Mecanismos de Transição para Implementar a Comunicação IPv4/IPv6 em Redes Móveis

Simone Storoz [*] [1] e Edgard Jamhour

Resumo—**Neste artigo, uma visão geral dos mecanismos de transição IPv4/IPv6 publicados é apresentada, e, um novo mecanismo é proposto, o "Transparent IPv6", que permite designar "virtualmente" endereços IPv6 para hosts IPv4 sem modificações de hardware ou software no host. Este mecanismo pode ser imediatamente empregado pelas tecnologias celulares IP Móvel.**

***Palavras-Chave*—IPv6, Mecanismos de Transição IPv4/IPv6, Endereços IP Privados, NAT, Redes Sem Fio.**

Abstract— This paper reviews the IPv4/IPv6 transition mechanisms published by IETF and proposes a new mechanism called "Transparent IPv6", which permits to "virtually" assign IPv6 addresses to IPv4 hosts without hardware or software modifications on the host. This mechanism can be employed by cellular technologies based on Mobile IP, as a possible solution for the IPv4-shortage problem.

***Index Terms*—IPv6, IPv4/IPv6 Transition Mechanisms, Private IP Addresses, NAT, Wireless Networks.**

I. INTRODUÇÃO

Neste artigo, abordamos a questão da implementação de IP Móvel [1] em redes celulares utilizando endereços IP privados. Esta questão tornou-se particularmente importante porque operadoras de redes celular de todo mundo têm adotado a tecnologia IP Móvel. Pode-se encontrar implementações de IP Móvel em soluções industriais aceitas mundialmente, tais como GPRS [2] e iDEN [3]. No entanto, essas implementações precisam considerar o problema da carência de endereços IP versão 4 (IPv4). O uso de endereços IPv4 privados [4] tem sido considerado uma solução temporária para o problema da carência de endereços IPv4 até que um novo esquema de endereçamento, como o protocolo IPv6, possa ser adotado [5]. Endereços IP privados não podem ser considerados uma solução final porque eles não são publicamente endereçáveis. Um host com um endereço IPv4 privado pode iniciar uma sessão com um host externo que possui um endereço IPv4 público, através de um mecanismo de tradução de endereços tal como *Network Address Translation* (NAT), porém o contrário não é viável [6].

O protocolo IPv6 resolve este problema oferecendo um espaço de endereçamento virtualmente ilimitado. No entanto, é necessário que exista um período de transição que permita os hosts IPv4 e IPv6 coexistirem e se comunicarem. Por esta razão, o IETF publicou recentemente um conjunto importante de mecanismos que permitem hosts IPv6 se comunicarem através de uma infraestrutura IPv4 existente, ou, ainda, permitem a comunicação entre hosts IPv4 e IPv6. Estes mecanismos são conhecidos como "*Transition Mechanisms*" [7]. Uma visão geral dos mecanismos publicados pelo IETF é apresentada neste artigo. Então, um novo mecanismo é proposto, com o intuito de combinar as características mais importantes dos mecanismos existentes. Este mecanismo permite designar "virtualmente" endereços IPv6 para hosts IPv4 sem que seja necessário efetuar mudanças de hardware ou software no host. O mecanismo é baseado na introdução de um gateway transparente na fronteira das redes privadas. Este mecanismo é chamado neste artigo de *Transparent IPv6* (TIP6, de forma abreviada). A idéia principal é prover os benefícios do endereçamento IPv6 minimizando as mudanças na infraestrutura IPv4 existente. De fato, este mecanismo pode ser imediatamente empregado pelas tecnologias celulares IP Móvel.

Embora o mecanismo TIP6 utilize técnicas similares às empregadas pelos mecanismos de transição, ele foca um aspecto diferente. A idéia principal não é permitir que um host IPv4 possa se comunicar com um host IPv6, mas permitir que dois hosts IPv4 com endereços IP privados possam se comunicar através da Internet. Para estes hosts, o uso do protocolo IPv6 é completamente transparente, como já indica o nome *Transparent IPv*6. O mecanismo TIP6 estende implementações de NAT padrão permitindo que um host IPv4 privado de uma rede TIP6 receba conexões de hosts IPv4 públicos, a partir de outras redes TIP6 ou a partir de hosts IPv6 "verdadeiros". Por este motivo, o TIP6 pode também ser considerado um mecanismo de transição, porque ele também permitirá a coexistência das implementações IPv6 emergentes com as redes IPv4 existentes.

