UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

GERENCIAMENTO DE TÚNEIS EM AMBIENTE MOBILE IP INTEGRADO A MPLS

ALEX HELDER CORDEIRO DE OLIVEIRA

ORIENTADOR: DR. PAULO HENRIQUE PORTELA DE CARVALHO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGENE.DM - 252A/06
BRASÍLIA/DF: MARÇO - 2006

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

GERENCIAMENTO DE TÚNEIS EM AMBIENTE MOBILE IP INTEGRADO A MPLS

ALEX HELDER CORDEIRO DE OLIVEIRA

DISSERTAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISÍTOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

_____

Prof. Paulo Henrique Portela de Carvalho, Dr. (ENE-UnB)
(Orientador)

_____

Prof. Ricardo Staciarini Puttini, Dr. (ENE-UnB)
(Examinador Interno)

_____

Prof. Jacir Luiz Bordim, PhD. (CIC-UnB)
(Examinador Externo)

BRASÍLIA/DF, 17 DE MARÇO DE 2006

FICHA CATALOGRÁFICA

OLIVEIRA, ALEX HELDER CORDEIRO DE
Gerenciamento de Túneis em Ambiente Integrado Mobile IP a MPLS [Distrito Federal] 2006.
15, 27p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2006). Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Mobile IP	2. Redes MPLS
3. MMPLS	4. Gerenciamento de Túneis
I. ENE/FT/UNB.	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

OLIVEIRA, A. H. C. (2006). Gerenciamento de Túneis em Ambiente Integrado Mobile IP a MPLS. Dissertação de Mestrado, Publicação PPGENE.DM-252A/06, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 27p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Alex Helder Cordeiro de Oliveira.
TÍTULO: Gerenciamento de Túneis em Ambiente Mobile IP Integrado a MPLS.

GRAU: Mestre ANO: 2006

_____

Alex Helder Cordeiro de Oliveira
SQS 215 Bloco G apt. 204.
CEP 70294-070 Brasília – DF - Brasil

DEDICATÓRIA

Dedico este trabalho aos meus pais e meu irmão, que sempre me apoiaram e incentivaram nos estudos e trabalhos necessários à minha formação profissional.

AGRADECIMENTOS

Agradeço primeiramente a Deus, que tornou possível a realização deste trabalho. Agradeço ao meu orientador, o professor Dr. Paulo Henrique Portela de Carvalho pela grande dedicação ao desenvolvimento deste trabalho. Agradeço também a meu pai, minha mãe e meu irmão pelo apoio dado para que eu realizasse este trabalho, me empenhando o máximo possível para desenvolver esta dissertação de mestrado.

Agradeço ainda à professora Dra. Cláudia Barrenco pelas sugestões dadas quanto à abordagem do tema, ao Msc. Georges Amvame que muito ajudou no estudo do *Mobile IP*, do MPLS e do NS-2. À Eng. Juliana Sombra, que foi a primeira pessoa a me mostrar a teoria da tecnologia Mobile IP. Ao Renato, Bruno e Breno, que ajudaram nos testes de desempenho que foram feitos, e que desenvolveram a ferramenta que foi utilizada nestes testes.

Agradeço também aos professores do Departamento de Engenharia Elétrica, e em especial ao professor Dr. Leonardo Rodrigues Araújo Xavier de Menezes pelo apoio e amizade.

Agradeço ainda aos colegas que freqüentaram o LABCOM ou o LEMOM, especialmente ao Msc. Marçal Chaiben, Msc. Carlos Tenório, Eng. Letícia Cardoso e aos que participaram do projeto Inova Mobile, pelas conversas enriquecedoras, ajuda em diversos aspectos, colaboração e amizade.

Agradeço ainda aos funcionários do departamento, em especial ao Fernando e à Cássia, que sempre ajudaram nos processos burocráticos, e ao apoio do CNPq, cuja bolsa em 2005 permitiu a dedicação exclusiva a este projeto. E a todos os meus amigos e colegas que direta, ou diretamente colaboraram com a realização deste trabalho.

A todos, meus sinceros agradecimentos.

RESUMO

GERENCIAMENTO DE TÚNEIS EM AMBIENTE MOBILE IP INTEGRADO A MPLS

Autor: Alex Helder Cordeiro de Oliveira

Orientador: Paulo Henrique Portela de Carvalho

Programa de Pós-graduação em Engenharia Elétrica

Brasília, março de 2006

Este trabalho tem como objetivo apresentar uma proposta de integração entre o Mobile IP e o MPLS de forma a garantir um roteamento mais eficiente e um bom desempenho nos procedimentos de *handoff*, visando a aplicação da tecnologia Mobile IP em redes contendo nós com razoável mobilidade e que deva oferecer determinado QoS a esses nós. São apresentadas, igualmente, uma descrição detalhada dos sistemas Mobile IP e MPLS, assim como diversas formas de implementação desses sistemas, que permitam a validação de determinadas funcionalidades e ajustes de parâmetros de desempenho.

A proposta desenvolvida neste trabalho fundamenta-se na definição de um protocolo de integração que realiza a substituição de túneis IP-em-IP próprios do Mobile IP por túneis LSP do MPLS, isto é, caminhos definidos por rótulos para um encaminhamento mais eficiente dos pacotes. Para a criação dos LSPs, os agentes do Mobile IP passam a gerar mensagens Path e Resv do RSVP, responsáveis pela criação e pela manutenção destes túneis, de acordo com a localização do nó móvel.

Além da substituição dos túneis, o protocolo proposto agrega ainda outras funcionalidades, que consistem na definição de hierarquia de agentes estrangeiros combinada com a otimização de roteamento, com pré-registo e *multicast* em ocasiões de *handoff*. O protocolo de integração proposto tem por finalidade reduzir a latência na troca de mensagens entre os nós móveis e seus respectivos correspondentes, tornando-se desnecessário o envio dos pacotes à rede nativa do nó móvel antes de eles serem encaminhadas ao destino, e permitindo que o processo de *handoff* seja o mais suave possível, permitindo que o registro possa ser validado nos agentes estrangeiros, e utilizando-se o *multicast* para garantir que os pacotes enviados ao nó móvel estejam disponíveis para ele quando o mesmo mudar de rede estrangeira.

ABSTRACT

TUNNELS MANAGEMENT IN MOBILE IP INTEGRATED MPLS ENVIRONMENT.

Author: Alex Helder Cordeiro de Oliveira

Supervisor: Paulo Henrique Portela de Carvalho

Programa de Pós-graduação em Engenharia Elétrica

Brasília, march of 2006

The goal of this work is show possible ways to implement a Mobile IP and MPLS integration, show the way it was decided to make it, expliciting the reasons to follow this way and show the result of the physical implementation and the theorical analyses of it. The achieve this goal, it is done the detailed explication of the Mobile IP and MPLS systems, it is showed many way of implementation of the integration, checking the advantages and disadvantages of each one, and only then it is detailed the implementation made in UnB.

The implementation done in the laboratory is basically made by the substitution of IP-in-IP tunnels of the mobile IP by the LSP tunnel, that is the way defined by labels to an efficient forward of packages. To make this LSP tunnels, the Mobile IP agents generate RSVP commands, which are responsible for the LSP creation in MPLS, when it is detected a changing of the mobile node position.

Beyond this basic integration, it is described in this work, a integration protocol with others features, that is basically foreign agents hierarchic combined with route optimization, and utilization of preregister and multicast during the handoffs. This protocol has the goal of reduce the latency of messages sent to the mobile node, make it unnecessary that the packets be sent to the home network from mobile node to be forwarded to him; and make the handoff as softer as possible, making the foreign agents able to validate the register and using multicast to assure that packets sent to de mobile node to be available for him when he moves from one foreign network to another.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

AP	*Access point* — Ponto de acesso.
ATM	*Assynchronous transfer mode* — Modo de transferência assíncrona
BGP	*Border gateway protocol* — Protocolo de gateway de borda
CN	*Correspondent node* — Nó correspondente
CoA	*Care-of address* — Endereço residente
DHCP	*Dynamic host configuration protocol* — Protocolo de configuração dinâmica de Servidor
FA	*Foreign agent* — Agente estrangeiro
FEC	*Forwarding equivalence class* — Classe de equivalência de encaminhamento
GFA	*Gateway foreign agent* — Agente estrangeiro *gateway*
GPL	*GNU general public license* — Licença pública geral GNU
GPS	*Global Positioning System* — Sistema de posicionamento global
HA	*Home agent* — Agente nativo
ICMP	*Internet control message protocol* — Protocolo de mensagem de controle da Internet
IETF	*Internet engineering task force* — Força-tarefa de engenharia da Internet
ILM	*Incoming label map* — Mapa de rótulos entrantes
IP	*Internet Protocol* — Protocolo de Internet
LAN	*Local area network* — Rede de área local
LDP	*Label distribution protocol* — Protocolo de distribuição de rótulos
LER	*Label edge router* — Roteador de bordas dos rótulos
LIB	*Label information base* — Base de informações de rótulos
LSP	*Label switched path* — Percurso comutado por rótulo
LSR	*Label switching router* — Roteador de comutação por rótulo
MIP	*Mobile IP* — IP móvel
MMPLS	*Mobile MPLS* — MPLS móvel
MN	*Mobile node* — Nó móvel
MPLS	*Multiprotocol label switching* — Multi-protocolo de comutação de rótulos
NAT	*Network address translation* — Tradução de endereços de rede
NS-2	*Network simulator* — Simulador de rede

OSPF	*Open shortest path first* — Caminho mais curto iniciado primeiro
QoS	*Quality of service* — Qualidade de serviço
RFA	*Regional foreign agent* — Agente estrangeiro regional
RFC	*Request for comments* — Chamada para comentários
RSVP	*Resource reservation protocol* — Protocolo de reserva de recursos
TCP	*Transmission control protocol* — Protocolo de controle de transmissão
UDP	*User datagram protocol* — Protocolo de datagrama de usuário
WAN	*Wide area network* — Redes de área ampla
W-LAN	*Wireless LAN* — Rede LAN sem fio

1 - INTRODUÇÃO

O aumento da utilização de redes de comunicação vem impulsionando o avanço na tecnologia utilizada nestas redes. Para um melhor roteamento de pacotes no *backbone* das redes, foi desenvolvido o protocolo MPLS (*Multi Protocol Label Switching*). Com o aumento da quantidade de tráfego, estes protocolos estão sendo implementados em pontos cada vez mais próximos à extremidade das redes.

Simultaneamente a isso, as redes sem fio estão se popularizando rapidamente, tornando necessários mecanismos que otimizem a transmissão de pacotes de um ponto a outro da rede e permitam que haja mobilidade sem que o usuário precise alterar constantemente suas configurações de rede. Para o problema relacionado à mobilidade, foi desenvolvido o *Mobile* IP (MIP), que se caracteriza por permitir que o usuário trafegue entre redes diferentes permanecendo com o mesmo endereço IP sem perder a capacidade de comunicação.

O MIP se baseia na utilização de agentes de mobilidade. Existem dois tipos de agentes de mobilidade no *Mobile* IP: agentes nativos, pertencentes à rede da qual o dispositivo móvel faz parte, e agentes estrangeiros, pertencentes às redes que o dispositivo móvel pode visitar. Quando o nó móvel se conecta a uma rede estrangeira, ele faz o registro, enviando ao agente estrangeiro algumas informações sobre si e sobre o seu agente nativo; o agente estrangeiro envia estas informações ao agente nativo e, se este agente aceitar o registro do nó móvel, enviará uma mensagem de resposta ao registro com um código que indica esta aceitação. A partir de então, toda mensagem que for enviada ao nó móvel, ao chegar à rede nativa, será capturada pelo agente nativo e enviada ao nó móvel através de um túnel IP-em-IP.

Existem dois problemas característicos do MIP. Um deles é o fato de que, quando o nó móvel se move de uma sub-rede para outra, ele precisa fazer um registro para que o agente nativo possa encaminhar pacotes ao nó móvel. Dependendo da distância do agente nativo à rede estrangeira na qual o nó móvel se encontra, o processo de registro pode demorar, fazendo com que o nó móvel esteja inacessível durante um período de tempo durante o *handoff*. Este período de tempo no qual o nó móvel está inacessível é chamado de “atraso

de *handoff*", que pode comprometer a implementação de determinados serviços inerentes às redes de comunicação.

O outro problema consiste no fato de que, quando o nó móvel está registrado em uma rede muito distante da sua rede nativa, os pacotes enviados a ele, por precisarem passar pela rede nativa do nó móvel, podem precisar percorrer um percurso muito maior do que o que seria necessário se eles fossem encaminhados diretamente da origem para o agente da rede estrangeira à qual o nó móvel está conectado. Este percurso maior causa deterioração em diversas características dos tráfegos direcionados ao nó móvel, que são o atraso no envio das mensagens, a variação de atraso, a perda de pacotes e a seqüência de chegada dos pacotes.

Para se minimizar o problema ocorrido no envio das mensagens ao nó móvel, vem-se propondo utilizar-se um núcleo MPLS com os agentes do *Mobile* IP nas bordas, obtendo-se assim resultados positivos no encaminhamento dos pacotes ao nó móvel. Os resultados, entretanto, podem ser ainda melhores se for feita uma integração entre os dois sistemas. Para isto, deve-se fazer com que os túneis criados com os rótulos do MPLS sejam gerenciados por informações de mobilidade do *Mobile* IP. A implementação desta integração, chamada MMPLS (*Mobile* MPLS), é o foco deste trabalho.

Existem diversas formas possíveis de se integrar estas tecnologias, tendo sido encontrada na bibliografia muitas integrações que variavam desde o protocolo de distribuição de rótulos às novas funcionalidades agregadas ao serviço. O protocolo de integração desenvolvido neste trabalho teve seu funcionamento básico da seguinte forma: quando um dispositivo móvel mudar de posição indo de uma rede para outra, ele deve fazer o registro da mesma forma que ele faz em uma rede *Mobile* IP simples, mas, após o registro, devem ser enviados pacotes Path e Resv, que são mensagens do RSVP que podem ser utilizadas para realizar a distribuição de rótulos MPLS entre os agentes, para estabelecer um túnel MPLS. Quando um elemento qualquer precisar se comunicar com o dispositivo móvel, este se comunicará com o agente responsável pela rede de origem do dispositivo, e este agente fará um redirecionamento que consiste em modificações na própria tabela de encaminhamento de rótulos MPLS.

O protocolo de integração desenvolvido neste trabalho envolve, além da substituição dos túneis IP-em-IP pelos túneis LSP, novos recursos, que buscam aumentar a eficiência do *Mobile* IP tanto no que diz respeito ao encaminhamento de pacotes ao nó móvel quanto no que diz respeito ao atraso de *handoff*. Estes recursos consistem em otimização de roteamento, *multicast* e pré-registro em um ambiente MIP hierárquico.

Para apresentar os resultados do trabalho realizado, esta dissertação foi estruturada em cinco capítulos. Após esta breve introdução, o segundo capítulo descreve com detalhes o *Mobile* IP, começando desde a motivação para a criação desta tecnologia, passando pela especificação do mesmo no IETF (*Internet engineering task force* — Força-tarefa de engenharia da Internet), detalhando a última RFC (*Request for comments* – Chamada para comentários) que especifica este sistema (RFC 3344), citando as implementações existentes, e apresentando as características do *Dynamics Mobile IP*, que foi utilizado neste projeto. Conterá também neste capítulo as informações sobre a forma de instalação, funcionamento básico e testes sobre o *Dynamics Mobile IP*.

O terceiro capítulo descreve o MPLS, partindo das suas motivações e objetivos, passando pelas especificações, características e funções que podem ser agregadas; detalhando o seu funcionamento e citando as implementações já encontradas e, em especial, a implementação utilizada no projeto. Também está apresentada, neste capítulo, a informação sobre a instalação e o teste de funcionamento do mesmo.

O capitulo quatro apresenta uma proposta de integração entre o *Mobile* IP e o MPLS, fundamentada por abordagens técnicas disponíveis na bibliografia, que objetivam a utilização integrada entre o *Mobile* IP e o MPLS. Após uma análise das vantagens e desvantagens dessas abordagens, mostrando compatibilidades entre diferentes possibilidades e as possibilidades ou problemas para realizar a implementação das mesmas, é apresentado o protocolo proposto neste trabalho, detalhando todos os processos realizados para o correto funcionamento da integração e das funcionalidades, e descrevendo as mensagens que são enviadas nestes processos. O capítulo traz, ainda, os resultados de uma implementação que consistiu na substituição do encapsulamento IP-em-IP por túneis LSP do MPLS.

Para encerrar, são apresentadas as conclusões deste trabalho assim como sugestões de futuros desenvolvimentos.

2 - MOBILE IP

A popularização dos computadores portáteis e a expansão das redes sem fio têm tornado crescente o desejo de muitos profissionais de poderem acessar os recursos disponíveis na rede de sua empresa em qualquer lugar e a qualquer momento. Considerando o fato de que a maior parte das empresas utiliza uma *intranet* com endereçamento privado não-roteável na Internet, *firewalls*, *gateways* com NAT, e opera com tecnologia IP básica [51], é muito difícil que um dispositivo móvel localizado em uma rede externa consiga acesso a todos os recursos específicos de sua rede de origem.

Uma proposta que permite este acesso é a tecnologia conhecida pelo nome Mobile IP [43], que pode ser traduzido com IP móvel. Esta tecnologia se baseia na utilização de agentes capazes de perceber onde o dispositivo móvel se encontra para poder redirecionar os pacotes gerados por ele ou endereçados a ele como se o dispositivo estivesse conectado diretamente na sua rede de origem.

Este capítulo descreve o sistema IP móvel, partindo das especificações criadas no IETF (*Internet engineering task force* — força-tarefa de engenharia da Internet) e analisando com detalhes a RFC (*request for comments* — chamada para comentários) mais recente sobre o suporte à mobilidade de IP para IPv4 [43]. O capítulo cita as implementações existentes e justifica a escolha do *Dynamics*, além de descrever o mesmo, apresentando informações sobre instalação e verificações a serem feitas para confirmar o seu correto funcionamento. O capítulo se encerra com análises realizadas a partir de simulações com o simulador de rede NS-2 (*Network Simulator version 2.0* — Simulador de Rede versão 2.0).

2.1 - SOBRE A ESPECIFICAÇÃO NO IETF

O IP móvel teve sua especificação desenvolvida por um grupo de trabalho do IETF [1, 2, 46]. O objetivo deste grupo foi desenvolver a especificação de um suporte a roteamento que permitisse a dispositivos IP usando IPv4 ou IPv6 fazer *roaming* em diferentes sub-redes ou meios de transmissão, desde que as diferenças nos meios de transmissão sejam transparentes para as camadas de rede acima da camada IP, incluindo manutenção de

conexões TCP ativas e ligações de porta UDP. Em julho de 2003, esse grupo de trabalho se dividiu em três outros grupos: mip4 (*Mobility for IPv4*), mip6 (*Mobility for IPv6*) e mipshop (*MIPv6 Signaling and Handoff Optimization*) [1, 47]. Esta divisão faz com que as especificações assumam um caráter mais especializado; por exemplo, se o grupo de trabalho do mip4 estiver desenvolvendo uma especificação, não há necessidade de se preocupar que esta especificação também seja válida para as redes de IPv6; entretanto, isso não impede que as especificações produzidas por um grupo de trabalho funcionem com a tecnologia trabalhada no outro grupo.

Desde outubro de 1996, já foram publicadas 23 RFCs. O suporte a IP móvel em dispositivos que utilizam IPv4 foi inicialmente especificado na RFC 2002 e revisado na RFC 3220 e, então, revisado na RFC 3344 de agosto de 2002. Esta especificação define os agentes necessários, a forma de comunicação entre eles e processos realizados que permitam ao dispositivo utilizar permanentemente seu endereço de rede e mover-se pela Internet sem perda de conexão. As outras RFCs sobre este sistema são extensões do Mobile IP para tecnologias específicas, segurança e detalhes sobre processos fundamentais para funcionamento do IP móvel. A tabela 2.1 apresenta as RFCs publicadas sobre o Mobile IP, ordenada por data de publicação em ordem decrescente.

Tabela 2.1 - Especificações sobre Mobile IP [1]

Número	**Título**	**Autor**	**Data**	**Substituído por**
RFC4093	*Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways*	F. Adrangi, H. Levkowetz	08/2005	
RFC4064	*Experimental Message, Extensions, and Error Codes for Mobile IPv4*	A. Patel, K. Leung	05/2005	
RFC3957	*Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4*	C. Perkins, P. Calhoun	03/2005	
Número	**Título**	**Autor**	**Data**	**Substituído por**

RFC3846	*Mobile IPv4 Extension for Carrying Network Access Identifiers*	F. Johansson, T. Johansson	06/2004	
RFC3776	*Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents*	J. Arkko, V. Devarapalli, F. Dupont	06/2004	
RFC3583	*Requirements of a Quality of Service (QoS) Solution for Mobile IP*	H. Chaskar, Ed.	09/2003	
RFC3543	*Registration Revocation in Mobile IPv4*	S. Glass, M. Chandra	08/2003	
RFC3519	*Mobile IP Traversal of Network Address Translation (NAT) Devices*	H. Levkowetz, S. Vaarala	05/2003	
RFC3344	*IP Mobility Support for IPv4*	C. Perkins, Ed.	08/2002	
RFC3220	*IP Mobility Support for IPv4*	C. Perkins, Ed.	01/2002	RFC3344
RFC3154	*Requirements and Functional Architecture for an IP Host Alerting Protocol*	J. Kempf, C. Castelluccia, P. Mutaf, N. Nakajima, Y. Ohba, R. Ramjee, Y. Saifullah, B. Sarikaya, X. Xu	08/2001	
RFC3115	*Mobile IP Vendor/Organization-Specific Extensions*	G. Dommety, K. Leung	04/2001	
RFC3025	*Mobile IP Vendor/Organization-Specific Extensions*	G. Dommety, K. Leung	02/2001	RFC3115
RFC3024	*Reverse Tunneling for Mobile IP, revised*	G. Montenegro, Ed.	01/2001	
RFC3012	*Mobile IPv4 Challenge/Response Extensions*	C. Perkins, P. Calhoun	11/2000	
Número	**Título**	**Autor**	**Data**	**Substituído por**

RFC2977	*Mobile IP Authentication, Authorization, and Accounting Requirements*	S. Glass, T. Hiller, S. Jacobs, C. Perkins	10/2000	
RFC2794	*Mobile IP Network Access Identifier Extension for IPv4*	P. Calhoun, C. Perkins	03/2000	
RFC2356	*Sun's SKIP Firewall Traversal for Mobile IP*	G. Montenegro, V. Gupta	06/1998	
RFC2344	*Reverse Tunneling for Mobile IP*	G. Montenegro, Ed.	05/1998	RFC3024
RFC2290	*Mobile-IPv4 Configuration Option for PPP IPCP*	J. Solomon, S. Glass	02/1998	
RFC2041	*Mobile Network Tracing*	B. Noble, G. Nguyen, M. Satyanarayanan, R. Katz	10/1996	
RFC2006	*The Definitions of Managed Objects for IP Mobility Support using SMIv2*	D. Cong, M. Hamlen, C. Perkins	10/1996	
RFC2002	*IP Mobility Support*	C. Perkins, Ed.	10/1996	RFC3220

A seguir, será detalhado sobre a atual especificação do Mobile IP para IPv4, a RFC 3344, por que é a partir dela que foram feitos as atuais implementações deste sistema, e sobre ela será feito o estudo necessário para realizar este trabalho.

2.2 - RFC 3344

Para compreender o IP móvel, deve-se considerar uma estrutura que envolve duas redes distintas, sendo uma a rede natural do dispositivo móvel e a outra, uma rede distinta, tendo, cada uma, um endereçamento de rede diferente. A rede à qual o dispositivo móvel pertence será chamada de rede nativa (na especificação é chamada *home network*) e a rede externa a partir da qual ele se conectará será chamada de rede estrangeira (*foreign network* na especificação). Em ambas as redes, deve haver pelo menos um agente capaz de verificar a presença do dispositivo móvel na rede, e capaz de manter ativa a conexão do dispositivo; o agente da rede nativa é conhecido como agente nativo (*home agent* — HA) e o da rede

estrangeira é conhecido como agente estrangeiro (*foreign agent* — FA). O outro elemento necessário é o nó móvel (*mobile node* — MN), que é o dispositivo móvel que pode se encontrar conectado fisicamente em qualquer das duas redes. A fig 2.1 apresenta o modelo da estrutura descrita acima.

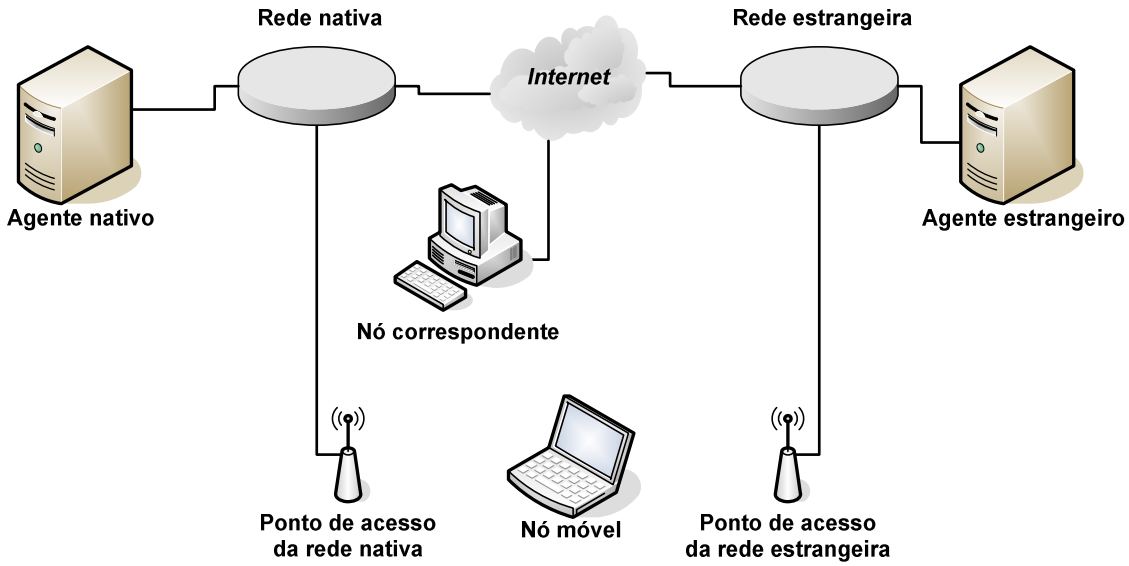


Figura 2.1 - Estrutura de uma rede que implementa Mobile IP.

No modelo de estrutura da fig. 2.1, têm-se ainda três elementos que não são obrigatórios, mas são comuns a esta estrutura: pontos de acesso (*access points*) em cada rede e o nó correspondente (*correspondent node*). O nó correspondente na verdade é algum dispositivo que pode ser acessado ou que pode acessar o nó móvel. Com relação aos pontos de acesso, eles são muito comuns nesta estrutura porque a motivação da criação desta tecnologia é a mobilidade, e a W-LAN está sendo uma plataforma de grande sucesso no que diz respeito à mobilidade; apesar disto, este sistema pode ser implementado em uma rede *ethernet* comum (IEEE 802.3). A diferença entre utilizar W-LAN e a rede *ethernet* nesta estrutura ocorre apenas como sendo a necessidade de o usuário conectar fisicamente o cabo de rede em seu dispositivo quando estiver se conectando em uma rede ethernet, pois com a W-LAN isto não é necessário.

Os agentes são o fundamento do IP móvel. Basicamente, seu funcionamento é o seguinte: se o dispositivo móvel com o nó móvel se conectar na rede nativa, ele se autentica diretamente no agente nativo e utiliza os recursos de rede normalmente; caso ele se conecte fisicamente na rede estrangeira, o agente estrangeiro identifica os dados referentes ao

dispositivo móvel e sua rede nativa para, a partir destas informações, entrar em contato com o agente nativo; ao se comunicar com o agente nativo, o agente estrangeiro faz a autenticação do nó móvel; se a autenticação for bem sucedida, os agentes iniciam um tunelamento entre si; os pacotes que forem endereçados ao nó móvel, ao chegar na rede nativa, serão capturados pelo agente nativo e enviados pelo túnel até o agente estrangeiro, que os envia ao nó móvel; os pacotes gerados pelo nó móvel são enviados ao agente estrangeiro, que pode enviá-los ao destino seguindo as regras comuns de TCP/IP (tunelamento triangular) ou enviar ao agente nativo (tunelamento reverso), para que este envie os pacotes a seus respectivos destinos [43]. A diferença entre estas duas formas de encaminhar as mensagens vindas do nó móvel reside no fato de que, através do tunelamento triangular, um pacote chega ao destino com um atraso menor que através do tunelamento reverso, mas em algumas redes, pode haver roteadores que descartem pacotes com endereço de origem diferente do esperado, levando o tunelamento reverso a ser mais recomendável para estes casos.

Nas seções seguintes, serão descritos os procedimentos mais importantes realizados pelo *Mobile IP*: descoberta de agentes, registro e roteamento de mensagens.

2.2.1 - Descoberta de agentes

Para que o dispositivo móvel identifique em qual rede ele se encontra e para que os agentes percebam que o dispositivo se conectou à sua rede, são utilizadas mensagens de anúncio de agentes e solicitação de agente (*agent advertisement* e *agent solicitation*, respectivamente). Este método também permite ao nó móvel determinar o endereço residente oferecido pelo agente estrangeiro. O endereço residente (*care-of address* — CoA) é o endereço IP que indica em que rede o agente nativo encontrará o nó móvel, isto é, após o registro do nó móvel, o agente nativo fará o túnel IP-em-IP (IP-in-IP) com este endereço para enviar as informações destinadas ao MN.

Duas configurações são possíveis para a descoberta dos agentes. Uma delas, a mais comum, se faz pelo envio periódico de anúncios de agentes no enlace por parte dos agentes; assim, quando o nó móvel entrar na área de cobertura da rede, ele logo receberá um anúncio, indicando em que rede ele se encontra e quais os endereços residentes disponíveis.

A outra possibilidade é configurar os agentes para enviar o anúncio somente após receber uma solicitação de agente por parte do nó móvel. Nesta situação, o nó móvel, ao perder conexão com a rede, passa a enviar solicitações de agente até receber um anúncio, indicando que ele entrou em uma rede que tenha suporte a IP móvel.

O anúncio de agente é uma variação da mensagem anúncio de roteador ICMP (ICMP *Router Advertisement*) descrita na RFC 1256 [22], que inclui uma extensão de anúncio de agente móvel (*Mobile Agent Advertisement*). A fig. 2.2 apresenta o formato desta mensagem; a região apresentada em amarelo é a parte da mensagem que faz parte do anúncio de roteador ICMP; a extensão referente ao anúncio de agente móvel é a região em verde.

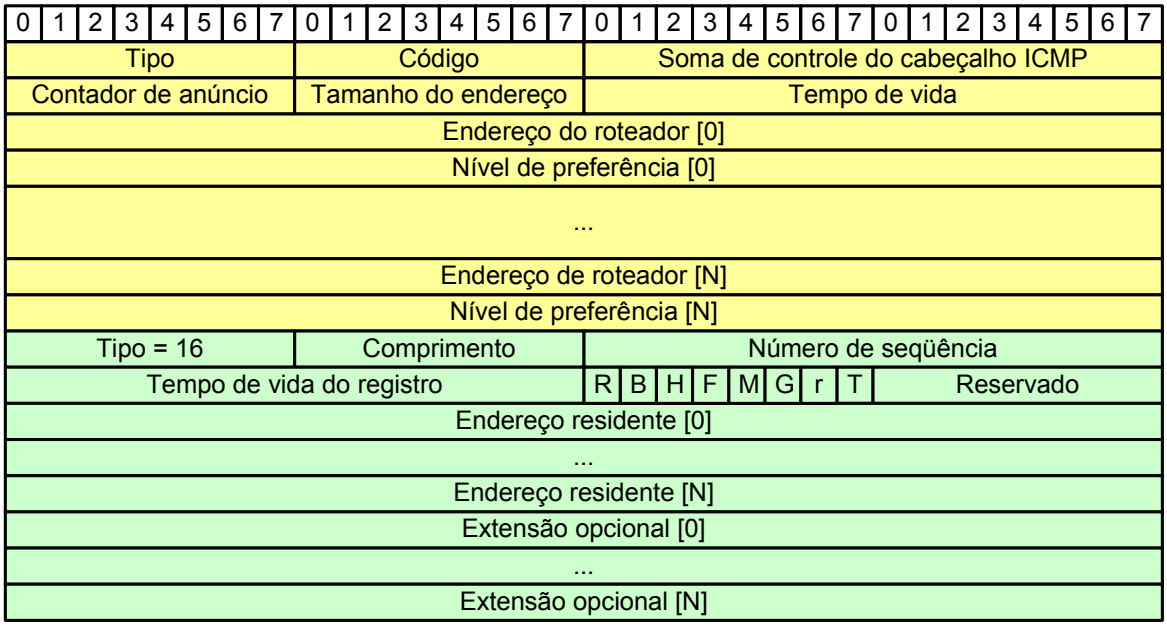


Figura 2.2 - Formato de mensagens de anúncio de agente móvel

Nesta mensagem, têm-se os seguintes elementos:

- **Tipo (ICMP):** 1 *byte* que deve ter valor 9 para que o dispositivo que o receba identifique que tipo de mensagem está recebendo;
- **Código:** 1 *byte* que deve ter valor 0 para indicar que é um anúncio de roteador normal ou valor 16, caso o roteador não faça roteamento de tráfego normal;
- **Soma de controle do cabeçalho ICMP:** 2 *bytes* utilizados para controle de erros;
- **Contador de anúncio:** 1 *byte* indicando a quantidade de anúncios de roteadores

(pares endereço de roteador / nível de preferência) contidas na mensagem;

- **Tamanho do endereço:** 1 *byte* com o número de palavras de 32 *bits* utilizadas para o endereçamento dos roteadores; normalmente tem valor 2 (endereço de roteador + nível de preferência);
- **Tempo de vida:** 2 *bytes* indicando o tempo máximo em segundos no qual os endereços dos roteadores na lista podem ser considerados válidos;
- **Endereço de roteador:** 4 *bytes* com o endereço IP do roteador anunciado;
- **Nível de preferência:** 4 *bytes* indicando o nível de preferência deste roteador com relação a outro roteador da mesma sub-rede;
- **Tipo (anúncio de agente móvel):** 1 *byte* com valor 16;
- **Comprimento:** 1 *byte* com valor $6 + 4 \times N$, onde N é a quantidade de endereços residentes anunciados;
- **Número de seqüência:** 1 *byte* com a quantidade de anúncios enviados desde a inicialização do agente.
- **Tempo de vida do registro:** 2 *bytes* com o tempo máximo, medido em segundos, em que este agente estará disponível para receber alguma requisição de registro. O valor 0xFFFF indica infinito. Este campo não tem nenhuma relação com o campo tempo de vida da parte original do anúncio de roteador ICMP da mensagem.
- **R:** 1 *bit* que indica que o registro neste agente estrangeiro (ou qualquer outro no enlace onde este anúncio está sendo transmitido) é necessário, mesmo quando está sendo utilizando um endereço residente obtido externamente (por meio de DHCP, por exemplo).
- **B:** 1 *bit* que indica se o agente estrangeiro está ocupado e não aceitará registros de nós móveis adicionais.
- **H:** 1 *bit* que indica se este agente oferece serviço de agente nativo no enlace no qual esta mensagem está sendo enviada.
- **F:** 1 *bit* que indica se este agente oferece serviço como agente estrangeiro no enlace sobre o qual este anúncio está sendo enviado.
- **M:** 1 *bit* que indica se este agente implementa recebimento de datagramas em túneis que usam o encapsulamento mínimo descrito na RFC 2004.
- **G:** 1 *bit* que indica se este agente implementa o recebimento de datagramas em túneis que usam encapsulamento GRE descrito na RFC 1701.
- **r:** 1 *bit* que é enviado como 0; ele é ignorado na recepção e não deve ser alocado

para nenhum uso.

- **T:** 1 *bit* que indica se o agente estrangeiro está configurado para realizar tunelamento reverso.
- **Reservado:** 1 byte enviado com zero que é ignorado na recepção.
- **Endereço residente:** Um anúncio de agente deve conter pelo menos um endereço residente se o *bit* F estiver marcado. A quantidade de endereços residentes presentes nesta mensagem é determinada pelo campo comprimento.

A especificação define as seguintes regras: um agente nativo deve sempre estar preparado para atender ao nó móvel que faz parte da sua rede; um agente estrangeiro pode estar ocupado demais para atender novos MNs que entrem em sua rede, apesar disso ele continua a enviar anúncios para que os nós móveis já registrados não percam a comunicação, pois se o tempo de vida do registro expirar e ele não enviar novo registro os agentes param de encaminhar o tráfego para o nó móvel, e para enviar requisições de registro, o nó móvel precisa receber anúncios de agente. A partir dessas regras a especificação define as seguintes conclusões sobre a marcação dos *bits* de controle: um agente nunca deve marcar o *bit* B se o F não estiver marcado, porque para estar ocupado (*bit* B), o agente precisa obrigatoriamente estar oferecendo serviço de agente estrangeiro (*bit* F); além disso, ou o *bit* F ou o H precisa estar marcado em uma mensagem de anúncio, pois os anúncios do IP móvel estão associados a algum tipo de agente, logo ou se tem o *bit* H marcado, indicando serviço de agente nativo ativo, ou o *bit* F marcado, indicando serviço de agente estrangeiro; um agente nunca deve marcar o *bit* R se o *bit* F não estiver marcado, pois para definir a necessidade de registro no dispositivo sob caráter de agente estrangeiro (*bit* R marcado) é necessário que ele ofereça serviço de agente estrangeiro (*bit* F marcado).

As extensões opcionais podem ser extensões de comprimento de prefixo, extensões de *byte* de enchimento ou alguma outra extensão que pode vir a ser definida no futuro. A extensão de comprimento de prefixo é utilizada para indicar a quantidade de *bits* do prefixo da rede de cada endereço de roteador listado na parte anúncio de roteador ICMP do anúncio de agente. Em outras palavras, o tamanho do prefixo define quantos bits do endereço IP são utilizados para indentificar a rede e quantos são utilizados para identificar o dispositivo dentro desta rede, identificando assim a máscara da rede. Seu formato segue o modelo apresentado na fig. 2.3.

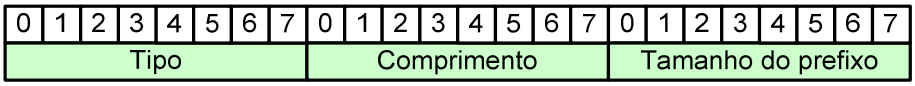


Figura 2.3 - Extensão de comprimento de prefixo.

Nesta extensão, temos os seguintes elementos:

- **Tipo:** 1 *byte* com valor 19 para indicar que se trata de uma extensão de comprimento de prefixo.
- **Comprimento:** 1 *byte* com o valor do campo contador de anúncio da parte anúncio de roteador ICMP.
- **Tamanho do prefixo:** É o número de *bits* que define o endereço da rede do respectivo endereço de roteador listado na mensagem, isto é, a máscara da rede. O comprimento de prefixo de cada endereço de roteador é armazenado como um *byte* separado na mesma ordem dos endereços dos roteadores.

As extensões de *byte* de enchimento podem ser utilizadas para transformar um comprimento impar de um anúncio de agente em um comprimento par. A motivação para a existência desta extensão se faz pelo fato de algumas implementações do protocolo IP insistirem em realizar enchimento de mensagens ICMP para obter sempre uma quantidade par de bytes.

O formato desta extensão é um único byte todo preenchido com 0, tal como apresentado na fig.2.4.

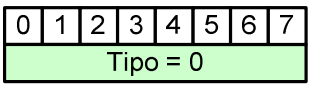


Figura 2.4 - Extensão de byte de enchimento.

Outro fator importante na criação de mensagens de anúncio é que o TTL (tempo de vida) do cabeçalho IP deve estar com valor 1. O endereço de destino, também do cabeçalho IP, tal como descrito na RFC 1256, deve ser 244.0.0.1, o que indica todos os elementos do enlace *multicast*, ou 255.255.255.255, que é o endereço de *broadcast* limitado. O endereçamento de *broadcast* limitado significa que este *broadcast* tem como alvo todas as máquinas de todos os enlaces que receberem esta mensagem, ressaltando que este pacote

se limitará ao *broadcast* na rede, isto é, ele não será roteado na Internet. Não deve ser utilizado o *broadcast* de sub-rede porque se este fosse utilizado, o nó móvel não reconheceria o prefixo da rede estrangeira, pois a camada IP da interface de rede não captura pacotes que tenham prefixo de rede diferente do prefixo da própria interface.

A solicitação de agente é uma mensagem idêntica à solicitação de roteador ICMP, também definido na RFC 1256 [22]; sua única diferença se faz no cabeçalho IP, no qual ela deve ter os campos tempo de vida com valor 1 e o endereço de destino, assim como o do anúncio de agente deve ser 255.255.255.255 ou 224.0.0.1. O motivo pelo qual são utilizados estes endereços é o mesmo pelo qual é utilizado no anúncio de agentes: possibilitar que os agentes identifiquem e recebam as mensagens. A fig. 2.5 apresenta o formato desta mensagem.

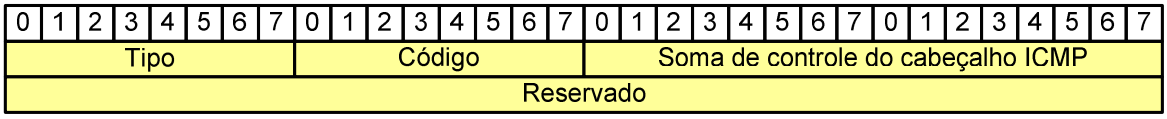


Figura 2.5 - Formato da mensagem de solicitação de agente móvel e solicitação de roteador ICMP.

Nesta mensagem, os elementos são:

- **Tipo:** 1 *byte* com valor 10.
- **Código:** 1 *byte* com valor 0.
- **Soma de controle do cabeçalho ICMP:** 2 *bytes* utilizados para controle de erros.
- **Reservado:** 4 *bytes* com valor 0.

2.2.2 - Registro

Após a identificação da rede e de seu agente por parte do nó móvel, inicia-se o processo de registro do dispositivo móvel, que é o mecanismo pelo qual o MN informa ao seu agente nativo sobre como alcançá-lo. Este processo é utilizado, essencialmente em 4 situações diferentes:

- Solicitar ao agente nativo o encaminhamento de serviços quando está em outra rede;
- Informar ao HA sobre o seu atual endereço residente;
- Renovar registros que estão prestes a expirar;

- Encerrar o registro na rede estrangeira ao voltar à rede nativa.

O processo de registro utiliza-se das mensagens de requisição de registro e resposta de registro. Existem dois tipos de registro diferentes: registro direto no agente nativo e registro por meio do agente estrangeiro. O registro direto no agente nativo ocorre quando o móvel está em sua própria rede, não precisando portanto passar por nenhum agente estrangeiro. O registro por meio de agente estrangeiro ocorre quando o nó móvel está conectado em uma rede estrangeira, e nesta situação ele precisa de um agente estrangeiro que possa encaminhar a sua requisição de registro ao agente nativo.

O registro direto no agente nativo é formado por dois passos, como ilustrado na fig. 2.6:

- O nó móvel envia a requisição de registro ao agente nativo;
- O agente nativo responde a requisição com uma resposta de registro permitindo ou negando a solicitação.

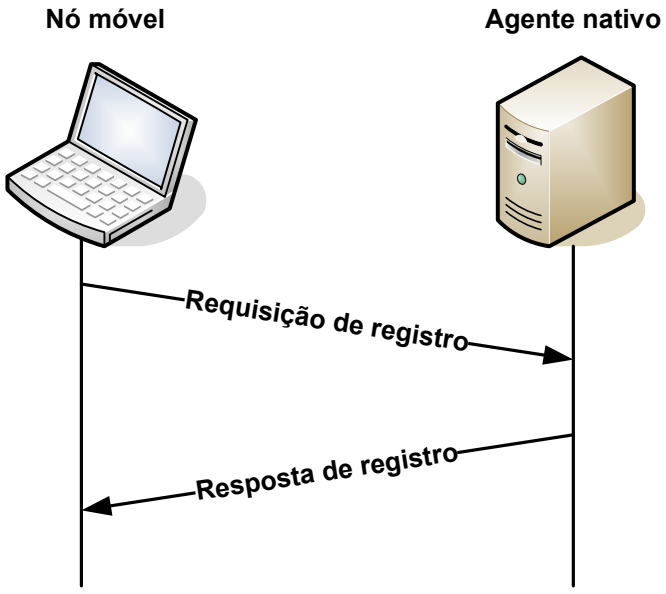


Figura 2.6 - Registro do nó móvel diretamente no agente nativo.

O registro por meio do agente estrangeiro é composto por quatro passos, conforme ilustrado na fig. 2.7:

- O MN envia uma requisição de registro para o agente estrangeiro;
- O FA processa as informações da requisição para, a partir destas informações, redirecionar corretamente esta requisição ao agente nativo;

- O agente nativo envia uma resposta de registro ao agente estrangeiro para permitir ou negar a solicitação;
- O FA processa a resposta e então o redireciona ao nó móvel para informá-lo sobre o resultado da solicitação.

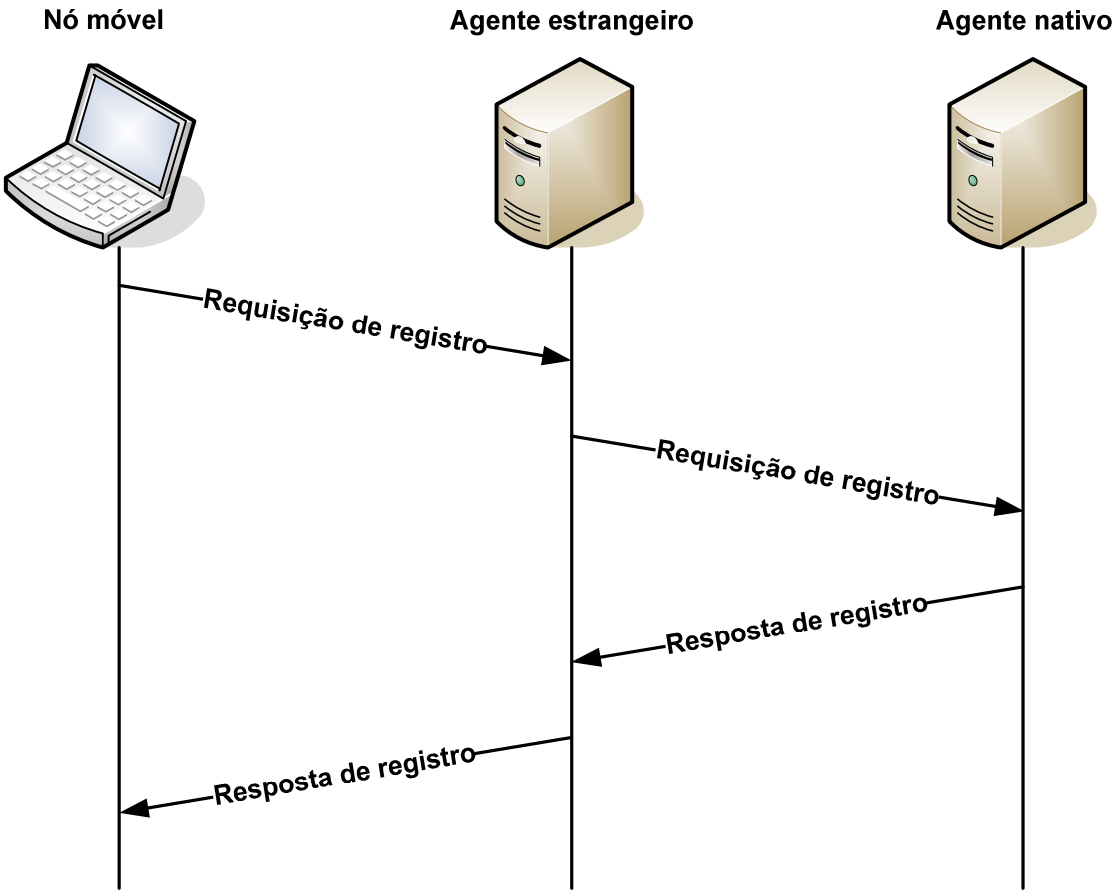


Figura 2.7 - Registro do nó móvel por meio do agente estrangeiro.

A mensagem de requisição de registro é um pacote UDP endereçado à porta 434 do agente nativo ou estrangeiro. Apesar de ser especificada a porta de destino, a porta de origem não é definida, podendo assumir qualquer porta desejada. Isto se faz porque é necessário que o agente esteja escutando uma porta específica, o que torna a padronização da porta de destino obrigatória, mas não há nenhum fator que torne obrigatória a utilização de uma porta específica para o envio, assim sendo, a especificação não define a porta de origem, deixando que cada desenvolvedor escolha uma porta para a sua implementação de forma livre e arbitraria. O formato da mensagem após o cabeçalho UDP é indicado na fig. 2.8.

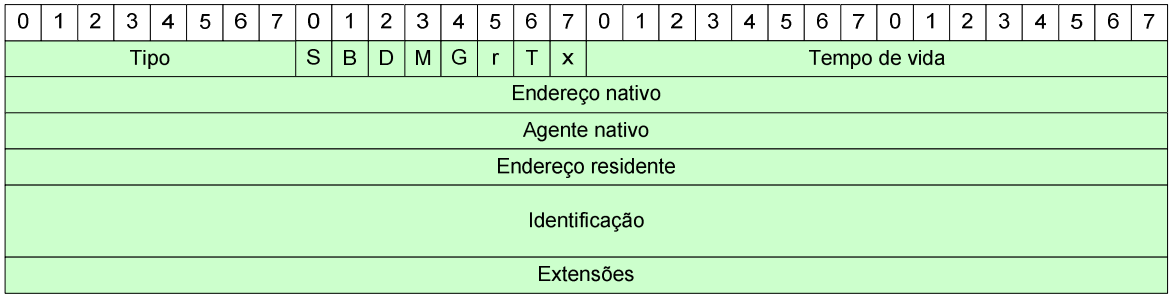


Figura 2.8 - Formato da mensagem requisição de registro.

Nesta mensagem, têm-se os seguintes campos:

- **Tipo:** 1 *byte* com valor 1.
- **S:** 1 *bit* que indica se o nó móvel está solicitando que o agente nativo mantenha a ligação anterior.
- **B:** 1 *bit* que indica se o nó móvel está solicitando que o agente nativo envie todos os datagramas em *broadcast* para ele por meio do túnel.
- **D:** 1 *bit* que indica se o desencapsulamento dos datagramas deve ser feito no próprio nó móvel.
- **M:** 1 *bit* que indica se o MN está solicitando que o agente nativo utilize encapsulamento mínimo.
- **G:** 1 *bit* que indica se o nó móvel está solicitando ao agente nativo que utilize encapsulamento GRE.
- **r:** 1 *bit* enviado como zero que é ignorado na recepção. Não deve ser alocado para uso nenhum.
- **T:** 1 *bit* que indica se o nó móvel está solicitando o tunelamento reverso.
- **x:** 1 *bit* que é enviado como zero e ignorado na recepção.
- **Tempo de vida:** 2 *bytes* com o tempo restante medido em segundos antes que o registro seja considerado expirado. Valor zero indica uma solicitação por encerramento de registro. Valor 0xFFFF indica tempo infinito.
- **Endereço nativo:** 4 *bytes* com o endereço IP do nó móvel.
- **Agente nativo:** 4 *bytes* com o endereço IP do agente nativo da rede a qual o nó móvel pertence.
- **Endereço residente:** 4 *bytes* com o endereço IP do fim do túnel utilizado para enviar pacotes ao MN.
- **Identificação:** 8 bytes utilizados para comparar a requisição de registro com a resposta de registro e proteger contra ataques de respostas às mensagens de registro.

- **Extensões:** A parte fixa da requisição de registro é seguida por uma ou mais extensões. As extensões possíveis de serem adicionadas à mensagem são:
    - **Extensão de Valor Calculado de Autenticação:** Deve proteger o conteúdo do pacote UDP, todas as extensões anteriores, o tipo, comprimento e SPI (Índice de Parâmetros de Segurança) da mensagem.
    - **Extensão de Autenticação do Móvel em Casa:** Utilizado para eliminar problemas de segurança referentes a TCP/IP.
    - **Extensão de Autenticação do Móvel na rede Estrangeira:** Utilizado em caso de associação de segurança entre o nó móvel e o agente estrangeiro.
    - **Extensão de Autenticação da Rede Estrangeira na rede Móvel:** Pode ser incluído a mensagens de registro caso exista alguma associação de segurança de mobilidade entre o agente estrangeiro e o nativo.

A mensagem resposta de registro, assim como a requisição de registro, é um pacote UDP. Este pacote é enviado como resposta à requisição e contém toda a informação necessária para informar ao nó móvel sobre a situação de sua solicitação de registro. A porta de origem desta mensagem UDP é variável, e a porta de destino é copiada da porta de origem da mensagem de requisição à qual esta resposta corresponde. O formato da mensagem após o cabeçalho UDP é indicado na fig. 2.9.

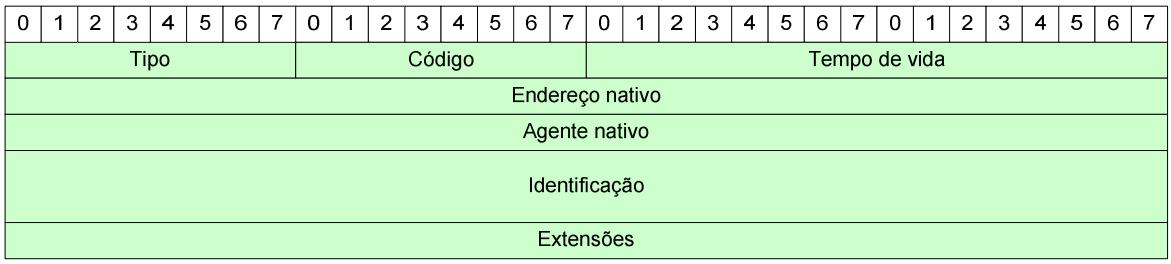


Figura 2.9 - Formato da mensagem de resposta de registro.

