UNIVERSIDADE FEDERAL DO PAMPA

Rodrigo Masera de Souza

Avaliação de Estratégias de Migração para Redes Definidas por Software

Alegrete
2018

Rodrigo Masera de Souza

Avaliação de Estratégias de Migração para Redes Definidas por Software

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciência da Computação da Universidade Federal do Pampa como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Marcelo Caggiani Luizelli

Coorientador: Prof. Me. Diego Luis Kreutz

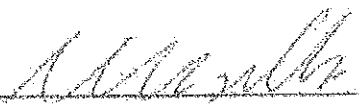
Alegrete
2018

Rodrigo Masera de Souza

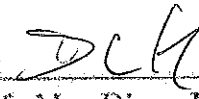
Avaliação de Estratégias de Migração para Redes Definidas por Software

Trabalho de Conclusão de Curso apresentado no Curso de Graduação em Ciência da Computação da Universidade Federal do Pampa como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação.

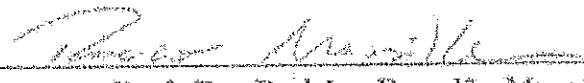
Trabalho de Conclusão de Curso defendido e aprovado em ..... de ..... de .....
Banca examinadora:



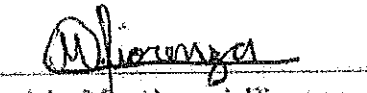
Prof. Dr. Marcelo Caggiani Luizelli
Orientador
UNIPAMPA



Prof. Me. Diego Luis Kreutz
Coorientador
UNIPAMPA



Prof. Dr. Rodrigo Braudão Mansilha
UNIPAMPA



Maurício Martinuzzi Fiorenza
UNIPAMPA

RESUMO

Redes definidas por software (*Software Defined Network* (SDN)) vem recebendo significativa atenção por parte da academia e da indústria nos últimos anos. Ao desacoplar o plano de controle e de dados, SDN permite criar aplicações de controle reativas e dinâmicas a eventos da infraestrutura – além de propiciar um novo ecossistema de inovação no gerenciamento e operação de infraestruturas de rede. Apesar de SDN ter atingido um significativo amadurecimento tecnológico, a sua implantação em redes corporativas e de campus é ainda pouco expressiva. O lento processo de adoção desta tecnologia é consequência direta (i) do custo da implantação, ou seja, substituição da infraestrutura existente, (ii) do planejamento e conhecimentos necessários para uma implantação gradativa, que requer a coexistência de tecnologias legadas e (iii) da falta de exemplos concretos de migrações gradativas bem sucedidas, motivo que também ajuda na falta de confiança na tecnologia. O objetivo deste trabalho é investigar estratégias para a migração de uma rede tradicional para uma rede SDN híbrida ou completa através da troca de *switches* tradicionais para SDN. Para isso foram propostas, implementadas e testadas três estratégias diferentes. A primeira prioriza *switches* que possuem o maior grau (número de conexões). A segunda leva em conta um ou mais parâmetros (largura de banda, horário de pico da rede ou qualquer outro aspecto que o operador ache relevante) que são chamados de peso dos links. Finalmente, a terceira prioriza a segurança da rede, priorizando dispositivos de encaminhamento que estão conectados às máquinas hosts. Para cada uma das estratégias foram avaliadas três métricas: (i) teste de latência; (ii) teste de vazão e (iii) teste de comprimento de caminho. Segundo os resultados, a estratégia baseada no grau dos *switches* se saiu melhor nos testes de latência. Já no teste de vazão a estratégia baseada na segurança da rede foi a melhor. Como forma de representar uma cenário real, a topologia de rede da Universidade Federal do Pampa (UNIPAMPA) campus Alegrete foi utilizada como base para este trabalho.

Palavras-chave: Software-Defined Networks(SDN). Redes Definidas por Software. Migração gradativa. Topologia de Redes.

ABSTRACT

Software Defined Network (SDN) has been receiving significative attention by both the academy and industry over the last years. By decoupling the control plane from the data plane, SDN allows the creation of control applications both reactive and dinamic to infrastrucutural events – moreover, it provides a new inovation ecosystem in network infrastructure managing and operation. Although its significant tecnological growth, its deployment in enterprise and campus networks still lacks expressiveness. This slow adoption process of this technology is a direct consequence (i) a full deployment that requires a large investiment, (ii) a gradual deployment that requires the coexistency with legacy tecnologies and (iii) the lackness of a concrete examples of well-known migrations, a reason that also explain that lack of trust on this technology. The objective of this work is to investigate strategies to migrate from a traditional network to a hybrid or full SDN network, through the trade between of traditional to SDN switches. To achieve this, it has been proposed, implemented and tested three different strategies. The first one prioritizes switch which possess the higher degree (number of connections). The second one takes on account one or more parameters (bandwidth, network rush hour or whatever other aspect the operator thinks it is relevant) which are called links's weight. Finally, the third one prioritizes the network security, prioritizing forwarding devices which are connected to host machines. For each one of the strategies, it was made three tests: (i) latency test; (ii) throughput test; (iii) path length test. Following results, the degree based strategy was the best in the latency tests. But in the throughput test the security based strategy was the best. As a way of presenting a real setting, the Universidades Federal do Pampa (UNIPAMPA) was used as basis for this work.

Key-words: Software-Defined Networks(SDN). gradual deployment. network topology.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ACL *Acess Control List*

AD *Active Directory*

ARP *Address Resolution Protocol*

BGP *Border Gateway Protocol*

DDoS *Distributed Denial of Service*

GRE *Generic Routing Encapsulation*

ICMP *Internet Control Message Protocol*

IETF *Internet Engineering Task Force*

IGMP *Internet Group Management Protocol*

IP *Internet Protocol*

IS-IS *Intermediate System to Intermediate System*

LDAP *Lightweight Directory Access Protocol*

MAC *Media Access Control*

MV Máquina Virtual

NOS *Network Operating System*

NSH *Network Service Header*

OSPF *Open Shortest Path First*

OvS *Open vSwitch*

RFC *Request For Comments*

SDN *Software Defined Network*

SDNc *SDN-controlled*

SIE Sistema de Informações para o Ensino

SNMP *Simple Network Management Protocol*

UNIPAMPA Universidade Federal do Pampa

VLAN *Virtual Local Area Network*

VoIP *Voice over IP*

VPN *Virtual Private Network*

SUMÁRIO

1 INTRODUÇÃO

Redes IP tradicionais são constituídas por dispositivos de encaminhamento de pacotes que contém tanto a lógica de controle (isto é, plano de controle) quanto a de encaminhamento de dados (isto é, plano de dados) acoplados fisicamente no dispositivo (FEAMSTER; REXFORD; ZEGURA, 2014). A lógica do plano de controle determina como o plano de dados opera. Por exemplo, o protocolo de roteamento OSPF é executado (de maneira distribuída) pelo plano de controle. Uma vez que o algoritmo é executado, o plano de dados é configurado para operar de acordo, isto é, encaminhar/descartar pacotes para interfaces físicas. Em geral, o plano de controle de um dispositivo de rede IP implementa dezenas de protocolos para tarefas como roteamento (*Border Gateway Protocol* (BGP), *Open Shortest Path First* (OSPF), *Intermediate System to Intermediate System* (IS-IS)), gerenciamento (*Simple Network Management Protocol* (SNMP), *Internet Group Management Protocol* (IGMP), *Internet Control Message Protocol* (ICMP)), tunelamento (*Generic Routing Encapsulation* (GRE), *Virtual Private Network* (VPN), *Network Service Header* (NSH)). Esses equipamentos são configurados de maneira manual – através de interfaces de linha de comando (CLI) específicas de cada fabricante – para operarem de acordo com as necessidades/requisitos da infraestrutura de rede. Dada a diversidade de dispositivos em uma infraestrutura de rede e a variedade de protocolos a serem configurados em cada dispositivo físico, as redes IP (em larga escala) são extremamente complexas e difíceis de se gerenciar e manter, exigindo conhecimento técnico do operador em cada tecnologia ou outras especificidades de cada fabricante (KREUTZ et al., 2015).

O paradigma de Redes Definidas por Software (SDN – *Software-defined Networking*) surgiu com o intuito de solucionar problemas antigos das redes IP em diferentes frentes, como roteamento, engenharia de tráfego e segurança. (FEAMSTER; REXFORD; ZEGURA, 2014; KREUTZ et al., 2015). Com a lógica de controle atrelada fisicamente ao dispositivo físico, a configuração do plano de dados, isto é, como o dispositivo opera, é um processo inerentemente local, no dispositivo. SDN busca flexibilizar a relação entre os planos de controle e de dados através do desacoplamento físico entre eles. Este novo paradigma opera sob quatro pilares: (i) o plano de controle é separado fisicamente do plano de dados. (ii) as decisões de encaminhamento no plano de dados são baseadas em regras de fluxo, ao invés de regras baseadas em destino; (iii) a aplicação de controle é executada externamente e gerenciada por um Sistema Operacional de Rede (NOS – *Network Operating System* – conhecido como controlador SDN), que se comunica com os dispositivos físicos através de um protocolo de comunicação padrão (por exemplo, OpenFlow (MCKEOWN et al., 2008a)); e (iv) a rede passa a ser programada através de aplicações, executadas sobre o NOS, que dita como o plano de dados deve operar. Os princípios do SDN implicam na diminuição da complexidade da operação/gerenciamento das infraestruturas de rede. Entre os principais benefícios podem ser citados a simplificação, agilidade e flexibilidade no desenvolvimento de novas aplicações de controle e a facilidade

de gerenciar e reconfigurar uma infraestrutura de rede (KREUTZ et al., 2015)

Apesar de SDN oferecer benefícios diretos para a operação das redes, a migração de infraestruturas legadas (por exemplo, no campus da Universidade) ou em redes de larga escala (provedores de infraestrutura)(AMIN; REISSLEIN; SHAH, 2018) ainda representam desafios. A implantação de SDN implica em adquirir equipamentos com suporte ao paradigma (por exemplo, switches que suportam o protocolo OpenFlow). Existem duas abordagens para a implantação desse paradigma. A primeira, considera-se a substituição de todos os equipamentos, conhecido como abordagem *clean slate* – adotada no contexto de novas infraestruturas (como as redes de *datacenter*). Na segunda abordagem, a substituição dos equipamentos é parcial e progressiva. Note que a substituição parcial dos equipamentos implica em desafios quanto a coexistência de tecnologias/protocolos já consolidados em redes IP tradicionais – como, por exemplo, protocolos de roteamento. Parte dos grandes provedores de infraestrutura ainda não adotaram tecnologia para SDN por entender que o processo, mesmo que progressivo e planejado, ainda é significativamente desafiador.

Com o objetivo de definir uma abordagem para implementar SDN no campus Alegrete, foi necessário estudar a topologia do campus, que é composta por pontos de acesso sem fio (*access points*) e comutadores fisicamente distribuídos nos diferentes ambientes internos dos prédios, como corredores, salas de aula e laboratórios. Os prédios da instituição estão conectados através de enlaces não guiados (via rádio) e guiados (fibra e par trançado) os quais são comutados através de dispositivos de encaminhamento, como *switches*. Na borda da infraestrutura, há dois roteadores que conectam o campus à Internet, sendo um link principal e outro de contingência. A instituição provê diferentes serviços à comunidade acadêmica como sistemas virtuais de ensino, VoIP (voz sobre IP), serviços de impressão, laboratórios de informática e uma grande variedade de programas específicos.

Neste contexto, o objetivo principal deste trabalho é propor e avaliar estratégias algorítmicas para a migração de dispositivos de encaminhamento tradicionais para SDN, para o cenário da UNIPAMPA, campus Alegrete. Para tanto, investiga-se as técnicas e estratégias já propostas para a migração progressiva de redes tradicionais existente na literatura recente (por exemplo, (LEVIN et al., 2014; CARIA; DAS; JUKAN, 2015)). As propostas de redes híbridas, necessárias para a migração progressiva, têm sido alvo recente de investigação e representam um dos desafios de pesquisa e implantação de SDNs. Para avaliar as estratégias de migração propostas, de forma a atingir a meta do trabalho, realizou-se um levantamento das características da infraestrutura de rede do campus de Alegrete. O estudo da topologia de rede, dos serviços implantados e das políticas adotadas na infraestrutura serviram como base para determinar as estratégias propostas. De maneira resumida, as principais contribuições deste trabalho são:

- a proposta de diferentes estratégias para a migração de dispositivos de encaminhamento para SDN;

- a avaliação das estratégias propostas em ambientes emulados com características similares às observadas na infraestrutura de rede da UNIPAMPA.