Neste artigo, a Seção 2 revisa alguns conceitos relacionados ao uso de endereços IP privados em redes com IP Móvel. A Seção 3 apresenta uma visão geral dos mecanismos de transição IPv4/IPv6 publicados. A Seção 4 apresenta os conceitos necessários para introduzir o mecanismo TIP6. A Seção 5 finalmente apresenta o mecanismo TIP6. A Seção 6 apresenta o emprego do *Transparent IPv6* em redes sem fio. A conclusão sugere que o mecanismo pode ser

[*] Simone Storoz e Prof. Dr. Edgard Jamhour, Programa de Pós-Graduação em Informática Aplicada, Pontifícia Universidade Católica do Paraná, Curitiba, Brasil, e-mails: simones@ppgia.pucpr.br, jamhour@ppgia.pucpr.br.

[1] Aluna do Mestrado em Informática Aplicada da PUCPR. Candidata à premiação como aluno.

imediatamente agregado as tecnologias celulares IP Móvel, compara o mecanismo *Transparent IPv6* com os mecanismos existentes e sugere desenvolvimentos futuros.

II. Endereços Privados em Redes Móveis

Endereços IP privados são definidos pela RFC 1918 [4]. Hosts com endereços IP privados podem trocar informações com outros hosts conectados à Internet somente utilizando um tradutor de endereços IP como Proxy ou NAT *(Network Address Translatio*n) [8]. Atualmente, muitas redes celulares operam utilizando endereços IPv4 privados. Endereços IPv4 privados podem ser utilizados sem restrição para desenvolvimento de serviços WAP [9], por exemplo, porque o gateway WAP pode agir como um Proxy clientes móveis. No entanto, WAP não é o único serviço de dados por pacotes que podem ser desenvolvidos sobre uma rede celular. Aplicações que utilizam o aparelho celular como um modem para computadores portáteis e as aplicações embarcadas como J2ME, por exemplo, necessitam de um outro mediador para acessar a Internet como NAT ou Proxy.

Quando utilizamos endereços IP privados com NAT ou Proxy precisamos considerar que todos os hosts móveis aparecerão para os outros hosts da Internet como sendo o "mesmo computador", isto porque eles utilizarão o mesmo endereço IP. Portanto, hosts com endereços IP privados não podem ser utilizados como servidores, porque não existe caminho para iniciar a comunicação com eles. Uma das soluções propostas pelo IETF para contornar esse problema é NAT Bidirecional [10]. O NAT Bidirecional é utilizado em conjunto com uma extensão DNS, implementada como um *DNS Application Level Gateway* (DNS_ALG) [11]. Neste mecanismo, os hosts com endereços IPv4 privados são identificados com *Fully Qualified Domain Names* (FQDN). Quando um host externo pesquisa um nome de host em uma rede privada, o DNS_ALG inicia uma sessão NAT no NAT Bidirecional, mapeando um endereço IPv4 público para o host privado. Este endereço IPv4 público mapeado é retornado para o host externo. Deve-se notar, no entanto, que o NAT Bidirecional requer um bloco de endereços IPv4 públicos para serem mapeados dinamicamente. Esta solução não provê endereçamento bidirecional para um número muito grande de hosts IPv4, mas somente para um número de hosts selecionados que requerem ser endereçados externamente. Dessa forma, o endereçamento de hosts com endereços IPv4 privados, em redes de grande porte, continua sendo um problema em aberto.

III. Mecanismos de Transição

Endereços do Protocolo de Internet Versão 6 (IPv6) [5,12] podem ser vistos como uma alternativa à utilização de endereços IP privados. O protocolo IPv6 permite endereçar um número virtualmente ilimitado de hosts através de um espaço de endereçamento de 16 bytes. Porém, os protocolos IPv4 e IPv6 são incompatíveis. O emprego de IPv6 requer que mudanças sejam efetuadas na infraestrutura existente, incluindo equipamentos de rede e usuários finais. Para permitir um emprego imediato de IPv6 sobre a infraestrutura IPv4 existente, mecanismos de transição podem ser empregados [7]. Estes mecanismos de transição permitem que ambos protocolos IPv4 e IPv6 possam interoperar sem que grandes mudanças sejam necessárias na infraestrutura de rede existente. Porém, ainda não existem mecanismos de transição que possam ser utilizados em qualquer situação, ou seja, não existe mecanismo de transição que resolva todos os problemas de compatibilidade entre IPv4 e IPv6. Cada mecanismo de transição busca resolver questões específicas de transição. Em muitas situações, mais do que um mecanismo de transição precisa ser utilizado para permitir uma comunicação adequada entre hosts e roteadores IPv4 e IPv6 [13].

Para facilitar a apresentação dos mecanismos de transição neste artigo, eles foram classificados em quatro categorias: Mecanismos Baseados em Pilha Dupla, Mecanismos Baseados em Gateway Transparente, Mecanismos Baseados em Gateways de Camadas Superiores e Mecanismos Baseados em Tunelamento. A seguir, é apresentado um resumo de cada categoria de mecanismos.

