Pós-Graduação em Ciência da Computação

Edivaldo Cavalcante de Albuquerque Junior

Wi-Flow: Uma Arquitetura baseada em SDN para o Gerenciamento e Mobilidade em redes Wi-Fi com Suporte à Autenticação 802.1x

Dissertação de Mestrado

Universidade Federal de Pernambuco

posgraduacao@cin.ufpe.br

www.cin.ufpe.br/~posgraduacao

RECIFE

2016

Edivaldo Cavalcante de Albuquerque Junior

Wi-Flow: Uma Arquitetura baseada em SDN para o Gerenciamento e Mobilidade em redes Wi-Fi com Suporte à Autenticação 802.1x

Trabalho apresentado ao Programa de Pós-graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Ciência da Computação.

Orientador: *Prof. Kelvin Lopes Dias*

Co-orientador: Prof. Paulo Roberto Freire Cunha

RECIFE

2016

Catalogação na fonte
Bibliotecário Jefferson Luiz Alves Nazareno CRB 4-1758

A245w Albuquerque Júnior, Edivaldo Cavalcante de.
Wi-Flow: uma arquitetura baseada em SDN para o gerenciamento e mobilidade em redes Wi-Fi com suporte à autenticação 802.1x / Edivaldo Cavalcante de Albuquerque Júnior. – 2016.
80 f.: fig., tab.

Orientador: Kelvin Lopes Dias.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn. Ciência da Computação, Recife, 2016.
Inclui referências e apêndice.

1. Redes de computação. 2. Sistemas distribuídos. I. Dias, Kelvin Lopes (Orientador). II. Titulo.

004.6 CDD (22. ed.) UFPE-MEI 2016-152

Edivaldo Cavalcante de Albuquerque Junior

Wi-Flow: Uma Arquitetura baseada em SDN para o Gerenciamento e Mobilidade em redes Wi-Fi com Suporte à Autenticação 802.1x

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação

Aprovado em: 30/08/2016.

BANCA EXAMINADORA

_____

Prof. Dr. Carlos André Guimarães Ferraz
Centro de Informática / UFPE

_____

Prof. Dr. Andson Marreiros Balieiro
Escola Politécnica de Pernambuco / UPE

_____

Prof. Dr. Kelvin Lopes Dias
Centro de Informática / UFPE
(**Orientador**)

Dedico esta dissertação ao meu filho Felipe e minha esposa Ruth Mayara, por seu apoio incondicional. A eles toda minha gratidão, respeito e amor.

Agradecimentos

Primeiramente a Deus toda minha gratidão por me conceder determinação e força nesta jornada.

Agradeço à minha família, meus pais Edivaldo e Verônica e em especial ao meu filho, Felipe e minha esposa, Ruth Mayara, que deram todo o suporte para que eu pudesse me dedicar nos meus estudos e chegar a este momento.

Ao Professor Kelvin Lopes Dias, que confiou em mim desde o primeiro momento, dando-me total tranqüilidade para o desenvolvimento desta dissertação.

Ao amigo, Edson Adriano Avelar, que sempre se prontificou a compartilhar seu conhecimento.

“Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes”.

— MARTHIN LUTHER KING

Resumo

As redes corporativas têm evoluído para um ambiente heterogêneo (rede sem fio e cabeada). Estas redes consideram a autenticação do usuário um elemento primordial para garantir níveis adequados de segurança no acesso aos serviços estratégicos da organização. Nas instituições de ensino e pesquisa, o sistema federado baseado na autenticação 802.1x chamado Eduroam (Education Roaming) permite que estudantes e pesquisadores obtenham conectividade sem fio utilizando as mesmas credenciais de suas instituições em qualquer lugar do mundo com suporte a este sistema. Contudo, a qualidade de serviço (QoS) percebida pelo usuário pode ser degradada quando da necessidade de mudança do ponto de acesso sem fio (handover) devido à mobilidade e necessidade de reautenticação de uma sessão em andamento. Apesar das inúmeras soluções existentes na literatura para o gerenciamento de mobilidade, o suporte à autenticação do usuário no processo de handover é um aspecto negligenciado. Esta dissertação propõe um arcabouço para o gerenciamento integrado de redes cabeadas e sem fio baseado em software de código aberto e de baixo custo. A proposta visa tornar o gerenciamento mais simples e centralizado utilizando o paradigma de redes definidas por software (SDN – *Software Defined Networking*) através do protocolo OpenFlow (OF). Via interface Web é possível obter informações da rede, gerenciar fluxos e controladores OF, criar *slices* de rede e aplicar políticas de QoS. No contexto do gerenciamento de mobilidade, a proposta implementa e avalia uma estratégia de cache de autenticação que otimiza a qualidade de experiência (QoE) durante o processo de *handover* e ambiente com autenticação 802.1x/Eduroam. A avaliação foi realizada num ambiente de experimentação e a proposta obteve como resultados os seguintes ganhos: 15,8% na vazão, 25% no atraso médio e 20,5% no PSNR em relação ao cenário de não utilização da proposta de cache de autenticação. Os resultados obtidos demonstram a aplicabilidade da proposta no gerenciamento mobilidade seguro, bem como sua eficácia no suporte aos requisitos de QoS/QoE para sessões de tráfego de vídeo de usuários móveis.

Palavras Chaves — Gerenciamento de Rede. Eduroam. Handover. OpenFlow. SDN. QoS. QoE.

Abstract

Corporate networks have evolved into a heterogeneous environment (wired and wireless networks). These networks consider user authentication as a key element to ensure adequate levels of security access to the organization's strategic services. In educational and research institutions, the federated system based on 802.1x authentication called Eduroam (Education Roaming) allows students and researchers to gain wireless connectivity using the same credentials of their institutions anywhere in the world that supports this system. However, the quality of service (QoS) perceived by the user can be degraded when they need to change the wireless access point (handover) due to mobility and re-authenticate a session in progress. Despite numerous existing solutions in the literature for mobility management, support for user authentication in the handover process is a neglected aspect. This dissertation proposes a framework for the integrated management of wired and wireless networks based on low cost and open source software. The proposal aims to make simpler and centralized management using the SDN (Software Defined Networking) paradigm via OpenFlow protocol (OF). Through web interface is possible to obtain information from the network, manage flows and OF controllers, create network slices, and apply QoS policies. In the mobility management context, this proposal implements and evaluates a strategy that improves the quality of experience (QoE) environment with 802.1x authentication / Eduroam. In the evaluated experimental environments, the proposed technique achieved gains up to 15.8% on throughput, 25% on average delay and 20.5% on PSNR in comparison to the baseline scenario without authentication cache. Thus, the obtained results demonstrate the applicability of the integrated network management, as well as its effectiveness in supporting of QoS / QoE requirements for video traffic sessions of the mobile users.

