CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA

PAULA SOUZA FACULDADE DE TECNOLOGIA DE

INDAIATUBA DR. ARCHIMEDES LAMMOGLIA

TECNOLOGIA EM REDES DE COMPUTADORES

SAMUEL FELIPE DE BRITO PROENÇA

REDES DEFINIDAS POR *SOFTWARE*: UM ESTUDO ANALÍTICO DE SUA APLICAÇÃO E MECANISMOS

Indaiatuba

2024

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA

PAULA SOUZA FACULDADE DE TECNOLOGIA DE

INDAIATUBA DR. ARCHIMEDES LAMMOGLIA

TECNOLOGIA EM REDES DE COMPUTADORES

SAMUEL FELIPE DE BRITO PROEÇA

REDES DEFINIDAS POR SOFTWARE: UM ESTUDO ANALITICO DE SUA APLICAÇÃO E MECANISMOS

Projeto de Trabalho de Graduação apresentado por Samuel Felipe de Brito Proença como pré-requisito parcial para a conclusão do Curso Superior de Tecnologia em Redes de Computadores, da Faculdade de Tecnologia de Indaiatuba, elaborado sob a orientação do Prof. André Luiz Silva.

Indaiatuba
2024

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA

PAULA SOUZA FACULDADE DE TECNOLOGIA DE

INDAIATUBA DR. ARCHIMEDES LAMMOGLIA

TECNOLOGIA EM REDES DE COMPUTADORES

SAMUEL FELIPE DE BRITO PROENÇA

Banca Avaliadora:

Prof. André Luiz Silva	**Orientador**
Prof.	
Prof.	

Data da defesa: ___/___/___

DEDICATORIA

Dedico este trabalho a minha família, que muito me apoiou e me incentivou a chegar neste ponto tão perto de me formar, foi uma jornada difícil, mas conseguimos.

AGRADECIMENTOS

Primeiramente, agradeço a Deus por mais este feito, Aos professores André Luiz Silva e ao Dr. Eng. Sergio Gustavo Medina Pereira pela orientação de ambos durante o desenvolvimento deste trabalho, agradeço também meus amigos que me incentivaram a escrever em especial ao Bruno e a Stefanie e a minha família que me apoiou nesse processo até o presente momento.

RESUMO

No cenário presente com o crescente de redes de computadores evoluindo diariamente, com cada vez mais soluções, aplicações disponíveis na *web*, o gerenciamento de recursos, tal como agilidade, flexibilidade e programabilidade das redes se faz mais e mais importante, soluções diversas foram adotadas para tentar resolver esses problemas e atender a demanda que se faz presente. Este trabalho explora o conceito de redes definidas por *software* com o objetivo de esclarecer este tópico para os leitores, tornando claro o que é e como se difere de uma rede de computadores tradicional. Os temas que se destacaram como de grande relevância para a compreensão geral das redes de computadores modernas foram discutidos. As redes *SDN* vem apresentando significativa evolução dia após dia e a cada nova solução implementada é possível se observar uma ampla gama de possibilidades em aplicações, soluções de segurança, flexibilidade, agilidade e compatibilidade. No entanto, devido ao fato de ainda ser uma estratégia em desenvolvimento também apresenta certos desafios para alcançar seu potencial máximo.

LISTA DE FIGURAS

LISTA DE AREVIATURAS

API	Application Programming Interface
ARPANET	Advanced Research Project Agency Network
BGP	Border Gateway Protocol
ICMP	Internet Control Message Protocol
IOT	Internet of Things
ISO	International Standards Organization
IP	Internet Protocol
LAN	Local Area Network
MAN	Metropolitan Area Network
MIB	Management Information Base
NFV	Network Function Virtualization
NIC	Network Interface Card
ONF	Open Network Foundation
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAN	Personal Area Network
QoS	Quality of Service
SA	Source Address
SDN	Software Defined Networking
SD-WAN	Software Defined Wide Area Networking
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
VU	Victory University
WAN	Wide Area Network

SUMÁRIO

INTRODUÇÃO

A alguns anos atrás as pessoas precisavam se locomover até a agência de correios mais próxima para realizar o envio de um pacote, o encaminhamento de mensagens era feito de forma totalmente manual e demorava para que uma mensagem fosse encaminhada de um ponto a outro. Quanto maior a distância entre os prontos, maior o tempo de espera para que o remetente recebesse o pacote. Isso, claro, quando a entrega era realizada com sucesso. Durante a Guerra Fria o Departamento de Defesa dos Estados Unidos iniciou um projeto de pesquisa chamado *ARPANET (Advanced Research Project Agancy Network).* A intenção inicial deste projeto de pesquisa era criar uma rede de computadores que pudesse resistir a falhas de comunicação mesmo durante ataques, com a ideia de descentralizar as informações por meio de computadores, de forma que se um nó fosse danificado, a informação continuaria a fluir através de rotas alternativas. Em 1969, a primeira mensagem foi enviada entre dois computadores conectados a *ARPANET*, sendo o início do nascimento do que hoje é conhecido como *Internet.*

Como citado por (GUILHEN, BRUNO *et. al*., 2021, p 1)

> "Além de sobrecarregar a infraestrutura de roteadores da Internet, os novos serviços possuem requisitos mais elevados de flexibilidade, confiabilidade e escalabilidade exigindo um novo paradigma de encaminhamento de pacotes na rede, bem como, novos elementos de segurança (KREUTZ, et al., 2015). Por isso, diversas instituições acadêmicas e a indústria se debruçaram para estudar uma solução para a Internet do futuro, uma nova arquitetura de rede conhecida como "Redes Definidas por Software (SDN)" (OKTIAN, LEE, LEE, & LAM, 2017). "

Com o crescimento da demanda por processos mais eficientes nas redes de computadores, tornou-se necessário pesquisar e desenvolver abordagens que otimizem a utilização dos recursos e funcionamento das redes. A ideia era unir maquinas que antes atuavam de forma independente, permitindo que trabalhassem como uma única entidade. Dessa forma, uma supriria a necessidade da outra e não haveria desperdício de recursos ociosos.

Junto a isso, cada vez mais protocolos e mais otimizados eram aplicados para garantir a integridade, eficiência e segurança das comunicações. Sendo assim, as redes de computadores e *Internet* atuais usam uma série de protocolos para sua operacionalização, um exemplo desses protocolos é o *BGP* (*Border Gateway Protocol*) que permite a imposição de muitos tipos de políticas de tráfego entre *SAs* (*Autonomos systems*), "Em

geral as políticas (ou normas) envolvem considerações políticas, econômicas e de segurança e são configuradas manualmente em cada roteador *BGP." (*TANEMBAUM, 2016).

Um Protocolo é um conjunto de regras que ditam como serão as interações dos dispositivos em uma rede, isso será melhor abordado no capitulo 1.1.3, assim como em um evento social existem regras de etiqueta, que são acordos de como se deve comportar e interagir, nas redes de computadores os protocolos desempenham essa função. Os protocolos visam garantir que os dados sejam transmitidos de forma confiável e compreensível entre diferentes dispositivos, operando em diferentes camadas cujas quais tem funções específicas que facilitam a comunicação de ponto a ponto. (TANEMBAUM, 2011).

Um modelo lógico pode ser usado para abstrair uma rede de computadores, o que aumenta a facilidade de compreensão de cada camada da rede, sendo assim, o modelo mais utilizado ainda atualmente é o modelo *OSI (Open System Interconnection)* que retrata uma rede dividida em sete camadas, sendo elas: Física, Enlace, Rede, Transporte, Sessão, Apresentação e aplicação, cada camada do modelo *OSI* é responsável por explicar os detalhes de implementação e para cada camada, uma série de protocolos será aplicada para garantir o funcionamento correto e seguro da rede.

Quando a comunicação ocorre em um único *AS* ou seja, em uma rede interna de uma empresa por exemplo o protocolo de roteamento recomendado é o *OSPF* (*Open Shortest Path First*), o *OSPF* se tornou o padrão nos anos de 1990 e ele se tornou o principal protocolo *gateway* interior. (TANEMBAUM, 2016).

Como dito por (TANEMBAUM, 2016)

> O OSPF funciona transformando o conjunto de redes, roteadores e linhas reais em um grafo orientado, no qual se atribui um custo (distância, retardo etc.) a cada arco. Em seguida, o OSPF calcula o caminho mais curto com base nos pesos dos arcos. Uma conexão serial entre dois roteadores é representada por um par de arcos, um em cada sentido. Seus pesos podem ser diferentes. Uma rede de multiacesso é representada por um nó para a própria rede e por um nó para cada roteador. Os arcos entre o nó da rede e os roteadores têm peso 0 e foram omitidos do grafo.

O uso desses protocolos permitiu a internet continuasse crescendo e operando da melhor forma disponível, porém nos últimos anos, as redes de computadores experimentaram um crescimento exponencial em tamanho, de modo que tem aumentado também a complexidade e demanda de serviços. O desenvolvimento constante das redes

e a necessidade de tornar mais eficiente a administração delas, trouxeram à luz soluções potenciais para este problema. Neste contexto, surgem conceitos como *clusters*, malhas e nuvens.

Um cluster é uma técnica de computação na qual agrupa-se um determinado ou indeterminado número de aparelhos como computadores ou servidores em um mesmo sistema para que trabalhem em conjunto de forma eficiente compartilhando recursos, sendo assim, não sobra nem falta recurso para nem um dos componentes do cluster, uma vez que um componente de *hardware* ajuda a suprir a demanda do outro.

Uma malha por sua vez é um tipo de topologia de rede em que cada nó está conectado a todos os outros nós, assim como em um tecido, a vantagem nesta abordagem é a transmissão eficiente de dados, uma vez que existem várias toras possíveis de ponto a ponto.

De acordo com a descrição da (MICROSOFT, 2024)

> A nuvem não é uma entidade física, mas uma vasta rede de servidores remotos ao redor do globo que são conectados e operam como um único ecossistema. Esses servidores são responsáveis por armazenar e gerenciar dados, executar aplicativos e fornecer conteúdos ou serviços, como transmissão de vídeos, webmail, software de produtividade ou mídias sociais

Ou seja, uma nuvem é uma abstração de componentes físicos, (servidores), unidos para um propósito de realizar e oferecer serviços para outras empresas ou para a empresa dona da arquitetura, a Google por exemplo oferece seus recursos em nuvem para outras empresas e também utiliza em sua própria infraestrutura.

Uma das soluções encontradas é a implementação de Redes definidas por *Software (Software Defined Networking ou SDN)* que tem visto um interesse crescente tanto da indústria quanto da academia, e neste trabalho focaremos em entende-la melhor.

De acordo com (KREUTZ et al., 2015), o *SDN* é uma abordagem inovadora para o gerenciamento de rede que separa o plano de controle do plano de dados, permitindo maior flexibilidade e automação na configuração e gerenciamento da rede. Vários estudos investigaram as vantagens e desvantagens da implementação de *SDN* em diferentes ambientes, como *data centers*, redes corporativas e redes de operadoras.

As Redes Definidas por *Software* (*SDN*) constituem um novo polo para o desenvolvimento de pesquisas em redes, a qual tem ganho maior atenção de parte da comunidade acadêmica e da indústria. Boa parte da atenção tem sido voltada para o padrão *OpenFlow*, um dos elementos que tornaram possível esse enfoque. No entanto, as

SDNs vão além de *OpenFlow*, abrindo novas perspectivas em termos de abstrações, ambientes de controle e aplicações de rede que podem ser desenvolvidas de forma simples e livre das limitações das tecnologias de rede atuais.

Segundo (COMER, 2016), "A partir dos anos de 1970, a comunicação via computador transformou-se em uma parte essencial de nossa infraestrutura. A ligação de computadores em rede é usada em cada aspecto dos negócios." Sendo assim, cria-se uma demanda maior para aplicações mais eficientes das redes, que utilizem melhor a largura de banda e fornecem maior segurança.

Com a crescente dependência das redes para a comunicação e os negócios, emerge esta necessidade por aplicações de rede mais eficientes, porém, a implementação dessas aplicações é desafiadora devido a complexidade inerente das redes de computadores, Como afirma (TANEMBAUM, 2011), "A internet não é de modo algum uma rede, mas sim um vasto conjunto de redes diferentes que utilizam certos protocolos comuns e fornecem determinados serviços comuns". Ou seja, qualquer aplicação de rede deve ser capaz de operar em uma variedade de contextos de rede diferentes, cada um com suas próprias características e desafios.

