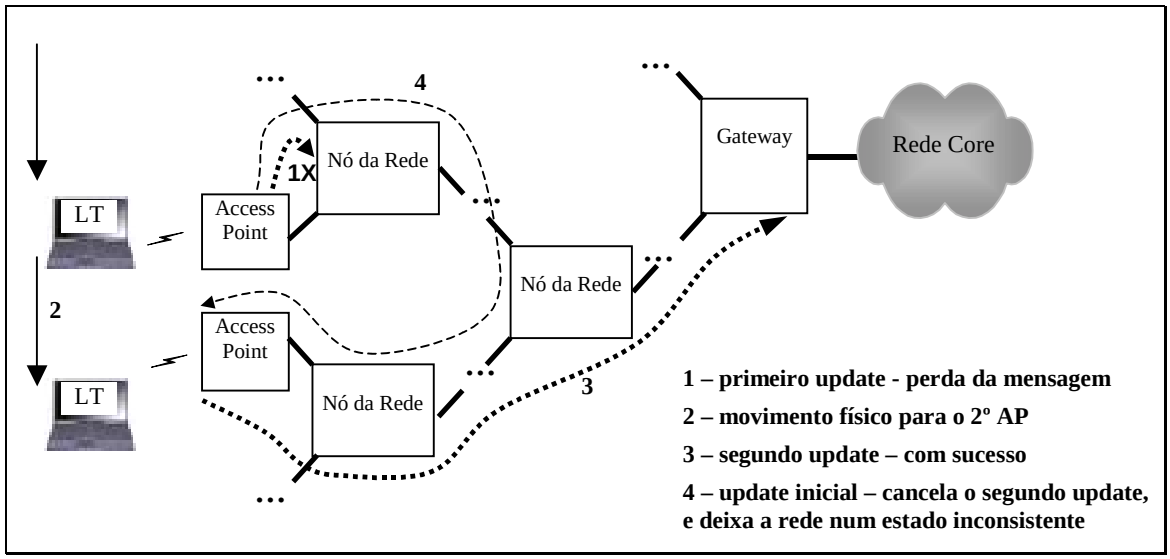


Figura 85: Inconsistência do handover

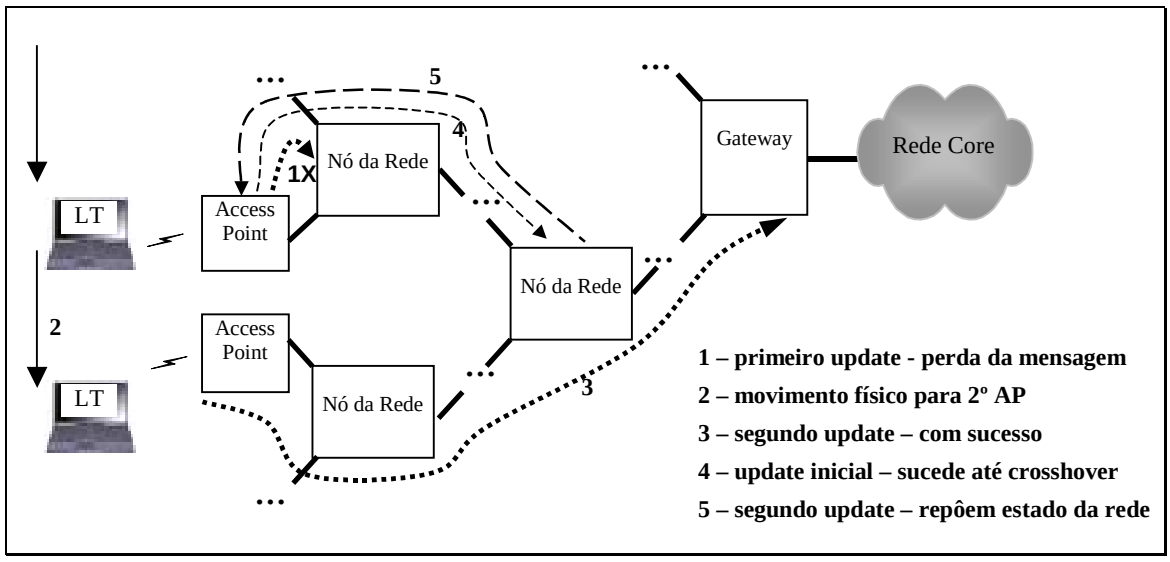


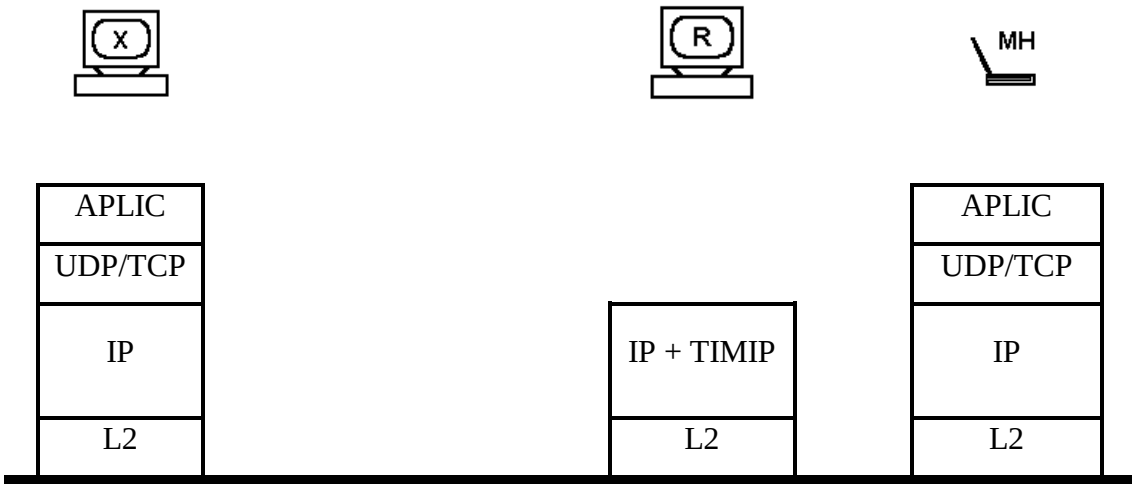
Figura 86: Resolução da inconsistência do handover

Anexo 8 Opções do protocolo TIMIP

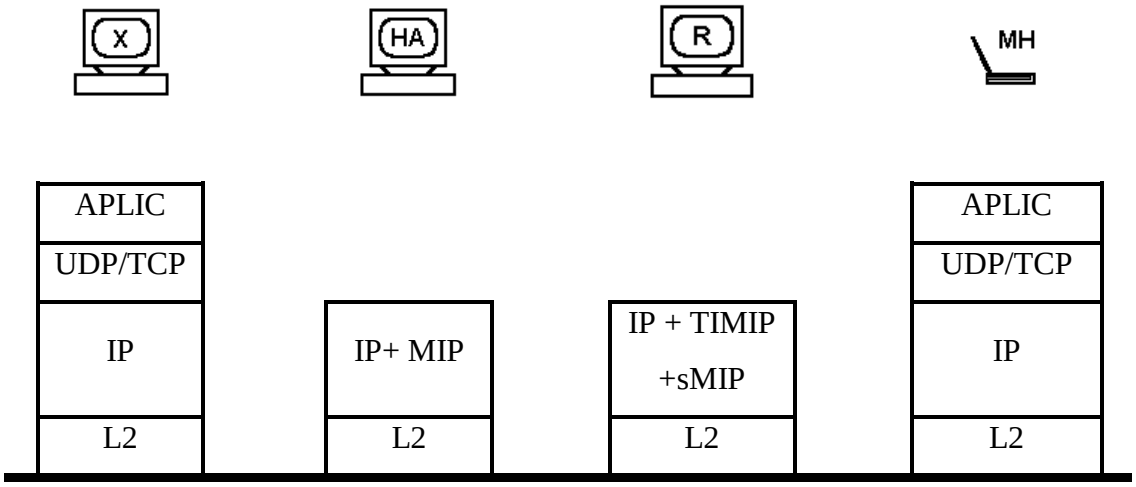
Parâmetro	Significado	valor por omissão
Timeout_ack	tempo que o nó espera até aparecer o ack de um *update*	1 segundo
Timeout_remove	tempo máximo *consecutivo* do registo softstate do terminal sem refrescamento	120 segundos
Timeout_min	tempo mínimo para o valor dinâmico do timeout do refrescamento	1 segundo
Timeout_start	tempo inicial de espera sem refrescamento do terminal antes de lhe enviar um ping	10 segundos
Timeout_max	tempo máximo para o valor dinâmico do timeout do refrescamento	60 segundos

nota: timeout_remove > timeout_max + timeout_max/2 + timeout_max/4 + ... + timeout_min