Keywords: Network Manager. Eduroam. Handover. OpenFlow. SDN. QoS. QoE.

Lista de Figuras

Lista de Tabelas

Lista de Acrônimos

AAA	Authentication, Authorization and Accounting
AP	Access Point
API	Application Programming Interface
cMAG	Current MAG
CN	Correspondent Node
DDMC	Data-driven Distributed Mobility Control
DHCP	Dynamic Host Configuration Protocol
FHMIP	Fast Handover MIP
HMIP	Hierarchical MIP
IETF	Internet Engineering Task Force
IP	Internet Protocol
LMA	Local Mobility Anchor
MAG	Mobility Access Gateway
MIH	Media Independent Handover
MIP	Mobile IP
MIPv6	Mobile IPv6
MN	Mobile Node
MSU	Video Quality Measurement Tool
NetLMMM	Network-Based Localized Mobility Management
ODL	Opendaylight
OLMA	Openflow Local Mobility Anchor
OMAG	Openflow Mobility Access Gateway
PBA	Proxy Binding Ack
PBU	Proxy Binding Update
PDMC	Partially Distributed Mobility Control
PIS	Proxy Information Server
PMIP	Proxy Mobile IP
PSNR	Peak Signal to Noise Ratio
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SDMC	Signal-driven Distributed Mobility Control
SDN	Software-Defined Networking
SSL	Secure Sockets Layer
TERENA	Trans-European Research and Education Network Association
VLAN	Virtual Local Area Network
VTN	Virtual Tenant network
VQEG	Video Quality Experts Group
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN

Sumário

1

INTRODUÇÃO

Com o aumento do tamanho das redes de computadores e conseqüente incremento na complexidade destas, gerenciamento é uma função cada vez mais crítica para a operação e confiabilidade na execução dos serviços fornecidos pelas redes aos usuários, bem como para o provimento de novas funcionalidades. Diversas corporações e instituições de ensino possuem atualmente uma rede composta por infraestrutura mista (cabeada e sem fio).

A crescente utilização de tecnologias de redes sem fio e o aumento no acesso à Internet vias smartphones, tablets e notebook em qualquer lugar e a qualquer momento, bem como a convergência de várias tecnologias para redes IP, permite cada vez mais que o usuário faça uso de dispositivos móveis para dispor de serviços e aplicações em seu dia-a-dia. Para atender tal demanda, as instituições de ensino têm ampliado a cobertura das redes sem fio, particularmente, baseadas no padrão IEEE 802.11/Wi-Fi (*Wireless Fidelity*), como forma de prover acesso à toda comunidade acadêmica. A ampliação dos pontos de acesso de rede sem fio gera novas questões e desafios quanto ao gerenciamento eficiente e centralizado, bem como ao provimento de vários requisitos atuais, tais como: acesso seguro, continuidade do serviço enquanto o usuário se desloca entre pontos de acesso, denominada de *handover* e também aspectos de Qualidade de Serviço/Experiência (QoS – Quality of Service/QoE – Quality of Experience).

Redes sem fio corporativas consideram a autenticação do usuário um elemento primordial para garantir níveis adequados de segurança no acesso aos serviços estratégicos da organização. Contudo, a qualidade de serviço (QoS) percebida pelo usuário pode ser degradada quando da necessidade de mudança do ponto de acesso sem fio (*handover*) devido à mobilidade e necessidade de reautenticação de uma sessão em andamento. Apesar das inúmeras soluções existentes na literatura para o gerenciamento de mobilidade, o suporte à

autenticação do usuário no processo de handover é um aspecto negligenciado, fazendo com que estes novos requisitos de QoS e QoE não possam ser garantidos.

Outra demanda crescente em redes de produção é o isolamento de trafego, tanto para fins provisionamento de QoS, quanto como forma de criar redes virtuais, hoje pouco flexíveis e, geralmente, implementadas através de VLANs (*Virtual Local área network*). A criação de redes virtuais permite a distribuição de carga, serviços diferentes isolados logicamente e a delegação da administração para desonerar o operador central.

Com o advento do paradigma SDN (Software-Defined Networking) e com penetração cada vez maior no mercado de equipamentos com a tecnologia OpenFlow (OF), tornou-se possível prover soluções inovadoras que possam entregar o gerenciamento de rede flexível, dinâmico e programável, bem como independente de fabricante. A grande evolução oferecida por este paradigma é a programabilidade da rede, que proporciona maior flexibilidade no seu gerenciamento, através de uma visão global da rede, aliado à possibilidade de efetuar a implementação de uma gerencia dinâmica e reconfiguração de políticas de QoS, segurança, virtualização e mobilidade, para citar apenas algumas.

Estas aplicações podem ser desenvolvidas em uma linguagem de propósito geral, viabilizando a inovação e permitindo a implementação de soluções, antes apenas permitidas e implementadas pelos próprios fabricantes.

Nesse contexto, soluções baseada no protocolo IP, que não foram amplamente difundidas pelos fabricantes que utilizam suas próprias soluções fechadas, podem ser redesenhadas considerando os benefícios do emprego do paradigma SDN. Assim a gerencia de mobilidade pode utilizar-se desta filosofia de rede aberta e programável, para viabilizar a implementação de idéias promovidas pela abordagem baseada em NetLMMM (*Network-Based Localized Mobility Management*), tais como PMIP (*Proxy Mobile IP*), onde a gerencia de mobilidade é realizada com a isenção de sinalização nos dispositivos clientes, ficando esta sinalização a cargo do núcleo da rede (Internet Engineering Task Force, 2010). Além disso, as soluções de mercado separam o ambiente de gerenciamento com ferramentas específicas para parte cabeada e para sem fio, o que não permite ter uma visão integrada fim-a-fim para o gerenciamento efetivo da infraestrutura.

