Dissertação de Mestrado

Inatel
Instituto Nacional de Telecomunicações

Avaliação de tecnologias estatísticas para serviços de teleproteção

Luiz Felipe Fernandes de Almeida

Outubro / 2020

Avaliação de Tecnologias Estátisticas para Serviços de Teleproteção.

Luiz Felipe Fernandes de Almeida

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

ORIENTADOR: Prof. Dr. Antônio Marcos Alberti.

Santa Rita do Sapucaí
2020

Almeida, Luiz Felipe Fernandes de
A447a
Avaliação de tecnologias estatísticas para serviços de teleproteção. / Luiz Felipe Fernandes de Almeida. – Santa Rita do Sapucaí, 2020.
109p.

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

1. Flex-LSP 2. IP Hard-Pipe 3. IP/MPLS 4. Redes Determinísticas. 5. Redes Estatísticas. 6. 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

Inatel
Mestrado em Telecomunicações

FOLHA DE APROVAÇÃO

Dissertação defendida e aprovada em _____ /_____ /_____,
pela comissão julgadora:

Prof. Dr. Antônio Marcos Alberti
INATEL

Prof. Dr. Alexandre Baratella Lugli
INATEL

Prof. Dr. Paulo Ricardo da Silva Pereira
UNISINOS

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

Agradecimentos

Inicialmente gostaria de agradecer a deus pela oportunidade oferecida.

Agradeço a minha mãe Maria do Carmo por todo o apoio e motivação durante esta caminhada.

Agradeço ao meu orientador Prof. Antônio Marcos Alberti por sua dedicação, orientação, profissionalismo e incentivo.

Agradeço aos meus amigos e colegas do Laboratório de Tecnologias da Informação e Comunicações (ICT Lab) pela convivência, apoio e cooperação.

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

Ao pessoal da FITec, parceiros no projeto D0640, por sua dedicação, paciência e contribuições.

Agradeço ao Inatel, pelo apoio durante esta caminhada, bem como a todos os professores por seus preciosos ensinamentos.

Por fim agradeço aos membros da banca, os senhores Antônio Marcos Alberti, Alexandre Baratella Lugli e Paulo Ricardo da Silva Pereira, por sua disposição e valiosas contribuições.

Sumário

Lista de Figuras

Lista de Tabelas

Acrônimos

ADSS All-Dieletric Self-Supporting

ANEEL Agência Nacional de Energia Elétrica

ANSI American National Standards Institute

APS Automatic Protection Switching

BFD Bidirectional Forwarding Detection

B Botton of Stack

CAPEX Capital expenditure

CESoPSN Circuit Emulation Service over Packet-Switched Network

DWDM Dense Wavelength Division Multiplexing

ECMP Equal Cost MultiPath

E-LSP EXP-Inferred Label Switched Path

FEC Forwarding Equivalence Class

GFP Generic Framing Procedure

H-QoS (Hierarchical Quality of Service

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IWF Interworking Function

IP Internet Protocol

ITU International Telecommunication Union

ITU-T International Telecommunication Union-Telecommunication Standardization sector

LDP Label Distribution Protocol

LCAS Link Capacity Adjustment Scheme

LSP Label Switched Path

MPLS Multi Protocol Label Switching

MPLS-TP Multi Protocol Label Switching - Transport Profile

MTU Maximum Transmission Unit

OaM Operations, Administration, and Management

ONS Operador Nacional do Sistema Elétrico

OPEX Operational Expenditure

OPGW Optical Ground Wire

OSPF Open Shortest Path First

OSI Open System Interconnection

PCM Pulse Code Modulation

PDH Plesiochronous Digital Hierarchy

PHP Penultimate Hoping Popping

PWE3 Pseudo Wire Emulation Edge-to-Edge

QoS Quality of Service

RTDS Real Time Digital Simulator

RSVP Resource Reservation Protocol

SATOP Structure-Agnostic Time Division Multiplexing over Packet

SCADA Supervisory Control and Data Acquisition

SEP Sistema Elétrico de Potênca

SDH Synchronous Digital Hierarchy

SyncE Synchronous Ethernet

SIN Sistema Interligado Nacional

SNR signal-to-noise ratio

SONET Synchronous Optical Network

TDM Time Division Multiplexing

TC Traffic Class

TTL Time to Live

VCAT Virtual Concatenation

WDM Wavelength Division Multiplexing

Publicações

1. L. F. F. De Almeida et al., "Control Networks and Smart Grid Teleprotection: Key Aspects, Technologies, Protocols and Case-Studies,"in IEEE Access, doi: 10.1109/ACCESS.2020.3025235.

2. LEITE, L. H. M. ; FERNANDES, R. A. ; ALMEIDA, L. F. F. ; ALBERTI, A. M. ; SOUZA, S. H. ; SANTOS, R. S. J. . Challenges in the Migration to Packet Switched Networks for Teleprotection Service of Power Transmission Lines. In: CIGRE Session, 2020, Paris. Proceedings of the CIGRE 2020, 2020. v. D2.

3. ALMEIDA, L. F. F. ; LEITE, L. H. M. ; FERNANDES, R. A. ; SANTOS, R. S. J. ; MACHADO, R. J. ; SILVA, W. R. ; SANTOS, J. R. ; RODRIGUES, J. J. P. C. ; ALBERTI, A. M. . 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.

Resumo

O consumo energético vem crescendo continuamente, sendo um dos principais pilares do crescimento e desenvolvimento econômico apresentado pela sociedade atual. Neste cenário, as concessionárias de energia provêm meios de interligar as fontes geradoras aos consumidores finais. Sistemas como os de teleproteção são utilizados para garantir que as falhas presentes nas redes elétricas não afetem os consumidores. Tradicionalmente, as concessionárias de energia utilizam tecnologias *Time-Division Multiplexing* (TDM) como meio de comunicação para os sistemas de teleproteção, porém a sua ineficiente alocação de recursos e o seu final de ciclo de vida abrem espaço para a utilização de novas tecnologias, tais como as baseadas em IP (*Internet Protocol*). Este trabalho tem como objetivo a avaliação de desempenho de redes estatísticas para o serviço de teleproteção, com ênfase na tecnologia IP-MPLS e seus variantes, através de soluções proprietárias. A metodologia de avaliação empregada foi baseada na elaboração de cadernos de testes e na realização de experimentos laboratoriais com equipamentos utilizados em campo pelas concessionárias de energia. Os resultados dos testes mostram a potencial viabilidade da utilização de redes estatísticas em relação aos requisitos operacionais de teleproteção, constituindo um passo importante para a realização de implementações em campo.

Almeida, L. F. F. [dissertação de mestrado]. Santa Rita do Sapucaí: Instituto Nacional de Telecomunicações; 2020.

.

Palavras-chave: *Flex-LSP*; *IP Hard-Pipe*; *IP/MPLS*; Redes Determinísticas; Redes Estatísticas; Teleproteção.

Abstract

Energy consumption has been growing continuously, being one of the main pillars of growth and economic development presented by today's society. In this scenario, electric utilities provide the means to connect generating sources to final consumers. Systems such as teleprotection ones are used to ensure that faults in electrical networks do not affect consumers. Traditionally, energy utilities use Time-Division Multiplexing (TDM) technologies as a means of communication for teleprotection systems. However, their inefficient allocation of resources and their end of the life cycle make possible the use of new technologies, such as those ones based on IP (Internet Protocol). This work aims to evaluate the performance of statistical networks for the teleprotection service, with an emphasis on IP-MPLS technology and its variants, through proprietary solutions. The evaluation methodology used was based on the elaboration of test books and the realization of laboratory experiments with equipment used in the field by the energy utilities. The results of the tests show the potential feasibility of using statistical networks in relation to the operational requirements of teleprotection, constituting an important step for carrying out implementations in the field.

Almeida, L. F. F. [masters dissertation]. Santa Rita do Sapucaí: Instituto Nacional de Telecomunicações; 2020.

.

Keywords: Deterministic Networks; Flex-LSP; IP Hard-Pipe; IP/MPLS; Statistic Networks; Teleprotection.

Capítulo 1

Introdução

As redes de comunicação presentes no cenário de missão crítica abrangem diversos setores, sendo eles o ramo de Energia (eletricidade, gás, extração de petróleo...), militar (patrulhamento de fronteiras, monitoramento das tropas, entre outros), transporte e aplicações governamentais [1]. No setor de energia elétrica, foco deste trabalho, as redes de comunicações foram construídas, principalmente, para o transporte de dados entre os centros de controles e os terminais remotos. Essa troca de informações entre as partes envolvidas tem como objetivo o monitoramento, controle do sistema, gerenciamento dos dispositivos da rede, faturamento dos clientes, dentre outros [2].

Tradicionalmente, as concessionárias de energia utilizam redes de telecomunicações baseadas em tecnologias *TDM*, como *Synchronous Optical Network* (SONET), *Synchronous Digital Hierarchy* (SDH) e *Plesiochronous Digital Hierarchy* (PDH) para suportar serviços de missão crítica. Dentre estes serviços pode-se destacar, comunicação com religadores e centros de comando, teleproteção e auto-cura.

A disponibilização das aplicações de missão crítica é um dos diversos serviços prestados pelas subestações de energia e, apesar de não ser o que exige maior largura de banda, é um dos que exigem maiores cuidados durante o seu dimensionamento. Isso porque a sua perfeita operação é vital para que todo o sistema de energia opere sem maiores preocupações [2].

Baseado em sua criticidade, a utilização de tecnologias *TDM* visa, principalmente, atender às rigorosas demandas exigidas pelos sistemas de proteção, sendo esses, extremamente sensíveis a variações na latência, *jitter*, simetria e recuperação de canal.

Como uma de suas principais características, as comunicações baseadas em tecnologias *TDM* oferecem uma largura de banda garantida para as aplicações demandadas pelas concessionárias criando, assim, circuitos com larguras de banda fixa para a transmissão de dados em intervalos de tempo pré estabelecidos, evitando problemas com latências e *jitter* na rede.

A simetria de canal é garantida pela própria estrutura e os protocolos utilizados pelas tecnologias *TDM*. Desta maneira, as informações trafegadas nas redes são transmitidas e recebidas pelos mesmos *timeslots*, de forma que, seja possível garantir os requisitos de qualidade tanto para o envio, quanto para o recebimento de informações.

Referente ao problema de recuperação de canal em caso de falhas, as tecnologias *TDM* oferecem uma ótima solução. Isso pois, em sua grande maioria, proporcionam redundância dos caminhos de tráfego através de anéis ópticos de comunicação garantindo, assim, a transição do caminho primário para o secundário em menos de 50 milissegundos [3].

Outra característica a ser destacada é a segurança na utilização destas tecnologias, onde cada conexão possuirá o seu próprio circuito de ponta a ponta no sistema. Caso a concessionária utilize um serviço de telecomunicações oferecido por terceiros, os dados da rede referentes a cada cliente não poderão ser visualizados ou alterados pelos demais.

O fato de se tratar de sistemas determinísticos proporciona aos sistemas de telecomunicações um controle maior sobre os dados trafegados pela rede, de forma que, o administrador do sistema possa conhecer os caminhos percorridos pelos dados, facilitando a disponibilização de suporte para situações onde ocorram falhas nos canais de comunicação [3].

Apesar de suas qualidades, as tecnologias *TDM* utilizadas pelas concessionárias de energia estão caindo em desuso, ou seja, não estão recebendo grandes investimentos para inovações. Outro ponto relevante está em sua ineficiente alocação de banda. Caso o cliente não esteja utilizando o canal para o envio de informações, o mesmo se torna ocioso. Desse modo, a largura de banda é perdida e não pode ser compartilhada por outras aplicações ou clientes.

Com a chegada das *Smart Grids* e a adoção em massa dos conceitos e aplicações estabelecidos por elas, seria possível tornar a rede de energia mais confiável, eficiente e resiliente do que o modelo convencional?

De forma geral, com a adoção destes conceitos seria possível melhorar a qualidade da energia fornecida ao cliente; reduzir a geração de energia excedente, uma vez que ocorreria uma maior gerência da carga demandada; implementar o conceito de geração distribuída de energia, fazendo com que a energia gerada pelos clientes seja incorporada à rede de forma mais fácil e segura; além de reduzir a vulnerabilidade dos sistemas e possibilitar a identificação e correção de falhas de maneira autônoma e eficiente [4].

Porém, a tecnologia de comunicação legada das concessionárias enfrentará grandes problemas para se adequar aos requisitos demandados por essas novas aplicações, principalmente pela sua alocação de banda ineficiente, se apoiando no fato de que a maioria destes novos tráfegos possuem a característica de partidas em "rajadas". Neste cenário, um grande espaço na largura de banda do canal é consumido momentaneamente para o envio de uma quantidade massiva de dados, desocupando-o para que outras aplicações o utilizem quando o envio for terminado [5].

Com isso as concessionárias estão verificando a possibilidade de evoluir sua infraestrutura de comunicação para tecnologias baseadas no padrão *TCP/IP*, de forma a adequar-se às tendências atuais e futuras. A utilização dessas tecnologias ocorre principalmente pelo grande número de padrões que já se encontram em um estado maduro o suficiente para a sua adoção em massa, servindo de ponte para a interconexão de diversas aplicações. Vale ressaltar que essa evolução na infraestrutura deve ocorrer de forma suave, minimizando os riscos e preservando os investimentos já realizados [5].

Com a adoção de tecnologias baseadas no padrão *TCP/IP* no ramo de missão crítica,

diversos benefícios podem ser observados, como uma maior eficiência do sistema operacional, crescimento na produtividade, garantia de expansão para as aplicações futuras e suporte para os serviços legados, além de oferecer uma maior flexibilidade para alteração nos serviços vigentes, contrastando aos sistemas *TDM*, onde a atribuição dos *slots* de tempo é realizada de forma estática.

Dentre as diversas tecnologias baseadas no padão *TCP/IP* disponíveis no mercado, a solução *Multi Protocol Label Switching* (MPLS) tem se destacado para os serviços de missão crítica [6]. A convergência entre as redes utilizadas neste cenário e as utilizadas em outras aplicações e serviços para uma única rede *IP/MPLS* acarretaria em uma redução de custo total, tanto no *CAPEX* como no *OPEX* das concessionárias.

Em relação ao *CAPEX*, ocorreria uma economia considerável, tendo em vista que equipamentos utilizados em tecnologias *TDM* e *IP*, tradicionalmente separados, possuem um valor excedente ao valor de um único roteador *MPLS*. Referente ao *OPEX*, a utilização de uma única tecnologia garantiria a redução no número de equipamentos físicos necessários e no consumo de energia [7].

Como observado anteriormente, a migração dos sistemas de teleproteção para redes *IP/MPLS* oferecem a garantia de que o sistema legado *TDM* não precise ser substituído. Através de sistemas "*pipes*" é possível a criação de *links TDM*, utilizando arquiteturas como o *PWE3*, do inglês, *Pseudo Wire Emulation Edge-to-Edge* [8]. Através dessa emulação dos canais legados sobre *IP/MPLS* é possível garantir, em tese, todos os benefícios presentes nos sistemas *TDM*, além de contar com os benefícios obtidos ao se utilizar uma rede *MPLS*. Neste cenário, não há desperdício de banda, onde a mesma será consumida apenas quando utilizada para o envio das informações [7].

Através desta tecnologia, é possível a obtenção de baixas latências na rede devido à minimização do número de nós entre os pontos que desejam manter a comunicação e dos *Dejitter buffers* com tamanhos pequenos. Outra medida que pode ser adotada para a redução de latência é a priorização de níveis de qualidade de serviço, em Inglês *Quality of Service* (QoS), para serviços de missão crítica, de forma a garantir que os dados não sejam afetados por redes congestionadas. A adoção desta técnica pode acarretar na perda de pacotes para serviços com menores prioridades, mas garantirá a qualidade necessária para os serviços prioritários [9].

Além da redução de latência e dos problemas relacionados ao *jitter*, é necessária uma solução para a assimetria de canal. Através da tecnologia *IP/MPLS*, isso é possível devido ao envio e recebimento de informações pelos sistemas de missão crítica através dos mesmos *LSPs*, do Inglês, *Label Switched Path*, que podem ser configurados de forma estática ou através da solução MPLS-TP [9].

Mediante as informações citadas anteriormente, este trabalho possui o intuito de realizar uma avaliação de desempenho na utilização de redes estatísticas para os serviços de teleproteção de linhas de transmissão de energia. Para isto, serão realizados testes laboratoriais com equipamentos utilizados em campo pelas concessionárias de energia e através de duas soluções proprietárias baseadas na tecnologia *IP/MPLS* (e suas variantes, quando possível). A análise e avaliação dos resultados serão realizados mediante a comparação dos valores

obtidos com os valores estabelecidos pelas entidades normativas do setor de energia.

1.1 Organização do Texto

Este trabalho está dividido em 6 capítulos. O Capítulo 1 possui o objetivo de introduzir o leitor ao assunto, de forma a construir uma base para as informações que serão discutidas durante o estudo. Neste capítulo é evidenciado o cenário atual das redes de telecomunicações utilizadas pelas concessionárias de energia para o serviço de teleproteção, apresentando seus benefícios e limitações. Também é apresentada uma breve introdução da tecnologia que será o objetivo deste estudo (*IP* e *MPLS*), realizando uma comparação com o cenário atual, apresentando seus prós e contras e justificando sua escolha.

No Capítulo 2 é fornecido ao o leitor todo o embasamento teórico necessário para a contextualização do trabalho realizado. Este capítulo inicia-se com os conceitos de redes de comutação de circuitos e de pacotes, seguido pelos conceitos gerais de teleproteção, funções de proteção aplicadas nos sistemas elétricos, lógicas de comparação utilizadas em sistemas de teleproteção, tecnologias de comunicação para sistemas de teleproteção e, por fim, as soluções proprietárias utilizadas para as experimentações neste trabalho.

No Capítulo 3 é realizado um levantamento dos principais trabalhos relacionados ao tópico de teleproteção de redes de energia via tecnologias de comunicação com multiplexação estatística.

No Capítulo 4 é apresentado todo o cenário de testes utilizado para a validação da dissertação. Inicialmente são apresentados os equipamentos utilizados juntamente com uma topologia de testes genérica, realizando uma breve descrição da função de cada equipamento nesta topologia. Nas subseções seguintes são apresentados os cadernos de testes utilizados para cada uma das soluções, expondo as principais configurações da rede, e detalhando os testes que serão realizados em cada solução.

No Capítulo 5 São apresentados os resultados obtidos para cada um dos experimentos realizados, juntamente com uma análise dos resultados obtidos. Para a validação dos resultados são utilizados embasamentos estatísticos, assim como indicadores fornecidos em processos normativos.

No Capítulo 6 são apresentadas as considerações finais desta dissertação, tomando como base os experimentos realizados e concluindo quais hipóteses levantadas são de fato verdadeiras. Ainda, apresenta-se as possíveis propostas de continuidade para este estudo.

Por fim, são apresentadas as referências bibliográficas utilizadas.

Capítulo 2

Background

Este capítulo abrange os principais aspectos necessários para um bom entendimento do que será proposto nesta dissertação.

De modo que, primeiramente, se discutirá os conceitos referentes às redes de comutação por circuitos e pacotes e, em seguida, será exposto o cenário de teleproteção com os seus principais requisitos.

Ademais, será apresentado ao leitor as principais funções e lógicas de proteção da rede de energia, bem como as tecnologias de comunicação utilizadas nos cenários de teleproteção.

2.1 Redes de Comutação de Circuitos e de Pacotes

Como descrito anteriormente, as tendências atuais caminham para as tecnologias de pacotes e consequentemente a adoção em massa das redes baseadas no padrão *TCP/IP*. Esse cenário não se faz diferente nas concessionárias de energia, que vislumbram uma possível substituição dos seus sistemas atuais baseados em tecnologias de comutação de circuitos, por sistemas baseados em comutação por pacotes.

A comutação de pacotes busca melhorar a flexibilidade e a eficiência do uso dos recursos dos enlaces através do seu compartilhamento, enquanto a comutação de circuitos trabalha com recursos dedicados. A seguir será realizada uma abordagem mais detalhada sobre os conceitos referentes às comutações tradicionais baseadas em circuitos e as comutações baseadas em pacotes.

2.1.1 Comutação de Circuitos

Implica na existência de um enlace dedicado de comunicação entre dois usuários, que é composto por uma sequência de enlaces conectados entre si através dos nós da rede. Os enlaces dedicados podem ser físicos (um cabo ou uma fibra óptica, por exemplo), ou fatias virtuais de um enlace físico (um *slot* de tempo, um canal de frequência, etc.). As fatias

virtuais são criadas através de alguma técnica de multiplexação, sendo a mais comum o sistema *TDM* [10].

Em cada nó, os comutadores de circuitos devem ter a inteligência para alocar canais e recursos de comutação para os circuitos em construção e encontrar uma rota através da rede (função chamada de roteamento) por onde o circuito vai passar. Essas funções são realizadas pelo plano de controle da rede, sendo tipicamente chamadas de sinalização de controle. Os nós da rede reservam canais para atender as requisições dos novos circuitos e enviam adiante mensagens de sinalização, até que um circuito fim a fim seja estabelecido entre os usuários finais [10].

A comutação de circuitos pode ser ineficiente, pois a capacidade alocada para cada enlace nem sempre é utilizada por completo, gerando gastos desnecessários. Entretanto, uma vez estabelecida a conexão, os dados são transportados a uma taxa praticamente constante e com atrasos, em grande parte, determinísticos [11].

Uma das maiores vantagens da comutação de circuitos é a sua transparência. Uma vez que o circuito é estabelecido, é realizada uma ligação direta entre dois usuários sem a necessidade de gerenciamento de tráfego. As informações seguem como um fluxo contínuo, *bit* atrás de *bit*. A comutação dos enlaces virtuais transfere *bits* de uma porta de entrada para uma porta de saída, continuamente [11].

2.1.2 Comutação de Pacotes

Neste sistema não existe um enlace dedicado para a comunicação entre dois usuários, fazendo com que os pacotes compartilharem um ou mais enlaces da rede. Desta forma, os enlaces não estão explicitamente reservados para os usuários e suas conexões. Todo o compartilhamento é realizado na camada de enlace e os dados dos usuários são transmitidos em pacotes, que podem ser de tamanho fixo ou variável.

Quando um usuário tem uma mensagem muito grande para ser transmitida, esta mensagem pode ser fragmentada em vários pacotes, através de um procedimento chamado de segmentação. No destino, os pacotes são remontados na mensagem original através de um procedimento chamado de remontagem [12].

Cada pacote contém uma porção com os dados do usuário (carga útil ou *payload*) e uma porção com informações de controle e de endereçamento (cabeçalho ou *header*), que são utilizadas para rotear/encaminhar os pacotes pela rede. Em cada nó da rede, os pacotes são recebidos, armazenados e comutados para o próximo nó, em função dos dados de controle presentes em seus cabeçalhos.

Seus recursos de comutação e de armazenamento podem, ou não, serem reservados para atender o tráfego de pacotes dos usuários. Isso depende do suporte a mecanismos de *QoS*. Em muitas redes, nada é feito para garantir a qualidade de certos pacotes em detrimento de outros, mas existem tecnologias que oferecem garantias de *QoS*, permitindo uma engenharia de tráfego fina dos pacotes que transitam pela rede [13].

Na comutação de pacotes, a utilização dos canais é alta, pois eles podem ser dinamicamente compartilhados por muitos pacotes de vários usuários ao mesmo tempo. Desta forma, realiza-se a chamada multiplexação estatística dos enlaces, permitindo que tráfegos de uma conexão utilizem recursos dos enlaces que não estão sendo utilizados por outras conexões em um dado momento. Como consequência do congestionamento de pacotes, os mesmos podem enfrentar atrasos variáveis ou até serem descartados, dependendo do nível de congestionamento da rede [14].

Redes de comutação de pacotes possibilitam a utilização de prioridades ou mecanismos sofisticados de justiça, permitindo, portanto, beneficiar a qualidade de serviço de algumas conexões em prol de outras. Para isso, é preciso que os nós implementem algoritmos de *QoS* e que as configurações apropriadas em todas as tecnologias da rede sejam feitas via engenharia de tráfego.

2.2 Conceitos Gerais sobre Teleproteção

Os componentes dos sistemas de potência estão, normalmente, instalados em ambientes externos, sendo expostos a situações adversas, como é o caso: das linhas de transmissão, transformadores de potência, barramentos de alta tensão, transformador abaixador de tensão, subestações, entre outros. Portanto, é de extrema importância o dimensionamento de sistemas de proteção que possam garantir o seccionamento de partes da rede em situações de risco iminente.

Em um sistema de potência, a maioria das falhas que podem ocorrer em uma linha de transmissão, estão relacionadas ao rompimento do isolamento dielétrico entre fase e terra. Sendo essas, muitas vezes associados a elevações repentinas de tensão causadas por descargas atmosféricas e manobras na rede. As falhas também podem ocorrer devido ao desgaste imposto aos dielétricos quando expostos a queimadas ou através do acumulo de impurezas na superfície dos isoladores [15].

Com o intuito de evitar essas falhas, todo o sistema elétrico possui um sistema de proteção. Neste sistema, os relés e os dispositivos de proteção atuam com o intuito de supervisionar os equipamentos que devem ser protegidos e, em caso de anomalias, realizar o isolamento de toda a parte afetada.

Desta forma, a teleproteção é a técnica empregada a sistemas de proteção baseados em telecomunicações, com o intuito de interligar equipamentos de proteção que se encontram fisicamente distantes. A comunicação entres estes componentes é efetuada através de lógicas que realizam comparações entre as condições verificadas por ambos os relés localizados nas extremidades da linha [16].

Para que haja interoperabilidade entre os equipamentos de teleproteção e as redes de telecomunicações, é necessária a utilização de funções que realizam a conversão dos sinais e mensagens enviadas e recebidas. Estas funções podem ser realizadas pelos próprios relés, por equipamentos presentes nos sistemas de telecomunicações ou através de equipamentos

dedicados, denominados de 'equipamentos de teleproteção'. Um sistema de teleproteção genérico pode ser observado na Figura 2.1 [17].

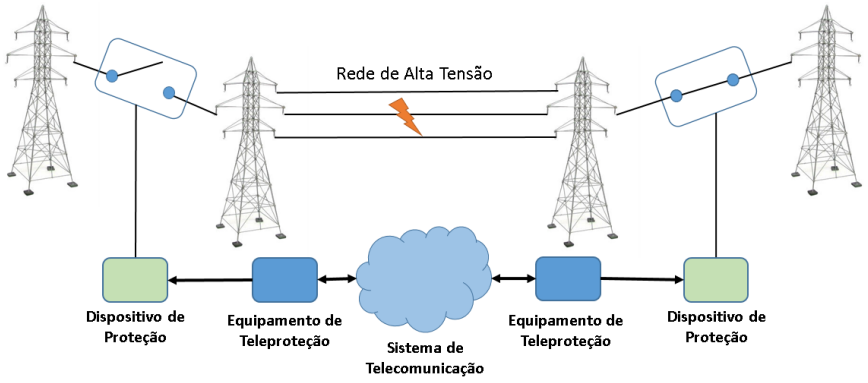


Figura 2.1: Topologia genérica de teleproteção para linhas de transmissão de energia. Adaptado de [17]

Tendo em vista que boa parte dos sistemas de transmissão de energia são interligados em anel, é necessário que ocorra o desligamento em ambos os terminais para a isolação de uma falta na linha. Assim, para lidar com esse problema, quando há uma falta na linha de transmissão, o relé de proteção da subestação mais próxima deverá detectar a ocorrência do problema e realizar a comutação de um lado do terminal. Diante disso, os dados serão coletados pelo equipamento de teleproteção que enviará a informação ao outro equipamento, disponível no terminal remoto adjacente, permitindo que ocorra a ação no relé da sua respectiva subestação, e consequentemente, o isolamento da linha faltosa [18].

Para que o sistema apresente um desempenho satisfatório, é necessário que requisitos como seletividade, rapidez, sensibilidade, segurança, confiabilidade e economia sejam considerados. A seguir será realizada uma breve explicação sobre os tópicos levantados anteriormente.

- **Seletividade:** Remete a capacidade do sistema em identificar e isolar o circuito defeituoso com o menor impacto possível na rede, assegurando a operabilidade do restante da linha de transmissão.
- **Rapidez:** O sistema de proteção deve agir de forma rápida e, se possível, possibilitar o seu religamento, de modo que a rede seja minimamente afetada. A teleproteção garante um ganho relativo em relação à redução de tempo de extinção da falta quando comparado a sistemas sem esquemas de teleproteção.
- **Sensibilidade:** O sistema deve ser sensível e confiável, podendo identificar a diferença entre uma condição faltosa e uma normal, além de ser capaz de tomar a decisão correta.
- **Segurança:** Atrelado à sensibilidade, a segurança está relacionada ao cenário onde o esquema de proteção deva atuar apenas em caso de falhas, evitando, assim, *Trips*

indevidos nos relés de proteção. Onde os *trips* correspondem a sinais de desligamento enviados pelos relés.

- **Confiabilidade:** Expressa a característica de um sistema que, quando solicitado, não falhe, garantindo a integridade da rede de energia. Neste cenário, expressa a necessidade do sistema em emitir e receber comandos válidos mesmo na ocorrência de interferências e ruídos no canal de comunicação.
- **Economia:** Verifica o custo-benefício da implementação de um sistema de teleproteção em determinada linha de energia, através da análise de custo e viabilidade técnico econômica.

2.3 Funções de Proteção Aplicadas nos Sistemas Elétricos

Os relés de proteção podem ser empregados para a proteção dos sistemas de transmissão e distribuição, realizando a proteção das linhas de energia e das cargas que estão conectadas nas mesma. Sendo assim, são responsáveis por fornecer um mecanismo de segurança para todos os equipamentos envolvidos no Sistema Elétrico de Potência (SEP) [19].

Resumidamente, um relé é um dispositivo sensor que mediante a presença de anomalias no sistema protegido, executa o comando de abertura dos disjuntores, realizando o seccionamento de determinados blocos do sistema [20]. Esses mecanismos realizam o monitoramento do meio elétrico e, baseado na análise de grandezas como tensão, corrente, potência e impedância, tomam as medidas de proteção adequadas.

Um ponto de extrema importância nos sistemas de proteção é a capacidade de identificar a diferença entre uma situação faltosa e uma situação padrão. Neste cenário, o relé deve ser capaz de distinguir as situações e atuar apenas quando for necessário. Baseado nas informações disponibilizadas anteriormente, pode-se concluir que as funções primordiais dos relés são [21]:

- Monitorar o meio elétrico através de determinadas grandezas;
- Identificar uma anomalia no sistema;
- Localizar o ponto de falha com a maior exatidão possível;
- Avisar o operador do sistema sobre a ocorrência de uma falta;
- Enviar um sinal de comando para os disjuntores.

Diferentes tipos de relés podem ser empregados ao sistema de proteção. Estes equipamentos são representados através de uma numeração definida pela norma IEEE C37.2-1991 [22], de acordo com as funções realizadas. A seguir, será apresentada uma abordagem dos relés mais utilizados.

2.3.1 Relé Sobrecorrente

Representado pelos números 50 (relé de sobrecorrente instantâneo) e 51 (relé de sobrecorrente temporizado), os relés de sobrecorrente utilizam a corrente elétrica como grandeza de atuação. Os mesmos atuam quando o valor de corrente mensurado ultrapassa um valor pré ajustado, enviando um sinal de abertura para que o disjuntor isole a falta [23].

Assim como descrito anteriormente, os reles de sobrecorrente podem ser classificados como instantâneo ou temporizado. O relé de sobrecorrente instantâneo possui o objetivo de identificar e eliminar as falhas mais severas, buscando sempre minimizar os efeitos aplicados ao sistema elétrico [23].

Nos relés de sobrecorrente temporizados, dois parâmetros devem ser pré configurados, sendo eles, o ajuste de corrente e o tempo de atuação. No momento em que a corrente mensurada ultrapassa o valor pré ajustado, uma contagem de tempo é iniciada. Quando o tempo pré-configurado é atingido, o relé envia um sinal de abertura para o disjuntor, realizando sua abertura e, consequentemente, isolando a falha [23].

2.3.2 Relé Direcional

Representado pelo número 67, os relés direcionais tem como característica a atuação quando a corrente presente no sistema possui um sentido pré-estabelecido, de acordo com a sua referência de polarização [24]. Quando uma falta ocorre no sentido contrário, gerando uma corrente reversa, o relé não é capaz de identificá-la e desta forma não atua.

Tipicamente, este relé é empregado em linhas de transmissão de energia que operam na topologia em anel, onde é difícil obter níveis aceitáveis de seletividade empregando relés de sobrecorrente. Uma representação de uma topologia em anel com proteção direcional pode ser observada na Figura 2.2.

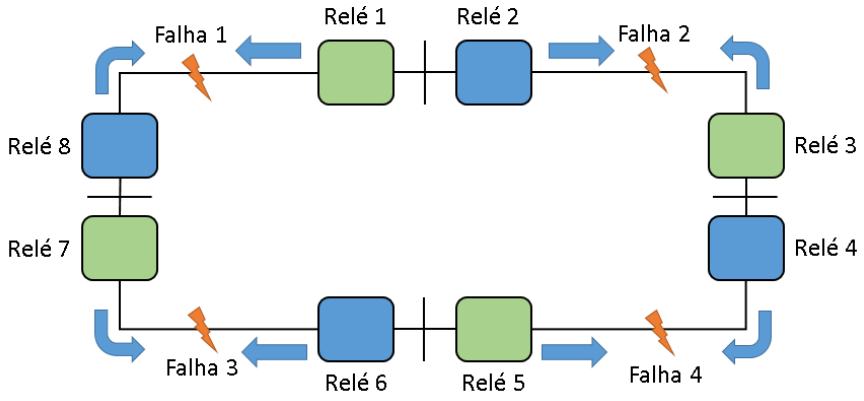


Figura 2.2: Topologia em anel com proteção direcional. Adaptado de [21]

Como pode ser observado na Figura 2.2, a proteção do sistema no sentido horário é reali-

zada pelos relés pares e a proteção do sistema no sentido anti-horário é realizada pelos relés ímpares. A seletividade da proteção é garantida, uma vez que, a ocorrência de qualquer uma das falhas, resultará na atuação de ambos os relés que se encontram em suas extremidades. Como exemplo, pode-se considerar a ocorrência da falha 3. Neste cenário, há o acionamento dos relés 6 e 7, ocasionando o seccionamento e extinção da zona faltosa.

2.3.3 Relé de Distância

Representado pelo número 21, os relés de distância abordam uma classe de relés conhecidos por relé de impedância, relé de admitância (mho), relé de reatância e relé quadrilateral. Onde estes, realizam as medida das grandezas carregadas em seu nome, da linha de transmissão até o ponto de falha ou da carga [25].

Os relés são representados de acordo com suas características e zonas de operação. sendo isto apresentado através da Figura 2.3.

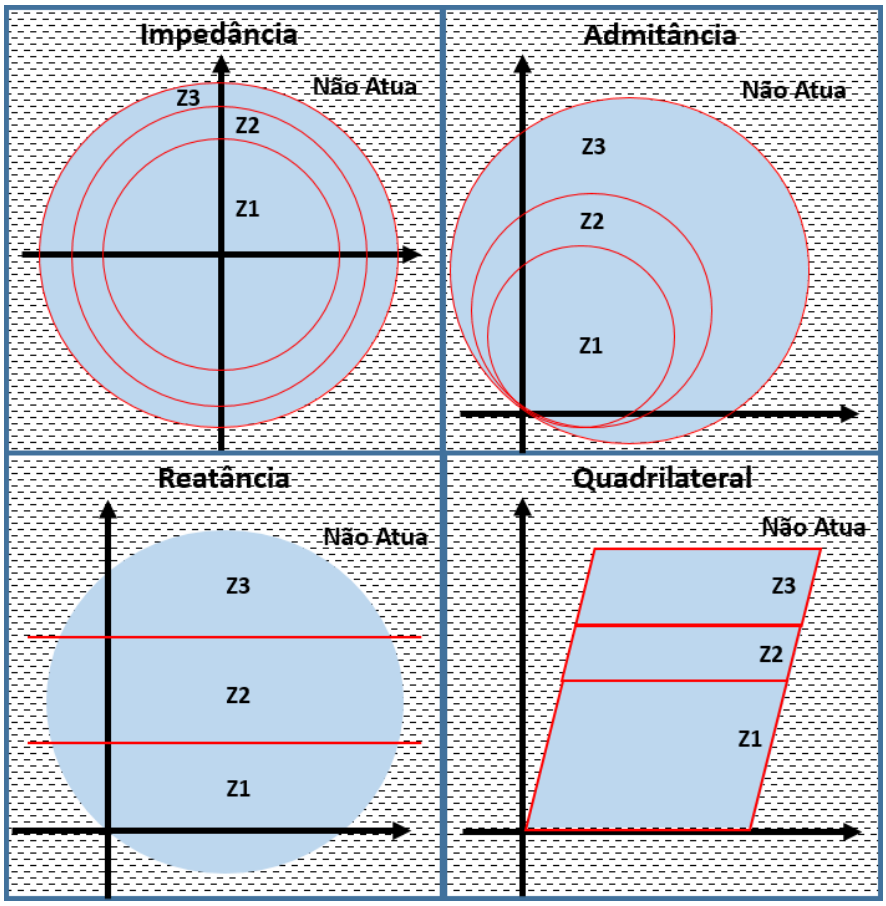


Figura 2.3: Zonas de proteção dos relés de teleproteção. Adaptado de [21]

Em relação aos relés de impedância, os mesmos são ajustados para operar na ocorrência de faltas que produzam valores de impedâncias localizadas dentro dos círculos. Desta forma, valores de impedância superiores não podem ser observados pelos relés. Devido ao seu dimensionamento, podem ser identificadas faltas que ocorram tanto para frente quanto para trás do ponto onde foi instalado [26].

Como a maioria dos sistemas de proteção são empregados em anel, para a utilização do relé 21, uma unidade direcional deve ser empregada no sistema (relé direcional 67). Normalmente os relés 21 são ajustados para 3 zonas de atuação, onde os ajustes variam de acordo com o caso de implementação [26].

2.3.4 Relé Diferencial

Representado pelo número 87, o relé diferencial é baseado na comparação das correntes elétricas de entrada e de saída de um determinado equipamento. Sua operação é fundamentada na primeira lei de *Kirchhoff* orientada aos equipamentos, podendo existir três cenários possíveis. No primeiro cenário, se a corrente de entrada em um equipamento é igual a de saída o relé não atua, pois o equipamento não apresenta nenhum defeito.

O segundo cenário pode ser obtido quando o resultado da subtração da corrente de entrada no equipamento pela corrente de saída for inferior ao da corrente de ajuste do relé, de forma a não atuá-lo. Por fim, o último cenário ocorre quando o resultado da subtração entre as correntes de entrada e saída do equipamento for superior à corrente de ajuste do relé, levando à atuação do sistema de proteção por verificar uma anomalia e possível defeito no equipamento protegido [21].

As zonas de proteção empregadas neste sistema são delimitadas pelos transformadores de corrente. Os elementos a serem protegidos podem ser transformadores de potência, máquinas síncronas, cabos subterrâneos e até linhas de transmissão de energia. Sua atuação pode ser empregada para sistemas em anel ou radial. A representação um sistema de proteção diferencial genérico pode ser observado na Figura 2.4.