Os seguintes campos fazem parte desta mensagem:

- **Tipo:** 1 *byte* com valor 3 indicando que é uma mensagem de resposta de registro.
- **Código:** 1 *byte* que indica o resultado do registro. Os valores de código definidos podem ser encontrados na tabela 2.2.
- **Tempo de vida:** 2 *bytes*. Caso o campo código indique que o registro foi aceito, o campo tempo de vida indicará a quantidade de tempo em segundos que ainda resta

antes que o registro expire. Valor 0 indica que o registro do móvel expirou e valor 0xFFFF indica tempo infinito. Caso o campo código indique que o registro foi negado, o tempo de vida é então desconsiderado.

- **Endereço nativo:** 4 *bytes* com o endereço IP do nó móvel.
- **Agente nativo:** 4 *bytes* com o endereço IP do agente nativo.
- **Identificação:** 8 *bytes* utilizados para comparar requisições de registro com respostas de registros de forma a proteger contra ataque de respostas a mensagens de registro. Valor baseado no campo identificação da mensagem de requisição de registro e no tipo de proteção utilizada no contexto de segurança entre o nó móvel e seu agente nativo.
- **Extensões:** A parte fixa da resposta de registro é seguida por uma ou mais extensões. A resposta de registro utiliza as mesmas extensões da requisição de registro: Extensão de Valor Calculado de Autenticação, Extensão de Autenticação do Móvel em Casa, Extensão de Autenticação do Móvel na rede Estrangeira e Extensão de Autenticação da Rede Estrangeira na rede Móvel.

Tabela 2.2 - Códigos da Resposta de Registro [43]

Registro bem sucedido:	
Código	**Resposta**
0	Registro aceito.
1	Registro aceito, mas sem suporte à *binding* de mobilidade simultâneo.
Registro negado pelo agente estrangeiro:	
Código	**Resposta**
64	Razão não-especificada
65	Proibido administrativamente
66	Recursos insuficientes
67	Autenticação falhou no nó móvel
68	Autenticação falhou no agente nativo
69	Tempo de vida solicitado muito grande

70	Requisição mal-formada
71	Resposta mal-formada
72	Encapsulamento pedido indisponível
73	Reservado e indisponível
77	Endereço residente inválido
78	Tempo do registro expirado
80	Rede nativa inalcançável (erro de ICMP recebido)
81	*Host* agente nativo inalcançável (erro de ICMP recebido)
82	Porta do agente nativo inalcançável (erro de ICMP recebido)
88	Agente nativo inalcançável (erro de ICMP recebido)
Registro negado pelo agente nativo:	
Código	**Resposta**
128	Razão não-especificada
129	Proibido administrativamente
130	Recursos insuficientes
131	Autenticação falhou no nó móvel
132	Autenticação falhou no agente estrangeiro
133	identificação de registro não-compatível
134	Requisição mal-formada
135	muitos *binding* de mobilidade simultâneos
136	Endereço do agente nativo desconhecido

Apesar de importante no que diz respeito à segurança da rede, e fundamental para o encaminhamento dos pacotes do IP móvel, o registro é uma fonte de atraso durante o *handoff* do nó móvel. Quando o nó móvel se move de uma área de cobertura para outra, mesmo que ele não tenha área sem cobertura entre a área das duas redes, quando ele se

desconectar da primeira rede, ainda levará um certo tempo até que ele tenha conexão novamente. Este tempo consiste no período gasto até que o nó móvel receba um anúncio de agente da nova rede somado ao tempo gasto no encaminhamento da requisição de registro até o agente nativo e o tempo gasto com o encaminhamento da resposta de registro enviado pelo agente nativo. Conclui-se que quanto mais distante o agente nativo estiver da atual localização do nó móvel, maior será o tempo no qual o nó móvel estará sem conexão durante o *handoff*.

Para solucionar este problema, um dos mecanismos mais aceitos é a utilização do registro regional, que resulta na implementação de uma rede com IP móvel hierárquico. Este mecanismo é utilizado para o que é conhecido pelo nome de micromobilidade, que consistem em criar domínios e autenticar o dispositivo móvel dentro deste domínio e gerenciar a mobilidade do dispositivo dentro de subredes deste domínio. O Mobile IP hierárquico está descrito na seção 2.3 deste trabalho.

2.2.3 - Roteamento

Caso o dispositivo móvel receba permissão para utilizar os recursos da rede no processo de registro, se o móvel estiver na rede nativa, sua comunicação ocorrerá da mesma forma que ocorreria se não houvesse o IP móvel de forma a não haver redução no desempenho de sua comunicação, mas caso ele esteja em uma rede estrangeira, ele se comunicará através de um túnel, que permitirá a ele se comunicar como se estivesse na própria rede.

Caso o móvel esteja utilizando um endereço residente de origem externa, isto é, ele já tenha um endereço reservado para ele utilizar como endereço residente na rede estrangeira onde ele se conectou ou caso ele tenha obtido um endereço residente disponibilizado por DHCP, por exemplo, então o túnel será feito entre ele e o agente nativo; e ele utilizará algum dos agentes estrangeiros, encontrado através do processo de descoberta de agentes, como roteador ao qual ele deve encaminhar os pacotes tunelados. A outra possibilidade é a utilização de um endereço residente disponibilizado pelo agente estrangeiro, que muitas vezes é o próprio endereço IP do agente. Nesta situação, o túnel será realizado entre o agente nativo e o agente estrangeiro; e o FA, após receber os pacotes tunelados, os desencapsulará e os enviará ao respectivo nó móvel.

O método de tunelamento padrão para o IP móvel é o encapsulamento IP-em-IP descrito na RFC 2003 [42], mas a especificação também prevê a utilização do encapsulamento mínimo da RFC 2004 e o encapsulamento GRE (encapsulamento para roteamento genérico) da RFC 1701.

O tunelamento IP-em-IP consiste em acrescentar um novo cabeçalho IP que permita ao pacote chegar até um destino que não seria alcançado usando apenas o cabeçalho IP original. O processo de envio de um pacote em um ambiente com túnel ocorre da seguinte forma: um elemento gera um pacote que deve ser enviado até um destino que não é alcançável com o cabeçalho IP deste pacote. A extremidade do túnel, ao receber o pacote, o encapsula através do acréscimo de um novo cabeçalho IP que pode ser roteado até a outra extremidade do túnel, a partir da qual é possível chegar ao destino com o cabeçalho original. Ao chegar na outra extremidade do túnel, o pacote é desencapsulado, isto é, o cabeçalho IP colocado na primeira extremidade do túnel é retirado e o pacote então volta a ser roteado a partir das informações do cabeçalho IP original e desta forma chega ao seu destino. Uma ilustração deste processo é apresentado na fig. 2.10.

O encapsulamento descrito na especificação RFC 2003 foi criado justamente por causa do Mobile IP, mas ainda pode ser utilizado para outras finalidades, tais como m*ulticast*, escolha de rotas específicas e políticas de roteamento, entre outros.

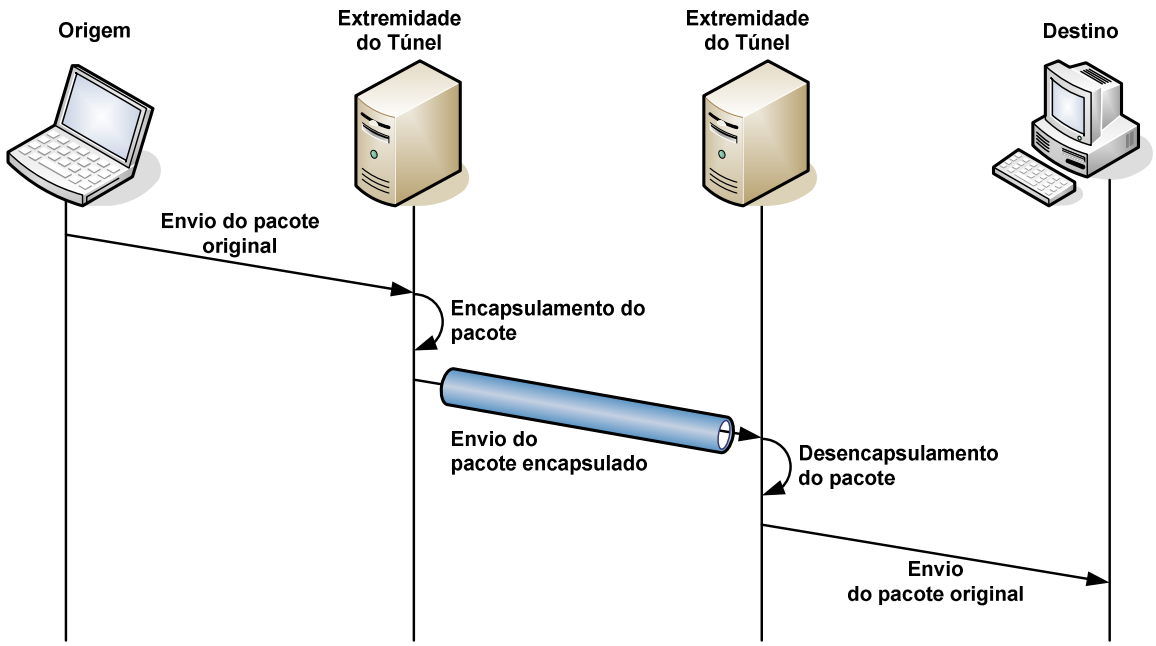


Figura 2.10 - Processo de envio de um pacote em um túnel.

A estrutura de um pacote encapsulado tem a estrutura conforme apresentado na fig. 2.11. Nesta figura, tem-se que o conteúdo do pacote original é a região em azul, o cabeçalho do pacote original é a região em amarelo e o cabeçalho IP adicionado pela extremidade do túnel é a região em verde. Para os roteadores localizados entre as duas extremidades do túnel, o cabeçalho original será considerado como conteúdo do pacote.

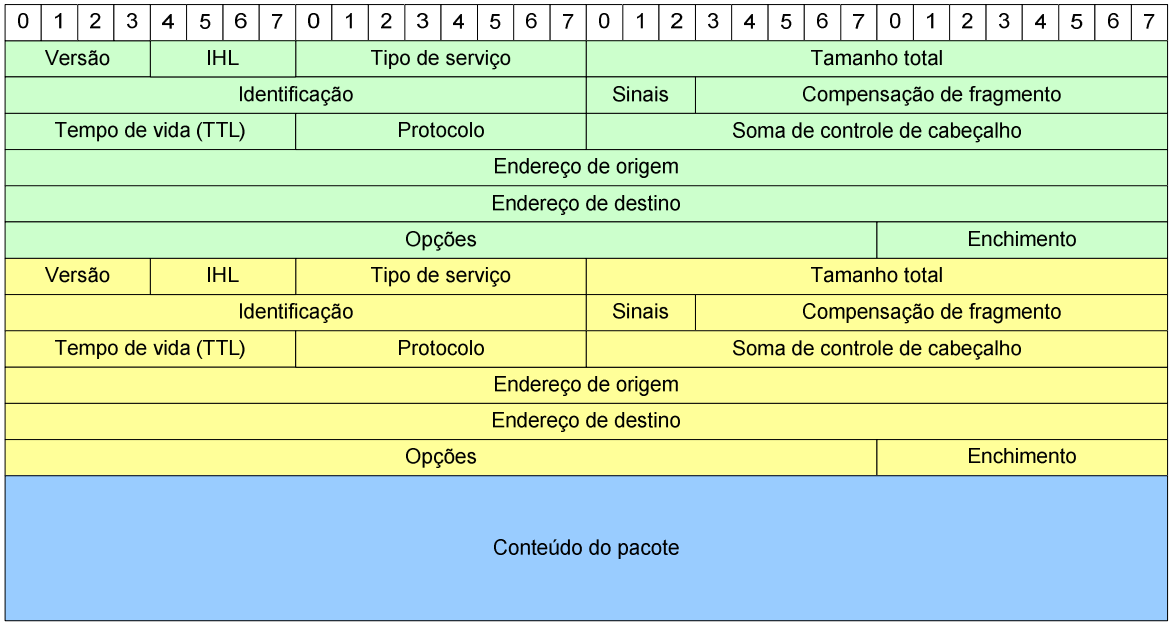


Figura 2.11 - Estrutura de um pacote encapsulado em um túnel IP-em-IP.

Na extremidade do túnel, ao se criar o cabeçalho IP encapsulante, são atribuídos valores aos campos de forma que este pacote seja considerado pela Internet um pacote IPv4 comum, isto é, o encapsulamento é transparente para as redes por onde o pacote passar. Para isso, as opções referentes a características próprias do pacote, tais como soma de controle do cabeçalho e tamanho do pacote são calculadas para o pacote encapsulado, e opções tais como tipo de serviço são copiadas do cabeçalho original. A seguir, têm-se detalhes sobre a configuração de valores de alguns campos:

- **Versão:** Colocado valor 4;
- **IHL (tamanho do cabeçalho Internet):** Valor com o tamanho do cabeçalho encapsulante apenas;
- **Tipo de serviço:** É copiado do cabeçalho IP original;
- **Tamanho total:** Valor com o tamanho do pacote inteiro (cabeçalho encapsulante, cabeçalho original e conteúdo);
- **Sinais:** Caso o bit de fragmentação desabilitada esteja marcado no cabeçalho original, ele será marcado no cabeçalho encapsulante também; caso ele não esteja marcado no cabeçalho original, ele pode ser marcado. O objetivo desta regra é melhorar a eficiência de processamento da extremidade do túnel e dos roteadores que estiverem no caminho percorrido pelo túnel, pois com não-fragmentação dos pacotes, além de não haver o processamento referente à divisão e à restauração do pacote, evita-se o aumento na quantidade de cabeçalhos a serem processados em cada roteador;
- **Tempo de Vida:** É ajustado um valor apropriado para a entrega do pacote encapsulado à outra extremidade do túnel;
- **Protocolo:** Deve ser preenchido com valor 4;
- **Endereço de Origem:** É colocado o endereço IP da extremidade do túnel que faz o encapsulamento do pacote, isto é, o ponto de entrada do túnel;
- **Endereço de Destino:** É colocado o endereço IP da extremidade do túnel que faz o desencapsulamento do pacote, isto é, o ponto de saída do túnel;
- **Opções:** Não é esperado que ocorra uma cópia das opções do cabeçalho original para o cabeçalho encapsulante, isto porque podem ser adicionadas novas opções especificas para o percurso do túnel; apesar disso, algumas opções de segurança do cabeçalho original podem afetar as opções de segurança do cabeçalho encapsulante.

Existem dois tipos de tunelamento IP-em-IP: tunelamento reverso e tunelamento triangular. No tunelamento reverso, todas as informações de e para o nó móvel são roteadas para ele via agente nativo, passando pelo túnel IP-em-IP. A fig. 2.12 apresenta uma ilustração do funcionamento do tunelamento reverso. No tunelamento triangular, apenas o que é enviado para o MN precisa passar pelo HA, sendo que os dados enviados pelo nó móvel são direcionados para o destino diretamente a partir do agente estrangeiro. É mais comum a utilização do tunelamento reverso porque, em algumas redes, é comum ser encontrada política de segurança de não rotear pacotes com endereço de origem que não seja próprio da rede de onde o pacote está vindo; esta política pode vir a descartar pacotes enviados pelo nó móvel, caso este esteja mandando-os sem tunelamento. Uma ilustração do processo realizado no tunelamento triangular pode ser encontrada na fig. 2.13.

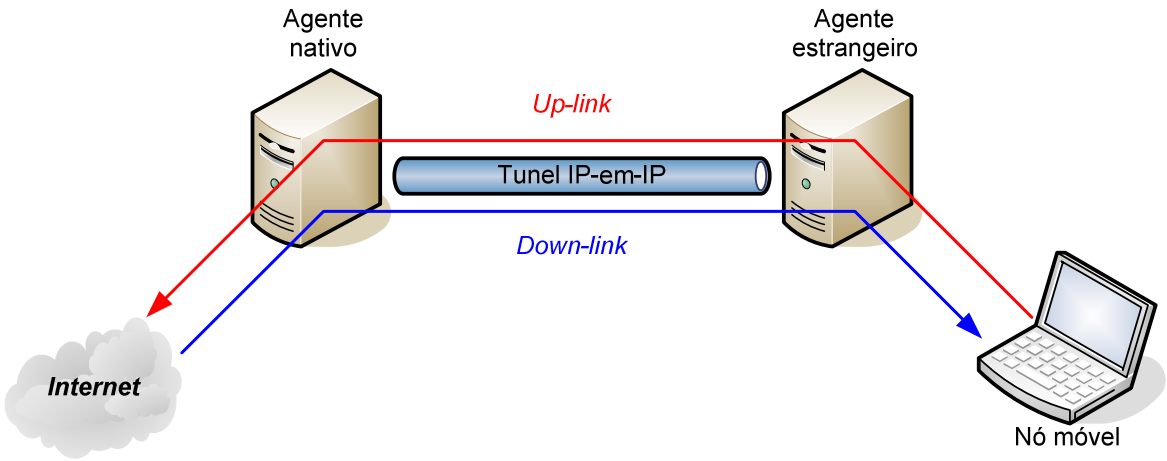


Figura 2.12 - Tunelamento Reverso

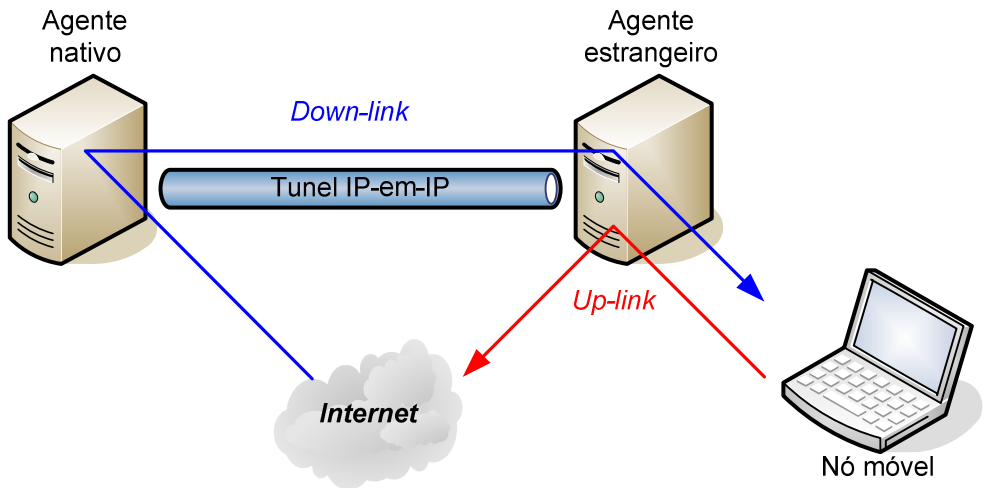


Figura 2.13 - Tunelamento Triangular

Quando ocorrem situações nas quais o agente nativo se encontra muito distante do agente estrangeiro, pode ser que a utilização do tunelamento, apesar de fundamental para o funcionamento da tecnologia, venha a causar um atraso no envio de pacotes. Em situações na qual o nó móvel esteja em outro país, por exemplo, se um dispositivo localizado no mesmo país onde o dispositivo móvel está lhe enviar um pacote, este pacote tem de ir à rede nativa do MN para que o seu agente nativo a encaminhe de volta ao país no qual o nó móvel se encontra, para então o agente estrangeiro poder entregar o pacote.

Além do atraso, a necessidade de toda mensagem destinada ao nó móvel também traz deterioração em outras características de rede. Visto que o percurso percorrido é maior, maior será também a quantidade de *jitter* que o tráfego vai sofrer, e maior a probabilidade de perda de pacotes. Desta forma, este mecanismo pode vir a prejudicar o desempenho do nó móvel no seu acesso à Internet, e a utilização de qualidade de serviços (QoS).

2.3 - MOBILE IP HIERÁRQUICO

O registro regional faz com que o nó móvel, ao se mover de um agente estrangeiro para outro dentro de um mesmo domínio, se registre em uma nova entidade de rede, chamada agente estrangeiro de entrada (*Gateway Foreign Agent* - GFA). Como conseqüência, tem-se uma redução na quantidade de mensagens enviadas ao agente nativo, o que reduz a carga na rede nativa, e ocorre uma redução no tempo de espera do nó móvel pelo registro, que seria elevado em uma rede MIP sem registro regional em que o agente nativo se encontra muito distante do agente estrangeiro.

O IP móvel hierárquico tem algumas alterações em comparação com o IP móvel padrão da RFC 3344. Os anúncios de agente enviados pelo FA contêm não apenas o endereço do agente estrangeiro local disponível para endereço residente, mas também o do agente estrangeiro de entrada. Quando um nó móvel chega a um domínio, ele envia uma requisição de registro com o endereço do GFA como endereço residente e o agente nativo envia de volta uma resposta de registro contendo uma chave de registro, que é armazenada tanto no nó móvel quanto no agente estrangeiro de entrada. Apesar de o MN se registrar no agente nativo com o endereço residente do GFA, ele terá como endereço residente o

endereço do agente estrangeiro local ao qual ele se conecta. Como resultado, ocorrem dois túneis IP-em-IP: um do agente nativo ao agente estrangeiro de entrada e outro do agente estrangeiro de entrada ao agente estrangeiro local, como ilustrado na fig. 2.14.

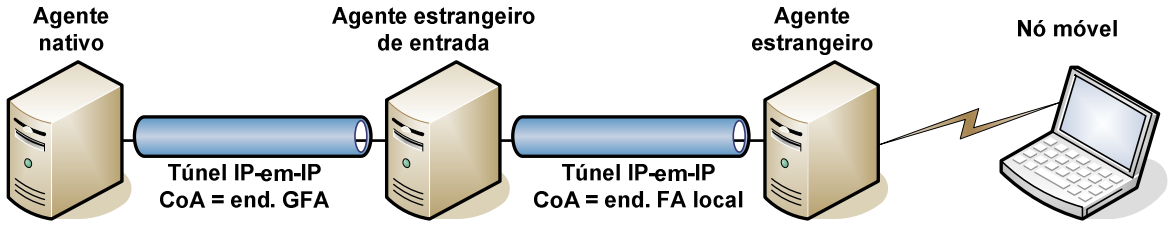


Figura 2.14 - Tunelamento realizado através de registro regional.

Quando o nó móvel se move de uma área de cobertura de um agente estrangeiro para a área de cobertura de outro agente estrangeiro dentro de um mesmo domínio, isto é, ambas as áreas possuem um mesmo agente estrangeiro de entrada, ao receber o anúncio de agente, o MN compara o endereço do GFA com o que ele registrou na área anterior e verifica que está no mesmo domínio, então ele envia uma mensagem de requisição de registro regional contendo a chave de registro, que recebeu do agente nativo, para o agente estrangeiro de entrada; este, ao verificar que esta chave combina com a que recebeu durante o registro do nó móvel no agente nativo, envia uma resposta de registro regional ao nó móvel e atualiza o seu registro de localização do MN. Os tráfegos de mensagens do registro no agente nativo e do registro regional estão ilustrados na fig. 2.15 e na fig. 2.16, respectivamente, e a mudança no tunelamento durante um *handoff* do nó móvel dentro de um mesmo domínio está ilustrado na fig. 2.17.

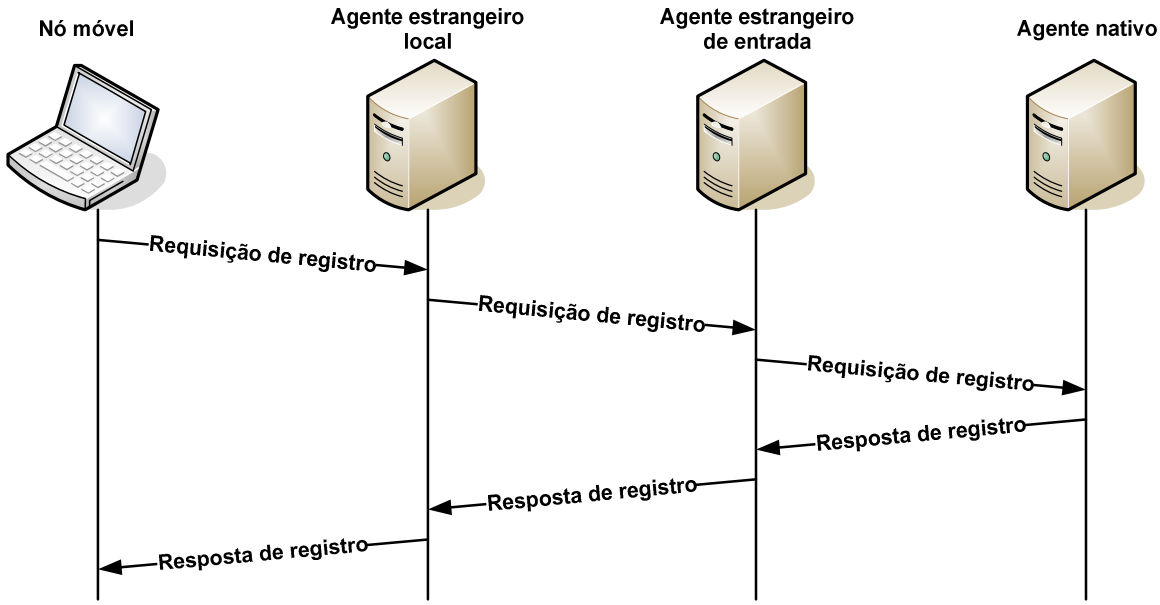


Figura 2.15 - Registro do nó móvel no agente nativo.

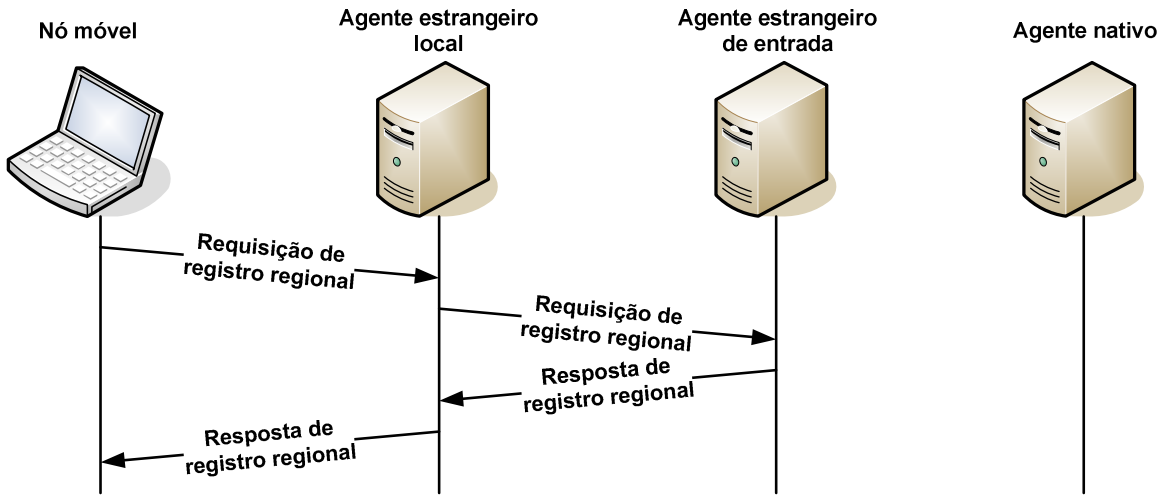


Figura 2.16 - Registro regional do nó móvel.

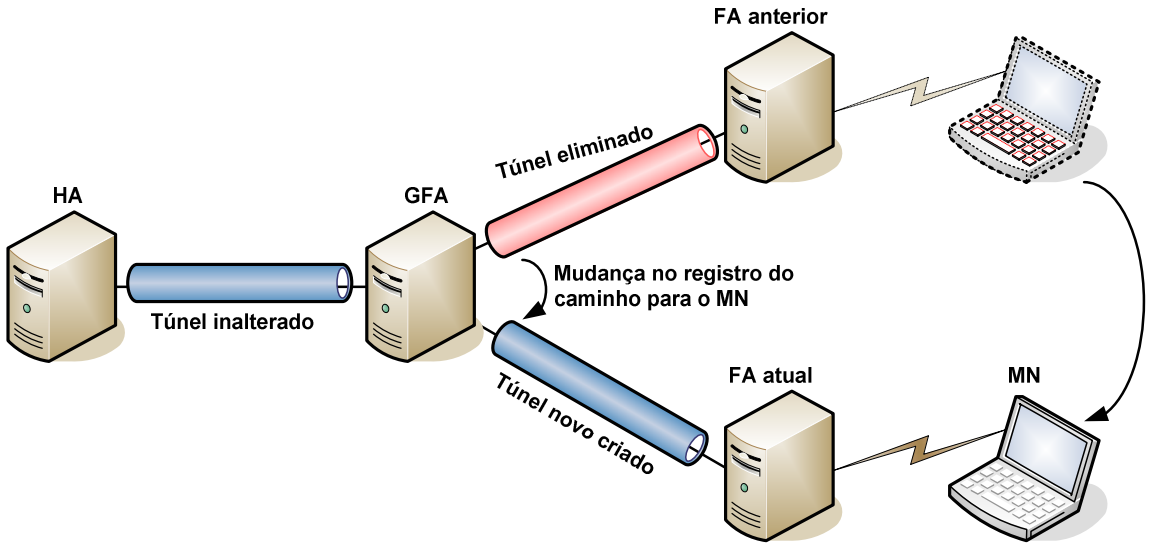


Figura 2.17 - *Handoff* do nó móvel em ambiente com registro regional.

Para hierarquias maiores, além do GFA, também existem os RFAs (agentes estrangeiros regionais), que estão na hierarquia entre o agente estrangeiro de entrada e os agentes estrangeiros locais. Pode haver tantos níveis hierárquicos quanto o necessário ou desejado pelo administrador da rede. Neste cenário, os anúncios de agentes devem conter os FAs de todas as hierarquias no caminho do GFA ao FA local que está enviando o anúncio. Ao se registrar, o nó móvel armazena o endereço de todos os agentes estrangeiros do anúncio, o agente nativo armazena o endereço do agente estrangeiro de entrada como endereço residente do nó móvel e todos os agentes estrangeiros do caminho até ao MN, com exceção do FA local, armazenarão o endereço do agente de hierarquia logo inferior como endereço residente, criando assim diversos túneis. Ao mover-se de um FA para outro dentro do mesmo domínio, o nó móvel verifica qual o FA de hierarquia mais baixa contida no novo anúncio que faz parte, também, da lista de FA armazenada durante o registro anterior e faz o registro regional nele, tal como ilustrado na fig. 2.18.

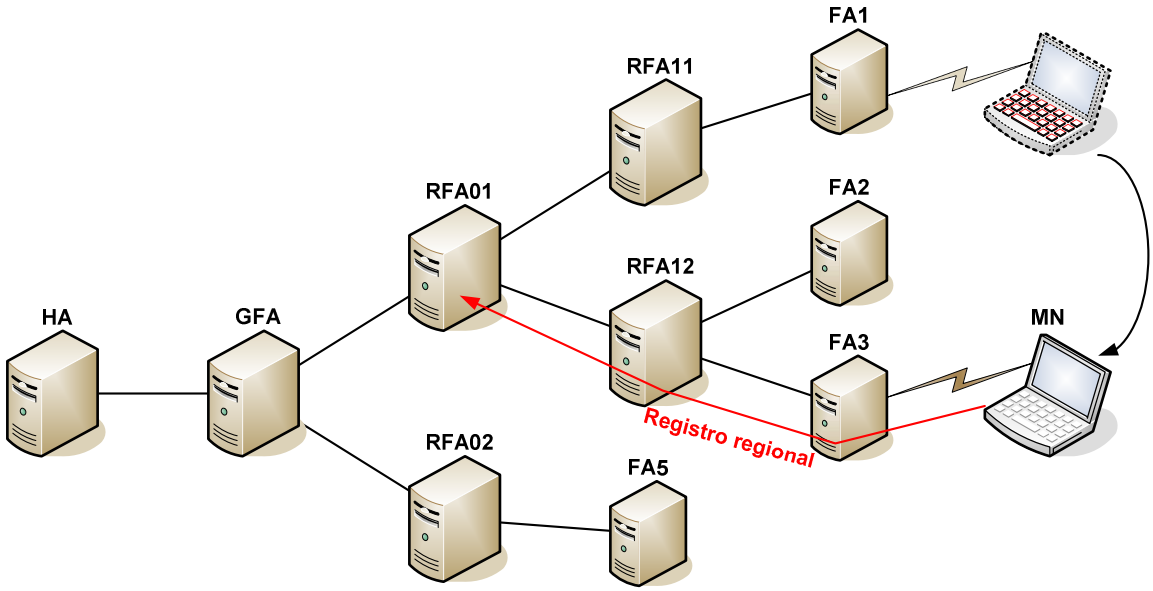


Figura 2.18 - *Handoff* em uma rede IP móvel hierárquica.

2.4 - IMPLEMENTAÇÕES DO MOBILE IP

Desde o desenvolvimento da primeira RFC referente ao IP móvel, foram desenvolvidas implementações deste sistema por diversas empresas. Na tabela 2.3, tem-se uma lista com as principais implementações que foram informadas ao grupo de trabalho de MIP no IETF.

Tabela 2.3 - Implementações de IP móvel informadas ao respectivo grupo de trabalho no IETF [2]

MIPv4			
Sistema Operacional	**Nome**	**Licença**	**Observações**
Windows	Birdstep	comercial	
sistemas embarcados	Birdstep	comercial	
Cisco IOS	Cisco Mobile IP	comercial	
Linux	Dynamics	GPLv2	2001 - Helsinki University of Technology
Windows client	Dynamics	GPLv2	2001 - Helsinki University of Technology
Windows	EcuTel	comercial	
HP-UX 11.11	HP	comercial	Mobile IPv4 HA/CN, Tunelamento Reverso, Otimização de Roteamento e suporte a AAA
Userland, (plataforma	HP Mobile IP	restrita	1997

independente)			
Windows	ipUnplugged	comercial	
FreeBSD 2.2.2	Monarch	tipo BSD	1998 - Rice University
NetBSD 1.1	Monarch	tipo BSD	1998 - Rice University
Linux kernel 2.2.16	MosquitoNet	GPL	2000 - Stanford University
Windows/Linux	Netseal MPN	comercial	Alta disponibilidade. HA - Linux; MN - Windows
Windows	Roamin	proprietária	2000 - distribuição binária apenas para uso não comercial
Linux	Secgo Mobile IP	comercial	
Windows	Secgo Mobile IP	comercial	
FreeBSD 2.2.8, 4.6, 4.8, 4.9, 5.2	Secure Mobile Net	tipo BSD	2003 - Portland State University
Linux	Secure Mobile Net	tipo BSD	2003 - Portland State University
Solaris	Sun Mobile IP	comercial	
SO embarcado independente	Treck Inc.	comercial	
Linux	UoB-NOMAD	SPL	2003 - baseado no NOMADv4
MIPv6			
Sistema Operacional	**Nome**	**Licença**	**Observações**
Cisco IOS	Cisco Mobile IP	comercial	2003 - demonstração tecnológica
Linux	HMIPv6	GPL ou tipo BSD	2003 - Monash University, baseada em MIPL
HP-UX 11.11, 11.23	HP	comercial	Mobile IPv6 HA/CN, draft-24
Tru64 UNIX 5.1B	HP	comercial	2003 - draft -24
FreeBSD 3.4	INRIA HMIPv6	tipo BSD	2000
FreeBSD 4.9	KAME	tipo BSD	2004 - Estável, código MIP experimental
NetBSD 1.6.1	KAME	tipo BSD	2004 - Estável, código MIP experimental
Linux	Lancaster MIPv6 Pkg	?	1998 - Lancaster University
Windows	Microsoft Research	?	2000 - suporte parcial a MIP v6
Linux 2.4.0	MIPL	GPL	2003 - draft -24
FreeBSD 2.2.2 com INRIA's IPv6	Monarch	tipo BSD	1997 - Rice University, (draft - 03)
BSD	NEC MIPv6	?	2001 - NEC
FreeBSD	SFC-MIP	tipo BSD	2002 - SFC do WIDE
Linux 2.4	TKN HMIPv6	?	2002 - Technical University of Berlin
SO embarcado independente	Treck Inc.	comercial	

Neste contexto, encontram-se 15 implementações voltadas à IPv6 e 21 voltadas para IPv4. Percebe-se também a existência de 8 implementações para Windows, 22 implementações para algum tipo de UNIX (linux, freeBSD etc) e 6 para outras plataformas. Outra informação que se obtem é que pelo menos 14 destas implementações têm licença GPL (Licença pública geral GNU) ou BSD (licença de distribuição de software Berkeley), isto é, são implementações livres.

A opção escolhida para este projeto foi o *Dynamics*, porque ele baseia-se em IPv4, que é a tecnologia de rede utilizada no laboratório no qual é realizado este projeto; possui licença GPL, que o torna livre; e não é restrito a distribuições ou *kerneis* específicos do linux.

2.5 - DYNAMICS MOBILE IP

O *Dynamics Mobile IP* foi inicialmente desenvolvido na Universidade de Tecnologia de Helsinki (HUT – *Helsinki University of Technology*) e, desde julho de 2003, tornou-se um projeto aberto no *SourceForge.Net*. Esta implementação está escrita em linguagem de programação C, tem licença GPL (GNU General Public License).

Ele tem como sistemas operacionais alvo todos os sistemas POSIX (linux, BSD e sistemas operacionais do tipo UNIX), especialmente o linux. Possui também uma implementação do nó móvel para Microsoft Windows de 32 bits (95/98/NT/2000/XP), entretanto esta implementação precisa do emulador de linux conhecido por *Cygwin* em conjunto com uma biblioteca de análise de rede e captura de pacotes chamada *Winpcap*. A versão de nó móvel para Windows não está 100% funcional: algumas opções tais como desencapsulamento no MN não estão implementadas, e mesmo as funções implementadas não foram testadas exaustivamente, mas apenas de forma superficial [10]. O *Dynamics*, além de implementar a especificação contida na RFC 3344 [43] também implementa o registro regional [29], que possibilita o IP móvel hierárquico. Portanto, neste projeto, foi escolhido trabalhar com a versão de linux do nó móvel.

2.5.1 - Instalação e funcionamento básico do Dynamics

Foram realizados, neste projeto, alguns testes sobre o funcionamento do Dynamics, para confirmar o funcionamento, na prática, dos processos do IP móvel descritos na especificação do IETF. Devido à limitação de recursos, os testes foram limitados à verificação das trocas de mensagens dos anúncios, registros e encapsulamento de pacotes comuns. Para isso, utilizou-se a distribuição 0.8 do Dynamics, disponível na *Internet* [10]. A distribuição 0.9 do Dynamics, que deve trazer novas funcionalidades, não foi utilizada por estar ainda em fase de desenvolvimento.

A instalação do Mobile IP para demonstração foi feita com a topologia informada na fig. 2.19. Esta topologia foi conseguida através da utilização de dois laboratórios da UnB, LEMOM (Laboratório de Estruturas de Microondas e Ondas Milimétricas) e LABCOM (Laboratório de comunicações da UnB). A *Internet* citada na figura corresponde, na realidade, à rede da UnB, que passa por diversos institutos além do Departamento de Engenharia Elétrica.

Na rede nativa, foi utilizado endereço de rede privada não-roteável na Internet, 172.1.16.0. Os outros endereços utilizados são reservados para os laboratórios utilizados na demonstração.

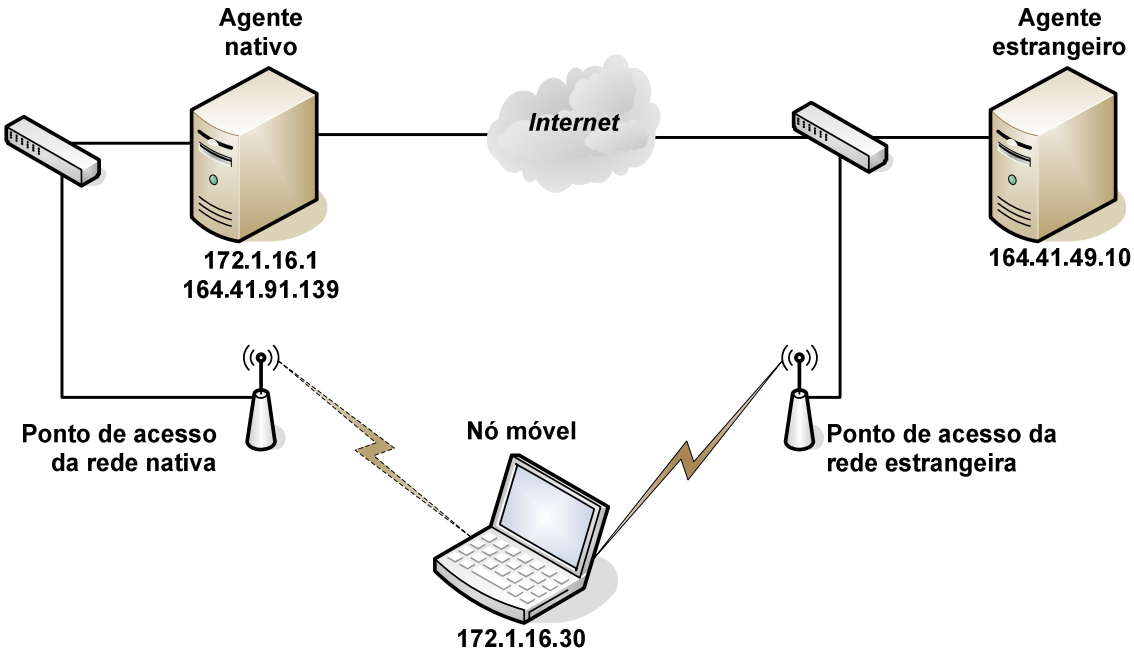


Figura 2.19 - Topologia utilizada na instalação do Mobile IP

Os equipamentos deste sistema que precisaram de alguma configuração específica foram os agentes e o nó móvel, que precisaram da instalação dos respectivos módulos do Dynamics sob o sistema operacional linux. A instalação destes módulos se fez através do comando básico de instalação RPM: `rpm -ihv <nome_do_pacote>`. Os *hubs* foram utilizados apenas para permitir a concentração de tráfego e os APs foram colocados em "modo *hub*", isto é, eles apenas repassam os pacotes da interface aérea para as interfaces ethernet e o inverso também.

Além de instalar o Dynamics, deve-se também ajustar os seus arquivos de configuração: dynhad.conf, dynfad.conf e dynmnd.conf. As configurações essenciais para o funcionamento do sistema são o cadastro das interfaces de rede utilizadas pelo sistema, o endereço do agente nativo na configuração do nó móvel e a lista de endereços que têm permissão para se conectarem no sistema IP móvel nas configurações dos agentes.

O processo de teste, propriamente dito, começou pela inicialização dos agentes, e em seguida pela inicialização do nó móvel dentro da área de cobertura da rede nativa. Em seguida, o dispositivo móvel foi deslocado para uma região onde o sinal emitido pelo ponto de acesso da rede nativa não tinha mais potência suficiente para manter o *link* e o

sinal do AP da rede estrangeira estava forte o suficiente para que houvesse conexão. Por fim, o nó móvel retornou a sua rede de origem.

O *software* do Dynamics é um *daemon* que executa na memória do dispositivo, e, portanto, não apresenta uma tela principal ou *frame* de execução, mas ele possui um programa auxiliar que executa em linha de comando e permite analisar as informações sobre a condição do sistema IP móvel no dispositivo. Este programa auxiliar, que será chamado ferramenta de diagnóstico, e o Ethereal, que é um *sniffer*, isto é, um capturador de pacotes, muito popular para linux, foram utilizados para verificar o funcionamento do IP móvel no teste realizado.

Ao iniciar os agentes, eles periodicamente passam a mandar mensagens de anúncios, tal como pode ser visto na fig. 2.20, que apresenta os pacotes capturados no agente estrangeiro. Os campos da seção ICMP nesta figura podem ser comparados com o formato dos anúncios apresentados na Figura 2.2. Tal como determinado na especificação, estes pacotes foram enviados com destinatário 255.255.255.255, que é o endereço de *broadcast* limitado. Este endereço é utilizado porque, caso fosse utilizado um endereço de *broadcast* comum, 164.41.49.255 neste caso, o nó móvel que entrasse na rede não identificaria a mensagem, por se tratar de um endereço de rede distinto do seu.

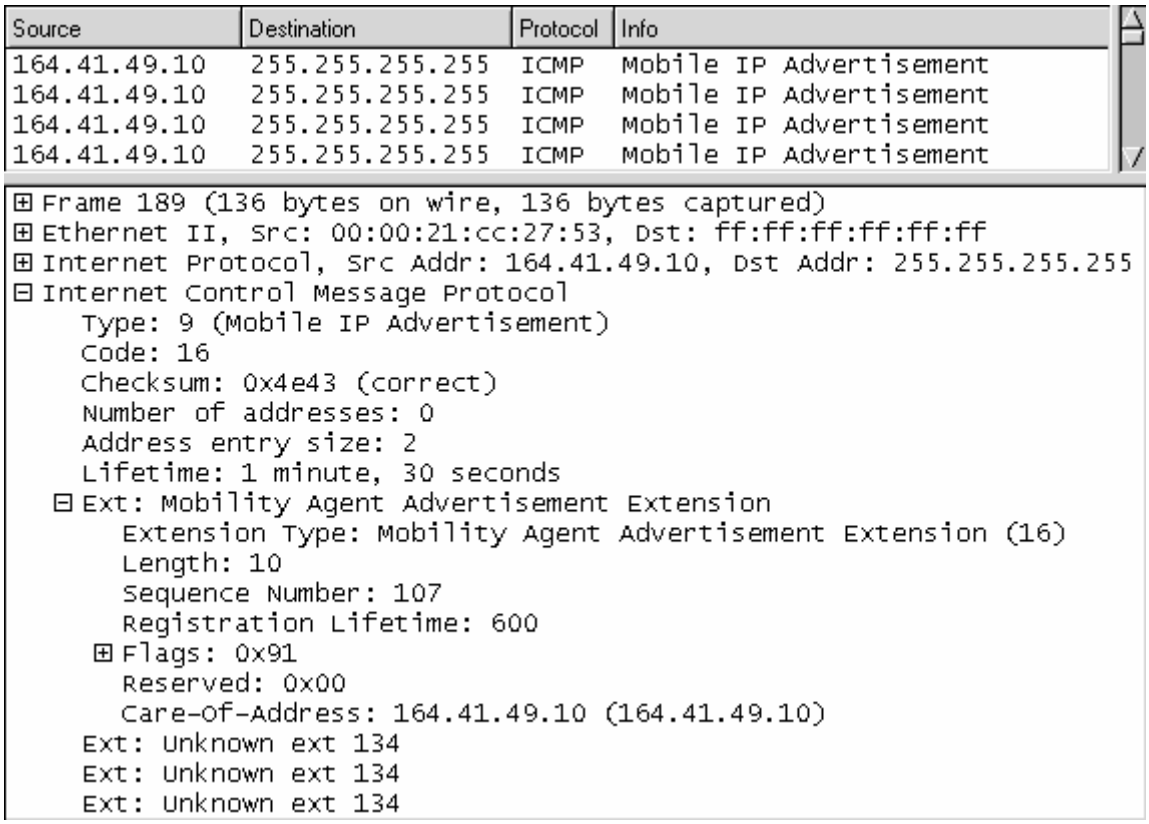


Figura 2.20 - Anúncios de agente móvel enviados durante o teste.

Ao iniciar o serviço do nó móvel e antes de o mesmo ter entrado na área de cobertura de algum agente, obteve-se um tempo de espera em que o dispositivo aguardou por anúncios de agente móvel; não tendo recebido nenhum porque não havia ainda sido conectado em nenhuma das duas redes, ele enviou então uma solicitação de agente móvel, que pode ser visualizada na fig 2.21. Assim como o anúncio, esta mensagem pode também ser comparada com o formato da mensagem apresentado na fig. 2.5.

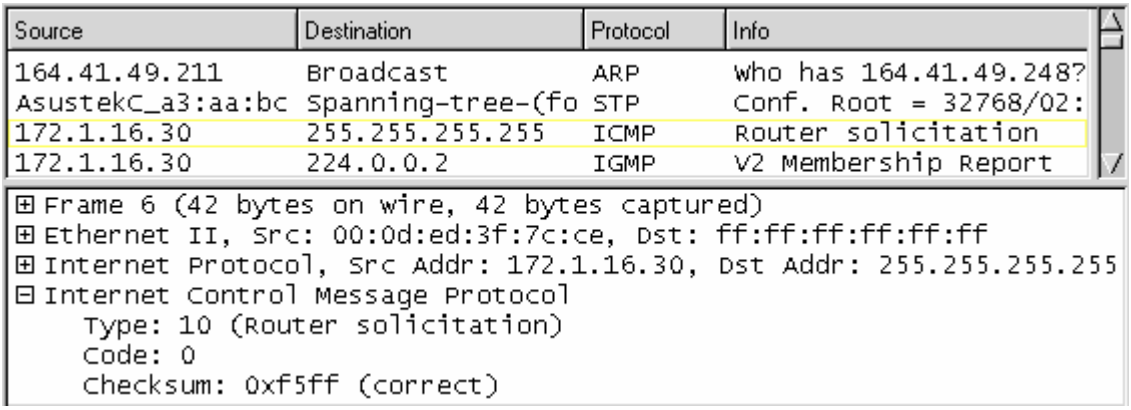


Figura 2.21 - Solicitação de agente móvel durante o teste.

Neste momento, antes de entrar com o nó móvel em qualquer das áreas de coberturas, o resultado das ferramentas de diagnóstico dos agentes indicavam a ausência de túneis, tal como indicam a fig. 2.22 e a fig. 2.23, e a ferramenta de diagnóstico do nó móvel apresenta um estado de busca passiva, não havendo túnel e não tendo nenhum endereço registrado como endereço do agente estrangeiro nem de endereço residente, e seu texto informativo indica que ele se encontra tentando conectar. A tela capturada da ferramenta de diagnóstico do nó móvel está apresentada na fig. 2.24.

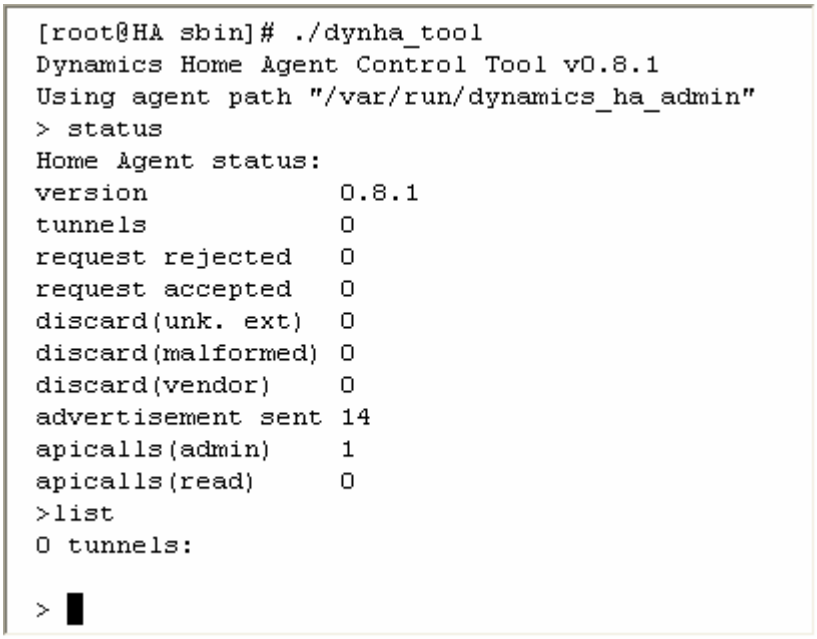


Figura 2.22 - Ferramenta de diagnóstico do agente nativo com nó móvel não-conectado.

```
[root@FA sbin]# ./dynfa_tool
Dynamics Foreign Agent Control Tool v0.8.1
Using agent path "/var/run/dynamics_fa_admin"
> status
Foreign Agent status:
version            0.8.1
tunnels            0
pending reg.req.   0
request rejected   0
request accepted   0
reply rejected     0
reply accepted     0
discard(unk. ext)  0
discard(malformed) 0
discard(vendor)    0
advertisement sent 253
apicalls(admin)    1
apicalls(read)     0
>list
0 tunnels:

>
```

Figura 2.23 - Ferramenta de diagnóstico do agente estrangeiro com nó móvel não-conectado.

```
[root@MN sbin]# ./dynmn_tool
Dynamics Mobile Agent Control Tool v0.8.1
Using agent path "/var/run/dynamics_mn_admin"
> status
Mobile status:
      state              Passive Find
      local addr         172.1.16.30
      co-addr            0.0.0.0
      FA-addr            0.0.0.0
      HA-addr            164.41.91.139
      Home addr          172.1.16.30
      tunnel is          down
      tunneling mode     full tunnel
      info text          trying to connect
      active devices     1
      discarded msgs     0
> list
List of heard mobility agents:
>
```

Figura 2.24 - Ferramenta de diagnóstico do nó móvel enquanto o mesmo encontra-se não-conectado.

