PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

PAULO HENRIQUE MENONI

UM DISPOSITIVO *WHITE-LABEL* COM TECNOLOGIA SD-WAN PARA CIDADES INTELIGENTES

CAMPINAS

2022

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS
PROGRAMA DE PÓS-GRADUAÇÃO EM GESTÃO DE REDES DE TELECOMUNICAÇÕES

PAULO HENRIQUE MENONI

UM DISPOSITIVO *WHITE-LABEL* COM TECNOLOGIA SD-WAN PARA CIDADES INTELIGENTES

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Gestão de Redes de Telecomunicações do Centro de Ciências Exatas, Ambientais e de Tecnologias, da Pontifícia Universidade Católica de Campinas, como exigência para obtenção do título de Mestre em Gestão de Redes de Telecomunicações.

Orientadora: Prof(a). Dr(a). Cecília de Freitas Morais

CAMPINAS
2022

Ficha catalográfica elaborada por Fabiana Rizziolli Pires CRB 8/6920
Sistema de Bibliotecas e Informação - SBI - PUC-Campinas

006.22
M827d

Menoni, Paulo Henrique

Um dispositivo white-label com tecnologia SD-WAN para cidades inteligentes / Paulo Henrique Menoni. - Campinas: PUC-Campinas, 2022.

99 f.: il.

Orientador: Cecília de Freitas Morais.

Dissertação (Mestrado em Gestão de Redes de Telecomunicações) - Programa de Pós-Graduação em Gestão de Redes de Telecomunicações, Centro de Ciências Exatas, Ambientais e de Tecnologia, Pontifícia Universidade Católica de Campinas, Campinas, 2022.
Inclui bibliografia.

1. Internet das coisas. 2. Cidades inteligentes. 3. Interconexão em rede (Telecomunicações). I. Morais, Cecília de Freitas. II. Pontifícia Universidade Católica de Campinas. Centro de Ciências Exatas, Ambientais e de Tecnologia. Programa de Pós-Graduação em Gestão de Redes de Telecomunicações. III. Título.

CDD - 22. ed. 006.22

PAULO HENRIQUE MENONI

UM DISPOSITIVO WHITE-LABEL COM TECNOLOGIA SD-WAN PARA CIDADES INTELIGENTES

Dissertação apresentada como exigência para obtenção do título de Mestre em Gestão de Redes de Telecomunicações ao Programa de Pós-Graduação em Gestão de Redes de Telecomunicações do Centro de Ciências Exatas, Ambientais e de Tecnologias.
Área de Concentração: Gestão de Redes e Serviços.
Orientador (a): Profa. Dra. Cecília de Freitas Morais.

Dissertação defendida e aprovada em 11 de março de 2022 pela Comissão Examinadora constituída dos seguintes professores:

Cecília de Freitas Morais

Profa. Dra. Cecília de Freitas Morais
Orientadora da Dissertação e Presidente da Comissão Examinadora
Pontifícia Universidade Católica de Campinas

Profa. Dra. Lia Toledo Moreira Mota
Pontifícia Universidade Católica de Campinas

Profa. Dra. Maria Cristina Aranda
Faculdade de Tecnologia de Americana - FATEC Americana

Dedico a minha esposa Vanessa e minha filha Julia, que são a razão de todo meu esforço e dedicação. Só se educa pelo exemplo.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus por permitir que eu chegasse até aqui com determinação e perseverança, à minha orientadora Professora Dr(a). Cecília de Freitas Morais pelo apoio prestado durante a construção deste trabalho, à PUC Campinas e aos docentes pela dedicação dispensada e aos meus amigos que me ajudaram e apoiaram durante todo o curso.

RESUMO

Recentemente, o conceito de cidades inteligentes tem recebido uma grande atenção de pesquisadores, empresas e autoridades. Nesse contexto, surge a dúvida: como conectar a grande diversidade de sensores e agregar os dados de serviços coletados por diferentes tecnologias associadas à Internet das coisas (do inglês *Internet of Things* - IoT)? Sabe-se que a arquitetura para redes IoT é composta por quatro camadas: percepção, rede, suporte e aplicação, sendo que na camada de rede é onde os dados são agregados e transmitidos, usualmente, através de conexões WAN (*Wide Area Network*) de Internet ou privadas MPLS (*Multi-Protocol Label Switching*). No entanto, por apresentarem recursos distintos em termos de dados, tamanho, área de cobertura, requisitos de latência e capacidade, as soluções baseadas em redes WAN mostraram-se ineficientes e até proibitivas no que diz respeito a custos e operacionalização para aplicações em cidades inteligentes. Uma alternativa é o emprego da SD-WAN (*Software-Defined Wide Area Network*) que, por meio de uma arquitetura estruturada por *hardware* e *software*, consegue virtualizar as conexões WAN. As principais características da SD-WAN são: a capacidade de seleção dinâmica dos caminhos facilitando o fluxo de dados e aumentando a resiliência do sistema; o suporte a múltiplos tipos de conexão (*links* ADSL, VDSL, FTTH ou 3G/4G) aumentando a área de cobertura em comparação à WAN; o emprego de uma interface mais fácil de configurar e gerenciar; a redução de despesas de capital e operação; o aumento da agilidade e flexibilidade de serviço; a implementação de uma plataforma de controle e monitoramento centralizado com custos reduzidos. Nesse sentido, foi desenvolvida uma solução SD-WAN embarcada *white-label*, de baixo custo e de baixo consumo de energia para uso comercial e acadêmico buscando atender às seguintes demandas: redução de custos frente aos *links* MPLS, usando como base os *softwares* Linux Ubuntu, Floodligth SDN Controller, OpenvSwitch e o *hardware* Raspberry Pi3. O protótipo foi validado usando técnicas de emulação de redes.

Palavras-chave: SD-WAN. Cidades Inteligentes. Internet das Coisas. Gestão de Redes de Comunicação.

ABSTRACT

Recently, the concept of smart cities has received a lot of attention from researchers, companies and authorities. In this context, a question arises: how to connect a wide variety of sensors and aggregate the service data collected by different technologies related to the Internet of Things (IoT)? It is known that the IoT architecture consists of four layers, namely perception, network, support and application, in such a way that the network layer is where the data is gathered and transmitted, usually, through WAN (Wide Area Network) or private MPLS (Multi-Protocol Label Switching) connections. However, since WAN based solutions present different resources in terms of data, size, coverage area, latency and capacity requirements, they become inefficient or even prohibitive regarding operating costs on smart city applications. An alternative is the use of SD-WAN (*Software*-Defined Wide Area Network), which combines hardware and *software* appliances or is *software* based only, consisting on the virtualization of WAN connections. The main characteristics of SD-WAN are: the ability to do dynamic path selection, facilitating data flow and increasing system resilience; the support to multiple connection types (ADSL, VDSL, FTTH or 3G/4G), enlarging the coverage area when compared with traditional WAN; the employment of a simple interface (easy to configure and manage); the capital and operation expenditure reduction; the increase of service agility and flexibility; the implementation of a centralized control and monitoring with lower costs. In this sense, it was developed an SD-WAN embedded white-label solution, of low cost and low energy consumption for commercial and academic use employing *software*s Ubuntu Linux, Floodligth SDN Controller, OpenvSwitch and the Raspberry Pi3 hardware. The validation of the prototype was performed by network emulation.

Keywords: SD-WAN, Smart Cities, Internet of Things, Communication Network Management

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

LISTA DE ABREVIAÇÕES E SIGLAS

ADSL	*Assymetrical Digital Subscriber Line*
AI	*Artificial Intelligence*
API	*Application Programming Interface*
ARPANET	*Advanced Research Projects Agency Network*
ASIC	*Application Specific Integrated Circuits*
ATM	*Asynchronous Transfer Mode*
AWS	*Amazon Web Services*
CoS	*Class of Service*
D-ITG	*Distributed Internet Traffic Generator*
FD	*Forwarding Devices*
FFTH	*Fiber to the Home*
GEE	Gases do Efeito Estufa
GRE	*Generic Routing Encapsulation*
GUI	*Graphical User Interface*
IaaS	*Infrastructure as a Service*
iBGP	*interior Border Gateway Protocol*
IoT	*Internet of Things*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
LACP	*Link Aggregation Control Protocol*
LSP	*Label Switching Paths*
LTE	*Long Term Evolution*
ML	*Machine Learning*
MPLS	*Multi-Protocol Label Switching*
NETCONF	*Network Configuration Protocol*
NFV	*Network Functions Virtualization*
NHRP	*Next Hop Resolution Protocol*
NI	*Northbound Interface*
NIC	*Network Interface Card*
NOS	*Network Operating System*
ONAP	*Open Network Automation Platform*
OSPF	*Open Shortest Path First*
OVS	*Open vSwitch*
OVSDB	*Open vSwitch Database Management Protocol*
POP	*Point of Presence*
QoE	*Quality of Experience*
QoS	*Quality of Service*
REST	*Representational State Transfer*
RTP	*Real-Time Transport Protocol*
SaaS	*Software as a Service*
SASE	*Secure Access Service Edge*
SDN	*Software Defined Network*

SD-WAN	*Software-Defined Wide Area Network*
SI	*Southbound Interface*
SIP	*Session Initiation Protocol*
SLA	*Service Level Agreement*
TCP	*Transmission Control Protocol*
TDM	*Time-division Multiplexing*
TI	Tecnologia de Informação
TICs	Tecnologias de Informação e Comunicação
UDP	*User Datagram Protocol*
VCO	*VeloCloud Orchestrator*
VDSL	*Very-high-bit-rate Digital Subscriber Line*
VLAN	*Virtual Local Area Network*
VoIP	*Voice of IP*
VPN	*Virtual Private Network*
vRNI	*vRealize Network Insight*
VTN	*Virtual Tenants Network*
WAN	*Wide Area Network*

1 INTRODUÇÃO

Na última década, vários estudos foram realizados dedicados a entender qual é a melhor forma de implementar na prática o abrangente conceito de “cidades inteligentes”. Em vários cenários, a pergunta que permeou as discussões foi: qual é a melhor forma de interligar essa rede de aplicações que vão desde iluminação pública, estacionamentos, até atendimento em postos de saúde (CHAN, 2019).

O paradigma da cidade inteligente está recebendo atenção significativa de pesquisadores, empresas e autoridades em todo o mundo. Uma cidade inteligente permite uma gama de serviços, desde monitoramento ambiental até controle de tráfego e estacionamento inteligente. Estes serviços são baseados em dados gerados por uma diversidade de sensores e coletados por meio de várias tecnologias diferentes que, juntas, coincidem com a criação da chamada Internet das coisas (do inglês *Internet of Things* – IoT). Os dados requeridos por esses serviços são agregados por meio de uma arquitetura modular orientada a eventos (DALLA CIA et al., 2018).

Cidade inteligente é um modelo conceitual de desenvolvimento urbano baseado no uso de recursos humanos associado ao emprego de tecnologia para proporcionar uma melhoria na qualidade de vida e prestação de serviços nas grandes áreas urbanas. Porém, o planejamento estratégico para cidades inteligentes ainda possui uma ideia bastante abstrata por vários motivos, dentre eles pode-se citar a interdependência de várias áreas de pesquisa e disciplinas que ainda não estão bem estabelecidas. Partes interessadas no desenvolvimento desse conceito, tais como governos locais, instituições de pesquisa, fornecedores de tecnologia e indústrias, geralmente são motivados por interesses conflitantes. A tendência em acreditar que o simples fato de se implantar uma tecnologia inovadora transforma automaticamente uma cidade em uma cidade inteligente pressupõe o uso tendencioso da palavra da moda “inteligente” em ambientes fragmentados ou superficiais, o que na verdade dificulta ainda mais o esclarecimento do assunto (ANGELIDOU, 2014).

A percepção de que existe uma necessidade de uma solução integradora e abrangente é evidente, pois há a necessidade de integrar os dados entre aplicativos e dispositivos com segurança. Isso é especialmente verdade quando as cidades inteligentes implantam sensores de IoT em vários lugares e esses dispositivos produzem dados que são compartilhados entre muitas entidades diferentes para satisfazer vários casos de uso. Grande parte dos aplicativos desenvolvidos para cidades inteligentes baseados em dispositivos IoT permitem a conexão com os diversos tipos de redes, como redes sem fio, redes móveis (*Long Term Evolution* –

LTE, 4G), redes de Internet banda larga e redes privativas, também conhecidas como WAN (Rede de longa distância ou Rede de Área Ampla, do inglês *Wide Área Network*) (MEHMOOD et al., 2017).

As soluções baseadas em redes WAN tradicionais existentes no mercado atualmente mostraram-se ineficientes para a aplicação em cidades inteligentes e muitas vezes tornam-se proibitivas no que diz respeito aos custos e operacionalização da estrutura de rede (MICROCITY, 2017). Em muitos casos, apresentam recursos distintos em termos de dados, tamanho, área de cobertura, requisitos de latência e capacidade. Uma alternativa inovadora para a questão da conectividade e gerenciamento de redes é a SD-WAN (abordagem definida por *software* para gerenciar a rede de longa distância, do inglês *Software-Defined Wide Area Network*). Através de uma arquitetura estruturada por *hardware* e *software*, a SD-WAN consegue virtualizar todas as conexões WAN e oferecer diferentes serviços, de acordo com as necessidades da empresa ou organização. A SD-WAN ainda permite uma área de abrangência maior em comparação à WAN, se porventura um *link* dedicado ou MPLS (Comutação de Rótulos Multi-protocolos, do inglês *Multi-Protocol Label Switching*) não estiver disponível onde está localizada a cidade inteligente, mas, em contrapartida, os *links* ADSL (ou Linha Digital Assimétrica para Assinante, do inglês *Assymetrical Digital Subscriber Line*), VDSL (ou Linha Telefônica Digital com Taxa de Bit Muito Alta, do inglês *Very-high-bit-rate Digital Subscriber Line*), FTTH (ou Fibra para o lar, do inglês *Fiber-to-the-Home*) e 3G/4G estão acessíveis, além de serem mais baratos (MICROCITY, 2017).

A SD-WAN fornece um painel de controle único que oferece visibilidade em tempo real do desempenho da rede e elimina a necessidade do uso de várias interfaces e suposições da resolução de problemas para otimizar o gerenciamento contínuo da rede (CABRA, 2019).

1.1 MOTIVAÇÃO: APLICAÇÃO EM CIDADES INTELIGENTES

De acordo com a Organização das Nações Unidas (ONU), em 2050, 66% da população mundial viverá em cidades, o que implica em desafios significativos relativos à sustentabilidade ambiental e social (mudança climática, consumo de energia, economia, mercados, poluição e saúde). As cidades consomem cerca de 70% dos recursos mundiais e, portanto, são grandes consumidoras de recursos energéticos e contribuintes significativos para as emissões de gases de efeito estufa (GEE) devido à densidade da população urbana e à intensidade das atividades econômicas e sociais relacionadas, além da ineficiência do ambiente construído (BIBRI; KROGSTIE, 2017).

Para minimizar os efeitos negativos da super população nas cidades, surgiu pela primeira vez em 1992 o conceito de cidades inteligentes (KOZMETSKY; SMILOR; GIBSON, 1992), o qual parte da premissa de empregar funcionalidades modernas (por exemplo, sistemas de energia sustentáveis, redes de energia inteligentes e redes de transporte inteligentes, etc.) utilizando-se as tecnologias de informação e comunicação (TICs), a fim de provocar uma melhoria na eficiência das mesmas. O funcionamento correto das cidades inteligentes necessita de uma variedade de infraestruturas interdependentes e de alta complexidade. Essas infraestruturas, por sua vez são críticas e operam de forma interdependente para melhorar o desempenho dessa rede interconectada, o que acaba por se traduzir na melhoria da qualidade de vida dos cidadãos (AMINI et al., 2018). Nesse contexto, a Internet das Coisas (IoT) é um dos principais atores na atualização das áreas urbanas atuais para cidades inteligentes.

Uma das formas de tornar o conceito de cidades inteligentes menos abstrato é por meio do desenvolvimento de modelos ou *frameworks* que descrevam as principais características dessas cidades como o apresentado em (GIFFINGER et al., 2007), no qual são listadas seis características que devem ser atendidas para que a cidade seja considerada inteligente:

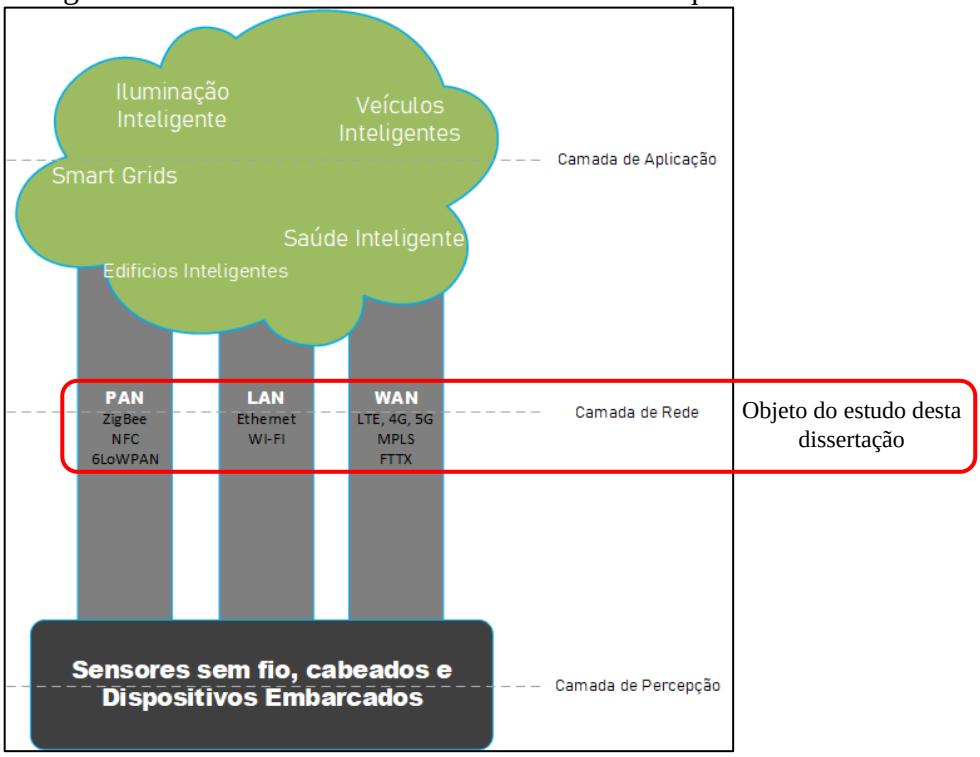
- **Economia Inteligente** – Reúne inovação e produtividade para adaptar mercado e trabalhadores e desenvolver novos modelos de negócios resilientes capazes de competir local e globalmente;
- **Governança Inteligente** – Compreende a utilização de tecnologia para potencializar a participação política, serviços aos cidadãos e o funcionamento da administração;
- **Cidadão Inteligente** – Uma cidade inteligente precisa que o cidadão participe para que as iniciativas tenham sucesso. Investimento em educação é um dispositivo importante para melhorar essa dimensão, bem como promover iniciativas para incentivar perfis criativos;
- **Mobilidade Inteligente** – Aproveita os recursos tecnológicos disponíveis para fornecer informações aos usuários e planejadores, permitindo a reformulação dos padrões de mobilidade urbana, aprimorando multimodalidade através da integração de diferentes meios de transporte;
- **Ambiente Inteligente** – Utiliza a coleta de dados de diversos serviços oferecidos na cidade, a fim de estabelecer as principais áreas de ação em planejamento urbano e planejamento de infraestrutura urbana;

- **Qualidade de vida Inteligente** – Compreende vários aspectos da qualidade de vida como cultura, saúde, segurança, habitação entre outros, além de gerenciamento inteligente de instalações, espaços públicos e serviços usando tecnologias de TIC.

Independentemente da abordagem usada para classificação, o conceito de cidade inteligente se baseia no uso de TICs como ferramentas para aprimoramento urbano e a tecnologia é um dos principais componentes-chave para promover a inteligência. Nesse sentido, quando se observa o espectro de temas relevantes sob a ótica de cidades inteligentes tem-se, em uma extremidade, uma variedade de dispositivos e sistemas inteligentes que já estão integrados ao ambiente. Esses dispositivos inteligentes podem variar muito em sua finalidade. Eles podem ser sensores embarcados em dispositivos de vestuário tais como roupas, relógios e óculos. Alternativamente, os sensores podem ser embutidos no ambiente para atuação e automação, e em sistemas de controle em residências e escritórios, como controle de iluminação com base na ocupação, sistemas de controle de temperatura programáveis e controle de consumo de água em banheiros. Existem também sensores ambientais embutidos nas unidades de bordo em veículos para evitar colisões e manutenção de veículos. Esses dispositivos são chamados inteligentes pois além de prover monitoramento também podem possuir capacidade de processamento e comunicação que possibilitam seu emprego em sistemas de atuação, automação e controle. Além disso, esses dispositivos estão associados a elementos da rede, como roteadores e *switches*, os quais estão todos integrados à rede IoT que, por sua vez, viabiliza a existência das cidades inteligentes. Na extremidade oposta do espectro, estão os *datacenters* de alto desempenho, escalonáveis e confiáveis da nuvem. Prevê-se que qualquer um dos aplicativos e serviços disponibilizados em uma cidade inteligente será hospedado na nuvem. Portanto, residentes de cidades inteligentes e provedores de serviços podem contar com serviços em nuvem para hospedar, construir e ou implantar seus serviços e aplicativos de cidades inteligentes. No entanto, a disparidade nos protocolos de comunicação, a existência de *softwares* proprietários específicos do fornecedor e diferenças intrínsecas de *hardwares* inibem a ampla implantação de cidades inteligentes. Avanços recentes em virtualização e *software* de várias funcionalidades das camadas de transporte e rede podem superar alguns desses desafios. Tecnologias habilitadoras incluem virtualização das funções de rede, redes definidas por *software* e computação em nuvem, as quais permitem a integração de dispositivos e sistemas e facilitam o gerenciamento e troca de dados provenientes de dispositivos IoT em cidades inteligentes (GHARAIBEH et al., 2017).

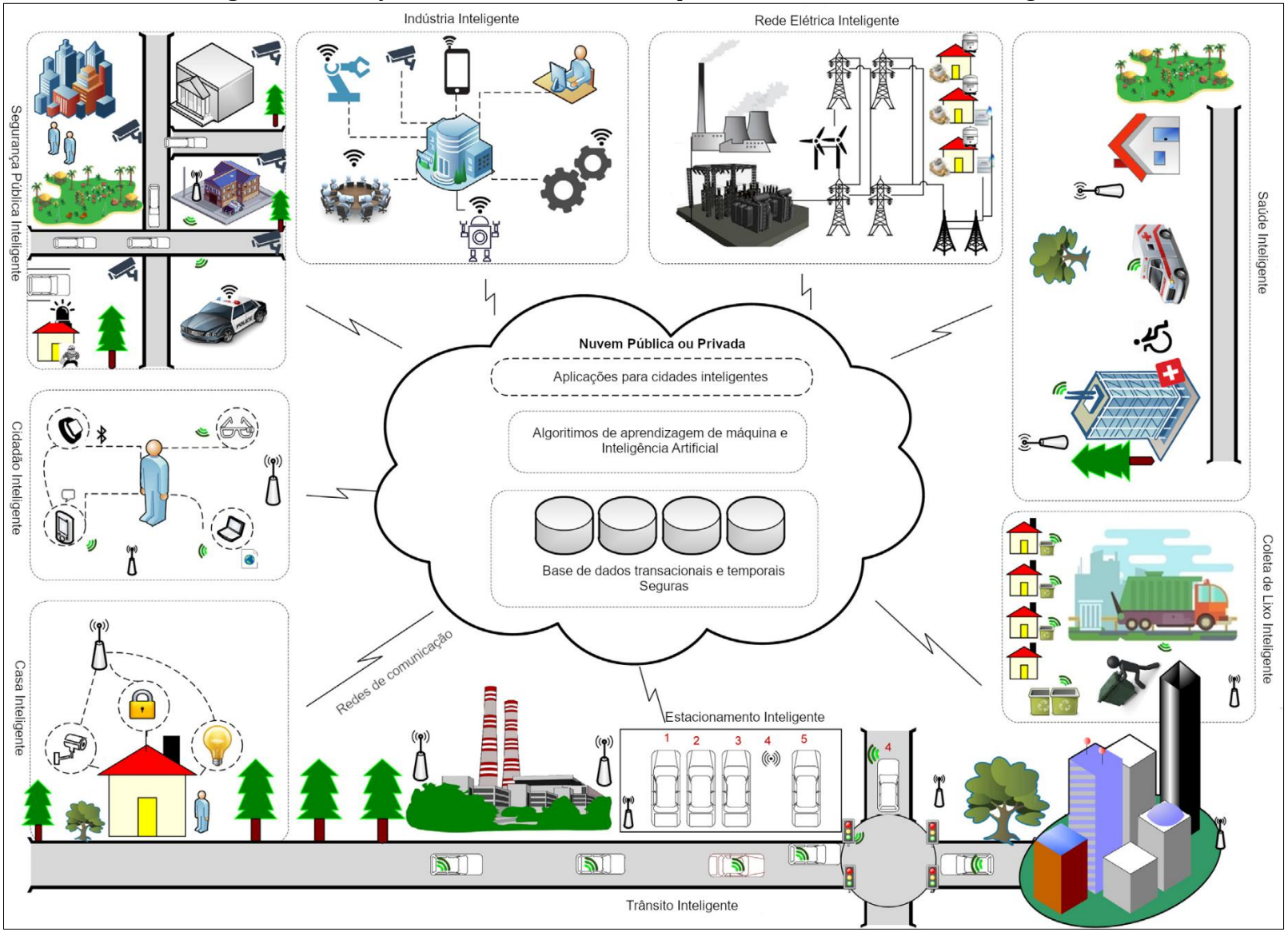
Este trabalho se encaixa nesse contexto e usa como elemento motivador os desafios anteriormente mencionados e a possibilidade de superá-los por meio dos avanços recentes em virtualização de *software* de várias funcionalidades de camadas de rede e transporte. Sendo assim, foi desenvolvida uma solução na qual dispositivos heterogêneos podem ser conectados por meio de redes de acesso a bordas convergentes, *datacenters* e nuvens tradicionais de grande escala utilizando o recurso de virtualização de redes de longas distâncias (SD-WAN). Uma característica das redes de cidades inteligentes é a capacidade de incorporar um grande número de pequenos dispositivos e sensores, introduzindo novas ameaças à segurança e à privacidade. Essas redes distribuídas fisicamente dificultam o fornecimento de segurança física e aumentam a superfície de ataque. Da mesma forma, o uso de sensores e dispositivos proprietários baratos anuncia novas ameaças à segurança e à privacidade. A Figura 1 define como as camadas do modelo de arquitetura IoT se relacionam. A SD-WAN é nesse sentido uma solução holística que visa proteger esses dispositivos de ameaças criando uma camada virtualizada incorporando todos esses elementos e diminuindo assim a superfície de ataque. A Figura 2, ilustra de forma didática o modelo de arquitetura IoT no conceito de cidades inteligentes.

Figura 1. Diagrama de relacionamento entre as camadas da arquitetura IoT



Fonte: Adaptado de (GHARAIBEH et al., 2017)

Figura 2. Ilustração didática do modelo de arquitetura IoT em uma cidade inteligente



Fonte: Adaptado de (HASHEM et al., 2016)

1.2 OBJETIVOS

Tendo em vista o que foi descrito previamente, o objetivo principal deste trabalho foi desenvolver uma solução SD-WAN embarcada *white-label* (etiqueta branca), de baixo custo e de baixo consumo de energia para uso comercial e acadêmico. Nesse ponto é importante destacar que *white-label* é um conceito de mercado oposto ao de *private-label* (marca própria), portanto serve para descrever a terceirização do desenvolvimento de produtos e serviços, criando um molde que pode ser personalizado e redistribuído, de forma que, embora a empresa revendedora não possua direitos sobre a licença do produto ou serviço, também não necessita arcar com custos de criação da solução, podendo, inclusive, lucrar ao adicionar uma taxa e negociar com seus clientes. Em geral, uma solução *white-label* pode ser adotada por uma companhia que pretende expandir sua área de atuação mas não possui expertise suficiente para fazer isso, usando um modelo desenvolvido por uma parceira (FIA, 2020).

1.3 ORGANIZAÇÃO DO TRABALHO

A introdução dessa dissertação encontra-se no Capítulo 1, a qual apresenta uma visão geral das motivações para a realização desse trabalho e lista os objetivos a serem atingidos. O Capítulo 2 apresenta uma fundamentação teórica, com o intuito de introduzir alguns conceitos importantes ao leitor a respeito do tema tratado. O Capítulo 3 apresenta uma revisão bibliográfica, com o objetivo de contextualizar o leitor no estado da arte de SD-WAN. O Capítulo 4 apresenta a metodologia empregada para o desenvolvimento do trabalho, descrevendo de maneira detalhada e sistemática como as atividades de pesquisa foram realizadas, além dos detalhes técnicos de *Hardware* e *Software* utilizados para o desenvolvimento do protótipo proposto. Os principais resultados do trabalho são apresentados no Capítulo 5. Finalmente, uma discussão a respeito dos resultados dos testes de emulação de rede e as considerações finais são dispostas respectivamente nos Capítulos 6 e 7. O Capítulo 8 lista as referências bibliográficas utilizadas como base teórica para o desenvolvimento da pesquisa.

2 FUNDAMENTAÇÃO TEÓRICA

Apesar da adoção generalizada da Internet na sociedade digital e nas cidades inteligentes, as redes IP (do inglês *Internet protocol*) tradicionais são complexas e difíceis de gerenciar (BENSON; AKELLA; MALTZ, 2009) uma vez que precisam ser configuradas de acordo com políticas predefinidas (usando comandos de baixo nível e geralmente específicos do fornecedor) e reconfiguradas para responder a falhas e alterações de carga. Além da inexistência de mecanismos de reconfiguração automática nas redes atuais, soma-se o fato de que elas são integradas verticalmente, ou seja, os planos de controle (que decidem como lidar com o tráfego da rede) e de dados (que encaminham o tráfego de acordo com a decisão do controle) são agrupados. As redes IP atuais evoluem de uma maneira muito lenta, sendo assim, como um novo protocolo de roteamento pode levar vários anos para ser desenvolvido (projetado, avaliado e implantado), uma mudança da arquitetura da Internet, como a substituição do protocolo IP, pode ser considerada uma tarefa impraticável (RAGHAVAN et al., 2012).