A. *Mecanismos Baseados em Pilha Dupla*

Os mecanismos baseados em pilha dupla provêem suporte a ambos protocolos: IPv4 e IPv6 em hosts e roteadores. Pela seleção da API apropriada, a aplicação escolhe a pilha IPv6 ou IPv4 para a comunicação de rede. Isso requer que as aplicações IPv4 existentes sejam reescritas utilizando a API IPv6 para poderem acessar a pilha IPv6. Para resolver este problema, duas soluções foram propostas. A primeira é chamada de *Bump-in-the-Stack* (BIS) [14]. O mecanismo BIS permite que as aplicações IPv4 se comuniquem com aplicações IPv6 através de um tradutor integrado ao host com pilha dupla. Este tradutor é responsável por traduzir os cabeçalhos dos pacotes IPv4 em IPv6 e vice-versa. O mecanismo de tradução de cabeçalhos utilizado pelo BIS é baseado no SIIT [15]. A tradução ocorre quando um servidor DNS responde uma pesquisa efetuada pela aplicação IPv4 com um "registro AAAA". Quando o servidor DNS responde com um "registro A" a tradução não ocorre. Recentemente, um mecanismo similar chamado *Bump-in-the API* (BIA) [16] foi publicado como um *IETF Internet Draft*. O objetivo do mecanismo é semelhante ao do mecanismo BIS, porém ao invés de efetuar a tradução de cabeçalhos, o BIA provê um método de tradução entre APIs IPv4 e APIs IPv6. Um terceiro mecanismo chamado DSTM *(Dual Stack Transition Mechanis*m) [17] foca um aspecto diferente. Ele permite que hosts com pilha dupla conectados a redes IPv6 se comuniquem com hosts IPv4 da Internet. Isto é feito empregando uma técnica de tunelamento 4sobre6 que encapsula pacotes IPv4 em payloads de pacotes IPv6. Os pacotes são enviados para um gateway DSTM, localizado na fronteira da rede IPv6, que desencapsula os pacotes IPv4 e os envia para a Internet. No mecanismo DSTM, os endereços

IPv4 não são permanentemente alocados para os hosts com pilha dupla, estes somente recebem endereços IPv4 temporários quando necessitam se comunicar com hosts IPv4. Esta alocação de endereços IPv4 temporários para os hosts com pilha dupla é feita por um servidor DSTM.

B. Mecanismos Baseados em Gateways Transparentes

Mecanismos de transição baseados em gateways transparentes são similares ao NAT convencional. Porém, ao invés de mapear endereços privados em endereços públicos, eles mapeiam endereços IPv4 em IPv6. Esta abordagem permite a interconexão entre hosts IPv4 e IPv6 sem que seja necessário efetuar a instalação de algum programa específico no host cliente. Os mecanismos NAT-PT *(Network Address Translation - Protocol Translatio*n) e NAPT-PT *(Network Address and Port Translation - Protocol Translatio*n) podem ser citados como mecanismos que integram esta categoria [18]. Ambos habilitam a comunicação entre um host conectado a uma rede IPv6 e um host IPv4 da Internet. A comunicação IPv6 para IPv4 ocorre da seguinte forma: o host IPv6 envia um pacote para um gateway NAT-PT. O gateway NAT-PT mapeia o endereço IPv6 do host para um endereço IPv4 público, implementa a tradução de protocolo IPv6-para-IPv4 e por fim envia o pacote para o host IPv4 de destino. Os hosts IPv6 necessitam adicionar um prefixo pré-configurado PREFIX::/96 ao endereço IPv4 de destino. Somente os pacotes com o prefixo pré-configurado são direcionados para o gateway NAT-PT que constrói o endereço de destino IPv4 eliminando o prefixo. No NAT-PT tradicional somente hosts IPv6 possam iniciar sessões. Utilizando NAT-PT Bidirecional, as sessões podem se iniciadas a partir de hosts IPv4 ou IPv6. Para implementar o NAT-PT Bidirecional, DNS_ALGs *(DNS Application Level Gateway*s) [11] são necessários. Similarmente ao NAPT, NAPT-PT permite compartilhar um único endereço IPv4 público entre 63K conexões simultâneas. NAPT-PT é sempre unidirecional (somente hosts IPv6 iniciam sessões com os hosts IPv4).

