CURSO DE CIÊNCIA DA COMPUTAÇÃO

Vinícius Martins de Souza

UM ESTUDO EXPERIMENTAL DO PLANO DE CONTROLE EM REDES DEFINIDAS POR SOFTWARE

Santa Cruz do Sul

2017

Vinícius Martins de Souza

UM ESTUDO EXPERIMENTAL DO PLANO DE CONTROLE EM REDES DEFINIDAS POR SOFTWARE

Trabalho de Conclusão apresentado ao Curso de Ciência da Computação da Universidade de Santa Cruz do Sul, como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação.

Orientador: Prof. Me Lucas Fernando Müller

Santa Cruz do Sul
2017

“Anyone who has never made a mistake

has never tried anything new.”

— Albert Einstein

RESUMO

As redes de computadores fazem parte da vida cotidiana das pessoas, tornando-se estruturas cada vez mais amplas e complexas. Entretanto, este crescimento também agrega problemas, como uma rede pouco adaptável a mudanças. Devido a isso, o paradigma de Redes Definidas por Software (Software Defined Networking - SDN) surge para resolver as atuais dificuldades encontradas, ele prega a separação da rede em três diferentes planos, o plano de dados, o plano de controle e o plano de aplicação, cada um com suas tarefas distintas. Esta separação de planos, traz para redes SDN flexibilidade para gerenciamento da rede, dispondo de uma interface programável que possibilita a programação de comportamentos e serviços para rede através de um controlador de rede. Apesar disto, a comunidade de pesquisadores em redes levanta diversas questões sobre como se deve organizar a distribuição do plano de controle para melhor atender as necessidades da rede. Baseado sob esta problemática, o presente trabalho, teve como objetivo auxiliar na evolução do cenário atual das redes SDN. Como contribuições deste trabalho pode-se citar (i) a revisão em abrangência e profundidade do estado-da-arte no que se refere as diferentes maneiras de organizar uma rede SDN; (ii) o estudo e experimentação prática de um ambiente de testes (testbed) para emulação de diferentes cenários relacionados a organização do plano de controle das redes SDN através de um conjunto de componentes bastante consolidados na indústria e academia, e (iii) a análise prática sob o ambiente desenvolvido de diferentes cenários de organização dessas redes, visando a resposta de duas perguntas bem definidas, a primeira tratando da responsividade da rede e a segunda de interações de carga intensa que afetem o plano de controle das redes SDN.

Palavras-chave: Redes definidas por Software, Plano de Controle, Interface Programável.

ABSTRACT

Computer networks are a part of people's everyday life, becoming more large and complex each time. However, this growth also adds problems, as a network unadaptable to changes. Due to this, the Software Defined Networking (SDN) paradigm appears to solve the current found difficulties, it preaches the separation of the network in three different schemes, the data scheme, the control scheme and the application scheme, each one with its distinct tasks. This scheme separation, brings flexibility to SDN to manage the network, having a programmable interface that allows the programation of behaviours and services for the network in a controller. Despite this, the network research community, brings up various questions on how the distribution of control plans should be organized to better attend the necessities of the network. Based on this problem, the objective of the present work was to help in the evolution of the current scenario of SDN networks. The main contributions of this work can be stated as: (i) a comprehensive review of the state-of-the-art referring to the different ways to plan an SDN network; (ii) the study and practical experimentation of a testbed environment to emulate different scenarios related to distinct control plane organizations, all that by using a set of well-established components in industry and academia, and (iii) the execution of an practical analysis using the environment developed to emulate a set of different network organization scenarios aiming to answer to two well-defined questions, the first dealing with network responsiveness, while the second seeks to understand how the intense communication interactions can that affect the control plan of SDN networks.

Keywords: software defined networks, Control Plane, Programmable Interface.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Tal foi o crescimento na abrangência e diversificação das redes de computadores que elas se tornaram estruturas complexas e difíceis de gerenciar. No paradigma atual, a configuração de políticas de alto nível – as quais definem o comportamento da rede – precisa considerar cada dispositivo de encaminhamento da rede (por exemplo, roteadores e comutadores). Além disso, tais configurações devem fazer uso de interfaces proprietárias de cada fabricante e por vezes, são realizadas de forma manual. Essa situação restringe a eficiência no uso de recursos, dificulta a capacidade inovação e reduz a flexibilidade e a capacidade da reação perante situações inesperadas e/ou indesejadas (incluindo falhas, ataques e variações de carga) (BENSON; AKELLA; MALTZ, 2009).

Diante desse contexto o paradigma de Redes Definidas por Software (Software Defined Networking – SDN) trouxe vários benefícios à gerencia e operação de redes, facilitando a inovação e simplificando as atividades de controle (FEAMSTER; REXFORD; ZEGURA, 2014). Redes Definidas por Software é um novo paradigma de redes que propõe a separação do plano de controle do plano de dados. Dentre os objetivos deste novo paradigma está tornar os elementos de encaminhamento (switches e roteadores) mais simples, enquanto o processamento da lógica de encaminhamento será feita por um novo elemento introduzido na rede, o controlador (KREUTZ et al., 2014).

Neste novo paradigma, a lógica de controle não é mais embarcada no hardware do dispositivo e passa a ser implementada através de uma interface programável disponibilizada no controlador logicamente centralizado na rede (ISOLANI et al., 2014). Nesse sentido o protocolo Openflow (ONF, 2014) vem sendo adotado como padrão de fato, fornecendo as abstrações necessárias para programação dos dispositivos de encaminhamento de rede. O controlador (remoto) da rede, nesse caso, atua como uma entidade logicamente centralizada, que possui visão global da infraestrutura e gerencia uma coleção distribuída e programável de dispositivos de encaminhamento de pacotes (NUNES et al., 2014).

Um desafio fundamental para adoção de SDN em redes de grande escala é o problema de implantação (VISSICCHIO; VANBEVER; BONAVENTURE, 2014). SDN vem com seu próprio conjunto de desafios e limitações variando desde dificuldades (propósitos, custos e técnicos) na implantação até a busca por garantias relacionadas à lógica centralizada, por exemplo, em termos de sobrevivência, robustez e escalabilidade. Esses fatores acabam por gerar um conjunto de questões acerca de diferentes estratégias possíveis para se organizar a infraestrutura

de rede sob o paradigma SDN. Há diferentes abordagens, como aquelas que tratam o plano de controle centralizado, com um único controlador ligado a diversos elementos de encaminhamento, ou o plano de controle fisicamente distribuído, onde diversos controladores distribuídos geograficamente gerenciam conjuntos distintos de dispositivos de encaminhamento (TOOTOONCHIAN; GANJALI, 2010), (LEVIN et al., 2012).

Buscando colaborar com o paradigma SDN, esse trabalho contribuiu em três eixos principais: (i) expansão do estudo relacionado ao levantamento bibliográfico, resultando na organização e caracterização das principais estratégias adotadas para a organização do Plano de Controle em redes SDN; (ii) estudos avançados para emular um sub-conjunto das estratégias de organização do Plano de Controle e (iii) desenvolvimento de códigos necessários para viabilizar a execução e avaliação de estratégias, utilizando para isso o emulador de redes Mininet (LANTZ; HELLER; MCKEOWN, 2010), além do controlador distribuído ONOS (ONOS, 2016).

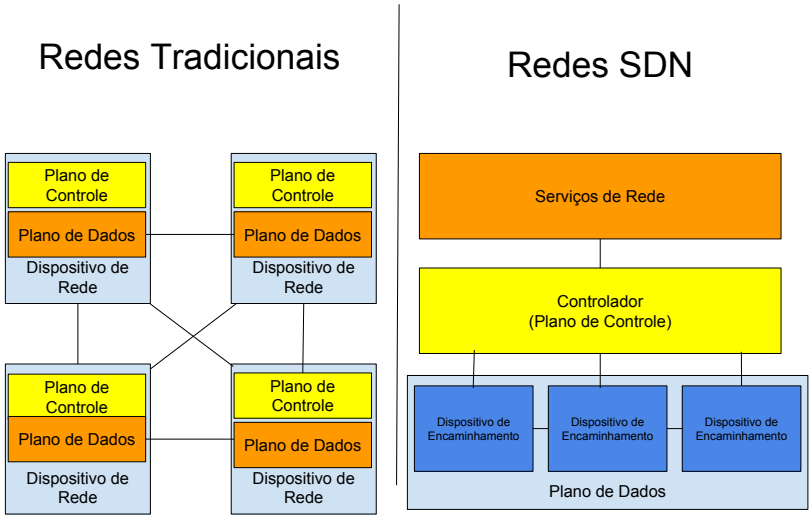
A seguir, no Capítulo 2, serão apresentados os fundamentos sobre SDN, descrevendo os conceitos sobre seu paradigma. No Capítulo 3 é apresentado o estado da arte em relação as formas de organização do plano de controle de uma rede SDN, os compromissos em sua implantação e alguns casos de implantação de sucesso. O Capítulo 4 apresenta a metodologia de avaliação do estudo dos efeitos da distribuição do plano de controle, objetivo desse trabalho. No Capítulo 5 serão expostos os resultados obtidos. Ao final, no Capítulo 6, são apresentadas as conclusões obtidas na realização desse trabalho.

2 REDES DEFINIDAS POR SOFTWARE

Atualmente as redes tradicionais operam com equipamentos de encaminhamento que possuem o plano de controle e o plano de dados embarcado no próprio hardware, o que torna a rede menos adaptável a mudanças, ocasionando no que muitos chamam de uma "ossificação das redes". Tal expressão foi cunhada já que, neste cenário, é necessário que cada equipamento seja configurado individualmente, e em se tratando de redes em larga escala, este processo se torna inviável (KREUTZ et al., 2014).

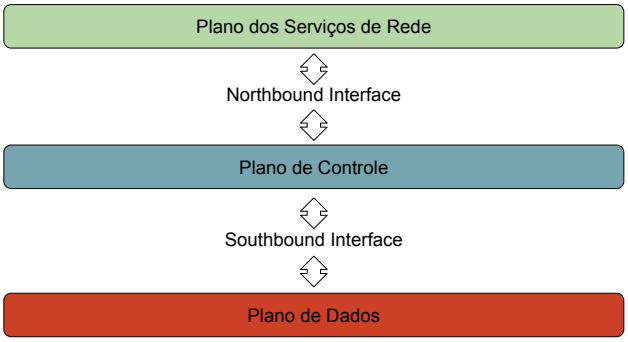
As Redes Definidas por Software são redes baseadas em um novo paradigma que visa a separação do plano de controle e do plano de dados nos dispositivos de encaminhamento, com a finalidade de viabilizar uma rede mais flexível a mudanças e de fácil gerenciamento (NUNES et al., 2014). Este novo paradigma surge como uma das principais soluções para suprir dificuldades encontradas com gerenciamento e a inovação das infraestruturas de redes de computadores de todos os níveis. A partir desta separação, se torna possível controlar toda a lógica da rede a partir de uma interface programável logicamente centralizada através de um novo elemento introduzido na topologia, chamado de controlador (KREUTZ et al., 2014). Com isso, se tem a separação da atual estrutura que é encontrada na Internet, retirando a lógica de roteamento de cada um dos equipamentos e passando para o controlador, conforme ilustrado na Figura 1. Deste modo, modularizamos a rede, tornando esta mais adaptável a mudanças e com maior flexibilidade no gerenciamento.

Figura 1 – Redes Tradicionais x SDN
Fonte: do autor



Desta forma, a modularização da rede será realizada em 3 partes, que são: o plano de dados responsável pelo encaminhamento dos pacotes para os determinados destinos, o plano de controle com a função de determinar a lógica de encaminhamento e os serviços de rede que se comunicam e interagem com todo conjunto da rede (ROWSHANRAD et al., 2014). Entretanto, para que seja possível realizar a comunicação entre os planos de dados, controle e serviços, se faz necessário o uso de duas interfaces que vão servir como intermediadoras. Estas são chamadas de interface northbound e interface southbound. Cada uma delas se posiciona especificamente entre os planos, realizando a função de interligá-los e proporcionar a comunicação dos mesmos, como exemplificado na Figura 2 (XIA et al., 2015).

Figura 2 – Arquitetura Padrão do Paradigma
Fonte: adaptado de (KREUTZ et al., 2014)



Neste Capítulo serão tratados os conceitos principais de cada parte desta arquitetura, dando mais detalhes sobre seu comportamento.

2.1 Plano de Controle

Atualmente os sistemas operacionais, no contexto de dispositivos pessoais, oferecem uma série de abstrações, realizando tarefas de baixo nível para que os usuários possam trabalhar em ambiente de alto nível. Porém, as redes de computadores vêm há muito tempo sendo configuradas e gerenciadas utilizando um baixo nível de abstração, tornando isso uma tarefa complexa (KREUTZ et al., 2014).

A arquitetura SDN vem com o intuito de sanar estes problemas, prevendo uma mudança no modo com que a lógica de roteamento é realizada, deixando de ser embarcada no dispositivo de encaminhamento e passando a ser controlada por um controlador logicamente centralizado.

Com esta separação, se estabelece o plano de controle, que será o responsável por processar cada uma das requisições e respondê-las aos dispositivos de encaminhamento conforme as regras estabelecidas (BENSON; AKELLA; MALTZ, 2009).

Um plano de controle é basicamente formado por duas partes: sistema operacional da rede e os serviços de rede. O sistema operacional da rede é responsável por gerenciar o controlador e oferecer abstrações de serviços básicos, facilitando o gerenciamento e o desenvolvimento de novos serviços, enquanto os serviços de rede tratam do gerenciamento e controle, para isto cada controlador detêm a visão global da rede e seu estado atual, com isso, é possível realizar tanto o gerenciamento quanto a implementação de novos serviços. Contudo é importante ressaltar, que esta visão que os controladores obtém, se trata de uma visualização lógica, possibilitando a existência cooperativa de vários controladores distribuídos. Num cenário que conta com múltiplas instâncias de controladores estes irão se comunicar para assim estabelecer uma visão global de rede (NUNES et al., 2014).

2.2 Plano de Dados

O plano de dados corresponde aos dispositivos de encaminhamento, que deixam de processar a lógica implementada em hardware, se comunicando com o controlador através de uma interface southbound para realizar o devido encaminhamento do fluxo de rede (VISSICCHIO; VANBEVER; BONAVENTURE, 2014).

2.3 Interface Southbound

Em Redes Definidas por Software, a interface southbound realiza a comunicação dos dispositivos de encaminhamento de forma que, através dela o controlador possa receber informações e gerenciar cada um dos dispositivos. Embora existam muitas opções de interfaces southbound, o protocolo OpenFlow (ONF, 2014) é definido como o padrão de fato (ROWSHANRAD et al., 2014).

