Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Edwin Santos Cordeiro

Comparação de técnicas de transição do IPv4 para o IPv6

São Paulo

2014

Edwin Santos Cordeiro

Comparação de técnicas de transição do IPv4 para o IPv6

Dissertação de Mestrado apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, como parte dos requisitos para a obtenção do título de Mestre em Engenharia de Computação.
Área de concentração: Redes de Computadores.

Data da aprovação ____/____/_____

_____
Prof. Dr. Wagner Luiz Zucchi (Orientador)
IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Membros da Banca Examinadora:

Prof. Dr. Wagner Luiz Zucchi (Orientador)
IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Prof. Dr. Demi Getschko (Membro)
Pontifica Universidade Católica de São Paulo

Prof. Dr. Geraldo Lino de Campos (Membro)
IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Edwin Santos Cordeiro

Comparação de técnicas de transição do IPv4 para o IPv6

Dissertação de mestrado apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, como parte dos requisitos para a obtenção do título de Mestre em Engenharia de Computação
Área de concentração: Redes de Computadores

Orientador: Prof. Dr. Wagner Luiz Zucchi

São Paulo

2014

Ficha Catalográfica
Elaborada pelo Departamento de Acervo e Informação Tecnológica – DAIT
do Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT

C794c **Cordeiro, Edwin Santos**
Comparação de técnicas de transição do IPv4 para o IPv6. / Edwin Santos Cordeiro. São Paulo, 2014.
94p.

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

Orientador: Prof. Dr. Wagner Luiz Zucchi

1. Técnica de transição 2. IPv4 3. IPv6 4. Pilha dupla restrita 5. Avaliação de desempenho 6. Viabilidade técnica 7. Viabilidade econômica 8. Redes de computadores 9. Tese I. Zucchi, Wagner Luiz, orient. II. IPT. Coordenadoria de Ensino Tecnológico III. Título

14-40 CDU 004.7(043)

Dedicatória

Dedico este trabalho a minha esposa Leila e sua paciência nos momentos que não lhe dei a atenção devida para que eu pudesse me dedicar a este trabalho. Também dedico aos meus pais, Estrela e Eudoxio, aos meus irmãos, Etienne e Ewald, a minha avó Floripes e as madrinhas Celina e Rose Mary por entenderem que meu desaparecimento de eventos familiares foram motivados pelos intermináveis fins de semanas necessários para a realização deste trabalho.

Agradecimentos

Agradeço ao Professor Wagner Luiz Zucchi cuja orientação guiou este trabalho.

Agradeço ao NIC.br, personificado pelo seu Diretor-presidente Demi Getschko, pelo auxílio estudantil que ajudou no custeio deste mestrado e pelo empréstimo de alguns equipamentos utilizados nos testes e a equipe do CEPTRO.br, com Milton Kashiwakura como Diretor, Antonio M. Moreiras como Gerente de Projetos e ao restante da equipe que ajudou direta ou indiretamente, Rodrigo R. dos Santos, Alexandre Harano, Heitor Ganzeli, Eduardo Barasal, Tiago Jun Nakamura e Tuany Tabosa. E um agradecimento especial a Rodrigo Carnier que ajudou com realização da parte mais braçal dos testes, e pelas fotos no teste do Skype onde ele aparece.

Agradeço também a Avnet do Brasil que custeou o primeiro ano deste mestrado.

Resumo

A transição do IPv4 para o IPv6 é necessária por causa do esgotamento de endereços IPv4. A técnica originalmente planejada para esta transição, a pilha dupla, não está sendo utilizada em larga escala e não resolve o problema de comunicação entre redes que só possuem uma versão do protocolo IP. Este fato levou à criação de técnicas que pudessem alongar o período de transição. Este trabalho tem o objetivo de fazer uma comparação entre as técnicas de pilha dupla restrita, desenvolvidas pelo grupo Softwire do IETF, que buscam compartilhar endereços IPv4 entre múltiplos usuários e transportar estes pacotes IPv4 através de rede somente IPv6. O compartilhamento pode ser feito através de NAT no provedor de acesso (CGN) ou da restrição de portas utilizáveis atribuídas a cada usuário final (A+P). O transporte pode ser feito através do encapsulamento de pacotes IPv4 como dados de pacotes IPv6 ou da dupla tradução. As técnicas analisadas são o DS-Lite, o 464XLAT, o MAP-E, o MAP-T e o NAT444. A avaliação destas técnicas é feita com base na medição da utilização da rede e mensuração do *overhead* gerado pelas técnicas, na medição do processamento e memória RAM utilizados nos equipamentos de rede que executam estas técnicas e no funcionamento ou não, através de redes com estas técnicas de transição, dos programas mais comuns que fazem uso da Internet.

Palavras chaves: Técnicas de transição de IPv4 para IPv6, pilha dupla restrita, desempenho, experiência do usuário, viabilidade

Abstract

A comparison of IPv4 to IPv6 transition techniques

The IPv4 to IPv6 transition is needed due to the exaustion of IPv4 addresses. The original transition technique, the dual stack, is not largely deployed yet and doesn't allow the communication between networks with only one version of the IP protocol. This fact caused the creation of techniques to extend the transition period. This research does a comparison on the limited dual stack transition techniques, developed by the IETF's Softwire Group, that share IPv4 addresses with multiple users and transport IPv4 packets through IPv6 only networks. The sharing of IPv4 addresses may be through NAT at the Internet service provider (CGN) or through the an restriction on the ports that each final user may use (A+P). The transport may be by encapsulation of IPv4 packets as data of IPv6 packets or by double translation. The analyzed techniques are DS-Lite, 464XLAT, MAP-E, MAP-T and the NAT444. The evaluation of those techniques is made by comparing the network throughput and overhead of each technique, the processor and RAM memory used on the network equipment running the techniques and by checking if the most common usages and programs that use the Internet work correctly on the test networks.

Keywords: IPv4 to IPv6 transition techniques, Limited dual stack, performance, user experience, feasibility

Lista de Figuras

2.1 Taxonomia das técnicas de transição do IPv4 para o IPv6 31

2.2 Topologia do DS-Lite 33

2.3 Diagrama de Sequência do DS-Lite 34

2.4 Topologia do MAP-E 36

2.5 Diagrama de Sequência do MAP-E 37

2.6 Topologia do 464XLAT 38

2.7 Diagrama de Sequência do 464XLAT 39

2.8 Topologia do MAP-T 40

2.9 Diagrama de Sequência do MAP-T 41

2.10 Topologia do NAT444 42

2.11 Diagrama de Sequência do NAT444 43

3.1 Topologia usada para os testes 51

4.1 Skype em uma rede com IPv4 público versus Skype em uma rede com 464XLAT, para um cliente Windows 61

5.1 Uso de CPU no CPE x Tamanho do Pacote x Técnica 67

5.2 Atraso de Propagação x Técnica 68

5.3 *Jitter* x Tamanho do Pacote x Técnica 69

5.4 Perda de Pacotes x Tamanho do Pacote x Técnica 70

5.5 Banda Efetiva x Tamanho do Pacote x Técnica 71

A.1 Foto dos equipamentos utilizados 87

A.2 Configuração DS-Lite no CPE 88

A.3 Configuração DS-Lite no roteador de borda 88

A.4 Configuração 464XLAT no CPE CLAT 89

A.5 Script de inicialização do 464XLAT no CPE CLAT 89
A.6 Configuração 464XLAT no roteador de borda PLAT 90
A.7 Script de inicialização do 464XLAT no roteador de borda PLAT 90
A.8 Configuração MAP-E no CPE 91
A.9 Configuração MAP-E no roteador de borda 92
A.10 Configuração MAP-T no CPE 93
A.11 Configuração MAP-T no roteador de borda 94

Lista de Tabelas

1.1 Recursos necessários para a realização do trabalho 28

2.1 Comparativo de funcionamento entre as técnicas de pilha dupla restrita 32

3.1 Sistemas utilizados para a realização dos testes 51

4.1 Resultado para buscas na Internet 54

4.2 Resultado para acesso a e-mail 55

4.3 Resultado para acesso a rede social 55

4.4 Resultado para acesso a video *on line* 56

4.5 Resultado para baixar arquivos usando redes *peer to peer* 57

4.6 Resultado para ler notícias 58

4.7 Resultado para acesso a banco via Internet 59

4.8 Resultado para chamada de vídeo 59

4.9 Resultado para jogos via Internet 60

4.10 Resultado para VPN IPSec/L2TP 62

Lista de abreviaturas e siglas

AFTR	*Address Family Transition Router*
APNIC	*Asia Pacific Network Information Centre*
A+P	*Address plus Port*
CERNET	*China Education and Research Network*
CETIC.br	Centro de Estudos sobre as Tecnologias da Informação e da Comunicação
CGN	*Carrier-grade NAT*
CLAT	*Customer-side Translator*
CPE	*Customer Premises Equipment*
CPU	*Central processing unit*
DS-Lite	*Dual-Stack Lite*
IANA	*Internet Assigned Numbers Authority*
IETF	*Internet Engineering Task Force*
IGD-PCP IWF	*Internet Gateway Device - Port Control Protocol Interworking Function*
IMAP	*Internet Message Access Protocol*
IP	*Internet Protocol*
IPSec	*Internet Protocol Security*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
ISATAP	*Intra-Site Automatic Tunnel Addressing Protocol*
LACNIC	Registro de Endereçamento da Internet para América Latina e Caribe
LSN	*Large Scale NAT*
L2TP	*Layer 2 Tunneling Protocol*
MAP-E	*Mapping of Address and Port with Encapsulation*
MAP-T	*Mapping of Address and Port using Translation*
MPLS	*Multiprotocol Label Switching*

NAT	*Network address translation*
NAT444	*Network address translations at customer's private network and carrier's private network*
NAT64	*Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*
PCP	*Port Control Protocol*
PLAT	*Provider-side Translator*
ps	*Process Status*
RIPE	*Regional Internet Registry for Europe*
sar	*System Activity Reporter*
SMTP	*Simple Mail Transfer Protocol*
TCP	*Transmission Control Protocol*
top	*Terminal Process Overview*
UDP	*User Datagram Protocol*
UPnP	*Universal Plug and Play*
VPN	*Virtual private network*
464XLAT	*Combination of Stateful IPv6 to IPv4 and Stateless IPv4 to IPv6 Translations*
6over4	*Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*
6PE	*IPv6 Provider Edge router*
6to4	*Connection of IPv6 Domains via IPv4 Clouds*

Sumário

1 INTRODUÇÃO **21**

1.1 Motivação 22

1.2 Objetivo 23

1.3 Contribuições 24

1.4 Método de trabalho 24

1.5 Organização do trabalho 26

1.6 Recursos Necessários 27

2 ESTADO DA ARTE **29**

2.1 Técnicas de Transição de IPv4 para IPv6 29

2.1.1 Taxonomia das Técnicas de Transição de IPv4 para IPv6 30

2.1.2 Detalhamento das Técnicas Comparadas neste Trabalho 30

2.1.2.1 Detalhamento DS-Lite 32

2.1.2.2 Detalhamento MAP-E 33

2.1.2.3 Detalhamento 464XLAT 35

2.1.2.4 Detalhamento MAP-T 38

2.1.2.5 Detalhamento NAT444 40

2.2 Comparações de Técnicas de Transição de IPv4 para IPv6 42

3 CRITÉRIOS DE COMPARAÇÃO **47**

3.1 Critérios para análise qualitativa 47

3.2 Critérios para análise quantitativa 48

3.3 Critérios para análise de viabilidade 49

3.4 Definição dos testes 49
3.5 Topologia de rede 50

4 RESULTADOS EXPERIMENTAIS 53

4.1 Resultados da Análise Qualitativa 53
4.1.1 Busca na Internet 54
4.1.2 Acesso a e-mail 54
4.1.3 Rede social 55
4.1.4 Vídeo *on line* 56
4.1.5 Transferência de arquivos usando redes *peer to peer* 56
4.1.6 Ler notícias 58
4.1.7 Banco via Internet 58
4.1.8 Chamada de vídeo 59
4.1.9 Jogos via Internet 60
4.1.10 IPSec / L2TP 62

5 COMPARAÇÃO QUANTITATIVA 65

5.1 Resultados da Análise Quantitativa 65
5.2 Comparação com Outros Trabalhos 71

6 ANÁLISE DE VIABILIDADE 73

6.1 Viabilidade Técnica 73
6.2 Viabilidade Econômica 75

7 CONCLUSÕES 79

REFERÊNCIAS 83

A Apêndice A: Detalhamento das configurações dos testes 87

A.1 Equipamentos Utilizados 87
A.2 Configurações do DS-Lite 88
A.3 Configurações do 464XLAT 89
A.4 Configurações do MAP-E 91
A.5 Configurações do MAP-T 93

1 INTRODUÇÃO

O famoso pesquisador Vinton Cerf, por muitos considerado o pai da Internet, foi perguntado em entrevista sobre o que ele faria de diferente com relação ao TCP/IP se pudesse voltar ao passado. Sua resposta foi: "Eu gostaria de ter notado que nós iríamos precisar de mais que 32 bits de endereçamento! Na época, eu achei que ainda era um experimento e que, se bem sucedido, nós iríamos desenvolver a versão de produção. Eu acho que o IPv6 é a versão de produção!" (CERF, 2011).

Além de 7,9 x 10^{28} vezes mais endereços e quatro vezes a quantidade de bits de endereçamento do Protocolo Internet versão 4 (IPv4 - *Internet Protocol version 4*) (IETF - RFC 791, 1981), o Protocolo Internet versão 6 (IPv6 - *Internet Protocol version 6*) (IETF - RFC 4291, 2006) acrescentou funções que não faziam parte do protocolo IPv4, entre elas a descoberta de vizinhança. Outra mudança importante é que o cabeçalho passou a ter um tamanho fixo e para colocar informações adicionais, como fragmentação, são utilizados cabeçalhos de extensão que não existiam na versão anterior.

A não utilização do protocolo IPv6 pode ocasionar a criação de diversas redes privadas de operadoras. Isto fará com que os clientes de uma determinada operadora somente tenham acesso aos serviços e conteúdos de interesse desta operadora, permitindo a discriminação do tráfego e de provedores de conteúdo. Esta interferência fere o princípio da neutralidade da rede, uma das bases para o bom funcionamento da Internet. Outra consequência da não utilização do IPv6 é que um mesmo endereço IPv4 terá que ser compartilhado entre múltiplos usuários finais, fazendo com que uma investigação baseada em IP retorne múltiplos clientes de uma operadora ao invés de somente um como ocorre hoje e dificultando ou até impossibilitando a identificação do responsável.

Para evitar problemas com a rede IPv4 já em funcionamento, a transição foi planejada para que os dispositivos começassem a usar endereçamento IPv6 paulatina-

mente e em um determinado momento, quando os endereços IPv4 acabassem, toda a Internet já estaria utilizando IPv6. Assim o IPv4 poderia ser desativado aos poucos. Entretanto o IPv6 ainda não está em toda a Internet e os endereços IPv4 já estão acabando. Eles estão esgotados no estoque central, IANA (*Internet Assigned Numbers Authority*), e nos estoques regionais da Ásia (APNIC) e Europa (RIPE) (HUSTON, 2014). A previsão de esgotamento para o Brasil é Agosto de 2014 (HUSTON, 2014), junto com o estoque regional da América Latina (LACNIC), do qual o país faz parte.

1.1 Motivação

As duas versões do protocolo IP são incompatíveis entre si e a não execução da transição conforme o planejamento inicial, através da pilha dupla (IETF - RFC 4213, 2005), gerou uma necessidade urgente da comunicação entre redes que estão com somente um dos protocolos e entre redes com a mesma versão do protocolo, mas que necessitam enviar pacotes através de uma rede com protocolo incompatível. Desta demanda sugiram técnicas de transição do IPv4 para o IPv6, como o 6to4 (IETF - RFC 3056, 2001), DS-Lite (IETF - RFC 6333, 2011), 464XLAT (IETF - RFC 6877, 2013), NAT64 (IETF - RFC 6146, 2011), 6rd (IETF - RFC 5969, 2010) e outras. Apesar da grande quantidade de técnicas, ainda não existe um consenso no IETF (*The Internet Engineering Task Force*) sobre qual é a técnica poderia ser adotada como novo padrão, em substituição a pilha dupla, que não foi foi implementada em larga escala antes do esgotamento do IPv4. Isto ocorre pois nenhuma técnica resolve o problema da transição sem adicionar alguma restrição de funcionamento como, por exemplo, a necessidade de realização de NAT (*Network Address Translation*) por parte do provedor de acesso.

No IETF ainda existe o desenvolvimento de novas técnicas de transição, entre elas o MAP-E (IETF - draft-ietf-softwire-map-10, 2014) e MAP-T (IETF - draft-ietf-softwire-map-t-05, 2014). Elas seguem a mesma ideia básica do DS-Lite e 464XLAT, considerando um cenário futuro onde os núcleos das redes das operadoras serão somente IPv6, mas usarão alguma técnica de compartilhamento de endereços IPv4 para os casos onde este ainda for necessário, estas técnicas serão doravante denominadas pilha dupla restrita. Uma rede que utilize NAT444 (IETF - draft-shirasaki-nat444-06, 2012) e IPv6 também pode ser considerada uma rede com pilha dupla restrita, apesar do núcleo da rede não ser somente IPv6, pois o IPv4 recebido pelo usuário final também é compartilhado entre múltiplos usuários.

Conforme apresentado em Moreiras et al. (2012), existem ao menos 15 técnicas de transição. A técnica de transição recomendada como padrão pelo IETF, a pilha dupla, não é capaz de resolver o problema de comunicação através de redes com diferentes versões de IP e também não oferece uma solução para redes que não possuem endereços IPv4 suficientes para todos os dispositivos. As técnicas que tratam da comunicação entre IPv4 e IPv6 ou formas de compartilhamento de endereços IPv4 ainda estão em desenvolvimento ou em fase de amadurecimento, não existindo, portanto, uma solução definitiva para este cenário onde os endereços IPv4 estão esgotados.

Outro ponto que dificulta a definição da nova técnica padrão é a maneira como o IETF define padrões, que é pelo de consenso dos pesquisadores e desenvolvedores. O grande número de técnicas dificulta o consenso, pois as técnicas foram criadas por grupos de pesquisadores diferentes e cada grupo de desenvolvimento defende seu trabalho como o padrão a ser adotado. As particularidades de cada uma das técnicas também dificultam aos fabricantes de equipamentos ofereçam suporte a todas elas, o que permitiria a criação do padrão baseado no uso e na experiência prática das operadoras.

As dificuldades acima são agravadas pela falta de estudos comparativos e de desempenho que incluam as técnicas mais novas e que utilizam pilha dupla restrita. Os mais atuais trabalhos somente comparam a pilha dupla com técnicas de transição mais antigas como o 6to4 (WU; ZHOU, 2011) ou fazem comparação de desempenho entre IPv4 e IPv6 (NARAYAN; SHANG; FAN, 2009). Esta falta de comparativos com as técnicas mais recentes complica a escolha e dificulta que as técnicas mais eficientes ou adequadas sejam priorizadas e definidas como padrão pelo IETF.

1.2 Objetivo

Este trabalho tem o objetivo de fazer uma comparação de desempenho, de funcionamento e de viabilidade técnica e econômica entre as técnicas de transição do IPv4 para o IPv6 que permitem aos dispositivos trabalhar em pilha dupla restrita, seja usando um endereço IPv4 privado, seja utilizando um endereço IPv4 público através da restrição às portas utilizáveis.

As técnicas de transição comparadas nesta dissertação são recentes, fazem uso de pilha dupla restrita e não foram encontradas comparações entre elas. As técnicas

são o 464XLAT, o DS-Lite, o MAP-E, o MAP-T e o NAT444 já citados.

1.3 Contribuições

Os mais atuais comparativos não incluem as técnicas de transição com pilha dupla restrita (464XLAT, DS-Lite, MAP-E, MAP-T e NAT444) e somente comparam o desempenho da pilha dupla com técnicas de transição mais antigas como o 6to4, ISATAP, 6PE, 6over4 e 6bone (SASANUS; KAEMARUNGSI, 2012), (NARAYAN; TAUCH, 2010), (YUNOS; NOOR; AHMAD, 2010) e (WU; ZHOU, 2011) ou fazem comparação de desempenho entre IPv4 e IPv6 (NARAYAN; SHANG; FAN, 2009).

A única análise técnica disponível para uma destas técnicas mais recentes, o MAP-T, é um trabalho que foi desenvolvido pelo autor desta dissertação (IETF - draft-cordeiro-experience-mapt-00, 2014). Ela é feita com foco na experiência do usuário, testando se a experiência é positiva ou não na utilização de diversas aplicações de uso comum por usuários da Internet.

Este trabalho contribui pela comparação de desempenho, de funcionamento e de viabilidade técnica e econômica que é realizada entre estas técnicas, permitindo que este trabalho possa ser utilizado nas discussões de padronização do IETF.

1.4 Método de trabalho

Este trabalho de comparação das técnicas de transição que utilizam pilha dupla restrita é constituído dos seguintes elementos.

- Análise bibliográfica:

  Análise bibliográfica incluindo a análise das funcionalidades, particularidades e limitações das técnicas comparadas neste trabalho.

- Definição dos critérios de comparação:

  Definição dos critérios técnicos que são utilizados para a comparação entre as técnicas. São utilizadas três aspectos de comparação, o primeiro, qualitativo, é baseado na experiência do usuário, com teste de funcionamento dos principais programas que utilizam a Internet, este teste tem o objetivo de verificar se a utilização da técnica gera impacto nos usuários que estão obtendo acesso através desta, pois a técnica de transição não deve interferir nesta experiência.

O segundo critério, quantitativo, considera a medição do uso de memória e de processamento nos equipamentos executando as técnicas de transição e também no uso de banda adicional no meio físico.

O terceiro critério, viabilidade, considera aspectos técnicos e econômicos que podem impactar na escolha, na implantação, na manutenção e em outros pontos, de cada uma das técnicas comparadas.

- Definição dos testes:

  Uma vez definidos os critérios de comparação são definidos os programas a serem testados e parâmetros como velocidade de transmissão no meio físico que possibilitam a obtenção de dados de funcionamento dos programas e de uso de recursos para que as comparações sejam realizadas.

- Definição da topologia de rede:

  Com a definição dos testes é definida a topologia ou as topologias de redes necessárias para a realização dos testes. Esta topologia deve conter no mínimo:

  - um roteador de borda - interface entre a rede de testes e a Internet;
  - um CPE (*Customer Premises Equipment*) - equipamento que implementa a técnica de transição e fica instalado no cliente final;
  - um dispositivo de acesso à Internet - computador ou outro equipamento de acesso à Internet que é utilizado pelo cliente final e
  - um roteador para representar o núcleo da rede da operadora e que faz a ligação entre o roteador de borda e o CPE.

- Implantação da rede de testes:

  Montagem e configuração da topologia física e lógica da rede de testes, bem como a instalação e configuração dos programas que implementam as técnicas de transição. Instalação e configuração dos programas que são testados e o *software* necessário para a coleta dos dados usados na comparação, por exemplo, pacotes trafegados, velocidade de transmissão, utilização de memória etc.