O restante deste trabalho está organizado como segue. O Capítulo 2 apresenta a fundamentação teórica e um breve estado da arte em redes SDN híbridas. No Capítulo 3, discute-se a infraestrutura de rede do campus de Alegrete da UNIPAMPA. O Capítulo 4 apresenta as estratégias de migração proposta, enquanto que o Capítulo 5, a avaliação das mesmas. Por fim, o Capítulo 6 conclui esta monografia de conclusão de curso e apresenta perspectivas de trabalhos futuros.

2 FUNDAMENTOS E REVISÃO DO ESTADO DA ARTE

Este capítulo é dividido em duas partes. Na primeira parte, são apresentados a história, conceitos relacionados e potenciais benefícios das redes SDN. A segunda parte discute os trabalhos relacionados ao problema de migração de redes tradicionais para SDN.

2.1 Evolução das infraestruturas de rede até SDN

Em meados das décadas de 80-90, a Internet começava a extrapolar os domínios das Universidades e laboratórios de pesquisa para alcançar um público mais diversificado e abrangente (FEAMSTER; REXFORD; ZEGURA, 2014). Por conta desse acesso proliferado à Internet houve o surgimento de inúmeros novos serviços e no desenvolvimento de novos protocolos. O processo de tornar um protocolo "válido" na Internet passa pela aprovação em consenso pelo *Internet Engineering Task Force* (IETF) [1]. Em geral, o processo de discussão de uma ideia até sua concepção como uma recomendação (conhecido como *Request For Comments* (RFC)) demora de alguns meses a alguns anos. Motivados por esse processo lento de amadurecimento das tecnologias, surgiram alternativas para tornar as redes menos dependentes do processo desenvolvido pelo IETF. Em outras palavras, havia um anseio por modelos mais "abertos" e "ágeis". Dentro desse contexto, o primeiro conceito (e ancestral à ideia de SDN) são as redes ativas (ou *Active Networks*) (TENNENHOUSE et al., 1997).

Uma *Active Network* consiste em um padrão de comunicação que permite que os pacotes que passam por uma infraestrutura modifiquem dinamicamente a operação da rede (TENNENHOUSE et al., 1997). Essa abordagem é baseada no modelo conhecido como modelo em cápsula, no qual os pacotes que transitam na infraestrutura carregam o código a ser executado nos nós desejados – isto é, nos roteadores e *switches*. *Active Networks* forneceram três contribuições diretas para a concepção de SDN: (i) funções programáveis diminuem a barreira de inovação, (ii) virtualização e a capacidade de demultiplexar programas baseados em cabeçalhos de pacotes e a (iii) visão arquitetural unificada para orquestração de funções (ou *Middleboxes*).

Como mencionado, o processo lento de estabelecimento de um consenso no IETF prejudica a evolução ágil das infraestruturas e serviços. As *Active Networks* focaram na "programação" dos dispositivos através de instruções adicionadas aos fluxos, enquanto SDN prevê a "programação" dos dispositivos de maneira centralizada e mais coordenada. O conceito de redes ativas, neste contexto, é considerado a primeira tecnologia em direção a infraestruturas dinâmicas e flexíveis, como SDN. Em redes ativas, existem alguns componentes chave como, por exemplo, o sistema operacional, máquinas virtuais e programas. O sistema operacional gerencia recursos compartilhados na infraestrutura rede;

[1] <https://www.ietf.org/>

as máquinas virtuais coordenam a execução dos programas de rede. O processo de identificação das máquinas virtuais acontece através da de-multiplexação do cabeçalho do pacote. Similarmente, essa prática de de-multiplexação de pacotes se aplica no hardware dos dispositivos de encaminhamento SDN (através de regras aplicadas aos fluxos).

Apesar das *Active Networks* não terem sido implementadas em larga escala, lições no desenvolvimento arquitetural desse conceito foram essenciais para o desenvolvimento arquitetural do plano de controle das redes SDN. Nos anos 2000, o volume de tráfego das redes aumentou exponencialmente em comparação com a década anterior (TENNENHOUSE et al., 1997) – a principal razão deste aumento foi a proliferação de acesso residencial à Internet e os novos serviços. Ao mesmo tempo em que o tráfego de dados crescia nas infraestruturas, crescia também a preocupação com métricas de confiabilidade, previsibilidade e desempenho por parte dos provedores de infraestrutura. Esse fato motivou os operadores a buscarem alternativas para se obter um maior controle sobre a operação/gerenciamento das infraestruturas. Um exemplo clássico consiste no problema de determinar um caminho (rota) adequado para que os pacotes atinjam um determinado destino/prefixo. Os métodos existentes, na época, ainda eram limitados para se ter uma maior flexibilidade no controle sobre os caminhos adotados para o roteamento do tráfego. Um exemplo é o próprio algoritmo de caminhos mínimos (algoritmo de Dijkstra) implementado pelo protocolo OSPF (LONG H.; SHAH, 2018). Para se ter um maior nível de flexibilidade, os operadores ajustavam os "pesos" dados aos enlaces de maneira semi-manual para "forçar" a escolha de um determinado caminho (BURIOL et al., 2005). Ao longo dos anos, os pesquisadores, que reconheceram as frustrações dos operadores, buscaram as melhores soluções existentes e os esforços resultaram na separação entre o plano de dados e o de controle.

Os resultados da pesquisa resultaram em duas inovações: (i) uma interface de comunicação aberta entre os planos (ForCES – Forwarding and Control Element Separation) (DORIA A.; HALPERN, 2010); e (ii) um controle logicamente centralizado (arquitetura Routing Control Platform ou RCP) (CAESAR et al., 2005). Mesmo com a criação de ForCES, a interface acabou não tendo ampla adoção pelos fabricantes de dispositivos de encaminhamento. Por outro lado, o protocolo BGP popularizou-se como mecanismo para "programar" as tabelas de encaminhamento nos roteadores legados – permitindo a implantação imediata de caminhos alternativos entre domínios. Outra contribuição direta em relação ao ForCES consiste nos aspectos gerenciais de tais infraestruturas, os quais mais tarde ajudariam nas definições adotadas pelas redes SDN.

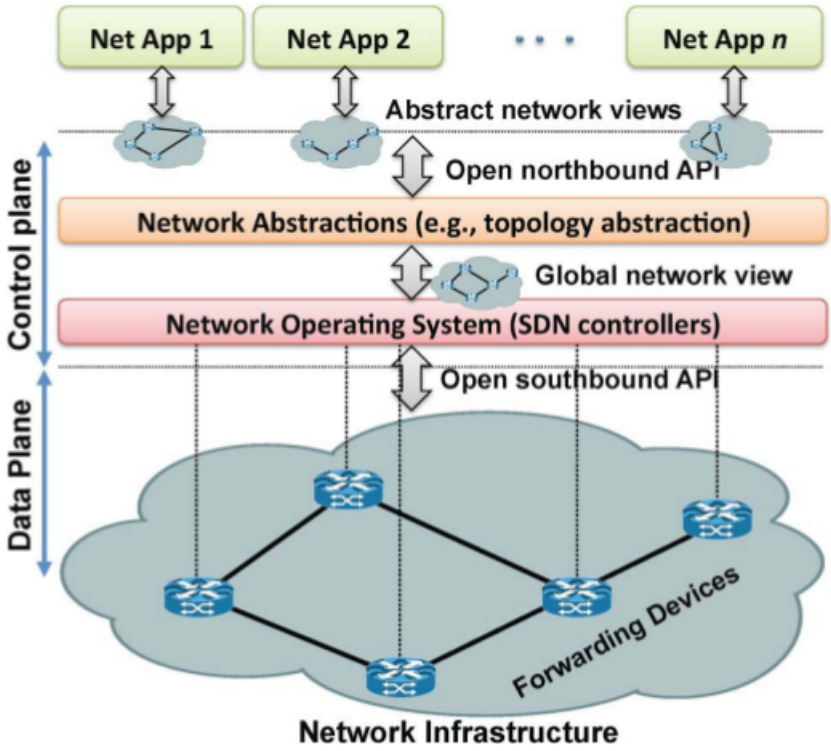
Até meados de 2008, a comunidade científica e a indústria compartilhavam de uma incerteza em relação a viabilidade técnica/prática de uma infraestrutura programável. O protocolo OpenFlow (MCKEOWN et al., 2008a) surgiu como uma resposta para esse problema, demonstrando o que poderia ser feito, na prática, com uma rede programável. OpenFlow é um protocolo de comunicação que permite interagir com o plano de dados

de um dispositivo de encaminhamento. Por meio de um software de controle, é possível controlar o comportamento dos dispositivos da infraestrutura – como discutido a seguir.

2.2 Redes Definidas por Software

SDN é um paradigma que busca desacoplar a camada de dados da camada de controle e promover a interação do operador da rede com aplicações de alto nível que executam sob a camada de controle (KREUTZ et al., 2015). As redes SDN são arquiteturalmente divididas em três camadas: (i) camada de aplicação, (ii) camada de controle e (iii) camada de dados, como ilustrado na Figura 1.

Figura 1 – Modelo em camadas do paradigma Redes Definidas por Software.



Fonte: Kreutz et al. (2015)

Na camada de aplicação, residem as aplicações que coordenam o funcionamento da infraestrutura (representadas no topo da Figura 1). As aplicações são escritas em linguagem de programação procedurais (como Java/Python) ou por meio de linguagens de domínio específico (por exemplo, Pyretic (REICH C. MONSANTO; WALKER, 2013) e Frenetic (FOSTER et al., 2010)) e são capazes de definir as políticas de funcionamento da rede pelo operador (TROIS et al., 2016). Por exemplo, uma aplicação poderia dinamicamente fornecer balanceamento de carga entre caminhos que interconectam dois ou

mais dispositivos em uma infraestrutura. Note que, mesmo neste exemplo simples, há uma enorme dificuldade de ser materializado em redes tradicionais IP – devido, principalmente, à dificuldade de se configurar equipamentos dinamicamente e de ter controle preciso das políticas de encaminhamento em operação. Outras aplicações incluem aspectos de segurança (por exemplo, Firewall sendo executado no plano de dados), ou a viabilização de encaminhamento de tráfego *Multicast* (ainda pouco expressivo nas infraestruturas de rede) – para mencionar algumas possíveis aplicações.

A camada de controle (na Figura 1, representado pelo controlador SDN – *SDN controller* – e abstrações de rede – *Network Abstractions*) é responsável pela interação entre as aplicações e os dispositivos de encaminhamento da infraestrutura. A camada de controle também é comumente conhecida por *Network Operating System* (NOS). A camada de controle tem ciência global dos elementos da infraestrutura de rede – sendo uma entidade logicamente centralizada, esse conhecimento permite manter informações sobre dispositivos de encaminhamento e enlaces ativos – assim como métricas de desempenho de cada um (por exemplo, número de pacotes transitados em uma interface de um determinado dispositivo). Essas informações são utilizadas como entrada para as aplicações executadas na camada de aplicação para o processo de tomada de decisão, como determinar a mudança de uma determinada rota. A camada de controle se comunica com a camada de aplicação através de uma interface conhecida como interface norte, ou *Northbound Interface*, enviando instruções aos dispositivos de encaminhamento, informando como tratar os fluxos de rede, através de uma interface, que precisa ser habilitada nesses dispositivo, conhecida como interface sul, ou *Southbound Interface*. É importante ressaltar que embora a interface *Southbound* mais utilizada seja o protocolo OpenFlow (MCKEOWN et al., 2008a) – que é amplamente adotada – não existe ainda um consenso sobre a interface *Northbound*, sendo esta dependente do controlador SDN em uso.

Na camada de dados, residem os dispositivos de encaminhamento de dados da infraestrutura. Os fluxos de dados são manipulados pelos dispositivos através de um sistema que filtra os pacotes e aplica ações, conhecido como *FlowTables*. Os filtros são definidos por via de regras para selecionar pacotes através de cabeçalhos conhecidos ou características presentes neles, como fluxos TCP ou fluxos TCP endereçados para porta 80. Uma vez que os pacotes são filtrados, aplica-se um conjunto de ações sobre os mesmos. Exemplos de ações incluem o envio do pacote para uma determinada interface do dispositivo ou o seu descarte. Na ausência de uma regra específica, aplica-se a regra geral, isto é, enviar para o controlador, que, em conjunto com a camada de aplicação, é responsável por instruir o dispositivo de encaminhamento em sua ação.

