

DEIVIS FERNANDES PIRANI

ANÁLISE DE CAMPO DO DESEMPENHO DE
ACESSOS WEB EM IPv6

CAMPINAS

2013

DEIVIS FERNANDES PIRANI

ANÁLISE DE CAMPO DO DESEMPENHO DE
ACESSOS WEB EM IPv6

Dissertação apresentada como exigência para obtenção do
Título de Mestre em Engenharia Elétrica, ao Programa de
Pós Graduação Stricto Sensu em Engenharia Elétrica,
Pontifícia Universidade Católica de Campinas.

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

CAMPINAS

2013

Ficha Catalográfica
Elaborada pelo Sistema de Bibliotecas e
Informação – SBI – PUC-Campinas

t001.64404 P667a Pirani, Deivis Fernandes.
Análise de campo do desempenho de acessos Web em IPv6 / Deivis
Fernandes Pirani. – Campinas: PUC-Campinas, 2014.
104 p.

Orientador: Marcelo Luís Francisco Abbade.

Dissertação (mestrado) - Pontifícia Universidade Católica de Campinas,
Centro de Ciências Exatas, Ambientais e de Tecnologias, Pós-Graduação
em Engenharia Elétrica.

Inclui bibliografia.

1. Internet. 2. Redes de computadores. 3. TCP/IP (Protocolo de redes
de computação) 4. Teleinformática. 5. Sites da Web. I. Abbade, Marcelo
Luís Francisco. II. Pontifícia Universidade Católica de Campinas. Centro de
Ciências Exatas, Ambientais e de Tecnologias. Pós-Graduação em Enge-
nharia Elétrica. III. Título.

18.ed.CDD – t001.64404

DEIVIS FERNANDES PIRANI

ANÁLISE DE CAMPO DO DESEMPENHO DE ACESSOS
WEB EM IPv6

Dissertação apresentada ao Curso de Mestrado Profissional em Gestão de Redes de Telecomunicações do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas como requisito parcial para obtenção do título de Mestre Profissional em Gestão de Redes de Telecomunicações.

Área de concentração: Gestão de Redes e Serviços

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

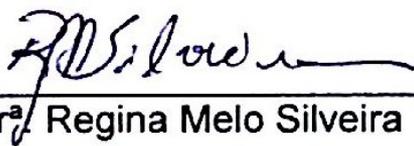
Dissertação apresentada e aprovada em 7 de fevereiro de 2014 pela Comissão Examinadora constituída dos seguintes professores:



Prof. Dr. Marcelo Luís Francisco Abbade
Orientador da Dissertação e Presidente da Comissão Examinadora
Pontifícia Universidade Católica de Campinas



Prof. Dr. Juan Manuel Adan Coello
Pontifícia Universidade Católica de Campinas



Prof.ª Dr.ª Regina Melo Silveira
USP

Dedico este trabalho a minha esposa Livia
e aos meus pais,
a quem tanto amo.

AGRADECIMENTOS

Agradeço primeiramente a Deus por me conceder saúde e perseverança para encarar os desafios aos quais a vida nos remete.

Agradeço a minha esposa querida pela compreensão, carinho e apoio que tanto me ajudaram a concluir este trabalho.

Agradeço aos meus pais por sempre me incentivaram nos estudos, pelo amor e pelos exemplos de honestidade e dignidade dados por eles.

Agradeço ao meu orientador, Prof. Dr. Marcelo Abbade, não só pelo direcionamento deste trabalho mas também pelo aprendizado que tive convivendo com ele nesses dois anos.

Agradeço ao meu amigo e sócio Fernando Siqueira pela compreensão, apoio e por ter mantido, muitas vezes sozinho, nosso “ganha pão” em pleno funcionamento enquanto eu me dedicava a este trabalho.

Agradeço a todos os professores do programa. Foi uma honra ter recebido atenção e ensinamentos de pessoas tão qualificadas.

Agradeço aos amigos da turma pelo companheirismo durante esses dois anos. Todos enfrentamos problemas e dificuldades e a solidariedade de todos sempre esteve a disposição nessas horas.

Agradeço à PUC Campinas pela bolsa de estudos.

RESUMO

Este trabalho apresenta um estudo de campo, comparativo, sobre a utilização dos protocolos IPv4 e IPv6 no acesso a páginas *web*. Foi considerada a perspectiva de um usuário real deste tipo de serviço, no atual período de transição do IPv4 para o IPv6. Para que tal estudo pudesse ser realizado, foi desenvolvido um arranjo no qual três configurações de endereçamento do Protocolo de Internet, IPv4, IPv6 e Pilha Dupla (IPv4+IPv6), foram utilizadas nos acessos às 100 páginas *web*, com suporte ao IPv6, mundialmente mais visitadas. Além disso, foram desenvolvidas uma série de *shell scripts* que possibilitaram mais de 600 acessos simultâneos do IPv4, IPv6 e Pilha Dupla, a cada uma dessas páginas. Tais acessos foram executados de hora em hora, durante o período de um mês, possibilitando a obtenção de mais de 20 GB de informações relativas ao acesso *web*. Os resultados do estudo mostraram que os tempos de carregamento menores obtidos pelo IPv6 e pela Pilha Dupla, estão relacionados com a aquisição parcial do conteúdo. De fato, para o IPv6, o número de páginas *web* com tempos de carregamento menores diminuiu de 57 para 20% quando a média do número de *bytes* obtidos pelo IPv6 e pelo IPv4 é similar. Para a Pilha Dupla, dadas as mesmas condições, o número diminuiu de 25 para 5%. Também foi observado que para 18 das 100 páginas *web* consideradas, nenhum conteúdo foi apresentado ao usuário em mais de 50% dos acessos efetuados. Com relação à preferência pelo IPv6 ao IPv4, na Pilha Dupla, observou-se que 90% da aquisição do conteúdo, de 27 das 100 páginas *web*, ocorreu pelo IPv6.

Palavras-Chave – *IPv6, Pilha Dupla, Acesso Web, Páginas Web, Perspectiva do Usuário, Usuário final, Análise de Campo, Happy Eyeballs.*

ABSTRACT

This paper shows a field-trial investigation comparing the use of IPv4 and IPv6 protocols on web pages access considering the real user perspective and the transition period from IPv4 to IPv6. To perform this study, it was developed a testbed in which three addressing configurations of Internet Protocol, IPv4, IPv6, and Dual Stack (IPv4+IPv6), were used to access the top 100 world most visited web pages with an IPv6 enabled address. In addition, several software tools were developed, that enabled more than 600 simultaneous accesses between IPv4, IPv6 and Dual Stack, to each of these pages. Those accesses were performed every hour during the period of a month, enabling to obtain more than 20 GB of information on the web access. Results showed that lower loading times obtained by IPv6 and Dual Stack are related to the partial acquisition of the content. In fact, for IPv6, the number of web pages with faster loading times goes from 57 to 20% when the average number of bytes obtained by IPv6 and the IPv4 is similar. For Dual Stack the number goes from 25 to 5% given the same conditions. It was also noted that 18 of the 100 pages which were considered, no content would be presented to the user in more than 50% of the performed accesses. Regarding the preference for IPv6 instead of IPv4, on Dual Stack it was observed that 90% of the acquired content for 27 of 100 web pages was made by IPv6.

Key words – *IPv6, Dual Stack, Web Access, Web Pages, User Perspective, End User, Field-trial, Happy Eyeballs.*

LISTA DE FIGURAS

Figura 1. Alterações feitas no cabeçalho do IPv6.....	14
Figura 2. Posicionamento dos cabeçalhos de extensão.....	16
Figura 3. Modelo de camadas TCP/IP com pilha dupla.....	17
Figura 4. Túnel roteador para roteador.....	19
Figura 5. Túnel dispositivo final para roteador.....	19
Figura 6. Túnel dispositivo final para dispositivo final.....	20
Figura 7. Túnel roteador para dispositivo final.....	20
Figura 8. Encapsulamento e desencapsulamento do datagrama IPv6.....	21
Figura 9. Dispositivo tradutor de endereços IP.....	23
Figura 10. Modelo de esgotamento dos blocos de endereços IPv4 nos RIRs (HUSTON, 2013).....	25
Figura 11. Definição das métricas relativas para medidas atípicas.....	36
Figura 12. Visão geral do arranjo.....	39
Figura 13. Esquema de virtualização dos agentes e do Servidor WPT.....	42
Figura 14. Variação do tempo médio de carregamento de cada página web.....	49
Figura 15. Variação do completamento visual de cada página web.....	50
Figura 16. Variação do número de bytes obtidos de cada página web.....	51
Figura 17. Relação com o IPv4 de referencia das medidas atípicas inferiores (a) e superiores (b) para do tempo de carregamento.....	52
Figura 18. Relação das medidas atípicas inferiores (a) e superiores (b) do tempo de carregamento para as 100 páginas avaliadas e relação das medidas atípicas inferiores (c) e superiores (d) do tempo de carregamento para as 23 páginas com média similar do número de bytes obtidos.....	54
Figura 19. Relação com o IPv4 de referência, das medidas atípicas superiores para as páginas web com média de bytes similar.....	55
Figura 20. Tempo de carregamento da página 6.....	56
Figura 21. Número de bytes (a) e consultas DNS (b) da página 6.....	57
Figura 22. Tempo de carregamento (a) e número de bytes obtidos (b) da página 24.....	58
Figura 23. Tempo de carregamento (a) e número de bytes obtidos (b) da página 69.....	60

Figura 24. Relação com o IPv4 de referência, das medidas atípicas inferiores (a) e superiores (b) para o tempo de completamento visual.....	60
Figura 25. Relação das medidas atípicas inferiores (a) e superiores (b) do tempo de completamento visual para as 100 páginas avaliadas e relação das medidas atípicas inferiores (c) e superiores (d) do tempo de completamento visual para as 23 páginas com média similar do número de bytes obtidos.....	62
Figura 26. Número de medidas com tempo de completamento visual igual a zero	63
Figura 27. Relação com o IPv4 de referência, das medidas atípicas inferiores (a) e superiores (b) para o número de bytes.....	65
Figura 28. Número de bytes obtidos pelo IPv4 e pelo IPv6 no agente DS.....	68
Figura 29. Número de bytes obtidos pelo IPv4 e pelo IPv6 no agente DS para páginas com médias semelhantes do número de bytes.....	69
Figura 30. Visão geral da interação entre os scripts desenvolvidos.....	79
Figura 31. Esquema organizacional do Webpagetest.....	88

LISTA DE TABELAS

Tabela 1. Campos do cabeçalho principal do IPv6	15
Tabela 2. Dados do Brasil e dos 10 países com maior número de usuários IPv6.	26
Tabela 3. Especificações de hardware e software do Roteador inter-AS.....	40
Tabela 4. Especificação de hardware e software do Servidor DNS recursivo.....	41
Tabela 5. Especificação de hardware e software do Hospedeiro.....	42
Tabela 6. Especificação dos softwares e do hardware virtual do Servidor WPT...	43
Tabela 7. Especificação dos softwares e do hardware virtual dos agentes.....	44
Tabela 8. Métricas disponibilizadas pelo arranjo desenvolvido.....	47
Tabela 9. Páginas web que tiveram mais de 50% das medidas do tempo para completamento visual com valor igual a zero.....	64
Tabela 10. Páginas web com comportamento atípico para o número de bytes....	67

LISTA DE ABREVIATURAS E SIGLAS

IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
DNS	Domain Name Service
HTTP	Hipertext Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
HTML	Hypertext Markup Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
RTT	Round Trip Time
IETF	Internet Engineering Task Force
GRE	Generic Routing Encapsulation
CPU	Central Processing Unit
RIR	Regional Internet Registry
AS	Autonomous System
IXP	Internet Exchange Point
WPT	Webpagetest
DS	Dual Stack
XML	Extensible Markup Language
HAR	HTTP Archive
CSV	Comma-separeted Values
KB	Kilobyte
MB	Megabyte
CDN	Content Delivery Network
API	Application Programming Interface

SUMÁRIO

1 INTRODUÇÃO.....	1
1.1 Estudos relacionados ao desempenho do IPv6.....	4
1.2 Desempenho das aplicações web quando acessadas pelo IPv6.....	6
1.3 Medição do desempenho das aplicações web acessadas pelo IPv6.....	8
1.4 Objetivos.....	9
1.5 Contribuições.....	9
1.6 Organização da dissertação.....	10
2 PROTOCOLO INTERNET VERSÃO 6.....	12
2.1 Características do IPv6.....	12
2.2 Técnicas de transição.....	16
2.2.1 Pilha Dupla.....	16
2.2.2 Tunelamento.....	18
2.2.3 Tradução.....	22
2.3 Estado atual da implantação.....	24
3 TÉCNICAS PARA MEDIÇÃO DE DESEMPENHO DO IPV6 NA INTERNET.....	29
3.1 Medições baseadas no envio e recebimento de pacotes de dados.....	29
3.2 Medições baseadas no protocolo HTTP.....	31
3.3 Proposta para medição do acesso web efetuado com o IPv6.....	33
4 DESCRIÇÃO DO EXPERIMENTO.....	38
4.1 Arranjo para as medições de campo.....	38
4.2 Processo de medição.....	45
5 RESULTADOS.....	48
5.1 Relação das métricas avaliadas com as páginas web.....	48
5.2 Tempo de carregamento.....	51
5.3 Tempo para completamento visual.....	60
5.4 Número de bytes.....	65
6 CONCLUSÕES.....	70
6.1 Críticas ao método de classificação das medidas.....	72
6.2 Perspectivas para continuidade do trabalho.....	73
TRABALHO PUBLICADO.....	74
REFERÊNCIAS.....	75

APÊNDICE A - Descrição dos programas (scripts) desenvolvidos.....	78
A1 Operação geral dos scripts.....	78
A1.1 Script run_tests.....	80
A1.2 Script get_data.....	82
A1.3 Script filter_data.....	83
A1.4 Script site_aty_calc.....	85
Apêndice B - Plataforma Webpagetest.....	87
ANEXO.....	90

1 INTRODUÇÃO

Desde os anos 90, a comunidade técnica da Internet faz estudos de previsão e propõe soluções para o esgotamento dos endereços do Protocolo Internet versão 4 (*Internet Protocol version 4*, IPv4). Alterações feitas no modo como os endereços IPv4 eram organizados e distribuídos, bem como o uso de técnicas para o compartilhamento desses endereços prolongaram o tempo de utilização do espaço de endereços do IPv4. A solução definitiva foi a criação de um novo protocolo, o Protocolo Internet versão 6 (*Internet Protocol Version 6*, IPv6), que além de otimizar e ampliar as funcionalidades do IPv4, também resolve o problema da falta de endereços IP (HUSTON, 2013).

Um dos maiores desafios na implantação de um novo protocolo de internet é que ele deve ser introduzido em todos os equipamentos que fazem parte dela (HUSTON, 2013). Isso significa que todos os computadores pessoais, servidores, roteadores, *firewalls* e demais dispositivos, que já utilizam o IPv4, devem receber uma atualização ou então serem substituídos para suportar o IPv6. Neste contexto, dada a quantidade de dispositivos presentes na Internet e o fato da administração dos mesmos ser descentralizada, é esperado que a implantação do IPv6 aconteça de forma segmentada e ao longo do tempo (NORDMARK; GILLIGAN, 2005). Sendo assim, em algum ponto do processo de transição existirão dispositivos portando diferentes versões do IP (NORDMARK; GILLIGAN, 2005).

Para manter a compatibilidade entre os dispositivos IPv6 e os IPv4, é necessária a utilização de técnicas de transição. Essas técnicas permitem que datagramas originados em dispositivos IPv6 sejam encaminhados para destinos

IPv4 e vice-versa, e elas também podem ser utilizadas em conjunto, de acordo com a topologia da rede na qual são implementadas. Segundo Waddington e Chang (2002) e Metz (2003) elas podem ser divididas em três categorias, a pilha dupla, o tunelamento e a tradução, que serão abordadas com detalhes na Seção 2.2.

Em muitos casos, além da atualização ou inserção de equipamentos, do uso das técnicas de transição, e da instalação de novos enlaces de comunicação, as redes também necessitam de configurações adicionais de dispositivos de *firewall*, sistemas de detecção de intrusão, sistemas de balanceamento de carga, entre outros (WADDINGTON; CHANG, 2002; WING; YOURTCHENKO, 2012). Nestes casos, além da sobrecarga e complexidade adicionais, introduzida pelos protocolos de transição, falhas nos novos equipamentos e nas suas configurações podem afetar a estabilidade e o desempenho das redes IPv6, e conseqüentemente das aplicações que funcionam sobre elas (WING; YOURTCHENKO, 2012).

De modo geral, o acesso às aplicações na Internet ocorre por meio de uma conexão efetuada a um servidor remoto identificado por um endereço IP. Para descobri-lo é necessário utilizar um sistema de Resolução de Nomes de Domínio (*Domain Name Service*, DNS). Esse sistema recebe como solicitação um nome de dispositivo, no caso o nome do servidor remoto, e envia ao solicitante o endereço IP correspondente. Após este procedimento, o solicitante pode iniciar a comunicação com o servidor da aplicação.

Para as páginas *web*, esse processo ocorre diversas vezes a cada acesso efetuado, pois essas páginas são formadas por conjuntos de objetos como

imagens, textos, vídeos ou até mesmo outras aplicações que podem estar distribuídas em vários servidores. Isso significa que além da diversidade do tipo de conteúdo e do tamanho dos objetos, o acesso às páginas *web* exige diversas interações com o sistema de DNS e o estabelecimento de conexões com um ou vários servidores.

Considerando que tanto as conexões com os servidores remotos como as interações com o sistema de DNS são efetuadas por meio do protocolo IP, um cliente operando com o IPv6 pode estar sujeito aos problemas de desempenho e instabilidades decorrentes da transição do IPv4 para o IPv6. Além disso, sistemas DNS com configurações inadequadas e servidores *web* sem conectividade IPv6 podem fazer com que a experiência do usuário seja afetada pela indisponibilidade total ou parcial da página *web*.

No ano de 2009, a *web* (HTTP) correspondia a 57% de todo o tráfego do maior provedor de acesso à Internet da Europa (MAIER et al, 2009). Nesse mesmo ano Labovitz et al analisaram o tráfego de 110 provedores de acesso à Internet e de provedores de conteúdo, localizados nas Américas, Ásia e Europa. Neles o tráfego HTTP correspondia a 52% do total.

Como as aplicações *web* são as mais utilizadas na Internet (GEBERT et al, 2012), torna-se importante conhecer o seu comportamento quando acessadas por meio de uma estrutura na qual o IPv6 esteja presente. Este tipo de informação pode auxiliar provedores de acesso e de conteúdo na tomada de decisão sobre a implantação ou manutenção do IPv6, bem como pode prover indicadores sobre a eficiência das técnicas utilizadas no período de transição.

1.1 ESTUDOS RELACIONADOS AO DESEMPENHO DO IPV6

A necessidade de informações sobre o comportamento do IPv6 nas diversas partes que compõem um processo de comunicação na Internet, fez com que uma série de trabalhos relacionados ao assunto fossem desenvolvidos. Os estudos são voltados para os sistemas operacionais e aplicações que operam nos dispositivos clientes e servidores e, também, para os enlaces de comunicação, dispositivos e técnicas de transição que operam no núcleo da Internet.

Ao analisarem o desempenho do IPv4 e do IPv6 no Windows 2000 e no Linux, Ahuja e Dendukuri (2006) observaram que para ambos os sistemas operacionais, as transmissões feitas pelo Protocolo de Controle de Transmissão (*Transmission Control Protocol*, TCP) tiveram a taxa de dados média degradada de 3 a 10% com o uso do IPv6. Também neste sentido, porém utilizando cinco versões do sistema operacional Microsoft Windows com IPv4 e IPv6, Narayan et al (2010) observaram que a taxa de dados média do TCP pelo IPv6 foi de 2 a 5% menor do que a do IPv4 para todas as versões do sistema operacional Windows testadas. Observou-se que Ahuja e Dendukuri (2006) e Narayan et al (2010) não mencionaram os algoritmos de controle de congestionamento utilizado pelo TCP nos sistemas operacionais avaliados. Neste caso, a forma pela qual o TCP se recuperaria de possíveis perdas de seguimentos poderia influenciar os resultados obtidos tanto pelo IPv4 quanto pelo IPv6.

Ao fazer estimativas sobre o comportamento de aplicações de voz e vídeo sobre IP, Zhou et al (2006) concluíram, com base em informações de perda e atraso de pacotes IP medidas na Internet, que as diferenças obtidas pela utilização do IPv4 e do IPv6 não influenciariam a qualidade das transmissões de

voz e vídeo, se o IPv6 fosse utilizado. Também avaliando a performance de transmissões de voz sobre IP, porém em redes locais, Yasinovskyy et al (2009) não observaram diferenças significativas de performance ou qualidade da conversação relacionadas ao uso do IPv4 ou do IPv6.

Em estudos de campo, Wu et al (2005) apresentaram resultados de medições feitas no núcleo da Rede Avançada de Ensino e Pesquisa de Taiwan (*Taiwan Advanced Research and Education Network*, TWAREN). A taxa de dados efetiva mais alta obtida pelo Protocolo de Datagrama de Usuário (*User Datagram Protocol*, UDP), operando sobre IPv6, chegou a 94% daquela obtida pelo IPv4, e a do TCP a 98%.

Também por meio de medições de campo originadas na Rede de Ensino e Pesquisa da China (*China Education and Research Network*, CERNET), Wang et al (2005) utilizaram servidores *web* configurados com IPv4 e IPv6 distribuídos por 44 países para observar métricas como conectividade e perda de pacotes. Os resultados mostraram que durante o período de um dia, 85% dos servidores se mantiveram acessíveis via IPv4. Para o IPv6, esta porcentagem variou de 67 a 78%. A taxa média de pacotes perdidos foi de 3% para o IPv6 e 0,7% para o IPv4.

Um estudo proposto por Law et al (2008), utilizou mais de 2.000 dispositivos configurados com pilha dupla e mostrou que o núcleo IPv6 da Internet evoluiu consideravelmente, sendo capaz de proporcionar 95% de conectividade para os locais (*sites*) avaliados no trabalho. Os resultados com relação ao desempenho mostraram que o IPv6 obteve taxas de dados mais elevadas do que aquelas obtidas pelo IPv4, justificadas pela menor utilização dos enlaces IPv6.

A utilização da *web* como fonte de dados para a obtenção de informações sobre o desempenho do IPv6 também tornou-se frequente dada a grande quantidade de servidores *web* distribuídos pelo mundo. O trabalho desenvolvido por Nikkhah et al (2011) utilizou a lista das 1 milhão de páginas *web* mundialmente mais acessadas para analisar diversos aspectos da adoção e do desempenho do IPv6 na Internet. Métricas como conectividade, contagem de saltos até o destino e taxa de dados efetiva no *download* de objetos HTTP, possibilitaram aos autores concluir que a conectividade IPv6 no núcleo da Internet é comparável à do IPv4, e que os menores índices de desempenho para a taxa de dados obtida por meio do IPv6 no *download* dos objetos HTTP são relativos aos caminhos diferentes do IPv4 percorridos pelos pacotes. A mesma conclusão para a taxa de dados efetiva foi obtida por Dhamdhre et al (2012) ao aplicar o mesmo método proposto por Nikkhah et al (2011).

