MEC-SETEC
INSTITUTO FEDERAL MINAS GERAIS - *Campus* Formiga
Curso de Ciência da Computação

FERRAMENTA DE AFERIÇÃO PERIÓDICA E AUTOMATIZADA DE MÉTRICAS DA QUALIDADE DE SERVIÇO DA CONEXÃO RESIDENCIAL À INTERNET

Thomas do Vale

Orientador: Prof. Me. Everthon Valadão

Formiga - MG

2023

THOMAS DO VALE

FERRAMENTA DE AFERIÇÃO PERIÓDICA E AUTOMATIZADA DE MÉTRICAS DA QUALIDADE DE SERVIÇO DA CONEXÃO RESIDENCIAL À INTERNET

Monografia do trabalho de conclusão de curso apresentado ao Instituto Federal Minas Gerais - Campus Formiga, como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação.

Orientador: Prof. Me. Everthon Valadão

Formiga - MG

2023

Vale, Thomas do
V149f Ferramenta de aferição periódica e automatizada de métricas da qualidade de serviço da conexão residencial à internet / Thomas do Vale -- Formiga : IFMG, 2023.
75p. : il.

Orientador: Prof. MSc. Everthon Valadão
Trabalho de Conclusão de Curso – Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais – *Campus* Formiga.

1. Internet. 2. QoS. 3. Medições. 4. Par-a-par. 5. DHT. I. Valadão, Everthon. II. Título.

CDD 004

Ficha catalográfica elaborada pela Bibliotecária Msc. Simoni Júlia da Silveira

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS
Campus Formiga
Diretoria de Ensino
Docência Área Acadêmica de Computação
Rua São Luiz Gonzaga, s/n - Bairro São Luiz - CEP 35570-000 - Formiga - MG
- www.ifmg.edu.br

THOMAS DO VALE

Ferramenta de Aferição Periódica e Automatizada de Métricas da Qualidade de Serviço da Conexão Residencial à Internet

Trabalho de Conclusão de Curso apresentado ao Instituto Federal de Minas Gerais - Campus Formiga, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

APROVADO em: 27 de junho de 2023.

BANCA EXAMINADORA

Prof. Everthon Valadão dos Santos (orientador, IFMG)

Prof.ª Danielle Costa de Oliveira (IFMG)

Prof.º Ricardo Pagoto Marinho (IFMG)

Este trabalho é dedicado primeiramente a Deus e após ele a meus pais Gilberto e Eunice e também aos meus tios Gilmar e Elizabete. Todos foram imprescindíveis para a realização deste projeto.

Agradecimentos

Primeiramente gostaria de agradecer a Deus pela força, pela inteligência e pela oportunidade de concluir mais essa etapa em minha vida. Agradeço a meu pai Gilberto do Vale por todo o suporte e orientação, que se fizeram vitais para que eu sempre estivesse no caminho certo e pudesse me dedicar aos estudos. Agradeço à minha mãe Eunice, pois seus esforços permitiram minha permanência no curso, especialmente durante a Pandemia. Agradeço também a meus tios Gilmar e Elizabete Veillard que sempre me apoiaram, principalmente nos momentos mais desafiadores dessa jornada. Também gostaria de agradecer ao professor Everthon Valadão por seu notável empenho como orientador.

"Se vi mais longe foi por estar de pé sobre ombros de gigantes."
Isaac Newton

Resumo

A Anatel regulamenta a Qualidade de Serviço (QoS) mínima que os Provedores de Acesso à Internet (ISPs) devem manter. Todavia, nos meios populares de aferição como o site Speedtest.net, há uma possível interferência nos resultados do teste ao se aferir contra um servidor hospedado na própria infraestrutura do ISP. A aferição realizada dessa maneira não captura a qualidade do acesso à internet pública, contratada pelo cliente, mas sim a qualidade do acesso à rede interna privada do ISP. Além disso, as ferramentas de aferição convencionais não são periódicas, limitando a avaliação da rede a um instante específico (sem informar a qualidade média da conexão), e possuindo fragilidades inerentes ao modelo cliente-servidor. Como solução para tal problema, neste trabalho foi desenvolvida uma ferramenta par-a-par (P2P) chamada Peertest para aferição periódica das métricas de qualidade do serviço prestado pelo ISP. A rede DHT do BitTorrent foi utilizada como ponto de encontro dos pares da Peertest e o STUN seguido da técnica UDP *Hole Punching* visou o alcance da conectividade fim-a-fim entre eles, mesmo que estivessem atrás de NATs, possibilitando as aferições entre os pares. A ferramenta desenvolvida foi capaz de aferir de forma mais realista as métricas de latência e perda de pacotes, registrando um ritmo circadiano e com valores mais heterogêneos que a popular ferramenta Speedtest.net. O protótipo foi validado em ambiente operacional relevante (par em residência and par na Amazon AWS). Já em relação às velocidades de *download* e *upload*, nos testes de campo tais aferições da ferramenta Peertest ficaram limitadas a um platô, afetada por alguma limitação específica no ambiente do experimento, devido a provável *traffic shaping* aplicado por alguns ISPs. Além da ferramenta desenvolvida, foi documentado o uso das técnicas de Tradução de Protocolo de Transporte e do UDP Hole Punch, bem como diversas particularidades encontradas em ISPs para se viabilizar conexão fim-a-fim. Também é apresentado um algoritmo de seleção de par que pode subsidiar soluções semelhantes e derivativas. A ferramenta pode ser obtida e utilizada diretamente via uma imagem de contêiner Docker. Já o código-fonte da ferramenta, bem como os resultados do experimento, estão disponibilizadas no GitHub.

Palavras-chave: Internet, QoS, medições, par-a-par, DHT.

Abstract

In Brazil, the Anatel Agency specifies the minimum Quality of Service (QoS) that internet service providers (ISPs) should maintain. Although there may be potential interferences in internet quality measurements on popular tools such as Speedtest.net, when the user tests against a Speedtest server hosted within the ISP infrastructure, they are actually evaluating the quality of access to their intranet, rather than the actual quality of internet access they are paying for. Furthermore, conventional benchmarking tools are not periodic, limiting the network assessment to a specific instant (without capturing the average connection quality), and it also has the limitations of the client-server model. As a solution to this problem, in this work a peer-to-peer (P2P) measurement tool named Peertest has been developed for periodic measuring of metrics related to the quality of service maintained by the ISP in a typical residential internet access connection. The BitTorrent DHT network was leveraged as a rendezvous point for Peertest peers and STUN followed by the UDP Hole Punch technique aimed to achieve end-to-end connection between them, even if they were behind NATs, so they could measure one against the other. The developed tool was able to measure latency and packet loss metrics in a more realistic manner, reporting a circadian rhythm and more heterogeneous values in comparison with Speedtest.net tests. The prototype was validated in a relevant operating environment (peer at home and peer on Amazon AWS). In the field tests, the download and upload speeds were limited due to some specific limitations in the experiment environment. This was likely due to traffic shaping applied by some ISPs. In addition to the developed tool, the utilization of Transport Protocol Translation and UDP Hole Punch techniques was documented, along with several peculiarities observed in ISPs in order to achieve end-to-end connection. Furthermore, a pair selection algorithm that is capable of accommodating both similar and derivative solutions is also presented. The tool can be obtained directly via a Docker container image. The tool's source code and the results of the experiment are available on GitHub.

Keywords: Internet, QoS, measurement, peer-to-peer, DHT.

Lista de ilustrações

Lista de quadros

Lista de abreviaturas e siglas

ANATEL	Agência Nacional de Telecomunicações
API	*Aplication Programming Interface*
AS	*Autonomous System*
CGNAT	*Carrier Grade Network Address Translation*
CRON	Serviço do Linux encarregado de executar programas periodicamente
DHT	*Distributed Hash Table*
ESAQ	Entidade de Suporte à Aferição da Qualidade
GNU	*GNU's not UNIX*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
LAN	*Local Area Network*
Mosh	*Mobile Shell*
MSS	*Maximum Segment Size*
MTU	*Maximum Transmission Unit*
NAT	*Network Address Translation*
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
NPM	*Node Package Manager*
PON	*Passive Optical Network*
POSIX	*Portable Operating System Interface*
PPP	Prestadora de Pequeno Porte
QoS	*Quality of Service*
RFC	*Request For Comments*
RPI	*Raspberry Pi*

RQUAL	Regulamento de Qualidade dos Serviços de Telecomunicações
RTT	*Round-Trip Time*
SLA	*Service Level Agreement*
SOCKS4	*Socks Protocol version 4*
SOCKS5	*Socks Protocol version 5*
STUN	*Session Traversal Utilities for NAT*
TCC	Trabalho de Conclusão de Curso
TCP	*Transmission Control Protocol*
TI	Tecnologia da Informação
TOR	*The Onion Routing*
UDP	*User Datagram Protocol*

Sumário

1 Introdução

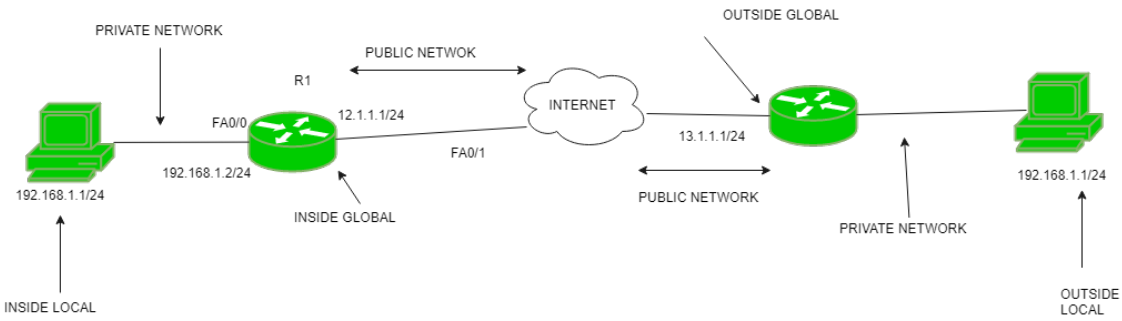
São direitos do consumidor, segundo o Marco Civil da Internet (BRASIL, 2014): a manutenção da qualidade contratada de acesso à internet e a neutralidade de rede. Ou seja, o provedor deve tratar com isonomia qualquer pacote de dados, independente da origem, destino, conteúdo, hospedeiro ou aplicação. Porém, segundo Roberts J. (2004), os mecanismos para a manutenção da qualidade de serviço da rede são inadequados. Ao utilizar uma política de melhor esforço generalista para todos os nós da rede na busca da diminuição do preço de operação e de capitalização, há o desdobramento de desvantagens críticas. O usuário de uma rede com a política de melhor esforço [como a internet], por si só, não tem garantia da aceitação das suas requisições, da existência de um tempo limite de resposta a ser respeitado, da constância de vazão e nem da disponibilidade do serviço requisitado (MENASCE D., 2002). Desta forma, a qualidade do serviço, sem nenhuma regulamentação, geralmente, tende a ser ruim (ROBERTS J., 2004). Por isso, ao oferecer um serviço de TI, uma empresa deve fazer um Acordo de Nível de Serviço (SLA - *Service Level Agreement*), comprometendo a entregá-lo ao cliente conforme a qualidade definida no documento. Entretanto, no caso de acesso residencial à internet, tipicamente não há uma definição clara do SLA que deveria ser prestado pela provedora de acesso. Por isso, a ANATEL regulamenta a Qualidade de Serviço (QoS - *Quality of Service*) mínima que deve ser entregue pelos provedores aos seus clientes. Caso esse mínimo não esteja sendo cumprido, o cliente pode recorrer administrativa e legalmente para cobrar seus direitos como consumidor.

Atualmente, para o usuário verificar as métricas de qualidade de serviço de internet como latência, variação da latência (*jitter*), vazão e perda de pacotes, a opção mais viável é a utilização de websites *online* como Speedtest.net e beta.simet.nic.br. Há, todavia, dois problemas proeminentes quanto a utilização dessas ferramentas. O primeiro, é que provedores de internet, muitas vezes hospedam dentro de sua intranet (rede interna) servidores de sites como o Speedtest.net. Isso faz com que os resultados do teste pelo site não sejam coerentes com a realidade do cliente. Como o teste é feito dentro da própria intranet do provedor, este produz tipicamente resultados melhores, porque o teste afere somente a qualidade de conexão cliente-provedor, e não a qualidade de conexão cliente-internet. O segundo problema é que, os testes nessas ferramentas não são periódicos, ou seja, toda vez que o cliente desejar aferir sua conexão, ele necessita ativamente visitar os sites e iniciar os testes.

Uma possível abordagem para solucionar o primeiro problema é fazer aferições da qualidade de serviço de acesso à internet não no modelo cliente/servidor, mas sim no modelo par-a-par, entre pares que sejam clientes de provedores diferentes. Desta forma,

há a garantia de que os resultados dos testes sejam da conexão cliente-internet, e não da conexão cliente-provedor. O desafio aqui é fazer uma conexão par-a-par entre nós que estejam atrás de roteadores com o *Network Address Translation* (NAT) habilitado, uma vez que a utilização desse dispositivo viola a comunicação ponta-a-ponta para qual a internet foi projetada. Como explica Silva (2018), nós atrás de NATs (roteadores NAT) ficam isolados em suas redes locais e impossibilitados de se comunicarem diretamente com outros nós na internet, uma vez que o NAT/roteador de borda é o responsável por intermediar essa comunicação. Explicando de forma simples, o NAT faz o mapeamento de uma ponta de comunicação (*endpoint*) local em uma ponta de comunicação pública na rede. Ele guarda esse mapeamento em uma tabela de repasse a qual ele consulta para saber para qual destino encaminhar os pacotes que chegam para ele. Uma ponta de comunicação nada mais é que uma tupla composta por IP e porto. O efeito prático desse mapeamento, realizado pelo NAT, é permitir vários computadores em uma rede local compartilharem um único endereço IP válido na internet. Veja a Figura 1, por exemplo, nela os roteadores (com NAT habilitado) conectam as redes privadas à rede pública (internet). Os hospedeiros das redes privadas possuem endereços IP que não são válidos na internet, como 192.168.1.1/24 (REKHTER et al., **RFC 1918**. 1996). O roteador NAT faz o intermédio da comunicação entre a rede privada e a internet, pois ele tem um IP válido publicamente (IPs 12.1.1.1 e 13.1.1.1 localizados nas interfaces dos roteadores NAT com a internet pública na Figura 1).

Figura 1 – Roteadores NAT



FONTE: <https://www.geeksforgeeks.org/network-address-translation-nat/>. Acesso em: 02 jun 2023

Entretanto, existem algumas técnicas de travessia de NAT, que possibilitam recuperar até determinado ponto a capacidade de conectividade ponta a ponta perdida ao se utilizar NATs. Uma delas é o UDP *Hole Punching*, documentado na RFC 5128[1] por Srisuresh, Ford e Kegel (**RFC 5128**. 2008), que permite alcançar a conexão direta entre pares atrás de certos tipos de NATs. Para executar essa técnica, dois pares precisam descobrir para qual ponta de comunicação pública seus respectivos NATs estão mapeando sua ponta de comunicação local. Após isso, eles trocam essa informação entre si e mandam mensagens UDP um para a ponta do outro, abrindo uma espécie de "buraco" em seus

[1] "RFC 5128: State of Peer-to-Peer (P2P) Communication across... ." <https://www.rfc-editor.org/rfc/rfc5128#section-3.3>.

respectivos NATs, por onde será possível a troca de dados. Outra técnica que auxilia a travessia de NATs é denominada STUN: através dela, um cliente se comunica com um servidor STUN, que responde para ele qual para qual ponta pública o NAT mapeou tal comunicação. Essa técnica está documentada na RFC 5389[2] por Matthews et al. (**RFC 5389**. 2008).

Em ambos os casos, para colocar os dois pares em contato, é necessário um terceiro computador visível na internet pública, para atuar como intermediário na troca das informações sobre os mapeamentos realizados pelos NATs. Essa máquina, denominada Servidor de Encontro (Rendezvous[3] Server), é responsável por trocar as informações de IP (Internet Protocol) e Porto mapeados entre os pares que querem se conectar diretamente através do UDP *Hole Punching*, pois, de início, eles não sabem as pontas públicas uns dos outros. Esse terceiro computador só é necessário para trocar essa informação entre os pares, para que eles possam iniciar uma comunicação direta (SRISURESH; FORD; KEGEL, **RFC 5128**. 2008).

Considerando tudo exposto acima, para auxiliar no monitoramento da qualidade do serviço prestado pela provedora de acesso à internet aos usuários residenciais, a proposta deste trabalho é o desenvolvimento de uma ferramenta de aferição periódica e automatizada de métricas da qualidade de serviço da conexão residencial à internet.

1.1 Justificativa

A ANATEL aprovou, em 23 de dezembro de 2019, o Regulamento de Qualidade dos Serviços de Telecomunicações (RQUAL[4]). A saber, esse regulamento define a atribuição de selos de qualidade para as provedoras de acesso à internet via uma entidade que fará a aferição da qualidade de serviço geral mantida pela provedora. O rebaixamento do selo de qualidade não exime a provedora de manter os benefícios auferidos para o consumidor no momento da contratação. Além disso, os próprios consumidores podem, por testes, comprovar o descumprimento individual de contrato e recorrer administrativa e legalmente para cobrar seus direitos. As Prestadoras de Pequeno Porte (PPPs), apesar de não serem obrigadas a cumprir o RQUAL, não são isentas de responsabilidade quanto à manutenção da qualidade do serviço.

Embora os testes de velocidade hospedados na infraestrutura do ISP sejam considerados precisos, eles podem não fornecer uma medição completa da qualidade do serviço oferecido pelo provedor de acesso à internet (ISP - Internet Service Provider). Isso ocorre

[2] "RFC 5389: Session Traversal Utilities for NAT (STUN)." <https://www.rfc-editor.org/rfc/rfc5389>.

[3] "Rendezvous protocol - Wikipedia." <https://en.wikipedia.org/wiki/Rendezvous_protocol.> Acessado em 5 out. 2022.

[4] "RQUAL - Regulamento de Qualidade - Governo Federal.", <https://www.gov.br/anatel/pt-br/dados/qualidade/indicadores-de-qualidade/rqual-regulamento-de-qualidade>.

porque o usuário contrata o acesso à internet pública (redes após o ISP) e, fatores externos, como o congestionamento nas redes adjacentes, podem afetar a qualidade do serviço. Por isso, o teste par-a-par é uma alternativa para medir a qualidade do serviço, já que ele fornece uma visão abrangente do desempenho da rede. Além disso, confiar apenas nos testes de velocidade cliente-servidor pode ser problemático, pois os ISPs tecnicamente poderiam manipular os resultados dos testes para fazer com que seus serviços pareçam mais rápidos do que realmente são. Considerando, na aferição em meios convencionais, a possível interferência pelo provedor nos resultados dos testes, as fragilidades do modelo cliente/servidor e a falta de periodicidade nos testes para um melhor acompanhamento na qualidade do serviço, uma ferramenta que contorne esses problemas traria benefício significativo para o consumidor. Assim, complementar o teste cliente-servidor com o teste par-a-par pode fornecer ao usuário uma medida mais abrangente e precisa da qualidade do serviço.

1.2 Objetivos

1.2.1 Objetivo Geral

Desenvolver uma ferramenta capaz de aferir de maneira periódica e automatizada a qualidade da conexão residencial à internet, por comunicação direta (par-a-par) entre dois computadores de redes privadas distintas.

1.2.2 Objetivos Específicos

- Revisar a literatura em busca de trabalhos similares a fim de identificar técnicas úteis para o projeto;
- Determinar uma maneira de estabelecer conexão par-a-par entre computadores atrás de NATs;
- Levantar o conjunto de bibliotecas auxiliares a serem utilizadas;
- Definir técnicas adequadas para aferir a qualidade de serviço de acesso à internet;
- Realizar experimentos com a ferramenta em diferentes cenários de conexão com a internet a fim de minimizar a existência de falhas e validar seu funcionamento;

No próximo capítulo será apresentada a fundamentação teórica, contendo as normas de qualidade de serviço no acesso à internet, as métricas de qualidade de serviço, as técnicas e conceitos utilizadas na solução desenvolvida bem como os trabalhos similares. Logo após, serão apresentados os materiais utilizados e a metodologia do experimento. Depois é apresentada a seção de projeto e desenvolvimento que documenta a execução das técnicas

utilizadas e também esclarece alguns aspectos do desenvolvimento da ferramenta. Em seguida é apresentada a análise e os resultados do experimento para as métricas aferidas e também as particularidades encontradas em alguns ISPs. Por fim é apresentada a conclusão.

2 Fundamentação Teórica

O presente trabalho se apoia em um conjunto previamente desenvolvido de tecnologias e conceitos, tais como alguns protocolos. A compreensão de todo o suporte para o projeto é necessária para um melhor entendimento daquilo que se pretende alcançar. As próximas seções irão prover mais detalhes sobre os referenciais teóricos que oferecem suporte para a realização do trabalho.

2.1 Normas sobre a Qualidade de Serviço (QoS) no acesso à Internet

Segundo a ANATEL[1],

> Sempre que as prestadoras com mais de 5% de participação em algum dos mercados nacionais de varejo em que atuam oferecerem serviços de conexão à Internet fixa, elas têm que respeitar os padrões mínimos de qualidade definidos na regulamentação. Esses padrões estão sendo reformulados desde a implementação do novo Regulamento de Qualidade dos Serviços de Telecomunicações (RQUAL). [...] Essas informações assim como restrições à utilização do serviço devem ser descritas no contrato ou termo de adesão por todas as operadoras.

Além das obrigações de velocidade, as prestadoras têm outras obrigações técnicas tais como limites de perda de pacotes transmitidos, latência bidirecional e *jitter*.

Regulamento de Qualidade do Serviço de Telecomunicações (RQUAL)

O RQUAL (Resolução nº 717/2019/ANATEL[2]) é uma norma que estabelece as condições mínimas de qualidade para os serviços de telecomunicações em geral, incluindo os serviços de internet banda larga fixa. No que se refere aos serviços de internet, o RQUAL define as características e os requisitos que devem ser cumpridos pelos Provedores de Acesso à Internet para garantir a qualidade do serviço oferecido aos usuários. As operadoras (Provedores de Acesso à Internet, ISPs) devem fornecer informações transparentes sobre a qualidade dos serviços prestados aos usuários e informá-los sobre eventuais falhas e indisponibilidades da rede. Conforme informações disponíveis na página web da ANATEL sobre o Regulamento de Qualidade do Serviço de Telecomunicações[3], "o RQUAL entrou totalmente em vigor em março de 2022 e

[1] "Conheça seus direitos: Velocidade de conexão à Internet" 18 nov.. 2020, <https://www.gov.br/anatel/pt-br/consumidor/conheca-seus-direitos/telefonia-movel/velocidade-de-conexao-a-internet>. Acessado em 3 abr.. 2023.

[2] "Resolução nº 717/2019 - ANATEL" 26 dez.. 2019, <https://www.in.gov.br/web/dou/-/resolucao-n-717-de-23-de-dezembro-de-2019-235328441>. Acessado em 3 abr.. 2023.