Em seguida, o nó móvel entrou na área de cobertura do agente caseiro. Ao receber um anúncio, o nó móvel enviou a requisição de registro. Por se tratar da rede nativa, o MN preencheu em seu endereço residente o próprio endereço, pois o seu endereço já indica a

rede em que ele se encontra e o agente nativo não precisa fazer tunelamento para mandar mensagens para ele. A fig. 2.25 apresenta a requisição de registro vista pelo *Ethereal* no agente nativo. Podem ser verificados, nesta figura, os endereços do MN, HA e endereço residente que o nó móvel envia na requisição. A partir destas informações o agente nativo determina se o móvel faz parte da sua rede e aceita o registro. Pode ser verificado ainda a utilização da porta UDP 434 para destino, tal como especificado; mas para a porta de origem, foi utilizada uma porta escolhida aleatóriamente pelo desenvolvedor (a implementação do *Dynamics* utiliza UDP 32770 no nó móvel). Os dados contidos na fig. 2.25 podem ser comparados com os dados do formato da requisição de registro apresentado na fig. 2.8.

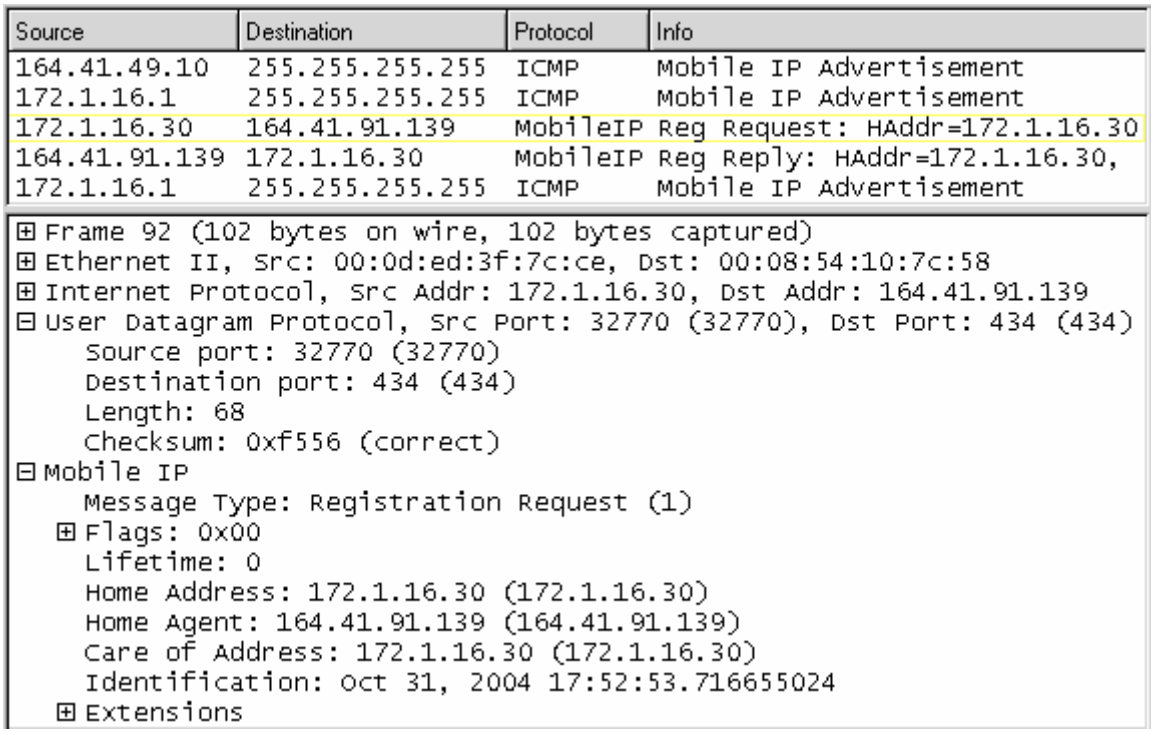


Figura 2.25 - Mensagem de requisição de registro na rede nativa.

A resposta do registro, visualizada na fig. 2.26, traz o código de registro 0, que indica registro aceito. Tem-se aqui a utilização da porta de origem da requisição, isto é, porta UDP 434, como sendo a porta de destino. Este fato, que faz parte da especificação, tem como finalidade especificar a porta que o móvel deve estar ouvindo para receber a resposta do registro. A utilização da porta UDP 434 como porta de origem na resposta não faz parte da especificação, ela foi escolhida pelos desenvolvedores do Dynamics de forma não-

obrigatória. Esta mensagem pode ser também comparada com a fig. 2.9 para visualização do preenchimento dos dados na estrutura da mensagem.

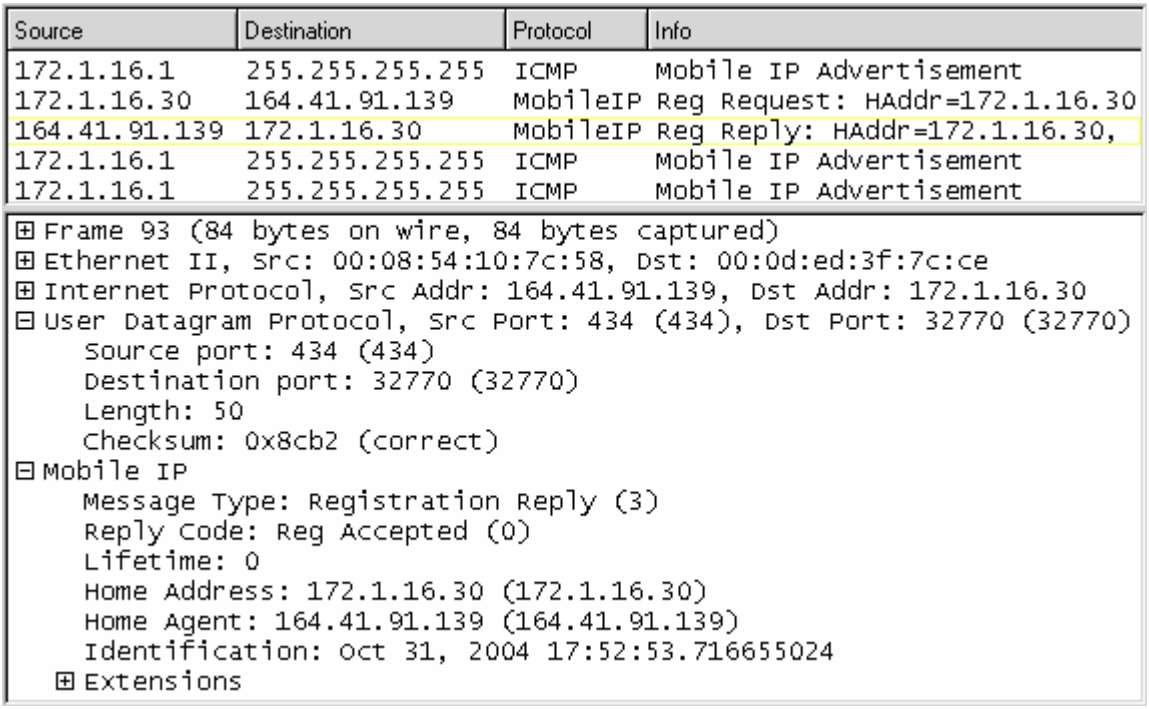


Figura 2.26 - Mensagem de resposta de registro na rede nativa.

Após esta conexão, foram capturadas as telas das ferramentas de diagnóstico do nó móvel e do agente nativo, apresentadas nas figs. 2.27 e 2.28. No diagnóstico do MN, apresenta-se o estado em casa, que indica que o móvel encontra-se em sua rede nativa, endereço residente como sendo o próprio endereço do nó móvel, registro aceito, indicando que o mesmo foi realizado com sucesso e túnel desativado. O fato de o túnel estar desativado ocorre por não ser necessário o tunelamento, pelo fato de ele ter acesso a todos os seus recursos de rede quando se encontra em sua rede nativa. A lista de agentes móveis encontrados limita-se ao agente nativo de sua rede, pelo fato de não haver nenhum outro agente de mobilidade enviando anúncios nesta rede. No diagnóstico do agente nativo, verifica-se a presença de requisições aceitas, mas ausência de túneis, o que está de acordo com o diagnóstico do nó móvel e com a especificação do IP móvel.

```
[root@MN sbin]# ./dynmn_tool
Dynamics Mobile Agent Control Tool v0.8.1
Using agent path "/var/run/dynamics_mn_admin"
> status
Mobile status:
      state              At Home
      local addr         172.1.16.30
      co-addr            172.1.16.30
      FA-addr            164.41.91.139
      HA-addr            164.41.91.139
      Home addr          172.1.16.30
      tunnel is          down
      tunneling mode     full tunnel
      last request       340s ago; Sun Oct 31 17:44:53 2004
      last reply         340s ago; Sun Oct 31 17:44:53 2004
      reply code         0 - registration accepted
      info text          connection established
      active devices     1
      discarded msgs     0
> list
List of heard mobility agents:
164.41.91.139     eth0  prio 0 (-  0%), age 9s HA DYN IN-USE CURRENT
>
```

Figura 2.27 - Ferramenta de diagnóstico do nó móvel quando conectado na rede nativa.

```
[root@HA sbin]# ./dynha_tool
Dynamics Home Agent Control Tool v0.8.1
Using agent path "/var/run/dynamics_ha_admin"
> status
Home Agent status:
version            0.8.1
tunnels            0
request rejected   0
request accepted   2
discard(unk. ext)  0
discard(malformed) 0
discard(vendor)    0
advertisement sent 304
apicalls(admin)    2
apicalls(read)     0
>list
0 tunnels:

>
```

Figura 2.28 - Ferramenta de diagnóstico do agente nativo quando o nó móvel encontra-se conectado na rede nativa.

Para verificar que o IP móvel realmente permitiu acesso à rede, foram efetuados 2 tipos de teste de conexão: visita a alguma página *web* da Internet e testes de *ping* endereçados por e para um dispositivo da rede nativa. As figs. 2.29 e 2.30 apresentam os pacotes que

trafegaram durante a pesquisa na *Internet*. O importante destas figuras é a demonstração de que, tanto no *downlink* quanto no *uplink*, não ocorre o tunelamento, isto é, há apenas um cabeçalho IP em torno dos pacotes TCP que estão trafegando do nó móvel para qualquer rede, seja ela a rede nativa ou alguma outra rede qualquer da Internet.

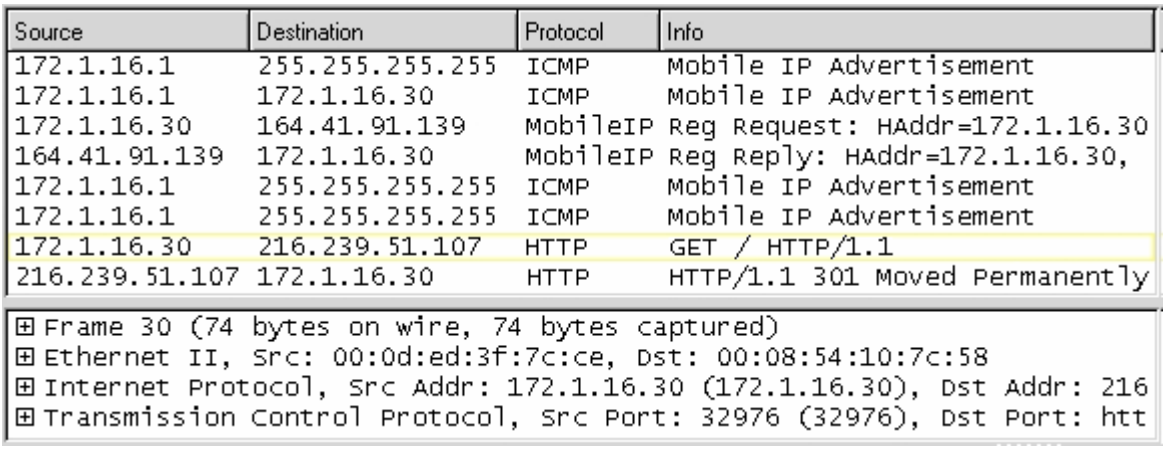


Figura 2.29 - Comunicação do nó móvel na rede nativa: detalhes do uplink.

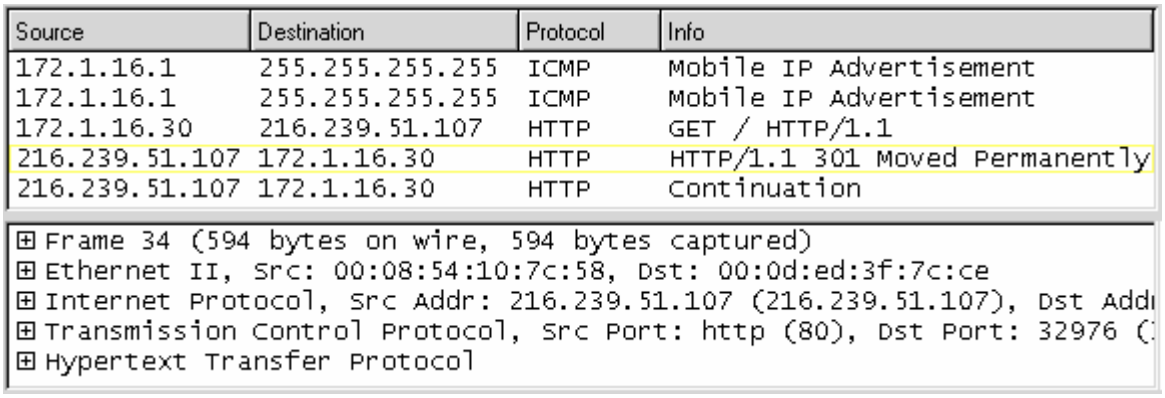


Figura 2.30 - Comunicação do nó móvel na rede nativa: detalhes do *downlink*.

Após a verificação de que o móvel foi registrado com sucesso na rede nativa, e que ele teve acesso à Internet e a recursos da sua rede, ele foi transferido para a área de cobertura da rede estrangeira, onde foram capturadas novas mensagens de registro. A fig. 2.31 apresenta a mensagem de requisição de registro capturada no nó móvel. É interessante perceber a utilização do endereço do agente estrangeiro como endereço residente. Isto se faz devido ao fato de este endereço ser o encontrado pelo MN na mensagem de anúncio de agente móvel recebido nesta rede.

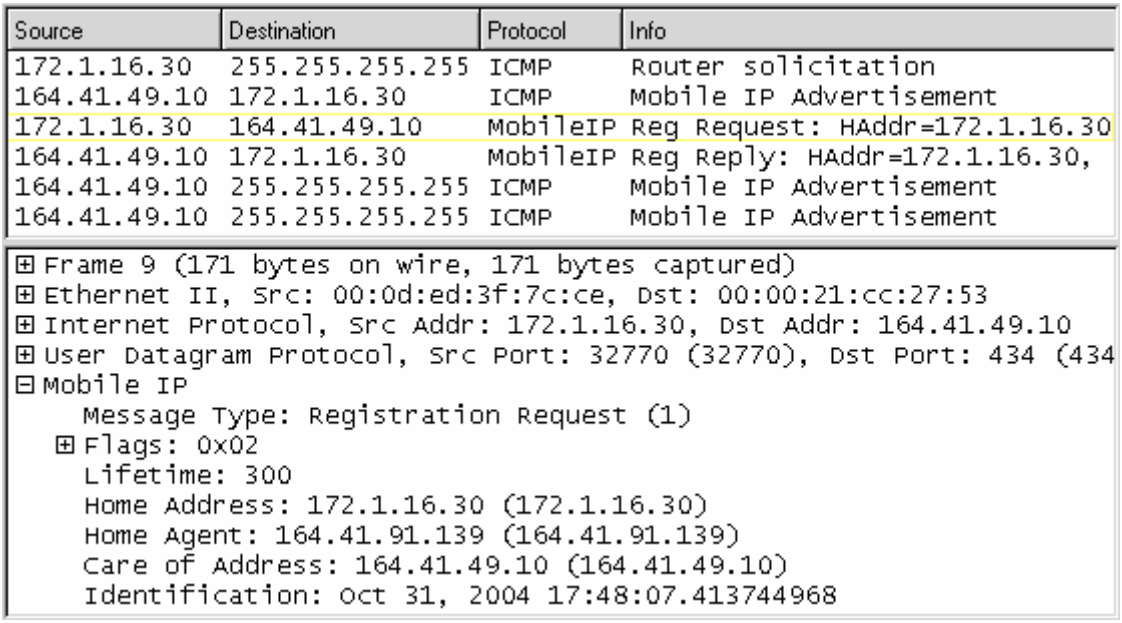


Figura 2.31 - Mensagem de requisição de registro na rede estrangeira vista a partir do nó móvel.

Na fig. 2.32, tem-se a resposta a esta requisição capturada no agente estrangeiro. O fato de haver nesta janela duas requisições de registro e duas respostas se dá ao fato de que uma das requisições foi recebida pelo agente estrangeiro, e a outra é a mesma requisição, agora enviada por ele ao agente nativo do nó móvel; da mesma forma, uma das respostas é a que ele recebeu do HA e a outra é o encaminhamento desta resposta ao nó móvel. Este procedimento pode ser revisto na Figura 2.7. O tempo de vida, apresentado com valor 300, indica que a cada 300 segundos o registro deve tornar a ser executado, para que o nó móvel e os agentes tenham confirmação de que o móvel ainda encontra-se na rede estrangeira à qual está conectado.

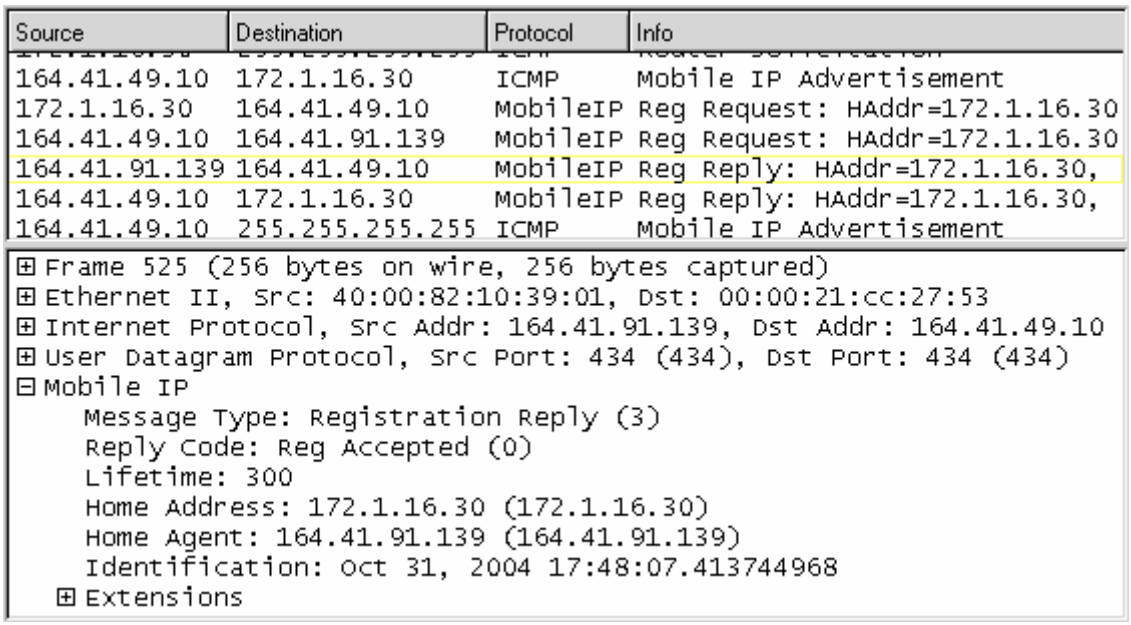


Figura 2.32 - Mensagem de resposta de resgistro na rede estrangeira vista a partir do agente estrangeiro.

Após o registro, o móvel apresenta, em sua ferramenta de diagnóstico, as informações apresentadas na fig. 2.33. Desta vez, as informações apresentadas são o estado conectado, endereço residente igual ao do agente estrangeiro, registro aceito, túnel ativo e a lista de agentes de mobilidade apresenta apenas o agente estrangeiro.

```
[root@MN sbin]# ./dynmn_tool
Dynamics Mobile Agent Control Tool v0.8.1
Using agent path "/var/run/dynamics_mn_admin"
> status
Mobile status:
      state              Connected
      local addr         172.1.16.30
      co-addr            164.41.49.10
      FA-addr            164.41.49.10
      HA-addr            164.41.91.139
      Home addr          172.1.16.30
      tunnel is          up
      lifetime left      261s
      tunneling mode     full tunnel
      last request       39s ago; Sun Oct 31 17:48:07 2004
      last reply         39s ago; Sun Oct 31 17:48:07 2004
      reply code         0 - registration accepted
      info text          connection established
      active devices     1
      discarded msgs     0
> list
List of heard mobility agents:
164.41.49.10      eth0  prio 100 (-  0%), age 13s FA DYN IN-USE CURRENT
>
```

Figura 2.33 - Ferramenta de diagnóstico do nó móvel quando conectado na rede estrangeira.

A ferramenta de diagnóstico do agente nativo apresenta, além do aumento na quantidade de requisições aceitas, um túnel para o móvel de endereço 172.1.16.30, isto é, o nó móvel do teste. A tela capturada do diagnóstico do agente nativo e do agente estrangeiro estão apresentadas respectivamente nas figs. 2.34 e 2.35. No diagnóstico do agente estrangeiro, tem-se também um túnel apenas, que comunica o nó móvel com o agente nativo.

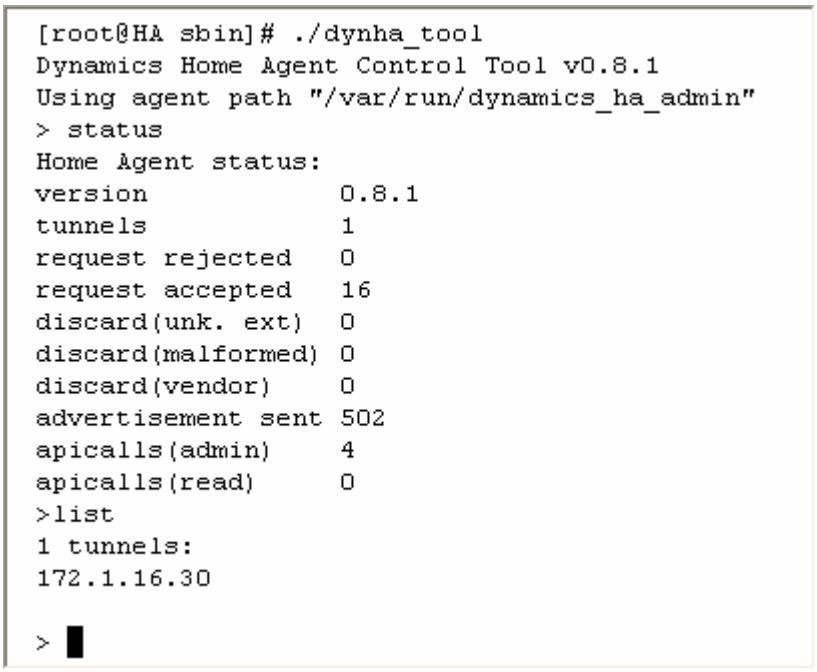


Figura 2.34 - Ferramenta de diagnóstico do agente nativo quando o nó móvel encontra-se conectado na rede estrangeira.

Figura 2.35 - Ferramenta de diagnóstico do agente estrangeiro quando o nó móvel encontra-se conectado em sua rede.

Da mesma forma como na rede nativa, o teste de conectividade foi realizado através de pesquisa em páginas *web* da Internet e através de execução de *ping* de e para algum dispositivo da rede nativa para o nó móvel. Ambos os testes tiveram sucesso, resultando em conectividade plena do móvel como se estivesse em sua rede. As figs. 2.36 e 2.37 apresentam a comunicação de *ping* realizado pelo móvel, que apesar de ser capturada no agente estrangeiro, apresenta os pacotes capturados na interface que se comunica com o nó móvel, de forma a mostrar que o caminho do MN ao agente estrangeiro não possui tunelamento.

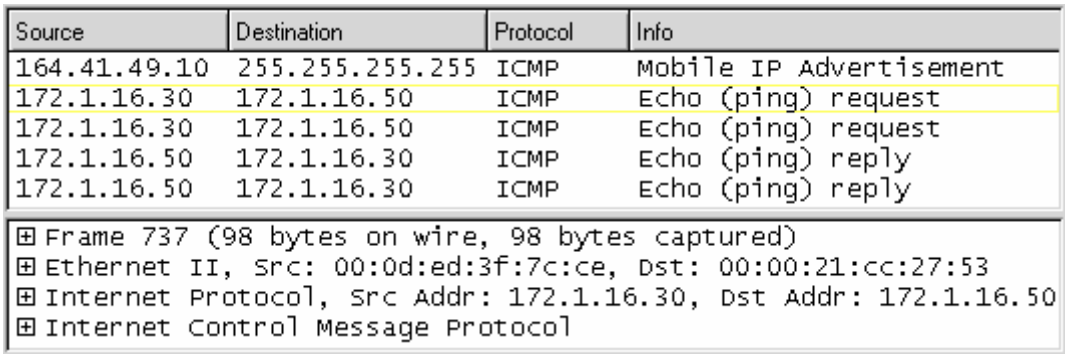


Figura 2.36 - Comunicação do nó móvel a partir de uma rede estrangeira; *uplink* entre o nó móvel e o agente estrangeiro.

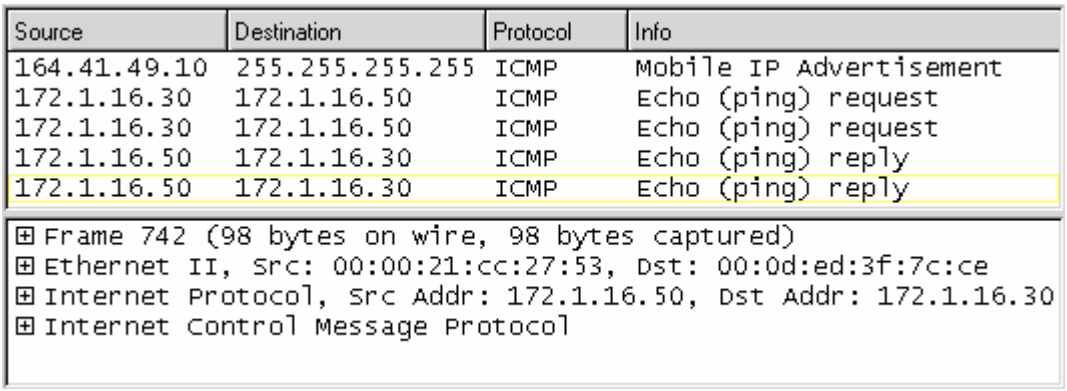


Figura 2.37 - Comunicação do nó móvel a partir de uma rede estrangeira; downlink entre o nó móvel e o agente estrangeiro.

As figs. 2.38 e 2.39 apresentam a mesma comunicação, também capturada no agente estrangeiro, mas sendo visualizada pela interface que comunica com a Internet, e conseqüentemente com o agente nativo. Pode ser vista, na estrutura dos pacotes tanto de *uplink* quanto de *downlink*, a existência de dois cabeçalhos IP: o primeiro traz os endereços dos agentes nativo e estrangeiro, e o segundo, o endereço do nó móvel e da máquina que está recebendo as solicitações de *ping*. O teste de comunicação realizado através do *ping* foi mais interessante, nesta situação que o de conexão com a Internet, pois ele foi realizado com uma máquina que faz parte da rede privada à qual o dispositivo móvel faz parte; se estivesse sendo utilizado DHCP ou qualquer outro recurso de rede para se conseguir conexão com Internet que não fosse o IP móvel, não seria possível efetuar este *ping*, pois o endereço 172.1.16.50 não é roteável pela Internet.

Source	Destination	Protocol	Info
164.41.49.10	255.255.255.255	ICMP	Mobile IP Advertisement
172.1.16.30	172.1.16.50	ICMP	Echo (ping) request
172.1.16.30	172.1.16.50	ICMP	Echo (ping) request
172.1.16.50	172.1.16.30	ICMP	Echo (ping) reply
172.1.16.50	172.1.16.30	ICMP	Echo (ping) reply

```
⊞ Frame 740 (118 bytes on wire, 118 bytes captured)
⊞ Ethernet II, Src: 00:00:21:cc:27:53, Dst: 40:00:82:10:00:19
⊞ Internet Protocol, Src Addr: 164.41.49.10, Dst Addr: 164.41.91.139
⊞ Internet Protocol, Src Addr: 172.1.16.30, Dst Addr: 172.1.16.50
⊞ Internet Control Message Protocol
```

Figura 2.38 - Comunicação do nó móvel a partir de uma rede estrangeira; *uplink* entre o nó móvel e o agente estrangeiro.

Source	Destination	Protocol	Info
164.41.49.10	255.255.255.255	ICMP	Mobile IP Advertisement
172.1.16.30	172.1.16.50	ICMP	Echo (ping) request
172.1.16.30	172.1.16.50	ICMP	Echo (ping) request
172.1.16.50	172.1.16.30	ICMP	Echo (ping) reply
172.1.16.50	172.1.16.30	ICMP	Echo (ping) reply

```
⊞ Frame 741 (118 bytes on wire, 118 bytes captured)
⊞ Ethernet II, Src: 40:00:82:10:39:01, Dst: 00:00:21:cc:27:53
⊞ Internet Protocol, Src Addr: 164.41.91.139, Dst Addr: 164.41.49.10
⊞ Internet Protocol, Src Addr: 172.1.16.50, Dst Addr: 172.1.16.30
⊞ Internet Control Message Protocol
```

Figura 2.39 - Comunicação do nó móvel a partir de uma rede estrangeira; downlink entre o nó móvel e o agente estrangeiro.

Ao retornar à rede nativa, foram verificados os mesmos resultados obtidos no primeiro registro do móvel, isto é, as telas obtidas através do Ethereal ou das ferramentas de diagnóstico foram semelhantes às apresentadas entre as figs. 2.25 e 2.30.

2.6 - ANÁLISE DE DESEMPENHO DO MOBILE IP

Após a verificação de que existem implementações do MIP que realmente alcançam o objetivo proposto na especificação, foi feito outro teste, que tem por objetivo determinar o desempenho de um sistema que oferece o serviço de IP móvel. Devido à falta de recursos, não foi possível realizar um teste que verificasse o desempenho do Mobile IP durante *handoffs*. O teste realizado verificou então apenas o desempenho no recebimento de pacotes vindos da Internet.

Para realização do teste, foi simulado um ambiente de Internet através da utilização de um *backbone* composto de quatro roteadores e um enlace de rádio. O enlace de rádio tem capacidade de 1Mbps e entre os quatro roteadores, tem-se enlaces de 2Mbps. Em cada um dos roteadores foram incluídos aproximadamente 64.000 registros na tabela de roteamento, e no *backbone*, foi aplicado um tráfego auto-similar, que é o modelo de tráfego que tem mesmo tipo de comportamento que a Internet, de 1Mbps.

O teste teve duas etapas. Na primeira etapa, manteve-se o nó móvel na rede nativa e o serviço de IP móvel desativado, então foram calculadas as características de banda utilizada, perda de pacotes, atraso e variação de atraso para tráfegos de 8kbps e de 256kbps que este dispositivo recebeu de um nó correspondente do outro lado do *backbone*. Na segunda etapa, iniciou-se o serviço de IP móvel e, em seguida, o nó móvel foi movido para uma rede estrangeira, também localizada do outro lado do *backbone*, então foram feitos os mesmos testes da etapa anterior. A estrutura montada para este teste está apresentada nas figs. 2.40 e 2.41. O endereçamento utilizado neste ambiente está apresentado na tabela 2.4 e o sentido do envio dos pacotes durante o teste está apresentado nas figuras através de um caminho desenhado em vermelho.

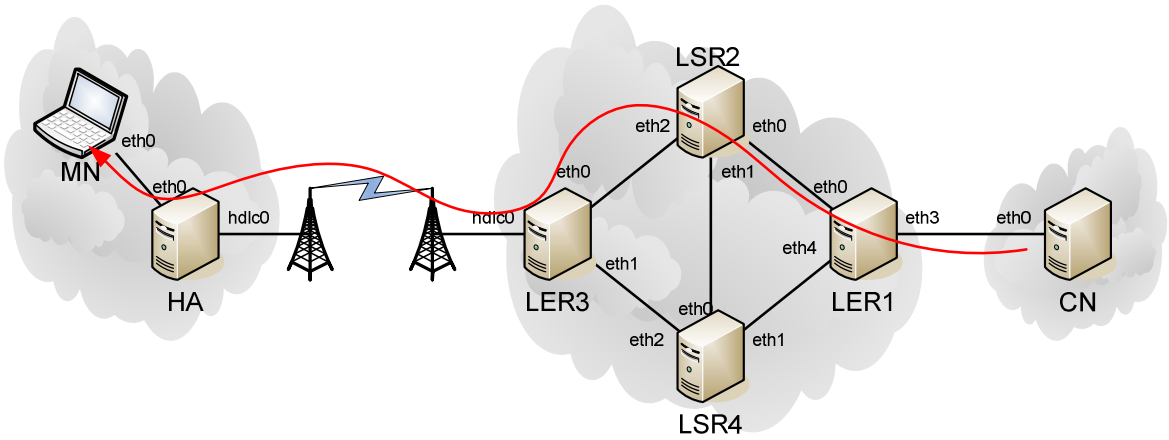


Figura 2.40 - Ambiente de testes durante a primeira etapa do teste.

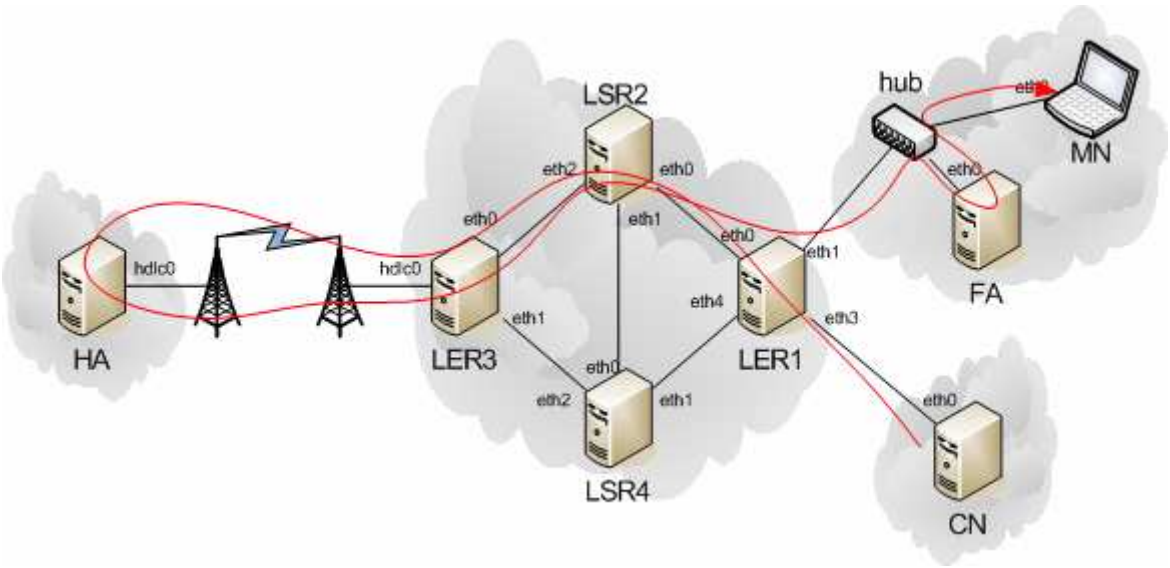


Figura 2.41 - Ambiente de testes durante a segunda etapa.

Tabela 2.4 - Endereços usados no ambiente de testes.

Dispositivo	**Interface**	**endereço**
LER1	eth0	10.0.7.1
	eth1	172.24.1.111
	eth3	192.168.2.1
	eth4	10.0.9.1
LSR2	eth0	10.0.7.2
	eth1	10.0.8.2
	eth2	10.0.6.2
LER3	eth0	10.0.6.3
	eth1	10.0.10.3
	hdlc0	10.0.5.1
LSR4	eth0	10.0.8.4
	eth1	10.0.9.4
	eth2	10.0.10.4
HA	eth0	192.168.1.1
	hdlc0	10.0.5.2
MN	eth0	196.168.1.2
FA	eth0	172.24.1.14
CN	eth0	172.24.1.178

Para a realização da análise de desempenho, foi utilizado um *software* desenvolvido pelo departamento de engenharia elétrica da Universidade que realiza sincronismo, gera tráfego, coleta dados e analisa os dados coletados [13]. Este software funciona sobre uma filosofia cliente-servidor, sendo que os pacotes enviados para análise durante uma geração de tráfego seguem um caminho apenas de ida, de um servidor para um cliente. Com este programa, foram criados os tráfegos tanto auto-similar, para simulação de um ambiente *Internet* na rede de teste, quanto para a geração dos tráfegos cuja qualidade foi medida.

Para tráfegos gerados com este programa, ao tamanho do pacote especificado na configuração do tráfego, ainda deve se considerar o acréscimo dos cabeçalhos das camadas 3, 2 e 1 da pilha de protocolos. Para se obter medidas precisas, antes de se criar o tráfego e analisá-lo, deve-se sincronizar os dispositivos para que possam analisar os dados recebidos de forma adequada. As características que este software analisa a partir dos tráfegos recebidos são: atraso, que é o tempo que o pacote leva para chegar ao seu destino após ser gerado na origem; variação de atraso, que é um parâmetro muito importante para se avaliar a QoS de um sistema; a banda ocupada pelo tráfego que está sendo verificado e a perda de pacotes acumulada.

A escolha das taxas utilizadas no fluxo cujas características estavam sendo analisadas se fez pela escolha da taxa de duas codificações. A primeira codificação escolhida foi a codificação de voz em CELP [26, 24], resultando em um tráfego de 8kbps. A segunda codificação é a codificação CIF (Formato Intermediário Comum) a uma taxa de 256k que pode ser utilizada com os protocolos H.261 e H.323 para utilização de videoconferência sob qualidade de serviço [36]. Para que o sistema tenha uma qualidade de serviço muito boa, é necessário que apresente atraso menor que 150ms, variação de atraso menor que 20ms e perda de pacotes inferior a 1%. Para que seja uma qualidade baixa, mas aceitável, precisa ter atraso menor que 400ms, variação de atraso menor que 60ms e perda de pacotes menor que 5% [26].

A primeira fase apresentou, para 8kbps, um comportamento de banda constante, um atraso médio de 2,5ms com poucos picos acima de 7,5ms, uma variação de atraso que se manteve entre 0 e 1,5 com poucos picos acima de 5ms e sem perda de pacotes durante 100 segundos. Os gráficos que apresentam o comportamento do sistema para esta taxa estão apresentados nas figs. 2.42, 2.43, 2.44 e 2.45.

Figura 2.42 - Banda ocupada pelo tráfego de 8kbps na primeira fase do teste.

Na fig. 2.42, é verificado um gráfico que se mantém constante na maior parte do percurso, tendo apenas uma oscilação que aparenta ter sido causada por erro na marcação de tempo no programa. Na fig. 2.43, o gráfico apresenta um comportamento estável para a informação de atraso, mantendo uma média de 2,5 ms e variando entre 1,5 e 4ms. Os picos que são verificados tanto nos gráficos de atraso quanto nos gráficos de variação se devem a erros de sincronização que ocorriam esporadicamente no sistema. Estes valores, entretanto, podem ser descartados na análise dos resultados.

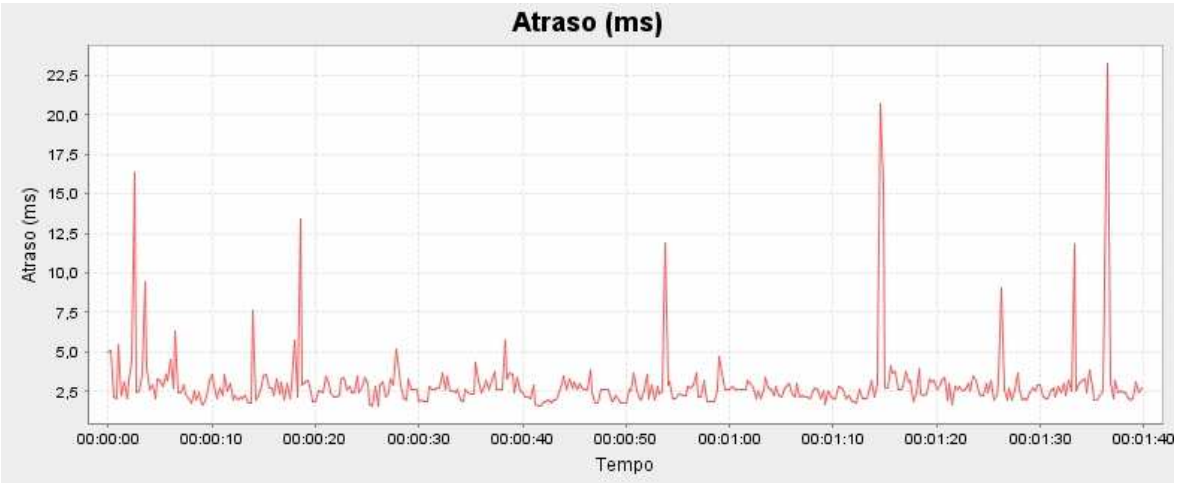


Figura 2.43 - Atraso do tráfego de 8kbps na primeira fase do teste.

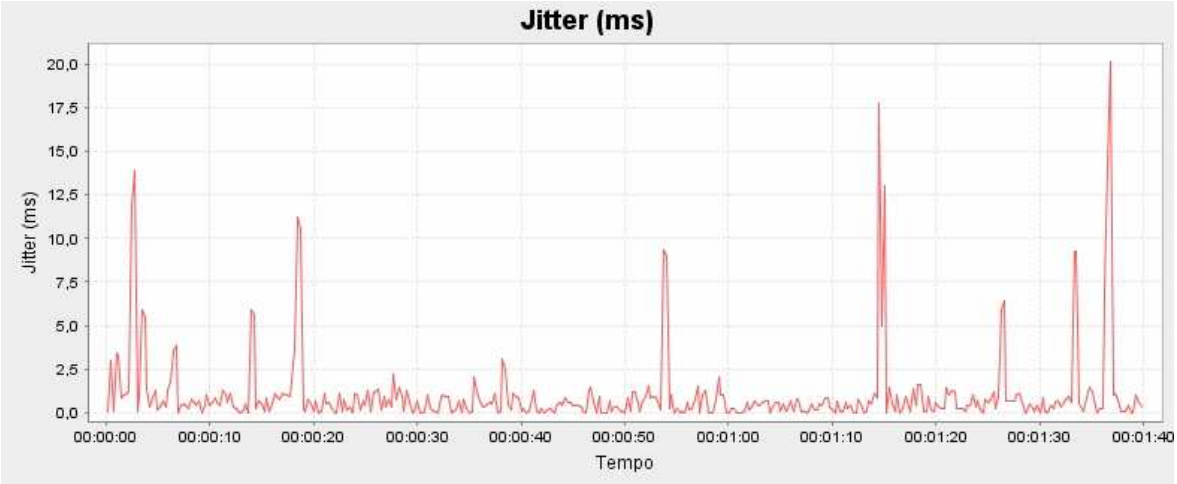


Figura 2.44 - Variação de atraso do tráfego de 8kbps na primeira fase do teste.

A variação de atraso esteve variando principalmente entre 0 e 1,5ms, como pode ser visualizado no gráfico da fig. 2.44 e a quantidade de pacotes perdidos nesta etapa dos testes foi nulo, como pode ser verificado na fig. 2.45.

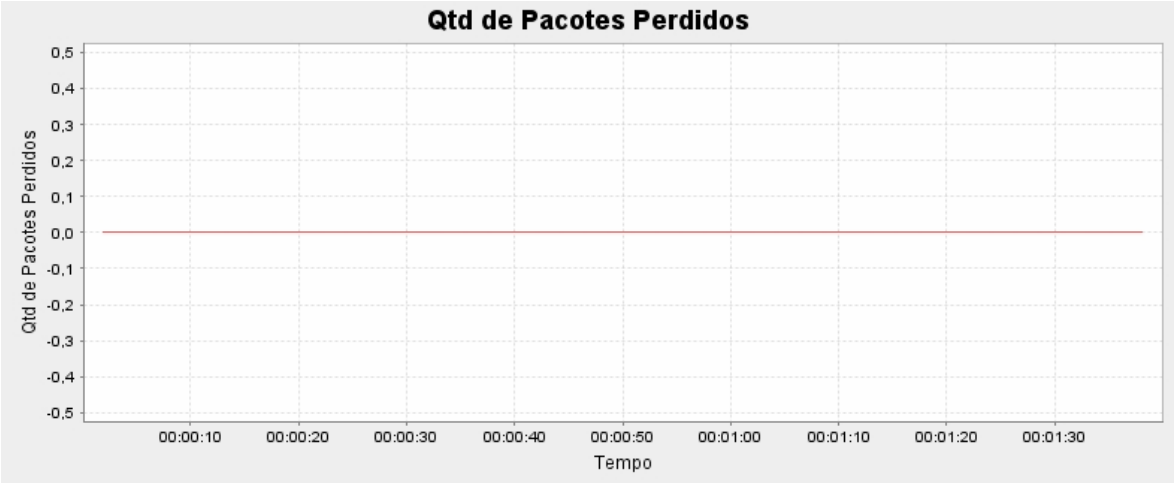


Figura 2.45 - Quantidade de pacotes perdidos na transmissão do tráfego de 8kbps na primeira fase do teste.

Com o tráfego de 256kbps, obtivemos uma taxa de transmissão oscilante, com atraso variando entre 1,5ms e 32ms; a variação de atraso esteve entre 0 e 4ms e uma perda de mais de 90 pacotes em 100 segundos de transmissão. Percebe-se então uma deterioração das características do tráfego de acordo com o aumento na sua taxa de transmissão. Os gráficos das características deste tráfego podem ser vistos nas figs. 2.46, 2.47, 2.48, 2.49, 2.50 e 2.51.

Figura 2.46 - Banda ocupada pelo tráfego de 256kbps na primeira fase do teste.

A taxa de transmissão, para esta taxa esteve oscilando entre 285kbps e 307kbps, mantendo uma média de aproximadamente 302kbps. O atraso, que pode ser visto na fig. 2.47 e com mais detalhes na fig. 2.48, esteve variando entre 1,5 e 32 ms.

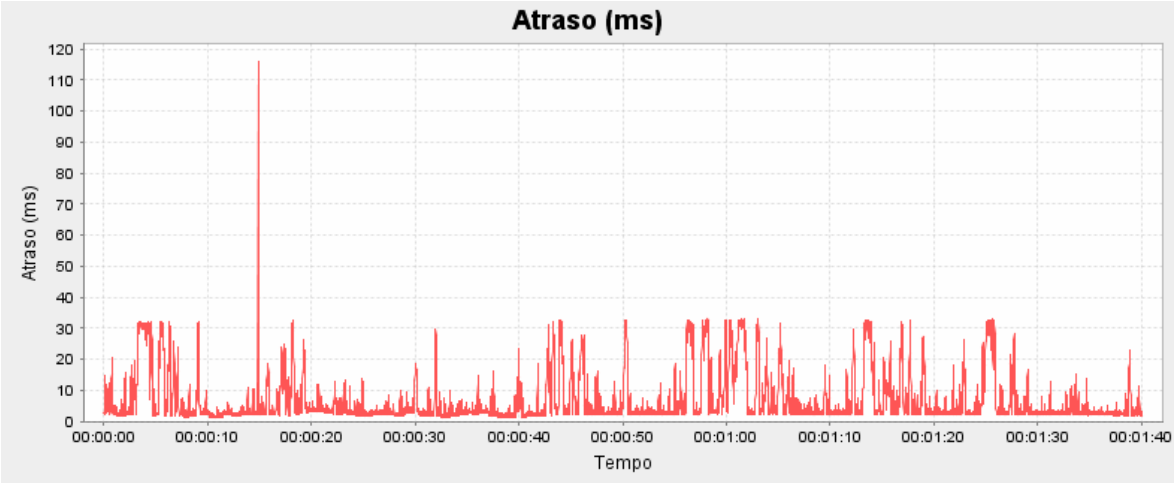


Figura 2.47 - Atraso do tráfego de 256kbps na primeira fase do teste.

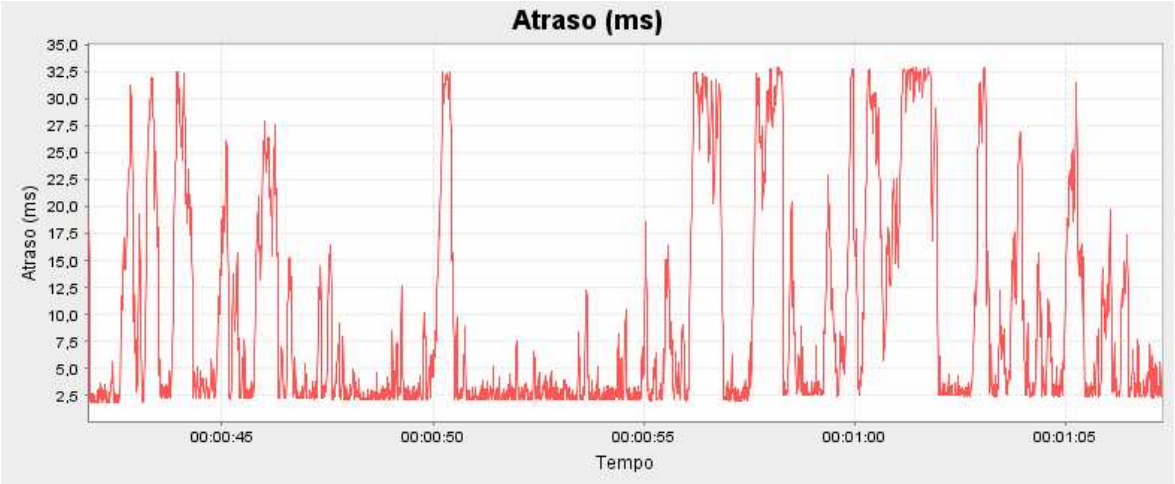


Figura 2.48 – Detalhes do atraso do tráfego de 256kbps na primeira fase do teste.

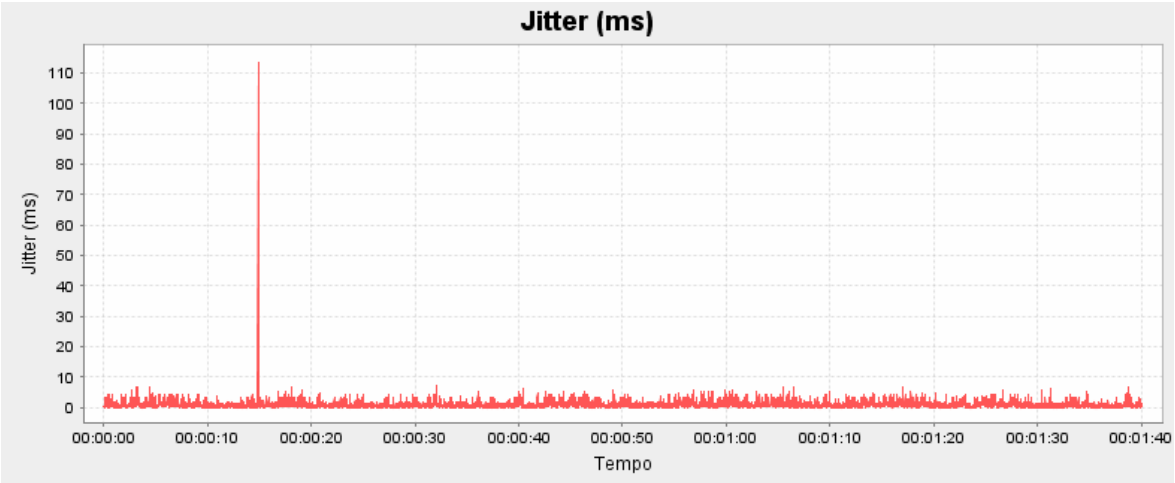


Figura 2.49 - Variação de atraso do tráfego de 256kbps na primeira fase do teste.

É verificado, através do gráfico apresentado na fig. 2.49 e 2.50, que a variação do atraso esteve entre 0 e 4ms. Na fig. 2.51, temos o gráfico da perda de pacotes acumulada, que apresenta uma perda maior que 90 pacotes em 100 segundos de teste.

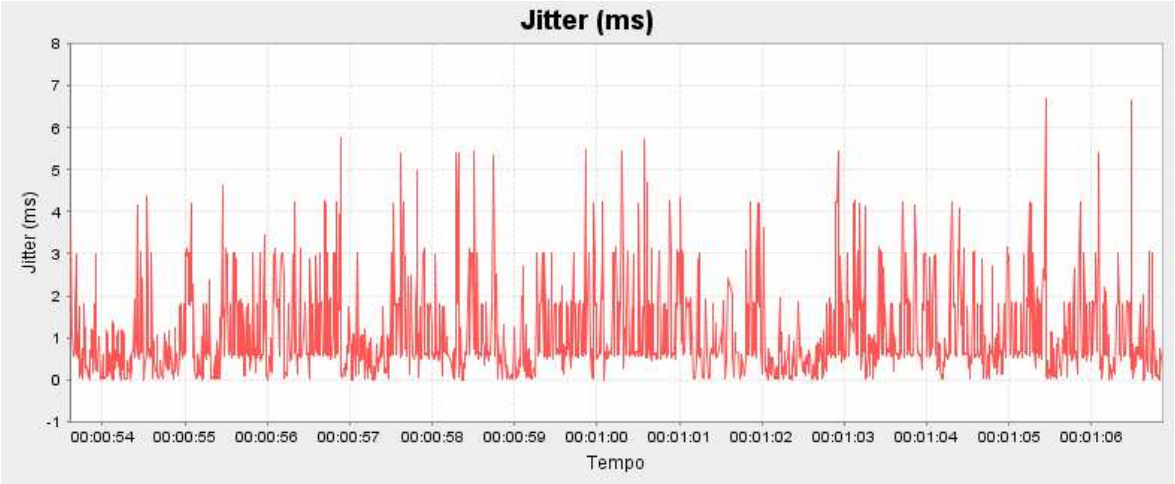


Figura 2.50 – Detalhes da variação de atraso do tráfego de 256kbps na primeira fase do teste.

