TRABALHO DE CONCLUSÃO DE CURSO (TCC)

Sistemas de Informação / **2020**

BLOQUEIO DE ANÚNCIOS UTILIZANDO FILTRO DE DNS COM RASPBERRY PI

SILVA, Gustavo Henrique[1]
FRANCISCO, Renato Crepisky[2]
TODESCO, Antero Sewaybricker[3]
MASSARO JÚNIOR, Flávio Rubens[4]

Centro Universitário Hermínio Ometto – UNIARARAS, Araras – SP, Brasil

Resumo

Devido à evolução do Marketing e com a saturação de anúncios digitais atualmente, o presente trabalho propõe controlar o aproveitamento da banda de internet bloqueando anúncios, com uma aplicação Raspberry que filtra dados, tendo em vista a extensa quantidade de dados que anúncios consomem da banda de internet. O dispositivo foi construído com um Raspberry Pi 3 B+, onde foram instalados o Raspberry Pi OS como sistema operacional e Pi-Hole como um filtro de DNS incluindo uma lista negra de URLs de anúncios. O aparelho é capaz de bloqueá-los em todos os dispositivos conectados na rede. Após realizar múltiplos testes de monitoramento, a comparação dos resultados obtidos mostrou que com a utilização do bloqueador o consumo de banda foi consideravelmente menor quando comparado ao consumo de banda sem o bloqueador de anúncios, assim concluindo com êxito o objetivo desse trabalho.

Palavras chave: Pi-Hole, Controle de Banda, Tráfego de Rede, Custo de Largura de Banda.

1 Introdução

1.1 Contextualização

Com o decorrer dos anos e o aumento exponencial de pessoas online simultaneamente, o marketing evoluiu com a tecnologia da informação e anunciantes usam a internet como base para distribuir anúncios e atingir o máximo de possíveis clientes.
Aproveitando o instantâneo e, na maioria das vezes, gratuito acesso à informação, empresas multinacionais geram seus lucros disponibilizando espaços digitais para anúncios publicitários de outras empresas através de serviços de publicidade como Google AdSense, criando um ciclo que incentiva usuários comuns a consumirem esse conteúdo de forma gratuita e empresas pagarem para serem vistas por essa ampla audiência.

[1] FHO|UNIARARAS. Gustavo Henrique Silva, gustavo_henrique_silva@alunos.fho.edu.br
[2] FHO|UNIARARAS. Renato Crepisky Francisco, renatocfrancisco@alunos.fho.edu.br
[3] FHO|UNIARARAS. Antero Sewaybricker Todesco, antero@fho.edu.br
[4] FHO|UNIARARAS. Flávio Rubens Massaro Junior, frmassaro@fho.edu.br

Segunda a Anatel (2018) em seu relatório de acompanhamento do setor de telecomunicações que contempla o último trimestre de 2018, o cidadão brasileiro paga R$3,50 por 1 Mbps (Mega bytes por segundo), sendo que a média de velocidade contratada é de 24,62 Mbps por mês, o que resultaria em um custo mensal de R$86,17, sendo que grande parte desse valor pode estar sendo gasto com o *download* dos anúncios e não apenas com o conteúdo em que usuário pretende consumir.
A quantidade/velocidade da banda de internet que essas propagandas consomem do usuário comum é um fator que interfere no desempenho e no carregamento de páginas *web* durante a navegação, já que os anúncios são obrigatórios e considerando que existem vários tipos de anúncios: *banners, links, "pop-ups"* e vídeos, cada um desses consome uma fração diferente da sua banda de internet.

1.2 Motivações e Justificativas

Atualmente, anúncios digitais são mais complexos, com mais qualidade de imagem e consequentemente precisando de mais tempo de *download*. Para conexões mais lentas, a situação piora (SINGH, 2009).
O relatório da PageFair (2017) expõe os motivos dos usuários para bloquear anúncios na internet, sendo a privacidade dos dados e a confidencialidade de atividades *online* o fator mais importante, além da demora do carregamento de sites e a sobrecarga de anúncios em páginas *web*.

1.3 Objetivos

Montar um dispositivo utilizando um *Raspberry* junto com o *software Pi-hole* com o fim de bloquear anúncios para justificar em uma comparação de dados, o seu desempenho e o aproveitamento da banda de internet.

2 Revisão Bibliográfica

2.1 Conceitos Relacionados

Para o entendimento do projeto como um todo, foi preciso um aprofundamento em conceitos específicos e variados tanto sobre o microcontrolador quanto a infraestrutura que o dispositivo possui quando configurado e instalado em uma rede.

2.1.1 Raspberry PI

Segundo o manual de usuário do *Raspberry* escrito por UPTON (2017), é um dispositivo de placa única, criado em 2012 pela *Raspberry Pi Foundation* (Fundação Raspberry Pi), com o objetivo de ser um computador extremamente pequeno, barato e que estimulasse o interesse dos estudantes pela programação já que estava sendo uma área de baixo interesse; o nome do projeto vem de uma brincadeira com a fruta *Raspberry* que em português é chamado de framboesa, e PI vem da linguagem de programação *Python* que foi escolhida por ser a ideal para rodar em dispositivo menos potente.

2.1.1.2 Funções

Como descrito por Upton (2017) no manual do usuário “A beleza do Raspberry Pi é que ele é apenas um computador de propósito geral muito pequeno”. Por ser um computador do tamanho de um cartão de crédito ele pode ser ideal para diversos tipos de projetos, por ter uma versão do S.O. (sistema operacional) baseado em Linux chamado *Raspberry PI OS*, pode-se construir um computador portátil ou até mesmo montar uma máquina fliperama com o uso de programas que emulam o sistema dos jogos antigos.

2.1.1.3 Aplicação

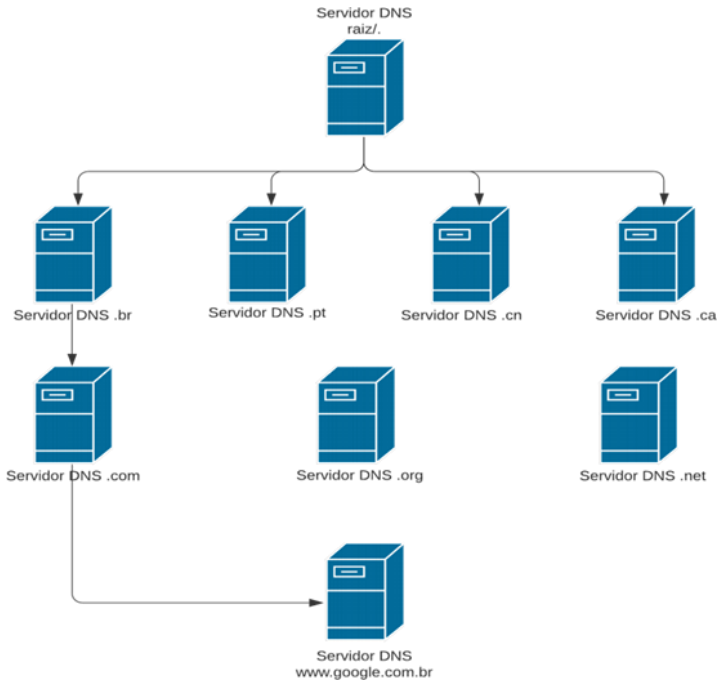
Devido a sua funcionalidade, o dispositivo permite a criação de várias aplicações em diversas áreas de estudo.
Upton (2017, p.9) se impressiona com os vários projetos envolvendo *Raspberry* Pi: um robô aspirador de pó, um robô controlado por ondas cerebrais e também lançamentos de *Raspberry* Pi em foguetes e balões para projetos em órbita terrestre. Visto essa diversificação, o dispositivo se faz perfeito para o propósito do trabalho, pois, é pequeno e pode ser conectado ao roteador não interferindo no espaço residencial, além de ter também um preço acessível.