2.3 Protocolo OpenFlow

O conceito de SDN por si só já era uma grande evolução, mas ainda faltava uma interface para sua materialização e essa interface é o protocolo OpenFlow. Esse protocolo

surgiu a partir do estudo (CASADO et al., 2012) e seu propósito foi estimular vendedores a implementá-lo para que o problema da falta de inovação na área de redes de computadores fosse resolvido, que ocorre em um ritmo lento graças à grande quantidade de riscos, que podem resultar em um custo elevado por conta da dificuldade de gerenciamento das redes tradicionais. O protocolo OpenFlow fornece uma padronização para o SDN, utilizando diferentes cabeçalhos pré-definidos e um hardware já existente até mesmo em *switches* adicionais que são as *FlowTables*. As *FlowTables* são tabelas onde cada registro contém uma ação de acordo com um tipo de cabeçalho, uma ação a ser tomada de acordo com esse tipo e contadores que servem para medir estatísticas. Os registros da FlowTable de cada *switch* que possui o OpenFlow implementado são instalados pela controladora toda vez que o *switch* manda um requisição até ela pedindo instruções do que deve fazer com um certo fluxo de dados. Essa requisição ocorre quando um fluxo chega no *switch* SDN e ele não possui uma entrada para o cabeçalho; caso o *switch* já possua esse cabeçalho cadastrado ele irá simplesmente seguir as instruções recebidas anteriormente pela controladora.

2.4 Benefícios e potenciais casos de uso de SDN

O desacoplamento entre o plano de dados e o plano de controle, aliado com a visão global da infraestrutura, traz benefícios diretos para o gerenciamento e operação de infraestruturas de rede. Exemplos de casos de uso e seus benefícios incluem monitoramento e balanceamento de carga – descritos a seguir.

Dispositivos de encaminhamento com suporte ao protocolo OpenFlow permitem coletar informações relacionadas aos contadores de pacotes/bytes por interface ou regra de encaminhamento do dispositivo, possibilitando que esses dados sirvam de entrada para uma aplicação de monitoramento. Por exemplo, se há algum problema físico em algum dos enlaces ou se o padrão de tráfego da rede é alterado – é possível a identificação (e a reação) pela aplicação de controle. Essa funcionalidade também pode ser obtida em redes tradicionais, através de protocolos como o SNMP. Porém existem limitações, como (i) uma infraestrutura adicional, onde haveria a necessidade de um servidor que centraliza as estatísticas dos dispositivos de encaminhamento e (ii) a necessidade de implementar mais um protocolo ao dispositivo de encaminhamento.

A visão global da infraestrutura facilita e simplifica o balanceamento de carga entre os enlaces disponíveis (ou caminhos já estabelecidos). Suponha que a aplicação de controle identifique rajadas intermitentes (*burst*) de dados entre nós da infraestrutura, por exemplo, entre dois comutadores: C1 e C2. Em C2, considera-se que há um servidor de aplicação servindo um conjunto de requisições. As requisições, neste caso, são todas oriundas de C1. Entre C1 e C2 existem alternativas de interconexão (isto é, caminhos válidos). Na presença de rajadas de dados, a aplicação de controle – tendo ciência da infraestrutura (como, por exemplo, utilização do enlaces) – pode reencaminhar parte das requisições entre C1 e C2 por um caminho alternativo. Em outras palavras, as

aplicações de controle podem reagir aos dados monitorados de maneira dinâmica a fim de permitir um melhor desempenho e previsibilidade dos serviços de rede. Por fim, é importante ressaltar que os benefícios e casos de uso proporcionados pelo emprego de SDN em infraestruturas de rede não são limitados aos descritos nesta seção – pelo contrário, SDN permite uma grande variedade de casos de uso. A chave de tamanha flexibilidade em SDN reside no fato das interfaces entre os planos de controle e de dados são completamente abertas. Possibilitando, por exemplo, que desenvolvedores inovem ao projetar aplicações de controle disruptivas.

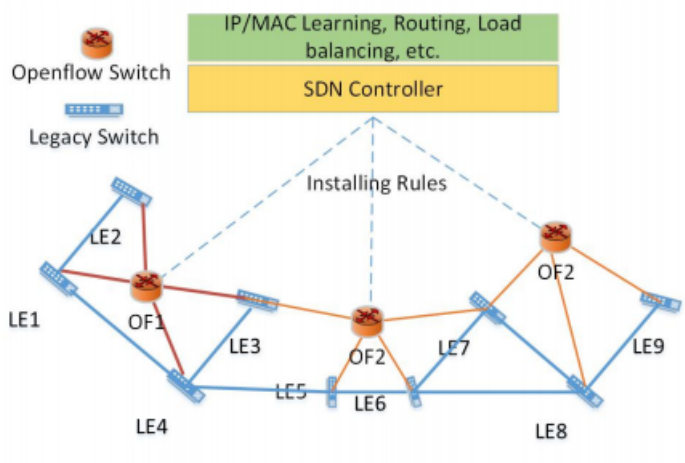
2.5 Redes híbridas

No contexto de uma migração progressiva e incremental, as infraestruturas contém dispositivos IP legados e novos dispositivos SDN disponíveis. Essa coexistência de dispositivos SDN e IP é conhecida como rede híbrida. A Figura 2 contém um exemplo de uma topologia híbrida, onde os comutadores SDN se comunicam com o controlador para obter informações de encaminhamento, enquanto que coexistem com comutadores legados. Existem dois principais fatores que limitam a utilização de SDN: (i) custo e (ii) a chance do risco acontecer (AMIN; REISSLEIN; SHAH, 2018). A migração progressiva e incremental é uma das formas de minimizar o impacto desses dois limitantes. Primeiro, ela permite a amortização de custos, já que os *switches* da rede serão trocados aos poucos e não todos de uma só vez. Segundo, ela permite diminuir a chance de riscos, como retroceder a rede programável à rede tradicional, ocorrerem, já que implementando *switches* SDN aos poucos faz com que os operadores da rede se adaptem melhor com a tecnologia. Outro exemplo de mitigação de risco ocorre por via de comutadores que implementam tanto o OpenFlow, quanto outros protocolos mais clássicos, resultando na possibilidade de voltar ao estado original da rede.

Antes de sugerimos infraestrutura para implantação de SDN na Unipampa, estudos diferentes trabalhos que propuseram suas próprias sugestões. Um deles foi (MCKEOWN et al., 2008b), onde os autores tinham o intuito de prover uma rede SDN para realizar pesquisa e, dessa forma, promover métodos inovadores, que têm sido escassos. Para isso, a rede SDN ocupava só parte da rede e garantia a separação do pesquisador, que usufruir das funcionalidades do paradigma sem prejudicar outros usuários normais, fazendo com que somente quem estivesse conectado a um *switch* de acesso SDN, teria a usabilidade do protocolo openflow.

Uma mudança nas redes tradicionais a partir da utilização de SDN também foi proposta em (CASADO et al., 2012). Porém, essa arquitetura busca englobar métodos tradicionais, como MPLS, junto com a utilização das controladores SDN, dizendo que o cabeçalho dos protocolos openflow são mais complexos (o que acaba exigindo mais do hardware) e a quantidade de cabeçalhos possíveis é muito grande e só tende a crescer (resultando em um problema de escalabilidade do protocolo openflow). O resultado é uma

Figura 2 – Rede híbrida com *switches* SDN.



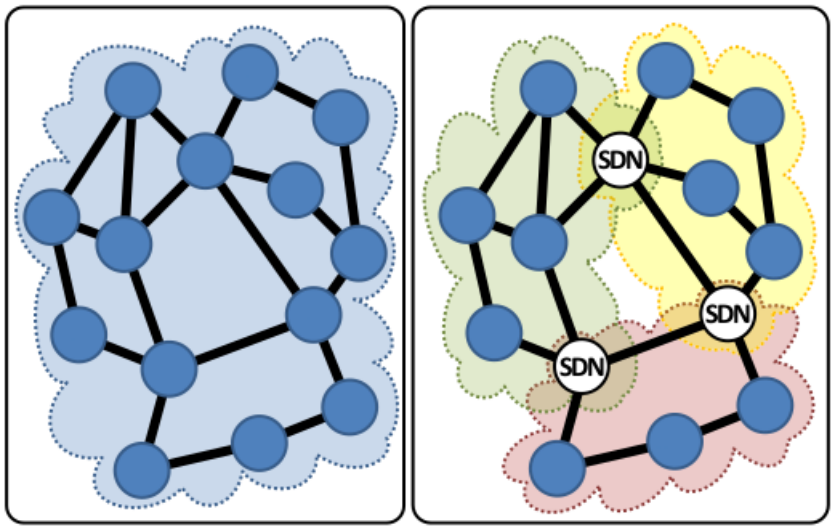
Fonte: Amin, Reisslein e Shah (2018)

arquitetura separada por dois grupos de *switches*: (i) *switches* SDN, que desempenham o papel do acesso a rede e (ii) *switches* tradicionais, que são os dispositivos de distribuição. Cada um desses dois grupos estão conectados a uma controladora diferente e logicamente separada. Os *switches* SDN aplicam tanto às exigências por parte do host quanto às políticas da rede, enquanto os *switches* comuns realizam o encaminhamento de pacotes.

No trabalho de Caria *et al.* (CARIA; DAS; JUKAN, 2015), propõe-se uma topologia de rede SDN híbrida buscando otimizar aspectos de roteamento interno e externo. O roteamento interno é realizado a partir do protocolo OSPF (por dispositivos IP legados) e o roteamento externo é realizado a partir de aplicações de controle SDN. Os roteadores de borda interagem diretamente com uma controladora SDN e, portanto, fornecem uma visão global da infraestrutura de rede. A aplicação de controle ajusta, de maneira dinâmica, o roteamento e as prioridades dos fluxos de acordo com as condições observadas na rede. A topologia de rede híbrida proposta por Caria *et al.* considera que os roteadores de borda de cada domínio operaram sob uma controladora SDN, enquanto que os dispositivos internos de cada domínio permanecem legados (ilustrado na Figura 3). De acordo com os autores, essa estratégia permite que uma menor proporção de dispositivos sejam modificados/migrados, enquanto que é possível beneficiar a infraestrutura das operações mais dinâmicas de SDN.

Em (LEVIN et al., 2014) é proposta uma estratégia de coexistência entre dispositivos, legados e SDN, baseada em dois princípios: (i) *policy enforcement* e (ii) *fine-grained control*. *Policy enforcement* garante que, para qualquer caminho de roteamento estabelecido na infraestrutura, deva existir pelo menos um dispositivo com suporte a SDN entre os dispositivos do caminho. Assim, é possível aplicar as políticas de operação da rede para qualquer fluxo que transita pela infraestrutura – já que em qualquer caminho, há

Figura 3 – Topologia com dispositivos IP legados (esquerda) vs. topologa híbrida (direita).



Fonte: Caria, Das e Jukan (2015)

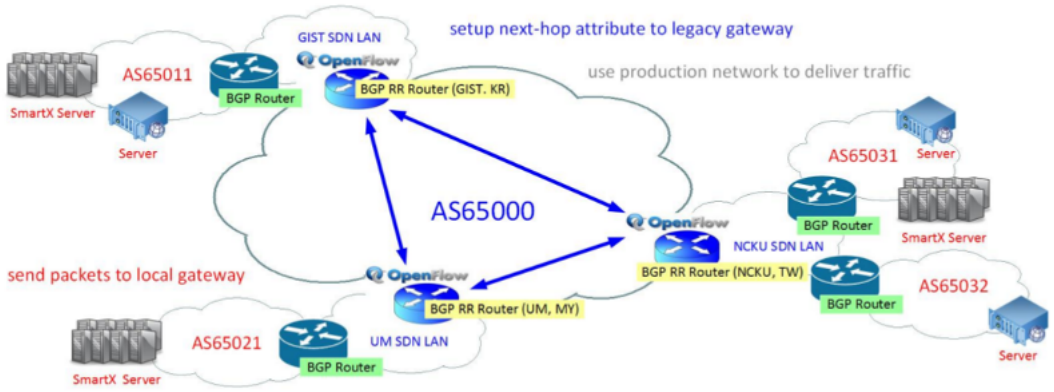
pelo menos um dispositivo SDN. Já *fine-grained control* garante que, se um determinado fluxo é encaminhado por mais de dois dispositivos SDN em um caminho, é possível realizar/aplicar políticas de tráfego mais específicas – por exemplo, balanceamento de carga.