[3] "RQUAL - Regulamento de Qualidade - ANATEL." 8 abr.. 2022, <https://www.gov.br/anatel/pt-br/dados/qualidade/qualidade-dos-servicos/rqual-regulamento-de-qualidade>. Acessado em 3 abr.. 2023.

uniformiza as regras da telefonia fixa e móvel, banda larga fixa e TV por assinatura e traz indicadores que refletem com mais precisão a qualidade dos serviços utilizados pelos consumidores." O RQUAL é importante para garantir a qualidade dos serviços de internet oferecidos aos usuários no Brasil e visa melhorar a experiência dos usuários na navegação na internet. As operadoras que não cumprirem as exigências estabelecidas pelo regulamento estão sujeitas a sanções administrativas e podem ser multadas pela ANATEL.

Regulamento de Gestão da Qualidade do Serviço de Comunicação Multimídia (RGQ-SCM)

Antes de 2022, o RGQ-SCM (Resolução nº 574/2011/ANATEL[4]) era a norma que estabelecia as metas de qualidade, a serem cumpridas pelas prestadoras do Serviço de Comunicação Multimídia (SCM), os critérios de avaliação, de obtenção de dados e acompanhamento da qualidade da prestação do serviço. Entre as principais exigências da Resolução nº 574/2011 da ANATEL estão indicadores de qualidade[5] como a garantia de uma velocidade média de conexão mínima de 80% da velocidade contratada em 95% das medições mensais, e uma velocidade instantânea de pelo menos 40% da velocidade contratada em todas as medições. A norma também estabelece requisitos de estabilidade, latência bidirecional (inferior a 80 ms), variação de latência, (inferior a 50 ms) e taxa de perda de pacotes (inferior a 2%) para as conexões de internet. As metas de qualidade descritas no RGQ-SCM estão estabelecidas do ponto de vista da rede e do assinante e devem ser cumpridas por todas as prestadoras que não se enquadrarem na definição de Prestadora de Pequeno Porte.

Prestadora de Pequeno Porte

Conforme informações disponíveis na página web da ANATEL sobre Qualidade na Banda Larga Fixa[6], "até o início da vigência completa do Regulamento de Qualidade dos Serviços de Telecomunicações – RQUAL, aprovado pela Resolução nº 717/2019, o que ocorreu no mês de março de 2022, a Anatel monitorava a qualidade da banda larga fixa, por meio de indicadores operacionais das prestadoras não enquadradas como de pequeno porte" (prestadoras de SCM com até cinquenta mil acessos em serviço). Ainda, a mesma página web da ANATEL explica que:

> O conceito de prestadora de pequeno porte (PPP), trazido no âmbito do RGQ-SCM, foi revogado por meio da Resolução nº

[4] "Resolução nº 574/2011 (REVOGADA) - ANATEL" 31 out.. 2011, <https://informacoes.anatel.gov.br/legislacao/resolucoes/2011/57-resolucao-574>. Acessado em 3 abr.. 2023.

[5] "Indicadores de Qualidade para Banda larga Fixa" 20 nov.. 2020, <https://www.gov.br/anatel/pt-br/dados/qualidade/qualidade-dos-servicos/indicadores-de-qualidade-do-servico-de-banda-larga-fixa-scm>. Acessado em 3 abr.. 2023.

[6] "Qualidade - Banda Larga Fixa - ANATEL" 16 nov.. 2015, <https://www.gov.br/anatel/pt-br/dados/qualidade/qualidade-dos-servicos/controle-banda-larga>. Acessado em 3 abr.. 2023.

> 704/2018. Com a publicação da Resolução nº 694/2018 [...], as PPPs passaram a ser definidas como grupos detentores de participação de mercado nacional inferior a 5% (cinco por cento) em cada mercado de varejo em que atuam. Assim, as obrigações de atendimento aos indicadores de qualidade relativos à banda larga fixa previstas no RGQ só se aplicavam à Claro (+ Nextel), Oi, Sky, TIM e Vivo.

Marco Civil da Internet

É uma lei brasileira (Lei n° 12.965/2014) que estabelece princípios, direitos e deveres para o uso da internet no país (BRASIL, 2014). Tal lei visa promover a liberdade de expressão, a privacidade dos usuários, a inovação e a segurança da rede. Entre os principais pontos do Marco Civil estão a garantia da neutralidade de rede, que impede a discriminação de conteúdos, serviços ou aplicações na internet, e a proteção de dados pessoais dos usuários, que devem ser coletados e tratados de forma transparente e respeitando a privacidade dos indivíduos. A lei também estabelece regras para a responsabilização de provedores de internet e usuários por conteúdos ilícitos na rede, bem como para a proteção da propriedade intelectual na internet.

Neutralidade de Rede

Conforme o Marco Civil da Internet no Brasil, a Neutralidade de Rede[7] é exigida para garantir que os Provedores de Acesso à Internet tratem todo o tráfego de dados de forma isonômica, sem discriminação ou preferência por conteúdos, serviços ou aplicações específicas. Assim, a Neutralidade de Rede exige que todos os dados sejam tratados igualmente, sem priorização ou bloqueio de determinados conteúdos, ou serviços, em detrimento de outros. Essa medida é importante para garantir a liberdade de expressão, o acesso à informação e a concorrência no mercado de serviços de internet.

2.2 Métricas de Qualidade de Serviço (QoS) no acesso à Internet

Velocidade (ou Vazão)

A Resolução 717 da ANATEL[8] define velocidade como a capacidade da rede para transferência de dados por segundo. Essa capacidade é definida em bits por segundo, ou seja, 'bps'. A velocidade é definida pela ANATEL como um indicador da qualidade do serviço dos provedores. A vazão de *download* é importante para aplicações que requerem a transferência de grandes quantidades de dados, como vídeo sob demanda em alta definição, downloads de arquivos grandes, dentre outros. A vazão de *upload*

[7] "Entenda o que é neutralidade de rede..." 16 dez.. 2017, <https://agenciabrasil.ebc.com.br/geral/noticia/2017-12/entenda-o-que-e-neutralidade-de-rede-e-como-e-o-seu-funcionamento-no-brasil>. Acessado em 3 abr.. 2023.

[8] "Resolução nº 717/2019 - ANATEL." 23 dez. 2019, <https://informacoes.anatel.gov.br/legislacao/resolucoes/2019/1371-resolucao-717>.

é especialmente importante para aplicações que exigem que o usuário envie uma grande quantidade de dados, como videoconferências, envio de arquivos grandes, compartilhamento de arquivos em nuvem e jogos *online multiplayer*. Quanto maior a vazão de *upload*, mais rapidamente os dados serão enviados para o destino, com as aplicações sendo executadas de forma mais fluida e sem interrupções.

Latência

Valadão, Guedes e Duarte (2017) definem a latência bidirecional ou RTT (Round-Trip Time) como a soma do atraso de A para B com o atraso de B para A, considerando dois nós A e B em uma rede. Os autores apontam que tal indicador é utilizado para prever o comportamento do protocolo TCP e para aplicações que utilizam o princípio de requisição e resposta. Aplicações par-a-par também recorrem ao indicador para escolher vizinhos com menor tempo de resposta. A ANATEL também define o RTT como um indicador da qualidade do serviço dos provedores.

Jitter

Segundo Tanembaum A. e Whetherall (2013) *jitter* corresponde a variação no atraso de chegada dos pacotes. A pertinência desse indicador é dada pelo fato de que altas taxas do mesmo influenciam na qualidade de serviços web amplamente utilizados, como *streaming* de vídeo e de áudio. Para exemplo, consideremos um serviço de *streaming* de vídeo em tempo real. Nele, os pacotes referentes a uma dada imagem são enviados do transmissor ao receptor. Se o *jitter* estiver suficientemente alto, pacotes da imagem chegarão em intervalos irregulares e o poderia perder inteligibilidade pelo vídeo ficar fora de sincronia com o áudio. Este é outro indicador de qualidade estabelecido pela ANATEL.

Taxa de Perda de Pacotes

Kurose e Ross (2013) definem que a perda de pacotes acontece quando o *buffer* de saída de um comutador de pacotes se enche. Nesse contexto, pacotes que chegarem para esse comutador serão descartados enquanto não houver espaço no *buffer*. Este é outro indicador utilizado pela ANATEL para calcular a qualidade do serviço das provedoras. A perda de pacotes se manifesta como um problema especialmente em aplicações que exigem uma alta taxa de transferência de dados, como jogos *online*, videoconferências, transmissão de vídeo ou áudio em tempo real, entre outros. O motivo é que perda de pacotes pode causar interrupções, distorções e outros problemas de comunicação. Essa perda pode ocorrer devido a várias razões, como congestionamento na rede (local, metropolitana ou além), problemas de conexão (com o ISP), falhas em algum hardware intermediário ou provocadas por software, interferência eletromagnética (em enlaces metálicos ou de radiofrequência), entre outras.

2.3 Técnicas e conceitos utilizados na solução desenvolvida

NAT

Kurose e Ross (2013) apresentam o Network Address Translation (tradução de endereços na rede) como uma técnica para que vários computadores de uma mesma sub-rede possam compartilhar de um mesmo endereço IP para comunicação na internet. Os ISPs utilizam o NAT principalmente devido à escassez de endereços IPv4 disponíveis. O IPv4 utiliza endereços de 32 bits, o que permite um total de aproximadamente 4,3 bilhões de endereços únicos. Com o crescimento exponencial da Internet e o aumento do número de dispositivos conectados, essa quantidade limitada de endereços IPv4 se tornou insuficiente. Para contornar essa limitação, os ISPs implementaram o NAT, que permite que vários dispositivos em uma rede local compartilhem um único endereço IP público fornecido pelo ISP.

Nessa técnica, só o roteador do provedor de acesso à internet possui um IP válido na internet. Os hospedeiros atrás de tal roteador tem endereços IPs válidos somente na sua sub-rede. O truque consiste em montar uma tabela de repasse no roteador que mapeia o IP e porto de um hospedeiro (ponta privada) em um IP (esse sempre será o IP válido na internet do roteador de borda) e porto (ponta pública) no roteador. Assim, quando um pacote chega para o roteador, em determinado porto e contendo o IP dele válido na internet, ele sabe pela tabela de repasse para qual dos hospedeiros atrás dele direcionar o pacote. NATs podem ser configurados de diversas maneiras, mas eles podem ser caracterizados em três tipos[9]: NAT tipo 1 (Aberto), NAT tipo 2 (Moderado), e NAT tipo 3 (Estrito). Não é possível estabelecer comunicação par a par entre dois hospedeiros atrás de NAT tipo 3. Já o NAT tipo 2 aceita requisições vindas de um par B para uma ponta pública de um par A somente se este último realizar antes uma requisição ao primeiro por essa ponta pública (A tiver feito uma requisição a B). Assim, esse NAT, apesar de mais restrito, também permite a comunicação par a par. Por fim, o NAT tipo 1 aceita requisições vindas de um par B para uma ponta pública de um par A mesmo que este último não tenha feito antes uma requisição ao primeiro através dessa ponta. Dessa forma, esse tipo de NAT também permite a comunicação par a par.

UDP *Hole Punching*

Técnica documentada na RFC 5128 por Srisuresh, Ford e Kegel (**RFC 5128**. 2008), que permite alcançar a conexão direta entre pares atrás de certos tipos de NATs. Para executar essa técnica, dois pares precisam descobrir para qual ponta de comunicação pública seus respectivos NATs estão mapeando sua ponta de comunicação local. Após

[9] <https://www.centralxbox.com.br/2020/04/15/nat-aberta-como-solucionar-os-problemas-e-ter-supervelocidade-de->

isso, eles trocam essa informação entre si e mandam mensagens UDP um para a ponta pública do outro, abrindo uma espécie de "buraco" em seus respectivos NATs, por onde será possível a troca de dados.

Para executar essa técnica, é necessário um terceiro computador visível na internet. Essa máquina, denominada Servidor de Encontro, é responsável por trocar as informações de IP e porto mapeados entre os pares que querem se conectar diretamente através do UDP *Hole Punching*, pois, de início, eles não sabem as pontas públicas uns dos outros, descobertas através do STUN (Session Traversal Utilities for NAT). Esse terceiro computador só é necessário para trocar essa informação entre os pares, para que eles possam iniciar uma comunicação direta (SRISURESH; FORD; KEGEL, **RFC 5128**. 2008). O Servidor de Encontro, ao invés de uma única máquina fixa, poderia ser implementado como os milhares de nós da Mainline DHT (Distributed Hash Table) utilizada pela rede BitTorrent, conferindo uma maior disponibilidade e robustez a este aspecto do sistema.

STUN

Session Traversal Utilities for NAT ou (STUN) é um protocolo utilizado como ferramenta para outros protocolos e está documentado na RFC 5389 por Matthews et al. (**RFC 5389**. 2008). Sozinho, ele não é suficiente para realizar a travessia de NATs, ou seja, fazer com que dois computadores atrás de NATs comuniquem entre si. Neste protocolo, após o cliente enviar uma requisição, o servidor responde para ele informando qual a ponta de comunicação pública alocada pelo NAT que corresponde à ponta de comunicação local pela, qual saiu requisição no cliente. Além disso, esse protocolo permite descobrir o tipo de NAT que está à frente de um hospedeiro. Esta informação é útil, pois dependendo do tipo do NAT, sua travessia não é possível.

BitTorrent

O BitTorrent é um protocolo para o compartilhamento descentralizado de arquivos, utilizando uma rede *peer-to-peer* (COHEN, 2008). Neste protocolo, os pares que desejam um determinado arquivo, solicitam pedaços do mesmo a outros nós que o possuem. Quando um par tem todos os pedaços, o arquivo completo é montado. Nesse protocolo, os pares se comunicam com um ou mais servidores chamados *trackers* para encontrar outros pares e, então, compartilhar os arquivos entre si.

DHT BitTorrent

É uma extensão ao protocolo BitTorrent que torna a rede ainda mais descentralizada (SILVA, 2018 apud LOEWENSTERN; NORBERG, 2008, p. 22). Com ela, os pares não precisam mais se comunicar com os *trackers* para encontrar outros pares e compartilhar arquivos. Em suma, com essa extensão, cada par atua como um *tracker*, por meio de uma tabela *hash* distribuída (SILVA, 2018).

Wrapper

Boulanger, Lazzarini e Mathews (2010) definem *Wrapper* como um software que provê funcionalidades de uma linguagem A, como funções e classes, na forma e sintaxe de outra linguagem B. Assim, o programador não precisa fazer com que seu programa seja escrito em A. Por exemplo, um *wrapper* pode oferecer em Python funcionalidades de uma API escrita em C++.

Traffic Shaping

O *traffic shaping* (ou modelagem de tráfego) é uma prática utilizada por alguns ISPs para gerenciar o fluxo de tráfego de rede, controlando e priorizando determinados tipos de dados ou aplicações. O objetivo do *traffic shaping* é otimizar o desempenho da rede, melhorar a qualidade do serviço e evitar congestionamentos. O *traffic shaping* envolve o monitoramento e a manipulação do tráfego de rede, aplicando políticas e regras para controlar a largura de banda alocada para diferentes tipos de tráfego. Isso permite que o ISP gerencie o fluxo de dados de acordo com suas políticas e prioridades, garantindo uma distribuição justa e eficiente dos recursos de rede. Por exemplo, um provedor pode priorizar o tráfego de vídeo em *streaming* em detrimento de *downloads* de arquivos, uma vez que o primeiro exige uma conexão mais estável e rápida. Essa técnica pode ser polêmica, uma vez que pode afetar a qualidade de serviço e a neutralidade de rede, que exige o tratamento isonômico do tráfego, sendo importante que as operadoras a utilizem de forma transparente e conforme as normas regulatórias e os contratos firmados com os usuários.

Saturação

É uma técnica para aferição de vazão (velocidade) de um *link* de acesso à internet. Como explicado por Macmillan et al. (2023), ela consiste em transferir a maior quantidade possível de dados por meio de um *link*, saturando a capacidade do mesmo por um determinado tempo. Depois, computa-se a quantidade de dados transferidos de um hospedeiro a outro, obtendo assim a vazão entre eles.

2.4 Trabalhos Relacionados

2.4.1 Speedtest.net, da Ookla

O Speedtest.net[10] é um *website* que permite aferir métricas de conexão à internet como: velocidade de *download*, velocidade de *upload*, *jitter* e latência, além de mostrar um histórico de aferições. Não mede a perda de pacotes e não afere de forma periódica. Por ser um serviço no modelo cliente-servidor, caso o *website* ou o servidor central que coordena

[10] <https://www.speedtest.net/pt> Acesso em 20 mai. 2023

os testes fique fora do ar o usuário não conseguiria fazer medições. Além disso, provedores de internet podem hospedar servidores do Speedtest dentro de sua intranet, o que interfere nos resultados para dar impressão aos clientes de tais ISPs que a qualidade de seu acesso à internet pública seja tão bom quanto a comunicação na rede interna privada do ISP.

2.4.2 Brasil Banda Larga, da ESAQ

Ferramenta[11] governamental da ESAQ (Entidade de Suporte à Aferição da Qualidade). Possibilita aferir métricas de conexão à internet como: velocidade de *download*, velocidade de *upload*, *jitter*, latência e perda de pacotes. As aferições são feitas contra servidores alocados em pontos de troca na infraestrutura do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), portanto, a medição nesse website tende a condizer mais com a realidade pelo tráfego efetivamente passar pela internet pública brasileira. Outro ponto positivo é que o site armazena o histórico das medições do usuário. Todavia, por ser um serviço no modelo cliente-servidor, também sofre das limitações em relação à disponibilidade. Além disso, não faz aferição periódica de forma automatizada.

2.4.3 SIMET (beta.simet.nic.br)

Ferramenta governamental[12] do NIC.br (Núcleo de Informação e Coordenação do Ponto BR). Afere a velocidade de *download*, velocidade de *upload*, *jitter*, latência e perda de pacotes. Também utiliza os servidores do NIC.br. É utilizado o modelo cliente servidor, além disso, não realiza medições periódicas e não armazena o histórico de medições do usuário.

2.4.4 CheesePI

O CheesePI (GUULAY B, 2015) é um hardware dedicado ao monitoramento das métricas de latência, perda de pacotes e potência do sinal Wi-Fi (quando instalado em redes *wireless*). Ele é composto por um Raspberry PI com as ferramentas ping, httping e traceroute instaladas. O CheesePI é conectado ao roteador do usuário residencial e realiza as aferições periodicamente e com o mínimo de interferência na experiência de acesso à internet. Existe um servidor central que determina quando o CheesePI deve realizar as aferições e contra quais servidores (ex: www.facebook.com ou www.google.com). O usuário pode visualizar o histórico da qualidade da sua conexão via um *dashboard* hospedado no Raspberry PI. O *dashboard* utiliza a aplicação de código aberto Grafana[13] para exibir as métricas coletadas.

[11] <https://www.brasilbandalarga.com.br/> Acesso em 20 mai. 2023
[12] <https://beta.simet.nic.br/> Acesso em 20 mai. 2023
[13] "Grafana: The open observability platform" <https://grafana.com/> Acesso em 20 mai. 2023

2.4.5 Jitlat

O Jitlat (MCLACHLAN; BRIND-ARMOUR, 2011) é uma ferramenta desenvolvida para o Departamento de Pesquisa e Desenvolvimento de Defesa do Canadá e utilizada para mensurar o desempenho de uma rede para aplicações que exigem transferência constante de dados, como Voz sobre IP (VoIP). Seu método de aferição consiste na utilização de um cliente transferindo dados a um servidor. Este último é responsável por analisar os dados recebidos e enviar os resultados de volta para o cliente, que os exibe para o usuário. São aferidas as métricas de latência mínima, média e máxima, *jitter* mínimo, médio e máximo e número de pacotes perdidos, duplicados ou recebidos fora de ordem. São exibidos também gráficos de latência, de rajadas de latência (isto é, latência vs tempo de chegada dos pacotes) e histograma da perda de pacotes, sendo esses dois últimos importantes para aplicações que exigem transferência de dados contínua.

2.4.6 Iperf3

O Iperf3[14] é um software desenvolvido pela Rede de Ciências e Energia e pelo Laboratório Nacional Lawrence Berkeley nos Estados Unidos. É uma ferramenta já consolidada, presente há mais de 10 anos no mercado e continua sendo mantida e atualizada. O Iperf3 permite a aferição das métricas de velocidade, latência, perda de pacotes e *jitter* de uma rede, no modelo cliente-servidor. Todavia, as métricas de velocidade e de latência só estão disponíveis na aferição TCP.

2.4.7 Peer-network

A Peer-network (SILVA, 2018) é uma biblioteca escrita em JavaScript e publicada no repositório NPM. Ela permite que hospedeiros consigam alcançar conectividade par-a-par ao realizar a travessia de NATs tipo 1 e 2 utilizando a própria rede DHT do BitTorrent como ponto de encontro entre os pares. A biblioteca Peer-network não é especificamente voltada para aplicações de medição de velocidade da internet, mas foi utilizada como tecnologia básica neste trabalho de TCC, possibilitando que os pares se encontrassem via DHT para, posteriormente, realizarem entre si as aferições das métricas de qualidade de acesso à internet.

[14] <https://github.com/esnet/iperf>

3 Materiais e Métodos

Neste capítulo serão abordados os materiais e a metodologia utilizada para a construção da Peertest, de forma que o leitor entenda quais etapas foram necessárias para o desenvolvimento da ferramenta. São apresentados também os percalços e desafios que influenciaram as decisões de projeto.

3.1 Materiais

Peer-Network

Biblioteca escrita em JavaScript e disponibilizada publicamente no registro do NPM. Ela estabelece uma comunicação fim-a-fim entre nós atrás de NATs, utilizando a DHT do BitTorrent como ponto de encontro (SILVA, 2018).

Iperf3

Iperf [1] é uma ferramenta de linha de comando desenvolvida pela Rede de Ciências de Energia (ESnet) em parceria com o Laboratório Nacional Lawrence Berkeley, nos Estados Unidos. Voltada para aferir métricas de qualidade em redes de computadores como velocidade (vazão), *jitter*, latência e perda de pacotes. Possui extensa funcionalidade e é uma ferramenta referência, existindo há mais de 10 anos.

Wrapper Iperf3

O Iperf3-python[2] é um *wrapper* para a ferramenta Iperf3, que a encapsula na sintaxe Python, linguagem utilizada para o desenvolvimento da ferramenta de aferição neste trabalho. Além disso, o *wrapper* também é útil para recuperação dos resultados do Iperf3 em forma de objeto.

Ncat / Netcat

O Ncat[3] (ou Netcat) é uma ferramenta de linha de comando para estabelecer conexões TCP, enviar datagramas UDP, e ouvir em portos TCP/UDP.

