Universidade Federal da Bahia
Escola Politécnica / Instituto de Matemática
Programa de Pós-Graduação em Mecatrônica

JERÔNIMO AGUIAR BEZERRA

MOBILIDADE IP COM O PROTOCOLO LISP: AVALIAÇÃO PRÁTICA

DISSERTAÇÃO DE MESTRADO

Salvador
2012

JERÔNIMO AGUIAR BEZERRA

MOBILIDADE IP COM O PROTOCOLO LISP: AVALIAÇÃO PRÁTICA

Dissertação apresentada ao Programa de Pós-Graduação em Mecatrônica da Escola Politécnica e do Instituto de Matemática, Universidade Federal da Bahia, como requisito parcial para obtenção do grau de Mestre.

Orientador: *Prof. Dr. Luciano Porto Barreto*

Salvador
2012

TERMO DE APROVAÇÃO

JERÔNIMO AGUIAR BEZERRA

MOBILIDADE IP COM O PROTOCOLO LISP: AVALIAÇÃO PRÁTICA

Dissertação aprovada como requisito parcial para obtenção do grau de Mestre em Mecatrônica, Universidade Federal da Bahia - UFBA, pela seguinte banca examinadora:

Prof. Dr. Luciano Porto Barreto (Orientador)
Doutor em Ciência da Computação, Universite de Rennes I, U.R.I., França
Professor da Universidade Federal da Bahia

Prof. Dr. Flávio Morais de Assis Silva (Examinador PPGM)
Doutor em Informática, Technische Universitat Berlin, Alemanha
Professor da Universidade Federal da Bahia

Prof. Dr. Daniel Macêdo Batista (Examinador Externo)
Doutor em Ciência da Computação, Universidade Estadual de Campinas, Brasil
Professor da Universidade de São Paulo

Prof. Dr. Paul Regnier (Examinador Externo)
Doutor em Ciência da Computação, Universidade Federal da Bahia, Brasil
Professor da Universidade Federal da Bahia

Salvador, 20 de Dezembro de 2012.

À minha família.
À minha noiva.
Aos meus amigos.

AGRADECIMENTOS

Um trabalho de mestrado com um tema que está associado a um tópico quente e polêmico em discussão no momento na IETF não se faz sem ajuda de diversos amigos e parceiros. Por isso, gostaria de agradecer a todos que direta ou indiretamente estão envolvidos com este trabalho, sua ajuda foi fundamental.

Porém, seria injustiça minha não citar algumas pessoas tiveram papel fundamental, que sem elas ou seria impossível, ou seria muito difícil este trabalho:

- Claudete e Luiz Cláudio, meus chefes eternos, que colocaram na minha cabeça que eu tinha que fazer o mestrado, pois era importante, etc e tal, e além da motivação, me deram todas as oportunidades para assistir aulas, fazer trabalhos, etc. Além disso, disponibilizaram toda infra para que eu montasse os laboratórios no PoP-BA/RNP;

- Meu Orientador, Prof. Luciano Porto, que desde o primeiro momento ouviu minhas propostas e apoiou a minha entrada no mestrado, mesmo sabendo que eu era muito ocupado e que poderia ser um risco. Além disso, compartilhou diversas experiências para me ajudar;

- Pessoal do Grupo de Trabalho do LISP: Apesar de estarem sempre envolvidos com as discussões mais baixo nível possível na especificação do LISP, sempre abriram espaço nas suas agendas para tirar dúvidas e me ajudarem, pois não é fácil acompanhar um protocolo em desenvolvimento: Dino Farinacci, Vince Fuller, Gregg Schudel, David Meyer e Darrel Lewis;

- Pessoal do LISPMob: Fabio Maino e Lori Jakab, que mesmo desenvolvendo o LISP-Mob, me ajudaram com minhas dúvidas;

- Ari Frazão, da RNP, que desde o início enxergou a importância e apoiou o projeto emprestando inclusive um dos roteadores utilizados pelo projeto e nos colocando no mapa-mundi do LISP;

- Professor Sérgio Gorender, que além de participar da minha qualificação com diversos comentários interessantes, ainda me emprestou o outro roteador utilizado nos laboratórios;

- Thiago Bomfim, Ítalo Valci, Fábio Costa, Luiz Barreto, Ibirisol e Humberto Galiza, amigos do PoP-BA que compraram a causa do LISP e transformaram em um serviço no PoP-BA, além de me ajudarem em todos os laboratórios;

- Alex Santana, Bruno Nunes, Orlando Filho e Társio Cavalcante, equipe que foi montada aleatoriamente na disciplina de Sistemas Mecatrônicos, mas se mostrou extremamente coesa e competente, além de muito divertida;

- Pessoal do PPGM, não só professores e funcionários, mas os demais colegas, sempre atentos e solícitos;

- Professores da banca, Prof. Daniel, Prof. Paul, Prof. Flávio que se dispuseram a participar da minha defesa mesmo sendo véspera do Natal;

- Ao pessoal da Internet Society: Leni Nazare, Steve Conte e Connie Kendig que por duas vezes fizeram possível minha participação nas reuniões do IETF, na China em 2010 e no Canadá em 2011, para discutir LISP, mobilidade e outros assuntos da área;

- Aos meus amigos Rodrigo Nazaré e Douglas Damálio, que de última hora viraram revisores do meu trabalho, com dicas muito úteis;

- E por último, mas não menos importante, minha amada Tassiane Sampaio e minha querida família, mãe, pai e irmãos, que sempre me estimularam e entenderam que, às vezes, eu precisava me ausentar para me dedicar a este trabalho.

  A todos vocês, meus profundos agradecimentos.

The measure of a man is what he does with power.

—PLATO

RESUMO

O crescimento não previsto para a Internet, de acadêmica-regional para comercial-global, traz, a cada dia, novas demandas por aplicações avançadas, entre elas Voz sobre IP - VoIP, vídeo sob demanda e videoconferência. Além de novas aplicações, novas funcionalidades se mostram interessantes para um futuro próximo, como mobilidade, *multihoming* e segurança fim-a-fim. Esse crescimento da Internet também trouxe à tona a preocupação com a sua escalabilidade, dado que a tabela de roteamento global tem crescido exponencialmente. Apesar de ser um tópico antigo dentro da comunidade de Internet, uma possível proposta que tem ganhado força é a separação dos espaços de roteamento (*namespaces*) da Internet, separando o núcleo da rede de usuários. Nesse novo contexto, este trabalho detalha como será possível inserir uma dessas novas funcionalidades, a mobilidade IP, de maneira nativa, evitando ao máximo a necessidade de intervenções futuras para o pleno funcionamento. Será usado o protocolo *Locator/ID Separation Protocol* (LISP) como estudo de caso, e o mesmo será experimentado de forma prática através de cenários que farão a avaliação do tempo de convergência.

BGP, Roteamento Internet, Separação Localização Identificação, Mobilidade, Escalabilidade da Internet

ABSTRACT

The unpredicted Internet growth, from academic-local to business-global, brings everyday, new demands for advanced applications, as Voice over IP (VoIP), on-demand video and videoconference. Besides new applications, new features have been shown as interesting for the near future, e.g. mobility, multihoming and end-to-end security. This Internet growth also brought concerns about the Internet scalability, once the global routing table has grown exponentially in the last years.

Although it is an old topic inside the Internet community, a very interesting proposal is to separate Internet routing's namespaces, where will be separated the core of the Internet from the edge, which is where all users are. Considering this new context, this work will detail how will be possible insert one of these new functionalities, the IP mobility, avoiding as much as possible the necessity for new interventions in the future for full operation. It will be used the Locator/ID Separation Protocol - LISP as a case study, and it will be evaluated in scenarios which will measure its convergence time.

BGP, Internet Routing, Loc/ID Separation, Mobility, Internet Scalability, LISP

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ANATEL - Agência Nacional de Telecomunicações

ARP - Address Resolution Protocol

ASN - Autonomous System Number

BGP - Border Gateway Protocol

CN - Correspondent Node

CoA - Care of Address

ANATEL - Agência Nacional de Telecomunicações

ARP - Address Resolution Protocol

ASN - Autonomous System Number

BGP - Border Gateway Protocol

CN - Correspondent Node

CoA - Care of Address

CPU - Central Processing Unit

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

EID - Endpoint IDentification

ETR - Egrees Tunnel Router

FA - Foreign Agent

FN - Foreign Network

FoA - Foreign Address

FQDN - Fully Qualified Domain Name

HI - Host Identity

HIP - Host Identification Protocol

HIT - Host Identification Tag

HN - Home Network

HoA - Home Address

IETF - Internet Engineering Task Force

IAB - Internet Architecture Board

ICMP - Internet Control Message Protocol

ILNP - Identifier-Locator Network Protocol

IP - Internet Protocol

ITR - Ingress Tunnel Router

ITU-T - International Telecommunication Union - Telecommunication Standardization Sector

LAN - Local Area Network

LISP - Locator/ID Separation Protocol

LISP-ALT - Locator/ID Separation Protocol - Alternative Topology

LISP-MN - Locator/ID Separation Protocol - Mobile Node

LLOC - Local LOCator

MIP - Mobile Internet Protocol

MIPv6 - Mobile Internet Protocol version 6

MN - Mobile Node

MR - Map-Resolver

MR-MS - Map-Resolver/Map-Server

MS - Map-Server

MTCP - Mobile TCP

MTU - Maximum Transmission Unit

NAT - Network Address Translation

PETR - Proxy Egress Tunnel Router

PITR - Proxy Ingress Tunnel Router

PxTR - Proxy Ingress/Egress Tunnel Router

QoS - Quality of Service

RFC - Request for Comments

RLOC - Routing Locators

RTR - Re-encapsulating Tunnel Router

RTT - Round-Trip Time

RVS - Rendezvous Server

SCTP - Stream Control Transmission Protocol

SMR - Solicit Map-Request

SN - Stationary Node

SSH - Secure SHell

SSID - Service Set IDentifier

TCP - Transmission Control Protocol

TTL - Time To Live

UDP - User Datagram Protocol

VoIP - Voice over Internet Protocol

xTR - Ingress/Egress Tunnel Router

Wi-Fi - Wireless Fidelity

CONTEÚDO

CAPÍTULO 1

INTRODUÇÃO

A sociedade atual vive um momento diferenciado na história, um momento onde existe a necessidade ter acesso à informação de qualquer lugar, com fácil acesso e a todo momento. Segundo as estatísticas da Agência Nacional de Telecomunicações - ANATEL [ANATEL, 2012], em Abril de 2012, o Brasil possuía 253 milhões de linhas telefônicas móveis ativas, com 21,46% destas com o serviço de banda larga móvel 3G. Um pouco antes, um estudo da Cisco[Cisco, 2012] publicado em Fevereiro de 2012, mostrou que é esperado que o tráfego Internet de dispositivos móveis no mundo cresça 19 vezes até 2016, superando em três vezes a quantidade de tráfego de dispositivos não-móveis. Tais estatísticas comprovam que a necessidade de estarmos sempre conectados é real, e que a mobilidade no contexto do protocolo IP [Postel, 1981a] -um dos protocolos responsáveis pelo funcionamento da Internet- merece destaque.

Apesar da vasta cobertura das tecnologias de redes banda larga celulares e da consolidação do Wi-Fi [Crow et al., 1997], as áreas de cobertura possuem uma região limitada, definidas em projeto. No momento em que saímos de uma região de cobertura de uma empresa ou tecnologia, de 3G para Wi-Fi, por exemplo, ocorre uma desconexão e uma nova conexão, seja na mesma ou outra tecnologia, seja na mesma ou outra operadora de telecomunicações. Como exemplo, podemos citar um trem de passageiros que percorre diversos países. Este pode, ao longo do seu percurso, entrar e sair em diversas redes de cobertura celular 3G/4G diferentes, forçando os dispositivos dos usuários a desconectarem e se reconectarem em outra rede, processo conhecido como *roaming*. Além disso, o próprio trem pode fazer uso da Internet para prover informações de gerência e monitoramento remoto, em tempo real, para uma estação central. Então, neste momento de *roaming*, se este ocorrer entre tecnologias ou operadoras diferentes, os dispositivos que estiverem fazendo uso do serviço de dados serão obrigados a reiniciarem todas as co-

nexões previamente estabelecidas, sejam elas *download* de arquivos, ligações telefônicas, videoconferências, acesso remoto, etc.

A reinicialização das conexões durante o *roaming* se faz necessária devido à falta de suporte nativo para mobilidade do protocolo IP. Esta mesma situação se aplica a outros dispositivos mecatrônicos móveis, como aviões, navios, ônibus e mesmo carros. Em um futuro em que se almeja que os dispositivos móveis sejam altamente automatizados e gerenciados remotamente, é fundamental que a mobilidade IP seja um requisito atendido plenamente, a fim de evitar que as conexões de gerenciamento e automação, por exemplo, sejam reiniciadas apenas devido à troca da tecnologia de conexão sem fio (*wireless*). Assim sendo, a falta de suporte para mobilidade do protocolo IP precisa ser contornada, seja por adição de novos protocolos ou componentes com este fim ou mesmo a adoção de um novo protocolo roteado para a Internet que possua suporte nativo para mobilidade.

Além da falta de suporte à mobilidade, o protocolo IP possui diversas outras fragilidades, mas uma vez que o mesmo é a base da Internet, não é possível simplesmente substituí-lo. Problemas de escalabilidade, segurança, mobilidade, entre outros, têm gerado diversas discussões na *Internet Engineering Task Force*[1] - IETF, que é a entidade responsável pelas especificações dos protocolos utilizados na Internet. Dentre as diversas discussões em andamento nos grupos de trabalho da IETF, um tópico muito abordado no momento é o de escalabilidade da Internet, com diversas propostas em andamento com intuito de propor a "Internet do futuro".

1.1 INTERNET DO FUTURO

O fato de a Internet não ter sido planejada para suportar tráfego além do acadêmico fez com que a mesma crescesse de maneira desordenada, e, ao longo dos últimos anos, muitas adaptações têm sido feitas para que não haja um colapso. Novos protocolos de roteamento e identificação, conceitos de "espaços de roteamento", tunelamento, técnicas contra exaustão de endereçamento, e protocolos/métodos de segurança foram e ainda estão sendo

[1]IETF: http://www.ietf.org

incorporados à rede já existente. Essa falta de planejamento inicial está fazendo a tabela de roteamento global crescer exponencialmente, segundo [Bates and Huston, 2009]. Além disso, temos um perfil de rede cada vez mais dinâmico, onde aplicações convergentes e mobilidade cada vez mais são requeridas e utilizadas por usuários e provedores, comprometendo ainda mais a tabela de roteamento global.

Neste contexto, em 2006, no Workshop de Roteamento e Endereçamento da *Internet Architecture Board* (IAB) da IETF, foram debatidas questões pertinentes à escalabilidade da Internet, onde foi desenvolvido um pensamento comum sobre o assunto e foi proposta como tarefa posterior, que os participantes pensassem e propusessem soluções [Meyer et al., 2007]. A partir dessa reunião, o conceito que mais se evidenciou, e vem criando cada vez mais adeptos, é o conceito da separação dos espaços de roteamento. Esse conceito visa retirar da tabela de roteamento global os endereços referentes aos *hosts* -dispositivos dos usuários-, fazendo com que na tabela de roteamento global constem apenas os endereços dos localizadores dos usuários. Nesta nova abordagem, considerada informalmente como a "Internet do futuro", os dispositivos dos usuários teriam endereços para identificação desassociados dos endereços utilizados para roteamento na Internet, permitindo não só a escalabilidade da mesma, como também a adição de novos recursos, principalmente a mobilidade IP.

Baseado nas mudanças das necessidades dos usuários bem como nas propostas de mudanças no funcionamento do roteamento da Internet, este trabalho visou detalhar as dificuldades existentes para uso da mobilidade IP na Internet atual, introduzir as propostas de mudanças para a "Internet do futuro", para assim, fazer um estudo sobre a viabilidade do serviço de mobilidade IP nesta nova Internet, comparando as diversas abordagens de solução. Pretendeu-se também, demonstrar na prática a eficiência e eficácia de uma das soluções propostas que já possui implementação mundial, o protocolo LISP - *Locator/ID Separation Protocol*. Este estudo mostra-se muito importante neste momento de discussões sobre o futuro da Internet e, a partir dele, propostas e questionamentos serão levados aos grupos de trabalho na IETF.

Essa demonstração prática foi realizada através de três experimentos, cujo o foco está no tempo de convergência que a solução LISP apresenta:

1) Experimento 1 - Tempo de convergência entre dois domínios LISP. Neste experimento foi avaliado o tempo de convergência que o dispositivo móvel observa quando migra entre dois domínios LISP;

2) Experimento 2 - Tempo de convergência entre domínio LISP e a Internet. Neste experimento foi avaliado o tempo de convergência que o dispositivo móvel observa quando migra de um domínio não-LISP, como a Internet atual, para um domínio LISP, e vice-versa;

3) Experimento 3 - Tempo de convergência com LISP-MN na Internet atual. Neste experimento foi avaliado o tempo de convergência que o dispositivo móvel observa quando faz uso apenas da Internet atual, simulando uma aplicação imediada.

Em todos os experimentos foi utilizada uma ferramenta livre disponibilizada pela comunidade do LISP, chamada de LISPMob[2]. Para o propósito de avaliação da convergência, esta ferramenta recebeu algumas modificações focadas na avaliação e redução do tempo de convergência. O LISPMob e as modificações efetuadas serão apresentadas no Capítulo 4.

Além disso, no que tange a avaliação prática, para que os experimentos ocorressem, foi necessária a participação na rede de testes do LISP, chamada de LISP *beta-network*[3], o que trouxe diversos resultados diretos e indiretos, resultados estes citados na Seção 1.2.

1.2 RESULTADOS ALCANÇADOS

Este trabalho foi iniciado, desenvolvido e concluído ao longo das discussões do protocolo LISP e de sua extensão para mobilidade, o LISP *Mobile Node*, ou LISP-MN

[2]LISPMob - http://www.lispmob.org
[3]LISP beta-network: http://www.lisp4.net/beta-network/

[Farinacci et al., 2012a]. Esta característica trouxe desafios extras, pois protocolos em desenvolvimento na IETF recebem correções e adições com relativa frequência por parte dos membros dos grupos de trabalho. A proposta do protocolo LISP-MN iniciou através da primeira especificação (chamado de *draft* na IETF) em Julho de 2009 [Farinacci et al., 2012b] e atualmente está na versão 08 [Farinacci et al., 2012a]. O procolo LISP, que teve seu primeiro *draft* submetido em Janeiro de 2007, já foi atualizado trinta e seis vezes, tornando-se um protocolo formalizado pela IETF em Janeiro de 2013, através da *Request for Comments* - RFC 6830 [Farinacci and Fuller, 2012].

Essas constantes alterações se mostraram como desafios uma vez que obrigavam a releitura das especificações, atualização de código inicialmente desenvolvido (e depois descontinuado) e montagem de cenários que dependiam da LISP *beta-network*, que é a rede mundial de testes do protocolo LISP. Mesmo a LISP *beta-network* precisou ser atualizada em diversos momentos devido às correções sugeridas às especificações envolvendo o protocolo LISP. Porém, estes desafios serviram de motivadores no momento que gerou oportunidades de interação com os membros do grupo de trabalho do LISP e com a IETF, sempre adeptos de novos participantes. Essa interação trouxe como resultados diretos, além da inclusão do autor no grupo de trabalho com espaço para discussões e propostas, a publicação de um artigo no *1st Workshop Research on the Future Internet*[4], com o título "*LISP as a solution for Internet scalability*", em 2010, em Gramado, RS.

A seguir, serão listados alguns dos resultados indiretos deste trabalho, com uma pequena contextualização do mesmo no ambiente da Universidade Federal da Bahia.

1.2.1 Resultados indiretos

A história do LISP na UFBA começou em 2008, quando, através da parceira com o NIC.Br[5], o Centro de Processamento de Dados da UFBA decidiu apoiar a realização do evento do LACNIC[6] em Salvador. Neste evento, houve uma palestra sobre o LISP[Reis, 2008],

[4]WPEIF - http://sbrc2010.inf.ufrgs.br/anais/data/pdf/wpeif.pdf
[5]Núcleo de Informação e Comunicação do Ponto BR - http://nic.br
[6]LACNIC - http://www.lacnic.net/web/eventos/inicio

ministrada por Eduardo Ascenço, que havia participado do *IETF Meeting*[7] daquele ano. Foi proposto então, em 2009, o assunto LISP para o então estudante de computação da UFBA e funcionário do CPD da UFBA, Humberto Galiza, como trabalho de conclusão de curso, tendo o Professor Dr. Luciano Porto Barreto como orientador e o funcionário Jerônimo Bezerra como co-orientador. Desde então, a seguinte trajetória foi percorrida:

- Em 2009, Humberto Galiza apresentou seu trabalho de conclusão de graduação com o assunto "*A escalabilidade da Internet e uma nova perspectiva do roteamento com o protocolo LISP*"[Freitas, 2009];

- Ainda em 2009, foram iniciadas as conversas com os membros do grupo de trabalho do LISP para tornar possível a participação da UFBA na rede de testes, chamada na época de LISP-ALT;

- Em 2010, o autor deste, Jerônimo Bezerra, foi aceito na vaga de aluno regular no Mestrado de Mecatrônica da UFBA, e desde o início, tem trabalhado com o tema de mobilidade usando o LISP;

- Ainda em 2010, após novas conversas com o grupo de trabalho, a UFBA teve sua participação aprovada, e a empresa *Cisco Systems*[8] forneceu um roteador para funcionar como o servidor de mapeamento LISP do Brasil;

- Ainda naquele ano, a UFBA obteve emprestado da Rede Nacional de Ensino e Pesquisa[9], um outro roteador, e assim, pôde começar os experimentos práticos com LISP;

- Dado esse envolvimento com o LISP, a UFBA teve dois funcionários/estudantes contemplados no programa *Fellowship Program* da *Internet Society*[10], onde estes tiveram as passagens, diárias e hotéis pagos pelo programa, tendo a oportunidade de discutir *in loco* com os pesquisadores envolvidos nos temas relacionados, como

[7]IETF Meetings - http://www.ietf.org/meeting/
[8]Cisco Systems - http://www.cisco.com
[9]RNP - http://www.rnp.br
[10]ISOC - http://www.isoc.org

LISP, mobilidade, entre outros. Humberto Galiza participou do evento na Holanda, e Jerônimo Bezerra, participou do encontro em Pequim, na China;

- Ainda em 2010, um artigo da UFBA foi aprovado no *1st Workshop Research on the Future Internet*, com o título "*LISP as a solution for Internet scalability*"[Bezerra et al., 2010a], em Gramado, RS;

- Nos meados de 2010, a UFBA entrou no mapa-mundi da rede de testes do LISP, conforme Figura 1.1, passando a ser a primeira e única participante brasileira deste piloto;

- Em 2011, a UFBA novamente foi contemplada pela *Internet Society*, agora no programa *Returning Fellow*, para discutir sobre LISP, entre outros. Desta vez, o autor teve a oportunidade de participar na reunião que ocorreu no Quebec, Canadá;

- Também em 2011, o Professor Dr. Luciano Porto obteve uma bolsa na FAPESB para um estudante de graduação, para trabalhar com LISP. Este estudante, Fábio Costa, mesmo após o fim da bolsa, continua voluntariamente trabalhando com LISP;

- No final de 2011, dado o envolvimento com LISP, bem como a escrita de um código em C para funcionar no Linux para LISP-MN, a UFBA obteve acesso ao código em desenvolvimento de LISP de uma empresa da área de rede de computadores. A partir daquele momento, a iniciativa existente de desenvolvimento do próprio código foi descontinuada e a UFBA passou a ajudar nesta nova versão, fazendo testes de funcionamento.

Conforme citado anteriormente, muitos dos feitos listados acima, foram e são extremamente importantes para os envolvidos, bem como para a UFBA, que começa a conviver e estimular o envolvimento com o LISP, a pesquisa de protocolos e com a IETF.

Após esta introdução e dando início a este trabalho, o mesmo está assim organizado: no Capítulo 2 serão apresentados os conceitos fundamentais para o entendimento

Figura 1.1. UFBA no cenário LISP+ALT.

deste, além de serem apresentadas soluções correlatas para mobilidade IP e mobilidade IP no contexto da Internet do futuro; no Capítulo 3 será apresentado o *LISP Mobile Node*[Farinacci et al., 2012a], que é a simplificação do LISP para ser usado nos dispositivos dos usuários a fim de permitir a mobilidade; no Capítulo 4, o *LISP Mobile Node* será testado em um ambiente prático e real a fim de validar se o mesmo atende os requisitos propostos para mobilidade IP definidos pelo *Mobile IP - MIP* [Perkins et al., 2010] e de desempenho para comunicação interativa, usando parâmetros do [ITU-T, 2000]. E no último capítulo serão apresentadas as conclusões de viabilidade e possíveis modificações que podem ser aplicadas ao protocolo LISP a fim de otimizá-lo.

CAPÍTULO 2

FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão introduzidos os conceitos fundamentais que servirão para o entendimento do trabalho, assim organizados: na Seção 2.1 será explicado como o protocolo IP cria a deficiência para a escalabilidade da Internet e dificulta o serviço de mobilidade. Na Seção 2.2, serão apresentados conceitos de mobilidade, mobilidade em redes locais, além do *Mobile IP* [Perkins et al., 2010], que é o principal mecanismo criado a fim de permitir a mobilidade com o protocolo IP; na Seção 2.3 será apresentado o *Border Gateway Protocol*, que é o protocolo utilizado para roteamento IP na Internet; na Seção 2.4 serão apresentados os problemas atuais que forçam a IETF na busca de soluções para a escalabilidade da Internet; na Seção 2.5, será apresentado o *Locator/ID Separation Protocol* - LISP, que é uma das propostas até então apresentadas com mais maturidade e aceitação na IETF, possuindo inclusive uma rede de testes mundial. E por fim, na Seção 2.6, serão apresentados dois protocolos correlatos, que resolvem o problema da mobilidade IP existente, a título de comparação com o protocolo LISP.

2.1 SOBRECARGA DE SEMÂNTICA DO PROTOCOLO IP

No funcionamento das redes atuais, baseadas no protocolo IP, um dispositivo de usuário, ou *host*, para poder fazer uso da rede, precisa obter um endereço IP pertinente à rede na qual está localizado, seja por configuração de endereçamento estático ou via algum protocolo de alocação dinâmica, como o *Dynamic Host Configuration Protocol* - DHCP [Droms, 1997]. Tendo o endereçamento IP configurado, o *host* poderá fazer uso da rede utilizando o endereço atribuído como endereço de origem para os pacotes IP, e, juntando com endereço da camada de transporte -as portas-, estabelecerá conexões com *hosts* remotos, enviando o pacote com um endereço IP e porta de origem para um

endereço IP e porta de destino. Esse conjunto de <IP Origem, Porta Origem, IP Destino, Porta Destino> será usado para definir a conexão estabelecida. Neste contexto, o endereço IP está sendo utilizado para **identificar** os *hosts* envolvidos na conexão.

No momento em que o *host* envia o pacote IP para a rede local, os roteadores farão o encaminhamento do pacote, roteador por roteador, até que este pacote chegue ao destino. Para isso, os roteadores consultam as tabelas de rotas para descobrir como fazer o encaminhamento, ou seja, encontrar o melhor caminho para o envio do pacote, seja buscando o endereço IP de destino no envio do pacote, seja buscando o endereço IP de origem no retorno do pacote. Então, neste contexto, o endereço IP está sendo utilizado para **localizar** o *host*, seja na rede local LAN (*Local Area Network*), seja na Internet.

Essa sobrecarga de semântica do protocolo IP, com a função de identificar e de localizar o *host*, impossibilita que qualquer conexão entre *hosts* permaneça funcional após a troca de qualquer um dos componentes utilizados para definir a conexão estabelecida. Ou seja, em caso de troca de qualquer um dos elementos envolvidos, IP ou portas, a conexão será interrompida e uma nova conexão precisará ser estabelecida, comprometendo a comunicação anterior, como, por exemplo, um *download* de um arquivo.

