INSTITUTO DE PESQUISAS TECNOLÓGICAS DO ESTADO DE SÃO PAULO

FÁBIO XAVIER ALBERTONI

Laboratório Didático para o ensino de mobilidade IPv6

São Paulo
2005

FÁBIO XAVIER ALBERTONI

Laboratório Didático para o ensino de mobilidade IPv6

Dissertação apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, para obtenção do título de Mestre em Engenharia de Computação.

Área de concentração: Redes de Computadores

Orientador: Prof. Dr. Antonio Luiz Rigo

São Paulo
2005

Ficha Catalográfica
Elaborada pelo Centro de Informação Tecnológica do IPT

A329l Albertoni, Fábio Xavier
Laboratório didático para o ensino de mobilidade Ipv6. / Fábio Xavier Albertoni. São Paulo, 2005.
79p.

Dissertação (Mestrado em Engenharia de Computação) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Área de concentração: Redes de Computadores.

Orientador: Prof. Dr. Luiz Antonio Rigo

1. Mobilidade Ipv6 2. Laboratório 3. Redes wireless móveis 4. Customização Knoppix 5. Tese I. Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Centro de Aperfeiçoamento Tecnológico II. Título

05-12 CDU 654.9:004.7(043)

Resumo

A disseminação provocada pelo barateamento dos equipamentos de redes sem fio criou a demanda por mobilidade entre diferentes sub-redes. Para suprir esta necessidade foi criado o IPv4 Móvel, primeira versão da mobilidade no IP, que permite o deslocamento do usuário de uma célula à outra, sem perder a conexão. O seu sucessor, abordado neste trabalho, surgiu para resolver deficiências existentes na primeira versão e, por nascer integrado ao protocolo, aproveita-se de todos os mecanismos inerentes ao IPv6, trazendo melhorias de funcionalidade e desempenho.

Atualmente o material de aprendizado da mobilidade IPv6 restringe-se a apostilas e tutoriais sobre o assunto. Para suprir a necessidade de ferramenta de ensino, implementou-se o IPv6 móvel no Knoppix, umas das mais importantes e bem sucedidas distribuições do tipo live CD do Linux, o único sistema operacional que está de acordo com a última especificação do padrão de mobilidade. A utilização do CD agiliza a entrada em operação da atividade experimental, admite mobilidade, é compatível com os laboratórios existentes nas instituições acadêmicas e permite que um novo tema seja desenvolvido sem interferir na configuração dos equipamentos existentes.

Através dos exercícios didáticos que exploram a conexão FTP e roteamento, os alunos poderão fixar o conhecimento adquirido na sessão de aprendizagem teórica. Os estudantes poderão implementar experimentos que concretizam os conceitos aprendidos, fazendo com que seu rendimento aumente, duvidas sejam esclarecidas, melhorando o entendimento global do assunto e o interesse pelo tema abordado. O professor pode tirar proveito da ferramenta, aplicando exercícios práticos de IPv6 móvel para avaliar o nível de conhecimento do aluno.

Palavras Chave: IPv6 móvel; IPv4 móvel, configuração do Knoppix; MIPv6 Knoppix; roteamento IPv6 móvel; laboratório didático.

Abstract

The dissemination allowed by price reduction in wireless equipments created the demand for mobility between different sub-nets. The Mobile IPv4, the first version of IP mobile, was created to reach this target to allow user displace from cell to cell, without losing the connection. Its successor, boarded in this work, appeared to overcome existing deficiencies in the first version and, because it had born integrated to the protocol, it takes advantage of all the inherent IPv6 mechanisms, bringing improvements on functionality and performance.

Currently the existing material to learn IPv6 mobility is restricted to literacy and tutorials about the subject. To supply education tool, the mobile IPv6 was implemented in the Knoppix, one of the most important and successful distribution of Linux type named LIVE COMPACT DISC, the only operational system in accordance with the last mobility specification standard. The use of COMPACT DISC speeds the start up of experimental activities, admits mobility, is compatible with the existing laboratories in academic institutions and allows a new subject to be developed without interfering with the existing equipment configuration.

Through didactic exercises that explore FTP Connection and routes, students will be able to memorize the acquired knowledge in the learning theoretical session. The students will be able to implement experiments that materialize the learned concepts, doubt are clarified, increasing its income, improving the global agreement of the subject and the interest for the boarded subject. The professor can take advantage of the tool, applying practical exercises of mobile IPv6 to evaluate the knowledge level of pupil.

Keywords: IPv6 mobile; IPv4 mobile, Knoppix configuration; MIPv6 Knoppix; IPv6 mobile routing; didactic laboratory.

Lista de Figuras

Lista de Tabelas

Sumário

1 Introdução

O domínio da tecnologia e o crescimento da oferta de soluções para redes sem fio estão habilitando muitas estações de trabalho a tornarem-se móveis. Estudantes podem conectar-se à rede de qualquer lugar do campus, membros das famílias podem checar e-mails de qualquer local da residência e vizinhos podem compartilhar o acesso à Internet de alta velocidade. As redes sem fio mudam substancialmente o modo das pessoas trabalharem e se divertirem. O modo de utilizar as redes no futuro próximo não terá precedente. Testemunha-se mais uma quebra de paradigma no revolucionário mundo WEB.

Com a evolução da tecnologia surgiu a necessidade das pessoas adquirirem mobilidade no acesso às redes de computadores, em qualquer lugar que elas estejam, sem perder a conexão com a sua rede de origem. O usuário percorre várias redes e não perde sua conexão durante a transição de uma rede para outra, de forma análoga aos telefones fixos e móveis. Quando há troca de uma antena de transmissão para outra a ligação do telefone celular não é interrompida.

Rede baseada em IP fixo não oferece mobilidade nativa, ou seja, se um indivíduo sair de uma sub-rede para uma sub-rede diferente, a conexão com a primeira é perdida. Para solucionar este problema o IETF (*Internet Engineering Task Force*) criou o suporte de mobilidade para o IP, para as versões 4 e 6 (MIPV4 – IP móvel versão 4 e MIPV6 – IP móvel versão 6), a solução para IPV4 já não está mais sendo desenvolvida e todos os esforços estão concentrados na nova versão do protocolo IPv6 móvel.

A figura 1 mostra o campus de uma universidade com diferentes redes wireless. Usando IP móvel o estudante pode andar livremente pelo campus sem se preocupar com a perda da conexão e sua pasta de arquivos compartilhados estará disponível para qualquer usuário autorizado de outra

sub-rede, ou seja, a mobilidade é transparente para o usuário: em qualquer lugar que esteja, ele pode ser contatado e contatar outros usuários abrigados em outras sub-redes.

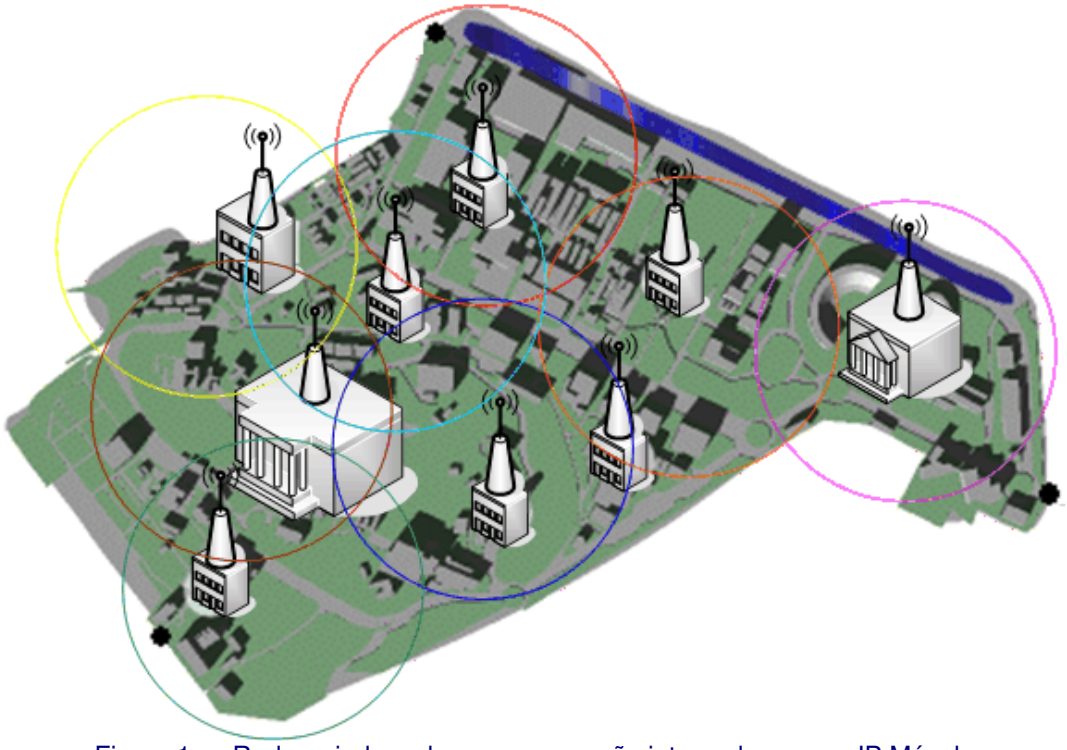

Figura 1 Redes wireless de um campus são integradas com o IP Móvel.

1.1 Objetivo

O objetivo deste trabalho é montar um laboratório didático de IPv6 móvel utilizando o Knoppix, uma distribuição de Linux executada diretamente do CD [3]. O Knoppix é um pacote pertencente à categoria LIVE e possui todos os recursos disponíveis do Debian. A mobilidade poderá ser obtida incorporando-se no Knoppix o suporte à IPv6 móvel, ajustando-se parâmetros do *kernel* (núcleo do sistema operacional) e procedendo-se à montagem do CD.

1.2 Motivação

O material de ensino da tecnologia IPv6 móvel, atualmente, restringe-se a apostilas e apresentações escritas sobre o assunto, não existindo qualquer material prático de apoio ao aprendizado do IPv6 móvel. O Linux apresenta-se como o sistema operacional mais apropriado para o estudo das novas tecnologias de rede, sendo a única implementação que oferece suporte para a tecnologia de mobilidade.

Os laboratórios de informática das instituições de ensino, geralmente, são compartilhados por diversas disciplinas e utilizam as mais diversas combinações de redes e sistemas operacionais (Linux, Windows, Macintosh, Novell e outros). A preparação do ambiente para o ensino de mobilidade IP pode interferir na instalação pré-existente.

O Knoppix foi adotado por não ser invasivo e não introduzir qualquer item adicional na instalação presente no disco rígido da estação de trabalho, por facilitar e agilizar o aprendizado através da exposição dos alunos à tecnologia do IPv6 móvel, na prática. A rede formada explora o assunto com profundidade, melhorando o entendimento teórico e prático através da observação de mobilidade IP contida no experimento implementado.

A característica principal desse tipo de ferramenta é que o software contido no CD não precisa ser instalado no disco rígido. O material assim estruturado dispensará a preparação do ambiente computacional no laboratório didático e, em poucos minutos, todo o cenário estará disponível para a demonstração e experimentação dos mecanismos de operação de uma rede sem fio com mobilidade IP.

1.3 Justificativa

Os avanços tecnológicos no mundo das redes sem fio em conjunto com a versão do protocolo IP de nova geração (IPv6), elaborada com suporte nativo à mobilidade, admitem o trânsito de estações móveis entre

diferentes redes de maneira transparente ao usuário. Como a versão quatro do protocolo IP não possui suporte a mobilidade, a peregrinação (*roamming*) sem perda de conexão, fica restrita ao segmento de redes sem fio no qual o usuário foi autenticado.

Além de um grande suporte a mobilidade, o IPv6 possui segurança reforçada e, certamente, estes benefícios vão impulsionar a disseminação de redes sem fio utilizando o IPv6 móvel não somente a computadores e equipamentos portáteis, mas para eletrodomésticos, carros e outros dispositivos de uso corrente no nosso dia-a-dia.

A implementação atual do IPv6 móvel está disponível publicamente para Linux. Os sistemas operacionais Windows XP (atualizado com service packs 1 ou 2) e Windows Server 2003 implementam apenas suporte à estação, móvel ou fixa (*correspondent node*), que inicia uma conexão com a estação móvel baseado na versão 13 do draft "*Mobile IPv6 Internet*", já obsoleto. Através de documento publicado em setembro de 2004, a Microsoft Research oferece, restrito a participantes e sob pedido, "*The Mobile Technology Preview*" suporte total a funcionalidades "*correspondent node*", "*mobile node*" e "*home agent*" descritas nas RFCs 3775 [5] e 3776 [14].

O processo de instalação do IPv6 móvel requer uma modificação na estrutura do *kernel* e após esta adequação da configuração é necessário que o *kernel* seja compilado. O processo é complexo e requer conhecimento avançado de Linux. A partir da elaboração do CD, o laboratório pode ser montado em poucos minutos e do aluno não é exigido um conhecimento profundo sobre Linux. Utilizando o CD e um disquete podem-se criar redes móveis sem danificar os sistemas operacionais existentes nos laboratórios, pois a instalação não faz uso de disco rígido.

Por todos os motivos apresentados, acredita-se que o tema dessa dissertação seja bastante atual e deve contribuir com os estudantes no aprendizado do mundo da mobilidade de redes sem fio.

1.4 Metodologia

A metodologia utilizada neste trabalho foi indutivo-experimental. O desenvolvimento apoiou-se nas facilidades oferecidas por uma distribuição LiveCD Linux, que foi adaptada para o ensino da mobilidade IPv6. O CD produzido permite criar um ambiente que implementa todas as entidades da especificação IPv6 móvel, sobre as quais são elaborados os experimentos didáticos. Como exemplo de utilização, foi preparado um roteiro de laboratório (laboratório didático) para o ensino de tópicos de roteamento IP para ambientes sem infra-estrutura pré-existente visando demonstrar a persistência de conexão durante a transição do dispositivo móvel entre os segmentos de rede. O ambiente dispõe de três máquinas, duas delas são configuradas pela ferramenta com suporte a IPv6 móvel e a terceira sem suporte a IPv6.

1.5 Estrutura da dissertação

Capítulo 1 – Introdução: Nela está o objetivo, a motivação e justificativa da dissertação.

Capítulo 2 – Conceitos Básicos: Constam os conceitos básicos de funcionamento das redes sem fio, o padrão 802.11 com a sua história, o WEP que é o suporte padrão de criptografia deste padrão.

Capítulo 3 – Outros métodos de mobilidade de Host: Este capítulo mostra alternativas de mobilidade do host que existiam na época da definição de um padrão para a mobilidade e a justificativa do uso do IP móvel.

Capítulo 4 - IPv4 móvel ou IP móvel versão 4, a primeira versão da mobilidade IP.

Capítulo 5 – IPv6 Móvel: Apresenta todas as características e justificativas da utilização deste novo padrão de mobilidade wireless.

Capítulo 6 – Roteamento: Mostra como o roteamento é realizado no IPv4 móvel e no IPv6 móvel, suas diferenças e as principais vantagens.

Capítulo 7 – Knoppix em ação: Descreve como foi feita a implementação do suporte ao IP móvel versão 6.

Capítulo 8 – Laboratório Didático: Mostra como utilizar a ferramenta, a principal contribuição desse trabalho, exemplificada através de um roteiro de aula.

Capítulo 9 – Conclusão: Descreve os resultados obtidos no desenvolvimento do trabalho e finaliza com sugestões de trabalhos futuros.

Referências – Lista dos documentos de apoio utilizados neste trabalho.

Glossário – Descrição de termos encontrados nesta dissertação.

Anexos – Materiais de consulta: conceitos de IPv4 e IPv6.

2 Conceitos básicos

2.1 802.11

A família de protocolos 802.11 provê a interoperabilidade básica entre equipamentos wireless de diferentes fabricantes. Um computador que utiliza produto de um fabricante, aderente à especificação 802.11b pode perfeitamente se comunicar com o produto de outro fabricante que siga a mesma especificação. Afirmação análoga pode ser feita para os protocolos 802.11a e 802.11g.

2.1.1 A história do padrão 802.11

O Instituto de Engenheiros Elétricos e Eletrônicos é reconhecido internacionalmente como criador e regulamentador de padrões. Os padrões são elaborados por vários comitês. O comitê IEEE 802 trabalha com redes locais e metropolitanas, a tabela 1 relaciona alguns temas associados com a série de padrões 802.x.

802.1	Ligações e gerenciamento
802.2	Camada física
802.3	Método de acesso CSMA/CD
802.4	Método de acesso *Token-Passing Bus*
802.7	Redes LAN com Banda larga (tv a cabo)
802.11	Wireless

Tabela 1 Alguns dos grupos de trabalho da série 802.

O grupo de trabalho 802.11 foi formado em setembro de 1990. O seu principal objetivo foi criar redes locais sem fio que operem no espectro ISM (*Industrial, Scientific, and Medical* - Industriais, Científicas e Médicas). O primeiro padrão foi lançado em 1997.

O comitê indicado construiu o conjunto de especificações 802.11 de modo a compatibilizar o meio físico, substituindo apenas as camadas mais baixas do modelo OSI. A série 802.11 redefine a camada física (PHY) e uma parte da camada de enlace (DLL). No modelo OSI, a camada de enlace pode ser subdividida em duas partes: a subcamada Controle de Enlace Lógico, independente do meio - *Logical Link Control* (LLC) - e a subcamada de Controle de Acesso ao Meio, dependente do meio físico – Media Access Control (MAC). A série 802.11 redefine a subcamada MAC e incorpora a subcamada LLC utilizada por outros padrões 802, sem qualquer modificação. Esse artifício é responsável pela transparência dos dispositivos wireless, que convivem em completa harmonia com os demais nós da rede cabeada.

