INSTITUTO FEDERAL
Catarinense

TECNOLOGIA E REDES DE COMPUTADORES

9ª EDIÇÃO

VANDERLEI FREITAS JUNIOR
EDMILSON ESPINDOLA DOS SANTOS

INSTITUTO FEDERAL
Catarinense

TECNOLOGIA E REDES DE COMPUTADORES

9ª EDIÇÃO

VANDERLEI FREITAS JUNIOR
EDMILSON ESPINDOLA DOS SANTOS

2023

Instituto Federal Catarinense

INSTITUTO FEDERAL
Catarinense

INSTITUTO FEDERAL CATARINENSE

REITORA
Sônia Regina de Souza Fernandes

PRÓ-REITORA DE ENSINO
Josefa Surek de Souza

PRÓ-REITOR DE EXTENSÃO
Fernando José Taques

PRÓ-REITORA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
Fátima Peres Zago de Oliveira

PRÓ-REITORA DE DESENVOLVIMENTO INSTITUCIONAL
Jamile Delagnelo Fagundes da Silva

PRÓ-REITOR DE ADMINISTRAÇÃO
Stefano Moraes Demarco

CÂMPUS AVANÇADO SOMBRIO

DIRETOR GERAL
Victor Martins de Sousa

DIRETOR DE ENSINO, PESQUISA E EXTENSÃO
Jeferson Mendonça de Limas

INSTITUTO FEDERAL CATARINENSE,
CÂMPUS AVANÇADO SOMBRIO
Av. Prefeito Francisco Lummertz Júnior, 931
CEP 88960-000 - Sombrio/SC
www.sombrio.ifc.edu.br

INSTITUTO FEDERAL
Catarinense

Direção Editorial	Vanderlei Freitas Junior
Capa e Projeto Gráfico	Claiton Andrade Junior
Editoração Eletrônica	Edmilson Espíndola dos Santos
Comitê Editorial	Armando Mendes Neto
	Cleber Luiz Damin Ferro
	Diego Monsani
	Guilherme Klein da Silva Bitencourt
	Jéferson Mendonça de Limas
	Joédio Borges Junior
	Marco Antônio Silveira de Souza
	Matheus Lorenzato Braga
	Sandra Vieira
	Vanderlei Freitas Junior
	Victor Martins de Sousa
Revisão	Gilnei Magnus dos Santos
Organizador	Vanderlei Freitas Junior
	Edmilson Espíndola dos Santos

As informações contidas no livro são de inteira responsabilidade dos seus autores.

INSTITUTO FEDERAL
Catarinense

ISBN: 978-6-50089-141-6

Ficha catalográfica elaborada por Diego Monsani - CBR 14/1192

T255 Tecnologias e Redes de Computadores / Vanderlei Freitas Junior; Edmilson Espíndola dos Santos (org.). -- 9 ed.-- Sombrio : Instituto Federal Catarinense, 2023.
185 f.

ISBN 978-65-00-57444-9

1. Redes de computadores - Gerência. 2. Proteção de dados I.Freitas Junior, Vanderlei - 1980-. II. Título.

CDD: Ed. 21 -- 004.6

INSTITUTO FEDERAL
Catarinense

Agradecimentos

Agradecemos as valiosas contribuições de Claiton Andrade Junior, Diego Monsani, além dos alunos e professores que contribuíram com suas pesquisas para o engrandecimento desta publicação.

Esta é uma publicação do
Curso Superior de

Tecnologia em

REDES DE COMPUTADORES

INSTITUTO FEDERAL
Catarinense

Sumário

Sumário de Autores

Desenvolvimento de um simulador de rede para fins didáticos utilizando computação na nuvem

André Cardoso de Oliveira[1], Christhian Trevisan[1], Jeferson Mendonça de Limas[2], Vanderlei Freitas Junior[2]

[1] Acadêmicos do Instituto Federal Catarinense – Campus Avançado Sombrio – 88960000 – Sombrio – SC – Brasil

[2] Docentes do Instituto Federal Catarinense – Campus Avançado Sombrio – 88960000 – Sombrio – SC – Brasil

andreolive@live.com,christhiangaiva99@gmail.com, {jeferson.limas,vanderlei.freitas}@ifc.edu.br

Abstract:*This article presents a technological research in which it was possible to identify freely distributed technologies for the construction of a simulator that helps teaching in the disciplines of the course Redes de Computadores (Computer Networking) at Instituto Federal Catarinense - Campus Avançado Sombrio. The proposed system uses cloud computing through Openstack for the construction of virtual network environments that allows the student to carry out practical experiences of the theories seen in the classroom. The system was tested with students of the 6th Phase of the Computer Networking course and was able to perform the proposed objectives for the tasks to be performed in class.*

Resumo*: Este artigo apresenta uma pesquisa tecnológica em que possibilitou-se identificar tecnologias distribuídas gratuitamente para a*

construção de um simulador que auxilie o ensino nas disciplinas do curso de Redes de computadores do Instituto Federal Catarinense - Campus Avançado Sombrio. O sistema proposto utiliza computação na nuvem através do Openstack para a construção de ambientes virtuais de rede que possibilita ao aluno realizar experiências práticas das teorias vistas em sala de aula. O sistema foi testado com alunos da 6ª Fase do curso superior de Tecnologia de Redes de Computadores e mostrou-se capaz de desempenhar os objetivos propostos para as tarefas a serem realizadas em aula.

1. Introdução

A tecnologia tem contribuído com diversas áreas, disponibilizando ferramentas, técnicas e métodos capazes de facilitar o desenvolvimento de diferentes atividades. A educação não fica de fora deste cenário, passando a se apropriar das tecnologias da informação e comunicação para ensinar novas competências, desenvolver novos conhecimentos e preparar profissionais para os desafios do mundo do trabalho.

O ensino em componentes curriculares do curso de Redes de Computadores, como Serviços de Rede e Segurança de Rede, possui ferramentas que auxiliam o professor a desenvolver laboratórios virtuais para os alunos experimentarem as teorias vistas em sala de aula. Dentre essas ferramentas, encontra-se softwares para construção de ambientes, onde é possível simular uma rede de computadores completa como em um ambiente real.

Testes e experiências práticas são muito importantes para fixação dos conhecimentos teóricos e para a execução das atividades, os professores podem fazer o uso de simuladores e

emuladores de redes de computadores. Uma pesquisa feita no Instituto Federal Catarinense *Campus* de Sombrio por Isoppo et al. (2018), apontou que o sistema EVE-NG, na percepção dos alunos, é melhor nos quesitos de interface, variedade de marcas/modelos de equipamentos a serem emulados, proximidade com a realidade e facilidade de uso. No entanto, o custo da versão completa do sistema pode tornar a ferramenta financeiramente inviável para muitas instituições de ensino.

Outra alternativa aos laboratórios virtuais são os laboratórios físicos, onde o aluno precisa estar presente na instituição de ensino para experimentação de seus projetos. Porém, apenas grandes centros educacionais possuem condições para a construção e mantimento de um laboratório físico de redes (Filippetti, 2008).

Simuladores são capazes de desempenhar um importante papel em atividades de ensino, pois através de simuladores é possível criar situações que normalmente não seriam viáveis de se reproduzir em um laboratório real (Pinheiro, 2022).

Ao observar as disciplinas de Serviços de Redes e Segurança de Redes, pôde-se concluir que a falta de um simulador que não necessite de uma ampla capacidade computacional para cada aluno é um problema recorrente, durante as aulas práticas e para os trabalhos feitos em casa. Além disso, o software VirtualBox, que é utilizado em sala de aula, e também é muito utilizado pelos alunos para fazer os trabalhos em casa, dificulta o processo, pois ele não é desenvolvido especificamente para fins educacionais.

Com base neste contexto, o presente estudo tem por objetivo desenvolver um sistema que simule um ambiente computacional, priorizando a melhor experiência do aluno/professor e visando reduzir o custo para as instituições de ensino. O sistema tem como foco eliminar a necessidade de uma

alta capacidade de processamento do computador pessoal do aluno e dos professores para as atividades práticas, assim como facilitar e tornar o ensino e a aprendizagem mais interativos em qualquer disciplina da área da ciência da computação através do seu uso como ferramenta didática. O usuário poderá utilizar computadores e dispositivos de redes virtuais na nuvem e fazer experiências de forma remota e colaborativa, em um sistema computacional virtual. Além disso, o sistema deve ser uma opção viável e de baixo custo comparado às outras opções presentes no mercado.

O presente artigo organiza-se em seis seções. Na primeira, tem-se os argumentos a título de introdução. Na seção 2 são apresentados trabalhos que apresentam alguma relação com o tema proposto; Na seção 3 encontra-se o referencial teórico onde são apresentadas principais tecnologias empregadas para o desenvolvimento do sistema; A seção 4 apresenta a metodologia adotada, bem como identifica o problema para pesquisa e apresenta o desenvolvimento do sistema. A seção 5 apresenta os resultados obtidos após os testes; E, por fim, na seção 6 encontram-se as considerações finais obtidas após a conclusão do artigo.

2. Trabalhos Relacionados

Alguns estudos disponíveis na literatura já procuraram desenvolver simuladores para apoio ao ensino da área específica, relacionando-se com o presente trabalho.

Isoppo et al. (2018), realizaram uma análise da percepção dos alunos a respeito dos simuladores e emuladores utilizados nas disciplinas do curso e aplicaram um questionário para a turma da 4ª Fase do Curso de Redes de Computadores do ano de 2018. Conforme presente nas questões aplicadas no questionário, as autoras concluíram, a partir das respostas coletadas, que nos quesitos facilidade de uso, auxílio na

aprendizagem, desempenho do usuário na execução de tarefas, o software EVE-NG foi considerado mais proveitoso.

Filippetti (2008) apresenta uma arquitetura que permite a construção de laboratórios de redes de computadores que possam ser acessados remotamente, permitindo assim que os alunos coloquem em prática as teorias vistas em sala de aula. O autor, ainda, afirma que a estruturação de laboratórios remotamente acessíveis implica não somente em sua disponibilidade remota, mas na criação de uma interface que facilite a interação do aluno com a estrutura, e que permita o desenvolvimento de cursos usando a ferramenta como um recurso pedagógico.

Entretanto, Santos (2016), reforçou que o ensino e aprendizagem ficam prejudicados diante das restrições impostas pela forma tradicional de ensinar, caso a instituição de ensino não busque alternativas para contemplar o ensino prático necessário.

3. Referencial Teórico

Nesta seção serão descritas as teorias e tecnologias utilizadas para o desenvolvimento da ferramenta.

3.1 Uso de ferramentas para o ensino em Redes De Computadores

O processo de ensino de redes de computadores possui muitas disciplinas e assuntos com uma grande quantidade de conhecimentos técnicos e específicos. Além disso, diversos deles requerem mais do que uma simples explicação teórica, porém, nem sempre as instituições de ensino conseguem prover um laboratório adequado para tal. No estudo de redes de computadores, livros e artigos podem fornecer o embasamento teórico necessário, contudo, sem a possibilidade de experimentação, muitos dos conceitos passados em sala de aula acabam perecendo na memória dos estudantes (Filippetti, 2008).

Para a simulação em sala de aula, uma tecnologia bastante empregada tem sido a virtualização. A virtualização consiste na criação e execução de um ambiente virtual que simula fielmente um ambiente real, permitindo que um mesmo dispositivo execute diversos ambientes que geralmente necessitam de diversos dispositivos. Carissimi (2008), cita que a virtualização pode ser definida como uma forma de dividir um sistema principal em diversos sistemas distintos e independentes um do outro.

3.2 Openstack

Conforme o site OpenStack.org (2022), o Openstack é um sistema operacional de nuvem que controla grandes porções de computação, armazenamento e recursos de rede por meio de um centro de dados, tudo provido e gerenciado através de sua API. Outrossim, o OpenStack fornece aos administradores do sistema um painel para controlar e gerenciar os recursos.

3.3 Devstack

De acordo com OpenStack.org (2022), o DevStack é uma série de scripts extensíveis usados para trazer rapidamente um ambiente OpenStack completo, com base nas versões mais recentes da plataforma. Ele é usado interativamente como um ambiente de desenvolvimento e como base para grande parte dos testes funcionais do projeto OpenStack.

3.4 JavaScript

Uma vez definido que o usuário teria acesso ao sistema via web, a linguagem escolhida para o desenvolvimento foi JavaScript. Uma das vantagens de se usar essa linguagem é que é possível utilizar a mesma linguagem de programação tanto no lado do cliente quanto no lado do servidor. O cliente foi desenvolvido utilizando a biblioteca React e para o servidor foi utilizado o Node.js, ambas tecnologias que utilizam JavaScript.

3.4.1 React

De acordo com React (2022): “React é uma biblioteca JavaScript para construção de interfaces de usuário[...]”, sendo ela focada especificamente no front-end para desenvolvimento de interfaces de usuário web, possuindo um melhor desempenho durante a renderização das mesmas.

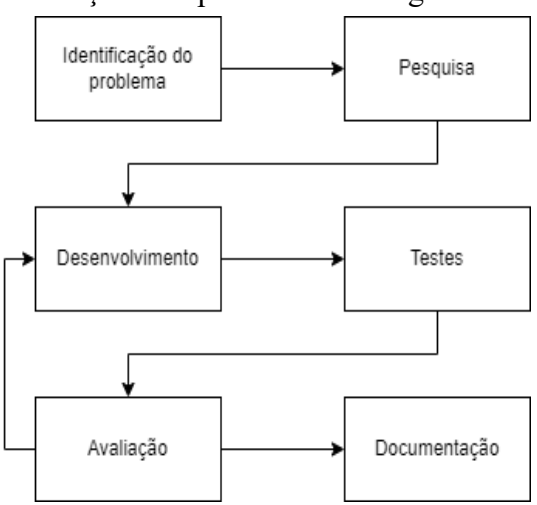
3.4.2 Node.js

Segundo Node.js (2022): “[...] o Node.js é projetado para desenvolvimento de aplicações escaláveis de rede.”. Ou seja, é um software para construção e execução de códigos javascript sem a necessidade de utilizar um navegador web.

4. Metodologia

A presente pesquisa classifica-se como pesquisa tecnológica, uma vez que tem como foco o desenvolvimento de um artefato que atenda aos objetivos especificados, tendo sido empregada a metodologia Design Science Research Methodology (DSRM), demonstrada na Ilustração 1.

Ilustração1:Etapas da metodologia



Fonte: Os Autores, 2022.

4.1 Identificação do Problema e Pesquisa

Para o aluno executar em casa os trabalhos propostos em sala no Instituto Federal Catarinense *Campus* Avançado Sombrio, como por exemplo, nas disciplinas de Serviços de Rede e Segurança de Redes, o aluno é orientado a utilizar o software VirtualBox para a virtualização de sistemas. Dessa forma, ele pode testar serviços e a segurança desses serviços de rede nesse ambiente virtualizado.

Visto que diversos alunos do curso de Tecnologia de Redes de Computadores não possuem um hardware que dê um bom suporte à virtualização de múltiplos sistemas, uma solução viável é a utilização da computação na nuvem para a virtualização. Com o uso dessa tecnologia o aluno poderá executar testes em ambientes virtualizados na nuvem, eliminando a necessidade de um hardware específico para esse fim.

Iniciou-se uma pesquisa das tecnologias atuais que possam ser úteis para alcançar os objetivos propostos. Visto que o simulador EVE-NG teve uma melhor posição na percepção dos alunos do curso de Redes de Computadores, buscou-se desenvolver um sistema que se assemelhe ao EVE-NG, que pudesse ser acessado de qualquer navegador e que seus recursos fossem semelhantes ao mais votado na pesquisa.

4.2 Desenvolvimento

Após uma ampla pesquisa por tecnologias disponíveis gratuitamente, encontrou-se na plataforma Openstack uma alternativa adequada para o desenvolvimento da ideia principal do projeto, uma vez que a plataforma possui uma API pronta que recebe solicitações, como por exemplo: implantar uma máquina virtual, conectá-la em uma determinada rede, ligar, desligar e excluir a máquina. Assim, todo o processo de criação de redes e máquinas virtuais estão prontas e disponíveis através da API do

Openstack. Com a finalidade de agilizar e simplificar a construção do ambiente de desenvolvimento do projeto, foi utilizado o Devstack, que também é disponibilizado pela plataforma.

Com o ambiente de desenvolvimento pronto, o próximo passo foi desenvolver o Backend, utilizando o Node.js. O Backend é responsável por fazer as solicitações através da API do Openstack. O Backend recebe essas solicitações do Frontend e as envia ao Openstack, que então fornecerá seus serviços de virtualização e responderá com as informações necessárias para o funcionamento básico do sistema.

Foi escolhido o desenvolvimento de uma interface semelhante ao simulador mais bem avaliado na pesquisa de Isoppo et al. (2018) para a melhor experiência do aluno e do professor, dentro e fora da sala de aula. O Frontend e o Backend se comunicam de forma bilateral em tempo real e o servidor envia constantemente informações das máquinas virtuais ao Frontend para dar um retorno visual ao usuário sobre o status dos dispositivos virtuais criados. Essa comunicação é feita através do protocolo WebSocket, que torna esse tipo de comunicação possível. O protocolo WebSocket é mais eficiente pois verificou-se que o tempo de resposta e o tráfego de rede que o WebSocket utiliza é bem menor, com custo relativamente baixo de largura de banda e servidor, comparado com outras tecnologias (SANTOS; SOUZA; ANDERLE, 2015).

4.2.1 IfCloud

Juntamente com o desenvolvimento, foi decidido que o nome para a ferramenta seria IfCloud, que consiste no termo presente em programação “if” e o apelido dado pelos estudantes ao Instituto Federal Catarinense *Campus* Avançado Sombrio, junto do termo *cloud* que significa nuvem na língua inglesa, já que o sistema se trata de computação em nuvem.

5. Resultados e Discussões

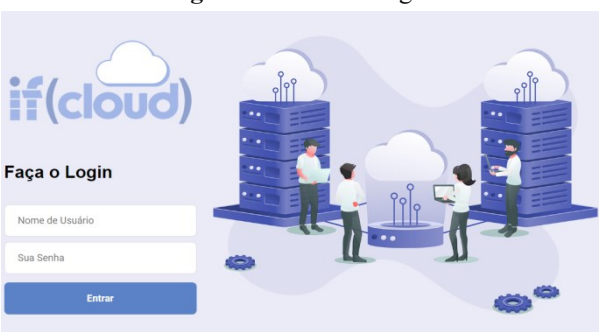
Nessa seção serão apresentados os resultados obtidos após o desenvolvimento da ferramenta, bem como discussão de pontos importantes sobre a mesma.

5.1 Telas do Sistema

No Frontend há duas telas principais, a tela de login onde o aluno entra com um usuário e senha para ter acesso a um ambiente virtual previamente disponibilizado pelo administrador do sistema. Para o gerenciamento de ambientes virtuais e usuários, o sistema conta com o keystone que é instalado pelo Devstack. Com ele, é possível criar políticas e métodos de controle de acesso altamente complexos, ou seja, garantir que os usuários tenham autorização para acessar somente o que lhes compete.

Os ambientes virtuais e usuários podem ser criados através da interface gráfica Horizon presente no próprio Openstack, eliminando assim a necessidade de criar uma interface exclusivamente para essa finalidade. Uma vez criado o ambiente e atribuído a ele um usuário, é possível agora fazer login, conforme a Figura 1, e dar início ao desenvolvimento do ambiente que deseja simular.

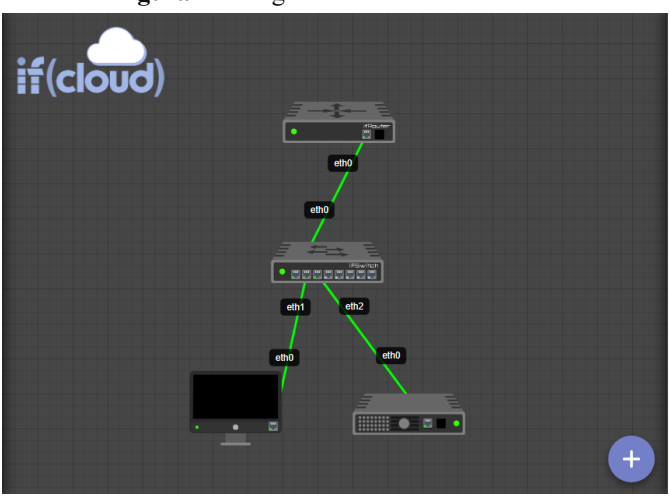
Figura 1 - Tela de Login



Fonte: Autores, 2022

A segunda tela do sistema é a tela onde o ambiente a ser simulado é montado. O usuário, clicando no sinal de adição, como visto na Figura 2, pode escolher através de um menu o tipo de dispositivo que deseja adicionar ao ambiente. No menu o usuário tem opções de dispositivos a serem construídos no ambiente virtual, como máquinas desktop com distribuições GNU/Linux e também máquinas para atuar como servidor. Os tipos de máquinas e sistemas já estão prontos no menu, o usuário apenas arrasta do menu e solta no diagrama do projeto para criar a máquina no ambiente virtual. Parâmetros de configuração da máquina virtual, como a quantidade de núcleos do processador, a quantidade de memória bem como a espaço em disco, são predefinidos pelo administrador do sistema, a fim de promover mais desempenho para uma maior quantidade de alunos utilizarem o sistema com a menor configuração possível de servidor para o IfCloud.

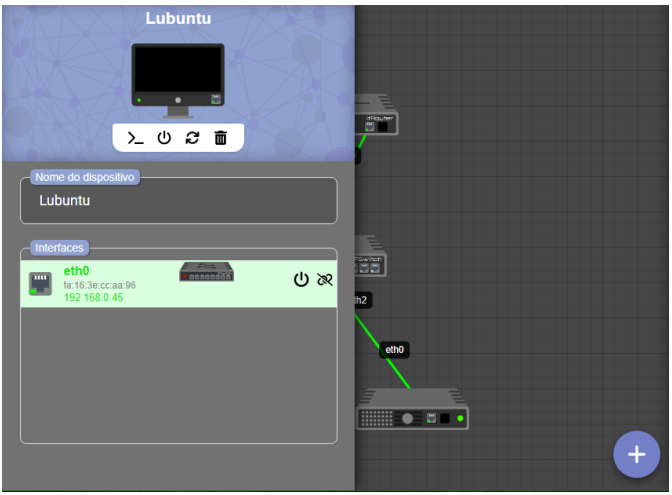
Figura 2 - Diagrama do ambiente Virtual



Fonte: Autores, 2022

O menu de configurações pode ser acessado através de um clique em um dos dispositivos, selecionando o dispositivo a ser configurado, onde o usuário além de obter informações de rede, pode ligar, desligar, reiniciar e acessar o dispositivo virtual, além de interagir com as interfaces de rede, conforme demonstrado na figura 3.

Figura 3 - Menu de Configuração do dispositivo



Fonte: Autores, 2022

5.2 Discussão

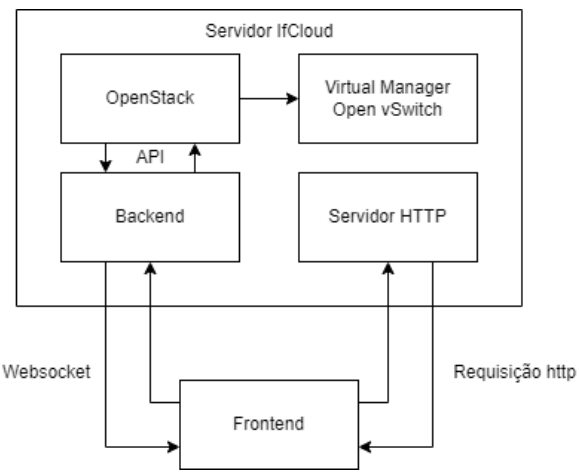
A necessidade da virtualização para criação de ambientes de rede, que simulam uma situação real em uma empresa,se mostrou presente em boa parte do curso de Redes de Computadores e a computação na nuvem gerenciada pelo Openstack é uma ótima ferramenta didática, combinada com uma interface web que traz para o aluno e o professor um retorno visual da estrutura da rede, conforme será demonstrado na seção 5.3.

Um dos motivadores para a construção dessa ferramenta foi a necessidade do aluno possuir um computador com um bom desempenho, para virtualizar um ambiente de rede em sala de aula. O IfCloud propõe a dispensa dessa necessidade uma vez que todos os dispositivos virtuais criados pelo aluno estão na nuvem.

A ferramenta também cumpre o objetivo criando ambientes virtuais de forma fácil e rápida e consegue simular os serviços de rede como em uma situação real. Os testes realizados pelos desenvolvedores do sistema e pelos alunos em sala de aula mostraram que a ferramenta pode ser útil na criação de ambientes para aula, de maneira mais interativa e visual.

Para manter a interface funcional, foi necessário desenvolver o sistema utilizando uma arquitetura em que foi possível obter dados em tempo real do servidor, para dar um retorno visual ao aluno do estado das máquinas virtuais e do ambiente de rede. Ao final dos testes iniciais pode-se chegar a arquitetura, como mostra a Figura 3.

Figura 3 - Menu de Configuração do dispositivo virtual



Fonte: Autores, 2022

Também foram realizados testes em sala de aula com alunos da disciplina de Serviços de Rede no dia 08/12/2022, com o objetivo de utilizar a ferramenta para construir um ambiente de rede com serviços, como um servidor Apache, sistema de compartilhamento de arquivos entre as máquinas virtuais, firewall, dentre outros serviços de rede.

Com o resultado da avaliação do sistema, pode-se verificar que ele permite ao usuário criar, configurar e acompanhar o funcionamento de um ambiente com diversos dispositivos distintos, pertencentes a uma ou mais redes. Como o sistema proposto se trata de um sistema em nuvem, além da facilidade de criação, também permite que um aluno que não disponha de um hardware adequado para construção do mesmo ambiente em outra plataforma, consiga construir esse mesmo ambiente de forma mais simples e rápida.

O Openstack, embora tenha se mostrado muito eficiente no gerenciamento de múltiplas estruturas virtualizadas, alguns detalhes técnicos na integração do ambiente gráfico ao sistema precisam ser bem analisados. Algumas funcionalidades na interface gráfica, como um simples arrastar e soltar de um cabo virtual que liga uma máquina a um switch, desencadeia uma série de funções no lado do gerenciador da nuvem. Essas funções necessitam ser executadas em uma dada ordem para que tudo funcione corretamente. Por conta disso, a decisão de desenvolver um sistema intermediário entre a interface web e o Openstack foi uma saída para evitar problemas no sistema, uma vez que esse sistema intermediário orquestra todas as funções e abstrai um clique em várias operações no lado do servidor.

5.3 Testes e Aplicação do Ambiente em Sala

Como forma de aferir-se a satisfação dos objetivos propostos, os autores realizaram pesquisa envolvendo seis alunos do Curso Superior de Tecnologia em Redes de Computadores, do *Campus* Avançado Sombrio, no dia 08/12/2022. Esta pesquisa foi realizada após a utilização do sistema por parte dos usuários e é constituída de um questionário composto de 11 questões, sendo 10 com respostas avaliativas de 0 a 5, em que 0 corresponde a completamente insatisfeito e 5 completamente satisfeito, uma questão com nota de 0 a 10 e, por fim, apresenta-se uma questão descritiva de sugestão de melhoria.

Conforme os resultados presentes na Tabela 1, concluiu-se que o sistema é capaz de simular uma rede simples de computadores para auxiliar os alunos na construção de ambientes virtuais para experimentação de serviços de rede,conforme os objetivos previamente definidos,

Tabela 1 - Resultados do Questionário

Questão	Nota Média
O usuário ficou satisfeito com a interface do sistema?	4,8
Facilidade em aprender a utilizar o software?	4,5
Uma vez que aprendido a usar o software, o usuário consegue ser produtivo?	4,5

O objeto virtual de aprendizagem simula bem a realidade?	4,6
O software oferece as funções necessárias para a realização das tarefas que o usuário precisa executar?	4,5
O objeto virtual de aprendizagem estimula o aprendizado?	5
O usuário tem acesso remoto a utilização do emulador de rede?	4,8
Este objeto de aprendizado virtual beneficia a aprendizagem no IFC Campus Avançado Sombrio?	4.8
Como você avaliaria a experiência aluno/professor durante o uso da ferramenta?	9.3

Fonte: Os Autores, 2022.

Ao serem questionados sobre possíveis melhorias, os alunos relataram a falta da virtualização de sistemas de roteadores e switches como IOS da Cisco ou RouterOS da Mikrotik, pois o roteador disponível no catálogo de dispositivos do sistema é um roteador simulado pelo Openstack, que possibilita a simulação do ambiente, mas limita os protocolos de camada 2 ao gerenciador de redes do Openstack que fornece serviços de rede em camada 3. Mais detalhes em relação a este tópico serão debatidos na seção de considerações finais.

6. Considerações Finais

Este trabalho teve como objetivo construir um sistema que auxiliasse os professores e alunos do curso de Redes de Computadores do Instituto Federal Catarinense com as atividades práticas, que requerem a construção, instalação e teste de diferentes sistemas e serviços de redes em ambientes virtuais, o que ocasiona problemas de compatibilidade e muitas vezes falta do hardware necessário para execução dessas atividades.

Para a conclusão deste propósito, levou-se a efeito uma pesquisa tecnológica, apoiada pela metodologia DSRM, desenvolvendo-se a ferramenta que realiza a simulação de rede com propósitos didáticos.

Após testes no sistema, pode-se concluir que ele cumpre com os objetivos propostos, tornando mais rápido a construção de um ambiente virtual para a realização de testes de serviços de redes, deixando as aulas mais dinâmicas e possibilitando que professores de diversas matérias possam realizar atividades práticas com os alunos.

Uma vez que todo ambiente pode ser construído em uma interface gráfica de fácil uso, e a demanda por processamento fica por conta da nuvem, o aluno não tem mais problemas de compatibilidade com software ou falta de hardware.

O Openstack mostrou-se eficiente para execução de máquinas virtuais e ambientes de rede e como se pode observar, a interface gráfica do sistema simplificou a criação de um ambiente virtual, onde diversos serviços de rede estão disponíveis para simular uma rede de computadores.

O professor tem controle sobre o sistema, podendo inspecionar os ambientes criados por seus alunos a qualquer momento. O aluno só tem acesso ao sistema através do professor, que cria a conta do aluno e pode a qualquer momento retirar ou

restringir o acesso dos usuários a determinadas funções do sistema.

O sistema testado se mostrou seguro, uma vez que utiliza a autenticação presente no próprio OpenStack, garantindo que não haja acessos não autorizados ao sistema de computação na nuvem privada do Instituto Federal Catarinense *Campus* Avançado Sombrio.

Um dos principais desafios encontrados foi gerenciar redes em camada 2 utilizando o OpenStack, o que não tornou possível a emulação de sistemas de roteadores, como o IOS da Cisco e o RouterOS da Mikrotik, pois protocolos de camada 2, como o DHCP, em dispositivos virtualizados, não funcionaram como o esperado devido ao OpenStack gerenciar toda a rede em camada 3.

Sendo assim, para trabalhos futuros, os autores sugerem pesquisar por tecnologias para o gerenciamento de redes de camada 2, como o Open Switch, para integrá-las ao sistema e, assim, fazer com que a simulação do ambiente fique mais próxima do real, podendo assim emular sistemas de roteadores e switches que possuem protocolos operantes na camada 2, em adição com a realização de testes com uma quantidade maior de usuários simultâneos.

7. Referências

CARISSIMI, Alexandre. Virtualização: da teoria a soluções. **26º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**, [s. l.], 2008. Disponível em: https://jvasconcellos.com.br/wp-content/uploads/2012/01/cap4-v2.pdf. Acesso em: 5 dez. 2022.

FILIPPETTI, Marco Aurélio. **Uma arquitetura para a construção de laboratórios híbridos de redes de computadores remotamente acessíveis.** 2008. 129 p. Dissertação (Mestrado) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, [S. l.], 208. Ebook (129 p.).

ISOPPO, Karine Teixeira et al. **Utilização de emuladores e simuladores como suporte no ensino-aprendizagem de redes de computadores.** Tecnologia e Redes de Computadores, [s. l.], ed. 4, 2018. Ebook (344 p.).

NODE.JS. About Node.js®. In: **Node.js.** [S. l.], 2022. Disponível em: https://nodejs.org/en/about/. Acesso em: 30 nov. 2022.

OPENSTACK.ORG. Openstack. In: **What is Openstack?**. [S. l.], 2022. Disponível em: https://www.openstack.org/software/. Acesso em: 30 nov. 2022.

OPENSTACK.ORG. DevStack. In: DevStack. [S. l.], 2022. Disponível em: https://docs.openstack.org/devstack/latest/. Acesso em: 30 nov. 2022.

PINHEIRO, Ricardo Paranhos. A Utilização De Simulação no Ensino De Redes De Computadores. **Revista de Extensão Guará**, [s. l.], ed. 13, p. 90 -101, 11 mar. 2022. DOI https://doi.org/10.30712/guara.v1i13.21175. Disponível em: https://periodicos.ufes.br/guara/article/view/21175. Acesso em: 22 ago. 2022.

REACT. React. In: React. [S. l.], 2022. Disponível em: https://pt-br.reactjs.org. Acesso em: 30 nov. 2022.