2.1.2 DNS

O *DNS* é responsável por interpretar o nome do hospedeiro (*hostname*) e levar o IP que em o site solicitado pelo usuário se encontra. Uma comparação feita por Kurose (2013) torna esse entendimento mais simples, em que, a maneira mais fácil de se memorizar em sociedade é através do nome de batismo ou apelidos e não pelo número do seu documento (RG, CPF etc.), do mesmo jeito seria extremamente complicado navegar pela internet utilizando apenas os endereços IP, então por isso criou-se o *DNS*.
Para entender o funcionamento do *DNS*, deve-se entender como o protocolo é estruturado.

- É um sistema hierárquico, como demonstrado na Figura 1.
- É um banco de dados distribuído com os domínios e IP de máquinas, servidores e outros servidores *DNS*.
- Existem 13 *clusters* de servidores-raiz (*root server* ou “.”).
- São espalhados pelo mundo, e o principal motivo é a segurança para evitar que a internet mundial seja interrompida por quais quer motivos.
- Existem centenas de domínios *top-level* genéricos (gTLDs), como por exemplo: .com, .net, .org, etc.
- Há também domínios de nível superior, que são os códigos de cada país (ccTLDs), como por exemplo .br, .pt, .cn, .caetc.

Figura 1 – Hierarquia de Servidores *DNS*

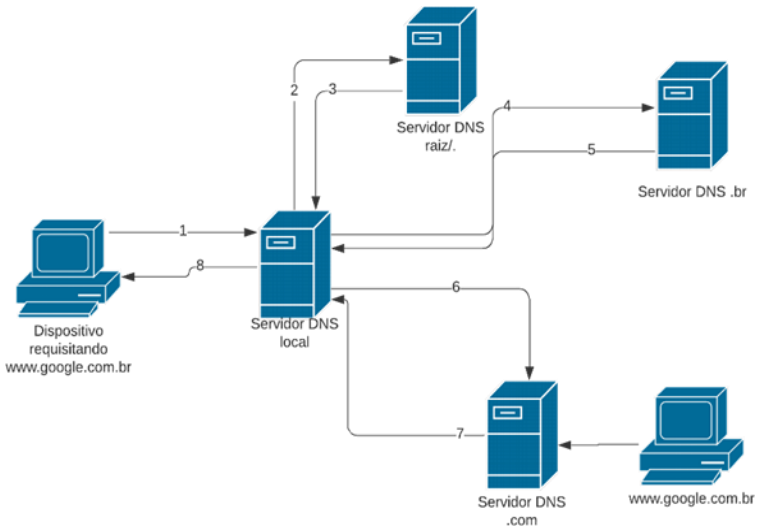


Fonte: Os autores.

2.1.2.1 *DNS Resolver*

O mecanismo de *DNS resolver* é responsável por iniciar as consultas em um servidor *DNS*, interpretar e seguir as instruções, e finalmente chegar ao resultado que é o endereço desejado. Existem dois tipos de consultas: recursivas e iterativas, e por muitas vezes pode haver uma combinação entre elas.

Figura 2 – Consulta Iterativa



Fonte: Os autores.

Consulta Iterativa: O servidor DNS local segue solicitando o endereço para outros servidores DNS e eles vão encaminhando até o endereço solicitado. Como na Figura 2 exemplifica, o passo 1 se refere a solicitação do usuário sendo enviada ao servidor DNS local, que por não saber o endereço começa a solicitar para o servidor raiz (passo 2) que por sua vez envia o endereço do servidor DNS ".br" para que a busca continue e assim segue até encontrar o endereço "www.google.com.br".

2.1.3 Anúncios Digitais

Há vários modelos para anúncios digitais, como por exemplo: *banner*, *pop-up*, *advertorial*, *marketing* de mensagens, e-mail *marketing*, anúncios em mecanismos de busca etc. "No início eram os *spams* e os *banners*. Hoje, a Internet tem dezenas de formatos para serem explorados na promoção de marcas e venda de produtos e serviços" (CANESSO; 2004, p.1).
Dentre os modelos, o mecanismo de busca é um modelo de publicidade não intrusiva para com o usuário, de acordo com Abramek et al (2019, p.3). O modelo utiliza dos sites e ferramentas de buscas da internet, comprando o direito de aparecer no "topo" da pesquisa conforme alguma palavra-chave esteja relacionado a busca do usuário.
Por outro lado, o *pop-up* é considerado o modelo de anúncio mais irritante para os usuários, segundo Canesso (2004, p.3). São janelas que se abrem automaticamente quando a página *web* é carregada, podendo conter imagens, imagens animadas (*gifs*) ou vídeos. Também existem outras versões do *pop-up* como o *pop-under* e o *pop-behind*, que são anúncios executados em segundo plano e só serão visualizados quando o usuário minimizar ou fechar a página carregada. É um modelo mais eficiente de disponibilizar anúncios, já que o usuário não interrompe o carregamento do conteúdo (CANESSO, 2004, p.4).

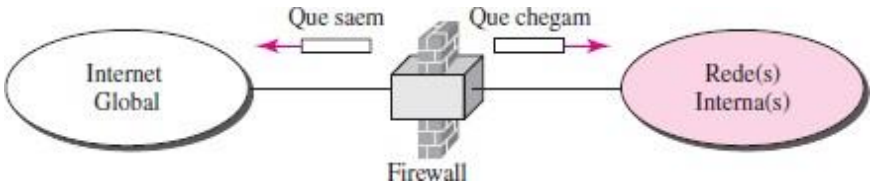
2.1.4 Filtro de Pacotes

De acordo com Kurose (2014), em uma rede corporativa normalmente tem um roteador de borda que conecta a rede interna com a internet pública. Tudo que sai ou entra na rede passa por esse roteador e nele ocorre a filtragem de pacotes. Um filtro de pacotes examina os dados e decide se podem ser trafegados ou não, baseado em regras específicas definidas pelo administrador da rede.
O administrador configura um *firewall* com base na sua política de rede. A política pode considerar a produtividade do usuário, uso de largura de banda e a segurança da rede.

