Dissertação de Mestrado

Inatel
Instituto Nacional de Telecomunicações

Análise de Desempenho de Redes de Teleproteção de Sistemas de Distribuição de Energia utilizando Simulação e Emulação

José Rodrigo dos Santos

Julho de 2022

ANÁLISE DE DESEMPENHO DE REDES DE TELEPROTEÇÃO DE SISTEMAS DE DISTRIBUIÇÃO DE ENERGIA UTILIZANDO SIMULAÇÃO E EMULAÇÃO

JOSÉ RODRIGO DOS SANTOS

Dissertação apresentada ao Instituto Nacional de Telecomunicações, como parte dos requisitos para obtenção do Título de Mestre em Telecomunicações.

ORIENTADOR: Prof. Dr. Antônio Marcos Alberti.

Santa Rita do Sapucaí
2022

Santos, José Rodrigo dos
A334a
Análise de desempenho de redes de teleproteção de sistemas de distribuição de energia utilizando simulação e emulação. / José Rodrigo dos Santos – Santa Rita do Sapucaí, 2022.
94 p.

Orientador: Prof. Dr. Antônio Marcos Alberti
Dissertação de Mestrado em Telecomunicações – Instituto Nacional de Telecomunicações – INATEL.

1. Simulação 2. Teleproteção 3. Missão crítica 4. Integração de sistemas 5. Mestrado em Telecomunicações. I. Alberti, Antônio Marcos II. Instituto Nacional de Telecomunicações – INATEL. III. Título.

CDU 621.39

Ficha Catalográfica elaborada pelo Bibliotecário da Instituição
CRB6-2718 – Paulo Eduardo de Almeida

Colophon

Inatel
Mestrado em Telecomunicações

FOLHA DE APROVAÇÃO

Dissertação defendida e aprovada em 22/ 07/ 2022,
pela comissão julgadora:

Prof. Dr. Antônio Marcos Alberti
INATEL

Prof. Dr. Joel José Puga Coelho Rodrigues
Faculdade Senac Ceará

Prof. Dr. Samuel Baraldi Mafra
INATEL

Coordenador do Curso de Mestrado
Prof. Dr. José Marcos Câmara Brito

"O ser humano é um animal filosofante: só pode renunciar à filosofia renunciando a uma parte da sua humanidade. É preciso filosofar, portanto: pensar tão longe quanto pudermos, e mais longe do que sabemos. Com que finalidade? Uma vida mais humana, mais lúcida, mais serena, mais razoável, mais feliz, mais livre..."

André Comte-Sponville

Dedico esse trabalho ao professor Antônio Marcos Alberti, meu orientador, pela confiança, amizade e apoio imprescindível durante a realização dos trabalhos em campo e no laboratório. Sem sua ajuda nada seria possível. Aos amigos do curso de Mestrado em Telecomunicações, especialmente a todos os membros do laboratório no período o qual estivemos trabalhando e se apoiando.

José Rodrigo do Santos

Agradecimentos

Em primeiro lugar agradeço a Deus. Agradeço aos meus pais (Rita e Bráz) e meus irmãos (Fernando/Luciana), e em especial meu irmão Juliano, o qual não deixou que desistisse mesmo nos momentos mais difíceis. A todos os colegas do Inatel que estudaram comigo e contribuíram direta ou indiretamente, em especial todos os colegas do ICTLab, meu muito obrigado.

Agradeço também a todos da CEMIG que através do projeto No D0640, Modelo de Referência para a Rede Operacional de Dados da CEMIG, financiado pela FAPEMIG / CEMIG que possibilitaram a execução deste trabalho

Agradeço ao meu orientador, Prof. Alberti, por sua paciência e orientação.

Sumário

Lista de Figuras

Lista de Tabelas

Acrônimos

Ack Acknowledgement

SG Smart Grids

REI Redes Elétricas Inteligentes

FITec Fundação para Inovações Tecnológicas

MPLS Multiprotocol Label Switching

MPLS-TE Multi Protocol Label Switching Traffic Engineering

HAN Home Area Network

BAN Building Area Network

IAN Industrial Area Network

NAN Neighborhood Area Network

FAN Field Area Networks

WAN Wide Area Network

TDM Time Division Multiplexing

RTDS Real Time Digital Simulator

MATLAB Matrix Laboratory

NS-3 Network Simulator 3

SDN Software Defined Networking

IP Internet Protocol

OSPF Open Shortest Path First

TE Traffic Engineering

PE Provider Edge

CE Customer Edge

LER Label Edge Router

FEC Forwarding Equivalent Class

LSR Label Switching Router

PR Provider Router

LSP Label Switched Path

RSVP Resource Reservation Protocol

(RSVP-TE Resource Reservation Protocol with Tunneling

CR-LDP Constrained-based Label Distribution Protocol

AD Administrative Distance

Flex LSP Flex Label Switched Paths

LDP Label Distribution Protocol

BFD Bidirectional Forward Detect

CDP Cisco Discovery Protocol

VPN Virtual Private Network

L2VPN Layer 2 Virtual Private Network

VPLS Virtual Private LAN Service

VPWS Virtual Private Wire Service

PW Pseudowire

API Application Programming Interface

EMS Energy Management System

PDH Plesiochronous Digital Hierarchy

SDH Synchronous Digital Hierarchy

NG-SDH Next Generation - Synchronous Digital Hierarchy

ARP Address Resolution Protocol

Publicações

Publicações do projeto CEMIG

1. L. F. F. de Almeida, José Rodrigo dos Santos, Luiz Augusto Melo Pereira, Arismar Cerqueira Sodré, Luciano Leonel Mendes, Joel J. P. C. Rodrigues, Ricardo A. L. Rabelo e Antonio Marcos Alberti, "Control Networks and Smart Grid Teleprotection: Ky Aspects, Technologies, Protocols and Case-Studies", in IEEE Access, DOI: `https://doi.org/10.1109/ACCESS.2020.3025235`

2. L. F. F. de Almeida, L. H. M. Leite, R. A. Fernandes, J. R. dos Santos, R. J. Machado, W. R. Silva, J. J. P. C. Rodrigues e A. M. Alberti, "Análise de Redes de Dados Estatísticas para Teleproteção de Linhas de Transmissão de Energia", in VIII Simpósio Brasileiro de Sistemas Elétricos, 2020, Santo André. Anais do SBSE, 2020.

Publicações de outros projetos

1. Santos, J., Rezende, T., Silva, T., Rosário, E., Alberti, A. (2020). Proposta de Arquitetura para Distribuição de Conteúdos Nomeados em NovaGenesis com P4. In Anais do XI Workshop de Pesquisa Experimental da Internet do Futuro, (pp. 32-37). Porto Alegre: SBC. https://doi.org/10.5753/wpeif.2020.12472

2. Alberti, A.M.; Bontempo, M.M.; Dos Santos, J.R.; Sodré, A.C., Jr.; Righi, R.D.R. NovaGenesis Applied to Information-Centric, Service-Defined, Trustable IoT/WSAN Control Plane and Spectrum Management. Sensors 2018, 18, 3160. https://doi.org/10.3390/s18093160

3. Alberti, A., Santos, J., Morais, E., Santos, R., Magalhães, V. (2018). Forwarding/-Routing with Dual Names: The NovaGenesis Approach. In Anais do IX Workshop de Pesquisa Experimental da Internet do Futuro. Porto Alegre: SBC.

4. DOMINGUES DAVILA, Victor Hugo; ROSÁRIO, Élcio; DOS SANTOS, José Rodrigo; ALBERTI, Antonio Marcos . NovaGenesis NameBindings: Avaliação de Virtualização em Escala. In: WORKSHOP DE PESQUISA EXPERIMENTAL DA INTERNET DO FUTURO (WPEIF), 10. , 2019, Gramado. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019 . p. 7-12. ISSN 2595-2692. DOI: https://doi.org/10.5753/wpeif.2019.7692.

5. ALMEIDA, Fabio ; BONTEMPO, Marília M.; DOS SANTOS, José Rodrigo ; ALBERTI, Antonio Marcos . Uma Proposta de Contramedida ao Ataque Jamming em Redes IEEE 802.15.4 utilizando Rádio Cognitivo. In: WORKSHOP DE SEGURANÇA CIBERNÉTICA EM DISPOSITIVOS CONECTADOS (WSCDC), 2. , 2019, Gramado. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019 . p. 12-22. DOI: https://doi.org/10.5753/wscdc.2019.7702.

6. A. M. Alberti, E. C. do Rosário, G. Cassiano, J. R. dos Santos, V. H. D'Ávila and J. R. Carneiro, "Performance evaluation of NovaGenesis information-centric network,"2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech), 2017, pp. 1-6.

Resumo

SANTOS, J. R. dos, Análise de Desempenho de Redes de Teleproteção de Sistemas de Distribuição de Energia utilizando Simulação e Emulação [dissertação de mestrado]. Santa Rita do Sapucaí: Instituto Nacional de Telecomunicações; 2022.

A crescente necessidade por redes de energia mais confiáveis, eficientes e resilientes tornou-se indispensável com o desenvolvimento tecnológico recente. A evolução tecnológica e o crescimento industrial geram uma demanda cada vez maior por energia elétrica. Criando assim uma continua necessidade de expansão no serviços de distribuição de energia. Contudo esta expansão levanta diversas questões, seja no setor privado ou governamental, sobre a gestão, a segurança e custos, para o desenvolvimento das mesmas. Desta forma, entendemos que o uso das telecomunicações, vinculada as redes elétricas para implementação de um serviço de teleproteção eficiente, é crucial para o bom desenvolvimento e operação do sistema de redes elétricas. Atualmente, várias tecnologias de comunicações foram aplicadas, afim de buscar uma solução mais eficiente no uso de teleproteção vinculada a redes elétricas. No decorrer deste trabalho vamos abordar diferentes aspectos de algumas destas tecnologias. Afim de tratar a problemática de gestão de serviços de teleproteção em redes elétricas. Dentre estas tecnologias, podemos citar alguns exemplos como: Flex LSP da CISCO, Hard Pipe da Huawei, protocolo para comutação de pacotes MPLS/IP e software GNS3. Será apresentado uma estrutura de cenários que foram desenvolvidos a partir do projeto CEMIG para estudo de redes de teleproteção vinculados a redes elétricas, de tal forma que fazemos uso de tecnologia de comutação de pacotes, envolvendo equipamentos CISCO e Huawei na construção de cenários físicos para testes. Desta maneira, temos a intenção de obter resultados comparativos de um cenário físico com um cenário de software. O software em questão é um simulador de rede de teleproteção, que possui características de emulação quando representa os equipamentos físicos de teleproteção e relés da rede elétrica. Nesta dissertação defendemos a hipótese que o uso de um sistema simulador, capaz integrar as redes de telecomunicações com as redes de distribuição de energia, vai apresentar ganhos no desenvolvimento tecnológico, bem como na economia de recursos de projeto.

Palavras-chave: Teleproteção; Simuladores de redes de telecomunicações; Simuladores de redes de energia

Abstract

SANTOS, J. R. dos, Performance Analysis of Teleprotection Networks of Energy Distribution Systems using Simulation and Emulation [masters dissertation]. Santa Rita do Sapucaí: Instituto Nacional de Telecomunicações; 2021.

The growing need for more reliable, efficient, and resilient power grids has become indispensable with recent technological development. Technological evolution and industrial growth generate increasing demand for electricity. As a consequence, it also creates a continuous need for expansion in energy distribution services. However, this expansion raises several questions, whether in the private or government sectors, about management, security, and costs for their technological development. In this way, we understand that the use of telecommunications, linked to electrical networks for the implementation of an efficient teleprotection service, is crucial to boost the development and operation of the electrical network system. Currently, several communications technologies have been applied to seek a more efficient solution in using teleprotection linked to electrical networks. In this work, we will approach different aspects of some of these technologies to address the problem of managing teleprotection services in electrical networks. Among these technologies, we can mention some examples such as Flex LSP from CISCO, Hard Pipe from Huawei, MPLS/IP packet switching protocol and GNS3 software. A framework of scenarios will be presented that were developed from the CEMIG project to study teleprotection networks linked to electrical networks, in such a way that we make use of packet switching technology, involving CISCO and Huawei equipment in the construction of physical scenarios for tests. In this way, we compare the results of a physical scenario with a software scenario. The software is a teleprotection network simulator, representing the physical teleprotection equipment and relays of the electrical network. In this dissertation, we defend the hypothesis that the use of a simulator system, capable of integrating telecommunications networks with energy distribution networks, will present gains in technological development and the economy of project resources.

Keywords: Teleprotection; Telecommunication Networks Simulators; Power Grid Simulators

Capítulo 1

Introdução

As redes de energia atuais foram construídas a partir de 100 anos atrás, e desde então fornecem a energia gerada em larga escala aos consumidores [1], e sua estrutura possui três segmentos principais: geração, transmissão e distribuição, como pode ser observado na Figura 1.1[2]. Com as demandas e novas formas de produção e consumo, se transformaram em cinco segmentos: extração (óleo, gás e carvão), geração, comercialização ou atacado, transporte (transmissão e distribuição) e por fim, varejo. Para entender a mudança no setor elétrico em andamento atualmente, a organização desse negócio pode ser vista em três modelos distintos: tradicional, de transição e virtual.

- **Organização tradicional:** Integração vertical, ausência de forças competitivas, predominância dos antigos monopólios estatais ou privados. Controle absoluto. Desincentivos à busca de eficiência e superação de limites.
- **Organização de transição:** Tendência de integração horizontal de negócios dentro de todos os segmentos, compartilhamento de recursos físicos, compartilhamento de informações e conhecimento. Ocasiona novos padrões de propriedades e terceirização, pois o conhecimento estava fora do núcleo de aplicação.
- **Organização virtual:** Com a fragmentação da estrutura vertical, surgem diversas unidades moldando novas estruturas flexíveis, custos variáveis e modelos de negócios emergentes, todos apoiados pelo avanço tecnológico. E a premissa passa a ser integração funcional e estratégica.

O setor elétrico brasileiro foi tradicionalmente denotado como monopolista. O que alterou e motivou um comportamento mais dinâmico foram as privatizações, que se iniciaram em 1995, participando grupos nacionais e multinacionais (Estados Unidos, Europa, América Latina). De 1995 até 2001, 19 empresas de distribuição e 4 de geração foram privatizadas. Uma transferência superior a 50% para a iniciativa privada. Com os mercados de energia da Europa em baixa, as empresas expandiram seus negócios para o Brasil e América Latina, trazendo suas estratégias de expansão dos negócios e visão de futuro.

O cenário é de transformação de riscos em grandes oportunidades de negócios, como por exemplo, pela segmentação da indústria, pela participação de capital estrangeiro, pela possibilidade dos consumidores escolherem seu fornecedor, e pela convergência tecnológica entre setores fundamentais (aguá, gás, telecomunicações e outros). Contudo, a parte fundamental das transformações foram as facilidades e melhorias proporcionadas através das tecnologias da informação [3].

Dois mundos de tecnologias evoluindo paralelamente, tecnologias da informação para as redes de telecomunicações e tecnologias para área de energia:

- **Tecnologia da informação:** As redes de telecomunicações digitais, trouxeram a possibilidade do transporte de informações de controle entre os elementos da rede elétrica.

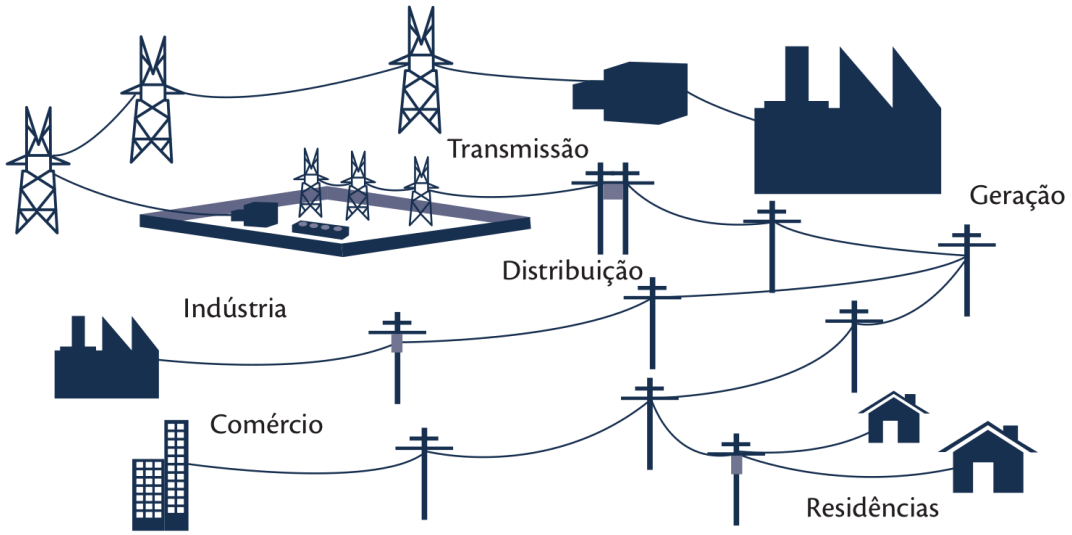

Figura 1.1: Rede elétrica.

Dispositivos capazes de realizar entrega de informações quase em tempo real, melhorando o desempenho de inúmeras aplicações, interconectando centros de controle e subestações distintas, aumentando drasticamente o número de ações rápidas e remotas, etc.

- **Tecnologia para redes de energia:** As tecnologias da rede de energia também evoluíram, pois com um significativo aumento demográfico, o que torna o consumo de energia cada vez maior, novos dispositivos foram necessários, e portanto desenvolvidos, como por exemplo, relés mecânicos, eletrônicos e, finalmente digitais.

É inerente o impacto do consumo de energia na sociedade, seja em suas residências, locais de trabalho, hospitais, supermercados entre outros. Diante desse cenário, a operação incorreta de um dispositivo de proteção, pode levar a interrupção de grandes blocos de fornecimento de energia, desligamentos em cascata; e em cenários piores, ocasionar queima de equipamentos e até mesmo causar mortes; acarretando grandes prejuízos para as concessionárias de energia, através de multas e degradação do nome da empresa; e para os consumidores através de perda de mercadorias, interrupções de jornada de trabalho e limitação nos serviços essenciais.

Mesmo com o crescimento exponencial da demanda, as redes de transmissão de energia evoluíram de forma limitada para enfrentar esses desafios, ainda que usando muitas tecnologias legadas (de telecom e energia) para realizar o controle e a gerência das diversas linhas de transmissão e distribuição de energia elétrica. As *utilities* já enfrentam problemas como: interconexão das redes de distribuição com a energia gerada pelas usinas a partir de fontes alternativas e a energia gerada pelo próprio cliente; monitoramento da demanda de energia para evitar as demandas de pico; adaptação da geração de energia para a chegada dos veículos elétricos; dentre outros [4]. Para enfrentar estes problemas e futuras mudanças, as distribuidoras de energia precisam repensar seu modelo de trabalho.

Neste contexto, o que é extremamente difícil de realizar é a integração de todas as equipes de trabalho e áreas correlatas, em redes de teleproteção para redes de transmissão de energia, pois a exigência de conhecimento é muito amplo e complexo, tornando extremamente árduo entender todos os requisitos, configurações, detalhes e riscos envolvidos, dificultando a integração de áreas distintas que convergem para o mesmo objetivo. Uma situação de alta complexidade.

Para enfrentar os desafios atuais e futuros, promover segurança, sustentabilidade e tornar o sistema elétrico acessível, é preciso inserir fontes renováveis, inteligência autônoma para agir apropriadamente em todos os níveis e promover um maior envolvimento dos consumidores finais, pois suas necessidades determinam o rumo do progresso.

É necessário que todo o sistema seja mais robusto e capaz de superar dificuldades de integração, tornando as operações diárias mais seguras contra falhas, possíveis ataques cibernéticos, provendo escalabilidade para demandas futuras e integração com fontes de energia renováveis [5].

Para revolucionar a forma de pensar e agir, e suprir as necessidades citadas anteriormente, surgiram as Redes Elétricas Inteligentes (REI) ou *Smart Grids* (SG), que trazem evolução na forma de produção, distribuição e consumo de energia, pois usam tecnologia digital avançada, monitorando e gerenciando o fluxo bidirecional de informações entre o sistema gerador e o cliente. E com as SGs surgiram novas demandas, novos aparelhos e um aumento da necessidade de integrações geográficas. A utilização de energia elétrica está no coração de quase todas as indústrias, serviços, e em quase todos os lares nas cidades as quais tenham ao menos uma infraestrutura básica de atendimento aos cidadãos.

Colocado o contexto em que esse trabalho se apresenta, ressaltamos ainda que essa dissertação de mestrado faz parte do "Projeto D0640 - Modelo de Referência para a Rede Operativa de Dados da CEMIG", que foi realizado em parceria entre FITec (Fundação para Inovações Tecnológicas) e Inatel (Instituto Nacional de Telecomunicações). O projeto teve seu inicio em em 11/2018 e finalização em 3/2020. Esse trabalho começou pela revisão bibliográfica, tanto do ponto de vista acadêmico, quanto de casos de uso de mercado e as tecnologias utilizadas em redes operativas de dados em ambiente de transmissão, distribuição de energia e *smart grid*.

Foram realizados estudos e análises de tecnologias de redes de comunicação por circuitos (determinísticas) e por pacotes (estatísticas) envolvendo características de transmissão de dados, qualidade de serviço, equipamentos, tecnologias aplicáveis e tendências de mercado, e agregação novos serviços sem que esses impactassem negativamente aqueles de missão crítica. Desenvolveu-se uma revisão do estado da arte das tecnologias de comunicação [6] para os diversos domínios da rede de energia (HAN, NAN/FAN e WAN), levando em consideração tecnologias de comunicação por circuitos e tecnologias de comunicação por pacotes, que pudessem prover a coexistência de novos serviços com os serviços de missão crítica e medição inteligente. Tecnologias chaves como PDH, SDH, NG-SDH, PLC, MPLS, PON, OTN, WiMAX, 3G, 4G, radioenlaces e satélites, dentre outras, foram analisadas e correlacionadas com o tema do projeto. Tendo como foco missão crítica, teleproteção, auto-cura, comunicação com religadores e centros de comando.

Em SGs modernizar as redes de telecomunicações para evoluir a teleproteção de redes de distribuição de energia é uma demanda fundamental e urgente. Os processos envolvidos no desenvolvimento e implantação de um novo produto ou uma nova tecnologia, precisam atender fatores cruciais como, tempo, custo, qualidade e segurança. O cenário observado para evoluir de forma convergente as redes de energia e teleproteção possui diversas dificuldades, dentre elas estão a complexidade do produto/serviço e o melhor uso dos recursos(humano ou matéria prima) disponíveis. Levando em consideração este contexto, existem três formas de avaliar opções de modernização de SGs, sendo elas (com suas vantagens e desvantagens):

- **Experimentos em laboratórios ou de campo:** Os experimentos em laboratório das próprias *utilities* facilitam muito a pesquisa e desenvolvimento, pois o coração do projeto e das implementações estão ali. É muito fácil ver todas as variáveis envolvidas, ter acesso a todos os equipamentos e a todas as equipes como um todo, sejam elas de implantação, desenvolvimento ou suporte. As desvantagens percebidas são diversas, dentre elas: (i) fornecedor disposto a oferecer equipamentos para testes; (ii) é necessário ter equipamentos para realizar as medidas adequadamente; (iii) é necessário ter janelas de testes na empresa; (iv) deve haver interesse de todas as equipes para a realização da pesquisa e desenvolvimento, pois é difícil poucas pessoas dominarem todo o *know-how* necessário; e (v) ter especialistas disponíveis nas datas agendadas.

- **Modelos analítico e matemático:** Sistema de equações obtidos de situações-problema, ou seja, fórmulas matemáticas desenvolvidas, normalmente de forma manual, conseguem definir variáveis diversas para inúmeras situações. Possui baixo custo, precisão bem maior e respostas rápidas e diretas, pois os resultados são gerados com maior agilidade. Entre-

tanto, facilmente se tornam intratáveis, principalmente quando a complexidade do sistema sendo modelado é alto, em especial SGs e teleproteção.

- **Simulações e emulações:** Capacidade de avaliar em um mesmo ambiente, todos os sistemas e dispositivos envolvidos. Produz boas aproximações e permite ampliação das análises em geral. As vantagens são: (i) a integração de simuladores com emuladores permite aproximar o cenário computacional ao de experimentação; (ii) custo reduzido, que é uma das demandas para países em desenvolvimento como o Brasil; (iii) flexibilidade para alterar cenários, realizando rapidamente novos testes; (iv) facilidade para integração de equipes, pelo fato do ambiente estar em uma única máquina ou local, facilita reuniões e discussões *online* com compartilhamento de tela; (v) pesquisa e desenvolvimento de novas funcionalidades sem depender de *hardware* específico. Como desvantagens tem-se: (a) não produzir resultados exatos, dependendo das abstrações adotadas e dos requisitos considerados; (b) limitação das configurações de *hardware* do computador, por exemplo, processador e memória RAM, pois a taxa de erro é menor com menor quantidade de memória [7]; (c) nem sempre os equipamentos existentes no mundo físico existem da mesma forma no virtual.

  Nesta dissertação será feito o uso de um software que é um simulador de rede, contudo, este possui características de emulador de nós. O software simula uma rede de teleproteção e o tráfego entre o *link* principal e o *link* secundário. O mesmo software é capaz de emular dispositivos de teleproteção e relés para a rede elétrica.

As simulações computacionais são revolucionárias e extremamente eficientes em todas as áreas da pesquisa científica. É muito importante simular o que se deseja implementar ou até mesmo realizar alterações em fase inicial de projeto. Ao serem levantados os principais requisitos, as simulações conseguirão abstrair as respostas dos sistemas reais em uma sucessão de ocorrências. Isso torna possível um ganho enorme de conhecimento.

Podemos definir simulação com uma abstração computacional de um sistema ou rede para fins de experimentação e avaliação de desempenho. Para tanto, os principais aspectos da tecnologia em estudo devem ser abstraídos para um modelo computacional, que representa na quantidade de detalhes necessária o problema em questão. A simulação difere da emulação, onde algo físico é emulado *ipsis litteris*.

As principais vantagens ao se implementar as simulações são percebidas em poucas palavras, como por exemplo em [8], ao se realizar as simulações conseguimos uma redução de custos, pois nem sempre equipamentos voltados para as redes de teleproteção são baratos e de fácil acesso. A utilização de simulação reduz o tempo necessário para análise de desempenho quando comparado as duas outras soluções possíveis: modelamento analítico e experimentação em campo. Além disso, a simulação é importante para validar resultados obtidos por esses dois outros métodos.

Esse trabalho é baseado em simulações, entretanto para o melhor entendimento, é preciso separar e definir os conceitos de simulação e emulação. Simular é imitar o comportamento de um sistema, sem necessariamente reproduzir todos os seus componentes e detalhes internos. Nesse trabalho, a simulação de sistemas completos de teleproteção em redes de transmissão de energia é utilizada para provar nossa hipótese de pequisa, que será descrita nos próximos parágrafos.

Emular é reconstruir em *software* o sistema de um equipamento, um dispositivo, em todos os seus detalhes, de forma que um cliente não consegue ver diferença em relação a um sistema físico. No contexto deste trabalho, a emulação de alguns equipamentos de rede foi realizada; ou seja, principalmente os roteadores que realizam a comunicação entre as subestações de transmissão de energia. Uma ferramenta que permita a simulação e/ou a emulação de equipamentos de diferentes fabricantes, possibilita que a complexidade de todo o sistema modelado possa ser drasticamente reduzida, devido as abstrações adotadas na parte de simulação.

Desta forma, converge-se em um ambiente único as plataformas de experimentação e avaliação de desempenho, unificando configurações e execuções, visto que, o pesquisador ou desenvolvedor responsável, tem acesso a todas as partes dos recursos envolvidos no ambiente físico,

podendo então realizar testes que não são possíveis de serem realizados em campo. Assim sendo, podemos responder com mais segurança as principais perguntas que ocorrem em redes de teleproteção de sistemas elétricos de potência atualmente, que são: é possível trocar alguma tecnologia legada (de telecomunicações ou da parte elétrica) por outra atual e que comprovadamente possui um desempenho melhor? Se for possível trocar, o desempenho será melhor.

Nesse contexto, essa dissertação trata da integração de ferramentas de simulação e emulação em laboratório visando avaliar possibilidades de modernização da teleproteção em redes de energia, em especial para atender a demanda da operadora CEMIG (no contexto do Projeto P&D 0640). Este tema foi escolhido pois o ambiente de simulação/emulação em redes de teleproteção está muito pobre de recursos e integrações, tendo em vista que pessoas de áreas específicas nem sempre estão dispostas ou até mesmo, não possuem o espirito de pesquisa e desenvolvimento; além da falta de recursos e agenda para avaliar a modernização das redes de teleproteção de energia. Outro aspecto é que algumas das ferramentas que encontramos no inicio do Projeto P&D 0640 possuem alto custo. Ou seja, buscar ferramentas de baixo custo que possam ajudar nesse processo de transformação e modernização da teleproteção é de suma importância.

Espera-se com esse trabalho tornar possível a análise de desempenho acessível e abrangente de opções tecnológicas para modernização das redes de teleproteção de energia, integrando simulação/emulação, facilitando a convergência de diferentes equipes e áreas de conhecimento nas operadoras de energia (em especial, na CEMIG), oferecendo visão do sistema como um todo, para todos os colaboradores. Além disso, para validar a ferramenta integrada de avaliação de teleproteção por simulação/emulação uma comparação com resultados de laboratório obtidos na CEMIG do Anel Rodoviário de Belo Horizonte é fornecida, dentro do contexto dos trabalhos realizados no Projeto P&D 0640.

A solução proposta via simulação/emulação tem custo inferior, maior flexibilidade, ferramentas integradas em um único ambiente, ferramentas modulares/escaláveis/flexíveis, possibilidade de implantação de serviços como *softwares*, facilidade nas configurações de integração, permitindo realizar estudos na área de transmissão de energia e redes de teleproteção. Deste modo, os principais requisitos serão elencados para que testes e validações com baixo custo e alta precisão de acerto, possam ser realizados em aplicações de SG ou em sistemas de geração e distribuição de energia com a ajuda da softwarerização.

A solução para diversos problemas em distribuição de energia elétrica está em integrar ou substituir equipamentos responsáveis pela gerência e controle da distribuição de energia, aos equipamentos de telecomunicações, capazes de realizar a comunicação IP, através da comutação de pacotes (com multiplexação estatística). E com isso, acompanhar os novos serviços que já possuem interfaces de comunicação e estão operando com as tecnologias IP, as quais fornecem uma maior flexibilidade e eficiência ao gerenciar o compartilhamento dos recursos dos enlaces e dos centros de controle. Nas redes IP, o principal protocolo a ser estudado e testado para a integração ou migração em SG, é o Multiprotocol Label Switching (MPLS) [9], o qual tem a missão de entregar acessos a multiserviços, estabilidade, confiabilidade, fácil escalabilidade e uma fácil detecção e gestão de falhas. Essa é talvez a principal possibilidade de modernização da rede de teleproteção de energia principal proposta no Projeto P&D 0640. Entretanto, outros caminhos serão explorados para fim de comparação.

Assim sendo, o principal objetivo deste trabalho é alcançar a maior proximidade possível, em um ambiente simulado/emulado, do ambiente de redes de teleproteção em redes de transmissão de energia experimentado no Projeto P&D 0640 em laboratório da CEMIG. Realizar comparações de desempenho e levantar todos os requisitos necessários para que, um ambiente de híbrido de simulação/emulação seja construído, aproximando ao máximo o ambiente de testes real desenvolvido no contexto do projeto P&D 0640.

Ou seja, esse trabalho ataca o problema da modernização e/ou migração das redes de teleproteção de energia para tecnologias baseadas em pacotes. Pretende superar as limitações existentes tanto na análise experimental, quanto analíticas quando se pretende validar novas tecnologias de telecomunicações para teleproteção. Nossa hipótese é que o uso de emulação e simulação computacional de redes de telecomunicações é um importante aliado no processo

de modernização e comprovação de benefícios de novas tecnologias de telecomunicações para teleproteção. Para tanto, integramos diversas ferramentas de emulação e simulação em um cenário que se aproxima de experimentos reais. Provamos que o ambiente integrado pode obter resultados simulares e ser utilizado para planejamento de SGs e novas redes de teleproteção.

1.1 Motivação e Questão de Pesquisa

Esta dissertação tem como principal motivação, buscar e analisar as melhores formas de responder as seguintes questões:

É válido e eficiente implementar nas redes de transmissão de energia equipamentos capazes de realizar os serviços de teleproteção e comunicação através de MPLS-IP? É possível a criação de um ambiente de simulação/emulação, capaz de abranger parte do sistema de teleproteção da CEMIG?

O cerne dessa dissertação é buscar ao máximo, extrair das principais formas de simulação e/ou emulação, as melhores formas de realizar a integração de equipamentos que, compõem uma rede de teleproteção em uma rede de transmissão de energia. Equipamentos que tenham as mesmas funcionalidades de acordo com as normas globalmente difundidas, entretanto, podendo ser de diferentes fabricantes.

A tendência global em todas as áreas é, analisar os serviços ofertados e transformá-los em *software* quando possível (softwarização). Desta forma, inúmeras oportunidades podem ser criadas, como por exemplo, integrações de tecnologias de fabricantes diferentes se tornarão comuns. Portanto, ambientes de co-criação e simulações/emulações precisam evoluir o mais rápido possível desbravando estes caminhos.

1.2 Objetivos

Este trabalho tem como objetivo principal analisar o desempenho de alternativa de modernização da rede de teleproteção de energia da CEMIG usando redes de pacotes com MPLS-IP, para a migração das redes operativas de missão critica, no contexto do projeto P&D D0640 - Modelo de Referência para a Rede Operativa de Dados da CEMIG.

O principal foco deste trabalho é criar uma simulação/emulação, que se aproxime ao máximo de uma rede de teleproteção real da CEMIG, utilizando o *software* GNS3 (posteriormente, será explorada a questão de escolha da ferramenta usada nesse trabalho). Construir uma topologia simulada semelhante a uma topologia de rede física real, e configurar os protocolos de forma que se aproximem ao máximo de uma rede construída em laboratório. Realizar testes e uma comparação entre os resultados obtidos nos equipamentos reais e nas simulações/emulações dentro do contexto do projeto P&D 0640.

Para atingir o objetivo geral, foram definidos os seguintes objetivos específicos:

(i) Realizar um estudo sobre o estado da arte relacionado a todos os tipos de simuladores/emuladores disponíveis no mercado e academia, que possam ser usados para construir modelos semelhantes para redes de teleproteção;

(ii) Realizar uma comparação dos trabalhos encontrados neste estudo com base em critérios similares e encontrar lacunas de convergência;

(iii) Adotar um modelo de simulação/emulação que preencha as lacunas encontradas nos ambientes de simulação/emulação pesquisados e realização de testes;

(iv) Avaliar o protótipo de simulação/emulação dentro do ambiente GNS3 [10], com base em um conjunto de protocolos que mais se aproximam do ambiente real da CEMIG;

(v) Analisar os resultados obtidos e comparar estes resultados, com os resultados obtidos em testes utilizando equipamentos reais.

1.3 Publicações

Neste tópico estão listados a seguir trabalhos e artigos publicados pelo autor que corroboram direta e indiretamente para a construção do trabalho final de dissertação de mestrado.

1.3.1 Publicações do projeto CEMIG

1. L. F. F. de Almeida, José Rodrigo dos Santos, Luiz Augusto Melo Pereira, Arismar Cerqueira Sodré, Luciano Leonel Mendes, Joel J. P. C. Rodrigues, Ricardo A. L. Rabelo e Antonio Marcos Alberti, "Control Networks and Smart Grid Teleprotection: Ky Aspects, Technologies, Protocols and Case-Studies", in IEEE Access, doi: 10.1109/ACCESS.2020.3025235.

2. L. F. F. de Almeida, L. H. M. Leite, R. A. Fernandes, J. R. dos Santos, R. J. Machado, W. R. Silva, J. J. P. C. Rodrigues e A. M. Alberti, "Análise de Redes de Dados Estatísticas para Teleproteção de Linhas de Transmissão de Energia", in VIII Simpósio Brasileiro de Sistemas Elétricos, 2020, Santo André. Anais do SBSE, 2020.

1.3.2 Publicações de outros projetos

1. Santos, J., Rezende, T., Silva, T., Rosário, E., Alberti, A. (2020). Proposta de Arquitetura para Distribuição de Conteúdos Nomeados em NovaGenesis com P4. In Anais do XI Workshop de Pesquisa Experimental da Internet do Futuro, (pp. 32-37). Porto Alegre: SBC. doi:10.5753/wpeif.2020.12472

2. Alberti, A.M.; Bontempo, M.M.; Dos Santos, J.R.; Sodré, A.C., Jr.; Righi, R.D.R. NovaGenesis Applied to Information-Centric, Service-Defined, Trustable IoT/WSAN Control Plane and Spectrum Management. Sensors 2018, 18, 3160. https://doi.org/10.3390/s18093160

3. Alberti, A., Santos, J., Morais, E., Santos, R., Magalhães, V. (2018). Forwarding/-Routing with Dual Names: The NovaGenesis Approach. In Anais do IX Workshop de Pesquisa Experimental da Internet do Futuro. Porto Alegre: SBC.

4. DOMINGUES DAVILA, Victor Hugo; ROSÁRIO, Élcio; DOS SANTOS, José Rodrigo; ALBERTI, Antonio Marcos . NovaGenesis NameBindings: Avaliação de Virtualização em Escala. In: WORKSHOP DE PESQUISA EXPERIMENTAL DA INTERNET DO FUTURO (WPEIF), 10. , 2019, Gramado. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019 . p. 7-12. ISSN 2595-2692. DOI: https://doi.org/10.5753/wpeif.2019.7692.

5. ALMEIDA, Fabio ; BONTEMPO, Marília M.; DOS SANTOS, José Rodrigo ; ALBERTI, Antonio Marcos . Uma Proposta de Contramedida ao Ataque Jamming em Redes IEEE 802.15.4 utilizando Rádio Cognitivo. In: WORKSHOP DE SEGURANÇA CIBERNÉTICA EM DISPOSITIVOS CONECTADOS (WSCDC), 2. , 2019, Gramado. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019 . p. 12-22. DOI: https://doi.org/10.5753/wscdc.2019.7702.

6. A. M. Alberti, E. C. do Rosário, G. Cassiano, J. R. dos Santos, V. H. D'Ávila and J. R. Carneiro, "Performance evaluation of NovaGenesis information-centric network,"2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech), 2017, pp. 1-6.

1.4 Organização da dissertação

Esta dissertação está organizada em 6 capítulos. Após a introdução apresentada no Capítulo 1, os conceitos principais para o entendimento e compreensão do restante do trabalho e da pesquisa proposta são apresentados no Capítulo 2; o Capítulo 3 apresenta uma lista com trabalhos relacionados ao tema proposto nesta pesquisa; no Capítulo 4 evidência os tipos de testes e abordagens que foram realizados com equipamentos reais e simulação/emulação; o Capítulo 5 apresenta uma análise dos resultados que comprovam nossa hipótese, bem como um comparativo entre eles; por fim, o Capítulo 6 apresenta as conclusões e as considerações finais do presente trabalho.

Capítulo 2

Fundamentação Teórica

Neste capítulo, foram levantados os conceitos para o entendimento do cenário de trabalho como um todo, visando o melhor entendimento desta dissertação. É realizada uma pesquisa sobre as redes de energia, a qual se enquadra em uma rede de missão crítica, portanto, usa as redes de telecomunicações para criar uma infraestrutura de redes de teleproteção. Em seguida, é feita uma avaliação de todas as oportunidades de pesquisa e desenvolvimento, que podem ser realizados ao utilizar todo o poder computacional para se realizar simulações/emulações, em todos os níveis de uma rede de transmissão de energia.

2.1 Redes de Transmissão de energia

A energia elétrica ao sair das usinas, geradores elétricos ou alguma fonte alternativa de energia, é transportada utilizando cabos aéreos, cobertos por camadas isolantes e fixos em grandes torres de metal. Formando o sistema de distribuição de energia e normalmente de alta tensão, que é ramificado em níveis menores de tensão dentro das próprias concessionárias ou em outros pontos estratégicos.

As linhas de transmissão percorrem grandes distâncias e conectam os sistemas geradores aos sistemas consumidores, que podem ser empresas de grande porte, como por exemplo, mineradoras ou empresas distribuidoras de energia, as quais repassam a energia aos consumidores de menor porte.

Existem linhas de transmissão de baixa, média e alta tensão e são classificadas de acordo o nível operação. De acordo com a ANEEL [11], é considerado alta tensão quando a voltagem é superior a 69 kV indo até 230 kV. São consideradas redes básicas do sistema. Média tensão é superior a 1 kV até 69 kV. Normalmente, a responsabilidade por essas linhas são das empresas distribuidoras. Por fim, baixa tensão é inferior a 1 kV.

Distribuidoras de energia trabalham com média e baixa tensão, conhecidas como redes primárias e secundárias. As redes de média tensão trabalham com tensões entre os valores de 2,3 kV e 44 kV, podendo ser observadas nas cidades, em suas ruas e avenidas, normalmente compostas por 3 cabos aéreos em cruzetas de madeira, localizadas em postes de concreto [12]. Já nas redes de baixa tensão, os valores de voltagem podem variar entre 110 V e 440 V, de acordo a região.