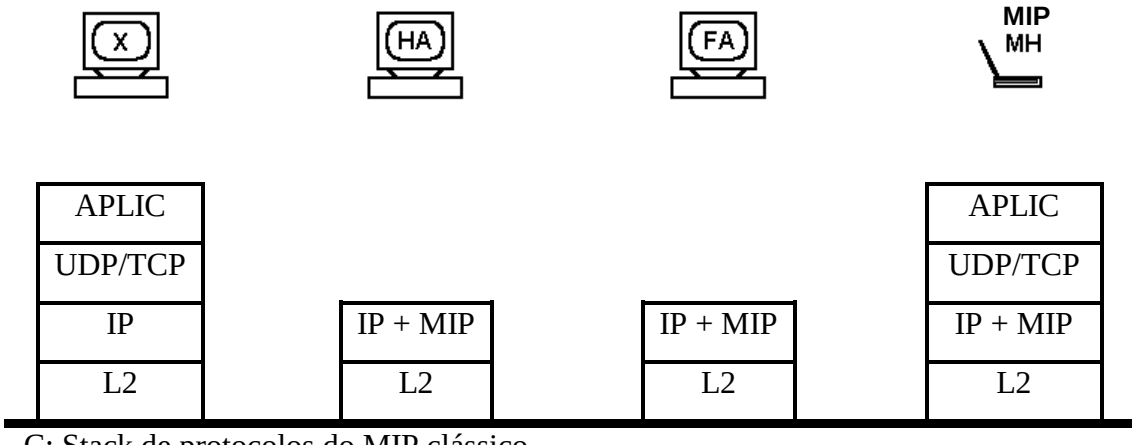
Anexo 9 Stack de protocolos



C: Stack de protocolos do TIMIP



B: Stack de protocolos do TIMIP+sMIP



C: Stack de protocolos do MIP clássico

Anexo 10 Detalhes da Ilha do INESC

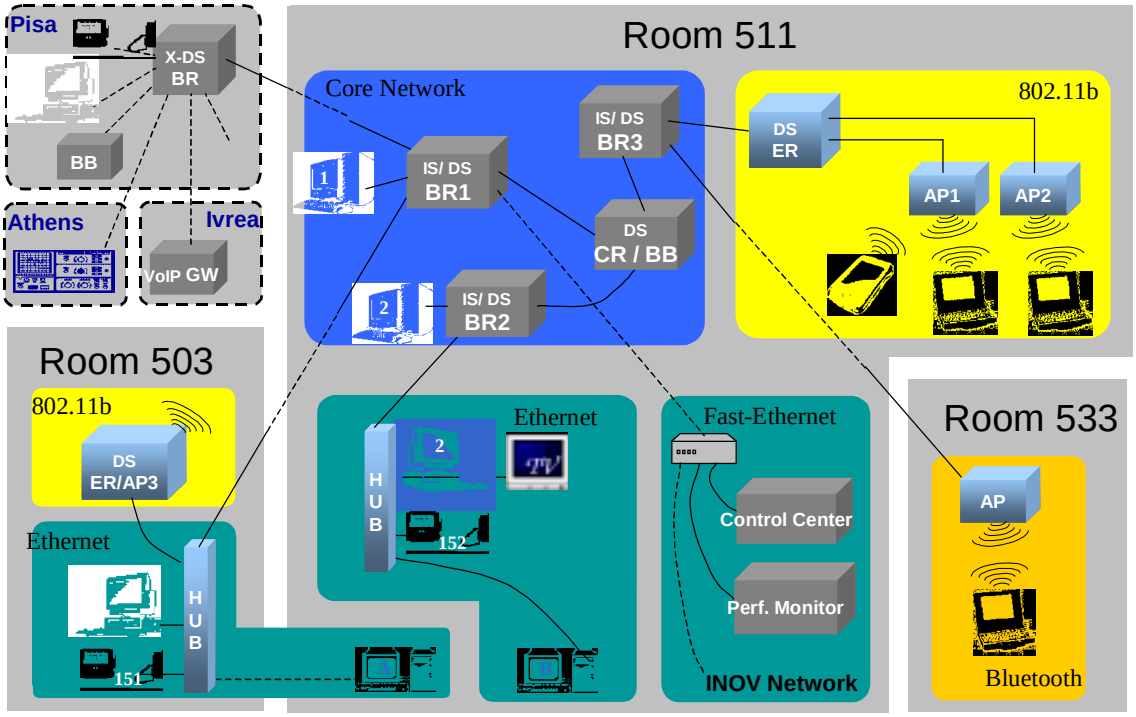


Figura 87: Esquema da ilha do INESC no demonstrador do MOICANE

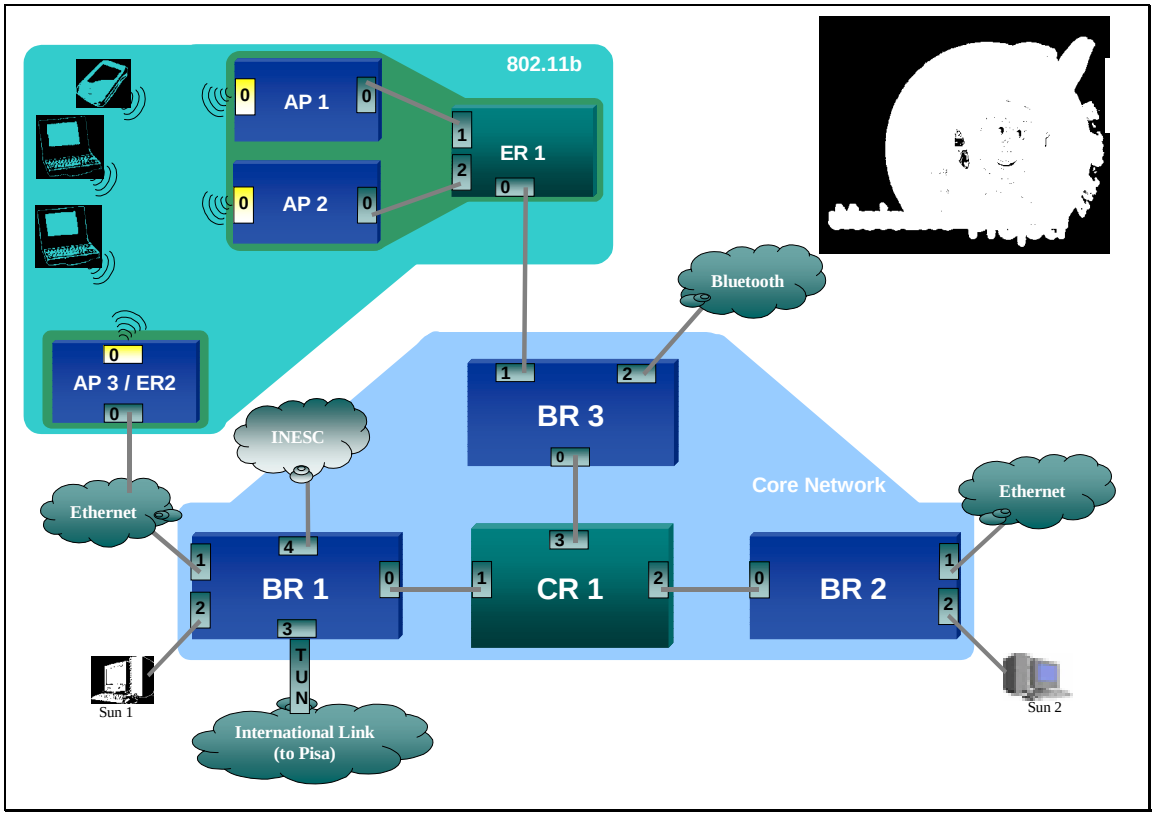


Figura 88: Ilha do INESC – Sistema de Monitorização

Anexo 11 Codepoints utilizados pelo Diffserv

Classe	DSCP
BE	0x00
EF	0xB8
AF1X	0b00101000, 0b00110000, 0b00111000
AF2X	0b01001000, 0b01010000, 0b01011000
AF3X	0b01101000, 0b01110000, 0b01111000
AF4X	0b10001000, 0b10010000, 0b10011000
Controlo	0xCC

Tabela 13: Codepoints das classes Diffserv já normalizadas pelo IETF

Anexo 12 Detalhes da interface PCAP

recolha de pacotes de CONTROLO:

```
match ip protocol 1 and icmp[0]=200
```

recolha de pacotes de DADOS:

caso 1) interface wireless 802.11 no AP

```
match ip dst 224.0.0.1 or ip dst 255.255.255.255 or ( not ether src
<THIS_ITF> and ether dst <THIS_ITF> )
```

caso 2) interface ethernet ligada a um nó descendente

```
match ether src <NODE_ITF> and ether dst <THIS_ITF>
```