Nesse cenário, emergiu uma nova solução baseada em *software* (SD-WAN) com o intuito de: separar a lógica de controle da rede dos roteadores e *switches* subjacentes que encaminham o tráfego, promovendo assim a centralização (lógica) do controle da rede e introduzindo a capacidade para programá-la. A chave para alcançar a flexibilidade desejada é quebrar o problema de controle de rede em partes tratáveis a fim de simplificar o gerenciamento da mesma e facilitar sua evolução (KREUTZ et al., 2015). É importante enfatizar que um modelo programático logicamente centralizado não corresponde a um modelo fisicamente centralizado, de forma que, para garantir níveis adequados de desempenho, escalabilidade e confiabilidade, os projetos de rede SD-WAN recorrem a planos de controle fisicamente distribuídos (JAIN et al., 2013; KOPONEN et al., 2019). A separação do plano de controle do plano de dados pode ser realizada por meio de uma interface de programação de aplicativos (do inglês *Application Programming Interface* –API) bem definida, como a OpenFlow (MCKEOWN et al., 2008a), entre os *switches* e o controlador SDN (do inglês *Software Defined Network*).

Neste capítulo pretende-se promover uma familiarização do leitor com o conceito de SD-WAN, apresentando seus componentes, topologias, arquitetura, discutindo alguns resultados relacionados a desempenho e segurança, fazendo uma revisão histórica de como vem ocorrendo a migração da arquitetura WAN/MPLS para a SD-WAN e destacando os principais benefícios que servem como agentes impulsionadores para a substituição das redes tradicionais por essa tecnologia emergente. Em um esforço para antecipar a evolução futura

deste novo paradigma, são descritas ao final do capítulo, algumas soluções SD-WAN disponíveis comercialmente e uma comparação entre elas.

2.1 REDES TRADICIONAIS IP

As redes de computadores tradicionalmente podem ser divididas quanto à funcionalidade em: planos de dados (composto por dispositivos de rede responsáveis por encaminhar os dados de maneira adequada); controle (protocolos usados para preencher as tabelas de encaminhamento dos elementos do plano de dados) e gerenciamento (que inclui os serviços de *software* usados para monitorar e configurar remotamente a funcionalidade de controle). A política de rede é definida no plano de gerenciamento, executada no plano de dados sob imposição do plano de controle. Nos primórdios da Internet, considerou-se que a melhor maneira de garantir a resiliência da rede era embutir os planos de controle e dados nos mesmos dispositivos da rede, como é feito até hoje em redes IP tradicionais. Apesar dessa abordagem ser eficaz em termos de desempenho de rede, a arquitetura torna-se muito complexa e pouco flexível (BENSON; AKELLA; MALTZ, 2009; KREUTZ et al., 2015; RAGHAVAN et al., 2012). Por esse motivo, um único dispositivo mal configurado pode resultar em perdas de pacotes, *loops* de encaminhamento, configuração de caminhos não intencionais ou violações de contrato de serviço, comprometendo o funcionamento correto de toda a Internet por horas (BUTLER et al., 2010).

Para suportar o gerenciamento de rede, um pequeno número de fornecedores oferecem soluções proprietárias de *hardware* especializado, sistemas operacionais e programas de controle (aplicativos de rede). Os operadores de rede, por sua vez, devem adquirir e manter diferentes soluções de gestão e equipes especializadas, o que implica em um custo operacional de construção e manutenção da infraestrutura de rede significativo, o qual dificulta a inovação e adição de novos recursos e serviços (por exemplo, controle de acesso, balanceamento de carga, eficiência energética, engenharia de tráfego). Para compensar a falta de recursos de *hardware*, uma infinidade de componentes especializados como *firewalls*, sistemas de detecção de intrusão e mecanismos de inspeção profunda de pacotes, proliferam nas redes atuais, o que implica no efeito adverso do aumento de complexidade de projeto e operação da rede (KREUTZ et al., 2015).

2.1.1 Redes WAN e sua evolução

Normalmente, a rede de longa distância (WAN) é projetada para permitir a entrega de dados com o menor esforço e não oferece qualquer garantia para os requisitos da aplicação, uma vez que o tráfego de dados é entregue via *links* físicos vulneráveis e dispositivos de rede em condições adversas (ZUO et al., 2018). Por esse motivo, falhas em *links* e dispositivos ocorrem com frequência, o que afeta severamente o desempenho de transmissão de dados e a qualidade de serviço percebida pelo usuário (do inglês *Quality of Experience* – QoE) (MICHEL; KELLER, 2017). Além disso, as redes de longa distância tradicionais usam protocolos distribuídos para selecionar caminhos de roteamento para os pacotes e a estratégia de melhor esforço não contribui para fornecer um serviço satisfatório (YANG et al., 2019a). Novos aplicativos e cenários operacionais aumentam os requisitos de precisão nas transmissões de dados em redes de longa distância, como por exemplo, os requisitos de baixa latência de rede exigidos no contexto de jogos em nuvem a fim de garantir as interações entre os jogadores e melhorar a experiência do usuário; e no contexto de telemedicina para realizar operações em tempo real. Esses novos aplicativos e cenários não são compatíveis com a mentalidade desatualizada de melhor esforço usada pela rede de longa distância tradicional (ZUO et al., 2018).

A eficiência de custos das redes WAN também incomoda os provedores de rede pois a largura de banda em redes WAN é um recurso caro e, com o rápido crescimento do volume de tráfego na Internet, as operadoras de rede precisam instalar muito mais capacidade de largura de banda para atender aos requisitos de transmissão (YANG et al., 2019a). Apesar da largura de banda em redes de longa distância ser um recurso escasso e valioso, a utilização média mesmo dos *links* mais ocupados em redes de longa distância entre *datacenters* é de apenas 40 a 60% (HONG et al., 2013). Existem dois motivos que levam à ineficiência:1) as redes de longa distância geralmente são super provisionadas para mascarar as falhas de *link* e de dispositivo recorrentes nesse tipo de rede (além de perda de pacotes e picos de tráfego) e 2) a falta de coordenação entre os serviços que usam a mesma rede e enviam tráfego quando querem e quanto querem, o que causa um grande aumento no uso da largura de banda (HONG et al., 2013).

A WAN moderna teve seu início em 1969 com a implantação da ARPANET (Rede da Agência para Projetos de Pesquisa Avançada do inglês *Advanced Research Projects Agency Network*), que foi a precursora da Internet de hoje. Além da evolução contínua da Internet, o período de vinte anos que começou por volta de 1984 viu a implantação de quatro gerações distintas de tecnologias de WAN corporativas. Por exemplo, em meados da década de 80,

tornou-se comum para organizações de tecnologia de informação (TI) corporativas implantar WANs baseadas em TDM (Multiplexação por divisão de tempo, do inglês *time-division multiplexing*) integradas para transportar tráfego de voz e dados. No início da década de 90, as organizações de TI começaram a implantar WANs baseadas em *Frame Relay*, com o intuito de reduzir custos e complexidade. Em meados da década de 90, algumas organizações de TI substituíram suas WANs baseadas em *Frame Relay* por WANs baseadas na tecnologia ATM (do inglês *Asynchronous Transfer Mode*) com o objetivo de aumentar a largura de banda. Em seguida, com a intenção de reduzir custos e melhorar o desempenho, as Redes Privadas Virtuais (do inglês *Virtual Private Network* – VPN) começaram a ser implementadas. No entanto, o *design* de VPN IP não oferece suporte a serviços diferenciados, engenharia de tráfego e reserva de recursos, então na primeira década do século 21, muitas organizações de TI substituíram seus *Frame Relay* ou WANs baseados em ATM por WANs baseados em MPLS para fornecer roteamento simplificado, suporte à engenharia de tráfego e melhor qualidade de serviço (do inglês *Quality of Service* – QoS) na WAN (METZLER, 2015).

O emprego da tecnologia MPLS é considerado um marco no histórico das redes WAN, pois fornece conectividade *full-mesh*, alto rendimento, boa largura de banda e maior velocidade. Ao invés de roteamento baseado em IP salto a salto (do inglês *hop-by-hop*), o MPLS usa encaminhamentos baseados em rótulo (DINCER; ALVIZU; MAIER, 2018), encaminhando pacotes para o roteador de destino com rotas predeterminadas chamadas caminhos de comutação de rótulo (do inglês *label switching paths* – LSPs) o que permite suporte para muitos serviços, como MPLS VPN (DAUGHERTY; METZ, 2005), que simula a operação de uma WAN privada na Internet pública.

Basicamente, MPLS é uma técnica para transportar rapidamente os dados de qualquer protocolo e moldar o fluxo da rede permitindo realizar engenharia de tráfego em redes IP e fornecer uso eficiente de seus recursos. Dessa forma, pode-se listar as seguintes vantagens no uso do MPLS (DINCER; ALVIZU; MAIER, 2018):

- Um único circuito de portadora pode suportar MPLS, Internet e SIP (Protocolo de Iniciação de Sessão do inglês *Session Initiation Protocol*);
- Mantém a qualidade dos protocolos em tempo real, como VoIP (do inglês *Voice of IP*);
- Entrega os pacotes com alta QoS e confiabilidade;
- Gerencia de maneira proficiente o fluxo de pacotes;
- Evita perda de pacotes;

- Apresenta a capacidade de controlar onde e como o tráfego é roteado em sua rede para gerenciar capacidade, priorizar serviços diferentes e evitar congestionamento;
- Permite a implementação de redes multisserviço;
- Tem a capacidade de fornecer serviços de transporte de dados, bem como serviços de roteamento IP, na mesma infraestrutura de rede comutada por pacotes.

Apesar dos aspectos positivos, o emprego de MPLS apresenta alguns pontos negativos (DINCER; ALVIZU; MAIER, 2018):

- O alto custo da largura de banda (o megabyte MPLS custa excepcionalmente mais do que um megabyte de banda larga mensal);
- Não oferece proteção de dados integrada;
- Configuração sobrecarregada: cada dispositivo deve ser configurado separadamente;
- Tempo necessário para transição/atualização/operação está diretamente relacionado ao número de filiais e dispositivos de borda.
- Suporte limitado para cargas de trabalho em nuvem.

Anos atrás, quando a WAN foi projetada pela primeira vez, a arquitetura era simples. Hoje, o fluxo de tráfego de aplicativos está mudando, os aplicativos corporativos estão migrando para a nuvem e as empresas estão usando aplicativos de *software* como serviço (do inglês *Software as a Service* - SaaS) com mais frequência, de forma que grande parte do tráfego está fluindo pela Internet (VMWARE, 2019). A WAN foi construída inicialmente para conectar a filial ao *data center*, por meio de redes privadas virtuais do provedor de serviços. O tráfego entre a origem e o destino era baseado nos endereços TCP/IP, nas tabelas da lista de controle de acesso e em outros protocolos de roteamento complexos (THE TARASPAN BLOG, 2020). Esse modelo funcionou bem, pois todos os aplicativos eram hospedados nos *data centers* corporativos. No entanto, com a inclusão da nuvem, essa estratégia não é mais eficiente, pois a nuvem é acessada pela Internet onde o desempenho não é ideal e nem seguro.

2.1.2 Redes WAN e suas limitações

No relatório chamado "*The* 2015 *Guide to WAN Architecture & Design*" (METZLER, 2015) foram identificadas as principais preocupações que as organizações de rede tem com os dois serviços de WAN ainda usados (MPLS e Internet) listados em sua ordem de importância:

- MPLS: custo, tempo de atividade, latência, tempo de espera para implementar novos circuitos, segurança, tempo de espera para aumentar a capacidade dos circuitos existentes, perda de pacotes, *jitter*;
- Internet: segurança, tempo de atividade, latência, custo, perda de pacote, tempo para incrementar a capacidade dos circuitos existentes, tempo para implementar novos circuitos, *jitter*.

As redes de longa distância (WANs) tradicionais baseadas em *hardware* geralmente são incapazes de atender às necessidades de operações remotas por serem complexas, rígidas, frágeis e requerem uma quantidade significativa de infraestrutura para dar suporte a operações remotas. Alguns dos principais problemas associados a essas redes são (THE TARASPAN BLOG, 2020):

- Dependência de protocolos de roteamento tradicionais: muitos protocolos e instâncias de protocolo precisam ser configurados e gerenciados, incluindo MPLS, iBGP (do inglês *interior Border Gateway Protocol*), OSPF (do inglês *Open Shortest Path First*), NHRP (do inglês *Next Hop Resolution Protocol*), etc. Cada um desses protocolos requer interação e troca significativa de estado entre eles e qualquer mudança na topologia requer um reajuste ou um reprojeto de seus protocolos de roteamento, os quais interagem com os protocolos de roteamento do provedor de serviços, aumentando ainda mais a complexidade e reduzindo a capacidade de resposta.
- Incapacidade de obter facilmente visibilidade em aplicativos de nuvem e SaaS: a equipe de TI precisa ser capaz de visualizar as métricas de desempenho para solucionar problemas, mas em uma rede tradicional, os serviços que estão fora da rede não podem ser monitorados. Algumas ferramentas podem ser adquiridas no mercado para fornecer a visibilidade necessária de cada um dos elementos, mas essas ferramentas são incompletas e às vezes impossíveis de implementar, adicionando complexidade a um sistema já frágil.
- A adição de um novo site ou mudanças no existente requer um processo manual exaustivo;
- Visibilidade e segurança da aplicação comprometidas: As tecnologias de rede tradicionais não são adequadas para implementar dinamicamente uma nova postura de segurança com base na mudança de topologia ou ameaça;
- Gerenciamento complicado e estático de configurações da rede;

- Dependência total do provedor de serviços de Internet: redes WAN baseadas em *hardware* geralmente são construídas com *switches* e roteadores proprietários de um fornecedor. A cada três a cinco anos, eles precisam passar por uma atualização, o que significa que muitas vezes é necessário um orçamento de centenas de milhares de dólares para isso, incluindo custos de suporte e manutenção.
- Ocorrência de falha completa da rede, uma vez que o *link* de *backup* vem de um único ISP (provedor de serviço de Internet, ou do inglês, *Internet Service Provider*);
- Não apresenta nenhum modelo verificável para segurança e conformidade, dificultando seu monitoramento contínuo.

2.2 SD-WAN

A arquitetura estática e inflexível da rede WAN baseada em *hardware* é inadequada para lidar com as tendências de rede cada vez mais dinâmicas do cenário atual e atender aos requisitos de QoE dos usuários modernos que incluem dispositivos IoT e cidades inteligentes em geral. Os principais objetivos da implantação de redes de longa distância definidas por *software* (SD-WAN) é simplificar as operações, otimizar o gerenciamento e introduzir inovação e flexibilidade em comparação com as arquiteturas de rede WAN baseadas em *hardware* (BANNOUR; SOUIHI; MELLOUK, 2018).

Uma vez que as SD-WANs consistem na aplicação dos conceitos das SDNs em redes geograficamente distantes, a seguir serão apresentados alguns detalhes relacionados à definição e à estrutura das SDNs.

2.2.1 Rede definida por Software (SDN)

Em KREUTZ et al. (2015), uma SDN é definida como uma arquitetura de rede com quatro pilares:

1. Os planos de controle e dados são desacoplados de forma que a funcionalidade de controle é removida dos dispositivos de rede, os quais tornam-se simples elementos de encaminhamento de pacotes;
2. As decisões de encaminhamento são baseadas no fluxo, ao invés de baseadas no destino: No contexto SDN, um fluxo é uma sequência de pacotes entre uma origem e um destino, os quais recebem políticas de serviço idênticas nos dispositivos de encaminhamento e cuja abstração permite unificar o

comportamento de diferentes tipos de dispositivos de rede (como roteadores, *switches, firewalls* e *middleboxes*);

3. A lógica de controle é movida para uma entidade externa, o chamado controlador SDN ou Sistema Operacional de Rede (do inglês *Network Operating System* – NOS), uma plataforma de *software* que funciona com tecnologia de servidor de *comodity* e fornece os recursos e abstrações essenciais para facilitar a programação de dispositivos de encaminhamento com base em uma visão de rede logicamente centralizada e abstrata.
4. A rede é programável por meio de aplicativos de *software* executados no NOS que interagem com os dispositivos de plano de dados subjacentes.

Particularmente, a centralização da lógica de controle: i) aumenta a simplicidade e reduz os erros decorrentes da modificação de políticas de rede que passam a ser feitas via linguagens de alto nível e componentes de *software*, ao invés de configurações específicas em dispositivos de baixo nível; ii) mantém as políticas de alto nível intactas ao implementar um programa de controle capaz de reagir automaticamente a mudanças espúrias do estado da rede; iii) permite um conhecimento global do estado da rede, o que simplifica o desenvolvimento de funções, serviços e aplicativos mais sofisticados.

2.2.2 Estrutura das SDN

O primeiro termo que é importante ser identificado para o melhor compreendimento das redes SDN é o termo “dispositivos de encaminhamento” (do inglês *Forwarding Devices*-FD). Os FD são dispositivos de plano de dados baseados em *hardware* ou *software* que executam um conjunto de operações elementares e têm conjuntos de instruções bem definidas (por exemplo, regras de fluxo) usadas para realizar ações nos pacotes de entrada (por exemplo, encaminhar para portas específicas, descartar, encaminhar para o controlador, reescrever algum cabeçalho).

As redes SDN possuem duas interfaces de programação de aplicativos (API) bem definidas(DINCER; ALVIZU; MAIER, 2018; KREUTZ et al., 2015):

- *Southbound Interface* (SI):define o protocolo de comunicação entre os dispositivos de encaminhamento e os elementos do plano de controle formaliza a comunicação/interação entre os dispositivos do plano de dados e plano de controle (“OpenFlow”(MCKEOWN et al., 2008b) é o protocolo SI mais comum).

- *Northbound Interface* (NI): realiza a comunicação entre os serviços e aplicativos em execução na rede e o controlador SDN. O sistema operacional de rede pode oferecer uma API para desenvolvedores de aplicativos que representa uma interface comum para o desenvolvimento de aplicativos, abstraindo os conjuntos de instruções de baixo nível usados pelas SI para programar os dispositivos de encaminhamento.

Adicionalmente, as redes SDN podem ser divididas em três planos de funcionalidade (DINCER; ALVIZU; MAIER, 2018):

- Plano de dados: compreende os dispositivos de encaminhamento interconectados sendo responsável por encaminhar os dados pela rede. Os dispositivos de encaminhamento são interconectados por meio de canais de rádio sem fio ou cabos com fio.
- Plano de controle: é o cérebro da rede, representa os protocolos e algoritmos usados para preencher as tabelas de encaminhamento no plano de dados. Os dispositivos de encaminhamento são programados por elementos do plano de controle por meio de modalidades SI bem definidas.
- Plano de gerenciamento: Inclui os serviços de *software* para monitorar e configurar remotamente a funcionalidade do plano de controle. O plano de gerenciamento é o conjunto de aplicativos que potencializam as funções oferecidas pela NI para implementar o controle de rede e a lógica de operação. Isso inclui aplicações de roteamento, *firewalls*, balanceadores de carga, monitoramento e assim por diante. Essencialmente, um aplicativo de gerenciamento define as políticas, que são traduzidas em instruções específicas para a SI que programam o comportamento dos dispositivos de encaminhamento.

2.2.3 Arquitetura da SD-WAN

Ao complementar as redes tradicionais com SD-WAN, os dispositivos conectados encontrarão certos problemas que devem ser resolvidos obrigatoriamente. Portanto, é essencial pensar sobre alguns pontos importantes, como:

- A escolha entre um modelo local ou baseado em nuvem precisa levar em consideração: latência, largura de banda, desempenho etc.
- Os dados de missão crítica precisam garantir que estão dentro dos SLAs (do inglês *Service Level Agreements*), com referência à disponibilidade, latência e desempenho.

- Não negligenciar as ferramentas de otimização de WAN que são indispensáveis em termos de desempenho.

Com as transformações na rede, o ecossistema de segurança também é afetado. Se for uma rede privada, a atuação ocorre na zona segura, no entanto, quando a rede está conectada a uma rede pública aberta, é necessária uma maneira mais segura. Assim, pode-se afirmar que a segurança também deve ser contabilizada nos benefícios oferecidos pela SD-WAN, uma vez que:

- A SD-WAN tem um recurso que permite à organização elaborar políticas de segurança uniformes em toda a empresa.
- A adição de SD-WAN fornece um ecossistema de segurança seguro e equilibrado para as empresas que têm despesas de segurança remendadas em suas filiais.
- A implementação rápida de políticas de segurança permite que as organizações configurem a infraestrutura em menos tempo, o que permite uma resposta mais rápida.

Recursos analíticos, estatísticos, de monitoramento e de visualização devem estar alinhados para gerenciar o fluxo de tráfego, políticas etc., implicando em bons resultados, como:

- Dados analíticos e de desempenho alavancam os gerenciadores de rede para adquirir um bom entendimento das cargas de trabalho, desempenho e outros fatores significativos.
- Além disso, atributos importantes de monitoramento SD-WAN incorporam monitoramento de QoS, monitoramento de terminais e componentes, gerenciamento de acesso e análise de dados de rede etc.

A separação do encaminhamento de dados do plano de controle simplifica o roteamento do tráfego de rede, sendo o principal benefício da tecnologia SD-WAN. Anteriormente, as unidades remotas de empresas e organizações eram conectadas ao *data center* que, por sua vez, era conectado à nuvem, portanto, a falha em uma única linha alugada levaria a uma queda do tráfego de toda a rede. Com SD-WAN, todas as filiais são individualmente conectadas diretamente ao *data center* e à nuvem. Nesse caso, se qualquer uma das linhas alugadas cair, o SD-WAN redirecionará a rota não afetando as outras linhas de rede. Além disso, com SD-WAN, uma empresa pode utilizar várias redes sem medo de latência, perda de pacotes, *jitter* e falha de rede.

Componentes da arquitetura SD-WAN:

- **Segurança Integrada** (ARPITA SAXENA (TARASPAN BLOG), 2020): Com a transição do uso limitado da Internet para a Internet em limitação de largura de banda, a segurança torna-se a principal preocupação com SD-WAN, de forma que maior desempenho deve ser diretamente proporcional à conformidade de segurança. Um dos benefícios da arquitetura WAN por *software* é que, em vez de contratar uma solução de segurança à parte, é possível incrementá-la na própria SD-WAN.
- **Suporte de nuvem nativa** (ARPITA SAXENA (TARASPAN BLOG), 2020): A integração em nuvem fornece às empresas uma base para gerenciar a rede localmente e via Internet. Como vantagem, algumas das soluções SD-WAN oferecem monitoramento e roteamento inteligente no nível da aplicação para obter uma experiência de usuário de alta qualidade, mesmo que a conexão com a Internet não seja boa. Algumas das empresas optam por provedores de nuvem pública, como AWS (*Amazon Web Services*), que oferecem duas opções: conectividade inicial para a nuvem e a solução de *backup* robusta para longo prazo.
- **Virtualização** (REDAÇÃO VIVO MEU NEGÓCIO, 2019): Uma solução que já é realidade em tecnologia de informação é a virtualização das infraestruturas de *data centers* e servidores para as nuvens públicas, privadas ou híbridas e a virtualização de redes, ou seja, parte do trabalho de estruturação de redes passa a ser desempenhada por máquinas virtuais via *software* não sendo mais necessário ter um *hardware* dedicado. Tudo pode ser feito em um ambiente virtual, situado na nuvem. Serviços como *firewall* e soluções que previnem o ataque de intrusos são alocados inteiramente em *data centers* dos provedores destes serviços. Essa tecnologia que garante serviços mais rápidos, com alta escalabilidade, sob demanda e melhor custo-benefício do que os modelos físicos por não necessitar de alocação de equipamento dedicado e específico, manutenção constante e visitas técnicas, conhecida como Virtualização das Funções de Rede (NFV, do inglês *Network Functions Virtualization*).
- **Automação** (ARPITA SAXENA (TARASPAN BLOG), 2020): A maioria dos fornecedores de SD-WAN permite a automação (com o intuito de reduzir complexidade) por meio do portal de gerenciamento central, oferecendo a

capacidade de provisionar um novo *site* com rapidez, resolver problemas e notificar sobre ameaças e problemas em potencial.

2.2.4 Tipos de arquiteturas SD-WAN

- *ON-PREMISE ONLY* (ARPITA SAXENA (TARASPAN BLOG), 2020*)*: Esta arquitetura SD-WAN conecta apenas os *sites* da empresa por meio de uma caixa SD-WAN ou roteador *plug-n-play*. A caixa SD-WAN no local não se conecta a nenhum dos *gateways* de nuvem. De fato, ela executa a modelagem de tráfego em tempo real em cada lugar (apenas nos vários *sites* de uma empresa). Essa arquitetura é perfeita para as organizações que têm aplicações e operações internas, isto é, não em infraestrutura baseada em nuvem. Consiste numa configuração comum que acomoda rede MPLS para voz, vídeo ou *desktop* virtual, enquanto a Internet pública, controlada por SD-WAN, é alocada para todo o resto. Dentre os pontos positivos pode-se citar: desempenho aprimorado de todos os aplicativos WAN; balanceamento de carga Multi-circuit/ISP; recuperação de desastres aprimorada;
- *CLOUD-ENABLED*: Esta estrutura compreende uma caixa SD-WAN que está conectada a uma nuvem ou *gateway* virtual. Aproveita as vantagens da arquitetura local (modelagem de tráfego em tempo real e balanceamento de carga/*failover* de vários circuitos), juntamente com os recursos de infraestrutura em nuvem, confiabilidade e desempenho aprimorado. Além disso, o *gateway* de nuvem está diretamente conectado com os principais provedores de nuvem - Office 365, AWS, Salesforce, DropBox, Azure etc. No caso, se o seu circuito de Internet cair, a sessão de nuvem ainda permanecerá ativa. Além disso, se a empresa usa a linha secundária de Internet, o SD-WAN redirecionará seu aplicativo em nuvem para essa linha secundária, sem perder a sessão atual. Perfeito para empresas que usam muitos serviços baseados em nuvem - como Office 365, Salesforce ou aplicativos executados na AWS. Dentre os pontos positivos dessa arquitetura vale a pena destacar: aumento do desempenho dos aplicativos em nuvem; confiabilidade aprimorada de aplicativos em nuvem; balanceamento de carga Multi-circuit/ISP;
- *CLOUD-ENABLED PLUS BACKBONE*: Esta solução inclui uma caixa SD-WAN que conecta o *site* da empresa ao ponto de presença (do inglês *point of*

presence - POP) de rede mais próximo do provedor SD-WAN, onde seu tráfego será transferido para o *backbone* de rede privada do provedor, o que garante a redução do nível de latência, *jitter* e perda de pacotes e, consequentemente, leva a um aumento no gráfico de desempenho do tráfego de rede. Além disso, como a arquitetura baseada em nuvem, o *backbone* está diretamente conectado com os principais fornecedores de aplicativos em nuvem - *Office 365* e AWS etc., o que melhora a confiabilidade e o desempenho geral desses aplicativos. É a arquitetura perfeita para as empresas que estão prestes a eliminar sua rede MPLS e, ao mesmo tempo, executar muitos aplicativos de rede em tempo real. Dentre os pontos positivos, vale a pena destacar: aplicativos de missão crítica em *backbone* privado levam à melhoria no desempenho de todos os aplicativos de rede; o *gateway* de nuvem aumenta o desempenho e a confiabilidade dos aplicativos em nuvem; e o balanceamento de carga *Multi-circuit/*ISP.

A seguir, apresenta-se uma visão geral das arquiteturas lógica e física da rede de longa distância definida por *software* baseada em YANG et al. (2019).

2.2.5 Arquitetura Lógica

Existem três camadas no modelo de arquitetura SD-WAN:

- Camada de dados - As funções da camada de dados podem ser classificadas em virtualização de largura de banda e encaminhamento de dados. Geralmente, existem vários tipos de redes em uma rede WAN, por exemplo, MPLS, Internet, 4G e assim por diante. Para utilizar totalmente os recursos de largura de banda, a virtualização de largura de banda combina diferentes *links* de rede. Por outro lado, o encaminhamento de dados consiste em um conjunto distribuído de elementos de encaminhamento por rede (principalmente *switches*) encarregados de encaminhar pacotes usando a largura de banda fornecida pela virtualização de largura de banda (BANNOUR; SOUIHI; MELLOUK, 2018). Ambas funções recebem comandos do controlador de rede da camada superior por meio de protocolos de interface como o OpenFlow (MCKEOWN et al., 2008b).
- Camada de controle - Existem muitas funções de rede na camada de controle (MICHEL; KELLER, 2017). Tais funções de rede são implementadas e gerenciadas de forma independente. O desacoplamento dessas funções permite que os operadores de rede desenvolvam, modifiquem, depurem e removam qualquer uma delas a um custo baixo, sem afetar outras. Além de funcionar de

forma independente, as funções de rede podem ser conectadas ou encadeadas para criar serviços múltiplos e aumentar a flexibilidade da SD-WAN (GEMBER-JACOBSON et al., 2015). Por exemplo, o monitoramento de rede fornece uma visão global da rede para a engenharia de tráfego, com a qual esta última calcula uma solução de escalonamento ótima para executar na rede(JAIN et al., 2013). A garantia de QoS se encarrega de satisfazer os requisitos da aplicação durante a transmissão de dados (NAM et al., 2014).

- Camada de aplicação – permite que os provedores de rede e desenvolvedores de aplicativos declarem seus requisitos específicos para a rede por meio de expressão de rede e expressão de aplicativo, sendo que ambos são capazes de traduzir requisitos de alto nível expressos quase em linguagem natural em configurações de rede compatíveis (HARTERT et al., 2015). À medida que mais e mais aplicações surgem com diversos requisitos muitas vezes conflitantes, é necessário customizar as políticas de rede levando em consideração as características da aplicação (YIN et al., 2015). Por exemplo, o serviço de *streaming* de vídeo ao vivo espera alta taxa de bits e baixa latência para satisfazer os usuários, mesmo que esses dois objetivos sejam conflitantes. Com a expressão de aplicativos, os desenvolvedores de aplicativos podem declarar suas estratégias sobre como lidar com esses requisitos e executá-los na WAN subjacente. Semelhante à expressão de aplicação, a expressão de rede é projetada para relatar requisitos de rede, como rede econômica (JALAPARTI et al., 2016) e rede multiobjetivo (NAM et al., 2014). A camada de aplicação permite que os provedores de rede e desenvolvedores de aplicativos se envolvam mais no controle da rede.