SANTOS, Walter dos; CARDOSO, Ana Maria Pereira. **Uso De Simuladores Como Ferramenta No Ensino E Aprendizagem De Redes De Computadores Em Um Novo Modelo De Ensino**. 2016. Dissertação (Mestrado) - UNIVERSIDADE FUMEC, [S. l.], 2016. Disponível em: https://repositorio.fumec.br/xmlui/handle/123456789/407. Acesso em: 25 ago. 2022.

SANTOS, Jair Vargas dos; SOUZA, Marco Antônio Silveira De; ANDERLE, Daniel Fernando. **Controlando Dispositivos em Tempo Real Através do WebSocket.** Tecnologia e Redes de Computadores: Estudos Aplicados, [s. l.], ed. 1, 2015. Ebook (231 p.).

Implementação do Zabbix para gerência de redes de um provedor de internet

Guilherme Lucas Barbosa[1], João Vitor Dagostin Ghellere[2], Jéferson Mendonça de Limas[3]

[1, 2,] Acadêmicos do Instituto Federal Catarinense – Campus Avançado Sombrio – 88960000 – Sombrio – SC – Brasil

[3] Docente do Instituto Federal Catarinense – Campus Avançado Sombrio – 88960000 – Sombrio – SC – Brasil

{guilhermelucasbarbosa@gmail.com, joaovitordg@hotmail.com, jeferson.limas@ifc.edu.br}

Abstract: *In this study a network monitoring environment was built using the Zabbix tool to demonstrate its operation and the solution of a network problem actively. The goal is to demonstrate in a practical way a bandwidth problem using the SNMP protocol. For this a monitoring environment was built in an internet provider in the city of Jacinto Machado in the state of Santa Catarina in order to demonstrate the importance of monitoring computer networks and offer quality bandwidth actively through an open source tool. In the following sections are described the bandwidth problems encountered, followed by a solution in the field and monitoring after the exchange of network equipment for certification of complete solution of the problem.*

Resumo: *Neste estudo construiu-se um ambiente de monitoramento de redes utilizando a ferramenta Zabbix para demonstrar seu funcionamento e a solução de um problema de rede de forma ativa. O objetivo é demonstrar de forma prática um problema*

de largura de banda utilizando o protocolo SNMP. Para isso construímos este ambiente de monitoramento em um provedor de internet da cidade de Jacinto Machado no estado de Santa Catarina com a finalidade de demonstrar a importância do monitoramento de redes de computadores e oferecer qualidade da largura de banda de forma ativa através de uma ferramenta open source. Nas seções seguintes são descritos os problemas de largura de banda encontrados, seguindo de uma solução em campo e monitoramento após a troca de equipamentos de rede para certificação de solução completa do problema.

1. Introdução

Os provedores de internet ISPs (*Internet Service Provider*) estão em constante crescimento e buscam apresentar soluções tecnológicas e inovadoras para seus consumidores. Szapiro (2007), afirma que o setor de telecomunicações passou por um amplo processo de reestruturação internacional a partir da década de 1980 e que as inovações tecnológicas obrigaram a diversas alterações na organização das atividades.

Szapiro (2007), salienta que a indústria de telecomunicações desenvolveu grandes inovações do setor até a década de 1990, através dos laboratórios técnicos. Atualmente, embora as empresas fornecedoras estejam desempenhando um papel de destaque no processo de inovação da indústria de telecomunicações, as operadoras, e mais especificamente, os seus laboratórios, continuam exercendo uma função fundamental no processo de evolução tecnológica das telecomunicações e da qualidade do atendimento do serviço.

Segundo o blog da CCN Telecom, em um artigo publicado em 08 de agosto de 2019, a estrutura interna de um provedor de internet ISPs (*Internet Service Provider*) é o ponto

determinante entre o sucesso e o fracasso da organização e aponta que é necessário investir tempo e recursos no planejamento, para que o crescimento seja constante.

Diante disso, entende-se que os laboratórios das operações de serviços, normalmente conhecidas como centro de comando e controle, em inglês *network operations center*, podem ser definidos como o núcleo de um ISP e é parte essencial da construção de inovação dentro da empresa.

Szapiro (2007), ressalta a importância da diversificação tecnológica utilizada pelos ISPs para que a competitividade da indústria seja mantida e da importância da evolução tecnológica para a evolução constante e maior bem-estar da sociedade como um todo.

Neste contexto, este projeto tem como objetivo apresentar uma ferramenta tecnológica para monitoramento de rede e demonstrar a aplicação prática em um provedor de internet da região do extremo sul de Santa Catarina (SC) identificando possíveis excessos de uso nos recursos, tais como, alto uso de processamento (CPU) e tráfego de rede (largura de banda). Pretende-se, também, detalhar a análise do monitoramento para solução de problemas e, consequentemente, a melhoria do serviço de internet oferecido pelo provedor aos seus consumidores finais.

Esta pesquisa busca evidenciar a importância de utilização de ferramentas de monitoramento para melhoria de qualidade da rede.

Considera-se essencial conhecer ferramentas que auxiliem a gerência de forma ativa, ou seja, sem que os consumidores precisem entrar em contato com o suporte técnico da empresa para que o problema seja identificado.

As seções a seguir detalham o referencial teórico do artigo; os materiais e métodos utilizados para realização deste

projeto; os resultados e problemas encontrados no andamento da implementação e análise da ferramenta; considerações finais e as referências bibliográficas.

2. Referencial Teórico

Nesta seção será descrito o referencial teórico do desenvolvimento deste projeto, tal como a definição de gerência de redes, a importância de monitoramento de rede nos provedores de internet (ISPs), os conceitos básicos dos protocolos de redes utilizados para gerenciar redes de computadores e demais conceitos básicos que foram utilizados no desenvolvimento desse estudo.

2.1 Provedores de internet no extremo sul catarinense

Na região do extremo sul de santa Catarina identificou-se diversos provedores de internet locais (ISPs), totalizando uma quantidade aproximada de 20 provedores locais que podem utilizar deste estudo para melhorar a qualidade da rede a seus consumidores ao utilizar uma ferramenta open source, conhecida como Zabbix.

2.2 Gerência de Redes

Segundo Xavier, Koch e Westphall (2002), o principal objetivo da gerência de redes de computadores é prover qualidade de serviços das aplicações que requerem o uso da estrutura da rede. Para Black (2008), a partir do gerenciamento é possível ter controle dos recursos da rede, além de permitir a identificação e prevenção de problemas.

O crescimento dos serviços oferecidos por diversas empresas, destacando-se o setor de telecomunicações, teve muito crescimento na última década. Em um relatório anual apontado pela Anatel em 2004, afirma-se que o crescimento do mercado de telecomunicações representa, para o Brasil, a modernização da economia da informação. Abrange o

desenvolvimento de equipamentos e disseminação do conhecimento e de utilização de informações.

Evidenciou-se no relatório anual de 2004 pela Anatel (Agência nacional de telecomunicações), a crescente da geração de empregos no setor de telecomunicações com um percentual de 8,4% em 2003 e 16,8% em 2004, ou seja, representando um crescimento significativo ao Brasil neste mercado tecnológico.

No relatório anual de 2008, apresentado pela Anatel, demonstra-se que o uso de banda larga fixa em 2018 teve 31,18 milhões de acessos.

Black (2008), demonstra em seus estudos que a expansão dos dispositivos na rede que possuem o recurso de serem gerenciados, se fez necessário o uso de softwares específicos para realizar a gerência de redes através de protocolos de comunicação.

Diante do crescimento deste mercado, destaca-se na seção a seguir a importância de monitorar as redes em empresas de telecomunicações.

2.3 A importância de monitoramento nos provedores de internet (ISPS)

Monitoramento pode ser definido como um acompanhamento contínuo e periódico de alguma atividade específica. Ele é realizado por meio da coleta e análise e está presente na grande maioria das gerências de redes atuais.

De acordo com Bueno (2012), define-se gerência de rede como um conjunto de ferramentas compostas por hardware e software, que permite a geração de dados históricos e estatísticos com o objetivo de identificar possíveis falhas ou indisponibilidades.

Atualmente, os modelos de gerências de rede utilizam em grande parte o protocolo SNMP (Seção 2.5), que cresceu em larga escala no cenário mundial.

De acordo com Black (2008), uma rede de computadores, por menor e mais simples que seja, necessita de um gerenciamento com o objetivo de assegurar a disponibilidade de serviços em grau satisfatório. Sendo assim, com a evolução no número de dispositivos que utilizam os serviços e sistemas da rede, tornou-se comum utilizar os sistemas de gerência.

Com a recorrente expansão das redes, a complexidade de seu gerenciamento aumentou, logo, adotar ferramentas de gerenciamento tornou-se indispensável para o monitoramento e controle.

Neste contexto, observa-se a importância de estudar e aplicar a gerência de redes em uma empresa de telecomunicações e demonstrar os resultados obtidos com o monitoramento de redes através de protocolos de comunicação padronizados.

2.4 Principais Ferramentas de Monitoramento

Em tecnologia, existem diversas alternativas para diferentes serviços e funções. No monitoramento de redes, encontramos algumas aplicações bastante difundidas, tanto aplicações open source quanto aplicações proprietárias. Alguns exemplos de ferramentas para monitoramento são o Cacti, Nagios, PRTG, The Dude e Zabbix.

2.4.1 Cacti

Segundo o grupo Cacti (2020):

> “O Cacti é uma interface completa do RRDTool, ele armazena todas as informações necessárias para criar gráficos e preenchê-los com dados em um banco de dados MySQL.”

2.4.2 Nagios

Segundo o site Nagios.org (2020), o Nagios é um sistema de monitoramento completo para identificar e resolver problemas de infraestrutura de TI, oferecer monitoramento, notificações, planejamentos e manutenção.

2.4.3 PRTG

Ferramenta proprietário disponibilizada comercialmente com preços diferentes e versão gratuita com recursos limitados. O PRTG oferece monitoramento de diversos tipos de infraestrutura, protocolos e serviços de rede. Segundo o site oficial Paessler (2020), tudo é incluído no PRTG e não precisa de plugins ou downloads adicionais, diante disso a solução exige menos expertise da equipe de TI.

2.4.4 The Dude

O The Dude é um software disponibilizado pela Mikrotik. Segundo a empresa, a aplicação serve para monitoramento de rede dos equipamentos da Mikrotik e oferece uma plataforma para desenhar os dispositivos, monitorar serviços de rede e criar alertas.

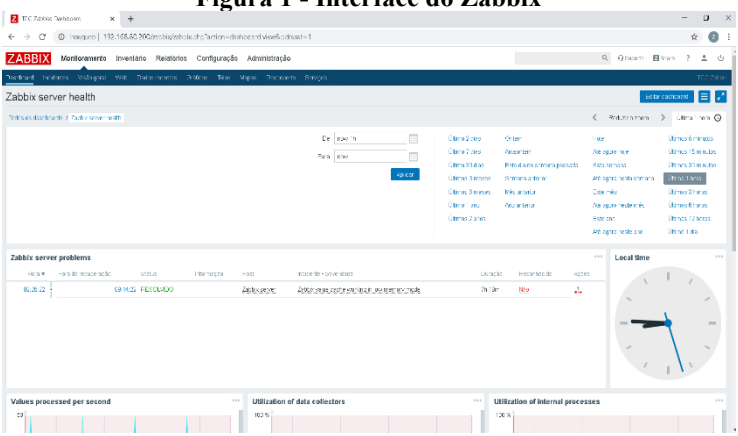
Alguns recursos segundo o site são:

- Autodescoberta de rede
- Ícones em formato .svg
- Fácil instalação e uso
- Suporte a protocolos SNMP, ICMP, DNS.

2.4.5 Ferramenta Zabbix

Atualmente mantido e suportado pela Zabbix SIA, o Zabbix é uma solução de código aberto (open source), com suporte a monitoramento distribuído. Tem como função monitorar parâmetros de rede, servidores (hosts) e demais componentes de uma rede de computadores. Isso torna o Zabbix uma ferramenta completa que oferece a possibilidade de planejamento de capacidade de uma rede. Através desta aplicação é possível configurar e-mails para eventos que aconteçam na rede que está sendo monitorada (Zabbix, 2020).

Figura 1 - Interface do Zabbix



Fonte: Autores (2020)

Criado em 1998 por Alexei Vladischev, após um descontentamento com os softwares de monitoramento que trabalhava na época em um banco na Letônia, surgiu a ideia de criar o Zabbix. A primeira versão foi lançada em 2001 com a licença sob a GL e, apenas em 2004, foi lançada a versão mais estável do Zabbix.

Em 2005, houve a necessidade de criar a empresa Zabbix SIA para profissionalizar a ferramenta e dar andamento no desenvolvimento da aplicação. A figura 1 mostra a interface principal do Zabbix sendo executado em um servidor de aplicações.

Através do protocolo SNMP, citado anteriormente, o Zabbix possui a capacidade de monitorar milhares de itens em uma plataforma, possibilitando a aplicação de monitoramento distribuído. Dessa forma, é possível ter um servidor central de monitoramento e vários outros servidores subordinados a ele enviando métricas para o servidor central ou apenas replicar as informações. (LIMA, 2014, p.6)

Conforme LIMA (2014), o Zabbix pode ser dividido em 3 elementos, que são:

- **Zabbix Server:** coleta as informações de todos agentes e armazena em um banco de dados, que é possível visualização através da interface web.
- **Zabbix Proxy:** elemento opcional, Zabbix server não depende dele para funcionar. É um agregador de dados que faz a coleta nos agentes na rede remota. Após a coleta, consolida esses dados e transmite um pacote contendo todos os dados para o Zabbix Server.
- **Zabbix Agent:** criado para consumir pouco hardware e não afetar o uso do cliente, Zabbix Agent envia os dados para o Zabbix Server ou Zabbix Pro.

A documentação completa do Zabbix pode ser acessada no seguinte endereço:

https://www.zabbix.com/documentation/3.0/pt/start

2.5 Protocolo SNMP

O protocolo simples de gerenciamento de rede, SNMP (*Simple Network Management Protocol*) foi criado em agosto de 1988 e definido na RFC 1067. Atualmente é um dos principais protocolos usados para o gerenciamento e monitoramentos de dispositivos IP. O gerenciamento de redes baseia-se na função de controlar os recursos, analisar os resultados e tomar decisão para correção de possíveis falhas nas redes, fazendo com que essas se mantenham estáveis e funcionais (Mauro e Schmidt, 2001).

Com o crescimento das redes de computadores, o protocolo SNMP necessitou se adequar à questões de gestão de grandes redes, desenvolvimento de melhorias de segurança e de desempenho para obtenção de melhores resultados no gerenciamento de redes maiores (Pinheiro, 2002).

Mauro e Schmidt (2001) apontam as vantagens que SNMP oferece aos usuários, com um conjunto simples de operações (e das informações obtidas por essas operações) que permitem o gerenciamento remoto dos dispositivos, oferecendo ao administrador a possibilidade de monitorar a velocidade de uma interface, qual a temperatura de dispositivos, qual a porcentagem de uso da unidade central de processamento ou Central Processing Unit (CPU), notificando possíveis falhas aos administradores de redes.

Segundo Stallings (2005), o protocolo SNMP é composto por quatro componentes básicos, que são: gerente; agente; protocolo de gerenciamento de rede e base de informações e gerenciamento (MIB);

O protocolo SNMP é o responsável por executar a comunicação entre os componentes básicos, conhecido por Stallings como protocolo de gerenciamento de rede.

Nas subseções a seguir, define-se cada um dos componentes básicos utilizados em uma gerência através do protocolo SNMP.

2.5.1 Gerente

O gerente (NMS – *Network Management Station*) tem como responsabilidade uma única operação ou várias operações de gerenciamento de redes. Mauro e Schmidt (2001), demonstram em seus estudos que o gerente (NMS) é responsável pela operação de *polling* e por receber *traps* de agentes na rede.

Uma *poll*, segundo Mauro e Schmidt (2001), é a parte do software executada nos dispositivos da rede que podem ser gerenciados pelo administrador.

Mauro e Schmidt (2001) também definem *traps* como uma forma de notificar o gerente (NMS) enviando *traps* para ele, informando sobre atualizações de dados. Por exemplo, uma *trap* conhecida como *"all clear"* demonstra que um estado de defeito foi alterado para um estado correto.

2.5.2 Agente

Mauro e Schmidt (2001), definem o agente como um software que controla todas as comunicações de SNMP com e de qualquer dispositivo compatível com o protocolo. Existem variações de agentes, alguns podem ser básicos e retornar um limite de informações, outros, no entanto, podem trazer informações mais detalhadas dos dispositivos.

2.5.3 Base de Informações e Gerenciamento (MIB)

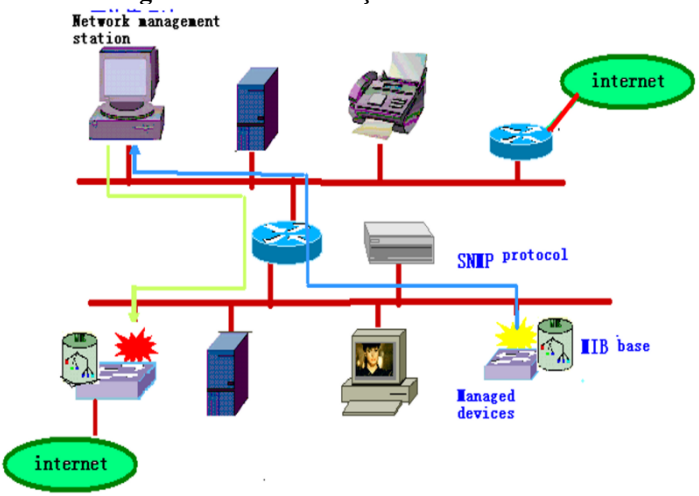
A MIB é definida por Mauro e Schmidt (2001) como um banco de dados de objetos gerenciados que o agente rastreia e informa o NMS (*Network Management System*) através de traps. Informações diversas dos dispositivos são definidas pela MIB (*Management Information Base* ou Base de informações e gerenciamento).

2.5.4 Demonstração Gráfica do Protocolo SNMP

A figura abaixo demonstra o funcionamento do protocolo SNMP e ilustra os componentes básicos definidos nas seções anteriores deste estudo. O gerente é demonstrado na figura 2 como o *Network Management Station*, ou seja, a estação host[1] responsável por gerenciar o recebimento de informações através do Protocolo de Gerenciamento de Rede, na imagem definido por SNMP Protocol.

O dispositivo da figura definido como *Managed devices*, refere-se aos agentes definidos anteriormente e o local que guarda as informações para serem transmitidas é identificado na figura 02 como a *MIB Base,* definida na seção 2.3.4 deste estudo como base de informações e gerenciamento.

Figura 2 - Demonstração Gráfica do SNMP



Fonte: Google Imagens

[1]Qualquer máquina ou computador conectado a uma rede, podendo oferecer informações, recursos, serviços e aplicações aos usuários ou outros nós na rede.

2.6 Versões do Protocolo SNMP

O protocolo SNMP atualmente possui 3 versões. O SNMPv1 está definido na seção 2.3 deste artigo. As versões desenvolvidas posteriormente são detalhadas nas subseções a seguir.

2.6.1 SNMPv2

O padrão SNMPv2 (*Simple Network Management Protocol* version 2), foi publicado em abril de 1993 pela IETF (Internet Engineering Task Force), grupo internacional aberto que desenvolve padrões para internet. Essa revisão trouxe grandes avanços relacionados ao protocolo SNMPv1.

2.6.2 SNMPv3

De acordo com os estudos de Mauro e Schmidt (2001), a segurança do protocolo SNMP sempre foi considerada um ponto fraco. A autenticação nas versões 1 e 2 do SNMP são através de senhas básicas.

A versão 3 do SNMP busca lidar com os problemas de segurança das versões anteriores. Mauro e Schmidt (2001), reiteram que nesta versão não foram realizadas alterações em funções que não sejam relacionadas à segurança. Explicam que nesta versão os gerentes e agentes são tratados como entidades visando a melhoria de segurança.

2.7 Virtualização

Atualmente existem diversas definições do conceito de virtualização. Singh (2004), define em suas pesquisas uma introdução do que é virtualização. Ele afirma que virtualização é um framework ou metodologia para dividir os recursos de um computador em múltiplos ambientes de execução com possibilidade de simular completamente ou parcialmente uma máquina.

De maneira simplificada, virtualização pode ser definida como uma técnica que permite dividir um sistema operacional em diversos sistemas. Cada um desses sistemas é capaz de oferecer um ambiente distinto, denominado de máquina virtual (CARISSIMI, 2008).

2.8 Software Open Source

De acordo com o site *CanalTech* (2020), Open source é um termo em inglês que significa código aberto. Essas aplicações não possuem custo de licença e oferecem oportunidades de utilização gratuita com o objetivo de desenvolver maiores investimentos em TI.

Segundo o artigo publicado pelo *CanalTech*, existem alguns pontos importantes para definir se um software é open source, entre eles, estão a disponibilização gratuita da aplicação, disponibilização do código fonte à comunidade e alguns outros tópicos relacionados à licença da aplicação.

A ferramenta Zabbix, utilizada neste estudo, é considerada uma ferramenta open source diante dos termos apresentados.

2.8.1 Debian

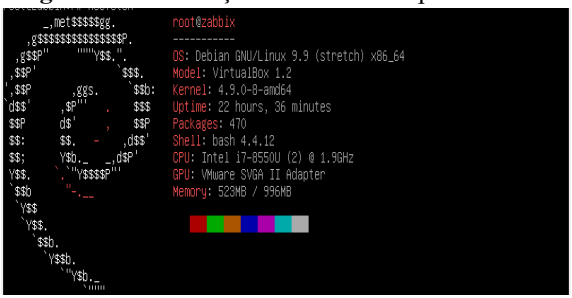
As seções anteriores mostraram conceitos básicos do que foi apresentado neste estudo. A presente seção busca definir o sistema operacional utilizado nos testes efetuados.

O sistema operacional utilizado nesta pesquisa foi o Debian, que também é considerado um software open source, ou seja, é distribuído gratuitamente para utilização em computadores de qualquer espécie.

De acordo com o site oficial, debian.org, o sistema operacional é (SO), é um sistema desenvolvido para executar em qualquer computador e provê um sistema operacional puro, com

mais de 59000 pacotes e um formato fácil de instalação.

Figura 3 - Informações do Sistema Operacional



Fonte: Autores (2020)

2.9 Estudos alternativos

No Instituto Federal Catarinense (IFC), foram apresentados alguns trabalhos relacionados ao tema deste estudo. Podemos citar o trabalho intitulado *Implementação da Ferramenta de Monitoramento de Redes Zabbix no Instituto Federal Catarinense Campus Avançado Sombrio,* desenvolvido pelos alunos Christopher Ramos dos Santos e Guilherme Rodrigues de Campos, com orientação dos professores Jeferson Mendonça de Limas e Marcos Henrique de Morais Golinelli. O estudo demonstra o monitoramento de dispositivos considerados essenciais no campus IFC utilizando o Zabbix e demonstra as demandas de rede através de gráficos para projetos de redes futuros.

3 Materiais e Métodos

Para a elaboração deste trabalho, foi realizada uma pesquisa bibliográfica em livros, artigos publicados e disponibilizados em sites da internet.

De acordo com Rauen (2015), a pesquisa pode ser definida como procedimentos aplicados na busca, apuração ou exploração tendo a finalidade de conhecimento em torno de um

fato ou fenômeno parcialmente ou desconhecido.

3.1 Ambiente de Pesquisa

A inicialização do desenvolvimento do projeto foi dada em sala de aula, com auxílio de uma rede simulada no Instituto Federal Catarinense – Campus Avançado Sombrio (IFC), onde foram efetuadas as instalações básicas, as configurações e alguns testes preliminares com o auxílio de um dos professores do curso.

Após a fase inicial desenvolvida no Instituto Federal, a aplicação prática foi realizada em um provedor do sul de Santa Catarina, localizado na cidade de Jacinto Machado – SC, com o objetivo de levantar informações reais e demonstrar neste estudo como a implementação de uma ferramenta de monitoramento pode auxiliar a gestão da rede de computadores em grande escala.

O provedor conta atualmente com 1850 clientes e possui planos de largura de banda de até 200 megabytes (Mb) na fibra óptica e 5 megabytes (Mb) em planos através de rede sem fio (rádio frequência). Aproximadamente 1100 clientes na fibra óptica e 750 clientes utilizando tecnologia de rádio frequência.

Possui 500 Mb de link de trânsito, mas não possui limite em apenas 500mb, possibilitando picos de uso de até 700mb e 2GB de CDN, Content Delivery Network (ou Rede de Distribuição de Conteúdo).

O provedor de internet atende as regiões de Jacinto Machado, Ermo, Turvo, Timbé do Sul e Araranguá. Todas as cidades estão localizadas em Santa Catarina.

Na infraestrutura de rede, o provedor possui aproximadamente 40 roteadores, na grande maioria da marca Mikrotik e aproximadamente 187 antenas em torres e repetições espalhadas pelas cidades citadas anteriormente, em sua grande maioria equipamentos da marca Ubiquiti.

O desenvolvimento do projeto foi realizado em ambiente virtualizado aplicado a uma rede de computadores de média escala. O sistema operacional utilizado foi o Debian 9 Stretch para a instalação e configuração do ZABBIX Server.

3.2 Compreensão do Problema

Para desenvolvimento deste estudo foram preparados os materiais e métodos detalhados nesta seção, buscando evidenciar o objetivo citado na introdução de aplicar o monitoramento em um ambiente real. E, também, demonstrar como a ferramenta de monitoramento de rede pode auxiliar a identificar problemas como os excessos de uso nos recursos. Por exemplo, o alto uso de processamento (CPU), tráfego de rede (largura de banda), a temperatura e apontar as soluções aplicadas e o resultado do antes e depois do monitoramento com o reparo realizado, caracterizando uma situação completa de identificação de problema, planejamento de solução, execução do ajuste e um pós acompanhamento para certificar a conclusão do problema de forma completa.

3.3 Implementação da Ferramenta

A criação do ambiente virtual foi realizada em um Notebook com as seguintes configurações:

- Marca: Lenovo;
- Processador: Intel Core i7 8 Gen.;
- Memória RAM: 8 GB;
- SSD: 480 GB;
- HDD: 1 TB;
- Sistema operacional: Windows 10 x64.

No sistema operacional Windows, foi criado o ambiente virtual utilizando o software Virtual Box Versão 6.0.4. De acordo com a Oracle (2020), o Virtual Box é uma das aplicações mais populares do mundo para criação de ambientes virtuais e permite que seja executado sistemas operacionais Windows, Linux, Mac

OS ou Oracle Solaris.

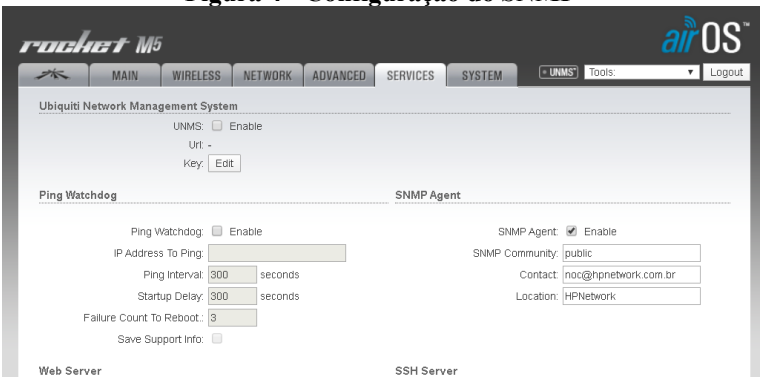
No ambiente virtual foi instalado o sistema operacional *Debian 9 Stretch* e instalado a ferramenta Zabbix na versão 4.2.1 disponibilizada no site https://www.zabbix.com/download

Para complementar a instalação do Zabbix, foi instalado as aplicações conhecidas como LAMP, ou seja, Linux, Apache, MySQL e PHP. Por definição, LAMP é uma combinação entre softwares livres e de código aberto (Wikipedia, 2020).

Como citado anteriormente, o protocolo SNMP faz a comunicação entre equipamentos gerente e agentes, neste caso foi necessário habilitar e configurar o protocolo SNMP nos equipamentos de rádio para que fosse possível a conversação entre servidor Zabbix e os equipamentos.

A figura 4 demonstra como é feita a configuração do protocolo SNMP em equipamentos de rádio Rocket M5, da marca Ubiquiti. O sistema operacional destes equipamentos é o AirOS, um sistema operacional proprietário da marca Ubiquiti (UBNT, 2020).

Figura 4 - Configuração do SNMP



Fonte: Autores (2020)

Através das informações inseridas nos dispositivos de rede, o Zabbix pode visualizá-los e acompanhar o desempenho em tempo real e com este monitoramento pode avisar os administradores das ações que estão acontecendo na rede.

Neste contexto, foi configurado para disparar um e-mail aos administradores, demonstrado na imagem como *joaovitordg,* quando a capacidade de largura de banda atingir 95% de tráfego.

A figura 5 demonstra o e-mail enviado automaticamente pelo servidor Zabbix ao ser acionada a trigger[2] de alto uso de largura de banda, ou seja, foi configurado no servidor Zabbix uma trigger (gatilho), e através deste gatilho é possível configurar a ferramenta para tomar certas decisões de forma automática.

[2]Alarme acionado em serviços de redes ou aplicações para efetuar alguma ação de forma automática.

Figura 5 - E-mail de alerta

Fonte: Autores (2020)

O email da figura 5 é disparado utilizando as configurações de SMTP aplicadas ao servidor Zabbix, ou seja, a aplicação permite que seja configurado um servidor SMTP (Send Mail Transfer Protocol) responsável por fazer o envio de mensagens aos destinos configuradas no gatilho *(trigger)*.

A configuração da conta de e-mail utilizada pelo SMTP para avisar os administradores de rede por mensagem é configurada na aplicação e com os ajustes citados nessa seção será possível evidenciar os resultados obtidos para solucionar o problema proposto neste estudo. Na seção a seguir demonstra-se os resultados e discussões do projeto.

4 Resultados e discussões

Esta seção exibe os resultados obtidos após a utilização dos métodos e das ferramentas citadas anteriormente.

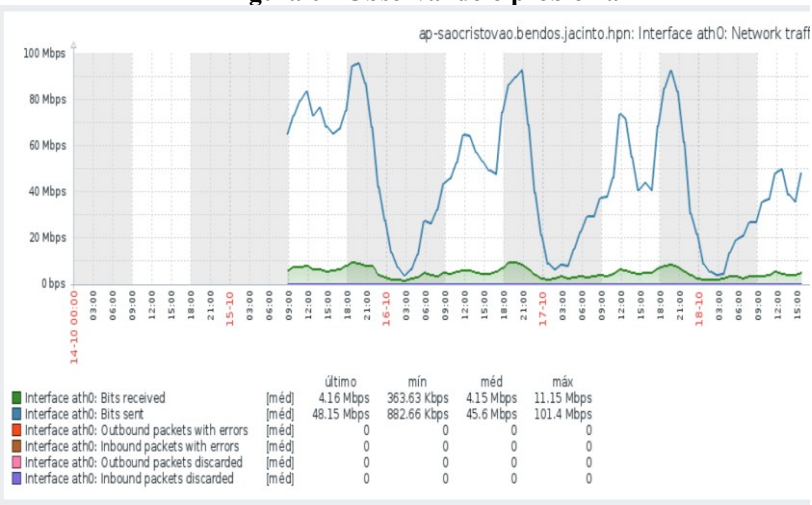
Para evidenciar um problema de largura de banda com a ferramenta Zabbix foi efetuado uma conexão de rede Wireless com antenas Rocket M5, da marca Ubiquiti. Após a configuração inicial do Zabbix, a criação da *trigger e a* configuração do servidor SMTP (responsável pelo envio de email), foi necessário monitorar a largura de banda da conexão Wireless durante alguns dias para que a ferramenta efetue a

criação de gráficos de monitoramento e possibilite identificar possíveis problemas a serem solucionados.

Em alguns dias, deixou-se o servidor configurado em um notebook fazendo o monitoramento do link e acompanhando como a largura de banda se comportava nessa conexão de rede. Foi constatado que o tráfego, em alguns momentos do período da noite, alcançava mais do que 90% da capacidade de transmissão dos equipamentos de rádio.

Observe na figura 6 que a quantidade máxima atingida neste gráfico foi de 101.4Mbps, ou seja, a conexão entre os equipamentos de rádio analisados estava alcançando o limite no período da noite.

Figura 6 - Observando o problema



Fonte: Autores (2020)

Ao monitorar a largura de banda, também foi possível acompanhar outras informações através do protocolo SNMP, tais como a temperatura e o uso de processador dos equipamentos responsáveis pelo roteamento da rede. As imagens abaixo, figura 7, figura 8 e figura 9, detalham os dados obtidos através do Zabbix.