2.1.5 *Firewall*

Conforme Forouzan (2010), *Firewall* é um dispositivo instalado entre uma rede doméstica ou corporativa e o resto da internet. Aparelho projetado para encaminhar e filtrar pacotes de dados. O funcionamento do firewall é mostrado na Figura 3.
Geralmente é classificado como *firewall* de filtragem de pacotes e *firewall* baseado em *proxy.*

Figura 3 – Funcionamento de um *Firewall*

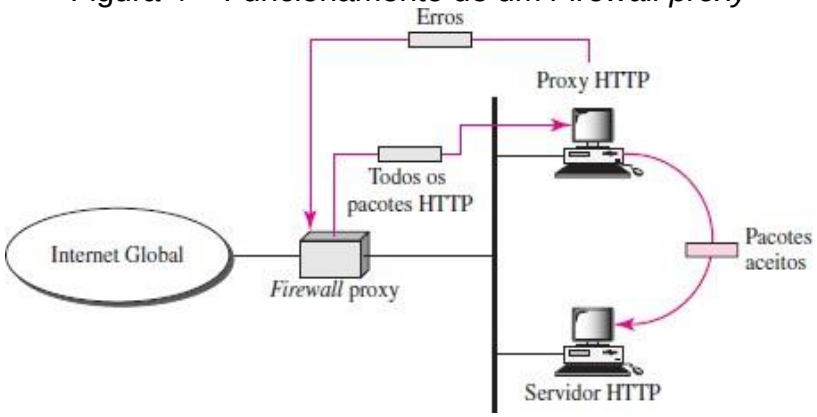


Fonte: Forouzan, 2010, p.1022.

2.1.5.1 *Firewall Proxy*

De acordo com Forouzan (2010) e a figura abaixo, um *Firewall Proxy* filtra os pacotes de solicitações *web* (HTTP) de um navegador de internet. O usuário envia um pacote e o *Proxy* executa um processo de servidor para receber a solicitação, verificando se a solicitação é permitida.
O servidor baseia as filtragens nos endereços das páginas *web* (por meio de URLs) requisitadas e decide se o usuário pode acessá-las.

Figura 4 – Funcionamento de um *Firewall proxy*



Fonte: Forouzan, 2010, p.1023

2.2 Trabalhos Relacionados

Dhenn et al. (2018) tiveram como objetivo implantar um sistema bloqueador de anúncios usando um *Raspberry* Pi 3 e o *software Pi-Hole* para filtrar as páginas *web*. Na metodologia, utilizaram o sistema operacional Linux “Diet Pi”, o *software* PuTTY para utilizar o computador numa sessão remota SSH, atribuíram um endereço IP estático e configuraram o *Pi-Hole* com um roteador para filtrar os anúncios de um computador *desktop*.
Os autores concluíram que um bloqueador de anúncios em nível de rede é mais seguro do que bloqueadores de anúncios tradicionais, instalados como extensões de navegadores, que são mais suscetíveis a conterem vírus, o que leva ao usuário desenvolver problemas no dispositivo.

Sankala (2020) realizou uma tese para investigar e encontrar formas de bloquear anúncios durante a navegação na internet em dispositivos *desktop* ou móveis. Usaram *Raspbian* como sistema operacional para instalar o *Pi-Hole* para bloquear anúncios e *OpenVPN* como servidor VPN, simultaneamente acessando páginas *web* com o navegador *Tor*.

Sankala (2020) afirma que extensões de navegador para bloqueio de anúncios são inferiores, pois são feitas para bloquearem em um só dispositivo, já bloqueadores como *Pi-Hole* funcionam com todos os dispositivos que estiverem conectados à rede local. Devido ao baixo consumo de energia, poder ficar ligado por bastante tempo e com um preço barato, *Raspberry* Pi tem vantagens comparado a outros sistemas e utilizando VPN com um navegador web anônimo como *Tor* proporciona alta segurança de rede enquanto o usuário navega pela internet.

3 Metodologia

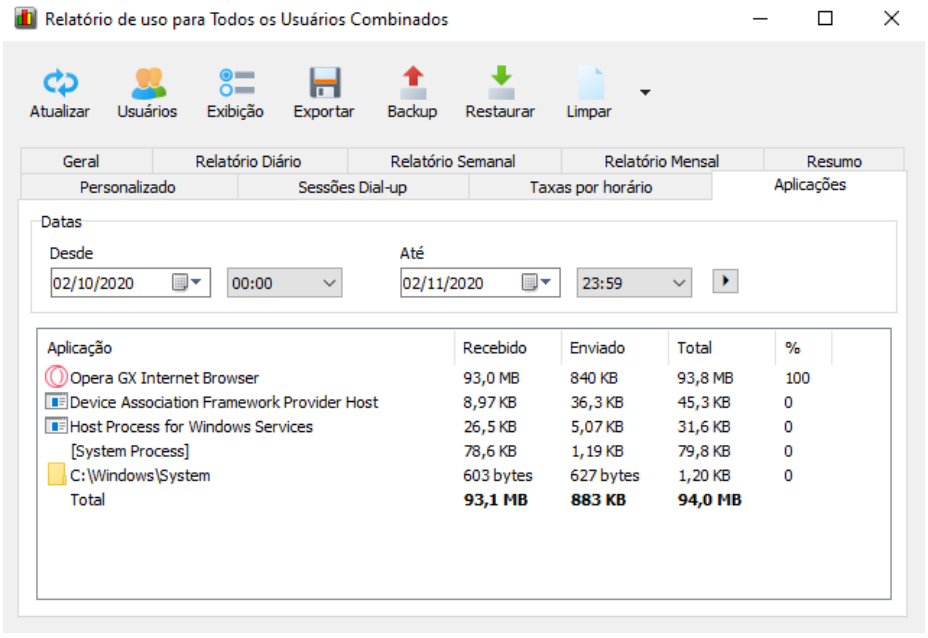
3.1 Materiais

- **Software Pi-Hole (v.5.0)** para bloqueio de anúncios e filtro de DNS, software de código aberto, fácil de instalar e funciona perfeitamente com requisitos mínimos de hardware. Transforma um servidor DNS local em um bloqueador de anúncios em nível de rede. Não só anúncios, mas conteúdo indevidos, pornografia, fraudes e redes sociais tem seus DNS anulados se inserir os links específicos ou blacklists personalizada na interface web do Pi-Hole.
- **Placa *Raspberry* Pi 3 Modelo B+ Anatel**, a revisão de 2018 do terceiro modelo do *Raspberry* Pi, tem um processador de *quad-core* de 1.4 GHz, 1GB de memória RAM com conexões Wi-Fi, Ethernet e Bluetooth. Para usar o mini computador, estamos usando uma Fonte de Energia DC Chaveada 5V 3A MicroUSB, um Cartão de Memória MicroSD de 16GB para instalar o sistema operacional e um mouse e teclado USB. Escolhemos esta placa pelo preço e processamento para evitar má performance na área de trabalho.
- **Sistema Operacional *Raspberry* Pi OS (v.4.19)**, oficialmente chamado de Raspbian, criado pela fundação *Raspberry* Pi e feito para rodar em placas *Raspberry* Pi. Simples de instalar usando NOOBS, um gerenciador de instalação de sistema operacional para o *Raspberry* ou inserindo a imagem de disco do sistema em Cartões SD usando *softwares* de gravação como o BalenaEtcher.
- **Software Networx (v.6.2.8)** para relatórios de monitoramento de largura de banda e uso de dados geral, diários ou por aplicação.
- **Sistema Operacional Windows 10** para instalar o *software* NetWorx e realizar os testes de monitoramentos de tráfego de dados.
- **Roteador Wireless TP-LINK TL-WR940N** para conexão de rede, gerar o IP Estático para o Pi-Hole e coletar as consultas DNS do servidor DNS local.