A figura 2 mostra um desenho comparativo das camadas de nível mais baixo do modelo OSI com a correspondente estrutura da série dos protocolos 802.

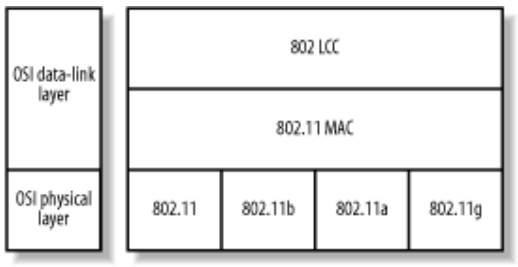

Figura 2 As camadas do modelo OSI e a correspondente na estrutura 802.

Fonte: Gast, M. S. “802.11b Wireless Networks - The definitive guide”, Abril de 2002.

Há diferentes padrões de camada física utilizados hoje. A especificação original 802.11 documenta alguns mecanismos: o primeiro utiliza Infravermelho (IR), pouco difundido, e os demais usam portadoras de RF em 2.4 ou 5.8 GHz com modulação baseada em espalhamento de espectro por salto de freqüência (*Frequency Hopping Spread Spectrum* - FHSS), espalhamento de espectro por seqüência direta (*Direct Sequence Spread Spectrum* - DSSS) [1] ou multiplexação por divisão de freqüências ortogonais (*Orthogonal Frequency Division Multiplexing* – OFDM). A

especificação original 802.11 oferecia baixa taxa de transferência (de 1 a 2 Mb/s), dependendo da qualidade do sinal e apresentava problemas de interoperabilidade: dispositivos com o mecanismo DSSS não podiam comunicar-se com dispositivos que utilizavam FHSS.

A tecnologia 802.11b, implementada em 1999, além de manter compatibilidade com a versão anterior, especificou uma nova PHY que aumentou para 11Mb/s a taxa de transferência de bits usando DSSS em 2.4 GHz. Devido à alta taxa de transferência e o aumento da interoperabilidade, os produtos 802.11b ganharam uma rápida aceitação no mercado.

A especificação 802.11a foi lançada em 2001, opera em 5 GHz, provê a transferência de dados com taxas de até 54 Mb/s e usa um novo método de modulação denominado OFDM, uma técnica de multiplexação por divisão de freqüências ortogonais. Alguns fabricantes possuem implementações proprietárias que dobram a taxa de transferência para até 108 Mb/s.

O padrão 802.11g é a quarta especificação do grupo IEEE 802.11. Opera na freqüência de 2.4 GHz como o modelo 802.11b, mas usa o OFDM como na 802.11a. A tabela abaixo mostra algumas especificações da camada física da série 802.11.

802.11 PHY	Máxima taxa de transferência	Freqüência	Modulação
802.11	2Mb/s	2.4GHz e IR	FHSS e DSSS
802.11b	11Mb/s	2.4GHz	HR-DSSS
802.11g	54Mb/s	2.4GHz	OFDM
802.11ª	54Mb/s	5 GHz	OFDM

Tabela 2Especificações PHY.

Fonte: Gast, M. S. “802.11b Wireless Networks - The definitive guide”, Abril de 2002.

O padrão mais utilizado atualmente nas redes sem fio é o 802.11b. Onze canais, no Brasil, ocupam o intervalo de 2.4 GHz. Estes canais têm bandas de freqüências, como ilustrado na figura 3. Utilizando-se canais superpostos em redes próximas pode haver interferência. Os canais 1, 6 e 11 são os mais indicados para a composição de células quando se deseja estender a área de cobertura e oferecer mobilidade ao usuário de redes sem fio.

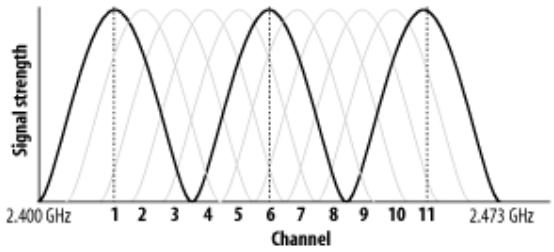

Figura 3 Os canais da 802.11b para o Brasil.

Fonte: Gast, M. S. “802.11b Wireless Networks - The definitive guide”, Abril de 2002.

2.2 Privacidade equivalente à rede cabeada

A tentativa do IEEE em dirigir-se aos conceitos de transgressões de endereços culminou no padrão opcional de privacidade equivalente à rede de fios (WEP - *Wired Equivalent Privacy*), que é encontrado na cláusula 8.2 da 802.11. O WEP é usado por estações para proteção dos dados que atravessam o meio sem fio [4]. Após cruzarem o ponto de acesso, entrega-os desprotegidos à rede cabeada.

As redes tornaram-se importantes para fazer o negócio. A segurança transformou-se em uma preocupação cada vez mais necessária. O WEP foi introduzido inicialmente no mercado como a solução de segurança para LANs wireless, entretanto seu projeto possui muitas falhas. O WEP é tão vulnerável que sua aplicação não é recomendada em muitos casos.

Algumas falhas severas de projeto foram identificadas e sua segurança foi quebrada em 2001. Há um problema latente com a cifragem criptográfica usada pelo WEP com implicações para a segurança da rede, abordadas neste capítulo. Nele são apresentadas algumas heranças da criptografia WEP e listas das falhas do projeto e, ao final, sugere-se recomendações no uso do WEP. A recomendação básica é não confiar no WEP como recurso de proteção único.

2.2.1 Background Criptográfico do WEP

Antes de apresentar o projeto WEP, é necessário expor alguns conceitos básicos de criptografia. O WEP utiliza a cifragem RC4 para proteger dados, usando uma cifra simétrica (chave-secreta) para tornar o fluxo de dados incompreensível. O RC4 aplica um conjunto de transformações a uma cadeia de caracteres gerando uma seqüência de caracteres denominada *keystream*. O *keystream* é combinado com a mensagem original, descaracterizado-a totalmente, produzindo a mensagem cifrada (ciphertext). A mensagem cifrada preserva as propriedades do fluxo original e, portanto, admite a reversibilidade. A mensagem original é recuperada processando-se a mensagem cifrada com o mesmo *keystream* no receptor. O RC4 usa a operação OU exclusivo (XOR) para combinar o *keystream* com a mensagem cifrada. A figura 4 ilustra o processo.

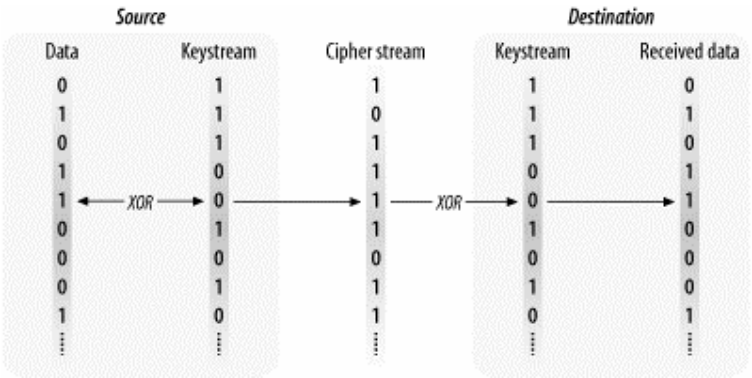

Figura 4 Operação genérica da cifra do fluxo.

Fonte: Gast, M. S. “802.11b Wireless Networks - The definitive guide”, Abril de 2002.

A maioria dos processos de cifragem de fluxo inicia com uma chave secreta relativamente curta, expandindo-a posteriormente com a agregação de um *keystream* pseudo-randômica. Este processo é ilustrado na figura 5. O gerador do número pseudo-randômico (*Pseudo Random Number Generator* - PRNG) segue um conjunto de regras para expandir a chave. Para recuperar os dados, ambos os lados devem compartilhar a mesma chave secreta e, portanto, devem usar o mesmo algoritmo para expandir a chave.

A segurança de uma cifra de fluxo é inteiramente dependente do *keystream* randômico, o algoritmo de expansão da chave muito importante. Quando o RC4 foi selecionado pelos grupos de trabalho 802.11 acreditava-se que ele era seguro. As falhas só foram identificadas após a adoção.

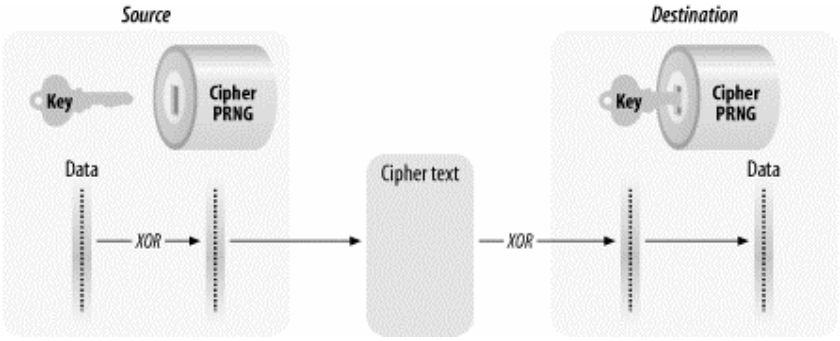

Figura 5 Operação fechada da chave da cifra do fluxo.

Fonte: Gast, M. S. “802.11b Wireless Networks - The definitive guide”, Abril de 2002.

2.2.2 Processamento de dados do WEP

A confiabilidade e a integridade são garantidas simultaneamente, como ilustrado na figura 6. Antes da encriptação, o frame é submetido a um algoritmo de verificação da integridade, gerando uma seqüência de 32-bit denominada valor da verificação da integridade (*Integrity Check Value* - ICV). O ICV protege o conteúdo do frame para que ele não possa ser

mudado durante o trajeto. O frame e o ICV são encriptados, assim o ICV está indisponível aos intrusos.

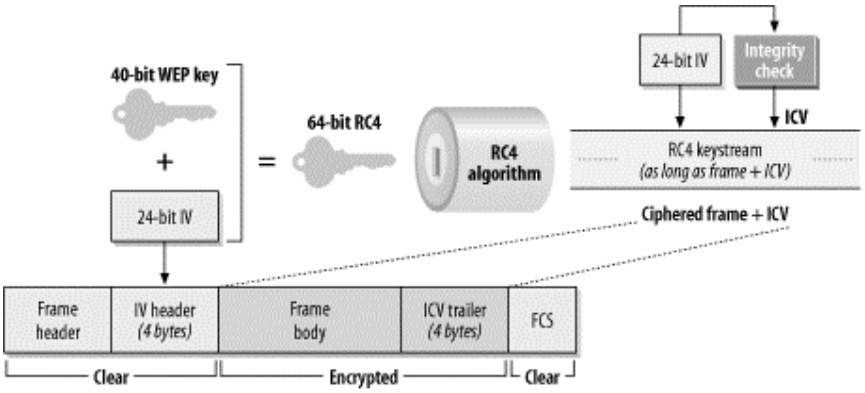

Figura 6 Operações do WEP.

Fonte: Fonte: Gast, M. S. “802.11b Wireless Networks - The definitive guide”, Abril de 2002.

O WEP especifica uma chave secreta de 40-bit. A chave secreta do WEP é combinada com um vetor de iniciação (IV) de 24-bit para criar uma chave RC4 de 64-bit; os primeiros 24 bits da chave RC4 são o IV, seguido pela chave de 40-bit WEP. O RC4 usa os 64 bits para gerar uma *keystream* igual ao comprimento do corpo do frame acrescido do comprimento do IV. A *keystream* é combinada (XORed) com o corpo do frame e o IV para cifrá-lo. Para o receptor decifrar a mensagem cifrada, o IV é colocado no cabeçalho do frame.

2.2.3 Falhas do Projeto WEP

As falhas de projeto de WEP ganharam evidência quando o grupo de segurança em internet, de aplicações, autenticação e criptografia (*Internet Security, Applications, Authentication and Cryptography* - ISAAC) da Universidade da Califórnia, Berkeley, publicaram os resultados preliminares baseados em sua análise do padrão WEP. Aqui está um sumário dos problemas que eles encontraram:

1. A gerência manual de chave sobrecarrega o administrador com tarefas operacionais. A chave secreta, compartilhada com o grupo de usuários torna-se pública. Ataques passivos de sniffing apenas requerem o conhecimento das chaves WEP, dificilmente mudadas, tornando a rede vulnerável.

2. O padrão WEP oferece segredo compartilhado de somente 40 bits embora a tecnologia tenha evoluído, admitindo chaves 128-bit. Nenhum padrão especifica chaves mais longas e não se garante a interoperabilidade das redes entre fabricantes com chaves WEP maiores que 40-bit. O IEEE não sinaliza trabalho futuro com esse escopo.

3. As cifras do fluxo são vulneráveis a análise quando a *keystream* é reutilizado. A utilização do "*Initialization Vector*" impede que o invasor reuse um *keystream*. Dois frames que compartilham o IV quase certamente usam as mesmas chaves secretas e a *keystream*. Este problema ocorre em implementações que não adotam IVs aleatórios.

4. Chaves não renovadas permitem que os intrusos montem o que a equipe de Berkeley chama de dicionários de decriptação, que são grandes coleções de frames cifrados com as mesmas *keystream*. Com mais frames usando a mesma pilha IV, mais informações estão disponíveis sobre os frames não encriptados, mesmo se a chave secreta não é recuperada.

5. O WEP usa um CRC para a verificação da integridade. Embora o valor da verificação da integridade seja cifrado pelo *keystream* RC4, os CRCs não são criptograficamente seguros. O uso de uma verificação fraca de integridade permite aos invasores modificar quadros transparentemente.

6. O ponto de acesso ocupa uma posição privilegiada para decifrar frames. Conceitualmente, esta característica pode ser atacada enganando o ponto de acesso em retransmitir os frames que foram cifrados pelo WEP. O frame recebido pelo ponto de acesso é decifrado e retransmitido para

estação do invasor. Se o invasor usasse WEP, o ponto de acesso cifraria o frame usando a chave do invasor.

2.2.4 Considerações e recomendações

O WEP foi projetado para fornecer a proteção mínima no segmento de rede sem fio. Não foi projetado para ambientes que exigem um alto nível de segurança e oferece conseqüentemente um nível reduzido de proteção. O grupo de trabalho do IEEE 802.11 devotou um conjunto inteiro de tarefas relacionadas à segurança. Esse grupo está trabalhando ativamente em um padrão específico para segurança. Alguns equipamentos oferecem itens de segurança proprietários que permitem uma autenticação mais forte da chave pública e das chaves aleatórias de sessão, com impactos na interoperabilidade. Segue uma lista das conclusões e das recomendações:

1. WEP não é útil, pois não protege contra ataques ocasionais de captura de tráfego. O WEP não garante confidencialidade.
2. A gerência manual de chave exige configuração de cada nó individualmente e chaves estáticas não adicionam segurança ao sistema.
3. WEP depende do compartilhamento de chaves secretas. Segredo compartilhado não é segredo.
4. Dados confidenciais devem usar sistemas criptográficos mais fortes. Sugere-se a utilização de IPSec ou SSH.
5. Ao usar 802.11 como extensão de uma LAN cuja segurança não deva ser comprometida, considere:
    a. Células remotas devem ser protegidas por sistemas criptográficos fortes de VPN tais como IPSec. Usar 802.11 em posições remotas pode aumentar o risco de interceptações. Os invasores podem capturar pacotes que trafegam em redes sem fio, mas o IPSec foi projetado para assegurar confidencialidade de dados em ambientes expostos.

   b. VPNs que ligam escritórios a suas filiais são tipicamente enlaces site-a-site e protegem somente a borda para o acesso ao *link* da matriz. O IPSec não protege a rede central de ações realizadas dentro do escritório remoto deixando-a vulnerável a sniffing.
6. WEP não protege usuários entre si. Se todos os usuários têm a chave WEP, qualquer tráfego pode ser facilmente decifrado. As redes *wireless* devem proteger um usuário do outro com soluções VPN ou com aplicações contendo segurança interna forte.

É perigoso supor que protocolos como IPSec e SSH sejam suficientes para resolver todos os problemas de segurança. Outros recursos também devem ser considerados tais como WPA (*Wireless Protected Access*), RADIUS (*Remote Authentication Dial In User Service*), TKIP (*Temporal Key Integrity Protocol*), *MAC filters* (Filtro por endereço MAC) e outros.

3 Métodos de mobilidade do host

Além do IP móvel, existem outras duas alternativas de arquitetura para mobilidade dos hosts que não foram tratadas pelo IETF: o Migrate [6] e HIP (*Host Integration Protocol*) [7].

3.1 Migrate

Migrate trabalha com FQDN (*Fully Qualified Domain Names* - nome de domínio totalmente qualificado) com o nome do host constante. Em sua aproximação com o IP móvel, a portabilidade pode ser adquirida usando-se DHCP. Entretanto, a determinação da posição é feita com base em lookups no DNS em uma base por sessão [13]. Na figura 7, cada vez que um host quer iniciar uma nova sessão com um usuário ou um host o DNS é consultado. Quando o host se move, ele atualiza os registros A e o PTR (mapeamentos entre hostnames e os endereços IP) no servidor DNS com o nome do domínio do host. Esta característica produz avanços nos protocolos seguros de atualização do DNS que estão disponíveis nas distribuições de DNS. Os antigos DNS *bindings* são evitados fazendo o *binding* sem o cache, colocando zero no campo TTL dos registros [8].