caso 3) interface ethernet na GW ligada ao exterior

```
match none
```

Anexo 13 Arquitectura Diffserv

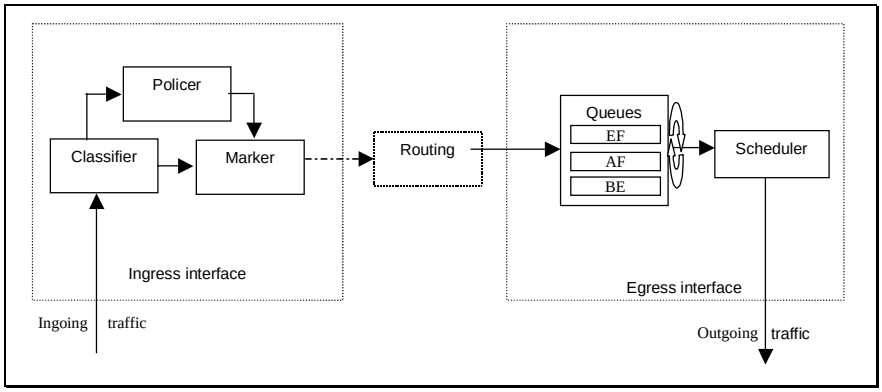


Figura 89: Interface edge Diffserv

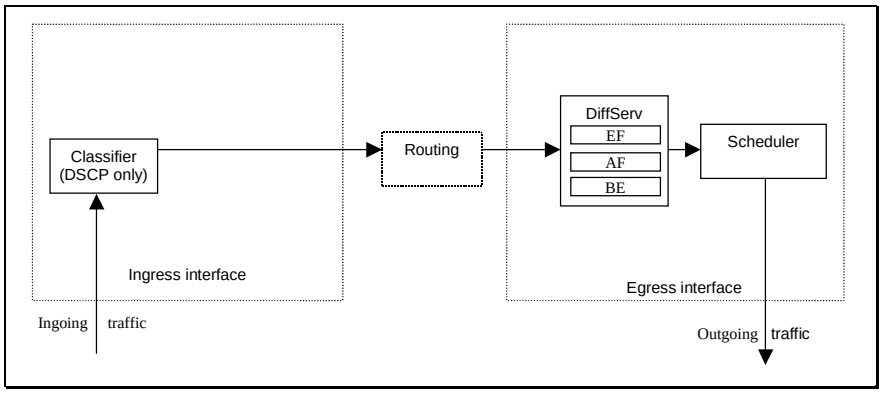


Figura 90: Interface core Diffserv

Anexo 14 Módulos de Controle de Tráfego em Linux

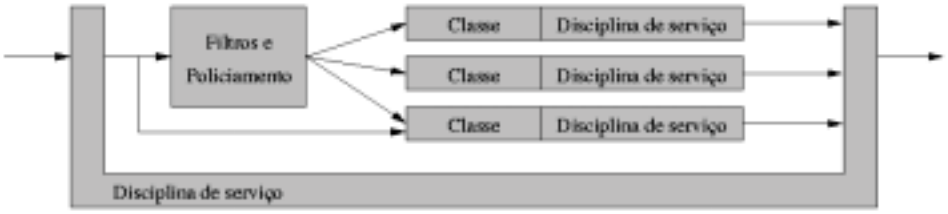


Figura 91: Elementos de controlo de tráfego no Linux

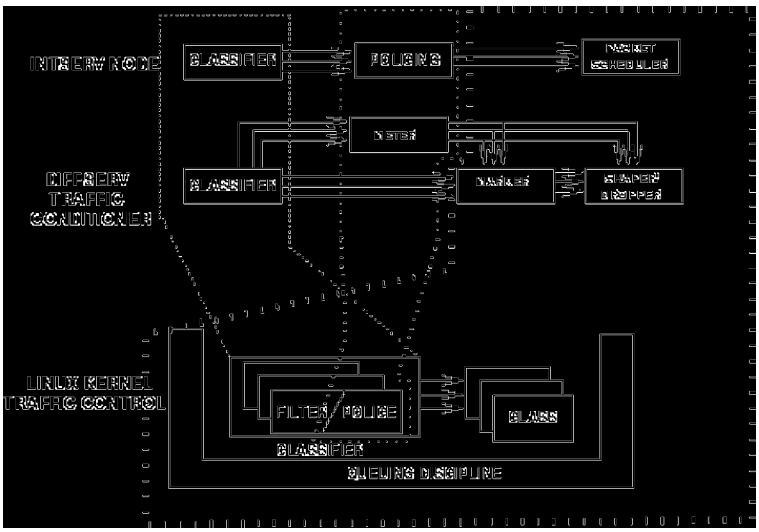


Figura 92: Mapeamento da Arquitectura Diffserv nos elementos de TC do Linux

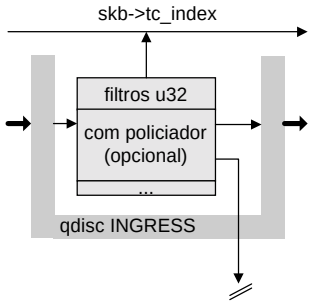


Figura 93: Arquitectura de TC criada pelo DSR nas Interfaces Ingress

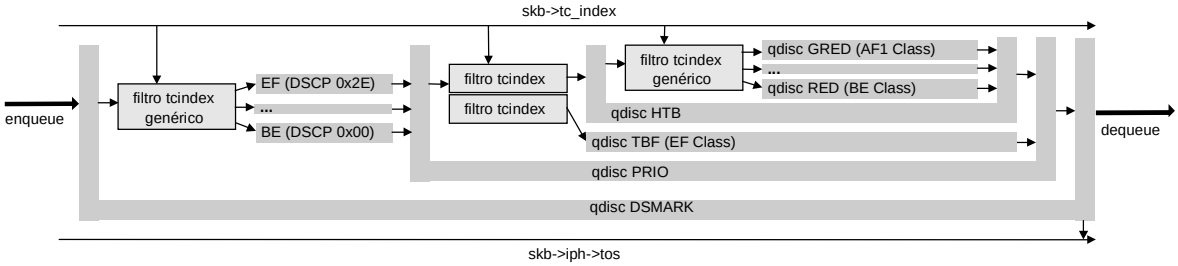


Figura 94: Arquitectura de TC criada pelo DSR nas Interfaces Egress

Anexo 15 Arquitectura dos nós da rede

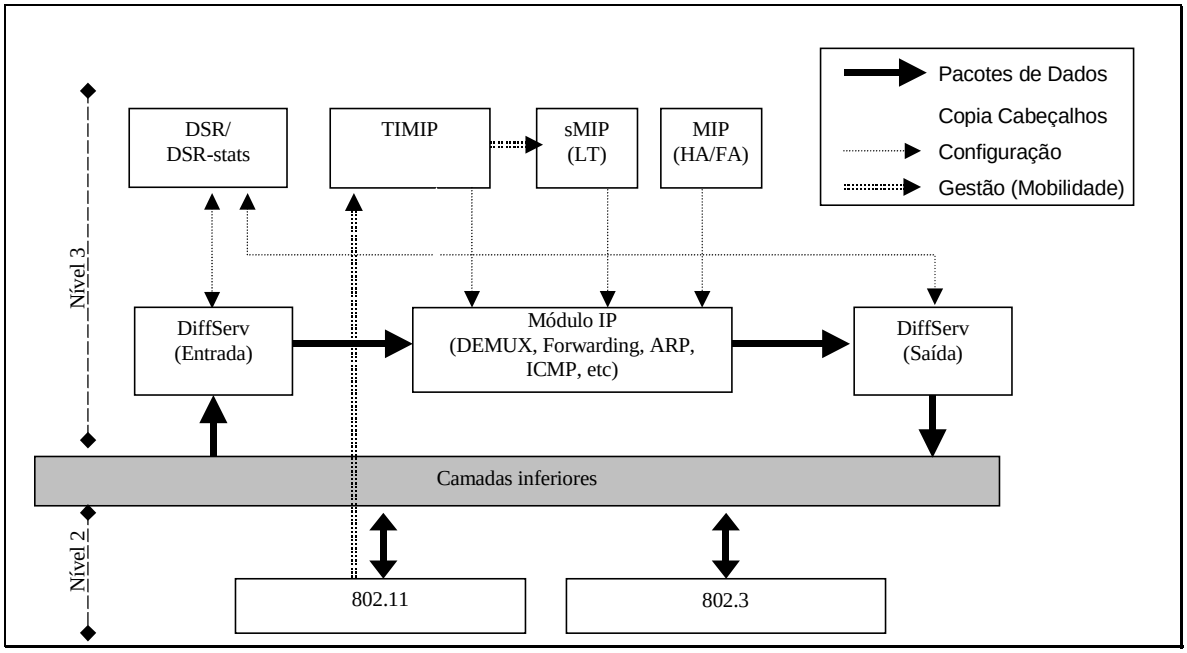


Figura 95: Detalhes da arquitectura dos nós da rede TIMIP

(inclui vida dos pacotes de dados e acções de gestão, e não inclui sinalização de controlo TIMIP/MIP)

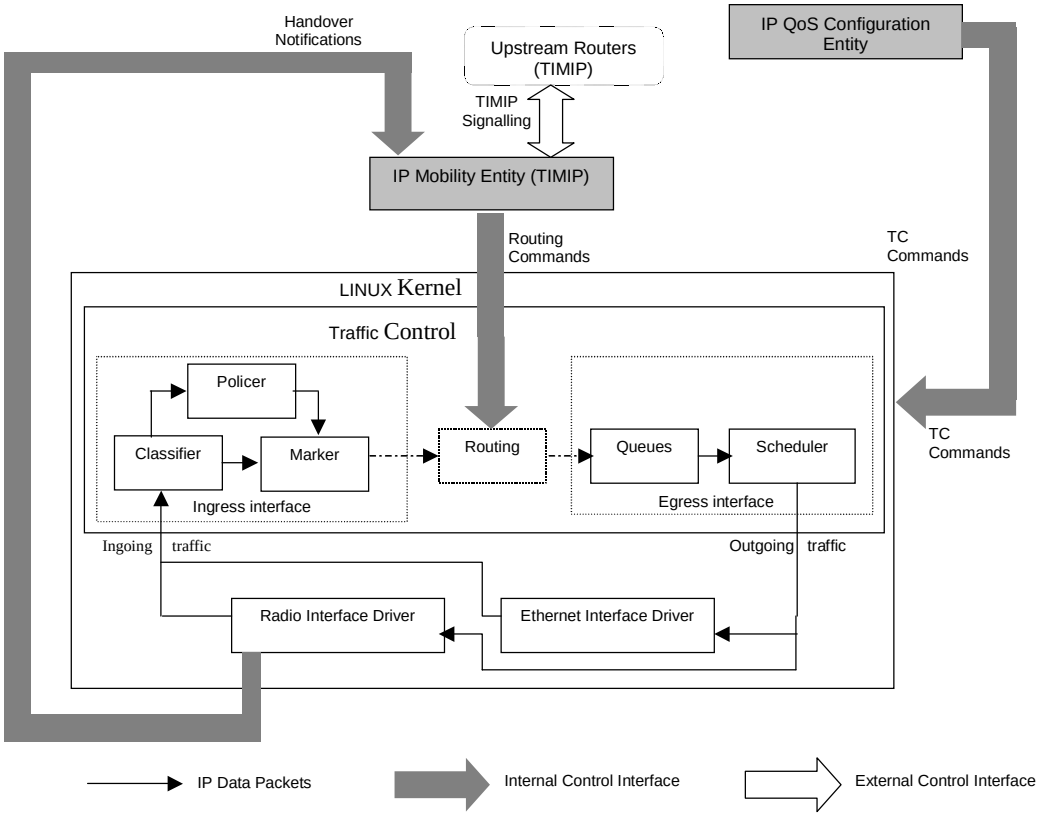


Figura 96: Detalhe da arquitectura dos nós da rede TIMIP (integrado com Diffserv)

Anexo 16 Cartões de Teste

Testes		Conectividade IP básica Inter-Domain
TESTE A-1	**Objectivo**	Avaliar a conectividade proporcionada pelo TIMIP, e o encaminhamento utilizado numa situação de comunicação entre redes (inter-domain).
	Cenário	Um terminal legado LT está ligado por 802.11 ao AP1; um PC externo está ligado fora da rede por ethernet à GW (ver Figura 66)
	Método	
	Resultado	Todos os pedidos PING foram respondidos correctamente pelo terminal, seguindo estes pelo caminho mais directo na árvore de nós (PC->GW->AP1->LT)

Testes		Conectividade IP básica Intra-Domain
TESTE A-2	**Objectivo**	Avaliar a conectividade proporcionada pelo TIMIP, e o encaminhamento utilizado numa situação de comunicação no interior da rede (intra-domain).
	Cenário	Um terminal legado LT1 está ligado por 802.11 ao AP1, comunicando com um segundo terminal Legado LT2 ligado ao AP2 (ver Figura 67)
	Método	LT2 emite pedidos de PING e TRACEROUTE destinados a LT1
	Resultado	Todos os pedidos PING foram respondidos correctamente por LT1, seguindo estes pelo caminho mais directo na árvore de nós (LT2->AP2->GW->AP1->LT1)

Testes		Mobilidade IP no interior da rede (teste Inter-Domain)
TESTE B-1	**Objectivo**	Avaliar a mobilidade proporcionada pelo TIMIP no interior da rede por um emissor *fora* da rede.
	Cenário	ver teste A-1
	Método	O PC externo emite pedidos de PING e TRACEROUTE destinados a LT, que se movimenta entre os dois APs
	Resultado	Todos os pedidos PING foram respondidos correctamente pelo terminal, seguindo estes pelo caminho mais directo na árvore de nós conforme a sua localização (PC->GW->AP1->LT) ou (PC->GW->AP2->LT)

Testes		Mobilidade IP no interior da rede (teste Intra-Domain)
TESTE B-2	**Objectivo**	Avaliar a mobilidade proporcionada pelo TIMIP no interior da rede por um emissor *dentro* da rede.
	Cenário	ver teste A-2
	Método	LT2 emite pedidos de PING e TRACEROUTE destinados a LT1, que se movimenta entre os dois APs
	Resultado	Todos os pedidos PING foram respondidos correctamente pelo terminal, seguindo estes pelo caminho mais directo na árvore de nós conforme a sua localização (LT2->AP2->GW->AP1->LT1) ou (LT2->AP2->LT1)

Testes		Garantia de entrega das mensagens de controlo TIMIP
TESTE B-2	**Objectivo**	Avaliar a mobilidade proporcionada pelo TIMIP no interior da rede por um emissor *dentro* da rede.
	Cenário	Um terminal legado LT1 está ligado por 802.11 ao AP1; um PC externo está ligado fora da rede por ethernet à GW A ligação do backbone entre AP2 e a GW está cortada.
	Método	O PC externo emite pedidos de PING e TRACEROUTE destinados a LT; depois da transição, a ligação do backbone é reestabelecida
	Resultado	Depois da ligação do backbone for reestabelecida, a conectividade do terminal foi reposta após um atraso de 1 segundo, relacionado com o *timeout* de controlo TIMIP

Testes		Conectividade IP básica Inter-Domain
TESTE C-1	**Objectivo**	Avaliar a mobilidade global e o encaminhamento proporcionada pelos protocolos TIMIP + sMIP, distinguindo a utilização de macro e micro-mobilidade
	Cenário	Um terminal legado LT está ligado por 802.11 a um domínio de teste; um PC externo de teste está ligado fora da rede; a rede de acesso do MOICANE é o segundo domínio TIMIP (ver Figura 71)
	Método	O PC externo emite pedidos de PING e TRACEROUTE destinados a LT, que se movimenta entre os dois domínios, e no interior de um destes, entre os dois APs do mesmo domínio.
	Resultado	Em todas as situações descritas, os pedidos PING foram respondidos correctamente pelo terminal. Por outro lado, o programa TRACEROUTE mostrou que os pacotes as regras exactas de encaminhamento TIMIP/sMIP. a) PC->...->GW1->LT b) PC->...->GW1-> (túnel) ->GW2->AP1->LT

Testes		Filtragem DiffServ
TESTE D-1	**Objectivo**	
	Cenário	Um emissor no exterior da rede a gerar um fluxo de teste UDP de 1Mbit/s destinado a um terminal no interior da rede
	Método	Na GW: definem-se filtros compostos, que verificam ou não as características do fluxo estabelecido, e uma acção de drop.
	Resultado	Quando o filtro composto correspondia exactamente às características do tráfego, então os pacotes deixavam se serem recebidos no receptor.