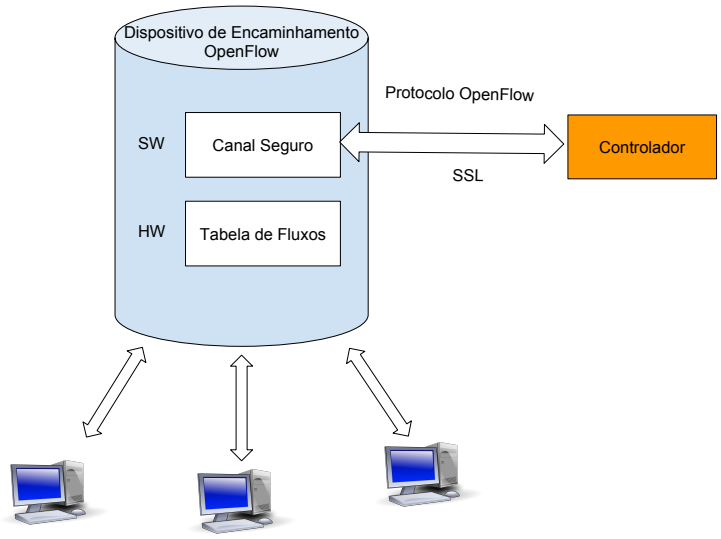
2.4 OpenFlow

O OpenFlow é um protocolo aberto para redes SDN que oferece uma interface programável possibilitando o desenvolvedor/gerente da rede controlar cada dispositivo de encaminhamento diretamente. Ele habilita a interação com o plano de dados através de instruções que o controlador irá encaminhar, manipulando como serão tratadas as mensagens recebidas em cada

dispositivo, de acordo com as regras presentes na tabela de fluxos (ONF, 2014).

O padrão especificado pelo protocolo OpenFlow compreende a interação de diferentes partes, conforme pode ser visualizado na Figura 3.

Figura 3 – Dispositivo de Encaminhamento OpenFlow
Fonte: adaptado de (ONF, 2014)



- Tabela de Fluxos: é uma tabela na qual cada entrada de fluxo será composta por determinadas regras, ações e informações de estatística. Com base nesta tabela os dispositivos terão as informações necessárias para encaminhar os pacotes.
- Protocolo OpenFlow: é o protocolo que estabelece a comunicação entre o plano de dados e o plano de controle, ligando cada dispositivo de encaminhamento com o controlador por um canal de comunicação seguro.
- Controlador: o controlador é o responsável por adicionar ou remover regras na tabela de fluxos dos dispositivos de rede, respeitando possíveis políticas nele implementadas.
- Canal Seguro: tem a função de garantir que se estabeleça um canal seguro de comunicação (via protocolo Secure Socket Layer (SSL), por exemplo) entre cada um dos elementos das redes SDN, visando garantir que a rede não receba ataques mal-intencionados.

Portanto, o OpenFlow ira comunicar os dispositivos de encaminhamento e o plano de controle, estabelecendo uma comunicação segura e estável entre eles, fornecendo assim os recursos necessários para que se possa implementar a modularização da rede como prevê o paradigma SDN (COSTA, 2013).

2.5 Interface Northbound

A interface northbound é a parte responsável por comunicar os serviços de redes SDN com o controlador. Esta interface oferece abstrações necessárias para que se torne mais simples a implementação de novos serviços de rede em um controlador. Em uma rede SDN é de suma importância que os controladores se comuniquem entre si, para que seja possível manter em cada um deles a visão global da rede e para que sob a apresentação de falhas na rede, seja possível que os controladores reajam para contornar estas falhas tomando decisões sob os dispositivos de encaminhamento, além de manter sincronizados os serviços de rede que rodam em várias instâncias (ROWSHANRAD et al., 2014).

Importante lembrar, que esta interface, assim como a southbound, é imprescindível para a modularidade de uma rede SDN. Enquanto a southbound irá abstrair a parte de hardware, a interface northbound realizará a abstração da parte de software, para oferecer um ambiente de alto nível propício para o desenvolvimento de novos serviços (KREUTZ et al., 2014).

3 ESTADO DA ARTE DO PROJETO DO PLANO DE CONTROLE EM SDN

Neste Capítulo são apresentados os principais conceitos sobre a organização do plano de controle em redes SDN, as suas vantagens e desvantagens. Além disso,a Tabela 1 apresenta de forma consolidada a discussão realizada ao longo do Capítulo, fazendo um paralelo das diferentes formas de se projetar o plano de controle, com suas vantagens e desvantagens, e trabalhos relacionados cada grupo.

3.1 Organização do Plano de Controle

O plano de controle no âmbito de redes SDN, tem o intuito de oferecer a abstração necessária aos administradores, para que seja possível concentrar sobre as atividades de gerência e administração da rede. Além disso, o plano de controle oferece uma visão logicamente centralizada da rede, possibilitando que novos serviços sejam implantados mais facilmente e, que a rede consiga se adaptar melhor a mudanças. Contudo, para que seja possível ofertar estas funcionalidades, o plano de controle conta com um sistema operacional, o qual irá desempenhar o papel de intermediador nos dispositivos de controle, tornando possível a realização destas tarefas (GUDE et al., 2008).

Para viabilizar o que fora exposto, o sistema operacional no plano de controle, deve levar em conta questões importantes. Segundo (KOPONEN et al., 2010) os principais pontos que esta plataforma deve abordar são:

- Generalidade: a plataforma de controle deve permitir o maior alcance possível para serviços dos mais variados contextos.
- Escalabilidade: com o grande crescimento das redes de computadores, a plataforma deve ser capaz de permitir e gerenciar efetivamente os dispositivos conforme o crescimento da topologia.
- Simplicidade: a tarefa de gerenciamento e desenvolvimento de serviços de rede deve ser simplificada o máximo possível através da plataforma de controle.
- Desempenho do Plano de Controle: a plataforma de controle deve garantir o melhor desempenho possível para o plano de controle, sem interferir nos serviços de rede e nos demais itens abordados acima, como por exemplo, a generalidade.

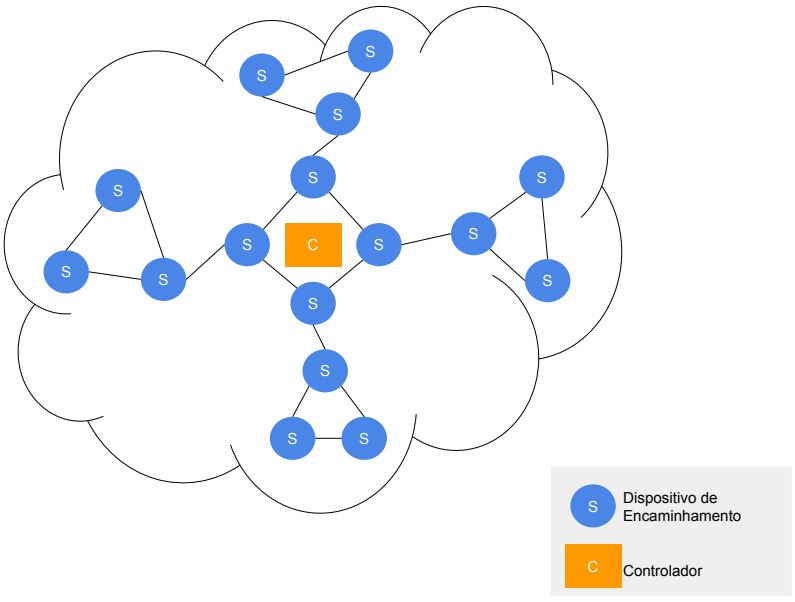
Nesta direção, são identificadas questões importantes relacionadas aos compromissos assumidos nas diferentes formas de organização do plano de controle em redes SDN. Esta or-

ganização, refere-se ao modo com que os dispositivos do plano de controle serão distribuídos. Sendo assim, nas sessões abaixo são discutidos pontos sobre a organização do plano de controle centralizado, fisicamente centralizado com cluster de controladores, distribuído hierárquico e totalmente distribuído, verificando suas diferenças e como se comporta a estrutura de controle.

3.1.1 Plano de Controle Clássico Centralizado

A organização do plano de controle clássico centralizado consiste em uma topologia de rede, na qual o controlador é posicionado fisicamente em um ponto central e estratégico da infraestrutura da rede. Enquanto todos os dispositivos de encaminhamento serão distribuídos ao redor do mesmo e, mantidos sob controle diretamente pelo controlador central, como pode ser observado na Figura 4. Neste tipo de organização, um único controlador irá responder para toda rede. Porém, não é preciso muito para perceber que em redes de grande escala como em redes WAN, por exemplo, conforme o número de dispositios de encaminhamento for aumentando, o número de requisições ao nosso controlador vai crescer da mesma forma e, ocasionalmente teremos problemas envolvendo escalabilidade (TOOTOONCHIAN et al., 2012).

Figura 4 – Plano de Controle Centralizado
Fonte: do autor

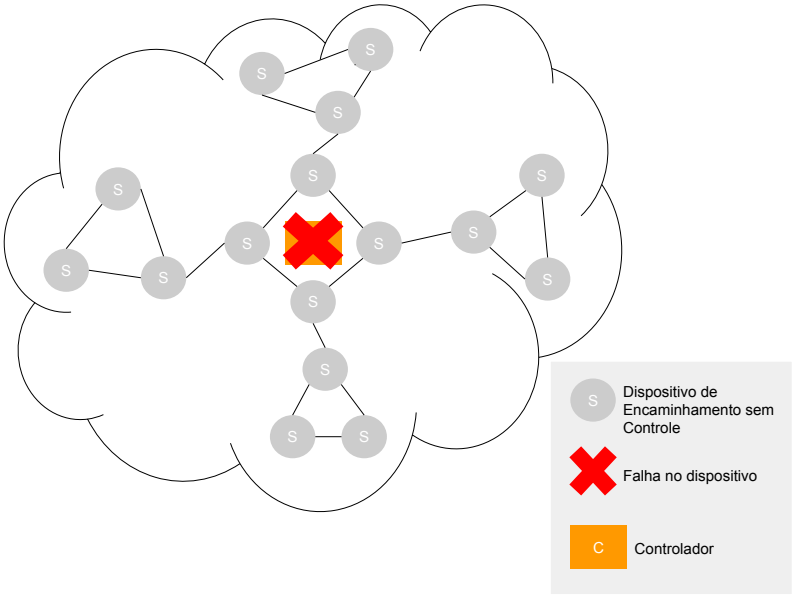


Além disso, determinadas plataformas de controle em seu estado atual, não proporcionam paralelismo, ou seja, não são capazes de garantir um desempenho adequado conforme acontece a expansão da infraestrutura em termos de equipamentos de encaminhamento. Contudo, ao longo do tempo foram sendo propostas novas soluções, como por exemplo o sistema Maestro (CAI; COX; NG, 2010) que oferece um sistema para controle da rede de modo escalável,

utilizando o protocolo OpenFlow.

Outro ponto importante é a tolerância a falhas em redes com o plano de controle centralizado, pois o controlador se torna um único ponto de falha crítica. Diversos fatores como ataques, problemas estruturais, falha de energia, podem contribuir para o surgimento de uma falha, fazendo com que se perca o controle na rede, como mostrado na Figura 5 (LEVIN et al., 2012).

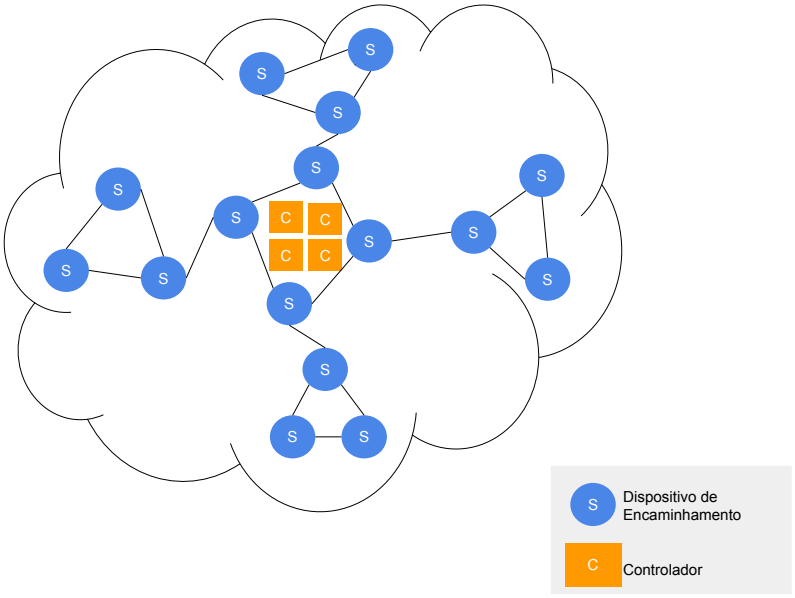
Figura 5 – Falha no Controlador Central
Fonte: do autor



Uma das formas que se encontra para contornar este problema é a implantação de uma organização centralizada com um cluster de controladores. Neste tipo de organização, são agrupados controladores na forma de um cluster, para que todos atuem juntos como uma única entidade central, como mostrado na Figura 6.

Atualmente, algumas soluções como o controlador Opendaylight (OPENDAYLIGHT, 2016) e Onix(KOPONEN et al., 2010) permitem a realização de clusters com controladores, em alguns casos, como em partes da rede no backbone da Google (JAIN et al., 2013), já se pode observar a inserção de clusters com Onix.

Figura 6 – Plano de Controle Centralizado com Cluster
Fonte: do autor



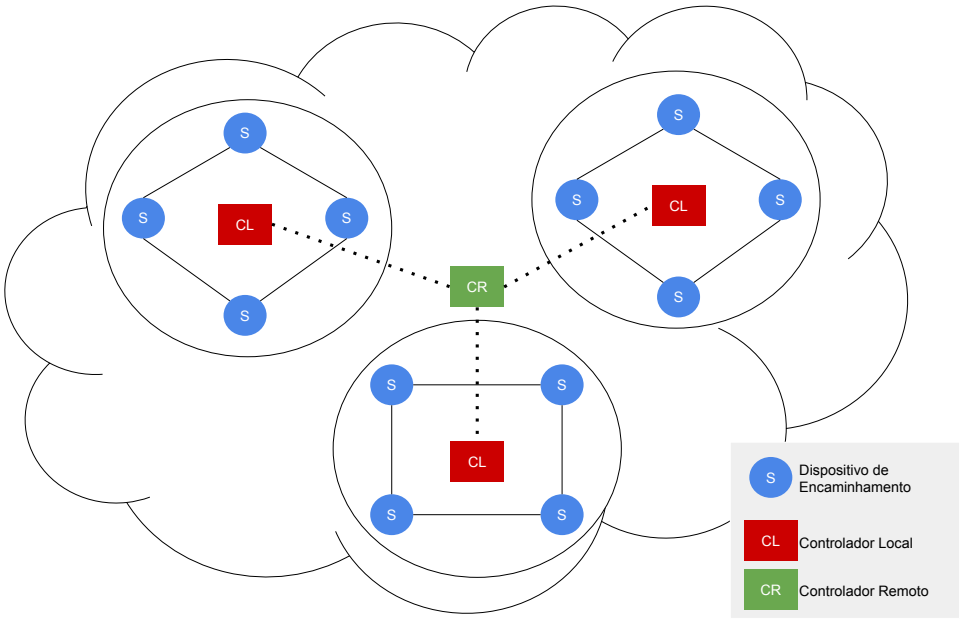
Contudo, este tipo de organização não apresenta somente desvantagens. Conforme centralizamos o plano de controle, se torna mais fácil a implantação de serviços na rede, pois, como irá haver um controle centralizado, não será necessário preocupações referentes a questões de sincronização entre controladores.

3.1.2 Plano de Controle Distribuído Hierárquico

A organização do plano de controle em modo hierárquico, se trata de uma topologia na qual o plano de controle irá respeitar uma hierarquia de controladores, trabalhando com dois níveis fundamentalmente: controladores locais e os remotos, conforme pode ser visualizado na Figura 7. Os controladores remotos, serão responsáveis por manter a consistência global entre todas as instâncias de controle, além de definir e enviar as regras de encaminhamento que devem ser instaladas nos dispositivos para os controladores locais. Os controladores locais, por sua vez, irão configurar diretamente os dispositivos de encaminhamento e compartilhar com o controlador remoto o seu estado da rede (YEGANEH; GANJALI, 2012).