Esta dissertação propõe um arcabouço para o gerenciamento Web integrado de redes cabeadas e sem fio, chamado Wi-Flow (*Wi-Fi management based on*

OpenFlow), que tem sua concepção totalmente baseada em software aberto e livre, flexível, de baixo custo, de forma a prover um maior nível de gerencia de rede com menor custo.O Wi-Flow propõe tornar o gerenciamento mais simples e eficaz. Através de uma interface Web, será possível: obter informações sobre os pontos de acesso e switches de rede; gerenciar os fluxos instalados; criar um mapa de rede para todos os elementos instalados na rede; gerenciar aplicações de múltiplos controladores OpenFlow; bem como, criar e remover *slices*[1]da rede e aplicar políticas de QoS sobre a rede virtual criada. No contexto do gerenciamento de mobilidade, a proposta implementa uma estratégia de mobilidade com suporte a autenticação 802.1x e integrado ao serviço Eduroam.

1.1 Objetivo da pesquisa

A seguir, serão apresentados os objetivos gerais e específicos da pesquisa desenvolvida nesta dissertação.

1.1.1 Objetivos Gerais

O objetivo geral é desenvolver um arcabouço centralizado para o gerenciamento de rede com a utilização do paradigma de redes definidas por software, que auxilia o administrador na gerencia de redes complexas, bem como viabilize, através do SDN, a gerência de mobilidade com continuidade de serviço para redes sem fio com suporte à autenticação e integração ao serviço Eduroam.

1.1.2 Objetivos Específicos

a) Implementar estratégia de gerenciamento de mobilidade baseada no paradigma SDN, que considere o *handover* suave entre os pontos de acesso e autenticação 802.1x;
b) Projetar mecanismo para gerencia de fluxos no ambiente web;
c) Elaborar arquitetura web para gerencia de múltiplos controladores Openflow;
d) Propor estratégia para QoS baseado em mecanismos do Openflow1.3;

[1] Fatia de rede física mapeada em uma rede virtual

e) Implementar esquema de criação de redes virtuais através de interface Web.

1.2 Estrutura da dissertação

Esta dissertação está dividida da seguinte forma. O Capítulo 2 apresenta os fundamentos teóricos sobre as tecnologias envolvidas com a proposta. No Capítulo 3 são discutidos os trabalhos relacionados. O Capítulo 4 descreve todo o arcabouço e funcionamento da proposta Wi-Flow. Em seguida, no Capítulo 5, será realizada a avaliação da proposta de gerenciamento de mobilidade. O Capítulo 6 destaca as considerações finais e discute alguns direcionamentos para trabalhos futuros.

2

FUNDAMENTAÇÃOTEÓRICA

Neste capítulo, as tecnologias que deram base ao desenvolvimento da proposta Wi-Flow serão apresentadas. Ele está dividido em quatro subseções. A Seção 2.1 aborda o paradigma SDN e seus componentes essenciais para proposta. A Seção 2.2 disserta o processo de autenticação em redes sem fio, aplicado nesta proposta. Na Seção 2.3 aborda o gerenciamento de mobilidade e os protocolos que foram utilizados para a solução.

2. 1 Redes Definidas por Software

As redes IP tradicionais foram adotadas de forma generalizada como padrão para comunicação de rede, mas apesar de sua grande adoção estas continuam a ser muito complexas para serem gerenciadas (T. Benson et al.,2009).

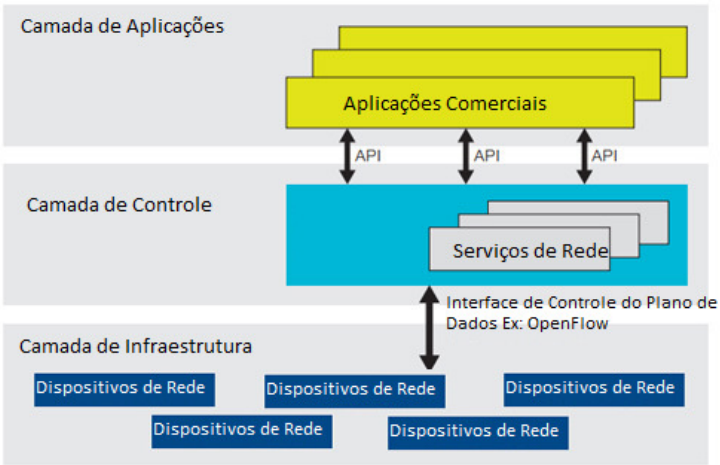
Para o gerenciamento das políticas e execução de otimizações que buscam a melhora no desempenho da rede faz-se necessário que os administradores realizem configurações complexas de baixo nível separadamente em cada dispositivo, muitas vezes de diferentes fornecedores. A complexidade inerente ao gerenciamento das redes IP encontra outro entrave nos requisitos atuais, como resiliência a falhas, adaptabilidade à carga da rede, ambas características providas por mecanismos dinâmicos não presentes nas redes IP, o que torna o gerenciamento das políticas de rede ainda mais desafiador.

Outro desafio para o gerenciamento e evolução das redes, reside na arquitetura atual dos dispositivos de rede, onde o plano de controle, responsável pela decisão de como realizar o encaminhamento de tráfego, e o plano de dados, responsável pelo encaminhamento do tráfego, são implementados internamento nos dispositivos de rede, tornando menos flexível e impedindo a inovação e evolução da rede.

A primeira ação para resolução dos entraves presentes nas redes IP foi a criação do IPv6 e conseqüente transição do IPv4 para o IPv6, mas esta iniciativa além de representar apenas uma atualização do protocolo no qual a maioria dos entraves não serão resolvidos, está em andamento há mais de duas década e ainda continua incompleta.Como evidenciado, um novo protocolo pode levar mais de uma década para ser totalmente desenvolvido e implantado. Já uma abordagem *Clean-slate*[2] voltada para uma mudança na arquitetura da rede de forma a solucionar a chamada ossificação da Internet não se mostra viável (B. Raghavan et al.,2012).

Para resolver o impasse/ossificação da Internet e viabilizar inovação na rede uma das tecnologias mais promissoras foi o paradigma de Redes definidas por Software (SDN -*Software defined Networking*). SDN permite a separação entre os planos de controle e de dados, sendo o primeiro totalmente programável (McKeownet al., 2008). A Figura 2.1 mostra a visão lógica da arquitetura SDN. A inteligência da rede está centralizada na camada de controle, que possui a visão global da rede, o plano de encaminhamento de dados reside dentro dos elementos de rede que compõe a camada de Infraestrutura. Com o SDN, as instituições e as operadoras ganham controle sobre toda a rede, independente do fornecedor, e em um único ponto lógico, o que melhora bastante o gerenciamento da rede.