SoCAT

O SoCAT[4] é uma ferramenta de linha de comando que estabelece fluxos bidirecionais de bytes e transfere dados por eles. Pode ser usada para variados propósitos. Neste

[1] "iperf3: A TCP, UDP, and SCTP network bandwidth measurement tool." <https://github.com/esnet/iperf>.
[2] "thiezn/iperf3-python: Python wrapper around iperf3 - GitHub." <https://github.com/thiezn/iperf3-python>.
[3] "ncat: Netcat for the 21st Century - Nmap." <https://nmap.org/ncat/>.
[4] "socat: Multipurpose relay - Dest-unreach!" <http://www.dest-unreach.org/socat/>.

trabalho, ela foi utilizada para traduzir conexões TCP em datagramas UDP e também para o redirecionamento de fluxos.

PV (PipeViewer)

O PV[5] é uma ferramenta de linha de comando para monitorar a transferência de dados em um pipe UNIX.

Stuntman

O Stuntman[6] é uma ferramenta de linha de comando para descoberta do mapeamento (ponta privada para ponta pública) do NAT utilizando servidores STUN que implementam as RFCs 5389, 5769, 5780 e 3489.

Ultraping

O Ultraping[7] é uma ferramenta em Python para aferição de latência em redes por meio de datagramas UDP. Como ela é do ano de 2016, foi provavelmente escrita para Python 2. Sendo assim, algumas funcionalidades não executam no Ubuntu 20.04 (ambiente de desenvolvimento utilizado), pois ele utiliza o Python3. Foi necessário modificar essa ferramenta para executá-la no Ubuntu.

Amazon Elastic Compute Cloud

Para testar a solução com um par em uma intranet de provedor diferente, foi utilizada uma máquina virtual na nuvem da Amazon. Teve-se que recorrer a essa alternativa devido à impossibilidade de executar a ferramenta tanto no próprio campus, pela presença de um firewall de aplicação, quanto pelo próprio orientador, devido ao fato que seu provedor de internet utilizava um NAT estrito (tipo 3). Vale notar que tal máquina foi usada somente para fins de desenvolvimento da ferramenta, pois há um limite de banda no plano gratuito que, se excedido, acarreta cobranças financeiras para o utilizador. Sendo assim, ela não foi utilizada para realizar os experimentos.

Speedtest-cli

Versão do Speedtest.net que oferece as mesmas funcionalidades do teste feito pelo site, porém, via interface de linha de comando. É desenvolvido pelo próprio Speedtest.net.

3.2 Metodologia

Na ferramenta desenvolvida neste TCC, é utilizada a biblioteca Peer-Network para possibilitar com que os pares se encontrem na internet de forma descentralizada

[5] "pv (Pipe Viewer): monitor progress of data through pipe - ivarch.com." <http://www.ivarch.com/programs/pv.shtml>.

[6] "stuntman: open source STUN server - StunProtocol." <https://www.stunprotocol.org/>.

[7] "mrahtz/ultra_ping: Measure UDP packet latency - GitHub." <https://github.com/mrahtz/ultra_ping>.

utilizando a DHT do BitTorrent. São utilizados servidores STUN, possibilitando cada par descobrir sua ponta pública, e informá-la ao par correspondente para ser possível executar a técnica de UDP *Hole Punching*, estabelecendo a comunicação entre os pares, fora da DHT BitTorrent. Utilizamos um algoritmo desenvolvido para a seleção de pares para aferição. Uma vez estabelecida a comunicação ponto-a-ponto entre pares, são aferidas as métricas de qualidade do acesso à internet utilizando o protocolo UDP. Devido a uma política imposta por ISP utilizado nos experimentos de teste de campo, foi necessário configurar os pacotes UDP para tamanho de até 1492 bytes, para a comunicação efetiva entre os pares. As ferramentas PipeViewer (pv) e Netcat (nc) foram utilizadas para aferir a vazão de *download* e *upload*. A ferramenta Ultraping foi utilizada para aferir a latência bidirecional (RTT). No caso das aferições de *jitter* e perda de pacotes o software Iperf3 é utilizado e, para tal, fez-se necessário uma tradução de protocolo das conexões TCP em rajadas UDP, por conta da adoção de Hole Punching UDP como forma de transpor os NATS dos ISPs.

Para testar a hipótese que uma ferramenta de aferição P2P poderia capturar as características da conexão de acesso à internet, e não de acesso à intranet do provedor, foi realizada uma pesquisa experimental com aspectos também quantitativos. O experimento foi realizado entre os dias 28/01/2023 e 07/02/2023 (11 dias). A cada 15 minutos, eram realizadas as aferições das métricas de qualidade da internet com a Peertest e, logo após, com o Speedtest. Na Peertest, os dois pares estavam localizados em redes privadas distintas para assegurar que se aferisse as métricas de qualidade da internet, e não da intranet do provedor. Já em relação ao Speedtest, seu próprio algoritmo selecionava o servidor para os testes. Dessa forma em alguns momentos ele escolheria o servidor dentro do provedor e em outros não.

Na análise dos resultados, comparou-se a Peertest contra esses dois cenários do Speedtest, através de análise estatística descritiva. Os resultados são apresentados na forma de gráficos contendo as estatísticas descritivas bem como os seguintes *plots*:

- Histograma, para averiguar a distribuição de frequência do conjunto de dados. Além da representação visual da forma da distribuição dos dados, o histograma pode revelar padrões nos dados (picos, lacunas, agrupamentos). Tais informações são úteis para identificar comportamentos incomuns e entender melhor a natureza dos dados.
- *Rug Plot*, para visualizar todas as observações individuais do conjunto de dados e obter uma visão completa de como eles estão distribuídos no eixo. Complementando o histograma, o *Rug Plot* mostra a densidade das observações em cada ponto do eixo, o que permite uma análise mais detalhada.
- *Boxplot*, para se observar a variabilidade, assimetria e existência de valores atípicos. Nele, pode-se analisar a dispersão dos dados, observando-se o intervalo interquartil

(que contém a maioria dos dados).

- *Curva de Distribuição Cumulativa*, para identificar qual a probabilidade de uma amostra assumir um valor menor ou igual a um dado valor, o que permite determinar a chance de observar um evento em um determinado intervalo. E, ao comparar as CDFs de duas ou mais distribuições, é possível visualizar e comparar as características de cada uma.

4 Projeto e Desenvolvimento

Neste capítulo serão apresentadas as técnicas utilizadas para a construção da ferramenta, possibilitando entender como é o seu funcionamento. Além disso, são feitas algumas ressalvas sobre os principais aspectos do desenvolvimento.

4.1 *Hole Punching*

As tentativas de executar a técnica de *Hole Punching* para viabilizar a conexão P2P entre os pares, para fins de aferição de qualidade da internet, obtiveram sucesso. Registre-se que foi efetuado o *Hole Punching* UDP que já oferece subsídio para aferir os parâmetros da qualidade da internet desejados. Apesar da existência do Hole Punch TCP, ele não foi utilizado neste trabalho. Como explica Ford, Srisuresh e Kegel (2005), "o estabelecimento de conexões TCP ponto a ponto entre hosts por trás de NATs é um pouco mais complexo do que para UDP. Como a perfuração não é tão bem compreendida pelo NAT, é atualmente suportado por uma quantidade menor de NATs existentes". Dessa forma, o UDP *Hole Punch* é mais confiável, no sentido em que ele tem maior probabilidade de ser suportado em um determinado roteador NAT. A seguir será detalhado como foram os testes para se obter o *Hole Punching* UDP.

4.2 *UDP Hole Punching*

Para realizar a técnica de *Hole Punching*, que consiste em ambos os pares tentarem se comunicar pelas pontas públicas um do outro, abrindo um "buraco"no NAT, é necessário que cada um deles primeiro descubra qual a sua ponta pública. Para isso, como mostra a Quadro 1 e a Quadro 2, foram feitas requisições a um servidor STUN[1] que informa a cada par a sua respectiva ponta pública após o mapeamento realizado pelo NAT para essa mesma requisição. O parâmetro –localport especifica de qual porta local do dispositivo a requisição ao STUN será enviada.

Após isso, foi utilizado também o software Netcat para gerenciar os detalhes de conexão dos pares automaticamente, para fins de depuração. Depois da resposta do comando STUN, o Netcat foi executado via linha de comando em ambos os computadores e devidamente configurado para o IP e porto externos de cada par (conforme resposta do servidor STUN).

[1] "STUN" - <https://www.rfc-editor.org/rfc/rfc5389>

Quadro 1 – Comando para obter via STUN o mapeamento NAT de um determinado porto local (par 1)

```
$ stunclient --localport 2000 --mode full stun.stunprotocol.org

Binding test: success
Local address: 192.168.0.110:2000
Mapped address:   186.233.160.141:28769
Behavior test: success
Nat behavior: Endpoint Independent Mapping
Filtering test: success
Nat filtering: Address and Port Dependent Filtering
```

Quadro 2 – Comando para obter via STUN o mapeamento NAT de um determinado porto local (par 2)

```
$ stunclient --localport 2000 --mode full stun.stunprotocol.org

Binding test: success
Local address: 192.168.0.105:2000
Mapped address:   45.70.35.52:12870
Behavior test: success
Nat behavior: Endpoint Independent Mapping
Filtering test: success
Nat filtering: Address and Port Dependent Filtering
```

Especificamente, conforme se observa no Quadro 3 e no Quadro 4, a chamada ao programa Netcat consistiu da opção -u para especificar uma conexão UDP, e o parâmetro -p para especificar o porto de origem da conexão, visto que essa porto deve ser igual ao porto da ponta local mapeada pelo NAT e informada pela máquina que fez a requisição ("cliente") ao servidor STUN (parâmetro –localport). Para concluir a parametrização do Netcat, é informado a ponta pública (endereço IP e porto externos do par) mapeada pelo NAT na conexão feita na máquina destino com o servidor STUN.

Quadro 3 – Comando Netcat no par 1

```
$ echo 'abrindo buraco para par 2' | nc -u -p 2000   45.70.35.52 12870
```

Quadro 4 – Comando Netcat no par 2

```
$ echo 'oi' | nc -u -p 2000   186.233.160.141 28769
```

Na prova de conceito, para verificar a viabilidade do *Hole Punching*, é parametrizada manualmente a chamada ao Netcat em cada computador, como citado acima, observando os respectivos IPs e portos necessários para cada um, conforme mapeado pelos respectivos NATs. Após essa etapa, o processo de conexão se deu da seguinte maneira:

- O par 1 executa a chamada do Netcat para se conectar com o par 2, enviando a mensagem "abrindo buraco para par 2". Esta mensagem não chega para o par 2, pois seu NAT não a reconhece, portanto, descarta o pacote. Entretanto, no NAT do par 1 é configurada uma regra que deixará que os dados vindos da ponta pública do par 2 cheguem até o par 1.
- O par 2 executa a chamada do Netcat para se conectar com o par 1 enviando a mensagem "oi". Agora, essa mensagem e todas as subsequentes partindo de qualquer um dos dois pares chegará no outro. Isso acontece, pois ao executar essa chamada, é criada uma regra no NAT do par 2 análoga à regra do passo anterior.

Vale destacar que essa abordagem não funcionou quando os pares estavam na mesma rede, mas funcionou quando eles estavam em redes diferentes, portanto, atrás de NATs diferentes. O motivo é que quando os pares estão na mesma rede, é necessário que o NAT esteja configurado para permitir que os sistemas finais atrás dele consigam se comunicar utilizando suas pontas de comunicação públicas. Porém, essa configuração não estava habilitada no NAT do Provedor de Acesso à internet utilizado pelo autor.

4.3 Protocolo de *Rendezvous*

Para que os pares se encontrem no intuito de realizar medições periódicas da qualidade de serviço na internet, é necessário superar o desafio de fazer com que mesmo atrás de NATs eles consigam se encontrar e se comunicar. O protocolo BitTorrent é uma base propícia para se achar a solução, uma vez que através desse sistema distribuído, milhares de usuários atrás de NATs tem conseguido se comunicar e compartilhar arquivos durante as últimas décadas.

A resposta para o desafio está na biblioteca Peer-network. Ela utiliza a rede BitTorrent como ponto de encontro dos pares e o protocolo BitTorrent DHT (Distributed Hash Table), para, desta forma, conseguir realizar a técnica de UDP *Hole Punching* e estabelecer uma comunicação direta entre eles. Sendo assim, utilizando a DHT, a solução se beneficiará da robustez oferecida pela abundância de nós nessa rede.

Considerando o acima exposto, foram realizados testes com a biblioteca Peer-network para verificar se ela poderia ser utilizada como suporte para viabilizar dois computadores atrás de NATs de diferentes provedores de internet se encontrarem e se

comunicarem diretamente, através do UDP *Hole Punching*. Os testes obtiveram sucesso e a biblioteca Peer-network conseguiu conectar computadores que estivessem atrás de mais de uma camada de NAT (ex.: NAT do roteador da LAN e NAT do roteador do provedor de internet). Posteriormente, os testes foram repetidos, desabilitando a habilidade da biblioteca de configurar automaticamente encaminhamento de porto através do protocolo UPnP. Mesmo neste cenário, a biblioteca ainda obteve sucesso em conectar os pares entre si. Desta forma, a biblioteca não exige o encaminhamento de portos via UPnP para funcionar.

4.4 Comunicação com a Peer-network

A biblioteca Peer-network, utilizada como base neste TCC, foi desenvolvida em JavaScript. Entretanto, a linguagem Python foi utilizada para a construção da ferramenta de aferição por questões de familiaridade e agilidade em prototipação. Para fazer com que os dois programas se comunicassem, foram utilizados *sockets*. O código da Peer-network foi modificado para incluir um *socket* que recebe e envia mensagens para o *socket* da solução em Python. Algumas dessas mensagens são: Notificação de novo par na DHT, notificação de saída de par da DHT, mensagens para coordenar a execução dos testes, envio de resultados e retransmissões. Adicionalmente, o código em Python também chama a execução da biblioteca Peer-network, evitando que as duas sejam chamadas separadamente. Assim, simplifica-se a execução da ferramenta de aferição na totalidade.

4.4.1 Seleção de par para medições cliente-servidor

O algoritmo de seleção de par para medições funciona conforme ilustrado pela Figura 2. Basicamente, em um laço de repetição (*loop*), cada par vai disparar ofertas para até 3 pares e aguardar pelo menos um deles responder, então a aferição será realizada. Caso aconteça de um par enviar essas ofertas e receber uma oferta antes que algum par aceite a sua, ele aceita a oferta recebida e retira suas ofertas enviadas anteriormente. De outra forma, caso algum par aceite a oferta enviada, ele retira as ofertas enviadas aos outros 2 pares na primeira etapa. Além disso, um par que aceitou determinada oferta fica de prontidão esperando o outro par iniciar o teste, desmarcar ou o estouro do tempo limite de espera.

Este algoritmo é executado periodicamente quando um par deseja encontrar outro par para realizar os testes. Assim que um par é encontrado, são realizados consecutivamente para cada um deles os testes de vazão, *jitter*, perda de pacotes e latência (RTT). Todavia, nada garante que os mesmos pares se encontrarão na próxima iteração do algoritmo.

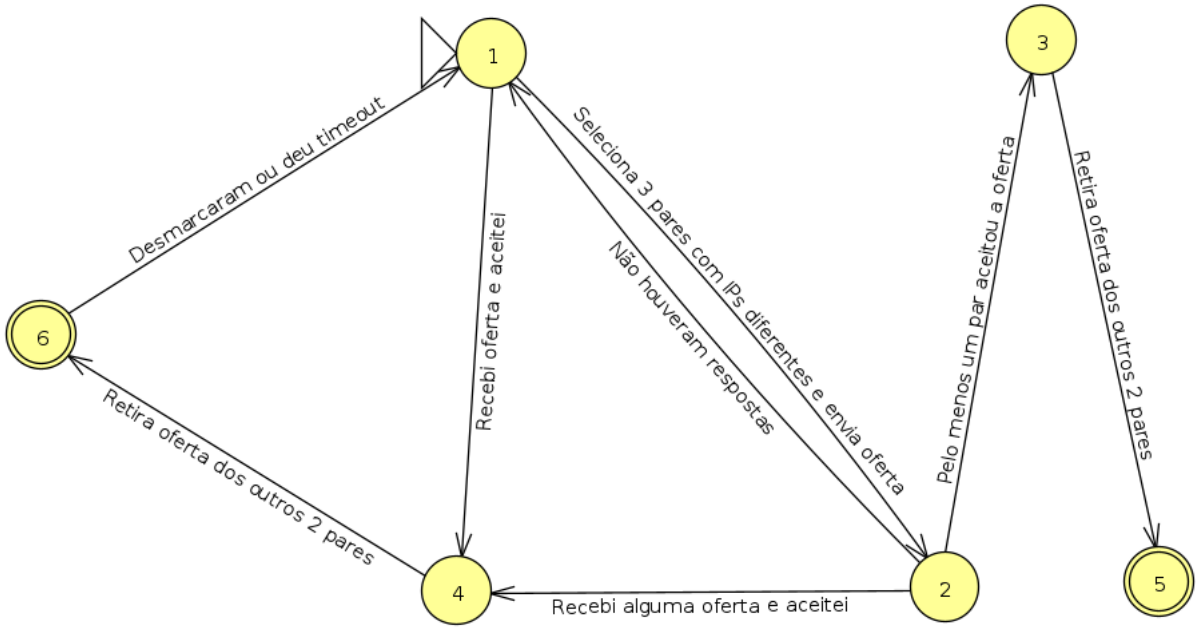


Figura 2 – Máquina de estados do algoritmo de seleção de par

4.5 Tradução de Protocolos de Transporte

O software Iperf3 utiliza, em sua aferição UDP, uma conexão de controle TCP para coordenar a execução do teste, e uma rajada de datagramas UDP para a transmissão dos dados do mesmo. Além disso, na chamada de tal software, só é possível passar como parâmetro um porto destino para se conectar.

Quadro 5 – Comando para aferição UDP no Iperf3

```
$ iperf3 -u -c 186.233.160.141 -p 7000
```

Considerando o quadro acima, a conexão TCP de controle e a rajada UDP de dados tentariam se comunicar com o porto 7000 do destino (parâmetro -p). A opção -u define que será feito uma aferição UDP e o parâmetro -c especifica qual o IP do servidor Iperf3.

Deve-se considerar, no entanto, que o buraco furado pela Peer-network é UDP. Desta forma, a conexão de controle não seria estabelecida entre origem e destino. Sendo assim, foi utilizado a ferramenta Socket CAT (SoCAT). Ela traduz um fluxo TCP em rajadas UDP ou vice-versa. A estratégia foi a seguinte:

No par Cliente : redirecionar o fluxo TCP (conexão de controle) e a rajada UDP (canal de dados) do Iperf3 para um porto local no qual o SoCAT estará escutando. O SoCAT então, traduz a conexão de controle em UDP e manda a rajada traduzida

para o par servidor. Note que para o canal de dados UDP do Iperf3, não é necessário traduzi-lo. Basta enviá-lo.

No par Servidor : o SoCAT escuta em um porto X pela conexão de controle (convertida em uma rajada UDP). Quando ele a recebe, ele traduz o UDP de volta para TCP (pois é esse o formato exigido) e entrega para o Iperf3 em seu porto Y. Já a rajada de dados UDP, que não precisa ser traduzida, chega diretamente no porto Y do Iperf3, pois o SoCAT no cliente é configurado para enviar diretamente para tal porto. Ou seja, a conexão de controle e o fluxo de dados percorrem caminhos diferentes para chegar a um mesmo destino, devido à necessidade de se traduzir a conexão de controle com o SoCAT.

Desta forma, a comunicação é estabelecida com sucesso. No cliente há uma instância do Iperf3 e dois SoCATs, no servidor há uma instância do Iperf3 e somente um SoCAT como mostra a Figura 3.

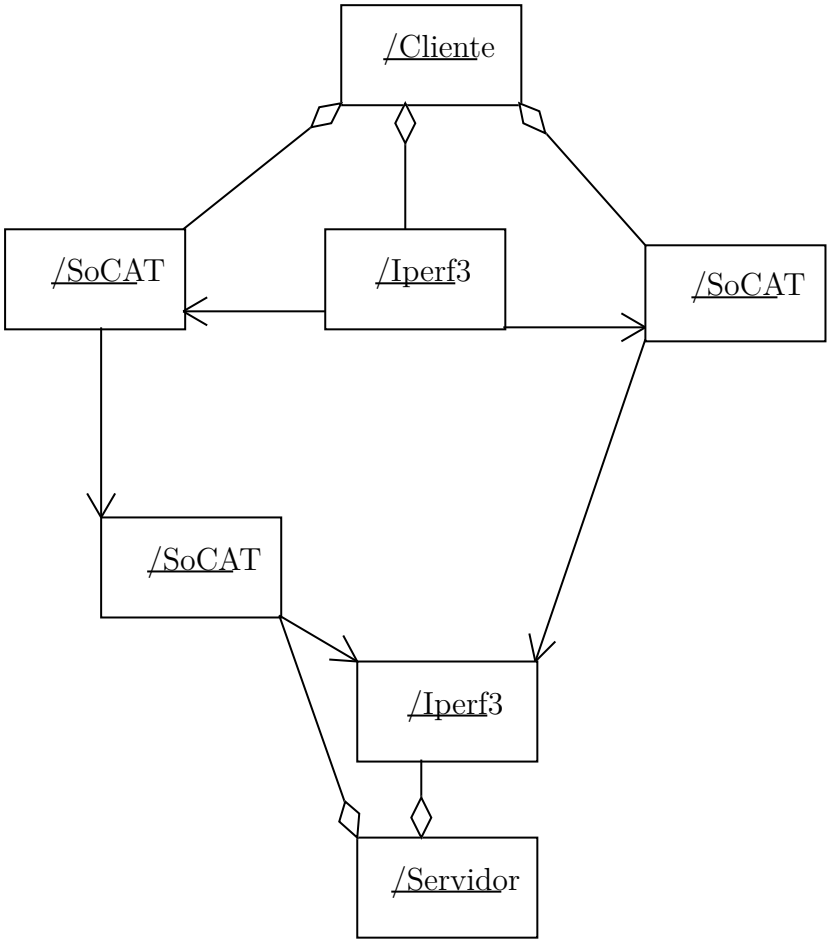


Figura 3 – Diagrama do percurso da comunicação no teste de *jitter* e perda de pacotes

Todavia, a tradução de TCP para UDP vem com alguns efeitos colaterais como: ausência de garantia de entrega, de retransmissões e de controle de congestionamento. Além disso, a técnica inviabiliza o cálculo do RTT (latência) pelo próprio teste TCP do

Iperf3. Este é o motivo pelo qual foi necessário utilizar complementarmente o Ultraping (seção 3.1). Devido aos efeitos colaterais causados pela tradução de TCP em UDP, em uma rede com perda de pacotes suficientemente alta, a aferição através do Iperf3 pode ser interrompida abruptamente ou sequer iniciada. Um pacote perdido pode interromper a comunicação necessária pelo canal de controle e isso afetará a execução do teste. Felizmente, não foi observado durante o desenvolvimento da ferramente e nem durante os experimentos a não inicialização de um teste pelo motivo citado, somente o encerramento abrupto do mesmo, em alguns casos. Todavia, isso não foi suficiente para interromper o funcionamento da Peertest.