Para garantir esses dois princípios, o operador deve selecionar um conjunto de portas a serem controladas pelo controlador SDN. Essas portas são conhecidas por portas *SDN-controlled* (SDNc). O problema consiste em garantir que todo fluxo de rede passe por, pelo menos, uma porta SDNc. O princípio de garantir que todo o tráfego seja encaminhado através de um ponto da infraestrutura é conhecido com *SDN Waypoint Enforcement*. A operacionalização desse conceito é realizada através de encaminhamentos minuciosos do tráfego de rede pelas aplicações de controle. Os dispositivos legados são configurados com *spanning trees* específicas para garantir que o tráfego (mesmo que oriundo de dispositivos IP legados) sejam encaminhados corretamente para alguma porta SDNc.

O trabalho de Tsai *et al.* (USMAN ARIS CAHYADI RISDIANTO, 2016) propõe uma solução para a operação híbrida em infraestruturas WAN tradicionais. O objetivo consiste em monitorar o tráfego de rede por meio de soluções baseadas em SDN e, através da visão global coletada da infraestrutura, auxiliar na tomada de decisão de protocolos IP legados, como o protocolo de roteamento BGP. A abordagem proposta pelos autores considera que a comunicação inter-domínio é determinada através de roteamento tradicional BGP, como ilustrado na Figura 4. Ainda, os dispositivos de borda (roteadores BGP) são habilitados ao protocolo OpenFlow, o que permite monitorar as trocas de mensagens BGP e padrões de tráfego de maneira flexível e dinâmica – oferecendo a possibilidade de

rotas eventualmente mais otimizadas entre domínios.

Figura 4 – Rede híbrida com dispositivos de encaminhamento SDN em uma rede IP legada.



Fonte: Usman Aris Cahyadi Risdianto (2016)

Há também outros trabalhos que exploram os aspectos de SDN em redes híbridas para mitigar ataques em infraestruturas de rede. Como exemplo desses trabalhos, é possível citar a abordagem de Ubaid *et al.* (UBAID FAISAL BIN UBAID; IQBAL, 2018), que propõe detectar automaticamente ataques e mitigá-los em um infraestrutura SDN híbrida. Redes SDN adotam novos mecanismos para proteger usuário de diferentes tipos de ataques, como por exemplo, *Distributed Denial of Service* (DDoS) ou *spoofing* do protocolo *Address Resolution Protocol* (ARP) ou *Internet Protocol* (IP). Esses ataques funcionam de modo que o atacante modifica os pacotes/frames a fim de mascarar seu endereço de origem (IP e/ou *Media Access Control* (MAC)) por um já existente na infraestrutura de rede. Esse tipo de mascaramento é comum em ataques do tipo *man-in-the-middle*. No contexto de redes SDN, é importante garantir a segurança da aplicação de controle (e do NOS da rede) – para o correto funcionamento das aplicações. O trabalho de Ubaid *et al.* (UBAID FAISAL BIN UBAID; IQBAL, 2018) objetiva prevenir às redes SDN híbridas de ataques como DDoS, *spoofing* e ataques de inundação do enlace (LFA). No mecanismo proposto, a controladora SDN é protegida dos atacantes através de estratégias que desviam o tráfego malicioso para um "black hole". Além disso, a aplicação de controle encaminha mensagens ARP para um servidor em que as mensagens ARP são analisadas – podendo detectar um possível ataque.

3 TOPOLOGIA DE INFRAESTRUTURA

A migração parcial da infraestrutura do campus Alegrete para SDN requer o detalhamento da infraestrutura subjacente. Assim como outras Infraestruturas IP em operação, é complexa e fornece uma boa quantidade de serviços. Em uma rede de campus, como é o caso, o número de dispositivos de acesso e de agregação de tráfego é elevado, assim como a gama de serviços oferecidos. Essas são algumas das razões pelas quais concluímos que a migração da rede do campus (mesmo que parcial e incremental) deve ser planejada de maneira a não causar disrupção nos serviços em operação.

A infraestrutura de rede do campus é centrada no *datacenter* do campus, o qual concentra os equipamentos mais críticos e com maior relevância para a infraestrutura de serviços da instituição, como os servidores de aplicação (tais como o Moodle), roteadores de borda, firewall e controladora wireless. Os demais dispositivos, como pontos de acesso sem fio e *switches* de distribuição, estão localizados em salas e corredores dos prédios, conforme ilustrado na Figura 5. Logo abaixo da desta figura, está a sua legenda, representada na Figura 6.

O *switch* principal da rede (*switch core*) é o dispositivo com melhor desempenho (capacidade) e concentra o roteamento da infraestrutura interna do campus – além de controlar o acesso à rede interna por meio de *Acess Control List* (ACL). ACLs, em geral, estão definidas de acordo com a *Virtual Local Area Network* (VLAN) que o dispositivo está atribuído. Ele também está conectado ao firewall, cuja função é implementar e aplicar as políticas de tráfego.

Os demais *switches* da infraestrutura dividem a responsabilidade de agregar o fluxo de dados e prover acesso a dispositivos finais – como workstations, pontos de acesso sem fio, antenas e outros ativos. Os pontos de acesso sem fio operam o protocolo 802.1x, o qual permite a autenticação dos usuários de forma dinâmica. Este protocolo permite, também, vincular automaticamente um usuário a uma VLAN. Por fim, ainda existem as comunicações sem fio ponto-a-ponto que interligam a maioria dos prédios do campus.

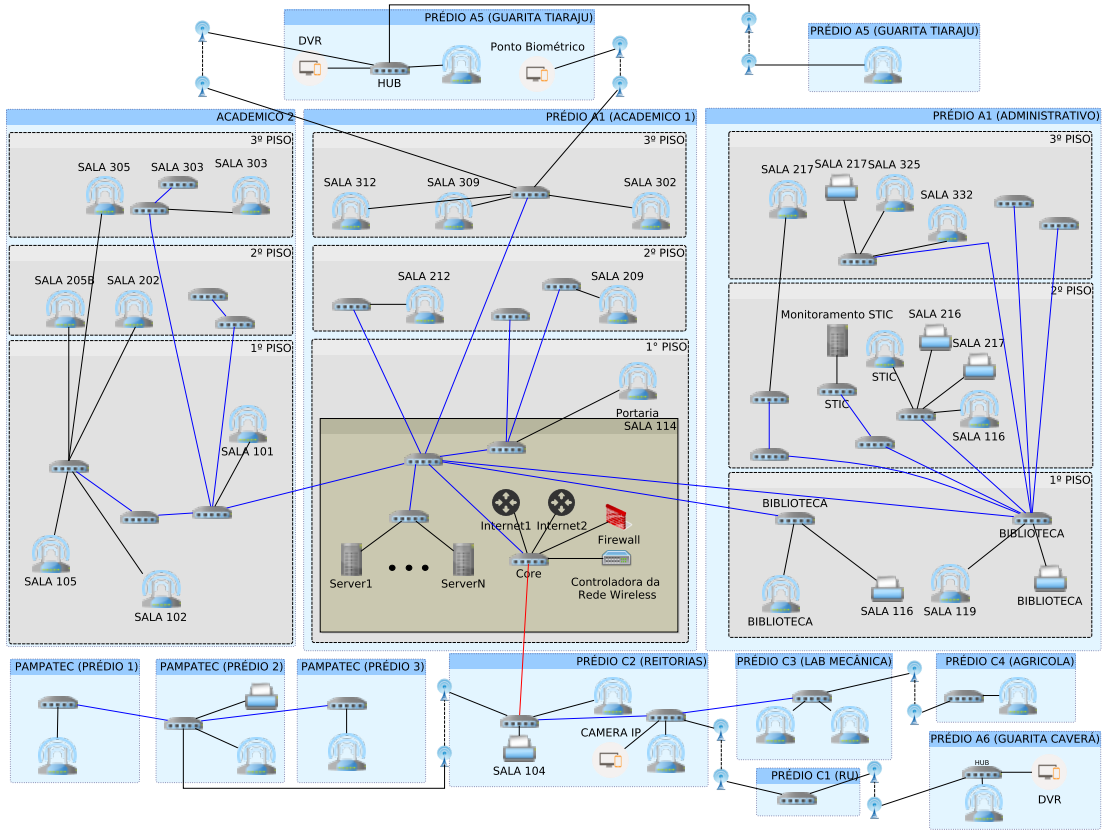
O domínio do campus é dividido em cinco grupos, armazenados em um serviço de diretório implementado através do protocolo *Lightweight Directory Access Protocol* (LDAP) chamado de *Active Directory* (AD), cuja função é manter as informações dos usuários para consultas de autenticação. Esses grupos são os seguintes: Alunos, Docentes, Técnicos, Visitantes e Bolsistas. Integrantes dos grupos Alunos, Docentes e Técnicos e Visitantes são inseridos automaticamente, sendo os integrantes dos três primeiros grupos inseridos após o cadastro no Sistema de Informações para o Ensino (SIE) e o último no cadastro de usuários externos. Integrantes do grupo Bolsistas devem ser inseridos manualmente. Depois que um usuário está cadastrado no sistema, ele passa a ter acesso a três redes diferentes no campus, dependendo do grupo em que foi cadastrado. A rede UNIPAMPA oferece acesso à Internet e à rede interna do campus e permite que somente os grupos Docentes, Técnicos e Bolsistas, que são autenticados na rede via matrícula e

senha, se conectem a ela via protocolo 802.1x. A rede UNIPAMPA-ALUNOS oferece somente acesso à Internet e permite acesso aos grupos Alunos, Visitantes, Docentes e Técnicos, via autenticação web. A rede UNIPAMPA-VISITANTES se difere da rede UNIPAMPA-ALUNOS apenas pelas faixas de endereços IPs atribuídos – sendo as políticas de gerenciamento as mesmas.

Para flexibilizar o gerenciamento da rede e fornecer mais segurança, a rede do campus é dividida em duas VLANs: a eduroam e a unipampa. Essas VLANs limitam o acesso aos equipamentos institucionais ou provém acesso às redes do campus. Algumas VLANs oferecem funcionalidades mais específicas, como a VLAN *Voice over IP* (VoIP) – que oferece o serviço de telefonia IP do campus. Outro exemplo é a VLAN Servidores, que oferece acesso aos diversos serviços da rede interna.

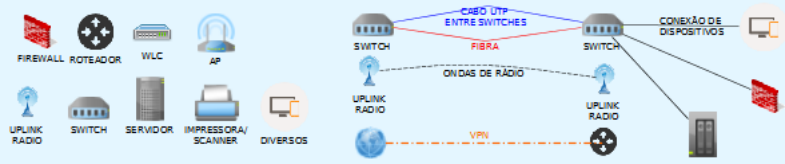
Por fim, vale destacar que nos horários de pico, os enlaces da rede são utilizados em toda sua capacidade, e para que se possa manter serviços essenciais (VoIP, SIE, entre outros), há a priorização (ou limitação) de serviços por meio de reserva de banca no firewall. Essa priorização dos serviços fazem com que serviços que não essenciais sofram uma perde de desempenho.

Figura 5 – Topologia da rede do campus de Alegrete. Legenda representada na Figura 6



Fonte: Adaptado da topologia fornecida pelo NTIC

Figura 6 – Legenda da figura da Topologia do campus Alegrete



Fonte: Adaptado da topologia fornecida pelo NTIC

4 ESTRATÉGIAS PROPOSTAS DE MIGRAÇÃO

Neste capítulo são apresentadas as estratégias algorítmicas propostas para realizar a migração de uma rede tradicional para SDN. Como mencionado anteriormente, a migração de dispositivos tradicionais de rede para SDN deve ser feita progressivamente de maneira que o impacto na operação da infraestrutura seja mínimo. Foram propostas três estratégias: *(i)* baseada no número de interconexão de cada dispositivo; *(ii)* baseada no peso de cada enlace de interconexão; e *(iii)* baseada em aspectos de segurança de cada dispositivos (por exemplo, aqueles mais suscetíveis a ataques). Nestas estratégias propostas, considera-se que a infraestrutura de rede é representada por um grafo $G = (V, E)$ onde o conjunto V representa os dispositivos de encaminhamento, e o conjunto E representa os enlaces interconectando pares de dispositivos $(u, v) \in V$. O método utilizado para a criação do conjunto E, está representada no Algoritmo 1. As seções abaixo descrevem as estratégias propostas.

```
graph = nx.Graph();
add_switches();
add_hosts();
weighted_edges = array();
for node1 in node_dictionary do
    for node2 in node_dictionary[node1] do
        if node2 != 'switch' then
            weighted_edges.add( (node1, node2, 500) );
        else
            weight = random.generate_random_number_from(1, 60)
             weighted_edges.add( (node1, node2, weight) );
        end
    end
end
graph.add_weighted_edges_from(weighted_edges)
```

Algorithm 1: Método utilizado para adicionar nodos na topologia.