3.2 Métodos

1. Foi baixado a versão do *Raspberry* Pi OS com *Desktop* no site oficial do sistema e foi gravado a imagem de disco no Cartão de Memória MicroSD com o *software* balenaEtcher.
2. Foi instalado o sistema operacional *Raspberry* Pi OS inserindo o cartão de memória no *Raspberry* Pi 3 e conectando-o a fonte de energia para ligar o computador.
3. Foi atribuído um endereço IP estático para o *Raspberry* Pi utilizando a interface *web* do Roteador (apêndice A), para que o *Pi-Hole* funcione corretamente.
4. Foi instalado o *software* "*Pi-Hole*" no sistema operacional (apêndice B) por linha de comando. Assim identificando o IP estático e instalando a interface e servidor *web* do *Pi-Hole*. Não foram adicionadas *blacklists* personalizadas, utilizando assim apenas as *blacklists* padrões do software.
5. Foi conectado o *Raspberry* PI com o Sistema Operacional Windows 10 como Servidor DNS (apêndice C). Desse modo, as consultas DNS serão filtradas.
6. Foi instalado o *software* Networx pelo site oficial e monitoramos e coletamos os dados de banda de internet verificando o relatório de uso de dados por aplicação.

Figura 6 - Relatório de uso de dados por aplicação no NetWorx



Fonte: Os Autores

7. Para calcular a porcentagem de diferença entre os resultados obtidos com e sem o bloqueador foi utilizado uma regra de três onde a média do consumo sem o bloqueio é 100% e a média com o bloqueio é a porcentagem a ser

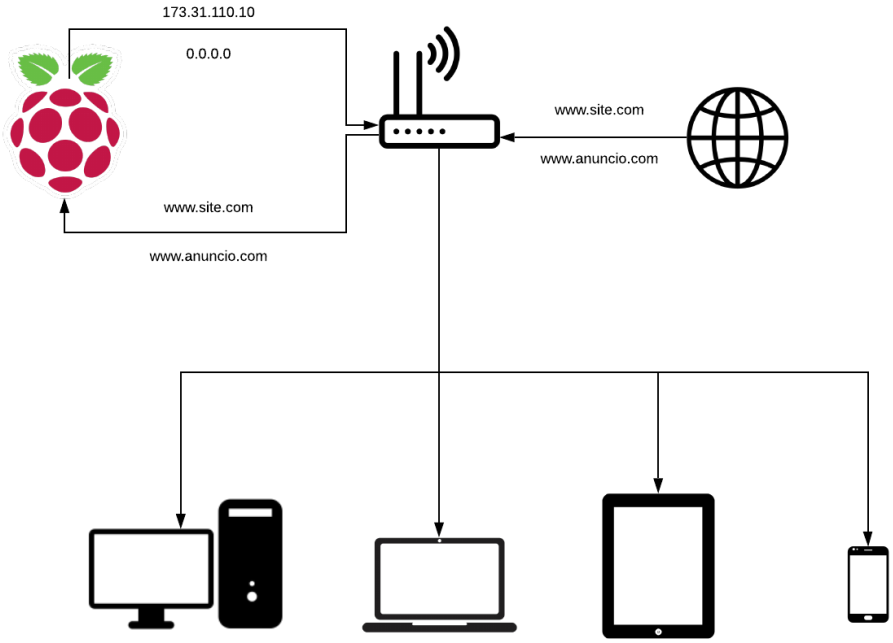
descoberta, e após subtrair este valor do 100% para obter a porcentagem com apenas o consumo de banda correspondente aos anúncios.

8. Sabendo a porcentagem apenas do consumo de anúncios e com base nos valores tirados do relatório da Anatel, pode-se utilizar novamente uma regra de três onde 100% é R$86,17 e a porcentagem obtida no tópico acima é o valor em reais a ser descoberto.

3.3 Infraestrutura com o Dispositivo

Quando o dispositivo está instalado na rede o sistema de *download* presente na rede é alterado, pois como o dispositivo filtra os DNS caso ele seja um anuncio o dispositivo entrega ao roteador como um IP “0.0.0.0” e que por sua vez repassa ao dispositivo que solicitou o pacote de dados.

Figura 5 – Infraestrutura com o Dispositivo



Fonte: Os autores.

Como ilustrado na Figura 5, primeiramente é representado dois *DNS* provenientes da internet e sendo entregues ao roteador, sendo um *DNS* de um site e o outro dos anúncios presentes nele, neste esquema a infraestrutura residencial é diferente da comum, pois ao invés do roteador já entregar os dados para o dispositivo que solicitou ele encaminha para o *Raspberry* realizar a filtragem, e por fim o bloqueador devolve o endereço IP dos *DNS* ao dispositivo solicitante, porém o que ele identificou como anúncio passa a ser um endereço zerado, assim não só bloqueando os anúncios mas também nem permitindo que o dispositivo faça o *download* dos mesmos.

3.4 Plano de Testes

Foi elaborado um plano de teste que se aproxima do uso de um usuário de internet navegando pela *homepage* de um site, onde foi percorrido toda a estrutura da página para que assim pudesse ser baixado todo o conteúdo presente nela.
Baseado na base de dados disponibilizado pela Alexa em 2020, onde lista os sites mais acessados do Brasil, foi selecionado os três principais portais de notícias para que assim o foco do site e parte de sua estrutura seja semelhante.
Os testes foram separados em cinco utilizando o bloqueador e cinco sem o bloqueador por site, totalizando trinta testes, onde ficaram sendo monitorados por 12 minutos a cada teste, pois alguns sites têm um mecanismo de recarregar a página após um certo tempo, para que o conteúdo do site seja baixado novamente. O monitoramento foi feito utilizando o programa NetWorx, onde após o período de 12 minutos era coletado o consumo e esses dados foram separados e organizados em uma planilha e ilustrados por meio de gráficos para que se pudesse visualizar melhor a diferença.