A manutenção da sessão é um grande desafio, talvez o mais árduo. Requer a participação fim a fim entre hosts, em particular, modificações no TCP. Os autores do método de movimento propõem uma opção Migrate no TCP permitindo que as conexões TCP existentes migrem para um novo endereço IP. Esta migração da conexão TCP pode ser realizada trocando-se dois segmentos TCP (SYN com a opção Migrate e o ACK deste segmento). Para impedir a invasão na conexão, a troca pode ser criptografada com o uso do IPsec [8].

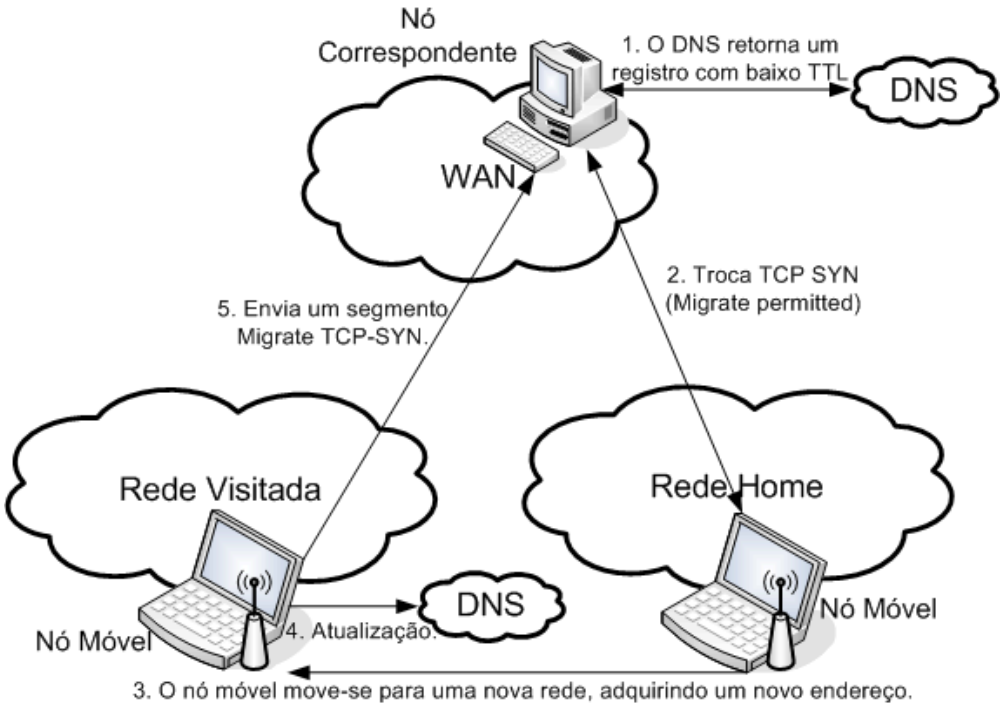

Figura 7 Operação do Migrate.

Fonte: Henderson, T.R. ,"Host Mobility for IP Networks: A Comparison", IEEE Network, Novembro/Dezembro 2003.

3.2 Host Identity Protocol

A idéia fundamental é atribuir (estaticamente) um nome global para qualquer estação que utiliza o IP, fazendo este nome ser criptografado (chave pública). Esta identidade do host pode ser usada para autenticar transações. Uma camada do protocolo HIP é interposta efetivamente entre o IP e a camada de transporte, permitindo o desacoplamento de conexões de transporte de endereços IP e de todos os pacotes que carregam uma representação de identidade do host, implicitamente ou explicitamente. A identidade do host pode ser armazenada em um DNS ou em uma infra-estrutura de chave pública (PKI) ou pode ser anônima, na qual pode ser utilizada para prevenir invasões de conexão [12].

O HIP requer um *handshake* inicial de quatro pacotes para iniciar a conexão, embora os datagramas possam ser criptografados e adicionados após os dois primeiros pacotes [11]. Neste aspecto, ele opera como uma versão mais simples do protocolo da troca da chave de Internet (IKE - *Internet Key Exchange*). Quando usado com IPsec, os pacotes subseqüentes não requerem um HIP adicional, desde que a identidade pode ser implícita no índice do parâmetro de segurança (SPI) carregado dentro dos pacotes IPsec protegidos . A identidade do host para um host conhecido pode ser obtida como parte do processo de resolução do nome [12].

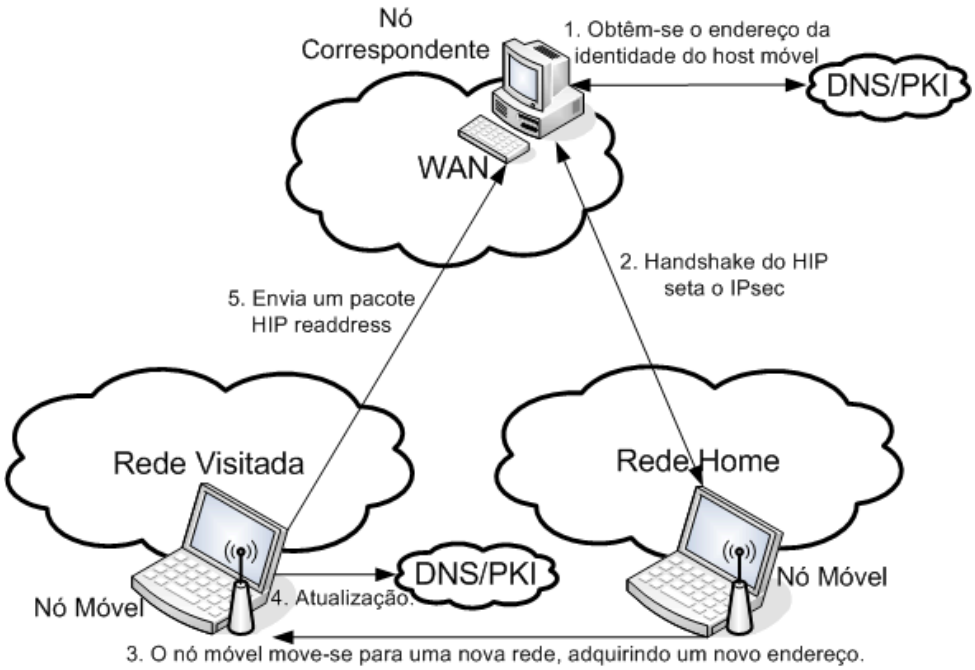

Figura 8 Funcionamento do HIP.

Fonte: Henderson, T.R. ,"Host Mobility for IP Networks: A Comparison", IEEE Network, Novembro/Dezembro 2003.

Pela figura 8, quando um host muda seu endereço durante uma conexão no HIP, ele pode emitir um pacote de *Readdress* do HIP para qualquer par correspondente HIPenabled. O pacote de *Readdress* do HIP contém o número de seqüência do atual ESP e o SPI para fornecer proteção ao denial-of-service (ataque de negação) e a proteção replay, sendo

autenticado com uma assinatura HIP. A mobilidade do usuário pode ser assegurada através das atualizações seguras do DNS, apenas na mobilidade fim-a-fim, mas na proposta do HIP sugere uma otimização na forma de um pequeno suporte de infra-estrutura chamado de rendezvous server.

O registro do DNS do servidor grava o endereço de um servidor *rendezvous*. Os usuários móveis emitirão um pacote de *Readdress* do HIP ao servidor rendezvous para mantê-lo atualizado com o atual endereço (que remove desse modo as atualizações do DNS na transação). A função de um servidor *rendezvous* é enviar simplesmente o pacote inicial do HIP a posição atual do servidor, em seguida o *handshake* prossegue com os endereços atuais [8]. Note que este servidor rendezvous proposto se assemelha a um agente *home* do IP móvel.

3.3 A escolha do IP Móvel

O IETF escolheu o IP móvel como seu foco de pesquisa de mobilidade de host por este se mostrar uma solução mais completa que a do HIP e Migrate. O suporte de ganhos de micro-mobilidade e sub-redes móveis é muito difícil de ser implementada em soluções fim a fim como HIP e Migrate. O Migrate necessita de mudanças na implementação do TCP em ambas pontas, o HIP apresenta pouca implementação, pouca experiência no desenvolvimento e um alto tráfego em pequenas transações. É claro que o IP móvel apresenta algumas desvantagens, mas são bem menos problemáticas que as apresentadas nestas duas alternativas e por isto foi escolhida como o padrão de desenvolvimento.

4 IPv4 móvel

A versão do protocolo IPv4 assume que o endereço IP de um nó é unicamente identificado por um ponto de nó conectado na rede [2]. Conseqüentemente, o nó deve estar situado na rede indicada pelo seu endereço IP para poder receber datagramas destinados a ele, se não, os datagramas destinados a ele não serão entregues. Para um nó mudar o seu ponto de acesso sem perder sua habilidade de comunicação deve-se utilizar um dos dois mecanismos:

a) O nó deve mudar o seu endereço IP sempre em que ocorre a mudança do seu ponto de acesso, ou
b) As rotas específicas ao host devem ser propagadas por toda estrutura de roteamento da rede.

Ambas alternativas são inaceitáveis. Um nó móvel deve comunicar-se com outros nós após mudar o seu ponto de acesso na rede sem mudar o seu endereço IP. A RFC 3344 elaborada pelo IETF (*The Internet Engineering Task Force*) especifica o IP móvel como a solução que permite que um nó móvel utilize dois endereços IP: um endereço fixo de *home* e um endereço mutável *care-of address*, que é mudado a cada ponto de acesso [2].

O IP móvel possibilita ao nó mover-se de uma sub-rede IP para outra. É também apropriado tanto para a mobilidade através de meios homogêneos quanto para heterogêneos. Isto é, o IP móvel facilita o movimento do nó de um segmento Ethernet para outro, assim como ele acomoda o movimento do nó de um segmento Ethernet para uma LAN wireless, mantendo o mesmo endereço IP após o movimento. O IP móvel faz a mobilidade transparente para as aplicações e aos protocolos das camadas de alto nível como o TCP [9].

As seguintes etapas explicam o processo de operação do IP móvel [2]:

- Os agentes móveis (isto é, agentes estrangeiros e agentes *home*) anunciam a sua presença através das mensagens *Agent Advertisement*. Um nó móvel pode opcionalmente solicitar uma mensagem *Agent Advertisement* de qualquer agente móvel presente no *link* através de uma mensagem de *Agent Solicitation*.
- Um nó móvel recebe estes *Agent Advertisements* e determina se está em sua rede *home* ou em uma rede estrangeira.
- Quando o nó móvel detecta que está em sua rede *home*, ele opera sem os serviços de mobilidade. Se ele está retornando para a sua rede *home*, estando registrado em outro lugar, o nó móvel cancela o registro com o seu agente *home* através de uma troca de mensagens *Registration Request* e *Registration Reply*.
- Quando um nó móvel detecta que se moveu para uma rede estrangeira, ele obtém um *care-of address* nesta rede. Um *care-of address* pode ser determinado por qualquer aviso de um agente estrangeiro ou por algum mecanismo externo de atribuição, como um DHCP.
- O nó móvel opera fora de sua *home* e registra o seu novo *care-of address* com seu agente *home*, que é efetuado com a troca das mensagens de *Registration Request* e *Registration Reply*, através de um agente estrangeiro.
- Os datagramas enviados ao endereço *home* do nó móvel são interceptados por seu agente *home*, e tunelados pelo agente *home* a um *care-of address* do nó móvel, recebendo-o no fim do túnel e finalmente entregue ao nó móvel.
- No sentido reverso, os datagramas enviados pelo nó móvel são geralmente entregues ao seu destino usando mecanismos de roteamento IP.

Quando está fora de sua rede *home*, o IP móvel usa o tunelamento de protocolo para esconder o endereço *home* do nó móvel entre a rede *home* e a sua posição atual. O túnel termina no *care-of address* do nó móvel. O *care-of address* deve ser um endereço na qual os datagramas possam ser enviados através de um roteamento IP. No *care-of address*, o datagrama original é removido do túnel e entregue ao nó móvel [2].

O IP móvel fornece duas modalidades para a aquisição de um *care-of address*:

a) Um *care-of address* do agente estrangeiro - É um *care-of address* fornecido por um agente estrangeiro através de suas mensagens de *Agent Advertisement*. Neste caso, o *care-of address* está em um endereço IP do agente estrangeiro. Nesta modalidade o agente estrangeiro é o ponto final do túnel e que com o recebimento de datagramas tunelados ele desencapsula o datagrama e entregua-o ao nó móvel. Esta modalidade de aquisição é a preferida, porque ela permite aos nós móveis o compartilhamento do mesmo *care-of address* e conseqüentemente não coloca demandas desnecessárias no espaço de endereços do IPv4.

b) *Care-of address* co-localizado - É um *care-of address* adquirido pelo nó móvel como um endereço IP local com algum meio externo, na qual o nó móvel associa-se com uma de suas interfaces de rede. O endereço pode ser adquirido dinamicamente como um endereço provisório pelo nó móvel, como no DHCP, ou pode ser criado pelo nó móvel como um endereço de longo prazo para utilizá-lo apenas enquanto estiver visitando uma rede estrangeira. Ao usar um *care-of address* co-localizado o nó móvel serve como ponto final do túnel e executa a desencapsulação dos datagramas tunelados para ele.

Ao se utilizar um *care-of address* co-localizado tem-se uma vantagem que é permitir que nó móvel funcione sem um agente estrangeiro em redes que não possuem ainda um agente estrangeiro. Este método coloca uma carga adicional no espaço de endereços IPv4 porque requer um *pool* de endereços dentro da rede estrangeira para disponibilizar aos nós móveis visitantes.

É importante compreender a distinção entre *care-of address* e as funções do agente estrangeiro. O *care-of address* é simplesmente um ponto final do túnel. Pode certamente ser um endereço de um agente estrangeiro (um *care-of address* do agente estrangeiro), mas pode ser um endereço adquirido temporariamente pelo nó móvel (*care-of address* co-localizado). Um agente estrangeiro é o agente de mobilidade que fornece serviços aos nós móveis.

Por exemplo, a figura 9 ilustra o roteamento dos datagramas para e do nó móvel para fora de sua *home*, uma vez que o nó móvel já se registrou com o seu agente *home*. Na figura, o nó móvel está usando um *care-of address* de um agente estrangeiro, não um *care-of address* co-localizado.

Figura 9 Operação do IPv4 Móvel.

Fonte: C. Perkins, Ed., "IP Mobility Support for IPv4," RFC 3344, Agosto de 2002.

Um agente *home* deve ser capaz de atrair e interceptar os datagramas que são destinados ao endereço *home* de qualquer nó móvel registrado. Usando o *proxy* e o mecanismo de *Gratuitous ARP*, esta exigência pode ser satisfeita se o agente *home* tiver uma interface de rede no *link* indicado pelo endereço *home* do nó móvel [2].

Se um nó móvel estiver usando *care-of address* co-localizado, o nó móvel deve estar localizado no *link* identificado pelo prefixo de rede deste *care-of address*. Se ele não estiver, os datagramas são descartados.

5 IPv6 Móvel

O projeto de suporte do IP móvel do IPv6 se beneficia das experiências ganhas do desenvolvimento do suporte móvel do IPv4. O IPv6 móvel compartilha muitas características do IPV4 móvel, mas é integrado com o IPv6 e oferece muitas outras vantagens.

As principais diferenças entre o IPv4 móvel e o IPv6 são:

- Não há necessidade de desenvolver roteadores especiais como os agentes estrangeiros (*foreign agents*), como no IPv4 móvel. O IPv6 móvel opera em qualquer lugar sem nenhum suporte do roteador local.
- Suporte para otimização de rotas é uma parte fundamental do protocolo, ao invés de um conjunto de extensões não padronizadas.
- A otimização da rota IPv6 móvel pode operar com segurança sem associações de segurança. Espera-se que a otimização da rota possa ser desenvolvida em uma escala global entre os nós móveis e nós correspondentes.
- O alcance de detecção vizinha de IPv6 assegura a alcançabilidade simétrica entre o nó móvel e seu roteador na posição atual.
- A maioria de pacotes transmitidos a um nó móvel quando está fora de sua *home* no IPV6 móvel são enviados usando o cabeçalho de roteamento IPv6 que é muito melhor que encapsulamento IP, utilizado no IPv4 móvel, reduzindo o tamanho do pacote.
- O IPv6 móvel utiliza a busca da vizinhança IPv6 ao invés do ARP, isto lhe garante uma robustez do protocolo.
- O uso da encapsulação IPv6 (e o cabeçalho de roteamento), dispensa a necessidade do IPv6 móvel de controlar o estado do túnel de software.
- O mecanismo dinâmico da descoberta do endereço do agente *home* no IPv6 móvel retorna a uma única resposta ao nó móvel. O

broadcast direcionado usado no IPv4 retorna respostas separadas de cada agente *home*.

Para entender a operação do IPv6 móvel devem-se conhecer alguns conceitos de IPv6. Os endereços IPv6 são indicações de 128 bits que estão distribuídos em oito grupos de quatro dígitos hexadecimais, separados por dois-pontos (:) e entre os grupos, ele possui o seguinte formato:

CDCD:910A:2222:5498:8475:1111:3900:2020

O número possível de endereços do IPv6 é de 2^{128}. O formato do cabeçalho básico do IPv6 é simplificado, possuindo apenas oito campos, enquanto o IPv4 possui 14 campos, sendo os campos alinhados e múltiplos de oito bits. Apesar do tamanho do endereço IPv6 ter aumentado quatro vezes, o tamanho do cabeçalho IPv6 é apenas duas vezes maior que o cabeçalho IPv4 [10]. A figura 10 mostra o cabeçalho básico do IPv6.