Este tipo de organização tem o benefício de tornar simples a implantação de novos serviços para rede, que podem ser configurados diretamente no controlador remoto e depois distribuídos aos demais controladores. Entretanto, este fato também pode causar problemas, pois acaba tornando necessário que cada tipo de controlador seja configurado corretamente de acordo com o seu nível (lembrando que podem haver mais níveis na hierarquia, dois é o mínimo). Além disso, outro problema que surge, é que caso a infraestrutura da rede conte com somente um con-

Figura 7 – Plano de Controle Hierárquico
Fonte: do autor



trolador remoto, será possível que ainda haja na rede um único ponto central de falha (CURTIS et al., 2011).

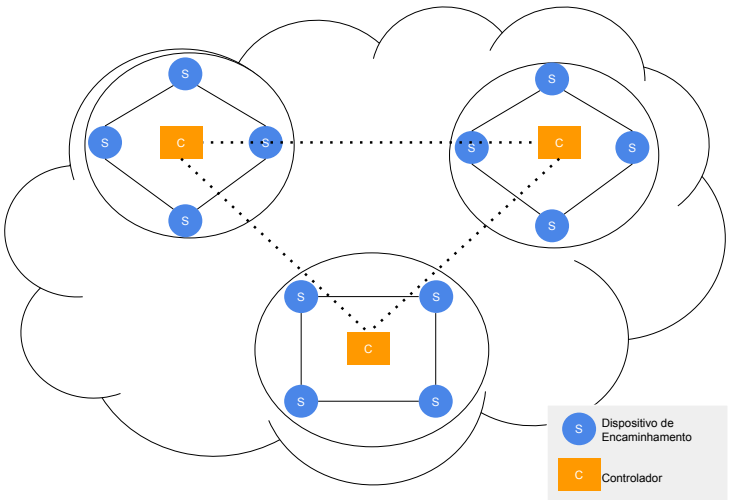
Contudo, este tipo de cenário é recomendado para redes que não irão necessitar de um desempenho tão alto, pois, como as requisições vão ser processadas por dois controladores, dependendo do número de dispositivos de encaminhamento (ou controladores locais no caso de um controlador remoto) que cada controlador atender, a latência da rede pode aumentar, prejudicando seu desempenho (YEGANEH; GANJALI, 2012).

3.1.3 Plano de Controle Totalmente Distribuído

Neste tipo de organização do plano de controle em redes SDN, a topologia será implementada de forma que cada um dos controladores estará mantendo uma comunicação contínua com os outros dispositivos do plano de controle para manter a visão global de rede, e cada um dos controladores, terá seu próprio conjunto de dispositivos de encaminhamento, como demonstra a Figura 8.

O plano de controle totalmente distribuído é composto por instâncias de controladores com papéis e capacidades bastante semelhantes. A coordenação entre todas as instâncias é essencial para que eles em conjunto consigam configurar os dispositivos de encaminhamento de modo adequado, garantindo as políticas da rede, ao mesmo tempo em que garantem um bom desempenho no funcionamento global dessa infraestrutura.

Figura 8 – Plano de Controle Distribuido
Fonte: do autor



Trabalhos como Koponen et al. (2010), Tootoonchian e Ganjali (2010) introduzem os conceitos de como um plano de controle distribuído deve ser executado. Ambos argumentam que um plano de controle simples, contando com controladores centralizados podem sofrer com grandes atrasos nas respostas pelo controlador ao passo em que acontece o crescimento da infraestrutura em quantidade de dispositivos de encaminhamento – implicando numa sobrecarga do controlador – e no diâmetro dessa rede (vez que as mensagens de controle precisam percorrer longos caminhos para manter a conectividade com o controlador e seus dispositivos de encaminhamento). Uma preocupação comum sobre tal distribuição diz respeito a encontrar o melhor compromisso de um esquema de distribuição agnóstico para as aplicações ou serviços de rede (isto é, que se mantenha simples a implementação de novos serviços numa infraestrutura mais robusta) e o bom desempenho nas operações de controle (isto é, reações rápidas a ocorrência de eventos na infraestrutura da rede).

Uma rede distribuída pode oferecer diversos benefícios quanto à escalabilidade, pois sua capacidade de crescimento é maior que das outras organizações possíveis discutidas anteriormente (KOPONEN et al., 2010). Além disso, o controle de falhas em redes distribuídas torna-se mais robusto, pois no contexto de que existem mais controladores na rede, no momento da falha de algum deles, os outros devem garantir a sobrevivência da rede (MüLLER et al., 2014).

Contudo, apesar de o plano de controle distribuído oferecer uma melhor solução quanto a sua escalabilidade e tratamento a falhas, no momento em que se implementa uma infraestrutura distribuída, questões como: qual o número de controladores a rede necessita? Qual o número de dispositivos de encaminhamento cada controlador irá atender? E de qual forma eles devem

ser distribuídos? Como controlar as atualizações na rede?, são algumas das quais surgem no momento em que administradores planejam suas infraestruturas SDN distribuídas. Estes fatores acabam por tornar a implantação mais complexa, tanto para o desenvolvimento de aplicações quanto para o gerenciamento de fluxos da rede.

3.2 Compromissos no Projeto do Plano de Controle SDN

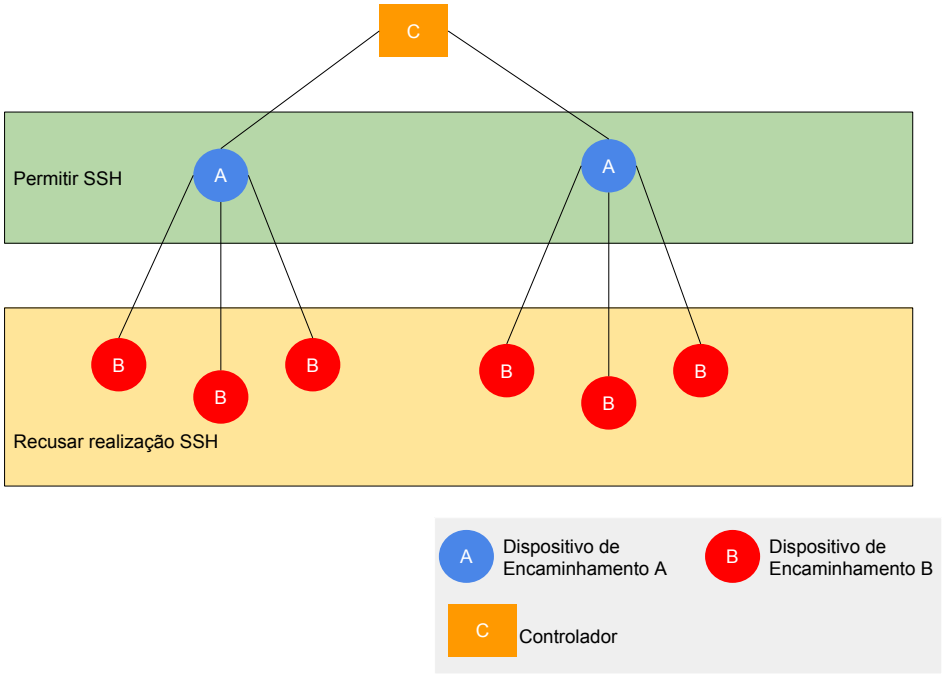
A literatura de SDN inclui discussões sobre diferentes compromissos assumidos no projeto de um plano de controle. A separação do plano de controle e dados é frequentemente apontada como um benefício, posto que se recorre ao uso de abstrações para possibilitar desse modo a evolução independente de cada um dos planos. Entretanto, também acaba por apresentar um desafio, devido a dependência herdada entre os dispositivos de encaminhamento associados com cada controlador. Os trabalhos apresentados abaixo focam em aspectos particulares desse fato e em outras opções do espaço de projeto do plano de controle, de modo a demonstrar quais são as melhores escolhas diante de cada projeto de uma rede SDN, de acordo com seus pré-requisitos.

O trabalho realizado por Levin et al. (2012) aborda questões de consistência do estado da rede no controlador, discutindo sobre as duas opções disponíveis. Uma destas opções é chamada de eventualmente consistente, ela integra as informações a medida que estas tornam-se disponíveis, e reconciliam as atualizações conforme cada domínio de controladores aprende sobre elas. Com isso, reagem mais rapidamente e são capazes de processar uma maior taxa de atualizações, porém, como o seu estado não é totalmente consistente, erros de roteamento podem ser ocasionados, como por exemplo, roteamento em loop. O outro modo de consistência do estado da rede é chamado de fortemente consistente. Neste segundo modo, o controlador opera com uma visão totalmente consistente da rede, de maneira que erros de roteamento são menos comuns, garantindo assim um comportamento mais correto da rede. Entretanto, trabalhar com uma visão consistente da rede, impõe uma alta sobrecarga sobre os equipamentos o que pode vir a causar muito tempo de processamento e limitar a taxa de requisições respondidas.

No trabalho realizado por Reitblatt et al. (2012) são levantadas questões sobre quais os problemas que as atualizações podem causar em um rede SDN. Em uma rede SDN, o plano de aplicação torna simples a implementação de novos serviços para rede e o controle do tráfego interno da rede, entretanto, organizar o modo com que as atualizações serão aplicadas sobre o plano de dados, é importante para que os serviços, atualizações e regras de roteamento funcio-

nem de maneira adequada. No cenário do plano de dados, diferentes dispositivos de encaminhamento estão atuando sobre diferentes rotas e a flexibilidade de uma rede SDN, nos permitiria por exemplo, aplicar regras diferentes a dois conjuntos de dispositivos de encaminhamento, entretanto, caso estes conjuntos de dispositivos estejam conectados entre si, as regras criadas para um dos grupos pode vir a interferir no outro. Por exemplo, conforme a situação ilustrada na Figura 9, os dispositivos A, irão permitir SSH e os Dispositivos B deverão recusar que se realize conexão SSH. S, as atualizações de A forem aplicadas antes que as atualizações de B. O grupo de usuários dos dispositivos B, poderiam acessar dispositivos A, rompendo com a segurança.

Figura 9 – Exemplo do desafio de consistência e ordenamento das atualizações em redes SDN
Fonte: Adaptado de (REITBLATT et al., 2012)

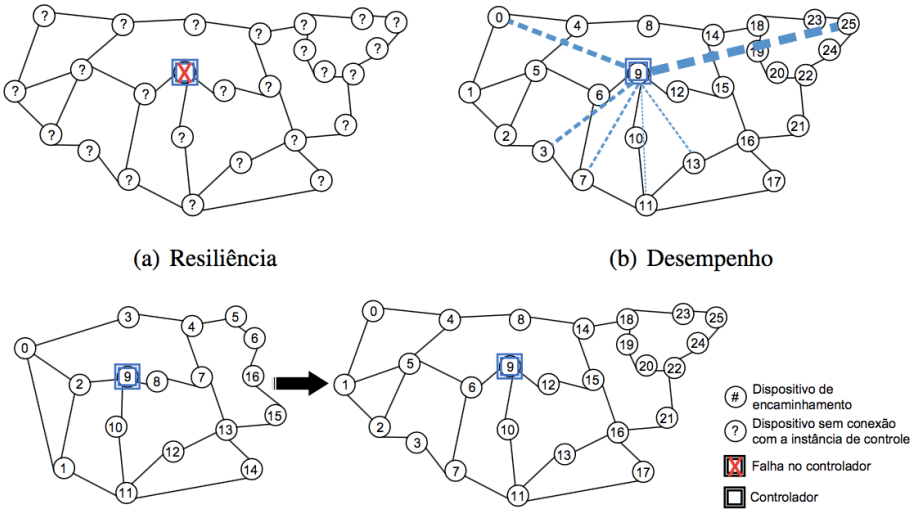


A partir disso, pode-se deduzir que a localização do dispositivo dentro da topologia pode causar problemas com atualizações, fatores como distância, disponibilidade do controlador e velocidade na resposta de requisições estão fortemente entrelaçados neste tipo de compromisso.

Ainda tratando sobre problemas relacionados a localização de dispositivos em redes SDN, este mesmo problema pode englobar instâncias de controladores. O trabalho realizado por Heller, Sherwood e McKeown (2012) aponta que a decisão no número de controladores e o modo com que eles serão dispostos geograficamente, irá se relacionar com a latência e a comunicação, tanto com os próprios controladores, quanto com os dispositivos de encaminhamento, pois, a distância geográfica, pode acabar por atrasar a comunicação entre os controladores e dispositi-

vos de encaminhamento. Quanto mais distante fisicamente eles estiverem posicionados maior será o impacto no atraso de comunicação que poderá surgir, além disso, o número de controladores deve ser relacionado ao número de dispositivos de encaminhamento na rede, isto é, se um grande número de dispositivos de encaminhamento forem direcionados para somente um controlador, as chances deste controlador ter problemas relacionados com latência de comunicação será bem alto, como é mostrado na Figura 10.

Figura 10 – Possíveis Impactos Causados pelo Posicionamento dos Controladores
Fonte:(MüLLER et al., 2014)



Levando ainda em consideração a disposição geográfica das instâncias de controle, Müller et al. (2014) discute, em seu trabalho, questões sobre a sobrevivência da rede no caso de falhas, como a rede iria se recuperar em casos de perder uma das instâncias de controle e o quanto isto viria a afetar todo o plano de controle, tratando sobre pontos específicos de estratégias para reduzir as distâncias dentro da rede, a busca de rotas alternativas (uso de múltiplos caminhos) entre as instâncias de controle para que a rede volte a operar rapidamente em casos de falhas. Com isto, se pode chegar a conclusão, de que a disposição geográfica dos controladores influenciará diretamente o modo de operação de rede e quais os possíveis problemas e/ou benefícios que cada tipo de arquitetura irá trazer.

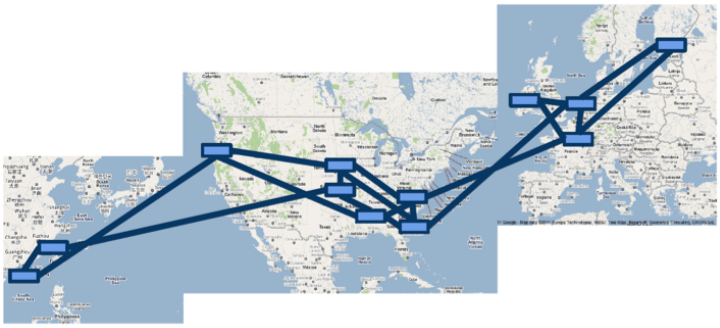
3.3 Implantação de SDN em Redes WAN

Atualmente no cenário de redes SDN, se tem duas importantes implementações de sucesso do paradigma SDN sobre redes WAN. Uma delas diz respeito a rede do Google, chamada B4 (JAIN et al., 2013). Enquanto a outra sobre a rede implementada pela Microsoft, chamada

SWAN (HONG et al., 2013). Nesta seção, serão apresentadas algumas características destas redes.

A rede B4, implantada em 2011, trata-se da rede de backbone Google, isto é, a rede WAN que interconecta todas as redes de datacenter da empresa no mundo. Ela realiza a ligação dos datacenters espalhados pelo globo, como mostra a Figura 11. Através dela são realizadas atividades como backup de dados dos usuários (referente aos serviços prestados pela empresa aos usuários), acesso para armazenamento remoto de fontes distribuídas e sincronização no envio de dados dos estados através de múltiplos datacenters (JAIN et al., 2013).