Figura 2.1 Arquitetura SDN



Fonte: ONF (2012)

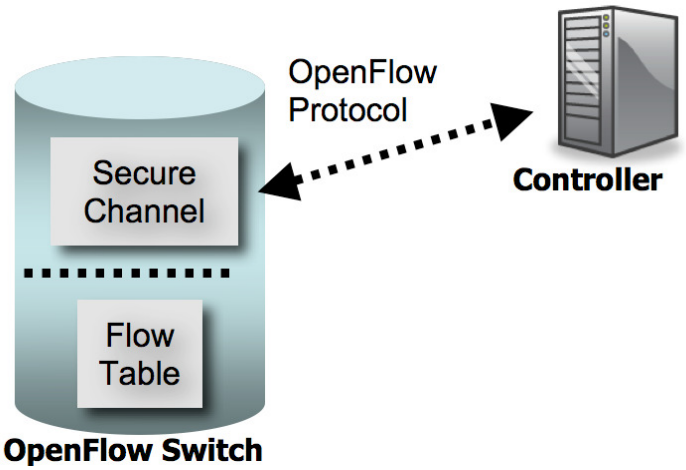
[2] Abordagem que visa substituir totalmente a arquitetura da internet atual por uma nova otimizada e sem compatibilidade com a anterior

2.1.1 OpenFlow

O OpenFlow é um padrão aberto, desenvolvido pela universidade de Stanford (Stanford, 2008), que implementa o conceito SDN. Uma das idéias centrais do protocolo OpenFlow é disponibilizar a plataforma aberta para que qualquer fabricante possa adotá-la. A Figura 2.2 mostra a arquitetura do OpenFlow. Ela é composta de três partes. A primeira consiste na tabela de fluxos, que possui ações bem definidas para cada fluxo. A segunda parte consiste no canal de comunicação seguro que faz a comunicação do switch OpenFlow com o controlador. A terceira parte trata-se do protocolo utilizado nessa comunicação, chamado protocolo OpenFlow.

A tabela de fluxo contém uma listagem de entradas de fluxo. Cada entrada de constante na tabela é composta por campos de correspondência, contadores e ações. Quando um pacote chega ao dispositivo, este é comparado com os campos de correspondência das entradas e caso haja correspondência é verificada a ação prevista esta entrada e atualizado os contadores para manutenção das estatísticas sobre os pacotes. Caso não haja correspondência o pacote pode ser encapsulado e enviado ao controlador para que este possa tomar/definir uma ação para o pacote.

Figura 2.2 Arquitetura OpenFlow



Fonte: OF Spec 1.0 (2009)

2.1.1.1 Especificações OpenFlow

As especificações Openflow descrevem o protocolo aberto para permitir que aplicações sejam desenvolvidas e inseridas nas tabelas de fluxo de dispositivos de diferentes fabricantes. Desde o seu lançamento em março de 2008, foram disponibilizados diferentes especificações do protocolo Openflow. A Tabela 2.1 mostra a evolução das especificações OF 1.0 (OF Spec 1.0, 2009), OF 1.1(OF Spec 1.1, 2011), OF 1.2(OF Spec 1.2, 2011), OF 1.3(OF Spec 1.3, 2012), OF 1.4(OF Spec 1.4, 2013) e OF 1.5(OF Spec 1.5, 2014)

Tabela 2.1 - Comparação de especificações OpenFlow

Funções presentes	Especificações OpenFlow					
	OF 1.0	**OF 1.1**	**OF 1.2**	**OF 1.3**	**OF 1.4**	**OF 1.5**
Flow Table	Única	Múltiplas	Múltiplas	Múltiplas	Múltiplas	Múltiplas
MPLS	NÃO	SIM	SIM	SIM	SIM	SIM
IPv6	NÃO	NÃO	SIM(Básico)	SIM	SIM	SIM
Comunicação simultâneacom múltiplos controladores	NÃO	NÃO	SIM	SIM	SIM	SIM
GroupTable	NÃO	NÃO	NÃO	SIM	SIM	SIM
Meter	NÃO	NÃO	NÃO	SIM	SIM	SIM
Suporte a interfaces de Fibra óptica	NÃO	NÃO	NÃO	NÃO	SIM	SIM
Egress Tables	NÃO	NÃO	NÃO	NÃO	NÃO	SIM

Fonte: O Autor.

2.1.2 Controladores OpenFlow

Um controlador é uma das entidades mais importantes do OpenFlow, ele gerencia o ambiente de rede remotamente de forma centralizada. Na arquitetura OpenFlow, as aplicações que são executadas no controlador são responsáveis por prover a inteligência da rede. O controlador comporta-se como um sistema operacional de Rede onde o mesmo gerencia os seus recursos. Todas as comunicações entre aplicações e dispositivos têm que passar pelo controlador. O protocolo OpenFlow conecta software controlador para dispositivos de rede de modo que o software do servidor pode dizer aos dispositivos de rede para onde os pacotes deverão ser enviados.

O controlador utiliza o protocolo Openflow para manipular a tabela de fluxo dos dispositivos. Para isto o controlador utiliza-se de um canal seguro na comunicação com estes dispositivos e por meio deste, ele é capaz de gerenciar as entradas de fluxo e receber e enviar pacotes para os dispositivos.

Diversos controladores já foram propostos pela comunidade de redes definidas por software. Na Tabela 2.2 são descritos os principais controladores OpenFlow.

Tabela 2.2 - Controladores OpenFlow

Controladores	Linguagem	Documentação	Open Source	Referência
Opendaylight	Java	Muito Rica	Sim	(OpenDayligh, 2013)
ONOS	java	Muito Rica	Sim	(Onos project), 2014)
NOX	C++/Python	Rica	Sim	(Nicira Networks, 2010)
Maestro	Java	Razoável	Sim	(Rice University, 2011)
Trema	C/Ruby	Pobre	Sim	(NEC, 2011b)
Beacon	Java	Boa	Sim	(Stanford University,2011)
Helios	C	-	Não	(NEC, 2011a)
BigSwitch1	Java	-	Não	(Big Switch Networks, 2011)
Floodlight	Java	Muito Rica	Sim	(Big Switch Networks, 2012)

Fonte: O Autor.