As subestações de energia são o ponto de conexão entre geradores, empresas distribuidoras e consumidores. A função principal é elevar o nível de tensão para centenas e milhares de volts, possibilitando vantagens enormes, como por exemplo, redução de corrente elétrica, redução das seções dos cabos proporcionando redução de custos e perdas de energia. As subestações possuem equipamentos para manobras de manutenção, disjuntores, equipamentos medidores de tensão e corrente e equipamentos de proteção, como por exemplo, para raios e relés. E com estes dispositivos, principalmente os relés, será capaz de aprofundar o estudo sobre redes de missão critica, que é o assunto da próxima seção.

2.2 Redes de Missão Crítica

Missão crítica esta vinculada a tudo que diz respeito a disponibilidade de recursos. Sejam recursos físicos, aplicações, quaisquer serviços ou processos. E ao gerar interrupção, os danos colaterais serão enormes.

Missão crítica esta vinculada a um ambiente tecnológico que utiliza inúmeros equipamentos e técnicas para evitar a interrupção de um serviço. Em redes de transmissão de energia, as técnicas de missão crítica precisam garantir que as falhas não ocorram na rede, que os equipamentos e serviços devam fornecer alta confiabilidade e disponibilidade de funcionamento. Do ponto de vista dos serviços de telecomunicações, o sistema deve possuir enlaces redundantes e resilientes em termos de segurança cibernética.

Além dos extremos de temperatura que pode ocorrer nas regiões onde serão instalados, os equipamentos de comunicação de missão crítica para os serviços públicos, também estão expostos a campos magnéticos e elétricos, que são particularmente severos durante eventos de curto-circuito. Para manter os altos níveis de disponibilidade necessários, especialmente em situações de emergência, os equipamentos de comunicação da concessionária devem oferecer um *design* robusto e confiável, com capacidade comprovada para fornecer funcionalidade precisa sob condições extremas.

2.2.1 Redes de Teleproteção

As redes de teleproteção usam as redes de telecomunicações. Através delas, os equipamentos de teleproteção atuam, localizados em duas extremidades de uma linha de energia. Em caso de falha, enviam e recebem comandos em alta velocidade, que alteram o comportamento de um ou mais dispositivos na rede.

O sistema de teleproteção é geralmente instalado em redes de transmissão de energia de alta voltagem, com objetivo de prevenir a instabilidade nas linhas de transmissão e, consequentemente, a danificação dos equipamentos das subestações, desastres ou até mesmo mortes.

Sua principal função é monitorar as linhas de transmissão, coordenando mensagens rápidas entre os relés de proteção dos terminais da rede para rapidamente isolar possíveis faltas na mesma. Visto que boa parte de sistemas de transmissão de energia são interligados em anel, é necessário o desligamento em ambos os terminais para a isolação de uma falta na linha. Para lidar com esse problema, o sistema de teleproteção é composto de relés de proteção e equipamentos de teleproteção, ambos inseridos nas subestações. Desta forma, quando há uma falta na linha de transmissão, o relé de proteção da subestação mais próxima detectará a ocorrência do problema, realizando a comutação de um lado do terminal, enquanto que os dados serão coletados pelo equipamento de teleproteção, que enviará a informação ao outro equipamento disponível no terminal remoto para que haja a ação no relé da sua respectiva subestação e, consequentemente, se isole a linha com a falha [13].

2.3 Redes de Telecomunicações

As redes de telecomunicações abrangem toda a infraestrutura necessária para atender os serviços do usuário final. Elas podem ser classificadas de acordo com sua área de cobertura e as taxas de dados necessários para operação correta de acordo com a aplicação. Neste contexto, as redes de operações são dividas em HAN (Home Area Network) /BAN (Building Area Network)/IAN (Industrial Area Network), NAN (Neighborhood Area Network) /FAN (Field Area Networks) e WAN (Wide Area Network).

Nas redes de telecomunicações existem equipamentos que realizam a liberação e escolha dos melhores caminhos os quais possibilitarão realizar a comunicação com o usuário final. Esta técnica é conhecida como comutação, sendo utilizada para encaminhar informação de um entrada para uma saída em um equipamento de rede.

Elas podem ser desenhadas com comutação de circuitos ou de pacotes. A comutação de circuitos teve sua origem na telefonia, enquanto a comutação de pacotes surgiu como uma alternativa ao modelo de rede estabelecido na época (década de 60). A comutação de pacotes busca melhor flexibilidade e eficiência do uso dos recursos dos enlaces através do seu compartilhamento. A comutação de circuitos trabalha com recursos dedicados.

2.3.1 Comutação de Circuitos

É a existência de recursos de comunicação fim a fim, completamente alocado para dois terminais, sendo composto por troncos adjacentes dedicados e conectados entre si, por meio de conexão física, como por exemplo, fibra óptica, ou através de conexão virtual, realizadas mediante técnicas de multiplexação, sendo a mais comum a TDM (Time Division Multiplexing) [14], criando assim, fatias de um enlace físico, por exemplo, *slot* de tempo ou um canal de frequência. Este circuito fisico ou lógico criado, passa por todos os elementos da rede e permanecendo exclusivo até encerrar a conexão.

Para utilizar a comutação de circuito cada nó precisa ter aplicações com capacidade de alocação de recursos, para os circuitos que forem solicitados e poder de roteamento para descobrir os melhores caminhos. Uma grande desvantagem da comutação de circuitos é que os recursos alocados nem sempre terão sua taxa de utilização máxima, portanto, ficarão alocados em sua totalidade e não serão utilizados.

2.3.2 Comutação de Pacotes

Na comutação de pacotes não existe um caminho dedicado durante a comunicação entre dois terminais. As informações são encapsuladas e trafegam dentro de pacotes. Se forem informações grandes serão fragmentadas em partes menores, capazes de trafegar na rede. Ao longo do caminho, também podem ter seus tamanhos alterados pela fragmentação necessária de algum enlace com capacidade menor. Os pacotes podem viajar através de inúmeros caminhos diferentes, pois ao longo do percurso, podem existir algoritmos de roteamento diferentes, que através de suas métricas são capazes de identificar enlaces congestionados, escolhendo uma nova rota, portanto, os caminhos em sua maioria são dinâmicos.

Cada pacote possui cabeçalhos, caudas e *payload*. Os cabeçalhos ou caudas contém informações de controle e endereçamento, portanto são capazes de trafegar pela rede e chegar ao destino. O **payload** é a carga útil, ou seja, a informação a ser entregue.

2.4 Ferramentas de simulação

Nesta seção serão abordadas ferramentas de simulação de sistemas físicos que atuam em uma rede de transmissão de energia, como por exemplo relés. E ferramentas de simulação das redes de comunicação.

Foi realizado um levantamento das ferramentas disponíveis no mercado ou academia, que tem o potencial de levar os cenários presentes nos sistemas de missão crítica para um ambiente controlado de simulação/emulação.

Avaliando as opções disponíveis que permitissem simular/emular os cenários desejados, diversas dificuldades foram enfrentadas para encontrar ferramentas que contemplassem tanto a parte de potência (relés, transformadores, etc), quanto a parte de telecomunicações, uma vez que o simuladores/emuladores disponíveis, ou possuem o foco em sistemas de controle ou em sistemas de comunicação. A primeira abordagem para continuar os estudos foi criar uma solução para resolver esse impasse, verificado a possibilidade de um ambiente de simulação/emulação, onde um simulador/emulador seria responsável por toda parte de comunicação e o outro seria responsável pela parte de potência do sistema. Solução implementada e explicada com mais detalhes no Capítulo 3.

A principal vantagem do ambiente de simulação/emulação proposto está na possibilidade de avaliar o comportamento geral do sistema, uma vez que isso não é possível quando é avaliado o sistema de controle e o sistema de comunicação separadamente. Além disso, em sistemas de simulação/emulação, podemos avaliar o comportamento de ambientes complexos, onde múltiplos *loops* de controle e de comunicação estão presentes, o que seria inviável de realizar matematicamente.

Desta forma, a seguir é realizado o levantamento das ferramentas, separando-as em ferramentas de sistemas físicos e ferramentas de simulação/emulação de sistemas de comunicação.

2.4.1 Simuladores de sistemas físicos

Nesta subseção serão apresentados os principais simuladores/emuladores para sistemas físicos.

RTDS

O Real Time Digital Simulator (RTDS) é uma poderosa ferramenta de simulação, sendo utilizada na análise de comportamento dos sistemas de energia e dos componentes presentes neste sistema. Esta ferramenta possui uma grande utilização na avaliação de elementos que estão prontos para serem incorporados às redes de distribuição de energia. Além disto, o simulador pode ser utilizado durante o processo de desenvolvimento de novos dispositivos, principalmente nos que se refere a área de controle e de proteção dos sistemas elétricos. Através desta ferramenta é possível avaliar as respostas desses novos componentes ao sistema já existente, possibilitando a alteração e o aprimoramento destes novos dispositivos de acordo com as necessidades da rede.

O simulador conta com um Hardware e um *Software* personalizável. O *Hardware* atual utilizado pelo RTDS é chamado de NovaCor, sendo este, baseado em uma estrutura metálica (Chassi) composta por poderosos processadores *multicore* que permitem acesso escalável através do licenciamento de núcleos. Caso ocorra um aumento na demanda de processamento, o proprietário pode optar pela adição de mais processadores ao hardware original. Ainda referente ao Hardware, o simulador conta com locais para a instalação de cartões I/O e outros componentes. Os cartões I/O possuem a funcionalidade de permitir que o simulador opere com dispositivos externos, tais como relés de proteção, por exemplo. O RTDS possui um *software* proprietário chamado RSCAD. O *software* foi desenvolvido especificamente para o RTDS, possuindo uma interface amigável ao operador e tendo como princípio o fornecimento de todos os recursos necessários para o operador em apenas uma ferramenta. Assim sendo, o software conta com um ambiente para a criação e execução das simulações, além de fornecer uma interface para a análise dos resultados obtidos.

Com a característica de operar em tempo real, o sistema simulado pode atuar de forma semelhante ao sistema de energia real. Através disto, o operador pode realizar alteração nos parâmetros da rede e observar o impacto dessas alterações no sistema, verificando como o sistema de energia emulado responde em tempo real. Devido seu grande poder de processamento e sua capacidade de simulação em tempo real, o RTDS pode ser utilizado em diversos domínios, sendo eles: simulações de microgrids, segurança cibernética, *hardware* de energia em *loop*, testes de sistemas de proteção, eletrônica de potência, testes de sistemas de controle, *smart grids* e geração distribuída, IEC 61850 [15], estudos em unidade de medição fasorial, entre outras áreas.

MATLAB/Simulink

A ferramenta MATLAB (*Matrix Laboratory*) é uma ferramenta de alto desempenho e interativa voltada para cálculos numéricos. Essa ferramenta foi criada no início dos anos 1970 pelo então professor de matemática Cleve Moler enquanto ele fazia parte do departamento de ciência da computação da universidade do Novo México (EUA). Após conhecer a linguagem MATLAB através de uma visita de Cleve Moler a *Stanford* em 1983, o então engenheiro Jack Little, reconhecendo o grande potencial da ferramenta, se juntou a Cleve Moler e Steve Bangert

para juntos reescreverem o MATLAB para a linguagem C, adicionar os arquivos .M toolboxes e ferramentas gráficas mais poderosas. Juntos os três fundaram a MathWorks em 1984 [16].

O *software* é um dos simuladores mais utilizados para a representação de sistemas físicos, possuindo uma grande variedade de ferramentas e algorítimos para uma maior garantia de precisão dos modelos, além de um extensivo leque de funções base já desenvolvidas, contando também com um suporte de grande qualidade para os usuários através de seu site oficial e de fóruns espalhados pela web [17].

Também desenvolvido pela MathWorks, o Simulink se apresenta como uma poderosa ferramenta para a modelagem, simulação e avaliação de sistemas dinâmicos. Esta ferramenta utiliza uma interface gráfica com uma biblioteca repleta de blocos que podem ser empregados para representar diferentes sistemas. Os projetos desenvolvidos pelos usuários no Simulink podem ser implementados interligando os diferentes blocos presentes na biblioteca ou através de blocos criados pelo próprio usuário, além de oferecer uma terceira alternativa onde os blocos são escritos através da linguagem C, tomando como base um modelo denominado S-Function. Através da interconexão das ferramentas MATLAB e Simulink, é possível combinar a programação gráfica e textual para obter o design dos sistemas desejados. Via interação entre os *software* é possível utilizar os milhares de algoritmos já desenvolvidos para o MATLAB, adicionando o código a um bloco do Simulink [**?**].

É possível a criação de relés com atuação sobre tensão, subtensão e sensíveis às variações de frequências da rede. Os relés de sobre tensão e subtensão podem ser desenvolvidos conforme os modelos ANSI/IEEE C37.2 que operam quando a tensão excede ou quando é menor que um limite inferior ou superior é pré-determinado na simulação, normalmente ficando entre 1 % a 25 % do valor de tensão nominal que a rede opera. As especiações do atraso de sobre tensão e subtensão podem ser especificadas entre 0,1s a 30s. Os relés que atuam com as variações de frequências também seguem o modelo ANSI/IEEE C37.2, porém com atuações com valores excedidos de 1% a 20 % da frequência nominal da rede.

Ficou comprovado a possibilidade do uso de MATLAB/Simulink para o modelamento dos relés e equipamentos utilizados nos sistemas de missão crítica, porém é necessário a obtenção de diversas *toolboxes* diferentes, acarretando em um custo elevado para esta implementação, portanto, sendo descartada a hipótese de usar o MATLAB/Simulink em nosso trabalho.

2.4.2 Simuladores de redes de comunicação

Nesta seção, será realizado um levantamento dos principais simuladores de redes de telecomunicações, presentes no mercado, que permitem simular a rede IP sobre MPLS (e/ou MPLS-TP) necessária para concluir o projeto.

Riverbed Modeler

Anteriormente, conhecido como OPNET Modeler, o Riverbed Modeler surgiu com a aquisição da empresa OPNET Technologies Inc em outubro de 2012 pela Riverbed Technology. O Riverbed Modeler é um simulador de eventos discretos criado para o design e análise de redes de comunicação. A ferramenta se trata de um *software* proprietário, porém possui uma versão Open Source denominada Riverbed Modeler Academic Edition [18].

O *software* oferece suporte para o modelamento de diferentes tecnologias de rede como: VoIP, TCP, OSPFv3, MPLS, IPv6, dentre outras [18]. Através destes modelos, é possível verificar o impacto de diferentes *designs* de tecnologias no comportamento de ponta a ponta de determinada rede de comunicação. O simulador permite que os desenvolvedores testem e demonstrem seus projetos antes de sua implementação real, aumentando a eficiência dos grupos de pesquisa e desenvolvimento. A ferramenta também prove os mecanismos necessários para o desenvolvimento de tecnologias e protocolos sem fio, além de permitir a avaliação de melhorias realizadas em protocolos baseados em padrões já consolidados [17].

O *software* utiliza uma estratégia hierárquica para organizar os modelos básicos com o

intuito de construir o cenário presente em uma rede de telecomunicações. Iniciando pela nível inferior, temos o modelo de processo composto por máquinas de estado finitas, códigos em C e funções PROTO.C que definem o modo que um modelo irá reagir mediante a um evento. No segundo nível estão localizados os modelos dos nós, sendo estes representados por um conjunto organizado de módulos, responsáveis por descrever as diversas funções empregadas em cada nó da rede. Por fim, no topo da hierarquia está localizado o modelo de rede, sendo este responsável pelo layout da rede que caracteriza os atributos dos nós para um cenário específico.

Esta ferramenta não foi considerada como uma possível solução para o sistema de teleproteção que se deseja simular/emular. A razão é a mesma do Matlab/Simulink: seria necessário a compra de uma licença de alto custo para a sua utilização. Assim sendo, nossa busca apontou pela utilização exclusiva de ferramentas *open source*, como o GNS3, eNSP e NS-3.

NS-3

O Network Simulator 3 (NS-3) é um simulador de rede baseado em eventos discretos. Seu desenvolvimento se iniciou em meados de 2006 sendo este o sucessor do simulador NS-2. Apesar disso, o NS-3 não é uma extensão do NS-2. Ou seja, ele não suporta as APIs do seu antecessor.

O NS-3 é uma ferramenta Open Source, desenvolvida para a pesquisa e o ensino sobre redes de comunicação baseadas ou não em IP. Sendo assim, a ferramenta fornece módulos como por exemplo pilhas de protocolos da Internet, modelos de canais sem fio, módulos para a implementação da camada física e MAC, e muitas outras alternativas, oferecendo assim, os mecanismos de simulação de rede de pacotes necessários para que os usuários possam conduzir os seus experimentos.

O simulador foi estruturado como um conjunto de bibliotecas que podem ser combinadas entre si. Ainda, pode-se combinar com bibliotecas externas as da ferramenta. Os usuários podem realizar seus experimentos através de linha de comando estruturados na linguagem C++ e/ou Python. A plataforma permite a integração de diferentes interfaces gráficas externas, assim como ferramentas de análise e visualização de dados. Por fim, o NS-3 não é proprietário de nenhuma empresa. Portanto, o suporte a plataforma é realizado através de um fórum direcionado aos usuários da ferramenta [19].

Seu funcionamento é baseado na execução sequencial do código fornecido pelo usuário, ou seja, a ferramenta executa todo o código, enquanto mantém uma lista de eventos atualizada. Durante o período de execução, a ferramenta processa os eventos em cascata, seguindo um após o outro até que toda a lista de eventos seja executada ou até que um ponto especificado pelo o usuário como o fim da simulação seja atingido. Todos os eventos são realizados mediante a instruções do programa ou podem ainda ocorrer devido a outros eventos que ocorram durante o tempo de execução [19].

Essa ferramenta foi considerada como uma possível solução para simular o sistema de teleproteção, porém a disponibilidade de ferramentas mais completas acabaram fazendo que os projetos com NS-3 fossem descontinuados.

eNSP

A ferramenta eNSP é uma plataforma gratuita de simulação de redes, desenvolvida pela empresa chinesa Huawei em meados de 2012, com o objetivo de oferecer suporte a alunos e profissionais da área para aprimorarem suas habilidades profissionais no cenário de redes de comunicação e experimentarem as soluções da empresa para equipamentos de rede. A plataforma é utilizada pela Huawei principalmente no que se refere a simulação de experimentos relacionados às certificações emitidas pela empresa, sendo elas, HCDA, HCDP-Enterprise e HcIE-Enterprise. Além disso, a ferramenta de simulação é utilizada para dar início a projetos, estudos e verificações teóricas e para a análise de desempenho protocolos, por exemplo: *Open Shortest Path First*(OSPF) [20], *Border Gateway Protocol* (BGP) [21] e *Spanning Tree Protocol* (STP) [22].

A ferramenta possui como características, a possibilidade de conectar dispositivos reais ao simulador via cartões de rede e oferece também a possibilidade de rodar as simulações/emulações com um único servidor ou multi-servidores. Ou seja, é capaz de dividir a carga da simulação em vários servidores em caso de redes grandes e complexas.

Em seu desenvolvimento foi aplicada a filosofia: "Utilize o ponto forte dos outros, e evite suas fraquezas", ou seja, durante o projeto da ferramenta os desenvolvedores se preocuparam em verificar e absorver as qualidades de outros simuladores de rede e também buscaram alternativas aos problemas encontrados em outras ferramentas com o intuito de oferecer uma grande experiência ao usuário. A partir desses estudos, uma série de vantagens foram atribuídas a ferramenta, sendo elas: interface gráfica amigável, ou seja, de fácil utilização, oferecendo estruturas de topologias simples e de configuração rápida; disponibilização de uma ferramenta de captura e análise de pacotes em tempo real já embutida ao *software*; conectividade de multi-servidores e implementação distribuída. Como já descrito anteriormente, a ferramenta oferece a possibilidade de fragmentar a simulação de uma rede grande e complexa em diversos servidores, com o intuito de reduzir a carga de processamento e obter resultados mais rápidos [3].

Esta ferramenta foi considerada como uma possível solução para a simulação do sistema de teleproteção desse projeto. Entretanto, dificuldades de integração com outros equipamentos diferentes e outros fabricantes, fizeram-a ser descontinuada.

GNS3

O GNS3 é uma ferramenta de simulação e emulação de redes complexas, desenvolvida por Jeremy Grossman com o intuito de auxiliá-lo em seus estudos para os exames de certificação CCNP [10]. A princípio, a ferramenta foi desenvolvida apenas para emular equipamentos Cisco, porém nas versões atuais é possível emular equipamentos de diversos fornecedores. Como um de seus principais atributos, o simulador é uma ferramenta Open Source capaz de virtualizar diversos equipamentos de diferentes fornecedores (CISCO, ALCATEL, etc.) e implementá-los em redes complexas a fim de avaliar a sua compatibilidade e seu funcionamento em diversas tecnologias de rede, tais como Virtualização das Funções da Rede em inglês NFV (*network functions virtualization*), rede definida por Software em inglês SDN (*Software Defined Networking*), Docker entre outras.

Devido sua característica de ser um software aberto e multiplataforma, a ferramenta pode ser executada em qualquer OS, desde que o mesmo possua um ambiente de execução da linguagem de programação Python. É possível encontrar no site do GNS3 versões da plataforma para Windows, Linux e MAC.

Para a utilização do máximo que a plataforma pode oferecer, dois componentes de software são necessários, sendo eles: (i) a componente de interface gráfica do usuário (GNS3-*all-in-one*), onde o usuário pode criar suas topologias e avaliar o desempenho para diferentes *setups*; (ii) além de uma máquina virtual (GNS3 *virtual machine*). Para a execução da topologia criada pelo usuário através da interface gráfica, os dispositivos criados necessitam ser armazenados e executados através de um processo do servidor. A plataforma GNS3 oferece aos seus usuários 3 possibilidades de servidor. A primeira leva em consideração um servidor local, onde o servidor GNS3 está localizado no mesmo computador que a interface gráfica. A segunda leva em consideração uma máquina virtual local e a terceira uma máquina virtual remota. É recomendado pelo fabricante que o usuário utilize máquinas virtuais para rodar o servidor.

Caso o usuário opte por esse procedimento, é possível rodar a máquina virtual em seu próprio computador através de softwares de virtualização como o Virtualbox, Virtual PC ou VMware Workstation, ou executar a máquina virtual remotamente em um servidor utilizando o VMware ESXi ou através de uma nuvem computacional como a da Amazon.

A seguir será realizado um breve levantamento das principais vantagens e desvantagens da utilização da plataforma GNS3 para a emulação e simulação de redes de comunicação. Uma das principais vantagens da plataforma está na sua gratuidade e em seu código aberto, onde o seu código-fonte pode ser acessado através da plataforma de hospedagem de código-fonte, GitHub.

Além da gratuidade da plataforma, uma grande vantagem em relação a outros softwares está no número ilimitado de dispositivos que podem ser inseridos no modelo utilizado para a simulação, tendo como único limitante, a capacidade do hardware que a executará. O GNS3 oferece suporte para diferentes tipos de comutadores, como por exemplo: ESW16 Etherswitch, IOU/IOL Layer 2 imagese VIRL IOSvL2, além do suporte para dispositivos de diferentes fornecedores.

A ferramenta possui a capacidade de rodar com ou sem hipervisores e em caso da sua utilização a ferramenta oferece suporte para *hypervisors* pagos ou gratuítos, como por exemplo, Virtualbox, VMware workstation, ESXi, Fusion e VMware player. A ferramenta oferece dispositivos para *download*, gratuitos, pré-configurados e otimizados, sendo esses utilizados para simplificar a implantação da rede simulada. Oferece suporte nativo para o sistema operacional Linux sem se fazer necessária a utilização de um *software* de virtualização adicional. Por fim, a ferramenta conta com uma comunidade ativa com mais de 800.000 membros.

Essa ferramenta foi considerada a mais abrangente ao se tratar de possíveis integrações com diferentes equipamentos, *softwares* e fabricantes distintos. Portanto, foi a escolhida para a realização das simulações/emulações que provam nossa hipótese nesse trabalho.

2.5 Protocolos de Rede

Nas seções anteriores foram comentados os principais pontos das redes de transmissão de energia, redes de teleproteção e as principais ferramentas de simulação. Seguindo a construção do cenário, nesta seção serão listados todos os protocolos de rede utilizados tanto nos testes em campo, quanto os utilizados na simulação, incluindo o estabelecimento das primeiras conexões, para que ocorra uma comunicação efetiva e de qualidade entre os componentes em avaliação.

Ao conectar fisicamente um roteador em outro roteador na topologia, é preciso seguir alguns passos de configurações de protocolos para que ocorra a comunicação. É necessário realizar a combinação de protocolos que possuem objetivos diferentes, para fornecer o serviço desejado.

2.5.1 Endereçamento

Nesta subseção serão descritos as principais formas para realizar o endereçamento, de todas as interfaces de redes interconectadas entre si, formando os enlaces que interconectam os roteadores em seus vizinhos. Ou seja, a topologia que foi montada para os testes em laboratório e nas simulações/emulações. Evidenciar o uso de interfaces de *loopback*, suas funções e formas de endereçamento.

Endereçamento IP

O Internet Protocol (IP) permite a concepção e o transporte dos pacotes de dados, identifica o remetente e o destinatário das mensagens devido a três principais campos de endereço, sendo eles: endereço IP (identifica o nó ou componente da rede); máscara de sub-rede (identifica qual parte do endereço é referente a rede em que o nó esta presente) e *gateway* (identifica o elemento principal de entrada e saída das informações na rede).

A Cisco e a Huawei utilizaram abordagens um pouco diferentes para realizar o endereçamento de todos as interfaces dos roteadores presentes nos experimentos do Projeto de P&D040. Por exemplo, a Huawei utilizou sub-redes /30, ou seja, com apenas dois endereços válidos disponíveis por enlace. Já a Cisco utilizou endereços de rede /31, ou seja, apenas um endereço para identificar determinada interface de rede.

Ambos os tipos de endereçamento não possuem diferença na aplicação prática nestes testes. A diferença poderá ocorrer em campo, pelo fato de poder aproveitar todos os endereços de rede disponíveis em uma faixa de endereços. Com isso ganha-se endereços caso o *range* de endereços seja limitado.

Interface de loopback

A interface de *loopback* é uma interface de rede virtual a qual permite que serviços clientes e servidores em um mesmo roteador, comuniquem entre si. Muito usada para testes de conectividade ou testes de configurações de protocolos, pois os pacotes enviados a uma interface de *loopback* normalmente não chegam a interface física. Na topologia de testes em laboratório e na topologia de simulações/emulações, cada roteador possui sua respectiva interface de *loopback* configurada com um endereço IP.

2.5.2 OSPF

Para realizar a comunicação entre os roteadores dos experimentos práticos na CEMIG e o estabelecimento de rotas, tanto na topologia estruturada para os testes, quanto nas simulações/emulações foi utilizado o Open Shortest Path First (OSPF).

OSPF é um protocolo de estado de enlace, que ao conhecer a identificação e o respectivo peso dos enlaces conectados diretamente em cada roteador. O protocolo OSPF realiza cálculos de melhores custos das possíveis rotas e envia os resultados em *broadcast* para os vizinhos, que executam os mesmos cálculos elencando as melhores rotas, esses passos. Podem suportar diversas métricas, como por exemplo, tempo, custo por bit ou confiabilidade. Possibilitando uma decisão melhor sobre qual será a melhor rota.

Tanto a Huawei quanto a Cisco utilizaram o OSPF como base para realizar a comunicação intra-AS da topologia de testes, ou seja, ao utilizar o OSPF todos os roteadores são capazes de reconhecer todos os outros roteadores da topologia.

2.5.3 Multi Protocol Label Switching (MPLS)

A tecnologia Multiprotocol Label Switching (MPLS) é uma forma inteligente de integrar as vantagens do roteamento, com a eficiência e reservas de recursos que existem nas redes que utilizam pacotes em circuitos virtuais. É um padrão criado pela Internet Engineering Task Force (IETF) e possui objetivo de melhorar a velocidade, qualidade de serviço, escalabilidade e provisionamento de serviços, bem como trazer a Traffic Engineering (TE) para o núcleo da rede no contexto de *internet*. Com a capacidade de operar em LAN, WAN, e/ou Serviços corporativos, o trabalho do protocolo MPLS é basicamente adicionar *labels* nos pacotes os quais trafegam no CORE da rede.

Como pode ser visto na Figura 2.1 [23], o cabeçalho MPLS possui 32 *bits*, divididos da seguinte forma: O rótulo MPLS é um pequeno identificador de circuito virtual acrescentado no cabeçalho dos pacotes MPLS, e possui o tamanho fixo de 20 bits. O campo EXP é de uso experimental e normalmente usado como um campo de classe de serviço, possui 3 bits. O campo S representa base da pilha, pois o cabeçalho MPLS pode ser empilhado, possui 1 bit, e o valor 1 representa que ele é o último cabeçalho empilhado. E por último tem-se o campo TTL, o qual define o máximo de saltos que o pacote pode percorrer, possui 8 bits.

O MPLS também é conhecido como protocolo de camada 2.5, pois opera entre a camada 2 (enlace) e a camada 3 (redes). O cabeçalho MPLS é encapsulado na camada 2, porém, também pode encapsular protocolos na camada 3.

Realiza uma divisão da rede em plano de encaminhamento e plano de roteamento:

- **Plano de Encaminhamento:** Os datagramas são encaminhados através da rede com base nos *labels* presentes em seus cabeçalhos. Podem ocorrer troca ou até agregação de *labels* ao longo do percurso. Ou seja, sob a ação do plano de controle, faz a função de *pushing* (empurrar), *swapping* (trocar) e *popping* (retirar) os *labels*.
- **Plano de Controle:** Neste plano é o local que os protocolos de roteamento normalmente utilizado pelo IP e encaminhamento de *labels* existem. Como por exemplo, tabelas, funções de roteamento, sinalizações e policiamento de tráfego. É neste plano que são iniciadas

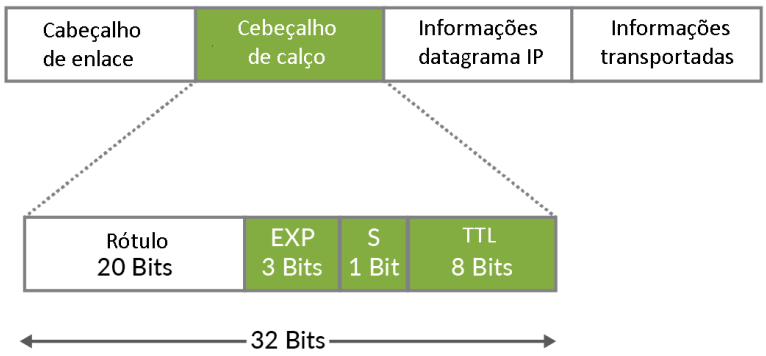

Figura 2.1: Cabeçalho MPLS.

todas as recuperações de falhas de sistemas, por exemplo, Fast Reroute (FF) e Disaster Recovery (DR).

Na Figura 2.2 [24] é possível observar uma arquitetura MPLS com seus principais elementos, sendo listados juntamente com suas funções abaixo:

- **Customer Edge (CE):** Usuário final ou aplicação final.
- **Provider Edge (PE) ou Label Edge Router (LER)**: Conecta os nós ou serviços locais ao núcleo da rede. Realiza o papel de roteador de borda, ou seja, rotulando ou desrotulando qualquer pacote ao chegar. É capaz de atribuir os pacotes em suas respectivas Forwarding Equivalent Class (FEC), que são um conjunto de parâmetros que determinarão o devido caminho para aquele fluxo de pacotes, todos os pacotes enviados por uma determinada FEC seguirão sempre o mesmo caminho.
- **Label Switching Router (LSR):** Também conhecido como Provider Router (PR), são os dispositivos que executam os algoritmos de encaminhamento e retém as tabelas de encaminhamento. Em um domínio MPLS, o integrantes se comunicam utilizando LDP e RSPV estendido. Os LSRs enviam as informações apenas utilizando os *labels*.
- **Label Switched Path (LSP):** Formam o caminho ou o túnel dentro de uma rede MPLS, através de uma determinada sequência de*labels* entre dois LERs.

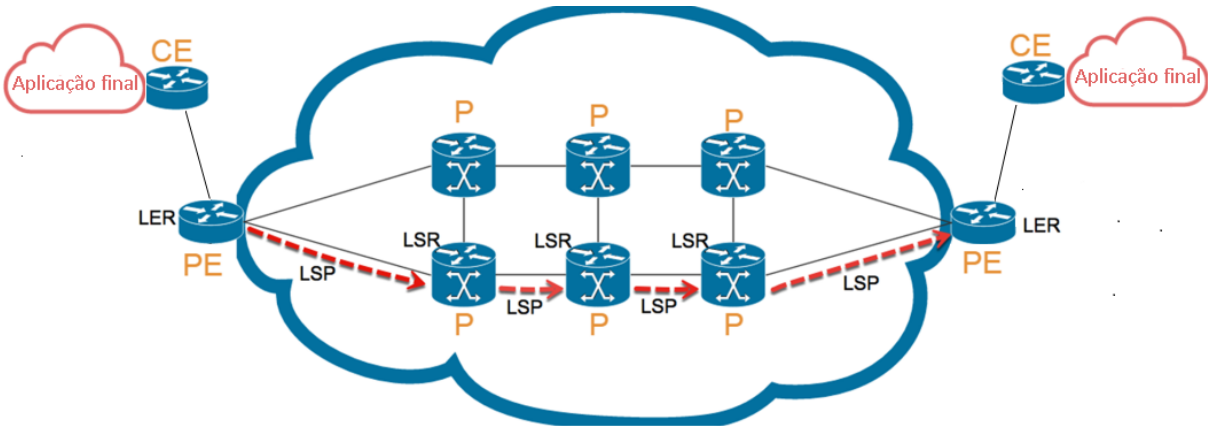

Figura 2.2: Arquitetura de rede MPLS.

Com sua grande flexibilidade, o MPLS é capaz de fornecer suporte a inúmeros protocolos de TE e possui os seus próprios protocolos de TE, como por exemplo, Resource Reservation

Protocol with Tunneling (RSVP-TE) e o Constrained-based Label Distribution Protocol (CR-LDP) [25]. Nas próximas subseções, serão aprofundados os conceitos e formas de trabalho dos protocolos citados acima, e como é a integração desses protocolos com MPLS e QoS.

Multi Protocol Label Switching Traffic Engineering (MPLS-TE)

O MPLS-TE é uma tecnologia que foi desenvolvida para mitigar um problema de roteamento oriundo do protocolo IP. Tem por objetivo realizar um uso mais eficiente dos recursos disponíveis da rede. Desta forma é possível realizar a prevenção da sub-utilização de determinadas partes da rede em determinados períodos, possibilita implementação de mecanismos de segurança contra falhas, assegura níveis de serviços competitivos e agressivos, realiza mapeamento das classes de tráfegos para os túneis de TE e possibilita um maior alcance de QoS fim-a-fim.

Alguns fundamentos listados abaixo precisam ser estudados mais profundamente.

- **Administrative Distance (AD):** Elas conseguem estipular os critérios de confiabilidade em relação a origem das informações do ponto de vista do software do nó da rede (roteador). Os processos que gerenciam a Routing Information Base (RIB), através dos protocolos de roteamento, definem uma AD para cada rota.
- **Métricas:** Definem como será o tratamento de cada protocolo de roteamento para localizar o melhor caminho. Podem ser definidas métricas como: contagem de saltos, custo, bandwidth, delay, etc.
- **Incidência sobre o prefixo mais especifico:** Determinará entre as rotas presentes, qual delas será escolhida para o encaminhamento da informação

IP Hard-Pipe Flex LSP

Essas duas tecnologias podem ser usadas como ferramentas para analise de rede de teleproteção em rede elétrica. Chegando a serem utilizadas e detalhadas em outros trabalhos de dissertação. Vale assim fazer uma descrição rápida sobre as mesmas, para entediamento de trabalhos citados no decorrer dessa dissertação.

- IP Hard-Pipe

  Consiste em uma tecnologia de acesso baseada em rede IP com transmissão de ponta a ponta. Ela isola estritamente *soft Pipes* e *Hard Pipes*, reservando *hardware em roteadores*.Dessa maneira oferece garantia de largura de banda e baixo atraso por meio de hardware dedicado e pipes independentes. Pode permitindo que as redes IP forneçam serviços de transmissão com qualidade de serviço. Dessa forma podeos afirma que essa tecnologia pode antecipar e/ou fornecer recursos de largura de banda, além disso o Hard Pipe pode fornecer baixo atraso para os serviços de linha alugada de clientes de alto valor.

- Flex LSP(*label switched paths*)

  Flex *Label Switched Paths* são instâncias de LSP onde os caminhos de direção direta e reversa são configurados, monitorados e protegidos independentemente e associados durante a comunicação. O Flex LSP fornece caminhos comutados de rótulo bidirecional (LSPs) configurados dinamicamente por meio do Resource Reservation Protocol–Traffic Engineering (RSVP-TE), essa tecnologia vale resaltar não suporta LSPs não co-roteados.

Quality of Service (QoS)

Após as configurações de MPLS, devem ser realizadas as configurações de alguns protocolos que, ao realizarem seu trabalho, interagem fornecendo uma maior QoS. A QoS é uma forma de priorização de certos tipos de tráfegos, que garante um tratamento prioritário a determinados fluxos de dados, provenientes de um serviço estabelecido precisam receber a atenção necessária.

QoS é extremamente importante ao se tratar de serviços ou aplicações em tempo real, por exemplo, voz ou transmissão de comandos de teleproteção.

Para ter QoS uma rede necessariamente precisa garantir largura de banda para uma determinada aplicação sob várias circunstâncias de congestionamento e falhas. Outra abordagem de QoS é que os algoritmos de roteamento precisam identificar a rota mais eficiente para o destino. Para tal, utilizam duas abordagens com este objetivo: identificar o caminho mais curto minimizando os custos e identificar o caminho que está com menor utilização [26]. Nos testes físicos realizados em laboratório, a Cisco configurou um QoS com dois mapeamentos e três politicas.

Label Distribution Protocol (LDP)

O MPLS não tem restrições em protocolos para distribuição de rótulos, com isso, inúmeros protocolos para este fim foram desenvolvidos. Para esta função de distribuição de *labels* ao longo do domínio MPLS, o protocolo mais utilizado é o LDP, que possui mensagens e um conjunto de processos que mapeia detalhes de roteamento da camada de rede para a camada de enlace [27]. O LDP relaciona uma FEC a cada LSP criado. A FEC ao ser relacionada ao LSP realiza um mapeamento dos pacotes específicos do respectivo LSP.

A evolução do protocolo LDP é o CR-LDP, que é uma extensão do LDP e trabalha com sinalizações, tem por objetivo estabelecer os LSPs com suas restrições de encaminhamento explicito. Tornando possível a reserva de valores específicos como taxa média, taxa de pico ou variação máxima de atraso.

Resource Reservation Protocol (RSVP)

O RSVP interage com os demais protocolos trabalhando para uma melhor QoS. Normalmente utilizado por um *host* ou nó da rede, ao longo do percurso, para requisitar qualidade de serviços, ou seja, alocar recursos direcionados para uma determinada aplicação.

Os principais componentes do RSVP são: Transmissores, Receptores e roteadores. Requisições de qualidade de serviço possuem tratamento lógico distinto entre transmissor e receptor. Entretanto, o processo transmissor pode ser analisado como receptor [28].

Ao receber a mensagem de solicitação de reserva de recurso, o receptor realiza a demanda avisando os demais nós em sua rede, sobre sua preparação para receber um fluxo de dados com uma pré determinada, qualidade de serviço [29]. Nesta solicitação de demanda serão informados os seguintes requisitos, endereço IP de origem e destino, taxa de transferência necessária e tempo mínimo de atraso. Fazendo-se uso de dois padrões de decisão, controle de admissão e policiamento de admissão, é determinado se o nó dispõe de recursos.para fornecer o QoS necessário.

O protocolo RSVP-TE é uma extensão do RSVP para a utilização de tuneis LSPs e fornece suporte a engenharia de tráfego, reservando banda e avaliando os requisitos de tráfego. Os tuneis LSPs presentes no protocolo RSVP-TE, são capazes de analisar as demandas de QoS e com isso podem determinar as melhores rotas para o envio dos pacotes em suas sessões. É um protocolo independente de muitos protocolos padrões, como por exemplo, ICMP, IGMP e até mesmo, independente de protocolos de roteamento.

2.5.4 Protocolos para Tratar Falhas de *Link*

Nesta subseção serão descritos alguns protocolos que são utilizados para identificar o status dos enlaces.

Bidirectional Forward Detect (BFD)

O BFD é um protocolo de rede amplamente utilizado para a identificação de falhas entre dois elementos de encaminhamento conectados através de um enlace. Possibilita a identificação

de falhas de *low-overhead* até mesmo em meios físicos os quais não suportam detecções de falhas de qualquer categoria.

O BFD não é dependente de protocolo de roteamento e quando instalado, seu uso pode ser integrado com outros protocolos como por exemplo, MPLS, OSPF, etc. Este protocolo pode trabalhar de duas formas, modo assíncrono ou sob demanda. O modo mais utilizado é o assíncrono, o qual fica enviando pacotes *hello* que são os pacotes de controle do BFD, e quando não são recebidos os *hellos* a sessão é interpretada como estando *down*.

Cisco Discovery Protocol (CDP)

Este é um protocolo proprietário e foi utilizado apenas nos experimentos realizados em laboratório como os equipamentos da Cisco e nas simulações com o GNS3.