Figura 11 – Backbone B4 - Implantação 2011
Fonte: (JAIN et al., 2013)



Adotar o paradigma SDN partiu de uma decisão para flexibilizar a rede permitindo ter uma visão centralizada do estado da rede, onde se torna possível ajustar as rotas e coordenação da rede de maneira simples, além da capacidade de trocar os dispositivos de encaminhamento antigos por novos. Além destes fatores, também foram motivados pela arquitetura SDN habilitar a rápida iteração a novos protocolos e a simplificação no ambiente de testes (JAIN et al., 2013).

O outro exemplo de implantação de SDN em redes WAN é a rede SWAN. Ela foi implementada pela Microsoft com o mesmo objetivo, isto é, realizar a ligação entre seus datacenters. Foi cogitado utilizar protocolos como MPLS TE (ROSEN; VISWANATHAN; CALLON, 2001), porém, este protocolo apresenta problemas com eficiência (isto é, não utilizam toda a capacidade do link) e com compartilhamento (isto é, problemas na alocação de recursos e compartilhamento de serviços). A partir deste ponto, paradigma SDN foi escolhido por oferecer suporte e flexibilidade para o controle de tráfego em um ambiente de compartilhamento em toda sua extensão (HONG et al., 2013). Os resultados apresentados nos estudos realizados por Hong et al. (2013) demonstram que a eficiência da utilização do link chega a 99%, enquanto os melhores resultados apresentados pelo protocolo MPLS TE chegam próximos a 65,4%.

Tabela 1 – Resumo do Estado-da-Arte na Organização do Plano de Controle – estratégias e trabalhos relacionados.

Organização	Vantagens	Desvantagens	Exemplos de Destaque
Centralizado Clássico	Simplicidade na implantação de serviços	Ponto central de falhas, limites de escalabilidade.	I. Nox (GUDE et al., 2008) II. Maestro (CAI; COX; NG, 2010)
Centralizado com Cluster de Controladores	Simplicidade na implantação de serviços, com desempenho e escalabilidade mais altos que o centralizado clássico	Ponto central de falhas, limites de escalabilidade, porém oferece uma solução melhor que o centralizado clássico para estes problemas.	I. Opendaylight (OPENDAYLIGHT, 2016)
Hierárquico	Facilidade na implantação de novos serviços na rede	Problemas de desempenho, em alguns casos pode haver um ponto central de falhas.	I. DevoFlow (CURTIS et al., 2011)
Totalmente Distribuído	Alta Escalabilidade, bom controle a erros	Implementação complexa, Dificuldades para o desenvolvimento de novos serviços	I. HyperFlow (TOOTOONCHIAN; GANJALI, 2010) II. Onix (KOPONEN et al., 2010) III. Onos (ONOS, 2016)

4 ESTUDO DE DISTRIBUIÇÃO DO PLANO DE CONTROLE

Este estudo visa uma análise dos compromissos gerados pela distribuição do plano de controle em cenários de redes WAN. As seguintes perguntas de pesquisa são definidas para conduzir o processo de análise das estratégias de clusterização e distribuição geográfica do plano de controle da rede:

- **Como fazer para simular a comunicação distribuída do plano de controle em redes de larga escala?**
- **Como a latência de comunicação da rede afeta as trocas de tráfego na rede, de acordo com as diferentes estratégias de organização do plano de controle?**
- **Como a organização do plano de controle adotada impacta diante da situação da rede enfrentar momentos com uma alta taxa de fluxo de dados sendo transmitidos?**

4.1 Ambiente de Avaliação

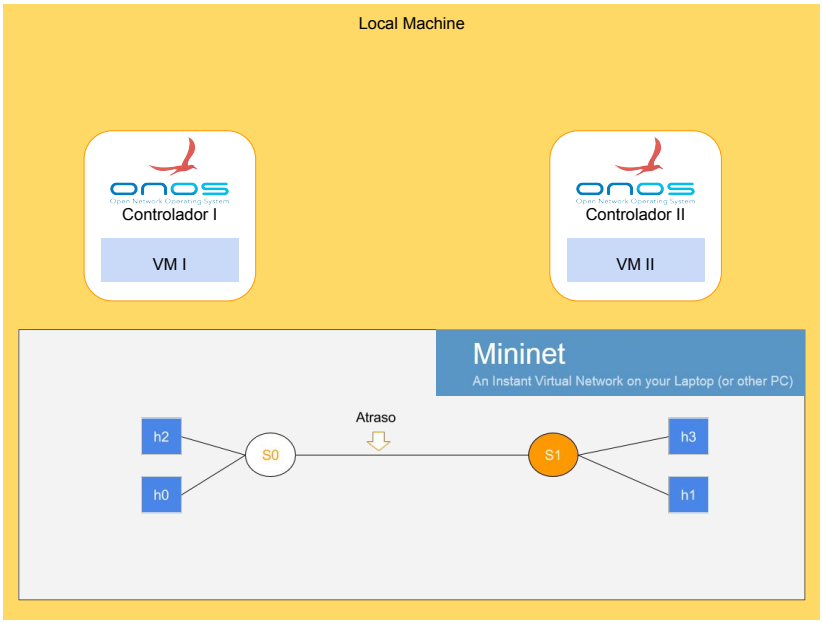
Para viabilizar a realização desse trabalho o primeiro desafio enfrentado foi elaborar o ambiente para a experimentação. A dificuldade de tal objetivo é mensurada pela complexidade dos diversos componentes envolvidos na construção desse ambiente. Não há hoje na literatura uma solução pronta, que ofereça suporte nativo para a experimentação com plataformas de controle distribuídos. Desse modo, foi realizado o estudo apronfundado dos principais componentes e, antes de chegar à solução final (detalhada a seguir), foram elaboradas e experimentadas diferentes propostas arquiteturais que se provaram inviáveis.

Como forma de contribuir para trabalhos futuros é importante reconhecer alternativas que foram avaliadas e experimentadas, porém não foram bem sucedidas. Duas alternativas antes da versão final adotada foram avaliadas. Primeiro o uso do Mininet (MININET, 2016) combinado com a plataforma Docker (DOCKER, 2016), onde um host Mininet foi substituido em tempo de execução por um Docker host para que fosse possível habilitar a plataforma de controle ONOS em cada Docker Host dentro do Mininet. O fato é que tal combinação gerou dificuldades na manipulação do ambiente como um todo, pelo fato da necessidade de ser preciso garantir a comunicação correta e coerente entre todos os componentes, porém nesse formato o processo estava demorando muito para realizar o processo de inicialização do ambiente. Após as dificuldades relatadas, a segunda abordagem avaliada foi experimentar, levantar e organizar o ambiente todo em máquinas virtuais diretamente na Amazon, no serviço EC2 (AMAZON,

2017). Nesta segunda abordagem, o Mininet é colocado numa máquina virtual isolada de todas as plataformas de controle e para cada controlador era instanciada uma nova máquina virtual, separada, de modo a garantir o isolamento necessário para a plataforma ONOS. Para habilitar a interconexão do conjunto de máquinas virtuais instanciadas na Amazon EC2, recorreu-se ao conceito de formação de redes virtuais. Por fim, nessa segunda abordagem a dificuldade ficou por conta da manipulação remota dos recursos do ambiente definido por restrições de segurança da Amazon EC2.

De modo a viabilizar o testbed e, assim a análise das diferentes formas de organização do plano de controle centralizado e distribuído, a arquitetura final definida conta com a plataforma de controle ONOS (ONOS, 2016), os dispositivos de encaminhamento são switches OpenFlow implementados através do software Open vSwitch (Open vSwitch, 2016) que, juntamente com os hosts são instanciados e gerenciados através da plataforma de emulação de redes Mininet (MININET, 2016). A estrutura final elaborada conta com todo o ambiente sendo levantado em única máquina base, sendo apenas os controladores iniciados através de máquinas virtuais utilizando o software Virtualbox (VIRTUAL BOX, 2017). Dessa maneira, temos o sistema operacional base da máquina executando o Mininet e as instâncias dos controladores ONOS sendo levantadas de modo isolado em máquinas virtuais separadas. A Figura 12 demonstra o resultado da arquitetura final do testbed construído.

Figura 12 – Visão Geral do Ambiente de Experimentação.
Fonte: do autor



Os efeitos da escala geográfica da rede em avaliação foram possíveis através de ferramen-

tas como Netem (NETEM, 2016) que executa manipulações da disciplina de filas do controle de tráfego, sendo ela utilizada junto com outras na base da arquitetura do emulador de redes Mininet. Vale ressaltar que este conjunto de ferramentas são amplamente adotadas e aceitas em publicações científicas da área de Redes de Computadores (YAN; MCKEOWN, 2017) (LANTZ; O'CONNOR, 2015).

No que segue são apresentados e explicados os componentes que fazem parte do testbed elaborado neste trabalho. Se tratam de aplicações com uma complexidade bastante elevada de operação, entretanto, apresentam ampla adoção pela comunidade de Redes de Computadores. Primeiro é apresentado a implementação em software de switch de rede, o Open vSwitch (Subseção 4.1.1); seguindo com detalhes da plataforma Mininet (Subseção 4.1.2), a descrição da plataforma de controle distribuída ONOS (Subseção 4.1.3); concluindo com a especificação do ambiente utilizado para o desenvolvimento do trabalho (Subseção 4.1.4).

4.1.1 Open vSwitch

Open vSwitch é um software de código aberto utilizado como base na ferramenta Mininet (MININET, 2016) para iniciar os dispostivos de encaminhamento da rede, que tem o objetivo de instanciar switches virtuais, realizar a comunicação de máquinas virtuais entre si ou com a rede física. Segundo Spenneberg (2011) "o Open vSwitch suporta fluxos de dados, VLANs, entroncamento e a agregação de portas exatamente como os principais switches do mercado.", ou seja, com o Open vSwitch, se torna possível a construção de estruturas de rede mais complexas e robustas para avaliação.

O Open vSwitch, foi implementado para dar suporte a um ambiente virtualizado de larga escala, oferecendo funcionalidades como fácil adaptação, programabilidade, ser controlado e monitorado de forma remota o tornam uma boa solução. Segundo o Open vSwitch (2016) Open vSwitch se destaca pelas seguintes características:

- Mobilidade de Estado: os estados da rede são facilmente identificados e migrados entre os diferentes hosts.
- Resposta para dinamicidade das redes: ambientes virtuais muitas vezes são associados a uma grande taxa de mudanças. O Open vSwitch contém uma série de ferramentas para responder e se adaptar a essas mudanças, como por exemplo, o suporte ao OpenFlow.
- Manutenção de Tags Lógicas: dispositivos virtuais distribuídos grande parte das vezes mantém o controle lógico da rede, adicionando ou manipulando tags nos pacotes. Essas

tags podem ser usadas para expressar o contexto ou a relevância no domínio lógico. O Open vSwitch possui vários métodos para especificar e manter regras sobre as tags, além de permitir que regras e mapeamento de rotas sejam configuradas, alteradas e migradas.

- Integração com o Hardware: o Open vSwitch possui uma otimização para que o plano de controle seja capaz de lidar com os dispositivos de encaminhamento implementados puramente em software e também com os dispositivos físicos.

4.1.2 Mininet

O Mininet é uma ferramenta que possibilita a simulação de Redes Definidas por Software. Ele torna possível a prototipação rápida de uma rede SDN, oferecendo a possibilidade de criar grandes redes virtuais em apenas um computador. Além disso, as redes criadas sob o ambiente Mininet também são escaláveis e implementam a comunicação dos dispositivos de encaminhamento e o(s) controlador(es) via protocolo OpenFlow. Desta forma, é possível que topologias de redes SDN, sejam criadas, configuradas e alteradas, conforme for necessário (LANTZ; HELLER; MCKEOWN, 2010).

De acordo com (MININET, 2016), o Mininet:

- Provê uma maneira barata para o teste e desenvolvimento de aplicações OpenFlow.
- Torna possível o trabalho conjunto de mais de um desenvolvedor.
- Permite emular diferentes tipos de topologias de rede e que estas sejam testadas sem que seja necessário um equipamento físico.
- Habilita depurar e realizar testes em toda rede.
- Disponibiliza API's em Python para o desenvolvimento de serviços para rede.

Isso posto, o ambiente Mininet se mostra uma boa escolha. O Mininet também possuí a vantagem, de habilitar a sua execução nos sistemas operacionais Mac, Linux e Windows.

4.1.3 Onos

Onos (Open Network Operation System), é um sistema operacional para redes SDN que tem por objeto prover escalabilidade, alta disponibilidade, alta performance e abstrações para oferecer um ambiente simples de criar e implementar novos serviços na rede (ONOS, 2016). A partir dele, é possível ter-se uma visão logicamente centralizada de toda a rede para desenvolvimento de serviços, estando o plano de controle organizado de forma centralizada ou distribuída.

O projeto Onos foi desenvolvido seguindo pré-requisitos fundamentais. Primeiro, implementa a visão logicamente centralizada da rede em uma plataforma distribuída, para lidar com escalabilidade e tolerância à falhas (BERDE et al., 2014). Segundo, o Onos é focado para melhorar o desempenho do sistema operacional de rede.

No que se refere a escalabilidade, o Onos permite a execução distribuído em vários servidores, cada um como um controlador OpenFlow mestre, responsável por um conjunto de dispositivos de encaminhamento. Cada instância do Onos tem a responsabilidade de propagar as mudanças de estado entre os dispositivos de encaminhamento, além de controlar e manter a visão global da rede.

Por fim, no quesito de tolerância a falhas um dispositivo de encaminhamento pode se conectar várias instância Onos, porém, somente uma dessas pode ser a mestre em dado instante de tempo. A instância mestre tem a função de descobrir as informações da rede e configurações de cada dispositivo de encaminhamento. Quando falha, as demais instâncias de controle presentes na rede, elegem uma nova que se tornará a mestre, tornando-se a responsável por manter as funções citadas anteriormente.

4.1.4 Especificações do Ambiente

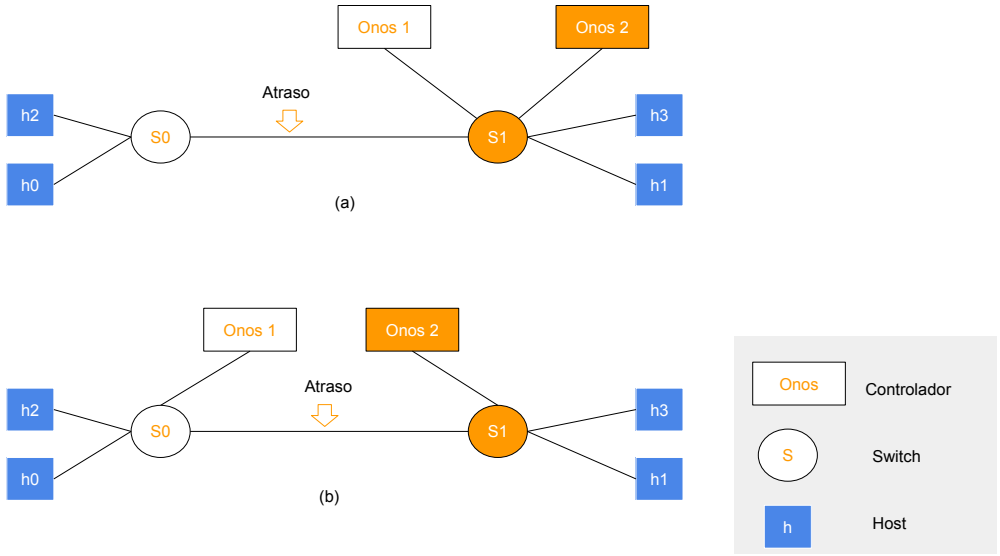
As avaliações sobre o ambiente desenvolvido foram executados em uma máquina com processador Intel(R) Core^{TM} i5-5200U CPU @ 2.20GHz x 4, executando o sistema operacional Ubuntu (64 bits) 16.04 (kernel 4.4.0-47-generic) com 8GB de memória RAM. Sera utilizado o VirtualBox 5.1.18 juntamente do Open vSwitch 2.6.1, ONOS 1.10.0, Mininet 2.2.2, e OpenFlow 1.5.