- Execução dos testes:

  Execução dos testes previamente definidos para verificar o funcionamento dos programas escolhidos e o uso dos recursos computacionais e de rede.

Nesta etapa também é executada a análise inicial dos dados para verificar se houveram falhas na coleta dos mesmos e se os testes propostos foram capazes de coletar informações relevantes para a análise comparativa fazendo novos testes ou ajustes necessários.

- Análise Comparativa dos Resultados:

  A tabulação de dados e criação gráficos é feita para permitir a comparação das técnicas. Análise comparativa dos desempenhos obtidos por cada uma das técnicas, salientando as vantagens e desvantagens delas nos critérios de desempenho definidos.

- Comparação dos resultados obtidos com trabalhos previamente publicados:

  Comparação dos resultados obtidos com previsões teóricas de trabalhos anteriores e com outras análises que possam ter sido feitas até a obtenção destes resultados. Esta comparação auxilia no objetivo de definir quais os cenários existentes em redes de provedores de acesso à Internet cada uma das técnicas é recomendada.

1.5 Organização do trabalho

Além da seção 1 esta dissertação possuí mais 6 seções e 1 anexo.

Na seção 2, Estado da Arte, são apresentados trabalhos relacionados, incluindo explicações sobre o funcionamento das técnicas de transição do IPv4 para o IPv6 e a taxonomia destas técnicas. As técnicas comparadas neste trabalho, que usam pilha dupla restrita, são explicadas detalhadamente. Esta seção também inclui informações de trabalhos que fazem comparação de desempenho entre técnicas de transição mais antigas.

A seção 3, Critérios de Comparação, detalha os critérios utilizados para fazer a comparação entre as técnicas de transição. Estes critérios são o funcionamento ou não dos programas mais comuns que necessitam acesso à Internet, a utilização de memória e processamento nos elementos da rede que implementam a técnica de transição e a ocupação adicional de banda que a utilização da técnica causa. Nesta seção também são definidos os testes necessários para que os parâmetros de comparação possam ser mensurados e as topologias de rede utilizadas nos testes.

Na seção 4, Resultados Experimentais, encontram-se os resultados dos experimentos realizados com uma análise qualitativa dos resultados. Esta análise verifica se os testes realizados produziram dados suficientes para as comparações propostas.

A seguir, na seção 5, Comparação Quantitativa, são realizadas as comparações com base nos critérios definidos na seção 3. Eventuais comparações complementares produzidas como efeito secundário dos testes também são feitas. Os resultados também são comparados com outros trabalhos relacionados.

Após a análise qualitativa e quantitativa, estas são revisitadas e com a adição de novos aspectos e estimativas é apresentada na seção 6, Análise de Viabilidade, uma análise técnica e econômica para a viabilidade da utilização das técnicas em redes de provedores de serviço de Internet.

Finalizando a dissertação, a seção 7, Conclusões, apresenta as conclusões do trabalho. Estas conclusões incluem as vantagens e desvantagens de cada técnica e apresenta cenários onde cada uma delas seria melhor aproveitada.

O anexo 1 inclui detalhamento das redes utilizadas nos testes com as configurações dos equipamentos e programas utilizados.

1.6 Recursos Necessários

Aqui são apresentados os recursos, equipamentos e programas, utilizados na realização dos testes necessários para a comparação entras as técnicas de transição analisadas neste trabalho e que são necessários para uma repetição dos testes de medição.

A tabela 1.1 apresenta a lista de equipamentos utilizados nos testes.

Tabela 1.1: Recursos necessários para a realização do trabalho

Função	Recurso	Quantidade Necessária
Computador na Internet	Computador com Linux	1
Roteador de borda	Computador com Linux	1
Roteador somente IPv6	Roteador TP-Link TL-WR1043ND	1
Roteador CPE	Roteador TP-Link TL-WR1043ND	4
Dispositivo de acesso à Internet	Computador com Linux	1
Dispositivo de acesso à Internet	Computador com Windows 7	1
Dispositivo de acesso à Internet	Computador com MAC Os	1
Dispositivo de acesso à Internet	Celular com Android	1
Dispositivo de acesso à Internet	*Tablet* com IOS	1
Programa para medição de tráfego	Programa iperf (*software* livre)	1
Programa para o DS-Lite	Programa referência desenvolvido pela Internet Systems Consortium	1
Programa para o 464XLAT	Programa TAYGA (*software* livre)	1
Programa para o MAP-T	Programa referência desenvolvido pela CERNET	1
Programa para o MAP-E	Programa referência desenvolvido pela CERNET	1

Fonte: Elaborado pelo autor

2 ESTADO DA ARTE

A necessidade utilização do IPv6 é inadiável e conforme Byrne (2012), responsável pela implantação de IPv6 na rede de uma grande operadora estadunidense de celular, a T-Mobile, as redes das operadoras caminham para que o núcleo seja somente IPv6 para economizar os escassos endereços IPv4 e para facilitar a manutenção da rede, pois só um protocolo estaria em execução no núcleo da rede. Esta visão também é compartilhada por diversos membros do IETF que participam do grupo *Softwire* (IETF - RFC 4925, 2007), conforme pode ser notado nas listas de discussão do grupo (IETF - Lista de email, 2012). Outro ponto de consenso no grupo é que o compartilhamento de endereços por usuários distintos, usando IPv4 restrito, será necessário pois o IPv6 ainda não está sendo usado em larga escala.

Nesta seção são apresentadas as técnicas de transição do IPv4 para o IPv6 que são comparadas na parte prática do trabalho e as técnicas que serviram de base para o surgimento das mesmas. Também são analisados trabalhos que realizam comparativos de desempenho entre as versões 4 e 6 do protocolo internet e entre técnicas de transição.

2.1 Técnicas de Transição de IPv4 para IPv6

O IPv6 não foi criado para ser compatível com o IPv4. Conforme planejado pelo IETF na RFC 2893 (IETF - RFC 2893, 2000) a transição do IPv4 para o IPv6 seria feita da forma gradativa, colocando-os em funcionamento simultâneo, usando pilha dupla. Isto permitiria que o IPv6 fosse implantado enquanto os endereços IPv4 não se esgotassem e que no momento do esgotamento toda a Internet estaria com IPv6, permitindo a gradual desativação do IPv4.

Entretanto a transição não ocorreu conforme o planejamento inicial e, em 2007, notou-se que uma nova linha de pesquisa para técnicas de transição seria necessária. Para isto o IETF criou um novo grupo de pesquisa, o *Softwire* (IETF - RFC 4925,

2007). Este grupo passou a desenvolver técnicas para permitir tráfego IPv4 através de redes que utilizassem exclusivamente endereçamento IPv6 ou tráfego IPv6 através de redes que usassem exclusivamente endereçamento IPv4.

As técnicas analisadas neste trabalho foram propostas pelo grupo *Softwire*, entretanto esta pesquisa não analisa todas as técnicas propostas por esse grupo. Este trabalho se limita as técnicas de pilha dupla restrita (464XLAT, DS-Lite, MAP-E, MAP-T e NAT444).

2.1.1 Taxonomia das Técnicas de Transição de IPv4 para IPv6

Com o intuito de facilitar o entendimento das relações entre as técnicas de transição, foi elaborada a taxonomia da figura 2.1. As classificações e divisões das técnicas são os retângulos brancos. As técnicas são representadas na figura por retângulos cinza claro com arestas contínuas. Os retângulos cinza escuro com arestas tracejadas são agrupamentos de técnicas distintas mas que possuem uma característica, definida por este retângulo, em comum.

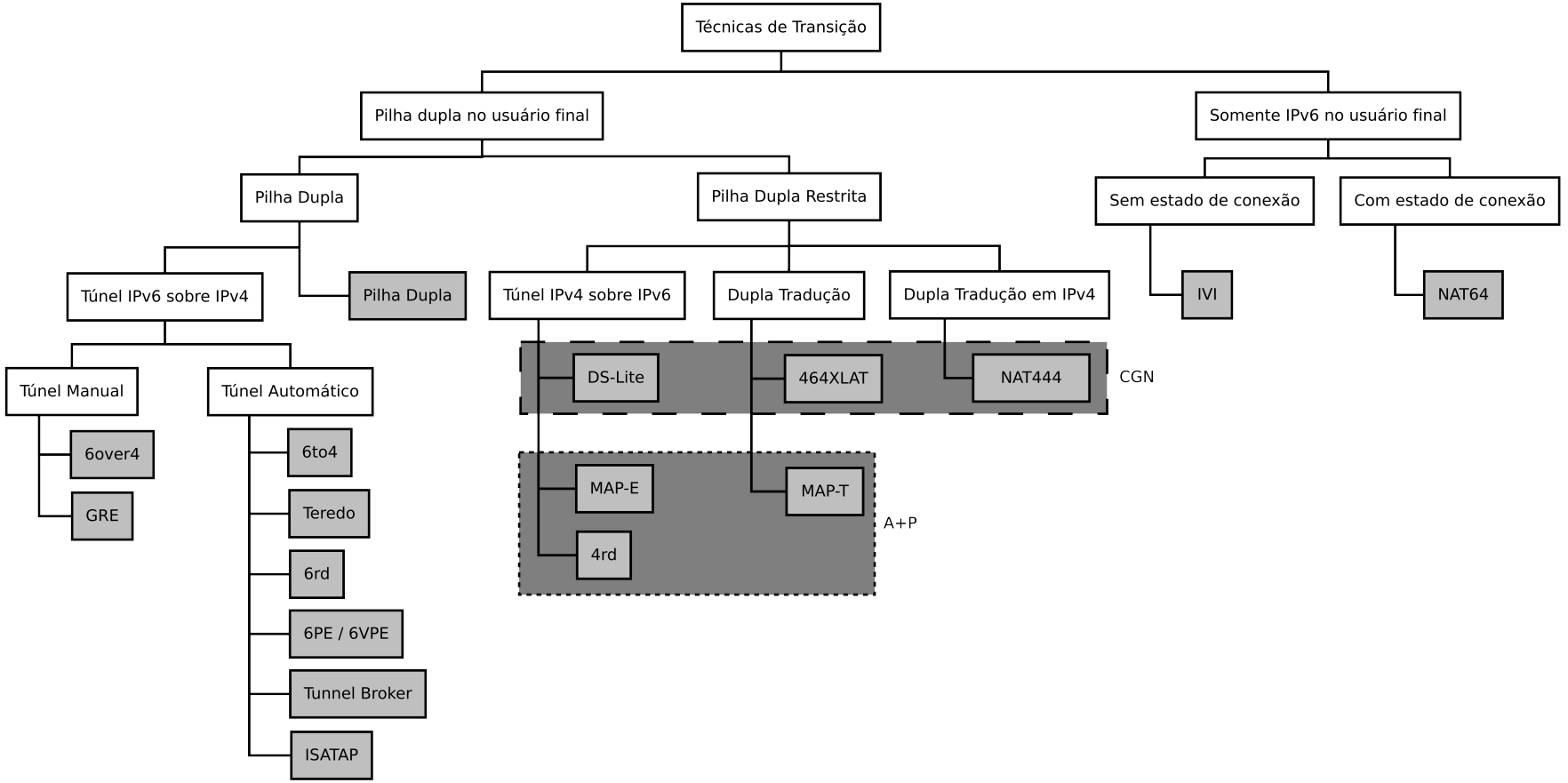
2.1.2 Detalhamento das Técnicas Comparadas neste Trabalho

As técnicas comparadas neste trabalho consideram um cenário onde prefixo IPv6 globalmente roteável é atribuído ao usuário junto com um IPv4 restrito, que pode ser privado (IETF - RFC 1918, 1996), ou público com limitação de portas que podem ser utilizadas (MAENNEL et al., 2008) ou compartilhado (IETF - RFC 6598, 2012). Estes três tipos de endereços IPv4 serão doravante denominados IPv4 restrito, e a pilha dupla formada por um endereço IPv6 globalmente roteável e um endereço IPv4 restrito será denominada pilha dupla restrita.

A operação da pilha dupla restrita considera que se for possível estabelecer a conexão em IPv6, está será feita sem nenhum mecanismo adicional e a conexão é feita sem restrições. Caso a origem ou destino não tenham suporte a IPv6 a conexão é estabelecida utilizando o IPv4 restrito, usando o mecanismo apropriado para transformar o IPv4 restrito em IPv4 público.

O pacote IPv4, gerado no cliente, pode ser transportado pela rede que só tem endereços IPv6 da operadora de dois modos. No primeiro, ele é encapsulado em um pacote IPv6, e desencapsulado para sair para a Internet IPv4 (IETF - RFC 3056, 2001). O segundo modo utiliza tradução, onde o pacote é traduzido do IPv4 para o

Figura 2.1: Taxonomia das técnicas de transição do IPv4 para o IPv6



Fonte: Elaborado pelo autor

IPv6 para ser roteado dentro da operadora e depois é traduzido do IPv6 para o IPv4 para ser encaminhado para a Internet IPv4 (IETF - RFC 6145, 2011), no caso do NAT444 as duas traduções são de IPv4 para IPv4, a primeira de IPv4 privado (IETF - RFC 1918, 1996) para IPv4 compartilhado (IETF - RFC 6598, 2012) para trafegar na rede da operadora e a segunda de IPv4 compartilhado para IPv4 público para o pacote ser encaminhado para a Internet.

O IPv4 restrito a ser atribuído ao cliente pode ser de dois tipos. O primeiro tipo faz o compartilhamento de IPv4 usando equipamento na operadora para fazer a tradução de IPv4 privado ou compartilhado do cliente para um IPv4 público, conhecido como CGN (*Carrier Grade NAT*) ou NAT444 (IETF - draft-shirasaki-nat444-06, 2012). O segundo tipo usa endereços IPv4 públicos, mas com restrição às portas utilizáveis e é conhecido como A+P (*Address Plus Port Sharing*) (MAENNEL et al., 2008).

A tabela 2.1 é um resumo comparativo entre os modos de funcionamento do DS-Lite, MAP-E, 464XLAT, MAP-T e NAT444.

Tabela 2.1: Comparativo de funcionamento entre as técnicas de pilha dupla restrita

Técnicas de Transição	Técnicas Utilizadas			
	Tunelamento	Dupla Tradução	CGN	A+P
DS-Lite	X		X	
MAP-E	X			X
464XLAT		X	X	
MAP-T		X		X
NAT444		X	X	

Fonte: Elaborado pelo autor

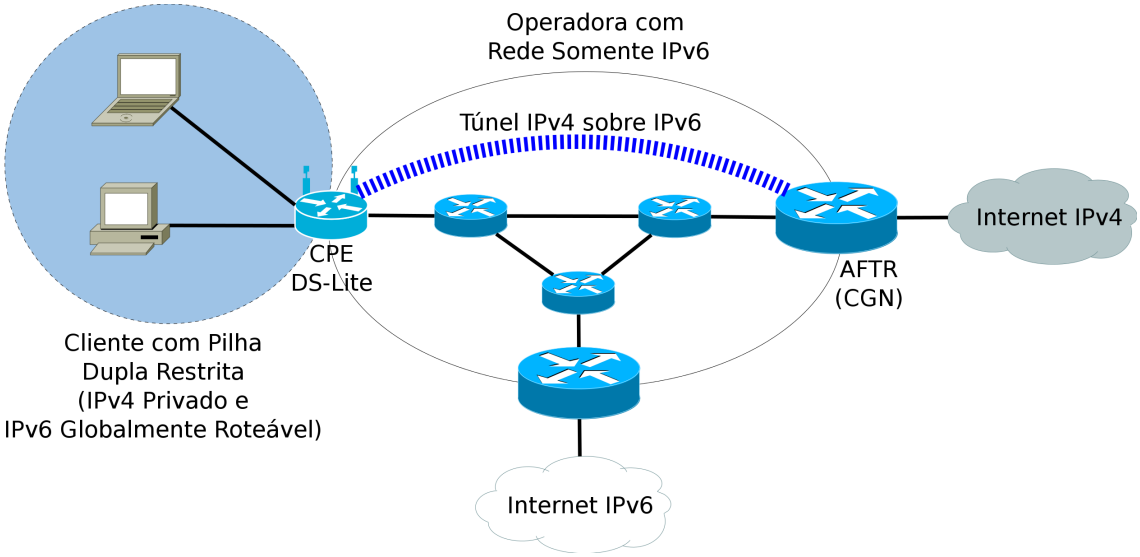
2.1.2.1 Detalhamento DS-Lite

A mais antiga técnica analisada neste trabalho é o DS-Lite (IETF - RFC 6333, 2011). Seu funcionamento considera que o provedor de acesso não possui endereços IPv4 no núcleo da rede, entretanto entrega ao cliente endereços IPv4 privados, conforme especificado na RFC 1918 (IETF - RFC 1918, 1996), e um prefixo IPv6 globalmente roteável. O cliente não deve ser obrigado a fazer NAT deste endereço IPv4 privado, apesar de ser possível este modo de operação, e é responsabilidade da operadora entregar a quantidade de endereços IPv4 privados necessários para a rede do cliente. Se o acesso do cliente for em IPv6 o pacote não necessita de um tratamento especial. Entretanto, caso o pacote do cliente seja IPv4 ele será encapsulado, no CPE,

em um pacote IPv6 para transitar por um túnel na rede da operadora até um roteador de borda da operadora que possua conexão com a Internet IPv4. Neste equipamento o pacote IPv4 é desencapsulado, e passa por um NAT, que guarda o estado da conexão, para receber um IPv4 público e poder seguir pela Internet. A resposta chega ao equipamento de borda que recupera o endereço original da tradução, encapsula o pacote em IPv6 e o envia para o cliente correto através do túnel IPv4 na rede IPv6. Ao retornar ao CPE o pacote IPv4 é desencapsulado e entregue ao dispositivo originador. Este NAT feito na operadora é conhecido como *Carrier Grade NAT* (CGN) ou *Large Scale NAT* (LSN) (IETF - draft-shirasaki-nat444-06, 2012) . A figura 2.2 apresenta a topologia de uma rede utilizando DS-Lite e a figura 2.3 apresenta o diagrama de sequência para uma comunicação IPv4 realizada nesta técnica de transição.

O equipamento na borda da rede da operadora, que faz a terminação do túnel do túnel IPv6, o CGN e encaminha o pacote IPv4 para a Internet é denominado *Address Family Transition Router* (AFTR).

Figura 2.2: Topologia do DS-Lite

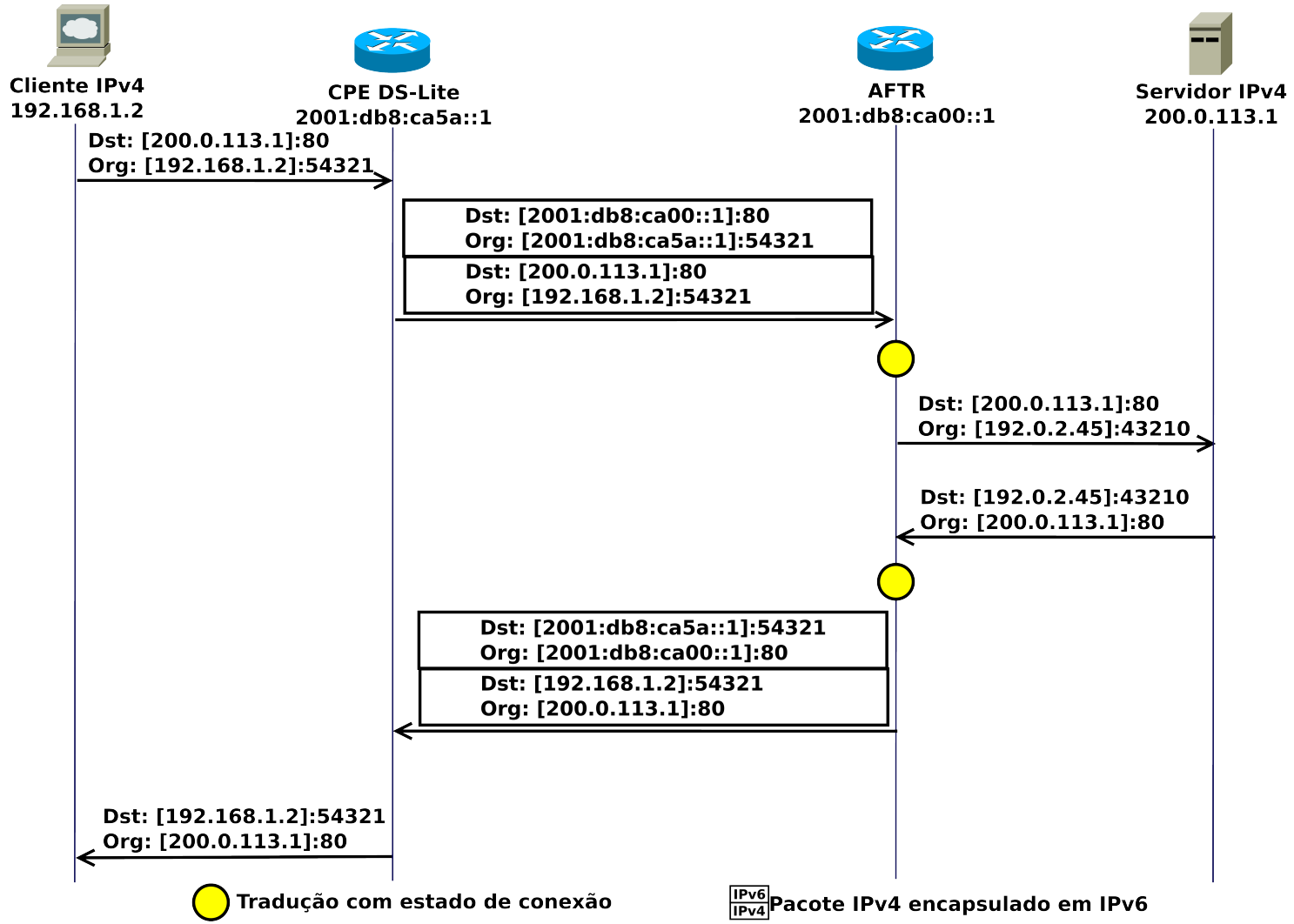


Fonte: Elaborado pelo autor

2.1.2.2 Detalhamento MAP-E

O CGN não é a única maneira de fazer o compartilhamento dos endereços IPv4. Ele pode ser compartilhado com a utilização da porta de origem como uma extensão do endereço, conforme explicado em Maennel et al. (2008). Com isto, mais de um

Figura 2.3: Diagrama de Sequência do DS-Lite



Fonte: Elaborado pelo autor

CPE irá possuir o mesmo IPv4 público, mas cada um estará limitado a usar um conjunto específico das 65536 portas existentes. Por exemplo, o CPE A somente poderá receber e enviar pacotes usando as portas de 10000 a 14999, o dispositivo B utilizaria da porta 15000 até a 19999 e assim por diante. Esta técnica é conhecida como A+P (*Address Plus Port Addressing*) e mantém a inteligência da Internet nas pontas enquanto o CGN leva a inteligência para a rede do provedor de acesso. Neste caso a identificação única de um dispositivo na rede não pode ser feita somente com o endereço IPv4, é necessária a combinação de endereço IPv4 e porta de origem para que o pacote possa ser devolvido a origem.