C. Mecanismos Baseados em Gateways de Camadas Superiores

O mecanismo mais conhecido de tradução em camadas superiores é o Proxy SOCKS64 [19], que e é baseado no mecanismo de SOCKS convencional [20]. No mecanismo SOCKS64, o gateway SOCKS é implementado como um host com pilha dupla IPv4/IPv6 e, no host cliente é implementado um programa específico denominado SOCKS LIB, entre as camadas de aplicação e transporte, que tem por função interceptar as pesquisas DNS e respondê-las com endereços IPv4 falsos. Quando o cliente chama a API de conexão, o SOCKS LIB troca o endereço IP falso pelo FQDN original e envia o pacote "socksified" para o proxy que executa a pesquisa DNS real. Se o servidor DNS responde com um "registro AAAA", o proxy abre um socket para o host de destino utilizando a interface IPv6. Caso contrário, ele utiliza a interface IPv4. O mecanismo SOCKS64 é uma solução bidirecional porque permite que os hosts IPv4 abram sessões com host IPv6 e vice e versa. Porém, os endereços IPv4 necessitam ser públicos. Um problema do mecanismo SOCKS64 é que ele quebra o modelo cliente-servidor, pois o gateway SOCKS64 internamente mantém dois sockets um para IPv4 e outro para IPv6. Outro mecanismo desta categoria o *Transport Relay Translator* (TRT) [21] permite a comunicação entre hosts IPv6 e hosts IPv4, sem que mudanças de *software* sejam necessárias. O TRT implementa um mecanismo similar ao SOCKS64, porém de forma transparente para os clientes, pois não necessita que seja instalado um programa específico no host cliente. Quando um host IPv6 deseja se comunicar com um host IPv4 ele deve adicionar um prefixo falso (por exemplo, C6::/64) ao endereço IPv4 do host de destino. Na infraestrutura de rede é inserido um equipamento intermediário que age como um *transport relay translator* (TRT) que é configurado para interceptar todos os pacotes IPv6 que contenham endereços de destino montados com o prefixo falso (C6::/64). Após interceptar os pacotes IPv6, o TRT abre uma conexão TCP IPv4 ou envia datagramas UDP IPv4 para o host de destino IPv4, de forma similar ao mecanismo SOCKS64. Teoricamente, para que o mecanismo torne-se bidirecional é necessário adicionar ao TRT um bloco de endereços IPv4 públicos e mecanismos de mapeamento de endereços, para que hosts IPv4 possam iniciar conexões com hosts IPv6 utilizando endereços IPv4 mapeados temporariamente. O TRT também quebra o modelo cliente/servidor.

D. Mecanismos Baseados em Tunelamento

Os mecanismos de transição baseados em tunelamento têm por finalidade permitir a conectividade IPv6 para hosts isolados ou redes que não possuem uma infraestrutura de rede IPv6 completa. A solução básica consiste em encapsular pacotes IPv6 em payloads de pacotes IPv4. O IETF propôs várias soluções de tunelamento. O mecanismo 6over4 permite interconectar hosts IPv6 isolados a um roteador 6over4 [22]. O túnel entre o host e o roteador é implementado através da criação de um grupo multicast IPv4. O mecanismo 6to4 também encapsula pacotes IPv6 em payloads de pacotes IPv4, porém é destinado a permitir a interconexão entre redes IPv6 isoladas através da Internet legada (IPv4) [23,24]. O mecanismo 6to4 é utilizado neste artigo para implementar o mecanismo *Transparent IPv*6, e por este motivo, será apresentado em detalhes na seção 3. A terceira solução baseada em tunelamento é o mecanismo *Tunnel Broker* [25] que permite aos hosts com pilha dupla isolados na Internet IPv4 se comunicarem a uma rede IPv6 através da criação de túneis IPv6 sobre IPv4. A arquitetura do *Tunnel Broker* é formada por servidores dedicados, denominados *Tunnel Broker*s, (TB) e por um roteador com pilha dupla denominado *Tunnel Server* (TS), conectado à Internet IPv4. Quando um host com pilha dupla isolado quer se conectar a uma rede IPv6, ele requisita ao TB a criação de um túnel. Então, o TB define um TS para ser utilizado como ponto final do túnel e designa um endereço IPv6 para o host.

Após essas operações, o TB envia para o host informações de configuração, tais como parâmetros do túnel e nomes DNS. Após estes passos de configuração o host isolado pode se conectar com redes IPv6, com as quais o TS escolhido como ponto final do túnel tenha conectividade. Uma limitação do mecanismo *Tunnel Broker* é que ele não pode ser empregado para hosts que possuem endereços IPv4 privados que utilizam recursos de NAT. Existem outras técnicas de tunelamento propostas pelo IETF, porém são similares aos três mecanismos já citados.

IV. TÚNEIS DINÂMICOS COM O MECANISMO 6TO4

Apesar, de grande parte do espaço de endereçamento IPv6 ainda estar indefinido, a IANA já vem trabalhando em conjunto com grupos IETF para definir o uso desses endereços. De qualquer forma, um importante segmento de endereços denominado de AGGR - *Aggregatable Global Unicast* [26] já está definido. Este segmento representa 1/8 do total do espaço de endereçamento IPv6. O endereço AGGR tem um formato padrão, como apresenta a Fig.1. O campo TLA *(Top Level Aggregation Identifie*r) é utilizado para segmentar o espaço do endereço AGGR em blocos menores.