É aqui que as *SDN*s entram em cena. Elas oferecem uma maneira de administrar essa complexibilidade, permitindo um controle mais específico sobre o comportamento da rede facilitando a implementação de aplicações de rede eficientes.

Diante deste cenário, este projeto de trabalho de graduação visa conceituar as *SDN*s e analisar vantagens e desvantagens da implementação. A motivação para este estudo reside na importância de entender as implicações práticas da adoção do *SDN*, e de fornecer *insights* sobre sua implementação através de revisões literárias, estudo da arte e revisão bibliográfica.

Este trabalho de graduação visa analisar através de uma revisão bibliográfica e do estudo da arte e compreender as diferenças deste tipo de rede com o método tradicional e servir de material de revisão para estudos e trabalhos futuros referentes a esta tecnologia. A motivação para este estudo reside na importância de entender as implicações práticas da adoção do *SDN*, e de fornecer *insights* sobre suas aplicações no dia a dia tal qual questões discutidas de segurança e flexibilidade.

Sendo assim, a primeira metade deste trabalho será dedicada a trazer os conceitos mais presentes das redes de computadores tradicionais, servindo de fundamentação teórica e base para a apresentação dos temas abordados posteriormente tal como base de

comparação, para a aquisição dessas informações foram realizadas pesquisas de artigos e livros da área de redes, os quais apresentarão diferenças e semelhanças com as tecnologias e métodos tradicionais, ao pesquisar sobre o tema usando as palavras chave (*SDN*, redes definidas por software e *Software Defined Networking*) e filtrando os últimos 12 anos, após esta breve introdução o tema de redes definidas por software será aprofundado através de revisões bibliográficas de livros e artigos que se ligam ao tema dos últimos 12 anos, a pesquisa resultou em 2.110 artigos dos quais 13 artigos principais foram usados como peças primordiais na construção deste trabalho com base nos assuntos apresentados, os trabalhos relacionados sobre o tema foram usados com a intenção de trazer ao leitor de forma simples o que é, como funciona e quais são os principais usos nos dias atuais das redes *SDN*, incluindo questões de segurança e flexibilidade.

A segunda metade deste trabalho será dedicada a apresentar, descrever e trazer maior nível de conhecimento referente as redes definidas por *software,* de modo que assim, contribuam para estudos posteriores.

Motivação e Desafios

Com a rápida ascensão das redes de computadores no mundo atual, torna-se importante trazer a discussão sobre melhorias na rede de internet. Visto a ascensão de novas abordagens de gerenciamento de rede, este trabalho toma a iniciativa de trazer uma discussão sobre uma das mais populares abordagens dos últimos anos, as redes definidas por *software.*

Com foco principal no padrão *OpenFlow* que de acordo com (McKeown *et al.*, 2008), foi o grande responsável pela definição do *SDN* como modelo de rede, apenas depois da padronização desse protocolo permitiu-se a criação de uma interface entre o plano de controle e o plano de dados. Segundo a *ONF* (*Open Networking Foundation*) (2016), o *OpenFlow* é o protocolo que atualmente dispõe de maior estudo e investimento.

Relevância

A transformação digital está em andamento em diversos setores, e as redes de computadores desempenham um papel crucial neste processo. As *SDNs* oferecem recursos que facilitam a integração de tecnologias emergentes, como computação em

nuvem, internet das coisas (*IoT Internet of Things*) e redes 5G. Compreender as redes definidas por software pode ajudar a impulsionar a transformação digital e a adotar soluções mais eficientes e flexíveis.

As *SDNs* também têm potencial de aumentar a eficiência e otimização das redes de computadores, permitindo a alocação mais eficiente de recursos, o balanceamento de carga rápida e a rápida adaptação às demandas em constante mudança. A compreensão destes princípios pode ajudar a ajudar também a aumentar a satisfação do usuário e reduzir custos operacionais.

Objetivos

Nesta seção serão apresentados os objetivos geral e específico do trabalho relativos ao problema anteriormente apresentado.

Objetivo geral

Trazer compreensão embasada no estudo da arte e revisões bibliográficas do funcionamento de redes definidas por software.

Objetivo específico

Esta pesquisa tem como objetivo a apresentação e análise de um ambiente de redes definida por software virtual com o intuito de desenvolver uma discussão sobre o tema de modo que se possa comparar as dificuldades de implementação com a abordagem tradicional e promover o conhecimento relacionado a esta tecnologia.

Promover um estudo da arte sobre o tema trazendo maior entendimento para futuros trabalhos relacionados.

Analisar e revisar conteúdos bibliográficos sobre o tema com a intenção de entender a escalabilidade e flexibilidade da rede.

CAPÍTULO 1

1. Fundamentação Teórica

Neste capítulo são apresentados os componentes a serem utilizados no desenvolvimento deste trabalho, além da sua fundamentação teórica, a fim de auxiliar no seu entendimento, com base em artigos acadêmicos que possuem alguma correlação com este trabalho.

1.1 Introdução as Redes de Computadores

A seguir serão apresentados os conceitos básicos: incluindo arquitetura, camadas, protocolos e dispositivos de rede.

Uma rede de computadores é um conjunto de dispositivos eletrônicos, chamados de nós, interconectados por meio de canais de comunicação para compartilhar informações. Esses dispositivos podem incluir Computadores, Roteadores, Servidores, Switches, Impressoras e outros dispositivos de eletrônicos. O principal objetivo de uma rede é permitir que os usuários possam trocar pacotes de dados de forma segura e eficiente ou seja, seus dados devem permanecer protegidos e o encaminhamento deve ser realizado em tempo hábil para que o destinatário receba a mensagem corretamente. (TANEMBAUM, 2016).

As Redes de Computadores, ou seja, o conjunto de vários equipamentos conectados que se comunicam e trocam informações através de nós, podem ser divididas de várias formas, como sua escala geográfica, topologia, arquitetura e protocolos de comunicação utilizados.

Uma rede de computadores se baseia em protocolos que são responsáveis por determinar como os dados são transmitidos e recebidos, assim como também garante maior segurança e eficiência na comunicação entre os dispositivos, os dispositivos que são o *hardware* físico da rede, como o computador, roteador, switch etc. E a topologia, que é a forma como os dispositivos estão conectados entre eles.

1.1.1 **Arquitetura de Redes**

De acordo com (TANEMBAUM, 2016), “um conjunto protocolos e camadas é conhecido como arquitetura de rede”. Uma arquitetura de rede depende então das regras de comunicação e comportamento passados para os dispositivos e das camadas da rede. É possível aqui fazer uma alegoria com um hotel, pense em cada camada como um andar cada andar atende clientes distintos e oferece serviços distintos, por exemplo, no térreo teria a recepção, cuja função é recepcionar e fazer os *checkin* e *checkout* dos clientes do hotel, em outro andar poderia ter um restaurante que pode atender clientes que estão passando uma temporada no hotel, em outros andares os quartos, cuja função é de ser um espaço onde os hospedes passarão suas noites, outro para lazer, outro para esportes, etc.

Sendo assim, se cada uma serve a um propósito e é por onde os clientes trafegam, os protocolos são as regras e normas deste hotel, para que cada serviço funcione perfeitamente bem, eles ditarão as normas deste hotel, de modo em que se os clientes quiserem ir de um andar a outro precisarão seguir determinado caminho, se quiserem um quarto, antes precisão realizar o *check-in,* se quiserem serviço de quarto precisaram solicitar com antecedência, não poderiam andar apenas de sunga por exemplo no saguão ou correr perto da piscina etc. Normas e regras cujas quais servem ao propósito de manter todos os setores do hotel em ordem e segurança, da mesma forma que os funcionários seguiriam certos modos ao recepcionar os clientes, falariam certas línguas para clientes de outras regiões e atuariam diligentemente em certos horários para manter o processo eficiente.

Protocolos de rede atuam por camada, que seguindo o modelo *OSI* que abstrai as camadas de forma que facilite o entendimento, são sete no total: Física, Enlace, Rede, Transporte, Sessão, Apresentação e Aplicação.

Essas camadas e os seus protocolos serão melhor desenvolvidos nos subcapítulos posteriores.

1.1.1 **Camadas de Rede**

Como dito anteriormente, pode-se imaginar uma camada de rede como andares de um hotel no qual, cada andar serve a uma função. Para exemplificar o conceito, a figura 1 apresenta o modelo *OSI* o qual é utilizado como forma de abstrair as camadas de uma rede para facilitar o entendimento geral.

Figura 1 - Modelo OSI

Fonte: Platzi.com

Neste modelo, são apresentados os conceitos de cada camada de forma ilustrativa para facilitar ao leitor, as camadas da rede operam de uma forma a qual cada camada se comunica diretamente com a camada de baixo para cima ou de cima para baixo a depender

da função em execução, para que desta forma os pacotes sejam encaminhados corretamente e de forma segura.

Cada camada deste modelo exerce uma função distinta, de modo que a operação em conjunto dessas camadas e dos protocolos que cada uma possui proporcionam o funcionamento correto da rede. O modelo divide a rede em sete camadas, sendo elas:

Camada Física: De acordo com (TANEMBAUM, 2011). Na camada física é realizada a transmissão de dados puros através de *bits* puros que simbolizam 0 e 1, essa transmissão ocorre através de um canal de comunicação (os cabos de rede) e é desenvolvido de modo que o bit que foi enviado por um dos lados seja recebido da mesma forma que saiu, ou seja, um bit 1 seja recebido exatamente como um bit 1 no outro dispositivo. (TANEMBAUM, op. cit.), "Os aspectos de design têm muito a ver com interfaces mecânicas, elétricas e de temporização, além do meio físico de transmissão, que está sob a camada física.".

Voltando a analogia do hotel, o edifício é envolto em muitos detalhes, como a estrutura física do prédio (as interfaces mecânicas), e o agendamento de quando os quartos devem ser limpos e quando o café da manhã deve ser servido (a temporização). O meio físico de transmissão seria então como os corredores e elevadores deste hotel, sendo assim, é a infraestrutura real e tangível que permite que o hotel funcione.

Camada de Enlace de Dados: Esta camada é responsável por estabelecer e manter um enlace entre os dispositivos, assegurando que os dados sejam transmitidos de maneira precisa e eficiente além de verificar e corrigir erros o que garante que os dados sejam recebidos corretamente.

Aqui se enviam os dados que sertão convertidos em bits, adiciona-se o endereço físico da camada de rede e chega-se a camada de rede.

Camada de Rede: Aqui é onde ocorre o controle das rotas e sub redes, os caminhos por onde os dados serão encaminhados, essas rotas podem ser baseadas em tabelas estáticas pré-definidas que são profundamente ligadas a rede e raramente sofrem

alterações ou tabelas dinâmicas que são determinadas para cada pacote de modo que reflita a carga atual da rede (TANEMBAUM, 2011).

Algumas vezes pode ocorrer um grande encaminhamento de diversos pacotes em uma mesma sub rede ao mesmo tempo e dividindo o mesmo caminho, de modo que se possa gerar um gargalo ou congestionamento. Para que isso não ocorra, o controle é realizado já na camada de rede, estabelecendo novas rotas e administrando as já existentes.

De acordo com (TANEMBAUM, 2011, p. 46)

> Quando um pacote tem de viajar de uma rede para outra até chegar a seu destino, podem surgir muitos problemas. O endereçamento utilizado pela segunda rede pode ser diferente do que é empregado pela primeira rede. Talvez a segunda rede não aceite o pacote devido a seu tamanho excessivo. Os protocolos podem ser diferentes e assim por diante. Cabe à camada de rede superar todos esses problemas, a fim de permitir que redes heterogêneas sejam interconectadas.

Camada de Transporte: "Esta camada é responsável por aceitar os dados da camada acima dela, dividi-los em unidades menores caso necessário, repassar essas unidades à camada de rede e assegurar que todos os fragmentos chegarão corretamente a outra extremidade" (TANEMBAUM, 2011).

Ou seja, nesta camada ocorre o recebimento dos dados transmitidos na camada de transporte, dados esses que são cuidadosamente verificados, e divididos em pacotes que possam ser transmitidos de um ponto a outro na rede sem a perda significativa de informações, isso também resulta em uma maior eficiência na transmissão desses dados e segurança. Além disso, essa camada também determina o tipo de serviço que será fornecido na camada de sessão.

Camada de Sessão: Essa camada é responsável por estabelecer a conexão entre diferentes usuários e manter certo controle da conexão, para que as duas partes não possam executar a mesma função simultaneamente, estejam sincronizadas e mantêm o controle de quem deve transmitir a cada momento. (TANEMBAUM, 2011).