4.1 Estratégia baseada no número de interconexão de cada dispositivo

A estratégia baseada no número de interconexões considera o grau de cada dispositivo (isto é, o número de enlaces incidentes) como mecanismo de seleção (ou priorização) de dispositivos IP a serem substituídos por dispositivos SDN. Esta estratégia prioriza dispositivos que potencialmente tenham maior volume agregado de tráfego na infraestrutura de rede. Dessa forma, ao substituir tais dispositivos, a operação da infraestrutura como um todo é flexibilizada a partir dos benefícios de SDN.

Na estratégia baseada no número de interconexões de cada dispositivos, ordena-se os vértices V em relação ao grau de cada vértice ($\delta(v)$). Posteriormente, seleciona-se os k primeiros dispositivos de encaminhamento (isto é, com maior grau) para serem migrados

para SDN. A ordenação dos vértices está representada no Algoritmo 2. Observe-se que a complexidade de pior caso do procedimento é expressa por $O(nlogn)$.

```
degree_array = graph.degree_array;
sorted_list = list(sort( degree_array, key=lambda x: x[1], sort=Decreasing ) )
```

Algorithm 2: Estratégia baseada no número de interconexão de cada dispositivo.

4.2 Estratégia baseada no peso do enlace de interconexão

Diferente da estratégia anterior, a qual prioriza a migração de dispositivos bem interconectados, esta estratégia objetiva priorizar o "peso"dos enlaces considerados. Os pesos atribuídos aos enlaces podem ser atributos relevantes para a infraestrutura, como o volume de tráfego medido, a importância (ou criticidade) do enlace, ou a largura de banda aprovisionada. O algoritmo proposto é agnóstico ao tipo de peso e considera pesos arbitrário. Na prática, tais pesos podem ser substituídos de acordo com a necessidade da infraestrutura ou do operador.

Inicialmente, atribui-se um peso aos enlaces do grafo que representa a topologia da infraestrutura. Para isso, itera-se entre todos os pares de vértices do grafo, atribuindo um peso para cada enlace. Note que este procedimento tem complexidade $O(n^2)$. O Algoritmo 3 ilustra o procedimento proposto. No algoritmo, caso os vértices sejam dispositivos de encaminhamento (*switches*), eles são adicionados em um vetor “peso_nodos ”, criado com a finalidade de armazenar todos os nodos que não são hosts. Ao final do procedimento, retorna-se o vetor que contém a informação dos vértices e o peso da aresta. Por fim, a estrutura é ordenada de maneira crescente de acordo com o peso – procedimento com complexidade $O(nlogn)$.

```
Function get_weighted_switches(graph, switches):
    weighted_switches = [];
    for switch in switches do
        switch_weight = 0;
        for s1,s2 in graph.edges(switch) do
            switch_weight+ = graph[s1][s2]['weight'];
        end
        weighted_switches.add( (switch, switch_weight) );
    end
    return weighted_switches
End Function
weighted_switches_array = get_weighted_switches();
sorted_list = list(sort( weighted_switches_array;, key=lambda x: x[1],
 sort=Ascending ) )
```

Algorithm 3: Estratégia baseada em aspectos de peso dos enlaces.

4.3 Estratégia baseada em questões de segurança

Diferente das estratégias anteriores, em que o foco está relacionado com propriedades da infraestrutura (grau de vértice e pesos de enlaces), esta estratégia foca na criticidade de serviços em operação. Esta estratégia visa utilizar a programabilidade dos dispositivos de encaminhamento para garantir maiores níveis de segurança entre os hosts finais. Para isso, o mecanismo proposto prioriza a substituição de dispositivos de encaminhamento mais próximos dos hosts finais. Já que a parte da rede onde um usuário comum tem acesso a rede é justamente em uma máquina hosts, possibilitando uma série de diferentes ameaças.

Para ordenar os *switches*, foram utilizados dois vetores, um que continha somente *switches* conectados aos hosts e outro que continha todos os *switches* da rede. Para cada um desses vetores foram realizadas iterações por via de laços. No primeiro laço, o vetor iterado é o que contém todos os *switches* que possuem ligação com hosts da rede, para cada *switch* da iteração, foi atribuído um valor que corresponde a relevância do *switch*. Já no segundo laço, todos os *switches* da rede são iterados, sendo adicionado somente os que ainda não estão na lista. Quando *switches* novos, os que não foram adicionados no primeiros laço, são adicionados na nova lista, eles são atribuídos com um valor menor que os *switches* iterados anteriormente, o que explicita uma menor relevância em relação a sua troca na topologia.

```
Function get_secure_switches(switches, switches_with_hosts_array):
    secure_switches = [];
    for switch in switches_with_hosts_array do
        secure_switches.add( (switch, 1) )
    end
    for switch in switches do
        if not_in_secure_switches(switch) then
            secure_switches.add( (switch, 0) )
        else

        end
    end
    return secure_switches;
End Function
secure_switches_array = get_secure_switches();
sorted_list = list(sort( secure_switches_array;, key=lambda x: x[1],
 sort=Ascending ) )
```

Algorithm 4: Estratégia baseada em aspectos de segurança.

5 AVALIAÇÃO

Esta seção apresenta a avaliação analítica e por meio de emulação da implementação das estratégias de migração propostas neste trabalho. A Seção 5.1 descreve o ambiente e os parâmetros utilizados na avaliação, enquanto que a Seção 5.2 apresenta e discute os resultados obtidos.

5.1 Ambiente e Carga de Trabalho

As estratégias foram implementadas na linguagem Python, em sua versão 2.7 com o auxílio das bibliotecas `graphviz` e `networkx`. Em todos os experimentos, a topologia da UNIPAMPA (descrita no Capítulo 3) foi utilizada. A topologia é composta por 80 dispositivos de encaminhamento e 79 enlaces físicos. Para o propósito desta avaliação, considera que cada dispositivo de encaminhamento tem um host diretamente conectado a ele – totalizando 80 hosts na topologia. As avaliações foram realizados em uma máquina virtual Máquina Virtual (MV), cujas especificações estão presentes na tabela 1. A máquina virtual foi executada em um notebook, suas configurações estão representadas na tabela 2. A máquina virtual utilizada é livremente disponibilizada[1] por Mininet. O Mininet é um ambiente de emulação SDN que permite criar redes virtuais executadas diretamente no Kernel de sistemas operacionais Linux. Os dispositivos de encaminhamento são criados a partir de instâncias de *switches* virtuais com suporte a SDN (por exemplo, *Open vSwitch* (OvS)) e interconectados através de *bridges* virtuais. Isso permite instanciar e emular qualquer topologia de rede em uma única máquina.

O objetivo da avaliação consiste em comparar as estratégias propostas de maneira a definir qual estratégia seria a mais adequada para a migração da rede tradicional para uma infraestrutura SDN no contexto da infraestrutura de rede da UNIPAMPA. Essas comparações foram feitas a partir de três métricas de desempenho: *(i)* o atraso médio

[1] <http://mininet.org/>

Ambiente Físico	**Especificações**
Cores	1
Memória RAM	1 GB
Sistema Operacional	Ubuntu Server 14.10

Tabela 1 – Ambiente virtual

Ambiente Físico	**Especificações**
Processador	Intel core i5, 2a geração
Memória RAM	1 GB
SSD	240 GB
Sistema Operacional	Ubuntu 17.10

Tabela 2 – Ambiente físico

fim-a-fim entre hosts *(ii)* a vazão máxima atingida e *(iii)* o comprimento do caminho entre os hosts (medido pela quantidade de enlaces por onde a informação passou até chegar no destino, também conhecido pelo nome de "hops"). Para cada experimento, variou-se o número de dispositivos de encaminhamento migrados para SDN de 1 até 9 (isto é, número de dispositivos da infraestrutura), dado que o um gráfico contendo 80 resultados prejudicaria a visibilidade dos dados. Para a condução dos experimentos que medem o atraso fim-a-fim na infraestrutura emulada, executou-se o comando `ping` em todos os pares de hosts da infraestrutura através da função `pingFull()` disponibilizada pela API do Mininet. Para a condução de experimentos de vazão, executou-se a ferramenta `iperf` (configurada para modo de transmissão TCP) em todos os pares de hosts da infraestrutura configurada. Foram feitas 10 execuções para cada um dos pares de hosts considerados tanto nos testes de medição do atraso quanto nos de vazão. Por fim, avaliou-se o comprimento dos caminhos adotados pelos pares de hosts da infraestrutura. Em todos os experimentos conduzidos, considera-se que os fluxos de rede entre quaisquer pares hosts conectados à infraestrutura devem ser encaminhados por, no mínimo, um dispositivo de encaminhamento SDN. Por fim, vale destacar que os experimentos de cada estratégia foram realizados em execuções diferentes (por exemplo, na primeira execução foi medida a estratégia baseada por grau).

5.2 Resultados

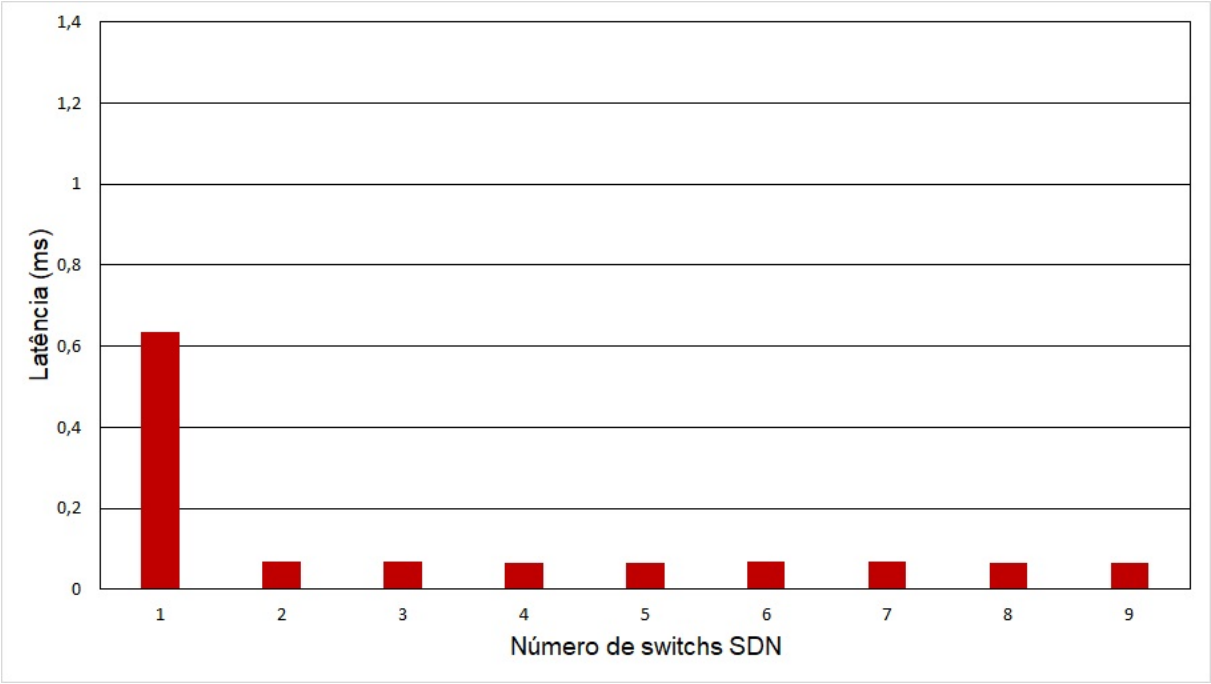
5.2.1 Atraso fim-a-fim introduzido pelas estratégias de migração.

As Figuras 7, 8 e 9 ilustram o atraso médio observado na infraestrutura emulada da UNIPAMPA quando aplicada as diferentes estratégias de migração propostas. A Figura 7 ilustra o atraso médio introduzido pela migração de dispositivos de encaminhamento seguindo a estratégia baseada no número de interconexões dos dispositivos, enquanto que as Figuras 8 e 9 ilustram, respectivamente, os atrasos introduzidos pela estratégia baseadas no peso dos enlaces e baseada em questões de segurança.

