Relatório do Trabalho Final de Curso
(Regime Integrado)

Estudo e Implementação da Macro-Mobilidade na Internet

Autor: Pedro Vale Estrela Nº 42703
Orientador: Prof. Mário Serafim Nunes

IST/INESC 2000

Resumo

Este Trabalho Final de Curso vai analisar quais as tecnologias genéricas existentes que fornecem o suporte aos Terminais Móveis da Macro-Mobilidade – o tipo de Mobilidade relativa a grandes distancias geográficas, entre quaisquer Redes Locais distintas de uma mesma Rede Global. Este tipo de Mobilidade tem as suas próprias características derivadas desta grande escala, sendo analisada genericamente a implementação desta em Redes Globais que não tenham sido desenhadas com esta característica de Mobilidade.

Esta análise vai suceder ao estudo destes conceitos na Internet, a grande Rede de Dados Mundial, que é instanciada no novo protocolo Mobile IP. Este protocolo é a extensão do protocolo IP para a Mobilidade dos Terminais Móveis ao longo de toda a Internet, sendo esta adicionada de uma forma transparente para a infra-estrutura já existente.

Este estudo do Protocolo MIP vai levar à descrição da Implementação Prática deste protocolo em sistemas Linux, baseados em Computadores Pessoais, num ambiente Multi-Rede Ethernet. Esta implementação cobre convenientemente o protocolo MIP, sendo descritos Testes Funcionais que provam a aplicação da análise genérica inicial à Internet; esta implementação é também um bom ponto de partida para futuros desenvolvimentos no âmbito desta tecnologia.

Palavras chave: Mobile IP, Macro-Mobilidade, Terminal Móvel, Agentes Mobilidade, Linux, PCs, Ambientes “Wired”, Encapsulamento de Pacotes

Abstract

In this Document, it will be described which generic technologies exists today that can support the Mobile Host's Macro-Mobility in a Global Network. This type of Mobility is related to a very large scale of Host Movements, between any Local Area Network of a Global Network, and for this, it has it's own special characteristics. In addition, special insight is provided on the deployment of this type of mobility, regarding older Global Networks which weren't designed for Mobility.

Afterwards, these concepts will be developed in the Internet, by the means of a new protocol called Mobile IP. As it name implies, this protocol is an extension to the standard IP protocol, which adds Macro-Mobility capabilities to the Mobile Hosts through the Internet, without changing the whole infrastructure already deployed.

After the description of the MIP protocol and its capabilities, an implementation of the protocol will be outlined, which has been developed in the Linux Operating System, on a Multi-LAN environment based on Ethernet LANs. As Functional Tests shown, this work is a fairly complete implementation of the protocol, and it's also a good starting point for future work in this area.

Keywords - Mobile IP, Macro-Mobility, Mobile Host, Mobile Agents, Linux, PCs, "Wired" Environments, Packet Encapsulation

Índice Geral:

ÍNDICE DE FIGURAS:

1 – Introdução

Neste Trabalho Final de Curso vão ser estudadas e implementadas as mais recentes tecnologias genéricas que suportam a mobilidade de terminais de Dados e Voz, em redes Públicas e Privadas, tendo uma especial relevância para a implementação destas funcionalidades na Internet. Actualmente a mobilidade física dos terminais está a tornar-se uma necessidade cada vez maior, uma vez que são já comuns os terminais móveis de Dados (PCs Portáteis equipados com a tecnologia "Wireless", PDAs) e de Voz (Telefones "Wireless", Terminais DECT), em que os utilizadores exigem uma conectividade constante dos seus equipamentos, em todas as localizações físicas. Neste sentido, têm que ser assegurados e criados os mecanismos necessários para que estes terminais possam ter a todo o momento uma ligação permanente, fiável e segura, qualquer que seja a sua localização física actual. Por outro lado, o domínio incontornável da Internet como a grande Rede de Dados Mundial (e previsivelmente, no futuro, também como rede de Voz) obriga a que esta inclua estes mecanismos para ser capaz de suportar esta nova geração de utilizadores.

Os mecanismos que suportam esta Mobilidade são divididos em dois grandes grupos, de acordo com a **escala** pretendida de Mobilidade. É este factor que vai determinar as diferentes características de cada grupo, como as diferentes eficiências esperadas, a frequência das movimentações dos terminais, os atrasos esperados e as perdas aceitáveis de pacotes de informação. Esta divisão vai-se encaixar bem no modelo OSI de camadas de protocolos, podendo-se considerar o suporte à mobilidade de uma forma diferenciada nos níveis 2 (nível "Data-Link") e 3 (nível Rede) do Modelo OSI.

Assim, a **Micro-Mobilidade** (também denominada de **Mobilidade Horizontal**) está relacionada com os mecanismos necessários para garantir a mobilidade de um Terminal Móvel numa área geográfica pequena, como uma rede local IP formada por um conjunto de Estacões de Base "Wireless", ou um conjunto de células GSM na rede pública móvel. Esta escala geográfica está implicitamente associada ao nível 2 OSI, pelo que genericamente o suporte da micro-mobilidade numa rede local estará localizado neste nível OSI.

Para as redes que se estendem por uma escala geográfica superior (a uma escala Nacional ou mesmo Mundial), formadas pelo conjunto de diversas redes locais ligadas entre si por encaminhadores (as WANs, exemplificadas na **figura 1**), este nível de mobilidade apenas vai permitir que os terminais móveis tenham a liberdade de se deslocarem no interior da sua Rede Local. Para suportar a mobilidade dos terminais móveis em todo o domínio da WAN vai ser necessário um novo nível de mobilidade, a chamada **Macro-Mobilidade** (também intitulada de chamada ou **Mobilidade Vertical**). Esta mobilidade tem características substancialmente diferentes da forma de mobilidade anterior, o que leva a que o seu suporte esteja presente apenas no nível 3

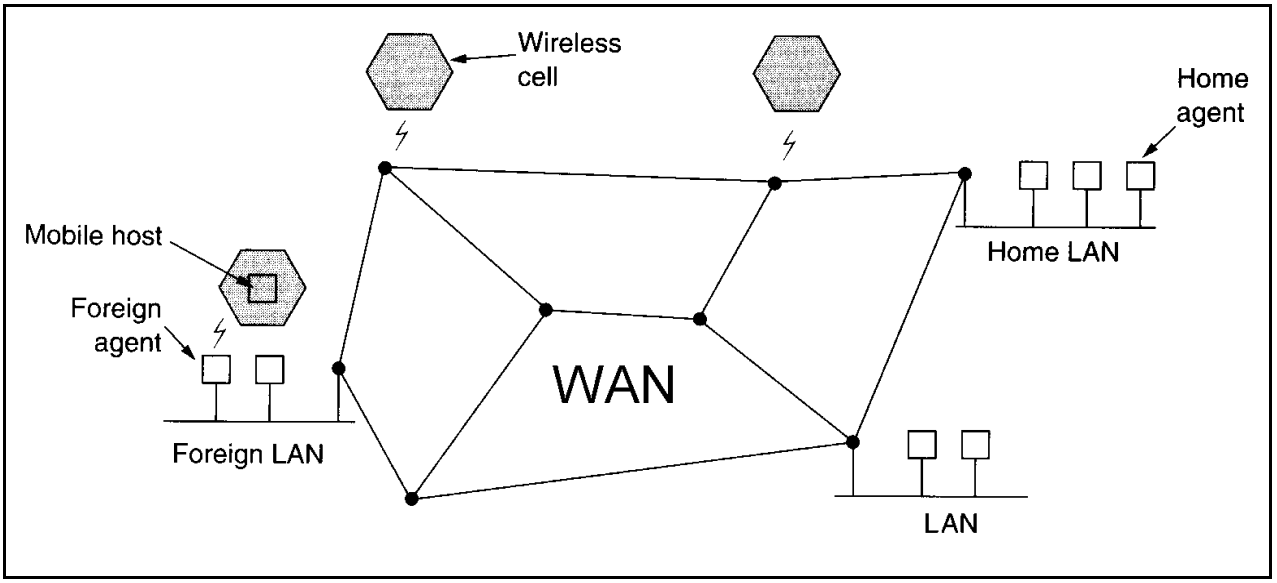


Figura 1 - Uma WAN formada por várias LANs

OSI.

Para a aplicação prática da Macro-Mobilidade em redes públicas e privadas existem duas tecnologias diferentes, vocacionadas para dois tipos de redes de grande escala (WANs) totalmente distintas – o protocolo MIP ("Mobile IP" – IP Móvel) [1] e o sistema GPRS ("General Packet Radio Service") [2].

O Protocolo **MIP** especificado pelo IETF ("Internet Engineering Task Force") oferece o suporte à Macro-Mobilidade ao longo de toda a extensão da Internet, através de um conjunto de extensões ao protocolo IP que dão a liberdade a qualquer "host" IP de transitar livremente e sem quaisquer limitações entre diferentes redes IP (isto é, diferentes redes locais). Tal como o IP, este protocolo é completamente genérico, podendo ser baseado sobre qualquer tipo de redes (Redes "Wireless", Redes "Wired", Ligações Ponto-a-Ponto), não requerendo quaisquer modificações nos protocolos específicos de suporte ao meios físicos já existentes. Por outro lado, todos os diferentes protocolos de nível superior (de nível Aplicação como o HTTP, o FTP ou o TELNET) também irão ficar completamente inalterados com a introdução da mobilidade ao nível do IP, dado que o MIP é apenas uma extensão do IP. Além da vantagem da generalidade, o MIP é também passível de implementação com um nível de alterações mínimo em relação às infra-estruturas já existentes, uma vez que apenas requer que alguns "hosts", bem definidos, tenham que possuir o suporte da Macro-Mobilidade.

Na rede pública GSM ("Global System for Mobile Communications")está neste momento a ser introduzido o **sistema GPRS** como extensão para comunicação orientada a pacotes. Embora o GPRS inclua diversos princípios do MIP, ao contrário deste é totalmente dependente da tecnologia GSM, pelo que não poderá ser utilizado em qualquer rede, como o IP. Por outro lado o débito oferecido pelo GPRS encontra-se limitado a 120 Kbps por célula GSM [2], o que faz com que seja neste momento apenas adequado a aplicações específicas para redes móveis, como as aplicações WAP.

O objectivo deste Trabalho Final de Curso é estudar em diferentes tipos de sistemas já existentes (redes de Dados) a **Macro-Mobilidade**, tendo uma especial relevância para implementação destes conceitos na Internet. Quando esta tecnologia for completamente dominada e implementada, será posteriormente aprofundada num contexto mais complexo no qual se integram os dois tipos de mobilidade de forma a obter a **Mobilidade Total**.

Pelas vantagens anteriormente referidas, o protocolo MIP será estudado e implementado neste Trabalho, num ambiente multi-rede, em que cada rede local será baseada numa tecnologia "Wired" – a Ethernet. Cada Rede terá os seus agentes de mobilidade (os "routers" IP que implementam as extensões MIP) baseados em computadores pessoais com o Sistema Operativo Linux, o que vai simplificar a implementação deste protocolo uma vez que este sistema operativo, derivado do Unix, oferece grandes funcionalidades e flexibilidades relacionadas com todas as tecnologias de "networking".

Uma vez este passo atingido (e estando assim criado um ambiente sólido e testado de trabalho do MIP) poder-se-á avançar para outras aplicações da Macro-Mobilidade a desenvolver no seguimento deste Trabalho Final de Curso.

O presente relatório está estruturado em 6 capítulos e 8 Anexos. Nas restantes secções deste Capítulo é efectuada uma análise sumária dos 2 tipos de mobilidade apresentadas: Micro-Mobilidade e Macro-Mobilidade. No capítulo 2 vai-se analisar, recorrendo a exemplos, a criação da Macro-Mobilidade em qualquer rede de dados genérica, sendo esta dividida em 3 fases distintas. O capítulo 3 abordará a implementação da Macro-Mobilidade na Internet, sendo apresentado o protocolo MIP e a forma como este realiza as três fases referidas.

O capítulo 4 focará a implementação prática deste protocolo no stack TCP/IP do sistema operativo Linux, onde se aplicaram as considerações dos capítulos 2 (Redes Genéricas) e 3 (Internet). O capítulo seguinte vai focar os Testes Funcionais que foram efectuados à implementação do MIP desenvolvida, que provam a sua validade. O sexto e último capítulo é reservado às conclusões do trabalho realizado, sendo apresentada, igualmente, uma perspectiva de possíveis evoluções da solução desenvolvida.

Por último, a bibliografia de suporte a este Trabalho Final de Curso é presente no Capítulo 7, seguido de diversos Anexos com detalhes suplementares referenciados pelo texto.

1.1 – Descrição da Micro-Mobilidade

Uma rede que cubra uma área geográfica pequena (uma Rede Local) suporta a Mobilidade dos seus terminais quando permite que estes possam mover-se fisicamente sem quaisquer restrições no seu interior de uma forma automática e minimizando as perdas de pacotes de voz e dados; esta operação nunca deverá exigir a mudança do endereço do terminal, nem a quebra das ligações já estabelecidas com outros terminais.

Para garantir a mobilidade física considera-se normalmente meios de acesso de tecnologia "Wireless" [3] (redes DECT, redes 802.11, rede públicas GSM) em que os terminais podem, dentro da sua Rede, movimentar-se fisicamente sem restrições ao seu movimento, dado que a transmissão da informação é efectuada utilizando tecnologias de transmissão por rádio ou ondas de alta frequência. Nestes casos existirão diversas Estações de Base que estão espalhadas geograficamente, de forma a cobrir convenientemente a rede a concretizar, de tal forma que cada terminal deverá estar sempre no alcance de transmissão de (pelo menos) uma estação de base (**ver figura 2**).

Existem vários modelos possíveis para realizar a troca de pacotes entre terminais dentro da rede. Tipicamente, os terminais podem comunicar directamente entre si se estiverem no alcance um do outro; quando isso não acontece, os terminais vão trocar os seus pacotes de informação por intermédio das estações de base existentes.

É neste tipo de mobilidade que existem certas dificuldades relacionadas com a escala geográfica destas redes locais que são tratadas pelos protocolos de nível 2. Estas dificuldades estão relacionadas com a partilha do meio físico entre os diversos terminais, as diferentes qualidades de serviço disponíveis nas comunicações prestadas pela rede, a alocação de recursos partilhados (Banda) por parte dos terminais, a operação de mudança das comunicações já estabelecidas de estação de base em estação de base (denominada de "handover") exigida pelo movimento de um Terminal Móvel, a segurança das comunicações para garantir a confidencialidade destas, ou o tratamento do problema da "estação escondida" (relacionado com o **controlo** do acesso ao meio de uma forma **distribuída** quando este é partilhado por vários terminais e/ou estações de Base) [3].

Considerando apenas o nível 2 OSI, os terminais destas redes móveis só poderão comunicar uns com os outros utilizando os mecanismos disponibilizados por este nível, o que significa que

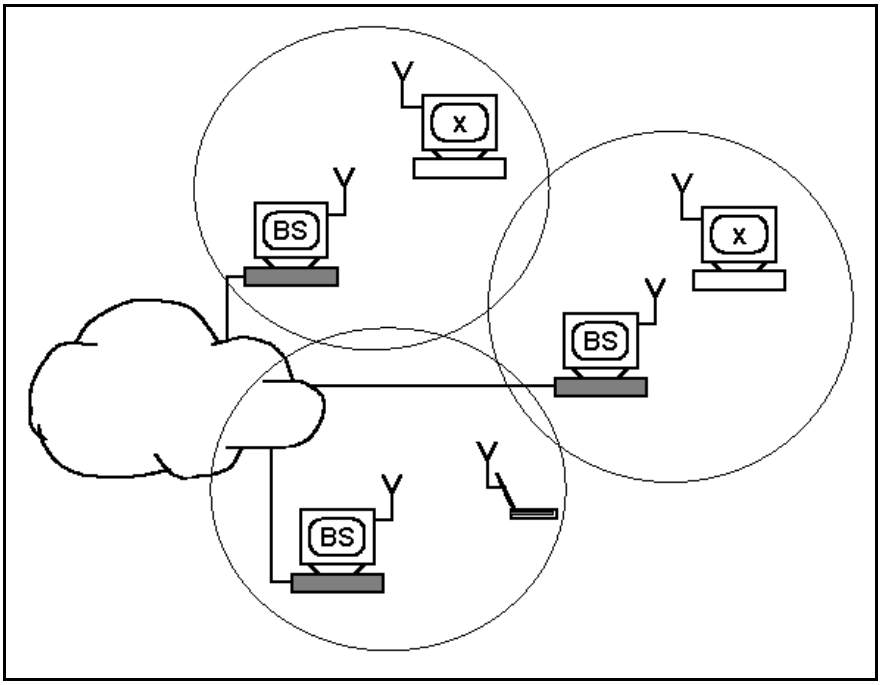


Figura 2 - Uma Rede Local Wireless com 3 Estações de Base

estes apenas poderão trocar pacotes com os outros terminais existentes na mesma rede móvel. Como tipicamente esta rede local vai estar integrada numa WAN que agrupe diversas LANs, vai ser da responsabilidade do nível 3 OSI o encaminhamento dos pacotes de informação destinados aos terminais que pertençam a outras redes distintas. Assim, e no contexto das redes móveis, tipicamente as redes locais "Wireless" irão estar ligadas umas às outras por intermédio de ligações "Wired", sendo estas ligações estabelecidas por encaminhadores ("routers"). Embora enderecem dois tipos de problemas semelhantes, os mecanismos de encaminhamento do nível 2 e 3 são completamente distintos, devido às diferentes escalas geográficas em que cada um opera.

1.2 – Descrição da Macro-Mobilidade

A Macro-Mobilidade é a forma de mobilidade que está associada às WANs [4] em que se pretende que os terminais móveis possam trocar o seu ponto de ligação à WAN sem quaisquer restrições, podendo percorrer desta forma grandes distâncias, ficando sucessivamente ligados a cada rede local (uma de cada vez) e transitando para outra quando saírem do interior da rede local actual. Este tipo de mobilidade terá que ser suportado no nível 3 OSI e tem os mesmos objectivos gerais da micro-mobilidade (embora adaptados para a escala geográfica superior). É importante verificar que a mobilidade física dos terminais, enquanto estão completamente contidos no interior de uma rede local, vai ser apenas da responsabilidade exclusiva da micro-mobilidade dessa rede, pelo que para a Macro-Mobilidade apenas são relevantes as transições dos terminais **entre** rede locais.

Assim, a Macro-Mobilidade terá que suportar diversas características que advêm da sua grande escala. A característica mais relevante da Macro-Mobilidade é que não existam limitações geográficas ao movimento do Terminal Móvel, isto é, que quando o terminal se ligar numa qualquer rede local da rede global este continue a ter a capacidade de enviar e receber pacotes de informação de uma forma transparente, sem obrigar necessariamente a modificações no estado das ligações, nos encaminhadores que estabelecem a ligação, nem nos terminais receptores das comunicações estabelecidas.

Outra característica decisiva prende-se com a importância de o Terminal Móvel ter de continuar sempre a ser acessível pelo seu endereço global (o endereço "fixo"), independentemente da sua localização ou meio de transmissão actual. Neste sentido, o interlocutor de um Terminal Móvel não terá que saber se está a comunicar com um **terminal fixo** que está na sua rede local habitual, ou se está a comunicar com um **Terminal Móvel** que está neste momento localizado numa qualquer outra rede local. Este requisito poderá ser eventualmente relaxado com vista a optimizar o desempenho dos mecanismos da mobilidade, sendo no entanto importante garantir que qualquer entidade possa comunicar com um Terminal Móvel da mesma forma que comunica com os terminais fixos "normais".

É necessário também que o momento da transição do Terminal Móvel de uma Rede Local para outra seja uma operação completamente automática e transparente, de forma a tentar reduzir ao mínimo o tempo em que o terminal vai estar não acessível (isto é, desligado da WAN). Só tendo em atenção este aspecto é que se poderá reduzir ao mínimo a quantidade de informação (pacotes de dados e voz) que o Terminal Móvel irá perder, quando este trocar o seu ponto de ligação à WAN.

Todas estas operações descritas terão necessariamente que ser efectuadas de uma forma segura e autenticada, de forma a garantir que as mudanças dinâmicas necessárias que suportam a Macro-Mobilidade no nível 3 OSI serão sempre concedidas apenas aos terminais móveis que foram explicitamente autorizados a realizá-las, de tal forma que o fluxo de informação do Terminal Móvel (que será redireccionado dinamicamente por estes processos), irá sempre para a localização real deste e não para outro qualquer ponto da WAN.

Qualquer implementação da Macro-Mobilidade (especialmente numa rede que não tenha sido desenhada desde o início para suportar a Macro-Mobilidade, como é o caso da Internet) terá por fim que ser o mais genérica possível, de forma a modificar sempre o mínimo da infra-estrutura já existente, sendo idealmente totalmente independente dos diferentes tipos de rede (nível 2) existentes.

2 - Análise da Macro-Mobilidade em Redes de Dados

2.1 - Conceitos Gerais

2.1.1 - Introdução

Tendo em conta as utilizações e os benefícios descritos da Macro-Mobilidade, vai ser descrita de seguida a forma como esta é disponibilizada aos utilizadores das redes de dados globais. Para este efeito, estas redes dividem-se em dois grupos, consoante a sua mobilidade "nativa":

O primeiro grupo integra as redes de dados mais antigas, com protocolos e implementações simples. Estas redes não tiveram desde o seu aparecimento a preocupação da Macro-Mobilidade nos seus protocolos, pelo que têm apenas um endereçamento **estático** para qualquer entidade constituinte da rede. É este tipo de endereçamento estático a principal razão da simplicidade dos protocolos de encaminhamento, mas o que também vai impossibilitar a Macro-Mobilidade **nativa** nestas redes, sendo a Internet o melhor exemplo deste grupo.

O segundo grupo integra as redes de dados mais recentes, que têm protocolos de encaminhamento mais poderosos e complexos do que as anteriores, que foram especificados com o suporte **explícito** à Macro-Mobilidade. Um exemplo deste grupo será o sistema GPRS, que é uma extensão de rede de pacotes à rede pública GSM. Dado que o GSM surgiu de início como uma rede global de terminais móveis de voz, que não têm restrições de mobilidade, esta rede tem automaticamente o suporte nativo à Macro-Mobilidade dos seus terminais.

As redes globais de dados mais antigas, com endereçamento estático, foram desenhadas considerando que os terminais nunca iriam sair dos limites de cada rede local. Desta forma, os endereços das entidades podem conter uma relação com a localização física destas, o que simplifica o seu encaminhamento por toda a rede: cada encaminhador só precisa de conhecer a localização de cada rede local, e não de cada entidade específica. No entanto, esta forma de endereçamento vai inviabilizar a Macro-Mobilidade nativa, uma vez esta assumpção implica que cada entidade terá sempre que estar localizada no interior da sua rede local, de forma a poder ser endereçada correctamente.

Nestas redes, que só têm endereçamento estático, a única hipótese de criar a Macro-Mobilidade será pela introdução de novas entidades de suporte (ou pela modificação das já existentes), que vão cooperar de forma a disponibilizarem a Macro-Mobilidade para os terminais móveis que a necessitem, utilizando apenas o endereçamento estático existente. Este processo é alcançado quando são efectuadas, dinamicamente, nestas entidades de suporte as acções necessárias para os terminais móveis deixarem de estar associados permanentemente às suas redes de origem.

Quando estes processos estão em curso, os terminais móveis irão ter a possibilidade de vaguear livremente por todas as redes que constituem a rede global, uma vez que haverá um processo de encaminhamento especial para estas entidades móveis. No entanto, terá que existir uma interoperabilidade perfeita com toda a restante rede, que continuará a utilizar o endereçamento estático habitual, pois esta não terá necessariamente que ser modificada para instanciar a Macro-Mobilidade na rede global. Desta forma os mecanismos que introduzem a Macro-Mobilidade em redes de dados globais terão que ser **transparentes**.

2.1.2 - Terminologia

A Macro-Mobilidade irá introduzir as seguintes entidades, que podem ser derivadas das já existentes:

O **Terminal Móvel**, denominado de **"Mobile Host"**:
Esta entidade é o nó da rede global que pretende ter uma conectividade constante enquanto desfruta de uma mobilidade sem restrições. Isto significa que esta entidade poderá estar ligada à rede global por uma qualquer rede local, sendo o objectivo da

Macro-Mobilidade a criação de um endereçamento especial que seja independente da localização física desta entidade.

O **Agente de Mobilidade de Origem**, denominado de **"Home Agent":**
Esta entidade possibilita a Macro-Mobilidade dos terminais móveis de uma rede local. O Agente de Mobilidade de Origem é um encaminhador que está permanentemente localizado numa rede local e que cria as condições necessárias para que os **seus** terminais móveis (pertencentes a essa rede de origem) possam vaguear para qualquer outra parte da rede global. É esta entidade que tem a responsabilidade de gerir e controlar os **seus** terminais móveis que necessitam dos mecanismos da Macro-Mobilidade, aos quais reenvia os pacotes de informação que lhe são destinados para as suas localizações actuais.

O **Agente de Mobilidade de Visitantes**, denominado de **"Foreign Agent**":
Esta entidade é também um encaminhador com endereçamento fixo, sendo este o complementar do Home Agent. O Foreign Agent está permanentemente localizado numa rede local, e terá a responsabilidade de gerir e criar a Macro-Mobilidade para os terminais móveis que pertencem a outra rede, mas que estão neste momento localizados na sua rede local (terminais móveis visitantes). Para este efeito é esta entidade que possibilita a comunicação entre o Terminal Móvel e todos os outros nós da rede global, e que lhe entregará os pacotes que lhe são reenviados pelo Home Agent.

Os outros nós da rede global em geral, denominados de "**Hosts**"**:**
Todos os outros nós já existentes na rede global com qual o Terminal Móvel vai comunicar não terão que ser alterados, continuando sempre a referenciar o Terminal Móvel utilizando o seu endereço fixo. Esta característica significa que a adição da Macro-Mobilidade a estas redes globais de dados será um processo transparente. Opcionalmente, estas entidades podem ser também acrescidas da Macro-Mobilidade, o que apenas vai tornar o processo de encaminhamento especial para os terminais móveis mais eficiente.

Os outros encaminhadores da rede global em geral, denominados de "**Routers**"**:**
Todos os outros encaminhadores da rede global, quer estejam localizados no núcleo da rede global, ou que apenas façam a ligação entre redes locais, vão apenas encaminhar os pacotes que os outros Hosts estão a trocar com o Terminal Móvel (embora possam também estabelecer ligações com este). Estes encaminhadores também não têm necessariamente que ser acrescidos da Macro-Mobilidade, continuando a efectuar um endereçamento estático relativamente aos terminais móveis; No entanto, estas entidades também podem ser acrescidas da Macro-Mobilidade com vista a tornar o encaminhamento mais eficiente.

2.1.3 - Exemplo de Aplicação

De seguida vai ser descrito pormenorizadamente o processo da Macro-Mobilidade nas redes de dados, com o recurso ao exemplo representado nas **figuras 3 a 5**:

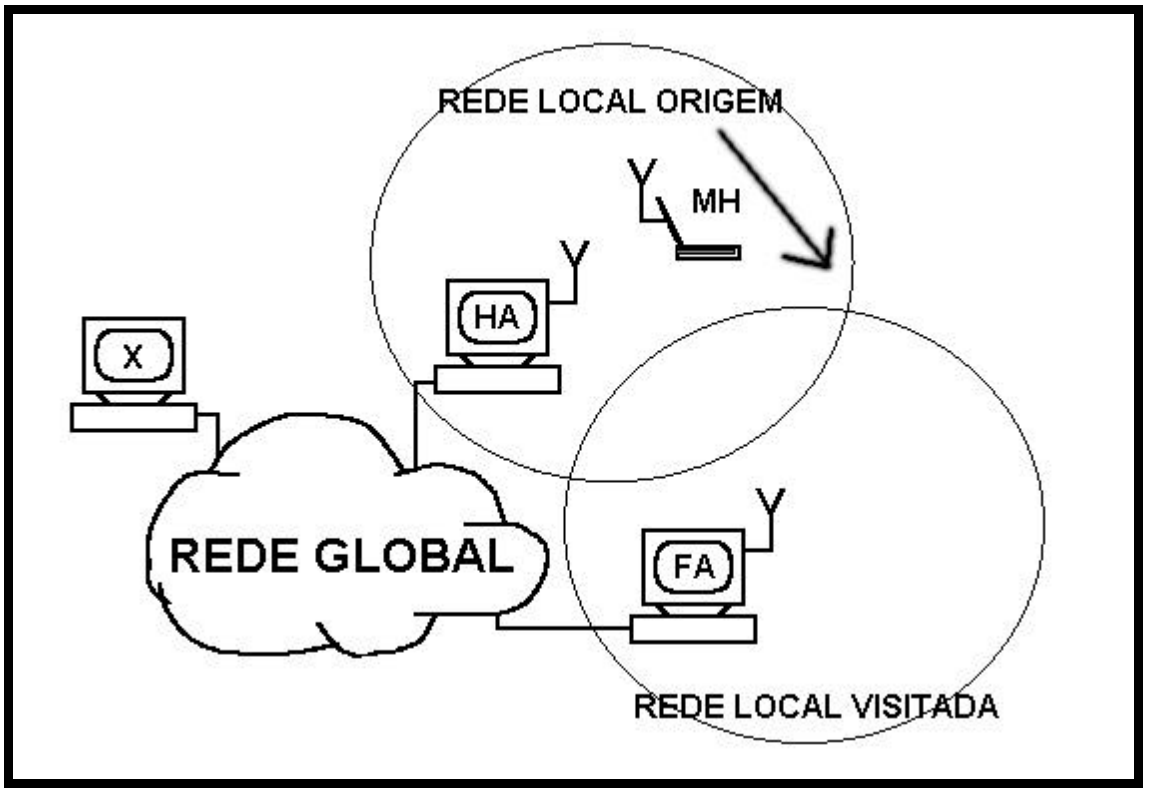


Figura 3 - Um Terminal Móvel MH vai mudar a sua localização física.

Na situação inicial, representada na **figura 3**, um Terminal Móvel **MH** está a comunicar com um nó da rede Global (denominado por **X**), estando localizado fisicamente na sua rede de origem. Nesta situação, o endereçamento estático vai resultar em pleno, dado que o endereço fixo do Terminal Móvel corresponde à sua localização física actual. Os mecanismos normais de encaminhamento existentes na rede global são suficientes para garantir a conectividade do Terminal Móvel, porque encaminham correctamente os pacotes de informação trocados com o seu interlocutor pela "nuvem" de encaminhadores e outras redes locais. Embora o Terminal Móvel esteja a movimentar-se, enquanto estiver no interior da sua rede local de origem, nunca perderá a conectividade, porque a Micro-Mobilidade da rede "wireless" é suficiente para entregar correctamente todos os pacotes destinados ao Terminal Móvel.

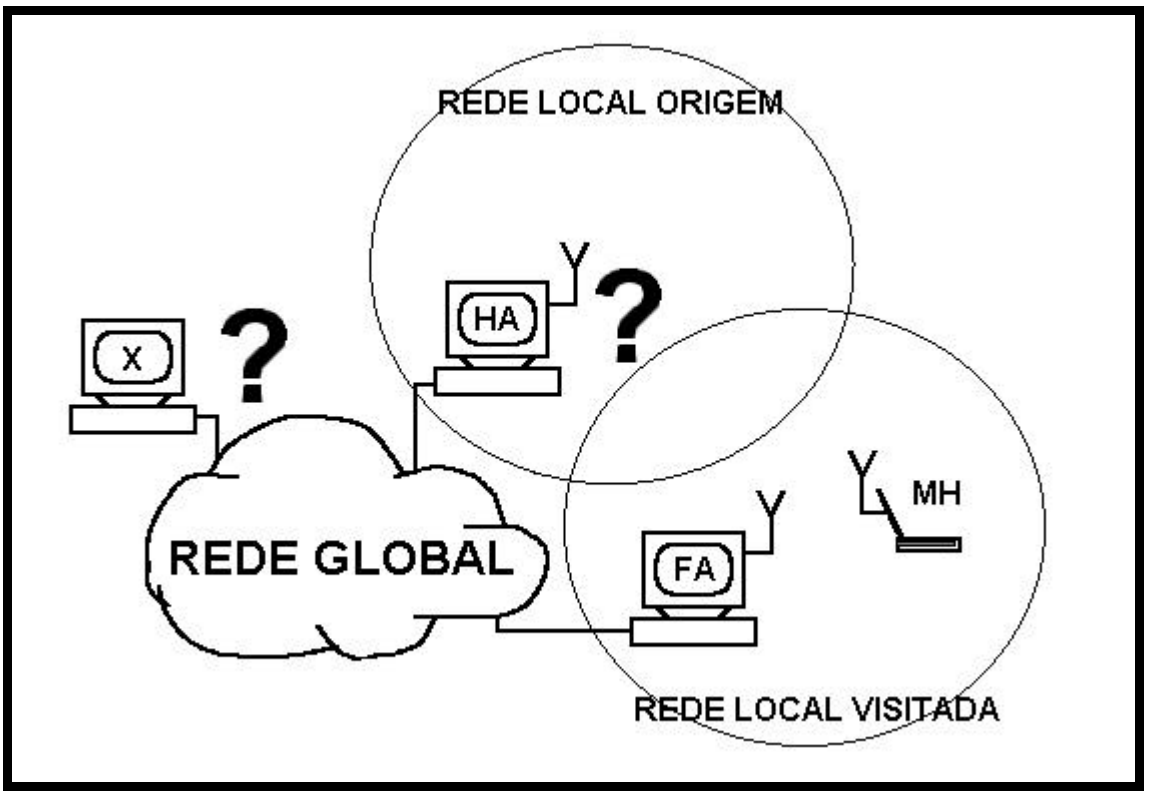


Figura 4 - Sem a Macro-Mobilidade, o Terminal Móvel perde a conectividade.

Na situação representada na **figura 4**, o mesmo Terminal Móvel moveu-se fisicamente de tal forma que saiu da sua rede de origem, estando agora no interior de uma outra (a rede visitada). Sem a Macro-Mobilidade, a conectividade do Terminal Móvel será interrompida, dado que o seu endereço fixo corresponde apenas ao interior da sua rede de origem.

Assim, o último encaminhador (o nó **HA**, na figura) não irá encontrar o Terminal Móvel no interior da sua rede, onde o seu endereço estático indica que terá que estar fisicamente localizado. Neste sentido, o encaminhador vai informar o interlocutor do Terminal Móvel que este não se encontra contactável. O nó **X** vai tentar de novo a ligação até que, eventualmente, vai desistir quando assumir que o Terminal Móvel foi desligado.