Com essa sobrecarga mapeada, muitos trabalhos tem sido propostos para contornar essa deficiência, pois uma vez que o protocolo IP, neste caso IPv4, está consolidado na Internet, é impossível substituí-lo rapidamente. Muitos dos trabalhos tem, então, buscado diminuir ou eliminar a sobrecarga de semântica baseando-se em duas abordagens: alterando os *hosts*(*host-based*) ou alterando as redes (*network-based*). Nas abordagens baseadas nos *hosts*, novos protocolos são inseridos na pilha TCP/IP (ilustrada na Figura 2.1) -a fim de contornar a sobrecarga-, ou mesmo altera-se a pilha TCP/IP, para aplicar uma solução definitiva. Para a primeira opção, diversos protocolos foram e estão sendo definidos, entre eles o *Stream Control Transmission Protocol* - SCTP [Koh et al., 2004], *Session Initiation Protocol* - SIP [Schulzrinne et al., 1999] e o *Multipath TCP* - MTCP [Kuang et al., 2004]. Na segunda abordagem, a ideia é criar uma nova camada na pilha TCP/IP, entre a Camada de Rede e a Camada de Transporte para adicionar uma

camada de identificação, cujo propósito seria permitir que os *hosts* pudessem mudar de endereçamento IP e fazer uso de múltiplas interfaces de rede, entre outras funcionalidades, sem nenhuma dependência do endereço IP, garantindo assim o fim da sobrecarga de semântica mencionado. Como exemplo, podemos citar o *Host Identification Protocol* [Moskowitz, 2012], que será detalhado na Seção 2.6.1.

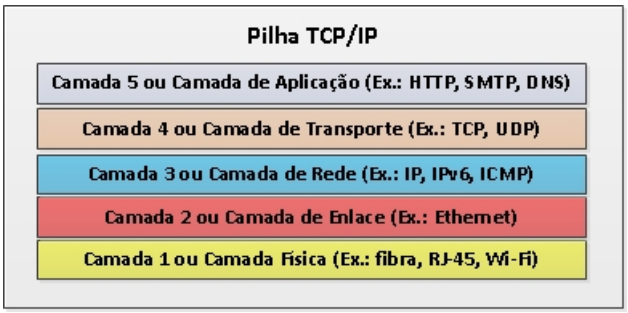

Figura 2.1. Pilha TCP/IP.

Uma vez que este trabalho visa estudar a implantação de mobilidade IP no novo contexto proposto para a Internet, onde a separação da identificação da localização no protocolo IP seria feito no núcleo da rede, serão apresentados conceitos e abordagens baseadas na rede, com pouco impacto para os *hosts*. Como será exposto mais à frente, apesar de haver adição de funcionalidade nos *hosts*, essa solução é caracterizada como baseada na rede, por existir total dependência dos componentes de rede para seu funcionamento. Porém, antes, se faz necessário apresentar a solução baseada em rede para o ambiente de Internet já existente. Em 1996, a RFC 2002 [Perkins, 1996] apresentou o *Mobile IP*, um conjunto de técnicas e funcionalidades cujo objetivo era permitir que, mesmo com a sobrecarga do endereço IP, fosse possível fazer uso da mobilidade. Essa solução será apresentada na SubSeção 2.2.2.

2.2 MOBILIDADE

Nesta seção serão apresentados conceitos referentes à mobilidade em geral, mobilidade em redes locais -redes internas das instituições fortemente baseadas na Camada de Enlace-, além de conceitos de mobilidade IP, utilizando como referência o MIP, ou *Mobile Internet*

Protocol.

No tema da mobilidade, uma das características fundamentais é o tempo de convergência entre pontos de associação, que são os equipamentos de rede aos quais o *host* se conecta. Esse tempo de convergência, conhecido por *handover* ou *handoff* na literatura acadêmica e comercial, é o tempo decorrido para que o dispositivo do usuário "migre" de um ponto de associação para outro e mantenha ativa sua conexão, seja ela de dados ou de voz. Para isso, dependendo da aplicação, o tempo tem que ser o mínimo possível para o *host* se desassociar do ponto de associação, buscar por um novo ponto, associar-se a este novo ponto e fazer a autenticação, para então, continuar a trafegar normalmente.

Além do tempo do *handover*, outras características são requisitos para definir se uma solução suporta mobilidade ou não, e estes requisitos estão listados abaixo [Perkins et al., 2010]:

- Dispositivos móveis podem se comunicar com dispositivos legados sem necessidade de alteração no código destes;
- Dispositivos móveis devem manter o mesmo endereço IP durante o processo de mobilidade;
- A comunicação não deve ser reiniciada após a mobilidade ser concluída;
- Apenas os roteadores envolvidos no processo de mobilidade precisam suportar mobilidade.

Conforme citado anteriormente, existem dois contextos para uso da mobilidade: redes locais e a Internet. Nas subseções a seguir serão apresentadas as particularidades de cada contexto.

2.2.1 Mobilidade em redes locais

Nas redes locais, que podem ser Wi-Fi[1] corporativo ou redes celulares da mesma operadora (GSM, CDMA, LTE, 3G, etc.), as tecnologias existentes são baseadas na Camada de Enlace da pilha TCP/IP, e evoluíram drasticamente nos últimos 10 anos.

Nas redes Wi-Fi, quando utiliza-se equipamentos individuais, ou *standalones*, é comum se observar tempos de convergência (*handover*) entre pontos de associação superiores a 30 segundos [Mandeville, 2012]. Porém, com a evolução dos sistemas *wireless* corporativos, onde uma entidade central é responsável por toda parte de admissão e os pontos de associação são "apenas" conversores de sinal elétrico para rádio frequência, observam-se *handovers* inferiores a 20 ms em alguns fabricantes de equipamentos de rede, como a *Extreme Networks*[Group, 2005].

Nas redes locais, com a implantação de serviços Wi-Fi corporativos e com gerência centralizados, o serviço de mobilidade já é tratado como um serviço básico, uma vez que, operando na Camada de Enlace e com tempo de convergência extremamente baixo, a implantação é trivial e transparente para os *hosts*, atendendo todos os requisitos citados acima. Porém, no âmbito da Internet, baseada na Camada de Rede da pilha TCP/IP, a mobilidade possui características completamente diferentes, e estas particularidades serão tratadas na SubSeção 2.2.2.

2.2.2 Mobilidade IP

A fim de permitir a mobilidade no âmbito da Internet, em 1996, a IETF lançou a padronização do *Mobile IP* (MIP) através da *Request For Comments* - RFC 2002, tendo Editor Perkins, da IBM, como autor. Em 2002, a RFC 3220 [Perkins et al., 2002b] tornou a RFC 2002 obsoleta, que logo tornou-se obsoleta pela RFC 3344[Perkins et al., 2002a] e, em 2010, também virou obsoleta com a RFC 5944[Perkins et al., 2010]. Ao longo dos 14 anos entre a criação e o lançamento da última especificação, o *Mobile IP* não conseguiu

[1]Wireless Fidelity - http://www.wi-fi.org

virar um serviço na Internet por diversos motivos que serão detalhados a seguir. Porém, sua proposta de funcionamento serve como um referencial para novos protocolos *network-based*, uma vez que diversos termos foram criados e assimilados pela comunidade da IETF.

Segundo a RFC 5944, *Mobile IP* é um protocolo de comunicação padrão, definido para permitir que dispositivos móveis de usuários se movam de uma rede IP para outra enquanto mantém seus endereços IP permanentes e, consequentemente, suas conexões ativas. Para explicar seu modo de funcionamento, serão detalhados os componentes envolvidos no processo de mobilidade IP usando o MIP:

- **Home Network** (HN): Rede da qual o *host* faz parte;
- **Home Address** (HoA): Endereço IP do *host* na *HN*;
- **Home Agent** (HA): Roteador com suporte ao MIP da rede da qual o *host* faz parte;
- **Foreign Network** (FN): Rede para a qual o *host* migra;
- **Care-of-Addres** (CoA): Endereço IP obtido na rede de destino, ou *FN*;
- **Foreign Agent** (FA): Roteador com suporte ao MIP na rede de destino;
- **Mobility Binding**: A associação entre o HoA e o CoA;
- **Mobile Node** (MN): Dispositivo que está fazendo uso da mobilidade
- **Correspondent Node** (CN): Dispositivo com que o MN está se comunicando.

Para ilustrar o funcionamento, observe a Figura 2.2. Na "Situação Inicial" é possível observar que o dispositivo MN está associado a um dispositivo de rede sem fio Wi-Fi na sua rede de origem HN, e faz uso da rede da maneira tradicional para se comunicar com o CN. Neste caso, o roteador *Home Agent* (HA) funciona como um roteador qualquer.

Na ilustração "Após Mobilidade" da Figura 2.2 ocorre a mobilidade IP, da seguinte maneira:

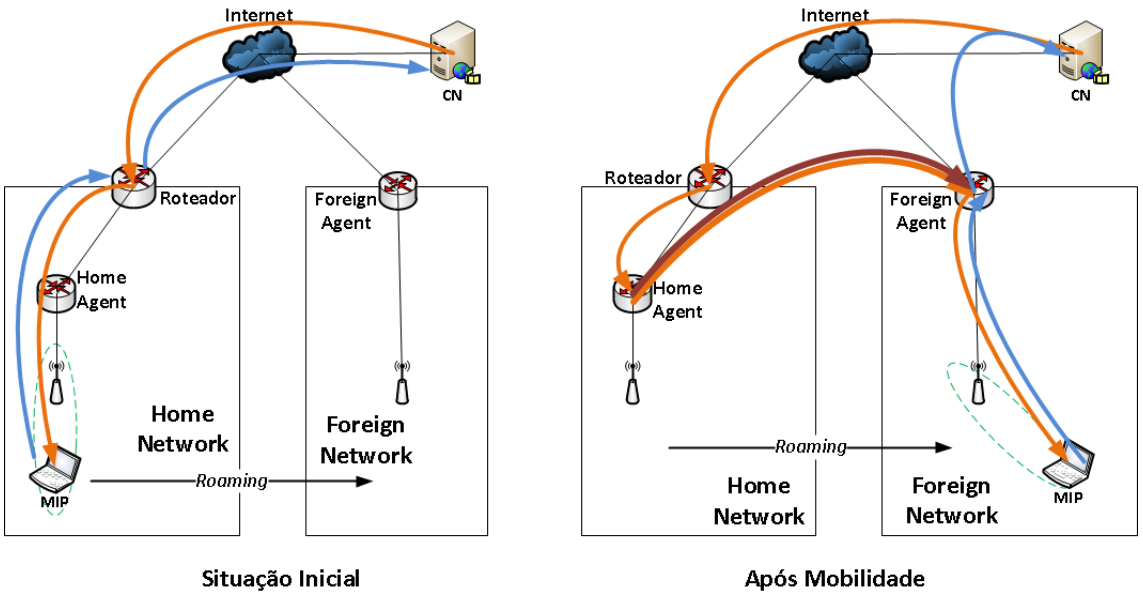

Figura 2.2. Mobilidade usando *Mobile IP*.

1) O MN se desassocia do dispositivo Wi-Fi da sua HN e se associa ao dispositivo WiFi da *Foreign Network* (FN);

2) Na FN, o MN recebe o endereço IP da FN -CoA-, via DHCP;

3) Com esse novo endereço IP, o MN solicita registro ao *Foreign Agent* da associação <HoA:CoA>;

4) O FA se registra com o HA;

5) Após o registro, é criado um *Mobility Binding* entre o HoA e o CoA no HA;

6) O HA cria um túnel entre ele e o FA;

7) O FA envia a confirmação para o MN e, a partir desse momento, todo pacote entre o MN e um dispositivo externo (CN) serão encaminhados por esse túnel.

É possível observar que existem diversos pontos negativos nesse modo de funcionamento:

- Exige que todo MN tenha um HA em sua rede de origem;

- Em redes que possuem filtro de pacote baseado no endereço IP de origem, o FA deve encaminhar todos os pacotes do MN para o HA, via túnel, criando atraso na entrega do pacote;

- Em redes que não possuem filtro de pacotes baseado no endereço IP de origem, existe assimetria de tráfego, ou roteamento triangular, pois todo tráfego destinado ao MN precisa primeiro ir para o HA, depois para o FA e depois ser entregue ao MN. Porém no sentido oposto, o MN pode enviar os pacotes diretamente para o CN, fazendo com que o caminho de ida e volta sejam diferentes, dificultando resolução de problemas e aplicação de QoS;

- O HA pode ter problemas de escalabilidade caso existam muitos MN na HN;

- *Handover* extremamente alto, com tempos superiores à 200 ms para a convergência, como pode ser visto em [Ergen et al., 2002], [Diab, 2004] e [Rathi and Thanushkodi, 2009], inviabilizando aplicações multimídia, sensíveis a perda de pacotes [ITU-T, 2000].

Apesar disso, diversos trabalhos têm sido publicados para tentar melhorar o funcionamento do MIP, e algumas soluções foram incorporadas no MIPv6 [Johnson et al., 2004], mas como o funcionamento do MIPv6 e do IPv6 [Deering and Hinden, 1998] são similares ao IPv4 na sua concepção, muitas das dificuldades acima listadas se aplicam ao MIPv6.

Na subseção a seguir, serão apresentados os conceitos pertinentes ao *Border Gateway Protocol*(BGP)[Rekhter and Li, 1995], que é o responsável pelo roteamento dos pacotes IP na Internet.

2.3 BORDER GATEWAY PROTOCOL

A Internet, enquanto uma rede de computadores, é o conjunto de diversas redes distintas, composta por provedores de trânsito, provedores de acesso de usuários e provedores de conteúdo -chamados de Sistemas Autônomos (ou *Autonomous Systems*)- usando um

protocolo roteado comum, o *Internet Protocol* (IP). Para permitir que os pacotes IP sejam roteados pela Internet, é necessário que exista um protocolo de roteamento conectando os diversos sistemas autônomos envolvidos. Atualmente, o protocolo utilizado é o *Border Gateway Protocol* - BGP [Rehkter, 1995] que contém em sua tabela todos os prefixos IP utilizados pelos provedores que compõem a Internet, a fim de realizar o roteamento dos pacotes.

O protocolo BGP funciona através de sessões BGP estabelecidas entre os roteadores de borda dos sistemas autônomos, sendo estas sessões estabelecidas chamadas de *peerings* BGP. Cada *peer* da sessão BGP possui sua própria política de roteamento, e esta política define quais prefixos IP o *peer* irá divulgar e o que fazer com os prefixos recebidos do outro *peer*. É através desta política que caracteriza-se um sistema autônomo como um provedor de trânsito -que divulga todos os prefixos recebidos de todos os *peers*- ou provedor de usuários e/ou conteúdo -que divulga apenas prefixos IP utilizados internamente no provedor. No contexto do protocolo BGP, cada sistema autônomo é identificado de maneira única na Internet, através de um número chamado de *Autonomous System Number*, ou ASN. A fim de apresentar simplificadamente o funcionamento do protocolo BGP, considere a Figura 2.3. Nela pode-se observar três sistemas autônomos, representados pelos ASNs 10, 20 e 30.

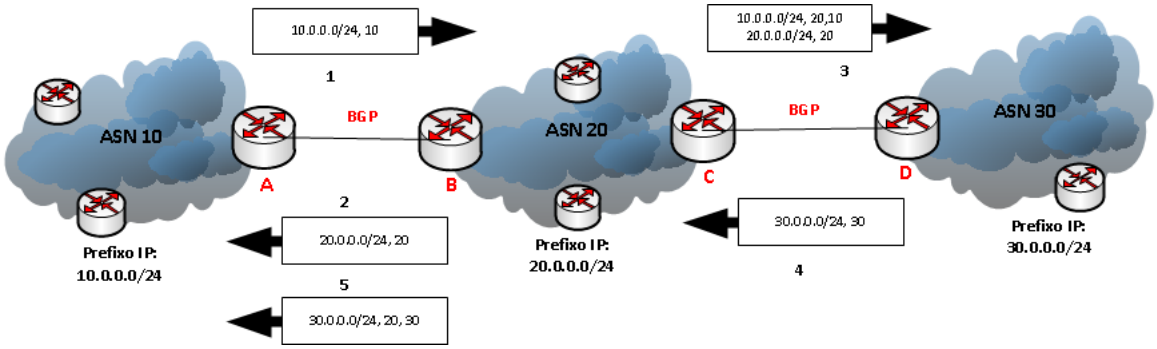

Figura 2.3. Funcionamento do protocolo BGP.

- Passo 1: No primeiro momento, os roteadores de borda dos ASNs 10 (**A**) e 20 (**B**) estabelecem uma sessão BGP, e através desta sessão, o roteador **A** envia uma mensagem BGP para o roteador **B** com o prefixo IP alocado ao mesmo e o seu

ASN, neste caso, "**10.0.0.0/24, 10**". O envio do ASN é fundamental para criar o **AS-PATH**, ou seja, informar por quais provedores um pacote IP irá passar para chegar no prefixo IP do AS 10. Como o prefixo **10.0.0.0/24** está alocado ao próprio AS 10, o AS-PATH é representado apenas pelo ASN, neste caso, 10;

- Passo 2: Após ter a sessão BGP estabelecida, o roteador **B**, assim como roteador **A**, envia uma mensagem BGP com o prefixo IP alocado ao mesmo e o seu ASN, neste caso, "**20.0.0.0/24, 20**". Como no Passo 1, o roteador que envia a mensagem BGP precisa informar o AS-PATH, e para isso, envia seu próprio ASN, uma vez que o prefixo IP **20.0.0.0/24** está alocado ao mesmo;

- Passo 3: Em um segundo momento -que pode ser após a criação de uma conexão física entre os roteadores **C** e **D**- o roteador **C** estabelece uma sessão BGP com o roteador **D**, e envia uma mensagem BGP com o prefixo IP alocado ao mesmo e o AS-PATH para alcançá-lo, neste caso, "**20.0.0.0/24, 20**". Além disso, uma vez que o AS 20 é um sistema autônomo de trânsito, o mesmo envia, através da mensagem BGP, o prefixo IP do AS 10 e o AS-PATH, porém, neste caso, o AS 20 deve alterar o AS-PATH adicionando seu próprio ASN ao mesmo, resultando no AS-PATH "**20,10**". Com isso, o roteador **D** saberá que, ao enviar um pacote IP com destino à rede **10.0.0.0/24**, o mesmo irá passar primeiramente pelo AS 20 e, em seguida, pelo AS 10;

- Passo 4: Também após o estabelecimento da sessão BGP, o roteador **D** envia a mensagem BGP para o roteador **C** com a seguinte informação: prefixo **30.0.0.0/24**, AS-PATH 30;

- Passo 5: Ao receber a mensagem BGP do roteador **D**, o roteador **C** envia uma mensagem BGP para o roteador **B**, ambos pertencentes ao mesmo AS, e então o roteador **B** envia para o roteador **A** o novo prefixo IP recebido, adicionando ao AS-PATH seu próprio ASN: prefixo **30.0.0.0/24**, AS-PATH 20,30.

- Após este momento, cada sistema autônomo possuirá os prefixos IP dos demais e

assim, poderão fazer o roteamento dos pacotes entre eles.

No cenário demonstrado na Figura 2.3, os sistemas autônomos envolvidos não precisam fazer uso de técnicas de engenharia de tráfego, uma vez que todas as conexões são únicas. Porém, na Internet, muitos provedores fazem uso de duplas conexões com outro provedor ou mesmo conexões para provedores diferentes. Esta técnica é conhecida como *multihoming* BGP, e é útil para eliminar pontos únicos de falha, uma vez que é possível convergir o tráfego de uma conexão para outra em caso de queda da conexão ou mesmo de provedor. A Figura 2.4 exemplifica um cenário onde o AS 20 possui duas sessões BGP, com provedores distintos, a fim de garantir redundância para acesso à Internet.

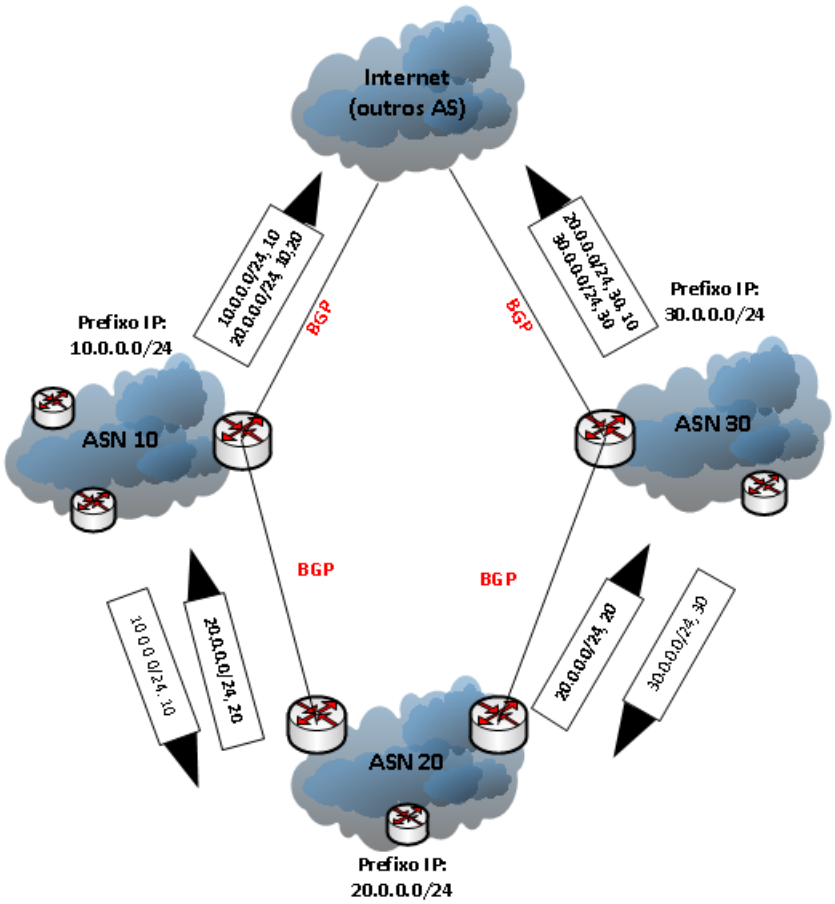

Figura 2.4. Sistema autônomo conectado com *multihoming*.

Neste cenário, o AS 20 envia seu prefixo **20.0.0.0/24** para ambos os AS 10 e AS 30 e ambos funcionam como provedores de trânsito, logo os mesmos repassam para outros

provedores na Internet o prefixo recebido. Porém, nesse cenário, quando um pacote IP originado em um AS na Internet é enviado para o AS 20, este possui duas abordagens para controlar por qual conexão ele deseja receber o pacote:

1) Via manipulação do AS-PATH: nesta abordagem, o AS 20 poderia fazer uma adição ao AS-PATH enviado para um dos provedores, concatenando seu ASN mais uma vez. Desta maneira, o AS 20 enviaria a mensagem BGP para um provedor com AS-PATH "20,20" e para o outro, apenas "20". Com isso, os AS 10 e AS 30 enviariam o pacote para o AS com o menor AS-PATH. Esta abordagem utiliza apenas recursos de engenharia de tráfego do BGP, sendo considerada mais simples de implementar, porém menos eficiente, como será explicado a seguir. Além disso, esta abordagem estaria redirecionando **todo** o tráfego por apenas um provedor;

2) Via fragmentação de prefixos: nesta abordagem, supondo que o AS 20 queira manipular o tráfego de entrada, onde os pacotes destinados ao prefixo **20.0.0.0/25** ele deseja receber via conexão com AS 10 e pacotes destinados ao prefixo **20.0.0.128/25** ele deseja receber via conexão com o AS 30, o mesmo precisará manipular as políticas BGP, fazendo anúncios mais específicos para cada provedor. Este cenário pode ser observado na Figura 2.5.

Na Figura 2.5, é possível observar que o AS 20 está fazendo balanceamento de carga através da fragmentação de prefixos, fazendo com que o tráfego destinado ao prefixo IP **20.0.0.128/25** seja encaminhado via AS 10 e tráfego destinado ao prefixo IP **20.0.0.0/25** seja encaminhado via AS 30. Isso ocorre pois todos os roteadores IP, por padrão, sempre enviam pacotes para a interface que possui a rota para o prefixo mais específica em sua tabela de rotas. Neste caso, um prefixo "/25" é mais específico que um "/24". Os critérios de desempate do BGP, como por exemplo, menor AS-PATH, só funcionam no momento em que ambos os prefixos possuem mesmo tamanho.

Utilizando a técnica de fragmentação de prefixos IP, um provedor consegue forçar que o tráfego seja redirecionado da maneira mais conveniente, porém adiciona mais prefixos nas

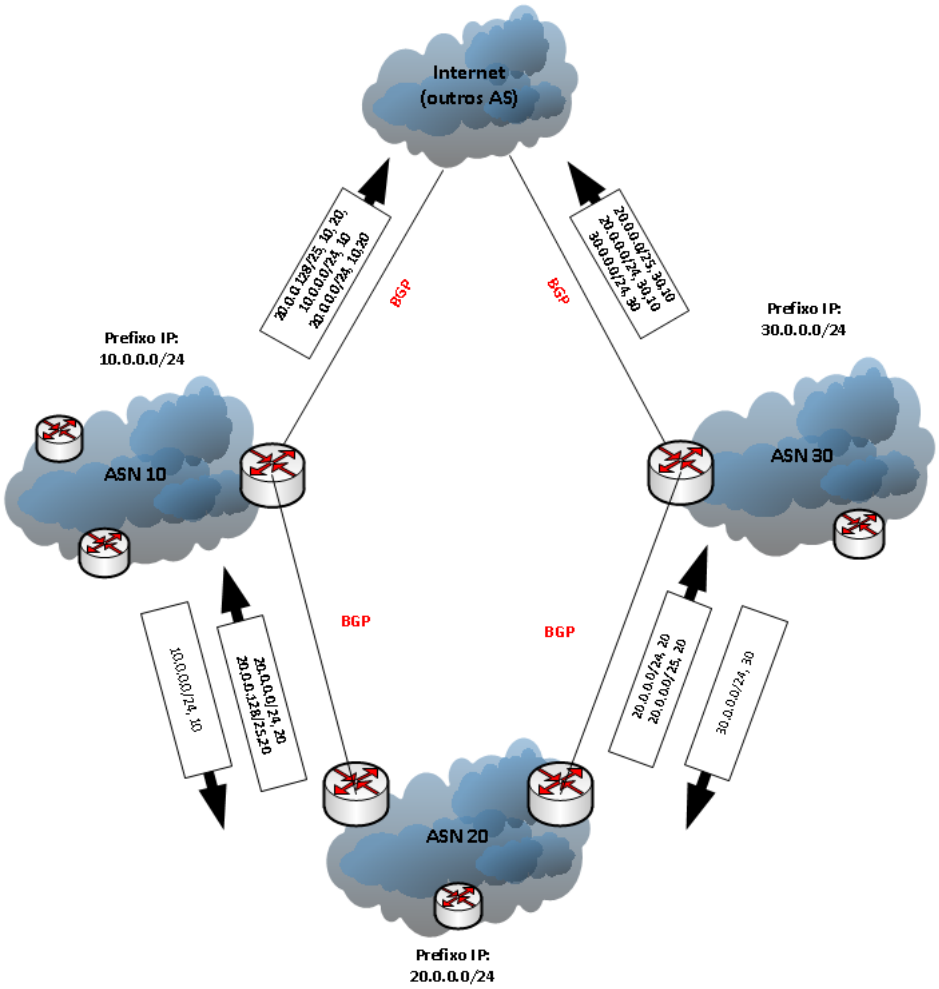

Figura 2.5. Fragmentação de prefixos usando BGP

tabelas de roteamento dos outros sistemas autônomos na Internet. Por exemplo, um AS qualquer na Internet possuirá na sua tabela de rotas uma rota para o prefixo **20.0.0.0/24**, uma para o prefixo **20.0.0.0/25** e mais uma para o prefixo **20.0.0.128/25**, totalizando três rotas para um único AS de destino. Essa adição de diversos prefixos fragmentados na Internet tem gerado preocupações na IETF com relação à escalabilidade das tabelas de roteamento da Internet, que tem crescido exponencialmente, e esta preocupação e uma possível solução estão detalhado na Seção 2.4.

2.4 INTERNET DO FUTURO

Segundo [Carpenter, 2009], de 1994 até 2009, a tabela BGP da Internet cresceu exponencialmente, em decorrência, principalmente, da engenharia de tráfego utilizando fragmentação de prefixos pelos Sistemas Autônomous, conforme explicado anteriormente. Esse crescimento pode ser observado na Figura 2.6[2], já atualizada até 2012, e pode, em breve, se tornar um problema para a escalabilidade da Internet. Diante desta observação, no encontro da *Internet Architecture Boarding* (IAB) (entidade responsável pela condução de novos temas relacionados à Internet dentro da *Internet Society*) de 2006, este assunto foi foco da reunião e, conforme foi mencionado anteriormente, foi produzido o documento *Report from the IAB Workshop on Routing and Addressing* [Meyer et al., 2007], solicitando prioridade dos participantes na busca por soluções a fim de evitar problemas futuros. Desde este encontro da IAB, diversos grupos de pesquisa têm apresentado propostas com enfoque, principalmente, na separação de *namespaces* da Internet [Bonaventure, 2007], remontando ao fato de que a sobrecarga de semântica do protocolo IP é o principal motivo para este crescimento da tabela BGP, o que já havia sido evidenciado em [Saltzer, 1993].