2.2.6 Arquitetura Física

Na camada de dados, há um conjunto de *switches* SDN interconectados entre si por *links* físicos (BANNOUR; SOUIHI; MELLOUK, 2018). Um controlador de rede é responsável por esses dispositivos. Normalmente, o controlador de rede é um servidor ou *cluster*, dependendo do tamanho e da complexidade da rede (SHUHAO LIU; BAOCHUN LI, 2015). Várias funções de rede são carregadas pelo controlador de rede. No topo do controlador de rede estão os aplicativos específicos. Os desenvolvedores de aplicativos e provedores de rede podem expressar seus requisitos ao controlador de rede, e o controlador de rede os transformará em políticas e configurações compatíveis. Geralmente, há mais de um controlador de rede distribuído em locais diferentes, em que um deles é selecionado como

controlador mestre e os outros como controladores de *backup* (BERDE et al., 2014). Quando o controlador mestre falha, um dos controladores de *backup* assume imediatamente (BANNOUR; SOUIHI; MELLOUK, 2018).

2.3 MIGRAÇÃO: WAN/MPLS → SD-WAN

Segundo TOSTES (2020), com a transição das organizações para um modelo de negócios digital, o aumento do trabalho remoto e a adoção de várias nuvens, há um impacto significativo nas topologias de rede, levando ao crescimento exponencial no número de dispositivos, usuários, banda larga, tráfego criptografado e aplicativos na nuvem em redes WANs corporativas. Ao contrário das arquiteturas WAN tradicionais, as SD-WANs podem distribuir o tráfego a vários locais de forma dinâmica, enquanto atendem automaticamente às políticas de aplicativos em constante evolução. As SD-WANs também são agnósticas em termos de transporte e operadora, isso quer dizer que o MPLS de alto custo pode ser substituído por conexões mais econômicas (por exemplo, Internet e LTE), permitindo funções que economizam tempo e reduzem os custos, como a seleção do caminho mais inteligente. Apesar do MPLS manter a qualidade de dados durante o fluxo e não reconhecer o termo "perda de pacotes", o custo de largura de banda é uma característica desvantajosa, a qual é superada pelo SD-WAN que, por sua vez, reduz as despesas operacionais gerais, tornando-se a solução perfeita para empresas que buscam tecnologias WAN baseadas em nuvem, abertas, flexíveis e que requerem boa largura de banda. Tendo isso em vista, a seguir tem-se uma lista de características de redes nas quais foram comparados o tradicional MPLS com SD-WAN (RATHORE, 2020):

- Problemas de largura de banda: MPLS tem problemas com alto uso de largura de banda, tornando os custos de circuitos mensais excessivos. Por outro lado, a SD-WAN utiliza várias conexões de Internet de alta largura de banda da organização o que permite que as empresas tenham uma Internet mais rápida a custos mais baixos.
- Desempenho aprimorado: MPLS fornece uma conexão de rede com classe de serviço (do inglês *Class of Service* – CoS) estática. Classe de serviço é uma forma de gerenciar vários perfis de tráfego em uma rede, dependendo da prioridade do tráfego. Com SD-WAN, se uma empresa tiver várias conexões ISP, o tráfego será enviado através do circuito com a rota mais rápida. A capacidade de enviar tráfego ao longo do melhor caminho, consequentemente, leva a um melhor desempenho.

- SD-WAN possui a capacidade de priorizar aplicativos para aprimorar a experiência do usuário. O SD-WAN está no topo da rede e une o MPLS subjacente e outras conexões de Internet, o que os ajuda a encaminhar o tráfego crítico pelo melhor caminho disponível.
- SD-WAN oferece os mesmos benefícios, independentemente de qual ISP que a empresa esteja usando. A empresa pode adicionar e remover ISPs a qualquer momento e em qualquer local sem qualquer aborrecimento, tornando-o muito mais escalonável.
- Em termos de segurança, no MPLS, há linhas dedicadas e o tráfego de Internet é enviado de volta ao *data center* para inspeção. No SD-WAN, a segurança é incorporada na forma de *firewalls*, VPN automática e segmentação de rede.
- No SD-WAN, há acesso direto à nuvem, enquanto no MPLS é feito *backhaul* (porção de uma rede hierárquica de telecomunicações responsável por fazer a ligação entre o núcleo da rede, ou *backbone*, e as sub-redes periféricas) para o *data center* e depois para a nuvem.

2.4 RECURSOS DA SD-WAN

Antes de propor um novo dispositivo *white-label* com tecnologia SD-WAN, faz-se necessário considerar quais recursos devem ser fornecidos pelo projeto (THE TARASPAN BLOG, 2020):

- Endpoints: Certificar de que a solução SD-WAN deve se conectar a todos os terminais, como a qualquer aplicativo, *software*, outros tipos de recursos - IaaS/SaaS (IaaS vem do inglês *Infrastructure as a Service*, que significa infraestrutura como serviço) ou usuários móveis.
- Rede de sobreposição criptografada: Primeiro, o tráfego em toda a rede de sobreposição deve ser criptografado completamente para evitar quaisquer ameaças e a sobreposição deve ser orientada por políticas.
- Políticas baseadas em aplicativos: As políticas configuráveis devem definir para os aplicativos, alternativas de *failover* e o limite máximo e mínimo para *jitter*, latência e perda.
- Roteamento baseado em políticas: a SD-WAN deve incluir algoritmos que podem descobrir o caminho ideal para uma aplicação específica, com base nas estatísticas em tempo real e nas políticas configuradas da aplicação.

- Independência de serviços de dados: SD-WAN deve se conectar a várias estações com várias categorias de serviços de dados de Internet, como xDSL, 4G/LTE, fibra, cabo etc.
- Monitoramento em tempo real: O equipamento SD-WAN deve ter a capacidade de coletar a latência em tempo real e as estatísticas de perda de pacotes da linha conectada.
- Balanceamento de carga: A técnica de balanceamento de carga gerencia várias solicitações de tráfego de entrada e saída e garante que a largura de banda seja utilizada corretamente.
- Resiliência: a SD-WAN deve suportar recursos de redundância e *failover*. Na verdade, o núcleo da rede deve ser totalmente redundante com os usuários e deve ser conectado automaticamente ao próximo POP (Ponto de Presença) no caso de alguma falha.
- Seleção de caminho dinâmico: sempre deve-se certificar que sua SD-WAN acomodou o atributo de monitoramento em tempo real. Esse atributo é responsável por estudar os padrões como perda de pacotes, latência, *jitter* etc. e selecionar o canal ideal entre muitos para que a saída seja produtiva e organizada.
- Gerenciamento de tráfego flexível: O controle de acesso e o encaminhamento do tráfego para as conexões WAN é uma etapa vital, especialmente no caso da largura de banda limitada. Portanto, o fornecedor deve prover o suporte do tipo de modelagem de tráfego, taxa limitada e QoS (Qualidade de Serviço) entre o usuário final e a borda do provedor.

Além dos recursos/características mandatórias de uma SD-WAN descritos acima, ainda existem algumas outras características recomendáveis (THE TARASPAN BLOG, 2020):

- Recursos avançados de segurança e VPN: Junto com os recursos de segurança fundamentais, é necessário que o SD-WAN também tenha recursos de segurança avançados. Se a rede e a segurança estiverem equipadas, a implantação se tornará mais fácil, simplificada e econômica. Na ausência da versão avançada dos atributos de segurança na empresa e em todas as suas estações de filiais, uma ameaça sempre persiste. Portanto, sempre deve-se certificar de que os três indicadores a seguir devem ser acoplados ao SD-WAN:
    - *Firewall* de última geração

- *Gateway* da Web seguro
- Proteção Avançada contra Ameaças

Para as filiais:

- Dispositivos finais de segurança local
- Função de rede virtual
- Firewall como serviço (FwaaS)

- Recursos de mobilidade: A mobilidade se tornou um elemento indispensável da era da tecnologia atual. Na verdade, é uma vantagem da tecnologia que tornou a conexão mais interativa. Esta é a razão pela qual a mobilidade é um componente obrigatório do SD-WAN. A inclusão da nuvem torna a mobilidade, o componente impossível de ignorar. Qualquer SD-WAN deve estar em sincronia com o celular e outros recursos /usuários, independentemente da hora e local. Os dispositivos dos usuários móveis devem ser integrados ao *software* do cliente para se conectar com SD-WAN com segurança. A próxima etapa é que o usuário móvel deve ter o *backup* das mesmas políticas de segurança, roteamento otimizado e controles de gerenciamento que os usuários de qualquer escritório ou unidade da organização remotos possuem. Portanto, os seguintes recursos são requeridos:
  - Seleção automática de rota ideal
  - Parâmetro de Segurança Avançada
  - Controle de acesso
- Recursos de gerenciamento: O console de controle e gerenciamento é o elemento de verificação obrigatória do SD-WAN pois é a base para tornar todas as operações livres de congestionamento e simplificadas. Ele deve estar equipado com todas as políticas de roteamento, protocolos de gerenciamento centralizado e controles de acesso para observar e rastrear todo o processo. Portanto, os recursos a seguir devem ser os complementos para o modelo SD-WAN:
  - Protocolos de gerenciamento e APIs
  - Engenharia analítica e integração
  - Métricas de uso detalhadas
  - Visibilidade abrangente em tempo real
  - Definição de políticas baseadas em aplicativos

Apesar de que nenhum modelo SD-WAN seja projetado e implantado de forma equivalente, devendo levar em consideração a estrutura da rede corporativa, os requisitos e o orçamento, para adquirir uma sobreposição SD-WAN funcional completa, é necessário considerar as seguintes etapas (THE TARASPAN BLOG, 2020):

- Número de *sites* remotos
- Dimensionamento correto do modelo de implantação (com base na contagem de usuários finais e no uso esperado de WAN)
- Avaliação de todos os aplicativos, serviços e cargas de trabalho
- Opções de conectividade WAN disponíveis
- Seleção de um modelo de implantação
- Plano prévio para coleta de fluxo de dados WAN pós-implantação
- Melhoria constante na análise WRT.

2.5 ABORDAGEM SDN COM IPV6

O rápido incremento de usuários da Internet em todo o mundo e o aumento dos dispositivos inteligentes (IoT) criaram uma tendência de mudança para o ambiente de rede convergente, incentivaram pesquisadores, desenvolvedores e empresas de rede em todo o mundo a aprimorar a inteligência nas tecnologias de rede, contribuindo para criar um modelo de nova geração. Baseado nesse novo paradigma, o mecanismo de endereçamento IPv6 (versão mais atual do Protocolo de Internet, ou "nova geração do IP", que deve funcionar lado a lado com o IPv4 e, a longo prazo, substituí-lo) e as soluções baseadas em SDN possuem forte sinergia para capturar os benefícios de ambas as tecnologias. A disponibilidade de endereços IP fornecidos pelo IPv6 permite a interligação e comunicação de dispositivos inteligentes requeridas pela evolução do conceito de IoT, ao mesmo tempo que o recurso de programação das SDN ajuda a introduzir inteligência em todos os dispositivos. Essas tecnologias, reconhecidas como camada de operação de rede, são operadas por provedores de serviços, enquanto os serviços fornecidos ao cliente por ISPs e Telcos (companhias de telecomunicações, do inglês *telecommunications company*) constituem as atividades da camada de serviço. SDN e IPv6 tornaram-se cada vez mais importantes no ambiente de rede moderno como resultado das mudanças de paradigma nas comunicações móveis provocadas pela conceituação e execução do modelo de dados 5G. Como resultado, a disponibilidade de 5G, SDN e IPv6 está amplamente relacionada à computação em nuvem, computação em névoa e computação de borda, desde a rede principal até o provisionamento de serviços de rede de acesso final (DAWADI et al., 2022).

2.6 SOLUÇÕES COMERCIAIS DISPONÍVEIS

De acordo com FOREST; LERNER; SINGH, (2020) o mercado de infraestrutura de redes de longa distância (WAN) está evoluindo de roteadores de filiais tradicionais comumente chamados de “roteadores de borda do cliente” usados em implementações de MPLS, para uma arquitetura descentralizada com cargas de trabalho em nuvem. Ele está passando por mudanças dramáticas, impulsionadas pela necessidade de transformação de negócios digitais e a alta demanda de novos produtos e soluções baseadas em *cloud computing* (computação em nuvem) com segurança embarcada.

O quadrante mágico da Gartner (relatório anual, que classifica empresas de tecnologia em quatro principais categorias: os líderes, os desafiantes, os visionários e os competidores de nicho) de 2020 (FOREST; LERNER; SINGH, 2020), destaca os líderes de mercado tecnológico conforme apresentado na Figura 3. Como comparativo neste trabalho serão utilizados os quatro principais *players* do quadrante Líderes (*Leaders*) que são:

- VMware
- Fortinet
- Versa Networks
- Cisco

Figura 3. Quadrante mágico da Gartner de 2020

Fonte: (FOREST; LERNER; SINGH, 2020)

2.6.1 VMware

A VMware é um dos líderes no quadrante mágico apresentado na Figura 3. Seu produto é denominado VMware SD-WAN com tecnologia *VeloCloud,* que inclui principalmente dispositivos SD-WAN, *gateways* e um orquestrador SD-WAN. A VMware está sediada na Califórnia, EUA, e o Gartner Group (empresa de consultoria fundada em 1979 por Gideon Gartner) estima que ela tenha mais de 9.000 clientes SD-WAN. Suas operações são diversificadas geograficamente em uma base global, com clientes em todos os setores e tamanhos.

Pontos Fortes: A VMware tem produtos sólidos, uma base instalada considerável de clientes SD-WAN e um canal global maciço, com fortes recursos financeiros, indicando uma forte viabilidade de mercado no futuro. A VMware tem forte capacidade comprovada de oferecer suporte a clientes de grande escala em 1.000 filiais e mais. Ela avalia o roteiro do fornecedor para fornecer quantidades crescentes de segurança e análises, fortemente alinhadas com as necessidades do cliente (FOREST; LERNER; SINGH, 2020).

Pontos Fracos: O fornecedor tem recursos de segurança nativos limitados, em comparação com alguns outros fornecedores. Isso pode fazer com que os clientes tenham que adquirir, gerenciar e integrar fornecedores de segurança adicionais. A plataforma de gerenciamento de VCO (do inglês *VeloCloud Orchestrator*) desse fornecedor tem várias peças separadas opcionais, incluindo vRNI (do inglês *vRealize Network Insight*) e Nyansa, que podem aumentar a complexidade e os custos. A experiência do cliente da VMware está na faixa média dos fornecedores avaliados nesta pesquisa (FOREST; LERNER; SINGH, 2020).

2.6.2 Fortinet

A Fortinet é líder no Quadrante Mágico da Gartner. Sua oferta é o *Fortinet Secure SD-WAN*, que inclui *hardware* FortiGate e dispositivos virtuais com *software* de rede e segurança (FortiGuard) gerenciado pelo orquestrador no FortiManager. A Fortinet está sediada na Califórnia, EUA, e o Gartner estima que tenha 30.000 clientes periféricos de WAN e mais de 8.000 clientes SD-WAN. Suas operações são globais e atendem a clientes de todos os tamanhos nos setores de varejo, saúde, manufatura, finanças e educação. Espera-se que a Fortinet faça investimentos futuros em SASE (do inglês *Secure Access Service Edge*), AI/ML (do inglês *Artificial Intelligence /Machine Learning*) para solucionar problemas de SD-branch / SD-WAN e orquestração de nuvem/multicloud.

Pontos fortes: Fortinet tem uma das soluções de segurança mais robustas quando combinada com a funcionalidade SD-WAN. O fornecedor continua a melhorar sua presença no

mercado, fechando negócios e expandindo seus canais de atendimento, especialmente com provedores de serviços. Os investimentos contínuos da Fortinet em circuitos integrados específicos de aplicativos (do inglês *Application Specific Integrated Circuits*- ASICs) resultam em um preço competitivo, ao aproveitar o conjunto completo de recursos SD-WAN locais (FOREST; LERNER; SINGH, 2020).

Pontos Fracos: A Fortinet é vista pelo mercado como um fornecedor de segurança e que ainda não tem tanta experiência em arquiteturas complexas em comparação com outros fornecedores listados nesta pesquisa, sua chegada tardia ao mercado de SDN acabou limitando-a a interligar redes do tipo matriz-filial (FOREST; LERNER; SINGH, 2020).

2.6.3 Cisco

A Cisco é um dos líderes neste quadrante mágico. Ela tem uma oferta com a marca Cisco SD-WAN com tecnologia Viptela, que inclui Viptela OS ou *software* IOS XE com orquestração vManage. A outro tecnologia Cisco SD-WAN é desenvolvida pela Meraki, que inclui dispositivos MX e *software* com orquestração. A Cisco Umbrella pode ser implantada opcionalmente para recursos aprimorados de segurança em nuvem. A Cisco está sediada na Califórnia, EUA, e o Gartner estima que tenha mais de 30.000 clientes SD-WAN. Suas operações são globais, com clientes em todos os setores e tamanhos. Espera-se que a Cisco faça investimentos futuros no aprimoramento dos recursos de segurança, melhorando a visibilidade da nuvem e usando ML para otimizar o desempenho.

Pontos fortes: a Cisco tem uma grande base instalada e canais para mercados em todo o mundo, o que lhe dá uma forte capacidade de alcançar clientes e leva à viabilidade de mercado a longo prazo. A Cisco tem um roteiro sólido para fornecer recursos de segurança crescentes de maneira integrada, direcionando para uma arquitetura SASE (do inglês *Secure Access Service Edge*). A Cisco oferece amplitude e profundidade de recursos que atendem a quase todos os cenários de uso e geografias do cliente (FOREST; LERNER; SINGH, 2020).

Pontos Fracos: O portfólio SD-WAN da Cisco inclui partes separadas, que não têm integração total na camada de *software* ou *hardware* e podem levar a proteção limitada do investimento conforme as necessidades mudam ou um requisito para gerenciar várias plataformas se desenvolve. Com base na consulta do cliente, os clientes da Cisco relatam quase o dobro da taxa de preocupações com relação a produtos e preços, em comparação com outros fornecedores. Há uma adoção limitada de implantações de SD-WAN baseadas em IOS-XE (Sistema Operacional da Cisco) em escala para redes com mais de 100 *sites*, em comparação com outros fornecedores (FOREST; LERNER; SINGH, 2020).

2.6.4 Versa Networks:

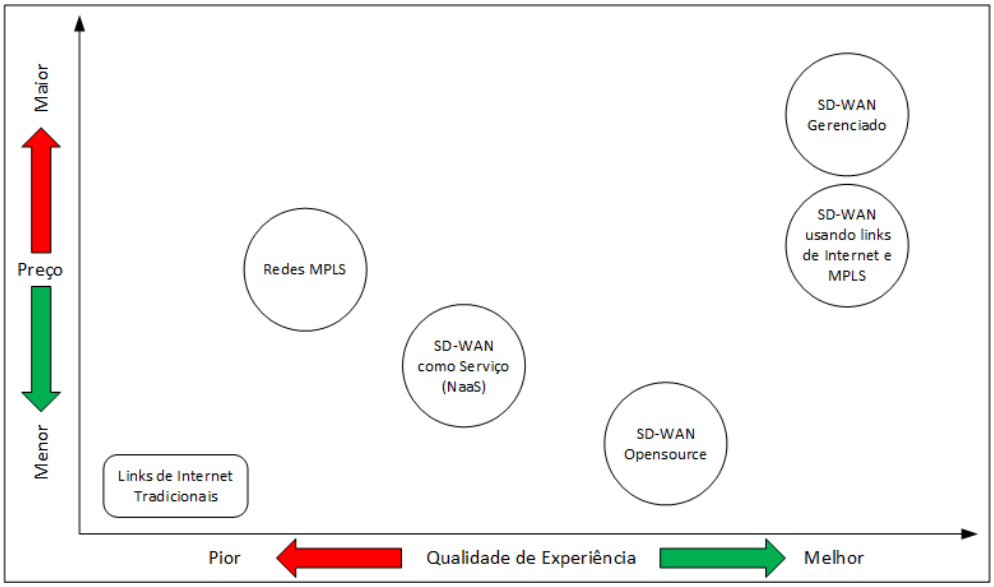
A Versa Networks também é um dos líderes de mercado. Ela tem duas ofertas, com a principal sendo o produto VOS completo (anteriormente Flex VNF), que pode ser entregue como serviço na *Versa Cloud Services Gateways* (CSG) ou *hardware* de terceiros, junto com o *Versa Director* e *Versa Analytics*. A segunda oferta é o *Versa Titan*, uma solução mais simples baseada em nuvem com recursos nativos limitados. A Versa está sediada na Califórnia, EUA, e o Gartner estima que tenha mais de 5.000 clientes de SD-WAN. Ela opera globalmente e atende clientes de todos os tamanhos e setores, principalmente por meio de provedores de serviços.

Pontos fortes: O produto *Versa* VOS oferece uma solução abrangente com fortes recursos de rede, integração de acesso à nuvem e segurança. O serviço *Titan* da Versa oferece uma solução simplificada para MPEs que buscam uma experiência de usuário mais fácil.

Pontos Fracos: O amplo catálogo de produtos da Versa apresenta o risco de não possuir uma qualidade e segurança no código onde foi desenvolvido, o que pode afetar experiência do cliente durante a implementação. De acordo com alguns clientes do Gartner (usuários finais e parceiros de canal), o Versa VOS continua sendo um produto complicado de operar. Como resultado, tem adoção limitada em alguns casos(FOREST; LERNER; SINGH, 2020).

Em resumo, a SD-WAN é uma solução adequada para organizações e empresas que pretendem diminuir seus custos de conectividade e melhorar seu gerenciamento, combinando os *links* de Internet com a tecnologia SDN (LUCIANI, 2019). Deve-se levar em conta que, conforme indicado pela Figura 4, as soluções comerciais possuem qualidade e gerenciamento superiores frente as soluções *opensource*, bem como uma capacidade de pesquisa e desenvolvimento muito à frente das soluções livres, contudo, é preciso mensurar os custos recorrentes das soluções comerciais que podem ser um fator determinante na escolha para projetos de cidades inteligentes, pois, as redes metropolitanas baseadas em IoT tendem a ter um grande número de dispositivos o que pode gerar uma despesa que inviabilize o projeto. Em contrapartida, as soluções SD-WAN baseadas em *software opensource* não possuem custos recorrentes, porém necessitam de profissionais especializados para implementar e manter a solução desenvolvida (LUCIANI, 2019). A Figura 4 ilustra de forma qualitativa o posicionamento de cada tipo de solução SDN avaliando os critérios preço e qualidade de experiência. Observe que a boa relação custo-benefício entre esses dois critérios conflitantes, justifica o desenvolvimento de uma solução SD-WAN *opensource*, como proposto neste trabalho.

Figura 4. Avaliação qualitativa dos critérios para escolha da SD-WAN



Fonte: Adaptado de (LUCIANI, 2019)

2.7 PARÂMETROS PARA ANÁLISE DE QUALIDADE DE SERVIÇO

De acordo com HAFIZ; SUSIANTO (2019), os parâmetros que verificam a qualidade dos serviços de redes também conhecidos como parâmetros de QoS, referem-se à capacidade de uma rede fornecer melhores serviços para um determinado tráfego de rede por meio de tecnologias diferentes através de atributos fornecidos de forma qualitativa ou quantitativa. Nesta dissertação, os parâmetros que foram considerados para avaliar a QoS fornecida pelo dispositivo SD-WAN proposto são listados a seguir:

- **Largura de banda:** É a medida da capacidade de transmissão de uma conexão ou rede em bits por segundo;
- **Vazão:** É o parâmetro que indica a taxa de transmissão efetiva dos dados, medida em bytes por segundo;
- **Perda de pacote:** É um parâmetro que indica a quantidade de pacotes que foram enviados, mas não foram entregues ao destino;
- **Latência:** Indica o tempo que os dados levam para viajar da origem ao destino e é medida em milissegundos (ms);
- ***Jitter*:** Corresponde às variações no atraso de entrega de pacotes de dados em uma rede dentro de um intervalo de tempo, tendo uma relação direta com a demanda de uso da rede.O *jitter* é calculado pelo tempo total em que os dados são enviados menos a latência média, depois dividido pelo total período de tempo em que os dados são enviados. Quanto menor o valor do *jitter*, melhor será a rede.

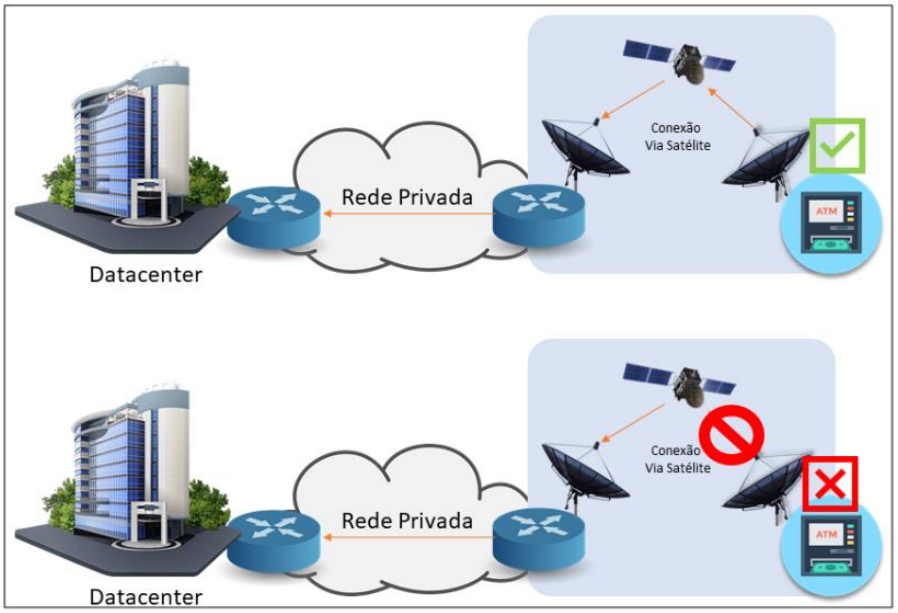
3 REVISÃO BIBLIOGRÁFICA

Este capítulo é dedicado à apresentação e discussão de trabalhos correlatos voltados ao gerenciamento e à utilização da tecnologia SDN. A abordagem centralizada da lógica da rede vem sendo discutida sob diversas óticas considerando cenários variados e sendo empregada para diferentes finalidades. A seguir serão analisados alguns casos de implementação bem-sucedida com abordagem SD-WAN no contexto de cidades inteligentes.

3.1 CONECTIVIDADE PARA CAIXAS ELETRÔNICOS USANDO SD-WAN

Em 25 de agosto de 2017, uma falha no Satélite Telkom 1, causou a desconexão de 8.800 ATMs (do inglês *Automatic Teller Machine*) na Indonésia de suas redes. Existem relatos que o BCA Bank (do inglês *Bank Central Asia*) gastou de cinquenta a setenta bilhões de rúpias, cerca de noventa e três milhões de dólares em moeda atual, para reparar sua rede de ATMs reposicionando suas conexões para outros satélites, mudando para redes de acesso de diferentes tecnologias tais como, fibra óptica e MPLS. Em virtude dessa falha, esses bancos também sofreram perdas financeiras devido à incapacidade de oferecer transações realizadas nos ATMs devido ao desligamento de sua rede de caixas eletrônicos (ANDROMEDA; GUNAWAN, 2020). A Figura 5 ilustra o modelo de conectividade usando apenas satélites como solução primária e como uma falha na conectividade afeta o serviço.

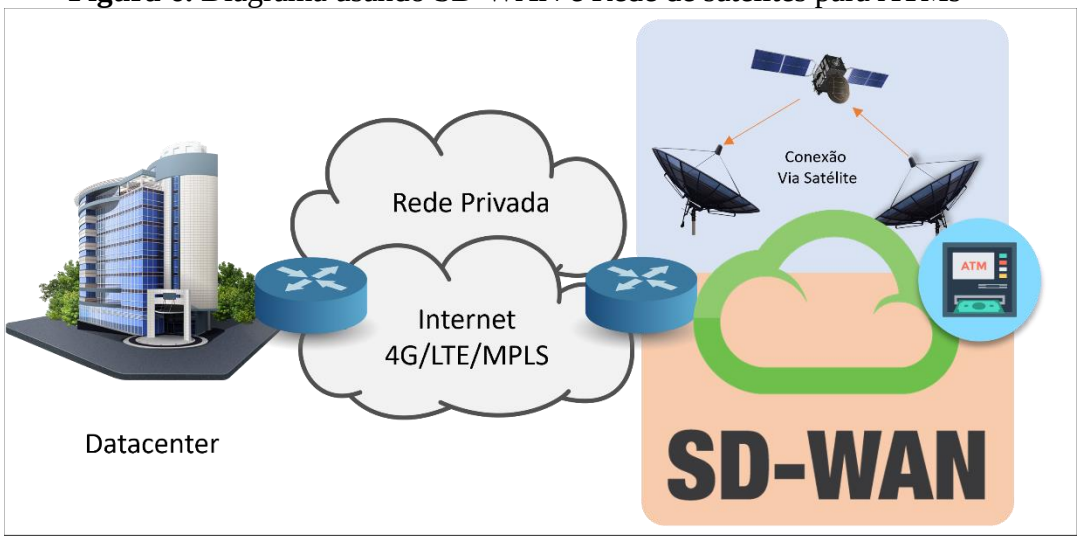
Figura 5. Diagrama de conectividade dos ATMs via Satélite



Fonte: Adaptado de (ANDROMEDA; GUNAWAN, 2020)

Este problema criou uma oportunidade para uma implementação baseada na tecnologia SD-WAN utilizando redes móveis 4G/LTE para fornecer uma conexão redundante para a rede de ATMs. Portanto, os ATMs terão pelo menos duas conexões WAN com sua rede e caso haja descontinuidade em algum dos dois serviços, o tráfego de rede será comutado automaticamente para uma das conexões. A Figura 6 ilustra a interoperação entre as duas tecnologias de conexão conforme relatado no respectivo artigo:

Figura 6. Diagrama usando SD-WAN e Rede de satélites para ATMs



Fonte: Adaptado de (ANDROMEDA; GUNAWAN, 2020)

Nessa arquitetura proposta, a rede SD-WAN, gerencia o comportamento do tráfego e a comutação entre conexões de rede caso haja interrupção em um dos dois serviços. Do ponto de vista técnico, uma conexão redundante para a rede ATM pode ser feita usando a tecnologia SD-WAN com 4G / LTE. Em ANDROMEDA e GUNAWAN (2020), verificou-se que essa solução só poderia ser implantada em áreas urbanas como as ilhas de Java e Bali no momento do estudo devido à limitação da cobertura 4G / LTE. A arquitetura proposta emprega o *link* via satélite como o *link* principal para encaminhar o tráfego e 4G/LTE como um *backup* no estado de espera (sem enviar tráfego). Ou seja, o *link* de dados 4G/LTE é usado apenas se a conexão via satélite estiver inativa ou com baixo desempenho, como em um dia chuvoso por exemplo. Além disso, ele se mantém no modo de espera porque sua velocidade muda em função da quantidade de usuários (não dedicados), bem como para economizar sua franquia de dados. Do ponto de vista econômico, os resultados da análise de viabilidade de investimentos realizados no estudo conduzido por ANDROMEDA e GUNAWAN, (2020) mostraram que os valores investidos e os benefícios percebidos, proporcionaram um rápido retorno de investimento.