O CDP é um protocolo de camada de enlace proprietário da Cisco, muito utilizado entre os dispositivos que estão conectados diretamente, para obtenção de informações que podem, como por exemplo, descobrir equipamentos na rede facilitando o entendimento da topologia e arquitetura de toda a rede, descobrir versão do sistema operacional, estado da interface, ou seja, muito utilizado para a realização de manutenção e nas soluções de problemas da rede.

Comum em todos os equipamentos de rede da Cisco, é independente dos meios físicos e dos respectivos protocolos de rede que estão em uso [30]. Por ser uma solução fechada, outros *vendors* seguiram esta boa prática de implementação e criaram suas versões com o mesmo objetivo. O IEEE então criou um protocolo unificando e tornando padrão conhecido como, IEEE 802.1AB com o respectivo nome de Link Layer Discovery Protocol (LLDP).

2.5.5 Layer 2 Virtual Private Network (L2VPN) sobre MPLS

O objetivo principal da L2VPN é construir uma conexão ponto a ponto conectando dispositivos finais através de uma VPN. Com a existência de dois tipos de serviços de Virtual Private Network (VPN) nas redes MPLS, sendo eles, Virtual Private Wire Service (VPWS) que implementa uma conexão ponto-a-ponto e Virtual Private LAN Service (VPLS) que utiliza o conceito multiponto. Com a utilização de equipamentos legados em utilização por diversos ramos da industria, como por exemplo, as distribuidoras de energia, muitos protocolos de camada 2 trafegam através de caminhos virtuais conhecidos como *Pseudowire* (PW) [31].

A solução VPWS ou PW utilizada tanto nos testes físicos em laboratório quanto nos testes das simulações, funcionam trabalhando nos roteadores PE, pois eles inserem ou retiram os *labels* dos *frames* de camada 2, interconectando máquinas que ficarão na mesma rede.

2.5.6 Interface Tunnel

Uma interface *tunnel* é uma interface que pode ser lógica ou virtual. Cria uma enlace ponto-a-ponto entre dois roteadores, encapsulando ou "tunelando"um protocolo dentro de outro. A principal utilização de interfaces *tunnel* é a possibilidade de criar a segregação de tráfegos, que advém de diferentes aplicações, tornando possível realizar diferentes políticas de tráfego para cada *tunnel* criado. O *tunnel* suporta inúmeros recursos que podem melhorar ou contribuir para um QoS mais eficaz, por exemplo, pode ser possível utilizar engenharia de tráfego, limitar banda, escolher caminhos pré definidos, etc. Nos testes físicos realizados em laboratório e nos testes realizados nas simulações/emulações, foram criados duas interfaces *tunnel*, uma interface *tunnel* recebe todo o tráfego oriundo dos dispositivos de teleproteção e o outro *tunnel*, recebe o tráfego dos demais serviços existentes na rede da CEMIG.

2.6 Gerador de tráfego - Ostinato

Ostinato é uma aplicação multiplataforma *open-source* que pode ser executado em *Windows*, Linux e MAC. Possibilita a configuração de uma arquitetura cliente/servidor, tornando possível a geração e analise de fluxos de dados, que podem ser formados pelo protocolo desejado de pesquisa, como por exemplo, ethernet, ARP, IPv4, IPv6, IP-in-IP, tunelamento IP (6over4, 4over6, 4over4, 6over6), TCP, UDP, ICMPv4, ICMPv6, IGMP, MLD, HTTP, SIP, RTSP, NNTP, etc. É possível a escolha de diferentes taxas de transmissão, captura e visualização de pacotes ".pcap". Sua arquitetura é baseada em dois binários distintos, sendo eles, controlador e agente. O controlador trabalha como front-end, possui uma amigável *Application Programming Interface* (API) e pode exercer controle sobre a geração e captura dos diferentes tráfegos.

Ostinato viabiliza a criação e o envio de tráfego constante ou em rajadas, podendo ser alterados os tamanhos dos pacotes, o tempo de envio dos mesmos, alteração do conteúdo do *payload*, pode ser configurado pra trabalhar com diferentes taxas de transmissão [32] e é possível ser integrado ao GNS3. Desta forma, viabilizando o objetivo de integração de diferentes ferramentas em um único ambiente de simulação. Também é possível utilizar o Ostinato em diferentes dispositivos que suportem sua instalação e implementa-los em ambientes maiores [33], podendo ter vários controladores e vários agentes. Ele é construído em cima de um sistema operacional Linux otimizado, conhecido como TinyCore Linux [34].

2.7 Trabalhos relacionados

Neste capítulo realizamos o levantamento de diversos trabalhos relacionados com: MPLS, *Smart Grid*, teleproteção de redes de energia que venham a corroborar diretamente (ou indiretamente) com o uso *softwares* de emulação/simulação de redes abordados nesta dissertação.

No artigo [35], S. Premkumar et al. trata sobre a rede elétrica integrar *Multi Protocol Label Switching* em *backbones* existentes em redes de comunicação entre subestações e centros de controle. Os autores falam que o MPLS é uma tecnologia emergente para redes de comunicação de *smart grid*. O MPLS usa rótulos para identificar o pacotes. Este artigo propõe proteção de caminho usando tráfego MPLS engenharia para rede de comunicação de sistema de barramento IEEE 30 para rede inteligente.

Os autores defendem que a resiliência de rede é alcançada por meio de recursos de restauração da mesma que permitem que a rede redirecione o caminho em torno de uma falha. A abordagem proposta no artigo é validada usando a ferramenta OPNET. Foi observado que em arquitetura na comunicação *Smart Grid*, oferece uma gama de benefícios e melhorias. A proteção de caminho usando MPLS-TE em redes inteligentes é proposto no final do artigo, além disso, falhas de link no caminho de comunicação podem ser recuperados por meio de caminho proteção usando MPLS-TE.

Existe o processo de notificação de falhas enviadas pelo roteador correspondente. Essas são realizadas antes que o link com falha seja responsável por reencaminhar o tráfego e enviar os pacotes que são incapazes de chegar ao destino. Qualquer falha em qualquer ponto ao longo do caminho de um circuito fará com que os nós finais movam o tráfego de um nova rota. Um LSP de *backup* é estabelecido antecipadamente para fornecer proteção contra falhas para os LSPs que estão carregando tráfego de rede.

Assim, os resultados da simulação realiza pelos autores, mostram um atraso de ponta a ponta apropriado ao tráfego enviado e recebido e o redirecionar o tempo de tráfego de rede em situações de falha.Ao final do artigo foi constatado que o desempenho dos sistemas de barramento IEEE 30 rede de comunicação usando a tecnologia MPLS. Por meio de simulação o artigo comprova que o atraso é reduzido e tem tempo mínimo ao redirecionar o tráfego usando o engenharia de tráfego MPLS [35].

No artigo [36], S. ALAM et al. dizem que a gestão de energia em sistemas de distribuição tem ganhado atenção nos últimos anos. A coordenação da geração e consumo de eletricidade é crucial

para economizar energia, reduzir os preços da energia e alcançar metas de emissão. Devido à importância do assunto, este artigo traz uma revisão de literatura de pesquisa sobre sistemas de gestão de energia e classifica os trabalhos com base em vários fatores, incluindo energia objetivos de gestão, as abordagens adotadas para realizar a gestão de energia e algoritmos de solução.

Além disso, o artigo revisa algumas das técnicas e metodologias adotadas e/ou desenvolvidas para resolver o problema de gerenciamento de energia de forma comparar as mesmas. Os desafios e limitações atuais dos sistemas de gerenciamento de energia são explicados de forma geral no decorrer do artigo. O mesmo ainda fornece uma revisão abrangente da pesquisa publicada sobre gerenciamento de energia em sistemas de distribuição, incluindo aplicativos, desenvolvimentos mais recentes e pesquisar.

Os artigos estudados e apresentados nesse único artigo são uma combinação de conferências e *journals*, bem como revistas e relatórios da indústria de energia com objetivos de gerenciamento de energia, abordagens e algoritmos de solução de gestão de redes elétricas. Limitações e os desafios do EMS (*Energy Management System*) nos sistemas de distribuição são investigados. Como resultado, pesquisas extensas ainda são necessárias para tornar o EMS utilizável e confiável para consumidores.

Além disso, as preocupações com a confiabilidade do sistema devem ser estudado minuciosamente para modos de operação fora da rede e ainda precisam de exploração substancial. Fica claro no artigo que a pesquisa em gestão de energia está aumentando e atraindo ainda mais no interesse de acadêmicos e das indústrias. Por fim este artigo enfatiza ainda mais a importância de gerenciamento de energia e economiza a pesquisadores e engenheiros tempo valioso coletando tais informações [36].

O artigo [37] de Mohamed H. A. Hamied et al. afirma que a Rede elétrica clássica que é formada por um conjunto de ativos gerando e transmitindo eletricidade de uma maneira a partir de do local de produção ao local do consumidor não pode atender às novas demandas dos clientes. Os cientistas desenvolveram a clássica rede elétrica usando informação e comunicação tecnologias para permitir a troca de informações e eletricidade em duas direções, e o novo termo é a *smart grid*.

Isso requer comunicação rápida e confiável entre elementos distribuídos e permite a troca de informações em tempo real entre clientes e operadores para melhorar a gestão da rede. Mas a maioria dos sistemas de comunicação de rede de hoje foram implementados por décadas. A implantação de nova infraestrutura é cara e levará muito tempo para obter um retorno econômico. A principal dificuldade que esse artigo tenta resolver encontrar uma forma de integração de rede elétrica e gestão da mesma estudando protocolos de roteamentos na camada 2 e camada 3 de rede.

Este trabalho apresentado fornece um cenário de avaliação de um infraestrutura de medição avançada usando informações e tecnologia de comunicação (TIC) para um sistema inteligente e automatizado projeto de rede de comunicação. Os autores comparam o desempenho de comunicação HDLC (*High-level data-link control*), PPP (*Point-to-point protocol*) e MPLS usando o protocolo de roteamento OSPF (Open shortest path first). O desempenho do MPLS é melhor (convergência, taxa de transferência, atraso) do que de outras tecnologias legadas.

O artigo [6] de L. F. F. De Almeida e J. R. dos Santos et al. por sua vez foi escrito e publicado por nossa equipe do ICT Lab. Inatel. Falamos sobre o apelo por redes elétricas mais confiáveis, eficientes, resilientes e como tornou-se importante. É reforçado nesse artigo a ideia de crescente desenvolvimento tecnológico, além da demanda por energia elétrica.

O trabalho defende que esses objetivos podem ser alcançados através da introdução de sensores e atuadores na rede elétrica, com o objetivo de possibilitar um controle inteligente da rede. Todos os dispositivos de energia devem ser conectados usando uma rede de comunicação confiável, que deve ser capaz de operar mesmo quando a rede elétrica falhar. Atualmente, várias tecnologias de comunicações foram aplicadas para dar suporte a este novo cenário das redes elétricas.

O artigo [6] tem como objetivo revisar tanto os trabalhos acadêmicos, bem como casos de uso

de mercado para tecnologias aplicadas à missão crítica, redes de controle e aplicações de SGs, tais como teleproteção, autorrecuperação, comunicação com centros de controle e dispositivos de campo, entre outros. Mais especificamente, os principais aspectos, tecnologias potenciais, principais protocolos e casos de uso de redes de dados operacionais em ambientes de transmissão de energia, distribuição de energia e redes inteligentes, incluindo tecnologias de comutação de circuitos e pacotes, são discutidas em detalhes.

Além disso, a resiliência e as principais tecnologias de telecomunicações utilizadas em redes elétricas são exploradas, bem como a correlação entre elas. O artigo fornece uma ampla discussão sobre as melhores opções de telecomunicações para construir os sistemas de distribuição de energia inteligentes emergentes, abrangendo redes de controle, teleproteção e aplicações de rede inteligente.

A rede de comunicação é uma parte vital do sistema de missão crítica em uma rede elétrica. Com a popularização do tecnologias baseadas em pacotes e seu uso em massa nos vários campos tecnológicos, esperava-se que os revendedores revisassem seus sistemas legados, já baseados em tecnologias determinísticas, buscando uma migração gradual para tecnologias dinâmicas, como MPLS e IP.

O artigo ainda enfatiza possíveis tecnologias de comunicação que possam atender aos requisitos das concessionárias na transmissão e distribuição de energia setores e evolução das Smart Grids. Com esta pesquisa, observa-se a possibilidade de integrar tecnologias de circuitos e pacotes na mesma rede, a fim de preservar os investimentos feitos pelas concessionárias de energia. Segundo o autor [6] é possível observar uma migração da estrutura de 'rede legada' para tecnologias mais modernas com uso de pacotes. Um dos principais fatores que corrobora essa afirmação é o surgimento de aplicativos e softwares com conceitos de rede inteligente. Essas novas tecnologias estão sendo desenvolvidas baseadas em pacotes [6]. Nesse artigo especifico o autor acreditar estarmos vivendo o fim do ciclo de vida das tecnologias TDM legadas.

É possível observar que a descentralização causada por tecnologias disruptivas (como IoT, microgeração, Blockchain, etc.) também afetam a interoperabilidade de redes de controle de missão crítica. Portanto, mesmo que os operadores de energia decidam não migrar para tecnologias de pacotes, eles devem interoperar com novos entrantes no cenário de microgeração e descentralização potencializados pela disrupção tecnológica recursiva.

A convergência de tecnologias discutidas neste artigo leva à criação de mercados de energia dinâmicos baseados em TCP/IP/MPLS, Ethernet, IoT, 5G e Blockchain. O mundo de tráfego dinâmico é melhor suportado por tecnologias de comutação de pacotes. A iniciativa para a evolução das redes de comunicação nas concessionárias de energia já pode ser vista em vários países, contudo no Brasil o processo é mais lento.

O artigo [38], de Rahman Dashti et al. trata sobre o levantamento dos métodos de previsão de falhas em redes de distribuição de energia elétrica. Nesse artigo é abordado que um dos principais fatores que interrompem a confiabilidade e o fornecimento de energia é a ocorrência de falhas nas redes de distribuição.

Assim, a previsão e localização precisas e rápidas de falhas nas redes de distribuição são essenciais para aumentar a confiabilidade, restauração rápida, consumo ideal de energia elétrica e satisfação do cliente. Este estudo revisa e investiga tópicos de previsão de falhas e localização de falhas. Para tanto, os métodos e visões existentes no contexto de previsão de falhas são revisados primeiro; então, a localização da falta é investigada.

O artigo [38] investiga vários métodos, suas vantagens, desvantagens, relatórios técnicos e patentes em redes de distribuição convencionais, smart-grids e micro-grids. A comparação deste estudo com outras pesquisas indica que esse é mais abrangente. Além disso, inclui uma revisão atualizada dos métodos de medição de distância e localização de faltas considerando diferentes tipos de rede (AC/DC), presença de DG, padrões de comunicação e automação, medição síncrona e não síncrona, medição magnética e estimativa de estado.

Considerando a importância da confiabilidade em sistemas de energia, especialmente DNs (*distribution networks*), e o impacto direto da falta, pesquisadores propuseram vários métodos para previsão e localização de falhas. Nesse artigo [38], vários métodos modernos propostos para

previsão e localização de falhas em DNs visando aumentar a confiabilidade da rede, recuperação rápida, energia elétrica ideal consumo de energia e satisfação do cliente foram avaliados.

Ainda neste artigo, várias falhas são investigadas e métodos de previsão de falhas foram estudados. Então, a localização da falta em DN é dividida em distância determinação e detecção da seção defeituosa devido à existência de várias ramificações considerando os dispositivos de rede e o algoritmo utilizado. Então, métodos de impedância, métodos diferenciais e ondas viajantes têm sido estudados para a determinação da distância de falta.

Cada método tem vantagens e desvantagens para implementação no DN. No detecção da seção defeituosa, a implementação de um algoritmo de localização de falhas é difícil e complicada, uma vez que bancos de dados precisos e maciços, alta taxa de amostragem e informações precisas da rede são requeridos. Em alguns métodos, uma pequena mudança na topologia da rede altera todos os projetos para localização de falhas.

Uma vez que os DNs possuem características, várias condições de operação e dispositivos como um capacitor, auto-booster, compensador, religador, seccionador, seccionador fusíveis e interruptores VIT para operação ideal, localização de falhas nestes redes seria complicado que requer uma abordagem abrangente que pode responder a todos os requisitos dos DNs. Com todas essas interpretações, problemas de implementação para localização e previsão de falhas não são resolvidos e requerem mais pesquisas.

2.8 Considerações Parciais

O Capítulo 2 apresentou conceitos fundamentais para a compreensão das tecnologias e protocolos utilizados para o entendimento deste trabalho. O objetivo foi o entendimento da integração de todas as técnicas necessárias para o funcionamento básico de uma rede de telecomunicações e, avançando para combinações essenciais de protocolos que ao se integrarem, fornecem o desempenho e a qualidade de serviço desejada. Tudo isso para migrar das atuais redes de telecomunicações de teleproteção de redes de energia usando técnicas de comutação de circuitos para pacotes.

Na Seção 2.1 apresentou-se conceitos essenciais de construção e integração das redes de transmissão de energia. Na Seção 2.2 descreveu-se a importância e necessidade de um estudo profundo sobre as redes de missão crítica. Na Seção 2.3 explicamos os conceitos essenciais das redes de telecomunicações. Na Seção 2.4 foram descritas as ferramentas de simulação/emulação tanto de sistemas físicos, quanto sistemas de redes de comunicação. E na Seção 2.5 são listados e correlacionados todos os protocolos de rede que puderam ser configurados e integrados tanto na parte experimental, quanto simulações/emulações. Na Seção 2.6 apresenta-se uma explicação do gerador de tráfego utilizado na simulação/emulação de redes de teleproteção sobre MPLS.

Na seção 2.7 por sua vez apresenta uma lista de trabalhos relacionados com o assunto proposto nesta dissertação. Os mesmos mostram uma visão de diferentes pesquisas na área, bem como da evolução da gestão de redes de energia. Os artigos abordados neste subtópico, em linhas gerais, apresentam temas ligados ao que é proposto sobre aplicação de sistemas de teleproteção e gestão de redes elétricas.

Capítulo 3

Metodologia de Avaliação e Cenários Propostos

Neste capítulo serão apresentados todos os requisitos necessários para a construção de topologias e execução de testes visando prova de nossa hipótese de pesquisa. São apresentados os pontos necessários para implementação de três cenários: Cenário 1, Cenário 2 e Cenário 3. No decorrer deste capítulo vamos descrever cada um dos cenários citados. Desta forma, serão descritos os passos para reconstrução dos mesmos, caso alguém tenha interesse em replicar os testes realizados. A Figura 3.1 ilustra a evolução dos cenários de testes, de tal forma que podemos observar a topologia e a aplicação dos mesmos. Ela mostra a evolução na configuração, testes, desenvolvimento de topologia de rede de teleproteção, etc. ao longo desse trabalho.

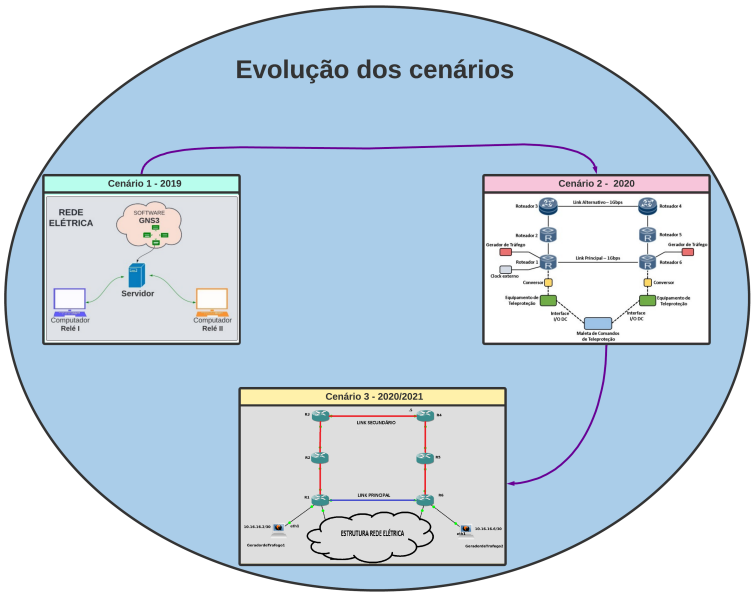

Figura 3.1: Evolução dos cenários de redes de teleproteção em subestações elétricas.

Ainda neste capítulo serão listados todos os equipamentos que foram utilizados no laboratório da CEMIG para a realização do projeto "D0640 - Modelo de Referência para a Rede Operativa de Dados da CEMIG", para o Cenário 2 e Cenário 3. Ele também descreve as configurações necessárias para funcionamento de uma rede de teleproteção no projeto CEMIG.

3.1 Cenário 1

Essa é a primeira parte de experimentos preliminares (logo no inicio dos trabalhos) que nos levam a construção de cenário para os testes finais executados. Esse cenário é importante para contextualização do trabalho, análise de resultados e construção de novos cenários voltados aos estudos de análise de desempenho da rede de telecomunicações para teleproteção com simulador/emulador.

A Figura 3.2 ilustra o primeiro cenário de estudo preliminar utilizando o software GNS3 e dois computadores para simular o comportamento de relés na rede. Como pode ser visto pela Figura 3.2, a construção do cenário exigiu o uso de computadores e softwares, com objetivo de simular o ambiente de distribuição de potência da rede elétrica e os diferentes tipos de relés. A intenção desses testes foi estudar o comportamento e utilização dos relés nos sistemas de teleproteção.

Metodologia do cenário 1

Se fez necessário criar um ambiente de teste para avaliar com confiabilidade os cenários necessários para simular redes elétricas com serviço de teleproteção. A fim de solucionar essa necessidade, primeiramente foi estruturada uma rede física com três máquinas no Inatel, dentro do ICT Lab. Essa rede serviu para emulação do comportamento dos relés na rede elétrica, onde foram realizados testes de comportamento do relé em cenários distintos. Logo durante nossas simulações, desenvolvemos a configuração de comportamento dos relés com atuação: (i) sobre tensão, (ii) subtensão e (iii) sensibilidade às variações de frequências da rede. Esse desenvolvimento seguiu como base os modelos da ANSI/IEEE C37.2. Dessa forma, os relés entravam em operação quando a tensão excedia ou era menor que o limite (inferior ou superior) pré-determinado durante a simulação. Esses valores em geral ficam normalmente entre 1% a 25% do valor de tensão nominal que a rede opera.

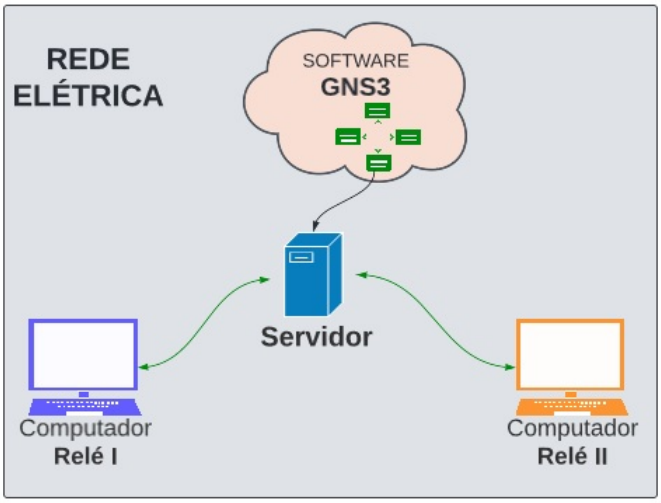

Figura 3.2: Cenário 1 de testes preliminares usando computadores para simular comportamento dos relés na rede elétrica.

Nesse momento, foi validado o cenário 1 no qual tem-se duas máquinas A e B, trocando informações através de uma rede MPLS composta por 6 roteadores em topologia anel, rodando em um servidor com o software GNS3. Este cenário pode ser visto na Figura 3.3 e na Figura 3.4.

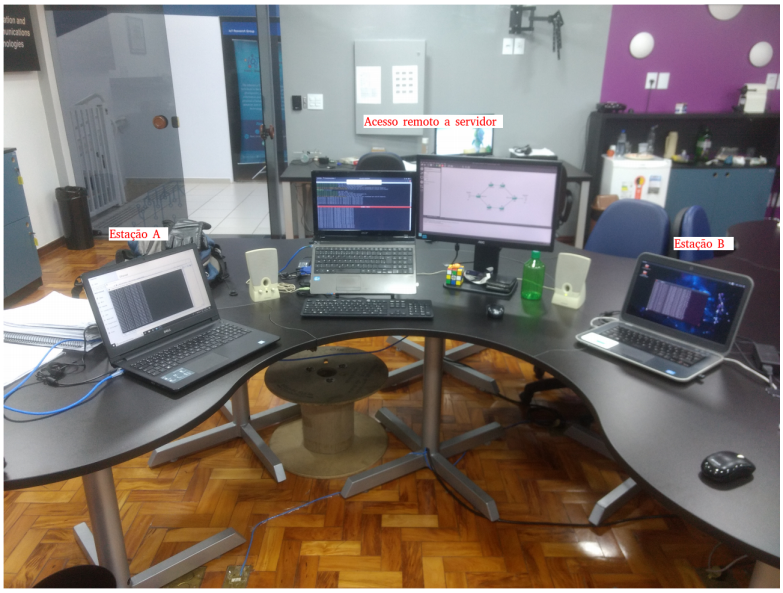

Figura 3.3: Integração do cenário 1 (maio de 2019).

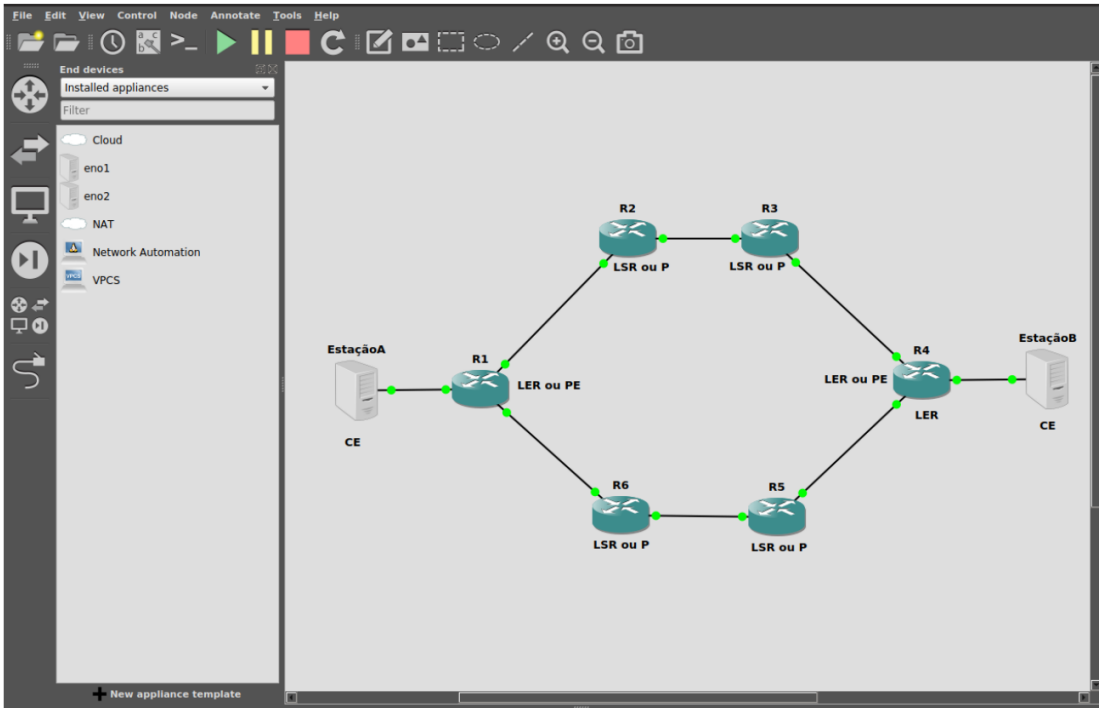

Figura 3.4: Interface gráfica do GNS3.

As especificações do atraso de sobretensão e subtensão ficam entre 0,1s a 30s. Os relés que atuam com as variações de frequências também seguem o modelo ANSI/IEEE C37.2, porém com atuações com valores excedidos de 1% a 20% da frequência nominal da rede.

Com a evolução dos experimentos, foram estendidos os tipos de relés que são empregados nos sistemas de teleproteção. Outros trabalhos de dissertação tiveram sua origem a partir do modelos da ANSI/IEEE C37.2 ligados ao projeto CEMIG, cada um com seu foco específico.

A descrição dos trabalhos citados está na seção 5 de conclusão deste trabalho. Nessa dis-

sertação estamos focando na inclusão do software GNS3 para simular e emular de forma completa a rede elétrica com o sistema de teleproteção. Reforçando a hipótese que se faz necessário o uso de simuladores para desenvolvimento mais confiável de uma rede com sistema de teleproteção. A Figura 3.5 representa a estrutura da rede simulada em software.

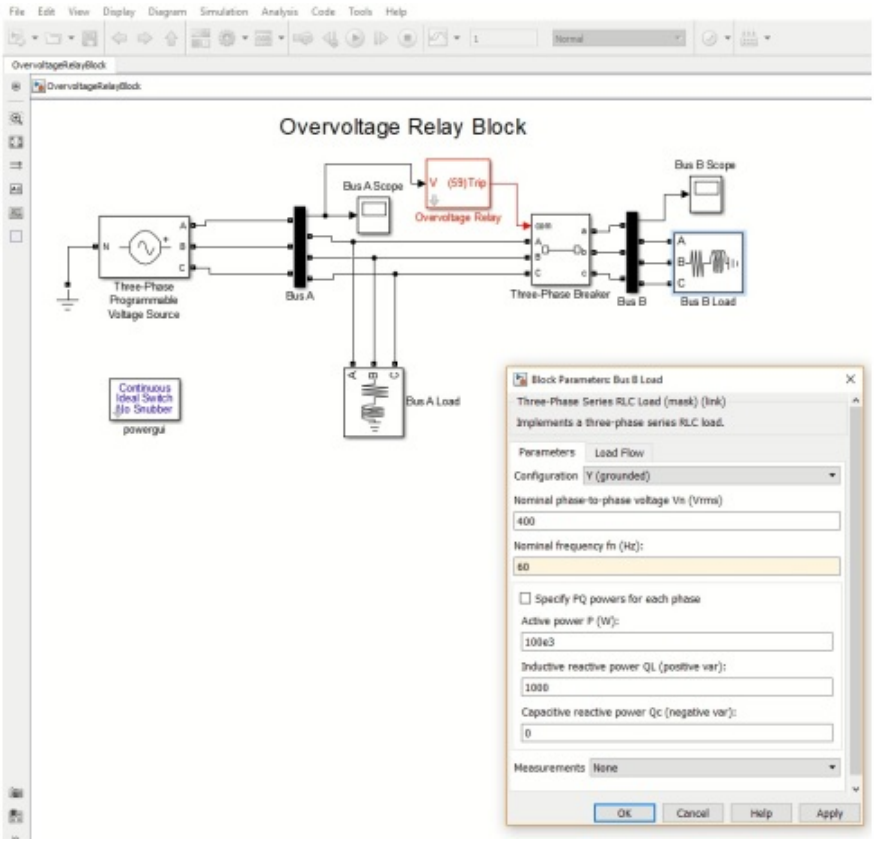

Figura 3.5: Interface do relé de sobre tensão.

Dessa forma, o caminho de experimentos [39] serviu para validar o caminho das simulações/emulações alvo principal dessa dissertação. Iniciaremos a próxima seção comentando sobre o trabalho de dissertação "Avaliação de Tecnologias Estatísticas para Serviços de Teleproteção"[40], que está diretamente ligado a estrutura de dispositivos físicos. Em seguida, apresentaremos detalhes do laboratório construído pela CEMIG junto ao anel viário de Belo Horizonte e que hospedou os equipamentos dos fornecedores parceiros do projeto, viabilizando assim um caderno de testes e experimentos reais de avaliação da rede MPLS como alternativa ao *status quo* de comutação de circuitos existente na maioria das redes de teleproteção no Brasil. Vale ressaltar que também participei de todos os trabalhos experimentais realizados em conjunto com o Sr. Luiz F. F de Almeida.

Analise de implementação do cenário 1

Foram realizados testes iniciais de experimentação dentro do Cenário 1. Contudo, no decorrer dos testes optamos por não utilizar este cenário para provar a hipótese final dessa dissertação. A descontinuidade do Cenário 1 não significa que o mesmo não apresentou nenhum tipo de contribuição para a evolução dos cenários que se seguiram. Neste tópico, vamos detalhar os resultados analíticos que levaram a descontinuidade do Cenário 1, bem como as contribuições retiradas do mesmo.

A primeira bateria de testes de simulação realizada para avaliar a ferramenta foi configurada com um servidor físico executando o simulador GNS3. Este servidor foi conectado por meio

de uma interface de rede a dois computadores (*notebooks*). Cada uma dessas máquinas foi responsável por emular o comportamento da estação A, e estação B, respectivamente.

Na Figura 3.6 é possível observar o resultado de teste com o relé de sobretensão. No plano cartesiano com onda senoidal, verificamos que os valores correspondem a tempo (frequência da onda elétrica) na horizontal e na vertical temos a amplitude da onda elétrica, sobre o relé.

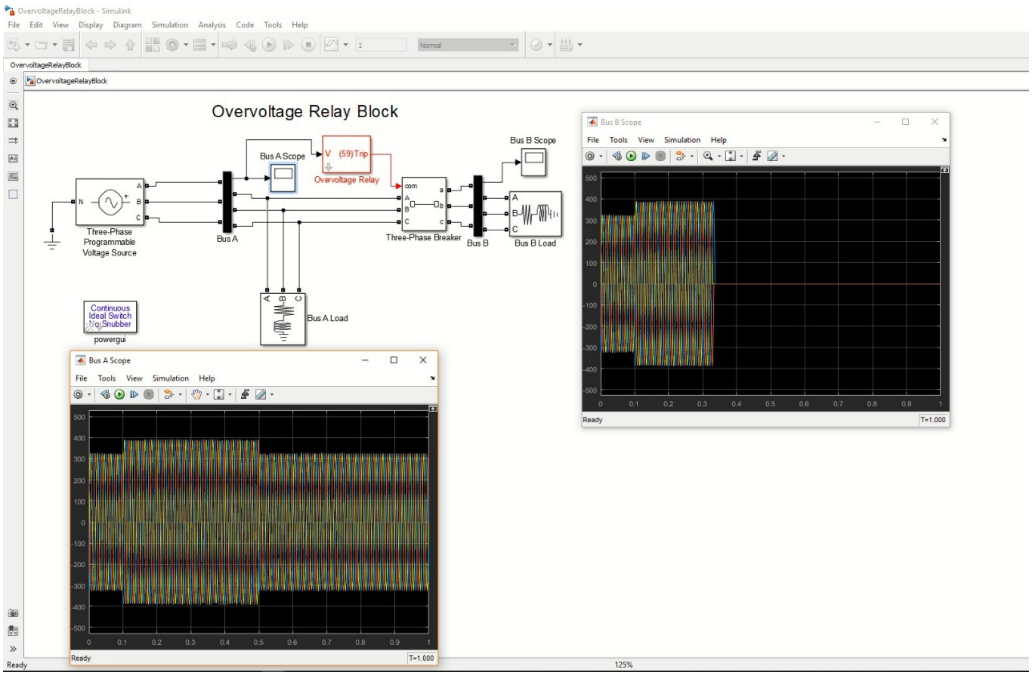

Figura 3.6: Resultado do primeiro cenário de teste preliminar com relé de sobre tensão.

Para executar os softwares foi importante uma etapa de configuração inicial onde observamos corretamente o comportamento do relé. Nas Figuras 3.7 e 3.8 são mostradas respectivamente, a interface de configuração do software para relé de subtensão, e a alteração na configuração de frequência. Observamos através dessas figuras o formato de onda resultante desse experimento.

A medida que realizamos alterações nas configurações de software dentro desse Cenário 1 preliminar de simulação, fomos obtendo uma maior variedade de resultados. Alguns desses podem ser observados nas Figuras 3.9 e 3.10. Observando os resultados é possível afirmar que esse caminho poderia ser promissor pelo fato de possibilitar a implementação física dos relés. Porém, devido ao tempo estimado para finalizar o projeto não permitir esperar a CEMIG, resolver internamente, questões burocráticas para poder realizar a aquisição dos módulos necessários do Matlab/Simulink para criação dos relés, a viabilidade de continuar melhorando este cenário se tornou inviável. Contudo, o conhecimento adquirido não foi perdido, servindo como base para o desenvolvimento dos Cenários 2 e 3 a seguir.

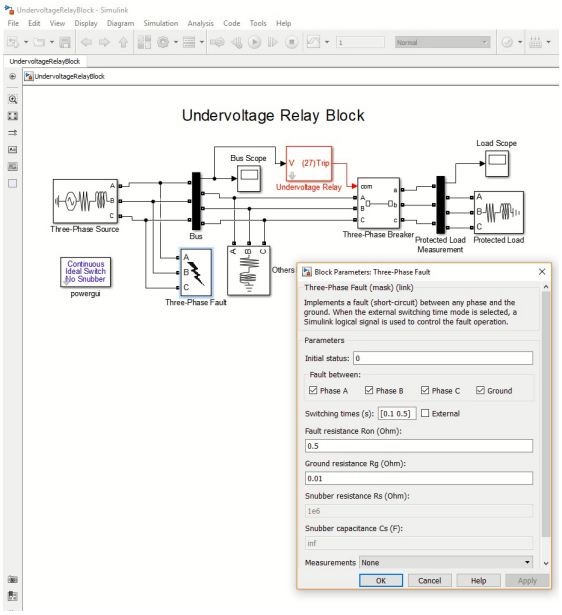

Figura 3.7: Interface de configuração do software para relé de subtensão.

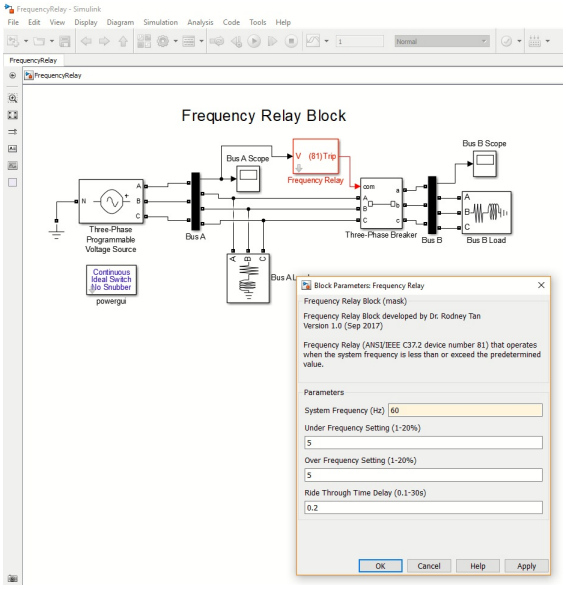

Figura 3.8: Interface de configuração de software para simulação da relé de frequência.

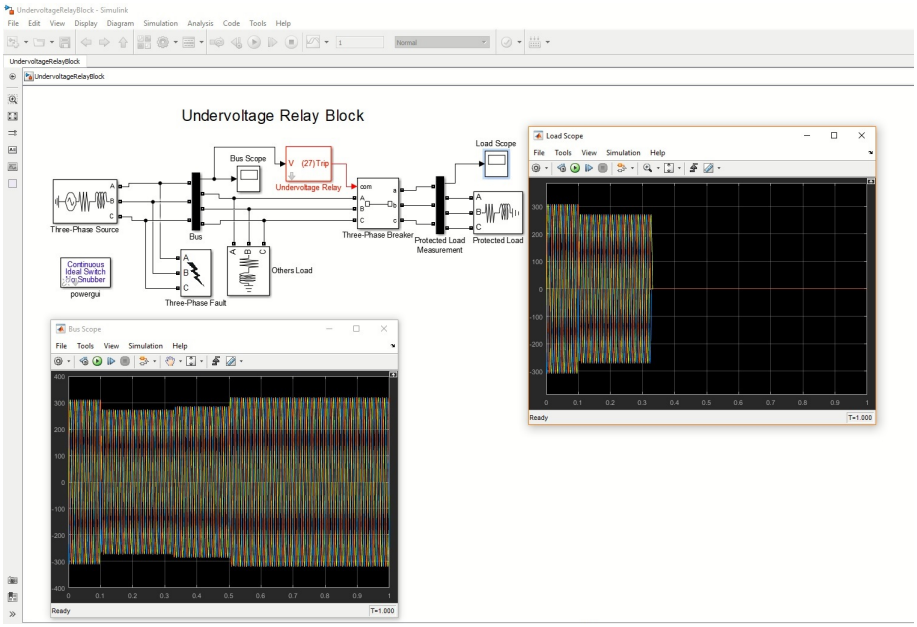

Figura 3.9: Resultado do Software Configurando Relé de Subtensão.