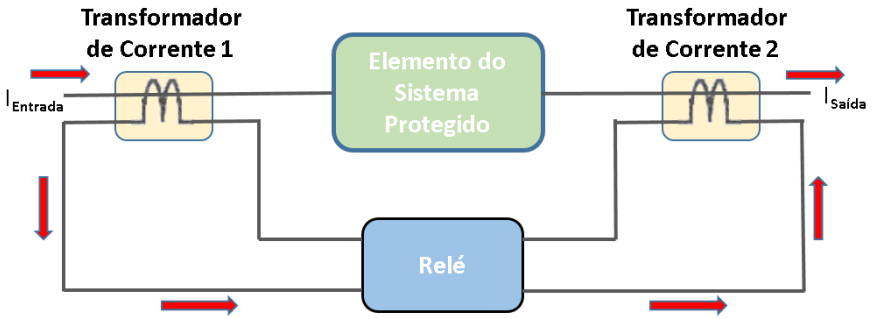


Figura 2.4: Sistema de proteção diferencial genérico. Adaptado de [21]

2.4 Lógicas de Comparação Utilizadas em Sistemas de Teleproteção

Para a elaboração de um esquema de teleproteção, diversas lógicas de comparação podem ser utilizadas, sendo divididas em sua grande maioria entre lógicas permissivas e de bloqueio, conforme apresentado em [27]. A seguir, será realizada uma breve abordagem sobre algumas delas, como, por exemplo, *Permissive Intertrip, Direct Underreaching Transfer Trip (DUTT), Permissive Underreaching Transfer Trip (PUTT), Permissive Overreaching Transfer Trip (POTT) e Directional Comparison Blocking (DCB).*

2.4.1 Direct Underreaching Transfer Trip (DUTT)

O esquema de teleproteção DUTT, em português, transferência direta de disparo por subalcance, necessita apenas de funções de subalcance. Este esquema é utilizado no sistema elétrico, quando se deseja realizar o desligamento direto do disjuntor através de um sinal de comunicação [26]. Sempre que o sistema identificar uma falha na Zona 1, um sinal de disparo é enviado para o terminal remoto através do transmissor Tx. No momento em que o mesmo é identificado pelo receptor Rx do terminal remoto, um sinal é enviado para que ocorra a abertura imediata do disjuntor.

Vale ressaltar a importância do dimensionamento do sistema de comunicação para este esquema de teleproteção. Isso porque um defeito no canal de comunicação, possivelmente, resultará em uma transmissão errônea do sinal e realizará o desligamento indevido do disjuntor [28].

A representação do sistema DUTT pode ser observada na Figura 2.5.

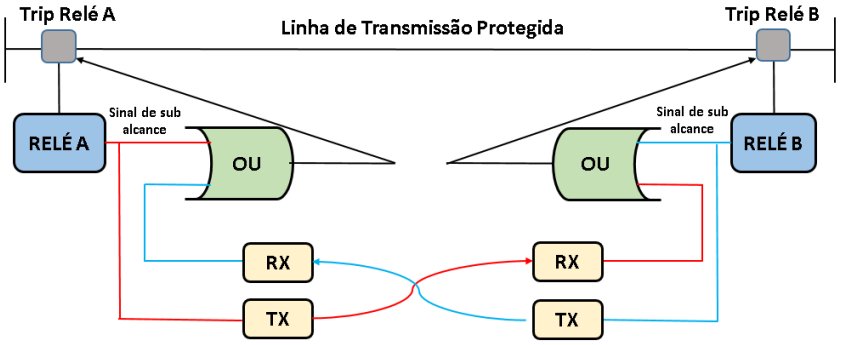


Figura 2.5: Lógica básica para o esquema DUTT. Adaptado de [28]

2.4.2 Permissive Underreaching Transfer Trip (PUTT)

O esquema de teleproteção PUTT, em português, disparo permissivo por subalcance, necessita de funções de subalcance e sobrealcance. Neste esquema, quando o relé detecta uma falha dentro da Zona 1, o mesmo realiza o desarme do disjuntor local e envia um sinal de disparo permissivo para o relé localizado na outra extremidade da linha de transmissão. Caso o relé remoto receba o sinal de disparo permissivo e verifique a ocorrência de uma falha dentro da Zona 2, o mesmo realizará o desarme de seu disjuntor local, ocasionando o seccionamento daquele circuito.

Como o esquema PUTT utiliza, no relé receptor, uma função que monitora a zona 2, é possível empregar um sistema de sinalização menos rigoroso. Esta afirmação deve-se ao fato de que caso ocorra o envio errôneo de um sinal de disparo por parte do sistema de comunicação, a unidade direcional do relé receptor não permitirá o acionamento do disjuntor local [26].

Tradicionalmente, o disparo permissivo por subalcance é amplamente aplicado em linhas de transmissão de circuito duplo. Isso se deve ao fato do esquema não necessitar da utilização de uma lógica adicional para garantir a segurança em cenários de correntes reversas [29].

Em situações onde as linhas de transmissão possuem um comprimento insuficiente para a aplicação de proteção de Zona 1, ou em linhas multi-termais, a utilização desta lógica de proteção não é indicada, pois seu emprego pode levar a cenários de operação indevida do sistema de proteção [30]. A representação do sistema PUTT pode ser observado na Figura 2.6.

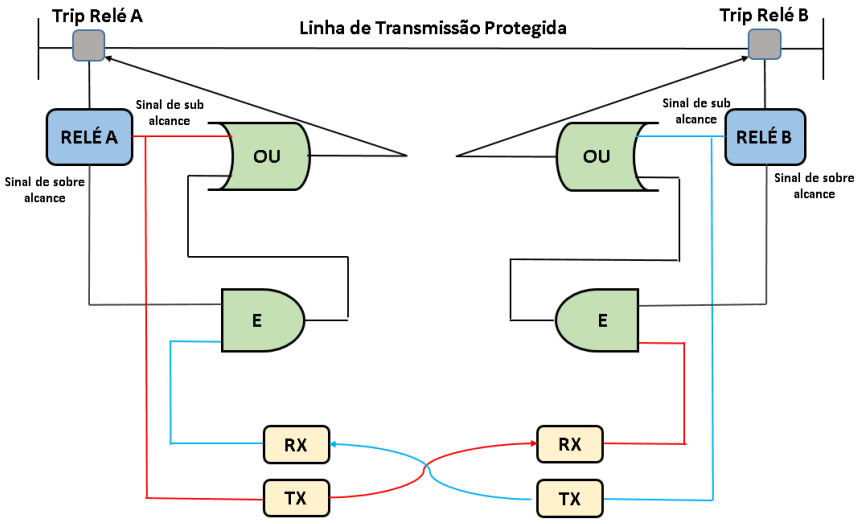


Figura 2.6: Lógica básica para o esquema PUTT. Adaptado de [28]

2.4.3 Permissive Overreaching Transfer Trip (POTT)

Os esquema de teleproteção POTT, em português, transferência permissiva de disparo por sobrealcance, utiliza um elemento de Zona 2 de sobrealcance para realizar o desarme do disjuntor local e enviar um sinal de disparo permissivo para o relé localizado na outra extremidade da rede. Caso o elemento de Zona 2 remoto detecte uma falha na rede, o relé remoto realizará o desarme do disjuntor assim que receber um sinal permissivo [25].

Tipicamente, para a implementação deste esquema são utilizados relés de sobrecorrente de distância (21) e relés direcionais (67). A configuração aplicada a estes relés garante que o sistema possa detectar falhas que ocorram adiante. Tornando possível a cobertura de 120 a 150% da linha protegida e, consequentemente, alcance o terminal localizado na outra extremidade.

Este esquema também é passível da implementação de uma sinal de guarda, possibilitando o monitoramento continuo dos canais de comunicação. Através deste procedimento é possível impedir que os mesmos sejam afetados, de forma errônea, por ruídos derivados de falhas internas ou descargas atmosféricas [31].

Por fim, a utilização do esquema de teleproteção POTT, é adequado para sistemas que incorporem equipamentos de teleproteção digitais aplicados a sistemas de fibra óptica e rádio (multiplexados e diretos). Este sistema precisa fornecer um alto nível de segurança e uma elevada velocidade de resposta.

Na Figura 2.7 é possível observar um esquema simplificado referente a lógica POTT.

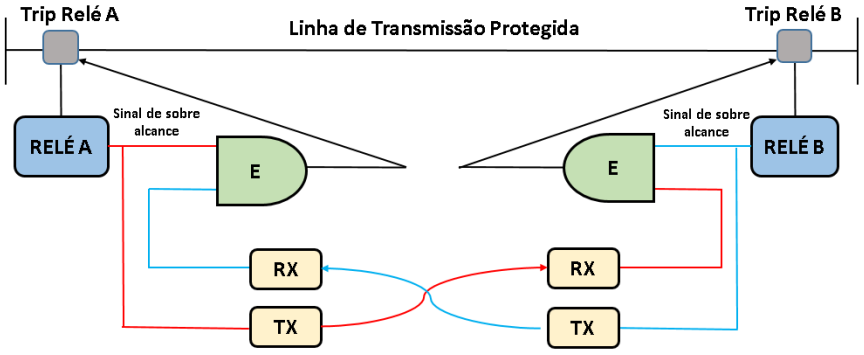


Figura 2.7: Lógica básica para o esquema POTT. Adaptado de [28]

2.4.4 Directional Comparison Blocking (DCB)

O esquema de proteção DCB, em português, sistema de bloqueio por comparação direcional, realiza a utilização do meio de comunicação presente para o envio de um comando de bloqueio ao disjuntor localizado na extremidade da rede. O esquema de proteção em questão é utilizado para impedir a abertura do disjuntor mesmo que as proteções locais assinalem

para sua abertura [28]. A representação do esquema de proteção DCB pode ser observada na Figura 2.8.

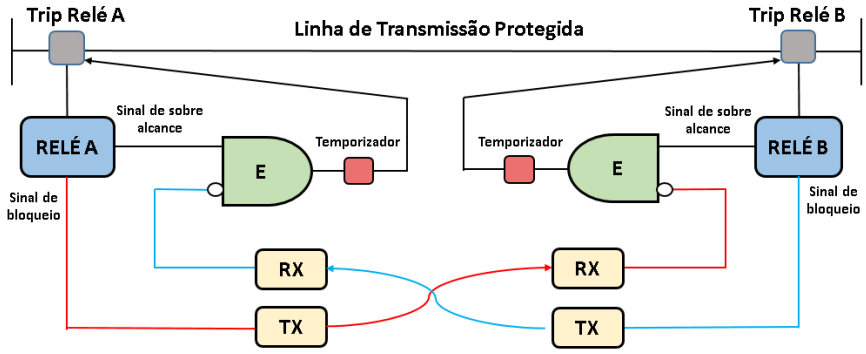


Figura 2.8: Lógica básica para o esquema DCB. Adaptado de [28]

Ao contrário dos esquemas POTT, que enviam um comando de *trip* quando detectam uma falha na direção direta, o sistema DCB utiliza o meio de comunicação presente para o envio de um sinal de bloqueio quando detecta uma falha na direção reversa [32].

Em sua filosofia, quando o elemento de Zona 3 identificar uma falha no sentido reverso, o mesmo direciona um sinal de bloqueio para o disjuntor localizado na extremidade remota, garantindo que a linha não seja acionada em uma falha externa. Caso o elemento de Zona 2 presente no sistema detectar uma falha e não detectar um sinal de bloqueio, ocorrerá o desarme do disjuntor remoto [32].

2.5 Tecnologias de Comunicação para Sistemas de Teleproteção

Como descrito anteriormente, as aplicações de teleproteção se baseiam em tecnologias de telecomunicações responsáveis por interligar equipamentos de proteção que se encontram geograficamente distantes. A comunicação entre os equipamentos é realizada através de lógicas que comparam os estados de cada relé localizados nas extremidades da linha de transmissão.

Diversas tecnologias de comunicação podem ser utilizadas para este propósito. A seguir, uma breve abordagem sobre cada uma delas será realizada.

2.5.1 Power Line Communications (PLC)

As *Power Line Communications* ou *Power Line Carries* são muito populares no setor elétrico [33]. Esta tecnologia utiliza as linhas de transmissão de energia para o envio de

dados, como telecontrole, telemetria, teleproteção, entre outros. Através da mesma, é possível utilizar o meio físico já existente para estabelecer uma comunicação entre duas subestações de forma simultânea com a transmissão de energia, sem que ocorra interferência entre os serviços [34].

Em [35], os autores avaliam os benefícios da tecnologia PLC para as concessionárias de energia, sendo os mais relevantes a robustez, visto que o enlace da tecnologia suporta altos níveis de ruído; confiabilidade, uma vez que quando bem dimensionado, o sistema é capaz de verificar se o sinal recebido é valido ou se trata de um ruído de canal; rapidez, onde o sistema oferece altos valores de taxa de comunicação e por fim a grande cobertura geográfica alcançada por essa tecnologia, dispensando a utilização de dispositivos ou estações intermediarias entre as extremidades do enlace de comunicação.

Em contrapartida, os sistemas baseados na tecnologia PLC requerem um alto nível de manutenção, sendo superior ao demandado por outras tecnologias de comunicação. Além disso, há a probabilidade de que o ruído introduzido por uma falha na linha protegida possa interferir no sinal recebido. Essa interferência é mitigada através do aumento da potência de saída para o estado de comando ou desarme, melhorando a *Signal-to-Noise Ratio* (SNR) do sistema durante condições de falha [32].

De forma simplificada, quando empregado em serviços de teleproteção, a estrutura demandada pelo sistema PLC é constituída por um conjunto de acopladores compostos por caixas de sintonia, capacitores de acoplamento e bobinas de bloqueio [36]. Além disso, o dimensionamento dos componentes deve ser criterioso para que seu funcionamento ocorra adequadamente [37]. Uma representação simplificada do sistema de onda portadora pode ser observado na Figura 2.9.

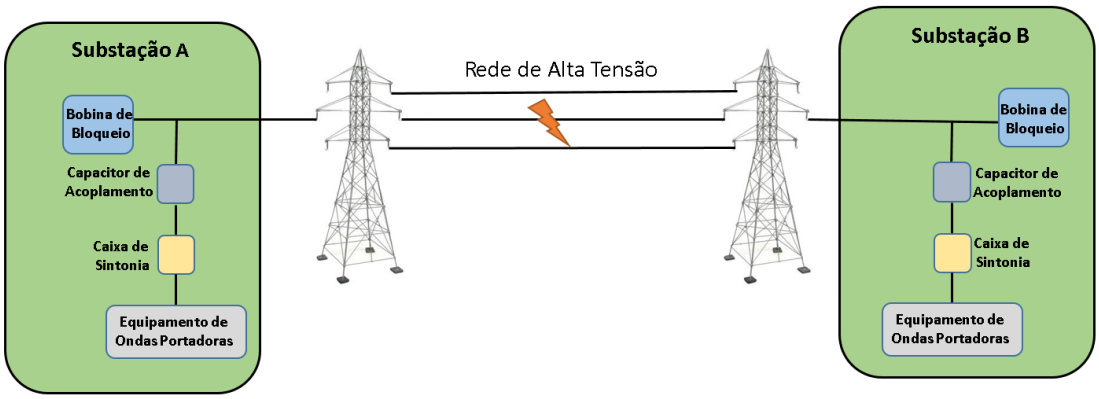


Figura 2.9: Representação de um sistema de onda portadora para teleproteção. Adaptado de [37]

2.5.2 Fibra Óptica

Os sistemas de comunicação baseados em fibra óptica também são amplamente adotados para serviços de teleproteção. Suas características incluem, imunidade a interferência eletromagnética e eletroestática, grande capacidade de transmissão, precisão nos dados transmitidos, ampla largura de banda e grande cobertura geográfica a custo de uma pequena atenuação [38].

Quando empregada em sistemas de teleproteção, a tecnologia de fibra óptica pode atuar através da conexão direta dos dispositivos de proteção, ser multiplexada utilizando tecnologias *TDM* ou ser multiplexada utilizando tecnologias de pacotes.

Na conexão direta, os relés de proteção ou equipamentos de teleproteção são diretamente interligados entre si. Neste tipo de sistema, o sinal elétrico, obtido pelos dispositivos, é dirigido ao transdutor fotoelétrico, que por sua vez o converte em um sinal luminoso equivalente. O sinal obtido, que possui uma determinada frequência dentro do espectro de infravermelho, é enviado através do *link* de fibra óptica até a outra extremidade do sistema, estabelecendo comunicação entre as extremidades da linha protegida [39].

Mediante o recebimento do sinal enviado pelo relé ou equipamento de teleproteção, e de acordo com a lógica de proteção adotada, os dispositivos podem atuar ou não. Neste cenário, os dispositivos também podem bloquear ou permitir a ação de abertura do disjuntor remoto, bem como bloquear o religamento do sistema [21].

Nesta configuração são observadas baixas latências, além de um alto grau de confiabilidade e segurança. Isso ocorre em função da interconexão direta dos dispositivos que utilizam *links* de fibra óptica. Como desvantagem, o sistema apresenta a necessidade de que um par de fibra (transmissão e recepção) seja dedicado para cada conjunto de equipamentos por segmento da linha. Normalmente, não há *links* de fibra suficientes para implementar esse método por toda a rede protegida [21].

Quando empregada para o transporte de tráfego de tecnologias *TDM* e de pacotes, os links de fibra óptica podem utilizar a tecnologia *Dense Wavelength Division Multiplexing* (DWDM) para aumentar o número de aplicações ou circuitos que podem ser transportados por um único par de fibra óptica. No DWDM, o sistema transmite diversos feixes de luz com comprimentos de onda distintos em um mesmo meio físico. O espaçamento entre os canais foi definido pela *International Telecommunication Union* (ITU), através da recomendação ITU-T G 694.1 [40].

Os multiplexadores DWDM não são implantados como dispositivos ponto-a-ponto, mas fornecem conectividade entre muitas subestações e/ou dispositivos conectados à rede de energia. A eficiência do uso de fibra é ainda maior, pois os multiplexadores geralmente possuem aplicações de controle de supervisão e aquisição de dados, do inglês *Supervisory Control and Data Acquisition* (SCADA), acesso de engenharia, telefonia e segurança.

Diferentemente da conexão direta citada anteriormente, os sistemas com multiplexadores inserem novos dispositivos nos sistemas de proteção, tornando o meio mais susceptível a falhas. Para contornar este problema, durante o projeto das topologias, são inseridas re-

dundâncias de *Hardware*. Esses sistemas também aderem topologias em anel, fornecendo rotas alternativas caso o caminho primário seja danificado. Uma representação do sistema de proteção utilizando multiplexadores pode ser observada na Figura 2.10

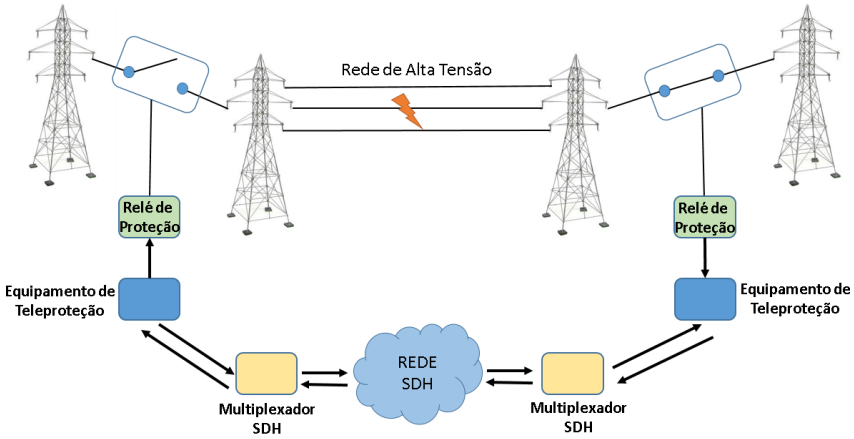


Figura 2.10: Representação de um sistema de teleproteção utilizando fibra óptica. Adaptado de [17]

2.5.3 Plesiochronous Digital Hierarchy (PDH)

Os sistemas de multiplexação de sinais surgiram com o advento das necessidades de expansões nas linhas telefônicas. Inicialmente, 32 canais de voz de 3,4 kHz eram convertidos de analógico para digital com a técnica *Pulse Code Modulation* (PCM) e multiplexados no domínio do tempo. Essa técnica ficou reconhecida pela sigla *PCM/TDM*, sendo amplamente empregada no cenário de missão crítica até os dias atuais.

As redes *TDM* permitem transmitir 32 canais de voz por um único meio, porém em tempos diferentes. Devido à sua natureza de rede quase síncrona, recebeu o nome de multiplexação *Presiochronous Digital Hierarchy* (PDH). O sistema *PDH* utiliza uma hierarquia de sinais digitais. Para esta tecnologia, existem três padrões mundiais diferentes, o padrão Europeu, o Americano e o Japonês.

As soluções *PDH*, ponto-a-ponto, fornecem atraso de propagação e taxas de erros de *bits* menores que os valores especificados para os serviços de teleproteção [41]. Entretanto, o número de saltos nas redes *PDH* podem comprometer o tempo de ação na proteção.

2.5.4 Synchronous Digital Hierarchy (SDH)

Com o crescimento da demanda, ficou claro que os sistemas de 2 Mbps (T1) não seriam suficientes para atender a demanda no tronco da rede. Então, iniciou-se o desenvolvimento de níveis superiores, que seriam utilizados para multiplexar vários sinais T1 em um único

sinal de nível mais alto. Com isso, foi desenvolvida e padronizada pela *American National Standards Institute* (ANSI) a rede *Synchronous Optical Network* (SONET) para ser utilizada nos Estados Unidos [42]. Ao mesmo tempo, na Europa, foi desenvolvida e padronizada pelo ITU-T a tecnologia de comutação de circuitos *Synchronous Digital Hierarchy* (SDH) para ser utilizada internacionalmente [43–45].

A rede *SDH* é constituída de equipamentos que operam de forma síncrona. Cada equipamento possui um relógio escravo interno que deve, diretamente ou indiretamente, ser sincronizado com um relógio de alta estabilidade, chamado de Relógio Primário de Referência. Como as informações são transportadas como fluxos de *bits*, a sincronização dos equipamentos é fundamental para que os diversos sinais sejam multiplexados e demultiplexados adequadamente, com o mínimo de desvio das taxas nominais de cada nível.

Essa característica é essencial para os sistemas de teleproteção presentes no mercado, de forma que as informações cheguem corretamente nas extremidades das linhas de transmissão de energia, evitando o *trip* indevido dos relés [46].

A tecnologia *SDH* possui recursos de comutação automática de proteção, do inglês *Automatic Protection Switching* (APS), que permitem a troca automatizada de canais virtuais por onde os circuitos passam em caso de falha. Entretanto, enlaces virtuais de reserva devem estar disponíveis em um evento de falha, de forma que os mecanismos de proteção possam chaveá-los.

Nesse contexto, canais virtuais com a mesma taxa dos canais operacionais podem ser reservados (técnica conhecida como espelhamento), baixando a utilização da rede para menos de 50%. Esta técnica é utilizada para obter proteção para cada canal de missão critica da rede. [46]

Segundo [47], as soluções que combinam rede de núcleo *SDH* e acesso *PDH* são comumente usadas pelas concessionárias de energia para atender os requisitos de comunicação em redes de alta tensão, incluindo ações de teleproteção e religamento à distância. O *NG-SDH* oferece alta disponibilidade, gerenciabilidade abrangente e muitas funcionalidades de monitoramento da rede, o que é ideal para missão critica.

2.5.5 NG-SDH

Como evidenciado anteriormente, as redes determinísticas se estabeleceram como uma importante tecnologia para as concessionárias de energia. O *SDH* emprega um papel fundamental nas redes de teleproteção, realizando o transporte de informações de uma extremidade à outra da linha protegida.

Para se adaptar a este novo cenário, as instituições de padronização se esforçaram no desenvolvimento de recomendações que, realizassem a padronização de soluções focadas na transmissão de multi serviços através de redes *SDH* de forma eficiente. Assim, a tecnologia SDH evoluiu para o NG-SDH, tornando a rede capaz de realizar o tráfego tanto de dados *TDM* como de pacotes, sendo os dados de pacote baseados no protocolo *TCP/IP* [48].

As três técnicas mais importantes que facilitam a convergência de serviços em redes *NG-SDH* são: *Generic Framing Procedure* (GFP), *Virtual Concatenation* (VCAT) e *Link Capacity Adjustment Scheme* (LCAS).

Definida pela padronização ITU-T G.7041, o *GFP* é uma técnica de multiplexação utilizada para a adaptação de sinais. Essa técnica realiza o mapeamento de qualquer tipo de tráfego para *SDH*, ou para uma rede de transmissão óptica através do *Wavelength Division Multiplexing* (WDM). O *GFP* permite o encapsulamento de quadros de dados, tanto de estrutura fixa quanto variável, e garante a interoperabilidade quando são utilizados equipamentos de diferentes fabricantes [49].

Definida através das padronizações ITU G.707/Y.1322 e G.78, o *VCAT* é uma técnica de multiplexação inversa que permite a combinação de vários canais de baixa velocidade em um canal agregado de velocidade superior. Isso é realizado com o intuito de se obter um aumento proporcional na largura de banda disponível para o link agregado. Através dessa técnica, é possível alcançar uma maior eficiência do transporte de dados quando comparado com o modelo *SDH* de largura de banda fixa.

Por fim, definida através da padronização ITU G.7041/Y.1305. O LCAS é um protocolo que fornece ajustes de largura de banda do *VCAT*, através de requisições vindas do *Network Management System* (NMS) [50].

Em [51], é comprovada a vantagem do *NG-SDH*, em termos de utilização dos enlaces, quando comparada a uma solução com *SDH* puro. A solução *NG-SDH* permite transportar tráfego determinístico e estatístico no mesmo equipamento. Entretanto, as redes *NG-SDH* e *PDH* possuem alto custo operacional [47].

2.5.6 Multiprotocol Label Switching (MPLS)

Desenvolvido inicialmente pelo IETF através da RFC 3031, a solução *MPLS* é uma tecnologia de encaminhamento de pacotes localizada entre as camadas 2 e 3 do modelo *Open System Interconnection* (OSI) [6]. O *MPLS* se propõe, de forma inteligente, a agregar as vantagens do roteamento, com a eficiência e a reserva de recursos existentes nas redes de comutação de pacotes baseadas em circuito virtual.

A tecnologia *MPLS* é baseada em um sistema de rotulamento dimensionado para compor múltiplos protocolos. Ao contrário das redes *IP* tradicionais, que avaliam os cabeçalhos presentes na camada 3, o *MPLS* utiliza o seu sistema de rotulamento para a tomada de decisão assim que um novo pacote adentra na rede. Sendo esta, uma característica que o torna independente dos protocolos da camada 3 do modelo *OSI* [52].

Em sua estrutura, a rede é composta por dois tipos de roteadores, sendo eles *Label Edge Router* (LER) e *Label Switch Router* (LSR). OS LERs estão localizados na borda da rede e possuem a função primaria de classificar e selecionar os *labels* adequados para cada fluxo de dados entrante. No mais, estes roteadores possuem a função de remover os *labels* na saída da rede. Neste cenário, os *LERs* realizam a conversão de pacotes *IP* em pacotes *MPLS* e vice-versa.

Em contrapartida, Os *LSRs* estão localizados no núcleo da rede, sendo estes, comutadores de alta velocidade, cujo principal objetivo é encaminhar pacotes rapidamente [52].

Um *LSP* é um caminho definido através de uma sequência de *labels* entre dois *LERs*. Todos os pacotes pertencentes a um *LSP* seguem o mesmo caminho pré-definido. Uma estrutura de rede *MPLS* genérica pode ser observada na Figura 2.11

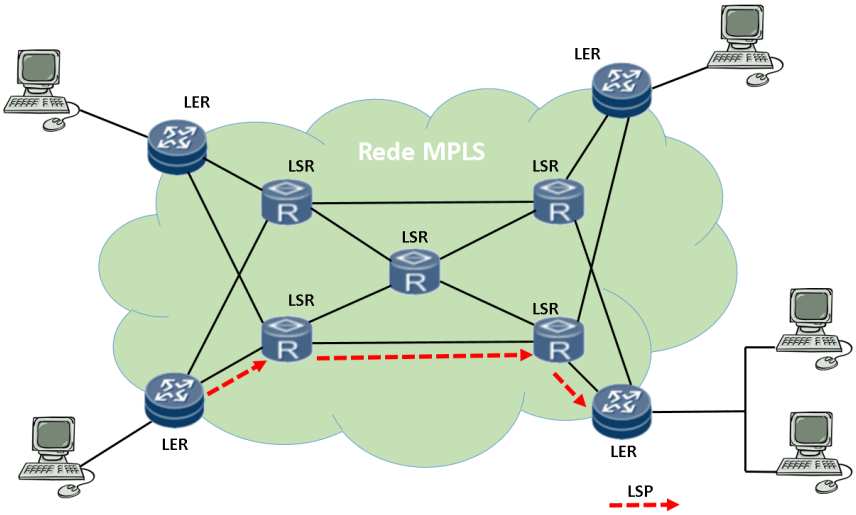


Figura 2.11: Topologia *MPLS* genérica. Adaptado de [52]

O cabeçalho *MPLS* possui os campos *Label Value*, *Traffic Class* (TC), *Botton of Stack* (S) e *Time to Live* (TTL), sendo composto por um total de 32 bits, como pode ser observado na Figura 2.12 [53].

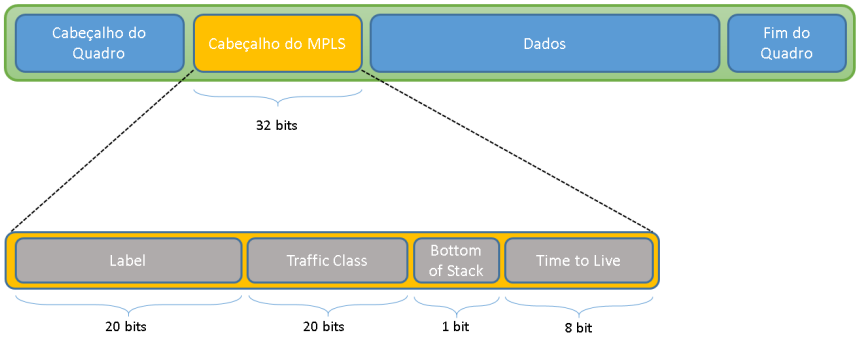


Figura 2.12: Estrutura do quadro *MPLS*. Adaptado de [52]

Um *label MPLS* é um pequeno identificador de circuito virtual de tamanho fixo (20 *bits*). O campo *TC* é formado por 3 *bits*, sendo responsável por mapear informações da arquitetura de serviços diferenciados para o *MPLS*. O campo *S* é composto por 1 *bit* e é utilizado no

empilhamento de pacotes para identificar o último *Label MPLS*. Por fim, o campo *TTL* é composto por 8 *bits*, sendo utilizado para identificar o número máximo de saltos que um pacote pode realizar na rede antes de ser descartado, evitando situações de *looping* [53].

Para classificar os pacotes que pertencem a um *LSP*, utiliza-se as *Forwarding Equivalence Class* (FECs). Todos os pacotes pertencentes a uma *FEC* recebem o mesmo tratamento. Várias *FECs* podem ser utilizadas para classificar o tráfego de um *LSP*. Quando um *LSP* transporta o tráfego classificado por mais de uma *FEC*, o campo *TC* é utilizado para identificar a qual *FEC* pertence o pacote.

Este *LSP* é chamado de *EXP-Inferred* LSP (E-LSP). Como o campo *TC* possui três bits, podem ser definidas até 8 *FECs* em um *LSP*, sendo associado um tronco a cada uma. Este tronco é utilizado para definir como será o monitoramento e o escalonamento dos pacotes pertencentes a cada *FEC* do *LSP* [53].

De forma geral, o *MPLS* oferece aos seus clientes diversas vantagens, tais como roteamento explícito de pacotes; criação de *Virtual Private Netwoks* (VPNs); suporte a múltiplos protocolos, *links* e a todos os tipos de tráfegos; facilidade de evolução e roteamento interdomínio [54].

No entanto, o MPLS possui inúmeras deficiências quando implementado em redes de transporte. Essa ineficiência abriu caminho para o desenvolvimento do *Multiprotocol Label Switching - Transport Profile* (MPLS-TP), que será abordado a seguir.

2.5.7 Multiprotocol Label Switching - Transport Profile (MPLS-TP)

Tradicionalmente construída através de dispositivos *TDM* como *SDH/SONET* e *PDH*, as redes de transporte se tornam muito complexas, ineficientes e onerosas quando construídas através de redes de pacotes tradicionais. Isso se deve aos requisitos exigidos pelas redes de transporte, tais como QoS de ponta a ponta; funções de *Operations, Administration, and Management* (OAM) para a identificação e isolação de falhas, bem como mecanismos de restauração de falhas rápidos que minimizem a quantidade de informações perdidas [55].

Buscando o desenvolvimento das extensões necessárias, para que a tecnologia *MPLS* contemple os requisitos exigidos pelas redes de transporte, o *IETF* em conjunto com o *International Telecommunication Union-Telecommunication Standardization sector* (ITU-T) iniciaram o desenvolvimento da tecnologia *MPLS-TP* [56]. Tendo em vista os requisitos citados anteriormente, os objetivos almejados pelo *MPLS-TP* são: Permitir a implantação da tecnologia *MPLS* em uma rede de transporte, de forma a operar de maneira semelhante às tecnologias *TDM* existentes (*SDH/SONET*), além de fornecer ao *MPLS* suporte para serviços de transporte de pacotes com um grau semelhante de previsibilidade, confiabilidade e *OAM* empregados nas redes *TDM* [57].

Algumas funções como *Penultimate Hoping Popping* (PHP), *LSP MERGE* e *Equal Cost MultiPath* (ECMP) utilizadas no *MPLS* tradicional para otimizar o roteamento *IP* sobre os

LSPs foram desativadas no *MPLS-TP*, com o intuito de tornar a rede a mais determinística possível.

Implementada nas redes *MPLS* para a redução da carga de processamento nos *LERs*, a função *PHP* é referente ao processo onde o *LSR* retira o *label* mais externo de um determinado pacote, antes que o mesmo seja encaminhado ao *LER* adjacente. Essa função foi removida no *MPLS-TP* uma vez que o último *label* agora é utilizado para funções de *OAM*.

A função *LPS Merge* é empregada no *MPLS* para realizar a combinação de *LSPs* que possuam um destino em comum. Essa função garante ao sistema uma redução de carga no processamento e um aumento na velocidade de transmissão de dados. Porém, no *MPLS-TP* não ocorre a combinação entre os *LSPs*, pois cada identificação se mantém do inicio ao fim do percurso, invalidando a utilização desta função [58].

Introduzido para o balanceamento de carga de tráfego no *MPLS*, a função *ECMP* permite que o tráfego direcionado para um mesmo destino seja compartilhado por vários caminhos com o mesmo custo. Assim como nas redes determinísticas, o *MPLS-TP* oferece suporte apenas para *LSPs* bidirecionais congruentes, ou seja, o *LSP* utilizado para o envio de uma informação necessariamente deve ser o mesmo utilizado para o recebimento de uma outra informação.

Além disso, no *MPLS-TP* não é permitida a combinação de *LSPs*. Essas características impedem que ocorra o balanceamento de carga utilizando múltiplos percursos, porém oferece ao sistema características de tráfego determinístico. No mais, fornecem aos provedores uma maior capacidade de monitoramento de tráfego na rede [58].

Apesar de algumas funções serem retiradas, para garantir um maior determinismo da rede, o *MPLS-TP* ainda mantém algumas características do *MPLS* tradicional. As quais, garantem uma maior eficiência do sistemas, tais como a arquitetura MPLS/PWE3, o plano de controle dinâmico e o encaminhamento de *labels*.

Como descrito anteriormente, o *MPLS-TP* agrega ao tradicional características como caminhos bidirecionais e convergentes, *LSPs* estáticos e funcionalidades de *OAM*. Uma comparação entre o *MPLS* tradicional e o *MPLS-TP* pode ser observado na Figura 2.13.

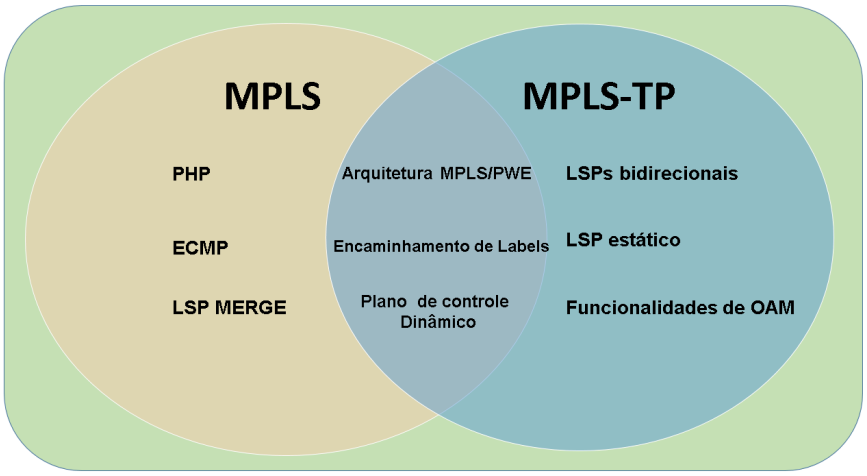


Figura 2.13: Correlação entre o *MPLS* tradicional e o *MPLS-TP*. Adaptado de [58]

2.6 Soluções Proprietárias Avaliadas

Nesta seção, será realizada uma descrição conceitual das tecnologias proprietárias utilizadas durante o desenvolvimento deste trabalho. Primeiramente, será abordada a tecnologia *IP Hard-Pipe*, apresentando suas principais características e premissas. Em seguida, de forma análoga à anterior, será apresentada a tecnologia *Flex-LSP*.

2.6.1 Solução - *IP Hard-Pipe*

Definida através da RFC 7625, a solução busca oferecer um serviço de transporte baseado em tecnologias de pacotes (*IP/MPLS*) que ofereça uma rede flexível de alta confiabilidade e estabilidade, assim como as redes legadas determinísticas [59].

Essa solução prevê a divisão da rede física em dois planos, sendo eles o *Hard-Pipe* e o *Soft-Pipe*. O *Hard-Pipe* é destinado ao fornecimento de serviços de alta prioridade, garantindo baixos valores de latência e uma grande largura de banda. Já o *Soft-Pipe* executa serviços básicos para o cliente, implementando o *QoS* do *MPLS* para o compartilhamento de banda [60].

Além disso, essa tecnologia atua com a premissa de que os planos sejam isolados um do outro, de forma que um congestionamento nos serviços prestados pelo *Soft-Pipe* não afete os serviços localizados no *Hard-Pipe*. Apesar deste isolamento, a solução oferece a possibilidade de ajuste nas capacidades de largura de banda de ambos os planos a qualquer momento. Uma representação da solução pode ser observada na Figura 2.14.