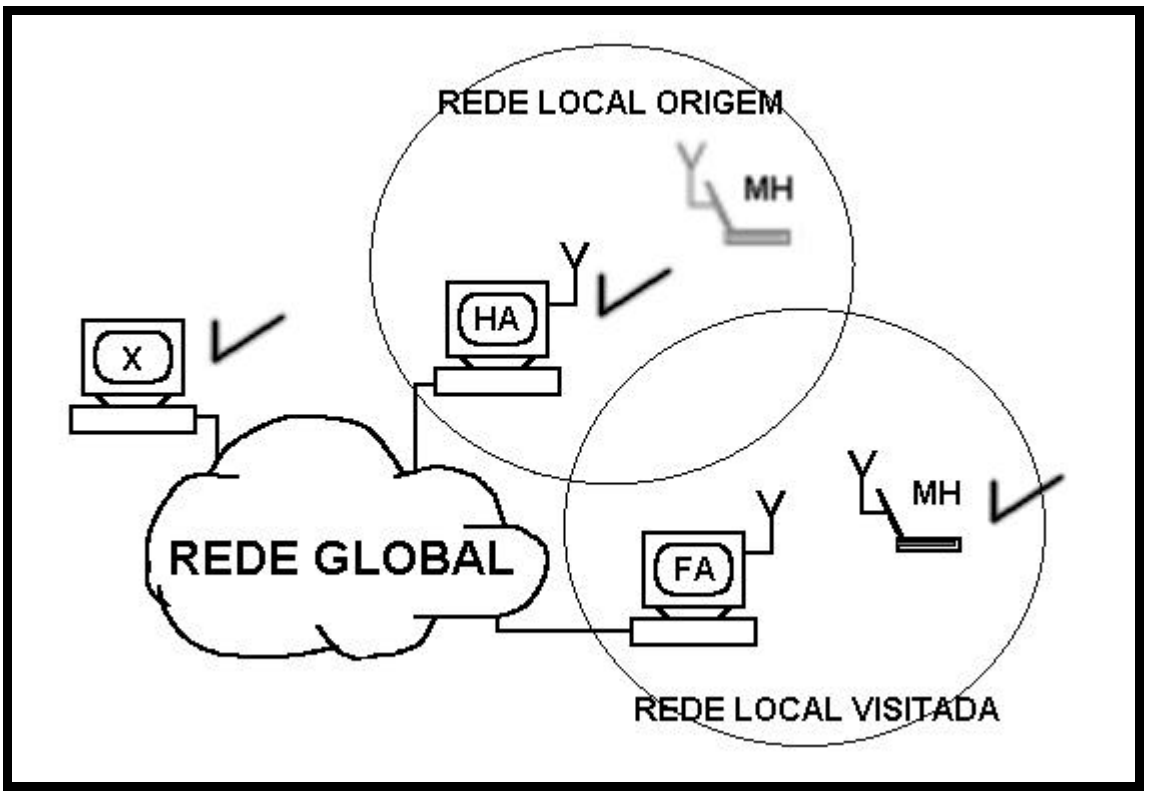


Figura 5 - Com a Macro-Mobilidade, o Terminal Móvel tem sempre conectividade mesmo com endereçamento estático.

Com os mecanismos de Macro-Mobilidade (**figura 5**), o Terminal Móvel vai poder verificar que já não se encontra na sua rede de origem (**fase de localização**), pelo que vai encontrar e comunicar com o Foreign Agent **FA**. Seguidamente, irá contactar o seu Home Agent **HA** (**fase de registo**) de forma a registar-se. Este, se aceitar, cria os mecanismos necessários para entregar os pacotes destinados ao Terminal Móvel para a sua localização actual, junto do Foreign Agent (**fase de execução**). Assim, os pacotes que o nó **X** está a enviar ao Terminal Móvel vão ser recebidos pelo Home Agent (em nome do Terminal Móvel), e enviados pelos mecanismos de endereçamento normal ao Foreign Agent (dado que este é uma entidade fixa). Os pacotes enviados serão depois entregues, de forma directa (sem encaminhamento), ao Terminal Móvel.

Isto significa que todos os pacotes destinados ao Terminal Móvel são correctamente recebidos por este, esteja ele onde estiver, parecendo aos outros nós que o Terminal Móvel está sempre fisicamente localizado na sua rede de origem (representado na **figura 5** pela "sombra" do Terminal Móvel). Por outro lado, os pacotes que o Terminal Móvel emite aos seu interlocutor também vão ser entregues sem problemas, porque o destino desses pacotes é o nó fixo **X**, que é endereçável estaticamente.

Esta conjunção de características define que o Terminal Móvel passou a desfrutar de Macro-Mobilidade nestas redes de dados globais: consegue **enviar/receber** correctamente pacotes de informação para/de todos os nós da rede, independentemente da sua localização física.

Neste processo o Terminal Móvel tem um **papel activo**: uma vez que é este que se move, é também este que tem que tomar a iniciativa de se localizar, registar e manter a operação deste mecanismo activa. Por outro lado, o Home Agent é a **entidade reactiva** deste processo, uma vez que só age quando é contactado pelo Terminal Móvel no processo de registo. Por fim, o Foreign Agent tem um **comportamento passivo**, dado que neste processo serve apenas de apoio para as outras entidades poderem comunicar.

2.2 - Operações da Macro-Mobilidade

2.2.1 - Fase1 - Localização

O objectivo desta primeira fase do processo de Macro-Mobilidade é o de possibilitar ao Terminal Móvel a indicação permanente da sua localização física e dos agentes de mobilidade que existem no seu alcance, dado que será desta forma que o Terminal Móvel descobre quando é que transita de rede local. e em que situações é que necessita da Macro-Mobilidade.

Este mecanismo é baseado em mensagens especiais de localização, que os agentes de mobilidade emitem regularmente, se possível em difusão. Estas mensagens são transmitidas apenas no interior da rede local, sem serem encaminhadas para outras partes da rede global. Desta forma cada rede local terá as suas próprias mensagens de localização, pelo que a recepção destas mensagens pelos terminais móveis é o suficiente para estes tomarem conhecimento da sua localização actual e de qual o agente de mobilidade existente no seu alcance.

Quando o Terminal Móvel, pelas informações recolhidas por este processo, toma conhecimento que já não está no interior da sua rede de origem, vai deduzir em que rede está localizado e que Foreign Agent deverá contactar, de forma a iniciar o processo da Macro-Mobilidade. Este processo também é utilizado sempre que, devido ao seu movimento, o terminal muda de rede visitada, ou volta para o interior da sua rede de origem.

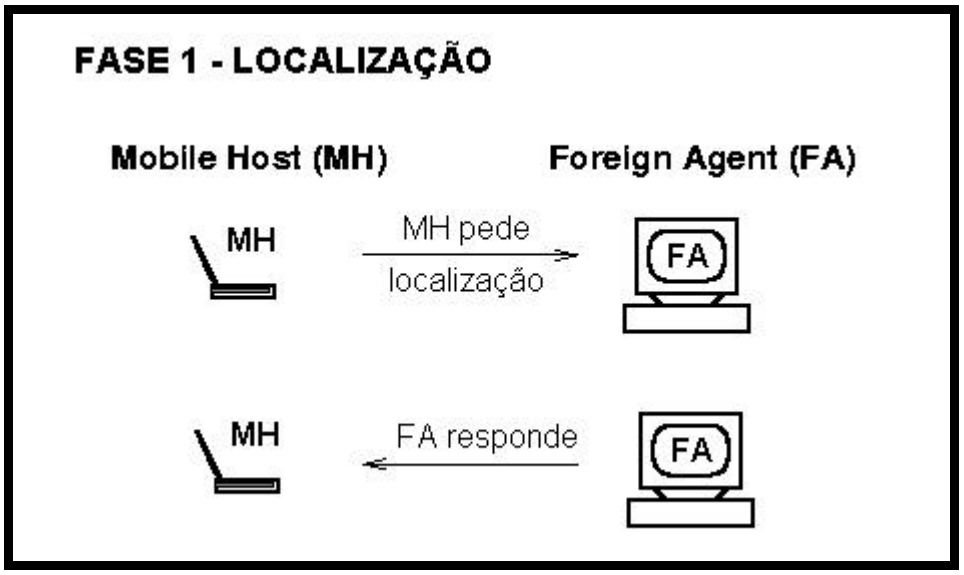


Figura 6 – Representação da fase de Localização

Por outro lado, se o Terminal Móvel suspeitar que já não se encontra na mesma localização, vai querer rapidamente a informação actualizada acerca da sua localização física. Para isso, o Terminal Móvel pode emitir um pedido de localização em todo o seu alcance (**figura 6**). Todos os agentes que receberem este pedido irão responder ao Terminal Móvel com anúncios de localização que são entregues ao Terminal Móvel em difusão. Desta forma, o Terminal Móvel vai tomar conhecimento de todos os agentes de mobilidade que estão próximos deste. Estas respostas podem ser também utilizadas para definir qual o agente a utilizar, isto é o que está mais próximo através da medição da intensidade dos sinais das respostas. Esta fase do processo de Macro-Mobilidade é activada periodicamente, pois é vital para o correcto conhecimento da localização física de cada Terminal Móvel.

Outra utilização desta fase está relacionada com as possíveis quebras de serviço dos agentes de mobilidade. Pelo processo descrito o terminal sabe sempre a todo o momento o estado do seu agente de mobilidade, de tal forma que se este falhar por qualquer razão o Terminal Móvel poderá rapidamente escolher um outro agente de mobilidade, activando as restantes fases do processo; quando o agente original voltar a estar activo, este poderá voltar a ser escolhido pelo Terminal Móvel, que se registará novamente.

2.2.2 - Fase2 - Registo

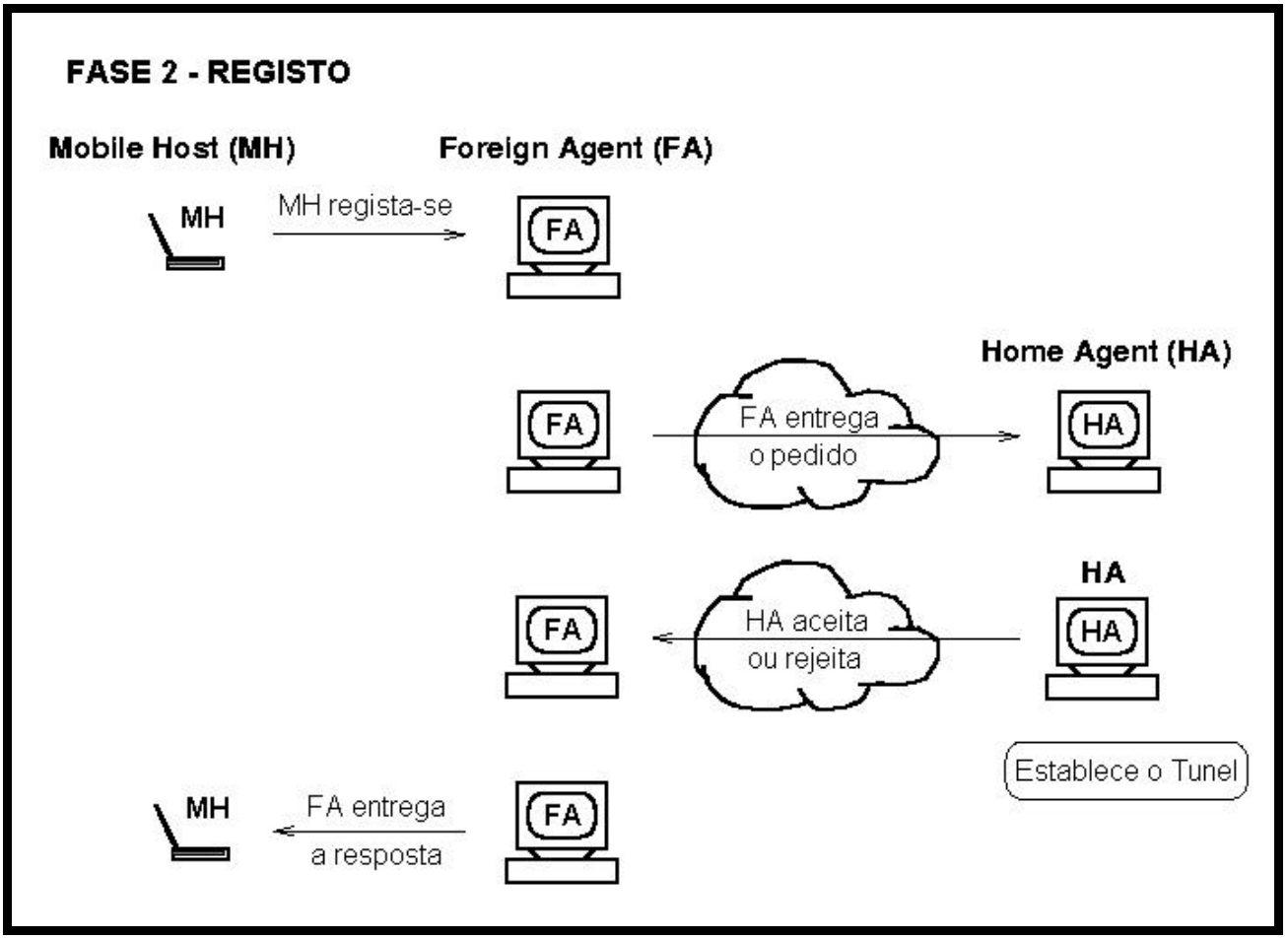


Figura 7 – Representação da fase de Registo

Esta fase é activada quando o Terminal Móvel chega à conclusão que já não está na mesma localização física que anteriormente estava, pelo que vai informar o seu Home Agent da sua localização física actual, pelos passos detalhados na **figura 7.** Assim, o Terminal Móvel vai formular o seu pedido de registo, no qual identifica a sua localização física, que é o endereço fixo do Foreign Agent escolhido.

O Terminal Móvel vai entregar o seu pedido de registo de uma forma directa ao Foreign Agent que tomará desta forma conhecimento da existência do Terminal Móvel visitante. O Foreign Agent poderá, quando receber o pedido de registo, recusar desde logo o serviço ao Terminal Móvel, por razões administrativas. Neste caso o processo irá recomeçar, tendo o Terminal Móvel que escolher um novo agente de mobilidade. Se o Foreign Agent aceitar o serviço ao Terminal Móvel, irá enviar, pelo mecanismo normal ao Home Agent indicado a mensagem de registo do Terminal Móvel.

Quando o Home Agent receber este pedido de registo irá ficar a conhecer a localização física do Terminal Móvel, dado que este está adjacente ao Foreign Agent que lhe enviou a mensagem. Se o Home Agent também estiver em condições de servir o Terminal Móvel, este vai criar os mecanismos de Macro-Mobilidade que vão possibilitar, na última fase do processo, que os pacotes destinados ao Terminal Móvel lhe sejam entregues na sua localização actual.

A resposta que o Home Agent emitir vai ser recebida pelo Foreign Agent, que saberá assim se o pedido de registo foi aceite; se o tiver sido, então o Foreign Agent irá também criar os mecanismos de Macro-Mobilidade para o Terminal Móvel.

Por fim a resposta dada pelo Home Agent vai ser entregue, de uma forma directa, ao Terminal Móvel que iniciou todo este processo. Se o registo teve sucesso então o Terminal Móvel

passa a estar contactável para todos os nós da rede global. Caso contrário, o terminal será informado da causa do insucesso, podendo eventualmente reparar o problema de forma a tentar um novo registo.

Esta fase de Registo é utilizada sempre que o Terminal Móvel muda de localização física. Assim sendo, quando o Terminal Móvel detecta que voltou à sua rede de origem, vai tomar as acções necessárias para terminar a sua Macro-Mobilidade, uma vez que nesta rede possui a conectividade normal de qualquer outro nó da rede global. Para este efeito o Terminal Móvel vai cancelar o registo no seu Home Agent, o que faz com que os mecanismos criados por este para o suporte à Macro-Mobilidade sejam terminados convenientemente. Outra situação em que o Terminal Móvel vai tomar a iniciativa de terminar a Macro-Mobilidade é quando sabe que não a vai utilizar durante um período alargado de tempo (quando o Terminal Móvel vai ser desligado, por exemplo).

Nesta fase do processo a característica mais importante das mensagens trocadas pelas entidades envolvidas é que estas terão necessariamente que serem autenticadas pelos seus emissores, de tal forma que os receptores tenham a absoluta certeza que as mensagens são enviadas pelas entidades que dizem ser, para só ai confiar sem reservas nas informações contidas nelas. Se esta precaução adicional não fosse tomada poderiam existir vários problemas de segurança potencialmente muito perigosos [4][5].

2.2.2.1 - Opções disponíveis nesta fase do Processo

Existem duas opções que podem ser utilizadas, consoante o número de entidades que têm o suporte da Macro-Mobilidade nas redes de dados. A primeira opção deverá ser utilizada quando se quer minimizar as entidades que têm de possuir o suporte à Macro-Mobilidade; a segunda será utilizada no caso oposto, em que se pode maximizar o número de entidades que têm este suporte.

A primeira opção considera que **só** os terminais móveis e os seus Home Agents têm que possuir o suporte à Macro-Mobilidade, dado que estas são as entidades mais fáceis de controlar, pelo facto de estarem necessariamente sobre o domínio da mesma organização; pelo contrário, a existência ou não de Foreign Agents nas redes visitadas já é algo que não se pode controlar facilmente, porque as redes visitadas já não são normalmente pertença da organização possuidora do Terminal Móvel.

Esta opção vai possibilitar que os terminais móveis continuem a ter Macro-Mobilidade nas redes visitadas que **não tenham Foreign Agents**, tendo os terminais móveis de arranjar alternativas para o serviço que era prestado pelo Foreign Agent:

- **Localização** - Os terminais móveis passam a ficar "cegos" relativamente às suas localizações físicas, uma vez que as mensagens de localização já não estão disponíveis. Assim, o Terminal Móvel tem que possuir uma outra forma de se localizar, tipicamente questionando outros encaminhadores genéricos existentes, que *podem* fornecer essas informações.
- **Endereço fixo para comunicar** - o segundo serviço prestado pelo Foreign Agent era o ser o ponto de apoio do Terminal Móvel, que possibilitava que este comunicasse com as outras entidades da rede global. Se o Terminal Móvel conseguir, por outros meios, alocar para o seu uso pessoal um **endereço fixo** da rede onde está localizado, de uma forma **temporária** durante a sua estadia nesta rede, poderá enviar e receber pacotes pelo novo endereço, o que vai possibilitar a sua comunicação com o seu Home Agent. O problema passa a ser a alocação desse endereço temporário, o que poderá novamente ser concretizado com a ajuda dos encaminhadores genéricos presentes nesta rede visitada.

Pelo processos descritos na fase de execução, os pacotes de dados destinados ao Terminal Móvel são enviados utilizando o endereçamento estático habitual para a sua Rede de Origem; uma vez aí o Home Agent vai reenviar estes pacotes para a localização física do Terminal Móvel (Foreign Agent ou endereço fixo temporário da rede visitada, como foi visto), o que implica que os

pacotes não percorrem tipicamente o caminho mais curto desde a sua origem até ao Terminal Móvel (dado que têm **sempre** que passar pelo Home Agent). Esta situação tem o nome de **triangulação** e vai implicar um maior atraso na entrega dos pacotes ao Terminal Móvel.

A segunda opção da fase do registo considera o caso oposto ao anterior, em que bastantes nós da rede global têm o suporte da Macro-Mobilidade. Nesta fase de registo, o Home Agent poderá contactar os interlocutores do Terminal Móvel e informá-los da verdadeira localização do Terminal Móvel. Se os interlocutores contactados não tiverem o suporte da Macro-Mobilidade, então todo o processo ficará inalterado; no entanto, se esta condição se verificar, então estes podem enviar os pacotes de informação directamente para a localização física do Terminal Móvel, pelo caminho mais curto existente, dado que estes já não têm passar pelo Home Agent. Este opção vai, resolver o problema da triangulação no encaminhamento dos pacotes para terminais que desfrutam de Macro-Mobilidade. Consegue-se garantir desta forma um maior desempenho relativamente ao caso normal de triangulação nomeadamente nos aspectos relativos aos atrasos.

2.2.3 - Fase3 - Execução

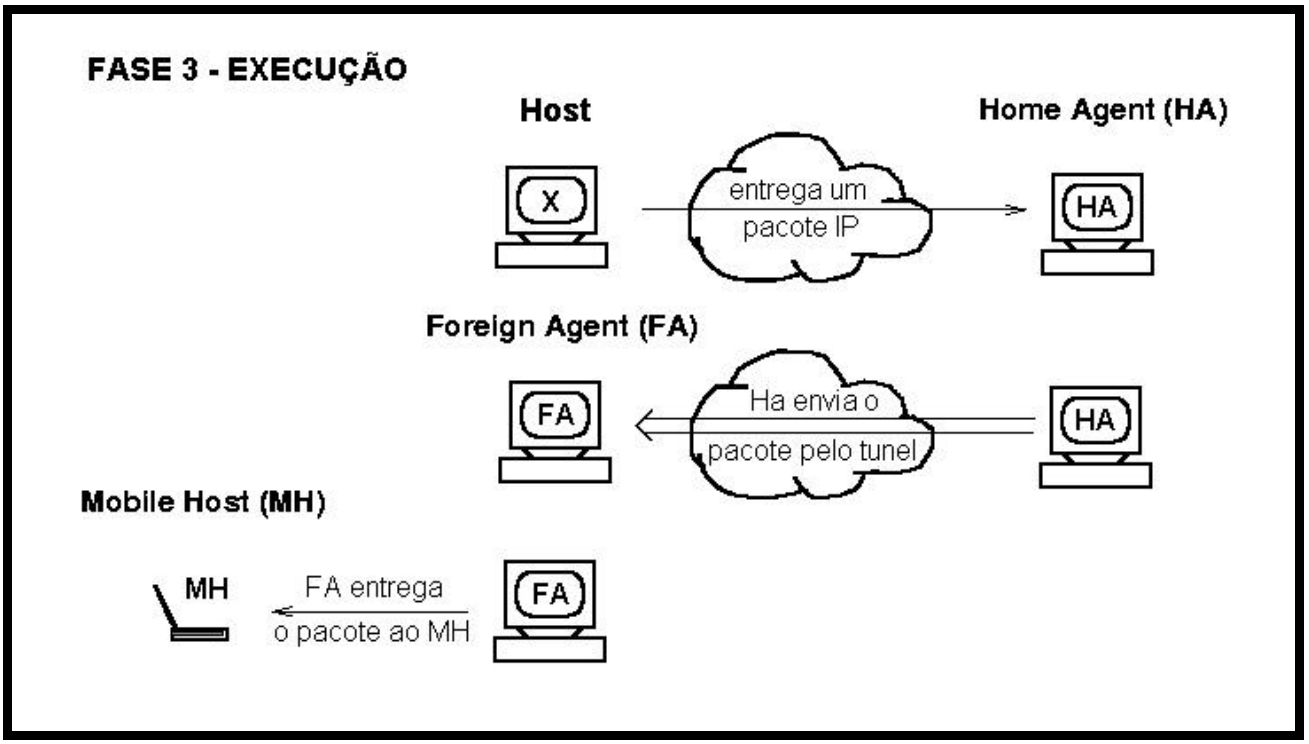


Figura 8 - Representação da fase de Execução

É nesta fase de Execução da Macro-Mobilidade que vão ser activados os mecanismos que vão suportar a conectividade de Terminais Moveis quando estes estão localizados em redes que não a de Origem; estes mecanismos sequenciais estão representados na **figura 8**.

O primeiro mecanismo de suporte vai ser protagonizado pelo Home Agent, pois este terá que agir em nome do Terminal Móvel, que agora está presente noutra rede. Assim, este terá que forçar os encaminhadores e Hosts presentes na rede de origem a associarem a sua (Home Agent) **identidade** ao **endereço** do Terminal Móvel. Este processo é suficiente para que todo o tráfego destinado ao Terminal Móvel seja entregue ao Home Agent.

De seguida o Home Agent vai enviar os pacotes de dados para a localização física do Terminal Móvel, utilizando para este processo apenas endereçamento estático (para manter este processo completamente transparente). Assim, o Home Agent vai entregar os pacotes para o Foreign Agent do Terminal Móvel, ou caso este não exista, para o endereço temporário alocado pelo Terminal Móvel na rede visitada (opção descrita na fase de registo).

Para a entrega dos pacotes é desejável que estes sejam transportados de uma forma transparente, isto é, que cheguem intactos e exactamente iguais aos originais. Este processo é conseguido pela criação de um canal lógico de comunicação, unidireccional, entre o Home Agent e o Foreign Agent/endereço Temporário do Terminal Móvel chamado **túnel** (**figura 8**).

No caso da opção referida na fase de registo de optimização dos interlocutores que já têm o suporte à Macro-Mobilidade, estes irão criar os seus próprios canais de comunicação pelo qual enviam os seus pacotes ao Terminal Móvel sem a triangulação existente no caso normal.

O Foreign Agent vai receber assim os pacotes encapsulados, emitidos pelo emissor do túnel, pelo que bastará desencapsula-los para obter os pacotes originais; são estes pacotes originais que serão entregues ao Terminal Móvel de uma forma directa, que os receberá como se estivesse na sua rede de origem. No caso de o receptor do túnel ser o próprio Terminal Móvel, então será este a desencapsular os pacotes que lhe são destinados.

Todos estes mecanismos têm sempre que serem geridos com muita precaução, dado que a Macro-Mobilidade possibilita o redireccionamento de qualquer destino de tráfego para **qualquer** outro ponto da rede global. É por esta razão que todas as mensagens trocadas na fase anterior de registo têm que ser **sempre autenticadas**, por forma a garantir que os fluxos de tráfego são sempre redireccionados para os locais físicos onde efectivamente está o Terminal Móvel, e não uma qualquer outra entidade (que nessa situação teria acesso a todo o tráfego destinado ao Terminal Móvel).

3 – Macro-Mobilidade na Internet - MIP

3.1 – Conceitos gerais do MIP

A versão actual do protocolo IP (versão 4) faz várias assumpções e generalizações que simplificam o encaminhamento dos pacotes que circulam pela Internet. Todos os nós IP têm um endereço IP que terá **sempre** que ser suficiente para o identificar univocamente na rede global. No entanto o protocolo IP considera que se pode deduzir de cada endereço IP informação a respeito da localização física do seu dono, uma vez que todos os terminais são supostos de estar **sempre** fisicamente localizados no interior da rede associada ao seu endereço IP. Esta forma de endereçamento é típica de um **espaço de nomes impuros** [5], uma vez que o algoritmo de resolução dos nomes (isto é, o processo de **localização física** de um terminal IP) utiliza esta informação contida em cada endereço IP na localização dos terminais.

Esta simplificação possibilita que os encaminhadores da Internet não necessitem que ter as rotas específicas para os milhões de terminais existentes, mas apenas para conjuntos de Redes ou Redes Individuais. Esta é uma das razões que contribuem para o protocolo IP ser escalável, o que é uma condição para qualquer protocolo poder ter um desempenho aceitável, à medida que o número de utilizadores aumenta.

Na nova situação de terminais, que pretendem mobilidade entre redes, esta simplificação do protocolo IP vai-se mostrar fatal no que respeita à desejada mobilidade à escala mundial, uma vez que o protocolo exige que os terminais estejam sempre dentro da sua rede para estes poderem receber e enviar com sucesso os seus pacotes de informação. Quando o Terminal Móvel transitar de rede, o seu endereço IP fixo já não vai reflectir correctamente o seu ponto de ligação à rede. Todos os pacotes destinados a este terminal vão ser encaminhados pelos encaminhadores da Internet para a rede de origem, e não para a rede actual onde o terminal está neste momento.

Com o protocolo IP básico a única medida que *poderia* ser utilizada para tentar manter a conectividade seria a de o Terminal Móvel se reconfigurar quando mudasse a sua localização física, mudando o seu endereço IP para um novo, adequado à sua nova localização (isto é, o Terminal Móvel teria que adquirir e passar a utilizar um novo endereço IP pertencente à rede visitada).

Esta solução é problemática no sentido em que este processo nem sempre seria possível em todas as redes, porque estas **não têm** que dispor de endereços IP reservados para visitantes; mesmo que os tivessem, este processo de troca de endereço poderá ter que ser manual (logo não automático e sujeito a erros e falhas humanas).

Por outro lado, e talvez mais importante que isto, todas as ligações já estabelecidas seriam necessariamente **perdidas** (sem aviso para os interlocutores), uma vez estas eram referentes ao **endereço anterior** do Terminal Móvel; ;esmo no caso que esta dificuldade não surgisse, ter-se-ia de restabelecer todas as ligações com o novo endereço, que já não identifica automaticamente o Terminal Móvel junto dos seus interlocutores (porque não existe partida nenhuma forma de relacionar estas **novas** ligações com as **antigas**). Por fim, a mudança caso-a-caso de endereço IP do Terminal Móvel também implica que este nó não vai poder continuar a ter um nome (válido) associado, uma vez que para isso seria necessário alterar todas as caches da base de dados de nomes sempre que o Terminal Móvel mudasse de rede, o que não seria escalável.

Todos estes problemas significam que esta medida apenas poderia ser utilizada em casos pontuais e bem determinados, como por exemplo a situação em que um portátil pretende estar em períodos prolongados em uma de duas redes, tendo disponível para seu uso pessoal um endereço IP de cada rede.

Conforme já foi referido anteriormente, o protocolo MIP é uma extensão ao protocolo IPv4, foi normalizado com o objectivo de disponibilizar a Macro-Mobilidade aos terminais móveis ao longo de toda a Internet. Em conformidade com a análise já realizada da Macro-Mobilidade em redes de dados (**capitulo 2**), o MIP vai possibilitar que os terminais móveis mantenham sempre a conectividade em qualquer rede e que sejam sempre referenciados pelos seus endereços IP “fixos” em todas as localizações.

Este novo protocolo, sendo uma extensão ao protocolo IPv4, não requer quaisquer mudanças nos protocolos já existentes (IP, ICMP, TCP), nem na infra-estrutura já existente ("routers", redes, "hosts"), uma vez que apenas são introduzidas novas entidades que suportam a mobilidade dos terminais móveis; neste sentido **qualquer** nó da Internet poderá comunicar com os novos terminais móveis, sem ter de possuir as extensões MIP no seu "stack" TCP/IP.

Este protocolo tem um funcionamento completamente automático, sendo definidas novas mensagens standard MIP de localização e de registo/cancelamento de registo entre os terminais móveis e as entidades de suporte da mobilidade.

O protocolo também define, e exige claramente a existência de mecanismos de segurança nos processos MIP, obrigando a que todas as mensagens de registo a sejam autenticadas, de forma a garantir a autoria destas. Este mecanismo de autenticação também está relacionado com a protecção de repetição das mensagens por terceiros ("relay protection").

No entanto este protocolo tem algumas deficiências que estão a ser estudadas neste momento, tendo sido criado um "Working Group" específico para o MIP. Os colaboradores deste grupo apresentam as suas propostas sobre a forma de "drafts", e destinam-se à discussão pública, focando nomeadamente assuntos relacionados com o encaminhamento, a segurança, o desempenho, a configuração.

As considerações do capítulo 2 aplicam-se no MIP de forma directa:

Cada Terminal Móvel tem sempre um endereço IP "fixo" que lhe está associado por um longo período de tempo. É sempre utilizando este endereço que todos os outros terminais vão referenciar o terminal por forma a estabelecer a comunicação entre eles.

Tal como foi descrito, todos os pacotes destinados a um dado terminal serão encaminhados pelos mecanismos normais de encaminhamento do nível IP (nível 3) sempre na direcção da rede ao qual o terminal pertence. Quando o pacote IP chegar a um encaminhador que tenha uma interface que o liga à rede pretendida (rede origem), então os mecanismos de nível 2 vão realizar a entrega do pacote ao terminal, uma vez que é assumido que o terminal terá que lá estar (no interior da sua rede de origem).

Este último passo do encaminhamento dos pacotes é realizada utilizando o protocolo de Resolução de Endereços **ARP (**"Adress Resolution Protocol"**) [11]** , que estabelece a relação entre os endereços IP (nível 3) e os endereços MAC (nível 2). Em meios físicos de **difusão** este processo é simples, bastando o encaminhador emitir um pedido ARP com o endereço IP pretendido, que será recebido por todos os nós IP presentes nesta rede IP; o terminal que possuir o endereço IP referenciado responderá ao emissor com o seu próprio endereço MAC, sendo assim fácil de criar e manter "caches" de pares ARP, para melhorar o desempenho deste passo. Por outro lado, no caso de meios físicos que não sejam de difusão (como o ATM), são normalmente utilizados servidores ARP dedicados que guardam as correspondências entre endereços IP ←→ endereços MAC.

Todo este processo apenas tem sucesso quando o Terminal Móvel está na sua rede de origem; quando este estiver fisicamente localizado numa outra rede visitada, este processo falhará, sendo retornado ao emissor uma mensagem ICMP "host unreachable", o que avisa que este terminal não está disponível.

É para fornecer aos terminais móveis a Macro-Mobilidade que o MIP define os agentes de mobilidade já descritos, que vão cooperar com os terminais móveis para que estes possam ter a conectividade constante. Os agentes de mobilidade são encaminhadores IP fixos que estão localizados fisicamente numa rede IP e que suportam os processos MIP dos terminais móveis em duas vertentes separadas distintas (normalmente as duas vertentes são implementadas no mesmo encaminhador, mas não necessariamente).

Um agente de mobilidade é um **Home Agent**, quando fornece os serviços MIP aos terminais moveis que pertencem a **esta** rede de origem (têm o seu endereço "fixo" desta rede) mas que estão neste momento localizados fisicamente numa **outra** rede visitada qualquer.

Por outro lado, um **Foreign Agent** é um agente de mobilidade que fornece os serviços MIP aos terminais móveis que pertencem a **outras** redes de origem mas que estão neste momento localizados fisicamente **nesta** rede.

Os terminais moveis têm a responsabilidade de detectar qual o seu ponto de ligação à Internet actual, e de iniciar o processo de registo quando for apropriado, de forma a criar e manter a Macro-Mobilidade em IP. Para este processo os agentes de mobilidade MIP são as entidades preferenciais que o Terminal Móvel vai contactar, podendo no entanto ser utilizados outros encaminhadores genéricos para este efeito.

Depois do Terminal Móvel verificar que necessita do MIP activo, este vai-se registar no seu Home Agent para que este redireccione o tráfego IP para a sua localização actual, de tal forma que todas as suas ligações permaneçam inalteradas.

3.2 - Arquitectura de protocolos

Relativamente ao MIP pode-se identificar dois fluxos de informação distintos envolvidos: o controlo e os dados MIP. O primeiro fluxo vai ser constituído pelas mensagens de controlo e localização trocadas entre os intervenientes do MIP, que permitem que os dados MIP sejam direccionados sucessivamente para cada localização do Terminal Móvel. Estas mensagens de controlo apenas estão presentes durante a fase de localização e registo (**fases 1 e 2**), que se executam da forma periódica já descrita. Estas mensagens trocadas de controlo têm a sua própria estrutura de protocolos, que é esquematizada na **figura 18**; nesta figura são representados os intervenientes MIP no caso mais comum (isto é, sem optimizações MIP), sendo as mensagens MIP de controlo baseadas em UDP, que é um protocolo não fiável.