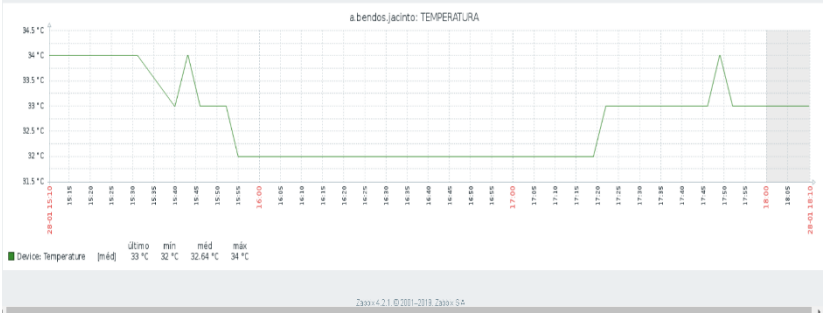
Os gráficos detalham o uso de CPU e de temperatura, respectivamente, do roteador com o nome de **“a.bendos.jacinto”.**

Figura 7 - Monitoramento do Roteador

Fonte: Autores (2020)

Na imagem acima, constatou-se no período analisado, que o roteador utilizou no máximo 29% de processamento, evidenciando que não é necessária nenhuma ação em relação a este equipamento.

Figura 8 - Monitoramento do Roteador



Fonte: Autores (2020).

A figura 8 demonstra que a temperatura máxima alcançada pelo roteador foi de 34°C, evidenciando também que não é necessária nenhuma ação preventiva em relação a este equipamento.

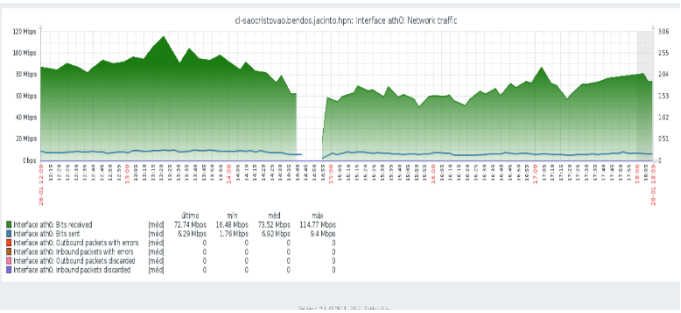
Diante destes gráficos, podemos afirmar que a largura de banda está sendo limitada nos equipamentos de conexão sem fio, devido a porta ethernet possuir velocidade máxima de conexão de 100Mbps, ou seja, não permite uma largura de banda maior que 100Mbps em sua porta de comunicação de rede.

Para solução deste problema, foi necessário efetuar a troca dos equipamentos de rádios Rocket M5 por outros dois (2) equipamentos chamados de Rocket AC, da marca Ubiquiti (UBNT) e que possuem interface de rede com conexão a 1000Mps, permitindo tráfego de rede até 1gb.

Após efetuar a troca em campo e fazer a conexão wireless ficar estabilizada, a conexão foi novamente monitorada com o servidor desenvolvido neste estudo, com o objetivo de certificar a solução completa do problema evidenciado nas figuras anteriores.

A figura 9 apresenta os dados obtidos no monitoramento executado após a troca dos equipamentos da conexão sem fio. Através deste gráfico, é possível observar que o limite de 95% não foi encontrado, ou seja, o problema foi resolvido com êxito.

Figura 9 - Monitoramento de Largura de Banda



Fonte: Autores (2020).

Esta seção buscou demonstrar como o monitoramento de rede pode antecipar problemas e solucioná-los de forma assertiva. A seção a seguir apresenta as considerações finais e o que foi alcançado com este estudo.

5. Considerações finais

O setor de telecomunicações está em constante crescimento e busca apresentar soluções tecnológicas e inovadoras para seus consumidores em qualquer lugar do mundo.

Szapiro (2007), afirma que o setor de telecomunicações passou por um amplo processo de reestruturação internacional a partir da década de 1980 e reforça que a indústria de telecomunicações desenvolveu grandes inovações do setor até a década de 1990.

No entanto, o autor também ressalta a importância da diversificação tecnológica utilizada pelos ISPs para que a competitividade da indústria seja mantida e da importância da evolução tecnológica para a evolução constante.

Diante deste contexto, o presente estudo buscou aplicar uma ferramenta de monitoramento de rede e demonstrar a aplicação prática em um provedor de internet da região do extremo sul de Santa Catarina (SC) com a implementação detalhada nas seções deste estudo. Observamos que a identificação de problemas em redes é facilitada quando utiliza-se uma ferramenta de gerência de redes através da comunicação SNMP.

Pode-se afirmar que a evolução tecnológica dos dias de hoje certamente permite que a qualidade seja determinada pela utilização de ferramentas auxiliares, como por exemplo a ferramenta Zabbix, demonstrada nesta pesquisa.

Para realização deste trabalho, encontramos alguns problemas relacionados à pesquisa acadêmica. Através de pesquisas bibliográficas e em artigos disponibilizados na rede mundial de computadores (internet) verificou-se que os conteúdos são mais técnicos e, às vezes, pode-se mostrar definições vagas por falta de conteúdo para pesquisa.

Na aplicação da ferramenta constatou-se problemas comuns na aplicação Zabbix que necessitavam alguns ajustes na memória cache para que a aplicação não apresentasse instabilidade de operação.

Para trabalhos futuros, sugere-se o desenvolvimento de pesquisas para o monitoramento completo de uma rede de um provedor, incluindo antenas de clientes, energia/bateria de nobreaks e diversos dispositivos de rede com objetivo de efetivar a utilização do Zabbix como ferramenta central de gestão de rede.

6. Referências

ABNT-Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, ABNT, 2005.

AG, Paessler. About PRTG. 2020. Disponível em: https://www.br.paessler.com/prtg. Acesso em: 18 maio 2020.

AIROS: Operating System for Ubiquiti. Operating System for Ubiquiti. User guide. Disponível em: https://dl.ubnt.com/guides/airOS/airOS_UG.pdf. Acesso em: 15 maio 2020.

A simple Network Management Protocol. Disponível em: https://tools.ietf.org/html/rfc1067#section-5. Acesso em 27 de janeiro de 2020.

BUENO, Edimilson Moreira. MONITORAMENTO DE REDES DE COMPUTADORES COM USO DE FERRAMENTAS DE SOFTWARE LIVRE. 2012. 73 f. Monografia (Especialização) - Curso de Especialista em Software Livre Aplicado A Telemática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, 2012.

BLACK, T. L. Comparação de Ferramentas de Gerenciamento de Redes. Instituto de Informática da Universidade Federal do Rio Grande do Sul (INF - UFGRS) - Porto Alegre, 2008. Disponível em: https://www.lume.ufrgs.br/handle/10183/15986. Acesso em: 14 jul. 2019.

CARISSIMI, Alexandre. Virtualização: da teoria a soluções. 26ʃ Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, Porto Alegre, p.174-207, maio 2008.

DEBIAN. About Debian. 2020. Disponível em: https://www.debian.org/intro/about. Acesso em: 18 maio 2020.

GROUP, Cacti. What is Cacti? 2020. Site Oficial. Disponível em: https://www.cacti.net/what_is_cacti.php. Acesso em: 18 maio 2020.

INC., Ubiquiti. Ubiquiti Rocket AC. 2020. Site Oficial. Disponível em:

https://www.ui.com/airmax/rocket-ac/. Acesso em: 18 maio 2020.

LIMA, Janssen dos Reis. Monitoramento de redes com Zabbix: monitore a saúde dos servidores e equipamentos de rede. Rio de Janeiro: Braspor, 2014.

MAURO, Douglas R. SCHMIDT, Kevin J. SNMP Essencial: ajuda para os administradores de sistemas e redes. Elsevier Editora, 2001.

Mercado das Telecomunicações. Disponível em: https://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?null&filtro=1&documentoPath=biblioteca/Publicacao/relatorios/relatorio_pdf/mercado_telecom.pdf Acesso em 27 de janeiro de 2020.

MIKROTIK. The Dude: software. Software. 2020. Site Oficial. Disponível em: https://mikrotik.com/thedude. Acesso em: 18 maio 2020.

MOCELIN, Daniel Gustavo; BARCELOS, Régis Leonardo Gusmão. TECNOLOGIA, COMPETITIVIDADE E REGULAÇÃO: a estruturação do mercado das telecomunicações no brasil.: a estruturação do mercado das telecomunicações no Brasil. Caderno Crh, Salvador, v. 25, n. 66, p. 409-432, Dez / 2012.

ORACLE. Oracle VM VirtualBox. 2020. Site Oficial. Disponível em: https://www.oracle.com/br/virtualization/virtualbox/. Acesso em: 18 maio 2020.

PINHEIRO, José Maurício dos Santos. Gerenciamento de Redes de Computadores. 2. 2002. 105 p.

POSTEL, Jonathan B. SIMPLE MAIL TRANSFER PROTOCOL. 1982. RFCs Oficiais. Disponível em: https://tools.ietf.org/html/rfc821 SMTP. Acesso em: 18 maio 2020.

Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2), 1993. Disponível em: https://tools.ietf.org/html/rfc1448. Acesso em 27 de janeiro de 2020.

RAUEN, Fábio José. Roteiros de investigação científica: os primeiros passos da pesquisa científica desde a concepção até a produção e a apresentação. Tubarão: Editora Unisul, 2015.

Singh, An introduction to virtualization, 2004, Disponível em: http://www.kernelthread.com/publications/virtualization/. Acesso em 29 de janeiro de 2020.

SOLUTIONS, Nagios. Nagios Overview: what is nagios? 2020. Disponível em: https://www.nagios.org/about/overview/. Acesso em: 18 maio 2020.

STALLINGS, William. Redes e Sistemas de Comunicação de Dados. Rio de Janeiro: Campus, 2005.

SZAPIRO, Marina. As mudanças recentes do setor de telecomunicações e os desafios impostos ao sistema de inovação brasileiro. Revista de Economia Política de Las Tecnologías de La Información y Comunicación, [s. l.], v., n. 2, p.1-28, ago. 2007.

TECH, Redação Canal. O que é open source? Disponível em: https://canaltech.com.br/produtos/O-que-e-open-source/. Acesso em: 18 maio 2020.

TECH, Redação Canal. O que é modelo OSI? 2020. Disponível em: https://canaltech.com.br/produtos/o-que-e-modelo-osi/. Acesso em: 18 maio 2020.

TELCOMANAGER. O que é SNMP? 2020. Disponível em: https://www.telcomanager.com/o-que-e-snmp/. Acesso em: 18 maio 2020.

TELECOM, Ccn. A importância da estrutura interna de um provedor de internet. 2019. Disponível em: https://ccntelecom.com.br/gestao/a-importancia-da-estrutura-interna-de-um-provedor-de-internet/.. Acesso em: 18 maio 2020.

WIKIPEDIA. LAMP. Site Colaborativo. Disponível em: https://pt.wikipedia.org/wiki/LAMP. Acesso em: 18 maio 2020.

XAVIER, E.; KOCH, F. L.; WESTPHALL, C. B. Avaliação de Variações da Configuração de Agentes Móveis na Gerência de Redes. Laboratório de Redes e Gerência da Universidade Federal de Santa Catarina (LRG –

UFSC) - 2002. Disponível em: https://www.researchgate.net/profile/Carlos_Westphall/publication/254862018_Avaliacao_de_Variacoes_da_Configuracao_de_Agentes_Moveis_na_Gerencia_de_Redes/links/0deec52c427b8ac7c8000000/Avaliacao-de-Variacoes-da-Configuracao-de-Agentes-Moveis-na-Gerencia-de-Redes.pdf. Acesso em: 15 jul. 2019.

ZABBIX. Zabbix Documentation 3.0. 2018. Disponível em: https://www.zabbix.com/documentation/3.0/pt/manual/ Acesso em: 05 ago. 2019.

Sistema de Visualização de Dados Para Uma Interface Facilitadora de Práticas Experimentais

Vitória Rodrigues dos Santos[1], Helena Borges Daré[2], Helmo Alan Batista de Araújo[1], Matheus Lorenzato Braga[1]

[1] Instituto Federal Catarinense,
[2] Universidade Federal de Santa Catarina

{vitoria373@gmail.com, helenaborgesdare@gmail.com, helmoalan@ifc.edu.br, matheus.braga@ifc.edu.br}

Abstract. *In this work a Data Visualization System (SVD) was developed for the data acquisition module to facilitate experimental practices. In the system, real-time graphics are used to assist in the realization of didactic experiments in the areas of mathematics, nature sciences and their technologies, through sensors and actuators. The development process was based on the connection between an Arduino microcontroller and the Java programming language, in which system validation tests were performed by integrating two sensors and one actuator. The system can be applied in different contexts and pedagogical environments for use by teachers and students at different levels and teaching-learning processes.*

Keywords: *Data Visualization, Didactic Experiments, Java, Arduino.*

Resumo. *Neste trabalho foi desenvolvido um Sistema de Visualização de Dados (SVD) para o módulo de aquisição de dados a fim de facilitar práticas experimentais. No sistema utilizam-se gráficos em*

tempo real para auxiliar na realização de experimentos didáticos nas áreas de matemática, ciências da natureza e suas tecnologias, por meio de sensores e atuadores. O processo de desenvolvimento pautou-se na conexão entre um microcontrolador Arduino e a linguagem de programação Java, no qual realizaram-se testes de validação do sistema integrando-se dois sensores e um atuador. O sistema pode ser aplicado em diferentes contextos e ambientes pedagógicos para uso de professores e alunos em diferentes níveis e processos de ensino-aprendizagem.

Palavras Chave: *Visualização de Dados, Experimentos Didáticos, Java, Arduino.*

1 Introdução

O século XXI é palco de transformações no âmbito econômico, político, social e educacional devido ao uso de Tecnologias da Informação e da Comunicação (TICs). As TICs proporcionam soluções úteis, rápidas e acessíveis nos mais variados campos do conhecimento, inclusive no processo de ensino-aprendizagem. Nesse contexto, muitos professores buscam a associação de novos recursos tecnológicos (computador, internet e TV) às aulas teóricas, objetivando estimular o aluno à aprendizagem dentro e fora do ambiente escolar.

À vista disso, existem tecnologias que auxiliam tanto na educação a distância (EaD), como na educação presencial, cita-se como exemplo as plataformas, já consolidadas, Moodle (MOODLE), Google Maps (GMAPS, 2005), GeoGebra (GEOGEBRA, 2002), PhET (PHET, 2002). Essas, por sua vez, possibilitam a integração entre diversas temáticas, através de experimentos, mapas, produção e compartilhamento de

conteúdo. As tecnologias afetam profundamente a educação que ainda está presa a lugares e tempos determinados, como escola e sala de aula (MORAM, 2013).

Assim, esse trabalho buscou desenvolver um software com fundamento educacional, a fim de facilitar práticas de ensino-aprendizagem experimentais com enfoque nas áreas de matemática, ciências da natureza e suas tecnologias. Entretanto, a realização de experimentos, por vezes, requer tempo e necessitam de ferramentas, mecanismos e pessoas com algum conhecimento técnico para organizá-los, o que acaba por dificultar a execução desses durante a aula, dada a falta de estrutura de laboratórios de ciências nas escolas do Brasil.

No primeiro SITED (2017) foi apresentada uma proposta de interface para facilitar práticas experimentais (ARAÚJO; BRAGA, 2017), entretanto para a execução de experimentos de forma simples, acessível e funcional nessa proposição, acarretou-se a necessidade do desenvolvimento de um aplicativo de visualização dos dados obtidos através dessa interface.

Contudo, o SVD foi desenvolvido com base na proposta de utilização de soluções de baixo custo, que facilitem o uso das TICs no desenvolvimento do ensino-aprendizagem através de atividades experimentais relacionadas à matemática, ciências da natureza e suas tecnologias.

2. Embasamento teórico

Apresentam-se nesse tópico os conceitos técnicos necessários para o entendimento deste artigo e das etapas realizadas.

2.1 Arduino

A plataforma Arduino, segundo McRoberts (2011), é um pequeno computador, também chamada de plataforma física ou embarcada, podendo programá-la para processar entradas/saídas

(input/output, ou I/O) entre dispositivos e componentes externos ligados a esta. O ambiente de desenvolvimento do Arduino é uma aplicação multiplataforma desenvolvida em Java, possui código-fonte aberto, funcionando no Windows, Linux e Mac (ARDUINO, 2016).

Entretanto, por se tratar de hardware e software livre, encontram-se inúmeros tipos de placas disponíveis no mercado, assim como esquemas eletrônicos para a construção de sua própria placa (ARDUINO, 2016). Dentre modelos mais comuns de Arduino disponíveis, segundo a classificação de Evans (2013), encontram-se o Arduino Uno, Arduino Duemilanove, Arduino Ethernet, Arduino Mega, Arduino Lilypod e Arduino Nano.

2.2 Java

A linguagem Java surgiu a partir de um projeto de pesquisa denominado Green Project, onde buscava-se a junção entre computador, eletrodomésticos e equipamentos eletrônicos. Dessa forma, a linguagem Java foi anunciada formalmente em maio de 1995, para aperfeiçoar aplicações dos servidores Web (ANSELMO, 2005; DEITEL; DEITEL, 2010).

Ademais, a linguagem Java é simples, com elementos menos complexos que a linguagem C ou C++. De igual modo, após o conhecimento dos conceitos básicos de POO (Programação Orientada a Objetos) é possível utilizar Java, visto que POO é um paradigma de programação de computadores, no qual empregam-se classes e objetos para reproduzir e processar dados (ANSELMO, 2005; SANTOS, 2013).

O código-fonte de um programa ou classe em Java tem a possibilidade de ser compilado em diversos computadores, podendo ser executado desde celulares a mainframes. Além disso, de acordo com Ascencio e Campos (2007), existem bibliotecas e um conjunto de classes já implementadas e testadas

no JDK (Java Development Kit - Kit de Desenvolvimento Java) que auxiliam no desenvolvimento das aplicações.

3 Metodologia

Para a implementação da aplicação descrita neste trabalho fez-se necessária a conexão entre sensor, Arduino e Java, como representado no esquema da figura 1:

Figura 1: Vínculo entre sensor, Arduino e Java.

Fonte: As autoras, 2016.

Utilizou-se a interface, proposta por Araújo e Braga (2017), de recepção/envio de dados que possui como framework uma placa Arduino, uma vez que essa palataforma pode enviar informações para basicamente qualquer sistema eletrônico. E também tem a capacidade de realizar o processo inverso, de enviar comandos do computador para o Arduino, controlando dispositivos conectados a essa palatforma (o Arduino) por intermédio do computador. Após os procedimentos descritos, procedeu-se a etapa que condiz ao desenvolvimento da aplicação através da linguagem de programação Java.

O desenvolvimento do SVD foi pautado nos seguintes requisitos funcionais:

- RF01. O SVD deve captar os dados da interface facilitadora e ilustrá-los de modo gráfico em tempo real.
- RF02. Deve possuir um botão de iniciar a captação de dados;
- RF03. Deve possuir um botão de pausar a captação de dados;
- RF04. Deve possuir um botão de reiniciar a captação de dados.

E requisitos não funcionais:

- RNF01. Deve conter fontes que facilitem a leitura dos dados;
- RNF02. Deve ser operacionalizado em Linux e Windows;
- RNF03. Deve ser implementado em JAVA;
- RNF04. Deve ter janelas de fácil navegação.

Para implementação do SVD, foram utilizados os sensores de distância, temperatura e um LED como atuador. Esses, por sua vez, respondem a um estímulo físico ou químico, sendo que, por exemplo, os sensores de temperatura (transdutores) convertem a temperatura em sinal elétrico, que pode ser interpretado pelo Arduino e enviado ao microcomputador.

Assim, inicialmente aconteceu a captação de estímulos do ambiente por meio dos sensores. Em seguida, o controlador Arduino recebe (lê) a informação do sensor, envia (escreve) essa informação ao Java e aplica os dados vindos do Arduino ao gráfico por meio da biblioteca JFreeChart.

O vínculo entre Java e Arduino estabeleceu-se através de uma classe específica, onde determinaram-se as configurações da porta serial. Assim, a cada segundo ou 1.000 microssegundos são capturados os dados e mostrados no gráfico, visto que o menor valor aceito para o tempo é de 1 microssegundo, enquanto o tempo máximo consiste em 8.388.480 microssegundos.

Estabeleceu-se a comunicação entre Java e a porta serial do computador através da biblioteca RXTX do Java. A mesma é um API de comunicação serial RXTX para leitura e escrita em portas seriais, sendo portada para Windows, Linux e Mac, disponível pelo site: http://www.rxtx.org, na seção de download.

Após o download, extraíram-se os arquivos compactados, onde criou-se uma pasta rxtx2.1-7-bins-r2, que possui uma biblioteca chamada RXTXcomm.jar, bem como os

arquivos rxtxParallel.dll e rxtxSerial.dll., de acordo com a arquitetura de 64bits(x64). Para adicionar a biblioteca RXTXcomm.jar ao projeto, clicou-se com o botão direito sobre esse, selecionou-se Propriedades, em seguida, Biblioteca e por fim, Adicionar JAR/Pasta, na qual informou-se o diretório que esta encontra-se.

Além disso, é de fundamental importância copiar o arquivo rxtxSerial.dll para dentro da pasta de instalação do Java (SDK) e em seguida para dentro do JRE (Java Runtime Environment - Ambiente de Tempo de Execução Java) na pasta /bin, visto que esse arquivo determina a comunicação serial, permitindo que outros usuários rodem o executável.

O ambiente de desenvolvimento Netbeans IDE (Ambiente Integrado de Desenvolvimento) foi utilizado na etapa de codificação dos gráficos, pois suporta diversas linguagens de programação, que por sua vez, permite escrever, depurar e compilar o programa de visualização dos dados. Empregou-se a linguagem de programação Java para o desenvolvimento dos experimentos de "variação de temperatura", "variação de distância" e "variação de frequência". Além de ser estudada ao longo do curso, é a linguagem mais utilizada no mundo e está presente em muitos lugares, desde notebooks e telefones celulares a datacenters e supercomputadores científicos, usufruindo da portabilidade e sendo compilado ou executado em diferentes plataformas suportadas pela tecnologia. Além disso, Java é seguro, segue os princípios da orientação a objetos e possui extensa biblioteca de rotinas.

Dentre as diversas bibliotecas da linguagem Java, escolheu-se a biblioteca Jfreechart para o desenvolvimento do Sistema de Visualização de Dados da Plataforma ExpeRT. Para isso adicionou-se a mesma ao ambiente de desenvolvimento, sendo assim possível criar a janela para construção de gráficos

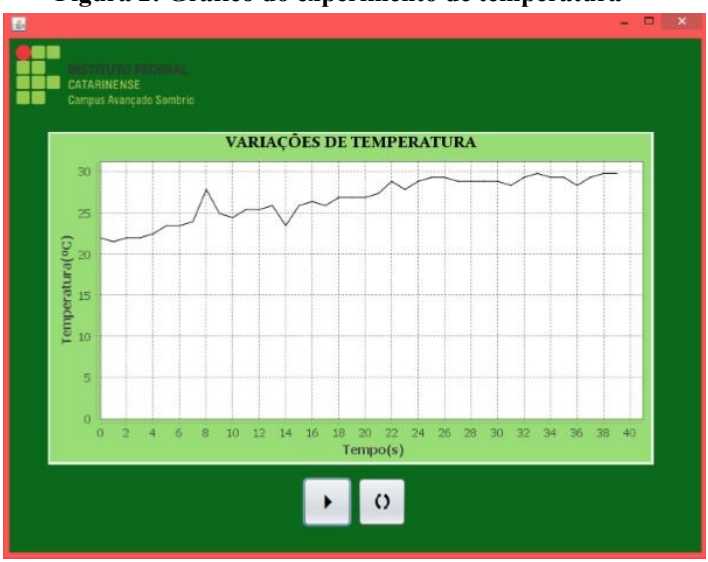
em tempo real, utilizando-se dos dados disponibilizados através do módulo de aquisição de dados.

A implementação do sistema de visualização de dados ocorreu com a utilização de três dispositivos, são eles: um sensor de distância, um sensor de temperatura e um LED, que podem vir a ser utilizados em diferentes experimentos didáticos.

4. Resultados e Discussões

Durante a implementação do SVD foram realizados alguns testes de validação e integração com a interface sugerida por Araújo e Braga (2017). O primeiro teste realizado teve como objetivo verificar o funcionamento e integridade do programa executável, referente ao experimento de temperatura. A primeira aplicação utilizou-se do sensor de temperatura LM35 para a captação dos valores alusivos à temperatura em dado instante.

Figura 2: Gráfico do experimento de temperatura



Fonte: As autoras, 2016.

O segundo teste teve o intuito de reproduzir o gráfico de distância, com o auxílio do sensor HCSR-04 para a captação dos dados. Assim, o experimento de distância, similarmente ao experimento de temperatura, consiste na criação de um gráfico a partir dos valores advindos do Arduino com objetivo de analisar variações de distância, como apresentado na ilustração a seguir.

Figura 3: Gráfico do experimento utilizando sensor de distância.

Fonte: As autoras, 2016.

O terceiro teste teve como propósito validar o experimento que calcula a frequência do LED a partir do intervalo de tempo necessário para executar uma oscilação (período). Sendo que, no campo correspondente ao período, mostra-se o tempo em segundos, condizente com os valores captados pelo Arduino e, também, no campo relativo à frequência, exibe-se o resultado do cálculo do inverso do período. Além disso, tem-se os botões de início e pausa, para

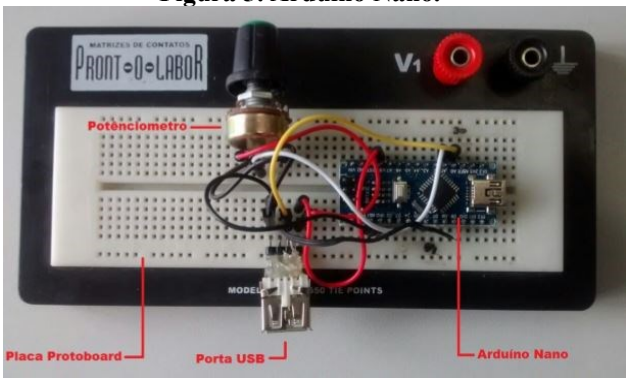
começar a colocação dos dados e parar a inserção desses, respectivamente, e o botão de limpar, com o intuito de apagar os valores dos campos.

Figura 4: Tela de mostragem do tempo e frequência do LED.

Fonte: As autoras, 2016.

Durante o desenvolvimento do Sistema de Visualização de Dados utilizou-se o Arduino Uno para a captação dos dados. Porém, para verificar a compatibilidade do sistema com outros módulos de aquisição de dados, também foi conduzido um teste com o Arduino Nano.

Figura 5: Arduino Nano.



Fonte: As autoras, 2016

Assim, constatou-se a conservação das funcionalidades do sistema em diferentes módulos de aquisição de dados, como verificado na Figura 5.

5. Considerações Finais

A fim de implementar os objetivos, buscou-se primeiramente por ferramentas que permitissem a conexão entre a linguagem Java e o módulo Arduino. No decorrer dessa procura, as ferramentas que se destacaram para atingir os requisitos foram a biblioteca JfreeChart e biblioteca RXTX SERIAL.

Amparado na fundamentação teórica e nas ferramentas pesquisadas, desenvolveu-se o Sistema de Visualização de Dados da Plataforma Arduino. Esse sistema permite a construção de gráficos utilizando dados em tempo real de sensores de distância, temperatura e também controlar um atuador LED, dispositivos estes que permitem a elaboração de práticas pedagógicas experimentais.

Ademais, sucederam-se ao transcorrer do desenvolvimento os testes de validação do Sistema de Visualização de Dados (SVD). De início, com a verificação individual do funcionamento de cada dispositivo, e, em segundo momento, com a associação dos dispositivos através de uma interface. Os testes foram realizados com sucesso e demonstraram a validação do SVD.

Em relação a trabalhos futuros, preconiza-se inserir outros sensores e atuadores (ex. sensor de luminosidade, motor elétrico, sensor de pressão) a fim de aumentar a gama de possibilidades de práticas experimentais e acrescentar ao sistema a funcionalidade de armazenamento dos dados para uma possível análise e comparação desses números em outras atividades de ensino-aprendizagem.

6. Referências

ANGELOTTI, Elaine Simoni. Banco de Dados. Curitiba: Livro Técnico, 2010. 120 p.

ANSELMO, Fernando. Aplicando Lógica Orientada a Objeto em Java. 2. ed. Florianópolis: VisualBook, 2005. 178 p.

ARDUINO. Arduino. 2016. Disponível em: <http://www.arduino.org/>. Acesso em: 20 mai 2016.

ARAÚJO, Helmo A. B.; BRAGA, MATHEUS L. Ensino de Ciências da Natureza e Arduino: Uma Proposta de Interface Para Facilitar Práticas Experimentais. Revista Tecnologias na Educação, 2017. Disponível em: <http://tecedu.pro.br/wp-content/uploads/2017/10/Art10-vol.21-Edi%C3%A7%C3%A3o-Tem%C3%A1tica-V-Outubro-2017.pdf>. Acesso em 20/02/2018

ASCENCIO, Ana F. G.; CAMPOS, Edilene A. V. Fundamentos da programação de computadores. 2. ed. São Paulo: Pearson Prentice Hall, 2007. 428 p.

BANZI, Massimo. Primeiros Passos com o Arduino. São Paulo: Novatec, 2011. 151 p.

DEITEL, Harvey M.; DEITEL, Paul. Java: Como programar. 8. ed. São Paulo: Pearson Prentice Hall, 2010. xl, 1108 p.

EVANS, Martin. Arduino em Ação. São Paulo: Novatec, 2013. 424 p.

GEOGEBRA. GeoGebra. 2002. Disponível em <https://www.geogebra.org/?lang=pt_BR>. Acessado em 15/02/2018

GMAPS, Google Maps. 2005. Disponível em <https://www.google.com.br/maps/>. Acessado em 15/02/2017.

MCROBERTS, Michael. Arduino Básico. São Paulo: Novatec, 2011. 456 p.

MOODLE. Moodle, 2001. Moodle. Disponível em <https://moodle.org/>.Acessado em 15/02/2017

MORAM, José. A Educação que desejamos: novos desafios e como chegar lá. 5 ed. Campinas. Papyrus, 2013. p.89-90

PHET. Phet Interactives Simulations. 2002. Disponível em: <https://phet.colorado.edu/pt_BR/>. Acesso em 15/02/2018

SANTOS, Rafael. Introdução à programação orientada a objetos usando Java. 2. ed. Rio de Janeiro: Elsevier, 2013. 336 p.

SCHILDT, Herbert; SKRIEN, Dale. Programação com Java: uma introdução abrangente. Porto Alegre: AMGH, 2013. xxiv, 1128 p.

Análise de desempenho dos protocolos VPN: IPSec, WireGuard e OpenVPN em firewall PfSense

César Carvalho Felisberto[1] , Guilherme da Silva Klein Bitencourt[2]

[1]Discente do Curso Superior de Tecnologia em Redes de Computadores - Instituto Federal Catarinense – Campus Avançado Sombrio 88.960-000 – Sombrio – SC – Brasil

[2]Docente do Curso Superior de Tecnologia em Redes de Computadores - Instituto Federal Catarinense – Campus Avançado Sombrio 88.960-000 – Sombrio – SC – Brasil

cesarfelisbetoo@gmail.com,
guilherme.bitencourt@ifc.edu.br

Abstract. *This work aims to evaluate the performance of VPN tunnels (Virtual Private Network) by measuring the minimum bandwidth, average and maximum, as well as the CPU utilization of virtual servers during the use of tunnels configured with the VPN protocols available in the Pfsense firewall - IPSec, OpenVPN and WireGuard. The evaluation is done through the IPerf test tool in a Site-to-Site VPN scenario. According to the results obtained it was possible to conclude that in this scenario the IPSec protocol obtained the best results in relation to bandwidth (due to its implementation in the kernel), despite the high CPU consumption compared to the WireGuard and OpenVPN protocols.*

Keywords. *VPN, PfSense, Site-to-Site.*

Resumo. *Este trabalho tem como objetivo avaliar o desempenho dos túneis VPN (Virtual Private Network, "rede virtual privada") através da medição da largura de banda mínima, média e máxima, bem como da utilização de CPU dos servidores virtuais durante o uso dos túneis configurados com os protocolos VPN disponíveis no firewall PfSense – IPSec, OpenVPN e WireGuard. A avaliação é feita através da ferramente de teste IPerf em um cenário VPN Site-to-Site. De acordo com os resultados obtidos, foi possível concluir que neste cenário o protocolo IPSec obteve os melhores resultados em relação a largura de banda (devido a sua implementação no kernel), apesar do alto consumo de CPU em comparação aos protocolos WireGuard e OpenVPN.*

Palavras-chave. *VPN, PfSense, Site-to-Site.*

1. Introdução

Em uma organização a comunicação segura entre matriz e filiais é um ponto crucial para o sigilo dos dados internos. Existem várias soluções no mercado para atingir tal objetivo e a VPN (Virtual Private Network, "Rede Virtual Privada"), é uma solução muito adotada na atualidade.

Conforme Lima et al. (2013), uma rede VPN garante a confiabilidade no transporte dos dados, bem como a segurança na comunicação, tornando-se uma alternativa interessante comparada a outras alternativas.

Soluções como links dedicados de fibra ótica ou rádio acarretam altos custos e dependem dos Provedores de Serviço de Internet para manter a rede dedicada de longa distância, o que pode dificultar na viabilidade de implantação em pequenas e médias empresas.

Neste cenário a VPN representa uma solução

interessante quando utilizada através da rede pública de internet para efetuar a comunicação entre os pontos de conexão, diminuindo, assim, os custos de implantação.