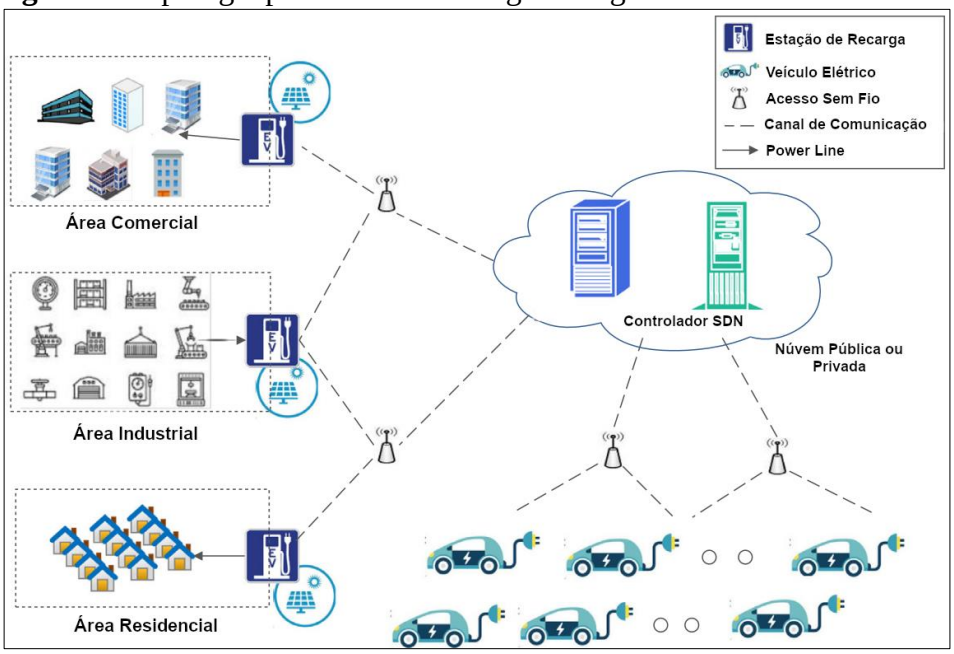
Portanto, com base na análise técnico-econômica, a implementação do SD-WAN com 4G/LTE para fornecer uma conexão redundante para a rede ATM foi considerada viável e rentável.

3.2 COMERCIALIZAÇÃO DE ENERGIA EM SISTEMA DE TRANSPORTE INTELIGENTE USANDO SDN

De acordo com SINGH AUJLA; JINDAL e KUMAR (2018), os setores de transporte e energia passaram por uma grande transformação com a popularização dos veículos elétricos ou EVs (do inglês *Electric Vehicles*). O grande impulso dos EVs no setor de transportes aconteceu por causa de suas múltiplas vantagens, dentre as quais destaca-se a nula emissão direta de combustíveis fosseis. Os EVs formam uma grande rede de energia nas cidades inteligentes, em que cada bateria pode armazenar, transportar e injetar ou consumir energia da rede de tempos em tempos, conforme necessário. Uma rede de energia tão grande, se não for gerenciada de maneira adequada, pode sobrecarregar ainda mais a utilização geral de energia em uma cidade inteligente, no entanto, se manuseado de maneira adequada, pode ser aproveitado para tornar as cidades autossustentáveis.

No entanto, os paradigmas de redes de telecomunicações tradicionais podem ser insuficientes para lidar com as grandes solicitações e volumes de dados gerados pelos componentes e as solicitações de entrada de uma rede de energia tão grande. Portanto, um novo modelo de rede definida por *software* (SDN) tem sido amplamente utilizado pelos pesquisadores para lidar com as solicitações de entrada dos usuários. As entidades associadas como EVs e as estações de recargas também conhecidas como CSs (do inglês *Charging Stations*), estão presentes no plano de dados cujos dados de comunicação são encaminhados para o plano de controle onde as decisões de controle de fluxo são tomadas. A vantagem mais importante em se usar SDN em substituição às redes tradicionais é o fato que a SDN é capaz de alternar convenientemente entre conexões que mudam dinamicamente. Como o controlador é implementado como um pacote de *software* no plano de controle na SDN, ele pode ser programado para lidar com a solicitação de entrada de diferentes maneiras, tornando a rede mais robusta. Na Figura 7, observa-se que tanto os EVs quanto os CSs em toda a cidade estão conectados a um servidor de nuvem central por meio de tecnologias de comunicação, tais como – WI-FI IEEE 802.11 a/b/n/p, LTE, 4G e WiMAX.

Figura 7. Topologia para redes de recarga inteligentes usando SDN



Fonte: (SINGH AUJLA; JINDAL; KUMAR, 2018)

Como os EVs e CSs devem se comunicar uns com os outros, a arquitetura de rede habilitada para SDN subjacente é escolhida para transferir as solicitações de comunicação. Conforme mostrado na Figura 7, o servidor de nuvem tem um controlador SDN o qual gerencia o fluxo de dados de todas as entidades envolvidas (ou seja, EVs e CSs). O gerenciamento da tabela de fluxo agiliza todo o processo de comunicação e torna a rede mais robusta. Além do controlador SDN, o servidor nuvem também contém um controlador de serviço que fornece os serviços de comercialização de energia às entidades envolvidas.

O esquema proposto por SINGH AUJLA; JINDAL e KUMAR (2018) é avaliado usando um estudo de caso com respeito à implantação realista de CSs. Os resultados obtidos mostram que os EVs atuam na dupla função de equilibrar a demanda de energia, aumentando assim o lucro nas duas pontas (EVs e CSs). Finalmente, o impacto do modelo SDN também é analisado em termos de latência, taxa de transferência e utilização da rede. Os resultados obtidos mostram a superioridade do esquema proposto sobre as redes convencionais para fornecer um *backbone* de comunicação robusto.

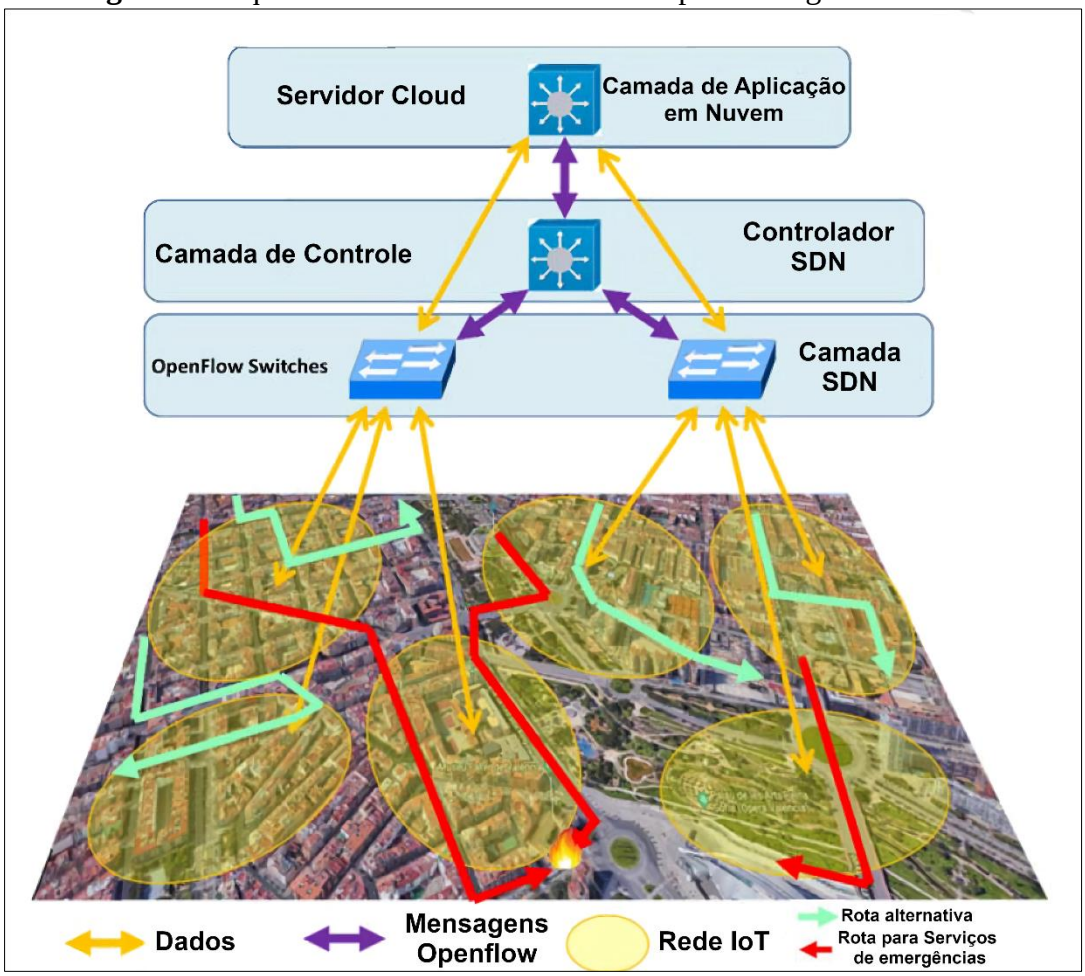
3.3 USANDO SDN EM SITUAÇÕES DE EMERGÊNCIA EM CIDADES INTELIGENTES

De acordo com REGO et al. (2018), incêndios, acidentes, desastres naturais ou ataques terroristas podem ocorrer em qualquer lugar do planeta. Pode ser especialmente desafiador evacuar uma área urbana de maneira eficiente. É importante considerar que o comportamento humano é um aspecto crítico na hora de realizar as evacuações. O estresse e a ansiedade podem afetar os motoristas em situações de emergências, induzindo-os a tomar decisões precipitadas. No entanto, o comportamento humano pode ser racional e as evacuações bem-sucedidas quando se prevê um conjunto de ações a serem seguidas em situações de emergências. A tecnologia pode ser empregada para orientar os motoristas, a fim de garantir sua segurança e uma intervenção mais rápida e eficiente das forças de segurança e equipe médica. Por exemplo, o uso do conceito de SDN em cidades inteligentes permite um controle centralizado e rápido dos sistemas de gestão de tráfego urbano, facilitando a criação de aplicativos inteligentes e melhorando a segurança nas estradas, especialmente em situações de emergência. A implantação do SDN no contexto de cidades inteligentes e particularmente em sistemas de gestão de tráfego urbano, poderia melhorar o desempenho do sistema e facilitar a criação de novas aplicações inteligentes para melhorar a vida das pessoas e aumentar a segurança nas estradas e situações de emergência onde essa arquitetura permite modificar por exemplo, as rotas dos veículos dando instruções aos semáforos inteligentes implantados em toda a cidade. Esses semáforos são capazes de coordenar entre si e modificar a duração de suas luzes verdes, amarelas e vermelhas. Um sistema todo baseado em redes IoT, pode orquestrar todos os recursos necessários em caso de emergência e desviar o trânsito para rotas menos movimentadas, assim, liberando espaço para equipes de intervenção e emergência alcançarem as pessoas que necessitam de apoio. Considerando os benefícios de empregar a SDN em cidades inteligentes e a gestão de tráfego urbano, investir no desenvolvimento de soluções baseadas em SDN para cidades inteligentes é importante para que as pesquisas se beneficiem de todo potencial que esse tipo de rede (baseada em *software*) tem a oferecer.

A Figura 8 ilustra a topologia utilizada neste estudo, onde as rotas de trânsito são modificadas baseadas nos dados coletados por sensores IoT, promovendo assim, uma rota alternativa para o fluxo de trânsito e criando uma rota para serviços de emergências. Esta aplicação usando SDN, tem a adaptabilidade para encaminhar o tráfego urbano utilizando semáforos inteligentes e outros elementos de tráfego que estejam conectados às redes IoT. O controlador SDN se comunica com serviços de nuvem e locais remotos para coletar os dados necessários e fazer as melhores mudanças para gerenciar as emergências. Este modelo também

pode integrar sensores para monitorar a poluição do ar com o intuito de modificar o trânsito de grandes áreas diminuindo a poluição em grandes centros urbanos.

Figura 8. Arquitetura do cenário usando SDN para emergências.



Fonte: (REGO et al., 2018)

4 METODOLOGIA

Esta seção apresenta de maneira sistemática quais caminhos foram percorridos para se alcançar os objetivos propostos. A seguir será realizada uma caracterização da pesquisa desenvolvida sob as óticas de natureza e objetivos, destacando-se os procedimentos técnicos que foram seguidos e a metodologia empregada.

Do ponto de vista de natureza, este trabalho se enquadra na categoria de pesquisa aplicada, ou seja, uma pesquisa cujos objetivos são gerar conhecimentos para aplicação prática dirigidos à solução de um problema específico (SILVA; MENEZES, 2000).

Do ponto de vista de objetivos, esta dissertação pode ser categorizada como uma pesquisa exploratória (GIL, 2018), pois visa proporcionar maior familiaridade com o problema do uso da tecnologia SD-WAN em cidades inteligentes. Nesse sentido, este trabalho envolve levantamento bibliográfico e assume a forma geral de um estudo de caso para abordar o problema.

Para realizar essa dissertação foram utilizados os seguintes procedimentos técnicos (GIL, 2018):

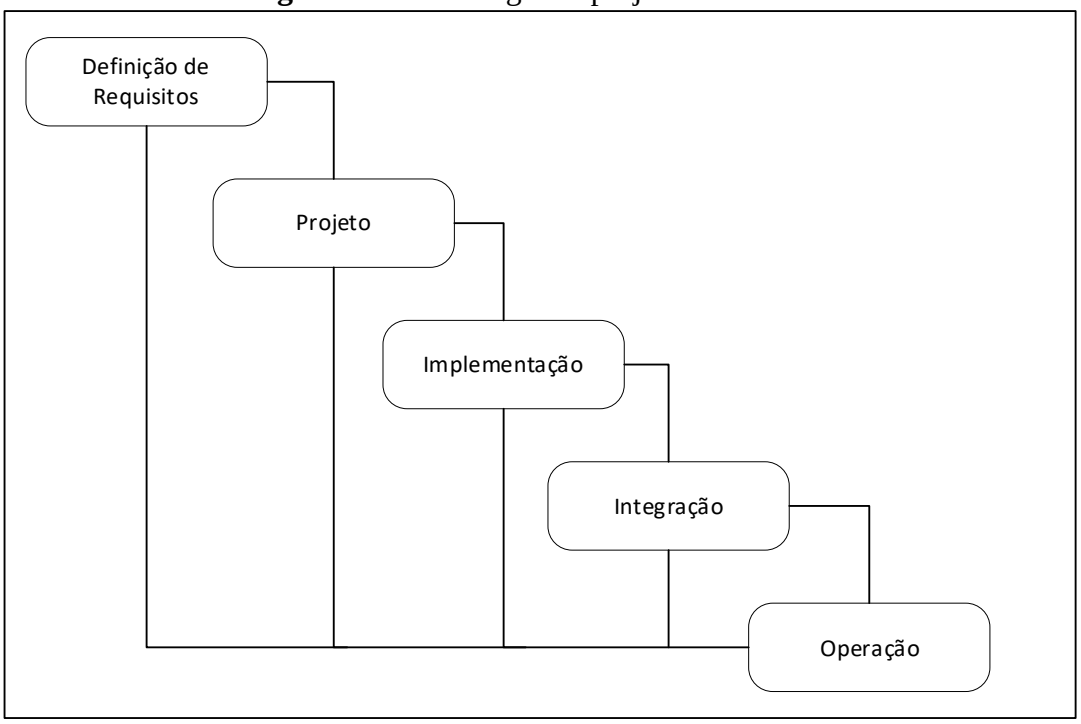
- Pesquisa bibliográfica elaborada a partir de livros, artigos de periódicos e materiais disponibilizados na Internet para dar fundamentação teórica ao tema investigado;
- Pesquisa experimental, em que se determina um objeto de estudo, selecionam-se as variáveis que são capazes de influenciá-lo, define-se as formas de controle e observação dos efeitos que a variável produz no objeto;
- Estudo de caso, pois envolve o estudo profundo e exaustivo de um objeto de maneira que se permita seu amplo e detalhado conhecimento.

Este trabalho foi realizado com a metodologia em cascata, de acordo com SOMMERVILLE (2011). O modelo em cascata é um exemplo de processo dirigido a planos, ou seja, deve-se planejar e programar todas as atividades do processo antes de começar a trabalhar nelas (SOMMERVILLE, 2011). Essa metodologia possui as seguintes partes e características destacadas na Figura 9.

- **Definição de Requisitos**: é realizada uma análise das necessidades e requisitos para considerar as características que o protótipo terá;
- **Projeto**: será proposto um projeto que atenda aos requisitos listados na etapa anterior;

- **Implementação**: dá prosseguimento à implementação do protótipo com base no desenho da etapa anterior;
- **Integração**: as unidades individuais de programa são integradas para garantir que os requisitos sejam atendidos;
- **Operação**: concluída as fases de implementação e integração, são realizados testes para verificar se os objetivos do protótipo foram alcançados.

Figura 9. Metodologia de projeto em cascata



Fonte: (SOMMERVILLE, 2011)

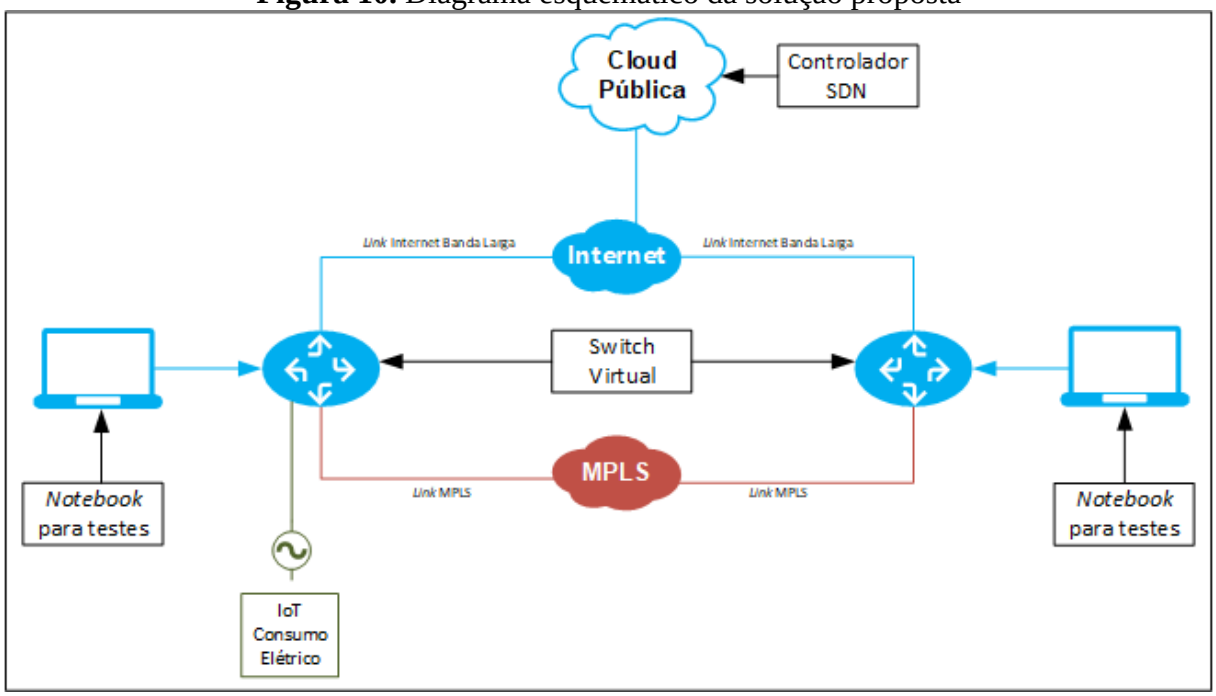
4.1 PROPOSTA DE UM DISPOSITIVO SD-WAN

Neste item foram avaliados os componentes necessários referentes ao *hardware* e *software*, bem como a descrição do experimento que irá validar as funcionalidades necessárias para o correto funcionamento do dispositivo. Os componentes para o desenvolvimento do protótipo e a avaliação de desempenho foram listados abaixo:

- *Hardware* de baixo custo com 3 placas de rede
- *Software* controlador SDN *opensource*
- *Software* para *switch* virtual *opensource* com suporte ao protocolo Openflow
- Serviço de Nuvem Pública
- Sistema Operacional para o protótipo
- IoT para medição do consumo elétrico
- *Link* de dados MPLS
- *Link* de dados Internet Banda Larga
- Dois *notebooks* para os testes de desempenho

O diagrama esquemático apresentado na Figura 10, ilustra a proposta para a solução do problema.

Figura 10. Diagrama esquemático da solução proposta



Fonte: Autoria própria

4.2 DESCRIÇÃO DO *SOFTWARE*

4.2.1 Floodlight

O controlador Floodlight (FLOODLIGHT, 2016), usado neste projeto, é um controlador SDN popular para uso acadêmico que possui licença Apache, e pode ser executado em plataforma Java, é modular e projetado para ter bom desempenho (ALENCAR et al., 2014). Por ser modular, este controlador suporta uma série de aprimoramentos e subsídios para sua extensão, além de ser bastante flexível e facilitar o desenvolvimento de novas aplicações SDN (MORALES et al., 2016).

O projeto do Floodlight usou como base o Beacon, que foi um dos primeiros controladores SDN a habilitar programadores iniciantes a utilizarem ambientes SDN em maior escala. Atualmente possui suporte de uma comunidade de desenvolvedores e recebe incentivos de uma *startup* que desenvolve produtos comerciais compatíveis, a The Big Switch Networks (ALENCAR et al., 2014). Por ser desenvolvido em Java, o controlador Floodlight suporta várias plataformas de sistemas operacionais, possui um bom gerenciamento de memória, e oferece suporte a múltiplos *threads*. Suporta uma variedade de comutadores físicos e virtuais, facilitando o desenvolvimento de experimentos e agilizando o desenvolvimento e módulos auxiliares em ambientes virtuais (MORALES; et al. 2016). Empregou-se o controlador Floodlight neste trabalho devido ao suporte e documentação disponível, facilidade de instalação e configuração, desempenho e portabilidade.

Uma pesquisa realizada em LAISSAOUI et al. (2016) compara os quatro mais populares controladores SDN de código aberto e conclui que, de maneira geral, Floodlight é melhor que o Beacon, Pox e Ryu em uma rede SDN com suporte a OpenFlow versão 1.0, o que reforça a escolha de Floodlight. De acordo com SALMAN et al. (2016), o Floodlight é uma boa escolha como um controlador SDN completo. Possui suporte a uma variedade de aplicações e oferece uma chance real de se tornar um supercontrolador. Sua integração com vários tipos de dispositivos IoT e novas SI específicas para IoT, o torna o primeiro candidato na eleição do controlador da “Internet do futuro”.

A Tabela 1 faz um comparativo entre vários candidatos a controlador SDN, onde são avaliados os seguintes requisitos:

Linguagem de Programação: O primeiro critério avaliado para escolha de um controlador SDN é a linguagem de desenvolvimento segundo a qual foi concebido, basicamente porque afeta o desempenho do controlador e a velocidade de desenvolvimento. As linguagens, Java, Python e C++ são as linguagens mais comuns para programação de controladores SDN. Em geral, os controladores codificados em Java têm a característica de rodar em plataformas diversas e apresentam boa modularidade. Os controladores codificados em C fornecem alto desempenho, mas necessitam de alta modularidade, bom gerenciamento de memória e boa GUI (interface gráfica do usuário, do inglês *Graphical User Interface*). Finalmente, os controladores SDN codificados em Python carecem de manipulação multitarefa real, o que em muitos casos se torna complexo e caro.

Interface Gráfica: O segundo critério diz respeito a interface de gerenciamento gráfico do controlador, fundamental para a operação eficiente do controlador SDN. Neste contexto, as interfaces baseadas em Web (do inglês *Web-Based*) são reconhecidamente as mais completas e fáceis de implementar que outras interfaces.

Documentação: O terceiro critério está relacionado à documentação disponível. Normalmente a qualidade da documentação está relacionada a quantidade de parceiros que o projeto possui.

Modularidade: O quarto critério é o quão modular é o *software* do controlador SDN. Quando, eventualmente, o controlador tem um baixo nível de modularidade, sua construção, manutenção e extensão são dificultadas e o controlador se torna tão resistente a novas inovações quanto as redes tradicionais definidas por *hardware*.

Arquitetura Distribuída ou Centralizada: Esse critério define o tipo de arquitetura que a solução usa.

Suporte a Plataformas: Critério que avalia quais plataformas são compatíveis com o controlador SDN.

Tabela 1. Comparativo entre as soluções de controladores SDN

Controlador SDN	Linguagem de programação	Interface Gráfica	Documentação	Modularidade	Distribuída ou Centralizada	Suporte a plataformas	Northbound APIs	OpenStack Support	Southbound APIs
OpenDayLight	Java	Web Based	Muito Boa	Alta	D	Linux, MAC OS e Windows	REST API	Sim	OF1.0, 1.3, 1.4, NETCONF/ YANG, VSDB, PCEP, BGP/LS, LISP, SNMP
ONOS	Java	Web Based	Boa	Alta	D	Linux, MAC OS Windows	REST API	Não	OF1.0,1.3, NETCONF
NOX	C++	Python + QT4	Ruim	Baixa	C	Linux	REST API	Não	OF 1.0
POX	Python	Python + QT4	Ruim	Baixa	C	Linux, MAC OS Windows	REST API	Não	OF 1.0
RYU	Python	Web Based	Ruim	Baixa	C	Linux	REST API	Sim	OF 1.0, 1.2, 1.3,1.4, NETCONF, OFCONFIG
Beacon	Java	Web Based	Ruim	Média	C	Linux, MAC OS Windows	REST API	Não	OF 1.0
Maestro	Java	-	Ruim	Baixa	C	Linux, MAC OS Windows	REST API	Não	OF 1.0
Floodlight	Java	Web/Java Based	Muito Boa	Alta	D	Linux, MAC OS Windows	REST API	Sim	OF 1.0, 1.3

Fonte: Adaptado de(SALMAN et al., 2016).

4.2.2 OpenvSwitch

O OpenvSwitch é um *switch* baseado em *software* de código aberto, que visa implementar uma plataforma de *switch* de nível de produção que oferece suporte a interfaces de gerenciamento padrão e permite funções de encaminhamento e controle por meio da programação. Este *software* funciona como um *switch* virtual expondo visibilidade padrão e interfaces de controle para a camada de rede virtual. OpenvSwitch é compatível com sistemas Linux e é desenvolvido na linguagem de programação C, o que lhe dá independência da plataforma onde se deseja utilizá-lo. A versão mais atual é compatível com as seguintes funções:

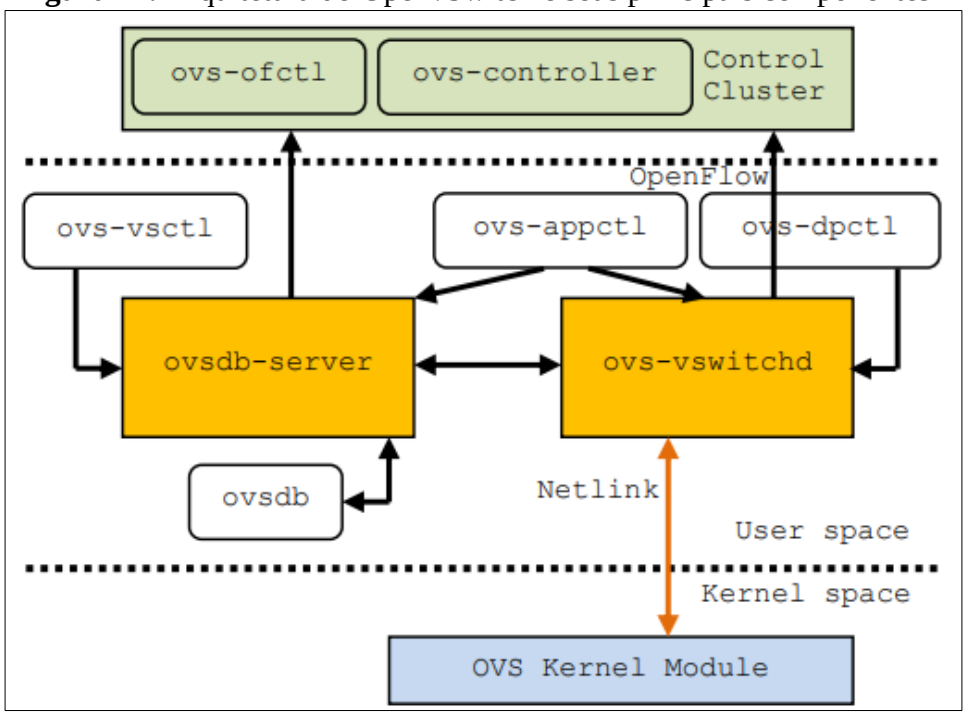
- VLAN (rede local virtual, do inglês *Virtual Local Area Network*) padrão IEEE 802.1q com portas de tronco e acesso;
- Ligação NIC (do inglês *Network Interface Card)* com ou sem LACP (do inglês *Link Aggregation Control Protocol*) no *switch upstream*;
- NetFlow, sFlow e espelhamento para maior visibilidade;
- Configuração de QoS para maior vigilância;
- Túneis GRE, VXLAN, STT e LISP;
- Gerenciamento de falha de conectividade 802.1ag;
- OpenFlow 1.0 mais numerosas extensões;
- Banco de dados transacional com ligações e Python;
- O módulo de kernel Linux incluído é compatível com Linux 3.10 e superior.