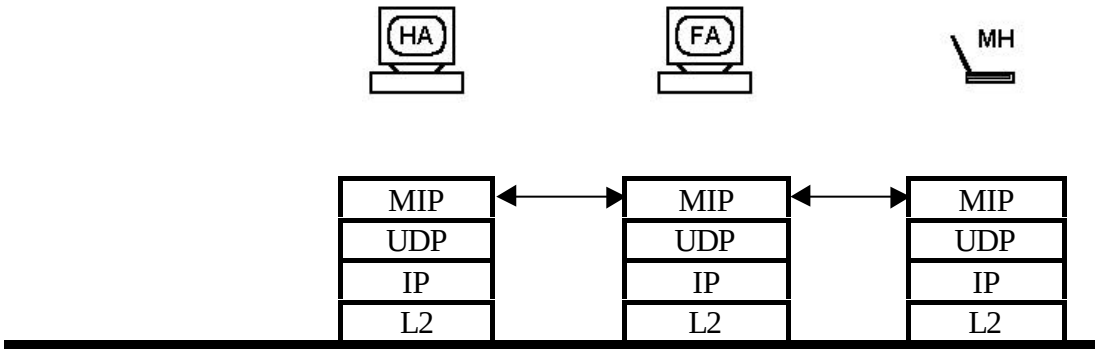


Figura 9 - Controlo MIP

O outro fluxo é constituído pelas mensagens de dados MIP, que são os pacotes IP que são encapsulados dentro do túnel IPIP desde o Home Agent até ao Terminal Móvel. Estes pacotes constituem a fase de execução (a fase 3, descritos na **secção 3.3.3**), pelo que representam a maior parte das mensagens MIP trocadas entre os intervenientes. Os dados MIP estão esquematizados em pilhas de protocolos relativos a cada interveniente do processo (**figura 21**).

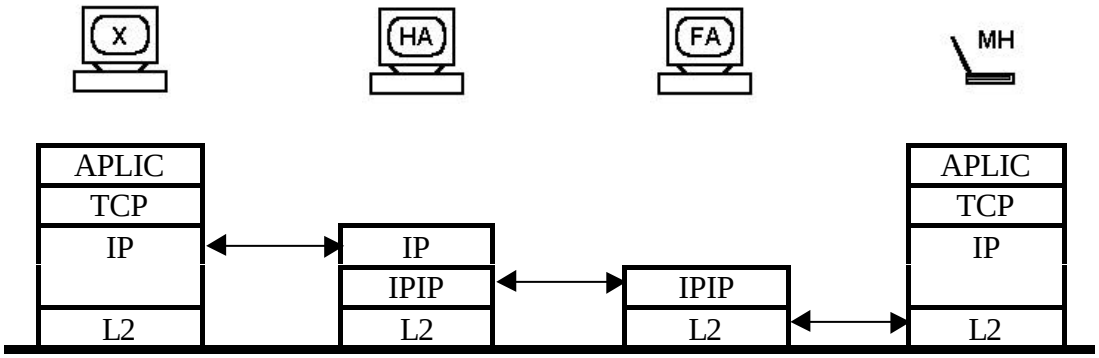


Figura 10 - Dados MIP

Nesta figura os níveis de aplicação do Terminal Móvel **MH** e de um Host genérico **X** estão a comunicar, utilizando a comunicação garantida TCP. Os pacotes IP destinados ao Terminal Móvel são encaminhados, como é normal, até à rede de origem do destinatário **MH**, onde serão adquiridos

pelo Home Agent **HA**. Este entrega estes pacotes IP encapsulados dentro de um túnel IPIP destinado ao Foreign Agent **FA**, que está adjacente ao Terminal Móvel. Uma vez os pacotes desencapsulados pela entidade **FA**, os pacotes são entregues de uma forma directa, pelo protocolo de nível 2 existente (isto é, sem utilizar o protocolo IP de encaminhamento). No final o Terminal Móvel recebe os pacotes IP como se estivesse na sua rede de origem, e serão entregues ao nível de aplicação como se tudo estivesse inalterado.

Seguidamente vão ser descritas detalhadamente as três fases da Macro-Mobilidade no MIP, sendo em cada situação detalhadas as mensagens trocadas em diagramas temporais simples. No **anexo G**, estão presentes os diagramas temporais completos de todas as opções MIP, com de todas as fases integradas num único diagrama para a melhor compreensão dos mesmos.

3.3 - Operações da Macro-Mobilidade no MIP

3.3.1 - Fase1 - Localização

O objectivo desta primeira fase do MIP é o de possibilitar ao Terminal Móvel a indicação permanente da sua localização física e dos agentes de mobilidade que existem no seu alcance, dado que será desta forma que o Terminal Móvel descobre quando é que transita de rede local, e em que situações é que necessita da Macro-Mobilidade.

Para isto os agentes MIP vão emitir periodicamente mensagens de localização em difusão, para que os terminais moveis as recebam sempre que estão no seu alcance. Por outro lado o próprio Terminal Móvel pode pedir explicitamente o aparecimento destas mensagens, se julgar que já não está localizado fisicamente no mesmo lugar, emitindo ele próprio uma mensagem de solicitação de localização em difusão.

Durante a fase de localização, o protocolo MIP, vai reutilizar as mensagens standard ICMP[8] já existentes de “router solicitation”, como base para os pedidos de localização, e de “router advertisement”, para os anúncios de localização. Estas mensagens são anteriores ao protocolo MIP, tendo sido definidas genericamente para a auto-configuração das tabelas de encaminhamento dos terminais de uma rede local, pois contêm no seu interior endereços de encaminhadores genéricos para serem utilizados pelos terminais.

Para servirem de mensagens de localização, o MIP estende as mensagens ICMP de anúncios de encaminhadores, com uma extensão especifica do MIP, na qual vão estar presentes os endereços IP dos agentes de mobilidade presentes nesta rede local IP.

Neste sentido, a sequência de fase de localização de um Terminal Móvel pode ser representada no diagrama temporal representado na figura 11:

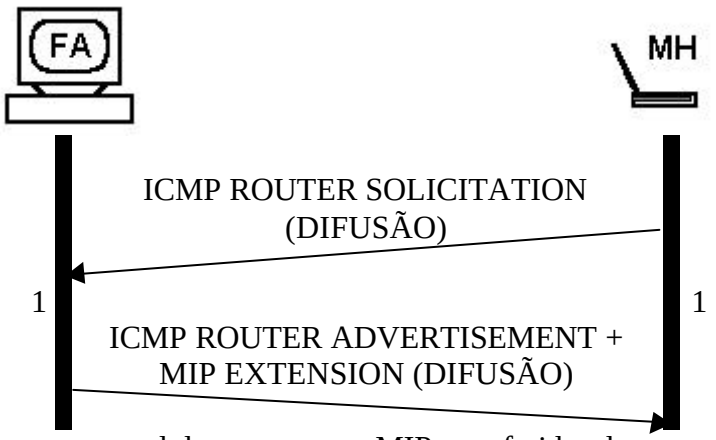


Figura 11 - Diagrama temporal das mensagens MIP transferidas durante a Fase de Localização

Tanto o cabeçalho ICMP, como esta extensão MIP que torna estas mensagens anúncios de agentes de mobilidade estão detalhados no **anexo A;** É esta extensão MIP do pacote ICMP que vai detalhar as características que os agentes de mobilidade anunciados nesta extensão detêm. Estas

mensagens são numeradas sequencialmente entre anúncios, de forma aos terminais móveis poderem se aperceber de falhas nos agentes. As mensagens têm sempre um campo que determina o tempo de de alocação (em segundos) dos serviços de Macro-Mobilidade nos agentes de mobilidade por parte dos terminais móveis, de tal forma que estes deverão utilizar o valor máximo admissível no seu pedido de registo.

Existe um campo flags referente às características e opções do protocolo MIP dos agentes anunciados, que o agente suporta. Assim, as flags vão indicar se este agente de mobilidade é um Home Agent e/ou Foreign Agent, se o agente exige que os terminais móveis se registem com ele e quais as optimizações que o agente suporta (minimal encapsulation [7], GRE encapsulation, e compressão do cabeçalhos de Van Jacobson).

Existe também uma flag, para uso dos Foreign Agents, que tem como objectivo indicar aos terminais móveis que este agente não tem (neste momento) recursos suficientes para suportar novos clientes MIP. Mesmo assim, neste caso, esta mensagem é útil para o Terminal Móvel tomar conhecimento da sua localização actual (embora tenha que de se registar junto de outro Foreign Agent, caso exista).

No final da mensagem estão presentes os endereços dos agentes de mobilidade existentes nesta rede. É através da inspecção destes endereços que o Terminal Móvel tem o conhecimento da sua localização física. Em particular, a recepção de um anúncio do seu Home Agent indica ao Terminal Móvel que este está na sua rede de origem, onde não vai necessitar dos mecanismos MIP; esta certeza deriva de mensagens de localização apenas existem no interior da rede onde foram emitidas, porque estas mensagens ICMP têm sempre um TTL (“time to live”) unitário.

Todos os pacotes ICMP têm um campo no cabeçalho denominado de **Tempo de Vida**, expresso em segundos. Este campo estabelece o tempo máximo de validade do pacote ICMP, e vai ser utilizado pelos terminais móveis no seu mecanismo de detecção da sua localização actual.

Assim quando um Terminal Móvel estiver localizado fisicamente numa rede local, este vai periodicamente receber os anúncios de localização do agente onde se registou. No entanto, quando este terminal sair do interior da rede actual e transitar para uma nova rede, este vai deixar de receber os anúncios de localização do agente anterior, ao mesmo tempo que vai começar a receber novos anúncios de localização dos agentes da nova rede. No entanto, o Terminal Móvel vai abster-se logo de iniciar as suas medidas de transição de rede, uma vez que a ausência de anúncios do agente anterior pode ter sido causado apenas por perdas desses pacotes na rede, uma vez que os anúncios são emitidos em UDP, que é um protocolo simples sem garantias de entrega.

Só quando o último anúncio recebido do agente expirar o seu tempo de vida, é que o Terminal Móvel chega à conclusão que já não está localizado na mesma rede, pelo que inicia neste momento o seu processo de registo junto do novo agente de mobilidade.

Durante toda a estadia do Terminal Móvel numa dada rede, este terá de que verificar, continuamente, se permanece no interior dessa rede, isto é, se continua a receber os anúncios de localização do seu agente onde está registado. No caso de o terminal deixar de receber os referidos anúncios de localização, este poderá registar-se imediatamente num novo agente de mobilidade que esteja no alcance do Terminal Móvel.

Quando o Terminal Móvel volta a receber os anúncios de localização do agente original este vai determinar se deixou de os receber porque saiu por momentos do alcance do agente (o que significa que o agente continua a suportá-lo), ou se houve uma falha neste agente. Nesta última situação o Terminal Móvel tem de se registar de novo no agente, uma vez que o serviço MIP que lhe estava a ser prestado, foi interrompido.

Para esta operação vai ser utilizada o campo **número de sequencia**, existente nos anúncios dos agentes. Cada agente usa o campo para numerar os seus anúncios, começando a contagem sempre em 0 e incrementando o valor do campo por cada novo anúncio. Uma vez que este campo é limitado a 16 bits, um máximo de 65536 anúncios vão poder ser numerados sequencialmente. Quando os agentes vão numerar o anúncio seguinte ao máximo, esse anúncio vai ser o número 256, em vez do natural 0. Desta maneira, um agente que emita anúncios com a numeração menor que 256 indica, garantidamente, que acabou de se re-inicializar.

Nestas condições, os terminais móveis verificam sempre a numeração dos anúncios e se esta numeração é sempre crescente. Quando isto não acontecer, isto é se o valor do anúncio for inferior a 256, então o Terminal Móvel apercebe-se da reinicialização do agente, pelo que se regista novamente. Este mecanismo é muito fiável para detectar reinicializações do agentes por parte dos terminais móveis, uma vez que só falharia no caso em que o Terminal Móvel perdesse os primeiros 256 anúncios seguidos de um agente, o que é um caso muito pouco provável.

O MIP também possibilita os mecanismos de Macro-Mobilidade aos terminais moveis que se movem para redes visitadas que não têm qualquer agente de mobilidade que sirva de Foreign Agent para o Terminal Móvel. Nesta situação, o Terminal Móvel não vai receber quaisquer anúncios de agentes de mobilidade e vai ter de alocar para o seu uso um endereço IP da rede onde está e de encontrar um encaminhador genérico que lhe receba os seus pacotes IP.

Dois protocolos que conseguem fornecer ao Terminal Móvel estas duas informações são o **DHCP [9]** ("dynamic host configuration protocol") e o **PPP** ("point-to-point protocol"). Quando o Terminal Móvel se configura por estes meios, vai-se registar (**fase 2**) directamente no seu Home Agente, e irá (**fase 3**) receber directamente os pacotes encapsulados enviados por este. Nesta situação, o anterior diagrama temporal é o que se representa na figura 12.

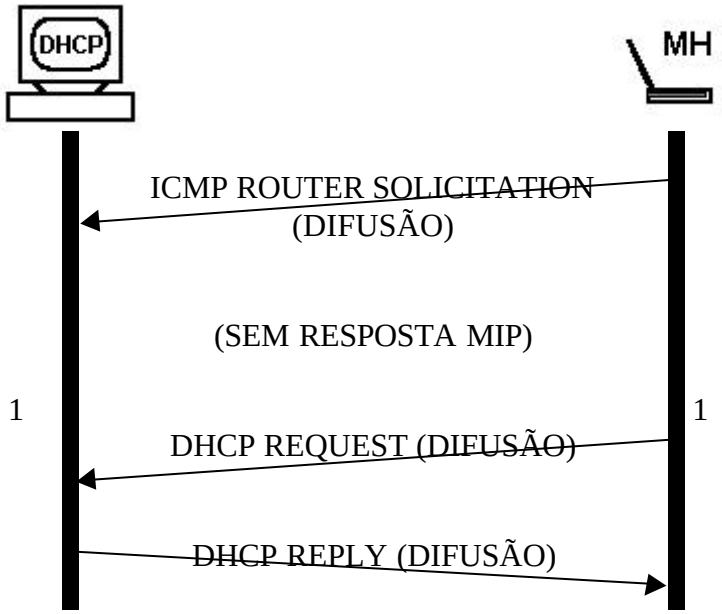


Figura 12 - Diagrama temporal das mensagens MIP Transferidas durante a Fase de Localização com o DHCP

3.3.2 - Fase 2 - Registo

A segunda fase do MIP é activada quando o Terminal Móvel chega à conclusão que já não está na mesma localização física que anteriormente estava, pelo que vai informar o seu Home Agent da sua localização física actual, que pode ser junto a um Foreign Agent ou "sozinho", quando este alocou por DHCP ou PPP um endereço temporário da rede actual para o MIP. Em todo o caso, do ponto de vista do Home Agent esta distinção é indiferente uma vez que este apenas necessita de saber qual é o endereço para onde vai enviar os pacotes IP destinados ao Terminal Móvel, isto é: para um Foreign Agent, ou para o endereço temporário do Terminal Móvel.

Para isto utilizam-se nesta fase do MIP mensagens de "registo" e "resposta de registo" que estão definidas no standard MIP. Estas mensagens são trocadas na forma especificada no diagrama temporal quando o Terminal Móvel está a usar um Foreign Agent (**figura 13**) ou quando está sozinho, com um endereço temporário (**figura 14**):

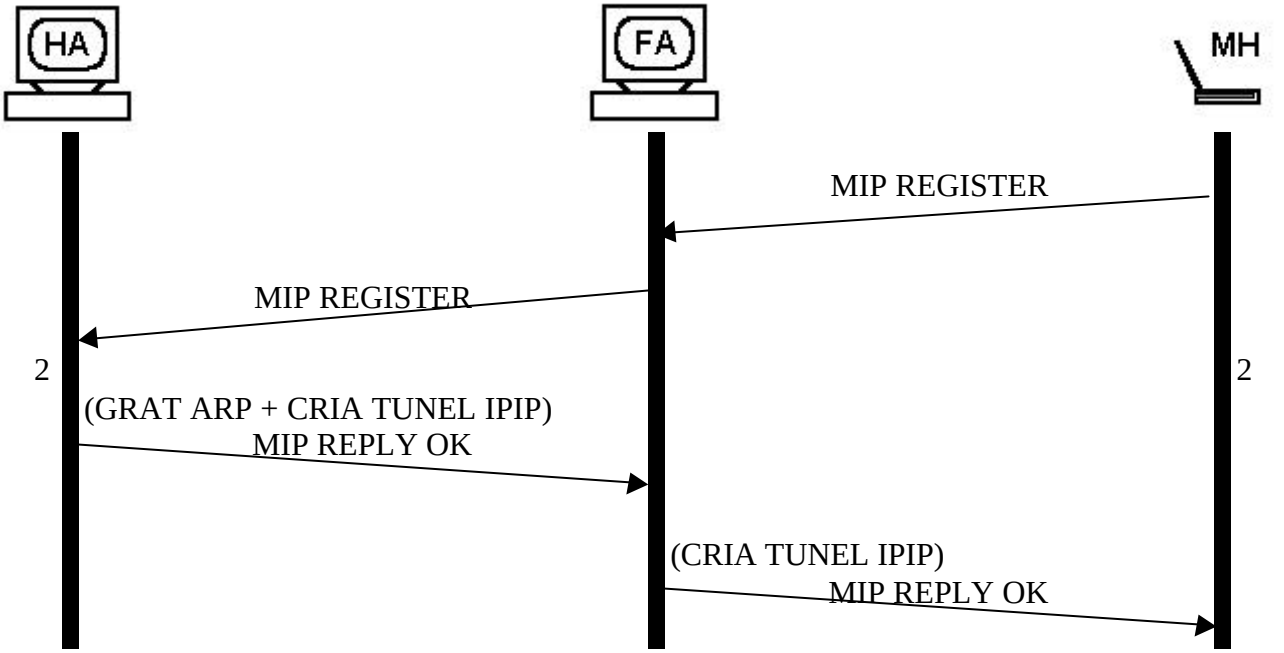


Figura 13 - Diagrama temporal das mensagens MIP transferidas durante a Fase de Registo

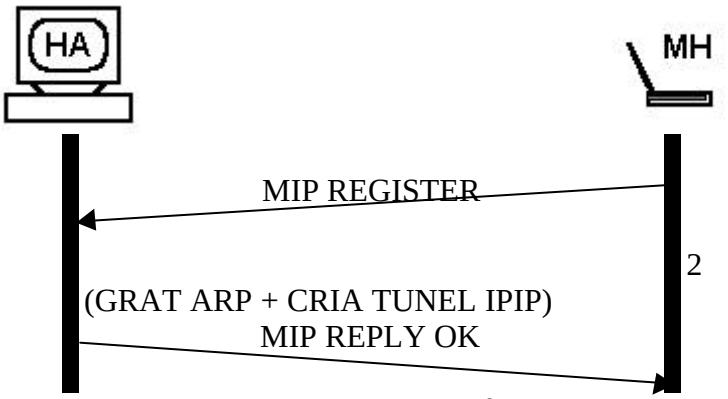


Figura 14 - Diagrama temporal das mensagens MIP transferidas durante a Fase de Registo, com DHCP

Quando um Terminal Móvel consegue aferir, univocamente, a respeito da sua localização actual então este vai comunicar com o seu Home Agent, informando-o da sua localização, com o objectivo que este possa criar e manter os mecanismos de Macro-Mobilidade para o Terminal Móvel.

As mensagens utilizadas nesta fase são ambas baseadas em UDP e têm desde a sua criação mecanismos de extensibilidade para novas versões do protocolo MIP.

A mensagem de pedido de registo está detalhada no **Anexo B**, e contem a identificação do Terminal Móvel que originou o pedido de registo, o endereço onde está localizado (endereço do Foreign Agent ou endereço temporário alocado) e por fim, o endereço do Home Agent.

Nesta mensagem existe um campo para o Terminal Móvel colocar o valor de tempo que pretende ter de utilização dos mecanismos e recursos da Macro-Mobilidade disponibilizados pelo seu Home Agent; neste campo o valor de zero é a indicação de que o Terminal Móvel pretende cancelar o registo no seu Home Agent, terminando assim os serviços de Macro-Mobilidade.

Por fim, existe um campo onde o Terminal Móvel pode requerer várias opções do registo MIP, tais como as opções MIP de Múltiplos Registos Simultâneos, a entrega de pacotes enviados em difusão na rede de origem, de desencapsulação dos pacotes pelo próprio Terminal Móvel e as optimizações MIP de Minimal encapsulation, GRE encapsulation, e compressão do cabeçalhos de Van Jacobson.

A mensagem de registo MIP é composta por este cabeçalho normalizado standard ao qual são acrescentadas as extensões MIP existentes. Para tal, é definido um esquema simples de extensibilidade do protocolo, o que permite que este possa sempre crescer, à medida que a tecnologia evolui e surgem novas necessidades, não previstas na versão inicial. Assim, todas as extensões têm o seguinte formato:

Extensão MIP

Tipo	Comprimento	Dados...

Neste sentido, todos as extensões ao protocolo terão um identificador (campo Tipo) que discrimina a extensão em causa, seguida de um campo – comprimento - que fornece o suporte a extensões de comprimento variável. Depois destes dois campos de extensão normalizda irão existir os campos específicos de cada extensão.

Uma vez que o formato da extensão está definido, de uma forma inequívoca, será sempre possível a inter-operabilidade de diferentes versões do protocolo MIP. Neste sentido, os agentes e terminais móveis MIP terão que processar o cabeçalho (que não varia) e as suas extensões (que podem variar em novas versões de protocolo MIP). Para todas as extensões conhecidas as entidades MIP terão a obrigação de as processar e considerar; No entanto, relativamente a extensões desconhecidas, isto é, que tenham um campo tipo não previsto na sua versão do protocolo MIP, estas poderão ser ignoradas, passando à análise da extensão seguinte.

No caso normal, o primeiro passo do registo é protagonizado pelo Terminal Móvel, em conjunção com o Foreign Agent escolhido, (tipicamente o mais próximo deste). Assim, o Terminal Móvel vai entregar o seu pedido de registo MIP ao Foreign Agent para que este o entregue ao seu Home Agent. No outro caso, o pedido é entregue directamente ao Home Agent.

Quando recebe o Foreign Agent este pedido do Terminal Móvel, vai efectuar um conjunto de validações sobre as informações contidas no registo, como por exemplo relativas à integridade do pedido ou à possibilidade de satisfazer as características exigidas neste. Por outro lado, o Foreign Agent pode implementar diferentes politicas de segurança e contabilização, pelo que este pode, desde logo, recusar a prestação dos serviços de mobilidade aos terminais móveis que não estejam explicitamente autorizados. Neste caso, o Foreign Agent pode, desde logo, enviar uma mensagem MIP, em resposta, que indique a negação do serviço ao Terminal Móvel.

Caso o Foreign Agent aceite fornecer o serviço ao Terminal Móvel, então vai enviar a mensagem original para o Home Agent requerido (o endereço do Home Agent está contido dentro da mensagem de registo do Terminal Móvel), sendo para isso utilizados os mecanismos normais de encaminhamento.

Quando o Home Agent do Terminal Móvel receber o pedido de registo, também este agente vai efectuar validações semelhantes às já referidas, nomeadamente de integridade da mensagem, aspectos de autenticação, autorização e segurança, ou contabilização. Se tudo estiver bem, então aí o Home Agent irá tomar as medidas necessárias para acatar o pedido do Terminal Móvel.

Assim, se o campo “tempo de vida” tiver o valor zero, significa que o Terminal Móvel está a requerer um cancelamento de registo. No caso de o pedido ser um registo, então o campo **Tempo de Vida** irá conter o período de tempo durante o qual o Terminal Móvel pretende os serviços do seu Home Agent activos. Tal como é típico nos serviços Internet, os recursos e mecanismos são sempre alocados de uma forma “soft-state”, isto é, necessitam sempre de serem requisitados periodicamente, uma vez que depois de passar o tempo acordado entre as duas partes para a alocação dos recursos, estes serão obrigatoriamente indisponibilizados. No entanto, dependente da politica de atribuição de recursos que exista no Home Agent, o tempo requisitado no pedido de registo poderá ser superior a um limite máximo de tempo, definido eventualmente caso-a-caso para cada Terminal Móvel. Neste caso, na mensagem MIP de resposta, o Home Agent pode sempre diminuir o tempo da alocação para o valor que entender, sendo depois o Terminal Móvel obrigado a

acatar o novo limite (continuando sempre a ser possível, com o recurso aos registo referidos, a extensão sucessiva do tempo total de serviço).

Será então pela mensagem de resposta ao registo MIP que os agentes de mobilidade irão informar o Terminal Móvel da aceitação/rejeição do registo, e em que condições o serviço irá ser prestado. Esta mensagem MIP está detalhada no Anexo B e contém a informação para registos bem sucedidos, do Tempo de Vida respectivo.

É no campo "código" que os agentes (Home e Foreign) indicam ao Terminal Móvel qual a situação do seu pedido de registo. Assim, existem vários códigos definidos no protocolo, podendo eventualmente serem definidos novos códigos (de aceitação e rejeição), que referenciem novas situações em próximas versões do protocolo MIP.

Neste momento, existem apenas dois códigos que indicam a aceitação, por parte do Home Agent, do registo de um Terminal Móvel. Este terminal é obrigado a aceitar o Tempo de Vida indicado pelo agente de mobilidade nesta mensagem. O código 0 indica uma aceitação de todas as condições requeridas pelo Terminal Móvel; o código 1 também indica a aceitação do suporte do Terminal Móvel, no entanto sem a capacidade de "registos simultâneos".

Todos os outros códigos vão indicar a rejeição, por parte do agente de mobilidade (Home ou Foreign Agent) do pedido de registo.

Estes códigos, utilizados nas respostas de registos, são separados entre as recusas por parte do Foreign Agent e as recusas Home Agent. Neste sentido, o Foreign Agent quando contactado pelo Terminal Móvel pode imediatamente recusar o serviço, enviando logo uma resposta negativa ao Terminal Móvel. Em ambos os casos será o Terminal Móvel que terá a responsabilidade de, caso queira, reformular e emitir um novo pedido de registo, que seja agora aceite no qual não exija certas opções MIP, por exemplo.

Assim os Foreign Agents podem sempre recusar os serviços MIP por varias razoes, sendo estas detalhadas no anexo B. A recusa pode ser devida a razões administrativas (códigos 65, 66, 69), de Segurança (códigos 67, 68), falta de opções do protocolo (códigos 72, 73), ou erros no protocolo (códigos 70, 71). Outras classes de erros só aparecem quando o Foreign Agent considere que o pedido é satisfatório, e tenta de seguida entregá-lo ao Home Agent indicado no registo, ficando de seguida à espera da resposta deste. No entanto a comunicação entre os dois agentes de mobilidade pode não ser possível de se concretizar (por exemplo, se não houver um caminho entre o dois agentes), pelo que será emitido um erro ICMP que indica este facto. Nestes casos o Foreign Agent irá informar o Terminal Móvel da situação que está a decorrer (códigos 80, 81, 82 e 88).

Finalmente outro problema não previsto nestes casos será respondido pelo Foreign Agent com o código 64.

Se, para o Foreign Agent, o pedido de registo for aceite, então este pedido é enviado para o Home Agent indicado. Este responderá com os mesmos códigos de aceitação do Foreign Agent (códigos 0 e 1), mas com diferentes códigos de recusa, detalhados na tabela existente no anexo B.

Assim o Home Agent pode recusar o serviço por razões administrativas (códigos 129, 130), de Segurança (códigos 131, 132, 133), falta de opções do protocolo (códigos 135), ou erros no protocolo (códigos 134). À semelhança dos códigos de recusa emitidos pelo Foreign Agent, qualquer outro problema não previsto nestes casos será respondido ao Terminal Móvel com o código 128.

O formato da resposta MIP é muito semelhante ao formato do pedido de registo; assim, depois do cabeçalho normalizado descrito pode existir um número variável de extensões, sendo a sua codificação e processamento igual para os dois tipos de mensagens. Tal como nos pedidos de registo, para as respostas só estão definidas as extensões de autenticação das mensagens já referenciadas, sendo no entanto expectável a utilização de novas extensões para as próximas versões do protocolo MIP, de forma a cobrir novas optimizações ao protocolo.

Depois do Terminal Móvel enviar o seu pedido de registo, este vai ficar à espera da resposta, que lhe será entregue pelo Foreign Agent. Quando esta é recebida o Terminal Móvel vai-se certificar se a resposta recebida é referente ao seu último pedido. Esta precaução é importante uma vez que as mensagens MIP são enviadas sobre o protocolo UDP, que não é fiável. Assim

convencionou-se, que os terminais móveis só irão considerar uma resposta se esta for exactamente correspondente ao último pedido efectuado.

Para este efeito vai ser utilizado o campo "identificação" presente tanto nos pedidos como nas respostas MIP, que tem a seguinte configuração:

Campo "identificação":

Parte "low" – último ID do Terminal Móvel
Parte "high" – último ID do Home Agent

Este campo está dividido em duas partes, uma para cada interveniente no processo de registo MIP. Cada vez que o Terminal Móvel emite um **novo** pedido de registo, introduz na sua parte deste campo um **novo** valor aleatório de 32 bits. Se o Terminal Móvel tiver que **retransmitir** um pedido já enviado, então nesse caso será enviado o último valor de identificação inalterado. Relativamente à parte "high", pertencente ao Home Agent, o Terminal Móvel preencherá este campo com o último valor "high" de uma resposta enviada pelo Home Agent.

Quando o Home Agent responder, o Terminal Móvel terá necessariamente que verificar se a parte "**low**" da **resposta** dada pelo Home Agent é igual à parte "**low**" do seu último **pedido**, enviado a este. Se este caso não acontecer, então esta resposta do Home Agent é ignorada, com a excepção do campo ID "high", que será utilizado para o próximo pedido.

De uma forma intercalada, o Home Agent está sempre à espera que os pedidos feitos por cada Terminal Móvel tenham o ID "high" igual ao último ID "high", dado pelo Home Agent na sua ultima resposta. Similarmente, se existir uma falha nos IDs tanto dos pedidos ou das respostas, o campo ID da outra parte interveniente é sempre actualizado.

Esta situação vai acontecer sempre no primeiro par de mensagens trocadas entre um agente e um terminal móvel: de início, nenhum sabe o ID da outra parte, pelo que ambos têm valores inválidos relativos ao ID. O protocolo, tal como foi descrito, é iniciado pelo Terminal Móvel com uma mensagem de registo, que terá um ID "low" novo, calculado pelo Terminal Móvel, e um ID "high" invalido. Quando esta mensagem for proveniente do Home Agent, haverá garantidamente uma falha de Identificação, uma vez que o campo ID "high" não estará certo. Assim, o Home Agente responderá com uma resposta com o código 133 (erro de identificação), mas incluindo o ID "high" certo do Home Agent para este Terminal Móvel. Quando este recebe a resposta, recolhe o novo ID "high", e verifica que houve um problema de identificação, o que o leva a enviar um novo pedido de registo, tendo agora o ID do agent correcto. Esta nova mensagem já será aceite, bem como todas as próximas (se não existisse percas de pacotes na rede). Este processo também é utilizado para garantir, em conjugação com a autenticação, que os pedidos não podem ser repetidos com sucesso por terceiros com o objectivo de baralhar o protocolo (este assunto vai ser descrito em detalhe na secção 3.4).

Pelo que foi descrito acima é o Terminal Móvel que tem a parte activa do processo de registo, isto é, é deste a responsabilidade de iniciar e garantir o sucesso do processo de registo, da detecção de perdas de mensagens MIP e de efectuar os seus re-registos junto do seu Home Agent. O Terminal móvel deverá iniciar sempre o processo de registo quando suspeitar que já não se encontra na mesma localização actual, quando existirem mudanças significativas nas interfaces activas IP do Terminal Móvel, quando este detecta que o seu agente de mobilidade próximo se reinicializou ou, finalmente, quando o registo corrente de mobilidade vai expirar. Estas considerações são apenas sugestões do protocolo, podendo ser tomadas como decisões de cada implementação, o que significa que diferentes implementações do protocolo MIP podem, por exemplo, transitar de rede mais rapidamente, embora também com diferentes utilizações dos recursos da rede.

No entanto, no processo de registo, se o Terminal Móvel suspeitar que o pedido enviado de registo foi perdido pode retransmitir o último pedido enviado exactamente como estava.

Quando uma entidade MIP recebe uma resposta afirmativa de um registo de um Terminal Móvel, então essa entidade terá que criar e manter, pelo tempo acordado, os mecanismos

necessários (descritos posteriormente) à Macro-Mobilidade, sendo sempre estes mecanismos abandonados quando o tempo de vida expirar, sem que entretanto esse prazo tenha sido convenientemente estendido por parte do Terminal Móvel.

3.3.2.1 - Opções MIP

Existem também algumas opções do protocolo, cuja utilização e suporte não é obrigatória. Conforme já foi referido antes, estas opções reflectem-se principalmente no campo "flags" presente no pedido de registo.

A primeira opção do protocolo está relacionada com terminais móveis que se movimentam em redes wireless. De acordo com o modelo clássico OSI dos protocolos dependentes do meio físico estão localizados nos níveis 1 e 2, sendo o protocolo de nível 3 independente destes.

No contexto Internet esta condição significa que o protocolo IP, de nível 3, será sempre o mesmo aplicado a uma rede wireless 802.11 ou a uma "clássica" Ethernet 802.3. Desta forma, e uma vez que o protocolo MIP é uma **extensão** ao protocolo IP, também este será independente dos possíveis meios físicos a serem utilizados pelos entidades MIP (terminais móveis/agentes).

No entanto, mesmo para o nível 3, podem existir diferenças que serão consideradas como optimizações ao protocolo. No caso de uma rede wireless, um Terminal Móvel que a visite poder-se-á movimentar livremente no interior desta rede. Por outro lado, se o Terminal Móvel estiver em constante movimento, este pode facilmente sair do interior desta para uma nova rede, com um novo Foreign Agent. Nesta situação o Terminal Móvel poderá estar muitas vezes no alcance de mais de um Foreign Agent, de diferentes redes. Pelo processo de registo que foi descrito o Terminal Móvel poderia a qualquer momento registar-se num agente de mobilidade, pedindo desta forma ao seu Home Agent que entregue os seus pacotes para esse Foreign Agent, que os entrega de seguida ao próprio Terminal Móvel.

No entanto, pelo processo de registo descrito, um novo registo para um novo Foreign Agent iria cancelar o envio de pacotes para o anterior Foreign Agent, passando a serem encaminhados em exclusivo para o último Foreign Agent.

Para esta situação o Terminal Móvel pode pedir, na sua mensagem de registo enviada ao Home Agent, o suporte deste de "registos simultâneos". Esta opção do registo, se aceite, implica que o Home Agent passe a enviar os pacotes destinados ao Terminal Móvel para ambos os agentes de mobilidade (eventualmente, para um qualquer número de agentes). Desta forma **ambos** os agentes vão entregar os pacotes encapsulados pelo Home Agent ao Terminal Móvel, o que vai aumentar significantemente a fiabilidade da entrega destes, embora também aumente largura de banda ocupada pelo Terminal Móvel que passa a receber os seus pacotes, no melhor dos casos, de duas (ou mais) fontes diferentes. É importante verificar que assim o Terminal Móvel vai, seguramente, receber pacotes duplicados com bastante frequência; no entanto esta situação não é "nova", uma vez que o serviço IP de encaminhamento de pacotes também prevê explicitamente a possibilidade de duplicação de pacotes. Desta forma serviços que não podem tolerar este problema, presente no protocolo IP simples e também nesta opção do MIP, utilizam certamente um protocolo que resolva esta questão (TCP em vez de UDP, por exemplo).

Esta opção requer também mais recursos disponíveis no Home Agent do Terminal Móvel, pelo que está prevista a aceitação do serviço mas com recusa desta opção (referente ao código de aceitação 1).