Camada de Apresentação: Aqui é estabelecido o controle e o gerenciamento da estrutura de dados e como os dados são apresentados para cada máquina e permite a definição e o intercâmbio de estruturas de dados de nível mais alto, uma vez que elas

podem dispor de diferentes representações de dados, sendo assim, para que não haja problemas, a estrutura desses dados pode ser definida de forma abstrata, juntamente com uma codificação padrão que será usada durante a conexão. (TANEMBAUM, 2011)

Camada de Aplicação: Nesta camada são aplicados protocolos de comunicação que permitem a transferência de arquivos de cliente para servidor e vice e versa, como o protocolo *HTTP* (*HyperText Transfer Protocol*), que é utilizado pelo navegador quando há a busca por uma página *web* através do nome no servidor, e então a página é transmitida de volta.

Sendo assim, cada uma das camadas apresentadas exerce seus papéis de modo que todas elas em conjunto possam cumprir seus papeis de modo ideal e isso depende de um padrão exercido. Como dito por (TANEMBAUM, p.43, 2013) “Existem muitos fabricantes de redes, cada qual com suas próprias ideias sobre como as coisas devem ser feitas. Sem coordenação, haveria um caos completo, e os usuários nada conseguiriam fazer”.

Sendo assim, fez-se visível a necessidade de se criar uma padronização para que não haja um caos generalizado nas redes modernas, para tanto a indústria inclinou-se para a criação de padrões de rede que além de permitirem a comunicação entre diferentes computadores, também trazem bons padrões para os produtos que aderem a essas regras. Isso gera um aumento no mercado e seguindo com o que foi dito por (TANEMBAUM, p.43, 2013). “Um mercado mais amplo estimula a produção em massa, proporciona economia de escala no processo de produção, melhores implementações e outros benefícios que reduzem o preço e aumentam mais ainda a aceitação do produto”.

1.1.2 **Protocolos de Rede**

Agora que o conceito de camadas ficou mais claro, é necessário entender também o que são protocolos e como atuam em uma rede. Como dito anteriormente neste capítulo, é possível imaginar os protocolos como as regras, linguagem e procedimentos do hotel, eles atuarão como peça fundamental em conjunto com as camadas da rede para garantir o funcionamento dela.

Os protocolos são projetados para a realização de tarefas específicas que operam em uma ou mais camadas do modelo *OSI* e para cada camada um conjunto de protocolos é aplicado. Cada protocolo tem um conjunto de regras e procedimentos que devem ser seguidos e definem como os dados são formatados, transmitidos, recebidos ou reconhecidos. Esses protocolos determinam também como as informações são processadas para cada camada, (andar do hotel), e como são transmitidas entre elas.

Os protocolos mais comuns por camada são:

Camada de Enlace de Dados: São utilizados nesta camada protocolos como *Ethernet, PPP* (*Point-to-Point Protocol*) e *HDLC* (*High-Level Data Link Control*), esses protocolos são responsáveis por fornecer uma interface confiável para a transmissão de quadros, gerenciam erros e controlam o fluxo o acesso.

Camada de Rede: São utilizados aqui os protocolos *IP* (*Internet Protocol*), *ICMP* (*Internet Control Message Protocol*), e *IGMP* (*Internet Group Management Protocol*). Que são responsáveis pelos endereçamentos de pacotes através de múltiplas redes e o controle do congestionamento da rede.

Camada de Transporte: *TCP* (*Transmission Control Protocol*) e *UDP* (*User Data Protocol*). Cujas funções são respectivamente fornecer uma comunicação confiável, controle de fluxo, segmentação e retransmissão de dados. Embora o *UDP* não ofereça uma comunicação confiável, controle de fluxo ou retransmissão ele é mais rápido.

Camada de Aplicação: Nesta camada uma grande gama de protocolos pode ser observada, eles são responsáveis por permitir que os aplicativos se comuniquem através da rede, sendo eles *HTTP* (que é usado para transferir páginas *web* e outros recursos na

World Wide Web, *SMTP (Simple Mail Transfer Protocol)*que é utilizado para o envio de *e-mails*, *FTP (File Transfer Protocol)* responsável pelo encaminhamento de arquivos, *DNS (Domain Name System)* que traduz nomes de domínios, *Telnet* que permite acesso remoto a servidores e dispositivos, *SSH (Secure Shell)* que fornece acesso seguro a servidores via linha de comando e *SNMP(Simple Network Management Protocol)* que gerencia e monitora os dispositivos de rede.

Como dito anteriormente, cada protocolo atua aplicando um conjunto de regras que são seguidas em uma ou mais camadas do modelo *OSI*, uma ilustração clara disso como analogia seria: um homem chega a um hotel, neste hotel primeiro ele precisa fazer o *check-in* pois reservou com antecedência seu quarto, então ele se dirige primeiramente ao saguão e questiona as(os) atendentes para verificar se seu quarto já está livre, as(os) atendentes por sua vês, vão verificar se as informações do cliente estão no sistema de acordo e de acordo, irão verificar que quarto é este que o mesmo reservou e se está ou não desocupado, no caso de estar desocupado será verificado se ele já está limpo e preparado para o cliente ser encaminhado para ele, caso todas as condições sejam cumpridas e seja seguro, alguém será encarregado de leva-lo junto a suas malas para o quarto, o caminho então será passado para ele, assim como os horários do hotel e lugares que estão disponíveis para o acesso dele ou de outros clientes.

Seguindo essa analogia, podemos dizer então que o “homem” seriam os dados ou pacotes, o *check-in* pode representar a camada de aplicação onde os dados são separados para a transmissão, o saguão e os(as) atendentes representam a camada de transporte pois verificam se a comunicação pode ser estabelecida, a camada de rede pode ser vista como a verificação de se o quarto está ou não limpo e determina a melhor rota/caminho para os dados “homem”, a camada de link de dados ou enlace, pode ser vista como o encarregado de levar as bagagens do “homem” pois transmite os dados ao próximo nó na rede ou seguindo a analogia, as malas para o próximo quarto, e o caminho que o homem vai percorrer, os horários e ligares disponíveis para acesso podem ser vistos como a camada física.

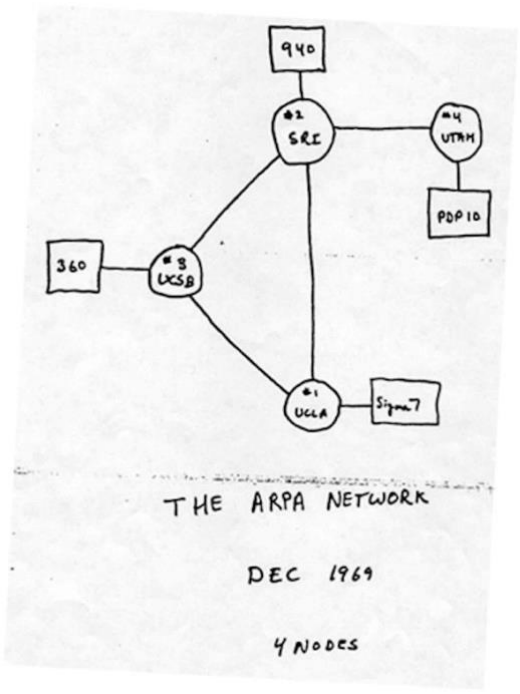
Todos estes procedimentos são realizados e administrados pelos protocolos aplicados a rede, e para tanto, é necessário também entender a topologia da rede, para que assim possa-se definir as melhores praticas rotas e protocolos a serem aplicados, o que será melhor explorado no subcapitulo subsequente

1.1.3 **Topologias de Rede**

Uma topologia de rede é o nome que se dá a forma como se organizam diferentes computadores/dispositivos em uma rede de computadores. Imagine que a rede é uma cidade e que cada dispositivo nessa cidade é uma casa. A “topologia” seria o mapa dessa cidade, mostrando como cada casa está conectada a outra através das estradas (os cabos de rede).

No início de tudo, durante a criação da *ARPANET* um modelo visual de topologia foi desenhado para representar a comunicação entre os computadores na rede, nessa época ainda não eram utilizados roteadores ou switches, então os próprios computadores trabalhavam na transmissão de dados e encaminhamento de pacotes dentre eles. A figura 2 apresenta a representação ilustrada na época:

Figura 2 - Ilustração que representa a *ARPANET*



Fonte: TheConversation.com, 2016

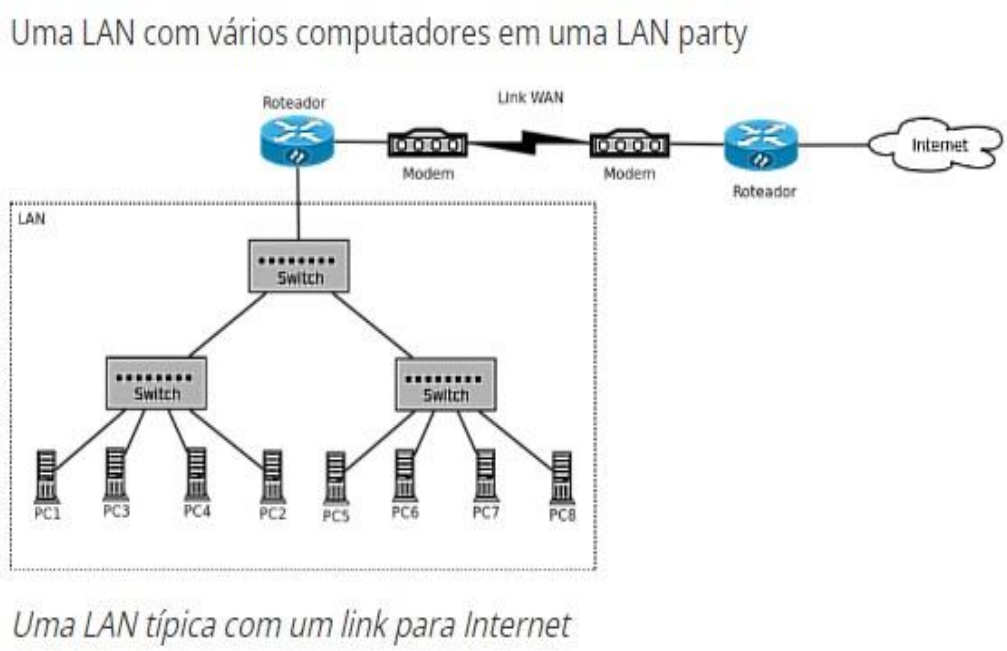
Hoje em dia as topologias evoluíram utilizando de outros dispositivos para a realização dessa carga de trabalho que antes era dada aos computadores interconectados. Ao mesmo tempo em que se passa a usar outros componentes na rede para a realização de tarefas específicas como roteamento, também foram criadas outras estruturas de

organização e disposição de dispositivos, essas estruturas são conhecidas como topologias. As Topologias mais comuns incluem:

• Por escala geográfica:

(Local Area Network ou LAN): Uma rede de acesso local, comumente montada dentro de um prédio por exemplo, nesta rede os dados não são compartilhados para fora e sua estrutura se concentra no edifício em que ela foi montada exemplo: A rede de uma escola seria caracterizada como uma rede LAN ou também chamada de rede de acesso local, onde não se é possível acessar o sistema da rede de fora. Na figura 3 é mostrado um exemplo de uma rede LAN típica com um link para internet.

Figura 3 - Exemplo de uma rede LAN

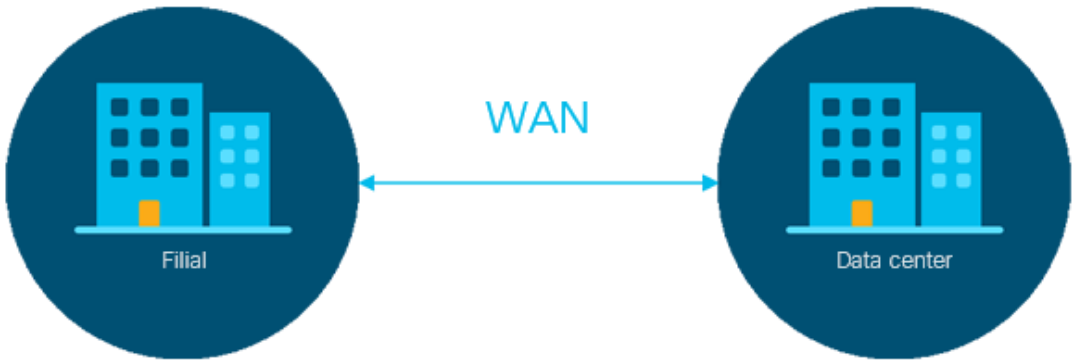


Fonte: IFSC.EDU, 2023

(Wide Area Network ou WAN): Uma rede de área larga, é montada a grandes distancias conectando um grande número de dispositivos pelo caminho, de modo que possa ser montada mesmo entre países, a Internet é uma WAN que conecta todos os dispositivos de rede do mundo uns aos outros e aos servidores da rede, em sua maioria por cabos, mas também pode conectar através de sinais de rádio wi-fi Em diversos países pelo mundo existem servidores conectados uns aos outros por meio de cabos muitas vezes submarinos, No Brasil mesmo a conexão com a Europa se tem por meio de cabos submarinos, os quais se conectam a servidores aqui e lá cruzando o oceano pacífico.