Além da criptografia, a VPN também deve fornecer garantia de QoS (Quality of Service, "Qualidade de Serviço") aos seus usuários. Para manter a QoS em um nível aceitável, a largura de banda reservada à VPN deve ser significativamente maior do que o valor médio do tráfego de dados no túnel (CUI; BASSIOUNI, 2003).

Deste modo, o desempenho de uma VPN é um aspecto importante no momento da escolha do protocolo a ser utilizado. Cada protocolo possui diferentes características de funcionamento que diretamente influenciam na taxa de transferência máxima da conexão, bem como o consumo de recursos dos servidores. É crucial escolher o protocolo mais adequado, para assim utilizar de forma mais eficiente o hardware disponível e obter o melhor desempenho da VPN.

Este artigo tem como objetivo apresentar a comparação de desempenho (largura de banda mínima, média, máxima e utilização de CPU) entre os protocolos de VPN: IPSec, WireGuard e OpenVPN utilizando *firewall* PfSense que possui estes protocolos disponíveis como pacotes nativos do sistema.

Os túneis VPN foram configurados em formato *Site-to-Site* através de dois *firewalls* PfSense, virtualizados via VirtualBox, entre duas máquinas físicas com sistema operacional Windows 10 como *host* de cada Hipervisor. A comunicação entre as máquinas físicas se dá através de uma conexão Ethernet de 1 Gbps utilizando um cabo *crossover* entre as duas máquinas.

A motivação original para a avaliação dos protocolos VPN surgiu com o intuito de avaliar os protocolos através da rede pública de Internet. Porém, isso não foi possível, visto que os Provedores de Internet não disponibilizam, de forma gratuita,

endereços IPv4 públicos aos clientes. O custo de aquisição de endereços IPv4 públicos é alto, logo inviabilizaria a realização desse trabalho. Deste modo, a solução foi realizar o teste em uma rede local.

Outro ponto a destacar foi a tentativa de avaliar a largura de banda dos túneis VPN (IPSec, OpenVPN e WireGuard) entre dois *hosts* virtuais Windows 10, via IPerf instalado em cada VM. Onde, assim, um *host* seria o cliente IPerf e a outro seria o servidor IPerf, de modo que um *host* estaria conectado na rede local do *firewall PfSense-SiteA* e o outro *host* estaria conectado na rede local do *firewall PfSense-SiteB.* Porém, não foi possível realizar esta avaliação devido às limitações de hardware dos computadores portáteis utilizados. Os testes dos túneis VPN apenas foram possíveis entre os dois servidores *firewall* virtuais (*PfSense-SiteA e PfSense-SiteB*) sem os *hosts* adicionais. Neste cenário os computadores utilizados foram capazes de suportar a demanda.

2. Referencial Teórico

Nesta seção, serão abordadas as definições e funcionamento de uma VPN. São descritos os protocolos IPSec, WireGuard e OpenVPN e apresentadas as ferramentas PfSense, IPerf e VirtualBox, utilizadas na implementação dos servidores.

2.1. VPN

De acordo com Ferguson e Huston (1998), uma VPN (Virtual Private Network, “Rede Virtual Privada”) é um ambiente de comunicação no qual o acesso é controlado para permitir conexões apenas dentro de uma comunidade definida de interesse, e é construído através de alguma forma de divisão de um meio de comunicação subjacente comum, onde este meio fornece serviços à rede de forma não exclusiva, ou seja, VPN é uma rede privada construída dentro de uma infraestrutura de rede pública, como a Internet.

Conforme Borges, Alves Fagundes, Nunes Da Cunha (2019), quando se cria uma conexão VPN está se criando um túnel entre as extremidades da conexão. Deste modo, os dados trafegam de forma segura entre os pontos de conexão. O tunelamento se dá quando em uma das extremidades da conexão, os dados são criptografados e depois o pacote de dados original é encapsulado dentro de um novo pacote para ser enviado através da rede.

Existem dois tipos de VPN: *Site-to-Site* (Ponto-a-Ponto) e *Remote-Access* (Acesso Remoto).

O tipo *Site-to-Site* (Ponto-a-Ponto) trata-se de uma conexão entre duas (ou mais) redes privadas através de uma rede pública como a Internet. Este tipo permite que qualquer dispositivo da primeira rede comunique-se com qualquer outro da segunda rede e vice-versa. É configurada ao nível dos dispositivos de rede para obter maior flexibilidade, onde qualquer dispositivo de uma rede se comunique diretamente com a outra (Tyson; Jeff 2013).

Por sua vez, o tipo *Remote-Access* (Acesso-Remoto) permite conectar clientes individuais diretamente às redes VPN. A configuração de acesso deve ser definida no dispositivo de cada cliente. Esta é a solução mais adequado para mobilidade contínua (Tyson; Jeff 2013).

2.2. Protocolos VPN

Segundo Vasques, Schuber (2002), os protocolos são necessários para que os dispositivos de redes possam comunicar-se "falando" o mesmo idioma.

2.2.1 IPSec

Conforme Chawla, Gupta e Sawhney (2014), o IPsec se define como um conjunto de protocolos de segurança

desenvolvido pela IETF (Internet Engineering Task Force) em 1998.

O IPSec fornece integridade de dados, autenticação básica e serviços de criptografia para proteger a modificação dos dados e/ou visualização não autorizada em redes IPv4 ou IPv6. Os três principais componentes do IPSec incluem os protocolos: Authentication Header (AH), Encapsulating Security Payload (ESP) e Internet Key Exchange (IKE) (Chawla; Gupta; Sawhney, 2014).

Este protocolo é controlado por um mecanismo de gerenciamento e política de chaves, que reside diretamente no *kernel* do sistema operacional (FreeBSD) (“ipsec(4)”, 2022).

2.2.2 WireGuard

De acordo com Anbarje, Sabbagh, Palacin (2020), o WireGuard foi desenvolvido por Jason Donenfeld. Este protocolo opera em redes IPv4 ou IPv6 e é baseado no protocolo UDP. Seu modelo de autenticação é baseado nas chaves autenticadas do SSH e possui menos de 4.000 linhas de código, o que facilita a verificação contra vulnerabilidades.

Este protocolo implementa a criptografia simétrica ChaCha20Poly1305 e utiliza algoritmos diferentes para trocas de chaves, sendo eles: Hashing Curve25519 para curva elíptica, Diffie–Hellman (ECDH) para acordo de chave anônima, BLAKE2s para hash (RFC7693), Sip-Hash24 para chaves de tabela de hash e HKDF para derivação de chave (RFC5869) (Anbarje; Sabbagh; Palacin, 2020).

A criptografia ChaCha20Poly1305, oferece um bom desempenho em software (espaço do usuário) em praticamente todas as CPUs. Porém, até o momento, não há um suporte

satisfatório para essa criptografia em nível de hardware (*kernel*) (Donenfeld, 2022).

2.2.3 OpenVPN

OpenVPN é um protocolo VPN de código aberto que foi desenvolvido por James Yonan em 2002. Pode ser configurado para usar os protocolos TCP ou UDP, suporta criptografia de até 256 bits e utiliza SSL-TLS para autenticação e criptografia (Anbarje; Sabbagh; Palacin, 2020).

Uma vez que o OpenVPN trabalha em nível de usuário do sistema operacional, para este tipo de implementação, por conta da criptografia e das trocas de contexto, existe uma sobrecarga na CPU que pode limitar o desempenho do protocolo ("We now have OpenVPN data channel offload: Here's what that means", 2021).

2.3. PfSense

O software PfSense é uma distribuição customizada gratuita e de código aberto do FreeBSD especificamente adaptada para uso como *firewall* e roteador totalmente gerenciada por meio da interface da web ("Learn About the PfSense Project", 2022).

Segundo Campos das Neves, Machado e Centenaro (2014), *firewall* é uma solução de segurança baseada em hardware ou software, que a partir de um conjunto de regras ou instruções, analisa o tráfego da rede para diferenciar operações válidas ou inválidas dentro de uma rede corporativa. Um *firewall* analisa o tráfego de rede entre a internet e a rede privada ou entre redes privadas como as VPN.

2.4. IPerf

O iPerf3 é uma ferramenta para medições ativas da largura de banda máxima alcançável em redes IP. Ele suporta o ajuste de

vários parâmetros relacionados aos protocolos (TCP, UDP, SCTP com IPv4 e IPv6). Para cada teste, este relata a largura de banda, consumo de CPU entre outros parâmetros (Gueant, 2013).

2.5. VirtualBox

O Oracle VM VirtualBox é um software de virtualização (hipervisor) de código-fonte aberto e multiplataforma que permite que vários sistemas operacionais sejam executados simultaneamente em um único dispositivo (“Oracle VM VirtualBox”, 2021).

Um hipervisor é um software que cria e executa máquinas virtuais (VMs) e isola o sistema operacional e os recursos do hipervisor das máquinas virtuais permitindo a criação e o gerenciamento dessas VMs. O hipervisor trata os recursos, como CPU, memória e armazenamento, como um conjunto de recursos que podem ser facilmente realocados entre máquinas virtuais existentes ou novas (“What is a hypervisor?”, 2020).

3. Materiais e métodos

Este artigo adotou como tipo de pesquisa a *Design Science Research Methodology*, e tem como objetivo apresentar a avaliação de desempenho entre os protocolos VPN: IPSec, WireGuard e OpenVPN implementados no *firewall* PfSense.

3.1. Materiais

Como materiais, foram utilizados dois computadores portáteis conectados através de um cabo *crossover,* cada computador contém o hipervisor VirtualBox instalado, e cada VirtualBox contém uma máquina virtual instalada, ambas as VMs são servidores PfSense *(PfSense-SiteA e PfSense-SiteB).*

Em seguida, foram realizadas as configurações das duas máquinas virtuais, onde cada uma possui duas placas de rede

virtuais, uma para comunicação entre os dois servidores virtuais PfSense (modo ponte com a placa de rede do computador portátil) e a outra para poder acessar a interface web do PfSense através da rede local de cada *firewall*. Foram também realizadas as configurações dos protocolos IPSec, WireGuard e OpenVPN em ambos os servidores virtuais para habilitar o funcionamento dos respectivos túneis VPN.

3.2. Métodos

Este estudo adotou como metodologia a *Design Science Research Methodology*.

Em primeiro momento, foram realizados estudos sobre o tema abordado, tecnologias e ferramentas utilizadas. Em seguida, foram configurados os protocolos VPN (IPSec, WireGuard e OpenVPN) nos servidores *PfSense-SiteA e PfSense-SiteB* para possibilitar a avaliação de desempenho, sendo como principal objetivo, avaliar a largura de banda mínima, média e máxima para cada túnel VPN, assim como o consumo de CPU durante o teste em cada servidor (*PfSense-SiteA e PfSense-SiteB*).

O computador portátil 01 (host do servidor PfSense-*SiteA*) possui como hardware: CPU Intel i5-7200U, 8GB de RAM e SSD de 480GB. O computador portátil 02 (host do servidor PfSense-*SiteB*) possui como hardware: CPU AMD Ryzen 5 3500U, 12GB RAM e SSD de 240GB.

O sistema operacional base utilizado em ambas as máquinas físicas foi o Microsoft Windows 10 Home Single Language versão 10.0.19045, Build 19045, para execução da VirtualBox.

Utilizou-se o hipervisor VirtualBox versão 7.0.2 r154219 (Qt5.15.2) para virtualização dos servidores PfSense. Cada máquina virtual possui 4 núcleos e 4GB de memória.

A versão utilizada do PfSense foi a 2.6.0-RELEASE (amd64) para criação dos túneis VPNs.

A configuração utilizada para o túnel VPN IPSec foi baseada no manual do fabricante do PfSense, Netgate ("PfSense® software configuration recipes — IPsec site-to-site VPN example with pre-shared keys", 2022).

Utilizou-se o método de chave pré-compartilhada e foram criadas regras de *firewall* para ser possível a conexão. O padrão de criptografia utilizado foi o AES com um comprimento de chave de 256 bits. Os endereços de rede estão descritos na tabela a seguir:

Tabela 1. Configurações de endereços IPSec

PfSense-SiteA		PfSense-SiteB	
Nome	Filial	Nome	Matriz
IP WAN	10.0.2.10	IP WAN	10.0.2.15
Subnet LAN	10.1.1.0/24	Subnet LAN	192.168.1.0/24
IP LAN	10.1.1.1	IP LAN	192.168.1.1

Fonte: Os autores, (2022).

Para o túnel VPN WireGuard, a configuração no PfSense também foi baseada no manual do fabricante do PfSense, Netgate ("PfSense® software configuration recipes — WireGuard site-to-site VPN configuration example", 2022).

Foi utilizado o método de chave pré-compartilhada e criou-se regras de roteamento e *firewall* para estabelecer a conexão. O WireGuard utiliza a criptografia ChaCha20Poly1305. Abaixo estão os endereçamentos utilizados:

Tabela 2. Configurações de endereços WireGuard

PfSense-SiteA		PfSense-SiteB	
Nome	Filial	Nome	Matriz
IP WAN	10.0.2.10	IP WAN	10.0.2.15
IP Túnel	10.6.210.0/31	IP Túnel	10.6.210.1/31
Porta	51820	Porta	51820
Subnet LAN	10.1.1.0/24	Subnet LAN	192.168.1.0/24

Fonte: Os autores, (2022).

O túnel VPN OpenVPN foi configurado no PfSense de acordo com o manual do fabricante do PfSense, Netgate ("PfSense® software configuration recipes — OpenVPN site-to-site configuration example with shared key", 2022).

Nesta configuração também foi utilizado o método de chave pré-compartilhada e configurado regras de *firewall* para estabelecer a conexão entre os dois pontos. O OpenVPN utiliza AES-256 como criptografia. A seguir está descrita a configuração de endereços utilizada:

Tabela 3. Configurações de endereços OpenVPN

PfSense-SiteA		PfSense-SiteB	
Nome	Filial	Nome	Matriz
IP WAN	10.0.2.10	IP WAN	10.0.2.15
Rede Túnel	10.3.100.0/30	Rede Túnel	10.3.100.0/30
Subnet LAN	10.1.1.0/24	Subnet LAN	192.168.1.0/24
IP LAN	10.1.1.1	IP LAN	192.168.1.1

Fonte: Os autores, (2022).

Utilizou-se a versão IPerf3 do software de teste IPerf para medir a largura de banda mínima, média e máxima, bem como a utilização de CPU dos dois servidores virtuais durante a avalição de cada protocolo.

O IPerf possui dois módulos no PfSense: cliente e servidor. O módulo cliente envia os dados e o módulo servidor, quando habilitado, fica disponível para receber conexões do módulo cliente e assim que a conexão for estabelecida medirá a largura de banda máxima, além da utilização de CPU de cada lado da conexão durante o período de execução. Os testes podem ser realizados enviando pacotes TCP ou UDP.

O servidor virtual PfSense-SiteA foi utilizado como IPerf cliente, e o servidor PfSense-SiteB foi utilizado como IPerf servidor. Durante a execução do teste, por padrão, o IPerf realiza os testes enviando a quantidade máxima de dados possível, através do túnel VPN, por segundo, durante 10 segundos. Finalizado o teste, obtém-se um resultado de largura de banda máxima para cada segundo do teste, e também, é obtido 1 resultado do consumo máximo de CPU do cliente e servidor que se deu durante o período teste.

Deste modo, foram realizados os testes por 5 vezes consecutivas, obtendo um total de 50 resultados de largura de banda máxima e um total de 5 resultados de consumo de CPU para os pacotes enviados via TCP e a mesma quantidade de resultados para os pacotes enviados via UDP.

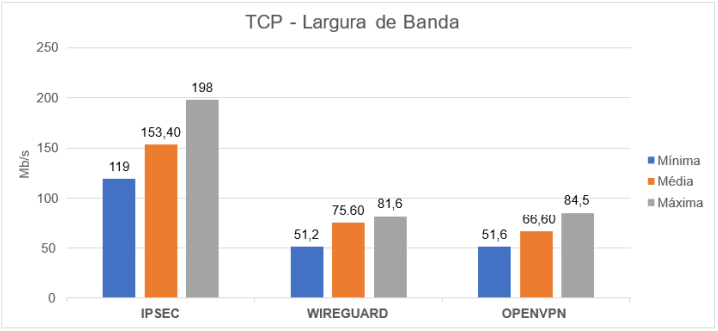
Durante a realização dos testes, enquanto um protocolo está sendo avaliado os outros ficam desativados para não interferir nos resultados.

Após a realização dos testes, foram analisados os resultados para cada protocolo VPN, nos dois cenários de teste (envio de pacotes TCP e UDP), determinando os valores mínimos, médios e máximos que foram apresentados em formato de gráfico para melhor visualização das comparações.

4. Resultados e Discussões

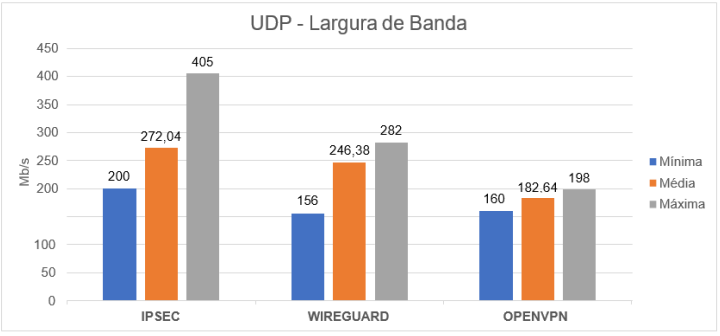
Nos gráficos a seguir pode-se observar os resultados de largura de banda para os protocolos VPN: IPSec, WireGuard e OpenVPN ao enviar pacotes em TCP e UDP:

Gráfico 1. TCP - Largura de Banda



Fonte: Os autores,(2022).

Gráfico 2. UDP - Largura de Banda

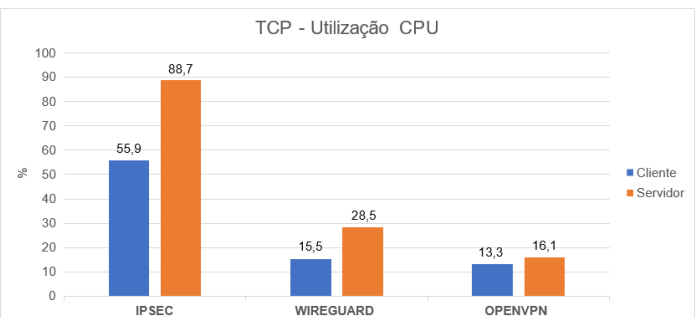


Fonte: Os autores, (2022).

Os resultados da avaliação mostram que o protocolo IPSec obteve o melhor desempenho em seu túnel VPN, visto que, obteve resultados de largura de banda superior aos demais protocolos avaliados em todas as métricas apresentadas (mínima, média e máxima). Este resultado era esperado devido ao fato do protocolo IPSec trabalhar em nível de *kernel* do sistema operacional, o que permite criptografia e descriptografia mais rápidas. Diferentemente do Wireguard e OpenVPN, que trabalham em nível de usuário do sistema operacional, não possuindo, assim, acesso direto ao hardware. Logo, são menos eficientes em comparação ao IPSec, obtendo um desempenho inferior a este.

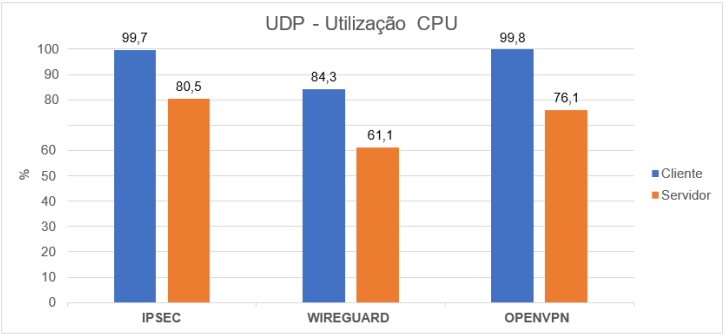
Durante o teste de largura de banda, também foi possível observar os resultados de utilização de CPU dos protocolos VPN IPSec, WireGuard e OpenVPN ao enviar pacotes em TCP e UDP:

Gráfico 3. TCP – Utilização CPU



Fonte: Os autores (2022).

Gráfico 4. UDP – Utilização CPU



Fonte: Os autores, (2022).

Podemos verificar que a utilização de CPU, de modo geral, foi maior para IPSec em ambos os testes, o que vai de acordo com o resultado de largura de banda, visto que esse protocolo obteve as maiores velocidades. Porém, em contra partida, foi o que mais demandou uso de CPU.

Os testes realizados representam uma sobrecarga simulada nos túneis VPN para possibilitar a identificação dos limites de cada protocolo. Em um cenário de utilização real, por exemplo, entre dois polos de uma organização, dificilmente veríamos esse consumo de CPU a todo tempo, no máximo picos eventuais ao transferir grandes arquivos. De qualquer modo é possível através de regras de *firewall* limitar a largura de banda para cada dispositivo que utiliza o túnel, a fim de evitar sobrecarga dos servidores e lentidão na rede.

O WireGuard e OpenVPN continuam sendo ótimas alternativas, mas de acordo com os resultados, recomenda-se o IPSec como principal protocolo a ser considerado para implementar uma VPN *Site-to-Site*.

5. Considerações Finais

O objetivo principal desse trabalho foi realizar a comparação de desempenho (largura de banda mínima, média, máxima e utilização de CPU) entre os protocolos IPSec, WireGuard e OpenVPN, instalados em dois servidores PfSense em um cenário VPN *Site-to-Site*.

O PfSense disponibiliza os protocolos IPSec, WireGuard e OpenVPN. Durante a avaliação, foi possível definir que o protocolo IPSec obteve os melhores resultados de largura de banda comparado aos demais protocolos testados, apesar do maior consumo de CPU, o que era esperado, devido a sua implementação no *kernel* do sistema operacional. Pode-se considerar o IPSec como o protocolo mais indicado para o cenário VPN *Site-to-Site*, o qual tem como objetivo obter a maior largura de banda possível em túnel VPN.

Entretanto, os resultados não foram os mais satisfatórios para uma conexão Gigabit que possui limite teórico de largura de banda de 1000Mbps. O resultado de largura de banda máxima atingido foi de 405Mbps, que está diretamente relacionado à capacidade de processamento do hardware dos computadores portáteis utilizados. Para obter melhores resultados, ou seja, velocidades que se aproximem do limite teórico da conexão, se faz necessário a utilização de computadores ou servidores com capacidade de processamento superior aos utilizados neste trabalho.

Como não foi possível avaliar os protocolos VPN através da rede pública de Internet (devido não ter acesso a IPs públicos) os testes foram realizados localmente entre os dois servidores *firewall* virtuais (*PfSense-SiteA e PfSense-SiteB*).

Como sugestão para novos estudos, poderá ser realizada a análise de desempenho dos protocolos aqui testados, em cenário real e não virtualizado, utilizando hardware com capacidade de processamento superior ao hardware utilizado

neste trabalho. Os protocolos VPN poderão também ser avaliados em um cenário VPN *Remote-Access*.

6. Referências

ANBARJE, A.; SABBAGH, M.; PALACIN, D. P. Evaluation of WireGuard and OpenVPN VPN Solutions. Disponível em: <https://www.diva-portal.org/smash/get/diva2:1467354/FULLTEXT01.pdf>. Acesso em: 24 out. 2022.

BORGES, F.; ALVES FAGUNDES, B.; NUNES DA CUNHA, G. VPN: Protocolos e Segurança. Disponível em: <https://www.lncc.br/~borges/doc/VPN%20Protocolos%20e%20Seguranca.pdf>. Acesso em: 24 out. 2022.

DAS NEVES, F. et al. Implantação de Firewall PfSense. Disponível em: <http://repositorio.utfpr.edu.br/jspui/bitstream/1/9787/2/CT_COTEL_2014_2_02.pdf>. Acesso em: 24 out. 2022.

LIMA, F. S. et al. VPN: Uma solução prática e economicamente viável. Disponível em: <https://www.researchgate.net/profile/Jocenio-Epaminondas/publication/360849741_VPN_Uma_Solucao_Pratica_e_Economicamente_Viavel/links/628e62538d19206823da58dd/VPN-Uma-Solucao-Pratica-e-Economicamente-Viavel.pdf>. Acesso em: 26 out. 2022.

CUI, W.; BASSIOUNI, M. A. Virtual private network bandwidth management with traffic prediction. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128603002172>. Acesso em: 26 out. 2022.

TYSON, JEEF. How virtual private networks work. Disponível em: <https://www.communicat.com.au/wp-content/uploads/2013/04/how_vpn_work.pdf>. Acesso em: 26 out. 2022.

PfSense® software configuration recipes — IPsec site-to-site VPN example with pre-shared keys. Disponível em: <https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-s2s-psk.html>. Acesso em: 5 nov. 2022.

PfSense® software configuration recipes — WireGuard site-to-site VPN configuration example. Disponível em: <https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-s2s-psk.html>. Acesso em: 5 nov. 2022.

PfSense® software configuration recipes — OpenVPN site-to-site configuration example with shared key. Disponível em: <https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-s2s-psk.html>. Acesso em: 5 nov. 2022.

FERGUSON, P.; HUSTON, G. What is a VPN? Disponível em:

<https://cpham.perso.univ-pau.fr/ENSEIGNEMENT/COMMUN/vpn_ferguson.pdf>.Acesso em: 12 nov. 2022.

GUEANT, V. iPerf - The TCP, UDP and SCTP network bandwidth measurement tool. Disponível em: <https://iperf.fr/>. Acesso em: 12 nov. 2022.

Learn about the PfSense project. Disponível em: <https://www.pfsense.org/about-pfsense/>. Acesso em: 12 nov. 2022.

ipsec(4). Disponível em:

<https://www.freebsd.org/cgi/man.cgi?query=ipsec&sektion=4&format=html>. Acesso em: 18 nov. 2022.

DONENFELD, J. A. Known limitations - WireGuard. Disponível em:

<https://www.wireguard.com/known-limitations/>. Acesso em: 18 nov. 2022.

We now have OpenVPN data channel offload: Here's what that means. OpenVPN, 30 ago. 2021. Disponível em:

<https://openvpn.net/blog/openvpn-data-channel-offload/>. Acesso em: 18 nov. 2022

What is a hypervisor? Disponível em:

<https://www.vmware.com/topics/glossary/content/hypervisor.html>. Acesso em: 19 nov. 2022.

Oracle VM VirtualBox. Disponível em: https://imagegrafix.in/wp-content/uploads/2021/07/ImageGrafix_oracle-virtualbox-datasheet.pdf. Acesso em: 19 nov. 2022.

CHAWLA; GUPTA; SAWHNEY. A Review on IPsec and SSL VPN. Disponível em:

<https://www.researchgate.net/profile/O-P-Gupta/publication/270271647_A_Review_on_IPsec_and_SSL_VPN/links/5b02f024a6fdccf9e4f7575f/A-Review-on-IPsec-and-SSL-VPN.pdf>. Acesso em: 29 nov. 2022.

VASQUES; SCHUBER. Implementação de uma VPN em Linux utilizando o protocolo IPSec. Disponível em: <http://www.fsnet.com.br/downloads/Manuais/vpn.pdf>. Acesso em: 29 nov. 2022.

QUIC para DNS: análise de Performance de DNS over Quic e DNS over HTTP/3

Arthur Cechinel Neves[1], Vanderlei Freitas Junior[2], Matheus Lorenzato Braga[2]

[1] Curso Superior de Tecnologia em Redes de Computadores – Instituto Federal Catarinense – Campus Avançado Sombrio (IFC-CAS) 88960-000 – Sombrio – SC – Brasil

arthur.c.neves@hotmail.com
{vanderlei.freitas,matheus.braga}@ifc.edu. br

[1]Acadêmico do Instituto Federal Catarinense – Campus Avançado Sombrio – 88960000 – Sombrio – SC – Brasil

[2]Docente do Instituto Federal Catarinense – Campus Avançado Sombrio – 88960000 – Sombrio – SC – Brasil

Abstract. *With the popularization of the Internet, new technologies were created to improve the performance and security of the network, such as the new transport layer protocol QUIC, which allowed new types of DNS (Domain Name System) to appear. DNS over QUIC (DoQ) and DNS over HTTP/3 (DoH3) were created from the DNS over HTTPS update. This research shows the concepts and characteristics of QUIC as well as its use in DNS with DoQ and DoH3, with the aim of carrying out Round Trip Time (RTT) tests between the three types of DNS, in addition to comparing them with traditional DNS, through the use of a DNS proxy. The first test, in a controlled environment scenario, failed due to a configuration failure. With a second test, in an uncontrolled environment scenario to visualize the RTT differences between traditional DNS, DoQ and DoH3 from the perspective of an end user located in Brazil a superiority of DoH3 over DoQ was showed.*

Keywords: *Dns, QUIC, DNS over QUIC, DNS over HTTP3.*

Resumo. *Com a popularização da internet novas tecnologias foram criadas para melhorar o desempenho e segurança da rede, como o novo protocolo de camada de transporte QUIC que possibilitou novos tipos de DNS (Domain Name System) aparecerem. Foram criados o DNS over QUIC (DoQ) e DNS over HTTP/3 (DoH3) da atualização do DNS over HTTPS. Essa pesquisa mostrar os conceitos e as características do QUIC bem como do seu uso no DNS com o DoQ e do DoH3, tendo por objetivo a realização de testes de Round Trip Time (RTT), entre os três tipos DNS, além de compará-los com o DNS tradicional, através do uso de um proxy DNS. O primeiro teste, em um cenário de ambiente controlado apresentou falha devido a uma provável falha de configuração. Com um segundo teste, em um cenário de ambiente não controlado para visualizar as diferenças do RTT entre o DNS tradicional, DoQ e DoH3 da visão de um usuário final localizado no Brasil, mostrou uma superioridade do DoH3 em relação ao DoQ.*

Palavras-Chaves: *Dns, QUIC, DNS over QUIC, DNS over HTTP3.*

1. Introdução

Cada vez mais, novos usuários estão se conectando à Internet, fazendo ela se expandir. Em um levantamento realizado pela Semrush, Casagrande (2022), mostra que nos dez sites mais acessados do Brasil no ano de 2022, somavam mais de 10 bilhões os acessos. Para atender essa demanda de tráfego, vários segmentos estão se adaptando e otimizando como os protocolos de redes com o desenvolvimento de um novo protocolo de transporte, o QUIC, e de novos tipos de DNS (*Domain Name System*) que atendem essas requisições de tráfego para os usuários com mais agilidade e segurança como o DNS over QUIC (DoQ) e DNS over HTTP/3 (DoH/3).

A ARPANET (*Advanced Research Projects Agency Network*) surgida em 1969, foi a primeira rede de computadores, tornando-se o prelúdio da atual Internet. Ela se popularizou graças à eficiência dos novos conjuntos de protocolos, sendo eles na camada de transporte os protocolos TCP/UDP (*Transmission Control Protocol/User Datagram Protocol*). Tanenbaum e Wetherall (2011, p. 44) esclarecem de maneira simples a função da camada de transporte como sendo responsável por receber os dados e dividi-los em partes menores, e enviá-los corretamente para o destino. A camada de redes deve definir o caminho para o destino com o uso protocolo IP (*Internet Protocol*). O IP realiza o endereçamento de cada máquina com uma série de números exclusivos. Assim, para a comunicação entre as máquinas ocorra é necessário que ambas possuam um protocolo da camada de transporte como TCP/UDP e de rede com o IP exclusivo de cada máquina que se quer acessar.

No entanto, saber de todos endereços IPs diferentes para acessar cada máquina se tornou inviável para os seres humanos, então durante a ARPANET a solução foi atrelar os nomes das

máquinas com o IP em um arquivo chamado HOST.TXT. Um arquivo que era manualmente editado por administradores e mantido pela NIC (*Network Information Center*) e distribuído para a rede por uma única máquina conhecida por SRI-NIC (Liu; Albitz, 2006, p.3). Contudo, Liu e Albitz (2006, p.3), explicam que o arquivo HOST.TXT apresentava três problemas, sendo o primeiro, a sobrecarga de tráfego gerado na rede pela atualização do arquivo HOST.TXT em todas as máquinas, outro problema era o conflito de nomes, devido à entrada de novas máquinas à rede com nomes que já existiam no arquivo HOST.TXT, e, por último, era a dificuldade de manter a atualização durante a expansão da rede.

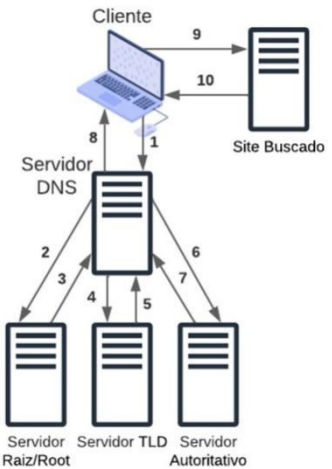
Com o intuito de solucionar essas falhas presentes no arquivo HOST.TXT. um novo sistema de nomes de domínio começou a ser desenvolvido nas RFCs (*Request for Comments*) 882, 883 e 973, mas foi somente na RFC 1034 e 1035 que o atual *Domain Name System* (DNS) foi ratificado.