Pelos mecanismos de Macro-Mobilidade descritos do MIP, os terminais móveis vão poder receber todos os pacotes que lhe são explicitamente destinados tal e qual como se o terminal estivesse localizado fisicamente na sua rede de origem. No entanto existe uma classe de pacotes que não são explicitamente destinados ao Terminal Móvel, mas que este iria receber, caso estivesse localizado na sua rede de origem – os pacotes enviados em difusão, destinados a todos os nós de uma dada rede de meio partilhado. Dentro desta classe de pacotes os mais comuns são os pacotes ARP, já referenciados, que estabelecem as correspondências entre endereços IP nível 3 e endereços MAC nível 2.

No caso dos pacotes emitidos em difusão serem de interesse para o Terminal Móvel, então este poderá pedir a entrega destes pacotes (além dos "normais" que lhe são destinados) também utilizando uma flag específica do campo respectivo no pedido de registo. No entanto, devido ao aumento de recursos que irão ser ocupados com esta opção, os agentes de mobilidade podem sempre negar a satisfação desde pedido ao Terminal Móvel.

Existe também um procedimento, que ainda não está normalizado, que visa resolver o problema já referido da triangulação dos pacotes IP destinados ao Terminal Móvel, uma vez que no caso normal todos os pacotes têm de ser encaminhados pelo Home Agent, que os encapsula para o Terminal Móvel, (não indo assim pelo caminho mais directo). O problema desta opção MIP é que os interlocutores do Terminal Móvel terão necessariamente de possuir as extensões MIP para eliminar a triangulação.

Nesta opção, quando o Terminal Móvel se regista, o seu Home Agent vai poder tomar a liberdade de avisar os interlocutores do Terminal Móvel acerca da verdadeira localização deste, com uma mensagem especial MIP. Nesta situação, os emissores dos pacotes destinados ao Terminal Móvel que tenham o MIP implementado vão poder enviar os pacotes **directamente** para a localização física do Terminal Móvel (endereço do Foreign Agent/endereço temporário alocado), o que elimina a triangulação; esta acção adicional é descrita no diagrama temporal representada na figura 15:

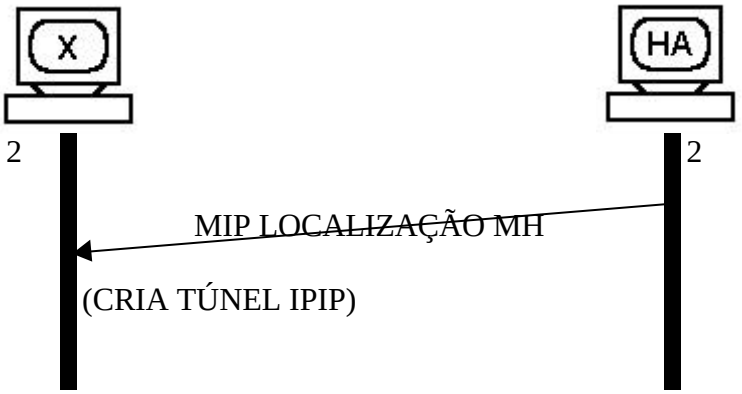


Figura 15 - MIP sem Triangulação - Fase 2

3.3.3 - Fase 3 - Execução

Todos os mecanismos, processos e acções que até agora foram descritas têm o objectivo de assegurar que as entidades MIP agem e cooperam, de uma forma controlada e segura, na aplicação e manutenção das medidas que vão criar a Macro-Mobilidade de qualquer nó da Internet.

Assim, pelos processo de localização descrito os terminais móveis podem descobrir que já não se encontram na sua rede de origem, o que implica que deixaram de estar contactáveis; Com a ajuda de um Foreign Agent (ou sozinhos, como foi descrito), este vai-se registar no seu Home Agent, passando este e o Foreign Agent (caso seja utilizado) a fornecerem os serviços MIP de Mobilidade descritos de seguida; periodicamente o Terminal Móvel irá registar-se de forma a manter o serviço, eventualmente numa outra rede física, continuando o Home Agent a fornecer o serviço para a localização actual do Terminal Móvel. Quando o Terminal Móvel desejar finalizar os serviços MIP, irá cancelar o registo no seu Home Agent; se não o fizer, o serviço expirará naturalmente, sendo terminado nessa ocasião.

Durante todo este processo, apenas os agentes de mobilidade envolvidos têm o conhecimento da verdadeira situação que está em curso. Todos os outros nós da Internet não conhecem o estado de mobilidade do Terminal Móvel, pelo que comunicarão com este da mesma forma que com qualquer outro nó (fixo) da Internet.

Quando um Terminal Móvel está localizado na sua rede de origem, os mecanismos de Macro-Mobilidade estarão inactivos, ficando o terminal a funcionar da mesma forma que qualquer

outro nó fixo da Internet, dado que o seu enderece IP reflecte correctamente a sua localização. Assim, todos os pacotes destinados a este terminal serão enviados de encaminhador em encaminhador por toda a Internet até a rede de origem do terminal, uma vez que o endereço IP de destino destes assim o indica. Quando o encaminhador que detêm neste momento o pacote IP tem uma interface directa para a rede de destino (isto é, quando o pacote chegar à "fronteira" da sua rede de destino), então este pacote passa a ser entregue pelos mecanismos previstos pelo Nível 2 (uma vez que o encaminhamento de nível 3 só entrega pacotes **entre** diferentes redes). Este caso também se aplica quando o emissor dos pacotes for um nó que também pertença à mesma rede que o seu destinatário.

Nestas condições, não é da responsabilidade do protocolo IP a entrega final dos pacotes dentro da mesma rede, sendo definida caso a caso para cada protocolo de nível 2 (sendo estes relacionados com o meio físico existente). No entanto existe um ponto de convergência entre o protocolo IP e o protocolo de nível 2, no que respeita à conversão dos endereços de ambos (uma vez que os dois espaços de endereçamento são distintos).

Este conversão é efectuada pelo protocolo ARP (Address Resolution Protocol), que é definido caso a caso para cada diferente nível 2, e que estabelece correspondências entre os dois tipos de endereços. Este protocolo pode ser trivial ou muito complexo:

- No caso de uma rede com capacidade de difusão, como uma Ethernet 802.3 ou um rede Wireless 802.11, bastará enviar em difusão um pedido simples ARP com o intuito de resolver um endereço IP; como resposta, o possuidor do endereço IP em causa irá responder com o seu endereço de nível 2 (endereço MAC). Esta resposta poderá ser envida também em difusão para permitir que todos os outros terminais possam tomar conhecimento da correspondência endereço IP ←→ endereço MAC
- No caso de um meio físico que não seja de difusão, como uma rede ATM, a solução requer o uso de servidores dedicados ARP que guardam as correspondências entre endereço IP ←→ endereço MAC, existindo um protocolo de registo de novos terminais que sejam adicionados à rede.

Neste contexto, a única característica do encaminhamento a configurar para um qualquer Terminal Móvel que esteja localizado na sua rede de origem (e, neste caso, também de qualquer terminal fixo) prende-se apenas na escolha de um encaminhador "default" para o qual são enviados para processamento os seus pacotes. Esta configuração é usada, tipicamente, para reduzir ao mínimo a complexidade dos mecanismo e tabelas de encaminhamento dos terminais (fixos e móveis) simples, concentrando os aspectos avançados de encaminhamento nos "routers". Esta configuração pode ser feita manualmente, ou com a ajuda das mensagens standard ICMP (as já descritas ICMP Router Solicitation/Advertisement).

Quando um Terminal Móvel estiver localizado numa rede distinta da sua rede de origem, então posteriormente ao seu processo de registo serão criados os seguintes novos mecanismos de encaminhamento:

O Home Agent passará a ter a responsabilidade de receber, em nome do Terminal Móvel, todos os pacotes que lhe são destinados. No contexto IP, este requerimento é instanciado quando o Home Agent executa os mecanismos ARP, de forma a que todos os nós da rede associem o endereço IP do Terminal Móvel ao endereço MAC do Home Agent, de tal forma que entreguem sempre os pacotes (destinados ao Terminal Móvel) ao Home Agent. Este mecanismo tem o nome de "proxy ARP" e, tal como o ARP, é especifico de cada meio físico. Seguindo a divisão ARP efectuada acima, nos meios de difusão o proxy ARP é efectuado quando o Home Agent responde com o seu próprio endereço MAC a todos os pedidos ARP destinados ao Terminal Móvel. Nos meios que não são de difusão o proxy ARP é concretizado quando o Home Agent modifica as entradas relativas ao Terminal Móvel com o seu próprio endereço MAC, nos servidores ARP existentes na rede IP de origem.

Este mecanismo descrito garante que os novos fluxos de comunicação destinados ao Terminal Móvel são sempre entregues ao Home Agent. No entanto os fluxos já existentes permaneceram errados, uma vez que os nós da Internet guardam sempre as correspondências ARP

na memória cache, de forma a aumentar o desempenho. Pelo mecanismo de Proxy ARP estas "caches" só vão ser alteradas com a nova informação correcta quando as entradas relevantes expirarem naturalmente, o que vai atrasar o processo MIP para os fluxos já existentes. Este problema é resolvido forçando a alteração das caches dos nós envolvidos, de forma a que estes fiquem coerentes. Este mecanismo, denominado de "Gratuitous ARP"[1][11], consiste na emissão voluntária (não solicitada), por parte do Home Agent, de uma resposta ARP referente ao Terminal Móvel, que obrigue todos os nós a alterarem as suas "caches" ARP com a nova informação.

Desta forma o Home Agent irá receber todos os pacotes IP que são destinados ao Terminal Móvel. O próximo passo será entregá-los, intactos, ao Terminal Móvel na sua localização actual. Quando este está registado por um Foreign Agent, o Home Agent enviará os pacotes IP inteiros (cabeçalho IP + dados IP) para o Foreign Agent, que já os estará a aguardar (devido ao processo de registo que ocorreu previamente). Quando o Foreign Agent recebe estes pacotes, então bastará que os entregue ao Terminal Móvel pelos mecanismos de nível 2 existentes, para este os receber tal e qual, como se estivesse localizado fisicamente na sua rede de origem. É importante notar que se o Foreign Agent entregasse ao Terminal Móvel os seus pacotes **pelos mecanismos de nível 3** iria ser criado um ciclo de encaminhamento sem solução, uma vez que estes iriam voltar (novamente) à rede de origem do Terminal Móvel (porque o endereço fixo nível 3 do terminal móvel diz que este esta localizado na sua rede de Origem sempre).

Existe também uma outra situação possível (já descrita): Quando o Terminal Móvel se movimentar para uma rede que não possua um Foreign Agent, então este poderá estabelecer os mecanismos de Macro-Mobilidade sozinho, necessitando neste caso de alocar um endereço IP na rede visitada, durante o período que lá estiver localizado. No seu processo de registo, o Terminal Móvel vai indicar ao Home Agent que deverá enviar os pacotes que lhe eram destinados para este endereço IP temporário.

Relativamente aos pacotes enviados no sentido oposto da comunicação (isto é, os pacotes enviados pelo Terminal Móvel para os seus interlocutores) estes podem ser simplesmente encaminhados pelos mecanismos normais de encaminhamento da Internet. Esta simplificação deriva do facto do encaminhamento ser sempre efectuado com base no endereço de destino dos pacotes. Eventualmente, estes pacotes poderão destinar-se a terminais também móveis, pelo que neste caso os mecanismos de Macro-Mobilidade irão aplicar-se nos dois sentidos do tráfego IP. Uma excepção a este caso está presente na opção de privacidade da localização, já referida anteriormente.

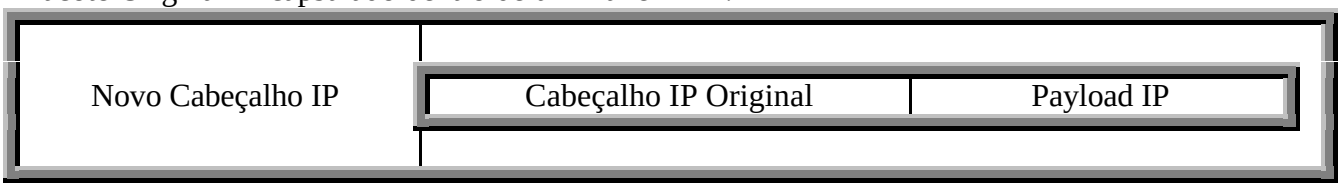
Por fim, falta apenas descrever a forma como os pacotes irão viajar desde o Home Agent até ao Foreign Agent correspondente (ou directamente para o Terminal Móvel, como foi visto). Para manter todo o resto do stack TCP/IP inalterado, o Terminal Móvel terá que receber os pacotes IP perfeitamente intactos, tal e qual como se estivesse localizado na sua rede de origem. Isto significa que todos os campos do pacote IP (cabeçalho + opções + "Payload") terão que possuir os valores originais. No entanto os encaminhadores da Internet têm competências para modificar, se necessário, os campos do cabeçalho dos pacotes IP (em particular o campo TTL, "time-to-live"), o que significa que os pacotes originais terão que viajar desde o Home Agent até ao seu destino de uma forma protegida.

A forma mais simples de efectuar esta entrega, nas condições acima referidas, será o estabelecimento de um túnel IP [6] entre os dois agentes de mobilidade. Neste túnel são enviados os pacotes IP originais destinados ao Terminal Móvel (que dentro do túnel serão considerados dados), o que garante que não poderão ser alterados no seu percurso. Assim, o Home Agent vai encapsular os pacotes IP originais, destinados ao Terminal Móvel, dentro de novos pacotes IP, destinados ao Foreign Agent (ou ao endereço temporário do Terminal Móvel na rede visitada). Por sua vez o Foreign Agent desencapsula os pacotes quando os receber, de forma a obter o pacote IP original. Quando os pacotes IP forem reconstituídos, estes já poderão ser entregues ao seu destinatário, o Terminal Móvel.

Este mecanismo de encapsulamento pode ser visualizado pelos seguintes esquemas:

Pacote Original IP:

Pacote Original Encapsulado dentro de um Túnel IPIP:



Ou então pelo esquema detalhado, presente no **anexo C.**

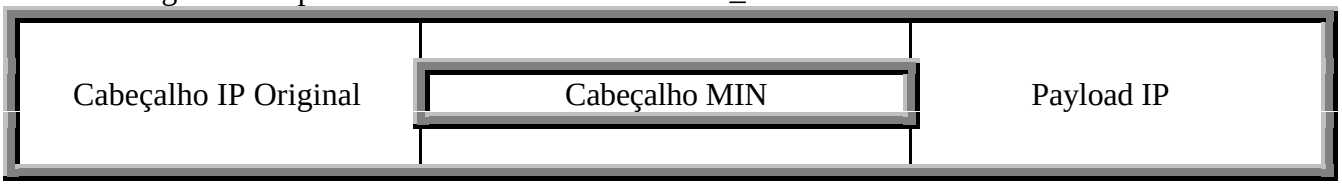
Esta forma de encapsulamento é bastante simples, o que leva a que o encapsulador e o desencapsulador sejam também bastante simples. No entanto, esta facilidade tem o custo de ser pesada relativamente à de utilização dos recursos (uma vez que o IP Móvel está vocacionado para operar em ambientes wireless, nos quais a largura de banda é um recurso escasso), devido a adicionar ainda mais 20 bytes por cada pacote de informação. Para este problema o protocolo MIP prevê a utilização de um tipo de encapsulamento mais eficiente, chamado de "minimal encapsulation". Este novo encapsulamento é bastante semelhante ao IPIP, com a diferença que vai aproveitar as semelhanças dos dois cabeçalhos IP (do pacote original e do pacote Envolvente) para reduzir o "overhead".

Assim este encapsulamento vai utilizar e modificar o cabeçalho IP original, e um novo cabeçalho (mínimo) de encapsulamento é introduzido antes dos dados IP. Este novo cabeçalho vai ser tratado como dados (pelo que não pode ser modificado), e contém os campos necessários para reconstituir o cabeçalho IP original no destino.

Este encapsulamento é facilmente descrito nos seguintes esquemas:

Pacote Original IP:

Pacote Original Encapsulado dentro de um Túnel MIN_IPIP:



O esquema detalhado encontra-se no anexo C.

Este encapsulamento permite poupar 8 bytes de overhead por pacote, tendo um máximo de 12 bytes adicionais. No entanto, quando o emissor do pacote original for o mesmo que está a encapsular o pacote, mediante a utilização de uma flag apropriada no campo flags (MIN) é possível reduzir este overhead para 8 bytes, ao não incluir o campo referente ao endereço IP original (dado que seria igual ao campo endereço Origem, presente no cabeçalho IP envolvente).

Para esta encapsulamento vão haver também dois outros campos que desaparecem: Offset de Fragmentação e TTL, sendo utilizados apenas os campos do cabeçalho IP envolvente para este efeito. Estas ausências (que reduzem o "overhead") implicam que este encapsulamento só se poderá aplicar a pacotes IP que não estejam fragmentados, e que o número de "hops" que separam as extremidades do túnel MIN_IPIP passam a tornar-se visíveis.

Relativamente à operação de desencapsulamento do pacote IP original, esta é concretizada no fim do túnel por substituição do endereço IP de destino, guardado no cabeçalho MIN, e opcionalmente do endereço IP de origem (conforme a flag, tal como foi descrito).

Todo o processo desta fase pode ser visualizado nas figuras 16 a 19, que descrevem os diagramas temporais da situação normal do MIP, do Terminal móvel com DHCP, dos Interlocutores com MIP e das duas opções simultaneamente.

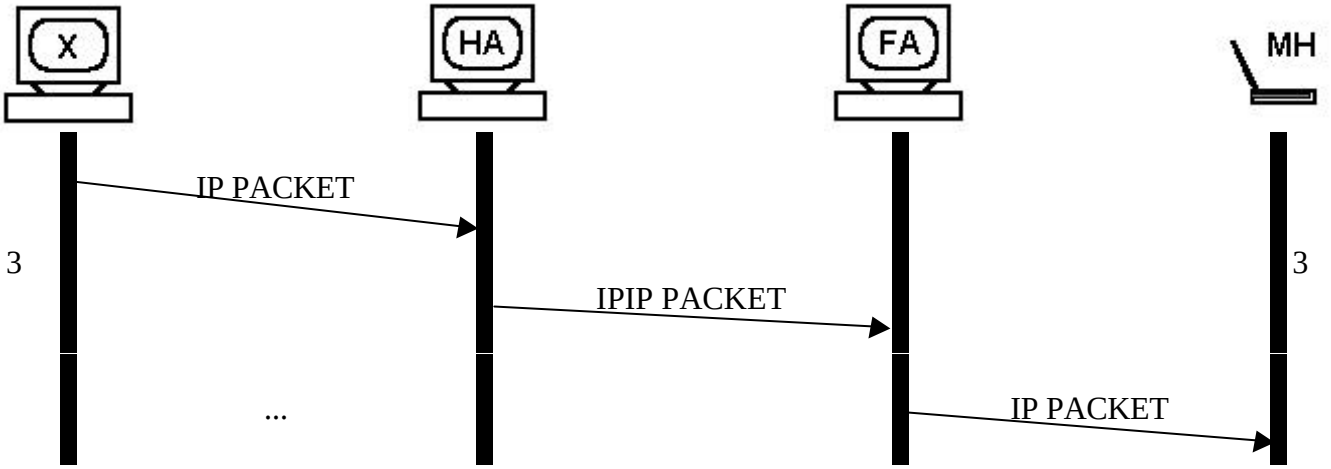


Figura 16 - MIP - Caso Normal - Fase 3

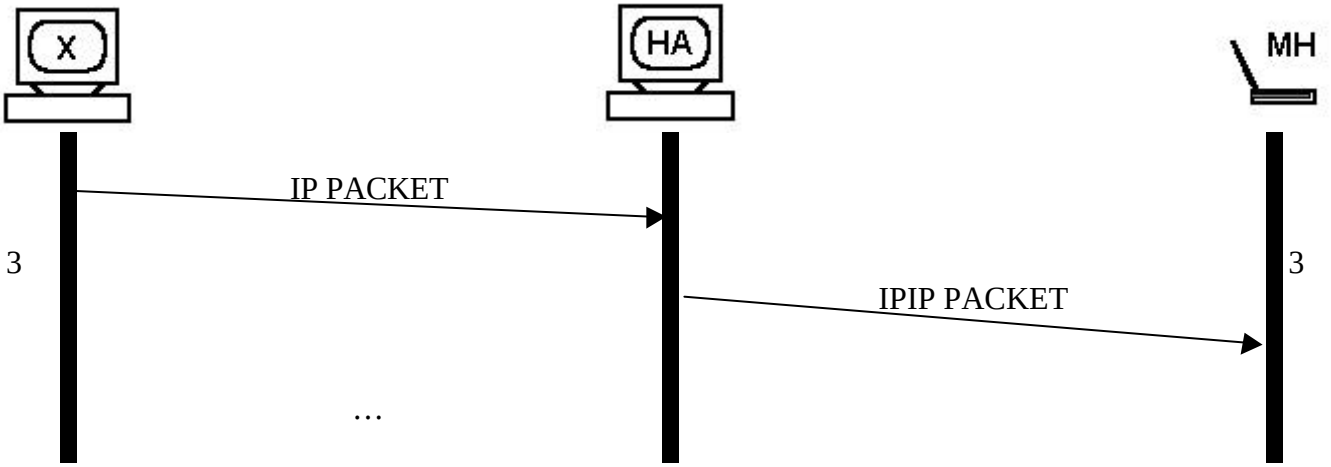


Figura 17 - MIP - Terminal Móvel sozinho sem Foreign Agent - Fase 3

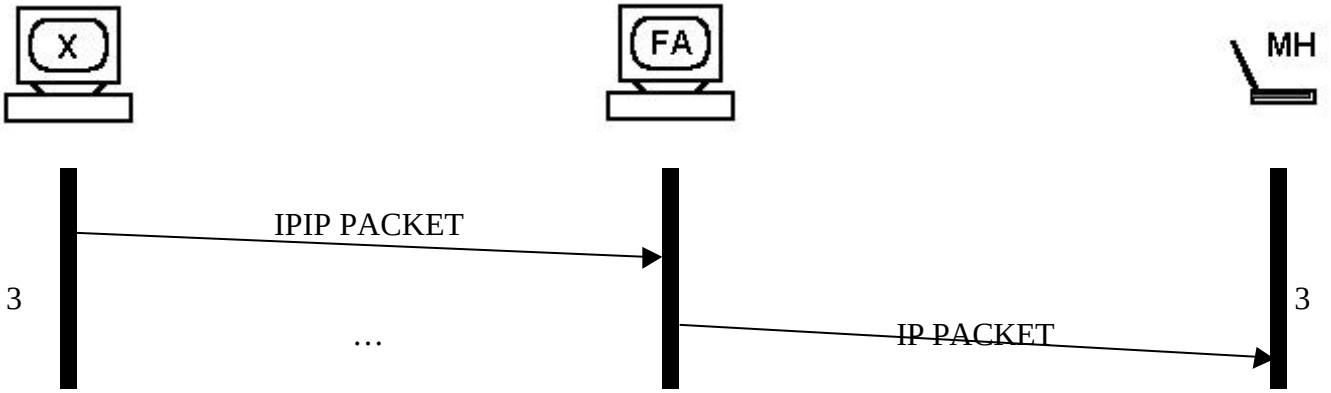


Figura 18 - MIP - Encaminhamento Sem Triangulação - Fase 3

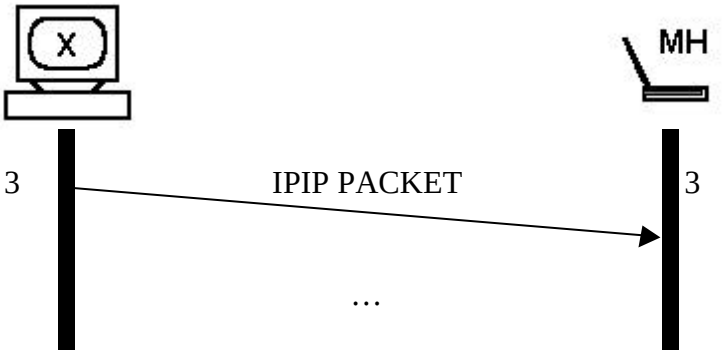


Figura 19 - MIP - Terminal Móvel Sozinho sem Foreign Agent + Sem Triangulação - Fase 3

Modificações no Encaminhamento dos Pacotes e "Firewalls"

A utilização do MIP faz surgir novas situações potencialmente muito perigosas, pelo que terão sempre que serem tratadas de forma muito cuidadosa e controlada. O tipo de encapsulamento utilizado pelo MIP na entrega dos pacotes ao Terminal Móvel pode abrir novas brechas da segurança, pois é possível "injectar" pacotes IP no interior de qualquer rede, através deste processo.

Tipicamente, as redes têm mecanismos de segurança de filtragem de pacotes nas suas ligações ao exterior ("firewalls"), que verificam todos os pacotes que entram e saem da rede a proteger, onde se podem criar diferentes políticas de aceitação e recusa dos pacotes. Assim é normal as "firewalls" recusarem todas os fluxos de dados iniciados de fora para dentro e aceitar os fluxos iniciados de dentro para fora, mas só de alguns protocolos. Estas regras genéricas podem ter excepções relativas a certos utilizadores privilegiados, por meio de autenticação.

Uma vez que o protocolo de encapsulamento IPIP (e derivados) pode constituir uma falha grave de segurança as firewalls vão, por defeito, barrar este protocolo, que constitui o mecanismo base de operação do MIP. Por outro lado, mesmo as firewalls que aceitem pacotes encapsulados terão que ter o cuidado de efectuar as suas filtragens no pacote IP **interno**, pois se procederem como normalmente irão filtrar os pacotes baseados no cabeçalho envolvente, que é distinto do verdadeiro pacote IP (agora encapsulado).

Estes problemas são muito comuns, estando neste momento em estudo pelo IETF. A solução que se apresenta como mais promissora passa por novas extensões ao protocolo, que são utilizadas em novas interacções MIP autenticadas entre os agentes de mobilidade e as firewalls que estejam no seu caminho, com o intuito de abrir canais privilegiados de comunicação pela firewall, entre os dois agentes de mobilidade, o que possibilitaria o envio com sucesso dos pacotes encapsulados IPIP destinados a terminais móveis.

Desta maneira é natural que os mecanismos proporcionados pelo protocolo MIP falhem quando existe uma firewall no caminho que liga o Home Agent ao Foreign Agent (a menos que se trate de uma firewall muito pouco restritiva, o que não daria garantias de segurança para as outras situações).

3.4 - Segurança

O Mobile IP é, tal como foi apresentado, um protocolo poderoso no sentido em que permite redireccionar **todo** o tráfego destinado a um Terminal Móvel para uma qualquer localização da Internet. No entanto, sem os mecanismos que serão apresentados de seguida, seria absolutamente trivial um utilizador mal intencionado poder atacar o sistema e efectuar duas acções distintas, com dois níveis de gravidade diferentes [4][5]:

1 – emitir periodicamente, em nome do Terminal Móvel, pedidos de cancelamento de registo aleatórios, destinados ao Home Agent e aos Foreign Agents, que baralhem o protocolo e saturem os agentes de mobilidade. Este ataque seria **grave**, uma vez que teria como consequência que os serviços de Macro-Mobilidade não iriam ser fornecidos, ficando o Terminal Móvel permanentemente inacessível aos nós da Internet, em todas as situações que não estivesse na sua rede de origem.

2 – Emitir periodicamente, em nome do Terminal Móvel, pedidos de **Registo** para uma localização diferente da que o Terminal Móvel efectivamente está. Desta forma o atacante tomaria o lugar do Terminal Móvel, passando a receber todo os pacotes destinados ao Terminal Móvel. Uma vez que qualquer nó da Internet pode emitir pacotes IP com os campos que entender, o atacante também poderia assim responder aos interlocutores do Terminal Móvel como se fosse o terminal, o que efectivamente criava uma situação que, do ponto de vista dos seus interlocutores, o atacante era o Terminal Móvel. Esta situação seria **muito grave**, pois qualquer entidade que "acredite" na identidade do Terminal Móvel pode-lhe enviar dados confidenciais, sem reservas.

Esta situação seria um ataque **activo**, uma vez que o atacante poderá enviar e receber pacotes em nome do Terminal Móvel; também trivial seria o ataque **passivo**, em que o atacante faria passar por si todos os fluxos de informação destinados ao Terminal Móvel, inspeccionava-os, e entregava-os ao seu verdadeiro destinatário. Desta maneira, o Terminal Móvel nunca se iria aperceber do ataque que estava a acontecer, ficando o atacante com a possibilidade de conhecer todos os pacotes do Terminal Móvel. Nesta, situação bastaria a apreensão de um pacote TCP que contivesse uma password enviada a descoberto, situação normal dos protocolos Telnet/FTP não seguros, para este poder imediatamente fazer novos ataques.

Este ataque é semelhante ao caso em que um utilizador mal-intencionado escuta a linha, com mecanismos apropriados que apanham todos os pacotes presentes (as ferramentas de "packet sniffing", por exemplo) e que executam, posteriormente, a mesma filtragem referida, uma vez que nestes casos as informações confidenciais são enviadas a descoberto. No entanto, a grande diferença é que neste caso o atacante teria que estar localizado **fisicamente** na rede do Terminal Móvel; Com as capacidades MIP esta restrição desaparece, podendo o atacante estar localizado fisicamente em qualquer ponto da terra e conseguir escutar "remotamente" os pacotes destinados ao Terminal Móvel.

Por estas razões a segurança é um aspecto fundamental no protocolo MIP, sendo esta mandatória entre os terminais móveis e os Home Agents e opcional entre os terminais móveis e os Foreign Agents e entre estes últimos e os Home Agents.

Assim todas as mensagem MIP trocadas entre o Terminal Móvel e o seu Home Agent têm **sempre** que conter uma extensão de autenticação, calculado por um algoritmo previamente estabelecido, que garanta que todas as informações presentes nesta mensagem (os diversos campos do cabeçalho MIP e as extensões presentes) foram de certeza emitidos pela entidade correcta. Esta certeza vai-se basear em duas pecas chave do processo de autenticação:

- o algoritmo de autenticação - hoje em dia existem algoritmos genéricos muito poderosos, do domínio publico, denominados de "não invertíveis", que a partir de um conjunto de dados (de qualquer tamanho), criam um pequeno resumo (denominado de "digest"). Este resumo vai ser adicionado à própria mensagem, e garante aos potenciais interessados a autoria destes dados.

- A chave secreta – enquanto houve o cuidado de garantir que os algoritmos de autenticação fossem tornados públicos (de forma a serem estudados exaustivamente), esta a informação terá necessariamente de permanecer secreta entre as duas partes (emissor e receptor). Assim, a chave secreta é um conjunto de dados que, pelos algoritmos acima referenciados, transforma os dados originais no seu pequeno resumo.

Esta transformação (Dados Originais + Algoritmo + Chave = Resumo) tem importantes características que derivam de o algoritmo ser, como foi referenciado, não invertível. Assim os mesmos dados originais produzem resumos completamente diferentes quando são aplicadas diferentes chaves, e diferentes (mesmo que ligeiramente) dados originais resultarão em resumos completamente distintos (mesmo no caso em que são aplicadas a mesma chave de resumo). Uma vez que pequenas diferenças na chave ou, nos dados originais, produzem sempre resultados substancialmente diferentes significa que não se pode, em tempo útil, estabelecer relações entre os dados originais e os seus resumos, o que impossibilita que se extrai-a a parte secreta do processo, a chave, com base apenas nos dados e nos seus resumos.

Considerando sempre que a chave permanece secreta entre emissores e receptores, os emissores produzem os dados e acrescentam à mensagem o resumo calculado com a chave secreta, emitindo para a rede este par (dados+resumo).

Quando o receptor recebe a mensagem vai-se certificar da autoria dos dados, uma vez que irá (também) calcular o resumo dos dados que recebeu, com a (mesma) chave secreta que está partilhada entre as duas entidades. Depois, vai comparar o resumo calculado com o resumo presente na mensagem, e apenas se estes forem exactamente iguais é que o receptor terá a certeza que estes dados foram produzidos e enviados pelo emissor pretendido.

Este mecanismo é muito seguro, uma vez que um atacante que modificasse as mensagens escutadas na rede, ou que as criasse ele próprio com o objectivo de enganar o receptor, não teria o acesso à chave secreta partilhada (nem a consegue descobrir, com foi descrito), o que implica que não iria conseguir criar um resumo da mensagem válido.

Desta forma, é garantida a segurança da comunicação no que respeita à autoria das mensagens trocadas. No entanto existe um caso, em que um atacante mesmo sem conhecer a chave secreta vai conseguir baralhar o sistema, e causar desta forma dano. Para isso o atacante tem apenas que escutar e guardar as mensagens trocadas entre emissores e receptores, e reenviá-las quando desejar, o que vai repetir o efeito que estas têm no protocolo. Por exemplo, um atacante que consiga capturar uma mensagem de cancelamento de registo MIP de um dado Terminal Móvel poderá enviá-la de novo, quando quiser, com o objectivo de cancelar de registo o Terminal Móvel em qualquer altura (o que causara a inacessibilidade deste). Quando o Home Agent recebe esta mensagem (repetida pelo atacante) este vai aceita-la e processa-la, uma vez que o seu resumo corresponde exactamente à mensagem original (porque o atacante apenas reenviou a mensagem, **sem a alterar**).

Esta situação tem uma solução simples que obriga a que um receptor nunca aceite duas vezes a mesma mensagem. Para isso é reservado um campo na mensagem que será utilizado especificamente para esta protecção adicional. Existem dois processos comuns de protecção:

- Protecção por tempo actual – Neste caso o emissor coloca o seu tempo actual juntamente com os dados da mensagem, e o receptor terá a responsabilidade de verificar se este tempo está suficientemente próximo do seu próprio tempo, de forma a que tenha a certeza que esta mensagem foi criada pelo emissor à poucos instantes, e não se trata de uma repetição de uma mensagem anterior por parte de um atacante. Para este processo é essencial que os relógios do emissor e receptor estejam (minimamente) sincronizados, sendo uma decisão de implementação o valor de tempo que se considera máximo para o atraso da mensagem (isto é, o valor de tempo em que o receptor deixa de aceitar mensagens).
- Protecção por Identificadores Aleatórios – Neste tipo de protecção tanto o emissor como o receptor marcam as suas mensagens com Identificadores aleatórios, exigindo que as

respostas às suas mensagens contenham exactamente o mesmo identificador enviado. Sempre que o emissor pretende mandar uma **nova** mensagem, vai colocar um **novo** identificador (diferente de todos os outros, uma vez que este é gerado aleatoriamente), e só vai aceitar uma resposta que contenha exactamente esse Identificador, ignorando todas as outras. Este processo é o que foi descrito relativamente ao campo "Identificação" nas mensagens de Registo e Resposta MIP.

Tendo em vista este processo complementar fica claro que um atacante (sem saber a chave secreta partilhada entre emissor e receptor) nunca conseguirá atacar este sistema, uma vez que se modificar/criar mensagens MIP o resumo nunca será aceite, e se este repetir mensagens verdadeiras estas serão sempre ignoradas.