4 Resultados Obtidos

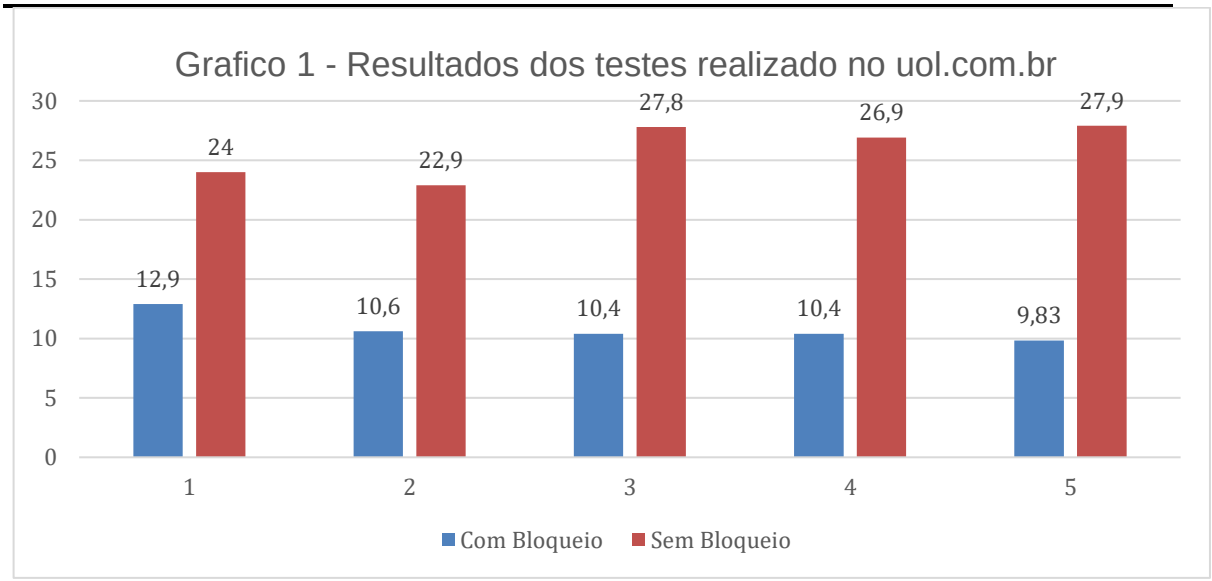
Após a utilização do dispositivo proposto por esse trabalho, foram coletados os dados da Tabela 1, nela consta-se as médias dos resultados obtidos em cada site durante o monitoramento, sendo possível observar que há um aumento significativo nos MB consumidos em todos os sites quando não havia a interferência do dispositivo.

Tabela 1 – Média de Consumo de Banda

Site Monitorado	Com Bloqueio (MB)	Sem Bloqueio (MB)	(%) Consumo de banda dos anuncios
uol.com.br	10,82	25,6	57,74
g1.com.br	4,706	9,572	50,84
metropoles.com	2,486	33,34	92,55
MÉDIA	6,00	22,84	-

Fonte: Os autores.

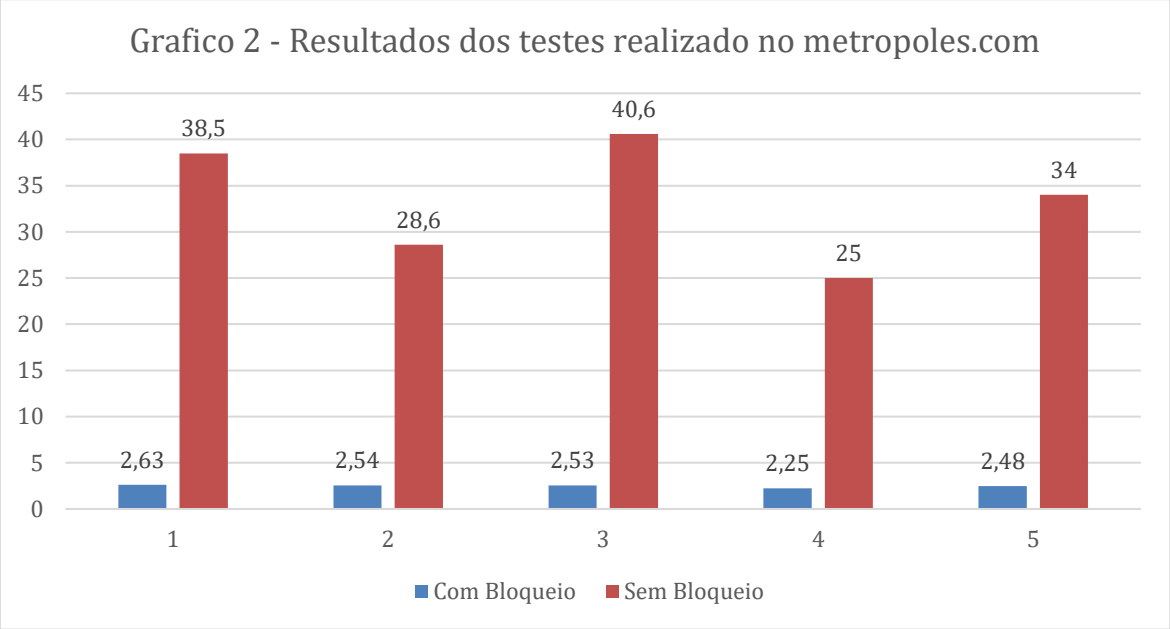
Os resultados de todos os testes realizados no site uol.com.br constam no Gráfico 1, e nele é possível analisar que apenas a estrutura do site e seu conteúdo é estável com uma variação mínima, porém quando os anúncios são baixados com a estrutura e conteúdo, mostra uma variação maior no consumo de banda, o que significa que o tipo do anúncio influencia no consumo de banda.



Fonte: Os autores.

Comparando os dados obtidos no Gráfico 1, entre o menor (9,83) e maior (27,9) consumo presente nos testes, pode-se afirmar que houve um aumento percentual de 183,82 no consumo de dados.

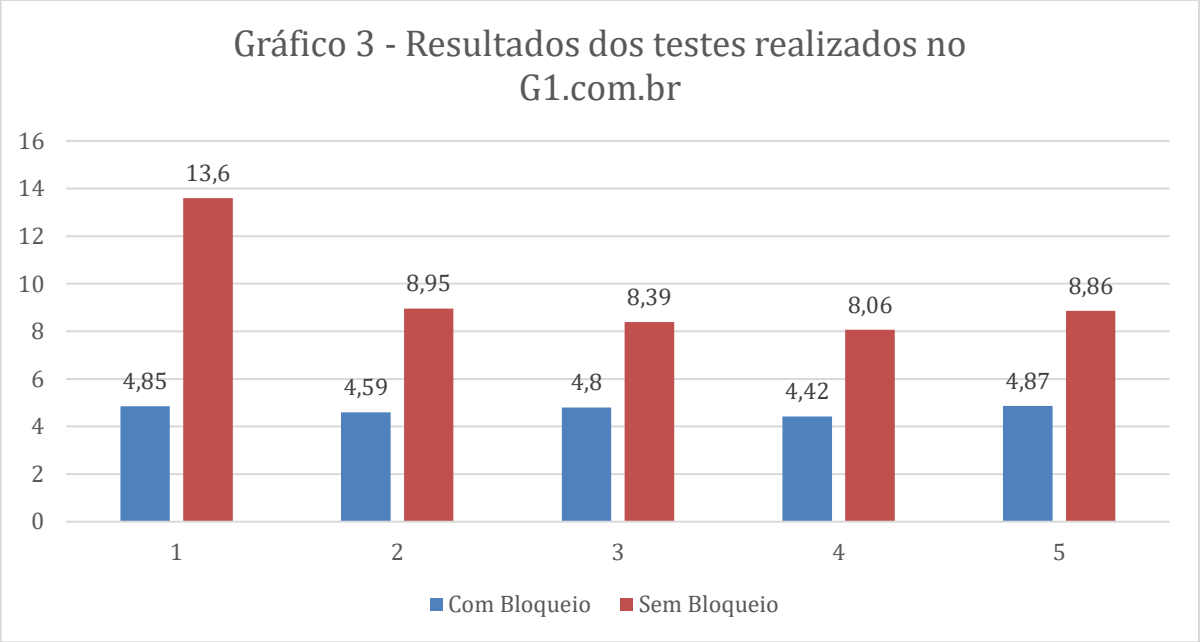
No Gráfico 2 constam todos os resultados obtidos nos testes utilizando o site metrópoles.com, e nele foi possível notar uma grande diferença entre os dados obtidos com e sem o bloqueio, pois como foi observado ao longo dos testes, o site utiliza bastante do tipo de anuncio de vídeos em alta resolução e imagens animadas (*gifs*), e utiliza a estratégia de recarregar automaticamente para que os anúncios sejam baixados novamente ou trocados por outros, assim aumentando o consumo consideravelmente.