Testes		Policiamento DiffServ
TESTE D-2	**Objectivo**	Avaliar a implementação do policiamento Diffserv para vários débitos de tráfego conforme um SLA fixo
	Cenário	ver teste D-1
	Método	Na GW: definem-se filtros compostos para classificar o tráfego, com a acção de descarte para os pacotes não-conformantes além de 1Mbit/s.
	Resultado	Quando o filtro é activado, o fluxo que chega ao receptor (~1.05 Mbit/s) é apenas constituído pelo débito conformante, com uma margem adicional relacionada com o *burst* do filtro. Estes resultados estão presentes no Anexo 21

Testes		Marcação DiffServ
TESTE D-3	**Objectivo**	Avaliar a implementação da marcação Diffserv para várias classes.
	Cenário	ver teste D-1
	Método	Na GW: definem-se filtros compostos, que verificam as características do fluxo estabelecido, e com a acção de marcar o pacote em classes, variando estas.
	Resultado	Os pacotes saíram do encaminhador com a marcação correcta no campo DSCP da sua classe (especificada no filtro).

Testes		Fluxos *Downstream* BE
TESTE E-1	**Objectivo**	Avaliar a implementação das classes de serviço (escalonador HTB)
	Cenário	Um emissor no exterior da rede gera um fluxo BE de prova para LT1 (4.2 Mbit/s); um segundo emissor gera um fluxo BE de carga para LT2 (0.768 Mbit/s de pacotes de 48 bytes). LT1 move-se entre os APs e LT2 está fixo no AP2.
	Método	O fluxo de prova é medido alternadamente quando em LT1 está localizado no AP1 e no AP2.
	Resultado	O fluxo BE de prova é recebido na sua totalidade apenas quando o terminal LT1 está localizado no AP1, porque a carga apenas satura o meio *wireless*, e não o backbone. Quando estiver ligado pelo AP saturado, o fluxo vai perder pacotes por competir com o fluxo de carga, sendo recebidos apenas 0.5821 Mbit/s.

Testes		Fluxos *Downstream* EF e BE
TESTE E-2	**Objectivo**	Avaliar a implementação das classes de serviço (escalonador HTB)
	Cenário	ver Teste E-1, com a diferença que o tráfego de prova é classificado em EF
	Método	ver Teste E-1.
	Resultado	O fluxo EF de prova é recebido na sua totalidade em ambos os APs, dado que a rede IP garante os requisitos do EF.

Testes		Fluxo Prova EF *downstream* e Fluxo carga BE *upstream*
TESTE E-3	**Objectivo**	Avaliar o resultado de apenas existir QoS de Nível 3 ao longo de todo o caminho, sem existência de QoS de nível 2 no 802.11.
	Cenário	ver Teste E-2, com a diferença que o tráfego de carga é gerado no sentido upstream
	Método	ver Teste E-2
	Resultado	O fluxo EF de prova é recebido na sua totalidade apenas quando o terminal está em AP1, devido à célula 802.11 do AP2 estar saturada usando o mecanismo DCF. Recebendo o tráfego de prova nos APs, e não em LT1, este é sempre recebido na sua totalidade.

Testes		Velocidade do *handover* TIMIP
TESTE F	**Objectivo**	Medição rigorosa do tempo necessário para efectuar um *handover* com micro-mobilidade IP de um terminal 802.11, considerando as componentes separadas do 802.11 e do TIMIP.
	Cenário	Um emissor no exterior da rede gera um fluxo de teste periódico de um pacote por cada milisegundo, a ser recebido num terminal móvel que transita continuamente entre os dois APs.
	Método	Depois de ocorrer uma transição física e o subsequente handover 802.11 e TIMIP, é verificado: - o tempo t0 do último pacote recebido pelo AP anterior; - o tempo t2 do primeiro pacote recebido pelo novo AP;
	Resultado	Este teste foi efectuado 21 vezes, para garantir resultados confiáveis (detalhados no Anexo 17). Nestes, chegou-se à conclusão que o TIMIP demora em média 2.03 ms a transitar (0,224 ms desvio padrão), enquanto que o 802.11 demora 101.06 ms a transitar (25,650 ms desvio padrão)

Testes		Velocidade do handover TIMIP em mobilidade Global sMIP
TESTE G	**Objectivo**	Medição rigorosa do tempo necessário para efectuar handovers de macro-mobilidade sMIP, destinguido entre saídas e retornos à rede de origem, e micro-mobilidade TIMIP em domínios visitados, considerando as componente separadas do 802.11 e do TIMIP.
	Cenário	Um emissor no exterior da rede gera um fluxo de teste periódico de um pacote por cada milisegundo, a ser recebido num terminal móvel que transita continuamente entre domínios TIMIP, e no interior do domínio visitado.
	Método	Tanto para a macro como para a micro-mobilidade, em cada tipo de transição é verificado; - o tempo t0 do último pacote recebido pelo AP anterior; - o tempo t1 da chegada do pacote de associação ao novo AP; - o tempo t2 do primeiro pacote recebido pelo novo AP;
	Resultado	Relativamente à componente de micro-mobilidade em domínios visitados obteu-se resultados em todo coincidentes com o teste anterior (2/3 ms), devido à independência dos dois tipos de mobilidade. Relativamente à componente de macro-mobilidade entre domínios, verificou-se que as transições com destino em domínios visitados têm uma latência elevada (~ 3 segundos), motivada pelos processos inerentes MIP. No caso particular do retorno em macro-mobilidade ao domionio de origem, esta apresenta latências da ordem da micro-mobilidade.

Testes		Débito oferecido pelo 802.11b
TESTE H	**Objectivo**	Medição rigorosa do debito oferecido pelo 802.11b, variando o tamanho dos pacotes do fluxo de dados
	Cenário	Um emissor num AP emite um fluxo constante de 11 Mbit/s para um terminal *wireless* (fixo).
	Método	Para cada tamanho de pacote, é verificado o débito atingido
	Resultado	os débitos efectivamente atingidos variam entre **0.404 Kbit/s** e **5.5 Mbit/s** conforme o tamanho dos pacotes, sendo assim bastante mais baixos que os 11 Mbit/s nominais do 802.11b

Testes		Atraso da classe EF
TESTE I	**Objectivo**	Avaliar a implementação do atraso da classe de serviço EF
	Cenário	Um emissor no exterior da rede gera um fluxo EF de prova para LT1; um segundo emissor gera um fluxo BE de carga para LT2. Os nós da rede têm os seus relógios sincronizados entre si.
	Método	A latência do fluxo de prova necessária para chegar até ao receptor é medida quando o Diffserv está inactivo (resultado **a**), quando a carga esta inactiva (**b**) e quando está activa (**c**).
	Resultado	Em todas as situações os três valores medidos estiveram na mesma ordem de grandeza (média: 1ms/1ms/6ms). Comparando as médias de a) e b), verifica-se que a adição do *software* de Diffserv à rede de acesso tem *overhead* marginal; Comparado b) com c) verifica-se que mesmo no pior caso, os SLAs associados aos tráfegos agregado EF continuam a serem cumpridas

Anexo 17 Medições da velocidade do TIMIP

	TESTE: VELOCIDADE DO HANDOVER TIMIP						
						TEMPO TOTAL	
Last Packet	ASSOC	First Packet		TEMPO TIMIP		N2+N3	(ajustado)	
t0	t1	t2		(First-Assoc)		(First-Last)		
0,728735	0,8202699	0,821986		1,716057716		93	93	
0,382186	0,42097	0,423445		2,475036926		41	41	
0,996395	0,16065	0,162491		1,840985123		-834	166	
0,453759	0,53653	0,538345		1,814982147		84	84	
0,7031	0,78423	0,786275		2,04500618		83	83	
0,969334	0,04732	0,049759		2,439003643		-920	80	
0,907012	0,035236	0,03696		1,723998985		-871	129	
0,286822	0,36678	0,368845		2,064957352		82	82	
0,399911	0,4887	0,49052		1,819967766		90	90	
0,423115	0,50711	0,509695		2,585000343		86	86	
0,101889	0,19643	0,198639		2,20903212		96	96	
0,632414	0,71447	0,716567		2,096971123		84	84	
0,885041	0,9644901	0,966532		2,041943962		81	81	
0,343908	0,42329	0,425481		2,190985733		81	81	
0,091151	0,17975	0,181783		2,033034332		90	90	
0,124574	0,2283601	0,230217		1,856943123		105	105	
0,023699	0,12473	0,126768		2,038009041		103	103	
0,001434	0,12108	0,122678		1,597959068		121	121	
0,610148	0,76709	0,769053		1,963037041		158	158	
0,134105	0,25603	0,258638		2,608036507		124	124	
0,483099	0,6700799	0,671748		1,668053482		188	188	
		Média:		**2,039476272**	ms		103,0952381	ms
		Desvio padrão:		**0,224877254**	ms		25,65079365	ms

Valor máximo de desvio dos relógios de cada nó a uma referência central: 0.500 ms