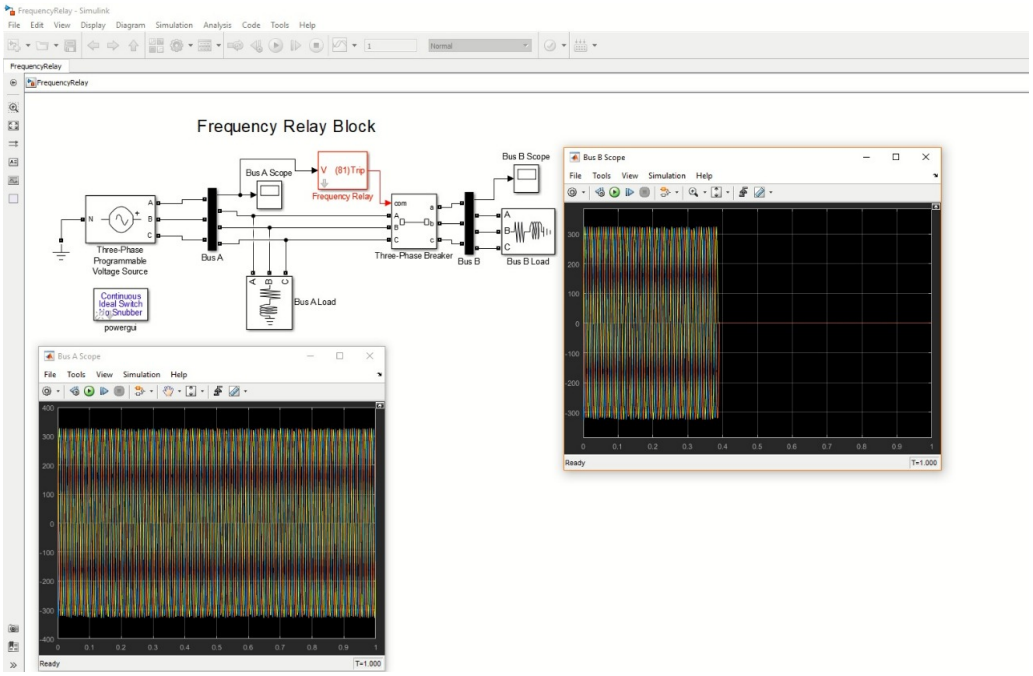

Figura 3.10: Resultado do Software Configurando Relé de Frequência.

3.2 Cenário 2

O Cenário 2 ou cenário físico foi desenvolvido em paralelo com cenário de software proposto nesta dissertação (Cenário 3). A diversidade de estudos de sistemas com os componentes de teleproteção são utilizados para garantir que as falhas presentes nas redes elétricas não afetem os consumidores. Dessa forma, ter estudos de cenários diversos voltados para dispositivos físicos das redes e softwares de simulação/emulação, é bastante desejado. Para fins de testes utilizamos o Cenário 2 com equipamentos CISCO e repetimos o cenário com equipamentos Huawei.

Nas referências [39] e [40], sendo esta última a dissertação de L. Almeida também parte do mesmo projeto, estudos e experimentos voltados para cenário com dispositivos físicos em sistemas de teleproteção em rede elétricas foram realizados. L. Almeida [40] afirma que tradicionalmente as concessionárias de energia utilizam tecnologias *Time-Division Multiplexing* (TDM) como meio de comunicação para os sistemas de teleproteção. Porém, o autor aborda que uma ineficiência na alocação de recursos abriria espaço para a utilização de novas tecnologias, tais como as baseadas em IP e MPLS.

O trabalho apresentado faz avaliação de desempenho de redes estatísticas para o serviço de teleproteção [40]. A metodologia de avaliação empregada foi baseada na elaboração de testes e na realização de experimentos laboratoriais com equipamentos utilizados em campo pelas concessionárias de energia. Em outros trabalhos que se utilizaram dos resultados dos testes do Cenário 2 apresentado é possível observar testes realizados em laboratório utilizando as tecnologias proprietárias IP *Hard-Pipe* da Huawei e *Flex*-LSP da CISCO [40].

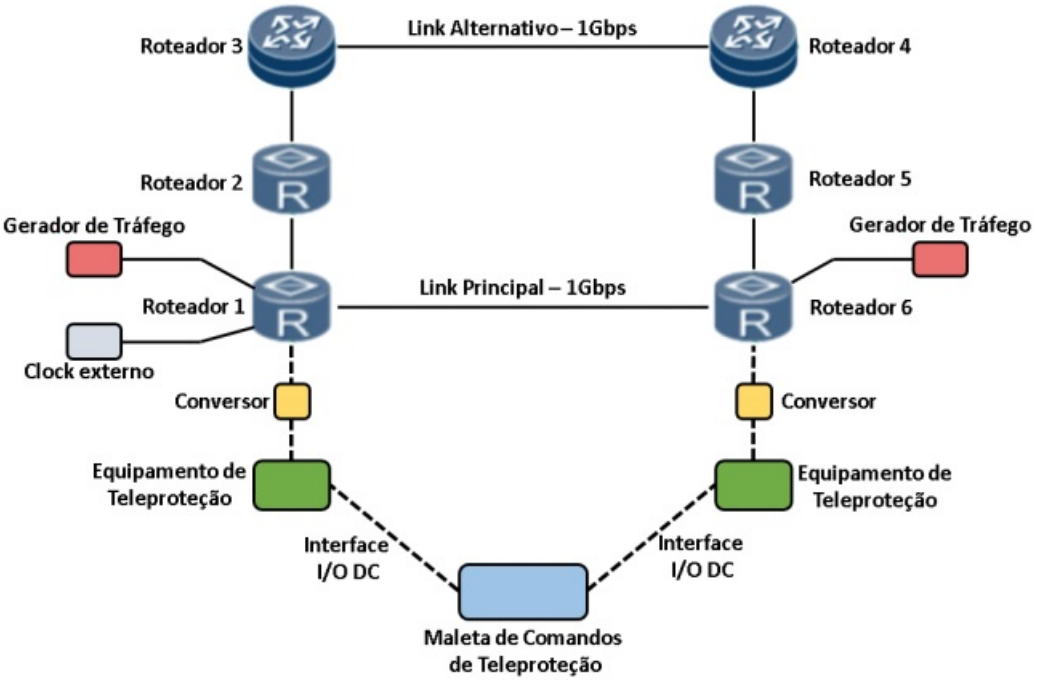

Figura 3.11: Topologia de testes de teleproteção.

Neste trabalho de dissertação, o Cenário 2 implementa experimentos físicos em uma rede prototipada. Participamos da construção deste cenário desde a definição de topologia e equipamentos, até a realização dos testes finais em campo. Os resultados do Cenário 2 foram tão amplos que deram origem a diferentes artigos e trabalhos de dissertação. No decorrer deste trabalho vamos detalhar alguns dos resultados de experimentos obtidos no Cenário 2, afim de compará-los com os resultados obtidos no Cenário 3, que ainda será descrito.

A Tabela 3.4 apresenta a lista dos equipamentos utilizados durante a elaboração dos cenários previstos para os testes em cenário físico na CEMIG [40]. Os equipamentos para montar a rede

Tabela 3.1: Tabela de equipamentos disponibilizados para a execução do Cenário 2.

No.	Equipamento	Quantidade
1	Roteadores Huawei NE08E-S6E	2
2	Roteadores Huawei NE05E-SQ	2
3	Roteadores Huawei NE05E-S2	2
4	Roteadores Cisco ASR903	6
5	*Software* de Gerência EPN-M Cisco	1
6	Gerador de Tráfego *Jperf*	1
7	Gerador de Trafego TSW900ETH (WISE)	2
8	Equipamento de Teleproteção modelo e-terra Gridcom DIP 5000 (Alstom/GE)	2
9	Maleta de Comandos de Teleproteção	1
10	Conversores Datacom DM 704C V.35/G.703 2Mbps	2
11	Conversores de interface C3794 / G.703 Codirecional 64kbps	2
12	Osciloscópio Digital	1

de simulação e elaboração de cenários foram compartilhados entre essa dissertação e o trabalho com cenário físico na CEMIG [40]. A ideia usada no Cenário 2 foi a base para construção do Cenário 3 deste trabalho. Ela prove os subsídios necessários para construção do Cenário 3, dentro do software de simulação. Isso pode ser visto em detalhes na Seção 3.3 com a estrutura de rede definida no simulador.

Tabela 3.2: Tabela de protocolos CISCO para o Cenário 2.

Pilha de protocolos - CISCO
OSPF(Open Shortest Path First)
BGP(Border Gateway Protocol)
BFD(Bidirectional Forward Detect)
VRF(Virtual Route and Forwarding)
LDP(Label Distribution Protocol)
MPLS(Multiprotocol Label Switching)
MPLS-TE(Multiprotocol Label Switching - Traffic Engineering)
RSVP(Resouce Reservation Protocol)
QoS(Quality of Service)
Túneis
Configurações de caminhos
XConnect
CDP(Cisco Discovery Protocol)
PTP(Precision Time Protocol)
SyncE
Solução para teleproteção
Flex LSP

A estrutura de topologia de rede do Cenário 2 é a mesma que foi usada no trabalho de dissertação [40] e pode ser vista na Figura 3.11. A Tabela 3.2 descreve a estrutura de protocolos que foi utilizada na construção do Cenário 2 com equipamentos CISCO. A Tabela 3.3 trata da estrutura de protocolos para Cenário 2 com equipamentos Huawei.

Tabela 3.3: Tabela de protocolos Huawei para o Cenário 2.

Pilha de protocolos - Huawei
OSPF(Open Shortest Path First)
BGP(Border Gateway Protocol)
BFD(Bidirectional Forward Detect)
VRF(Virtual Route and Forwarding)
LDP(Label Distribution Protocol)
MPLS(Multiprotocol Label Switching)
MPLS-TE(Multiprotocol Label Switching - Traffic Engineering)
RSVP(Resouce Reservation Protocol)
QoS(Quality of Service)
Túneis
Configurações de caminhos
Solução para teleproteção
Hard Pipe

Metodologia do Cenário 2

A metodologia de avaliação em estrutura real fez uso das tecnologias Hard-Pipe e Flex LSP, ambas descritas no capítulo de fundamentação desse trabalho. As mesmas não são relevantes para essa dissertação com foco em software de simulação. Detalhes sobre a metodologia de uso dessas tecnologias podem ser encontrados em [40]. Os testes realizados no Cenário 2 focaram em duas estruturas físicas, sendo elas, a estrutura de rede com tecnologia CISCO e estrutura de rede com tecnologia Huawei, que podem ser vistas na Figura 3.12 e na Figura 3.13, respectivamente.

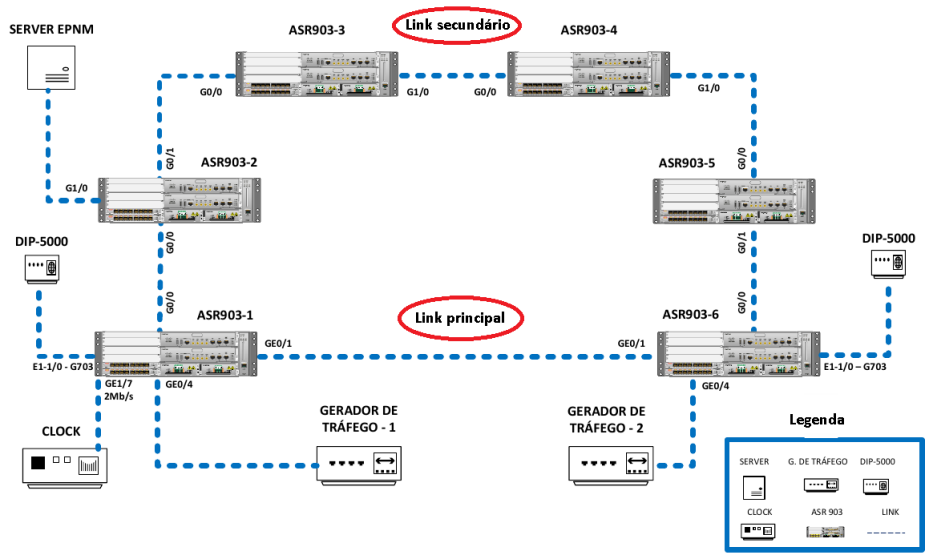

Figura 3.12: Topologia de testes de teleproteção.

É possível observar que ambas as Figuras 3.12 e 3.13, representam uma topologia em anel com sistema de teleproteção implementado em uma rede elétrica. As Figuras servem para destacar os diferentes equipamentos utilizados para reconstruir a mesma topologia de comunicação. Os testes realizados no Cenário 2 tanto para CISCO quanto para Huawei são importantes para comparação com o Cenário 3. O Cenário 2 foi amplamente estudado conforme [40].

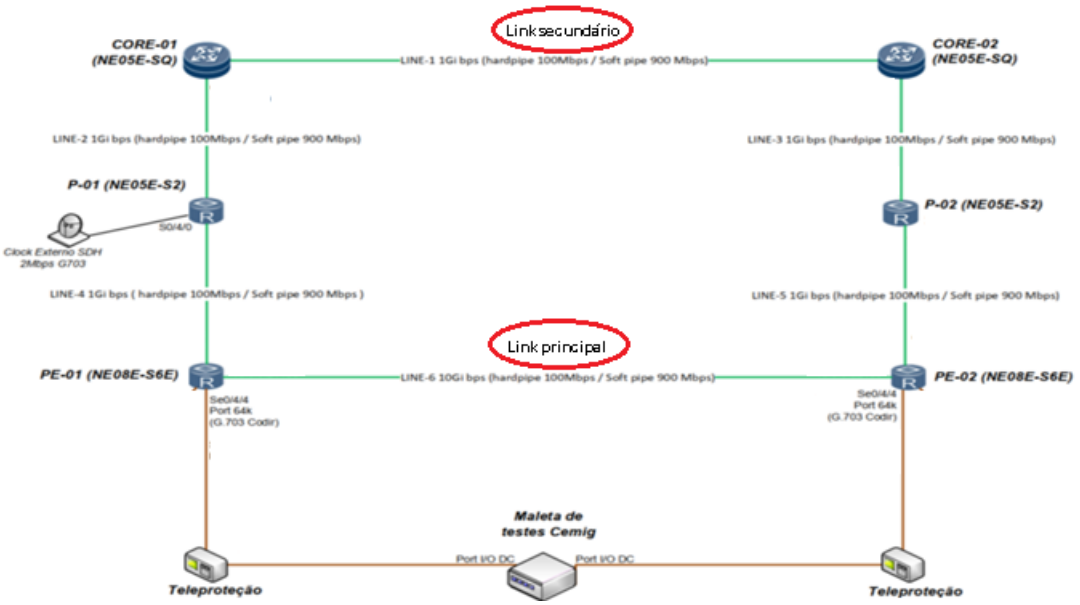

Figura 3.13: Topologia de testes de teleproteção.

A Figura 3.14 mostra uma das estruturas de testes práticos em cenário real utilizados pelo mesmo. Como resultado, esse caminho demandou de uma certa complexidade para execução de instalação de equipamentos reais na CEMIG [39].

Na Figura 3.14 observamos no campo legenda os elementos: *'SERVER'*, representando o software de gerência da CISCO, responsável por fornecer um método de gerência sofisticado; 'G DE TRÁFEGO', responsável por gerar tráfego de dados corporativos; 'dip5000', relés; '*CLOCK*', responsável por sincronizar os horários de todos os elementos da topologia; 'ASR 903', são os roteadores; '*Link*', conexão que interliga todos os equipamentos dentro da topologia.

Figura 3.14: Cenário 2 com estrutura física de equipamentos CISCO.

A Figura 3.17 representa a estrutura física do cenário 2 utilizando equipamentos da Huawei para construção do mesmo. A Figura é composta por elementos que representam roteado-

res, relés de Teleproteção, gerador de tráfego, gerador de clock externo para sincronismo de equipamentos, e link de comunicação para o caminho principal e secundário.

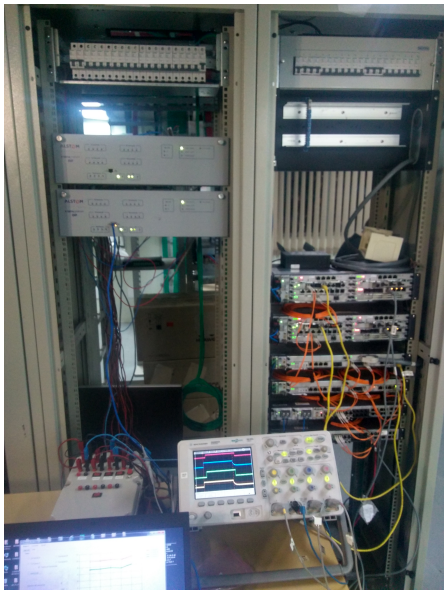

Figura 3.15: Cenário 2 com estrutura física de equipamentos Huawei.

Uma parte crucial na estruturação do Cenário 2 foram os códigos de configuração para cada equipamento, dentro das diferentes tecnologias CISCO e Huawei. Foram utilizados 6 roteadores, e cada um deles necessitou de uma configuração específica para cada teste realizado. Desta forma, foi grande o volume de linhas de código necessárias para a realização dos testes. Os códigos utilizados para configuração em cada roteador seja na tecnologia CISCO ou Huawei são extensos, de forma que vamos mostrar apenas uma pequena parte dos mesmos a seguir. A Figura 3.16 a seguir mostra parte do código de configuração em um roteador CISCO, dentro do Cenário 2 para realização de um dos testes. Já a Figura 3.17 mostra parte da configuração em um roteador Huawei, também dentro do Cenário 2.

```
ASR903-1#sh running-config
Building configuration...

Current configuration : 12214 bytes
!
! Last configuration change at 12:18:42 UTC Fri Jan 10 2020 by didata
!
version 16.6
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform bfd-debug-trace 1
platform xconnect load-balance-hash-algo mac-ip-instanceid
platform tcam-parity-error enable
platform tcam-threshold alarm-frequency 1
!
hostname ASR903-1
!
boot-start-marker
boot system bootflash:Image/packages.conf
boot-end-marker
!
!
vrf definition CORP
 rd 100:100
 !
 address-family ipv4
  route-target export 100:100
  route-target import 100:100
 exit-address-family
!
```

Figura 3.16: Parte do código roteador CISCO - Cenário 2.

```
<PE-01>display current-configuration
!Software Version V300R003C10SPC500
!Last configuration was updated at 2019-08-22 05:41:57-03:00 by root
!Last configuration was saved at 2019-08-22 05:46:57-03:00
#
loop-detect trigger enable
#
clock timezone 1 minus 03:00:00
#
sysname PE-01
#
set neid a36459
lldp enable-dcn authentication %^%#/vH]8;MUZ$kCQ=R-i!<-CADoCJ*zC3k]UwY)bg($%^%#
#
check code-signature default
#
ntp-service server disable
ntp-service ipv6 server disable
ntp-service unicast-server 172.16.0.1
#
vlan batch 1001
#
dot1x-template 1
#
router id 172.16.0.5
#
diffserv domain default
#
```

Figura 3.17: Parte do código roteador Huawei - Cenário 2.

É importante salientar que o Cenário 2 utilizando equipamentos CISCO ou Huawei, necessitou de uma pessoa especializada em cada uma destas respectivas tecnologias. Isso por que a configuração de equipamentos do Cenário 2 para CISCO é diferente da necessidade de con-

figuração de equipamentos Huawei, pois ambas não seguem a mesma estrutura de sintaxe de comandos. Ficou assim observada a necessidade de conhecimento em configuração de equipamentos das tecnologias CISCO e Huawei respectivamente, para a construção do ambiente de testes dentro do Cenário 2.

No tópico voltado para resultados dentro deste trabalho será possível observar o comportamento do Cenário 2, com diferentes tecnologias (CISCO e Huawei) em comparação com o Cenário 3. Dentro dos testes propostos observou-se o comportamento desses cenários com: i) presença de tráfego + comandos de teleproteção, ii) apenas comandos de teleproteção, iii) diferentes rotas, sendo elas, rota principal e rota secundária e iv) diferentes bandas utilizadas, variando entre 2Mbps, 10Mbps e 100Mbps.

Configurações de testes

A Tabela 4.4 se refere as condições necessárias para a realização de testes e obtenção de resultados. Essas condições envolvem desde a definição do cenário, como topologia e tecnologia, bem como nıveis esperados de latência. Podemos ver na tabela informações pertinentes a configuração e protocolos utilizados para cada respectivo cenário de teste. Outra informação importante descrita na tabela que impacta na realização de testes é a taxa de comunicação que será utilizada.

Tabela 3.4: Condições de testes

Condições de Testes					
Cenário	**Taxa (Mbps)**	**Tecnologia**	**Rota**	**Condições de Testes**	**Objetivo**
2	2 10 100	CISCO	P e/ou S	-Equipamentos interconectados -Protocolos de comunicação configurados e testados -Software gerador dos comandos de teleproteção configurado -Em testes com inserção de tráfego, verificar as configurações do gerador de tráfego	Obter delay do envio dos comandos de teleproteção menor que 10 ms
2	2 10 100	Huawei	P e/ou S	-Equipamentos interconectados -Protocolos de comunicação configurados e testados -Software gerador dos comandos de teleproteção configurado -Em testes com inserção de tráfego, verificar as configurações do gerador de tráfego	Obter delay do envio dos comandos de teleproteção menor que 10 ms
3	2 10 100	Simulação	P e/ou S	-Equipamentos interconectados -Protocolos de comunicação configurados e testados -Software gerador dos comandos de teleproteção configurado -Em testes com inserção de tráfego, verificar as configurações do gerador de tráfego -Verificar o consumo de recursos físicos da maquina host durante os testes para evitar atrasos e consequentemente erros durante a execução dos testes	Obter a maior aproximação possível de configuração dos protocolos utilizados nos equipamentos reais Obter delay do envio dos comandos de teleproteção menor que 10 ms

A Figura 3.18 ilustra através de um fluxograma o passo a passo necessário para configuração dos cenários de testes. Através deste fluxograma podemos entender melhor o Cenário 2 e Cenário 3, sua construção, configuração e realização de testes, bem como a analise de resultados obtidos.

O campo 'Comandos A, B, C e D' está ligado diretamente a formas de diferentes configurações para relés atuarem na rede. A e B são comandos diretos, C e D são comandos de bloqueio. Estão presentes na maleta de testes da CEMIG, sendo possıvel realizar a configuração combinada destes comandos relacionados aos conceitos de:

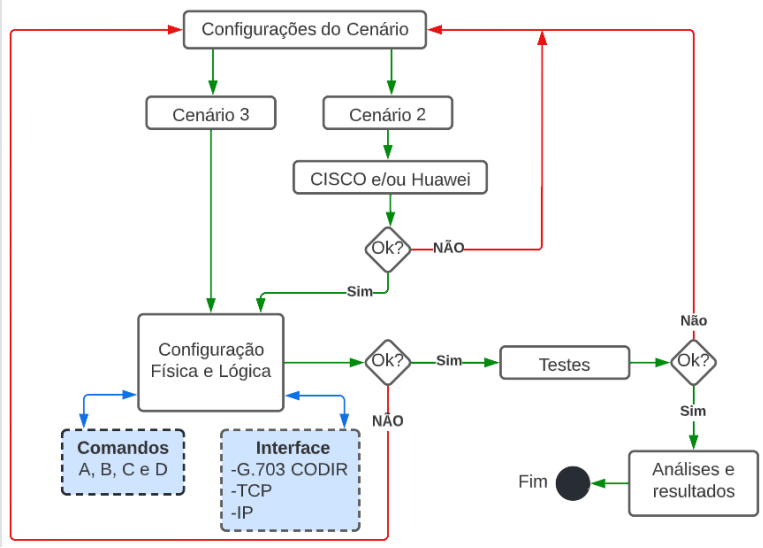

Figura 3.18: Fluxograma das configurações dos cenários

- **DUTT** (Direct Underreaching Transfer Trip) - Bloqueio: Utilizado no sistema quando deseja realizar um desligamento direto do disjuntor.
- **PUTT** (Permissive Underreaching Transfer Trip) - Direto: Utilizado quando o relé identifica uma falha em sua região, o disjuntor é desarmado e na sequência é enviado um sinal para o outro relé do enlace.
- **POTT** (Permissive Overreaching Transfer Trip) - Direto: Faz uso de alguma informação do relé que é seu par, para assim poder atuar.
- **DCB** (Directional Comparison Blocking) - Bloqueio: Envia um sinal de bloqueio quando identifica alguma falha na direção reversa.

Dessa forma é obtido usando no Cenário 2, diferentes valores de latência como resposta. Vale observar que o experimento realizado no Cenário 3 envolvendo o campo 'Comandos A, B, C e D' está diretamente relacionados ao gerador de tráfego (OSTINATO), responsável, pelo tráfego neste Cenário. Os comandos de teleproteção gerados para o Cenário 3 com PING, tem sua estrutura modificada, fazendo uso do protocolo TCP para garantir estabelecimento do link de comunicação com confiabilidade na realização dos testes.

O campo configuração 'Configuração Fısica e Lógica' apresentado na Figura 4.18 envolve os pontos de configuração de equipamento e software seja no Cenário 2 ou no Cenário 3. No campo 'Interface G.703 CODIR' 2 Mbps representa o tipo de comunicação entre equipamentos de teleproteção e roteadores. Fazendo uso de interface G.703 CODIR 2 Mbps.

3.3 Cenário 3

Tanto o Hard-Pipe, quanto Flex-LSP são boas ferramentas para redes de teleproteção. Contudo, possuem limitações que inviabilizam comparações via simuladores. Dessa forma, não foi viável realizar comparações via testes no cenário 3 abordando o Flex LSP e Hard Pipe, visto que estes protocolos de teleproteção não estão disponíveis para CISCO e Huawei em seus respectivos simuladores. Portanto, foram utilizadas versões de MPLS com funções semelhantes as tecnologias Hard Pipe e Flex LSP.

A base inicial de configuração e protocolos para o uso dessas tecnologias, de forma operacional esta implementado na imagem dos roteadores utilizados no cenário 3. Na Tabela 3.3 é possível realizar um comparativo de configuração de protocolos utilizados entre fabricantes CISCO, Huawei e simulador GNS3 (CISCO).

Entretanto, a estrutura inicial de protocolos implementados é a mesma usada em ambos os cenários físicos. Isso possibilita reproduzir pelo menos em parte os cenários desses fornecedores, ainda que sem essas tecnologias específicas para teleproteção, mas contemplando MPLS e vários outros protocolos idênticos aos usados no experimento na CEMIG.

A topologia desejada e elaborada em conjunto com a CEMIG tinha como objetivo a replicação de um cenário real, trazendo para o laboratório todos os detalhes de uma rede de transmissão de energia da operadora, integrada a uma rede de teleproteção. De forma geral, essa topologia é composta por seis roteadores interligados em anel, um sistema de comandos de teleproteção e geradores de tráfego, utilizados para adequação das interfaces nos roteadores de forma a construir o Cenário 3 proposto.

Tendo em vista a necessidade de atender requisitos para caracterizar uma rede de teleproteção, nas redes de transmissão de energia demanda-se por confiabilidade, seleção de caminhos, redundância de equipamentos, desempenho para ações rápidas como desligamento ou religamento automático, visando desta forma, a completa eliminação de falhas nas linhas de transmissão, falhas que podem causar enormes prejuízos e até mesmo fatalidades ou danos ao meio ambiente.

Os comandos de teleproteção enviados na rede são gerados por equipamentos compatíveis aos sistemas de telecomunicações e vice-versa. Desta forma, esses comandos podem ser executados por diversos equipamentos da rede, por exemplo, relés ou outros equipamentos dedicados de teleproteção e até mesmo os equipamentos de telecomunicações, caso estes identifique alguma anormalidade. Uma topologia genérica de uma rede de transmissão de energia acoplada a uma rede de teleproteção pode ser vista na Figura 3.19 [41].

Ambas as topologias de rede apresentadas nas Figuras 3.19 e 3.11 são similares. Podemos afirmar que em ambas, os comandos de teleproteção são enviados pelo *link* principal. Esse *link* por sua vez está representando um *link* de comunicação direto entre os roteadores um e seis na Figura 3.11 e R1 e R6 na Figura 3.19.

Dentro desse cenário proposto abordamos a simulação do comportamento da rede elétrica com tráfego e sem tráfego, tanto no *link* principal, quanto no *link* secundário, entre as subestações. Como pode ser observado em ambas as figuras, o *link* secundário por sua vez é composto por seis roteadores e é responsável por trafegar os comandos de teleproteção quando o caminho principal estiver inoperante. Logo, é possível afirmar que essa representação do sistema de proteção principal e proteção secundária, faz uso de interligação de comunicação com topologia em anel.

Metodologia do Cenário 3

Para realização de testes nesse cenário vamos utilizar o mesmo *software* GNS3 dos testes do Cenário 1 . O GNS3 é capaz de aproximar bastante o usuário da sensação de estar trabalhando diretamente com uma rede real. Com ele é possível emular diversos tipos de equipamentos, como por exemplo: Roteadores, comutadores, telefones, *firewalls*, sistemas operacionais completos, ou seja, é uma ótima ferramenta para testes em redes avançadas. Ele consegue integrar ferramentas

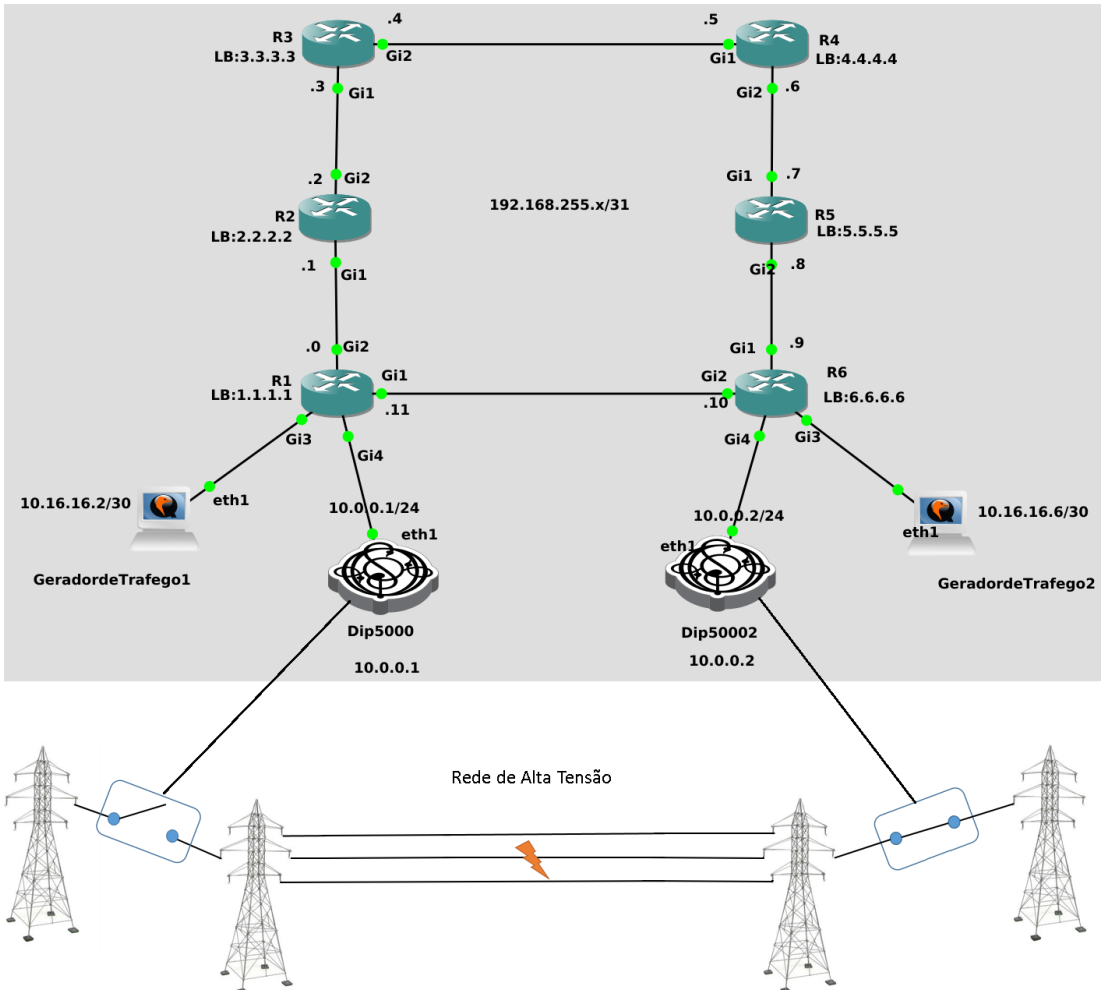

Figura 3.19: Representação completa de testes no simulador.

de virtualização como o VirtualBox e a Qemu, as quais podem integrar inúmeras máquinas virtuais e sistemas estudados com o simulador, emulando-os.

A facilidade de uso contribuiu muito com a montagem de uma topologia que se assemelha a pensada para os testes em laboratório na CEMIG, pois as imagens de roteadores utilizados são as mais recentes liberadas para uso em qualquer simulador de rede compatível. Uma observação importante é que existe diferença entre serviços oferecidos nos sistemas de simulação/emulação com os recursos de equipamentos físicos da CISCO. Entretanto, isso não invalida o uso da solução de software de simulação/emulação como ferramenta para a avaliação e estruturação de redes de pacotes, como alternativa as redes de circuitos em teleproteção em redes de energia.

Na Figura 3.20 pode ser vista uma parte da topologia que inclui os geradores de tráfego 1 e 2, e os relés de teleproteção DIP5000 e DIP5002, dentro do Cenário 3. Desta forma, foi possível a simulação/emulação dos geradores de tráfegos e dos relés dentro do GNS3. Vale ressaltar que o uso do micro sistema operacional conhecido como TinyCore [42], possibilitou toda a integração e construção do Cenário 3 para os testes que se seguiram. O Tiny core foi utilizado como ferramenta em outros projetos de pesquisa, dentre eles, um gerador de tráfego conhecido como OSTINATO, que pode ser integrado para uso dentro do GNS3, o qual foi amplamente utilizado no Cenário 3. O gerador de tráfego OSTINATO [43] pode gerar tráfego na topologia desejada dentro do próprio GNS3. Dessa maneira, dispensamos o uso do modelo inicial de simulação do cenário 1. A interface gráfica do OSTINATO pode ser observada na Figura 3.21.

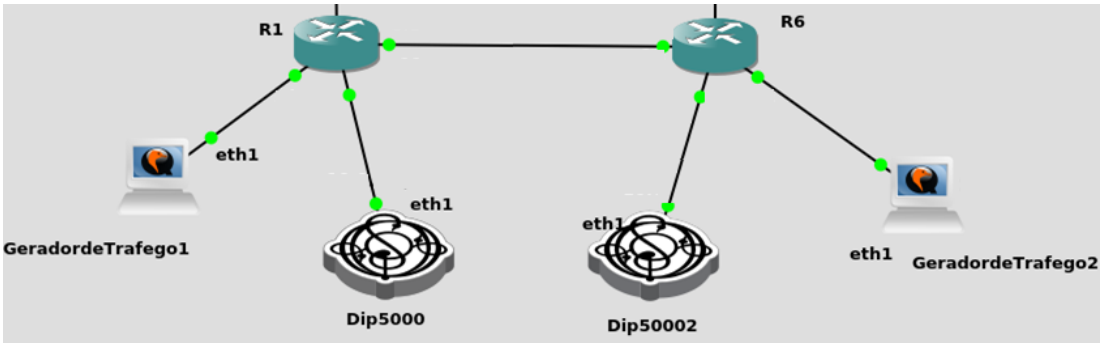

Figura 3.20: Equipamentos configurados com o OSTINATO.

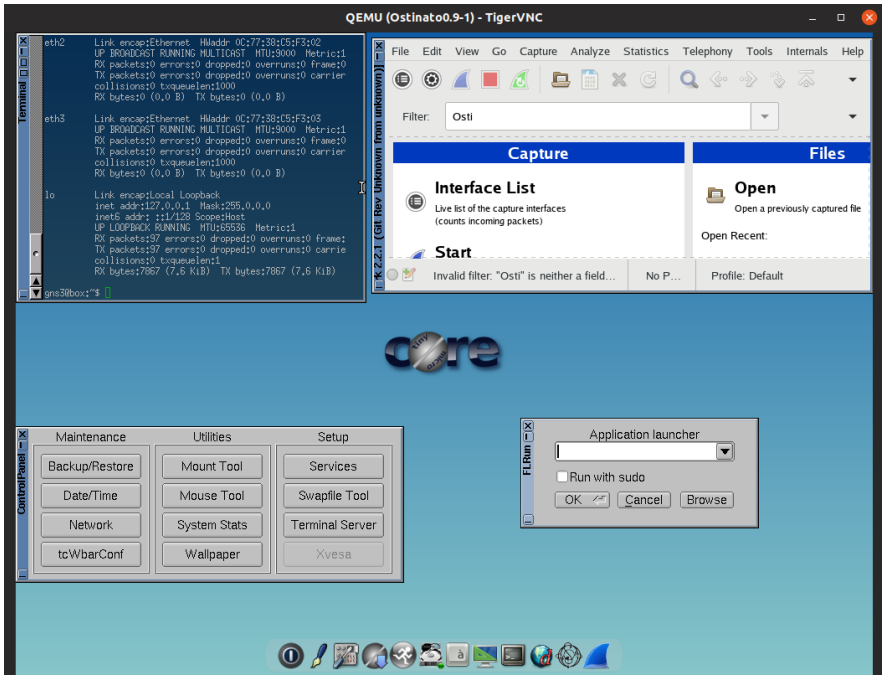

Figura 3.21: Ostinato - Gerador de Tráfego utilizado para simular tráfego de controle de teleproteção no GNS3.

A estrutura desenvolvida para o Cenário 3, além de se ajustar ao que foi feito no laboratório da CEMIG para o Cenário 2, ainda não apresenta custo financeiros adicionais a sua utilização. Somando a vantagem de considerar componentes muito próximos (emulados) dos utilizados na prática. A instalação e configuração do OSTINATO dentro do GNS3, bem como todos os testes relacionados ao projeto CEMIG deram origem ao desenvolvimento desse trabalho de dissertação.

A Figura 3.22 apresenta a primeira tela de configuração do software do gerador de tráfego OSTINATO. É possível observar informações de configuração definidas em tela para testes que foram realizados para o Cenário 3.

A Figura 3.23 e a Figura 3.24 representam telas de configurações do software gerador de tráfego OSTINATO. Onde podemos ver as configurações de camadas e a definição de fluxo de pacotes, respectivamente. A configuração de software referente as camadas visto na Figura 3.23, possibilita alterar informações a nível de camada 1, 2, 3, 4 e 5 referentes aos *Layers* 'L'. A partir desta imagem é possível compreender e alterar a construção de configurações do datagrama usado nas comunicações entre os geradores de tráfegos. Já na Figura 3.24 é possível configurar

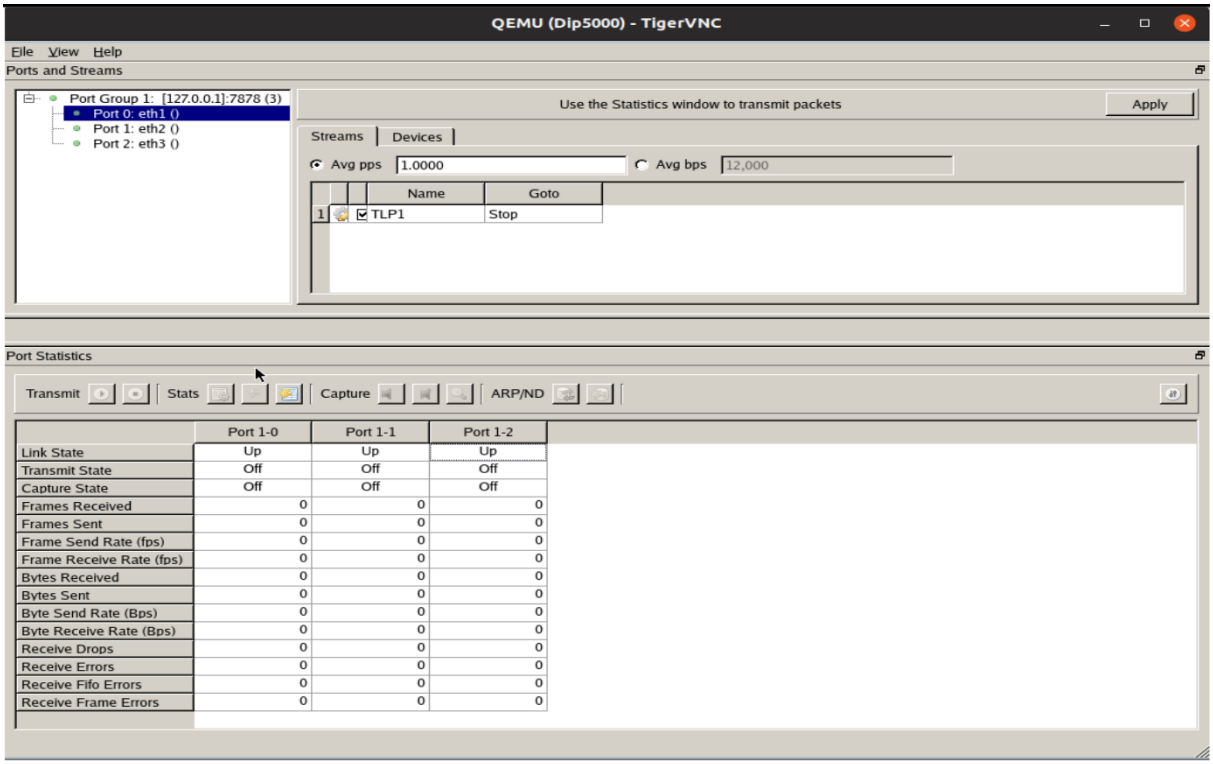

Figura 3.22: Tela 1 de configuração do gerador de tráfego.

a quantidade de pacotes e a taxa de transmissão desejada para testes.