1.2 DESEMPENHO DAS APLICAÇÕES *WEB* QUANDO ACESSADAS PELO IPV6

As informações das páginas e das aplicações *web*, são formatadas e apresentadas no navegador *web* do usuário por meio de uma linguagem de hipertexto conhecida como Linguagem de Marcação de Hipertexto (*Hipertext Markup Language*, HTML). A transferência dessas informações, também conhecidas como recursos ou objetos, é feita de um servidor *web* para o navegador do usuários pelo Protocolo de Transferência de Hipertexto (*Hipertext Transfer Protocol*, HTTP), utilizando conexões TCP/IP. No HTTP, cada objeto é identificado por um Identificador Uniforme de Recurso (*Uniform Resource Identifier*, URI), conhecido também como Localizador Uniforme de Recurso

(*Uniform Resource Locator*, URL), que possibilita a localização do objeto em um servidor remoto (FIELDING et al, 1999). O navegador *web* localiza e transfere os objetos HTTP para o computador cliente, processa as informações HTML e disponibiliza o conteúdo ao usuário final.

As páginas *web* modernas são formadas por um conjunto de objetos HTTP que podem estar distribuídos em diversos servidores em uma rede local ou na Internet. Para acessá-los, os sistemas clientes necessitam interagir diversas vezes com o Sistema de Nomes de Domínio (*Domain Name System*, DNS) para obter os endereços IP desses servidores. Logo após, conexões TCP são estabelecidas possibilitando o *download* dos objetos HTTP.

Tanto as consultas DNS quanto o estabelecimento das conexões TCP dependem de fatores da rede como o Tempo de Ida e Volta (*Round Trip Time*, RTT) dos pacotes IP, bem como de características relacionadas ao *hardware* e ao *software* dos sistemas finais. Para o caso específico das páginas *web*, o estudo feito por Meenan (2013), mostra que o tempo de carregamento delas diminui conforme o RTT fica menor. Em Sundaresan et al (2013), os fatores de degradação de performance dominantes, no acesso a páginas *web*, são atribuídos ao tempo de consulta DNS e ao estabelecimento das conexões TCP.

Além disso, problemas de conectividade podem implicar em um aumento do tempo de carregamento dos objetos HTTP de uma página *web*, ou até mesmo na indisponibilidade do conteúdo. Tais problemas podem estar relacionados com o funcionamento da rede ou, também, com a configuração incorreta dos servidores *web*, DNS, *firewalls*, dentre outros. Páginas *web* parcialmente disponibilizadas em IPv6 podem fazer com que os navegadores *web* executem

processos adicionais de estabelecimento de conexões TCP se o sistema operacional estiver configurado com IPv4 e IPv6, aumentando o tempo de carregamento da página (WING; YOURTCHENKO, 2012). Caso o cliente tenha apenas o IPv6 configurado, somente o conteúdo parcialmente disponibilizado em IPv6 será carregado.

1.3 MEDIÇÃO DO DESEMPENHO DAS APLICAÇÕES WEB ACESSADAS PELO IPV6

Para que informações de desempenho e do comportamento do acesso às aplicações *web*, efetuados pelo IPv6, sejam relevantes para provedores de acesso, de conteúdo e para os usuários finais, é necessário que elas sejam extraídas da Internet pois é neste ambiente que o IPv6 pode influenciar as dinâmicas do acesso *web*, conforme descrito na Seção 1.2. Sendo assim, uma técnica apropriada para a obtenção dessas informações são as medições ativas de campo de acesso a páginas *web* reais na Internet.

Considerando, ainda, que a influência do período de transição do IP pode afetar as dinâmicas de carregamento das páginas *web* nos aspectos do desempenho e da disponibilidade do conteúdo, as informações obtidas pelas medições devem contemplar métricas para a avaliação nesses dois sentidos. Com relação ao desempenho, as possíveis variáveis associadas, como a taxa de dados efetiva dos protocolos de transporte e aplicação, o tempo para o estabelecimento de conexões TCP, tempo de consulta DNS e o RTT influenciam, conseqüentemente, o tempo de carregamento dos objetos HTTP da página. No caso da indisponibilidade do conteúdo, seja pela implementação parcial do IPv6 nos servidores ou por problemas de configuração de DNS, *firewall*, etc., a

quantidade de objetos HTTP e o número de *bytes* recebidos da página *web* podem ser comprometidos.

Tanto o desempenho quanto a indisponibilidade do conteúdo podem, juntos ou isoladamente, influenciar a experiência do usuário no acesso a páginas *web*. Mais especificamente, os usuários podem experimentar intervalos de tempo maiores na apresentação de partes da página ou no carregamento dela por completo ou, até mesmo, deixar de visualizar determinados conteúdos que estejam disponíveis apenas por meio do IPv4.

1.4 OBJETIVOS

O objetivo deste trabalho é desenvolver um estudo de campo comparando o desempenho de acessos *web* em IPv6 com o desempenho de acessos *web* em IPv4 e, sempre que possível, efetuar investigações para identificar a causa de possíveis impactos negativos que a utilização IPv6 possa vir a causar nestes acessos. Além disso, o trabalho objetiva o desenvolvimento de um arranjo e de programas que possibilitem a aquisição automatizada de informações relativas ao acesso *web*.

1.5 CONTRIBUIÇÕES

As contribuições proporcionadas por este estudo relacionam-se com o arranjo e com as programas em *shell script* desenvolvidos para a aquisição de dados relativos ao acesso *web*, bem como com as análises dos resultados obtidos pelas medições executadas. O arranjo proporciona uma forma de aquisição de informações do acesso *web* voltadas não apenas para o desempenho da rede, mas também das aplicações e da experiência dos usuários

na visualização das páginas *web*. Os resultados obtidos pelas medições avaliam, de forma comparativa ao IPv4, o desempenho dessas métricas considerando a utilização do IPv6.

Sendo assim, uma vez que as páginas *web* avaliadas sejam utilizadas pelos usuários de um determinado provedor de acesso à Internet, ele poderá utilizar os resultados das avaliações como indicadores de apoio à tomada de decisão sobre a implantação do IPv6 para esses usuários. Além disso, esses provedores podem utilizar o arranjo desenvolvido neste trabalho, bem como o método de comparação com o IPv4 proposto, na avaliação do acesso *web* executado por meio de sua própria estrutura IPv6, para aquelas páginas *web* que lhe convêm. Para os provedores de conteúdo, os resultados podem indicar possíveis problemas relacionados ao desempenho da implantação do IPv6 nos Centros de Dados (*Datacenters*) e servidores HTTP, enlaces de comunicação ou até mesmo problemas de configuração em seus equipamentos.

1.6 ORGANIZAÇÃO DA DISSERTAÇÃO

O Capítulo 2 apresenta conceitos básicos sobre o IPv6 e sobre técnicas de transição utilizadas para interoperar dispositivos IPv4 com IPv6 e vice-versa. Também no Capítulo 2, é mostrado um panorama geral do estado atual da implantação do IPv6 na Internet.

O Capítulo 3 mostra as principais técnicas utilizadas para avaliar o desempenho do IPv6 na Internet e os motivos pelos quais elas não se mostram suficientes para medir o desempenho do IPv6 no acesso às aplicações e páginas

web. Ainda no Capítulo 3 é apresentada a proposta para medição do comportamento das aplicações *web* quando acessadas pelo IPv6.

No Capítulo 4 são descritos os recursos de *hardware* e *software* utilizados nos experimentos deste trabalho. Além disso, são descritos os processos envolvidos nas medições efetuadas e as métricas observadas pelo método de medição proposto.

O Capítulo 5 mostra os resultados com relação ao estudo comparativo do IPv4 e do IPv6 no acesso *web*. Esses resultados se referem à análise dos dados de três métricas que foram obtidos pelas medições executadas às 100 páginas *web* mundialmente mais visitadas.

Por fim, o Capítulo 6 apresenta as conclusões deste trabalho mediante a análise dos principais resultados obtidos. Também neste Capítulo, são mostradas as limitações e as possibilidades para continuação deste trabalho.

2 PROTOCOLO INTERNET VERSÃO 6

Neste capítulo as principais características do IPv6 serão apresentadas na Seção 2.1. A Seção 2.2 abordará as técnicas mais relevantes utilizadas no processo de transição do IPv4 para o IPv6 e que podem influenciar a qualidade e o desempenho das aplicações *web* na Internet. A Seção 2.3 apresentará um quadro geral do estado de implantação do IPv6 na Internet.

2.1 CARACTERÍSTICAS DO IPV6

O IPv6 foi desenvolvido pela Força Tarefa de Engenharia da Internet (*Internet Engineering Task Force*, IETF) para ser o sucessor do IPv4. As principais modificações feitas com relação ao IPv4 podem ser categorizadas em cinco grupos (DEERING; HINDEN, 1998): Expansão da capacidade de endereçamento, simplificação no formato do cabeçalho, otimização do uso de campos opcionais, capacidade de prover fluxos baseados em rótulos e autenticação e privacidade.

Os campos de endereços de origem e destino foram aumentados em 96 *bits* com relação ao IPv4, disponibilizando um espaço de 128 *bits* para endereçamento. Esta característica do IPv6 resolve o problema da falta de endereços IP pelo qual a Internet está passando e por este motivo, torna-se uma das características mais importantes do IPv6.

Os campos do cabeçalho IPv6 foram simplificados proporcionando um cabeçalho de tamanho fixo, mais simples e eficiente com relação aos recursos computacionais utilizados para o seu processamento. Algumas funcionalidades providas por campos do IPv4 removidos no IPv6, são disponibilizados por meio de

cabeçalhos de extensão. Esta característica permite, além da simplificação do cabeçalho principal, a expansão das funcionalidades do IPv6 pela criação de novos cabeçalhos de extensão.

Assim como o IPv4, o IPv6 permite aos sistemas finais e roteadores intermediários, a identificação de datagramas que necessitam de tratamento especial de encaminhamento. Essa característica mantém para o IPv6 a compatibilidade com as classes de serviço já utilizadas nas redes IPv4. Além disso, o IPv6 possui o campo Rótulo de Fluxo que permite a marcação e diferenciação de datagramas para serviços que não se enquadram nas classes de serviços contempladas pelo campo Classe de tráfego.

Funções de autenticação e privacidade, que no IPv4 só eram possíveis com a utilização de protocolos auxiliares, foram incorporadas ao IPv6 por meio dos cabeçalhos de extensão. Essas funcionalidades são opcionais tanto para uso como para implementação na pilha TCP/IP dos dispositivos que suportam o IPv6.

O cabeçalho base do IPv6 possui oito campos principais (DEERING; HINDEN, 1998), ilustrados de forma comparativa com o do IPv4 pela Figura 1. Na Tabela 1, são mostradas as funções de cada campo do IPv6, bem como a quantidade de *bits* ocupados por eles no cabeçalho.

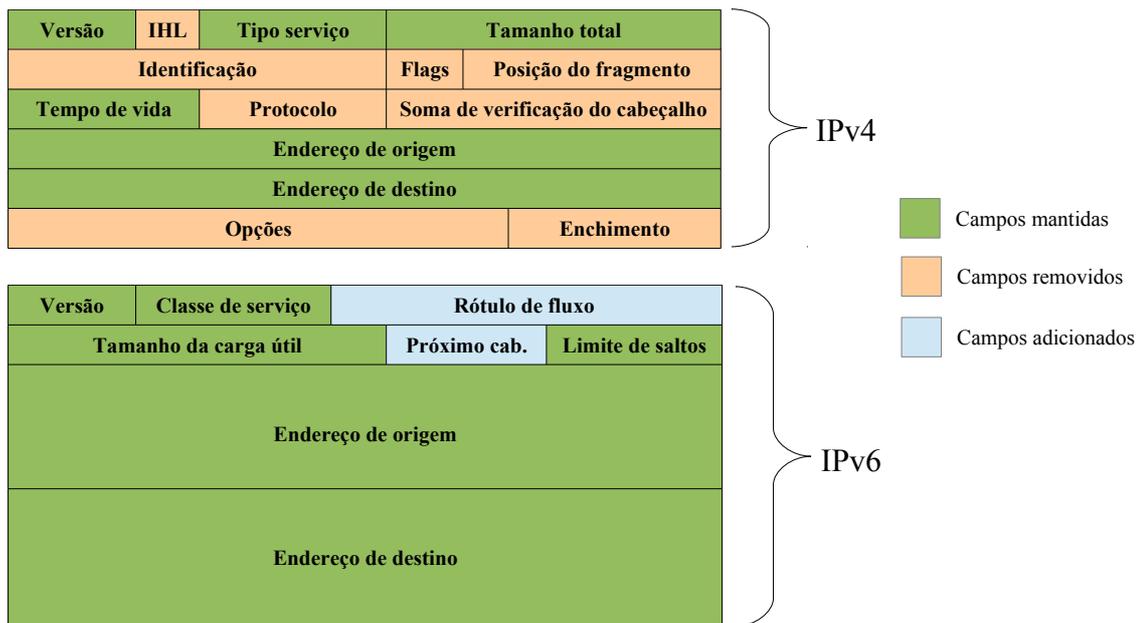


Figura 1. Alterações feitas no cabeçalho do IPv6

Observa-se que mesmo com um espaço de endereçamento quatro vezes maior do que o de seu antecessor, o protocolo IPv6 possui um cabeçalho base com tamanho total de 320 *bits*, correspondendo a menos do que o dobro do tamanho do cabeçalho IPv4. Isto foi possível com a remoção de campos que no IPv4 eram opcionais (DEERING; HINDEN, 1998).

Tabela 1. Campos do cabeçalho principal do IPv6

Campo	Tamanho	Função
Versão	4 bits	Identifica a versão do protocolo IP, no caso preenchido com o número 6.
Classe de tráfego	8 bits	Permite a dispositivos finais e também a roteadores, a diferenciação de classes e prioridades a que determinados datagramas IPs possam pertencer.
Rótulo de fluxo	20 bits	Pode ser utilizado pelo dispositivo IP de origem para identificar datagramas que precisam de um tratamento especial não especificado pelas classes de qualidade de serviço.
Tamanho da carga útil	16 bits	Tamanho dos dados que o datagrama IP está transportando, descontado o cabeçalho base. Cabeçalhos de extensão são considerados como carga útil.
Próximo cabeçalho	8 bits	Identifica o tipo de cabeçalho de extensão que vem imediatamente após o cabeçalho base.
Limite de saltos	8 bits	Identifica a quantidade máxima de enlaces que um datagrama pode atravessar sendo decrementado de um em um pelos roteadores pelos quais o datagrama for encaminhado. Se o valor 0 for alcançado, o datagrama é descartado.
Endereço de origem	128 bits	Endereço do dispositivo IP que originou o datagrama.
Endereço de destino	128 bits	Endereço do dispositivo IP para o qual o pacote deve ser entregue.

Informações e funcionalidades opcionais da camada de roteamento, no IPv6, são disponibilizados por meio de cabeçalhos de extensão. Eles são inseridos entre o cabeçalho principal e o cabeçalho do protocolo da camada superior, conforme ilustrado pela Figura 2. Os cabeçalhos de extensão padronizados são: *Cabeçalho de Opções Salto-a-Salto*, *Cabeçalho de Opções de Destino*, *Cabeçalho de Roteamento*, *Cabeçalho de Fragmento*, *Cabeçalho de Autenticação* e *Cabeçalho de Encapsulamento de Conteúdo Seguro*.

Cabeçalho base IPv6 Próximo cabeçalho: Roteamento	Cabeçalho roteamento Próximo cabeçalho: Fragmento	Cabeçalho fragmento Próximo cabeçalho: TCP	Cabeçalho TCP + Dados...
---	---	--	-----------------------------

Figura 2. Posicionamento dos cabeçalhos de extensão

Esses cabeçalhos não são processados nos roteadores intermediários, com exceção do *Cabeçalho de Opções Salto-a-Salto* (DEERING; HINDEN, 1998). Exemplos da utilização do *Cabeçalho de Opções Salto-a-Salto* podem ser vistos nos protocolos padronizados em (DEERING; FENNER, 1999) e (PARTRIDGE; JACKSON, 1999).

2.2 TÉCNICAS DE TRANSIÇÃO

Os protocolos IPv4 e IPv6 não são nativamente compatíveis. Dispositivos portando somente a versão 4 do protocolo são incapazes de se comunicar diretamente com dispositivos que possuam apenas a versão 6. Desta forma, para evitar problemas de conectividade entre esses dispositivos é necessária a utilização de técnicas de transição que permitam a coexistência dos dois protocolos. Essas técnicas são divididas em três categorias, a pilha dupla, o tunelamento e a tradução (WADDINGTON; CHANG, 2002; METZ, 2003).

2.2.1 PILHA DUPLA

A técnica de transição de pilha dupla, discutida a seguir, consiste em capacitar um dispositivo de rede para suportar as duas versões do protocolo IP. Isto significa que um dispositivo operando com pilha dupla possui uma implementação completa das duas versões do protocolo IP, sendo capaz de enviar e receber datagramas IPv4 e IPv6. Este tipo de técnica pode ser visto

como a forma mais direta de se manter a compatibilidade de novos dispositivos IPv6 com a atual infraestrutura IPv4 (NORDMARK; GILLIGAN, 2005).

A Figura 3 ilustra a pilha de protocolos TCP/IP com uma implementação da pilha dupla. Observa-se que as camadas superiores e inferiores à camada de rede não necessitam de nenhuma alteração para suportar as duas versões do protocolo IP.

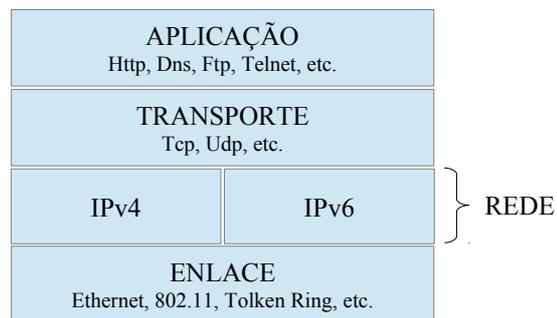


Figura 3. Modelo de camadas TCP/IP com pilha dupla

Um dispositivo de rede que possui a pilha dupla implementada não necessariamente possuirá um endereço IPv4 e outro IPv6, isto significa que uma versão ou outra do protocolo pode ser desativada por questões administrativas ou operacionais. Nestes casos, dispositivos com a pilha IPv6 desativada irão funcionar exatamente como dispositivos que possuam apenas a implementação da pilha IPv4, e vice-versa. É importante notar que as aplicações em execução nos dispositivos com pilha dupla podem optar pela versão do protocolo IP que irão utilizar (NORDMARK; GILLIGAN, 2005).

Ao se utilizar a pilha dupla, deve ser considerado que os mecanismos de resolução de nomes de domínios (*Domain Name Service*, DNS) também devem estar aptos em responder às solicitações DNS com registros do tipo AAAA. Os

registros DNS são unidades de informação do protocolo DNS utilizadas para transportar repostas às consultas feitas pelos clientes. Em específico, registros AAAA informam ao solicitante o endereço IPv6 de destino solicitado.

2.2.2 TUNELAMENTO

Túneis são canais virtuais de comunicação que permitem o encapsulamento de um protocolo sobre outro. As técnicas de tunelamento, discutidas a seguir, objetivam encapsular datagramas IPv6 por meio da estrutura IPv4 já existente ou vice-versa. No caso da transição do IPv4 para o IPv6, este tipo de prática pode ser utilizada em redes que não possuam estrutura de roteamento IPv6 operacional ou conectividade IPv6 com outras redes ou mesmo com a Internet. Considerando que na maioria dos cenários a estrutura IPv6 é implementada de forma gradativa, as técnicas de tunelamento são amplamente utilizadas para iniciar o processo até que uma estrutura IPv6, nativa, esteja disponível (NORDMARK; GILLIGAN, 2005).

Os túneis podem ser utilizados para interconectar regiões específicas de uma rede ou da Internet, ou até mesmo conectar dispositivos diretamente, utilizando a estrutura de roteamento IPv4 já existente. Isto pode ser feito nos seguintes formatos (NORDMARK; GILLIGAN, 2005).

1. *Roteador para roteador*: um túnel é configurado entre dois roteadores permitindo o encaminhamento de datagramas IPv6 entre eles. Esta abordagem pode ser utilizada para interconectar redes IPv6 por meio da infraestrutura IPv4, conforme mostrado na Figura 4.

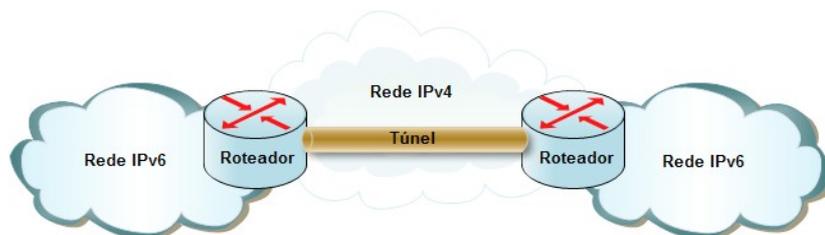


Figura 4. Túnel roteador para roteador

2. *Dispositivo final para roteador*: o túnel é configurado entre um dispositivo final e um roteador intermediário alcançável por meio da estrutura IPv4 e que possua conectividade com a rede IPv6. O dispositivo final pode ser uma estação, um servidor, ou qualquer outro dispositivo que tenha a necessidade de acessar um endereço IPv6 remoto.

Como exemplo, a Figura 5 apresenta uma estação de trabalho IPv4 que necessita de acesso a dispositivos na Internet IPv6. A estação em questão não possui conectividade com uma rede IPv6 e, portanto, precisa conectar-se ao roteador por meio de um túnel IPv6 sobre IPv4.

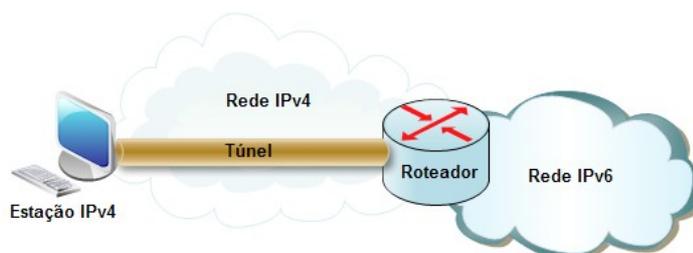


Figura 5. Túnel dispositivo final para roteador

3. *Dispositivo final para dispositivo final*: um túnel é configurado entre dois sistemas finais, permitindo que eles se comuniquem via IPv6 sobre a estrutura IPv4 existente. Neste caso, o túnel abrange todo caminho fim-a-fim entre os dispositivos.

Para ilustrar esta situação, a Figura 6 mostra uma estação de trabalho IPv6 que precisa acessar, pela Internet IPv4, um recurso localizado em um servidor remoto que possui apenas endereçamento IPv6. Neste exemplo específico, os dois dispositivos precisam apenas de uma comunicação direta entre si, não havendo a necessidade de se comunicar com outros dispositivos.



Figura 6. Túnel dispositivo final para dispositivo final

4. *Roteador para dispositivo final*: este tipo de túnel permite que roteadores intermediários encaminhem, por meio da estrutura IPv4 existente, datagramas IPv6 diretamente para um dispositivo final. Este modelo é bastante parecido com o modelo *Dispositivo final para roteador* porém, neste caso, o fluxo da comunicação se dá de um dispositivo dotado de acesso à rede IPv6 para um servidor remoto sem acesso a ela, conforme ilustrado na Figura 7.

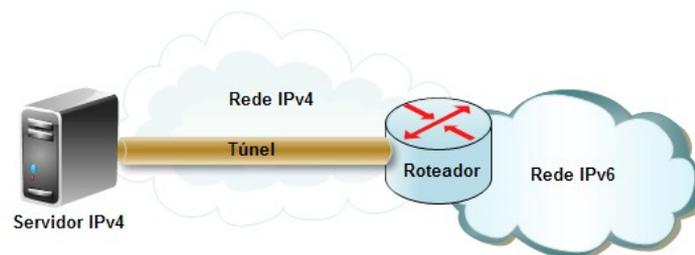


Figura 7. Túnel roteador para dispositivo final

Independente do modelo de túnel utilizado, ou até mesmo dos protocolos disponíveis para tal, existem mecanismos fundamentais que promovem o

funcionamento deste tipo de técnica. O dispositivo de entrada do túnel, chamado de encapsulador, deve criar o cabeçalho de encapsulamento e transmitir o datagrama IP pelo túnel. No dispositivo de saída do túnel, o cabeçalho de encapsulamento deve ser removido e o datagrama IP processado normalmente.