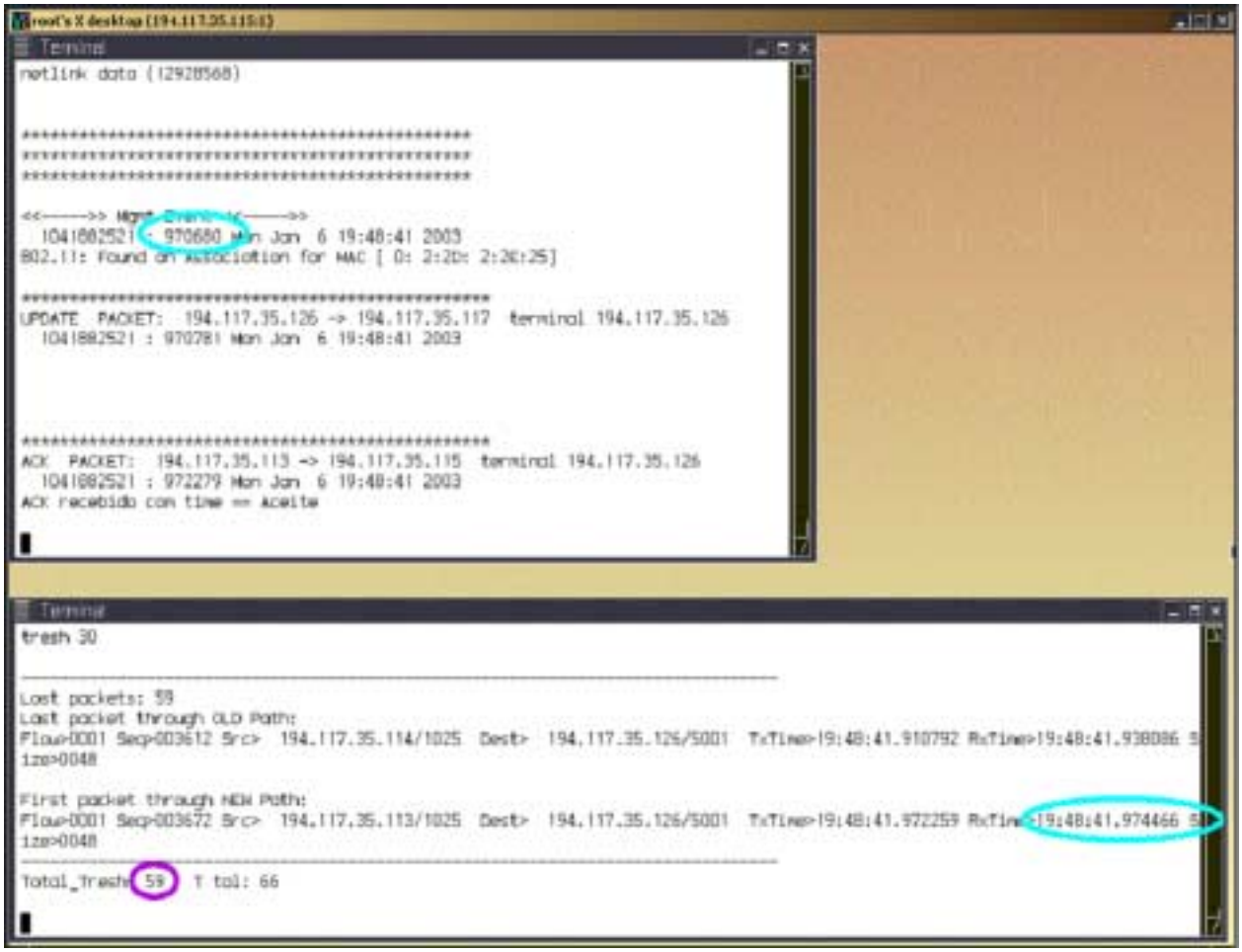


Figura 97: Exemplo de recolha de Dados TIMIP

Valor Roxo	Número de pacotes perdidos (Tempo Total do Handover)
Valores Azul-Claros	Tempo de recepção do primeiro pacote e tempo de recepção da mensagem de Associação (Tempo do TIMIP)

Anexo 18 Medições da velocidade do sMIP+TIMIP

TIPO	FROM	DEST	802.11 ASSOC	TIME		PAC_LOST	TIME_FIRST		assoc	first	timip	timip(ms)
	ap3	ap2	917588	21:41:24		3248	21:41:28	63916				
1	ap3	ap2	942615	21:32:41		3057	21:32:44	967625				
	ap3	ap2	581883	21:40:01		3046	21:40:04	584873				
				MÉDIA tipo 1		3117,00 ms						
	ap2	ap1	471783	21:29:18		43	21:29:18	474673	0,4718	0,474673	0,003	2,89
2	ap2	ap1	214438	21:29:37		37	21:29:37	218424	0,2144	0,218424	0,004	3,986
	ap2	ap1	910719	21:34:04		37	21:34:04	913612	0,9107	0,913612	0,003	2,893
				MÉDIA tipo 2		39,00 ms				MÉDIA TIMIP tipo1		3,26 ms
	ap1	ap2	983791	21:29:25		41	21:29:25	986640	0,9838	0,98664	0,003	2,849
3	ap1	ap2	82539	21:29:47		41	21:29:47	83941	0,0825	0,083941	0,001	1,402
	ap1	ap2	841724	21:31:57		42	21:31:57	843742	0,8417	0,843742	0,002	2,018
				MÉDIA tipo 3		41,33 ms				MÉDIA TIMIP tipo1		2,09 ms
	ap2	ap3	485595	21:30:14		35	21:30:14	492127	0,4856	0,492127	0,007	6,532
4	ap2	ap3	441298	21:32:16		38	21:32:16	445885	0,4413	0,445885	0,005	4,587
	ap2	ap3	198042	21:40:45		42	21:40:45	201427	0,198	0,201427	0,003	3,385
				MÉDIA tipo 4		38,33 ms				MÉDIA TIMIP tipo2		4,83 ms

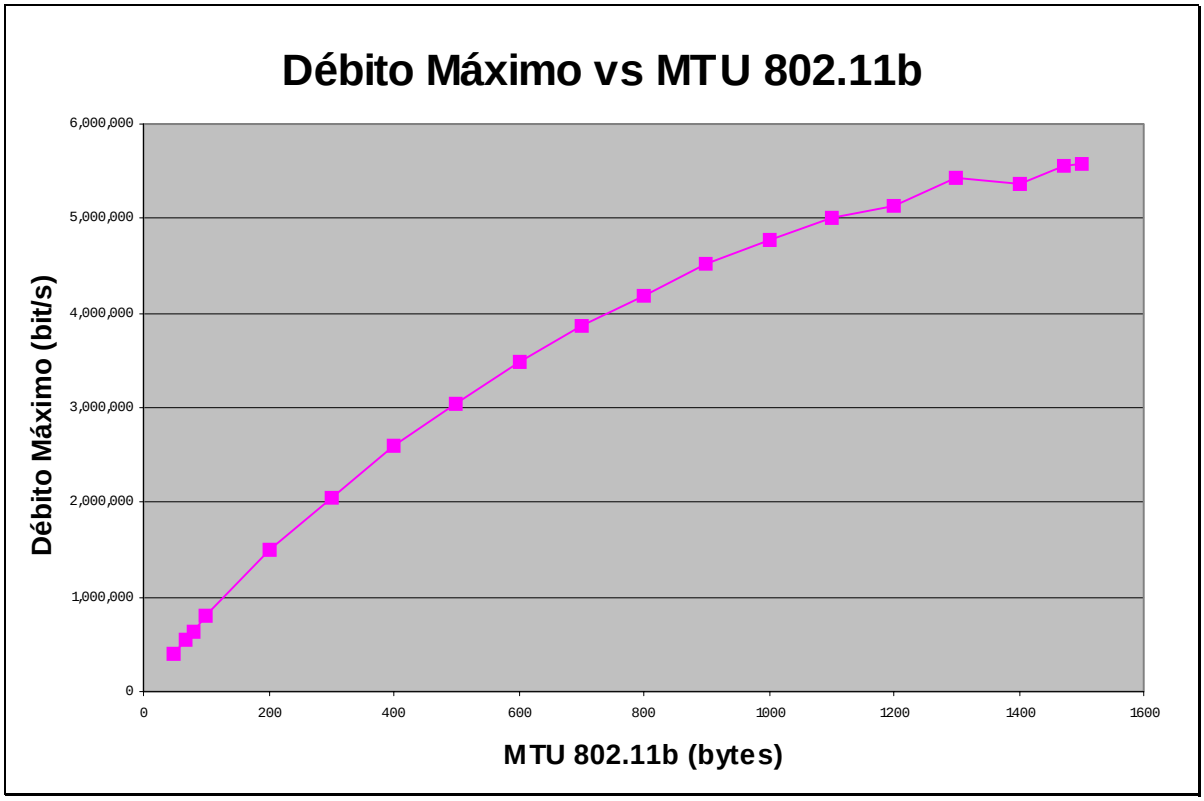
TIPO	origem	destino	Mobilidade:	Descrição	Latência
1	AP3	AP2	Macro+Micro	entrada num domínio visitado	3117 ms
2	AP2	AP1	Micro	movimentação em domínio visitado	3 ms
3	AP2	AP2	Micro	movimentação em domínio visitado	2 ms
4	AP2	AP3	Macro+Micro	retorno ao domínio de origem	5 ms

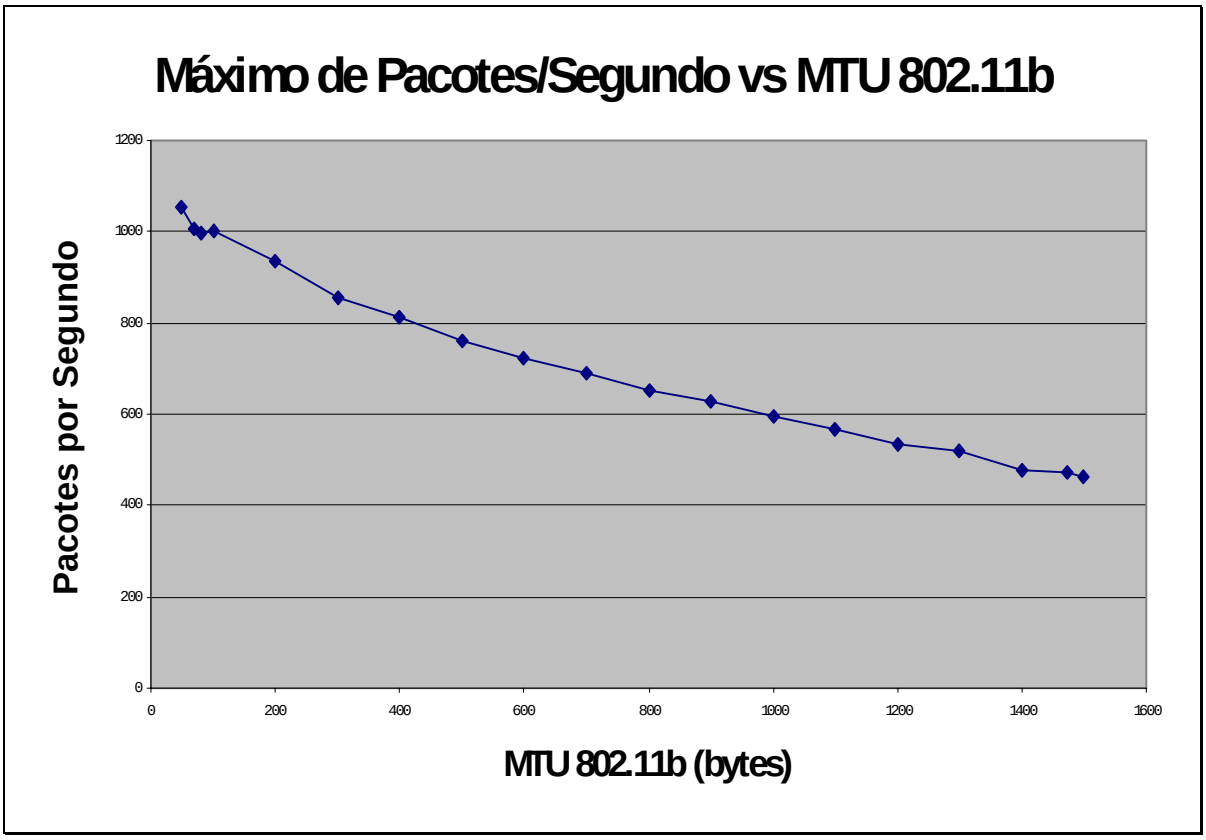
Valor máximo de desvio dos relógios de cada nó relativamente a uma referência central: 0.500 ms