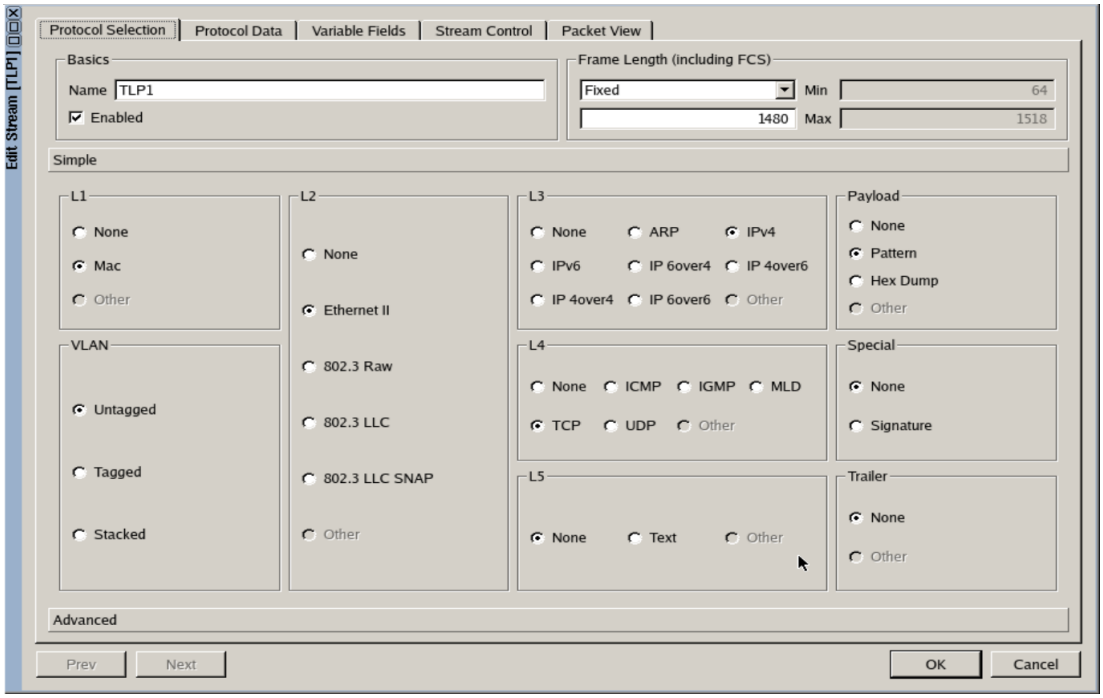

Figura 3.23: Tela 2 de configuração do gerador de tráfego.

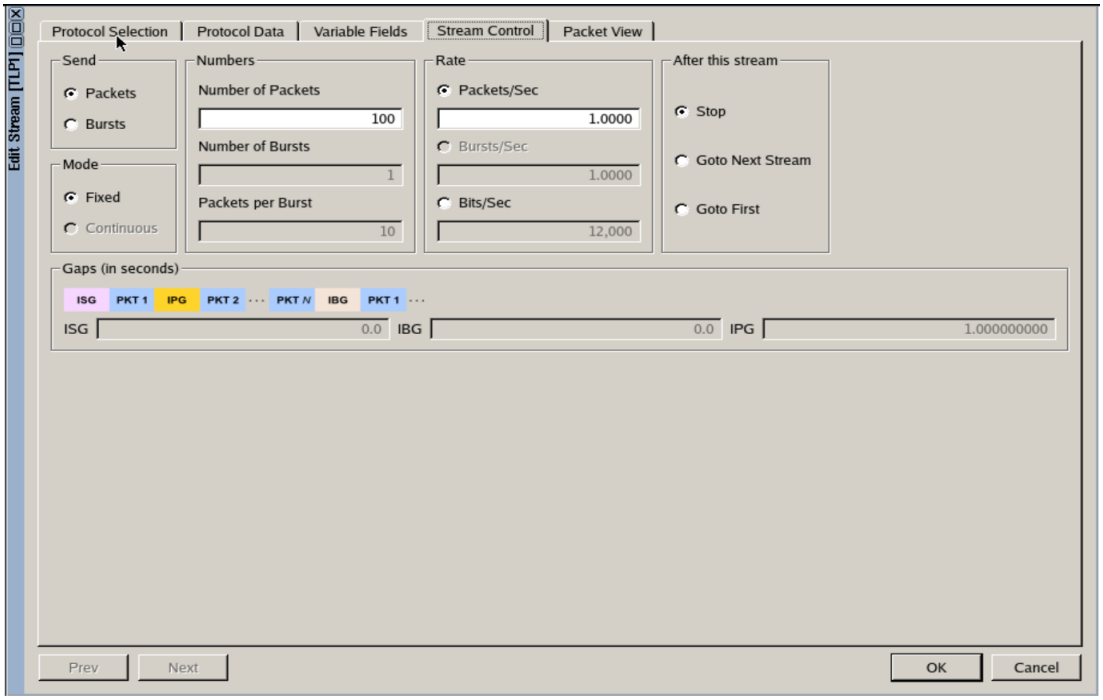

Figura 3.24: Tela 3 de configuração do gerador de tráfego.

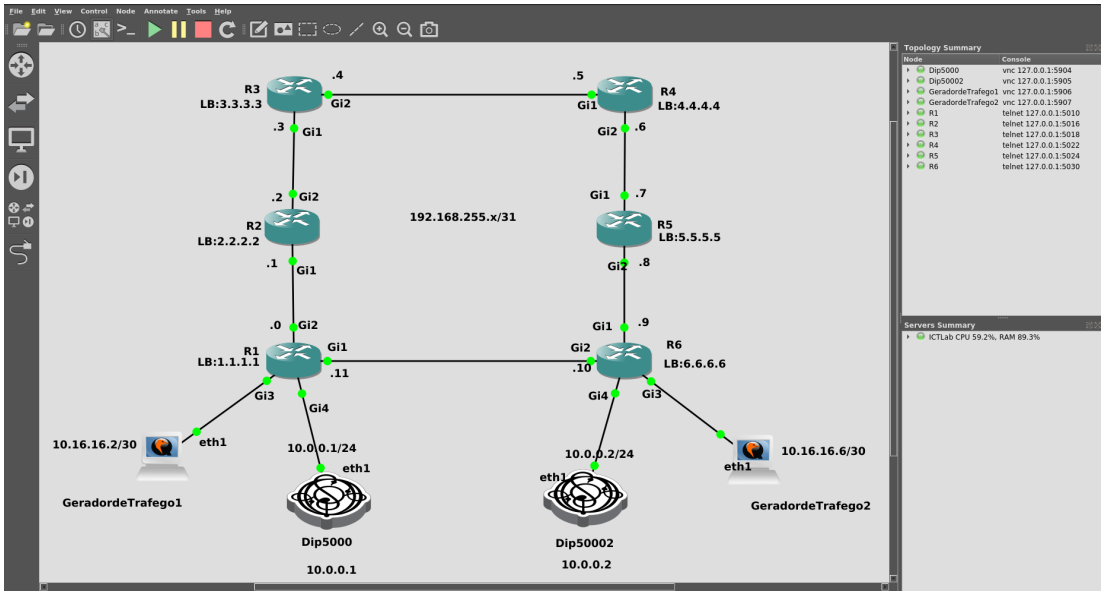

Figura 3.25: Topologia completa do Cenário 3.

Tendo conhecimento dos elementos necessários para construção do Cenário 3, podemos ver na Figura 3.25 a estrutura de rede deste cenário dentro do software GNS3. Esta estrutura foi construída utilizando informações retiradas do Cenário 2, seguindo o modelo de topologia em anel dentro do simulador, afim de garantir a verossimilhança para fins de comparação de resultados de testes, tal qual pode ser observado na Figura 3.25. Reproduzimos o mais fiel possível o Cenário 2 no Cenário 3, mesmo sem as tecnologias Hard-Pipe e Flex-LSP. Mesmo assim, acreditamos que uma comparação justa pode ser feita entre ambos os cenários.

Foram escolhidos endereços de rede /31, ou seja, 192.168.255.x/31, para o endereçamento de todas as interfaces dos enlaces presentes na topologia. Ainda na Figura 3.25 pode ser observada a seguinte estrutura, 6 (seis) roteadores e 4 (quatro) geradores de tráfego OSTINATO. Dentre os equipamentos geradores de tráfego, 2 (dois) deles simulam o tráfego de controle e comunicação entre relés (DIP5000), ou seja, teleproteção. Os outros 2 (dois) geradores de tráfego estão encarregados de simular a injeção de tráfego de dados da rede corporativa.

Para realizar os testes e poder utilizar o *wireshark* presente dentro do OSTINATO, os testes foram executados levando em conta os seguintes aspectos. Foram enviados 100 comandos de teleproteção, um a cada segundo. Essas amostras foram realizadas com tráfego TCP, o qual emulou de forma equivalente o tráfego gerado pelo equipamento DIP5000 no Cenário 2, e recebido pelo DIP5002, que respondia com um ACK. Os DIPS podem ser visualizados na Figura 3.20.

A captura desse tráfego foi realizada por duas instâncias do programa *Wireshark*, um em cada DIP. O *wireshark* inicia a captura de pacotes no instante de tempo zero. Ao receber o primeiro pacote em ambos os lados, estes foram descartados pois o método de medição de atraso na rede não pode ser aplicado. Uma representação do problema enfrentado nas simulações podem ser visto na Figura 3.26

O tempo setado pelo *wireshark* a partir do segundo pacote, é o tempo de processamento do mesmo na máquina virtual que o recebeu. Portanto, foi feita uma subtração do tempo de uma das instâncias do *wireshark* em relação a outra, em todos os pacotes ACKs. Com isso, pode-se obter um tempo estimado de latência no enlace. Por não ter um *clock* interno configurado, a base de tempo adotada é a do Host onde está rodando o GNS3.

O protocolo de roteamento interno escolhido foi o OSPF, sendo todos os roteadores colocados na área zero desse protocolo. Nesse cenário, também foi habilitado o MPLS e a engenharia de tráfego MPLS-TE em todos os roteadores. Para realizar uma coleta de estatísticas de carga

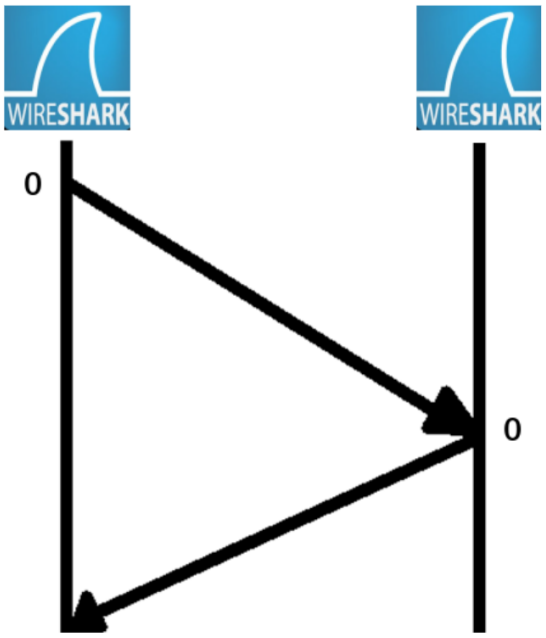

Figura 3.26: Representação dos tempos internos do *wireshark*.

do enlace, foi configurado um **load-interval** de 30 segundos nas interfaces. Para elevar a detecção de falha de *link* na rede, foi habilitado nos roteadores o BFD (*Bidirectional Forwarding Detection*), um protocolo de rede utilizado para detectar falhas entre dois equipamentos. Outra ferramenta habilitada nos roteadores foi o CDP (*Cisco Discovery Protocol*), que é um protocolo proprietário que tem como objetivo obter informações dos dispositivos conectados diretamente, operando na camada 2.

Foi habilitado nos roteadores o RSVP (*Resource Reservation Protocol*), o qual é um protocolo capaz de reservar recursos na rede, oferecendo portanto garantias de QoS para os tráfegos individuais. Algo muito semelhante a um circuito virtual ATM (*Asynchronous Transfer Mode*). As configurações de cenário e seus respectivos protocolos de simulação podem ser visualizadas na Figura 3.27. Essa figura apresenta parte das configurações existentes no roteador R1 da simulação. Nela, podem ser visualizadas as configurações das interfaces G1 (gerador um) e G2 (gerador dois). A Tabela 3.3 por sua vez faz uma comparação entre estrutura de protocolos utilizados no Cenário 2 para equipamentos CISCO e para equipamentos Huawei, com a estrutura de protocolos utilizados no Cenário 3.

Foi criada também uma *cross* conexão, conhecida também como *pseudo-wire* ou *xconnect*. Ou seja, uma ligação ponto a ponto entre as interfaces G4 em que estão conectados os relés (geradores de tráfego de controle simulados) de R1 E R6. Com isso, eles se reconhecem como elementos da mesma rede. Essa *cross* conexão pode ser visualizada na Figura 3.28, a qual esta aplicada na interface G4 de R1, que por sua vez, está atrelada em um túnel, chamado de *tunnel* 0.

Tabela 3.5: Tabela de comparação de protocolos: CISCO, Huawei e Simulação.

Comparando pilha de protocolos em diferentes cenários		
Pilha de protocolos - Huawei	**Pilha de protocolos - CISCO**	**Pilha de protocolos - Simulação**
OSPF(Open Shortest Path First)	OSPF(Open Shortest Path First)	OSPF(Open Shortest Path First)
BGP(Border Gateway Protocol)	BGP(Border Gateway Protocol)	BGP(Border Gateway Protocol)
BFD(Bidirectional Forward Detect)	BFD(Bidirectional Forward Detect)	BFD(Bidirectional Forward Detect)
VRF(Virtual Route and Forwarding)	VRF(Virtual Route and Forwarding)	VRF(Virtual Route and Forwarding)
LDP(Label Distribution Protocol)	LDP(Label Distribution Protocol)	LDP(Label Distribution Protocol)
MPLS(Multiprotocol Label Switching)	MPLS(Multiprotocol Label Switching)	MPLS(Multiprotocol Label Switching)
MPLS-TE(Multiprotocol Label Switching - Traffic Engineering)	MPLS-TE(Multiprotocol Label Switching - Traffic Engineering)	MPLS-TE(Multiprotocol Label Switching - Traffic Engineering)
RSVP(Resouce Reservation Protocol)	RSVP(Resouce Reservation Protocol)	RSVP(Resouce Reservation Protocol)
QoS(Quality of Service)	QoS(Quality of Service)	QoS(Quality of Service)
Túneis	Túneis	Túneis
Configurações de caminhos	Configurações de caminhos	Configurações de caminhos
----	XConnect	XConnect
----	CDP(Cisco Discovery Protocol)	CDP(Cisco Discovery Protocol)
----	PTP(Precision Time Protocol)	N/A
----	SyncE	N/A
Solução para teleproteção	**Solução para teleproteção**	**Solução para teleproteção**
Hard Pipe	Flex LSP	N/A

```
interface GigabitEthernet1
 ip address 192.168.255.11 255.255.255.254
 ip ospf 1 area 0
 ip ospf cost 1
 load-interval 30
 negotiation auto
 cdp enable
 mpls ip
 mpls traffic-eng tunnels
 bfd interval 50 min_rx 50 multiplier 3
 no mop enabled
 no mop sysid
 ip rsvp bandwidth percent 100
!
interface GigabitEthernet2
 ip address 192.168.255.0 255.255.255.254
 ip ospf 1 area 0
 ip ospf cost 1
 load-interval 30
 negotiation auto
 cdp enable
 mpls ip
 mpls traffic-eng tunnels
 bfd interval 50 min_rx 50 multiplier 3
 no mop enabled
 no mop sysid
 ip rsvp bandwidth percent 100
```

Figura 3.27: Configurações de protocolos no cenário de simulação.

Outro *tunnel* foi criado e denominado de *tunnel* 1. Neste *tunnel* 1 foi inserido o tráfego corporativo de fundo, ou seja, o tráfego dos geradores de dados que estão conectados nas interfaces G3 de R1 e R6, simulando o tráfego da rede corporativa. As configurações do *tunnel* 1 podem ser vistas na Figura 3.29.

```
pseudowire-class VPNL2
 encapsulation mpls
 preferred-path interface Tunnel0
!
interface GigabitEthernet4
 no ip address
 ip ospf 1 area 0
 negotiation auto
 no keepalive
 no mop enabled
 no mop sysid
 xconnect 6.6.6.6 100 encapsulation mpls pw-class VPNL2
!
```

Figura 3.28: Conexão direta ou *Cross* Conexão.

```
interface Tunnel1
 ip unnumbered Loopback0
 ip ospf cost 10
 mpls traffic-eng tunnels
 tunnel mode mpls traffic-eng
 tunnel destination 6.6.6.6
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 4 4
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 10 dynamic
```

Figura 3.29: Túnel Para Tráfego Corporativo.

3.4 Considerações Parciais

Neste capítulo, foi abordada a evolução dos cenários de avaliação propostos nessa dissertação, juntamente com a metologia de avaliação de desempenho para cada cenário específico. Observamos que no Cenário 1 foi criada uma estrutura para testes que envolviam tanto uma parte física, quanto uma parte lógica, visando emular topologias da rede elétrica e o comportamento dos relés, que atendiam esse modelo inicial. Foi citado o trabalho de dissertação anterior do Sr. Luiz F. F de Almeida que abordou de forma mais detalhada os aspectos físicos do Cenário 2 [40], experimental, implantando na CEMIG em Belo Horizonte. E por fim, o Cenário 3 que representa a principal contribuição dessa dissertação, que é simulação/emulação da estrutura da rede de teleproteção e de telecomunicações equivalente no simulador/emulador GNS3. No próximo capítulo, vamos discutir os resultados dos testes realizados em cada cenário.

Capítulo 4

Resultados e Análises

Neste capítulo serão apresentados os resultados obtidos com os testes, que foram realizados com o Cenário 2 e o Cenário 3. Realizamos uma comparação dos valores obtidos entre os diferentes cenários e tecnologias. O cenário 1 foi descontinuado não devido seu alto custo financeiro. A Tabela 4.1 apresenta um panorama geral de todos os testes realizados com o cenário físico (Cenário 2), tanto fazendo uso de tecnologia CISCO, quanto da Huawei. A mesma também apresenta os resultados do Cenário 3 obtidos no simulador, possibilitando assim a comparação entre cenários e o acompanhamento no desenrolar dos testes apresentados neste capítulo. Assumimos nesta dissertação que as configurações de teleproteção mesmo não sendo apresentadas na Tabela 4.1, estão presentes em cada um dos testes realizados do Cenário 2, e simulados em todos os testes do Cenário 3.

Tabela 4.1: Tabela geral de análise de resultados.

Taxa (Mbps)	Link	Cenário	Tecnologia	C/ dados corporativos	S/ dados corporativos	Latência (ms)	Localização no texto
2	P	3	Simulação		x	0,58	Tabela 5.6
2	P	3	Simulação	x		1,012	Tabela 5.6
2	P	2	CISCO		x	4,38	Tabela 5.2
2	P	2	CISCO	x		4,73	Tabela 5.4
2	P	2	Huawei		x	5,51	Tabela 5.3
2	P	2	Huawei	x		5,54	Tabela 5.5
2	S	3	Simulação		x	1,87	Tabela 5.7
2	S	3	Simulação	x		1,34	Tabela 5.7
2	S	2	CISCO		x	4,49	Figura 5.1
2	S	2	CISCO	x		10,05	Figura 5.2
10	P	3	Simulação		x	0,89	Tabela 5.6
10	S	3	Simulação		x	1,53	Tabela 5.7
10	P	2	CISCO		x	4,44	Figura 5.3
10	S	2	CISCO		x	4,53	Figura 5.4
10	P	2	Huawei		x	5,62	Figura 5.5
10	S	2	Huawei		x	6,15	Figura 5.6
100	P	3	Simulação		x	1,07	Tabela 5.6
100	S	3	Simulação		x	1,72	Tabela 5.7
100	P	2	CISCO		x	4,53	Figura 5.7
100	S	2	CISCO		x	4,55	Figura 5.8

A Tabela 4.1 apresenta os resultados de testes por ordem de banda de transmissão, sendo respectivamente, 2 Mbps, 10 Mbps e 100 Mbps. A primeira coluna **'Taxa Mbps'** trata do valor de banda utilizado em cada teste, seja no link principal ou no link secundário. A segunda coluna 'Link', como o próprio nome se refere, trata em qual link foi realizado o teste em questão. A coluna **'Cenário'** por sua vez determina juntamente com a coluna **'Tecnologia'**, o cenário e o fornecedor com sua respectiva tecnologia utilizada. No caso da simulação, utilizamos o *label* "Simulação". A coluna **'C/ dados corporativos'** e a coluna **'S dados corporativos'** tratam, respectivamente, da presença ou ausência dos dados corporativos durante a realização dos testes. A coluna **'Latência'** apresenta o melhor valor obtido na transmissão do referido teste. E por ultimo a coluna 'Localização no texto', mostra onde os resultados podem ser consultados neste texto.

4.1 Resultados do Cenário 2

Analisando os resultados do Cenário 2, foi possível observar uma deficiência na alocação de recursos de rede. Ou seja, na construção do Cenário 2 foram constatadas vantagens em se trabalhar com tecnologias como: IP, MPLS, Hard Pipe e Flex LSP. Como descrito no trabalho [40]. Na Tabela 4.2 é possível observar o campo comando com itens A, B, C e D. Sendo esses comandos informações especificas de configuração dentro do Cenário 2.

4.1.1 Cenário 2 - 2 Mbps

1. Link principal com presença de comandos de teleproteção, sem tráfego de dados, utilizando taxas de 2Mbps no Cenário 2.

   - CISCO

Tabela 4.2: CISCO - 2Mbps.

	Comando	Intervalo de confiança (ms)	Latência média (ms)
G.703 2 Mbps	**A**	**4,6689 e 4,6951**	**4,6820**
	B	**4.6524 e 4.6776**	**4,6650**
	C	**4,3963 e 4,4217**	**4,4090**
	D	**4,3746 e 4,3994**	**4,3870**

   - Huawei

Tabela 4.3: Huawei 2Mbps

	Comando	Intervalo de confiança (ms)	Latência média (ms)
G.703 2 Mbps	**A**	**5,7773 e 5,8057**	**5,7915**
	B	**5,7626 e 5,7914**	**5,7770**
	C	**5,5012 e 5,5298**	**5,5155**
	D	**5,5064 e 5,5346**	**5,5205**

2. Link principal com presença de comandos de teleproteção, com tráfego de dados, utilizando taxas de 2Mbps no Cenário 2.

   - CISCO

Tabela 4.4: CISCO - 2Mbps.

	Comando	Intervalo de confiança (ms)	Latência média (ms)
G.703 2 Mbps	**A**	**5,0164 e 5,0536**	**5,0350**
	B	**5,0085 e 5,0395**	**5,0240**
	C	**4,7459 e 4,7801**	**4,7630**
	D	**4,7158 e 4,7542**	**4,7350**

- Huawei

Tabela 4.5: Huawei 2Mbps

	Comando	Intervalo de confiança (ms)	Latência média (ms)
G.703 2 Mbps	**A**	**5,8021 e 5,8299**	**5,8160**
	B	**5,8002 e 5,8248**	**5,8125**
	C	**5,5272 e 5,5538**	**5,5405**
	D	**5,5321 e 5,5599**	**5,5460**

As Tabelas 4.2 e 4.3, se referem a testes realizados no link principal do Cenário 2, com comandos de teleproteção e sem a presença de tráfego de dados corporativos. As Tabelas 4.4 e 4.5 por sua vez, se referem aos testes realizados com a mesma configuração, porém com a presença de tráfego corporativos e comandos de teleproteção, simultaneamente.

A partir deste ponto, utilizamos resultados e testes dentro do Cenário 2 que não estão descritos no trabalho de dissertação do [40], visto que não foram utilizados pelo mesmo, referentes ao link secundário de 2 Mbps. Estes valores foram obtidos nas mesmas circunstâncias de testes descritas para o Cenário 2, utilizando os mesmos equipamentos. Contudo, foram realizados apenas no link secundário para a arquitetura CISCO, com 2 Mbps.

1. CISCO

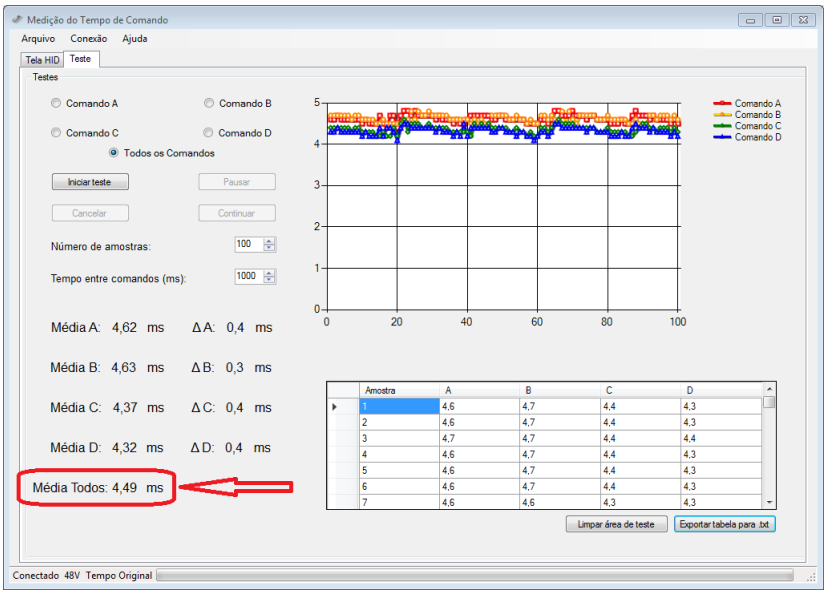

Figura 4.1: Resultado CISCO 2 Mbps link secundário, sem tráfego de dados corporativos e com comandos de teleproteção.

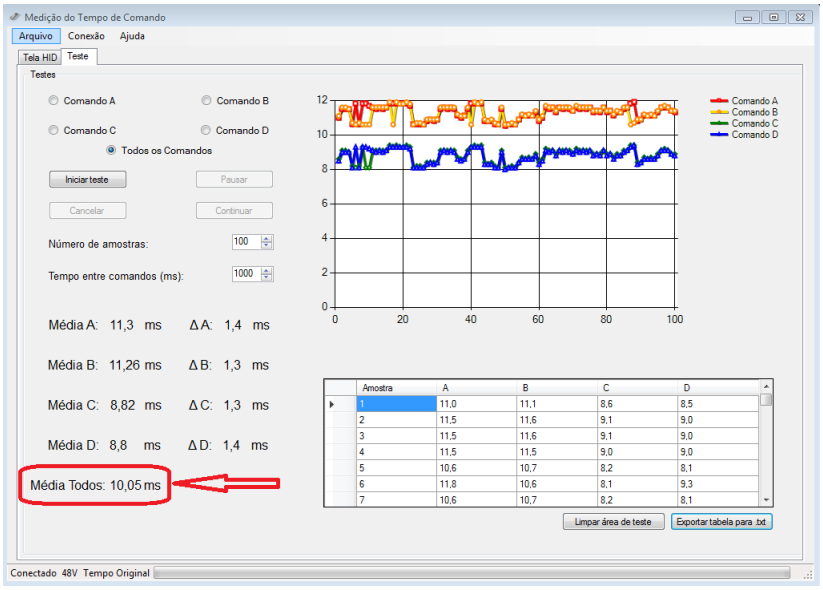

Figura 4.2: Resultado CISCO 2 Mbps link secundário, com trafego de dados corporativos e com comandos de teleproteção.

As Figuras 4.1 e 4.17 mostram os resultados do software responsável por gerar comandos que simulam o funcionamento de relés no projeto CEMIG (Cenário 2). A Figura 4.1 apresenta os resultados com melhor média de comunicação sem tráfego de dados e com comandos de teleproteção no link secundário, para 2 Mbps. A Figura 4.17 apresenta os resultados com melhor média de comunicação com tráfego de dados e com comandos de teleproteção no link secundário, para 2 Mbps.

4.1.2 Cenário 2 - 10 Mbps

Neste tópico vamos apresentar os resultados para testes no Cenário 2 envolvendo banda de 10 Mbps, com equipamentos CISCO e Huawei para o link principal e link secundário deste teste. Importante salientar que estes testes de 10 Mbps realizados no Cenário 2, foram feitos para este trabalho de dissertação. Isso com o objetivo de comparar os mesmos com o Cenário 3, proposto a seguir. A Figura 4.3 representa os testes obtidos no link principal com uso de tecnologia CISCO no Cenário 2. É possível observar o valor médio de latência de 4,44 ms para uma banda de transmissão de 10 Mbps. Por sua vez, a Figura 4.4 representa os testes obtidos no link secundário com uso de tecnologia CISCO. É possível observar o valor médio de latência de 4,53 ms para uma banda de transmissão de 10 Mbps.

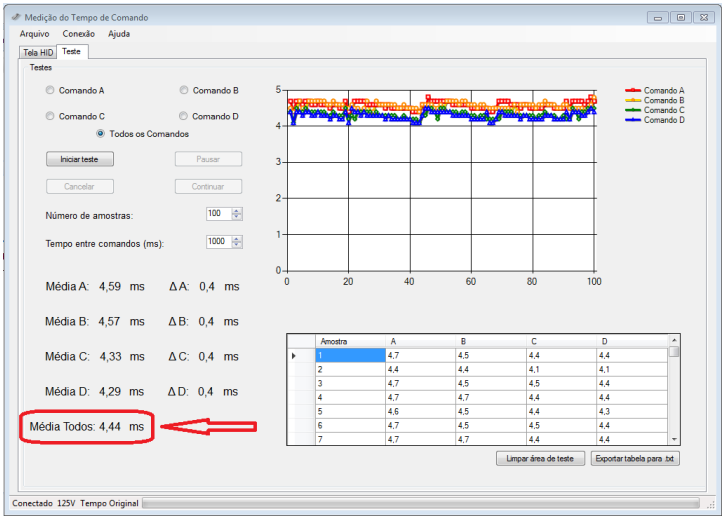

Figura 4.3: Resultado CISCO 10 Mbps link principal.

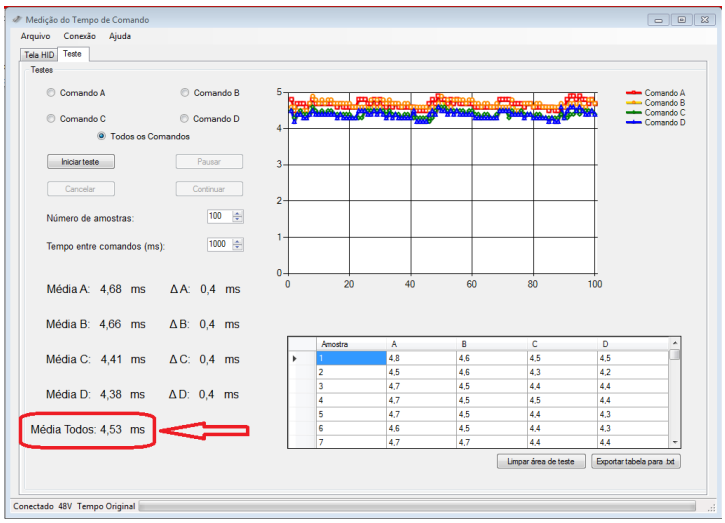

Figura 4.4: Resultado CISCO 10 Mbps link secundário.

A Figura 4.6 representa o resultado obtido com a arquitetura Huawei para o Cenário 2, com taxa de 10 Mbps no link principal. É possível observar que neste caso o valor médio de latência ficou em 6,15 ms. A Figura **??** por sua vez apresenta os resultados no mesmo cenário e arquitetura para o link secundário com o valor médio de 5,62 ms.

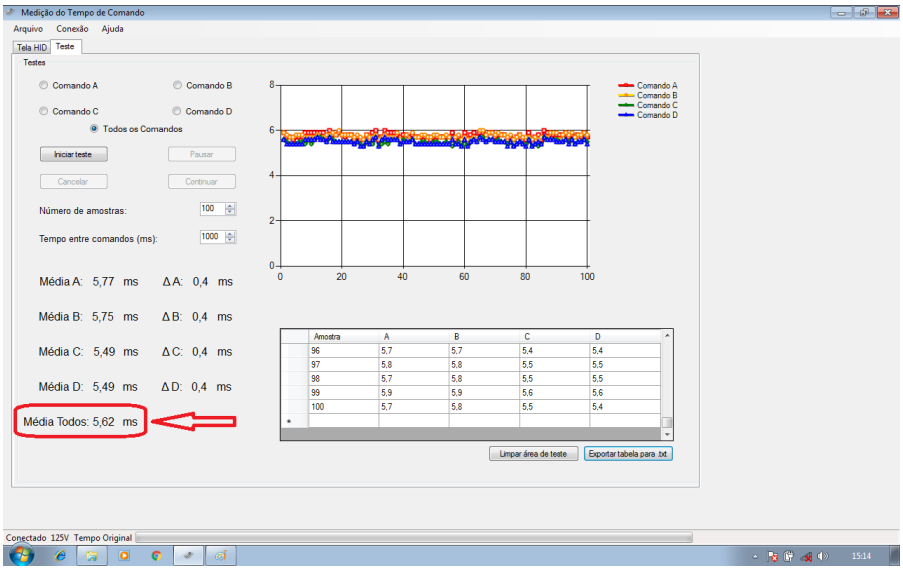

Figura 4.5: Resultado Huawei 10 Mbps link principal.

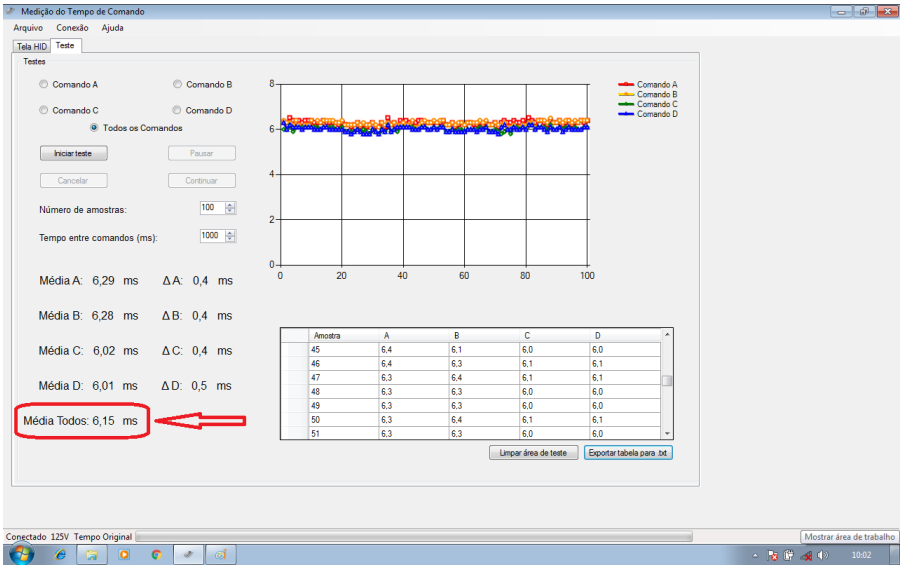

Figura 4.6: Resultado Huawei 10 Mbps link secundário.

4.1.3 Cenário 2 - 100 Mbps

Dando continuidade aos testes do Cenário 2, optamos por aumentar a taxa de transmissão da banda de testes para 100 Mbps, afim de obter mais resultados de comparação com o Cenário 3. Nos testes a seguir, vamos fazer uso apenas de equipamentos CISCO no cenário 2. A Figura 4.7 se refere a taxa de transmissão no link principal com banda de 100 Mbps. É possível observar que a média de latência ficou com valor de 4,53 ms. O resultado segue o padrão dos resultados de testes apresentados anteriormente, de forma que as Figuras 4.7 e 4.8 foram capturadas da tela do software utilizado para configuração de relés pela CEMIG. A Figura 4.8 por sua vez se refere as informações obtidas com teste no link secundário, com valor médio de latência 4,55 ms.

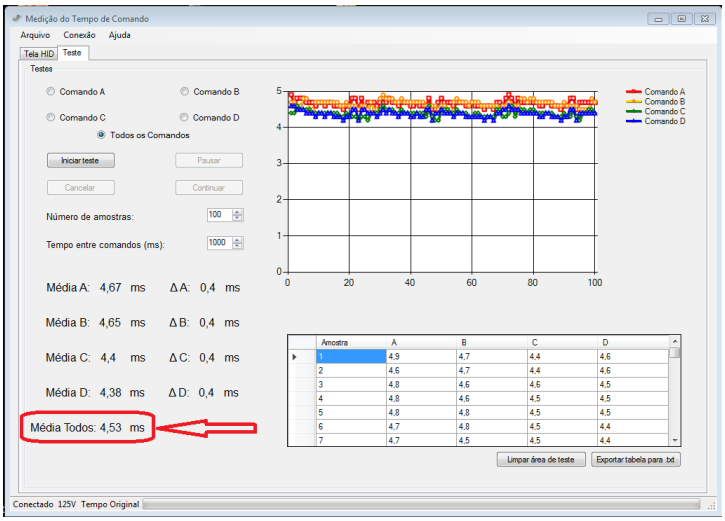

Figura 4.7: Resultado CISCO 100 Mbps link principal.

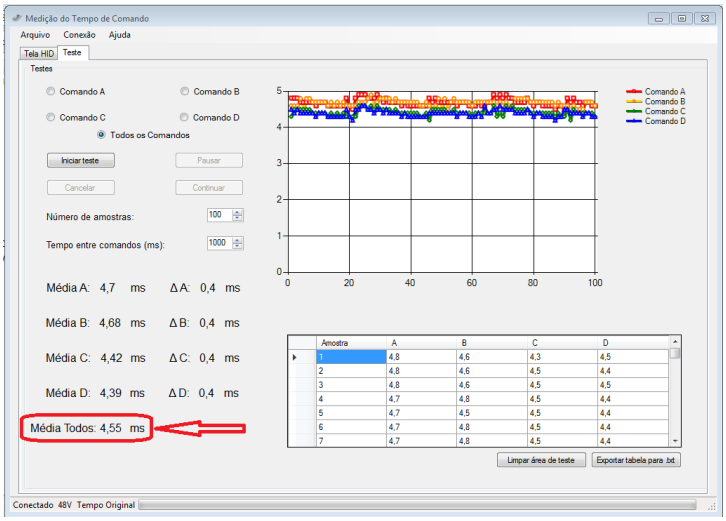

Figura 4.8: Resultado CISCO 100 Mbps link secundário.

4.2 Resultados do Cenário 3

Com a utilização do software de simulação GNS3, foi realizada uma bateria de testes envolvendo o link principal e o link secundário. Os componentes da rede foram emulados, enquanto os links de comunicação simulados. Apresentamos a seguir os resultados obtidos com as configurações propostas para cada um dos links com o software de simulação.

4.2.1 Valores obtidos

Na Figura 4.9, apresentamos um *printscreen* da tela da ferramenta *Wireshark* com o tempo de resposta de uma amostra relativo a uma mensagem *ping* do protocolo ICMP no *link* principal. Como se pode ver, o valor de latência ficou em 0.013 ms. Na Figura 4.10 tem-se o tempo de resposta do *link* secundário, o valor de latência, 0.016 ms. Os valores de tempo de resposta demonstrados neste teste e observados nas Figuras 4.9 e 4.10, confirmam a melhor amostra para o *link* principal no Cenário 3. É importante ressaltar que a busca pelo menor valor de latência é ideal visto que o mesmo impacta diretamente no desempenho de ativação do relé ao receber os comandos de teleproteção, seja qual for o cenário..

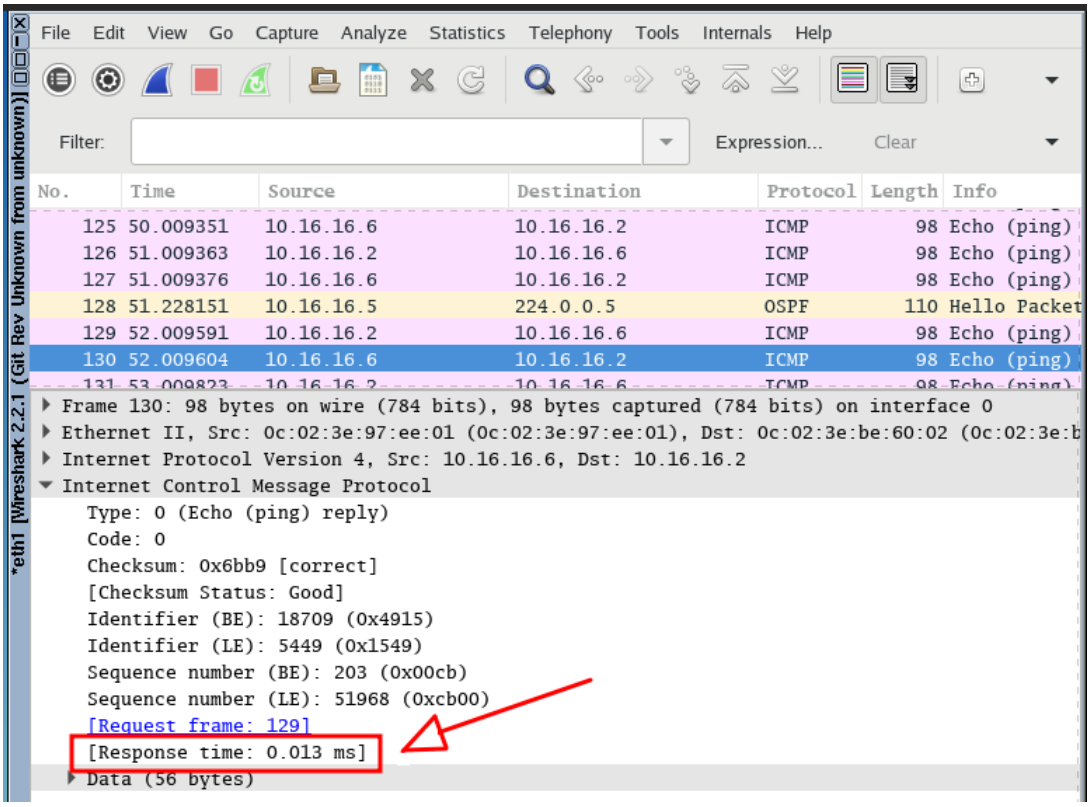

Figura 4.9: Tempo de resposta do *link* principal (*ping*).