Fonte: Os autores.

Comparando os dados obtidos no Gráfico 2, entre o menor (2,25) e maior (40,6) consumo presente nos testes, pode-se afirmar que houve um aumento percentual de 1704.44 no consumo de dados.

No Gráfico 3 constam os resultados dos testes realizados no G1.com.br, no primeiro teste sem o bloqueio de anúncios foi demonstrado que ele é o que mais consumiu dados quando comparado com os demais testes, já que durante sua realização foi verificado a presença de vários banners com gifs em alta resolução, enquanto que nos outros foi notado que esse tipo de anúncio teve diminuição, sendo substituído por *banners* com apenas uma imagem estática em alta resolução e quando tinham *gifs* presentes, era em uma quantidade consideravelmente menor do que no primeiro teste.



Fonte: Os autores.

Comparando os dados obtidos no Gráfico 3, entre o menor (4,42) e maior (13,6) consumo presente nos testes, pode-se afirmar que houve um aumento percentual de 207,70 no consumo de dados.

A quantidade de consumo em sites com anúncios é representada por 100%, então para se descobrir a porcentagem de consumo apenas dos anúncios, é necessário descontar desses 100%, a quantidade gasta sem a presença de anúncios, que é fornecida pelo teste realizado.
Diante disso e com os dados coletados e disponibilizados pela Anatel no seu relatório de 2018, a velocidade média contratada pelos brasileiros é de 24,62 Mbps, sendo que o Brasil tem como média de custo de R$3,50 por Mbps, totalizando um valor mensal de R$86,17 para o bolso do brasileiro. Sabendo disso, pode-se calcular a média de porcentagem dos anúncios. A média de consumo dos sites com anúncios foram de

22,84 Mbps, e sem anúncios foi de 6 Mbps, o que corresponde a 26,27%, ou seja, 73,73% do consumo é apenas para o *download* dos anúncios, então se consegue determinar que no cenário brasileiro, o usuário paga R$63,53 apenas para baixar os anúncios presentes nos sites acessados.

5 Considerações Finais

Como apresentado anteriormente, ter um bloqueador de anúncios fazendo parte da sua infraestrutura é mais confiável do que quando comparado a *softwares* de terceiros (*plugins*), pois não dependeria dos donos da ferramenta cuidarem da falhas e segurança do *software*. Colocando mais um dispositivo na sua rede residencial ou empresarial seria mais um obstáculo para que um vírus ou *malware* infecte e roube seus dados e informações pessoais, garantindo uma privacidade maior.

O microcontrolador *Raspberry* Pi 3 B+ se mostrou muito versátil, e foi o dispositivo ideal para este projeto por conta do tamanho reduzido o que torna ele mais um dispositivo que pode fazer parte de qualquer infraestrutura residencial ou empresarial, e também por conta de seu processamento eficiente e suficiente para suportar essa funcionalidade de filtro de *DNS*, mas principalmente por seu baixo custo e por ter uma curva de aprendizado curta e simples.

Conclui-se que o projeto através da comparação dos resultados obtidos de dados de consumo de banda de internet como descritos na metodologia e realizando os métodos de cálculo de porcentagem de consumo em sites com anúncios, foi possível evidenciar que na presença do dispositivo a economia de dados foi maior e consequentemente o usuário utiliza a franquia que realmente paga, pois todos os pacotes de internet e a velocidade do plano contratado seria para consumir o conteúdo ou informação desejada e não os anúncios presentes nos sites, assim atingindo com êxito o objetivo deste trabalho.

Referências Bibliográficas

ABRAMEK, Edyta; STRZELECKI, Artur; SOTYSIK-PIORUNKIEWICZ, Anna. **Technical and Social Reasons for Blocking Web Advertising in the Context of Sustainable Development of E-Business.** In: INTERNATIONALCONFERENCE ON PERSPECTIVES IN BUSINESS INFORMATICS RESEARCH (BIR 2019), 18.2019, Katowice, Polônia. Joint Proceedings of the BIR 2019 Workshops and Doctoral Consortium. Katowice, Polônia: Ceur-ws, 2019. p. 39 -50.

ALEXA (org.). **Alexa - Top Sites in Brazil - Alexa**. 2020. Disponível em: https://www.alexa.com/topsites/countries/BR. Acesso em: 01 dez. 2020.

ANATEL (Brasil) (org.). **Relatório de acompanhamento do setor de telecomunicações**: serviço de comunicação multimídia - banda larga fixa. Brasília: Anatel, 2018. 32 p. Disponível em: https://www.abranet.org.br/doc/relatorio_servicos_banda_larga_fixa_scm_2018.pdf?UserActiveTemplate=s. Acesso em: 03 nov. 2020.

CANESSO, Natacha Stefanini. **Publicidade na Internet: um estudo dos formatos de anúncios on-line.** In: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 27., 2004, Porto Alegre. XXVII Congresso Brasileiro de Ciências da Comunicação -Intercom. Comunicação, acontecimento e memória. Porto Alegre: Intercom, 2004. p. 1 -11. Disponível em: http://www.intercom.org.br/papers/nacionais/2004/resumos/R0150-1.pdf. Acesso em: 14 nov. 2019.

DHENN Sanoaf. et al. NETWORK-WIDE RANGE AD-BLOCKER USING RASPBERRY PI. **International Journal Of Pure And Applied Mathematics: Special Issue on ICISER'18 by NPSBCET, Chennai, Tamilnadu, India.** Coimbatore, p. 1771-1775. 2018. Disponível em: https://acadpubl.eu/jsi/2018-119- 10/articles/10b/59.pdf. Acesso em: 30 abr. 2020.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores.** 4. ed. Porto Alegre: AMGH, 2010

KRAMMER, Viktor. **An Effective Defense against Intrusive Web Advertising.** In: ANNUAL CONFERENCE ON PRIVACY, SECURITY AND TRUST, 6.2008, Fredericton.2018 16th Annual Conference on Privacy, Security and Trust (PST).New Brunswick, Canada: Nb, 2008. p. 3-14.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet: uma abordagem top-down.** 6. ed. São Paulo: Pearson Education do Brasil, 2013.