Anexo 19 Medições Práticas do Débito Máximo vs MTU do 802.11b

Tamanho Pacote IP (bytes)	Débito Médio (bit/s)	Pacotes por Segundo
48	404.339	1052
68	548.758	1008
80	638.826	998
100	802.459	1003
200	1.500.410	937
300	2.051.732	854
400	2.603.112	813
500	3.050.142	762
600	3.478.919	724
700	3.864.118	690
800	4.182.089	653
900	4.520.987	627
1000	4.769.577	596
1100	5.008.725	569
1200	5.128.050	534
1300	5.435.140	522
1400	5.359.503	478
1472	5.562.734	472
1500	5.582.651	465

Tabela 14: Medições Práticas do débito máximo do 802.11b

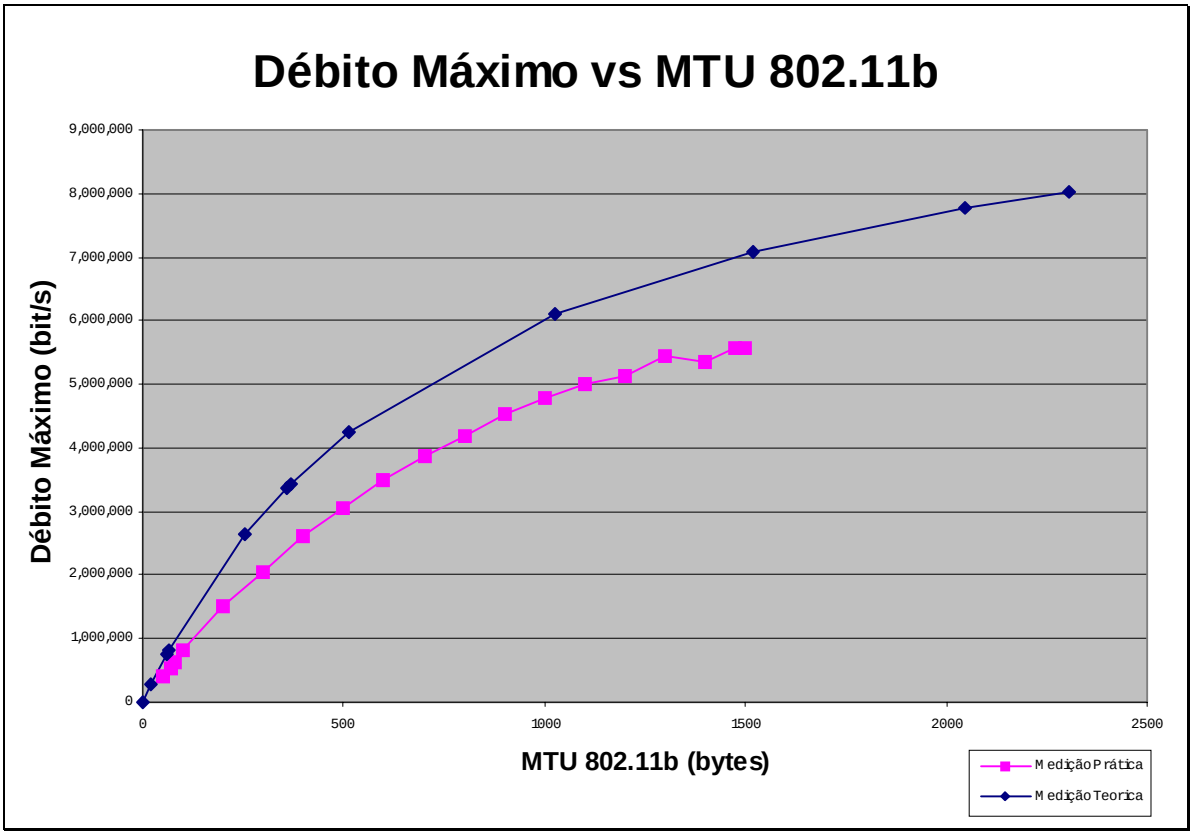

Débito Máximo vs MTU 802.11b
Débito Máximo (bit/s)
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
0
200
400
600
800
1000
1200
1400
1600
MTU 802.11b (bytes)


Máximo de Pacotes/Segundo vs MTU 802.11b
Pacotes por Segundo
1200
1000
800
600
400
200
0
0
200
400
600
800
1000
1200
1400
1600
MTU 802.11b (bytes)

Anexo 20 Comparação do Débito Máximo do 802.11

Tamanho Pacote IP (bytes)	Débito Médio (bit/s)
0	0
20	268000
60	765000
64	812000
256	2650000
357	3370000
368	3440000
512	4250000
1024	6090000
1518	7090000
2048	7780000
2304	8030000

Tabela 15: Medições Práticas do débito máximo do 802.11b



Anexo 21 Teste de Policiamento Diffserv

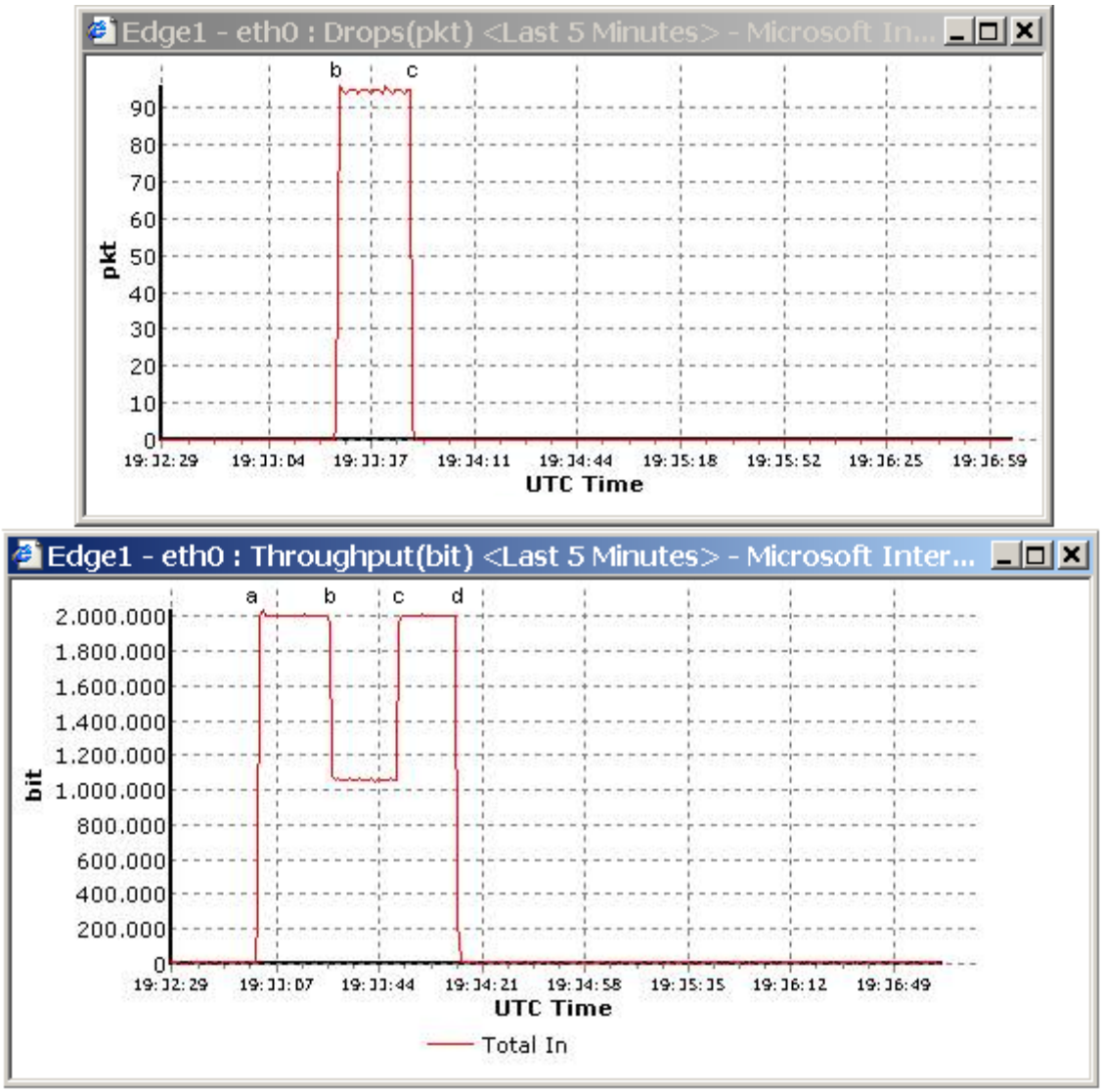


Figura 98: Entrada no domínio DiffServ: pacotes perdidos e débito transmitido

Passo	Descrição	Valor Recebido
a	Início do fluxo de teste de 2 Mbit/s	2 Mbits/s
b	Aplicação de um Policiador de 1 Mbit/s na entrada da rede	~ 1.05 Mbits/s
c	Remoção do Policiador	2 Mbits/s
d	Fim do fluxo de teste	0 Mbits/s