4.2 Cenários de Avaliação

A topologia empregada na avaliação foi escolhida de acordo com a forma como suas características contribuiriam para a análise. Nessa decisão priorizou-se a capacidade de fornecer resultados generalizáveis. Desta forma, foi definida a topologia linear simples para uso nos cenários da avaliação, que serão apresentados abaixo.

Topologia Linear Simples. Em primeiro lugar, se buscou isolar comportamentos específicos de cada forma de organização do plano de controle sob análise. Esse requisito levou a conceber uma topologia geral mais simples, permitindo identificar e capturar características importantes. A Figura 13 ilustra a topologia em questão, denominada topologia linear simples

Figura 13 – Casos centralizados (superior) e distribuído (inferior) utilizados para as avaliações. Observe que, no caso centralizado, ambas as instâncias de controle estão localizadas no switch S1.
Fonte: do autor



em todo o trabalho.

Nesta topologia, são limitados os números de instâncias de controle, bem como o número de dispositivos de encaminhamento, para dois. Cada dispositivo de encaminhamento tem dois hosts conectados a ele. A idéia por trás dessas opções de design foi reproduzir, com um cenário genérico controlado, que tivesse suporte a dois tipos de interações: (i) interações locais entre hosts co-localizados (hosts conectados ao mesmo switch) e, (ii) interações globais entre hosts separados geograficamente (cada host conectado a um switch diferente). Foram utilizados dois esquemas de distribuição das instâncias de controle: um em que ambas as instâncias estão conectadas ao mesmo switch (S1, neste caso) - centralizado (Figura 13, a) - e outro onde cada instância é localizada em uma região diferente e conectada a um dispositivo de encaminhamento diferente - distribuído (Figura 13, b).

Nesses cenários, foi variado o atraso de propagação imposto no enlace entre os dispositivos de encaminhamento (switches), a fim de entender melhor os efeitos de um cenário de WAN, e isso em cada esquema de plano de controle em avaliação. Em ambos os esquemas de plano de controle avaliados, existe um canal de sincronização que liga os dispositivos de controle (usando uma ponte OVS, Open vSwitch, ou também chamada bridge OVS). No caso centralizado, o planejamento foi medir a menor latência para as interações locais que se aproximam das instâncias de controle (por exemplo, h1-h3 - consulte a Figura 11-a), enquanto que as interações globais (por exemplo, h0-h1) e as interações locais que ocorrem longe (por exem-

plo, h0-h2) devem apresentar piores resultados, mas menor variabilidade em geral. Quanto ao caso descentralizado, imagina-se obter resultados de latência variáveis (principalmente devido a problemas de sincronização de estado), com alta latência ainda. No entanto, no caso de interações locais, dado um mapeamento apropriado de controladores-para-switches, espera-se ver uma latência baixa nas interações para ambas as regiões da rede, uma vez que cada instância de controle poderia simplesmente configurar um dispositivo de encaminhamento vizinho sem ter muita necessidade de sincronização.

Por fim, cabe citar que, além dos cenários recém apresentados se tinha o objetivo de desempenhar avaliações considerando também a topologia da rede acadêmica norte americana Internet2 que possui 10 dispositivos de encaminhamento e 15 enlaces distintos. Entretanto, não foi possível. Assim, a avaliação utilizando a topologia da Internet2 fica como sugestão de trabalhos futuros.

Dentre os principais fatores que impossibilitaram a experimentação em topologias de rede de maior escala temos: a complexidade da instrumentação do ambiente para as avaliações e a dificuldade de experimentar em topologias maiores. No primeiro, foi necessário investir um tempo grande no desenvolvimento do ambiente para conectar todos os componentes necessários, fazê-los funcionar adequadamente para o propósito do trabalho e, lidar com todos os desafios da operação de bootstrap (inicialização) das topologias de rede emuladas. E no segundo, para se ter uma ideia, apenas o processo de bootstrap mencionado, que envolve a inicialização de equipamentos e controladores no ambiente emulado, somado a experimentos iniciais desempenhados com a topologia da Internet2 estava exigindo para cada cenário avaliado mais de 22h de execução.

4.3 Metodologia Empregada na Experimentação

Nas seções a seguir, é descrita a metodologia empregada nos experimentos para comparar planos de controle centralizados e fisicamente distribuídos. Os experimentos são executados considerando um ambiente de emulação já inicializado como pré-condição. A Seção 4.3.1 descreve a métrica de latência do plano de dados, envolvendo reatividade do plano de controle. A Seção 4.3.2, por outro lado, apresenta a segunda métrica, que se concentra na determinação dos efeitos da configuração do plano de controle empregado em interações de plano de dados intensivo.

4.3.1 Tempo de Ida e Volta dos Hosts (Round-Trip Time)

O tempo de ida e volta dos hosts, popularmente conhecido na área de redes como RTT (Round-Trip Time), se refere ao tempo que um pacote leva para atingir seu destino e retornar a confirmação do recebimento para o emissor (KUROSE; ROSS, 2012). Este tipo de métrica é importante, pois através dela é possível entender aspectos relacionados ao desempenho de todo conjunto da rede. Com isso, o tempo de resposta entre dois hosts afeta o quão responsivos os serviços são, e isso por sua vez vai afetar a qualidade do serviço que vai ser oferecido ao usuário final (STROWES, 2013).

Para avaliar este ponto, a cada par de hosts foram executadas uma série de repetições do envio de mensagens do tipo ICMP echo usando a ferramenta ping. Isto requer que os dispositivos de encaminhamento interajam com seus controladores, de modo a definir relativamente um caminho que habilita a conectividade a ser mantida entre os hosts. Além disso, foi colocado um atraso no link que conecta os dois switchs das topologias lineares. Este atraso foi definido em 0 (corresponde a um caso ideal, onde nenhum atraso de propagação influenciaria o testbed), 5, 10, 15, 20 e 25 ms (milissegundos) para cada mensagem ICMP enviada sob a topologia e então gerado um arquivo de log, no qual é possível analisar a média do RTT presente na comunicação de cada host com os demais. Ao fazer isso, espera-se entender melhor a capacidade de resposta do esquema de controle subjacente sempre que for necessário para o plano de controle atuar em eventos do plano de dados.

4.3.2 Vazão (throughput) dos Hosts

A vazão, no contexto de redes de computadores, trata-se da medida que caracteriza a capacidade de transmissão do canal de conexão entre dois hosts. Sendo assim, a vazão de uma rede é a quantidade de D bits que um host A consegue transmitir para um host B em um dado espaço de tempo T segundos. Logo, pode-se dizer que a rede tem uma vazão de D bits por T segundos. Assim sendo, quanto maior a vazão que se pode disponibilizar ao canal de rede, maior será a capacidade de transmissão (KUROSE; ROSS, 2012).

Para avaliar os pontos deste experimento, cada host enviou um volume pré-definido de tráfego para todos os outros durante um tempo também pré-definido. Este tráfego foi transmitido sob os protocolos UDP e TCP, e foram gerados arquivos de log com os resultados obtidos. Durante realização deste experimento foi utilizada a ferramenta Iperf3 (IPERF, 2017), que possibilita que a média de vazão dos hosts seja mensurada. Ao realizar esta etapa, busca-se o

entendimento sobre os efeitos que a configuração do plano de controle tem em interações intensivas no plano de dados. Isto é, o objetivo principal desta avaliação é obter uma noção de como o throughput (vazão) do host é afetado para cada tipo de esquema de organização do plano de controle.

5 RESULTADOS

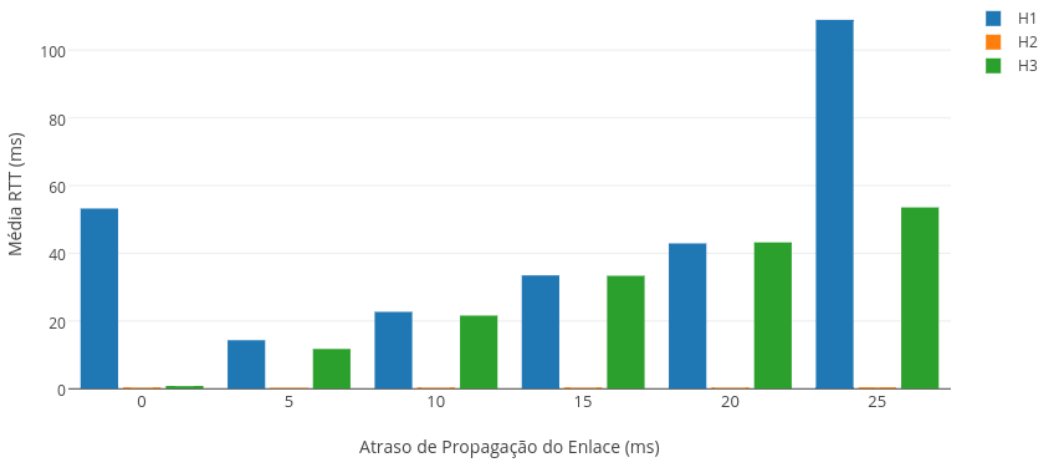
Neste Capítulo serão apresentados os resultados dos experimentos previamente definidos. Como já exposto no Capítulo 4, o objetivo é responder as seguintes questões: (a) como a latência de comunicação da rede afeta as trocas de tráfego na rede, de acordo com as diferentes estratégias de organização do plano de controle? e, (b) como a organização do plano de controle adotada impacta diante da situação da rede enfrentar momentos com uma alta taxa de fluxo de dados sendo transmitidos? Nessa direção, a Seção 5.1 trata dos experimentos utilizando a primeira métrica (tempo de ida e volta - RTT entre hosts), que busca responder a primeira questão colocada, relacionada a responsividade do plano de controle em reação de eventos na rede. A Seção 5.2, por sua vez, aborda os experimentos da segunda métrica (vazão da rede ou throughput), buscando compreender os efeitos da distribuição do plano de controle quando a rede enfrenta situações de carga intensa. Todos resultados são relacionados a topologia linear que foi apresentada no Capítulo 4.

5.1 Responsividade do Plano de Controle

Esta seção apresenta as descobertas para a primeira métrica do nosso estudo. Busca-se identificar resultados e princípios gerais, analisando os resultados experimentais sobre a topologia linear simples (exibida na Figura 13) se buscou analisar o seguinte ponto (i) entender como a latência em um único salto pode afetar a comunicação entre hosts, considerando um plano de controle distribuído.

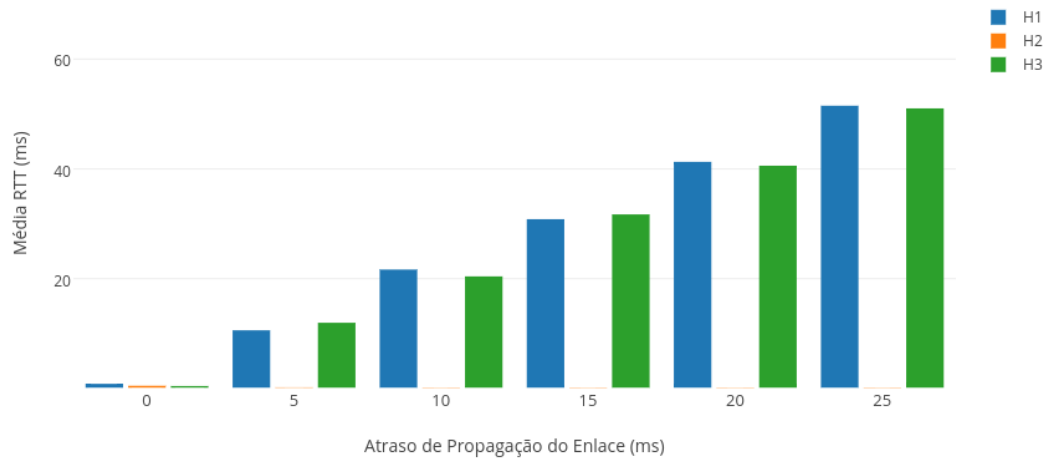
Topologia Linear I - Centralizado

Figura 14 – Média RTT H0 Topologia Linear I - Centralizado
Fonte: do autor



Os resultados são exibidos nos gráficos das Figuras 14 e 15. Os gráficos apresentam a relação média de RTT entre cada par de hosts considerando o atraso de propagação. Como é possível notar na Figura 14, o RTT de h0 para os demais hosts tende a aumentar linearmente, conforme o atraso no enlace entre os dois switches também aumenta. Este atraso não interfere no RTT entre h0 e h2, já que os dois hosts estão conectados no mesmo switch. Entretanto, no caso do primeiro experimento, envolvendo h0 e h1, se percebeu um RTT acima da média. O motivo disto é que durante os experimentos, as primeiras 6 mensagens ICMP enviadas de h0 para h1 foram perdidas, pois o plano de controle ainda não havia estabelecido uma rota entre eles. Devido a isto, a média foi calculada somente entre as outras mensagens, o que ocasionou uma valor acima do usual.

Figura 15 – Média RTT H3 Topologia Linear I - Centralizado
Fonte: do autor

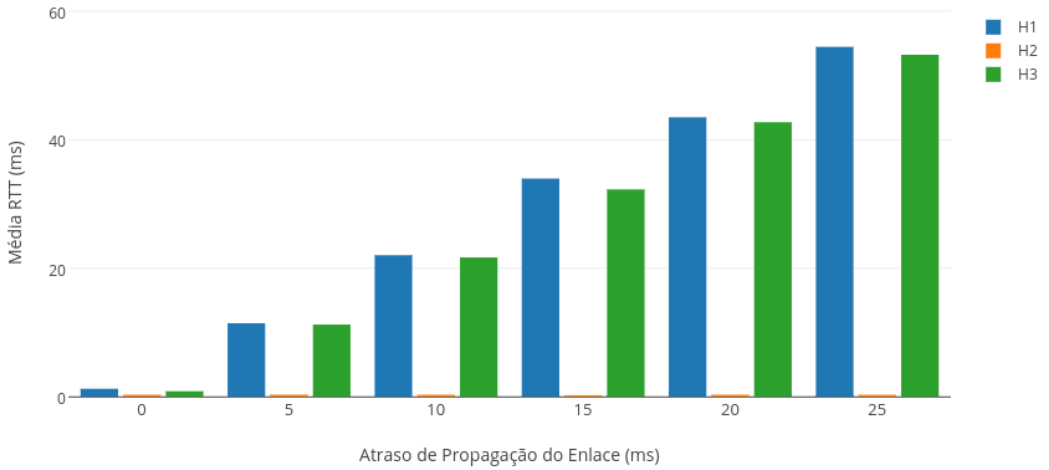


Conforme pode-se ver na Figura 15, ela trata dos valores de RTT adquiridos sobre comunicação de h3 para os demais hosts da rede. Pode-se notar que o comportamento envolvendo estes valores é semelhante aos da Figura 14, já que o tempo de comunicação entre o host co-localizado se mantém na mesma média, enquanto as interações globais entre hosts separados geograficamente (hosts conectados a um switch diferente) tendem a aumentar linearmente conforme o atraso é incrementado.