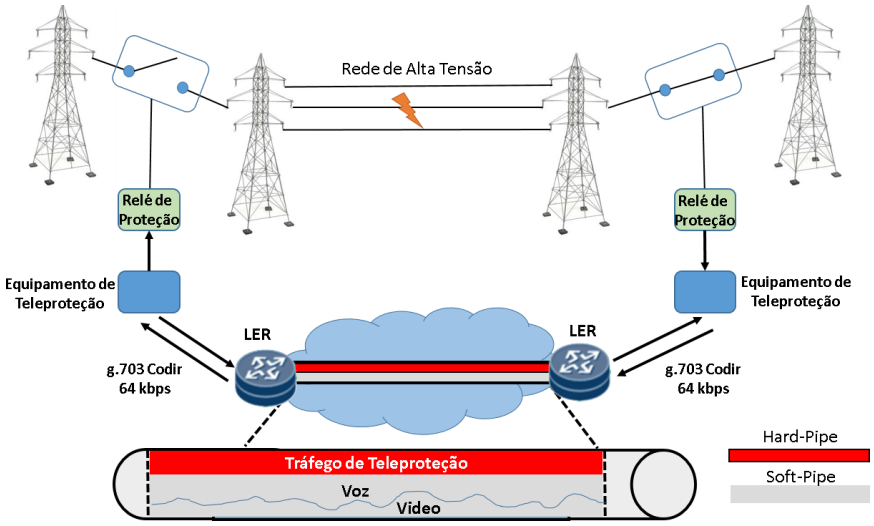


Figura 2.14: Solução *Hard-Pipe* aplicada em sistemas de teleproteção. Adaptado de [60]

Os roteadores da família NE, utilizados para a implementação da tecnologia *Hard-Pipe*, quando conectados a equipamentos de teleproteção que possuam interfaces E1/C37.94 ou outros tipos de interface *TDM*, utilizam da tecnologia *PWE3* para realizar a transmissão de tráfego *TDM* sobre a rede de pacotes. O suporte à tecnologia *Synchronous Ethernet* (SyncE) garante que os sinais de *clock* sejam transmitidos através de *links* Ethernet, permitindo o sincronismo de frequência dos sinais *TDM* de ponta a ponta [60].

Para garantir valores aceitáveis de latência e latência assimétrica, os roteadores utilizam *pseudo wires* sobre *LSPs* bidirecionais estáticos e co-roteados para a transmissão dos dados de teleproteção. Esta solução é empregada para oferecer um controle semelhante ao utilizado pelos serviços *TDM* em teleproteção. Para garantir a comutação rápida do canal primário para um alternativo (*failover*), os roteadores contam com o *OAM* do *MPLS-TP* ou com o protocolo de rede *Bidirectional Forwarding Detection* (BFD) [60].

2.6.2 Solução - *Flex-LSP*

Também conhecida como *LSP* bidirecional associado, essa solução se baseia na combinação do *MPLS-TP* estático bidirecional e do *MPLS-TE* dinâmico. O *Flex-LSP* são instâncias *LSPs*, em que os caminhos bidirecionais são configurados, monitorados e protegidos de forma independente, sendo estes sempre associados a uma sinalização. A solução utiliza o *Resource Reservation Protocol*(RSVP) para vincular os *LSPs* bidirecionais, com o intuito de criar um túnel TE bidirecional co-roteado [61].

O *Flex-LSP* permite a associação de um túnel *MPLS-TE* a um *LSP MPLS-TE* ativo. Desta forma, é possível realizar a proteção do *LSP* em funcionamento e garantir a redundância do *link* operante. Portanto, quando um *LSP* ativo apresenta uma falha, interrompendo a

troca de dados, o *LSP* de proteção é ativado automaticamente [61].

Para a garantia de uma comutação rápida entre os *links* primário e secundário, que atenda os requisitos de teleproteção, é necessária a habilitação da proteção *WRAP*. Através dela, cada *LSP* sinaliza mediante a um *label WRAP*, o canal secundário que deve ser tomado caso ocorra a falha do *link* principal [61].

Mediante a estas informações, a configuração dos *Flex-LSPs* co-roteados utilizados para os cenários de teleproteção, são realizadas através de cinco passos, sendo eles, habilitação da engenharia de tráfego básica do MPLS nos roteadores e no RSVP; configuração do *flex* LSP; habilitação da proteção WRAP; habilitação do gerenciamento de falhas OAM; e por fim, realização do mapeamento dos *pseudo-wires* para os tuneis *Flex-LSP* específicos.

Uma representação simplificada da solução Flex-LSP pode ser observada na Figura 2.15.

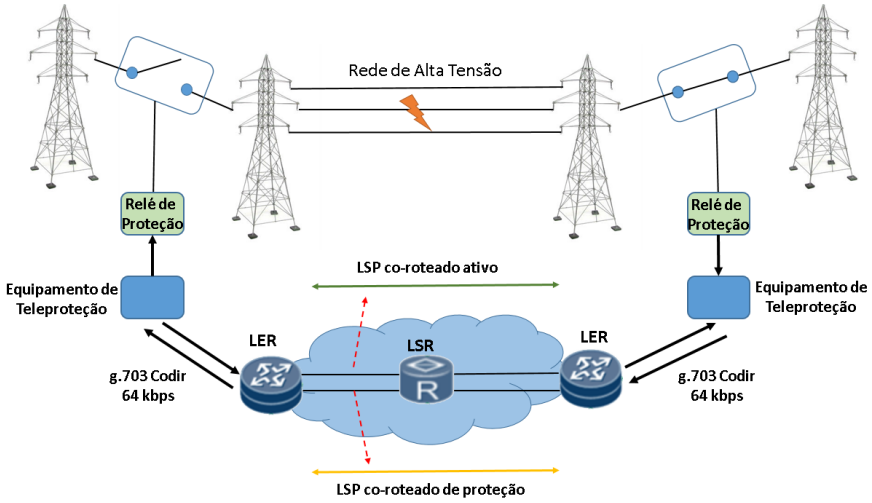


Figura 2.15: Solução *Flex-LSP* aplicada em sistemas de teleproteção. Adaptado de [61]

2.7 Requisitos de Teleproteção

O bom desempenho do sistema de teleproteção é alcançado quando os requisitos de segurança, confiabilidade e velocidade são atendidos. Assim, cada esquema de teleproteção possui diferentes exigências relacionadas ao canal de comunicação, de forma a garantir seu bom funcionamento e atender o desempenho desejado do sistema. Nesta seção, serão abordados os principais requisitos empregados nos sistemas de teleproteção.

2.7.1 Regulamentação do Operador Nacional do Sistema Elétrico (ONS)

Criada em 26 de agosto de 1998, o ONS atua como o órgão governamental responsável por coordenar e controlar as operações de geração e transmissão de energia elétrica no Sistema Interligado Nacional (SIN). Também é de responsabilidade da ONS o planejamento das operações dos sistemas isolados do país, sendo estes executados sob a fiscalização da Agência Nacional de Energia Elétrica (ANEEL) [62].

A Lei nº 9.648/98, em seu Artigo 13, alínea "f", com redação dada pela Lei nº 10.848/2004, estabelece como atribuição do ONS, propor regras para a operação das instalações de transmissão da rede básica do SIN a serem aprovadas pela ANEEL. As regras descritas anteriormente são consolidados nos documentos denominados "Procedimentos de rede", sendo estes responsáveis por estabelecer os requisitos técnicos necessários para garantir o livre acesso às instalações de transmissão de energia, realização das atividades de planejamento, programação da operação eletro energética, entre outros [62].

Dentro dos procedimentos de rede, o módulo 2 intitulado "Requisitos mínimos para instalações de transmissão e gerenciamento de indicadores de desempenho" é responsável por definir os requisitos mínimos para as instalações de transmissão. Sendo assim, capaz de estabelecer a sistemática para o gerenciamento dos indicadores de desempenho e das funções de transmissão da rede básica [62].

O submódulo 2.6 intitulado "Requisitos mínimos para os sistemas de proteção, de registro de perturbações e de teleproteção" [63], assim como descrito em seu nome, é responsável por estabelecer os requisitos mínimos para os sistemas de teleproteção. No que se refere aos sistemas de teleproteção de linhas de transmissão de energia, o submódulo 2.6 enfatiza três pontos, sendo estes:

- Os canais de teleproteção dedicados específicos para proteção, não podem ser compartilhados com outras aplicações [63];
- Os esquemas utilizados para teleproteção devem ser independentes e redundantes para as proteções principal e alternada, utilizando meios físicos distintos para a transmissão das informações [63];
- Os esquemas de transferência de disparo devem ser independentes e redundantes para a proteção primária e alternada [63].

2.7.2 Norma IEC 60834

A norma IEC 60834 foi desenvolvida pela *International Electrotechnical Commission* (IEC), tendo como principal objetivo a avaliação de desempenho e a elaboração de testes para os equipamentos de teleproteção presentes nos sistemas de energia. A norma avalia a comunicação dos dados associados aos equipamentos de proteção, sendo estes referentes a grandezas elétricas como amplitude e fase.

Essa norma é dividida em duas partes, denominadas IEC 60834-1 [64] e 60834-2 [65], onde a parte 1 se refere aos sistemas de comando e a parte 2 se refere aos sistemas de comparação analógica. Ambas serão detalhadas a seguir.

A parte 1 aborda os sistemas de telecomunicações utilizados para o envio de comandos, operando em conjunto com os equipamentos de teleproteção. Em seu conteúdo são estabelecidos requisitos de desempenho e metodologias de testes para os diferentes tipos de comandos utilizados em equipamentos de teleproteção (Esquemas de disparo permissivos, *trip* direto e bloqueio). Estes, podendo conter informações no formato digital ou analógico [64].

Já a parte 2 aborda os requisitos de desempenho e metodologias de teste para os equipamentos de teleproteção de comparação analógicos, sendo esses utilizados para conexão com os sistemas de proteção de redes de energia. Esta parte se aplica a sistemas de banda estreita e banda larga, onde a primeira se limita a operações dentro de uma banda de 4 kHz e a segunda a operações acima de 4 kHz. Os meios são utilizados para a transmissão de informações analógicas referentes a grandezas primárias como amplitude e fase [65].

Os principais requisitos presentes na norma podem ser observados na Tabela 2.1.

Tabela 2.1: Requisitos de teleproteção presentes na norma IEC 60834-1. Adaptado de [64]

Requisitos de Teleproteção	**Valores**	**Observações**
Tempo de transmissão máximo	10 ms	Para os meio de comunicação digitais
Qualidade de Canal	BER mínimo de $10^{-6} bps$	Período de 10 segundos consecutivos
Segurança	Comandos de bloqueio 10^{-4} Comandos permissivos 10^{-7} Comandos diretos 10^{-8}	*
Confiabilidade	Comandos de bloqueio 10^{-3} Comandos permissivos de subalcance 10^{-2} Comandos permissivos de sobrealcance 10^{-3} Comandos diretos 10^{-4}	**
Assimetria de canal	inferior a 4 ms	

Tomando como referência a Tabela 2.1, o requisito de tempo de transmissão máximo representa o tempo decorrido entre o instante da mudança de estado na entrada e o instante de mudança de estado na saída do comando. Nele estão incluídos o tempo de propagação pela rede de telecomunicação e os possíveis atrasos adicionais provenientes de ruídos.

O requisito de qualidade de canal representa a taxa de erros de *bits* aceitável nos canais de teleproteção. A taxa de erros de *bits* indica a proporção de *bits* recebidos de forma errônea, pelo total de *bits* que são enviados durante um intervalo de tempo específico.

A segurança representa a capacidade do sistema em evitar que interferências e ruídos ocasionem uma mudança de estado na extremidade receptora quando nenhum comando é transmitido. Desta forma, o requisito de segurança é calculado através da Equação 2.1:

$$1 - \frac{N_T - N_R}{N_T} \tag{2.1}$$

Sendo NT o número de comandos enviados e NR o número de comandos recebidos.

A confiabilidade está relacionada a capacidade do sistema em enviar e receber um comando valido na presença de interferência ou ruído. O requisito de confiabilidade é calculado através da Equação 2.2:

$$1 - \frac{N_{uc}}{N_B} \tag{2.2}$$

Sendo Nuc o número de comandos errôneos registrados e NB o número de rajadas de erros.

Por fim, a assimetria de canal é representada pela diferença máxima entre os tempos de propagação dos comandos de teleproteção na direção de transmissão e recepção. Este requisito se apresenta de forma crítica para os sistemas de proteção diferencial. Isto se deve a característica do sistema, que realiza a medição do atraso de ida e volta e assume que o atraso unidirecional é a metade deste valor.

Capítulo 3

Trabalhos Relacionados

Neste capítulo será realizado um levantamento dos principais trabalhos relacionados ao tópico de teleproteção de redes de energia via tecnologias de comunicação com multiplexação estatística.

Em [66], Rahman et al. reportam os resultados dos testes utilizados na preparação da migração de relés de proteção de subestações da *San Diego Gas & Electric* (SDG&E) de *SONET* para *MPLS*. Os testes apresentados no artigo foram realizados tanto em laboratório quanto em modelo de simulação usando o *Real Time Digital Simulator* (RTDS). O artigo apresenta os requisitos para teleproteção e destaca como o *MPLS* fornece técnicas para garantir mínima assimetria, roteando e transmitindo caminhos de teleproteção sobre os mesmos nós da rede de dados. Uma metodologia de como aplicar *MPLS* em teleproteção é fornecida. Os autores concluem que as redes *MPLS* são um meio de comunicação viável para o tráfego de telecomunicações de relés de proteção se projetados adequadamente, considerando a latência, a assimetria, *failover* e a disponibilidade.

Em [67], Tan e Cole descrevem a experiência de uma empresa de energia australiana em realizar o transporte de tráfego de teleproteção via *MPLS* através de uma rede física compartilhada. Neste trabalho, são apresentados os estados de expansão da rede da empresa de energia, desde uma rede *MPLS* simples a uma rede *MPLS* transportando diversos serviços de dados e, por fim, o cenário atual onde o serviço de teleproteção é transportado junto com os demais serviços de dados. Os requisitos operacionais, motivação comercial e a abordagem adotada também são apresentados. Testes de laboratório foram realizados com o intuito de verificar a adequação do sistema proposto aos requisitos apresentados anteriormente, onde foram verificados os valores de latência do comando de teleproteção trafegando sobre a rede *MPLS* compartilhada. Por fim, os autores concluem que o modelo implementado pela empresa é um método simples, econômico e eficiente de se implementar teleproteção sobre uma rede *MPLS* já existente.

Em [68], Bächli et al. apresentam uma visão de como as redes de teleproteção podem ser implementadas através de redes de pacotes sem que os principais parâmetros de desempenho das aplicações sejam afetados. Neste trabalho, são avaliados os sistemas de proteção de

distância e diferencial. A proteção de distância é abordada via aplicação de uma *Interworking Function* (IWF), baseada em um gerador de pacotes que é independente da estabilidade da fase do sistema. A proteção diferencial é abordada através de dois cenários: o primeiro através da emulação de circuitos utilizando o *Structure-Agnostic Time Division Multiplexing over Packet*(SATop)/*Circuit Emulation Service over Packet-Switched Network*(CESoPSN) e o segundo apresentando uma nova abordagem para a emulação de circuitos, utilizando *clocks* explícitos. Para a validação das propostas, foram realizados testes em laboratório apoiados por resultados obtidos em campo. Os resultados obtidos foram satisfatórios, comprovando a capacidade e o desempenho das soluções apresentadas.

Em [69], Robertson et al. apresentam uma solução de rede de transporte determinística que oferece baixos valores de latência para o transporte de tráfegos de serviços críticos. A solução apresentada é testada com as tecnologias MPLS e *Carrier Ethernet*. Para a validação da solução, foram realizados testes em laboratório, contribuindo para avaliar o desempenho nos principais requisitos de teleproteção, tais como Latência, assimetria de canal e *Jitter*. O cenário de teste foi dimensionado através de um par de relés diferenciais de corrente com interfaces IEEE C37.94 [70], utilizados para o estabelecimento do circuito de teleproteção diferencial através de uma rede estatística. Os resultados apontaram que a solução se mostrou eficiente para o envio de comandos críticos na rede sem afetar o desempenho do sistema.

Em [71], Blair et al. investigam a utilização da tecnologia *IP/MPLS* para o serviço de proteção diferencial de corrente. Os autores se atentaram principalmente para os rigorosos requisitos de teleproteção (baixa latência, *jitter* e latência assimétrica) e para a necessidade de segurança no envio do tráfego de teleproteção. Para a solução destes itens, duas metodologias são propostas: a primeira é um mecanismo de criptografia em tempo real para tráfegos de teleproteção sobre *IP/MPLS* e a segunda é uma metodologia para a compensação de latência assimétrica devido ao *Jitter* apresentado pelas redes de pacotes. Um cenário de testes contendo simuladores RTDS, relés de proteção e roteadores *IP/MPLS* é utilizado para a validação das soluções. Por fim, foi constatado que os serviços de teleproteção podem ser criptografados em tempo real sem que o desempenho do sistema seja impactado significativamente e também que a metodologia imposta para a compensação de latência se mostrou eficiente, eliminando o impacto do *jitter* e da latência assimétrica na rede de comunicação.

Em [72], Moreira apresentou um estudo realizando a comparação entre os sistemas *TDM(SDH)* e Ethernet(*MPLS-TP*) para o envio de sinais de teleproteção. Testes em laboratório e estudos teóricos foram utilizados para garantir a viabilidade técnica dessas aplicações. Foram realizados testes de proteção de distância e proteção diferencial. Para isso, foram utilizados relés de proteção, quatro multiplexadores FOX615 da empresa ABB ligados em anel e equipamentos para a medição e obtenção dos resultados. Os resultados obtidos verificaram a possibilidade de se utilizar tecnologias de pacotes para o envio de sinais de teleproteção pela rede de missão crítica.

Em [73], Adrah et al. propõem uma solução para mitigar os problemas de variação de latência e perda de pacotes em sistemas de teleproteção que utilizam a tecnologia Ethernet para a comunicação. Essa solução é baseada na adequação do princípio de comutação de pacotes FUSION para os serviços de teleproteção. Desta forma, busca-se atingir a qualidade

de serviço que é oferecida pelos meios de comunicação determinísticos, como baixos valores de latência, perdas de pacotes e variações nas latências. Todo o processo de avaliação da solução é realizado através de simulações, sendo estas realizadas através do simulador NS-3. Os resultados obtidos demonstram que a utilização desta solução podem garantir valores de latência fixos e variações de latência e perdas de pacotes zero para o sistema de proteção. Para os tráfegos de baixa prioridade, os autores mostram que através de um bom dimensionamento da rede é possível adequar seus valores de latência para níveis aceitáveis.

Apesar do foco deste trabalho se tratar da utilização de sistemas de proteção para as linhas de transmissão de energia, também é possível verificar na literatura, trabalhos que abordam a utilização dos sistemas de proteção para aplicações de *smart grids*. Em [74], Wei et al. verificaram as dificuldades de segurança encontrada pelas redes de distribuição com a chegada das *smart grids* e expõem a importância da proteção de relés no cenário das redes inteligentes. O conceito de proteção de área ampla, do inglês *Wide Area protection*, e a estrutura de proteção são avaliados, juntamente com uma análise do principio e as características do algorítimo de proteção de área ampla para os cenários de distribuição de energia nas *smart grids*.

Com o desenvolvimento das *smart grids* e a ampla utilização das redes de média tensão para a interconexão das fontes de energia renováveis, se torna cada vez mais necessária a reavaliação e o ajuste das proteções de relés de sobrecorrente existentes. Pensando nisso, Mehmed-Hamza e Stanchev [75] avaliaram os requisitos de seletividade e sensibilidade do sistema de proteção de sobrecorrente, quando submetido a falhas, na interconexão das fontes de energia renováveis as redes de média tensão. Outros artigos que abordam o tema de redes estatísticas para os serviços de teleproteção de linhas de energia podem ser observados nas referências [76–79]

Capítulo 4

Metodologias e Cenários de Avaliação

Neste capítulo serão apresentados os cenários de testes empregados para a avaliação de desempenho de um sistema de teleproteção utilizando as tecnologias *IP Hard-Pipe* e *Flex lSP* descritos na Seção 2.6.

Primeiramente, são apresentados os equipamentos utilizados, juntamente com uma topologia de testes genérica, realizando uma breve descrição da função de cada equipamento nesta topologia. Posteriormente, é fornecido um detalhamento dos cenários avaliados para cada uma das soluções, evidenciando suas topologias, pré-requisitos, procedimentos de execução e resultados esperados.

4.1 Topologia Genérica e Equipamentos Utilizados

Os testes foram realizados em um laboratório fornecido pela empresa CEMIG, localizada no Bairro Camargos da cidade de Belo Horizonte. O laboratório foi responsável por fornecer a infraestrutura necessária para a instalação de *racks*, roteadores, equipamentos de teleproteção, entre outros dispositivos essenciais para o prosseguimento dos experimentos. A Tabela 4.1 apresenta os equipamentos utilizados durante a elaboração dos cenários previstos no caderno de testes.

Tabela 4.1: Equipamentos disponibilizados para a execução dos cenários.

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**

Os cenários de testes foram elaborados com o intuito de simular, em laboratório, as principais situações presentes em campo, referentes aos sistemas de teleproteção de linhas de transmissão de energia. O principal objetivo dos testes é a verificação do desempenho de tecnologias *IP*, com ênfase em *IP/MPLS*, como solução de meio de comunicação, em comparação às redes existentes nas concessionárias, como por exemplo, *PLC*, *TDM* e óptica.

Os *links* entre os roteadores presentes nos cenários, que serão apresentados nas seções a seguir, utilizam fibra óptica, visando simular a utilização de cabos *Optical Ground Wire* (OPGW), *All-Dieletric Self-Supporting* (ADSS) e *DWDM* presentes nas redes das concessionarias.

De forma geral, as topologias são compostas por seis roteadores interligados em anel, uma maleta de comandos de teleproteção, dois equipamentos de teleproteção, relógio externo e conversores utilizados para adequação das interfaces nos roteadores (sua utilização será detalhada durante a apresentação dos cenários de teste) . Uma topologia genérica pode ser observada na Figura 4.1.

Nesta topologia, os comandos de teleproteção são normalmente enviados pelo *link* principal, representado pela conexão direta entre os roteadores 1 e 6, com o intuito de simular as extremidades da linha de transmissão a ser protegida entre as subestações. O caminho alternativo é composto por seis roteadores e é responsável por trafegar os comandos de teleproteção quando o caminho principal estiver inoperante.

Com isso, é possível representar um sistema com proteção principal e proteção alternativa através de um caminho secundário interligado em anel, respeitando as exigências estabelecidas pela *ONS* no submódulo 2.6 [62].

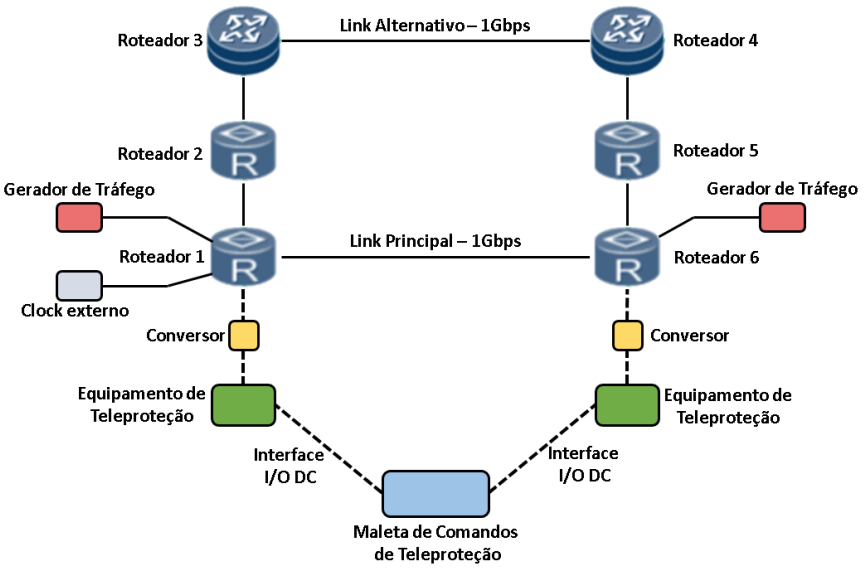


Figura 4.1: Topologia de testes de teleproteção genérica.

A maleta de comandos de teleproteção utilizada durante os experimentos foi desenvolvida pelos funcionários da CEMIG, e tem o objetivo de reproduzir os comandos enviados pelos relés. Através de sua interface gráfica, é possível configurar o número de amostras, os tipos de comandos (DUTT, PUTT, POTT e DCB) que serão enviados, o tempo de duração de cada amostra e o intervalo entre o envio de cada uma delas.

Vale ressaltar que a maleta realiza a configuração dos tipos de comandos em pares, ou seja, dois comandos DUTT e dois PUTT, dois DUTT e dois DCB, quatro DUTT, quatro DCB e assim por diante. Ao final dos experimentos, a interface possibilita a criação de uma tabela com o valor de latência referente a cada comando enviado do equipamento de teleproteção A para o equipamento B, além dos valores de média e variância do conjunto de comandos estipulados pelo usuário no inicio do teste. Por fim, um gráfico é reproduzido em tempo real, apresentando os valores obtidos para cada um dos comandos enviados. A maleta e sua interface podem ser observadas na Figura 4.2.

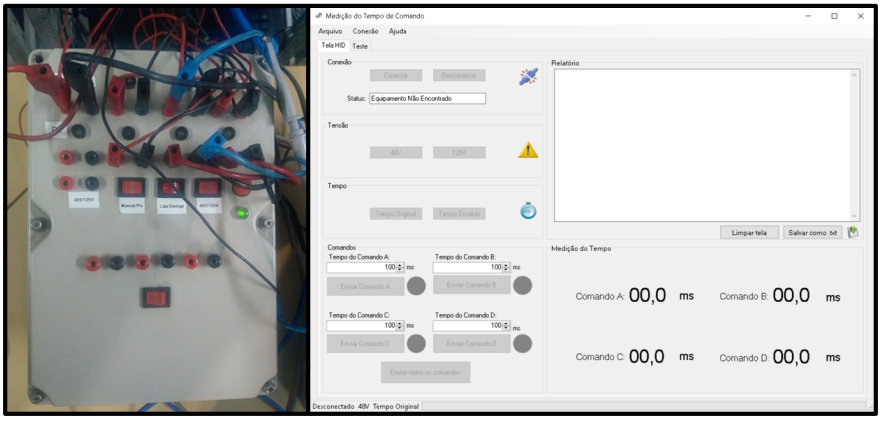


Figura 4.2: Equipamento utilizado para o envio dos comandos de teleproteção e sua interface gráfica.

Os equipamentos de teleproteção possuem a função de realizar a transferência dos comandos de um equipamento de teleproteção A para um B de forma rápida, segura e confiável. Estes equipamentos também devem possibilitar o envio dos comandos através de uma grande gama de mídias de comunicação, como digitais, analógicas e ópticas. Para estes experimentos foi utilizado o equipamento DIP 5000 da empresa Alstom.

A geração de tráfego na rede foi realizada com o objetivo de verificar a capacidade do sistema em se manter dentro dos requisitos estipulados pelas normas, mesmo quando submetido a diferentes tipos de tráfego de dados de naturezas distintas, não degradando o desempenho do circuito de teleproteção configurado na rede *IP*. Inicialmente, foi utilizado o aplicativo computacional *Jperf* e, posteriormente, o equipamento TSW900ETH da empresa Wise. A interface do aplicativo computacional *Jperf* e o equipamento TSW900ETH podem ser observados na Figura 4.3.

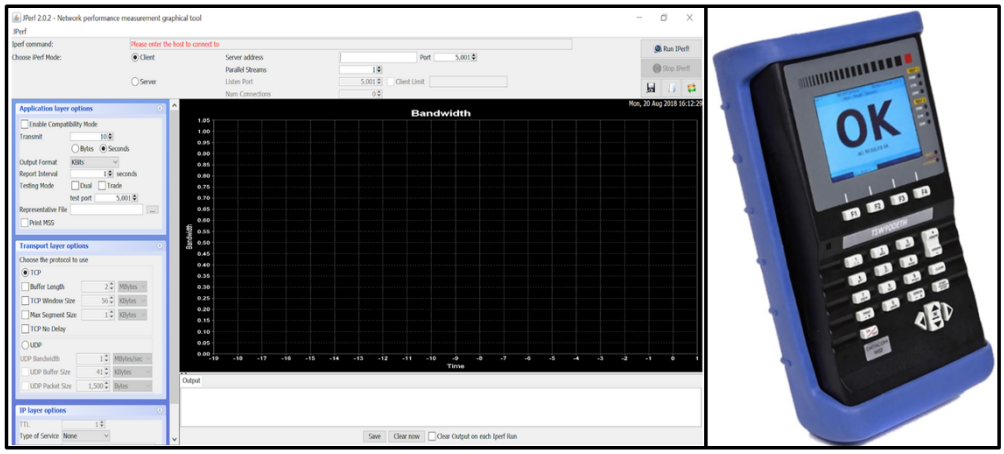


Figura 4.3: Geradores de tráfego utilizados durante os experimentos.

As topologias foram planejadas para que ambas as soluções fossem avaliadas utilizando como comunicação, entre os equipamentos de teleproteção e roteadores, as interfaces G.703 Codir 64 kbps e G.703 2 Mbps. Devido à indisponibilidade de algumas interfaces nos roteadores, foi necessária a utilização de conversores.

Para a realização dos testes com interface G.703 2 Mbps na solução *IP Hard-Pipe*, foi necessária a implementação do conversor de interface V.35/G.703 2 Mbps modelo DM704C do fabricante Datacom do Brasil. Já nos testes com interface G.703 64 Kbps para a solução *Flex-LSP*, foi necessária a inclusão de um *Mux TDM*, modelo AMDII, do fabricante Digitel, para a conversão da interface G.703 64 kbps em G.703 2 Mbps. Os equipamentos podem ser observados na Figura 4.4.

Figura 4.4: Conversores utilizados durante os experimentos.

Nas seções a seguir, será realizado um maior detalhamento dos testes propostos, separando-os em dois cenários mais amplos: o primeiro referente aos testes com a solução proprietária *IP Hard-Pipe* e o segundo com a solução proprietária *Flex-LSP*. Vale ressaltar que os testes com ambos são similares, com o intuito de que não ocorra o favorecimento de nenhuma solução.

4.2 Caderno de Testes da Solução *IP Hard-Pipe*

Nesta seção, serão abordados os principais tópicos referentes a configuração da rede e do caderno de testes com a solução *IP Hard-Pipe*. Todos os testes foram realizados com interface G.703 Codir de 64 kbps e interface G.703 de 2 Mbps. Um diagrama de blocos com os principais procedimentos realizados durante a execução dos testes com a solução *IP Hard-Pipe* pode ser observado na Figura 4.5.

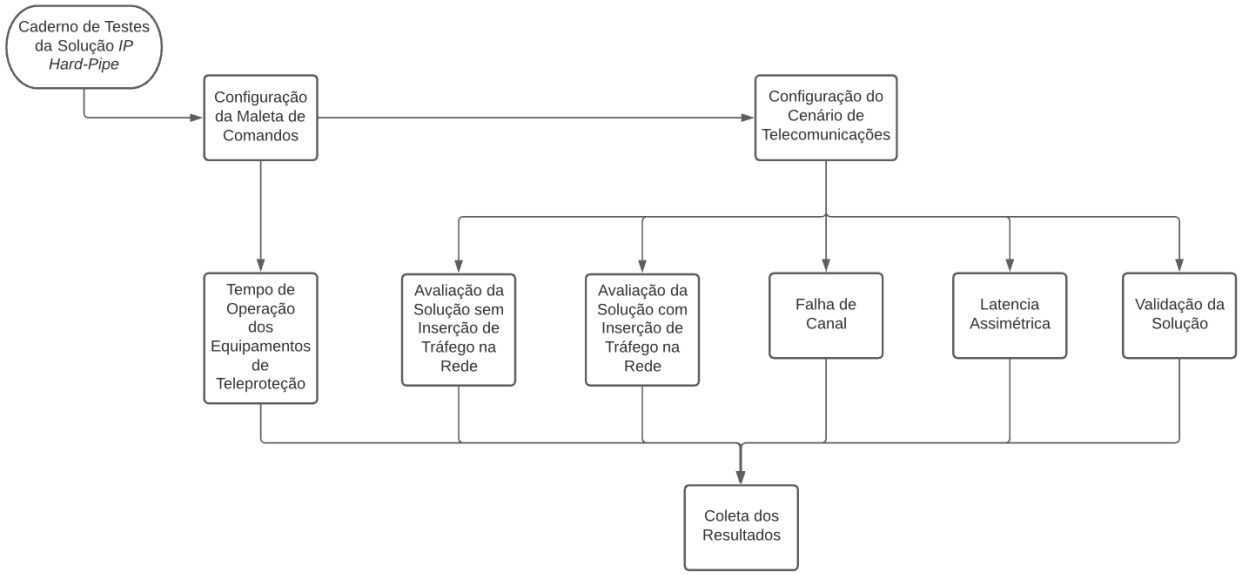


Figura 4.5: Diagrama genérico para os procedimentos realizados com a solução *IP Hard-Pipe*

Durante os experimentos a maleta de comandos foi configurada para o envio de duzentas amostras, contendo quatro comandos em cada (dois DUTT e dois DCB). Cada amostra foi espaçada através de um intervalo de um segundo e cada comando de teleproteção foi configurado com um comprimento de cem milissegundos.

Assim como descrito anteriormente, de forma geral, os cenários são compostos por seis roteadores (PE-01, PE-02, P-01, P-02, CORE-01 e CORE-02); dois equipamentos de teleproteção DIP 5000 interligados aos roteadores PE-01 e PE-02 via interface G.703 Codirecional de 64 kbps e G.703 de 2 Mbps, sendo o último empregado juntamente com a inclusão dos conversores DM704C; dois geradores de tráfego do TSW900ETH; quatro computadores com o *software Jperf* (três clientes e um servidor); uma maleta de comandos; e finalmente, um relógio externo proveniente da rede *SDH* do laboratório.

A disponibilidade física dos roteadores pode ser observada na Figura 4.6. Já a disponibilidade física dos equipamentos presentes no laboratório pode ser observada na Figura 4.7.

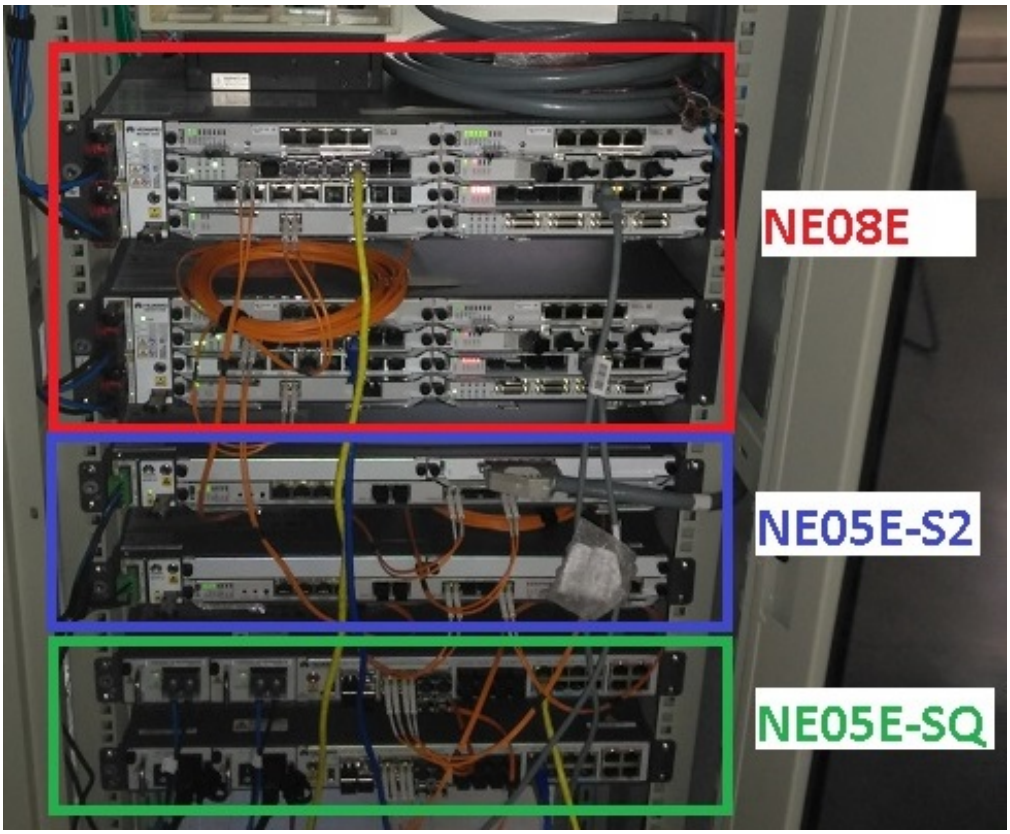


Figura 4.6: Disponibilidade física dos roteadores no laboratório.

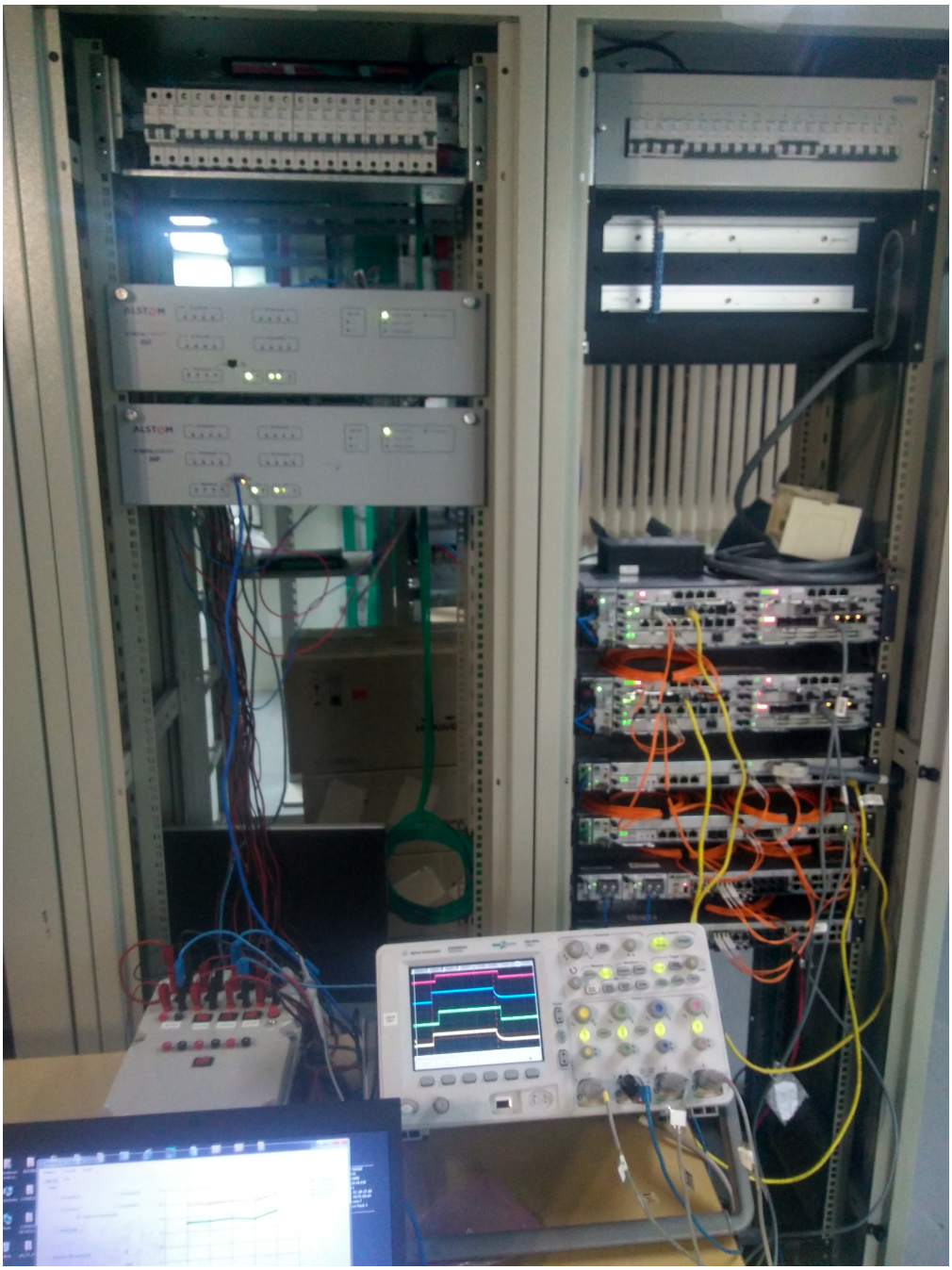


Figura 4.7: Disponibilidade física do cenário de testes com a solução *IP Hard-Pipe*.