Chen et. al. (2022), explicam que o DNS é um sistema de banco de dados hierárquico distribuído que mapeia endereços IP e de nomes de domínio e entre si. Tanenbaum e Wetherall (2011, p.612), exemplificam sua utilização como resolvedor/cliente enviando uma consulta contendo o nome para um Servidor DNS local, que procura o nome e retorna uma resposta contendo o endereço IP ao resolvedor. Trata-se, portanto, de uma estrutura de funcionamento simples e dividido em uma estrutura de dados em árvore para evitar sobrecargas.

Mas o DNS foi desenvolvido com o uso do protocolo UDP para evitar a latência do protocolo TCP, diferente do TCP o UDP não é criptografado, assim criando vulnerabilidades de DNS. Chen et al (2022), contam que devido à pequena escala da Internet da época, apenas a escalabilidade era considerada, sem considerar a privacidade e

segurança, assim possibilitando ataques *Man in the Middle* e de *DNS Spoofing*. Como meio de solução veio o DNSSEC especificado nas RFCs 4033, 4034 e 4035. Entretanto, para muitos se viu uma necessidade da criação de um novo DNS nativamente criptografado. A seguir, a figura 01 mostra um exemplo de consulta ao DNS.

Figura 01 – Exemplo de consulta ao DNS



Fonte: Os autores (2023).

Diante deste cenário, esta pesquisa tem por objetivo mostrar os novos tipos de DNS baseado no uso do protocolo QUIC e testar o *Round Trip Time* (RTT), além de compará-los com o DNS tradicional, através do uso de um proxy DNS.

A organização deste trabalho é a seguinte: a Seção 2 apresenta o referencial teórico dos protocolos de transporte UDP, QUIC e dos DNS com base no uso do protocolo QUIC, sendo ele os DNS over QUIC e DNS over HTTP/3, como

também um trabalho relacionado e os rumos das pesquisas do protocolo QUIC. Na Seção 3 apresenta-se a metodologia utilizada na pesquisa, configuração e testes. A Seção 4 expõe os resultados e discute sobre os dados obtidos. Por fim, a Seção 5 conclui este artigo.

2. Referencial Teórico

Nesta seção será abordado o referencial teórico que foi utilizado para o desenvolvimento desta pesquisa, uma explicação sobre os protocolos de camada de transporte UDP e QUIC, também introduzir os diferentes tipos de DNS: DNS over QUIC e DNS over HTTP/3 como apresenta um trabalho relacionado e os rumos das pesquisas do protocolo QUIC.

2.1 User Datagram Protocol (UDP)

O *User Datagram Protocol* (UDP) é um protocolo da camada de transporte que foi descrito na RFC 768. O UDP fornece uma maneira para os aplicativos enviarem datagramas IP encapsulados sem a necessidade do estabelecimento de uma conexão (Tanenbaum; Wetherall, 2011).

O protocolo UDP tem um funcionamento simples, sendo escrito em texto não criptografado. O cabeçalho UDP possui quatro campos, porta de origem e destino para identificar a aplicação. Só a porta de destino é obrigatória, seguindo depois pelo campo de comprimento com o tamanho total do datagrama e campo de *checksum* para verificação. O UDP encapsula os dados camada da aplicação e então encapsulados em um datagrama UDP que é enviado ao dispositivo destino (Barghash; Hammad; Gharaibeh, 2022). O UDP não oferece muitas funções quando comparado a outros protocolos de transporte, como o TCP. Assim, o UDP não possui mecanismo para garantir a chegada ao destino, retransmissão. Ele também

não faz controle de fluxo ou controle de congestionamento. Sendo um protocolo usado em aplicações que não são afetadas pela perda de dados ou a aplicação que necessitam uma maior velocidade na entrega dos dados como aplicações de tempo real.

Abaixo a figura 02 mostra os campos do cabeçalho UDP.

Figura 02 – Cabeçalho UDP

Fonte: Os autores (2023).

2.2 Protocolo QUIC

Este protocolo foi publicamente proposto pela Google em 2013 como *Quick UDP Internet Connections* (QUIC), mas na RFC 9000 padronizada pela IETF (*Internet Engineering Task Force*) optou pelo abandono do acrônimo, mas mantendo o QUIC como um nome do protocolo.

O QUIC é um protocolo de propósito geral, multiplexado que possui um estrutura de cliente/servidor, sendo construído sobre o UDP. O QUIC é visto como UDP pela rede e pelas *middlebox* (dispositivo intermediário na rede com outro objetivo que não o encaminhamento dos pacotes). Os benefícios disso são explicados por Haile et al (2022), sendo o QUIC implemento do lado do usuário que torna a atualização de novos recursos ao protocolo mais fácil.

O QUIC integra o *handshake* criptografado do TLS 1.3 para o estabelecimento de conexão em cliente/servidor, sua junção foi padronizada na RFC 9001. Sy et al (2019), explana o handshake criptografado do QUIC tendo dois estados o handshake completo com *Round Trip Time* (1-RTT), sendo

necessário para a conexão inicial entre o cliente-servidor, e com *Round Trip Time* zero (0-RTT), usado para a comunicação depois do estabelecimento de conexão inicial, utilizando informações armazenadas em *cache* de conexões anteriores entre o respectivo par cliente-servidor.

Outra vantagem do QUIC é o ID de Conexão que permite a migração da conexão a outra rede sem a necessidade de recarregamento da página. Num exemplo, com o uso do protocolo TCP quando um celular usa os dados móveis e troca para o uso de Wi-fi, nesse processo há uma troca de endereços IP ou porta, causando a perda de seção e recarregamento da página.

Zverev et al (2021), comenta que as conexões QUIC são organizadas em fluxos para evitar os atrasos produzidos pelo bloqueio de head-of-line existentes no TCP.

Um dos principais usos do QUIC foi na atualização do HTTPS (HTTP/2) com a sua definição válida atualmente RFC 9113, que objetiva aumentar o aproveitamento dos recursos de rede e diminuir a latência funcionando sobre TCP. Na atualização para o HTTP/3 padronizado na RFC 9114, manteve-se as funções anteriores, porém o TCP foi trocado pelo QUIC que possui vários recursos que são desejáveis, como multiplexação de fluxo, controle de fluxo por fluxo e estabelecimento de conexão de baixa latência.

2.3 DNS over QUIC (DoQ)

O DNS over QUIC foi padronizado em maio de 2022 pela IETF na RFC 9250, que trata de conexões de DNS dedicadas sobre o QUIC. O DoQ se baseia em três princípios, manter um padrão de segurança dos DNS criptografados, assegurar melhor validação de endereço de origem dos

servidores DNS comparado ao DNS tradicional e remover limitações do tamanho do MTU *(Maximum Transmission Unit)* para respostas DNS enviadas.

O DoQ segue o estabelecimento de conexão com o *handshake* do protocolo QUIC 1-RTT e pode oferecer retomada de conexão 0-RTT, enquanto o funcionamento do DNS de consulta/resposta mantém o padrão do DNS.

Chen et al. (2022), explica como o DoQ pode evitar efetivamente ataques tipo *man in the middle* e outros modos de ataque e assegurar efetivamente a privacidade dos usuários. Chen et al. (2022), ainda ressalta que atualmente apenas o resolvedor de DNS público do AdGuard DNS suporta o protocolo.

2.4 DNS over HTTP/3 (DoH3)

O DNS over HTTP/3 é evolução do conceito do DNS over HTTPS padronizado na RFC 8484, com a substituição do uso HTTPS para o uso de HTTP/3 padronizado da RFC 9114.

Até o presente momento desta pesquisa, não existem muitos artigos sobre o DNS over HTTP/3. Chen et al. (2022) propuseram o DNS over HTTP/3, onde usa o QUIC com UDP na camada de sessão e camada de transporte do HTTP/3, sendo a privacidade dos usuários efetivamente garantida pelo encapsulamento de mensagens DNS no protocolo HTTP/3, com a segurança dos dados para garantir pela criptografia TLS 1.3, tendo o *handshake* de 1-RTT e reconexão com 0-RTT do QUIC.

Um dos apoiadores do DoH3 é a Google,que no seu blog, Maurer e Yu (2022) anunciaram o suporte a DoH3 no Android.

2.5 Trabalho Relacionado

Batenburg (2022), pesquisou sobre a performance do DNS over QUIC, em busca de avaliar se o DoQ era mais rápido do que os outros DNS alternativos. Na pesquisa comparou quatro tipos de DNS, sendo eles: o DNS tradicional UDP, o DNS over LTS, o DNS over HTTPS e o DNS over QUIC.

A sua metodologia de pesquisa consiste na configuração de um servidor DNS autoritativo com software BIND9, tendo sido configurado com um nome de domínio, com também um resolvedor recursivo de DNS. O objetivo é de realizar os testes com múltiplos tipos de DNS, no entanto o BIND9 não possui suporte para todos os tipos de DNS avaliados, então em ambos foram instalados e configurados com o software dnsproxy da adguard com cada um dos tipos de DNS testados.

A pesquisa focou no tempo de resposta entre o solucionador recursivo e o servidor de nomes autoritário. Os testes foram feitos localmente e pela internet com servidores DNS localizados a Oeste da EU, Leste dos EUA, Leste da AU com o cliente estando na Holanda.

A conclusão obtida dos testes foi que o DNS sobre QUIC tem um efeito menor na latência de curtas e médias distâncias para um servidor de nomes, enquanto localmente e em longas distâncias outros tipos de DNS tiveram um desempenho ligeiramente melhor.

Entre as dificuldades apresentadas e trabalhos futuros estava a impossibilidade de testar o DNS over HTTP/3 pois não havia nenhuma ferramenta com suporte.

Recentemente a ferramenta Dnsproxy da Adguard foi atualizada e acrescentada o DNS-over-HTTPS com HTTP/3, que atua como o DNS over HTTP/3. Um dos objetivos nesta pesquisa utilizar de uma metodologia inspirada na pesquisa de

Batenburg (2022), para realizar testes com o DoQ e DoH3.

2.6 Rumos das Pesquisas do Protocolo QUIC

Para a busca de pesquisas sobre o QUIC, optou-se pelo uso do formato de uma revisão sistemática da literatura.

Uma revisão sistemática da literatura segundo Kitchenham (2004), é um meio que permite ao pesquisador identificar todas as pesquisas disponíveis relevantes e assim, avaliá-las e interpretá-las usando uma determinada questão de pesquisa. Assim, há várias razões para uma revisão sistemática da literatura. Kitchenham (2004), explica algumas razões como a de resumir as evidências existentes sobre um determinado tema e dá o exemplo de resumir as evidências empíricas dos benefícios como das limitações deste tema, ou a revisão servir de base para futuras pesquisas.

A presente pesquisa seguiu a proposta de revisão sistemática de Kitchenham (2004), que divide a revisão em três fases: Planejando a Revisão, Conduzindo a Revisão, Relatando a Revisão.

- Planejando a Revisão;
- Identificação da necessidade de uma revisão.
- Desenvolvimento de um protocolo de revisão.
- Conduzindo a Revisão;
- Identificação da pesquisa.
- Seleção de estudos primários.
- Avaliação da qualidade do estudo.
- Extração e monitoramento de dados.

Síntese de dados.
Relatando a Revisão;
Apresentação da revisão.

Além disso, Kitchenham (2004), salienta que os passos não são necessariamente sequenciais, mas também envolvem a iteração, principalmente no planejamento.

Seguindo as fases propostas por Kitchenham (2004), começa-se selecionando a palavra-chave e bases de dados a serem usadas para a revisão.

Escolheu-se como fonte de dados para pesquisa o portal de periódicos CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior), que contém um acervo com dezenas de bases de dados relacionados com a área pesquisada. A palavra-chave utilizada como termo de pesquisa foi QUIC.

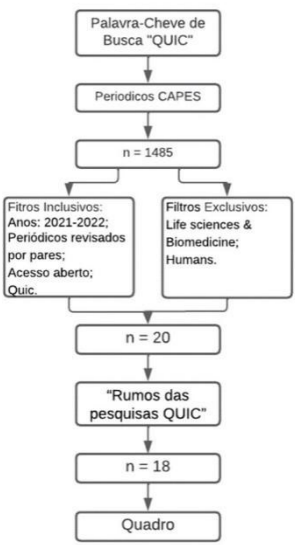
A busca inicial retornou com 1485 resultados de pesquisa. Após foram adicionados os filtros inclusivos, periódicos revisados por pares, como Kitchenham (2004), sugeriu como apropriado para estar em uma revisão, o filtro acesso aberto para leitura completa de todos os resultados e o filtros Quic, sendo uma palavra-chave.

Em seguida, foram aplicados os filtros restritivos, Life Sciences & Biomedicine, como o filtro Humans,para não retornar pesquisas relacionadas à área da saúde do acervo CAPES. Outro método de filtro foi o período da publicação, marcando os anos 2021 e 2022, para selecionar as publicações mais recentes sobre o tema. O resultado obtido foi de 20 publicações.

Seguindo as fases de Kitchenham (2004) a parte mais importante durante o planejamento é a criação da pergunta de pesquisa. Que fora definida como “Rumos das pesquisas QUIC?” pergunta que pretende analisar o foco das publicações recentes em dois, a melhora e testes do protocolo QUIC ou

aplicação do protocolo QUIC em uso diferentes como proposto inicialmente, simplificando os avanços no uso do QUIC e apresentar seus resultados. Com isso seguiu-se com leitura na íntegra das publicações para verificar compatibilidade com a pergunta de pesquisa. Assim duas publicações foram descartadas por não atender a pergunta de pesquisa, totalizando 18 publicações. Abaixo, segue a figura 03 com o procedimento da revisão e, no quadro 1, com análise das publicações com os resultados da revisão sistemática.

Figura – 03 Procedimento da revisão sistemática



Fonte: Os autores (2023).

Quadro 1 – Análise das publicações

Autor Ano	Teste, Melhoria	Avanço	Descrição da Publicação
KUHN et al., 2021		X	QUIC em sistemas de banda larga via satélite.
CHEN et al., 2021	X		Análise de segurança e comparação do TCP(TFO)/LTS 1.3, QUIC over Udp e QUIC/LTS 1.3.
ZHAN; WANG; TANG, 2021	X		Investigou a vulnerabilidade do GQUIC, IQUIC e HTTPS ao ataque WFP sob a perspectiva da análise de tráfego.
ZVEREV et al., 2021	X		Apresentação do rQUIC, uma integração do protocolo QUIC e um módulo de codificação FEC e seus testes comparando o rQUIC com QUIC.
LEE; AN, 2022	X		É proposto um algoritmo de autoajuste para suportar comunicação de baixa latência no protocolo QUIC.
FERNÁNDEZ et al., 2021		X	O desenvolvimento de nova implementação do MQTT com QUIC e a comparação em cenário de IIoT com o MQTT/TLS/TCP tradicional.
ZHANG et al., 2021	X		Desenvolvimento do protocolo de handshake QUIC e análise de segurança da criptografia com as ferramentas ProVerif e Verifpal.
HAILE et al., 2022		X	Desenvolvimento do RBBR usado para controle de congestionamento para rede de celulares.Feito com o algoritmo BBR, filtro de Kalman e QUIC.

SMITH; MITTAL; PERRIG, 2021	X		Utiliza métodos Fingerprinting no QUIC e compara com o TCP, os métodos Fingerprinting atuais não foram eficazes no QUIC.
KRÄMER et al., 2022		X	Avaliação de desempenho do MP-QUIC usando técnica trace-based, mostra resultados que podem superar o uso do single-path em celulares voláteis.
FIRMANSYA H; JUNG; KOH, 2021		X	Demonstração de desempenho superior de um proxy MP-QUIC entre os clientes e servidor IoT
BASYONI et al., 2021		X	Apresenta e faz uma análise de segurança e anonimato do QuicTor um projeto do uso do QUIC como solução para os problemas de desempenho da rede de anonimato Tor que emprega atualmente o TCP.
TAGA et al., 2022	X		Em um cenário com NAPT, com bloqueio QUIC faz experimentos de desempenho do QUIC com o pseudo cabeçalho TCP.
MATSUZAWA ; ICHIKAWA, 2022	X		Foco no desenvolvimento do período de transição para HTTP/3 Explica a futura ineficiência do Alt-Svc e propõe um novo método de verificação de conectividade para uso durante o período de transição, inova o algoritmo Happy Eyeballs.

HATONEN; RAO; TARKOMA, 2022		X	Apresenta o protótipo do MULTI uma solução para ulticonectividade que possibilita os aplicativos definirem os seus requisitos e possam ser ampliados para solicitar a rede os atenda feito, baseado no QUIC e MOSH
YAN; YU, 2022		X	É proposto o QQUIC (Quantum-assisted Quick UDP Internet Connections), uma modificação QUIC com distribuição quântica de chaves em vez dos algoritmos clássicos originais na etapa de troca de chaves e seus testes.
TRAN et al., 2021	X		Faz uma análise de desempenho entre HAS/3 que usa QUIC, e HAS/2 que usa TCP, onde o HAS/3 teve a vantagem.
BARGHASH; HAMMAD; GHARAIBEH, 2022		X	No QUIC comparado ao TCPa taxa de transferência RDMA é maior, o QUIC é mais rápido e melhor para transferir vídeos em sua taxa ideal e o DPDK funciona melhor em arquiteturas Intel. RDMA se encaixa na comunicação de data centers.

Fonte: Os autores (2022).

Através desta revisão podemos concluir um equilíbrio das pesquisas envolvendo o protocolo QUIC. Aqueles que buscam conhecer o limite do QUIC atual, propondo atualizações e correções, e aqueles que buscam adaptar o protocolo QUIC em outros segmentos, até então ocupados por outros protocolos, podendo essas implantações se transformarem em extensões do protocolo QUIC.

3. Materiais e Métodos

Essa pesquisa ocorreu em várias etapas, sendo a primeira a busca de pesquisas na literatura já existentes sobre os seguintes temas: protocolo QUIC, DNS e de DNS com uso do QUIC, para adquirir-se uma melhor compreensão sobre tais temas e tendo-se como propósito de definir e refinar os objetivos propostos na presente pesquisa e, assim aumentar o embasamento teórico. Optou-se pelo desenvolvimento de uma revisão sistemática sobre o QUIC, usando a metodologia de Kitchenham (2004), com os resultados sendo os conteúdos apresentado nas seções 1 e 2.

Nesta seção 3 explica-se de forma específica os dois testes realizados nesta pesquisa. O primeiro teste foi realizado em um cenário controlado, inspirado no método proposto por Batenburg (2022), visando a comparação entre os tipos de DNS que usam QUIC. Enquanto o segundo teste, em um ambiente não controlado, pretende-se compreender o tempo de resposta do estado atual dos servidores públicos de DNS alternativos para usuários localizados no Brasil, e comparar os resultados entre os tipos DNS.

A seção 4 expõe e discute os resultados obtidos nos testes desta pesquisa e, na seção 5, apresenta-se as considerações finais.

3.1 Teste em cenário de ambiente controlado

Para os testes em cenário de ambiente controlado foi implementado uma arquitetura Cliente/Servidor DNS, com um resolvedor recursivo e um servidor DNS autoritativo instalados em máquinas virtuais com o sistema operacional da distribuição Debian 11.5 com 3GB de RAM, utilizando o software de virtualização VirtualBox da Oracle.

Configuração do servidor DNS autoritativo: Foi instalado o software BIND9 como servidor DNS. O servidor foi configurado como servidor autoritativo e com o nome de domínio arthur.red.br com IP apontando para o próprio servidor.

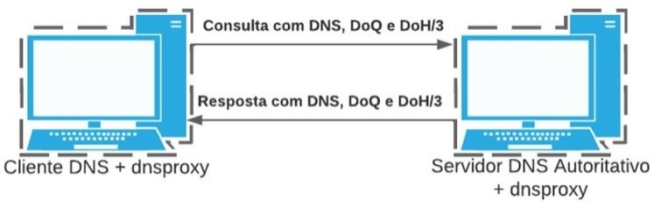
Como o BIND9 não possui suporte aos diferentes tipos de DNS, houve a necessidade do uso de um proxy DNS para fazer o encaminhamento dos múltiplos tipos de DNS, que foram necessários para este trabalho. Foi escolhido Dnsproxy da Aguard, até onde se sabe, é o único que suporta todos os DNS escolhidos para a pesquisa.

Configuração do resolvedor recursivo: Para a configuração do resolvedor recursivo o Dnsproxy da Aguard também foi usado para servir de encaminhador para a busca do nome de domínio registrado no DNS autoritativo.

Para a configuração se seguiu a documentação oficial do Dnsproxy da Adguard, tanto na configuração do servidor autoritativo quanto a do resolvedor recursivo. Tendo configurado com o DNS tradicional, DNS over QUIC, para ambos o Dnsproxy da Adguard segue a padronização das RFCs, mas sobre o DNS over HTTP/3 vale ressaltar que ele não possui padronização própria, assim sendo, seu suporte no Dnsproxy da Adguard é uma atualização do DNS over HTTPS, já pertencente a ferramenta com o uso do HTTP/3 em vez do HTTPS, com o nome declarado na ferramenta sendo como de DNS over HTTPS upstream com forçado HTTP/3, o funcionamento interno desta opção está fora do escopo desta pesquisa. O Dnsproxy foi configurado para salvar os registros da consulta em um arquivo de log, permitindo o processo de coleta e tratamento dos dados obtidos.

Testes realizados: Cada um dos DNS testados foi individualmente ativo no servidor DNS e no resolvedor recursivo durante seu teste, com um script. Realizou-se os testes executando cem vezes o comando de teste dig com um intervalo de 5 segundos, com o comando dig com o endereço ip de loopback (local) buscando arthur.red.br no endereço ip servidor DNS autoritativo, assim trazendo o registro A do nome de domínio arthur.red.br. Posteriormente, o script coletou os dados do RTT dentro do arquivo de log e gerou um novo arquivo. A figura 04 permite visualizar o cenário do teste.

Figura 04 - Teste em cenário de ambiente controlado



Fonte: Os autores (2023).

3.2 Teste em ambiente não controlado

O segundo teste feito, em um ambiente não controlado apresentado nesta pesquisa, está dividido em duas partes. Foram realizados testes no tempo de consulta de ida e volta (RTT) com a base de usuários localizados no Brasil. Para assim consultar os cinco sites com mais acesso no mundo, baseado na lista mensal da Similarweb (2022), sendo eles os sites do Google.com em primeiro, Youtube.com em segundo, Facebook.com em terceiro, Twitter.com em quarto e o Instagram.com em quinto, através do uso dos servidores de DNS públicos para todo os tipos DNS testados.

Os testes foram realizados em seis computadores

diferentes com uma máquina virtual instalada pelo VirtualBox da Oracle com o sistema operacional Debian 11.5 com 3GB de RAM da seguinte forma:

O primeiro teste visa coletar os dados do primeiro RTT obtidos da consulta a um site, pois ainda não possui *cache* do servidor, assim o DoQ e DoH3 tem um tempo mais longo já que tem que estabelecer uma conexão, ao contrário do DNS tradicional que não estabelece conexão, seu teste serve como para base de comparação. A realização do teste aconteceu com ativação individual de cada um dos tipos de DNS, todos foram configurados através do uso do Dnsproxy da Adguard, utilizando os servidores públicos de DNS de cada um dos três tipos de DNS testados. Os servidores públicos de DNS foram escolhidos através da documentação oficial do Dnsproxy da Adguard, para garantir maior compatibilidade.

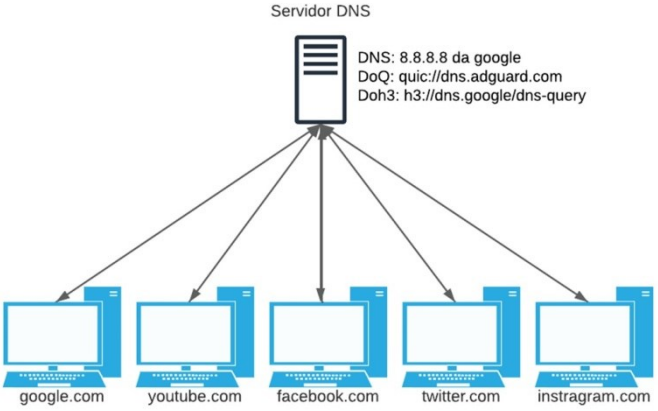
Assim, foram utilizados para os testes os servidores públicos. De DNS tradicional foi selecionado o 8.8.8.8 da Google. Para o DNS over QUIC foi utilizado o DNS da adguard quic://dns.adguard.com, e para de DNS over HTTPS upstream com forçado HTTP/3 o h3://dns.google/dns-query da Google. Assim, cada um dos cinco sites foram consultados 10 vezes para cada um dos três tipos de DNS. Para não deixar a ferramenta Dnsproxy obter *cache* ela foi reiniciada para cada uma das consultas individuais. Os dados de RTT foram registrados no log e extraídos por um script, como no teste anterior.

Para a segunda parte do teste em cinco máquinas diferentes, em que cada uma foi responsável por um dos cinco sites, com objetivo de mensurar o tempo médio em um site quando há cache, cada uma das máquinas seguiu a mesma configuração dos servidores públicos do teste anterior. Os testes foram realizados simultaneamente nas cinco máquinas

seguindo a ordem DNS tradicional, DNS over QUIC e DNS over HTTPS com HTTP/3.

Os testes foram efetuados com um script que executa em loop de 101 vezes o comando dig para um dos sites com um intervalo de 5 segundos entre cada consulta. Depois o script extraia o RTT do arquivo de log do Dsproxy em um novo arquivo. O primeiro dado coletado é descartado por estar estabelecendo a conexão, assim totalizando 100 amostras para cada tipo de DNS. Abaixo, a figura 05 demonstra o cenário usado para a segunda parte dos testes.

Figura 05 - Cenário de teste em ambiente não controlado



Fonte: Os autores (2023).

4. Resultados e Discussões

Nesta seção discutem-se os dados obtidos na realização dos dois ambientes de testes apresentados anteriormente na seção 3 desta pesquisa.

4.1 Discussão do teste em cenário de ambiente controlado

A realização dos testes em um cenário de ambiente controlado não foi possível, por problemas na criação da montagem do cenário. Não foi localizado qualquer material de apoio para a montagem da configuração do cenário, com relação aos múltiplos tipos de DNS, além da documentação do Dnsproxy da Adguard, onde não há um passo a passo. Assim sendo, foi necessário a criação através da tentativa e erro, porém pela falta de tempo para a pesquisa e limitação ao uso de recursos físicos, não foi possível a conclusão do experimento.

O erro apresentado foi provavelmente devido a um erro de configuração do servidor de DNS ou do Dnsproxy que não foi determinado. Com as configurações feitas, o comando de teste dig foi executado, ocorrendo uma falha, não retornando o endereço IP do domínio requisitado, como mostrado abaixo na figura 06.

Figura 06 - Print da tela do teste de execução

```
suporte@ns1:~/dnsproxy$ dig arthur.red.br @127.0.0.1

; <<>> DiG 9.16.33-Debian <<>> arthur.red.br @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 53116
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;arthur.red.br.                 IN      A

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Feb 08 11:42:23 -03 2023
;; MSG SIZE  rcvd: 31
```

Fonte: Os autores (2023).

4.2 Resultado do teste em ambiente não controlado

Esse teste tem por objetivo medir a média de tempo de consulta RTT do DNS tradicional, DoQ e DoH3. Esses resultados dependem da localização do usuário que realiza os testes, neste caso, os testes foram feitos no Brasil. Como já mencionado na seção anterior, o DNS tradicional não estabelece conexão. Os resultados esperados são tempos similares entres os 5 sites testados com o mesmo tipo de DNS.

Os resultados obtidos para o primeiro teste de tempo médio de resposta de primeira conexão em um ambiente não controlado são apresentados abaixo na tabela 1 e tabela 2.

Tabela 1 - Tempo médio de resposta de primeira conexão

Sites	DNS(ms)	DoQ(ms)	DoH3(ms)
google.com	46,74	309,63	156,27
youtube.com	73,43	304,31	202,59
facebook.com	20,66	503,08	129,83
twitter.com	18,51	287,33	127,95
instagram.com	25,71	312,89	130,29

Fonte: Os autores (2023).

Tabela 2 - Desvio padrão médio de resposta primeira conexão

Sites	DNS(ms)	DoQ(ms)	DoH3(ms)
google.com	48,10	41,99	50,65
youtube.com	47,00	51,42	56,74
facebook.com	1,59	241,00	36,01
twitter.com	0,82	39,35	33,97
instagram.com	16,37	62,75	35,10

Fonte: Os autores (2023).

Análise dos resultados do primeiro teste: No tempo médio da tabela 1 o DNS tradicional mostra-se mais rápido, como esperado, já que não há necessidade de estabelecer uma conexão como o DoQ e o DoH3, mas ele não é um opção não criptografada, assim não oferecendo o mesmo nível de segurança que as outras opções. O resultado indicou que DoH3 obteve um tempo mais rápido do que DoQ. Pode se teorizar pelo resultado que o DoH3 pode ter mais servidores do que o DoQ ou pela velocidade de funcionamento do DoH3 ser efetivamente mais ágil do que o DoQ, assim necessitando de mais testes para mais conclusões.

Na tabela 2 o DoQ e o DoH3 mostram-se mais oscilantes, pode-se teorizar que é devido à infraestrutura atual da rede com o DNS tradicional ser mais difundido, o que pode melhorar com a popularização dos novos DNS. Numa comparação entre o DoQ e DoH3, o DoH3 se demonstrou mais rápido e com menor oscilação, apesar de não muito diferente. Para o caso do Facebook do DoQ, que obteve um tempo mais alto, é provável que um gargalo tenha acontecido em algum ponto da rede no momento do teste, havendo assim um desvio maior, uma vez que o teste foi realizado com apenas 10 amostras.

Os resultados obtidos para o primeiro teste de tempo médio de resposta de uso contínuo em um ambiente não controlado são apresentados abaixo na tabela 3 e tabela 4.

Tabela 3 - Tempo médio de resposta de uso contínuo

Sites	DNS(ms)	DoQ(ms)	DoH3(ms)
google.com	35,92	132,20	29,55
youtube.com	37,14	128,69	25,99
facebook.com	19,68	128,00	22,66
twitter.com	18,39	124,01	21,03
instagram.com	19,85	129,17	21,85

Fonte: Os autores (2023).

Tabela 4 - Desvio padrão médio de resposta de uso contínuo

Sites	DNS(ms)	DoQ(ms)	DoH3(ms)
google.com	36,76	64,26	46,42
youtube.com	40,77	46,82	19,89
facebook.com	2,49	39,65	8,14
twitter.com	2,62	12,44	5,86
instagram.com	1,11	48,66	6,03

Fonte: Os autores (2023).

Análise dos resultados do segundo teste: O segundo teste mostra um resultado similar ao anterior, mas com DoH3 tendo demonstrado uma maior vantagem contra o DoQ, como também tendo um tempo similar ao do DNS tradicional, sendo este um resultado não esperado. Para determinar com veemência o motivo, seria necessário analisar o funcionamento interno da ferramenta Dnsproxy da Adguard e dos servidores públicos de DNS usados nos testes, o que está fora do escopo desta pesquisa, que foca somente em observar os tempos de resposta (RTT).

5. Considerações Finais

Com a popularização da Interne, novas tecnologias foram criadas para melhorar o desempenho e segurança da rede, como o novo protocolo de camada de transporte QUIC que possibilitou a melhoria dos DNS.

Assim, pessoas e empresas que prezam por uma melhor segurança no uso da Internet podem começar a utilizar novas opções de DNS mais seguras que o DNS tradicional e outras opções aos típicos DNS alternativos.

Essa pesquisa visou mostrar os conceitos e as características do QUIC, como seu uso no DNS com o DoQ e do DoH3, como também objetivou realizar testes de RTT entre os três tipos DNS.

Apesar de não ter sido possível concluir o primeiro experimento de teste que havia sido planejado para essa pesquisa, os resultados obtidos na primeira parte do segundo experimento de teste mostram a vantagem no RTT do DNS tradicional em relação aos outros, já que não realiza conexão.

Com os resultados entre o DoQ e DoH3 houve uma superioridade do DoH3, esse tempo pode ser atribuído por uma possível maior quantidade de servidores públicos DoH3, com esse tempo pode ser diminuído conforme mais servidores públicos de DoQ são adicionados a rede. Outro fator analisado é a própria agilidade do DoH3 contra o DoQ, o que necessita de mais pesquisa. Quanto à segunda parte do teste de tempo de uso contínuo mostrou ambos DoQ e DoH3 com tempos estáveis, com o DoH3 tendo um tempo similar ao DNS tradicional, sendo necessário mais pesquisas para uma conclusão exata.

Para trabalhos futuros, recomenda-se a implementação e teste do primeiro da subseção 3.2 e a aplicação do segundo teste com uma máquina virtual localizada em outros países para observar a diferença entre os tempos.

6. Referências

BARGHASH, A.; HAMMAD, L.; GHARAIBEH, A. Traditional vs. Modern Data Paths: A Comprehensive Survey. **Computers**, v. 11, n. 9, p. 132, 31 ago. 2022.

BASYONI, L. et al. QuicTor: Enhancing Tor for Real-Time Communication Using QUIC Transport Protocol. **IEEE Access,** v. 9, p. 28769–28784, 2021.

BATENBURG, B. **Performance of DNS over QUIC**. Essay (Bachelor)— EEMCS: Electrical Engineering, Mathematics and Computer Science:2022.