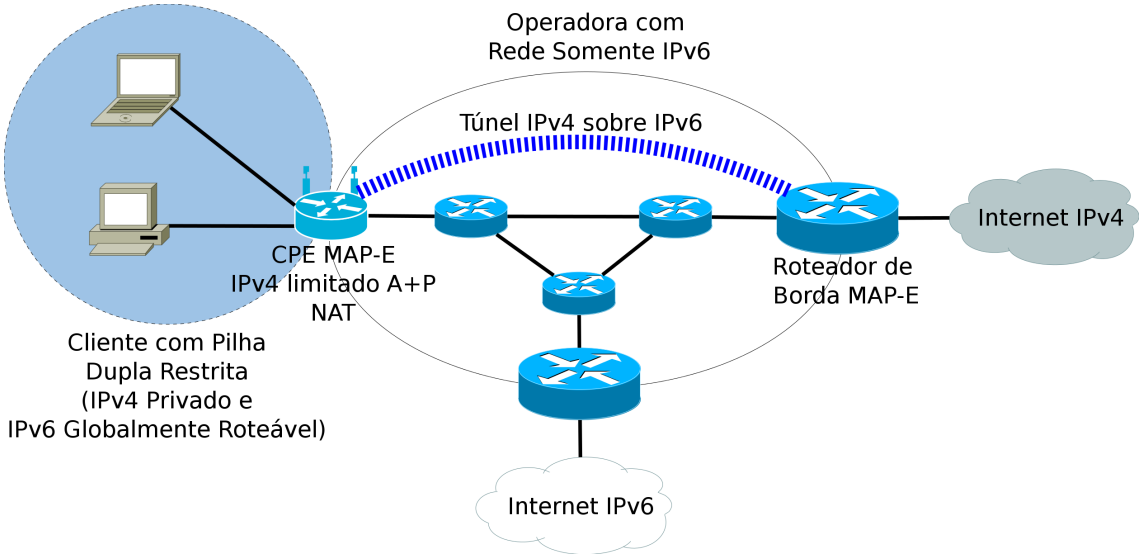
As vantagens do A+P sobre o CGN também são explicadas em Maennel et al. (2008). A principal consiste em não ser necessária a guarda dos estados de conexões no provedor de internet. Isto é possível pois o CPE recebe do provedor as informações de quais as portas que podem ser utilizadas junto com o IPv4 público recebido. De maneira semelhante a que ocorre nas redes atualmente o NAT é realizado no CPE, mas limita-se as portas que podem ser utilizadas nesta tradução com guarda de estado. Após esta tradução, o pacote encaminhado para a rede da operadora possui endereço IPv4 público e porta de origem dentro do conjunto de portas atribuído ao cliente.

O MAP-E (*Mapping of Address and Port with Encapsulation*) (ZHU et al., 2008) e (IETF - draft-ietf-softwire-map-10, 2014) utiliza o A+P na atribuição dos endereços dos dispositivos clientes, dando a estes IPv4 públicos com limitação das portas que podem ser usadas ao invés atribuir endereços IPv4 privados. Apesar do endereço recebido ter um número reduzido de portas, o dispositivo pode estabelecer conexões de entrada e de saída com elas. De maneira similar ao DS-Lite o pacote IPv4 continua sendo transportado no núcleo da rede da operadora, que não possui IPv4, através de tunelamento. A figura 2.4 apresenta a topologia de uma rede utilizando MAP-E e a figura 2.5 apresenta o diagrama de sequência para uma comunicação IPv4 realizada nesta técnica de transição.

2.1.2.3 Detalhamento 464XLAT

O transporte de pacotes IPv4 em uma rede que tem somente endereços IPv6 pode ser feito de outro modo, diferente do tunelamento. Esta alternativa é baseada na tradução de pacotes IPv4 em pacotes IPv6 e vice-versa. O mecanismo de tradução, foi definido pelo IETF na RFC 6145 (IETF - RFC 6145, 2011), consiste em mapear as

Figura 2.4: Topologia do MAP-E

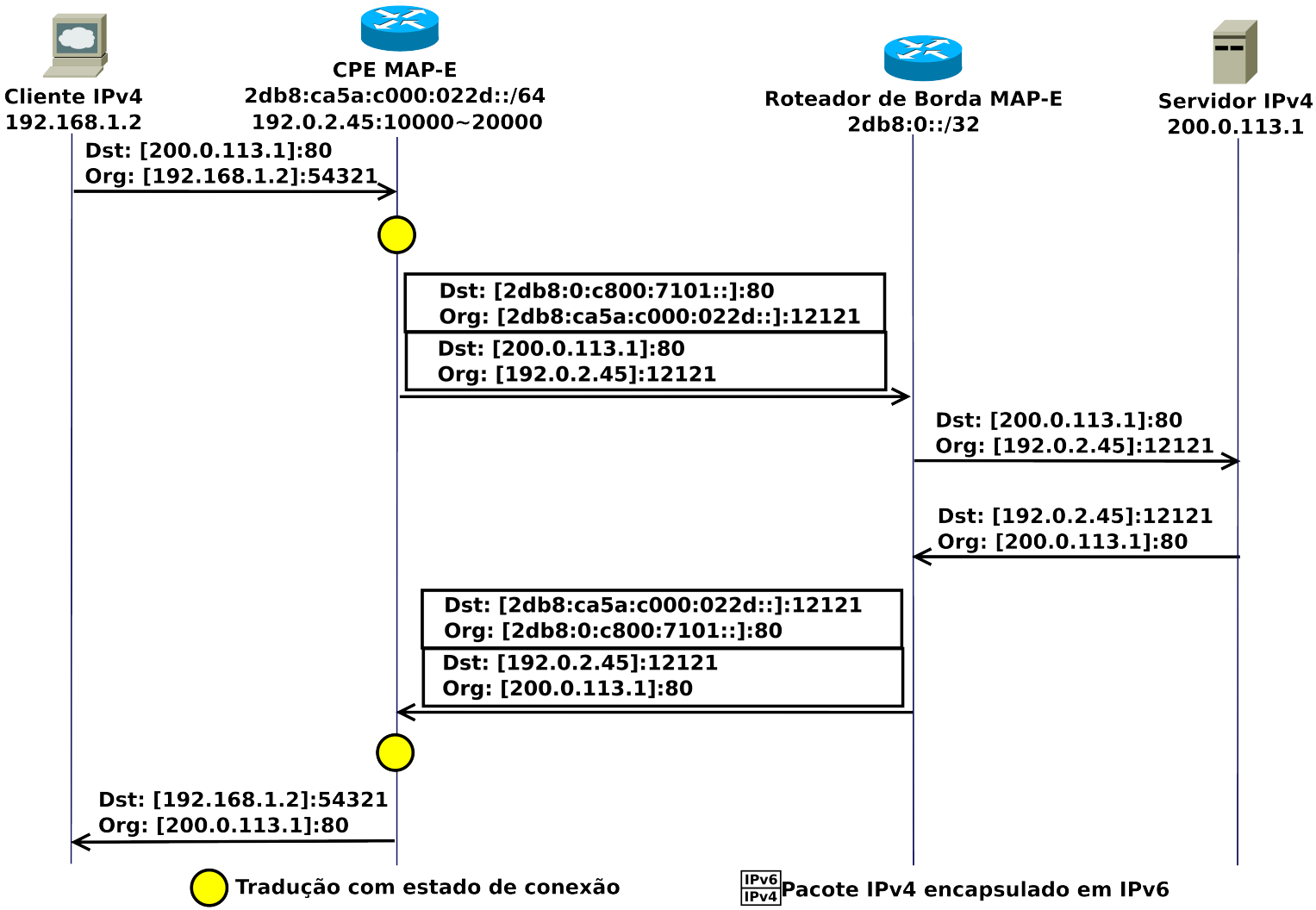


Fonte: Elaborado pelo autor

informações dos campos de um pacote IPv4 para campos de um pacote IPv6, bem como o contrário. Na RFC 6144 (IETF - RFC 6144, 2011) são explicados os possíveis cenários onde a tradução pode ser realizada, entretanto a utilização de somente uma tradução permite que um pacote IPv4 trafegue em uma rede IPv6 ou um pacote IPv6 trafegue em uma rede IPv4, mas não permite uma comunicação fim a fim IPv4 através de uma rede que somente tem endereços IPv6. Para obter esta funcionalidade é preciso traduzir o pacote original de IPv4 para IPv6 e fazer uma nova tradução de IPv6 para IPv4 com o intuito de restaurar o pacote original para encaminha-lo para a Internet IPv4. Como este mecanismo utiliza duas traduções ele é conhecido como dupla tradução.

O 464XLAT (IETF - RFC 6877, 2013) é uma técnica bastante similar aos DS-Lite, mas que possui duas diferenças fundamentais. A primeira delas é a utilização de dupla tradução de IPv4 para IPv6 e novamente de IPv6 para IPv4 ao invés do tunelamento de IPv4 em IPv6. A segunda diferença é que a tradução, com guarda do estadp de conexão, feita no CGN não é de IPv4 privado para IPv4 público, mas sim de IPv6 para IPv4 público. Esta tradução, definida na RFC 6146 (IETF - RFC 6146, 2011), é conhecida como NAT64. Quando o pacote é traduzido de IPv6 para IPv4, o NAT64 utiliza o endereço IPv6 globalmente roteável ao invés de recuperar o endereço IPv4 privado para depois traduzi-lo para IPv4 público, evitando com isto uma terceira tradução no processo. A figura 2.6 apresenta a topologia de uma rede utilizando 464XLAT e a fi-

Figura 2.5: Diagrama de Sequência do MAP-E

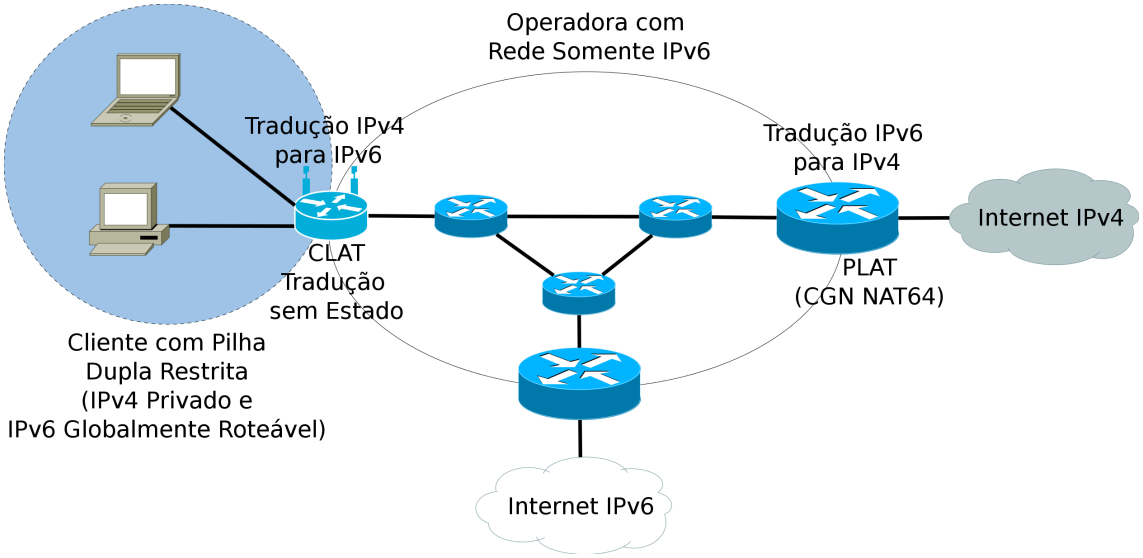


Fonte: Elaborado pelo autor

gura 2.7 apresenta o diagrama de sequência para uma comunicação IPv4 realizada nesta técnica de transição.

O equipamento na borda da rede da operadora, que faz a tradução com guarda de estado de conexão de IPv6 para IPv4 público (CGN NAT64) e encaminha o pacote IPv4 para a Internet é denominado *Provider-side Translator* (PLAT). O CPE na rede do cliente, que faz a tradução sem guarda de estado de conexão de IPv4 privado para IPv6 e encaminha o pacote IPv6 para a rede da operadora é denominado *Customer-side Translator* (CLAT).

Figura 2.6: Topologia do 464XLAT

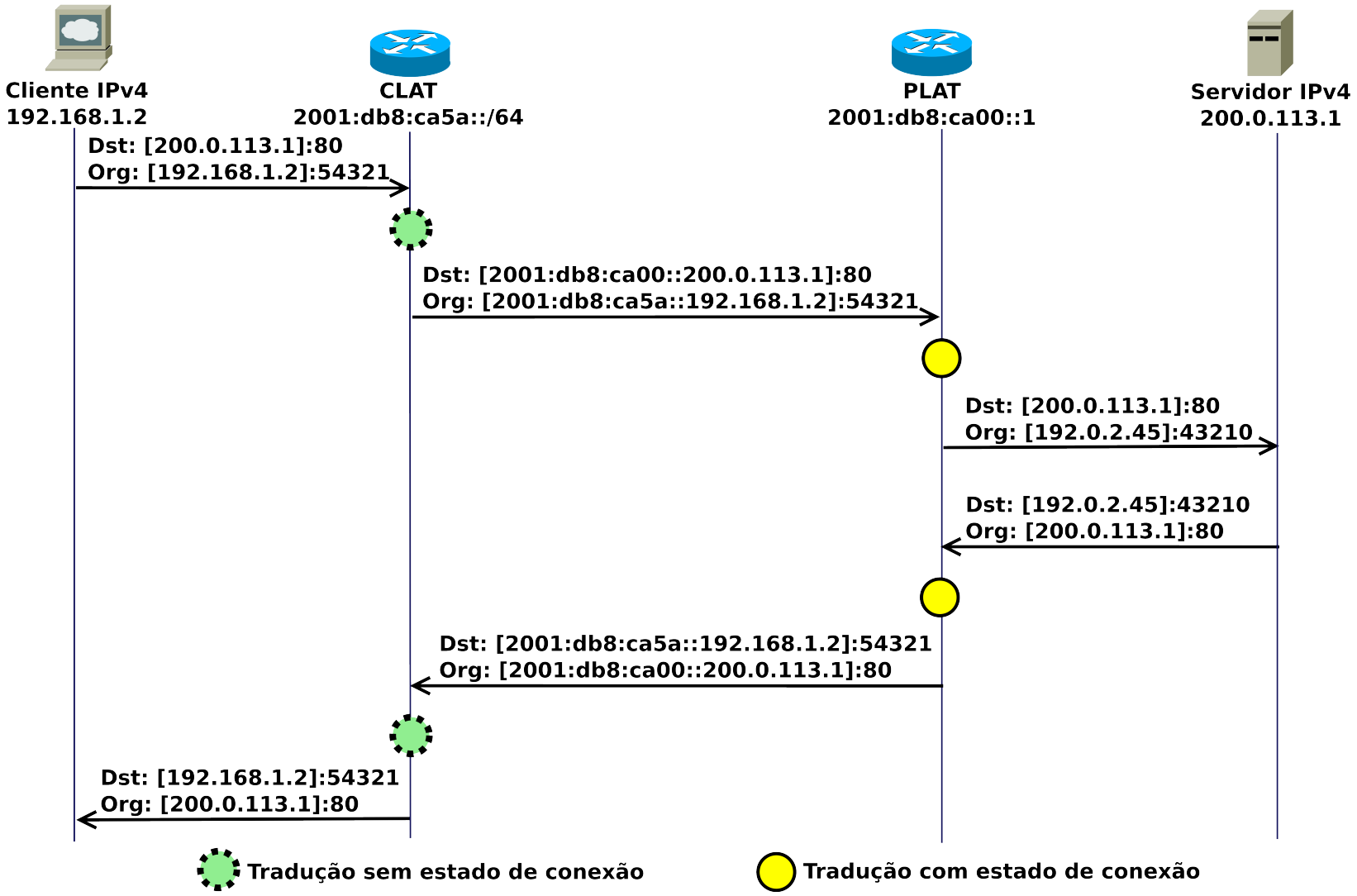


Fonte: Elaborado pelo autor

2.1.2.4 Detalhamento MAP-T

Outra técnica que utiliza a dupla tradução é o MAP-T (IETF - draft-ietf-softwire-map-t-05, 2014), que é uma variação do MAP-E. O MAP-T utiliza o A+P como o MAP-E, mas substituí o tunelamento de IPv4 em IPv6 pela dupla tradução de IPv4 para IPv6 para IPv4. Como ele utiliza A+P, a segunda tradução, de IPv6 para IPv4, recupera os endereços IPv4 públicos mas com portas restritas que originaram as conexões. O MAP-T não guarda estado das conexões na operadora, sendo esta a sua diferença para o 464XLAT. A figura 2.8 apresenta a topologia de uma rede utilizando MAP-T e a figura 2.9 apresenta o diagrama de sequência para uma comunicação IPv4 realizada nesta técnica de transição.

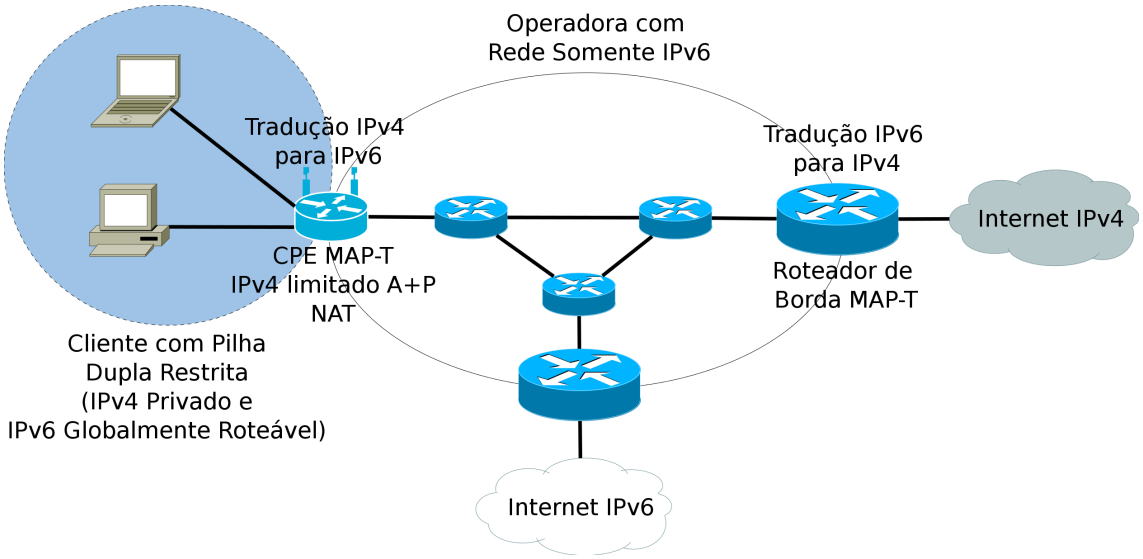
Figura 2.7: Diagrama de Sequência do 464XLAT



Fonte: Elaborado pelo autor

Para manter a informação dos endereços IPv4 de origem e destino quando o pacote IPv4 é traduzido para um pacote IPv6, os 32 bits do endereço IPv4 de origem são colocados como parte endereço IPv6 de origem e o endereço IPv4 de destino é colocado dentro do endereço IPv6 de destino. Este mecanismos permite que os endereços sejam recuperados no roteador de borda do MAP-T sem a necessidade de guardar o estado da conexão.

Figura 2.8: Topologia do MAP-T



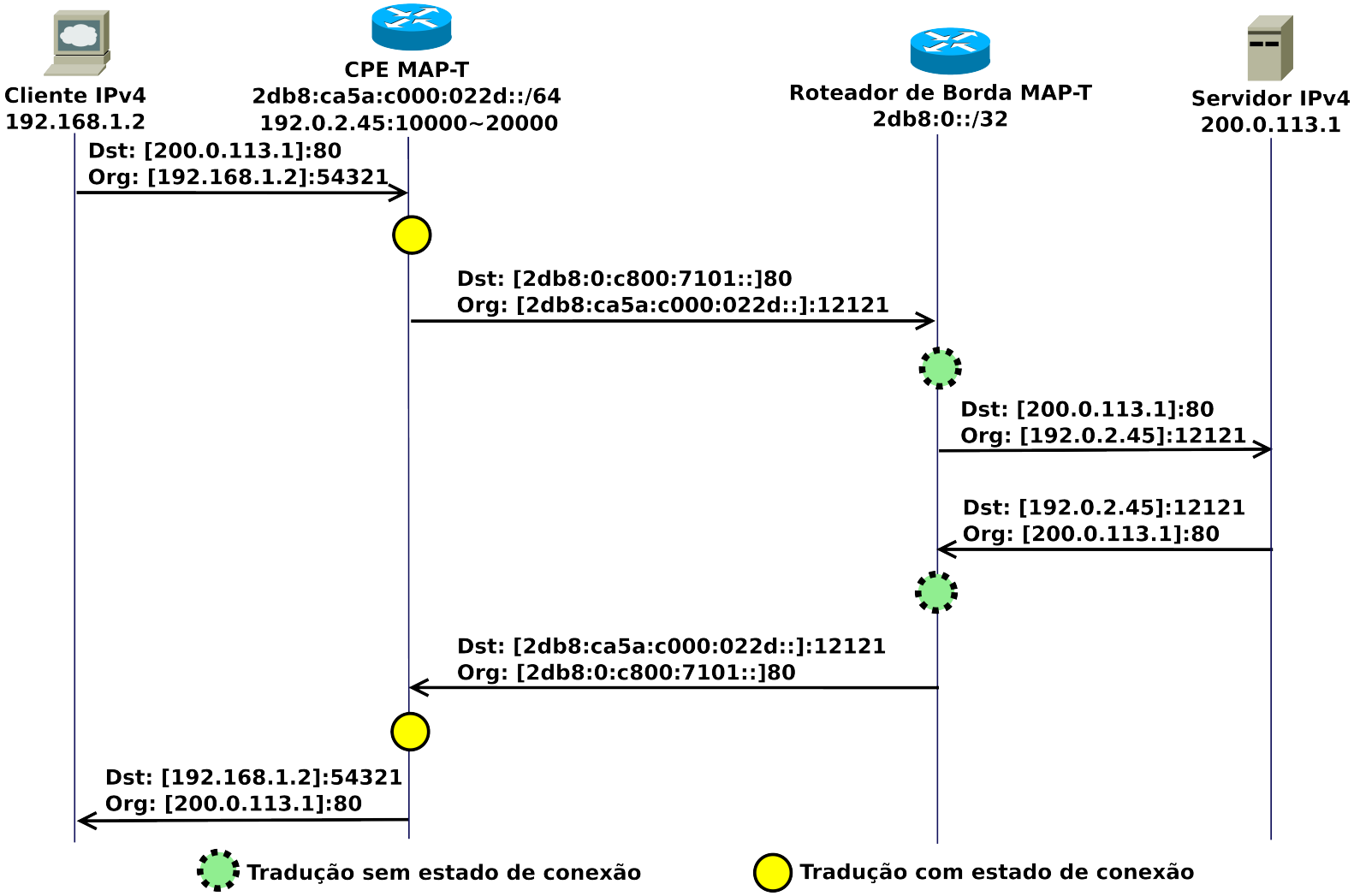
Fonte: Elaborado pelo autor

2.1.2.5 Detalhamento NAT444

O NAT444 (IETF - draft-shirasaki-nat444-06, 2012) se combinado com a utilização de endereços IPv6 globalmente roteáveis pode ser considerado uma técnica de pilha dupla restrita, mesmo que a rede da operadora continue utilizando endereços IPv4. Isto ocorre pois o cliente recebe endereço IPv6 e um endereço IPv4 que terá limitações em seu uso. A utilização do NAT444 é, na visão de alguns provedores de serviços de Internet, inevitável no período de transição do IPv4 para o IPv6 como medida paliativa ao esgotamento dos endereços IPv4 e por isso, mesmo mantendo endereços IPv4 na rede da operadora, ele foi escolhido para ser comparado com as outras quatro técnicas explicadas anteriormente.