Tabela 16: Teste de Policiamento Diffserv – descrição dos passos

Anexo 22 Teste de QoS e Mobilidade com Aplicações Multimédia

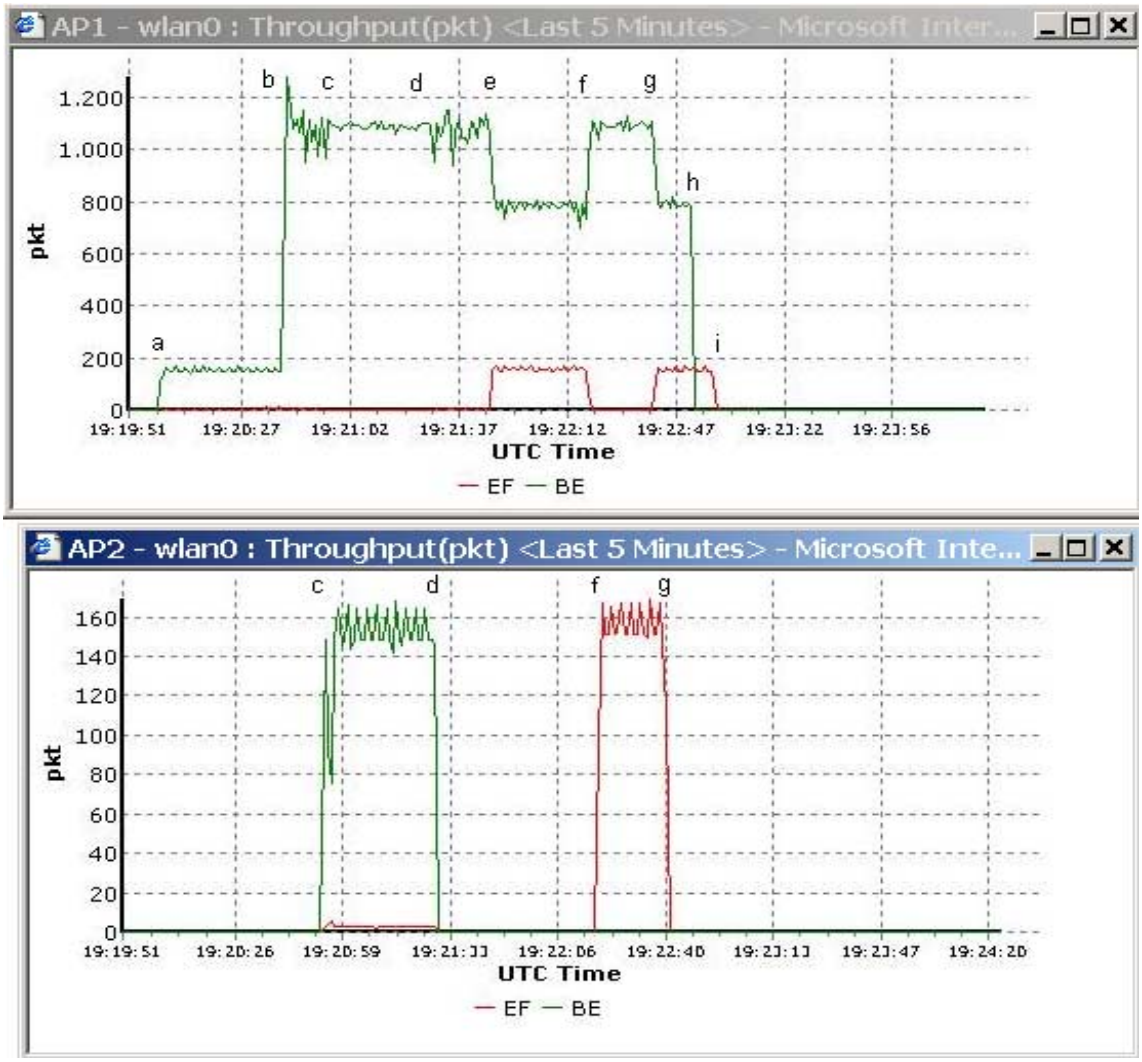


Figura 99: Interface *wireless* 802.11 do AP1 e AP2

Passo	Descrição	Qualidade do Vídeo
a	Início do *streaming* do Vídeo (sem QoS)	Boa
b	Início da Geração da Carga	Má
c	PC1 movimenta-se para o AP2	Boa
d	PC1 volta para o AP1	Má
e	Utilização dos filtros estáticos de QoS	Boa
f	PC1 movimenta-se para o AP2	Boa
g	PC1 volta para o AP1	Boa
h	Fim da Carga	Boa
I	Fim do Vídeo	Boa

Tabela 17: Teste de performance com aplicações multimédia – descrição dos passos

Bibliografia

Referências de organismos de Normalização

[1] Internet Engineering Task Force, www.ietf.org

[2] Institute for Electric and Electronics Engineering, www.ieee.org

[3] Mobile IP Charter, http://www.ietf.org/html.charters/mobileip-charter.html

[4] 802.11 Group, http://grouper.ieee.org/groups/802/11/index.html

Referências relativas ao protocolo MIP de Macro-Mobilidade

[5] C. Perkins, ed., "IP Mobility Support for IPv4" (Proposed Standard), IETF RFC 3320, Janeiro 2002, www.ietf.com

[6] D. Johnson, ed., "IP Mobility Support for IPv6", draft-ietf-mobileip-ipv6-16.txt, Março 2002.

[7] D. Johnson, “Route Optimization in Mobile IP,” Internet draft, draft-ietf-mobileip-optim-11, work in progress, Setembro 2001.

[8] G. Montenegro, Ed., “Reverse Tunneling for Mobile IP, revised” (Proposed Standard), RFC 3024, Janeiro 2001.

[9] C. Perkins and P. Calhoun, “AAA Registration Keys for Mobile IP” (work in progress), draft-ietf-mobileip-aaa-key-09.txt, Fevereiro 2002.

[10] S. Glass, M. Chandra, “Registration Revocation in Mobile IPv4”, draft-ietf-mobileip-reg-revok-04.txt, work in progress, Agosto 2002

[11] H. Levkowetz, S. Vaarala, “Mobile IP NAT/NAPT Traversal using UDP Tunnelling”, work in progress, Maio 2002

[12] H. Chaskar, ed, “Requirements of a QoS Solution for Mobile IP”, work in progress, draft-ietf-mobileip-qos-requirements-03.txt, Julho 2002

[13] J. Kristoff, “Mobile IP”, http://condor.depaul.edu/~jkristof/mobileip.html

Referências relativas a protocolos de Micro-Mobilidade

[14] A. Campbell, et al, "Design and Performance of Cellular IP Access Networks" , IEEE Personal Communications, edição especial dedicada a IP-Based Mobile Telecommunications Networks, Agosto 2000.

[15] R. Ramjee, et al, “IP-Based Access Network Infrastructure for Next-Generation Wireless Data Networks”, IEEE Personal Communications, Vol. 7 Nº4, Agosto 2000.

[16] R. Ramjee, et al, “Paging support for IP mobility using HAWAII”, draft-ietf-mobileip-paging-hawaii-00.txt, work in progress, Junho 1999

[17] E. Gustafsson, A. Johnsson, and C. Perkins, “Mobile IP Regional Registration,” Internet draft, draft-ietf-mobileip-reg-tunnel-06, work in progress, Março 2002.

[18] K. El-Malki and H. Soliman, “Low Latency Handoffs in Mobile IPv4” Internet draft, draft-ietf-mobileip-lowlatency-handoffs-v4-03.txt, work in progress, Novembro 2001.

[19] E. Gustafsson, ed., “Requirements on Mobile IP from a Cellular Perspective”, Internet draft, draft-ietf-mobileip-cellular-requirements-02, work in progress, Junho 1999.

[20] A. Campbell, et al, "Comparison of IP MicroMobility Protocols”, IEEE Wireless Communications, Fevereiro 2002.

[21] S. Das et al, “TeleMIP: Telecommunication-Enhanced Mobili IP Architecture for Fast Intradomain Mobility”, IEEE Personal Communications, 7(4):50-58, Agosto 2000

[22] A. O’ Neill, G. Tsirtsis, S. Corson, “Edge Mobility Architecture (EMA)”, draft-oneill-ema-01.txt”, work in progress, Março 2000

Referências relativas a protocolos de suporte IP

[23] C. Perkins, ed., "IP encapsulation within IP", IETF RFC 2003, Outubro 1996.

[24] C. Perkins, ed., "Minimal Encapsulation in IP", IETF RFC 2004, Outubro 1996.

[25] S. Deering, Editor, "ICMP Router Discovery Messages", RFC 1256, Setembro 1991.

[26] Postel, J., “Internet Control Message Protocol - DARPA Program Protocol Specification”, RFC 792, Setembro 1981.

[27] R. Braden, Ed., “Requirements for Internet Hosts - Communication Layers”, RFC 1122, Outubro 1989

[28] R. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, Abril 1992.

[29] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, Março 1997.

[30] B. Aboba, M. Beadles, “The Network Access Identifier”, RFC 2486, Janeiro 1999

[31] D. Plummer, “An Ethernet Address Resolution Protocol”, RFC 826, MIT-LCS, 1982

[32] J. Postel, “Assigned Numbers”, RFC 1700, Outubro 1994.

[33] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, Março 1992.

Referências relativas a Suporte de Qualidade de Serviço

[34] S. Blake, ed., “An Architecture for Differentiated Services”, RFC 2475, Dec 1998.

[35] K. Nichols, ed., “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”, RFC 2474, Dezembro 1998

[36] B. Davie, ed., “An Expedited Forwarding PHB (Per-Hop Behavior)”, RFC 3246, Março 2002

[37] J. Heinanen, ed., “Assured Forwarding PHB group”, RFC 2597, June 1999

[38] B. Braden, ed., “Recommendations on Queue Management and Congestion Avoidance in the Internet.”, RFC 2309, Abril 1998.

[39] P Fergunson, D. Senie, “Integrated Services in the Internet Architecture: an Overview”, RFC 1633, Junho 1994.

[40] S. Floyd, V. Jacobson, “Link-sharing and Resource Management models for packet networks”, IEEE/ACM Transactions on Networking 3(4), 1995

Referências relativas ao 802.11

[41] IEEE, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, IEEE Std. 802.11, 1997.
http://standards.ieee.org/getieee802/download/802.11-1999.pdf

[42] IEEE, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer Extension in the 2.4 Ghz Band”, IEEE Std. 802.11b, 1999.
http://standards.ieee.org/getieee802/download/802.11b-1999.pdf

[43] IEEE Std. 802.11f/D3, “Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation”, (Draft Supplement to IEEE Std 802.11, 1999 Edition), January 2002

[44] A. Grilo, M. Macedo, M. Nunes, “Service Disciplines for Support of Inteserv and Diffserv in IEEE 802.11 Access networks”, draft paper, 2001

Referências genéricas de redes e sistemas distribuidos

[45] S. A. Tanenbaum – “Computer Networks”, 3nd Edition, Prentice Hall International, 1996

[46] S. Keshav, S; “An Engineering Approach to Computer Networking, ATM Networks, The Internet and the Telephone Network”, AT&T Research, Addison-Wesley Publishing, 1997.