A configuração de todo o cenário de telecomunicações utilizado durante os experimentos com a solução *IP Hard-Pipe*, pode ser observado através do diagrama de blocos apresentado na Figura 4.8.

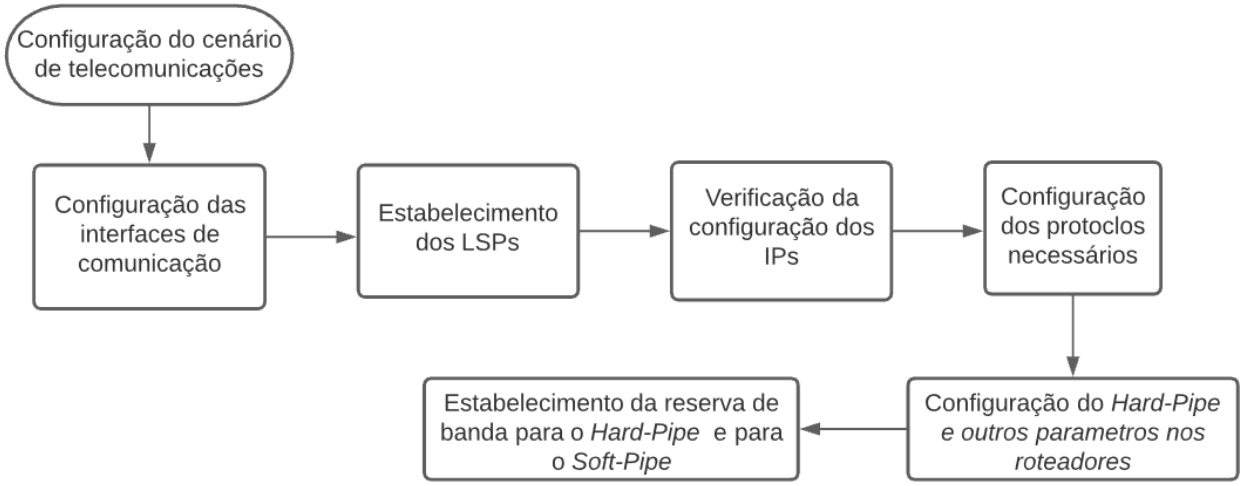


Figura 4.8: Representação da configuração do cenário de telecomunicações para o cenário com a solução *IP Hard-Pipe*.

Através do diagrama apresentado na Figura 4.8, pode-se evidenciar os seguintes passos:

- Configuração das interfaces Ethernet e das interfaces utilizadas para a conexão dos equipamentos de teleproteção (G.703 Codir de 64 Kbps ou G.703 de 2 Mbps) aos roteadores;
- Estabelecimento de seis *LSPs* bidirecionais estáticos entre os roteadores PE-01 e P-01, P-01 e CORE-01, CORE-01 e CORE-02, CORE-02 e P-02, P-02 e PE-02 (*Link* alternativo) e por fim, entre os roteadores PE-02 e PE-01 (*Link* principal);
- Verificação da configuração dos *IPs* e interfaces de *loopback*;
- Implementação dos protocolos *Open Shortest Path First* (OSPF), *Bidirectional Forwarding Detection* (BFD) e *Resource Reservation Protocol* (RSVP);
- Configuração do *Hard-Pipe*,*Maximum Transmission Unit* (MTU), *Jitter buffer* e compensação de latências;
- Reserva de banda de 10 Mbps para o *Hard-pipe* e banda de 990 Mbps para o *Soft-pipe*.

A topologia obtida ao final destas configurações pode ser observada na Figura 4.9.

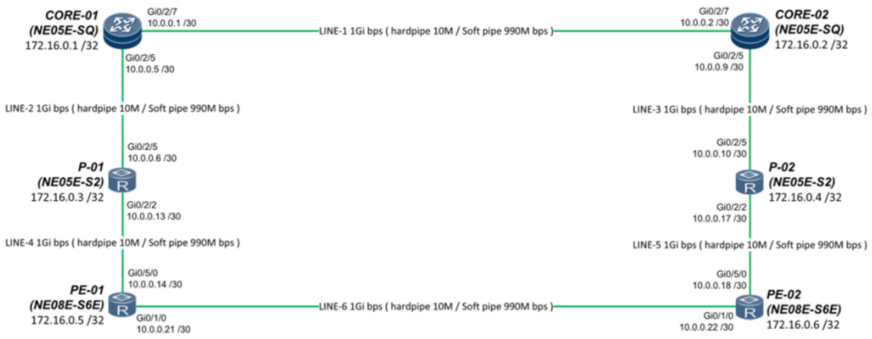


Figura 4.9: Disponibilização da rede *MPLS* para a solução *IP Hard-Pipe*.

A fim de demonstrar as configurações implementadas, foi utilizado como referência o roteador PE-01. A configuração desse pode ser observada na figura 4.10 na qual mostra-se evidente, a partir de uma análise do interior do retângulo vermelho, a configuração do *MPLS*, dos protocolos *RSVP* e *BFD* e, por fim, do algoritmo *CSPF*. O *Hard-Pipe* foi habilitado nas interfaces *GigabitEthernet* 0/1/0 (amarelo) e *GigabitEthernet* 0/5/0 (azul), para os caminhos principal e alternativo respectivamente. Por fim, o protocolo *LDP* foi habilitado (branco).

```
mpls lsr-id 172.16.0.5
#
mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te bfd all-interfaces enable
 mpls rsvp-te hello
 mpls rsvp-te hello support-peer-gr
 mpls te cspf
 lsp-trigger all
 mpls bfd enable
#
bidirectional static-cr-lsp ingress Tunnel1
 forward outgoing-interface GigabitEthernet0/1/0 nexthop 10.0.0.22 out-label 20
 backward in-label 17
 hard-pipe enable
#
bidirectional static-cr-lsp ingress Tunnel2
 forward outgoing-interface GigabitEthernet0/5/0 nexthop 10.0.0.13 out-label 160
 backward in-label 30
 hard-pipe enable
#
mpls l2vpn
#
pw-aps 1
#
mpls ldp
 #
```

Figura 4.10: Configuração do roteador PE-01.

A configuração da interface *GigabitEthernet* 0/5/0 pode ser observada na Figura 4.11. Nela, pode-se observar a implementação do protocolo *MPLS* (vermelho), do protocolo de roteamento *OSPF* (amarelo), *RSVP* (verde), *LDP* (azul), *MTU* (branco), *clock* (cinza), além da configuração do *QoS* do *Hard-Pipe* e sua banda (roxo).

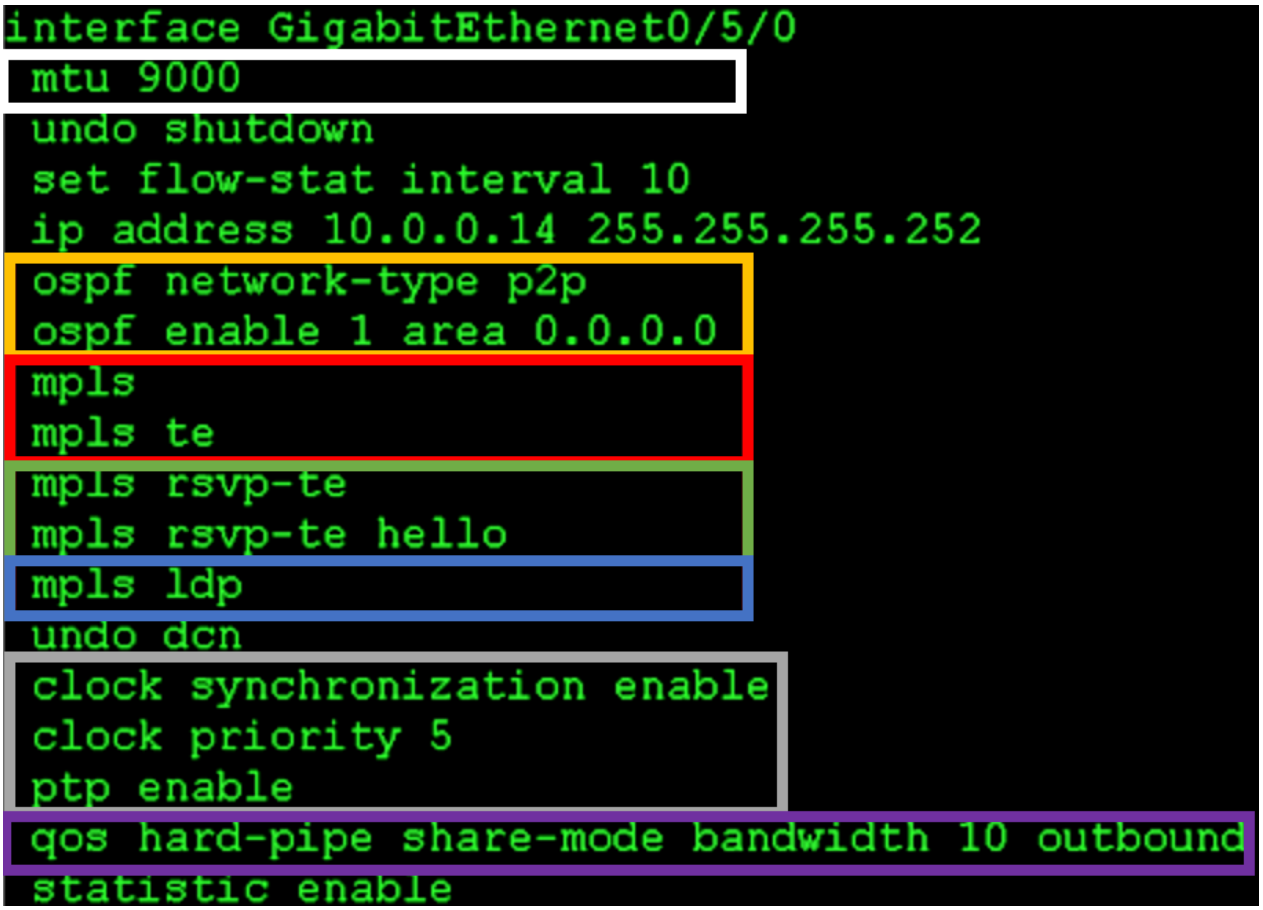


Figura 4.11: Configuração do *MPLS* e do protocolo de roteamento para a interface *GigabitEthernet* 0/5/0.

Análogo à interface 0/5/0, a configuração da interface *GigabitEthernet* 0/1/0 pode ser observada na Figura 4.12. Nesta, pode-se observar a implementação do protocolo *MPLS* (vermelho), do protocolo de roteamento *OSPF* (amarelo), *RSVP* (verde), *LDP* (azul), *MTU* (branco), *clock* (cinza), além da configuração do *QoS* do *Hard-Pipe* e sua banda (roxo).

```
interface GigabitEthernet0/1/0
 mtu 9000
 undo shutdown
 set flow-stat interval 10
 ip address 10.0.0.21 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
 mpls ldp
 undo dcn
 clock synchronization enable
 clock priority 5
 ptp enable
 qos hard-pipe share-mode bandwidth 10 outbound
 statistic enable
```

Figura 4.12: Configuração do *MPLS* e do protocolo de roteamento para a interface *GigabitEthernet* 0/1/0.

Nos cenários de interface G.703 Codir 64 kbps, a configuração da interface serial 0/4/4, utilizada para realizar a conexão entre o equipamento de teleproteção DIP 5000 e o roteador PE-01, pode ser observada na Figura 4.13.

```
interface Serial0/4/4
 portmode codir
 link-protocol tdm
 mpls static-l2vc destination 172.16.0.6 1 transmit-vpn-label 100 receive-vpn-label 100 tunnel-policy CEMIG-LINE-1 control-word tdm-encapsulation 2 jitter-buffer 1 rtp-header
 mpls static-l2vc destination 172.16.0.6 2 transmit-vpn-label 200 receive-vpn-label 200 tunnel-policy CEMIG-LINE-2 control-word tdm-encapsulation 2 jitter-buffer 1 rtp-header secondary
 mpls l2vpn hard-pipe expand-ratio 980
 mpls l2vpn stream-dual-receiving
 mpls l2vpn pw-aps 1 admin
 time-delay compensation value 2500 secondary 2500
```

Figura 4.13: Configuração da interface serial 0/4/4 para o cenário com interface G.703 2 Mbps.

Nos cenários com interface G.703 Codir 2 Mbps, a configuração da interface serial 0/4/4,

utilizada para realizar a conexão entre o equipamento de teleproteção DIP 5000 e o roteador PE-01, pode ser observada na Figura 4.14.

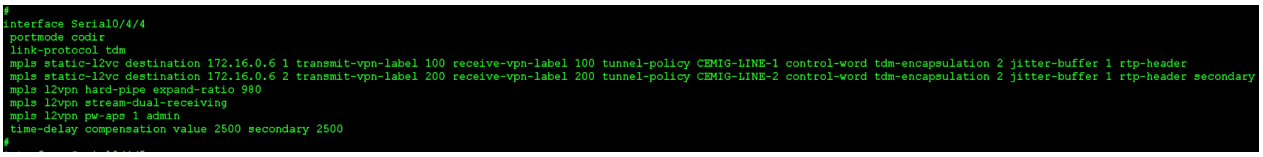


Figura 4.14: Configuração da interface serial 0/4/4 para o cenário com interface G.703 2 Mbps.

O sincronismo da rede foi estabelecido via *Clock* Externo, sendo este derivado da rede *SDH* presente no laboratório, com padrões IEEE C37.238 1588v2 e *SyncE*.

Após a realização dos procedimentos citados anteriormente, a rede se tornou apta para a execução dos experimentos que estão associados aos cenários de teleproteção.

Os seguintes testes foram executados para a solução *IP Hard-Pipe*:

- Tempo de operação dos equipamentos de teleproteção;
- Avaliação da solução *Hard-Pipe* sem a inserção de tráfego na rede;
- Avaliação da solução *Hard-pipe* com a inserção de tráfego na rede;
- Falha de Canal na solução *Hard-Pipe*;
- Latência assimétrica na rede *IP* com solução *Hard-Pipe*;
- Validação da solução.

4.2.1 Tempo de Operação dos Equipamentos de Teleproteção

Neste cenário, o objetivo principal se resume em determinar o tempo gasto para o processamento e o envio dos comandos de proteção pelos equipamentos de teleproteção. Para isso, não se considera o tempo gasto para os comandos serem transportados pela rede de telecomunicações, pois, esses serão avaliados posteriormente nos testes 4.2.2 e 4.2.3.

Para a realização deste teste foi adotada uma topologia no qual um equipamento de teleproteção é diretamente interligado ao outro (*Back to Back*). Além disso, a maleta de testes envia os comandos do equipamento de teleproteção A para o equipamento B. Isso faz com que seja possível a obtenção dos valores de latência média que serão fornecidos pelos equipamentos de teleproteção ao sistema. Essa topologia pode ser observada na Figura 4.15.

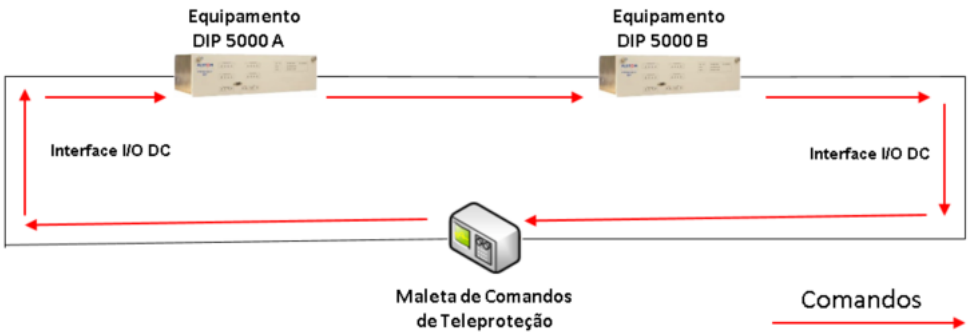


Figura 4.15: Topologia *Back to Back*.

A Tabela 4.2 apresenta os pré-requisitos, procedimentos e resultados esperados para o teste.

Tabela 4.2: Desempenho do sistema *Back to Back* de teleproteção com interface G.703 Codir de 64 Kbps e interface G.703 de 2 Mbps.

Pré-condições	- Energizar os equipamentos de teleproteção DIP5000 e interligá-los via *back-to-back* com interface G.703 Codir 64 kbps ou G.703 2Mbps.
Procedimentos do teste	- Configurar um dos DIP 5000 com *clock* interno; - Configurar as interfaces G.703 Codir 64 kbps e G.703 2 Mbps; - Através da maleta de teleproteção, realizar o envio de duzentas amostras contendo quatro comandos cada (dois DUTT e dois DCB). Os comandos são espaçados em um intervalo de um segundo entre o envio de cada amostra, possuindo um comprimento de cem milissegundos; - Verificar a latência através do *software* da maleta de comandos.
Resultados esperados	Obter as medidas de desempenho do sistema, com valores de latência inferiores a dez ms.

4.2.2 Avaliação da Solução *Hard-Pipe* sem a Inserção de Tráfego na Rede

Este teste prevê a avaliação do sistema de teleproteção com a solução analisada, quando a rede não apresentar uma inserção de tráfego no *Soft-Pipe*. De modo que, apenas os comandos de teleproteção irão trafegar pela rede de comunicação. Esses comandos são enviados do equipamento DIP 5000 A para o equipamento DIP 5000 B através do caminho principal.

As topologias que descrevem o cenário acima, podem ser observadas na Figura 4.16 e Figura 4.17, respectivamente, sendo que a primeira se refere à topologia com interface G.703 Codir 64 kbps e a segunda com interface G.703 2 Mbps.

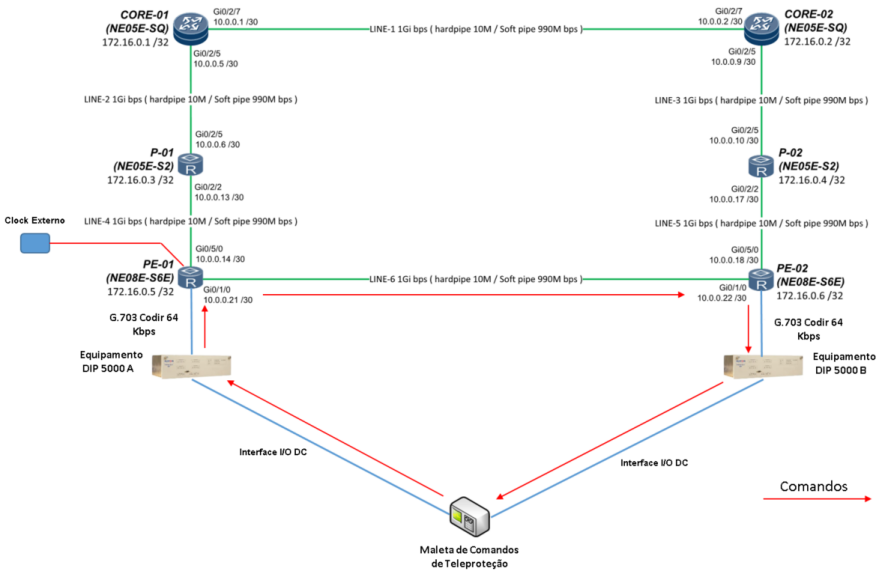


Figura 4.16: Topologia adotada para a avaliação do *Hard-Pipe* sem a inserção de tráfego e com interface G.703 Codir 64 kbps.

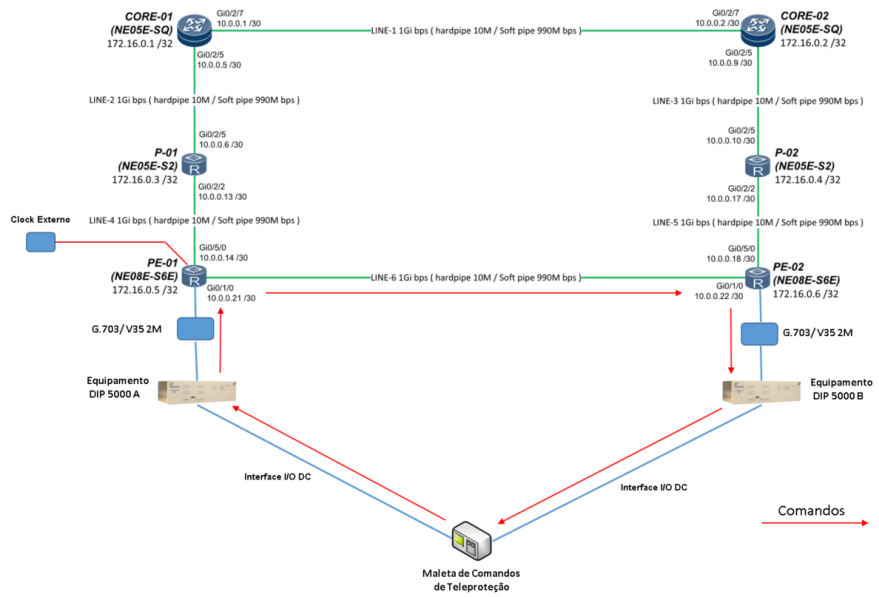


Figura 4.17: Topologia adotada para a avaliação do *Hard-Pipe* sem a inserção de tráfego e com interface G.703 2 Mbps.

A Tabela 4.3 apresenta os pré-requisitos, procedimentos e resultados esperados para o teste.

Tabela 4.3: Desempenho da rede *IP* sem tráfego com interface G.703 Codir 64 Kbps e interface G.703 2Mbps.

Pré-condições	Que a rede de telecomunicações esteja configurada corretamente e que todos os equipamentos estejam conectados, energizados e aterrados.
Procedimentos do teste	- Conectar os equipamentos de teleproteção DIP 5000 aos roteadores PE-01 e PE-02, através das interfaces G.703 Codir e G.703 2 Mbps; - Através do *software* da maleta de comandos de teleproteção, realizar o envio de duzentas amostras contendo quatro comandos em cada (dois DUTT e dois DCB). Os comandos são espaçados num intervalo de um segundo entre o envio de cada amostra, possuindo um comprimento de cem milissegundos.
Resultados esperados	Obter valores de latência para os comandos de teleproteção inferiores a dez ms.

4.2.3 Avaliação da Solução *Hard-Pipe* com a Inserção de Tráfego na Rede

Esse cenário tem o objetivo de testar o desempenho dos comandos de teleproteção que foram enviados e recebidos pelos equipamentos via rede *IP*, similar ao teste 4.2.2, mas com inserção de tráfego no *Soft-Pipe* através de uma interface Ethernet. Para o cenário com interface G.703 Codir 64 kbps, foi utilizado o *software Jperf*, sendo esse instalado em quatro computadores (três clientes e um servidor).

Além disso, os clientes foram interligados ao roteador PE-01 e o servidor foi interligado ao roteador PE-02, de modo a permitir que o caminho principal fosse avaliado. Essa topologia pode ser observada na Figura 4.18.

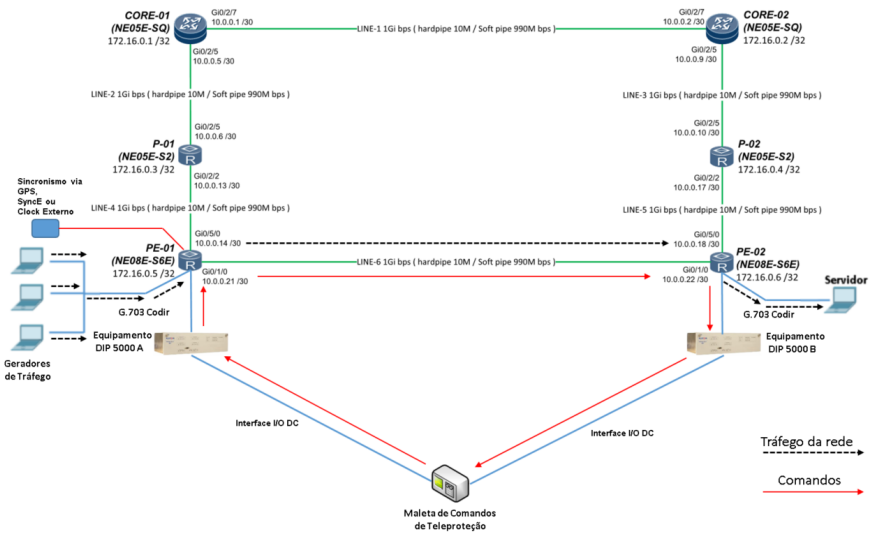


Figura 4.18: Topologia adotada para a avaliação do *Hard-Pipe* com a inserção de tráfego e com interface G.703 Codir 64 kbps.

Para o cenário com interface G.703 2 Mbps, foram utilizados os equipamentos *Wise* TSW900ETH. Esses foram conectados aos roteadores PE-01 e PE-02, garantindo o envio de tráfego através do *link* principal. A topologia descrita pode ser observada na Figura 4.19.

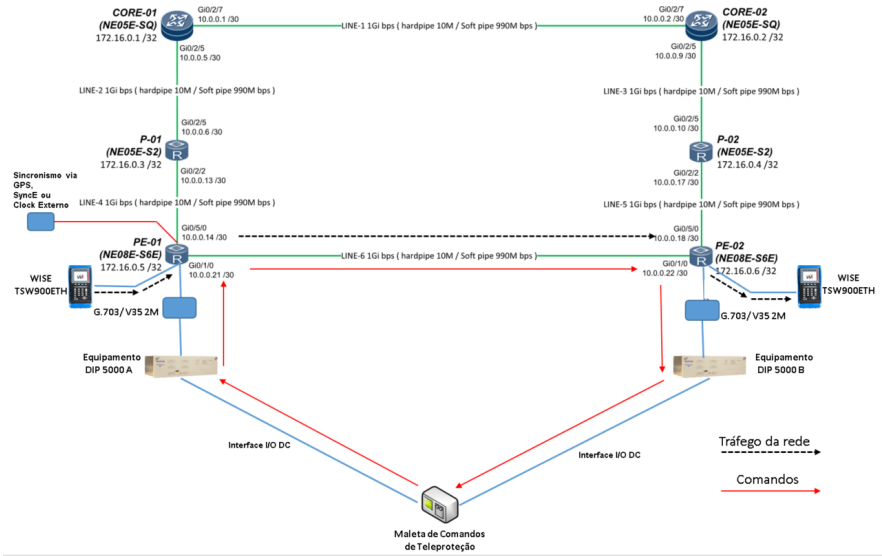


Figura 4.19: Topologia adotada para a avaliação do *Hard-Pipe* com a inserção de tráfego e com interface G.703 2 Mbps.

A Tabela 4.4 apresenta os pré-requisitos, procedimentos e resultados esperados no teste.

Tabela 4.4: Desempenho da rede *IP* com tráfego e interface G.703 Codir 64 Kbps ou interface G.703 2Mbps.

Pré-condições	- Teste 4.2.2 executado com sucesso; - Conexão dos geradores ao roteador PE-01 e o servidor ao roteador PE-02; - Conexão dos equipamentos TSW900ETH aos roteadores PE-01 e PE-02.
Procedimentos do teste	Para a interface Codir: - Através do *software Jperf*, injetar o tráfego de aproximadamente um Gbps no *Soft-Pipe* através das interfaces Ethernet; - Enviar duzentas amostras contendo quatro comandos em cada (dois DUTT e dois DCB). Os comandos são espaçados em intervalos de um segundo entre o envio de cada amostra, possuindo um comprimento de cem milissegundos; - Verificar a latência dos comandos de teleproteção através do *software* de teleproteção. Para a interface 2 Mbps: - Através do gerador TSW900ETH, injetar o tráfego de um Gbps Ethernet no *Soft-Pipe*; - Enviar duzentas amostras contendo quatro comandos em cada (dois DUTT e dois DCB). Os comandos são espaçados em intervalos de um segundo entre o envio de cada amostra, possuindo um comprimento de cem milissegundos; - Verificar a latência através do *software* de teleproteção; - Verificar os resultados no gerador de tráfego.
Resultados esperados	Obter as medidas de desempenho do sistema nessa topologia, com valores de latência inferiores a dez ms e *Jitter* de aproximadamente de 15,6 μs.

4.2.4 Falha de Canal na Solução *Hard-Pipe*

Esse cenário tem o objetivo de avaliar a solução *Hard-Pipe* quando essa é submetida a uma falha de canal, na qual será obrigada a migrar do canal principal para o canal alternativo. Essa migração faz com que os comandos, que antes eram enviados através de dois roteadores, sejam direcionados por um caminho com seis roteadores. A falha é induzida no sistema quando a maleta envia a quinquagésima amostra.

Através deste cenário, pode-se avaliar o impacto de um maior número de saltos no sistema. A topologia que descreve este cenário pode ser observada na Figura 4.20. Importante ressaltar que a única diferença entre os cenários com interface G.703 Codir 64 kbps e o de G.703 2 Mbps está na implementação do conversor DM704C entre os equipamentos de teleproteção e os roteadores PE-01 e PE-02.

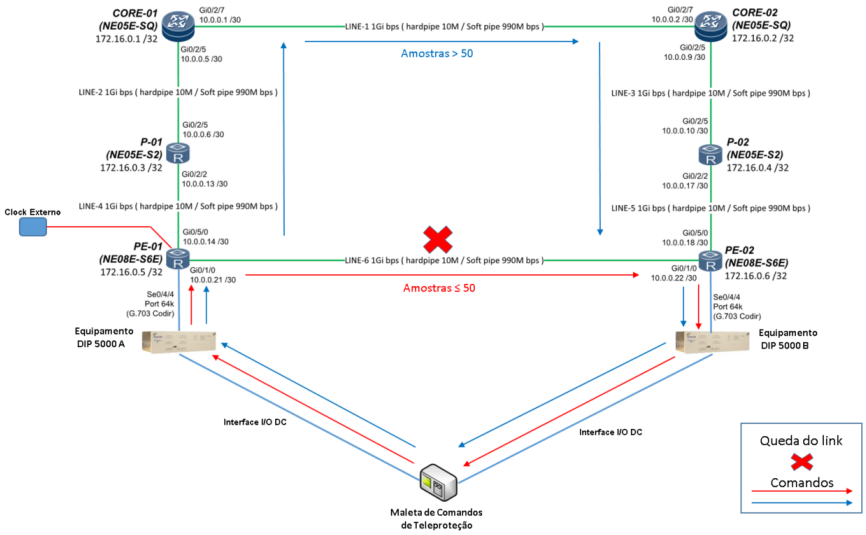


Figura 4.20: Topologia adotada para a avaliação do cenário de falha de canal na solução Huawei.

Os pré-requisitos, procedimentos e resultados esperados do teste podem ser observados na Tabela 4.5.

Tabela 4.5: Desempenho do sistema de proteção com interfaces G.703 Codir 64 kbps e G.703 2Mbps quando submetidos a falha de canal.

Pré-condições	- Teste 4.2.2 executado com sucesso.
Procedimentos do teste	- Utilizar interfaces G.703 Codir 64kbps entre os roteadores e DIP5000; - Através do *software* da maleta de comandos de teleproteção, realizar o envio de duzentas amostras contendo quatro comandos em cada (dois diretos e dois de bloqueio). Quando o *software* de teleproteção enviar a quinquagésima amostra, o caminho principal (caminho direto entre os roteadores 1 e 6) será derrubado manualmente e o restante das amostras será enviado através do *link* secundário (Caminho que engloba todos os rotadores); - Verificar a latência dos comandos de teleproteção através do *software* de teleproteção.
Resultados esperados	Obter valores de *delay* do sistema, aproximados àqueles que foram obtidos nos testes anteriores.

4.2.5 Latência Assimétrica na Rede *IP* com a Solução *Hard-Pipe*

Neste cenário, é avaliada a condição de assimetria do canal em uma topologia que utiliza a solução *Hard-Pipe* para o serviço de teleproteção. Para a execução deste teste, é realizada a comparação entre as latências dos comandos enviados do equipamento de teleproteção DIP 5000 A para o B, bem como dos comandos enviados do equipamento DIP 5000 B para o A. Este cenário pode ser observado na Figura 4.21.

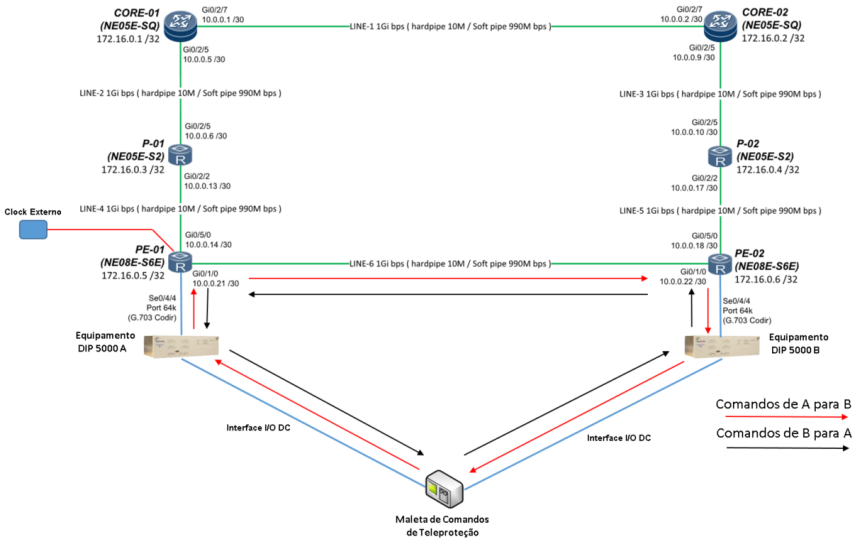


Figura 4.21: Topologia adotada para a avaliação de latência assimétrica na solução *Hard-Pipe*.

Os pré-requisitos, procedimentos e resultados esperados para esse teste pode ser observado na Tabela 4.6.

Tabela 4.6: Latência assimétrica para a solução Huawei com interface G.703 Codir 64 kbps e interface G.703 2Mbps.

Pré-condições	- Teste 4.2.2 executado com sucesso.
Procedimentos do teste	- Utilizar a interfaces G.703 Codir 64kbps entre os roteadores e equipamentos de teleproteção DIP 5000; - Através do *software* da maleta de comandos de teleproteção, realizar o envio duzentas amostras contendo quatro comandos em cada (dois DUTT e dois DCB). Os comandos são espaçados num intervalo de um segundo entre o envio de cada amostra, possuindo um comprimento de cem milissegundos; - Inicialmente os comandos serão enviados do roteador PE-01 para o PE-02 e depois do PE-02 para o PE-01; - Verificar a latência dos comandos através do *software* de teleproteção.
Resultados esperados	Obter valores de latência assimétrica inferiores a quatro ms.

4.2.6 Validação da solução

Esse teste possui o intuito de verificar os principais pontos de comparação com as redes *TDM*, no qual a solução prevê a isolação do tráfego entre o *Soft-Pipe* e o *Hard-Pipe*. Para executá-lo, o limite de tráfego suportado pelo *Soft-Pipe* foi excedido com o auxílio do gerador de tráfego, possibilitando a verificação da integridade da isolação.

O gerador utilizado para este cenário foi o *Jperf*. Porém, tendo em vista a limitação da ferramenta quanto ao valor de tráfego gerado, não foi possível que o cenário utilizado desde o inicio dos testes fosse mantido. Diante disso, foi realizado um novo dimensionamento do *Soft* e *Hard-Pipe*.

Assim, em um primeiro momento foi realizado o dimensionamento do *Hard-Pipe* para 800 Mbps e o *Soft-Pipe* para 200 Mbps e, posteriormente, o *Hard-Pipe* foi alterado para 980 Mbps e o *Soft-Pipe* para 20 Mbps. Para esse fim, foi realizada a alteração no dimensionamento da interface *GigabitEthernet* 0/5/0 do roteador PE-01. A topologia para o primeiro cenário de teste pode ser observada na Figura 4.22.

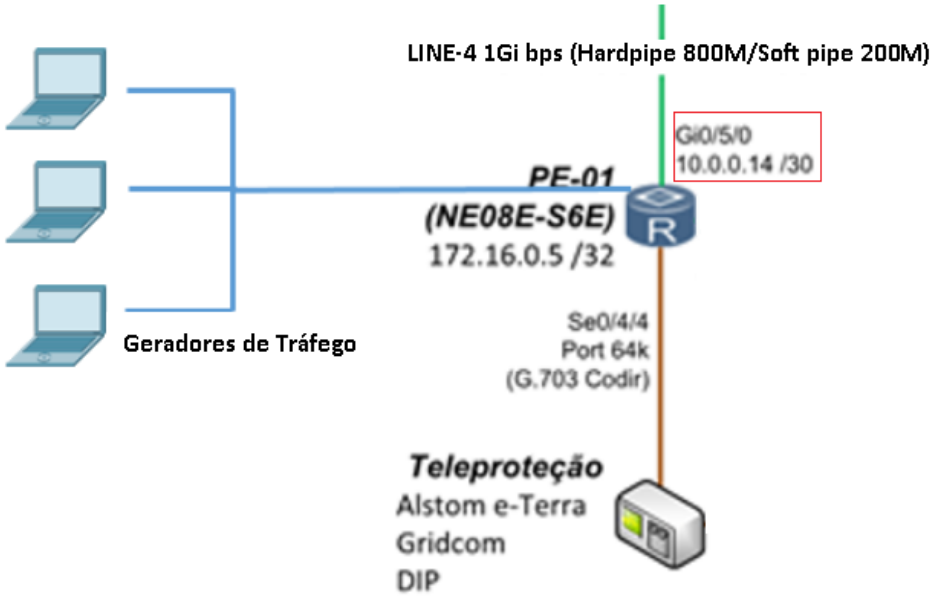


Figura 4.22: 1º cenário para avaliação da tecnologia *Hard-Pipe*.

A topologia para o segundo cenário de teste pode ser observada na Figura 4.23.

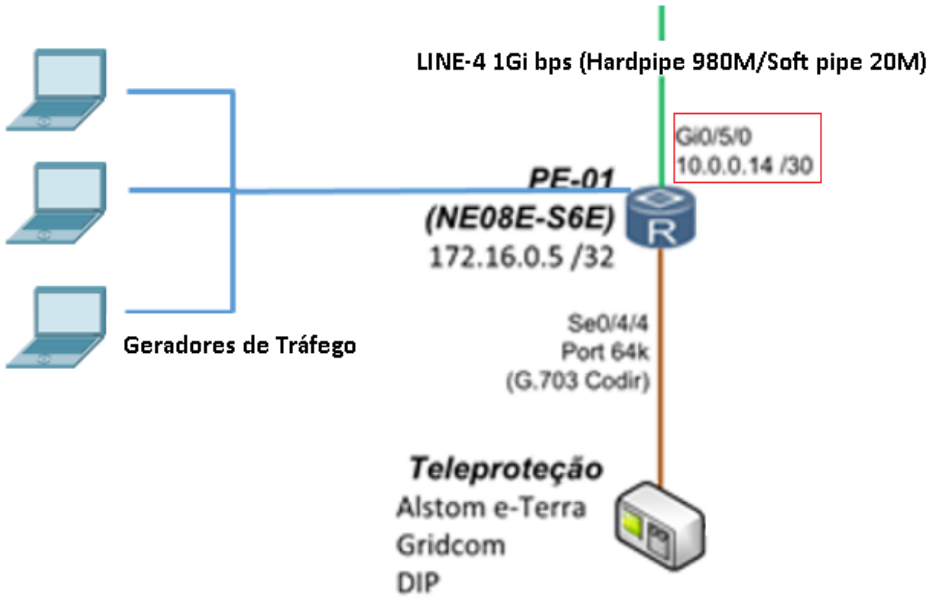


Figura 4.23: 2º cenário para avaliação da tecnologia *Hard-Pipe*.