Esta técnica consiste na atribuição ao CPE do cliente de um novo tipo de endereço IPv4, o endereço compartilhado, estabelecido na RFC 6598 (IETF - RFC 6598, 2012) como sendo os endereços da rede 100.64.0.0/10. Estes endereços são atribuídos ao

Figura 2.9: Diagrama de Sequência do MAP-T

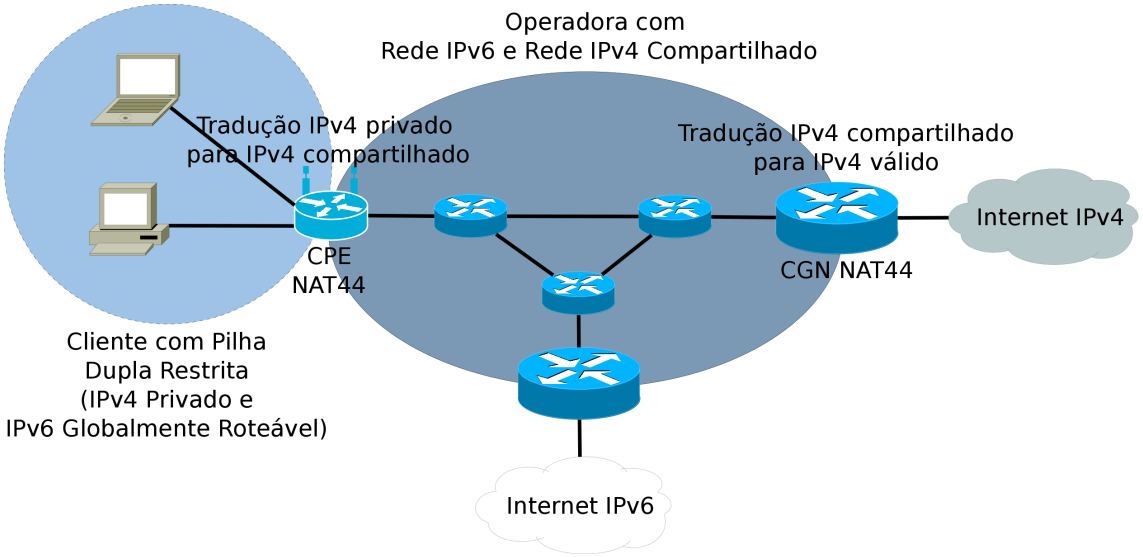


Fonte: Elaborado pelo autor

CPE dos clientes ao invés de endereços IPv4 privados ou endereços IPv4 públicos. Eles foram reservados com o objetivo de evitar que os endereços privados definidos na RFC 1918 fossem utilizados com esta finalidade e, assim, evitar potenciais conflitos na tradução que podem ocorrer se o mesmo bloco de endereços privados fosse utilizado ao mesmo tempo na rede interna do cliente e no núcleo da rede da operadora.

A figura 2.10 apresenta a topologia de rede e a figura 2.11 demonstra o funcionamento de uma comunicação em uma rede com NAT444, que utiliza duas traduções com estado de endereços IPv4. A primeira tradução de endereço IPv4 privado (RFC 1918) para endereço IPv4 compartilhado (RFC 6598) ocorre no CPE do cliente e a segunda tradução, de endereço IPv4 compartilhado para um endereço IPv4 público, ocorre no roteador de borda da operadora. É importante notar que o NAT444 isoladamente não é uma técnica de transição do IPv4 para o IPv6 e que seu uso sem IPv6 não é recomendado.

Figura 2.10: Topologia do NAT444

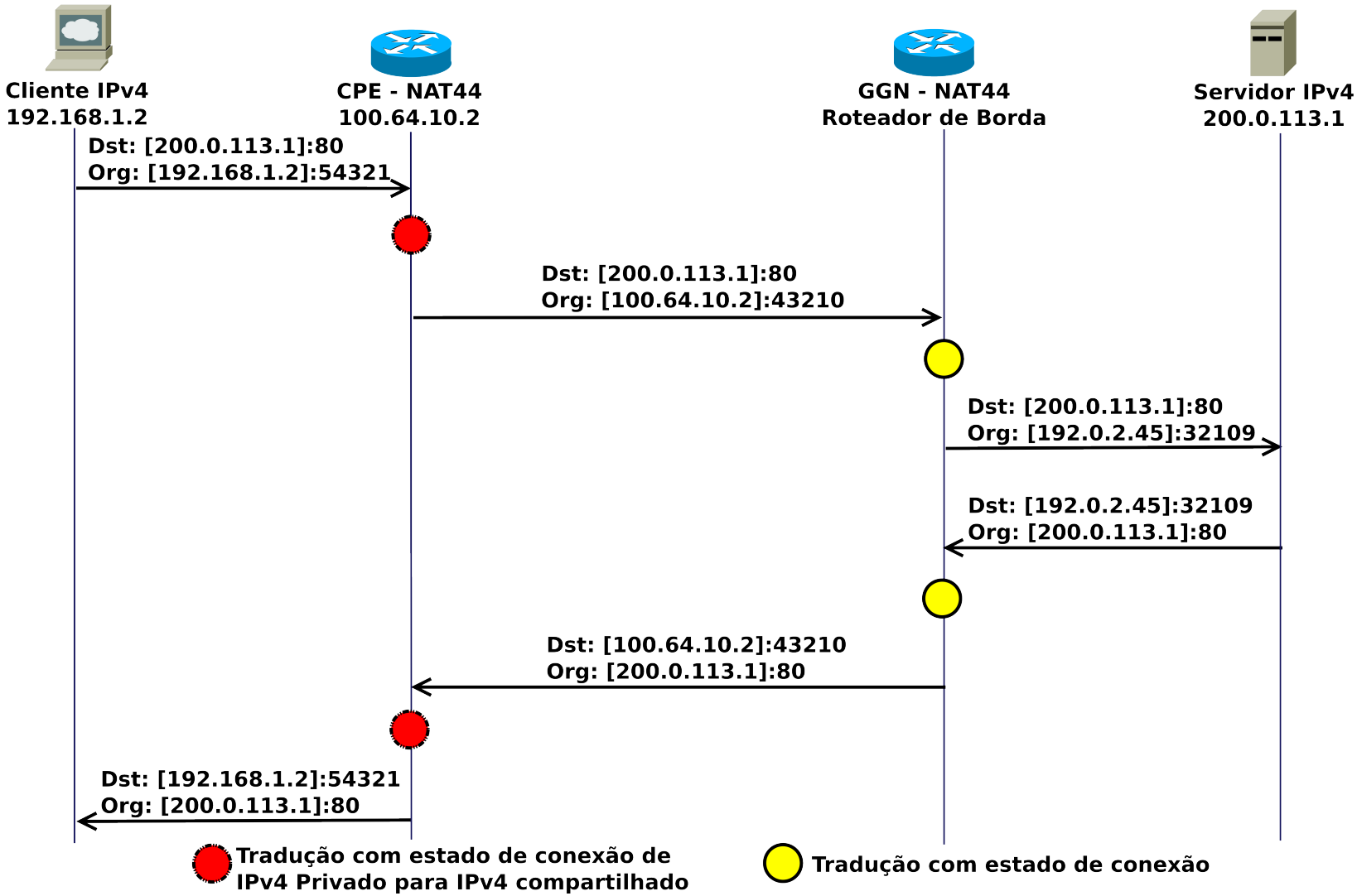


Fonte: Elaborado pelo autor

2.2 Comparações de Técnicas de Transição de IPv4 para IPv6

Os autores Wang, Ye e Li (2005), Narayan, Shang e Fan (2009), Law et al. (2008) e Narayan e Shi (2009) sugerem alguns parâmetros para comparações de desempenho para redes IPv4, redes IPv6 e redes com pilha dupla. Os parâmetros por eles utilizados nas comparações foram a taxa de transferência de dados em TCP e UDP, o atraso

Figura 2.11: Diagrama de Sequência do NAT444



Fonte: Elaborado pelo autor

médio (latência) TCP e UDP, o *jitter* (variação entre os atrasos) TCP e UDP, a variação na carga de processamento, o comportamento em diferentes sistemas operacionais ou *software*, a perda de pacotes e a quantidade de roteadores entre a origem e o destino.

A limitação desses trabalhos é que eles somente comparam redes IPv4, redes IPv6 e redes com pilha dupla e não consideram técnicas de transição, nem mesmo as mais antigos como 6to4 ou túneis manuais, nas medições. Os trabalhos de Sasanus e Kaemarungsi (2012), Narayan e Tauch (2010), Yunos, Noor e Ahmad (2010) e Wu e Zhou (2011) utilizam os parâmetros acima, ou parte deles, para fazer suas comparações, possuindo como vantagem o fato de incluírem algumas técnicas de transição em suas comparações. As técnicas que aparecem em suas comparações são o 6to4 (IETF - RFC 3056, 2001) (túnel automático), ISATAP (IETF - RFC 5214, 2008) (túnel somente entre redes internas), 6PE (IETF - RFC 5214, 2008) (IPv6 através de MPLS IPv4), 6over4 (IETF - RFC 2529, 1999) (túnel manual) e 6bone (rede IPv6 criada para testes). Com exceção ao 6PE que foi planejado para utilização em redes MPLS de provedores de acesso, as demais técnicas analisadas foram desenvolvidas com o objetivo de testes ou para prover acesso IPv6 através de redes IPv4. Estas técnicas não podem ser utilizadas no cenário que pode acontecer em breve, onde a rede do provedor somente terá IPv6. O ISATAP, como determinado em seu próprio nome, *Intra-Site Automatic Tunnel Addressing Protocol*, não foi projetado para acessar a Internet e o 6to4 e 6over4 não foram pensados para escalar para grandes redes, já que tinham o objetivo de conseguir conectividade IPv6 quando as redes ainda não permitiam o tráfego deste protocolo.

Nos testes realizados pelo autor desta dissestação (IETF - draft-cordeiro-experience-mapt-00, 2014) é possível encontrar uma análise de funcionamento de alguns dos programas usados na internet através de uma rede que implementa o MAP-T. Este trabalho foi realizado pelo autor desta dissertação, em parceria com outros funcionários do NIC.br, sendo uma das inspirações para esta dissertação. Apesar de vários programas e protocolos terem sido testados (navegadores, *peer-to-peer*, mensagens instantâneas, *ping*, *traceroute* e outros) e em múltiplos sistemas operacionais (Windows 7, Windows XP e Linux) esse teste teve como base a experiência do usuário, isto é, se esta experiência foi satisfatória ao utilizar os programas ou protocolos. Os testes avaliaram se os protocolos ou programas funcionavam e, caso funcionassem, se era perceptível aos usuários alguma redução de desempenho ou de qualidade. Análises de desempenho como latência, taxa de transferência, entre outros, não foram realiza-

dos e outras técnicas de pilha dupla restrita não foram incluídas na análise.

Os trabalhos de Wu et al. (2013) e Skoberne et al. (2013) se concentraram em uma análise teórica das técnicas de transição, fazendo classificações e comparações teóricas de mecanismos.

O artigo de Wu et al. (2013) é uma pesquisa sobre o estado da arte das técnicas de transição. Seu trabalho inclui, entre outras, as técnicas de pilha dupla restrita em sua pesquisa e cria uma classificação das técnicas similar a que foi proposta na taxonomia proposta neste trabalho. Em sua conclusão o artigo considera que o DS-Lite, MAP-E e MAP-T, além de algumas outras técnicas, são factíveis para implantação em alguns cenários, mas que antes destas técnicas serem aplicadas em grandes redes serão necessárias análises de funcionamento e de desempenho, como as que são realizadas neste trabalho. Wu et al. (2013) não apresenta uma análise experimental para que possa ser feita uma comparação com os resultados aqui obtidos.

O trabalho de Skoberne et al. (2013) propõe uma classificação, em nove classes, dos mecanismos de compartilhamento de endereços IPv4. Esta classificação considera mecanismos que trabalham somente com IPv4, o NAT444, as demais técnicas de pilha dupla restrita e ainda outras técnicas de transição. As nove categorias incluem técnicas de compartilhamento de IPv4 que não são técnicas de transição para o IPv6, gerando assim mais categorias do que as utilizadas na taxonomia proposta neste trabalho. Apesar de não fazer uma análise experimental, é feita também uma análise comparativa dos mecanismos competidores, isto é, quais são as vantagens e desvantagens de usar A+P ou CGN, tunelamento ou dupla tradução e tradução com ou sem guarda de estado. Em sua análise o trabalho declara que a dupla tradução consome menos processamento que o tunelamento, e tal declaração é analisada neste trabalho com os resultados da análise quantitativa.

Nas pesquisas realizadas na *Budapest University of Technology and Economics* (LENCSE; REPAS, 2013), (REPAS; HAJAS; LENCSE, 2014) redes de testes do NAT64 são montadas com o *software* Tayga no Linux e com o *Packet Filter* (PF), que faz parte do OpenBSD. A análise das aplicações feita em Repas, Hajas e Lencse (2014) é similar a apresentada nos resultados experimentais deste trabalho, mas a técnica de transição analisada, o NAT64 não é alvo desta dissertação pois não é uma técnica de pilha dupla restrita. Entretanto as comparações realizadas por Lencse e Repas (2013) são relevantes e comparáveis com os resultados quantitativos obtidos neste trabalho, pois foi utilizado o TAYGA para a implantação do NAT64, mesmo *software* utilizado

neste trabalho na montagem da rede com 464XLAT para implementar o CLAT e o PLAT.

3 CRITÉRIOS DE COMPARAÇÃO

Esta seção apresenta os critérios que são utilizados para fazer a comparação entre as técnicas de transição. Estes critérios são qualitativos e quantitativos com o objetivo de mensurar o impacto técnico e verificar se as técnicas geram algum problema perceptível ao usuário final. É feita também uma análise de viabilidade das técnicas e o impacto destas técnicos nos projetos de transição do IPv4 para o IPv6.

3.1 Critérios para análise qualitativa

As técnicas são comparadas para verificar se geram algum impacto ao usuário de uma operadora que esteja utilizando uma das técnicas de pilha dupla restrita. Esta análise é subjetiva e não leva em conta medições técnicas.

São utilizados dez aplicativos ou serviços que fazem uso da Internet e cada um deles é testado em cada uma das cinco técnicas, para verificar se estes funcionam adequadamente e se, de alguma maneira perceptível, a técnica impacta a experiência de utilização do usuário. A escolha dos programas ou serviços é baseada nas pesquisas do CETIC.br / NIC.br (2012b) sobre o uso da Internet no Brasil e da Pew Internet & American Life Project (2013) sobre os usos mais comuns da Internet nos Estados Unidos. Os programas e serviços escolhidos e as funcionalidades testadas neles são:

- Busca na Internet: buscar no serviço de buscas do Google palavras escolhidas aleatoriamente em um dicionário;
- Acesso a e-mail: acessar o serviço de *webmail* do Google e da Microsoft, ler uma mensagem da caixa de entrada e enviar um e-mail; receber e enviar um e-mail usando os protocolos IMAP e SMTP.
- Rede social: acessar a conta de um usuário cadastrado no Facebook, enviar uma imagem para esta conta e buscar um nome aleatório;

- Vídeo *on line*: acessar o Youtube, assistir o vídeo mais assistido do dia, fazer uma busca com uma palavra aleatória e assistir o quinto vídeo retornado nesta busca;
- Transferência de arquivos usando redes *peer to peer*: transferir a versão mais recente do sistema operacional Linux Ubuntu utilizando o protocolo *bittorrent*;
- Ler notícias: abrir uma notícia de capa de dois sites de notícias;
- Banco via Internet: acessar uma conta corrente e solicitar o extrato de 90 dias;
- Chamada de vídeo: realizar uma chamada de vídeo utilizando o Skype;
- Jogos via Internet: participar de uma partida de um jogo via Internet e
- IPsec / L2TP: configurar uma VPN IPsec / L2TP com uma máquina na Internet e realizar testes de conectividade.

3.2 Critérios para análise quantitativa

Para a análise quantitativa são realizadas transmissões de pacotes através das redes que implementam cada uma das técnicas de transição. O objetivo é verificar se e como as técnicas de transição impactam nesta transmissão.

A transmissão e medição é feita utilizando o programa iperf (DUGAN, 2011), que realiza a medição de desempenho TCP e UDP, com informações de banda, *jitter*, perda de pacotes e outras. Este programa também permite que configurar os parâmetros para envio dos pacotes.

A medição do uso de CPU e uso de memória nos equipamentos de rede é feita com a utilização do sar (*System Activity Reporter*) e análise dos processos em execução através das ferramentas top (*Terminal Process Overview*) e ps (*Process Status*). Os três são programas que estão presentes por padrão no sistrma operacional Linux.

Para todos os testes são medidos os seguintes parâmetros:

- Atividade de processamento: utilização de CPU e de memória nos equipamentos responsáveis por implementar a técnica de transição;
- Banda etefiva: banda efetivamente consumida no núcleo da rede com somente endereçamento IPv6 e

- Parâmetros de qualidade de rede: latência, *jitter*, perda de pacotes e velocidade real obtida na comunicação fim a fim.

Latência é definida como o tempo necessário para que um pacote de parta da origem até ao seu destino e que a resposta retorne a origem. Esta medição pode ser impactada por eventos temporários, assim sendo uma quantidade relevante de pacotes é necessária para que a média entre as medidas possa ser um resultado representativo. *Jitter* é definido como a variação do atraso entre os pacotes sucessivos de dados. Assim como a latência, também pode ser impactado por eventos temporários e necessita de uma quantidade relevante de pacotes para que possa ser considerado um resultado representativo.

3.3 Critérios para análise de viabilidade

A análise de viabilidade considera aspectos técnicos e econômicos. Na análise técnica são consideradas as opções disponíveis para a implantação de cada uma das técnicas, a dificuldade e necessidade de adaptação das redes e o grau de especialização da equipe técnica requerido para o sucesso para da implantação.

A viabilidade econômica considera o custo de equipamentos, sejam eles necessários para a implantação e operação, tais como roteadores e CPEs, ou itens complementares necessários, por exemplo um servidor de armazenamento de dados para guardar os *logs* de conexão necessários para a identificação unívoca de usuários. Também são analisadas eventuais perdas de receita dos provedores geradas por problemas decorrentes do uso destas técnicas.

3.4 Definição dos testes

Os testes da análise qualitativa consistem em fazer a utilização dos programas e protocolos escolhidos, simulando o uso de um usuário comum e verificam se a aplicação ou protocolo sofrem algum problema ou deficiência perceptível ao usuário.

A máquina cliente está conectada ao CPE que executa a técnica de transição. O CPE recebe a pilha dupla restrita mas, para garantir que o teste envolve a tradução ou encapsulamento, a rede entre o CPE e a máquina cliente somente possui endereço IPv4 privado. A máquina cliente é representada pelos seguintes dispositivos: computador com Windows, computador com Linux, computador com MAC OS, celular

com Android e *tablet* com IOS. Caso algum teste não possa ser realizado em alguma plataforma por questões técnicas, isto é evidenciado nos resultados.

Para os testes de análise quantitativa são gerados fluxos em IPv4 de 100 Mbps na máquina cliente e são variados os seguintes parâmetros:

- Protocolo de transmissão de pacotes: TCP e UDP e
- Tamanho do pacote enviado: 100 bytes, 500 bytes, 1000 bytes e 1400 bytes.

A máquina geradora de tráfego é o cliente conectado ao CPE que implementa a técnica e a máquina receptora é um dispositivo externo a rede da técnica de transição, simulando um computador na Internet.

3.5 Topologia de rede

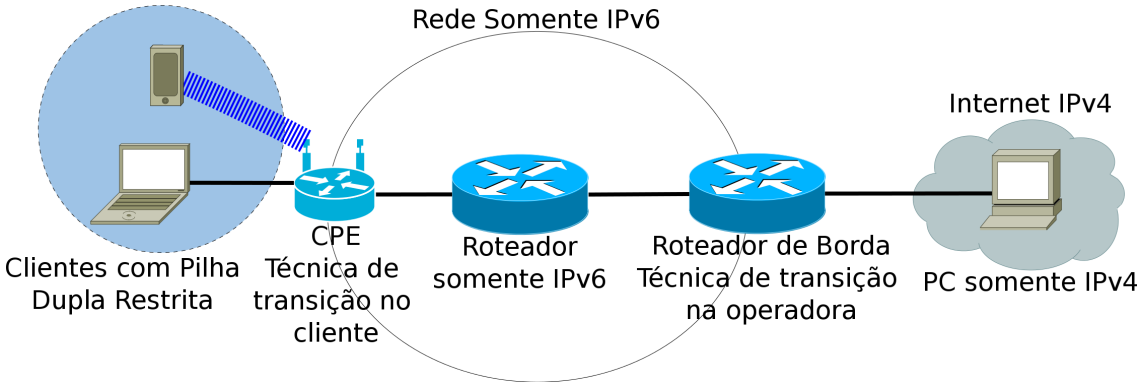
A topologia de rede e equipamentos utilizados são os mesmos para todas as técnicas, para evitar influência da topologia e dos equipamentos nos resultados. O *software* utilizado para implementar as técnicas são código aberto e publicados na Internet.

A figura 3.1 apresenta a topologia usada nos testes. Ela é constituída dos seguintes elementos:

- Clientes com pilha dupla restrita: dispositivos conectados ao CPE que implementa a técnica de transição. Recebem IPv6 globalmente roteável se possuírem suporte IPv6. Recebem IPv4 privado que é traduzido (NAT44) para o IPv4 restrito que a técnica de transição implementa e atribui ao CPE;
- CPE técnica de transição no cliente: CPE que implementa a técnica de transição no lado do cliente. Recebe IPv6 globalmente roteável na interface com a operadora e um prefixo IPv6 para anunciar na rede do cliente. Recebe IPv4 restrito e distribui IPv4 privado para a rede cliente, fazendo NAT deste endereço IPv4 privado para o endereço IPv4 restrito;
- Roteador somente IPv6: roteador que somente possui endereços IPv6, por isto incapaz de rotear pacotes IPv4. Na topologia este único roteador representa toda uma rede sem endereçamento IPv4 de uma operadora;

- Roteador de borda técnica de transição na operadora: roteador de borda que implementa a técnica de transição na operadora, fazendo a ligação entre a rede somente IPv6 da operadora e a Internet IPv4 e
- PC somente IPv4: dispositivo que possui Não possui endereço IPv6, por isto incapaz de transmitir e receber pacotes IPv6. É a máquina alvo para o qual são feitas as medições quantitativas. Nas análises qualitativas é representado pelos servidores originais dos serviços na Internet.