Este tipo de conexão permite o envio de dados de grandes distâncias, no geral sem a perca destes pacotes que são retransmitidos de servidor em servidor, seguindo a rota de menor caminho, o que permite uma conexão global destes dispositivos. Na figura 4 é exibido um exemplo de uma WAN. (KUROSE e ROSS, 2016)

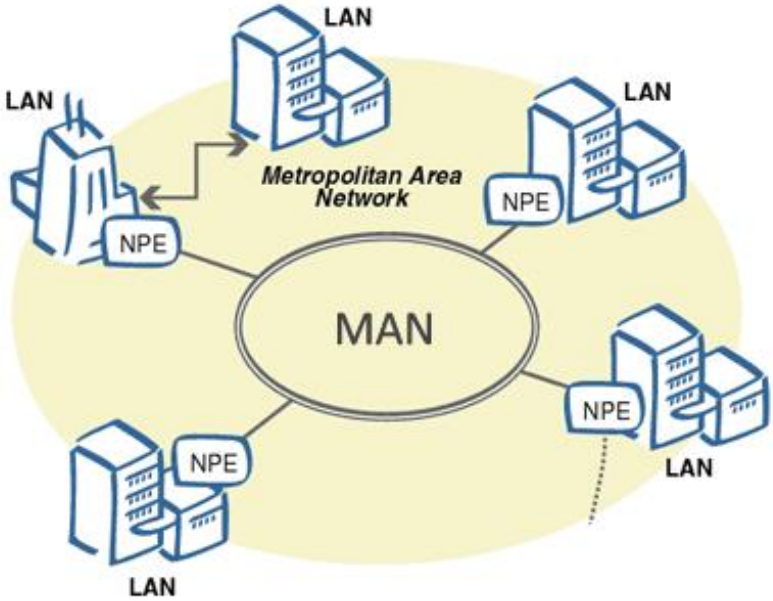
Figura 4 - Exemplo de uma rede *WAN*



Fonte: Cisco, 2023

(Metropolitan Area Network ou MAN): Uma Rede Metropolitana é a rede que conecta uma cidade, geralmente é esse tipo de conexão de rede que se tem em uma cidade, pode-se também conectar uma cidade a outra gerando uma WAN, algumas cidades usam essa conexão para mandar dados de um ponto a outro, monitorando dados de tráfego, movimentação e monitorar dados importantes da cidade para manter uma boa gestão e as transformando em cidades inteligentes com o uso também de internet of Thinks, (IOT). Na figura 5 é apresentado um exemplo de uma rede MAN típica. (KUROSE e ROSS, 2016).

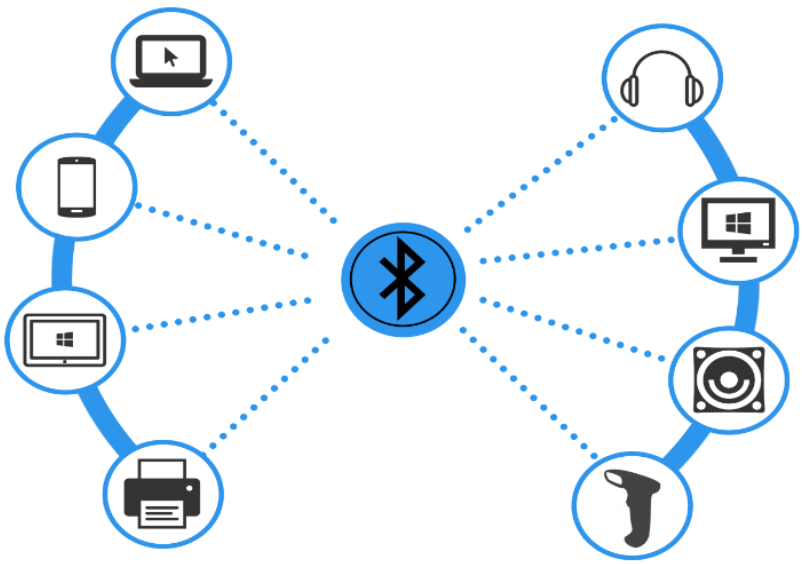
Figura 5 - Exemplo de uma rede MAN



Fonte: Cisco, 2023

***Personal Area network* ou (*PAN*)**: Uma Rede de Área Pessoal é uma rede que se interliga, mas é limitada ao espaço individual de um indivíduo, conectando por exemplo: Seu celular aos seus headphones e ao seu smartwatch ou ainda dentro de um quanto por exemplo, introduzindo a conexão de um computador aos periódicos e dispositivos presentes neste ambiente restrito. (KUROSE e ROSS, 2016). Representação de uma rede *PAN* na figura 6:

Figura 6 - Exemplo de uma rede PAN

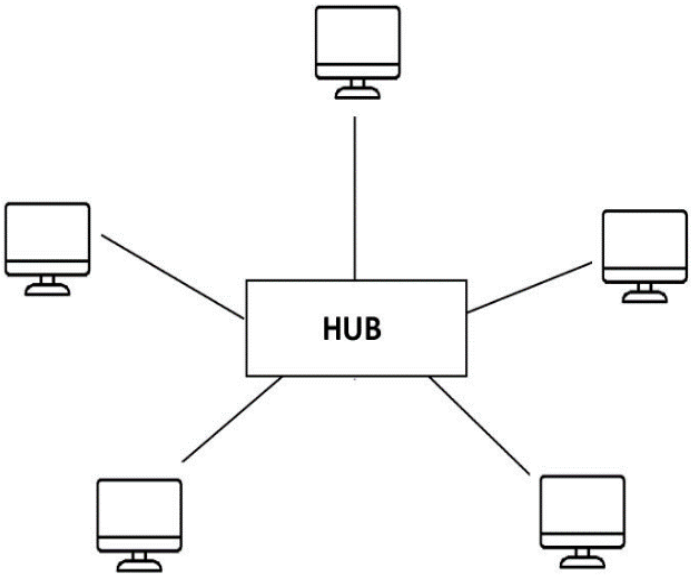


Fonte: pngWing, 2023

No fim, todas essas redes se cruzam e podem trocar informações, mas essas são suas definições através da escala geográfica.

As redes de computadores também podem ser dispostas em diversos arranjos topológicos, como Estrela no qual todos os computadores estão conectados a um dispositivo central de controle como um switch ou um hub. Na figura 7 é apresentado um exemplo de uma topologia em estrela. (KUROSE e ROSS, 2016).

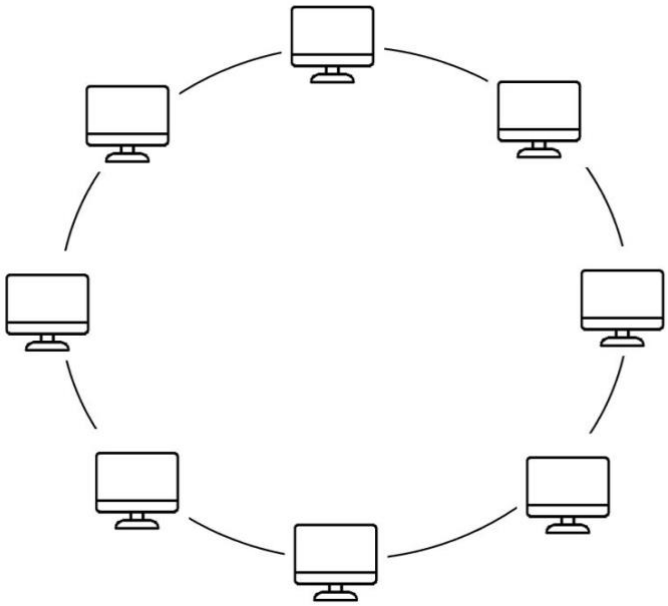
Figura 7 - Exemplo de Topologia Estrela



Fonte: Xpeducação, 2022

Temos também a rede em Anel, no qual os "nós" estão conectados em um loop fechado de modo que cada nó possa se comunicar com todos os presentes na rede encaminhando pacotes através dos outros nós da rede. Na figura 8 é apresentado um exemplo de uma topologia *Ring* (Anel). (KUROSE e ROSS, 2016).

Figura 8 - Exemplo de Topologia Anel

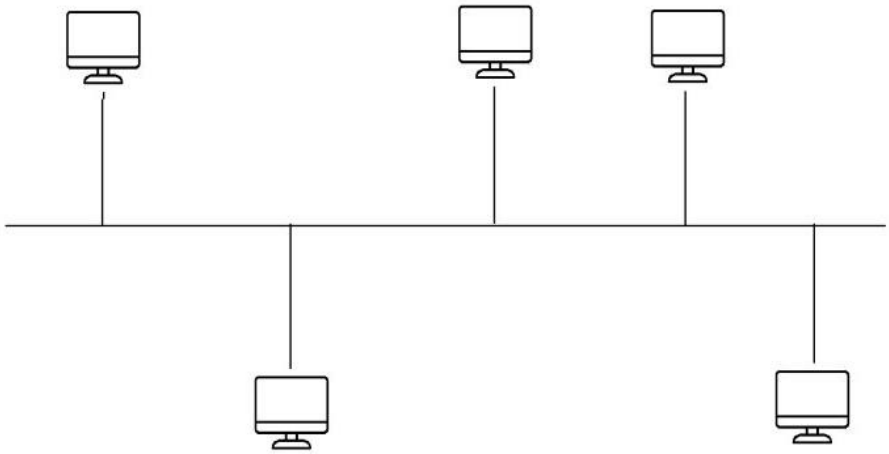


Fonte: Xpeducação, 2022

Tem-se também a topologia de Barramento - nesta configuração todos as estações ligam-se ao mesmo meio de transmissão. São geralmente compartilhadas em tempo e frequência, permitindo a transmissão da informação. Cada equipamento possui um único endereço que o identificará inequivocamente na rede. A informação é disponibilizada para todas as estações da rede, mas só poderá ser lida e interpretada pela estação que possuir o endereço de destino especificado.

Na figura 9 é apresentado um exemplo deste tipo de topologia. (KUROSE e ROSS, 2016).

Figura 9 - Exemplo de topologia de Barramento



Fonte: xpeducação, 2022

Além das topologias, as redes de computadores também utilizam de diversos protocolos para operarem de forma eficiente e segura, esses protocolos são como o livro de regras ou manual de instruções para os computadores, são eles que ditam como a comunicação entre as máquinas serão realizadas, as políticas a serem seguidas, as regras de comportamento e caminhos tomados e o mais importante, como as máquinas devem trocar informações entre elas.

Sem os protocolos de rede, a internet como se apresenta hoje, provavelmente não seria possível e algo muito menos seguro e confiável estaria tomando seu lugar. É graças a esses protocolos que as pessoas podem se sentir seguras ao navegar pela internet, ao mesmo tempo que desfrutam de um ambiente muitas vezes rápido e confortável, com acesso a informações ilimitadas.

Na tentativa de padronizar internacionalmente os protocolos empregados nas diversas camadas, foi desenvolvido com base na proposta feita pela *ISO* (*International Standards Organization*) um modelo chamado *OSI* (*Open Systems Interconnection*) que trata a interconexão de sistemas abertos a comunicação com outros dispositivos, (TANEMBAUM, 2011).

O modelo OSI é dividido em sete camadas, sendo elas: física responsável pela transmissão física dos dados que são encaminhados como sinais elétricos ou ópticos via

cabo, o enlace que gerencia o acesso aos meios físicos e identifica erros na transmissão através de switches por exemplo, a camada de rede que é responsável pelo roteamento e encaminhamento de pacotes através de roteadores por exemplo, a de transporte, que é responsável pelo controle de fluxo, segmentação e retransmissão, camada de sessão que estabelece, gerencia e encerra conexões, a camada de apresentação que traduz o formato de dados entre sistemas e pôr fim a camada aplicação que é responsável por fornecer serviços diretamente aos usuários. Embora este modelo tenha sido criado para padronizar os protocolos presentes em cada camada ele é bastante teórico, porém serve como uma boa referência de padronização.