A Figura 8 ilustra o encapsulamento e desencapsulamento de um datagrama IPv6 transmitido por um túnel do tipo IPv6 sobre IPv4. Neste tipo de túnel, o valor do campo “protocolo” do cabeçalho IPv4 inserido no processo de encapsulamento deve ser preenchido com o valor “41”, indicando que a carga útil do datagrama IPv4 é um datagrama IPv6 (NORDMARK; GILLIGAN, 2005).

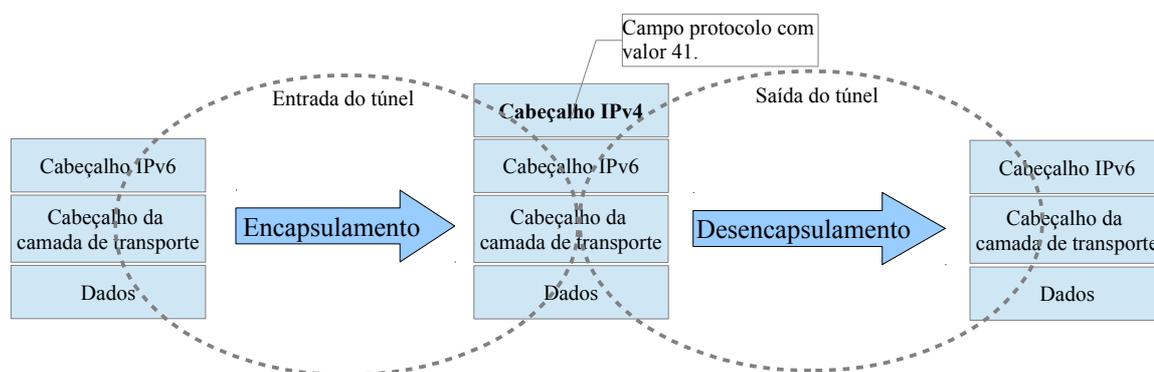


Figura 8. Encapsulamento e desencapsulamento do datagrama IPv6

As técnicas de tunelamento podem ser classificadas como estáticas ou dinâmicas, de acordo com o processo pelo qual o túnel é estabelecido. Túneis estáticos são aqueles configurados manualmente em ambas as extremidades, sejam elas roteadores ou dispositivos finais. Os túneis 6over4 (NORDMARK; GILLIGAN, 2005) e túneis GRE (FARINACCI et al, 2000), são exemplos de túneis estáticos que necessitam de configuração manual nas duas extremidades.

Os túneis dinâmicos são aqueles estabelecidos de forma automática pela atuação de protocolos especificamente voltados para esta função, não havendo a

necessidade da intervenção manual para a configuração das extremidades. Em muitos casos, esse tipo de túnel é utilizado por provedores de acesso à Internet para disponibilizar acesso à Internet IPv6, por meio de um *software* cliente que faz o estabelecimento do túnel com um servidor remoto. Exemplos de protocolos que utilizam o estabelecimento dinâmico do túnel são o Teredo (HUITEMA, 2006) e o *Tunnel Broker* (DURAND et al, 2001).

Por fim, as técnicas e protocolos de tunelamento podem ou não manter informações de estado dos túneis estabelecidos. Técnicas que necessitam manter estado dos endereços IP ou dos pacotes transmitidos, utilizam mais recursos de CPU e memória dos dispositivos e, em muitos casos, podem não ser escaláveis. De um modo geral, técnicas que não utilizam informações de estado são preferíveis, uma vez que possuem melhor desempenho tornando-se mais escaláveis.

2.2.3 TRADUÇÃO

As técnicas de transição de pilha dupla e tunelamento abordadas respectivamente em 2.2.1 e 2.2.2, consideram um ambiente de transição no qual os dispositivos de rede possuem conectividade IPv4 e precisam se comunicar com dispositivos IPv6 ou IPv4/IPv6. Nestes casos, a atribuição de um endereço IPv4 é explicitamente necessária, o que pode vir a ser um problema dada a atual escassez desse tipo de endereçamento. Sendo assim, são esperados casos em que dispositivos dotados apenas de conectividade IPv6 necessitem acessar serviços em redes apenas IPv4 (NORDMARK; GILLIGAN, 2000; LI et al, 2011).

As técnicas de transição baseadas em tradução de endereços possibilitam a conectividade de dispositivos somente IPv6 com dispositivos somente IPv4 e vice-versa. Isto é feito com a adição de um elemento de tradução posicionado na fronteira entre a rede IPv6 e a rede IPv4, conforme ilustrado pela Figura 9. Este dispositivo faz, de acordo com o sentido da comunicação, o mapeamento dos campos do cabeçalho IPv6 em um cabeçalho IPv4 ou vice-versa, bem como a adequação dos endereços de origem e destino (NORDMARK; GILLIGAN, 2000; LI et al, 2011).

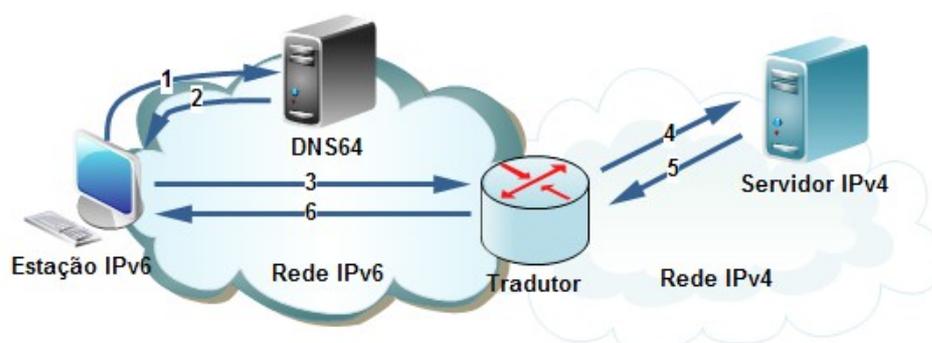


Figura 9. Dispositivo tradutor de endereços IP

Para que o mecanismo de tradução funcione, é necessária a utilização de um servidor DNS capaz de entregar à estação solicitante um endereço de destino IPv6, mesmo que o servidor remoto tenha apenas um endereço IPv4 configurado no DNS. Para isso, o servidor DNS em questão deve implementar algum protocolo como, por exemplo, o DNS64 (BAGNULO et al, 2011) que o habilite a compor mensagens DNS de resposta, com endereços de destino IPv6, baseados nas informações de endereçamento IPv4 contidas no banco de dados do DNS. A composição do endereço IPv6 de resposta, no caso do DNS64, é feita pelos mecanismos descritos por Bao et al (2010), que especificam como representar um endereço IPv4 em um endereço IPv6.

Depois de receber o endereço de destino do DNS64 (passos 1 e 2 na Figura 9), a estação IPv6 inicia o processo de conexão com o servidor de destino (passo 3). Neste ponto, o tradutor deve converter a solicitação feita em IPv6 para IPv4 (passo 4) e então encaminhá-la ao servidor de destino. A seleção do endereço IPv4 que irá representar a estação IPv6 pode ser feita de diversas formas, dependendo do protocolo de tradução utilizado. Esses protocolos também podem ou não manter informações de estado das conexões em curso (BAO et, 2010). Quando a resposta IPv4 vinda do servidor passar pelo tradutor (passo 5) ele deve traduzi-la de volta para o IPv6 e encaminhá-la para a estação que originou a comunicação, finalizando o processo (passo 6 da Figura 9).

Assim como as técnicas de tunelamento, os protocolos de tradução que mantêm informações de estado das comunicações em curso tendem a consumir mais recursos computacionais dos dispositivos de rede, introduzindo sobrecarga adicional ao processo de comunicação. Por outro lado, as técnicas de tradução que não mantêm informações de estado e que são mais eficientes do ponto de vista computacional, podem não oferecer um nível suficiente de compartilhamento dos endereços IPv4 disponíveis.

2.3 ESTADO ATUAL DA IMPLANTAÇÃO

O processo de implantação do IPv6 deveria ocorrer em tempo hábil antes do esgotamento do IPv4. De modo geral, os sistemas operacionais que funcionam nos dispositivos finais possuem suporte ao IPv6 já há algum tempo. Estima-se que 50% de todos os dispositivos conectados à Internet possuem suporte ao IPv6, porém a rede e dispositivos intermediários, responsáveis por conectá-los à

Internet não seguiram o mesmo caminho. Como resultado, o crescimento rápido do IPv6 não aconteceu à medida como era esperado e a implantação do novo protocolo vem acontecendo de forma tímida, mediante a velocidade com que o espaço de endereçamento IPv4 está se esgotando (HUSTON, 2013).

Os Registros Regionais da Internet (*Regional Internet Registry*, RIR) são responsáveis por coordenar a distribuição dos endereços IP em suas respectivas regiões. A Figura 10 (HUSTON, 2013) mostra um modelo previsto do esgotamento dos blocos IPv4, medidos em quantidades de prefixos “/8” remanescentes nos RIRs. É possível observar que alguns deles já esgotaram seus estoques de endereços IPv4.

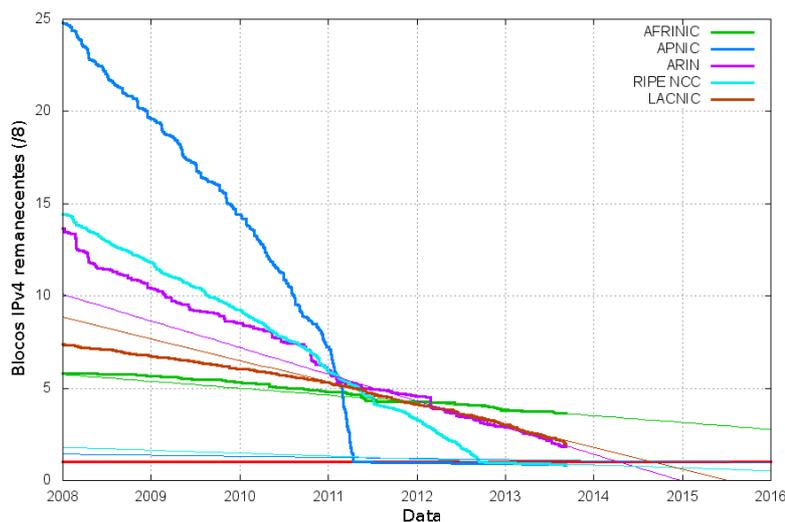


Figura 10. Modelo de esgotamento dos blocos de endereços IPv4 nos RIRs (HUSTON, 2013)

A adoção do IPv6 pelos usuários finais da Internet chega a 1,19 % do total mundial segundo APNIC (2013). Nas estatísticas apresentadas por GOOGLE, (2013), essa porcentagem é de 1,92%. A Tabela 2 apresenta a porcentagem desses usuários para os 10 países com maior adoção e também para o Brasil (APNIC, 2013). Observa-se que os índices são consideravelmente baixos se

comparados com a quantidade total dos usuários que já utilizam o IPv4. Segundo Huston (2013) , esses índices são atribuídos ao fato de que apenas uma pequena parcela dos provedores de acesso se mostram atuantes no oferecimento do IPv6 a seus clientes.

Tabela 2. Dados do Brasil e dos 10 países com maior número de usuários IPv6

POSIÇÃO	PAÍS	USUÁRIOS INTERNET	% USUÁRIOS COM IPV6
1	Romênia	8.650.698	10,59 %
2	Luxemburgo	471.571	9,27 %
3	Suíça	6.463.969	7,81 %
4	França	50.288.459	5,63 %
5	Japão	100.667.128	4,63 %
6	Alemanha	67.917.826	4,52 %
7	EUA	250.426.508	4,26 %
8	Bélgica	8.495.919	4,19 %
9	Butão	101.125	3,88 %
10	Peru	10.585.308	3,45 %
69	Brasil	88.032.091	0,02 %

Os Sistemas Autônomos (*Autonomous Systems, AS*) da Internet são entidades que possuem um conjunto de roteadores sob uma administração técnica centralizada. Os AS utilizam métricas comuns e um protocolo de roteamento interno para encaminhar pacotes pela rede. Comunicam-se com outros AS por meio de um protocolo de roteamento externo, pelo qual anunciam seus blocos IP para a Internet (HAWKINSON; BATES, 1996).

A adoção do IPv6 pelos AS é o primeiro passo para que exista conectividade entre sistemas finais por meio deste protocolo. Neste aspecto, segundo Dhamdhere et al (2012) cerca de 11% dos AS mundiais anunciavam blocos IPv6 em 2012. Entre esses AS, os enlaces de comunicação IPv6 correspondiam a 13% dos enlaces IPv4, também no ano de 2012. O mesmo estudo mostra, ainda, que a partir de 2007 o modelo de crescimento dos AS anunciando prefixos de rede IPv6 e dos enlaces de comunicação IPv6, passou de

linear para exponencial saltando, respectivamente, de pouco mais de 500 AS em 2007 para cerca de 4500 em 2012 e de 2000 para cerca de 16000 enlaces no mesmo período. Em 2013 a porcentagem de AS anunciando prefixos IPv6 na Internet corresponde a 16% dos AS mundiais (LABER, 2013; RIPE, 2013). Para o Brasil, segundo a Cisco (<http://6lab.cisco.com/stats>), o número de AS de trânsito anunciando prefixos IPv6 chega a cerca de 40% do total.

Os Pontos de Troca de Tráfego da Internet (*Internet Exchange Points*, IXP) são locais neutros onde operadores de rede, provedores de acesso à Internet, provedores de conteúdo e outras empresas do setor podem instalar seus equipamentos e interconectar suas redes. Geralmente esses locais concentram grande parte do tráfego Internet e, por este motivo, um grande volume de tráfego IP é encaminhado por eles. Atualmente, os dois maiores IXPs do mundo são a DE-CIX Frankfurt e a AMS-IX Amsterdam. A soma dos volumes diários do tráfego IPv6 nesses dois IXPs é de 25 Gbps em horário de pico, com uma média de 16 Gbps (AMX-IX, 2013; DE-CIX, 2013). Isto corresponde a 0,5 % do volume de tráfego IPv4 nesses IXPs (AMX-IX, 2013; DE-CIX, 2013). No Brasil o IXP mais relevante com relação ao volume de tráfego é o ponto de troca de tráfego da cidade de São Paulo (<http://sp.ptt.br>). Nele, a média mensal do tráfego agregado do IPv6 é de cerca de 140 Mbps, sendo os picos de cerca de 396 Mbps. Esses valores correspondem, respectivamente, a 0,0008% e 0,001% do tráfego do IPv4.

Com base nas informações apresentadas, observa-se que a utilização do IPv6 pelos usuários da Internet ainda é baixa, representada por 1,92% do total de usuários IPv4. Com relação à adoção do novo protocolo por parte dos AS, os

índices se mostram melhores com cerca de 16% dos AS mundiais anunciando prefixos IPv6 para a Internet.

3 TÉCNICAS PARA MEDIÇÃO DE DESEMPENHO DO IPV6 NA INTERNET

O Capítulo 2 abordou as principais características do cabeçalho IPv6 de forma a mostrar sua incompatibilidade com o IPv4. Foram apresentadas as técnicas de transição utilizadas para contornar esse problema e as características dessas técnicas que podem influenciar a performance do IPv6. Por fim, foi apresentado um panorama geral do estado atual da implantação do IPv6 na Internet.

Neste Capítulo serão apresentadas as principais técnicas utilizadas para avaliar a estabilidade e o desempenho do IPv6 na Internet. Na Seção 3.1 são abordadas as técnicas baseadas no envio e recebimento de pacotes de dados e na Seção 3.2 as técnicas de medição que utilizam o acesso *web* por meio do protocolo HTTP. Na Seção 3.3 será detalhada a proposta desenvolvida neste trabalho para possibilitar a aquisição de informações relacionadas ao acesso *web*.

3.1 MEDIÇÕES BASEADAS NO ENVIO E RECEBIMENTO DE PACOTES DE DADOS

O principal objetivo deste tipo de técnica é a aquisição de informações que permitam analisar por meio do IP, a conectividade, o atraso, a variação do atraso (*jitter*) e a perda de pacotes dos enlaces de comunicação da Internet. Duas abordagens são utilizadas por essas técnicas no que diz respeito ao envio e ao recebimento dos pacotes, a abordagem de sentido único e a de tempo de ida e volta (RTT) (ZHOU et al, 2006; LAW et al, 2008).

As técnicas que utilizam a abordagem de sentido único, enviam pacotes de dados contendo informações sobre o tempo de partida para um destino na Internet. Ao receber este pacote, o dispositivo calcula as informações relativas à

transmissão efetuada como, por exemplo, o tempo de trânsito da origem para o destino ou a perda do pacote. Uma vez que o desempenho de determinadas aplicações relaciona-se apenas com uma das direções percorridas pelos pacotes, essa abordagem permite análises individuais dos caminhos de ida e volta percorridos pelos pacotes da origem para o destino e vice-versa (ALMES et al, 1999^A; ZHOU et al, 2006; SOUMYALATHA et al, 2013).

Nas técnicas baseadas em RTT, os dispositivos que originam as medições enviam um pacote de dados para um determinado dispositivo de destino na Internet e aguardam um pacote de resposta. Ao recebê-lo, o dispositivo de origem calcula o tempo que o pacote de dados levou no percurso de ida e volta até o destino, ou registra a falha na comunicação caso o pacote de resposta não seja recebido (LAW et al, 2008; SOUMYALATHA et al, 2013). Este tipo de abordagem pode ser conveniente quando o sistema de medição não prevê o controle dos dispositivos de destino para os quais os pacotes são endereçados. Ela também pode ser utilizada na análise dos impactos que o caminho de ida e volta dos pacotes pode causar nos protocolos da camada de transporte, como o TCP, que necessita de confirmação de recebimento. Esses protocolos podem ter sua performance degradada, e conseqüentemente as aplicações que operam sobre eles, caso qualquer um dos sentidos da comunicação seja prejudicado (ALMES et al, 1999^B).

O principal objetivo das propostas de medição baseadas no envio e recebimento de pacotes de dados é a análise dos enlaces de comunicação da Internet. Deste modo, os arranjos para as medições geralmente contemplam equipamentos instalados em pontos estratégicos da Internet (pontos de

observação), distribuídos por diversos países dos cinco continentes. As medições são efetuadas, entre os equipamentos, de forma automatizada e com intervalos de tempo pré-estabelecidos que, na maioria dos casos, baseiam-se no comportamento do tráfego nos enlaces analisados (LAW et al, 2008; ZHOU et al, 2006).

Alcançado o período de medição estabelecido, os dados coletados em cada ponto de observação são correlacionados com o objetivo de detectar comportamentos ou problemas de desempenho das rotas percorridas pelos pacotes. No caso dos estudos voltados para o IPv6, os processos de medição são executados de forma paralela ao IPv4, e as informações obtidas durante o período de medição são analisadas de forma comparativa entre os dois protocolos.

De modo geral, as medições baseadas no envio e recebimento de pacotes permitem a identificação de problemas de desempenho relacionados aos enlaces de comunicação e aos dispositivos intermediários da Internet, que podem afetar os protocolos de transporte e de aplicação. Porém, nenhuma dessas técnicas acessa de forma direta esses protocolos nos sistemas finais e, por esse motivo, não permitem a aquisição de informações nessas camadas. Sendo assim, não seria possível a utilização dessas técnicas para observar métricas relativas, por exemplo, às páginas e aplicações *web*.

3.2 MEDIÇÕES BASEADAS NO PROTOCOLO HTTP

A utilização do protocolo HTTP para o estabelecimento de mecanismos de medição de desempenho do IP, na Internet, tem como principal fundamento a

grande quantidade de servidores deste tipo de aplicação instalados em localizações distintas pelo mundo, proporcionando acesso aos principais enlaces de comunicação da Internet e a informações relativas aos protocolos de transporte e aplicação. A principal métrica de desempenho proporcionada por este tipo de medição é a taxa de dados efetiva da aplicação obtida na conexão entre o cliente e o servidor HTTP (LAW et al, 2008; NIKKHAH et al, 2011; DHAMDHERE et al, 2013). Além disso, por meio desse método, seria possível acessar outras informações de desempenho das camadas de transporte e de aplicação como, por exemplo, o tempo para estabelecimento de conexões TCP e o tempo de resposta às solicitações dos objetos HTTP.

Para coletar essas informações, clientes HTTP com funcionalidades básicas são instalados em computadores localizados em diferentes pontos da Internet (pontos de observação). A partir deles, são iniciados *downloads* automatizados de objetos HTTP de tamanhos variados, em intervalos de tempo pré-estabelecidos, e as informações da transferência desses objetos são armazenadas para as análises posteriores. Como as medições são efetuadas considerando diversos pontos de observação, o relacionamento dos dados coletados pode proporcionar informações sobre rotas específicas da Internet (LAW et al, 2008; NIKKHAH et al, 2011; DHAMDHERE et al, 2013).

Em se tratando do IPv6, informações como a taxa de dados dos protocolos de transporte e aplicação são coletadas paralelamente com o IPv4 e as análises são efetuadas de modo comparativo. Este tipo de abordagem proporciona um panorama geral do desempenho do IPv6 com relação ao IPv4 para a taxa de

dados dos protocolos de transporte e aplicação, em regiões específicas da Internet.

Os métodos de medição baseados no protocolo HTTP proporcionam acesso à camada de aplicação, porém não remetem, principalmente no que se refere à aplicação cliente (navegador *web*), à forma pela qual os usuários reais da Internet utilizam esse recurso. Além disso, esse método não permite análises que considerem a perspectiva da experiência do usuário, relativa à quantidade de conteúdo recebido dos servidores HTTP e nem como ela é mostrada no navegador *web*.

3.3 PROPOSTA PARA MEDIÇÃO DO ACESSO *WEB* EFETUADO COM O IPV6

A proposta desenvolvida neste trabalho objetiva uma análise de campo do desempenho de acessos *web* em IPv6 quando comparados com acessos *web* em IPv4. Para alcançar tal objetivo foi necessário o desenvolvimento de um método que fosse capaz de efetuar a aquisição de dados de métricas relativas ao acesso *web*. As métricas observadas pelo método proposto possuem relação com a rede, com as aplicações cliente e servidor (navegador *web* e servidor HTTP), com a quantidade de conteúdo recebido e com a forma como este conteúdo é apresentado no navegador do usuário. De fato, essas métricas são o tempo de carregamento dos objetos HTTP (relação com a rede), a quantidade de *bytes* recebidos (relação com as aplicações cliente/servidor e com o conteúdo) e o tempo total para que a página *web* seja completamente mostrada (relaciona-se com a experiência do usuário) no navegador do usuário.

Para estabelecer um sistema de medição capaz de fazer a aquisição das métricas mencionadas, foi utilizado um navegador *web* comumente utilizado por usuários reais da *web*, Mozilla Firefox. Esse tipo de aplicativo proporciona a interpretação e execução de códigos de *software* que são atualmente utilizados no desenvolvimento *web* como, por exemplo, aplicações escritas em *Flash*, *Java/Javascript*, *Silverlight*, entre outros. Essas aplicação são responsáveis, em muitos casos, pela obtenção de outros objetos HTTP não contidos na página inicialmente acessada. Sem a utilização deste tipo de navegador *web*, o processo de medição não iria contemplar o mesmo comportamento experimentado pelos usuários deste tipo de aplicação. Além disso, por meio desse tipo de navegador, é possível acessar métricas importantes relacionadas à experiência visual do usuário com relação ao carregamento da página *web*, como o tempo médio em que os objetos HTTP são mostrados no navegador e o tempo total que a página *web* levou para ficar visivelmente completa para o usuário.