PAGEFAIR LIMITED (Canadá). Blockthrough Inc. **The state of the blocked web**: 2017 global adblock report. Toronto, 2017. 20 p. Disponível em: https://f.hubspotusercontent10.net/hubfs/4682915/Adblock%20Reports/PageFair%20Report%202017.pdf. Acesso em: 02 nov. 2020

PI-HOLE. **Pi-hole documentation.** 2020. Disponível em: https://docs.pi-hole.net/

RASPBERRY PI FOUNDATION. **Raspberry Pi Documentation.** 2020. Disponível em: https://www.raspberrypi.org/documentation/

RASPBERRY PI FOUNDATION. **Raspberry Pi OS - Raspberry Pi Documentation.** 2020. Disponível em: https://www.raspberrypi.org/documentation/raspbian/

SANKALA, Jesse. **MAINOSTEN ESTO-OHJELMISTO PI-HOLE**: linux-käyttöjärjestelmille paikallisen verkon kattava mainosten esto-ohjelma. 2020. 35 f. Tese (Doutorado) - Curso de Bacharel em Ciências, Tecnologias de Informação e Comunicação, Turku University Of Applied Sciences, Turku, Finlândia, 2020. Disponível em:

https://www.theseus.fi/bitstream/handle/10024/343792/Sankala%20Jesse%20PiHole.pdf?sequence=2 . Acesso em: 19 out. 2020.

SINGH, Ashish; POTDAR, Vidyasagar. **Blocking online advertising - a state of the art.** In: INTERNATIONAL CONFERENCE ON INDUSTRIAL TECHNOLOGY (ICIT 2009), 12.2009, Victoria, Australia. Proceedings of the international conference on industrial technology (ICIT 2009). Victoria, Australia: Ieee, 2009. p. 1 -10.

SOFTPERFECT (Australia). **NetWorx: bandwidth monitor, connection speed test, data usage log.** 2020. Disponível em: https://www.softperfect.com/products/networx/. Acesso em: 17 ago. 2020.

TANENBAUM, Andrew S. **Redes de Computadores.** 4. ed. Rio de Janeiro: Editora Campus (elsevier), 2003. UPTON, Eben; HALFACREE, Gareth. Raspberry Pi - Manual do Usúario.Rio de Janeiro: Alta Books, 2017

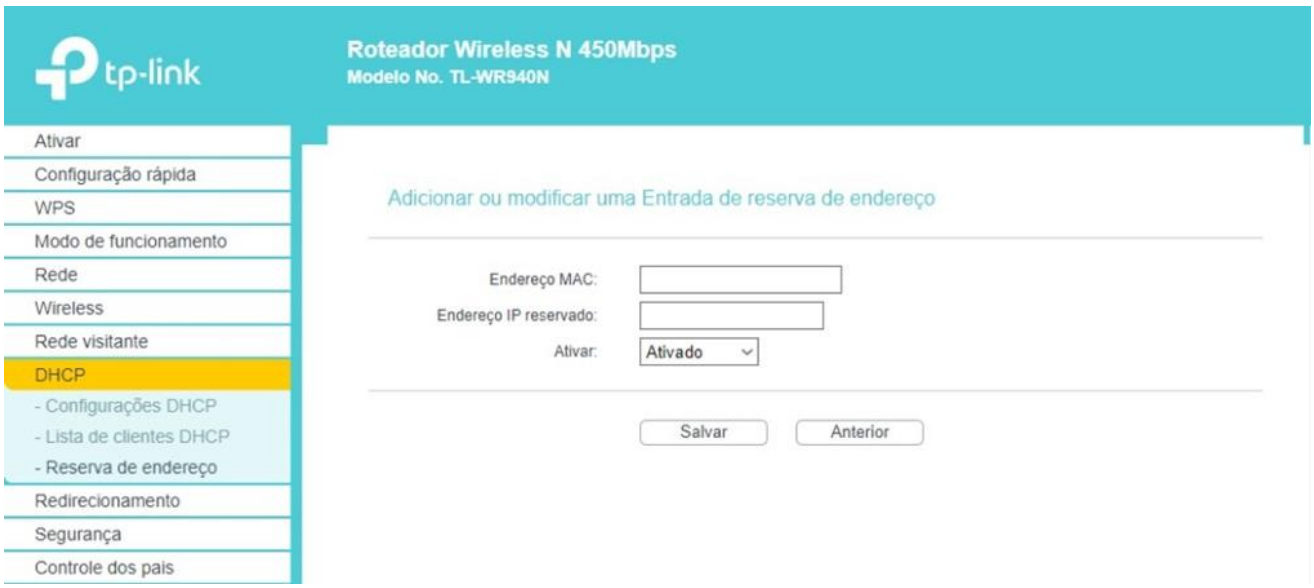
TP-LINK. **TL-WR940N V6 User Guide.** 2020. Disponível em: https://www.tp-link.com/us/user-guides/TL-WR940N_V6/. Acesso em: 02 out. 2020.

UPTON, Eben; HALFACREE, Gareth. **Raspberry Pi - Manual do Usúario**. Rio de Janeiro: Alta Books, 2017.

APÊNCIDE A – Atribuir Endereço de IP Estático no Raspberry Pi

1. Revelar o endereço IP/MAC do Raspberry Pi com o comando ifconfig no terminal; endereços nas tags: inet e ether.
2. Entrar na página de administrador do roteador TL-WR940N (http://192.168.1.1/) com usuário e senha padrão:“admin”.
3. Na Aba “DHCP”, no menu “Reserva de Endereço”, adicione manualmente os endereços IP/MAC obtidos e confirme as alterações.

Figura 1 – Reserva de Endereço no Roteador TL-WR940N



Fonte: Os autores.

4. Reconectar a energia do Raspberry Pi para o roteador atribuir o IP Estático.

APÊNDICE B - Instalar o Software “Pi-Hole” no Sistema Operacional

1. Inserir o comando no terminal: curl –sSL https://install.pi-hole.net | bash

2. Nas telas de configuração do “Pi-Hole” escolher as opções:

- Google DNS como Provedor de DNS
- Host List (ou Lista de Hosts): Selecionar Todas
- Selecionar o protocolo IPv4
- Confirmar o IP Estático do Raspberry
- Instalar a interface Web do “Pi-Hole”
- Instalar o servidor web do “Pi-Hole”
- Ativar “LogQueries”
- Ativar “Privacy mode for FTL”

3. Depois de confirmar as opções, acesse a interface web do “Pi-Hole” com a url http://pi.hole/admin ou com a url substituindo o “pi.hole” com o IP Estático previamente atribuído.