Para este projeto, o pacote OpenvSwitch, permitirá o acesso ao protocolo OpenFlow que está integrado nele, de forma a poder realizar a interação entre o *host* que contém o *switch* virtual e o controlador SDN. A utilização deste pacote oferece vantagens como a execução de comandos que implicam no controle do *switch*, refletindo os eventos gerados por esses comandos no controlador, podendo realizar a administração local do dispositivo (LINUX FOUNDATION, 2016). A arquitetura do OpenvSwitch é organizada pelos módulos estruturados de acordo com a Figura 11 e descritos a seguir:

- **ovsdb-server:** é um banco de dados que armazena as configurações de *switch* e as definições das pontes (*bridges*), interfaces e tunelamentos de rede, assim como os endereços do OVSDB (do Inglês *OpenvSwitch Database Management Protocol*) e do controlador SDN.

- **ovs-vswitchd:** é o módulo que executa o *switch* de fato, em conjunto com o módulo de *kernel* para encaminhamentos baseados em fluxos. É configurado pelo utilitário ovs-vsctl e fornece comunicação com os controladores através de interfaces que utilizam o protocolo OpenFlow, além de se conectar ao OVSDB através do ovsdb-server e ao módulo do Kernel por meio de uma conexão de rede;
- **ovs-vsctl:** utilitário utilizado para consultar e alterar as configurações do ovs-vswitchd, sendo uma interface de alto nível para o banco de dados de configurações (ovsdb-server), de onde obtém as informações de configuração;
- **ovs-appctl:** aplicativo que submete comandos para *daemons* do *OpenvSwitch* que estão sendo executados no ambiente;
- **ovs-ofctl:** utilitário utilizado para consultar e controlar os *switches* e controladores OpenFlow;
- **ovs-dpctl:** ferramenta específica para configurar o módulo de *kernel* do *switch* OpenFlow;
- **OVS Kernel Module:** módulo de *kernel* do OVS (do inglês *OpenvSwitch*) capaz de estabelecer uma comunicação eficaz entre o *hardware* e os recursos de sistema em *software*.

Figura 11. Arquitetura do OpenvSwitch e seus principais componentes

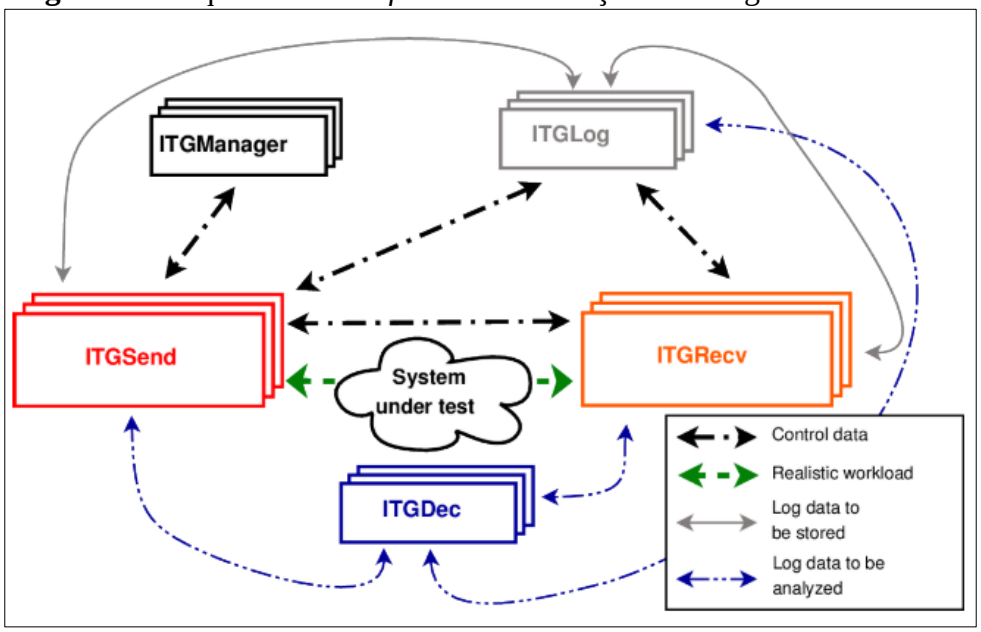


Fonte: Adaptado de (ANAN et al., 2016)

4.3 D-ITG (DISTRIBUTED INTERNET TRAFFIC GENERATOR)

O D-ITG (do *inglês Distributed Internet Traffic Generator*) é uma plataforma capaz de produzir tráfego IPv4 e IPv6 replicando com precisão a carga de trabalho das aplicações atuais da Internet e redes IP. Ao mesmo tempo, o D-ITG também é uma ferramenta de medição de rede capaz de medir as métricas de desempenho mais comuns (por exemplo, taxa de transferência, atraso, *jitter*, perda de pacote) no nível do pacote. D-ITG pode gerar tráfego seguindo modelos estocásticos para tamanho de pacote e tempo que imitam o comportamento do protocolo no nível do aplicativo. Ao especificar as distribuições de variáveis é possível escolher diferentes processos de geração de pacotes onde o D-ITG é capaz de replicar propriedades estatísticas de tráfego de diferentes aplicações bem conhecidas (por exemplo, Telnet, VoIP - G.711, G.723, G.729, detecção de atividade de voz, RTP (do *inglês Real-Time Transport Protocol*) compactado - DNS, jogos de rede). Na camada de transporte, o D-ITG atualmente suporta TCP (Protocolo de Controle de Transmissão do inglês *Transmission Control Protocol*), UDP (do inglês *User Datagram Protocol*) (BOTTA et al., 2019). A Figura 12 mostra como funciona a arquitetura do *software* D-ITG.

Figura 12. Arquitetura do *software* de emulação de tráfego I-DTG



Fonte: Adaptado de (BOTTA et al., 2019)

Os principais componentes do D-ITG são:

- ITGSend: é responsável por gerar fluxos de tráfego e pode funcionar através de um fluxo simples de dados (*single flow*) ou múltiplos fluxos (*multi flow*).
- ITGRecv: é responsável por receber múltiplos fluxos de tráfego paralelos gerados por uma ou mais instâncias IT-GSend. Através deste componente é gerada a saída com os dados a serem analisados posteriormente.
- ITGDec: é responsável por decodificar e analisar os arquivos de log armazenados durante os experimentos conduzidos usando o D-ITG.

Neste trabalho o D-ITG fará o papel de simulador de tráfego de banda afim de aferir a capacidade de entrega do dispositivo tanto pelo *link* de Internet banda larga quanto pelo *link* MPLS e no final dos testes apresentará graficamente os resultados obtidos. A Figura 13 a seguir, apresenta uma amostra de um teste executado com o *software* D-ITG e os parâmetros analisados.

Figura 13. Amostra dos resultados do teste com D-ITG

```
root@desktop-lab01:/home/desktop# ITGDec send_log_file
ITGDec version 2.8.1 (r1023)
Compile-time options: sctp dccp bursty multiport
/------------------------------------------------------------
Flow number: 1
From 192.168.100.1:36553
To    192.168.100.2:9501
------------------------------------------------------------
Total time                =     9.999625 s
Total packets             =         9216
Minimum delay             =     0.000000 s
Maximum delay             =     0.000000 s
Average delay             =     0.000000 s
Average jitter            =     0.000000 s
Delay standard deviation  =     0.000000 s
Bytes received            =      6891689
Average bitrate           =   5513.557958 Kbit/s
Average packet rate       =    921.634561 pkt/s
Packets dropped           =             0 (0.00 %)
Average loss-burst size   =     0.000000 pkt
------------------------------------------------------------


**********  TOTAL RESULTS   ******************
```

Fonte: Autoria Própria

4.3.1 Ubuntu Server

Ubuntu é um sistema operacional de código aberto, baseado no sistema operacional Debian GNU / Linux. Ubuntu é um sistema operacional adequado para projetos de IoT usando Raspberry Pi. Assim, espera-se desenvolver um dispositivo para redes SD-WAN sem custos com *software* licenciados e que seja eficiente para a proposta deste trabalho.

4.3.2 Amazon Web Services (AWS)

Antes de comentar a respeito da plataforma Amazon Web Services, faz-se necessário apresentar uma definição formal para o conceito de computação em nuvem (do inglês *cloud computing*). A computação em nuvem é a entrega de recursos de TI sob demanda por meio da Internet com definição de preço de pagamento conforme o uso. Isso significa que, ao contrário de comprar, possuir e manter *datacenters* ou servidores físicos, um indivíduo ou empresa pode acessar serviços de tecnologia como capacidade de computação, armazenamento e bancos de dados conforme sua necessidade a partir de um provedor de nuvem.

A AWS (do inglês *Amazon Web Services*) é uma das plataformas de computação em nuvem mais utilizadas mundialmente e possui um conjunto diversificado de serviços. Os serviços da AWS são oferecidos em diferentes formas e formatos, desde tecnologias de infraestrutura como computação, armazenamento e bancos de dados até tecnologias emergentes, como *machine learning* e inteligência artificial, *data lakes*, análise de dados e IoT. Graças ao modelo de pagamento conforme o uso, o usuário pode experimentar diferentes tecnologias até encontrar aquela que se adapta às suas necessidades e diminuir seu tempo de chegada ao mercado. Dessa maneira, as *startups* concluem a criação de seus produtos e recursos mais rapidamente, mantendo o custo mínimo.

A AWS fornece como serviço a possibilidade de utilizar máquinas virtuais com capacidade de processamento e armazenamento ilimitados que, em teoria, suporta todos os tipos e tamanhos de projetos de virtualização. Para este trabalho foi utilizado o serviço de máquina virtual denominado EC2 (do inglês *Elastic Computing*) na versão gratuita do serviço, conforme descrito pela Tabela 2.

Tabela 2. Serviço de Máquinas virtuais AWS EC2

Família	Tipo	vCPUs	Memória (GB)	Desempenho de Rede	IPv6
t2	t2 nano	1	0.5	Baixo	Sim
t2	t2 micro	1	1	Baixo	Sim

Fonte: Autoria Própria

4.4 DESCRIÇÃO DO HARDWARE

4.4.1 Raspberry Pi

Raspberry Pi (RASPBERRY PI FOUNDATION, 2014) é um nano computador composto por um cartão eletrônico do tamanho de um cartão de crédito, ao qual pode ser conectado um monitor, um *mouse* e um teclado. É uma plataforma que permite que os usuários explorem a ciência da computação e aprendam linguagens como *Scratch* e *Python*. Tem a capacidade de realizar tarefas como um computador *desktop*, navegar na Internet, reproduzir vídeos, fazer planilhas, processamento de texto e jogos. O Raspberry Pi tem uma grande capacidade de interagir com o mundo exterior e pode ser usado em uma ampla gama de projetos.

Neste projeto, o Raspberry Pi terá um papel fundamental, uma vez que sua função é ser um *switch* de rede SDN, utilizando OpenvSwitch, que fornece a capacidade de virtualizar um *switch* que integra o protocolo OpenFlow, o que permite a interação entre controladores SDN, permitindo que altere o controle dos dados que são gerenciados neste dispositivo por meio de regras que são executadas no controlador centralizado. Tendo em vista que o Raspberry Pi pode utilizar diferentes sistemas operacionais, neste projeto optou-se por utilizar o Ubuntu *Server*, que é o sistema operacional largamente utilizado no mundo todo e possui interoperabilidade com Raspberry Pi, o que permite executar comandos para interagir entre o *switch* virtual, o sistema operacional e o controlador SDN. Apesar de existirem várias versões do Raspberry Pi no mercado, este projeto concentra-se nos modelos “B”, pela facilidade e disponibilidade do equipamento para os testes detalhados na Tabela 3.

Tabela 3. Comparativo de modelos de hardware Raspberry Pi

Produto	SoC (*System on a chip*)	Velocidade	RAM	Portas USB	Ethernet	Wireless	Bluetooth
Raspberry Pi Model A+	BCM2835	700MHz	512MB	1	Não	Não	Não
Raspberry Pi Model B+	BCM2835	700MHz	512MB	4	100Base-T	Não	Não
Raspberry Pi 2 Model B	BCM2836/7	900MHz	1GB	4	100Base-T	Não	Não
Raspberry Pi 3 Model B	BCM2837A0/B0	1200MHz	1GB	4	100Base-T	802.11n	4.1
Raspberry Pi 3 Model A+	BCM2837B0	1400MHz	512MB	1	Não	802.11ac/n	4.2
Raspberry Pi 3 Model B+	BCM2837B0	1400MHz	1GB	4	1000Base-T	802.11ac/n	4.2
Raspberry Pi 4 Model B	BCM2711	1500MHz	2GB	2xUSB2, 2xUSB3	1000Base-T	802.11ac/n	5.0
Raspberry Pi 4 Model B	BCM2711	1500MHz	4GB	2xUSB2, 2xUSB3	1000Base-T	802.11ac/n	5.0
Raspberry Pi 4 Model B	BCM2711	1500MHz	8GB	2xUSB2, 2xUSB3	1000Base-T	802.11ac/n	5.0
Raspberry Pi Zero	BCM2835	1000MHz	512MB	1	Não	Não	No
Raspberry Pi Zero W	BCM2835	1000MHz	512MB	1	Não	802.11n	4.1
Raspberry Pi Zero WH	BCM2835	1000MHz	512MB	1	Não	802.11n	4.1
Raspberry Pi 400	BCM2711	1800MHz	4GB	1xUSB2, 2xUSB3	1000Base-T	802.11ac/n	5.0

Fonte: Adaptado de (RASPBERRY PI FOUNDATION, 2014)

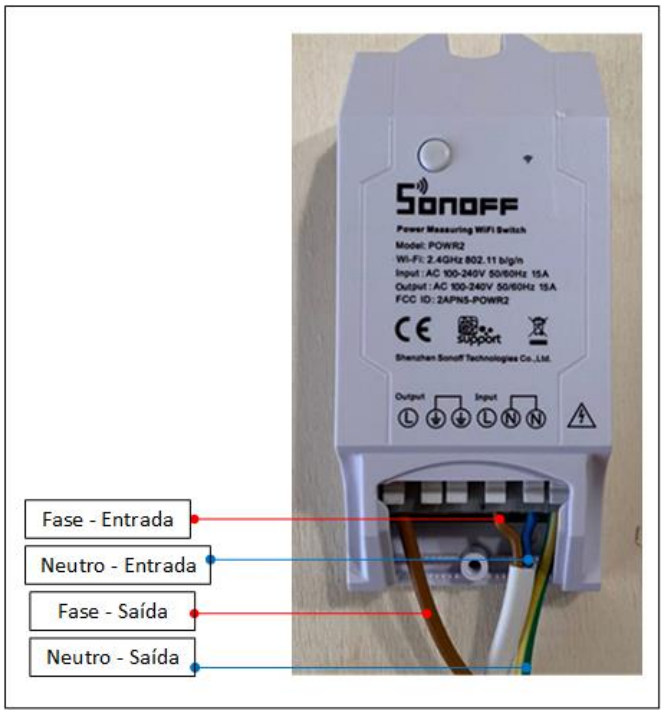
4.4.2 Sonoff Pow R2

O Sonoff Pow R2 é um dispositivo IoT para monitoração de consumo elétrico inteligente com conectividade WI-FI que permite gerenciar, monitorar e controlar remotamente os dispositivos acoplados a ele (TOKOH, 2018). A seguir são apresentadas as características técnicas relacionadas ao dispositivo:

- Faixa de tensão: 100-240 V AC;
- Corrente máxima: 15A;
- Potência máxima: 3500W;
- Dimensões do produto: 114 x 52 x 32 mm;
- Frequência sem fio: 802.11 b / g / n;
- Mecanismo de segurança: WPA-PSK / WPA2-PSK;
- Material do invólucro: ABS V0 ignífugo;
- Temperatura de operação: 0ºC-40ºC (32 ° F-104 ° F);
- Umidade operacional: 5% -90% UR, sem condensação;
- Peso: 91,0g.

A Figura 14 ilustra a modelo de ligação do dispositivo Sonoff Pow R2 usado para monitorar o consumo elétrico do protótipo.

Figura 14. Ilustração do modelo de ligação do Sonoff Pow R2

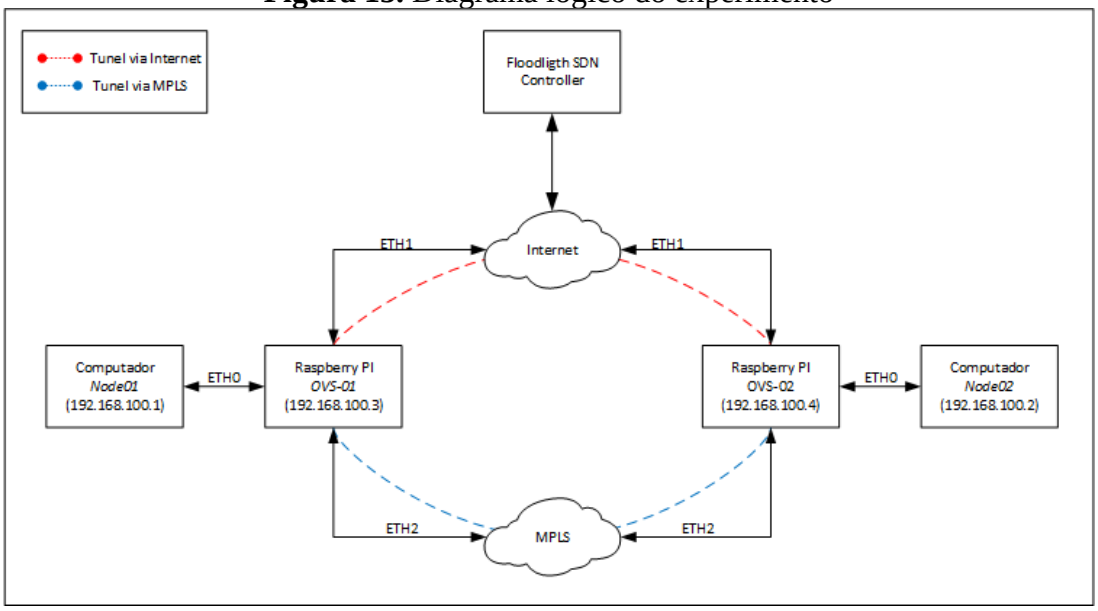


Fonte: Adaptado de (TOKOH, 2018)

4.5 DESCRIÇÃO DA MONTAGEM EXPERIMENTAL

Nesta seção descreve-se como foi realizada a montagem experimental que permitiu a realização de testes no protótipo para posterior validação do mesmo. Foram executados testes de conectividade e funcionalidades usando dois computadores aqui descritos como *Node01* e *Node02* para a geração do tráfego IP a fim de aferir o funcionamento do protótipo aqui dividido em dois dispositivos Raspberry PI nomeados OVS-01 e OVS-02 e verificar se os requisitos descritos nos objetivos deste trabalho estavam aderentes. Para isso foi usado o *software* I-DTG capaz de gerar um tráfego IP considerando dois diferentes cenários. No primeiro, usando um *link* de conectividade MPLS e no segundo cenário usando um *link* de Internet banda larga. A Figura 15 a seguir, ilustra a topologia desenhada para a execução dos testes

Figura 15. Diagrama lógico do experimento



Fonte: Autoria Própria.

O pacote OpenvSwitch foi instalado nos dispositivos Raspberry PI, os quais são conectados com dois túneis de serviço entre si e conectados ao controlador Floodlight que foi configurando em uma máquina virtual na AWS. Todas as conexões são configuradas com túneis do tipo GRE (do inglês *Generic Routing Encapsulation*) com o intuito de garantir a segurança dos dados que trafegam por eles. Conforme mencionado anteriormente, há duas conexões fornecidas por diferentes tecnologias, uma conexão do tipo Internet banda larga e uma conexão por *link* privado MPLS ponto a ponto, conforme ilustrado pelo diagrama da Figura 14.

4.6 CUSTOS DE CONECTIVIDADE

No que diz respeito aos custos de conectividade, é possível observar uma redução expressiva nos valores utilizando tecnologias de Internet banda larga frente aos serviços MPLS. Em uma pesquisa realizada com um grande *player* de conectividade corporativa no Brasil (EMBRATEL, 2020), obteve-se uma estimativa de preços médios de *links* de Internet banda larga versus *links* MPLS. A Tabela 4 compara os custos em reais e dólares (taxa PTAX em 2020 igual a R$ 5,15) relacionados dos dois serviços com capacidades semelhantes. Nesta tabela é possível observar de maneira quantitativa um dos principais motivadores do emprego da tecnologia SD-WAN. Em comparação com as WANs tradicionais, as SD-WANs podem levar a economias substanciais, por meio de uma melhor utilização de suas conexões, por exemplo, permitindo que um tráfego menos crítico possa ser fornecido pelo *link* mais barato (ilustrado na tabela pelo serviço de Internet banda larga).

Tabela 4. Comparativo de valor entre serviço banda larga versus MPLS

Serviço	Capacidade	Valor Mensal em Reais	Valor Mensal em Dólares
Serviço de Internet Banda Larga	100Mbps simétrico	R$ 1.496,00	U$ 290,00
Serviço de Conectividade MPLS	100Mbps simétrico	R$ 5.959,00	U$ 1.157,00

Fonte: (EMBRATEL, 2020)

4.7 EFICIÊNCIA ENERGÉTICA

Atualmente, uma das características importantes que devem ser levadas em consideração ao realizar a substituição de alguma tecnologia ou dispositivo tecnológico é garantir o uso racional de energia. Nesse sentido, a atualização deve ser feita de maneira a garantir que o novo dispositivo seja eficiente energeticamente, ou seja, possua habilidade de realizar as mesmas funções ou até mais com uma quantidade menor de recursos energéticos. Com isso em mente, a Tabela 5 compara a potência elétrica em watts (W) entre os principais fabricantes de *edge-gateway* disponíveis no mercado. Além do consumo elétrico do protótipo, que será avaliado em maiores detalhes no capítulo seguinte, é importante comparar as características elétricas nominais do *hardware*

utilizado no protótipo proposto (baseado em Raspberry PI) e os *hardwares* disponíveis no mercado que apresentam funções similares ao protótipo SD-WAN desenvolvido neste trabalho.

Tabela 5 - Comparativo de características elétricas entre *edge-gateways*

Fabricante	Potência (Watts)
Raspberry PI 3	3.7
VMWareVelocloudEdge 510	45
Cisco vEdge-100:	28
Fortinet FG40F	16,6

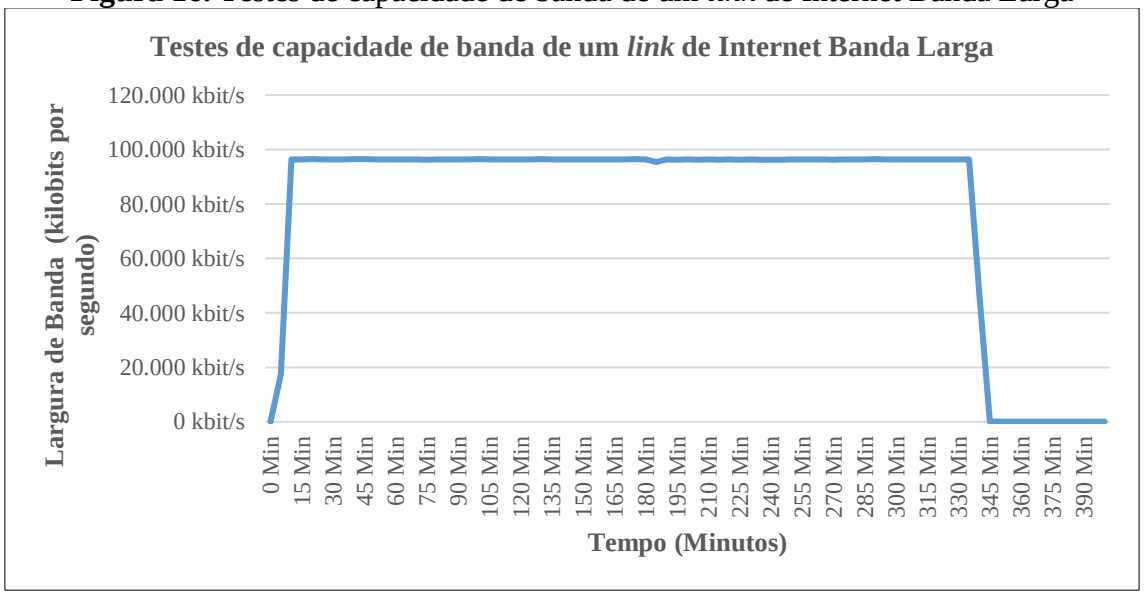
Fontes: (“Power Consumption Benchmarks | Raspberry Pi Dramble”, [s.d.]), (“Cisco SD-WAN vEdge Routers”, 2020), (FORTINET, 2021), (TRADELENS, 2019), (VMWARE, 2020)

5 RESULTADOS

5.1 TESTES DE LARGURA DE BANDA

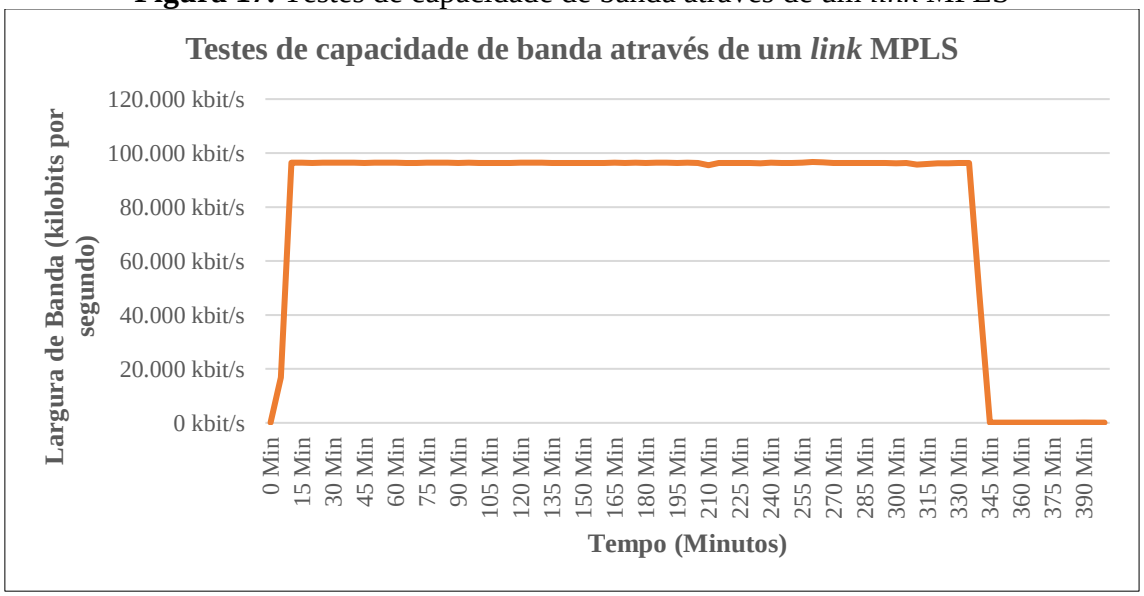
A largura de banda (do inglês *bandwidth*) é a medida da capacidade de transmissão de um determinado meio, conexão ou rede, ou seja, é ela que determina a quantidade de dados que podem ser transmitidos através da rede em um período fixo, sendo medida em *bits* por segundo e suas variações (kbps, Mbps, etc.). Certos serviços demandam maior largura de banda para funcionar (como, por exemplo, aplicações de multimídia e videoconferência). As demandas por largura de banda, em especial em cidades inteligentes, estão aumentando cada vez mais, sobrecarregando as empresas e cidades que estão sujeitas a contratos inflexíveis de largura de banda de MPLS. Uma SD-WAN fornecida por nuvem pode resolver esses desafios, permitindo que as empresas aproveitem a banda larga de baixo custo sem prejudicar a qualidade de serviço. Dito isso, o objetivo deste teste é obter os dados de desempenho relacionados à capacidade de largura de banda. O teste é realizado por meio da imposição de uma situação de *stress* usando o *software* D-ITG a fim de comparar o desempenho do dispositivo SD-WAN usando ora o *link* de Internet banda larga e ora o *link* privativo MPLS. Este experimento foi monitorado através do protocolo de monitoração de rede SNMP (Protocolo Simples de Gerência de Rede, do inglês, *Simple Network Management Protocol*) e, posteriormente, os resultados obtidos foram plotados em gráficos para possibilitar uma análise visual. As Figura 16 e Figura 17 respectivamente exibem os resultados dos testes de largura de banda realizados por cinco horas ininterruptas sobre o dispositivo SD-WAN usando um *link* de Internet banda larga (Figura 16) e um *link* privativo MPLS (Figura 17).

Figura 16. Testes de capacidade de banda de um *link* de Internet Banda Larga



Fonte: Autoria própria.

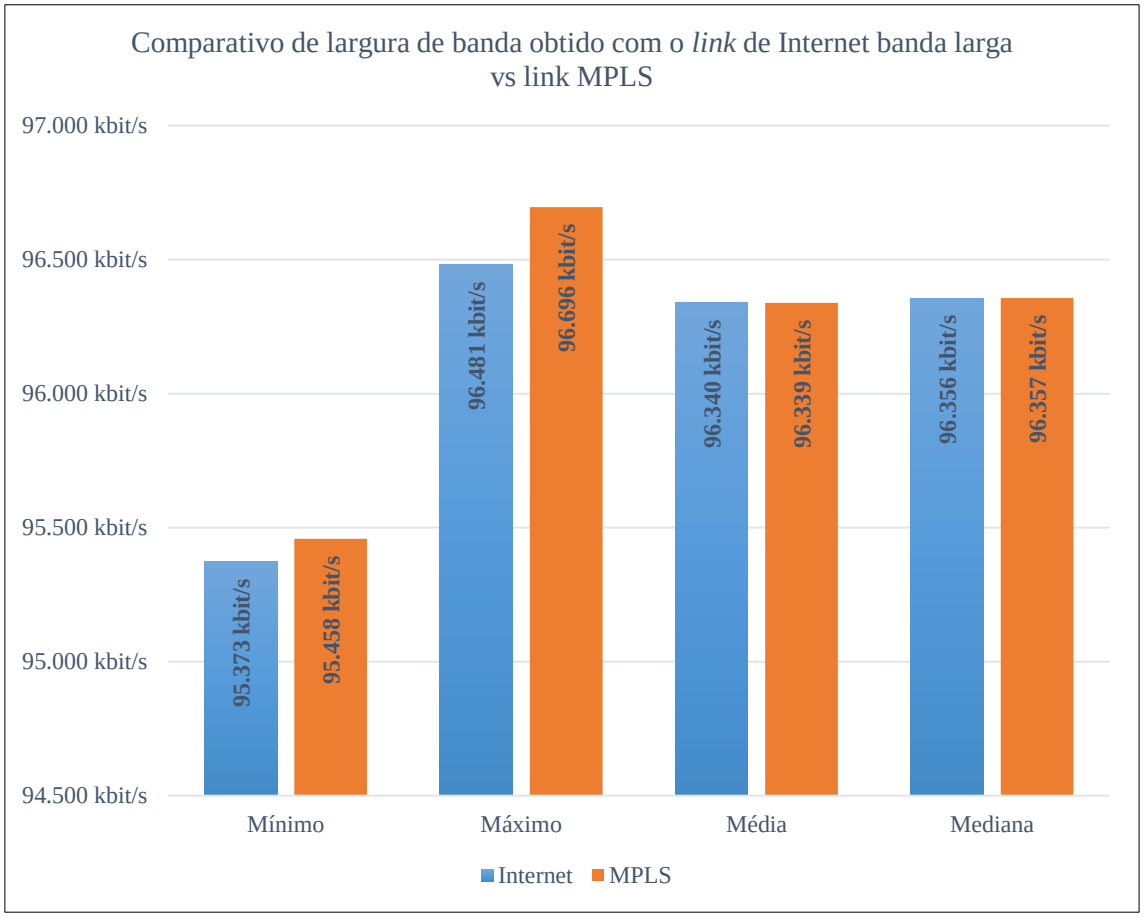
Figura 17. Testes de capacidade de banda através de um *link* MPLS



Fonte: Autoria própria.