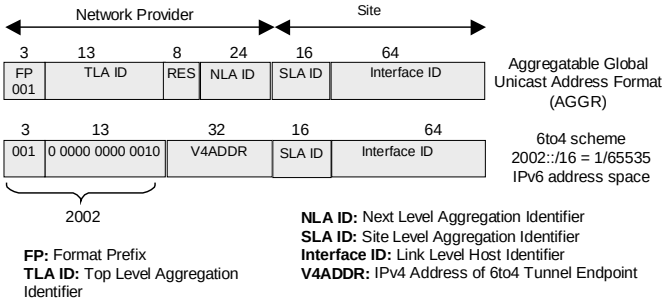

Fig. 1. Formato do Endereço Aggregatable Global Unicast e esquema 6to4.

Um desses blocos TLA já foi reservado para um especial esquema de endereçamento denominado *6to4*. Seu valor numérico é 0x0002, ou, 2002::/16 quando expresso como um endereço IPv6. A Fig. 1 apresenta o formato de endereço do esquema 6to4. Este esquema permite a criação de túneis dinâmicos para transportar pacotes IPv6 sobre uma infraestrutura IPv4 existente. A Fig. 2 apresenta este princípio.

Para implementar o mecanismo 6to4, a rede IPv6 necessita ter no mínimo um endereço IPv4 público, referenciado como V4ADDR, que é o endereço IPv4 da interface do roteador IPv6to4 que conecta a rede IPv6 à Internet. A outra interface do roteador, ligada à rede IPv6, possui um endereço IPv6. Este roteador precisa suportar o esquema de endereçamento 6to4 para permitir a criação de tunelamento dinâmico de pacotes IPv6 enviados para a Internet. A técnica de tunelamento consiste no encapsulamento de um pacote IPv6 em um pacote IPv4 usando o protocolo IPv4 tipo 41, como definido na RFC 2893 [7].

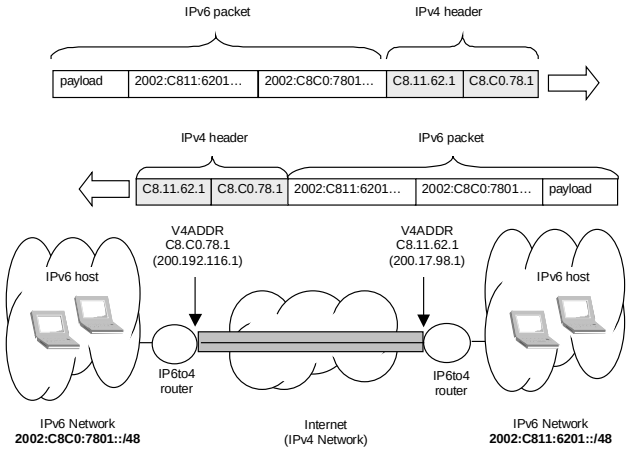

Fig. 2. Esquema 6to4 com túneis dinâmicos.

O roteador IPv6to4 pode criar dinamicamente túneis sem que configurações prévias sejam necessárias, somente analisando o campo V4ADDR dos endereços de destino dos pacotes IPv6. Desta forma, pode-se dizer que os túneis criados por ele são *stateles*s, porque toda informação necessária para a criação dos túneis é extraída dos pacotes.

V. MECANISMO TRANSPARENT IPV6

Esta seção apresenta um mecanismo para designar endereços IPv6 para equipamentos IPv4 sem que seja necessário efetuar qualquer modificação em software ou hardware. Este mecanismo é chamado neste artigo de *Transparent IPv6* (TIP6). O mecanismo TIP6 é a combinação do mecanismo de tunelamento 6to4 do IETF e de técnicas de mapeamento de endereços similares ao NAT-PT. A idéia principal é prover os benefícios do endereçamento IPv6 sem introduzir mudanças na infraestrutura IPv4 existente. De fato, este mecanismo pode ser imediatamente empregado por redes utilizando o padrão IPv4 Móvel para designar endereços IPv6 para equipamentos móveis, sem qualquer modificação de hardware ou software.

No TIP6, um host com um endereço IPv4 privado é mapeado para um endereço IPv6, de acordo com a Fig. 3. O endereço IPv6 pertence ao bloco TLA 2002::/16, de acordo com o mecanismo 6to4. O campo de identificador de interface é definido utilizando-se o endereço IPv4 como os 32 bits de baixa ordem. Apesar de não existir restrição imposta para o identificador no mecanismo TIP6, os 32 bits de alta ordem do identificador de interface serão mantidos iguais a zero para adaptar com os padrões existentes [22]. Para muitas implementações, o SLA ID pode ser mantido igual a zero, pois o mesmo só é requerido em casos onde ocorre sobreposição de espaços de endereçamento IPv4 privados.