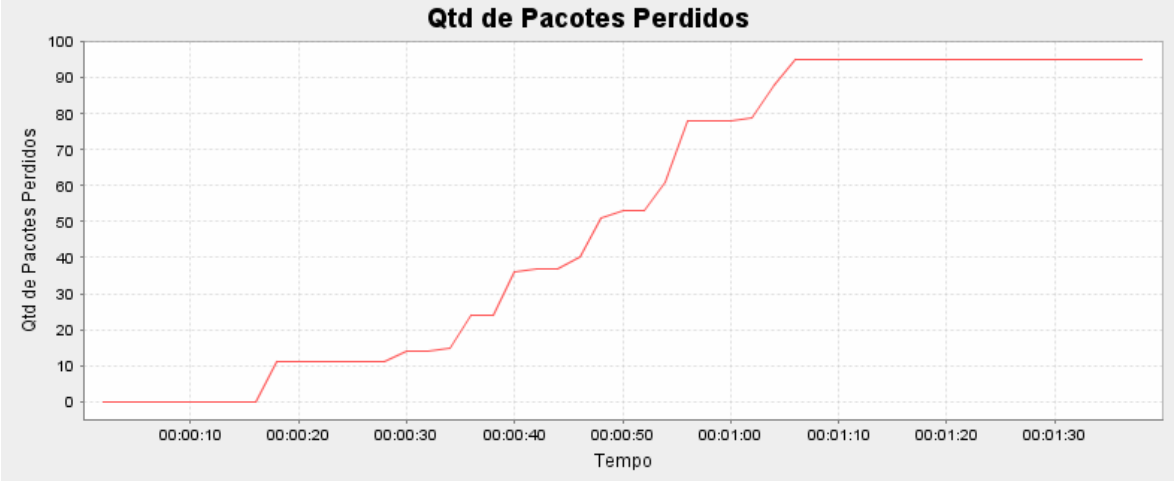


Figura 2.51 - Quantidade de pacotes perdidos na transmissão do tráfego de 256kbps na primeira fase do teste.

Na segunda etapa do teste, foi verificado que, para 8kbps, a taxa permaneceu constante; o atraso médio foi de 5ms com alguns picos de 7,5ms; a variação de atraso esteve entre 0 e 2ms com poucos picos maiores que 5ms; e não houve perda de pacotes. Para 256kbps, entretanto, teve-se uma taxa de transmissão oscilante, um atraso que esteve principalmente entre 4,5 e 12,5ms chegando até a 35ms com variação de atraso entre 0 e 4ms, e perda de aproximadamente 173 pacotes durante os 100s de transmissão. Os gráficos destas características de rede estão apresentados nas figs. 2.52 a 2.61.

Figura 2.52 - Banda ocupada pelo tráfego de 8kbps na segunda fase do teste.

É verificado novamente, para 8kbps uma taxa de transmissão constante em 9,6kbps. Na fig. 2.53, tem-se um atraso médio de 5ms distribuídos entre 4 e 6ms.

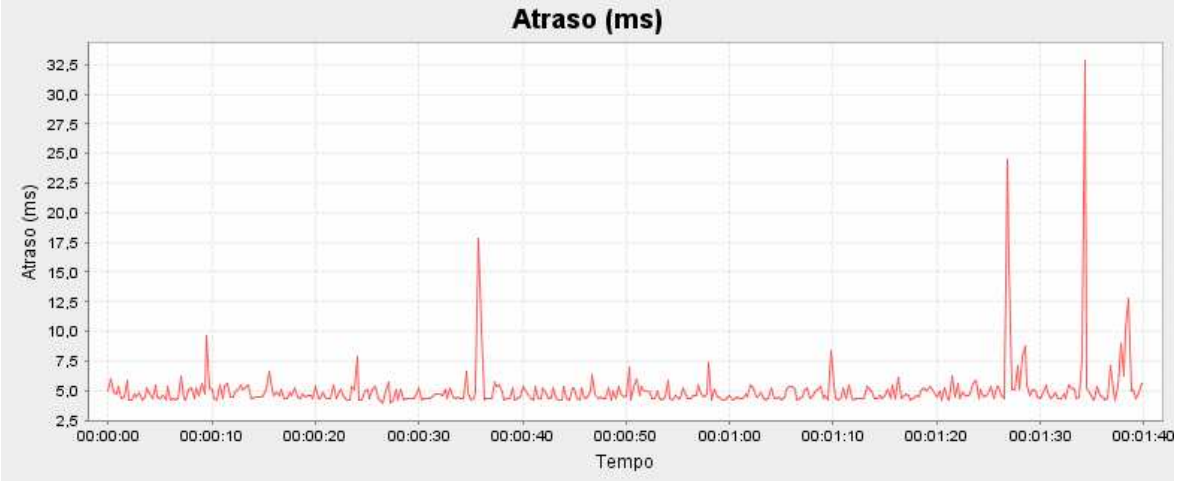


Figura 2.53 - Atraso do tráfego de 8kbps na segunda fase do teste.

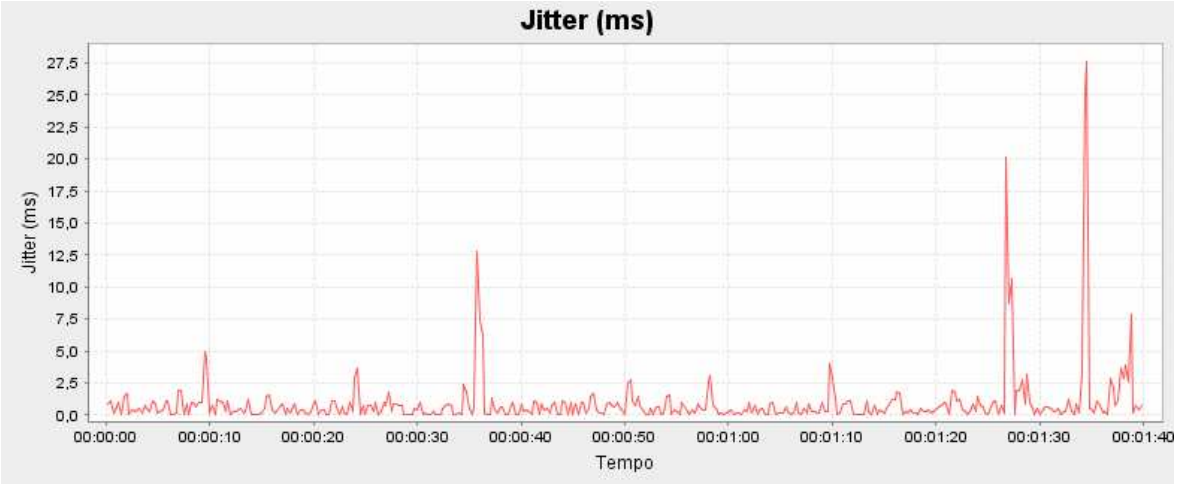


Figura 2.54 - Variação de atraso do tráfego de 8kbps na segunda fase do teste.

Foi verificada na fig. 2.54 uma variação de atraso que variou entre 0 e 2ms. Na fig. 2.55, encontrou-se um gráfico de demonstrou que nenhum pacote foi perdido durante esta fase dos testes com a taxa de 8kbps.

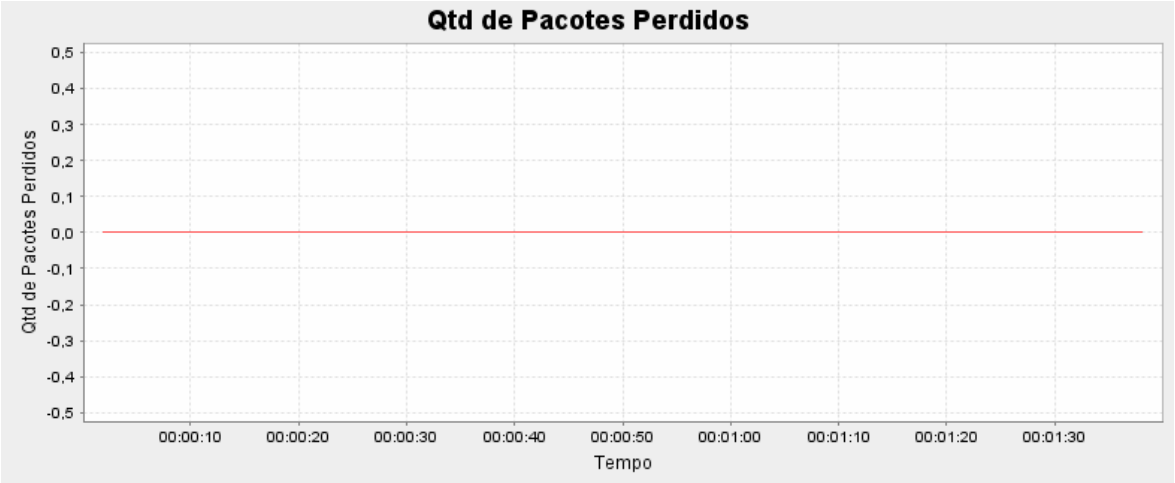


Figura 2.55 - Quantidade de pacotes perdidos na transmissão do tráfego de 8kbps na segunda fase do teste.

Figura 2.56 - Banda ocupada pelo tráfego de 256kbps na segunda fase do teste.

Para 256kbps na segunda fase do teste, foi verificada, através da fig. 2.56, uma taxa de transmissão que oscilou entre 265kbps e 310kbps, tendo como média aproximadamente 305ms. O atraso, nesta fase do teste, esteve em sua maior parte, distribuído entre 4,5ms e 12,5 ms, alcançando diversas vezes o valor de 32 ms.

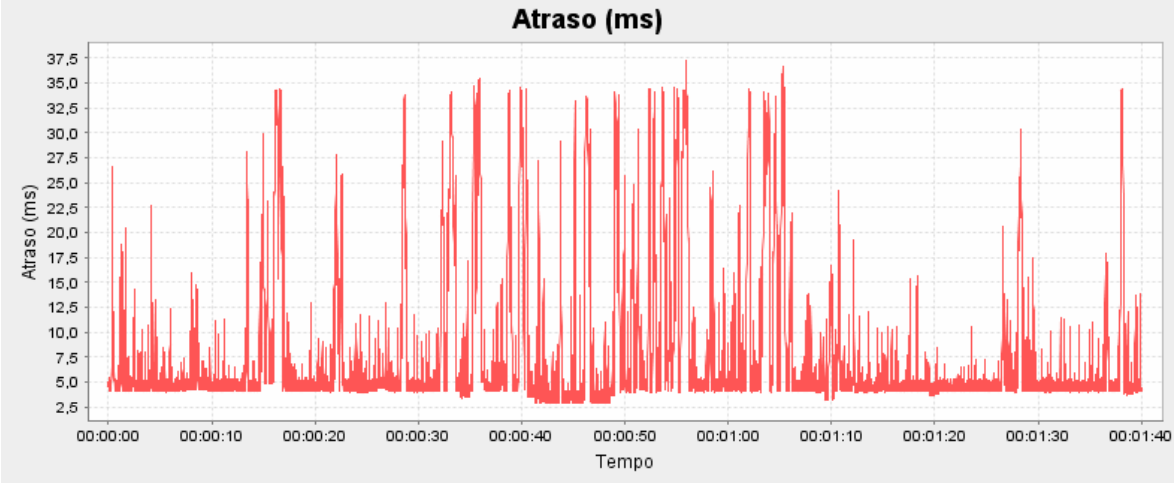


Figura 2.57 - Atraso do tráfego de 256kbps na segunda fase do teste.

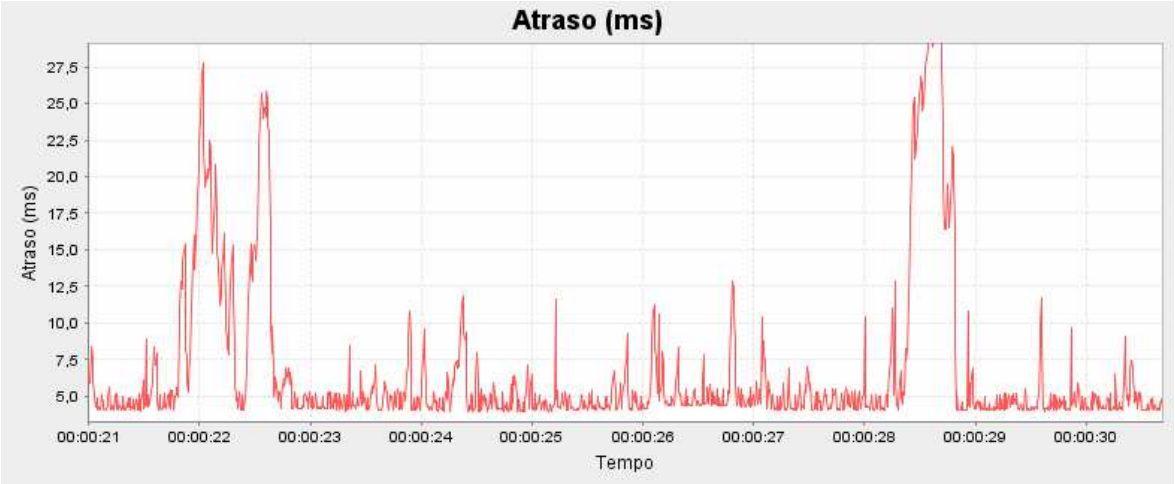


Figura 2.58 – Detalhes do atraso do tráfego de 256kbps na segunda fase do teste.

A variação de atraso, para 256kbps nesta etapa dos testes, variou entre 0 e 4ms, como apresentado nas figs. 2.57 e 2.58. Ocorreu, nesta fase, uma perda de pacotes acumulada maior que 170 pacotes durante 100 segundos de transmissão.

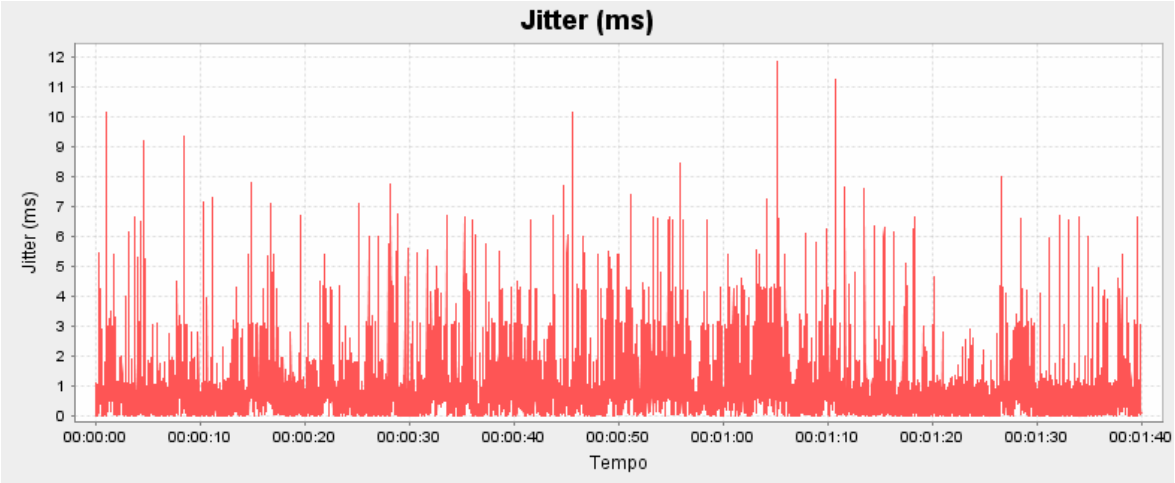


Figura 2.59 - Variação de atraso do tráfego de 256kbps na segunda fase do teste.

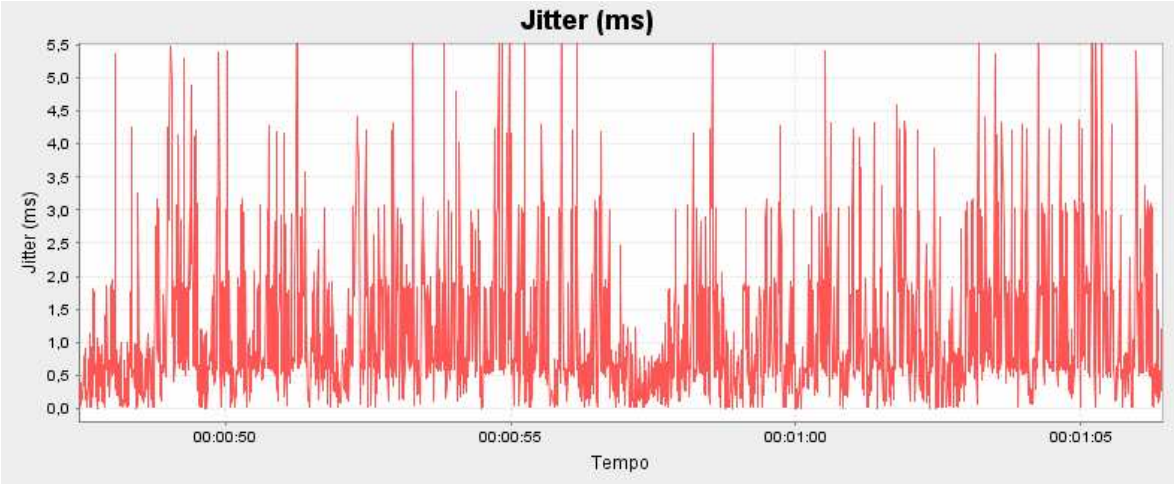


Figura 2.60 – Detalhes da variação de atraso do tráfego de 256kbps na segunda fase do teste.

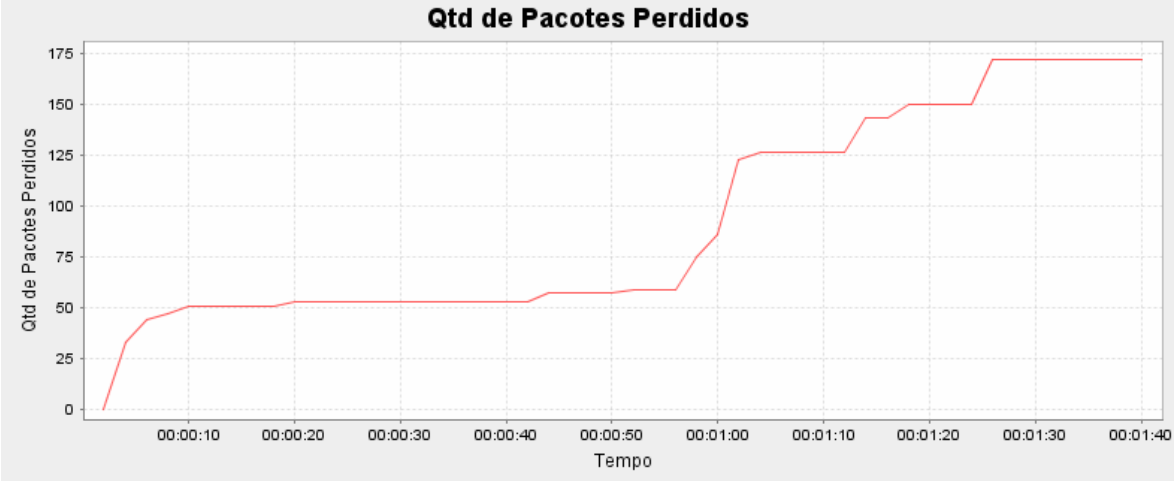


Figura 2.61 - Quantidade de pacotes perdidos na transmissão do tráfego de 256kbps na segunda fase do teste.

Ao utilizar o Mobile IP, o tráfego teve de passar pela rede que simula a Internet duas vezes. Uma saindo do nó correspondente e indo à rede nativa, e outra voltando encapsulado à rede estrangeira. Isto fez com que o atraso dobrasse de média de 2,5 a 5 ms. A variação de atraso sofreu deterioração também, mas se comparado com o atraso, a deterioração foi pouca. A banda permaneceu praticamente sob a mesma situação: constante para o tráfego de 8kbps e oscilante para 256kbps, embora a oscilação tenha sido maior na segunda etapa. A oscilação da banda utilizada pelo tráfego foi um reflexo da variação de atraso no sistema. A perda de pacotes teve uma piora significativa, passando de aproximadamente 95 a aproximadamente 173 pacotes em 100 segundos de teste com tráfego de 256kbps.

Apesar de não estar fora do padrão considerado aceitável para qualidade de serviço, os resultados encontrados demonstram que para taxas maiores, ou para situações em que a rede esteja sobre um estresse maior, o encaminhamento através da rede nativa do IP móvel pode ser um mecanismo que faça com que um sistema perca a qualidade de serviço.

2.7 - CONCLUSÕES SOBRE O IP MÓVEL

O IP móvel realmente proporciona a mobilidade sem necessidade de alterações na configuração das interfaces de rede, permitindo acesso aos recursos da rede como se o dispositivo estivesse em sua rede nativa tal como verificado nos testes de funcionamento, entretanto, no que diz respeito ao desempenho, existem dois problemas a serem trabalhados. O primeiro é o fato de que quando o agente estrangeiro está muito distante do agente nativo, ocorre uma perda considerável de desempenho devido ao fato de os pacotes obrigatoriamente passarem pelo agente nativo para depois serem encaminhados à atual localização do nó móvel. O outro é o tempo gasto para se fazer o registro durante um *handoff*; pois se o móvel se encontrar muito distante da rede nativa, pode causar um tempo demasiadamente alto para que o processo de registro pode ser feito.

Para resolver este segundo problema, deve-se procurar algoritmos ou ferramentas de micromobilidade, que permitam ao móvel fazer o registro com outros elementos, mais próximos à sua atual localização. O MIP hierárquico é um excelente exemplo desta micromobilidade. Para o primeiro, uma das formas mais simples de reduzir o problema é a utilização de algum mecanismo que aumente a eficiência do roteamento nos *backbones*. Um sistema capaz de ajudar neste aspecto é o MPLS (*Multiprotocol Label Switching* - multiprotocolo de comutação de rótulos), que reduz o tempo de atraso nos roteadores graças à sua comutação que exige baixo processamento para verificação do próximo enlace a ser seguido. Por este motivo, no capítulo seguinte será descrita a tecnologia MPLS e verificadas as vantagens da sua utilização neste projeto.

3 - MPLS

A Internet, nos últimos anos, tem apresentado um crescimento muito intenso, e inspirado o desenvolvimento de uma grande variedade de novas aplicações e serviços. Estes novos serviços, que em grande parte envolvem transmissão de voz e vídeo, normalmente produzem altas taxas de tráfego e necessitam de garantia de banda nos *backbones* da rede. A Internet se expandiu através da absorção e convergência desses serviços, entretanto a demanda gerada por todas estas aplicações e serviços tem sobrecarregado os recursos de banda e velocidade na infra-estrutura da *Internet*. Junto a esse problema, acrescenta-se também a necessidade cada vez maior de realizar a diferenciação no tratamento dos diversos serviços oferecidos para melhor atender cada tipo de serviço.

Como resposta a esse panorama, os provedores de serviço *Internet* e os administradores de grandes redes corporativas uniram esforços no sentido de encontrar soluções de baixo custo e eficientes para solucionar ou minimizar os problemas com relação à largura de banda, desempenho e escalabilidade das redes.

Os roteadores, que fazem parte da estrutura de uma rede IP comum permitindo flexibilidade e distribuição organizada dos endereços, sob elevadas taxas de tráfego se tornam pontos críticos. Este fato leva a utilização de comutadores com a intenção de melhorar o desempenho na transmissão de dados. Têm-se estudado novas formas de agregar as vantagens dos equipamentos de comutação às redes IP. Uma dessas formas é o MPLS (*Multiprotocol label switching* – Multi-protocolo de comutação de rótulos), que está sendo padronizado pelo IETF.

O MPLS propõe um método para gerar uma estrutura de comutação sob qualquer rede de datagramas, criando circuitos virtuais a partir das rotas organizadas pelos protocolos de roteamento da camada de rede. O nível de enlace é preservado, sendo possível aplicar o MPLS a redes *Ethernet*, ATM, *Frame Relay*, *Token Ring*. A comutação opera por intermédio de software, em uma camada que poderia ser considerada intermediária entre o nível de enlace e o de rede. Dessa forma, após gerar um circuito, uma rede MPLS processa o cabeçalho de rede de um pacote que trafegue nela apenas no primeiro roteador do caminho. Isto permite que os roteadores IP subseqüentes funcionem apenas como

gerenciadores dos circuitos de comutação, apresentando um desempenho melhor na passagem dos pacotes.

O paradigma de encaminhamento de mensagens usado no MPLS traz como vantagens a capacidade de ter o encaminhamento de mensagens por comutadores que não tem capacidade de processamento suficiente para analisar cabeçalhos de camada de rede em velocidade adequada; a utilização, no roteador de entrada, de qualquer informação do pacote, mesmo a porta de destino do pacote, para determinação da FEC (classe de envio equivalente — *Fowarding Equivalence Class* à qual o pacote deve ser atribuído; decisões de encaminhamento que dependem do roteador de entrada podem ser implementadas de forma muito mais simples do que em roteamento convencional; podem ser feitas considerações complexas e de alto custo computacional para se atribuir pacotes a FECs sem que isso cause impacto nos roteadores que encaminharão os pacotes rotulados; é possível forçar um pacote a seguir um determinado caminho definido explicitamente, que não necessariamente corresponde ao caminho que seria escolhido através de algoritmos de roteamento dinâmico, sem precisar que o pacote carregue uma identificação da rota definida; o MPLS é independente dos protocolos de comunicação da camada 2 e da camada 3; ele especifica mecanismos que gerenciam fluxos de tráfego de vários níveis, tais como fluxos de diferentes dispositivos, ou fluxos de diferentes aplicações; e é compatível com protocolos de roteamento existentes tais como o RSVP (*resource reservation protocol* — protocolo de reserva de recursos), OSPF (*open shortest path first* — protocolo de abertura do menor caminho primeiro) e BGP (*border gateway protocol* — protocolo de *gateway* de borda).

Este capítulo tem por objetivo, apresentar a tecnologia MPLS, apresentando o paradigma de comutação dos pacotes com base em rótulos, descrevendo o sistema apresentado nas especificações das RFCs. Busca-se ainda demonstrar as suas vantagens em relação ao roteamento IP e verificar a melhora de eficiência que e se pode obter pela sua utilização em um sistema Mobile IP.

3.1 - ESPECIFICAÇÃO DO MPLS

Desde 1995, começaram a ser feitas propostas de integração entre os protocolos baseados em roteamento sobre a estrutura de comutação da tecnologia ATM (*assynchronous transfer mode* — modo de transferência assíncrona). Os principais envolvidos nesta integração foram o ATM Fórum e o IETF. O objetivo que se pretendia alcançar era uma rede de fácil gerenciamento, com reserva de largura de banda, que satisfaz os requisitos de qualidade de serviço e tenha suporte nativo a multicast. Os primeiros resultados deste trabalho foram os protocolos MPOA *(multiprotocol over* ATM — multi-protocolo sobre ATM) e o I-PNNI (*integrated private network to network interface* — interface integrada rede para rede privada). A desvantagem destes protocolos é a sua elevada complexidade, que torna o gerenciamento e implementação do sistema difícil.

Em 1996, algumas empresas de informática passaram a propor soluções para a integração entre as redes comutadas e roteadas. A primeira destas propostas foi o IP Switching, desenvolvido pela Ipsilon. O IP Switching utiliza comutadores ATM, determinando fluxos de pacotes com endereços similares e verificando se tais fluxos devam ser roteados ou comutados. Outra proposta feita foi o Tag Switching, proposto pela Cisco, que adiciona um rótulo, que foi chamado *tag*, ao cabeçalho de cada pacote, permitindo a sua transmissão em circuitos virtuais. Este rótulo fez com que não fosse necessário uma análise das informações de roteamento em cada etapa do percurso, uma vez que a decisão do próximo nodo é baseada apenas no rótulo e não no conteúdo de cabeçalho dos pacotes. Outra vantagem deste sistema é o fato de suportar outros protocolos de nível 2 além do ATM. Apesar da utilização de rótulos, o Tag Switching não é baseado em fluxos. No final de 96, a Toshiba e a IBM criaram o Cell Switched Router (CSR) e o Aggregate Route-Based IP Switching (ARIS) respectivamente. Ambos são variantes do Tag Switching.

Em 1997 foi criado um grupo de trabalho (*working group*) no IETF específico para a especificação do MPLS. Em setembro de 1999 foi aprovada a primeira RFC deste grupo, a RFC2702 - *Requirements for Traffic Engineering Over MPLS*. Desde então já foram aprovadas outras 33 RFCs, totalizando 34 RFCs deste working group. Destes 34, 14 tratam do LDP (*label distribution protocol* - protocolo de distribuição de rótulos), que é o protocolo de distribuição de rótulos diretamente desenvolvido para a utilização pelo MPLS, entretanto o MPLS foi desenvolvido para aceitar gerenciamento dos seus túneis através de outros protocolos de roteamento, dos quais podemos citar o BGP, OSPF e RSVP.

3.2 - FUNCIONAMENTO DO MPLS

No MPLS, a cada pacote que entra na rede é atribuído uma classe de envio equivalente (*Fowarding Equivalence Class* — FEC). Esta atribuição utiliza um rótulo, que identificará a FEC. O rótulo é, então, inserido no cabeçalho e, em cada roteador por onde o pacote passar dentro da rede MPLS, ele será o único elemento a ser analisado para determinar o próximo roteador para onde deve ser encaminhado. O processo de análise do rótulo recebe o nome de permuta de rótulos (*label swapping*). Para realizar a permuta de rótulo, são analisados 4 bytes, que é o tamanho do rótulo. Em uma rede IP é analisado um cabeçalho de 20 bytes ou mais para se determinar o próximo roteador para onde enviar o pacote.

Em cada roteador por onde o pacote trafega, o roteador verifica qual o próximo nodo para onde deve encaminhar o pacote, e qual o próximo rótulo que deve ser utilizado neste pacote. Desta forma, o rótulo que é utilizado por uma determinada FEC muda de nó para nó. Isto é bom para facilitar a distribuição de rótulos em diferentes roteadores de borda em uma rede MPLS, e faz com que um rótulo utilizado em uma parte do túnel esteja disponível para ser utilizado em outra parte da rede MPLS.

3.2.1 - Rótulo

Após um pacote receber um rótulo, ele passa a pertencer a uma FEC e pode ser comutado. A atribuição de um rótulo pode ser feita em um campo do pacote que tenha sido criado especificamente para esta finalidade ou em um campo qualquer já existente no cabeçalho de rede ou de enlace, desde que esteja disponível, tal como representado na fig. 3.1. O cabeçalho das células ATM (nível 2), por exemplo, suportam rótulos nos campos de VCI / VPI (identificador de caminho virtual / identificador de circuito virtual), ou o cabeçalho do IPv6 (nível 3), no campo de fluxo de rótulos [50].

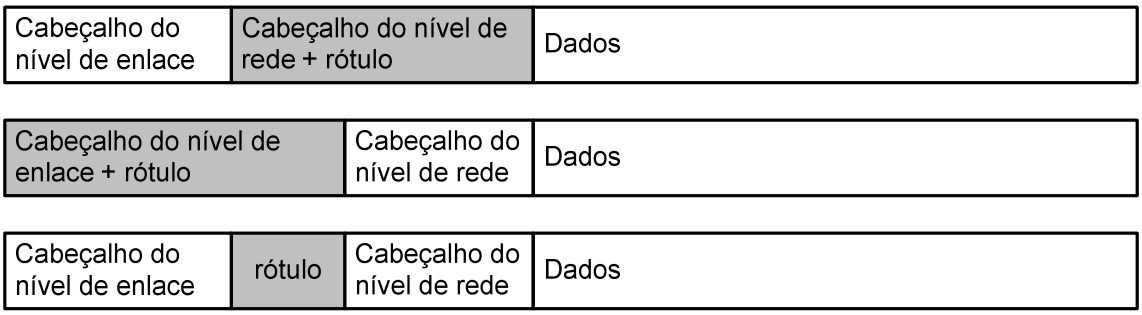


Figura 3.1 - Localização do label MPLS no cabeçalho da camada de enlace, rede ou entre o cabeçalho destes níveis

Um rótulo MPLS comum é formado por 4 bytes, e contém os campos rótulo, que é formado por 20 bits que contém o valor utilizado para identificar a FEC; o campo Exp, de 3 *bits*, que indica a classe de serviço do pacote e é utilizado no gerenciamento de filas de espera e rejeição; o campo B, que é um bit que marca o último rótulo antes do cabeçalho IP e é utilizado em hierarquia de rótulos, e o tempo de vida, que, assim como no cabeçalho IP, tem a finalidade de detectar *loops* [61]. O formato do rótulo está ilustrado na fig. 3.2.

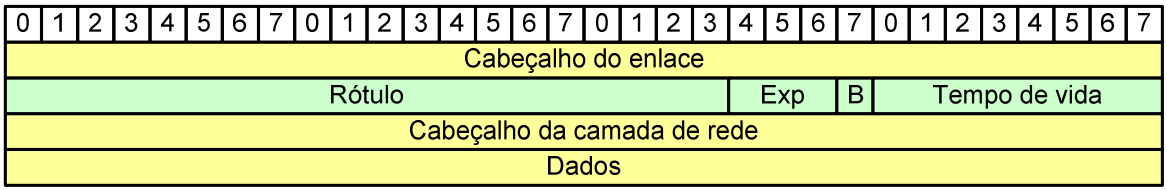


Figura 3.2 - Formato do rótulo MPLS.

3.2.2 - LER e LSR

Os dispositivos que participam de um sistema MPLS podem ser classificados em roteador de rótulo de borda (LER — *label edge router*) e roteador comutador de rótulo (LSR - *label switching router*). O LSR é um dispositivo do núcleo de uma rede MPLS que participa do estabelecimento de túneis LSP (*label switched path* — caminho comutado por rótulo) usando um protocolo de sinalização de rótulos adequado e comutando em alta velocidade o tráfego de dados baseado nos caminhos estabelecidos. O LER é um dispositivo que opera na borda entre a rede de acesso e a rede MPLS. O LER tem importância fundamental na atribuição e remoção de rótulos a medida que o tráfego entra e saí da rede MPLS. A fig. 3.3 ilustra a distribuição dos LER e LSR em uma rede MPLS.

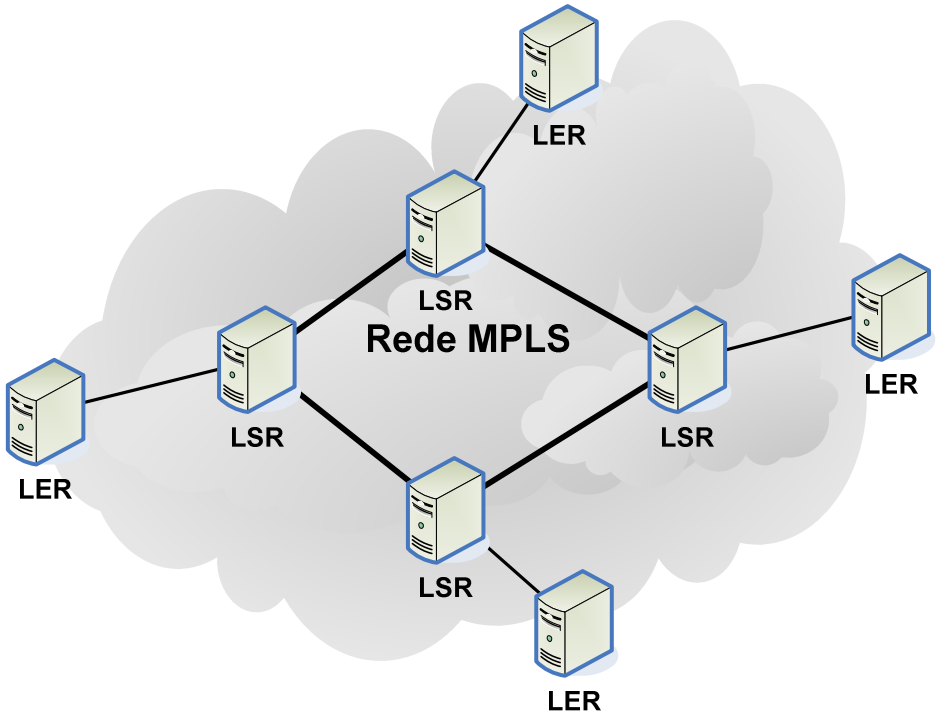


Figura 3.3 - LERs e LSRs em uma rede MPLS.

Quando dois LSRs concordam em usar um rótulo qualquer para indicar a transmissão de um para o outro com relação a uma FEC, o LSR emissor é considerado estar *upstream* na transmissão, e o LSR receptor é considerado estar *downstream*. Na especificação do MPLS, a determinação do rótulo sempre é feita pelo LSR *downstream* no caminho do pacote. A escolha do rótulo pode ser feita segundo uma requisição do LSR *upstream* ou diretamente através de iniciativa do LSR *downstream* no envio do pacote. Os protocolos de distribuição de rótulo são responsáveis pela troca de mensagens entre os LSRs no sentido de gerar as tabelas de rótulos. Cada vez que se associa um rótulo a uma FEC, este passa a ter certos atributos que são definidos também pelo protocolo de distribuição. A arquitetura MPLS suporta tipos de protocolo de distribuição de rótulos diferentes. Alguns outros protocolos de roteamento ou outros serviços tem inclusive sofrido modificações para padronizar mecanismos de indicação de rótulos, como o MPLS-BGP e o MPLS-RSVP.

3.2.3 - FEC, LIB e LSP

A classe de envio equivalente é a representação de um grupo de pacotes que compartilham as mesmas requisições de transporte. Todos os pacotes de um FEC recebem um mesmo tratamento no seu encaminhamento ao destino. Diferente do protocolo de roteamento IP, a

atribuição de um pacote a uma determinada FEC é feita apenas uma vez, quando o pacote entra na rede MPLS. Uma FEC pode ser determinada por um ou mais parâmetros, dentre os quais podemos citar: endereço IP de origem ou destino, porta de origem ou de destino, identificação do protocolo IP ou classe de serviço. Cada LSR cria uma tabela para especificar como um pacote deve ser encaminhado. Esta tabela é conhecida como base de informações de rótulos (*label information base* — LIB) e é composta por associações entre rótulos e FECs. A tabela 3.1 apresenta um exemplo de tabela LIB. Um LSR com esta tabela, ao receber um pacote com rótulo 3 na porta 1, terá este pacote enviado pela porta 3 com rótulo 6.

Tabela 3.1 - Exemplo de tabela LIB.

Porta de entrada	**Rótulo de entrada**	**Porta de saída**	**Rótulo de saída**
1	3	3	6
2	9	1	7

O caminho comutado por rótulo (*label switched path* — LSP) consiste em um caminho por onde os pacotes de uma determinada FEC irão passar dentro da rede MPLS. Cada FEC define um LSP, isto é, ao receber um pacote, o roteador de entrada LER da rede MPLS verifica a qual FEC o pacote pertence e o encaminha através da LSP correspondente. Novos LSPs são criados apenas com a criação de novas FECs, o que acontece apenas na borda da rede. Visto que a criação de LSPs somente ocorre na entrada de uma rede MPLS, os demais roteadores, os LSR, apenas chavearão os rótulos encaminhando o pacote de acordo com a LSP pré-determinada, não precisando mais fazer um roteamento dos pacotes. Os rótulos são distribuídos no momento do estabelecimento das LSPs. Um LSP é unidirecional, portanto, para se estabelecer uma comunicação bidirecional entre dois dispositivos é necessário estabelecer dois LSPs. Um para a comunicação em um sentido e outro para a comunicação no sentido contrário [27].

3.2.4 - Protocolos de distribuição de rótulos

Para o estabelecimento de túneis LSPs, é necessário a utilização de um conjunto de procedimentos pelos quais um LSR informa outro sobre a associação rótulo/FEC que está sendo feita. Este conjunto de procedimentos é conhecido como protocolo de distribuição

de rótulos. Dois LSRs que trocam informações de associações rótulo/FEC através de protocolo de distribuição de rótulo são chamados pares de distribuição de rótulos.

A arquitetura do MPLS definida na RFC 3031 [55] não assume apenas um único protocolo de distribuição de rótulos. Diversos protocolos de roteamento existentes como o RSVP e OSPF são suportados pelo MPLS e alguns tiveram extensões padronizadas para se obter maior qualidade no MPLS, tal como o RSVP-TE, e houve também protocolos desenvolvidos especialmente para execução em MPLS tal como o LDP (*label distribution protocol* — protocolo de distribuição de rótulos) e o CR-LDP (*constraint-based routing* LDP — LDP de roteamento baseado em coação).

3.2.4.1 - LDP

O protocolo LDP é um conjunto de procedimentos e mensagens pelos quais os LSRs estabelecem LSPs através da rede por mapeamento de informações de rotemento da camada de rede para os caminhos comutados da camada de enlace [8]. O LDP associa uma FEC com cada LSP que ele cria. Dois LSRs que usam LDP para trocar informações de mapeamento rótulo/FEC são chamados pares LDP e entre eles existe uma seção LDP. Uma única seção LDP permite cada par conhecer o mapeamento de rótulos do outro, tornando assim, o protocolo LDP bi-direcional. Existem quatro categorias de mensagens LDP: mensagens de descoberta, usadas pelos LSRs para indicar sua presença na rede; mensagens de seção, usadas para estabelecer, manter e terminar seções entre pares LDP; mensagens de anúncio, usadas para criar, alterar e excluir mapeamento de rótulos para os FECs; e Mensagens de notificação, usadas para prover informações para consultas e informações de erro de sinalização.

Os LSRs informam sua presença na rede enviando mensagens Hello, que são mensagem de descoberta, periodicamente para todos os roteadores da sub-rede. Se um LSR decide estabelecer seção com outro LSR encontrado através de mensagens Hello, ele utilizará o procedimento de inicialização LDP sobre transporte TCP. Ao completar com sucesso o procedimento, os dois LSRs serão pares LDP e podem trocar mensagens de anúncio. Com exceção das mensagens de descoberta, que usam protocolo UDP, as mensagens de

sinalização do LDP utilizam protocolo TCP para garantir entrega de mensagens confiável e em ordem.

Existem duas formas de se distribuir uma associação FEC/rótulo: enviando a associação em resposta a uma requisição explicita de outro LSR, na chamada distribuição de rótulo em demanda; ou enviando a associação para LSRs que não os solicitaram explicitamente, na chamada distribuição não-solicitada.

Na distribuição em demanda, ao necessitar de um túnel LSP, o LER de entrada envia uma mensagem de requisição de rótulo ao próximo LSR no caminho ao LER de saída do túnel. Cada LSR que recebe a requisição encaminha a requisição ao próximo nó. Quando a requisição chega ao LER de saída, este gera uma mensagem de mapeamento de rótulo e a envia em resposta à requisição. Novamente a mensagem é enviada nó a nó até chegar ao LER de entrada. Se for utilizada a distribuição não-solicitada, o processo ocorre diretamente com o envio nó a nó da mensagem de mapeamento de rótulo. As figs. 3.4 e 3.5 ilustram a distribuição em demanda e a não-solicitada, respectivamente.

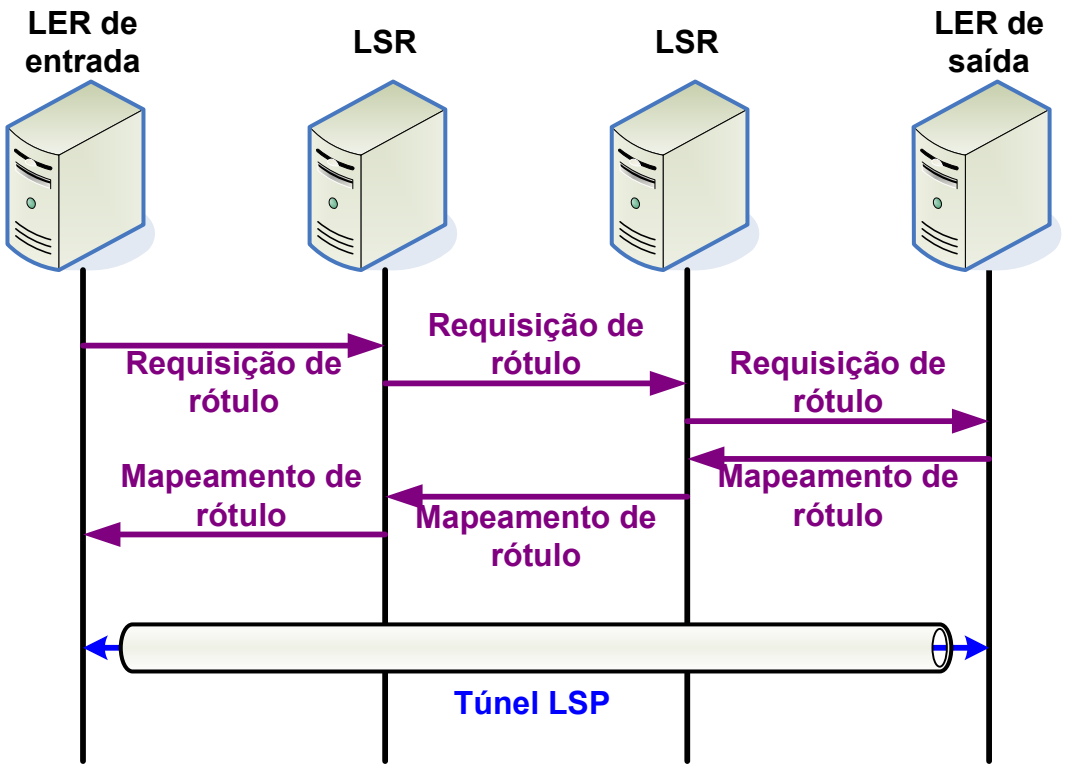


Figura 3.4 - Distribuição de rótulos em demanda usando LDP.

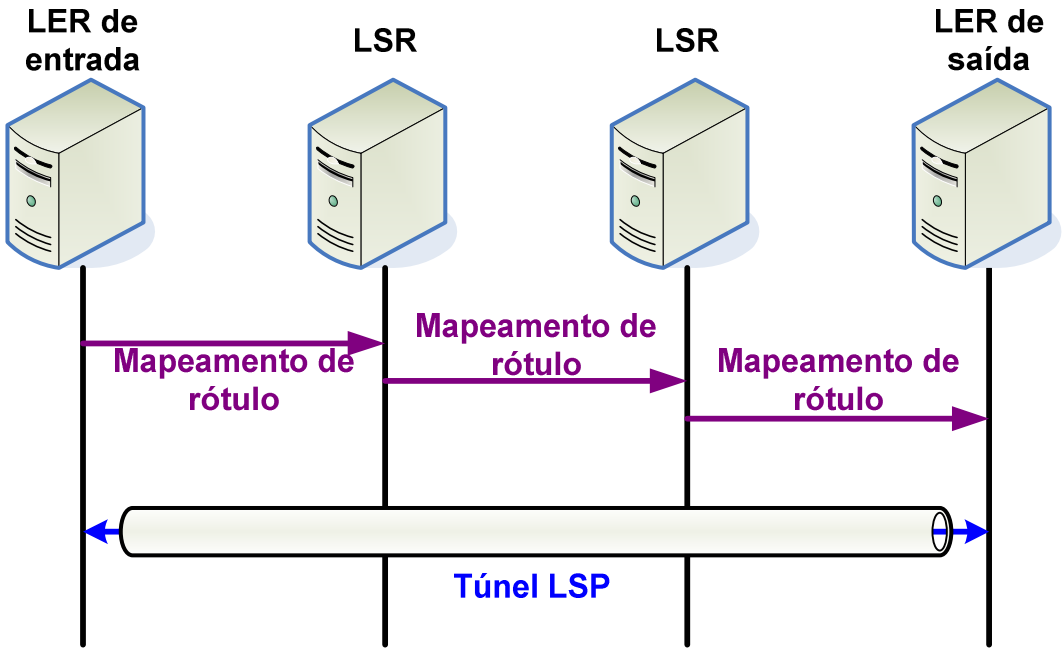


Figura 3.5 - Distribuição de rótulos não-solicitada usando LDP.

3.2.4.2 - CR-LDP

Roteamento baseado em coação (*Constraint-based routing* — CR) oferece a oportunidade de criar rotas de encaminhamento de pacotes que não seriam encontradas através dos protocolos de roteamento. CR é um mecanismo que pode ser utilizado para alcançar os requisitos de engenharia de tráfego. O CR-LDP é uma extensão do LDP para suportar caminhos comutados por rótulos com roteamento baseado em coação [34].

O CR-LDP incorpora novos parâmetros ao LDP, mantendo o mesmo formato de pacote que havia no LDP. O parâmetro mais importante adicionado é o parâmetro ER (*explicity route* — roteamento explicito), que é anexado a uma mensagem de requisição de rótulo e contém uma lista que identifica a seqüência de LSRs que farão parte do novo LSP a ser criado. Outro parâmetro que também é introduzido pelo CR-LSP é o parâmetro TP (*traffic parameters* — parâmetros de tráfego), cuja função é dimensionar as características de tráfego do LSP.

Outros recursos foram adicionados como a capacidade inequívoca de identificação de cada LSP no domínio (através do parâmetro LSPID), além da possibilidade de fixar todos os nós

de um determinado LSP, o que impede que este LSP passe por outros nós que não os explicitados.

A criação de um LSP com parâmetro ER acontece pelo mapeamento de um determinado fluxo em uma FEC com intervenção direta de um operador no LER de entrada, formando um novo LSP que atravesse uma seqüência específica de roteadores até o LER de saída. Então, o roteador de borda de entrada envia uma mensagem de requisição de rótulo com parâmetro ER com a seqüência dos LSRs que farão parte do LSP, e envia a mensagem para o próximo nó, que é o primeiro na seqüência dos LSRs contidos no parâmetro ER. O LSR, ao receber a mensagem, verifica a sua identificação na relação de nós do ER, retira a sua identificação da relação e envia a requisição para o próximo nó. Cada LSR no percurso ao LER de saída repete a mesma ação, e ao chegar ao LER de saída, este responde a requisição com um mapeamento de rótulo, que faz o percurso inverso, passando por todos os roteadores até atingir o LER de entrada, estabelecendo então o LSP.

Se for desejado que o LSP possua algum requisito especial de reserva de recursos, o CR-LSP utiliza o parâmetro TP na mensagem de requisição de rótulo informando o perfil de tráfego do LSP a ser estabelecido, como taxa de dados médio, taxa máxima, tamanho da rajada e outros. Esses dados servem para que os LSRs modelem o tratamento que darão ao fluxo, o que se refletirá no tipo de enfileiramento dos pacotes e na largura de banda reservada para o LSP que está sendo criado.

3.2.4.3 - BGP

O protocolo de *gateway* de borda (BGP) é um protocolo de roteamento entre sistemas autônomos (AS — *autonomous system*) [52]. A definição de sistema autônomo para o protocolo BGP é um conjunto de roteadores sobre uma única administração técnica, usando um protocolo interno para pacotes dentro do AS e um protocolo externo para rotear os pacotes para outros ASs.

A função primária de um sistema BGP é trocar informações de alcance de rede com outros sistemas BGP. Esta informação de alcance de rede inclui uma lista de sistemas autônomos

que a informação de alcance atravessou. Esta informação é suficiente para construir um grafo da conectividade pelo qual *loops* podem ser evitados.

O BGP utiliza o protocolo TCP para garantir o transporte confiável de seus pacotes, eliminando assim a necessidade de implementar sistema com retransmissão, notificações de recebimento, fragmentação e ordenação de pacotes. Dois sistemas BGP iniciam uma conexão TCP entre eles e enviam, um para o outro, toda a informação da tabela de roteamento BGP. Outras informações são enviadas apenas quando a tabela de roteamento é alterada. Para assegurar que a conexão está ativa, são enviadas periodicamente mensagens KeepAlive.

Quando o BGP é usado para distribuir uma rota particular, ele também pode ser usado para distribuir rótulos MPLS que são mapeados para a rota que está sendo distribuída [53]. A vantagem desta distribuição de rótulo se faz quando dois LSRs adjacentes são também pares BGP, podendo ser feita a distribuição de rótulos sem a necessidade de outro protocolo de distribuição de rótulo. A distribuição de rótulos com o BGP é feita pela inclusão do rótulo nos atributos de uma extensão e sendo indicado no campo identificador da família de endereços que o atributo contém um rótulo.

3.2.4.4 - OSPF

O protocolo OSPF é classificado como um protocolo de roteamento interno, isto é, ele distribui informações de roteamento entre roteadores pertencentes a um único sistema autônomo [40]. Este protocolo foi desenvolvido expressamente para ambiente *Internet*, incluindo suporte explicito para sub-redes e roteamento baseado em tipo de serviço. O OSPF também provê autenticação para atualizações de rotas e utiliza *multicast* IP no envio e recepção das atualizações. Ele é um protocolo dinâmico, que busca detectar mudanças de topologia no AS de forma rápida e calcular novas rotas sem loops após um período de convergência. Este período de convergência é curto e envolve um mínimo de roteamento de tráfego.

O OSPF encaminha pacotes IP baseado apenas no endereço IP de destino e tipo de serviço encontrados no cabeçalho IP da mensagem. Todos os roteadores OSPF rodam o mesmo

algoritmo em paralelo. Do banco de dados da topologia, cada roteador constrói uma árvore de menores caminhos com a raiz sendo ele mesmo. Esta árvore provê a rota para cada destino no sistema autônomo. Quando um roteador detecta uma mudança na topologia do AS, este envia uma mensagem com a atualização da topologia para os roteadores adjacentes, que encaminham a mensagem por todos os outros enlaces com exceção do enlace por onde a mensagem chegou. Este método é chamado de inundação (*flooding*). Em seguida, todos os roteadores calculam novamente a partir da base de dados atualizada a nova árvore de menores caminhos.