4.3 Caderno de Testes da Solução *Flex-LSP*

Nesta seção, serão abordados os principais tópicos referentes aos testes com a solução *Flex-LSP*. Todos os testes foram realizados com interface G.703 Codir 64 kbps e interface G.703 2 Mbps. Um diagrama de blocos com os principais procedimentos realizados durante a execução dos testes com a solução *Flex-LSP* pode ser observado na Figura 4.24.

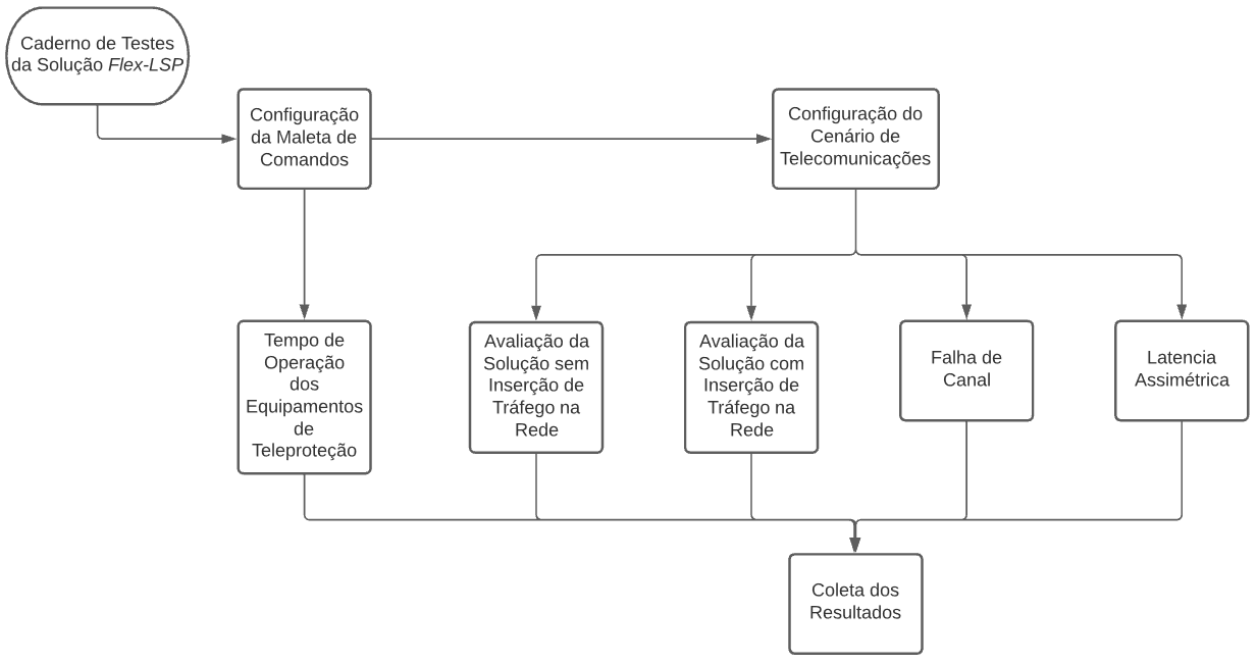


Figura 4.24: Diagrama genérico para os procedimentos realizados com a solução *Flex-LSP*

Durante a realização dos experimentos a maleta de comandos foi configurada para realizar o envio de duzentas amostras, contendo quatro comandos em cada (dois DUTT e dois DCB). Cada amostra foi espaçada através de um intervalo de um segundo e cada comando de teleproteção foi configurado com um comprimento de cem milissegundos.

De modo geral, os cenários são compostos por seis roteadores (ASR903); dois equipamentos de teleproteção DIP 5000 conectados aos roteadores 1 e 6 via interface G.703 Codir 64 kbps e G.703 2 Mbps; dois geradores de tráfego TSW900ETH; uma maleta de comandos de teleproteção e um *clock* externo proveniente da rede *SDH* presente no laboratório.

Vale ressaltar que, para a utilização da interface Codir 64 kbps, foi necessária a inclusão de um *MUX TDM* para a conversão de C37.94 para G.703 Codir. Ademais, a disponibilidade física dos equipamentos para os experimentos com a solução *Flex-LSP* pode ser observada na Figura 4.25.

Figura 4.25: Disponibilidade física do cenário de testes Cisco.

De forma análoga à sistemática dos testes realizados anteriormente, inicialmente foi realizada a configuração de todo o cenário de telecomunicações. Sendo essa utilizada como base para os testes que serão apresentados posteriormente. Ademais, o diagrama de blocos que representa essa configuração pode ser observada na Figura 4.26.

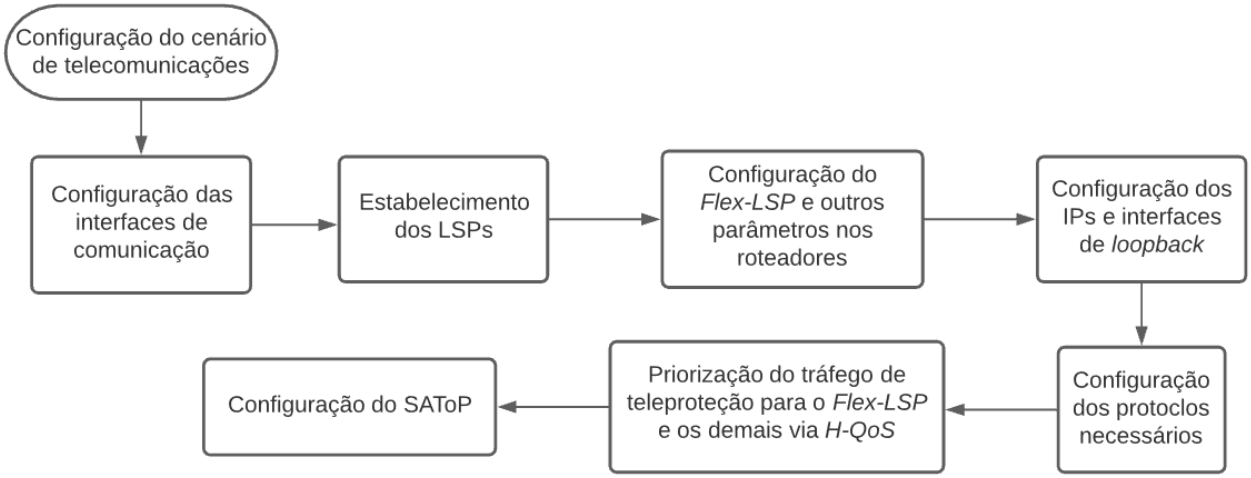


Figura 4.26: Representação da configuração do cenário de telecomunicações para o cenário com a solução *Flex-LSP*.

Através do diagrama apresentado na Figura 4.26, é possível evidenciar os seguintes passos:

- Configuração das interfaces Ethernet para *links* de um Gbps e configuração das interfaces utilizadas para a conexão dos equipamentos de teleproteção (G.703 Codir 64 Kbps ou G.703 2 Mbps) com os roteadores;
- Estabelecimento de *LSPs* bidirecionais estáticos entre os roteadores ASR903-1 e 6 para o *link* principal. Através dos roteadores ASR903-1, ASR903-2, ASR903-3, ASR903-4, ASR903-5 e ASR903-6 para o *link* alternativo;
- Configuração do túnel *Flex-LSP*, *MTU* e *Jitter Buffer*;
- Configuração dos *IPs*, interfaces de *loopback* em cada uma das conexões;
- Implementação dos protocolos de roteamento *OSPF* e *Label Distribution Protocol* (LDP). Além da configuração dos protocolos *RSVP* e *BFD* em todas as interfaces de *UPLINK*;
- Priorização de banda de 10 Mbps ou 100 Mbps para o tráfego que passa pelo *Flex-LSP* e o restante para os demais tráfegos via *Hierarchical Quality of Service* (H-QoS);
- Configuração do *SAToP* para o encapsulamentos de *bits TDM* em redes de pacotes.

A topologia obtida ao final destas configurações, pode ser observada na Figura 4.27.

Figura 4.27: Disponibilização da rede MPLS para a solução Cisco.

Para a demonstração das configurações implementadas foi tomado como referência o roteador ASR903-1. A configuração da interface *GigabitEthernet* 0/0/1 pode ser observada na Figura 4.28. Nesta imagem pode-se observar a implementação do protocolo *MPLS* (vermelho), do protocolo de roteamento *OSPF* (amarelo), do protocolo de rede *BFD* (azul), da *MTU* (branco) e, por fim, da reserva de banda via procolo *RSVP* (verde).

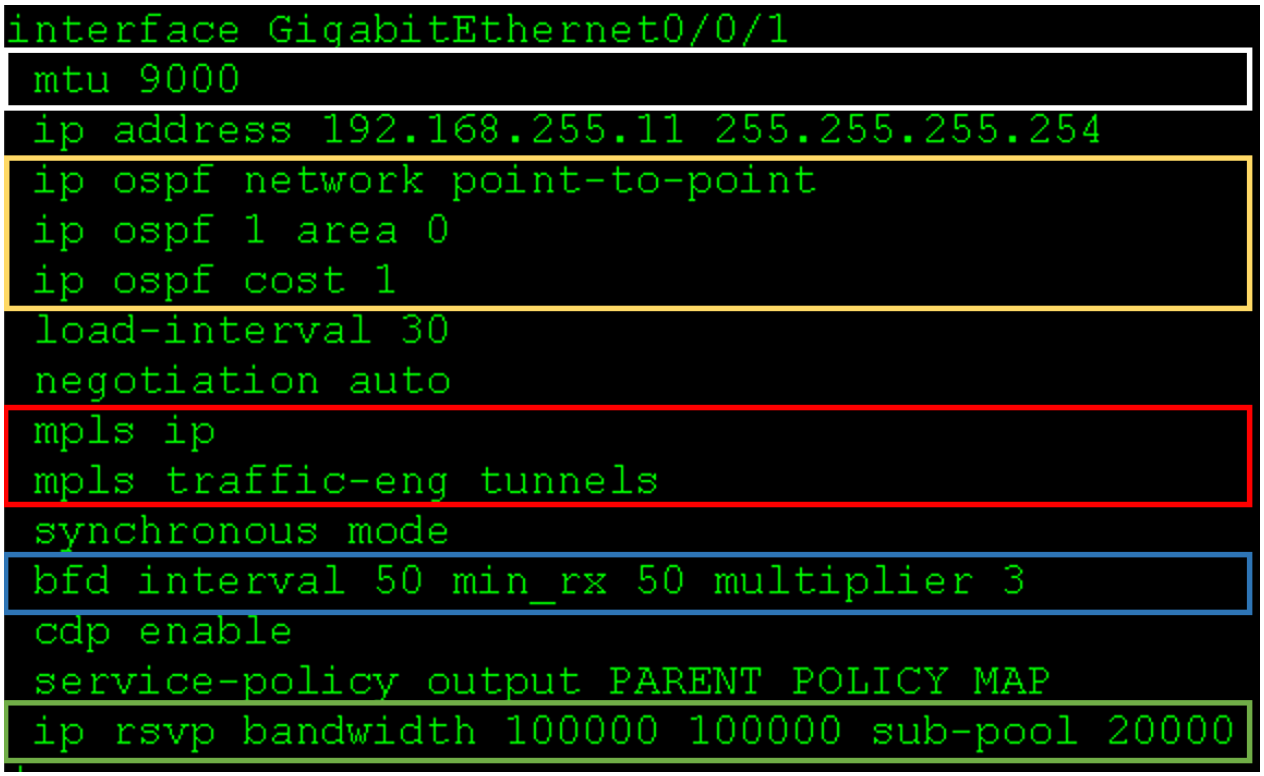


Figura 4.28: Configuração da interface *GigabitEthernet* 0/0/1 do roteador ASR903-1.

Análogo à interface 0/0/1, a configuração da interface *GigabitEthernet* 0/0/0 pode ser observada na Figura 4.29. Nesta imagem, é possível verificar a implementação do protocolo *MPLS* (vermelho), do protocolo de roteamento *OSPF* (amarelo), do protocolo de rede *BFD* (azul), da *MTU* (branco) e, por fim, da reserva de banda via procolo *RSVP* (verde).

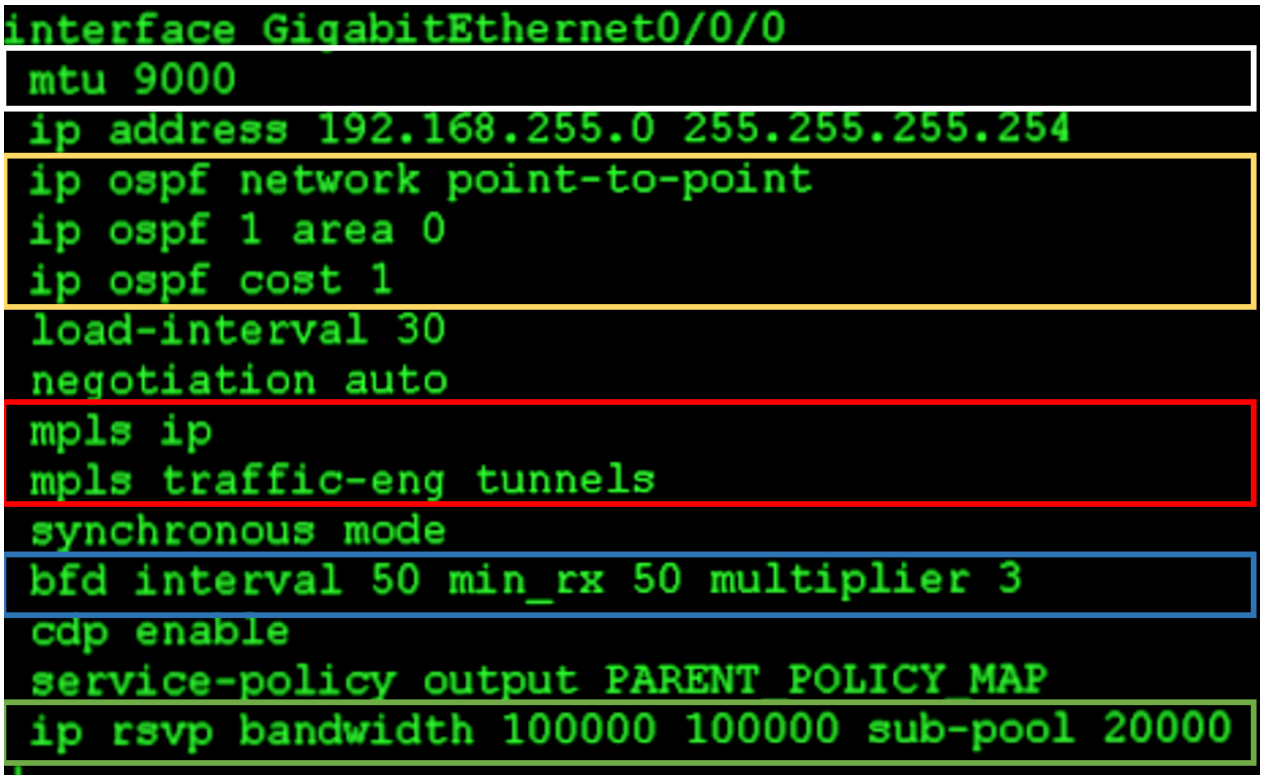


Figura 4.29: Configuração da interface *GigabitEthernet* 0/0/0 do roteador ASR903-1.

A configuração do túnel principal pode ser observado na Figura 4.30. Nessa, é possível verificar o estabelecimento de uma interface de *loopback*(azul), da engenharia de tráfego do *MPLS*(amarelo) e a banda do túnel sendo configurada para 10 Mbps(vermelho).

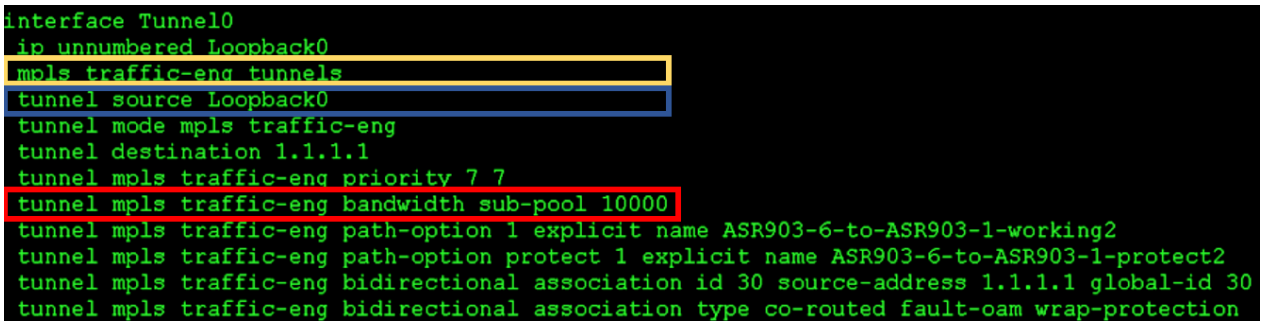


Figura 4.30: Configuração do *link* principal entre os roteadores ASR903-1 e ASR903-6.

Para os cenários com a solução *Flex-LSP*, foi disponibilizado o *software* de gerência *EPN-M*. Esta ferramenta é capaz de fornecer um método de gerência simplificado, convergente e

completo para a rede presente no sistema. Além disso, aquela é capaz de oferecer uma maior eficiência operacional, através de operações automatizadas de dispositivos e um provisionamento rápido para soluções.

Para a implementação dessa ferramenta, foi necessária a utilização de um servidor configurado na interface *GigabitEthernet* 0 do roteador ASR903-2. Este equipamento recebeu o *ip* 10.20.157.201 e a máscara de rede 255.255.255.0, conforme se observa na Figura 4.31.

```
!
interface GigabitEthernet0
 description GERENCIA
 vrf forwarding Mgmt-intf
 ip address 10.20.157.201 255.255.255.0
 negotiation auto
!
```

Figura 4.31: Configuração do *software* de gerência *EPN-M* no roteador ASR903-2.

As interfaces do *software* *EPN-M*, que demonstram a topologia adotada para os roteadores, e os equipamentos cadastrados na gerência podem ser observadas, respectivamente, nas Figuras 4.32 e 4.33.

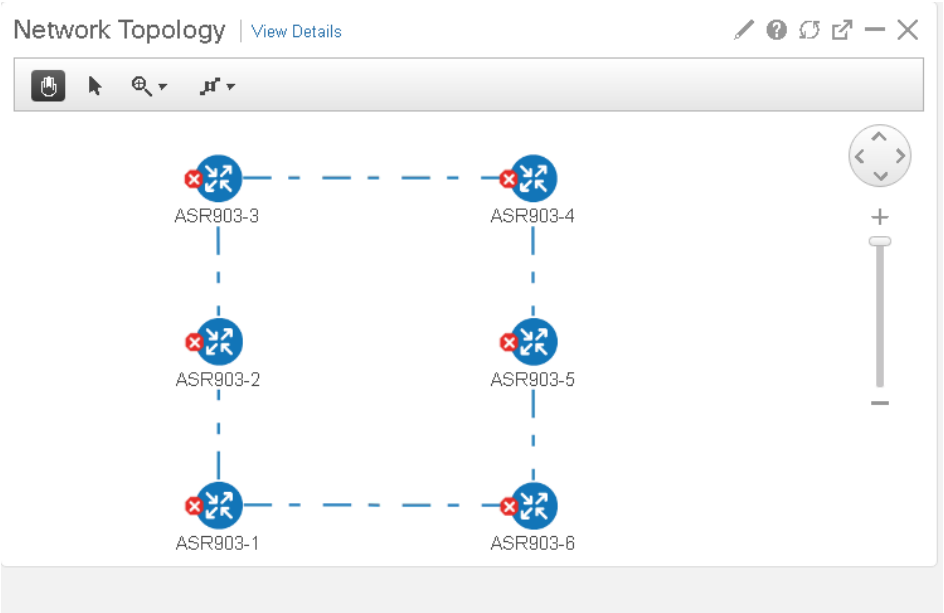


Figura 4.32: Topologia dos roteadores através do *software* de gerência *EPN-M*.

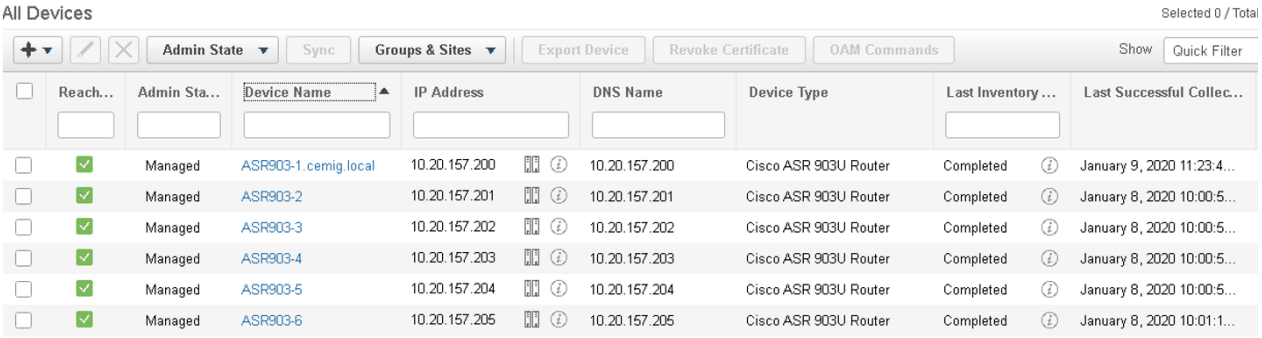


Figura 4.33: Equipamentos cadastrados na gerência *EPN-M*.

O sincronismo da rede foi estabelecido via *Clock* Externo, sendo este derivado da rede *SDH* presente no laboratório, com padrões IEEE C37.238 1588v2 e *SyncE*.

Após a configuração do cenário de telecomunicações, a rede se tornou apta para realizar a execução dos experimentos relacionados com a solução *Flex-LSP*. Sendo assim, os seguintes testes foram realizados:

- Tempo de operação dos equipamentos de teleproteção (Análogo a subseção 4.2.1);
- Avaliação da solução *Flex-LSP* sem a inserção de tráfego na rede;
- Avaliação da solução *Flex-LSP* com a inserção de tráfego na rede;
- Falha de canal na solução *Flex-LSP*;
- Latência assimétrica na rede *IP* com a solução *Flex-LSP*.

4.3.1 Avaliação da Solução *Flex-LSP* sem a Inserção de Tráfego na Rede

Neste experimento, foi realizada a verificação da solução *Flex-LSP* quando a rede não apresenta inserção de tráfego, ou seja, quando apenas os comandos de teleproteção são trafegados pela rede de telecomunicações. Esses comandos são enviados do equipamento DIP 5000 A para o equipamento DIP 5000 B, através do caminho principal.

As topologias que descrevem o cenário acima podem ser observadas na Figura 4.34 e Figura 4.35, respectivamente, sendo a primeira referente à topologia com interface G.703 Codir 64 kbps e a segunda com interface G.703 2 Mbps.

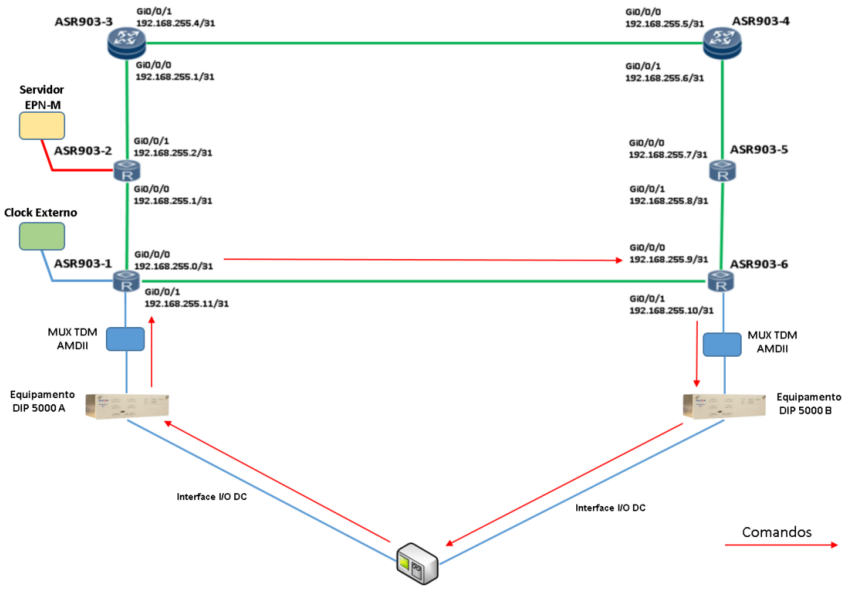


Figura 4.34: Topologia adotada para a avaliação do *Flex-LSP* sem a inserção de tráfego e com interface G.703 Codir 64 kbps.

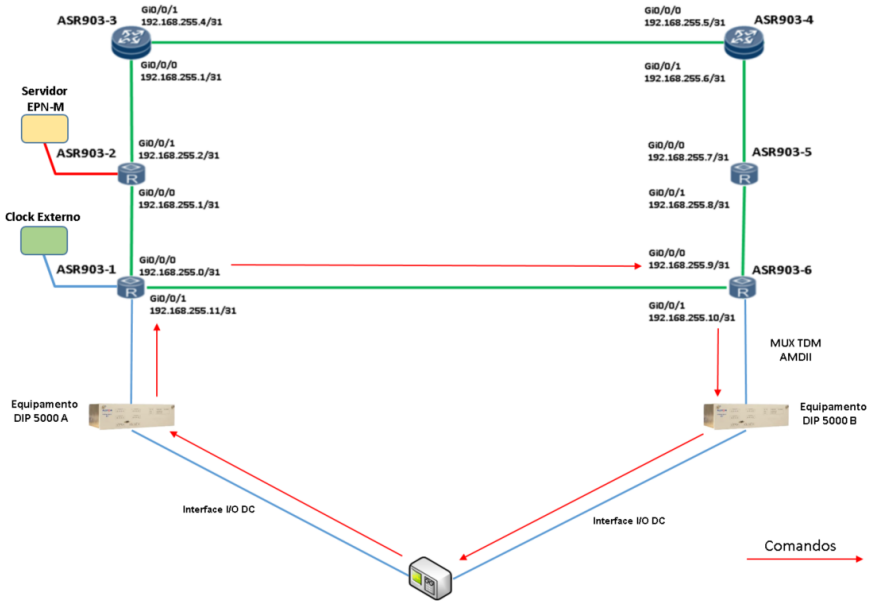


Figura 4.35: Topologia adotada para a avaliação do *Flex-LSP* sem a inserção de tráfego e com interface G.703 2 Mbps.

A Tabela 4.7 contém as pré-configurações, procedimentos e resultados esperados.

Tabela 4.7: Desempenho da rede *IP* sem tráfego e interface G.703 Codir 64 kbps ou interface G.703 2Mbps.

Pré-condições	Que a rede de telecomunicações esteja configurada corretamente e que todos os equipamentos estejam conectados, energizados e aterrados.
Procedimentos do teste	- Alinhar as portas dos equipamentos de teleproteção DIP 5000, nas interfaces G.703 Codirecional 64 kbps e G.703 2 Mbps, aos roteadores ASR903-1 e ASR903-6; - Enviar duzentas amostras através do equipamento de teleproteção DIP 5000 pelo caminho principal. Cada amostra é composta por quatro comandos (dois diretos e dois de bloqueio). As amostras são espaçadas em intervalo de um segundo e os comandos possuem o comprimento de cem ms.
Resultados esperados	Obter o valor de *delay* nos comandos de teleproteção inferior a dez ms.

4.3.2 Avaliação da solução *Flex-LSP* com a inserção de tráfego na Rede.

Neste cenário, a solução *Flex-LSP* é avaliada mediante a inserção de tráfego externo na rede de telecomunicações. Para isso, são utilizados dois equipamentos TSW900ETH interligados aos roteadores ASR 903 1 e 6, respectivamente. Os comandos são enviados do equipamento DIP 5000 A para o equipamento DIP 5000 B através do caminho principal.

Semelhante ao teste 4.3.1, para a realização dos experimentos com interface G.703 Codir 64 kbps foi necessária a utilização de um *Mux TDM* para realizar a conversão C.3794/G.703 Codir 64kbps. As topologias utilizadas para este experimento podem ser observadas na Figura 4.36 e Figura 4.37.

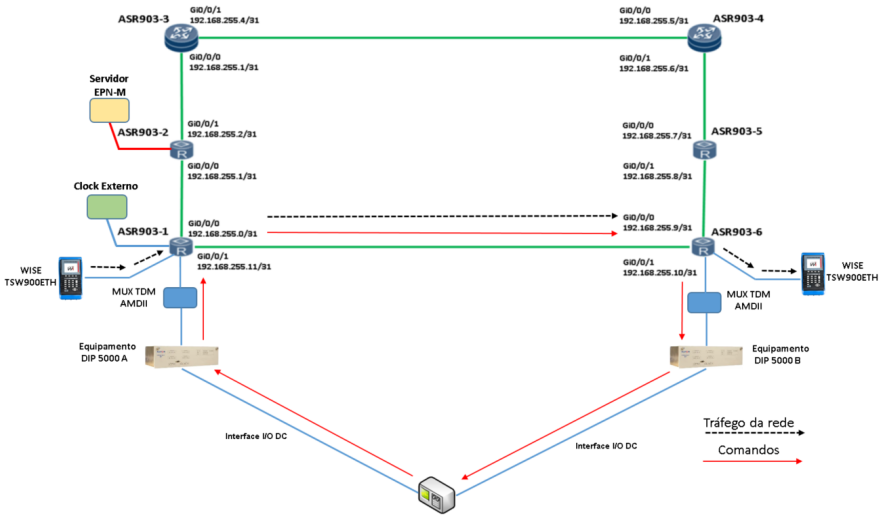


Figura 4.36: Topologia adotada para a avaliação do *Flex-LSP* com a inserção de tráfego e com interface G.703 Codir 64 kbps.

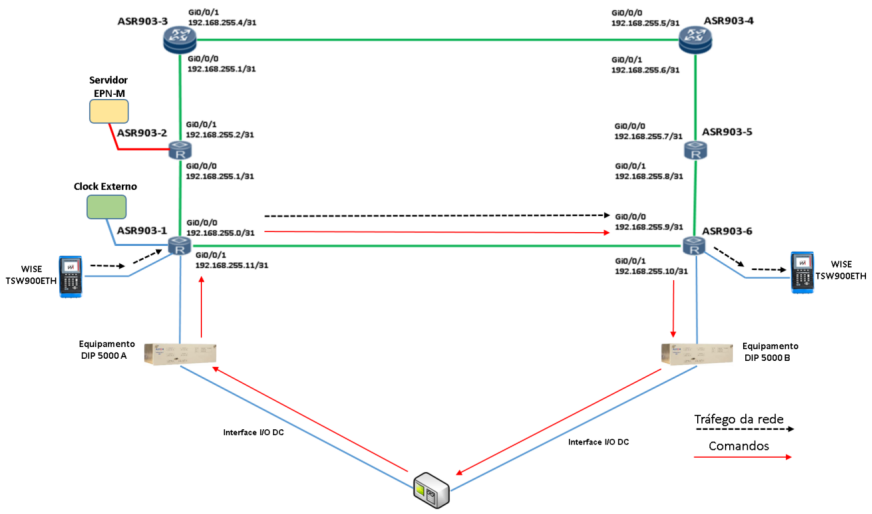


Figura 4.37: Topologia adotada para a avaliação do *Flex-LSP* com a inserção de tráfego e com interface G.703 2 Mbps.

Os pré-requisitos, procedimentos e resultados esperados dos testes podem ser observados na Tabela 4.8.

Tabela 4.8: Desempenho da rede *IP* com tráfego e interface G.703 Codir 64 kbps ou interface G.703 2Mbps.

Pré-condições	- Teste apresentado nas Subseção 4.3.1 executado com sucesso; - Conectar os geradores de tráfego aos roteadores ASR903-1 e ASR 903-6.
Procedimentos do teste	- Utilizar interface G.703 Codirecional 64 kbps e 2 Mbps entre os roteadores e DIP 5000, realizar testes com cada interface separadamente; - Injetar tráfego de um Gbps na rede *IP*, através dos geradores de tráfego modelo TSW900ETH; - Enviar duzentas amostras via equipamento de teleproteção DIP 5000 pelo caminho principal. Cada amostra é composta por quatro comandos (dois diretos e dois de bloqueio). As amostras são espaçadas em intervalo de um segundo e os comandos possuem o comprimento de cem ms; - Verificar a latência dos comandos de teleproteção através do *software* de teleproteção.
Resultados esperados	- Obter o valor de *delay* do sistema inferior a dez ms e *jitter* de aproximadamente 15.6 s.

4.3.3 Falha de Canal na Solução *Flex-LSP*

Neste experimento foi avaliado o desempenho do sistema quando submetido a uma queda de canal no caminho primário, sendo este obrigado a realizar o envio dos comandos de teleproteção pelo caminho alternativo. Os comandos de teleproteção são enviados do equipamento DIP 5000 A para o equipamento DIP 5000 B.

A falha é introduzida no cenário manualmente quando o equipamento de teleproteção envia a quinquagésima amostra. A topologia adotada para esse teste pode ser observada na Figura 4.38. Para este experimento, foi avaliado o cenário com a menor largura de banda entre os equipamentos de teleproteção e roteadores (pior caso), ou seja, com interface G.703 Codir 64 kbps.

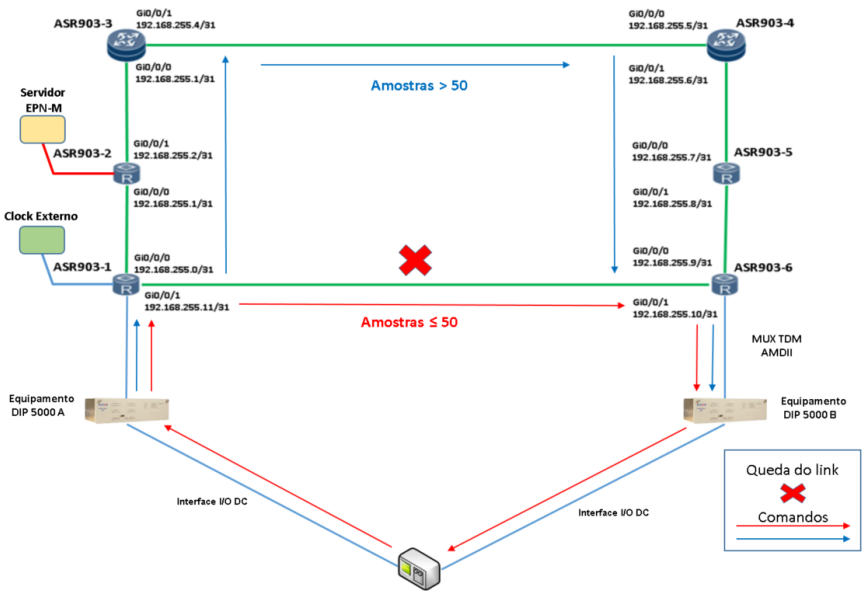


Figura 4.38: Topologia adotada para a avaliação do *Flex-LSP* quando submetida a uma falha no canal principal.

Os pré-requisitos, procedimentos e resultados esperados do teste podem ser observados na Tabela 4.9.

Tabela 4.9: Desempenho do sistema de proteção com interfaces G.703 Codir 64 kbps e G.703 2Mbps quando submetidos a falha de canal.

Pré-condições	- Teste apresentado na subseção 4.3.1 executado com sucesso.
Procedimentos do teste	- Utilizar interfaces G.703 Codir 64kbps entre os roteadores e DIP5000; - O *software* de teleproteção do DIP 5000 realizará a transmissão de duzentas amostras contendo quatro comandos em cada (dois diretos e dois de bloqueio). Quando o *software* de teleproteção enviar a quinquagésima amostra, o caminho principal (Caminho direto entre os roteadores 1 e 6) será derrubado manualmente e o restante das amostras será enviado através do *link* secundário (Caminho que engloba todos os rotadores); - Verificar a latência dos comandos de teleproteção através do *software* de teleproteção.
Resultados esperados	Obter valores de *delay* do sistema aproximados ao que se foi obtido nos testes anteriores.

4.3.4 Latência Assimétrica na rede *IP* com a Solução *Flex-LSP*

Neste cenário foi avaliada a condição de assimetria de canal em uma topologia que utiliza a solução *Flex-LSP* para o serviço de teleproteção. Este teste é realizado mediante a comparação entre as latências dos comandos enviados do equipamento de teleproteção DIP 5000 A para o B e dos comandos enviados do equipamento DIP 5000 B para o A. Este cenário pode ser observado na Figura 4.39.

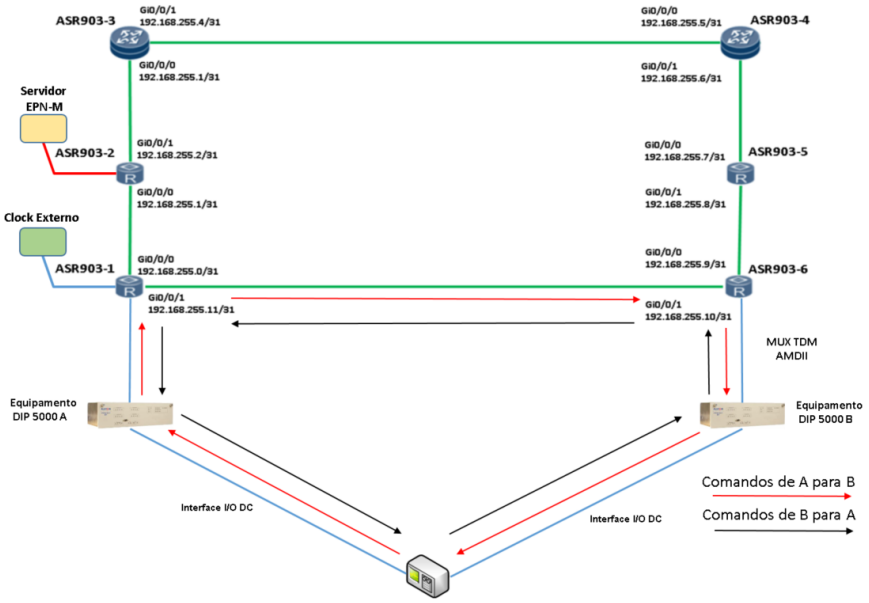


Figura 4.39: Topologia adotada para a avaliação de latência assimétrica na solução *Flex-LSP*.

Os pré-requisitos, procedimentos e resultados esperados para esse teste podem ser observado na Tabela 4.10.

Tabela 4.10: Latência assimétrica para a solução Cisco com interface G.703 Codir 64 kbps ou interface G.703 2Mbps.