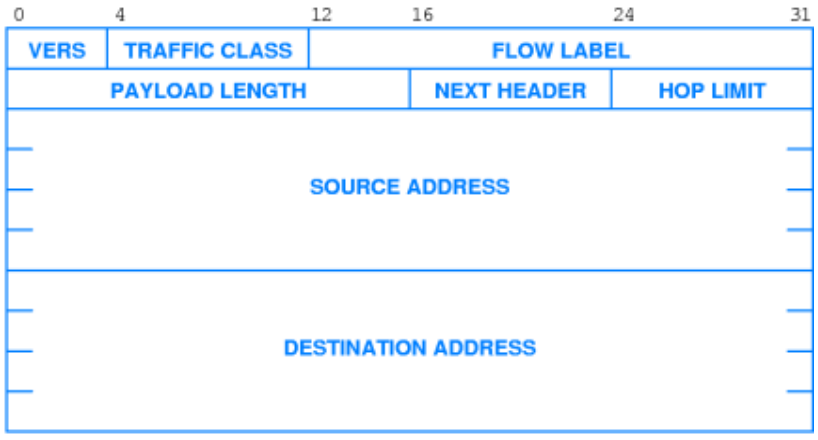

Figura 10 Cabeçalho básico do IPv6.

Fonte: S. Deering, R.Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, Dezembro de 1998.

A finalidade do IPv6 móvel é de aproveitar todas melhorias na nova versão do protocolo e das novas otimizações de roteamento e a não presença de um agente estrangeiro para tunelar os pacotes. O IPv4 móvel

apresenta um problema de roteamento triangular, que o grupo IETF não tem muito interesse em resolver este problema, aconselhando a todos mudarem para o IPv6 móvel.

5.1 Operação básica

Quando um nó móvel está conectado a alguma rede fora da sua *home*, ele também é endereçável em um ou mais *care-of address*. Um *care-of address* é um endereço IP associado a um nó móvel que tem um prefixo de sub-rede de um *link* estrangeiro. O nó móvel pode adquirir o seu *care-of address* através dos mecanismos convencionais do IPv6, na implementação utilizada no laboratório didático o *care-of address* é criado através de uma mistura da máscara de rede com o endereço MAC address da placa de rede. O nó móvel também pode aceitar pacotes de diversos care-of-address, por exemplo, quando está se movendo, mantendo ainda a sua ligação precedente.

A associação entre um endereço *home* de um nó móvel e o care-of-address é conhecida como "*binding*" para o nó móvel [5]. Quando o nó móvel está afastado de sua rede *home*, o nó móvel registra seu primeiro care-of-address com o roteador em seu *home link*, pedindo para este roteador executar a função de um agente *home* para o nó móvel. O nó móvel executa este registro obrigatório emitindo um *Binding Update* ao agente *home*.

Existem duas modalidades possíveis para comunicações entre o nó móvel e um nó correspondente. A primeira modalidade, conforme a figura 11, mostra o tunelamento bidirectional que não requer o suporte IPv6 móvel do nó correspondente e está disponível mesmo se o nó móvel não tiver registrado o seu atual *binding* com o nó correspondente. Pacotes do nó correspondente são distribuídos ao agente *home* e são tunelados ao nó móvel. Os pacotes para o nó correspondente são tunelados do nó móvel para o agente *home* ("tunelamento reverso") e distribuídos normalmente da rede *home* ao nó correspondente.

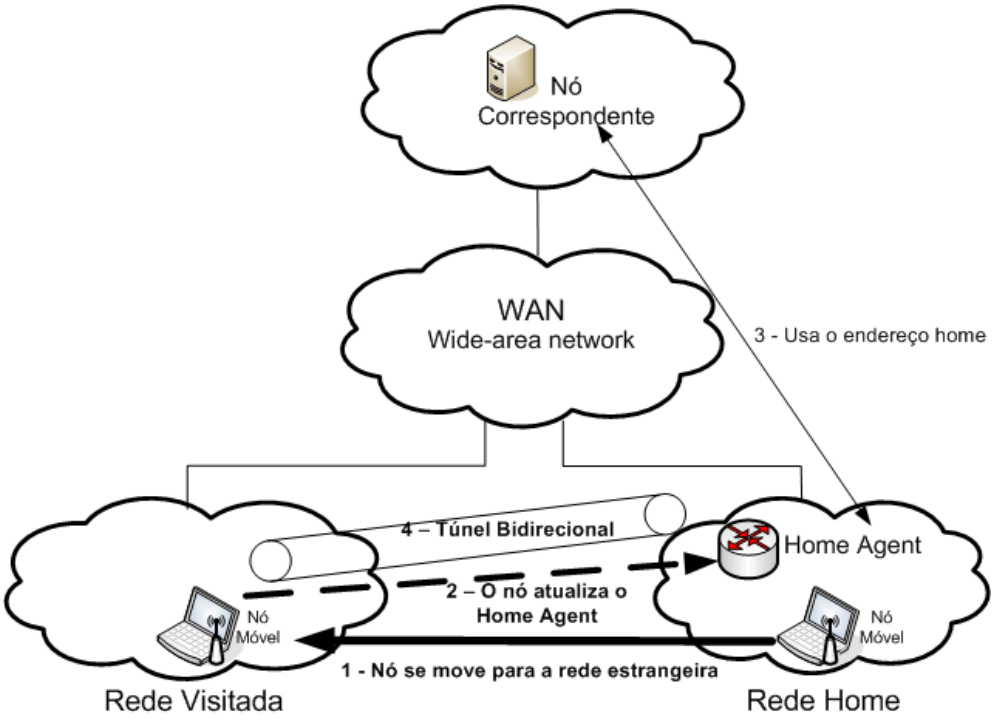

Figura 11 IP móvel baseado no Agente *home*.

Fonte: Henderson, T.R. ,"Host Mobility for IP Networks: A Comparison", IEEE Network, Novembro/Dezembro 2003.

A segunda modalidade, mostrada na figura 12, com otimização da rota, requer que o nó móvel registre seu atual *binding* no nó correspondente. Pacotes do nó correspondente podem ser distribuídos diretamente ao care-of-address do nó móvel. Ao enviar um pacote a algum destino IPv6, o nó correspondente verifica seus *bindings* em cache para ver se há uma entrada para o endereço de destino do pacote. Se um *binding* armazenado para este endereço de destino é encontrado, o nó usa um novo cabeçalho de roteamento do IPv6.

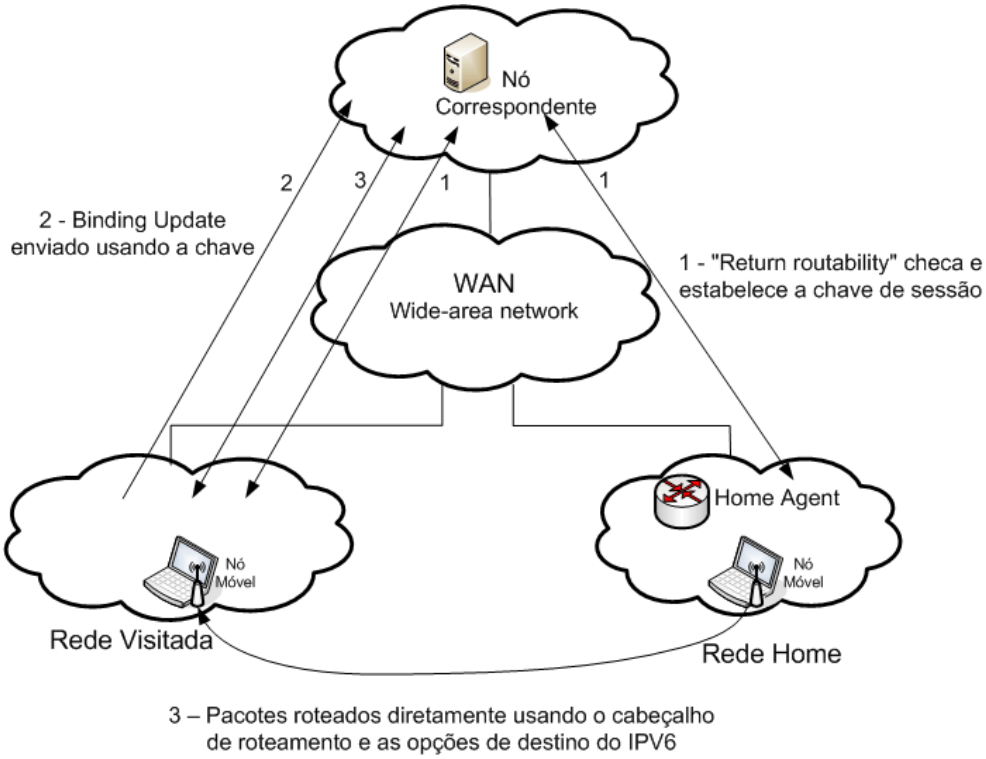

Figura 12 IP móvel com extensões de otimização da rota.

Fonte: Henderson, T.R. ,"Host Mobility for IP Networks: A Comparison", IEEE Network, Novembro/Dezembro 2003.

O IPv6 móvel fornece também o suporte para agentes *home* múltiplos e suporte limitado para a reconfiguração da rede *home*. Nestes casos, o nó móvel não poderá saber o endereço IP dos seus próprios agente *home*, e mesmo os prefixos de subrede da área *home* podem mudar o tempo excedente. Um mecanismo, conhecido como a descobrimento dinâmico do endereço do *home* do agente (*dynamic home agent address discovery*) possibilita ao nó móvel descobrir dinamicamente o endereço IP de um agente *home* em seu *link home*.

5.2 *Binding Updates* para os agentes home

O nó móvel e o agente *home* devem usar uma associação de segurança IPsec para proteger a integridade e a autenticidade dos *Binding*

Updates e seus reconhecimentos. Os nós móveis e os agentes *home* devem suportar e usar o cabeçalho de encapsulação do *payload* de segurança (*Encapsulating Security Payload* - ESP) na modalidade do transporte e devem usar um algoritmo de autenticação de *payload* não nulo para fornecer o reconhecimento da origem dos dados, a integridade das conexões e a proteção anti-replay opcional.

5.3 *Binding Updates* aos nós correspondentes

A proteção dos *Binding Updates* enviados aos nós correspondentes não requer a configuração de associações de segurança ou a existência de uma infra-estrutura de autenticação entre o nó móvel e os nós correspondentes. Este método não protege a ação de *hackers* que estão no trajeto entre a rede *home* e o nó correspondente. Entretanto, intrusos em tal posição são capazes de executar os mesmos ataques mesmo sem o IPv6 móvel. A principal vantagem do procedimento de retorno de roteamento é que limita os potenciais *hackers* que têm acesso a um trajeto específico dentro da rede, e evita *Binding Updates* forjados de qualquer lugar da rede.

6 Roteamento

O roteamento em redes móveis segue uma estrutura diferente das redes cabeadas, quando um nó móvel está em uma rede estrangeira com o seu *care-of address*, o Agente *Home* cria um *proxy* para o nó móvel interceptando todos pacotes destinados ao nó móvel, este procedimento é conhecido como *proxy* ARP, e o Agente *Home* tunela os pacotes para o *care-of address* do nó móvel, este procedimento é feito para o IPv4 móvel, no IPv6 móvel este procedimento foi substituído pela otimização de rota que não utiliza o ARP e sim os mecanismos de otimização de rota, utilizando a encapsulação IPv6 e cabeçalho de roteamento que diminui o tráfego na rede e é mais seguro.

6.1 Roteamento no IPv4 Móvel

O roteamento IPv4 utiliza o Proxy ARP, que é um pacote ARP enviado por um nó que está indisponível ou incapaz de esperar suas próprias requisições ARP. O nó que envia um Proxy ARP reverte o campo endereço de destino e o de origem do protocolo. O nó que está recebendo a reposta associa-se ao endereço da camada de enlace com o endereço IP do nó de destino [2].

O *Gratuitous ARP* é um pacote ARP enviado por um nó que causa a atualização da tabela de entradas do cache ARP dos outros nós na rede. Sem o *Gratuitous ARP*, o pacote ARP tem que ser transmitido como um *broadcast* local no *link* [2].

Enquanto o nó móvel estiver registrado em uma rede estrangeira, o seu Agente *Home* utiliza o Proxy ARP para responder as requisições ARP, ele busca o endereço do nó da camada de enlace. Quando o nó está recebendo uma requisição ARP, o Agente *Home* examina o endereço IP de destino da requisição e este endereço IP deve ser igual ao endereço *home* de qualquer nó móvel que está registrado através do *binding* móvel, o Agente *Home* transmite um ARP Reply para o nó móvel. Quando o nó móvel

registra-se em uma rede estrangeira, o Agente *Home* utiliza o *Gratuitous* ARP para atualizar a tabela cache dos nós da rede *home* [2].

6.2 Roteamento no IPv6 Móvel

O IPv6 móvel define um novo cabeçalho de roteamento chamado de cabeçalho de roteamento do tipo 2, que permite que pacotes sejam roteados diretamente do nó correspondente para o *care-of address* do nó móvel, este processo é conhecido por otimização de rota. O *care-of address* do nó móvel é inserido no campo de destino do IPv6. Quando o pacote chega no *care-of address*, o nó móvel recupera o seu endereço *home* do cabeçalho de roteamento e este é usado como o endereço de destino para o pacote.

Formato

O cabeçalho de roteamento do tipo 2 tem o formato mostrado na figura abaixo:

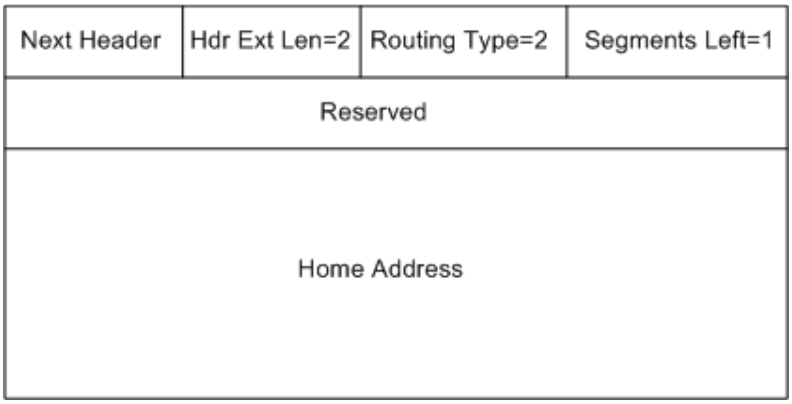

Figura 13 Cabeçalho de roteamento do tipo 2.

Next Header

Seletor 8-bit. Identifica o tipo de cabeçalho imediatamente seguido do cabeçalho de roteamento. Utiliza o mesmo valor do campo IPv6 *next header*.

Hdr Ext Len

Valor=2 (8-bit inteiro não assinado) É o tamanho do cabeçalho de roteamento em unidades de oito octetos, não inclui os oito primeiros octetos.

Routing Type

Valor=2 (8-bit inteiro não assinado).

Segments Left

Valor=1 (8-bit inteiro não assinado).

Reserved

Campo de 32-bit reservados. O valor deve iniciar com 0 pela estação que envia o pacote e deve ser ignorada pelo receptor.

Home Address

O endereço *home* do nó móvel de destino.

A maioria dos pacotes enviados pelo nó móvel enquanto estiver fora de sua rede *home* são enviados através do cabeçalho de roteamento do IPv6, diferente da encapsulação do IP, utilizada no IPv4 Móvel, reduzindo o tráfego na rede. Com a utilização da otimização de rota, não é mais necessário que o IPv6 móvel gerencie os túneis, obrigatórios no IPv4 Móvel.

7 Knoppix em ação

Para facilitar o ensino de redes wireless com suporte a mobilidade IPv6 em instituições educacionais deverá ser utilizado o Knoppix com o suporte do IPv6 móvel apresentado neste trabalho, como ferramenta de ensino. O Knoppix é uma distribuição de Linux tipo Live CD, na qual o CD é inserido no CDROM da máquina, é disparado o boot e o sistema é carregado em RAM, com o linux reconhecendo o *hardware* e tornando-se operacional sem fazer uso do disco rígido. Esta distribuição pode ser personalizada de acordo com a necessidade.

Alguns dos softwares contidos na distribuição oficial:

- *Kernel* 2.4.x ;
- KDE V3.1.x ;
- X Multimedia System MPEG-video, MP3, o player *Ogg Vorbis Audio* e o xine ;
- Conexão com a internet através do *kppp, pppoeconf (DSL)* e o *isdn-config ;*
- *Gnu Image Manipulation Program* (GIMP);
- Utilitários para recuperação e reparos de sistema, inclusive para outros sistemas operacionais como o Windows;
- Ferramentas de análise e segurança de redes;
- Open Office, a versão GPL do velho e conhecido Star Office, suíte similar e compatível com Microsoft Office;
- Muitas linguagens de programação, ferramentas de desenvolvimento e bibliotecas disponíveis para desenvolvedores;
- Um total de mais de 900 pacotes de softwares instalados.

Destes, o OpenOffice será excluído para abrir espaço no CDROM e possibilitar a inclusão dos pacotes que implementam o IP móvel e o código fonte do *kernel*. O suporte ao IPv6 móvel não está presente na distribuição padrão, sendo necessário realizar um processo denominado remasterização

do Knoppix. Através desse processo, podem-se substituir os pacotes existentes no CDROM e adequá-lo às necessidades específicas de um projeto, compilando ou até mesmo desenvolvendo novos programas. Após a escolha do aplicativo a ser incluído na remasterização pode ser gerado um CDROM a partir do formato ISO, para ser distribuído.