APÊNDICE C - Conectar Raspberry PI com o Sistema Operacional Windows 10 como Servidor DNS

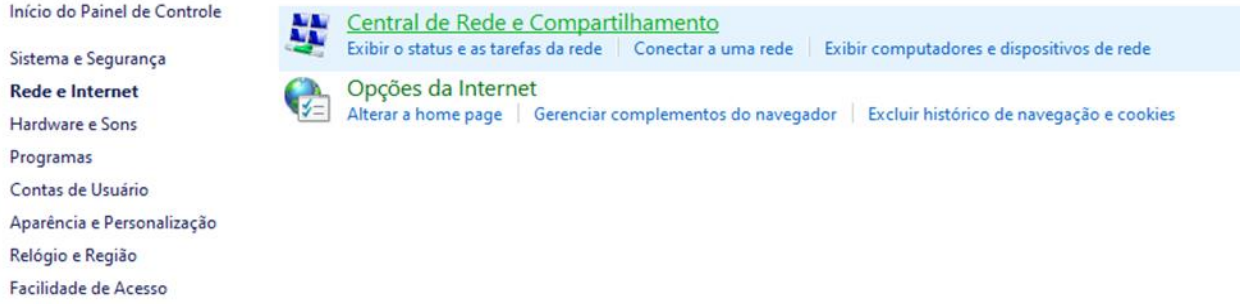
1. Entre no Painel de Controle do Windows 10 e selecione Rede e Internet

Figura 2 – Opção “Rede e Internet” no Menu “Painel de Controle”

Fonte: Os autores.

2. Selecione “Central de Rede e Compartilhamento”

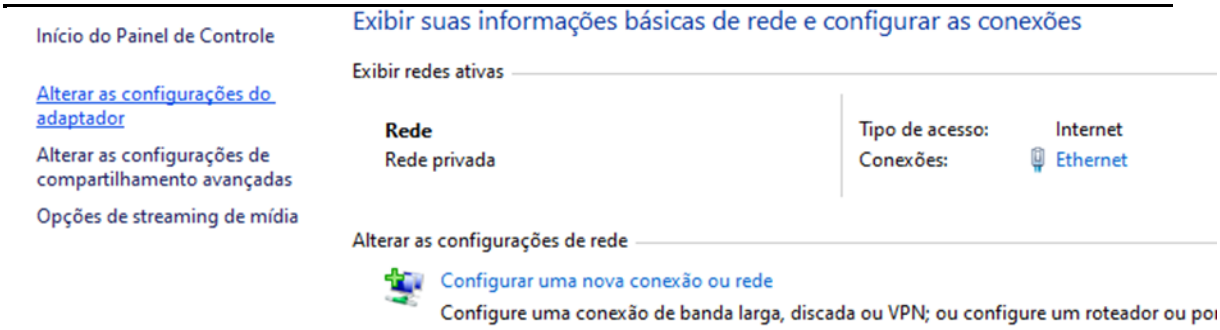
Figura 3 – Opção “Central de Rede e Compartilhamento”



Fonte: Os autores.

3. Selecione “Alterar Configurações do Adaptador”

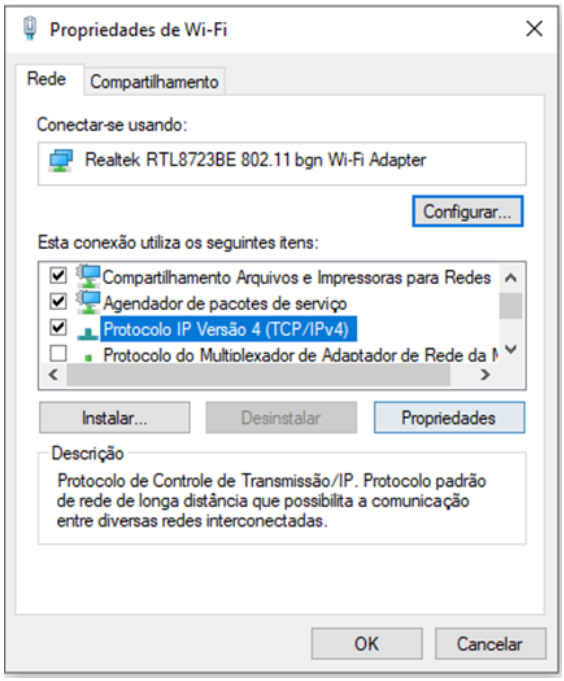
Figura 4 – Opção “Alterar as Configuração do Adaptador”



Fonte: Os autores.

4. Nas conexões de rede, entre nas propriedades do roteador TL-WR940N
5. Selecione “Protocolo IP Versão 4 (TCP/IPv4)” e clique em “Propriedades”

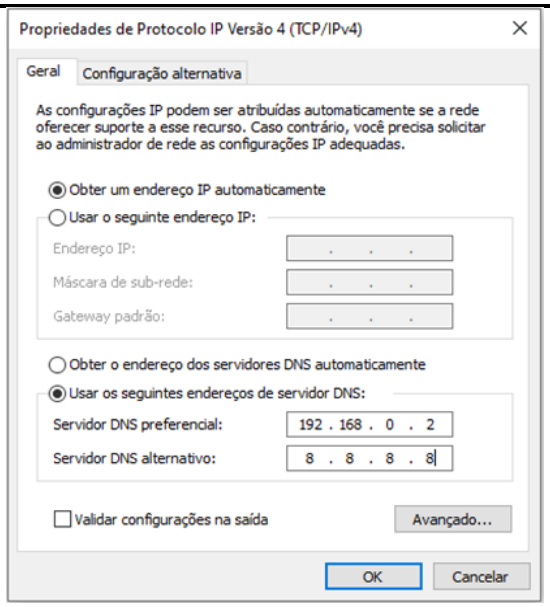
Figura 5 – Propriedades de Wi-Fi nas Conexões de Rede do Windows 10



Fonte: Os autores.

6. Selecione “Usar os seguintes endereços de servidor DNS:” e insira como Servidor DNS preferencial o IP Estático do Raspberry Pi e o Servidor do Google (8.8.8.8) como Servidor DNS alternativo.

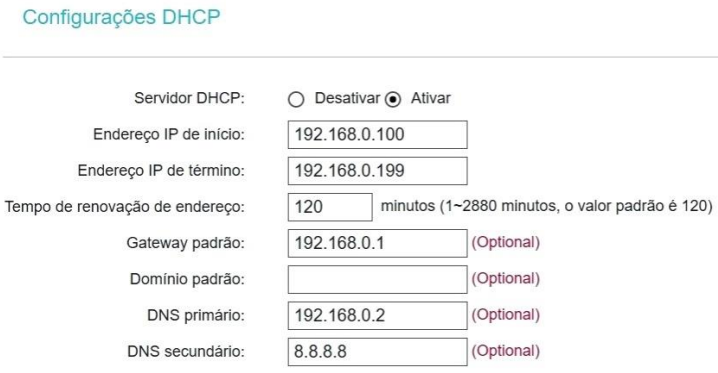
Figura 6 – Propriedades do Protocolo IPv4 do Roteador no Windows 10



Fonte: Os autores.

7. Alternativamente, é possivel configurar o DNS primário e secundário na página de Administrador do Roteador nas configurações DHCP.

Figura 7 – Configurações DHCP do Roteador TP-LINK TL-WR940N



Fonte: Os autores.