Figura 3.1: Topologia usada para os testes



Fonte: Elaborado pelo autor

Os detalhes das versões dos sistemas operacionais e *hardware* utilizados na função de "Clientes com Pilha Dupla Restrita" são apresentados na tabela 3.1.

Tabela 3.1: Sistemas utilizados para a realização dos testes

Sistema Operacional	Versão do Sistema Operacional	Descrição do *Hardware*
Linux	Ubuntu 12.04	Processador Intel Core2 Quad Q9550 @ 2.83GHz e 4 GB Memória RAM
Windows	Windows 7 Service Pack 1	Intel Core2 Quad Q6600 @ 2.40GHz @ 2.83GHz e 6 GB Memória RAM
MAC OS	MAC OS 10.8.4	Macbook 2009 Intel Core2 Duo P7550 @ 2.26GHz 2 GB Memória RAM
IOS	IOS 6.1.3	IPAD 2 16 GB
Android	Android 4.1.2	Samsung Galaxy S3 16 GB

Fonte: Elaborado pelo autor

4 RESULTADOS EXPERIMENTAIS

Nesta seção são apresentados os resultados dos experimentos realizados com uma análise qualitativa dos resultados. Esta análise identifica se cada um dos programas teve um comportamento igual ou pior do que em uma rede sem a técnica de pilha dupla restrita. Caso o desempenho da técnica tenha sido pior, uma investigação para identificar o motivo é apresentada.

4.1 Resultados da Análise Qualitativa

As técnicas são comparadas para verificar se gerariam algum impacto ao usuário de uma operadora que esteja utilizando uma das técnicas de pilha dupla restrita. Esta análise foi subjetiva e não levou em conta medições técnicas.

A seguir são apresentados os resultados obtidos nos testes de dez aplicativos ou serviços que fazem uso da Internet. Cada um destes foi testado em cada uma das cinco técnicas de pilha dupla restrita que são foco deste trabalho, para verificar se estes funcionam adequadamente e se, de alguma maneira perceptível ao usuário, a técnica impacta a experiência do usuário.

Os resultados são apresentados nas seguintes seções em tabelas utilizando as seguintes palavras para apresentar os resultados:

- Igual: para expressar que a experiência do usuário utilizando a técnica foi igual a experiência em uma rede com IPv4 público
- Pior: para expressar que a experiência do usuário utilizando a técnica foi pior a experiência em uma rede com IPv4 público
- Erro: para expressar que a aplicação não funcionou adequadamente quando testada na rede com a técnica de transição

- Indisponível: para expressar que não é possível realizar o teste neste sistema operacional

4.1.1 Busca na Internet

Foi utilizado o serviço de buscas do Google para procurar por palavras escolhidas aleatoriamente em um dicionário. Os resultados estão disponíveis na tabela 4.1.

Tabela 4.1: Resultado para buscas na Internet

Técnicas de Transição	Sistema Operacional Utilizado				
	Linux	Windows 7	MAC OS	IOS	Android
DS-Lite	Igual	Igual	Igual	Igual	Igual
MAP-E	Igual	Igual	Igual	Igual	Igual
464XLAT	Igual	Igual	Igual	Igual	Igual
MAP-T	Igual	Igual	Igual	Igual	Igual
NAT444	Igual	Igual	Igual	Igual	Igual

Fonte: Elaborado pelo autor

Não foi notada qualquer diferença entre fazer buscas em uma rede que utilize as técnicas de pilha dupla restrita ou uma rede com IPv4 público. Em todas as técnicas o resultado foi obtido sem problemas e sem atrasos perceptíveis.

4.1.2 Acesso a e-mail

Foi utilizado o serviço de *webmail* do Google e da Microsoft para ler uma mensagem da caixa de entrada e enviar um e-mail. Nos sistemas operacionais Linux, Windows e MAC OS foi utilizado o programa Thunderbird para enviar mensagens via SMTP e receber mensagens via IMAP. No IOS e Android foi utilizado o cliente de email padrão de cada plataforma para os testes com SMTP e IMAP. Os resultados estão disponíveis na tabela 4.2.

Os serviços de *webmail* do Google, Gmail, e da Microsoft, Outlook.com, funcionaram sem problemas em todas as redes de teste. Foi possível enviar e receber e-mails em todos os testes sem qualquer problema notável.

Os testes de recebimento e envio de e-mails via IMAP e SMTP também transcorreram sem problemas perceptíveis em todas as técnicas testadas, todas as mensagens

Tabela 4.2: Resultado para acesso a e-mail

Técnicas de Transição	Sistema Operacional Utilizado				
	Linux	Windows 7	MAC OS	IOS	Android
DS-Lite	Igual	Igual	Igual	Igual	Igual
MAP-E	Igual	Igual	Igual	Igual	Igual
464XLAT	Igual	Igual	Igual	Igual	Igual
MAP-T	Igual	Igual	Igual	Igual	Igual
NAT444	Igual	Igual	Igual	Igual	Igual

Fonte: Elaborado pelo autor

foram enviadas e recebidas pelos clientes de e-mail, Thunderbird no Windows, Linux e MAC OS ou pelos clientes nativos do Android e IOS, sem impactos na experiência do usuário.

4.1.3 Rede social

Foi acessada a conta de um usuário cadastrado no Facebook, enviada uma imagem para esta conta e buscado um nome aleatório. Os resultados estão disponíveis na tabela 4.3.

Tabela 4.3: Resultado para acesso a rede social

Técnicas de Transição	Sistema Operacional Utilizado				
	Linux	Windows 7	MAC OS	IOS	Android
DS-Lite	Igual	Igual	Igual	Igual	Igual
MAP-E	Igual	Igual	Igual	Igual	Igual
464XLAT	Igual	Igual	Igual	Igual	Igual
MAP-T	Igual	Igual	Igual	Igual	Igual
NAT444	Igual	Igual	Igual	Igual	Igual

Fonte: Elaborado pelo autor

Não houve qualquer problema perceptível ao usuário no acesso e na realização das atividades comuns de um usuário de redes sociais.

4.1.4 Vídeo *on line*

Foi acessado o Youtube, assistido o vídeo mais visualizado do dia, feita uma busca com uma palavra aleatória e assistido o quinto vídeo retornado nesta busca. Os resultados estão disponíveis na tabela 4.4.

Tabela 4.4: Resultado para acesso a video *on line*

Técnicas de Transição	Sistema Operacional Utilizado				
	Linux	Windows 7	MAC OS	IOS	Android
DS-Lite	Igual	Igual	Igual	Igual	Igual
MAP-E	Igual	Igual	Igual	Igual	Igual
464XLAT	Igual	Igual	Igual	Igual	Igual
MAP-T	Igual	Igual	Igual	Igual	Igual
NAT444	Igual	Igual	Igual	Igual	Igual

Fonte: Elaborado pelo autor

A visualização de filmes no Youtube ocorreu sem problemas em todas as plataformas através de todas as redes de teste. Não houve problemas perceptíveis, não foi notado um aumento no tempo de carregamento e nem uma redução na resolução de exibição dos vídeos assistidos.

4.1.5 Transferência de arquivos usando redes *peer to peer*

Foi transferida a versão 12.04 do sistema operacional Linux Ubuntu utilizando o protocolo *bittorrent*. Os sistemas operacionais para dispositivos portáteis IOS e Android não foram desenvolvidos para esta finalidade devido ao alto consumo de bateria que seria necessário, assim sendo, estes sistemas não foram testados. Os resultados estão disponíveis na tabela 4.5.

Em todos os sistemas e em todas as técnicas o *seeding* do *bittorrent* não funcionou quando o *download* foi concluído já que nenhuma das redes testadas tem suporte para receber conexões entrantes não vinculadas a conexões saintes. *Seeding* é o termo utilizado para o compartilhamento de um arquivo quando o usuário já concluiu o recebimento do mesmo.

Este problema pode ser mitigado nas redes com MAP-E e MAP-T fazendo o encaminhamento dos pacotes recebidos no conjunto de portas válidas do IPv4 público atribuído ao CPE para os equipamentos presentes na LAN. Este encaminhamento

Tabela 4.5: Resultado para baixar arquivos usando redes *peer to peer*

Técnicas de Transição	Sistema Operacional Utilizado				
	Linux	Windows 7	MAC OS	IOS	Android
DS-Lite	Pior	Pior	Pior	Indisponível	Indisponível
MAP-E	Pior	Pior	Pior	Indisponível	Indisponível
464XLAT	Pior	Pior	Pior	Indisponível	Indisponível
MAP-T	Pior	Pior	Pior	Indisponível	Indisponível
NAT444	Pior	Pior	Pior	Indisponível	Indisponível

Fonte: Elaborado pelo autor

pode ser feito através de configuração no CPE, mas é uma solução que depende de intervenção manual do usuário para fazer a configuração do encaminhamento das portas, algo que pode ser complicado já que este precisaria saber quais as portas atribuídas ao CPE. A alternativa para a automatização do encaminhamento de portas é o uso do protocolo *Universal Plug and Play* (UPnP) (UPnP Foum, 2011), mas o suporte a este protocolo não está implementado ainda na versão de referência da CERNET que foi utilizada nas redes de teste.

Nas redes com DS-Lite, 464XLAT e NAT444 a configuração do encaminhamento de portas e o uso do UPnP não são possíveis pois o equipamento que faz a tradução com estado não está sobre o controle do cliente, mas sim do provedor. O protocolo *Port Control Protocol* (PCP) (IETF - RFC 6887, 2013) foi desenvolvido com o intuito de permitir um encaminhamento automático de portas no CGN realizado na operadora para a rede do cliente, mas este protocolo ainda não está amplamente implementado. A sua implementação e utilização não é trivial pois ele depende que a aplicação executando no dispositivo cliente faça a solicitação de porta via PCP, que o CPE do cliente entenda e encaminhe esta solicitação para o CGN da operadora e que o CGN da operadora seja um servidor PCP que possua capacidade de atender a demanda de portas recebidas de todos os clientes cujos pacotes são traduzidos neste equipamento.

Uma segunda tentativa de resolver o problema com o PCP, permitindo o uso de *bittorrent* em todas as técnicas de pilha dupla restrita, é uma simplificação do PCP, denominada *Internet Gateway Device - Port Control Protocol Interworking Function* (IGD-PCP IWF) (IETF - RFC 6970, 2013). O IGD-PCP IWF permite que o mecanismo UPnP, já utilizado por muitas aplicações, seja traduzido pelo CPE em PCP e assim a solicitação das portas necessárias recebidas pelo CPE via UPnP são encaminhadas

via PCP ao CGN. Este mecanismo também não está em uso em larga escala devido a ausência de suporte ao protocolo IGD-PCP IWF em CPEs.

O fato do dispositivo que faz o *download* não conseguir fazer *upload* faz com que alguns rastreadores, dispositivos que armazenam a disponibilidade das partes de um arquivo compartilhado via *bittorrent*, punam o dispositivo que faz *download* sem compartilhar, fazendo com que a velocidade de conexão seja reduzida ou até mesmo que o dispositivo fique proibido de realizar o *download*. Esta limitação de velocidade foi notada em todas as redes de teste, fazendo com que a velocidade fosse, em alguns casos, menor que a metade da velocidade obtida em um rede com IPv4 público no dispositivo cliente. Detalhes complementares do impacto do CGN e do NAT no CPE no protocolo *bittorrent* podem ser obtidos na análise disponível em IETF - draft-boucadair-pcp-bittorrent-00 (2012).

4.1.6 Ler notícias

Foi acessada uma notícia de capa de dois portais, o UOL (www.uol.com.br) e o MSN (www.msn.com). Os resultados estão disponíveis na tabela 4.6.

Tabela 4.6: Resultado para ler notícias

Técnicas de Transição	Sistema Operacional Utilizado				
	Linux	Windows 7	MAC OS	IOS	Android
DS-Lite	Igual	Igual	Igual	Igual	Igual
MAP-E	Igual	Igual	Igual	Igual	Igual
464XLAT	Igual	Igual	Igual	Igual	Igual
MAP-T	Igual	Igual	Igual	Igual	Igual
NAT444	Igual	Igual	Igual	Igual	Igual

Fonte: Elaborado pelo autor

As páginas principais dos portais e subsequente notícias carregaram sem problemas ou atrasos perceptíveis nos testes de todas as técnicas e em todos os sistemas operacionais.

4.1.7 Banco via Internet

Foi acessada uma conta corrente do banco Itaú (www.itau.b.br) e solicitado o extrato de 90 dias. Os resultados estão disponíveis na tabela 4.7.

Tabela 4.7: Resultado para acesso a banco via Internet

Técnicas de Transição	Sistema Operacional Utilizado				
	Linux	Windows 7	MAC OS	IOS	Android
DS-Lite	Igual	Igual	Igual	Igual	Igual
MAP-E	Igual	Igual	Igual	Igual	Igual
464XLAT	Igual	Igual	Igual	Igual	Igual
MAP-T	Igual	Igual	Igual	Igual	Igual
NAT444	Igual	Igual	Igual	Igual	Igual

Fonte: Elaborado pelo autor

Nos testes de todas as técnicas e em todos os sistemas operacionais a operação para obtenção do extrato de 90 dias foi bem sucedida sem qualquer problema ou atraso relevante.

4.1.8 Chamada de vídeo

Foi utilizado o Skype para realizar uma chamada de vídeo entre dois usuários, um na rede com a técnica de transição e o segundo na Internet. Os resultados estão disponíveis na tabela 4.8.

Tabela 4.8: Resultado para chamada de vídeo

Técnicas de Transição	Sistema Operacional Utilizado				
	Linux	Windows 7	MAC OS	IOS	Android
DS-Lite	Pior	Igual	Pior	Pior	Pior
MAP-E	Igual	Igual	Pior	Pior	Pior
464XLAT	Pior	Pior	Pior	Pior	Pior
MAP-T	Pior	Pior	Pior	Pior	Pior
NAT444	Igual	Igual	Pior	Pior	Igual

Fonte: Elaborado pelo autor

Todas as técnicas geraram perdas de qualidade na chamada de vídeo em alguns dos sistemas operacionais. O MAP-T e 464XLAT tiveram o pior comportamento e ocasionaram imagens degradadas em maior ou menor grau em todos os sistemas operacionais. O DS-Lite apresentou perdas em todos os sistemas operacionais, com exceção do Windows. O MAP-E gerou perdas nos dispositivos móveis e no MAC OS. O NAT444 gerou perdas somente nos sistemas operacionais da Apple. Estes resul-

tados indicam que a chamada de vídeo do Skype funciona melhor com o encapsulamento do que com a dupla tradução nas técnicas de pilha dupla restrita. Analisando o fluxo de rede não foi possível identificar um motivo para este comportamento, mas o principal suspeito neste caso é que alguma informação que o Skype analisa ou considera no cabeçalho IPv4 acaba sendo perdida nos processos de tradução entre IPv4 e IPv6.

A perda de qualidade pode ser notada nas imagens da vídeo chamada nos dois lados da comunicação, pois as imagens ficaram mais pixeladas e borradas do que em uma vídeo chamada em uma rede sem NAT no CPE ou CGN. Com exceção a rede com NAT444 onde o Skype para Android não apresentou problemas, nas demais redes foi o sistema que teve as piores degradações nas imagens. As capturas de tela das vídeo chamadas realizadas presentes na figura 4.1 demonstram respectivamente a qualidade da chamada em uma rede sem NAT no CPE ou CGN e em uma rede com 464XLAT para um cliente Skype executando no Windows.

4.1.9 Jogos via Internet

Foi acessado o servidor do jogo League of Legends, um dos mais populares do ano de 2013, procurada uma partida para jogar e jogada uma partida. O jogo somente está disponível para Windows e MAC OS, logo não foi possível fazer os testes nos demais sistemas operacionais. Os resultados estão disponíveis na tabela 4.9.

Tabela 4.9: Resultado para jogos via Internet

Técnicas de Transição	Sistema Operacional Utilizado				
	Linux	Windows 7	MAC OS	IOS	Android
DS-Lite	Indisponível	Igual	Igual	Indisponível	Indisponível
MAP-E	Indisponível	Pior	Igual	Indisponível	Indisponível
464XLAT	Indisponível	Igual	Igual	Indisponível	Indisponível
MAP-T	Indisponível	Pior	Igual	Indisponível	Indisponível
NAT444	Indisponível	Igual	Igual	Indisponível	Indisponível

Fonte: Elaborado pelo autor

Nas redes de teste com MAP-E e com MAP-T o jogo funcionou no Windows, mas a conexão com o servidor apresentou instabilidades com queda de conectividade em alguns momentos. Nas demais redes e sistemas operacionais o jogo funcionou corretamente e não foi notado qualquer impacto na jogabilidade que seriam ocasionados

Figura 4.1: Skype em uma rede com IPv4 público versus Skype em uma rede com 464XLAT, para um cliente Windows.

Fonte: Elaborado pelo autor

por altas latências ou um grande *jitter*.

4.1.10 IPSec / L2TP

Foi configurada uma VPN IPSec com uma máquina na Internet IPv4 através do protocolo L2TP, utilizado o comando ping para testar a conectividade até os servidores web do Google (www.google.com) e do UOL (www.uol.com.br) e depois a página destes dois servidores web foi acessada via um navegador. Os resultados estão disponíveis na tabela 4.10.

Tabela 4.10: Resultado para VPN IPSec/L2TP

Técnicas de Transição	Sistema Operacional Utilizado				
	Linux	Windows 7	MAC OS	IOS	Android
DS-Lite	Pior	Igual	Erro	Erro	Igual
MAP-E	Erro	Erro	Erro	Erro	Erro
464XLAT	Erro	Erro	Erro	Erro	Erro
MAP-T	Erro	Erro	Erro	Erro	Erro
NAT444	Igual	Igual	Erro	Erro	Igual

Fonte: Elaborado pelo autor

Apesar da VPN IPSec/L2TP funcionar corretamente no MAC OS e no IOS quando é utilizada uma rede sem CGN e NAT no CPE, não foi possível estabelecer esta VPN em nenhuma das redes de teste nestes dois sistemas operacionais da Apple, o problema entretanto não foi igual em todos os casos. Nas redes de teste do DS-Lite e NAT444 as etapas inicias de configuração da VPN funcionam, a negociação de chaves do IPSec é concluída e alguns pacotes criptografados com IPSec chegam a ser trocados, entretanto assim que uma mensagem denominada NATkeepalive é enviada a VPN encerra a conexão, levando a conclusão que as implementações possuem algum problema para estabelecer e manter VPN L2TP / IPSec em redes com NAT.

A VPN funcionou adequadamente no Windows, Linux e Android na rede com NAT444 e também não teve problemas na rede com DS-Lite no Windows e Android. Na rede com DS-Lite o Linux apresentou um comportamento inesperado pois a VPN foi estabelecida corretamente e testes de conectividade com o protocolo ICMP mostravam que a VPN possuía acesso a Internet, entretanto quando o acesso aos servidores web era iniciado a VPN simplesmente desconectava sem que nenhuma mensagem de erro ou de diagnóstico fosse gerada ou recebida e sem que qualquer *log* do incidente fosse gerado.

Nas redes com MAP-E e MAP-T nenhum dos sistemas operacionais funcionou,

levando a conclusão que a implementação referência, desenvolvida pela CERNET, destas técnicas não deve incluir algum mecanismo necessário para o correto funcionamento da VPN IPSec / L2TP. Uma possível opção para o mecanismo faltante pode ser um *Application Layer Gateway* (ALG) que faz traduções específicas para o correto funcionamento de uma aplicação ou protocolo, por exemplo, a tradução de portas bem definidas para portas não padronizadas. Outra opção pode ser a ausência de suporte para a negociação do NAT Transversal (NAT-T) (IETF - RFC 3947, 2005) que é utilizado pelo protocolo de trocas de chaves para estabelecimento do IPSec.

Após a análise dos resultados experimentais nota-se que a maioria das aplicações utilizadas por um cliente residencial, em especial as aplicações web, funcionam sem problemas e não são impactadas pelas técnicas de pilha dupla restrita. Entretanto algumas aplicações um pouco mais complexas, possuem limitações de desempenho ou não ainda não funcionam nestas redes. Os problemas parecem estar relacionados em alguns casos, como a VPN L2TP / IPSec, a falta de maturidade das técnicas, em outras circunstâncias a presença de NAT no CPE ou CGN, como no *bittorrent*, parece ser a causa do problema e a terceira causa possível de problema, aparentemente no caso do Skype, está relacionada com a dupla tradução entre IPv4 e IPv6.

5 COMPARAÇÃO QUANTITATIVA

Nesta seção são realizadas as comparações quantitativas com base nos critérios definidos na seção 3. Inicialmente são apresentados os resultados experimentais com o desempenho de cada uma das técnicas nos quesitos analisados. Na sequência os resultados obtidos neste trabalho são comparados com outros trabalhos que fazem análises sobre técnicas de transição.

5.1 Resultados da Análise Quantitativa

Para a análise quantitativa foram realizadas transmissões de pacotes através das redes que implementam cada uma das técnicas de transição. Foram medidos os seguintes parâmetros:

- Atividade de processamento: utilização de CPU e de memória nos equipamentos responsáveis por implementar a técnica de transição;
- Banda real consumida: banda efetivamente consumida na rede somente IPv6 e
- Parâmetros de qualidade de rede: latência, *jitter*, perda de pacotes e banda real obtida na comunicação fim a fim.