Nas outras ferramentas utilizadas (Netcat e Ultraping) não foi necessário realizar a tradução do protocolo, visto que possuem configurações para trabalham em cima do protocolo UDP. Essa estratégia foi utilizada para possibilitar a execução do teste de *jitter* e perda de pacotes através do Iperf3. Os pares sabem para quais pontas se comunicarem, pois através da DHT são trocadas as pontas públicas após a perfuração de buracos UDP.

4.6 Teste de Vazão (Velocidade)

O teste de vazão é baseado na técnica de Saturação (ver Seção 2.3) e realizado da seguinte maneira: O par cliente enviará por 10 segundos, via Netcat, bytes ao par servidor. Os dados passam por um buraco furado nos NATs de ambos os pares. Esse novo buraco é informado ao par correspondente usando-se o canal de controle. O par servidor estará recebendo os dados via Netcat, e por um *pipe*, passará os dados recebidos ao PipeViewer, que fará o cálculo da vazão. Essa abordagem se fez necessária devido à limitação do teste UDP do Iperf3 de descobrir a vazão (Velocidade) máxima de uma conexão entre dois sistemas finais.

4.7 Teste de Latência

O Iperf3 possui aferição de latência, mas somente em conexões TCP. Devido à utilização do SoCAT como tradutor de protocolo, não é possível realizar esse tipo de aferição com o Iperf. O Iperf3 entrega os dados ao SoCAT localmente, e o SoCAT tem a função de realizar a tradução do protocolo e enviar, via interface de rede, os dados ao par correspondente. Quando o Iperf entrega os dados ao SoCAT, este retorna um ACK imediatamente ao Iperf e ele utiliza esse ACK para calcular a latência. Porém, esse ACK é local, e não representa a latência entre os pares da aferição (ver Figura 4).

Sendo assim, foi utilizada a biblioteca Ultraping escrita em Python. Ela calcula a latência como a média dos RTTs dos datagramas enviados e recebidos de volta. Para realizar o teste de latência é necessário furar dois buracos no par cliente e no par servidor.

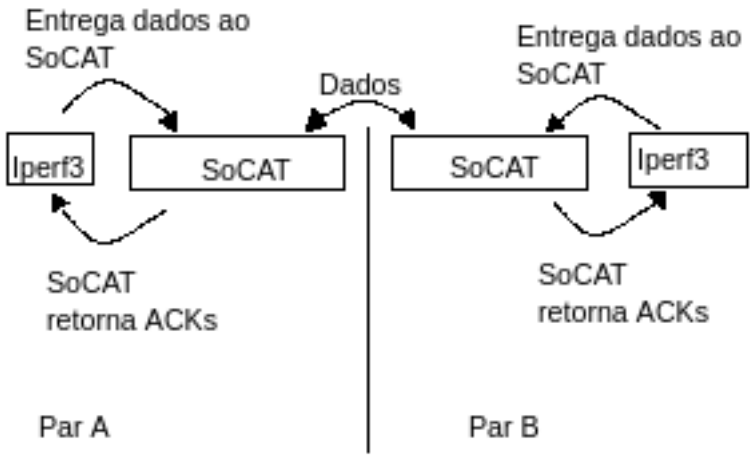


Figura 4 – ACKs trocados localmente entre as instâncias do Iperf3 e do SoCAT

Esses buracos são furados via STUN, sendo informados entre os pares pelo canal de controle previamente estabelecido e descoberto via DHT. No cliente, um buraco será para enviar datagramas UDP, e o outro buraco será para recebê-los de volta do servidor. No servidor, um buraco será para receber os datagramas, e outro para enviá-los ao cliente.

4.8 Portabilidade do Software

No repositório <https://github.com/Konomaster/TCC> se encontram instruções detalhadas para instalar a ferramenta (e suas dependências) nos ambientes GNU/Linux e POSIX (UNIX-like, ex.: MacOS, FreeBSD e afins). Adicionalmente, é possível também instalar e executar a ferramenta no Windows, e também nos ambientes citados anteriormente, através de contêiner Docker. Após a instalação do Docker[2], é necessário baixar a imagem da ferramenta disponibilizada publicamente através dos comandos:

```
docker pull konomaster/tcc:multiarch
```

```
docker run -it konomaster/tcc:multiarch bash
```

Execute o seguinte comando para aceitar a licença do Speedtest. O Código também fará aferições através dessa ferramenta, possibilitando comparar os resultados.

```
speedtest
```

[2] "*Install Docker Engine*" <https://docs.docker.com/engine/install/>

E, finalmente, execute a ferramenta dentro do contêiner através do comando:

```
python3 PoC.py
```

Após executar a ferramenta pelo comando acima, resultados das aferições estarão nos arquivos “results.txt” para a Peertest e “results_speedtest.txt” para o Speedtest.

4.9 Limitações em NATs

Foi observado que o NAT no qual o autor se encontrava não permitia a passagem de datagramas UDPs maiores que 1492 bytes. Sendo assim, no *wrapper* para o Iperf3, no SoCAT e no PipeViewer, foram adicionadas *flags* para assegurar que a comunicação UDP utilize pacotes com tamanhos menores que o limite descrito acima. Esse limite é uma característica implementada pelo provedor de acesso à internet do autor deste TCC e pode variar entre provedores.

No mês de setembro de 2022, a ferramenta desenvolvida neste trabalho passou a se comportar de forma incorreta sem que houvessem alterações no seu código-fonte. Por meio de experimentos, foi descoberto que o comportamento NAT do provedor de acesso à internet contratado pelo autor deste TCC havia sido alterado. Foi observado que o NAT passou a ser do tipo estrito, também conhecido como NAT tipo 3, que permite que determinado par A (atrás de um NAT estrito) se conecte a outro par B (numa rede diferente), somente se A enviar uma requisição primeiro a B.

De forma específica, considere dois pares A e B atrás de um NAT tipo 3. Suponha que A e B vão tentar executar a técnica de UDP *Hole Punching* para se conectarem diretamente. Sendo assim, A e B utilizam um servidor STUN para saber suas pontas públicas e trocam essa informação entre si. A envia uma mensagem para a ponta pública de B. Como explicado anteriormente, essa mensagem não chega para B, mas cria um mapeamento no NAT de A. Agora, como B está atrás de um NAT do tipo 3, essa primeira mensagem tem um efeito adicional: além do NAT de B não reconhecer a mensagem e descartar o pacote, ele também criará uma regra que forçará um novo mapeamento de ponta pública para B, caso ele tente se comunicar com A. Sendo assim, B tenta enviar uma mensagem à ponta pública de A. Agora, haverá o mapeamento de uma nova ponta pública para B, diferente da original. E diferente de antes em que a mensagem chegava para A e a técnica era executada com sucesso, agora o NAT de A não reconhecerá a mensagem vindo de B e descartará o pacote. Da mesma forma, se os papéis de A e B se inverterem, como ambos estão atrás de um NAT tipo 3, o problema persiste. Poderia ser feita a observação de que simplesmente fazer uma nova requisição STUN informaria o novo mapeamento realizado pelo NAT. Observe, entretanto, que o novo mapeamento é realizado somente se

B tenta se comunicar com A. Caso B tente se comunicar com o servidor STUN, ele ainda informaria a ponta pública original.

Registre-se que após experimentos, constatou-se que no mesmo mês outro provedor (o do orientador), também mudou seus NATs para o tipo 3. Isso sugere uma tendência dos provedores da região em utilizar esse tipo de NAT. Desta forma, para se conseguir realizar os experimentos, foi solicitado ao suporte técnico do ISP a alocação de um IP fixo fora do NAT, pois não havia a opção de retornar ao NAT tipo 2.

5 Apresentação e Análise e Resultados

Neste capítulo serão apresentados a configuração do experimento bem como a análise dos resultados, comparando as aferições da ferramenta Peertest contra as aferições do trabalho relacionado Speedtest. Serão avaliadas as métricas de perda de pacotes, latência, *jitter*, *download* e *upload*, fundamentais para avaliar o desempenho da conexão de internet e identificar possíveis problemas que possam afetar a qualidade do serviço prestado pelo ISP.

5.1 Configuração do Experimento

Materiais utilizados:

Nos experimentos, foram utilizados dois computadores: um notebook (Sistema operacional Ubuntu 20.04) e um Raspberry Pi 3 (Sistema operacional Raspberry Pi OS, baseado em Debian). A instalação da ferramenta Peertest foi feita através do passo a passo disponível no repositório[1] GitHub do projeto.

Topologia da rede: O notebook estava conectado à internet através do provedor TOP 37, utilizando uma conexão cabeada Ethernet. Já o Raspberry Pi conectou-se à internet através do provedor MAP, diretamente ao roteador também através de uma conexão Ethernet. Ambos os provedores atuam na cidade de Formiga-MG e região, trabalhando com a tecnologia de fibra ótica (PON). Através de solicitação de suporte técnico aos provedores, conseguiu-se migrar do NAT tipo 3 (que impediria qualquer experimento, como será detalhado nas considerações finais) para o NAT tipo 1, presente em ambas as pontas do experimento.

A vazão (velocidade) contratada era de 100 Mbits/s na conexão da TOP37 e de 250 Mbits/s na conexão da MAP Fibra. Vale notar, porém, que foram utilizados cabos Ethernet para conectar os sistemas finais diretamente ao roteador, em portas Fast Ethernet. Esse meio limita a vazão a um valor máximo de cerca de 100 Mbits/s.

A topologia de rede na direção do notebook até o Raspberry Pi se encontra abaixo:

```
thomas@Thomas-Predator:~$ sudo nmap -sn --traceroute 177.221.181.156
[sudo] password for thomas:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-28 17:42 -03
Nmap scan report for 156-181-221-177.mapminas.com.br (177.221.181.156)
Host is up (0.030s latency).
```