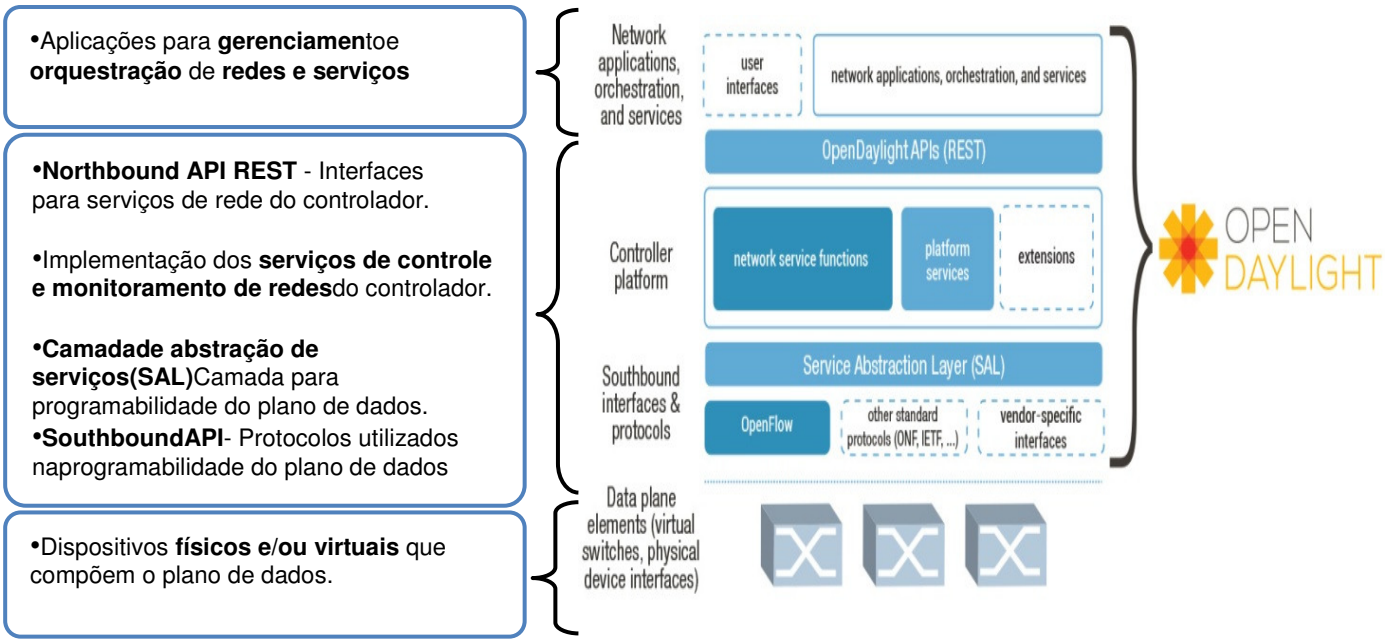
2.1.3 OpenDaylight

Dentre os vários controladores comparados na tabela anterior, será melhor detalhado o controlador Opendaylight pois este foi adotado na proposta.

O opendaylight (ODL) é um controlador SDN desenvolvido em linguagem java e mantido atualmente pela Linux Foundation, uma grande comunidade open-source, e por grandes empresas do segmento de redes. A arquitetura do controlador OpenDaylight é apresentada na Figura 2.3. Nesta é possível verificar a composição baseada em camadas. Na camada superior temos o espaço de aplicações para gerenciamento, orquestração de rede e serviços orientados a modelo de negócio. Na camada central têm-se as *APIs northbound* e *southbound* para uso das aplicações residentes na camada superior, os serviços de controle e monitoramento

da rede do controlador e a camada de abstração de serviços, utilizada para programabilidade do plano de dados. Já a camada inferior consiste nos dispositivos físicos e/ou virtuais que compõem o plano de dados.

Figura 2.3 Arquitetura do ODL

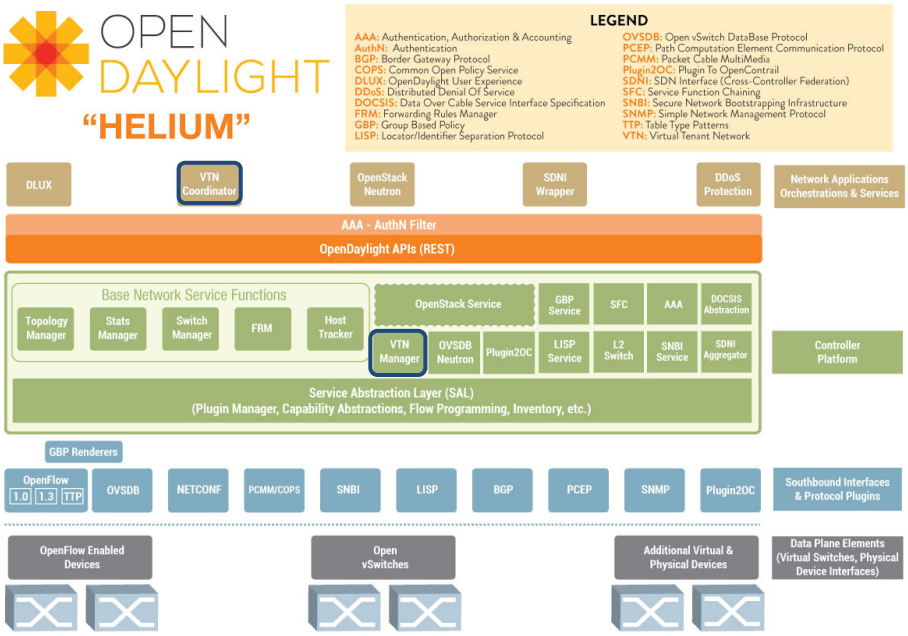


Fonte: Opendaylight User-guide (2015)

Por ser um projeto *opensource*, o Opendaylight inclui muitas contribuições em sua arquitetura. Na camada superior, muitas aplicações estão disponíveis para implementação, entre elas, o projeto *Virtual Tenant Network* (VTN), que propõe a implementação da funcionalidade de virtualização de redes *multi-inquilino* com uso do paradigma de SDN.

Os componentes do projeto VTN visualizados na Figura 2.4 denotam uma integração total com Opendaylight.

Figura 2.4 Componentes VTN do ODL Helium



Fonte: Opendaylight User-guide (2015).