3.2.4.5 - RSVP

O protocolo RSVP é usado por um dispositivo para solicitar qualidades de serviços especificas da rede para fluxos de dados de aplicações específicas [11]. RSVP também é utilizado por roteadores para entregar requisições de qualidade de serviço para todos os nós ao longo do caminho de um fluxo e para estabelecer e manter a qualidade de serviço solicitada. requisições RSVP normalmente resultam em recursos sendo reservados em cada nó ao longo do percurso dos dados.

RSVP solicita recursos para fluxo *simplex*, isto é, ele requer recursos em apenas uma direção. Ele trata um remetente diferente de um destinatário, apesar de que algumas aplicações possam usar um mesmo dispositivo como remetente e destinatário ao mesmo tempo. O RSVP opera sobre o IPv4 ou o IPv6, ocupando o lugar do protocolo de transporte na pilha de protocolos. O protocolo de reserva de recursos não é um protocolo de roteamento, ele é desenvolvido para operar com protocolos de roteamento tanto *unicast* quanto *multicast*, consultando a tabela de roteamento para obter a rota para a qual enviar os pacotes.
´

Existem dois tipos fundamentais de mensagens RSVP: mensagens Resv e mensagens Path. Quando se pretende fazer um fluxo de dados, o remetente dos dados envia uma mensagem Path ao destinatário, roteando pelo protocolo de roteamento disponível. Em cada roteador por onde as mensagens Path atravessam, é armazenado um estado, que inclui o endereço do roteador do nó anterior, o qual é usado para enviar a mensagem Resv no sentido reverso.

O receptor, após receber a mensagem Path, responde com uma mensagem Resv, solicitando a reserva de recursos. A mensagem Resv deve atravessar exatamente o caminho reverso da mensagem Path. Os roteadores por onde esta mensagem passa então entram no estado de reserva, e reservam os recursos solicitados para o fluxo específico para o qual o remetente gerou a mensagem Path.

3.2.4.6 - RSVP-TE

Para poder suportar engenharia de tráfego em ambiente MPLS, foi desenvolvida uma extensão do protocolo RSVP, que ficou conhecida como RSVP-TE [9]. Esta extensão suporta a criação de rotas LSPs explicitas com ou sem reserva de recursos além de suportar re-roteamento suave de LSPs e detecção de *loops*. O protocolo de sinalização utiliza a distribuição de rótulos em demanda. Uma requisição para associação de rótulos para um túnel LSP específico é iniciada por um LER de entrada com uma mensagem Path. Por este motivo, à mensagem Path, foi acrescentado uma requisição de rótulo. Os rótulos são alocados e distribuídos por meio de mensagens Resv, que foi estendida com o acréscimo do rótulo.

O protocolo de sinalização também suporta capacidade de roteamento explicito através da incorporação de um objeto chamado EXPLICIT_ROUTE à mensagem Path. Este objeto encapsula uma concatenação de nós que constituem o caminho explicito. Usando este objeto, o caminho tomado pelos fluxos comutados por rótulo podem ser pré-determinados, independente do roteamento convencional. A rota explicita pode ser especificada manualmente por um administrador ou computada automaticamente por uma entidade baseando-se nos requisitos e políticas de QoS.

Para criar um túnel LSP, o primeiro nó MPLS no caminho cria uma mensagem Path com um tipo de seção LSP_TUNNEL_IPv4 e insere uma requisição de rótulo nesta mensagem. Esta requisição indica que a requisição de um rótulo associado a este caminho. Se o remetente souber de uma rota que alcança os requisitos de QoS do túnel, ou que satisfaz os critérios de política definidos, ele pode acrescentar um objeto EXPLICIT_ROUTE para especificar a rota que ele pretende utilizar. Se, depois de uma seção ser estabelecida com

sucesso, o remetente descobrir uma rota melhor, ele pode dinamicamente re-rotear a seção, alterando o objeto EXPLICIT_ROUTE.

A mensagem Path é encaminhada nó a nó seguindo a lista concatenada de nós especificados no objeto EXPLICIT_ROUTE ou através dos nós definidos por protocolo de roteamento dinâmico até chegar ao LER de saída, que responde com uma mensagem Resv que contém um objeto rótulo. A mensagem Resv é enviada de volta pelo caminho reverso ao feito pelo Path. Cada nó por onde a mensagem Resv passar utilizará o objeto rótulo para associar o rótulo definido na mensagem com o túnel LSP. Quando a mensagem Resv chega ao LER que enviou o Path, o túnel LSP está estabelecido com sucesso.

As mensagens RSVP são compostas por uma lista de objetos. Na fig. 3.6, é apresentada a seqüência de objetos presentes na mensagem Path. Os objetos em verde são os objetos obrigatórios e os marcados em amarelo são objetos opcionais. A fig. 3.7 apresenta a seqüência de objetos presentes na mensagem Resv, utilizando o mesmo padrão de cores para diferenciar os objetos obrigatórios dos opcionais. O processo de estabelecimento de um túnel com RSVP-TE pode ser visto na fig. 3.8

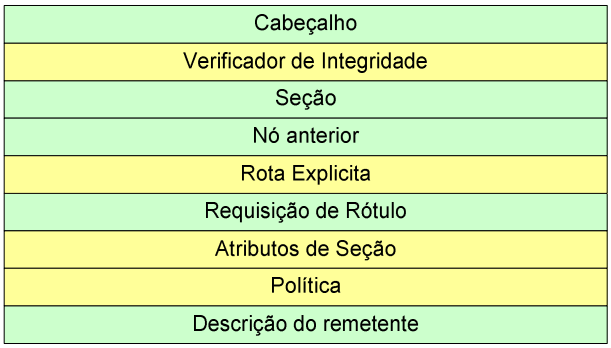


Figura 3.6 - Objetos da mensagem Path.

Cabeçalho
Verificador de Integridade
Seção
Nó seguinte
Tempo
Confirmação Resv
Escopo
Política
Estilo
Lista descritora de fluxos

Figura 3.7 - Objetos da mensagem Resv.

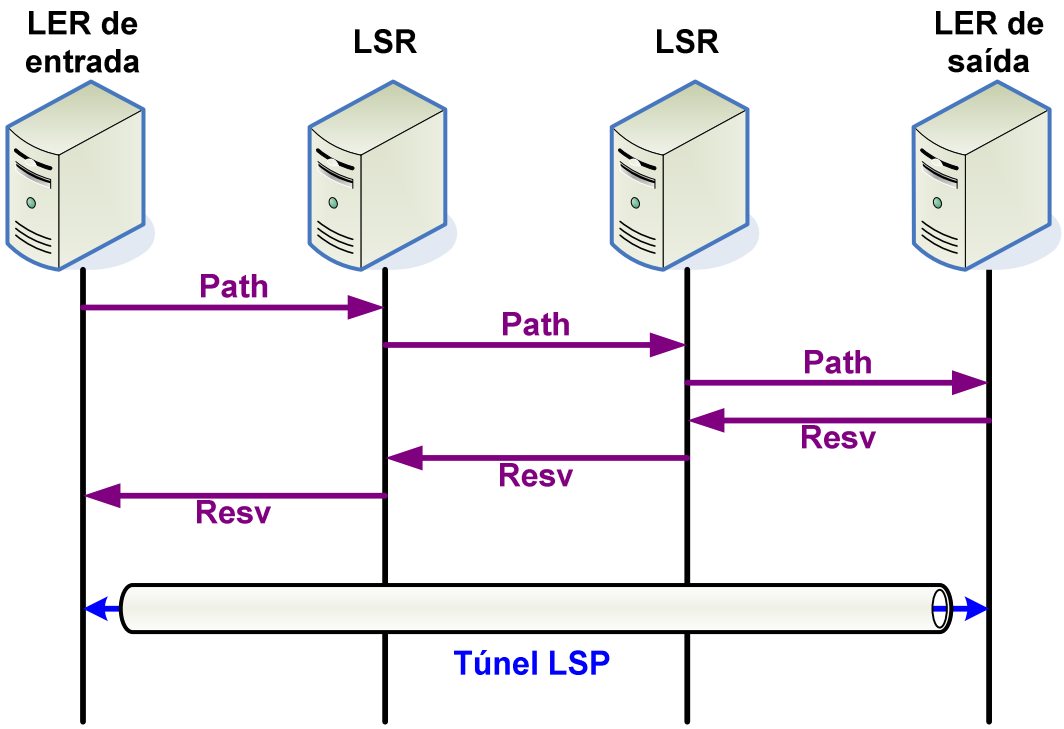


Figura 3.8 - Processo de estabelecimento de um túnel LSP através do protocolo RSVP.

3.3 - IMPLEMENTAÇÕES DO MPLS

Dentre as implementações realizadas, podemos citar:

- MPLS for Linux, que está sendo desenvolvido no SourceForgeNet, é muito voltada ao protocolo LDP, que é a implementação usada neste trabalho;
- NIST Switch, que é uma implementação desenvolvida para Linux e FreeBSD voltada principalmente para o tunelamento por meio do RSVP-TE;

- Implementação realizada pela Universidade de Cambridge, também voltada para Linux;
- Implementação realizada pelo Ayame Project, desenvolvida para NetBSD;
- Implementação desenvolvida pelo IIT Bombay, também voltada para Linux e para LDP;
- Implementação desenvolvida pela Atlantis, baseada na implementação da SourceForgeNet, que utiliza RSVP-TE com aplicação de DiffServ.

Dentre todas as implementações encontradas, as que demonstraram serem mais adequadas foram a implementação da SourceForgeNet [37], devido ao fato de ter código livre com licença GPL, ser desenvolvida para linux e a implementação da Atlantis [31, 32], que também é para linux e se baseia no núcleo MPLS desenvolvida na SouceForgeNet. Visto que esta última foi a mesma implementação utilizada no laboratório de comunicações da UnB (LABCOM), já tendo sido testada tanto quanto ao funcionamento quanto no desempenho [3, 4, 5, 6, 7], e também o fato de utilizar o RSVP-TE, que foi o protocolo de distribuição de rótulos escolhido para fazer a integração entre o Mobile IP e o MPLS, como será visto no capítulo seguinte, esta foi a implementação selecionada para este trabalho.

Esta implementação é composta de diversos elementos. O *patch* para *kernel* 2.4.19 do linux, baseado no *patch* desenvolvido pela SourceForgeNet é o que permite os dispositivos realizarem o chaveamento por rótulos. A implementação ainda conta com o Zebra, que é um conjunto de *daemons* e ferramentas que podem ser utilizados para controle do roteamento, como é o caso do OSPF, que encontra os menores caminhos para o roteamento de um pacote. E a implementação ainda disponibiliza o RSVP-TE para criação de LSPs com reserva de recursos e suporte a DiffServ.

3.4 - INSTALAÇÃO E VERIFICAÇÃO DE FUNCIONAMENTO DO MPLS

A instalação do sistema se inicia pela recompilação do *kernel* do linux com o *patch* do MPLS em todos os dispositivos que farão parte da rede MPLS. Deve-se posteriormente criar as rotas, ou utilizar algum protocolo que as crie automaticamente. Caso seja escolhida

a utilização de criação de rotas automaticamente, pode-se optar pelo OSPF, disponibilizado no Zebra. E por fim a instalação do RSVP.

Para se validar a instalação e funcionamento do MPLS com RSVP, foi montado o ambiente apresentado na fig. 3.9 com os endereços utilizados na tabela 3.2.

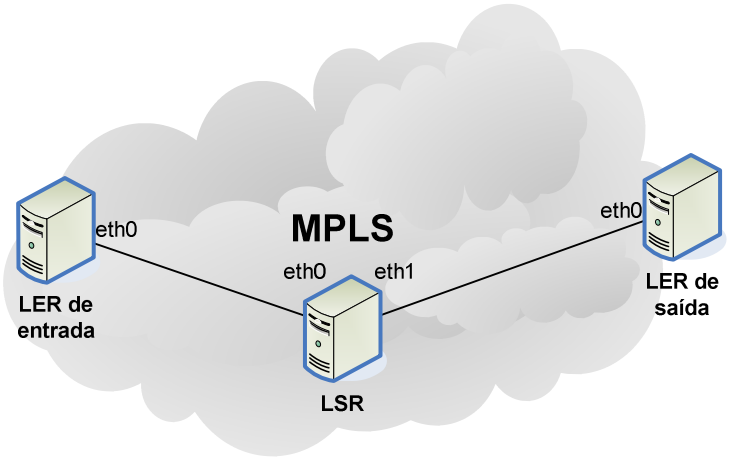


Figura 3.9 - Ambiente montando para verificação do funcionamento do MPLS.

Tabela 3.2 - Endereços utilizados na verificação de funcionamento do MPLS.

dispositivo	**endereço da interface eth0**	**endereço da interface eth1**
LER de entrada	10.10.0.1	
LSR	10.10.0.2	10.10.2.1
LER de saída	10.10.2.2	

A execução do RSVP inicia um console do próprio RSVP, onde é possível criar túneis LSPs manualmente. O RSVP foi iniciado nos dispositivos através do comando `./rsvpd -D`, no LER de saída foi iniciado o serviço que aceita a criação de túneis automaticamente através do comando `./rapirecv_auto`, e a partir do LER de entrada, no console do RSVP, foi iniciado o túnel. A fig. 3.10 apresenta a tela capturada da criação do túnel e a partir de então foi detectado na rede, com a ajuda do *sniffer* Ethereal, mensagens Path e Resv, mantendo o túnel ativo. As mensagens Path e Resv capturadas com *sniffer* estão apresentadas nas figs. 3.11 e 3.12, respectivamente.

```
[root@LER1 rsvpd]# ./rsvpd -D

T1> dest lsp tcp 10.10.2.2/12

T1> sender 10.10.0.1/12

T1>
```

Figura 3.10 - Criação de um túnel RSVP.

```
Source      Destination  Protocol  Info
10.10.0.1   10.10.2.2    RSVP      PATH Message. SESSION: IPv4-LSP, Tunnel ID 12
10.10.0.2   10.10.0.1    RSVP      RESV Message. SESSION: IPv4-LSP, Tunnel ID 12
10.10.0.1   10.10.2.2    RSVP      PATH Message. SESSION: IPv4-LSP, Tunnel ID 12
10.10.0.2   10.10.0.1    RSVP      RESV Message. SESSION: IPv4-LSP, Tunnel ID 12

⊞ Frame 16 (102 bytes on wire, 102 bytes captured)
⊞ Ethernet II, Src: 00:e0:7d:ee:60:f1, Dst: 00:00:21:cc:27:32
⊞ Internet Protocol, Src Addr: 10.10.0.1, Dst Addr: 10.10.2.2
⊟ Resource ReserVation Protocol (RSVP): PATH Message. SESSION: IPv4-LSP,
   ⊞ RSVP Header. PATH Message.
   ⊞ SESSION: IPv4-LSP, Destination 10.10.2.2, Tunnel ID 12, Ext ID 0.
   ⊞ HOP: IPv4, 10.10.0.1
   ⊞ TIME VALUES: 30000 ms
   ⊞ LABEL REQUEST: Basic: L3PID: IP (0x0800)
   ⊞ SENDER TEMPLATE: IPv4-LSP, Tunnel Source: 10.10.0.1, LSP ID: 12.
```

Figura 3.11 - Mensagem Path capturada com o Ethereal.

```
Source      Destination  Protocol  Info
10.10.0.1   10.10.2.2    RSVP      PATH Message. SESSION: IPv4-LSP, Tunnel ID 12
10.10.0.2   10.10.0.1    RSVP      RESV Message. SESSION: IPv4-LSP, Tunnel ID 12
10.10.0.1   10.10.2.2    RSVP      PATH Message. SESSION: IPv4-LSP, Tunnel ID 12
10.10.0.2   10.10.0.1    RSVP      RESV Message. SESSION: IPv4-LSP, Tunnel ID 12

⊞ Frame 17 (106 bytes on wire, 106 bytes captured)
⊞ Ethernet II, Src: 00:00:21:cc:27:32, Dst: 00:e0:7d:ee:60:f1
⊞ Internet Protocol, Src Addr: 10.10.0.2, Dst Addr: 10.10.0.1
⊟ Resource ReserVation Protocol (RSVP): RESV Message. SESSION: IPv4-LSP
   ⊞ RSVP Header. RESV Message.
   ⊞ SESSION: IPv4-LSP, Destination 10.10.2.2, Tunnel ID 12, Ext ID 0.
   ⊞ HOP: IPv4, 10.10.0.2
   ⊞ TIME VALUES: 30000 ms
   ⊞ STYLE: Fixed Filter (10)
   ⊞ FILTERSPEC: IPv4-LSP, Tunnel Source: 10.10.0.1, LSP ID: 12.
   ⊞ LABEL: 2200
```

Figura 3.12 - Mensagem Resv capturada com o Ethereal.

Em seguida, foi mapeado o fluxo de pacotes de qualquer protocolo com destino ao endereço 10.10.2.2 ao túnel criado, de rótulo 12. Em seguida foi feita uma comunicação com o dispositivo com endereço 10.10.2.2 e foi verificado, pela captura dos pacotes com o

sniffer Ethereal, que eles estavam sendo enviados com o rótulo MPLS entre o cabeçalho Ethernet e o cabeçalho IP, isto é, entre o cabeçalho de camada 2 e de camada 3. Na fig. 3.13 temos a tela capturada com o mapeamento do fluxo de dados para o túnel já criado, e na fig. 3.14 temos o pacote *ping* capturado.

```
[root@LER1 labeltest]# ./tunnel -m -a -d 10.10.2.2/32 -l 12

Adding fwmark 1 table 1 rule
Add gw T2200eth0 to table 1
LSPID:12
[root@LER1 labeltest]# ./tunnel -L -c

LSPID    Destination (type label/ phb/        viface) Packets   Byte
E 12     10.10.2.2    ( gen  2200/  BE/     T2200eth0)       0      0
  |      Destination DSCP  Proto   Packets     Bytes  Packets   Byte
  \->    10.10.2.2     BE    nop         0         0        0      0
```

Figura 3.13 - mapeamento de fluxo de dados para um túnel LSP.

Source	Destination	Protocol	Info
10.10.0.1	10.10.2.2	ICMP	Echo (ping) request
10.10.2.2	10.10.0.1	ICMP	Echo (ping) reply
10.10.0.1	10.10.2.2	ICMP	Echo (ping) request

```
⊞ Frame 32 (102 bytes on wire, 102 bytes captured)
⊞ Ethernet II, Src: 00:e0:7d:ee:60:f1, Dst: 00:00:21:cc:27:32
⊟ MultiProtocol Label Switching Header
    MPLS Label: Unknown 12
    MPLS Experimental Bits: 0
    MPLS Bottom Of Label Stack: 1
    MPLS TTL: 255
⊞ Internet Protocol, Src Addr: 10.10.0.1, Dst Addr: 10.10.2.2
⊞ Internet Control Message Protocol
```

Figura 3.14 - Tráfego de pacotes em uma rede MPLS.

3.5 - DESEMPENHO DO MPLS

Para avaliar se o MPLS é realmente capaz de melhorar a eficiência do encaminhamento de pacotes em ambientes Mobile IP, é necessário analisar o desempenho desta tecnologia. O desempenho do MPLS sem a utilização de Mobile IP já foi verificado por pesquisadores do LABCOM, não sendo necessário fazer novamente estes testes. Nos parágrafos seguintes há uma descrição destes testes. Foi realizado, neste trabalho, teste para verificar o

desempenho do MPLS entre os agentes de mobilidade do MIP. Estes testes estão descritos na seção 3.5.1. desta dissertação.

O desempenho do MPLS foi verificado em diversos testes, realizados sobre um núcleo MPLS montado no laboratório de comunicações da UnB, LABCOM [3, 4, 5, 6, 7]. Os testes sempre se basearam na utilização da infra-estrutura da rede do LABCOM. Um teste validando o *Diffserv* foi realizado com a utilização de 4 tráfegos diferentes sendo medidos, cada um com uma classe de serviço diferente. Foi verificado que, ao final do teste, houve 0% de perda de pacotes para os dois tráfegos de classe de serviço de maior precedência, enquanto o de terceira maior precedência teve 26,3% de perda e o tráfego de menor precedência, com classe de serviço padrão de *Internet*, teve a maior perda de pacotes: 36,7%. Isto demonstra que os pacotes de maior precedência estavam ocupando a banda que eles necessitavam enquanto que os de menor precedência utilizavam a banda restante.

Em teste comparativo, foi verificado que o MPLS com aplicação de Diffserv causa um aumento de latência no encaminhamento dos pacotes em relação ao MPLS comum. Este aumento de latência, que pode tornar a latência maior que a encontrada com um *backbone* de rotemento IP, se deve ao processo de classificação e enfileiramento dos pacotes, que consome muito processamento dos comutadores. Este aumento de latência pode ser considerado como um custo a se pagar por uma vantagem desejada, no caso a diferenciação nos serviços prestados.

Em um teste de recomposição de falhas, foi feita uma comparação entre o MPLS e uma rede IP. Para que a rede IP se assemelhasse a uma rede Internet, foram adicionadas 65.500 rotas e aplicados um tráfego cíclico de 640kB em cada roteador. Neste experimento, foi aplicada uma falha no enlace físico, e observou-se que em ambiente IP, houve um atraso de aproximadamente 10 segundos para o sistema se recompor da falha, enquanto no MPLS o atraso foi muito menor: aproximadamente 5 segundos.

A utilização do MPLS sem Diffserv encontra uma latência no envio de pacotes menor que a encontrada em redes IP, entretanto quando se insere outros fatores, tais como a falha, é comum a latência média aumentar devido a processos de re-mapeamento do tráfego na configuração dos novos LSPs, influenciando o resultado dos valores de latência encontrados.

Desta forma percebe-se, que de maneira geral, o MPLS traz mais eficiência na sua utilização nos *backbones* de rede. Quando seu desempenho em relação a latência das mensagens apresenta um resultado inferior, é porque está ocorrendo algum processo tal como um re-mapeamento dos túneis LSP, o que resulta em alguma melhora significativa tal como uma recomposição do sistema em tempo menor que o tempo de recomposição no ambiente IP.

3.5.1 - Desempenho do MPLS no *backbone* de uma rede Mobile IP

Para avaliar a capacidade do MPLS de aumentar a eficiência do Mobile IP com relação à latência de mensagens enviadas em ocasião do nó móvel registrado em uma rede estrangeira muito distante de sua rede nativa, foi realizado mais um teste semelhante ao da seção 2.6 deste trabalho. O ambiente montado está ilustrado na fig. 3.16 com os endereços apresentados na tabela 3.3. A seta vermelha indica o sentido do fluxo de dados cujas características estão sendo avaliadas neste teste. O programa utilizado neste processo foi novamente o analisador de rede desenvolvido no laboratório LABCOM [13].

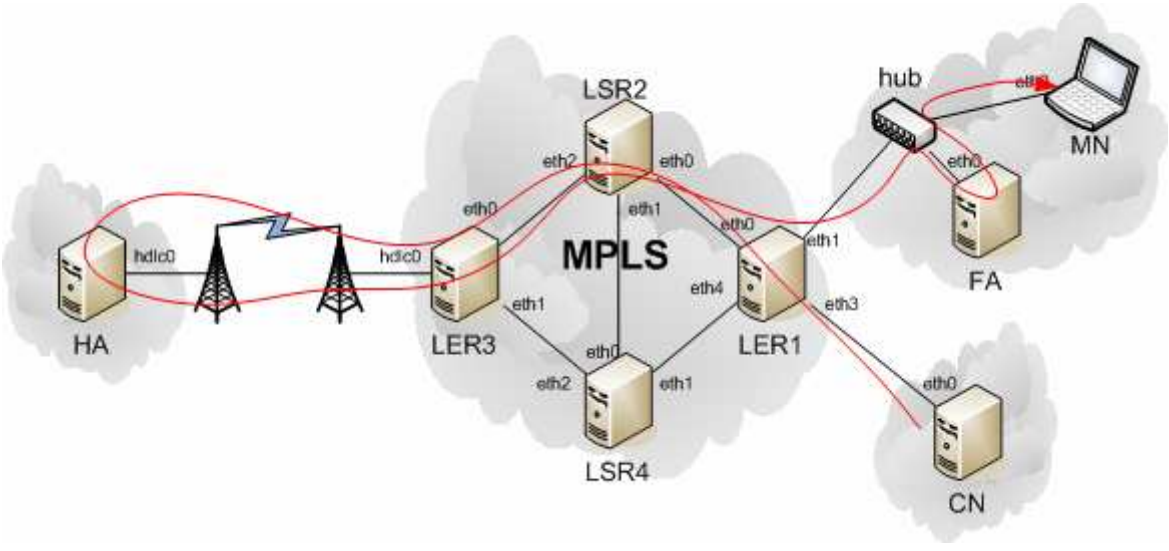


Figura 3.15 - Ambiente montado para o teste de desempenho do MPLS no núcleo de uma rede IP móvel.

Tabela 3.3 - Endereços usados no ambiente de testes.

Dispositivo	**Interface**	**endereço**

LER1	eth0	10.0.7.1
	eth1	172.24.1.111
	eth2	192.168.1.1
	eth3	192.168.2.1
	eth4	10.0.9.1
LSR2	eth0	10.0.7.2
	eth1	10.0.8.2
	eth2	10.0.6.2
LER3	eth0	10.0.6.3
	eth1	10.0.10.3
	hdlc0	10.0.5.1
LSR4	eth0	10.0.8.4
	eth1	10.0.9.4
	eth2	10.0.10.4
HA	eth0	192.168.1.1
	hdlc0	10.0.5.2
MN	eth0	196.168.1.2
FA	eth0	172.24.1.14
CN	eth0	172.24.1.178

Novamente foram verificados os resultados da banda ocupada pelos tráfegos gerados, o atraso, a variação do atraso e a perda de pacotes para tráfegos de 8kbps e 256kbps. Os resultados estão apresentados nas figs. 3.17 a 3.26.

Figura 3.16 - Banda ocupada pelo tráfego de 8kbps.

Foi verificada, para a taxa de 8kbps, uma taxa de transmissão constante de 9,6kbps. Nesta taxa, foi verificado um atraso médio de aproximadamente 4,75 ms.

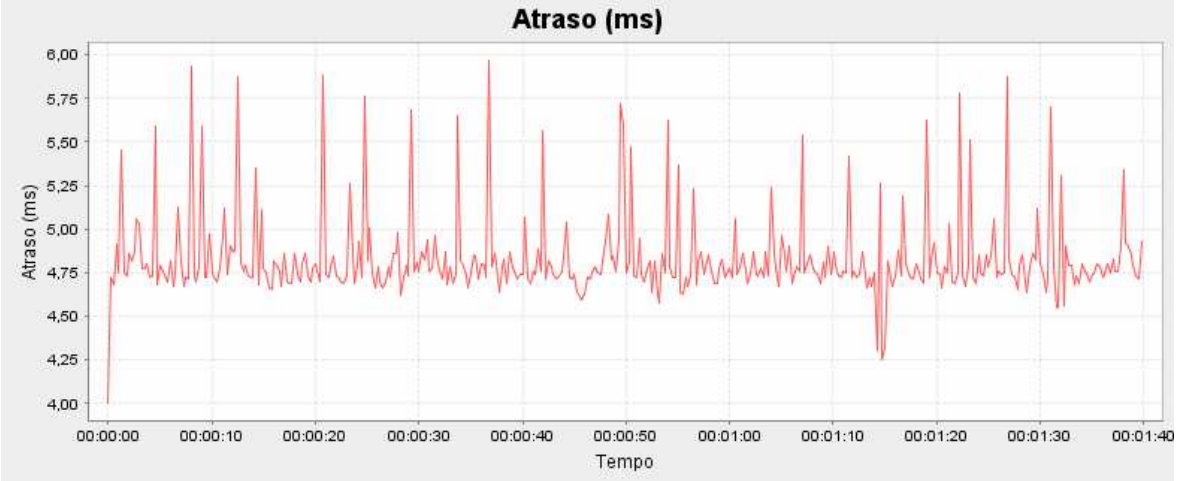


Figura 3.17 - Atraso do tráfego de 8kbps.

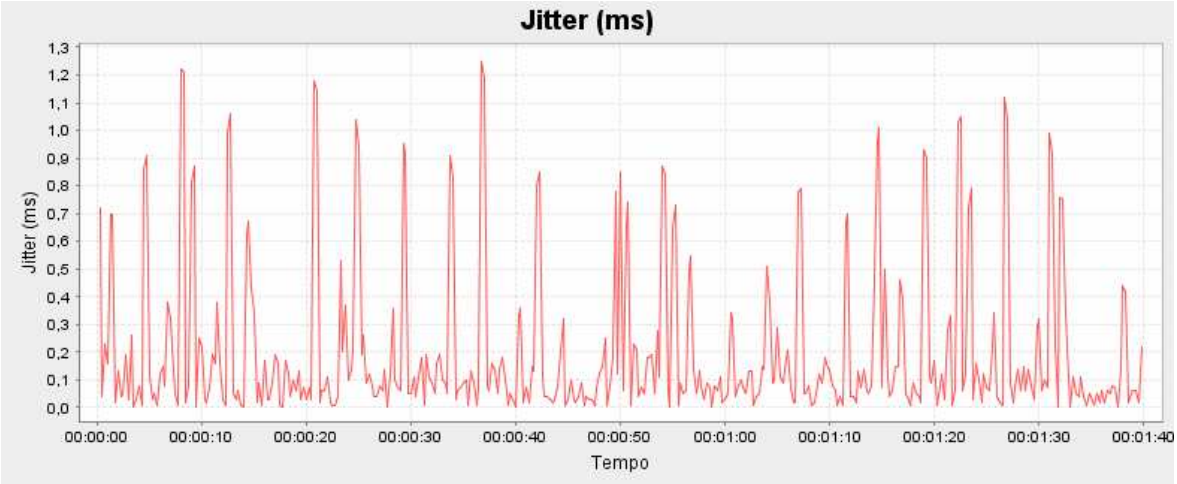


Figura 3.18 - Variação de atraso do tráfego de 8kbps.

Foi obtida uma variação de atraso predominantemente entre 0 e 0,25 ms com alguns picos que podiam alcançar 1,25ms. Não houve perda de pacote nos 100 segundos de teste deste tráfego.

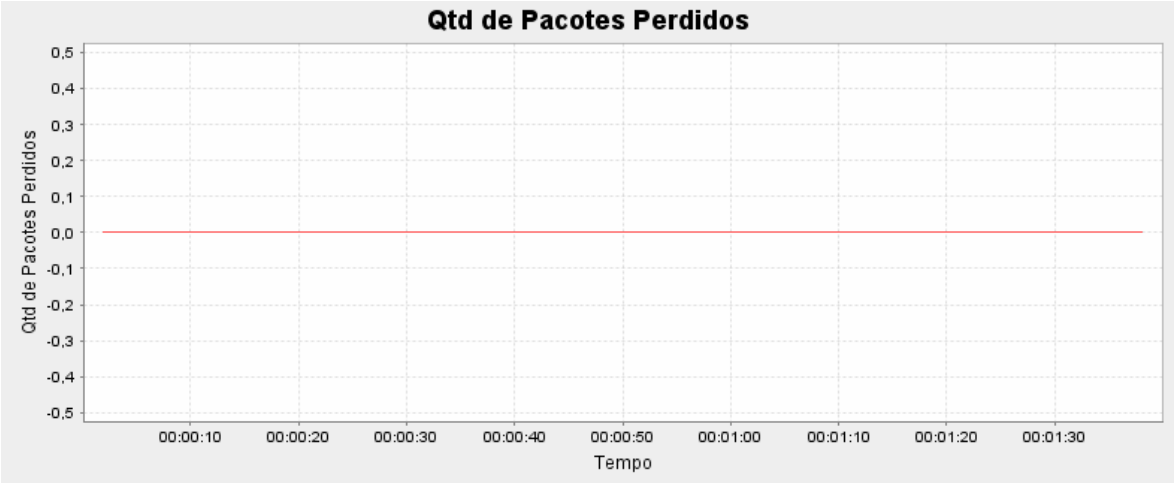


Figura 3.19 - Quantidade de pacotes perdidos na transmissão do tráfego de 8kbps.

Figura 3.20 - Banda ocupada pelo tráfego de 256kbps.

A banda ocupada pelo tráfego que estava sendo gerado, para 256kbps com um núcleo MPLS no *backbone* da rede, se manteve com comportamento constante em 273,5 kbps. O atraso encontrado, nestas condições, esteve entre 4,25ms e 4,75ms.

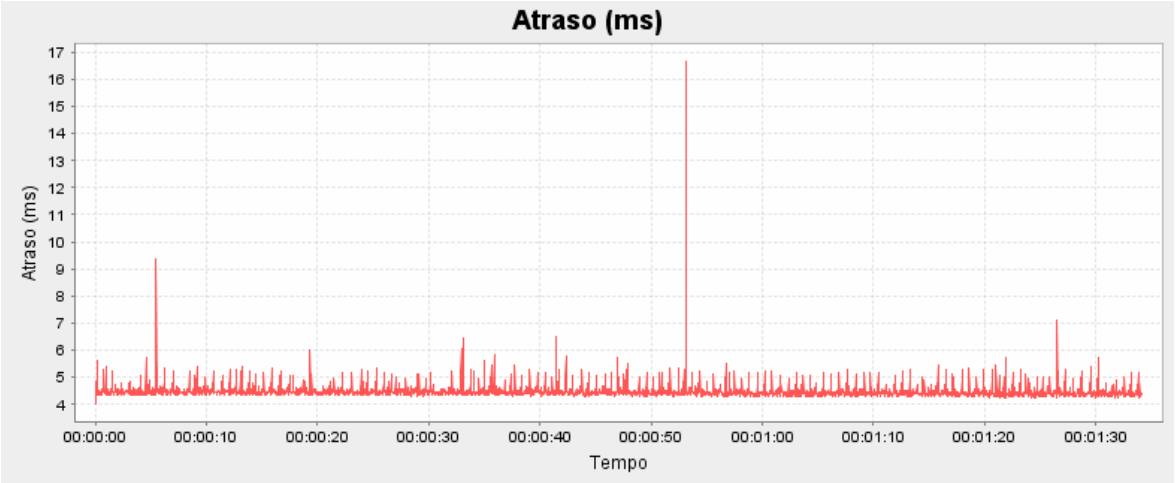


Figura 3.21 - Atraso do tráfego de 256kbps.

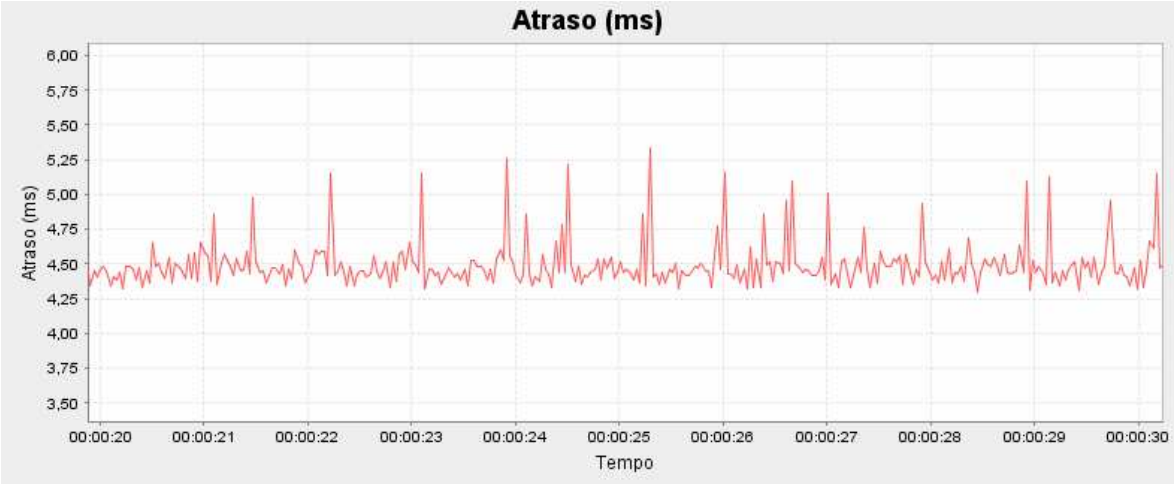


Figura 3.22 – Detalhes do atraso do tráfego de 256kbps.

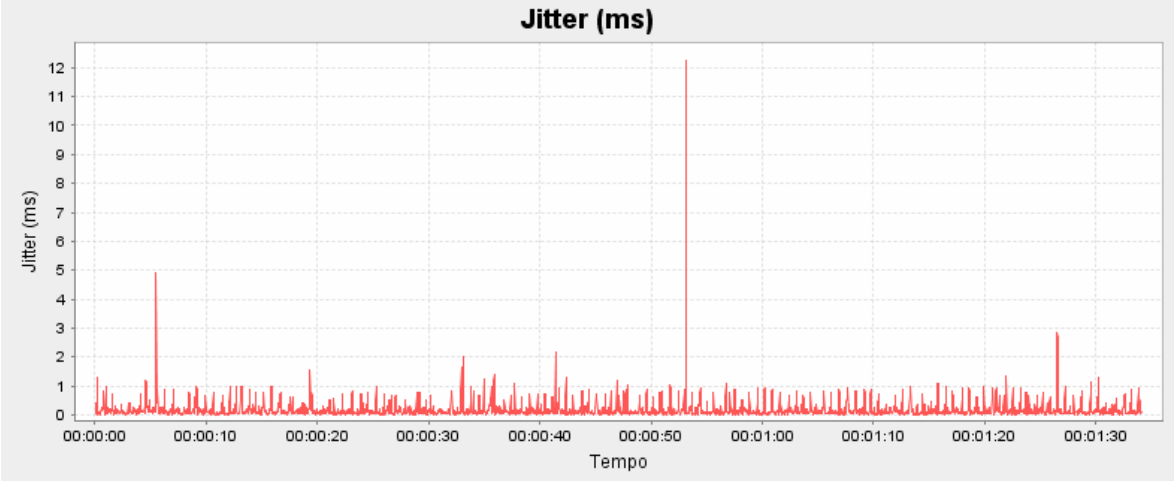


Figura 3.23 - Variação de atraso do tráfego de 256kbps.

Foi verificado uma variação de atraso entre 0 e 0,2 ms nesta etapa do teste, e não ocorreu nenhuma perda de pacotes nesta etapa de teste no período de 100 segundos.

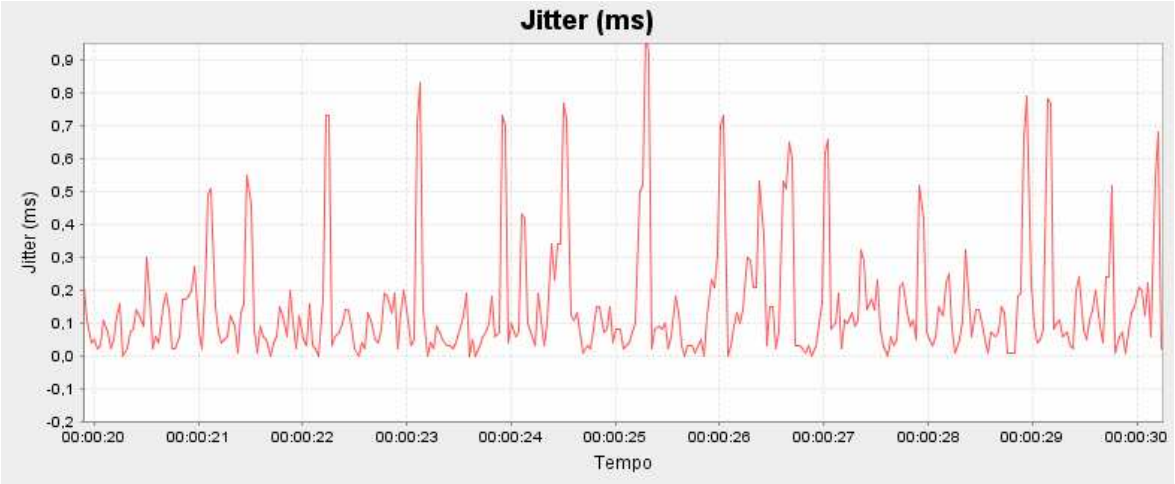


Figura 3.24 – Detalhes da variação de atraso do tráfego de 256kbps.

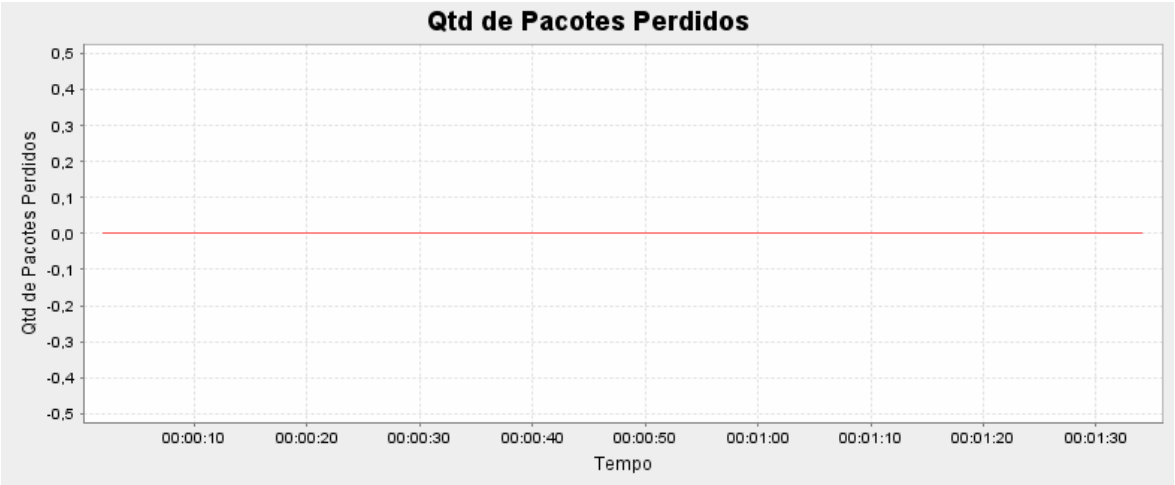


Figura 3.25 - Quantidade de pacotes perdidos na transmissão do tráfego de 256kbps.

Para 8kbps, foram encontradas uma banda ocupada constante, um atraso médio de 4,75 ms com alguns picos acima de 5,25ms, uma variação de atraso entre 0 e 1,25ms na qual a maior parte foi abaixo de 0,25ms, e nenhum pacote perdido no intervalo de 100 segundos. Para 256kbps também foi obtida uma taxa de transmissão constante. O atraso com a taxa de 256kbps ficou entre 4,25 e 4,75 ms com poucos picos acima de 5,25ms, a variação de atraso esteve em sua maior parte entre 0 e 0,2ms com poucos picos acima de 0,8ms e teve perda de pacotes nula.

Verifica-se que pelo encaminhamento dos pacotes ser mais eficiente com a comutação feita com o MPLS que com o roteamento feito em uma rede IP, os resultados encontrados neste teste foram superiores aos encontrados na segunda fase do teste da seção 2.6. A taxa de transmissão, que para 256kbps em rede IP, mesmo sem a aplicação do MIP, estava

oscilando devido à grande variação de atraso passou a ser constante da mesma forma que para o tráfego de 8kbps. O atraso teve uma leve redução em 8kbps, passando de 5 para 4,75ms. Esta baixa redução provavelmente está no fato de que a maior parte do atraso encontrado estavam nos enlaces físicos. Para o tráfego de 256kbps, o atraso mudou de um intervalo que variava entre 4,5 e 12,5ms para um que varia entre 4,25 e 4,75ms. A variação de atraso teve uma melhora considerável, passando de uma margem de 2ms para 0,25ms no tráfego de 8kbps e de 4ms para 0,8ms na taxa de 256kbps. A perda de pacotes também demonstrou uma significativa melhora, passando de 170 pacotes perdidos para nenhum pacote perdido durante os 100 segundos de teste.

Verifica-se que diferente do que acontecia com o roteamento IP, que a medida que aumentava-se a taxa de transmissão, o desempenho do sistema se deteriorava, com a aplicação do MPLS o sistema continuou apresentando praticamente o mesmo resultado de desempenho. Este ambiente poderia se trafegar voz com codificação CELP de taxa 8kbps e vídeo com codificação CIF e protocolo H.261 a uma taxa de 256kbps com uma qualidade de serviço excelente, pois foram obtidos atrasos menores que 7ms, onde se poderia chegar a 150ms; a variação de atraso, que poderiam alcançar 20ms com qualidade boa esteve abaixo de 2ms, com exceção de três picos que não ultrapassam 13ms. E não houve perda de pacote, quando é possível ter 1% de perda.

Com isso, o MPLS demonstrou grande capacidade de melhorar o desempenho de uma rede IP móvel. Para obter resultados melhores no sistema, deve-se integrar o Mobile IP com o MPLS, reduzindo assim o tamanho de cada pacote transferido do agente nativo ao agente estrangeiro, pois os pacotes enviados no túnel criado pelo IP móvel têm dois cabeçalhos IP, aumentando o tamanho do pacote em, pelo menos, 20 bytes. A integração também reduz o tempo de processamento pelo fato de o agente e o roteador de borda serem o mesmo elemento e não haver o tempo de processamento que ocorre no encapsulamento IP-em-IP no agente nativo e desencapsulamento IP-em-IP no agente estrangeiro.

3.6 - CONCLUSÃO SOBRE O MPLS

Como foi verificado neste capítulo, o MPLS apresenta resultados de desempenho muito melhores que o roteamento IP. A sua aplicação entre os elementos de um sistema IP móvel,

constituindo o que é conhecido como Mobile IP sobre MPLS, apresentou um ganho elevado no desempenho do sistema, justificando a sua utilização para melhorar a qualidade do IP móvel no que diz respeito ao atraso que os pacotes sofrem quando o nó móvel se encontra em uma rede estrangeira muito distante da sua rede nativa.

Com a utilização do MPLS entre os dispositivos, torna-se desnecessária a utilização do túnel reverso, podendo os pacotes do nó móvel serem enviados diretamente ao destino, devido ao fato de os comutadores MPLS não analisarem o cabeçalho IP e, portanto, não havendo risco de os pacotes serem descartados devido ao endereço de origem não condizente com o esperado. Entretanto, os pacotes direcionados ao nó móvel continuam tendo de passar pela rede nativa e a pura aplicação do MPLS não é capaz de resolver este problema.

No próximo capítulo, discute-se a integração do MPLS com o IP móvel, apresentando soluções para a necessidade dos pacotes enviados ao nó móvel terem de passar pelo agente nativo e para o atraso de *handoff*, que resulta em um curto período no qual o nó móvel permanece sem comunicação. Apresentando um sistema que tenha o mínimo de atraso e utiliza o MPLS para uma comutação eficiente dos pacotes endereçados de e para o no móvel.

4 - INTEGRAÇÃO ENTRE MOBILE IP E MPLS

A necessidade de otimização do sistema IP móvel, tanto no que diz respeito à latência no envio de pacotes, quanto no que diz respeito ao atraso de *handoff*, incentivou muitas pesquisas que analisam diversas formas de se minimizar os atrasos do MIP. Como exemplo de forma de reduzir atraso no *handoff*, podem ser citadas as implementações de micro-mobilidade tais como o IP móvel hierárquico [29], descrito na seção 2.4 desta dissertação e alguns algoritmos que otimizam este sistema, tais como o protocolo de autenticação rápida do IP móvel [23] que realiza o registro do móvel no agente estrangeiro, que estabelece um túnel com o agente estrangeiro ao qual o móvel estava conectado anteriormente até que o agente nativo seja notificado da movimentação do nó móvel. Para a otimização no IP móvel no que diz respeito ao atraso ocorrido pela distância entre os agentes, pode-se citar a utilização de uma rede MPLS entre os agentes, pois isto já traria um ganho em relação à rede IP convencional, como foi visto no Capítulo 3 desta monografia.

Este capítulo consiste na análise de diversas possibilidades de realização da otimização do IP móvel através da utilização de túneis MPLS descritas em diversos artigos, proposta para uma integração destas tecnologias de forma a procurar um bom desempenho e descrição da implementação básica de integração realizada no laboratório LEMOM.

4.1 - IMPLEMENTAÇÕES SUGERIDAS EM ARTIGOS

Dentre as pesquisas mais interessantes encontradas em congressos e periódicos, houve análise sobre a utilização do RSVP sobre IP móvel para suporte a QoS (qualidade de serviço) [16, 21, 25, 33, 38, 57, 58, 59, 60, 62]; a substituição dos túneis IP-em-IP por túneis LSP [41]; pesquisas sobre a aplicação do MPLS em micro-mobilidade [17, 28, 35, 56, 64]; a utilização da otimização de roteamento, que consiste em enviar pacotes de um nó correspondente ao nó móvel sem necessariamente passar pelo agente nativo [45] e sua utilização com um *backbone* MPLS [15, 19, 54]; utilização do MPLS como base para a aplicação de hierarquia e para otimização de roteamento [18, 20]; e aplicação de hierarquia e *multicast* em um ambiente IP móvel integrado a MPLS para realização de um *handoff* suave [63]. A seguir, têm-se pequenas descrições e críticas sobre estas pesquisas.

4.1.1 - RSVP sobre IP móvel

A justificativa para se verificar a viabilidade e formas de se integrar o MIP com o RSVP se baseia no fato de esta tecnologia permitir que comunicações ponto-a-ponto ou ponto-multiponto tenham recursos reservados no caminho da origem ao destino de uma comunicação. Esta reserva é um fator de grande importância para se garantir qualidade de serviço, que é importante para assegurar qualidade em transmissão de áudio e vídeo em tempo real.

Quando se aplica o protocolo sobre o IP móvel, têm-se alguns problemas que devem ser resolvidos. O primeiro problema encontrado diz respeito à pré-reserva de recursos. Quando um dispositivo se move de uma rede para outra, o caminho que o fluxo de pacotes percorre também muda, e torna-se necessário restabelecer o túnel. É possível que no novo caminho não haja recursos disponíveis, causando assim degradação da qualidade de serviços. Uma forma de tentar corrigir esta situação seria reservar recursos para todas as redes em que o móvel possa passar. Esta alternativa entretanto causaria desperdício de recursos nas redes que o móvel não estiver no momento, além da complexidade em se determinar quais as redes nas quais se deve fazer a reserva.

Ao se fazer o tunelamento RSVP desde o remetente até o destinatário de um pacote, parte do caminho estará entre o agente estrangeiro e o nativo, fazendo com que as mensagens RSVP passem de forma transparente aos roteadores, resultando no não estabelecimento do túnel RSVP. Uma solução proposta para este problema consiste na classificação dos pacotes encapsulados com IP-em-IP por seus cabeçalhos internos [25], entretanto isso requer modificação em todos os roteadores, além de aumentar a carga de processamento deles. Outra solução se faz pela criação de uma outra sessão RSVP entre os agentes nativo e estrangeiro de forma que esta sessão possa ser iniciada pela detecção do início de uma sessão RSVP entre o nó móvel e o nó correspondente [16, 21].

Para manter um túnel RSVP, é necessário que haja envio periódico de mensagens PATH e RESV. Considerando o fato de que uma considerável parcela dos nós móveis é dependente de bateria, o envio periódico destas mensagens reduzirá o tempo de carga desta. Para se

contornar este problema, deve-se ou reduzir a freqüência do envio de mensagens RESV ou ter algum dispositivo não-dependente de bateria enviando estas mensagens pelo dispositivo móvel. Para redução na freqüência de envio das mensagens, foi proposta uma nova mensagem, chamada de SMRP (protocolo de reserva com suporte a mobilidade) que combina as mensagens PATH e RESV [38]. Nesta alteração do protocolo, o remetente transmite o SMRP ao nó móvel e este responde a este pacote para aceitar a reserva. A mensagem SMRP só precisa ser enviada novamente pelo remetente novamente quando ocorrem longos períodos sem transmissão de dados. Para resolver o problema através de outro dispositivo enviando as mensagens pelo nó móvel, foi proposta a utilização de agentes chamados *proxy* de mobilidade, sendo que haveria um *proxy* na rede onde o móvel se encontra e outros nas redes vizinhas. Estes *proxys*, além de operar como uma ancora para o móvel, podem ser utilizados para a pré-reserva de recursos a fim de obter um *handoff* mais estável [57, 58, 59].

Quando uma nova reserva precisa ser estabelecida durante um *handoff* ou uma pré-reserva, é muito provável que o novo caminho e o velho caminho tenham uma parcela do percurso em comum. Assim sendo, apenas uma parte do caminho precisa passar pelo processo de estabelecimento de túnel. Para isso, foi proposta a análise dos rótulos de fluxos para identificar o fluxo comum e assim determinar onde se encontra o caminho comum [33, 62]. Nesta proposta, a solicitação de reserva de recursos é transmitida a partir do móvel, e, em cada roteador do caminho, o rótulo do fluxo solicitado é comparado com sua tabela de rótulo de fluxos. O roteador que verificar a existência do rótulo de fluxo em sua tabela deverá liberar o antigo caminho RSVP e enviar a mensagem PATH de volta pelo caminho ao móvel para estabelecer o novo tunelamento na parte alterada do túnel.

4.1.2 - Substituição do tunelamento IP-em-IP por LSP do MPLS

A integração do IP móvel com o MPLS traz diversos benefícios, dentre os quais podem ser citadas a diferenciação no tratamento de diferentes fluxos de dados de acordo com políticas pré-determinadas pelo administrador da rede, o suporte a classe de serviços e qualidade de serviço para serviços diferenciados, suporte a engenharia de tráfego e compatibilidade com IP e com diferentes protocolos de roteamento tais como ATM.