CASAGRANDE, Erich. **Top 100 sites mais acessados no Brasil [Edição 2022]**. Disponível em: <https://pt.semrush.com/blog/top-100-sites-mais-vi sitados/>. Acesso em 14 dez. 2022.

CHEN, Q. et al. Research on DNS Encryption Technology. **Lecture Notes in Electrical Engineering**, p. 1395–1405, 2022.

CHEN, S. et al. Secure Communication Channel Establishment: TLS 1.3 (over TCP Fast Open) versus QUIC. **Journal of Cryptology**, v. 34, n. 3, 24 maio 2021.

FERNÁNDEZ, F. et al. Even Lower Latency in IIoT: Evaluation of QUIC in Industrial IoT Scenarios. **Sensors**, v. 21, n. 17, p. 5737, 26 ago. 2021.

FIRMANSYAH, M. H.; JUNG, J.-H.; KOH, S.-J. Proxy-Based Adaptive Transmission of MP-QUIC in Internet-of-Things Environment. **Electronics**, v. 10, n. 17, p. 2175, 6 set. 2021

HAILE, H. et al. RBBR: A Receiver-Driven BBR in QUIC for Low-Latency

in Cellular Networks. **IEEE Access**, v. 10, p. 18707–18719, 2022.

HATONEN, S.; RAO, A.; TARKOMA, S. Programmable Session Layer MULTI-Connectivity. **IEEE Access**, v. 10, p. 5736–5752, 2022.

KITCHENHAM, B. **Procedures for performing systematic reviews**. Keele, UK, Keele University, v. 33, n. 2004, p. 1–26, 2004.
KRÄMER, Z. et al. On the Potential of MP-QUIC as Transport Layer Aggregator for Multiple Cellular Networks. **Electronics**, v. 11, n. 9, p. 1492, 6 maio 2022.

KUHN, N. et al. QUIC: Opportunities and threats in SATCOM. **International Journal of Satellite Communications and Networking**, nov. 2021.

LEE, S.; AN, D. Enhanced Flow Control for Low Latency in QUIC. **Energies**, v. 15, n. 12, p. 4241, 1 jan. 2022.

LIU, C.; ALBITZ, P. **DNS and BIND**. 5. ed. Sebastopol: O'Reilly Media, Inc., 2006.

MATSUZAWA, T.; ICHIKAWA, K. Implementation and Evaluation of HTTP/3 Connectivity Check Using Happy Eyeballs Algorithm. **Network**, v. 2, n. 3, p. 389–397, 28 jun. 2022.

MAURER, M.; YU, M. **DNS-over-HTTP/3 in Android Security Google Blog,** 19 jul. 2022. Disponível em: https://security.googleblog.com/2022/07/dns-over-h ttp3-in-android.html>. Acesso em: 12 dez. 2022

SIMILARWEB. **Ranking dos Sites Principais Sites Mais Visitados do Mundo**. Disponível em: <https://www.similarweb.com/pt/top-websites/>. Acesso em: 14 dez. 2022.

SMITH, J.-P.; MITTAL, P.; PERRIG, A. Website Fingerprinting in the Age of QUIC. **Proceedings on Privacy Enhancing Technologies**, v. 2021, n. 2, p. 48–69, 29 jan. 2021

SY, E. et al. A QUIC Look at Web Tracking. **Proceedings on Privacy Enhancing Technologies**, v. 2019, n. 3, p. 255–266, 1 jul. 2019.

TAGA, K. et al. Firewall Traversal Method by Pseudo-TCP Encapsulation. **IEICE Transactions on Information and Systems**, v. E105.D, n. 1, p. 105–115, 1 jan. 2022.

TANENBAUM, Andrew S; WETHERALL, David J. **COMPUTER NETWORKS**. 5. ed. Boston: Pearson, 2011.

TRAN, C. M. et al. Cross-Protocol Unfairness between Adaptive Streaming Clients over HTTP/3 and HTTP/2: A Root-Cause Analysis. **Electronics**, v. 10, n. 15, p. 1755, 21 jul. 2021.

YAN, P.; YU, N. The QQUIC Transport Protocol: Quantum-Assisted UDP Internet Connections. **Entropy**, v. 24, n. 10, p. 1488, 18 out. 2022.

ZHAN, P.; WANG, L.; TANG, Y. Website fingerprinting on early QUIC traffic. **Computer Networks**, v. 200, p. 108538, dez. 2021.

ZHANG, J. et al. Formal Analysis of QUIC Handshake Protocol Using Symbolic Model Checking. **IEEE Access**, v. 9, p. 14836–14848, 2021.

ZVEREV, M. et al. Robust QUIC: Integrating Practical Coding in a Low Latency Transport Protocol. **IEEE Access**, v. 9, p. 138225–138244, 2021.

Sistema de Monitoramento de Longa Distância Aplicado na Agricultura através de Rede LoRa®

Dionatan Justo da Luz[1], Marco Antonio Silveira de Souza[2]

[1] Acadêmico do Instituto Federal Catarinense – Campus Avançado Sombrio (IFC-CAS)
Caixa Postal 88960-000 – Sombrio – SC – Brasil

[2] Docente do Instituto Federal Catarinense – Campus Avançado Sombrio (IFC-CAS)
Caixa Postal 88960-000 – Sombrio – SC – Brasil

dionatanjusto99@gmail.com, marco.souza@ifc.edu.br

Abstract. *The present work deals with the development of a long-distance monitoring system to obtain some data in the field of agriculture, given the difficulty of connection in agricultural properties, which have a large territorial extension. The research aims to achieve a long range of data transmission between Heltec Esp32 Lora² modules, using the concept of Internet of Things (IoT) and radio frequency technology, Lora. For the execution of the proposed objective, technological research was carried out based on the Design Science Research methodology. Added new antennas, for a greater distance gain, compared to the ones that come originally. This project presented a viable solution for the farmer, meeting the expectations proposed in the development phase.*

Resumo. *O presente trabalho trata-se do desenvolvimento de um sistema de monitoramento de longa distância, para a obtenção de alguns dados no ramo da agricultura, tendo em vista a dificuldade de conexão em propriedades agrícolas, que possuem uma grande extensão territorial. A pesquisa tem como objetivo geral atingir um longo alcance de envio de dados entre módulos Esp32 LoRa® da Heltec, utilizando o conceito de Internet of Things (IoT) e tecnologia de rádio frequência, LoRa®. Para a execução do objetivo proposto, realizou-se a pesquisa tecnológica com base na metodologia Design Science Research. Adicionadas novas antenas, para um ganho maior de distância, comparando com as que vem originalmente. Este projeto apresentou uma solução viável para o agricultor, atendendo as expectativas propostas na fase de desenvolvimento.*

1. Introdução

A agricultura é uma das principais fontes econômicas no Brasil, influenciando o desenvolvimento do país. A cada ano que passa, o trabalho no campo se torna mais moderno, através da tecnologia, que vem em uma crescente evolução. Isso facilita e favorece muito a vida dos agricultores, pois os meios tecnológicos empregados nas lavouras faz com que a produtividade aumente, quando tais meios são usados a seu favor.

É indubitável que a questão de sinais ruins, tanto telefônicos, como redes sem fio em lugares mais distantes no campo, dificulta a ajuda que a tecnologia poderia oferecer. Também, há lugares onde esses sinais são alcançados, porém se encontram uma grande extensão territorial de plantio e não se consegue suprir toda a área trabalhada, deixando de oferecer o que ela poderia proporcionar.

Outrossim, destaca-se as condições climáticas, que por meio delas as plantas precisam para a sua sobrevivência e evolução, como sol, chuva, temperatura, umidade e etc. Todavia, essas condições climáticas também podem se tornar desfavoráveis e prejudiciais quando ocorrem fortes ventos, chuvas elevadas, granizos, umidades e temperaturas muito baixas ou elevadas. Tais condições acabam sendo vilãs para quem trabalha no campo, podendo causar uma grande perda na produção e se tornando um enorme prejuízo para o agricultor.

Neste contexto, o presente trabalho visa implementar uma solução que atenda às exigências de monitoramento ambiental onde a cobertura de sinal em redes, como 3G/4G ou WiFi, não são presentes. O principal objetivo é o desenvolvimento de um sistema de monitoramento e envio de dados através da conectividade entre módulos com uma tecnologia de rádio frequência, denominada rede LoRa. Esses dados coletados na agricultura, se dão por meio do sensor BME280, que acompanha fatores, como umidade, pressão atmosférica e temperatura do ambiente. Esta implementação é de grande importância para que os agricultores consigam estar informados, antes que alguma condição climática desfavorável ocorra e não os pegue de surpresa.

Para solucionar a questão de sinais ruins no campo e para lugares onde há muitos hectares de terra com plantações, onde a conectividade se torna um problema, foram implantadas também, junto com os módulos e a rede LoRa, antenas mais potentes, fazendo com que essa conexão alcance uma longa distância e consiga suprir esse problema. A comunicação ocorre pela transmissão dos dados coletados por sensor para o primeiro módulo, e este se comunicando e enviando os dados via rede LoRa para o segundo módulo, obtendo assim, o maior alcance de conexão possível, através das novas e mais potentes antenas.

Em seguida, foram comparadas essas antenas com aquelas que vem originalmente.

Ainda, foi feito o levantamento de todos os custos para a aplicação deste projeto. Por último, foi disponibilizado resultados finais em tempo real no painel visual Oled do módulo Esp32 LoRa Receptor.

2. Referencial Teórico

Para que sejam abordados os aspectos aos quais esse estudo se propõe, se faz necessário, primeiramente, realizar uma pesquisa abrangendo os principais assuntos que são relevantes ao desenvolvimento do projeto: agricultura de precisão, internet of things (IoT), rede LoRa®, módulo Esp32 LoRa®, sensor Bme280 e por fim, os trabalhos relacionados.

2.1 Agricultura de Precisão

O Ministério da Agricultura, Pecuária e Abastecimento define a agricultura de precisão como sendo "um sistema de gerenciamento agrícola baseada na variação espacial e temporal da unidade produtiva e visa ao aumento de retorno econômico, à sustentabilidade e à minimização do efeito do manejo agrícola ao ambiente" (MAPA,2018).

Portanto, a Agricultura de precisão (AP) consiste no uso diversificado de ferramentas de mecanização e automação através da tecnologia, sob medida dos fatores de produção, levando em consideração diversas variações, como temporal e espacial do potencial produtivo do ambiente e as necessidades específicas das culturas, a fim de aumentar a eficiência de seu uso e, assim, melhorar o rendimento econômico e reduzir o impacto da atividade agrícola no meio ambiente (Coelho; Silva, 2009).

Tanto o presente quanto o futuro da tecnologia na agricultura parecem promissores devido ao uso crescente de equipamentos de alto avanço tecnológico a custos mais baixos e

à elevação do nível educacional dos agricultores, que permitem maiores estruturas de apoio técnico à agricultura (Coelho; Silva, 2009).

.

2.2 Internet of Things (IoT)

O conceito de IoT ou “Internet das Coisas” em português, é uma amplitude da internet atual, permitindo que objetos do cotidiano, mas com capacitância computacional e de comunicação, possam ser ligados à Internet. A conexão permitirá controlar objetos remotamente e acessá-los como provedores de serviços. Novas aptidões desses objetos comuns criam muitas oportunidades nos campos acadêmico e industrial. No entanto, essas possibilidades carregam riscos e figuram ampla gama de desafios técnicos e sociais (Santos, 2016).

São sistemas automatizados que conseguem fazer múltiplos serviços, desde acender as luzes e aquecer sua comida quando percebem que você está voltando do trabalho para casa. Acessórios inteligentes que permitem compartilhar com amigos quanto tempo você passou a pé ou de bicicleta durante o dia na cidade ou sensores que alertam automaticamente os fazendeiros em seus múltiplos trabalhos. Todos esses exemplos são manifestações do que são consideradas tecnologias inovadoras ligadas à ideia de que a IoT está sendo construída (Magrani, 2018).

Há muitas diferenças no conceito de IoT, portanto, não há uma única ideia que possa ser considerada pacífica ou unificadora. De maneira geral, pode ser pensado como um ambiente onde objetos físicos são conectados à Internet por meio de minúsculos sensores embarcados, criando um ambiente computacional ubíquo, voltado para facilitar o dia a dia das pessoas, introduzindo soluções práticas em tarefas rotineiras. Todas as definições da IoT se concentram em como computadores, sensores e objetos interagem uns com os

outros e processam informações e dados em um ambiente hiper conectado (Magrani, 2018).

As tecnologias cuja identificação se dá por meio de radiofrequência e de redes de sensores sem fio, estão se tornando mais acessíveis. Há um potencial de crescimento muito significativo para a aplicação de conceitos de IoT no setor agrícola, e assim surgiu o termo smart farms (fazendas inteligentes). Nessas fazendas, o agricultor faz uso dessas tecnologias relacionadas à localização móvel, associadas através de rastreamento e monitoramento de objetos em tempo real (Kaloxylos, 2012).

2.3 Rede LoRa®

LoRa® foi desenvolvida pela Semtech Corporation e promovida pela LoRa® Alliance. A tecnologia LoRa®, cujo nome significa Longo alcance, é uma nova tecnologia de comunicação sem fio. Uma organização com associação aberta e objetivos sem fins lucrativos que inclui grandes corporações globais com interesse no desenvolvimento e uso da rede LoRa® para a IoT (Teixeira; Almeida, 2017).

Suas principais características, além da comunicação à longa distância, também se dão pela imunidade a ruídos, consumo reduzido de energia e segurança de dados, assim justificando o seu uso em ambientes rurais (Augustin, 2016).

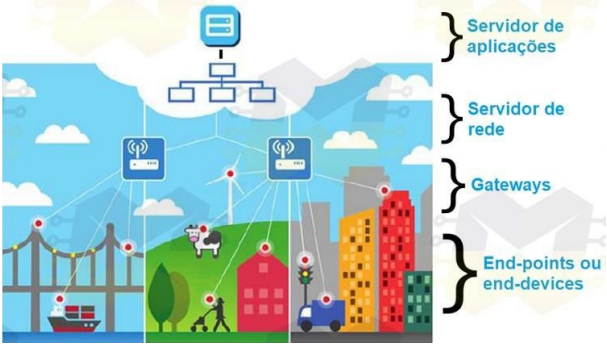
Alguns conceitos são necessários para compreender melhor o funcionamento das redes LoRa®. Complementando, o sistema consiste em um módulo instalado nos dispositivos finais e nos gateways. Esses componentes permitem que os dados saiam de uma rede LoRa e se conectem a servidores locais ou remotos por meio de uma conexão IP. Os módulos enviam e recebem dados dos gateways de maneira semelhante às redes WiFi, mas com um alcance muito maior. Suas principais aplicações para o sistema de IoT, incluem sensores remotos e

monitores de pressão, luz, temperatura, umidade e outras variáveis. Particularmente aqueles que funcionam com baterias e, em certos casos, estão localizados em locais distantes (Pereira; Cruvinel, 2019).

Outras tecnologias de transmissão de dados, como WiFi, Bluetooth e Zigbee, estão disponíveis para atender à demanda de IoT. No entanto, quando detectados com a tecnologia LoRa, apresentam algumas desvantagens. A tecnologia de comunicação LoRa apresenta a melhor relação custo-benefício, com características que a tornam uma escolha adequada para a instalação de redes de sensores sem fio para uso em áreas rurais, com alcance de até surpreendentes 5 km, mas quando turbinado, pode chegar perto de 11 km (Silva, 2017).

Os transceptores LoRa, ou seja, um dispositivo utilizado para a comunicação entre microcontroladores em longas distâncias, esses disponíveis comercialmente, usam frequências de mega-hertz dentro de bandas não licenciadas como 433MHz, 868MHz e 915MHz. Algumas nações estabeleceram as faixas de frequência nas quais as mesmas entidades poderiam operar. Nos Estados Unidos, Austrália e Brasil, essa frequência é de 915 MHz (CATTANI, 2017).

Figura 1. Arquitetura da Rede LoRa.



Fonte: Oliveira (2019).

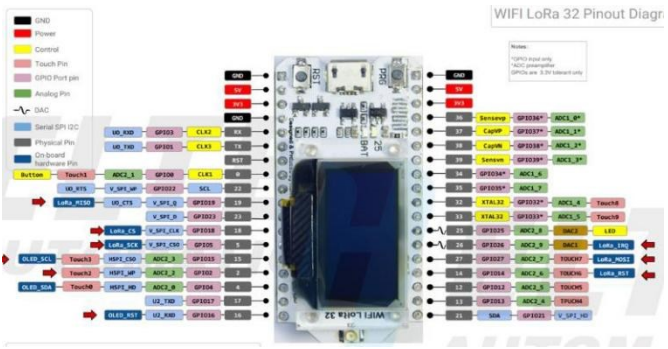
2.4 Módulo Esp32 LoRa®

A placa LoRa ESP32 Heltec é descendente do ESP8266 e foi criada como resultado da união de LoRa e ESP32. Por incluir WiFi, Bluetooth e LoRa, esta é uma plataforma completa de hardware e software projetada para prototipagem de Internet of Things (Oliveira, 2019).

A Placa também possui um Display OLED de 0,96" 128X64, ou seja, uma tela ou dispositivo usado para apresentar informações, que permite exibir em tempo real, consequentemente, toda a purificação das informações que pode ser verificada sem o uso de uma ferramenta externa. Também há um conector U. FL padrão de 2 mm para a conexão da antena no lado da tela (Oliveira, 2019).

Ainda, Segundo Oliveira (2019), uma das vantagens de se utilizar a Placa LoRa ESP32 é a possibilidade de conectar módulos e sensores ao dispositivo para coleta de dados ou execução de ações, sendo que tudo pode ser obtido ou ativado através da comunicação LoRa. Além disso, é possível criar uma interface para que as informações obtidas pelo LoRa sejam acessadas via Bluetooth ou WiFi e posteriormente disponibilizadas online, por exemplo, utilizando o protocolo TCP/ IP, MQTT ou IFTTT.

Figura 2. Pinagem do módulo Esp32 LoRa da Heltec.



Fonte: (Pereira; Cruvinel, 2019).

2.5 Sensor BME280

O baixo consumo de energia e o tamanho do sensor BME280, desenvolvido especificamente para aplicações móveis e de pequena escala, são fatores cruciais para sua construção. O dispositivo tem a capacidade de combinar alta exatidão e precisão para medições de temperatura, pressão e umidade. Seu sistema ideal teria baixo consumo de energia, estabilidade duradoura e alta robustez. É crucial para o presente trabalho que a sensibilidade à unidade apresente uma resposta rápida. A sensibilidade à pressão exibe alta precisão e resolução e um nível de erro toleravelmente baixo. O sensor de temperatura foi projetado com a intenção de apresentar baixo ruído e maior precisão que outros sensores (BOSCH, 2015).

2.6 Trabalhos Relacionados

Existem alguns trabalhos acadêmicos relacionados com a tecnologia LoRa. Portanto, como essa tecnologia é nova, se encontra menos quando envolvida com a agricultura. Trabalhos de Zanoti; Moraes (2013) e Oliveira; Souza (2013), apresentam aspectos semelhantes e relacionados à comunicação de sensores

de fio, coletando dados da agricultura. Porém, nenhum usa a metodologia de envio de dados através de rede LoRa e nem se faz o uso de antenas, fazendo com que a distância seja pequena entre a conexão das placas.

O primeiro trabalho, de Zanoti; Moraes (2013) é sobre o monitoramento da bananicultura e o segundo, de Oliveira; Souza (2013), é sobre Smart Farms (fazendas inteligentes) em uma pequena lavoura de maracujá. Ambos com o propósito de coletar dados da agricultura, como temperatura e umidade e enviar esses dados para o destino escolhido através de outras tecnologias de redes sem fio.

O trabalho em relação aos dos citados anteriormente, tem o propósito de aprimorar todo sistema, desenvolvendo com alguns aspectos a mais e se diferenciando pela questão do uso da rede LoRa, sendo potente e moderna, ganhando uma longa distância de comunicação, através de novas antenas. Também, não só focando em uma plantação específica, mas na agricultura de modo geral.

Outros trabalhos que contribuíram para esse projeto e todo o referencial teórico, foram dos seguintes autores: Santos (2016), Magrani (2018), Teixeira (2017), Pereira; Cruvinel (2019).

3. Aspectos metodológicos

Este projeto de pesquisa quanto a seus métodos é denominado como uma pesquisa tecnológica. Segundo Cupani (2006), o objetivo da pesquisa tecnológica é o conhecimento prescritivo, pois a vida artificial consiste em sistemas que são adaptados ao seu entorno para fins humanos específicos, bem como objetos (artefatos) que são fabricados de acordo com planos e especificações e possuem propriedades desejadas.

Para a realização dos objetivos deste trabalho, empregou-se a Design Science Research Methodology

(DSRM). De acordo com Carstensen; Bernhard (2019), a metodologia de pesquisa em ciência do design é uma abordagem qualitativa na qual o próprio processo de design é o objeto de estudo. Em outras palavras, gera conhecimento tanto sobre o método utilizado para projetar uma obra quanto sobre a própria obra.

A seguir, as características de cada um dos passos da metodologia deste trabalho, que serão mencionados na figura 3:

Figura 3 - Metodologia

Fonte: Adaptado de Jappur (2014).

Na etapa 1, é apresentado os problemas e as motivações deste trabalho. Em primeiro lugar, é evidente que a falta de acesso a sinais telefônicos e redes sem fio em áreas mais remotas do campo dificulta qualquer assistência que a tecnologia possa oferecer.

Ainda assim, existem locais onde esses sinais são alcançados. No entanto, esses locais costumam ter uma expansão territorial significativa da lavoura e não conseguem abranger completamente a área de trabalho, privando-a da capacidade de fornecer todo o conforto e assistência que poderia oferecer.

Também se destaca as condições climáticas das quais as plantas dependem para sua sobrevivência e desenvolvimento, incluindo luz solar, precipitação, temperatura, umidade e outras. No entanto, as mesmas condições climáticas também podem se tornar desfavoráveis e prejudiciais quando ocorrem ventos fortes, chuvas fortes, granizos, umidade e temperaturas extremamente baixas ou altas. Isso acaba sendo uma grande desvantagem para todos que trabalham na agricultura e tem o potencial de causar perdas significativas na produção e prejuízos ao agricultor.

A seguir, se encontra a etapa 2, mostrando os objetivos e soluções do problema, que visa desenvolver um sistema de monitoramento e transmissão de dados utilizando a conectividade de módulos e a tecnologia de radiofrequência conhecida como rede LoRa. Os dados coletados na agricultura são fornecidos pelo sensor Bme280 que rastreia fatores como umidade, pressão atmosférica e temperatura do ambiente. Esta solução é fundamental para que os agricultores possam ser informados em caso de condições climatéricas desfavoráveis, para que não sejam apanhados de surpresa.

Juntamente com os módulos e a rede LoRa, também foram instaladas antenas mais fortes para garantir que essa conexão pudesse chegar à longas distâncias e resolver o problema de ruínas no campo, bem como áreas onde existem muitos hectares de terra cobertos por plantações.

Na etapa 3 encontra-se o design e o desenvolvimento do artefato criado, mostrando todas ferramentas e tecnologias necessárias para realização do projeto.

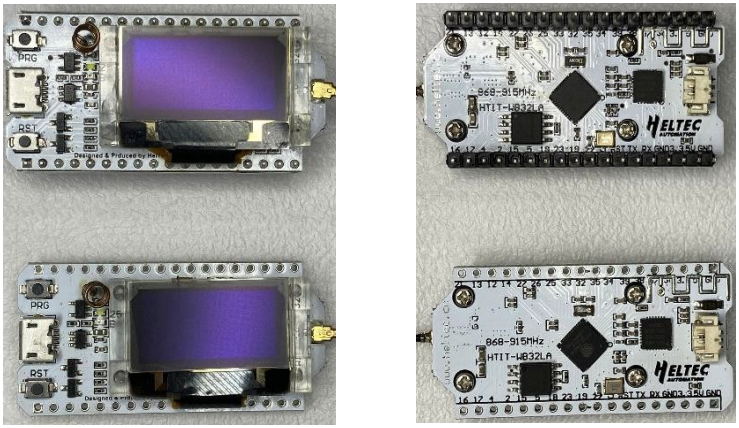
Responsável pelas coletas dos respectivos dados, como temperatura, umidade e pressão atmosférica em pascal, tem-se o Sensor BME280, demonstrado na figura 4.

Figura 4. Sensor BME280.

Fonte: Autor (2022).

A seguir, os dois microcontroladores ESP32 LoRa da Heltec, 915mhz, com os displays. Na figura 5, observa-se a frente e a parte de trás dos módulos.

Figura 5. Frente e atrás dos Módulos Esp32 LoRa Heltec,915mhz.



Fonte: Autor (2022).

Na figura 6, as antenas originais, com 915mhz e 2dbi, que vem juntamente com os módulos.

Figura 6. Antenas originais do Esp32 LoRa Heltec, 915mhz e 2dbi

Fonte: Autor (2022).

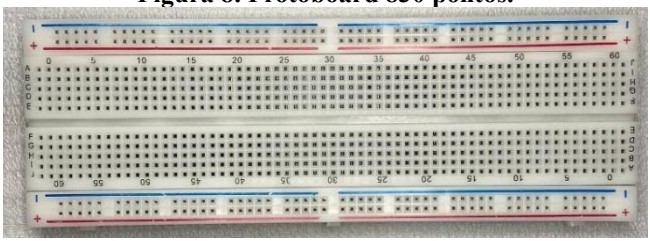
Já, na figura 7, encontra-se as novas antenas obtidas, 915mhz e 6dbi, para se ter um maior alcance de conectividade.

Figura 7. Antenas maiores, 915mhz e 6dbi.

Fonte: Autor, (2022).

O software utilizado para programar os módulos foi o Arduino IDE versão 2.0.2. A linguagem usada foi a C++. Também foram necessários quatro cabos jumpers fêmea-macho para fazer a conectividade entre o sensor BME280 e uma das placas Esp32 LoRa Heltec. Por fim, foi utilizada uma protoboard com 830 pontos, como é mostrada na figura 8.

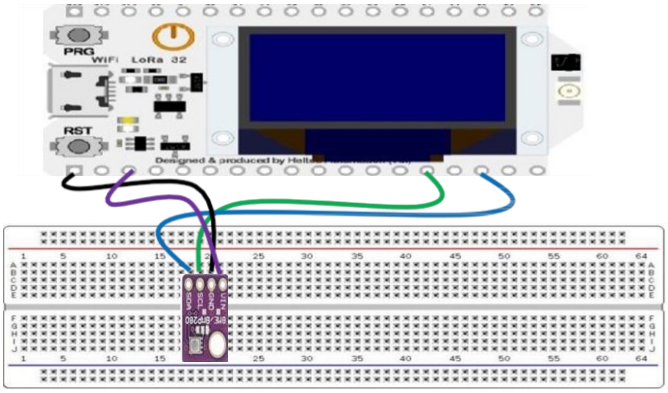
Figura 8. Protoboard 830 pontos.



Fonte: Autor (2022).

Na etapa 4 encontra-se a implementação do projeto, exemplificando o artefato real. A figura 9 mostra a conexão do sensor BME280 com o módulo Esp32 LoRa. Este módulo se chamará de Emissor, que será responsável de mandar os dados lidos pelo sensor para o segundo módulo, o Receptor.

Figura 9. Conectividade entre o sensor BME280 e o módulo Esp32 LoRa Emissor.

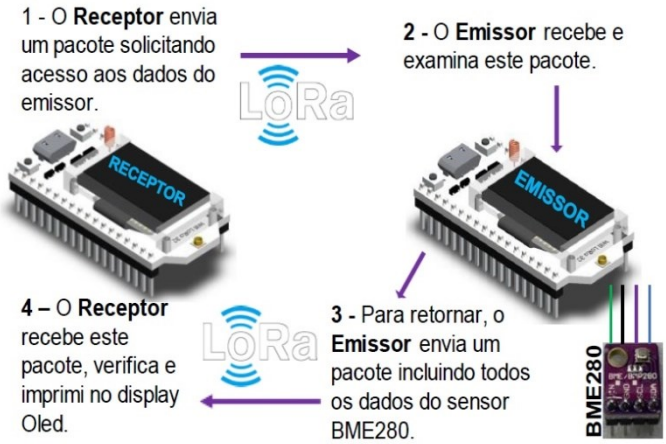


Fonte: Autor (2022).

Na figura 10, observa-se a comunicação destes módulos por rádio frequência LoRa. Primeiro, o receptor enviará um

pacote para o emissor, para receber os dados. Em seguida o emissor receberá o aviso, encaminhando para o módulo receptor os dados lidos pelo sensor BME280.

Figura 10. Comunicação entre os dois módulos Esp32 LoRa Heltec.



LoRa Heltec. Fonte: Autor (2022).

A etapa 5 consiste na avaliação do projeto. Foi visto, anteriormente, todos os passos e reavaliados para obter um resultado melhor. Conclui-se que todos os passos mostrados nas etapas anteriores foram alcançados com sucesso. A respeito dos alcances de sinais via rádio frequência, foram satisfatórios com as antenas originais. Já com as antenas novas obteve-se um salto ainda mais longe.

Por fim, a etapa 6 prevê a publicidade do projeto, valorizando e ajudando aqueles que pretendem estudar e obterem informações sobre determinados assuntos discutidos no trabalho.

4. Resultados e discussão

Antes de dar início aos resultados, é importante salientar que após a programação estar toda pronta no Arduino Ide, compilava-se o programa feito em C++ nos módulos, porém não funcionava. Foram dois dias de pesquisa, para que fosse encontrado a causa do problema. O SDA e o SCL do sensor Bme280 estavam mais precisamente nos pinos 21 e 22 colocados pela Heltec, tendo que modificar a pinagem I2C do Esp32 LoRa, pois a biblioteca da Adafruit não aceita esses pinos. Mudando assim para 4 e 15 respectivamente. Sendo assim, sem essa alteração não funcionaria o sensor Bme280 no módulo, fazendo que não coletasse nenhum dado.

Portanto, a figura 11 mostra os seguintes pinos alterados, encontrado através do arquivo: C:\Users\dionatan\AppData\Local\Arduino15\packages\esp32\hardware\esp32\1.0.6\variants\heltec_wifi_lora_32.

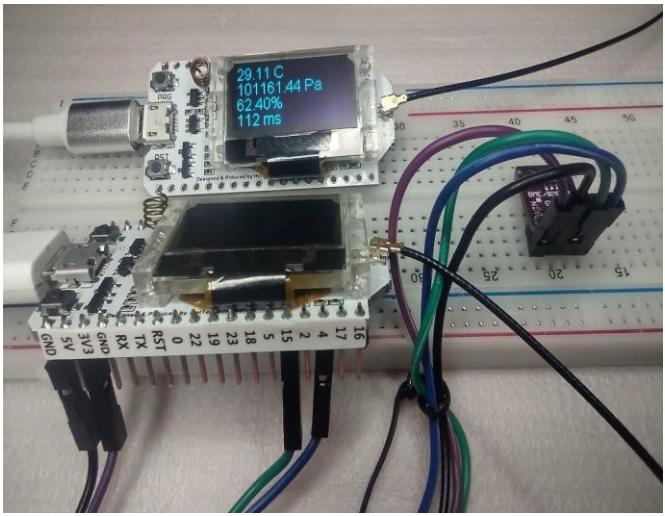
Figura 11. Modificação dos pinos no SDA e SCL.

```
//static const uint8_t SDA = 21;
//static const uint8_t SCL = 22;
static const uint8_t SDA = 4;
static const uint8_t SCL = 15;
```

Fonte: Autor (2022).

Segue a apresentação do artefato pronto após a resoulução do problema, mostrado na figura 12, a seguir.

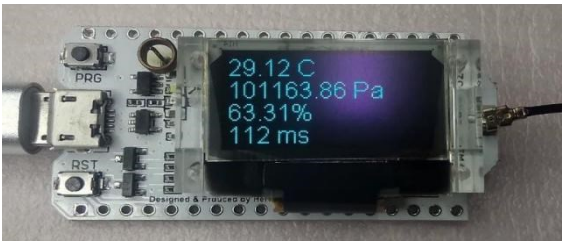
Figura 12. Artefato montado.



Fonte: Autor (2022).

Na figura 13observa-se de perto o display Oled do módulo Esp32 LoRa, denominado Receptor. Na primeira linha encontra-se a temperatura do ambiente em graus Celsius, na segunda, a pressão atmosférica em hectopascal, já na terceira linha, é a umidade em porcentagem. E por fim, na última linha mostra o tempo que o módulo emissor levou para obter os dados e encaminhar para o módulo receptor em milissegundos.

Figura 13. Módulo Receptor com os dados recebidos e impressos no display Oled.



Fonte: Autor (2022).

A seguir, os respectivos testes foram feitos em área rural mostrando a distância alcançada de cada uma das antenas, tanto as originais, quanto as de 6dbi, obtidas para um ganho maior de alcance.

O primeiro teste foi feito em uma área rural, onde há muitos obstáculos entre a transmissão dos dois módulos, como casas, diversidade de vegetações, árvores pequenas e grandes, entre outros. As antenas foram deixadas aproximadamente 1,5 metros do chão e todos cálculos de distâncias foram feitos em linha reta. Com as antenas originais conseguiu-se sem falha alguma, 210 metros de distância entre um e outro. Após, continuou-se recebendo dados, mas com algumas falhas e travamentos, obtendo-se, assim, um alcance de 360 metros. O mesmo teste foi realizado com as antenas mais potentes, onde na primeira etapa, sem falhas, se obteve 460 metros. A partir de então começaram as falhas e travamentos, conseguindo atingir um alcance de até 640 metros.