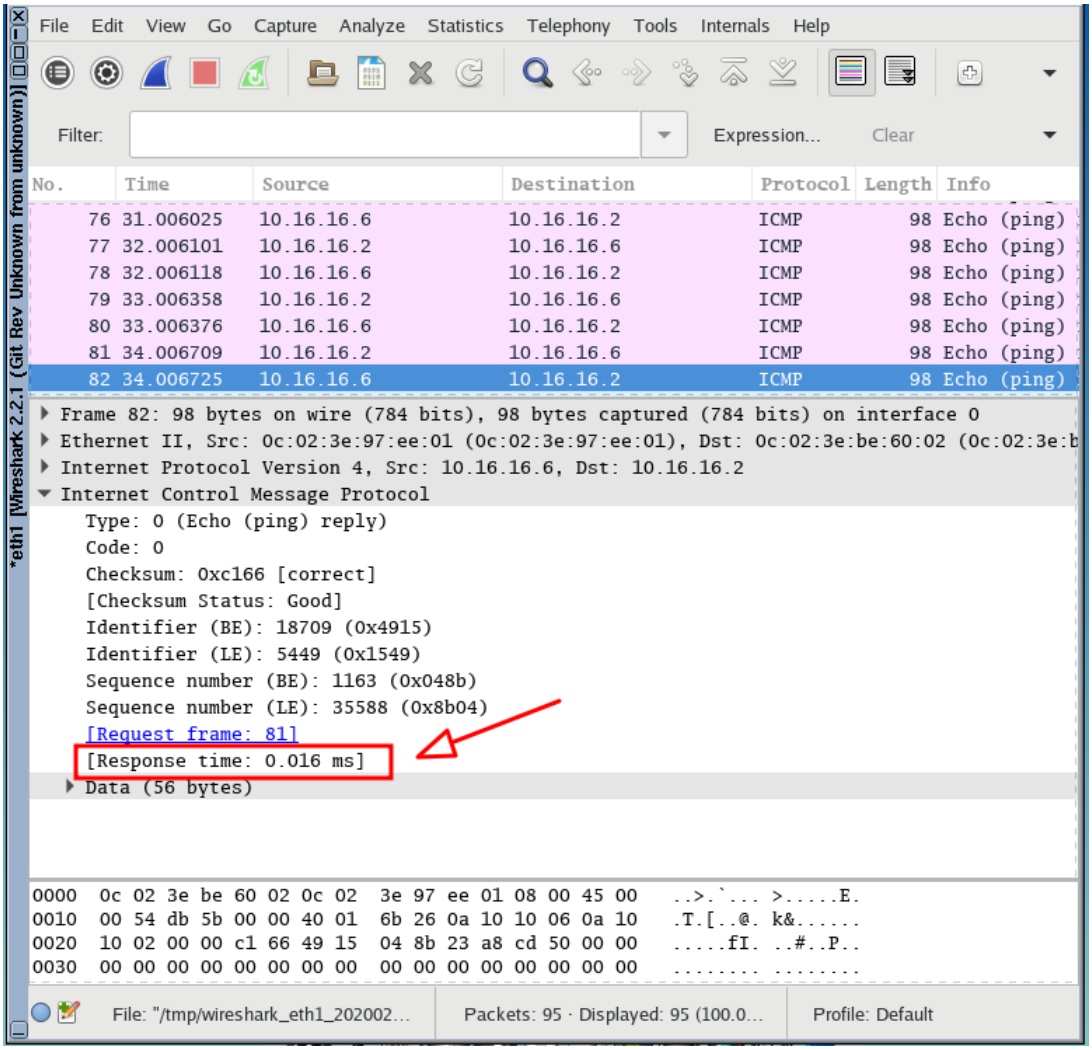

Figura 4.10: Tempo de resposta do *link* secundário (*ping*).

Na Figura 4.11, bem como nas Figuras 4.9 e 4.10 podem ser vistos os tempos de resposta dos testes de conectividade (*ping*) entre os geradores de tráfego. Com as possíveis configurações que foram citadas acima, podemos alterar algumas características dos tuneis, como por exemplo, a taxa de transmissão alocada. Para uma análise em maiores detalhes, foram realizadas verificações dos tempos de resposta em ambos os geradores.

A Figura 4.12 mostra uma tela capturada pela ferramenta Wireshark mostrando os pacotes TCP recebidos, destacados em vermelho, e os pacotes TCP ACK de resposta, destacado em preto. Pacotes que simulam comandos de teleproteção através do enlace principal. O protocolo TCP é diretamente responsável pelo estabelecimento do link de comunicação. O equipamento ao receber um pacote TCP, envia uma resposta, desta forma confirmando o recebimento dos comandos simulados.

Os pacotes TCP simulam o tráfego de comandos de controle de teleproteção no equipamento após o enlace principal.

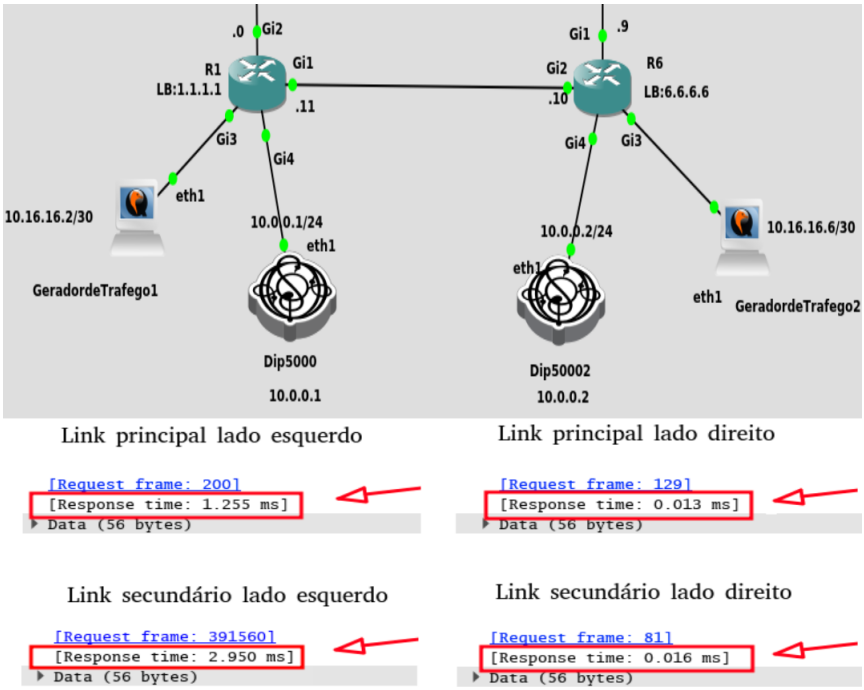

Figura 4.11: Tempos de resposta no link principal e *link* secundário (*ping*).

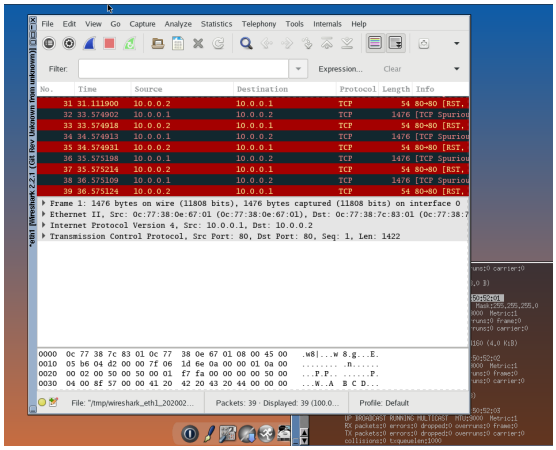

Figura 4.12: *Printscreen* da tela do Wireshark.

O tráfego máximo que conseguimos através do gerador, foi um pouco mais de 900 Mbps, como pode ser visto na Figura 4.13. Somente conseguimos gerar esse tráfego máximo de 916 Mbps ao manter ligados apenas os geradores e os roteadores R1 e R6, pois o consumo de CPU e memória do *host* chegavam ao limite, como pode ser visto na Figura 4.14.

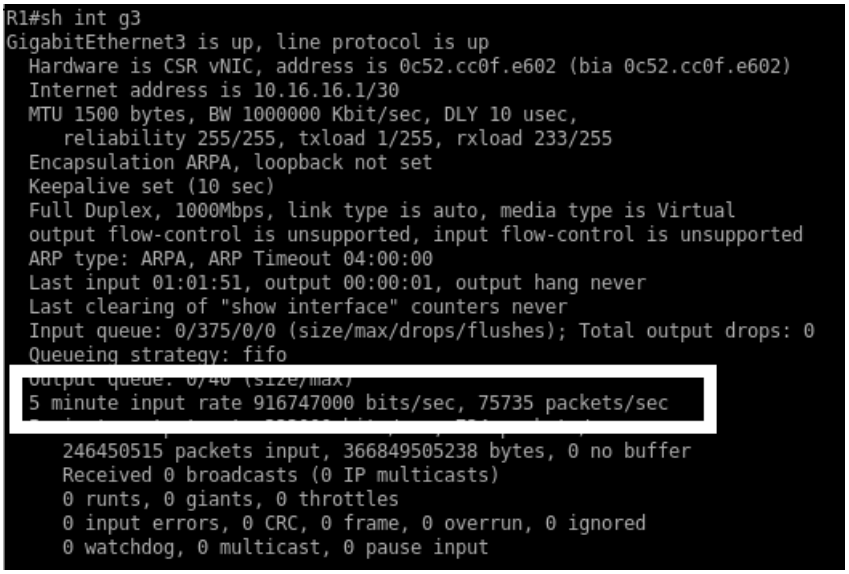

Figura 4.13: Tráfego máximo pelo *host*.

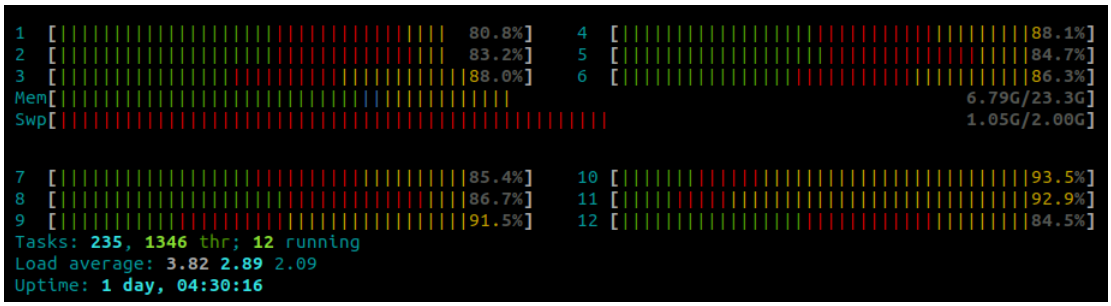

Figura 4.14: Visualização do consumo dos recursos de hardware do *host*.

4.3 Análise dos resultados do Cenário 3

O consumo de processamento foi uma das dificuldades que enfrentamos no decorrer das simulações. Esse problema chegou a ocasionar falhas e/ou travamento da máquina *host*. Por questão de segurança e confiabilidade nos testes, o máximo tráfego ativo na simulação foi de 10 Mbps. Contudo é importante realizar a separação entre volume de tráfego ativo com banda de tráfego alocada em cada link, seja principal ou secundário. Os testes realizados no Cenário envolvem banda de comunicação com taxa variando entre 2 Mbps, 10 Mbps e 100Mbps.

Todos os resultados consolidados das simulações podem ser visualizados nas Tabelas 4.6 e 4.7. Os valores obtidos para estruturação dessas tabelas também podem ser observados nas Figuras: 4.15, A.1, A.2,...,A.23, referentes a cada teste do 1º (primeiro) ao 24º (vigésimo quarto) teste. Os resultados dos testes 2 ao 24, podem ser consultados nos anexos deste trabalho de dissertação.

Cabe observarmos que o volume de testes realizados tanto no cenário 2 e no cenário 3, se fizeram necessários para corroborar a hipótese defendida neste trabalho de dissertação. Ao final da análise de resultados vai ser possível ao leitor confirmar que o simulador apresenta resultados muito similares aos obtidos nos testes do cenário 2. Tal conclusão não seria possivel caso não existisse a variação de testes em link principal, secundário e bandas de comunicação no meio.

Analisando os resultados da Tabela 4.6 que corresponde ao link principal, é possível observar seu melhor resultado e seu pior resultado, referentes aos testes realizados. Logo é possível

Tabela 4.6: Tabela Geral de Resultados para o Cenário 3.

Link de Comunicação Principal					
Tráfego + Comandos de Teleproteção					
Nº do Teste	**Taxa de Tx**	**Vel.Tx/Sem QoS**	**Nº do Teste**	**Taxa de Tx**	**Vel.Tx/Com QoS**
Teste 1	2 Mbps	0,5873ms	Teste 4	2 Mbps	0,7235
Teste 2	10 Mbps	0,577ms	Teste 5	10 Mbps	0,6026ms
Teste 3	100 Mbps	0,7323ms	Teste 6	100 Mbps	0,7365ms
Comandos de Teleproteção					
Teste 7	2 Mbps	1,012ms	Teste 10	2 Mbps	0,2071ms
Teste 8	10 Mbps	0,8966ms	Teste 11	10 Mbps	0,9921ms
Teste 9	100 Mbps	1,077ms	Teste 12	100 Mbps	1,25ms

Tabela 4.7: Tabela Geral de Resultados para o Cenário 3.

Link de Comunicação Secundário					
Tráfego + Comandos de Teleproteção					
Nº do Teste	**Taxa de Tx**	**Vel.Tx/Sem QoS**	**Nº do Teste**	**Taxa de Tx**	**Vel.Tx/Com QoS**
Teste 13	2 Mbps	1,349ms	Teste 16	2 Mbps	1,401
Teste 14	10 Mbps	1,269ms	Teste 17	10 Mbps	1,353ms
Teste 15	100 Mbps	1,348ms	Teste 18	100 Mbps	1,105ms
Comandos de Teleproteção					
Teste 19	2 Mbps	1,87ms	Teste 22	2 Mbps	1,688ms
Teste 20	10 Mbps	1,536ms	Teste 23	10 Mbps	1,78ms
Teste 21	100 Mbps	1,762ms	Teste 24	100 Mbps	1,178ms

afirmar que a melhor resposta de atraso médio de transmissão nesse cenário é de 0,577ms. Esse resultado foi obtido no Teste 2 com taxa de transmissão de 10 Mbps, e pode ser comprovado via Figura A.1. Por sua vez, o pior resultado obtido no link principal foi de 1,25ms. O mesmo corresponde ao Teste 12 com taxa de transmissão de 2 Mbps, ele poder ser visto na Figura A.11.

Observando os resultados da Tabela 4.7 que corresponde ao link secundário, podemos afirmar que seu melhor resultado e pior resultado são respectivamente os Teste 18 e Teste 19. O Teste 18 usou taxa de transmissão igual á 100 Mbps, obteve um atraso médio de transmissão de 1,105 ms, sendo esse o melhor cenário. Já o Teste 19 utilizou taxa de transmissão de 2 Mbps e obteve um atraso médio de transmissão de 1,87 ms.

Todas a figuras a seguir seguem o mesmo padrão. Assim, para não tornar esse trabalho de dissertação repetitivos vamos analisar a estrutura apenas da Figura 4.15. Obviamente, considerando os valores e gráficos de resposta de forma individual a cada Figura tem-se variações. Na Figura 4.15, plotada em um plano cartesiano apresenta duas linhas em sua legenda. A linha azul se refere ao níveis de latência do teste. A linha vermelha mostra o resultado médio de atraso de transmissão (0,5873 ms). Nesse caso, a taxa de transmissão era de 2 Mbps. Informações de tempo, taxa, amostra e gráfico de latência média de transmissão podem ser observada em todas a imagens plotadas dos testes subsequentes.

Os resultados obtidos foram utilizados para montar as Tabelas 4.6 e 4.7 do Cenário 3. Tendo posse desses resultados, foi possível realizar uma analise comparativa de forma quantitativa em relação ao valor de latência obtido em cada teste do Cenário 3.

Nos tópicos a seguir deste dissertação, será possível definir de posse desses resultados obtidos, qual cenário obteve melhor desempenho. Levando em consideração a largura de banda e a rota utilizada, *link* principal ou *link* secundário

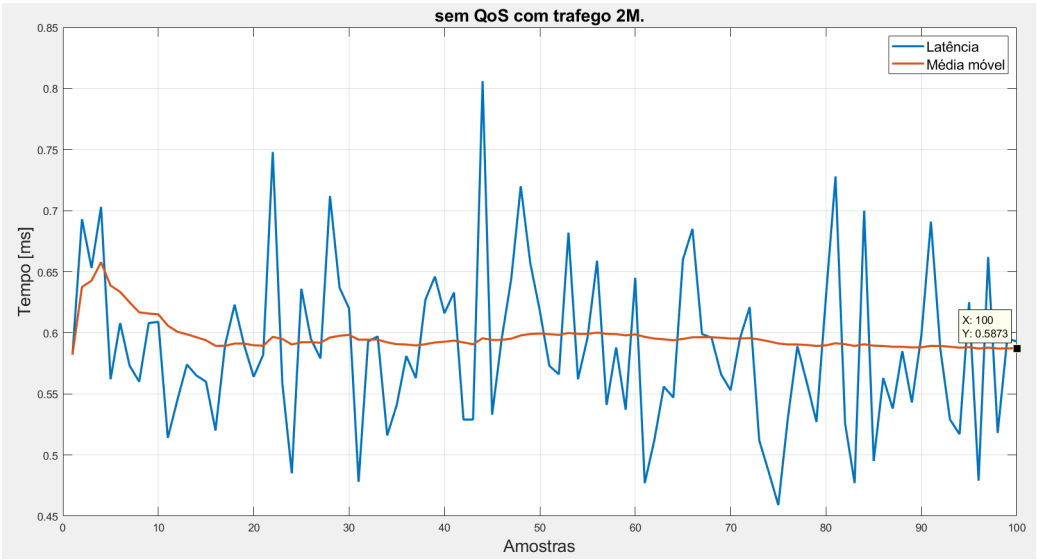

Figura 4.15: Teste 1.

4.4 Comparando resultados do Cenário 2 e 3

Neste tópico, realizaremos um comparativo dos resultados obtidos, entre diferentes testes que foram realizados e apresentados neste trabalho de dissertação até o momento. Os referidos testes fizeram uso de diferentes taxas de transmissão, diferentes estruturas de rede, ora envolvendo a presença ou ausência de tráfego de dados corporativos, ora alternando o uso de tecnologias CISCO e/ou Huawei para construção do cenário 2. Durante os testes o uso do link principal, link secundário e comandos de teleproteção estavam presentes em todas as situações apresentadas, tanto para o Cenário 2 quanto para o Cenário 3. Reforçamos que o Cenário 2 representa os testes em meio físico, enquanto os do Cenário 3 buscam a equivalência através de um cenário simulado/emulado.

4.4.1 Comparando resultados de cenários - 2 Mbps

A partir deste ponto comparamos os resultados de transmissão com taxa de 2 Mbps, para *link* principal e *link* secundário, dentro do Cenário 2, com estrutura Huawei, comparando os mesmos com o Cenário 3.

Huawei

Neste tópico serão analisados os resultados de transmissão do Cenário 2 com tecnologia Huawei para banda de comunicação de 2Mbps. Foram testes com o objetivo de comparar os resultados obtidos no Cenário 2 Huawei, com os resultados obtidos no Cenário 3 de simulação. A Tabela 4.8 trata dos resultados em Cenário 2 com equipamento Huawei, sem inserção de tráfego corporativo e com banda de 2 Mbps, apenas com a presença de comandos de teleproteção. Esses resultados foram reestruturados a partir do trabalho [40] e estão destacados na Tabela 4.8.

Vale ressaltar que em todos os testes, buscamos o menor valor de latência, como sendo o mais desejável. Isso ocorre pois impacta diretamente no tempo de resposta do sistema de teleproteção. Isso se aplica em todos os testes, independente da banda de comunicação utilizada.

A Tabela 4.9 apresenta resultados do Cenário 3, com melhor valor 1,012 ms de latência, ao passo que a Tabela 4.8 tem como melhor valor 5,5155 ms de latência. Esses resultados mostram que a ordem de grandeza do atraso para os comandos de teleproteção (físicos no Cenário 2 e simulados com TCP no Cenário 3) é muito próxima. O Cenário 3 com seus protocolos e condições de simulação/emulação apresentou um atraso levemente menor que o Cenário 2 com Hard-PIPE (Huawei). Ou seja, o resultado do Cenário 3 para a seguinte condição: 'Comandos de teleproteção no link principal, sem a presença de sinal de dados corporativos', é superior ao Cenário 2 com equipamentos Huawei em ambos os casos (físicos no Cenário 2 e emulados no Cenário 3).

Observa-se que o resultado no Cenário 3 é superior ao obtido no Cenário 2 com uso de tecnologia Huawei. Esse resultado se deve entre outros fatores, ao fato que o Cenário 2, necessita do uso de conversores, além de existência de atrasos de comunicação provenientes do meio físico. Vale destacar que a Tabela 4.8 apresenta 4 resultados, contudo, optamos por escolher o melhor entre os mesmos para fins de comparação com Cenário 3. Isso é justificável, pois em ambos os casos temos comandos de teleproteção semelhantes.

Tabela 4.8: Cenário 2 - Teste na rota principal com meio físico sem inserção de tráfego - Huawei.

	Comando	Intervalo de confiança (ms)	Latência média (ms)
G.703 2 Mbps	**A**	**5,7773 e 5,8057**	**5,7915**
	B	**5,7626 e 5,7914**	**5,7770**
	C	**5,5012 e 5,5298**	**5,5155**
	D	**5,5064 e 5,5346**	**5,5205**

Tabela 4.9: Tabela Geral de Resultados para o Cenário 3.1.

Link de Comunicação Principal					
Tráfego + Comandos de Teleproteção					
Nº do Teste	**Taxa de Tx**	**Vel.Tx/Sem QoS**	**Nº do Teste**	**Taxa de Tx**	**Vel.Tx/Com QoS**
Teste 1	2 Mbps	0,5873ms	Teste 4	2 Mbps	0,7235
Teste 2	10 Mbps	0,577ms	Teste 5	2 Mbps	0,6026ms
Teste 3	100 Mbps	0,7323ms	Teste 6	2 Mbps	0,7365ms
Comandos de Teleproteção					
Teste 7	2 Mbps	1,012ms	Teste 10	2 Mbps	0,2071ms
Teste 8	10 Mbps	0,8966ms	Teste 11	2 Mbps	0,9921ms
Teste 9	100 Mbps	1,077ms	Teste 12	2 Mbps	1,25ms

Na Tabela 4.10 referente ao Cenário 2 são apresentados os resultados no link principal com presença de tráfego corporativo acrescidos de comandos de teleproteção. Nela, é possível observar que o melhor resultado para transmissão de 2 Mbps é de 5,5405 ms de latência. Na Tabela 4.11 referente ao Cenário 3, é possível ver que para a mesma taxa de transmissão nos enlaces o resultado é de 0,583ms de latência, também executando transmissão de dados mais comandos de teleproteção. Novamente, foi observado um resultado superior no cenário com software de simulação GNS3. Ou seja, o resultado do Cenário 3 para a seguinte condição: 'Comandos de teleproteção no link principal, com a presença de sinal de dados corporativos', é superior ao Cenário 2 com estrutura Huawei. Acreditamos que o motivo é o mesmo do caso anterior. O cenário de simulação não usa conversores de mídia.

Tabela 4.10: Teste na rota principal com meio físico, com inserção de tráfego mais comandos de teleproteção - Huawei.

	Comando	**Intervalo de confiança (ms)**	**Latência média (ms)**
G.703 2 Mbps	**A**	**5,8021 e 5,8299**	**5,8160**
	B	**5,8002 e 5,8248**	**5,8125**
	C	**5,5272 e 5,5538**	**5,5405**
	D	**5,5321 e 5,5599**	**5,5460**

Tabela 4.11: Tabela Geral de Resultados para o Cenário 3.2.

Link de Comunicação Principal					
Tráfego + Comandos de Teleproteção					
Nº do Teste	**Taxa de Tx**	**Vel.Tx/Sem QoS**	**Nº do Teste**	**Taxa de Tx**	**Vel.Tx/Com QoS**
Teste 1	2 Mbps	0,5873ms	Teste 4	2 Mbps	0,7235
Teste 2	10 Mbps	0,577ms	Teste 5	2 Mbps	0,6026ms
Teste 3	100 Mbps	0,7323ms	Teste 6	2 Mbps	0,7365ms
Comandos de Teleproteção					
Teste 7	2 Mbps	1,012ms	Teste 10	2 Mbps	0,2071ms
Teste 8	10 Mbps	0,8966ms	Teste 11	2 Mbps	0,9921ms
Teste 9	100 Mbps	1,077ms	Teste 12	2 Mbps	1,25ms

CISCO

Dando continuidade no comparativo de resultados do Cenário 2 com o Cenário 3, foram refeitos os testes do Cenário 2 fazendo uso de tecnologia CISCO, para banda de comunicação de 2 Mbps. A Tabela 4.12 apresenta os resultados de testes na rota principal sem inserção de tráfego corporativo para o Cenário 2, com infraestrutura CISCO. Todos os resultados estão em destaque na tabela, contudo o que mais se destacou foi o de 4,387ms de latência, ainda usando a taxa de transmissão de 2 Mbps. Observando a Tabela 4.9 temos os resultados de 1,012 ms de latência para link de 2 Mbps, sem trafego de dados corporativo, no Cenário 3. Desta forma, podemos afirmar que o resultado do Cenário 3 para a seguinte condição: 'Comandos de teleproteção no link principal, sem a presença de sinal de dados corporativos', é superior ao Cenário 2 com estrutura CISCO devido aos valores obtidos de latência.

Tabela 4.12: Cenário 2 - Teste na rota principal com meio físico sem inserção de tráfego - CISCO.

	Comando	Intervalo de confiança (ms)	Latência média (ms)
G.703 2 Mbps	**A**	**4,6689 e 4,6951**	**4,6820**
	B	**4.6524 e 4.6776**	**4,6650**
	C	**4,3963 e 4,4217**	**4,4090**
	D	**4,3746 e 4,3994**	**4,3870**

A Tabela 4.13 trata de resultados com meio físico, com inserção de tráfego de fundo adicionado aos comandos de teleproteção, no Cenário 2 com infraestrutura CISCO. O melhor resultado obtido em destaque na Tabela foi de 4,735ms de latência. Na Tabela 4.11 referente ao Cenário 3, para mesma estrutura de rede aplicada em software de simulação, o melhor resultado obtido foi de 0,5873 ms de latência, com taxa de transmissão 2 Mbps no link principal. É possível afirmar que o resultado do Cenário 3 para a seguinte condição: 'Comandos de teleproteção no link principal, com a presença de sinal de dados corporativos', é superior ao Cenário 2 com infraestrutura CISCO, devido aos valores de latência obtidos nos testes que foram comparados.

Tabela 4.13: Teste na rota principal com meio físico, com inserção de tráfego mais comandos de teleproteção - CISCO.

	Comando	Intervalo de confiança (ms)	Latência média (ms)
G.703 2 Mbps	**A**	**5,0164 e 5,0536**	**5,0350**
	B	**5,0085 e 5,0395**	**5,0240**
	C	**4,7459 e 4,7801**	**4,7630**
	D	**4,7158 e 4,7542**	**4,7350**

Fazendo o uso de tecnologia CISCO, para o Cenário 2, realizamos novos testes agora no link secundário com uma taxa de transmissão configurada para 2 Mbps. A Figura 4.16 apresenta o valor médio de latência destacado, sendo este de 4,49 ms, para o link secundário sem tráfego de dados corporativos. Podemos observar na mesma que os valores A, B, C e D ainda estão presentes. Contudo, optamos por trabalhar com o valor médio apresentado pelo software gerador de comandos de teleproteção usado no laboratório físico da CEMIG.

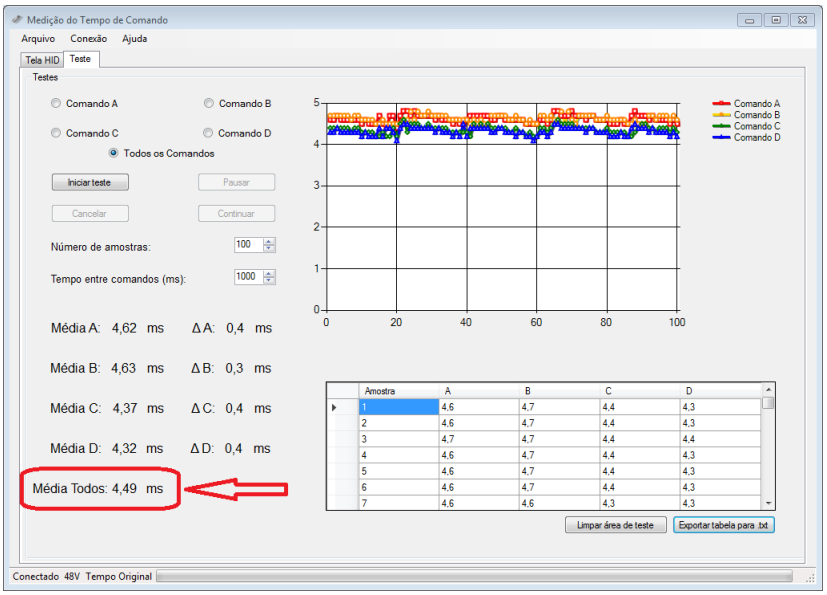

Figura 4.16: Resultado CISCO 2 Mbps no link secundário, sem tráfego de dados corporativos e com comandos de teleproteção.

A Tabela 4.14 apresenta destacado o melhor resultado obtido no Cenário 3, sendo esse de 1,87 ms em uma banda de comunicação de 2 Mbps no enlace secundário. Esse resultado foi obtido no link secundário, sem presença de tráfego de dados corporativos de fundo e com comando de teleproteção. Desta maneira afirmamos que o resultado do Cenário 3 para a seguinte condição: 'Comandos de teleproteção no link secundário, sem a presença de dados corporativos', é superior ao Cenário 2 com estrutura CISCO, devido aos valores de latência obtidos nestes testes.

Tabela 4.14: Tabela com resultados do Cenário 3 para 2 Mbps - Secundário.

Link de Comunicação Secundário					
Tráfego + Comandos de Teleproteção					
Nº do Teste	**Taxa de Tx**	**Vel.Tx/Sem QoS**	**Nº do Teste**	**Taxa de Tx**	**Vel.Tx/Com QoS**
Teste 13	2 Mbps	1,349ms	Teste 16	2 Mbps	1,401
Teste 14	10 Mbps	1,269ms	Teste 17	10 Mbps	1,353ms
Teste 15	100 Mbps	1,348ms	Teste 18	100 Mbps	1,105ms
Comandos de Teleproteção					
Teste 19	2 Mbps	1,87ms	Teste 22	2 Mbps	1,688ms
Teste 20	10 Mbps	1,536ms	Teste 23	10 Mbps	1,78ms
Teste 21	100 Mbps	1,762ms	Teste 24	100 Mbps	1,178ms

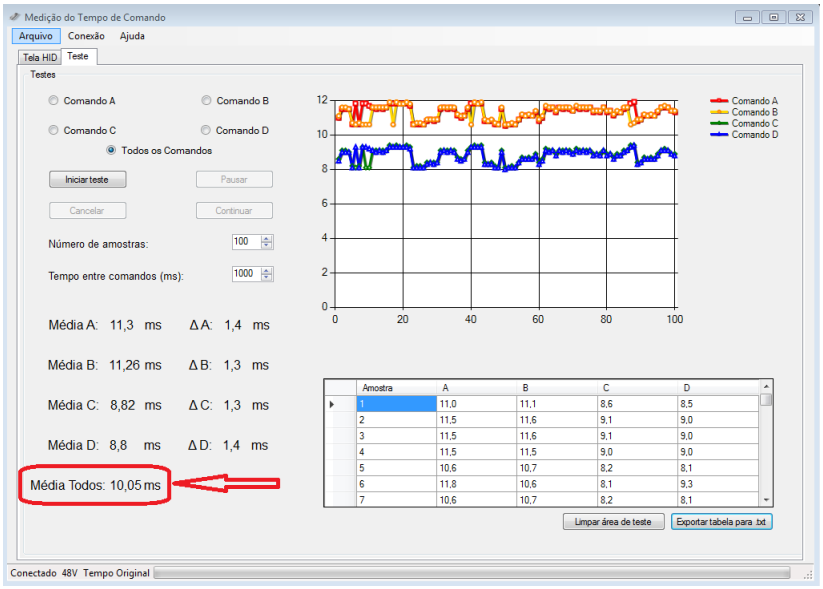

Figura 4.17: Resultado CISCO 2 Mbps no link secundário, com tráfego de dados corporativos e com comandos de teleproteção.

A Figura 4.17 apresenta o resultado no link secundário do Cenário 2, com tráfego de dados corporativos e comandos de teleproteção. O valor médio de latência destacado foi de 10,05 ms. A Tabela 4.15 por sua vez apresenta o melhor valor no link secundário para o Cenário 3, sendo este de 1,34 ms. Esse valor trata do tráfego com presença de dados corporativos e comandos de teleproteção com banda de 2 Mbps no enlace secundário.

Tabela 4.15: Tabela com resultados do Cenário 3 com tráfego corporativo, para uma largura de banda de 2 Mbps no link secundário.

Link de Comunicação Secundário					
Tráfego + Comandos de Teleproteção					
Nº do Teste	**Taxa de Tx**	**Vel.Tx/Sem QoS**	**Nº do Teste**	**Taxa de Tx**	**Vel.Tx/Com QoS**
Teste 13	2 Mbps	1,349ms	Teste 16	2 Mbps	1,401
Teste 14	10 Mbps	1,269ms	Teste 17	10 Mbps	1,353ms
Teste 15	100 Mbps	1,348ms	Teste 18	100 Mbps	1,105ms
Comandos de Teleproteção					
Teste 19	2 Mbps	1,87ms	Teste 22	2 Mbps	1,688ms
Teste 20	10 Mbps	1,536ms	Teste 23	10 Mbps	1,78ms
Teste 21	100 Mbps	1,762ms	Teste 24	100 Mbps	1,178ms

4.4.2 Comparando resultados de cenários - 10 Mbps

Dando continuidade a análise de resultados, a Figura 4.18 e a Figura 4.19 apresentam os resultados obtidos com banda de 10 Mbps no Cenário 2, utilizando equipamentos CISCO. Em ambos os testes, neste caso específico, foram realizados apenas sem a presença de tráfego de dados corporativo de fundo e com a presença de comandos de teleproteção. Este padrão de testes ocorreu tanto para o link principal, quanto no link secundário para o Cenário 2, com 10 Mbps.

Cenário 2 - CISCO 10 Mbps

A Figura 4.18 apresenta o valor médio de latência de 4,44 ms para ida e volta de comandos de teleproteção no link principal do Cenário 2. A Tabela 4.16 por sua vez apresenta destacado o valor de 0,896 ms de latência. Assim foi observado no Cenário 3 que, ao enviarmos comandos de teleproteção no link principal, os resultados foram melhores que os resultados do Cenário 2, o qual possui atraso de propagação devido ao meio físico.

Tabela 4.16: Tabela com resultados do cenário 3 para 10 Mbps - Primário.

Link de Comunicação Principal					
Tráfego + Comandos de Teleproteção					
Nº do Teste	**Taxa de Tx**	**Vel.Tx/Sem QoS**	**Nº do Teste**	**Taxa de Tx**	**Vel.Tx/Com QoS**
Teste 1	2 Mbps	0,5873ms	Teste 4	2 Mbps	0,7235
Teste 2	10 Mbps	0,577ms	Teste 5	2 Mbps	0,6026ms
Teste 3	100 Mbps	0,7323ms	Teste 6	2 Mbps	0,7365ms
Comandos de Teleproteção					
Teste 7	2 Mbps	1,012ms	Teste 10	2 Mbps	0,2071ms
Teste 8	10 Mbps	0,8966ms	Teste 11	2 Mbps	0,9921ms
Teste 9	100 Mbps	1,077ms	Teste 12	2 Mbps	1,25ms

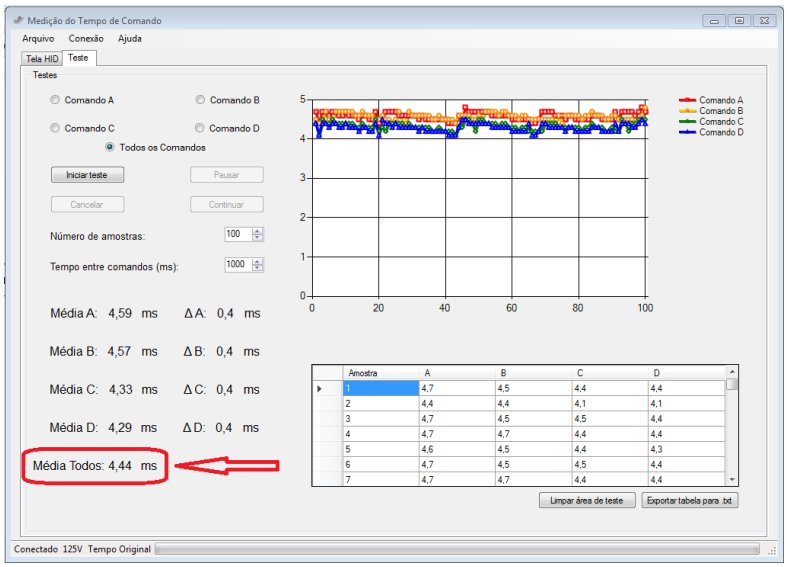

Figura 4.18: Link principal 10 Mbps CISCO

A Figura 4.19 apresenta o valor médio de latência de 4,53 ms no link secundário no cenário 2. A Tabela 4.17 por sua vez apresenta destacado o valor de 1,536 ms. Concluindo desta maneira que o resultado do cenário 3 para a seguinte condição: 'Comandos de teleproteção no link secundário', foi melhor do que o obtido no cenário 2 utilizando estrutura CISCO, fato que deve ao levarmos em conta os atrasos do meio físico.

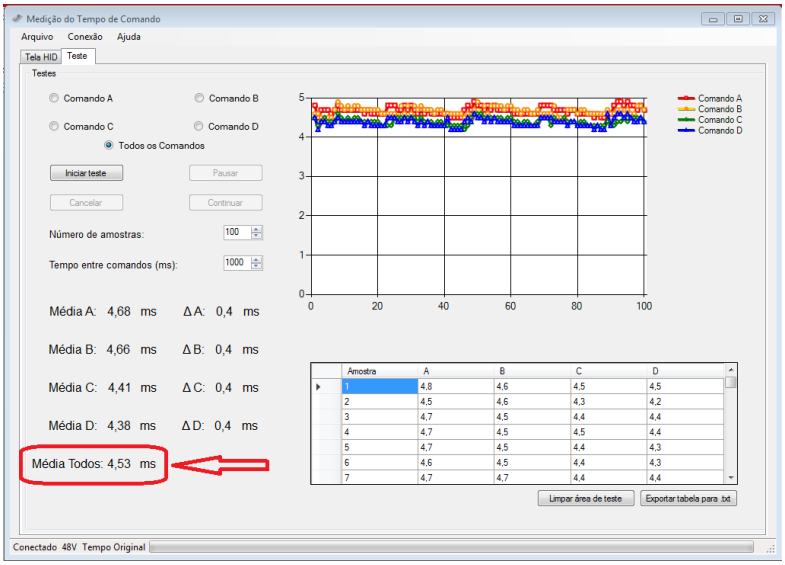

Figura 4.19: Link secundário 10 Mbps CISCO

Tabela 4.17: Tabela com resultados do cenário 3 com tráfego corporativo para 2 Mbps - Secundário.