Para integração entre as duas tecnologias, devem-se implementar os roteadores de borda de rótulos (LER) com as funcionalidades dos agentes da rede IP móvel [41]; assim sendo, haverão agentes LER/HA e LER/FA. Neste cenário, não há necessidade de alteração no protocolo utilizado pelo nó móvel: o processo de descoberta de agentes de mobilidade permanece inalterado e o registro, visto a partir do móvel, também permanece inalterado. Imediatamente após o processo de registro, o LER/HA envia uma mensagem de requisição de rótulo ou mensagem Path ao LER/FA, que responderá com uma mensagem de mapeamento de rótulo ou mensagem Resv, tal como ilustrado na fig. 4.1. O estabelecimento do túnel pode ser feito através da utilização de qualquer protocolo suportado pelo MPLS tais como RSVP-TE ou CR-LDP. Após o registro e conseqüente estabelecimento do caminho comutado por rótulo (LSP) toda comunicação feita entre algum nó correspondente qualquer e o nó móvel, ao chegar ao agente nativo, será enviado através do LSP estabelecido sem o encapsulamento IP-em-IP.

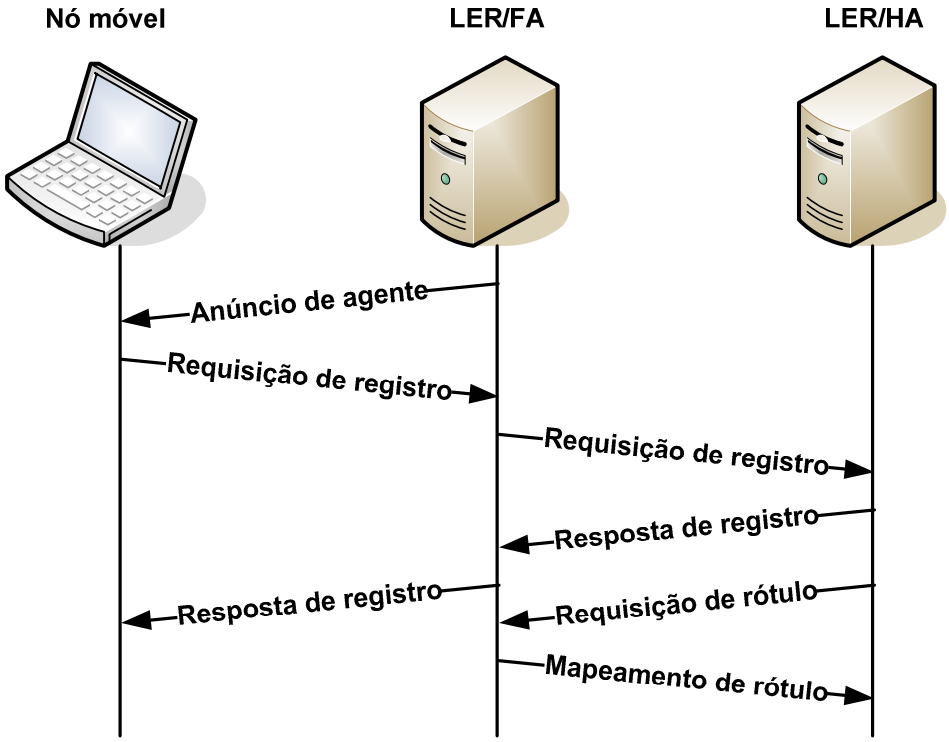


Figura 4.1 - Registro e estabelecimento de túnel em ambiente IP móvel integrado com MPLS.

Dentro deste contexto, elimina-se a necessidade de utilizar o túnel reverso, isto é, não há necessidade nenhuma de que as mensagens enviadas pelo nó móvel obrigatoriamente passem pelo agente nativo, pois esta medida era utilizada para evitar que roteadores

viessem a descartar estas mensagens ao analisar o endereço do remetente no cabeçalho IP. Visto que o MPLS apenas roteará as mensagens de acordo com o rótulo, sem análise do cabeçalho IP delas, não haverá descarte das mesmas tal como poderia acontecer numa rede IP comum.

Quando uma comunicação entre um nó correspondente e o nó móvel estiver sendo estabelecida, o LER/HA pode associar o rótulo e a interface por onde estão chegando as mensagens vindas do nó correspondente com o rótulo e interface do túnel que ele tem estabelecido com o agente estrangeiro, assim sendo, ele passa a funcionar como um roteador comutador de rótulos, sem necessidade de realizar muito processamento sobre a comunicação que está ocorrendo entre o nó correspondente e o nó móvel.

4.1.3 - Aplicação do MPLS em micro-mobilidade

A aplicação do MPLS para a realização de um *handoff* com latência menor pode ter diferentes formas de implementação, variando desde a simples aplicação do MPLS entre o agente estrangeiro de entrada e os agentes estrangeiros locais, com aplicação de RSVP e serviços diferenciados para proverem qualidade de serviço [35], a aplicações mais complexas como o aperfeiçoamento do protocolo de autenticação rápida para realização de um *handoff* mais eficiente [28].

Para este aperfeiçoamento, foi sugerida a utilização de registro regional, isto é, hierarquia de agentes estrangeiros. Entre o agente estrangeiro de entrada e o agente nativo, poderia ser utilizado o tunelamento comum do IP móvel, o encapsulamento IP-em-IP, mas, entre o GFA e os agentes estrangeiros locais, é utilizada uma rede MPLS. O primeiro registro que o móvel faz ao entrar em alguma sub-rede deste sistema é processado de forma normal, sendo enviada a requisição de registro ao agente nativo e este autenticando o móvel com o endereço residente como sendo o endereço do agente estrangeiro de entrada. O agente estrangeiro de entrada estabelecerá um túnel MPLS entre ele e o agente estrangeiro local para poder alcançar o nó móvel.

Quando o móvel se move para a área de cobertura de outro agente estrangeiro desta rede, ele deverá enviar um pacote UDP informando o endereço do agente estrangeiro local ao

qual ele estava conectado logo antes. Com esta informação, o novo agente estrangeiro estabelecerá um túnel LSP com o agente estrangeiro local anterior para receber as informações destinadas ao móvel. A fig. 4.2 apresenta, através do percurso indicado, o caminho percorrido pelos pacotes para alcançar o nó móvel logo em seguida ao *handoff*. Assim, se o móvel se mover repetidamente entre células do mesmo domínio, o agente estrangeiro ao qual ele estava conectado anteriormente servirá de âncora para as comunicações que já foram estabelecidas e reduzira a quantidade de perda de pacotes neste sistema.

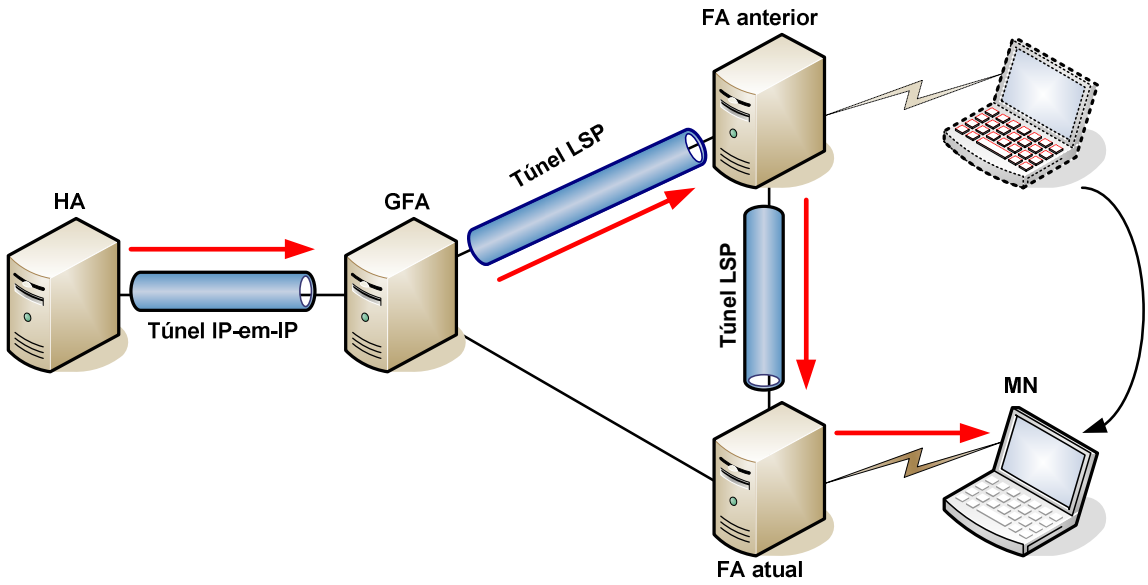


Figura 4.2 - Envio de pacotes logo após o handoff em um sistema que aperfeiçoa a autenticação rápida através de MPLS.

Após a realização do *handoff* com MPLS, é recomendável que o móvel, ao receber um anúncio de agente do novo agente estrangeiro, realize o registro. Uma vez que o registro aconteça, os pacotes passarão diretamente do agente estrangeiro de entrada para o agente estrangeiro local atual, não sendo necessária a utilização de um túnel com o agente estrangeiro local anterior. Então os agentes estrangeiros devem desfazer o túnel para liberar recursos da rede. O interessante desta implementação é o fato de o tempo do *handoff* não depender da distância entre os agentes locais e o agente estrangeiro de entrada, podendo este se situar longe sem causar perda de qualidade no sistema.

4.1.4 - Otimização de roteamento em Mobile IP

Quando um nó correspondente qualquer na Internet se comunica com um nó móvel localizado em uma rede estrangeira qualquer, pela implementação descrita na RFC 3344, ele deve enviar os pacotes à rede nativa do nó móvel para que o seu agente nativo as encapsule e as envie ao agente estrangeiro para que este as entregue ao móvel. Se a distância entre as redes for grande, o fluxo de pacotes poderá percorrer um caminho muito mais longo que o que seria percorrido se fosse enviado diretamente do nó correspondente ao agente estrangeiro para que este pudesse entregá-lo ao nó móvel. Este envio direto de pacotes é o que vem sendo chamado de otimização de roteamento [45].

A otimização de roteamento em Mobile IP se faz por meio de mensagens de ligação (*binding messages*). Para que o sistema funcione, os nós correspondentes precisam ter um serviço instalado e executando que seja capaz de receber estas mensagens de ligação, tratá-las e efetuar a alteração na tabela de roteamento e tunelamento necessários para o direcionamento das mensagens diretamente para o agente estrangeiro da rede onde o nó móvel se encontra.

Um nó correspondente habilitado para executar a otimização de roteamento tem uma tabela com informação dos nós móveis sobre os quais ele recebeu mensagens de ligação, que será chamada, neste trabalho, de tabela de ligação (*binding cache*). Sempre que o nó correspondente enviar um pacote a um nó móvel, ele verifica se este MN para quem ele deve enviar o pacote encontra-se na tabela de ligação. Se ele estiver na tabela, o CN encapsula o pacote com um novo cabeçalho IP com endereço de destinatário como sendo o endereço do agente estrangeiro da rede a qual o nó móvel está conectado, isto é, faz um tunelamento IP-em-IP para enviar a mensagem. Caso o nó correspondente não tenha o nó móvel em sua tabela de ligação, ele envia os pacotes pela tabela de roteamento IP, e quando os pacotes chegarem na rede nativa, o agente nativo se encarregará de enviá-los pelo túnel ao nó móvel, caso ele esteja em uma rede estrangeira.

Ao receber um pacote para um nó móvel que se encontra em uma rede estrangeira, o agente nativo o enviará pelo túnel até o agente estrangeiro para que este as entregue ao nó móvel e também enviará uma mensagem de atualização de ligação (*binding update message*) ao remetente do pacote, para informá-lo da atual posição do nó móvel. Assim

que o remetente dos pacotes receber a mensagem de atualização, ele acrescentará na tabela de ligação as informações sobre a localização do nó móvel, e a partir do próximo pacote que precise ser enviado ao nó móvel, ele realizará o tunelamento da mensagem diretamente ao agente estrangeiro da rede na qual o móvel se encontra. Este processo está ilustrado na fig. 4.3. Após o envio da mensagem de atualização de ligação, não é necessário envio de resposta por parte do nó correspondente, caso ele não receba a mensagem de atualização, quando ele enviar outro pacote para o móvel e este pacote passar pela rede nativa, o agente nativo perceberá que ele não recebeu a mensagem e torna a enviá-la.

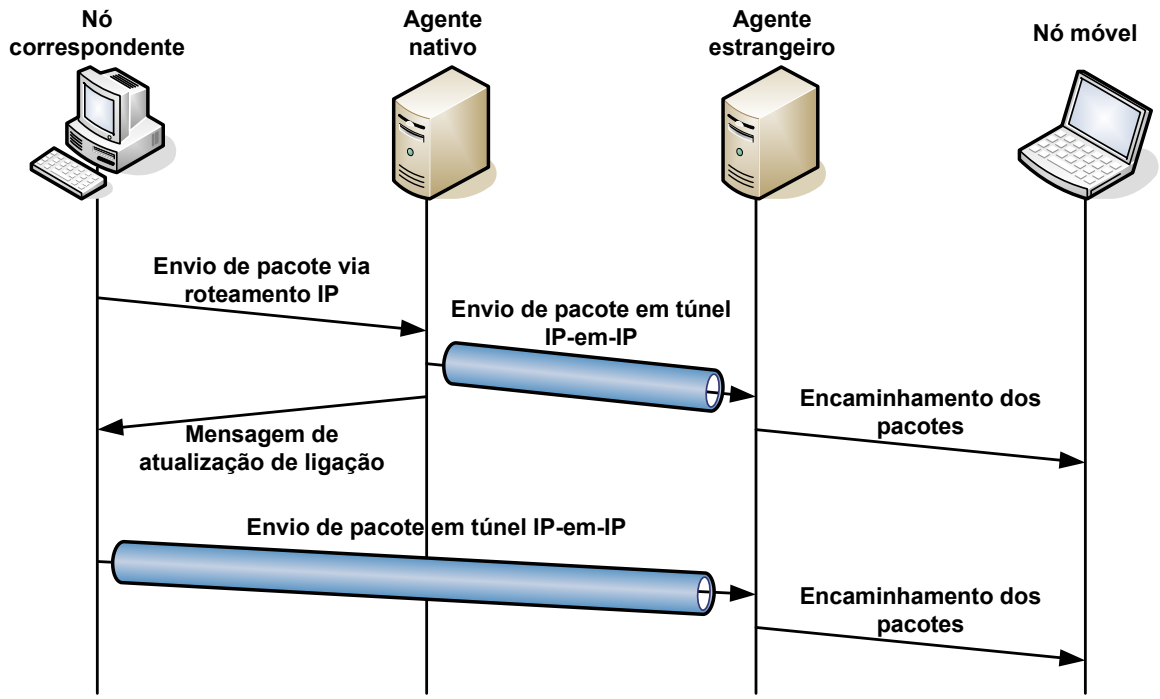


Figura 4.3 - Processo de atualização das informações de mobilidade para otimização de roteamento em Mobile IP.

Assim como o registro do nó móvel no MIP, cada registro na tabela de ligação tem um tempo de vida. Se o nó correspondente estiver mantendo uma comunicação crítica com o nó móvel que precise do melhor desempenho possível, ele pode enviar mensagens de requisição de ligação (*binding request message*) ao agente nativo pouco antes de o tempo de vida do registro do nó móvel na sua tabela de ligação expirar, solicitando a confirmação de que o móvel ainda se encontra na rede estrangeira especificada na tabela. Caso contrário, ele permitirá que o registro expire, e, na próxima comunicação com o nó móvel, ele enviará o pacote à rede nativa e o agente nativo novamente enviará a mensagem de ligação para que o nó correspondente atualize sua tabela. Não foi especificada, entretanto, a forma

de se definir se a comunicação entre o nó correspondente e o nó móvel é uma comunicação crítica, para se avaliar se deve ou não utilizar as mensagens de requisição de ligação.

Quando ocorre um *handoff*, o novo agente estrangeiro ao qual o nó móvel se conectou deve enviar uma mensagem ao antigo FA notificando o novo endereço residente do nó móvel. Esta notificação tem por finalidade avisar ao agente estrangeiro anterior para liberar os recursos de rede que estavam sendo utilizados pelo nó móvel caso haja esses recursos, e permitir que os pacotes que cheguem a ele sejam direcionados ao novo endereço residente, pois pode haver nós correspondentes que estejam enviando pacotes ao nó móvel diretamente para a rede estrangeira, e enquanto o registro em sua tabela não expirar, eles não entrarão em contato com o agente nativo, podendo assim perder muitos pacotes se estes não forem roteados ao destino correto.

Após um *handoff*, se o agente estrangeiro antigo receber um pacote tunelado para o nó móvel, caso ele ainda tenha o registro do móvel em seu registro, ele tunelará o pacote recebido ao novo endereço residente do nó móvel e enviará uma mensagem de aviso de ligação (*binding warning message*) ao agente nativo do nó móvel para que este mande a mensagem de atualização de ligação ao nó correspondente que enviou o pacote. Caso o agente estrangeiro já não tenha mais o registro do nó móvel em sua memória, ele descarta o pacote recebido e envia o aviso de ligação diretamente ao nó correspondente. Apesar de a proposta prever o descarte dos pacotes que chegam a um agente estrangeiro que não tem registro da posição do nó móvel, poder-se-ia evitar esta perda através do envio destes pacotes à rede nativa através do roteamento IP do pacote desencapsulado.

As figs. 4.4 e 4.5 apresentam diagramas que representam o processo de comunicação entre um nó correspondente e o nó móvel após um *handoff*. Na fig. 4.4, tem-se a situação na qual o agente estrangeiro registrado como endereço residente do nó móvel na tabela de ligação do CN ainda possui o registro do atual endereço residente do MN. Na fig. 4.5, tem-se a situação na qual o agente estrangeiro anterior já descartou as informações sobre o novo endereço residente do nó móvel.

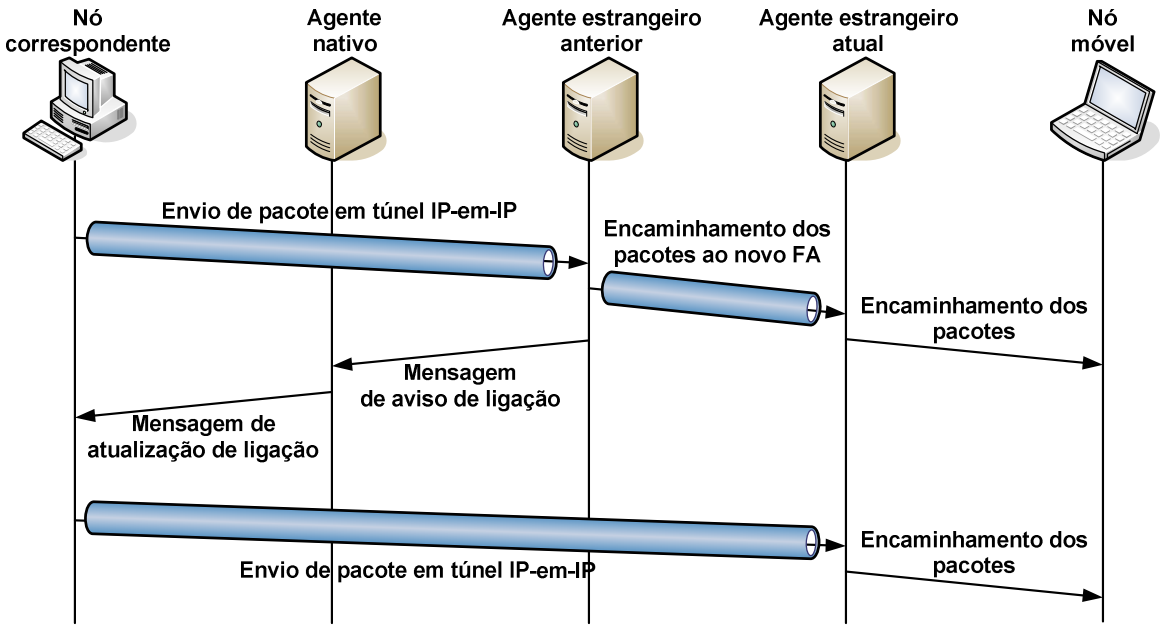


Figura 4.4 - Processo de aviso após o *handoff* em otimização de roteamento com atual localização do nó móvel conhecida pelo antigo agente estrangeiro.

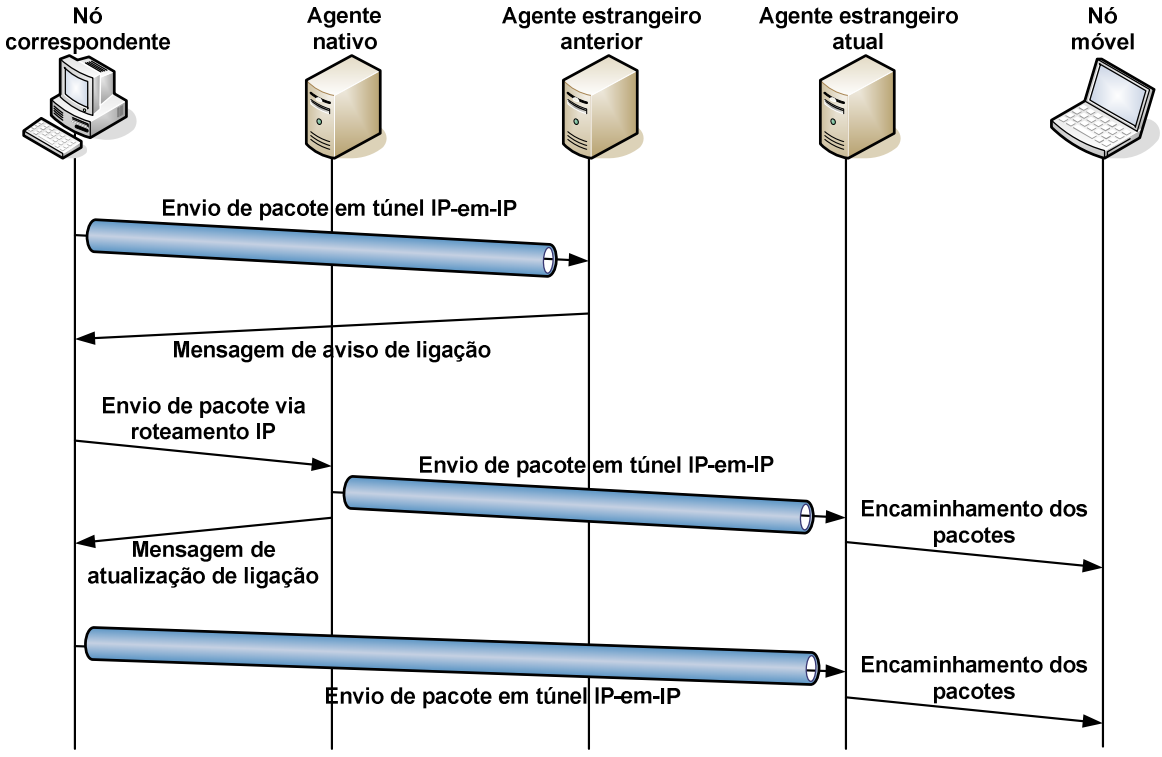


Figura 4.5 - Processo de aviso após o *handoff* com otimização de roteamento onde o agente estrangeiro anterior não conhece a atual posição do nó móvel.

4.1.5 - Otimização de Roteamento em MIP baseado em ambiente MPLS

A otimização de roteamento demonstra ser capaz de melhorar o desempenho do Mobile IP no que diz respeito à latência devido a eliminar a necessidade de todo pacote enviado ao nó móvel precisar passar pela rede nativa. Entretanto, pode-se aperfeiçoar esta tecnologia ainda um pouco mais, através da utilização do MPLS nesta otimização. Os benefícios obtidos por esta integração são os mesmos procurados ao se fazer uma integração entre o MIP especificado na RFC 3344 e o MPLS: obter um sistema independente do protocolo utilizado na camada de enlace da rede, que oferece suporte a engenharia de tráfego, diferenciação de serviços e reserva de recursos, além de oferecer um encaminhamento de pacotes de grande eficiência por não precisar processar cabeçalhos extensos em cada roteador interno para definir por onde enviar os pacotes.

A implementação desta otimização em MPLS pode ser realizada pela simples substituição dos túneis IP-em-IP presentes na otimização de roteamento em MIP comum pelos caminhos comutados por rótulos definidos pelo MPLS [19], como pode ser também realizada através de outros mecanismos, dentre os quais tem-se a otimização por meio de mensagens de mudança de caminho (*path change message*) enviadas pelo agente estrangeiro ao roteador de borda ao qual o nó correspondente está conectado [54].

A mensagem de mudança de caminho está prevista em uma proposta que parte do princípio de que os agentes são roteadores de borda do núcleo MPLS. Nesta proposta, ao receber um nó móvel, o agente estrangeiro deve enviar a mensagem de mudança de caminho para o endereço do nó correspondente, e quando esta mensagem chegar ao roteador de borda ao qual o CN está conectado, este roteador armazenará o endereço do nó móvel e enviará uma mensagem de requisição de rótulo ao endereço residente do nó móvel. Após receber a requisição de rótulo, o agente estrangeiro enviará a mensagem de mapeamento de rótulo para o roteador de borda conectado ao CN e este, ao receber esta mensagem, gravará o rótulo definido junto ao registro do nó móvel na tabela de encaminhamento. Ao receber um pacote, o roteador de borda verificará se o destino deste pacote está registrado em sua tabela de encaminhamento, e se estiver ele encaminha diretamente através do rótulo que define o caminho que ele deve percorrer para alcançar o agente estrangeiro da rede na qual o móvel está conectado. A fig. 4.6 apresenta a troca de mensagens efetuada para realização desta otimização.

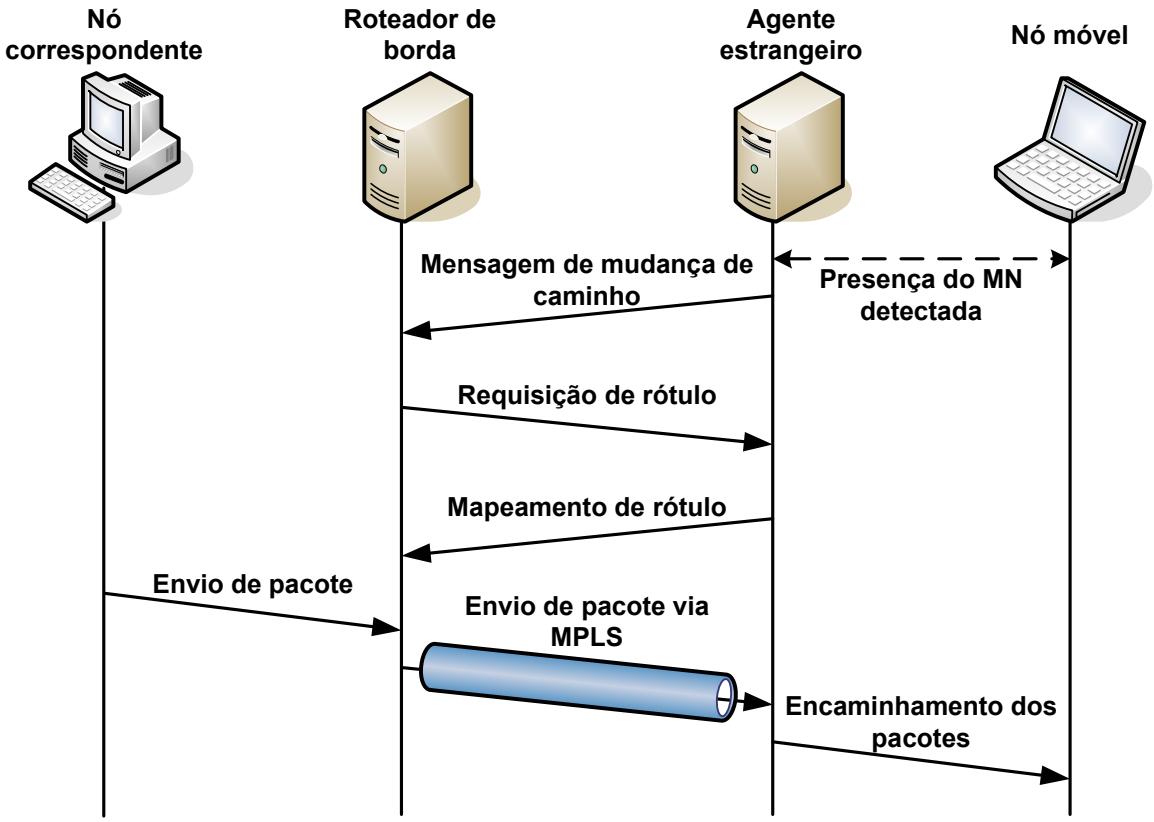


Figura 4.6 - Otimização de roteamento em MPLS com mensagem de mudança de caminho.

A desvantagem desta implementação se faz pela necessidade de o agente estrangeiro conhecer previamente o nó correspondente que deve se comunicar com o nó móvel. Mesmo que o nó correspondente fosse um computador especifico que o agente estrangeiro já conhecesse, ainda haveria outra desvantagem que seria o fato de serem enviadas mensagens na rede e gerados túneis que talvez não sejam utilizados, pois o túnel é estabelecido a partir da entrada do móvel na rede estrangeira, e não a partir da necessidade de envio de pacotes ao nó móvel.

4.1.6 - MPLS como base para a aplicação de Mobile IP hierárquico e para otimização de roteamento em MIP

Nas propostas publicadas em congressos ou em revistas acadêmicas, a otimização de roteamento sempre aparece separada do Mobile IP Hierárquico, mesmo quando se utiliza MPLS. Os artigos que propõem estes dois aperfeiçoamentos do MIP em conjunto com o MPLS trazem sempre estes aperfeiçoamentos como cenários distintos, isto é, tem um

cenário no qual se utilizam LSPs no tunelamento do IP móvel hierárquico e outro cenário distinto, no qual se utilizam túneis LSP na otimização de roteamento em MIP [18, 20].

Em cada um dos cenários apresentados, a sugestão de integração com o MPLS consiste na utilização do LDP para estabelecer túneis LSPs onde, nas sugestões dadas para MIP, tinha-se o tunelamento IP-em-IP. Na aplicação do MPLS no cenário de otimização de roteamento, tem-se a utilização direta do protocolo descrito no *draft* do IETF desta funcionalidade [45] onde os túneis IP-em-IP estabelecidos entre o nó correspondente e o agente estrangeiro e entre o agente estrangeiro antigo e o agente estrangeiro atual são substituídos pelos LSPs estabelecidos através das mensagens de requisição de rótulo e mapeamento de rótulo do LDP. Da mesma forma, a aplicação do MPLS no cenário de Mobile IP com hierarquia é a utilização direta do protocolo descrito no *draft* do IETF sobre o registro regional [29] com túneis definidos entre o agente nativo e o agente estrangeiro de entrada, entre o agente estrangeiro de entrada e o agente estrangeiro regional e entre o agente estrangeiro regional e o agente estrangeiro local. Neste último cenário, a cada registro local, o agente estrangeiro que autentica o nó móvel tem de fazer uma alteração na tabela de roteamento, indicando a nova interface e o novo rótulo a ser utilizado no encaminhamento de pacotes ao nó móvel o novo rótulo é definido a partir das mensagens de requisição de rótulo e mapeamento de rótulo que são trafegadas entre o agente que realiza a autenticação do nó móvel o agente estrangeiro local da sub-rede na qual o móvel está conectado.

O motivo para a separação dos cenários certamente se encontra no fato de que são necessárias diversas adaptações para integração entre estes aperfeiçoamentos. O maior problema a ser enfrentado com certeza é o fato de que o agente nativo mantém, como endereço residente do nó móvel, o endereço do agente estrangeiro de entrada, o que não corresponde ao endereço do agente estrangeiro local. Assim sendo se fosse realizada a otimização de roteamento, o nó correspondente receberia um endereço que não chega diretamente ao móvel, não obtendo assim a função procurada pela otimização. Esta falha está apresentada de forma ilustrativa na fig. 4.7. Vê-se pelas setas vermelhas, nesta figura, o caminho pelo qual os pacotes teriam de passar, mesmo com a otimização de roteamento. Neste exemplo, temos que o pacote provavelmente chegaria com latência menor se fosse enviado diretamente ao agente estrangeiro local no qual o nó móvel se registrou.

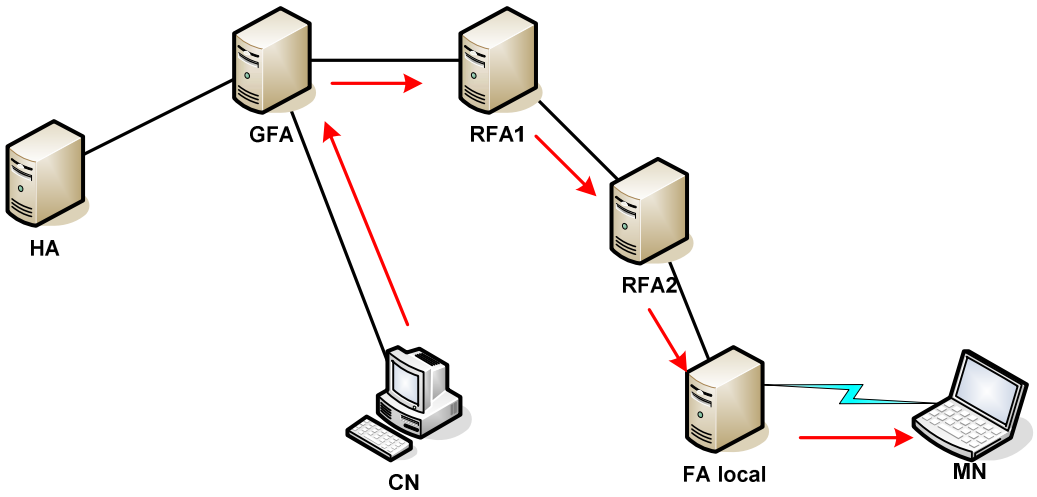


Figura 4.7 - Envio de mensagens em ambiente MIP com otimização de roteamento e hierárquia sem os devidos ajustes.

Os ajustes necessários para que a otimização de roteamento realmente obtenha sucesso consiste na criação de novas mensagens e alterações em algumas mensagens já especificadas, e estas mensagens estão especificadas na seção 4.2 desta monografia, onde é descrita a sugestão criada para uma integração eficiente das tecnologias de Mobile IP e MPLS para obter latência reduzida tanto no *handoff* quanto na comunicação quando os agentes encontram-se muito distantes um do outro.

4.1.7 - *Handoff* suave em Mobile IP integrado a MPLS através de *Multicast*

A utilização do *Multicast* provavelmente é a que traz o melhor desempenho no que diz respeito ao *handoff* em um mesmo domínio. A proposta traz a situação na qual se utiliza o Mobile IP hierárquico em uma rede MPLS onde cada agente estrangeiro regional é responsável por um domínio [63]. Ao entrar em um domínio da rede, o móvel envia uma requisição de registro ao agente estrangeiro local que o envia ao agente estrangeiro regional, e após o registro, o RFA estabelecerá túneis LSP através de mensagens LDP de requisição de rótulo e mapeamento de rótulo com o agente estrangeiro local onde o nó móvel está conectado e com os agentes das sub-redes vizinhas. O conjunto de LSPs formado após o registro do móvel é chamado de grupo LSP.

Quando chegam pacotes endereçados ao nó móvel no agente estrangeiro regional, ele enviará estes pacotes em todos os túneis LSPs do grupo LSP criado para atender o nó

móvel. Desta forma, quando o nó móvel se mover de uma célula para outra deste domínio, os dados encontram-se disponíveis para ele. A fig. 4.8 ilustra o envio dos pacotes para um nó móvel durante seu *handoff* neste sistema. Nesta figura, os cilindros azuis representam os túneis LSPs e as setas vermelhas indicam a transmissão de pacotes de dado para o nó móvel.

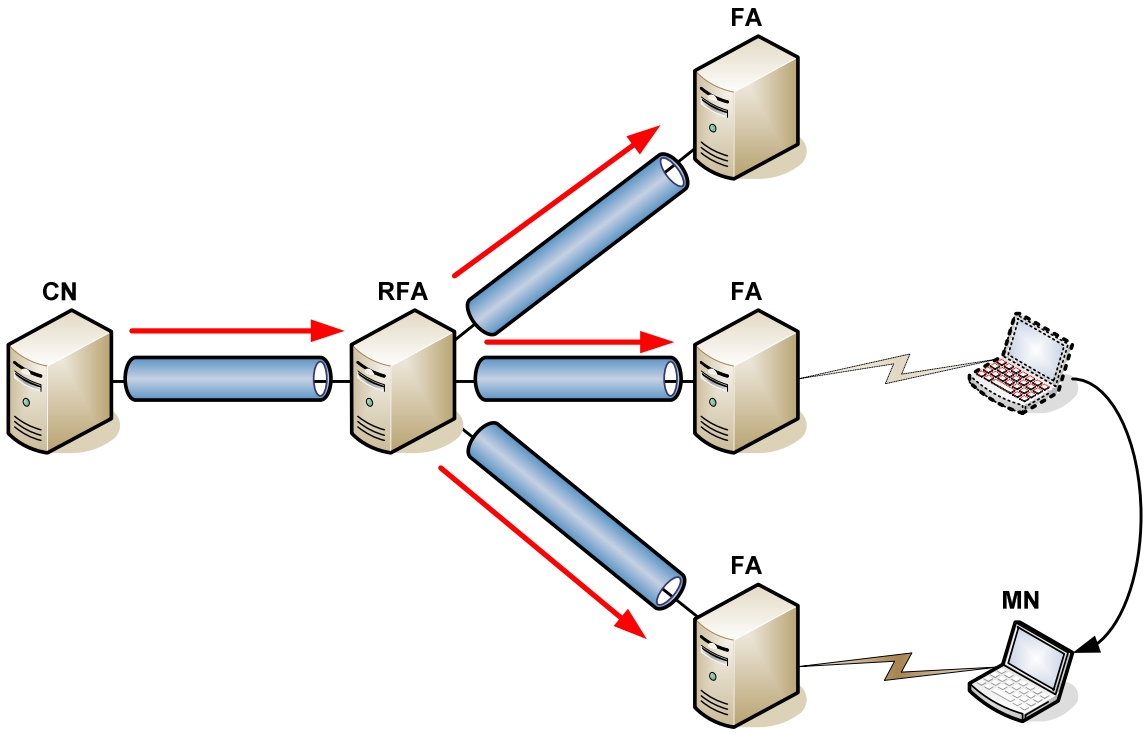


Figura 4.8 - Envido de pacotes por meio de *multicast* durante um *handoff*.

Após o *handoff* neste sistema, o agente estrangeiro local no qual o nó móvel se conectou deve enviar uma mensagem de notificação da nova posição do nó móvel dentro deste domínio para o agente estrangeiro regional para que este atualize o grupo LSP referente a este nó móvel, isto é, retirar do grupo e encerrar os túneis que levam a células que não são mais vizinhas, criar túneis com células vizinhas à atual localização do nó móvel e que ainda não eram vizinhas da célula onde o móvel se encontrava anteriormente e acrescentar estes novos túneis no grupo LSP.

Apesar de esta proposta apresentar uma ferramenta que pode vir a ser capaz de apresentar o melhor desempenho na redução da latência de *handoff*, ela apresentou duas falhas. A primeira foi não definir como é feito o registro do nó móvel quando realizando a mudança de célula. Se for considerado que ele faz o registro regional comum, podem-se perder

alguns pacotes entre o momento em que o móvel envia a requisição de registro regional e o momento em que recebe a resposta de registro. Caso seja considerado que, pelo fato de o agente estrangeiro local precisar mandar uma notificação ao agente estrangeiro regional avisando do *handoff*, o nó móvel já está autenticado antes mesmo de mudar de célula, não ficou definido como ele faz para realizar este pré-registro.

O outro problema a ser considerado é o fato de que durante o período em que o nó móvel não estiver fazendo *handoff*, o sistema estará ocupando desnecessariamente banda entre o agente estrangeiro regional e os agentes estrangeiros locais das células vizinhas. Caso o nó móvel se conectar durante muito tempo em uma única célula deste sistema e depois desligar, o sistema terá ocupado a banda em todos os vizinhos da célula onde o nó móvel se encontrava durante todo o tempo sem fazer uso da mesma. Uma forma eficiente de se lidar com este problema é buscar uma forma de determinar quando um *handoff* está em andamento para então iniciar o envio de pacotes em *multicast* para os FAs locais de todas as células vizinhas.

A seguir, é apresentada a proposta desenvolvida neste trabalho para o aperfeiçoamento do protocolo IP móvel, integrando-o à tecnologia MPLS de forma a reduzir latência de *handoff* e a latência no envio de mensagens de um nó correspondente qualquer para o nó móvel.

4.2 - PROPOSTA DESENVOLVIDA PARA A INTEGRAÇÃO DO MOBILE IP COM MPLS

Com base nas propostas verificadas nos artigos e textos técnicos, foi desenvolvida uma proposta que une diferentes funcionalidades das propostas analisadas de forma a obter redução tanto no atraso de *handoff*, quanto no atraso no envio de pacotes. Foi desenvolvido, nesta proposta, um pré-registro que se baseia nas informações utilizadas pelos agentes estrangeiros regionais para autenticar os nós móveis. Foi criado um novo processo de otimização de roteamento que permite a otimização combinada com o MIP hierárquico, trazendo as vantagens destes dois mecanismos simultaneamente. O processo de *multicast*, que em propostas anteriores ocorria constantemente nas células vizinhas à localização do

nó móvel, nesta proposta é feita apenas quando é detectado baixo nível de potência, indicando que um provável *handoff* deve ocorrer logo.

As vantagens desta proposta estão no fato de obter a mesma eficiência de otimização de roteamento que se obtém através do protocolo de otimização anterior aliado a um atraso de *handoff* que se espera que seja menor que os apresentados pelas propostas verificadas na bibliografia. A desvantagem do protocolo proposto está na grande quantidade de mensagens de sinalização que são trafegadas por ele.

Nesta proposta, buscou-se otimizar o Mobile IP de forma a solucionar o problema de latência durante o *handoff* e o problema de latência encontrada devido ao fato de os pacotes endereçados ao nó móvel terem de passar pela rede nativa para então serem encaminhadas à rede onde o nó móvel se encontra no momento. Para melhorar o desempenho no envio de pacotes de um nó correspondente ao nó móvel, deve-se substituir o tunelamento IP-em-IP por túneis LSP do MPLS.

A escolha do MPLS para ser utilizado como *backbone* da rede IP móvel se baseia nos benefícios que esta tecnologia oferece: independência com relação à camada de enlace, podendo ser implantado sobre redes de enlace Ethernet, ATM, protocolo ponto-a-ponto, Frame Relay, e outros; suporte à engenharia de tráfego, diferenciação de serviços e reserva de recursos, elementos fundamentais para implantação de uma rede com qualidade de serviço; e reduzida latência no encaminhamento de pacotes devido ao fato de o tamanho do rótulo ser menor que um cabeçalho IP encapsulante do túnel IP-em-IP e, principalmente, devido ao processamento do rótulo nos roteadores internos ao núcleo MPLS ser muito menor que o realizado por um roteador IP comum da *Internet*.

Para o protocolo de distribuição de rótulos, todos os protocolos suportados pelo MPLS podem ser utilizados para que o sistema proposto funcione, mas a recomendação que se faz nesta proposta é a utilização do protocolo RSVP-TE, devido à sua característica de reserva de recursos e a seu suporte à engenharia de tráfego [9], que permitem a utilização de serviços diferenciados. A utilização do RSVP-TE faz com que a aplicação de QoS no sistema exija menos adaptações o mesmo.

No sistema proposto, o MPLS se estenderá até os agentes, não alcançando o nó móvel. É considerado que o enlace entre o nó móvel e o agente estrangeiro causa pouca deterioração no desempenho do sistema, e para se manter um túnel LSP deve-se enviar mensagens periódicas indicando o estado do túnel, o que reduziria o tempo de carga da bateria do nó móvel. Presume-se também que os agentes estrangeiros locais e o agente nativo sejam roteadores de borda da rede MPLS, e os roteadores comutadores de rótulos sejam capazes de realizar registro regional do IP móvel, isto é, podem exercer a função de agente estrangeiro regional e agente estrangeiro de entrada.

Para reduzir a latência no envio de pacotes, além do *backbone* MPLS, foi utilizada também a otimização de roteamento. Para que não seja necessário instalar nenhum elemento em dispositivos fixos comuns, o dispositivo que participará da otimização não será o nó correspondente, mas o roteador de borda que faz interface entra a rede do CN e o núcleo MPLS. Assim como no caso do link do nó móvel, foi considerado que o link entre o nó correspondente e o LER de sua rede não causa grande impacto no desempenho do sistema.

No que diz respeito à latência de *handoff*, serão utilizados os recursos de hierarquia de agentes estrangeiros em conjunto com *multicast* e pré-registro. Para que a hierarquia e a otimização de roteamento funcionem em conjunto, devem-se fazer algumas alterações, dentre as quais podem ser citados o envio de informações sobre o endereço residente local do nó móvel, isto é, o endereço do agente estrangeiro local da sub-rede à qual o móvel está conectado, ao agente nativo, para que este possa informar aos roteadores de borda dos nós correspondentes sobre a atual localização do nó móvel para que a otimização funcione da forma desejada.

O *multicast* é realizado de forma semelhante ao descrito na seção 4.1.7 deste trabalho, mas com a diferença de que ele deve ocorrer unicamente durante a transição do móvel de uma sub-rede para outra. Para se alcançar esta característica, deve-se fazer alguma análise sobre a qualidade do sinal, seja potência do sinal recebido, taxa de transmissão ou utilização do *hardware* para determinar se existe outro sinal que esteja com potência suficiente para que possa vir a ocorrer o *handoff*.

Para que o *multicast* realmente obtenha o resultado esperado, deve-se fazer um sistema de pré-registro, para que não seja necessário esperar o móvel fazer um registro regional no

agente estrangeiro regional. Este pré-registro ocorre através do envio da chave de registro que se encontra no RFA para os FAs locais das redes vizinhas no momento em que se percebe a possibilidade de *handoff*, isto é, junto com o início do *multicast* para que, quando o nó móvel se mover para uma célula vizinha, a única pausa na comunicação seja o tempo de envio do pacote de requisição de registro e recebimento do pacote de resposta de registro.

Os processos fundamentais para que este sistema funcione são a descoberta de agentes, que permanece inalterado em relação à RFC 3344, o registro no agente nativo, o registro regional, que ocorre quando um nó móvel já registrado se move para outra rede, o processo de encaminhamento de mensagens através da otimização de roteamento e o encaminhamento de pacotes durante *handoffs*.A seguir, tem-se a descrição destes processos detalhando a troca de mensagens entre os elementos do sistema para que o mesmo funcione e o formado destas mensagens para que contenham toda a informação necessária para que os elementos consigam realizar as tarefas.

4.2.1 - Descoberta de Agentes

Na especificação do Mobile IP hierárquico, há uma pequena alteração no processo de descoberta de agentes, que consiste no acréscimo de uma extensão no anúncio de agente, contendo o endereço do agente estrangeiro de entrada e dos agentes estrangeiros regionais. A utilização desta extensão implica a utilização de uma hierarquia bastante rígida, isto é, o agente estrangeiro local tem uma única conexão que leve ao agente nativo de qualquer nó móvel que venha a se conectar em sua rede.

Para permitir maior liberdade quanto à formação da rede, os agentes estrangeiros de hierarquia maior não são pré-configurados nos agentes locais, mas descobertos durante a execução do 1° registro do móvel na rede. Em situações nas quais o agente estrangeiro local tiver mais de uma interface para se comunicar com as redes nas quais podem-se encontrar os agentes nativos, com esta adaptação no protocolo, ele pode escolher o caminho mais curto ao agente nativo do nó móvel que deseja se conectar. Outra vantagem desta escolha é o fato de o nó móvel poder portar uma implementação da RFC 3344 ao invés da implementação com registro regional.

Visto que não será informado ao nó móvel o endereço dos agentes estrangeiros de hierarquia maior através do anúncio de agentes, será utilizado o formato de mensagem contido na RFC 3344 [43]. Caso o administrador da rede opte por utilizar o anúncio apenas em resposta a uma solicitação de agente do nó móvel, esta solicitação também seguirá o modelo especificado na mesma RFC.

4.2.2 - Registro no agente nativo

Mesmo em ambiente que implemente registro regional, é necessário que na primeira vez que um nó móvel se conecte a uma rede qualquer, ele se registre no agente nativo, isto é, a requisição de registro deve ser enviada ao agente nativo para que este aceite ou negue o seu registro. Este procedimento é bastante semelhante ao procedimento especificado na RFC 3344, mas existem algumas alterações: o acréscimo de uma extensão de endereço residente local na requisição de registro; utilização de chaves de registro na mensagem de resposta de registro e inicialização dos túneis LSP através das mensagens Path e Resv do RSVP-TE. A fig. 4.9 apresenta um diagrama com a troca de mensagens que ocorre no processo de execução do registro no agente nativo.

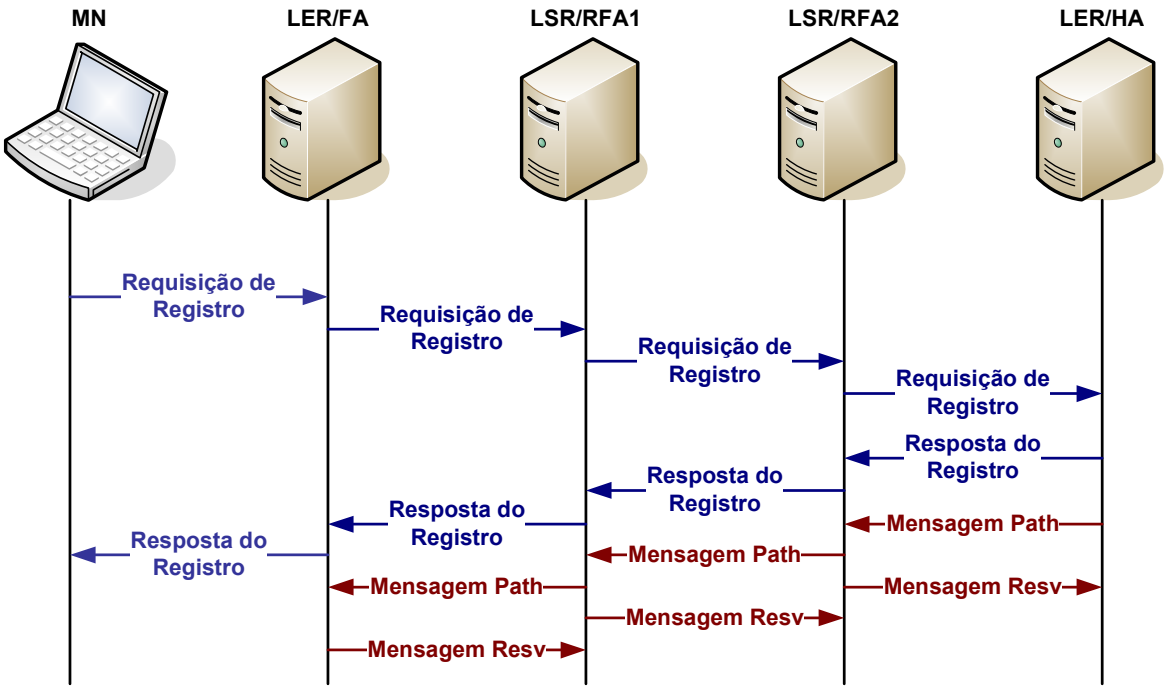


Figura 4.9 - Registro do nó móvel no agente nativo

Após receber um anúncio de agente, um nó móvel não registrado inicia o processo de registro enviando ao agente estrangeiro local uma mensagem de requisição de registro comum do Mobile IP. O agente estrangeiro local ao receber o registro, acrescenta uma extensão de endereço residente local no final do registro e o encaminha via roteamento IP ao agente estrangeiro regional mais próximo no caminho ao agente nativo. Uma ilustração da mensagem de registro com a extensão de endereço residente local se encontra na fig. 4.10.

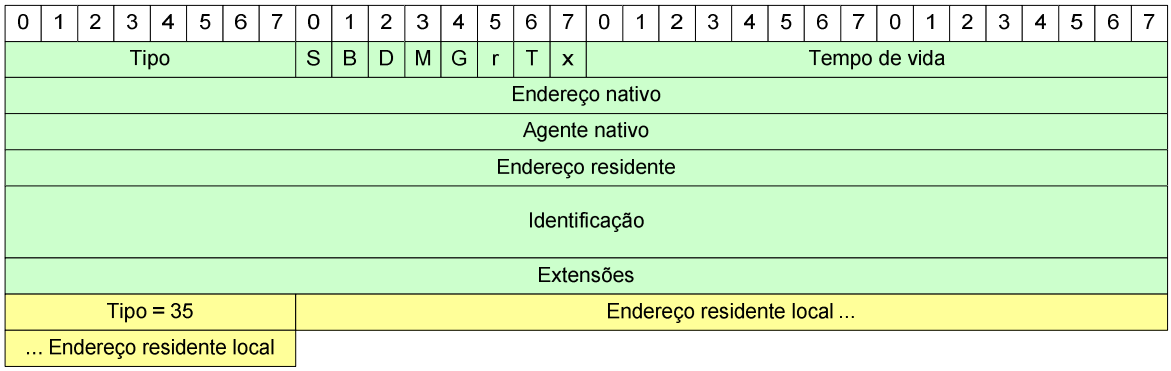


Figura 4.10 Formato da mensagem de requisição de registro com a extensão de endereço residente local.

A extensão de endereço residente local é importante porque é através dele que o agente nativo poderá conhecer o endereço do nó móvel para informá-lo ao roteador de borda de algum nó correspondente que deseje se comunicar com o nó móvel. Esta extensão é composta basicamente de dois valores. O primeiro valor, composto de 1 *byte*, precisa ter valor 35 para que os agentes saibam qual o tipo de extensão que está começando. Este valor foi escolhido pelo fato de ser o primeiro valor não ocupado desde os outros valores de tipos de extensão da requisição de registro. O outro valor, composto de 4 *bytes*, contém o endereço IP do agente estrangeiro local que está servindo o nó móvel que enviou a requisição.