O segundo teste foi feito em uma propriedade rural plana, onde em 80% da mesma se encontra plantações de arroz, tendo assim poucos obstáculos à frente, mostrada a seguir nas imagens obtidas através do Google Maps. A linha traçada do ponto A (módulo emissor) ao ponto B (módulo receptor), mostrará a distância alcançada em linha reta.

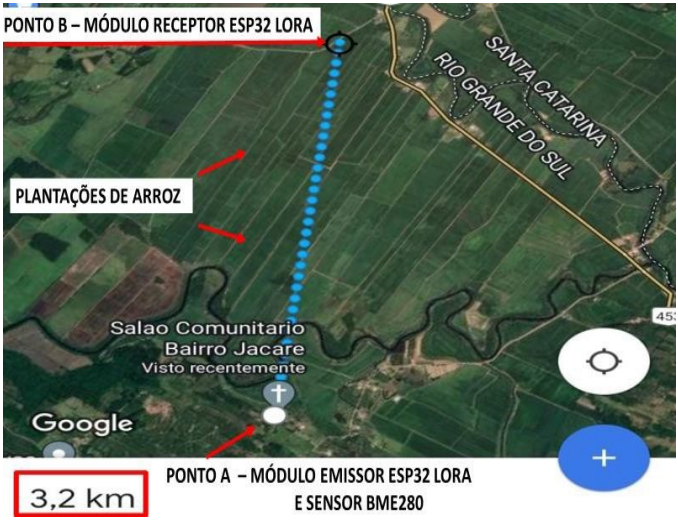
Primeiramente, testes realizados com as antenas

originais, onde o ponto A estava na encosta de um morro, em torno de 20 metros de altura, e o ponto B a 1,5 metro do chão. Ao centro destes pontos havia plantações de arroz.

Conseguiu-se aproximadamente 3,2 km de alcance (mostrado na figura 14), surpreendendo e muito com essa distância alcançada, para tão pequena antena. Supondo então, que alcance o mesmo na direção que corte a linha traçada, para uma propriedade rural, consegue-se suprir o total de 1.024 hectares de terra.

Por fim, testes realizados com as antenas maiores de 6dbi, onde o ponto A estava no mesmo lugar anteriormente, e o ponto B em uma lombada em torno de 5 metros de altura. Conseguiu-se aproximadamente 11 km de alcance (mostrado na figura 15), surpreendendo ainda mais com toda esta distância alcançada. Supondo, então, que alcance o mesmo na direção que corte a linha traçada, para uma propriedade rural, consegue-se suprir um total de 12.100 hectares de terra.

Figura 14. Resultado obtidos na agricultura com as antenas originais.



Fonte: Autor (2022).

Figura 15. Resultado obtidos na agricultura com as antenas maiores de 6dbi.

Fonte: Autor.

Por fim, tiveram-se custos para a montagem do projeto. A tabela 1 mostra todos equipamentos usados, com seus respectivos valores e o total gasto.

Tabela 1. Custos para a realização deste projeto.

EQUIPAMENTOS	QUANT.	VALOR CADA	VALOR FINAL
Módulo Wifi Esp32 LoRa Heltec, SX1276 868/915Mhz, display Oled	2	R$ 104,00	R$ 208,00
Sensor BME280 4 pinos - Datasheet	1	R$ 88,00	R$ 88,00
Antena para LoRa 868/915Mhz, 6dbi + cabo Ipex, 50 ohm	2	R$ 89,00	R$ 178,00
Protoboard 830 pontos	1	R$ 39,90	R$ 39,90
Conectores jumpers fêmea/macho	4	R$ 2,00	R$ 8,00
Soldagem dos Pinos no Esp32	1	R$ 20,00	R$ 20,00
Cabo micro usb	2	R$ 25,00	R$ 50,00
		VALOR TOTAL GASTO =	R$ 591,90

Fonte: Autor (2022).

5. Considerações finais

Era evidente que os sinais ruins no campo atrapalhavam muito o desenvolvimento da agricultura em relação ao uso da tecnologia. Mesmo onde eram encontrados esses sinais, o grande espaço territorial no campo, atrapalhava a tecnologia por não conseguir suprir toda extensão de plantio. Outro fator, são as condições climáticas desfavoráveis, que se torna um grande empecilho para o agricultor, podendo levar a um enorme prejuízo quando pego de surpresa, trazendo uma grande preocupação.

Para isto, foi implantado o sensor Bme280, para a obtenção de dados e envio para o módulo Emissor, encaminhando para o módulo Receptor, trazendo assim mais segurança para o agricultor em relação às condições climáticas, podendo se precaver antecipadamente. Foram implantadas, também, novas antenas para um ganho de distância maior, quando o terreno for de grande extensão, assim a tecnologia podendo ajudar.

Este projeto apresentou uma solução viável para trazer mais conforto para o agricultor e principalmente segurança, pois sabe-se que a agricultura se dá pelo trabalho árduo do homem no campo, mas também necessita de sorte em relação ao clima, pois muitas vezes são investidos uma quantia considerável alta de dinheiro e trabalho, para em algumas horas de tempestade se perder tudo.

Obteve-se um ganho significativo de conexão em áreas mais planas e com poucos obstáculos, alcançando múltiplos hectares, podendo-se, assim, coletar dados da terra, enviar ao fazendeiro ou agricultor e este em sua casa coletar todas as informações recebidas momentaneamente.

Por fim, como recomendação para trabalhos futuros que possam dar continuidade a este, ou seguir de exemplo e ajuda, pode ser desenvolvida a implantação de um servidor web, com um design visual trazendo todas informações obtidas através de sensores e uma visão mais profissional. Também se pode implementar antenas ainda mais potentes, porém tendo um custo mais elevado.

6. Referências

AUGUSTIN, Aloÿs et al. A study of LoRa: Long range & low power networks for the internet of things. Sensors, v. 16, n. 9, p. 1466, 2016.

BOSCH Sensortec. Datasheet: BME280 Combined humidity and pressure sensor. Alemanha, publicação electronica, 55p. 2015.

CARSTENSEN, Anna Karin; BERNHARD, Jonte.
Design science research – uma ferramenta poderosa para melhorar os métodos na pesquisa em educação em engenharia. European Journal of Engineering Education. 2019.

CATTANI, M., et al., An Experimental Evaluation of the Reliability of LoRa Long-Range Low- Power Wireless Communication. Journal of sensor and actuator networks. P.4-6, 2017.

COELHO, J. P. C; SILVA, J. R. M. Inovação e Tecnologia na formação agrícola. Associação dos Jovens Agricultores de Portugal. Lisboa. 2009.
CUPANI, Alberto. La peculiaridad del conocimiento tecnológico.
ScientiaeStudia, São Paulo, v. 4, n.
3, p. 353-71, 2006. Disponível em: < http://www.scielo.br/pdf/ss/v4n3/a01v4n3.pdf>. Acesso em: 06 abr. 2012.

JAPPUR, R. F. Modelo conceitual para criação, aplicação e de jogos educativos digitais. Universidade Federal de Santa Catarina. Florianópolis, SC. 2014.

KALOXYLOS, A. et al. Farm management systems and the Future Internet era. Computers and Electronics in Agriculture, 2012.

MAGRANI, Eduardo. A internet das coisas. Editora
FGV, 2018.

MINISTÉRIO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO. (MAPA). Projeções do Agronegócio.
Projeções de Longo Prazo. Brasília- DF, 2019.

OLIVEIRA, Euler. conhecendo-a-placa-wifi-lora- esp32-433mhz-868mhz-915mhz. Disponível em https://blogmasterwalker shop.com.br/embarcados/esp32/conhecendo-a- placa-wifi-lora-esp32-433mhz-868mhz-915mhz. 2019.

OLIVEIRA, Jadson da Silva; SOUZA, Jhonatan Matos. Smart Farm –

Monitoramento de temperatura e umidade de uma pequena lavoura de maracujá. 2013.

PEREIRA, Maurício; CRUVINEL, Paulo.
Desenvolvimento de um sistema de coleta automática de dados agrícolas baseado em rede LoRa e no microprocessador ESP32. In: Anais da X Escola Regional de Informática de Mato Grosso. SBC, 2019.

SANTOS, Bruno P. et al. Internet das coisas: da teoria à prática. 2016.

SILVA, Jonathan de Carvalho et al. LoRaWAN—A low power WAN protocol for Internet of Things: A review and opportunities. In 2nd International Multidisciplinary. 2017.

TEIXEIRA, Grazielle Bonaldi; ALMEIDA, João Víctor Peroni de. Rede LoRa® e protocolo LoRaWAN® aplicados na agricultura de precisão no Brasil. Trabalho de Conclusão de Curso. Universidade Tecnológica Federal do Paraná. 2017.

ZANOTI, Marcelo Rocha; MORAES, Priscila.
Monitoramento de temperatura e umidade na bananicultura através de rede de sensores sem fio. 2013.

SD-WAN: Um estudo bibliográfico sobre esta tecnologia

Clóvis Ficagna Junior[1], Jéferson Mendonça de Limas[2], Marco Antônio Silveira de Souza[3]

[1]Acadêmico do Curso Superior de Tecnologia em Redes de Computadores – Instituto Federal Catarinense – Campus Avançado Sombrio (IFC-CAS) 88960-000 – Sombrio – SC – Brasil

[2,3]Docentes do Curso Superior de Tecnologia em Redes de Computadores – Instituto Federal Catarinense – Campus Avançado Sombrio (IFC-CAS) 88960-000 – Sombrio – SC – Brasil

clovisficagnajr@gmail.com, {jeferson.limas, marco.souza}@ifc.edu.br

Abstract. *The objective of this article is to bring in an uncomplicated way, an overview of software-defined long-distance networks, or SD-WAN, and how this technology can contribute to the improvement of communication using long-distance networks. A bibliographic research was used as methodology. It used a bibliometric method, considering only articles published in different databases that had the term SD-WAN in the title. Some conclusions were verified after the analysis of the data collected, it is noteworthy that the SD-WAN technology had a jump in interest in the last 6 years, which shows a trend in understanding its operation and its advantages. The use of SD-WAN*

technology in the face of increasing internet demand by connected devices, becomes the solution not only for reducing the overhead faced by traditional WAN networks, but also for the advantages of infrastructure and costs involved.

Resumo. *O objetivo deste artigo é trazer, de forma descomplicada, uma visão sobre redes de longa distância definidas por software, ou SD-WAN, e como esta tecnologia pode contribuir na melhoria da comunicação utilizando redes de longa distância. Foi utilizada uma pesquisa bibliográfica como metodologia. A pesquisa utilizou-se de uma bibliometria, considerando apenas artigos publicados em diferentes bases de dados que traziam o termo SD-WAN no título. Algumas conclusões foram verificadas após a análise dos dados colhidos, destaca-se que a tecnologia SD-WAN teve um salto no interesse nos últimos 6 anos, o que mostra uma tendência na compreensão do seu funcionamento e suas vantagens. A utilização da tecnologia SD-WAN diante da demanda cada vez maior de internet por parte dos dispositivos conectados, passa a ser a solução não apenas para a diminuição da sobrecarga enfrentada pelas redes WAN tradicionais, como pelas vantagens de infraestrutura e custos envolvidos.*

1. Introdução

Redes de computadores são essenciais para a comunicação nos mais diversos segmentos empresariais. Elas são responsáveis pela comunicação interna na empresa, tanto através da *LAN* (*Local Area Network*), ou Rede Local, quanto pela comunicação externa da empresa com suas filiais, fornecedores e até mesmo com os funcionários, quando estes estiverem em trabalho remoto através da *WAN* (*Wide Area Network*), ou Rede de Longa Distância.

Com o aumento do tráfego de dados, principalmente pela internet, a utilização das redes, em especial as *WANs*, estão cada vez mais sobrecarregadas, impactando diretamente na utilização da largura de banda. Espera-se um aumento da largura de banda da *WAN* na casa de 20% a cada ano (LIU, et al, 2015). No cenário atual, as tecnologias *WAN* tradicionais não são capazes de lidar com a quantidade de dados que trafega atualmente e com este aumento na largura de banda.

Considerando estes fatores e suas consequências para o futuro das *WANs* tradicionais, torna-se indispensável a utilização de Redes de Longa Distância definidas por Software (*SD-WAN*).

Esta nova realidade é uma quebra de paradigmas, primeiro, por se tratar de uma tecnologia de "virtualização" da rede, uma abstração da estrutura da rede *WAN* que conhecemos e estudamos até hoje. Segundo, por trazer mudanças significativas na sua infraestrutura, funcionamento, gerenciamento entre outros benefícios. A virtualização já é a solução para uma grande parte de serviços computacionais, como *Storage* (Armazenamento), Infraestrutura de Rede, *Software* e outros. No que se refere a redes de computadores, principalmente as *WANs*, ela muda a percepção como as organizações enxergam a sua rede externa, diminuindo, e até mesmo eliminando a necessidade de uma infraestrutura interna,

responsável por todo acesso aos recursos da empresa.

O objetivo deste artigo é fazer uma explanação sobre o conceito, infraestrutura e o funcionamento da tecnologia *SD-WAN*.

2. Referencial Teórico

Neste tópico, serão destacados os pontos a serem analisados na pesquisa para uma melhor compreensão dos termos e conceitos que balizam este trabalho. Dentre eles, destacam-se: Conceituando *SD-WAN* (seção 2.1), Infraestrutura *SD-WAN* (seção 2.2) e o Funcionamento (seção 2.3).

2.1 Conceituando SD-WAN

Inicialmente, é preciso compreender que uma rede *WAN* tem por objetivo a comunicação entre *endpoints* (pontos) em locais distintos, por isso se trata de uma rede de longa distância. Estes *endpoints* podem estar em redes distintas em qualquer lugar do mundo. De acordo com (Tanenbaum, et. al, 2021), uma *WAN* é uma rede com uma cobertura até mesmo continental, que pode ser classificada como *WAN* Corporativa, atendendo uma empresa, como também pode ser considerada um serviço, no caso de uma rede de trânsito, como exemplo, a Internet. Para que esta rede de longa distância se estabeleça, são necessários equipamentos como roteadores, tanto no lado da matriz quanto da filial, um serviço de acesso à *internet* contratado junto a um provedor de *internet* ou um *MPLS* (link dedicado) contratado de uma empresa de telecomunicações, *switches* para a comutação entre os pontos da rede *LAN*. Esta é a infraestrutura mínima necessária nos pontos onde se quer a conexão, como por exemplo, a matriz e as filiais de uma empresa.

SD-WAN é a virtualização de recursos para a entrega de serviços, desempenho e disponibilidade em redes de longa distância *WANs*. De acordo com (Uppal, et. al, 2018), a grande diferença entre o modelo de *WAN* tradicional e a *SD-WAN* é a

separação do Plano de Controle (*Control Plane*) do Plano de Dados (*Data Plane*).

Conforme (Gordeychik; Kolegov, 2018), define-se *SD-WAN* como uma aplicação específica de Redes Definidas por Software (*SDN*) para redes de longa distância *WAN*. Segundo os autores, a tecnologia *SD-WAN* é uma tendência em se tratando de redes de longa distância, principalmente quando se considera a virtualização como uma solução para a crescente demanda de recursos computacionais em todos os segmentos.

Segundo (Michel; Keller, 2017), a tecnologia *SD-WAN* não faz uso de *hardware* dedicado e nem tecnologias especializadas, pois facilita a utilização de *switches* virtuais abertos e de Interfaces de Programação de Aplicativos (*APIs*) configuráveis. O grande diferencial da tecnologia *SD-WAN* é a separação dos planos de dados e controle da rede *WAN*, o que facilita o gerenciamento, a tomada de decisão, a segurança e a escalabilidade da rede.

Plano de Dados é a camada da rede responsável pela manipulação dos pacotes de dados que trafegam pela rede. Enquanto que o Plano de Controle é o responsável pela administração e gerenciamento das políticas estabelecidas na rede (Montoanelli, 2020).

Ainda, segundo o autor, no modelo tradicional de *WAN*, temos estes dois planos integrados nos equipamentos que compõem a rede *WAN*, como roteadores e *switches* de camada 3. Para que a rede possa ser escalável (expansível), é necessário muito trabalho manual dos analistas para, por exemplo, a inclusão de um novo site (local) na infraestrutura da rede *WAN* da empresa. Com a separação dos planos de dados e controle, esta "inclusão" do novo local na rede *WAN* da empresa se torna muito menos trabalhosa e mais eficiente, tendo em vista que o plano de controle da rede está localizado em um servidor e a operação pode ser feita de qualquer lugar, sem que haja a

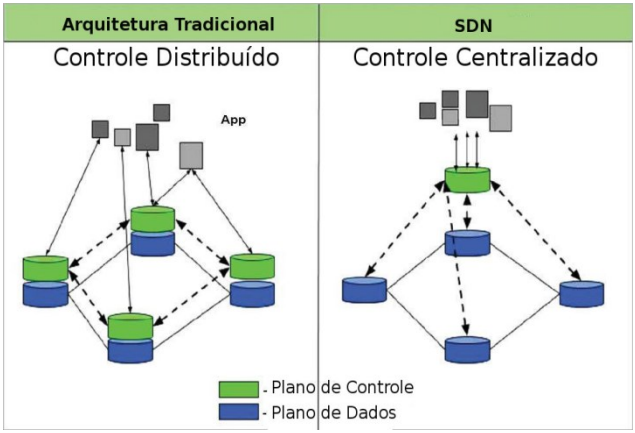
necessidade de uma visita do analista responsável no local a ser incluído na rede (Alves, 2020).

2.2 Infraestrutura *SD-WAN*

Com a separação dos planos de controle e plano de dados, o controlador é o responsável pela orquestração da rede (plano de controle). Toda a gerência da rede acontecerá neste dispositivo (ALVES, 2020).

Abaixo, a figura traduz como se dá a separação dos planos.

Figura 1. Rede Tradicional vs. Rede SDN



Fonte: errc.sbc.org.br 2019.

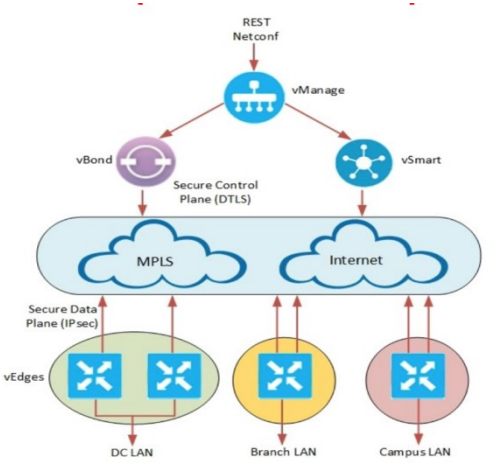
De acordo com a figura 1, na arquitetura tradicional temos os dois planos integrados num mesmo hardware, por exemplo, um roteador. O controle fica distribuído nos equipamentos que compõem a topologia, enquanto que na arquitetura *SDN* temos o controle centralizado, o qual fica responsável pela gerência dos equipamentos do plano de dados,

por exemplo, um *switch.* Conforme (Camera, Zanetti, 2019), algumas vantagens do desmembramento dos planos de dados e controle são a gerência unificada dos membros da rede, uniformização do comportamento de diferentes dispositivos de rede, como roteadores, *switches, firewalls*.

Diferentemente do plano de controle, o plano de dados fica restrito ao tráfego destes dados, responsável pelo roteamento dos pacotes previamente estabelecido pelo controlador da rede.

Nas infraestruturas *SD-WAN*, a topologia se apresenta conforme o exemplo a seguir.

Figura 2. Topologia *SD-WAN*_CISCO.



Fonte: www.routexp.com 2019.

A figura 2 representa a topologia *SD-WAN* Cisco e seus elementos.

Na base desta topologia, estão os equipamentos que operam na borda da rede dos clientes, que podem ser um *DC* (Data Center), uma Filial de uma empresa, ou até mesmo um

Campus. Estes equipamentos da borda da rede interna dos clientes utilizam *links* de internet ou mesmo *links* dedicados *MPLS (MultiProtocol Label Switching)* para acessarem a *Cloud* (Nuvem), local remoto onde estão localizados os equipamentos responsáveis pelo plano de controle da *SD-WAN*. O plano de controle na topologia da figura 2 é composto por elementos como o *vBond*, *vSmart* e o *vManage*.

O *vBond* trata-se de um software responsável pela autenticação inicial de dispositivos da borda da rede do cliente, os vEdges.

O *vSmart*, também baseado em software, é o responsável pela conexão segura entre os roteadores e a distribuição das rotas.

Já o *vManage*, compõe o plano de gerência da solução Cisco *SD-WAN*. Trata-se de um ambiente com uma *GUI* (Graphic User Interface) ou interface gráfica que monitora a operação da solução *SD-WAN Cisco (Brainwork, 2020).*

Esta comunicação entre os equipamentos de borda do cliente e os equipamentos do plano de controle se dá através de túneis criptografados, também chamados de *Secure Channel* (Canal Seguro). É por este canal que trafegam as informações que trafegam na rede. A literatura define que as tecnologias que migram para as *Clouds*, independentemente de serem públicas ou privadas, criam possibilidades de adaptação às mais diversas situações apresentadas, principalmente pelas empresas, que é a parte mais interessada na solução das questões envolvendo a tecnologia (Michel, Keller, 2017).

2.3 Funcionamento *SD-WAN*

Uma Rede de Longa Distância definida por Software (*SD-WAN*), diferentemente de uma Rede *WAN* tradicional, utiliza um orquestrador, que é o responsável pela gerência da

rede.

Este orquestrador é um software rodando em um servidor localizado em uma nuvem, que pode ser pública ou privada. No interior desta nuvem, está localizada a infraestrutura *WAN* virtualizada que fará a autenticação de acesso dos equipamentos de borda localizados nos clientes. Após a autenticação, os equipamentos já se encontram "conectados" à rede *SD-WAN,* portanto, a partir de agora, são gerenciados pelo controlador desta rede.

Segundo (Uppal, et. al 2018), ainda há mais benefícios do uso da *SD-WAN,* como a possibilidade de utilização de mais de um tipo de *link* para o transporte dos dados, como por exemplo, MPLS, já citado anteriormente, *LTE* (4G) tecnologia da rede celular e a própria Internet. A disponibilidade de redundância de *links* de saída dos dados melhora o desempenho das redes, visto que se a queda de algum dos *links* ocorrer, existirá a possibilidade de saída dos dados por outros caminhos e ao mesmo tempo, evita um eventual congestionamento da rede, visto que se utiliza ao mesmo tempo, mais de um caminho para a saída destes dados possibilitando o balanceamento de carga entre os links.

3. Metodologia

A proposta para este artigo foi uma pesquisa tecnológica, com base em artigos e periódicos relacionados à área pesquisada. Como fonte de pesquisa, foram utilizadas bases de dados de conhecimento científico reconhecidas no meio acadêmico.

A metodologia utilizada foi a pesquisa bibliográfica. Segundo (Marcelino, 2020), o pesquisador faz uso de material já construído e publicado por outros autores acerca do tema inicial. De posse deste material, extrai o conhecimento necessário para a produção do trabalho, que no caso deste artigo, é a coleta dos

dados referentes ao foco da pesquisa.

Para a realização da pesquisa bibliográfica, foi iniciada uma bibliometria referente ao tema central proposto pelo artigo, *SD-WAN*. A partir desta definição, foram consultadas 3 bases de dados de publicações científicas, o Portal de Periódicos da *CAPES*, a Base Scopus e a Base de Dados *IEEE* Xplore. Ficou definido que a consulta a estas bases de dados levaria em conta apenas artigos publicados e que no seus respectivos títulos, contivesse o termo *SD-WAN.* Iniciou-se, então, a pesquisa nas referidas bases de dados*,* delimitando a apuração do número de publicações sobre o tema no período de tempo de 12 meses a contar do primeiro ano em que houve a primeira publicação. Apuradas as quantidades publicadas versus o ano da publicação, foi construída uma tabela que continham esses dados. Essa tabela deu origem a um gráfico, que ilustra a evolução no interesse sobre o assunto *SD-WAN* ao longo do tempo.

4. Resultados e Discussões

Abaixo, seguem os resultados das pesquisas realizadas nas bases de dados acima mencionadas.

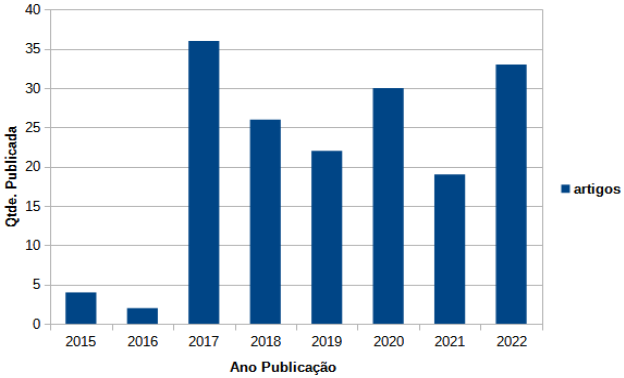
Tabela 1: Relação Ano x Quantidade

BASE DE DADOS CAPES	
ANO PUBLICAÇÃO	QUANTIDADE PUBLICADA (Artigos)
2015	4
2016	2
2017	36
2018	26
2019	22
2020	30

2021	19
2022	33

Fonte: Autores, 2023.

Gráfico 1: Quantidade Artigos x Ano Publicação.



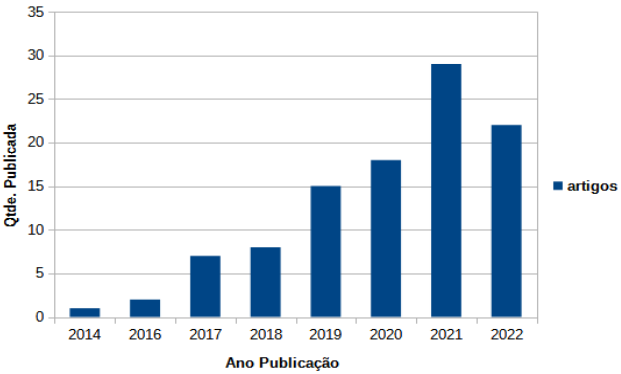
Fonte: Autores, 2023.

Tabela 2: Relação Ano x Quantidade

BASE DE DADOS SCOPUS	
ANO PUBLICAÇÃO	QUANTIDADE PUBLICADA (Artigos)
2014	1
2016	2
2017	7
2018	8
2019	15
2020	18
2021	29
2022	22

Fonte: Autores, 2023.

Gráfico 2: Quantidade Artigos x Ano Publicação.



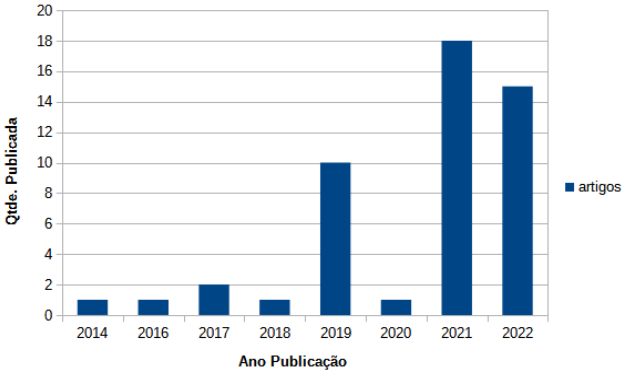
Fonte: Autores, 2023.

Tabela 3: Relação Ano x Quantidade

BASE DE DADOS IEEE XPLORE	
ANO PUBLICAÇÃO	QUANTIDADE PUBLICADA (Artigos)
2014	1
2016	1
2017	2
2018	1
2019	10
2020	1
2021	18
2022	15

Fonte: Autores, 2023.

Gráfico 3: Quantidade de Artigos x Ano Publicação.



Fonte: Autores, 2023.

Algumas conclusões são extraídas a partir da análise das tabelas e dos gráficos gerados sobre cada uma das bases analisadas. Ambas indicam um início de interesse sobre o assunto entre 2014 e 2015. Tendo em vista que a demanda sobre as redes *WAN* tradicionais não se comparava com o atual cenário, já havia a percepção de que o crescimento era inevitável e que soluções deveriam ser propostas para mitigar possíveis problemas nas *WANs* tradicionais.

A tecnologia foi ganhando relevância conforme a necessidade de implementação foi aumentando. Fatores como o aumento cada vez maior de dispositivos conectados, a virtualização como solução para diversos serviços computacionais, inclusive como *IaaS* (*Infraestructure as a Service*), infraestrutura como um serviço e a possibilidade de um gerenciamento centralizado, trouxeram a necessidade do uso da *SD-WAN* como solução completa e principalmente acessível.

5. Considerações Finais

A proposta inicial do artigo foi trazer uma breve explanação sobre o conceito de uma rede de longa distância definida por software, *SD-WAN,* sua infraestrutura e seu funcionamento.

A tecnologia *SD-WAN,* naturalmente, requer um conhecimento mais aprofundado sobre redes de computadores. Entretanto, a utilização desta tecnologia trará vantagens como as apresentadas no artigo, além do que, o custo de implementação será reduzido uma vez que a infraestrutura pode ser simplificada utilizando a existente no cliente. *SD-WAN*, também, surge como uma alternativa às *VPNs* (*Virtual Private Networks*), Redes Privadas Virtuais, não só pelo fato da conexão entre sites (localidades) ocorrer através de túneis criptografados, portanto, garantindo a segurança, como pelo fato de que, diferentemente das *VPNs*, pode conectar mais de dois sites ao mesmo tempo.

6. Referências

ALVES, João Pedro Camara. **Emulação de Roteamento Ciente de Aplicação em uma SD-WAN.** Trabalho de conclusão de curso, Universidade Federal Fluminense – Escola de Engenharia. Niterói, Rio de Janeiro, 2020.

CAMERA, Pedro Eduardo, ZANETTI, Alisson Borges. **Introdução à linguagem de programação P4, o futuro das redes**. Minicurso em Escola Regional de Redes de Computadores, 2019. Disponível em <https://errc.sbc.org.br/2019/mc/camera2019p4.pdf>. Acesso em: 15 de Nov. 2022.

GORDEYCHIK, Sergey and KOLEGOV, Denis. **SD-WAN Threat Landscape**. 2018. Disponível em <https://www.ArXiv.org>. Acesso em: 14 de Out. 2022.

LIU, Shuhao and LI, Baochun. **On scaling software-defined networking in wide-area networks. Tsinghua Science and Tecnology,** 20, (3), p.221-232, 19 de jun 2015.

MARCELINO, Carla Andréia Alves da Silva. **Metodologia da Pesquisa**, Contentus, 2020. Disponível em <https://plataforma.bvirtual.com.br/Leitor/Publicacao/186505/pdf/54?code=8vkgjRUqaF8Gxyd64cNxCTMSh+Ia+ndvYbh2x+iN4asYx+zt9SaQw8GmX+I/Ck8cauev1KiXVS1cSWYHUtP0UQ==>. Acesso em: 04 de Fev. 2023.

MICHEL, Oliver and KELLER, Eric. **SDN in wide-area networks: A survey. Fourth International Conference on Software Defined Systems (SDS)**, p. 37-42, 2017.

MONTOANELLI, Guilherme. **SD-WAN ganha visibilidade e se destaca como grande aliada na viabilização da transformação digital nas empresas.** 2020. Disponível em <https://www.mobiletime.com.br/artigos/09/09/2020>. Acesso em: 18 de Nov. 2022.

Ortega, About André. **Conceitos e Componentes Cisco SD-WAN**. 2020. disponível em:<https://brainwork.com.br/2020/06/30/conceitos-e-componentes-cisco-sd-wan/>. Acesso em: 08 de Dez. 2022.

Route-XP – Network Baseline Project. **Cisco SD-WAN Solution Viptela: Architecture Components and Configuration**. 2019. Disponível em:<https://www.routexp.com/2019/05/cisco-sd-wan-solution-viptela.html>. Acesso em 13 de Nov. 2022.

SANJAY, Uppal, WOO, Steve, PITT, Dan. **SD-WAN for Dummies**. John Wiley Sons, Inc., Hoboken, New Jersey, 2018.

TANENBAUM, Andrew, FEAMSTER, Nick, WETHERALL, David. **Redes de Computadores**. 6ª ed. Bookman, 2021. Disponível em:<https://books.google.com.br/books?id=DNFJEAAAQBAJ&hl=pt-BR&source=gbs_slider_cls_metadata_9_mylibrary&redir_esc=y>. Acesso em: 15 de Dez. 2022.

SystemPsi: Sistema Gerenciador para Psicólogos em Atuação Remota

Luís Antônio Scarabelot Fiabani[1], Sandra Vieira[2], Rosemary de Fátima de Assis Domingos[2], Tainá Fiabani[3]

[1] Discente do Instituto Federal Catarinense, Câmpus Sombrio
Sombrio – SC – Brasil
[2] Docente do Instituto Federal Catarinense, Câmpus Sombrio
Sombrio – SC – Brasil
[3] Mestra em Psicologia Clínica, IMED
Passo Fundo – RS – Brasil
{luisfiabani, tainafiabani}@gmail.com,
{sandra.vieira, rosemary.domingos}@ifc.edu.br.