O processo de medição foi efetuado mediante três configurações do protocolo IP, a primeira utilizando exclusivamente o IPv4, a segunda o IPv4 e o IPv6 (pilha dupla) e a última exclusivamente o IPv6. A configuração apenas IPv4 remete ao modelo utilizado atualmente pela maioria dos usuários da Internet, sendo esta a referência utilizada para analisar os dados das outras duas configurações do IP. A configuração em pilha dupla objetiva a avaliação do impacto que a preferência pela utilização do IPv6, nos sistemas operacionais e no navegador (WING; YOURTCHENKO, 2012), pode causar à experiência do usuário no acesso a uma página *web*. Por fim, a configuração que opera exclusivamente com o IPv6 avalia a experiência de um usuário no atual estágio

da transição para o IPv6, quando não existir um endereço IPv4 ou técnica de transição disponíveis para serem utilizados em conjunto com o IPv6.

Para que os dados obtidos pelos equipamentos que utilizam o IPv6 possam ser relacionados com os dados do equipamento que utiliza exclusivamente o IPv4, é necessário que as medições sejam feitas de forma simultânea por esses dispositivos. Para isto, foi desenvolvida neste trabalho uma ferramenta de *software* que coordena as medições para que elas ocorram de forma simultânea, essa ferramenta está disponível para *download* em (PIRANI; ABBADE, 2013) e é descrita no apêndice 1. O objetivo dos acessos simultâneos é evitar que possíveis oscilações de desempenho da rede ou dos servidores DNS e HTTP possam influenciar as medições de uma configuração específica do IP, que aconteça em um instante de tempo diferente das outras configurações.

Também neste sentido, é importante que o processo de medição seja automatizado e executado em intervalos de tempo que contemplem as oscilações de tráfego das conexões com a Internet utilizadas pelos equipamentos de medição. Para os resultados mostrados neste trabalho, todas as páginas *web* avaliadas foram acessadas de hora em hora, contemplando, desta forma, oscilações de carga de tráfego que ocorrem diariamente na Internet. Além disso, o processo de medição foi executado durante o período de um mês, contemplando também as características de tráfego neste intervalo de tempo. Os dados obtidos nas medições foram utilizados para as análises comparativas entre o IPv4 e o IPv6, do tempo de carregamento, tempo para completamento visual e o número de *bytes* obtidos das páginas *web*.

Para que as medidas obtidas de uma página *web*, acessada tanto pelo IPv4 quanto pelo IPv6 (ou pela Pilha Dupla), pudessem ser comparadas entre si, foi proposto um método baseado em métricas relativas para classificar as medidas como típicas ou atípicas. Uma medida típica é aquela que possui seu valor entre o limite mínimo e máximo estabelecido para uma determinada métrica e, medidas atípicas, aquelas em que seu valor permanece fora deste intervalo.

A Figura 11 ilustra como estes limites foram estabelecidos no presente trabalho. Observa-se que um valor arbitrário de 60%, para medidas típicas, foi estabelecido em torno da média das medidas obtidas pelo IPv4 e um valor de 20% para as medidas atípicas inferiores e também para as superiores.

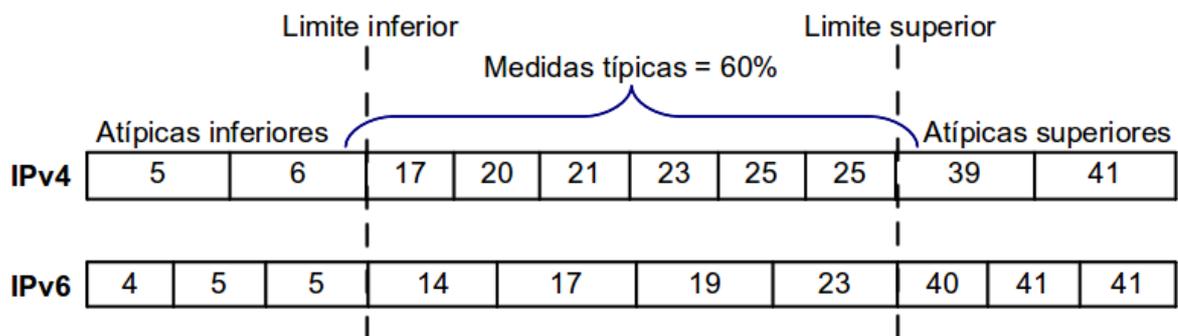


Figura 11. Definição das métricas relativas para medidas atípicas

Os limites inferior e superior deste intervalo definem os valores que serão utilizados na contagem das medidas típicas, atípicas inferiores e atípicas superiores, tanto para as medidas obtidas pelo IPv4 quanto para aquelas obtidas pelo IPv6 ou pela Pilha Dupla. As medias com valores maiores do que o limite inferior e menores do que o superior são contabilizadas como medidas típicas. Medidas que possuem valores iguais ou menores que o limite inferior, são

contabilizadas como atípicas inferiores e as que possuem valores iguais ou maiores do que o limite superior são contabilizadas como atípicas superiores.

4 DESCRIÇÃO DO EXPERIMENTO

No Capítulo 3 foram apresentadas as principais técnicas de medida utilizadas na obtenção de informações que permitam a avaliação do desempenho do IPv6 na Internet. Além das características e possibilidades que cada técnica oferece, foram apresentados os motivos pelos quais elas não proporcionam métricas adequadas para a análise das aplicações *web* na perspectiva do usuário real deste serviço. Por este motivo, foi apresentada na Seção 3.3 a proposta desenvolvida neste trabalho para se obter tais métricas e, por meio delas, efetuar as análises relativas ao desempenho do IPv6 no acesso às aplicações *web*.

Este Capítulo descreve na Seção 4.1 os recursos de *hardware* e *software* empregados na montagem do arranjo utilizado nas medições. Em 4.2 é descrito o processo de medição desde a submissão dos testes até o armazenamento das informações relativas aos acessos efetuados às páginas *web* medidas.

4.1 ARRANJO PARA AS MEDIÇÕES DE CAMPO

A Figura 12 mostra uma visão geral do arranjo considerando a disposição e a forma pela qual os equipamentos foram interconectados. Todos os dispositivos presentes na figura foram instalados na borda da rede de um Sistema Autônomo (*Autonomous System*, AS) da Internet, e as conexões IPv4 e IPv6 fornecidas a eles não passam por nenhum tipo de dispositivos de *firewall* ou de priorização de pacotes.

Além disso, é importante notar que o *Servidor WPT* e os quatro agentes presentes no arranjo foram implantados utilizando recursos de virtualização. Este

tipo de prática permite a operacionalização de diversos sistemas operacionais funcionando de forma simultânea em um mesmo computador físico otimizando, desta forma, a utilização de recursos de *hardware* e de *datacenter*. Os detalhes sobre como a virtualização foi utilizada serão apresentados mais adiante neste Capítulo.

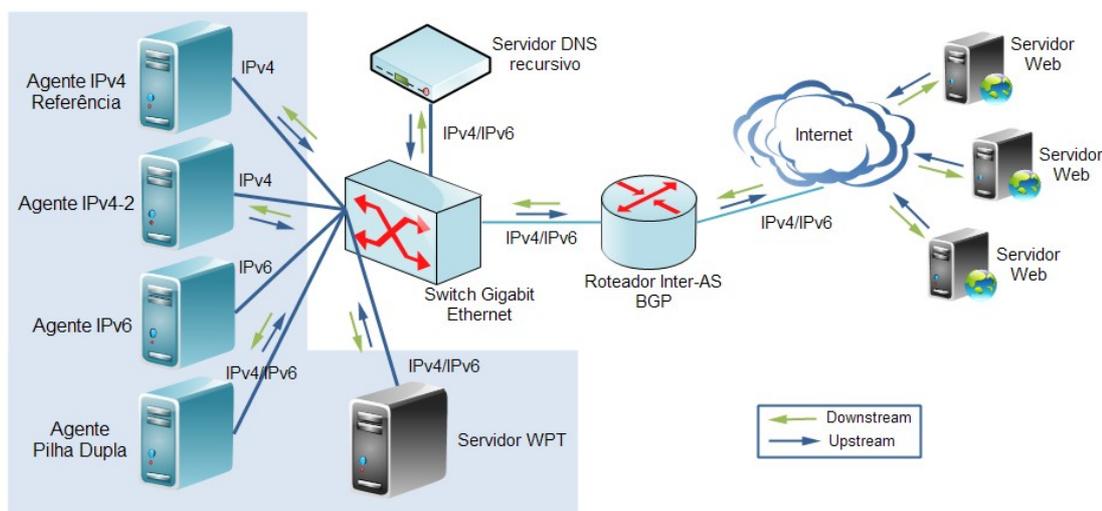


Figura 12. Visão geral do arranjo

O *Roteador inter-AS*, é o elemento de rede responsável por conectar o sistema autônomo, no qual as medições de campo foram efetuadas, com a Internet. Ele disponibiliza as rotas IPv4 e IPv6 necessárias para que os elementos localizados dentro do AS possam acessar outras redes na Internet. No caso específico do AS em questão, essas rotas são recebidas de duas operadoras comerciais de trânsito Internet e também de pontos de troca de tráfego localizados na cidades de São Paulo-SP e Campinas-SP, aos quais o AS está diretamente conectado. Com relação às configurações de *hardware* e *software* do *Roteador inter-AS*, a Tabela 3 apresenta essas informações de forma detalhada.

Tabela 3. Especificações de *hardware* e *software* do Roteador inter-AS

HARDWARE		
ITEM	QTDE	DESCRIÇÃO
Processador	2	Intel(R) Xeon Dual Core 3.0 GHz
Memória	2	Módulo ECC de 1 GB
Armazenamento	1	Flash Drive 4 GB
Interfaces de rede	4	Intel(R) PRO/1000 10/100/1000 Mbps
SOFTWARE		
Sistema operacional	-	Mikrotik RouterOS v5.24 level 4

É importante ressaltar que o Roteador inter-AS já fazia parte da estrutura de rede do AS origem das medições, desta forma, apenas uma conexão de rede deste equipamento foi disponibilizada para os elementos responsáveis pelas medições. Sendo assim, detalhes específicos da configuração do *Roteador inter-AS*, principalmente no que diz respeito aos protocolos de roteamento utilizados por ele, não serão apresentados neste trabalho.

O *Switch Gigabit Ethernet*, presente no arranjo, possui 24 portas 10/100/1000 Mbps e é responsável por conectar o restante dos elementos ao *Roteador inter-AS*. Este dispositivo, assim como o *Roteador inter-AS*, já fazia parte da rede do AS e não possui nenhuma configuração específica para o arranjo. Deste modo, ele opera como um *switch* de camada 2 convencional, comutando os quadros *ethernet* de uma porta para outra.

O *Servidor DNS recursivo* é mais um elemento disponibilizado pelo AS que já fazia parte da estrutura de sua rede. A função dele é receber as requisições de tradução de nomes de dispositivos para endereços IP, fazer as buscas necessárias na estrutura de DNS da Internet e responder às solicitações com o endereço IP do dispositivo em questão. A recursividade no servidor foi utilizada para remeter a mesma forma pela qual os servidores DNS do AS respondem às solicitações de consulta DNS efetuadas pelos clientes reais. Neste sentido, a

utilização de um servidor DNS não recursivo poderia implicar em um comportamento diferente do acesso *web*, uma vez que as Redes de Entrega de Conteúdo (*Content Delivery Network*, CDN) utilizam informações de origem da consulta DNS para selecionar servidores de conteúdo mais próximos do usuário. Não sendo o objetivo deste trabalho o estudo específico do impacto das CDNs no acesso *web* em IPv6, este tema poderia ser melhor investigado em trabalhos futuros.

Para que ele pudesse executar essa tarefa também para solicitações feitas via IPv6, foi designado a ele um endereço deste protocolo. A Tabela 4 apresenta as configurações de *hardware* e *software* do *Servidor DNS recursivo*.

Tabela 4. Especificação de *hardware* e *software* do Servidor DNS recursivo

HARDWARE		
ITEM	QTDE	DESCRIÇÃO
Processador	1	Intel(R) Xeon Quad Core 2.0 GHz
Memória	2	Módulo ECC de 2 GB
Armazenamento	1	Disco rígido SATA2 de 80 GB
Interfaces de rede	1	Intel(R) PRO/1000 10/100/1000 Mbps
SOFTWARE		
Sistema operacional	-	CentOS Linux v5.8
Servidor DNS	-	Bind v9.3.6-20.P1

Os dispositivos de rede diretamente responsáveis pelas medições de campo, propostas por este trabalho, são o *Servidor WPT* e os agentes IPv4 de referência, IPv4-2, IPv6 e Pilha Dupla (DS). Eles foram implementados utilizando recursos de virtualização de forma a otimizar o *hardware* e o espaço em *datacenter* disponibilizado pelo AS para a execução das medições. Os detalhes da configuração do servidor físico (hospedeiro) responsável pela virtualização são mostrados na Tabela 5.

Tabela 5. Especificação de *hardware* e *software* do Hospedeiro

HARDWARE		
ITEM	QTDE	DESCRIÇÃO
Processador	1	Intel(R) Xeon Quad Core 2.0 GHz
Memória	4	Módulo ECC de 4 GB
Armazenamento	1	Disco rígido SATA2 de 1 TB
Interfaces de rede	1	Intel(R) PRO/1000 10/100/1000 Mbps
SOFTWARE		
Sistema operacional	-	Citrix XenServer v6.0.1

Na Figura 13 é apresentado o esquema de virtualização utilizado, composto pelo *Hospedeiro* e pelas máquinas virtuais *Servidor WPT* e agentes IPv4 de referência, IPv4-2, IPv6 e Pilha Dupla (DS). O Hospedeiro possui conexão física com a rede local por meio de um cabo de rede que conecta sua placa de rede ao *Switch Gigabit Ethernet* da Figura 12. As máquinas virtuais, por sua vez, obtêm acesso à rede utilizando conexões virtuais ao *Switch Gigabit Ethernet*, disponibilizadas pela placa de rede física do hospedeiro, conforme ilustrado pela Figura 13.



Figura 13. Esquema de virtualização dos agentes e do Servidor WPT

O Servidor WPT é o elemento responsável por coordenar as medições dos quatro agentes, além disso ele processa e armazena os resultados de cada processo de medição executado. Para isso ele recebeu a instalação do servidor

da plataforma de testes de aplicações *web* Webpagetest (WPT) que, além de prover uma interface *web* para submissão de testes, disponibiliza uma interface de programação para automação deles. No *Servidor WPT* também foram desenvolvidas aplicações em linguagem *bash script* para que todo o processo de medição, desde a submissão até o armazenamento dos resultados pudesse ser automatizado. Os detalhes das aplicações instaladas no *Servidor WPT*, bem como a configuração do *hardware* virtual disponibilizado a ele são descritos na Tabela 6.

Tabela 6. Especificação dos softwares e do hardware virtual do Servidor WPT

HARDWARE VIRTUAL		
ITEM	QTDE	DESCRIÇÃO
Processador	1	Intel(R) Xeon Quad Core 2.0 GHz
Memória	1	2 GB
Armazenamento	1	100 GB
Interfaces de rede	1	Intel(R) PRO/1000 10/100/1000 Mbps
SOFTWARE		
Sistema operacional	-	CentOS Linux v6.4
Servidor HTTP	-	Httpd v2.2.15-28
Suporte a linguagem PHP	-	PHP v5.3.3-22
Suporte a linguagem Bash	-	Bash v4.1.2-14
Processamento de vídeo	-	Ffmpeg v0.6.5-1
Servidor WPT	-	Release v2.12

O acesso às páginas *web*, bem como a obtenção das medidas relativas às métricas analisadas por este trabalho, são efetivamente executados pelos quatro agentes que integram o arranjo ilustrado pela Figura 12. Eles representam o computador pessoal de um usuário real das aplicações *web* e, por este motivo, operam com um sistema operacional cliente e um navegador *web* moderno com suporte às tecnologias utilizadas no desenvolvimento *web*. Além disso, foi instalado nos agentes a parte cliente da plataforma WPT que permite a obtenção,

diretamente do navegador, das informações relativas aos acessos efetuados as páginas *web*. No final de cada medição, essas informações são enviadas ao *Servidor WPT* para que possam ser processadas e armazenadas.

Neste ponto cabe observar que o agente IPv4-2 foi adicionado ao arranjo para que as medidas obtidas por ele pudessem ser comparadas com o IPv4 de referência. O objetivo desta prática é o de identificar possíveis variações que possam ocorrer nas medidas, e que não estejam relacionadas com as configurações do IP utilizadas.

Os quatro agentes receberam os mesmos recursos de *hardware* virtual e de *software*, descritos na Tabela 7, diferenciando-se apenas na configuração dos endereços IP. Os agente IPv4 de referência e *IPv4-2* receberam, cada, apenas um endereço IPv4, o agente IPv6 somente um endereço IPv6 e o agente Pilha Dupla (DS) um endereço IPv4 e outro IPv6. O roteador que disponibiliza o acesso à Internet e o servidor DNS que responde às consultas de nomes de domínio são os mesmos para os quatro agentes, conforme ilustrado na Figura 12.

Tabela 7. Especificação dos *softwares* e do *hardware* virtual dos agentes.

HARDWARE VIRTUAL		
ITEM	QTDE	DESCRIÇÃO
Processador	1	Intel(R) Xeon Quad Core 2.0 GHz
Memória	1	2 GB
Armazenamento	1	20 GB
Interfaces de rede	1	Intel(R) PRO/1000 10/100/1000 Mbps
SOFTWARE		
Sistema operacional	-	Microsoft(R) Windows 7 Professional 32 bits
Navegador web	-	Mozilla Firefox v23
Suporte tecnologia Flash	-	Shockwave Player v11.8.800.94
Suporte a tecnologia Silverligh	-	Silverligh Plug-In v5.1.20513.0
Agente WPT	-	Release v2.12

4.2 PROCESSO DE MEDIÇÃO

Para que as medições pudessem cumprir com a proposta descrita na Seção 3.3, uma série de programas em *shell script (bash)* foram desenvolvidos pelo autor deste trabalho e encontram-se disponíveis para *download* em (PIRANI; ABBADE, 2013). Elas operam no *Servidor WTP* e são responsáveis por coordenar o início das medições, processar os dados adquiridos e armazená-los em formato de arquivo texto.

O processo de medição inicia-se no *Servidor WPT* com a execução de um *bash script*, denominado *run_tests*, que faz a leitura de um arquivo texto contendo uma lista das páginas *web* que devem ser medidas. Uma por vez, essas páginas são passadas como parâmetro para os agentes IPv4 de referência, IPv4-2, DS e IPv6 que iniciam o processo de medição. Cada agente utiliza uma determinada configuração de endereçamento IP, sendo dois agentes com o IPv4 (IPv4 de referência e IPv4-2), um com o IPv6 e o último com um endereço de cada versão do protocolo IP (IPv4 e IPv6). Ao receberem a solicitação de medição via aplicação cliente do Webpagetest (WPT), o navegador *web* é acionado e a página é acessada nos *Servidores Web* remotos. Diversos eventos que acontecem no navegador dos agentes são monitorados pelo cliente da plataforma WPT e as informações coletadas são enviadas ao *Servidor WPT* no instante em que o carregamento das páginas é finalizado ou quando o tempo máximo do teste, de 30 segundos, é alcançado.

A aplicação *run_tests* monitora a execução das medições nos agentes. Assim que o processo termina, um *bash script* denominado *get_data* é acionado paralelamente ao início de um novo processo de medição. O *get_data* armazena,

em diretórios específicos para cada medição, as informações adquiridas pelos agentes no processo de medição que foi concluído. Essas informações são armazenadas em diversos formatos, sendo um arquivo no formato de Linguagem de Marcação Extensível (*Extensible Markup Language*, XML) contendo todas as métricas disponibilizadas pela plataforma Webpagetest, um arquivo no formato de Arquivamento HTTP (*HTTP Archive*, HAR) contendo todas as transações HTTP efetuadas entre o navegador e os *Servidores web* remotos, um arquivo texto com valores separados por vírgula (*Comma-separated Values*, CSV) contendo informações sobre as consultas DNS e as conexões TCP efetuadas pelos agentes e, por fim, um arquivo de imagem com o conteúdo visual da página *web* exibida no navegador do agente.

Desta forma, por meio do processo de medição descrito e utilizando o processamento paralelo das medições, foi possível obter mais de 600 medições para as 100 páginas *web* com suporte ao IPv6 mundialmente mais acessadas. Essas medições foram efetuadas entre os dias 12 de agosto e 12 de setembro do ano de 2013, contemplando os períodos diários e mensais de oscilação de tráfego da Internet.

Terminado o processo de medição, as informações armazenadas foram processadas por um *bash_script*, denominado *filter_data*, e diversas métricas foram extraídas. Dentre elas, o tempo de carregamento dos objetos HTTP, o tempo para completamento visual da página no navegador do usuário e o número de *bytes* obtidos foram utilizadas na análises apresentadas no Capítulo 5. Além delas, outras métricas foram extraídas para auxiliar na identificação das causas relacionadas aos comportamentos identificados. A Tabela 8 apresenta uma

relação de todas as métricas disponibilizadas pelo arranjo proposto e que foram extraídas dos dados obtidos nas medições.

Tabela 8. Métricas disponibilizadas pelo arranjo desenvolvido

Métrica	Unidade	Descrição
Tempo de carregamento	Segundos	Tempo do início da navegação até o recebimento do último objeto HTTP
Número de <i>bytes</i>	<i>Bytes</i>	Número de <i>bytes</i> obtidos na camada de aplicação
Número de objetos HTTP	Unidade	Número de objetos HTTP recebidos da página <i>web</i> acessada
Índice de velocidade	Segundos	Representa o quão rápido a página <i>web</i> é mostrada no navegador (métrica da plataforma Webpagetest)
Completamento visual	Segundos	Intervalo de tempo do início da navegação até o instante em que a página para de sofrer mudanças visuais.
TTFB	Segundos	Tempo para recebimento do primeiro <i>byte</i> da página acessada
Pontuação CDN	%	Porcentagem dos objetos HTTP que foram recebidos de servidores pertencentes à Redes de Fornecimento de Conteúdo
Comparação de pixel	%	Comparação da imagem (<i>print screen</i>) da página <i>web</i> carregada no agente IPv4 com a imagem da página <i>web</i> carregada nos outros agentes
Consultas DNS	Unidade	Quantidade de consultas DNS efetuadas no acesso a página <i>web</i>
Conexões TCP	Unidade	Número de conexões TCP estabelecidas com o servidor <i>web</i> remoto
Retransmissões	Unidade	Número de seguimentos TCP retransmitidos
L2 Bytes	Unidade	Número de bytes recebidos na camada de enlace
Tempo bloqueado	Segundos	Tempo aguardando liberação de conexões TCP
Tempo DNS	Segundos	Soma dos tempos gastos nas consultas DNS de todos os nomes de hosts da página acessada
Tempo para conexão	Segundos	Tempo gasto no estabelecimento das conexões TCP
Tempo de envio	Segundos	Tempo gasto no envio das requisições HTTP ao servidor <i>web</i> remoto
Tempo aguardando	Segundos	Tempo gasto aguardando a resposta de uma requisição HTTP efetuada
Tempo de recebimento	Segundos	Tempo gasto recebendo do servidor <i>web</i> a resposta a uma requisição HTTP
Tempo SSL	Segundos	Tempo gasto na negociação de uma conexão segura SSL com o servidor <i>web</i> remoto

5 RESULTADOS

A aplicação do método proposto em 3.3, por meio do arranjo descrito no Capítulo 4, proporcionou a aquisição de informações que possibilitaram as análises apresentadas neste Capítulo. Na seção 5.1 são discutidas as variações que cada métrica apresenta de acordo com cada página *web*. Em 5.2 são mostrados os resultados das análises relativos ao comportamento do tempo de carregamento das páginas *web*, quando acessadas por meio da Pilha Dupla (IPv4+IPv6) e somente pelo IPv6. Na Seção 5.3 as análises são feitas considerando o tempo para completamento visual da página *web* no navegador do usuário e em 5.4 a métrica analisada é a quantidade de *bytes* transmitidos nos acessos a estas páginas.