O MIP só obriga à existência de autenticação entre os dois extremos da comunicação, isto é, entre o Terminal Móvel e o seu Home Agent, embora preveja (mas não obriga) o caso de autenticação destes com os Foreign Agents. Neste sentido, esta opção é considerada da responsabilidade de cada implementação e das suas politicas de Segurança/Administração/Confidencialidade. Existem vários assuntos importantes associados à segurança, mas que saem do âmbito do protocolo MIP. Entre estes incluem-se:

- Controlo/Difusão de Chaves – Como foi descrito a segurança do protocolo torna-se se tão boa quanto a segurança da entrega das chaves secretas, isto é, um atacante fica impotente sem a chave secreta, passando a conseguir agir sem restrições no momento que a adquire. Normalmente, a chave secreta é derivada de palavras chave (passwords), ou pode apenas ficar num ficheiro de configuração do emissor e receptor. Quando existir um protocolo eficiente e seguro de distribuição de chaves na Internet, então este problema irá ser resolvido.
- Contabilização e Taxação – a autenticação descrita é um bom meio para suportar estas operações num ambiente comercial, no qual a utilização de Macro-Mobilidade (em especial nos Foreign Agents) será sempre contabilizada, e fazendo eventualmente parte de um serviço Internet a cobrar aos seus utilizadores. Por outro lado a autenticação é uma forma administrativa de garantir que o serviço MIP só é prestado aos utilizadores autorizados de um Fornecedor de Serviços Internet.
- Escolha de verdadeiros números aleatórios – Todos os mecanismos de segurança baseiam-se no nível de secretismo de uma peca chave do sistema (neste caso, a chave secreta), pelo que se esta for gerada de uma forma perfeitamente aleatória irá ser ainda mais difícil de descobrir. Outra consideração prende-se com a dimensão da chave: tendo chaves maiores podem aumentar exponencialmente os recursos (tempo de computação) necessário para as quebrar; No entanto chaves maiores também aumentam o peso ("overhead" + tempo de cálculo) da segurança no protocolo a proteger. Outra situação que requer números aleatórios o mais verdadeiros possível é a protecção de repetições, tal como foi descrita acima.
- Privacidade de Dados – Os mecanismos descritos fornecem apenas Autenticação, isto é, só fornecem garantias relativamente à autoria das mensagens do protocolo. Se os próprios dados a trocar são confidenciais então dever-se-á utilizar mecanismos de encriptação, que os protejam de atacantes que estejam no caminho dos pacotes. Este problema também se põem mesmo sem os mecanismos de Macro-Mobilidade, pois no encaminhamento normal da Internet qualquer router que esteja no caminho dos pacotes tem acesso à parte de dados dos pacotes, podendo inspeccioná-los com o objectivo de encontrar informações confidenciais.
- Privacidade de Localização – este segundo tipo de privacidade só aparece com o aparecimento destes novos mecanismos de Macro-Mobilidade, pois como será descrito, o tráfego entregue ao Terminal Móvel será sempre enviado para a sua rede de origem (o que cria privacidade de localização, uma vez que os interlocutores não sabem

exactamente onde é que o Terminal Móvel se encontra), mas não o tráfego enviado por este para a rede (que será entregue de forma directa, pelos mecanismos normais de encaminhamento da Internet). Esta situação significa que os interlocutores do Terminal Móvel se podem aperceber da sua localização física exacta, o que poderá ser um problema para alguns utilizadores. Esta situação será resolvida nestes casos (como vai ser descrito) estabelecendo um segundo túnel entre o Foreign Agent e o Home Agent, destinado à entrega de pacotes emitidos pelo Terminal Móvel. Desta forma o Home Agent irá receber e enviar todos os pacotes do terminal, pelo que os pacotes emitidos irão entrar no encaminhamento da Internet na rede de Origem, o que vai dificultar bastante a localização física do Terminal Móvel.

O MIP define uma extensão de autenticação detalhada no anexo B, que deverá ser utilizada em todas as mensagens MIP.

O protocolo MIP possibilita a utilização de vários mecanismos de autenticação, sendo o MD5 obrigatório em todas as implementações. Este mecanismo é do domínio público, existindo implementações gratuitas. Este algoritmo suporta diferentes comprimentos de chaves de codificação e aplicado a um conjunto de dados irá produzir o resumo correspondente.

O MIP define a forma como o resumo é calculado, a partir do conjunto de dados. Assim, o algoritmo é aplicado (por esta ordem) ao conjunto da chave secreta, seguido do cabeçalho MIP da mensagem, seguido das extensões a proteger, seguido do campo “tipo” e “comprimento” desta extensão de autenticação e finalizado com a chave secreta novamente.

Por este processo irá ser calculado o resumo da mensagem MIP, que irá ser colocado no campo “Autenticação” desta extensão.

Quando o receptor da mensagem receber esta mensagem, então irá efectuar exactamente a mesma operação, sobre os mesmos campos da mensagem. Se o resumo calculado desta forma não coincidir com o presente nesta extensão, então o receptor não vai aceitar esta mensagem, porque a segurança não está garantida.

4 – Implementação do MIP em Linux

4.1 - Introdução da Implementação

Para a implementação prática do MIP foi escolhido o Sistema Operativo **Linux**, derivado do Unix, dado que este sistema oferece grandes funcionalidades e flexibilidade relacionadas com a utilização do seu stack TCP/IP. Embora este stack seja muito completo, este ainda **não dispõem de uma implementação do MIP**, o que o torna a escolha ideal para este Trabalho Final de Curso. Nestas condições foram desenvolvidos em linguagem **C,** dois programas de software que têm o comportamento de "**deamons**" Unix: um **cliente MIP**, que instancia a Macro-Mobilidade num **Terminal Móvel**, e um **servidor MIP**, que instancia os **agentes de mobilidade** (Home + Foreign Agents).

Relativamente ao MIP podem-se identificar dois fluxos de informação distintos envolvidos: o controlo e os dados MIP.

O primeiro fluxo vai ser constituído pelas mensagens de controlo e localização, que são transferidas durante as fases de Localização e Registo. O segundo fluxo é constituído pelas mensagens de dados MIP, que são os pacotes IP que são encapsulados dentro do túnel IPIP, sendo transferidas durante a fase de Execução.

Uma vez que os dados MIP constituem a grande maioria dos pacotes MIP, isso leva a que qualquer implementação separe estes dois fluxos de informação. Esta assimetria dados/controlo MIP conduziu a uma solução simples que privilegia o processamento do controlo MIP baseado nos dois deamons referidos que se executam fora do núcleo do sistema operativo (em "user-space") enquanto que o processamento dos dados MIP é efectuado no interior deste (em "kernel-space"). Desta forma consegue-se optimizar o desempenho do processamento dos dados e reutilizar o máximo de software genérico já existente, sem ter que realizar alterações nas restantes partes do stack TCP/IP.

Estes dois deamons (**host_mip** e **agent_mip)** foram escritos na linguagem **C** e destinam-se a ser compilados pelas ferramentas comuns de desenvolvimento do Linux **gcc** e **make**. Os novos deamons destinam-se a serem activados na inicialização do sistema operativo, e permanecem activos (em background) durante toda a vida deste. No entanto os "deamons" também podem ser iniciados e finalizados numa qualquer altura, não necessariamente na inicialização do sistema operativo.

Conforme já foi referido, a componente de dados MIP vai estar completamente baseada nos mecanismos já existentes no stack TCP/IP do Linux, no interior do núcleo do sistema operativo. Estes mecanismos vão ser controlados dinamicamente pelos "deamons", em conformidade com as mensagens de controlo MIP trocadas entre as várias entidades associadas ao processo de Macro-Mobilidade na Internet.

Estas interacções existentes com o stack TCP/IP do Linux são implementadas com o recurso aos comandos externos standard do sistema Linux, em que cada comando externo vai operar num módulo diferente do stack. Desta forma, ambos os programas foram desenhados para uma utilização intensiva e completamente automática, mas onde existiu a preocupação de minimizar o peso do novo protocolo no desempenho do sistema operativo.

4.2 - Funcionalidades do Sistema Operativo Linux

Para a implementação prática do Mobile IP deste Trabalho foi utilizado o Sistema Operativo **Linux** [12] a [15]. Este sistema é uma implementação bastante divulgada de um sistema Unix completo, existindo implementações para arquitecturas de computadores diferentes. A implementação de Linux para Computadores Pessoais baseados em microprocessadores x86 é sem dúvida a mais divulgada, existindo também implementações completas do Linux para sistemas embebidos.

O sistema Linux é desenvolvido e distribuído por uma política de desenvolvimento significativamente diferente de outros sistemas operativos proprietários: O sistema é completamente

grátis, o que significa que a sua divulgação está sempre a crescer. Por outro lado, o sistema é completamente **aberto** ao desenvolvimento por utilizadores normais, o que significa que é sempre possível obter o código fonte de qualquer parte do sistema, e das suas aplicações que correm sobre este, de forma a que tudo pode ser livremente modificado à medida das necessidades.

Estas duas características explicam o facto de este ser bastante robusto mesmo estando em constante desenvolvimento: existe neste momento uma enorme "massa humana" que trabalha continuamente no sistema para o beneficio da "comunidade Linux". Isto significa que falhas ("bugs") do sistema e das aplicações são continuamente descobertas e corrigidas. Esta enorme "massa humana" também é responsável pelo desenvolvimento rápido de "drivers" do sistema para uma parte considerável do hardware existente (adaptadores de rede, adaptadores de vídeo, discos rígidos, …).

Um sistema Linux é composto pelo núcleo do sistema (denominado de "kernel") e pelas suas aplicações de suporte, podendo cada parte interagir com a outra. Este último grupo é dividido em aplicações, comandos externos e deamons. É nas aplicações que existe um conjunto alargado de programas relativos a processadores de texto, ambientes de desenvolvimento, manipulação de imagem, aplicações vocacionadas para Internet, entre muitos outros. Os comandos externos são os comandos que interagem com o utilizador que lhe permitem manipular o sistema operativo. Por fim, os deamons são os programas que se executam permanentemente sem interagirem com o utilizador, e que executam diversos protocolos (fora do núcleo).

É no núcleo que estão presentes as funcionalidades mais básicas do sistema: gestão de processos, memória, drivers e stacks de protocolos (em particular o TCP/IP), entre outros módulos. Esta dualidade está representada na seguinte figura, onde estão presentes alguns dos constituintes mais importantes do Linux:

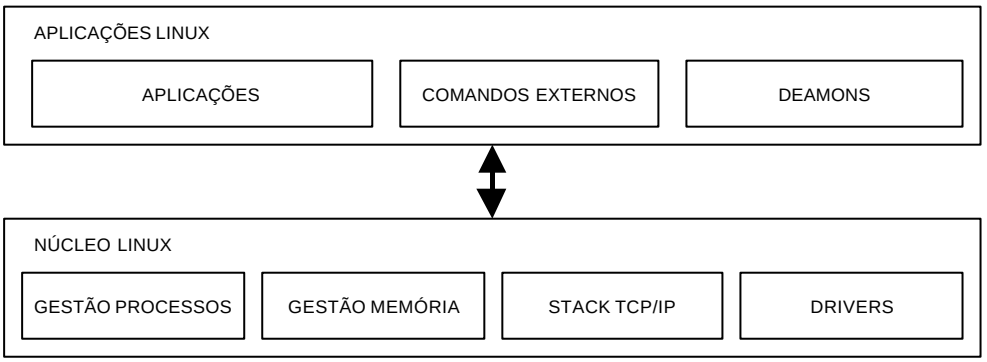


Figura 20 - Organização do Sistema Operativo Linux

Existem bastantes variações do Linux, sendo os dois aspectos mais importantes: a **versão** do núcleo e a **distribuição**. Actualmente existem sempre duas versões do núcleo do Linux activas: a versão de desenvolvimento (que acaba num número impar) e a versão estável (que acaba num número par). É na versão de desenvolvimento que são incorporados no núcleo do Linux as tecnologias mais recentes, mas que ainda não estão suficientes "maduras" para serem integradas na versão estável.

Neste sentido, para um sistema de utilização/desenvolvimento típico utiliza-se a versão estável do núcleo mais avançada que existe. Mesmo neste caso existem diferenças significativas de Linux para Linux, relativamente à distribuição escolhida. Uma distribuição de Linux é a soma de um núcleo Linux com um conjunto (maior ou menor) de aplicações de suporte. Assim, para a mesma versão do núcleo, a diferença vai residir na escolha das aplicações de suporte de cada distribuição. Esta flexibilidade significa que existem distribuições de Linux que cabem em duas "diskettes" (as mini-distribuições), passando pelas distribuições completas típicas de um a dois CDROMs, ate às mega-distribuições hiper-completas de seis CDROMs.

Assim qualquer distribuição actual de Linux é suficiente para a realização prática do MIP no Linux, uma vez que este trabalho se centra apenas no stack TCP/IP, presente no núcleo do Linux,

sem o recurso a aplicações externas que não as "standard". No caso concreto deste trabalho foi utilizada a distribuição de Linux da **RedHat**, versão **5.1**, sendo a versão do núcleo Linux a **2.2**. Entre diferentes versões do Linux existe compatibilidade ascendente imediata (de uma versão antiga para uma mais recente); a compatibilidade no sentido contrário não é garantida (pelo menos sem modificações ao código desenvolvido).

4.2.1 - Interacção com o Sistema

Para interagir com qualquer modulo do sistema operativo (em particular neste trabalho, com o stack TCP/IP), as aplicações podem recorrer a duas formas: os comandos internos e os externos [16].

Todas os módulos que constituem o núcleo do sistema Linux fornecem serviços às aplicações, sendo estes invocados através de funções genéricas, sendo a mais usada a função **ioctl**. Esta função tem nos seus parâmetros a informação respeitante ao módulo a interagir, a função específica a invocar e seus o(s) parâmetro(s). Desta forma é possível às aplicações do utilizador dispor de funcionalidades que nunca lhe estariam acessíveis, pois estas funções interagem directamente com as estruturas de dados do núcleo (de uma forma controlada).

Esta forma de invocar o sistema é a mais eficiente, mas também é a mais complexa e de difícil depuração, uma vez que qualquer erro na interacção com o sistema pode ter resultados potencialmente desastrosos. As aplicações que vão manipular as tabelas do núcleo têm necessariamente de serem executadas com privilégios, normalmente negados às aplicações normais (em Unix denominados de "root"), o que implica que não existem quaisquer restrições às acções destes programas. Na **figura 21** exemplifica-se a utilização dos comandos internos para a configuração directa do stack TCP/IP do Linux.

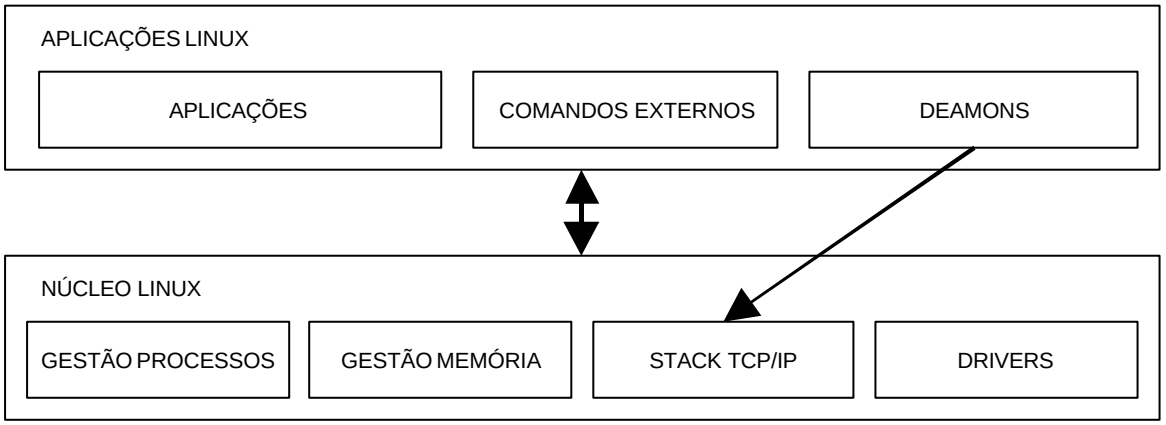


Figura 21 - Comandos Internos

Outra forma de obter o mesmo resultado (típica da programação em Unix), consiste em utilizar os comandos externos standard do sistema que são disponibilizados juntamente com os módulos do sistema para a sua configuração pelos programas (ver **figura 22**). Embora a execução de comandos externos seja substancialmente mais demorada que a invocação de funções do núcleo, esta forma de manipulação dos recursos do sistema é muito mais fácil de programar (e depurar), uma vez que estes comandos externos validam sempre os seus argumentos e não têm erros, porque já foram utilizados inúmeras vezes. Por outro lado, uma sequência de comandos externos é facilmente reconstituída por processos manuais, em qualquer altura, o que já seria difícil se fossem utilizados os comandos correspondentes internos. Estas características foram decisivas para privilegiar a utilização dos comandos externos para a configuração do stack TCP/IP do linux pelos novos "deamons" MIP

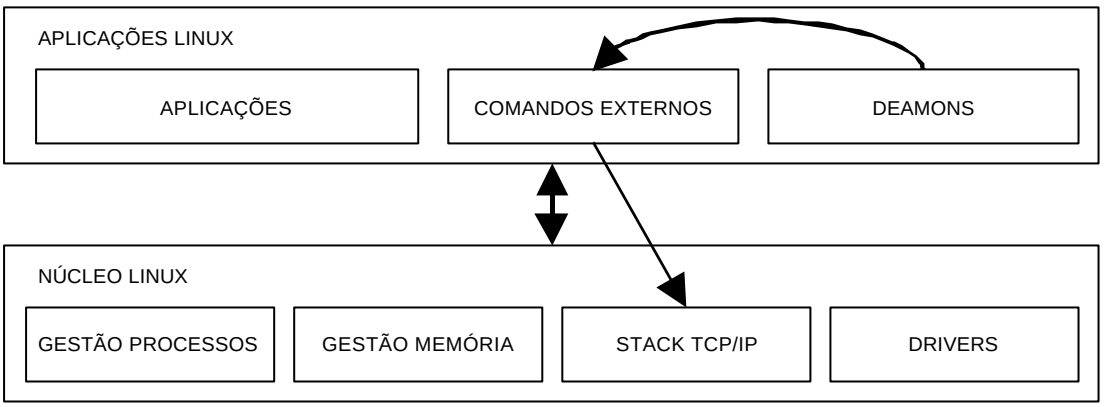


Figura 22 - Comandos Externos

4.2.2 - "Deamons" Unix

O protocolo MIP foi implementado em Linux com dois novos programas de software denominados de **host_mip** e **agent_mip**, implementando o primeiro a funcionalidade dos terminais móveis (clientes MIP), e o outro a dos agentes de mobilidade, nos dois papeis de Home Agent e Foreign Agent (servidores MIP). Ambos os programas foram desenhados para se comportarem como "deamons" de Unix, executando-se em "user space" [16].

Em Unix, um "deamon" é um programa de software que executa um determinado protocolo e que é normalmente invocado no arranque do sistema operativo. Ao contrário dos outros programas que acompanham o sistema operativo, os "deamons" não têm (tipicamente) qualquer interacção com o utilizador, sendo apenas configurados no seu arranque. Isso significa que os "deamons" executam-se continuamente em "background" durante toda a vida do sistema operativo (o que em Unix pode chegar a meses inteiros de execução continua, sem quebras de serviço).

Esta forma de execução significa que os "deamons" operam num ciclo infinito de execução, nunca terminando (voluntariamente) a sua execução. Neste ciclo, os deamons são processos que estão normalmente inactivos, presos nas filas de espera internas do núcleo do sistema operativo. A execução só acontece quando o processo é acordado pelo sistema operativo, o que pode ser quando existem explicitamente dados destinados ao processo, vindos da comunicação inter-processos, estruturas de semáforos ou caixas de correio internas do núcleo, quando existe actividade em sockets do "deamon", ou quando o núcleo envia um sinal ("signal") ao processo.

Em todos estas situações o processo é "acordado" pelo núcleo, continuando o seu fio de execução onde estava quando foi bloqueado (tipicamente numa chamada explicita de "sleep" ou numa leitura síncrona de dados), processando as mensagens entretanto acumuladas pelo núcleo para o deamon; depois deste processamento o deamon regressa ao seu estado de repouso, do qual apenas sairá posteriormente quando existirem novas mensagens para processamento.

Existe uma outra forma de codificar os "deamons" que apenas se justifica nos casos de componentes essenciais do sistema operativo, como a parte do sistema que implementa o próprio protocolo IP. Nestes casos o software pode, para total desempenho, ser compilado directamente no núcleo do sistema operativo, tendo assim acesso directo a todas as estruturas deste sem quaisquer restrições e não tendo nunca que invocar as chamadas de sistema Unix (que implicam sempre uma dispendiosa mudança de contexto no processo). Nestes casos, os "deamon" executam-se em "kernel-space", ao contrário dos normais que se executam em "user-space".

A grande desvantagem relativa aos deamons que são compilados juntamente com o núcleo do sistema é que o processo de desenvolvimento do software é substancialmente mais lento e complicado, uma vez que cada nova versão do software implica uma reinicialização completa do sistema. Outra desvantagem do software integrado no núcleo é que as ferramentas típicas de depuração não podem ser utilizadas; em caso de falhas, torna-se extremamente difícil encontrar as causas dos problemas.

4.2.3 - STACK TCP/IP

O núcleo do Linux é composto por várias partes, detendo este o suporte nativo a várias famílias de protocolos, em particular para o stack TCP/IP (que é o mais utilizado e difundido), detendo de implementações de ambas as versões 4 e 6 desta família de protocolos [17][18].

Relativamente à versão 4 (a versão actual do protocolo IP na Internet, e utilizado neste Trabalho), o stack TCP/IP presente no Linux é muito completo uma vez que todos os protocolos (mais relevantes) de todas as camadas da família IP estão convenientemente codificados e modularizados, tendo sido depurados por anos e anos de utilização contínua. No entanto, o protocolo MIP (ainda) não está presente neste stack, o que é a razão do interesse desta implementação do MIP em Linux. Uma característica importante que mostra o campo de acção deste stack é que qualquer sistema Linux pode assumir as funções de cliente, servidor e encaminhador IP, uma vez que todos estes protocolos estão implementados neste stack TCP/IP.

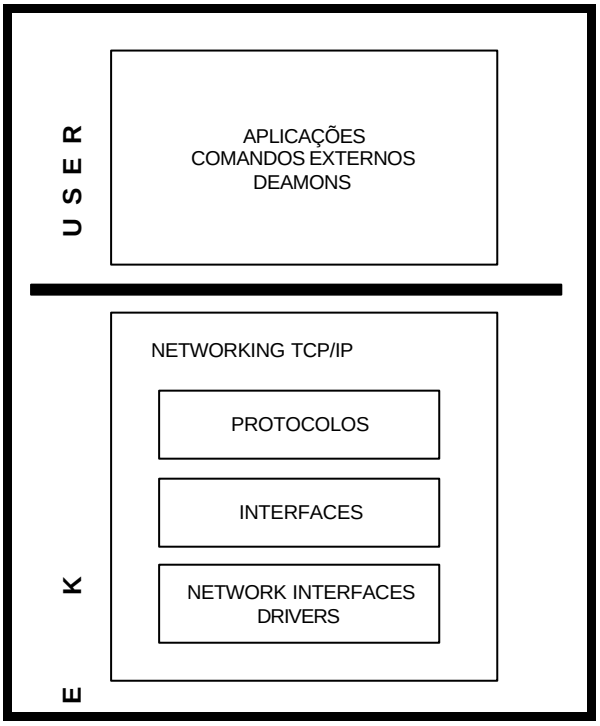


Figura 23 - Stack TCP/IP do Linux

Uma característica importante do stack TCP/IP é que este foi desenhado explicitamente para ser completamente flexível, sendo relativamente fácil de manipular os seus constituintes (tabelas de encaminhamento, "drivers", protocolos activos), de os alterar ou substituir por outras implementações sem ter que modificar todo o restante sistema estando este em funcionamento.

O Stack TCP/IP do Linux está organizado da forma presente na **figura 23**. O stack TCP/IP está completamente contido no núcleo do Linux, e dá o suporte às aplicações "user-space" que se executam sobre este.

O modulo de "networking TCP/IP" é dividido nas camadas de protocolos (onde estão os protocolos da família IP), na camada das interfaces (onde se definem entidades que podem enviar e receber pacotes IP) e por fim no conjunto dos drivers associados a cada interface física de acesso ao meio físico (EtherNet, RDIS, ATM, …).

4.2.3.1 - Interfaces

O stack de protocolos do Linux está organizado por **interfaces** [16][23]. Uma interface pode corresponder a uma instanciação física de uma peça de hardware existente no computador, ou ser apenas uma entidade lógica. Exemplos de interfaces físicas são os adaptadores de rede Ethernet ou Wireless, enquanto que uma entidade lógica pode ser criada apenas para realizar um protocolo específico. Todas as interfaces podem ser manipuladas extensivamente e é através das interfaces presentes num sistema Linux que os protocolos da família IP vão receber e enviar pacotes IP de/para a rede.

No respeitante às interfaces físicas, estas correspondem a adaptadores de rede, que executam o nível 2 da pilha de protocolos (tipicamente em hardware). Cada interface deste tipo vai ligar o nó a uma dada subrede IP, ficando a assim interface com um endereço IP único dessa subrede.

Neste sentido cada nó terminal da Internet (os nós que não sejam encaminhadores, isto é, que apenas enviem e recebam os **seus** pacotes) vai tipicamente possuir apenas **uma** única interface

referente ao seu adaptador Ethernet ou a um modem ligado à rede pública de voz. É apenas por esta interface que o stack TCP/IP vai comunicar com todo o mundo exterior.

Este conceito é facilmente estendido para o caso em que se pretende formar um encaminhador IP que ligue duas redes IP. Uma vez que o stack TCP/IP do Linux permite encaminhar os pacotes IP entre qualquer par de interfaces, um "router" é criado quando um sistema Linux tem duas interfaces físicas diferentes, uma para cada rede, e tem a sua tabela de encaminhamento (ver **secção 4.2.3.2**) correctamente configurada. Por outro lado o sistema Linux também permite facilmente que estes encaminhadores sejam ainda mais poderosos, pois o stack inclui outros protocolos mais avançados da família IP, específicos para o encaminhamento e aprendizagem dinâmica de caminhos (denominados de "rotas") da Internet.

Como exemplo destas capacidades mais avançadas do Linux pode-se considerar uma rede local Ethernet pertencente a uma organização em que todas as máquinas são nós simples da Internet, tendo apenas uma interface Ethernet que as liga à rede local; estas máquinas vão aceder ao exterior por um nó encaminhador designado que possui duas interfaces: a interface Ethernet para a rede local, e uma outra que efectua a ligação da rede local à rede pública. Este nó vai desempenhar o papel de "gateway" para as outras máquinas, pois todo o tráfego da rede local para o exterior é encaminhado por este nó. Este exemplo é uma das formas mais baratas e eficazes de estabelecer uma rede local completa, com acesso total ao exterior. O Linux também oferece, de base, aplicações completas que interagem com o stack TCP/IP para implementar nos encaminhadores outras funcionalidades avançadas como políticas de segurança, contabilidade e controlo de fluxo do tráfego existente.

Existem também as interfaces lógicas, que são apenas módulos de software que se executam no núcleo do Linux que implementam outros protocolos ou que são usados por aplicações especiais (que têm assim um acesso privilegiado ao núcleo do Linux). A grande vantagem desta organização do stack TCP/IP do Linux por interfaces é que todas as interfaces podem receber e enviar pacotes por elas, sendo o seu acesso e controlo sempre igual para qualquer tipo de interface. Um exemplo típico de uma interface lógica é a interface de teste "loopback".

Esta interface só existe na memória do computador, mas tem todas as características de uma interface física. Neste sentido esta interface tem um endereço IP, um endereço de subrede + máscara, e tem a característica especial que todos os pacotes enviados são retornados de volta (pela mesma interface). Isto significa que, para testar a parte **local** do stack TCP/IP de um sistema Linux apenas é necessário associar um endereço IP à interface "lo" e enviar pacotes para esse endereço (com o comando "ping"), sendo os pacotes enviados supostos de serem retornados iguais de volta.

A manipulação das interfaces pode ser feita pela utilização dos já referidos comandos internos, ou então pela utilização do comando externo "**ifconfig**", pelo qual se pode configurar e manipular as interfaces existentes neste sistema (físicas e lógicas); Com este comando é possível criar novas interfaces, associar-lhes endereços IP, associar-lhes um driver que a instancie e por fim remover as interfaces.

4.2.3.2 - Encaminhamento

O sistema de encaminhamento do Linux também segue o modelo de simplicidade das interfaces. Existe uma tabela de encaminhamento [22], com um número de entradas arbitrário, que relaciona destinos (endereços IP) com interfaces do sistema: os pacotes IP são encaminhados pela interface indicada na entrada respectiva nesta tabela. Uma vez que os destinos são explicitados na forma (endereço da subrede, máscara), a mesma tabela de encaminhamento é utilizada para endereços simples de nós isolados, para subredes IP inteiras e para um encaminhador por omissão ao qual são entregues todos os pacotes que não têm uma entrada específica nesta tabela.

Quando o protocolo IP recebe, por uma qualquer interface, um pacote IP, o endereço de destino vai ser comparado com esta tabela de encaminhamento; a entrada que melhor se adaptar (a que tiver a máscara mais comprida) vai ser escolhida, e o pacote será enviado pela interface correspondente. Para os nós simples da Internet que não têm todos os protocolos mais avançados de

encaminhamento, esta tabela também vai ser utilizada, mas agora só para indicar qual a "gateway" existente na rede local. Neste caso todo o tráfego emitido pelo nó será entregue a este encaminhador designado, sendo este quem terá que encaminhar os pacotes IP pela Internet.

Neste trabalho é muito frequente a interacção e manipulação com esta parte do stack TCP/IP. No entanto a tabela de encaminhamento é uma área extremamente sensível do sistema, o que significa que até o MIP estar desenvolvido sem qualquer erro de programação, as alterações mal executadas no sistema implicavam (normalmente) a perda irreversível de conectividade do sistema Linux.

Este módulo de encaminhamento tem o seu acesso facultado com o comando externo "**route**". Com este comando é possível inserir quaisquer novas linhas na tabela de encaminhamento, bem como remover linhas já existentes. No caso concreto do controlo MIP, é pela modificação desta tabela que os dados MIP são encaminhados da forma especial necessária à Macro-Mobilidade.

4.2.3.3 - ARP

Outra tabela importante é a tabela **ARP** [21][11] que estabelece as relações entre os **endereços IP** (nível 3) com os **endereços MAC** (nível 2). Todos os nós utilizam esta tabela como uma "cache" para guardarem as associações dos dois espaços de endereçamento, indispensáveis para a entrega de pacotes IP utilizando o nível 2.

Relativamente a esta tabela, as suas entradas são dinamicamente renovadas pelo protocolo **ARP** que se encarrega de descobrir as relações necessárias quando estas são desconhecidas do nó IP. No entanto o protocolo MIP tem a necessidade de inserir novas entradas, permanentes, na tabela de arp para o Home Agent poder publicitar a sua associação do **seu endereço MAC ao endereço IP do Terminal Móvel**, de forma a que este receba todo o tráfego destinado ao Terminal Móvel (uma vez que os outros nós vão pensar que o Home Agent **é** o Terminal Móvel).

Uma vez que esta operação é uma utilização especial do protocolo ARP, este efeito é só alcançado interagindo com o modulo ARP para forçar este caso especial, utilizando o comando externo "**arp**" .

4.2.3.4 - IPIP

Por fim existe um módulo genérico no stack TCP/IP do Linux bastante útil para a implementação do MIP, que é uma implementação de um túnel IPIP [19][20]. Este módulo inclui um encapsulador e o correspondente desencapsulador, e permite criar e manipular túneis IP dentro-de-IP.

As interfaces criadas com o módulo IPIP são configuradas com o endereço de origem e de destino do túnel, que são os endereços dos novos pacotes que vão encapsular os pacotes de dados MIP. Na recepção o mesmo módulo é configurado com os pares (origem, destino) dos pacotes aceites para desencapsulamento, e todos os pacotes que cumpram este requisito serão desencapsulados sendo o pacote original exposto no sistema, de tal forma que seja posteriormente processado por este.

Este módulo IPIP é uma das adições mais recentes ao sistema Linux, e para a sua manipulação (criar/remover túneis IPIP) é utilizado um comando recente denominado de "**ip**". Este programa já standard em linux (mas ainda inexistente noutros sistemas Unix) é utilizado pelos deamons MIP para manipular os túneis IPIP necessários para a encapsulação dos pacotes a redireccionar para cada localização sucessiva dos terminais móveis.

4.3 Deamon Host-MIP

O programa "host_mip" é o "deamon" que instancia o protocolo MIP nos clientes, que são os terminais móveis.

Este programa tem a sua configuração separada em parâmetros que lhe são fornecidos na activação e num ficheiro de configuração que deverá estar localizado em "/etc/mip-mh".

O programa tem os seguintes parâmetros de utilização:

> host_mip -a HOME_IP -m HOME_MASK -g HOMEAGENT_IP -d TEMPO

Nestes parâmetros o programa vai obter um conjunto de dados básicos para a sua execução, nomeadamente o endereço IP deste Terminal Móvel e o endereço IP do seu Home Agent. Existe uma última opção ("-d") que indica quanto tempo o cliente MIP vai esperar até activar automaticamente o protocolo DHCP (opção descrita posteriormente).

Quando o programa se inicia, o ficheiro de configuração é lido para obter a restante configuração. Este ficheiro terá que existir para a activação do "deamon", e contem o tipo de autenticação e o valor da chave secreta partilhada entre este Terminal Móvel e o Home Agent indicado na opção "-g", da seguinte forma:

<SPI> <tipo autenticação> <tamanho da chave> <chave...>

O único tipo de autenticação implementado é o **md5**. Este tipo de autenticação suporta chaves de qualquer de comprimento, até 64 bytes, sendo este indicado pelo campo respectivo. Como actualmente ainda não existe nenhum sistema na Internet de **difusão** segura de pares de chaves destinadas à autenticação, é necessário acordar manualmente uma chave secreta entre o Terminal Móvel e o Home Agent antes do próprio serviço MIP ser necessário. Esta forma de autenticação também vai significar que cada Terminal Móvel tem apenas um Home Agent que lhe fornece a Macro-Mobilidade. Esta limitação na implementação do MIP existe por dificuldades em difundir seguramente pares de chaves **md5**, pois desta forma cada chave é sempre partilhada **apenas** por **duas únicas** entidades – O Terminal Móvel e o seu Home Agent.

Este "deamon" vai interagir directamente com o sistema operativo, pelo que necessita de ser executado no modo privilegiado do sistema. Em Unix, apenas um administrador do sistema que tenha as permissões de "root" vai conseguir executar convenientemente o programa. Neste sentido é muito importante garantir que o ficheiro de configuração do cliente MIP está acessível para leitura, ao administrador da máquina, uma vez que no interior deste ficheiro está o valor da chave secreta, partilhada entre o cliente e o servidor MIP. Tal como foi descrito na **secção 3.4**, toda a segurança do protocolo MIP, baseada em autenticação, considera que a chave secreta partilhada permanece sempre **secreta**, acessível apenas aos dois intervenientes do protocolo MIP.

Quando se inicia o programa, a sua configuração vai ser verificada, para garantir que é uma configuração válida. Se esta condição não for atingida, então o programa irá abortar a sua execução. Caso contrário, o programa irá começar a suportar o protocolo MIP considerando que os servidores MIP também estão configurados e activos.