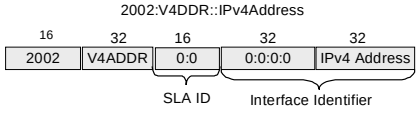

Fig. 3. Mapeamento de Endereços IPv6 para endereços IPv4 no mecanismo TIP6.

O mecanismo TIP6 é implementado pela combinação de técnicas de tunelamento e mapeamento um para um entre endereços IPv4 e IPv6. O mecanismo completo é apresentado na Fig. 4. Observe que ambas as redes são implementadas utilizando endereços IPv4 privados.

O elemento chave da arquitetura do TIP6 é o *Transparent IPv6to4 Gateway* (TIPG). O TIPG é um *dual home host* desenvolvido especialmente para suportar nosso propósito. Uma das interfaces do TIPG é configurada com um endereço IPv4 privado. A outra interface precisa ter um endereço IPv4 público registrado, utilizado como o V4ADDR para a criação de túneis dinâmicos. No mecanismo TIP6, os hosts IPv4 são endereçados utilizando *Fully Qualified Domain Names* (FQDN), isto é, hosts IPv4 precisam ter seus nomes registrados em um servidor DNS utilizando registros "AAAA" IPv6. Os nomes dos hosts são registrados utilizando os endereços IPv6 mapeados em seus endereços IPv4 privados, conforme indicado na Fig. 3.

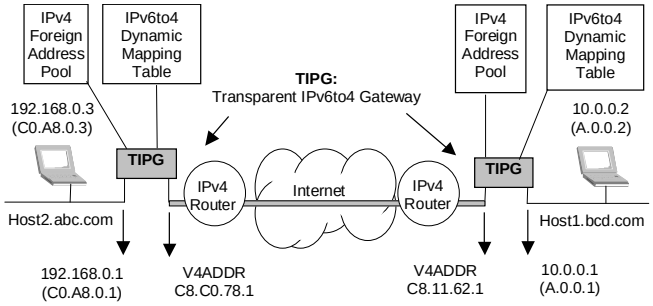

Fig. 4. Implementação do Mecanismo Transparent IPv6 (TIP6).

Os hosts móveis precisam ser configurados para utilizar o TIPG como servidor DNS. O TIPG não é um simples servidor de NAT. Ele é responsável por designar endereços IPv4 temporários *(IPv4 Foreign Address Pool*) para representar hosts IPv6 de redes externas. Esse mapeamento é feito através de uma tabela dinâmica *(IPv6to4 Dynamic Mapping Table*). O host IPv6 na rede externa pode ser um "verdadeiro host IPv6" ou um host IPv4 com um endereço IPv6 mapeado através do mecanismo TIP6 (conforme Fig. 5).

Para configurar o TIPG, o administrador de rede precisa definir um bloco de endereços IPv4 privados *(IPv4 Foreign Address Pool*) que não são utilizados na rede interna. Pelo fato do mapeamento não ser de caráter permanente, o tamanho do *bloco* define o número de sessões concorrentes que podem ser tratadas pelo TIPG.

Quando o TIPG recebe uma pesquisa DNS de um cliente interno, ele mapeia temporariamente um endereço IPv4 para representar o servidor IPv6 externo. Este endereço IPv4 é retornado para o cliente interno que constrói um pacote IPv4 simples e o envia para o roteador padrão (TIPG). O TIPG então executa duas operações seqüenciais sob o pacote. Primeiramente ele converte o pacote em um pacote IPv6 utilizando a abordagem NAT-PT. Em seguida, ele tunela o pacote adicionando um cabeçalho IPv4. Essas operações são apresentadas na Fig. 6.

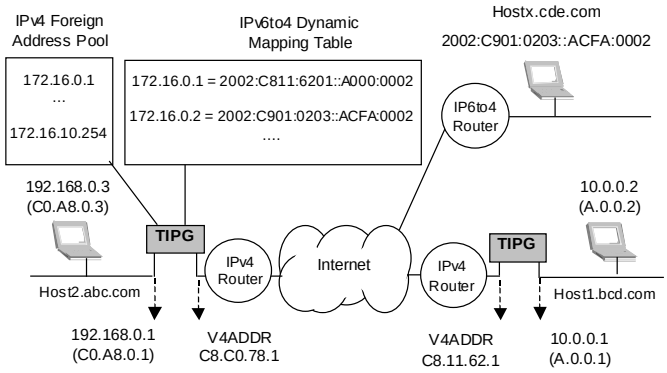

Fig. 5. Mapeamento IPv4 de hosts IPv6 externos no TIP6.

Na rede externa uma operação similar ocorre. O TIPG da rede de destino desencapsula o pacote recebido e executa uma operação de NAT-PT, construindo um pacote IPv4 com um endereço privado IPv4 temporariamente mapeado para o endereço IPv6 do cliente. A resposta do servidor também é apresentada na Fig. 6.