5.1 RELAÇÃO DAS MÉTRICAS AVALIADAS COM AS PÁGINAS *WEB*

O tempo de carregamento dos objetos HTTP de uma página *web* pode variar de acordo com uma série de características. Dentre elas estão o comportamento da rede como, por exemplo, o tempo de ida e volta dos pacotes (RTT), a taxa de dados máxima dos enlaces de comunicação e, até mesmo, a perda de pacotes. Além disso, o tempo de carregamento também pode variar de acordo com características da própria página *web*, como o seu tamanho em *bytes* e a quantidade e tipos dos objetos HTTP.

A Figura 14 mostra um gráfico de colunas para a média do tempo de carregamento das 100 páginas *web* utilizadas nas medições deste trabalho, quando acessadas pelo agente IPv4 de referência. O tempo de carregamento,

representado por *TC*, está expresso em segundos e, juntamente com ele, é apresentada a barra de indicação do desvio padrão das medidas de cada página.

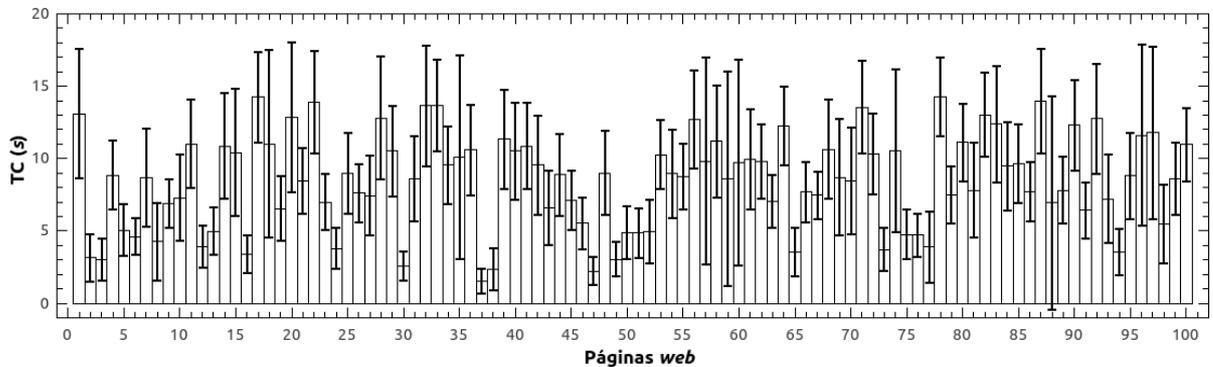


Figura 14. Variação do tempo médio de carregamento de cada página web

Observa-se, pela Figura 14, que a média do tempo de carregamento das páginas *web* varia de 1,52 a 14,25 segundos sendo estes valores relativos, respectivamente, às páginas 37 e 78. Com relação ao desvio padrão, observou-se variações de 0,88 a 7,42 segundos relativos, respectivamente, às páginas 37 e 59.

O completamento visual de uma página *web* é uma métrica que representa o instante de tempo em que a visualização completa da página *web* mostrou-se disponível para o usuário (MEENAM, 2013). Esta métrica relaciona-se com o tempo de carregamento dos objetos HTTP que, conforme ilustrado pela Figura 14, possui relação com cada página *web* em particular. Além disso, o completamento visual relaciona-se com os recursos computacionais (*hardware* e *software*) dos dispositivos finais que acessam as páginas *web*, com o tipo de conteúdo que os objetos da página representam e, também, com a forma pela qual os desenvolvedores das aplicações *web* optam por mostrar esses objetos.

A Figura 15 mostra, por meio de um gráfico de colunas, a média do tempo para completamento visual, em segundos, de cada página analisada, juntamente com o desvio padrão das medições. O tempo para completamento visual, na Figura, está representado por CV.

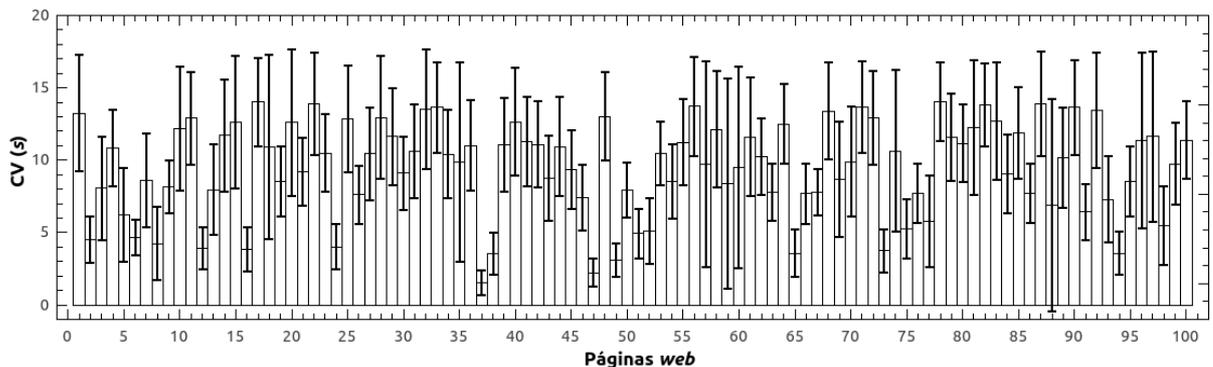


Figura 15. Variação do completamento visual de cada página web

Para o completamento visual, observa-se pela figura 15 que as médias variam de 1,53 a 14,04 segundos, respectivamente, para as páginas 37 e 78. Os desvios padrão vão de 0,88 segundos, relativo à página 37, a 7,32 segundos, relativo à página 88.

A métrica que representa a quantidade de *bytes* de uma página *web* também apresenta variações de acordo com cada página em específico. No caso desta métrica, os fatores relacionados às variações possuem ligação com a construção da página em si, que por sua vez pode utilizar quantidades distintas de objetos com tamanhos variados, com a utilização de técnicas de compressão dos objetos HTTP, atualizações dinâmicas de conteúdo e até mesmo com características de instabilidade da rede, que podem influenciar a quantidade de *bytes* transmitidos.

A Figura 16 apresenta um gráfico de colunas contendo as médias do número de *bytes*, em KB, representadas por N_B , e que foram obtidas pelas medições efetuadas às 100 páginas *web*. Juntamente com as médias, são apresentadas as barras contendo o desvio padrão das medidas de cada páginas *web*.

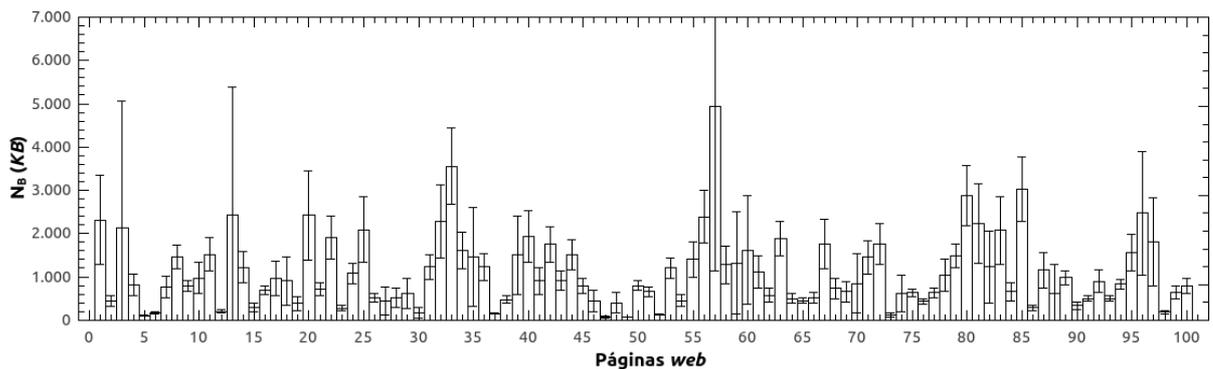


Figura 16. Variação do número de *bytes* obtidos de cada página *web*

Conforme mostrado pela Figura 16, a quantidade de *bytes* obtidos está vinculada com cada páginas *web* em particular. Observa-se que a página 47, por exemplo, obteve uma média de 62 KB. A página 57, por sua vez, apresentou uma média de 4.928 KB.

Conforme as informações apresentadas nas Figuras de 14 a 16, o comportamento das métricas utilizadas nas análises propostas por este trabalho possui relação específica com cada página *web*. Sendo assim, a utilização de métricas relativas mostrou-se uma opção plausível para as análises efetuadas.

5.2 TEMPO DE CARREGAMENTO

O gráfico da Figura 17 mostra a relação entre as medidas atípicas do tempo de carregamento obtidas pelos agentes IPv4-2, Pilha Dupla (DS) e IPv6

com as medidas atípicas obtidas pelo agente IPv4 de referência. Na Figura, a relação está representada por $T_{i/IPv4}$ e foi obtida da seguinte forma

$$A_{i/IPv4} = \frac{A_{i,j}}{A_{IPv4,j}}, \quad (1)$$

na qual A igual a T, C ou N representa, respectivamente, o tempo de carregamento da página *web*, o tempo para completamento visual e o número de *bytes* obtidos. A variável *i* igual a IPv4-Ref, IPv4-2, DS e IPv6 denotam, respectivamente, os agentes IPv4 de referência, IPv4-2, Pilha Dupla (DS) e IPv6 e, por fim, a variável *j*, representa a página *web* para a qual a relação é calculada.

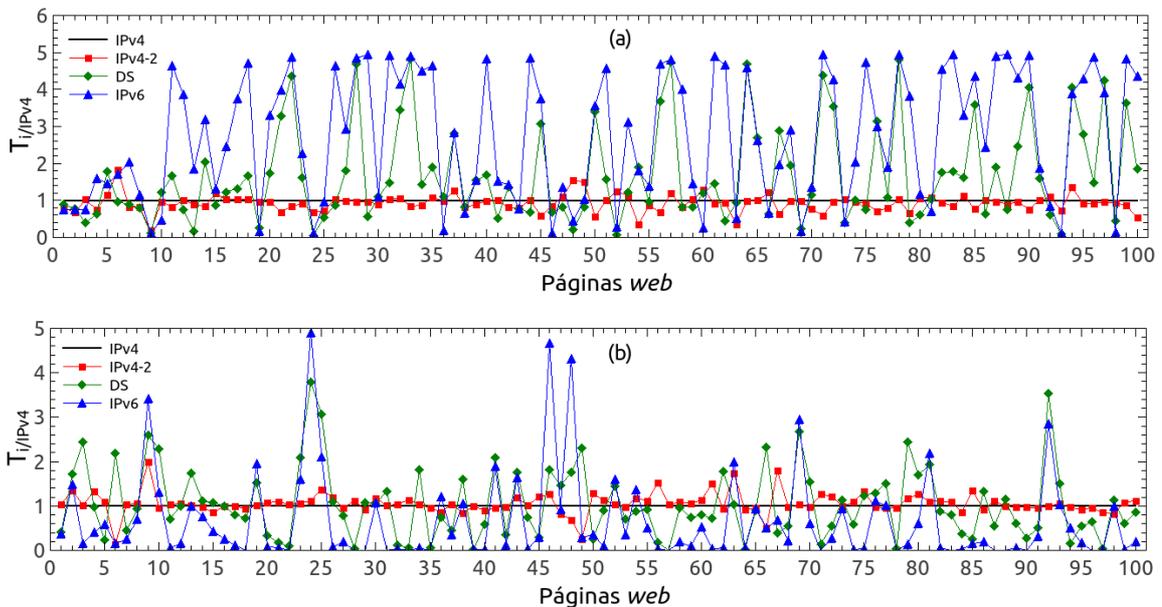


Figura 17. Relação com o IPv4 de referencia das medidas atípicas inferiores (a) e superiores (b) para do tempo de carregamento

Observa-se por meio da Figura 17 que as medidas atípicas obtidas pelos três agentes possuem comportamentos distintos, com relação ao IPv4 de referência, e que esses comportamentos estão relacionados não apenas com as páginas *web* acessadas mas, também, com a configuração de protocolo utilizada no acesso. Para o agente IPv4-2, nenhuma página *web* apresentou um número

de medidas atípicas inferiores maior do que o dobro daquele obtido pelo agente IPv4 de referência. Com relação aos agentes DS e IPv6, a quantidade de páginas *web* com número de medidas atípicas inferiores menor que o dobro daquele obtido pelo IPv4 foi de 75 e 43, respectivamente.

Para as medidas atípicas superiores o comportamento do agente IPv4-2 foi similar ao observado nas atípicas inferiores, sendo que nenhuma das páginas *web* obteve um número de medidas atípicas superiores maior do que o dobro daquele obtido pelo IPv4 de referência. Para os agentes DS e IPv6, o número de páginas *web* com menos do que dobro das medidas atípicas do IPv4 de referência foi de 87 e 91, respectivamente.

Considerando, ainda, as informações apresentadas pela Figura 17 (a) e (b), é possível observar que a variação do número de medidas atípicas dos agentes DS e IPv6, com relação ao agente IPv4 de referência, ocorre com mais frequência para as medidas inferiores. Medidas com tempos de carregamento atípicos inferiores podem estar relacionadas com características da rede como, por exemplo, taxas de dados mais elevadas ou com características relacionadas à página *web*, como a indisponibilidade do conteúdo.

A Figura 18 apresenta a relação com o IPv4 de referência, representada por $T_{i/IPv4}$, das medidas atípicas inferiores e superiores do tempo de carregamento, obtidas pelos agentes IPv4-2, DS e IPv6. Os gráficos (a) e (b) são referentes às 100 páginas *web* avaliadas, e os gráficos (c) e (d) apresentam a mesma informação para as 23 páginas *web*, que obtiveram médias de *bytes* com até 10% de diferença (para menos *bytes*), considerando os agentes IPv4 de referência, DS e IPv6.

As informações apresentadas pela Figura 18 (a) e (c) possibilitam observar que as medidas atípicas inferiores do tempo de carregamento dos agentes IPv4-2, DS e IPv6 tendem a convergir quando a quantidade de *bytes* obtidos das páginas é similar, dada, respectivamente, a redução de cerca de 25 para 5% e de 57 para 20%, para os agentes DS e IPv6, das páginas com número de medidas atípicas inferiores maior do que o dobro das obtidas pelo IPv4 de referência. Desta forma, estando os tempos de carregamento mais rápidos relacionados com a indisponibilidade do conteúdo, observa-se em (b) e (d) que o comportamento das curvas mantém-se similar para as medidas atípicas superiores do tempo de carregamento. Neste sentido, foram identificadas concentrações de cerca de 55 e 80%, respectivamente, para os agentes DS e IPv6, das páginas *web* com número de medidas atípicas superiores menor do que aquele obtido pelo IPv4 de referência.

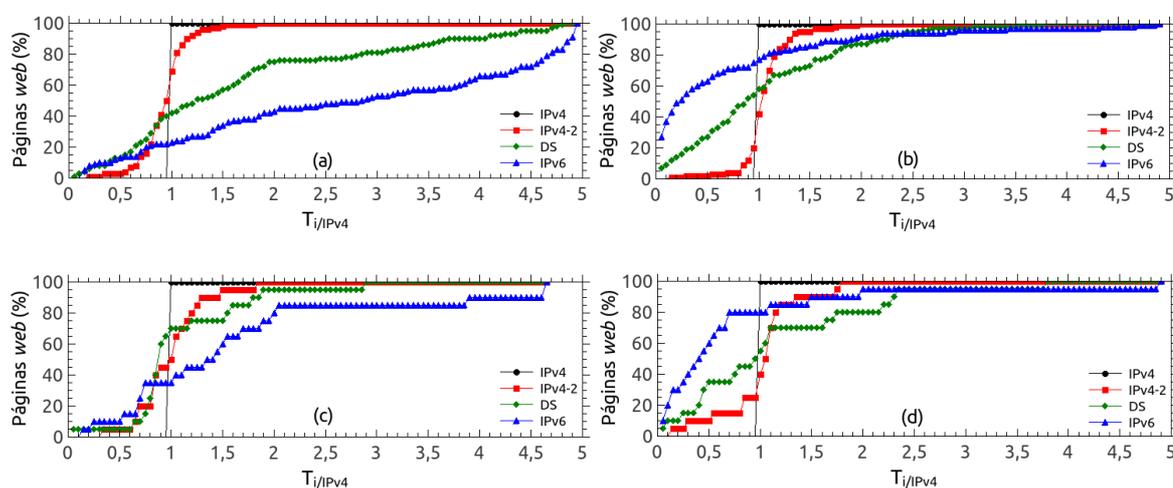


Figura 18. Relação das medidas atípicas inferiores (a) e superiores (b) do tempo de carregamento para as 100 páginas avaliadas e relação das medidas atípicas inferiores (c) e superiores (d) do tempo de carregamento para as 23 páginas com média similar do número de *bytes* obtidos

O gráfico da Figura 19 mostra para os agentes IPv4-2, DS e IPv6, a relação com o agente IPv4 de referência das medidas atípicas superiores do tempo de carregamento, obtidas no processo de medição de cada uma das 23 páginas *web*, consideradas na construção dos gráficos (c) e (d) da Figura 18. Na Figura, a relação com o IPv4 de referência está representada por $T_{i/IPv4}$ e foi obtida por (1).

Observa-se para a Pilha Dupla (agente DS), que 5 das 23 páginas *web*, mesmo com médias do número de *bytes* similares às do IPv4, apresentaram um número de medidas atípicas superiores maior do que o dobro daquele obtido pelo IPv4-2. Para essas 5 páginas, nota-se um comportamento similar entre as páginas 6, 49 e 66 e também entre as páginas 24 e 69.

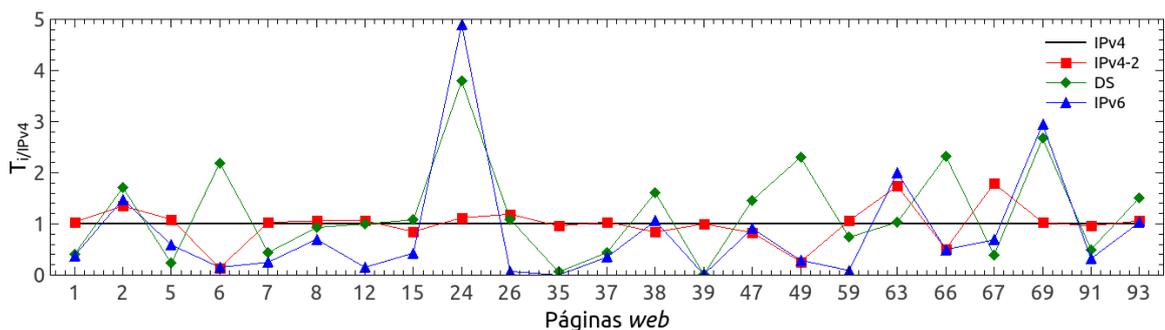


Figura 19. Relação com o IPv4 de referência, das medidas atípicas superiores para as páginas *web* com média de *bytes* similar

Para as páginas 6, 49 e 66, observou-se para o agente DS mais do que o dobro de medidas atípicas superiores do tempo de carregamento que aquelas obtidas pelo IPv4 de referência. As três páginas possuem características comuns, ambas são páginas com conteúdo estático, número de *bytes* e objetos HTTP reduzidos e, para o agente DS, a única métrica que apresentou diferenças consideráveis com relação ao agente IPv4 de referência e ao agente IPv6 foi o número de consultas DNS. Para exemplificar o comportamento observado, serão mostradas as análises efetuadas para a página 6.

A Figura 20 mostra, para os agentes IPv4 de referência, DS e IPv6, os histogramas das medidas relativas ao tempo de carregamento, TC , da página 6. Observa-se que a maior parte das medidas obtidas pelos três agentes concentram-se no intervalo de 2 à 6 segundos. Para o agente DS observa-se, ainda, certa de 25% das medidas distribuídas no intervalo de 6 a 12 segundos.

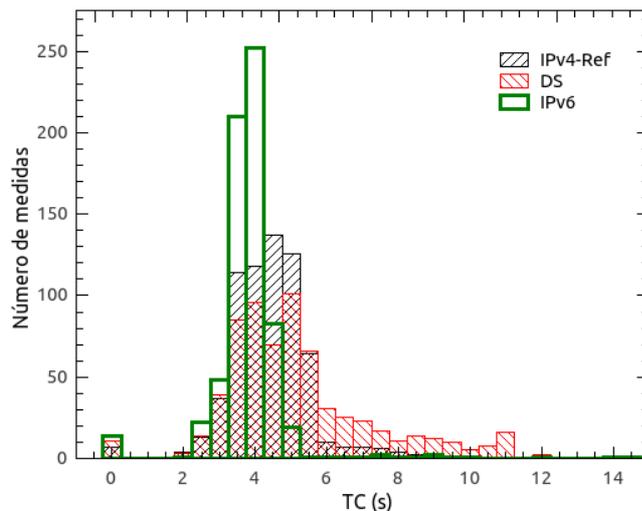


Figura 20. Tempo de carregamento da página 6

Os histogramas da Figura 21 (a) mostram o número de *bytes* recebidos da página 6, representado por N_B , e obtidos pelos agentes IPv4 de referência, DS e IPv6. Observa-se que o número de *bytes* recebidos nas medições possui variação dentro de um intervalo de 40 KB para os três agentes e, para o IPv4 de referência e o DS, o comportamento na obtenção dos *bytes* foi similar. A média de *bytes* obtidos para cada um dos três agentes foi de 160 KB.

A Figura 21 (b) mostra os histogramas do número de consultas DNS, representadas por N_{DNS} , executadas pelos agentes IPv4 de referência, DS e IPv6 nas medições efetuadas à página 6. Observa-se que o agente DS executou um número maior de consultas DNS, com relação aos outros dois agentes, em todo o

processo de medição da página 6. As médias foram de 7, 16 e 6 consultas, respectivamente, para os agentes IPv4 de referência, DS e IPv6.

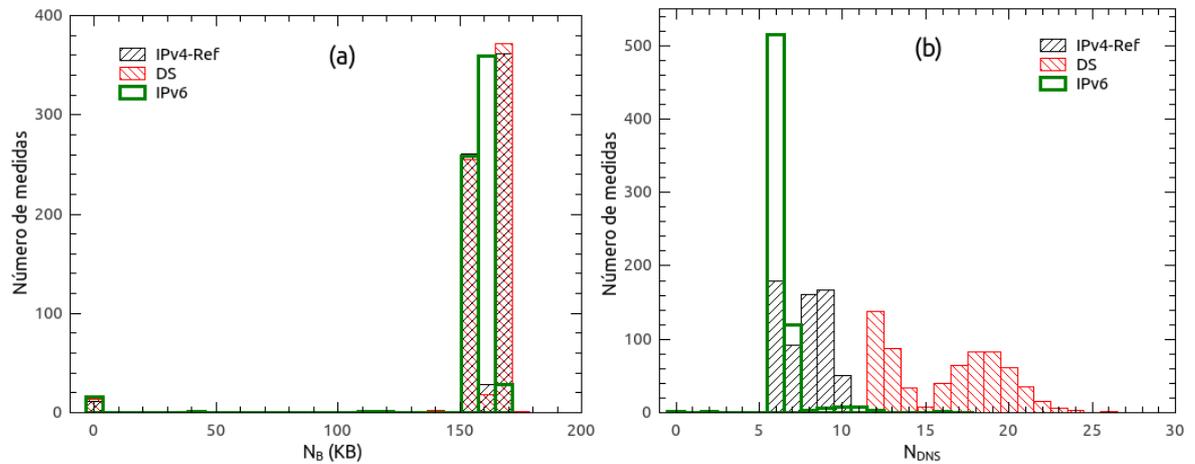


Figura 21. Número de bytes (a) e consultas DNS (b) da página 6

Para as páginas 24 e 69, os agentes DS e IPv6 obtiveram mais do que o dobro de medidas atípicas superiores do tempo de carregamento do que as obtidas pelo IPv4 de referência. Para estas duas páginas, notou-se que as rotas percorridas pelos pacotes até os servidores que as hospedam são diferentes para o IPv4 e para o IPv6.