[1] <https://github.com/Konomaster/TCC>

```
TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   0.86 ms  192.168.0.1     ## Residential Gateway
2   4.16 ms  100.64.100.1    ## Top37 Carrier-Grade NAT (RFC6598)
3   5.56 ms  198.18.61.177   ## Special IPV4 Benchmark Test (RFC2544)
4   19.23 ms 177.67.85.149   ## Wixnet
5   20.02 ms 198.18.100.5    ## Special IPV4 Benchmark Test (RFC2544)
6   19.59 ms 198.18.1.162    ## Special IPV4 Benchmark Test (RFC2544)
7   28.78 ms 177.39.206.250  ## MapMinas
8   28.89 ms 10.1.1.1        ## Private Network (RFC1918)
9   30.77 ms 177.221.181.156 ## MapMinas

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Com a ajuda do utilitário *whois*, que apresenta informações sobre cada IP, foi possível ter uma ideia geral desse Traceroute:

O IP da linha 2 é reservado para uso em NAT de nível de operadora (CGNAT[2], RFC 6598[3]), através do qual redes residenciais são configuradas com endereços de rede privada, que são convertidos em endereços IPv4 públicos por dispositivos embutidos na rede da operadora de rede, permitindo o compartilhamento de pequenos grupos (quantidade limitada) de endereços IP públicos entre muitos sistemas finais.

Já os IPs das linhas 3, 5 e 6 são endereços privados (BRADNER; MCQUAID, **RFC 2544**. 1999), aparentemente utilizados na rede interna de cada provedor ao qual eles pertencem. Até onde pudemos levantar, conforme consulta do servidor *whois* da IANA[4], endereços começando com 198.18 ou 198.19 são reservados para uso em redes de laboratório isoladas usadas para *benchmarking* e testes de desempenho. Pelas informações obtidas via IANA, "tais endereços IP nunca devem aparecer na Internet e se você vir tráfego na Internet usando esses endereços, eles estão sendo usados sem permissão". Entretanto, não pudemos levantar informações acerca de autorização especial para o uso de tais endereços IP.

O IP da linha 4 mostra que o tráfego passou por roteador do provedor[5] Wix Net do Brasil, baseado na cidade de Belo Horizonte/MG. O endereço IP da linha 8 também é de uso reservado em rede privada (REKHTER et al., **RFC 1918**. 1996), tipicamente

[2] "Carrier Grade NAT"<https://en.wikipedia.org/wiki/Carrier-grade_NAT>. Acessado em 7 fev.. 2023.
[3] <https://datatracker.ietf.org/doc/html/rfc6598>
[4] <https://query.milacnic.lacnic.net/search?id=198.18.61.177>
[5] <https://registro.br/tecnologia/ferramentas/whois/?search=177.67.85.14>

usado para redes locais (LANs - Local Area Networks) em ambientes residenciais, de escritório e corporativos. Os endereços de rede privada não são alocados para nenhuma organização específica. Portanto, qualquer pessoa pode usar esses endereços sem a aprovação dos órgãos de registro regional/local. Por fim, os IPs das linhas 7 e 9 correspondem a roteadores do provedor MAP.

Analisando esse *traceroute*, pode-se inferir que o trafego, após sair do hospedeiro, passou pela rede da TOP 37 (IPs 1 a 3), depois pela rede da Wix Net em Belo Horizonte (IPs 4 a 6) e finalmente pela rede da MAP (IPs 7 a 9).

As tentativas de obter a topologia na direção contrária, isto é, partindo do Raspberry Pi, foram infrutíferas. Aparentemente o *firewall* do provedor MAP bloqueia em sua rede interna os pacotes necessários ao funcionamento do software Traceroute, impossibilitando tal coleta. Essa informação seria interessante para que se possa ter uma noção da topologia de rede dentro da rede privada ao qual o Raspberry Pi estava conectado. Nem o Traceroute e nem o Nmap conseguiram fazer uma varredura da topologia na direção oposta, seja utilizando ICMP, seja utilizando UDP:

Dados coletados: Tanto nas aferições utilizando a ferramenta Peertest desenvolvida neste TCC (Par-a-Par) quanto utilizando o Speedtest-cli (Cliente-Servidor), foram coletadas as seguintes informações: horário da aferição (*timestamp*), vazão (velocidade) de *download* e *upload*, *jitter*, porcentagem de perda de pacotes e latência.

Naturalmente, a informação do ID do par na DHT com o qual a aferição foi realizada se encontra somente nos testes com a Peertest. Já as informações do provedor de internet do cliente, bem como qual servidor do Speedtest.net utilizado na aferição, são apresentados nos testes utilizando o software Speedtest-cli.

O experimento foi realizado entre os dias 28/01/2023 e 07/02/2023 (11 dias) e as aferições aconteciam a cada 15 minutos. Primeiro eram realizadas as aferições com a Peertest e, logo após, com o Speedtest.

5.2 Caracterização da coleta

Em relação às aferições realizadas, foram obtidos os seguintes resultados:

No notebook que estava localizado na intranet da TOP37:

- 680 linhas com resultados das aferições da Peertest (ferramenta desenvolvida). Após tratamento dos resultados aproveitou-se 659 linhas.
- 738 linhas com resultados das aferições do Speedtest. Não foi necessário descartar nenhum dos resultados.

No RPI localizado na intranet da MAP Fibra:

- 668 linhas com resultados das aferições da Peertest (ferramenta desenvolvida). Após tratamento dos resultados aproveitou-se 631 linhas.
- 737 linhas com resultados das aferições do Speedtest. Não foi necessário descartar nenhum dos resultados.

Através dos experimentos, pudemos observar que os resultados de latência, e perda de pacotes da Peertest sempre tiveram valores maiores em comparação ao Speedtest, nos dois pares do experimento. O motivo desse comportamento é que, quando o Speedtest faz a aferição contra servidores do próprio provedor de internet, os resultados obtidos refletem a intranet do provedor, o que tende a apresentar resultados muito melhores. Além disso, o teste feito dessa maneira não afere as condições de acesso à internet, o que é de fato contratado pelo cliente.

5.3 Impacto do ciclo circadiano no tráfego da internet

O ritmo circadiano refere-se ao ciclo de 24 horas que regula os processos biológicos em muitos organismos, incluindo os seres humanos. Algumas pessoas têm mais energia e atenção durante a manhã, enquanto outras podem ter um pico de produtividade à tarde ou à noite. Devido às flutuações no desempenho cognitivo ao longo do dia, é possível que o tráfego de internet varie conforme o horário. Durante os horários em que as pessoas estão mais produtivas, pode haver um aumento no tráfego de internet para atividades que exigem mais atenção e concentração, como realizar trabalhos *online* ou participar de reuniões virtuais. Já em horários de menor produtividade, é possível haver um aumento no tráfego para atividades de entretenimento, como navegar em redes sociais, disputar jogos eletrônicos ou assistir a vídeos online.

No geral, foi detectado que tipicamente houve mais perdas de pacote no horário entre 5:00 às 23:59. Essa tendência se mostrou presente em todos os experimentos realizados, seja via Peertest, seja via Speedtest. Outra tendência foi detectada nos testes do Speedtest contra o servidor VITALNET. A Figura 5 mostra *boxplots* na vertical, para cada dia da semana, em relação à variabilidade da taxa de perda de pacotes detectadas no referido servidor. Pôde-se observar, que nos horários de 19:00 às 22:00, houve perdas de pacotes. Esse comportamento também é ilustrado pela Figura 5 embora o agrupamento dos dados a cada duas horas dificulte a definição precisa do intervalo, mencionado acima, por esse gráfico. Além disso, esse era o único momento em que aconteciam perdas significativas (P75 $>$ P50 ou muitos valores atípicos) nos testes feitos contra esse servidor. Isto corrobora com a percepção atual sobre o horário de pico da internet brasileira, de acordo com tráfego agregado registrado pelo IX.br para a internet brasileira (ver Figura 6).

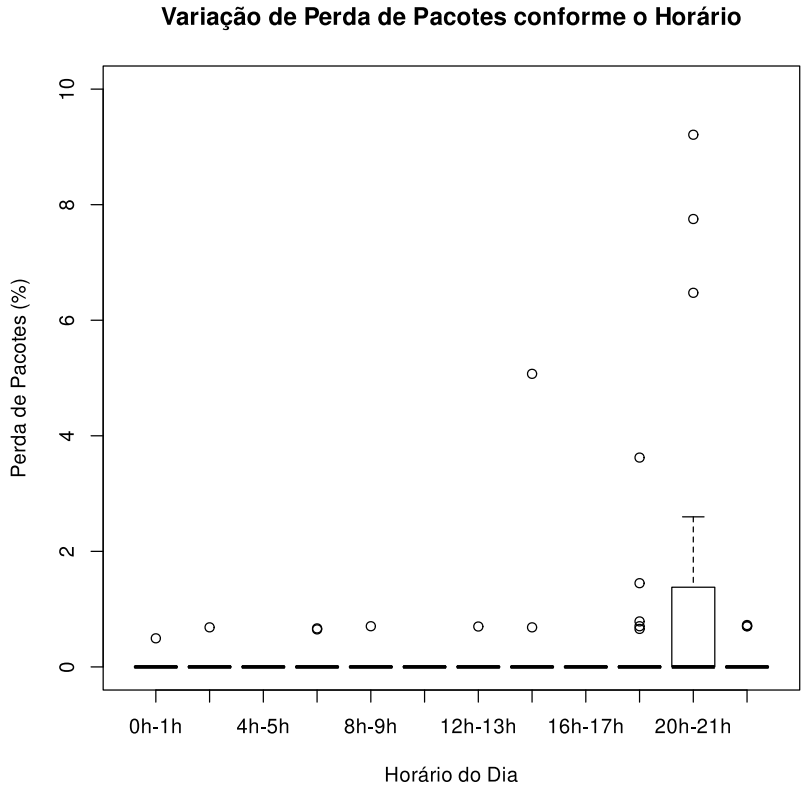


Figura 5 – Perda de pacotes (Speedtest), por hora do dia

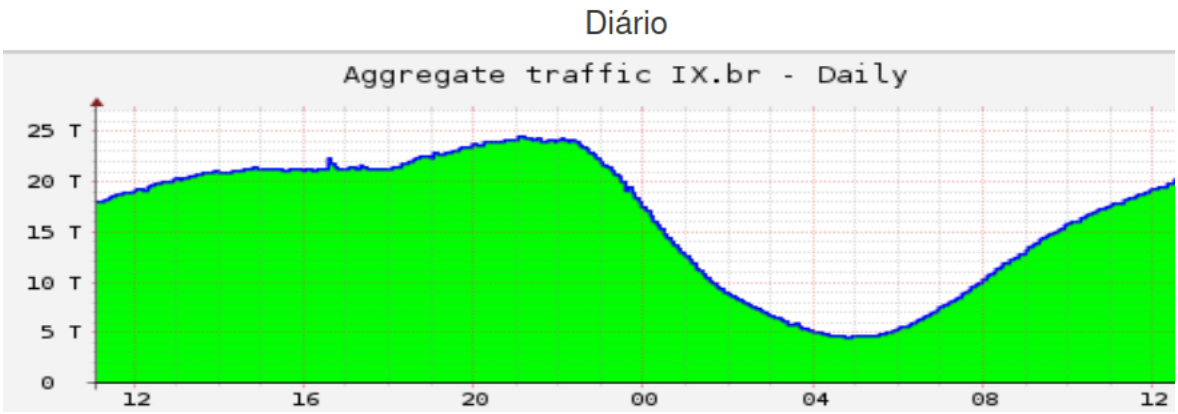


Figura 6 – Tráfego (Tbit/s) da internet brasileira, por hora do dia
FONTE: <https://ix.br/agregado/>

Os 5 primeiros *boxplots* da Figura 5 não foram distortos pela escala no eixo Y. O que aconteceu é que todos os quartis foram iguais a 0.

5.4 Análise da perda de pacotes

5.4.1 Peertest vs Speedtest (com servidor dentro do ISP)

O objetivo dessa seção é comparar os resultados da ferramenta desenvolvida com os resultados do Speedtest (com seu servidor dentro do mesmo provedor). Assim, será possível perceber se nesse caso, o Speedtest apresentaria resultados "otimistas", mas fora da realidade do acesso residencial à internet.

A Figura 7 mostra as principais estatísticas para a perda de pacotes aferida com a Peertest e a Figura 8 para o Speedtest (contra o servidor da TOP 37). Observa-se uma baixa taxa de perda de pacotes no Peertest (média=0,075%) e inexistente[6] no Speedtest (média=0%). Vale ressaltar que os computadores clientes nos quais os testes foram executados encontravam-se conectados ao roteador/ONU via cabo metálico (Ethernet) e dele ao provedor via fibra óptica (PON - *Passive Optical Network*), mídias que tipicamente apresentam baixa probabilidade de perda de pacotes se comparadas com acessos sem fio via radiofrequência. A Peertest apresentou uma maior variabilidade dos dados (CV=6,33), chegando a registrar um máximo de 10,6% de perda de pacotes.

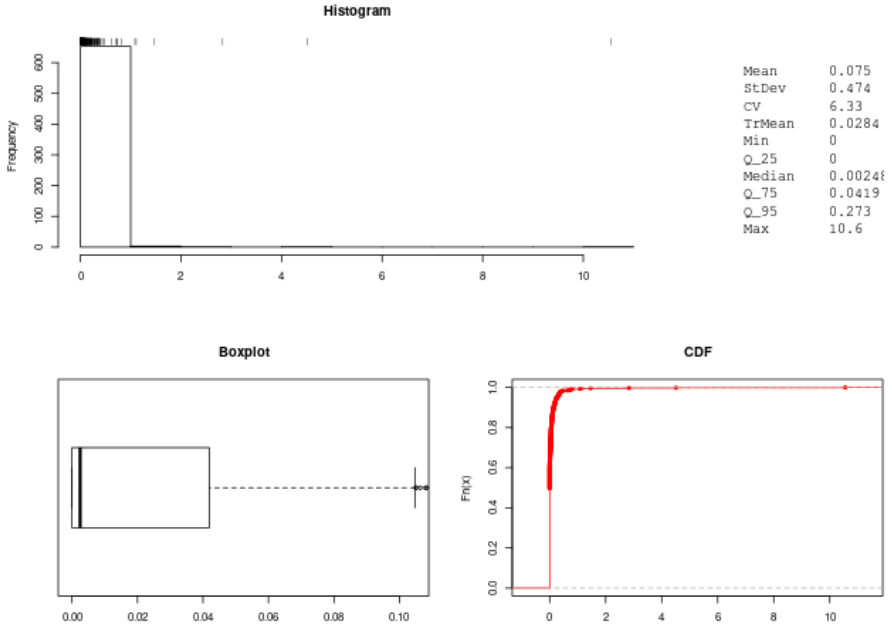


Figura 7 – Perda de Pacotes (%) aferida via Peertest

Comparando-se ambas as Figuras 7 e 8, observa-se que as medições com a Peertest registraram taxas de perda ligeiramente acima de 0%. Por exemplo, o quartil Q3 registra 0,0419% e 95% das medições (P95) estão abaixo de 0,273% de perda de pacotes. Isso é de se esperar pelo fato de que os pares utilizados nas medições do Peertest estarem em ISPs

[6] Todas as medições obtidas via cliente Speedtest contra o servidor do próprio provedor apresentaram 0,0% de perda de pacote.

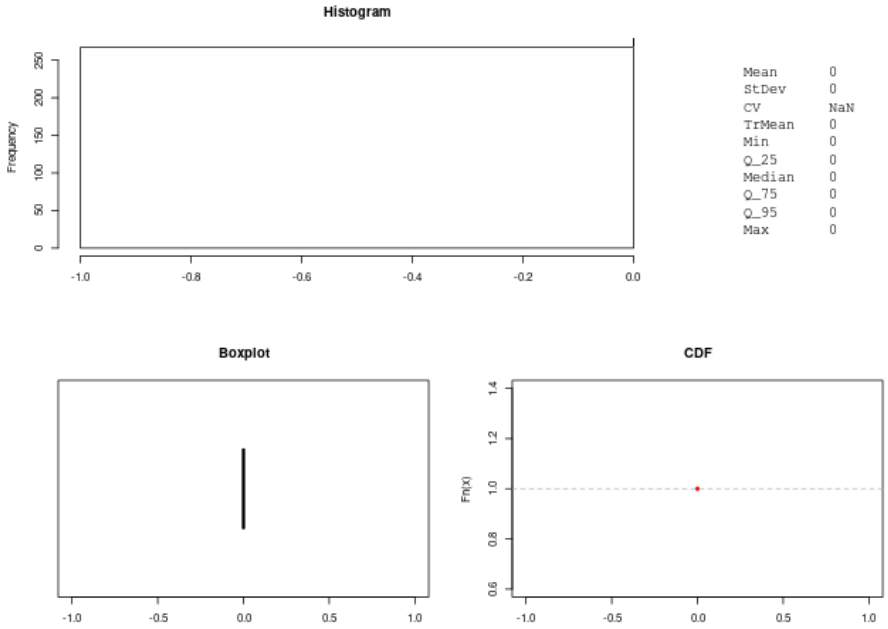


Figura 8 – Perda de Pacotes (%) aferida via Speedtest

diferentes (portanto percorrendo a internet) enquanto tanto o cliente quanto o servidor utilizado pelo Speedtest estarem ambos no mesmo ISP e, portanto, autocontidos na rede daquele sistema autônomo.

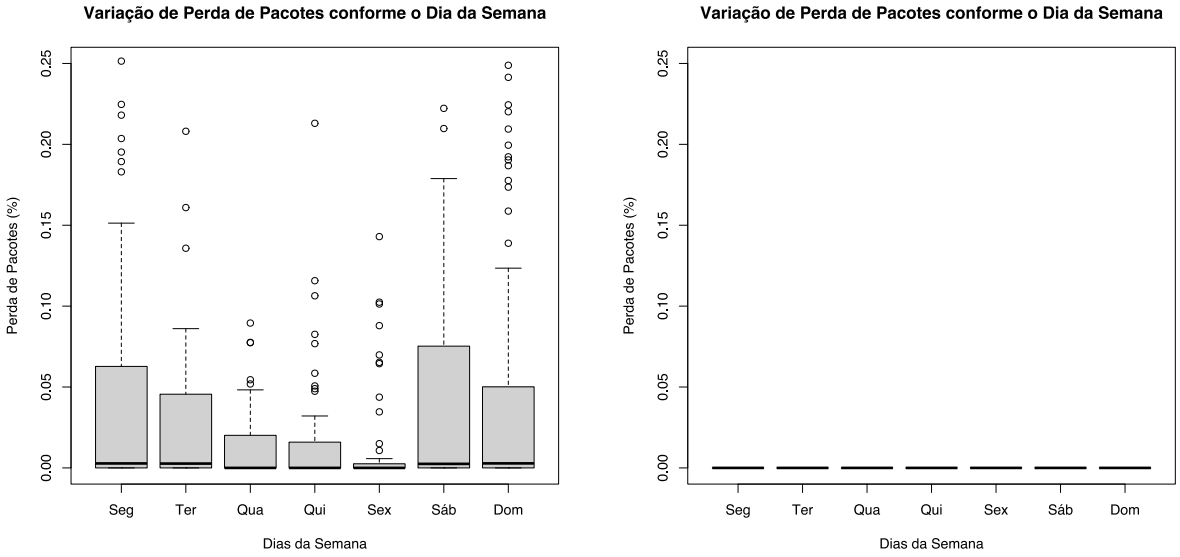
A perda de pacotes observada pode ser considerada satisfatoriamente baixa tanto no Peertest (P95 $<$ 0,27%) quanto no Speedtest (P95 $<$ 0,00%), considerando que 2% de perda de pacotes é o valor máximo permitido pela Resolução nº 574 da ANATEL, para o percentil de 95%.

5.4.2 Análise temporal: Peertest vs Speedtest (com todas as aferições)

Nessa seção são apresentadas análises temporais da latência para hora do dia e dia da semana. São consideradas na comparação, as aferições do Peertest e todas as aferições do Speedtest, incluindo as aferições com servidor dentro do ISP[7] e fora do ISP[8]. Desta maneira, evita-se limitar (ou enviesar) a análise apenas aos momentos em que houve medições através do Speedtest com servidor dentro ou através do Speedtest com servidor fora.

Conforme pode-se observar na Figura 9a, os dados de qualidade da internet coletados via Peertest demonstraram uma tendência de aumento na perda de pacotes com a proximidade dos finais de semana, em especial nos dias sábado, domingo e segunda-feira. Por outro lado, os dados coletados via Speedtest (ver Figura 9b) dão a impressão de que não haveria impacto algum do comportamento humano ao longo da semana na perda de

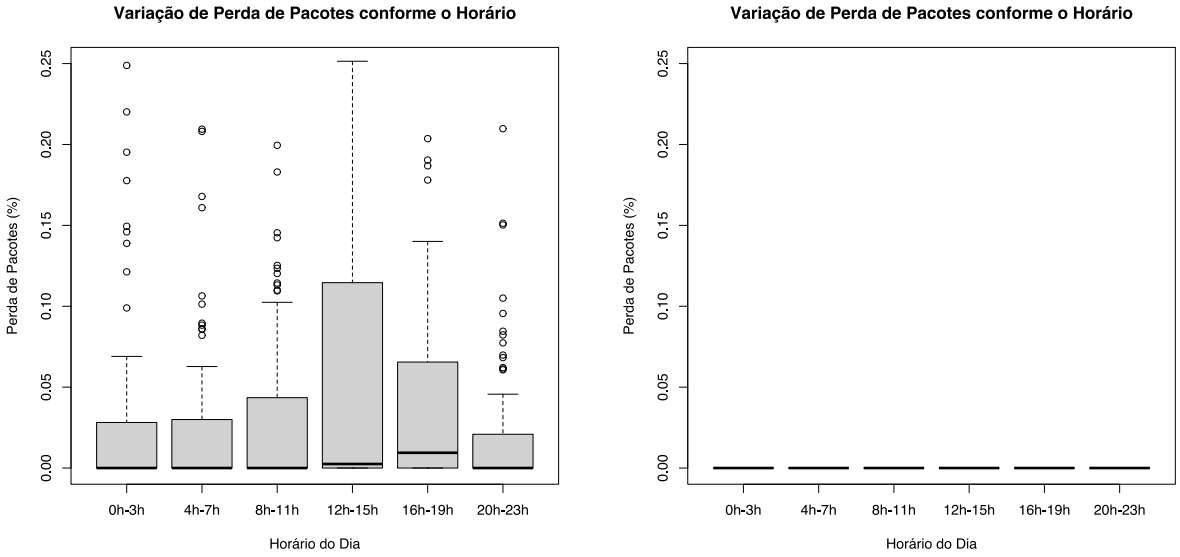
[7] 267 aferições
[8] 471 aferições



(a) Peertest (b) Speedtest

Figura 9 – Variação semanal na Perda de Pacotes

pacotes, como se não houvesse sobrecargas e congestionamentos no tráfego da internet independente do dia da semana.



(a) Peertest (b) Speedtest

Figura 10 – Variação horária na Perda de Pacotes

De forma equivalente, observa-se pela Figura 10a que os dados coletados via Peertest denotam uma tendência no aumento da perda de pacotes na proximidade do horário de almoço típico, com picos registrados entre 12h e 15h. Uma maior demanda de utilização dos equipamentos de rede durante o horário de almoço poderia explicar tal aumento sutil na taxa de perda de pacotes. Novamente, analisando-se a Figura 10b não se observa nenhuma flutuação na taxa de perda de pacotes ao longo do dia, como se não houvesse

maior demanda de utilização da internet e concentração de pessoas em horários específicos do dia/noite.

5.5 Análise da latência

Em geral, quanto maior a distância entre os dispositivos e mais congestionada a rede, maior será a latência. Vale destacar que a latência é um fator crítico em muitas aplicações de rede, especialmente aquelas que exigem uma resposta em tempo real, como jogos *online*, videoconferências e transmissão de áudio ou vídeo em tempo real. Uma latência alta pode causar um atraso na transmissão de dados, o que pode afetar a velocidade de carregamento de páginas web, por exemplo, ou tornar a navegação na internet mais lenta e menos responsiva. Também, em sistemas de transações financeiras ou de comércio eletrônico, uma latência alta pode causar falhas nas transações ou atrasos no processamento de pagamentos, o que pode afetar negativamente a experiência do cliente.

5.5.1 Peertest vs Speedtest (com servidor dentro do ISP)

A Figura 11 apresenta um resumo estatístico descritivo das medições realizadas para a métrica latência aferida com a ferramenta Peertest. Nela, observe que a mediana para a latência observada foi de 31,3 ms, com um valor mínimo de 26,9 ms e o máximo de 141 ms. Já a Figura 12 apresenta o resumo estatístico da latência aferida com a ferramenta Speedtest contra o servidor da própria TOP 37. Neste caso, foi constatada uma mediana para a latência de 1,13 ms, com mínimo de 0,9 ms e máximo de 8,47 ms.

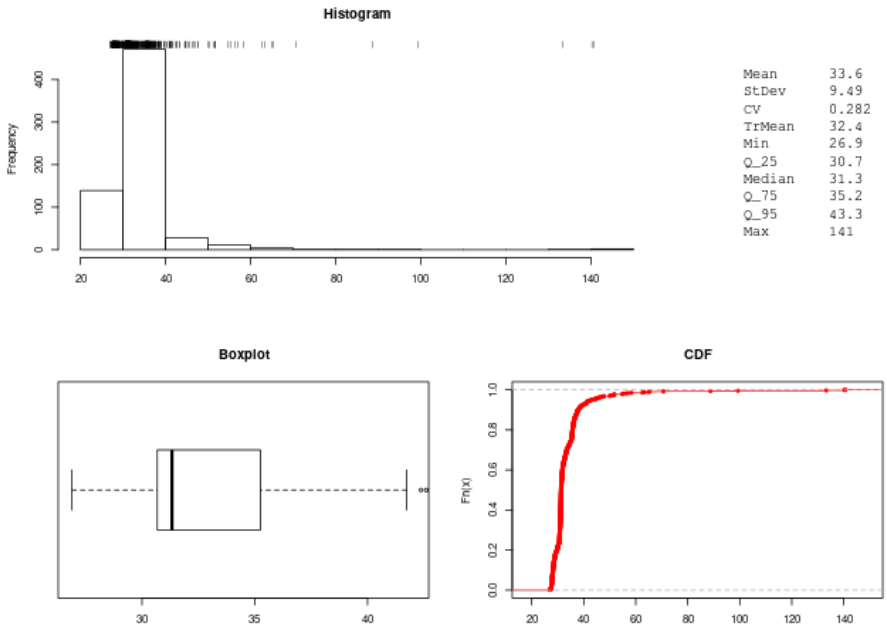


Figura 11 – Latência aferida via Peertest em ms

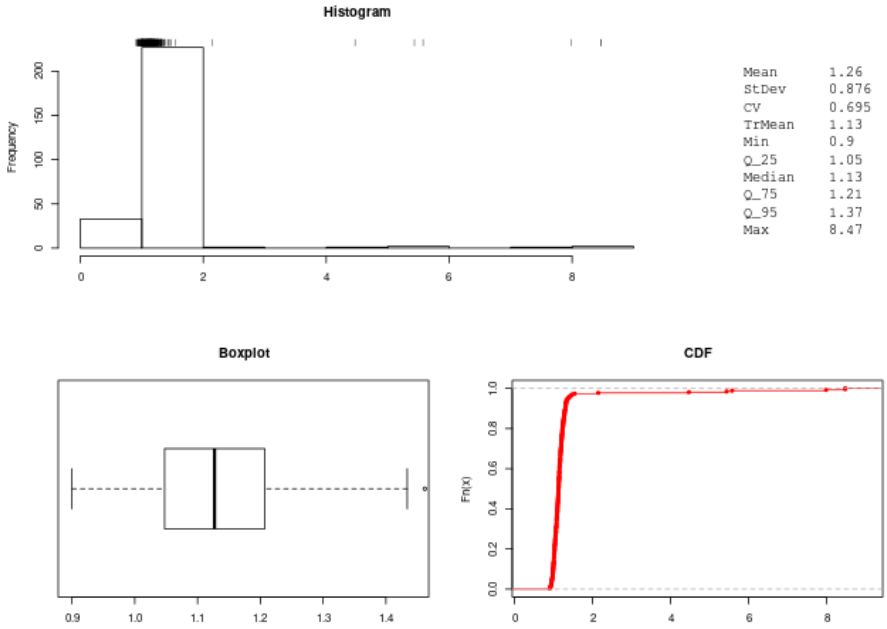


Figura 12 – Latência aferida via Speedtest em ms

Em termos gerais, o resultado do Speedtest apresentou latência 26 vezes melhor em comparação à Peertest. Tal diferença se explica pelo servidor do Speedtest estar localizado dentro da infraestrutura de rede do ISP ao passo que o par contactado via Peertest encontra-se efetivamente através da internet, em outro ISP.

Comparando as duas figuras, primeiramente observa-se pelos histogramas que as medições realizadas tanto pela Peertest quanto pelo Speedtest apresentam uma obliquidade (*skewness*) com cauda à direita. Também, as medições via Peertest apresentaram menor variabilidade estatística (CV=0,282) em comparação à Speedtest (CV=0,695). No *boxplot* (diagrama de caixa) da latência aferida via Peertest, observa-se uma distribuição mais assimétrica dos dados (considerando a posição da mediana em relação ao primeiro e terceiro quartis). Além disso, percebe-se também mais *outliers* (valores atípicos). Já no *boxplot* do Speedtest (ver Figura 12), claramente a distribuição dos dados é um pouco mais simétrica, mais previsível. Assim, devido ao coeficiente de variabilidade apresentado, bem como os outros fatores, as aferições realizadas pelo Speedtest passam a sensação de resultados mais confiáveis e estáveis.