Além do modelo *OSI* temos também o modelo *TCP/IP (Transmission Control Protocol)/(Internet Protocol)*, que diferente do modelo OSI é mais simples e prático, comumente descrito em quatro camadas, sendo elas: Aplicação, Transporte, Internet e Acesso à rede, (TANEMBAUM, 2011).

Assim como no modelo *OSI*, modelo *TCP/IP* tem suas responsabilidades atribuídas por camada, como demonstrado com a experiencia no modelo *OSI* as camadas de sessão e apresentação são pouco usadas na maioria das aplicações, o que fez com que elas não fossem incluídas no modelo *TCP/IP*, (TANEMBAUM, 2011).

1.2 Gerenciamento de redes tradicionais

O gerenciamento de redes tradicionais envolve o controle, monitoramento e manutenção de dispositivos de rede e de suas conexões, a fim de garantir a disponibilidade, desempenho e segurança dos recursos de rede. Neste modelo, a maior parte das atividades é realizada por humanos, profissionais de rede que configuram e mantém os dispositivos de rede, monitoram o tráfego, aplicam atualizações de patches implementam medidas de segurança e realizam outras tarefas relacionadas ao gerenciamento de redes o que atualmente gera certo nível de lentidão nos processos e abre brecha para falhas nas implementações.

As redes tradicionais são gerenciadas por meio de uma série de protocolos e ferramentas, como *Simple Network Management Protocol* (*SNMP*) que opera transmitindo informações *MIB* (*Management Information Base*) que é um conjunto de dados que representa um o estado e as configurações de dispositivos em uma rede, entre entidades de gerenciamento e agentes que executam em nome das entidades de gerenciamento. o *Internet Control Message Protocol* (*ICMP*) que é usado por *hosts* principalmente para o relatório de erros em uma rede e o protocolo de roteamento *OSPF* (*Open Shortest Path First*). (KUROSE e ROSS, 2016).

O SNMP é um protocolo amplamente utilizado para gerenciamento de redes, permitindo que os administradores de rede monitorem e configurem dispositivos de rede remotamente. O SNMP opera em uma arquitetura cliente-servidor, na qual os dispositivos de rede, como roteadores e switches, atuam como agentes, e o software de gerenciamento de rede age como um gerente. O gerente coleta informações dos agentes e pode emitir comandos para modificar a configuração do dispositivo, se necessário. Este protocolo fornece uma maneira eficiente de coletar informações sobre o status e desempenho dos dispositivos, bem como de configurá-los remotamente.

O *software* de gerenciamento de rede, que atua como gerente, é usado para monitorar e controlar os dispositivos de rede, podendo solicitar informações específicas dos agentes usando solicitações do tipo "*get*", ou pode receber notificações automatizadas dos agentes quando ocorre um evento importante, como uma falha no dispositivo.

No entanto, o gerenciamento de redes tradicionais apresenta algumas limitações, como a falta de flexibilidade e escalabilidade como citado no artigo (*SDN*: *A Compreehensive Survey*, 2015). (KREUTZ et. al, 2015). As redes tradicionais são baseadas em dispositivos de hardware específicos e em configurações estáticas, tonando

difícil a adaptação às mudanças nas demandas e requisitos de negócios. Além disso, as abordagens de gerenciamento centralizado e manual podem ser ineficientes e propensas a erros, especificamente em redes grandes e complexas.

Os protocolos de roteamento como o *OSPF*, desempenham um papel importante no gerenciamento de redes tradicionais segundo a Cisco no guia de designe do *OSPF*. O *OSPF* é um protocolo de roteamento baseado em estado de link que utiliza o algoritmo de Dijkstra para calcular o caminho mais curto entre dispositivos de rede. Embora o *OSPF* seja eficiente e escalável, ele não oferece flexibilidade e escalabilidade necessárias para lidar com a crescente demanda de Banda Larga, latência e qualidade de serviço (*QoS*) (*Quality of Services*) em redes modernas visto que cada vez mais temos componentes adicionados a rede, dês de novos celulares até aspiradores de pó. (CISCO, 2022).

Dado o aumento da complexibilidade das redes e a necessidade de maior flexibilidade, as redes definidas por *software* (*SDN*) surgira como uma alternativa promissora as abordagens tradicionais de gerenciamento de redes. A *SDN* permite uma maior automação e controle, simplificando o gerenciamento de redes e permitindo a rápida adaptação às mudanças nas condições da rede e nos requisitos de negócios. (CISCO, 2022).

Tendo isso em vista, o capítulo seguinte deste trabalho de graduação foi desenvolvido com a intenção de gerar melhor compreensão sobre o funcionamento e aplicações das redes *SDN* de modo que assim, se possa desenvolver compreensão sobre ambas as abordagens.

CAPÍTULO 2

2. Desenvolvimento

Neste capitulo serão apresentados os conceitos de redes definidas por *software* de modo que se possa compreender seu funcionamento, suas diferenças com uma rede de computadores tradicional, como essa abordagem é abstraída e algumas vantagens tais como os desafios de sua implementação, o objetivo deste capítulo é a apresentação desta abordagem de modo que, somada a fundamentação teórica anteriormente apresentada, possa-se desenvolver um maior entendimento da tecnologia vigente.

2.1 Redes definidas por software

Visto as dificuldades na administração de recursos da rede, da flexibilidade para a alteração de políticas ou implementação de novas automações na rede, escalabilidade na inclusão de novos dispositivos na rede de forma rápida e o gerenciamento manual das redes tradicionais, anteriormente citados, vem crescendo o desenvolvimento de abordagens diferentes para encarar esses problemas, seja por automação ou melhorias no processo de gerenciamento das redes (KREUTZ et al., 2015).

Considerando todos esses pontos, pode-se dizer que a criação das redes definidas por *software* valida-se e se dá devido a necessidade de otimização dos recursos da rede, o aumento da complexidade da rede, embora um fator que impulsiona novas soluções não foi diretamente aquele que trouxe as *SDNs* para o mundo.

As redes definidas por *software* (*SDN*) são uma das abordagens propostas para superar as limitações antes citadas das redes tradicionais e proporcionar mais flexibilidade, escalabilidade e automação (*ONF Open Networking Foundation*, 2021). Isso se deve justamente a separação do plano de dados do plano de controle, o plano de dados é justamente o responsável pela transmissão de dados e controle de fluxo, já o plano de controle atua como o cérebro da operação, ele é quem toma todas as decisões racionais das rotas, lógicas e políticas de segurança, seguindo o que foi programado anteriormente na camada de aplicação.

O plano de controle está a cargo de gerenciar os recursos da rede como o dono de uma empresa administra e gerencia seu negócio, e toma suas decisões com base no que antes foi pré-definido na camada de aplicação, programado pelo administrador humano

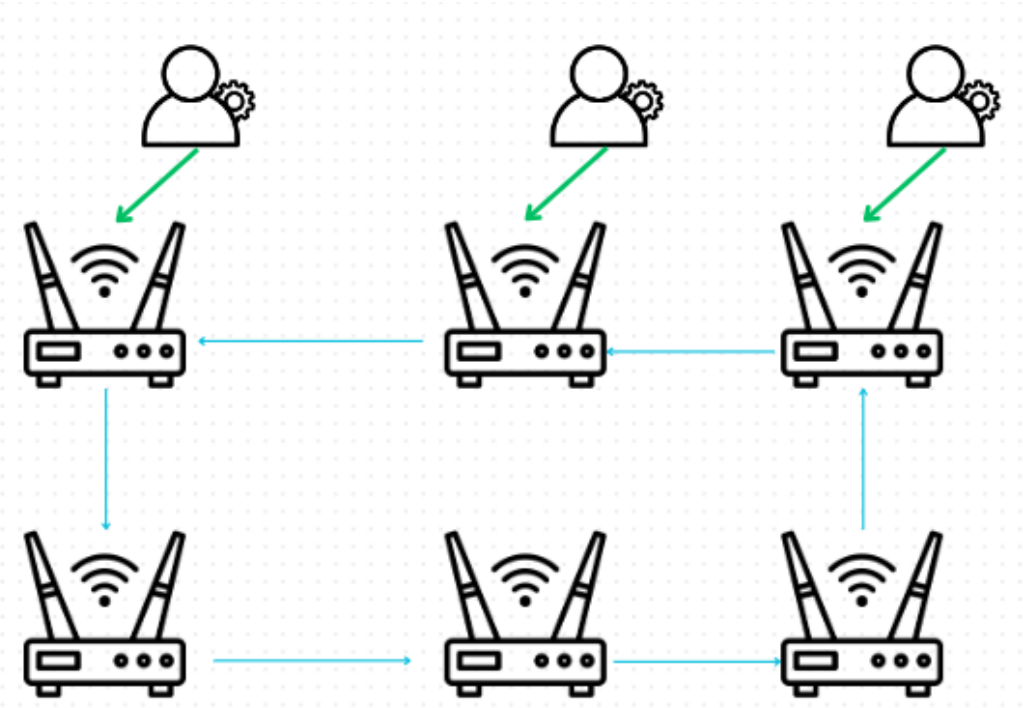
da rede, o plano de controle levará em conta as regras e políticas especificadas e seguirá tomando decisões de encaminhamento, segurança e rotas com base nisso. Já o plano de dados vai aplicar seu foco justamente em executar as ordens do controlador, uma vez que a decisão é tomada, os componentes desta camada executarão a tarefa fornecida sem a necessidade de tomar decisões lógicas.

Segundo (SCHALLER, 2017), “O trabalho atual com *SDN* começou por volta de 2008 com a publicação do protocolo *OpenFlow*, que possibilitou a separação do hardware de comutação. Ela informa que para o encaminhamento de pacotes essa foi uma função radical para o hardware de função fixa especializado com hardware integrado dentro da mesma caixa”. Segundo ela “Ele permitiu programar como o hardware lida com o tráfego de forma que antes era impossível”.

Com essa separação no plano de dados com o plano de controle, se tornam possíveis algumas mudanças na forma que se opera uma rede, sendo assim, tarefas que antes eram mais complexas e demandavam tempo, poderiam ser reduzidas a pequenas tarefes sendo realizadas no controlador. Por exemplo:

Imagine que você precise implementar uma nova política de segurança em sua rede corporativa a qual segmentará o tráfego entre os diferentes departamentos. Em uma rede tradicional você precisaria reconfigurar manualmente cada dispositivo da rede, algo que tomaria muito tempo dependendo do tamanho de sua rede e além de um processo exaustivo, tomaria o tempo que poderia estar sendo gasto na melhoria da rede ou em outras tarefas mais ou igualmente importantes. A figura 10 a seguir exemplifica o cenário em questão:

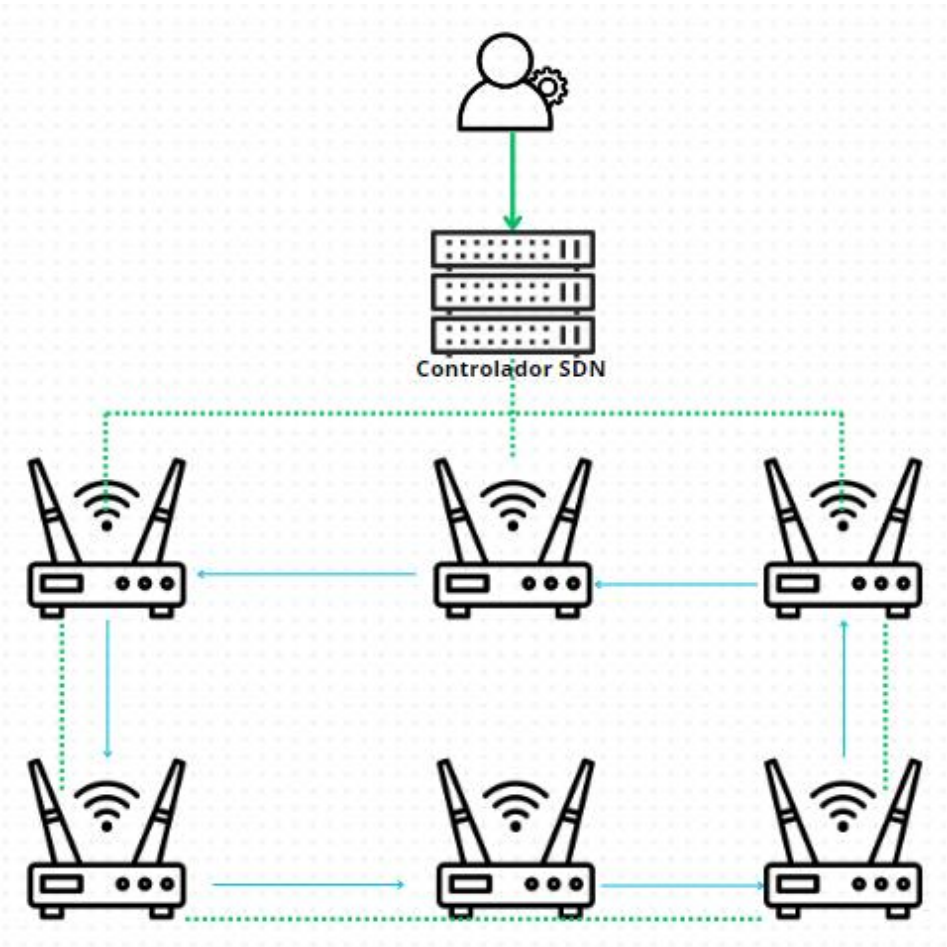
Figura 10 - Ilustração de configuração manual dos dispositivos