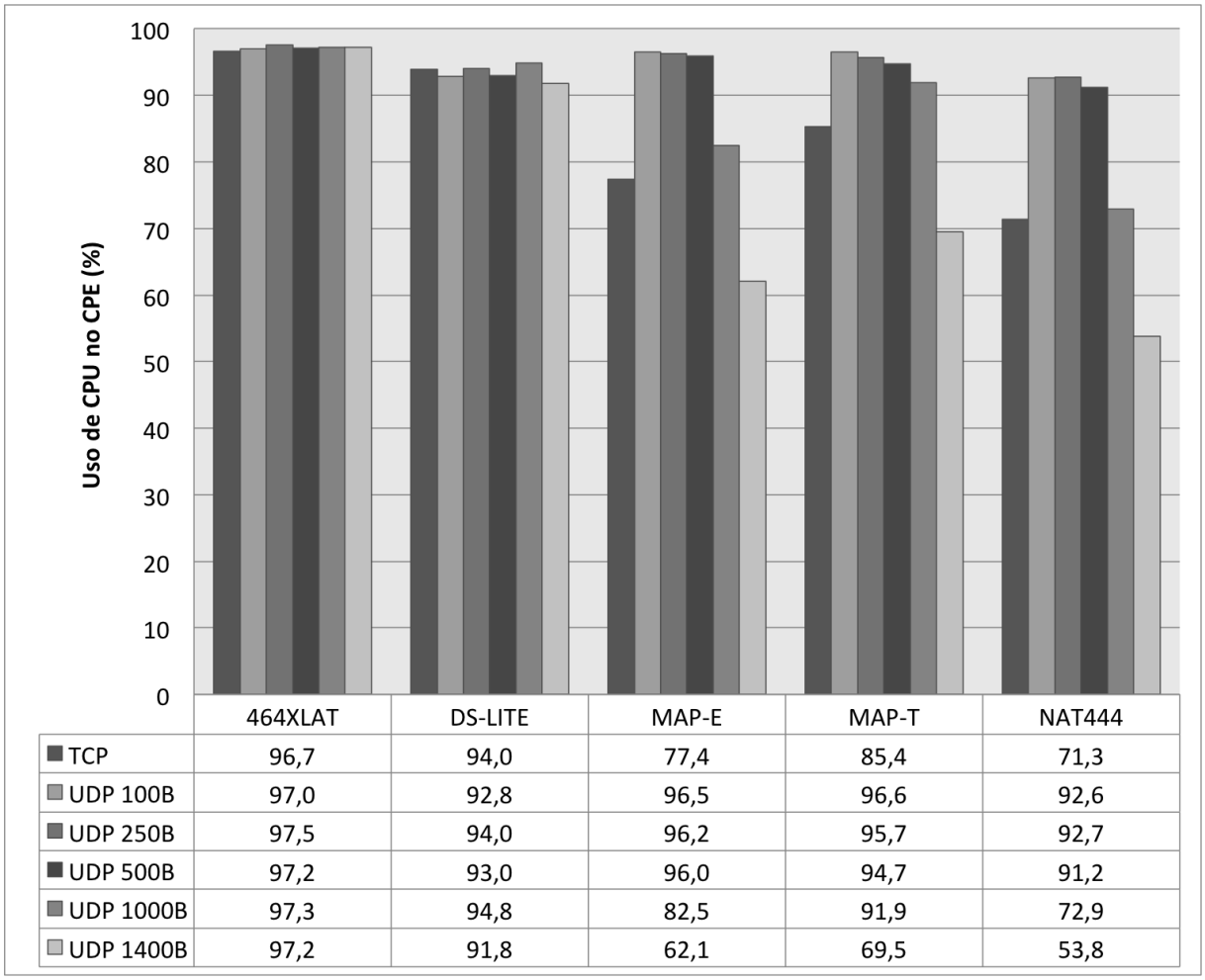
Analisando o processamento e consumo de memória dos equipamentos que executam as técnicas foi possível notar o impacto da quantidade de pacotes no uso da CPU no CPE conforme apresentado na figura 5.1. Os testes UDP solicitaram o envio de 100 Mbps. Já os testes utilizando TCP, devido aos controles e parâmetros adaptativos próprios deste protocolo de transporte, não tiveram uma velocidade de transmissão definida pois esta vai sendo incrementada até chegar ao máximo valor possível. A velocidade máxima final depende do tamanho da janela de recebimento, atraso de propagação e da probabilidade de perda de pacotes.

Os testes mostraram que houve saturamento da CPU em todos os testes do 464XLAT, sendo que a técnica utilizou mais de 90% da CPU em todos eles. No DS-Lite ocorreu uma saturação similar a do 464XLAT, com todos os testes fazendo grande uso da CPU independente do tamanho do pacote. Nas demais técnicas nota-se que o tamanho do pacote, e por consequência a quantidade de pacotes enviados, tem grande influência no uso da CPU. Os testes UDP para pacotes de 100, 250 e 500 bytes foram os que geraram o maior uso da CPU devido a grande quantidade de pacotes necessária para a transmissão dos 100 Mbps. Os testes TCP e UDP de 1000 e 1400 bytes mostram que uma menor quantidade de pacotes gera uma redução considerável no uso de CPU. Em todos os testes o NAT444 foi o que apresentou menor uso da CPU do CPE, isso é devido por ser uma implementação bastante madura e altamente otimizada já que a realização de NAT de IPv4 para IPv4 é algo que acontece em larga escala nas redes atuais.

No roteador de borda o uso de CPU não foi mensurável em nenhum dos testes, levando a conclusão que a maior capacidade de processamento deste equipamento permitiria um teste em uma maior escala. O uso de memória neste equipamento também não revelou uma relação direta entre a execução da técnica e o consumo de memória. No caso do CPE toda a memória do dispositivo consta como em uso desde o começo do experimento e não há variação durante o teste e tentativas de obtenção dos dados diretamente dos processos relacionados não se mostraram confiáveis pois algumas técnicas utilizam mais de um processo e outras não fazem alocações dinâmicas de memória fazendo uma reserva constante de memória que é alocada no início da execução.

Em todos os experimentos houve perda de pacotes no CPE, assim sendo, a velocidade real na rede IPv6 não pode ser diretamente comparada à velocidade real de transmissão. Por isto, ao invés de analisar a velocidade real de transmissão, foi medido o *overhead* por pacote em cada uma das técnicas. No NAT444 como a tradução é de IPv4 privado para IPv4 compartilhado e posterior tradução para IPv4 público, não ocorrem mudanças no tamanho do pacote pois somente o endereço de origem é alterado. No caso do MAP-T e 464XLAT que fazem dupla de tradução IPv4 para IPv6 e posteriormente de IPv6 para IPv4 o consumo adicional notado foi a diferença entre o tamanho do cabeçalho IPv4 do pacote original e o tamanho do cabeçalho do pacote traduzido para IPv6. Esta diferença foi de 20 bytes, que no pacote IPv4 de 100 bytes representou um aumento de 20% no tamanho do pacote e no pacote de 1400 bytes um aumento de 1,4%. Nas técnicas que fazem o encapsulamento do pacote IPv4 em

Figura 5.1: Uso de CPU no CPE x Tamanho do Pacote x Técnica



	464XLAT	DS-LITE	MAP-E	MAP-T	NAT444
TCP	96,7	94,0	77,4	85,4	71,3
UDP 100B	97,0	92,8	96,5	96,6	92,6
UDP 250B	97,5	94,0	96,2	95,7	92,7
UDP 500B	97,2	93,0	96,0	94,7	91,2
UDP 1000B	97,3	94,8	82,5	91,9	72,9
UDP 1400B	97,2	91,8	62,1	69,5	53,8

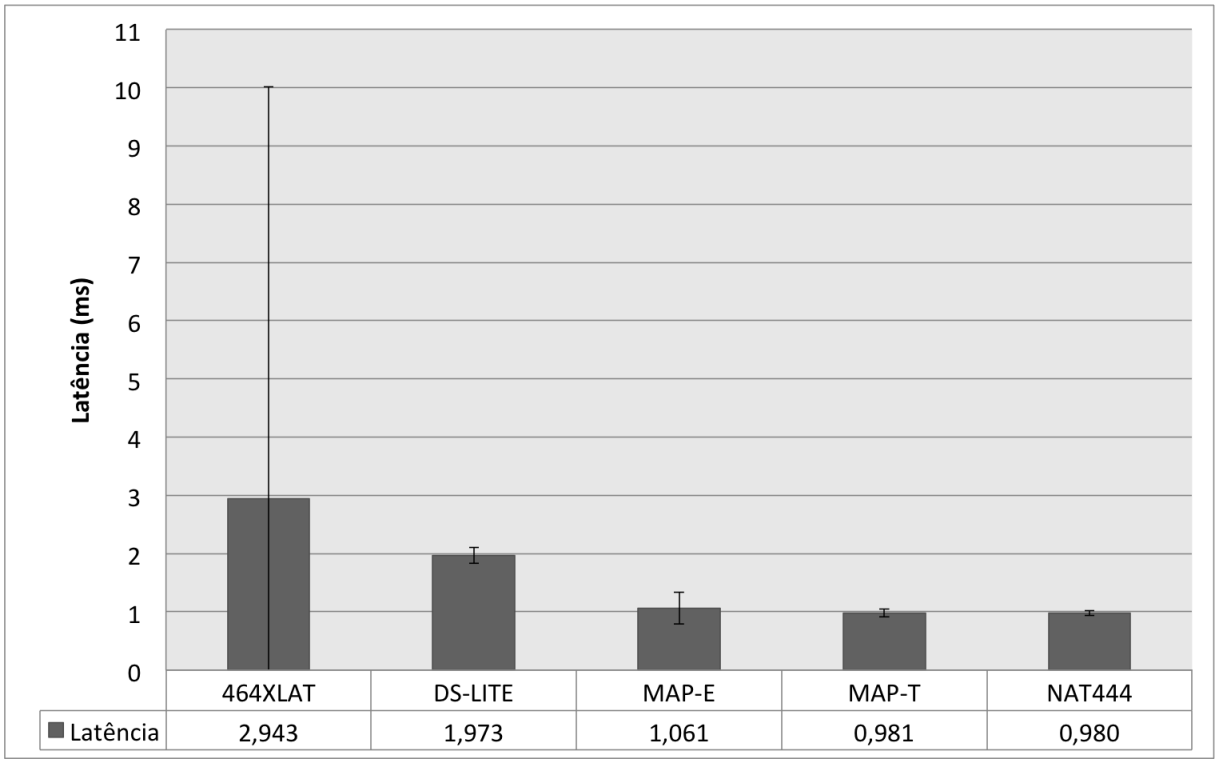
Fonte: Elaborado pelo autor

um pacote IPv6 o consumo adicional por pacote é de 40 bytes, pois o pacote IPv4 é mantido sem alteração e um novo cabeçalho IPv6 é adicionado, sendo que este cabeçalho IPv6 possuí tamanho fixo de 40 bytes. Isto representa um aumento de 40% no pacote de 100 bytes e de 2,8% no pacote de 1400 bytes. Considerando que aplicações de transmissão de áudio e vídeo tendem a utilizar pacotes pequenos enviados via UDP, a utilização das técnicas de pilha dupla restrita geraram um maior *overhead* nestas aplicações do que em aplicações que usem pacotes maiores.

Com relação aos parâmetros de rede eles apresentaram uma correlação com a utilização da CPU no CPE, onde quanto maior este uso de CPU, pior o desempenho da técnica. A latência, primeiro parâmetro de qualidade, apresentado na figura 5.2, mostra que o 464XLAT teve um atraso de propagação aproximadamente três vezes maior que as técnicas que consumiram menos CPU, MAP-E, MAP-T e NAT444. Já

o DS-Lite, que teve um consumo menor que o 464XLAT, mas maior que as demais técnicas teve uma latência aproximada de 2 ms, sendo 1 ms mais lento que o MAP-E, MAP-T e NAT444 e 1 ms mais rápido que o 464XLAT.

Figura 5.2: Latência x Técnica

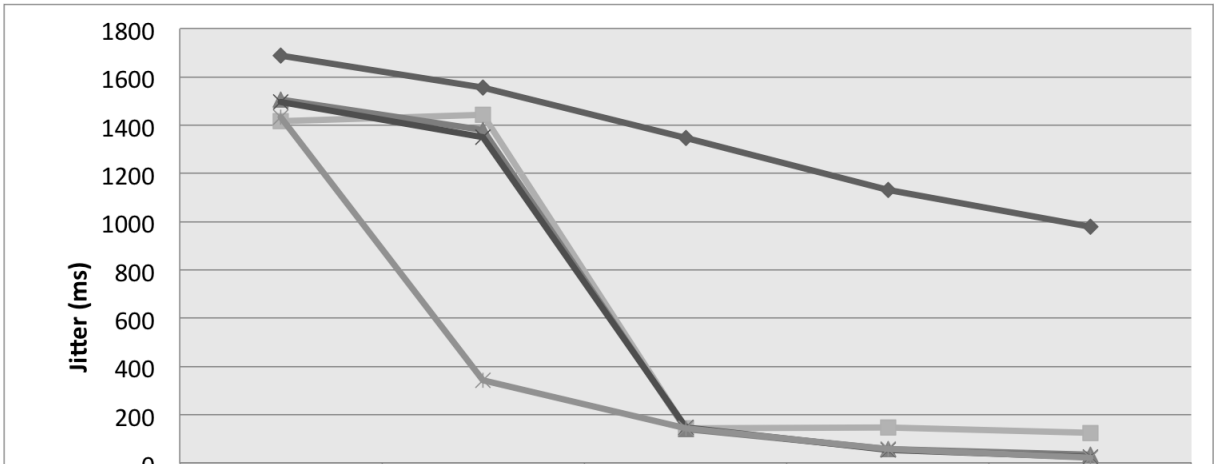


Fonte: Elaborado pelo autor

Já o segundo parâmetro de qualidade, *jitter*, teve um comportamento bastante similar para o MAP-E, MAP-T e DS-Lite com um alto valor quando o processador estava saturado com os pacotes de 100B, um valor bastante similar para os pacotes de 250B e uma signficativa melhora para os pacotes a partir de 500B. Entretanto a partir deste ponto o MAP-E e MAP-T obtiveram melhoras para os pacotes de 1000 e 1400 bytes, enquanto o DS-Lite se estabilizou no patamar similar ao dos pacotes de 500B. O 464XLAT foi o pior de todos neste parâmetro apresentando uma melhora praticamente linear com relação ao tamanho do pacote. Já o NAT444 teve um *jitter* muito ruim para pacotes de 100 bytes, entretanto teve uma melhora significativa para pacotes a partir de 250 bytes e teve o menor *jitter* entre todas as técnicas. Os resultados são apresentados na figura 5.3.

O parâmetro perda de pacotes pode ser avaliado na figura 5.4. A perda de pacotes de 100 bytes foi significativa para todas as técnicas e a que teve melhor desempenho,

Figura 5.3: *Jitter* x Tamanho do Pacote x Técnica



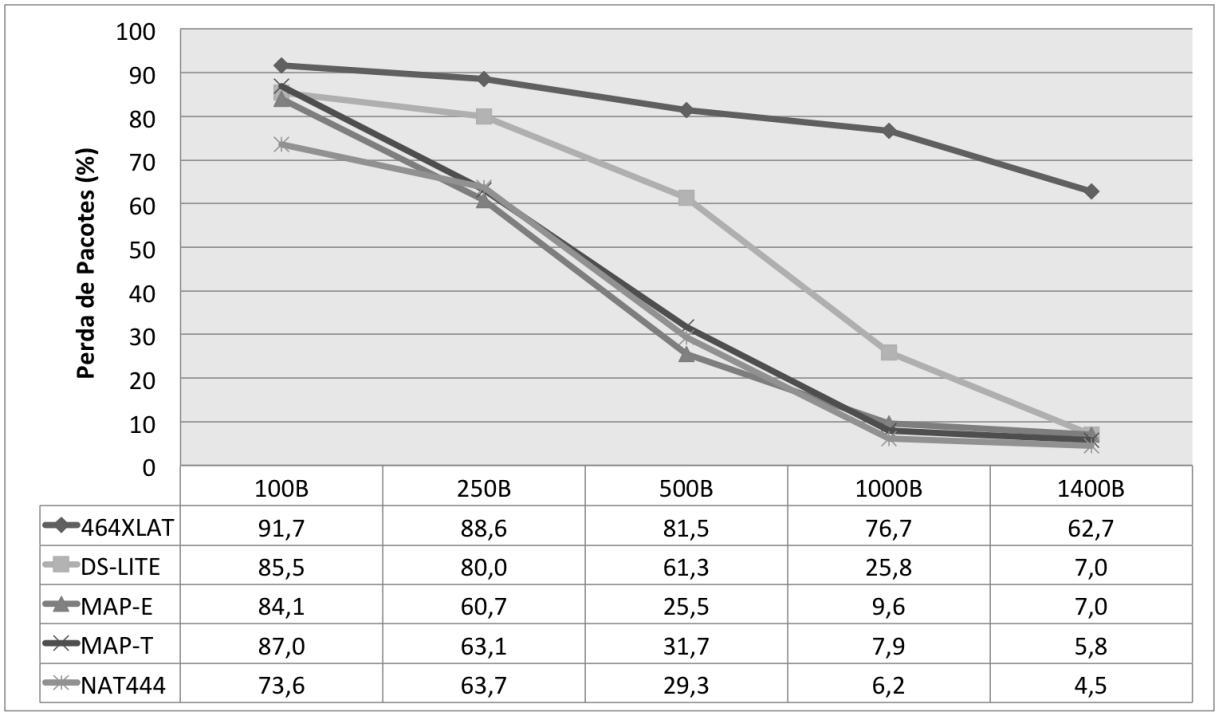
	100B	250B	500B	1000B	1400B
464XLAT	1689	1557	1348	1133	978
DS-LITE	1418	1444	145	146	125
MAP-E	1507	1380	139	58	33
MAP-T	1495	1349	148	54	24
NAT444	1432	344	144	59	22

Fonte: Elaborado pelo autor

o NAT444, perdeu 73,5% dos pacotes enviados e a pior delas, o 464XLAT, perdeu 91,7% dos pacotes. Para pacotes a partir de 250 bytes o MAP-E e MAP-T passaram a ter desempenho similar ao do NAT444. O DS-Lite e o 464XLAT também perderam menos pacotes quando os pacotes eram maiores, mas enquanto o DS-Lite chegou ao mesmo patamar do MAP-E, MAP-T e NAT444 para pacotes de 1400 bytes o 464XLAT continuou com um péssimo rendimento, perdendo mais de 60% dos pacotes de 1400 bytes.

Com relação ao parâmetro banda efetiva, exibido na figura 5.5, pode-se notar que o desempenho tanto em TCP quanto em UDP do MAP-E, MAP-T e NAT444 são bastante similares e para pacotes de 1000 bytes elas já obtiveram velocidade similar ao resultado em TCP, entretanto para pacotes pequenos as velocidades foram bem menores, já que houve grande perda de pacotes. O DS-Lite teve um desempenho crescente em função do tamanho do pacote obtendo resultados similares ao MAP-E, MAP-T e NAT444 para pacotes de 1400 bytes, entretanto o desempenho TCP foi inferior ao destas outras técnicas. Já o 464XLAT teve um desempenho bastante inferior e a velocidade máxima obtida foi aproximadamente 40 Mbps com pacotes TCP.

Figura 5.4: Perda de Pacotes x Tamanho do Pacote x Técnica



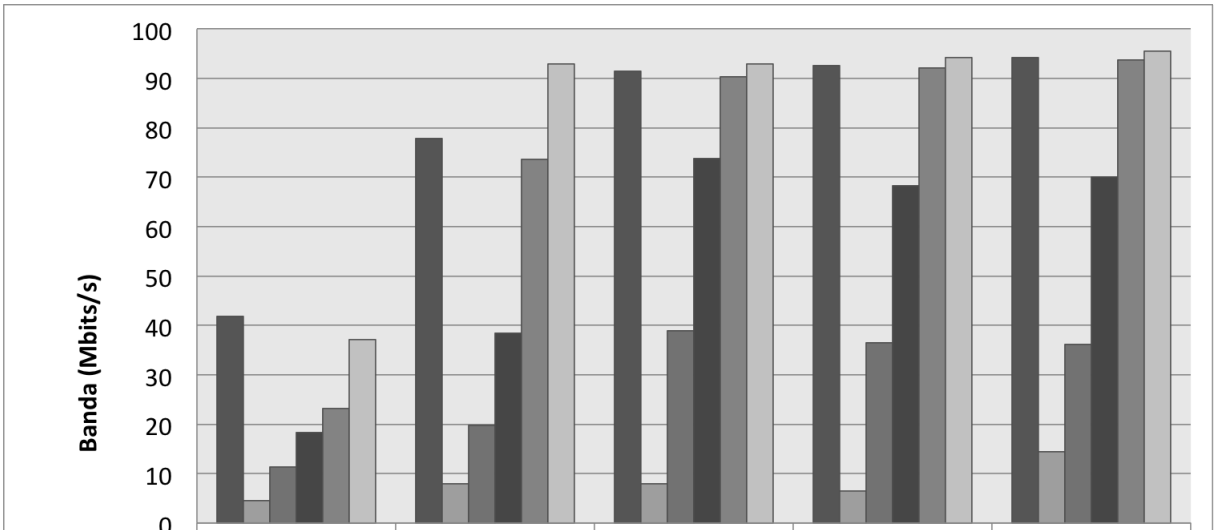
	100B	250B	500B	1000B	1400B
464XLAT	91,7	88,6	81,5	76,7	62,7
DS-LITE	85,5	80,0	61,3	25,8	7,0
MAP-E	84,1	60,7	25,5	9,6	7,0
MAP-T	87,0	63,1	31,7	7,9	5,8
NAT444	73,6	63,7	29,3	6,2	4,5

Fonte: Elaborado pelo autor

Os resultados experimentais permitiram perceber que NAT444 possui um *overhead* consideravelmente menor que as demais técnicas de pilha dupla restrita. Para pacotes de 100 bytes as técnicas que fazem encapsulamento (DS-Lite e MAP-E) possuem um *overhead* 40% maior e as técnicas que fazem dupla tradução geram um *overhead* 20% maior que o NAT444, por causa dos mecanismos de encapsulamento e de dupla tradução respectivamente. Como o aumento de bytes do encapsulamento e da dupla tradução são constantes, independente do tamanho do pacote, eles geram um menor impacto em pacotes grandes, por isso para os pacotes de 1400 bytes o *overhead* do encapsulamento é 2,8% maior e o *overhead* da dupla tradução é 1,4% maior em comparação com o NAT444.

Apesar do *overhead*, a diferença de velocidade obtida nos testes entre o NAT444 e as demais técnicas esteve diretamente relacionada ao consumo da CPU no CPE e não com os 40 bytes a mais que o encapsulamento necessita ou com 20 bytes a mais que a dupla tradução utiliza. O NAT já é utilizado em larga escala e melhor otimizado, por isso seu melhor desempenho da rede que utiliza dois NATs encadeados (NAT444) não foi uma surpresa. Adicionalmente, se as interfaces estivessem perto da saturação, o desempenho do 464XLAT, DS-Lite, MAP-E e MAP-T seriam significativamente

Figura 5.5: Banda Efetiva x Tamanho do Pacote x Técnica



	464XLAT	DS-LITE	MAP-E	MAP-T	NAT444
TCP	41,9	77,8	91,5	92,7	94,2
UDP 100B	4,5	7,9	8,0	6,5	14,5
UDP 250B	11,3	19,8	39,0	36,6	36,2
UDP 500B	18,3	38,4	73,9	68,3	70,1
UDP 1000B	23,1	73,6	90,4	92,1	93,8
UDP 1400B	37,1	93,0	93,0	94,2	95,5

Fonte: Elaborado pelo autor

afetados pelo *overhead* e o NAT444 teria um desempenho relativo ainda maior. Entretanto, neste experimento, as interfaces na rede da operadora eram de 1 Gbps e por isso longe da saturação, já que a velocidade máxima solicitada foi de 100 Mbps.