Mas esta alternativa cria um novo problema: como a distribuição fica gravada no CD-ROM, não é possível alterar os arquivos de configuração, geralmente localizados no diretório /etc das distribuições Linux. Deve-se buscar uma forma de ajustar a configuração básica para os laboratórios educacionais de redes sem fio, fazendo a distribuição Knoppix carregar as configurações do IPv6 móvel a partir de outro dispositivo que permita a gravação e leitura dos arquivos.

Através desta solução pode-se configurar o IP de cada máquina para formar uma rede IPv6 móvel. Esta customização oferece suporte a todas entidades do IPv6 móvel possibilitando a montagem de um laboratório completo desta tecnologia, com este CD-ROM será possível montar redes wireless de infra-estrutura e redes *ad-hoc*.

7.1 Roteiro de personalização do Knoppix

7.1.1 Exigências do Sistema:

- No mínimo 1 GB LIVRE de *RAM+Swap* (isto é 256M de RAM e 750M de *swap*) [15].
- 3 GB de espaço em disco de um sistema de arquivos Linux (ext2/3, xfs, etc..) com uma partição montada.

7.1.2 Instruções e pacotes a serem instalados:

- Inicializar a máquina com o CD do Knoppix [15].
- Configurar a conexão à Internet.

- Abrir o root *shell* (Kmenu->Knoppix->Root *Shell*) - todos os comandos abaixo são executados dentro deste root *shell*.
- Encontrar a partição que será utilizada. Neste exemplo será utilizada a **hda1**. A partição deve ter no mínimo 3 GB de espaço livre.
- Montar a partição (este comando deve ser executado conforme demonstrado, para evitar futuros erros na execução de chroot).

 # mount -rw /dev/hda1 /mnt/hda1

- Criar um diretório raiz para executar o trabalho:

 # mkdir /mnt/hda1/knx

- Se a máquina não tiver 1 GB RAM, será necessário criar um arquivo de *swap*:

 # cd /mnt/hda1/knx

 # dd if=/dev/zero of=swapfile bs=1M count=750

 # mkswap swapfile

 # swapon swapfile

- Crie 2 diretórios, um para o CD master e outro para o fonte, na partição do hard disk:

 # mkdir /mnt/hda1/knx/master;

 # mkdir /mnt/hda1/knx/source

 # mkdir /mnt/hda1/knx/source/KNOPPIX

- Copie os arquivos do KNOPPIX para o diretório fonte (este processo demora aproximadamente 30 minutos)

 # cp -Rp /KNOPPIX/* /mnt/hda1/knx/source/KNOPPIX

 # mkdir /mnt/hda1/knx/master/KNOPPIX

 # cp /cdrom/index.html /mnt/hda1/knx/master/

- Copie todo conteúdo do diretório /cdrom/KNOPPIX/ para **mnt/hda1/knx/master/KNOPPIX**/ , exceto o arquivo KNOPPIX

 # cd /cdrom/KNOPPIX;

 # find . -size -10000k -type f -exec cp -p --parents {}
/mnt/hda1/knx/master/KNOPPIX/ \;

- Execute o chroot para o Knoppix copiado:

 # chroot /mnt/hda1/knx/source/KNOPPIX

Se forem exibidas mensagens de erros **/dev/null permission denied**, verifique seu status da montagem da partição: **mount /dev/hdaX on /mnt/hdaX type ext3 (rw,nosuid,nodev)** (substituir X pelo número da partição) e se os erros persistirem, execute:

 # mount --bind /dev /mnt/hda/knx/source/KNOPPIX/dev

- Agora o diretório "/" é na verdade o "/mnt/hda1/knx/source/KNOPPIX"
- Para usar a Internet é necessário montar a proc

 # mount -t proc /proc proc

editar o arquivo /etc/resolv.conf e adicionar o servidor de nomes, no ambiente testado a resolução de nomes não foi possível; para utilizar o comando apt-get update foi necessário mudar o nome dos servidores da lista contida no arquivo /etc/apt/sources.list para números IP.

 # ping google.com ou 216.239.39.99

- Atualizar a lista de pacotes com o comando

 # apt-get update

- Agora os pacotes podem ser alterados.
- Para verificar a lista dos pacotes instalados, digite:

 # dpkg-query

- Para exibir a lista por ordem do tamanho do pacote:

 # dpkg-query -W --showformat='${Installed-Size} ${Package}\n' | sort –n

- Para remover um pacote:

 # apt-get remove <nome-do-pacote-a-ser-removido>

- Para verificar para ver se há pacotes órfãos:

 # deborphan

- Para adicionar um pacote:

 # apt-get install <nome-do-pacote>

- Para limpar o cache dos downloads dos pacotes, execute o seguinte comando:

 # apt-get clean

Neste momento deve ser instalado o *Mobile IPV6*, em ambientes unix existem duas distribuições:

- Lancaster Mobile IPv6 package
- MIPL *Mobile IPv6 for* Linux

A distribuição da Lancaster não é atualizada desde 1998, por isso deve-se considerá-la obsoleta. A distribuição MIPL (*Mobile IPv6 for* Linux) está na versão 2.0 RC1 e suporta o *kernel* versão 2.6.8.1, foi desenvolvida pela universidade de tecnologia de Helsinki, na Finlândia. A versão utilizada na customização do Knoppix 3.3 é 1.0, ela está totalmente de acordo com a especificação do *Mobile IPv6* (*draft* 24), não há o suporte ao IPSec nativo.

Para instalar o MIPv6 no Knoppix deve ser feito o download do software no site da universidade de Helsinki no endereço http://chasey.mobile-ipv6.org/software/download/mipv6-1.0-v2.4.22.tar.gz e extrair o arquivo para um diretório. A implementação do MIPv6 requer um patch no *kernel*. Ela modifica a estrutura do IPv6 no *kernel* do linux, sendo necessário uma recompilação deste *kernel*.

Extraia o arquivo mipv6−1.0−v2.4.22.tar.gz para o diretório /usr/local/src execute:

 # cd /usr/local/src ; tar zxfv mipv6−1.0−v2.4.22.tar.gz

Faça o download do fonte do *kernel* no formato de pacote do Debian no site: http://developer.linuxtag.net/knoppix/sources/*kernel*-source-2.4.22-

xfs_10.00.Custom_all.deb. Depois execute o comando para instalar a fonte do *kernel*:

 # dpkg –i kernel-source-2.4.22-xfs_10.00.Custom_all.deb
 # cd /usr/src
 # ln −s kernel-source-2.4.22-xfs linux
 # cd linux

Para o Knoppix poder detectar todos os dispositivos de *hardware* o arquivo.config do CD da distribuição deve ser substituído pelo existente no diretório do fonte do *kernel*, abra uma nova sessão do *shell* e execute o comando:

#cp /usr/src/linux/.config /mnt/hda1/knx/source/KNOPPIX/usr/src/linux

Agora todas as opções necessárias para que a estrutura básica do *kernel* funcione está pronta, agora adicione os módulos do IPv6 móvel, no *shell* que foi executado o chroot, digite estes comandos para aplicar MIPv6 patch:

 # patch −p1 −−dry−run < usr/local/src/mipv6−1.0−v2.4.22
/mipv6−1.0−v2.4.22.patch

Se não ocorrerem erros, execute:

 # patch −p1 < /usr/local/src/mipv6−1.0−v2.4.22/mipv6−1.0−v2.4.22.patch

Através destes comandos a estrutura do *kernel* foi modificada possibilitando a inclusão dos módulos do IPv6 Móvel. Execute o comando para adicionar os módulos do IPv6 móvel

 # make menuconfig

No menu *Networking Options* selecione as opções *IPv6 routing by source address, IPv6 over IPv6 tunneling, Ipv6 Mobility Support, MIPv6 Mobile Node support, MIPv6 Home Agent Support, MIPv6 Debug Messages*.

Saia do menuconfig, grave as modificações e execute o commando **mcedit .config** e confira se estas opções estão presentes:

CONFIG_EXPERIMENTAL=y
CONFIG_SYSCTL=y
CONFIG_PROC_FS=y
CONFIG_MODULES=y
CONFIG_NET=y
CONFIG_NETFILTER=y
CONFIG_UNIX=y
CONFIG_INET=y
CONFIG_IPV6=m
CONFIG_IPV6_SUBTREES=y
CONFIG_IPV6_IPV6_TUNNEL=m
CONFIG_IPV6_MOBILITY=m
CONFIG_IPV6_MOBILITY_MN=m
CONFIG_IPV6_MOBILITY_HA=m
CONFIG_IPV6_MOBILITY_DEBUG=y

Após esta verificação o *kernel* deve ser compilado. Execute os seguintes comandos:

 # make dep ;
 # make clean ;
 # make bzImage ;
 # make modules ;
 # make modules_install

A ferramenta de userspace **mipdiag**, arquivos de configuração e scripts de inicialização devem ser instalados para o módulo de MIPv6 funcionar corretamente, no *shell* que foi executado o comando chroot digite:

 # cd /usr/local/src/mipv6−1.0−v2.4.22
 # ./configure
 # make && make install

O módulo do MIPv6 precisa de uma entrada para o novo dispositivo:

 # mknod /dev/mipv6_dev c 0xf9 0

Os programas radvd e o ping6 e o driver para os equipamentos wireless compatíveis com o driver HostAP foram instalados:

 # dpkg –i iputils-ping_20020124i386.deb
 # dpkg –i radvd_0.7.1-5_i386.deb

O arquivo de configuração do IPv6 móvel e do radvd irá ser lido através do disquete, para que isto ocorra o *link* deve ser criado no diretório apontando para o disquete, o disquete deve ser formatado com o sistema de arquivos do linux, ext2 ou ext3 e o arquivo radvd.conf deve possuir permissões de leitura e gravação apenas para o dono e o resto deve ser deixado como zero com o comando **chmod 700 radvd.conf** .

 # cd /etc
 # cp radvd.conf radvd.conf.old
 # ln –s /mnt/auto/floppy/radvd.conf radvd.conf
 # cd sysconfig
 # cp network-mip6.conf network-mip6.conf.old
 # cp /mnt/auto/floppy/network-mip6.conf network-mip6.conf

A imagem do *kernel* deve ser copiada para o diretório de *boot*:

 # cp arch/i386/boot/bzImage /boot/vmlinuz-2.4.22-xfs
 # cp System.map /boot/System.map-2.4.22-xfs
 # ln –s /boot/System.map-2.4.22-xfs /boot/System.map

Esta distribuição utiliza o isolinux como forma de boot, abra uma nova sessão do *shell* e vá para o diretório /**mnt/hda1/knx/master/**, crie o diretório com o nome de **isolinux,** copie os arquivos do diretório boot para o isolinux, faça o download do arquivo **isolinux.bin** que pode ser obtido no pacote SysLinux no endereço http://www.*kernel*.org/pub/linux/utils/boot/syslinux/ :

 # cp /boot/* /mnt/hda1/knx/master/isolinux
 # rm ldlinux.sys
 # mv isolinux/syslinux.cfg isolinux/isolinux.cfg
 # cp /mnt/hda1/knx/source/KNOPPIX/boot/vmlinuz-2.4.22-xfs
/mnt/hda1/knx/master/isolinux/vmlinuz

7.1.3 Finalizando a personalização

Após ter removido ou adicionado a customização do Knoppix deve-se desmontar /proc. Execute o seguinte comando:

 # umount /proc

Depois pressione **CTRL+D** para deixar o chroot.

7.1.4 Criando o arquivo ISO

Execute uma limpeza:

 # remove .bash_history files, tmp files etc

 # rm -rf /mnt/hda1/knx/source/KNOPPIX/.rr_moved

Agora sera criado o arquivo KNOPPIX que é um arquivo comprimido do tipo ISO 9660:

 # mkisofs -R -U -V "KNOPPIX.netfilesystem" -P "KNOPPIX www.knoppix.net" -hide-rr-moved -cache-inodes -no-bak -pad /mnt/hda1/knx/source/KNOPPIX | nice -5 /usr/bin/create_compressed_fs - 65536 > /mnt/hda1/knx/master/KNOPPIX/KNOPPIX
 # cd /mnt/hda1/knx/master
 # rm -f KNOPPIX/md5sums; find -type f -not -name md5sums -not -name boot.cat -exec md5sum {} \; >> KNOPPIX/md5sums
 # mkisofs -pad -l -r -J -v -V "KNOPPIX" -no-emul-boot -boot-load-size 4 -boot-info-table -b isolinux/isolinux.bin -c isolinux/boot.cat -hide-rr-moved -o /mnt/hda1/knx/knoppix.iso /mnt/hda1/knx/master

Uma mensagem de erro informando que o arquivo não está em conformidade com os padrões da ISO será mostrada, mas esta mensagem deve ser ignorada, o arquivo ISO /mnt/hda1/knx/knoppix.iso será gravado. O arquivo iso é utilizado para gravar o cd.

8 Laboratório Didádico

Com a customização do Knoppix o CD possui suporte a todas entidades do IPV6 móvel, com os *links* do CD para o disquete é possível modificar os arquivos de configuração e mesmo após desligar as máquinas estas configurações não são perdidas, possibilitando que em poucos minutos este laboratório entre em funcionamento.

Será montado um ambiente contendo três máquinas: duas com suporte a mobilidade IPv6 e uma sem suporte. O nó móvel e o agente *home* estão configurados na rede com o essid **fabio** e o nó correspondente com o essid **visitnet**. Para testar a mobilidade, um servidor ftp será inicializado na máquina do agente *home*. O nó móvel iniciará uma conexão com o agente *home* e um arquivo começará a ser transferido e durante o download do arquivo o nó móvel irá trocar de essid, mudando de sub-rede, pois a rede visitnet está em um segmento diferente da rede fabio. A figura abaixo mostra a topologia e os endereços dos dispositivos do laboratório.

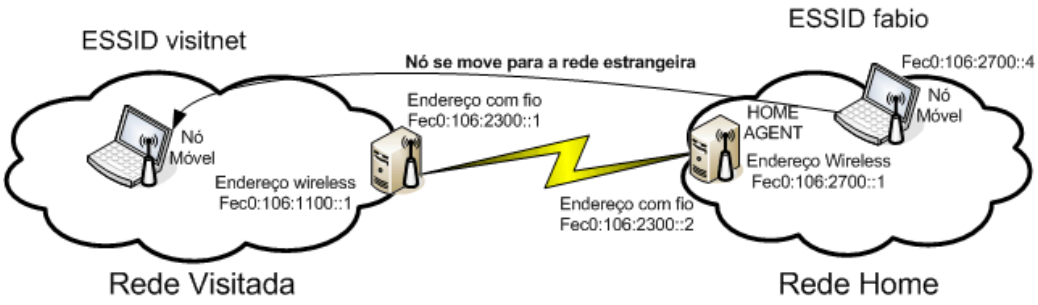

Figura 14 Arquitetura do laboratório didático.

O principal objetivo deste laboratório didático é implementar experimentos baseados na teoria apresentada, contribuir para entender o uso da tecnologia e fixar conceitos de mobilidade em redes sem fio com o IPv6. Através de logs do Ethereal pode-se mostrar a transição das redes e como o IPv6 móvel age para não perder a conexão e continuar a fazer o download do arquivo sem interrupção.

8.1 IP das estações de trabalho do laboratório

O nó móvel possui apenas uma placa sem-fio, o agente *Home* possui uma placa sem fio e uma com fio, e o nó correspondente possui uma com fio e outra placa sem fio. Os endereços IPv6 do tipo site local são:

- Nó móvel, localizado na rede com *essid* fabio com o IP **fec0:106:2700::4**.
- Agente *Home*, localizado na rede fabio com o IP **fec0:106:2700::1** e o IP **fec0:106:2300::2** na placa com fio que é ligada no nó correspondente através de um cabo com ligação direta (*cross over*).
- Nó correspondente localizado na rede visitnet com o IP sem fio **fec0:106:1100::1** e o com fio **fec0:106:2300::1** .