Link de Comunicação Secundário					
Tráfego + Comandos de Teleproteção					
Nº do Teste	**Taxa de Tx**	**Vel.Tx/Sem QoS**	**Nº do Teste**	**Taxa de Tx**	**Vel.Tx/Com QoS**
Teste 13	2 Mbps	1,349ms	Teste 16	2 Mbps	1,401
Teste 14	10 Mbps	1,269ms	Teste 17	10 Mbps	1,353ms
Teste 15	100 Mbps	1,348ms	Teste 18	100 Mbps	1,105ms
Comandos de Teleproteção					
Teste 19	2 Mbps	1,87ms	Teste 22	2 Mbps	1,688ms
Teste 20	10 Mbps	1,536ms	Teste 23	10 Mbps	1,78ms
Teste 21	100 Mbps	1,762ms	Teste 24	100 Mbps	1,178ms

Cenário 2 - Huawei 10 Mbps

As Figuras 4.20 e 4.21 apresentam os resultados no link principal e link secundário, respectivamente, para 10 Mbps no Cenário 2, agora com tecnologia Huawei. A Figura 4.20 apresenta o valor médio de latência de 5,62 ms no link primário no Cenário 2. Na Tabela 4.16 apresenta o valor de latência 0,896 ms de para link principal de 10 Mbps no Cenário 3. Comparando os dois valores nos respectivos testes, podemos afirmar que o Cenário 3 teve um valor menor para o atraso de ida e volta dos comandos de teleproteção (simulados). Desta forma, podemos observar que o resultado do Cenário 3 para a seguinte condição: 'Comandos de teleproteção no link principal', é superior ao obtido no Cenário 2 com estrutura Huawei para taxa de 10 Mbps, pois atrasos de propagação no meio físico estão presentes no Cenário 2.

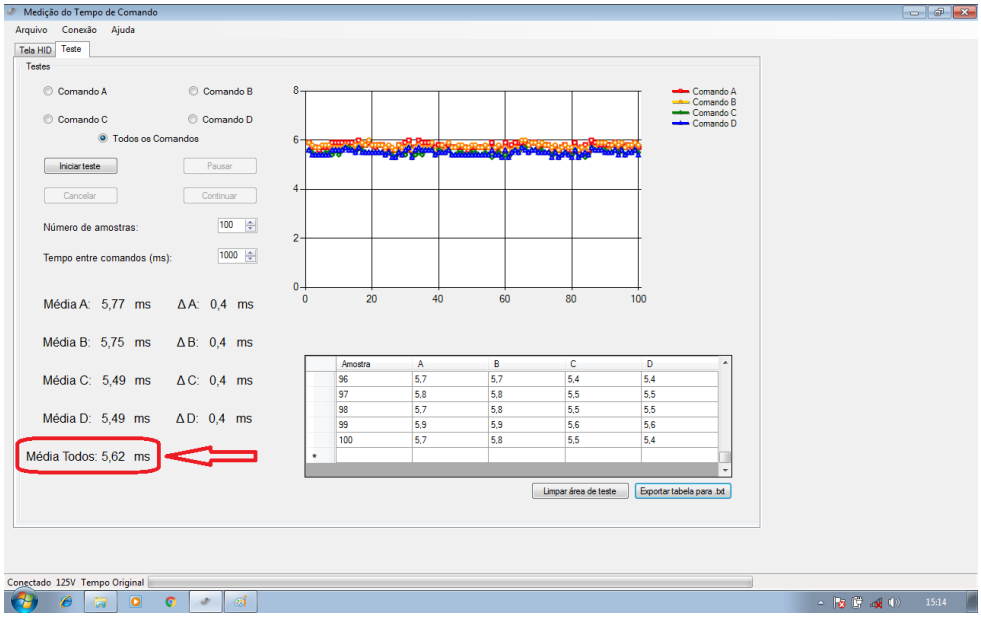

Figura 4.20: Link principal 10 Mbps Huawei.

A figura 4.21 apresenta o resultado no link secundário para taxa de comunicação 10 Mbps no cenário 2, com tecnologia Huawei. Na Tabela 4.15 é possível verificar o resultado no link secundário, para taxa de comunicação de 10 Mbps para o cenário 3, com o valor de 1,536 ms de latência. Comparando os resultados podemos concluir, que o resultado do cenário 3 para a seguinte condição: 'Comandos de teleproteção no link secundário', é superior ao obtido no cenário 2 com estrutura Huawei para taxa de 10 Mbps.

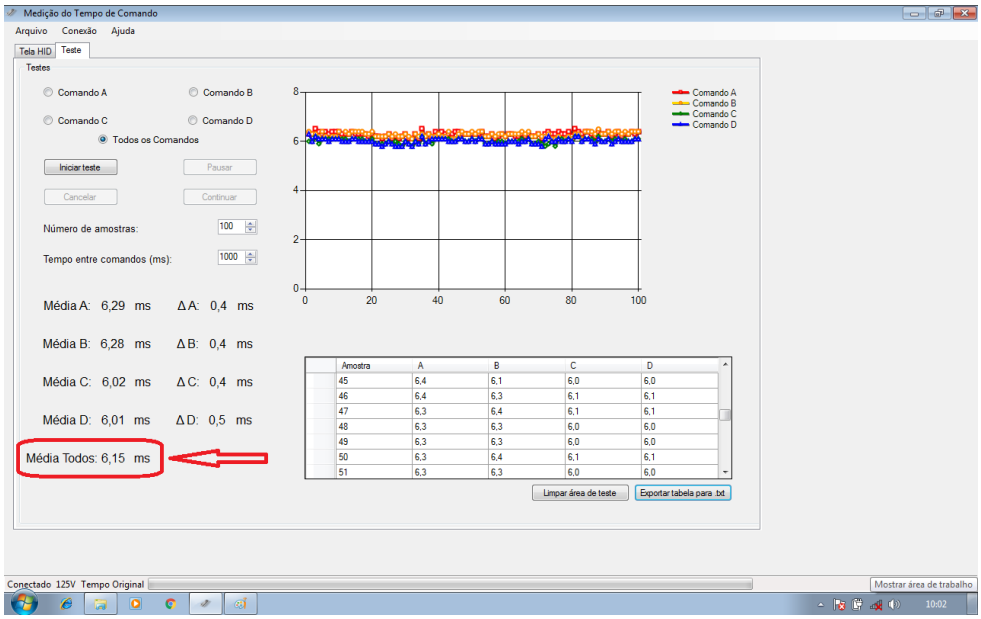

Figura 4.21: Link secundário 10 Mbps Huawei.

4.4.3 Comparando resultados de cenários - 100 Mbps

Apresentamos a seguir os resultados com banda de 100 Mbps no Cenário 2, fazendo uso de tecnologia CISCO. A Figura 4.22 representa o link principal com valor de latência de 4,53 ms para o Cenário 2. A Tabela 4.18 apresenta o resultado do Cenário 3 com valor de latência de 1.077 ms no link principal com banda de 100 Mbps. Ao compararmos os resultados do Cenário 2 com tecnologia CISCO, e Cenário 3, Vemos um desempenho melhor no Cenário 3 devido ao fato de não estar presente no ambiente de simulação, atrasos do meio físico.

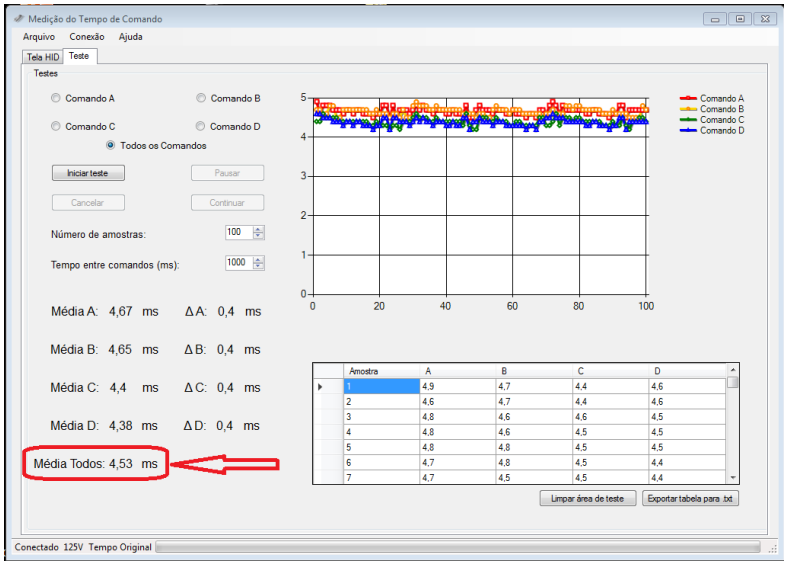

Figura 4.22: Link principal 100 Mbps CISCO.

Tabela 4.18: Tabela com resultados do cenário 3 para 100 Mbps - Primário.

Link de Comunicação Principal					
Tráfego + Comandos de Teleproteção					
Nº do Teste	**Taxa de Tx**	**Vel.Tx/Sem QoS**	**Nº do Teste**	**Taxa de Tx**	**Vel.Tx/Com QoS**
Teste 1	2 Mbps	0,5873ms	Teste 4	2 Mbps	0,7235
Teste 2	10 Mbps	0,577ms	Teste 5	2 Mbps	0,6026ms
Teste 3	100 Mbps	0,7323ms	Teste 6	2 Mbps	0,7365ms
Comandos de Teleproteção					
Teste 7	2 Mbps	1,012ms	Teste 10	2 Mbps	0,2071ms
Teste 8	10 Mbps	0,8966ms	Teste 11	2 Mbps	0,9921ms
Teste 9	100 Mbps	1,077ms	Teste 12	2 Mbps	1,25ms

Apresentamos a seguir os resultados com banda de 100 Mbps no Cenário 2, para o link secundário, fazendo uso de tecnologia CISCO. A Figura 4.19 apresenta taxa de latência de 4,55 ms para o mesmo. A Tabela 4.23 por sua vez, apresenta resultados de latência 1,762 ms para o link secundário e cenário 3, sendo assim, para o link secundário e com envio de comandos de teleproteção, o Cenário 3 foi superior ao Cenário 2 com equipamentos CISCO e taxa de transmissão de 100 Mbps, devido ao fato de ocorrer atrasos de propagação no meio físico.

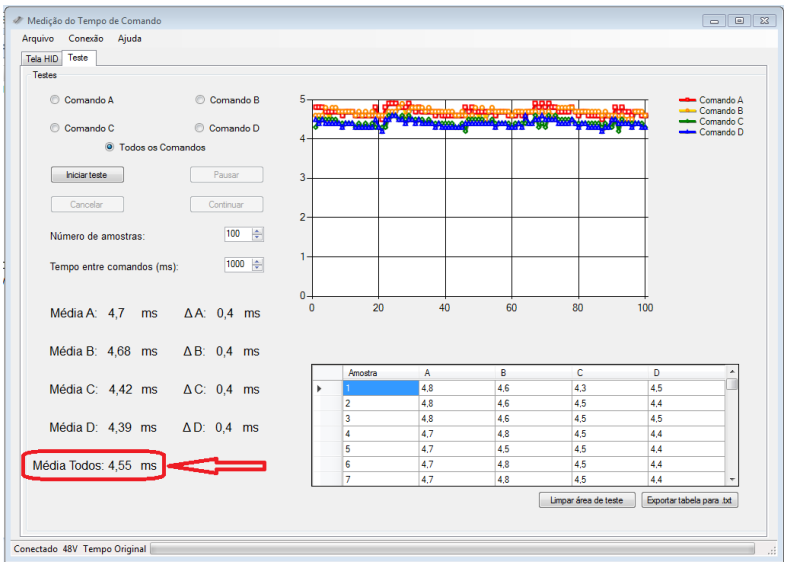

Figura 4.23: Link secundário 100 Mbps CISCO

Tabela 4.19: Tabela com resultados do cenário 3 para 100 Mbps - Secundário.

Link de Comunicação Secundário					
Tráfego + Comandos de Teleproteção					
Nº do Teste	**Taxa de Tx**	**Vel.Tx/Sem QoS**	**Nº do Teste**	**Taxa de Tx**	**Vel.Tx/Com QoS**
Teste 13	2 Mbps	1,349ms	Teste 16	2 Mbps	1,401
Teste 14	10 Mbps	1,269ms	Teste 17	10 Mbps	1,353ms
Teste 15	100 Mbps	1,348ms	Teste 18	100 Mbps	1,105ms
Comandos de Teleproteção					
Teste 19	2 Mbps	1,87ms	Teste 22	2 Mbps	1,688ms
Teste 20	10 Mbps	1,536ms	Teste 23	10 Mbps	1,78ms
Teste 21	100 Mbps	1,762ms	Teste 24	100 Mbps	1,178ms

4.5 Considerações Parciais

Neste capítulo apresentamos os resultados comparativos dos testes que foram realizados no Cenário 2 e no Cenário 3. Foram elaboradas diversas planilhas que abordam os aspectos fundamentais para analisar os resultados e realizar as comparações de valores. Os resultados contemplaram a realização de comparação de resultados obtidos utilizando equipamentos da empresa CISCO, com equipamentos da empresa Huawei, equipamentos estes que operam diretamente conectados com dispositivos que realizam a segurança da rede elétrica. Dentro dos cenários de teste foi possível determinar os valores de melhor tempo médio de resposta para o Cenário 2 e para o Cenário 3.

Foi possível concluir que em todos os testes, o menor resultado de latência foi obtido no Cenário 3. O que nos leva a concluir que independente da largura de banda ser de 2 Mbps,

10 Mbps ou 100 Mbps, o tempo de resposta para comandos de teleproteção, tem seu melhor desempenho aplicado no Cenário 3. Esses resultados foram obtidos e comprovados tanto no *link* principal quanto no *link* secundário, e independente da tecnologia ou Huawei, no Cenário 2.

Dessa maneira a hipótese defendida nesta dissertação, de que o uso de uma ferramenta de simulação pode replicar um cenário real, sendo este, com sistema de teleproteção integrado a rede elétrica de forma eficiente, se mostra eficaz. O uso de protocolos aplicados a comutação de pacotes, vinculados ao TCP/IP e MPLS possibilitaram a comunicação dentro do Cenário 3, replicando estrutura real proposta no Cenário 2 de forma mais fidedigna.

Importante salientar que o uso de ferramentas de simulação/emulação de um cenário físico esta livre de problemas reais como impedância, ruídos, atrasos e intempéries, a qual uma estrutura física em campo, por exemplo, estaria exposta. Desta maneira é natural que os resultados no Cenário 3 se mostrem mais promissores que o Cenário 2. Com os valores obtidos e toda a dificuldade envolvida com o Cenário 2, ficou evidente o ganho que o desenvolvimento deste projeto poderia ter, caso tivesse um simulador/emulador de redes de teleproteção integrado com redes de transmissão de energia.

Capítulo 5

Conclusões

Nesta dissertação podemos concluir através de testes e resultados apresentados, a importância da realização da migração tecnológica em sistemas de teleproteção legados, para sistemas dotados de novas tecnologias.

No decorrer desta dissertação foram citados trabalhos relacionados ao tema, tendo foco em apresentar soluções para melhoria de serviços de redes de telecomunicações, voltadas para redes de teleproteção, em redes de distribuição de energia elétrica. Dentre os artigos estudados concluímos que, suas publicações estavam devidamente atualizadas (entre 2017 a 2021) e nenhum artigo ou trabalho pesquisado fez menção ao estudo de *software* para simulação, de redes com teleproteção da mesma forma que abordamos nessa dissertação, com o mesmo nível de resultados e/ou profundidade que este trabalho apresenta até onde sabemos.

Alguns desses trabalhos apontaram soluções utilizando tecnologias como: MPLS, Smart Grid e até tratamento de pacotes (datagramas) voltados à teleproteção. Através da configuração do software de simulação, implementação de cenários e resultados obtidos, foi possível confirmar a possibilidade de uso da tecnologia MPLS, em redes voltadas para teleproteção.

Entendemos que a 'migração tecnológica' das atuais redes de telecomunicações voltadas para serviços de teleproteção de redes de energia elétrica é um processo em continuo desenvolvimento. Foi possível observar com esta dissertação que o uso de técnicas de comutação de circuitos, para comutação de pacotes é uma prática que vem aumentando em diferentes trabalhos.

Comprovamos durante o processo de análise de resultados da dissertação, que os atrasos no cenário 2 estão dentro do limite desejado, tanto para CISCO, quanto para Huawei. Podemos afirmar baseado nestes resultados que o simulador utilizado é capaz de replicar com confiabilidade os valores obtidos no cenário 2. Isso se torna possível uma vez que os resultados encontram-se na mesma ordem de grandeza.

É possível afirmar que o conjunto de protocolos do cenário 3, se assemelha quase que na totalidade com o cenário 2, diferenciando apenas a ausência de clock externo e o protocolo para teleproteção de cada fabricante (CISCO e Huawei) para o cenário 3. Por fim, podemos concluir que é valido o uso de um software de simulação para construção do cenário 3.

Observamos que o software se comporta como um simulador de rede, contudo existem características especificas de protocolos e configurações no mesmo, capazes de emular o comportamento de determinados equipamentos da rede de teleproteção e redes de energia.

Desta forma, deixamos claro que a principal contribuição deste trabalho vem na forma de confirmação do uso benéfico de simulador aplicado a sistemas de teleproteção. Essa contribuição é sustentada pelos resultados obtidos no cenário 3 em comparação com os resultados do cenário 2.

Podemos observar que há uma equivalência de resultados para uso de redes simuladas se comparada a rede física. Essa equivalência de redes não se restringe aos resultados de testes, mas é observada no processo de configuração dos cenários 2 e 3. O conjunto de protocolos

do cenário 3 se assemelha quase que na totalidade com o cenário 2. A principal diferença está apenas na ausência de *clock* externo e protocolos de teleproteção que são fornecidos pela CISCO e/ou Huawei.

Concluímos no decorrer dos testes que alguns *softwares* infelizmente não apresentaram uma resposta desejada durante os experimentos. Dentre eles, foi visto o software da Huawei eNSP, que é um simulador de redes de telecomunicações, contudo, em comparação ao GNS3, acabou sendo descartado devido a sua limitação de recursos, e atualmente foi descontinuado.

A fim de provar nossa hipótese que o uso de um software simulador facilita o processo de criação e gestão de redes com serviços de teleproteção em redes elétricas, foi proposto um modelo de arquitetura de rede com topologia em anel, em diferentes cenários. Os principais experimentos foram realizados no cenário físico (Cenário 2) e o cenário de simulação/emulação (Cenário 3). Estes foram dotados de um enlace de comunicação principal e outro enlace de comunicação secundária.

Foram realizados diversos testes comparando o Cenário 2 (físico) com o Cenário 3 (simulado/emulado). Estes testes envolveram uso de tecnologias distintas, como CISCO e Huawei, na construção do Cenário 2. Também foi feito o uso de diferentes taxas de transmissão, sendo essas de 2 Mbps, 10 Mbps e 100 Mbps. Concluímos através de análises de resultados que o Cenário 3 (simulador GNS3 - CISCO) obteve resultados simulares ao experimentados em campo, com resultados ligeiramente melhores em todos os resultados comparativos, no link principal e no link secundário. Assim sendo, podemos afirmar que a praticidade na construção de cenários e a integração de ferramentas oferecidas pelo simulador GNS3 é satisfatória para estudos similares. As pilhas de protocolos e os componentes de rede são semelhantes.

Podemos afirmar que a utilização de *software* de simulação pode replicar situações em cenários reais, bem como sua estrutura utilizada, de tal forma a obter melhores resultados nos testes de transmissão envolvendo teleproteção. Desta forma é possível concluir que o uso de software simulador é comprovadamente eficiente no auxilio de construção de cenários e desenvolvimento de ferramentas. Portanto, é possível obter redução de custos na análise de desempenho de redes elétricas com sistemas de teleproteção, bem como melhorar o planejamento de estruturas de redes de teleproteção como um todo, sem custo de aquisição de software ou hardware.

É possível concluir que o uso de ferramentas de simulação podem auxiliar na integração das equipes envolvidas nos projetos de manutenção e planejamento deste tipo de rede. O planejamento de relés utilizados em redes de teleproteção, se bem aplicado, com o software de simulação, pode gerar economia de custos em todo o projeto principalmente no que diz respeito, nas maletas de testes utilizadas por empresas como a CEMIG, para estudos em laboratório.

Por fim, esta dissertação confirma a viabilidade do uso de software de simulação em projetos de desenvolvimento e gestão de redes de teleproteção e rede elétricas, contribuindo diretamente para o avanço científico dentro desta área. A necessidade de pesquisas bem sucedidas para melhoria da estrutura de rede elétrica em todo pais, não só é importante, como se faz necessária para o continuo avanço da pesquisa e da industria dentro do cenário nacional.

5.1 Contribuições

Comprovamos com esse trabalho de dissertação a necessidade de um *software* de simulação para realizar implementação de projeto de redes elétricas com sistema de teleproteção. Dentre as principais contribuições podemos citar que com o desenvolvimento do projeto D0640 “Modelo de Referência para a Rede Operacional de Dados da CEMIG, financiado pela FAPEMIG/CEMIG”, houve um avanço concreto na área de pesquisa científica voltada para redes e sistemas de teleproteção em rede elétrica de sub-estações.

No contexto do projeto CEMIG foram desenvolvidas três dissertações, cada uma com seu cenário de atuação específico dentro dessa área de estudo. Os trabalhos (além desse) foram, respectivamente: (i) *IoT-based Energy Monitoring Flexible Solution: A New Smart Energy Meter*; (ii) Avaliação de Tecnologias Estatísticas para Serviços de Teleproteção; e (iii) Análise

de Desempenho de Redes de Teleproteção de Sistemas de Distribuição de Energia utilizando Simulação e Emulação. Ainda, ligados a pesquisa dessa dissertação (direta ou indiretamente) bem como ao "projeto CEMIG", podemos citar as seguintes publicações:

- *Control Networks and Smart Grid Teleprotection: Key Aspects, Technologies, Protocols and Case-Studies*. Autores: L. F. F. de Almeida, José Rodrigo dos Santos, Luiz Augusto Melo Pereira, Arismar Cerqueira Sodré, Luciano Leonel Mendes, Joel J. P. C. Rodrigues, Ricardo A. L. Rabelo e Antonio Marcos Alberti. Data da publicação: 18 de setembro de 2020.
- *Challenges in the Migration to Packet Switched Networks for Teleprotection Service of Power Transmission Lines*. Autores: L. H. M. Leite, R. A. Fernandes, L. F. F. de Almeida, A. M. Alberti, S. H. Souza, J. R. dos Santos. Data da publicação: 2020.
- Análise de Redes de Dados Estatísticas para Teleproteção de Linhas de Transmissão de Energia. Autores: L. F. F. de Almeida, L. H. M. Leite, R. A. Fernandes, J. R. dos Santos, R. J. Machado, W. R. Silva, J. J. P. C. Rodrigues e A. M. Alberti. Data da publicação: 14 de fevereiro de 2021.
- *Energy Meters Evolution in Smart Grids: A Review*. Autores: Danielly B. Avancini, Joel J. P. C. Rodrigues, Simion G. B. Martins, Ricardo A. L. Rabêlo, Jalal Al-Muhtadi, Petar Solic. Data da publicação: 20 de abril de 2019.
- *A Flexible IoT Energy Monitoring Meter*. Autores: Danielly B. Avancini, Simion G. B. Martins, Ricardo A. L. Rabelo, Petar Solic, Joel J. P. C. Rodrigues. Data da publicação: 30 de agosto de 2018.
- *A New IoT-based Smart Energy Meter for Smart Grid*. Autores: Danielly B. Avancini, Joel J. P. C. Rodrigues, Ricardo A. L. Rabêlo, Ashok K. Das, Sergey Kozloz, Petar Solic. Data da publicação: 03 de fevereiro de 2021.

5.1.1 Trabalhos Futuros

Como proposta para trabalhos futuros, podemos citar:

- Experimentação com novos *softwares* de simulação da Cisco, novas imagens de roteadores, com outras topologias, fazendo uso desses sistemas e comparando com outros existentes. Dessa forma, realizar uma análise e avaliação de desempenho de *softwares* voltados para simulação de redes para sistemas de teleproteção;
- Trabalhar no desenvolvimento de *software* capaz de implementar as funções dos relés e aceitar novos módulos de proteção. Dessa forma, diversificar testes visando o ganho de desempenho ao se projetar novos cenários para sistemas de teleproteção, bem como reduzir custos com estrutura de rede;
- Usar a arquitetura NovaGenesis (arquitetura de Internet do futuro), juntamente com *software* de simulação de teleproteção para testes envolvendo controle e projeto da redes elétricas;
- Fazer uso de plataformas de orquestração de serviços como Kubernetes para simular redes maiores e com mais recursos de flexibilidade e gestão. Dessa forma, possibilitar a criação dinâmica de novos cenários de teste com redes elétricas utilizando sistemas de teleproteção.

Referências Bibliográficas

[1] S. T. Collier, "Steps to a smarter grid," in *Rural E lectric Power Conference*, 2009.

[2] C. R. E. Inteligentes, "Contexto nacional," *Centro de Gestão e Estudos Estratégicos*, vol. 16, p. 172, 2012.

[3] G. F. Santos and A. G. Ghirardi, "Evolução estrutural da indústria de energia elétrica: o segmento de distribuição na região nordeste," *Organizações & Sociedade*, vol. 10, no. 27, pp. 93–110, 2003.

[4] B. Hamilton and M. Summy, "Benefits of the smart grid [in my view]," *IEEE Power and Energy Magazine*, vol. 9, no. 1, pp. 104–102, 2010.

[5] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, "Smart grid communication: Its challenges and opportunities," *IEEE transactions on Smart Grid*, vol. 4, no. 1, pp. 36–46, 2013.

[6] L. A. M. P. . A. C. S. J. . L. L. M. . J. J. P. C. R. . . F. I. R. A. L. R. . M. I. LUIZ FELIPE FERNANDES DE ALMEIDA1, JOSÉ RODRIGO DOS SANTOS1 and A. M. A. 1, "Control networks and smart grid teleprotection:key aspects, technologies, protocols, and case-studies," *IEEE Access, 2020.3025235*, vol. 8, pp. 1–31, 2020.

[7] F. C. da Silva, A. F. Bergamasco, and L. L. Vendite, "Modelos de simulação para análise e apoio à decisão em agrossistemas," 2004.

[8] F. EDITION, "Discrete-event system simulation."

[9] S. Roesler and R. Lobo, "Proving viability of line current differential over packet switched networks," in *2014 67th Annual Conference for Protective Relay Engineers*. IEEE, 2014, pp. 542–551.

[10] "Getting started with gns3," https://www.nsnam.org/, accessed: 2019-05-30.

[11] A. N. de Energia Elétrica. (2020, Oct.) Regulação dos serviços de distribuição. [Online]. Available: https://www.aneel.gov.br/regulacao-dos-servicos-de-distribuicao

[12] M. da Elétrica. (2020, Oct.) Redes de energia elétrica, tipos e características. [Online]. Available: https://www.mundodaeletrica.com.br/redes-de-energia-eletrica-tipos-e-caracteristicas/

[13] P. RUSH, "Proteção e automação de redes-conceito e aplicação," *Coordenação da tradução–José Antonio Jardini. Editora Blucher: Schneider*, 2011.

[14] X. Zhang, Y. Song, and L. Lu, "Time division multiplexing optical time domain reflectometry based on dual frequency probe," *IEEE Photonics Technology Letters*, vol. 24, no. 22, pp. 2005–2008, 2012.

[15] W. Huang, "Learn iec 61850 configuration in 30 minutes," in *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*, March 2018, pp. 1–5.

[16] MathWorks. (2020, Oct.) The origins of matlab. [Online]. Available: https://www.mathworks.com/company/newsletters/articles/the-origins-of-matlab.html

[17] W. Li, X. Zhang, and H. Li, "Co-simulation platforms for co-design of networked control systems: An overview," *Control Engineering Practice*, vol. 23, pp. 44–56, 2014.

[18] "Riverbed modeler: A suite of protocols and technologies with a sophisticated development environment," https://www.riverbed.com/products/steelcentral/steelcentral-riverbed-modeler.html, accessed: 2019-04-22.

[19] S. D. Anton, D. Fraunholz, D. Krummacker, C. Fischer, M. Karrenbauer, and H. D. Schotten, "The dos and don'ts of industrial network simulation: A field report," in *Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control*. ACM, 2018, p. 6.

[20] B. Fortz and M. Thorup, "Optimizing ospf/is-is weights in a changing world," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 4, pp. 756–767, 2002.

[21] S. T. Radhakrishnan and S. R. Mohanty, "Egress engineering over bgp label unicast in mpls-based networks," in *2021 IEEE International Conference on Networking, Architecture and Storage (NAS)*, 2021, pp. 1–4.

[22] R. Veisllari and S. Bjørnstad, "Employing ethernet spanning tree protocols in an integrated hybrid optical network," in *2011 13th International Conference on Transparent Optical Networks*, 2011, pp. 1–4.

[23] "Mpls core — principais conceitos em service provider," https://medium.com/techrebels/https-medium-com-ra-silva-mpls-core-principais-conceitos-em-service-provider-6a6b5300add0, accessed: 2020-11-23.

[24] "Multi-protocol label switching," https://www.gta.ufrj.br/ensino/eel879/vf/mpls/, accessed: 2020-11-23.

[25] "Redes mpls," https://wiki.sj.ifsc.edu.br/wiki/index.php/Redes_MPLS, accessed: 2020-11-23.

[26] J. L. Marzo, E. Calle, C. Scoglio, and T. Anjah, "Qos online routing and mpls multilevel protection: a survey," *IEEE Communications Magazine*, vol. 41, no. 10, pp. 126–132, 2003.

[27] M. Portnoi and J. Martins, "Cr-ldp: Aspectos e funcionamento," 06 2005.

[28] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, "Resource reservation protocol:(rsvp); version 1 functional specification," 1997.

[29] C. M. Pedroso, W. Godoy, and C. A. Bastos, "Integração em inter-redes ip utilizando rsvp sobre atm," *SENACITEL, Chile, Agosto de*, 1998.

[30] V. Veselỳ and T. Rajca, "Discovering neighbor devices in computer network: Development of cdp and lldp simulation modules for omnet++," *arXiv preprint arXiv:1709.02209*, 2017.

[31] W. P. d. Silva, "Ipv6 em redes mpls," 2013.

[32] "Máxima taxa de transmissão," https://srivatsp.com/ostinato/ostinato-ubuntu-maximum-transmit-rate/, accessed: 2020-12-22.

[33] B. R. Patil, M. Moharir, P. K. Mohanty, G. Shobha, and S. Sajeev, "Ostinato-a powerful traffic generator," in *2017 2nd International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS)*. IEEE, 2017, pp. 1–5.

[34] "Sistema operacional tinycore linux," http://tinycorelinux.net/welcome.html, accessed: 2020-12-22.

[35] S. PremKumar and V. Saminadan, "Performance evaluation of smart grid communication network using mpls," *International Conference on Communication and Signal Processing, April 6-8, 2017, India*, pp. 2116–2120, 2017.

[36] I. MD SHAHIN ALAM, (Student Member and I. SEYED ALI AREFIFAR, (Senior Member, "Simulation study of qos guaranteed atm transmission for future power system communication," *IEEE Access,2019.2927303*, vol. 7, pp. 1–23, 2019.

[37] E. E. T. C. E. Mohamed H. A. Hamied, "Performance evaluation of ami communication network using ospf routing protocol and wan technologies," *International Conference on Computing and Information Technology, University of Tabuk, Kingdom of Saudi Arabia.*, no. 2, pp. 72 – 76, 9th 1 0 Sep. 2020, 2020.

[38] M. D. b. H. M. e. a. Rahman Dashti a, **, "A survey of fault prediction and location methods in electrical energy distribution networks," *ScienceDirect - Published by Elsevier Ltd*, vol. 184, pp. 1 – 30, Agosto. 2021, 2021.

[39] L. A. e. a. L.H.M.Leite, R.A.Fernandes, "Challenges in the migration to packet switched networks for teleprotection service of power transmission lines," *CIGRE SESSION 48*, vol. D2-301, no. 2, p. 1 á 13. Paris 2020, 2020.

[40] L. F. F. de Almeida, "Avaliação de tecnologias estatísticas para serviços de teleproteção." *INATEL, Dissertação para obtenção do Título de Mestre em Engenharia de Telecomunicações*, pp. 1–131, 2020.

[41] N. Dorsch, H. Georg, and C. Wietfeld, "Analysing the real-time-capability of wide area communication in smart grids," in *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2014, pp. 682–687.

[42] "Micro sistema operacional," http://tinycorelinux.net/, accessed: 2020-12-22.

[43] "Gerador de tráfego ostinato," https://ostinato.org/, accessed: 2020-12-09.

Apêndice A

Anexo 1 - Testes no simulador

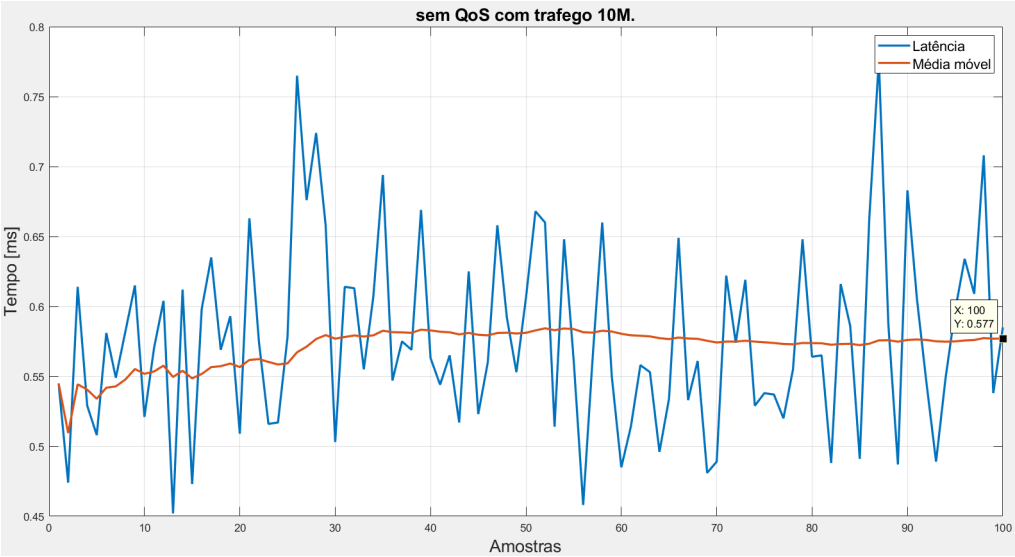

Figura A.1: Teste 2.

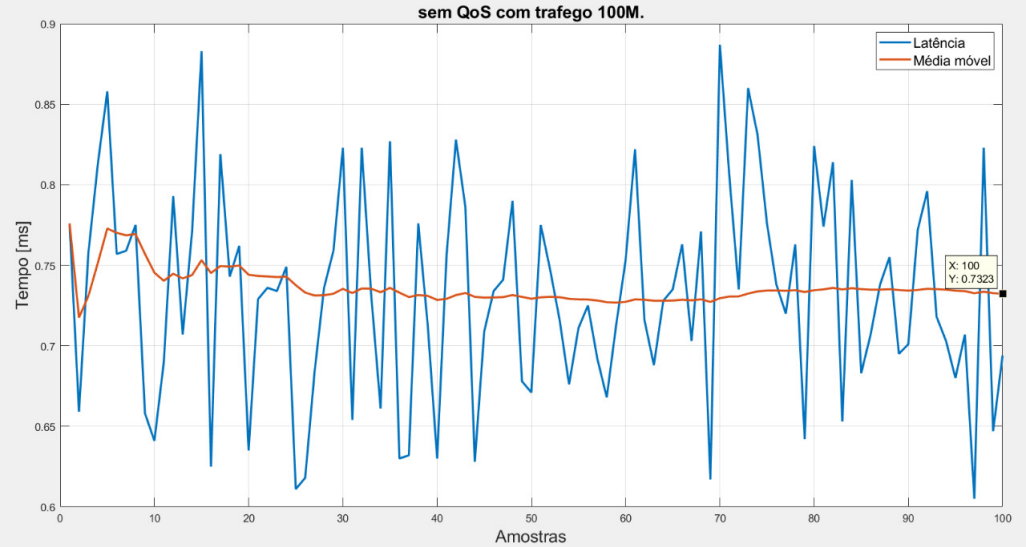

Figura A.2: Teste 3.

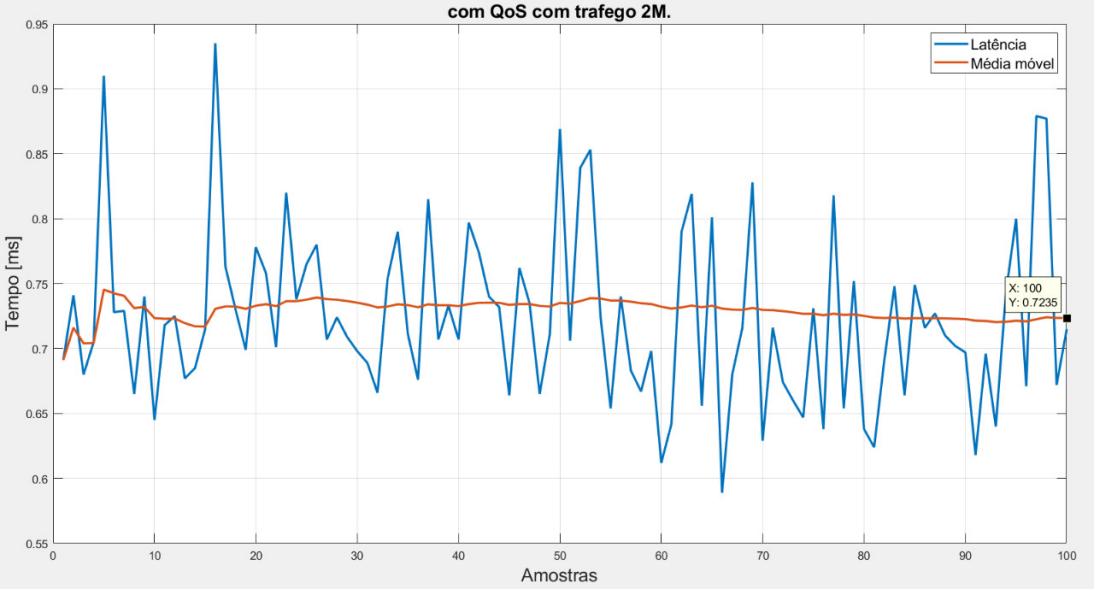

Figura A.3: Teste 4.

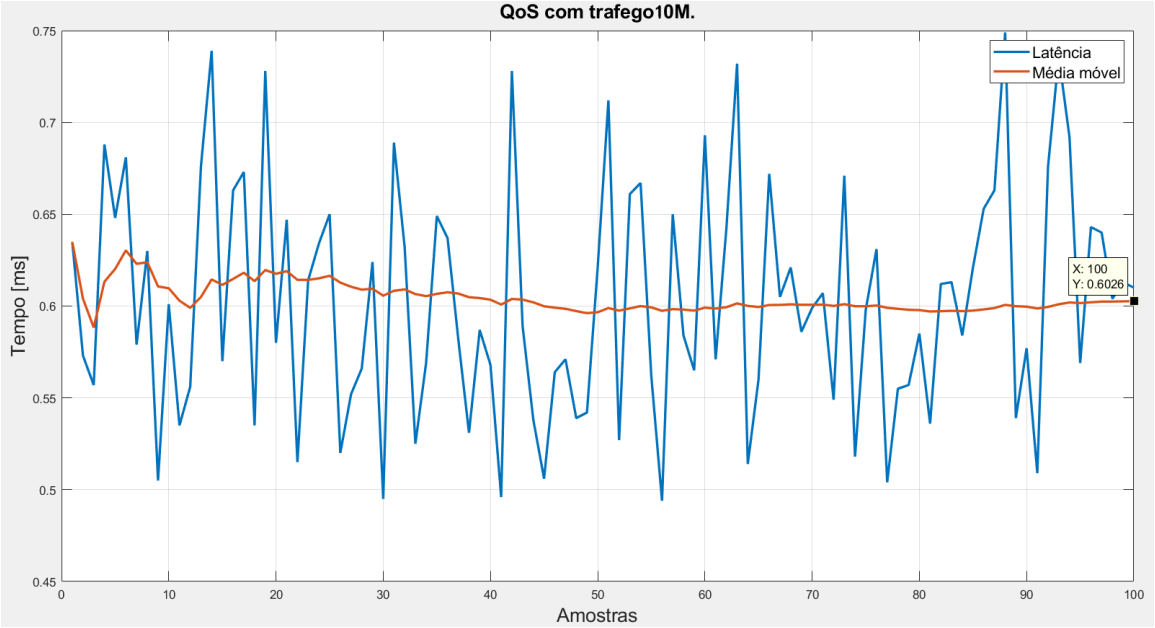

Figura A.4: Teste 5.