Observa-se que a aplicação das estratégias de migração de dispositivos de encaminhamento introduz um comportamento do atraso médio fim-a-fim similar em todas as estratégias, que há um valor: (i) alto e variado quando há somente 1 *switch* SDN na rede e (ii) consideravelmente menor, estável e similar nos outros casos. No caso da estratégia baseada no grau, a adição do primeiro *switch* gera uma latência 6 vezes maior em comparação aos outros resultados. Na estratégia baseada no peso, a diferença entre a adição do primeiro *switch* e dos outros dispositivos foi 10 vezes maior. Por último, a estratégia baseada na segurança resultou em uma diferença de aproximadamente 12 vezes maior em relação ao primeiro *switch* com os outros resultados, ou seja, esta estratégia representou a maior latência entre os três testes. O aumento significativo da latência na adição do primeiro *switch* ocorre porque no início da comunicação entre os hosts, o protocolo ARP ainda está estabelecendo o melhor caminho entre os hosts e gera um maior atraso entre as

comunicações. Já a diferença da latência no primeiro *switch* entre as diferentes estratégias ocorre em razão do aumento do comprimento dos caminhos entre os pares de hosts da infraestrutura. Quanto maior o número de dispositivos SDN presentes na infraestrutura (isto é, maior número de dispositivos de encaminhamento migrados), maior é a chance do dispositivo SDN migrado pertencer ao conjunto de dispositivos pertencentes ao caminho mínimo original entre os hosts da infraestrutura. À partir desta análise, conclui-se que a estratégia baseada por grau obteve os melhores resultados de latência, já que gerou o menor caminho entre os hosts, dado que seu atraso no primeiro *switch* da topologia foi o menor entre as três estratégias.

Figura 7 – Avaliação do atraso fim-a-fim introduzido pela migração de dispositivos de encaminhamento utilizando a estratégia baseada no número de interconexões dos dispositivos.



5.2.2 Vazão observada a partir das estratégias de migração.

As Figuras 10, 11 e 12 ilustram a vazão média observada na infraestrutura emulada da UNIPAMPA quando aplicada as diferentes estratégias de migração propostas. A Figura 10 ilustra a vazão média máxima alcançada quando os dispositivos de encaminhamento são migrados seguindo a estratégia baseada no número de interconexões dos dispositivos, enquanto que as Figuras 8 e 9 ilustram, respectivamente, as vazões máximas atingidas pela estratégia baseada no peso dos enlaces e baseada em questões de segurança.

Observa-se que a aplicação das estratégias de migração baseada no número de interconexões e na segurança dos enlaces tiveram os melhores resultados nesta medição,

Figura 8 – Avaliação do atraso fim-a-fim introduzido pela migração de dispositivos de encaminhamento utilizando a estratégia baseada no peso do enlaces.

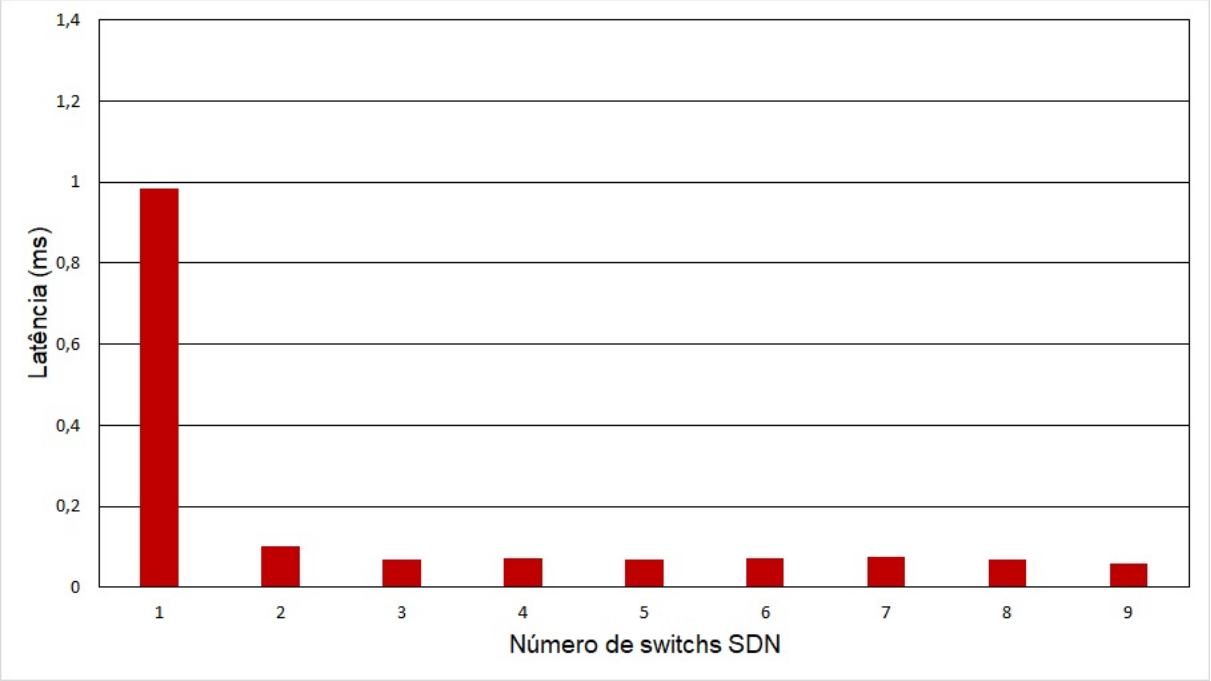
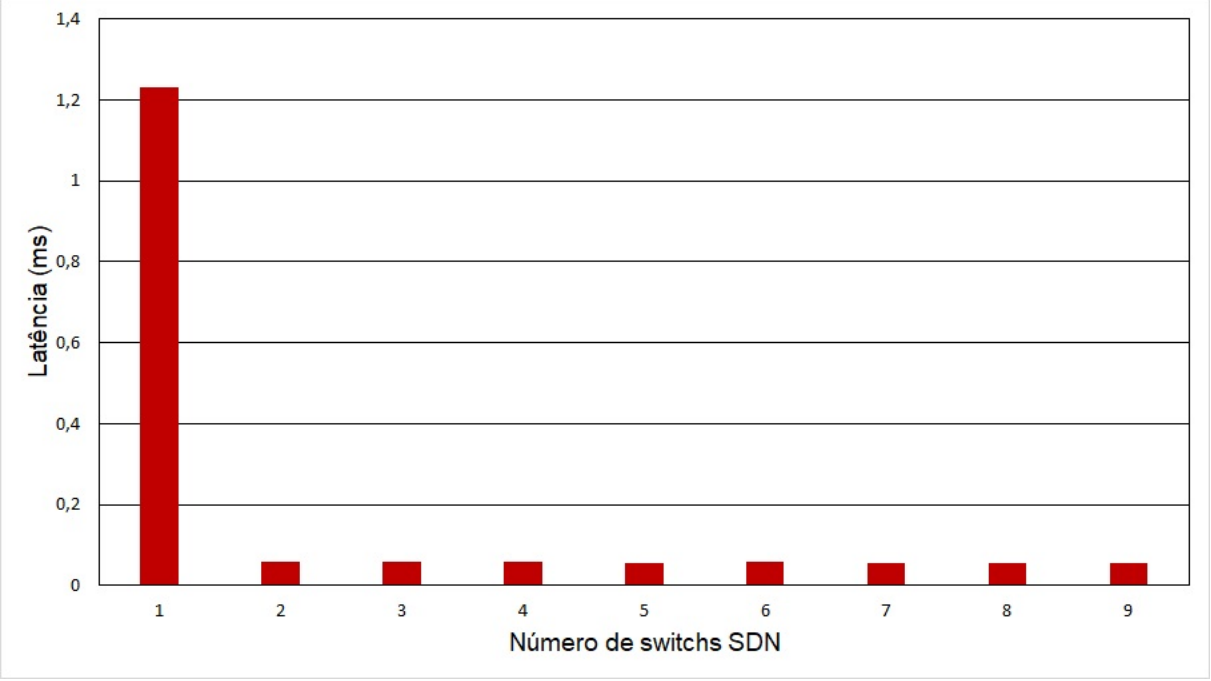


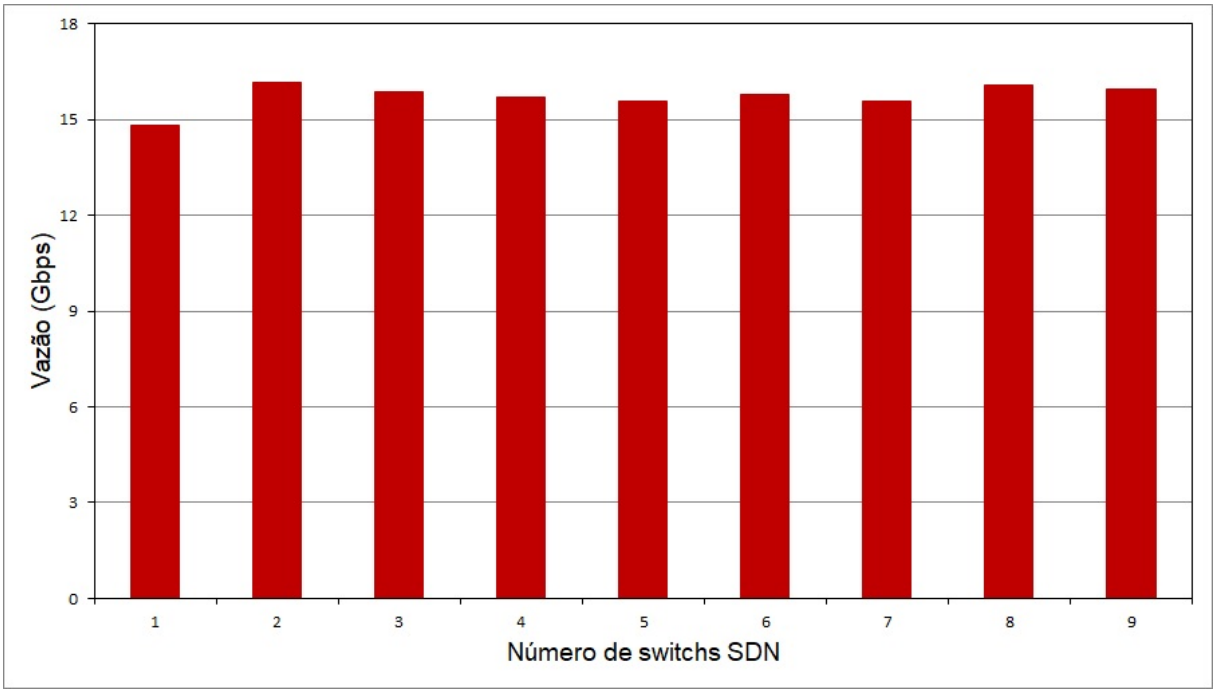
Figura 9 – Avaliação do atraso fim-a-fim introduzido pela migração de dispositivos de encaminhamento utilizando a estratégia baseada em aspectos de segurança.



enquanto a estratégia baseada por peso representou os piores resultados. Os resultados nessa medição, em todas as estratégias sofreram variações, sendo o valor os valores que

foram variados, variam conforme as estratégias. No caso das estratégias baseadas por grau e por segurança dos enlaces, esses valores variaram entre 15 à 16 Gbps, já na estratégia baseada por peso esses valores variaram entre 14 à 15 Gbps. Fazendo uma média geral entre todos os resultados obtidos de cada estratégia, as estratégias por grau, por peso e por segurança, obtiveram, respectivamente: 15,72 Gbps, 14,55 Gbps e 15,69 Gbps. Com isso é possível concluir que apesar da estratégia baseada em segurança ter obtido resultados melhores com a implementação do primeiro *switch*, de forma geral ela se demonstrou resultados inferiores em relação a estratégia por grau, mesmo que tenha sido por uma diferença pequena. Já a estratégia baseado no peso dos enlaces, demonstrou uma diferença maior no resultado de vazão, obtendo resultados com diferenças maiores que 1 Gbps em relação às outras duas estratégias. O motivo desses resultados pode ser explicado devido aos *switches* SDN selecionados para cada estratégia estarem mais próximos ou mais distantes das máquinas hosts durante a comunicação.