Pré-condições	- Teste apresentado nas Subseção 4.3.1 executado com sucesso.
Procedimentos do teste	- Utilizar interface G.703 Codir 64kbps; - Utilizar o *software* de teleproteção do DIP 5000 para a transmissão de cem amostras contendo quatro comandos em cada (dois DUTT e dois DCB). Os comandos são espaçados num intervalo de um segundo entre o envio de cada amostra e possuem um comprimento de cem milissegundos; - Inicialmente os comandos serão enviados do roteador ASR603-1 para o ASR603-6 e depois do ASR603-6 para o ASR603-1; - Verificar a latência dos comandos de teleproteção através do *software* de teleproteção.
Resultados esperados	Obter valores de latência assimétrica inferiores a quatro ms.

Capítulo 5

Resultados e Análises

Neste capítulo serão apresentados os resultados obtidos para os testes descritos no Capítulo 4. As ferramentas utilizadas para a validação dos resultados foram o *software* da maleta de comandos e o *software* de computação numérica MATLAB.

Através do *software* da maleta, tornou-se possível a coleta dos valores de cada amostra enviada, bem como uma pré-visualização das latências médias referentes a cada comando de teleproteção. Alem disso, a utilização da interface gráfica possibilitou a geração de um gráfico em tempo real referente a latência inserida por cada amostra, em seus respectivos comandos de teleproteção.

Para uma melhor visualização e análise dos resultados, foi utilizada a ferramenta de computação numérica MATLAB. Com a utilização de uma ferramenta de computação numérica, tornou-se possível a importação dos dados coletados pelo *software* da maleta de comandos e o manuseio das informações referentes a cada comando de teleproteção separadamente.

Para cada comando foram calculados a sua média móvel e seus intervalos de confiança. Os intervalos de confiança foram calculados adotando uma confiabilidade de 95% e seguindo uma distribuição Gaussiana.

Inicialmente, serão apresentados os resultados obtidos para os testes da solução *IP Hard-Pipe*, seguido pelos resultados da solução *Flex-LSP*.

5.1 Solução *IP Hard-Pipe*

Tomando como referência o caderno de testes apresentado na Seção 4.2, serão apresentados os resultados dos testes de tempo de operação dos equipamentos de teleproteção, avaliação da solução *Hard-Pipe* sem a inserção de tráfego na rede, avaliação da solução *Hard-Pipe* com a inserção de tráfego na rede, falha de canal na solução *Hard-Pipe*, latência assimétrica na rede *IP* com solução *Hard-Pipe*, e, por fim, a validação da solução.

5.1.1 Tempo de Operação dos Equipamentos de Teleproteção

Assim como descrito na Subseção 4.2.1, neste experimento foram enviados duzentos comandos de teleproteção do equipamento DIP 5000 A para o equipamento DIP 5000 B, sendo estes interligados diretamente. Inicialmente foram avaliados os cenários com interface G.703 Codir 64 kbps. A interface gráfica da maleta de comandos pode ser observada na Figura 5.1.

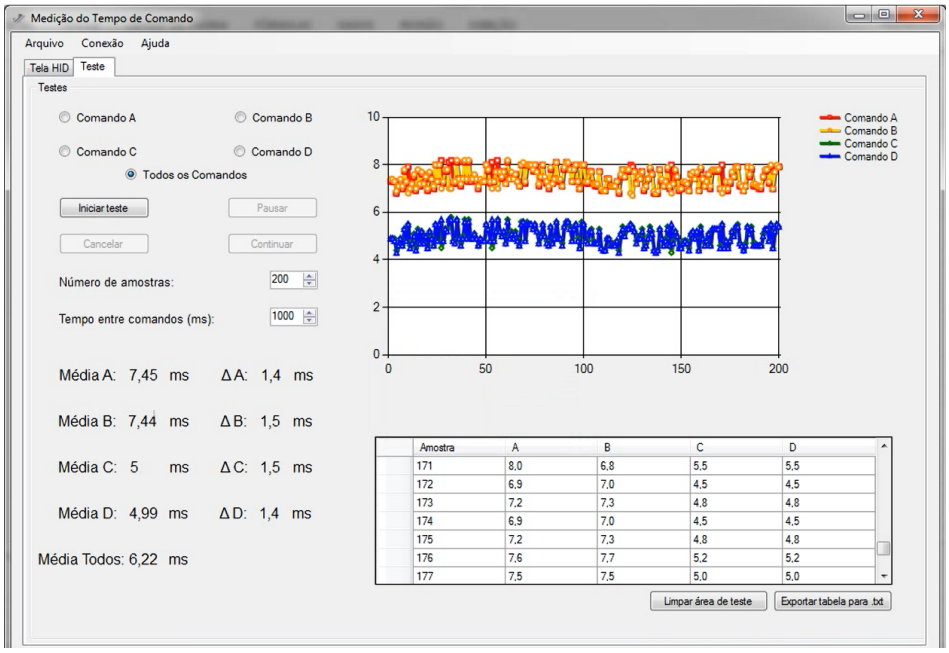


Figura 5.1: Valor médio dos comandos na topologia *Back to Back* com interface G.703 Codir 64 kbps.

Utilizando o *software* da maleta de comandos, foi possível realizar a coleta dos valores referentes à latência de cada amostra enviada. Para uma melhor visualização destes resultados, foi utilizada a ferramenta Matlab. Os resultados obtidos para os comandos diretos (A e B) podem ser observados na Figura 5.2.

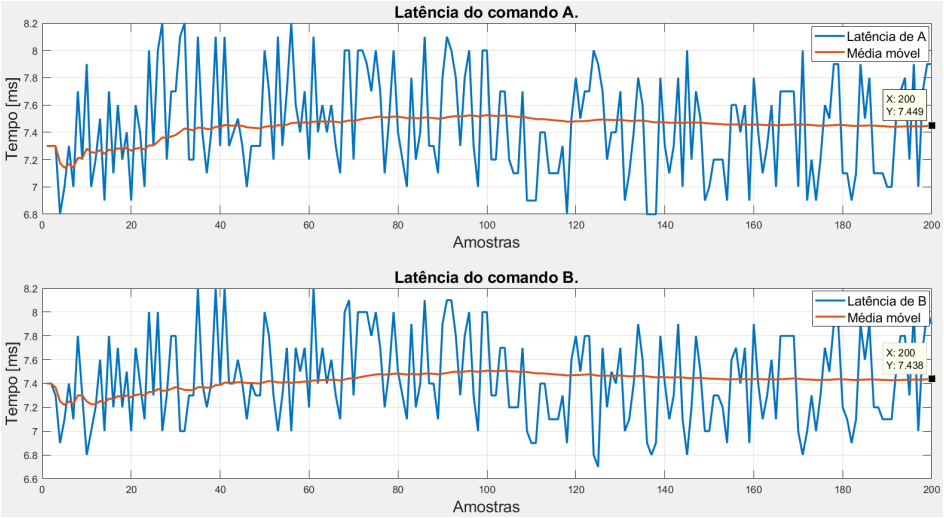


Figura 5.2: Resultados obtidos para os comandos diretos na topologia *Back to Back* com interface G.703 Codir 64 kbps.

Os resultados obtidos para os comandos de bloqueio (C e D) podem ser observados na Figura 5.3.

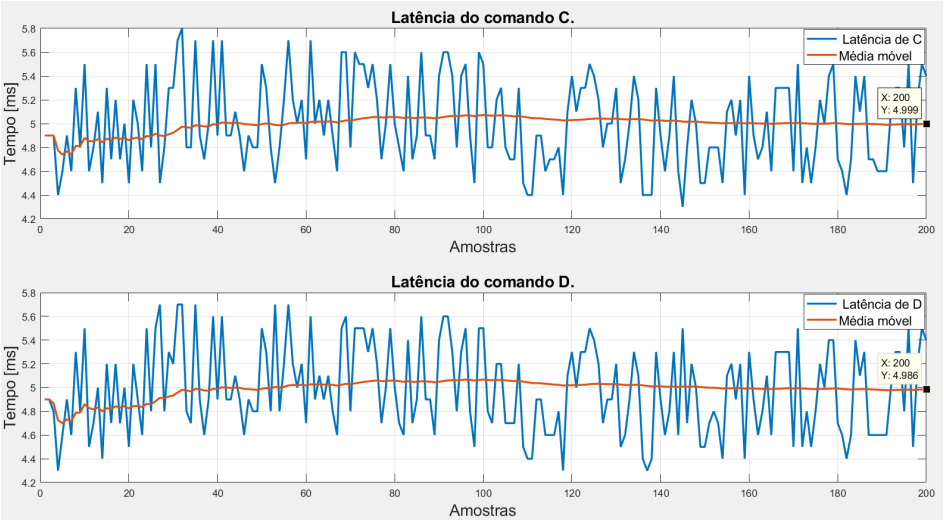


Figura 5.3: Resultados obtidos para os comandos de bloqueio na topologia *Back to Back* com interface G.703 Codir 64 kbps.

Em relação ao cenário com interface G.703 2 Mbps, os resultados obtidos para os comandos diretos (A e B) podem ser observados na Figura 5.4.

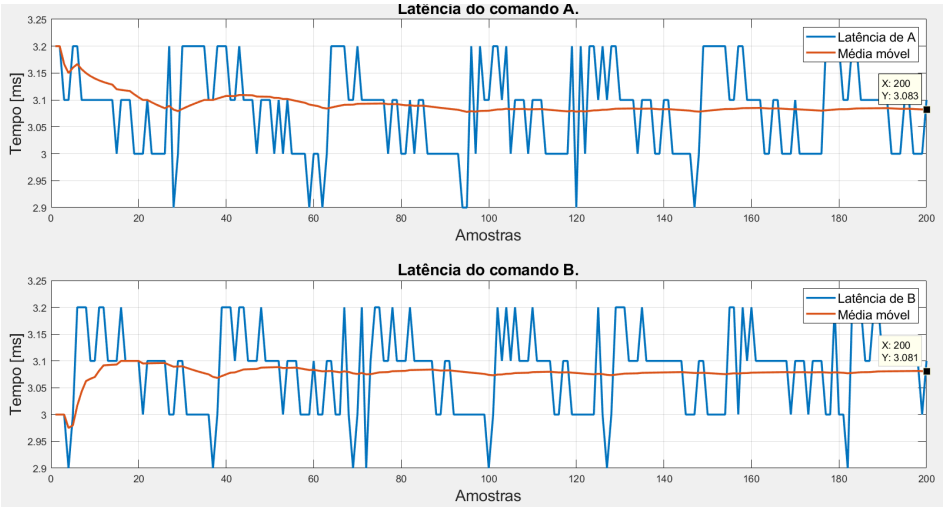


Figura 5.4: Resultados obtidos para os comandos diretos na topologia *Back to Back* com interface G.703 2 Mbps.

Os resultados obtidos para os comandos de bloqueio (C e D) podem ser observados na Figura 5.5.

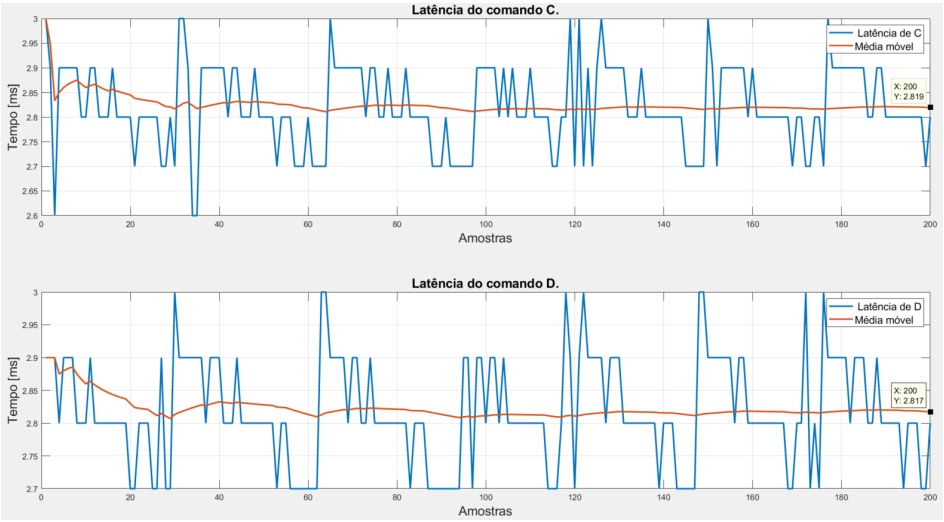


Figura 5.5: Resultados obtidos para os comandos de bloqueio na topologia *Back to Back* com interface G.703 2 Mbps.

Ainda utilizando o *software* Matlab, foi realizado o cálculo do intervalo de confiança dos vetores de comandos de teleproteção. A Tabela 5.1 apresenta os valores dos intervalos de confiança e da latência média obtida para os comandos A, B, C e D.

Tabela 5.1: Intervalos de confiança e latências médias para os comandos de teleproteção na topologia *Back to Back*.

	Comando	Intervalo de confiança (ms)	Latência média (ms)
G.703 Codir	**A**	**7,3966 e 7,5004**	**7,4485**
	B	**7,3870 e 7,4890**	**7,4380**
	C	**4,9480 e 5,0500**	**4,9990**
	D	**4,9351 e 5,0379**	**4,9865**
G.703 2 Mbps	**A**	**3,0710 e 3,09404**	**3.0825**
	B	**3,0702 e 3,0918**	**3,0810**
	C	**2,8077 e 2,8313**	**2,8195**
	D	**2,8063 e 2,8287**	**2,8175**

Pode-se observar através das Figuras 5.2, 5.3, 5.4 e 5.5 que a média calculada ponto-a-ponto tende à estabilidade com duzentas amostras. Também é possível verificar que o valor de latência média está abaixo dos dez ms padronizados através da norma IEC 60834-1.

Ao final deste teste, foram obtidos os valores de latência para os equipamentos de teleproteção. Com base nos resultados obtidos, pode-se avaliar tanto o tempo do sistema, como o tempo de rede nos próximos testes. O tempo de rede é obtido através de uma subtração entre o tempo do sistema e o tempo de operação dos equipamentos de teleproteção.

5.1.2 Avaliação da Solução *Hard-Pipe* sem a Inserção de Tráfego na Rede

Como descrito na subseção 4.2.2, neste cenário será avaliada a solução *Hard-Pipe* sem que ocorra a inserção de tráfego na rede. Após o envio das duzentas amostras, os resultados obtidos para os comandos DUTT na interface G.703 Codir 64 kbps podem ser observados na Figura 5.6.

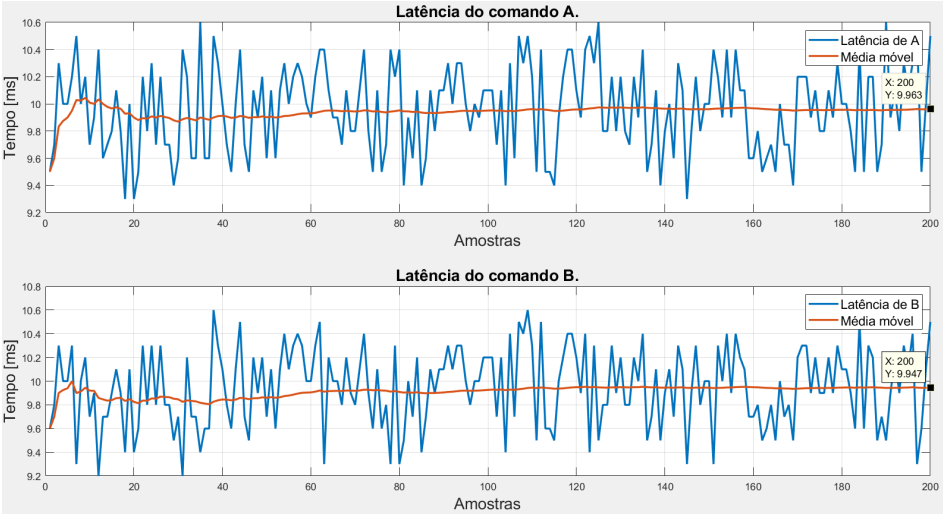


Figura 5.6: Resultados obtidos para os comandos diretos na topologia sem inserção de tráfego e com interface G.703 Codir 64 kbps.

Os resultados obtidos para os comandos DCB podem ser observados na Figura 5.7.

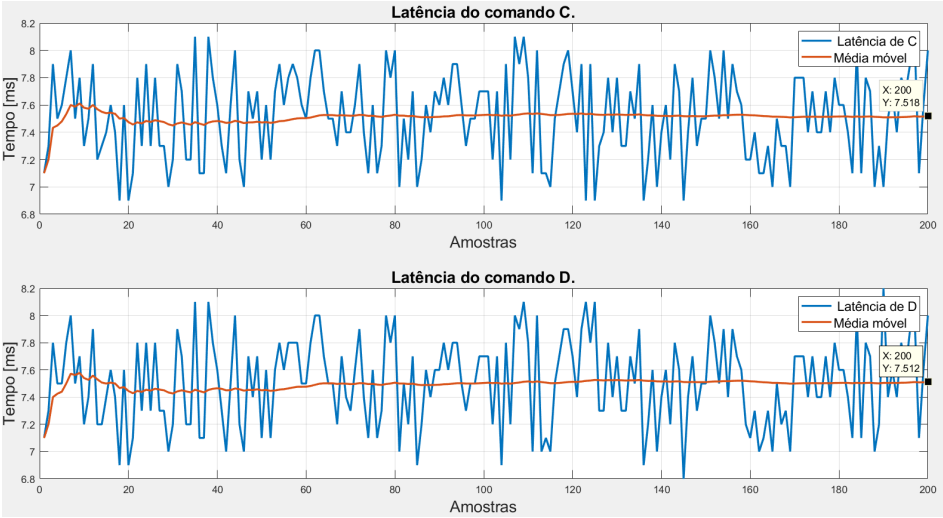


Figura 5.7: Resultados obtidos para os comandos de bloqueio na topologia sem inserção de tráfego e com interface G.703 Codir 64 kbps.

Os resultados obtidos para os comandos DUTT e DCB na topologia com interface G.703 2 Mbps podem ser observados, respectivamente, nas Figuras 5.8 e 5.9.

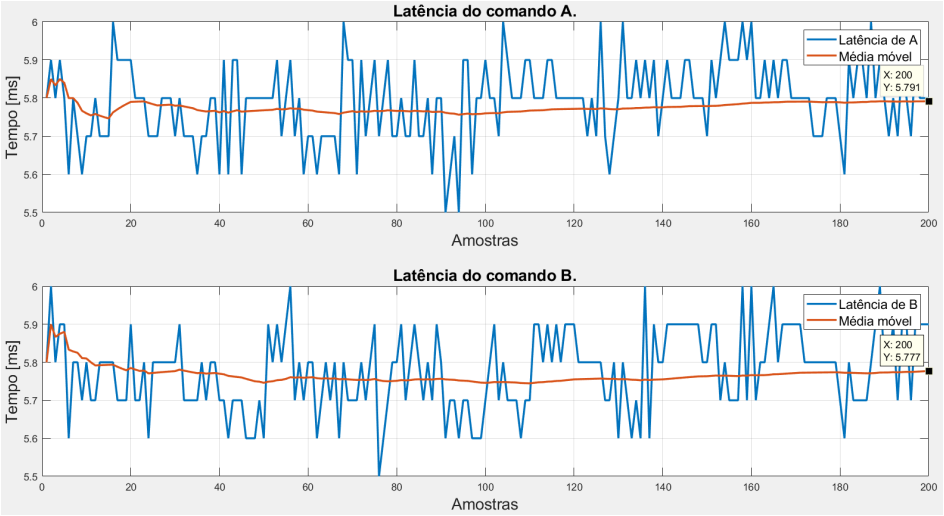


Figura 5.8: Resultados obtidos para os comandos diretos na topologia sem inserção de tráfego e com interface G.703 2 Mbps.

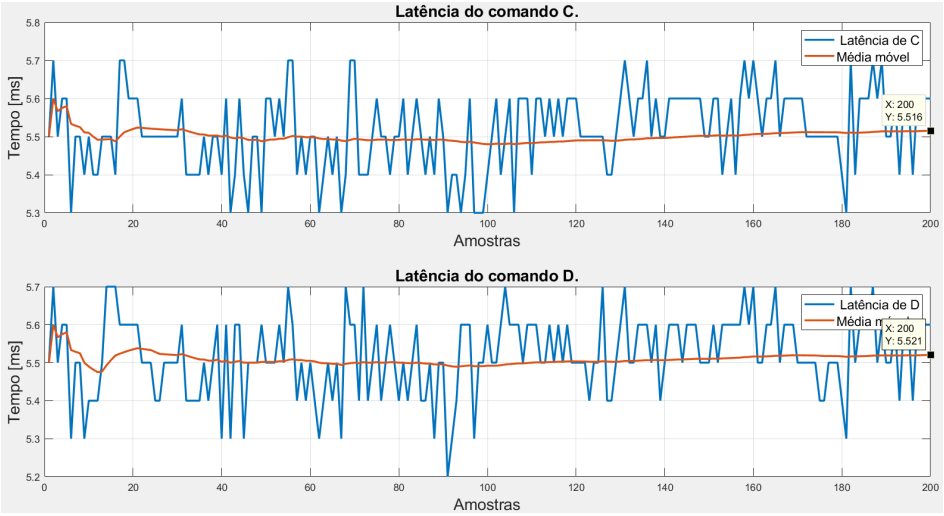


Figura 5.9: Resultados obtidos para os comandos de bloqueio na topologia sem tráfego e com interface G.703 2M.

Os valores referentes aos intervalos de confiança e latência média dos comandos de teleproteção podem ser observados na Tabela 5.2.

Tabela 5.2: Intervalos de confiança e latência média do sistema para os comandos de teleproteção com topologia sem inserção de tráfego na solução *IP Hard-Pipe*.

	Comando	Intervalo de confiança (ms)	Latência média (ms)
G.703 Codir	**A**	**9,9181 e 10,0079**	**9,9630**
	B	**9,9010 e 9,9930**	**9,9470**
	C	**7,4735 e 7,5625**	**7,5180**
	D	**7,4670 e 7,5560**	**7,5115**
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**

Com os valores de latência média do sistema obtidos durante este experimento e os valores de latência média encontrados no teste 5.1.1, tornou-se possível a obtenção dos tempos gastos pelos comandos de teleproteção na rede de comunicação. O valor médio do tempo de rede, como será referido daqui em diante, para os comandos A, B, C e D foram de, respectivamente, 2,5145 ms, 2,509 ms, 2,519 ms e 2,525 ms para a interface G.703 Codir 64 kbps e 2,709 ms, 2,696 ms, 2,696 ms e 2,703 ms para interface G.703 2 Mbps.

Através dos gráficos apresentados nas Figuras 5.6, 5.7, 5.8 e 5.9 pode-se observar que as médias tenderam a se estabilizar e que os valores obtidos estão dentro dos intervalos de confiança apresentados na Tabela 5.2. Os valores médios estão dentro dos dez ms estipulados, mas para os comandos diretos (A e B) no cenário com interface G.703 Codir 64 kbps, foi possível observar a incidência de amostras com valores superiores aos dez ms estipulados pela norma IEC 60834-1.

5.1.3 Avaliação da Solução *Hard-Pipe* com a Inserção de Tráfego na Rede

Nesta subseção, serão apresentados os resultados referentes aos cenários com inserção de tráfego na rede para a solução *IP Hard-Pipe*. Após o envio dos duzentas amostras, os resultados obtidos para os comandos diretos na topologia com interface G.703 Codir 64 kbps podem ser observados na Figura 5.10.

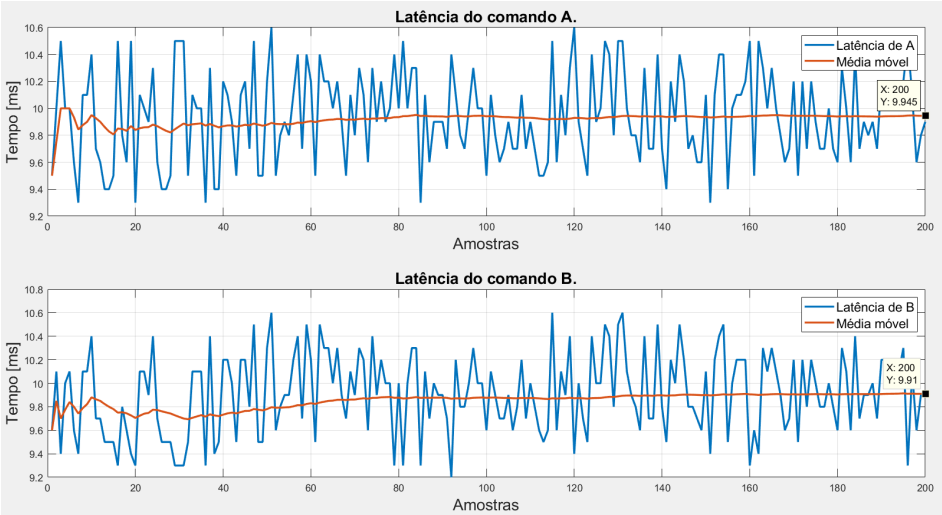


Figura 5.10: Resultados obtidos para os comandos diretos na topologia com inserção de tráfego e com interface G.703 64 kbps.

Os comandos de bloqueio podem ser observados na Figura 5.11.

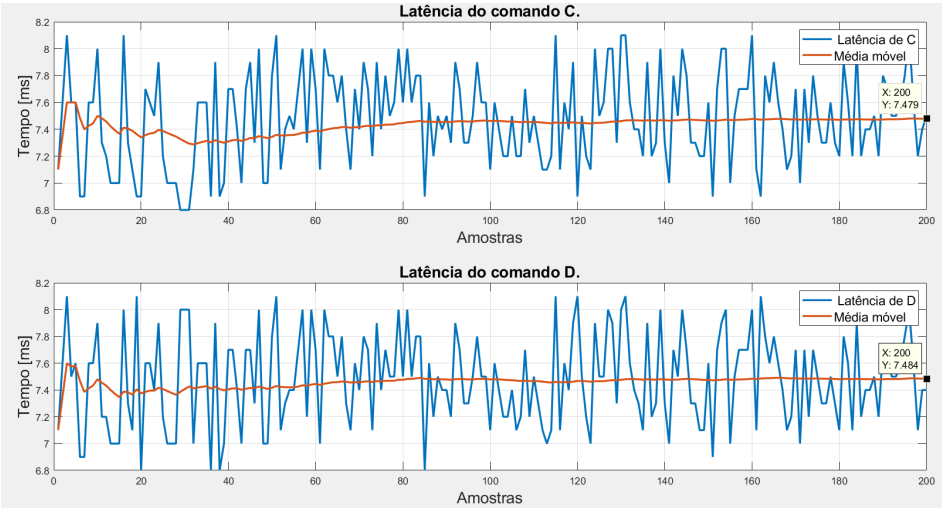


Figura 5.11: Resultados obtidos para os comandos de bloqueio na topologia com inserção de tráfego e com interface G.703 64 kbps.

A seguir serão apresentados os resultados obtidos para a topologia com interface G.703 2 Mbps. Os resultados referentes às latências médias e médias móveis dos comandos de teleproteção para os comandos DUTT e DCB podem ser observados, respectivamente, nas Figuras 5.12 e 5.13.

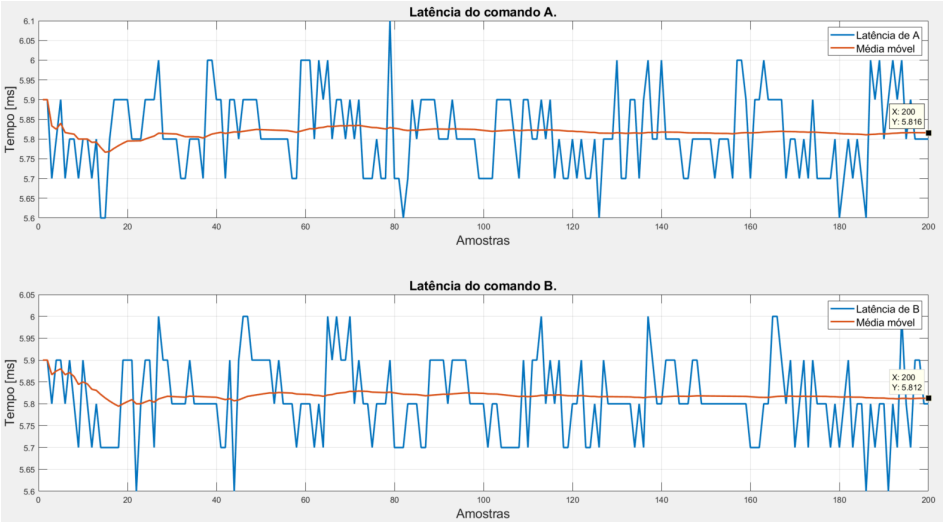


Figura 5.12: Resultados obtidos para os comandos diretos na topologia com inserção de tráfego e com interface G.703 2 Mbps.

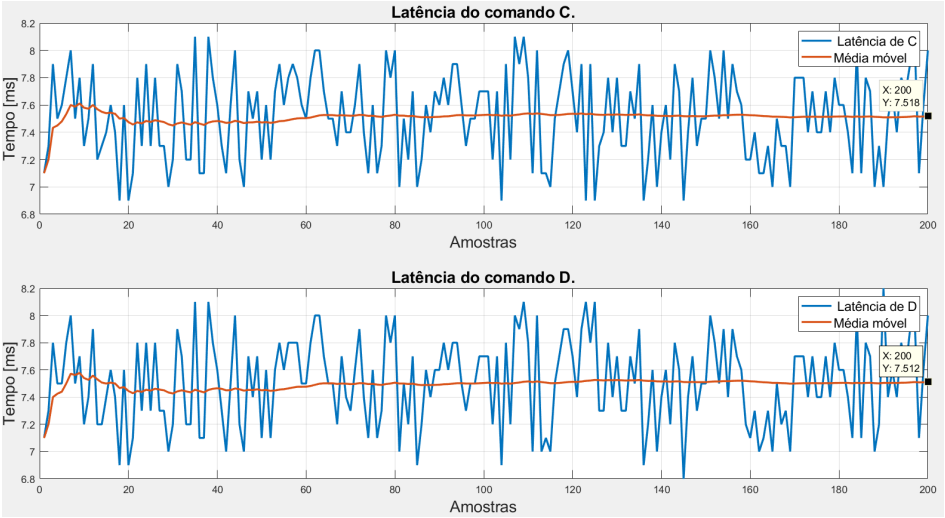


Figura 5.13: Resultados obtidos para os comandos de bloqueio na topologia com inserção de tráfego e com interface G.703 2 Mbps.

Para este experimento, os valores obtidos através do gerador de tráfego, referentes ao *Soft-Pipe* podem ser observados na Figura 5.14.

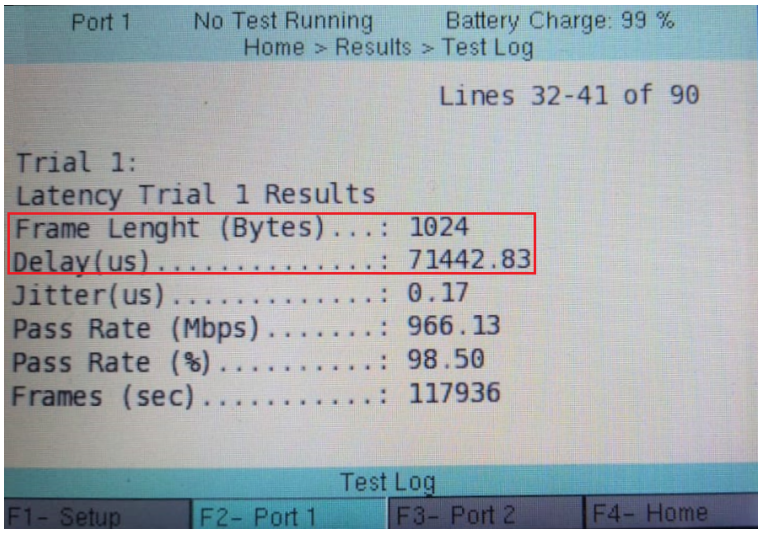


Figura 5.14: Resultados obtidos através do gerador de tráfego para o *Soft-Pipe* estabelecido no *link* Principal.

Como a solução prevê o isolamento entre os planos *Hard-Pipe* e *Soft-Pipe*, com o auxilio do equipamento TSW900ETH, foi realizado o envio de tráfego no *Hard-Pipe* para obtenção dos parâmetros referentes ao canal utilizado para o envio dos comandos de teleproteção. Sendo assim, os valores obtidos através do gerador de tráfego podem ser observados na Figura 5.15.

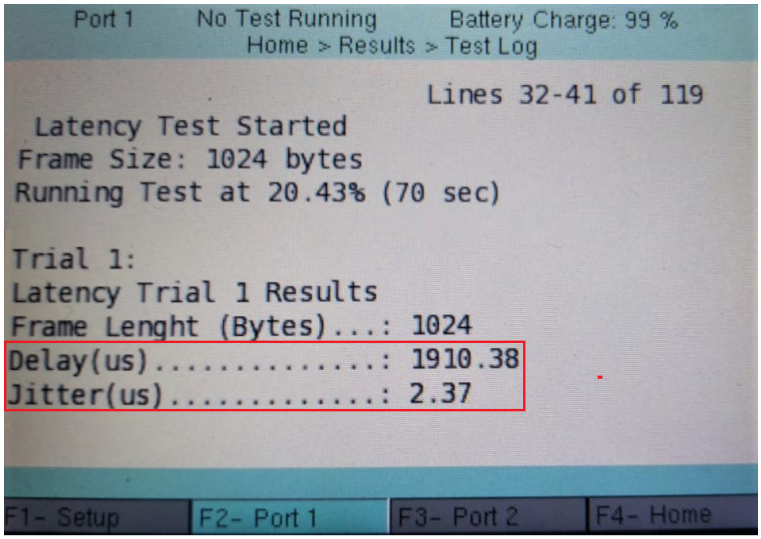


Figura 5.15: Resultados obtidos através do gerador de tráfego para o *Hard-Pipe* estabelecido no *link* Principal.

Os valores referentes aos intervalos de confiança e as latências médias dos comandos de teleproteção podem ser observados na Tabela 5.3.

Tabela 5.3: Intervalos de confiança e latências médias para os comandos de teleproteção com topologia com inserção de tráfego e interfaces G.703 Codir 64 kbps e G.703 2 Mbps.

	Comando	**Intervalo de confiança (ms)**	**Latência média (ms)**
G.703 Codir	**A**	**9,8979 e 9,9911**	**9.9445**
	B	**9,8627 e 9,9573**	**9,9100**
	C	**7,4314 e 7,5266**	**7,4790**
	D	**7,4374 e 7,5316**	**7,4845**
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**

Os valores médios de tempo de rede para os comandos A, B, C e D foram de, respectivamente, 2,496, 2,472, 2,48 e 2,498 ms para interface G.703 Codir 64 kbps, e 2,7335, 2,7315, 2,721 e 2,7285 ms para a topologia com interface G.703 2 Mbps.

Ao final deste experimento, pode ser constatado que os valores de latência média para os comandos A, B, C e D não foram afetados pela inserção de tráfego no *Soft-Pipe*. Posteriormente, será verificada a capacidade de isolação entre os planos *Hard-Pipe* e *Soft-Pipe*.

Os valores obtidos para a latência média dos comandos de teleproteção e o *Jitter* do canal se mantiveram dentro do estabelecido pela norma IEC 60834-1 (10 ms e 15.6 μs respectivamente), assim como os valores do intervalo de confiança. Como esperado para este cenário, também ocorreram valores de amostras superiores aos dez ms pré-estabelecidos.

5.1.4 Falha de Canal na Solução *Hard-Pipe*

Assim como descrito na Subseção 4.5, neste tópico serão apresentados os resultados obtidos para o teste de falha de canal do *link* principal. Os resultados obtidos para os comandos A e B com interface G.703 Codir 64 kbps podem ser observados na Figura 5.16.

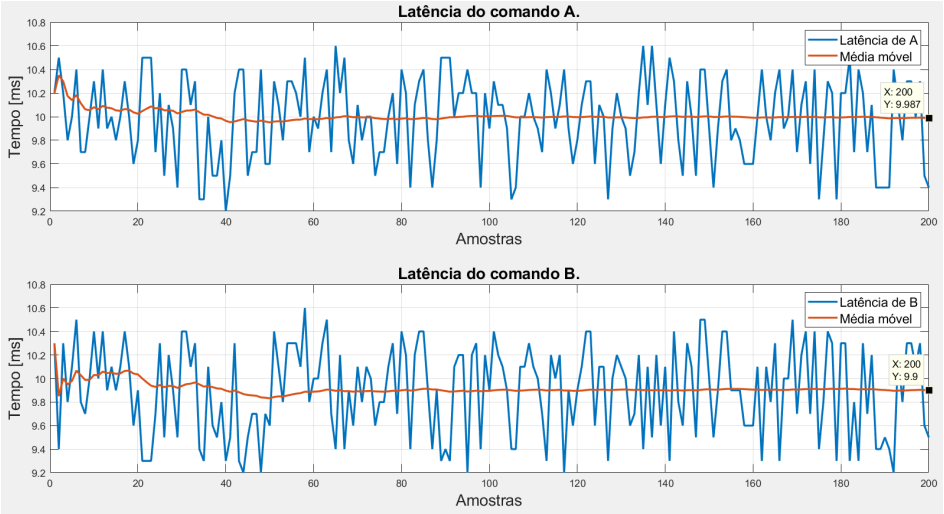


Figura 5.16: Resultados obtidos para os comandos diretos no teste de falha do canal principal com interface G.703 Codir 64 kbps.

Os resultados para os comandos C e D podem ser observados na Figura 5.17.

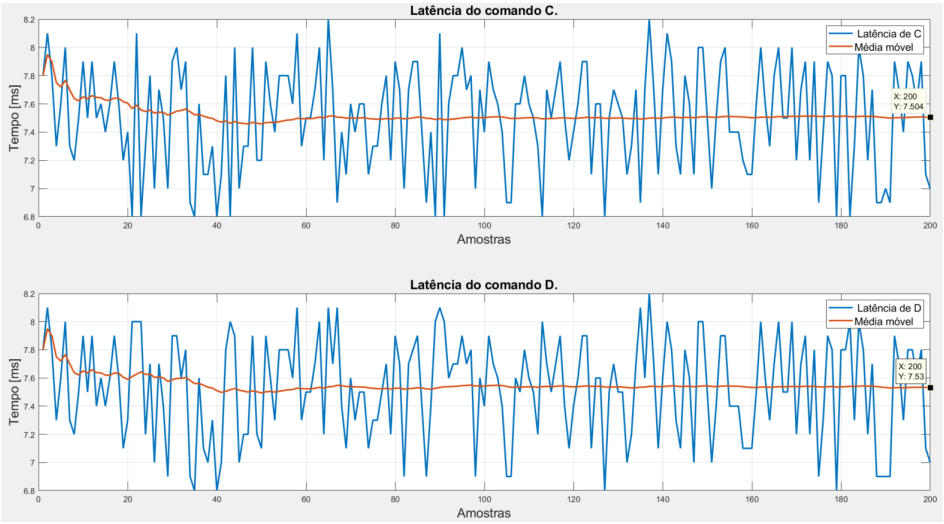
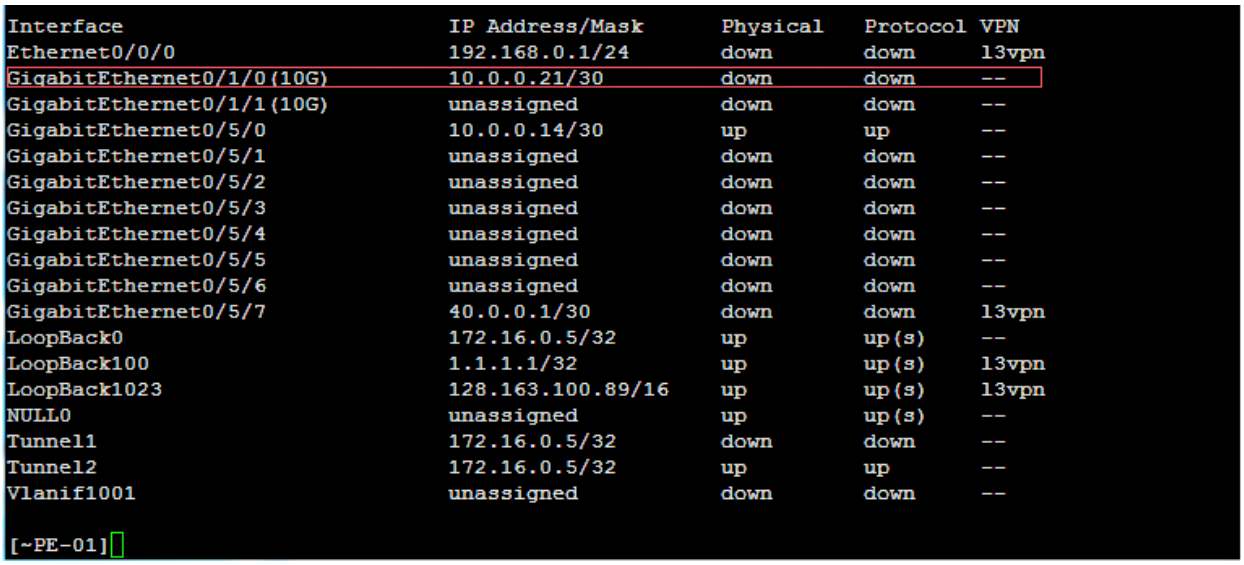


Figura 5.17: Resultados obtidos para os comandos de bloqueio no teste de falha do canal principal com interface G.703 Codir 64 kbps.