Deve se considerar, porém, que devido ao valor da média ser muito pequeno (1,26 ms enquanto a ANATEL exige abaixo de 80 ms) e, talvez até artificialmente baixo pelos testes serem realizados na intranet do próprio provedor, qualquer variação de poucos milissegundos tornarão o CV maior pelo fato dessa pequena flutuação ser um valor proporcionalmente grande em relação à média. Isso não acontece na Peertest que, por realizar aferições com pares através da internet, apresenta uma latência que incorpora atrasos provenientes de instabilidades na internet. Assim, por apresentar uma latência

média de magnitude bem acima, as variações ocorridas no Peertest, ainda que maiores numericamente se comparadas as do Speedtest, proporcionalmente tem menor impacto no CV (complementarmente, compare os respectivos *boxplots*). Dessa forma, percebe-se que a amplitude dos dados de latência observados no Speedtest é bem menor em comparação com a latência registrada via Peertest. Pondere, no cenário dinâmico da internet, quais desses comportamentos estariam mais próximos da realidade observada subjetivamente por usuários residenciais ao acessar recursos na internet por intermédio de seus respectivos ISPs.

Mediante uma inspeção visual, a função de distribuição cumulativa (CDF) da Figura 12 (Speedtest) demonstra uma baixa variância, ao contrário da CDF da Figura 11 (Peertest) que visivelmente apresenta uma maior variância, o que é de se esperar ao realizar aferições em um cenário mais dinâmico e, pode-se dizer, mais realista do ponto de vista da internet. Por exemplo, nos dados do Speedtest há uma baixa probabilidade de se deparar com uma latência acima de 2,13 ms (média + um desvio padrão). Por outro lado, há uma probabilidade significativamente maior de se deparar com latências maiores que 43,09 ms (média + um desvio padrão) nos dados do Peertest. Complementarmente, considere os histogramas das Figuras 11 e 12: neles, observa-se uma maior concentração dos dados na proximidade da média no caso do Speedtest em comparação ao Peertest. Vale destacar que, ao contratar um acesso à internet, deseja-se uma boa conexão não somente ao provedor de acesso (ISP) mas principalmente uma boa conexão com a internet pública brasileira (através da qual serão acessados os serviços desejados pelo cliente). Neste sentido, pode-se dizer que os resultados apresentados pelo Peertest representam melhor a experiência subjetiva que o cliente residencial observa ao utilizar sua internet contratada.

Em ambos os casos, tanto no Peertest quanto no Speedtest, a caracterização da latência se encontra bem abaixo do valor mínimo (P95 $<$ 80 ms) exigido pela ANATEL na Resolução nº 574, que até onde pudemos levantar, foi o último documento a especificar, de forma clara, limites para qualidade de serviço no provimento da internet por ISPs no Brasil.

5.5.2 Speedtest (com servidor fora do ISP)

Serão apresentados agora os resultados do Speedtest realizados contra servidores fora do mesmo ISP do cliente.

As aferições do Speedtest com servidor fora da intranet do provedor, como mostra a Figura 13, apresentaram uma média de 15,2 ms para a latência. Esse valor provavelmente é devido ao cenário "menos otimista" em relação às aferições. Além disso, o CV foi de 0,236, apresentando uma variabilidade mais próxima àquela constatada via Peertest. Aqui, novamente, como a média teve um valor bem acima do desvio padrão, proporcionalmente variações na latência tem menos impacto no coeficiente de variabilidade.

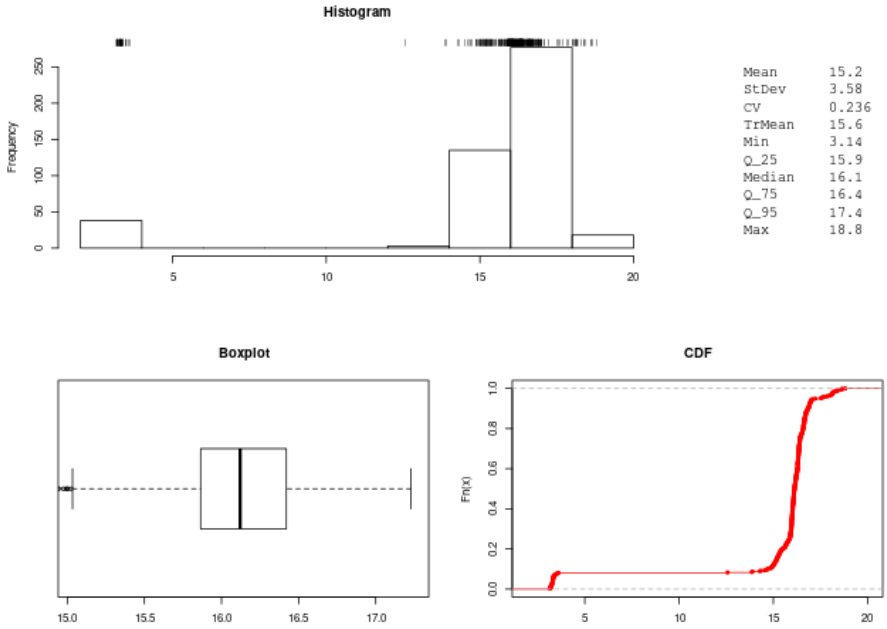


Figura 13 – Latência aferida via Speedtest (com servidor fora do ISP) em ms

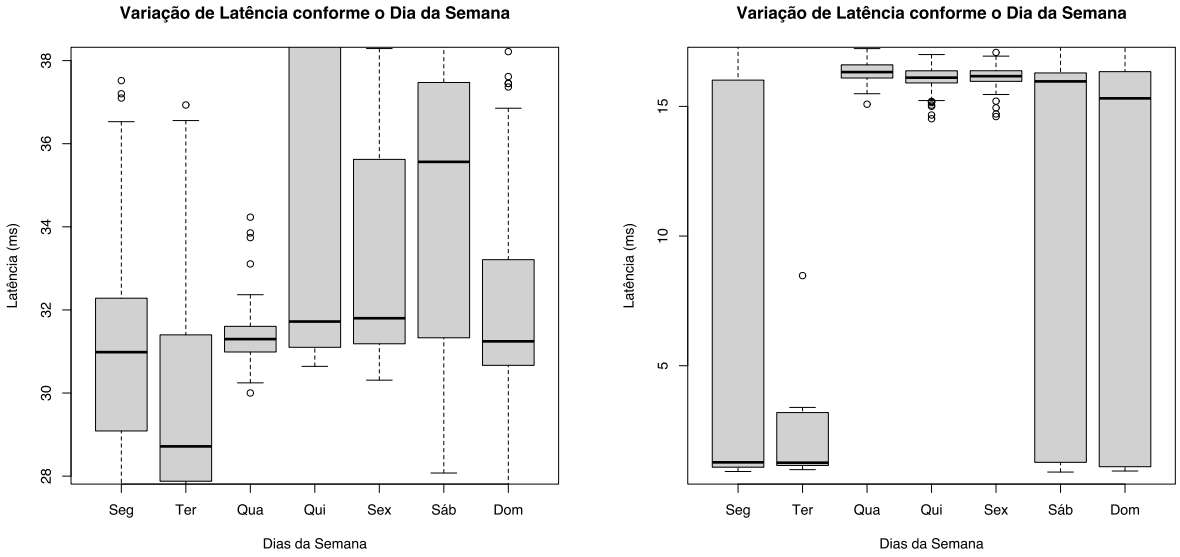
O histograma apresenta uma distribuição com cauda longa com obliquidade à esquerda, indicando que a maioria dos dados se concentram acima da média. O *boxplot* na Figura 13, assim como no Speedtest com servidor dentro do ISP (Figura 12), apresenta uma variabilidade semelhante entre os valores acima e abaixo da média, passando a sensação de resultados "mais estáveis" (baixa variabilidade).

Curiosamente, como também é mostrado no *rug plot*, houve uma quantidade significativa de *outliers* (valores atípicos) próximos a 3 ms. Esses resultados aconteceram de forma consecutiva após às 20:25 do dia 07/01/2023, sendo estatisticamente considerados comportamentos anômalos (ou mesmo erros experimentais). A CDF apresentou uma variância maior do que o Speedtest com servidor dentro do ISP (Figura 12). Devido aos *outliers* supracitados, essa variância também foi maior em relação àquela observada no Peertest (Figura 11). Dessa forma, como pudemos perceber, as aferições do Speedtest com servidor fora do ISP tiveram um comportamento diferente do Speedtest com servidor dentro do mesmo ISP do cliente, tendo apresentado resultados mais similares à Peertest.

Considerando a qualidade de serviço esperada, os resultados do Speedtest (com servidor fora do ISP) também se encontram dentro do limite especificado pela Anatel, com um P95 de 17,4 ms.

5.5.3 Análise temporal: Peertest vs Speedtest com todas as aferições

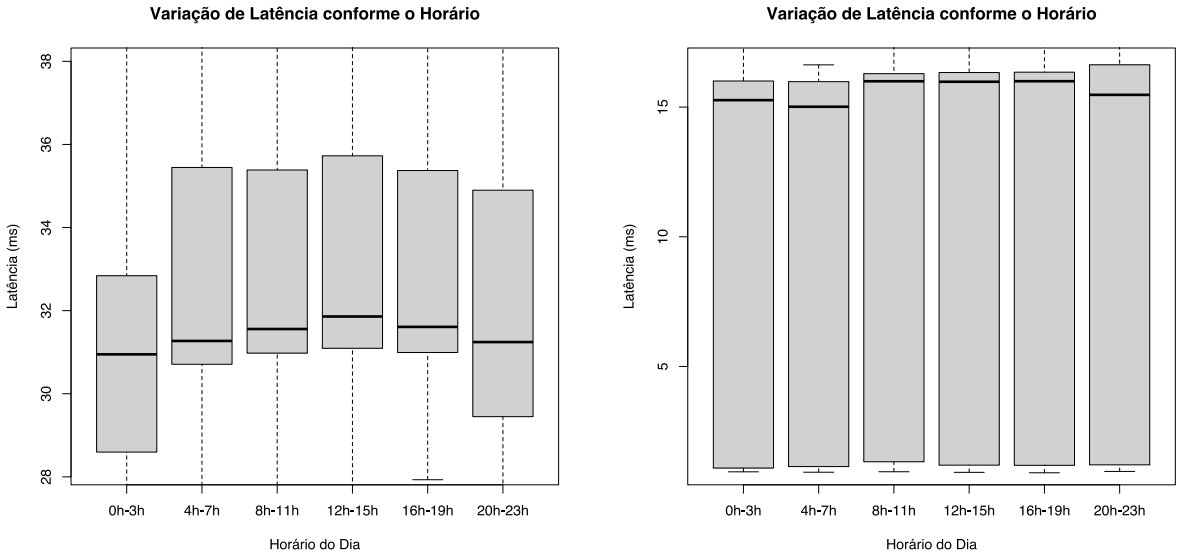
Analisando a Figura 14a, através dos dados coletados via Peertest, observa-se ao longo da semana uma tendência de crescimento na latência de comunicação de terça-feira



(a) Peertest (b) Speedtest

Figura 14 – Variação semanal na Latência

até sábado, com uma posterior tendência de decréscimo na latência nos dias subsequentes. Assim, as latências registradas foram menores às terças-feiras e maiores aos sábados. Por outro lado, nos dados aferidos via Speedtest (ver Figura 14b), notamos latências mais baixas às terças-feiras, com um aumento consistente e homogêneo de quarta a sexta-feira. Já nos dias de sábado a segunda-feira, é possível observar muita variabilidade na latência aferida conforme ilustram os respectivos *boxplots*. Vale destacar que, ignorando as diferenças de magnitude, é possível relacionar as duas tendências observadas tanto no Peertest quando no Speedtest.



(a) Peertest (b) Speedtest

Figura 15 – Variação horária na Latência

Complementarmente, considerando a tendência do tráfego de internet ao longo das horas do dia, pela Figura 15a constatamos nos dados do Peertest uma tendência de aumento da latência da manhã até o horário do almoço, com subsequente queda da latência ao longo da tarde e noite. Vale destacar que, conforme esperado, registramos os menores valores de latência durante a madrugada. Pela Figura 15b, pode-se observar um ligeiro aumento na mediana da latência pela manhã e tarde, com posterior redução à noite e de madrugada. Os dados coletados via Speedtest mostram uma grande variabilidade, porém represados abaixo de 15 ms aproximadamente. Vale destacar que, diferentemente dos dados apresentados no resumo de estatísticas descritivas da Figura 12 (max=8,47 ms), ao gerar os *boxplots* foram mantidas medições realizadas via Speedtest com servidores que não se encontravam necessariamente dentro da rede interna do ISP (max=18,8 ms). Ainda assim, pela magnitude dos valores, as medições realizadas via Speedtest ainda são demasiado otimistas e aparentemente não capturam o impacto do ritmo circadiano (ver Seção 5.3) dos seres humanos no tráfego da internet.

5.6 Análise do *jitter*

5.6.1 Peertest vs Speedtest (com servidor dentro do ISP)

A Figura 16 apresenta o resumo estatístico das medições realizadas para a métrica *jitter* aferida com a ferramenta Peertest (mediana=0,177 ms), ao passo que a Figura 17 apresenta as estatísticas do *jitter* com o Speedtest (mediana=0,126 ms).

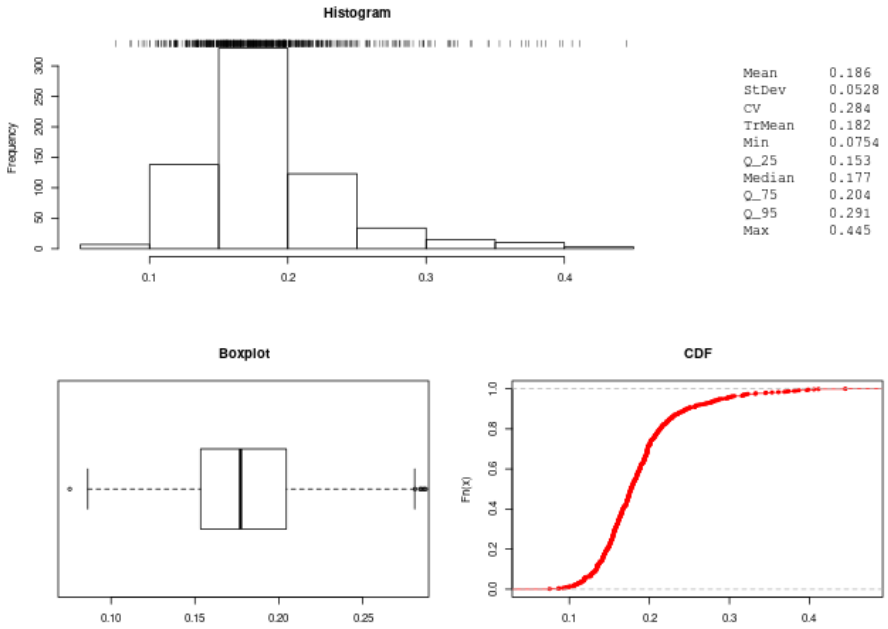


Figura 16 – *Jitter* aferido via Peertest em ms

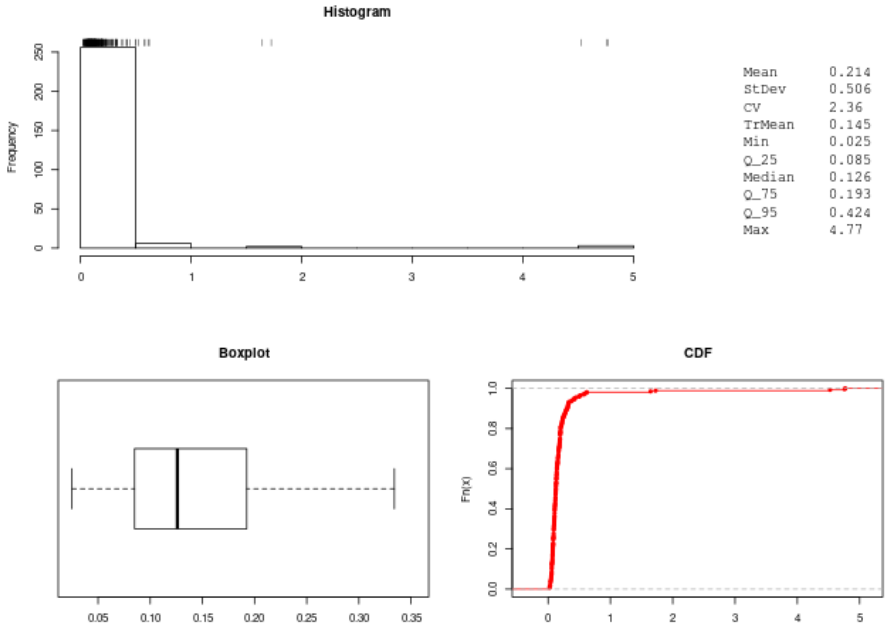


Figura 17 – *Jitter* aferido via Speedtest em ms

Comparando-se as Figuras 16 e 17, em ambos os casos, percebe-se que o *jitter* observado foi significativamente baixo tanto no Peertest (P95 < 0,291 ms) quanto no Speedtest (P95 < 0,424 ms).

O coeficiente de variação (CV) para o *jitter* pode ser utilizado para avaliar a estabilidade da latência da rede. Se o CV para o *jitter* for baixo, isso indica que a variação da latência é relativamente constante e previsível. Por outro lado, se o CV para o *jitter* for alto, isso indica que a variação da latência é mais imprevisível e instável, o que pode afetar a qualidade do serviço de internet. Portanto, quanto menor o CV para o *jitter*, melhor a qualidade do serviço de internet em termos de estabilidade de latência. No caso desta métrica, a Peertest capturou uma menor variabilidade (CV=0,284) do que o Speedtest (CV=2,36).

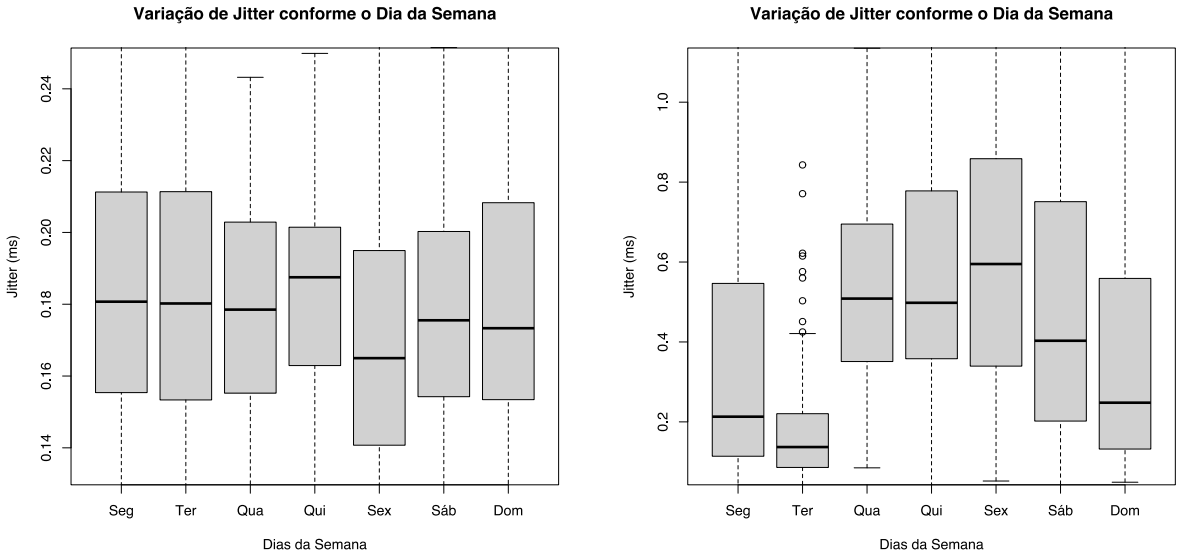
Analisando-se as distribuições de ambos, as medições de *jitter* via Speedtest tiveram grande obliquidade com cauda à direita (com a massa concentrada à esquerda, abaixo da média), enquanto via Peertest a obliquidade é mais neutra (há maior simetria ao redor da média), com o histograma do Peertest aparentando mais uma distribuição normal do que uma exponencial.

No Speedtest o *jitter* teve um comportamento de cauda longa, com a maioria das medições próximas da média, porém algumas delas extremamente distantes da média. Por exemplo, considere que no *jitter* do Speedtest, enquanto 95% dos dados (P95) estão abaixo de 0,424 ms, foi observado um valor máximo de 4,77 ms (9 desvios padrão após P75). Já no Peertest, há um comportamento de cauda curta, com uma obliquidade à direita, porém com muitos valores gradualmente se dissipando ao se distanciar da média (ver *rug plot*

acima das barras). Considere que, no *jitter* do Peertest, 95% dos dados (P95) estão abaixo de 0,291 ms e o valor máximo é de 0,445 ms (4,5 desvios padrão após P75). Ou seja, os dados no Peertest não estão tão distantes da média quando os dados do Speedtest. Vale destacar que os valores aferidos em ambas as ferramentas estão bem abaixo do máximo (P95 $<$ 50 ms) exigido pela Resolução nº 574 da ANATEL. Isso é um ponto positivo, pois o *jitter* é importante para aplicações interativas, como videoconferências.

5.6.2 Análise temporal: Peertest vs Speedtest (com todas as aferições)

No caso do *jitter*, não se observa uma tendência clara ao longo dos dias da semana, para os dados coletados via Peertest (ver Figura 18a), apenas que o *jitter* foi maior às Quintas e menor às sextas-feiras. Já nas medições realizadas via Speedtest (ver Figura 18b), há uma tendência de aumento do *jitter* de terça a sexta-feira e de redução nos dias posteriores.



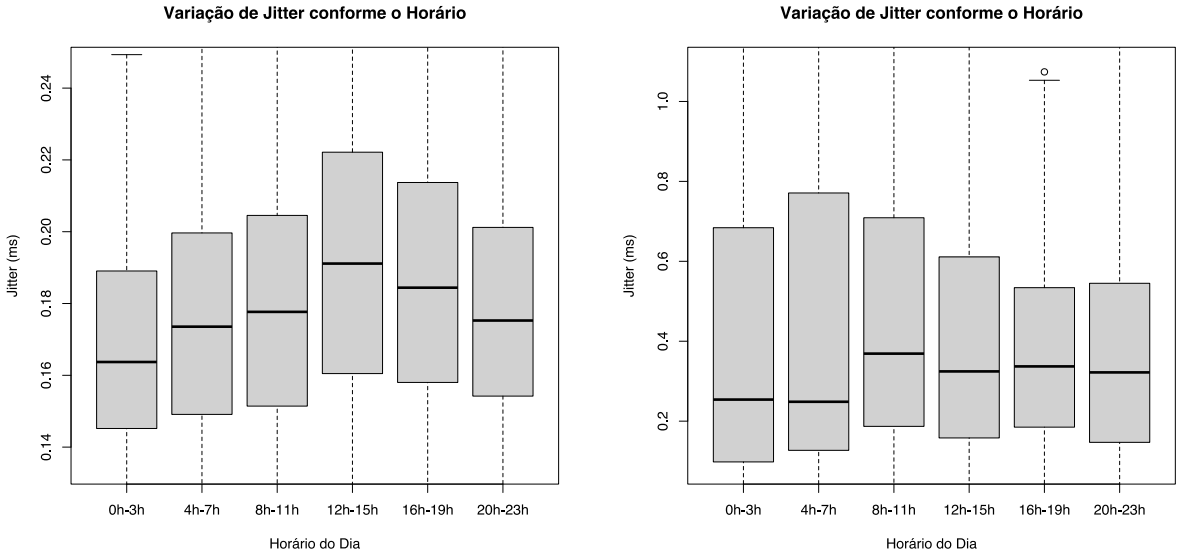
(a) Peertest (b) Speedtest

Figura 18 – Variação semanal no *Jitter*

Considerando o comportamento da métrica *jitter* ao longo das horas do dia, observa-se pela Figura 19a um acréscimo gradual da madrugada até o horário de almoço, com posterior redução ao longo da tarde e noite. No caso dos dados aferidos via Speedtest (ver Figura 19b), não se observa esta mesma tendência, apenas um *jitter* menor de madrugada e maior da manhã, tarde e noite.

5.7 Análise da vazão de *download*

A vazão de *download* é a medida de quanta informação pode ser descarregada ("baixada") em um determinado período, geralmente aferida em megabits por segundo



(a) Peertest (b) Speedtest

Figura 19 – Variação horária no *Jitter*

(Mbit/s). Popularmente, é a velocidade em que os dados são "baixados" da internet para o seu dispositivo: quanto maior a vazão, mais rapidamente os dados serão baixados, de forma mais fluida e com menos interrupções. É importante ressaltar que a velocidade pode ser influenciada por vários fatores, como a capacidade do dispositivo em processar e armazenar os dados transferidos e a quantidade de dispositivos conectados à mesma rede.

Em aferições P2P, a vazão de *upload* de um par espelha a vazão de *download* do outro (considerando que ambos atuam tanto como cliente quanto como servidor). Como exemplo, considere que o par cliente A consiga fazer um *upload* a 200 Mbits/s ao par servidor B. Se B tem uma vazão de *download* de 100 Mbits/s, essa será a maior vazão (velocidade) que ele conseguirá perceber e mensurar vindo de A. De forma análoga, quando os papéis se invertem, se A tem *download* de 200 Mbits/s e B tem *upload* de 50 Mbits/s, o valor máximo que A conseguirá mensurar vindo de B é 50 Mbits/s.

Essa é uma característica de aferições de vazão (velocidade) em arquiteturas par-a-par. Porém, com velocidades maiores cada vez mais acessíveis ao usuário residencial de internet (LARA, 2019), a relevância dos testes de *Download* e *Upload* tende a diminuir em relação aos outros testes. Pois, se dois usuários com conexões de 500 Mbits/s e 1 Gbits/s, respectivamente, fazem uma aferição P2P entre si, um resultado de *Upload* e Download de 500 Mbits/s não teria tanta importância, se tais usuários mal consumirem 100 Mbits/s em seu uso diário. Nesse contexto, as outras métricas afetariam mais significativamente a experiência de acesso à internet desses usuários.

Como mostrado na Seção 4.6, foi necessário implementar a aferição de vazão de maneira distinta, devido ao uso da técnica UDP *Hole Punching* e da inviabilidade de se

usar o Iperf3 (ver Subseção 2.4.6) para esse propósito. Dessa forma, a aferição de vazão foi baseada na técnica de Saturação, que proporciona uma simplicidade na implementação. Além disso, ela é utilizada por ferramentas como o Speedtest e o NDT7 (MACMILLAN et al., 2023).

5.7.1 Peertest vs Speedtest (com servidor dentro do ISP)

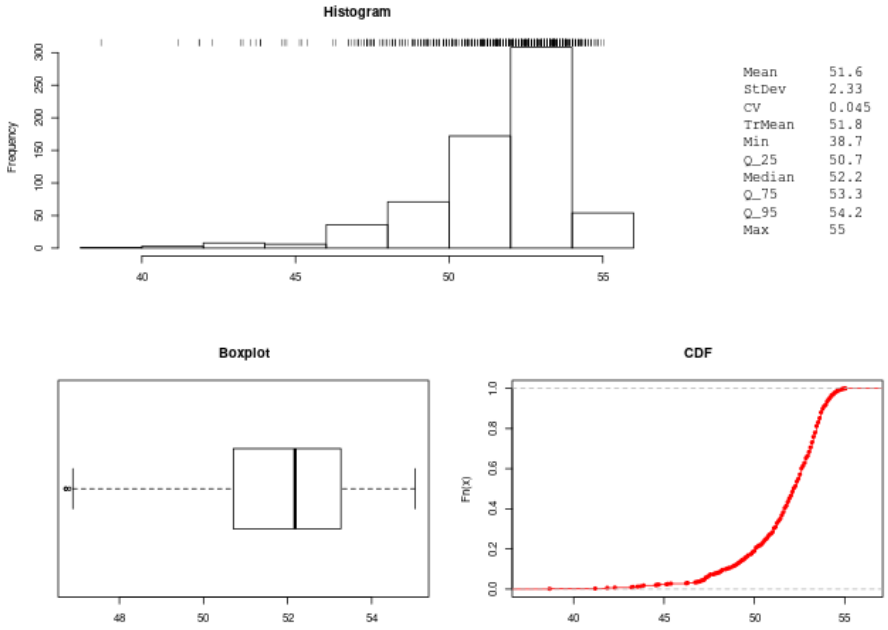


Figura 20 – *Download* aferido via Peertest em Mbits/s

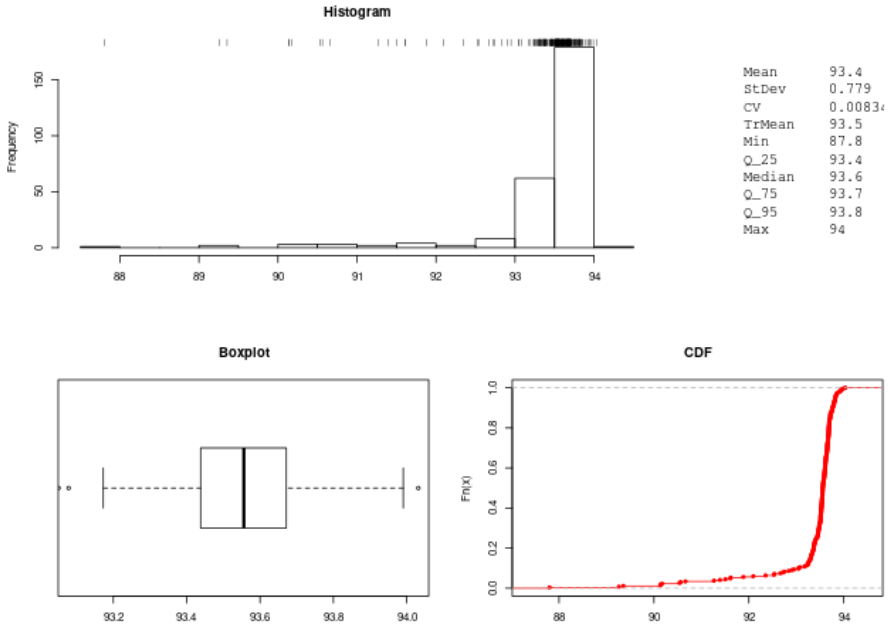


Figura 21 – *Download* aferido via Speedtest em Mbits/s

Comparando-se as Figuras 20 e 21, observa-se que a vazão de *download* no Peertest apresentou uma variabilidade 5,3 vezes maior que no Speedtest (CV=0,045 e CV=0,008, respectivamente). Complementarmente, comparando-se os respectivos *boxplots*, observa-se uma maior heterogeneidade nas vazões de *download* aferidas pelo Peertest do que naquelas aferidas pelo Speedtest.

Comparando-se os histogramas e CDFs das Figuras 20 e 21, mais uma vez percebe-se que os dados do Speedtest apresentam uma "cauda" mais longa e os dados do Peertest uma "cauda" mais pesada. Complementarmente, tal fato também pode ser inferido comparando-se o intervalo no eixo das abscissas em que se encontram ambos os pontos de inflexão da CDF do Peertest e do Speedtest, para a métrica *download*. Observa-se no Peertest (Figura 20) uma maior representatividade de valores abaixo da média (mean=51,6 Mbit/s): a menor vazão de *download* registrada foi de 38,7 Mbit/s e 75% dos dados estão entre 50,7 Mbit/s (P25) e 55 Mbit/s (max). Já no Speedtest (Figura 21) houve uma menor representatividade de valores abaixo da média (mean=93,4 Mbit/s): a menor vazão de *download* registrada foi de 87,8 Mbit/s, porém 75% dos dados estão entre 93,4 Mbit/s (P25) e 94 Mbit/s (max).

Os valores aferidos através da ferramenta Speedtest estão acima do mínimo exigido pela Resolução nº 574 da ANATEL: 95% dos dados devem apresentar vazão de *download* superior a 80% da velocidade contratada. No Speedtest, observa-se um P95 de 93,8 Mbit/s bem acima de 80 Mbit/s que seria o obrigatório (80% da velocidade contratada em 95% das medições). Isso é um ponto positivo, pois a vazão de *download* é importante para aplicações de vídeo sob demanda (ex.: *streamings* de seriados, filmes e demais categorias de vídeo), instalação de softwares (ex.: atualização de aplicativos) e obtenção de grandes arquivos (ex.: descarregamento de *backups*, bases de dados, *datasets*, grandes repositórios, dentre outros).