Cada agente estrangeiro regional que recebe a requisição de registro armazena o endereço IP do nó móvel, o endereço residente local contido na extensão de endereço residente local e o endereço residente em uma tabela que será chamada tabela de nós móveis registrados na região. Um exemplo desta tabela pode ser encontrado na tabela 4.1. Neste momento, o agente ainda não preenche a chave de registro. A chave de registro só é preenchida quando

o agente receber uma resposta de registro. Caso o agente não receba uma resposta de registro até o tempo de vida da requisição de registro expirar, ele deve retirar os valores anotados a partir da requisição de sua tabela. A seguir o agente estrangeiro regional substituirá o endereço residente da mensagem pelo seu próprio endereço, pois ele será visto pelo próximo agente como sendo o caminho para onde se devem enviar mensagens para as encaminhar ao nó móvel.

Tabela 4.1 - Tabela de nós móveis registrados na região.

Endereço do MN	Endereço residente	Endereço residente local	Chave de registro	Tempo de vida
10.0.13.2	172.22.20.13	192.168.0.13	1111011101001	130s
10.10.10.54	172.22.20.13	192.168.67.143		584s
10.150.55.67	172.30.40.231	192.168.55.201	1001111101110	57s

Quando a mensagem de requisição de registro chega ao agente nativo, ele avalia se o móvel tem ou não permissão para se registrar. Caso o agente nativo não aceite o registro do nó móvel, ele deve gerar uma mensagem de resposta de registro com código que indique que o registro foi negado e por qual o motivo. A mensagem então será enviada por cada agente estrangeiro até chegar ao nó móvel, e cada agente estrangeiro regional, ao receber esta mensagem, eliminará as informações sobre este nó móvel de sua tabela de nós móveis registrados na região.

Caso o registro do nó móvel seja aceito, o agente nativo deve gerar duas chaves criptográficas que serão utilizadas para a execução do registro regional do nó móvel com uma garantia de segurança. Estas chaves serão adicionadas como extensões de chave de registro no final da mensagem de resposta de registro. A troca de chaves em MIP normalmente envolve extensões de requisição de chave na mensagem de requisição de registro [12, 44, 49], mas como nesta implementação é sempre utilizada a chave devido ao registro regional, optou-se pela utilização do envio das chaves diretamente na resposta de registro.

Cada extensão de chave de registro terá 4 valores: 1 *byte* com valor 36, caso seja a chave a ser armazenada no nó móvel ou 37, caso seja a chave que deve ser armazenada nos agentes estrangeiros regionais; 1 *byte* contendo o subtipo, que é um número inteiro que indica qual

a forma de se utilizar a chave para fazer a autenticação do móvel (se através de MD5, Diffie-Hellman ou algum outro tipo de algoritmo de segurança); 2 *bytes* contendo o tamanha, em bytes, chave que está sendo enviada; e a chave de registro, cujo tamanho estará informado no valor anterior. O formato da mensagem de resposta de registro com as extensões de chave de registro está apresentado na fig. 4.11.

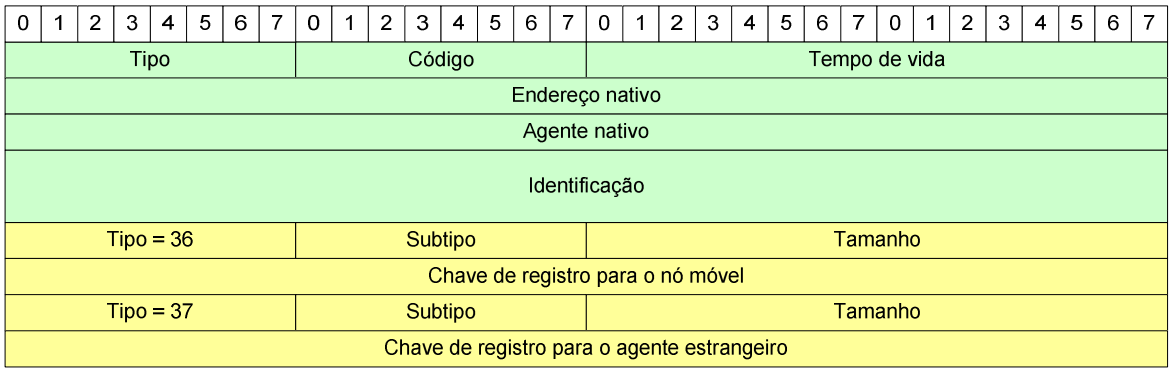


Figura 4.11 - Formato da mensagem de resposta de registro com as extensões de chave de registro.

Após gerar a mensagem de resposta de registro com as extensões de chave de registro, o agente nativo a enviará de volta ao nó móvel através dos agentes estrangeiros pelos quais a mensagem de requisição de registro passou. Cada agente estrangeiro regional pelo qual a mensagem passar, deve anotar a chave de registro presente na mensagem em sua tabela de nós móveis registrados na região, completando as informações sobre o nó móvel que se registrou. Ao chegar ao agente estrangeiro local, este retira a extensão de chave de registro destinada aos agentes estrangeiros regionais e envia ao nó móvel apenas a resposta de registro com a extensão de chave de registro destinada ao nó móvel.

Após o agente nativo enviar a mensagem de resposta de registro, ele inicia um túnel SLP com o agente estrangeiro regional cujo endereço chegou ao agente nativo como sendo o endereço residente. Para iniciar este túnel, o HA envia uma mensagem Path, que é respondida pelo agente estrangeiro regional com uma mensagem Resv, estabelecendo assim o túnel. Assim como o agente nativo, todos os agentes estrangeiros regionais que encaminham a mensagem de resposta de registro devem iniciar um túnel LSP com o próximo RFA pelo qual ele está encaminhando a mensagem.

O motivo da criação deste túnel se baseia no fato de antes do tempo de vida do registro expirar, devem-se trafegar pacotes de registro para confirmar que o nó móvel ainda está conectado à rede. Além da utilização do túnel pela sinalização, existe a utilidade deste túnel para enviar os primeiros pacotes de uma comunicação que um nó correspondente qualquer esteja iniciando com o nó móvel que se encontra em uma rede estrangeira, e possíveis comunicações entre nós correspondentes localizados na rede nativa e o nó móvel.

4.2.3 - Registro regional

O registro regional é o registro no qual um agente estrangeiro executa o processamento da mensagem de requisição de registro para decidir aceita ou não o registro do nó móvel. Nesta proposta, foram inseridas duas novas funcionalidades que tornam o processo de *handoff* mais transparente para o usuário do sistema: o *multicast* durante o *handoff* e o pré-registro. Para que estas funcionalidades executem da forma como especificado neste trabalho, é necessário que o dispositivo que contém o nó móvel possa informar, através do acesso a algum *driver* da interface de rede, alguma informação sobre o sinal que está recebendo. Dentre as informações que podem ser utilizadas, podem ser citados a potência recebida do sinal, atraso no envio de pacotes no enlace sem fio, perda no enlace sem fio, taxa de transmissão ou informações gerais sobre a qualidade de recepção.

Um diagrama simplificado da troca de mensagens referentes ao registro regional pode ser encontrado na fig. 4.12. O processo de registro regional se inicia quando o serviço de nó móvel que é executado no dispositivo móvel percebe que o mesmo está recebendo baixa potência no sinal. Ele então envia uma mensagem de notificação de provável *handoff*, cujo formato pode ser visto na fig. 4.13, ao agente estrangeiro.

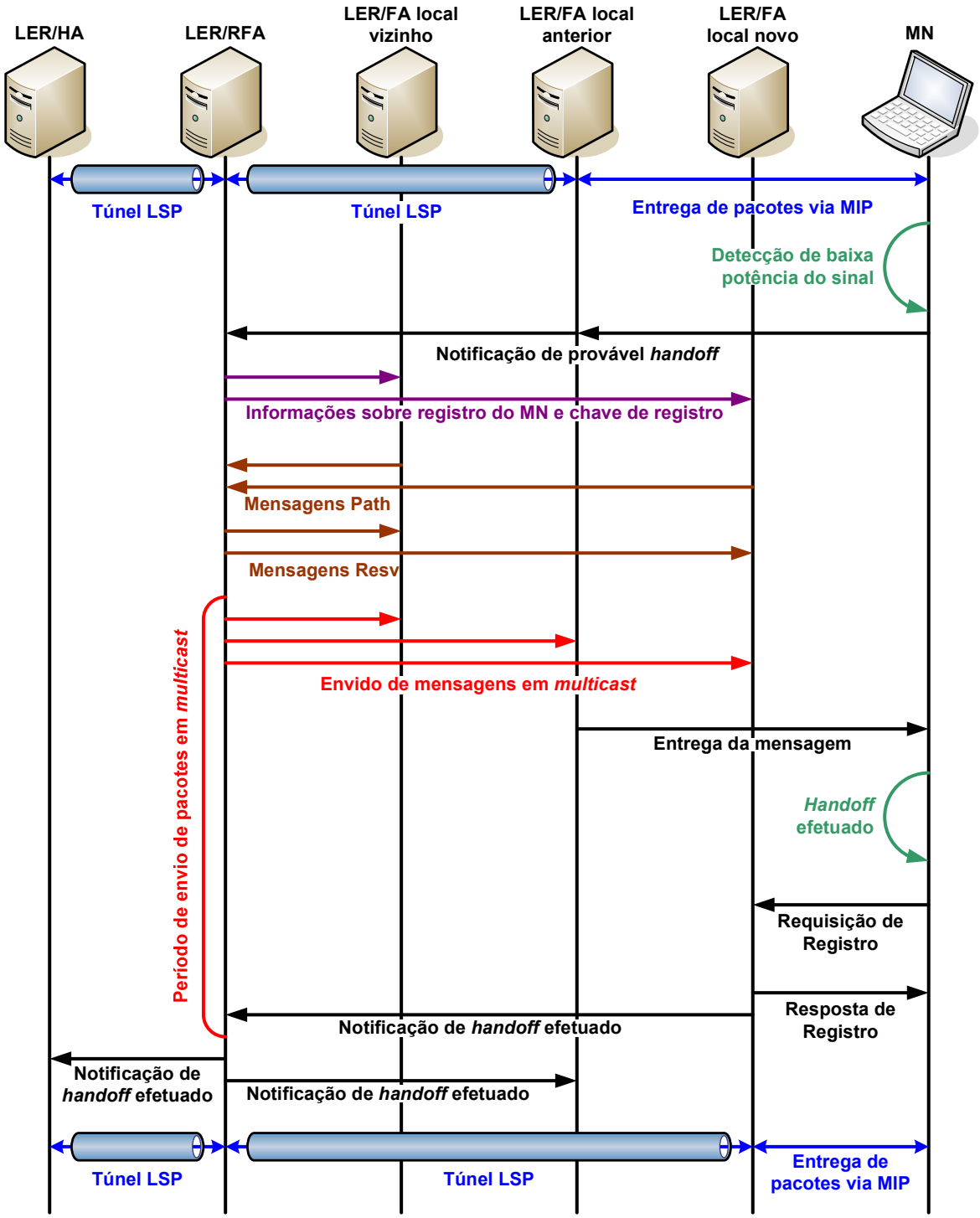


Figura 4.12 - Troca de mensagens durante registro regional com *multicast*.

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Tipo = 20								Tempo de vida																Endereço nativo ...							
... Endereço nativo																								Agente nativo ...							
... Agente nativo																								Endereço residente local ...							
... Endereço residente local																															

Figura 4.13 - Formato da mensagem de notificação de provável *handoff*.

A mensagem de notificação de provável *handoff* começa por um *byte* com valor 20 para identificar o tipo da mensagem, tem 2 *bytes* com o tempo de vida, que é utilizado para determinar quanto tempo o agente estrangeiro deve considerar o nó móvel em processo de *handoff* antes que o *handoff* seja efetuado, ou o nó móvel envie outra notificação de provável *handoff*. A mensagem traz ainda o endereço nativo do nó móvel, o endereço de seu agente nativo e o endereço residente local ao qual o MN está conectado.

Quando o agente estrangeiro local, ao receber esta mensagem a encaminha sem alterações ao agente estrangeiro regional mais próximo. Este, ao recebê-la, envia mensagem de pré-registro aos agentes estrangeiros das redes vizinhas à rede onde o nó móvel se encontra. A mensagem de pré-registro tem o formato de uma mensagem de resposta de registro; a sua diferença é que ela tem valor de tipo igual a 2, traz o endereço do agente estrangeiro regional que está enviando a mensagem e traz obrigatoriamente a extensão de chave de registro com o valor da chave que o agente estrangeiro regional tem armazenada para este nó móvel. O formato da mensagem de pré-registro está apresentado na fig. 4.14. O agente estrangeiro local, ao receber esta mensagem armazena os dados em uma tabela chamada tabela de pré-registros para que, ao receber uma requisição de registro regional, ele possa autorizar o móvel sem precisar enviar a mensagem de requisição de registro regional ao RFA. O formato da tabela de pré-registros está apresentado na tabela 4.2

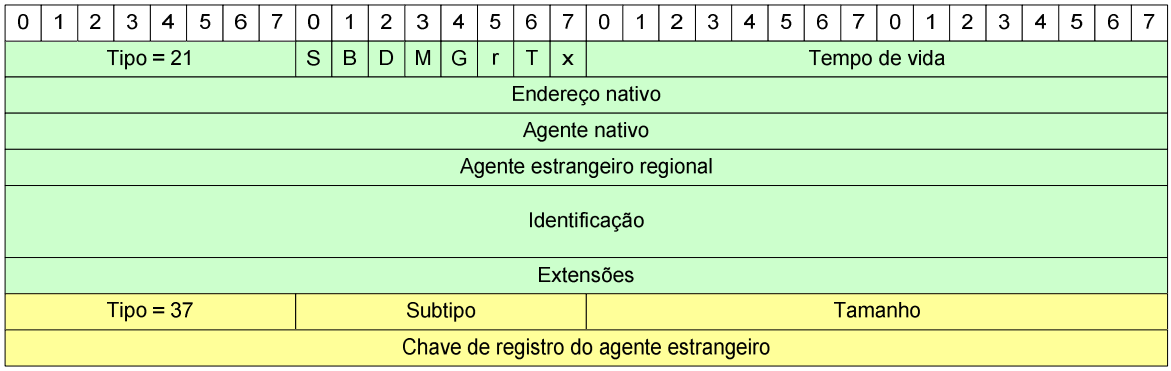


Figura 4.14 - Formato da mensagem de pré-registro.

Tabela 4.2 - Tabela de pré-registros.

End. do MN	End. do HA	End. do RFA	Chave de registro	Tempo de Vida
10.10.10.54	172.22.20.13	192.168.0.13	1111011101001	50s

10.150.55.67	172.30.40.231	192.168.67.143	1001111101110	13s

Para enviar esta mensagem aos agentes estrangeiros locais das redes vizinhas à atual rede do MN, o agente estrangeiro regional utiliza roteamento IP. Após receberem esta mensagem, os agentes estrangeiros locais enviam mensagens Path ao agente estrangeiro regional que enviou o pré-registro, que responde com mensagens Resv, estabelecendo assim túneis LSP. O agente estrangeiro regional acrescenta estes túneis em um grupo *multicast* com o túnel que leva ao agente estrangeiro local da rede onde o nó móvel se encontra. A partir de então todo pacote que é enviado ao nó móvel é enviado via *multicast* a todas as células vizinhas à posição do MN.

Quando o agente estrangeiro regional mais próximo ao agente estrangeiro local envia o pré-registro aos agentes das redes vizinhas, esta mensagem pode passar por outros agentes estrangeiros regionais. Quando o pré-registro passa por um RFA que não tem informações sobre o nó móvel que está realizando o *handoff*, este RFA apenas encaminha a mensagem ao destino e posteriormente fará parte de um dos túneis utilizados no *multicast*. Se o pré-registro passar por um agente estrangeiro regional que faz parte do túnel LSP que leva ao nó móvel, ele substituirá o endereço do agente estrangeiro regional na mensagem pelo seu próprio endereço e o encaminhará ao destino original, e ele acrescentará o endereço do RFA que enviou a mensagem a ele a um grupo *multicast* do qual o endereço para o qual ele enviou a mensagem faz parte. Esta execução elimina a necessidade de rigidez na utilização de hierarquias. Um exemplo de como o *multicast* pode funcionar neste ambiente encontra-se ilustrado na fig. 4.15.

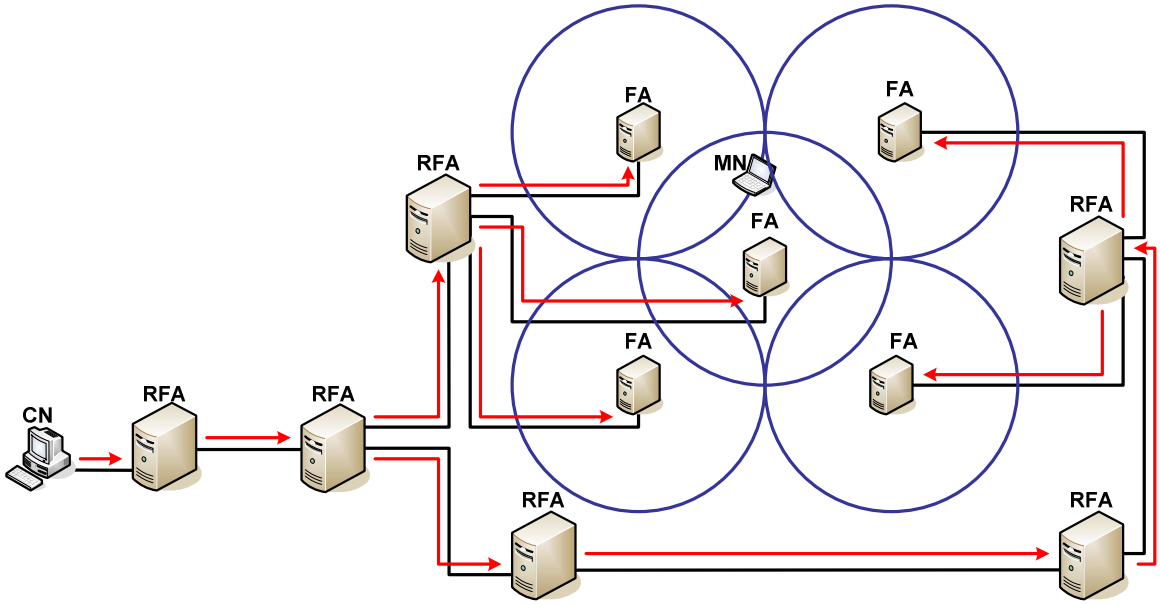


Figura 4.15 - *Multicast* em estrutura com diferentes níveis de hierarquia.

Caso o nó móvel envie uma notificação de provável *handoff*, e ele não executar o *handoff* dentro do tempo marcado no tempo de vida e o sinal recebido continue com baixa potência, ele deve enviar outra notificação para que o agente estrangeiro regional mantenha o *multicast* funcionando. Caso o móvel envie a notificação, mas não realize o *handoff* e a potência do sinal volte ao padrão normal, ao expirar o tempo de vida da notificação, o agente estrangeiro regional deve encerrar o grupo *multicast* e voltar a enviar os pacotes destinados ao nó móvel apenas para o agente estrangeiro local da rede do nó móvel. Da mesma forma, os agentes estrangeiros locais das redes vizinhas à rede onde o MN se encontra, se receberem o pré-registro e o tempo de vida do pré-registro expirar e eles não receberem novas mensagens de pré-registro nem receberem requisição de registro regional por parte do nó móvel, devem retirar as informações deste nó móvel de sua tabela de pré-registros.

Quando o nó móvel realiza o *handoff*, ele deve rapidamente enviar a mensagem de registro regional ao agente estrangeiro local da nova rede na qual ele se conectou. Para que o móvel envie esta mensagem, entretanto, é necessário que ele receba antes um anúncio de agente, pois o anúncio tem informações fundamentais para a criação da mensagem de registro. Para acelerar o envio da requisição de registro, pode-se fazer com que o agente estrangeiro local, quando tiver informações de pré-registro em sua tabela de pré-registro, envie os anúncios com maior freqüência do que o que ele faz quando não há *handoffs* em andamento. A mensagem de registro regional tem o formato apresentado na fig. 4.16

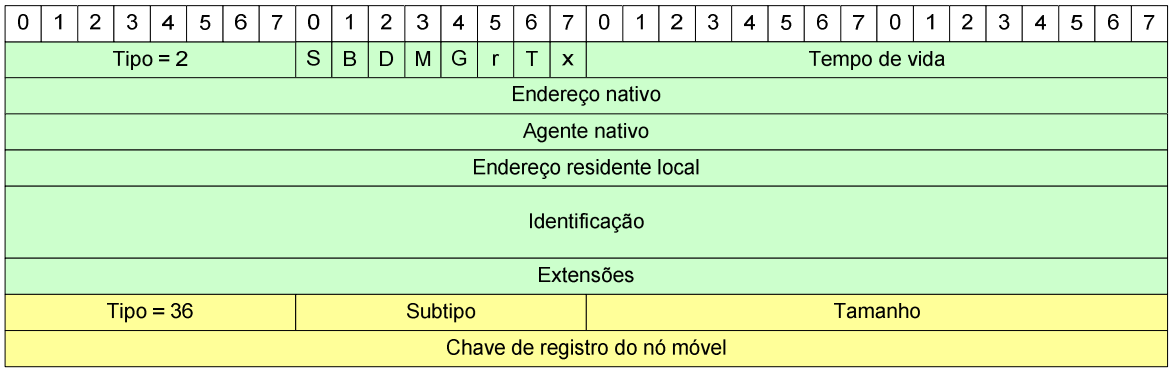


Figura 4.16 - Formato da mensagem de requisição de registro regional.

O agente estrangeiro local, ao receber a mensagem de requisição de registro regional, vai comparar a mensagem recebida com as informações armazenadas em sua tabela de pré-registro, e se esta mensagem combinar com as informações de um dos móveis descritos em sua tabela, ele autoriza o nó móvel na rede, responderá a sua requisição com a resposta de registro regional cujo formato está descrito na fig. 4.17, e encaminhará ao móvel, a partir de então todas as mensagens que então chegando para este móvel através do *multicast*. Nesta situação, o atraso de *handoff* encontrado será apenas o tempo que o móvel espera o anúncio, que dependerá da configuração realizada no agente estrangeiro local, somado ao tempo de envio da requisição do móvel ao FA local, processamento desta mensagem e o envio da resposta do registro. Não haverá, portanto o atraso que se esperaria obter se a mensagem de registro tivesse de ser encaminhada a outros dispositivos tais como um agente estrangeiro de entrada.

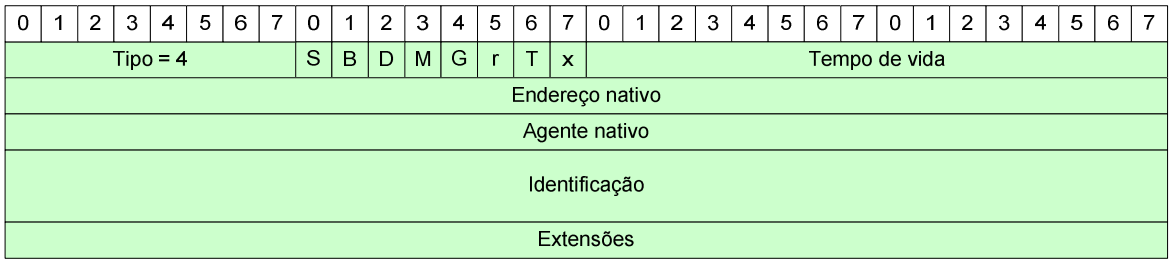


Figura 4.17 - Formato da mensagem de resposta de registro regional.

Outras propostas de se reduzir a latência de *handoff* através de alguns mecanismos que se assemelham a pré-registro, já foram feitas anteriormente. Em uma delas não ocorre pré-registro, mas o registro com o agente estrangeiro local anterior [23]. Nela, espera-se um atraso ainda maior do que o que se esperaria encontrar em uma rede com MIP hierárquico

[29]. Na outra, há um sistema de pré-registro muito semelhante ao especificado neste trabalho, com a diferença de que quem envia as informações para o pré-registro é o agente estrangeiro da rede anterior [39]. Nesta outra proposta parte do princípio de que o FA anterior sabe o endereço do agente da rede para a qual o nó móvel está se movendo, o que é complexo de se determinar. A proposta citada realmente apresenta uma *handoff* que deve ser bastante eficiente, mas poderia adquirir uma eficiência maior se utilizasse a base do MIP hierárquico.

Após o registro, o agente estrangeiro deve enviar uma mensagem de notificação de *handoff* efetuado ao agente estrangeiro regional, que a encaminhará ao agente nativo e ao agente estrangeiro local anterior. E em seguida, o agente regional eliminará o grupo *multicast* e enviará os pacotes em *unicast* ao atual agente estrangeiro do nó móvel. O formato da mensagem de notificação de *handoff* efetuado está representado na figura 4.18.

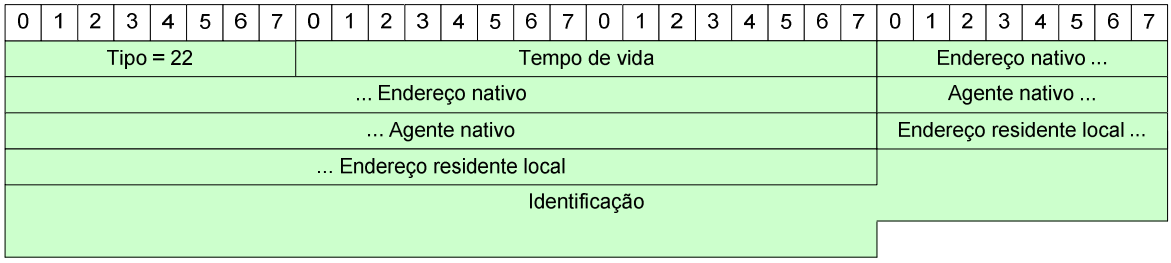


Figura 4.18 - Formato da mensagem de notificação de *handoff* efetuado.

A notificação de *handoff* efetuado deve ser enviada ao agente estrangeiro para que este atualize a sua tabela de localização de nós móvel para poder informar corretamente aos roteadores de borda dos nós correspondentes que venham a desejar se comunicar com o nó móvel. A notificação também deve ser enviada para o agente estrangeiro da rede à qual o nó móvel estava conectado anteriormente para que este envie mensagens de atualização de ligação aos roteadores de borda que já tinham túneis estabelecidos para se comunicar com o nó móvel. Este último procedimento será melhor detalhado na seção 4.2.5.

A utilização do *multicast* nesta proposta é dependente de os agentes estrangeiros regionais terem conhecimento de quais células são vizinhas das células que fazem parte da sua região. A alternativa mais simples de se implementar, e que é recomendada neste trabalho, é a configuração manual por parte do administrador da rede, isto é, o administrador de rede configuraria manualmente em cada RFA os endereços dos FAs locais das redes vizinhas de

cada célula da região. Outra alternativa é o protocolo chamado protocolo de descoberta de agentes de mobilidade vizinhos [21], que prevê duas formas de se determinar células vizinhas. A primeira forma se baseia no princípio de que as redes vizinhas tenham grande visibilidade entre si, para que o agente de uma rede possa receber os anúncios do agente da outra. A outra forma seria utilizando as informações do antigo endereço residente dos nós móveis para determinar as células vizinhas, isto é, o agente estrangeiro, ao receber a requisição de registro de um nó móvel colhe a informação do antigo endereço residente deste móvel e a coloca em uma tabela com os endereços dos agentes vizinhos.

As desvantagens de se adotar este protocolo é que, para a primeira forma de se determinar os vizinhos, teria de se criar células muito próximas umas das outras, perdendo assim área de cobertura, ou tendo de aumentar significativamente a quantidade de antenas transmissoras de sinal. Para a segunda forma, a desvantagem se baseia no fato de que os agentes podem não perceber a existência de uma célula vizinha devido a não ocorrência de *handoff* com esta célula até o momento presente, isto é, na primeira vez que ocorre um *handoff* entre duas células determinadas, o *multicast* e o pré-registro não funcionariam.

Após a determinação da vizinhança de cada célula, o que poderia ser considerado como próximo passo na melhoria de eficiência no envio de mensagens ao nó móvel via *multicast* deve ser procurar verificar para qual célula o móvel está se movendo. Se for possível determinar esta informação, ao invés de enviar *multicast* para um grupo de aproximadamente 7 células, poderia-se enviar o *multicast* apenas para 2 células, reduzindo assim o tráfego gerado durante o *handoff*. Dentre as possibilidades encontradas, há a utilização de informações das antenas que transmitem sinal para o móvel, tentar uma predição da trajetória do movimento do nó móvel através de dados estatísticos ou históricos e utilização de GPS (*global positioning system* —sistema de posicionamento global) para determinar a posição do móvel. A desvantagem da predição de trajetória está na grande probabilidade de erro associada a esta técnica. O GPS não atende muito bem às necessidades por que necessita de visada direta com satélite para funcionar, o que impediria o seu funcionamento em um ambiente com múltiplas células *indoor*. A desvantagem da utilização de informações das antenas transmissoras encontra-se na complexidade de se implementar este sistema, ainda assim esta é a melhor maneira de se coletar esta informação.

Após o registro regional, quando o tempo de vida do registro ocorrer, ele deve fazer novamente o processo de registro no agente nativo. Isso se faz necessário porque, pelo fato de o túnel estabelecido ser feito a partir do roteamento de mensagens do agente estrangeiro regional mais próximo à célula anterior até o novo agente estrangeiro, este pode não ser o caminho mais curto ao agente nativo. Como o caminho encontrado durante o registro regional não deve ser muito diferente do encontrado pelo registro no agente nativo, e túneis de nem todas as comunicações passam por este túnel devido à otimização de roteamento, então não há necessidade de se corrigir o tunelamento logo de imediato após o registro regional, pode-se manter o túnel LSP criado pelo registro regional até que o tempo de vida do registro expire. Uma vantagem de não se ajustar o túnel para o menor caminho logo de imediato é que, se o móvel estiver transitando entre diversas células em um curto período de tempo, será realizada menos sinalização entre o agente estrangeiro e o agente nativo.

Quando o tempo de vida do registro expira, o móvel envia uma requisição de registro para indicar que ainda está em área de cobertura. Esta requisição de registro e sua resposta são enviadas via roteamento IP, pois através dos dados da resposta de registro, os agentes estrangeiros regionais atualizam as suas tabelas de nós móveis registrados na região. O primeiro registro que o nó móvel faz após um registro regional inclui uma correção no tunelamento. Em cada roteador que a mensagem de registro atravessa, é verificado se o móvel faz ou não parte da tabela de nós móveis registrados na região. Caso o nó móvel não faça parte desta tabela, o agente estrangeiro acrescenta os dados do nó móvel na tabela e encaminha a mensagem, acrescentando o seu endereço no campo de endereço residente, tal como é feito no primeiro registro. Caso o nó móvel faça parte da tabela, o agente estrangeiro verifica se o endereço residente combina com o endereço residente apresentado na requisição de registro. Se o endereço residente não combinar, o agente estrangeiro armazena o endereço residente recebido na requisição de registro, e ao receber a resposta de registro, além de a encaminhar ao nó móvel, também iniciará o túnel LSP com o endereço residente armazenado. A fig. 4.19 apresenta uma ilustração de um túnel que pode vir a ser criado pelo processo de registro regional em rosa, e, em azul, o túnel que se encontra após a correção por meio do registro no agente nativo.

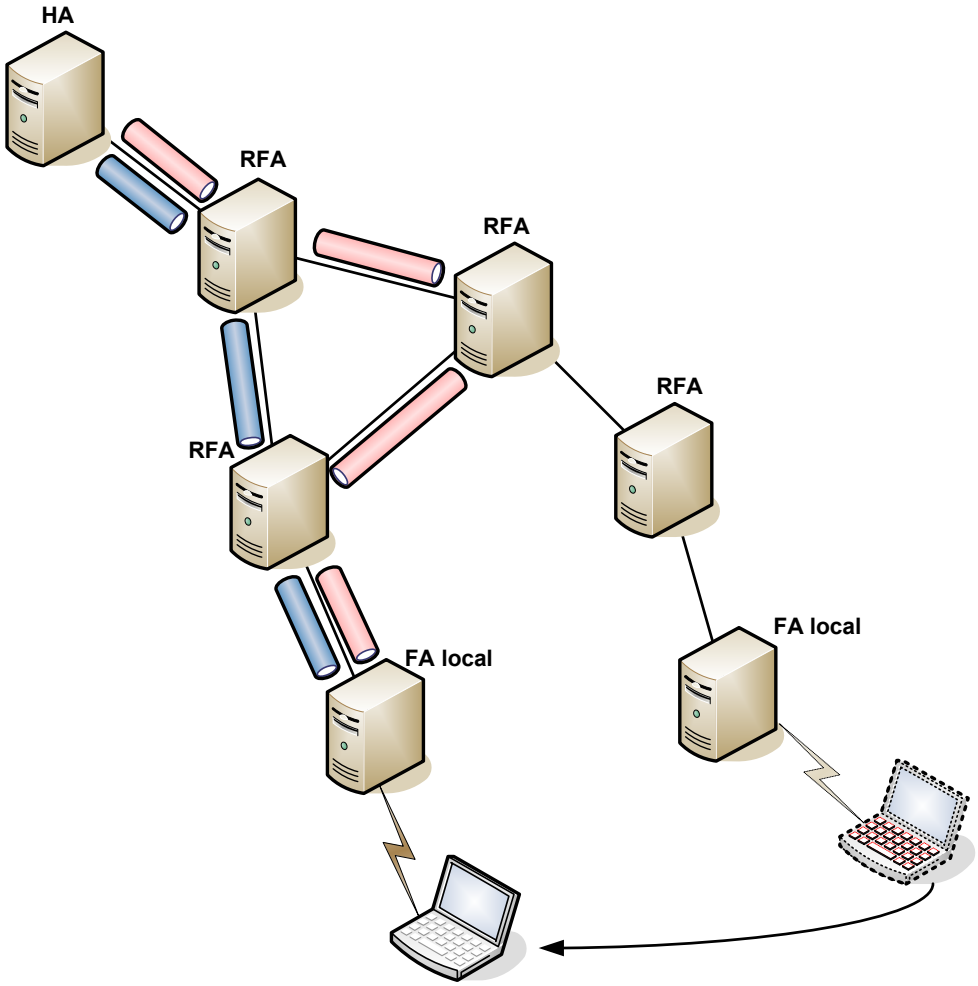


Figura 4.19 - Utilização do registro no agente nativo para atualização do túnel LSP.

4.2.4 - Encaminhamento de mensagens

Para redução na latência do encaminhamento de mensagens, foi adotado neste projeto o conceito de otimização de roteamento. A vantagem deste mecanismo está no fato de não ser necessário que toda mensagem endereçada ao nó móvel tenha de passar pelo agente nativo. A fig. 4.20 apresenta uma situação que ilustra esta vantagem. Em vermelho, está traçado o caminho que uma mensagem precisaria percorrer para ir de um nó correspondente ao nó móvel sem a otimização de roteamento, enquanto em azul está traçado o percurso da mesma mensagem, em uma situação com a otimização.

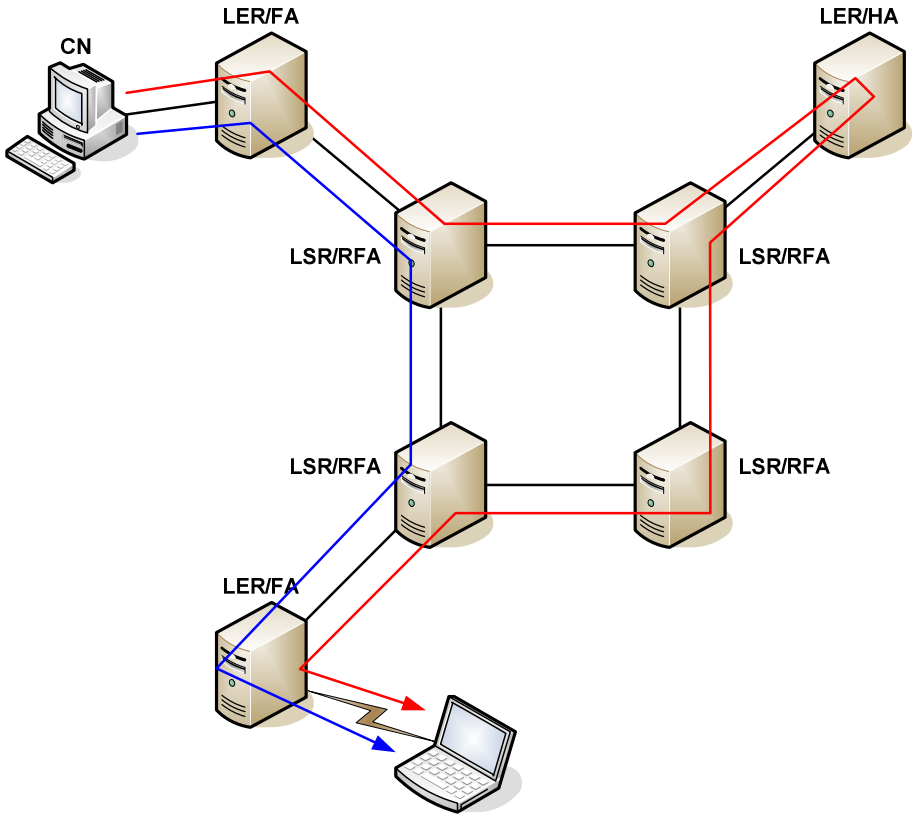


Figura 4.20 - vantagem na utilização da otimização de roteamento.

A otimização de roteamento se baseia na utilização de duas mensagens: a atualização de ligação e o aviso de ligação. Além destas duas mensagens básicas, neste trabalho foram desenvolvidas ainda duas outras mensagens chamadas de requisição de ligação e resposta de ligação. Esta mensagem foi criada para utilização dos benefícios da hierarquia em MIP não somente no registro e para os túneis entre o nó móvel e o agente nativo, mas também para comunicações entre um nó correspondente diretamente com o nó móvel. O formato das mensagens de atualização, aviso, requisição e resposta de ligação estão respectivamente nas fig. 4.21, 4.22, 4.23 e 4.24. As duas primeiras são aproveitadas diretamente da especificação da otimização de roteamento em MIP [45], a terceira é uma cópia da atualização de ligação com tipo diferente para que possa desempenhar a sua função específica, e a quarta é cópia da terceira com alteração de tipo e um campo que indica qual o próximo FA no caminho até o nó móvel.

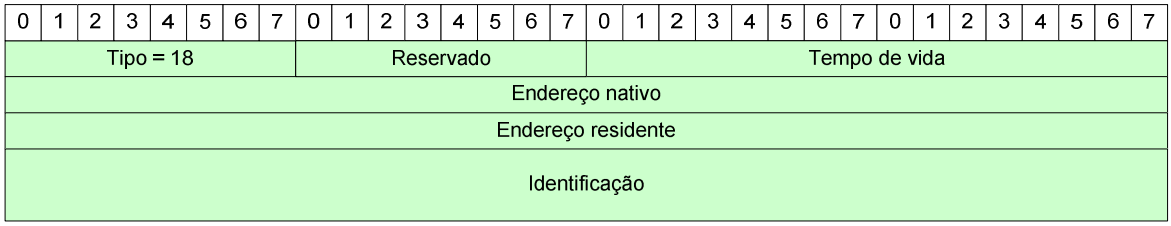


Figura 4.21 - Formato da mensagem de atualização de ligação.

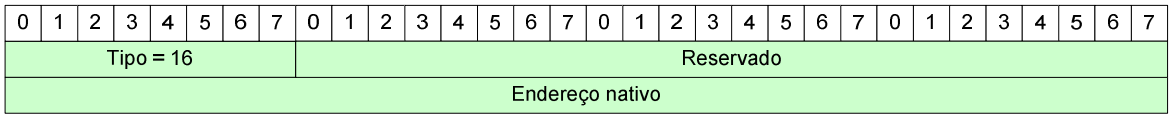


Figura 4.22 - Formato da mensagem de aviso de ligação.

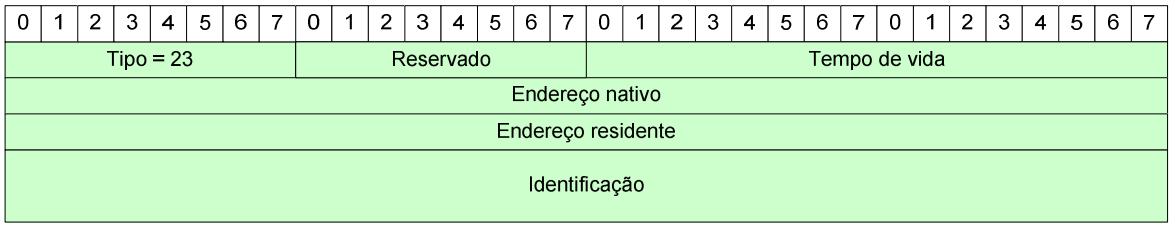


Figura 4.23 - Formato da mensagem de requisição de ligação.

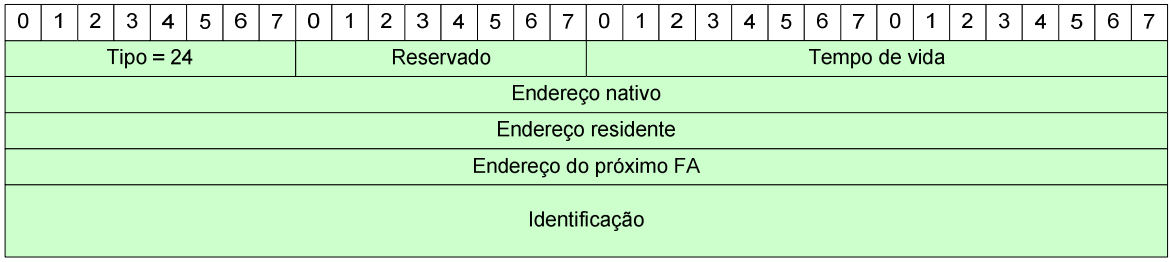


Figura 4.24 - Formato da mensagem de resposta de ligação.

A otimização de roteamento funcionará da seguinte forma: quando um nó correspondente envia pacotes ao nó móvel, se o roteador de borda da rede do CN não tiver informações sobre a localização do nó móvel, ele assumirá que o nó móvel está em sua rede nativa e enviará os pacotes normalmente. Quando os pacotes chegarem à rede nativa do móvel, o agente nativo capturará os pacotes, e os enviará ao nó móvel através do túnel LSP criado após o registro. Em seguida, o agente nativo enviará uma mensagem de atualização de ligação com o endereço do nó correspondente. Esta mensagem na verdade não chega ao nó correspondente, mas através do endereço do CN, ela atingirá o roteador de borda da rede dele. O roteador de borda da rede do nó correspondente, ao receber a mensagem de atualização, deve encaminhar uma mensagem de requisição de ligação com endereço de

destino como sendo o endereço residente do móvel e acrescentar o endereço do nó móvel, seu endereço residente e o tempo de vida em uma tabela chamada tabela de nós móveis conhecidos. O formato desta tabela está apresentado na tabela 4.3.

Tabela 4.3 - Tabela de nós móveis conhecidos.

Endereço do MN	Endereço residente	Próximo FA	Tempo de Vida
10.10.10.54	172.22.20.13	192.168.0.13	50s
10.150.55.67	172.30.40.231	192.168.67.143	13s

No percurso até o nó móvel, todo agente estrangeiro, tanto os agentes regionais quanto o agente local, que receber a requisição de ligação deve responder com uma resposta de registro, colocando no campo de endereço do próximo FA o seu próprio endereço, em seguida ele encaminhará a mensagem ao nó móvel trocando o endereço do remetente pelo seu próprio endereço, colocará as informações do nó móvel na tabela de nós móveis conhecidos e iniciará o túnel LSP com o agente que lhe mandou a requisição. Ao receber a mensagem de resposta de ligação, o agente deve completar a sua tabela de nós móveis conhecidas com o endereço do próximo FA e esperar a mensagem Path para responder com uma mensagem Resv, estabelecendo assim o túnel LSP por onde a comunicação entre o nó correspondente e o nó móvel atravessará. Um diagrama desta troca de mensagens pode ser visto na fig. 4.25.

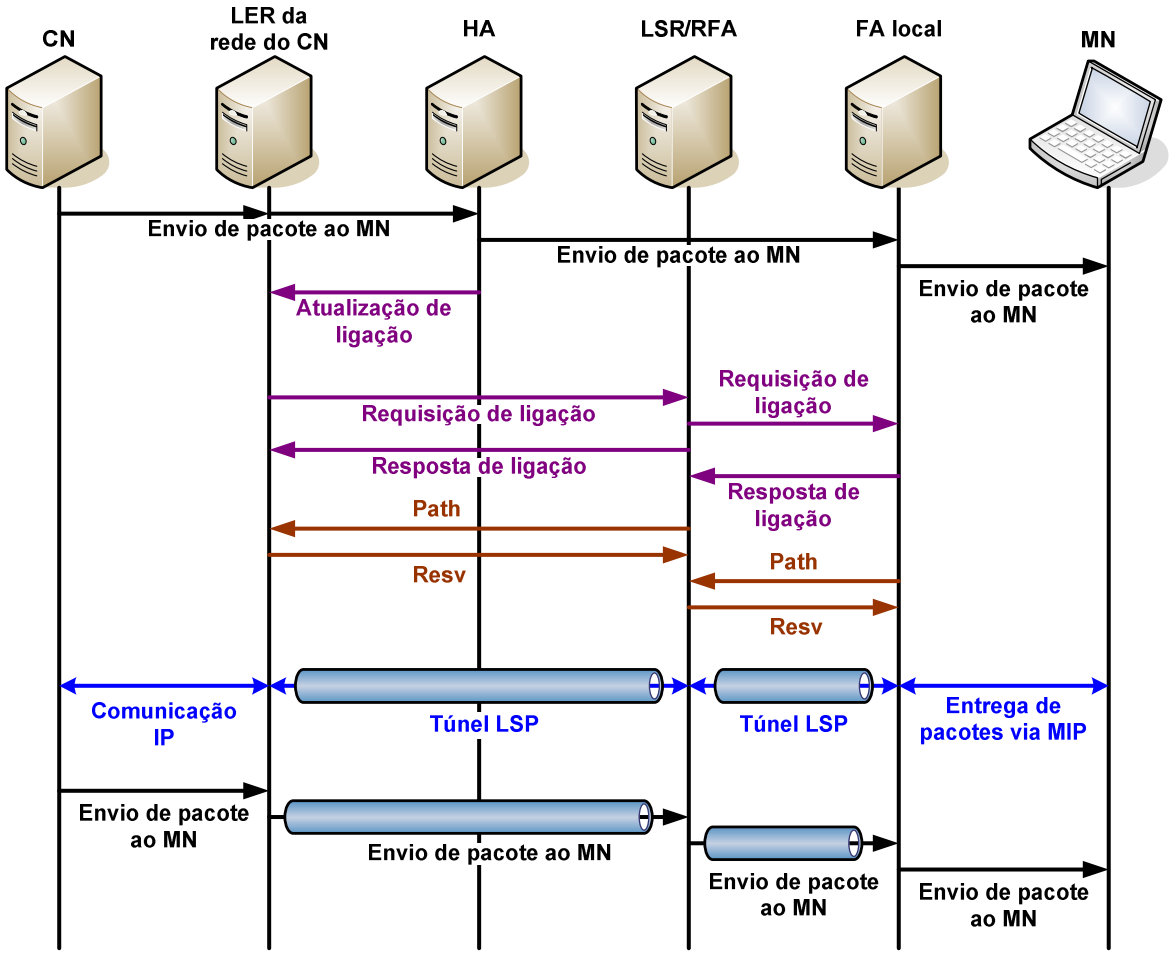


Figura 4.25 - Troca de mensagens para a otimização de rotemento com comunicação iniciada pelo nó correspondente.

Após o estabelecimento dos túneis entre o roteador de borda do nó correspondente e o agente estrangeiro local da rede onde o nó móvel se encontra, sempre que há uma comunicação do nó correspondente para o nó móvel, ela não precisa mais passar pelo agente nativo.

Quando o nó móvel inicia a comunicação com um nó correspondente, o envio da atualização de ligação é feito a partir do agente estrangeiro ao qual o nó móvel está conectado. Visto que em ambiente MPLS os roteadores não irão descartar mensagens baseados no seu endereço de origem, portanto não se utiliza tunelamento reverso neste ambiente, o que faz com que não seja necessária a otimização de roteamento para que as mensagens vindas do nó móvel trafeguem direto ao nó correspondente, mas muito provavelmente a comunicação iniciada pelo nó móvel terá respostas vindas do nó correspondente, o que justifica o envio da atualização de ligação. A troca de mensagens

para otimização de roteamento com a comunicação iniciando no nó móvel está ilustrada na fig. 4.26.

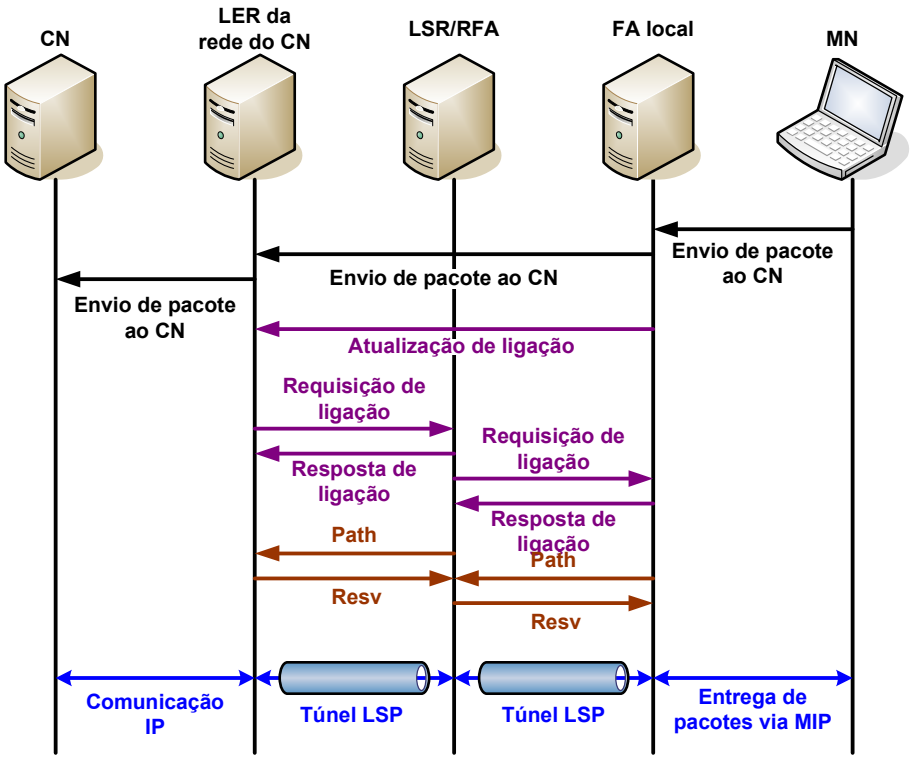


Figura 4.26 - Troca de mensagens para a otimização de rotemento com comunicação iniciada pelo nó móvel.

Se um nó correspondente tentar se comunicar com o nó móvel, e o seu roteador de borda tiver um registro na tabela de nós móveis conhecidos cujo tempo de vida ainda não expirou e o nó móvel já tiver saído da área cujo endereço residente se encontra na tabela de nós móveis conhecidos do roteador de borda do CN, então quando o agente estrangeiro local receber o pacote endereçado ao nó móvel, ele enviará um aviso de ligação endereçado ao nó correspondente. Este aviso será capturado pelo roteador de borda da rede do nó correspondente, que retirará as informações de localização do nó móvel de sua tabela de nós móveis conhecidos e enviará os pacotes endereçados ao nó móvel para a sua rede nativa. Após o envio do aviso, o agente estrangeiro encaminha os pacotes endereçados ao nó móvel à sua rede nativa, para que o agente nativo as encaminhe à atual localização do nó móvel. Esta troca de mensagens está ilustrada na fig. 4.27.