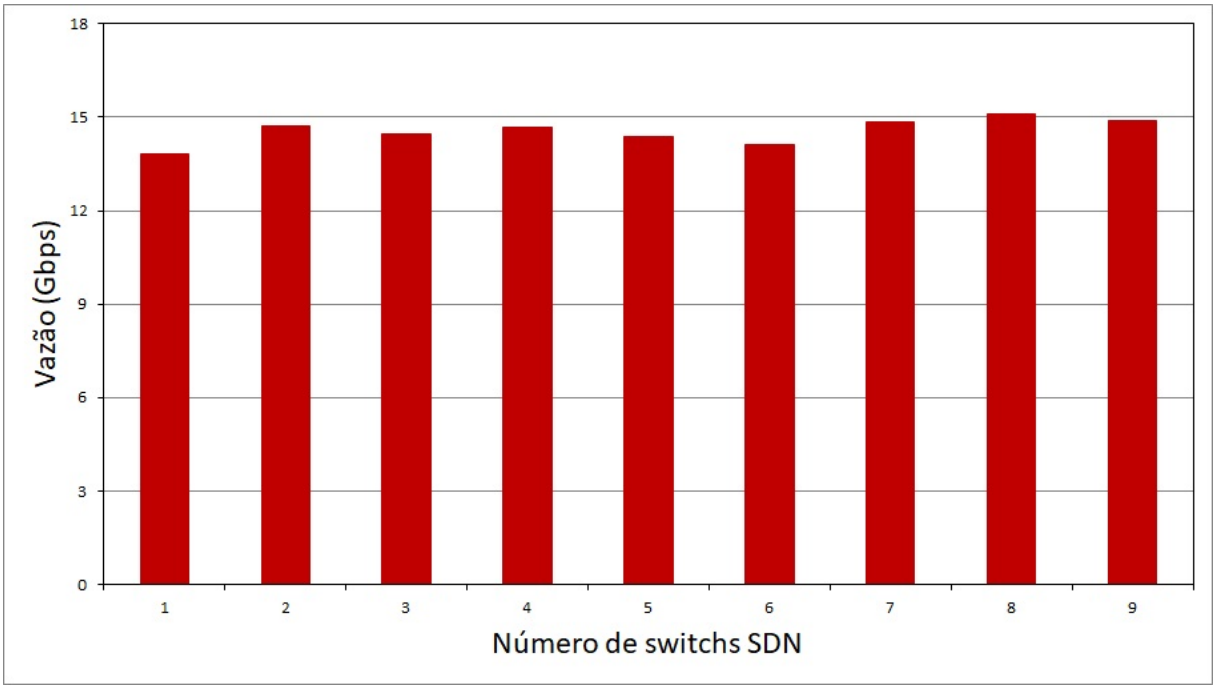
Figura 10 – Avaliação da vazão máxima atingida atraso quando dispositivos de encaminhamento são migrados utilizando a estratégia baseada no número de interconexões dos dispositivos.



5.2.3 Comprimento do caminho observada a partir das estratégias de migração.

Por fim, as Figuras 13, 14 e 15 ilustram o comprimento médio dos caminhos mínimos entre os pares de hosts da infraestrutura quando aplicada as diferentes estratégias de migração propostas. Esta avaliação suporta o experimento realizado quanto ao atraso,

Figura 11 – Avaliação da vazão máxima atingida atraso quando dispositivos de encaminhamento são migrados utilizando a estratégia baseada no peso do enlaces.



já que o motivo referente aos resultados da métrica de vazão foi a distância dos *switches* SDN selecionados em relação aos hosts e, como será visto a seguir, os resultados de comprimento do caminho demonstram essa explicação. Observa-se que o comprimento dos caminhos, independente da estratégia de migração adotada, decresce (ou pelo menos não se modifica) em função do aumento do número de dispositivos de encaminhamento SDN migrados na infraestrutura. As estratégias baseadas por grau e por peso apresentam resultados similares, enquanto a estratégia baseada por segurança demonstra resultados mais distantes. Realizando uma média geral entre os 9 resultados, apresentados nos gráficos, de cada estratégia, resultaram nos seguintes valores: (i) 8,891 hops com a estratégia baseada por grau; (ii) 8,894 hops com a estratégia baseada por peso e (iii) 10,222 hops com a estratégia baseado por segurança. A partir destes resultados podemos concluir que: (i) quanto mais dispositivos de encaminhamento são migrados, menor é a distância de um host até um dispositivos SDN qualquer – o que minimiza a média dos caminhos entre hosts da infraestrutura e (ii) a estratégia que obteve os melhores resultados foi a baseado por grau, mesmo está tendo valores similares a estratégia baseada por peso, enquanto a estratégia por segurança foi a estratégia que obteve os piores resultados desta métrica, variando entre 1 à 2 hops adicionais em comparação com as outras duas estratégias.

Figura 12 – Avaliação da vazão máxima atingida atraso quando dispositivos de encaminhamento são migrados utilizando a estratégia baseada em aspectos de segurança.

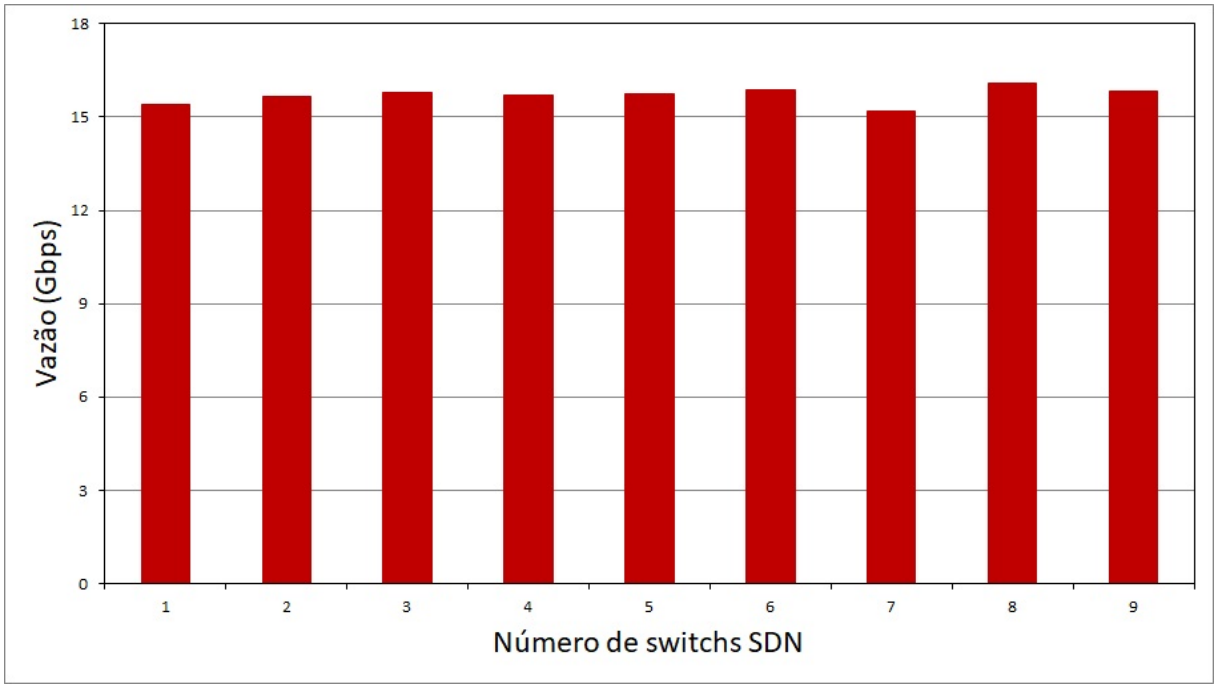


Figura 13 – Avaliação do comprimento médio dos caminho mínimos quando dispositivos de encaminhamento são migrados utilizando a estratégia baseada em aspectos de segurança.

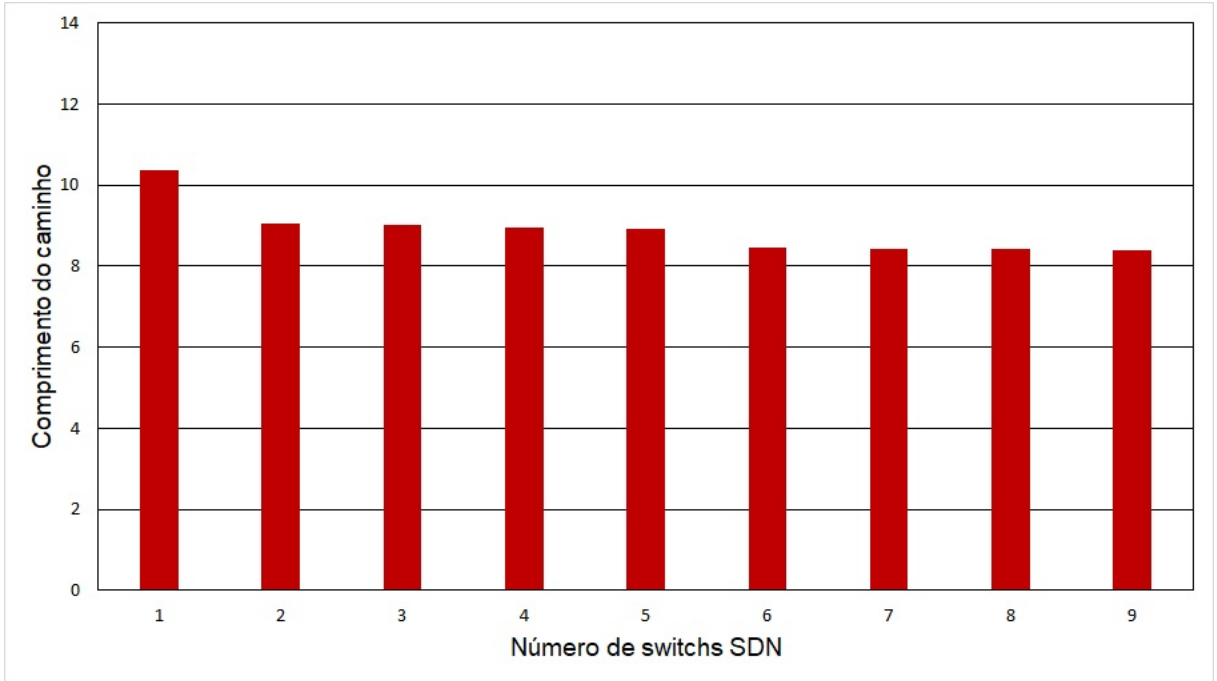


Figura 14 – Avaliação do comprimento médio dos caminho mínimos quando dispositivos de encaminhamento são migrados utilizando a estratégia baseada no peso do enlaces.