Abstract. *This article presents the process of developing a technological tool to assist psychology professionals working in the modality of remote care. This form of action, although already used especially in the pandemic, required these professionals to adapt to the new reality that did not allow social contacts. In addition, the pandemic increased the need for psychological care, given the increase in the number of people who needed these psychology professionals. It is noteworthy that the development process of the proposed tool had the integral monitoring of a professional in the field of psychology who participated in all stages, especially those that involved the tests of the tool.*

Resumo. *Este artigo apresenta o processo de desenvolvimento de uma ferramenta tecnológica para auxiliar os profissionais da psicologia que trabalham na modalidade de atendimento remoto. Esta forma de atuação, embora já tenha sido utilizada, sobretudo na pandemia, exigiu que estes profissionais se adequassem à nova realidade que não permitia contatos sociais. Além disto, a pandemia incrementou a necessidade de atendimentos psicológicos, dado o aumento do número de pessoas que necessitaram destes profissionais. Destaca-se que o processo de desenvolvimento da ferramenta*

proposta teve o integral acompanhamento de um profissional da área da psicologia que participou de todas as etapas, principalmente àquelas que envolveram os testes da ferramenta.

1. Introdução

As Tecnologias da Informação e Comunicação (TICs) contribuem com a difusão e a democratização dos serviços de ajuda e apoio à saúde mental, possibilitando que as pessoas tenham acesso ao uso desses serviços por meios mais otimizados. O Conselho Federal de Psicologia (CFP), no ano de 2018, por meio da resolução 011/2018, permitiu a aplicação dos serviços de psicologia através das TICs (CONSELHO FEDERAL DE PSICOLOGIA, 2018).

De acordo com a resolução, o profissional que pretende utilizar o modelo de atendimento online necessita cumprir algumas determinações, tais como, estar com o registro no Conselho Regional de Psicologia (CRP) ativo e realizar cadastro na plataforma virtual disponibilizada pelo CFP denominada *e-psi*[3]. A plataforma *e-psi* está disponível para a comunidade. O objetivo da plataforma é otimizar a busca por psicólogos previamente cadastrados e aptos para atender na modalidade remota, ou seja, de forma não presencial, mas *online* via recursos

[3]Segundo o CFP (2023) "O e-Psi lista as(os) profissionais que estão autorizadas(os) pelo Sistema Conselhos de Psicologia a prestarem serviços psicológicos on-line. Se a(o) profissional não estiver listada(o), ela(e) não está autorizada(o) a prestar esse serviço."

tecnológicos digitais (CONSELHO FEDERAL DE PSICOLOGIA, 2018).

A partir de março de 2020, com a chegada da pandemia da COVID-19[4], observou-se que a demanda por atendimento psicológico cresceu consideravelmente no Brasil. Estudos realizados durante a pandemia apontaram dentre uma série de fatores, que os reflexos do quadro pandêmico ainda se perpetuarão por algumas gerações. A pandemia forçou a população brasileira a isolar-se do convívio social, profissional e familiar. Essa mudança brusca de comportamento e de novos hábitos ocasionou um forte impacto à saúde física e mental dos indivíduos (Vianna, 2020).

Frente a essa afirmação, é incumbência tanto do psicólogo quanto do órgão regulamentador da profissão estarem vigilantes em relação à crescente demanda por saúde mental. Isso inclui não apenas os atendimentos oferecidos, mas também a ponderação da expansão de modelos de trabalho, com destaque para a ênfase no formato remoto. Bittencourt *et al*. (2020) apontaram os seguintes dados, fornecidos pelo Conselho Federal de Psicologia sobre a saúde mental durante a pandemia, os quais mostraram que em 2020, o sistema *e-psi* registrou mais de 30 mil acessos em um único dia.

Respectivamente, houve um aumento de profissionais psicólogos cadastrando-se na plataforma *e-psi* para a realização de atendimento psicológico de maneira remota, visto que a população brasileira encontrava-se em isolamento, restringindo

[4]"A Covid-19 é uma infecção respiratória aguda causada pelo coronavírus SARS-CoV-2, potencialmente grave, de elevada transmissibilidade e de distribuição global" (GOV, [s.d.]).

o atendimento presencial. De acordo com a Escola de Saúde Pública do Ceará-CE, a procura de psicólogos, pelo registro deste modelo de atendimento através da plataforma *e-psi*, teve um aumento de 800% (Vianna, 2020).

O psicólogo que escolhe por essa modalidade de atendimento comumente não possui uma equipe para o gerenciamento dos dados. Trata-se de um trabalho individual. Esse modelo de trabalho exige organização das atividades por parte do profissional, a saber: cadastro de pacientes, horários, prontuários, entre outras informações que ficam a cargo do psicólogo.

É comum, no processo burocrático administrativo, que muitos profissionais apresentem dificuldades de organizar seus dados e/ou gerenciar arquivos, dada sua inexperiência com as tecnologias digitais. De acordo com estudos realizados, a ausência de organização pode ocasionar sentimentos de improdutividade, falta de controle das informações e consequentemente ausência de segurança dos dados (Albuquerque *et al*., 2017).

Diante da constatação da dificuldade dos profissionais de psicologia com as ferramentas digitais, este trabalho tem como objetivo o desenvolvimento de um sistema para gerenciamento das atividades profissionais de um psicólogo que atua na modalidade remota.

O *SystemPsi* fornece ao profissional psicólogo uma gama de ferramentas com a finalidade de auxiliar na organização de seus atendimentos, agendamentos, prontuários e pacientes. Além de ser multiplataforma e permitir o acesso em vários dispositivos, dinamizando o modelo de atendimento.

Para o desenvolvimento deste sistema serão utilizadas ferramentas digitais envolvendo bancos de dados e programação. A metodologia utilizada segue uma sequência de etapas definida preliminarmente. Além disso, foi elaborado um cronograma visando o cumprimento de cada etapa dentro do prazo estipulado.

Espera-se que este sistema possa contribuir com a otimização do trabalho burocrático desenvolvido pelo psicólogo em seus atendimentos, destarte é possível que este sistema possa ter seu uso replicado por outros profissionais que trabalhem na mesma modalidade de atuação.

Este artigo está organizado em 5 sessões: introdução, referencial teórico, aspectos metodológicos, resultados e discussões e considerações finais.

2. Referencial teórico

A psicologia, diferentemente de outras áreas, não iniciou como uma ciência, e sim como um ramo da Filosofia na busca por entender pensamentos e ações dos seres humanos. O termo "psicologia" foi encontrado pela primeira vez em livros filosóficos do século XVI, e tem origem do Grego antigo "*psyque*", que significa "mente", e "*logos*", que significa "conhecimento ou estudo" (Gallardo, 2019).

Com o passar dos anos, a psicologia evoluiu e se tornou uma ciência independente, com sua própria teoria, método e técnicas de pesquisa. Atualmente, ela é uma disciplina que busca compreender o comportamento humano, bem como os processos mentais que o influenciam, tais como as emoções, os pensamentos e as percepções (Gallardo, 2019).

De acordo com um estudo realizado no Brasil sobre os impactos da pandemia da COVID-19 na saúde mental, 56% dos participantes relataram piora na qualidade do sono em decorrência do isolamento social, enquanto 80% apontaram aumento do estresse no contexto familiar (Vianna, 2020). Dessa forma, as condições desfavoráveis do isolamento social na pandemia, apontaram para uma possível tendência de agravamento das questões de saúde mental nas famílias brasileiras (Bezerra; Fernandes, 2020).

Com o isolamento social, a necessidade de atendimento remoto se tornou ainda mais evidente, uma vez que muitas pessoas passaram a evitar sair de casa e a buscar alternativas para manter sua saúde mental em dia.

O modelo de atendimento remoto tem se mostrado eficaz, proporcionando aos pacientes de diferentes locais e regiões do Mundo, acesso a tratamentos psicológicos de qualidade, bem como proporcionando aos profissionais, maior flexibilidade de horários e liberdade geográfica. Este modelo de atendimento tende ao crescimento, conforme afirma Marasca *et al.* (2020, p. 9):

> A regulamentação de atividades psicológicas online contribuiu para ampliar as possibilidades de atuação do psicólogo brasileiro e desempenhou um papel central na adaptação ao novo cenário de trabalho imposto pelas restrições da pandemia da COVID-19, indicando que esse formato tende a se expandir e consolidar.

Esse modo de atendimento traz consigo algumas dificuldades, sendo a mais substancial a ausência de habilidades com as TICs por parte dos profissionais, minimizando a produtividade e a segurança dos dados.

Diante desse contexto, surge a necessidade de um sistema que possa auxiliar psicólogos em atuação remota a gerenciar seus pacientes, de forma segura e eficiente. É nesse sentido que o *SystemPsi* se propõe a contribuir, oferecendo uma plataforma que permita o agendamento de consultas, o armazenamento de informações dos pacientes, o registro de evoluções, além de ferramentas para o acompanhamento e avaliação do tratamento.

Com o *SystemPsi*, espera-se que psicólogos em atuação remota possam otimizar seu trabalho, aumentando sua produtividade e qualidade dos serviços prestados, beneficiando tanto os profissionais quanto seus pacientes.

3. Aspectos metodológicos

Esta pesquisa se caracteriza como tecnológica pois seu objeto orientador é o artefato produzido. O autor utilizou a metodologia de desenvolvimento *Design Science Research Methodology*[5], que segue algumas etapas, que foram mantidas, com algumas ressalvas, no desenvolvimento deste projeto: Identificar o problema e sua motivação, definir os objetivos da

[5]Como afirma Júnior e Sousa (2018, p. 11) "A Design Science Research Methodology (DSRM) é uma metodologia de pesquisa amplamente empregada no desenvolvimento de investigações tecnológicas, isto é, cujo foco está na produção de um novo artefato".

solução, prototipação e desenvolvimento, demonstrar, avaliar e comunicar.

O problema foi inicialmente identificado observando a dificuldade em armazenar e recuperar os dados dos pacientes, além disto, observou-se a necessidade de possibilitar o acesso às informações através de diferentes dispositivos. A segunda etapa envolveu o levantamento de requisitos, identificando quais as funções necessárias ao sistema. A partir de conversas informais com uma psicóloga que atua exclusivamente na modalidade remota, observou-se que o sistema deveria ser capaz de gerenciar os pacientes, facilitando o acesso às suas informações. O sistema também deveria possibilitar a organização dos horários do psicólogo, gerenciar os atendimentos agendados por meio de um calendário dinâmico, auxiliar durante o atendimento, registrando informações e anotações.

Na terceira etapa da metodologia, iniciou-se o desenvolvimento do sistema, visando três principais objetivos: cumprir os requisitos identificados para seu funcionamento, permitir o acesso *mobile* com responsividade e zelar pela segurança dos dados, realizando *backups* periódicos. A partir do levantamento de requisitos foi realizada a modelagem conceitual através da ferramenta brModelo [6], visando identificar as entidades do sistema, bem como as relações entre as entidades, as cardinalidades e seus atributos. Durante esta pesquisa, destacaram-se três entidades: Psicólogo, com os atributos: ID, Nome, *E-mail*, Senha, Telefone e CRP (Conselho Regional de Psicologia) e Paciente, com os atributos: Nome, Telefone, Data

[6]O brModelo "[...] é uma ferramenta para modelagem de base de dados [...]" (ANGELOTTI, 2010, p. 19).

de Nascimento, Convênio, Foto, Gênero, *E-mail*, Prontuário e Anexos. Também, no mesmo modelo, foi acrescentada uma entidade-associativa entre as duas entidades já existentes, denominada Atendimento-Atender, com os atributos: Hora, Valor, Objetivo, Forma de Pagamento, Observações, Registro e Data. Entre as mesmas entidades foi colocado um relacionamento chamado Agendar.

Após a conclusão do modelo conceitual, foi realizado o processo de conversão para a modelagem lógica, que incluiu a especificação das chaves primárias, chaves estrangeiras e outras caracterizações desta modelagem, como o tratamento de situações com cardinalidades compostas. Em seguida, a modelagem lógica foi implementada usando a linguagem SQL[7] (*Structured Query Language*) através do Sistema Gerenciador de Banco de Dados MySQL Workbench[8] na versão 8.0. Após a finalização da modelagem física, deu-se início o desenvolvimento das telas do sistema, levando em consideração os requisitos mencionados na segunda etapa da metodologia. Para o desenvolvimento do código, o autor utilizou a ferramenta de edição de código-fonte Visual Studio Code[9] na versão 1.78.2.

[7]Conforme Angelotti (2010, p. 74) "A Linguagem SQL (Structured Query Language ou Linguagem de Consulta Estruturada) é uma linguagem para banco de dados relacional".

[8]O MySQL Workbench é um sistema gerenciador de banco de dados de código livre que integra desenvolvimento SQL (ANGELOTTI, 2010, p. 75).

[9]O Visual Studio Code é um software de edição de código-fonte desenvolvido pela Microsoft (VISUALSTUDIO, 2023).

Para auxiliar no desenvolvimento *front-end* e garantir a responsividade, optou-se pelo *framework* Bootstrap[10] na versão 5.

Paralelamente ao desenvolvimento das telas do sistema, foi realizada a conexão com o banco de dados, trazendo dinamicidade às telas, que até então eram estáticas. Para o desenvolvimento do *back-end*, o autor escolher a linguagem PHP[11] (PHP: Hypertext Preprocessor) como a principal para codificação. Além disso, o PHP Data Object foi utilizado para acessar e fazer consultas ao banco de dados. Durante o desenvolvimento do artefato, o autor também utilizou a ferramenta phpMyAdmin[12] para fazer alterações rápidas no banco de dados, por ser considerada mais intuitiva do que o MySQL Workbench. O sistema tinha necessidade de ser alocado em um servidor, a escolha feita foi o Xampp que se trata de um agrupamento com os principais servidores para desenvolvedores PHP. Ele contém os servidores para banco de dados MySQL e Apache no qual suporta as linguagens PHP e Perl. Em alguns casos, foi-se utilizado a linguagem JavaScript com a finalidade de dinamizar as páginas com novas funcionalidades.

Durante o processo de desenvolvimento, à medida que as funcionalidades eram concluídas, elas foram submetidas a testes realizados por uma profissional da psicologia, para suas

[10]"O Bootstrap é uma ferramenta gratuita para desenvolvimento HTML, CSS e JS. [...]" para desenvolvimento *front-end* (GETBOOTSTRAP, [s.d.]).

[11]O PHP é uma linguagem de programação para desenvolvimento *back-end* (PHP, 2023).

[12]O phpMyAdmin é um software destinado a administrar o MySQL pela Web (PHPMYADMIN, 2023).

considerações sobre as funcionalidades apresentadas. Pode-se afirmar que a terceira etapa da metodologia aconteceu em paralelo à quarta e à quinta etapas, pois todo o processo de desenvolvimento decorreu com a anuência da profissional. A avaliação do software se deu por etapas, corrigindo-se os possíveis problemas encontrados na sua execução. Devido à necessidade de implementação de funcionalidades específicas, o sistema foi hospedado em domínio público e permitiu que a profissional realizasse testes utilizando a plataforma disponibilizada e apresentasse suas considerações.

A última etapa da metodologia foi cumprida com êxito e concluída antes do prazo, o que garantiu o cumprimento de um cronograma prévio que seguia o calendário da instituição. O artefato encontra-se na sua primeira versão e apresenta diversas funcionalidades que serão explanadas na sequência.

4. Resultados e discussão

Nesta seção, apresentaremos os resultados obtidos durante o desenvolvimento do *SystemPsi*, bem como as discussões pertinentes aos principais aspectos encontrados.

Os resultados obtidos demonstraram que o *SystemPsi* atendeu os requisitos identificados, proporcionando uma ferramenta eficiente para o gerenciamento das atividades profissionais de psicólogos que atuam na modalidade de atendimento remoto. A seguir, apresentaremos os principais resultados encontrados durante o desenvolvimento do sistema:

1. **Identificação e Gerenciamento de Pacientes**: O *SystemPsi* permite o cadastro e gerenciamento de pacientes, facilitando o acesso às suas informações. Os psicólogos podem armazenar dados como nome, telefone, data de nascimento, convênio, foto, gênero, e-mail, prontuário e anexos. Essa funcionalidade proporciona uma visão abrangente dos pacientes atendidos, auxiliando na organização e acompanhamento dos tratamentos. O profissional também tem a opção de emitir um relatório com a ficha completa do paciente para impressão ou download com as informações cadastradas. Além disso, o sistema permite a identificação dos pacientes que estão ativos ou não.

2. **Agendamento de Consultas**: O sistema possui um calendário dinâmico que permite o agendamento de consultas de forma intuitiva. Os psicólogos podem verificar sua disponibilidade e marcar horários de atendimento. Essa funcionalidade contribui para a otimização dos horários do profissional, permitindo uma melhor distribuição das consultas ao longo do dia e/ou da semana. O sistema envia diariamente para cada psicólogo um resumo dos seus agendamentos naquele dia via *e-mail* e via WhatsApp[13].

3. **Registro de Evoluções e Anotações**: Durante as consultas, o *SystemPsi* possibilita o registro de evoluções e anotações relacionadas ao tratamento de cada paciente. Essa funcionalidade permite o acompanhamento

[13]O WhatsApp é um aplicativo que oferece “mensagens e chamadas privadas simples, seguras e gratuitas, disponíveis em todo o mundo” (WHATSAPP, 2023).

detalhado do progresso de cada indivíduo, fornecendo subsídios para uma melhor análise e avaliação do tratamento realizado. O profissional pode emitir um relatório de um único atendimento ou de todos os atendimentos realizados com o mesmo paciente para *download* ou impressão.

4. **Acesso Multiplataforma e Responsividade**: O *SystemPsi* foi desenvolvido com o suporte para diferentes dispositivos, sendo acessível tanto em computadores quanto em dispositivos móveis. A responsividade do sistema garante uma experiência consistente e amigável para os usuários, independentemente do dispositivo utilizado.

5. **Segurança de Dados**: Para garantir a segurança das informações, o *SystemPsi* permite a realização de *backups* periódicos dos dados armazenados. Essa medida contribui para a proteção e a integridade dos registros dos pacientes, evitando perdas ou acesso não autorizado dos dados sensíveis.

6. **Lembrete de Consultas**: o *SystemPsi* possui um recurso fundamental para a psicóloga entrevistada, que é o envio automático de *e-mails* e mensagens de WhatsApp de lembrete para as consultas agendadas. O sistema também faz o envio de mensagens de WhatsApp para os pacientes de forma automática, lembrando-os dos seus atendimentos. Essa funcionalidade foi implementada para solucionar o problema enfrentado pela psicóloga e pelos pacientes, que frequentemente esqueciam as consultas e horários agendados.

Para poder fazer os testes e a implementação destas funcionalidades, fez-se necessária a hospedagem do sistema temporariamente para que o disparo de *e-mails* e o envio de mensagens via WhatsApp funcionasse corretamente. Foi escolhido pelo autor o serviço de hospedagem *HostGator*[14]. Além disso, foi necessário a contração de uma API[15] para possibilitar o uso do WhatsApp como meio de notificação e lembrete.

O sistema, através do serviço de hospedagem, executa um arquivo que faz a consulta ao banco de dados automaticamente às 08h e localiza os pacientes que possuem horário agendado para o dia. Estes pacientes receberão uma mensagem no WhatsApp lembrando o horário do agendamento. O mesmo sistema de verificação envia um *e-mail*[16] e um WhatsApp para o psicólogo com um resumo dos atendimentos no dia.

A implementação dessa funcionalidade mostrou-se eficaz na redução dos esquecimentos de consultas pela psicóloga, proporcionando maior organização e pontualidade no atendimento aos pacientes. Além disso, as mensagens enviadas aos pacientes os auxiliam, pois recebem uma confirmação

---

[14]"HostGator é uma companhia de hospedagem de sites e que também oferece serviços correlatos, como servidores remotos na nuvem, e-mails, ferramentas para criação de websites e revenda de domínios" (GARRET, 2021).

[15]"As APIs são um conjunto de padrões que fazem parte de uma interface" (FABRO, 2020).

[16]O envio de *e-mails* pelo sistema se deu através de uma das bibliotecas mais conhecidas para disparo de *e-mails* com PHP, PHPMailer (PHP, 2018).

adicional do horário da consulta, aumentando a probabilidade de comparecimento e reduzindo as faltas.

Além disso, a hospedagem do *software* permitiu que a psicóloga pudesse testar o sistema de forma funcional. Esta ação ajudou na identificação e correção de erros encontrados no seu uso profissional.

É importante ressaltar que o envio de *e-mail* acontece somente para o psicólogo, já que o campo de *e-mail* é facultativo no cadastro da ficha do paciente.

Destaca-se que essa funcionalidade de envio de *e-mails* e mensagens de WhatsApp de lembrete foi desenvolvida levando em consideração a privacidade e a confidencialidade dos pacientes. O conteúdo dos *e-mails* e mensagens é cuidadosamente elaborado para evitar a divulgação indevida de informações sensíveis e proteger a privacidade dos indivíduos atendidos.

Essa funcionalidade adicional do *SystemPsi* demonstra o compromisso do sistema em atender às necessidades específicas dos profissionais da área da psicologia, buscando solucionar problemas reais enfrentados no cotidiano de trabalho. A implementação bem-sucedida do recurso de lembretes destaca a importância de abordar as questões práticas e operacionais enfrentadas pelos psicólogos e oferece soluções tecnológicas que possam melhorar sua eficiência e produtividade.

Os resultados obtidos durante o desenvolvimento e implementação do *SystemPsi* demonstram que o sistema oferece uma solução eficaz para os psicólogos que atuam na modalidade de atendimento remoto, ao possibilitar o gerenciamento organizado e seguro das atividades profissionais. O *SystemPsi*

contribui para a otimização do trabalho burocrático desses profissionais, permitindo que eles foquem mais na qualidade dos serviços prestados aos pacientes.

O *SystemPsi* encontra-se na sua primeira versão, que possui todas as funcionalidades destacadas. O desenvolvimento do sistema finalizou antes do prazo esperado, e contou com a etapa de realização de testes para aprimoramento da ferramenta. No entanto, é importante ressaltar que o sistema pode ser aprimorado. A seguir, discutiremos algumas considerações relevantes sobre o *SystemPsi*:

1. **Usabilidade e Experiência do Usuário**: Durante a fase de demonstração do sistema, foram coletados *feedbacks* de uma psicóloga usuária. Esses retornos foram utilizados para aprimorar a usabilidade e experiência do usuário do *SystemPsi*. Novas funcionalidades foram implementadas e melhorias na interface foram realizadas, tornando o sistema mais intuitivo e fácil de usar.

2. **Integrações com Outros Sistemas**: No futuro, será possível explorar integrações do *SystemPsi* com outros sistemas utilizados na área da saúde, como sistemas de faturamento/financeiro ou até integrar a ferramenta com o Google Calendar [17] . Essas integrações podem contribuir para uma maior interoperabilidade entre as soluções adotadas pelos profissionais, facilitando o fluxo de informações e o compartilhamento de dados relevantes.

[17] O Google Calendar é um calendário on-line promovido pelo Google.

Estes são apenas alguns aspectos discutidos com base nos resultados obtidos até o momento. É fundamental que futuras pesquisas e avaliações sejam realizadas para aprimorar e expandir o *SystemPsi*, buscando atender ainda mais às necessidades dos psicólogos e oferecer uma solução completa e eficiente para o gerenciamento de atividades profissionais na modalidade de atendimento remoto.

5. Considerações finais

O presente artigo abordou o desenvolvimento e implementação do *SystemPsi*, um sistema gerenciador destinado aos psicólogos que atuam na modalidade de atendimento remoto. O objetivo principal do sistema é otimizar a organização das atividades profissionais, desde o agendamento de consultas até o registro de evoluções e anotações dos pacientes.

O contexto da pandemia da COVID-19 destacou a importância dos serviços de saúde mental e a necessidade de adaptação dos profissionais da psicologia para atender à crescente demanda por atendimento remoto. O *SystemPsi* surge como uma resposta eficaz a essa demanda, oferecendo uma plataforma amigável, segura e eficiente.

Ao longo do desenvolvimento do *SystemPsi*, foram identificadas e superadas várias dificuldades relacionadas à gestão de dados, organização de consultas e necessidades específicas da profissão. As funcionalidades implementadas demonstraram sua eficácia, auxiliando tanto os profissionais quanto seus pacientes no gerenciamento de suas atividades.

Além disso, a flexibilidade e responsividade do sistema, permitindo o acesso em diferentes dispositivos, contribuem para uma experiência positiva para o profissional, potencializando de forma eficaz o atendimento.

O desenvolvimento do *SystemPsi* também ressalta a importância da colaboração entre profissionais da área e desenvolvedores de tecnologia. Os *feedbacks* fornecidos pela psicóloga usuária foram essenciais para aprimorar a usabilidade e a experiência do usuário, demonstrando a relevância de considerar as necessidades reais durante o desenvolvimento de sistemas tecnológicos.

Embora o *SystemPsi* tenha alcançado resultados promissores em sua primeira versão, é crucial reconhecer que a tecnologia está em constante evolução. A atualização contínua do sistema, levando em consideração novas demandas e tendências tecnológicas, é fundamental para garantir sua relevância e eficácia a longo prazo.

O presente estudo também ressalta a importância de integrar a tecnologia às práticas profissionais, especialmente em áreas sensíveis como a saúde mental. Através do *SystemPsi*, espera-se que mais psicólogos possam adotar o atendimento remoto, proporcionando maior acessibilidade e qualidade aos serviços prestados.

Em síntese, o desenvolvimento do *SystemPsi* representa um passo significativo em direção à modernização e otimização das atividades dos psicólogos que atuam remotamente. A integração entre psicologia e tecnologia oferece uma oportunidade valiosa para aprimorar os serviços de saúde mental, tornando-os mais eficientes, acessíveis e adaptados às necessidades contemporâneas.

6. Referências

ALBUQUERQUE, E. A. Y. et al. PRONTUÁRIO ELETRÔNICO DO PACIENTE E CERTIFICAÇÃO DE SOFTWARE EM SAÚDE: AVANÇOS QUE VISAM MAIOR SEGURANÇA DOS DADOS MÉDICOS. **Revista Brasileira de Inovação Tecnológica em Saúde - ISSN:2236-1103**, v. 7, 23 nov. 2017.

ANGELOTTI, E. S. **Banco de Dados**. [s.l.] Editora do Livro Técnico, 2010.

BEZERRA, A. R.; FERNANDES, A. V. G. COVID -19 E SAÚDE MENTAL: ABORDAGENS DO PENSAMENTO CRÍTICO. **HOLOS**, v. 3, p. 1–16, 6 ago. 2021.

BEZERRA, C. G.; MOURA, K. P.; DUTRA, E. Plantão psicológico on-line a estudantes universitários durante a pandemia da COVID-19. **Revista do NUFEN**, v. 13, n. 2, p. 58–70, 1 ago. 2021.

BITTENCOURT, H. B. et al. Psicoterapia on-line: uma revisão de literatura. **Diaphora**, v. 9, n. 2, p. 41–46, 2020.

CONSELHO FEDERAL DE PSICOLOGIA. **RESOLUÇÃO Nº 11, DE 11 DE MAIO DE 2018**. Disponível em: <https://site.cfp.org.br/wp-content/uploads/2018/05/RESOLU%C3%87%C3%83O-N%C2%BA-11-DE-11-DE-MAIO-DE-2018.pdf>. Acesso em: 26 ago. 2023.

CONSELHO FEDERAL DE PSICOLOGIA. **Nova resolução do CFP destaca diretrizes para a Avaliação Psicológica**. Disponível em: <https://site.cfp.org.br/nova-resolucao-do-cfp-destaca-diretrizes-para-a-avaliacao-psicologica/#:~:text=Foi%20publicada%20no%20Di%C3%A1rio%20Oficial>. Acesso em: 26 ago. 2023.

E-PSI. **Cadastro e-Psi - Psicólogas(os) cadastradas(os) para Atendimento on-line**. Disponível em: <https://e-psi.cfp.org.br/>. Acesso em: 26 ago. 2023.

FABRO, C. **O que é API e para que serve? Cinco perguntas e respostas**. Disponível em: <https://www.techtudo.com.br/listas/2020/06/o-que-e-api-e-

para-que-serve-cinco-perguntas-e-respostas.ghtml>. Acesso em: 26 ago. 2023.

GALLARDO, C. P. **Origem da PSICOLOGIA: RESUMO e autores**. Disponível em: <https://br.psicologia-online.com/origem-da-psicologia-resumo-e-autores-215.html>. Acesso em: 26 ago. 2023.

GARRETT, F. **HostGator é bom? Cinco perguntas sobre o site de hospedagem**. Disponível em: <https://www.techtudo.com.br/listas/2021/06/hostgator-e-bom-cinco-perguntas-sobre-osite-de-hospedagem.ghtml>. Acesso em: 26 ago. 2023.

GETBOOTSTRAP. **Bootstrap em Português**. Disponível em: <https://getbootstrap.com.br/>. Acesso em: 30 ago. 2023.

GOV. **Informações Covid-19**. Disponível em: <https://www.gov.br/saude/pt-br/coronavirus>. Acesso em: 30 ago. 2023.

JUNIOR, V. F.; SOUSA, V. M. DE. **Guia para a escrita de artigos científicos: uma perspectiva da pesquisa tecnológica**. Disponível em: <https://redes.sombrio.ifc.edu.br/wp-content/blogs.dir/9/files/sites/84/2023/02/Guia-de-artigos-cientificos.pdf>. Acesso em: 30 ago. 2023.

MARASCA, A. R. et al. **Avaliação psicológica online: considerações a partir da pandemia do novo coronavírus (COVID-19) para a prática e o ensino no contexto a distância**. Disponível em: <https://doi.org/10.1590/1982-0275202037e200085>. Acesso em: 26 ago. 2023.

MATSUMOTO, C. Y. A IMPORTÃ‚NCIA DO BANCO DE DADOS EM UMA ORGANIZAÇÃO. **Maringá Management**, v. 3, n. 1, 2006.

MICROSOFT. **Visual Studio Code**. Disponível em: <https://code.visualstudio.com/>. Acesso em: 30 ago. 2023.

PHPMYADMIN. **phpMyAdmin**. Disponível em: <https://www.phpmyadmin.net/>. Acesso em: 26 ago. 2023.

PINTO, E. R. As modalidades do atendimento psicológico on-line. **Temas em Psicologia**, v. 10, n. 2, p. 168–177, 1 ago. 2002.

SABBATINI, R. **A Telemedicina no Brasil: Evolução e Perspectivas**. [s.l: s.n.]. Disponível em: <https://www.sabbatini.com/renato/papers/Telemedicina_Brasil_Evolucao_Perspectivas.pdf>. Acesso em: 26 ago. 2023.

THE PHP GROUP. **PHP: Hypertext Preprocessor**. Disponível em: <https://www.php.net/>. Acesso em: 26 ago. 2023.

ULKOVSKI, E. P.; SILVA, L. P. D. DA; RIBEIRO, A. B. ATENDIMENTO PSICOLÓGICO ONLINE: perspectivas e desafios atuais da psicoterapia. **Revista de Iniciação Científica da Universidade Vale do Rio Verde**, v. 7, n. 1, 23 jul. 2017.

VIANA, D. M. ATENDIMENTO PSICOLÓGICO ONLINE NO CONTEXTO DA PANDEMIA DE COVID-19. **Cadernos ESP**, v. 14, n. 1, p. 74–79, 22 jul. 2020.

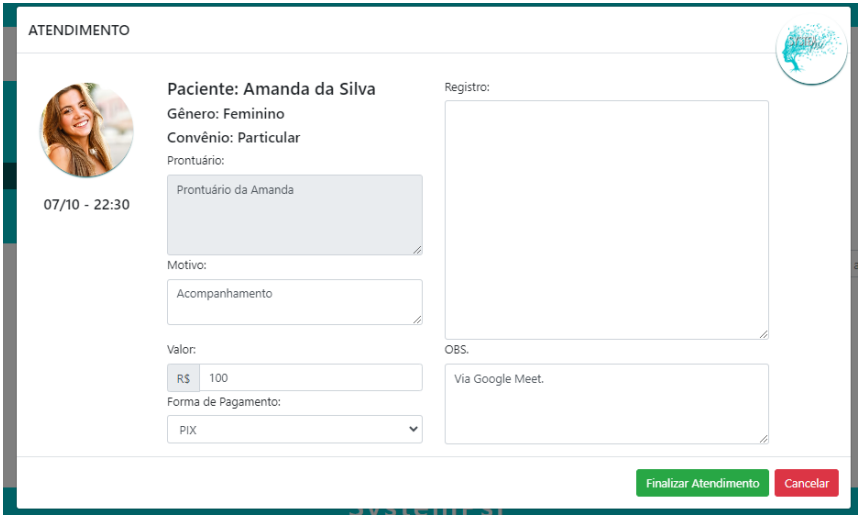
WHATSAPP. **WhatsApp**. Disponível em: <https://www.whatsapp.com/?lang=pt_br>. Acesso em: 30 ago. 2023.

Apêndice

Apêndice 1 – Tela de login

Apêndice 2 – Tela de pacientes

Apêndice 3 – Tela de edição/cadastro de pacientes



Apêndice 4 – Tela para agendamentos