Especificamente para página 24, foi observado que ela está hospedada em servidores de uma Rede de Fornecimento de Conteúdo (*Content Delivery Network*, CDN¹) para os quais a rota IPv4 ocorre por meio de roteadores localizados no Brasil. Por outro lado, observou-se que quando o IPv6 foi utilizado as rotas para os servidores da página 24 passam por roteadores internacionais o que pode, em alguns casos, influenciar características da rede como, por exemplo, o RTT, a perda de pacotes e a taxa de dados efetiva dos protocolos de transporte e aplicação.

¹CDNs são sistemas de fornecimento de conteúdo baseados em servidores distribuídos pela Internet que tem por objetivo otimizar o desempenho da entrega de conteúdo ao usuário final.

Os histogramas da Figura 22 (a) mostram, para os agentes IPv4 de referência, DS e IPv6, o comportamento do tempo de carregamento para as medições efetuadas à página 24. Observa-se os tempos de carregamento do IPv4 de referência variando no intervalo de 2 a 8 segundos, do DS de 3 a 9 e do IPv6 de 5 a 12 segundos. Com relação às médias do tempo de carregamento, elas foram de 3,8, 5,6 e 6,8, respectivamente, para os agentes IPv4 de referência, DS e IPv6.

A Figura 22 (b) mostra os histogramas do número de *bytes*, representado por N_B , obtidos pelos agentes IPv4 de referência, DS e IPv6 nos acessos à página 24. Observa-se que o comportamento do número de *bytes* recebidos pelos três agentes foi semelhante em todo o processo de medição. As médias relativas ao número de *bytes* recebidos pelos agentes IPv4 de referência, DS e IPv6 foram, respectivamente, de 1.088, 1.093 e 1.064 KB.

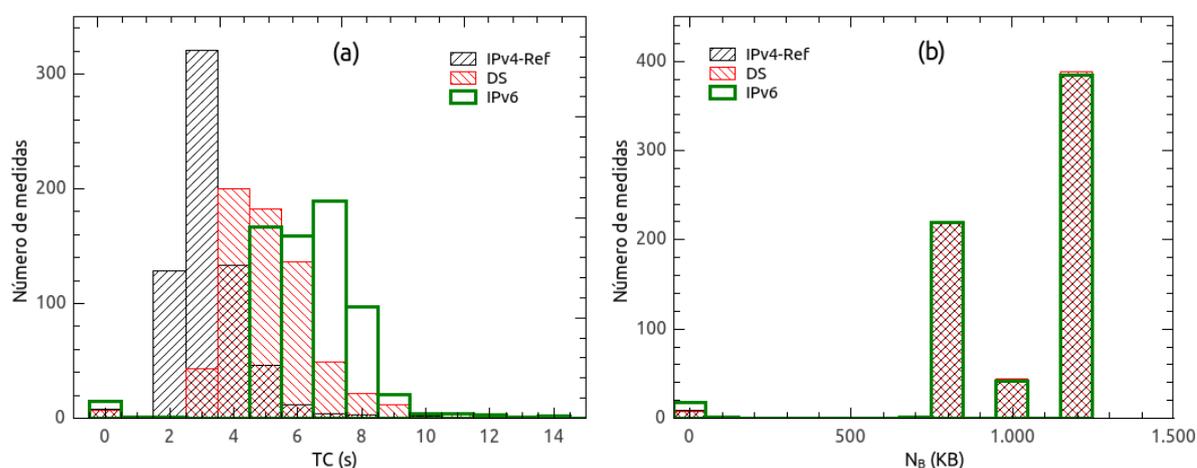


Figura 22. Tempo de carregamento (a) e número de *bytes* obtidos (b) da página 24

A página 69, que apresentou o mesmo comportamento da página 24 para o número de medidas atípicas superiores do tempo de carregamentos, não utiliza os recursos de CDN porém, foi observado que as rotas IPv4 e IPv6 para os

servidores que hospedam a página são disponibilizadas por operadoras distintas de trânsito IP internacional. Isso significa que o IPv4 e o IPv6 podem experimentar comportamentos distintos de RTT e perda de pacotes nos acessos a página *web* 69. Neste ponto cabe observar que cerca 32% dos acessos efetuados pelos agentes DS e IPv6 não carregaram por completo os objetos HTTP da página 69. Para o IPv4 de referência, esse número correspondeu a 10% dos acessos.

Os histogramas da Figura 23 (a) mostram, para os agentes IPv4 de referência, DS e IPv6, o comportamento do tempo de carregamento (*TC*) para as medições efetuadas à página 69. Observa-se para os agentes DS e IPv6 uma maior concentração das medidas do tempo de carregamento no intervalo de 14 a 15 segundos. Com relação às médias do tempo de carregamento, elas foram de 10, 12,4 e 13, respectivamente, para os agentes IPv4 de referência, DS e IPv6.

A Figura 23 (b) mostra os histogramas do número de *bytes*, representado por N_B , obtidos pelos agentes IPv4 de referência, DS e IPv6 nos acessos à página 69. Observa-se um comportamento similar entre os agentes DS e IPv6 para o número de *bytes* recebidos no intervalo de 400 a 750 KB. As médias dos agentes IPv4 de referência, DS e IPv6 foram, respectivamente, de 710, 652 e 659 KB.

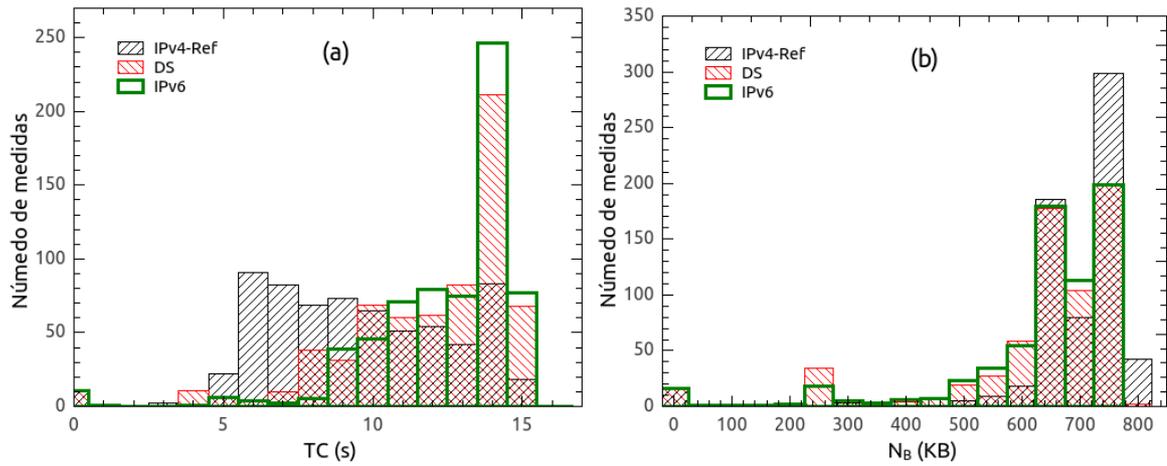


Figura 23. Tempo de carregamento (a) e número de *bytes* obtidos (b) da página 69

5.3 TEMPO PARA COMPLETAMENTO VISUAL

O gráfico da Figura 24 mostra a relação entre as medidas do tempo para completamento visual dos agentes IPv4-2, Pilha Dupla (DS) e IPv6 com relação às medidas obtidas pelo agente IPv4 de referência, para as 100 páginas *web* avaliadas. Na Figura, a relação está representada por $C_{i//IPv4}$ e foi obtida por (1).

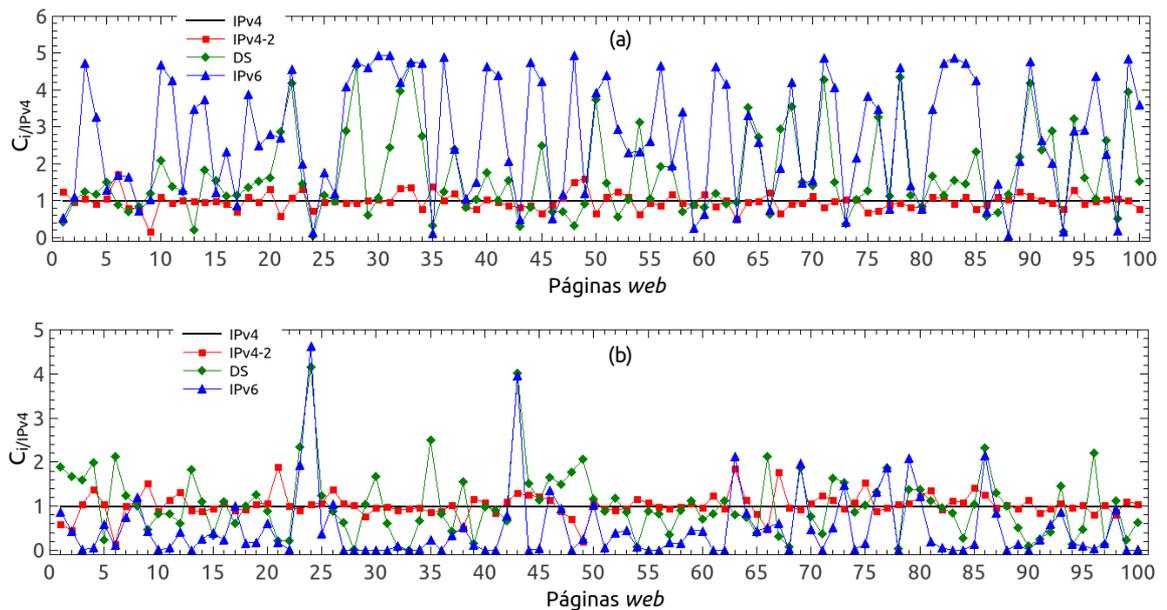


Figura 24. Relação com o IPv4 de referência, das medidas atípicas inferiores (a) e superiores (b) para o tempo de completamento visual

O gráfico da Figura 24 (a) permite observar que as medidas atípicas inferiores do tempo para completamento visual, obtidas pelos agentes DS e IPv6, possuem maior variabilidade com relação àquelas medidas obtidas pelo agente IPv4-2. As medidas obtidas pelo IPv4-2, para todas as páginas *web* testadas, não ultrapassaram o limite de duas vezes o número de medidas atípicas inferiores obtido pelo IPv4 de referência. Com relação ao DS e ao IPv6, 72 e 37% das páginas, respectivamente, mantiveram-se no limite de até duas vezes mais medições atípicas inferiores do que aquelas obtidas pelo IPv4 de referência.

Para as medidas atípicas superiores, obtidas pelos agentes DS e IPv6, observa-se pela Figura 24 (b) variações menores, com relação ao IPv4 de referência, se comparadas com aquelas obtidas para as medidas atípicas inferiores. As páginas *web* que tiveram medidas atípicas superiores com no máximo duas vezes o número daquelas obtidas pelo IPv4 de referência corresponderam a 91 e 95 %, respectivamente, para o DS e para o IPv6. Para o IPv4-2, nenhuma página avaliada obteve um número de medidas atípicas superiores maior do que o dobro daquele obtido pelo IPv4 de referência.

Assim como observado para o tempo de carregamento das páginas *web*, a disponibilidade do conteúdo pode influenciar o comportamento da métrica relacionada ao completamento visual. Esta influência ocorre, principalmente, para as medidas atípicas inferiores dada a forma como o completamento visual é computado. Se poucos objetos são carregados nos instantes iniciais da medição, a página não muda no decorrer do tempo e o sistema calcula o completamento visual total da página como sendo aquele apresentado no início da medição.

A Figura 25 apresenta a relação com o IPv4 de referência, $C_{i/IPv4}$, das medidas atípicas inferiores e superiores do tempo para completamento visual. As curvas das figuras (a) e (b) são relativas às medidas das 100 páginas *web* e as curvas das figuras (c) e (d) são referentes às medidas das 23 páginas *web* com médias do número de *bytes* equivalentes às obtidas pelo IPv4 de referência (considerando uma diferença de até 10% de *bytes* a menos). Os gráficos (a) e (c) mostram que para as páginas *web* com médias semelhantes, o comportamento das medidas atípicas inferiores do completamento visual, para os agentes DS, IPv6 e IPv4-2, tende a convergir.

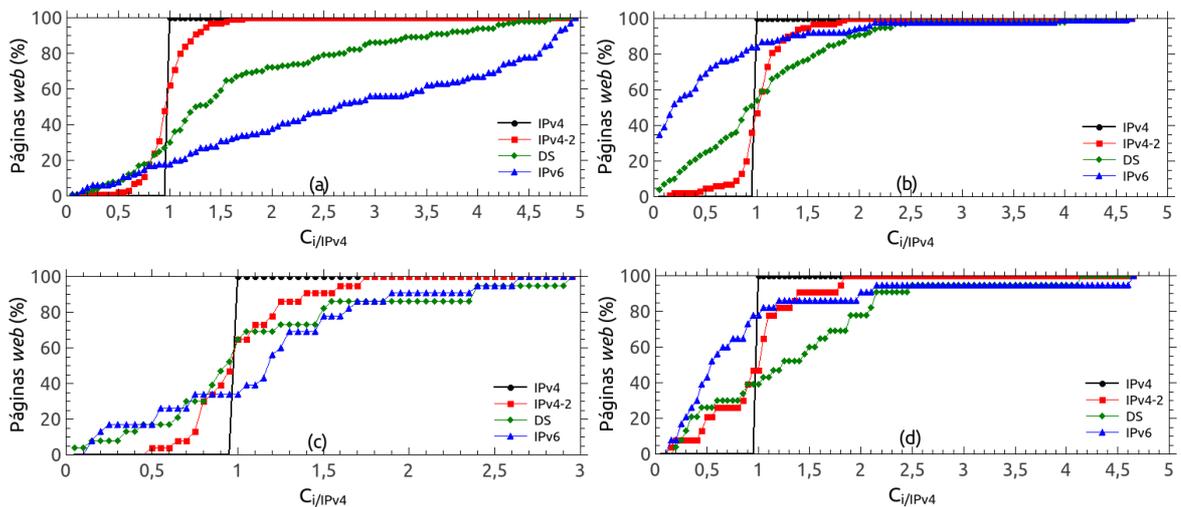


Figura 25. Relação das medidas atípicas inferiores (a) e superiores (b) do tempo de completamento visual para as 100 páginas avaliadas e relação das medidas atípicas inferiores (c) e superiores (d) do tempo de completamento visual para as 23 páginas com média similar do número de *bytes* obtidos

Além da relação observada entre o tempo para completamento visual com o número de *bytes* obtidos das páginas, observou-se também um comportamento bastante semelhante com o tempo de carregamento dos objetos HTTP, conforme mostram as Figuras 18 e 25. Neste caso o que se pode sugerir é que os recursos

computacionais utilizados pelos agentes não influenciaram no tempo de exibição dos objetos que compõem as páginas *web*. Ainda neste sentido, foram observados casos em que as medidas para o tempo de completamento visual foram muito menores ou, até mesmo, com valores iguais a zero, quando comparadas com o tempo de carregamento dos objetos HTTP.

O gráfico da Figura 26 mostra, para as 100 páginas *web* avaliadas, o número de medidas do tempo de completamento visual com valores iguais a zero, representado por $N_{CV=0}$. Esses valores indicam, para esta métrica, que nenhum objeto HTTP recebido da página acessada foi exibido no navegador do usuário. Sendo assim, este comportamento pode ser visto como o impacto negativo mais expressivo que poderia ser causado à experiência de navegação *web* do usuário.

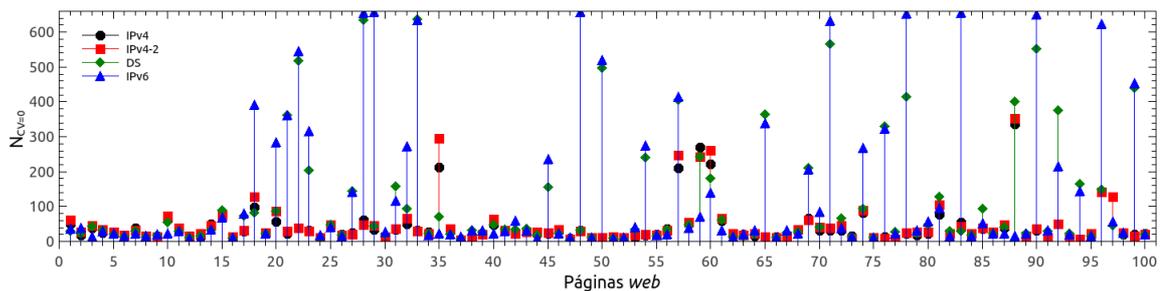


Figura 26. Número de medidas com tempo de completamento visual igual a zero

Observa-se que para os agentes IPv4 de referência e IPv4-2, apenas uma das páginas *web* obteve mais do que 50% das medições comprometidas. Com relação aos agentes DS e IPv6, esses números foram, respectivamente, de 13 e 16 páginas *web*. Também é possível observar que para casos como o da página 35, o IPv6 contribui para uma melhor experiência do usuário, com relação ao IPv4, nos acessos efetuados à página, uma vez que o número de medidas com completamento visual igual a zero foi menor para os agentes DS e IPv6.

A Tabela 9 apresenta informações relativas às 18 páginas *web* que apresentaram medidas do completamento visual com valores iguais a zero em mais de 50% das medições, considerando os agentes DS e IPv6. Na Tabela consta também a localização das páginas *web*, obtida por meio do acesso manual à página e confirmada via análise, também manual, da rota até o seu endereço IP de destino. Além disso, é apresentada para cada uma das páginas a informação sobre o uso de Redes de Fornecimento de Conteúdo (*Content Delivery Network*, CDN) e se o conteúdo ainda estava sendo disponibilizado em IPv6 no final das medições realizadas para este trabalho.

Tabela 9. Páginas *web* que tiveram mais de 50% das medidas do tempo para completamento visual com valor igual a zero

PÁGINA	18	21	22	28	29	33	48	50	57	65	71	78	83	88	90	92	96	99				
PAÍS	IN	FR	BR	JP	JP	JP	NZ	US	CA	US	FR	JP	US	RU	HU	PL	IL	CH				
CDN	N	N	N	N	N	N	N	S	N	S	N	N	S	N	N	N	N	N				
IPv6	N	S	S	S	S	N	S	S	S	S	S	S	N	S	S	S	S	S				
	IN – Índia	FR – França		BR – Brasil		JP – Japão		NZ – Nova Zelândia		US – Est. Unidos		CA – Canadá		RU – Rússia		HU – Hungria		PL – Polônia		IL – Israel		CH – Suíça

Observa-se pela Tabela 9 que todas as páginas com exceção da 22 são internacionais. As páginas 18, 33 e 83 tiveram seus endereços IPv6 removidos do DNS, o que pode sugerir que eles foram utilizados apenas para testes e posteriormente foram desativados por questões de instabilidade. As páginas 50 e 65, mesmo sendo disponibilizadas via CDN, apresentaram instabilidades nos acessos, inclusive em testes efetuados de forma manual, complementares às medições. Analisando-se as rotas IPv6 utilizadas para alcançar alguns servidores *web* da CDN que hospedam os objetos das páginas 50 e 65, observou-se que o caminho percorrido utilizou rotas internacionais, o que não acontece quando o IPv4 é utilizado.

5.4 NÚMERO DE *BYTES*

A Figura 27 mostra para os agentes IPv4-2, DS e IPv6, a relação das medidas atípicas inferiores e superiores, do número de *bytes*, com as medidas atípicas obtidas pelo agente IPv4 de referência. Na Figura, a relação está representada por $N_{i/IPv4}$ e é mostrada para cada uma das 100 páginas *web* avaliadas.

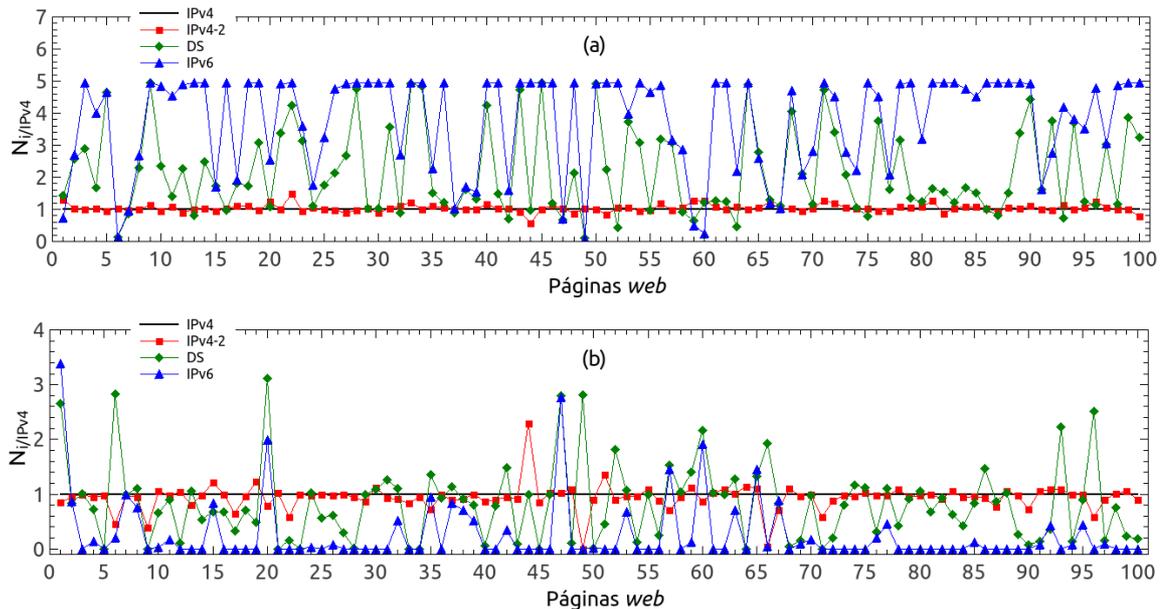


Figura 27. Relação com o IPv4 de referência, das medidas atípicas inferiores (a) e superiores (b) para o número de *bytes*

Pela Figura 27 observa-se que o comportamento das medidas atípicas, com relação ao agente IPv4 de referência, é distinto para os agentes IPv4-2, DS e IPv6. Para o agente IPv4-2, nenhuma página *web* apresentou um número de medidas atípicas inferiores maior do que o dobro daquele obtido pelo agente IPv4 de referência. Os agentes DS e IPv6, por sua vez, apresentaram, respectivamente, 44 e 83 páginas *web* com um número de medidas atípicas inferiores maior do que o dobro daquele obtido pelo IPv4 de referência. Para as

medidas atípicas superiores, observou-se que o agente IPv4-2 apresentou apenas uma página *web* com mais do que o dobro das medidas atípicas obtidas pelo agente IPv4 de referência. O número de páginas *web* com este mesmo comportamento, considerando os agentes DS e IPv6 foi, respectivamente, de 8 e 2 páginas.