8.2 Configuração das máquinas, passo a passo

Antes de inicializar os testes com o ftp e o roteamento, primeiramente deve ser montada a rede IPv6, inclusive deve ser feita a configuração do radvd (*Router Advertisement*), que é um componente do IPv6 necessário para a auto configuração *stateless*. O radvd envia mensagens de anúncio que as estações solicitam através da mensagem de solicitação do roteador (*Router Solicitation*). Digite os seguintes comandos em cada máquina:

Nó Móvel:

```
# modprobe ipv6
# ifconfig eth0 up
# iwconfig eth0 mode ad-hoc essid fabio enc off
# ifconfig eth0 inet6 add fec0:106:2700::4/64
# echo "0" > /proc/sys/net/ipv6/conf/eth0/forwarding
# echo "1" > /proc/sys/net/ipv6/conf/eth0/autoconf
# echo "1" > /proc/sys/net/ipv6/conf/eth0/accept_ra
# echo "1" > /proc/sys/net/ipv6/conf/eth0/accept_redirects
```

Agente *Home*:

```
# ifconfig eth0 inet6 add fec0:106:2300::2/64
# iwconfig wlan0 mode ad−hoc essid fabio enc off
# ifconfig wlan0 inet6 add fec0:106:2700::1/64
# echo "1" > /proc/sys/net/ipv6/conf/ wlan0/forwarding
# echo "0" > /proc/sys/net/ipv6/conf/ wlan0/autoconf
# echo "0" > /proc/sys/net/ipv6/conf/ wlan0/accept_ra
# echo "0" > /proc/sys/net/ipv6/conf/ wlan0/accept_redirects
# ip route add fec0:106:1100::1/64 via fec0:106:2300::1
```

Nó Correspondente:

```
# ifconfig eth0 inet6 add fec0:106:2300::1/64
# iwconfig eth1 mode ad-hoc essid visitnet enc off
# ifconfig eth1 inet6 add fec0:106:1100::1/64
# echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
# echo "0" > /proc/sys/net/ipv6/conf/all/autoconf
# echo "0" > /proc/sys/net/ipv6/conf/all/accept_ra
# echo "0" > /proc/sys/net/ipv6/conf/all/accept_redirects
# ip route add fec0:106:2700::/64 via fec0:106:2300::2
```

8.3 Configurando o IPv6 móvel

O arquivo network-mip6.conf deve ser configurado no nó móvel e no agente *home*, nesta distribuição o arquivo estará localizado no disquete. Digite o seguinte comando:

 # cat /etc/sysconfig/network-mip6.conf

O arquivo de configuração no nó móvel deve conter as configurações:

```
# Mobile Node configuration file
FUNCTIONALITY=mn
DEBUGLEVEL=1
TUNNEL_SITELOCAL=yes
MIN_TUNNEL_NR=1
MAX_TUNNEL_NR=3
HOMEDEV=mip6mnha1
HOMEADDRESS=fec0:106:2700::4/64 # MN's home adress
HOMEAGENT=0::0/64 # Descobrimento automático do Agente Home
```

O agente *Home* deve conter estas configurações:

 # cat /etc/network-mip6.conf

```
# Home Agent configuration file
FUNCTIONALITY=ha
DEBUGLEVEL=1
MIN_TUNNEL_NR=1
MAX_TUNNEL_NR=5
TUNNEL_SITELOCAL=yes
```

Em seguida, deve-se inicializar o serviço IPv6 Móvel nas duas estações:

 # /etc/init.d/mobile-ip6 start

```
Starting Mobile IPv6: OK
```

Através do comando ifconfig podemos ver que o IPv6 móvel foi inicializado com sucesso:

 # ifconfig

```
eth0  Link encap:Ethernet  HWaddr 00:04:75:BC:27:B6
      inet6 addr: fec0:106:2700::4/64 Scope:Site
      inet6 addr: fe80::204:75ff:febc:27b6/64 Scope:Link
      inet6 addr: fec0:106:2700:0:204:75ff:febc:27b6/64 Scope:Site
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:981 errors:0 dropped:0 overruns:0 frame:0
      TX packets:24 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:100
      RX bytes:0 (0.0 b)  TX bytes:2504 (2.4 KiB)
          Interrupt:3 Base address:0x100

lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:6 errors:0 dropped:0 overruns:0 frame:0
      TX packets:6 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0
      RX bytes:300 (300.0 b)  TX bytes:300 (300.0 b)

mip6mnha1 Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
      inet6 addr: fec0:106:2700::4/64 Scope:Site
      UP RUNNING NOARP  MTU:1460  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0
      RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

O mip6mnha1 é o túnel ativo e preparado para as conexões.

8.4 Configurando o radvd

O radvd deve ser configurado no Agente *Home* e no nó correspondente, o arquivo */etc/radvd.conf* deve estar no disquete e deve possuir esta configuração:

 # cat /etc/radvd.conf

```
interface eth1
{
AdvSendAdvert on;
AdvIntervalOpt on;
MinRtrAdvInterval 3;
MaxRtrAdvInterval 10;
AdvHomeAgentFlag off;
prefix fec0:106:1100::/64
 {
AdvOnLink on;
AdvAutonomous on;
AdvRouterAddr on;
 }
}
```

E no Agente *Home* deve ter estes parâmetros:

 # cat /etc/radvd.conf

```
interface wlan0
{
AdvSendAdvert on;
MaxRtrAdvInterval 3;
MinRtrAdvInterval 1;
AdvIntervalOpt off;
AdvHomeAgentFlag on;
HomeAgentLifetime 10000;
HomeAgentPreference 20;
AdvHomeAgentInfo on;
prefix fec0:106:2700::1/64
{
AdvRouterAddr on;
AdvOnLink on;
AdvAutonomous on;
AdvPreferredLifetime 10000;
AdvValidLifetime 12000;
};
};
```

Através do comando /**etc/init.d/radvd start** , o radvd é inicializado. A partir deste momento todas as máquinas devem ser alcançáveis, o comando ping6 IP da máquina deve funcionar para todas interfaces de todas máquinas.

8.5 Testes didáticos: movimento de sub-rede, ftp e roteamento

Para construir um laboratório didático é necessário criar algumas tarefas que demonstrem o assunto abordado. Neste trabalho didático serão abordadas duas funcionalidades do IPv6 móvel: a utilização do ftp e o processo de roteamento.

Uma sessão ftp é estabelecida na rede essid fabio com um download de um arquivo e durante esta transmissão o essid será alterado para a rede visitnet. Com a adição de rotas mostrada no item 8.2 pode verificar o comportamento do roteamento na rede IPv6 móvel. No Agente *Home* inicia-se um servidor de ftp que contém o arquivo wingate.log. No nó móvel digita-se o seguinte comando:

 # ftp fec0:106:2700::1

Digita-se o usuário e senha e dispara-se o download do arquivo wingate.log através do comando:

 # get wingate.log

Após o comando get deve-se mudar o essid para visitnet no nó móvel:

 # iwconfig eth0 essid visitnet

Após a mudança do essid um novo IP é gerado com a máscara da sub-rede visitnet, que pode ser visto usando-se ifconfig no nó móvel:

eth0 Link encap:Ethernet HWaddr 00:04:75:BC:27:B6

```
inet6 addr: fec0:106:2700::4/64 Scope:Site
inet6 addr: fe80::204:75ff:febc:27b6/64 Scope:Link
inet6 addr: fec0:106:1100:0:204:75ff:febc:27b6/64 Scope:Site
inet6 addr: fec0:106:2700:0:204:75ff:febc:27b6/64 Scope:Site
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:94905 errors:0 dropped:0 overruns:0 frame:0
TX packets:32030 errors:8 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:100
RX bytes:0 (0.0 b)  TX bytes:3399159 (3.2 MiB) Interrupt:3 Base address:0x100
```

O IP fec0:106:1100:0:204:75ff:febc:27b6/64 é criado com a máscara da rede visitnet, este endereço é gerado com a mistura do prefixo da rede visitnet e o endereço MAC da placa wireless. Na troca do essid o nó móvel envia um *Binding Update* para o agente *home*:

 # mipdiag -s

```
Mobile IPv6 Statistics
NEncapsulations            : 0
NDecapsulations            : 0
NBindRefreshRqsRcvd        : 0
NHomeTestInitsRcvd         : 0
NCareofTestInitsRcvd       : 0
NHomeTestRcvd              : 0
NCareofTestRcvd            : 0
NBindUpdatesRcvd           : 0
NBindAcksRcvd              : 1
NBindNAcksRcvd             : 0
NBindErrorsRcvd            : 0
NBindRefreshRqsSent        : 0
NHomeTestInitsSent         : 0
NCareofTestInitsSent       : 0
NHomeTestSent              : 0
NCareofTestSent            : 0
NBindUpdatesSent           : 1
NBindAcksSent              : 0
NBindNAcksSent             : 0
NBindErrorsSent            : 0
NBindUpdatesDropAuth       : 0
NBindUpdatesDropInvalid    : 0
NBindUpdatesDropMisc       : 0
NBindAcksDropAuth          : 0
NBindAcksDropInvalid       : 0
NBindAcksDropMisc          : 0
NBindRqsDropAuth           : 0
NBindRqsDropInvalid        : 0
NBindRqsDropMisc           : 0
```

Um *Binding Update* recebido NBindAcksRcvd: 1 e um *Binding Update* enviado NBindUpdatesSent : 1.

Através do log gerado pela ferramenta Ethereal pode-se observar o início da conexão e os comandos de ftp para realizar o download do arquivo:

Número Pacote	Origem	Destino	Proto-colo	Informações
18	fec0:106:2700::1	fec0:106:2700::4	FTP	Response: 220 Welcome to Fabio FTP service.
50	fec0:106:2700::1	fec0:106:2700::4	FTP	Response: 200 Switching to Binary mode.
52	fec0:106:2700::1	fec0:106:2700::4	FTP	Request: SIZE wingate.log
61	fec0:106:2700::1	fec0:106:2700::4	FTP	Request: RETR wingate.log
62	fec0:106:2700::1	fec0:106:2700::4	FTP	Response: 150 Opening BINARY mode data connection for wingate.log (125451577 bytes).
7401	fec0:106:1100:0:204: 75ff:febc:27b6	fec0:106:2700::1	MIPv6	Binding Update
7404	fec0:106:2700::1	fec0:106:1100:0: 204:75ff:febc:27b6	MIPv6	Binding Acknowledgement
7405	fec0:106:2700::1	fec0:106:1100:0: 204:75ff:febc:27b6	TCP	46792 > 32776 [ACK] Seq=0 Ack=0 Win=5712 [CHECKSUM INCORRECT] Len=1380 TSV=609323 TSER=530961
7408	fec0:106:1100:0: 204:75ff:febc:27b6	fec0:106:2700::1	TCP	32776 > 46792 [ACK] Seq=0 Ack=6900 Win=63480 [CHECKSUM INCORRECT] Len=0 TSV=531953 TSER=609323

Tabela 3Log da transmissão FTP no momento da mudança do essid.

O destino do arquivo na conexão ftp passa a ser para o *care-of address* adquirido a partir do pacote 7405, como se pode ver na tabela 3. Nesse momento o nó móvel exibe o novo endereço adquirido contendo o prefixo da rede visitnet. Antes desta mudança o nó móvel envia um *Binding Update* para o agente *Home* na rede fabio que responde com uma mensagem de Bind Acknowledgement. O Agente *Home* tunela os pacotes para o nó móvel utilizando o source address extraído do pacote de Bind Update. Pode-se obter a lista de *care-of address* através do comando:

 # mipdiag -c
Mobile IPv6 Binding cache
Home Address Care-of Address Lifetime Type
fec0:106:2700::4 fec0:106:1100:0:204:75ff:febc:27b6 924 2

O campo type identifica o tipo de roteamento utilizado, como neste exemplo a otimização de rota está sendo utilizada o cabeçalho de roteamento do tipo 2. O comando mipdiag –m executado no nó móvel mostra a qual Agente *Home* o nó está associado e o mipdiag –l mostra a lista de *Binding* do nó móvel:

 # mipdiag -m

If *Home* Address/prefix length *Home Agent* H R
05 fec0:106:2700::4 / 64 fec0:106:2700::1 0 1

 # mipdiag -l
Mobile IPv6 Binding update list
Recipient CN: fec0:106:2700::1
BINDING *home* address: fec0:106:2700::4 care-of
address:fec0:106:1100:0:204:75ff:febc:27b6
expires: 944 sequence: 0 state: 1 delay: 3 max delay 32 callback time: 744

A tabela de roteamento IPv6 é alterada quando ocorre a transição para a rede visitada. Antes da mudança de sub-rede a estrutura de roteamento apresenta-se assim:

```
root@ttyp0[floppy]# route -A inet6
Kernel IPv6 routing table
Destination        Next Hop  Flags Metric Ref    Use Iface
::1/128              ::       U     0      0        0 lo
fe80::204:75ff:febc:27b6/128 :: U   0      0        0 lo
fe80::/64            ::       UA   256     0        0 eth0
fe80::/64            ::       UA   256     0        0 mip6mnha1
fec0:106:2700::4/128 ::       U     0      23       0 lo
fec0:106:2700:0:204:75ff:febc:27b6/128 :: U 0 0     0 lo
fec0:106:2700::/64   ::       UA    256    313      0 eth0
fec0:106:2700::/64   ::       UA    256    0        0 mip6mnha1
ff02::1/128        ff02::1    UAC   0      4        0 eth0
ff00::/8             ::       UA    256    0        0 eth0
ff00::/8             ::       UA    256    0        0 mip6mnha1
::/0 fe80::20d:88ff:fe65:303f UGDA 1024    0        0 eth0
```

A rota padrão ::/0 está setada na placa eth0 no nó móvel, após a mudança de sub-rede a tabela apresenta-se desta forma:

```
root@ttyp0[floppy]# route -A inet6
Kernel IPv6 routing table
Destination                    Next Hop Flags Metric Ref Use Iface
::1/128                          ::       U     0      0    0 lo
fe80::204:75ff:febc:27b6/128     ::       U     0      2    0 lo
fe80::/64                        ::       UA    256    0    0 eth0
fe80::/64                        ::       UA    256    0    0 mip6mnha1
fec0:106:1100:0:204:75ff:febc:27b6/128 :: U  0     25850 0 lo
fec0:106:1100::/64               ::       UA    256    8    0 eth0
fec0:106:2700::4/128             ::       U     0    325141 5 lo
fec0:106:2700:0:204:75ff:febc:27b6/128 :: U  0      0    0 lo
ff02::1/128                   ff02::1   UAC    0      3    0 eth0
ff00::/8                         ::       UA    256    0    0 eth0
ff00::/8                         ::       UA    256    0    0 mip6mnha1
fec0:106:2300::1/128  fec0:106:2300::1 UDC   0      4    1 mip6mnha1
fec0:106:2700::1/128  fec0:106:2700::1 UDC   0      3    1 mip6mnha1
::/0                             ::       UD    64     0    0 mip6mnha1
::/0          fe80::204:75ff:febc:24e0 UGDA  1024  12867 2 eth0
```

Após a transição de sub-rede o IPv6 móvel, a tabela muda a rota padrão para o túnel, conforme destacado em negrito. Na transição do essid nota-se uma queda na taxa de transferência do arquivo, mas a conexão não é perdida. Informações exibidas no início do download do arquivo:

```
lftp knoppix@fec0:106:2700::1:~> get wingate.log
'wingate.log' at 26646420 (23%) 588.4K/s eta:3m [Receiving Data]
```

Durante a transição do essid a taxa do download diminui, mas não há uma perda da conexão:

```
lftp knoppix@fec0:106:2700::1:~> get wingate.log
'wingate.log' at 37888670 (33%) 278.7 K/s eta: 2m [Receiving Data]
```

9 Conclusão

Com a progressiva adoção de redes *wireless,* substituindo as redes cabeadas, o tema apresentado neste trabalho torna-se uma ótima referência para entender e utilizar na prática a tecnologia de mobilidade sem fio com o apoio de laboratórios didáticos. Os graves problemas apresentados pela mobilidade no IPv4 e o ainda nebuloso processo de transição para as redes IPv6 podem ser realçados com experimentos de laboratório evidenciando o significado da mobilidade e dos novos conceitos e melhorias oferecidas por este novo protocolo.

Através da elaboração de um material didático adequado e de reduzido impacto para as instalações existentes nos laboratórios das instituições de ensino, o aprendizado torna-se mais rápido e fácilmente absorvido pelos alunos. A inexistência de materiais práticos orientados ao aprendizado do IPv6 Móvel torna o CD modificado do Knoppix, uma ferramenta fundamental de disseminação do conhecimento e de utilização em testes reais, que quando aplicados, tornam as aulas mais interessantes para professores e alunos. O professor através da aplicação de exercícios práticos pode identificar os temas nos quais os alunos têm mais problemas e pode explicar as dúvidas e deficiências com exemplos práticos.

Através dos exercícios didáticos da mobilidade no IPv6, a conexão FTP, a configuração e o comportamento do roteamento confirmam toda a teoria aprendida confirmando a interrupção do download do arquivo, mostando ao aluno na prática como se comporta uma transmissão de arquivos durante a transição de sub-redes e pode acompanhar as alterações de roteamento ocorridas na transição. O roteiro de construção da ferramenta, os laboratórios realizados, complementados pelos trabalhos futuros sugeridos compõem um acervo para a disseminação da tecnologia de mobilidade IPv6 para toda a comunidade acadêmica referenciados no capítulo 8. Este material está compantilhado conforme descrito no anexo deste trabalho e

pode ser feito o download do CD e dos arquivos para se modificar a distribuição a quem deseja se especializar no assunto.

Trabalhos Futuros

Diversos temas podem ser desenvolvidos utilizando-se a plataforma básica apresentada buscando compor um conjunto de atividades práticas voltadas para o ensino de informática e cada tema pode constituir um novo trabalho de conclusão de curso. A titulo de exemplo podem ser citados: criptografia WEP para a comunicação entre todas estações do laboratório; IPSec para criptografar a comunicação entre o nó móvel e o Agente *Home*; QoS na transmissão de vídeo verificando-se o comportamento dos vídeos durante a transição de sub-rede; QoS na transmissão de voz sobre o IP durante a mudança.

Atualizar o CD do Knoppix para a última versão do pacote do IPv6 móvel, atualmente a versão MIPL 2.0 RC1, compatível com *kernel* 2.6.8.1 [17]. Junto com a atualização do *kernel* também deverá ser atualizada a versão do Knoppix, substituindo versão 3.3 utilizada neste trabalho para a versão 3.7 que já está em conformidade com *kernel* 2.6 [18].

Referência Bibliográfica

[1] Gast, M. S., “802.11b Wireless Networks - The definitive guide”, Abril de 2002.

[2] Perkins,C., “IP Mobility Support for IPv4,” RFC 3344, Agosto de 2002.

[3] Knopper, K. , “KNOPPIX - Live Linux Filesystem On CD”; http://www.knopper.net/knoppix/index-en.html, Maio 2004.

[4] IEEE Standards, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, Edição de 1999.

[5] Johnson, D. , Perkins, C. e Arkko, J., “Mobility Support in IPv6”, RFC 3775, Junho de 2004.

[6] Snoeren, A. e Balakrishnan, H. , “An End-to-End Approach to Host Mobility, Proc. ACM MOBICOM, Agosto de 2000, p. 155–66.

[7] Moscowitz, R., “Host Identity Payload and Protocol,” Internet draft, draft-moscowitzhip-05.txt, expirado; http://homebase.htt-consult.com/~hip/ , Novembro de 2001.

[8] Henderson, T.R. ,"Host Mobility for IP Networks: A Comparison", IEEE Network, Novembro/Dezembro de 2003.

[9] Perkins, C., “Mobile IP and the IETF”, Mobile Computing and Communications, Revisão, Volume 6, Número 2, Julho de 2002.

[10] Deering,S.; Hinden, R., “Internet Protocol, Version 6 (IPv6) Specification”, RFC 2460, Dezembro de 1998.

[11] Aura,T. e Nikander, P. , “Stateless Connections,” Proc. ICICS, Novembro de 1997,pg. 87–97.

[12] Bellovin,S. , “EIDs, IPsec, and HostNAT,” Apresentação no 41º encontro do IETF, Los Angeles, CA, Março de 1998.

[13] Awerbuch, B. e Peled, D. , “Concurrent On-Line Tracking on Mobile Users,” Proc. ACM SIGCOMM, Setembro de 1991, p. 221–33.

[14] Arkko, J. e Devarapalli, V. , “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and *Home* Agents”, RFC 3776, Junho de 2004.

[15] Knoppix.net, “Knoppix Remastering Howto”, http://www.knoppix.net/wiki/Main_Page , 22 de Janeiro de 2005.

[16] Stand, L., “Linux Mobile IPv6 HOWTO”, http://www.tldp.org/HOWTO/Mobile-IPv6-HOWTO/, 15 de Abril de 2004.

[17] “MIPL - Mobile IPv6”, http://www.mipl.mediapoli.com/software/, 22 de Fevereiro de 2005.

Glossário

Acknowledge É um caractere de controle de transmissão usado para indicar que uma mensagem transmitida foi recebida com sucesso, sem erros ou que uma estação que está pronta para aceitar transmissões. O receptor envia o código o código para o transmissor indicando que a transmissão foi aceita.

Care-of address É o endereço ip adquirido quando o nó móvel esta fora de sua rede *home*. O endereço adquirido é uma mistura do prefixo da rede visitada com o MAC *address* da placa de rede.

Care-of keygen Um *keygen token* é um número fornecido pelo nó correspondente no procedimento de *return routability*, habilitando o nó móvel a computar o gerenciamento de chaves de *binding*, necessário para a autorização de um *Binding Update*.

Checksum É um simples esquema de detecção de erro na qual cada mensagem transmitida é acompanhada de um valor numérico baseado no número de bits da mensagem. A estação receptora aplica a mesma fórmula para checar a se o número de bits da mensagem recebida é igual da mensagem transmitida.

DSSS Espalhamento de espectro por seqüência direta (*Direct Sequence Spread Spectrum*), é a tecnologia de transmissão onde o sinal da estação de envio é combinado com um bit de seqüência, ou chip, que divide os dados do usuário de acordo com a taxa de espalhamento.

ESP Encapsulamento do *payload* de segurança

	(*Encapsulating Security Payload*), é o mecanismo que provê confiabilidade e proteção de integridade para os datagramas IP.
ESSID	É o nome da rede *wireless*, para haver comunição entre as estações *wireless* eles devem estar no mesmo essid.
FHSS	Espalhamento de espectro por salto de freqüência (*Frequency Hopping Spread Spectrum*), alterna de uma freqüência para outra em um padrão aleatório. Sincronizado corretamente ele mantém um único canal lógico.
Handover L3	Ele acontece quando o nó móvel muda de sub-rede wireless (Camada 3), esta mudança pode ser gerenciada pelo IPv6 móvel.
HR-DSSS	*High Rate* DSSS – DSSS de alta taxa de transmissão
IEEE	Instituto dos Engenheiros Elétricos e Eletrônicos é o órgão responsável pela padronização das redes sem fio.
IETF	Força Tarefa de Engenharia da Internet é um grupo internacional aberto ao público, composto por engenheiros de redes, operadores, fabricantes e pesquisadores concentrados na evolução da arquitetura da Internet.
ISM	Industriais, Científicas e Médicas (*Industrial, Scientific, and Medical*), é a faixa de freqüência que os equipamentos *wireless* operam.
IPSec	Padrão para o transporte seguro do IP, ele é utilizado em túneis de VPN em segmentos de redes roteadas.
Kernel	Núcleo dos sistemas Unix, ele provê os serviços de baixo nível como interação do software com o hardware e gerenciamento de memória.
Octeto	Um octeto são 8 *bits* ou 1 *byte*.
Payload	São os dados essenciais que são transmitidos com um

	pacote or outra unidade de transmissão. O *payload* não inclui os dados adicionais requeridos para entregar o pacote ao destino.
PKI	Infra-estrutura de chave pública é a infra-estrutura necessária para a criptografia de chave pública. Ela requer uma autoridade de certificado para assegurar e verificar as chaves públicas, uma autoridade de registro que verifica a identidade de uma pessoa, um diretório de certificados públicos e um sistema de gerenciamento de certificados. A criptografia de chave pública pode ser utilizada para verificar a identidade ou criptografar dados ou mensagens.
PPP	Este é o padrão para conexões dial-up através de modems.
Ponto de acesso	Equipamento capaz de conectar redes com fio a equipamentos *wireless* permitindo que estes funcionem no modo de infra-estrutura aumentando o seu alcance.
RADIUS	(***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice*) É um sistema de autenticação de contas onde o usuário disca para um provedor e digita login e senha, validados pelo RADIUS.
Remasterizar	Processo de modificação da estrutura do Knoppix e a sua montagem em um CD para a utilização.
RC4	RC4 é um sistema de criptografia desenvolvido pela *RSA Security*. Um fluxo de cifras com chaves de tamanhos variáveis e operação orientada a *bytes*. O algoritmo é baseado em permutação aleatória.
Shell	Sessão para entrada de comandos via texto do linux.
Sniffing	Ataque a uma rede em que um programa monitora o tráfego e captura dados não autorizados.
SSH	Shell Seguro é um programa que se loga em outro computador através da rede e executa comandos na

	máquina remota e transfere arquivos de um máquina para a outra.
VPN	É uma rede privada conectada a uma rede pública utilizada para transmitir informações usando métodos seguros de criptografia.
WPA	(***Wireless P****rotected* ***A****ccess*) Ele foi desenvolvido para suprir as falhas do WEP, através da criptografia dos dados utilizando um protocolo de integridade de chave temporária (TKIP- *Temporal Key Integrity Protocol*) e uma autenticação de usuário.

Anexo 1 - Mobile IPv4

1.1 Novas entidades arquiteturais

O IP móvel introduz as seguintes entidades arquiteturais:

Nó Móvel

Um host ou um roteador que muda o seu ponto de acesso de uma rede ou sub-rede para outra. Um nó móvel pode mudar a sua localização sem mudar o seu endereço IP.

Agente Home

É um roteador na rede *home* de um nó móvel que tunela datagramas para serem entregues ao nó enquanto ele estiver ausente de sua rede *home*, e mantém a informação da posição atual do nó móvel.

Agente Estrangeiro

É um roteador na rede visitada pelo nó móvel que fornece serviços de roteamento ao nó móvel enquanto ele está registrado. Os agentes estrangeiros destunelam e entregam os datagramas do nó móvel que foram tunelados pelo agente *home* do nó móvel.

Um nó móvel possui um endereço IP em sua rede *home*. Este endereço *home* é administrado da mesma maneira que um IP "permanente", o endereço é fornecido a um host estacionário. Quando ele está afastado de sua rede *home*, um *care-of address* é associado com o nó móvel e reflete o ponto de localização do nó móvel. O nó móvel usa o seu endereço *home* como o endereço de origem de todos os datagramas IP que são enviados [2].

Outros termos:

Extensão de habilitação da autorização

Uma autenticação que faz uma mensagem aceitável ao último receptor da mensagem de registro.

Agent Advertisement

Uma mensagem de anúncio é construída anexando uma extensão especial a uma mensagem de anúncio do roteador.

Autenticação

O processo de verificação da identidade do emissor de uma mensagem.

Care-of Address

O ponto de término de um túnel para um nó móvel, para datagramas enviados a um nó móvel enquanto ele estiver ausente de sua *home*. O protocolo pode usar dois tipos diferentes de *care-of address*: "*care-of address* de um agente estrangeiro" é um endereço de um agente estrangeiro no qual o nó móvel está registrado, e um "*care-of address* co-localizado" é um endereço local obtido externamente na qual o nó móvel associou-se com um endereço de sua própria interface de rede.

Nó Correspondente

Uma estação na qual um nó móvel está comunicando. Um nó correspondente pode ser móvel ou estacionário.

Rede Estrangeira

Alguma rede, a exceção da rede *home* do nó móvel.

Gratuitous ARP

Um pacote ARP enviado por um nó que faz que os outros nós atualizem seu *cache* ARP.

Endereço Home

Um endereço IP que é atribuído por um longo período de tempo ao nó móvel.

Agente de Mobilidade

Um agente *home* ou um agente estrangeiro.

Binding de mobilidade

A associação de um endereço *home* com o *care-of address*, junto com o tempo de vida restante desta associação.

Associação de segurança da mobilidade

Uma coleção de contextos de segurança, entre um par de nós, que pode ser aplicada às mensagens de protocolo do IP móvel, trocadas entre elas. Cada contexto indica um algoritmo de autenticação e modalidade.

Nonce

Um valor aleatório, diferente das escolhas anteriores, introduzido para evitar a repetição das mensagens.

Índice Do Parâmetro De Segurança (SPI)

Um índice que identifica um contexto de segurança entre um par de nós entre os contextos disponíveis na associação da segurança da mobilidade.

Túnel

O trajeto percorrido por um datagrama enquanto ele está encapsulado. O datagrama é distribuído a um agente, que o desencapsula e entrega-o ao seu destino.

Lista Do Visitante

A lista dos nós móveis que estão visitando um agente estrangeiro.

Overwiew do Protocolo

Os seguintes serviços são definidos no IP móvel:

Agent Discovery

Os agentes *home* e os agentes estrangeiros podem anunciar a sua disponibilidade em cada *link* para fornecer o serviço. Um nó móvel pode enviar uma solicitação no *link* para saber se algum agente potencial está presente.

Registro

Quando o nó móvel está ausente de sua *home*, ele registra o seu *care-of address* com o seu agente *home*. Dependendo do método de acesso, o nó móvel registrará qualquer um diretamente com seu agente *home*, ou através de um agente estrangeiro que envia o registro ao agente *home*.

Descarte Silencioso

A implementação do IP móvel rejeita o datagrama sem processamento adicional e não indica um erro ao remetente. A implementação deve registrar o erro em logs, incluindo os índices de datagramas descartados, e deve gravar o evento em um contador.

1.2 *Agent Discovery*

O Agent Discovery é o método pelo qual um nó móvel determina se está conectado ou não na sua rede *home* ou a uma rede estrangeira e também permite ao nó móvel detectar se ele moveu-se de uma rede para outra.

O IP móvel utiliza o ICMP *Router Discovery* como o mecanismo primário para o *Agent Discovery*. Um *Agent Discovery* é formado pela inclusão da extensão do *Mobility Agent Advertisement* em uma mensagem ICMP *Router Advertisement*. Uma mensagem de *Agent Solicitation* é idêntica a uma ICMP *Router Solicitation*, exceto que o *time to live*(TTL) do IP deve estar ajustado para 1 [2]. Nenhuma autenticação é requerida para as mensagens *Agent Advertisement* e *Agent Solicitation*.

1.3 *Agent Advertisement*

Os *Agent Advertisement* são transmitidas por um agente de mobilidade que anuncia seus serviços em um *link*. Os nós móveis usam estas propagandas para determinar a sua posição atual na rede. O *Agent Advertisement* é um ICMP *Router Advertisement* que tem sido estendido para transmitir também um *Mobility Agent Advertisement Extension*, opcionalmente uma extensão do tamanho de prefixo e uma extensão de um *bit* de *padding*.

1.4 *Agent Solicitation*

Um *Agent Solicitation* é idêntico a um ICMP *Router Solicitation* com uma limitação em que o campo TTL (*time to live*) do IP deve ser ajustado para 1.

1.5 Detecção de Movimento

Dois mecanismos são fornecidos para que os nós móveis possam detectar quando eles se movem de uma sub-rede para outra [2].

1.5.1 Algoritmo 1

O primeiro método da detecção do movimento é baseado no campo de tempo de vida (TTL) do ICMP *Router Advertisement* em parte do *Agent Advertisement*. Um nó móvel deve gravar o tempo de vida recebido em todos *Agent Advertisements*, até este tempo de vida expirar.