Essa separação de *namespaces* proposta para a Internet funcionaria da seguinte maneira: os roteadores que estariam no núcleo da Internet teriam apenas os prefixos IP nas suas tabelas BGP pertinentes ao próprio núcleo da Internet, os roteadores das redes dos usuários teriam acesso apenas aos endereços da rede do usuário e os equipamentos de bordas teriam o papel de fazer as correlações (ou mapeamentos) necessárias para identificar para qual roteador encaminhar os pacotes. Esta abordagem, resolvendo o problema de sobrecarga de semântica do protocolo IP na Internet, é conhecida como "Internet do futuro" nos trabalhos apresentados na IETF [Bonaventure, 2007].

Na Figura 2.7 está ilustrada a nova arquitetura da Internet, criando os dois *namespaces*: *Egde Space* e *Transit Space* ou Espaço de Usuário e Núcleo. No *Site 1*, o *host SRC* deseja se comunicar com o *host DST* do *Site 2*. Os roteadores internos do *Site 1*

[2]Projeto Route-Views - http://www.cidr-report.org

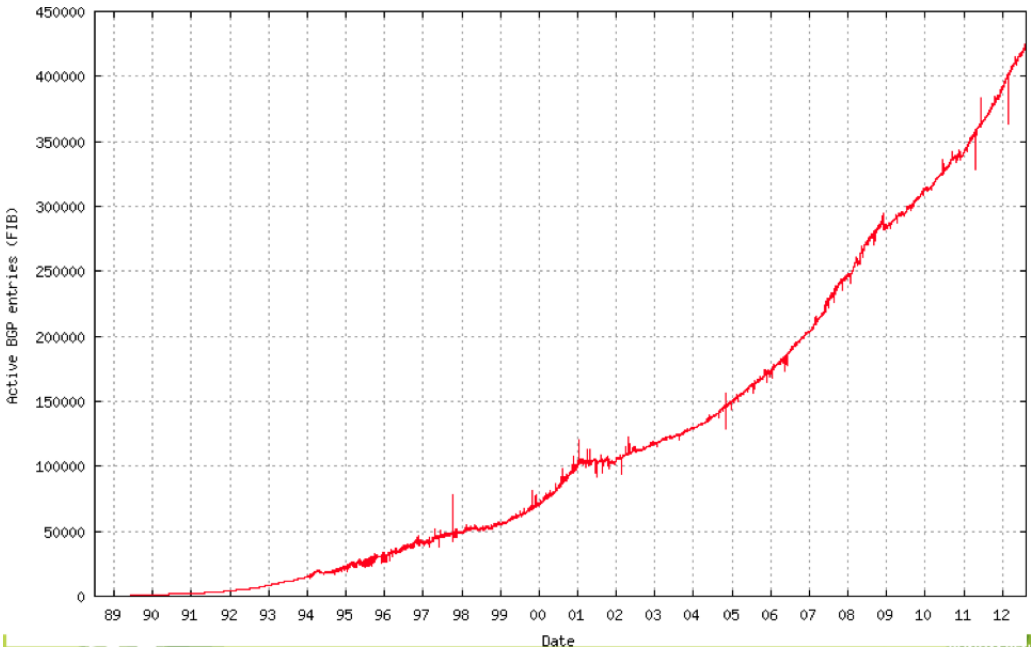

Figura 2.6. Crescimento da tabela BGP de 1989 até os dias atuais.

apenas possuem nas suas tabelas de roteamento a informação que os pacotes devem ser encaminhados aos roteadores de borda. O funcionamento seria o seguinte:

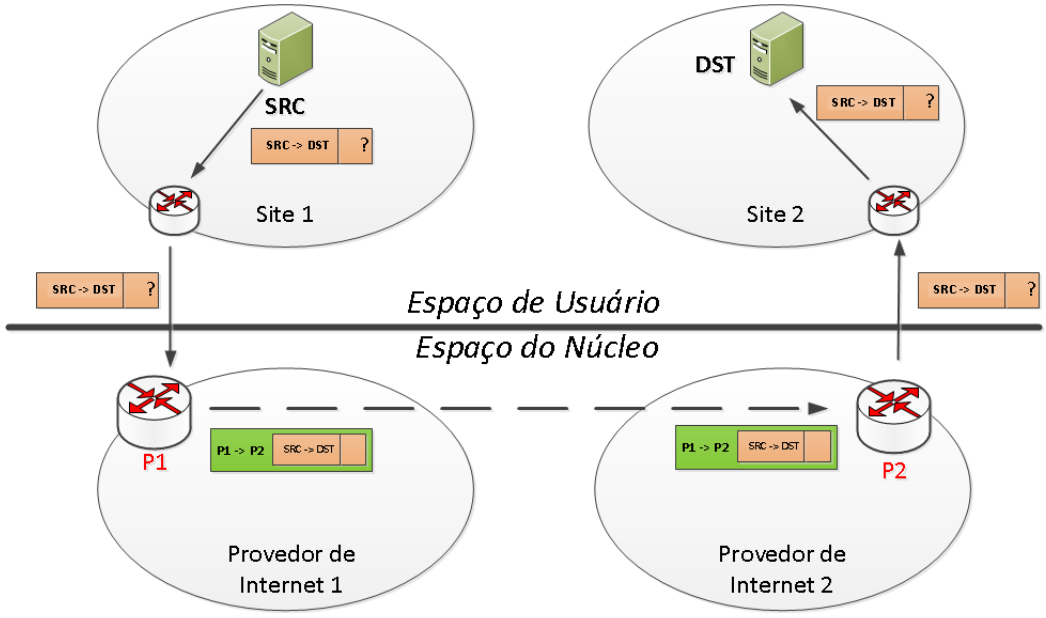

Figura 2.7. Funcionamento da Internet com separação de *namespaces*. Traduzido de [Jen et al., 2008]

1) O *host SRC* envia o pacote IP para o roteador da sua rede tendo como destino o

host DST no Site 2;

2) O pacote é roteado por todos os roteadores da rede interna até chegar no roteador de borda do usuário. Este envia para o roteador de borda do provedor de Internet, no caso P1;

3) O roteador de borda P1, então, consulta sua tabela de mapeamento para correlacionar o endereço *DST* com o roteador de borda apropriado do usuário remoto. Neste exemplo, o roteador P1 obteve a informação que o roteador P2 é responsável pelo endereço *DST*.

4) De posse do endereço do roteador P2, o roteador P1 encapsula o pacote IP em outro pacote IP (Figura 2.8), com endereço IP de origem P1 e destino P2;

5) Os roteadores do núcleo da Internet roteiam o pacote até o roteador P2;

6) O roteador P2 recebe o pacote e verifica que o destino é ele mesmo, então ele desencapsula o pacote, e observa o endereço de destino deste pacote encapsulado, neste caso *DST* e encaminha para o roteador de borda do usuário remoto;

7) O *host DST* recebe o pacote, trata o conteúdo e responde ao *host SRC*, e o processo se repete até que o pacote chegue ao *host SRC*.

Neste modo de funcionamento é observado que não há sobrecarga de semântica no protocolo IP, uma vez que agora o endereço IP é utilizado apenas para identificar os usuários, não mais servindo de localização. Seguindo esta abordagem, diversos protocolos foram propostos, e aquele com maior grau de maturidade e com rede de testes mundial é o *Locator/ID Separation Protocol*, ou LISP [Farinacci and Fuller, 2012]. O LISP, devido ao seu grau de desenvolvimento, possui um grupo de trabalho na IETF[3] e uma rede de testes mundial disponível para interessados[4]. Mais detalhes sobre o protocolo LISP serão apresentados na Seção 2.5 *LISP*.

[3]http://datatracker.ietf.org/wg/lisp/charter/
[4]http://www.lisp4.net

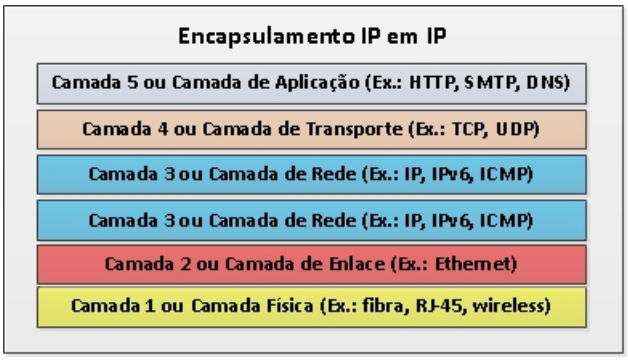

Figura 2.8. Encapsulamento IP em IP na Pilha TCP/IP.

2.5 LISP

O *Locator/ID Separation Protocol* ou LISP [Farinacci and Fuller, 2012] é uma das propostas existentes para resolver o problema de escalabilidade da Internet apresentado em [Bonaventure, 2007], cujo foco reside apenas na camada de rede, sem necessidade de alteração nos *hosts*. Atualmente, o LISP possui um grupo de trabalho dedicado no IETF, cujo foco é estudar a proposta original, propor alterações, discutir tópicos de segurança, funcionalidade, aplicações e escalabilidade.

Este problema de escalabilidade, conforme apresentado nas seções 2.3 e 2.4, deve-se ao fato de que os Sistemas Autônomos (ou *AS - Autonomous System*) de usuários e conteúdos utilizam das funcionalidades do protocolo BGP para fazerem suas políticas de engenharia de tráfego, geralmente fazendo uso da fragmentação dos prefixos IP. Essa fragmentação de prefixos faz com que a tabela de roteamento global, contida nos roteadores do núcleo da Internet, conforme Figura 2.6, cresça exponencialmente, o que comprometerá o crescimento da Internet. O LISP visa, neste contexto, fazer com que os prefixos IP utilizados pelos Sistemas Autônomos de usuários e conteúdos sejam removidos dos roteadores do núcleo da Internet, permitindo que apenas os prefixos IP responsáveis pelo roteamento na Internet constem nesses, diminuindo o processamento necessário para o roteamento dos pacotes IP.

Uma vez removidos do núcleo da Internet, estes prefixos IP passam a fazer parte de um sistema de mapeamento que será responsável por associar o prefixo IP do usuário ao

endereço IP do roteador responsável por aquele Sistema Autônomo. Na nomenclatura do protocolo LISP, os dispositivos necessários para fazer o mapeamento são chamados de Servidores de Mapeamento ou *Map-Servers* e os roteadores que compõem o núcleo da Internet são chamados de *Routing Locators* ou RLOC. Além disso, outros componentes fazem parte de uma rede com suporte ao LISP:

- Domínio LISP: rede de computadores composta por dispositivos que suportam o protocolo LISP;
- *Endpoint IDentifiers* ou EID: endereços IP utilizados para representar os Sistemas Autônomos dos usuários e conteúdos, sendo estes endereços removidos do núcleo da Internet;
- Pacote LISP: pacote IP original encapsulado em outro pacote IP/UDP/LISP, conforme Figura 2.9. Nesta é possível observar que o pacote IP mais externo contém os endereços IP RLOC de origem e destino, além do protocolo UDP e o cabeçalho LISP. O cabeçalho IP encapsulado contém como endereços IP de origem e destino, os endereços EID;
- *Ingress Tunnel Router* ou ITR: RLOC responsável por consultar os *Map-Servers* a fim de descobrir qual o RLOC responsável pelo prefixo IP de destino, encapsular o pacote IP em um pacote LISP e enviar para o RLOC de destino;
- *Egress Tunnel Router* ou ETR: RLOC responsável por receber o pacote LISP enviado pelo ITR, desencapsular o mesmo e enviar para o endereço IP de destino;
- *xTR*: RLOC que funciona como ETR e ITR;
- *Map-Resolver*: RLOC que possui a funcionalidade de consultar os *Map-Servers* a fim de identificar o ETR para o qual deve enviar o pacote LISP;
- *MR-MS*: Dispositivo que funciona como *Map-Resolver* e *Map-Server* ao mesmo tempo;

- *Proxy ITR* ou PITR: RLOC responsável por receber um pacote IP da Internet atual e enviar para um domínio LISP;
- *Proxy ETR* ou PETR: RLOC responsável por enviar um pacote IP de um domínio LISP para a Internet atual;
- *PxTR*: RLOC que funciona como PETR e PITR.

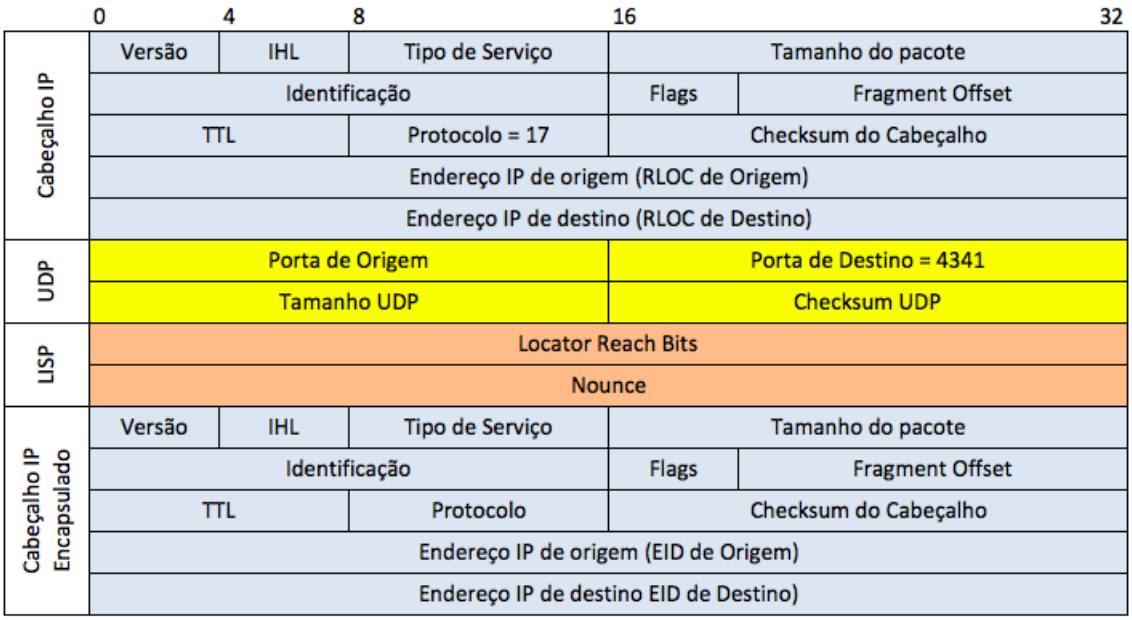

Figura 2.9. Encapsulamento LISP detalhado.

O funcionamento do LISP segue a abordagem *map-and-encap* [Deering, 1996], ou seja, o ITR antes de enviar o pacote para o ETR, consulta o *MR-MS* para saber qual é o endereço do ETR responsável pelo EID de destino. Caso a resposta do *MR-MS* não seja negativa, o ITR encapsula o pacote IP em um pacote LISP e envia para o próximo RLOC. Caso a resposta seja negativa, o ITR encaminha o pacote da forma tradicional, sem encapsulamento LISP. Na Figura 2.10, todo o processo é detalhado.

1) Após uma consulta DNS, por exemplo, o dispositivo com endereço IP "EID 1" envia um pacote IP da maneira tradicional para o endereço IP "EID 2". Este pacote IP pode estar transportando um pacote de voz utilizando como protocolo de transporte, o protocolo UDP;

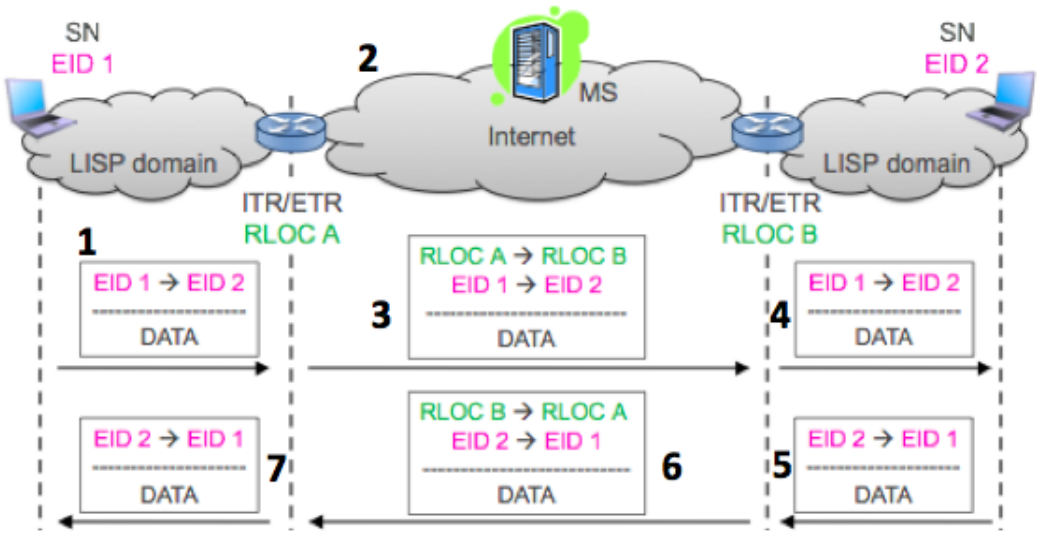

Figura 2.10. Funcionamento do LISP: comunicação entre dois domínios LISP. Fonte: [Menth et al., 2010]

2) Este pacote chega até o roteador ITR do domínio LISP de origem, que consulta o *Map-Server*(MS) pelo endereço IP do RLOC responsável pelo prefixo "EID 2". O MS retorna o endereço IP "RLOC B";

3) O ITR então guarda em sua memória *cache* a associação <EID 2,RLOC B> para uso futuro, encapsula o pacote IP original em um pacote LISP, onde o endereço IP de destino é "RLOC B" e o endereço IP de origem é "RLOC A".

4) O ETR "RLOC B" recebe o pacote IP, guarda em sua memória *cache* a entrada <EID 1, RLOC A>, desencapsula o cabeçalho IP externo e encaminha o pacote IP original para o "EID 2";

5) O dispositivo "EID 2" envia um pacote IP para o roteador da rede com a informação desejada destinada ao dispositivo "EID 1";

6) Este pacote chega até o ITR - que atuou como ETR no Passo 4- que, ao consultar sua memória *cache* pelo RLOC do "EID 1", verifica que deve enviar o pacote LISP para o endereço IP "RLOC A". Sendo assim, o mesmo encapsula o pacote IP num pacote LISP com endereço de destino "RLOC A" e endereço de origem "RLOC B"

e o envia.

7) Ao chegar ao “RLOC A”, o mesmo desencapsula o cabeçalho mais externo e envia o pacote IP original para o “EID 1”.

8) Os Passos de 1 a 7 se repetirão até o fim da comunicação, com exceção que agora o “RLOC A” possui em sua memória *cache* a relação <EID 2, RLOC B> não necessitando mais consultar o *Map-Server*.

Na Figura 2.11 é apresentado o processo de comunicação no momento de transição entre a Internet atual e a Internet baseada no protocolo LISP.

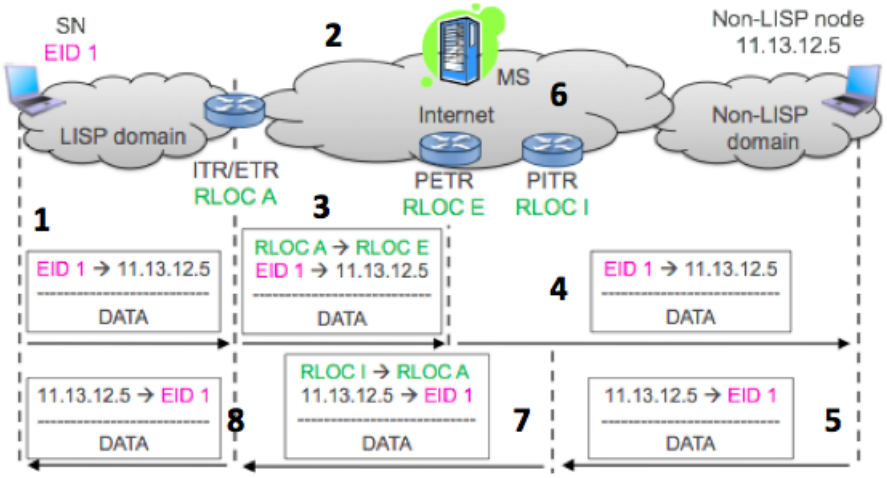

Figura 2.11. Funcionamento do LISP: comunicação entre um Domínio LISP e a Internet atual. Fonte: [Menth et al., 2010]

1) Após uma consulta DNS, por exemplo, o usuário com endereço IP “EID 1” envia um pacote IP da maneira tradicional para o endereço IP **11.13.12.5**;

2) Este pacote chega até o roteador ITR do Domínio LISP, consulta o *Map-Server*(MS). O MS retorna com uma resposta negativa, o que indica para o ITR que o IP de destino não está no Domínio LISP;

3) O ITR então guarda em sua memória *cache* a associação <EID 2,-1> para uso futuro, encapsula o pacote IP original em um pacote LISP, onde o endereço IP

de destino é o "RLOC E" e o endereço IP de origem é o "RLOC A". O endereço "RLOC E" pertence ao *Proxy Egress Tunnel Router* e foi previamente configurado no ITR, de forma estática, pelo responsável do dispositivo;

4) O PETR desencapsula o pacote LISP e envia da maneira tradicional tendo o IP **11.13.12.5** como destino;

5) O dispositivo de destino então envia um pacote de volta, com endereço de destino "EID 1". Na tabela de roteamento global, o PITR está anunciando os prefixos do domínio LISP via protocolo BGP da maneira tradicional, por isso, o pacote IP chegará até o mesmo;

6) Ao receber o pacote IP, o PITR consulta o MS para descobrir qual é o RLOC responsável pelo endereço IP "EID 1" e recebe como resposta o endereço "RLOC A";

7) De posse desse endereço, o PITR encapsula o pacote IP original num pacote LISP, com endereço de destino o endereço IP "RLOC A" e com endereço de origem o endereço IP "RLOC I";

8) Ao receber o pacote, o ETR -que operou como ITR no sentido contrário- desencapsula o pacote e envia ao dispositivo "EID 1".

9) Os Passos de 1 a 8 se repetem até o fim da comunicação, com exceção que agora os RLOCs possuem em suas memórias *caches* os endereços necessários para não mais consultar o MS.

Operando da maneira descrita, onde os prefixos dos usuários não constam mais na tabela BGP global, e sim apenas nos *Map-Servers*, o LISP permite redução de até uma ordem de magnitude desta tabela [Freitas, 2009], economizando CPU dos roteadores, melhorando o tempo de convergência e otimizando o roteamento da Internet.

Na seção a seguir, serão apresentados dois protocolos que possuem correlação com o tema deste trabalho: o *Host Identification Protocol - HIP* e o *Identifier-Locator Network*

Protocol - ILNP. Ambas as soluções apresentam abordagens para eliminar a sobrecarga de semântica do protocolo IP para permitir, entre outras coisas, a mobilidade IP. Além disso, o ILNP também possui foco na escalabilidade da Internet.

2.6 PROTOCOLOS CORRELATOS

Com o propósito de permitir comparativos com o MIP e o LISP, nesta seção serão apresentadas duas propostas em discussão na IETF que contemplam a mobilidade de forma nativa. Apesar de haver trabalhos como [Eddy, 2004], que tentam definir em qual camada da pilha TCP/IP deve estar o foco da mobilidade, vários grupos de trabalho, *drafts* e RFCs existem na IETF, com soluções para permitir que a mobilidade ocorra de forma nativa, tanto na Camada de Rede, quanto na Camada de Transporte e até mesmo na Camada de Aplicação. Além disso, existem trabalhos que, inclusive, propõem uma nova camada, dedicada apenas à identificação dos *hosts*. Na Seção 2.6.1 será apresentado o protocolo HIP - *Host Identification Protocol*, cujo foco é criar uma nova camada para identificação e na Seção 2.6.2 será apresentado o ILNP - *Identifier Locator Network Protocol*, cujo foco está na Camada de Rede.

2.6.1 Host Identification Protocol - HIP

Conforme apresentado na Seção 2.1, a sobrecarga de semântica do protocolo IP é o principal problema para a implementação de mobilidade atualmente, e, os protocolos em discussão na IETF para prover mobilidade focam em resolver essa sobrecarga. Com o crescimento da capacidade computacional dos dispositivos, associado às pesquisas na área de criptografia de chaves públicas, o protocolo HIP [Moskowitz, 2012] tem despontado como uma solução promissora, uma vez que o mesmo funciona utilizando a infraestrutura do IPSEC [Kent and Seo, 2008] e do sistema de chaves pública e privada [Guimaraes et al., 2006] para desassociar a localização da identificação. Os debates em torno do HIP iniciaram em 1999, com Bob Moskowitz, e o protocolo está definido na

RFC 4423[Nikander and Moskowitz, 2006].

2.6.1.1 Modo de funcionamento

A arquitetura do HIP oferece criptografia fim-a-fim, proteção contra certos ataques de negação de serviço, permite mobilidade e *multihoming* para IPv4 e IPv6, além de restaurar a identificação fim-a-fim mesmo na presença de dispositivos NAT no caminho. O foco principal está na criação de uma camada de identificação, chamada de *Host Identity - HI*, conforme Figura 2.12. A HI consiste de uma chave pública de um par de chaves pública e privada. Para que a Camada de Transporte possa fazer uso da HI, é gerada uma *Host Identification Tag - HIT*, que é um *hash* do HI limitado a 128 bits. De posse dessa HIT, toda conexão criada pela Camada de Transporte será associada ao HIT, e não mais ao endereço IP. Dessa maneira, o endereço IP passa a ser meramente utilizado para localização.

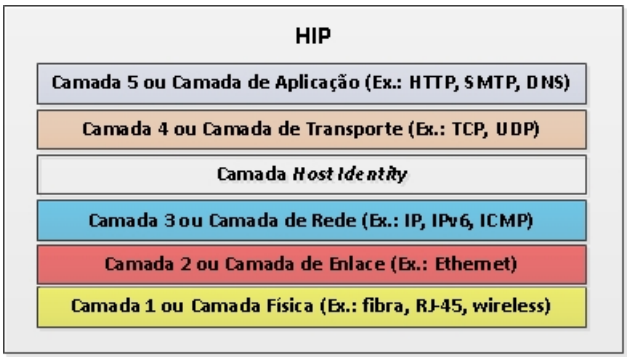

Figura 2.12. Introdução do HIP na pilha TCP/IP.

No HIP, a associação entre o endereço IP e o HI é feito enviando um pacote *Update* para o *Rendezvous Server - RVS*. O RVS funciona como um ponto de gerência de localização, permitindo que dois dispositivos HIP possam fazer mobilidade simultaneamente. Na Figura 2.13 é possível observar o processo de mobilidade do HIP e as etapas são detalhadas a seguir.

1) O dispositivo móvel (**MN**) registra a associação <HI-IP> no *Rendezvous Server*;

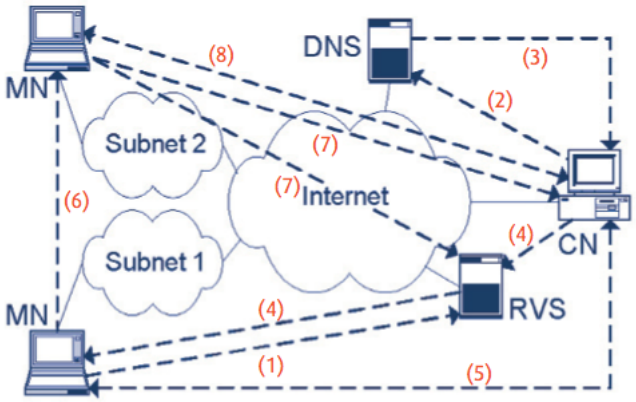

Figura 2.13. Funcionamento do HIP [Martinez, 2008].