A Figura 18 exibe os dados consolidados dos testes de largura de banda e a comparação de desempenho entre as duas tecnologias de conexão, destacando os valores mínimo e máximo alcançados por cada tecnologia, além da largura de banda média e a mediana (ou valor central do conjunto de dados coletados). Apesar do *link* de Internet banda larga sempre apresentar um desempenho levemente inferior ao do *link* privativo MPLS, em termos de largura de banda, no Capítulo 6 será discutido porque esse resultado é considerado adequado para os propósitos do projeto.

Figura 18. Comparativo de largura de banda obtido com o *link* de Internet banda larga vs *link* MPLS

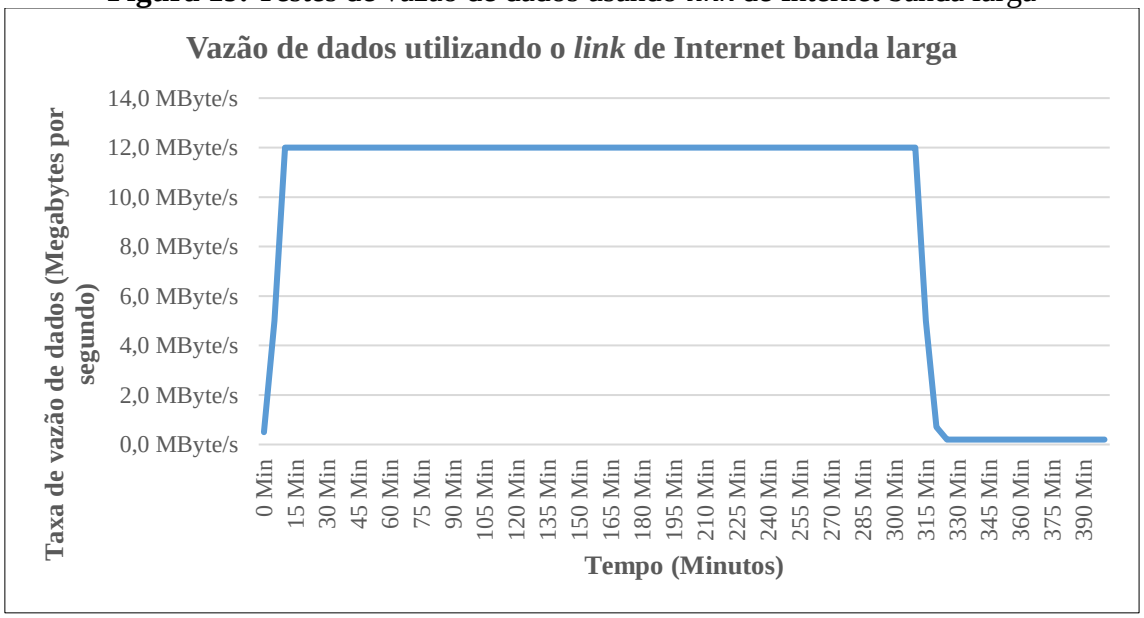


Fonte: Autoria própria.

5.2 VAZÃO DE BANDA (*THROUGHPUT*)

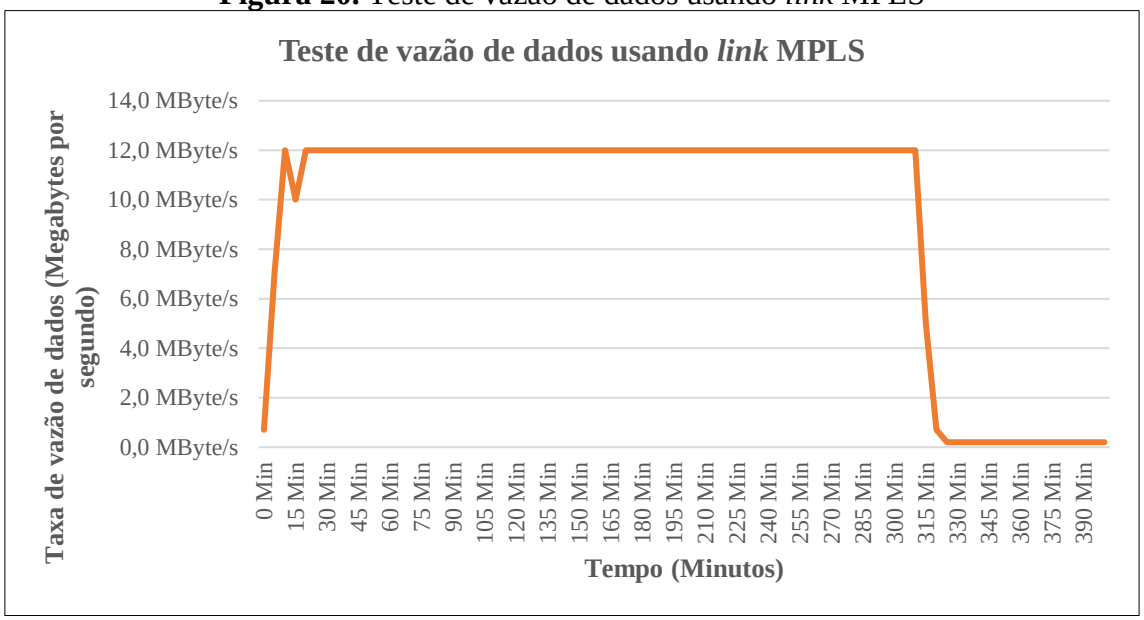
Enquanto a largura de banda se refere a capacidade de transmissão de dados em um determinado canal, a vazão de banda (do inglês *throughput*) determina a taxa em que os dados são efetivamente transmitidos, ou seja, a quantidade de dados movidos com êxito de uma fonte a um destino em determinado período. Nesse sentido, este teste tem como objetivo avaliar a performance do protótipo no que diz respeito à capacidade de vazão dos dados (média de dados entregues com sucesso por determinado canal de comunicação). Os testes foram realizados usando ambos os serviços: Internet banda larga e *link* privativo MPLS e os resultados são ilustrados nas respectivamente nas Figuras 19 e 20 após o dispositivo ser submetido a cinco horas de testes ininterruptas. Observa-se que os resultados usando ambos os tipos de conexão são similares. Uma análise mais detalhada dessa característica será realizada no capítulo seguinte.

Figura 19. Testes de vazão de dados usando *link* de Internet banda larga



Fonte: Autoria própria.

Figura 20. Teste de vazão de dados usando *link* MPLS

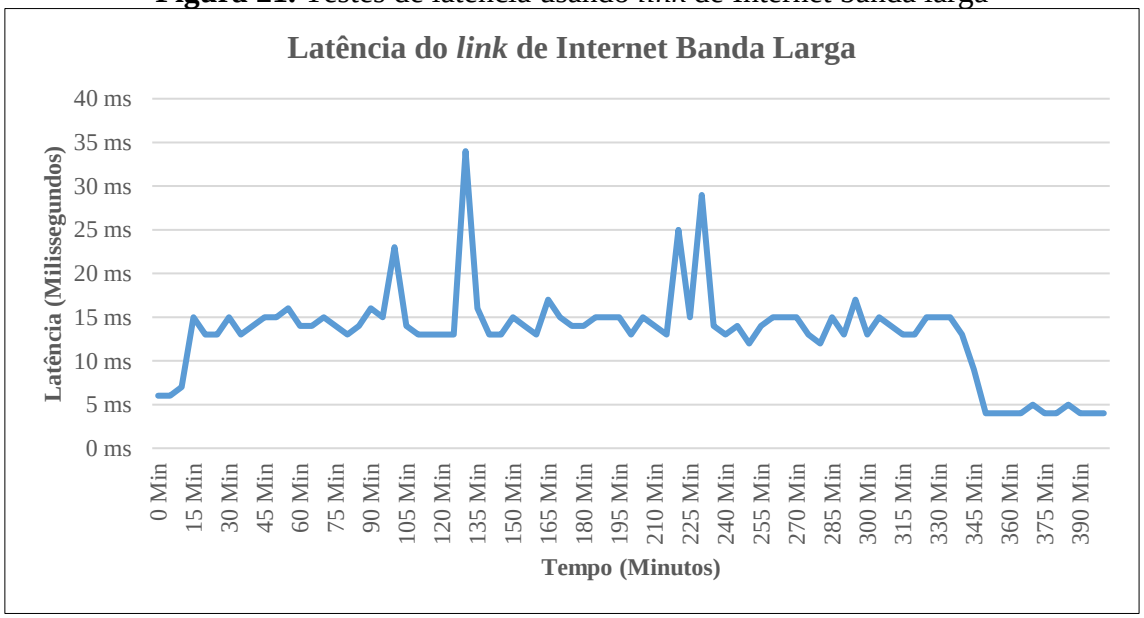


Fonte: Autoria própria.

5.3 TESTES DE LATÊNCIA

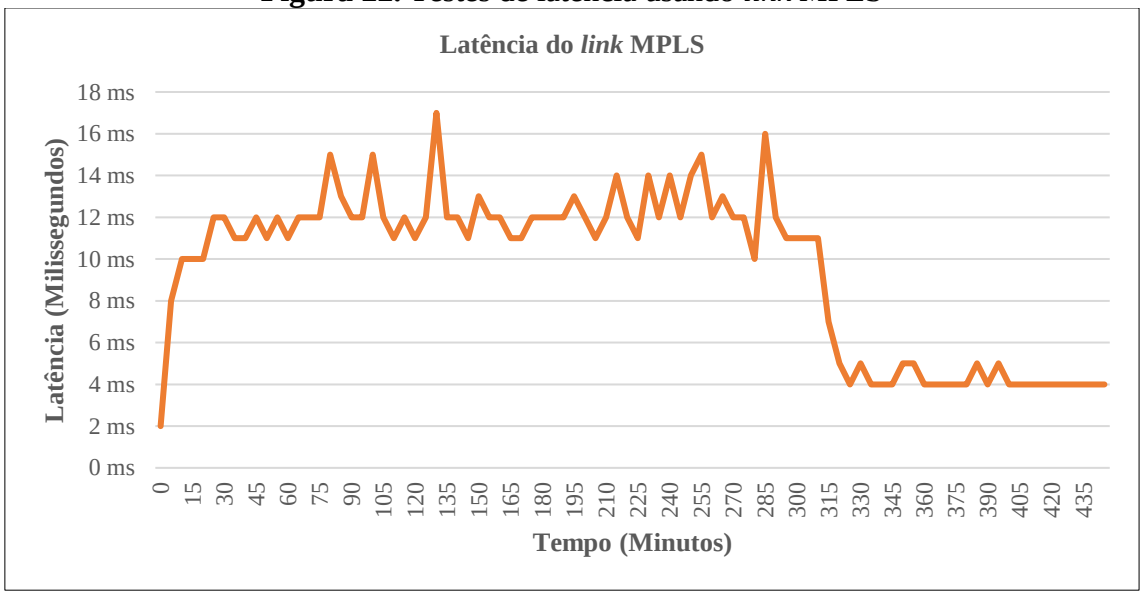
Sabe-se que a velocidade de uma rede está associada tanto à sua capacidade (largura de banda) e vazão, quanto à sua latência. Latência é a quantidade de tempo que um pacote de dados leva para viajar de um ponto a outro, ou seja, é o atraso entre o envio de um comando e sua execução podendo ser medida em milissegundos. Portanto, o objetivo do terceiro teste é verificar os índices de latência dos *link*s de Internet banda larga e MPLS durante um teste de *stress* do dispositivo SD-WAN. Os resultados obtidos para Internet banda larga e link privativo MPLS são apresentados respectivamente nas Figura 21 e Figura 22. Apesar do *link* MPLS apresentar visualmente uma latência menor, sendo, portanto, mais vantajoso, uma discussão mais apropriada dos resultados obtidos será conduzida no Capítulo 6.

Figura 21. Testes de latência usando *link* de Internet banda larga



Fonte: Autoria própria.

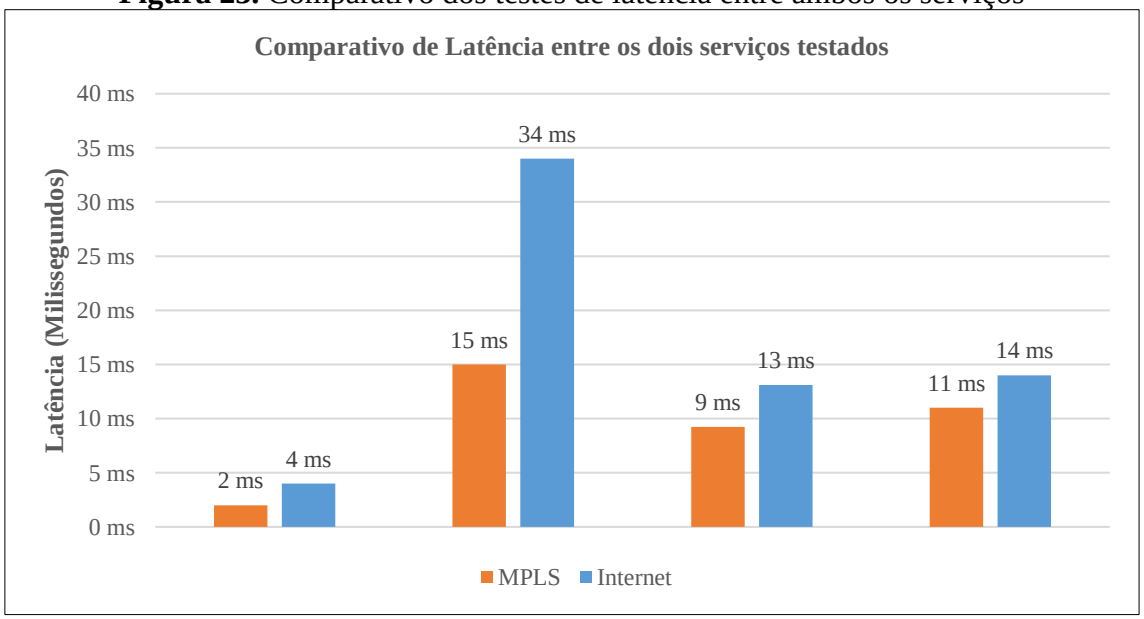
Figura 22. Testes de latência usando *link* MPLS



Fonte: Autoria própria.

A Figura 23 exibe os dados consolidados dos testes de latência do dispositivo e a comparação de desempenho entre as duas tecnologias de conexão, destacando os valores mínimo e máximo alcançados por cada tecnologia, além da latência média, a mediana e o desvio padrão do conjunto de dados coletados. É evidente que o *link* de Internet banda larga apresenta um desempenho inferior ao *link* privativo MPLS, produzindo de maneira consistente um atraso maior. No entanto, no Capítulo 6 será discutido porque, ainda assim, esse resultado atende os requisitos do projeto.

Figura 23. Comparativo dos testes de latência entre ambos os serviços

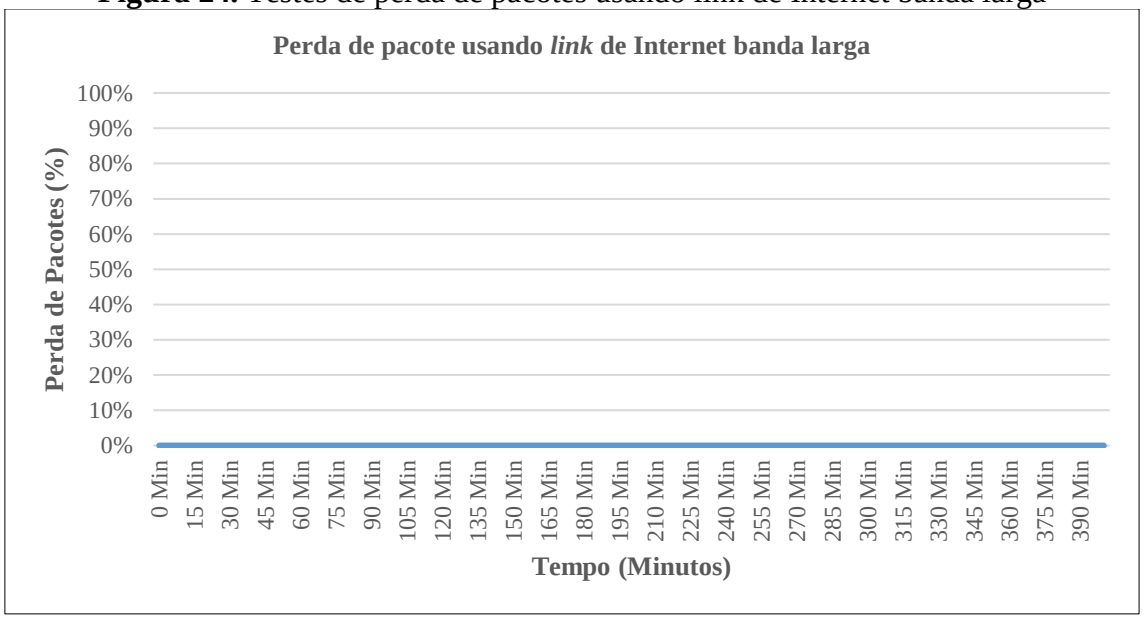


Fonte: Autoria própria.

5.4 TESTE DE PERDA DE PACOTES:

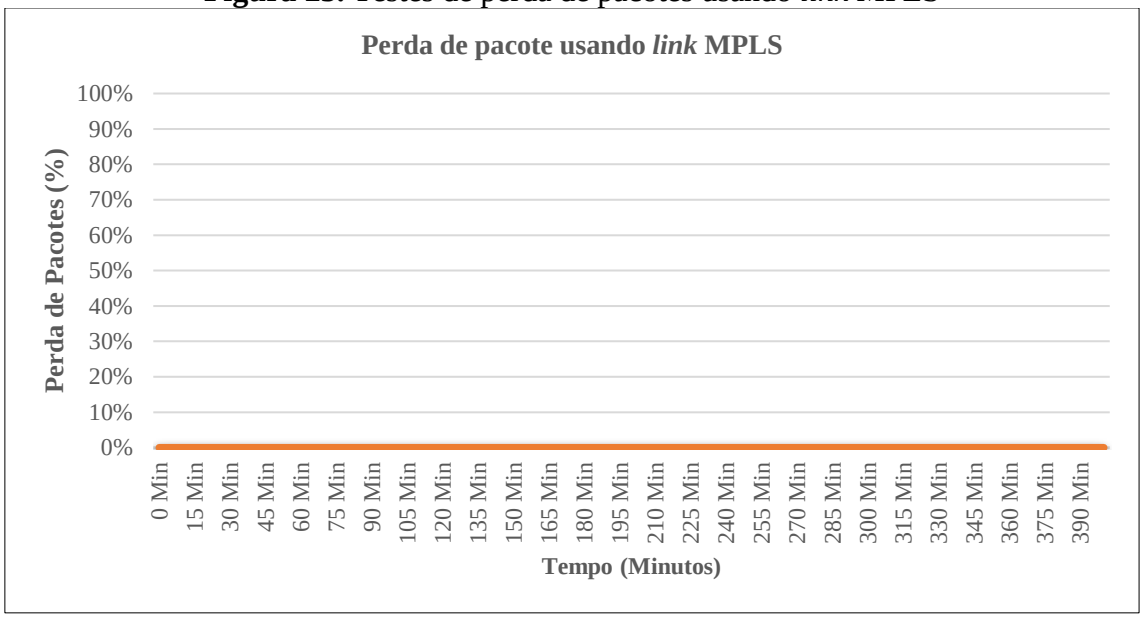
Sabe-se que os dados transmitidos em uma rede são divididos em unidades individuais chamadas pacotes, as quais são enviadas sequencialmente por uma fonte para alcançar o destino ou unidade receptora responsável por remontá-la de forma a fazer sentido. Por vários motivos, como congestionamento da rede, atrasos longos, super utilização dos dispositivos (acima de sua capacidade), erros de configuração ou mesmo ações maliciosas, tais pacotes podem ser perdidos e as falhas resultantes podem ser perceptíveis (como congelamento de imagem e fala ininteligível no caso de videoconferências e streaming de vídeos, por exemplo). Neste contexto, o objetivo deste teste é verificar os índices de percentuais de perda de pacotes dos links de Internet banda larga e MPLS durante o teste de stress. Conforme pode ser observado nas Figura 24 e Figura 25, independentemente do tipo de conexão utilizada, os testes realizados não produziram perdas de pacotes perceptíveis.

Figura 24. Testes de perda de pacotes usando link de Internet banda larga



Fonte: Autoria própria.

Figura 25. Testes de perda de pacotes usando *link* MPLS



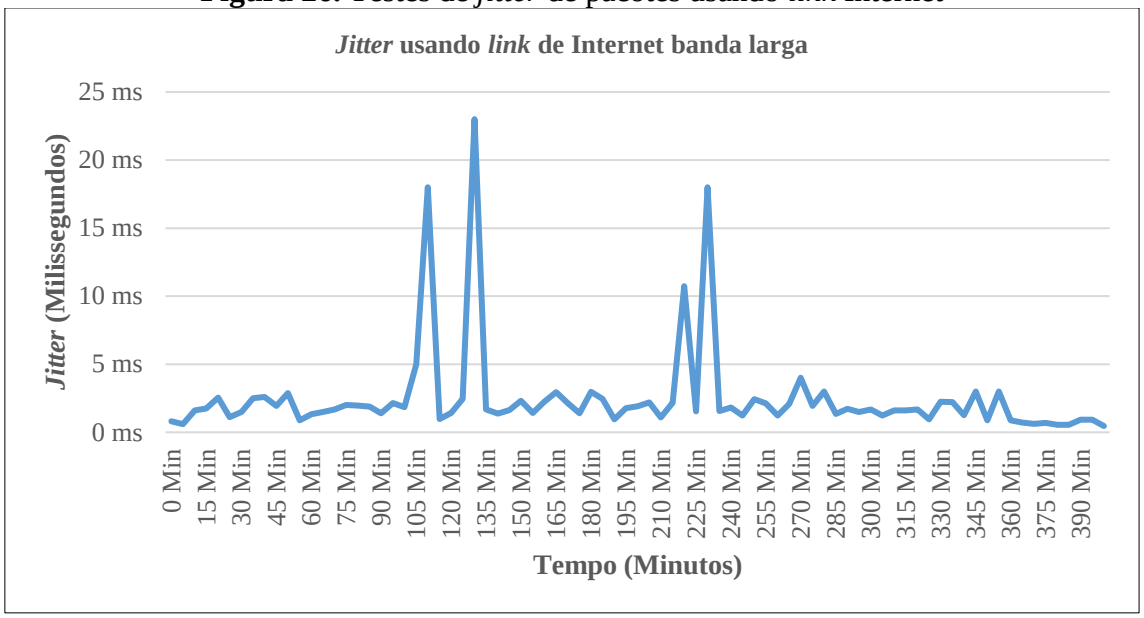
Fonte: Autoria própria.

5.5 TESTE DE *JITTER*

Basicamente o jitter é uma flutuação na latência de uma rede ou mudança na taxa de atraso de uma rede. Apesar de em muitas situações, isso não ser considerado um problema grave, permitindo que o destinatário seja capaz de reordenar os pacotes e compreendê-los normalmente (como no caso de transferência de arquivos), em alguns protocolos ou serviços, a instabilidade do atraso pode ser um defeito crucial. Os efeitos do jitter são mais perceptíveis, por exemplo, em qualquer protocolo em tempo real, como *streaming* de vídeo ou *Voice over* IP (VoIP), a tecnologia por trás de muitos sistemas telefônicos comerciais modernos.

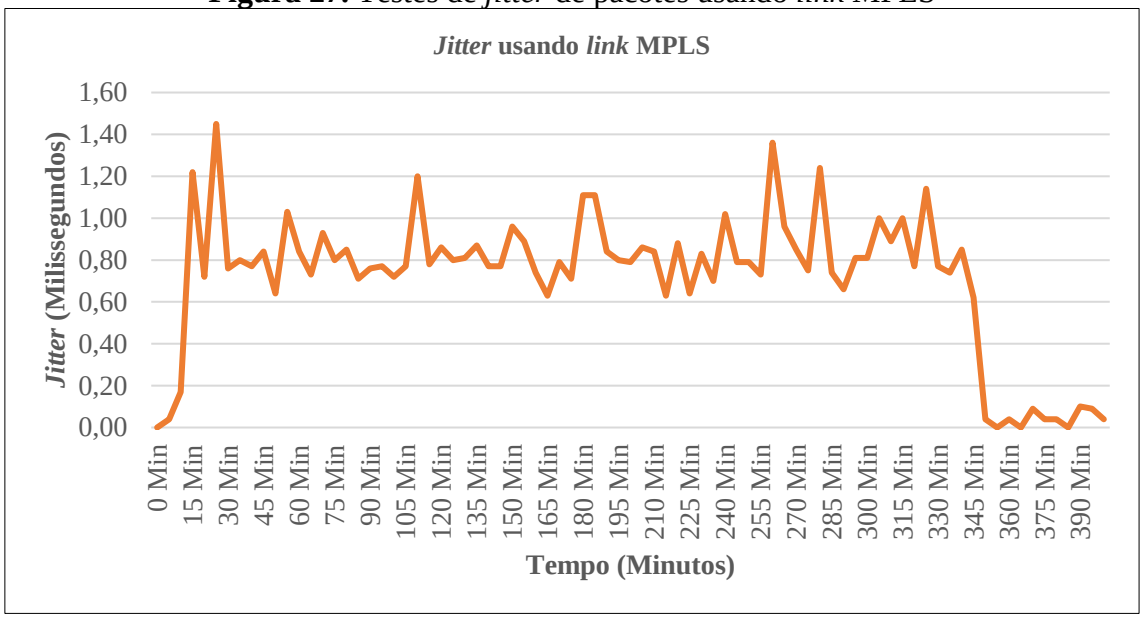
Dada essa discussão prévia, o objetivo deste teste é verificar os índices de *jitter* dos *links* de Internet banda larga e MPLS durante o teste de *stress*. Assim como a latência, o *jitter* é medido em milissegundos e os resultados dos dados coletados experimentalmente para o *link* Internet banda larga e *link* MPLS são apresentados respectivamente nas Figuras 26 e 27.

Figura 26. Testes de *jitter* de pacotes usando *link* Internet



Fonte: Autoria própria.

Figura 27. Testes de *jitter* de pacotes usando *link* MPLS

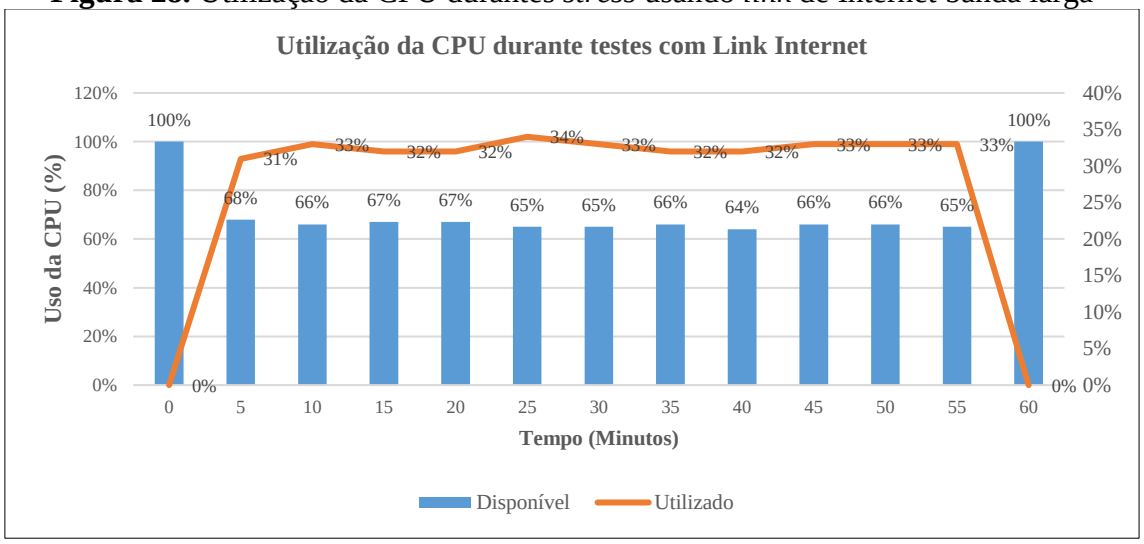


Fonte: Autoria própria.