Fonte: Autoria do autor

Porém, quando se trata de uma rede *SDN* a vantagem de se ter um controlador principal atuando como o cérebro da rede, permite que esta tarefa seja mais eficiente, uma vez que você pode programar o controlador para direcionar o trafego de acordo com as políticas especificas de cada departamento, cada dispositivo virtual dentro dessa rede conectado ao controlador seguirá as políticas programadas no controlador *SDN* isso ocorre pois o controlador atua como o cérebro da rede, de modo que ele é quem toma as decisões mais importantes, deixando os dispositivos da rede com a função de encaminhamento sem a necessidade de "pensarem por eles mesmos". A figura 11 ilustra este cenário no qual o administrador da rede reconfigura o controlador que usará essas novas políticas para definir as novas rotas de roteamento:

Figura 11 - Ilustração da configuração da rede através do controlador SDN



Fonte: Autoria do Autor

Essa é uma das características mais interessantes sobre redes definidas por *software*, que vem atraindo bastante atenção desde 2011 com a criação da *ONF* que assumiu a tarefa de publicar a primeira arquitetura *SDN* detalhada, que foi lançada em 2014, a *ONF* continuou trabalhando neste projeto de modo que em 2016, forneceram também uma atualização e extensão que forneciam melhores funcionalidades e compreensão sobre o controlador *SDN* anteriormente citado e sua relação com o restante do ambiente de rede.

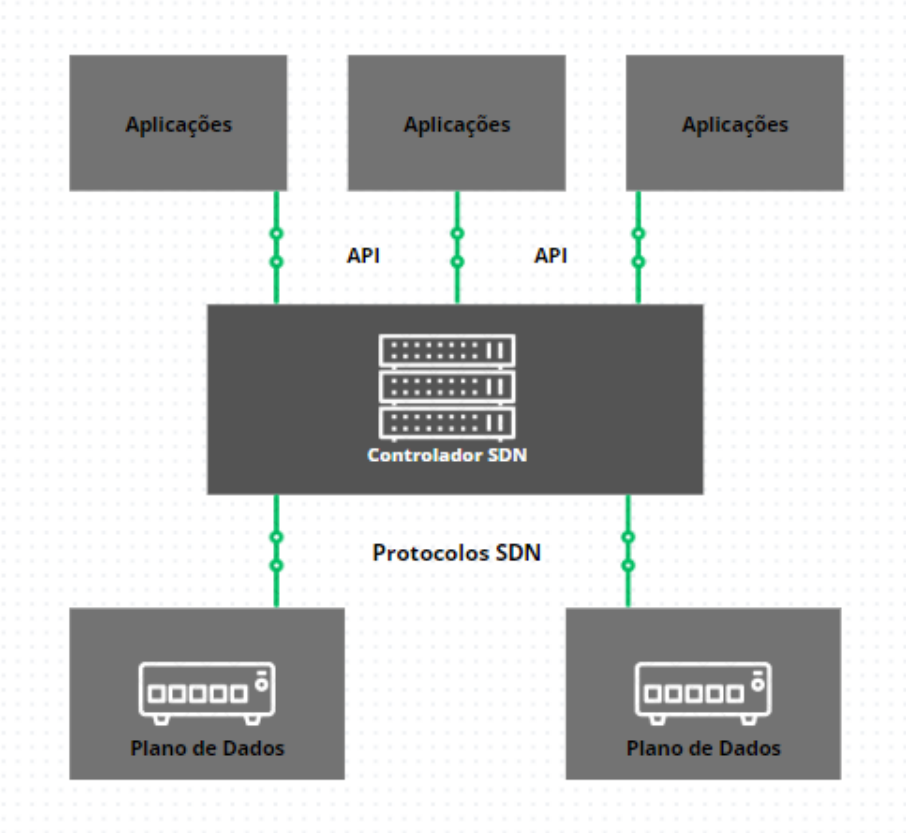
De acordo com (SCHALLER, 2017).

> A arquitetura SDN resultante é aplicável a todos os tipos de aplicativos nas áreas de rede corporativa, operadora, data center e campus, do cliente final ao proprietário do hardware, tanto para implantações de rede existentes completamente novas quanto em evolução. Ele acomoda SDN dentro e entre diferentes domínios (por exemplo, intra e inter-portador, intra e *inter-data* center).

Como dito antes, a *SDN* funciona separando o plano de controle do plano de dados o que permite que o gerenciamento e a tomada de decisões sejam centralizados em um controlador *SDN*, permitindo que os dispositivos de rede, como switches e roteadores, se concentram apenas no encaminhamento de tráfego o que reduz a carga de trabalho nestes componentes.

Nesta abordagem, o controlador desempenha um papel central como ponto de gerenciamento de comunicação entre dispositivos de rede, ou, o cérebro da rede e as aplicações que utilizam a rede (*ONF*, 2021). Essa arquitetura permite aos administradores da rede configurarem, monitorarem e ajustarem a rede de forma mais eficiente. Ao separar o Plano de controle do plano de dados, a *SDN* simplifica a implementação de políticas de rede e a orquestração de serviços em toda a infraestrutura da rede. A seguir a ilustração 12 representa uma abstração do modelo de uma rede *SDN*:

Figura 12 - Representação abstrata de uma rede SDN



Fonte: Autoria do autor

Como observa-se na figura 12 acima, as redes *SDN* são divididas em 3 camadas principais, o que as difere das tradicionais que como visto no capitulo 1 com o modelo

OSI são divididas em sete camadas, cada uma das camadas da rede *SDN* atende a um papel muito específico, essas camadas são: camada de aplicação, controle, plano de dados.

Para tal, um dos principais protocolos utilizados na *SDN* é o *OpenFlow*, que estabelece uma comunicação padronizada entre o controlador e os demais dispositivos da rede.

(MCKEOWN et al., 2008). Por meio do *OpenFlow* o controlador *SDN* pode instruir os dispositivos da rede sobre como processar e encaminhar pacotes, permitindo a implementação de políticas de rede e ajustes dinâmicos no comportamento da rede. Segundo (KREUTZ et al., 2015), "A *SDN* oferece grandes vantagens em comparação com as redes tradicionais, incluindo maior flexibilidade, automação e escalabilidade". Além disso, a *SDN* permite a integração com outras tecnologias emergentes, como a virtualização de funções de rede *Network Function Virtualisation* (*NFV*), melhorando ainda mais a eficiência e a agilidade das redes modernas.

Uma *NFV* embora compartilhe elementos com a *SDN* é outra tecnologia e ambas, independem uma da outra. No entanto, também podem combinar suas funcionalidades, a *NFV* é uma tecnologia que permite a virtualização dos serviços de rede, isso significa que, ao utilizar esta tecnologia, não há necessidade imediata de se ter uma *hardware* dedicado para cada função, uma vez que é possível utilizar serviços sobre demanda fornecidos pelos provedores, ela se assemelha a *SDN* em algumas características o que pode gerar certa confusão, mas são abordagens diferentes.

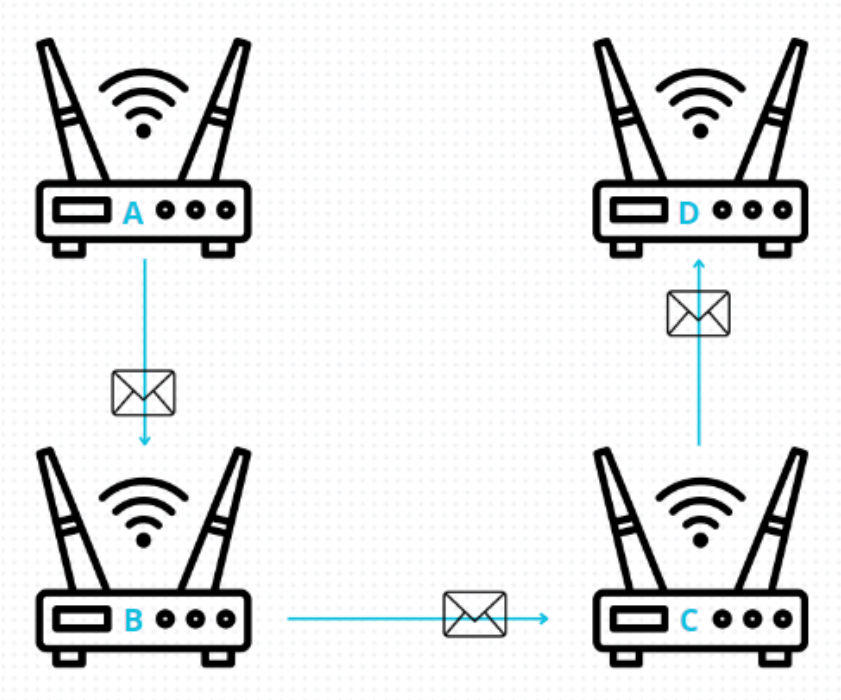
Em suma, as redes definidas por software têm representado uma evolução significativa no gerenciamento de redes, fornecendo uma abordagem diferente para atender as demandas crescentes das redes modernas. A adoção da *SDN* tem potencial de transformar a forma como as redes são gerenciadas e operadas, oferecendo benefícios significativos em termos de dinamismo para abranger novas tecnologias e suas funções, automação sendo possível programar a automatização de comportamentos e adaptabilidade com as mudanças nas condições da rede.

Como dito por (KREUTZ et. al., 2015) "torna-se mais fácil programar as aplicações uma vez que as abstrações fornecidas pela plataforma de controle ou pelas linguagens de programação de rede podem ser compartilhadas.". Não se torna necessário elaborar toda uma estratégia sobre a localização de uma nova funcionalidade visto que as aplicações podem reconfigurar dispositivos de encaminhamento de qualquer parte da rede.

Outra possibilidade interessante proporcionada por este tipo de abordagem é a diferença que elas apresentam no comportamento da camada de dados e de software, há diferenças entre essas camadas físicas e virtuais e uma dessas diferenças é a possibilidade de passar os dados de um dispositivo para o outro por um caminho que teoricamente não existe.

Enquanto em uma rede física o caminho padrão a se seguir seria como no exemplo da figura 8 a seguir:

Figura 13 - Exemplo de rede fisica encaminhando pacotes



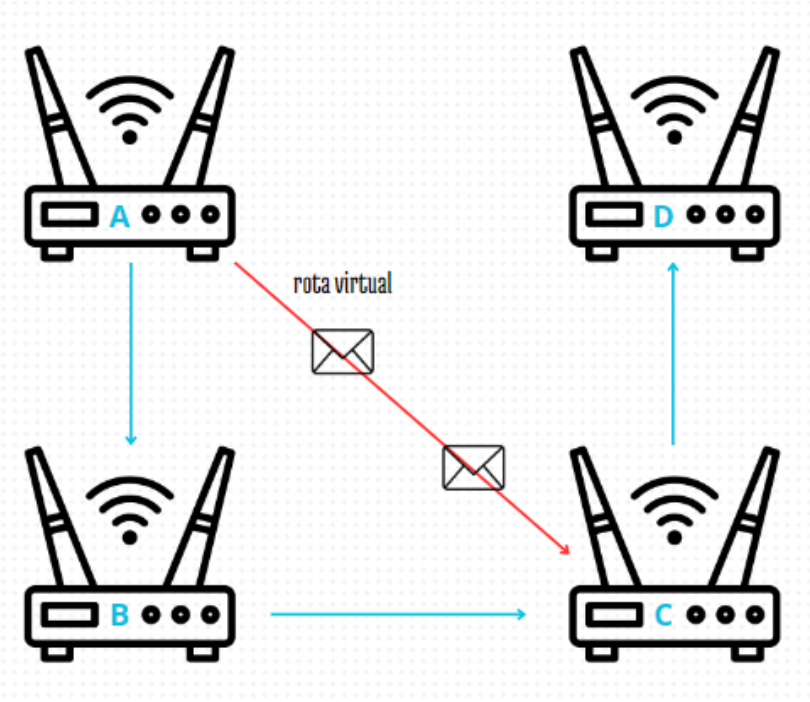
Fonte: Autoria própria

Vide o exemplo acima, é apresentada uma rede na qual existem quatro roteadores conectados entre si, A, B, C e D, os pacotes são encaminhados de uma para o outro e o ultimo não fecha o ciclo, sendo assim, para que o roteador A encaminhar uma pacote para o roteador C por exemplo, primeiro ele terá que sair do roteador A, passar para o roteador B que verificará o endereço destino e então reencaminhará para o roteador C.