2) O *Correspondent Node* (**CN**) inicia a comunicação buscando no servidor *Domain Name System* (DNS)[Mockapetris, 1987] o endereço IP do RVS;

3) O Servidor DNS responde com o endereço IP do RVS;

4) O **CN**, para estabelecer a sessão IPSec com o **MN**, envia uma mensagem IKE Fase 1 para o RVS, que encaminha para o **MN**;

5) O **MN** contacta o **CN** diretamente para estabelecer a sessão IPSec e posteriormente, a conexão de transporte. A partir deste momento, a comunicação é criptografada fim-a-fim;

6) O **MN** move da *Subnet 1* para a *Subnet 2*, obtendo endereço IP local da rede *Subnet 2* via DHCP, por exemplo;

7) O **MN** atualiza o RVS e o **CN** da nova associação <HI-IP> ;

8) A comunicação entre o **CN** e o **MN** volta a ocorrer normalmente.

É possível observar pela Figura 2.13, que não há modificação no encaminhamento dos pacotes (plano de dados), sendo a comunicação a mais direta possível. No plano de controle, existe a necessidade do RVS apenas para localizar o dispositivo desejado, no início da comunicação. No que tange ao desempenho, diversos trabalhos tem sido feitos

para avaliar a complexidade, o custo computacional e o tempo de convergência do HIP, como em [Arraez et al., 2011], [Khurri et al., 2009] e [Bokor et al., 2009].

No contexto da "Internet do futuro", cujo foco é a escalabilidade do núcleo da rede, é possível verificar que, apesar de focar na eliminação da sobrecarga de semântica do IP, o HIP não propõe alterar nenhuma característica do funcionamento do núcleo da Internet. Diante desse fato, o HIP pode funcionar em consonância com o LISP, sem fazer uso do LISP-MN, por exemplo. Além disso, o HIP adiciona a criptografia fim-a-fim, melhorando a segurança da comunicação.

Dentre as principais inconveniências do HIP, estão o ponto único de falha que o RVS representa, além de que o registro DNS não mais representa o dispositivo remoto, e sim RVS associado. Além disso, as aplicações e a Camada de Transporte devem ser alteradas para funcionar com o HIT, e não mais com o endereço IP. Apesar de ter o *Map-Server* como ponto de falha, o LISP-MN não requer alterações nas camadas superiores à Camada de Rede, uma vez que faz uso de endereço IP para a identificação do *host*, utilizando o endereço IP EID.

2.6.2 Identifier-Locator Network Protocol - ILNP

O *Identifier-Locator Network Protocol - ILNP*, definido na RFC 6740[5] é uma proposta para resolver o problema de escalabilidade da Internet, utilizando a abordagem baseada em rede (*network-based*). Para resolver o problema de escalabilidade da Internet, o ILNP propõe que os roteadores de borda dos usuários anunciem apenas os prefixos menos específicos recebidos dos provedores, e façam a engenharia de tráfego através do serviço de mapeamento. Diferentemente do LISP, o ILNP não usa a abordagem de *map-and-encap*, usa a abordagem de reescrita de endereços, onde os roteadores de borda dos domínios, ao invés de consultarem o mapeamento e encapsularem o pacote, consultam o mapeamento e reescrevem os endereços do pacote IPv6. Também diferentemente do LISP, o ILNP funciona apenas para IPv6, onde ocorre a eliminação da sobrecarga de semântica.

[5]ILNP - http://tools.ietf.org/html/rfc6740

Basicamente, o ILNP separa o endereço IPv6, que possui 128 bits, em duas partes: *Locator* (primeiros 64 bits) e *Identifier* (últimos 64 bits), conforme Figura 2.14. Como o próprio nome indica, o *Locator* tem a função apenas de localização do *host*, possuindo utilidade apenas na rede da qual faz parte, enquanto que o *Identifier* é utilizado para identificar exclusivamente aquele *host*, permanece o mesmo quando o dispositivo troca de endereço IPv6, e sendo utilizado pela Camada de Transporte para a criação das sessões. Então, em vez de o pacote IPv6 possui um endereço de origem de 128 bits e um endereço de destino de 128 bits, o mesmo passa a possuir: origem-*Locator* e origem-*Identifier*, destino-*Locator* e destino-*Identifier*. Os endereços origem-*Locator* e destino-*Locator* podem ser reescritos pelos roteadores de borda após a consulta ao serviço de mapeamento.

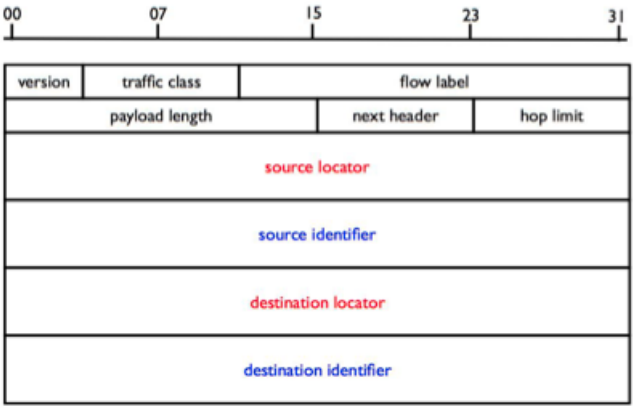

Figura 2.14. Cabeçalho IPv6 modificado pelo ILNP [Atkinson and Bhatti, 2006].

Para resolver o problema de escalabilidade da Internet, o ILNP possui abordagem similar ao LISP, porém, ao invés de utilizar um servidor de mapeamento exclusivo, o ILNP delega este papel aos servidores DNS, com novos tipos de registros de recursos DNS sendo adicionados ao serviço. Uma vez que, assim como o LISP, o funcionamento do dispositivo móvel (MN) é similar ao funcionamento de um Sistema Autônomo, na SubSeção 2.6.2.1 será detalhado o funcionamento do ILNP do ponto de vista do MN.

2.6.2.1 Funcionamento da mobilidade

O funcionamento do ILNP depende basicamente dos servidores DNS, tanto do Servidor DNS de encaminhamento (DNS_H) quanto do Servidor DNS Reverso (DNS_R), e ocorre da seguinte maneira:

1) O dispositivo MN, ao conectar-se à rede, recebe um prefixo IPv6 do AR (*Access Router* ou roteador de acesso da rede). Este prefixo IPv6 recebido, L_{IP1}, será utilizado como *Locator* do MN, uma vez que o mesmo autogerou o endereço I_{MN} a partir do endereço MAC, por exemplo;

2) O MN então, para se conectar ao dispositivo CN, busca no DNS pelo nome FQDN do CN para saber o endereço IPv6. O Servidor DNS responde informando o *Locator* L_{CN} e o *Identifier* I_{CN};

3) Supondo que o MN deseja estabelecer uma conexão TCP para porta 80 (HTTP), o mesmo escolhe uma porta de origem válida (P_{Ori}) e gera o seguinte pacote: <TCP:I_{MN},P_{Ori},I_{CN},80><ILNP: L_{IP1},L_{CN}>. Este pacote é, então, enviado para o CN;

4) Ao chegar ao roteador de borda, chamado de SBR (*site-border router*), o mesmo pode (1) reescrever o endereço IPv6 de origem, colocando o seu endereço *Locator* no lugar do endereço de *Locator* do MN[6] ou (2) manter o pacote da forma original. Após isso, o pacote é enviado ao destino;

5) O CN responde ao MN e a conexão é estabelecida.

Supondo que após um determinado momento, ocorre o processo de mobilidade do MN, enquanto ocorre a comunicação com o CN. Esse processo de mobilidade ocorre conforme ilustrado na Figura 2.15.

[6]Essa reescrita ocorre caso haja NAT ou políticas de engenharia de tráfego

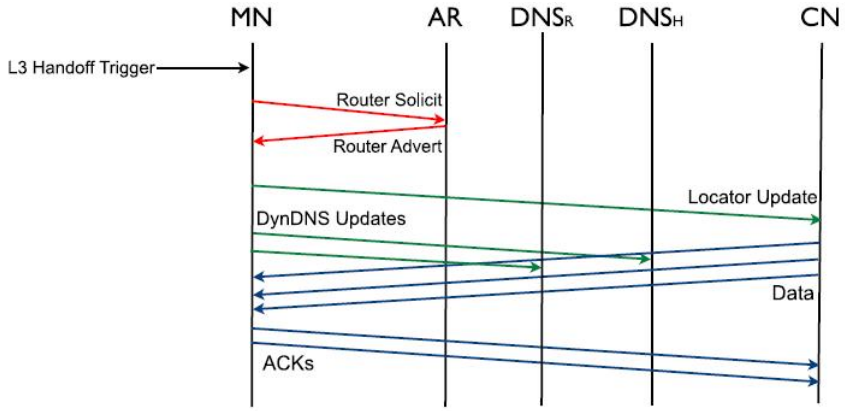

Figura 2.15. Troca de mensagens pelo MN no ILNP [Atkinson et al., 2009].

1) Ocorre o processo físico da mobilidade, fazendo com que o processo de *handoff* (ou *handover*) inicie, e o MN solicite um novo endereço IPv6 ao AR da rede de destino. O AR envia então o prefixo utilizado na rede local, que será utilizado pelo MN apenas para localização (R_{L2}), uma vez que o endereço de identificação I_{MN} permanece o mesmo;

2) De posse do novo endereço IPv6, o MN envia um pacote ICMP *Update* para o CN informando a nova associação $<I_{MN},L_{IP2}>$, e envia um DNS *Update* para forçar o Servidor DNS a também atualizar a associação $<I_{MN},L_{IP2}>$.

3) A partir da atualização do CN, a comunicação é reestabelecida e, a partir da atualização dos servidores DNS, novas conexões podem ser iniciadas.

É possível observar que não existe nenhuma entidade extra no plano de dados, sendo assim, a comunicação utiliza o menor caminho. No plano de controle, existem apenas os servidores DNS, que apenas informam os registros **L** e o **I** associados a um determinado FQDN. Pelo fato do ILNP não usar a abordagem *map-and-encap*, o mesmo não aumenta o tamanho do pacote, evitando problemas de MTU. Porém, devido ao uso da reescrita de endereço, é fundamental que os dispositivos façam uma autenticação no estabelecimento das conexões, e esta autenticação pode gerar um atraso no início da comunicação. Além disso, o ILNP obriga que as aplicações sejam alteradas para fazerem uso do **Identifier**, e algumas delas podem parar de funcionar, como o FTP e o SNMP[Atkinson et al., 2009].

No capítulo a seguir serão apresentados os conceitos e o funcionamento do *LISP Mobile Node*, que é uma proposta existente no grupo de trabalho do LISP para oferecer suporte à mobilidade para dispositivos IP usando a infraestrutura e conceitos do LISP.

CAPÍTULO 3

LISP MOBILE NODE

Conforme apresentado anteriormente, o esforço que existe hoje para fazer a mobilidade IP funcionar se deve, principalmente, à sobrecarga de semântica do endereçamento IP, onde este representa o identificador e o localizador. Através da abordagem utilizada pelo LISP, que desfaz essa relação, está sendo desenvolvida a especificação do *LISP Mobile Node* ou LISP-MN [Farinacci et al., 2012a]. Esta especificação propõe uma alteração na pilha TCP/IP dos dispositivos móveis, onde os mesmos devem implementar uma parte do protocolo LISP, funcionando como um roteador LISP ETR e ITR (conhecido como xTR) simplificado. Neste capítulo serão apresentados os conceitos que permeiam o funcionamento do LISP-MN, seu modo de funcionamento será detalhado, as vantagens sobre o MIP serão explicitadas e serão mencionadas possíveis inconveniências na especificação do protocolo que tem gerado discussões no grupo de trabalho do LISP.

3.1 CONCEITOS

A especificação do LISP-MN foi feita para atender os requisitos a seguir:

- Permitir que as conexões TCP permaneçam ativas após o *roaming*;
- Permitir que um dispositivo móvel se comunique com outro dispositivo móvel mesmo quando ambos fazem o *roaming* simultaneamente;
- Permitir que os dispositivos móveis possam fazer uso de *multihoming*, ou seja, utilizar várias interfaces de rede e tecnologias ao mesmo tempo;
- Permitir que o dispositivo móvel atue como um servidor de rede sendo acessado normalmente por quaisquer outros dispositivos, inclusive móveis;

- Prover o menor caminho bidirecional no plano de dados[1] entre o dispositivo móvel e qualquer outro dispositivo;
- Não exigir rotas mais específicas nas tabelas de roteamento para suportar mobilidade;
- Não exigir a necessidade do *Home Agent*, *Foreign Agent* ou outro dispositivo no plano de dados para suportar a mobilidade;
- Não exigir novas extensões ao cabeçalho IPv6.

Considerando que o LISP-MN faz uso dos componentes do LISP, detalhados na Seção 2.5, as especificações do LISP-MN apenas adicionam os seguintes termos:

- *Stationary Node* ou SN: Dispositivo não-móvel cujo endereço IP troca com pouca frequência;
- *Mobile Node* ou MN: Dispositivo com suporte ao LISP cujo endereço IP troca com frequência;
- *Roaming Event* ou *Roaming*: Alteração do endereço do RLOC do MN;
- *xTR Simplificado*: Implementação simplificada das especificações de ETR e ITR no mesmo dispositivo para suporte à mobilidade.

Na Seção 3.2 serão apresentados diversos cenários onde a mobilidade pode ocorrer, e cada caso será detalhado, a fim de facilitar o entendimento das simulações que serão realizadas no Capítulo 4.

[1]Plano de dados se refere às atividades de encaminhamento de quadros e pacotes nos roteadores e comutadores (*switches*), utilizando as tabelas de encaminhamento geradas pelos protocolos de roteamento, que operam no plano de controle, como por exemplo, a tabela de rotas. No plano de dados, a tabela de rotas é instalada em processadores dedicados à função de encaminhamento de quadros e pacotes.

3.2 FUNCIONAMENTO DO LISP-MN

Um dispositivo LISP-MN é um dispositivo de rede qualquer que possui uma implementação simplificada dos papéis de *Egress Tunnel Router* e *Ingress Tunnel Router*, uma vez que o mesmo sempre envia os pacotes encapsulados em pacotes LISP, com exceção de protocolos de gerência, como ARP, DHCP, etc. Uma outra característica do LISP-MN é o fato de possuir uma interface de rede virtual implementada que recebe o endereço EID, sendo este o endereço que será utilizado pelos protocolos de transporte, desconsiderando o endereço IP da interface física de rede do dispositivo. Essa característica é fundamental para a implementação da mobilidade, uma vez que quando fizer o *roaming*, o endereço IP da interface física irá mudar para usar o endereçamento da rede de destino. Este endereço IP da interface física é o endereço de *Routing Locator* do dispositivo, ou RLOC na terminologia utilizada na especificação do LISP. Porém, ao longo deste trabalho, a fim de evitar confusões com os RLOCs da rede LISP e facilitar o entendimento, será utilizada a nomenclatura utilizada em [Menth et al., 2010], que sugere que o endereço RLOC do LISP-MN seja chamado de *Local Locator* ou LLOC.

3.2.1 Funcionamento do plano de controle do LISP-MN

O funcionamento do plano de controle do LISP-MN se baseia no uso dos *Map-Servers*, uma vez que os mesmos tem a função de informar os RLOCs associados aos EIDs. Como o dispositivo LISP-MN possui um endereço EID associado a sua interface virtual, e o mesmo é uma implementação simplificada do xTR, ele precisa fazer uso do *Map-Server* para informar como seu EID deve ser localizado, ou seja, precisa manter atualizada a entrada <EID,LLOC> neste *Map-Server*. Por isso, a cada vez que o LISP-MN fizer o *roaming*, o mesmo precisará atualizar as entradas <EID,LLOC> do seu *Map-Server* e dos outros RLOCs que estiverem em conversação com o LISP-MN naquele momento.

Além disso, como o LISP-MN possui uma implementação do ETR, o mesmo pode responder as consultas feitas ao seu *Map-Server* interno, ou pode delegar esta função

ao *Map-Server* da sua rede. Esta possibilidade é importante pois evita que o LISP-MN consuma recursos (largura de banda, CPU e energia) ao executar atividades do plano de controle. Caso o LISP-MN opte por delegar esta função do *Map-Server*, todas as vezes que este responder a qualquer ITR ou PITR sobre a entrada <EID,LLOC>, esta resposta será identificada como não-autoritativa, e, desta maneira, o ITR e PITR ficarão sabendo que a resposta não veio do próprio LISP-MN. Isso faz com que sejam criadas entradas individuais para o endereço IP EID nas memórias *cache* dos ITR e PITR, uma vez que, sem esse recurso, os mesmos poderiam criar entradas agregadas impedindo o funcionamento da mobilidade.

Para garantir que a convergência ocorra, ou seja, que os pacotes IP passem a ser encaminhados ao novo LLOC que o LISP-MN possuirá após *roaming*, este precisa atualizar as memórias *cache* dos (P)ITRs. Para isso, o LISP-MN pode utilizar os seguintes métodos:

- *Data Driven SMRs*: um ETR pode enviar um *Solicit Map-Request* (SMR) para o (P)ITR para forçar a atualização da memória *cache* deste;
- Versionamento [Saucez et al., 2012]: se for utilizado, o ETR verifica se o *Map-Version Number* é menor que o valor atual. Caso seja, o ETR envia uma mensagem do tipo SMR para forçar que o ITR atualize sua memória *cache*;
- Escolha de TTLs pequenos: o ETR pode enviar um TTL (*Time-To-Live*) pequeno nas respostas do tipo *Map-Reply* para forçar o (P)ITR a fazer as consultas com relativa frequência;
- Armazenamento temporário de PITR: o ETR pode guardar os endereços dos PITR que enviaram consultas pelo LLOC do LISP-MN, para que quando este for atualizado, enviar um SMR para forçar a atualização das memórias destes.

Utilizando os métodos acima, o LISP-MN fará com que haja a convergência dos pacotes, e a comunicação continue ocorrendo.

3.2.2 Funcionamento do plano de dados do LISP-MN

O plano de dados do LISP-MN foi planejado para que este fosse ponto-a-ponto entre o dispositivo móvel e o outro ponto da comunicação, móvel ou não, ou seja, o LISP-MN não requer nenhum dispositivo extra para fazer o roteamento dos pacotes entre os dispositivos envolvidos. Esta característica é fundamental para evitar atrasos extras na comunicação, o que poderia inviabilizar aplicações de jogos e comunicação interativa (VoIP ou videoconferência, por exemplo). Esta característica só não é atendida em casos onde o dispositivo remoto não está em um domínio LISP. Neste caso, todos os pacotes enviados pelo dispositivo remoto para o LISP-MN serão destinados ao PETR que é a entidade responsável pela comunicação entre as redes atuais e as redes LISP. É opcional para o LISP-MN enviar os pacotes para o PETR quando quiser se comunicar com o dispositivo remoto, mas caso não o faça, estaria criando um roteamento triangular, que pode dificultar técnicas de QoS e resolução de problemas de roteamento, latência e perda de pacotes.

É importante mencionar que, para permitir que o plano de dados funcione ponto-a-ponto, é preciso que haja uma entidade externa que atue como ponto focal para encontrar o dispositivo LISP-MN, que nesse caso é o *Map-Server*. Porém, essa ação de localização é executada no plano de controle, apenas no momento de descobrir onde está localizado o dispositivo móvel.

Outra característica do plano de dados do LISP-MN é o fato de que o LISP-MN sempre enviará pacotes IP encapsulados em pacotes LISP, com exceção da comunicação com os *Map-Servers* e com a rede local da qual faz parte.

3.3 CENÁRIOS

A fim de facilitar o entendimento, serão detalhados três cenários de comunicação envolvendo um dispositivo LISP-MN descritos na especificação do LISP-MN:

3.3.1 Em comunicação com um dispositivo não-móvel (SN) em um domínio LISP

Este cenário está representado na Figura 3.1 e está dividido em três momentos: a situação inicial "A", o *roaming* acontecendo "B"e a situação final "C".

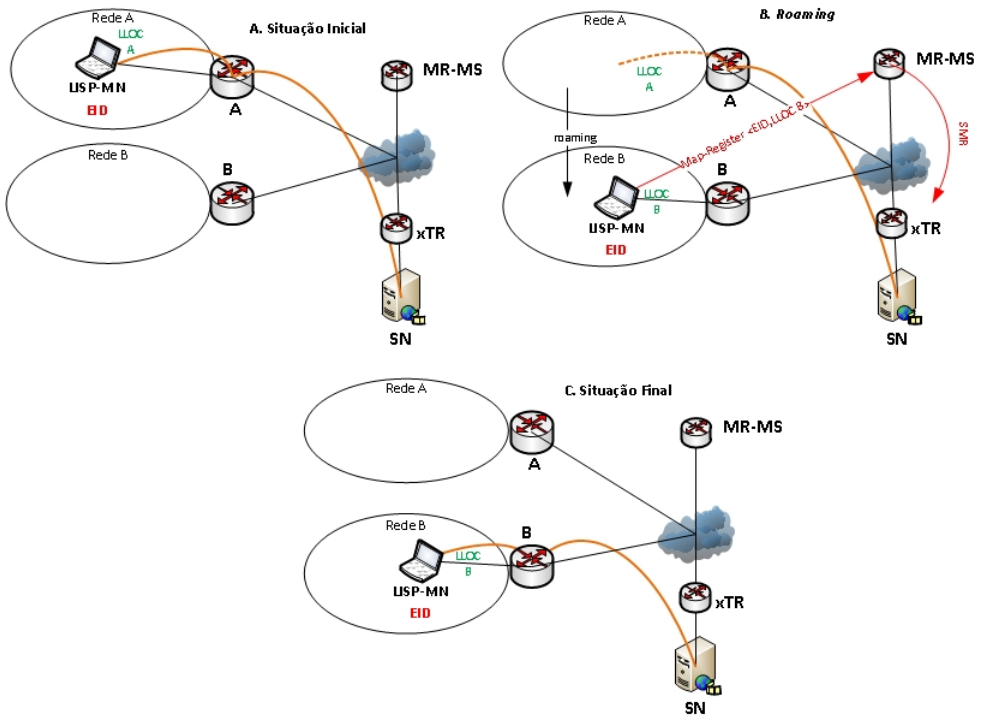

Figura 3.1. LISP-MN em comunicação com SN em um domínio LISP.

No momento "A", o dispositivo LISP-MN está conectado à rede local **A**, e possui um endereço IP **LLOC A** na interface física e o endereço IP **EID** na interface virtual, alocados por DHCP, por exemplo. O dispositivo **SN** faz parte da rede sob controle do roteador xTR, que possui como *Map-Resolver*, o dispositivo *MR-MS*. Neste contexto, é indiferente se o LISP-MN está em um domínio LISP ou conectado à Internet, pois o foco está no LISP-MN, no MR-MS e no xTR.

Supondo que a conexão tenha sido originada pelo **SN**, a mesma ocorreria da seguinte maneira:

1) O **SN** envia um pacote IP para o LISP-MN via o roteador padrão **xTR**, com endereço IP de origem **SN** e endereço IP de destino **EID**;

2) Ao receber o pacote IP, o **xTR** envia um *Map Request* para o **MR-MS** procurando pelo **RLOC** responsável pelo **EID**;

3) O **MR-MS** responde informando que o **RLOC** responsável pelo **EID** é o **LLOC A**. O roteador **xTR** guarda em sua memória *cache* esta informação, encapsula o pacote IP em um pacote LISP, com endereço de origem **xTR** e endereço de destino **LLOC A** e encaminha para o próximo roteador;

4) Roteador por roteador, este pacote chega até o LISP-MN, que remove o pacote LISP e processa o pacote interno;

5) O LISP-MN então responde ao **SN**, com o pacote IP mais interno (encapsulado) possuindo **EID** como endereço IP de origem e **SN** como endereço de destino. O pacote LISP, mais externo, possui como endereço IP de origem **LLOC A** e como endereço IP de destino, o endereço do **xTR**;

6) Ao receber o pacote, o **xTR** desencapsula o pacote IP mais interno e o envia para **SN**. Assim, a conexão comunicação, ilustrada pela linha alaranjada, é estabelecida;

7) A comunicação continua seguindo os passos anteriores, com exceção que não existe mais consultas ao **MR-MS**.

O momento "B"representa o processo de *roaming*, e ocorre da seguinte maneira:

1) O dispositivo LISP-MN se desconecta da rede local A, e se conecta à rede local B, por exemplo, via Wi-Fi. Neste processo de conexão, o LISP-MN recebe um endereço IP da rede local B, o endereço **LLOC B**;

2) Após o LISP-MN perceber a troca de endereçamento na interface física, o mesmo envia um pacote *Map-Register* informando que o **EID** agora está associado ao RLOC **LLOC B**;

3) O MR-MS envia então, um pacote LISP SMR, para forçar o xTR a atualizar sua memória *cache* com o novo RLOC associado ao endereço **EID**.

É possível observar, que, ao longo do processo de *roaming*, o SN continua enviando os pacotes com destino ao endereço **EID**, e o xTR continua enviando para o endereço **LLOC A**, até que o pacote SMR seja recebido e a memória *cache* seja atualizada.

Após a atualização da memória *cache* do xTR, a conexão volta a ocorrer novamente (linha alaranjada no momento "C"), porém agora o xTR encapsula os pacotes com RLOC de destino novo, o endereço **LLOC B**.

3.3.2 Em comunicação com um dispositivo não-móvel (SN) em um domínio não-Lisp

Neste cenário, o LISP-MN precisa fazer uso da infraestrutura de PxTR, pois os pacotes precisam ser encapsulados no retorno do SN para o LISP-MN. A Figura 3.2 apresenta o *roaming* em três momentos: momento "A"com o LISP-MN na sua *Home Network* se comunicando com o SN; momento "B", onde o LISP-MN migra para a *Foreign Network* e notifica o MR-MS; e o momento "C", onde a comunicação é reestabelecida.

No momento "A", o seguinte modo de funcionamento ocorre:

1) Para enviar pacotes IP para o SN, que não está em um domínio LISP, o LISP-MN encapsula o pacote IP em um pacote LISP, tendo como RLOC de destino o endereço **PETR** e como origem **LLOC A**. Para poder enviar este pacote para o PETR, o LISP-MN precisa ser configurado previamente com a informação sobre quem é o PETR que ele poderá utilizar;

2) Após o PETR receber o pacote LISP, o mesmo irá consultar o MR-MS, e irá receber uma resposta negativa deste sobre o fato do SN estar em um domínio LISP. Assim sendo, o mesmo desencapsula o pacote LISP, e envia o pacote interno para o SN, que possui como endereço de origem **EID** e destino **SN**;

3) Para enviar o pacote de volta para o LISP-MN, o SN envia o pacote com endereço de destino **EID**. Este endereço EID faz parte do prefixo IP que o PITR anuncia

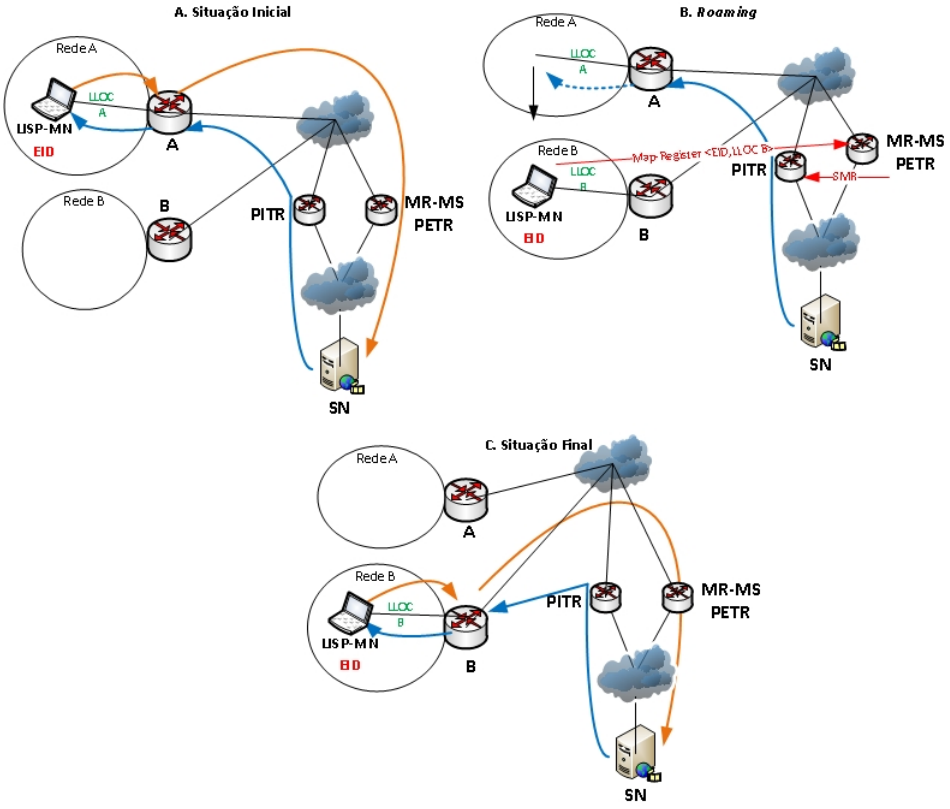

Figura 3.2. LISP-MN em comunicação com SN em um domínio não-LISP.

para a Internet via BGP, logo, este pacote acaba sendo roteado até o mesmo;

4) O PITR então, consulta o MR-MS sobre o endereço RLOC do endereço **EID**, e recebe do *Map-Server* o endereço **LLOC A**;

5) Com essa informação, o PITR encapsula o pacote IP em um pacote LISP e envia para o LISP-MN. A partir deste momento, tanto o PITR quando o PETR possuem em suas memórias *cache* a associação <EID, LLOC A>, não precisando consultar novamente o MR-MS.