Topologia Linear II - Distribuído

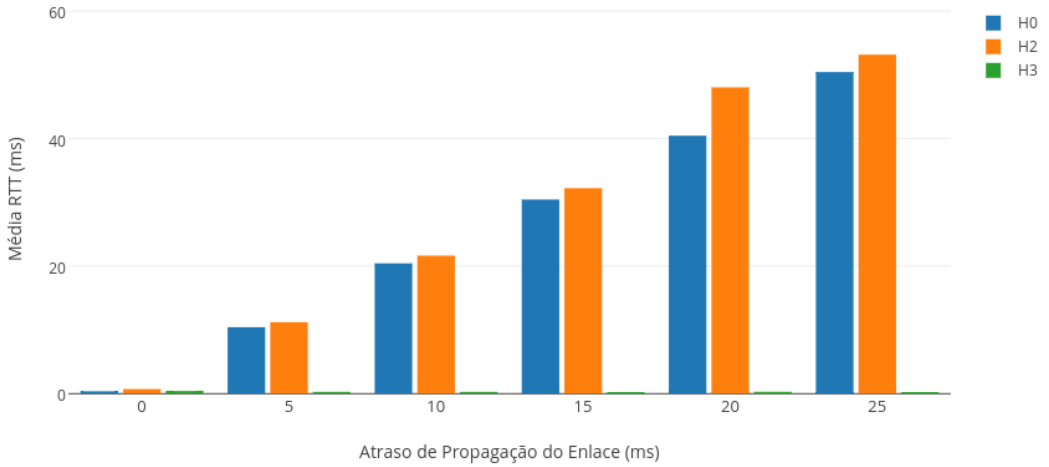
Contudo, ao partir para os gráficos que referem-se a topologia linear II, é possível ver que a Figura 16, que mostra o resultado da comunicação entre h0 e os demais hosts, nota-se uma diferença quando observado em perspectiva ao gráfico da topologia linear I, Figura 14, pois não houve média de RTT fora do padrão entre os primeiros hosts. Neste caso, a média de RTT se

Figura 16 – Média RTT H0 Topologia Linear II - Distribuído
Fonte: do autor



manteve com comportamento constante, isto é, ao variar o parâmetro de atraso no enlace o que se observa é o crescimento de tendência linear esperado para essa situação.

Figura 17 – Média RTT H1 Topologia Linear II - Distribuído
Fonte: do autor



Na Figura 17, que representa o resultado das outras parcelas da topologia da rede, nota-se que o comportamento em relação a responsividade manteve-se dentro do que apresenta ser o padrão, com o host h1 se comunicando com os demais, os valores em relação aos hosts separados geograficamente tendem a aumentar conforme o atraso do enlance é incrementado, enquanto o host que divide o mesmo switch, tende a continuar dentro da mesma média.

Além disso, as Figuras 18 e 19, dizem respeito a comunicação de h2 e h3 com os demais hosts da topologia linear II. Ao analisar os gráficos, observa-se o mesmo resultado, em que a comunicação com os hosts separados geograficamente tende a possuir uma média mais alta em

relação ao RTT, e esta média continua aumentando em função do parâmetro de atraso do enlace que foi variado nos experimentos. Do mesmo modo, os hosts co-localizados tendem a se manter em uma mesma média de RTT do início ao fim do experimento.

Figura 18 – Média RTT H2 Topologia Linear II - Distribuído
Fonte: do autor

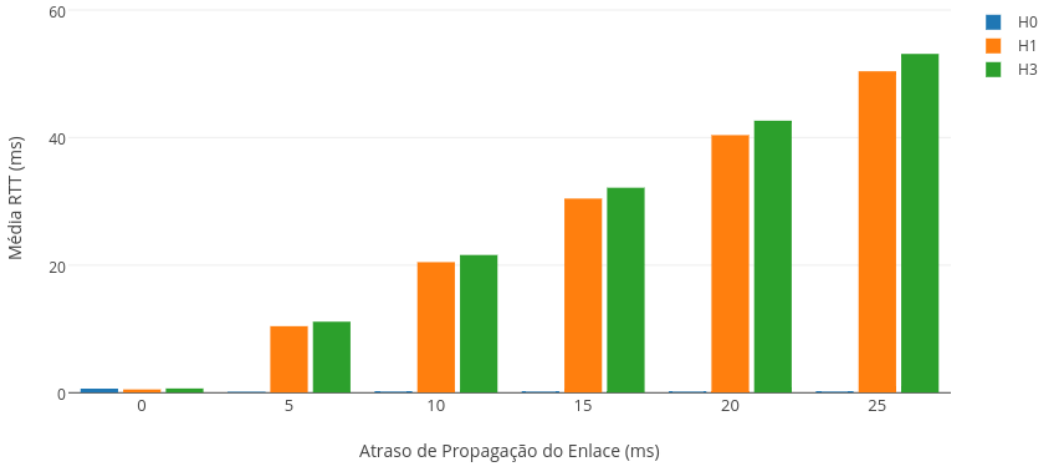
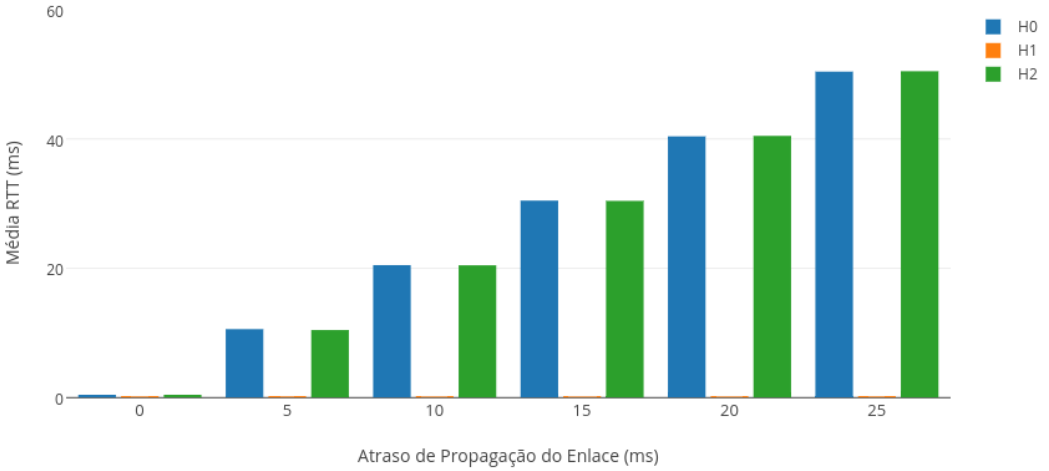


Figura 19 – Média RTT H3 Topologia Linear II - Distribuído
Fonte: do autor



Ao fim deste experimento, é visível que apesar de na maioria dos casos, as médias de RTT obtidas nas duas topologias se mostrassem semelhantes, nos casos da topologia linear II, as médias se mantiveram mais controladas, apresentando o crescimento esperado nessas situações, mesmo com a dependência dos dispositivos de encaminhamento de uma entidade externa como o controlador. Alguns pontos relevantes a se destacar das descobertas realizadas: (i) tanto no cenário centralizado como no distribuido o comportamento de crescimento segue uma

distribuição linear, (ii) equipamentos conectados a controladores em regiões distantes vão apresentar efetivamente atrasos maiores na reação a eventos na rede e, (iii) no cenário distribuído se observou que mesmo para casos onde os eventos poderiam ser facilmente tratados localmente pelos controladores em cada região, a plataforma de controle ONOS emprega a política de sincronização fortemente consistente, o que obriga a cada controlador antes de tomar sua decisão sincronizar com as demais instâncias presentes na rede - gerando assim atrasos adicionais na comunicação.

5.2 Efeitos de interações intensivas no Plano de Dados

Esta seção apresenta as descobertas para a segunda métrica do nosso estudo (vazão da rede). Da mesma forma que explicado antes, busca-se identificar resultados e princípios gerais, analisando os resultados experimentais sobre a topologia linear simples (exibida na Figura 13). O objetivo aqui foi: isolar e analisar o comportamento de encaminhamento do tráfego local e global sob cada tipo forma de organização do plano de controle.

Os primeiros resultados relacionados aos experimentos com o tráfego UDP são exibidos em formato de tabelas. Nestas tabelas, a coluna da esquerda representa o host de origem, enquanto a linha superior refere-se ao host de destino do tráfego. Os valores nela equivalem a Gbits/s (Gigabits por segundo).

Primeiramente, é realizado uma discussão dos resultados obtidos em relação ao tráfego UDP sobre as iterações relacionados a topologia linear I - Centralizado.

Tabela 2 – Vazão Topologia Linear I - Centralizado

	H0	H1	H2	H3
H0	—	5.51	8.78	5.56
H1	8.68	—	6.49	8.42
H2	10.0	6.73	—	6.41
H3	8.23	8.20	6.19	—

Na tabela 2, pode-se notar que primeiramente h0 consegue transmitir em torno de 8.78 Gbits/s para o host que está ligado no mesmo switch, porém para os hosts do outro switch apenas transmite em torno de 5.50 Gbits/s. Esta situação muda em relação ao h1, que mesmo estando em um switch diferente de h0, consegue transmitir a este a média de 8.68 Gbits/s, enquanto que para o h3, que está no mesmo dispositivo de encaminhamento, ele envia um valor abaixo, na média de 8.42 Gbits/s. No caso de h2, este comporta-se semelhante a h0, transmitindo mais para o host que compartilha o mesmo switch, neste caso ele consegue transmitir a capacidade

total de 10 Gbits/s. Finalizando com uma análise sobre h3, este mantém o comportamento de h1, transmitindo para h0 uma média semelhante ao que envia para o host no mesmo dispositivo de encaminhando, em torno de 8.20 Gbits/s.

Tabela 3 – Vazão Topologia Linear II - Distribuído

	H0	H1	H2	H3
H0	—	8.71	9.99	8.51
H1	7.89	—	8.38	9.41
H2	8.47	8.15	—	9.15
H3	7.60	9.98	8.97	—

Já na Tabela 3 é demonstrada a relação de vazão encontrada na topologia linear II - Distribuído. Esta topologia apresenta um comportamento semelhante a topologia centralizada, entretanto, os valores obtidos são consideravelmente maiores. Enquanto na topologia centralizada, os valores médios variam em torno de 5 Gbits/s a 8 Gbits/s, sendo que exclusivamente 1 valor chegou a marca de 10 Gbtis/s. Na topologia linear II, os valores variam na média de 7 Gbtis/s até 9 Gbtis/s, mesmo que em nenhum caso tenha ocorrido uma transmissão com total a capacidade de 10 Gbtis/s, ocorreram 4 casos em que se alcançaram a média de 9 Gbtis/s e desses 4 casos, 2 deles tiveram valores de 9.99 e 9.98 Gbits/s.

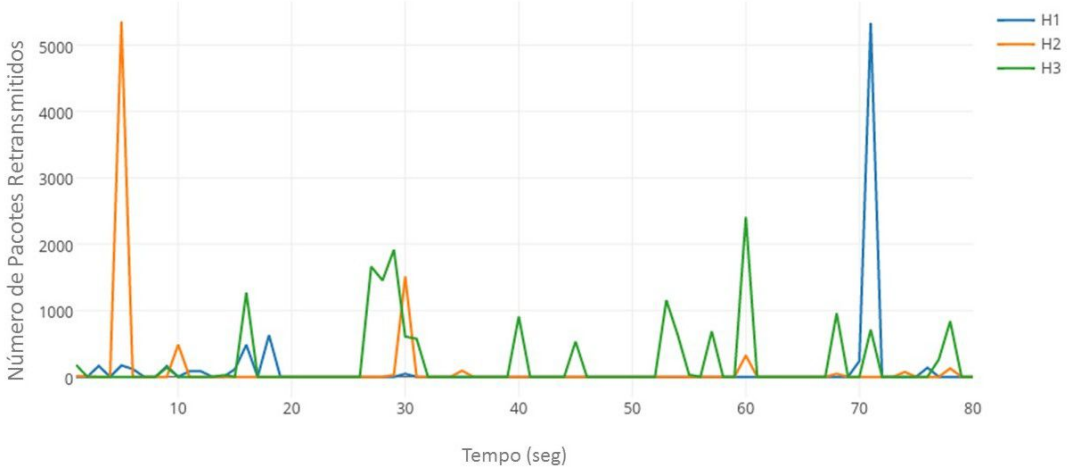
Além dos resultados discutidos até esse momento, é importante citar que foi realizado outra série de experimentos com o propósito de avaliar qual seria o impacto do atraso de propagação dos enlaces na vazão do tráfego da rede. Para tanto, assim como foi aplicado para a primeira métrica (RTT), foram desempenhados experimentos de vazão da rede com diferentes configurações de atraso sobre o enlace entre os switches da topologia. O que foi observado é que a vazão agregada entre os hosts apresentou uma variação muito baixa, mesmo quando houve a variação do atraso de propagação do enlace, portanto como os resultados não adicionariam novidades, foram suprimidos do presente trabalho de conclusão.

Dando continuidade, serão agora apresentados os gráficos obtidos em relação a vazão de tráfego TCP. Entretanto, é necessário ressaltar que nesta etapa, foi utilizada outra forma de avaliação dos resultados, pois o TCP conta com mecanismos que garantem o reenvio de pacotes que não foram devidamente entregues, devido a isto, o volume de tráfego entregue é sempre muito próximo ao enviado. Dessa maneira, para mensurar os resultados, foram gerados gráficos a partir da quantidade de pacotes reenviados para o destino, isto é, foi analisada a taxa de pacotes re-transmitidos ao longo do tempo da comunicação entre os hosts. Cada gráfico mostra o comportamento da quantidade de pacotes reenviados durante o período de 80 segundos

(tempo necessário para warm-up das conexões e troca de tráfego definido empiricamente através de experimentos prévios), na tentativa de transmissão de 10 Gbits/s, para o host em questão.

Topologia Linear I - Centralizado

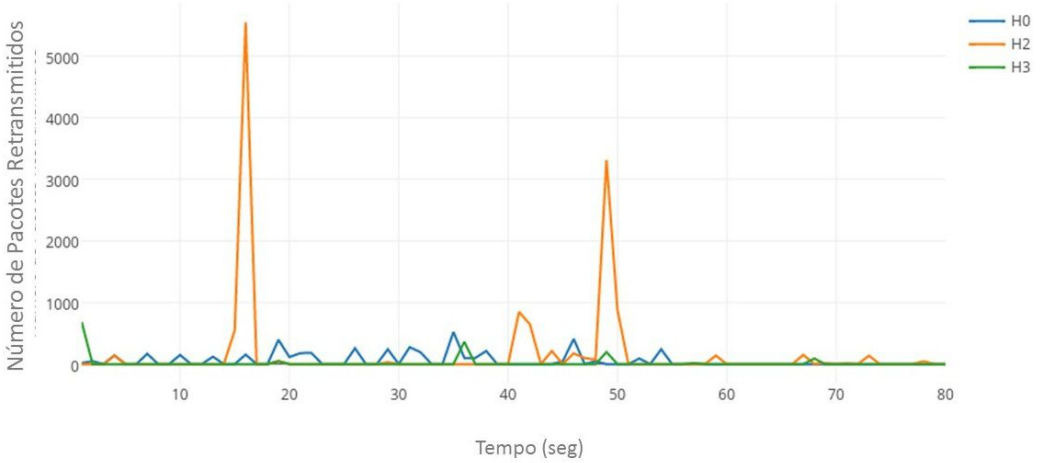
Figura 20 – H0 Retransmissão de Pacotes Topologia Linear I - Centralizado
Fonte: do autor



A Figura 20 apresenta o número de pacotes reenviados pelo host h0, durante 80 segundos. É possível notar que o host co-localizado, no caso h2, sofre um pico entre 0 e 10 segundos, reenviando mais de 5000 pacotes em um determinado instante, e volta a apresentar alguns picos durante o resto do experimento, porém nenhum deles apresenta um valor tão alto no reenvio das mensagens. Pelo que pode ser observado, essa situação ocorreu em razão do controlador centralizado ter dado prioridade no atendimento do switch distante para a definição das regras para o correto encaminhamento de pacotes. Quanto aos hosts que representam interações globais, h1 demonstra um ótimo desempenho, mesmo em um caso de um pico no qual também reenviou mais de 5000 pacotes (fato que ocorreu pelo tempo de expiração das regras inseridas pelo controlador nos switches), ele manteve-se a maioria do tempo em uma média igual ou inferior h2. Já h3 não demonstrou resultados tão bons, tendo vários picos na retransmissão dos pacotes, entretanto, nenhum desses picos superou 3000 pacotes, caso que deixa evidente que em situações de sobrecarga na rede existe uma tendência não negligível de que a sobrecarga afete a qualidade de comunicação de um modo geral na infraestrutura.