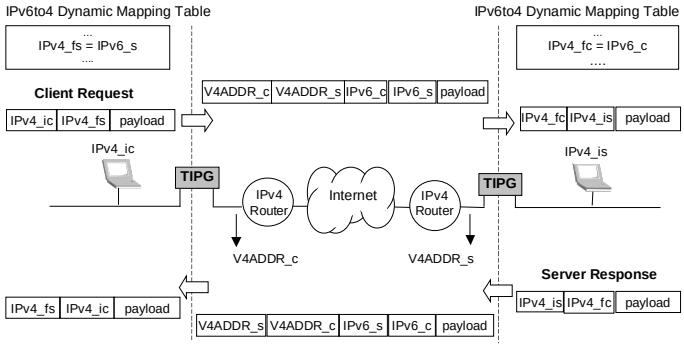

Fig. 6. NAT e tunelamento em TIP6.

Os símbolos utilizados na Fig. 6 estão descritos na Tabela 1.

TABELA I
LEGENDA S PARA A FIG. 6

IPv4_ic:	Endereço IPv4 privado do cliente interno.
IPv4_fs:	Endereço IPv4 temporariamente mapeado para o endereço IPv6 do servidor estrangeiro.
IPv6_s:	Endereço IPv6 do servidor estrangeiro (encontrado através de resolução DNS).
IPv6_c:	Endereço IPv6 do cliente interno (construído através da combinação de endereço IPv4 e V4ADDR).
IPv4_is:	Endereço IPv4 privado do servidor interno.
IPv4_fc:	Endereço IPv4 temporariamente mapeado para o endereço IPv6 do cliente estrangeiro
V4ADDR_c:	Endereço IPv4 do TIPG na rede cliente.
V4ADDR_s:	Endereço IPv4 do TIPG na rede do servidor.

VI. REDES MÓVEIS E TRANSPARENT IPV6

Esta seção apresenta como o *Transparent IPv6* (TIP6) pode ser utilizado para desenvolver grandes redes móveis sem o provisionamento de endereços IPv4 públicos. O mecanismo TIP6 é implementado em uma rede móvel através da conexão do *Transparent IPv6to4 Gateway* (TIPG) ao *home agent*, como é mostrado na Fig. 7. Nesta configuração o TIPG

precisa ser configurado como um servidor DNS para hosts móveis, mas não como *gateway* padrão. O *gateway* padrão é o *foreign agent*, como especificado pelo padrão IP Móvel. O mecanismo TIP6 requer que uma rota adicional seja configurada no *home agent*. Esta rota tem por finalidade direcionar todos os pacotes que possuem um endereço IPv4 pertencente ao *foreign address pool* para o TIPG. Todos os outros pacotes podem ser encaminhados diretamente para o *firewall*. Observe que a abordagem NAT padrão pode ainda ser utilizada para permitir que hosts móveis acessem redes IPv4 que não implementam o mecanismo TIP6.

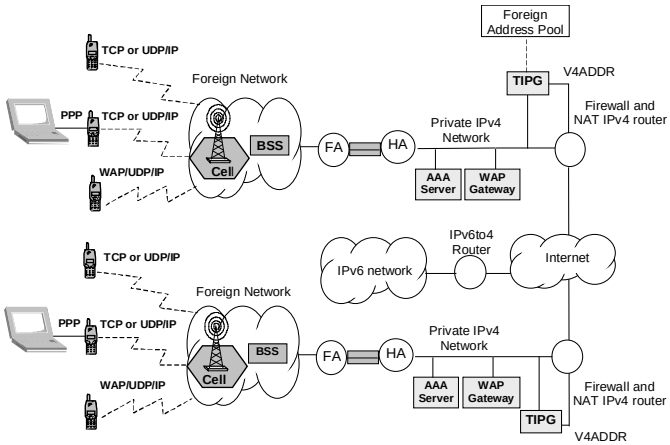

Fig. 7. Interoperação das Operadoras de Rede utilizando TIP6.

O mecanismo TIP6 permite a intercomunicação entre hosts móveis conectados a diferentes operadoras de rede que implementam o mecanismo TIP6 (ver Fig. 7) e permite que estas operadoras de rede possam utilizar sobreposição de endereços IPv4 privados, sem qualquer tipo de acordo prévio.