Considerado o atual período de transição do IPv4 para o IPv6, no qual nem todos os servidores *web* possuem suporte a nova versão do IP, era esperado que as medidas atípicas inferiores do agente IPv6 se mostrassem em maior número do que aquelas obtidas pelo IPv4. Este fato pode ser observado na Figura 27 (a), na qual para 40 das 100 páginas *web* as medidas atípicas inferiores do número de *bytes*, para o agente IPv6, chegaram ao limite de cinco vezes o número das medidas atípicas obtidas pelo agente IPv4 de referência. Isso significa que para as 40 páginas mencionadas, todas as medições efetuadas pelo agente IPv6 foram atípicas.

Para o agente DS, apenas duas páginas tiveram 100% de medidas do número de *bytes* classificadas como atípicas porém, 44 páginas apresentaram um número de medidas atípicas inferiores maior do que o dobro daquele obtido pelo IPv4 de referência. Para o número de *bytes*, as medidas atípicas inferiores indicam que algum conteúdo deixou de ser obtido, o que não seria esperado para o agente DS, uma vez que ele opera com as duas versões do protocolo IP.

Neste sentido, observou-se para o agente DS que 34 das 44 páginas *web* com medidas atípicas inferiores do número de *bytes* maiores que o dobro das obtidas pelo IPv4 de referência, não tiveram seus objetos HTTP carregados por completo, atingindo o tempo limite estabelecido para as medições em mais de

20% dos acessos efetuados. Também foi observado para 10 das 44 páginas, que o limite estabelecido para medidas atípicas inferiores mostrou-se muito restritivo, considerando diferenças muito pequenas, no número de *bytes*, como medidas atípicas.

A Tabela 10 mostra as 44 páginas *web* que apresentaram um número de medidas atípicas inferiores, do número de *bytes*, maior do que o dobro daquele obtido pelo IPv4 de referência. Na Tabela são mostradas, de forma separada, as páginas que apresentaram o Carregamento Parcial (CP) dos objetos HTTP, pelo agente DS, e aquelas cujo Limite para Medidas Atípicas (LA) mostrou-se muito restritivo na classificação das medidas atípicas inferiores do número de *bytes*.

Tabela 10. Páginas *web* com comportamento atípico para o número de *bytes*

	Páginas <i>web</i>																					
CP	21	22	23	27	28	31	33	45	48	50	54	57	65	69	71	72	76	78	90	92	94	99
	8	19	34	40	43	53	56	64	68	89	97	100										
LA	2	3	5	9	10	12	14	26	51	73												

Ainda considerando o comportamento do agente DS na obtenção de *bytes*, porém observando a preferência pelo IPv6 ao IPv4, a Figura 28 mostra em um gráfico de barras empilhadas, o número de *bytes* obtidos por cada versão do protocolo IP. Na Figura, o número de *bytes* está representado por N_B e é mostrado para cada uma das 100 páginas *web* medidas.

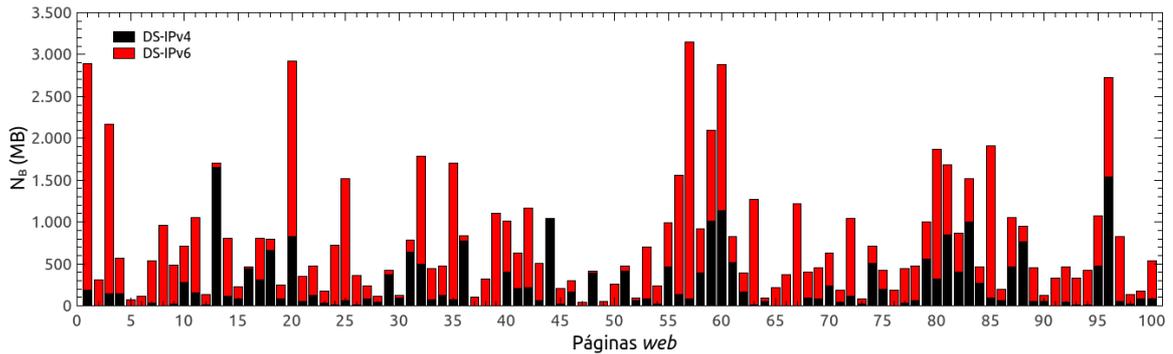


Figura 28. Número de *bytes* obtidos pelo IPv4 e pelo IPv6 no agente DS

Observa-se pela Figura 28 que o número de *bytes* obtidos pelos protocolos IPv4 e IPv6, no agente DS, variam de acordo com cada página *web*. Para a página 1, por exemplo, foram obtidos um total de 181 MB de dados pelo IPv4 e 2.710 MB pelo IPv6. Para a página 13, por sua vez, foram obtidos 1.655 MB pelo IPv4 e 52 MB pelo IPv6.

Conforme descrito em (WING; YOURTCHENKO, 2012), a preferência para o estabelecimento das conexões TCP, no navegador utilizado nas medições, é dada ao IPv6 contanto que as características da rede permitam que tais conexões ocorram dentro de um período máximo de 300 milissegundos. Após esse tempo, o navegador tentará inicializar as conexões utilizando o IPv4. Considerando que nem todos os objetos HTTP das páginas *web* medidas são disponibilizados igualmente em IPv4 e IPv6, não é possível observar pela Figura 28 a preferência pela utilização do IPv6 com relação ao IPv4, dada pelas características da rede.

Tendo em vista estas considerações, a Figura 29 apresenta o número de *bytes* obtidos pelos protocolos IPv4 e IPv6, no agente DS, para as 29 páginas *web* que obtiveram médias semelhantes do número de *bytes* (até 5 % menos *bytes*) nas medições efetuadas pelos agentes DS e IPv6. Na figura, o número de *bytes* está representado por N_B .

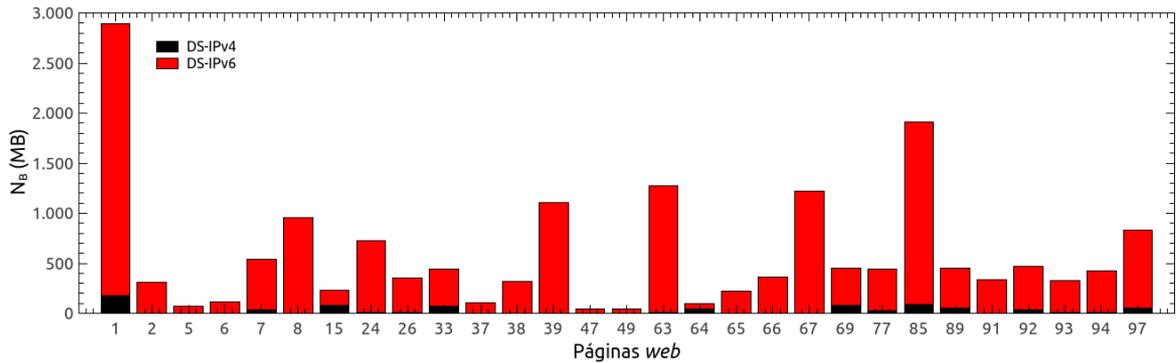


Figura 29. Número de *bytes* obtidos pelo IPv4 e pelo IPv6 no agente DS para páginas com médias semelhantes do número de *bytes*

Observa-se pela Figura 29 que para as 29 páginas *web*, mais de 50% do número de *bytes* foram obtidos pelo IPv6. Constata-se, ainda, que das 29 páginas 24 tiveram acima de 90% do número de *bytes* obtidos pelo IPv6, 3 tiveram entre 80 e 90% do total de *bytes* recebidos pelo IPv6, uma página 64% e uma página 51% do total de *bytes* recebidos pelo IPv6.

6 CONCLUSÕES

Este trabalho apresentou um estudo de campo, comparativo, sobre a utilização dos protocolos IPv4 e IPv6 no acesso a páginas *web*, considerando a perspectiva de um usuário real deste tipo de serviço no atual período de transição do IPv4 para o IPv6. Para que tal estudo pudesse ser realizado, foi desenvolvido um arranjo para a aquisição de informações relativas ao acesso a páginas e aplicações *web* de tal modo que esses acessos fossem efetuados de forma automatizada, com os mesmos recursos utilizados por um usuário real deste tipo de aplicação e, ainda, mediante a utilização dos protocolos IPv4 e IPv6.

Para a aquisição e armazenagem das informações, foram desenvolvidos programas em *shell script* que, além de coordenar a execução dos testes, são capazes de processar e armazenar os resultados relativos aos acessos contínuos às páginas *web* analisadas. Para que o arranjo pudesse efetuar os acessos da mesma forma pela qual um usuário real o faz, sistemas operacionais e navegadores *web* com recursos semelhantes aos utilizados por esses usuários foram utilizados.

Os resultados obtidos pelo trabalho são relativos às métricas do tempo de carregamento das páginas, tempo para completamento visual delas no navegador *web* e número de *bytes* obtidos das 100 páginas *web* mundialmente mais visitadas, com suporte ao IPv6, quando acessadas por meio do IPv6 e da Pilha Dupla (IPv4 e IPv6 juntos), em comparação aos acessos efetuados apenas pelo IPv4. Para que os comportamentos observados no IPv6 e na Pilha Dupla pudessem ser comparados ao comportamento do IPv4, foi proposto o uso de métricas relativas, calculadas com base em intervalos arbitrários de medidas

típicas. As análises utilizando o método proposto, basearam-se nas métricas do tempo de carregamento das páginas, quantidade de *bytes* obtidos e também no tempo de exibição dessas páginas no navegador do usuário. Os resultados mostraram que a utilização do IPv6, sozinho ou em Pilha Dupla, influenciou o número de medições atípicas obtidas para as três métricas analisadas.

Com relação ao tempo de carregamento conclui-se que o fator de maior impacto, principalmente no que se refere aos tempos mais baixos obtidos pelo IPv6 e pela Pilha Dupla, estão relacionados com o fato do conteúdo das páginas *web* não ter sido recebido em sua totalidade. Neste aspecto foi observado que para a Pilha Dupla a porcentagem de páginas *web* com um número de medições atípicas inferiores maior do que o dobro daquele obtido pelo IPv4 cai de 25 para 5% quando a média do número de *bytes* obtidos dessas páginas é semelhante para o IPv4 e para a Pilha Dupla. Para o IPv6 a porcentagem diminuiu de 57 para 20% também considerando as médias semelhantes do número de *bytes* para o IPv4 e o IPv6.

Para o tempo de completamento visual, a utilização do IPv6 impactou de forma negativa em 50% dos acessos efetuados a 18 das 100 páginas medidas. Nesse caso, e considerando a perspectiva do usuário no acesso a essas páginas, nenhum conteúdo teria sido exibido no navegador em metade dos acessos efetuados. Observou-se, ainda, que das 18 páginas mencionadas apenas uma foi acessada pelo IPv6 utilizando rotas nacionais, o que sugere uma maior instabilidade do acesso *web* às páginas hospedadas fora do Brasil quando o IPv6 é utilizado.

A análise do número de *bytes* obtidos mostrou que 44% das páginas *web* tiveram um número de medições atípicas inferiores maior do que o dobro daquele obtido pelo IPv4 de referência, considerando as medidas obtidas pelo agente DS. Dessas páginas, 34% deixaram de obter parte do conteúdo dos servidores HTTP, que não responderam às requisições no tempo máximo estabelecido para as medições. Além disso, para 27 das 29 páginas *web* com médias de *bytes* semelhantes entre a Pilha Dupla e o IPv6, observou-se que mais de 90% dos dados trafegaram pelo IPv6.

6.1 CRÍTICAS AO MÉTODO DE CLASSIFICAÇÃO DAS MEDIDAS

O método proposto na Seção 3.3, para classificação das medidas, mostrou-se eficaz na identificação de comportamentos típicos e atípicos do acesso *web* quando o IPv6 é utilizado. No entanto, para alguns casos como o de páginas *web* com conteúdo estático, os valores obtidos nas medições se mantiveram constantes. Neste sentido, observou-se que pequenas variações obtidas pelos agentes DS e IPv6, com relação ao IPv4 de referência, fizeram com que grande parte das medidas obtidas por eles fossem consideradas como atípicas. Este comportamento foi percebido principalmente para as medidas atípicas inferiores dada a indisponibilidade do conteúdo acessado via IPv6, seja ela causada pelo fato do servidor remoto não suportar o protocolo ou mesmo por instabilidades que possam ter ocorrido no momento do acesso. Para aprimorar o método de classificação das medidas proposto, sugere-se a utilização de limites variáveis para as medidas atípicas inferiores e superiores.

6.2 PERSPECTIVAS PARA CONTINUIDADE DO TRABALHO

Os resultados obtidos neste trabalho limitam-se ao Sistema Autônomo do qual as medições foram originadas e também às páginas *web* avaliadas. Com relação ao arranjo e programas desenvolvidos, eles podem ser aplicados em qualquer ambiente com acesso IPv4 e IPv6 à Internet para medições individuais ou em massa de qualquer tipo de aplicações *web*.

Como continuação deste trabalho, o método proposto pode ser aplicado considerando um número maior de pontos de observação em diferentes locais, preferencialmente em outros continentes. Neste sentido, os dados obtidos podem ser correlacionados no objetivo de identificar problemas em rotas específicas da Internet ou mesmo nas páginas *web* avaliadas. Além disso, tendo em vista o volume expressivo de transmissões de vídeo que são efetuadas por meio do protocolo HTTP, o método desenvolvido neste trabalho poderia ser aplicado para analisar o desempenho do IPv6 em páginas *web* cujo conteúdo predominante seja o de aplicações de vídeo.

TRABALHO PUBLICADO

PIRANI, D.; ABBADE, M. L. F. Análise De Campo Do Acesso *Web* Por Meio De Uma Estrutura IP Em Pilha Dupla. XXXI Simpósio Brasileiro de Telecomunicações – SBrT2013, DOI: 10.14209/sbrt.2013.81, 2013.

REFERÊNCIAS

- ^AALMES, G. et al. "RFC 2679. A One-way Delay Metric for IPPM," 1999.
- ^BALMES, G. et al. "RFC 2681. A Round-trip Delay Metric for IPPM," 1999.
- AHUJA, S. P.; DENDUKURI, K. An Empirical Evaluation of IPv6 in Linux and Windows Environments, Annual Review of Communications, Volume 59, p. 361-370, Novembro, 2006.
- ALEXA, "The Top 1 Million Sites on the Web", Alexa – The Web Information Company. Disponível: <http://www.alexa.com/topsites>, acessado: 29/07/2013.
- AMS-IX, "Aggregated traffic on all AMS-IX connected networks ports," AMS-IX Amsterdam. Disponível: <https://www.ams-ix.net/technical/statistics>, acessado: 09/09/2013.
- APNIC, "IP Resource Per Country Distribution Report, IPv6 Users by Country," APNIC, Setembro, 2013. Disponível: <http://labs.apnic.net/dists/v6dcc.html>, acessado: 08/09/2013.
- BAGNULO, M. et al. "RFC 6147. DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers," 2011.
- BAO, C. et al. "RFC 6052. IPv6 Addressing of IPv4/IPv6 Translators," 2010.
- DE-CIX, "Traffic Statistics," DE-CIX Frankfurt, Setembro, 2013. Disponível: <http://www.de-cix.net/about/statistics>, acessado: 09/09/2013.
- DEERING, S.; FENNER, W.; HABERMAN, B. "RFC 2710. Multicast Listener Discovery (MLD) for IPv6," 1999.
- DEERING, S.; HINDEN, R. "RFC 2460. Internet Protocol, Version 6 (IPv6) Specification," 1998.
- DHAMDHARE, A. et al. Measuring the deployment of IPv6: topology, routing and performance. Proceeding ACM IMC'12, p. 537-550, Novembro, 2012, Boston, Massachusetts, USA.
- DURAND, A. et al. "RFC 3053. IPv6 Tunnel Broker," 2011.
- FARINACCI, D. et al. "RFC 2784. Generic Routing Encapsulation (GRE)," 2000.
- FIELDING, R. et al. "RFC 2616. Hypertext Transfer Protocol - HTTP/1.1". Junho, 1999.
- GEBERT, S. et al. Internet Access Traffic Measurement and Analysis. Traffic Monitoring and Analysis Lecture Notes in Computer Science Volume 7189, p. 29-42, 2012.

GOOGLE, "A adoção do IPv6," GOOGLE, Setembro, 2013. Disponível: <http://www.google.com/ipv6/statistics.html>, acessado: 09/09/2013.

HAWKINSON, J.; BATES, T. "RFC 1930. Guidelines for creation, selection, and registration of an Autonomous System (AS)," 1996.

HUITEMA, C. "RFC 4380. Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)," 2006.

HUSTON, G. "A Primer on IPv4, IPv6 and Transition," PoliTICs, ed. 15, Junho, 2013.

LABER, M. "Global IPv6 Deployment Progress Report - Networks Running IPv6," Hurricane Electric Internet Services, Julho, 2013. Disponível: <http://bgp.he.net/ipv6-progress-report.cgi>, acessado: 09/09/2013.

LABOVITZ, C. et al. Internet inter-domain traffic. SIGCOMM '10 Proceedings of the ACM SIGCOMM 2010 conference, p. 75-86, 2010.

LAW, Y. et al. Empirical Performance of IPv6 vs. IPv4 under a Dual-Stack Environment. Communications, 2008. ICC '08. IEEE International Conference on Communications, Pequim, China, p. 5924-5929, Maio, 2008.

LI, X. et al. "RFC 6145. IP/ICMP Translation Algorithm," 2011.

MAIER, G. et al. On dominant characteristics of residential broadband internet traffic. IMC '09 Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference, p. 90-102, 2009.

MEENAN, P. "How fast is your website?". Magazine - Communications of the ACM, p. 49-55, Abril, 2013.

METZ, C. Moving Toward an IPv6 Future. Internet Computing, IEEE, v.7, p. 25-26, Maio, 2003.

NARAYAN, S. et al. TCP/UDP network performance analysis of windows operating systems with IPv4 and IPv6. IEEE 2nd International Conference on Signal Processing Systems (ICSPS), p. 219-222, Julho, 2010.

NIKKHAH, M. et al. Assessing IPv6 Through Web Access A Measurement Study and Its Findings. Proceeding ACM CoNEXT 2011, Dezembro, 2011, Tokyo, Japão.

NORDMARK, E.; GILLIGAN R. "RFC 4213. Basic Transition Mechanisms for IPv6 Hosts and Routers," 2005.

NORDMARK, E. "RFC 2765. Stateless IP/ICMP Translation Algorithm (SIIT)," 2000.

PIRANI, D.; ABBADE, M. L. F. "WProbe, Ferramenta para Automatização de Acessos a Páginas Web". Disponível: <http://sourceforge.net/projects/wprobe>, acessado: 11/12/2013.

PARTRIDGE, C.; JACKSON, A. "RFC 2711. IPv6 Router Alert Option," 1999.

RIPE, "IPv6 Enabled Networks," RIPE NCC, Julho, 2013. Disponível: http://v6asns.ripe.net/v/6?s=_ALL, acessado: 09/09/2013.

SOUMYALATHA, N. et al. IPv6-Based Network Performance Metrics Using Active Measurements. Proceedings of International Conference on VLSI, Communication, Advanced Devices, Signals & Systems and Networking (VCASAN-2013), Volume 258, p. 451-460, 2013.

SUNDARESAN, S. et al. Web performance bottlenecks in broadband access networks. SIGMETRICS '13 Proceedings of the ACM SIGMETRICS/international conference on Measurement and modeling of computer systems, p. 383-384, Junho, 2013.

WADDINGTON, D. G.; CHANG, F. Realizing the Transition to IPv6. IEEE Communications Magazine , v. 40, p. 138-147, Agosto, 2002.

WANG, Y. et al. Understanding Current IPv6 Performance: A Case Study from CERNET. Proceedings of 10th IEEE Symposium on Computers and Communications, ISCC 2005, p. 71-76, Junho, 2005.

WADDINGTON D. G.; CHANG, F. Realizing the Transition to IPv6. Communications Magazine, IEEE, p. 138-147, Agosto, 2002.

WING, D.; YOURTCHENKO, A. "RFC 6555. Happy Eyeballs: Success with Dual-Stack Hosts," 2012.

WU, T. et al. A measurement study of network efficiency for TWAREN IPv6 backbone. International Journal of Network Management, vol. 5, p. 411-419, Dezembro, 2005.

YASINOVSKYY, R. et al. A comparison of VoIP performance on IPv6 and IPv4 networks. AICCSA 2009, ACS/IEEE International Conference on Computer Systems and Applications, P. 603-609, Maio, 2009.

ZHOU, X. et al. Estimation of perceived quality of service for applications on IPv6 networks. Proceedings of the ACM international workshop on Performance monitoring, measurement, and evaluation of heterogeneous wireless and wired networks, Malaga, Espanha, p. 74-81, Outubro, 2006.

APÊNDICE A - DESCRIÇÃO DOS PROGRAMAS (*SCRIPTS*) DESENVOLVIDOS

A1 OPERAÇÃO GERAL DOS *SCRIPTS*

Os *scripts* desenvolvidos no presente trabalho tem por objetivo a automatização e coordenação do processo de medição, o processamento e a armazenagem nas informações obtidas e, por fim, a geração das informações necessárias para a análise de campo proposta. Mais especificamente, o *script* denominado *run_tests* tem a função de automatizar as medições, o *script* *get_data* de receber, processar e armazenar os resultados e o *script* *filter_data* tem a função de ler os dados armazenados e organizá-los em um arquivo com Valores Separados por Vírgula (*Comma-separated Values*, CSV). Além dos *scripts* anteriormente mencionados, o método de classificação das medidas obtidas, como típicas ou atípicas, conforme proposto em 3.3, foi implementado no *script* *site_aty_calc*. Esse conjunto de *scripts* foi desenvolvido em linguagem *Bash Script* resultando no pacote de *software* denominado Wprobe2, de código aberto, e que encontra-se disponível para *download* em <http://sourceforge.net/projects/wprobe>.

A Figura 30 ilustra a interação dos *scripts* *run_tests*, *get_data* e *filter_data* considerando a execução de um processo de medição. O *run_tests* verifica a disponibilidade dos agentes e, se todos estiverem disponíveis, envia uma nova solicitação de medição (passo 1). Assim que os agentes terminam o carregamento da página *web* que está sendo testada e os dados estejam disponíveis (passo 2), o *run_tests* aciona o *get_data* como um novo processo no

sistema operacional (passo 3) e a partir deste momento o *run_tests* pode iniciar um novo processo de medição independente do processamento dos dados do teste anterior. O *get_data* processa as informações adquiridas pelo Webpagetest na medição e as armazena no disco local do Servidor WPT (passo 4). Neste ponto o *script filter_data* pode ser executado manualmente para ler as informações das medições efetuadas de uma determinada página e gerar o arquivo CSV contendo as medidas coletadas. O *filter_data* pode ser executado sempre que um novo processo de medição tenha sido concluído, neste caso ele processará os novos dados obtidos e o arquivo CSV será gerado novamente contemplando as novas medidas obtidas.