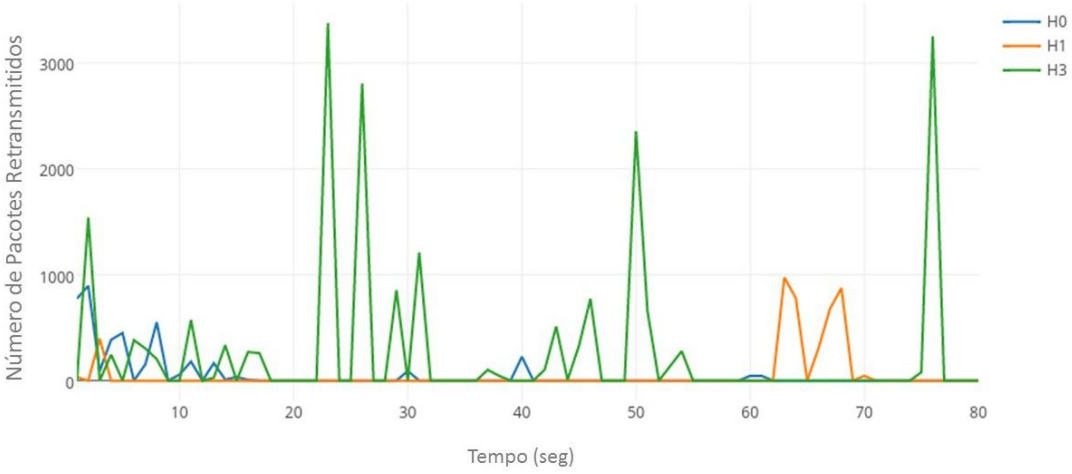
Já na Figura 21, são mostrados os dados referentes a interações envolvendo o envio do volume de dados a h1. Neste caso o host co-localizado a ele, h3, demonstrou um resultado ótimo, mesmo que começando com um pico próximo a 1000 retransmissões, logo retorna a valores baixos, sofrendo muito pouca variação durante os 80 segundos. O host h2 comporta-se

Figura 21 – H1 Retransmissão de Pacotes Topologia Linear I - Centralizado
Fonte: do autor



com um bom desempenho geral, porém apresenta alguns picos de retransmissões bem acima da média encontrada nesse gráfico, um destes com mais de 5000 reenvios. E por final, falando-se de h0, ele demonstrou um comportamento regular, mantendo-se quase sempre dentro de uma mesma média de retransmissões e esta média representando um valor abaixo de 1000.

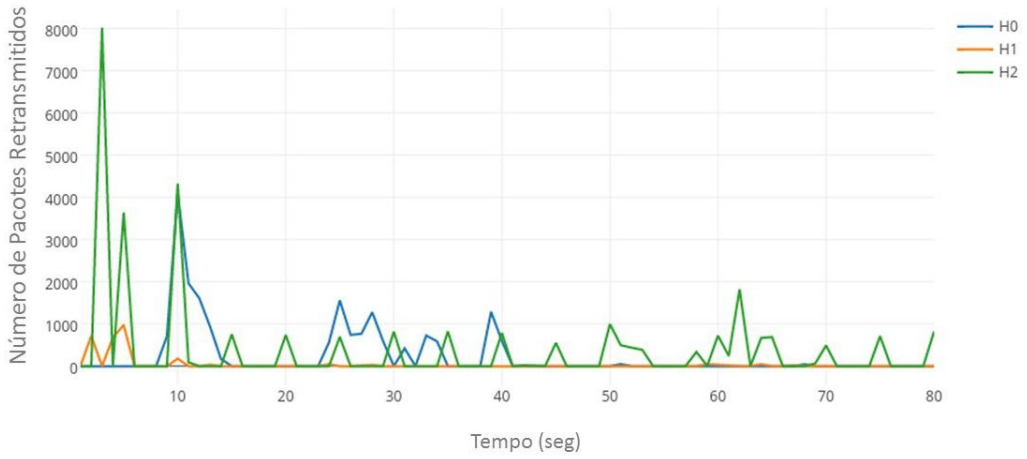
Figura 22 – H2 Retransmissão de Pacotes Topologia Linear I - Centralizado
Fonte: do autor



O próximo gráfico, apresentado pela Figura 22, diz respeito as interações envolvendo h2. Neste experimento o host co-localizado, h0, se mostrou instável nos primeiros 10 segundos com alguns picos de retransmissões, contudo antes mesmo de alcançar 20 segundos voltou a apresentar valores baixos e manteve-se assim quase todo o tempo, exceto por mais alguns pequenos picos de reenvios, porém nenhum desses de grande valor ou duração. O host h1 entretanto, apresentou um bom desempenho, sofreu uma pequena variação no inicio e após

manteve valores baixos até 60 segundos, entre os tempos de 60 e 70 segundos demonstrou alguma variação, mas logo voltou a reduzir o número de retransmissões. Já h3, exibiu um desempenho ruim neste caso, tendo vários picos de reenvios durante toda a execução, estes picos com valores acima de 2000 retransmissões.

Figura 23 – H3 Retransmissão de Pacotes Topologia Linear I - Centralizado
Fonte: do autor



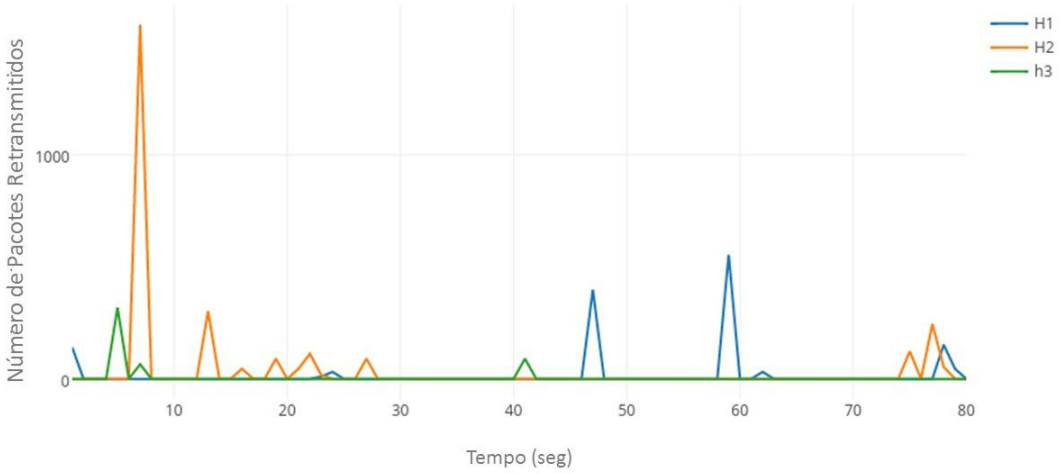
A Figura 23 demonstra o comportamento dos demais hosts referente a comunicação com h3. Neste experimento, o host h1, mostrou um desempenho ótimo, teve alguns picos de retransmissões durante os primeiros segundos, entretanto após não demonstrou nenhum outro aumento na taxa de retransmissões e continuou assim até o fim do tempo. Os hosts h0 e h2 já não exibiram um desempenho tão bom, h0 teve vários picos de retransmissões voltando a estabilizar somente após 40 segundos, enquanto h2 apresentou um altíssimo índice de reenvios no inicio do experimento, atingindo a taxa de 8000 reenvios em um ponto, além disso, se manteve instável durante todo o restante do tempo, com diferentes momentos de pico.

Como pode ser observado nos resultados do cenário centralizado com o tráfego TCP, existe uma sobrecarga natural do protocolo que requer o estabelecimento da conexão entre hosts (através do handshake de três vias), além de garantir que todas as mensagens de dados e controle sejam recebidas para regular os mecanismos de garantias de comunicação do protocolo. Essa sobrecarga é somada ao procedimento das plataformas de controle da rede que visam instalar as regras necessárias para os switches desempenharem corretamente suas ações de encaminhamento de pacotes. Diante dessa combinação o que se pode observar é que para todos os cenários executados foram registrados momentos de pico na retransmissão de pacotes, fato este comprovado pela sobrecarga de gerenciamento existente sobre um único ponto da rede

quando há uma situação de sobrecarga nas comunicações entre hosts.

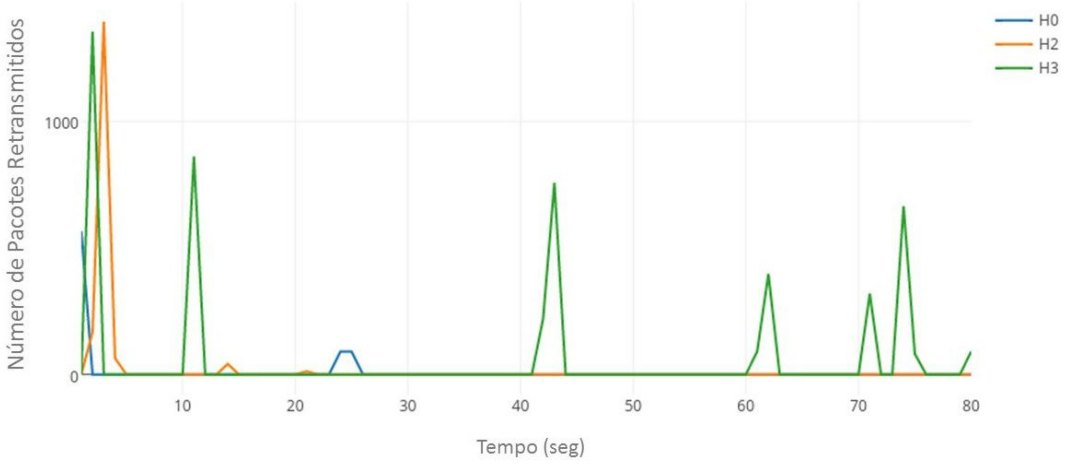
Topologia Linear II - Distribuído

Figura 24 – H0 Retransmissão de Pacotes Topologia Linear II - Distribuído
Fonte: do autor



A Figura 24 demonstra o resultado das interações com o host h0 da topologia distribuída. É possível ver que o host co-localizado, no caso h2, demonstra uma taxa de 1000 retransmissões próximo a 10 segundos e após apresenta outros pequenos picos. Entretanto, nenhum destes outros possui um valor tão elevado. H1 e h3 apresentam um comportamento semelhante, com alguns picos durante o tempo de transmissão, porém mantendo-se estáveis a maior parte do tempo.

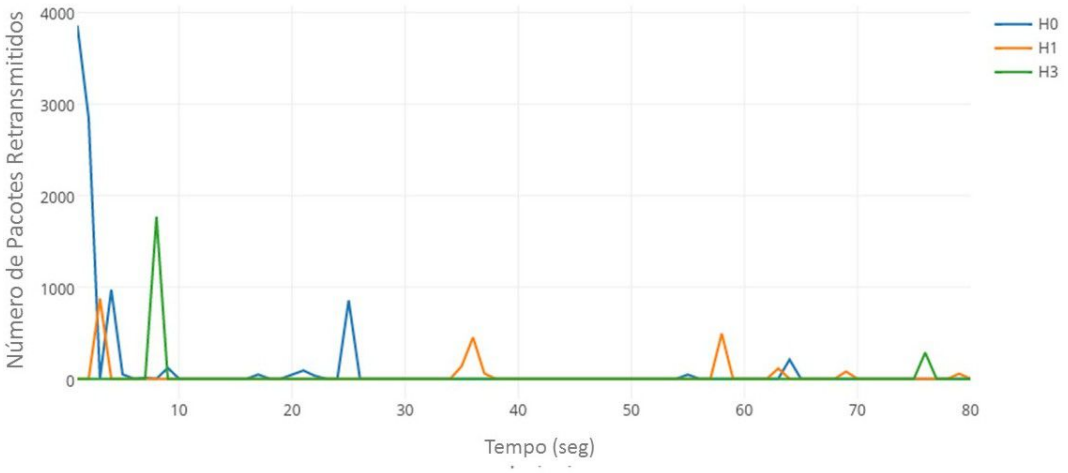
Figura 25 – H1 Retransmissão de Pacotes Topologia Linear II - Distribuído
Fonte: do autor



Na Figura 25 são apresentados os resultados referentes a interações com o host h1. Neste caso, é possível que tanto h2 quanto h3 começaram o experimento com um alto índice de re-

transmissões. H2 entretanto reduziu rapidamente este índice e se manteve estável após isso. Já h3 continuou a apresentar um desempenho ruim, mantendo sempre uma taxa elevada no reenviou dos pacotes. Contudo, h0 teve um bom desempenho, começando com uma taxa de reenvios em torno de 500 pacotes, mas logo em seguida conseguiu estabilizar e continuar com um baixo índice de retransmissões.

Figura 26 – H2 Retransmissão de Pacotes Topologia Linear II - Distribuído
Fonte: do autor

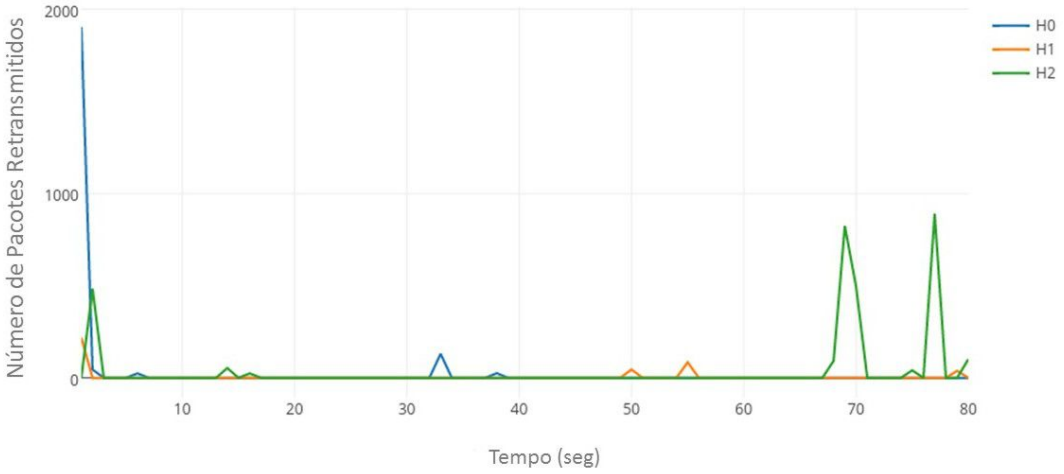


Na Figura 26 é demonstrado o resultado obtido em relação ao tráfego enviado para h2. Neste gráfico, é possível ver que h0 começa com uma taxa muito elevada de retransmissões, em torno de 4000, entretanto com o passar do tempo consegue baixar esta taxa e mesmo havendo mais alguns picos, na maior parte do tempo estava estável. Um comportamento semelhante ocorre para h1 e h3, que apresentam picos próximos a 1000 retransmissões. Em um dos casos h3 supera este número chegando próximo a 2000. Apesar disso, durante o restante do tempo, demonstram um comportamento estável com apenas algumas retransmissões.