VII. Conclusão

Este artigo apresentou um novo mecanismo para gerenciar o problema da carência de endereços IPv4 públicos para redes móveis de grande porte, que utilizam o padrão IP Móvel. Este mecanismo é chamado de *Transparent IPv6* (TIP6). A idéia principal é prover os benefícios do endereçamento IPv6 sem introduzir mudanças significativas na infraestrutura IPv4 existente. O TIP6 pode ser imediatamente agregado às tecnologias celulares que oferecem IP Móvel, tais como GPRS e iDEN, para designar endereços IPv6 para aparelhos celulares sem qualquer modificação de software ou hardware. Uma visão geral dos mecanismos de transição IETF publicados mostrou que nenhum desses mecanismos é adequado para gerenciar problemas de comunicação de hosts com endereços IPv4 privados. Técnicas baseadas em tunelamento são parte da solução, pois permitem utilizar a infraestrutura IPv4, mas não implementam qualquer tipo de mapeamento entre endereços IPv4 e IPv6. Técnicas de tradução de endereços como NAT-PT não tratam o problema da comunicação entre dois hosts com endereço IPv4 privado. O mecanismo TIP6 é uma combinação do mecanismo de tunelamento 6to4 IETF e NAT-PT. O TIP6 estende as funcionalidades de NAT padrão permitindo que um host com endereço IPv4 privado possa receber conexões de hosts externos fixos ou móveis conectados à Internet. Um host IPv4 de uma rede TIP6 pode se comunicar com outras redes TIP6 ou com "verdadeiros" hosts IPv6. Esta característica do TIP6 permite a coexistência das implementações IP Móvel IPv6 emergentes com as redes legadas IPv4. Trabalhos futuros são requeridos ainda para avaliar o efeito do mecanismo de transição sobre os protocolos de segurança fim-a-fim como o IPSEC, e protocolos de sinalização para QoS, como o RSVP.

Referências

[1] C. Perkins, ed., "IP Mobility Support", IETF RFC 2002, Oct. 1996.

[2] GSM Association. An Overview of GPRS (General Packet Radio Service). http://www.gsmworld.com/technology/gprs.html

[3] Motorola. Integrated Dispatch Enhanced Network (iDEN) System Overview..http://www.motorola.com/LMPS/iDEN/addl_info/overview/sys_overview.html

[4] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot , E. Lear, "Address Allocation for Private Internets", IETF RFC 1918, Febr. 1996.

[5] S. Deering and R. Hinden,"Internet Protocol, Version 6 (IPv6) Specification", IETF RFC 1883, Dec. 1995.

[6] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", IETF RFC 1631, May 1994.

[7] R. Gilligan, E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", IETF RFC 2893, Aug. 2000..

[8] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", IETF RFC 1631, May 1994.

[9] WAP Forum Technical Specifications. Wireless Application Protocol (WAP). http://www.wapforum.org/what/technical.htm

[10] P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", IETF RFC 2663, August 1999.

[11] P. Srisuresh, G. Tsirtsis, P. Akkiraju, A. Heffernam, "DNS extensions to Network Address Translators (DNS-ALG)", IETF RFC 2694, Sept. 1999.

[12] R. Hidden, S, " Deering. IP Version 6 Addressing Architecture", IETF RFC 2373, July 1998.

[13] A. Baudot, G. Egeland, C. Hahn, P. Kyheroinen, A. Zehl, "Interaction of Transition Mechanisms", IETF Internet Draft, Febr. 2002.

[14] K. Tsuchiya, H. Higuchi, Y. Atarashi, "Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS)", IETF RFC 2767 Feb. 2000.

[15] E. Nordmark, "Stateless IP/ICMP Translation Algorithm (SIIT)", IETF RFC 2765, Feb. 2000.

[16] M. Shin, Y. Kim, E. Nordmark, A. Durand, "Dual Stack Hosts using "Bump-in-the-API" (BIA)", IETF Internet Draft, April 2002.

[17] J. Bound, L. Toutain, O. Medina, F. Dupont, H. Affifi, A. Durand, "Dual Stack Transition Mechanism (DSTM)", IETF Internet Draft, Jan. 2002.

[18] G. Tsirtsis, P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", IETF RFC 2766, Feb. 2000.

[19] H. Kitamura, "A SOCKS-based IPv6/IPv4 gateway mechanism", IETF RFC 3089, April 2001.

[20] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas and L. Jones, "SOCKS Protocol Version 5", March 1996.

[21] J. Hagino, K. Yamamoto, "An IPv6-to-IPv4 Transport Relay Translator", RFC3142, June 2001.

[22] B. Carpenter, C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", IETF RFC 2529, March 1999.

[23] B. E. Carpenter, K. Moore, B. Fink, "Connecting IPv6 Routing Domains Over the IPv4 Internet", Cisco Internet Protocol Journal, Volume 3, Number 1, March 2000.

[24] B. Carpenter, K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", IETF RFC 3056, Feb. 2001.

[25] A. Durand, I. Guardini, D. Lento, "IPv6 Tunnel Broker", IETF RFC 3053, January 2001.

[26] R. Hidden, M. O'Dell, S. Deering, "An IPv6 Aggregatable Global Unicast Address Format", IETF RFC 2374, July 1998.