A virtualização, no sentido amplo em computação, é uma estratégia para resolver muitos problemas e criar novos serviços. No caso de virtualização de redes, recursos podem ser divididos em fatias (slices), considerando cada roteador da rede como um elemento que pode ser virtualizado. Assim, um roteador pode executar múltiplas instâncias e, dessa forma, com um único substrato físico a rede pode executar múltiplas redes virtuais.

A virtualização surge para resolver vários problemas, como: escalabilidade, segurança, portabilidade, redução de custos, aumento da eficiência energética, confiabilidade, além de ser apontada como fator de diversificação para o futuro do paradigma inter-redes, que pode contribuir na pesquisa e inovação para resolução do entrave da ossificação da internet (T. Anderson et al., 2005), (J. Turner and D. Taylor, 2005). Isso porque ela desacopla a função executada por um sistema de sua parte física (Chowdhury et al., 2010). A virtualização de redes pode ser alcançada através de várias formas, utilizando máquinas virtuais como roteadores ou programação de redes, como é feito com o OpenFlow (N. McKeownet al., 2008).

Em uma rede convencional, há um enorme investimento no sistema de rede, aliado a uma gama de despesas operacionais, por ocasião da implantação de cada departamento de uma empresa. Tais investimentos são necessários para que o inquilino (departamento) tenha o isolamento, segurança e confiabilidade necessária

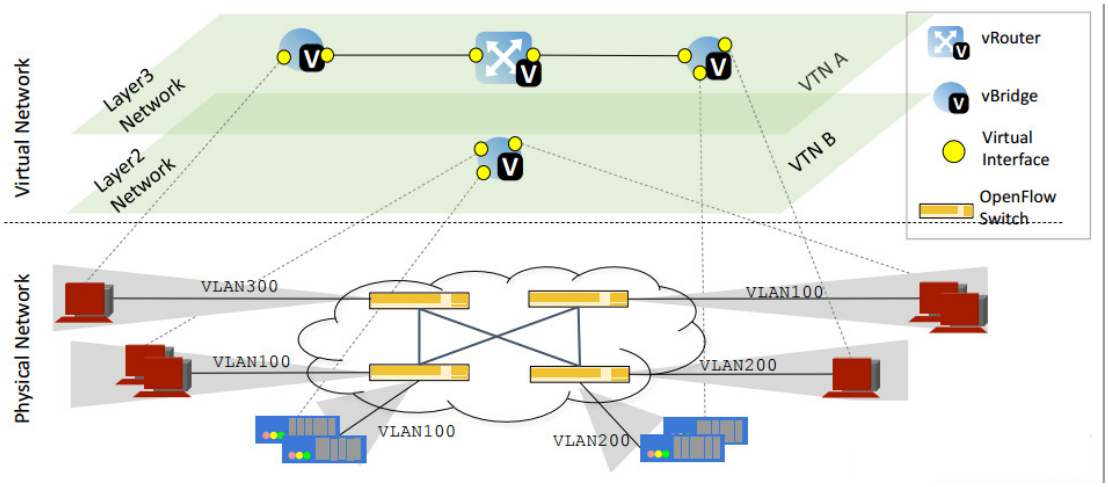
no uso da sua rede, o que gera tarefas de grande custo, como a operação de sistemas de rede complexas.

Neste contexto a aplicação *Virtual Tenant Network* (VTN) busca ofertar características como escalabilidade, segurança, portabilidade, redução de custos, aumento da eficiência energética, confiabilidade com a separação completa do plano lógico do substrato físico em redes multi-inquilinos (Opendaylight User-guide, 2015). Com o uso da VTN os usuários podem criar e implantar qualquer rede lógica sem o conhecimento da topologia da rede física. Uma vez definida uma nova VTN, esta é mapeada automaticamente no substrato físico, como visto na Figura 2.5. Este mapeamento se dá com a utilização da inserção de regras de fluxo nos ativos de rede pelo controlador SDN.

A utilização de VTN não só permite a abstração da complexidade da topologia do substrato físico, mas permite uma melhor gerencia dos recursos da rede, de forma a tornar a tarefa de gerenciamento mais simples, minimizando erros de configuração e reduzindo o tempo para reconfiguração de serviços de rede.

Além disso, neste ambiente, pode ser oferecido o gerenciamento para serviços fim-a-fim de forma personalizada dentro da infra-estrutura compartilhada (N.M.M.K. Chowdhury et al., 2009).

Figura 2.5 Mapeamento de VTN do em substrato Físico



Fonte: Opendaylight User-guide (2015).

Pelas características citadas anteriormente e após analisar e comparar as funcionalidades dos principais controladores do mercado, como suporte a alta disponibilidade, *clustering*, segurança e suporte a arquitetura distribuída, foi

escolhida a versão Helium-SR2 do Opendaylight para implementação da proposta desta dissertação.

2. 2 Autenticação em redes Wi-Fi

As redes sem fio são utilizadas para diversos fins, entre eles o acesso á Internet tem sua demanda largamente ampliada devido à proliferação de dispositivos móveis, como smartphones, notebooks e tablets. O crescimento do uso destes equipamentos deve-se a facilidades como mobilidade e portabilidade. O primeiro inerente a utilização da tecnologia sem fio e o segundo inerente aos dispositivos moveis que são facilmente portados por seus usuários.

A flexibilidade inerente ao meio sem fio e o crescente uso deste fez com que aspectos como autenticação, autorização e contabilização (AAA) cada vez mais fossem requisitos essenciais para um uso da tecnologia de forma segura.

No contexto da comunidade acadêmica, serviços de federação, como a iniciativa Eduroam, utilizam-se de uma estrutura de Proxy de autenticação para prover acesso seguro a usuários acadêmicos de diferentes instituições, colaborando para o aumento da facilidade no acesso a rede sem fio sem onerar aspectos de segurança.