No momento "B", o *roaming* acontece, seguindo os seguintes passos:

1) Após o LISP-MN detectar a troca do seu LLOC, saindo de **LLOC A** para **LLOC B**, o mesmo envia um *Map-Register* para o MR-MS, atualizando o registro <EID, RLOC>, com o RLOC sendo o endereço **LLOC B**;

2) Após esta atualização, o MR-MS envia um SMR para os (P)ITRs que o consultaram para forçar também a atualização da entrada nestes;

3) Assim que esta atualização ocorre, o fluxo, representado pelas linhas azul e laranja voltam a ocorrer, como representado no momento "C".

3.3.3 Em comunicação com outro dispositivo LISP-MN

Em caso de uma comunicação entre dois LISP-MN, os três cenários a seguir são possíveis:

- Situação "A": Um LISP-MN em um domínio não LISP e o outro em um domínio LISP;
- Situação "B": Ambos os LISP-MN em domínios LISP distintos;
- Situação "C": Ambos os LISP-MN no mesmo domínio LISP.

O principal diferencial do cenário de comunicação entre dois LISP-MN se deve ao fato que o pacote LISP será encapsulado fim-a-fim, uma vez que a comunicação se dá entre os EIDs.

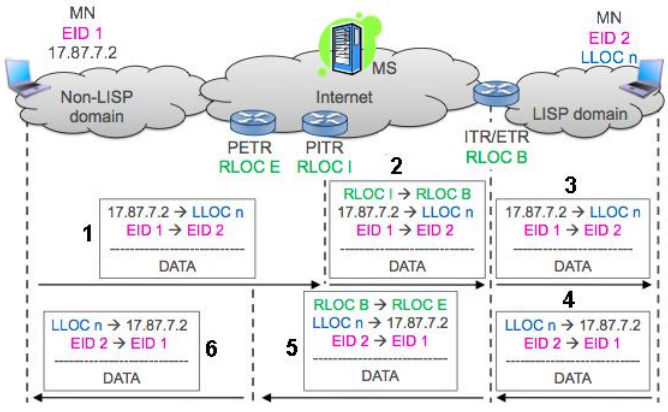

Figura 3.3. LISP-MN fora do domínio LISP e um LISP-MN em um domínio LISP [Menth et al., 2010]

Na Situação "A", representada na Figura 3.3, é possível observar que o que LISP-MN que está fora de um domínio LISP possui o **EID 1** e o LISP-MN em um domínio LISP possui o **EID 2**. Os seguintes passos precisam ocorrer para que esta comunicação funcione:

1) Antes de enviar o pacote para o **EID 2**, o LISP-MN fora do domínio LISP consulta o MR-MS para saber o RLOC do **EID 2**, e recebe como resposta o **LLOC n**. De posse deste valor, ele encapsula o pacote e envia para o **LLOC n**;

2) Porém, como o **LLOC n** faz parte de um domínio LISP, este pacote é roteado até o PITR, que possui RLOC **RLOC I**. Ao receber o pacote, o PITR consulta o MR-MS para saber o RLOC do **LLOC n**, e recebe como resposta o **RLOC B**. Assim sendo, o PITR encapsula o pacote novamente em um pacote LISP e envia para o RLOC B;

3) O RLOC B recebe o pacote, desencapsula o cabeçalho mais externo e encaminha para o LISP-MN;

4) No processo de volta, o LISP-MN envia o pacote para o endereço do LLOC do LISP-MN fora do domínio LISP, cujo endereço é **17.87.7.2**;

5) Ao chegar no RLOC B, este recebe resposta negativa do MR-MS -uma vez que o LISP-MN remoto não está em um domínio LISP-, encapsula o pacote em um outro pacote LISP destinado ao PETR, com RLOC **RLOC E**;

6) O PETR recebe o pacote, desencapsula o cabeçalho LISP mais externo e envia para o LISP-MN;

7) Estes passos irão se repetir ao longo da comunicação, com exceção das consultas ao MR-MS, uma vez que todos os dispositivos LISP guardarão as respostas na memória *cache*.

Na Situação "B", representada na Figura 3.4, é possível observar que não há nenhum PxTR envolvido na comunicação. Neste cenário, temos o LISP-MN com EID **EID 1** e

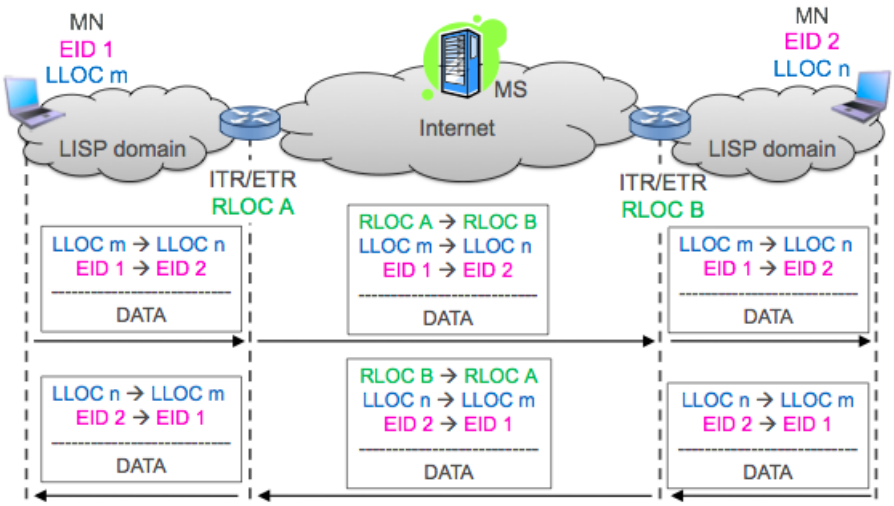

Figura 3.4. LISP-MN em um domínio LISP e um LISP-MN em outro domínio LISP [Menth et al., 2010]

LLOC **LLOC m** no domínio LISP do xTR **RLOC A** e o outro LISP-MN, com EID **EID 2** e LLOC **LLOC n** no domínio LISP do xTR **RLOC B**. Para que a comunicação ocorra, basta que ambos xTR consultem o MR-MS pelo RLOC responsável pelo EID do outro domínio LISP e encapsulem o pacote original em outro pacote LISP, fazendo novamente o pacote ter dois encapsulamentos.

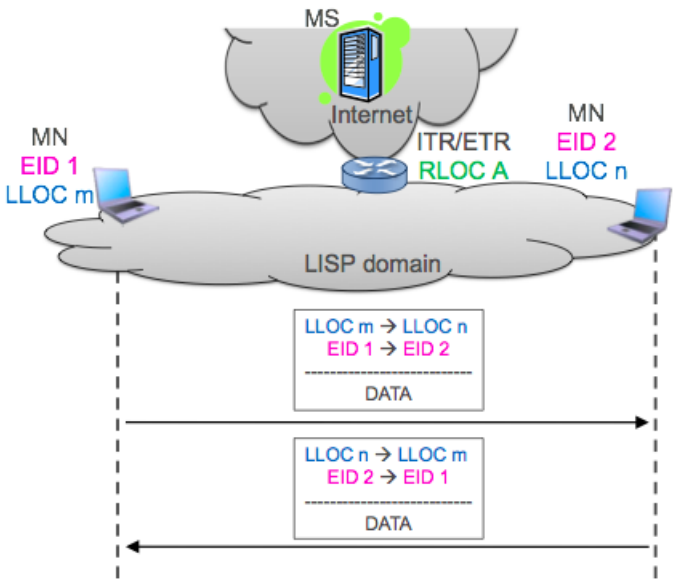

Figura 3.5. Dois LISP-MN no mesmo domínio LISP [Menth et al., 2010]

Por fim, na Situação "C", representada na Figura 3.5, é possível observar que, como ambos LISP-MN possuem LLOCs do mesmo domínio, a comunicação pode ser feita diretamente, porém com o pacote encapsulado usando os endereços de LLOC.

3.4 INCONVENIENTES NA ESPECIFICAÇÃO DO LISP-MN

Verifica-se, a partir dos cenários descritos, que o LISP-MN possui alguns inconvenientes que devem ser tratados pelo grupo de trabalho, entre eles:

1) O LISP-MN requer que a pilha TCP/IP dos *hosts* sejam alteradas, de maneira a suportar o LISP. Como o LISP-MN encapsula todos os pacotes em pacotes LISP, o tamanho do pacote pode superar o tamanho máximo do pacote (MTU - *Maximum Transmission Unit*) das redes locais;

2) Em cenários onde PITR recebe um pacote vindo de um dispositivo SN de um domínio não-LISP (Internet atual), este precisa fazer uma dupla consulta para poder encapsular o pacote para o LISP-MN: primeiro consulta pelo LLOC associado ao EID, depois pelo RLOC associado ao LLOC. Como o PITR não tem como diferenciar *Mobile Nodes* de dispositivos SN, a ativação do suporte para mobilidade força que todas as consultas no PITR sejam executadas essas duas vezes, para confirmar se é um LISP-MN. Esta duplicidade de consultas gera um atraso no início da comunicação, além de uma sobrecarga de CPU, por requer duas consultas para cada nova comunicação a ser estabelecida;

3) Quando o LISP-MN se comunica com um dispositivo em um domínio LISP, existe o duplo encapsulamento dos pacotes. Esse duplo encapsulamento aumenta o tamanho do pacote, que pode encontrar problemas com o MTU das redes ao longo do caminho, o que cria a fragmentação ou descarte de pacotes;

4) Existe o roteamento triangular quando uma das partes da comunicação está fora do domínio LISP, o que dificulta engenharia de rede, aplicação de QoS e resolução de problemas;

5) O LISP-MN não funciona em ambientes configurados com *Network Address Translator - NAT*[Egevang and Francis, 1994].

Diversos trabalhos tem sido feitos a fim de sanar ou diminuir o impacto dos inconvenientes listados, e os principais são:

- Em [Ping et al., 2011] e [Gohar and Koh, 2011], existem propostas de uma abordagem para mobilidade IP utilizando LISP sem alteração nos *hosts*, onde o primeiro equipamento de rede de acesso detectaria que existe um dispositivo fazendo *roaming* e faria a atualização do MR-MS para o prefixo EID deste dispositivo detectado. Estas abordagens, porém, requerem que todos os dispositivos roteadores suportem o protocolo LISP, incluindo até roteadores Wi-Fi.

- Em [Menth et al., 2010], existe a proposta de que o LISP-MN incorpore atividades de detecção pós-*roaming*, como checagem se há filtros por endereço IP de origem na *Foreign Network*, detecção se o LISP-MN está numa rede LISP ou não, utilização de um bit no cabeçalho LISP para identificar que o dispositivo é um LISP-MN e assim evitar a dupla consulta ao MR-MS quando não for um LISP-MN, além de mudanças no algoritmo para evitar o duplo encapsulamento LISP.

- [Klein et al., 2010] submeteu uma proposta ao grupo de trabalho do LISP para resolver o problema da falta de suporte ao NAT, propondo um novo elemento chamado *LISP Re-encapsulating Tunnel Router (RTR)*. A proposta visa criar um componente na rede LISP que funcionaria como âncora para os dispositivos LISP-MN.

3.5 VANTAGENS DO LISP-MN SOBRE O MOBILE IP

Com base no modo de funcionamento e das inconveniências listadas para o LISP-MN, é possível verificar que o LISP-MN possui diversas vantagens sobre o MIP:

- O LISP-MN só exige roteamento triangular quando em comunicação com a Internet tradicional. Uma vez que este migre para o LISP, esta necessidade não existirá;

- Não há a necessidade de dispositivos de rede específicos para mobilidade, como o *Home Agent* e o *Foreign Agent*;
- O LISP-MN permite fazer uso do *multihoming*, ou seja, utilizar várias interfaces de rede ao mesmo tempo para melhorar a convergência;
- Não exige nenhuma modificação ou cabeçalho extra no IPv6;
- Implementação simplificada, uma vez que a especificação do LISP-MN possui 22 páginas, enquanto que a especificação do MIP possui 100 páginas. Além disso, a especificação do LISP-MN é a mesma para IPv4 e IPv6, sendo que o MIP funciona apenas para IPv4. Para atender o IPv6, o MIPv6 foi criado e possui 165 páginas.

No próximo capítulo, o LISP-MN será avaliado em um ambiente real, onde a convergência e a troca de mensagens serão avaliadas e considerações sobre o tempo de convergência para aplicações VoIP serão apresentadas.

CAPÍTULO 4

AVALIAÇÃO PRÁTICA

Nos capítulos anteriores foram apresentados os conceitos referentes à "Internet do futuro" sob a perspectiva da IETF e o protocolo MIP, além de ter sido detalhado o protocolo LISP e seu funcionamento para permitir a mobilidade IP. Foram detalhados modos de funcionamento em diversos cenários e apresentadas possíveis inconveniências, principalmente em cenários de interação entre o modo de funcionamento proposto pelo LISP e o modo de funcionamento da Internet atual. De posse destas informações, neste capítulo serão apresentados cenários reais a fim de observar na prática o funcionamento do LISP-MN, onde serão feitas avaliações com foco no tempo de convergência (*handover*) e que tipo de impacto esse tempo poderia ter sobre aplicações multimídia, como Voz sobre IP (VoIP).

Primeiramente será apresentada a metodologia utilizada nos experimentos e as configurações serão detalhadas. Após isso, serão apresentados os resultados obtidos e os mesmos serão interpretados. Finalizando, serão apresentadas inconveniências detectadas nos experimentos e ações tomadas a fim de contorná-las.

4.1 METODOLOGIA

A opção pela abordagem prática de experimentos foi escolhida para servir de subsídio para as discussões em torno do protocolo LISP no grupo de trabalho na IETF, uma vez que, até o momento, toda discussão tem ocorrido em torno de teorias e propostas. Na prática, é possível observar como a arquitetura do protocolo e suas diversas opções de mensagens interagem com o ambiente, e assim, é possível identificar quais mensagens e sinalizações precisam/podem/devem ser melhoradas a fim de diminuir o tempo de convergência e a complexidade.

Para a realização destes experimentos, foram montados três experimentos com objetivo de avaliar como o LISP-MN interage com os dispositivos LISP e com a Internet atual. A fim de permitir a reprodução dos experimentos executados, todas as configurações e versões estão detalhadas no Apêndice A. Porém, uma breve descrição será apresentada a seguir.

4.1.1 Experimento 1 - Tempo de convergência entre dois domínios LISP

O primeiro experimento está representado na Figura 4.1. Este experimento foi composto da seguinte maneira: no domínio "LISP 01", existe um roteador atuando como xTR deste domínio, além de atuar como *Map-Resolver e Map-Server (MR-MS)* para ambos os domínios. Além disso, existe um *Wireless Access Point* usando Wi-Fi com SSID "lisp1", sem criptografia ou autenticação. O dispositivo LISP-MN possui como sua *Home Network* o domínio LISP 01. O domínio "LISP 02"possui um roteador atuando como xTR deste domínio, um *Wireless Access Point* usando Wi-Fi com SSID "lisp2"e um dispositivo estacionário SN.

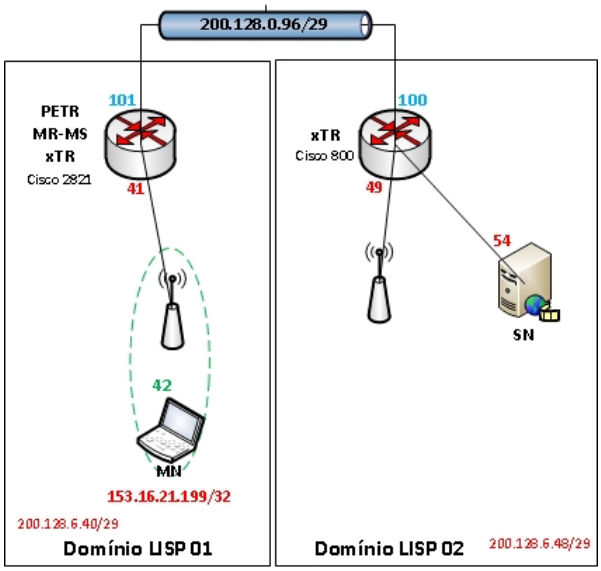

Figura 4.1. Experimento 1: Dois domínios LISP.

Esse experimento fará a avaliação do *roaming* do dispositivo LISP-MN entre dois

domínios LISP, onde serão avaliadas as trocas de mensagens e o tempo de convergência nos dois sentidos, tanto o LISP-MN migrando do domínio "LISP 01"para o "LISP 02"como voltando para o "LISP 01"a partir do "LISP 02".

4.1.2 Experimento 2 - Tempo de convergência entre um domínio LISP e a Internet

O segundo experimento está representado na Figura 4.2. Este experimento foi composto da seguinte maneira: no domínio "LISP 01" existe um roteador atuando como xTR e um *Wireless Access Point*. Entre o domínio "LISP" 01 e a Internet existe um roteador atuando como MR-MS e PxTR. E a Internet é representada por um roteador Linux, um *Wireless Access Point* e um dispositivo estacionário SN. É importante ressaltar que, neste caso, a representação da "Internet" foca no modo de roteamento dos pacotes IP, e não na sua escala e complexidade. O SSID definido para a rede LISP 01 foi "lisp1"e para a Internet foi o SSID "internet".

Esse experimento fará a avaliação do *roaming* do dispositivo LISP-MN, saindo de um domínio LISP indo para um domínio com funcionamento semelhante ao da Internet atual e depois voltando para sua *Home Network*. Serão avaliadas as trocas de mensagens e o tempo de convergência em ambos os sentidos de mobilidade.

4.1.3 Experimento 3 - Tempo de convergência com LISP-MN na Internet

O terceiro experimento ocorreu utilizando a rede LISP *beta-network*[1], que é uma rede de testes mundial, com mais de mil participantes, criada como uma rede virtual sobre a Internet. Essa rede possui diversos *Map-Servers*, *Map-Resolvers*, *xTRs* e *PxTRs* voluntários espalhados pelo mundo, inclusive com participantes comerciais, como a Google[2] e o Facebook[3]. Apesar de ser geograficamente bem espalhada, ainda não existem *Map-Servers*, *Map-Resolvers* e *PxTRs* na América Latina, o que aumenta a complexidade

[1]LISP *Beta Network* - http://www.lisp4.net/beta-network/
[2]Google - http://www.google.com/intl/en/about/
[3]Facebook - http://www.facebook.com/facebook

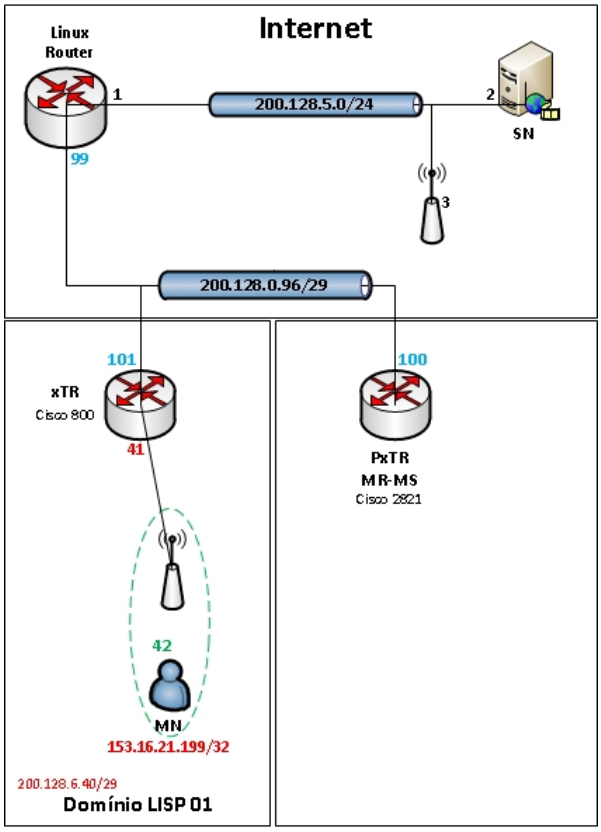

Figura 4.2. Experimento 2: Domínio LISP e Internet.

dos experimentos. Porém, uma vez que o objetivo é avaliar o LISP-MN em uma rede de produção, com tráfego, gargalos e perdas de pacotes reais, simulando o início da utilização do LISP-MN nos dias atuais, o experimento se mostra válido e interessante.

No experimento foi utilizado o mesmo dispositivo LISP-MN dos experimentos anteriores, com o mesmo EID, porém, com *MR-MS* e *PxTR* reais, considerados em produção. O *MR-MS* está localizado na Europa e o *PxTR* está localizado nos Estados Unidos. A Figura 4.3 abstrai as localizações fixas dos dispositivos envolvidos, apresentado uma visão geral do experimento. A fim de facilitar a contextualização do Experimento 3, no Apêndice B estão expostas as saídas das aplicações *traceroute* e *ping* a partir do LISP-MN e a partir do dispositivo SN. Explicações sobre o que são e como funcionam estas aplicações também estão contempladas neste apêndice.

Esse experimento fará a avaliação do *roaming* do LISP-MN entre dois LLOCs dentro

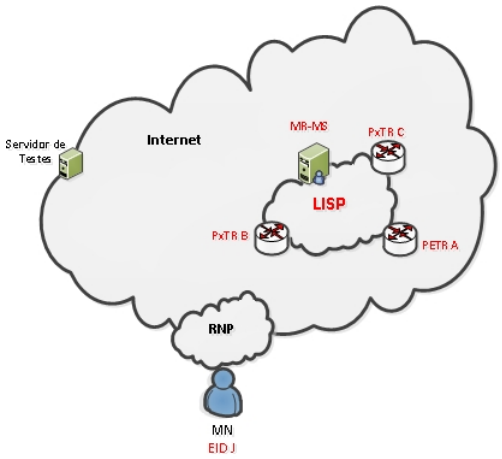

Figura 4.3. Experimento 3: LISP-MN e a *LISP beta-network*.

da mesma rede, em um domínio não-LISP, em comunicação com um dispositivo SN em outro domínio não-LISP. Serão avaliadas as trocas de mensagens, o tempo de convergência e as perdas de pacotes decorrentes do *roaming*.

4.1.4 LISP-MN com LISPMob

O dispositivo LISP-MN que será utilizado em todos os experimentos fará uso da aplicação LISPMob[4], uma aplicação livre, escrita utilizando a linguagem de programação C, que funciona em ambientes GNU/Linux, incluindo o Debian Linux[5], que é o sistema operacional utilizado nos experimentos. O LISPMob implementa um xTR simplificado, uma vez que encapsula todos os pacotes IP em pacotes LISP, com a possibilidade de delegar ao *MR-MS* as resposta por consultas ao EID utilizado na mobilidade. Na versão 0.2.x, o LISPMob implementa o plano de dados em espaço de *kernel*, enquanto o plano de controle é implementado em espaço de usuário.

Algumas alterações foram feitas no LISPMob a fim de permitir a coleta dos tempos de convergencia, e estão citadas na Subseção 4.1.5.

[4]LISPMob - http://www.lispmob.org
[5]Debian Linux - http://www.debian.org

4.1.5 Coleta dos dados

Para poder fazer as coletas de tempo de convergência nos diversos experimentos, o código do LISPMob foi alterado para alcançar dois objetivos:

- Diminuição do tempo de convergência: Para diminuir o *handover*, foram removidos ou reduzidos os controles de *race-condition*[Tanenbaum, 2007] existentes no código, a medida que os tempos de resposta eram obtidos nos experimentos. Como o LISPMob ainda é considerado um código em desenvolvimento, existem algumas condições de depuração e controle que facilitam a depuração de problemas de implementação, porém aumentam o tempo de convergência. Por exemplo, foram removidos alguns tempos de espera (*sleep*) e impressões no ambiente do *kernel*(*printk*);
- Cálculo e impressão de tempo de convergência: O LISPMob possui, neste momento, interesse em permitir a mobilidade IP usando o ambiente LISP, sem necessariamente focar no tempo de convergência. Por isso, foram feitas as alterações citadas anteriormente para diminuir o tempo de convergência, além de funções de cálculo e impressão dos tempos referentes a cada etapa do *handover*, como detecção da troca de endereçamento LLOC, recriação da tabela de rotas, envio do *Map-Register*, retorno das consultas *Map-Request Probes*, etc. Desta maneira, é possível obter do próprio LISPMob os valores de convergência observados em cada repetição de cada experimento.

4.1.6 Avaliação estatística

Em todos os experimentos, estão identificados os seguintes fatores como influenciadores dos resultados (erros):

- Fator Primário: tempo de resposta à solicitação de convergência do protocolo LISP;
- Fatores Secundários: protocolo Ethernet[Shoch et al., 1982], protocolo Wi-Fi[6], co-

[6]Especificações IEEE 802.11 - http://grouper.ieee.org/groups/802/11/

mutadores e roteadores com interfaces 100Mbps, conectadas via cabeamento Categoria 5e[Spurgeon, 2000].

Como métrica de desempenho destes experimentos, espera-se obter o tempo total de convergência, para então, avaliar o impacto desta convergência em aplicações multimídia.

De acordo com [Jain, 1991], a quantidade de repetições está relacionada com a precisão dos resultados da simulações, e, em ambientes de redes de computadores com apenas um fator primário, é sugerido utilizar a Distribuição Normal para obter o número de repetições necessárias, sendo sugerido o valor de quarenta em simulações com apenas um fator primário. Será utilizado esta quantidade de repetições nos Experimentos 1 e 2. No Experimento 3 -que utiliza a infraestrutura da Internet-, a fim de aumentar a precisão dos resultados, serão executadas sessenta repetições.

4.2 EXECUÇÃO DOS EXPERIMENTOS

A execução dos Experimentos 1 e 2 seguiu o mesmo procedimento, descrito a seguir:

1) Fluxos ICMP foram iniciados entre o LISP-MN e o SN, com intervalos de 20 milisegundos entre cada pacote, sempre usando como origem ou destino o endereço IP da interface EID do LISP-MN, ou seja, quando o LISP-MN enviava os pacotes com destino o SN, a interface de origem era a interface EID do LISP-MN (representado pelo endereço IP **153.16.21.199**), e quando o SN enviava os pacotes para o LISP-MN, enviava com destino o mesmo IP (**153.16.21.199**);

2) Uma conexão TCP foi estabelecida utilizando a aplicação de gerenciamento remoto SSH[7], a fim de confirmar que a conexão permanecia estabelecida mesmo após a troca do endereço IP da interface física do LISP-MN;

3) A mobilidade era iniciada a partir da associação ao SSID de destino.

[7] *Secure SHell: http://www.openssh.org*

A escolha do curto intervalo entre os testes ICMP (20 milisegundos) tinha como intenção forçar que o LISP-MN acelerasse todas as atividades de ARP e sinalizações LISP para buscar informações da rede de destino (*Foreign Network*).

Para promover o *roaming* entre as duas redes Wi-Fi disponíveis ("lisp1"e "lisp2"no Experimento 1 e "lisp1"e "internet"no Experimento 2) e assim, executar a mobilidade entre as redes definidas, no dispositivo LISP-MN foi executada uma migração forçada, ou seja, intencionalmente foi solicitada a troca de SSID para o SSID desejado. Como o objetivo do trabalho é avaliar os tempos e procedimentos envolvidos na mobilidade IP usando o LISP, o modo como a mobilidade ocorria na Camada Física e na Camada de Enlace eram indiferentes para os experimentos.