Se o nó móvel tiver recebido um *Agent Advertisement* de um outro agente na qual o tempo de vida não expirou ainda, o nó móvel pode registrar-se em outro agente *home*, se não, o nó móvel precisa descobrir um novo agente *home*.

1.5.2 Algoritmo 2

O segundo método usa prefixos da rede. As extensões do tamanho do prefixo podem ser usadas em alguns casos por um nó móvel para determinar se um novo *Agent Advertisement* é recebido da mesma subnet do *care-of address* do nó. Se os prefixos forem diferentes, o nó móvel pode supor que ele se moveu. Se o nó móvel está usando um *care-of address* de um agente estrangeiro o nó móvel não deve usar este método de detecção do movimento a menos que o agente atual e o novo agente incluam as extensões de tamanho dos prefixos em seus respectivos *Agent Advertisements*.

1.5.3 Retornando para a *home*

Um nó móvel pode detectar que retornou a sua rede *home* quando ele recebe um *Agent Advertisement* de seu próprio agente *home*. Assim ele deve cancelar o registro com o seu agente *home*.

1.6 Registro

O registro do IP móvel habilita aos nós móveis a capacidade de comunicar a sua atual informação de alcançabilidade para o seu agente *home*. Este é o método pelo qual os nós móveis:

- Solicitam serviços de reenvio enquanto estão visitando uma rede estrangeira.

- Informam ao seu agente *home* o seu atual *care-of address*.
- Renovam um registro após a sua expiração.
- Cancelam o registro quando retornam para a rede *home*.

As mensagens de registro trocam informações entre um nó móvel, um agente estrangeiro (opcionalmente) e um agente *home*. O registro cria ou modifica o *binding* de mobilidade no agente *home*, associando o endereço *home* do nó móvel com o seu *care-of address* para um tempo de vida específico.

1.6.1 Overview do Registro

O IP móvel define dois procedimentos de registro, um através de um agente estrangeiro que restabelece o registro para agente *home* do nó móvel, e um diretamente com o agente *home* do nó móvel. As seguintes regras determinam qual destes dois procedimentos de registro deve-se utilizar:

- Se um nó móvel está registrando um *care-of address* de um agente estrangeiro, o nó móvel deve registrar-se através desse agente estrangeiro.
- Se um nó móvel estiver usando *care-of address* co-localizado, e recebe um *Agent Advertisement* de um agente estrangeiro no *link* na qual ele está usando este *care-of address*, o nó móvel precisa registrar-se através desse agente estrangeiro se o bit 'R' estiver setado na mensagem *Agent Advertisement* recebida.
- Se um nó móvel está usando um *care-of address* co-localizado, o nó móvel deve registrar diretamente com o seu agente *home*.

Todos procedimentos de registro envolvem a troca de mensagens *Registration Request* e *Registration Reply* (figura 16). Quando o registro ocorre através de um agente estrangeiro, têm-se as seguintes mensagens:

Figura 15 Troca de mensagens do procedimento de registro.

Fonte: C. Perkins, Ed., "IP Mobility Support for IPv4," RFC 3344, Agosto de 2002.

a) O nó móvel envia um *Registration Request* para um possível agente estrangeiro para começar o processo de registro.
b) O agente estrangeiro processa o *Registration Request* e então ele retransmite ao agente *home*.
c) O agente *home* envia um *Registration Reply* ao agente estrangeiro para conceder ou negar o pedido.
d) O agente estrangeiro processa o *Registration Reply* e então retransmite ao nó móvel para informar a sua posição neste pedido.

Quando o nó móvel registra-se diretamente com seu agente *home*, o procedimento de registro possui as mensagens mostradas na figura 16:

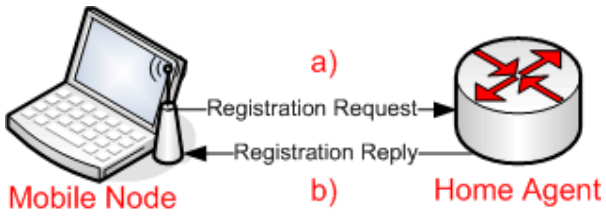

Figura 16 Registro direto do Mobile Node com o Agente *home*.

Fonte: C. Perkins, Ed., "IP Mobility Support for IPv4," RFC 3344, Agosto de 2002.

a) O nó móvel emite um *Registration Request* ao agente *home*.
b) O agente *home* emite um *Registration Reply* ao nó móvel, concedendo ou negando o pedido.

As mensagens do registro usam o *User Datagram Protocol* (UDP).

1.7 Autenticação

Cada nó móvel, agente estrangeiro e agente *home* devem ser capazes de suportar uma associação de segurança da mobilidade para entidades móveis, posicionada por seus SPI e endereços IP. As mensagens de registro entre um nó móvel e seu agente *home* devem ser autenticadas com uma extensão de autenticação.

1.7.1 Pedido de Registro (*Registration Request*)

Um nó móvel realiza o registro com seu agente *home* usando uma mensagem de *Registration Request* para que o seu agente *home* possa criar ou modificar o *binding* de mobilidade para aquele nó móvel. O pedido pode ser transmitido ao agente *home* pelo agente estrangeiro na qual o nó móvel está registrando, ou pode ser enviado diretamente para o seu agente *home* no caso em que o nó móvel estiver registrado um *care-of address* co-localizado.

1.7.2 Resposta do Registro (*Registration Reply*)

Um agente de mobilidade retorna uma mensagem *Registration Reply* a um nó móvel que enviou uma mensagem de *Registration Request*. Se o nó móvel está pedindo um serviço de um agente estrangeiro, este agente receberá a resposta do agente *home* e subseqüentemente a retransmissão ao nó móvel. A mensagem da resposta contém os códigos necessários para informar ao nó móvel o status do seu pedido, junto com o tempo de vida concedido pelo agente *home*, que pode ser menor que o pedido original.

Se o tempo de vida recebido no *Registration Reply* é maior que o *Registration Request*, o tempo de vida no pedido deve ser utilizado. Quando o tempo de vida recebido do *Registration Reply* for menor do que o *Registration Request*, o tempo de vida na resposta deve ser utilizado.

Anexo 2 - Mobile IPv6

2.1 Procedimento de *Return Routability*

O procedimento de *Return Routability* permite que o nó correspondente obtenha alguma garantia razoável e que o nó móvel esteja de fato endereçável no seu invocado *care-of address* assim como em seu endereço *home*.

Isto é feito testando-se os pacotes endereçados aos dois endereços distribuídos ao nó móvel. O nó móvel pode passar o teste somente se puder fornecer a prova de que recebeu os dados certos (*keygen tokens*) na qual o nó correspondente emite estes endereços. Estes dados são combinados pelo nó móvel na chave de gerenciamento *binding* (Kbm).

A figura 17 mostra o fluxo da mensagem para o procedimento de *return routability*.

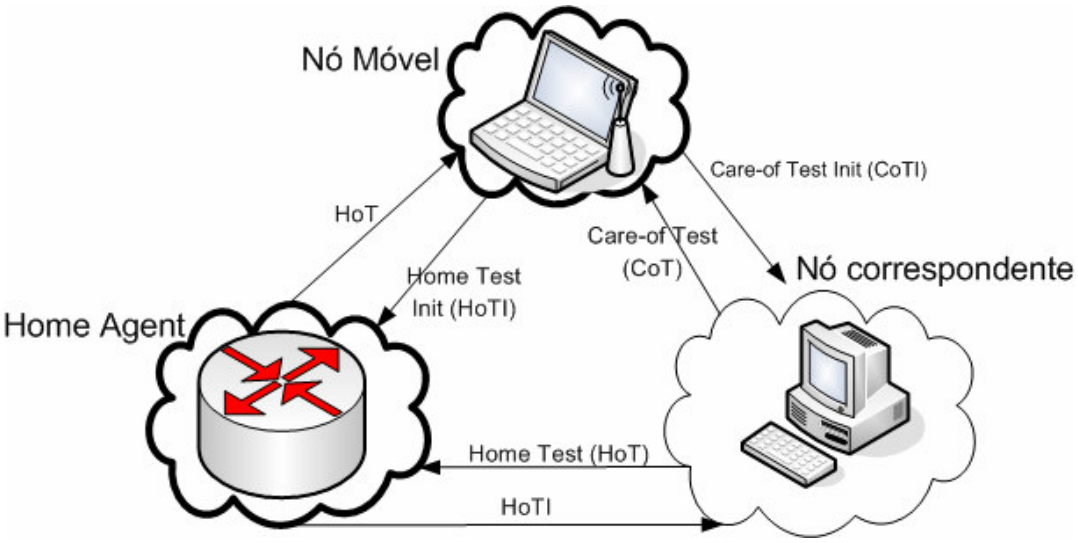

Figura 17 Fluxo da mensagem para o procedimento de return routability.

Fonte: D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", RFC 3775, Junho de 2004.

As mensagens *Home e Care-of Test Init* são enviadas ao mesmo tempo. O procedimento requer muito pouco processamento no nó correspondente, e as mensagens *Home e Care-of Test* podem ser retornadas rapidamente, quase simultaneamente. Estas quatro mensagens formam o procedimento de *return routability*.

- *Home Test Init*

Um nó móvel envia uma mensagem *Home Test Init* ao nó correspondente (através do agente *home*) para adquirir o *home keygen token*.

- *Care-of Test Init*

O nó móvel envia a mensagem *Care-of Test Init* ao nó correspondente (diretamente, não através do agente *home*) para adquirir o *care-of keygen token*.

- *Home Test*

A mensagem *Home Test* é emitida em resposta a mensagem *Home Test Init*. É emitida através do agente *home*.

- *Care-of Test*

Esta mensagem é enviada em resposta a informação *Care-of Test Init*. Esta mensagem não é enviada através do agente *home*, ela é enviada diretamente ao nó móvel.

2.2 Descoberta do prefixo móvel

O nó móvel e o agente *home* devem usar uma associação de segurança IPsec para proteger a integridade e a autenticidade da solicitação de prefixos móveis e anúncios. Os nós móveis e os agentes *home* devem suportar e usar o cabeçalho de encapsulamento do *payload* de segurança

(*Encapsulating Security Payload* - ESP) na modalidade de transporte com um algoritmo de autenticação do *payload* não nulo, para fornecer a autenticação da origem de dados, integridade da conexão e proteções opcionais *anti-replay*.

O cabeçalho de mobilidade é um cabeçalho de extensão usado por nós móveis, nós correspondentes, e agentes *home* em todas mensagens relacionadas à criação e gerenciamento de *bindings*.

2.2.1 Formato

O cabeçalho de mobilidade, figura 18, tem o seguinte formato:

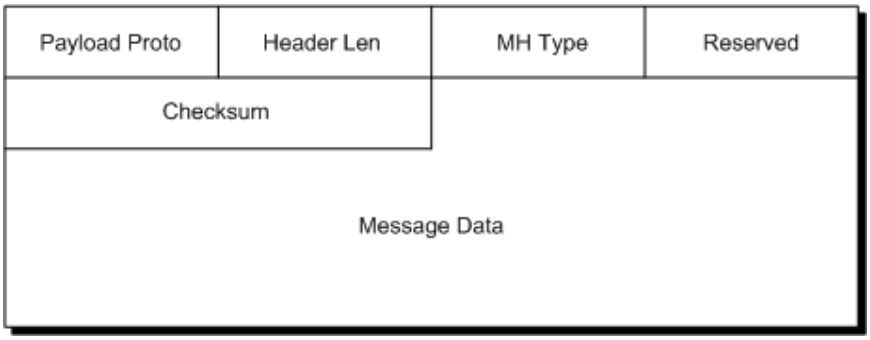

Figura 18 Cabeçalho de mobilidade.

Fonte: D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", RFC 3775, Junho de 2004.

Payload Proto

Um seletor de 8-bit. Identifica o tipo de cabeçalho após o cabeçalho de mobilidade.

Header Len

É um inteiro não assinado de 8-bit, representando o comprimento do cabeçalho de mobilidade em unidades de 8 octetos, excluindo os primeiros 8 octetos.

MH Type

Seletor de 8-bit. Identifica a mensagem particular da mobilidade em questão.

Reserved

Campo de 8-bit reservado para uso futuro.

Checksum

Inteiro não assinado de 16-bit. Este campo contém a soma de controle do cabeçalho da mobilidade. A soma de controle é calculada de um octeto de string consistindo de um "pseudo-header" seguido pelo cabeçalho de mobilidade começando com o campo *Payload Proto*. O *checksum* é um complemento de 16-bit de uma soma de complemento destra string.

Message Data

É um campo de comprimento variável que contém os dados específicos para o tipo indicado no cabeçalho de mobilidade.

2.3 Operação do Agente *Home*

Cada agente *home* deve manter um *Binding Cache* e uma lista de agentes *home*. A lista de agentes *home* é mantida por cada agente *home*, gravando informação sobre cada roteador no mesmo *link* que está atuando como um agente *home*, esta lista é usada pelo mecanismo de *home* agent address discovery. Um roteador sabe atuar como um agente *home*, se ele envia um *Router Advertisement* o bit de agente *home* é habilitado. Quando o tempo de vida para a lista de entrada expira, esta entrada é removida da lista de agentes *home*. As listas dos agentes *home* são similares às estruturas dos dados conceituais da lista padrão do roteador mantida por cada host para o *Neighbor Discovery* [5].

Cada agente *home* mantém uma lista separada de agentes *home* para cada *link* que serve um agente *home*. Cada entrada da lista de agente *home* contém os seguintes campos:

- O endereço IP do *link* local de um agente *home* no *link*.
- Um ou mais endereços globais de IP para este agente *home*.
- O tempo de vida máximo restante desta entrada da lista de agente *home*.
- A preferência para este agente *home*, altos valores indicam a preferência por este agente *home*.

2.4 Operação do nó móvel

Cada nó móvel deve manter uma lista de *Binding Update* e a informação de registros da lista de *Binding Update* para cada *Binding Update* enviado pelo nó móvel. A lista de *Binding Update* inclui todos os *binding* enviados pelo nó móvel a seu agente *home* ou ao nó correspondente.

Cada entrada da lista conceitual de *Binding Update* contém os seguintes campos:

- O endereço IP do nó de um *Binding Update* que foi enviado.
- O endereço *home* na qual este *Binding Update* foi enviado.
- O *care-of address* enviado neste *Binding Update*.
- O valor inicial do campo de tempo de vida enviado neste *Binding Update*.
- O tempo de vida restante deste *binding*.
- O valor máximo do campo de número de seqüência emitido em precedente *Binding Update* para este destino.
- O tempo em que um *Binding Update* foi enviado por último a este destino, quando necessário, para implementar a taxa que limita a restrição para enviar *Binding Updates*.

- O estado de qualquer retransmissão necessária para este *Binding Update*.

A lista de *Binding Update* é usada para determinar se um determinado pacote é enviado diretamente ao nó correspondente ou tunelado através do agente *home*.

2.5 Movimento

2.5.1 Detecção do Movimento

A detecção genérica do movimento usa o *Neighbor Unreachability Detection* para detectar quando o roteador padrão não for mais alcançável bidirecionalmente, que no caso do nó móvel deve descobrir um novo roteador padrão (geralmente em um novo *link*). Entretanto, esta detecção ocorre somente quando o nó móvel tiver pacotes para enviar, o nó móvel pode tornar-se inconsciente de um *handover L3* que ocorreu. Conseqüentemente, o nó móvel deve suplementar este método com outra informação sempre que estiver disponível.

Devido ao rompimento provisório do fluxo de pacotes e a sinalização de overhead em *bindings* de atualizações da mobilidade, o nó móvel deve evitar executar um handover L3 até que isto seja estritamente necessário. Especificamente, quando o nó móvel recebe um *Router Advertisement* de um novo roteador que contém um conjunto diferente de prefixos. Se o nó móvel detectar que o atual roteador padrão selecionado do *link* antigo é ainda alcançável bidirecionalmente ele deve continuar a usar o roteador antigo no *link* antigo, esta opção é melhor do que usar um novo roteador padrão.

2.5.2 Criando os novos *Care-of Addresses*

Um nó móvel pode dar forma a um não primário *care-of addresses* mesmo quando não tem comutado um novo roteador padrão. Um nó móvel pode ter somente um *care-of address* ao mesmo tempo (que é registrado

com o seu agente *home*), mas ele pode ter um adicional *care-of address* para quaisquer prefixos em seu *link* atual. Além disso, desde que uma interface wireless pode realmente permitir ao nó móvel ser alcançável em mais de um *link*, um nó móvel pode ter um *care-of addresses* em mais de um *link* de cada vez.

2.5.3 Usando o múltiplo *Care-of Addresses*

Um nó móvel pode usar mais de um *care-of addresses* em um determinado momento [5]. Particularmente no exemplo de muitas redes wireless, um nó móvel eficaz pode ser alcançável completamente em muitos *links* ao mesmo tempo (por exemplo, com a sobreposição de células wireless), nas quais diferentes prefixos de subredes podem existir. O nó móvel deve assegurar-se de que seu *care-of address* primário tenha sempre o prefixo que é válido no *link* do seu roteador padrão atual. Após ter selecionado um novo *care-of address* primário, o nó móvel deve emitir um *Binding Update* que contém o *care-of address* do seu agente *home*. O *Binding Update* deve ter o *home registration* (H) e os bits de reconhecimento (A) são ajustados em seu agente *home*.

Um nó móvel deve reter o seu preliminar precedente *care-of address*, como um (não-primário) *care-of address*, e deve ainda aceitar pacotes neste endereço, mesmo depois do seu novo registro preliminar do seu novo *care-of address* com seu agente *home*. Isto é aceitável desde que o nó móvel possa somente receber pacotes do seu preliminar *care-of address* se estiver conectado em seu *link*. Se o preliminar *care-of address* for alocado usando o autoconfiguração *stateful* do endereço, o nó móvel não pode liberar o endereço imediatamente após trocar para o novo *care-of address* primário.

Sempre que um nó móvel determinar que não está mais disponível em um *link*, ele deve invalidar todos *care-of addresses* associados com os prefixos do endereço que são dos roteadores do *link* inalcançável que não estão no atual conjunto de prefixos de endereços anunciados pelo novo roteador padrão.

3 Knoppix com IPv6 móvel na internet

Este trabalho está disponível na Internet no *website* http://www.geocities.com/fabioxa, neste endereço o internauta tem acesso a todas informações para montar o laboratório didático com instruções detalhadas. O site foi escrito no idioma Inglês para facilitar a disseminação do trabalho para todos os interessados no assunto. No site o internauta pode fazer o download do arquivo iso principal que é o knoppix-mipv6.iso, após o download deste arquivo o CD pode-se gravar um CD, criar o disquete com os arquivos de configuração do IPv6 móvel. No site há muitas referências sob o material usado como fonte de trabalho deste tema, o internauta pode ter acesso a mais detalhes sobre os assuntos abordados.

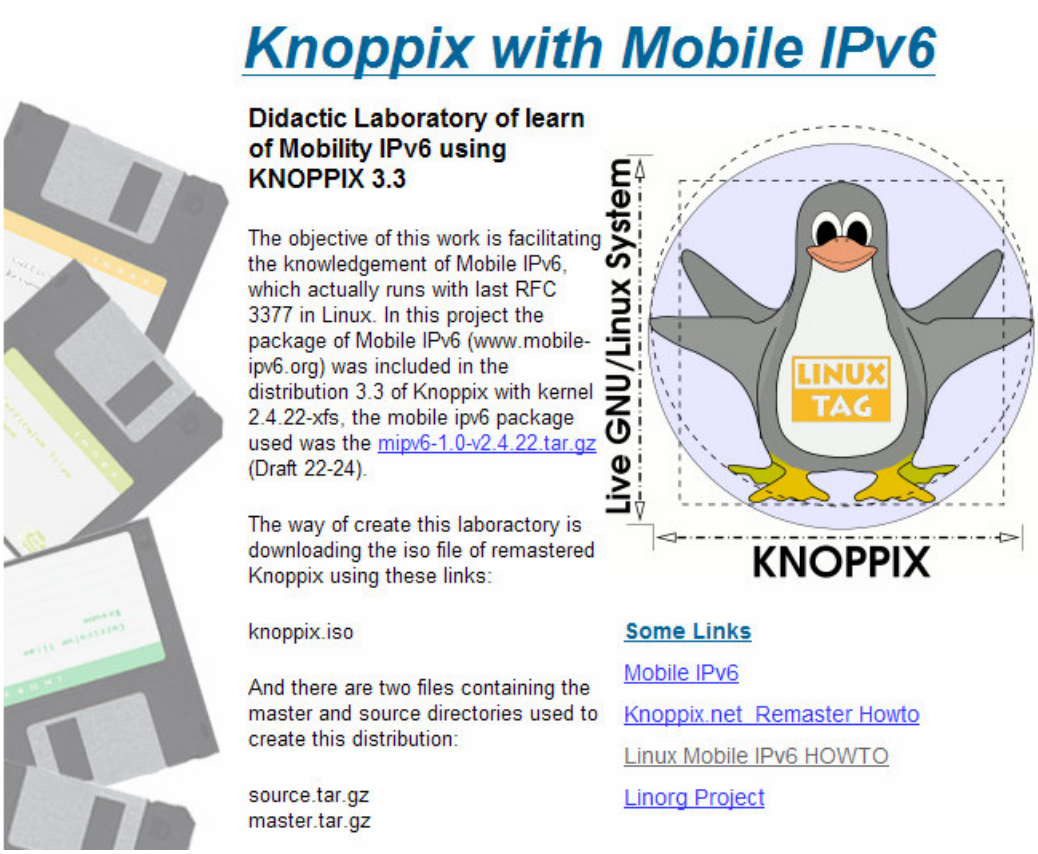

Figura 19 Mobile Ipv6 website http://www.geocities.com/fabioxa