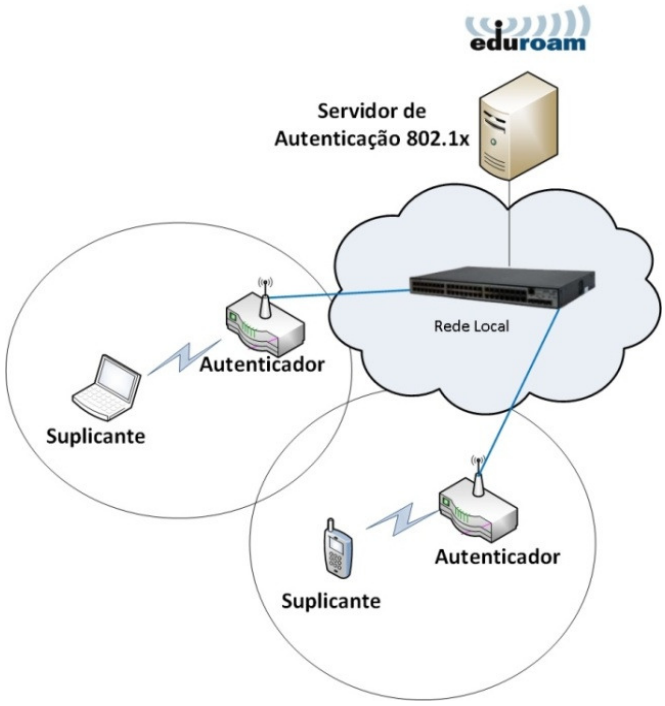
2.2.1 Eduroam

O Eduroam (*education roaming*) é um serviço de acesso sem fio seguro, desenvolvido pela TERENA (T*rans-European Research and Education Network Association*) para a comunidade internacional de educação e pesquisa. A iniciativa permite que estudantes, pesquisadores e as equipes das instituições participantes obtenham conectividade à Internet através de conexão sem fio (Wi-Fi), dentro de seus campi e em qualquer localidade que ofereça essa facilidade como provedora de serviço. Eduroam é baseado no protocolo IEEE802.1X (IEEE, 2006) e usa servidores proxy RADIUS (Rigneyet al. 2000) hierarquicamente estruturados. Este serviço proporciona o meio de autenticação e autorização seguro de forma a prover confiabilidade e segurança no aceso a redes sem fio.

2.2.2 IEEE 802.1X

O arcabouço de autenticação IEEE 802.1X, é um mecanismo para controle de acesso à rede baseado em porta(IEEE, 2006).O 802.1X descreve três entidades principais utilizadas para prover o funcionamento do protocolo, as quais são o suplicante, autenticador, e servidor de autenticação. O suplicante, no contexto das redes sem fio, são os *mobile nodes* (MN); O autenticador é representado pelo ativo de conexão, por exemplo, o ponto de acesso, roteador. Por fim, o servidor de autenticação, que neste caso será servidor RADIUS (Remote Authentication Dial In User Service), é o responsável por prover serviço de Autenticação, Autorização e Auditoria de forma a garantir a confiabilidade do acesso. Na Figura 2.6 são apontadas as entidades e arquitetura de autenticaçõa 802.1X/Eduroam.

Figura 2.6 Arquitetura 802.1X/Eduroam

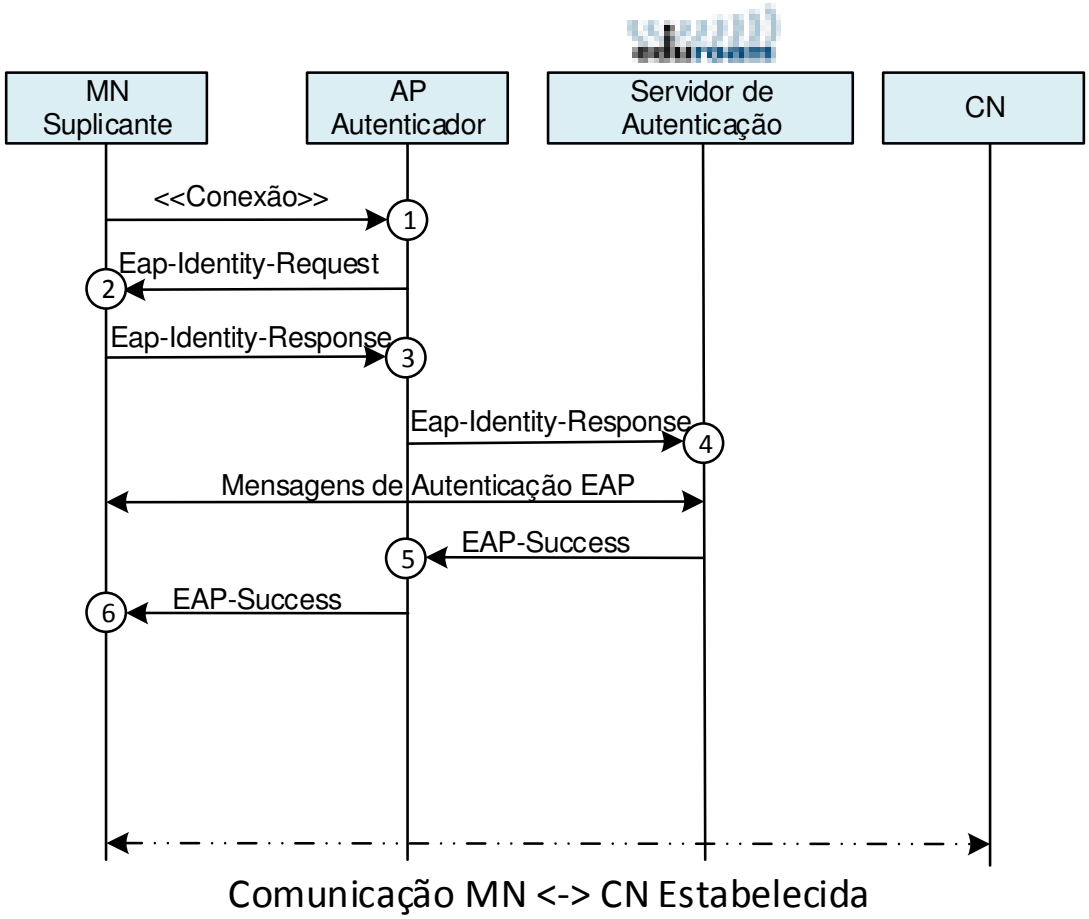


Fonte: O Autor.

A Figura 2.7 mostra o funcionamento do Arcabouço 802.1X. No passo 1 o suplicante solicita ao autenticador acesso à rede. O autenticador, que controla a porta de acesso a rede, recebe a solicitação e no passo 2 solicita as credenciais de acesso. No passo 3 o suplicante envia as credenciais de acesso à rede e o autenticador direciona as mensagens 802.1X para o servidor de autenticação no

passo 4. No passo 5 o servidor de autenticação autoriza ou não o acesso baseado nas credencias informadas, repassadas pelo autenticador e rertona mensagem de acesso aceito ou rejeitado ao autenticador, que diante desta mensagem realiza no passo 6 o repasse da mensagem do servidor de autenticação e executa ou não a comutação da porta controlada. No 802.1X, a porta controlada representa a associação entre o suplicante e o autenticador. Iniciamente, esta porta está no estado não autorizada. Após a autenticação com êxito do suplicante, é realizado o fechamento da porta controlada, acesso é provido e o suplicante se comunica com o CN(Correspondent Node).