5.6 UTILIZAÇÃO DO PROCESSADOR (CPU)

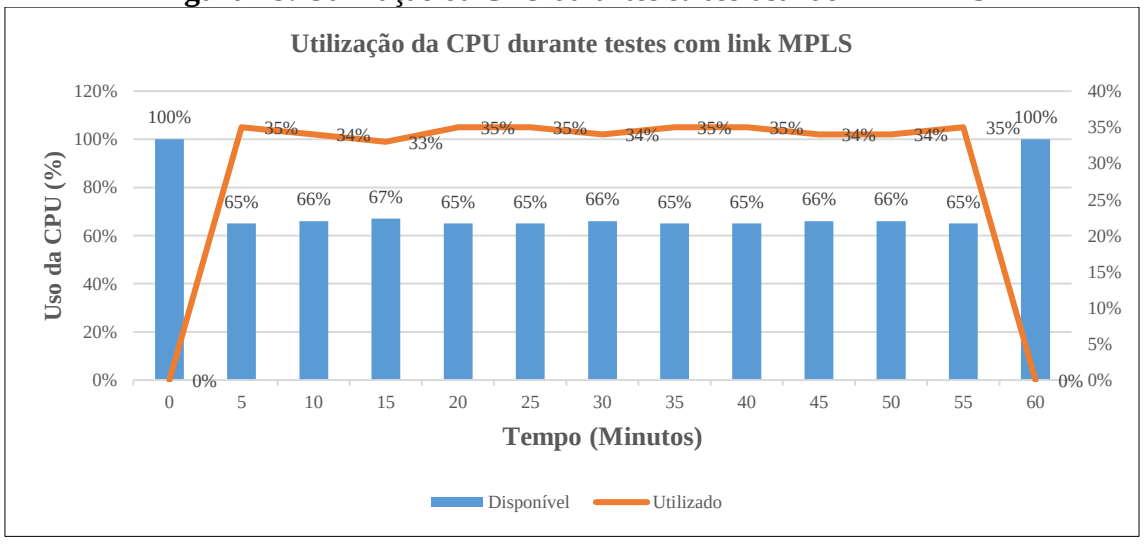
Analisar o percentual de utilização do processador (CPU) do sistema é importante pois o alto consumo do mesmo pode impor uma degradação de processamento considerável e limitar o desempenho geral das funções de rede do protótipo. O objetivo deste teste é aferir a utilização do processador (CPU) do protótipo Raspberry PI, a fim de verificar se não existe esgotamento dos recursos computacionais durante o experimento. Foram retiradas duas sequências de amostras de dados durante o teste de *stress*, uma utilizando o *link* de Internet banda larga e outra utilizando *link* privado MPLS, cujos resultados coletados durante uma hora mostrados são mostrados respectivamente nas Figuras 28 e 29.

Figura 28. Utilização da CPU durantes *stress* usando *link* de Internet banda larga



Fonte: Autoria própria.

Figura 29. Utilização da CPU durantes *stress* usando *link* MPLS



Fonte: Autoria própria.

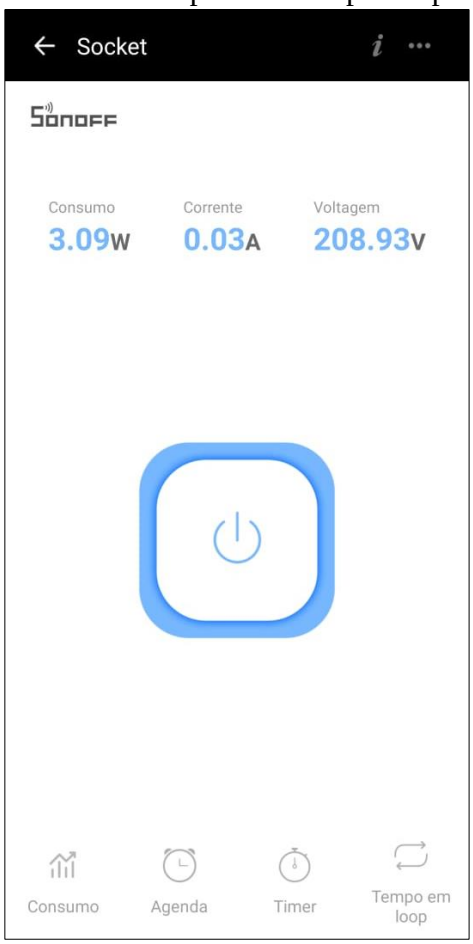
5.7 VERIFICAÇÃO DO CONSUMO ELÉTRICO

Para calcular o consumo de energia, pode-se utilizar a equação abaixo:

$$Consumo\ (kwh) = \frac{Potência\ Ativa\ (W)\ \ x\ Nº\ de\ Horas\ de\ operação}{1000}$$

A Figura 30 exibe uma amostra da captura dos dados em tempo real coletados pelo instrumento Sonoff POW R2.

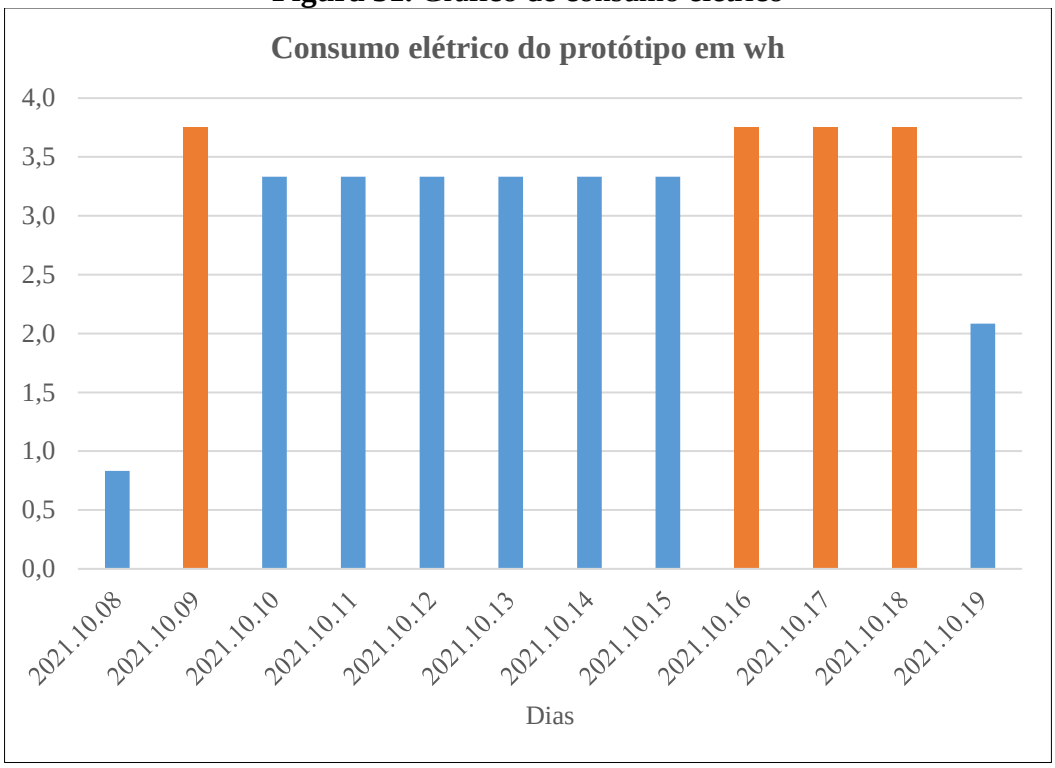
Figura 30. Medição de consumo de potência do protótipo em tempo real



Fonte: Autoria própria.

Baseado na monitoração do instrumento Sonoff POW R2, foram coletados dados de consumo, 24 horas por dia, entre os dias 8 de outubro e 19 de outubro de 2021. A Figura 31 consolida todas as coletas em forma gráfica.

Figura 31. Gráfico de consumo elétrico



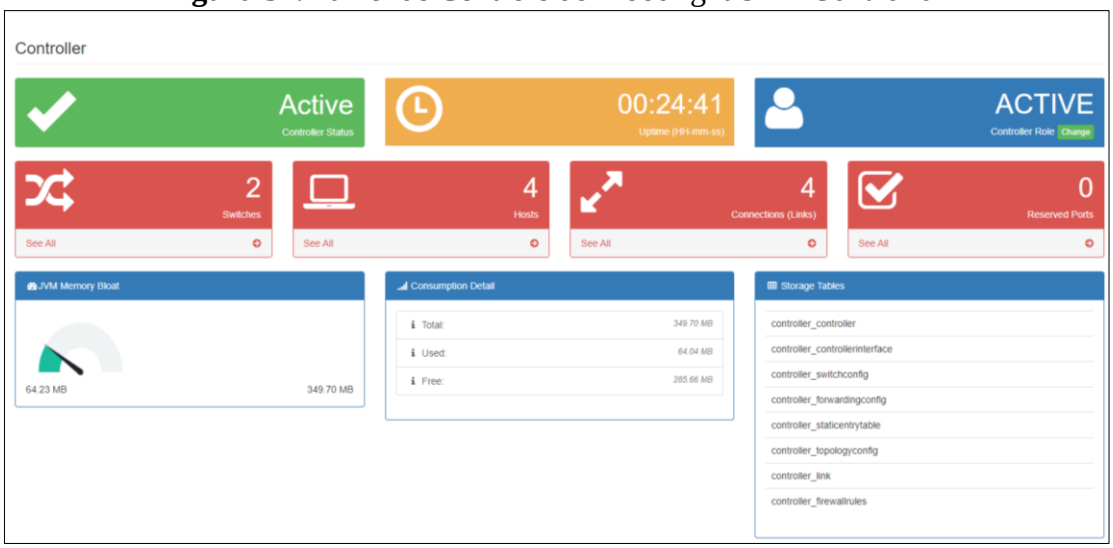
Fonte: Autoria própria

É possível constatar um incremento de 0,5 watts hora no consumo nos dias em que os testes de stress foram realizados. Nos dias 08 e 19 o consumo foi menor devido ao tempo de *uptime* do sistema.

5.8 TESTES COM O CONTROLADOR SDN *FLOODLIGHT*

Neste trabalho avaliou-se o emprego do controlador SDN *Floodlight* de acordo com os critérios de visualização dos recursos e facilidade na operação, funcionalidades de segurança embarcadas no *software* de controle e integração com o *software* OpenvSwitch. O controlador Floodlight foi escolhido para os testes porque oferece bom desempenho, portabilidade, ampla documentação disponível e facilidade de instalação e configuração. A Figura 32 exibe um painel de controle com informações relacionadas à qualidade e à disponibilidade do controlador SDN.

Figura 32. Painel de Controle do Floodlight SDN *Controller*

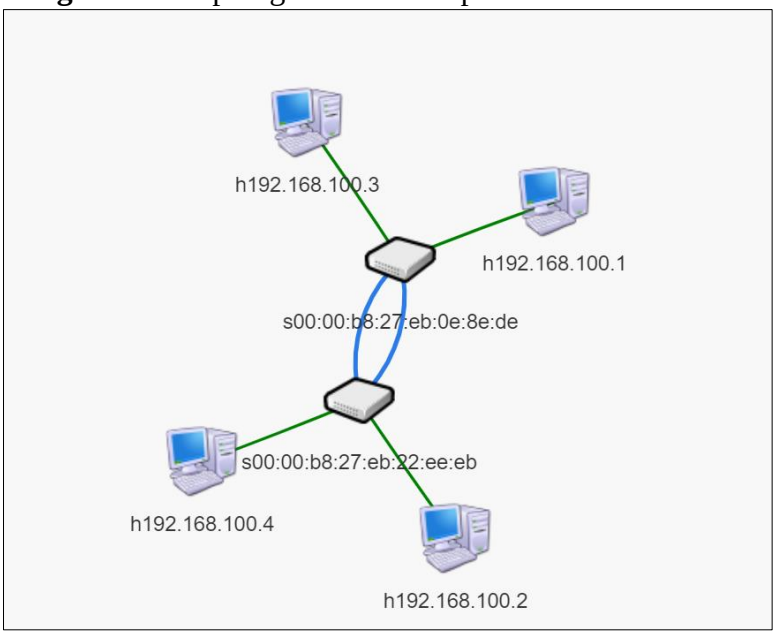


Fonte: Autoria própria

A interface gráfica do Floodlight apresenta uma lista dos *hosts* conectados à rede com as informações do endereço MAC de um *host*, endereço IPV4, endereço IPV6, endereço MAC do *switch* conectado, porta conectada do *switch* e hora da última visualização. Todos os *link*s entre os *switches* podem ser monitorados via GUI. Propriedades como direção dos *link*s, *switch* de origem e sua porta, switch de destino e sua porta e tipo de *link* (interno, externo) são as informações fornecidas.

A capacidade de aprender e descobrir a topologia do experimento bem como os elementos conectados ao mesmo, foram algumas das funções analisadas durante os testes com o controlador Floodlight, cuja topologia associada está representada na Figura 33.

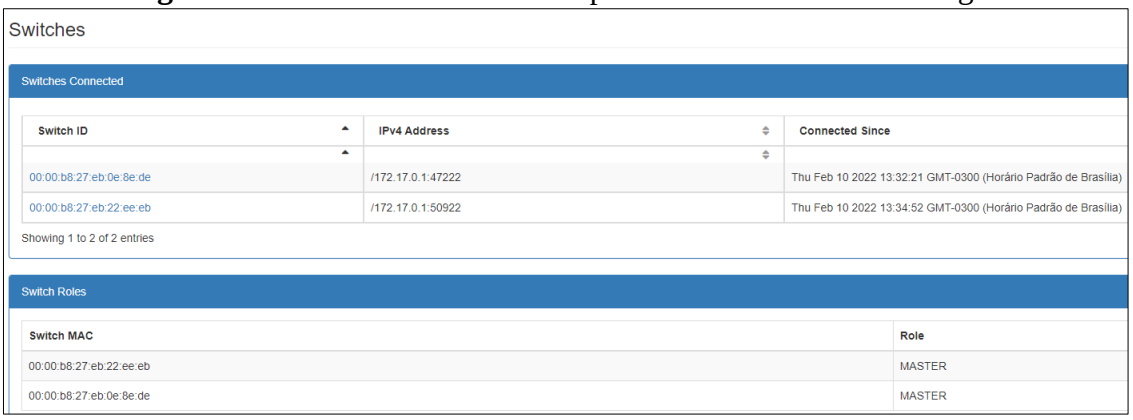
Figura 33. Topologia descoberta pelo controlador SDN



Fonte: Autoria própria

Foram verificadas a capacidade de reconhecimento dos protótipos OpenvSwitch nomeados como OVS-01 e OVS-02. A Figura 34 válida essas informações pela interface gráfica do controlador, enquanto a imagem apresentada na Figura 35 valida a capacidade de coleta dessas informações através da API disponível no controlador SDN, onde ambas interfaces atestam a capacidade de reconhecimento dos protótipos através de identificação única chamada ID que compõe a topologia.

Figura 34. Reconhecimento dos dispositivos via GUI do Floodlight



Fonte: Autoria própria

Figura 35. Reconhecimento dos Dispositivos via API do Floodlight

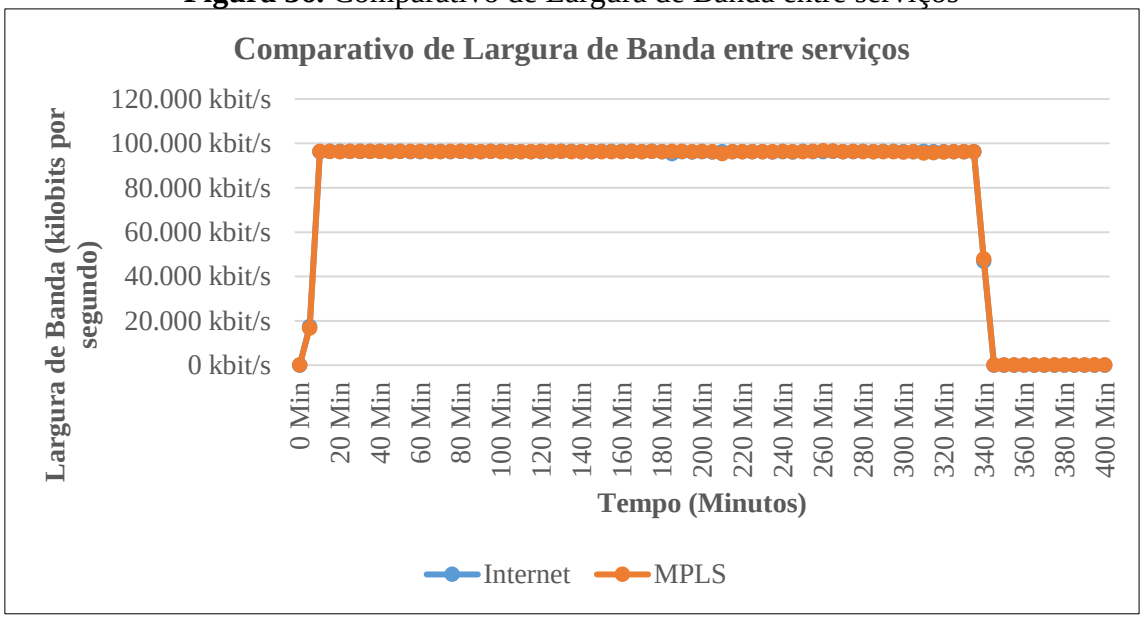

```
{
    "entityClass": "DefaultEntityClass",
    "mac": [
        "b8:27:eb:22:ee:eb"
    ],
    "ipv4": [
        "192.168.100.4"
    ],
    "ipv6": [
        "fe80::ba27:ebff:fe22:eeeb"
    ],
    "vlan": [
        "0x0"
    ],
    "attachmentPoint": [
        {
            "switch": "00:00:b8:27:eb:22:ee:eb",
            "port": "local"
        }
    ],
    "lastSeen": 1644512330386
},
{
    "entityClass": "DefaultEntityClass",
    "mac": [
        "b8:27:eb:0e:8e:de"
    ],
    "ipv4": [
        "192.168.100.3"
    ],
    "ipv6": [
        "fe80::ba27:ebff:fe0e:8ede"
    ],
    "vlan": [
        "0x0"
    ],
    "attachmentPoint": [
        {
            "switch": "00:00:b8:27:eb:0e:8e:de",
            "port": "local"
        }
    ],
    "lastSeen": 1644512329380
}
```


Fonte: Autoria própria.

6 DISCUSSÃO DOS RESULTADOS

Os testes de largura de banda do protótipo usando *link* de Internet banda larga e MPLS mostraram similaridades nos resultados, o que aponta uma equivalência no funcionamento de ambos os serviços, conforme apresentado de maneira conjunta na Figura 36 (ambos resultados em um mesmo gráfico). Neste ponto é importante salientar que *link*s de Internet banda larga atravessam redes de diferentes provedores de serviço, cada um com sua arquitetura, o que não garante uma otimização no seu *backbone* para garantir a entrega da largura de banda contratada.

Figura 36. Comparativo de Largura de Banda entre serviços

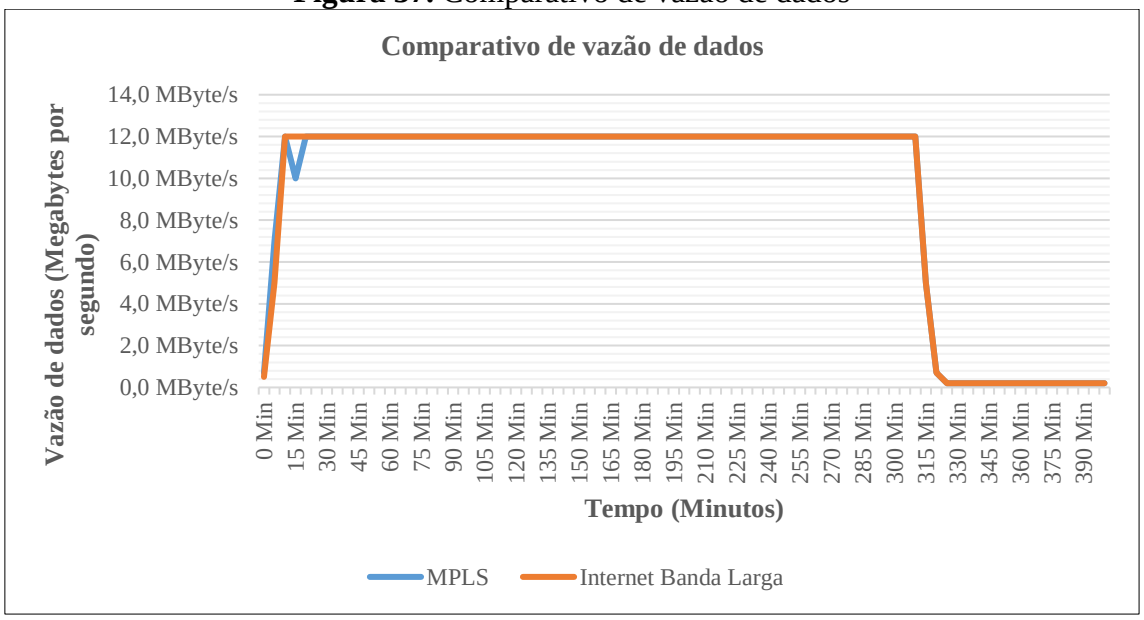


Fonte: Autoria própria.

Tendo como base os resultados de largura de banda coletados, acredita-se que, usando um link de Internet banda larga, o protótipo consegue entregar de forma satisfatória (sem uma degradação de desempenho relevante quando comparado ao link MPLS) a largura de banda requerida (em torno de 95% da largura de banda provida pelo link privativo).

Os testes de vazão de banda apresentados no capítulo anterior e retificados pela Figura 37 (em que se verifica um resultado de 12Mbps para ambos os tipos de conexão) demonstraram que o protótipo tem performance semelhante quando emprega o *link* de Internet banda larga e o *link* MPLS. Tal resultado certifica a entrega dos dados e comprova que ambos os serviços apresentam capacidades similares quando do uso de um dispositivo SD-WAN.

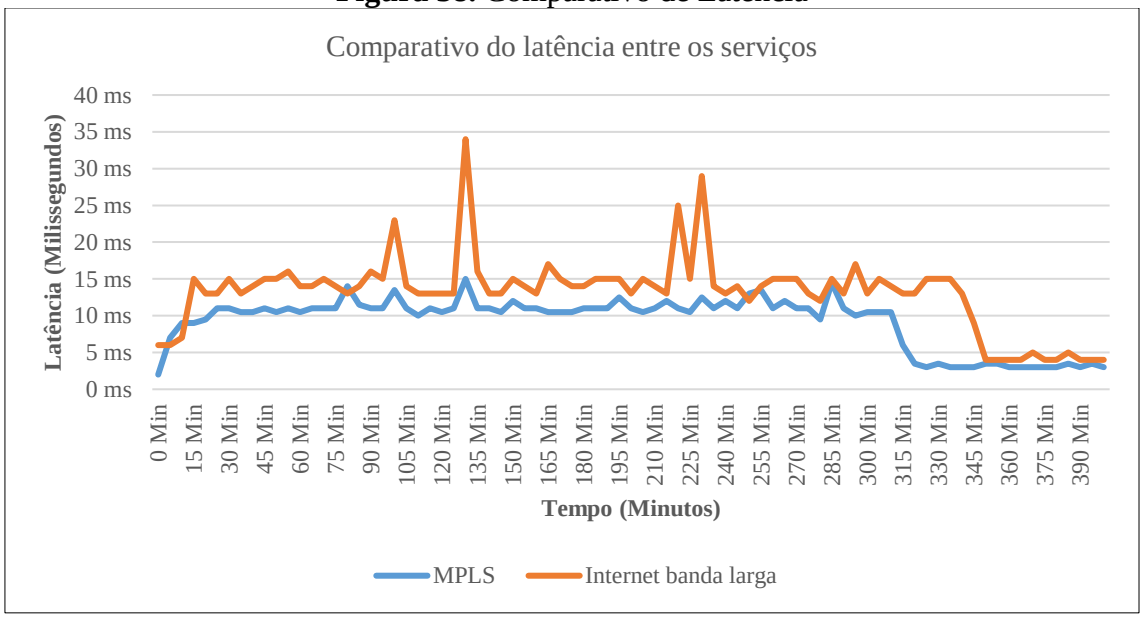
Figura 37. Comparativo de vazão de dados



Fonte: Autoria própria.

No que se refere aos testes de latência, o protótipo obteve um resultado semelhante em ambos os serviços, com uma ligeira degradação de 2 milissegundos na média usando o *link* de Internet banda larga, o que pode ser explicado pela natureza do serviço prestado pelos operadores de Internet. Essa variação entre os serviços acontece em virtude dos *links* de Internet banda larga atravessarem diferentes infraestruturas, isso acarreta uma degradação na qualidade que depende de cada provedor. Em algumas situações podem-se experimentar degradações mais severas diferente do que ocorre nos *links* baseados em MPLS os quais não sofrem esse tipo de degradação por tratar-se de circuitos privativos que na maioria dos casos estão contidos apenas na infraestrutura de provedor que fornece o serviço. Ainda assim, de acordo com a fabricante número um de equipamentos de rede (Cisco) uma latência geral da rede que pode ser considerada aceitável é de menos de 150 ms, que ainda é bem superior aos resultados apresentados na Figura 38 que reúne os dados coletados nos testes de latência para ambos os serviços durante os testes de *stress*. No que se refere às perdas de pacotes, o Capítulo 5 demonstrou graficamente que não foram relatadas situações de perdas durante a realização dos testes, o que é uma característica desejada, sendo que, ainda de acordo com a Cisco, é considerada admissível uma perda de pacotes de até no máximo 1%.

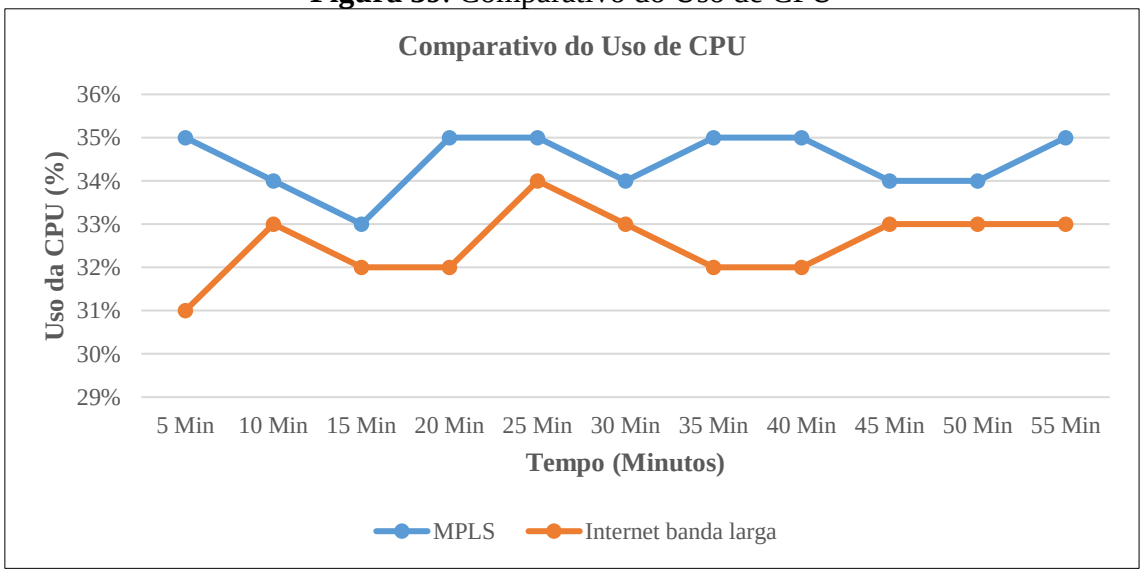
Figura 38. Comparativo de Latência



Fonte: Autoria própria.

O principal objetivo dos testes de desempenho de uso da CPU era indicar que não existe esgotamento dos recursos computacionais do *hardware* utilizado na montagem experimental. Nesse sentido, o protótipo mostrou a utilização de 30% em média dos recursos computacionais em ambos os serviços, conforme pode ser observado na Figura 39, que reúne os dados coletados com o uso do *link* MPLS e o *link* de Internet banda larga. Curiosamente, observa-se que diferentemente dos outros testes conduzidos, nesse caso, o uso da Internet banda larga foi vantajoso para o dispositivo, requerendo um menor uso de CPU do que quando optou-se pelo *link* MPLS.

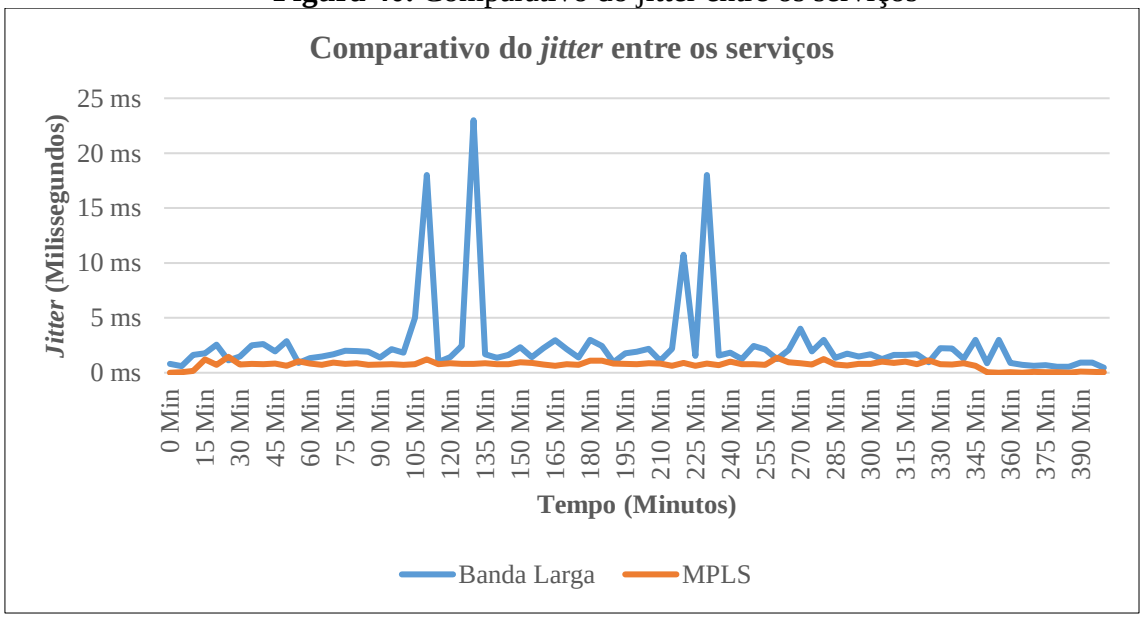
Figura 39. Comparativo do Uso de CPU



Fonte: Autoria própria.