Já os valores de *download* e averiguados via Peertest ficaram muito abaixo do exigido pela Anatel. Observa-se aqui um P95 de 54,2 Mbit/s muito distante dos 80 Mbit/s obrigatórios. Durante o desenvolvimento da ferramenta, ela não apresentara uma vazão consistentemente tão baixa. Mesmo assim, para verificar se o problema estava no código da Peertest, foram realizadas aferições contra um par hospedado na Amazon EC2, executando o mesmo código utilizado no experimento com ambos os pares em residências. Nessas aferições conseguiu-se alcançar vazões próximas a 100 Mbits/s tanto para *download* quanto para *upload*. Os testes acima foram realizados com um par localizado na rede do ISP TOP37, tendo uma conexão de 100 Mbis/s e o outro par localizado na rede da Amazon tendo uma conexão de 1 Gbit/s.

Sendo assim, parece provável que a limitação da velocidade aferida via Peertest a no máximo 55 Mbit/s seja alguma característica da rede do ISP MAP Fibra. Talvez

estivesse sendo realizado alguma forma de *traffic shaping*[9] que limitou a vazão dos testes da Peertest por categorizar o tráfego das aferições de compartilhamento de arquivos, já que os pares encontram-se através da DHT do BitTorrent para, depois, trocarem dados entre si. Essa técnica pode ser polêmica, uma vez que pode afetar a qualidade de serviço e a neutralidade de rede, sendo importante que as operadoras a utilizem de forma transparente e conforme as normas regulatórias e os contratos firmados com os usuários.

Reforçando esta hipótese, durante os testes preliminares no desenvolvimento do Peertest, foi detectado que o ISP Vivo Fibra, por exemplo, bloqueia completamente o tráfego de rede direcionado aos nós de engate (*bootstrap*) da DHT do BitTorrent, uma ação que aparentemente fere as proteções e garantias do Marco Civil da Internet (Lei n° 12.965/2014), indo contra o princípio de Neutralidade da Rede[10]. Exceto na hipótese do referido ISP estar cumprindo alguma ordem judicial que o obrigou a fazer tal bloqueio da DHT do BitTorrent. Em tempo, no Brasil, a Neutralidade de Rede é exigida para garantir que os provedores de acesso à internet tratem todo o tráfego de dados de forma isonômica, sem discriminação ou preferência por conteúdos, serviços ou aplicações específicas. Ou seja, a Neutralidade de Rede exige que todos os dados sejam tratados igualmente, sem priorização ou bloqueio de determinados conteúdos ou serviços em detrimento de outros. Essa medida é importante para garantir a liberdade de expressão, o acesso à informação e a concorrência no mercado de serviços de internet.

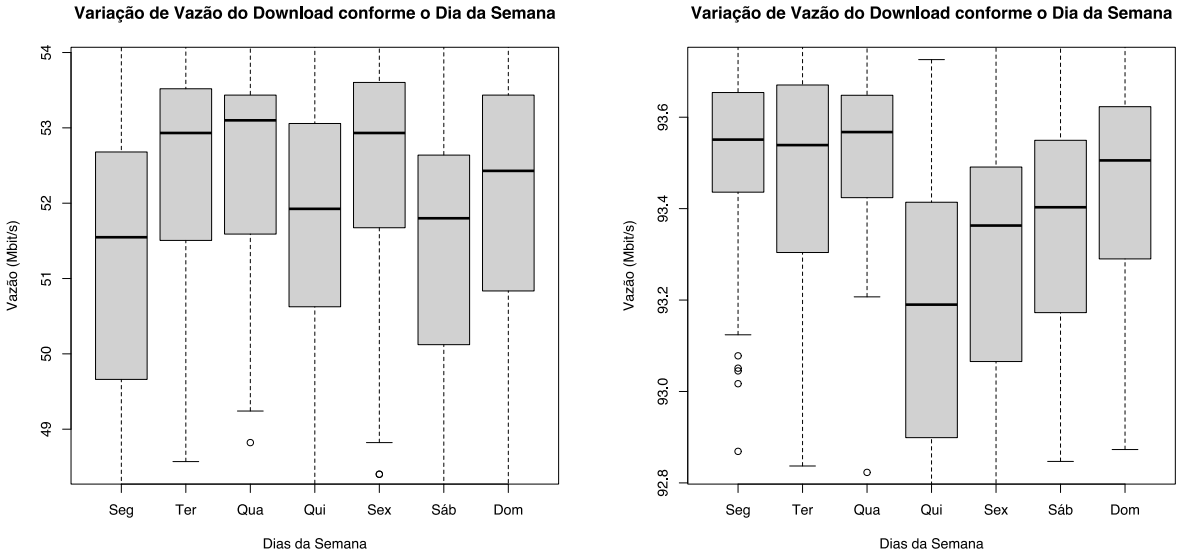
5.7.2 Análise temporal: Peertest vs Speedtest (com todas as aferições)

Via Peertest (ver Figura 22a) observa-se uma melhor disponibilidade da vazão de *download* de terça a sexta-feira, com posterior redução de sábado a segunda-feira. Nos dias de quinta-feira, foi notada uma queda na vazão de *download*, fugindo à tendência anteriormente expressa. Via Speedtest (Figura 22b), notamos que a vazão de *download* apresenta uma ligeira tendência de melhoria de quinta a segunda-feira, piorando às quartas-feiras.

Por outro lado, ao considerarmos a tendência ao longo das horas do dia para a vazão de *download*, nos dados do Peertest (ver Figura 23a) pode-se notar uma piora ao longo da manhã até o horário de almoço, com subsequente melhora na vazão de *download* ao longo da tarde e noite. Neste ponto, os dados do Speedtest (ver Figura 23b) demonstram uma tendência similar à observada no Peertest.

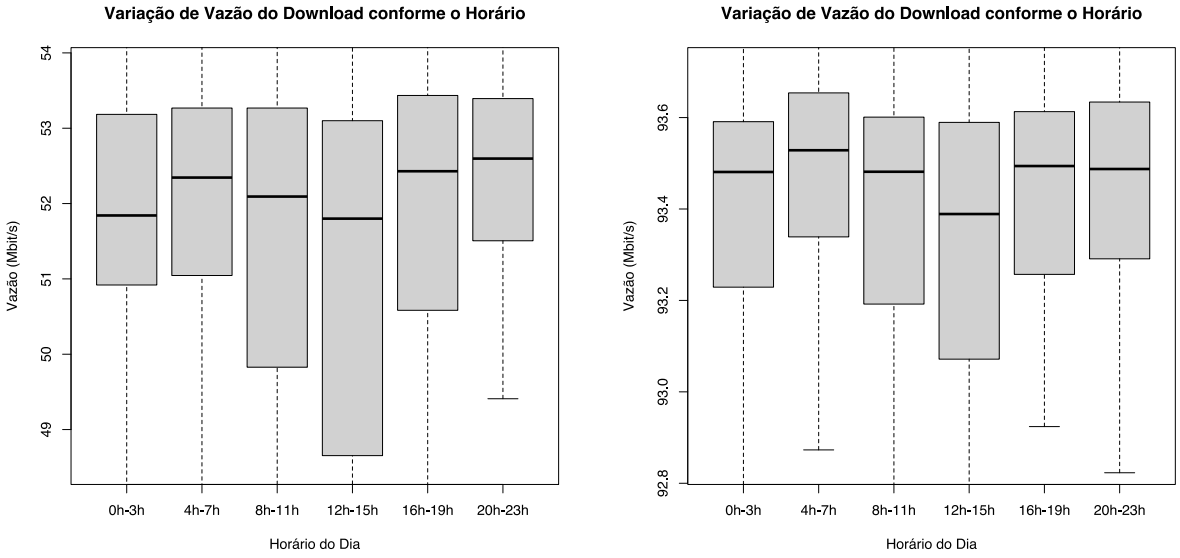
[9] *Traffic Shaping* é uma técnica utilizada pelos provedores de acesso à internet para gerenciar o tráfego de rede e controlar a velocidade de transferência de dados conforme a demanda e prioridades estabelecidas.

[10] Neutralidade de Rede é um princípio que exige que todo o tráfego de dados na internet seja tratado de forma isonômica, sem discriminação ou preferência por conteúdos, serviços ou aplicações específicas, ou seja, sem priorização ou bloqueio de determinados conteúdos ou serviços em detrimento de outros.



(a) Peertest (b) Speedtest

Figura 22 – Variação semanal na vazão de *Download*



(a) Peertest (b) Speedtest

Figura 23 – Variação horária na vazão de *Download*

5.8 Análise da vazão de *upload*

5.8.1 Peertest vs Speedtest (com servidor dentro do ISP)

Considerando as estatísticas descritivas da vazão de *upload*, observa-se para a Peertest (Figura 24) uma mediana de 43,3 Mbit/s, com uma vazão de *upload* mínima de 29,2 Mbit/s e máxima de 47,1 Mbit/s. Já para o Speedtest (Figura 25), a mediana foi de 93,5 Mbit/s, com as vazões mínima e máxima de 92,5 Mbit/s e 93,5 Mbit/s, respectivamente.

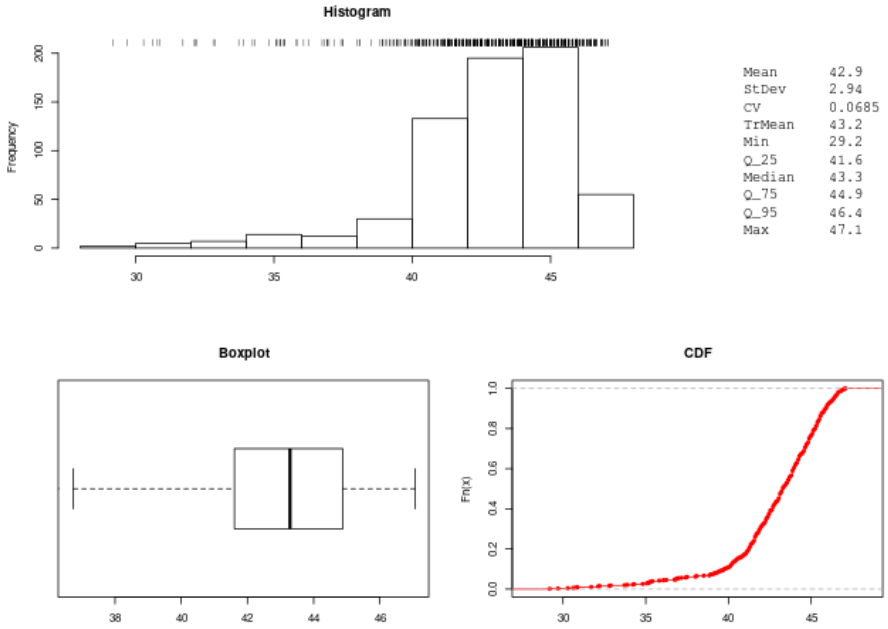


Figura 24 – *Upload* aferido via Peertest em Mbits/s

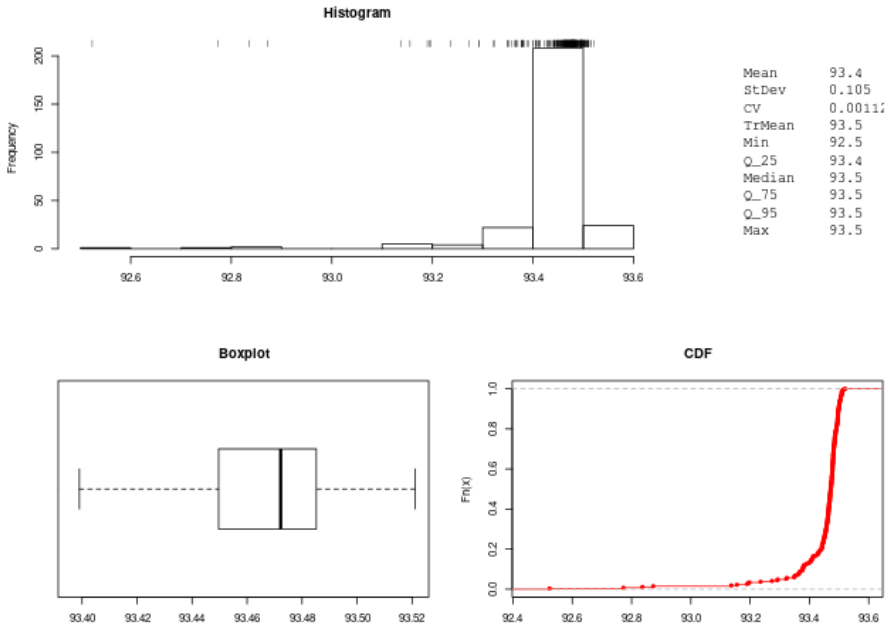


Figura 25 – *Upload* aferido via Speedtest em Mbits/s

Comparando os histogramas da vazão de *upload* do Peertest (Figura 24) e do Speedtest (Figura 25), observa-se que ambos os casos apresentam uma obliquidade à esquerda, de forma que a massa dos dados encontra-se concentrada à direita da média. A Peertest apresentou uma cauda mais pesada enquanto o Speedtest apresentou uma cauda mais longa, ambas à esquerda. Considerando os *boxplots*, a Peertest demonstra menos assimetria do que o Speedtest.

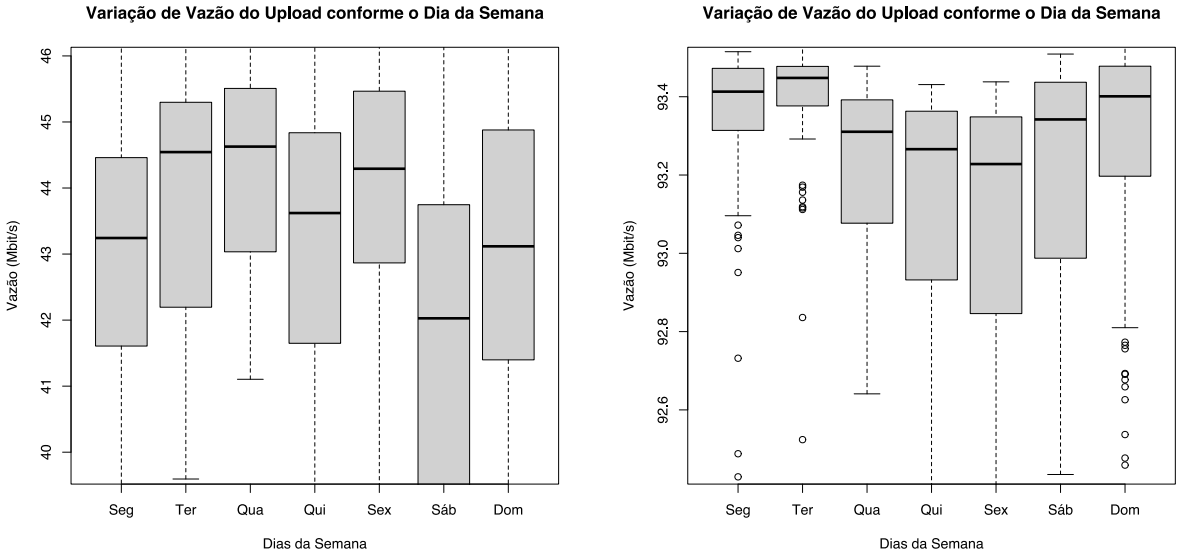
Analisando-se as curvas de suas CDFs, observa-se que a Peertest apresentou uma maior variância (CDF menos íngreme) para a vazão de *upload* do que o Speedtest (CDF mais íngreme). Tal fato se confirma ao analisarmos o coeficiente de variação: a Peertest (CV=0,0685) apresentou 62 vezes mais variabilidade nos dados de *upload* do que o Speedtest (CV=0,0011). Ou seja, as aferições do Speedtest demonstraram-se mais homogêneas e previsíveis, enquanto as medições de *upload* via Peertest apresentaram valores mais heterogêneos e variados. Adicionalmente, compare os *rug plots* de ambos (traços acima das barras do histograma): no Speedtest (Figura 25) observa-se uma alta concentração de valores na proximidade da média e poucos dados bem distanciados à esquerda dela; já no Peertest (Figura 24) observa-se um degradê da direita para a esquerda, com os valores espaçados próximos à média e bem mais espaçados longe dela.

Novamente os valores aferidos pelo Speedtest estão bem acima do mínimo exigido pela Resolução nº 574 da ANATEL: 95% dos dados devem apresentar vazão superior a 80% da velocidade contratada. No Speedtest, observa-se um P95 de 93,5 Mbit/s bem acima de 80 Mbit/s que seria o obrigatório (80% da velocidade contratada em 95% das medições). Isso é um ponto positivo, pois a vazão de *upload* é importante para aplicações como *backup online* de arquivos (ex.: armazenamento em nuvem, com sincronização de fotos, vídeos e documentos) e videoconferências. Entretanto, os valores das aferições com a Peertest se apresentaram bem abaixo do mínimo exigido pela Anatel, com um P95 de 46,4 Mbits/s. As considerações sobre uma possível explicação sobre esta limitação na vazão foram discutidas na Seção 5.7.

5.8.2 Análise temporal: Peertest vs Speedtest (com todas as aferições)

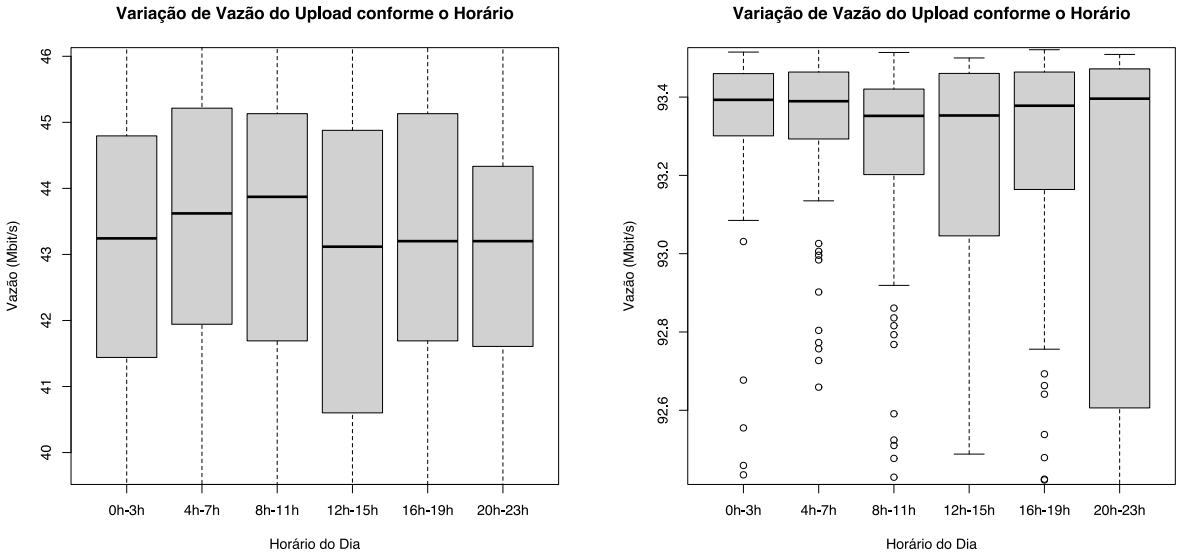
No caso da métrica vazão de *upload*, a tendência observada nos dados do Peertest (ver Figura 26a) é de melhoria de segunda a sexta-feira, com posterior tendência de piora na vazão de *upload* no sábado. Já no Speedtest (ver Figura 26b), nota-se uma tendência inversa, com uma tendência de melhoria de sábado até terça-feira e uma piora gradual na vazão de *upload* de quarta a sexta-feira. Neste caso, os dados aferidos com as duas ferramentas apresentam tendências conflitantes e distintas.

Por fim, considerando-se a tendência horária da vazão de *upload*, via Peertest (ver Figura 27a) observa-se uma melhoria ao longo da madrugada e manhã, com uma queda no horário de almoço, seguida de uma recuperação ao longo da tarde. As medições com o Speedtest (ver Figura 27b) seguiram uma tendência similar, discordando apenas no impacto que o período noturno tem na vazão de *upload*: uma maior variabilidade no Speedtest e menor no Peertest.



(a) Peertest (b) Speedtest

Figura 26 – Variação semanal na vazão de *Upload*



(a) Peertest (b) Speedtest

Figura 27 – Variação horária na vazão de *Upload*

5.9 Considerações

Desta forma, pôde-se perceber pela análise, que nas aferições de perda de pacotes e latência, a Peertest, apresentou resultados com valores maiores e mais heterogêneos, provavelmente devido a um cenário mais realista. E por realista consideramos que a aferição corresponderia melhor à percepção subjetiva do usuário de internet residencial, ao realizar suas tarefas de lazer e/ou trabalho através da internet contratada. Além disso, nessas aferições foram detectadas tendências destoantes entre as ferramentas, na perda de

pacotes, mas consonantes entre elas, na latência. Ainda, em relação à latência, notou-se que as medições com servidores fora do ISP, pelo Speedtest, apresentaram resultados mais realistas em um primeiro momento, mas com a presença de um número expressivo de aferições com valores muito baixos, próximos a 3 ms. Para essas métricas, tanto a Peertest quanto o Speedtest, apresentaram valores muito abaixo (dentro) do limite estabelecido pela Anatel, consistindo em um ponto positivo.

Em relação à métrica de *jitter*, as ferramentas apresentaram resultados similares, com a Peertest apresentando maior estabilidade nos dados. Porém, não foi possível encontrar tendências claras ou consonantes entre as ferramentas. Aqui, as duas ferramentas também apresentaram valores muito abaixo (dentro) do limite estabelecido pela Anatel.

No quesito vazão (velocidade) de *download* e *upload* o Speedtest apresentou resultados dentro do especificado pela Anatel, porém, mais estáveis, homogêneos e previsíveis. Já a Peertest apresentou um comportamento peculiar: as aferições realizadas através dela ficaram muito abaixo do exigido pela Anatel, limitadas por um platô virtual abaixo da vazão contratada. Foi discursado que uma suposta utilização da técnica de *traffic shaping* pelo ISP como provável responsável por esta limitação nos resultados do Peertest. Nessas duas métricas, foram encontradas, em sua maioria, tendências similares para ambas as ferramentas.

5.10 Particularidades em ISPs

Embora uma solução par-a-par teoricamente deva ser mais precisa para aferir a qualidade da internet de forma mais próxima da experiência real do consumidor, infelizmente, devido à possibilidade da prática[11] de *traffic shaping* pelo ISP, pelas tecnologias subjacentes a solução par-a-par apresentada pode indiretamente sofrer com limitações e bloqueios associados ao compartilhamento de arquivos via internet (ex.: ISPs cumprirem decisões judiciais, mas que impacte em algum subsistema do BitTorrent como sua DHT). Durante o desenvolvimento da Peertest, foram encontradas várias peculiaridades em relação às políticas implementadas por cada ISP no tratamento dispensado a aplicações P2P de forma diferente àquelas cliente-servidor. Tais questões são sumarizadas abaixo para poderem servir de alerta quando se for construir alguma outra aplicação P2P (ou aplicação cliente-servidor) que necessite transpor NATs impostos pelos ISPs.

Foi detectado que o ISP Vivo Fibra bloqueia o acesso à DHT do BitTorrent, dentre outras medidas voltadas a serviços de compartilhamento de arquivos[12]. Após experimentos de depuração, foi observado que o nó de engate (*bootstrap*) da DHT do BitTorrent também era bloqueado pelo seu endereço de IP. Infelizmente, como tal DHT é um componente

[11] apesar disso provavelmente ferir o Marco Civil da Internet

[12] "VIVO e outras operadoras bloqueiam por DNS acesso a ..." 11 jul.. 2021, <https://www.hardmob.com.br/threads/773572>. Acessado em 3 abr.. 2023.

essencial no funcionamento da ferramenta Peertest, clientes da referida operadora não conseguiriam utilizar a ferramenta desenvolvida neste trabalho. Vale destacar que o BitTorrent, sua DHT e tecnologias relacionadas não são responsáveis diretos por supostas infrações de direitos autorais, de forma que os bloqueios promovidos por ISPs deveriam ser direcionados aos servidores que hospedam ou anunciam arquivos Torrent contendo conteúdo protegido. Um ISP bloquear o protocolo BitTorrent e sua DHT seria o equivalente a bloquear todo tráfego HTTP e DNS como forma de evitar o acesso a alguns poucos servidores contendo conteúdo protegido, porém tendo como efeito colateral bloquear o acesso dos clientes daquele ISP a todos os milhões de demais *websites* não relacionados a conteúdo ilegal.

Foi detectada uma aparente limitação no tamanho dos datagramas UDP que o ISP TOP 37 permitia que trafegassem dentro de sua "intranet", apesar que a própria fragmentação IP poderia cuidar desses grandes datagramas UDP de forma transparente. Dessa forma, para executar as aferições de *jitter* e latência, foi necessário manualmente calibrar o tamanho máximo de cada datagrama para 1492 bytes (MSS geralmente associado à MTU de enlaces metálicos Ethernet). Até onde pudemos verificar, o ISP limitar implicitamente o tamanho máximo de datagramas UDP que ele "aceita" trafegar em sua intranet não é uma prática que deveria ser comum e nem aceita, por ferir a neutralidade de rede determinada pelo Marco Civil da Internet. Ainda assim, tal prática deveria no mínimo ser devidamente documentada pelo ISP, dando a devida publicidade a seus clientes, e não percebida por inferência pelos desenvolvedores quando algum software misteriosamente não funcionar como deveria segundo os padrões da pilha de protocolos da internet e as normas vigentes.

Já o ISP MAP Fibra aparentemente bloqueia (ou descarta) os protocolos e pacotes necessários para o funcionamento dos softwares Traceroute e Nmap impossibilitando, por exemplo, a descoberta de sua topologia interna. Além disso, há a suspeita de que, pela utilização da técnica de *traffic shaping* em datagramas UDP, os resultados de vazão (velocidade) da Peertest tenham ficados muito abaixo da vazão realmente contratada.

Observamos que os provedores de acesso à internet (ISPs) podem implementar um período arbitrário para a duração do mapeamento feito por seus respectivos NATs. Por exemplo, o ISP Signet (que atua na cidade de Caratinga - MG) utilizava uma duração de 10 minutos na persistência do mapeamento realizado pelo seu NAT, já o ISP TOP 37 utilizava uma duração de apenas 10 segundos na persistência do mapeamento.

Provedores poderiam utilizar *firewalls* ao nível de aplicação, que podem categorizar e preemptivamente bloquear tráfego associado a compartilhamento de arquivos (ex.: IP de *bootstrap* de uma DHT), a domínios específicos ou a protocolos "indesejados" pelo ISP. Por exemplo, em nossos experimentos observamos que o ISP Conecta Minas bloqueia via *firewall* protocolos tradicionais necessários para aferição de latência e verificação de disponibilidade de hospedeiros na internet (ex.: ICMP Echo Request / ICMP Echo Reply).