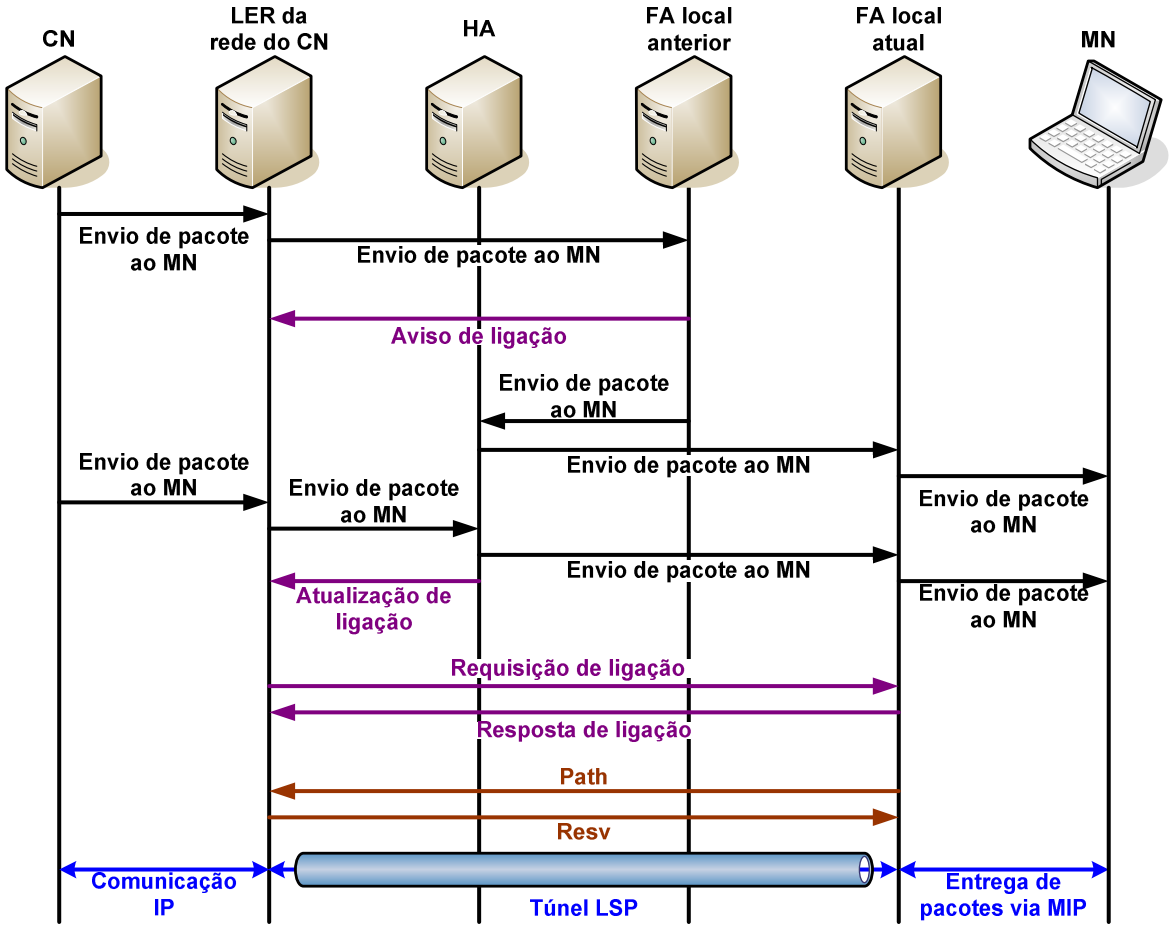


Figura 4.27 - Troca de mensagens realizada quando a tabela de nós móveis conhecidos está desatualizada.

4.2.5 - Encaminhamento de mensagens durante *handoff*.

Assim como as outras características da hierarquia estão sendo utilizadas para melhorar a eficiência da otimização de roteamento, também durante o *handoff*, são utilizados os mecanismos da comunicação com o agente nativo na otimização de roteamento, isto é, quando o nó móvel inicia o *handoff*, não só o túnel com o agente nativo passa pela fase de *multicast*, mas todos os túneis que tem contato com o nó móvel passam por este processo. Visto que muitas vezes os túneis coincidem na região próxima ao nó móvel, muito provavelmente o *multicast* de todas as comunicações será realizado em um mesmo conjunto de equipamentos. Além deste mecanismo, as comunicações existentes ainda passam por outro processo quando ocorre um *handoff* do nó móvel.

Quando ocorre um *handoff* do móvel, o agente estrangeiro regional envia duas notificações de *handoff* efetuado. Uma das notificações é enviada ao agente nativo para que as próximas mensagens de atualização de ligação tenham a informação correta da localização do nó móvel. A outra notificação é enviada ao agente estrangeiro local da rede onde o nó móvel estava conectado anteriormente. Este agente estrangeiro, ao receber a notificação de *handoff* efetuado, verifica todos os túneis LSP que estão estabelecidos com ele devido ao nó móvel de mudou de célula, e envia uma atualização de ligação às outras extremidades de cada túnel, de forma a manter as comunicações que estão ocorrendo com o nó móvel ininterruptas e o *handoff* mais suave possível. A fig. 4.28 apresenta o processo de atualização dos túneis para comunicação com o nó móvel durante o *handoff*.

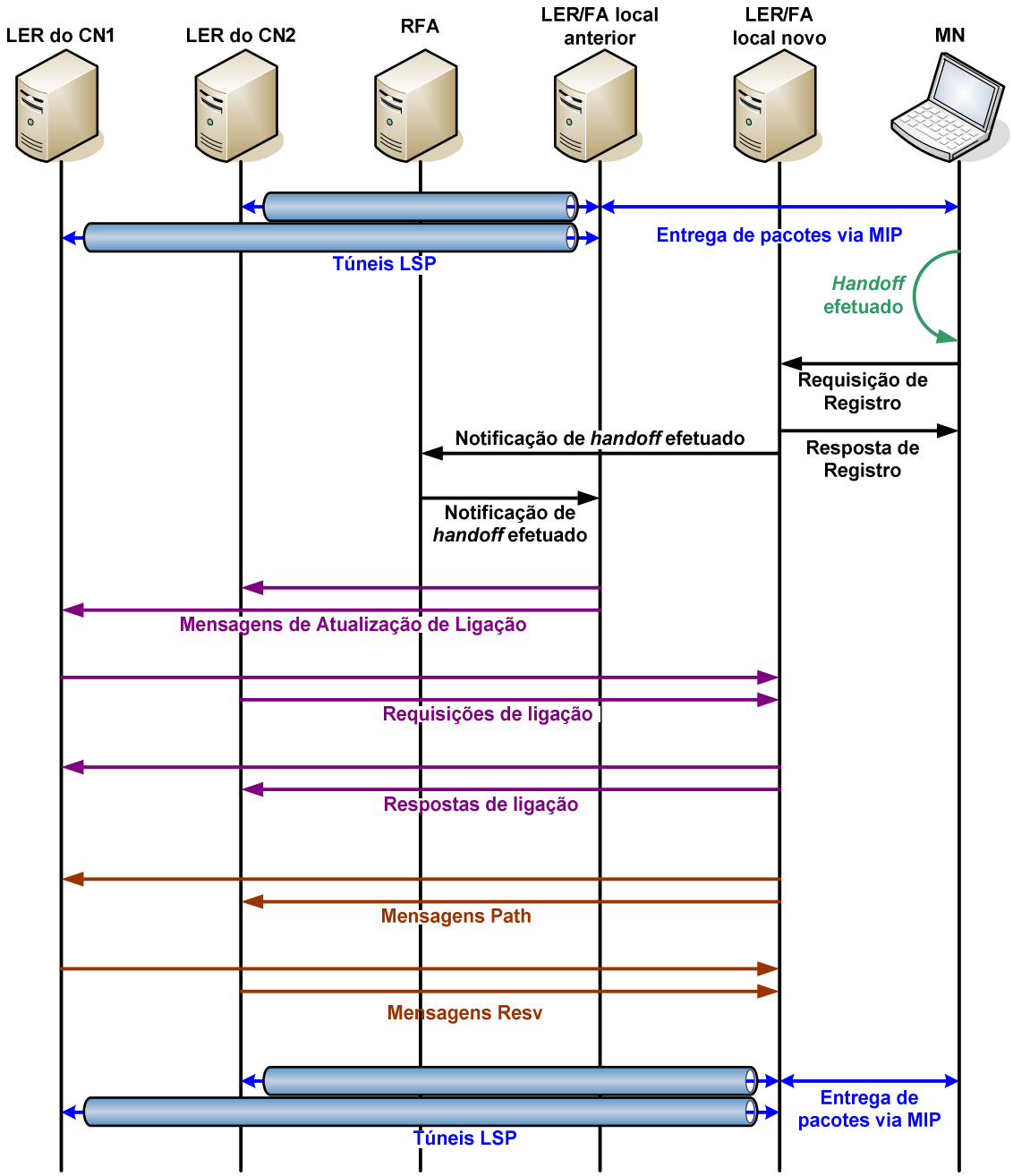


Figura 4.28 - Envio altomático de atualizações de ligação após *handoff*.

Com este mecanismo, a mensagem de aviso de ligação torna-se quase desnecessária, sendo utilizada apenas quando o roteador de borda do nó correspondente recebe uma atualização exatamente quando o nó móvel está realizando o *handoff*, e tenta estabelecer o túnel com o agente da rede estrangeira anterior quando o nó móvel já não se encontra na sua área de cobertura. Para se aprimorar a eficiência do sistema com relação ao *handoff*, pode-se programar o agente estrangeiro para continuar a enviar mensagens em *multicast* durante um tempo a mais depois de enviada a notificação de *handoff* efetuado, assim as mensagens

que chegarem ao agente da rede anterior não precisam ser enviadas ao agente nativo para que este as envie ao endereço residente atual do nó móvel.

4.3 - IMPLEMENTAÇÃO FÍSICA

Apesar de ter sido proposto neste trabalho um protocolo que integra o Mobile IP com o MPLS com otimização de roteamento, hierarquia de agentes, pré-registro e *multicast* para se obter um resultado mais eficiente no gerenciamento de túneis, não foi possível implementar estas funcionalidades num sistema físico. Infelizmente não foi possível criar um módulo que determinasse a potência recebida na interface aérea do nó móvel. A falta de informações sobre o sinal que está sendo recebido na placa de rede sem fio do dispositivo móvel impossibilitou a utilização do *multicast* e pré-registro do sistema proposto.

A implementação do MPLS com RSVP-TE encontrada não permitiu criar os túneis dinamicamente tal como era necessário para utilização da otimização de roteamento e hierarquia de agentes estrangeiros. Foi pensado utilizar o protocolo LDP descrito na RFC 3036 do IETF para poder se alcançar a flexibilidade necessária a este projeto, mas infelizmente a implementação de LDP disponível ainda estava em fase de desenvolvimento e ainda não está pronta para uso [37]. Isso resultou no impedimento de funcionamento da otimização de roteamento e de hierarquia de agentes.

Nesta implementação, utilizou-se o MPLS para linux da sourceforge com protocolo de distribuição de rótulos RSVP-TE do Centro Interuniversitário de Microeletronica da Bélgica [32]. Além da reserva de recursos e a possibilidade de aplicação de serviços diferenciados (*DiffServ*), a implementação de RSVP-TE utilizada permitiu a atribuição de rótulos a fluxos de tráfego existentes na rede MPLS através de linha de comando em terminais linux. Entretanto, houve algumas desvantagens também. Não foi possível realizar a distribuição dinâmica de rótulos, resultando no uso de rótulos pré-definidos. Não houve acesso à LIB (base de informações sobre os rótulos), o que levou à definição dos túneis apenas nas suas extremidades, impossibilitando a utilização de IP móvel hierárquico com otimização de roteamento. Como resultado, a implementação realizada consistiu apenas na substituição dos túneis IP-em-IP próprios de IP móvel por túneis RSVP estáticos.

4.3.1 - Características do sistema implementado

No sistema implementado, têm-se túneis estabelecidos através do RSVP-TE entre os agentes estrangeiros e o agente nativo. Quando um nó móvel se move para algum agente estrangeiro, o agente nativo mapeia toda a informação destinada a este nó móvel no túnel que leva ao agente estrangeiro da rede na qual o nó móvel se encontra. A fig. 4.29 ilustra a utilização dos túneis pré-definidos. Têm-se, nesta figura, três agentes estrangeiros, e para cada estrangeiro o agente nativo terá um túnel LSP, que está representado por um conjunto de segmentos de retas colorido.

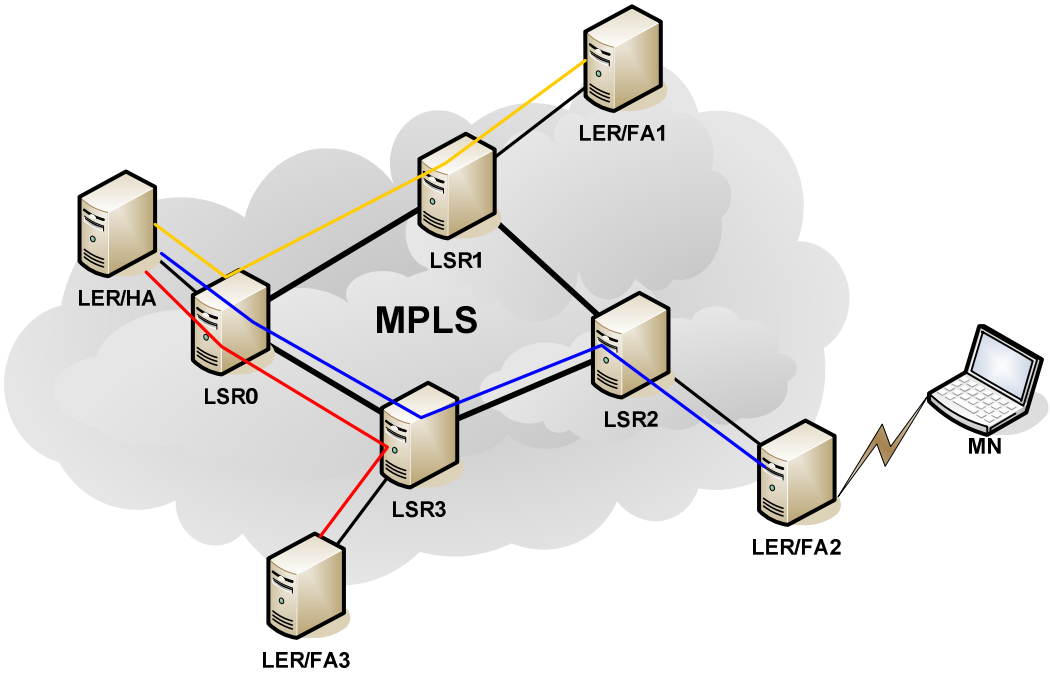


Figura 4.29 - Funcionamento da implementação realizada no laboratório.

Neste ambiente, quando ocorre um *handoff*, não é necessário realizar o processo de estabelecimento de túneis. Basta o agente nativo desfazer o mapeamento dos fluxos para o nó móvel do túnel anterior e criar um novo mapeamento para o nó móvel no túnel novo. Além do mapeamento, é necessário que o agente estrangeiro possa entregar as mensagens endereçadas ao nó móvel quando o mesmo estiver em sua rede, e para isso pode-se facilmente acrescentar novas regras na tabela de roteamento do agente estrangeiro quando

este recebe uma mensagem de resposta de registro com código 0 ou 1 endereçada ao nó móvel, através de linha de comando de terminal linux.

Não foi realizado nenhuma alteração de protocolo com relação aos pacotes enviados pelo nó móvel. O túnel reverso só é utilizado quando há possibilidades de que roteadores IP venham a descartar as mensagens do nó móvel enviadas diretamente ao destino devido ao endereço de origem não condizente com a região de origem da mensagem. Uma vez que no ambiente MPLS o cabeçalho IP não é analisado, o túnel reverso se torna uma fonte de atraso desnecessário, sendo, portanto descartado.

Este sistema realiza Mobile IP com tunelamento LSP ao invés do tunelamento IP-em-IP com tunelamento triangular. Este sistema traz as mesmas vantagens do MIP sobre MPLS com a vantagem de não haver o atraso por encapsulamento e desencapsulamento IP-em-IP nas mensagens enviadas ao nó móvel, e o tamanho dos pacotes serão aproximadamente 20 bytes menores devido ao fato de haver apenas um cabeçalho IP sob o rótulo MPLS.

4.3.2 - Adaptações realizadas em código fonte

As alterações que foram realizadas consistiram de acréscimos e substituições no agente nativo e no agente estrangeiro do Mobile IP. Foi utilizado para estes agentes o código fonte do Dynamics, disponível na página da Internet do Dynamics na SourceForge [10]. Basicamente, o procedimento consiste na criação do túnel no ato do registro bem sucedido e desativação do mesmo quando é verificado que o móvel não mais se encontra na rede estrangeira onde ele se cadastrou.

No agente nativo, deve-se eliminar o bloco de código responsável pelo encapsulamento IP-em-IP e acrescentar o mapeamento do nó móvel através do túnel que leva ao agente estrangeiro no qual ele está conectado. Para eliminar o encapsulamento, de uma forma muito simples e eficaz, podem-se retirar as chamadas da função `create_binding`, porque esta é a função responsável por criar uma associação entre os nós móveis localizados em uma rede estrangeira e associá-los a um endereço de agente estrangeiro para que seja feito o tunelamento IP-em-IP. Ao retirar esta função, sempre que o HA receber um pacote destinado ao MN ele tentará enviá-lo através da tecnologia de rede

disponível; o que pode significar uma tentativa de devolver o pacote inalterado à rede, caso não haja nenhuma indicação de roteamento direto para o MN.

Para o novo mapeamento de tráfego destinado ao nó móvel, logo após o envio do registro do móvel, que é realizado pela função `send_reg_repl`, deve-se utilizar o endereço do agente estrangeiro associado ao nó móvel que está fazendo registro para determinar qual o rótulo a ser utilizado para este móvel. Para isto, é necessário que o agente nativo tenha uma lista dos endereços dos agentes estrangeiros aos quais o nó móvel pode se conectar e o rótulo que deve ser utilizado no respectivo FA. A verificação do rótulo com base no endereço do agente estrangeiro pode ser verificado de forma simples através de comparações em estruturas if-else ou switch-case, tal como nos exemplos abaixo:

```
if (endereco_fa == endereco_fa1) {
    rotulo = rotulo1;
} else if (endereco_fa == endereco_fa2) {
    rotulo = rotulo2;
} else if (endereco_fa == endereco_fa3) {
    rotulo = rotulo3;
};
```

```
switch (endereco_fa) {
    case endereco_fa1:
        rotulo = rotulo1;
    case endereco_fa2:
        rotulo = rotulo2;
    case endereco_fa3:
        rotulo = rotulo3;
```

Em seguida, deve-se utilizar o rótulo definido na comparação e o endereço do nó móvel que está se registrando para criar o mapeamento do fluxo de pacotes para o móvel neste túnel. Para realizar este mapeamento, é utilizado o comando de terminal linux do RSVP. Este comando segue a seguinte sintaxe: `./tunnel -m -p <protocolo> -d <endereço de destino>/<máscara> -l <rótulo>.` Para se executar os

comandos de terminal linux através do código C ANSI, foi utilizado o comando `system()`.

No agente estrangeiro, deve-se também retirar o encapsulamento e ajustar a configuração do agente para fazer o tunelamento triangular, isto é, encaminhar os pacotes enviados pelo nó móvel diretamente ao destino, sem encaminhar ao agente nativo. Além disso, é necessário configurar as rotas IP para que, ao receber pacotes MPLS com destino ao MN registrado, ele possa saber em qual interface o nó móvel está. Para se retirar a criação do túnel no FA, basta retirar a chamada de função `mn_addr_add()`, que é a função responsável por cadastrar nós móveis para terem seus pacotes tunelados. Ao invés desta chamada de função, deve-se acrescentar as rotas para entrega de pacotes ao nó móvel através do comando linux `route`, cuja sintaxe é:

```
ROUTE ADD –NET <endereço da rede>/<máscara> -DEV <interface>
```

No comando `route`, deve-se utilizar o endereço do nó móvel como sendo o endereço da rede, e a mascara deve ser 32, ou 255.255.255.255, para especificar que esta rota acrescentada é para apenas um único endereço. A interface utilizada neste comando é a interface pela qual o agente estrangeiro acessa o nó móvel. No código do agente estrangeiro, a informação sobre qual a interface pode ser encontrada pela interface na qual a resposta de registro está sendo encaminhada para o nó móvel.

4.3.3 - Verificação do funcionamento da implementação

Para a validação da implementação feita, foi recompilado o Mobile IP com as alterações descritas acima e instalado nos respectivos agentes sob a topologia da fig.30, com o endereçamento indicado na tabela 4.4. Todas as máquinas, com exceção do nó móvel, fazem parte de uma rede MPLS, e portanto tiveram o *kernel* do Linux recompilado com o *patch* do MPLS. Foi utilizado como sistema operacional o Linux Red Hat 9.0 e os *kernels* 2.4.20-8 no nó móvel e 2.4.19 nos demais elementos do sistema.

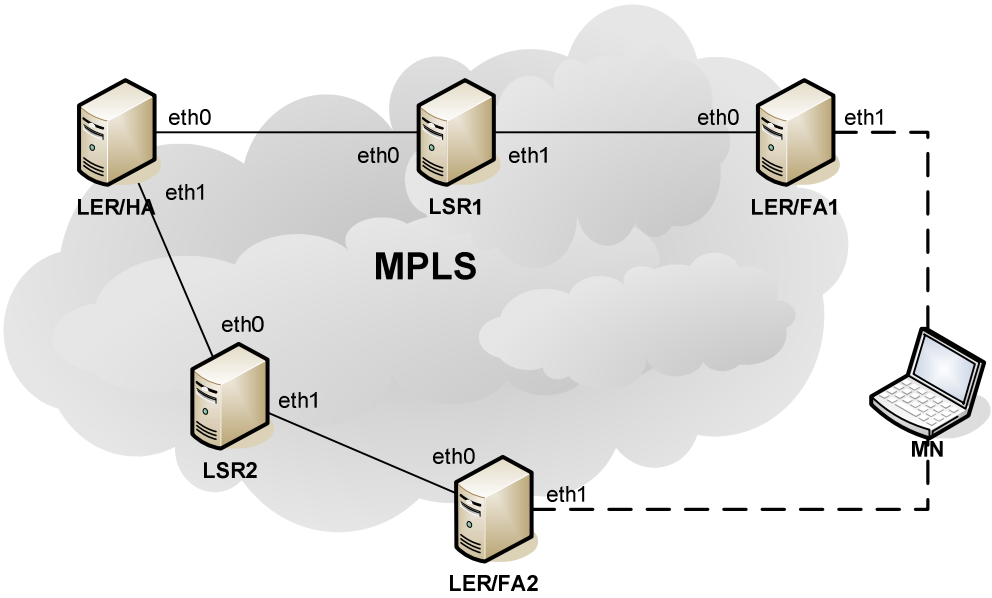


Figura 4.30 - Topologia utilizada no procedimento de avaliação da implementação.

Tabela 4.4 - Endereçamento utilizado no procedimento de avaliação da implementação.

equipamento	**endereço da interface eth0**	**endereço da interface eth1**
LER/HA	10.10.0.1	10.10.1.1
LSR1	10.10.0.2	10.10.2.1
LER/FA1	10.10.2.2	10.10.4.1
LSR2	10.10.1.2	10.10.3.1
LER/FA2	10.10.3.2	10.10.5.1
MN	10.10.0.3	-

Foi iniciado, em todas as máquinas que formam a nuvem MPLS, o serviço do RSVP através de linha de comando no console do linux. A partir do agente nativo foram criados os túneis com comandos no console do RSVP iniciado. Foram criados dois túneis: um com rótulo 12, que vai do HA ao FA1, e outro com rótulo 20, que vai do HA ao FA2. A fig. 4.31 faz uma representação de como foram distribuídos os rótulos. A partir de então, começou a haver o tráfego de pacotes de sinalização do RSVP, que são as mensagens Path e Resv. As mensagens Path são enviadas pelo nó onde foi definido o rótulo, isto é o agente nativo; e as mensagens Resv são as respostas enviadas pelo nó que recebe a requisição, isto é o agente estrangeiro. O tráfego das mensagens de Path e Resv pode ser visualizado na fig. 4.32. Então, foram iniciados os agentes do Mobile IP. Seguindo o seu funcionamento

normal, os agentes passaram a enviar pacotes de anúncio de agentes móveis, também visíveis na fig. 4.32.

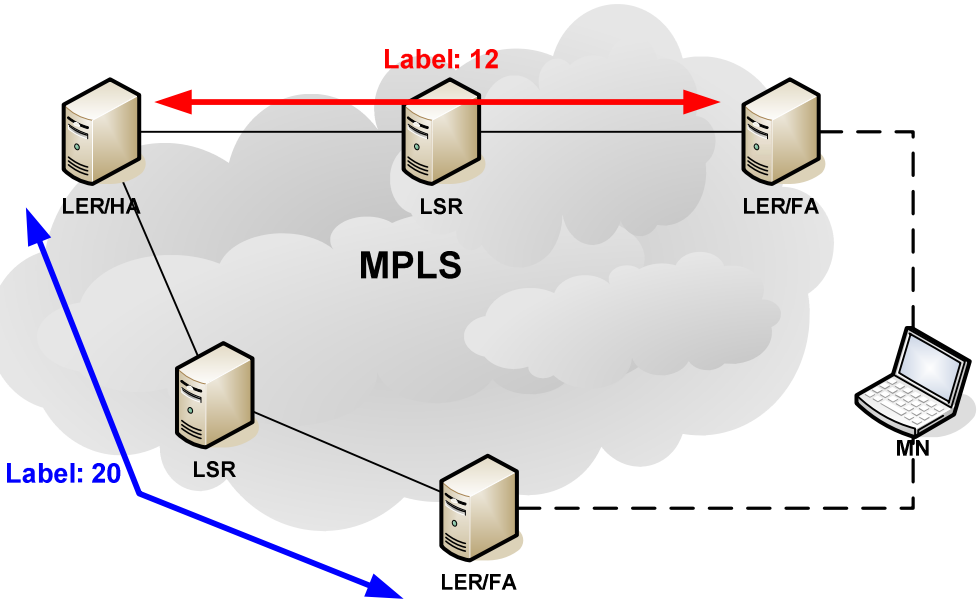
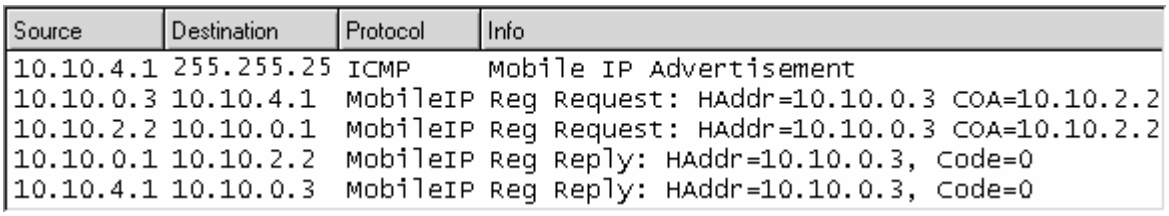


Figura 4.31 - Rótulos pré-definidos.

Source	Destination	Protocol	Info
10.10.2.2	255.255.25	ICMP	Mobile IP Advertisement
10.10.4.1	255.255.25	ICMP	Mobile IP Advertisement
10.10.0.1	10.10.2.2	RSVP	PATH Message. SESSION: IPv4-LSP, Tunnel ID 12
10.10.2.2	10.10.2.1	RSVP	RESV Message. SESSION: IPv4-LSP, Tunnel ID 12
10.10.4.1	255.255.25	ICMP	Mobile IP Advertisement

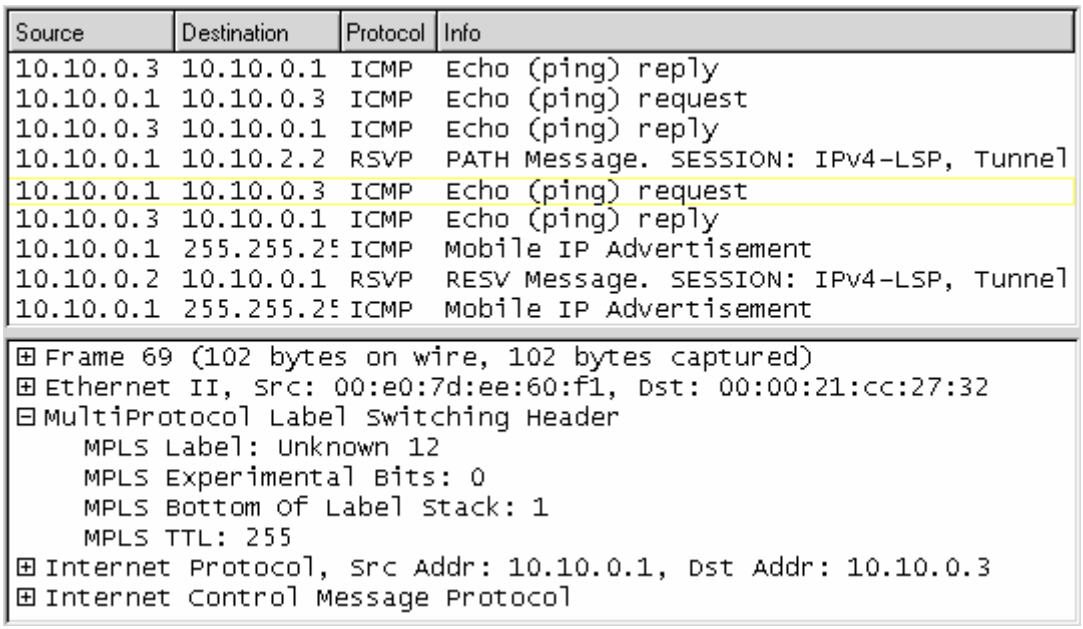
Figura 4.32 - Sinalização RSVP na implementação: Mensagens Path e Resv.

O registro do móvel, cujas mensagens não sofreram alteração, foi realizado com sucesso. A troca de mensagens do registro pode ser vista fig. 4.33. Em seguida foi feito um teste de *ping*, para confirmar se o nó móvel estava acessível mesmo em uma rede estrangeira. A fig. 4.34 apresenta o resultado do teste de *ping*. Através desta captura em *sniffer*, pode-se perceber que a mensagem ICMP de *ping* está encapsulada por um cabeçalho MPLS, isto é um rótulo do MPLS definido pelo RSVP. Isto demonstra que o túnel IP-em-IP foi substituído pelo túnel LSP com sucesso.



Source	Destination	Protocol	Info
10.10.4.1	255.255.25	ICMP	Mobile IP Advertisement
10.10.0.3	10.10.4.1	MobileIP	Reg Request: HAddr=10.10.0.3 COA=10.10.2.2
10.10.2.2	10.10.0.1	MobileIP	Reg Request: HAddr=10.10.0.3 COA=10.10.2.2
10.10.0.1	10.10.2.2	MobileIP	Reg Reply: HAddr=10.10.0.3, Code=0
10.10.4.1	10.10.0.3	MobileIP	Reg Reply: HAddr=10.10.0.3, Code=0

Figura 4.33 - Mensagens de registro do nó móvel no ambiente integrado.



Source	Destination	Protocol	Info
10.10.0.3	10.10.0.1	ICMP	Echo (ping) reply
10.10.0.1	10.10.0.3	ICMP	Echo (ping) request
10.10.0.3	10.10.0.1	ICMP	Echo (ping) reply
10.10.0.1	10.10.2.2	RSVP	PATH Message. SESSION: IPv4-LSP, Tunnel
10.10.0.1	10.10.0.3	ICMP	Echo (ping) request
10.10.0.3	10.10.0.1	ICMP	Echo (ping) reply
10.10.0.1	255.255.25	ICMP	Mobile IP Advertisement
10.10.0.2	10.10.0.1	RSVP	RESV Message. SESSION: IPv4-LSP, Tunnel
10.10.0.1	255.255.25	ICMP	Mobile IP Advertisement

```
⊞ Frame 69 (102 bytes on wire, 102 bytes captured)
⊞ Ethernet II, Src: 00:e0:7d:ee:60:f1, Dst: 00:00:21:cc:27:32
⊟ MultiProtocol Label Switching Header
    MPLS Label: Unknown 12
    MPLS Experimental Bits: 0
    MPLS Bottom Of Label Stack: 1
    MPLS TTL: 255
⊞ Internet Protocol, Src Addr: 10.10.0.1, Dst Addr: 10.10.0.3
⊞ Internet Control Message Protocol
```

Figura 4.34 - *Ping* na rede IP móvel integrado a MPLS.

Em seguida, o nó móvel foi transferido para o outro agente estrangeiro, novamente ele realizou o registro, e foi realizado o teste de conectividade através de mensagens de *ping*, e foi verificado que para este caso ele também obteve sucesso em substituir o túnel pelo MPLS. A fig. 4.35 apresenta a troca de mensagens capturadas com *sniffer*, referentes ao registro do nó móvel na segunda rede estrangeira em conjunto com as mensagens de *ping*.

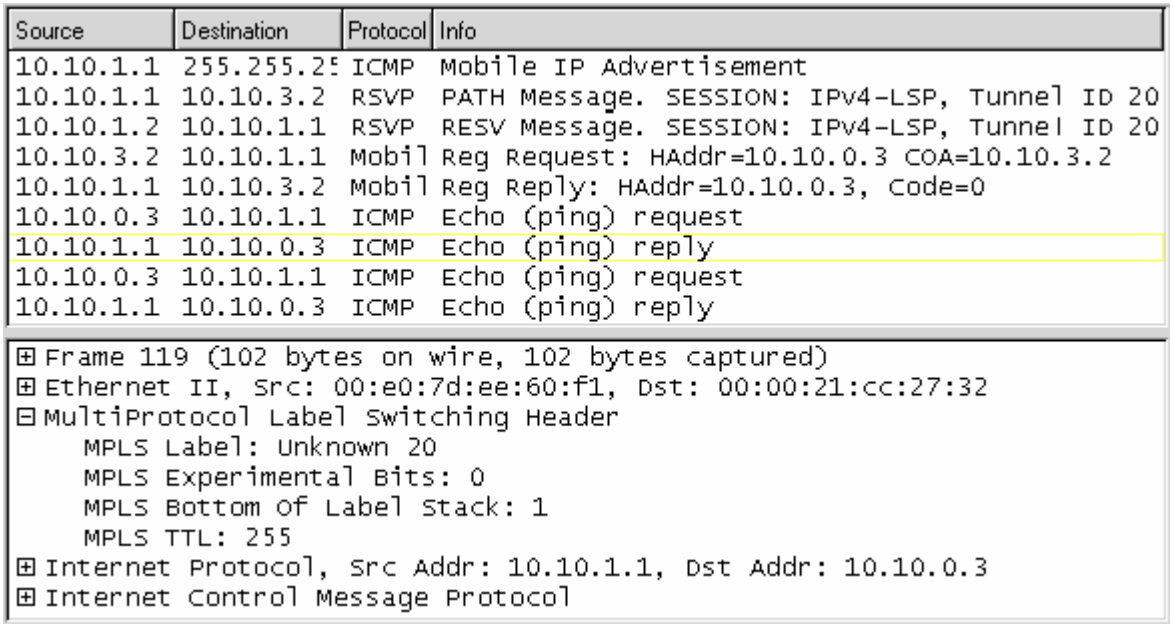


Figura 4.35 - Registro no segundo FA da implementação no laboratório.

Apesar da integração ter sido bem sucedida, foram enfrentadas algumas dificuldades, dentre as quais podemos citar a baixa quantidade de equipamentos e placas de rede disponíveis para a realização destes testes, e instabilidade no sistema operacional após a aplicação do *patch* do MPLS. A instabilidade se deu pelo fato de ter sido necessário trabalhar com um *kernel* anterior ao que estava instalado anteriormente no linux. Esta instabilidade fez com que algumas placas de rede que havia disponíveis no laboratório não funcionassem no sistema, reduzindo ao extremo a quantidade que foi utilizada.

Apesar de ter sido possível capturar mensagens com o *sniffer* demonstrando que a substituição dos túneis IP-em-IP por LSP no IP móvel, não foi possível realizar testes que demonstrassem algum ganho de desempenho. Durante alguns períodos que variavam entre alguns segundos e muitos minutos, as placas de rede paravam de responder, e posteriormente voltavam a responder, sem interferência externa. Além de alguns momentos sem responder, algumas vezes o sistema demorava alguns segundos para apresentar informações que haviam sido capturadas no *sniffer*, ou para apresentar as respostas das comunicações por *ping*.

5 - CONCLUSÃO

Este trabalho apresentou a tecnologia Mobile IP, que permite que um dispositivo móvel se mova entre diversas sub-redes sem a necessidade de reconfigurar o endereço IP da interface de rede do dispositivo, utilizando-se agentes para gerenciar a mobilidade dos nós móveis que fazem parte do sistema e permitir a conectividade destes dispositivos. Esta tecnologia torna a conectividade mais simples para os usuários finais e permite a utilização de recursos de rede quase da mesma forma que se o dispositivo móvel estivesse em sua rede nativa, mas traz perda de desempenho no envio de pacotes aos nós móveis quando o agente nativo encontra-se distante da rede estrangeira à qual o nó móvel esteja conectado.

Outro problema encontrado na utilização do Mobile IP diz respeito ao *handoff*, pois, para que o agente nativo possa enviar pacotes ao nó móvel na nova rede na qual ele se conectou, é necessário que o nó móvel faça o registro nesta nova rede à qual ele está conectado. Dependendo da distância entre o agente nativo e a rede estrangeira, o tempo gasto para realizar este registro pode ser demorado, deixando o nó móvel sem conexão durante um período de tempo.

Através deste estudo, foi comprovado, por testes de desempenho, que a utilização de um núcleo MPLS entre os dispositivos de um sistema Mobile IP traz ganho no desempenho do sistema, no que diz respeito ao encaminhamento de pacotes. Entretanto, este ganho pode ainda ser maior se for utilizada uma integração eficiente entre os dois sistemas. A integração por si só traz melhora de desempenho por não ser necessário o processamento de encapsulamento e desencapsulamento IP-em-IP, e reduz o tamanho dos pacotes que são transmitidos do agente nativo ao estrangeiro devido à não utilização de dois cabeçalhos IP.

Na proposta de protocolo desenvolvida neste trabalho, foram agregadas funcionalidades que se estima poderem trazer melhoria no desempenho tanto no que diz respeito à latência na transmissão das mensagens durante o envio de pacotes, quanto no que diz respeito ao atraso de *handoff*. Para o primeiro problema, foi proposta uma forma de otimização de roteamento, que faz com que pacotes a serem enviados ao nó móvel em uma rede estrangeira não precisem necessariamente passar inicialmente pela rede nativa. O problema

do *handoff* foi minimizado através do uso de um mecanismo de pré-registro aliado com um sistema de *multicast* montados sobre um ambiente que implementa IP móvel hierárquico.

A utilização do MIP hierárquico é muito importante para se definir a topologia sobre a qual é implementado o *multicast*, fazendo com que, a partir dessa hierarquia, se defina o caminho aos agentes estrangeiros das redes vizinhas da rede na qual o nó móvel encontra-se conectado para então poder iniciar o envio de mensagens para grupos *multicast*. Quando for iniciado o envio dos pacotes em *multicast*, deve-se também, enviar mensagens de pré-registro aos agentes estrangeiros das redes estrangeiras que fazem parte da vizinhança da localização do nó móvel. Espera-se que o pré-registro proposto neste trabalho reduza o tempo gasto pelo nó móvel no registro, permitindo assim um *handoff* quase instantâneo.

Ainda com relação ao *handoff*, foi proposto neste trabalho que, ao ocorrer um *handoff*, o agente estrangeiro da rede estrangeira da qual o nó móvel se desconectou deva utilizar os registros de túneis estabelecidos para o fluxo de tráfego direcionado ao nó móvel para encontrar os endereços dos dispositivos que estão em comunicação com o nó móvel enviar mensagens que informem a nova posição do nó móvel, evitando dessa forma, que estes dispositivos permaneçam com uma associação desatualizada sobre a localização do nó móvel.

Verificou-se que as funcionalidades de MIP hierárquico e de otimização de roteamento podem ser integradas simultaneamente ao sistema através da utilização de mensagens de controle que permitam a atualização dos dados sobre a localização do móvel tanto no agente nativo quanto dos dispositivos que estejam enviando informações ao nó móvel.

Para a comprovação de que a proposta de protocolo apresentada nesta dissertação alcança os objetivos propostos é necessário que sejam feitos alguns testes no desempenho da proposta, em especial verificando o desempenho da otimização de roteamento, e de comunicações durante o *handoff*, e então comparar os resultados deste teste com os encontrados em uma rede IP móvel simples para verificar se houve a melhora esperada na eficiência do sistema.

Para projetos futuros que possam vir a continuar este trabalho, pode ser feita uma análise dos aspectos de segurança sobre a proposta de integração, com determinação dos principais

pontos vulneráveis neste ambiente e quais os processos de criptografia e autenticação que poderiam ser utilizados para aumentar a segurança e proteger o ambiente. Outro estudo que pode ser aprofundado é a questão da qualidade de serviço, analisando o desempenho do sistema para tráfego de voz e videoconferência de alta qualidade sobre o ambiente proposto e verificação de sua garantia de qualidade.

Por fim, pode-se ainda fazer uma análise sobre como proceder para se transpor este ambiente para um sistema móvel celular tal como o UMTS, que deve utilizar voz sobre IP e um amplo ambiente IP com necessidade da aplicação de mobilidade. Um fator fundamental neste ambiente é garantir um *handoff* suave e transparente ao usuário final.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] "*IETF RFC Page*." Acessado em dezembro de 2005 no endereço http://www.ietf.org/rfc.html

[2] "*Mip4 Working Group Status Pages*." Acessado em dezembro de 2005 no endereço http://www.mip4.org/

[3] Abdalla, H.Jr., Soares, A.J.M., Carvalho, P.H.P., Barreto, P.S., Nzé, G.A. e Lambert, R. (2004). "*Implementação de um ambiente de teste e medição para redes convergentes*." Em: XXII Simpósio Brasileiro de Telecomunicações - SBrT'05, Campinas, Brasil.

[4] Abdalla, H.Jr., Soares, A.J.M., Carvalho, P.H.P., Barreto, P.S., Nzé, G.A., Macedo, V., e Amaral, I. (2004). "*An Experimental Environment for Evaluation of New Proposals for Next Generation Networks*." Em: LABCOM, Brasília, Brasil.

[5] Abdalla, H.Jr., Soares, A.J.M., Carvalho, P.H.P., Barreto, P.S., Nzé, G.A., Lambert, R., Macedo, V., Pastor, E., Tarchetti, P. e Amaral, I. (2004). "*Performance Evaluation of Shortest Path Computation for IP and MPLS Multi-Service Networks over Open Source Implementation*." Em: First International Workshop SAPIR 2004, Fortaleza, Brasil.

[6] Abdalla, H.Jr., Soares, A.J.M., Carvalho, P.H.P., Barreto, P.S., Nzé, G.A., Lambert, R., Pastor, E., Bravo, M. e Silva, L.M. (2004). "*Um ambiente SIP/MPLS/Diffserv para avaliação de seviço de VoIP*." Em: XXI Simpósio Brasileiro de Telecomunicações - SBT'04, Belém, Brasil.

[7] Abdalla, H.Jr., Soares, A.J.M., Carvalho, P.H.P., Barreto, P.S., Nzé, G.A., Macedo, V. e Tarchetti, P. (2004). "*Performance Analysis of a MPLS-Diffserv Platform for Net Generation Networks*." Em: LABCOM, Brasília, Brasil.

[8] Andersson, L., Doolan, P., Feldman, N., Fredette, A. e Thomas, B. (2001). "*LDP Specification*." RFC 3036, Nortel Networks, Ennovate Networks, IBM Corp. e Cisco Systems, 132p.

[9] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V. e Swallow, G. (2001). "*RSVP-TE: Extensions to RSVP for LSP tunnels*." RFC 3209, 61p.

[10] Björn, A., Forsberg, D., Hautio, J., Malinen, J.K., Mustonen, K., Weckström, T., Malinen, J. e Kari, H. "Dynamics Mobile IP." Acessado em dezembro de 2005 no endereço http://dynamics.sourceforge.net/

[11] Braden, R., Zhang, L., Berson, S., Herzog, S. e Jamin, S. (1997). "*Resource ReSerVation Protocol (RSVP).*" RFC 2205, ISI, UCLA, IBM Research e Universidade de Michigan, 76p.

[12] Calhoun, P.R. e Perkins, C.E. (2001). "*Diameter Mobile IP extensions.*" IETF-Draft, Sun Laboratories e Nokia Research Center, 32p.

[13] Carvalho, P.H.P., Soares, J.A.M., Abdalla, H.Jr., Barreto, P.S., Bizerra, R.S., Queiroz, B.G. e Carneiro, B.N. (2005). "*Uma Ferramenta em Código Aberto para Análise de Desempenho em Redes Convergentes*." Em: XXII Simpósio Brasileiro de Telecomunicações - SBrT'05, Campinas, Brasil

[14] Chao, H.C. e Chu, Y.M. (2003). "*An Architecture and Communication Protocol for IPv6 Pack-Based Picocellular Networks*." Em: *Mobile Networks and Applications*, 8, 663-674.

[15] Chaskar, H. e Koodli, R. (2001). "*A Framework for QoS Support in Mobile IPv6*." IETF-Draft, Nokia Research Center, 11p.

[16] Chen W.T. e Huang, L.C. (2000). "*RSVP Mobility Support: A Signaling Protocol for Integrated Services Internet with Mobile Hosts*." Em: *Proceedings IEEE INFOCOM 2000*, Tel Aviv, Israel, 1283-1292.

[17] Chen, Y.W. e Yan Z.J. (2003). "*Effect of the label management in mobile IP over MPLS networks*." Em: *IEEE International Conference on Advanced Information Networking and Applications* (AINA 2003), Xi'an, China,379-384.

[18] Choi, J.K. (2003). "*Draft new Recommendation Y.MIPoMPLS (Mobile IP Services over MPLS).*" *International Telecommunication Union ITU, Telecommunication Standardization Sector*, 38p.

[19] Choi, J.K., Kim, M.H. e Lee, Y.J. (2001). "*Mobile IPv6 support in MPLS Network.*" IETF-Draft, ICU e ETRI, 12p.

[20] Choi, J.K., Um, T.W., Lee, Y.K. e Yang, S.H. (2001). "*Extension of LDP for Mobile IP Service through the MPS Network.*" IETF-Draft, ICU e ETRI, 28p.

[21] Das, S.K., Jayaram, R., Kakani, N.K. e Sen, S.K. (1999). "*A resource reservation mechanism for mobile nodes in the Internet*." Em: *IEEE 49th Vehicular Technology Conference*, 1940-1944.

[22] Deering, E. (1991). "*ICMP Router Discovery Messages*." RFC 1256, Xerox PARC, 19p.

[23] Diab A., Mitschele-Thiel, A. e Xu, J. (2004). "*Performance analysis of the mobile IP fast authentication protocol*." Em: *Proceedings of the 7th ACM international*

symposium on Modeling, analysis and simulation of wireless and mobile systems, Veneza, Italia, 287-300.

[24] Fernandes, N.L.L. (1999). "*Voz sobre IP: uma visão geral.*" Em: Coppe, Universidade Federal do Rio de Janeiro

[25] Foo, C.C. e Chua, K.C. (2000). "*Implementing Resource Reservations for Mobile Hosts in the Internet using RSVP and Mobile IP*." Em: *Vehicular Technology Conference Proceedings* (VTC2000), Tóquio, Japão, 1323-1327.

[26] Garrison, J. (2002). "*Voice over IP design guide.*" Em: Alcatel, E.U.A.

[27] Greco, L.G. (2005). "*Estudo comparativo de mecanismos de tolerância a falhas para redes MPLS.*" Dissertação de mestrado, Universidade de Brasília, Brasil, 94p.

[28] Grimminger, J. e Huth, H.P. (2001). "*Mobile MPLS - a MPLS based micro mobility concept.*" Em: *Wireless World Research Forum*, Stockholm, Suécia.

[29] Gustafsson, E., Jonsson, A. e Perkins, C. (2004). "*Mobile IPv4 Regional Registration*." IETF-Draft, Ericsson e Nokia Research Center, 40p.

[30] Hanks, S., Li, T., Farinacci, D. e Traina, P. (1994). "*Generic Routing Encapsulation (GRE).*" RFC 1701, NetSmiths e Cisco Systems, 8p.

[31] Heuven, P.V. (2002). "*RSVP-TE daemon for DiffServ over MPLS under Linux*." Em: *9th International Linux System Technology Conference*, Cologne, Alemanha.

[32] Heuven, P.V., Berghe, S.V.D. e Coppens, J. "*IBCN's RSVP-TE for DiffServ over MPLS.*" Acessado em fevereiro de 2006 no endereço http://dsmpls.atlantis.ugent.be/.

[33] Jain, R., Raleigh, T., Graff, C. e Bereschinsky, M. (1998). "*Mobile Internet Access and QoS Guarantees using Mobile IP and RSVP with Location Registers*." Em: *Proceedings of the IEEE International Conference on Communications (ICC'98)*, Atlanta,E.U.A., 1690-1695.

[34] Jamoussi, B., Andersson, L., Callon, R., Dantu, R., Wu, L., Doolan, P., Worster, T., Feldman, N., Fredette, A., Girish, M., Gray, E., Heinanen, J., Kilty, T. e Malis, A. (2002). "*Constraint-based LSP setup using LDP*." RFC 3212, 42p.

[35] Kim, H., Wong, K.S.D., Chen, W. e Lau, C.L. (2001). "*Mobility-aware MPLS in IP-based wireless access networks*." Em: *Proceedings of the IEEE Globecom'01*, San Antonio, Texas, E.U.A., 3444–3448.

[36] Leopoldino, G.M. e Medeiros, R.C.M. (2001). "*H.323: Um padrão para sistemas de comunicação multimídia baseado em pacotes.*" Em: NewsGeneration – RNP, 5, 6.

[37] Leu, J.R. "*SourceForge.net: MPLS for Linux.*" Acessado em fevereiro de 2006 no endereço http://sourceforge.net/projects/mpls-linux/.

[38] Leu, S.J. e Chang, R.S. (2003). "*Integrated service mobile internet: RSVP over mobile IPv4&6*." Em: *Mobile Networks and Applications*, 8, 6, 635-642.

[39] Malki, K.E. (2005). "*Low latency handoffs in Mobile IPv4*." IETF-Draft, Athonet, 56p

[40] Moy, J. (1991). "*OSPF version 2*." RFC 1247, Proteon Inc., 189p.

[41] Palmieri, F. (2005). "*An MPLS-based architecture for scalable QoS and traffic engineering in converged multiservice mobile IP networks*." Em: *Computer Networks*, 47, 257-269.

[42] Perkins, C. (1996). "*IP Encapsulation within IP*." RFC 2003, IBM, 14p.

[43] Perkins, C. (2002). "*IP Mobility Support for IPv4*." RFC 3344, Nokia Research Center, 99p.

[44] Perkins, C. e Calhoun, P. (2005). "*Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4*." RFC 3957, Nokia Research Center e Airespace, 27p.

[45] Perkins, C. e Johnson, D.B. (2001). "*Route Optimization in Mobile IP*." IETF-Draft, Nokia Research Center e Carnegie Mellon University, 25p.

[46] Perkins, C.E. (1999). "*Mobile IP at IETF*." Em: *ACM Sigmobile Mobile Computing and Communications Review*, 3, 3, 28-31.

[47] Perkins, C.E. (2003). "*Mobile IP at IETF*." Em: *ACM Sigmobile Mobile Computing and Communications Review*, 7, 4, 1-4.

[48] Perkins, C.E. e Calhoun, P.R. (2001). "*Generalized Key Distribution Extensions for Mobile IP*." IETF-Draft, Nokia Research Center e Sun Microsystems Laboratories, 8p.

[49] Perkins, C.E., Johnson, D.B. e Asokan, N. (2000). "*Registration Keys for Route Optimization.*" IETF-Draft, Nokia Research Center e Carnegie Mellon University, 29p.

[50] Pinheiro, A.J.F., Cardoso, C.G.S., Figueiredo, G.B. e Figueiredo, M.E.B. (2000). "*Um Estudo do MPLS e sua Importância para o REMA.*" Em: Projeto REMAv, Salvador, Brasil, 14p.

[51] Postel, J. (1981). "*Internet Protocol*." RFC 0791, University of Southern California, 45p.

[52] Rekhter, Y. e Li, T. (1995). "*BGP-4*." RFC 1771, IBM Corp. e Cisco Systems, 57p.

[53] Rekhter, Y. e Rosen, E. (2001). "*Carrying label information in BGP-4*." RFC 3107, 8p.

[54] Ren, Z. e Tham, C. (2001). "*Integration of Mobile IP and Multi-Protocol Label Switching*". Em: *IEEE ICC 2001*, 2123–2127.

[55] Rosen, E., Viswanathan, A. e Callon, R. (2001). "*Multiprotocol label switching architecture.*" RFC 3031, Cisco Systems, Force10 Networks e Juniper Networks, 61p.

[56] Sethom, K., Afifi, H. e Pujolle, G. (2004). "*Wireless MPLS: a new layer 2.5 micro-mobility scheme.*" Em: *Proceedings of the second international workshop on Mobility management & wireless access protocols*, Philadelphia, E.U.A., 64-71.

[57] Talukdar, A.K., Badrinath, B.R. e Acharya, A. (1997). "*On Accommodating Mobile Hosts in an Integrated Services Packet Network.*" Em: *Proceedings of INFOCOM'97*, Kobe, Japão.

[58] Talukdar, A.K., Badrinath, B.R. e Acharya, A. (1998). "*Integrated Services Packet Networks with Mobile Hosts: Architecture and Performance.*" Em: *ACM/Baltzer Journal of Wireless Network*s, 5, 2, 1-16.

[59] Talukdar, A.K., Badrinath, B.R. e Acharya, A. (2001). "*MRSVP: a resource reservation protocol for an integrated services network with mobile hosts.*" Em: *Wireless Networks*, 7, 1, 5-19.

[60] Terzis, A., Srivastava, M. e Zhang, L. (1999). "*A Simple QoS Signaling Protocol for Mobile Hosts in the Integrated Services Internet.*" Em: *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, New York, E.U.A., 1011-1018.

[61] The International Engineering Consortium. "*Multiprotocol Label Switching (MPLS).*" Em: *Web ProForum Tutorials*. Acessado em fevereiro de 2006 no endereço http://www.iec.org/online/tutorials/mpls/.

[62] Tseng, C.C., Lee, G.C. e Liu, R.S. (2001). "*HMRSVP: A Hierarchical Mobile RSVP Protocol.*" Em: *Proceedings of the 21st International Conference on Distributed Computing Systems* (ICDCSW), Washington, DC, E.U.A., 467-472.

[63] Um, T.W. e Choi, J.K. (2001). "*Path Re-routing Algorithm for Mobile IP Service at the ATM-based MPLS Network.*" Em: ICATM'2001, Seoul, Korea.

[64] Xie, K., Wong, V.W.S. e Leung, V.C.M. (2003). "*Support of micro-mobility in MPLS-based wireless access networks.*" Em: *WCNC 2003 - IEEE Wireless Communications and Networking Conference*, New Orleans, E.U.A., 4, 1, 1242-1247.