[47] Alves Marques, Paulo Guedes, "Tecnologia de Sistemas Distribuídos", FCA editora, 1998

Referências genéricas do Sistema Operativo Linux

[48] Matt Welsh, "Linux Installation and Getting Started" , Linux Documentation Project, 1996

[49] Matt Welsh, Lar Kaufman, "Running Linux", O'Reilly & Associates inc., 1995

[50] Lars Wirzenius, "Linux System Administrators' Guide 0.6", Linux Documentation Project, 1997

[51] L. Torvalds, “Linux kernel release 2.4.xx REAME”, incluído no kernel, Outubro 2001

Referências relativas à componente de Rede do Linux

[52] G. Dhandapani, A. Sundaresan, “Netlink Sockets – Overview”, Information and Telecommunications Technology Center, Department of Electrical Engineering &

Computer Science, The University of Kansas, 1999, http://qos.ittc.ukans.edu/netlink/html/index.html

[53] G. Herrin, “Linux IP Networking - A Guide to the Implementation and Modification of the Linux Protocol Stack”, Maio 2000, http://kernelnewbies.org/documents/ipnetworking/linuxipnetworking.html

[54] Olaf Kirch, "The Network Administrators' Guide", Linux Documentation Project, 1996

[55] Terry Dawson, Linux NET-3-HOWTO (Linux Networking), Linux Documentation Project, 1998

[56] Paul Gortmaker, Linux Ethernet-Howto, Linux Documentation Project, 1998

[57] A. N. Kuznetsov, "IP Command Reference", IPRoute2 Documentation, 1999

[58] A. N. Kuznetsov, "Tunnels over IP in Linux-2.2", IPRoute2 Documentation, 1999

[59] Bob Edwards, “Proxy ARP Subnetting HOWTO”, Linux Documentation Project, 1997

[60] Alessandro Rubini, "Linux Device Drivers", O'Reilly & Associates inc., 1998

[61] Fred N. van Kempen, "ARP Man Page", Linux Programmer's Manual, net-tools Documentation, 1999

[62] Fred N. van Kempen, "Ifconfig Man Page", Linux Programmer's Manual, net-tools Documentation, 1997

[63] Phil Blundell, "Route Man page”, Linux Programmer's Manual, net-tools Documentation, 1997

[64] T. Carstens, “Programming with pcap”, http://www.tcpdump.org/pcap.htm, 2001

Referências relativas ao controlo de tráfego em linux

[65] W. Almesberger, “Linux Network Traffic Control - Implementation Overview (kernel 2.4)", Fevereiro 2001, ftp://icaftp.epfl.ch/pub/people/almesber/junk/tc-04FEB2001-0.ps.gz

[66] W. Almesberger, et al, "Differentiated Services on Linux", June 1999 (draft-almesberger-wajhak-diffserv-linux-01.txt) ftp://icaftp.epfl.ch/pub/linux/diffserv/misc/dsid-01.ps.gz, http://diffserv.sourceforge.net

[67] S. Radhakrishnan, “Linux - Advanced Networking Overview”, Information and Telecommunications Technology, Center Department of Electrical Engineering & Computer Science, The University of Kansas Lawrence, 1999, http://qos.ittc.ukans.edu/howto/index.html

[68] B. Hubert , et al, “Linux Advanced Routing & Traffic Control HOWTO”, Setembro 2000, http://lartc.org/howto/

[69] M. Devera, “HTB Linux queuing discipline manual”, http://luxik.cdi.cz/~devik/qos/htb/, Fevereiro 2002

[70] Pedro Catelas, José António Neves, “Monitorização de Qualidade de Serviço em redes IP com Serviços Diferenciados”, Relatório de Trabalho Final de Curso, Setembro 2002

[71] Rui Prior, “Qualidade de Serviço em Redes de Comutação de Pacotes”, Março 2001, http://telecom.inescn.pt/doc/msc/rprior2001_pt.html

[72] K. Wagner, “Short Evaluation of Linux's Token-Bucket-Filter (TBF) Queueing Discipline”, http://www.docum.org/stef.coene/qos/docs/other/tbf02_kw.ps, Maio 2001

Referências relativas aos Testes

[73] Rick Jones, "Network Performance Home Page" http://www.netperf.org/netperf/NetperfPage.html

[74] B. Adamson, Naval Research Laboratory (NRL): “Multi-Generator (MGEN) Toolset”, Version 3.1, http://manimac.itd.nrl.navy.mil/MGEN/

[75] G. Java, “IPTraf User's Manual”, Maio 2002, http://cebu.mozcom.com/riker/iptraf/2.7/manual.html

[76] Tcpdump group, Tcpdump Users Manual, http://www.tcpdump.org/tcpdump_man.html, 2002

[77] Richard Sharpe, Ed Warnicke, “Etheral User’s Manual”, http://www.ethereal.com/docs/user-guide/, 2002

[78] Moicane Deliverable D15, “Applications Documentation”, D15/ICCS/WP4/V1.0, Março 2002.

Referências relativas ao hardware 802.11 (Chipset Prism)

[79] Intersil, “PRISM Driver Programmer’s Manual v2.0”. Intersil Restricted Distribution.

[80] Intersil, “Product Development Software Release Form – Cw10 Tertiary Firmware” Intersil Restricted Distribution.

[81] J. Malinen, “Host AP driver for Intersil Prism2”, http://hostap.epitest.fi/, Setembro 2002

[82] J. Malinen, “Host AP ChangeLog”, http://hostap.epitest.fi/cgi-bin/viewcvs.cgi/*checkout*/hostap/ChangeLog?rev=HEAD&content-type=text/plain, Setembro 2002

[83] AbsoluteValue Systems, “Linux-wlan Project”, ftp://ftp.linux-wlan.org/pub/linux-wlan-ng/, Setembro 2002

[84] P. Miranda, R. Nunes, “Suporte de Qualidade de Serviço em Redes Sem Fios 802.11b”, Relatório de Trabalho Final de Curso, Setembro 2000

[85] Lucent Technologies, “Roaming with WaveLAN/IEEE 802.11”, WaveLAN Technical Bulletin 021/A, Decembro 1998

[86] D. Hinds, “Linux PCMCIA HOWTO”, http://pcmcia-cs.sourceforge.net/

[87] J. Tourrilhes, “Linux Wireless LAN Howto”, http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.html

[88] J. Tourrilhes, “Wireless Extensions for Linux”, http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.Extensions.html

Referências relativas a Trabalhos nesta área do Autor

[89] P. Estrela, A. Grilo, T. Vazão e M. Nunes, "Terminal Independent Mobile IP (TIMIP)", Internet draft, draft-estrela-timip-00.txt, work in progress, Março 2002.

[90] P. Estrela, "Estudo e Implementação da Macro-Mobilidade na Internet", Relatório de Trabalho Final de Curso (Regime Integrado), Setembro 2000

[91] P. Estrela, "Mobilidade em IP – "Estado da Arte ", Trabalho Final da Cadeira de Tópicos Avançados em Conectividade e Sistemas Distribuídos, Abril 2002

[92] P. Estrela, "Rede de acesso do MOICANE", Trabalho Final da Cadeira de Redes de Acesso Multi Serviço, Fevereiro 2002

Glossário

Estrangeirismo	Tradução
(tráfego) downlink/ downstream	(tráfego) no sentido descendente, *para* os terminais
(tráfego) uplink/ upstream	(tráfego) no sentido descendente, *dos* terminais
“early drop”	perda antecipada
access point	ponto de acesso
acknowledge	mensagem de confirmação
beacon	sonda
border router	encaminhador fronteira
bridge	encaminhador de nível 2
crossover	primeiro nó comum entre os dois caminhos envolvidos num handover, desde os terminais até ao topo da árvore de nós.
default router	encaminhador por omissão
digest	resumo de dados calculado por processos de hashing
driver	controlador
edge router	encaminhador fronteira
gateway	encaminhador central em domínios TIMIP
handover	(processo de) transição de terminais
handshake	processo de estabelecimento de uma ligação
hashing	
host	terminal IP ou encaminhador IP
legacy	legado
management	gestão
mobile host	terminal móvel
overhead	ineficiência/peso de protocolos de comunicação
performance	desempenho
poll	autorizações explícitas de acesso ao meio em 802.11 por parte do AP
premium	(tratamento) distinguido
proxy	(entidade) que efectua qualquer acção em nome de outra, sendo

	esta pedida explicitamente
rate	ritmo/débito
roaming	transição
router	encaminhador de nível 3
routing	encaminhamento
scheduler	calendarizador/escalonador
soft state	característica do *estado* que é automaticamente eliminado se não for utilizado
stack	pilha (de protocolos)
standard	normalizado
surrogate	(entidade) que efectua qualquer acção em nome de outra, sem que tal seja pedida tanto implícita como explicitamente
switches	encaminhador de nível 2 entre tecnologias de rede iguais
timeout	terminação do limite de tempo
timestamp	marcação temporal
video on demand	vídeo a pedido

Abreviatura	Significado
802.11	Wireless LAN, WaveLan
802.3	IEEE 802.3 (Ethernet)
AF	Assured Forwarding
ANG	Access Network Gateway
AP	Access Point
API	Application Programming Interface
ARP	Address Resolution Protocol
BB	Bandwidth Broker
BE	Best Effort
BR	Border Router
BS	Base Station
CBQ	Class Based Queuing
CIDR	Classless Inter Domain Routing
CIP	Cellular IP
CL	Controlled Load
COPS	Common Open Policy Server
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DIFFSERV	Differentiated Services
DSCP	Differentiated Services Code Point
EF	Expedited Forwarding
ETSI	European Telecommunications Standards Institute
FA	Foreign Agent
FCS	Frame Check Sequence
FIFO	First in First out
FTP	File Transfer Protocol
GW	Gateway
HA	Home Agent
HAWAII	Handoff-Aware Wireless Access Internet Infrastructure
HDRR	Home Domain Root Router
ICMP	Internet Control Message Protocol
IEEE	Institute for Electric and Electronics Engineering

IETF	Internet Engineering Task Force
INESC	Instituto Engenharia de Sistemas e Computadores
INESC	Institute of Engineering of Systems and Computers
INOV	INESC Inovação
INTSERV	Integrated Services
IP	Internet Protocol
ISO	International Standards Organization
ISP	Internet Service Provider
Kbit/s	Kilobits por segundo
LAN	Local Area Network
LLC	Logical Link Control
LOS	Line of Sight
LT	Legacy Terminal
MAC	Medium Access Control
Mbit/s	Megabits por segundo
MD5	Message Digest n5
MIB	Management Information Base
MIP	Mobile IP
MOICANE	Multiple Organisation Interconnection for Collaborative Advanced Network Experiments
MT	Mobile Terminal
MTU	Maximum Transfer Unit
NE	Network Element
NT	Network Termination
NTP	Network Time Protocol
OSI	Open Standards Initiative
PC	Personnel Computer
PHB	Per Hop Behaviour
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
QoS	Quality of Service
RED	Random Early Detection
RF	Radio Frequency

RFC	Request for Comments
RSVP	Resource Reservation Protocol
RTCP	Real-Time Control Protocol
RTP	Real Time Transport Protocol
SLA	Service Level Agreement
SNR	Signal to Noise Ratio
TCP	Transmission Control Protocol
TIMIP	Terminal Independent Mobility for IP
UDP	User Datagram Protocol
VoD	Video on Demand
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WDS	Wireless Distribution System
WWW	World Wide Web