No entanto, na virtualização desses recursos, é possível passar uma rota virtual que não existe de fato, por exemplo, encaminhando o pacote do roteador A

diretamente para o roteador C, mesmo não havendo um caminho físico para a passagem desses dados. Isso é ilustrado na figura 9:

Figura 14 - Exemplo de rede virtual encaminhando pacotes



Fonte: Autoria própria

Isso só é possível pois a virtualização de redes é uma tecnologia que permite a criação de redes virtuais dentro de infraestruturas físicas, a mesma insere uma camada de abstração entre o hardware e as aplicações e serviços, transformando a rede em uma rede baseada em software. Enquanto uma rede tradicional o roteamento é realizado pelos roteadores físicos seguindo a tabela de rotas e caminhos existentes fisicamente, em uma rede baseada em software isso não é necessariamente assim, redes que utilizam roteamento virtual podem criar rotar virtuais que não correspondem diretamente a conexões físicas.

Como nas redes definidas por *softwares* o controlador *SDN* gerencia o roteamento e as políticas de rede, torna-se possível utilizar roteamento com rotas virtuais dinâmicas, sem depender de configurações manuais nos roteadores físicos. “A maior vantagem do roteamento dinâmico é se adaptar às alterações nas condições da rede, como volume de tráfego, largura de banda e falha de rede” (AMAZON, 2023). Além disso, com a virtualização dos recursos, também se torna possível a criação de diversas redes virtuais em uma única infraestrutura física.

2.2 Protocolos e padrões SDN

As *SDN* vem cumprindo mudanças na forma como o encaminhamento de pacotes é realizado nas redes de internet, com a proposta de separar o plano de enlace e o plano de dados de modo que possa assim facilitar e acelerar o encaminhamento de pacotes, visto que desta forma a criação de engasgos na rede são reduzidas com um menor volume de informações sendo transmitidos sem a necessidade de excluir ou deixar pacotes para serem enviados depois.

Para tanto são necessários certos conjuntos de protocolos para atuar nessa operação e assim como no *BGP* (*Border Gateway Protocol*) e *OSPF* que são protocolos das redes tradicionais de internet, as *SDN* também possuem alguns protocolos padrão de encaminhamento de pacotes. Estes protocolos servem para que não haja problemas nos encaminhamentos e garanta uma maior segurança para o usuário.

Nas redes tradicionais o *OSPF* por exemplo é um protocolo de encaminhamento amplamente utilizado dentro de redes locais de empresas, permitindo que os endereços *IP* dentro desta rede sejam atualizados automaticamente e compartilhados entre os dispositivos da rede. Já o *BGP* segue um conceito semelhante usando rotas já pré-definidas com o menor caminho possível para que um pacote encaminhado passe de um ponto a outro, isto também é realizado com tabelas dinâmicas que são atualizadas todas as vezes em que um "nó" não está respondendo. (TANEMBAUM, 2011)

O protocolo *SND* mais famoso e mais utilizado é o *Openflow* que interage diretamente com a interface de *southbound* entre o plano de controle e o plano de dados, de modo que possa controlar as transmissões de dados de um ponto centralizado em um *switch* específico. (SILVA et al., 2018). O *Openflow* é primordial para o funcionamento de uma rede definida por *software*, sem ele, a comunicação entre as interfaces se torna mais complexa, porém, embora existam outras opções que serão citadas adiante, o foco deste trabalho será no *Openflow*.

Como citado, atualmente o protocolo mais amplamente utilizado e em constante desenvolvimento é o *OpenFlow*, no entanto há outros como *ForCES* (*Forwarding and Control Element Separation*) que também é um protocolo para a *southbound* interface que permite a separação de elementos de controle e encaminhamento em dispositivos de rede e o *P4*(*Programing Protocol-independent Packet Process*) que permite a programação de como os pacotes são processados pelos *switches*, roteadores e *NICs (Network Interface Card) ou placas de interface de rede*.

Além disso também existem redes *SDN* baseadas em *Overlay* ou (*Overlay-based SDN*) na qual cria-se uma rede virtual acima do *hardware* existente chamada *Overlay* ou *Fabric*, essas redes podem ser configuradas e gerenciadas de maneira independente da rede física a principal a vantagem desta abordagem é que ela permite muita flexibilidade e agilidade pois podem ser criadas, alteradas e excluídas rapidamente sem a necessidade de alterar as configurações da rede física.

Os protocolos de rede utilizados nesta variação incluem o *Virtual Extensible LAN* (*VXLAN*), *Network Virtualization using Generic Routing Encapsulation* (*NVGRE*), *Stateless Transport Tunneling* (*STT*), e outros. Estes protocolos são responsáveis pela encapsulação de pacotes de dados, o que permite que eles sejam transmitidos pela rede física como se estivessem em uma rede virtual separada.

Redes *SDN* baseadas em *API (Application Programming Interface)* ou (*API based SDN*) que usa interfaces de programação geralmente chamadas de *APIs southbound* de modo que, com isso as *APIs* controlem o fluxo de dados pela rede de cada dispositivo facilitando a comunicação entre diferentes componentes de uma rede. Nestas arquiteturas as *APIs* desempenham um papel crucial na divisão entre o plano de controle e o plano de dados, permitindo que o plano de controle interaja com os dispositivos de rede, com as instruções de como processar e encaminhar pacotes de acordo com as políticas de rede definidas.

No Modelo híbrido de *SDN* (*automation based SDN*) mistura-se o *SDN* e a rede tradicional permitindo que o protocolo ideal seja atribuído para cada tipo de tráfego este é frequentemente usado como uma abordagem de integração progressiva dele.

Até o momento, o conceito *SDN* mais implantado é o *OpenFlow*, que é um protocolo de comunicação que dá acesso ao plano de encaminhamento de switch de rede ou roteador pela rede. (KREUTZ et al., 2015).

2.3 OpenFLow

O protocolo *OpenFow* tornou-se o padrão de comunicação nos componentes *SDN*, sua padronização em 2008 pela *ONF* (*Open Networking Foundation*), permitiu um grande avanço e um aumento exponencial do interesse do mercado em redes *SDN*. (SILVA et al., 2018).

Como citado anteriormente no decorrer deste capítulo, as redes definidas por software possuem dois tipos de interface, a *northbound* e a *southnound* interface, a *northbound* é responsável pelas aplicações programáveis da rede, ela é responsável por permitir a comunicação entre o controlador e as aplicações, permitindo que as aplicações programem a rede e monitorem através de um controlador centralizado (ZOHAIB et al., 2019). A *southbound* por sua vez, realiza o vínculo dos elementos de controle e encaminhamento de dados, o que permite que o controlador programe o plano de dados remotamente (OLIVEIRA et al., 2021).

Segundo (STALINGS, 2013)

> A arquitetura *SDN (Software-Defined Networking)* e o padrão OpenFlow fornecem uma arquitetura aberta na qual a funcionalidade de controle é separada do dispositivo de rede e colocada em servidores de controle acessíveis. Isso permite que a infraestrutura subjacente seja abstraída para aplicativos e serviços de rede, que podem tratar a rede como uma entidade lógica.

O *OpenFlow* é aberto para a configuração de tabela de fluxo de dispositivos de rede determinando ações de encaminhamento de pacotes e particionando o tráfego de acordo com o interesse dos operadores. (OLIVEIRA et al., 2021)

A adoção do protocolo *OpenFlow* foi revolucionária separando o plano de controle do plano de dados permitindo que o controle seja centralizado em um controlador *SDN* o que permite que decisões sejam tomadas de forma programática e flexível, com base em políticas e lógica definidas pelo controlador. Os dispositivos de rede *OpenFlow* seguem as instruções do controlador e realizam o encaminhamento de acordo com as regras definidas por ele (*ONF*, 2021), isso permite uma maior agilidade na implementação de novos serviços, gerenciamento centralizado, balanceamento de carga dinâmico, otimização de tráfego e respostas mais eficientes a eventos e mudanças na rede, (GORANSSON et al., 2016)

2.4 Vantagens e desafios SDN

As Redes Definidas por Software (SDN) apresentam certas vantagens em comparação às abordagens tradicionais de gerenciamento de redes, mas também enfrentam desafios que precisam ser superados para que seu potencial seja plenamente aproveitado (KREUTZ et al., 2015).

2.4.1 Vantagens

Como foi dito no decorrer deste trabalho, as redes *SDN* oferecem certas vantagens sobre as redes tradicionais, vantagens essas que melhoram a flexibilidade, segurança, desempenho, melhor administração dos recursos da rede e a adaptabilidade da rede.

Uma das principais vantagens oferecidas por uma *SDN* é a flexibilidade e adaptabilidade da mesma. Uma rede *SND* permite uma adaptação dinâmica às mudanças nas condições de rede e nos requisitos de negócios, facilitando a implementação de políticas e a otimização de tráfego (*ONF*, 2021).

Ou seja, caso a empresa necessite por alguma razão mudar uma regra na forma como eles operam ou em sua infraestrutura, isso não representaria grandes problemas, visto que, dispondo dessa flexibilidade de adaptação da rede com a programação da mesma inclusive com linguagens como *java* e *python*, a rede pode ter suas regras reprogramadas e alteradas pelo administrador da rede, de modo que se mantenha o cumprimento das demandas da empresa, sem precisar contratar outra solução externa, além disso, devido ao uso do controlador *SDN* não são necessários muitos passos para adicionar novos componentes a rede, de modo que ao adicionar novos roteadores ou switches *SDN* a configuração desses dispositivos ficaria a cargo justamente do controlador.

Segundo (VALENTE e JÚNIOR, 2023), “O que ela faz é trazer o controle centralizado para um lugar só e proporciona uma maneira de programar unificada para diversos elementos da rede, como roteadores, *switches*, *firewall*. O que melhora a segurança e o desempenho da rede”. Sendo assim, A programabilidade centralizada da rede *SDN* também melhora a experiencia de controlar diversos componentes da rede e isso por sua vez pode melhorar a esses dois pontos antes citados se bem utilizada.

Junto a isso destaca-se também o gerenciamento centralizado que simplifica o controle e a supervisão das redes, permitindo visibilidade e análise do tráfego e a redução de custos que vem com a simplificação do gerenciamento de rede e permite uma utilização mais eficiente dos recursos de hardware (HALEPLIDIS et al, 2015).

O desempenho da rede também é melhorado, uma vez que a carga de trabalho dos switches *SDN* é reduzida, permitindo que eles foquem principalmente no encaminhamento de pacotes sem a necessidade de haver alguma tomada de decisão complexa por parte deles, ao que se refere às decisões de roteamento ou encaminhamento de pacotes, visto que todas essas decisões devem ser tomadas pelo controlador *SDN*.

Como citado por (VALENTE e JÚNIOR, 2023 apud GUBBI, J et al., 2013). “As tecnologias *SDN* permitem aos administradores da rede criarem políticas de segurança, monitorar o tráfego de rede, até detectar ameaças de segurança e responder de uma forma mais rápida e eficaz”. Assim sendo, uma das vantagens é também a segurança da rede se bem administrada.

Com o aumento no uso das redes móveis e novas tecnologias como redes 5G, as redes *SDN* se destacam como uma opção viável e compatível oferecendo vantagens que permitem melhor conectividade e desempenho, assim sendo, suas aplicações tornam-se infinitas, inclusive em cenários inesperados. Segundo (VALENTE e JÚNIOR, 2023).