A execução dos testes no Experimentos 3 seguiu o procedimento descrito a seguir:

1) No SN, o aplicativo IPERF[8] foi configurado para funcionar no modo servidor, recebendo a conexão originada pelo LISP-MN;

2) No LISP-MN, o aplicativo IPERF foi configurado para funcionar no modo cliente, e enviar para o servidor, um fluxo UDP simulando um fluxo VoIP com codec G.711[9]. Este fluxo ocorreu durante 10 segundos, onde pacotes UDP de 160 bytes (equivalente à 20 milisegundos de voz) eram enviados a cada 20 milisegundos;

3) Durante a ocorrência do fluxo, o processo de *roaming* ocorria, com a troca do endereço LLOC do LISP-MN, do **LLOC A** para o **LLOC B** ou o contrário.

4) Ao final do fluxo, os resultados eram coletados a partir dos relatórios do IPERF e do LISPMob.

[8]O IPerf é uma ferramenta criada para medir largura de banda utilizando UDP e TCP, que ao longo dos tempos, tem evoluído com ajustes que permitem até simular fluxos de voz utilizando o protocolo *Real-time Transport Protocol*[Schulzrinne et al., 2003] e está disponível em http://iperf.fr

[9]Codec G.711: http://www.itu.int/rec/T-REC-G.711/en

4.2.1 Execução do Experimento 1 - Tempo de convergência entre dois domínios LISP

A Figura 4.4 apresenta o endereçamento IP utilizado no Experimento 1 e o processo de mobilidade ocorrendo, com foco apenas nas mensagens LISP utilizadas para fins de mobilidade. É possível observar que o xTR do domínio LISP 01 atua também como *MR-MS* com endereço IP RLOC **200.128.0.101**. O xTR do domínio LISP 02 possui endereço IP RLOC **200.128.0.100**. Além disso, a figura apresenta dois momentos: momento "**a**", que representa o LISP-MN na sua *Home Network*, e momento "**b**", que representa o processo de *roaming*.

No momento "**a**", é possível observar o LISP-MN em comunicação com o SN, representada pelas linhas com setas alaranjadas, ocorrendo segundo o modo de funcionamento padrão do LISP, descrito na Seção 2.5. O endereço EID do LISP-MN é o **153.16.21.199**, o endereço LLOC é o **200.128.6.42**.

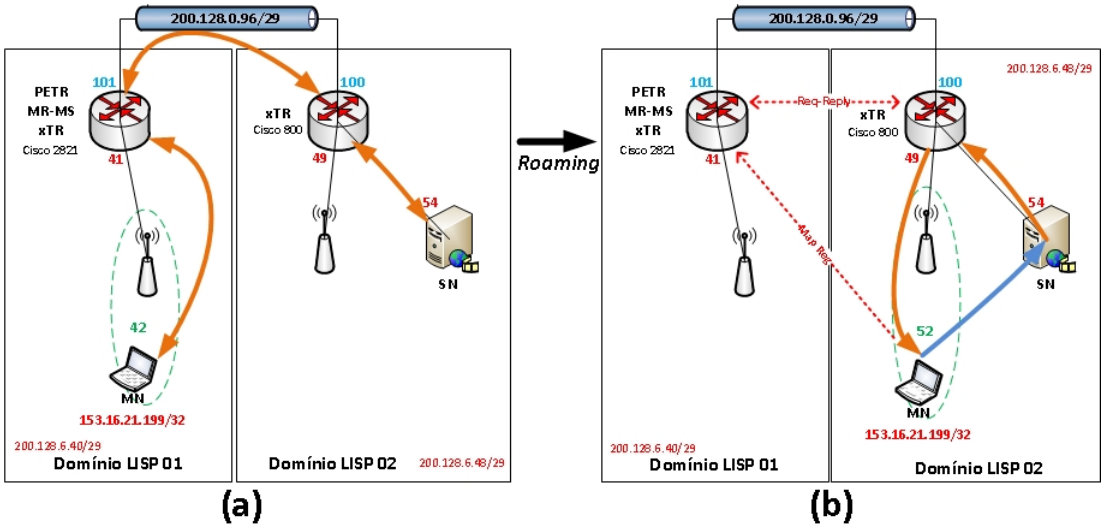

Figura 4.4. Processo de Mobilidade do Experimento 1: *roaming* para a *Foreign Network*.

Então, no momento "**b**", o LISP-MN executa o *roaming* indo para o domínio LISP 02, onde o mesmo recebe o endereçamento IP via DHCP deste domínio, **200.128.6.52**, e este endereço IP passa a ser o novo LLOC. É possível observar que o endereço EID do LISP-MN permanece o mesmo: **153.16.21.199**.

Após o LISP-MN detectar a troca do LLOC, o mesmo envia um *Map-Register* para o MR-MS com o novo LLOC(**200.128.6.52**). A seguir, o xTR do domínio LISP 02 percebe o prefixo EID do LISP-MN vindo de sua interface interna e faz uma consulta *Map-Request* para o MR-MS. Este então envia um *Map-Reply* informando o novo LLOC do LISP-MN. A partir deste momento, todo pacote que o xTR do domínio LISP 02 receber para o endereço IP **153.16.21.199**, o mesmo irá encapsular em um pacote LISP destinado ao endereço IP **200.128.6.52** (LLOC do LISP-MN).

Como o LISP-MN é um xTR simplificado, outras mensagens LISP precisam ser trocadas, conforme Figura 4.5, que representa também as mensagens entre o MR-MS e o xTR do domínio LISP 02 e deste para o LISP-MN. Esta representação, mostrando todas as mensagens trocadas, é importante para observar a sequência e também entender como os tempos de convergência foram obtidos. Estes tempos serão apresentados na Seção 4.3. Na Figura 4.5, a linha vermelha tracejada representa uma comunicação ICMP ocorrendo entre o dispositivo LISP-MN e o SN. A linha com seta azul ponto-tracejada representa o processo de mobilidade ocorrendo, onde o LISP-MN sai da rede de origem, com seu LLOC de origem (**200.128.6.42**) e faz o *roaming* para a rede de destino, onde obtém o endereço LLOC (**200.128.6.52**). Ao final, após a convergência ocorrer, a linha vermelha tracejada volta a aparecer, representando a continuidade de comunicação previamente iniciada. Como esta comunicação envolve o endereço EID do LISP-MN (**153.16.21.199**), a conexão TCP (SSH) não é reiniciada.

A seguir, estão detalhadas cada mensagem LISP trocada:

1) *Map-Register*: Esta mensagem é enviada pelo LISP-MN para o EID do MR-MS (previamente configurado) para informar o novo LLOC;

2) *Map-Notify*: Mensagem enviada pelo MR-MS para o antigo LLOC do LISP-MN para informá-lo da mudança. Esta mensagem é importante para atualizar a memória *cache* do LISP-MN, caso este tenha duas interfaces LLOC, por exemplo;

3) *Map-Request* (SMR) - **200.128.6.48/32**: O LISP-MN envia uma requisição para identificar quem é o RLOC responsável pela rede a qual ele faz parte, no caso,

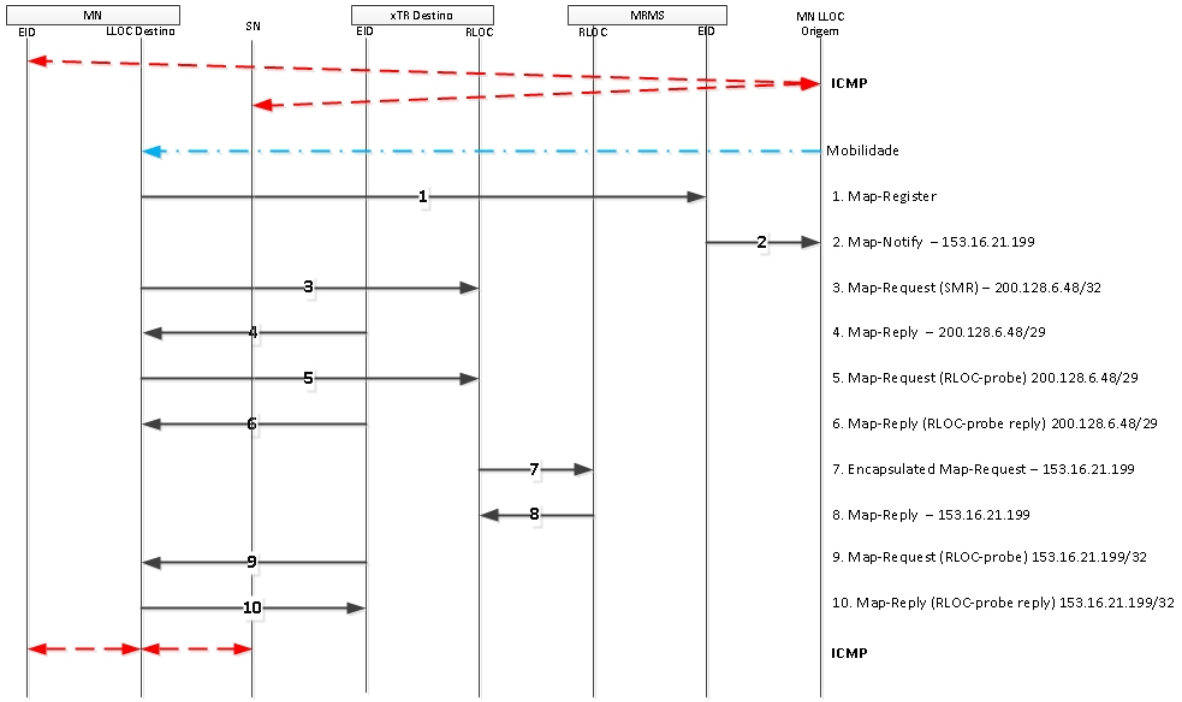

Figura 4.5. Troca de mensagens LISP: LISP 01 para LISP 02.

200.128.6.48. É importante observar que na consulta SMR, a busca foi realizada pelo prefixo de *host*, um prefixo de tamanho 32. A solicitação é feita ao RLOC do domínio LISP 02 pois o LISP-MN já possuía em sua memória *cache* este xTR, uma vez que já havia uma comunicação prévia com o SN (SSH e ICMP);

4) *Map-Reply* - **200.128.6.48/29**: O xTR do domínio LISP 02 envia a resposta via Map-Reply para o LISP-MN informando o RLOC daquele prefixo solicitado. É importante observar que na resposta, o xTR informa o RLOC (**200.128.0.100**) do prefixo da rede (/29) e não o prefixo de *host* (/32);

5) *Map-Request (RLOC Probe)* - **200.128.6.48/29**: o LISP-MN envia para o **200.128.6.100** uma consulta pelo prefixo recebido na última resposta (Map-Reply) a fim de confirmar se este ainda é o responsável;

6) *Map-Reply (RLOC Probe reply)* - **200.128.6.48/29**: O LISP-MN recebe a resposta do RLOC do domínio LISP 02(**200.128.6.100**);

7) Como o SN continua enviando pacotes destinados ao EID do LISP-MN, o xTR

do domínio LISP 02 envia uma consulta, via pacote encapsulado ao MR-MS, para identificar o RLOC responsável pelo EID **153.16.21.199**;

8) O MR-MS envia um *Map-Reply* informando o RLOC associado ao prefixo EID solicitado;

9) De posse da resposta, o "xTR Destino"envia um *Map-Request* para o RLOC associado em EID, neste caso, o RLOC é o LLOC **200.128.6.50**;

10) O LISP-MN responde ao "xTR Destino"confirmando que é o LLOC responsável pelo EID do LISP-MN.

11) A partir deste último passo, a comunicação é reestabelecida entre o LISP-MN e o SN. Foi possível verificar que a conexão TCP (SSH) continuou funcional.

De maneira análoga, foram realizados testes de *roaming* com o LISP-MN voltando para a *Home Network*, e os tempos e passos também foram mapeados. A Figura 4.6 representa o processo e mostra a sinalização LISP para mobilidade ocorrendo.

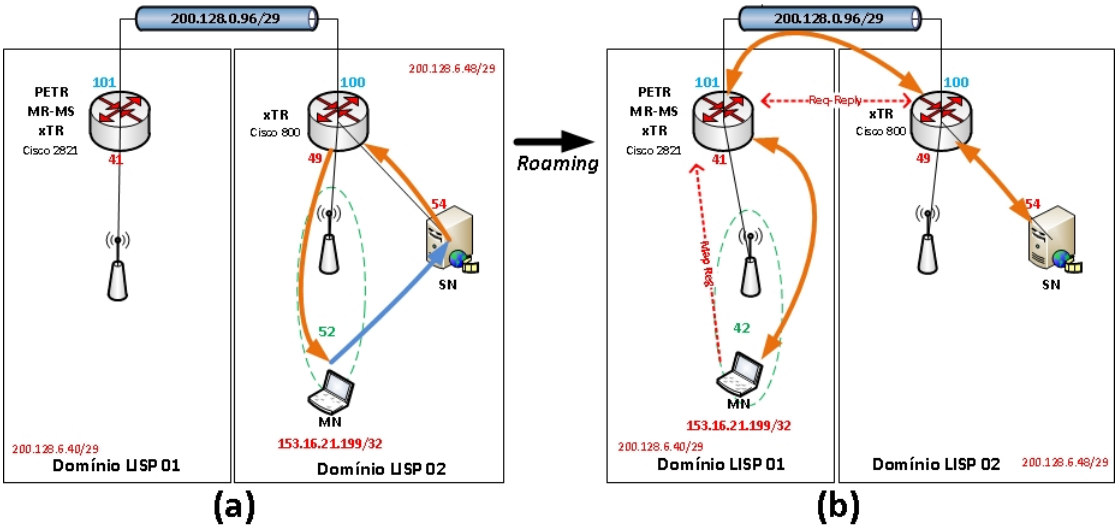

Figura 4.6. Processo de Mobilidade do Experimento 1: Volta para a *Home Network*.

Assim como no processo de *roaming* para a *Foreign Network*, o processo de sinalização LISP completo foi mapeado, e está representado na Figura 4.7. Na Figura 4.7, assim como

na representação da Figura 4.5, a linha vermelha tracejada representa uma comunicação SSH ou ICMP ocorrendo entre o dispositivo LISP-MN e o SN. A linha com seta azul ponto-tracejada representa o processo de mobilidade ocorrendo, onde o LISP-MN sai da rede de origem, com seu LLOC de origem (**200.128.6.52**) e faz o *roaming* para a rede de destino, onde obtém o endereço LLOC (**200.128.6.42**). Ao final, após a convergência ocorrer, a linha vermelha tracejada volta a aparecer, representando a continuidade de comunicação previamente iniciada. Assim como no caso anterior, a conexão TCP (SSH) não é reiniciada.

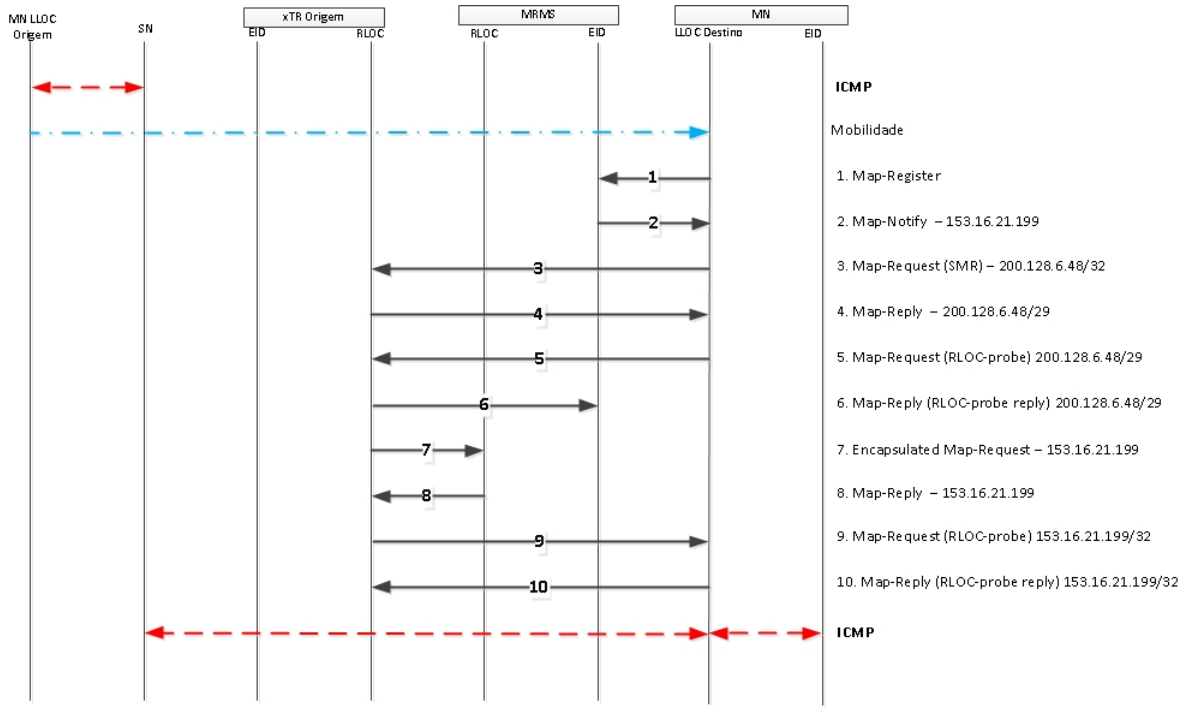

Figura 4.7. Troca de mensagens LISP: LISP 02 para LISP 01.

O fluxo das mensagens LISP trocadas no sentido LISP 02 para LISP 01 (Figura 4.7) segue a mesma lógica e sequência das mensagens trocadas quando o *roaming* foi no sentido LISP 01 para LISP 02 (Figura 4.5), acima detalhado.

4.2.2 Execução do Experimento 2 - Tempo de convergência entre um domínio LISP e a Internet

O Experimento 2 ocorreu de forma similar ao Experimento 1, porém, possui um diferencial, que é o fato de requerer o uso de roteador LISP do tipo PxTR, responsável pela comunicação entre domínios LISP e domínios Internet. A Figura 4.8 apresenta, assim como no Experimento 1, dois momentos: momento **a** e o momento **b**. O momento **a** mostra o LISP-MN na sua *Home Network* em comunicação com o SN, estando este fora do domínio LISP, no caso, no domínio Internet. Nesta representação da Internet, o roteamento e encaminhamento dos pacotes é feito da maneira tradicional, com todas as rotas nas tabelas de roteamento de todos os roteadores.

No momento **a**, as linhas alaranjadas tracejadas representam os pacotes sendo encaminhados seguindo o modelo tradicional da Internet, e as linhas alaranjadas contínuas representam os pacotes sendo encaminhados usando o LISP. É importante verificar o papel do roteador PxTR atuando como PETR: todos os pacotes que o xTR recebe do LISP-MN são encaminhados para este roteador, que remove o pacote LISP e encaminha para a "Internet". Na volta, quando os pacotes originados no SN são encaminhados para o *Linux Router*, este possui em sua tabela uma rota indicando que o prefixo do LISP-MN (**153.16.21.199**) deve ser encaminhado para o PxTR (agora atuando como PITR). Porém, uma vez que o pacote é recebido pelo PxTR, ao observar que o *Linux Router* e o xTR responsável pelo LISP-MN estão na mesma sub-rede (**200.128.0.96/29**), o PxTR envia um pacote ICMP para redirecionamento de tráfego, apontando diretamente para o IP do xTR (**200.128.0.100**). A partir do segundo pacote, o *Linux Router* passa a encaminhar os pacotes destinados ao LISP-MN diretamente para o xTR do domínio LISP 01.

No momento **b**, o LISP-MN faz o *roaming* para a rede **200.128.5.0/24**, que representa a Internet. Quando este percebe a troca do **LLOC**, o mesmo envia um *Map-Register* para o **MR-MS** informando a nova associação <EID,LLOC>, no caso, <153.16.21.199, 200.128.5.4>. Então, o **MR-MS** envia um *Map-Notify* para o xTR apenas para informá-

lo que o LISP-MN mudou de LLOC. Após ambos dispositivos LISP estarem atualizados, a comunicação seguirá o seguinte plano de dados:

- *Linux Router* enviará os pacotes destinados ao LISP-MN para o PxTR da forma tradicional;
- O PxTR encapsulará o pacote IP em pacote LISP e encaminhará para o roteador da rede do LLOC do LISP-MN. Neste caso, o LLOC é **200.128.5.4** e o roteador responsável por esta rede é o *Linux Router*;
- O *Linux Router* fará o roteamento do pacote para o LISP-MN, que receberá o pacote LISP, fará o desencapsulamento e o processamento do pacote IP interno;
- Para enviar o pacote de volta para o SN, o LISP-MN possui duas possibilidades:
    1) Enviar o pacote IP diretamente, sem encapsulamento LISP, com origem o IP do EID do LISP-MN;
    2) Encapsular o pacote IP em um pacote LISP e enviar para o PxTR, que fará a remoção do pacote LISP e enviará o pacote do modo tradicional.

Na Figura 4.8, a linha verde pontilhada indica a escolha pelo envio direto, uma vez que o experimento não possui filtros baseados no IP de origem.

Na Figura 4.9 temos a representação do plano de controle do LISP-MN, que agora estando na Internet, e não mais em um domínio LISP, precisa apenas notificar o MR-MS para que este notifique o PxTR. Porém, como neste experimento o MR-MS e o PxTR estão operando no mesmo equipamento, o plano de controle é extremamente simplificado. Assim como nas representações anteriores, a linha vermelha tracejada representa uma comunicação SSH ou ICMP ocorrendo entre o dispositivo LISP-MN e o SN. A linha com seta azul ponto-tracejada representa o processo de mobilidade ocorrendo, onde o LISP-MN sai da rede de origem, com seu LLOC Origem (**200.128.6.42**) e faz o *roaming* para a rede de destino, onde obtém o endereço LLOC Destino (**200.128.5.4**). Ao final, após a convergência ocorrer, a linha vermelha tracejada volta a aparecer, representando

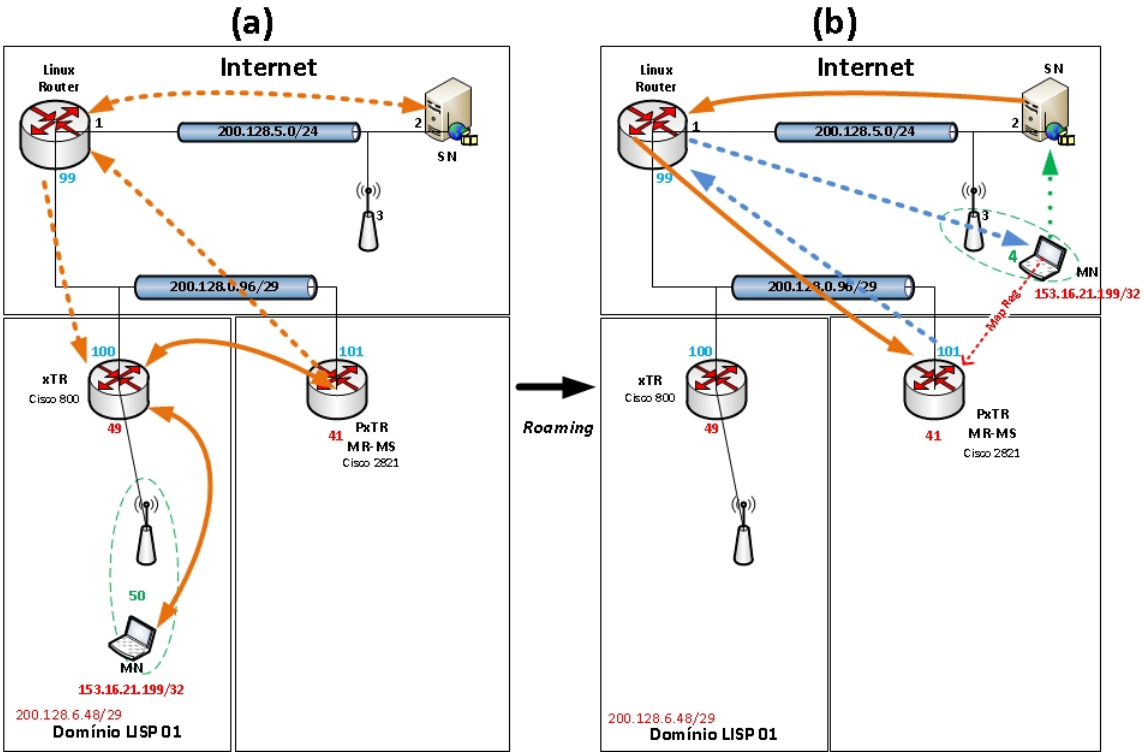

Figura 4.8. Processo de Mobilidade do Experimento 2: LISP 01 para Internet.

a continuidade de comunicação previamente iniciada. Mais uma vez, como esta comunicação envolve o endereço EID do LISP-MN (**153.16.21.199**), a conexão TCP (SSH) não é reiniciada.

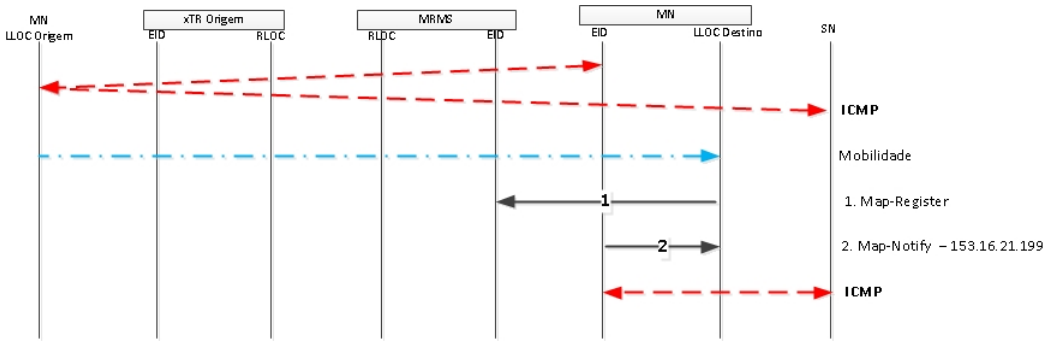

Figura 4.9. Troca de mensagens LISP: LISP 01 para Internet.

Assim como no Experimento 1, foram realizados testes de *roaming* com o LISP-MN voltando para a *Home Network*, e os tempos e passos também foram mapeados. A Figura 4.10 representa o processo e mostra a sinalização LISP para mobilidade ocorrendo.

É possível observar que no momento **b**, uma mensagem *ICMP Redirect* é enviada pelo PxTR para o *Linux Router*, a fim de criar uma rota dinâmica neste apontando para o xTR.

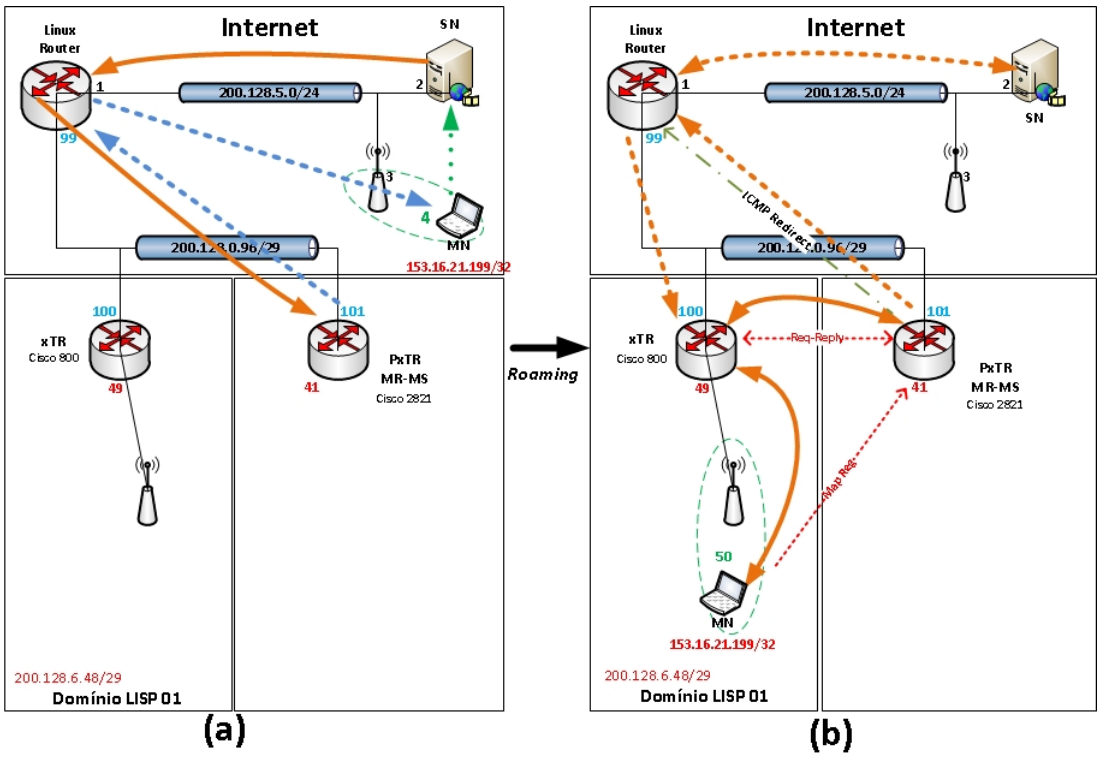

Figura 4.10. Processo de Mobilidade do Experimento 2: Internet para LISP 01.