Após o envio da quinquagésima amostra, o caminho principal foi derrubado manualmente e o restante das amostras foram trafegadas através do caminho alternativo. A queda do caminho principal, definido através da interface *GigabitEthernet* 0/1/0, após o envio da quinquagésima amostra, pode ser evidenciado na Figura 5.18.



Interface	IP Address/Mask	Physical	Protocol	VPN
Ethernet0/0/0	192.168.0.1/24	down	down	l3vpn
GigabitEthernet0/1/0(10G)	10.0.0.21/30	down	down	--
GigabitEthernet0/1/1(10G)	unassigned	down	down	--
GigabitEthernet0/5/0	10.0.0.14/30	up	up	--
GigabitEthernet0/5/1	unassigned	down	down	--
GigabitEthernet0/5/2	unassigned	down	down	--
GigabitEthernet0/5/3	unassigned	down	down	--
GigabitEthernet0/5/4	unassigned	down	down	--
GigabitEthernet0/5/5	unassigned	down	down	--
GigabitEthernet0/5/6	unassigned	down	down	--
GigabitEthernet0/5/7	40.0.0.1/30	down	down	l3vpn
LoopBack0	172.16.0.5/32	up	up(s)	--
LoopBack100	1.1.1.1/32	up	up(s)	l3vpn
LoopBack1023	128.163.100.89/16	up	up(s)	l3vpn
NULL0	unassigned	up	up(s)	--
Tunnel1	172.16.0.5/32	down	down	--
Tunnel2	172.16.0.5/32	up	up	--
Vlanif1001	unassigned	down	down	--

[~PE-01]

Figura 5.18: Queda do *link* principal.

Através da Figura 5.18, é possível observar que a interface dedicada para a formação do caminho principal apresenta o *status "down"*, enquanto a interface dedicada para a formação do caminho alternativo, *GigabitEthernet* 0/5/0, apresenta o *status "up"*, comprovando a queda do caminho principal e o envio dos comandos pelo caminho alternativo.

A Tabela 5.4 apresenta os valores obtidos para o cenário atual e o cenário de rede *IP* sem inserção de tráfego.

Tabela 5.4: Comparação entre os valores obtidos no teste de falha de canal e rede *IP* sem inserção de tráfego.

Comando	**Latência para os comandos no teste de falha de canal (ms)**	**Latência para os comandos no teste de rede IP sem tráfego (ms)**
A	**9,987**	**9,963**
B	**9,9005**	**9,947**
C	**7,5035**	**7,518**
D	**7,53**	**7,5125**

Através destes resultados, pode-se comprovar que a queda do caminho principal, e a necessidade de envio dos comandos por uma rota mais longa (seis roteadores), não afetou o desempenho do sistema. Isto pode ser justificado pela grande capacidade de processamento destes roteadores, sendo esses desenvolvidos para o processamento de uma quantidade massiva de dados e, também, pelo fato de que a distância entre os mesmos é pequena. Em um ambiente real, a distância entre os roteadores pode chegar na casa das centenas de km, enquanto no laboratório foi utilizado pouco mais do que dezenas de metros de fibra.

5.1.5 Latência Assimétrica na rede *IP* com Solução *Hard-Pipe*

Assim como descrito na Subseção 4.2.5, neste tópico serão apresentados os resultados para o cenário de assimetria de canal na topologia com interface G.703 Codir 64kbps. Inicialmente, é realizado o envio dos comandos do equipamento de teleproteção DIP 5000 A para o equipamento DIP 5000 B.

Os resultados obtidos para os comandos diretos (A e B) e os comandos de bloqueio (C e D) podem ser observados na Figura 5.19.

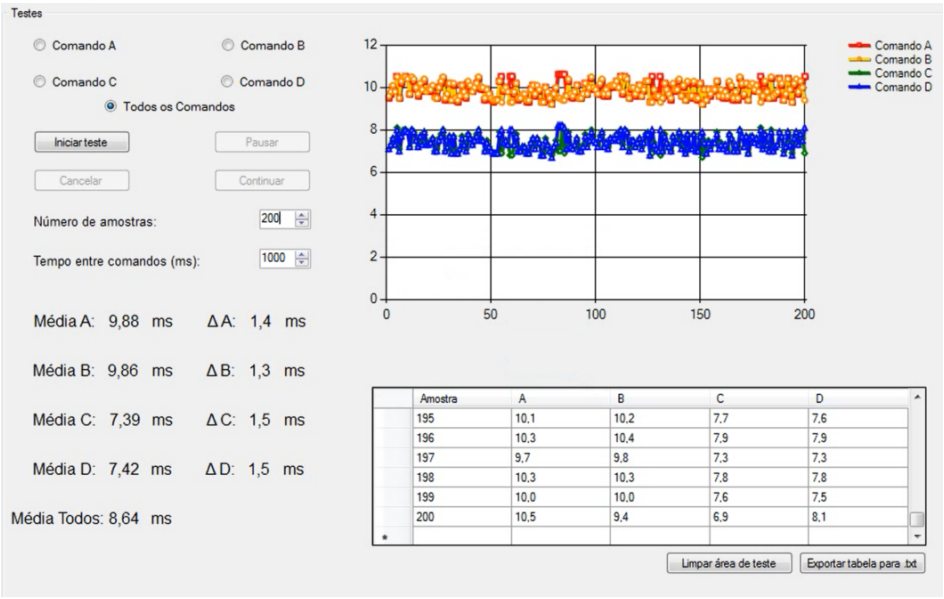


Figura 5.19: Resultados obtidos para os comandos enviados do Equipamento DIP 5000 A para o DIP 5000 B.

Os resultados obtidos para os comandos enviados do equipamento DIP 5000 B para o equipamento DIP 5000 A podem ser observados na Figura 5.20.

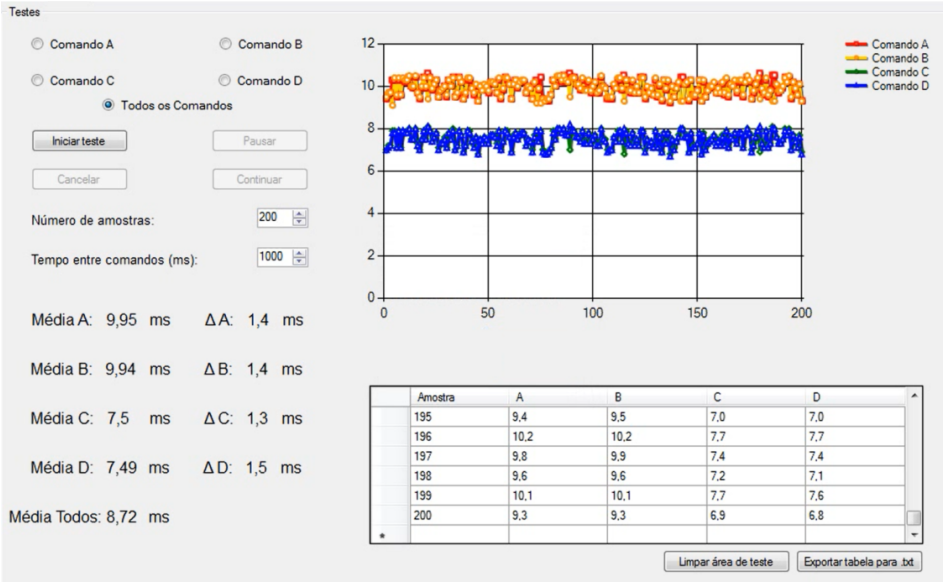


Figura 5.20: Resultados obtidos para os comandos enviados do Equipamento DIP 5000 B para o DIP 5000 A.

Através destes resultados, os valores de latência assimétrica média para os comandos A, B, C e D foram de, respectivamente, 0,07 ms, 0,08 ms, 0,11 ms e 0,07 ms. Os resultados obtidos foram menores que os quatro ms estabelecidos pela norma IEC 60834-1.

5.1.6 Validação da Solução

Neste teste são avaliados os principais pontos levantados pelo fabricante, assim como descrito na Subseção 4.2.6. O primeiro cenário foi elaborado com o *Hard-Pipe* dimensionado para 800 Mbps, o *Soft-Pipe* dimensionado para 200 Mbps e o auxilio de três computadores gerando, aproximadamente, 1 Gbps através do *software Jperf*.

Os resultados obtidos na interface *GigabitEthernet* 0/5/0 do roteador PE-02 podem ser observados na Figura 5.21. Vale ressaltar que todo o tráfego foi inserido através do *Soft-Pipe*.

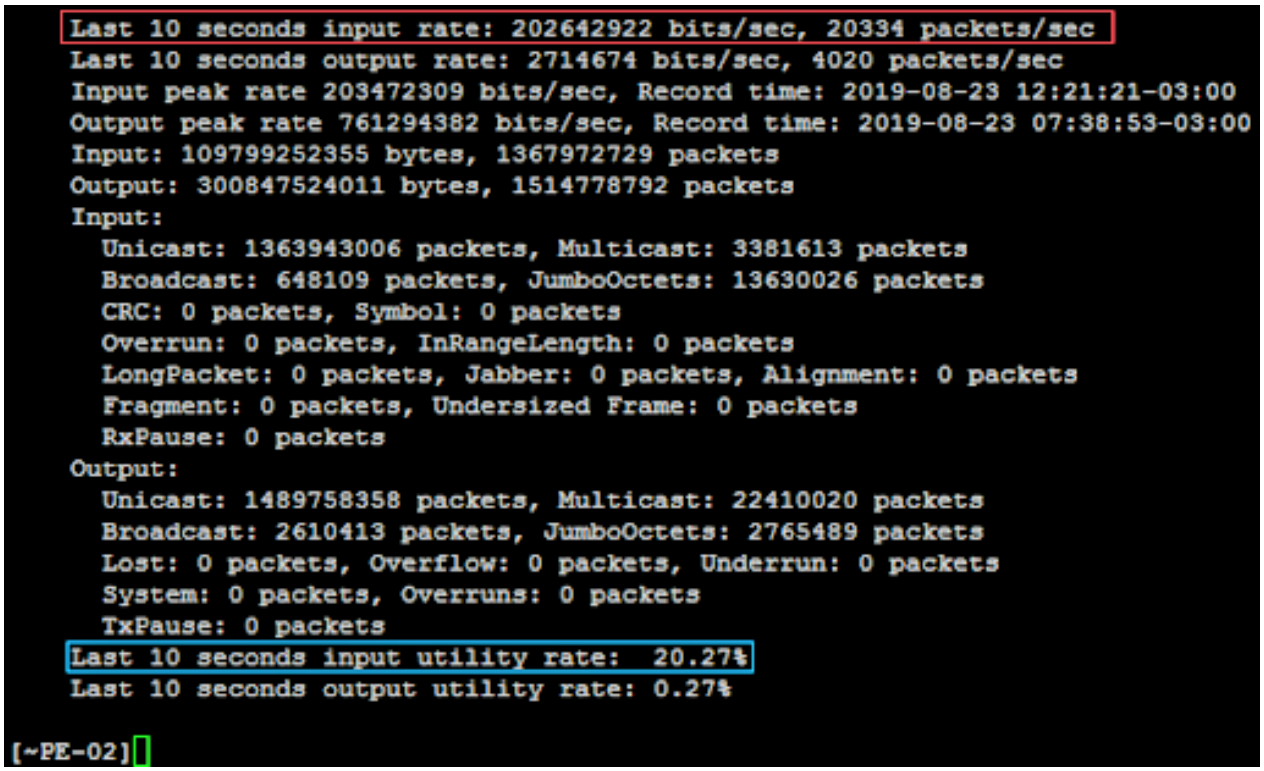


Figura 5.21: Valores obtidos para o cenário com *Hard-Pipe* dimensionado para 800 Mbps e o *Soft-Pipe* dimensionado para 200 Mbps.

O segundo cenário foi implementado com o *Hard-Pipe* dimensionado para 980 Mbps e o *Soft-Pipe* para 20 Mbps. Com o auxílio dos geradores de tráfego, os resultados obtidos na interface *GigabitEthernet* 0/5/0 do roteador PE-02 podem ser observados na Figura 5.22.

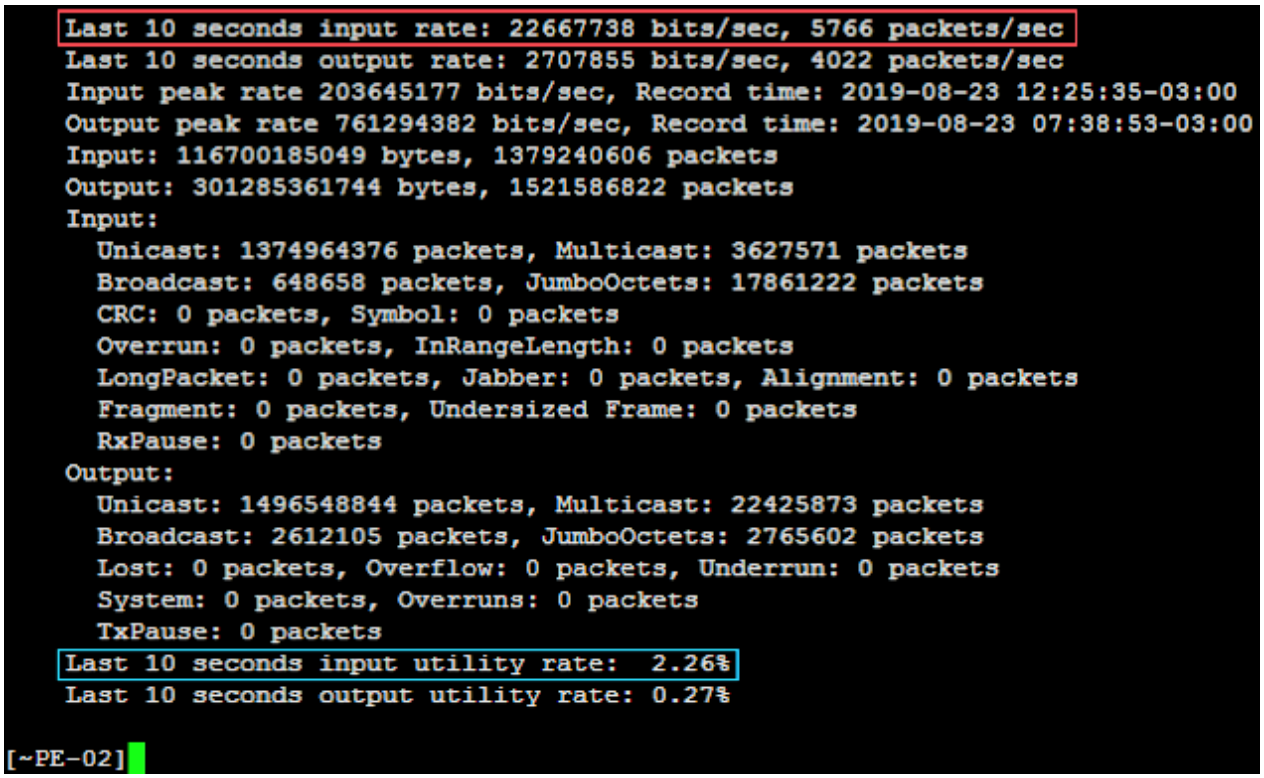


Figura 5.22: Valores obtidos para o cenário com *Hard-Pipe* dimensionado para 980 Mbps e o *Soft-Pipe* dimensionado para 20 Mbps.

Através destes resultados foi observado que houve uma isolação entre os planos conforme afirmados pelo fornecedor. No primeiro cenário, a solução permitiu que pouco mais que os 200 Mbps configurados trafegassem pelo *Soft-Pipe*, assim como no cenário 2, onde a solução permitiu que pouco mais do que os 20 Mbps configurados trafegassem pela rede.

5.2 Solução *Flex-LSP*

Tomando como referência o caderno de testes presente na Seção 4.3, serão apresentados os resultados dos testes de tempo operação dos equipamentos de teleproteção, avaliação da solução *Flex-LSP* sem inserção de tráfego na rede, avaliação da solução *Flex-LSP* com a inserção de tráfego na rede, falha de canal, e, por fim, latência assimétrica.

5.2.1 Tempo de Operação dos Equipamentos de Teleproteção

Análogo ao procedimento realizado durante os testes com a solução *IP Hard-Pipe*, neste experimento foi determinado o tempo de operação dos equipamentos de teleproteção DIP

5000. O teste foi realizado através do envio de duzentas amostras do equipamento DIP 5000 A para o Equipamento DIP 5000 B, sendo estes interligados diretamente.

Inicialmente, é abordado o cenário com interface G.703 Codir 64 kbps. Os resultados de latência obtidos para os comandos diretos A e B podem ser observados na Figura 5.23.

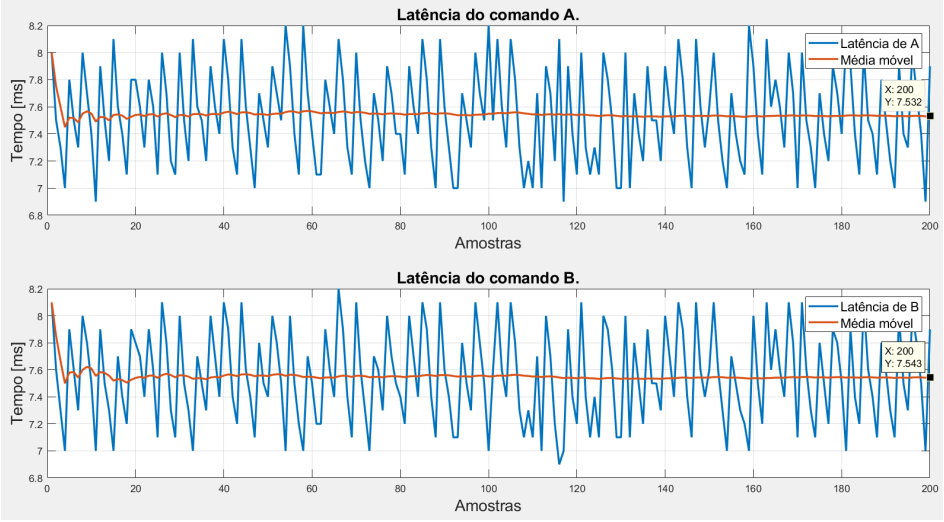


Figura 5.23: Resultados obtidos para os comandos diretos na topologia *Back to Back* com interface G.703 Codir 64 kbps.

Os resultados obtidos para os comandos de bloqueio C e D podem ser observados na Figura 5.24.

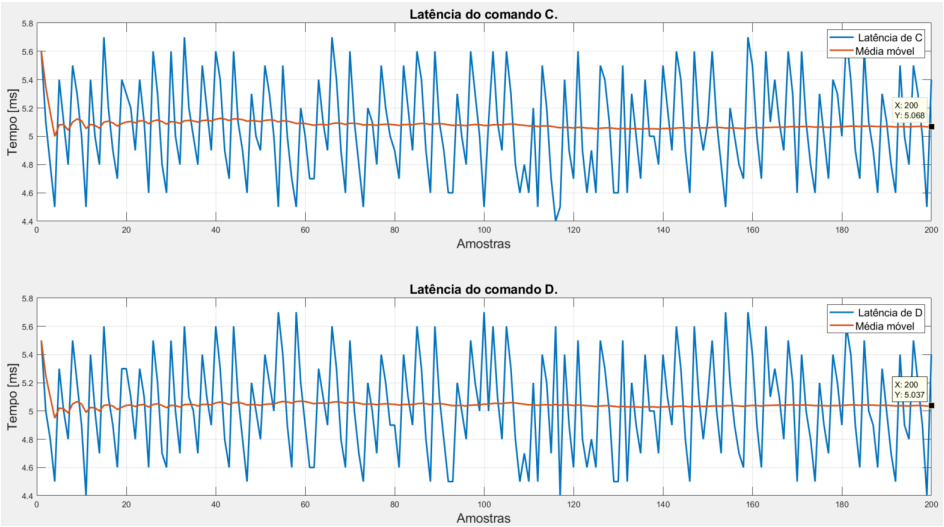


Figura 5.24: Resultados obtidos para os comandos de bloqueio na topologia *Back to Back* com interface G.703 Codir 64 kbps.

A seguir, serão apresentados os resultados obtidos para o teste com interface G.703 2 Mbps. Os resultados obtidos para os comandos DUTT podem ser observados na Figura 5.25.

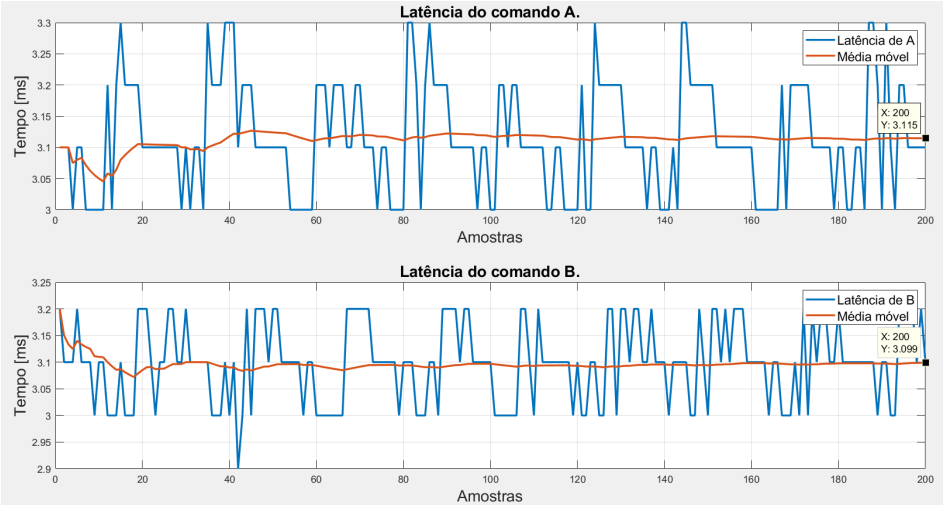


Figura 5.25: Resultados obtidos para os comandos diretos na topologia *Back to Back* com interface G.703 Codir 2 Mbps.

Os resultados obtidos para os comandos DCB podem ser observados na Figura 5.26.

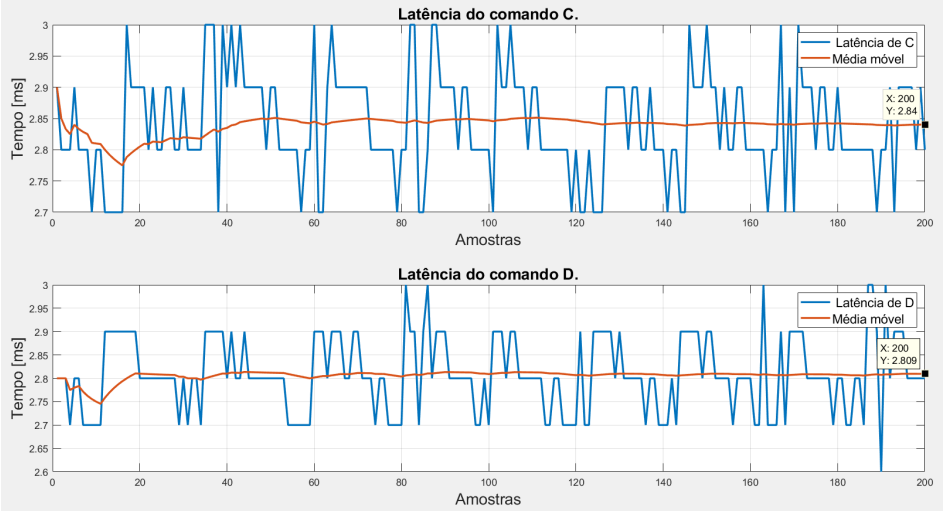


Figura 5.26: Resultados obtidos para os comandos de bloqueio na topologia *Back to Back* com interface G.703 Codir 2 Mbps.

Os valores dos intervalos de confiança, calculados através das amostras dos comandos de teleproteção obtidos através do teste de tempo de operação dos equipamentos de teleproteção, e as latências médias dos comandos de teleproteção podem ser observados na Tabela 5.5.

Tabela 5.5: Intervalos de confiança e latências médias para os comandos de teleproteção na topologia *Back to Back* com a solução *Flex-LSP*.

	Comando	Intervalo de confiança (ms)	Latência média (ms)
G.703 Codir	**A**	**7,4823 e 7,5807**	**7,5315**
	B	**7,4955 e 7,5915**	**7,5435**
	C	**5,0195 e 5,1165**	**5,0680**
	D	**4,9877 e 5,0863**	**5,0370**
G.703 2 Mbps	**A**	**3,1022 e 3,1268**	**3,1145**
	B	**3,0886 e 3,1094**	**3,0990**
	C	**2,8282 e 2,8518**	**2,8400**
	D	**2,7982 e 2,8208**	**2,8095**

Os valores obtidos para a latência dos comandos de teleproteção se mantiveram dentro dos dez ms estabelecidos pela norma IEC 60834-1. Estes resultados serão utilizados para o cálculo do tempo de rede nos testes subsequentes. O tempo de rede é obtido através da subtração entre os valores de latência do sistema e do tempo de operação dos equipamentos de teleproteção.

5.2.2 Avaliação da Solução *Flex-LSP* sem a Inserção de Tráfego na Rede

Tomando como referência os procedimentos apresentados na subseção 4.3.1, neste experimento é avaliado o desempenho da solução *Flex-LSP* quando não ocorre a inserção de tráfego no sistema. Após o envio das duzentas amostras, os resultados obtidos para os comandos DUTT na interface G.703 Codir 64 kbps podem ser observados na Figura 5.27.

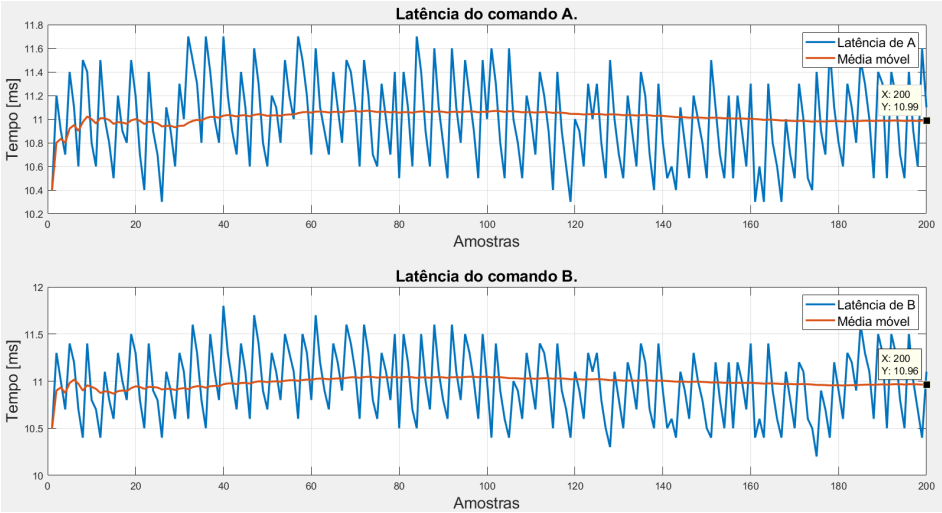


Figura 5.27: Resultados obtidos para os comandos diretos na topologia sem inserção de tráfego e com interface G.703 Codir 64 kbps.

Os resultados obtidos para os comandos DCB podem ser observados na Figura 5.28.

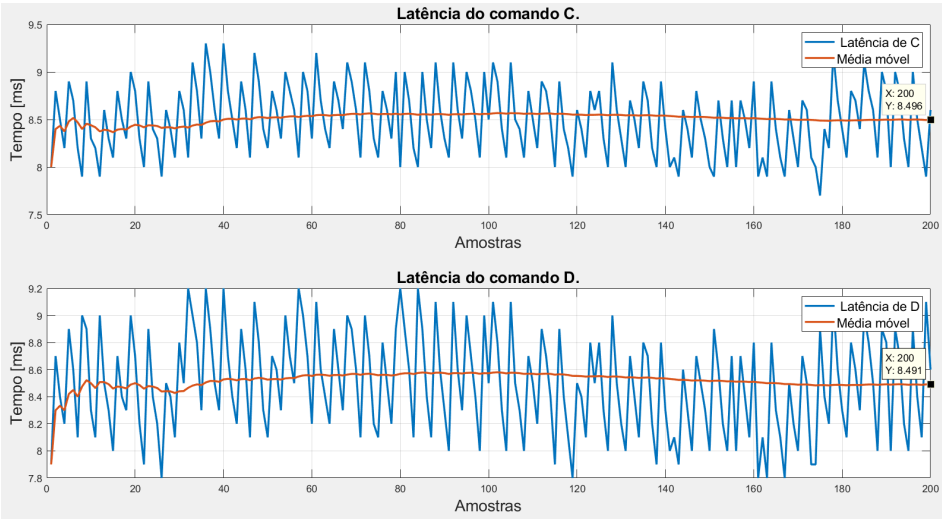


Figura 5.28: Resultados obtidos para os comandos de bloqueio na topologia sem inserção de tráfego e com interface G.703 Codir 64 kbps.

A seguir, serão apresentados os resultados referentes ao teste com topologia sem inserção de tráfego e com interface G.703 2 Mbps entre os equipamentos de teleproteção e roteadores. Os valores de latência média dos comandos DUTT e DCB podem ser observados, respectivamente, nas Figuras 5.29 e 5.30.

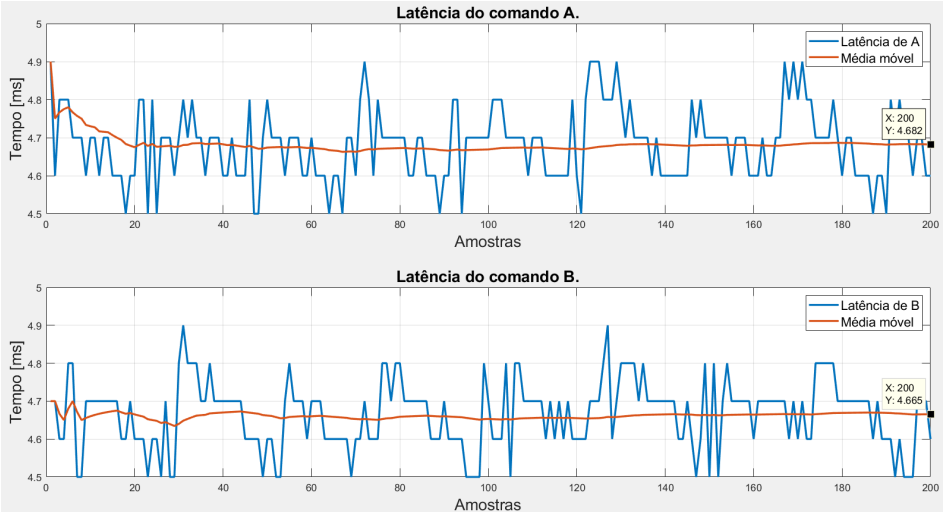


Figura 5.29: Resultados obtidos para os comandos diretos na topologia sem inserção de tráfego e com interface G.703 2 Mbps.

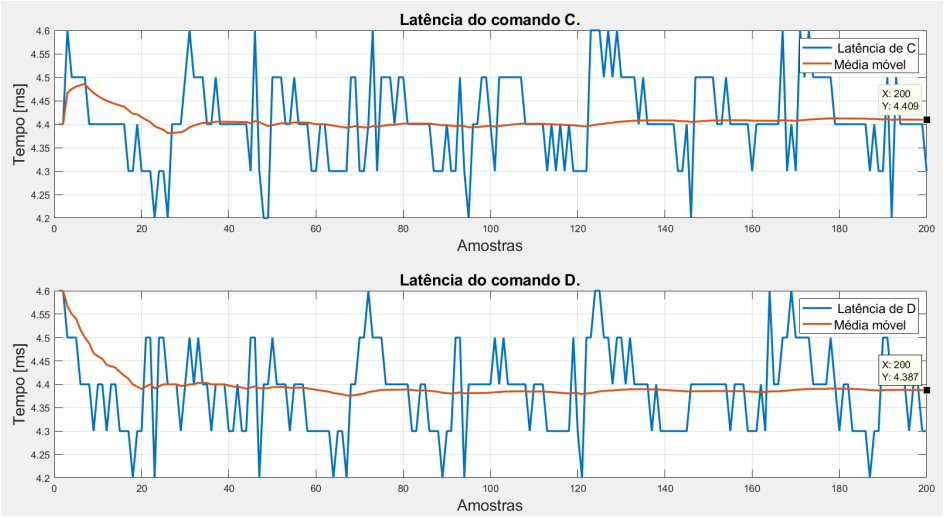


Figura 5.30: Resultados obtidos para os comandos de bloqueio na topologia sem inserção de tráfego e com interface G.703 2 Mbps.

Os valores referentes aos intervalos de confiança e latência média dos comandos de teleproteção para o teste com topologia sem inserção de tráfego podem ser observados na Tabela 5.6.

Tabela 5.6: Intervalos de confiança e latência média para os comandos de teleproteção com topologia sem inserção de tráfego na solução *Flex-LSP*.

	Comando	**Intervalo de confiança (ms)**	**Latência média (ms)**
G.703 Codir	**A**	**10,9361 e 11,0399**	**10,9880**
	B	**10,9129 e 11,0151**	**10,9640**
	C	**8,4438 e 8,5472**	**8,4955**
	D	**8,4394 e 8,5436**	**8,4915**
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**

Os valores médios de tempo de rede para os comandos A, B, C e D foram de, respectivamente, 3,4565 ms, 3,4205 ms, 3,4235 ms e 3,4545 ms para interface G.703 Codir 64 kbps e 1,5675 ms, 1,566 ms, 1,569 ms e 1,5775 ms para a topologia com interface G.703 2 Mbps.

Para este cenário, pode-se observar que os valores médios dos comandos diretos na interface G.703 Codir 64 kbps mantiveram-se superiores aos dez ms estabelecidos pela norma IEC 60834-1 devido à latência acrescentada pela inserção do *Mux TDM* AMDII entre o equipamento de teleproteção e os roteadores. Os demais valores estão de acordo com os pré estabelecidos pelas normas.

5.2.3 Avaliação da Solução *Flex-LSP* com a Inserção de Tráfego na Rede

Após a realização dos procedimentos descritos na Subseção 4.3.2, os resultados obtidos para os comandos diretos na topologia com inserção de tráfego e interface G.703 Codir 64 kbps podem ser observados na Figura 5.31.

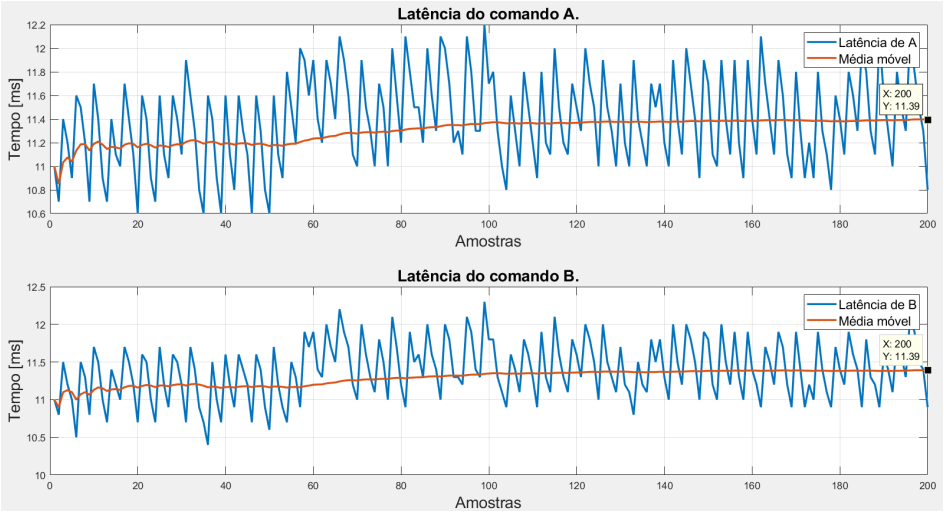


Figura 5.31: Resultados obtidos para os comandos diretos na topologia com inserção de tráfego e com interface G.703 Codir 64 kbps.

Os resultados obtidos para os comandos de bloqueio podem ser observados na Figura 5.32.

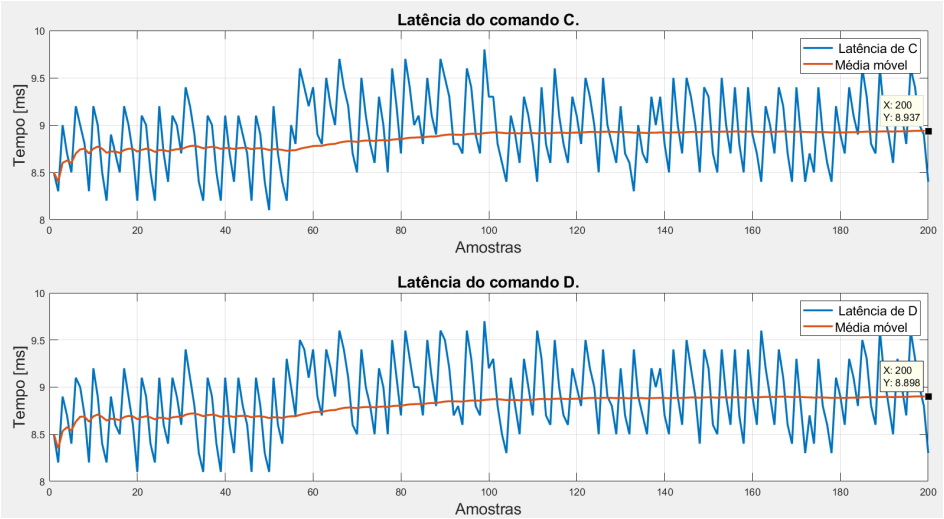


Figura 5.32: Resultados obtidos para os comandos de bloqueio na topologia com inserção de tráfego e com interface G.703 Codir 64 kbps.