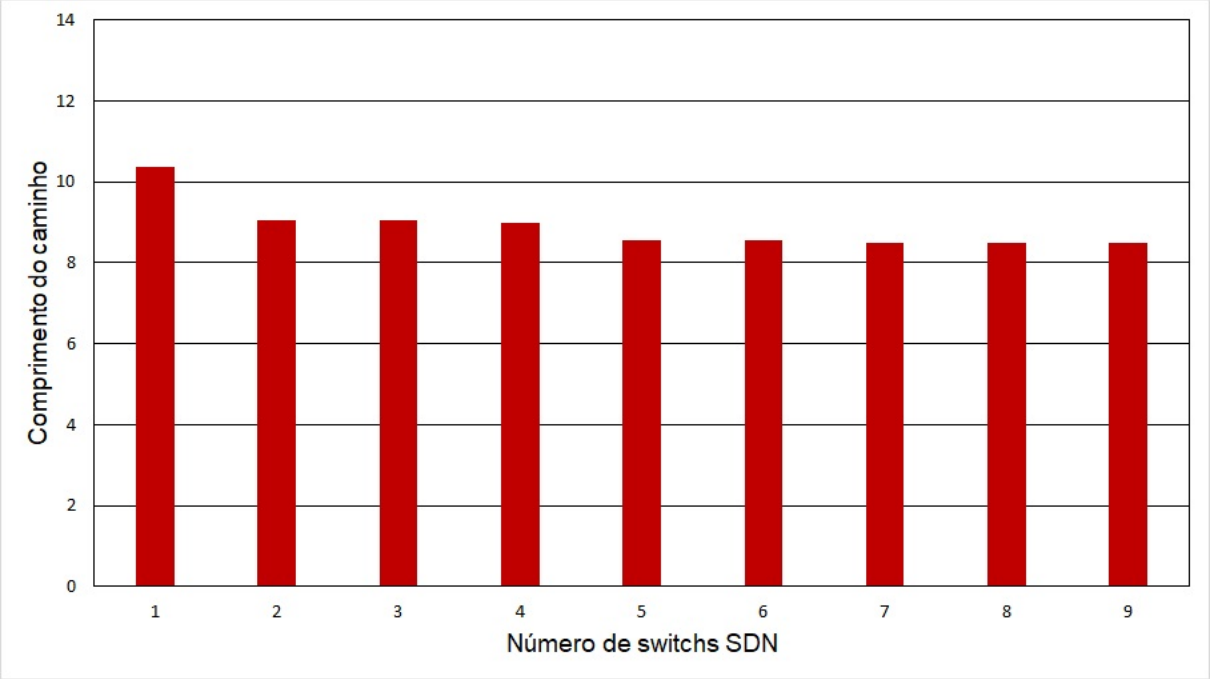
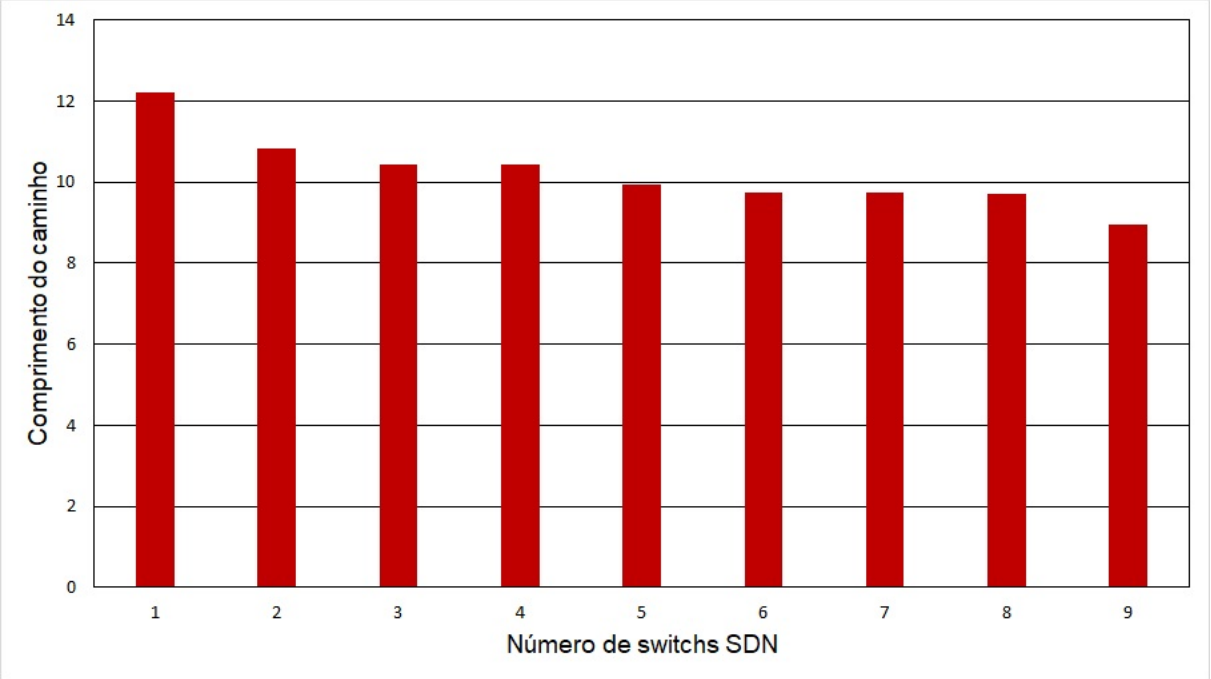


Figura 15 – Avaliação do comprimento médio dos caminho mínimos quando dispositivos de encaminhamento são migrados utilizando a estratégia baseada em aspecots de segurança.



6 CONSIDERAÇÕES FINAIS

Redes definidas por software receberam significativa atenção por parte da academia e da indústria nos últimos anos. Apesar de SDN ter atingido um significativo amadurecimento tecnológico, a sua implantação em redes corporativas e do campus é ainda pouco expressiva. O lento processo de adoção desta tecnologia pode ser explicado por causa *(i)* do custo da implementação, ou seja, substituição da infraestrutura existente, *(ii)* do planejamento e conhecimentos necessários para uma implantação gradativa, que requer a coexistência de tecnologias legadas e *(iii)* da falta de exemplos concretos de migrações gradativas bem-sucedidas, motivo que também ajuda na falta de confiança na tecnologia.

Neste trabalho, investigou-se estratégias para a migração de uma rede tradicional para uma rede SDN híbrida ou completa levando em conta a escolha de quais dispositivos devem ter maior relevância na troca. Para isso foram propostas, implementadas e avaliadas através de metodologia simulacional três estratégias diferentes. A primeira prioriza dispositivos que possuem mais conexões. A segunda leva em conta o peso dos enlaces. Finalmente, a terceira prioriza a segurança da rede, priorizando dispositivos que estão conectados às máquinas hosts. Para as estratégias propostas, avaliou-se o atraso fim-a-fim introduzido pela adoção da migração parcial, a vazão atingida e o comprimento dos caminhos.

Dentre as avaliações conduzidas, observou-se que o atraso fim-a-fim teve uma diferença significativa na inserção do primeiro dispositivo SDN em relação aos próximos. A estratégia que melhor se destacou nesta métrica foi a que levou em conta o grau do *switch* e a pior foi a estratégia baseada em aspectos de segurança. Na avaliação de desempenho que mediu a vazão máxima da infraestrutura, a estratégia proposta baseada em grau também se destacou melhor que as outras estratégias, mesmo tendo resultados similares à que era baseada na segurança da rede, sendo a estratégia baseada em peso dos enlaces a que demonstrou os piores resultados. Por fim, na avaliação do comprimento dos caminhos a estratégia baseada no grau dos *switches* também se saiu melhor com as outras (mesmo com a estratégia baseada pelo peso das conexões do *switch* representando resultados similares), sendo a estratégia baseada em segurança a que demonstrou os piores resultados. Vale destacar que a análise dos dados também demonstrou que conforme o número de dispositivos SDN são migrados, o comprimento do caminho é reduzido. Levando em conta essas informações, conclui-se que a estratégia baseada pelo número de conexões do *switch* resultaram na melhor estratégia entre as três a partir das métricas utilizadas. Como trabalho futuro, espera-se *(i)* estender a avaliação das estratégias propostas e *(ii)* implementar e avaliar as estratégias em um ambiente real.

REFERÊNCIAS

AMIN, R.; REISSLEIN, M.; SHAH, N. Hybrid sdn networks: A survey of existing approaches. **IEEE Communications Surveys Tutorials**, p. 1–1, 2018. Citado 3 vezes nas páginas 18, 26 e 27.

BURIOL, L. S. et al. A hybrid genetic algorithm for the weight setting problem in ospf/is-is routing. **Networks**, v. 46, n. 1, p. 36–56, 2005. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/net.20070>. Citado na página 22.

CAESAR, M. et al. Design and implementation of a routing control platform. In: **Proceedings of the 2Nd Conference on Symposium on Networked Systems Design & Implementation - Volume 2**. Berkeley, CA, USA: USENIX Association, 2005. (NSDI'05), p. 15–28. Disponível em: <http://dl.acm.org/citation.cfm?id=1251203.1251205>. Citado na página 22.

CARIA, M.; DAS, T.; JUKAN, A. Divide and conquer: Partitioning ospf networks with sdn. In: **2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)**. [S.l.: s.n.], 2015. p. 467–474. ISSN 1573-0077. Citado 3 vezes nas páginas 18, 27 e 28.

CASADO, M. et al. Fabric: A retrospective on evolving sdn. In: **Proceedings of the First Workshop on Hot Topics in Software Defined Networks**. New York, NY, USA: ACM, 2012. (HotSDN '12), p. 85–90. ISBN 978-1-4503-1477-0. Disponível em: <http://doi.acm.org/10.1145/2342441.2342459>. Citado 2 vezes nas páginas 25 e 26.

DORIA A., E. H. S. J. E. H. R. E. K. H. E. W. W. E. D. L. G. R.; HALPERN, J. **RFC 5810: Forwarding and Control Element Separation (ForCES) Protocol Specification**. 2010. Disponível em: <https://www.rfc-editor.org/info/rfc5810>. Citado na página 22.

FEAMSTER, N.; REXFORD, J.; ZEGURA, E. The road to sdn: An intellectual history of programmable networks. **SIGCOMM Comput. Commun. Rev.**, ACM, New York, NY, USA, v. 44, n. 2, p. 87–98, abr. 2014. ISSN 0146-4833. Citado 2 vezes nas páginas 17 e 21.

FOSTER, N. et al. Frenetic: A high-level language for openflow networks. In: **Proceedings of the Workshop on Programmable Routers for Extensible Services of Tomorrow**. New York, NY, USA: ACM, 2010. (PRESTO '10), p. 6:1–6:6. ISBN 978-1-4503-0467-2. Disponível em: <http://doi.acm.org/10.1145/1921151.1921160>. Citado na página 23.

KREUTZ, D. et al. Software-defined networking: A comprehensive survey. **Proceedings of the IEEE**, v. 103, n. 1, p. 14–76, Jan 2015. ISSN 0018-9219. Citado 3 vezes nas páginas 17, 18 e 23.

LEVIN, D. et al. Panopticon: Reaping the benefits of incremental SDN deployment in enterprise networks. In: **2014 USENIX Annual Technical Conference (USENIX ATC 14)**. Philadelphia, PA: USENIX Association, 2014. p. 333–345. ISBN 978-1-931971-10-2. Disponível em: <https://www.usenix.org/conference/atc14/technical-sessions/presentation/levin>. Citado 2 vezes nas páginas 18 e 27.

LONG H., Y. M. M. G. D. A.; SHAH, H. **RFC 8330: OSPF Traffic Engineering (OSPF-TE) Link Availability Extension for Links with Variable Discrete Bandwidth**. 2018. Disponível em: <https://www.rfc-editor.org/info/rfc8330>. Citado na página 22.

MCKEOWN, N. et al. Openflow: Enabling innovation in campus networks. **SIGCOMM Comput. Commun. Rev.**, ACM, New York, NY, USA, v. 38, n. 2, p. 69–74, mar. 2008. ISSN 0146-4833. Disponível em: <http://doi.acm.org/10.1145/1355734.1355746>. Citado 3 vezes nas páginas 17, 22 e 24.

MCKEOWN, N. et al. Openflow: Enabling innovation in campus networks. **SIGCOMM Comput. Commun. Rev.**, ACM, New York, NY, USA, v. 38, n. 2, p. 69–74, mar. 2008. ISSN 0146-4833. Disponível em: <http://doi.acm.org/10.1145/1355734.1355746>. Citado na página 26.

REICH C. MONSANTO, N. F. J. R. J.; WALKER, D. Modular sdn programming with pyretic. In: . [S.l.]: USENIX Association, 2013. v. 38. Citado na página 23.

TENNENHOUSE, D. L. et al. A survey of active network research. **IEEE Communications Magazine**, v. 35, n. 1, p. 80–86, Jan 1997. ISSN 0163-6804. Citado 2 vezes nas páginas 21 e 22.

TROIS, C. et al. A survey on sdn programming languages: Toward a taxonomy. **IEEE Communications Surveys Tutorials**, v. 18, n. 4, p. 2687–2712, Fourthquarter 2016. ISSN 1553-877X. Citado na página 23.

UBAID FAISAL BIN UBAID, R. A. F.; IQBAL, M. M. Mitigating address spoofing attacks in hybrid sdn. In: **2018 USENIX Annual Technical Conference (USENIX ATC 14)**. Philadelphia, PA: USENIX Association, 2018. p. 333–345. ISBN 978-1-931971-10-2. Disponível em: <https://www.usenix.org/conference/atc14/technical-sessions/presentation/levin>. Citado na página 29.

USMAN ARIS CAHYADI RISDIANTO, J. K. M. Resource monitoring and visualization for of@tein sdn-enabled multi-site cloud. In: **2016 USENIX Annual Technical Conference (USENIX ATC 14)**. Philadelphia, PA: USENIX Association, 2016. p. 333–345. ISBN 978-1-931971-10-2. Disponível em: <https://www.usenix.org/conference/atc14/technical-sessions/presentation/levin>. Citado 2 vezes nas páginas 28 e 29.

ÍNDICE