Apesar de nos experimento o xTR estar configurado para enviar todos os pacotes para o PxTR para este enviar para a Internet, existe a opção de configurar o xTR para não fazê-lo, fazendo este funcionar como xTR e PETR. Esta abordagem permite diminuir o caminho, porém, pode dificultar aplicação de técnicas de QoS e abrir brechas de segurança em uma rede com filtro de pacote baseado no IP de origem.

Na Figura 4.11, todas as mensagens LISP foram representadas para representar o processo de *roaming* de volta para a *Home Network*. Observa-se que o LISP-MN volta a participar de um domínio LISP, logo o mesmo precisa de informações sobre quem é o RLOC responsável por tal domínio. Neste caso, o plano de controle ficou similar aqueles do Experimento 1.

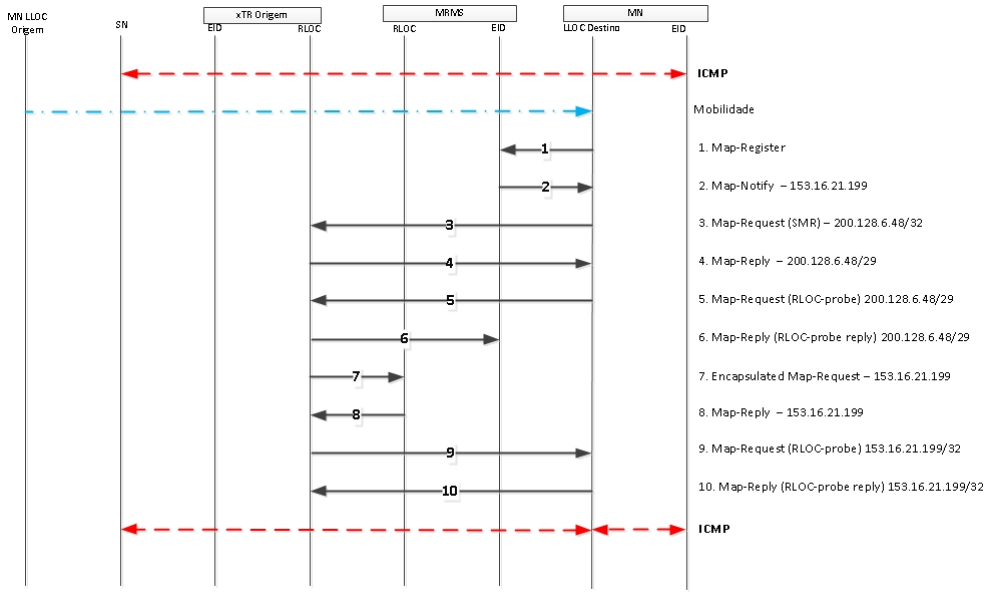

Figura 4.11. Troca de mensagens LISP: Internet para LISP 01.

4.2.3 Execução do Experimento 3 - Tempo de convergência com LISP-MN na Internet

No Experimento 3 foi utilizado o mesmo dispositivo LISP-MN dos experimentos anteriores, com o mesmo EID (**153.16.21.199**), porém, com *MR-MS* e PxTR reais. O *MR-MS* alocado pelos responsáveis da LISP *beta-network* possui o RLOC **217.8.97.6**, representado pelo FQDN[10] *intouch-mn-rtr.rloc.lisp4.net* e o PETR possui o RLOC **69.31.31.98**, representado pelo FQDN *eqx-ash-pxtr.rloc.lisp4.net*. O *MR-MS* está localizado na Europa, com 230.6 ms de média de RTT(*rount trip time*), e o PETR está localizado nos EUA, com 137.4 ms de média de RTT. Estas médias foram obtidas no momento anterior aos testes, onde foram enviados 100 requisições ICMP com intervalos de meio segundo, pacotes com 64 Bytes de tamanho e estas apresentadas no Apêndice B. O LISP-MN estava hospedado dentro da rede da Rede Nacional de Ensino e Pesquisa[11], onde foram cedidos, para fins de testes, dois endereços IP para serem utilizados como LLOC: **LLOC A** e **LLOC B**.

[10] *Fully Qualified Domain Name* - Nome DNS completo do dispositivo.
[11] RNP - http://www.rnp.br

Para fazer a avaliação do LISP-MN, nos foi cedido um servidor Linux/Debian hospedado nos EUA, com endereço IP **SN**, fora da rede LISP *beta-network*, ou seja, um servidor de rede na Internet. Este servidor hospedou a aplicação IPERF, no modo servidor, configurada de maneira a simular um tráfego de voz usando o codec G.711. Então, o LISP-MN, operando no modo cliente, estabeleceu um fluxo de 10 segundos, e durante esse fluxo, o processo de mobilidade ocorreu, com o LISP-MN trocando de LLOC, do **LLOC A** para o **LLOC B** e vice-versa.

Um ponto a ser observado é o fato que, por ser um ambiente real e corporativo, a rede da RNP faz filtro de pacotes IP baseados na origem, ou seja, o LISP-MN teve que ser configurado para enviar todos os pacotes LISP para o PETR, para que o mesmo enviasse para a Internet. E, a partir de testes de *traceroute*, foi observado que o PITR mais próximo utilizado pela LISP *beta-network* para receber os pacotes destinados ao prefixo **153.16.0.0/16** foi o *uninett-pxtr.rloc.lisp4.net*, com endereço IP **158.38.1.92**, também localizado na Europa, com média de 156.6 ms de RTT para o servidor SN. Todos os fluxos estão representados na Figura 4.12.

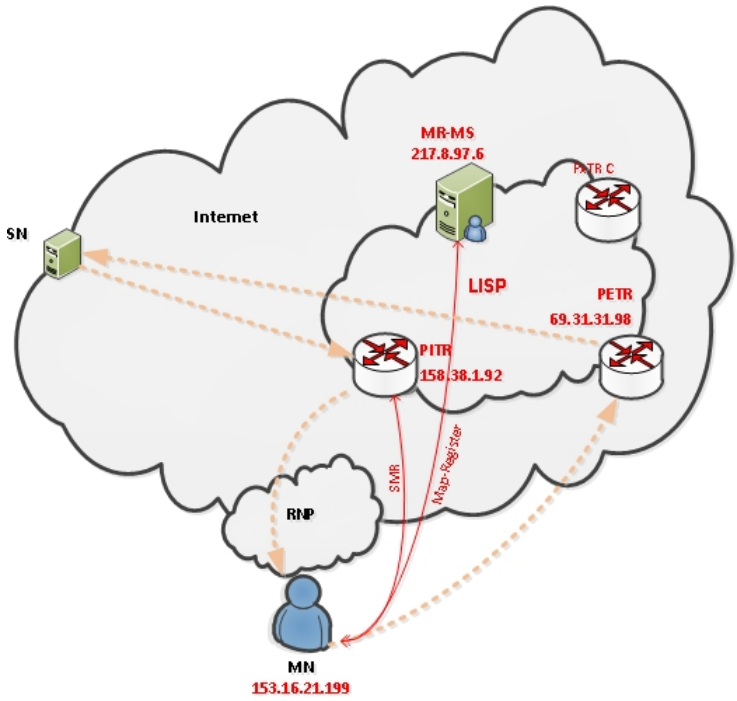

Figura 4.12. Fluxos do Experimento 3.

É possível observar que existe roteamento triangular na ida, uma vez que o LISP-MN tem que enviar os pacotes para o PETR, e existe na volta, pois o SN precisa enviar para o dispositivo PITR. Com isso, existe o chamado roteamento quadrangular, o que gera muita complexidade nos momentos de resolução de problemas.

O *roaming* ocorreu da seguinte maneira:

1) O LISP-MN, através do IPERF, estava enviando o fluxo UDP descrito acima (representado pela linha alaranjada pontilhada);

2) Intencionalmente, um *script* criado para trocar o endereço IP foi iniciado, mudando as configurações de rede. Com isso, o SN parou de receber o fluxo;

3) O LISP-MN, ao detectar que houve a troca do LLOC, envia um *Map-Register* para o MR-MS atualizando a nova associação <EID,LLOC>;

4) Após isso, o LISP-MN envia um SMR para os PITR configurados, atualizando suas memórias *cache* com a nova associação. Ambas as mensagens de controle estão representadas na linha vermelha contínua;

5) Após atualizar o PITR utilizado pelo SN, o SN volta a receber novamente o fluxo.

É possível observar que o LISP-MN apenas enviou dois tipos de mensagens para acionar o *handover*: o *Map-Register* para o MR-MS, e o SMR para os PITRs da rede de testes. O SMR é importante nessa etapa pois força uma rápida atualização das entradas da memória *cache*, melhorando o tempo de convergência. Espera-se que, no futuro, o próprio MR-MS faça o envio dos SMR para os PITRs, que, apesar de estar definido na especificação do LISP, não está implementado ainda. Com isso, haverá economia de recursos dos dispositivo móvel, como CPU, energia e largura de banda.

Na próxima seção, os tempos de convergência obtidos nos experimentos serão apresentados e a relação dos tempos com o VoIP será discutida.

4.3 RESULTADOS

Conforme já citado anteriormente, os principais problemas para a implementação de soluções de mobilidade baseadas na Camada de Rede do TCP/IP são a complexidade de implantação e o tempo de convergência. A complexidade do plano de controle do LISP-MN foi apresentada nos experimentos descritos na Seção 4.2, onde apenas poucas mensagens precisam ser trocadas, principalmente quando utilizando a Internet tradicional. Diferentemente do MIP, o LISP-MN não condiciona seu funcionamento à implantação de dispositivos para mobilidade na rede de origem e de destino.

4.3.1 Resultados para os Experimentos 1 e 2

A Figura 4.13 apresenta duas ilustrações, **a** e **b**, representando o Experimento 1 e o Experimento 2, respectivamente. Nestas ilustrações são representados os domínios de origem e destino em funcionamento, e um tempo de inatividade h que representa o *handover* ocorrendo. Durante o *handover*, a comunicação entre os dispositivos finais é interrompida até que todas as etapas envolvidas sejam concluídas. São elas:

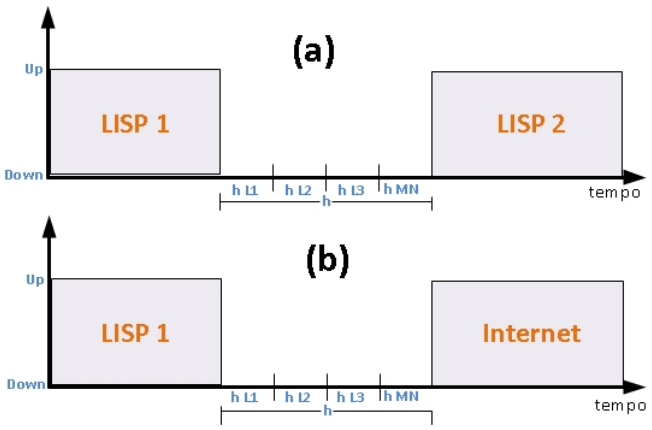

Figura 4.13. Tempo de convergência na mobilidade IP.

1) h_{L1}: Tempo de *handover* da Camada Física para buscar pela tecnologia desejada (Wi-Fi ou 3G, por exemplo), escanear a frequência e se associar a esta frequência;

2) h_{L2}: Tempo de *handover* da Camada de Enlace para fazer autenticação na rede conectada, bem como buscar parâmetros de conexão via DHCP, por exemplo;

3) h_{L3}: Tempo de *handover* da Camada de Rede, por exemplo, identificar roteador padrão da rede, auto gerar endereços, etc.

4) h_{MN}: Tempo de *handover* do LISP-MN, ou seja, se registrar no MR-MS e atualizar a memória *cache* dos ITR e PITR envolvidos na comunicação prévia.

O somatório destes tempos é caracterizado como o *handover* para aquele ambiente, seja utilizando Wi-Fi ou GSM/3G/4G, e esse deve ser o menor possível. Nos experimentos foram avaliados apenas os tempos de *handover* h_{MN}, ou seja, os atrasos gerados pelo LISP-MN utilizando 40 amostras para cada um dos *roamings* detalhados: "LISP 01 para LISP 02", "LISP 02 para LISP 01", "LISP 01 para Internet"e "Internet para LISP 01". As amostras para estes cenários foram plotadas na Figura 4.14, onde o eixo Y está representado em milisegundos (ms).

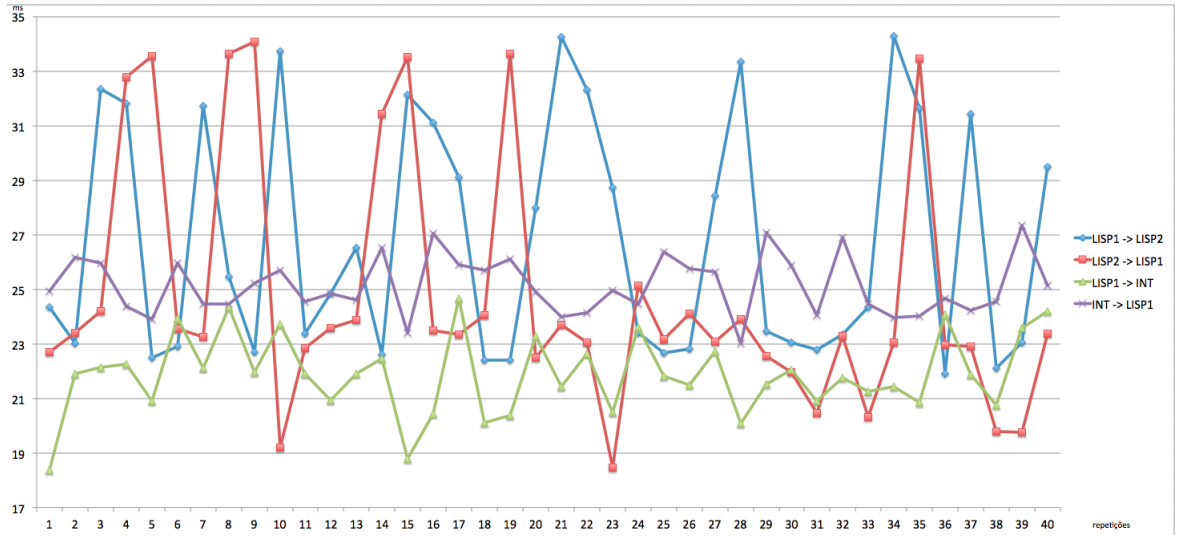

Figura 4.14. *Handovers* observados nos experimentos 1 e 2.

A fim de demostrar o que esses valores representam em uma aplicação real, será utilizada a tecnologia de VoIP como estudo de caso. O VoIP, ou Voz sobre IP, é um conjunto de protocolos e aplicações com objetivo de fazer o transporte de voz em uma

rede de pacotes IP. A principal característica do VoIP é a interatividade, ou seja, a capacidade de dois usuários do serviço fazerem uso da tecnologia de maneira natural, semelhante a uma interação pessoal, porém utilizando apenas a voz.

No âmbito das telecomunicações, onde o VoIP está incluído, a *International Telecommunication Union* - ITU[12] define diversas especificações a fim de padronizar os protocolos, as nomenclaturas, métricas e abordagens a serem utilizadas, e com isso, garantir interoperabilidade entre os diversos fabricantes. No que tange a qualidade, a ITU criou a especificação ITU G.114[ITU,1996] para definir as métricas mínimas de qualidade para transporte de voz, que possui os seguintes parâmetros principais:

- Atraso Unidirecional: o tempo para que a voz seja enviada pelo dispositivo de origem e chegue até o dispositivo de destino. Este tempo deve ser menor que 150 milisegundos para ligações nacionais e 300 milisegundos para ligações internacionais, principalmente quando utilizando satélites;
- *Jitter*: A variação no atraso unidirecional. Esta variação de atraso deve ser de 25 a 100 milisegundos;
- Perda de pacotes: pacotes que são enviados pela origem e não chegam ao destino por problemas no meio do caminho. Esta perda deve ser inferior a 1% no codec G.729[13] e até 2% no codec G.711[14].

Os codecs são os responsáveis por converter a voz analógica em voz digitalizada para ser enviada nos pacotes IP. Dentre o conjunto de codecs existentes, os mais populares atualmente são os codecs G.711 e G.729, e ambos funcionam com a taxa de transmissão de 50 pacotes por segundo, ou seja, um pacote a cada 20 milisegundos. Cada pacote possui 20 ms de voz digitalizada.

Considerando os tempos de *handover* observados nos experimentos nos experimento, associados à taxa de pacotes enviados por segundo pelos codecs, foram obtidos os seguin-

[12]ITU web site: http://www.itu.int/en/Pages/default.aspx
[13]Codec G.729: http://www.itu.int/rec/T-REC-G.729/en
[14]Codec G.711: http://www.itu.int/rec/T-REC-G.711/en

tes valores de perda de pacotes:

Experimento	Sentido	Tempo Médio	Desvio Padrão	Variância	Pacotes Perdidos
1	LISP 01 para LISP 02	26.91 ms	4.36	18.43	1 à 2
1	LISP 02 para LISP 01	24.78 ms	4.54	20.11	1 à 2
2	LISP 01 para Internet	21.87 ms	1.453	2.06	1 à 2
2	Internet para LISP 01	25.13 ms	1.07	1.11	2

Tabela 4.1. Comparativo das avaliações dos experimentos e associação com VoIP.

Ou seja, apesar de a perda de pacotes ser superior ao especificado (1%) em 1 segundo e esta perda ser em rajada, na prática, perdas de pacotes de até 5% podem ser toleradas pelo usuário[Sitolino, 2001] ou tratadas pelos codecs, como o G.729[Rosenberg, 2001].

Comparando com tempos apresentados para o MIP na SubSeção 2.2.2, onde os valores de convergência podem ser superiores à 300 milisegundos, os tempos de convergência observados nos experimentos para o LISP-MN foram aceitáveis dentro das métricas do VoIP. Porém, como será apresentado na Seção 4.4 e conforme foi apresentado na Seção 3.4, existem melhorias que podem ser implementadas no protocolo e nas implementações atuais que possibilitariam a melhoria do tempo de convergência do LISP-MN.

4.3.2 Resultados para o Experimento 3

No Experimento 3, o procedimento de coleta do tempo de convergência seguiu a mesma abordagem dos experimentos 1 e 2, onde o próprio LISPMob imprimiria o tempo após o *roaming* ocorrer. O resultado está apresentado na Figura 4.15 e na Tabela 4.2, informando a quantidade de pacotes perdidos durante o intervalo de *roaming*.

Tempo Médio	Desvio Padrão	Variância	Pacotes Perdidos
242.77 ms	10.36	105.51	13 unidades

Tabela 4.2. Avaliação do Experimento 3: Pacotes perdidos na convergência do LISP.

É possível observar pelos valores da Tabela 4.2, que os resultados podem ser considerados estáveis, mesmo para um ambiente de testes, e de escala mundial. O fato do tempo de propagação ser elevado, de 140 à 286 ms a depender do dispositivo envolvido, faz com

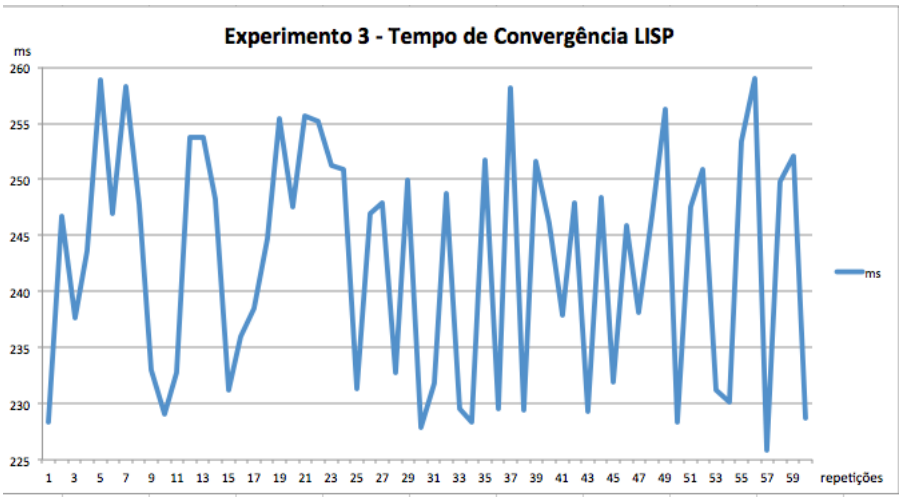

Figura 4.15. *Handovers* observados no experimento 3.

que os pacotes LISP enviados para atualizar as memórias *cache* demorem a chegar, e logo, a perda de pacotes acaba sendo elevada. Ainda assim, os experimentos confirmaram que o LISP-MN é uma solução funcional, que atende as suas especificações previstas e as recomendações listadas pelo *Mobile IP*, podendo ser utilizada atualmente, mesmo com o LISP-MN ainda em fase de especificação.

4.4 PROBLEMAS DETECTADOS

Apesar de o experimento ter sido composto por hardware e sistemas operacionais estáveis, o protocolo LISP ainda é uma proposta em construção, que desde o início da escrita deste projeto, recebeu mais de dez revisões e adições. Devido a este fato, tanto o software dos roteadores quanto o software do LISP-MN estão em fase de desenvolvimento constante, e por isso, alguns inconvenientes foram observados nos experimentos, e serão relatados abaixo.

4.4.1 Ausência de suporte para dupla consulta ao MR-MS nos roteadores

Conforme mencionado no Capítulo 3, os ITRs e PITRs, ao enviarem pacotes LISP para o LISP-MN, precisam fazer uma consulta para identificar quem é o LLOC responsável pelo EID do LISP-MN, e então fazer uma nova consulta, a partir do LLOC, para saber qual é o RLOC associado ao LLOC. Este fato força os roteadores LISP a terem que fazer duas consultas, e consequentemente, dois encapsulamentos LISP. Foi observado que os roteadores utilizados ainda não implementam tal funcionalidade, uma vez que a mesma tem uso apenas para o LISP-MN e engenharia de tráfego.

A ausência de suporte a essa funcionalidade faz com que, a partir da primeira consulta, os roteadores LISP precisem saber como alcançar o LLOC sem utilizar a abordagem do LISP, ou seja, foi necessário criar mapeamentos estáticos junto com rotas estáticas. Com isso, foi possível realizar os testes.

4.4.2 Ausência de suporte ao Map-Request do tipo SMR no MR-MS e ETR

Uma característica fundamental para diminuir o tempo de convergência do LISP-MN, é a capacidade dos ETRs e MR-MS atualizarem a memória *cache* dos ITR e PITR envolvidos na comunicação. Essa funcionalidade é possível através da mensagem *Map-Request SMR*, já prevista na especificação do LISP, porém a mesma ainda não foi implementada por ser uma funcionalidade nova, específica para mobilidade. Com isso, o experimento foi montado utilizando os recursos padrões do LISP. Esta funcionalidade será extremamente importante num cenário futuro de implantação do LISP-MN.

4.4.3 Travamentos nos códigos do roteador e do cliente

Além dos problemas referentes à ausência de implementação nos roteadores, outro problema detectado foi a falha do software do sistema operacional do roteador, onde em alguns momentos o equipamento parava de responder, ou perdia mensagens de atualização

de dados. Como o LISP funciona sobre protocolo UDP, estas perdas não eram percebidas pelo ambiente, o que fazia os roteadores descartarem tráfego em alguns momentos. Porém, dado que é um protocolo em fase de desenvolvimento e o código é de testes, é aceitável que este tipo de problema aconteça, e estes não foram impeditivos para que os experimentos acontecessem.

No próximo capítulo serão apresentadas as conclusões obtidas por este trabalho.

CAPÍTULO 5

CONCLUSÃO

O problema da sobrecarga de semântica do protocolo IP é o fator que mais dificulta a implantação da mobilidade, e, além disso, é o principal responsável pelo crescimento exponencial da tabela BGP global. Devido a estes problemas, diversas alternativas tem sido propostas na IETF nos últimos anos para solucionar essa sobrecarga. Nesse trabalho foi dado foco no protocolo LISP, cuja intenção inicial era resolver o problema de escalabilidade da Internet, mas, como o mesmo focou na separação da localização da identificação, tornou possível a adição de outras funcionalidades, como a mobilidade e o *multihoming*. Surgiu então o LISP *Mobile Node*, que apesar de ainda ser uma proposta, foi apresentado neste trabalho, avaliado e testado com resultados satisfatórios, tanto a nível de complexidade de implantação, como em tempo de convergência. O grande diferencial do LISP em relação às alternativas apresentadas -MIP, o HIP e o ILNP-, se apresenta no fato de que o LISP faz uso dos protocolos já existentes, sem exigir nenhuma alteração na implementação da pilha TCP/IP nos *hosts* para funcionar. O LISP-MN, por fazer uso da infraestrutura do LISP, aproveita essa vantagem, porém requer uma adição de código, apenas inserir o LISP-MN na pilha TCP/IP, mas, ainda assim, sem requerer mudanças nas demais camadas e aplicações. Além disso, funciona para o IPv4 e IPv6, e agrega a funcionalidade de *multihoming*.

Nos testes, foi verificado que o LISP-MN ainda possui pontos a serem trabalhados, principalmente relacionados ao duplo encapsulamento e dupla consulta aos *Map-Servers*, porém, estas fragilidades não inviabilizam o seu funcionamento, e o fato de fazer reuso de protocolos já existentes é um fator extremamente interessante para uma implementação gradual e interoperável do LISP no contexto da Internet.

Muitos dos resultados obtidos ao longo deste trabalho foram compartilhados com alguns membros do grupo de trabalho do LISP, porém, dado o caráter prático, é importante

ressaltar que o maior resultado obtido pelo trabalho foram os resultados indiretos, que foram obtidos pelo necessidade da interação com os envolvidos no LISP: a conscientização da comunidade de computação da UFBA sobre a IETF, sobre os grupos de trabalhos e oportunidades de pesquisa; o nome da UFBA que foi colocado no cenário mundial do LISP, sendo atualmente o único participante da América Latina; apresentação de artigo em evento de Internet do futuro[Bezerra et al., 2010b] ; o apoio da *Internet Society* para que alguns dos envolvidos no LISP na UFBA participassem das discussões nos Encontros do IETF, entre outros. Todos esses resultados indiretos estão mencionados na introdução.

A seguir, tópicos que ficam como sugestão para trabalhos futuros:

- Implementar as mudanças sugeridas em [Menth et al., 2010] e [Natal, 2012] e compará-las para verificar se existe melhoria no tempo de convergência do LISP ou se apenas adiciona funcionalidades;
- Realizar testes de convergência em ambientes com HIP e ILNP e compará-los com o LISP-MN, sob as mesmas condições;
- Divulgar a metodologia e resultados obtidos em Inglês para a comunidade do LISP;
- Implementar e testar, a fins de comparação, as abordagens de suporte ao NAT propostas no grupo de trabalho;
- Apoiar a implementação da ferramenta LISPMob, realizando testes e melhorias no código afim de reduzir o tempo de convergência.

APÊNDICE A

ESPECIFICAÇÕES TÉCNICAS DOS EXPERIMENTOS

Neste apêndice estão listados os equipamentos utilizados em cada experimento e suas as especificações:

A.1 EXPERIMENTO 1

O Experimento 1, que avaliou a mobilidade entre dois domínios LISP, estava assim composto:

- 1 roteador Cisco modelo 2821, com 256 MB de RAM e USBFLASH de 2 GB, versão do IOS: 15.2(4)XB10 e duas interfaces *Gigabit Ethernet* fazendo papel do **xTR** do domínio "LISP 1"e MR-MS de ambos os domínios;
- 1 roteador Cisco modelo 871, com 128 MB de RAM e FLASH de 28 MB, versão do IOS: 15.1(4).M5 e 5 interfaces *Fast Ethernet*, fazendo papel do **xTR** do domínio "LISP 2";
- 1 comutador D-Link DES-3526, com 24 interfaces *Fast Ethernet*, conectando todos os dispositivos físicos;
- 1 *Wireless Access Point* TP-Link 54G, com SSID "LISP 1", sem criptografia ou controles de acesso;
- 1 *Wireless Access Point* Linksys WRT54G, com SSID "LISP 2", sem criptografia ou controles de acesso;
- 1 notebook Dell Core i5, 4G de RAM com Debian Linux, kernel 2.6.32-5 com instalado com a última versão do LISPMob, fazendo papel do **LISP-MN**;

- 1 computador Dell Core i5, 4G de RAM com Microsoft Windows 7, fazendo papel de **SN**.