Quando o programa é activado na linha de comandos, ou num script de inicialização, este pode executar-se imediatamente em "background"; no caso contrário o programa vai-se executar em "foreground" e aceitará comandos muito simples do teclado para depuração interactiva, continuando porém a executar o protocolo MIP em paralelo. Estes comandos simples destinam-se à leitura de informações internas, para efeitos de depuração: visualizar as estatísticas internas, visualizar as variáveis internas mais importantes, controlar a quantidade de mensagens de depuração geradas pelo programa, controlar o ciclo de espera do programa e abortar o programa. Este último comando é útil para simular situações de falha do sistema, na qual o deamon é obrigado a terminar a sua execução, ficando assim o sistema sem o suporte da Macro-Mobilidade uma vez que o protocolo MIP deixa de ser suportado.

O programa tem também outras formas de depuração que foram desenhadas para tornar mais fácil este processo. Para isto, o programa envia continuamente todos os seus "traces" e informações de depuração para o ficheiro de registo "**mh_exec_log**", sendo este permanentemente actualizado. Em caso de falha remota, a sequência de execução do programa e outras informações importantes vão estar convenientemente registadas, em disco, neste ficheiro.

Internamente, o programa cliente MIP vai processar as mensagens de controlo MIP, tendo sido desenhado de forma a não ser uma carga para o sistema operativo. Assim o programa está tipicamente inactivo bloqueado nas filas de espera do Processo de Escalonamento do núcleo, sendo periodicamente acordado para efectuar o processamento necessário às mensagens MIP que eventualmente tenham aparecido destinadas ao Terminal Móvel; é esta forma de execução do deamon que torna a sua execução relativamente "leve" para o resto sistema. Este período entre activações tem o valor de um segundo (sendo porém configurável para outros valores) e define a relação **tempo de resposta / peso relativo** do programa no sistema operativo.

O valor escolhido significa que, apenas de segundo a segundo, é que o programa vai processar as mensagens MIP entretanto recebidas, pelo que se várias mensagens forem recebidas até à próxima activação do programa estas vão ser retidas e processadas todas de uma vez; por outro lado esta forma de programar também implica que o Terminal Móvel demora sempre uma média de meio segundo até processar uma mensagem MIP que tenha sido recebida de uma qualquer outra entidade MIP, o que é um valor aceitável.

Uma excepção a este comportamento é o processamento dos comandos interactivos do utilizador: neste caso o programa (que está deste modo a correr obrigatoriamente em "foreground") activa-se imediatamente de forma a responder ao utilizador sem demoras.

Para implementar o cliente do protocolo MIP, o programa vai espelhar as mesmas três fases já descritas anteriormente, de tal forma que os mecanismos desenvolvidos para cada fase podem ser descritas em sequência:

4.2.1 Fase 1: Localização

Na primeira fase, o programa vai constantemente informar-se da localização física do Terminal Móvel, que vai determinar a necessidade dos mecanismos de Macro-Mobilidade. Para isto o programa vai escutar todos os anúncios de encaminhadores que sejam emitidos (em difusão) e que o Terminal Móvel receba (**Anexo A**); por outro lado, o programa também vai periodicamente também forçar o aparecimento destes anúncios, através de solicitações expressas ICMP (**Anexo A**).

Quando estes anúncios de encaminhadores são recebidos pelo Terminal Móvel, estes vão ser guardados pelo sistema operativo até que o programa se active. Para este efeito o cliente MIP usa dois "sockets": um para a recepção de anúncios MIP e o outro para o envio das solicitações MIP. É no "socket" de recepção de anúncios que o sistema operativo vai guardar todas mensagens ICMP recebidas em difusão, enquanto o "deamon" cliente MIP está inactivo. Por outro lado, o outro socket de envio das solicitações é do tipo "difusão", o que é suficiente para que as mensagens enviadas sejam recebidas por todos os nós que se encontrem no alcance do Terminal Móvel.

Ao contrário dos "sockets" típicos, do tipo **datagrama UDP** ou **"stream" TCP**, estes dois "sockets" vão operar no protocolo **ICMP**. Para isso, os sockets são do tipo "**raw**" limitados ao protocolo **ICMP**. Esta forma de utilização dos "sockets" é suficiente para criar canais de comunicação flexíveis onde o programa tem acesso total ao "payload" IP, referente aos pacotes do protocolo ICMP (esta filtragem é efectuada pelo núcleo do sistema operativo). Utilizando estes canais, o cliente MIP vai ele próprio inserir o cabeçalho ICMP nas mensagens enviadas, tendo assim toda a flexibilidade ao nível do IP.

De acordo com a recepção dos anúncios e o seu tempo de vida, o cliente MIP vai seguir a máquina de estados presente na **figura 24**:

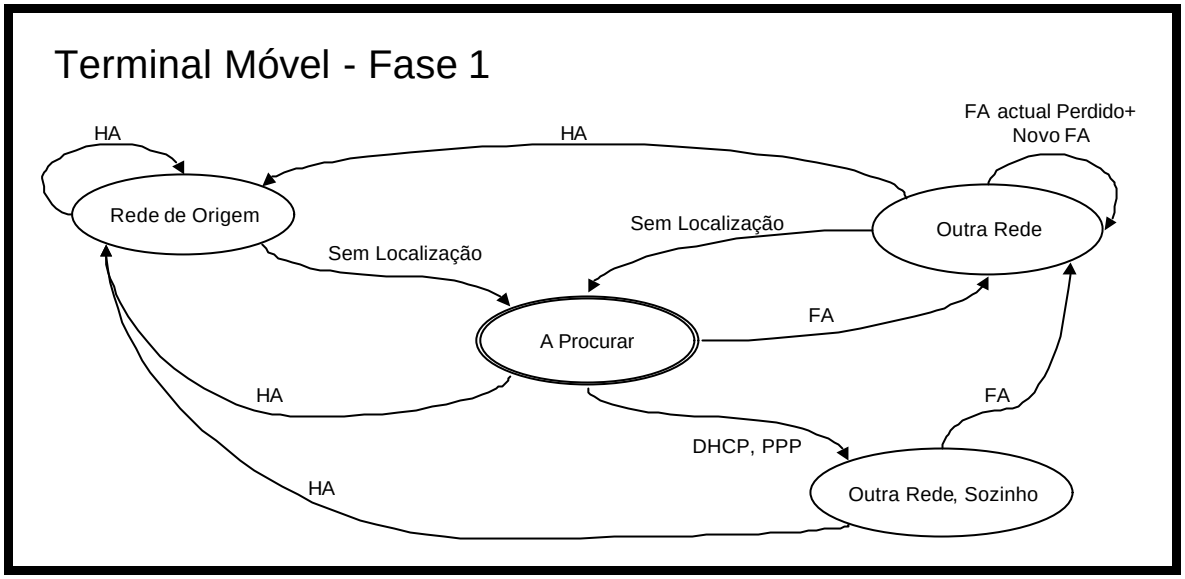


Figura 24 - Máquina de estado do Cliente MIP - Localização

De início, o Terminal Móvel não sabe qual a sua localização física, pelo que o cliente MIP inicia-se no estado **Procurar**. Nesta situação, o programa está constantemente a verificar todos os pacotes IP recebidos em difusão para ver se algum é um anúncio de encaminhadores ICMP, que tenham a extensão MIP, que é essencial para identificar os agentes de mobilidade MIP. O Terminal Móvel também toma a iniciativa de enviar solicitações, para forçar o aparecimento de anúncios de encaminhadores. Este mecanismo é desencadeado para tentar diminuir ao mínimo a permanência do Terminal Móvel neste estado de procura, dado que nesta situação ele está sem conectividade, se não se encontrar na sua rede de origem.

Conforme as mensagens recebidas de anúncios de encaminhadores, o programa irá determinar se o Terminal Móvel está localizado na sua rede de origem ou numa outra rede visitada, transitando assim para o estado correspondente. Dos anúncios recebidos, o programa dá sempre a preferência aos vindos do seu Home Agent, pois estes indicam a localização do Terminal Móvel na sua rede de origem, na qual a Macro-Mobilidade não é necessária.

Todos os anúncios de agentes de mobilidade têm um tempo de vida limitado a poucos segundos. Quando esse tempo passa, sem que tenha sido recebido um novo anúncio do mesmo agente, o programa assume que o Terminal Móvel já não está no alcance desse agente de mobilidade, voltando assim para o seu estado inicial de procura, ao mesmo tempo que força o aparecimento de anúncios com pedidos expressos em difusão. No entanto também pode acontecer que os anúncios tenham sido perdidos na rede por congestão: neste caso, quando o tempo de vida do último anúncio expirar, o cliente MIP vai considerar que o agente já não está disponível. Nesta implementação MIP, o período de aparecimento de anúncios de servidores MIP (sem solicitações expressas) é um terço do tempo de validade de cada anúncio. Desta forma, o cliente teria que perder três anúncios seguidos para considerar, erradamente, que um servidor deixou de estar disponível (estes valores referenciados são definíveis em tempo de compilação).

Outra característica associada à descoberta dos servidores MIP é o noção que estes estão a operar sem falhas. Para isso todos os anúncios são numerados sequencialmente, com início no número zero. Em caso de falha, a contagem começara de novo neste valor, o que é uma forma dos clientes MIP tomarem conhecimento da falha do servidor, por forma a registarem-se de novo nestes. Dado que a contagem é necessariamente finita, quando o contador de anúncios excede o valor máximo (65535) a contagem continua no valor 256 (e não no zero), de forma a não confundir os clientes MIP.

Pode acontecer que o Terminal Móvel esteja no alcance de vários agentes de mobilidade de diferentes redes IP ao mesmo tempo, recebendo assim diferentes anúncios ao mesmo tempo. Esta situação pode indicar que o Terminal Móvel, pelo seu movimento, vai transitar de rede, perdendo em breve o contacto com o agente de mobilidade actual. No entanto o programa vai-se abster de se

registar imediatamente no novo Foreign Agent, na medida em que, apenas considera novos agentes depois do actual deixar de ser ouvido, quando expira o seu tempo de vida sem novos anúncios (na **figura 24** este caso corresponde à transição "FA actual perdido + Novo FA").

O programa também suporta a Macro-Mobilidade mesmo em subredes IP que não disponham de Foreign Agents (conforme descrito na **secção 2.2.2.1**). Para isso, o sistema tem de ter alternativas ao serviço que era prestado pelo Foreign Agent: informação de localização e endereço fixo para comunicar. Neste contexto, podem ser utilizados outros programas (externos) que implementem protocolos que forneçam ao cliente MIP estes serviços.

Dois protocolos que podem fornecer os serviços prestados pelos Foreign Agents são o DHCP [25] (protocolo de configuração automática de hosts) e PPP (estabelecimento de IP sobre ligações ponto-a-ponto, tipicamente sobre linhas telefónicas / linhas série), pois ambos são capazes de configurar o sistema com um novo endereço IP e uma nova tabela de encaminhamento, ambos referentes à localização actual do Terminal Móvel.

Quando um destes programas externos é activado com sucesso, o cliente MIP vai poder utilizar a nova configuração para assim suportar a Macro-Mobilidade nesta localização; esta situação vai corresponder ao estado "**outra rede, sozinho**", na figura 24. Mesmo nesta situação é dada preferência a um eventual Foreign Agent que, posteriormente, esteja no alcance do Terminal Móvel, de forma a preservar os recursos da rede, uma vez que nesta situação o Terminal Móvel aloca dois endereços IP: o fixo e o temporário da rede visitada.

Esta máquina de estados vai estar integrada com uma outra referente à fase de registo (**fase 2**). Assim cada vez que o programa transita para um estado estável (todos menos o "a procurar"), vai ser despoletado um novo processo de registo/cancelamento do registo.

4.3.2 Fase 2: Registo

Nesta fase do MIP o Terminal Móvel vai executar o seu processo de registo, que consiste na emissão de um pedido de registo e na espera pela resposta. Ao contrário das mensagens existentes na fase anterior, o cliente MIP já não necessita de ter o acesso directo ao "payload" IP, uma vez que estas mensagens são baseadas em UDP. Assim o programa vai utilizar um "socket" normal do tipo **datagrama UDP** pelo qual envia e recebe as mensagens presentes nesta fase, sendo este associado a um porto UDP qualquer, no início do programa.

Motivado pela fase de localização, o cliente MIP vai seguir a seguinte máquina de estados relativa à fase de registo (**figura 25**):

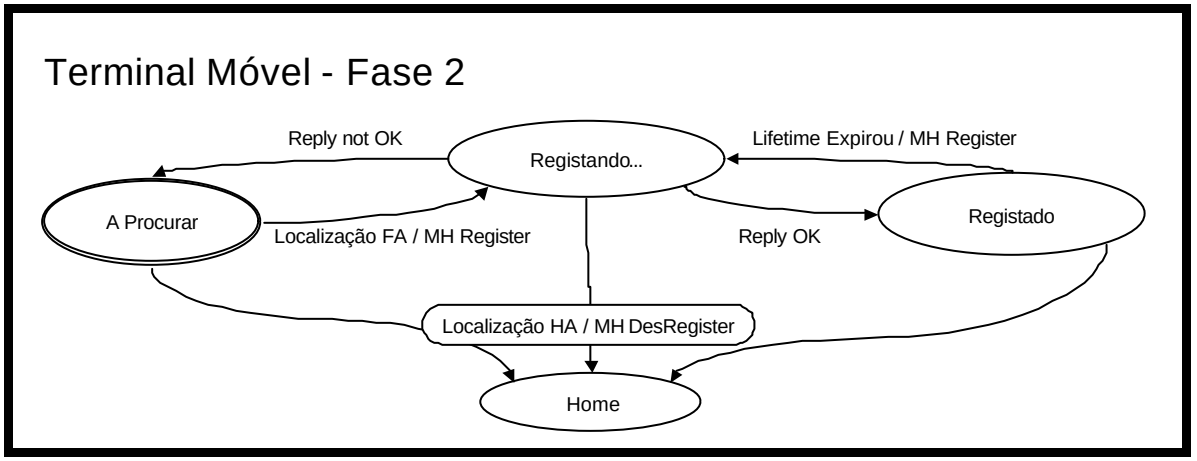


Figura 25 - Máquina de estado do Cliente MIP - Registo

Tal como na fase anterior, o estado inicial é o estado "a procurar". Quando o programa recebe a informação que se encontra numa rede visitada, vai iniciar o processo de registo entregando a sua mensagem de registo ao Foreign Agent escolhido da rede visitada, para este a entregar ao seu Home Agent. Toda a comunicação do Terminal Móvel com o Foreign Agent é

efectuada de uma forma directa sem encaminhamento IP, utilizando os mecanismos de nível 2. Esta solução só é possível porque ambas as entidades estão localizadas fisicamente no interior da **mesma rede IP**.

Depois da entrega do pedido de registo, o programa ficará à espera da resposta, sendo formulado um novo pedido quando detecta que o anterior se perdeu. Se a resposta recebida dos agentes de mobilidade for positiva, então o programa transita para o estado **registado** e activa a próxima fase do MIP, no qual permanecerá até perder o contacto com o Foreign Agent actual. Caso contrário, o pedido de registo não foi aceite, existindo diversos códigos que identificam a causa da negação do serviço.

O serviço pode ser negado tanto pelo Foreign Agent, como pelo Home Agent, por razões diversas: segurança, falha do protocolo MIP, indisponibilidade de recursos/servidores ou por razões administrativas (sendo estas opções de implementação, que o protocolo MIP deixa em aberto).

Das várias razões de recusa do pedido existentes, o programa pode tentar remediar algumas situações que estejam ao seu alcance, utilizando valores apropriados no seu novo registo, obtidos a partir da mensagem de recusa:

- O registo pode ser recusado porque o Terminal Móvel pediu um tempo de alocação dos recursos demasiado grande; neste caso a resposta tem o valor mais elevado permitido, sendo utilizado pelo Terminal Móvel para o novo registo.
- Por outro lado, a recusa pode-se dever a razões de segurança, tipicamente quando a **protecção de repetição de mensagens** do protocolo (**secção 3.4**) bloqueia o pedido; neste caso o Terminal Móvel recomeça um novo pedido, utilizando agora o campo **ID** presente na mensagem de recusa, que contém o próximo valor aleatório esperado pelo servidor;
- O Terminal Móvel pode ter pedido uma opção do protocolo MIP que o servidor não suporta, como a utilização de compressão de Van Jacobson ou de encapsulamento Minimal IP; nesta situação o cliente MIP teria que recomeçar um novo registo sem estas exigências (embora esta implementação particular de MIP em Linux nunca peça estas opções do MIP).
- Em outras situações o cliente MIP vai apenas emitir um novo pedido de registo num tempo posterior, pois isso pode ser o suficiente para o sucesso do registo, como no caso em que o Foreign Agent não tem recursos disponíveis para servir o Terminal Móvel (neste momento).

Além destes casos, existem também outras situações em que a causa da falha está fora do alcance do Terminal Móvel; por exemplo, se o Home Agent estiver indisponível, ou se a chave secreta partilhada entre ambos não coincidir exactamente, o processo de registo nunca será concluído com sucesso.

Tal como na fase anterior, o cliente MIP dá sempre preferência à sua localização na sua rede de origem. Assim sempre que o Terminal Móvel recebe um anúncio do seu Home Agent, o programa vai reagir cancelando o registo, por meio de uma mensagem de registo em que o tempo de vida tem o valor de zero segundos.

Quando o cliente MIP está registado num Foreign Agent, é da sua responsabilidade renovar os seus registos. Para o processo de renovação o cliente vai emitir um novo registo quando faltar metade do tempo acordado; se a mensagem for perdida, então o cliente emite um novo registo quando faltar um quarto do tempo, e assim sucessivamente.

Pode acontecer que o "deamon" cliente MIP esteja inactivo nas filas de espera do núcleo nos momentos em que é necessário enviar as renovações dos registos. Para este efeito, o programa vai utilizar a facilidade do sinal Unix de **alarme**, pela qual o sistema operativo força o programa a se desbloquear na altura programada.

As mensagens trocadas entre as entidades MIP nesta fase de registo vão determinar directamente os procedimentos posteriores da fase de execução, que têm os perigos apresentados na

secção 3.4 relativa à **segurança** do protocolo MIP. Desta forma, todas as entidades MIP (clientes e servidores) têm obrigatoriamente que proteger as mensagens utilizadas nesta fase por **autenticação** por meio de chave secreta partilhada.

Relativamente ao cliente MIP, este programa emite todas as suas mensagens com a extensão MIP de autenticação entre o Terminal Móvel e o seu Home Agent (**anexo B**), e só aceita e processa mensagens vindas de outras entidades que tenham esta extensão MIP com um resumo válido. Para a aprovação de um resumo o cliente MIP vai calcular o resumo da mensagem recebida, utilizando a sua chave secreta partilhada existente no ficheiro de configuração, e este resultado **terá** que ser igual ao presente na mensagem (se isto não se verificar a mensagem será ignorada).

O cálculo do resumo é realizado com o **algoritmo md5 [10].** Para este programa foi usada uma versão de distribuição gratuita que contém código fonte completo em C, incluído numa biblioteca completa de segurança, a **Lybcrypto**.

Quando o Terminal Móvel recebe a mensagem de aceitação do processo de registo, este vai activar a sua parte da fase final do MIP, a fase de execução.

4.3.3 Fase 3: Execução

Nesta fase o cliente MIP vai criar, manter e assegurar os mecanismos necessários para que este envie e receba pacotes IP utilizando o seu endereço fixo estando localizado numa rede visitada que não a sua rede de origem. Para concretizar esta situação o cliente MIP vai configurar o stack TCP/IP do sistema operativo com o recurso aos comandos externos do sistema.

Esta configuração vai possibilitar que os dados MIP sejam processados com sucesso pelo núcleo do sistema operativo, sendo a sua activação e manutenção despoletada pelo controlo MIP. Num ciclo de vida MIP típico, o cliente MIP vai apenas (re)configurar o stack TCP/IP quando é efectuado um registo que não se mantenha igual ao anterior. Desta forma, nos registos de renovação do serviço MIP o sistema mantêm a sua configuração actual; apenas quando o Terminal Móvel muda de Foreign Agent ou regressa à sua rede de origem é que o sistema é reconfigurado para a sua nova localização física.

Esta reconfiguração efectuada e mantida nesta fase é dividida em três casos distintos, relativos à localização do Terminal Móvel. Estes casos vão ser descritos seguidamente, sendo exemplos de comandos externos usados para cada configuração detalhados no **anexo D**.

1 - Rede visitada com Foreign Agent

Neste caso o Terminal Móvel vai comunicar com todo o resto da Internet pelo Foreign Agent escolhido: todos os pacotes IP (dados MIP) são enviados e recebidos por este nó da Internet, sendo a troca dos pacotes efectuada de uma forma directa, por nível 2, sem encaminhamento IP. Para isto o cliente MIP vai configurar o sistema de forma a que só o Foreign Agent esteja acessível, o que obriga a que todo o tráfego lhe seja entregue.

Utilizando o comandos externos de configuração o cliente MIP vai remover todas as entradas existentes na tabela de encaminhamento e na tabela de ARP, o que deixa o sistema num estado de completa inacessibilidade; depois desta operação vão ser criadas as duas únicas entradas na tabela de encaminhamento: uma que indica que o Foreign Agent está acessível directamente ao Terminal Móvel (pela interface que foi usada para estabelecer contacto na fase de localização) e a outra indica que todos os outros destinos têm como encaminhador designado o Foreign Agent.

2 - Rede visitada sem Foreign Agent, usando DHCP ou PPP

Neste caso o cliente MIP não vai contar com a ajuda de um Foreign Agent para poder comunicar com o resto da Internet. No entanto podem ser usados protocolos (como o DHCP ou o PPP) que configurem o Terminal Móvel para a rede actual. Estes protocolos podem ser activados externamente ao cliente MIP em qualquer instante, ou podem iniciados explicitamente pelo cliente MIP. Existe uma opção na activação do cliente MIP ("-d") que indica quanto tempo deve o cliente

esperar (quando não detecta a existência de agentes de mobilidade) até despoletar ele próprio o protocolo DHCP, para tentar assim configurar-se com um endereço IP temporário.

Na situação em que um destes protocolos foi activado com sucesso, estes protocolos vão configurar o sistema para com um novo endereço IP (da rede actual) e uma nova tabela de encaminhamento que seja referente à rede actual, com um novo encaminhador designado (o encaminhador por omissão). Quando isto acontece o cliente MIP vai-se aperceber da mudança ocorrida porque o endereço IP "default" do Terminal Móvel já não é o endereço IP fixo original.

Nesta situação o cliente MIP vai ler a informação de qual o novo endereço IP que o protocolo configurou o Terminal Móvel, para o utilizar como endereço temporário nesta rede visitada. Depois de saber este endereço, o cliente MIP vai configurar o sistema de novo com o endereço IP fixo do Terminal Móvel.

Agora o cliente vai configurar o sistema para que este possa aceitar livremente pacotes destinados ao endereço IP temporário do Terminal Móvel (o endereço que o DHCP tinha configurado o sistema); para isso é criada uma nova interface lógica "dummy" à qual é atribuída o endereço IP temporário. Por fim, basta que o Terminal Móvel possa desencapsular os pacotes que lhe vão ser enviados pelo Home Agent para o endereço temporário. Para isso, o módulo de desencapsulamento IPIP é configurado para aceitar todos os pacotes que respeitem o par origem/destino (Home Agent, endereço IP temporário).

Neste esquema o Home Agent envia pacotes IP destinados ao endereço fixo do Terminal Móvel dentro de pacotes IP destinados ao endereço temporário do Terminal Móvel (ver **anexo C**), que serão aceites pela interface lógica criada, dado que lhe são destinados; estes pacotes serão desencapsulados pelo módulo IPIP, uma vez que respeitam o par (origem/destino). Os pacotes originais expostos são aceites pela interface física do Terminal Móvel, porque lhe são destinados. Esta sequência de operações está explicita na **figura 26**:

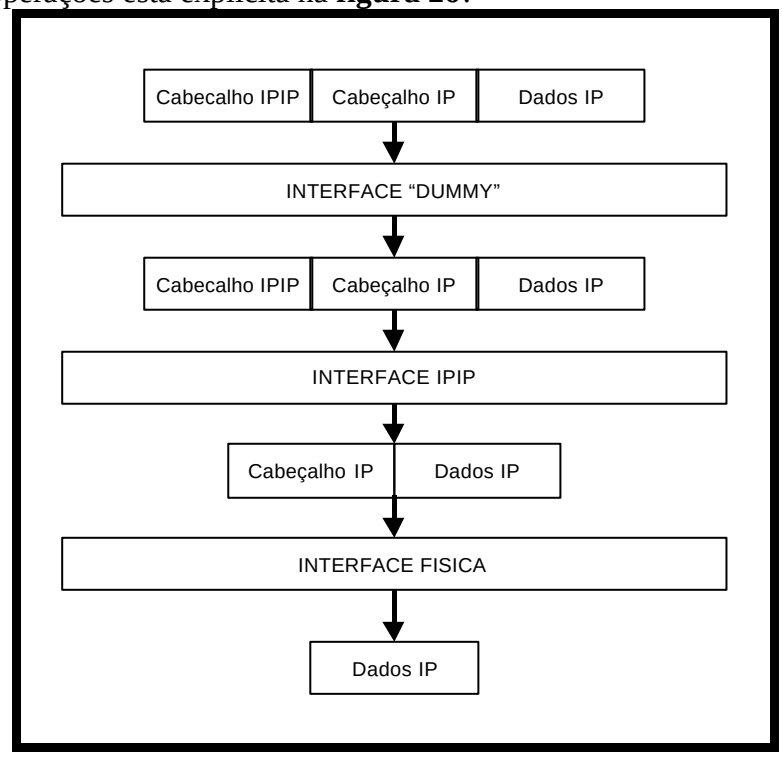


Figura 26 - Aceitação dos pacotes encapsulados pelo Terminal Móvel com DHCP

Por outro lado, os pacotes enviados pelo Terminal Móvel têm sempre como origem o endereço IP fixo deste, uma vez que este é sempre o endereço IP "default" (o endereço temporário apenas está atribuído à interface lógica criada para a recepção de pacotes). Estes pacotes enviados serão correctamente entregues ao destino pelo encaminhador designado que o DHCP ou PPP escolheram.

3 - Na Rede de Origem

Quando o cliente MIP detecta que o Terminal Móvel voltou para a sua rede de origem, este vai configurar o sistema para usar a conectividade normal de qualquer nó da Internet; em particular volta a ser possível, ao Terminal Móvel, comunicar directamente com qualquer outro nó que esteja presente na mesma rede IP.

Para isto o cliente MIP vai cancelar a utilização dos recursos que foram usados nos casos acima descritos, ao mesmo tempo que reconstrói a sua tabela de encaminhamento com os valores normais para utilização na sua rede de origem.

4.4 Deamon Agent-MIP

O programa "agent_mip" é o "deamon" que instancia o protocolo MIP nos servidores, que são os nós que possibilitam a Macro-Mobilidade aos terminais móveis ao longo de toda a Internet. Para um dado Terminal Móvel, estes servidores dividem-se em Home Agents e Foreign Agents; os primeiros estão permanentemente localizados na sua rede de origem, e os outros estão presentes nas diversas redes visitadas. O programa desenvolvido implementa um servidor **MIP completo nas duas vertentes de Home e Foreign Agent** em simultâneo, em que cada papel é utilizado caso-a-caso consoante o Terminal Móvel: o programa age como um Home Agent para o terminais móveis pertencentes à sua rede, e como um Foreign Agent para todos os outros terminais móveis pertencentes a outras redes IP.

Cada servidor MIP **suporta apenas uma única subrede IP**; no entanto é possível que um encaminhador com acesso a várias subredes IP (várias interfaces) possa executar simultaneamente várias instâncias do servidor, cada uma configurada convenientemente para cada subrede; por outro lado também é possível que uma subrede IP tenha vários agentes de mobilidade, cabendo aos terminais móveis a escolha dos agentes com quem vão interagir.

Este programa tem a sua configuração separada em parâmetros que lhe são fornecidos na activação, e em dois ficheiros de configuração para cada vertente do servidor, que terão que estar localizados em "/etc/mip-ha" e "/etc/mip-fa".

O programa tem os seguintes parâmetros de utilização:

> agent_mip -a HOME_IP -m HOME_MASK -h MAC_ADDR -i INTERFACE

Assim o programa vai esperar nos seus parâmetros todas as informação essenciais respeitantes à subrede IP sobre a qual este agente vai operar. Para isso é indicada a interface física de acesso à subrede, o endereço IP dessa interface, a máscara da subrede e o endereço MAC da interface (opções "-i", "-a", "-m", "-h" respectivamente).

Quando o programa se inicia, ambos os ficheiros de configuração são lidos e processados para configurar cada vertente do servidor MIP. Assim o ficheiro "/etc/mip-ha" contém as identidades dos terminais móveis pertencentes a esta rede que este Home Agent conhece, enquanto que o ficheiro "/etc/mip-fa" determina que terminais móveis de outras redes são autorizados a interagir com este Foreign Agent.

A informação relativa aos terminais móveis deste Home Agent é indicada da seguinte forma:

<Número de Terminais Moveis>
<Endereço IP Fixo> <SPI> <tipo autenticação> <tamanho da chave> <chave...>
<Endereço IP Fixo> <SPI> <tipo autenticação> <tamanho da chave> <chave...>
...

Desta forma a configuração de um Home Agent é semelhante à de cada Terminal Móvel, no sentido em que o ficheiro de configuração serve para guardar a chave secreta md5 partilhada entre o Home Agent e cada Terminal Móvel. Esta forma de configuração implica que cada par (Home Agent, Terminal Móvel) tem que possuir a sua própria chave secreta partilhada, tendo esta de ser acordada necessariamente **antes** da execução do MIP. Por outro lado, de um ponto de vista administrativo, cada novo Terminal Móvel de uma rede terá sempre que pré-acordar com o(s) Home Agent(s) existentes na sua rede de origem a disponibilidade do serviço antes do próprio serviço ocorrer, dado que os Home Agents apenas servem terminais móveis conhecidos.

O Foreign Agent tem uma configuração administrativa semelhante: no seu ficheiro de configuração estão presentes os pares (Terminal Móvel, Home Agent) conhecidos, da seguinte forma:

<Número de Terminais Moveis Visitantes>
<Endereço IP Fixo> <Endereço IP do Home Agent>
<Endereço IP Fixo> <Endereço IP do Home Agent>
...

Novamente de um ponto de vista administrativo, este servidor MIP só vai aceitar terminais móveis visitantes que conheça. No entanto, é importante notar que esta restrição poderia ser facilmente levantada (embora por simplicidade esta implementação não o faça) uma vez que os Foreign Agents não têm uma chave secreta partilhada com os terminais móveis (embora o protocolo MIP o suporte).

Tal como o "deamon" cliente MIP, este programa também vai interagir directamente com o sistema operativo, pelo que necessita também de ser executado no modo privilegiado do sistema (com permissões de "root"), devendo também os ficheiros de configuração ser apenas acessíveis para leitura ao administrador da máquina.

Depois do programa ser iniciado este irá suportar os terminais móveis registados que estejam localizados noutras redes, ao mesmo tempo que fornece o serviço aos terminais móveis conhecidos pertencentes de outras redes que estejam nesta subrede IP.

Tal como o cliente MIP, este programa pode executar-se como um "deamon" em background, sem qualquer intervenção do utilizador, ou em "foreground" no qual oferece a mesma interface simples de "debug". Tal como o cliente MIP, este programa cria um "trace" completo de mensagens internas para o ficheiro "**agent_exec_log**", o qual é permanentemente actualizado e útil em caso de falha do servidor.

Por si só o "deamon" servidor nunca termina a sua execução voluntariamente, podendo sofrer uma falha que o impossibilite de continuar a sua execução, o que pode acontecer quando o programa recebe sinais do sistema operativo relacionados com acessos ilegais à memoria ou outras situações.

No caso de ser o Foreign Agent a falhar, os terminais móveis adjacentes a este vão poder detectar esta situação pela falta de anúncios desta entidade (ver **secção 4.3.1**), podendo de imediato escolher um novo Terminal Móvel que os sirva.

No entanto a falha de serviço do Home Agent é bastante mais grave para o serviço MIP, uma vez que os clientes MIP estão sempre associados a um único Home Agent (com o qual acordaram a chave secreta partilhada), pelo que a falha deste compromete a Macro-Mobilidade. Por outro lado, os terminais móveis que estejam localizados fisicamente noutras redes **não vão poder saber directamente** se o Home Agent falhou, porque nesta situação estes só recebem anúncios de localização dos Foreign Agents.

Assim, o servidor MIP quando é reactivado vai tentar imediatamente restabelecer o seu serviço. Para isso o servidor vai guardar, entre activações, informação de estado no ficheiro "/etc/mip-agent.log" referente a que terminais móveis este estava a suportar no momento da falha do sistema, sendo essa altura gravada no interior do ficheiro.

Quando o servidor se inicia, este vai sempre processar o seu ficheiro de histórico e calcular quanto tempo passou desde a falha até ao instante presente, sendo este intervalo de tempo usado para actualizar (e se necessário, remover) os tempos de vida dos terminais móveis que estava a suportar. Para os terminais que ainda tiverem o seu registo activo, o Home Agent volta a fornecer o seu serviço automaticamente, sem ser necessário o processo de registo novamente.

Tal como o cliente MIP, o servidor vai apenas processar as mensagens de controlo MIP da mesma forma periódica (de segundo a segundo), para não comprometer o desempenho do sistema. Através das mensagens de controlo MIP, o servidor vai configurar o stack TCP/IP, com o recurso aos comandos externos do sistema, para que o núcleo processe convenientemente as mensagens de dados MIP, de uma forma automática.

Para implementar o servidor MIP, o programa vai também espelhar as três fases do protocolo MIP, de tal forma que os mecanismos desenvolvidos para cada fase podem ser descritas em sequencia:

4.3.1 Fase 1: Localização

Na primeira fase, de localização, o servidor MIP vai ter a responsabilidade de fornecer aos terminais móveis a informação da sua existência na subrede IP onde está localizado (cada servidor MIP opera sempre numa única subrede IP) por meio de anúncios de agente de mobilidade. Para isso o servidor vai emitir periodicamente, em difusão, para a sua subrede IP mensagens ICMP de localização de encaminhadores acrescidas da extensão MIP de existência de agentes de mobilidade (**Anexo A**). No entanto os terminais móveis podem solicitar expressamente estes anúncios, novamente em difusão; quando o servidor MIP recebe e processa uma solicitação de um Terminal Móvel que esteja no seu alcance, este vai imediatamente emitir um anúncio para o informar da sua localização.

Para estas operações são também usados no servidor MIP dois sockets do tipo "**RAW**" limitados ao protocolo **ICMP**, que dão ao programa o acesso directo ao "payload" dos pacotes IP. No entanto estes dois "sockets" têm outra característica especial: ambos estão **limitados à subrede** onde o servidor MIP está a operar. Se esta restrição não fosse seguida, o sistema operativo iria entregar ao servidor as mensagens ICMP recebidas desta subrede IP e de todas as outras a que este encaminhador estivesse ligado por outras interfaces físicas, o que iria confundir o servidor acerca da localização física dos terminais móveis.

Todos os anúncios emitidos pelo servidor MIP têm um tempo de vida limitado a poucos segundos, sendo emitidos pelo servidor 3 novos anúncios durante este tempo de vida. Desta forma os clientes MIP podem localizar-se convenientemente, pois se saírem do alcance deste agente de mobilidade vão deixar de receber os anúncios de localização deste agente.