Através do gráfico apresentado na Figura 27, é possível notar que durante a maior parte do tempo os hosts possuem um bom desempenho quanto a taxa de retransmissões. Apesar de h0 começar com um número elevado de reenvios, logo eles se normalizam e esta situação se repete para h1 e h2, com todos eles apresentando alguns picos durante a execução. Exceto por h2, que demonstrou alguns picos altos no índice de retransmissões entre os segundos finais do experimento.

Ao final dos experimentos envolvendo a vazão dos hosts, é possível notar que o cenário distribuído apresentou vantagens quanto ao centralizado. No cenário do protocolo UDP conseguiu transmitir um volume maior de dados, enquanto que, no cenário de vazão do protocolo

Figura 27 – H3 Retransmissão de Pacotes Topologia Linear II - Distribuído
Fonte: do autor



TCP, embora também demonstrasse algumas taxas de retransmissões, nenhuma delas superou as taxas envolvidas no cenário da topologia centralizada, onde apenas um ponto da rede ficou com a função de lidar com a sobrecarga de dados durante aquele instante de tempo. Além disso, os gráficos demonstraram um comportamento muito mais linear e estável se tratando do modelo de controle distribuído.

6 CONCLUSÕES

O presente trabalho, contribuiu para o desenvolvimento de um novo conhecimento sobre redes SDN, pois, a partir dos pontos apresentados, demonstra o cenário atual do paradigma SDN, além de contribuir como subsídio para pesquisas voltadas à implementação de redes SDN sob cenários reais. Não tendo a pretensão de alcançar todas as respostas, este trabalho expõem os pontos fortes e os pontos fracos das principais formas de organização do plano de controle no paradigma SDN, realizando uma diferenciação entre cada uma, para ajudar na criação de um novo conhecimento sobre como SDN pode ser empregado e quais suas vantagens e desvantagens em cada caso.

Durante o desenvolvimento deste trabalho, os objetivos propostos foram alcançados, no que se refere à expansão dos estudos relacionados a redes SDN, seus conceitos, organização e características das diversas topologias de implementação, os compromissos na implantação destas redes e discussão a respeito de algumas implantações de sucesso no meio SDN. Com isso, foi possível mostrar o modo de funcionamento destas redes em cada cenário, as vantagens e desvantagens sobre cada um deles e, quais as preocupações que se deve ter ao implantar uma rede SDN. Além disso, foi realizado um estudo sob as formas de distribuição do plano de controle em redes SDN, meios e tecnologias para emular topologias e realizar sua configuração. A partir deste estudo, foi definida a topologia para experimentação e tecnologias utilizadas para a parte prática.

A segunda parte do desafio foi lidar com a emulação destas redes. Primeiramente uma rede de testes (testbed) foi criada conforme as especificações necessárias para atingir os objetivos estabelecidos para esse trabalho. A partir deste ponto, foram desenvolvidos cenários de avaliação sob este ambiente de emulação, considerando as topologias selecionadas. Além disso, os experimentos realizados sob cada um dos cenários, geraram gráficos e tabelas, para demonstrar os dados obtidos.

Os resultados experimentais obtidos indicaram que, apesar dos potenciais benefícios de um plano de controle distribuído em termos de sua resiliência, a responsividade para eventos na rede não é garantidamente melhor que uma abordagem centralizada. Ao recorrer da estratégia distribuída estamos adicionando uma complexidade para o plano de controle, isto é, instâncias de controle deverão ser sincronizadas ao longo da infraestrutura da rede de modo constante, isto para que as decisões tomadas por cada uma delas seja a melhor possível, baseado num estado global da rede. Entretanto, essas comunicações possuem um custo e deve-se ponderar sobre o

compromisso da escolha de um plano distribuído e centralizado de acordo com o tamanho da rede e suas características de tráfego. Para atenuar tais questões sobre o cenário distribuído, uma etapa fundamental é o correto posicionamento das instâncias de controle sobre a topologia da rede, isto é, planejar adequadamente quantas instâncias são necessárias, onde as posicionar e quantos switches cada instância deverá atender simultâneamente.

Por outro lado, também foi possível perceber que apesar dos custos relatados anteriormente, o plano de controle distribuido lida muito melhor com a distribuição de carga na rede. Nas situações diversas que foram experimentadas, o plano de controle centralizado sofreu com severas limitações na sua responsividade e mais, quando na situação de carga intensa, potencialmente levou a perda elevada de pacotes durante as comunicações. Isso claro, sem comentar que o plano de controle centralizado limita o crescimento da infraestrutura de rede e o desempenho no atendimento da comunicação dos hosts presentes na rede.

Embora este estudo forneça os conhecimentos iniciais sobre os compromissos de distribuição de planos de controle, há muitas frentes de pesquisa abertas que podem ser exploradas nesta área. Uma iniciativa que deve ser explorada é a partir da base experimental que foi desenvolvida, isto é, buscar ampliar a capacidade desse ambiente para fazer experimentos com topologias maiores, diversificando assim as possibilidades de avaliações. Outras possibilidades ainda incluem o estudo da implementação do protocolo MPTCP (MultiPath TCP) junto do controlador e switches para possibilitar o uso de múltiplos canais de comunicação (por exemplo: ethernet e wifi) simultâneos para assegurar os pacotes de dados e pacotes de controle, mesmo em situações de perda de conectividade ou comunicações intensas na rede. Por fim, uma terceira frente é a análise de abordagens pró-ativas do plano de controle, isto é, buscar com que ele se antecipe as comunicações que podem vir a ocorrer na rede e já instale as regras antecipadamente.

REFERÊNCIAS

AMAZON. *Amazon Elastic Compute Cloud*. [S.l.]: Amazon, 2017. <https://aws.amazon.com/ec2/>. Accessed: 2017-05-20.

BENSON, T.; AKELLA, A.; MALTZ, D. Unraveling the complexity of network management. In: *Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation*. Berkeley, CA, USA: USENIX Association, 2009. (NSDI'09), p. 335–348. Disponível em: <http://dl.acm.org/citation.cfm?id=1558977.1559000>.

BERDE, P. et al. Onos: Towards an open, distributed sdn os. In: *Proceedings of the Third Workshop on Hot Topics in Software Defined Networking*. New York, NY, USA: ACM, 2014. (HotSDN '14), p. 1–6. ISBN 978-1-4503-2989-7. Disponível em: <http://doi.acm.org/10.1145/2620728.2620744>.

CAI, Z.; COX, A. L.; NG, T. S. E. Maestro: a system for scalable openflow control. In: . [S.l.: s.n.], 2010.

COSTA, L. R. Openflow e o paradigma de redes definidas por software. 2013.

CURTIS, A. R. et al. Devoflow: Scaling flow management for high-performance networks. *SIGCOMM Comput. Commun. Rev.*, ACM, New York, NY, USA, v. 41, n. 4, p. 254–265, ago. 2011. ISSN 0146-4833. Disponível em: <http://doi.acm.org/10.1145/2043164.2018466>.

DOCKER. *DOCKER*. [S.l.]: Linux Foundation, 2016. <https://www.docker.com/>. Acessado em: 2016-11-01.

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. Disponível em: <http://doi.acm.org/10.1145/2602204.2602219>.

GUDE, N. et al. Nox: Towards an operating system for networks. *SIGCOMM Comput. Commun. Rev.*, ACM, New York, NY, USA, v. 38, n. 3, p. 105–110, jul. 2008. ISSN 0146-4833. Disponível em: <http://doi.acm.org/10.1145/1384609.1384625>.

HELLER, B.; SHERWOOD, R.; MCKEOWN, N. The controller placement problem. In: *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*. New York, NY, USA: ACM, 2012. (HotSDN '12), p. 7–12. ISBN 978-1-4503-1477-0. Disponível em: <http://doi.acm.org/10.1145/2342441.2342444>.

HONG, C.-Y. et al. Achieving high utilization with software-driven wan. In: *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*. New York, NY, USA: ACM, 2013. (SIGCOMM '13), p. 15–26. ISBN 978-1-4503-2056-6. Disponível em: <http://doi.acm.org/10.1145/2486001.2486012>.

IPERF. *iPerf - The ultimate speed test tool for TCP, UDP and SCTP*. [S.l.]: Onos Project, 2017. <https://iperf.fr/>. Accessed: 2017-05-29.

ISOLANI, P. H. et al. Uma análise quantitativa do tráfego de controle em redes openflow. *IX Workshop de Gerência e Operação de Redes e Serviços (WGRS)*, 2014.

JAIN, S. et al. B4: Experience with a globally-deployed software defined wan. *SIGCOMM Comput. Commun. Rev.*, ACM, New York, NY, USA, v. 43, n. 4, p. 3–14, ago. 2013. ISSN 0146-4833. Disponível em: <http://doi.acm.org/10.1145/2534169.2486019>.

KOPONEN, T. et al. Onix: A distributed control platform for large-scale production networks. In: *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation*. Berkeley, CA, USA: USENIX Association, 2010. (OSDI'10), p. 351–364. Disponível em: <http://dl.acm.org/citation.cfm?id=1924943.1924968>.

KREUTZ, D. et al. Software-defined networking: A comprehensive survey. *CoRR*, abs/1406.0440, 2014. Disponível em: <http://arxiv.org/abs/1406.0440>.

KUROSE, J. F.; ROSS, K. W. *Computer Networking: A Top-Down Approach (6th Edition)*. 6th. ed. [S.l.]: Pearson, 2012. ISBN 0132856204, 9780132856201.

LANTZ, B.; HELLER, B.; MCKEOWN, N. A network in a laptop: Rapid prototyping for software-defined networks. In: *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*. New York, NY, USA: ACM, 2010. (Hotnets-IX), p. 19:1–19:6. ISBN 978-1-4503-0409-2. Disponível em: <http://doi.acm.org/10.1145/1868447.1868466>.

LANTZ, B.; O'CONNOR, B. A mininet-based virtual testbed for distributed sdn development. *SIGCOMM Comput. Commun. Rev.*, ACM, New York, NY, USA, v. 45, n. 4, p. 365–366, ago. 2015. ISSN 0146-4833. Disponível em: <http://doi.acm.org/10.1145/2829988.2790030>.

LEVIN, D. et al. Logically centralized?: State distribution trade-offs in software defined networks. In: *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*. New York, NY, USA: ACM, 2012. (HotSDN '12), p. 1–6. ISBN 978-1-4503-1477-0. Disponível em: <http://doi.acm.org/10.1145/2342441.2342443>.

MININET. *Mininet*. [S.l.]: An Instant Virtual Network on your Laptop (or other PC), 2016. <http://mininet.org/>. Accessed: 2016-10-30.

MüLLER, L. F. et al. Survivor: An enhanced controller placement strategy for improving sdn survivability. In: *2014 IEEE Global Communications Conference*. [S.l.: s.n.], 2014. p. 1909–1915. ISSN 1930-529X.

NETEM. *NETEM*. [S.l.]: Linux Foundation, 2016. <https://wiki.linuxfoundation.org/networking/netem>. Acessado em: 2016-11-01.

NUNES, B. A. A. et al. A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys Tutorials*, v. 16, n. 3, p. 1617–1634, Third 2014. ISSN 1553-877X.

ONF, O. N. F. A survey on sdn, the future of networking. p. 232–248, 2014.

ONOS. *ONOS*. [S.l.]: Onos Project, 2016. <http://onosproject.org/>. Accessed: 2016-10-29.

Open vSwitch. *Open vSwitch*. [S.l.]: Linux Foundation, 2016. <https://openvswitch.org/>. Acessado em: 2016-10-25.

OPENDAYLIGHT. [S.l.]: Linux Foundation, 2016. <https://www.opendaylight.org/>. Acessado em: 2016-11-03.

REITBLATT, M. et al. Abstractions for network update. In: *Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*. New York, NY, USA: ACM, 2012. (SIGCOMM '12), p. 323–334. ISBN 978-1-4503-1419-0. Disponível em: <http://doi.acm.org/10.1145/2342356.2342427>.

ROSEN, E.; VISWANATHAN, A.; CALLON, R. *Multiprotocol Label Switching Architecture*. 2001. IETF RFC 3031.

ROWSHANRAD, S. et al. A survey on sdn, the future of networking. p. 232–248, 2014.

SPENNEBERG, R. Troque a rota. v. 83, p. 48–51, 2011.

STROWES, S. D. Passively measuring tcp round-trip times. *Commun. ACM*, ACM, New York, NY, USA, v. 56, n. 10, p. 57–64, out. 2013. ISSN 0001-0782. Disponível em: <http://doi.acm.org/10.1145/2507771.2507781>.

TOOTOONCHIAN, A.; GANJALI, Y. Hyperflow: A distributed control plane for openflow. In: *Proceedings of the 2010 Internet Network Management Conference on Research on Enterprise Networking*. Berkeley, CA, USA: USENIX Association, 2010. (INM/WREN'10), p. 3–3. Disponível em: <http://dl.acm.org/citation.cfm?id=1863133.1863136>.

TOOTOONCHIAN, A. et al. On controller performance in software-defined networks. In: *Proceedings of the 2Nd USENIX Conference on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services*. Berkeley, CA, USA: USENIX Association, 2012. (Hot-ICE'12), p. 10–10. Disponível em: <http://dl.acm.org/citation.cfm?id=2228283.2228297>.

VIRTUAL BOX. *Virtual Box*. [S.l.]: Amazon, 2017. <https://www.virtualbox.org/>. Accessed: 2017-05-01.

VISSICCHIO, S.; VANBEVER, L.; BONAVENTURE, O. Opportunities and research challenges of hybrid software defined networks. *SIGCOMM Comput. Commun. Rev.*, ACM, New York, NY, USA, v. 44, n. 2, p. 70–75, abr. 2014. ISSN 0146-4833. Disponível em: <http://doi.acm.org/10.1145/2602204.2602216>.

XIA, W. et al. A survey on software-defined networking. *IEEE Communications Surveys Tutorials*, v. 17, n. 1, p. 27–51, Firstquarter 2015. ISSN 1553-877X.

YAN, L.; MCKEOWN, N. Learning networking by reproducing research results. *SIGCOMM Comput. Commun. Rev.*, ACM, New York, NY, USA, v. 47, n. 2, p. 19–26, maio 2017. ISSN 0146-4833. Disponível em: <http://doi.acm.org/10.1145/3089262.3089266>.

YEGANEH, S. H.; GANJALI, Y. Kandoo: A framework for efficient and scalable offloading of control applications. In: *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*. New York, NY, USA: ACM, 2012. (HotSDN '12), p. 19–24. ISBN 978-1-4503-1477-0. Disponível em: <http://doi.acm.org/10.1145/2342441.2342446>.

Santa Cruz do Sul, 17 de Novembro de 2017

_____

Vinícius Martins de Souza

_____

Prof. Me Lucas Fernando Müller