A.2 EXPERIMENTO 2

O Experimento 2, que avaliou a mobilidade entre um domínio LISP e o domínio "Internet", estava assim composto:

- 1 roteador Cisco modelo 2821, com 256 MB de RAM e USBFLASH de 2 GB, versão do IOS: 15.2(4)XB10 e duas interfaces *Gigabit Ethernet* fazendo papel do MR-MS e PxTR;
- 1 roteador Cisco modelo 871, com 128 MB de RAM e FLASH de 28 MB, versão do IOS: 15.1(4).M5 e 5 interfaces *Fast Ethernet*, fazendo papel do **xTR** do domínio "LISP 1";
- 1 comutador D-Link DES-3526, com 24 interfaces *Fast Ethernet*, conectando todos os dispositivos físicos;
- 1 *Wireless Access Point* TP-Link 54G, com SSID "LISP 1", sem criptografia ou controles de acesso;
- 1 *Wireless Access Point* Linksys WRT54G, com SSID "Internet", sem criptografia ou controles de acesso;
- 1 notebook Dell Core i5, 4G de RAM com Debian Linux, kernel 2.6.32-5 com instalado com a última versão do LISPMob, fazendo papel do **LISP-MN**;
- 1 computador Dell Core i5, 4G de RAM com Microsoft Windows 7, fazendo papel de **SN**.

A.3 EXPERIMENTO 3

O Experimento 3, que avaliou a mobilidade no ambiente real existente na Internet, foi composto da seguinte maneira:

- 1 notebook Dell Core i5, 4G de RAM com Debian Linux, kernel 2.6.32-5 com instalado com a última versão do LISPMob, fazendo papel do **LISP-MN**;
- 1 computador Dell Core i5, 4G de RAM com Debian Linux, fazendo papel de **SN**.

APÊNDICE B

INFORMAÇÕES ADICIONAIS PARA O EXPERIMENTO 3

Este apêndice tem por objetivo apresentar os valores obtidos de tempo de propagação (*rtt*), perda de pacotes e caminhos percorridos entre o LISP-MN e o SN para as demais entidades envolvidas no Experimento 3. Os valores médios de *rtt* são utilizados no experimento para dar noção de "distância"entre as entidades.

B.1 TESTES DE LATÊNCIA E PERDA DE PACOTES

A fim de obter os valores de latência (*rtt*) e perda de pacotes, foi utilizada a aplicação **ping**, disponibilizada por padrão na distribuição GNU/Linux Debian. O **ping** faz uso do protocolo ICMP[Postel, 1981b], onde o mesmo envia um conjunto de mensagens do tipo *ICMP Request* e recebe da entidade remota um conjunto de mensagens do tipo *ICMP Reply*. A diferença entre a quantidade enviada e recebida é utilizada para calcular a perda de pacotes, e a diferença de tempo entre o envio da mensagem *ICMP Request* e o recebimento da mensagem *ICMP Reply* é utilizada para calcular o tempo *round trip time* - *rtt*, que é o tempo de ida e volta.

Os testes de **ping** foram feitos enviando 200 pacotes com tamanho de 64 bytes. Nos testes realizados, é possível verificar o tempo *rtt* mínimo (min), médio (avg) e máximo (max), além do atraso médio gerado pelo próprio sistema operacional para fazer o teste solicitado (mdev). Estes valores podem ser observados a seguir:

- a partir do LISP-MN:

    1) Para o SN:

        – Perda de Pacotes: 0%

- rtt min/avg/max/mdev = 114.660/115.000/117.181/0.299 ms

2) Para o MR-MS (217.8.97.6):

- Perda de Pacotes: 0%
- rtt min/avg/max/mdev = 229.991/230.641/233.220/0.739 ms

3) Para o PETR (69.31.31.98):

- Perda de Pacotes: 0%
- rtt min/avg/max/mdev = 136.901/137.474/147.467/0.839 ms

4) Para o PITR (158.38.1.92):

- Perda de Pacotes: 0%
- rtt min/avg/max/mdev = 280.203/280.574/288.318/0.664 ms

- a partir do SN:

1) Para o MR-MS (217.8.97.6):

- Perda de Pacotes: 0%
- rtt min/avg/max/mdev = 114.361/114.466/114.811/0.255 ms

2) Para o PETR (69.31.31.98):

- Perda de Pacotes: 0%
- rtt min/avg/max/mdev = 26.855/27.434/40.590/1.300 ms

3) Para o PITR (158.38.1.92):

- Perda de Pacotes: 0%
- rtt min/avg/max/mdev = 156.562/156.669/162.044/0.614 ms

B.2 TESTES DE CAMINHOS

Para obter o caminho percorrido pelos pacotes entre o LISP-MN e o SN com os demais envolvidos no experimento, foram executados testes de mapeamento do caminho

utilizando a aplicação **traceroute**, disponível por padrão na distribuição GNU/Linux Debian. O funcionamento do **traceroute** se baseia no campo *Time To Live* do cabeçalho IP, e ocorre da seguinte maneira:

1) Um dispositivo de rede **Origem** gera um pacote IP, utilizando o protocolo UDP com porta 33434 e TTL igual a 1. Este pacote possui como endereço IP de destino o dispositivo que será testado, chamado pelo **traceroute** de **target** e é enviado para um roteador da rede do qual o dispositivo de rede faz parte;

2) Ao chegar ao roteador, o mesmo decrementa o TTL em uma unidade, resultando no TTL igual a 0. Ao verificar que o TTL é igual a 0, o roteador descarta o pacote e gera uma mensagem ICMP Tipo 11, Código 0, chamada de *time to live exceeded in transit* para o dispositivo **Origem**. O cabeçalho do pacote descartado é enviado na mensagem ICMP a fim ajudar o **Origem** a descobrir qual pacote foi descartado;

3) Ao receber a mensagem ICMP *time to live exceeded in transit*, o dispositivo **Origem** imprime o endereço IP de roteador que enviou a mensagem ICMP e o tempo *rtt*;

4) Em seguida, um novo pacote IP é gerado pelo dispositivo **Origem** com destino **target**, porém com TTL incrementado de 1, neste caso, 2. Este pacote é novamente enviado para um roteador da rede do qual **Origem** faz parte;

5) Após receber o pacote IP, o primeiro roteador decrementa o TTL, e como verifica que é maior que 0, encaminha para o próximo roteador. Este próximo roteador, decrementa o TTL, verifica que é 0 e envia uma mensagem ICMP *time to live exceeded in transit* para o dispositivo **Origem**.

6) Ao receber a mensagem ICMP *time to live exceeded in transit*, o dispositivo **Origem** imprime o endereço IP de roteador que enviou a mensagem ICMP e o tempo *rtt*, e envia um novo pacote IP para o mesmo destino porém com TTL incrementado em 1;

7) Esta sequência irá ocorrer até :

- ou que a mensagem ICMP *time to live exceeded in transit* recebida tenha sido enviada pelo dispositivo **target**;
- ou tenha alcançado um limite pré-estabelecido de TTL, no caso do **traceroute** do GNU/Linux Debian, 30.

A seguir, estão apresentados os testes de caminhos (**traceroute**) a partir do LISP-MN, utilizando parâmetros padrões do comando **traceroute** no GNU/Linux Debian:

Traceroute para o SN:

```
1  200.133.240.1 (200.133.240.1)  0.316 ms  0.295 ms  0.758 ms
2  200.133.241.222 (200.133.241.222)  1.512 ms  1.505 ms  1.493 ms
3  200.143.255.22 (200.143.255.22)  2.598 ms 2.598 ms  2.588 ms
4  200.0.204.129 (200.0.204.129)  3.033 ms  3.047 ms  3.036 ms
5  198.32.252.205 (198.32.252.205)  114.963 ms  114.977 ms  114.974 ms
6  SN (SN)  114.949 ms  114.732 ms  114.716 ms
```

Traceroute para o MR-MS:

```
1  200.133.240.1 (200.133.240.1)  0.332 ms  0.322 ms  0.316 ms
2  200.133.241.222 (200.133.241.222)  0.726 ms  0.722 ms  0.716 ms
3  200.143.255.22 (200.143.255.22)  2.500 ms 2.498 ms  2.492 ms
4  200.143.254.234 (200.143.254.234)  110.236 ms 110.234 ms  110.228 ms
5  195.22.199.209 (195.22.199.209)  110.223 ms 110.219 ms  110.215 ms
6  77.67.71.97 (77.67.71.97)  110.207 ms  110.261 ms 110.249 ms
7  89.149.182.242 (89.149.182.242)  224.409 ms  227.685 ms 227.676 ms
8  141.136.98.30 (141.136.98.30)  229.624 ms  230.482 ms  230.473 ms
9  217.8.98.5 (217.8.98.5)  227.585 ms  227.610 ms  227.885 ms
10  217.8.97.6 (217.8.97.6)  222.000 ms  221.992 ms  221.956 ms
```

Traceroute para o PITR:

```
1  200.133.240.1 (200.133.240.1)  0.266 ms  0.243 ms  0.232 ms
2  200.133.241.222 (200.133.241.222)  0.700 ms  0.697 ms  0.690 ms
3  200.143.255.22 (200.143.255.22)  2.509 ms 2.499 ms  2.466 ms
4  200.0.204.129 (200.0.204.129)  3.032 ms  3.039 ms  3.035 ms
5  62.40.124.137 (62.40.124.137)  220.392 ms  220.394 ms  220.374 ms
6  62.40.112.25 (62.40.112.25)  242.709 ms  242.804 ms  242.771 ms
7  62.40.112.14 (62.40.112.14)  242.720 ms  242.595 ms  242.599 ms
8  62.40.98.109 (62.40.98.109)  251.062 ms  251.086 ms  251.077 ms
9  62.40.98.133 (62.40.98.133)  265.173 ms  265.116 ms  265.147 ms
10  62.40.124.46 (62.40.124.46)  259.280 ms 259.296 ms  259.290 ms
11  109.105.97.14 (109.105.97.14)  259.716 ms  259.724 ms  260.417 ms
12  109.105.102.26 (109.105.102.26)  268.980 ms  268.938 ms  269.438 ms
13  128.39.255.49 (128.39.255.49)  272.725 ms  284.297 ms  279.553 ms
14  128.39.47.17 (128.39.47.17)  272.601 ms  268.204 ms  268.205 ms
15  128.39.255.46 (128.39.255.46)  275.660 ms  275.637 ms  275.633 ms
16  128.39.255.194 (128.39.255.194)  275.906 ms  275.677 ms  275.662 ms
17  128.39.230.186 (128.39.230.186)  275.615 ms  276.351 ms  276.336 ms
18  158.38.1.92 (158.38.1.92)  280.763 ms  280.359 ms 280.627 ms
```

Traceroute para o PETR:

```
1  200.133.240.1 (200.133.240.1)  0.376 ms  0.346 ms  0.333 ms
2  200.133.241.222 (200.133.241.222)  0.778 ms  0.769 ms  0.745 ms
3  200.143.255.22(200.143.255.22)  29.341 ms 2.487 ms  29.340 ms
4  200.143.254.234 (200.143.254.234)  109.944 ms 109.942 ms  110.176 ms
5  198.32.252.121 (198.32.252.121)  110.164 ms  110.158 ms  110.146 ms
6  108.59.27.16 (108.59.27.16)  111.919 ms  110.935 ms  112.174 ms
7  108.59.31.18 (108.59.31.18)  118.019 ms  118.278 ms  118.057 ms
8  108.59.31.16(108.59.31.16)  117.994 ms  118.025 ms  117.996 ms
9  137.164.131.53 (137.164.131.53)  136.600 ms 136.577 ms  136.517 ms
```

```
10  206.126.236.60 (206.126.236.60)  143.144 ms 143.122 ms  143.065 ms
11  69.31.31.130 (69.31.31.130)  144.089 ms  144.105 ms  144.429 ms
12  69.31.31.98 (69.31.31.98)  137.398 ms 137.594 ms 137.149 ms
```

A seguir, estão apresentados os testes de caminhos (**traceroute**) a partir do SN, utilizando parâmetros padrões do comando **traceroute** no GNU/Linux Debian:

Traceroute para o MR-MS:

```
 1  198.32.252.1 (198.32.252.1)  0.315 ms  0.347 ms  0.336 ms
 2  198.32.252.23 (198.32.252.23)  0.482 ms  0.565 ms  0.576 ms
 3  198.32.252.17 (198.32.252.17)  0.270 ms  0.247 ms  0.233 ms
 4  195.22.199.209 (195.22.199.209)  0.276 ms  0.309 ms  0.287 ms
 5  77.67.71.97 (77.67.71.97)  0.302 ms  0.308 ms  0.299 ms
 6  89.149.182.250 (89.149.182.250)  108.580 ms 115.388 ms  115.468 ms
 7  141.136.98.30(141.136.98.30)  115.032 ms  114.114 ms  113.920 ms
 8  217.8.98.5 (217.8.98.5)  115.152 ms  114.177 ms  114.109 ms
 9  217.8.97.6 (217.8.97.6)  114.946 ms  114.937 ms  113.552 ms
```

Traceroute para o PITR:

```
 1  198.32.252.1 (198.32.252.1)  0.377 ms  0.334 ms  0.396 ms
 2  198.32.252.238 (198.32.252.238)  13.339 ms  13.323 ms  13.327 ms
 3  64.57.28.7 (64.57.28.7)  26.175 ms  26.162 ms  26.171 ms
 4  64.57.28.192 (64.57.28.192)  31.254 ms  31.248 ms  31.236 ms
 5  109.105.98.9 (109.105.98.9)  35.669 ms  35.666 ms  35.645 ms
 6  109.105.97.14 (109.105.97.14)  135.975 ms 127.865 ms  127.859 ms
 7  109.105.102.26 (109.105.102.26)  136.974 ms  137.075 ms  137.044 ms
 8  128.39.255.85 (128.39.255.85)  148.838 ms  148.953 ms  148.999 ms
 9  128.39.47.17 (128.39.47.17)  140.454 ms  140.438 ms  140.417 ms
10  128.39.255.46 (128.39.255.46)  143.190 ms  143.170 ms  151.449 ms
```

```
11  128.39.255.194 (128.39.255.194)  157.019 ms  148.651 ms  148.679 ms
12  128.39.230.186 (128.39.230.186)  151.796 ms  143.337 ms  143.407 ms
13  158.38.1.92 (158.38.1.92)  148.467 ms  148.404 ms 148.479 ms
```

Traceroute para o PETR:

```
 1  198.32.252.1 (198.32.252.1)  0.381 ms  0.356 ms  0.432 ms
 2  198.32.252.23 (198.32.252.23)  0.563 ms  0.633 ms  0.758 ms
 3  198.32.252.17 (198.32.252.17)  9.118 ms  9.104 ms  9.186 ms
 4  198.32.252.121 (198.32.252.121)  0.279 ms  0.261 ms  0.245 ms
 5  108.59.27.16 (108.59.27.16)  2.152 ms  2.146 ms  2.135 ms
 6  108.59.31.18 (108.59.31.18)  8.416 ms  8.407 ms  9.781 ms
 7  108.59.31.16 (108.59.31.16)  8.232 ms  8.454 ms  8.473 ms
 8  137.164.131.53 (137.164.131.53)  26.719 ms  26.738 ms  26.722 ms
 9  206.126.236.60 (206.126.236.60)  26.734 ms  57.316 ms  26.784 ms
10  69.31.31.130 (69.31.31.130)  30.508 ms  31.051 ms  30.450 ms
11  69.31.31.98 (69.31.31.98)  27.158 ms  27.149 ms 27.039 ms
```

BIBLIOGRAFIA

[ANATEL, 2012] ANATEL (2012). Quantidade de acessos/plano de serviço/unidade da federação. *URL: http://sistemas.anatel.gov.br/SMP/Administracao/ Consulta/AcessosPrePosUF/tela.asp?SISQSmodulo=18267*. [Inserir mês Abril, ano 2012].

[Arraez et al., 2011] Arraez, L., Chaouchi, H., and Aydin, Z. (2011). Performance evaluation and experiments for host identity protocol. *International Journal of Computer Science*, 8(2):74–83.

[Atkinson and Bhatti, 2006] Atkinson, R. and Bhatti, S. (2006). An introduction to the identifier-locator network protocol (ilnp). *URL: http://www.cs.st-andrews.ac.uk/s̃aleem/papers/2006/lcs/ilnp/ab2006.pdf*. [Online; acessado em 08-Março-2013].

[Atkinson et al., 2009] Atkinson, R., Bhatti, S., and Hailes, S. (2009). Ilnp: mobility, multi-homing, localised addressing and security through naming. *Telecommunication Systems*, 42(3):273–291.

[Bates and Huston, 2009] Bates, T. and Huston, G. (2009). Routing table analysis reports. APNIC: Internet WebSite.

[Bezerra et al., 2010a] Bezerra, J., Galiza, H., Barreto, L., Mendonça, L., and Alves, C. (2010a). Lisp as a solution for internet scalability.

[Bezerra et al., 2010b] Bezerra, J., Galiza, H., Barreto, L. P., Mendonça, L. C., and Alves, C. (2010b). Lisp as a solution for internet scalability.

[Bokor et al., 2009] Bokor, L., Nováczki, S., Zeke, L., and Jeney, G. (2009). Design and evaluation of host identity protocol (hip) simulation framework for inet/omnet++. In *Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems*, pages 124–133. ACM.

[Bonaventure, 2007] Bonaventure, O. (2007). Reconsidering the internet routing architecture. Technical report, UCLouvain. draft-bonaventure-irtf-rrg-rira-00.txt.

[Carpenter, 2009] Carpenter, E. B. (2009). Observed relationships between size measures of the internet. *ACM SIGCOMM Computer Communication Review*, 39:5–12.

[Cisco, 2012] Cisco (2012). Global mobile data traffic forecast update. *URL: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html*.

[Crow et al., 1997] Crow, B., Widjaja, I., Kim, L., and Sakai, P. (1997). Ieee 802.11 wireless local area networks. *Communications Magazine, IEEE*, 35(9):116–126.

[Deering, 1996] Deering, S. (1996). The map & encap scheme for scalable ipv4 routing with portable site prefixes. *URL: http://irl.cs.ucla.edu/references/Deering-encap.pdf*.

[Deering and Hinden, 1998] Deering, S. and Hinden, R. (1998). Rfc2460: Internet protocol, version 6. *URL: http://tools.ietf.org/html/rfc2460*.

[Diab, 2004] Diab, A. (2004). Minimizing mobile ip handoff latency. *URL: http://researchwebshelf.com/uploads/168_P48.pdf*.

[Droms, 1997] Droms, R. (1997). Rfc2131: Dynamic host configuration protocol. *URL: http://tools.ietf.org/html/rfc2131.html*.

[Eddy, 2004] Eddy, W. (2004). At what layer does mobility belong? *Communications Magazine, IEEE*, 42(10):155–159.

[Egevang and Francis, 1994] Egevang, K. and Francis, P. (1994). Rfc1631: The ip network address translator (nat). *URL: http://tools.ietf.org/html/rfc1631*.

[Ergen et al., 2002] Ergen, M., Coleri, S., Dundar, B., Puri, A., Walrand, J., and Varaiya, P. (2002). Position leverage smooth handover algorithm for mobile ip. *URL: http://ofdm.eecs.berkeley.edu/ergen/docs/fastmip8-50x6-00.pdf*.

[Farinacci and Fuller, 2012] Farinacci, D. and Fuller, V. (2012). Rfc6830: The locator/id separation protocol (lisp). *URL: http://tools.ietf.org/html/rfc6830*.

[Farinacci et al., 2012a] Farinacci, D., Fuller, V., Lewis, D., and Meyer, D. (2012a). Lisp mobile node - draft 08. *URL: http://tools.ietf.org/html/draft-meyer-lisp-mn-08*.

[Farinacci et al., 2012b] Farinacci, D., Fuller, V., Meyer, D., and Lewis, D. (2012b). Lisp mobile node - draft 00. *URL: http://tools.ietf.org/html/draft-meyer-lisp-mn-00 (obsoleted)*.

[Freitas, 2009] Freitas, G. (2009). A escalabilidade da internet e uma nova perspectiva do roteamento com o protocolo lisp.

[Gohar and Koh, 2011] Gohar, M. and Koh, S. J. (2011). Distributed handover control in localized mobile lisp networks. In *Wireless and Mobile Networking Conference (WMNC), 2011 4th Joint IFIP*, pages 1–7. IEEE.

[Group, 2005] Group, T. (2005). Evaluation of wireless/voip roaming/performance and functionality. *URL: http://www.extremenetworks.com/libraries/products/Evr_Prod_SummitWM_Pub_PV_SummitWMTolllyReport.pdf/*. [Online; acessado em 20-Fevereiro-2013].

[Guimaraes et al., 2006] Guimaraes, A., Lins, R., de Oliveira, R., and Lins, R. (2006). *Segurança com redes privadas virtuais VPNs*. Brasport.

[ITU-T, 2000] ITU-T (2000). G. 114. *One-way transmission time*, 18.

[Jain, 1991] Jain, R. (1991). *Art of Computer Systems Performance Analysis Techniques For Experimental Design Measurements Simulation And Modeling*. Wiley Computer Publishing.

[Jen et al., 2008] Jen, D., Meisel, M., Yan, H., Massey, D., Wang, L., Zhang, B., and Zhang, L. (2008). Towards a new internet routing architecture: Arguments for separating edges from transit core. *Proceedings of the Seventh ACM Workshop on Hot Topics in Networks (HotNets-VII)*.

[Johnson et al., 2004] Johnson, D., Perkins, C., and Arkko, J. (2004). Rfc3775: Mobility support in ipv6. *URL: http://tools.ietf.org/html/rfc3775*.

[Kent and Seo, 2008] Kent, S. and Seo, K. (2008). Rfc4301: Security architecture for the internet protocol. *URL http://tools.ietf.org/html/rfc4301*.

[Khurri et al., 2009] Khurri, A., Kuptsov, D., and Gurtov, A. (2009). Performance of host identity protocol on symbian os. In *Communications, 2009. ICC'09. IEEE International Conference on*, pages 1–6. IEEE.

[Klein et al., 2010] Klein, D., Hartmann, M., and Menth, M. (2010). Nat traversal for lisp mobile node. In *Proceedings of the Re-Architecting the Internet Workshop*, page 8. ACM.

[Koh et al., 2004] Koh, S., Lee, M., Riegel, M., Ma, M., and Tuexen, M. (2004). Mobile sctp for transport layer mobility. *URL: http://tools.ietf.org/html/draft-sjkoh-sctp-mobility-04*.

[Kuang et al., 2004] Kuang, Y., Long, K., Chen, Q., and Li, Y. (2004). Mobile transmission control protocol (mtcp) for mobility management over ip networks. *URL: http://doc.tm.uka.de/i-d/individual/kuangyj/draft-kuangyj-mobile-tcp.pdf.gz*.

[Mandeville, 2012] Mandeville, B. (2012). Testing wlan roaming step by step. *URL:http://www.iometrix.com/whitepapers/Iometrix_WPv3.pdf/*. [Online; acessado em 21-Dezembro-2012].

[Martinez, 2008] Martinez, J. (2008). *Enabling efficient and operational mobility in large heterogeneous IP networks*. Jordi Palet Martinez Books.

[Menth et al., 2010] Menth, M., Klein, D., and Hartmann, M. (2010). Improvements to lisp mobile node. In *22nd International Teletraffic Congress (ITC)*, pages 1–8.

[Meyer et al., 2007] Meyer, D., Zhang, L., Fall, K., et al. (2007). Rfc2439: Report from the iab workshop on routing and addressing. *URL: http://tools.ietf.org/html/rfc2439*.

[Mockapetris, 1987] Mockapetris, P. (1987). Rfc1035: Domain names - implementation and specification. *URL: http://tools.ietf.org/html/rfc1035*.

[Moskowitz, 2012] Moskowitz, R. (2012). Rfc5201 : Host identity protocol architecture. *URL: http://tools.ietf.org/html/rfc5201.html*.

[Natal, 2012] Natal, A. (2012). Privacy extensions for lisp-mn. *URL: http://lispmob.org/sites/default/files/users/user6/memoria.pdf*.

[Nikander and Moskowitz, 2006] Nikander, P. and Moskowitz, R. (2006). Host identity protocol (hip) architecture. *URL: http://tools.ietf.org/html/rfc4423*.

[Perkins, 1996] Perkins, C. (1996). Rfc2002: Mobility support. *URL: http://tools.ietf.org/html/rfc2002*.

[Perkins et al., 2002a] Perkins, C. et al. (2002a). Rfc 3344: Ip mobility support for ipv4 (obseleted by rfc4721). *URL: Network Working Group*.

[Perkins et al., 2002b] Perkins, C. et al. (2002b). Rfc3220: Ip mobility support for ipv4 (obseleted by rfc3344). *Network Working Group*.

[Perkins et al., 2010] Perkins, C. et al. (2010). Rfc5944: Ip mobility support for ipv4. *URL: http://tools.ietf.org/html/rfc1631*.

[Ping et al., 2011] Ping, D., Jia, C., and Zhang, H. (2011). A network-based localized mobility approach for locator/id separation protocol. *IEICE Transactions on Communications*, 94(6):1536–1545.

[Postel, 1981a] Postel, J. (1981a). Rfc791: Internet protocol. *URL: http://tools.ietf.org/html/rfc791*.

[Postel, 1981b] Postel, J. (1981b). Rfc792: Internet control message protocol. *URL: http://tools.ietf.org/html/rfc792*.

[Rathi and Thanushkodi, 2009] Rathi, S. and Thanushkodi, K. (2009). Performance analysis of mobile ip registration protocols. *W. Trans. on Comp.*, 8(3):538–548.

[Rehkter, 1995] Rehkter, Y., L. T. (1995). Rfc1771: A border gateway protocol (bgp version 4). *URL: http://tools.ietf.org/html/rfc1771.html*.

[Reis, 2008] Reis, E. A. (2008). Irtf/rrg - resumo de trabalhos e o protocolo lisp - 25? reuni?o do gter - nic.br. Technical report, NIC.BR.

[Rekhter and Li, 1995] Rekhter, Y. and Li, T. (1995). Rfc 1771. *A Border Gateway Protocol*, 4:1–54.

[Rosenberg, 2001] Rosenberg, J. D. (2001). G. 729 error recovery for internet telephony. *URL: http://www.cs.columbia.edu/l̃ibrary/TR-repository/reports/reports-2001/cucs-016-01.pdf*.

[Saltzer, 1993] Saltzer, J. (1993). On the naming and binding of network destinations. Technical report, M.I.T. Laboratory for Computer Science.

[Saucez et al., 2012] Saucez, D., Bonaventure, O., and Iannone, L. (2012). Lisp map-versioning - draft 09. *URL: http://tools.ietf.org/html/draft-ietf-lisp-map-versioning-09*.

[Schulzrinne et al., 2003] Schulzrinne, H., Casner, C., Frederick, R., and Jacobson, V. (2003). Rfc3550: Real-time transport protocol. *URL: http://tools.ietf.org/html/rfc3550*.

[Schulzrinne et al., 1999] Schulzrinne, H., Schooler, E., and Rosenberg, J. (1999). Rfc2543: Session initiation protocol. *URL: http://tools.ietf.org/html/rfc2543*.

[Shoch et al., 1982] Shoch, J. F., Dalal, Y. K., Redell, D. D., and Crane, R. C. (1982). Evolution of the ethernet local computer network. *Computer*, 15(8):10–27.

[Sitolino, 2001] Sitolino, C. L. (2001). Voip: um estudo experimental. *URL: http://www.lume.ufrgs.br/bitstream/handle/10183/3182/000333405.pdf?sequence=1*.

[Spurgeon, 2000] Spurgeon, C. (2000). *Ethernet: The Definitive Guide*. O'Reilly.

[Tanenbaum, 2007] Tanenbaum, A. S. (2007). *Modern Operating Systems, Third Edition*. Prentice Hall.