É através dos anúncios de localização que os servidores vão informar os terminais móveis que acabaram de se reinicializar. No caso dos Home Agents estes vão retomar o serviço pela utilização do histórico já descrito, enquanto que os Foreign Agents não têm de o fazer. Assim, quando um Terminal Móvel detecta que o seu Foreign Agent voltou a estar disponível, este volta a registar-se, se entretanto não tiver mudado para um outro agente. Para isto os anúncios são numerados, sendo os primeiros 256 valores reservados para uma inicialização do agente de mobilidade.

Do ponto de vista de um Home Agent o serviço prestado é exactamente igual quando suporta um Terminal Móvel que está a utilizar um Foreign Agent, ou quando este está a usar um endereço temporário da rede visitada: em ambos os casos o Home Agent envia os pacotes destinados ao Terminal Móvel encapsulados para o endereço que este lhe deu no seu processo de registo (**secção 4.2.2**) - o endereço do Foreign Agent ou o endereço temporário da rede visitada.

4.3.2 Fase 2: Registo

Nesta fase do protocolo os servidores MIP vão esperar as mensagens de registo dos terminais móveis e aceitá-las ou negá-las. Tal como nos clientes, os servidores MIP vão utilizar para esta fase "sockets" normais do tipo **datagrama UDP**, uma vez que apenas é necessário o acesso pelo programa ao "payload" UDP (**anexo B**). Estes "sockets" do servidor já não são associados a um qualquer porto UDP, o que significa que os clientes nunca os iriam encontrar. Para isso, o servidor recebe os seus pedidos no endereço IP na sua subrede no porto UDP standard 434.

Os Servidores MIP vão executar máquinas de estados para implementar o processo de registo. No entanto, uma vez que cada Home e Foreign Agent suporta simultaneamente vários terminais móveis, o servidor MIP vai executar várias máquinas de estado ao mesmo tempo, uma por cada Terminal Móvel.

Assim cada Foreign Agent considera que os terminais móveis podem estar não registados,

em processo de registo e registados. A máquina de estados executada pelo Foreign Agent relativa a cada Terminal Móvel está presente na **figura 27**:

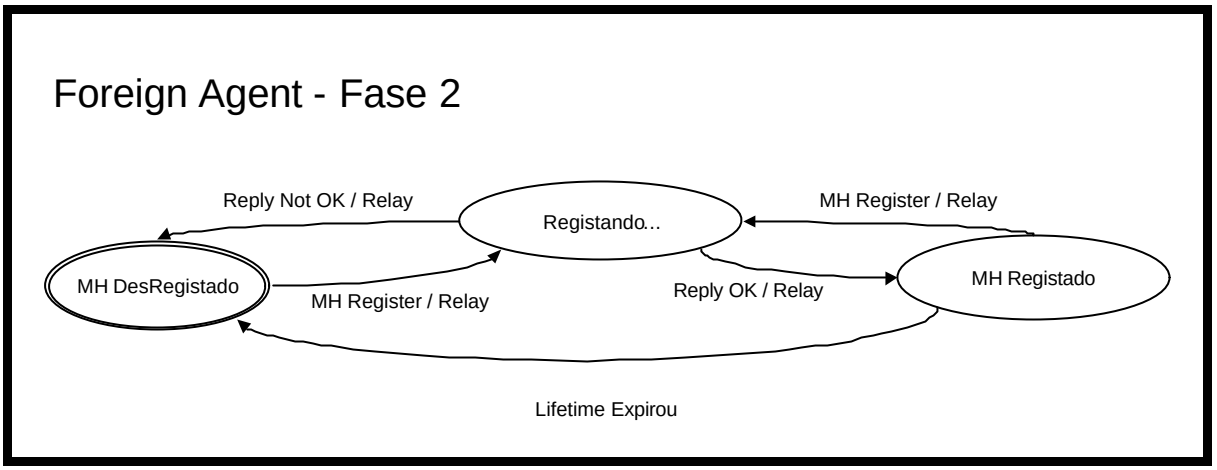


Figura 27 - Máquina de Estados do Foreign Agent - Registo de um Terminal Móvel

Para cada Foreign Agent, cada Terminal Móvel que conhece está inicialmente não registado, até que este o contacta com um pedido de registo. O Foreign Agent pode recusar o pedido de registo quando: este não está correctamente formulado, o Terminal Móvel pede uma opção do protocolo não implementado neste servidor MIP, ou o Terminal Móvel é desconhecido.

Se o pedido de registo estiver correcto, então o Foreign Agent envia-o para o Home Agent indicado, ficando depois à espera da resposta. Quando esta chega o Foreign Agent verifica-a e passa a suportar (ou não) o Terminal Móvel, activando a fase de execução MIP; por fim a resposta do Home Agent é entregue ao Terminal Móvel (da forma directa já referida).

É sempre da responsabilidade do Terminal Móvel a renovação do serviço acordado, pelo que este terá que periodicamente emitir novos pedidos de registo. No caso de um Terminal Móvel sair do alcance de um Foreign Agent o seu serviço vai expirar naturalmente quando o tempo de vida acordado passar sem a respectiva renovação.

De uma forma semelhante cada Home Agent vai seguir uma máquina de estado por cada Terminal Móvel, existindo apenas dois estados para cada Terminal Móvel (**figura 28**):

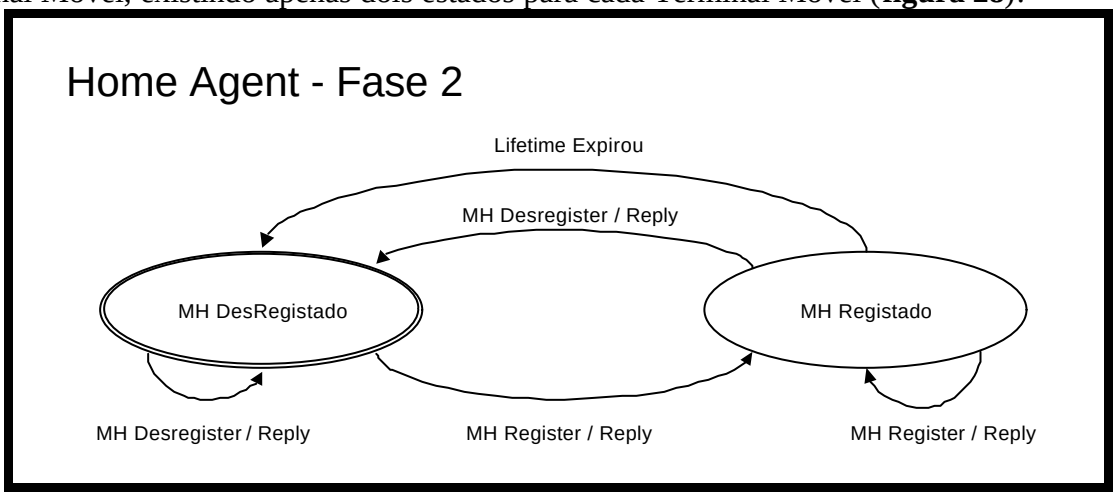


Figura 28 - Máquina de Estados do Home Agent - Registo de um Terminal Móvel

Assim cada Terminal Móvel está sempre registado ou desregistado. Quando o Home Agent recebe uma mensagem de registo de um Terminal Móvel este vai decidir se este Terminal Móvel está em condições de ser suportado. Assim o pedido tem que estar correctamente formulado, tem que ser de um Terminal Móvel pertencente a este Home Agent que não esteja a exigir opções MIP não implementadas neste servidor, e que os mecanismos de segurança do protocolo sejam respeitados: a autenticação desta mensagem não pode falhar (de acordo com a chave secreta

partilhada entre este Home Agent e o Terminal Móvel) e protecção de repetição de mensagens tem que conter o último valor aleatório enviado pelo servidor a este cliente. Da mesma forma que o cliente, o servido MIP vai também verificar se o resumo da mensagem corresponde à chave secreta partilhada utilizando o mesmo algoritmo standard **md5**.

Tal como no caso anterior, é sempre da responsabilidade do Terminal Móvel a renovação do serviço acordado, pelo que este terá que periodicamente emitir novos pedidos de registo. No caso de um Terminal Móvel deixar de renovar o seu registo o seu serviço vai expirar naturalmente quando o tempo de vida acordado passar sem a respectiva renovação.

Também pode acontecer que o Home Agent possa receber directamente um pedido de desregisto, que acontece quando o Terminal Móvel voltou à sua rede de origem e vai desactivar desta forma a Macro-Mobilidade IP.

Ambos os dois tipos agente de mobilidade vão activar e manter os mecanismos de suporte à Macro-Mobilidade IP para cada Terminal Móvel registado, na fase final do protocolo.

4.3.3 Fase 3: Execução

Nesta fase o servidor MIP vai criar, manter e assegurar os mecanismos necessários para que os terminais móveis possam enviar e receber pacotes IP utilizando o seu endereço fixo estando localizado numa rede visitada que não a sua rede de origem. Para concretizar esta situação o servidor MIP vai configurar o stack TCP/IP do sistema operativo com o recurso aos comandos externos já referidos.

Esta configuração vai possibilitar que os dados MIP sejam processados com sucesso pelo núcleo do sistema operativo, sendo a sua activação e manutenção despoletada pelo controlo MIP. Num ciclo de vida MIP típico, o servidor MIP vai apenas (re)configurar o stack TCP/IP quando é efectuado um registo que não se mantenha igual ao anterior. Desta forma, nos registos de renovação do serviço MIP o sistema mantêm a sua configuração actual; apenas quando o Terminal Móvel muda de Foreign Agent ou regressa à sua rede de origem é que o sistema é reconfigurado para a sua nova localização física.

Esta reconfiguração efectuada e mantida nesta fase é diferente tanto para o foreign como para o Home Agent e se o Terminal Móvel está registado ou desregistado. Cada situação vai ser descrita de seguida, sendo os exemplos de comandos externos usados para configurar cada uma destas situações presentes nos **anexos D e E**.

1 - Foreign Agent a suportar um Terminal Móvel visitante

Nesta situação o servidor MIP apenas necessita de configurar a tabela de encaminhamento do stack TCP/IP para que esta tenha uma nova entrada que indica que o Terminal Móvel está acessível **directamente** ao Foreign Agent (pela interface a que servidor está a utilizar), e configurar o módulo IPIP do núcleo para que este aceite todos os pacotes encapsulados vindos do Home Agent.

Nesta configuração, quando o sistema recebe os pacotes encapsulados do Home Agent, o módulo desencapsulador do núcleo vai expor os pacotes originais, sendo estes entregues directamente ao Terminal Móvel pela interface física indicada pela tabela de encaminhamento.

2 - Foreign Agent que deixou de suportar um Terminal Móvel visitante

Neste caso o servidor MIP vai voltar a configurar o sistema da forma normal relativamente a este nó da Internet, removendo a entrada específica na tabela de encaminhamento e configurando o módulo IPIP do núcleo para que este ignore os pacotes encapsulados vindos do Home Agent para este nó.

Esta configuração implica que para comunicar com o Terminal Móvel este sistema irá sempre enviar os seus pacotes para a rede de origem, como faz com qualquer nó fixo.

3 - Home Agent a suportar um Terminal Móvel que está numa outra rede visitada

Este é o caso mais complexo desta fase, porque o servidor vai ter que configurar o sistema de forma a que este receba os pacotes destinados ao Terminal Móvel, encapsulando-os e enviando-os para o endereço fixo utilizado por este (para o Foreign Agent, ou para o endereço temporário da rede visitada).

Para isto, o servidor vai configurar a tabela de ARP do sistema para associar o seu endereço MAC ao endereço IP do Terminal Móvel na interface em que está a operar, sendo esta uma entrada do tipo "pública". Isto significa que o protocolo ARP do Home Agent vai sempre responder a pedidos ARP referentes ao endereço fixo do Terminal Móvel (na sua rede de origem) com o seu próprio endereço MAC. Desta forma todos os pacotes destinados ao Terminal Móvel serão entregues a este Home Agent, sendo este processo denominado de "proxy ARP" [24].

No entanto os outros nós da mesma rede local podem já ter outras relações ARP referentes ao Terminal Móvel, que só quando expirarem é que serão actualizadas. Para isso o Home Agent vai forçar a actualização destas "caches" ARP emitindo uma mensagem ARP em difusão onde associa o seu endereço MAC ao endereço do Terminal Móvel, sendo este processo denominado de "gratitous ARP".

De seguida o servidor MIP vai interagir com o módulo IPIP do núcleo para criar uma nova interface lógica de um túnel IPIP em que a origem é o próprio Home Agent e o destino é o endereço fixo que dá o acesso ao Terminal Móvel (o endereço do Foreign Agent, ou o endereço temporário alocado da rede visitada).

Por fim o servidor MIP adiciona uma nova linha à sua tabela de encaminhamento a qual indica ao sistema que o Terminal Móvel está acessível através da nova interface lógica IPIP acabada de criar. Desta forma todos os pacotes são enviados para a interface lógica de túnel, encapsulados, e enviados para o destino do túnel, utilizando encaminhamento normal IP.

4 - Home Agent que deixou de suportar um Terminal Móvel

Neste caso o servidor MIP vai voltar a configurar o sistema da forma normal relativamente a este nó da Internet, removendo a entrada específica na tabela de encaminhamento e removendo a interface lógica de túnel criada anteriormente; por outro lado, é também removida a linha especial referente ao Terminal Móvel na tabela de ARP, terminando assim com o mecanismo de "proxy ARP".

5 - Ambiente de Desenvolvimento/Teste do MIP

Uma vez iniciado o processo de desenvolvimento dos dois programas descritos no INESC (Desenho/Codificação/Teste), houve a necessidade de criar um ambiente adequado para o Teste Funcional deste protocolo no INESC.

Embora o edifício do INESC na Alves Redol seja bastante grande com 9 andares, o que significa centenas de utilizadores, existe apenas uma grande subrede IP baseada em Ethernet, com capacidade para mais de mais de quatro mil endereços, onde todas as máquinas estão inseridas (existe a excepção de alguns centros no INESC que têm subredes privadas que utilizam NAT - endereçamento privado). Isto significa que, qualquer máquina desta rede pode estar indiferentemente em qualquer "**hub**", "**switch**" ou **andar** pois está sempre dentro da mesma subrede IP.

No sentido deste trabalho, esta configuração goza automaticamente de **micro-mobilidade**, uma vez que é pelo recurso ao nível 2 (isto é, pelos "hubs" e "switchs") que os pacotes são encaminhados no interior da rede até ao terminal correcto.

Considerando apenas esta grande rede, a Macro-Mobilidade só seria necessária para possibilitar que os terminais móveis na rede do INESC pudessem vaguear para outras redes, que não a rede existente no edifício da Alves Redol (como por exemplo para uma das redes do IST). No entanto, esta situação é impraticável porque estas redes não estão localizadas fisicamente no mesmo edifício, além do facto que existe uma "firewall" na ligação entre as duas redes que iria bloquear os pacotes encapsulados IPIP (o MIP ainda não suporta "firewalls" devido aos problemas de segurança descritos na **secção 3.4**).

Assim, criou-se uma outra alternativa que não tivesse os problemas da situação anterior, mas que fosse ao mesmo tempo flexível e real. Para isto foi essencial criar condições para os terminais móveis puderem transitar **fisicamente** de rede muito facilmente, o que implica que ambas as redes terão que existir muito próximas uma da outra. Por outro lado foi também muito importante criar um ambiente de teste que pudesse ser isolado caso-a-caso do resto da rede, por forma a não causar dano à rede e aos seus utilizadores devido a falhas de programação da implementação do software MIP (entupindo a rede com mensagens, por exemplo).

Para isto foi criada e gerida uma nova subrede IP denominada de **Rede de Teste** que é completamente disjunta da rede do INESC. Esta nova rede utiliza endereços IP públicos únicos, pelo que esta é completamente acessível de qualquer ponto da Internet. As duas redes são ligadas através de um encaminhador Linux que tem duas interfaces físicas Ethernet.

Desta forma, esta nova rede vai ter um "hub" Ethernet no qual se concentram todos os seus nós constituintes. A grande vantagem desta configuração é que os terminais móveis podem facilmente transitar de subrede IP, apenas pela mudança do "hub" ao qual estão ligados. É esta facilidade que cria as condições realistas para o teste da Macro-Mobilidade, porque se tratam de subredes IP **disjuntas** e **independentes** ligadas entre si por um encaminhador IP. Com a utilização destas duas redes é possível então estabelecer vários cenários de testes funcionais à implementação do protocolo, definindo-se para cada cenário as condições iniciais, os resultados esperados e os resultados efectivamente atingidos, de forma a verificar se esta implementação desenvolvida corresponde aos requisitos do protocolo.

Num sistema de teste genérico existem várias combinações possíveis de terminais móveis/agentes de mobilidade, pois qualquer máquina pode ser um Terminal Móvel (desde que se "mova" fisicamente entre as duas redes), e porque qualquer encaminhador pode ser um agente de mobilidade (fixo) da rede onde está localizado. Cada situação vai ser testada com quatro configurações típicas possíveis: sistema sem o MIP, sistema com o MIP activo, sistema com o MIP com falha na autenticação, e sistema com o MIP sem existir Foreign Agents na rede visitada.

5.1 - Teste 1

A primeira situação de teste envolve 3 máquinas, todas com o sistema operativo Linux: um PC portátil **MH** pertencente à rede do INESC que se move entre as duas redes, um encaminhador fixo **HA** pertencente à rede do INESC que assume o papel de agente de mobilidade (Home + Foreign Agent) para a rede do INESC, e um encaminhador **FA** fixo que liga as duas redes. Adicionalmente este último encaminhador FA também é o agente de mobilidade (Home + Foreign Agent) para esta rede separada, embora este papel pudesse estar integrado noutro encaminhador qualquer dessa rede. Esta situação está resumida e representada nas **figuras 29, 30 e 30A**, sendo os pormenores remetidos para o **anexo F**.

Nome	Rede Origem	Função	Notas
MH	INESC	PC portátil Terminal Móvel	Move-se entre as duas Redes
HA	INESC	Agente de Mobilidade da Rede INESC	Home Agent de MH
FA	TESTE	Agente de Mobilidade da Rede TESTE	Foreign Agent para MH
X	INESC	host Genérico	Comunica com MH
R+FA	INESC+TESTE	"router" que liga as duas Redes	2 Interfaces EtherNet

Figura 29 - Resumo do Teste 1

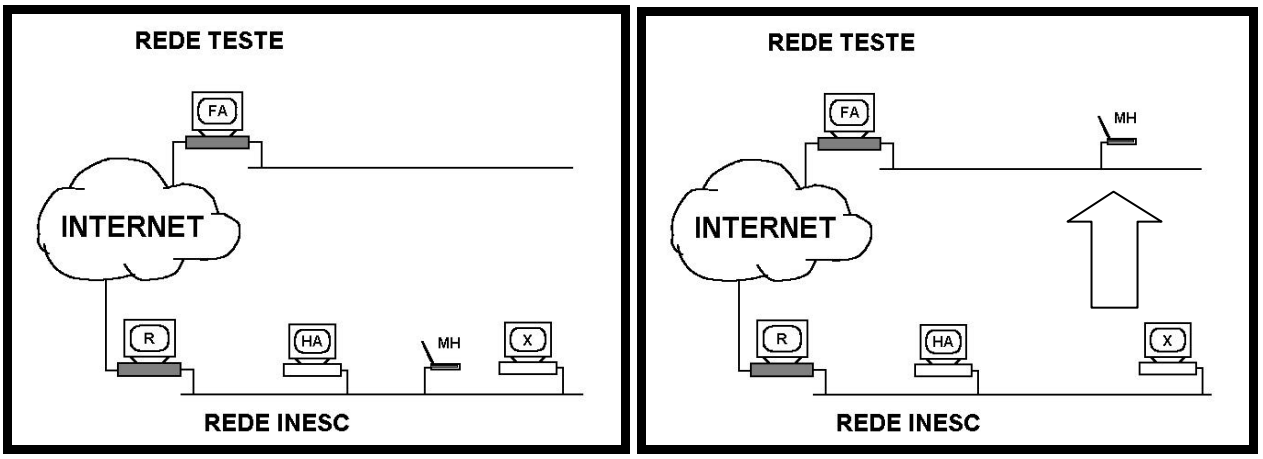


Figura 30 e 30A – Situação Inicial e Final

Nesta situação, para o teste à implementação vai-se considerar que o nó X, pertencente à rede do INESC, está a comunicar com o portátil MH durante toda esta operação, pelo que se esta comunicação se mantiver inalterada na situação final, o portátil passou a deter da Macro-Mobilidade desejada. Para testar esta comunicação vai-se utilizar o programa **ping**, que verifica continuamente se um dado nó da Internet está acessível. Na situação final podem-se considerar 3 casos distintos:

Caso 1: Sistema sem MIP

Para o primeiro caso vai-se testar esta configuração considerando que o software que implementa o MIP não está activo (no próprio portátil, ou nos agentes de mobilidade). Nesta situação o portátil MH não terá a Macro-Mobilidade, pelo que a ligação entre **X** e **MH** será sempre interrompida quando o portátil **MH** não estiver na sua rede de origem, o que se verifica na prática.

Caso 2: Sistema com MIP, sem falhas de segurança

Seguidamente, vai-se testar a mesma configuração considerando agora que o software que implementa o MIP está activo em ambas as redes (nos agentes de mobilidade) e no próprio Terminal Móvel. Neste caso a ligação entre **X** e **MH** será mantida quando o portátil está localizado fisicamente em qualquer das redes, o que também se verifica na prática.

Caso 3: Sistema com MIP, com falha de segurança

No último caso vão-se testar os mecanismos de segurança do MIP. Para isso, e com base no estado anterior, vai-se alterar a chave secreta partilhada do Terminal Móvel para uma nova. Desta

forma, os pedidos de registo do Terminal Móvel MH terão um resumo que não será aprovado pelo Home Agent, pois este não tem a mesma chave secreta que o Terminal Móvel. Nesta situação a Macro-Mobilidade não pode ser disponibilizada ao Terminal Móvel pelo Home Agent, o que se verifica na prática.

Este teste mostra que o MIP está correctamente implementado, uma vez que o portátil MH pode-se movimentar livremente entre as duas redes, ficando a conexão estabelecida com o nó X (que não tem MIP) inalterada em todas as situações; por outro lado, o serviço prestado pelos agentes é apenas concedido aos terminais moveis autorizados, pelo que esta implementação tem segurança.

5.2 - Teste 2

Desta base de trabalho também se podem derivar outras situações interessantes, como a segunda situação de teste em que se pretende que um Terminal Móvel possa dispor de Macro-Mobilidade mesmo quando não existir um Foreign Agent na rede visitada (**secção 2.2.2.1**). Para este teste vai-se criar uma situação oposta à anterior: o Terminal Móvel pertence agora à rede de Teste, estando acompanhado nesta rede de um agente de mobilidade HA (que é o Home Agent para o Terminal Móvel). O Terminal Móvel vai-se movimentar para a rede do INESC, que **não** vai propositadamente possuir nenhum agente de mobilidade MIP. Em alternativa, existe um servidor **DHCP** disponível que é utilizado para a configuração automática das máquinas desta rede, tendo um conjunto de endereços IP sob a sua gestão. Este teste está resumido e representado nas **figuras 31, 32 e 32A**, sendo os pormenores remetidos de novo para o **anexo F**.

Nome	Rede Origem	Função	Notas
MH	TESTE	PC portátil Terminal Móvel	move-se entre as duas Redes
HA	TESTE	Agente de Mobilidade da Rede TESTE	Home Agent de MH
DHCP	INESC	Servidor de Configuração da Rede INESC	fornece Configuração a MH
X	INESC	host Genérico	comunica com MH
R	INESC+TESTE	"router" que liga as duas Redes	2 Interfaces EtherNet

Figura 31 – Resumo do Teste 2

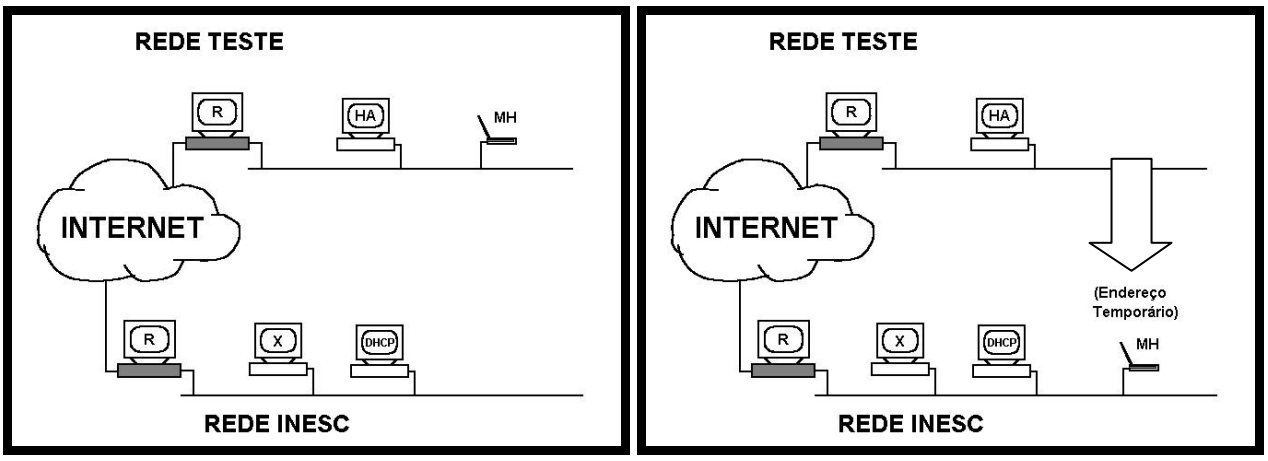


Figura 32 e 32A – Teste 2 – Situação Inicial e Final

Novamente pode-se considerar vários casos possíveis deste Teste, sendo a conexão estabelecida entre o portátil MH e o nó X.

Caso 1: Sistema sem MIP

Neste primeiro caso o software que implementa o MIP não está activo no próprio portátil: como é esperado, verifica-se que a conexão será imediatamente interrompida quando o portátil transita de rede.

Caso 2: Sistema sem MIP, utilizando DHCP para manter a conectividade mínima

Neste caso o portátil ainda não tem o MIP activo, mas vai-se configurar por DHCP utilizando o servidor existente para ter uma conectividade mínima, pois este vai dar ao Terminal Móvel um endereço IP da rede do INESC para utilização. Nesta situação o Terminal Móvel pode estabelecer uma nova ligação com o nó X, mas agora utilizando o seu novo endereço IP. O problema deste procedimento é que a conexão anterior foi irremediavelmente perdida.

Caso 3: Sistema com MIP, utilizando DHCP em vez de Foreign Agent

Neste último caso, vai-se recriar a transição de rede mas agora com o MIP activo no portátil. Quando este chega à rede visitada, vai procurar um agente de mobilidade (sem sucesso), até que inicia o protocolo DHCP automaticamente (ao fim de um certo tempo sem receber anúncios). Quando isto acontece, o portátil vai voltar a usar o seu endereço IP original (ficando o endereço dado pelo DHCP como endereço temporário), regista-se no agente HA, e desencapsula os seus pacotes que lhe são enviados pelo agente HA. Esta sequência de acções significa que a ligação com o nó X vai-se manter activa na situação final, o que se verifica na pratica com a utilização do comando "ping", o que mostra que esta implementação do cliente MIP suporta convenientemente a opção MIP de estar "sozinho" numa rede visitada sem agentes de mobilidade.

5.3 - Teste 3

Pode acontecer que nesta ultima situação do Teste 2 que o Terminal Móvel detecte a existência de um Foreign Agent na rede visitada onde está neste momento localizado, que só agora se tenha activado. Nesta nova situação, o Terminal Móvel vai automaticamente abdicar do seu endereço temporário e registar-se no novo agente **FA**, o que tem como efeito libertar o endereço IP temporário que tinha sido alocado por DHCP para outras utilizações (**figura 33**)

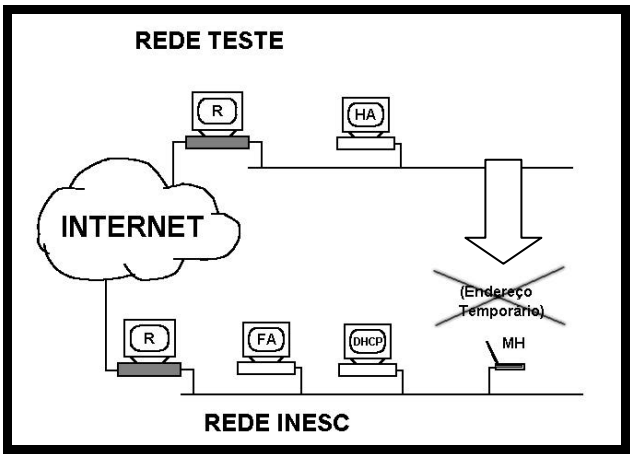


Figura 33 - Teste 3

Esta evolução do Teste anterior mostra que esta implementação do cliente MIP vai dar sempre preferência a deter da macro-mobilidade utilizando Foreign Agents (em vez de estar sozinho), o que é requerido pelo standard MIP.

5.4 – Ambiente de Teste "Wireless"

Esta implementação do protocolo MIP em sistemas Linux foi baseada numa tecnologia simples e muito difundida, as redes locais Ethernet. No entanto o MIP terá o seu máximo interesse

quando for implementado numa tecnologia de rede wireless, concretizando assim a Mobilidade Total, o que levantará indubitavelmente novos problemas a esta implementação.

Um exemplo será o problema previsível apenas existente num ambiente wireless em que as diferentes subredes IP vão poder estar parcialmente justapostas em certos locais, uma vez que estão no alcance das duas redes simultaneamente. Nesta situação os terminais móveis "wireless" irão receber simultaneamente vários anúncios de existência de vários agentes de mobilidade de diversas redes IP ao mesmo tempo, o que é uma situação que nunca acontece nas redes locais Ethernet onde cada terminal pertence e está no alcance apenas de uma única rede (**figura 34**).

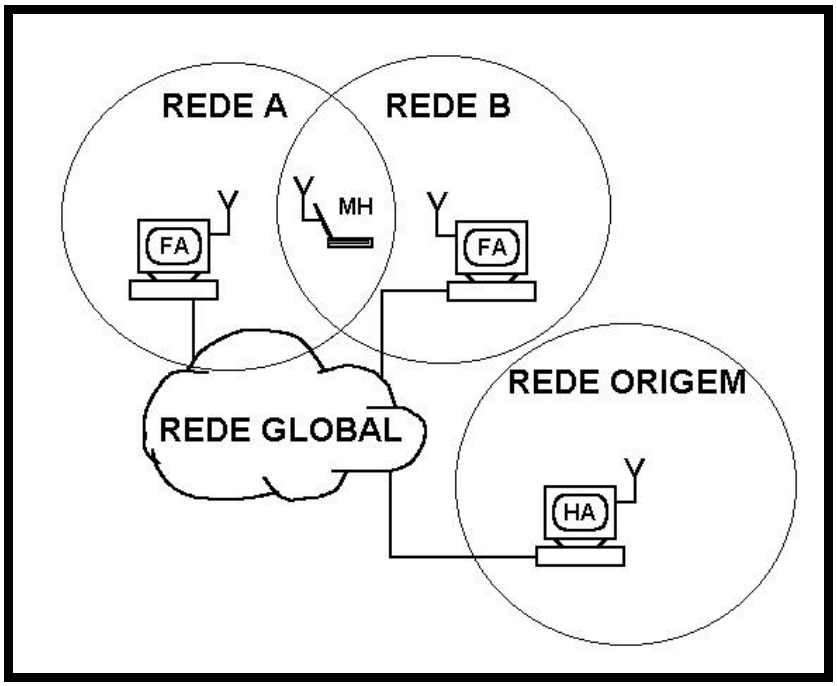


Figura 34 - Oscilação na escolha de Foreign Agents

Embora este problema não se manifeste actualmente nesta implementação de MIP em Ethernet, uma possível solução já foi desenhada e implementada que evita que os terminais móveis tenham um comportamento oscilatório na presença de vários agentes de mobilidade de várias redes diferentes (**secção 4.2.1**).

Por outro lado esta implementação em Linux também se mostra promissora relativamente a uma futura implementação sobre tecnologia "wireless": uma vez que ambas as tecnologias são semelhantes em alguns aspectos (ambos são meios de difusão, e os formatos dos pacotes dos protocolos de nível 2 são parecidos) leva a que haja actualmente drivers de interfaces "wireless" 802.11 que emulem uma Ethernet (com os mesmos tipos de pacotes e características), o que é suficiente (teoricamente) para executar este software sem quaisquer modificações nestes meios físicos. Um exemplo de uma placa com esta capacidade é a NCR Wavelan Card, com versões PCMCIA e ISA.

6 – Conclusões

O Trabalho descrito ao longo deste texto espelha de forma perfeita a organização do mesmo que conduziu, em última análise, à implementação correcta do protocolo MIP no sistema operativo Linux.

De início separou-se os dois grandes tipos de Mobilidade em Redes de Dados, sendo cada vertente separada pela sua escala geográfica, que é a maior característica de distinção entre os dois tipos de Mobilidade, concluindo-se quais os objectivos e área de acção de cada uma, ao mesmo tempo que se estabeleceu uma importante ligação de cada tipo de Mobilidade com os níveis de protocolos OSI. Outra conclusão importante foi verificar que a Macro-Mobilidade é relativa apenas ao movimento de Terminais Móveis **entre diferentes** redes Locais, sendo o seu complementar Micro-Mobilidade relativo apenas ao movimento de Terminais Móveis no interior das Redes Locais.

Seguidamente, foi a Macro-Mobilidade a vertente escolhida para o tema deste Trabalho, sendo aqui apenas focados os aspectos da sua disponibilização, implementação e manutenção em Redes de Dados **que não foram especificamente** desenhadas para ter esta característica nos seus Terminais. Na analise da solução genérica, verificou-se que estas Redes Globais têm apenas um endereçamento estático, o que simplifica os mecanismos de encaminhamento protocolo, mas ao mesmo tempo que obriga a que os Terminais Móveis estejam sempre no interior da sua Rede de Origem, de forma a serem correctamente endereçados em todas as situações. Isso significa que a mudança de rede por parte de um terminal móvel significaria a mudança obrigatória de endereço, o que impossibilitaria a manutenção das ligações já existentes ao longo do movimento de um terminal móvel.

No entanto foi descrito um mecanismo genérico que implementa a Macro-Mobilidade em **qualquer** Rede de Dados que utilize endereçamento estático, o que é concretizado com a introdução de novas entidades que vão cooperar com o objectivo de possibilitar a Macro-Mobilidade aos Terminais Móveis. Estas novas entidades são denominadas de agentes de mobilidade, e vão criar um endereçamento especial dinâmico relativo aos terminais moveis. Este endereçamento especial já vai possibilitar que estes detenham de conectividade total **(receber e enviar** pacotes de informação) numa qualquer Rede local da Rede Global, sempre endereçados pelo seu endereço Global. No Texto foram depois descritos pormenorizadamente estes mecanismos de suporte da Macro-Mobilidade, sendo estes divididos em 3 fases – Localização, Registo e Execução, de tal forma que os terminais moveis têm um papel Activo no processo, e os agentes de mobilidade têm um papel Reactivo/Passivo.