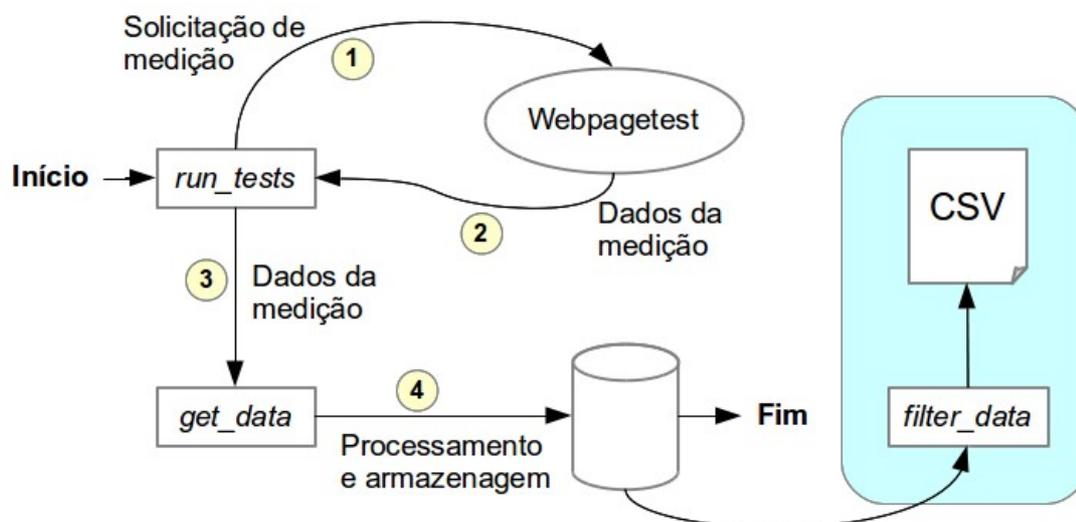


Figura 30. Visão geral da interação entre os *scripts* desenvolvidos

A1.1 SCRIPT RUN_TESTS

O *script run_tests* recebe como parâmetro apenas um arquivo de texto contendo linha a linha as páginas *web* que devem ser medidas naquela rodada de testes. O processo inicia-se com o envio da solicitação de medição da primeira página do arquivo texto. Esse processo é efetuado utilizando a Interface de Programação de Aplicativos (*Application Programming Interface*, API) do Webpagetest, e é executado para cada agente por meio de processos distintos e paralelos do sistema operacional no Servidor WPT. Posteriormente o *script* entra em um laço que verifica segundo a segundo o *status* da medição. Se um dos agentes não receber o teste em até dois segundos após o envio, o processo de medição atual é cancelado em todos os agente e um novo processo é iniciado. Um e-mail de notificação pode ser enviado para posicionar o responsável pela plataforma que o agente em questão não recebeu a solicitação de medição. Sendo o teste aceito pelos agentes, o *script* continua o processo de monitoração para verificar o instante em que o teste é concluído.

Quando um agente termina a medição, o *run_tests* aciona o *get_data*, também como um novo processo, passando a ele como parâmetro o identificador do teste e o diretório para armazenamento das informações obtidas. Assim que todos os agentes terminarem o processo de medição, um novo processo pode ser iniciado para próxima página independente do processamento dos dados do teste anterior. O envio das solicitações de medição por meio de processos paralelos, juntamente com os mecanismos de verificação dos agentes, possibilitam o recebimento simultâneo, com no máximo até 2 segundos de diferença, do testes nos agentes utilizados nas medições.

Envio dos testes para os agentes utilizando o navegador Mozilla Firefox:

```
# Agente IPv4
testid_ipv4=`curl -s --data-urlencode "url=$site" "http://localhost/runtest.php?
location=Wptdriver_IPv4:Firefox.Native&f=xml&fonly=1&private=1&noopt=1&noheaders=1&video=1&
"tcpdump=1"" |xmlstarlet sel -t -v "response/data/testId" &`
# Agente IPv4-2
testid_ipv4_2=`curl -s --data-urlencode "url=$site" "http://localhost/runtest.php?
location=Wptdriver_IPv4_2:Firefox.Native&f=xml&fonly=1&private=1&noopt=1&noheaders=1&video=1
&"tcpdump=1"" |xmlstarlet sel -t -v "response/data/testId" &`
# Agente IPv6
testid_ipv6=`curl -s --data-urlencode "url=$site" "http://localhost/runtest.php?
location=Wptdriver_IPv6:Firefox.Native&f=xml&fonly=1&private=1&noopt=1&noheaders=1&video=1&
"tcpdump=1"" |xmlstarlet sel -t -v "response/data/testId" &`
# Agente DS
testid_ds=`curl -s --data-urlencode "url=$site" "http://localhost/runtest.php?
location=Wptdriver_DStack:Firefox.Native&f=xml&fonly=1&private=1&noopt=1&noheaders=1&video=1
&"tcpdump=1"" |xmlstarlet sel -t -v "response/data/testId" &`
```

Recupera o *status* atual do teste (executado a cada 1 segundo):

```
# Agente IPv4
teststatus_ipv4=`curl -s "http://localhost/testStatus.php?f=xml&test=$testid_ipv4" |xmlstarlet sel -t -v
"response/data/statusCode"`
# Agente IPv4-2
teststatus_ipv4_2=`curl -s "http://localhost/testStatus.php?f=xml&test=$testid_ipv4_2" |xmlstarlet sel -t -v
"response/data/statusCode"`
# Agente IPv6
teststatus_ipv6=`curl -s "http://localhost/testStatus.php?f=xml&test=$testid_ipv6" |xmlstarlet sel -t -v
"response/data/statusCode"`
# Agente_DS
teststatus_ds=`curl -s "http://localhost/testStatus.php?f=xml&test=$testid_ds" |xmlstarlet sel -t -v
"response/data/statusCode"`
```

Conclusão da medição e acionamento do *get_data*:

```
# Teste concluído
if [[ ($teststatus_ipv4 == 200) && ($teststatus_ipv4_2 == 200) && ($teststatus_ipv6 == 200) &&
($teststatus_ds == 200) ]]; then
# Salva os dados dos testes de cada agente
for i in `echo -e
"Testbox_IPv4,$testid_ipv4\nTestbox_IPv4_2,$testid_ipv4_2\nTestbox_IPv6,$testid_ipv6\nTestbox_DS,
$testid_ds"; do
testbox_name=`echo $i |cut -d ',' -f1`
testid=`echo $i |cut -d ',' -f2`

# Cria diretório para armazenar os resultados dos testes de um determinado agente
data_dir="$wprobe2_dir/Data/$testbox_name/$site_name/$test_number"
if [ ! -d $data_dir ]; then
mkdir -p $data_dir
fi
# Baixa os dados em background
$wprobe2_dir/get_data "$data_dir" "$testid" > /dev/null 2>&1 &
```

A1.2 SCRIPT GET_DATA

O *get_data* recebe como parâmetro o identificador do teste que foi concluído e o diretório em que as informações deverão ser armazenadas após serem processadas. Primeiramente o *script* busca as informações da medição na estrutura de armazenamento do Webpagetest, selecionando os dados relevantes para as análises propostas no trabalho. Após os dados serem devidamente armazenados na estrutura de diretórios do Wprobe2, os dados do teste armazenados na estrutura de diretórios do Webpagetest são apagados. A opção por copiar apenas os dados relevantes e apagar todos os dados da medição da estrutura do Webpagetest foi necessária para que a utilização do espaço em disco do servidor fosse otimizada, uma vez que processos contínuos de medição geram um grande volume de informações.

Resgata dados da estrutura de armazenamento do Webpagetest:

```
# Armazena os resultados
cd $data_dir
# Dados "crus" da página em XML
curl -s "http://localhost/results.php?f=xml&test=$testid" > raw_page_data.xml
# Dados "crus" dos objetos em XML
curl -s "http://localhost/results.php?f=xml&requests=1&test=$testid" > raw_object_data.xml
# Compacta dados "crus" dos objetos
nice -n 15 tar jcf raw_object_data.xml.tar.bz2 raw_object_data.xml > /dev/null 2>&1 && rm -f
raw_object_data.xml > /dev/null 2>&1
# Dados do teste em formato HAR
curl -s "http://localhost/export.php?test=$testid" > test_data.har
# Compacta dados HAR
nice -n 15 tar jcf test_data.har.tar.bz2 test_data.har > /dev/null 2>&1 && rm -f test_data.har > /dev/null
2>&1
# Timeline dos eventos do navegador em JSON
curl -s "http://localhost/getTimeline.php?test=$testid&run=1" > devtools_timeline.json
# Compacta eventos JSON
nice -n 15 tar jcf devtools_timeline.json.tar.bz2 devtools_timeline.json > /dev/null 2>&1 && rm -f
devtools_timeline.json > /dev/null 2>&1
# Diretório onde ficam as imagens no servidor WPT
store_img_dir="${testid:0:2}/${testid:2:2}/${testid:4:2}/${testid:7:2}/${testid:10:100000}"
# Screen shot da página completamente carregada
wget -q "http://localhost/results/$store_img_dir/1_screen.jpg" -O fully_loaded.jpg
# Screen shot da página assim que os objetos acabaram de chegar
wget -q "http://localhost/results/$store_img_dir/1_screen_doc.jpg" -O document_complete.jpg
# Dados da captura do tcpdump
```

```
wget -q "http://localhost/result/$testid/1.cap" -O 1.cap
# Compacta dados da captura do tcpdump
nice -n 15 tar jcf tcpdump.pcap.tar.bz2 tcpdump.pcap > /dev/null 2>&1 && rm -f tcpdump.pcap > /dev/null
2>&1
```

Gera arquivo CSV com os dados do tcpdump:

```
# Processa o arquivo de captura do tcpdump
# Total de consultas DNS
total_dns=`nice -n 15 tshark -r 1.cap -R "udp.dstport == 53" |wc -l`
if [ -z $total_dns ]; then total_dns=0; fi
# Total de conexões TCP estabelecidas
total_tcpconnv4=`nice -n 15 tshark -r 1.cap -q -z conv,tcp,ip |grep "<->" |grep "http" |wc -l` # IPv4
total_tcpconnv6=`nice -n 15 tshark -r 1.cap -q -z conv,tcp,ipv6 |grep "<->" |grep "http" |wc -l` # IPv6
if [ -z $total_tcpconnv4 ]; then total_tcpconnv4=0; fi
if [ -z $total_tcpconnv6 ]; then total_tcpconnv6=0; fi
# Total de retransmissões TCP
total_retransv4=`nice -n 15 tshark -r 1.cap -R "ip and tcp.srcport == 80 or tcp.srcport == 443 and
tcp.analysis.retransmission" |wc -l` # IPv4
total_retransv6=`nice -n 15 tshark -r 1.cap -R "ipv6 and tcp.srcport == 80 or tcp.srcport == 443 and
tcp.analysis.retransmission" |wc -l` # IPv6
if [ -z $total_retransv4 ]; then total_retransv4=0; fi
if [ -z $total_retransv6 ]; then total_retransv6=0; fi
# Total de bytes obtidos
total_bytesv4=`nice -n 15 tshark -r 1.cap -R "ip and tcp.srcport == 80 or tcp.srcport == 443 and tcp.len > 0"
-T fields -E separator="," -e "tcp.len" |awk '{s+=$1} END {print s}'` # IPv4
total_bytesv6=`nice -n 15 tshark -r 1.cap -R "ipv6 and tcp.srcport == 80 or tcp.srcport == 443 and tcp.len >
0" -T fields -E separator="," -e "tcp.len" |awk '{s+=$1} END {print s}'` # IPv6
if [ -z $total_bytesv4 ]; then total_bytesv4=0; fi
if [ -z $total_bytesv6 ]; then total_bytesv6=0; fi
echo "DNS lookups,TCP conn IPv4,TCP conn IPv6,Retrans IPv4,Retrans IPv6,Bytes IPv4,Bytes IPv6" >
tcpdump_data.csv
echo "$total_dns,
$total_tcpconnv4,$total_tcpconnv6,$total_retransv4,$total_retransv6,$total_bytesv4,$total_bytesv6" >>
tcpdump_data.csv
rm -f 1.cap > /dev/null 2>&1
```

Apaga diretório da medição na estrutura do Webpagetest:

```
# Apaga diretório do teste
rm -fr /var/www/html/webpagetest/results/$store_img_dir > /dev/null 2>&1
```

A1.3 SCRIPT FILTER_DATA

O *script filter_data* não interage com os outros *scripts* descritos e que fazem parte, efetivamente, do processo de medição. Esta aplicação é executada manualmente, o que pode ser feito a qualquer momento, uma vez que existam dados de medições disponíveis. Como parâmetros de entrada, o *filter_data* recebe a páginas *web* para a qual se deseja gerar o CSV com as medidas, a

intervalo de medições que se deseja considerar, o diretório onde estão armazenadas as informações resgatadas pelo *get_data* e por fim o diretório no qual o arquivo CSV deverá ser salvo.

O *filter_data* processa as informações armazenadas na estrutura de diretórios do Wprobe2 e gera um arquivo CSV com as métricas descritas na Tabela 8. Este CSV é utilizado pelo *script site_aty_calc* que faz a classificação das medidas como típicas e atípicas, conforme proposto em 3.3. Ele também pode ser utilizado diretamente em outras análises que sejam convenientes.

Processamento das informações e armazenamento em arquivo CSV:

```
# Medidas do Webpagetest
loadTime=`xmlstarlet sel -t -v "response/data/run/firstView/results/loadTime" $data_dir/$testbox/$site/
$test_number/raw_page_data.xml`
bytesIn=`xmlstarlet sel -t -v "response/data/run/firstView/results/bytesIn" $data_dir/$testbox/$site/
$test_number/raw_page_data.xml`
requests=`xmlstarlet sel -t -v "response/data/run/firstView/results/requests" $data_dir/$testbox/$site/
$test_number/raw_page_data.xml`
SpeedIndex=`xmlstarlet sel -t -v "response/data/run/firstView/results/SpeedIndex" $data_dir/$testbox/$site/
$test_number/raw_page_data.xml`
VisualComplete=`xmlstarlet sel -t -v "response/data/run/firstView/results/visualComplete" $data_dir/
$testbox/$site/$test_number/raw_page_data.xml`
TTFB=`xmlstarlet sel -t -v "response/data/run/firstView/results/TTFB" $data_dir/$testbox/$site/
$test_number/raw_page_data.xml`
score_cdn=`xmlstarlet sel -t -v "response/data/run/firstView/results/score_cdn" $data_dir/$testbox/$site/
$test_number/raw_page_data.xml`
docTime=`xmlstarlet sel -t -v "response/data/run/firstView/results/docTime" $data_dir/$testbox/$site/
$test_number/raw_page_data.xml`
# Armazena medidas do Webpagetest em variável no formato CSV
csv_line="$loadTime,$bytesIn,$requests,$SpeedIndex,$VisualComplete,$SpeedIndexDT,
$VisuallyCompleteDT,$TTFB,$score_cdn,$docTime"
# Comparação de pixel (% de diferença com relação ao IPv4)
pixel_comp=`compare -metric MAE $data_dir/$testbox/$site/$test_number/fully_loaded.jpg
$data_dir/Testbox_IPv4/$site/$test_number/fully_loaded.jpg null: 2>&1 |cut -d " " -f2 |tr -d '(' |awk '{printf
"%0.2f\n", $1}' |head -n 1`
# Converte para porcentagem
pixel_comp=`echo "scale=2; $pixel_comp*100" |bc -l |awk '{printf "%0.2f\n", $1}'`
# Medidas obtidas do tcpdump (já processadas pelo get_data)
tcpdump_data=`sed -n "2 p" $data_dir/$testbox/$site/$test_number/tcpdump_data.csv`
# Medidas obtidas do arquivo HAR relativas aos tempos de DNS, bloqueio, conexão TCP, etc.
har_timings=`./har_timings.pl /tmp/$testbox/$site/$test_number/test_data.har`
# Concatena as medidas de comp. de pixel, tcpdump e HAR com as do Webpagetest
csv_line="$csv_line,$pixel_comp,$tcpdump_data,$har_timings"
# Grava em arquivo
echo $csv_line >> $store_dir/$testbox-$site.csv
```

A1.4 SCRIPT SITE_ATY_CALC

Uma vez que as medidas obtidas no processo de medição de uma ou de várias páginas *web* estejam disponíveis no formato CSV, o *script site_aty_calc* pode ser utilizado para classificá-las como típicas ou atípicas, de acordo com o método proposto em 3.3. Este *script* recebe como parâmetros de entrada a página *web*, o agente e a métrica aos quais as medidas se referem, a porcentagem arbitrária para medidas típicas, o diretório contendo os arquivos CSV gerados pelo *script filter_data*, a quantidade de medidas que se deseja classificar, e o tipo de métrica relativa (medidas típicas, medidas atípicas inferiores ou medidas atípicas superiores) que se deseja contabilizar.

Para contabilizar as medidas, o *script* armazena os valores em um vetor ordenado e, com base no intervalo arbitrário de medidas típicas passado como parâmetro, calcula o intervalo para medidas atípicas. Esse intervalo é dividido igualmente para as medidas atípicas inferiores e superiores, o *script* calcula as posições no vetor que delimitam os intervalos das medidas atípicas inferiores e superiores e, posteriormente, faz a contagem dos valores que se encontram entre os valores estabelecidos pela posição desses limites (medidas típicas), dos que estão acima do limite superior (atípicas superiores) e dos que estão abaixo do limite inferior (atípicas inferiores).

Contagem das medidas atípicas e atípicas para o IPv4 de referência:

```
# Acha posição dos valores para o limite superior e inferior
multiplier=$(bc <<< "scale=2; $perc/100")
subtraction=$(bc <<< "scale=2; $num_measurements*$multiplier")
upper_limit_pos=$(bc <<< "scale=2; $num_measurements-$subtraction")
upper_limit_pos=${upper_limit_pos/\.*} # Ignora casas depois do ponto
lower_limit_pos=$(bc <<< "scale=2; $num_measurements*$multiplier")
lower_limit_pos=${lower_limit_pos/\.*} # Ignora casas depois do ponto
# Pega o valor dos limites superior e inferior com base na posição
upper_limit_value=${array[$upper_limit_pos]}
```

```

lower_limit_value=${array[$lower_limit_pos]}

count=0
ipv4_typical=0
ipv4_atypical_upper=0
ipv4_atypical_lower=0

# Conta as medições típicas, atípicas superiores e atípicas inferiores do IPv4
for value in ${array[@]:0:$num_measurements-1}; do
  if [[ ($value -ge $upper_limit_value) ]]; then
    ipv4_atypical_upper=${$ipv4_atypical_upper+1}
  else
    if [[ ($value -le $lower_limit_value) ]]; then
      ipv4_atypical_lower=${$ipv4_atypical_lower+1}
    else
      ipv4_typical=${$ipv4_typical+1}
    fi
  fi
  count=${$count+1}
done

# Porcentagem de medições atípicas do IPv4
perc_ipv4_aty_low=$(bc <<< "scale=2; $ipv4_atypical_lower/$num_measurements")
perc_ipv4_aty_up=$(bc <<< "scale=2; $ipv4_atypical_upper/$num_measurements")

```

APÊNDICE B - PLATAFORMA WEBPAGETEST

A plataforma de teste de páginas web Webpagetest é um *software* de código aberto que anteriormente era desenvolvido e suportado pelo Google como parte do projeto "*Make the Web Faster*". Originalmente a ferramenta foi desenvolvida pela America Online (AOL) para uso interno e, em 2008, tornou-se uma ferramenta de código aberto mediante o modelo de licença de uso *Berkeley Software Distribution* (BSD). Atualmente ela continua sendo disponibilizada sob licença BSD e é mantida pela comunidade e por diversas empresas parceiras.

Além da versão online da aplicação, que possibilita a execução de testes de desempenho de páginas *web* utilizando agentes distribuídos em diversas localidades, é possível a instalação de uma instância privada do Webpagetest para a execução de testes internos. Independente da forma de uso, o Webpagetest possibilita a parametrização de diversas características do teste como, por exemplo, a localização de onde a página será acessa, o navegador *web* utilizado, o tipo de conexão com a Internet, etc.

A Figura 31 ilustra o esquema organizacional da plataforma Webpagetest. Na figura, é possível observar os elementos envolvidos na submissão dos testes como, o servidor Webpagetest, a interface *web* para submissão de testes, os agentes que efetivamente acessam as páginas *web* remotas e as APIs disponíveis para automatização de testes. Os usuários podem submeter testes manuais por meio da "interface *web* do usuário final" ou então por meio dos "*scripts* personalizados" que fazer uso da "API de automação". O servidor WPT envia os testes para os agentes por meio da "API dos agentes" e os "agentes"

acessadas as “páginas *web* a serem testadas”. Toda a comunicação entre os agentes e o servidor Webpagetest é feita por meio do protocolo HTTP.

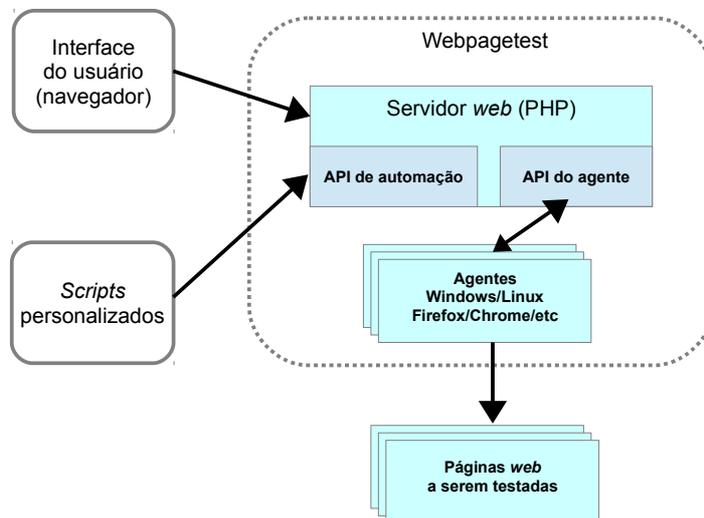


Figura 31. Esquema organizacional do Webpagetest

O Webpagetest é capaz efetuar a aquisição de diversas informações sobre o desempenho da página *web* testada como, por exemplo, o tempo de carregamento dos objetos HTTP, tempo para recebimento do primeiro *byte* da página, o número de *bytes* obtidos, número de requisições HTTP efetuadas, etc. Além disso, a plataforma provê informações sobre o nível de otimização da página, com base nos recursos utilizados pelos desenvolvedores como, por exemplo, o uso de compressão nos objetos HTTP, uso de conexões persistentes, utilização de *cache* dos objetos HTTP, uso de CDN, etc. A ferramenta também faz análises sobre a experiência do usuário com relação à forma como a página é mostrada no navegador. Neste sentido as métricas disponibilizadas são o tempo para completamento visual, que representa o intervalo de tempo do início da navegação até o instante em que a página parou de apresentar mudanças visuais

no navegador do usuário e o índice de velocidade, que representa o tempo médio em que as partes visíveis da página são mostradas para o usuário. As métricas contempladas pelo Webpagetest estão descritas com mais detalhes na página oficial de documentação da ferramenta (<https://sites.google.com/a/webpagetest.org/docs>).

ANEXO

Email do Sr. Geoff Huston autorizando o uso da Figura 10. Modelo de esgotamento dos blocos de endereços IPv4 nos RIRs (HUSTON, 2013).

Content-Type: text/plain; charset="iso-8859-1"
MIME-Version: 1.0 (Mac OS X Mail 6.6 \ (1510\))
Subject: Re: Authorization request.
From: Geoff Huston <gih@apnic.net>
In-Reply-To: <526440E3.8090405@gmail.com>
Date: Mon, 21 Oct 2013 21:07:36 +1100
Content-Transfer-Encoding: quoted-printable
Message-ID: <BA8557E9-A5A9-4433-A8AE-5E347C4CD1F2@apnic.net>
References: <526440E3.8090405@gmail.com>
To: Deivis Fernandes Pirani <devisfp@gmail.com>
X-Mailer: Apple Mail (2.1510)
Return-Path: gih@apnic.net

sure - that would be fine

thanks for asking

Geoff

On 21/10/2013, at 7:45 AM, Deivis Fernandes Pirani <devisfp@gmail.com> = wrote:

> Hello Mr. Huston,
>=20

> My name is Deivis Pirani, I'm a student on Eletrical Engineering = Undergraduation Program at Pontif=EDcia Universidade Cat=F3lica de = Campinas (PUC).

> I'm researching about IPv6 and would like to use some graphs from your = blog so I'm comming to ask for your authorization.
>=20

> Thank you very much.

>=20

> ---=20

> Deivis Fernandes Pirani