Em redes móveis 4G de diferentes operadoras, não foi possível ao par do Peertest se anunciar na DHT do BitTorrent, em comportamento similar ao observado no ISP Vivo Fibra. Também, de forma mais agressiva, alguns ISPs poderiam utilizar NAT tipo 3, o que impediria qualquer comunicação P2P e, em especial, a utilização da ferramenta Peertest desenvolvida neste TCC.

Por todos esses motivos, não é possível garantir que a técnica utilizada de *Hole Punching* do NAT funcionará como o esperado para todos os usuários que quiserem utilizar o software Peertest, desenvolvido neste TCC, pois cada provedor pode fazer a implementação/configuração de seu(s) NAT(s) de maneira distinta. Considerando isto, trabalhamos para o caso típico, mas exceções existem e podem não ser raras[13]. Nossa opinião é que a solução para este problema seria agilizar a ampla adoção do protocolo IPv6 pelos ISPs, protocolo cuja implantação global permanente foi promovida em 2012 e já é utilizado por cerca de 35-40%[14] dos internautas.

Nos próximos capítulos serão apresentados os principais resultados, bem como as sugestões de trabalhos futuros.

[13] "UDP hole punching not going through ..." 10 set.. 2012, <https://stackoverflow.com/a/12392916/17552592>. Acessado em 3 abr.. 2023.

[14] "IPv6 Statistics" <https://www.internetsociety.org/deploy360/ipv6/statistics/>. Acessado em 20 mai. 2023

6 Conclusão

O presente trabalho teve como objetivo o desenvolvimento de uma ferramenta chamada Peertest, para aferição periódica e automatizada da qualidade do serviço de internet provido pelo ISP ao usuário residencial, utilizando-se de comunicação direta (P2P) entre pares de computadores de redes privadas distintas. Os objetivos propostos no projeto foram alcançados e este capítulo tem como finalidade apresentar considerações a respeito das principais contribuições, bem como as possíveis implicações do estudo para a área de pesquisa em questão. O capítulo foi dividido em seções, começando pelos principais resultados, seguido pelas considerações finais e, por fim, sugestões de trabalhos futuros que possam ser realizados a partir das contribuições e limitações do presente estudo.

6.1 Principais Resultados

A ferramenta desenvolvida nesse trabalho (Peertest) tem utilidade, pois, através dos resultados do experimento, pode-se perceber que as aferições de latência e de perda de pacotes feitas com a Peertest apresentaram resultados mais realistas (heterogêneos) em comparação às aferições (mais homogêneas) realizadas com ferramentas cliente-servidor populares como a Speedtest.net. Por ser descentralizada, a solução Peertest tem o potencial de ser mais robusta e escalável em comparação às ferramentas governamentais oficiais como brasilbandalarga.com.br e beta.simet.nic.br, desde que a Peertest seja instalada e esteja em execução em uma quantidade suficiente de pares. Especificamente, como não há um servidor centralizado, é necessário a presença de pelo menos dois pares Peertest anunciados na DHT para que a ferramenta desenvolvida possa aferir a qualidade de internet de ambos os usuários residenciais.

Um ponto positivo para a qualidade da internet mensurada é que pelos resultados dos experimentos, tanto com Peertest quanto com Speedtest, as aferições se encontram em sua maioria bem acima dos limites mínimos estabelecidos pela Resolução nº 574 da Anatel, para a qualidade do serviço de internet fixa. Os contrapontos encontrados foram nas aferições de vazão de *download* e *upload* via Peertest, que ficaram limitadas a um platô por um provável *traffic shaping* aplicado pelo ISP, pois se constatou que a referida limitação não é inerente da ferramenta, como discutido no final da Seção 5.7. Todavia, com vazões (velocidades) mais altas cada vez mais acessíveis ao usuário residencial, a aparente limitação dos ISPs a tráfegos do modelo par-a-par tende se tornar cada vez menos comum.

A política de seleção de pares atualmente implementada garante que o par seja escolhido de forma aleatória, dentre aqueles pares Peertest anunciados na DHT. Dessa forma, visamos capturar a qualidade da internet do usuário de forma mais sistêmica,

"holística" e abrangente. Ademais, mitiga-se o risco de um par sempre fazer aferições contra pares Peertest possivelmente hospedados pelo próprio ISP e que se anunciem na DHT. Por exemplo, caso a política de seleção de pares priorizasse aqueles de menor latência, haveria uma maior probabilidade de que pares hospedados dentro da infraestrutura do próprio ISP fossem selecionados e, assim, produzissem um resultado artificialmente melhor (como já ocorre nas ferramentas cliente-servidor populares) do que a realidade percebida pelo usuário doméstico em seu acesso à internet.

A ferramenta Peertest descobre novos pares através do serviço da rede DHT do BitTorrent (uma DHT robusta, com milhões de usuários diariamente); então coordena os testes periódicos de vazão, *jitter*, perda de pacotes e latência entre pares Peertest. Entretanto, vale destacar que o bom funcionamento da ferramenta está sujeito às políticas implementadas pelos provedores de acesso à internet (ISPs), que podem interferir nos resultados ao, por exemplo, limitar o tamanho máximo dos datagramas UDP em sua rede interna, aplicar alguma forma de *traffic shaping*, utilizar um NAT tipo 3 ou, até mesmo, bloquear por completo pacotes destinados à DHT do BitTorrent, como relatado no final da Subseção 5.4.1.

Neste trabalho, além do desenvolvimento da ferramenta em si, podem ser identificadas outras contribuições, como documentação de algumas particularidades encontradas nos ISPs e nos diferentes tipos de NATs utilizados. Foram documentadas também a utilização das técnicas de UDP Hole Punch e de Tradução de Protocolos de Transporte (utilizando a ferramenta SOCAT), técnicas com detalhes de implementação pouco documentados até onde pudemos verificar. Também, foi demonstrado neste trabalho como essas técnicas podem ser utilizadas em conjunto para viabilizar a comunicação de dois computadores hospedeiros atrás de NATs tipo 1 e 2 (ou seja, ocultos da internet pública), mesmo que a aplicação nesses hospedeiros necessite de conexões TCP. Vale destacar que nesse último caso (TCP via tradução para UDP) existem algumas ressalvas, discutidas na Seção 4.5.

Também, foi apresentado o diagrama e a implementação de um algoritmo de seleção de pares, que pode ser utilizado e/ou adaptado dependendo das necessidades de aplicações futuras que se utilizem da arquitetura proposta e implementada neste trabalho. Em tempo, alertamos que caso se adapte a solução par-a-par desenvolvida para selecionar especificamente pares P2P dentro do mesmo ISP (clientes de um mesmo provedor de acesso à internet) para testar a qualidade de sua internet, a princípio tal abordagem poderia ter desvantagens: a seleção mútua de pares dentro do mesmo ISP pode não necessariamente fornecer uma representação precisa da velocidade de acesso à internet do cliente residencial, uma vez que os pacotes de ambos os pares trafegarão apenas dentro da infraestrutura do ISP. Portanto, comunicar-se-iam somente dentro da rede daquele sistema autônomo (que poderia estar superdimensionada ou ociosa) e não através da internet em si, onde os gargalos tipicamente se manifestam nas trocas de pacotes entre diferentes Sistemas

Autônomos (AS - *Autonomous System*).

Ainda assim, testes de qualidade de serviço (QoS) par-a-par podem fornecer uma representação mais precisa da qualidade da internet para o usuário do que a típica solução cliente-servidor, pois no P2P afere-se o desempenho da rede do ponto de vista de ambos usuários daquele provedor, podendo indicar sobrecargas internas na própria rede daquele ISP.

Por fim, outra contribuição são os dados dos testes realizados, disponibilizados em um repositório no Github <<https://github.com/Konomaster/TCC>>, que podem ser utilizados em análises complementares da qualidade de acesso residencial à internet, como um trace em simulações de comunicação via WAN e afins.

6.2 Trabalhos Futuros

É sugerido para trabalhos futuros o desenvolvimento de uma interface gráfica (*front-end*) para exibir os resultados dos testes de uma forma mais amigável e intuitiva para o usuário leigo. Por exemplo, a interface poderia ser um *website* hospedado localmente no próprio computador e exibido ao se iniciar a ferramenta (ou quando desejado, dada uma URL padrão ex.: http://localhost/qualidade-internet/). Poderia ser utilizada a aplicação de código aberto Grafana[1], como feito pelo trabalho relacionado CheesePI (vide Subseção 2.4.4), para exibição dos resultados das aferições.

Outra sugestão é a utilização de uma ferramenta (ex.: SG TCP/IP Analyzer[2]) para descobrir dinamicamente o tamanho máximo do segmento (MSS) antes de realizar os testes de *jitter* e taxa de perda de pacotes. O benefício seria uma aferição mais fiel ao evitar as perdas de pacote oriundas da fragmentação de pacotes IP maiores que a MTU (tamanho do quadro) do enlace mais restritivo (o de menor MTU) ao longo da rota entre os pares.

Outra possibilidade de trabalho sugerido é a realização de experimentos em mais cenários para verificar a exequibilidade da ferramenta em ambientes com a utilização do NAT tipo 2. É interessante também que os experimentos utilizem diversos pares posicionados em diferentes ISPs, o que demandaria a implantação da solução em dezenas de residências em bairros e cidades diferentes.

Sugere-se também uma rodada de experimentos para comparar os resultados da Peertest com aqueles obtidos pelas ferramentas governamentais como Brasil Banda Larga[3] (da ANATEL) ou SIMET[4]. Essas últimas utilizam servidores em pontos de troca de tráfego

[1] "Grafana Dashboards" <https://grafana.com/grafana/dashboards/> Acessado em 20 mai. 2023
[2] "SG TCP/IP Analyzer" <https://www.speedguide.net/analyzer.php> Acessado em 20 mai. 2023
[3] <https://www.brasilbandalarga.com.br/> Acessado em 20 mai. 2023
[4] <https://beta.simet.nic.br/> Acessado em 20 mai. 2023

do Núcleo de Informação e Coordenação do Ponto BR (NIC.br[5]). Então, teoricamente, são ferramentas que poderiam representar melhor a experiência subjetiva do usuário de acesso residencial à internet, desde que seu ISP não tenha configurado alguma priorização de tráfego com destino a tais servidores governamentais.

Por fim, outro trabalho sugerido é a modificação do algoritmo de seleção de par para permitir que os pares com largura de banda similares tenham preferência de escolha entre si para realizar as aferições. Considere que na comunicação entre dois pares hospedados por clientes de internet residencial, a vazão de *download* de um par pode ser superior à vazão de *upload* do outro par, e vice-versa, pelas velocidades de internet contratadas serem geralmente assimétricas, bem como ter magnitudes diferentes para clientes distintos. Para isso, os pares devem descobrir gradativamente sua real vazão máxima enquanto realizam os testes preliminares com outros pares. Após, passariam a priorizar pares com velocidades compatíveis. Dessa forma, seria possível uma melhor avaliação das métricas vazão de *download* e *upload* para cada cliente de internet residencial.

6.3 Agradecimentos

O autor deste TCC agradece ao Polo de Inovação do IFMG Campus Formiga[6] por ter gentilmente emprestado o Raspberry Pi, que viabilizou a condução do experimento realizado.

[5] "Sobre o NIC.br" <https://www.nic.br/quem-somos/> Acessado em 20 mai. 2023
[6] <https://www.polodeinovacao.ifmg.edu.br/> Acessado em 04 jun. 2023

Referências

BOULANGER, R.; LAZZARINI, V.; MATHEWS, M. *The Audio Programming Book*. MIT Press, 2010. ISBN 9780262014465. Disponível em: <https://www.google.com.br/books/edition/_/IL34DwAAQBAJ?hl=pt-BR&gbpv=1&pg=PA853&dq=wrapper+program+in+another+language>. Citado na página 26.

BRADNER, P.; MCQUAID, J. *Benchmarking Methodology for Network Interconnect Devices*. **RFC 2544**. 1999. Citado na página 44.

BRASIL. Lei n° 12.965, de 23 de abril de 2014. estabelece princípios, garantias, direitos e deveres para o uso da internet no brasil. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Citado 2 vezes nas páginas 15 e 22.

COHEN, B. *The BitTorrent Protocol Specification*. 2008. <http://www.bittorrent.org/beps/bep_0003.html>. Acesso em: 20 de novembro de 2021. Citado na página 25.

FORD, B.; SRISURESH, P.; KEGEL, D. Peer-to-peer communication across network address translators. In: *USENIX Annual Technical Conference, General Track*. [S.l.: s.n.], 2005. p. 179–192. Citado na página 33.

GUULAY B, G. *CheesePi: Measuring Home Network Performance Using Dedicated Hardware Devices*. 78 p. Dissertação (Mestrado) — KTH Royal Institute of Technology, Stockholm, 2015. Citado na página 27.

KUROSE, J.; ROSS, K. *REDES DE COMPUTADORES E A INTERNET Uma aboordagem top-down*. São Paulo - SP: Pearson Education, 2013. Citado 2 vezes nas páginas 23 e 24.

LARA, R. *Baixou 83% em 8 anos: por que a banda larga ficou mais barata no Brasil?* 2019. <https://www.uol.com.br/tilt/noticias/redacao/2019/04/12/baixou-83-em-8-anos-por-que-a-banda-larga-ficou-mais-barata-no-brasil.htm>. Acesso em: 30 de abil de 2023. Citado na página 59.

LOEWENSTERN, A.; NORBERG, A. *DHT Protocol*. 2008. <http://www.bittorrent.org/beps/bep_0005.html>. Acesso em: 20 de novembro de 2021. Citado na página 25.

MACMILLAN, K. et al. A comparative analysis of ookla speedtest and measurement labs network diagnostic test (ndt7). *Proc. ACM Meas. Anal. Comput. Syst. 7, 1, Article 19*, 2023. Disponível em: <https://doi.org/10.1145/3579448>. Citado 2 vezes nas páginas 26 e 60.

MATTHEWS, P. et al. *Session traversal utilities for nat (stun)*. **RFC 5389**. 2008. Citado 2 vezes nas páginas 17 e 25.

MCLACHLAN, D.; BRIND-ARMOUR, A. *Jitlat: A Jitter and Latency Measurement Tool*. 2011. 46 p. DRDC Ottawa TM 2011-047. Citado na página 28.

MENASCE D., A. Qos issues in web services. In: *IEEE Internet Computing, v. 6, n. 6, p. 72-75, nov.* [S.l.: s.n.], 2002. Citado na página 15.

REKHTER, Y. et al. *Address Allocation for Private Internets*. **RFC 1918**. 1996. Citado 2 vezes nas páginas 16 e 44.

ROBERTS J., W. Internet traffic, qos, and pricing. In: *Proceedings of the IEEE, v. 92, n. 9, p. 1389–1399, ago.* [S.l.: s.n.], 2004. Citado na página 15.

SILVA, J. M. *UTILIZANDO O PROTOCOLO BITTORRENT DHT PARA VIABILIZAR CONECTIVIDADE FIM-A-FIM DE PROPÓSITO GERAL EM REDES COM SERVIDORES NAT*. 54 p. Monografia (TCC (Graduação)) — Universidade Federal Rural do Semi Árido - Campus Pau dos Ferros, Pau dos Ferros, 2018. Citado 4 vezes nas páginas 16, 25, 28 e 29.

SRISURESH, P.; FORD, B.; KEGEL, D. *RFC 5128–State of PeertoPeer (P2P) Communica- tion across Network Address Translators (NATs)*. **RFC 5128**. 2008. Citado 4 vezes nas páginas 16, 17, 24 e 25.

TANEMBAUM A., S.; WHETHERALL, D. Redes de computadores. In: _____. [S.l.]: Pearson Education, 2013. cap. A camada de transporte, p. 310–380. Citado na página 23.

VALADãO, E.; GUEDES, D.; DUARTE, R. Caracterização de tempos de ida-e-volta na internet. In: . Porto Alegre, RS, Brasil: SBC, 2017. ISSN 1983-4217. Disponível em: <https://sol.sbc.org.br/index.php/rb-resd/article/view/72>. Citado na página 23.