Embora esta solução apresentada funcione, padece de dois grandes problemas, relativamente aos quais se apresentam as soluções genéricas. Por um lado, pelo que foi descrito, teriam que existir agentes de mobilidade espalhados por todas as redes locais para que os terminais tivessem sempre o suporte à a Macro-Mobilidade, o que não é garantido. Por outro lado, os pacotes de Informação não vão seguir o seu caminho mais curto desde o seu emissor até ao Terminal Móvel na sua localização actual, uma vez que estes têm sempre que passar pela rede de origem do Terminal Móvel (**Triangulação**).

De seguida foi analisada esta mesma solução aplicada à Internet, verificando-se que os conceitos descritos no capitulo anterior se encaixam de uma forma perfeita relativamente ao protocolo MIP, que é uma extensão do protocolo IP clássico para terminais Moveis. Este protocolo vai ter um comportamento completamente transparente com todo o resto da infra-estrutura já existente da Internet, pois este protocolo apenas exige a implementação do MIP nos Terminais Moveis e nos Agentes de Mobilidade, sendo no entanto enquadradas as fases referidas na descrição genérica e as opções do processo da Macro-Mobilidade no mundo IP. São também descritas a arquitectura de protocolos do MIP, bem como o formato das mensagens trocadas e os tipos de encapsulamentos standard do protocolo.

A descrição detalhada do MIP é finalizada com uma descrição importante dos processos de segurança que são obrigatórios nos processos MIP, tendo sido verificados quais os problemas graves que poderiam advir se este protocolo não fosse seguro. No entanto é também esta segurança que causa problemas administrativos graves, pelo que estas situações ainda estão em estudo no IETF.

Da descrição do MIP é detalhada a descrição da implementação deste protocolo, que serviu para complementar o estudo efectuado da Macro-Mobilidade em redes de dados. Neste sentido verificou-se que o sistema operativo Linux tinha diversas vantagens para a implementação do MIP, nomeadamente no seu Stack TCP/IP que é bastante completo e flexível, tendo este sido convenientemente detalhado. Uma vez que ainda não havia nenhuma implementação difundida do protocolo MIP para Linux, a escolha desta plataforma para a realização da parte prática deste Trabalho foi directa. Neste sentido desenhou-se uma implementação MIP baseada no paradigma Cliente/Servidor, baseado em "deamons" para minimizar o peso do novo protocolo no restante sistema. Também foi tomada em consideração a divisão do protocolo em 2 fluxos de dados distintos, tendo sido o Controlo MIP delegado para os "deamons" que implementam o novo software, controlando e configurando este o núcleo do Linux, onde iram ser processados os Dados MIP. Esta implementação foi posteriormente testada com testes funcionais, que confirmaram a validação desta implementação.

A implementação do protocolo MIP em sistemas Linux foi baseada numa tecnologia simples e muito difundida, as redes locais Ethernet. No entanto o grande interesse do MMIP surge no contexto da tecnologia de rede "wireless", concretizando assim a **Mobilidade Total.** Neste novo cenario, novos problemas irão surgir, não focados neste estudo e implementação. No entanto esta implementação do MIP em Linux mostra-se promissora relativamente a uma futura implementação sobre esta tecnologia, uma vez que a transição de Ethernet para 802.11 é um processo facilitado (devido às semelhanças dos pacotes e meios de difusão). Outra evolução possivel seria a implementação de novos clientes MIP em novas plataformas, nomeadamente a plataforma Windows.

Outro possível interesse nesta tecnologia de Macro-Mobilidade reside na sua utilização, no futuro, na nova situação dual em que irão existir duas novas redes separadas no **INESC**, derivada pela separação desta instituição em **INESC-INOV** e **INESC-ID**. Esta situação descrita já leva a uma necessidade real e premente destes mecanismos, pois a falta destes inviabiliza o movimento dos terminais moveis no interior do Edifício, em que nessa situação já existiram duas redes separadas.

Por fim, poder-se-ão considerar outros cenários mais abrangentes, que vão partir da base de mobilidade já atingida, onde nomeadamente se poderá estudar as questões da Macro-Mobilidade num ambiente que integre também de base **a Micro-Mobilidade** com garantias de **Qualidade de Serviço**.

7 – Referências Bibliográficas

[1] C. Perkins - IP Mobility Support, RFC2002, 1996

[2] Roger Kalden, Wireless Internet Access Based on GPRS, IEEE Personal Communications, April 2000

[3] Edward C. Prem, Wireless Local Area Networks

[4] S. A. Tanenbaum – "Computer Networks", 3nd Edition, Prentice Hall Internation, 1996

[5] Alves Marques, Paulo Guedes, "Tecnologia de Sistemas distribuidos", FCA editora, 1998

[6] C. Perkins, IP Encapsulation within IP, RFC 2003, 1996

[7] C. Perkins, Minimal Encapsulation within IP, 2004, 1996

[8] Deering, S., "ICMP Router Discorvery Messages", RFC 1256, 1989

[9] Droms, R., "Dynamic Host Configuration Protocol", RFC 1541, 1993

[10] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, 1992

[11] Plummer, D, "An EtherNet Address Resolution Protocol", RFC 826, MIT-LCS, 1982

[12] Matt Welsh, Lar Kaufman, "Running Linux", O'Reilly & Associates inc., 1995

[13] Olaf Kirch, "The Network Administrators' Guide", Linux Documentation Project, 1996

[14] Lars Wirzenius, "Linux System Administrators' Guide 0.6", Linux Documentation Project, 1997

[15] Matt Welsh, "Linux Installation and Getting Started" , Linux Documentation Project, 1996

[16] Alessandro Runini, "Linux Device Drivers", O'Reilly & Associates inc., 1998

[17] Terry Dawson, Linux NET-3-HOWTO (Linux Networking), Linux Documentation Project, 1998

[18] Paul Gortmaker, Linux Ethernet-Howto, Linux Documentation Project, 1998

[19] A. N. Kuznetsov, "IP Command Reference", IPRoute2 Documentation, 1999

[20] A. N. Kuznetsov, "Tunnels over IP in Linux-2.2", IPRoute2 Documentation, 1999

[21] Fred N. van Kempen, "ARP Man Page", Linux Programmer's Manual, net-tools Documentation, 1999

[22] Phil Blundell, "Route Man"page, Linux Programmer's Manual, net-tools Documentation, 1997

[23] Fred N. van Kempen, "Ifconfig Man Page", Linux Programmer's Manual, net-tools Documentation, 1997

[24] Bob Edwards, ProxyARP Subnetting HOWTO, Linux Documentation Project, 1997

[25] Vladimir Vuksan, DHCP mini-HOWTO (DHCPd/DHCPcd), Linux Documentation Project, 1998

ANEXOS

ANEXO A: Mensagens MIP da fase de Localização

Cabeçalho ICMP - Router Advertisement

Tipo	Código	Checksum
# Endereços		Tempo de Vida (ICMP)
1º Endereço de Router 2º Endereço de Router ...		

Tipo: 9 - "Router Advertisement"
Código: 0 se o agente é (também) um encaminhador. 16 caso contrário.
Checksum: Código de detecção de erros, aplicado à informação ICMP (cabeçalho + extensões MIP)
Tempo de Vida ICMP: o período, em segundos, que esta mensagem é valida.
 # Endereços: número de endereços de routers presentes neste anuncio.
Imediatamente a seguir ao cabeçalho ICMP vão estar presentes os endereços IP dos routers existentes nesta rede IP, sendo estes representados como o último campo (de comprimento variável) do esquema.

EXTENSÃO ICMP LOCALIZAÇÃO MIP

Tipo	Comprimento	Número de Sequencia
Tempo de Vida (Registo MIP)		Flags
1º Endereço de Agente de Mobilidade 2º Endereço de Agente de Mobilidade ...		

Tipo: 16 – indica que é a extensão ICMP de localização MIP.
Comprimento: 6 + 4 * N; N é o número de endereços de Agentes de Mobilidade presentes na mensagem.
Número de Sequencia: contador de anúncios enviados desde que o agente foi inicializado.
Tempo de Vida: o número máximo de segundos para a alocação de recursos que este agente está disposto a aceitar dos terminais móveis.
Flags: Opções do agente de mobilidade
Imediatamente a seguir à extensão MIP de localização vão estar presentes os endereços IP dos Agentes de mobilidade existentes nesta rede IP, sendo estes representados como o último campo (de comprimento variável) do esquema.

Cabeçalho ICMP - Router Solicitation

Tipo	Código	Checksum
		Tempo de Vida (ICMP)

Tipo: 10 - "Router Solicitation"
Código: 0

ANEXO B- Mensagens MIP da fase de Registo

MIP Registo

Tipo	Flags	Tempo de Vida
Endereço IP do Terminal Móvel		
Endereço IP do Home Agent do Terminal Móvel		
Endereço IP do Foreign Agent do Terminal Móvel		
Identificação		
Extensões...		

Tipo – 1 – "Register Request".
Tempo de Vida – o tempo expresso em segundos que o Terminal Móvel pretende ter de utilização dos mecanismos e recursos da Macro-Mobilidade.
Identificação – relaciona respostas a pedidos
Flags – Opções do registo de Macro-Mobilidade.

MIP Resposta do Registo

Tipo	Código	Tempo de Vida
Endereço IP do Terminal Móvel		
Endereço IP do Home Agent do Terminal Móvel		
Identificação		
Extensões...		

Tipo – 3 – "Register Reply"
Tempo de Vida – o tempo expresso em segundos concedido ao Terminal Móvel dos mecanismos de Macro-Mobilidade.
Identificação – relaciona respostas a pedidos
Código – Sucesso/Insucesso do registo.

Códigos de Recusa do Foreign Agent:

Código	Significado
64	Razão não específicada
65	Proibição administrativa
66	Falta de Recursos
67	Autenticação falhada - Terminal Móvel
68	Autenticação falhada - Home Agent
69	Tempo de Vida pedido demasiado grande
70	Pedido de Registo Mal-Formado
71	Resposta do HA Mal-Formada
72	Tipo de encapsulação indisponível
73	Compressão Van Jacobson indisponível
80	Rede de Origem não acessível
81	Home Agent não acessível
82	Porto UDP MIP do Home Agent inacessível
88	Outro erro de ICMP ao contactar o Home Agent

Códigos de Recusa do Home Agent:

Código	Significado
128	Razão não específicada
129	Proibição administrativa
130	Falta de Recursos
131	Autenticação falhada - Terminal Móvel
132	Autenticação falhada - Foreign Agent
133	Erro de Identificação
134	Pedido de Registo Mal-Formado
135	Demasiados registos simultâneos
136	Endereço de Home Agent desconhecido

EXTENSÃO MIP – Autenticação

Tipo	Comprimento	Tipo de Autenticação
Tipo de Autenticação (cont.)		Autenticação...

Tipo – 32 – Autenticação entre o Terminal Móvel e o Home Agent
33 – Autenticação entre o Terminal Móvel e o Foreign Agent
34 – Autenticação entre o Foreign Agent e o Home Agent.
Comprimento – indica o tamanho desta extensão
Autenticação – Campo de tamanho variável, que contem os dados produzidos pelo mecanismo de autenticação que está a ser utilizado.

ANEXO C – Tipos de encapsulamento dos pacotes IP na fase de Execução

Encapsulamento IPIP

Pacote Original IP:

Cabeçalho IP Original	Payload IP

Pacote Original Encapsulado dentro de um Túnel IPIP:

Novo Cabeçalho IP	Cabeçalho IP Original	Payload IP

Pacote Original IP:

Versão	IHL	TOS	Comprimento Total	
Identificação IP			Flags	Offset deste Fragmento
TTL		**Protocolo IP**	Checksum	
Endereço IP Origem Original				
Endereço IP Destino Original – Endereço Fixo do Terminal Móvel				
Payload IP: TCP / UDP / outros				

Pacote Original Encapsulado dentro de um Túnel IPIP:

Versão	IHL	TOS	Comprimento Total	
Identificação IP			Flags	Offset deste Fragmento
TTL		**Protocolo IPIP**	Checksum	
Endereço IP Origem (encapsulador) – Home Agent				
Endereço IP Destino (desencapsulador) - FA / Endereço Temporário do T.M.				
Versão	IHL	TOS	Comprimento Total	
Identificação IP			Flags	Offset deste Fragmento
TTL		**Protocolo IP**	Checksum	
Endereço IP Origem Original				
Endereço IP Destino Original – Endereço Fixo do Terminal Móvel				
Payload IP: TCP / UDP / outros				

Versão - 4
Internet Header Length – 5 palavras de 32 bits (20 bytes)
Type of Service – copiado do pacote encapsulado
Time to Live – um novo valor, apropriado para entregar o pacote encapsulado ao seu destino.

Protocolo – IPIP
Endereco Origem – a entrada do túnel, o Home Agent
Endereco Destino – a saída do túnel, o Foreign Agent ou o próprio Terminal Móvel (se estiver sozinho uma rede visitada, com um endereço IP local alocado)
Os campos flags, identificação IP e Offset de Fragmento são todos criados de novo para o cabeçalho envolvente.

Encapsulamento MINIMAL IP

Pacote Original IP:

Cabeçalho IP Original	Payload IP

Pacote Original Encapsulado dentro de um Túnel MIN_IPIP:

Cabeçalho IP Original	Cabeçalho MIN	Payload IP

Pacote Original IP:

Versão	IHL	TOS	Comprimento Total	
Identificação IP			Flags	Offset deste Fragmento
TTL		**Protocolo IP**	Checksum	
Endereço IP Origem				
Endereço IP Destino – Endereço Fixo do Terminal Móvel				
Payload IP: TCP / UDP / outros				

Pacote Original Encapsulado dentro de um Túnel IPIP:

Versão	IHL	TOS	Comprimento Total Original + 8/12	
Identificação IP			Flags	Offset deste Fragmento
TTL		**Protocolo MINIPIP**	Novo Checksum	
Endereço IP Origem (encapsulador) – Home Agent				
Endereço IP Destino (desencapsulador) - FA / Endereço Temporário do T.M.				
Protocolo IP	Flags (MIN)		Checksum (MIN)	
Endereço IP Destino – Endereço Fixo do Terminal Móvel				
(opcional) Endereço IP Origem original (se não for o encapsulador)				
Payload IP: TCP / UDP / outros				

ANEXO D - Configuração do Terminal Móvel por Comandos Externos

1 - Rede visitada com Foreign Agent

arp -d <enderecos>
route del <enderecos>
route add -host <FA> dev <device>
route add default gw <FA>

2 - Rede visitada sem Foreign Agent, usando DHCP ou PPP

ifconfig
route -n

arp -d <enderecos>
route del <enderecos>

ifconfig <interface fisica> <IP fixo>
ifconfig <interface logica> <IP temporario>
ifconfig <interface tunel> <Home Agent> <IP temporario>

route add -host <Router> dev <interface fisica>
route add default gw <Router>

3 - Rede de Origem

arp -d <enderecos>
route del <enderecos>

ifconfig <interface fisica> <IP fixo>
ifconfig <interface logica> down
ifconfig <interface tunel> down

route add -host <Router> dev <interface fisica>
route add -net <Rede Origem> dev <interface fisica>
route add default gw <Router>

ANEXO E - Configuração do Agente de Mobilidade por Comandos Externos

1 - Foreign Agent a suportar um Terminal Móvel visitante

ifconfig <interface tunel> <Home Agent> <Foreign Agent>
route add -host <Terminal Movel> dev <interface fisica>

2 - Foreign Agent que deixou de suportar um Terminal Móvel visitante

ifconfig <interface tunel> down
route del -host <Terminal Movel> dev <interface fisica>

3 - Home Agent a suportar um Terminal Móvel que está numa outra rede visitada

arp -i <Interface> -s <Terminal Movel> <MAC Home Agent> pub
ifconfig <interface tunel> <Home Agent> <Foreign Agent/IP temporario>
route add -host <Terminal Movel> dev <interface Tunel>

4 - Home Agent que deixou de suportar um Terminal Móvel

arp -i <Interface> -d <Terminal Movel> pub
ifconfig <interface tunel> down
route del -host <Terminal Movel>

ANEXO F - Exemplos de Testes do MIP

Estes testes esquematizam diversas situações reais de teste da implementação do MIP no INESC. Em todos estes testes pode existir uma qualquer combinação de routers e redes locais entre a rede de origem do Terminal Móvel e a rede visitada por este (representada pela "nuvem" Internet nas figuras), embora para efeitos de simplicidade na situação real no INESC apenas exista um único router que liga as duas redes (o que não faz perder a generalidade do protocolo MIP e nem desta implementação em particular).

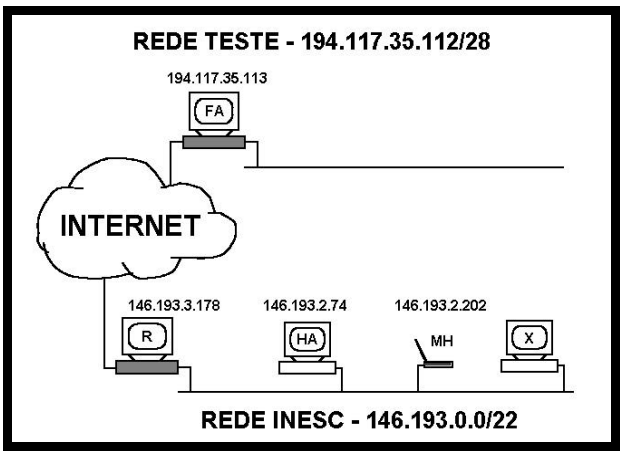
Rede do INESC (Alves Redol):

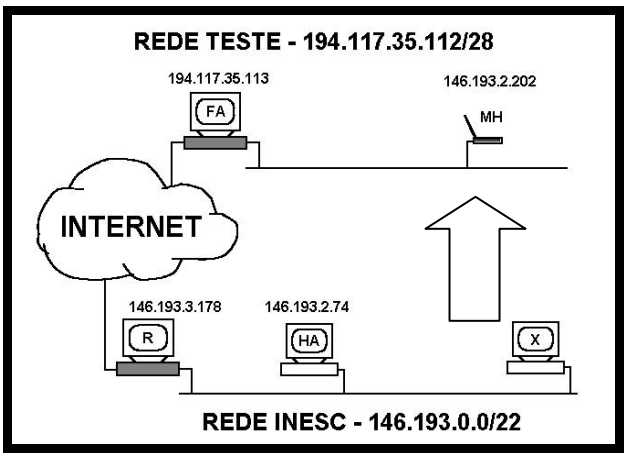
Endereço Rede	**146.193.0.0**
Netmask	**255.255.252.0 (10 bits, 4096 endereços)**
Encaminhadores	**146.193.3.178 - Interface com 194.117.35.112** **146.193.0.254 - Interface com o Exterior**
Servidores	**146.193.0.1 - DNS** **146.193.3.222 - DHCP**
Clientes MIP	**146.193.2.202**
Servidores MIP	**146.193.2.74** **146.193.2.221**

Rede de TESTE:

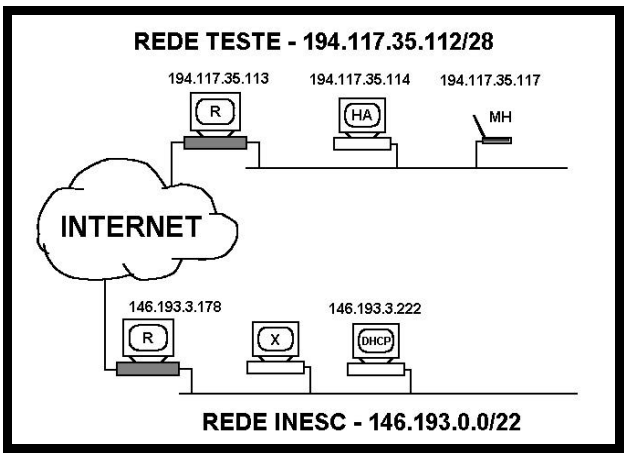
Endereço Rede	**194.117.35.112**
Netmask	**255.255.255.240 (4 bits, 16 endereços)**
Encaminhadores	**194.117.35.113 - Interface com 146.193.0.0**
Servidores	**194.117.35.113 - DHCP**
Clientes MIP	**194.117.35.117**
Servidores MIP	**194.117.35.113** **194.117.35.114**

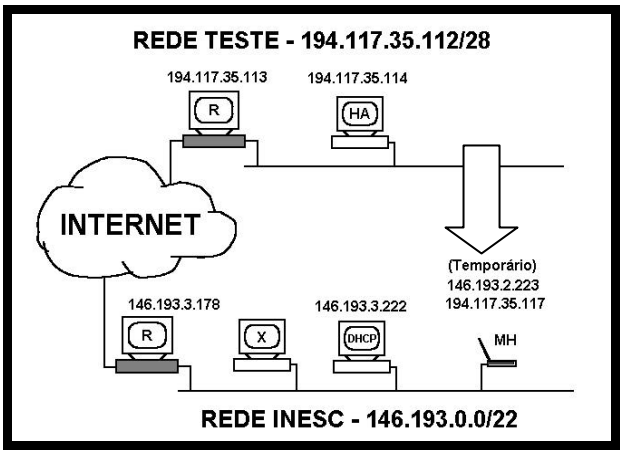
Teste 1

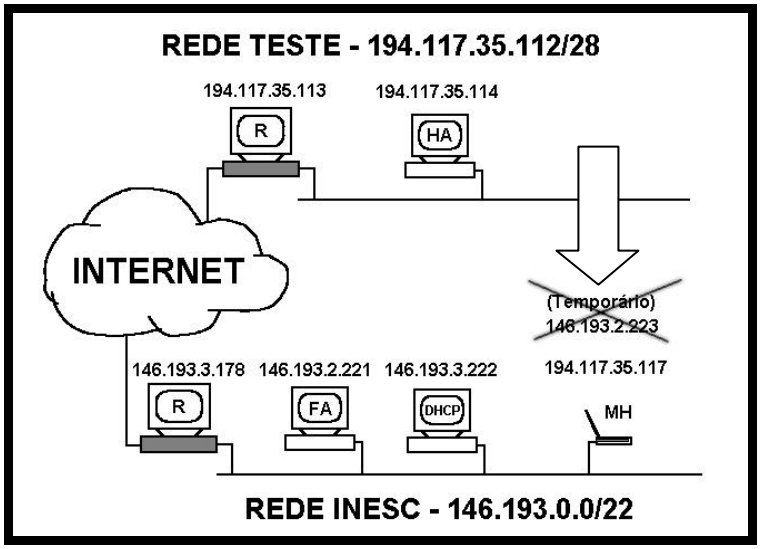




Teste 2:


REDE TESTE - 194.117.35.112/28
194.117.35.113
194.117.35.114
194.117.35.117
R
HA
MH
INTERNET
146.193.3.178
146.193.3.222
R
X
DHCP
REDE INESC - 146.193.0.0/22


REDE TESTE - 194.117.35.112/28
194.117.35.113
194.117.35.114
R
HA
INTERNET
(Temporário)
146.193.2.223
194.117.35.117
146.193.3.178
146.193.3.222
R
X
DHCP
MH
REDE INESC - 146.193.0.0/22


REDE TESTE - 194.117.35.112/28
194.117.35.113
194.117.35.114
R
HA
INTERNET
(Temporário)
146.193.2.223
146.193.3.178
146.193.2.221
146.193.3.222
194.117.35.117
R
FA
DHCP
MH
REDE INESC - 146.193.0.0/22

ANEXO G – Diagramas Temporais Completos do MIP

Diagrama temporal completo das fases da Macro-Mobilidade (Caso Simples) (Fase 1 - Localização; Fase 2 - registo; Fase 3 - Execução da Macro-Mobilidade)

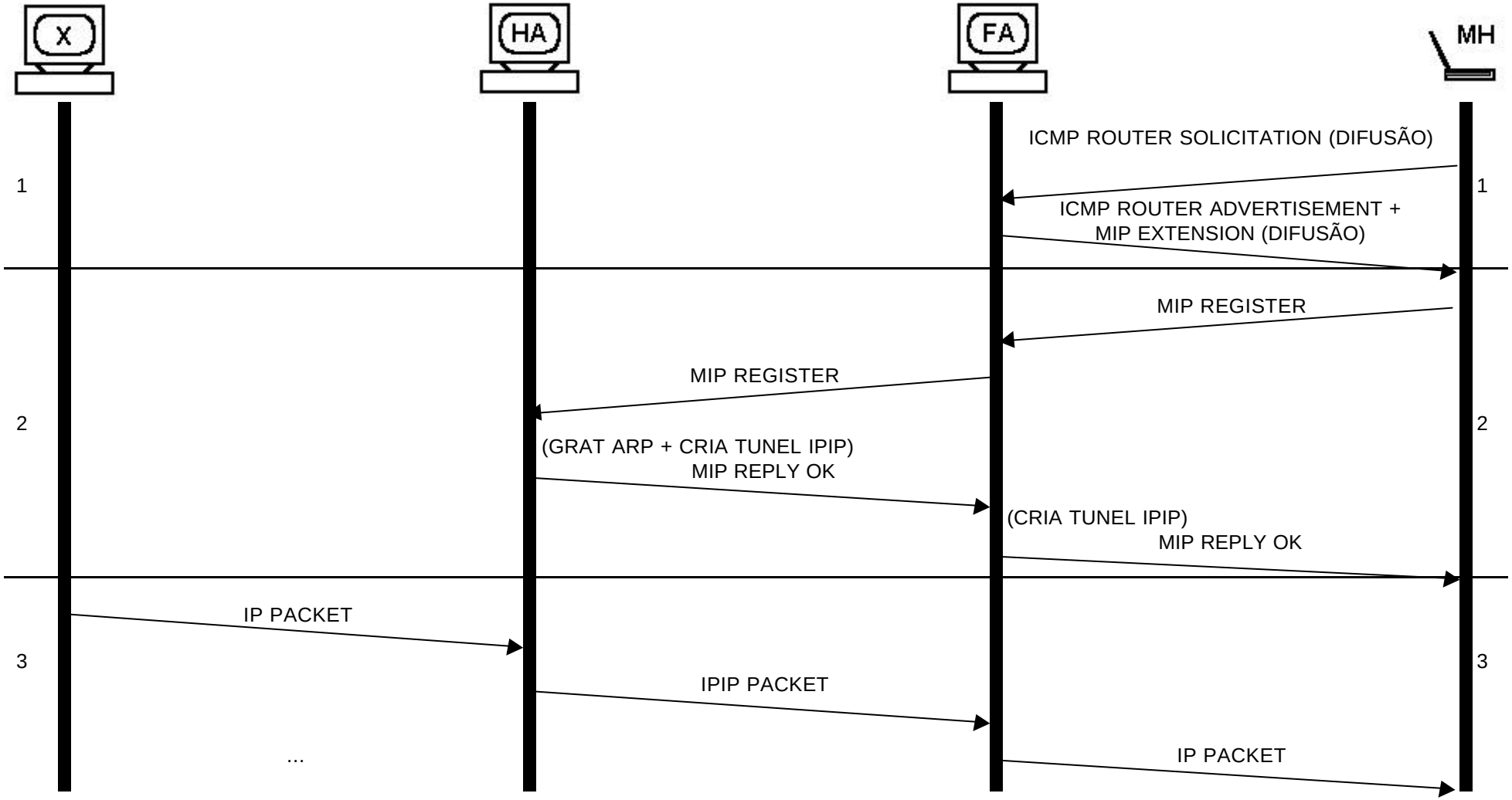


Diagrama temporal completo das fases da Macro-Mobilidade (Terminal móvel com DHCP)
(Fase 1 - Localização; Fase 2 - registo; Fase 3 - Execução da Macro-Mobilidade)

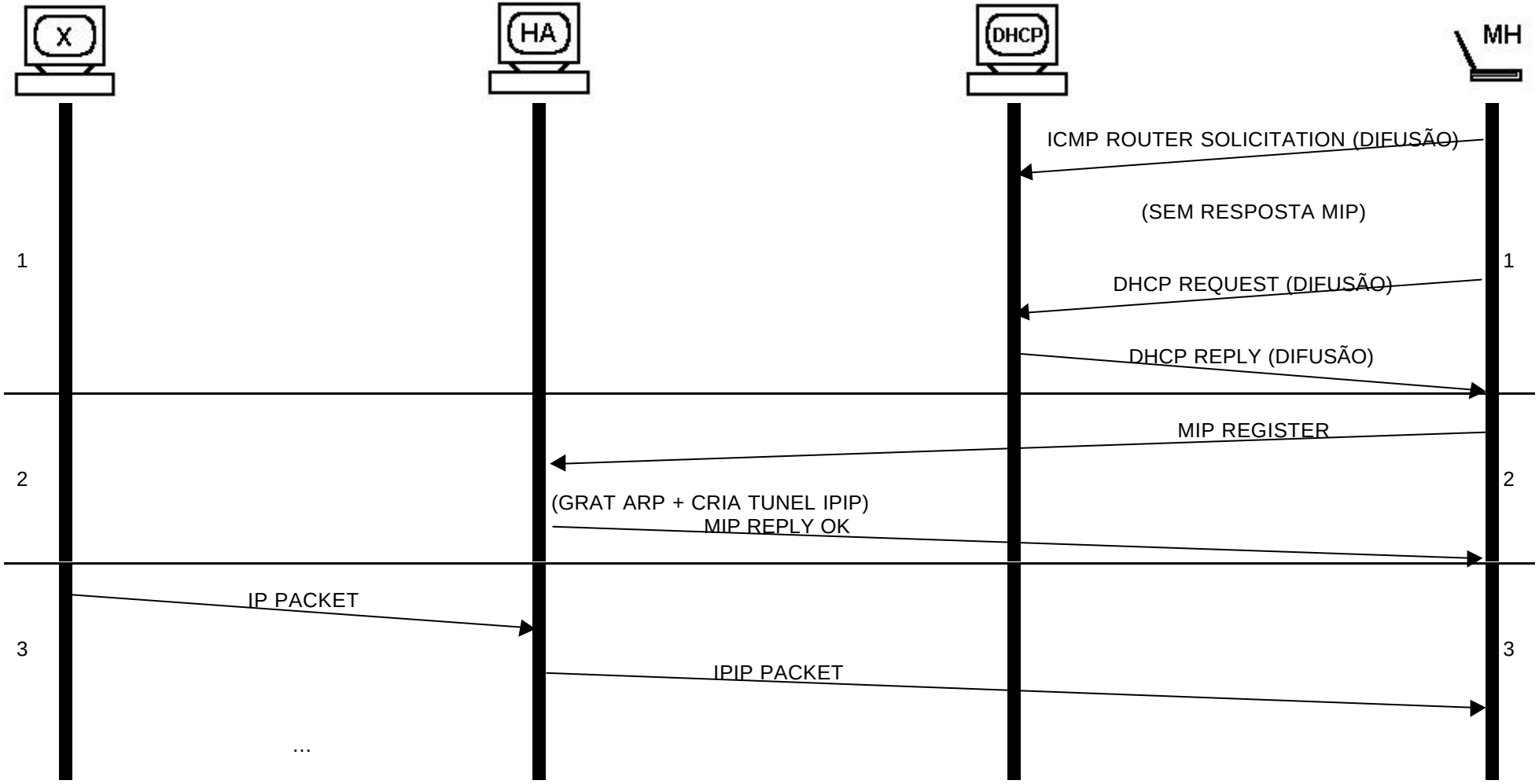


Diagrama temporal completo das fases da Macro-Mobilidade (Sem Triangulação)
(Fase 1 - Localização; Fase 2 - registo; Fase 3 - Execução da Macro-Mobilidade)

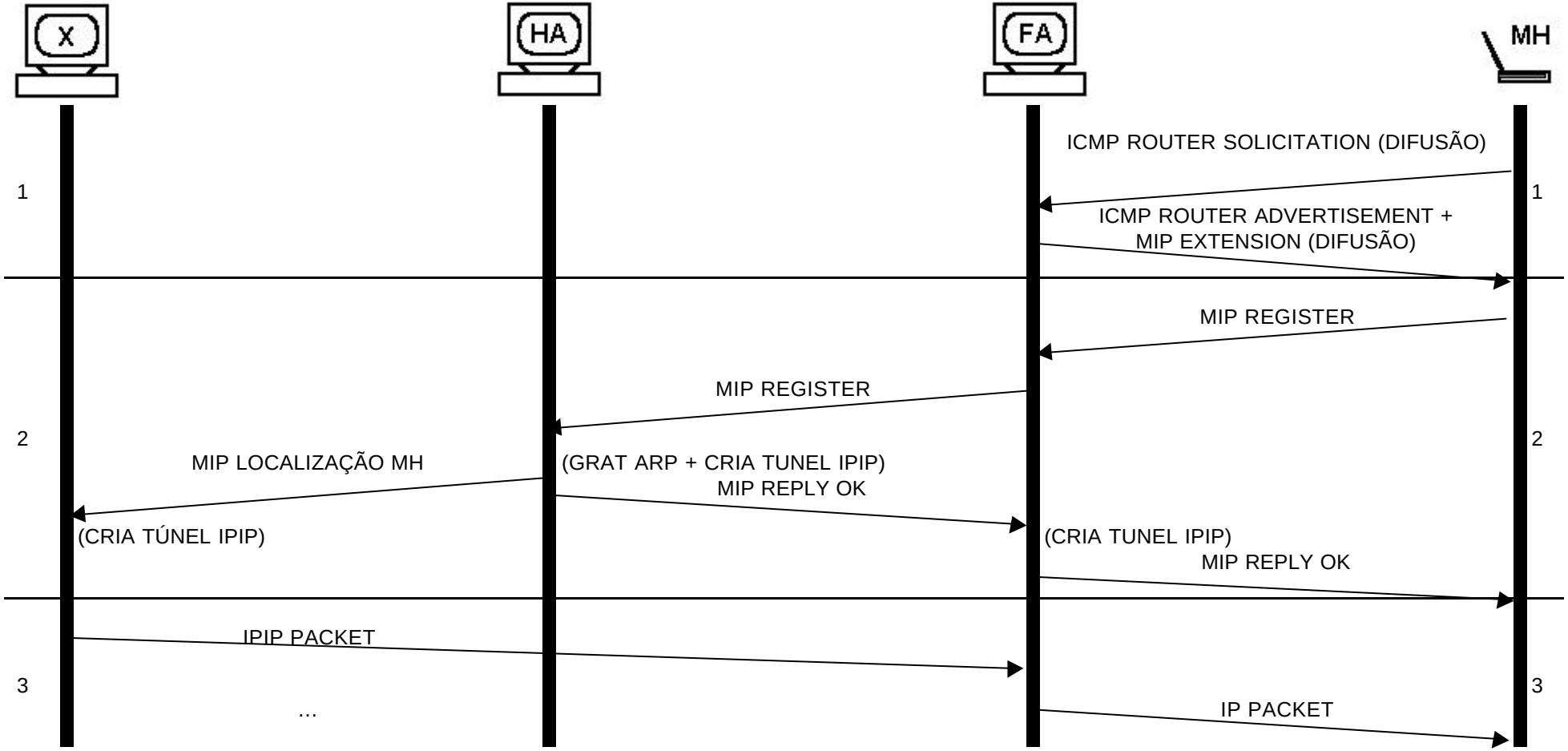


Diagrama temporal completo das fases da Macro-Mobilidade (MH com DHCP + Sem Triangulação)
(Fase 1 - Localização; Fase 2 - registo; Fase 3 - Execução da Macro-Mobilidade)