Com relação a comparação de encapsulamento versus dupla tradução não houve um claro vencedor já que o desempenho de duas técnicas que executam com o mesmo código fonte, MAP-E e MAP-T, foi bastante similar. Apesar da similaridade no desempenho de banda passante, *jitter* e perda de pacotes, foi possível notar que a tradução é computacionalmente mais intensa que o encapsulamento enquanto o encapsulamento possui um maior *overhead* na rede somente IPv6 que a dupla tradução.

5.2 Comparação com Outros Trabalhos

O trabalho de Skoberne et al. (2013) se concentra em uma análise teórica das técnicas de transição, fazendo classificações e comparações teóricas de mecanismos. Já os artigos de Lencse e Repas (2013) e Repas, Hajas e Lencse (2014), desenvolvi-

dos no Departamento de Telecomunicações da *Budapest University of Technology and Economics* fazem análises de desempenho e de funcionalidade de aplicações em redes NAT64, usando o Tayga como uma das ferramentas analisadas. Apesar do NAT64 não ser diretamente analisado nesta pesquisa, o Tayga é utilizado na montagem da rede com 464XLAT, para implementar o CLAT e o PLAT, e por isto os resultados destes artigos são relevantes para esta comparação.

A análise realizada no trabalho de Skoberne et al. (2013) declara que a dupla tradução consome menos processamento que o tunelamento, mas a análise experimental aqui realizada contradiz esta afirmação, já que duas técnicas que utilizam A+P e compartilham o mesmo código fonte (MAP-E e MAP-T), mostram que a tradução é um pouco mais intensiva no quesito processamento.

Nas pesquisas realizadas na *Budapest University of Technology and Economics*, em especial a comparação realizada por Lencse e Repas (2013) foram obtidos resultados similares ao deste experimento, mostrando que o programa Tayga possuí limitações quanto a sua escalabilidade e com aproximadamente 5 Mbps o equipamento que fazia o NAT64 já estava com 100% do processamento. O Tayga, utilizado nesta dissertação para implementar o 464XLAT, também teve problemas de escalabilidade atingindo no máximo 40 Mbps. Considerando que o 464XLAT já é usado em redes de produção da operadora de telefonia móvel estadunidense T-Mobile, é possível concluir que o baixo desempenho do 464XLAT neste experimento está relacionado ao Tayga e não a técnica em si.

6 ANÁLISE DE VIABILIDADE

Após a análise qualitativa e quantitativa, estas são revisitadas e, com a adição de novos aspectos e estimativas, uma análise de viabilidade técnica e econômica é apresentada nesta seção.

6.1 Viabilidade Técnica

A facilidade de implantação da técnica possuí um alto impacto na possibilidade de utilização da mesma. Isto significa que mesmo uma técnica com o melhor desempenho possível quando em operação, mas que é extremamente difícil de implantar pode acabar preterida por uma técnica de menor desempenho porém mais fácil de implantar. A viabilidade técnica também considera as vantagens que uma técnica oferece, a principal vantagem das técnicas de pilha dupla restrita, com exceção do NAT444, é a eliminação do IPv4 do núcleo da rede da operadora e por consequência o roteamento interno e gerência deixam de ser necessários em IPv4. Outra vantagem é a menor necessidade de *logs* nas técnicas que fazem uso de A+P, já que a identificação do usuário pode ser feita através de uma função matemática ao invés de guardar as portas atribuídas para cada cliente quando os pacotes passam pelo CGN.

Outro fator importante para de ser considerado neste contexto, e particularmente nas redes brasileiras, é a especialização técnica dos funcionários dos provedores de Internet. Conforme estatísticas divulgadas na pesquisa "TIC Provedores 2011" do CETIC.br (CETIC.br / NIC.br, 2012a) e (CETIC.br / NIC.br, 2013), em 2011 o Brasil tinha 1934 provedores de acesso à Internet, destes 54% possuíam 9 funcionários ou menos e 24% possuíam entre 10 e 19 funcionários, o que indica que 78% dos provedores são micro empresas. Considerando que micro empresas não possuem um grande faturamento é razoável considerar que estas empresas podem ter dificuldades em oferecer treinamentos de especialização para seus funcionários ou em manter um funcionário altamente especializado com um salário compatível com a média do

mercado, tendo assim mais dificuldades na utilização de técnicas complexas.

Analisando as técnicas comparadas neste trabalho, as técnicas de pilha dupla restrita, DS-Lite, 464XLAT, MAP-E e MAP-T, fazem uso de conceitos novos, mais avançados e complexos do que o NAT444. A própria experiência de montar, configurar e corrigir os erros nas redes de testes para as técnicas de pilha dupla restrita deste trabalho demonstrou-se muito mais complicada que a criação da rede com NAT444. Esta última nada mais é do que uma técnica já bastante difundida e bem conhecida em redes IPv4 mas que, devido a falta de endereços IPv4, é implementada dentro da rede do provedor usando equipamentos com maior capacidade de processamento que os equipamentos usados pelos clientes residenciais para fazer NAT em suas casas. Assim sendo, considero que para pequenos provedores, o NAT444 possui uma maior viabilidade técnica que as técnicas de pilha dupla restrita. Entretanto o NAT444 isoladamente não é uma técnica de transição para o IPv6 e os provedores que optarem pela facilidade e conhecimento prévio no uso de NAT devem utilizá-lo juntamente com o IPv6.

Mesmo para provedores maiores e com funcionários mais especializados as técnicas de pilha dupla restrita podem não ser triviais de serem implantadas. A vantagem técnica que elas oferecem com a extinção do IPv4 na rede do provedor, permitindo a configuração, manutenção e gerenciamento de menos redes e protocolos de roteamento, é contrabalanceada pela necessidade que equipamentos de rede dos provedores, incluindo o CPE do cliente, tenham suporte as estas técnicas. Somente o DS-Lite e o 464XLAT já foram padronizados pelo IETF e, destas duas, somente o DS-Lite já possui implementações maduras de diversos fabricantes, sendo hoje a única das quatro técnicas, que eliminam endereços IPv4 do núcleo da rede do provedor, factível de ser utilizada em larga escala.

Comparando as técnicas de pilha dupla restrita entre si alguns fatos podem impactar na viabilidade técnica. O DS-Lite precisa que uma terminação de túnel seja configurada no AFTR (*Address Family Transition Router*), equipamento na borda da operadora, para cada cliente, ou seja, se houver dez mil clientes, dez mil túneis serão configurados no equipamento de borda. O DS-Lite e o 464XLAT fazem uso de CGN, o que necessita de sistemas de armazenamento de *logs* similares ao NAT444, na rede da operadora. Como usa dupla tradução, o 464XLAT, não precisa da configuração e terminação dos milhares de túneis.

A principal deficiência das técnicas que fazem uso de CGN (DS-Lite, 464XLAT e

NAT444) é a impossibilidade de fornecer conexões entrantes ao usuário final. Esta inviabilidade pode vir a ser eliminada se o PCP (*Port Control Protocol*) passar a ser utilizado em ampla escala, mas não é possível prever quando e se realmente este protocolo será adotado em larga escala.

O MAP-E, por usar encapsulamento como o DS-Lite, também precisa da terminação dos túneis no equipamento de borda da operadora. Entretanto o MAP-E e também o MAP-T, não fazem uso de CGN e com isso o mecanismo de UPnP já presente em grande parte dos roteadores domésticos e sistemas operacionais poderia ser utilizado para receber conexões entrantes. Esta funcionalidade ainda não está disponível no programa de referência desenvolvido pela CERNET, mas seria facilmente implementada em um equipamento comercial. Esta falta de funcionalidade no MAP-E e no MAP-T não é grave para um programa com a função de ser uma prova de conceito, mas o fato de nenhum dos dois ter sido padronizados pelo IETF, ainda inibe sua adoção em equipamentos e sua utilização em redes de produção.

As técnicas de pilha dupla restrita, em sua maioria, não estão prontas para a utilização em larga escala nas redes de hoje, mesmo que ofereçam vantagens como uma menor quantidade de *logs* armazenados (MAP-E e MAP-T) ou a gerência de um só protocolo no núcleo da rede do provedor (464XLAT, DS-Lite, MAP-E e MAP-T). Entretanto este cenário deve mudar em alguns anos, a padronização, o aperfeiçoamento e maior quantidade de implementações das técnicas de pilha dupla restrita, pode justificar o uso delas no futuro, pois o esforço de implantação e gerenciamento de uma rede somente IPv6 pode vir a ser menor do que o esforço de expandir e gerenciar uma rede com IPv4 privado e IPv4 compartilhado, com seus respectivos *logs*, e IPv6.

6.2 Viabilidade Econômica

Fazer a estimativa do custo de implantação e operação das técnicas é uma tarefa bastante particular para cada provedor de acesso à Internet, pois cada um possui características próprias e utiliza equipamentos e fabricantes diferentes. Por exemplo, um pequeno provedor que oferece Internet via rádio e não é um sistema autônomo, provavelmente utiliza NAT444 na sua operação hoje e nenhum de seus equipamentos instalados em clientes é compatível com as outras técnicas de pilha dupla restrita, assim sendo, para ele é economicamente inviável a substituição de todos os equipamentos e talvez até implicando em uma mudança do meio de transmissão para implantar alguma destas técnicas. Neste exemplo, a única solução economicamente

viável a manutenção do NAT444 e a paulatina implantação de IPv6.

Considerando que a rede de cada provedor tem características únicas, esta seção baseia-se em análises de casos particulares para fazer as comparações, mesmo sabendo da grande quantidade de exceções que podem existir a estas comparações.

As técnicas 464XLAT, DS-Lite e NAT444 possuem um ponto comum que impacta a viabilidade econômica, o uso de CGN. Este depende de equipamentos caros na borda da operadora para executar a função de compartilhamento de endereços, pois necessita de grande quantidade de memória RAM e processamento para fazer o NAT em larga escala não gerar impacto na experiência dos usuários, mas este não é o único impacto econômico, pois também existe a necessidade de um grande sistema de armazenamento de *logs*, para que cada mapeamento de IPv4 privado (DS-Lite) ou de IPv4 compartilhado (NAT444) ou de IPv6 (464XLAT) em IPv4 público seja guardado. Estes *logs* não devem conter somente os endereços envolvidos, mas também a porta de origem vinculada ao IPv4 público. Isto é necessário pois, sem o armazenamento da porta de origem nos *logs*, é tecnicamente impossível a identificação unívoca do cliente já que a correlação de IPv4 público de origem, data e hora do evento investigados é insuficiente para tal identificação.

Outro ponto que impacta a viabilidade econômica é a falta de equipamentos no mercado que suportem o 464XLAT, MAP-E e MAP-T. Esta falta de suporte tem muito impacto econômico nos provedores de acesso à Internet que não conseguem fazer atualização remota dos equipamentos instalados nos clientes, isto significa que para a instalação destas técnicas de pilha dupla restrita seria necessária a troca destes equipamentos e o valor desta troca envolvem o custo do equipamento novo e também o custo uma visita técnica ao cliente (mão de obra, combustível etc). O impacto na viabilidade econômica da adoção das técnicas de pilha dupla restrita pode ser reduzido se a rede atual do provedor não tiver suporte IPv6, pois a adoção do IPv6 é inevitável e necessária para o provedor continuar crescendo e operando no futuro e, ao trocar o equipamento antigo por um novo com suporte IPv6, o suporte as técnicas de pilha dupla restrita já pode ser considerado.

Entretanto a viabilidade econômica não pode somente considerar gastos, é necessário considerar a potencial perda de receita. Esta estimativa é um exercício de futurologia ainda mais complicado que a estimativa de gastos, pois tem que considerar os custos de chamados técnicos e ligações para a central de atendimento gerados por problemas causados diretamente pelas técnicas e a perda de clientes pois al-

guma aplicação especifica, por exemplo VPN, não funciona na rede com a técnica utilizada. Nos trabalhos de Lee Horward (HORWARD, 2013), (HORWARD, 2012b) e (HORWARD, 2012c) ele considera sua experiência em um dos maiores provedores de Internet dos Estados Unidos, a Time Warner Cable, para a elaboração de modelos de custos para a transição de IPv4 para IPv6. Suas comparações consideram o NAT444 como base, mas podem ser extrapoladas e consideradas como modelo de custos válidos para o DS-Lite e 464XLAT que também fazem uso do CGN. Suas estimativas, consideram os custos de aquisição de equipamentos, manutenção da rede, perda de clientes, entre outros, e chegam a um valor de trinta dólares por ano por cliente para manter o NAT444, DS-Lite ou 464XLAT em operação por um período de cinco anos. Este é um valor alto, onde um provedor com dez mil clientes gastaria por ano trezentos mil dólares. As comparações de Lee Horward vão além do escopo analisado neste trabalho, mas dois pontos de suas conclusões se destacam:

1. Comprar endereços IPv4, hoje com preço estimado em quinze dólares, é mais barato que implantar e manter o NAT444, DS-Lite e 464XLAT. Entretanto esta opção não é válida para as políticas atualmente vigentes no LACNIC;

2. Uma rede sem endereçamento IPv4 é a única maneira de reduzir os custos do provedor de acesso à Internet mas, segundo seus estudos, isso somente será possível quando os quinze maiores provedores de conteúdo suportarem clientes somente IPv6 e cada endereço IPv4 custar quarenta dólares ou mais. É importante notar que os principais conteúdos hoje suportam IPv6, mas não suportam perfeitamente clientes que só tem IPv6. Muitas vezes o IPv4 é utilizado devido a problemas no IPv6 ou para carregar uma parte do conteúdo de uma página que ainda não esteja em IPv6, tal como uma propaganda baseada em geolocalização, mas isso não é notado pelo usuário final. Neste sentido a entrega de IPv4 através de técnicas de pilha dupla restrita podem ser um passo intermediário nesta transição para redes somente IPv6.

Ao utilizar a planilha de custos de Lee Horward (HORWARD, 2012a), usada por ele nas estimativas do NAT444, DS-Lite e 464XLAT, fiz as seguintes alterações para adaptá-la ao cenário de utilização do MAP-E e MAP-T:

1. redução no custo do sistema de *log* que é mais simples para o MAP-E e MAP-T;

2. redução na perda de clientes ocasionada pela falta de conexões entrantes, pois estas são possíveis de serem implementadas nestas técnicas;

3. aumento de cinquenta dólares por cliente para a troca de todos os CPEs de clientes, pois os CPEs hoje disponíveis não oferecem suporte a estas técnicas.

Estas alterações determinaram que o custo do MAP-E e do MAP-T seria ligeiramente menor que o das demais técnicas de pilha dupla restrita, com um valor aproximado de vinte e cinco dólares por cliente por ano em um período de cinco anos.

Entretanto um outro modelo de custos desenvolvido por Gottardi (2013) faz uma estimativa bastante diferente e considera que o MAP-E e o MAP-T possuem um custo decrescente ao longo dos anos, diferente do NAT444, DS-Lite e 464XLAT. Este modelo chega a conclusão de que no terceiro ano de utilização o MAP-E e o MAP-T custam trinta por cento menos e a partir do quarto ano cinquenta por cento mais barato que o DS-Lite, 464XLAT e NAT444.

As análises de viabilidade técnica e econômica, permitiram notar que as técnicas de pilha dupla restrita não são viáveis para a utilização em pequenos provedores, pois em alguns casos esses possuem NAT444 em suas redes hoje, em outros cenários trabalham com equipamentos que são incompatíveis com as técnicas ou mesmo possuem uma pequena equipe técnica, possivelmente sem a especialização necessária para implementar as complexas técnicas de pilha dupla restrita.

Se considerados os provedores de maior porte as técnicas de pilha dupla restrita passam a ser viáveis como meio para reduzir custos com o objetivo final de ter uma rede, incluindo clientes, com somente endereçamento IPv6. Neste cenário as estimativas mostram que as técnicas de pilha dupla restrita que utilizam A+P possuem menor custos e seriam mais interessantes economicamente, mas isto contrasta com a viabilidade técnica atual já que estas técnicas não estão maduras ainda, carecendo de padronização no IETF.

7 CONCLUSÕES

Este trabalho teve o objetivo de fazer uma comparação de desempenho, de funcionamento e de viabilidade técnica e econômica entre as técnicas de transição do IPv4 para o IPv6 que utilizam pilha dupla restrita. Este objetivo foi alcançado e os resultados aqui obtidos podem auxiliar o grupo *Softwire* do IETF em suas discussões sobre encapsulamento versus dupla tradução e CGN versus A+P, para as técnicas aqui analisadas (MAP-E, MAP-T, DS-Lite, 464XLAT e NAT444) e outras técnicas similares.

As técnicas de transição com pilha dupla restritas comparadas neste trabalho possibilitam a comunicação em IPv4 através de um provedor cujo núcleo da rede somente possui endereçamento IPv6. O IPv4 restrito recebido pelo cliente, pode ser privado ou público com portas limitadas, e é recebido juntamente com o IPv6 globalmente roteável. Já a rede com NAT444, não tem qualquer dependência do IPv6 e pode ser usada sem ele, mas ela foi analisada neste trabalho pois, se o IPv4 compartilhado for entregue ao cliente juntamente com IPv6 globalmente roteável, o NAT444 pode ser considerado uma técnica de pilha dupla restrita.

A análise dos resultados experimentais permitiu a constatação de que a maioria das aplicações utilizadas por um cliente residencial, em especial as aplicações web, funcionam sem problemas e não são impactadas pelas técnicas de pilha dupla restrita. Apesar disto, algumas aplicações mais complexas e específicas, possuem limitações de desempenho ou não funcionam adequadamente nestas redes. Os problemas destas aplicações estão relacionados em sua maioria a falta de maturidade das técnicas e de suas implementações ou, como no *bittorrent*, a existência do CGN é a causa do problema, já que este impede o recebimento de conexões entrantes.

Os resultados experimentais permitiram perceber que NAT444 possui um *overhead* consideravelmente menor que as demais técnicas de pilha dupla restrita. Por exemplo, para pacotes de 100 bytes as técnicas que fazem encapsulamento (DS-Lite e MAP-E) possuem um *overhead* 40% maior e as técnicas que fazem dupla tradução geram um

overhead 20% maior que o NAT444, por causa dos mecanismos de encapsulamento e de dupla tradução respectivamente. Como o aumento de bytes do encapsulamento e da dupla tradução são constantes, independente do tamanho do pacote, eles geram um menor impacto em pacotes grandes.

Apesar do *overhead*, a diferença de velocidade obtida nos testes entre o NAT444 e as demais técnicas esteve diretamente relacionada ao consumo da CPU no CPE e não com os 40 bytes a mais que o encapsulamento necessita ou com 20 bytes a mais que a dupla tradução utiliza. O NAT já é utilizado em larga escala e melhor otimizado, por isso seu melhor desempenho da rede que utiliza dois NATs encadeados (NAT444) não foi uma surpresa. Adicionalmente, se as interfaces estivessem perto da saturação, o desempenho do 464XLAT, DS-Lite, MAP-E e MAP-T seriam significativamente afetados pelo *overhead* e o NAT444 teria um desempenho relativo ainda maior.

Outra constatação experimental foi que pacotes menores, por consumirem mais processamento no CPE, tiveram muitos mais pacotes perdidos que os pacotes grandes e consequentemente uma velocidade muito menor.

Na comparação direta entre as técnicas de pilha dupla restrita não houve um claro vencedor, e as diferenças de velocidade estiveram mais relacionadas a eficiência das implementações do que a características das técnicas. Tal fato pode ser notado comparando o MAP-E e MAP-T, que utilizam A+P, e tiveram desempenho similar ao NAT444, que usa CGN. A diferença de desempenho entre encapsulamento e dupla tradução também não foi significativa, já que o desempenho de duas técnicas que executam com o mesmo código fonte, MAP-E e MAP-T, foi bastante similar. Apesar da similaridade no desempenho de banda passante, *jitter* e perda de pacotes, foi possível notar que a tradução é computacionalmente mais intensa que o encapsulamento enquanto o encapsulamento possui um maior *overhead* na rede somente IPv6 que a dupla tradução.

Na análise de viabilidade constatou-se que o 464XALT, DS-Lite, MAP-E e MAP-T não devem ser soluções viáveis para pequenos provedores, pois em alguns casos esses já possuem NAT444 em suas redes hoje ou trabalham com equipamentos que não suportam estas técnicas de transição ou possuem uma pequena equipe técnica que pode não ter a capacitação necessária para implantar estas técnicas que são mais complexas que o NAT444.

Considerando provedores de maior porte todas técnicas de pilha dupla restrita passam a ser viáveis. Entretanto esta viabilidade somente ocorre como meio para se

chegar a uma rede somente IPv6, que é a única maneira efetiva para reduzir custos nestes cenário de transição do IPv4 para o IPv6. As estimativas também demonstraram que as técnicas de pilha dupla restrita que utilizam A+P possuem menor custos e seriam mais interessantes economicamente, entretanto esta vantagem econômica contrasta com a baixa a viabilidade técnica destas, já que estas técnicas não estão maduras ainda, uma vez que o MAP-E e o MAP-T sequer foram aceitos como padrões pelo IETF.

Em resumo, todas as técnicas de pilha dupla restrita se provaram tecnicamente viáveis, apesar de terem algumas limitações, desde que seus equipamentos e implementações sejam devidamente desenvolvidos em produtos comerciais para poderem ser utilizadas em rede de produção, incluindo as soluções paliativas, baseadas no PCP (*Port Control Protocol*), para mitigar o impacto do CGN nas conexões entrantes. Entretanto a demora deste desenvolvimento pode ser um fator decisivo na escolha de uma das técnicas, já que a transição para IPv6 não pode esperar mais devido ao esgotamento dos endereços IPv4. A escolha de uma técnica neste momento, baseada em critérios técnicos e econômicos, provavelmente considerará que a técnica escolhida pelo provedor será a única a ser utilizada até que a transição para redes que utilizem somente endereçamento IPv6 venha ser concluída. Uma nova técnica ou o amadurecimento das técnicas existentes, mesmo sendo técnica e economicamente melhor, podem ser insuficientes para que esta técnica seja utilizada pois ela terá chegado tardiamente ao processo de transição.

As conclusões aqui apresentadas podem ser utilizadas em possíveis trabalhos futuros como, por exemplo, a criação de uma nova técnica de transição de pilha dupla restrita onde a utilização de encapsulamento ou dupla tradução é uma escolha dinâmica ou configurável, onde pacotes pequenos utilizem dupla tradução para ter um menor *overhead* e pacotes grandes sejam encapsulados para gastar menos processamento. Outra possibilidade de trabalho futuro é a comparação destas técnicas em redes muito maiores, tais como, pilotos de grandes operadoras que estejam analisando como fazer e os impactos da migração de IPv4 para IPv6.

REFERÊNCIAS

BYRNE, C. *Entrevistas por email e pessoalmente realizadas por Edwin Cordeiro durante o segundo semestre de 2012*. 2012. Não publicadas.

CERF, V. *Vint Cerf Answers Your Questions About IPv6 and More on Slashdot.org*. 2011. Disponível em: <http://interviews.slashdot.org/story/11/10/25/1532213/vint-cerf-answers-your-questions-about-ipv6-and-more>. Acesso em: 26 set. 2012.