> Quando relacionamos com a tecnologia 5G, a baixa latência junto de uma alta confiabilidade são importantes para integrar sistemas de produção e melhorar a eficiência de fabricas, pois torna possível uma comunicação em tempo real e automação facilitando as operações, monitoramentos e manutenções preventivas. No cenário automotivo, as SDNs junto ao 5g atua na comunicação direta de veículos autônomos maneira rápida, possibilitando uma melhor resposta para situações de tráfego, maior segurança e melhor coordenação

Uma das principais vantagens aplicadas é a o monitoramento em tempo real, isso permite respostas e decisões melhores e mais assertivas sobre os empecilhos que possam vir a surgir.

2.4.2 Desafios

No entanto, segundo (KREUTZ et al., 2015), “as redes *SDN* enfrentam desafios importantes, como segurança já que a centralização e a programação das redes *SDN* podem aumentar a exposição a ameaças de segurança, exigindo o desenvolvimento de novas abordagens e soluções de segurança”. Isso aplicasse principalmente a ataques de negação de serviço e ataques direcionados ao controlador *SDN* uma vez que, caso o cérebro da rede seja derrubado, não demoraria muito para a empresa começar a ter perdas, ainda assim é prematuro dizer que este seja um defeito da rede, já que o uso do controlador *SDN* traz muitas vantagens antes citadas para a rede.

Interoperabilidade: A coexistência e a integração da *SDN* com as tecnologias de rede existentes podem ser desafiadoras, e a padronização e a cooperação entre os fornecedores são cruciais para garantir a interoperabilidade (HALEPLIDIS et al., 2015). O que vem sendo resolvido nos últimos anos com o interesse crescente nesta abordagem por grandes empresas como a *cisco* e a *Google*. Ainda assim,

Embora a programabilidade das políticas da rede *SDN* possam apresentar grandes vantagens, como políticas flexíveis ou rígidas a depender das necessidades da empresa que estiver utilizando desta tecnologia, se faz importante considerar que se essas políticas programadas não forem bem escritas podem gerar pontos de vulnerabilidade na rede, e portanto, para empresas que não desejem correr este risco é uma opção bastante viável o uso de políticas já existentes e padronizadas, soluções prontas que são lançadas dia após dia.

Segundo (VALENTE e JÚNIOR, 2023). “A *SDN* abstrai a complexidade dos componentes de rede e automatiza os mecanismos de comutação e roteamento. No entanto, gerenciar e configurar ambientes *SDN* ainda pode ser complexo, especialmente ao integrar com infraestruturas existentes”. Sendo assim, é necessário se atentar as necessidades da rede e entender a fundo sua implementação antes de tomar a atitude de alterar a rede para uma rede *SDN*, caso a decisão de implementação dessa abordagem não seja tomada de forma assertiva e cuidadosa, a rede pode acabar sendo prejudicada como um todo.

2.5 Segurança em SDN

A segurança em redes definidas por software (*SDN*) representa um conjunto de desafios e oportunidades. De um lado, a centralização do controle e a natureza programável da *SDN* permitem uma visão global e em tempo real do estado da rede, oferecendo oportunidades para uma resposta de segurança mais eficaz e rápida (SHIN & GU, 2012).

No entanto, por outro lado, as *SDN* introduzem novas vulnerabilidades e pontos de ataque. O controlador *SDN*, sendo o cérebro da rede, torna-se um alvo atraente para os atacantes. Se um atacante conseguir comprometer o controlador, ele poderá ter controle total sobre a rede (KREUTZ et al., 2015).

Segundo (SHIN & GU, 2012) "Os protocolos de controle de redes *SDN*, como o *OpenFlow*, também podem ser explorados. Ataques como inundação de solicitações, *eavesdropping* e *spoofing* de mensagens do controlador podem levar a interrupções de serviço e vazamentos de dados."

Para mitigar esses riscos, várias estratégias de segurança podem ser adotadas. O uso de técnicas de autenticação e criptografia pode ajudar a proteger a comunicação entre o controlador *SDN* e os dispositivos de rede, prevenindo ataques de interceptação e falsificação.

O uso de *firewalls* e sistemas de prevenção de intrusões (*IPS*) também pode ser bastante útil. Além disso, é fundamental implementar políticas de controle de acesso e segmentação de rede para limitar o escopo potencial de um ataque (*ONF*, 2021).

A detecção e resposta a incidentes também são vitais. Ferramentas de monitoramento de rede e sistemas de detecção de intrusões (*IDS*) podem ser usados para identificar atividades suspeitas e tomar medidas corretivas (KREUTZ et al., 2015).

Segundo (VALENTE e JÚNIOR, 2023) por possuir algumas vulnerabilidades que podem ser abusadas, é essencial abordar questões de segurança dos ambientes SDN, questões como autenticação, autorização de usuários, trafego da rede, separação de redes virtuais autorizadas, violação de dados, interrupções da rede, criptografia e monitoramento da rede precisam ser bem especificadas antes da implementação desta arquitetura, e isso precisa ser feito por alguém que tenha conhecimento profundo sobre a arquitetura, protocolos vigentes e questões de segurança que estão rodando na arquitetura atual, para que assim possa realizar a mudança de forma segura.

CONCLUSÃO

As redes *SDN* representam uma evolução significativa na forma como se encaram as redes de *internet*, encaminhamento de pacotes e uso de recursos de uma rede, essa abordagem apresenta diferentes soluções para várias características das redes de computadores tradicionais, seja de flexibilidade, agilidade ou segurança.

A programabilidade da rede aumenta grandemente as soluções de segurança aplicáveis nas empresas uma vez que com isso, torna-se possível definir suas políticas de segurança rígidas ou mais compassivas a depender das necessidades em questão, além disso, a compatibilidade com virtualização ou redes tradicionais, permite que o administrador da rede gerencie os recursos de forma muito mais eficiente e traçar rotas ou prioridades de encaminhamento de pacotes conforme necessário na rede.

Enquanto as redes tradicionais apresentem algumas vezes problemas com desempenho ou perca de pacotes na transmissão de dados devido a engasgos na rede, as redes definidas por *software* podem apresentar uma solução interessante para casos nos quais desempenho seja uma necessidade inerente do negócio.

Em suma, grandes passos estão sendo dados na evolução do uso e pesquisas sobre esta abordagem, e com o constante crescimento do interesse de grandes empresas nessa tecnologia devido principalmente, ao aumento de *IaaS* (*Infrastructure as a Servisse*) como um negócio em foco nos últimos anos. Ainda assim, muito ainda deve ser desenvolvido nos próximos meses e anos, uma vez que a cada dia surgem soluções e pesquisas novas visando resolver problemas de segurança, compatibilidade e aplicações.

É importante destacar que este trabalho não aborda profundamente todos os temas propostos de modo que pode auxiliar no entendimento e estudos do assunto porém de modo algum, substituí uma literatura relacionada, este trabalho tinha como objetivo principal auxiliar nos estudos e entendimento do tema, algo que inclusive parece ter sido alcançado com sucesso, além disso, durante o desenvolvimento do trabalho novos artigos, soluções e pesquisas foram lançados, tanto para cobrir vulnerabilidades das *SDN* quanto para evidenciar as forças delas, e não puderam ser adicionados ao trabalho devido ao tempo.

Como proposta de trabalhos futuros, seria interessante a pesquisa experimental de uma rede *SDN* visando compreender melhor a programabilidade e os protocolos da rede, por exemplo, trazendo certas políticas de rede para ambientes específicos que visão ou

desempenho ou segurança e apresentar uma forma de lidar com isso utilizando as redes *SDN* para melhor utilizar os recursos da rede e comparar os desempenhos antes da aplicação programada e depois.

Outra proposta de trabalho futuro seria a abordagem dessas novas soluções que surgiram nos últimos três anos, visando cobrir o que mudou e como essas mudanças ajudaram a melhorar ou piorar a implementação das redes *SDN*, sendo um estudo documental sobre o assunto.

Bibliografia

AMAZON. O que é roteamento. Disponível em < http://aws.amazon.com/pt/what-is/routing/ >. Acesso em 28 Mai 2024.

CISCO. Compreender o OSPF (Open Shortest Path First) – Guia de Design. Disponível em: https://www.cisco.com/c/pt_br/support/docs/ip/open-shortest-path-first-ospf/7039-1.html. Acesso em: 30 maio 2023.

COMER, Douglas E. Redes de computadores e internet. 6. ed. Porto Alegre: Bookman, 2016.

OPEN NETWORKING FOUNDATION. SDN Architecture. Issue 1.1. 2016. Disponível em: https://opennetworking.org/wp-content/uploads/2014/10/TR-521_SDN_Architecture_issue_1.1.pdf. Acesso em: 27 Mai 2023.

OPEN NETWORKING FOUNDATION. SDN Enabled Broadband Access (SEBA). Versão 2.0. Março de 2021. Disponível em: https://onfstaging1.opennetworking.org/wp-content/uploads/2021/03/ONF-Reference-Design-SEBAv2.0FINAL3.pdf. Acesso em: 27 Mai 2023.

SHIN, Seungwon; GU, Guofei. Cloud Watcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?). In: 2012 20th IEEE international conference on network protocols (ICNP). IEEE, 2012.

GORANSSON, Paul; BLACK, Chuck; CULVER, Timothy. Software defined networks: a comprehensive approach. Morgan Kaufmann, 2016.

GUILHEN, Bruno Anselmo; SILVEIRA, Regina Melo; KOFUJI, Sergio Takeo. Computação forense em redes definidas por software (sdn): Uma revisão de literatura. In: Anais do XII Workshop de Pesquisa Experimental da Internet do Futuro. SBC, 2021. p. 13-24. Disponível em: Vista do Computação Forense em Redes Definidas por Software (SDN): Uma revisão de literatura (sbc.org.br)

HALEPLIDIS, Evangelos et al. Software-defined networking (SDN): Layers and architecture terminology. 2015. Disponível em: https://www.semanticscholar.org/paper/Software-Defined-Networking-(SDN)%3A-Layers-and-Haleplidis-Pentikousis/5f5ace2fb042369dd231267ce6e41e02df3a3222. Acesso em 06 Jun 2024.

KREUTZ, D.; RAMOS, F. M. V.; VERÍSSIMO, P. E.; ROTHENBERG, C. E.; AZODOLMOLKY, S.; UHLIG, S. Software-Defined Networking: A Comprehensive Survey. In: Proceedings of the IEEE, vol. 103, n. 1, p. 14-76, janeiro. 2015. Disponível em: 1406.0440.pdf (arxiv.org) acesso em: 22 Mai 2024.

ROSS, Keith W.; KUROSE, James F. Computer Networking: A Top-Down Approach. 7th ed. Boston: Pearson, 2017.

OKTIAN, Yohanes Edwin et al… Distributed SDN controller system: A survey on design choice. Computer Networks [S.l], v. 121, p.100-111, dezembro de 2017.Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1389128617301706. Acesso em 15 Out 2023.

MCKEOWN N., ANDERSON T., BALAKRISHNAN H., PARULKAR G., PETERSON L., REXFORD J., SHENKER S., TURNER J… OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review [S.l], v.38, nº2, p69-74, junho de 2008. Disponível em: ccr-2008mckeown.pdf (wustl.edu)

MICROSOFT, O que é nuvem?. Disponível em: http://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-is-the-cloud/. Acesso em 14 Mai 2024.

SILVA, A. C.et al. Avaliação de Controladores Software-Defined Networking Utilizando Metodologia Padrão para Benchmark. In: Workshop de Pesquisa Experimental da Internet do Futuro (WPEIF),2018. Disponível em:https://sol.sbc.org.br/index.php/wpietf/article/view/3209.Acesso em: 27 Mai 2023.

STALLINGS, W. Data and Computer Communications Pearson Education Limited [S.l], v10ª edição, p69-74, junho de 2013.

TANENBAUM, Andrew. S. Redes de Computadores. Pearson Prentice Hall [S.l], v5ª edição, p69-74, junho de 2011.

TANENBAUM, Andrew. S. Sistemas Operacionais Modernos, 4. ed. [S.1]: [s.n], 2016, p69-74

VALENTE, Felipe F. A; JÚNIOR, Ivon W. S. **Redes definidas por software (SDN):** Uma analise sobre as tecnologias de SDN, suas vantagens e desafios, sua aplicação em redes de computadores. Disponível em https://revistaft.com.br/redes-definidas-por-software-sdn-uma-analise-sobre-as-tecnologias-de-sdn-suas-vantagens-e-desafios-e-sua-aplicacao-em-redes-de-computadores. Acesso em 06 Jun. 2024.

Zohab Latif, et al., A Comprehensive Survey of Interface Protocols for Software Defined Networks. Disponível em: 1902.07913.pdf (arxiv.org). Acesso em 18 Abr. 2024.