Os testes de *jitter* mostraram que o *link* de Internet banda larga está sujeito a variações de latência regulares, porém dentro de limites que não penalizem o serviço. Já era esperado um melhor desempenho do *link* de MPLS, devido às suas características de qualidade de serviço. A Figura 40 apresenta o comparativo entre a média do *jitter* usando ambos os serviços. Vale a pena destacar que, segundo a Cisco, os níveis aceitáveis de instabilidade de latência/tremulação ou *jitter* são < 30ms, no entanto, para obter melhor desempenho, tais níveis devem ser mantidos abaixo de 20ms, o que é garantido pelo protótipo conforme ilustrado na Figura 40.

Figura 40. Comparativo do jitter entre os serviços



Fonte: Autoria própria.

De acordo com TANTISARKHORNKHET; WERAPUN (2017), os protocolos comuns mais utilizados possuem diferentes características com relação a perda de pacotes, *jitter* e latência. A Tabela 6 apresenta um resumo das típicas aplicações mais utilizadas e sua tolerância aos requisitos de qualidade testados.

Tabela 6. Requisitos de qualidade para aplicações típicas

Tipo de Aplicação	Demanda de *throughput*	Tolerância latência	Tolerância a *Jitter*	Tolerância a perda de pacotes
E-mail	Baixa	Alta	Alta	Alta
Navegação Web	Baixa	Alta	Alta	Alta
Transferência de arquivos (FTP)	Baixa -Alta	Alta	Alta	Alta
Mensagem instantânea (chat)	Baixa	Média	Média	Média
Vídeo sobre demanda	Alta	Média	Média	Baixa
Voz sobre IP	Baixa	Baixa	Baixa	Baixa
Vídeo conferência	Média-alta	Baixa	Baixa	Baixa

Fonte: Adaptado de (TANTISARKHORNKHET; WERAPUN, 2017).

Segundo YAN CHEN (2004), a especificação concisa dos requisitos de serviço é vital para a realização da garantia da qualidade nas redes de computadores. Como diferentes aplicativos possuem diferentes requisitos de serviço, é importante estabelecer parâmetros para validar os resultados do experimento. A Tabela 7 apresenta os requisitos relacionados a performance dos aplicativos mais comuns relacionados a redes IoT.

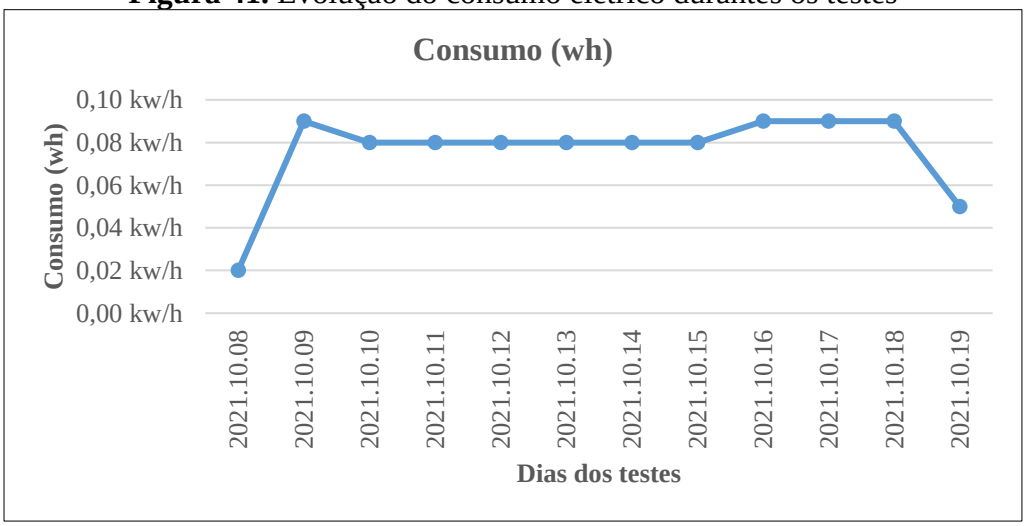
Tabela 7. Validação dos parâmetros relacionados aos requisitos de rede

Aplicação	Tipo de comunicação	Tempo de resposta	Latência	*Jitter*	Taxa de dados	Largura de banda	Perda de Pacotes (%)
			(ms)	(ms)	(Bps)	(bps)	
E-mail	Não Tempo Real e Simétrico	2–5 Segundos	Low	N/A	< 10 K	< 10 K	Zero
Mensagem instantânea (chat)	Não Tempo Real e Simétrico	1 Segundo	< 200	N/A	< 1 K	< 1 K	Zero
Navegação Web	Não tempo real e Assimétrico	2–4 Segundos	< 400	N/A	< 24 K	< 24 K	Zero
FTP	Não tempo real e Assimétrico	2–5 Segundos	Média	N/A	Alta	Alta	Zero
Vídeo Conferência	Tempo Real e Simétrico	< 100	< 150	< 400	64–1920K	80K–2M	<0.01%
Voz sobre IP	Tempo Real e Simétrico	< 150	< 100	< 400	40~16 K	50-22 K	< 1%
Vídeo sobre demanda	Tempo Real e Altamente Assimétrica	< 100	< 150	< 100	N/A	1.2–1.5M	<0.001%
Link Internet Banda Larga	Simétrico	N/A	< 13	<3	12 MB	96M	Zero
Link MPLS	Simétrico	N/A	< 9	< 1	12MB	96M	Zero

Fonte: Adaptado de (YAN CHEN, 2004)

Os resultados dos testes mostraram que o protótipo usando Raspberry Pi Model B+ consumiu relativamente uma baixa potência durante os testes de *stress*, um requisito importante para o sucesso de projetos de cidades inteligentes. Com dezenas de milhares de dispositivos transmitindo informações é importante que haja uma eficiência no consumo elétrico, a fim de garantir a sustentabilidade econômica da rede IoT. Figura 41 apresenta a evolução no consumo do dispositivo em estado de modo de espera e em regime de processamento.

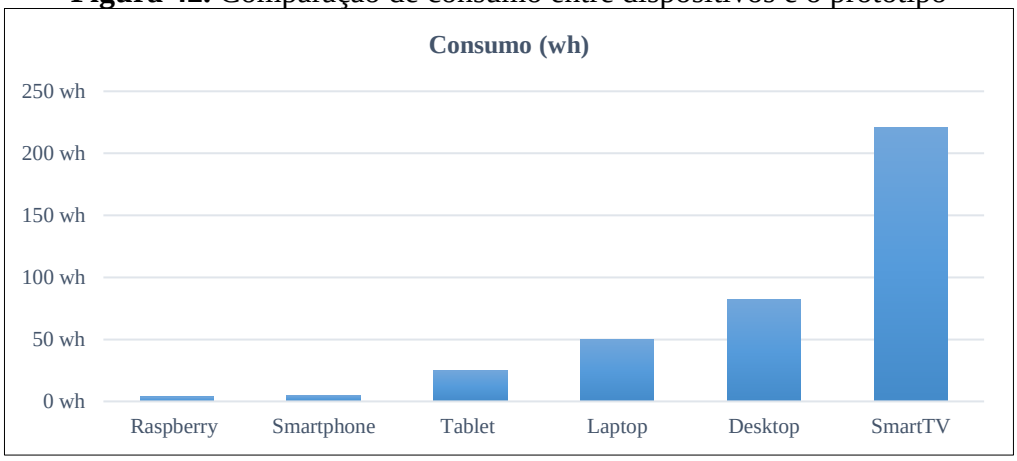
Figura 41. Evolução do consumo elétrico durantes os testes



Fonte: Autoria própria.

A Figura 42 faz um comparativo entre o consumo elétrico do protótipo com outros dispositivos com intuito de assegurar a premissa de baixo consumo elétrico.

Figura 42. Comparação de consumo entre dispositivos e o protótipo



Fonte: (ANWAAR; SHAH, 2015)

7 CONCLUSÕES E CONSIDERAÇÕES FINAIS

A solução SD-WAN proposta neste trabalho, que consiste no projeto de um dispositivo *white-label*, conseguiu atender os requisitos definidos nos objetivos. No que diz respeito ao desempenho, o equipamento mostrou-se robusto o suficiente e conseguiu atender de forma semelhante os requisitos de capacidade de banda, vazão, baixa latência e *jitter* aceitável para os propósitos da aplicação, além de baixo custo.

A solução usando conectividade de Internet banda larga se mostrou competitiva com os *links* MPLS, o que demonstra que os serviços de Internet banda larga disponibilizados no mercado, permitem a substituição dos dispendiosos *links* MPLS, gerando uma economia substancial e viabilizando projetos com muitos terminais para cidades inteligentes. Nos testes referentes ao consumo de energia, o protótipo conseguiu ter um baixo consumo elétrico, uma premissa importante por se tratar de um equipamento *low-cost* que pode ser usado em redes para cidades inteligentes.

Nos projetos de cidades inteligente as administrações públicas podem utilizar a tecnologia SD-WAN para acelerar a adoção de serviços inteligentes que podem melhorar a viabilidade, sustentabilidade e habitabilidade em suas cidades. Finalmente, considera-se que a solução SD-WAN baseada em *software opensource* e *hardware low-cost*, consegue atender as necessidades das empresas e organizações com custo e complexidade relativamente baixos.

7.1 TRABALHOS FUTUROS

Como já previa o IEEE, os dispositivos domésticos inteligentes ultrapassam os *smartphones* em 2021, com o número de dispositivos de Internet das Coisas (IoT) previsto para chegar a mais de 50 bilhões (CHEN, 2019). Os dispositivos inteligentes estão cada vez mais presentes em casa e no escritório, com consumidores e empresas exigindo conectividade mais rápida e confiável.

Para aprimorar a experiência de conexão dos usuários finais, a conectividade onipresente deve ser fornecida para todos os pontos de instalações residenciais e comerciais, ao mesmo tempo garantindo o gerenciamento adequado desses dispositivos conectados. Isso é fundamental se os provedores de serviço quiserem liberar todo o potencial do ecossistema de casas conectadas.

A tecnologia SD-WAN pode ser utilizada para otimizar o gerenciamento de redes domésticas e vários estudos neste sentido estão sendo realizados com o objetivo de padronizar as melhores práticas e tecnologias a serem utilizadas neste cenário, como sugestão de trabalhos futuros podem ser elencados o desenvolvimento de soluções *opensource* SD-WAN que podem ser embarcadas em dispositivos IoT para um melhor gerenciamento e segurança das soluções oferecidas ao usuário.

Esta solução pode ser introduzida em diversos sistemas tais como: Gerenciamento de geração de energia fotovoltaica residencial, gerenciamento de sistemas de sensores sem fio para diversas aplicações, gerenciamento e monitoração de redes de acesso WI-FI. Estudos sobre mobilidade de redes estão sendo pesquisados utilizando SD-WAN como *background* tecnológico para complementar os recursos baseados no protocolo IPv6.

Outro campo importante no desenvolvimento de aplicações residenciais usando SND, diz respeito a segurança dos dados que podem ser explorados por uma falha ou ataque de *malware*, o protocolo *OpenFlow* pode monitorar esse tráfego malicioso e informar o controlador SDN que uma providência precisa ser tomada.

Para finalizar, vale a pena mencionar que alguns dos gráficos resultantes dos testes do protótipo, os quais foram apresentados nos capítulos 5 e 6, apresentam "pontos fora da curva", que se diferenciam drasticamente do comportamento esperado e podem ter causado anomalias nas análises realizadas. Tais pontos merecem um estudo mais detalhado e poderiam ser considerados *outliers*. Nesse sentido, visando obter uma série mais confiável de dados para serem analisados e uma maior segurança na discussão dos resultados obtidos por essa pesquisa, propõe-se a realização de uma filtragem de dados em uma investigação futura.

8 REFERÊNCIAS

ALENCAR, F. et al. **How software aging affects SDN: A view on the controllers**. 2014 Global Information Infrastructure and Networking Symposium, GIIS 2014. **Anais**...2014Disponível em: <http://www.huawei.com/ucmf/groups/public/>. Acesso em: 27 dez. 2021

AMINI, H. et al. **Sustainable Interdependent Networks**. [s.l: s.n.].

ANAN, M. et al. Empowering Networking Research and Experimentation through Software-Defined Networking. **Journal of Network and Computer Applications**, 2016.

ANDROMEDA, S.; GUNAWAN, D. Techno-economic Analysis from Implementing SD-WAN with 4G/LTE, A Case Study in XYZ Company. **Proceedings - 2020 International Seminar on Intelligent Technology and Its Application: Humanification of Reliable Intelligent Systems, ISITIA 2020**, p. 345–351, 2020.

ANGELIDOU, M. Smart city policies: A spatial approach. **Cities**, v. 41, n. July 2014, p. S3–S11, 2014.

ANWAAR, W.; SHAH, M. A. Energy Efficient Computing: A Comparison of Raspberry PI with Modern Devices. **International Journal of Computer and Information Technology**, v. 4, n. 2, p. 410–413, 2015.

ARPITA SAXENA (TARASPAN BLOG). **SD-WAN Architecture Explained: An Overview and Components (2020 Update)**. Disponível em: <https://www.taraspan.com/blog/sd-wan-architecture-explained-an-overview-and-components/>. Acesso em: 5 maio. 2021.

BANNOUR, F.; SOUIHI, S.; MELLOUK, A. Distributed SDN Control: Survey, Taxonomy, and Challenges. **IEEE Communications Surveys and Tutorials**, v. 20, n. 1, p. 333–354, 2018.

BENSON, T.; AKELLA, A.; MALTZ, D. **Unraveling the complexity of network management**. Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2009. **Anais**...Boston, Massachusetts: USENIX Association, 2009Disponível em: <https://dl.acm.org/doi/10.5555/1558977.1559000>

BERDE, P. et al. **ONOS: towards an open, distributed SDN OS**. Proceedings of the third workshop on Hot topics in software defined networking. **Anais**...New York, NY, USA: ACM, 22 ago. 2014Disponível em: <https://dl.acm.org/doi/10.1145/2620728.2620744>

BIBRI, S. E.; KROGSTIE, J. Smart sustainable cities of the future: An extensive interdisciplinary literature review. **Sustainable Cities and Society**, v. 31, p. 183–212, 2017.

BUTLER, K. et al. A survey of BGP security issues and solutions. **Proceedings of the IEEE**, v. 98, n. 1, p. 100–122, jan. 2010.

CABRA, M. **3 Reasons Why Your IoT Initiatives Need SD-WAN**. Disponível em: <https://www.iotforall.com/sd-wan-iot/>. Acesso em: 30 mar. 2020.

CHAN, H. **Does your smart city have the network it needs? | Nokia Blog**. Disponível em: <https://www.nokia.com/blog/does-your-smart-city-have-network-it-needs/>. Acesso em: 29 mar. 2020.

CHEN, N. **MEF Leads SD-WAN Service Standardization & Certification:** Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8928157>. Acesso em: 12 out. 2021.

DALLA CIA ET AL. Using Smart City Data in 5G Self-Organizing Networks. **IEEE Internet of Things Journal**, v. 5, n. 2, p. 645–654, 2018.

DAUGHERTY, B.; METZ, C. Multiprotocol label switching and IP, Part I: MPLS VPNs over IP tunnels. **IEEE Internet Computing**, v. 9, n. 3, p. 68–72, maio 2005.

DAWADI, B. R. et al. TOWARDS SMART NETWORKING WITH SDN ENABLED IPV6 NETWORK. 2022.

DINCER;, S. S.; ALVIZU, R.; MAIER, G. A. **Experimental SD-WAN Testbed with Active and Passive Monitoring Capabilities**. [s.l.] Politecnico di Milano, 2018.

EMBRATEL. Book de Preços – Oferta Comercial MERCADO CORPORATIVO Recomendações. p. 1–98, 2020.

FIA. **White Label: o que é, vantagens e como funciona**. Disponível em: <https://fia.com.br/blog/white-label/>. Acesso em: 29 abr. 2021.

FOREST, J.; LERNER, A.; SINGH, N. Magic Quadrant for WAN Edge Infrastructure. **Gartner, Inc.**, n. September 2020, p. 1–34, 2020.

FORTINET. **FortiGate ® FortiWiFi 40F Series FG-40F and FWF-40F**. [s.l: s.n.].

GEMBER-JACOBSON, A. et al. **OpenNF: Enabling innovation in network function control**. Computer Communication Review. **Anais**...: SIGCOMM '14.New York, NY, USA: Association for Computing Machinery, 2015Disponível em: <https://doi.org/10.1145/2619239.2626313>

GHARAIBEH, A. et al. Smart Cities: A Survey on Data Management, Security, and Enabling Technologies. **IEEE Communications Surveys and Tutorials**, v. 19, n. 4, p. 2456–2501, 2017.

GIBSON, D. **Software-Defined WAN for dummies for Dummies**. 2. ed. Hoboken, NJ: John Wiley & Sons, Inc, 2015.

GIFFINGER, R. et al. **Smart Cities -Ranking of European medium-sized cities**. Vienna: [s.n.]. Disponível em: <http://www.smart-cities.eu/>.

GIL, A. C. **Como elaborar projetos de pesquisa**. 6. ed. ed. São Paulo, SP: Atlas, 2018.

HAFIZ, A.; SUSIANTO, D. **Analysis of Internet Service Quality Using Internet Control Message Protocol**. Journal of Physics: Conference Series. **Anais**...2019

HARTERT, R. et al. **A Declarative and Expressive Approach to Control Forwarding Paths in Carrier-Grade Networks**. Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication. **Anais**...New York, NY, USA: ACM, 17 ago. 2015Disponível em: <https://dl.acm.org/doi/10.1145/2785956.2787495>

HASHEM, I. A. T. et al. The role of big data in smart city. **International Journal of Information Management**, v. 36, n. 5, p. 748–758, 2016.

HONG, C. Y. et al. **Achieving high utilization with software-driven WAN**. SIGCOMM 2013 - Proceedings of the ACM SIGCOMM 2013 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication. **Anais**...New York, NY, USA: ACM, 27 ago. 2013Disponível em: <https://dl.acm.org/doi/10.1145/2486001.2486012>

JAIN, S. et al. **B4: Experience with a globally-deployed software defined WAN**. SIGCOMM 2013 - Proceedings of the ACM SIGCOMM 2013 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication. **Anais**...New York, NY, USA: ACM, 27 ago. 2013Disponível em: <https://dl.acm.org/doi/10.1145/2486001.2486019>

JALAPARTI, V. et al. **Dynamic Pricing and Traffic Engineering for Timely Inter-Datacenter Transfers**. Proceedings of the 2016 ACM SIGCOMM Conference. **Anais**...New York, NY, USA: ACM, 22 ago. 2016Disponível em: <https://dl.acm.org/doi/10.1145/2934872.2934893>

KOPONEN, T. et al. **Onix: A distributed control platform for large-scale production networks**. Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2010. **Anais**...Vancouver, BC, Canada: USENIX Association, 2019

KOZMETSKY, G.; SMILOR, R. W.; GIBSON, D. V. **The Technopolis phenomenon : smart cities, fast systems, global networks**. Lanham, Maryland, USA: Rowman & Littlefield Publishers Lanham, Md, 1992.

KREUTZ, D. et al. Software-defined networking: A comprehensive survey. **Proceedings of the IEEE**, v. 103, n. 1, p. 14–76, jan. 2015.

LAISSAOUI, C. et al. A measurement of the response times of various OpenFlow/SDN controllers with CBench. **Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA**, v. 2016- July, p. 0–1, 2016.

LINUX FOUNDATION. **What is Open vSwitch?** Disponível em: <https://docs.openvswitch.org/en/latest/intro/what-is-ovs/>. Acesso em: 6 maio. 2021.

LUCIANI, C. **From MPLS to SD-WAN : Opportunities , Limitations and Best Practices**. [s.l.] KTH ROYAL INSTITUTE OF TECHNOLOGY SCHOOL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, 2019.

MCKEOWN, N. et al. OpenFlow. **ACM SIGCOMM Computer Communication Review**, v. 38, n. 2, p. 69–74, mar. 2008a.

MCKEOWN, N. et al. OpenFlow: Enabling Innovation in Campus Networks. **ACM SIGCOMM Computer Communication Review**, v. 38, n. 2, p. 69–74, mar. 2008b.

MEHMOOD, Y. et al. Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. **IEEE Communications Magazine**, v. 55, n. 9, p. 16–24, 2017.

METZLER, A. **The 2015 Guide to WAN Architecture & Design**. [s.l: s.n.]. Disponível em: <http://www.webtorials.com/main/resource/papers/webtorials/2015-Guide-Wan-Architecture/2015_Guide_to_WAN_Architecture_and_Design.pdf>.

MICHEL, O.; KELLER, E. **SDN in wide-area networks: A survey**. 2017 4th International Conference on Software Defined Systems, SDS 2017. **Anais**...IEEE, maio 2017Disponível em: <http://ieeexplore.ieee.org/document/7939138/>

MICROCITY. **SD-WAN: entenda porque essa tecnologia é essencial para sua empresa - Microcity**. Disponível em: <https://www.microcity.com.br/sd-wan-entenda-porque-essa-tecnologia-e-essencial-para-sua-empresa/>. Acesso em: 30 mar. 2020.

MORALES, L. V.; MURILLO, A. F.; RUEDA, S. J. **Extending the floodlight controller**. Proceedings - 2015 IEEE 14th International Symposium on Network Computing and Applications, NCA 2015. **Anais**...2016

NAM, H. et al. **Towards QoE-aware video streaming using SDN**. 2014 IEEE Global Communications Conference. **Anais**...IEEE, dez. 2014Disponível em: <http://ieeexplore.ieee.org/document/7036990/>

RAGHAVAN, B. et al. **Software-defined internet architecture: Decoupling architecture from infrastructure**. Proceedings of the 11th ACM Workshop on Hot Topics in Networks, HotNets-11. **Anais**...New York, New York, USA: ACM Press, 2012Disponível em: <http://dl.acm.org/citation.cfm?doid=2390231.2390239>

RASPBERRY PI FOUNDATION. **Raspberry Pi Documentation**. Disponível em: <https://www.raspberrypi.org/documentation/faqs/>. Acesso em: 6 maio. 2021.

RATHORE, S. **SD-WAN vs MPLS: Pros & Cons (in 2020)**. Disponível em: <https://www.taraspan.com/blog/sd-wan-vs-mpls/>. Acesso em: 5 maio. 2021.

REDAÇÃO VIVO MEU NEGÓCIO. **Como a virtualização de rede pode impactar o seu negócio?** Disponível em: <https://vivomeunegocio.com.br/conteudos-gerais/expandir/virtualizacao-rede/>. Acesso em: 5 maio. 2021.

REGO, A. et al. Software Defined Network-based control system for an efficient traffic management for emergency situations in smart cities. **Future Generation Computer Systems**, v. 88, p. 243–253, 2018.

SALMAN, O. et al. SDN controllers: A comparative study. **Proceedings of the 18th Mediterranean Electrotechnical Conference: Intelligent and Efficient Technologies and Services for the Citizen, MELECON 2016**, n. April, 2016.

SHUHAO LIU; BAOCHUN LI. On scaling software-Defined Networking in wide-area networks. **Tsinghua Science and Technology**, v. 20, n. 3, p. 221–232, jun. 2015.

SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. Florianópolis: [s.n.]. Disponível em: <http://cursos.unipampa.edu.br/cursos/ppgcb/files/2011/03/Metodologia-da-Pesquisa-3a-edicao.pdf>.

SINGH AUJLA, G.; JINDAL, A.; KUMAR, N. EVaaS: Electric vehicle-as-a-service for energy trading in SDN-enabled smart transportation system. **Computer Networks**, v. 143, p. 247–262, 2018.

SOMMERVILLE, I. **Engenharia de Software**. 9. ed. São Paulo: Pearson Prentice Hall, 2011.

TANTISARKHORNKHET, P.; WERAPUN, W. **QLB: QoS routing algorithm for Software-Defined Networking**. 2016 International Symposium on Intelligent Signal Processing and Communication Systems, ISPACS 2016. **Anais**...2017

THE TARASPAN BLOG. **SD-WAN: The Definitive Guide (2020 Update)**. Disponível em: <https://www.taraspan.com/blog/sd-wan-the-definitive-guide/>. Acesso em: 29 abr. 2021.

TOKOH, M. **Sonoff Pow R2 User Guide**. Disponível em: <https://ewelink.coolkit.cc/?p=1567>. Acesso em: 14 out. 2021.

TOSTES, F. **Por que vale a pena migrar do modelo MPLS tradicional para SD-WAN?** Disponível em: <https://thehack.com.br/por-que-vale-a-pena-migrar-do-modelo-mpls-tradicional-para-sd-wan/>. Acesso em: 5 maio. 2021.

TRADELENS. Solution Brief. p. 1–11, 2019.

VMWARE. **The Evolution of WAN Architecture**. Palo Alto, CA: VMware, Inc, 2019.

VMWARE, I. **VMware SD-WAN Edge platform specifications**. Palo Alto, CA: [s.n.]. Disponível em: <https://wan.velocloud.com/rs/098-RBR-178/images/sdwan-927-edge-net-intell-ds-0920.pdf>. Acesso em: 20 jun. 2021.

YAN CHEN, T. F. AND N. Y. QoS Requirements of Network Applications on the Internet. **Information ● Knowledge ● Systems Management 4 (2004) 55–76 55 IOS Press**, v. 34, n. 4, p. 55–66, 30 ago. 2004.

YANG, Z. et al. Software-defined wide area network (SD-WAN): architecture, advances and opportunities. **Proceedings - International Conference on Computer Communications and Networks, ICCCN**, v. 2019- July, 2019a.

YANG, Z. et al. **Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities**. 2019 28th International Conference on Computer Communication and Networks (ICCCN). **Anais**...IEEE, jul. 2019bDisponível em: <https://ieeexplore.ieee.org/document/8847124/>

YIN, X. et al. **A Control-Theoretic Approach for Dynamic Adaptive Video Streaming over HTTP**. Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication. **Anais**...New York, NY, USA: ACM, 17 ago. 2015Disponível em: <https://dl.acm.org/doi/10.1145/2785956.2787486>

ZUO, X. et al. Low-Latency Networking: Architecture, Techniques, and Opportunities. **IEEE Internet Computing**, v. 22, n. 5, p. 56–63, set. 2018.

9 Apêndices

Instalação dos *softwares* no Raspberry pi-ovs01:

Instalando o protocolo de descoberta de rede (LLDP) e monitoração (SNMP):

```
apt-get install lldpd snmp
```

Instalação do Open vSwitch no Raspberry PI usando Ubuntu Server 20.04.2 LTS:

```
sudo apt-get install openvswitch-switch
```

Adicionando a interface *bridge* ao OpenvSwitch:

```
ovs-vsctl add-br ovs-br0
```

Adicionando a interface cliente ao OpenvSwitch:

```
ovs-vsctl add-port ovs-br0 eth0
```

Adicionando um IP de gerência à *bridge* no OpenvSwitch

```
ifconfig ovs-br0 192.168.100.3/24 up
```

Adicionando um IP ponto a ponto na interface do circuito MPLS:

```
ip add add dev eth2 10.0.1.1/24
```

Adicionando um IP na interface do circuito de Internet banda larga:

```
ip add add dev eth1 192.168.1.200/24
```

Criando um túnel GRE e adicionando na bridge para alcançar o segundo Raspberry (PI-OVS02) através da Internet:

```
ovs-vsctl add-port ovs-br0 gre1 -- set interface gre1 \
type=gre options:remote_ip=179.125.169.176
```

Criando um túnel GRE e adicionando na bridge para alcançar o segundo Raspberry (PI-OVS02) através da rede MPLS:

```
ovs-vsctl add-port ovs-br0 gre2 -- set interface gre2 \
type=gre options:remote_ip=10.0.1.2
```

Ativando o protocolo de redundância Spanning Tree:

```
ovs-vsctl set bridge ovs-br0 stp_enable=true
```

Configurando o controlador SDN:

```
ovs-vsctl set-controller ovs-br0 tcp:18.220.36.84:6653
```

Ativando fluxo de dados do protocolo Openflow

```
ovs-vsctl set bridge ovs-br0 protocols=OpenFlow13
```

Instalação dos *softwares* no Raspberry pi-ovs02:

Instalando o protocolo de descoberta de rede (LLDP) e monitoração (SNMP):

```
apt-get install lldpd snmp
```

Instalação do Open vSwitch no Raspberry PI usando Ubuntu Server 20.04.2 LTS:

```
sudo apt-get install openvswitch-switch
```

Adicionando a interface *bridge* ao OpenvSwitch:

```
ovs-vsctl add-br ovs-br0
```

Adicionando a interface cliente ao OpenvSwitch:

```
ovs-vsctl add-port ovs-br0 eth0
```

Adicionando um IP de gerência à *bridge* no OpenvSwitch

```
ifconfig ovs-br0 192.168.100.4/24 up
```

Adicionando um IP ponto a ponto na interface do circuito MPLS:

```
ip add add dev eth2 10.0.1.2/24
```

Adicionando um IP na interface do circuito de Internet banda larga:

```
ip add add dev eth1 192.168.1.200/24
```

Criando um túnel GRE e adicionando na bridge para alcançar o segundo Raspberry (PI-OVS01) através da Internet:

```
ovs-vsctl add-port ovs-br0 gre1 -- set interface gre1 \
type=gre options:remote_ip=201.77.127.129
```

Criando um túnel GRE e adicionando na bridge para alcançar o segundo Raspberry (PI-OVS02) através da rede MPLS:

```
ovs-vsctl add-port ovs-br0 gre2 -- set interface gre2 \
type=gre options:remote_ip=10.0.1.1
```

Ativando o protocolo de redundância Spanning Tree:

```
ovs-vsctl set bridge ovs-br0 stp_enable=true
```

Configurando o controlador SDN:

```
ovs-vsctl set-controller ovs-br0 tcp:18.220.36.84:6653
```

Ativando fluxo de dados do protocolo Openflow:

```
ovs-vsctl set bridge ovs-br0 protocols=OpenFlow13
```

Instalando o controlador SDN Floodlight

Instalando as dependências:

```
sudo apt-get install build-essential openjdk-7-jdk ant
maven python-dev eclipse
```

Instalando o controlador Floodligth:

```
git clone git://github.com/floodlight/floodlight.git
cd floodlight
git submodule init
git submodule update
ant

sudo mkdir /var/lib/floodlight
sudo chmod 777 /var/lib/floodlight
```

Atualizando a versão do controlador SDN:

```
cd floodlight
git pull origin master
git submodule init
git submodule update
```

Executando o Controlador SDN:

```
java -jar target/floodlight.jar
```

Listar os dispositivos que o Floodlight reconheceu via API:

```
curl http://localhost:8080/wm/device/ | python -m json.tool
```