CETIC.br / NIC.br. *Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil: TIC Provedores 2011*. 2012. Disponível em: <http://op.ceptro.br/cgi-bin/cetic/tic-provedores-2011.pdf>. Acesso em: 12 mar. 2014.

CETIC.br / NIC.br. *TIC Domicílios e Usuários 2011 - Total Brasil*. 2012. Disponível em: <http://www.cetic.br/usuarios/tic/2011-total-brasil/index.htm>. Acesso em: 8 fev. 2013.

CETIC.br / NIC.br. *TIC Domicílios e TIC Provedores 2012*. 2013. Disponível em: <http://ptt.br/pttforum/7/doc/TICs_Domicilios_e_rovedores2012TT_Forum7.pdf>. Acesso em: 12 mar. 2014.

DUGAN, J. *Software for measuring maximum TCP and UDP bandwidth performance - iperf*. 2011. Disponível em: <http://sourceforge.net/projects/iperf/?source=navbar>. Acesso em: 10 fev. 2013.

GOTTARDI, G. *MAP - Solving IPv6 Deployment and IPv4 Address Exhaustion without Stateful CGN: CKN TechAdvantage Webinar*. 2013. Disponível em: <http://www.slideshare.net/getyourbuildon/map-solving-ipv6-deployment-and-ipv4-address-exhaustion-without-stateful-cgn-ckn-techadvantage-webinar>. Acesso em: 13 mar. 2014.

HORWARD, L. *CGN Costs - Pricing Spreadsheet*. 2012. Disponível em: <http://asgard.org/images/pricing.xls>. Acesso em: 13 mar. 2014.

HORWARD, L. *Internet Access Pricing in a Post-IPv4 Runout World*. 2012. Disponível em: <http://asgard.org/images/pricing_v1.3.docx>. Acesso em: 13 mar. 2014.

HORWARD, L. *Total Cost of Ownership of Carrier-Grade NAT*. 2012. Disponível em: <http://asgard.org/images/TCO_of_CGN.pdf>. Acesso em: 13 mar. 2014.

HORWARD, L. *Total Cost of IPv4-IPv6 Transition*. 2013. Disponível em: <https://ripe67.ripe.net/presentations/188-The_Cost_of_IPv4-IPv6_Transition.pdf>. Acesso em: 13 mar. 2014.

HUSTON, G. *IPv4 Address Report*. 2014. Disponível em: <http://www.potaroo.net/tools/ipv4/>. Acesso em: 12 mar. 2014.

IETF - draft-boucadair-pcp-bittorrent-00. *Behavior of BitTorrent service in PCP-enabled networks with Address Sharing*. 2012. Disponível em: <http://tools.ietf.org/id/draft-boucadair-pcp-bittorrent-00.txt>. Acesso em: 12 mar. 2014.

IETF - draft-cordeiro-experience-mapt-00. *Experience from MAP-T Testing*. 2014. Disponível em: <http://tools.ietf.org/html/draft-cordeiro-experience-mapt-00>. Acesso em: 12 mar. 2014.

IETF - draft-ietf-softwire-map-10. *Mapping of Address and Port with Encapsulation (MAP)*. 2014. Disponível em: <http://tools.ietf.org/html/draft-ietf-softwire-map-10>. Acesso em: 12 mar. 2014.

IETF - draft-ietf-softwire-map-t-05. *Mapping of Address and Port using Translation (MAP-T)*. 2014. Disponível em: <http://tools.ietf.org/html/draft-ietf-softwire-map-t-05>. Acesso em: 12 mar. 2014.

IETF - draft-shirasaki-nat444-06. *NAT444*. 2012. Disponível em: <http://tools.ietf.org/html/draft-shirasaki-nat444-06>. Acesso em: 06 out. 2012.

IETF - Lista de email. *Lista de emails do grupo Softwire do IETF*. 2012. Disponível em: <http://www.ietf.org/mail-archive/web/softwires/current/maillist.html>. Acesso em: 10 nov. 2012.

IETF - RFC 1918. *Address Allocation for Private Internets*. 1996. Disponível em: <http://tools.ietf.org/html/rfc1918>. Acesso em: 06 out. 2012.

IETF - RFC 2529. *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*. 1999. Disponível em: <http://tools.ietf.org/html/rfc2529>. Acesso em: 04 out. 2012.

IETF - RFC 2893. *Transition Mechanisms for IPv6 Hosts and Routers*. 2000. Disponível em: <http://tools.ietf.org/html/rfc2893>. Acesso em: 04 out. 2012.

IETF - RFC 3056. *Connection of IPv6 Domains via IPv4 Clouds*. 2001. Disponível em: <http://tools.ietf.org/html/rfc3056>. Acesso em: 06 out. 2012.

IETF - RFC 3947. *Negotiation of NAT-Traversal in the IKE*. 2005. Disponível em: <http://tools.ietf.org/html/rfc3947>. Acesso em: 13 mar. 2014.

IETF - RFC 4213. *Basic Transition Mechanisms for IPv6 Hosts and Routers*. 2005. Disponível em: <http://tools.ietf.org/html/rfc4213>. Acesso em: 14 set. 2012.

IETF - RFC 4291. *IP Version 6 Addressing Architecture*. 2006. Disponível em: <http://tools.ietf.org/html/rfc4291>. Acesso em: 14 set. 2012.

IETF - RFC 4925. *Softwire Problem Statement*. 2007. Disponível em: <http://tools.ietf.org/html/rfc4925>. Acesso em: 05 out. 2012.

IETF - RFC 5214. *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*. 2008. Disponível em: <http://tools.ietf.org/html/rfc5214>. Acesso em: 05 out. 2012.

IETF - RFC 5969. *IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) – Protocol Specification*. 2010. Disponível em: <http://tools.ietf.org/html/rfc5969>. Acesso em: 14 set. 2012.

IETF - RFC 6144. *Framework for IPv4/IPv6 Translation*. 2011. Disponível em: <http://tools.ietf.org/html/rfc6144>. Acesso em: 06 out. 2012.

IETF - RFC 6145. *IP/ICMP Translation Algorithm*. 2011. Disponível em: <http://tools.ietf.org/html/rfc6145>. Acesso em: 06 out. 2012.

IETF - RFC 6146. *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*. 2011. Disponível em: <http://tools.ietf.org/html/rfc6146>. Acesso em: 05 out. 2012.

IETF - RFC 6333. *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*. 2011. Disponível em: <http://tools.ietf.org/html/rfc6333>. Acesso em: 05 out. 2012.

IETF - RFC 6598. *IANA-Reserved IPv4 Prefix for Shared Address Space*. 2012. Disponível em: <http://tools.ietf.org/html/rfc6598>. Acesso em: 05 out. 2012.

IETF - RFC 6877. *464XLAT: Combination of Stateful and Stateless Translation*. 2013. Disponível em: <http://tools.ietf.org/html/rfc6877>. Acesso em: 12 mar. 2014.

IETF - RFC 6887. *Port Control Protocol (PCP)*. 2013. Disponível em: <http://tools.ietf.org/html/rfc6887>. Acesso em: 13 mar. 2014.

IETF - RFC 6970. *Universal Plug and Play (UPnP) - Internet Gateway Device - Port Control Protocol Interworking Function (IGD-PCP IWF)*. 2013. Disponível em: <http://tools.ietf.org/html/rfc6970>. Acesso em: 13 mar. 2014.

IETF - RFC 791. *Internet Protocol*. 1981. Disponível em: <http://tools.ietf.org/html/rfc791>. Acesso em: 14 set. 2012.

LAW, Y.-N. et al. Empirical Performance of IPv6 vs. IPv4 Under a Dual-Stack Environment. In: *Communications, 2008. ICC '08. IEEE International Conference on*. [S.l.: s.n.], 2008. p. 5924 – 5929.

LENCSE, G.; REPAS, S. Performance analysis and comparison of the TAYGA and of the PF NAT64 implementations. In: *Telecommunications and Signal Processing (TSP), 2013 36th International Conference on*. [S.l.: s.n.], 2013. p. 71–76.

MAENNEL, O. et al. *A Better Approach than Carrier-Grade-NAT*. [S.l.], 2008. Acesso em: 06 out. 2012.

MOREIRAS, A. et al. *IPv6 Básico*. [S.l.]: Núcleo de Informação e Controle do Ponto BR, 2012. Disponível em: <http://ipv6.br/download/>. Acesso em: 28 set. 2012.

NARAYAN, S.; SHANG, P.; FAN, N. Performance Evaluation of IPv4 and IPv6 on Windows Vista and Linux Ubuntu. In: *Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09. International Conference on*. [S.l.: s.n.], 2009. v. 1, p. 653 – 656.

NARAYAN, S.; SHI, Y. Application layer network performance analysis of IPv4 and IPv6 on Windows operating systems. In: *Computers and Devices for Communication, 2009. CODEC 2009. 4th International Conference on*. [S.l.: s.n.], 2009. p. 1 – 4.

NARAYAN, S.; TAUCH, S. IPv4-v6 Transition Mechanisms Network Performance Evaluation on Operating Systems. In: *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*. [S.l.: s.n.], 2010. v. 5, p. 664 – 668.

Pew Internet & American Life Project. *Trend Data (Adults) - What Internet Users do Online*. 2013. Disponível em: <http://www.pewinternet.org/Trend-Data-(Adults)/Online-Activites-Total.aspx>. Acesso em: 8 fev. 2013.

REPAS, S.; HAJAS, T.; LENCSE, G. Application Compatibility of the NAT64 IPv6 Transition Technology. *submetido para 37th International Conference on Telecommunications and Signal Processing (TSP 2014), (Berlin, Alemanha, 2014. Julho, 1-3)*, 2014. Acesso em: 12 mar. 2014.

SASANUS, S.; KAEMARUNGSI, K. Differences in bandwidth requirements of various applications due to IPv6 migration. In: *Information Networking (ICOIN), 2012 International Conference on*. [S.l.: s.n.], 2012. p. 462 – 467. ISSN 1976-7684.

SKOBERNE, N. et al. IPv4 Address Sharing Mechanism Classification and Tradeoff Analysis. *Networking, IEEE/ACM Transactions on*, PP, n. 99, p. 1–1, 2013. ISSN 1063-6692.

UPnP Foum. *UPnP Forum - Standardized DCPs & Certification*. 2011. Disponível em: <http://upnp.org/>. Acesso em: 13 mar. 2014.

WANG, Y.; YE, S.; LI, X. Understanding current IPv6 performance: a measurement study. In: *Computers and Communications, 2005. ISCC 2005. Proceedings. 10th IEEE Symposium on*. [S.l.: s.n.], 2005. p. 71 – 76. ISSN 1530-1346.

WU, P. et al. Transition from IPv4 to IPv6: A State-of-the-Art Survey. *Communications Surveys Tutorials, IEEE*, v. 15, n. 3, p. 1407–1424, Third 2013. ISSN 1553-877X.

WU, Y.; ZHOU, X. Research on the IPv6 performance analysis based on dual-protocol stack and tunnel transition. In: *Computer Science Education (ICCSE), 2011 6th International Conference on*. [S.l.: s.n.], 2011. p. 1091 – 1093.

YUNOS, R.; NOOR, N.; AHMAD, S. Performance evaluation between IPv4 and IPv6 on MPLS Linux platform. In: *Information Retrieval Knowledge Management, (CAMP), 2010 International Conference on*. [S.l.: s.n.], 2010. p. 204 – 208.

ZHU, Y. et al. Stateless Mapping and Multiplexing of IPv4 Addresses in Migration to IPv6 Internet. In: *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*. [S.l.: s.n.], 2008. p. 1 – 5. ISSN 1930-529X.

A Apêndice A: Detalhamento das configurações dos testes

A.1 Equipamentos Utilizados

A figura A.1 apresenta os equipamentos utilizados nos testes.

Figura A.1: Foto dos equipamentos utilizados

Fonte: Elaborado pelo autor

A.2 Configurações do DS-Lite

A figura A.2 apresenta a configuração utilizada no CPE executando DS-Lite.

Figura A.2: Configuração DS-Lite no CPE

```
1  #!/bin/sh
2
3  modprobe ip6_tunnel
4  ip -6 tunnel add dsltun mode ipip6 remote
5    2001:db8:0:2000:: local 2001:db8:0:a::2 dev eth1
6  ip addr add 192.0.0.2 peer 192.0.0.1 dev dsltun
7  ip link set dev dsltun up
8  ip route add default dev dsltun
```

Fonte: Elaborado pelo autor

A figura A.3 apresenta a configuração utilizada no roteador de borda do provedor de acesso a internet executando DS-Lite.

Figura A.3: Configuração DS-Lite no roteador de borda

```
1  #!/bin/sh
2
3  aftr_start() {
4    set -x
5    ip link set tun0 up
6    ip addr add 192.0.0.1 peer 192.0.0.2 dev tun0
7    ip route add 203.0.113.131/32 dev tun0
8    ip -6 addr add fe80::1 dev tun0
9    ip -6 route add 2001:db8:0:2000::/64 dev tun0
10   arp -i eth0 -s 203.0.113.131 0a:0b:0c:0d:0e:f0 pub
11 }
12
13 aftr_stop() {
14   set -x
15   ip link set tun0 down
16 }
17
18 case "$1" in
19 start)
20   aftr_start
21   ;;
22 stop)
23   aftr_stop
24   ;;
25 *)
26   echo "Usage: $0 start|stop"
27   exit 1
28   ;;
29 esac
30 exit 0
```

Fonte: Elaborado pelo autor

A.3 Configurações do 464XLAT

A figura A.4 apresenta a configuração utilizada no CPE (CLAT) executando 464XLAT.

Figura A.4: Configuração 464XLAT no CPE CLAT

```
# nome do tunel
tun-device nat64

# endereco IPv4 do Tayga. Diferente do IPv4 do roteador
ipv4-addr 192.168.2.1

# prefixo NAT46
prefix 2001:db8:ca00:bbbb::/96

# enderecos usados no processamento interno do Tayga
dynamic-pool 192.168.2.0/24
data-dir /tmp

# mapeamento estatico realizado no CLAT
map 192.168.1.10 2001:db8:ca00:aaaa::c0a8:010a
```

Fonte: Elaborado pelo autor

A figura A.5 apresenta o script de inicialização utilizado no CPE (CLAT) executando 464XLAT.

Figura A.5: Script de inicialização do 464XLAT no CPE CLAT

```
#!/bin/sh

tayga --mktun
ip link set nat64 up

ip route add 192.168.2.0/24 dev nat64
ip route add default via 192.168.2.1
ip -6 route add 2001:db8:ca00:aaaa::c0a8:010a dev nat64

echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
```

Fonte: Elaborado pelo autor

A figura A.6 apresenta a configuração utilizada no roteador de borda do provedor de acesso a internet (PLAT) executando 464XLAT.

A figura A.7 apresenta o script de inicialização utilizado no roteador de borda do provedor de acesso a internet (PLAT) executando 464XLAT.

Figura A.6: Configuração 464XLAT no roteador de borda PLAT

```
# nome do tunel
tun-device nat64

# endereco IPv4 do Tayga. Diferente do IPv4 do roteador
ipv4-addr 192.168.255.1

# Prefixo NAT64
prefix 2001:db8:ca00:bbbb::/96

# enderecos usados no processamento interno do Tayga
dynamic-pool 192.168.255.0/24
data-dir /tmp
```

Fonte: Elaborado pelo autor

Figura A.7: Script de inicialização do 464XLAT no roteador de borda PLAT

```
#!/bin/sh
case "$1" in
  start)
    tayga --mktun
    ip link set nat64 up
    ip route add 192.168.255.0/24 dev nat64
    ip -6 route add 2001:db8:ca00:bbbb::/96 dev nat64
    ip -6 route add 2001:db8:ca00:aaaa::/96 via
        2001:db8:ca00:2::2
    iptables -t nat -A POSTROUTING -o eth2 -j MASQUERADE
    iptables -A FORWARD -i eth2 -o nat64 -m state --state
        RELATED,ESTABLISHED -j ACCEPT
    iptables -A FORWARD -i nat64 -o eth2 -j ACCEPT
    echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
    echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
    #inicializacao com debug
    tayga -d -c tayga64.conf
    ;;
  stop)
    ip route del 192.168.255.0/24 dev nat64
    ip -6 route del 2001:db8:ca00:bbbb::/96 dev nat64
    ip -6 route del 2001:db8:ca00:aaaa::/96 via
        2001:db8:ca00:2::2
    ip link set nat64 down
    ip link del nat64
    iptables -t nat -D POSTROUTING -o eth2 -j MASQUERADE
    iptables -D FORWARD -i eth2 -o nat64 -m state --state
        RELATED,ESTABLISHED -j ACCEPT
    iptables -D FORWARD -i nat64 -o eth2 -j ACCEPT
    echo 0 > /proc/sys/net/ipv4/conf/all/forwarding
    echo 0 > /proc/sys/net/ipv6/conf/all/forwarding
    ;;
esac
```

Fonte: Elaborado pelo autor

A.4 Configurações do MAP-E

A figura A.8 apresenta a configuração utilizada no CPE executando MAP-E.

Figura A.8: Configuração MAP-E no CPE

```
1  #!/bin/sh
2
3  ./control stop
4
5  # configure system profile
6  echo 1 > /proc/sys/net/ipv4/ip_forward
7  echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
8  echo 0 > /proc/sys/net/ipv6/conf/eth0/autoconf
9  echo 0 > /proc/sys/net/ipv6/conf/eth2/autoconf
10
11 # configure eth0 -- IPv6 interface
12 ip -6 link set eth0 down
13 ip -6 link set eth0 up
14 ip -6 addr add 2001:db8:6:e001::2/64 dev eth0
15 ip -6 route add default via 2001:db8:6:e001::1 dev eth0
16
17 # configure eth2 -- IPv4 interface
18 ip link set eth2 down
19 ip link set eth2 up
20 ip addr add 192.168.1.1/24 dev eth2
21
22 ./control start
23 ./utils/ivictl -r -d -P 2001:db8:6:d6ff::/64 -E
24 ./utils/ivictl -s -i eth2 -I eth0 -H -a 192.168.1.1/24 -A
       200.0.113.250/29 -P 2001:db8:6:d600::/56 -R 16 -M 2 -o
       0 -c 1400 -E
25
26 service iptables stop
27 service ip6tables stop
```

Fonte: Elaborado pelo autor

A figura A.9 apresenta a configuração utilizada no roteador de borda do provedor de acesso a internet executando MAP-E.

Figura A.9: Configuração MAP-E no roteador de borda

```
1  #!/bin/sh
2  ./control stop
3  # configure system profile
4  echo 1 > /proc/sys/net/ipv4/ip_forward
5  echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
6  echo 0 > /proc/sys/net/ipv6/conf/eth0/autoconf
7  echo 0 > /proc/sys/net/ipv6/conf/eth1/autoconf
8  echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
9  echo 0 > /proc/sys/net/ipv4/conf/eth1/rp_filter
10 # configure eth0 -- IPv6 interface
11 ip link set eth0 down
12 ip link set eth0 up
13 ip -6 addr add 2001:db8:6:e000::2/64 dev eth0
14 ip -6 route add 2001:db8:6:d600::/56 via 2001:db8:6:e000::1
       dev eth0
15 # configure eth1 -- IPv4 interface
16 ip link set eth1 down
17 ip link set eth1 up
18 ip addr add 192.0.2.171/27 dev eth1
19 ip -6 addr flush dev eth1
20 ip route add default via 192.0.2.161 dev eth1
21 ip -6 route add default via 2001:12ff:6:e000::1
22
23 ./control start
24 ./utils/ivictl -r -p 200.0.113.248/29 -P
       2001:db8:6:d600::/56 -R 16 -M 2 -b 0 -E
25 ./utils/ivictl -r -d -P 2001:db8:6:d6ff::/64
26 ./utils/ivictl -s -i eth1 -I eth0 -c 1400
27 service iptables stop
28 service ip6tables stop
```

Fonte: Elaborado pelo autor

A.5 Configurações do MAP-T

A figura A.10 apresenta a configuração utilizada no CPE executando MAP-T.

Figura A.10: Configuração MAP-T no CPE

```
1  #!/bin/sh
2
3  ./control stop
4
5  # configure system profile
6  echo 1 > /proc/sys/net/ipv4/ip_forward
7  echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
8  echo 0 > /proc/sys/net/ipv6/conf/eth0/autoconf
9  echo 0 > /proc/sys/net/ipv6/conf/eth2/autoconf
10
11 # configure eth0 -- IPv6 interface
12 ip -6 link set eth0 down
13 ip -6 link set eth0 up
14 ip -6 addr add 2001:db8:6:e001::2/64 dev eth0
15 ip -6 route add default via 2001:db8:6:e001::1 dev eth0
16
17 # configure eth2 -- IPv4 interface
18 ip link set eth2 down
19 ip link set eth2 up
20 ip addr add 192.168.1.1/24 dev eth2
21
22 ./control start
23 ./utils/ivictl -r -d -P 2001:db8:6:d6ff::/64 -T
24 ./utils/ivictl -s -i eth2 -I eth0 -H -a 192.168.1.1/24 -A
       200.0.113.250/29 -P 2001:db8:6:d600::/56 -R 16 -M 2 -o
       0 -c 1400 -T
25
26 service iptables stop
27 service ip6tables stop
```

Fonte: Elaborado pelo autor

A figura A.11 apresenta a configuração utilizada no roteador de borda do provedor de acesso a internet executando MAP-T.

Figura A.11: Configuração MAP-T no roteador de borda

```
1  #!/bin/sh
2  ./control stop
3  # configure system profile
4  echo 1 > /proc/sys/net/ipv4/ip_forward
5  echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
6  echo 0 > /proc/sys/net/ipv6/conf/eth0/autoconf
7  echo 0 > /proc/sys/net/ipv6/conf/eth1/autoconf
8  echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
9  echo 0 > /proc/sys/net/ipv4/conf/eth1/rp_filter
10 # configure eth0 -- IPv6 interface
11 ip link set eth0 down
12 ip link set eth0 up
13 ip -6 addr add 2001:db8:6:e000::2/64 dev eth0
14 ip -6 route add 2001:db8:6:d600::/56 via 2001:db8:6:e000::1
       dev eth0
15 # configure eth1 -- IPv4 interface
16 ip link set eth1 down
17 ip link set eth1 up
18 ip addr add 192.0.2.171/27 dev eth1
19 ip -6 addr flush dev eth1
20 ip route add default via 192.0.2.161 dev eth1
21 ip -6 route add default via 2001:db8:6:e000::1
22
23 ./control start
24 ./utils/ivictl -r -p 200.0.113.248/29 -P
       2001:db8:6:d600::/56 -R 16 -M 2 -b 0 -T
25 ./utils/ivictl -r -d -P 2001:db8:6:d6ff::/64
26 ./utils/ivictl -s -i eth1 -I eth0 -c 1400
27 service iptables stop
28 service ip6tables stop
```

Fonte: Elaborado pelo autor