Os resultados obtidos para os comandos DUTT e DCB no teste de topologia com inserção de tráfego e com interface G.703 2 Mbps podem ser observados, respectivamente, nas Figuras 5.33 e 5.34.

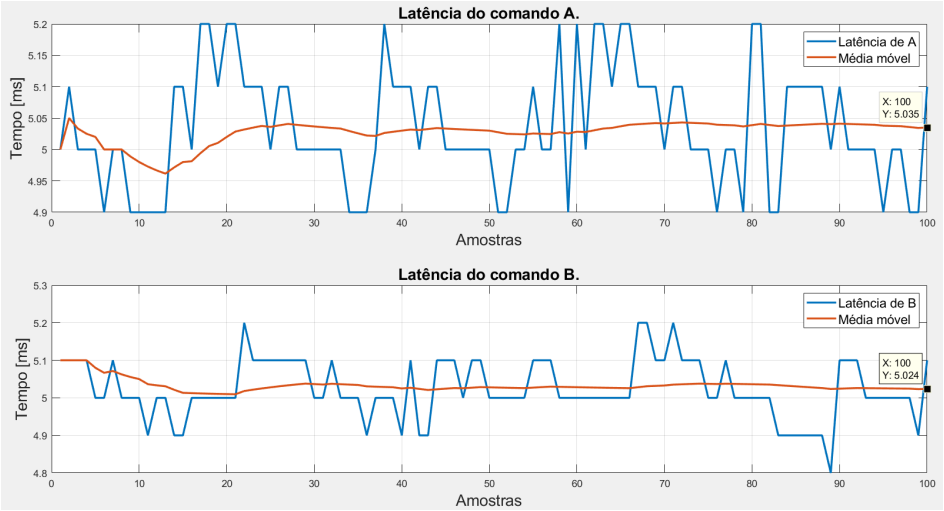


Figura 5.33: Resultados obtidos para os comandos diretos na topologia com inserção de tráfego e com interface G.703 2 Mbps.

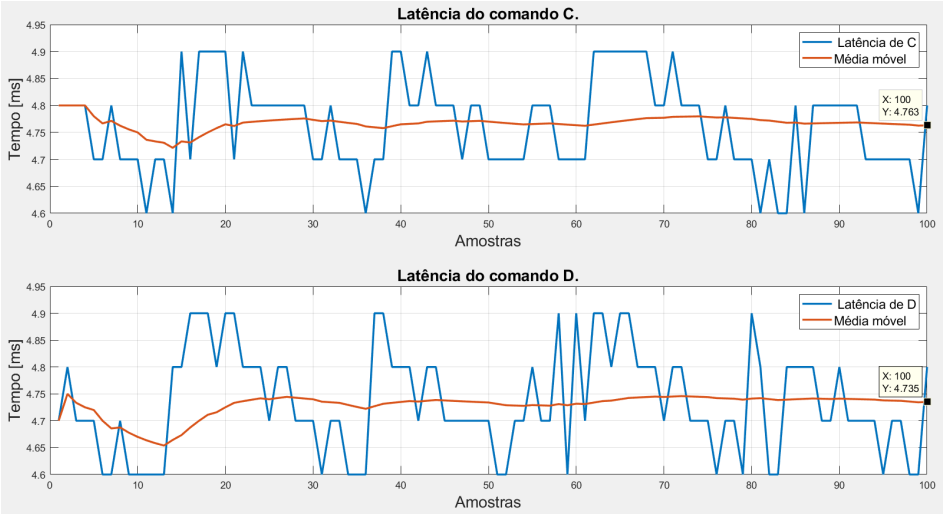


Figura 5.34: Resultados obtidos para os comandos de bloqueio na topologia com inserção de tráfego e com interface G.703 2 Mbps.

Os valores obtidos através do gerador de tráfego para o caminho principal podem ser observados na Figura 5.35.

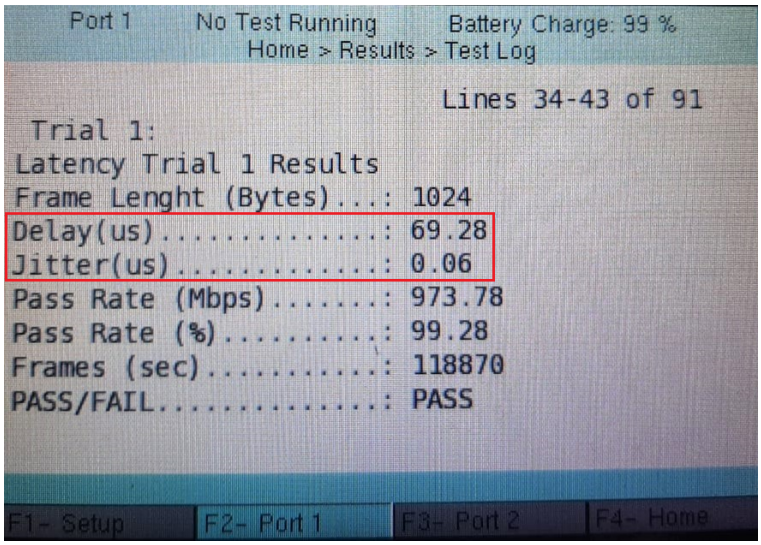


Figura 5.35: Resultados obtidos através do gerador de tráfego para o caminho principal na solução *Flex-LSP*.

Os valores dos intervalos de confiança e as latências médias dos comandos de teleproteção podem ser observados na Tabela 5.7

Tabela 5.7: Intervalos de confiança e latência média para os comandos de teleproteção na topologia com inserção de tráfego na solução *Flex-LSP*.

	Comando	**Intervalo de confiança (ms)**	**Latência média (ms)**
G.703 Codir	**A**	**11,3402 e 11,4478**	**11,3940**
	B	**11,3344 e 11,4426**	**11,3885**
	C	**8,8829 e 8,9901**	**8,9365**
	D	**8,8438 e 8,9522**	**8,8980**
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**

Os valores médios de tempo de rede para os comandos A, B, C e D foram de, respectivamente, 3,8625 ms, 3,845 ms, 3,8685 ms, 3,861 ms para interface G.703 Codir 64 kbps, e 1,9205 ms, 1,925 ms, 1,923 ms e 1,9255 ms para a topologia com interface G.703 2 Mbps.

Para os testes com inserção de tráfego na rede, pode-se observar que ocorreu uma pequena variação em relação aos testes sem inserção de tráfego, ou seja, a inserção de tráfego na rede acarretou em um aumento no tempo destinado ao envio dos comandos de teleproteção. Assim como no caso anterior, deve ser considerada a inserção do *Mux TDM* na solução com interface G.703 Codir 64 kbps.

5.2.4 Falha de Canal na Solução *Flex-LSP*

Assim como descrito na subseção 4.3.3, neste cenário serão apresentados os resultados para os comandos diretos e de bloqueio na solução *Flex-LSP* quando submetida a uma falha de canal no caminho principal. Após o envio da quinquagésima amostra, o caminho principal é desconectado, forçando os comandos a serem trafegados pelo caminho alternativo.

Os resultados obtidos para os comandos diretos e de bloqueio na topologia com interface G.703 Codir 64 kbps podem ser observados nas Figuras 5.36 e 5.37.

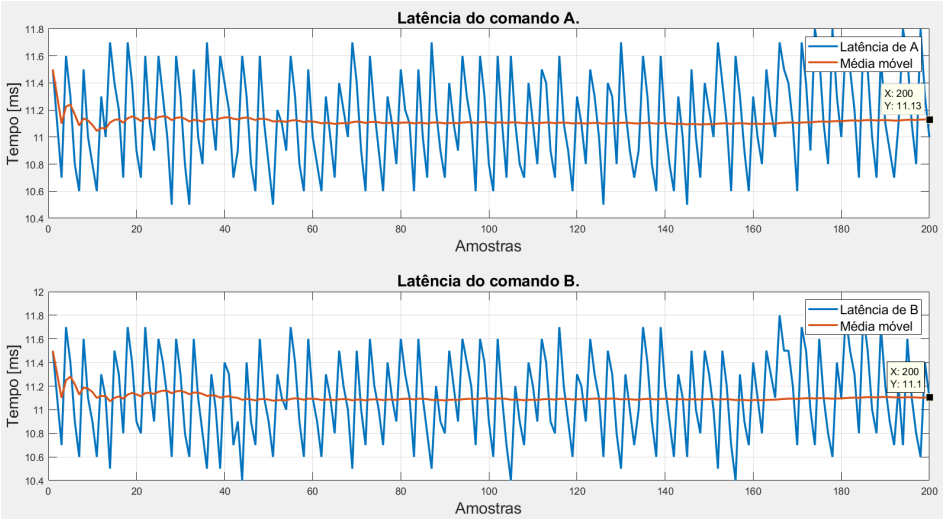


Figura 5.36: Resultados obtidos para os comandos diretos no teste de falha do canal principal com interface G.703 Codir 64 kbps.

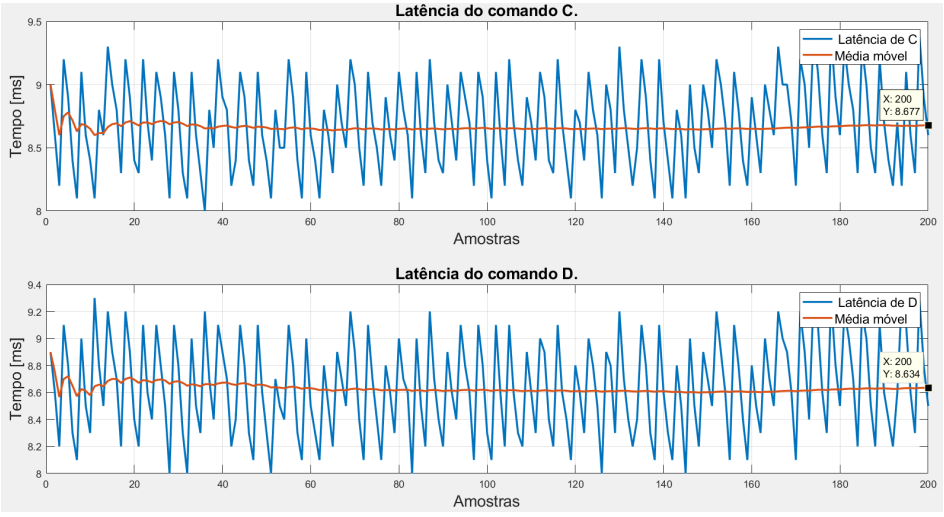


Figura 5.37: Resultados obtidos para os comandos de bloqueio no teste de falha do canal principal com interface G.703 Codir 64 kbps.

A Tabela 5.8 apresenta os valores obtidos para o cenário atual e o cenário de rede *IP* sem inserção de tráfego para a interface G.703 Codir 64 kbps.

Tabela 5.8: Comparação entre os valores obtidos no teste de falha de canal e rede *IP* sem inserção de tráfego com interface G.703 Codir 64 kbps.

Comando	**Latência para os comandos no teste de falha de canal (ms)**	**Latência para os comandos no teste de rede IP sem tráfego (ms)**
A	**11,1295**	**10,9880**
B	**11,1030**	**10,9640**
C	**8,677**	**8,4955**
D	**8,6340**	**8,4915**

Com os valores obtidos para esse teste, observa-se que houve um pequeno aumento no valor da latência média, quando comparado ao cenário sem inserção de tráfego. Porém, nota-se que apenas os valores de latência média dos comandos diretos na topologia com interface Codir 64 kbps não se adéquam aos requisitos de dez ms pré-estabelecidos.

Vale ressaltar que as distâncias entre os roteadores são muito pequenas, quando comparadas as que se encontram em campo, e, portanto, é necessária a realização de testes em um ambiente real para a obtenção de resultados mais fiéis.

5.2.5 Latência Assimétrica na Rede *IP* com a Solução *Flex-LSP*.

Assim como descrito na Subseção 4.3.4, neste experimento é realizado o envio de cem amostras do equipamento DIP 5000 A para o equipamento DIP 5000 B e, em seguida, são enviadas mais cem amostras do equipamento DIP 5000 B para o equipamento DIP 5000 A. Em ambos os cenários os comandos são enviados através do caminho principal.

Os resultados obtidos para os comandos enviados do equipamento de teleproteção DIP 5000 A para o B podem ser observados na Figura 5.38.

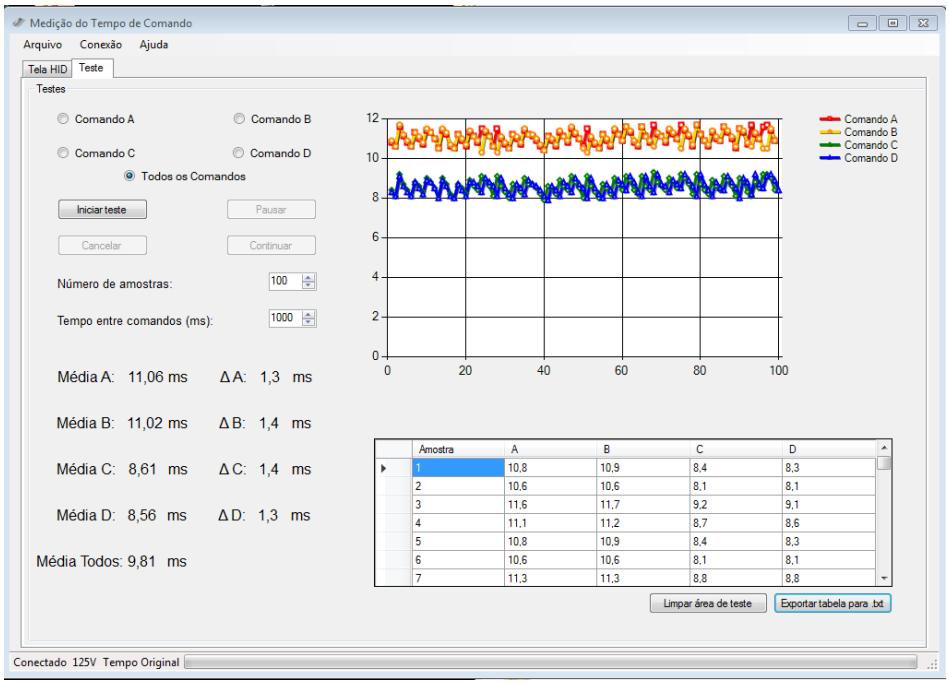


Figura 5.38: Resultados obtidos para os comandos enviados do Equipamento DIP 5000 A para o DIP 5000 B.

Os resultados obtidos para os comandos enviados do equipamento de teleproteção DIP 5000 B para o A podem ser observados na Figura 5.39.

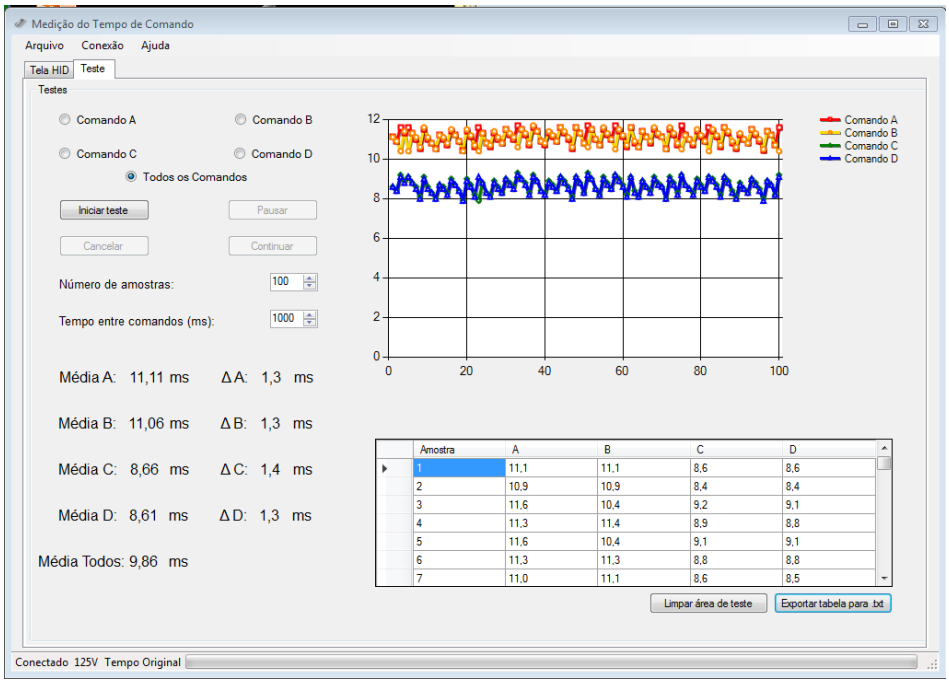


Figura 5.39: Resultados obtidos para os comandos enviados do Equipamento DIP 5000 B para o DIP 5000 A.

Através destes resultados, os valores obtidos de latência assimétrica média para os comandos A, B, C e D são de, respectivamente, 0,05 ms, 0,04 ms, 0,05 ms e 0,05 ms. Os resultados obtidos se mostraram inferiores aos quatro ms estabelecidos pela norma IEC 60834-1.

Capítulo 6

Considerações Finais e Trabalhos Futuros

Este trabalho apresentou como proposta a avaliação das tecnologias de comunicação com multiplexação estatística, redes de pacotes, voltadas aos serviços de teleproteção de linhas de transmissão de energia. Para isso, foram realizados testes em laboratório utilizando as tecnologias proprietárias *IP Hard-Pipe* e *Flex-LSP*.

No decorrer desta dissertação, observou-se que os comandos dos tipos direto e de bloqueio enviados pelo *software* da maleta de comandos de teleproteção se mantiveram, em média, abaixo dos dez ms estabelecidos pela norma IEC 60834-1. Os cenários em que aqueles ultrapassaram esses valores, decorreram da necessidade da utilização de conversores, para a adequação das interfaces de comunicação nos roteadores, o que deu origem a uma latência adicional ao sistema.

Em ambas as soluções, foi possível verificar que para os comandos DUTT e interface G.703 Codir 64 kbps, ocorreram amostras com valores superiores aos dez ms. Diante disso, foi concluído que, para a teleproteção com esquema de proteção DUTT, não é recomendado a utilização de interface G.703 Codir 64 kbps entre os equipamentos de teleproteção e roteadores.

Importante salientar que todos os equipamentos utilizados para a execução destes testes, foram cedidos pelas empresas proprietárias das soluções avaliadas. Além disso, os equipamentos disponibilizados para mercado apresentam as interfaces de comunicação e demais periféricos, de acordo com as necessidades dos clientes, mitigando o problema de latência acrescida pelos conversores.

Ademais, com a utilização das interfaces G.703 2 Mbps, para realizar a comunicação entre os equipamentos de teleproteção e os roteadores, pode-se observar uma redução considerável na latência dos comandos de teleproteção em comparação com o sistema utilizando interface G.703 Codir 64 kbps. Inclusive, em alguns testes essa redução atingiu cerca de 50 %.

A latência da rede *IP* foi de, aproximadamente, 2,517 ms quando utilizado o serviço de teleproteção com interface G.703 Codir 64 kbps na solução *IP Hard-Pipe* e de 1,57 ms para o

serviço de teleproteção com interface G.703 2 Mbps na solução *Flex-LSP*. Os resultados apresentados são referentes aos valores obtidos em ambientes sem equipamentos de teleproteção e de conversores.

Uma possível solução a ser implementada para obter melhores resultados, referentes à latência dos comandos, é a adequação dos sistemas de teleproteção para cenários que dispensam a utilização dos equipamentos de teleproteção e realizam a ligação dos relés diretamente aos roteadores. Isto pode ser comprovado pelo fato de que, como demonstrado durante os testes, a maior fonte de latência do sistema está no processamento dos equipamentos de teleproteção.

Outro ponto importante avaliado durante os experimentos, foi a inserção de tráfego na rede para a avaliação de seu desempenho. Nesse sentido, durante os testes foi realizada a inserção de um Gbps (Valor estipulado para a banda dos *links* dos roteadores), que simula a realização de outros serviços, como os executados nas redes IP corporativas. Para o *IP Hard-Pipe*, foi constatado que a inserção de tráfego na rede não afetou o desempenho da solução, logo, tornou legítima a reserva de banda configurada. Além disso, permitiu que trafegassem pelo canal apenas a diferença entre o valor injetado na rede e a banda estipulada para o túnel *Hard-Pipe*

Na solução *Flex-LSP* foi implementado o *QoS* para priorizar o tráfego de teleproteção, no qual foi possível verificar uma pequena variação entre os valores de latência obtidos para os cenários, com e sem tráfego. Diante disso, comprovou-se que, para esta solução, a inserção daquele na rede poderia causar uma pequena degradação do canal dedicado ao serviço de teleproteção. Vale ressaltar que, diferentemente da solução *IP Hard-Pipe*, na solução *Flex-LSP* os planos de controle e de dados não são separados, portanto, é justificável essa pequena influência.

Em ambas soluções, o comportamento do sistema se mostrou favorável ao ser submetido a uma falha no canal principal, já que não apresentou grandes variações entre os cenários experimentados. Porém, é necessário que o experimento seja avaliado com cautela, visto que, o laboratório disponibilizado para os testes não possuía as ferramentas necessária para representar, efetivamente, as grandes distâncias presentes entre os roteadores utilizados em campo.

Portanto, através dos resultados obtidos durante os experimentos, constata-se que as tecnologias estatísticas avaliadas se adéquam aos requisitos demandados para os cenários de teleproteção. De modo que, se apresentam como uma possível alternativa aos sistemas legados das concessionárias de energia que se baseiam em soluções de fluxo determinístico de *bits*.

6.1 Trabalhos Futuros

Deve-se salientar que todos os testes executados durante este estudo foram realizados em um ambiente de laboratório. Sendo estes, realizados para avaliar, de uma forma inicial,

a capacidade da utilização de soluções estatísticas baseadas na tecnologia *IP/MPLS* para o serviço de teleproteção de linhas de transmissão de energia. Portanto, para uma maior consolidação dos resultados, necessita-se de testes complementares em um ambiente real de produção, ou seja, em sistemas de teleproteção de linhas de transmissão de energia de alta tensão em operação.

Durante a execução dos testes, foi observado que grande parte da latência verificada nas topologias esta localizada nos equipamentos de teleproteção (aproximadamente 70%). Portanto, para um estudo futuro, uma solução que dispense a utilização de equipamentos de teleproteção, e realize diretamente a conexão dos relés aos roteadores, poderia ser elaborada para que fosse possível a obtenção de valores de latência inferiores aos obtidos durante a realização deste trabalho.

Assim como evidenciado durante a realização deste trabalho, as concessionárias de energia estão buscando novas tecnologias para a evolução do sistema legado. Pensando nisso, apresenta-se a possibilidade de avaliação das arquiteturas de internet do futuro para as aplicações de missão critica, controle da rede e *smart grids*. Projetos como Nova Genesis, XIA e RINA, podem oferecer recursos importantes para estas aplicações. Recursos como, orquestração, nomenclatura auto-verificada e expressividade podem contribuir para a obtenção de redes de computadores mais robustas e auto-organizadas no setor de energia.

Apesar do foco deste estudo se situar no âmbito da teleproteção de linhas de transmissão de energia, é possível estender a avaliação da utilização de sistemas de teleproteção com redes determinísticas para as *smart grids*, operando no domínio de distribuição de energia, aplicada principalmente as aplicações de geração de energia distribuída.

Por fim, atrelado aos comentários citados anteriormente, verifica-se a possibilidade de adaptação das topologias propostas, possibilitando a optimização dos cenários e obtenção de melhores resultados. Além da avaliação de novas soluções para os serviços prestados pelas concessionárias de energia.

Referências Bibliográficas

[1] S. Nagaraju, L. J. Gudino, N. Tripathi, S. V., and R. C.K., "Mobility assisted localization for mission critical wireless sensor network applications using hybrid area exploration approach," *Journal of King Saud University - Computer and Information Sciences*, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1319157818300740

[2] "Transformation of mission-critical communications networks," NOKIA, Espoo, Tech. Rep., 2018.

[3] M. A. Nunez, J. Denman, G. T. Corpuz, J. B. M. Jr, H. Chan, and I. Schonwald, "Case study protective relaying over ip/mpls: Myth to facts," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, April 2017, pp. 1–12.

[4] G. Dileep, "A survey on smart grid technologies and applications," *Renewable Energy*, vol. 146, pp. 2589 – 2625, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0960148119312790

[5] Alcatel, "Reliable ip communication for smart grids: Network transformation to ip/mpls infrastructures." Alcatel.Lucent, Tech. Rep., May 2014.

[6] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," IETF - Internet Engineering Task Force, RFC 3031, January 2001. [Online]. Available: https://tools.ietf.org/html/rfc3031

[7] S. M. Blair and C. Booth, "Real-time teleprotection testing using ip/mpls over xdsl," Glasgow, 2013. [Online]. Available: https://strathprints.strath.ac.uk/44247/

[8] S. Bryant and P. Pate, "Pseudo wire emulation edge-to-edge (pwe3) architecture," Internet Requests for Comments, RFC Editor, RFC 3985, March 2005.

[9] T. Rahman, J. Moralez, S. Ward, E. A. Udren, M. Bryson, and K. Garg, "Teleprotection with mpls ethernet communications—development and testing of practical installations," in *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*. IEEE, 2018, pp. 1–18.

[10] D. Medhi and K. Ramasamy, "Chapter 19 - circuit-switching: Hierarchical and dynamic call routing," in *Network Routing (Second Edition)*, second edition ed., ser. The Morgan Kaufmann Series in Networking, D. Medhi and K. Ramasamy, Eds. Boston: Morgan Kaufmann, 2018, pp. 646 – 672. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128007372000235

[11] A. Farrel and I. Bryskin, "Chapter 2 - an overview of transport networks," in *GMPLS*, ser. The Morgan Kaufmann Series in Networking, A. Farrel and I. Bryskin, Eds. San Francisco: Morgan Kaufmann, 2006, pp. 9 – 23. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780120884223500046

[12] S.Haykin and M. Moher, *Sistemas de Comunicação*, 5th ed. Porto Alagre: Bookman, Janeiro 2011.

[13] J. F. Ransome and J. W. Rittinghouse, "4 - packet technologies," in *Voice over Internet Protocol (VoIP) Security*, J. F. Ransome and J. W. Rittinghouse, Eds. Burlington: Digital Press, 2005, pp. 75 – 131. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9781555583323500078

[14] G. S. Ribeiro. (2019) Voz sobre ip i: A convergência de dados e voz. https://www.teleco.com.br/tutoriais/tutorialvoipconv/pagina_3.asp.

[15] R. S. Wanderson, "Experiência em implementação / manutenção de equipamentos de teleproteção digital e analógica abordando o novo cenário proposto aos equipamentos de teleproteção a partir das novas resoluções do ons descritas no procedimento de rede." in *XX SNPTEE Seminário Nacional de Produção E Transmissão de Energia Elétrica*, Novembro 2009, pp. 1–8.

[16] "The authoritative dictionary of ieee standards terms, seventh edition," *IEEE Std 100-2000*, pp. 1–1362, Dec 2000.

[17] V. H. Vaghef, M. Shabro, and B. G. Family, "Design and implementation of a teleprotection system with digital and analog interfaces," *Journal of Electrical and Electronic Engineering*, vol. 3, pp. 88–91, 2015.

[18] P. Rush, *Proteção e Automação de Redes: Conceito e Aplicação*, 1st ed. São Paulo: Edgard Blücher Ltda., 2011.

[19] V. A. dos Santos, "Proteção de distância aplicada a linhas de transmissão em circuito duplo," Master's thesis, Universidade Federal do Rio de Janeiro, Rio de Janeiro, Setembro 2007.

[20] O. S. E. Atwa, "Chapter 20 - protective relays testing and commissioning," in *Practical Power System and Protective Relays Commissioning*, O. S. E. Atwa, Ed. Academic Press, 2019, pp. 325 – 360. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128168585000204

[21] G. Kindermann, *Proteção de Sistemas Elétricos de Potência*, 2nd ed. Florianópolis: UFSC, 2014, vol. 2.

[22] "Ieee standard electrical power system device function numbers," *IEEE Std C37.2-1991*, pp. 1–24, 1991.

[23] A. E. C. Momesso, "Proteção adaptativa de relés de sobrecorrente com lógica fuzzy," Master's thesis, Universidade de São Paulo, São Carlos, 2017.

[24] G. S. Rolim, "Análise da utilização de relé direcional em sistemas elétricos com geração distribuída," monography, Universidade Federal da Paraíba, João Pessoa, Junho 2018.

[25] M. C. Siqueira, "Desempenho da proteção de distância sob diferentes formas de polarização," Master's thesis, Universidade Federal do Rio de Janeiro, Rio de Janeiro, Setembro 2007.

[26] G. Kindermann, *Proteção de Sistemas Elétricos de Potência*, 2nd ed. Florianópolis: UFSC, 2005, vol. 1.

[27] S. Brian, "Transmission protection overview," Hands-On Relay School, 2012, https://conferences.wsu.edu/forms/hrs/HRS15/Lectures/Overview/TransmissionOverview.pdf.

[28] A. M. Sleva, *Protective Relay Principles*, 1st ed. Florida, Boca Raton: CRC Press, Feb. 2009, vol. 1.

[29] E. O. Schweitzer III and J. J. Kumm, "Statistical comparison and evaluation of pilot protection schemes," in *Proc. of the 23rd Western Protective Relay Conference*, 1996, pp. 15–17.

[30] R. G. Sampaio, "Análise de características de operação quadrilateral para proteção de distância de linhas de transmissão," Ph.D. dissertation, Universidade de Brasília, Brasília, Dezembro 2014.

[31] E. M. Gonçalves, "Metodologias para validação de proteções de linhas de transmissão," Master's thesis, Universidade Federal de Minas Gerais, Belo Horizonte, Setembro 2012.

[32] S. V. Achanta, R. Bradetich, and K. Fodero, "Speed and security considerations for protection channels," in *2016 69th Annual Conference for Protective Relay Engineers (CPRE)*, April 2016, pp. 1–9.

[33] N. Andreadou, M. O. Guardiola, and G. Fulli, "Telecommunication technologies for smart grid projects with focus on smart metering applications," *Energies*, vol. 9, no. 5, p. 375, 2016.

[34] S. Mahmod, N. F. Mailah, and M. Radzi, "Effects of high power converter on power line carrier signal," in *4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings.*, Jan 2003, pp. 163–167.

[35] H. C. Ferreira, L. Lampe, J. Newbury, and T. G. Swart, *Powe Line Communication: Theory and Applications for Narrowband and Broadband Communications over Power Lines*, 1st ed. New York: Wiley, July 2011, vol. 1.

[36] Y. G. Santos, "Telecomunicação para o setor elétrico: Power line carrier," Master's thesis, Universidade Federal de Uberlândia - Compus de Patos de Minas, Patos de Minas, 2016.

[37] J. F. Adami, G. C. Fonseca, C. M. Haber, and A. C. Dallbello, "Modelagem de uma linha de transmissão com um sistema de ondas portadoras simulando disturbios de alta frequência através do matlab/simulink," in *SNTPEE-Seminário Nacional de Produção e Transmissão de Energia Elétrica*, oct 2007.

[38] J. Liu, H. Guo, and L. Zhao, "Resilient and low-latency information acquisition for fiwi enhanced smart grid," *IEEE Network*, vol. 31, no. 5, pp. 80–86, 2017.

[39] K. C. Behrendt, "Relay-to-relay digital logic communication for line protection, monitoring, and control," in *Proceedings of the 23rd Annual Western Protective Relay Conference*, 1996.

[40] "G.694.1 - spectral grids for wdm applications: Dwdm frequency grid," Intl. telecommunication union, Standard, October 2020.

[41] C. J. W. Group 35/35.11, "Protection using telecommunications," Cigré, Paris, Tech. Rep. 1, August 2001.

[42] "T1.105 - sonet — basic description including multiplex structure, rates, and formats," Standard, February 2001.

[43] "G.783 - characteristics of synchronous digital hierarchy (sdh) equipment functional blocks," Standard, March 2006.

[44] "G.784 - management aspects of synchronous digital hierarchy (sdh) transport network elements," Standard, March 2008.

[45] "G.707/y.1322 - network node interface for the synchronous digital hierarchy (sdh)," Standard, January 2007.

[46] J.-P. Vasseur, M. Pickavet, and P. Demeester, "Chapter 2 - sonet/sdh networks," in *Network Recovery*, ser. The Morgan Kaufmann Series in Networking, J.-P. Vasseur, M. Pickavet, and P. Demeester, Eds. Burlington: Morgan Kaufmann, 2004, pp. 39 – 130. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780127150512500168

[47] Siemens, "Fiber-optic communications on the way to carrier and utility grade packet transport networks," 2018, https://w3.siemens.com/smartgrid/global/en/products-systems-solutions/smart-communication/transmission/Pages/ip-ethernet-sdh-solutions.aspx.

[48] M. Chang and B. Liao, "Improving bandwidth utilization of ng-sdh by dynamic bandwidth management," in *2011 13th Asia-Pacific Network Operations and Management Symposium*, 2011, pp. 1–4.

[49] "G.7041/y.1303 - generic framing procedure," Standard, August 2016.

[50] Peng Wang, Biao Wang, Depeng Jin, and Lieguang Zeng, "Revising link capacity adjustment scheme for asic applications," in *2007 7th International Conference on ASIC*, Oct 2007, pp. 1309–1312.

[51] A. M. Alberti and R. Fernandes, "Ethernet-over-sdh: Technologies review and performance evaluation," *Revista Telecomunicações*, vol. 13, no. 1, Maio 2011.

[52] B. S. Davie and A. Farrel, "Chapter 3 - overview of mpls protocols," in *MPLS: Next Steps*, ser. The Morgan Kaufmann Series in Networking, B. S. Davie and A. Farrel, Eds. Burlington: Morgan Kaufmann, 2008, vol. 1, pp. 31 – 54. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780123744005000035

[53] D. Medhi and K. Ramasamy, "Chapter 22 - multiprotocol label switching (mpls)," in *Network Routing (Second Edition)*, second edition ed., ser. The Morgan Kaufmann Series in Networking, D. Medhi and K. Ramasamy, Eds. Boston: Morgan Kaufmann, 2018, pp. 734 – 764. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128007372000260

[54] I. Minei and J. Lucek, *MPLS-Enabled Applications: Emerging Developments and New Technologies*, 3rd ed. New York: Wiley, January 2011, vol. 1.

[55] L. M. Surhone, M. T. Tennoe, and S. F. Henssonow, *MPLS-TP*, 1st ed. Beau Bassin-Rose Hill: Betascript Publishing, September 2010, vol. 1.

[56] V. Joseph and S. Mulugu, "7 - mpls transport profile," in *Network Convergence*, V. Joseph and S. Mulugu, Eds. Boston: Morgan Kaufmann, 2014, pp. 553 – 575. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780123978776000072

[57] C. R. F. Costa, "Mecanismos para determinação de rotas de proteção em redes mpls-tp com topologia em malha," Ph.D. dissertation, Universidade de São Paulo, São Paulo, 2016.

[58] D. Sul, S. Kim, and J. Lee, "Lsp merge in point to multipoint in-band oam," in *2014 12th International Conference on Optical Internet 2014 (COIN)*, 2014, pp. 1–2.

[59] J. Hao, P. Maheshwari, P. Maheshwari, L. Andersson, and M. Chen, "Architecture of an ip/mpls network with hardened pipes," Internet Requests for Comments, RFC Editor, RFC 1654, August 2015.

[60] Huawei. (2019) Ip hard pipe solution. https://e.huawei.com/en/tech-topic/jp/ip-hard-pipe.

[61] Cisco. (2019) Flex lsp overview. https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/routers/ncs4200/configuration/guide/mpls/mp-basic-ncs4200-book/mp-basic-ncs4200-book_chapter_010.html.xml.

[62] M. T. Tolmasquim, *Novo modelo do setor elétrico brasileiro*, 2nd ed. Rio de Janeiro: Synergia Editora, Janeiro 2015.

[63] "Submódulo 2.6 - requisitos mínimos para os sistemas de proteção e de telecomunicações," Operador Nacional do Sistema Elétrico, Standard, Novembro 2011.

[64] "Iec 60834-1: Teleprotection equipment of power systems - performance and testing - part 1: Command systems," International Electrotechnical Commission, Standard, Nov. 1999.

[65] "Iec 60834-2: Performance and testing of teleprotection equipment of power systems - part 2: Analogue comparison systems," International Electrotechnical Commission, Standard, Jun. 1993.

[66] T. Rahman, J. Moralez, S. Ward, E. A. Udren, M. Bryson, and K. Garg, "Teleprotection with mpls ethernet communications — development and testing of practical installations," in *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*, March 2018, pp. 1–18.

[67] V. Tan and J. Cole, "Teleprotection over multiprotocol label switching (mpls): Experiences from an australian electric power utility," in *Session Papers and Proceedings Cigre*, 2018.

[68] R. Bachli, M. Hausler, and M. Kranich, "Teleprotection solutions with guaranteed performance using packet switched wide area communication networks," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, April 2017, pp. 1–6.

[69] P. Robertson, K. Fodero, and C. Gray, "Solving the inherent problem of transporting serial teleprotection circuits over mpls," in *Session Papers and Proceedings Cigre*, 2019.

[70] "Ieee standard for n times 64 kbps optical fiber interfaces between teleprotection and multiplexer equipment," *IEEE Std C37.94-2017 (Revision of IEEE Std C37.94-2002)*, pp. 1–23, July 2017.

[71] S. M. Blair, C. D. Booth, B. De Valck, D. Verhulst, C. Kirasack, K. Y. Wong, and S. Lakshminarayanan, "Validating secure and reliable ip/mpls communications for current differential protection," in *13th International Conference on Development in Power System Protection 2016 (DPSP)*, March 2016.

[72] M. R, "Teleproteção sobre mpls-tp características, demandas, testes e considerações," in *XXV SNPTEE - Seminário Nacional de Produção e Transmissão de Energia Elétrica.*, November 2019.

[73] C. M. Adrah, A. K. Kamath, S. Bjørnstad, and M. P. Tahiliani, "Achieving guaranteed performance for protection traffic in smart grid wide-area networks," in *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, Aug 2019, pp. 42–47.

[74] L. Wei, Y. Qi, and H. Qi, "Research on design and implementation of relay protection in smart grid," in *2018 Chinese Control And Decision Conference (CCDC)*, 2018, pp. 1439–1443.

[75] M. Mehmed-Hamza and P. Stanchev, "Overcurrent protection against faults in smart grids," in *2019 11th Electrical Engineering Faculty Conference (BulEF)*, 2019, pp. 1–4.

[76] K. Fodero, C. Huntley, and P. Robertson, "Deterministic communications for protection applications over packet-based wide-area networks," in *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*, March 2018, pp. 1–6.

[77] S. M. Blair, C. D. Booth, B. De Valck, D. Verhulst, and K. Wong, "Modeling and analysis of asymmetrical latency in packet-based networks for current differential protection application," *IEEE Transactions on Power Delivery*, vol. 33, no. 3, pp. 1185–1193, June 2018.

[78] R. G. Sierra, C. M. Etayo, and N. M. Mejia, "A tele-protection implementation experience at power substations using metro ethernet networks," in *22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013)*, June 2013, pp. 1–4.

[79] J. Ramirez, H. Cabrera, O. Bautista, and G. C. PLC, "Mpls-tp as packet platform for critical services in power transmission," in *CIGRE Int. Conf. and 21st Exhibition for Electrical Equipment, Paris, France*, vol. 6, 2016, pp. 1–14.