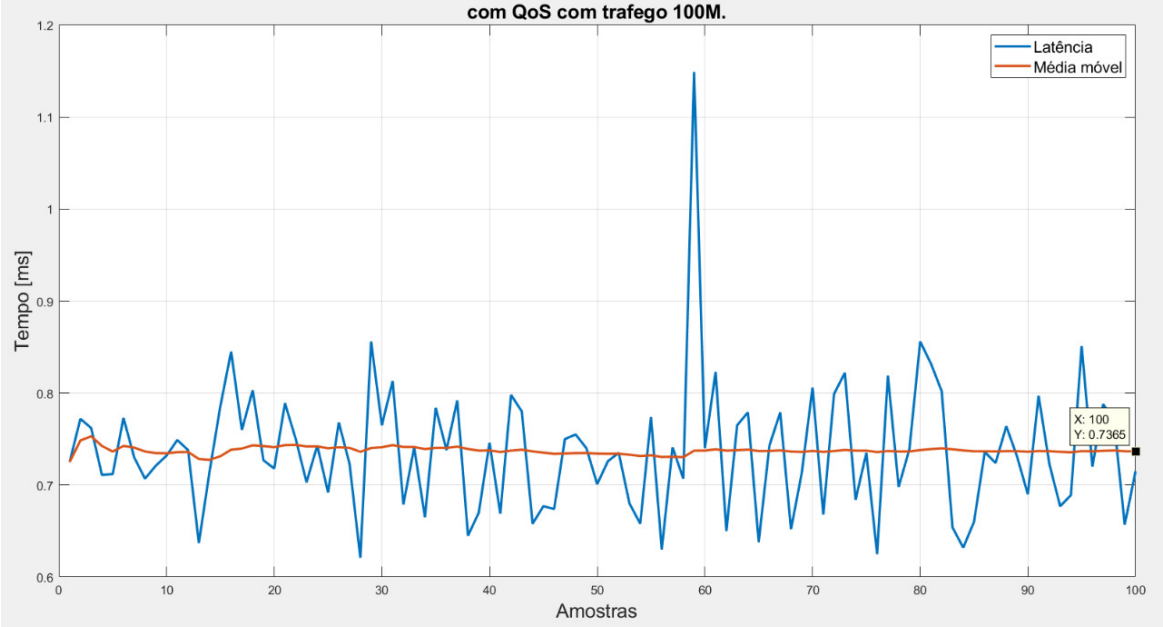

Figura A.5: Teste 6.

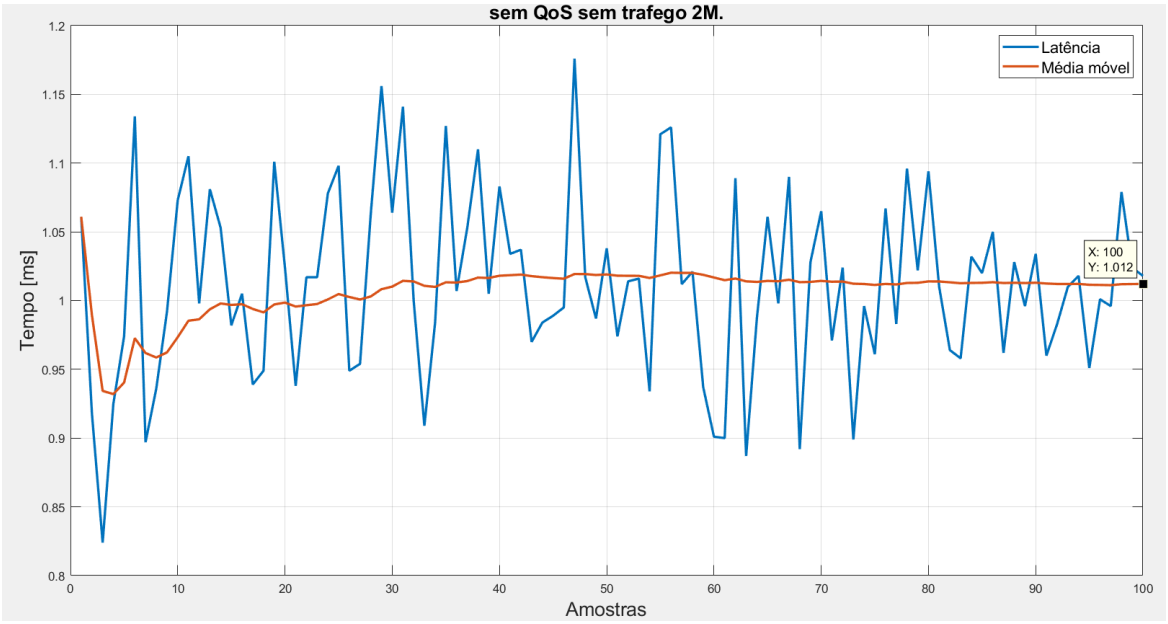

Figura A.6: Teste 7.

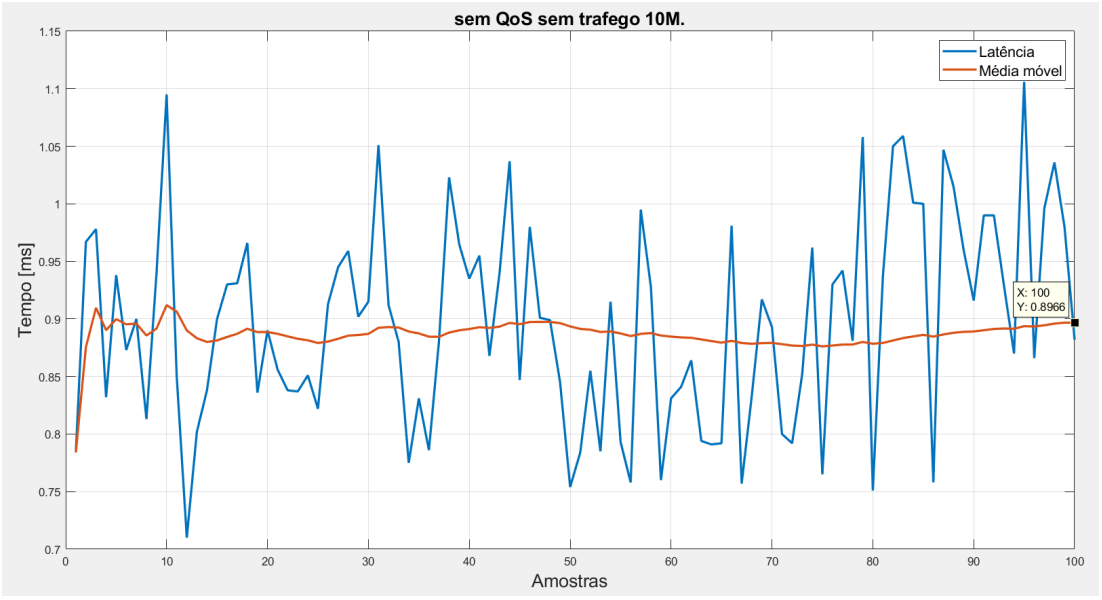

Figura A.7: Teste 8.

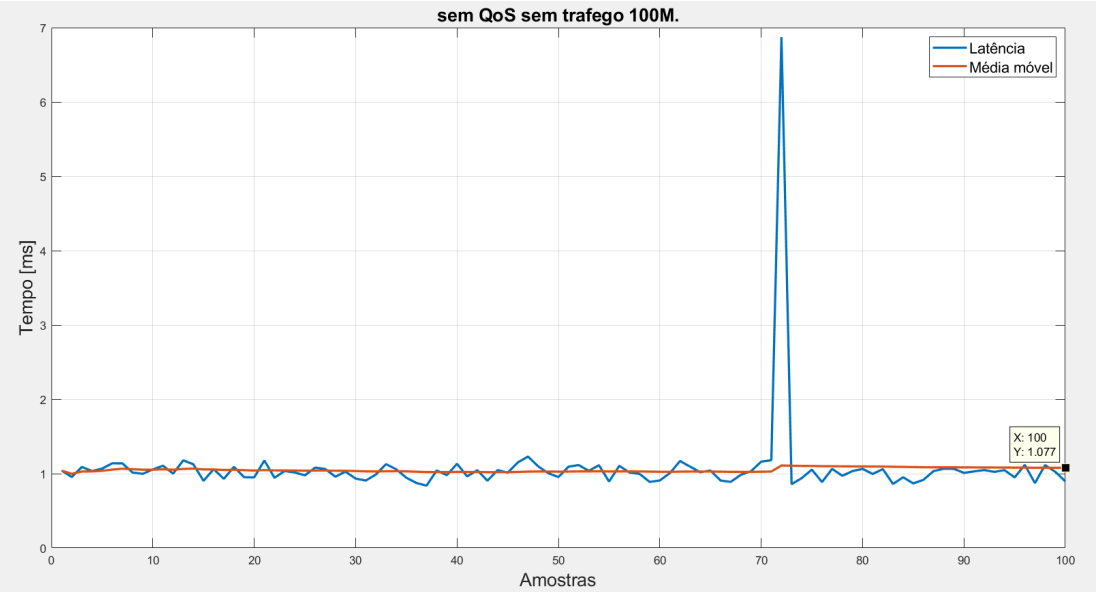

Figura A.8: Teste 9.

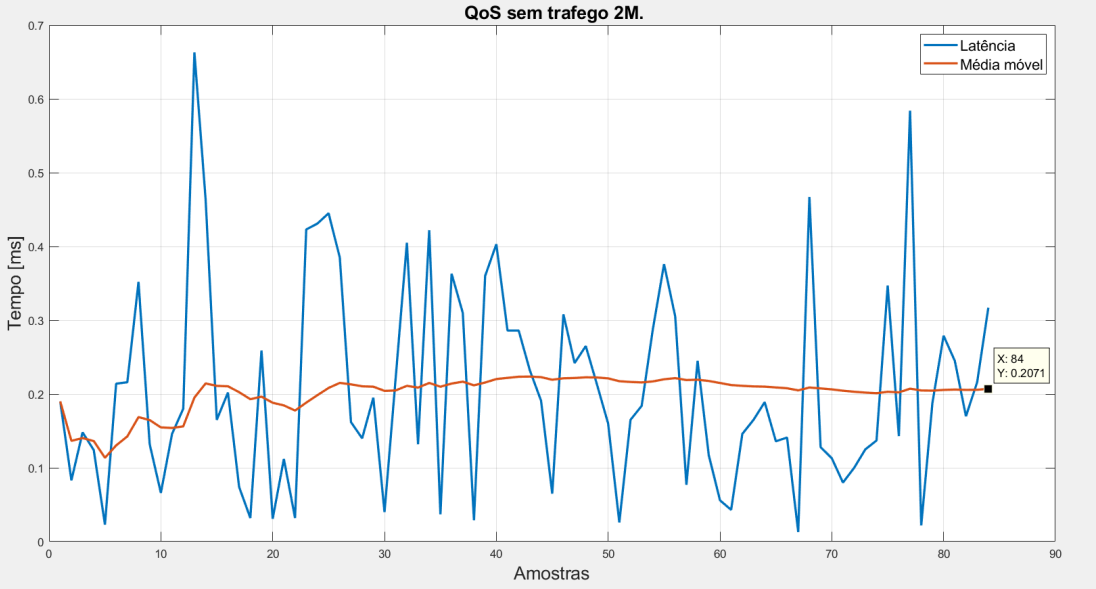

Figura A.9: Teste 10.

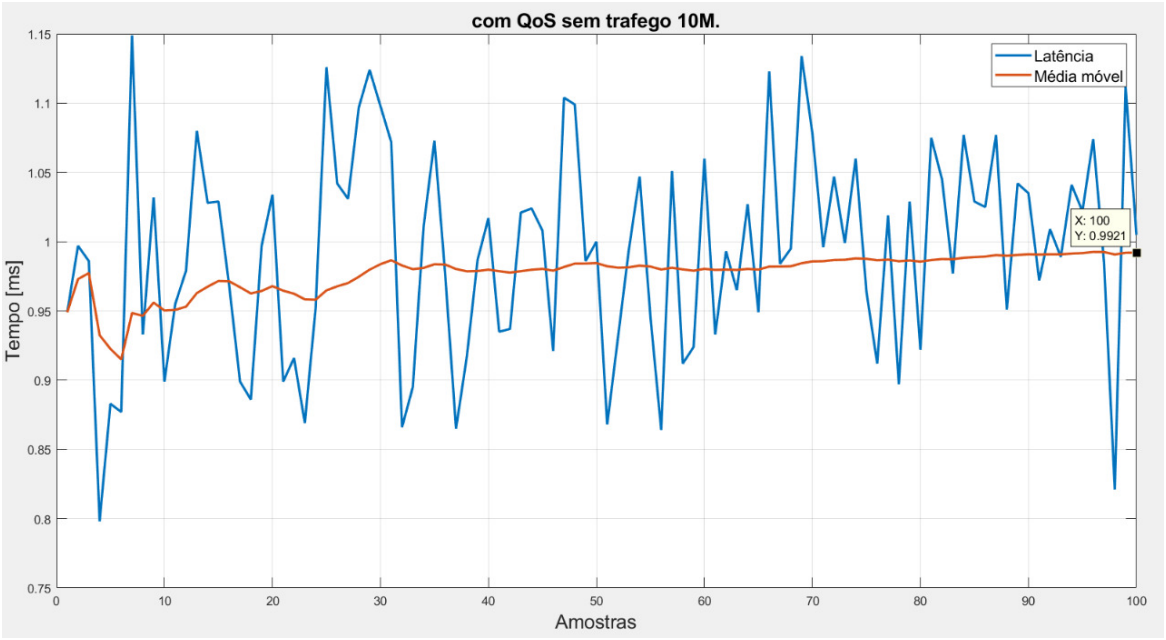

Figura A.10: Teste 11.

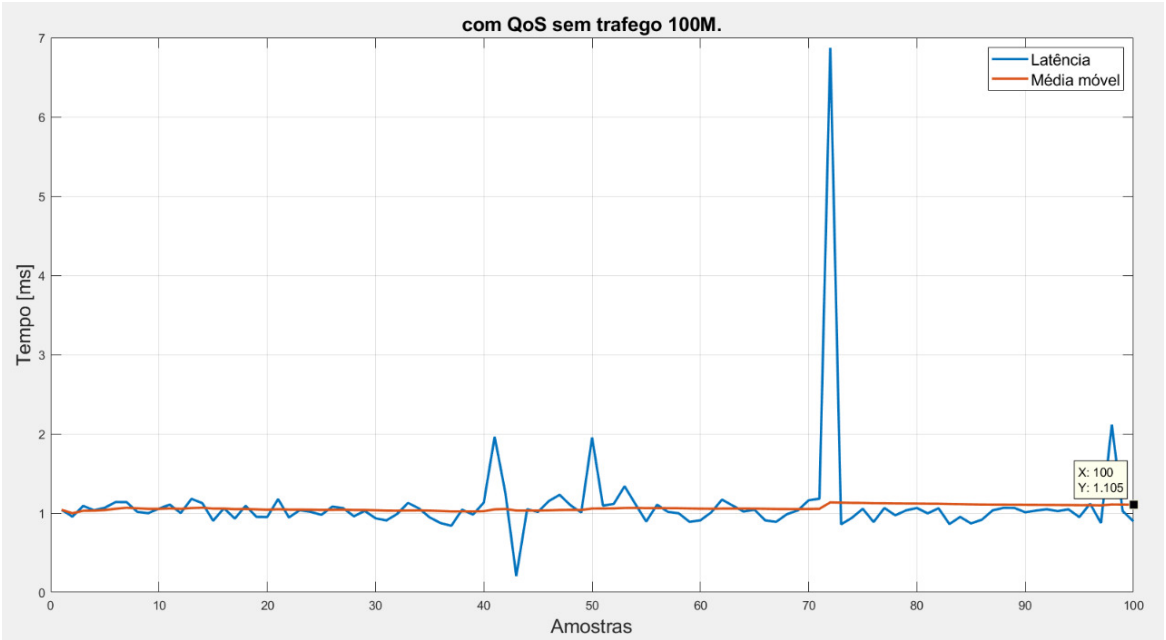

Figura A.11: Teste 12.

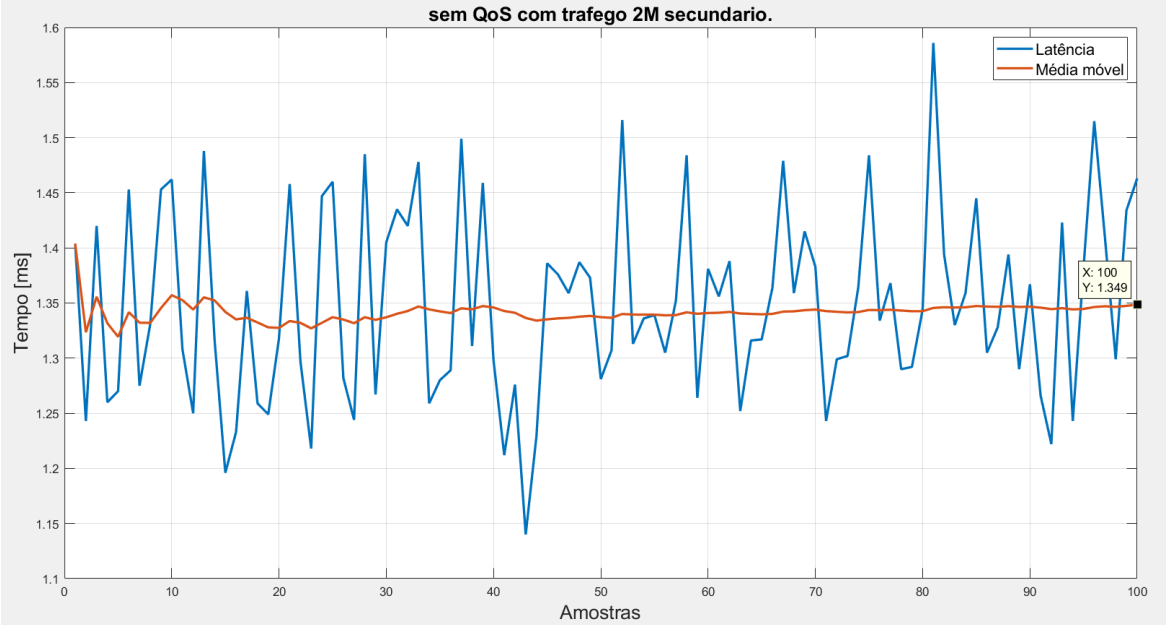

Figura A.12: Teste 13.

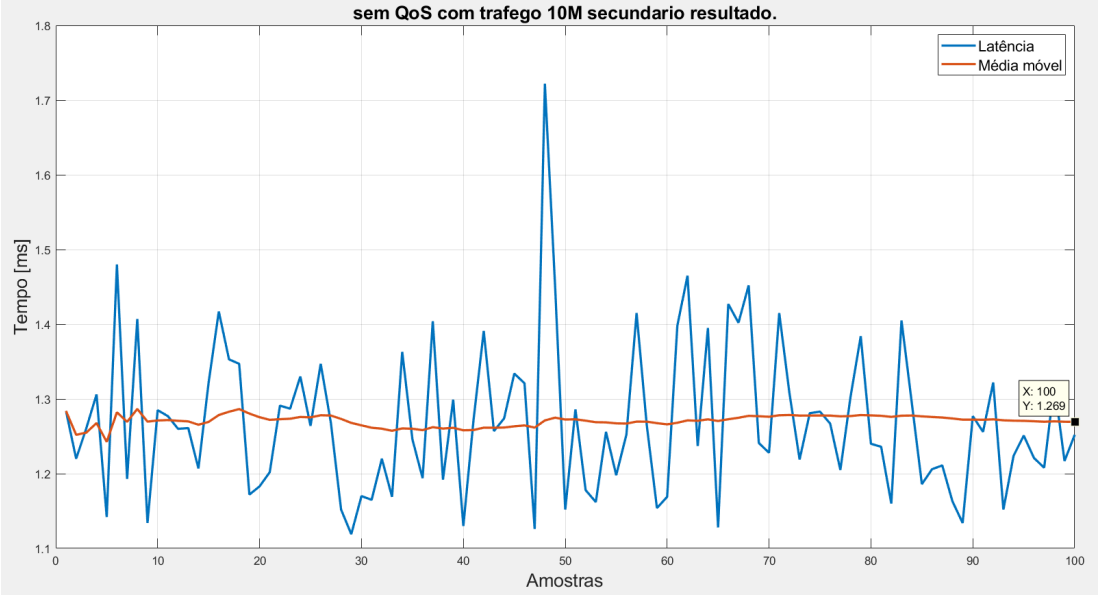

Figura A.13: Teste 14.

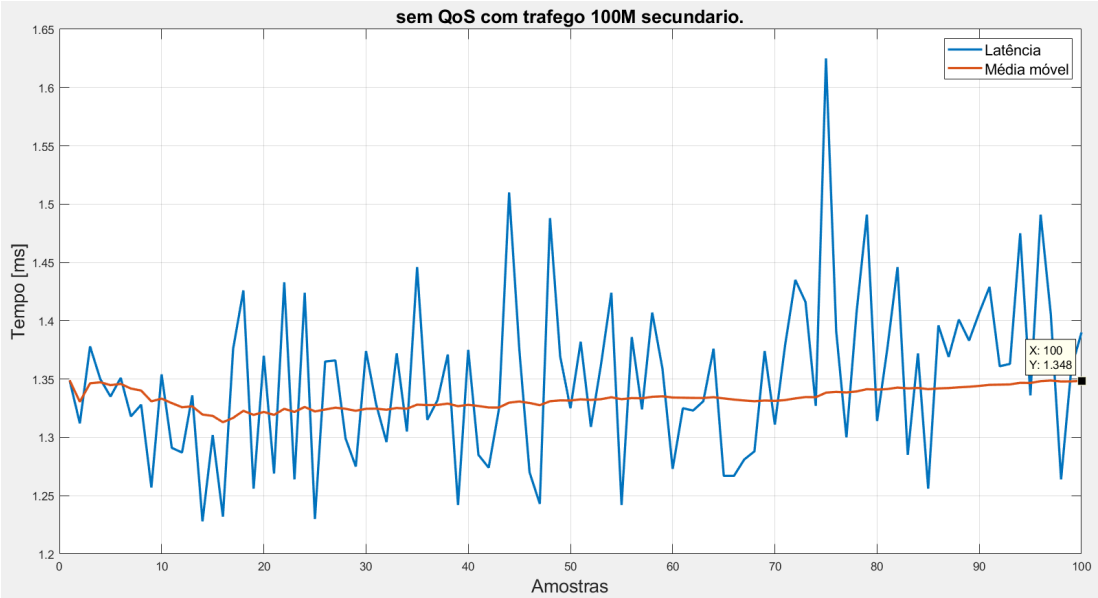

Figura A.14: Teste 15.

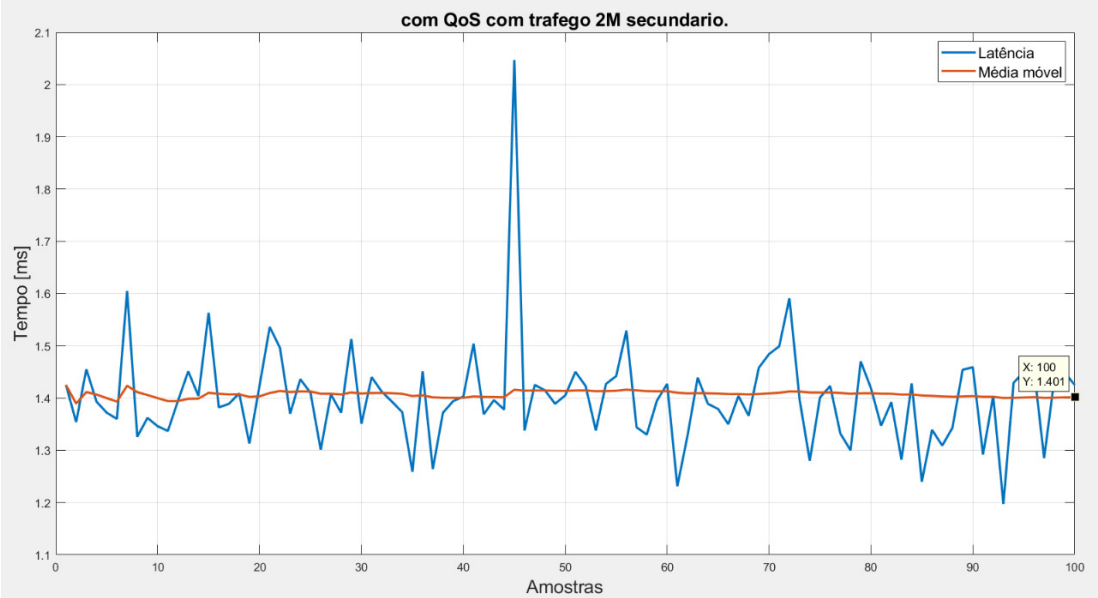

Figura A.15: Teste 16.

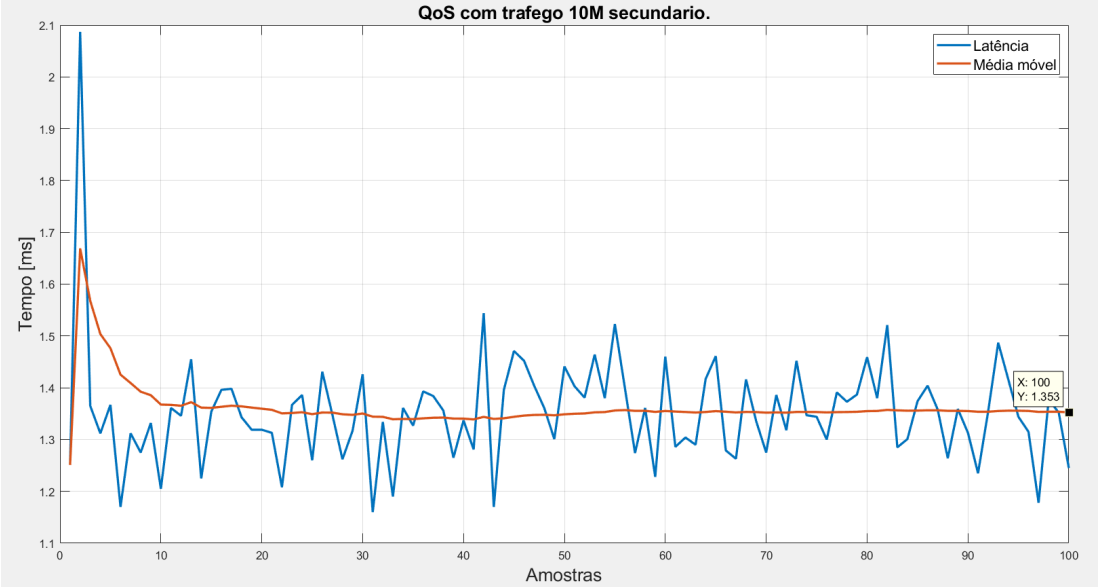

Figura A.16: Teste 17.

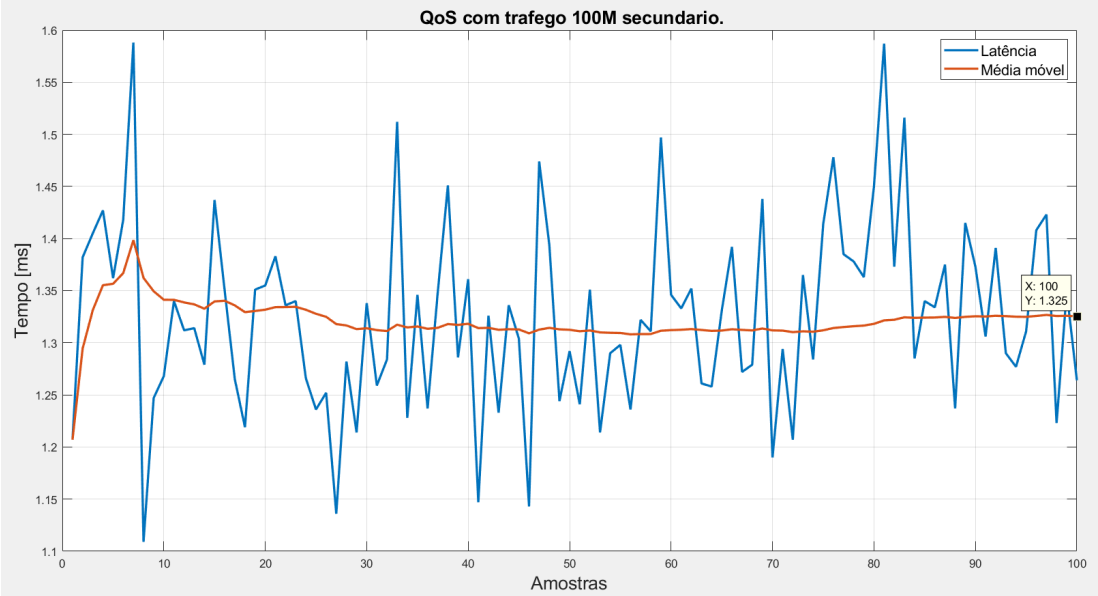

Figura A.17: Teste 18.

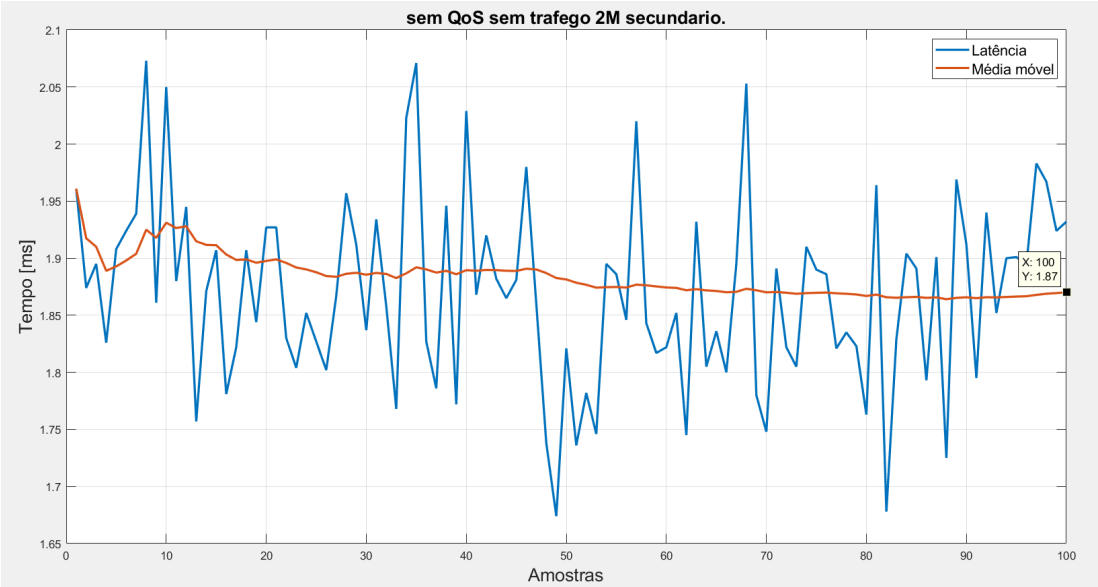

Figura A.18: Teste 19.

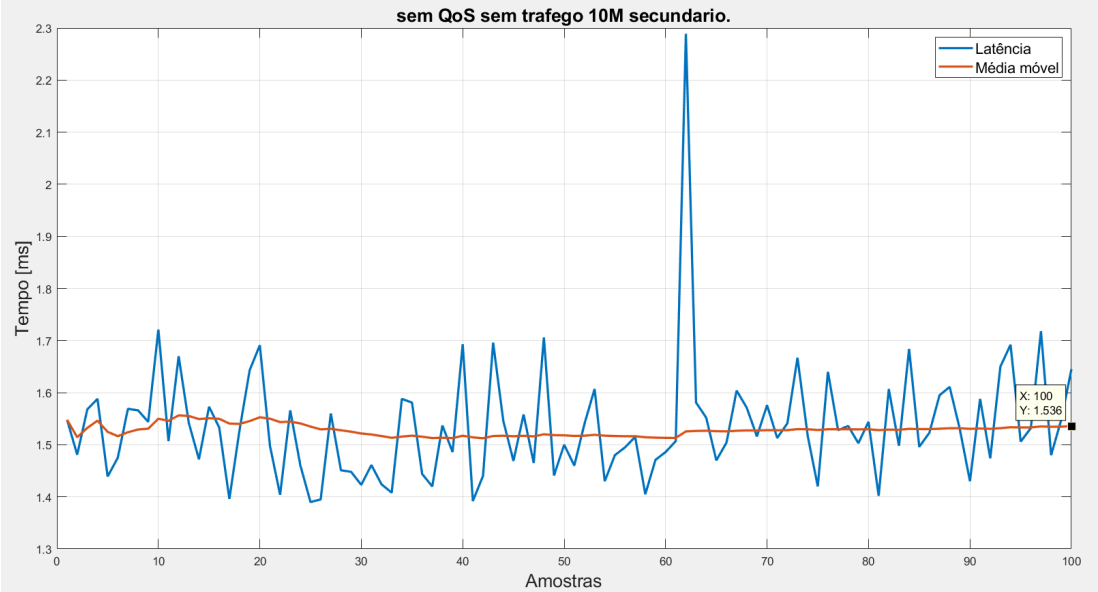

Figura A.19: Teste 20.

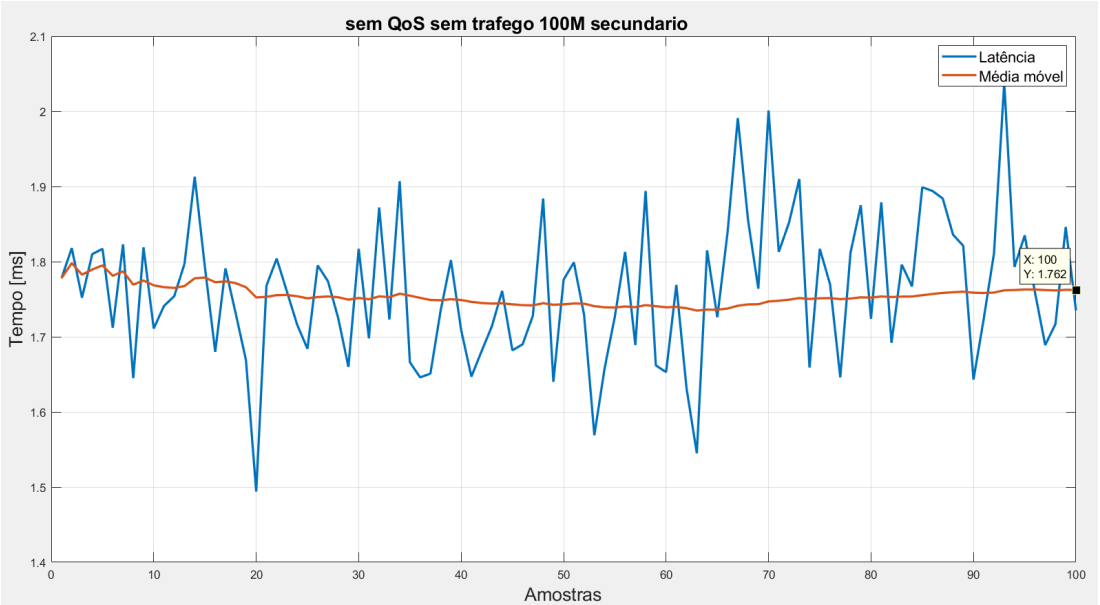

Figura A.20: Teste 21.

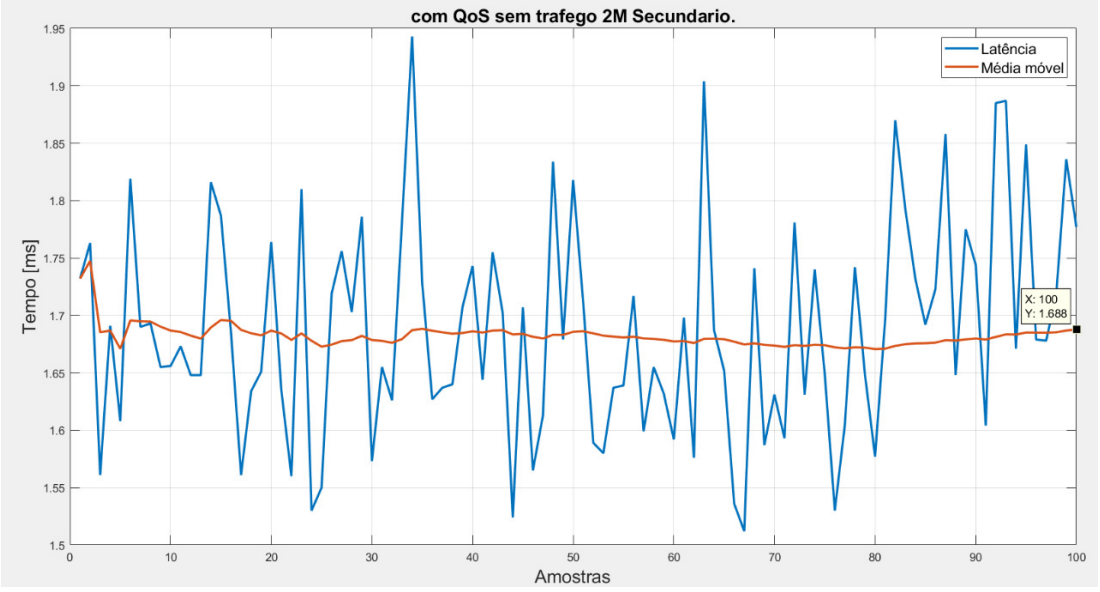

Figura A.21: Teste 22.

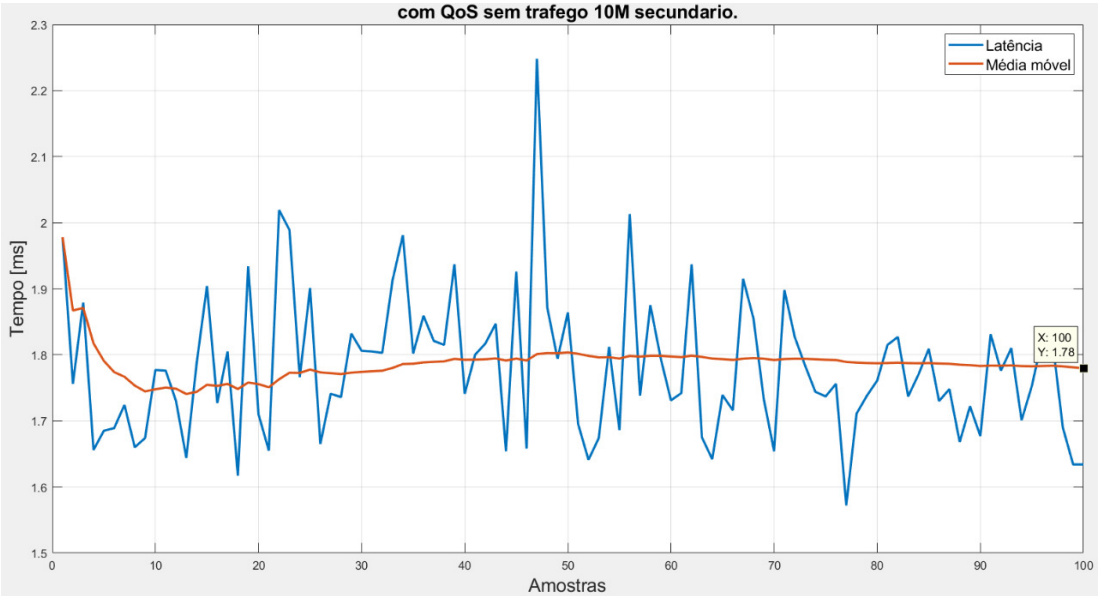

Figura A.22: Teste 23.

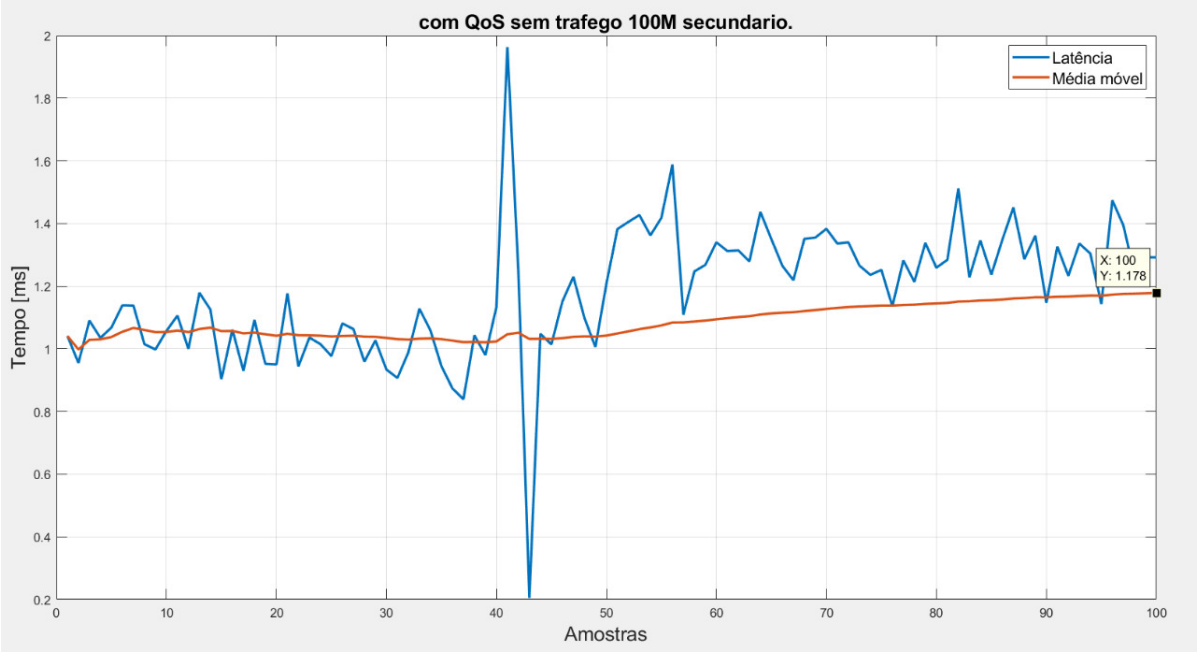

Figura A.23: Teste 24.