Figura 2.7 Autenticação 802.1X



Fonte: O Autor.

2. 3 Gerenciamento de Mobilidade

Apesar da vastíssima literatura sobre gerenciamento de mobilidade nas diversas camadas da pilha TCP/IP (*Transmission Control Protocol/Internet Protocol*) (Akyildizet al., 2014), serviços que usufruam efetivamente da mobilidade IP ainda não são difundidos nas redes de acesso sem fio de provedores e operadoras. Um dos grandes entraves à penetração de serviços móveis decorre das constantes otimizações e alterações na pilha de protocolos que devem estar presentes nos dispositivos dos usuários que desejam usufruir da mobilidade entre diferentes pontos de acesso ou coberturas sem fio, bem como da excessiva sinalização na interface aérea requerida pelos protocolos atuais.

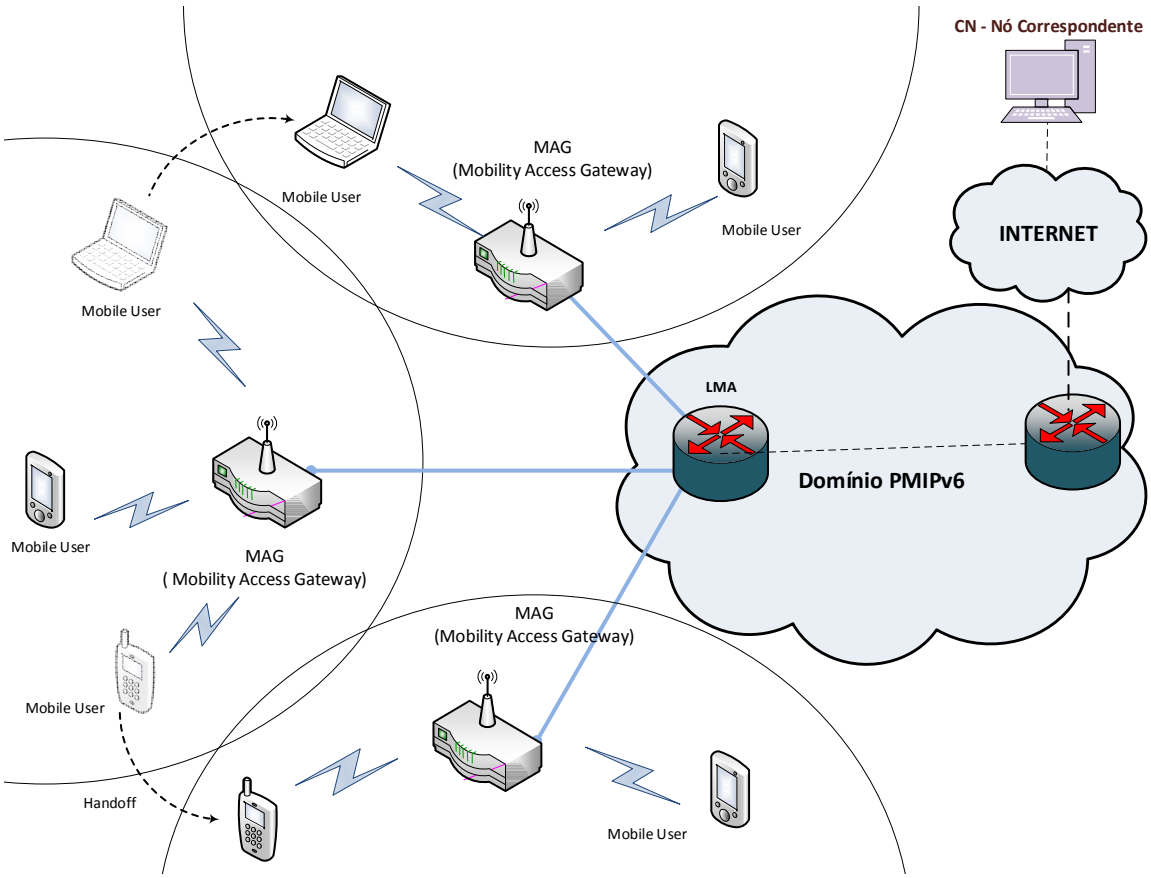
Na maioria das soluções de mobilidade baseadas no terminal, o dispositivo móvel necessita de mudanças para o funcionamento do protocolo de mobilidade. Os protocolos MIPv4, MIPv6, HMIP, FMIPv6, FHMIP entre outros necessitam que o terminal móvel adicione funcionalidades não nativas. Soluções desse tipo aumentam a participação do terminal no processo de mobilidade, o que gera um *overhead* extra de sinalização do dispositivo, o qual, muitas das vezes, é restrito ao uso de energia. Os problemas decorrentes do MIPv6 e suas variações (necessidade hardware especializada, arquitetura com ponto único de falha e necessidade do uso do IPv6) e a demanda por um protocolo que permitisse o gerenciamento de mobilidade baseada na rede, e não baseada no dispositivo móvel, motivou o desenvolvimento do protocolo do PMIPv6 (Proxy Mobile IPv6), padronizado pelo grupo de trabalho NETLMM (Network-based Localized Mobility Management) do IETF (Gundavelli et al., 2008), que diferentemente dos protocolos existentes para o gerenciamento de mobilidade IP, delega à rede a responsabilidade de executar o procedimento de handover.

O PMIPv6 disponibiliza o gerenciamento de mobilidade através de uma arquitetura baseada em um domínio PMIPv6. Este domínio é composto por duas entidades, o LMA (Localized Mobility Anchor), responsável pela disponibilidade do serviço de mobilidade, e o MAG (Mobility Access Gateway), tem a função de detectar a chegada de um Nó Móvel (MN) e realizar os procedimentos necessários para oferecer a mobilidade a este usuário.

Na comunicação com dispositivos externos ao domínio PMIPv6, todas as mensagens enviadas pelo Nó Móvel com destino ao Nó Correspondente(CN) passam pelo LMA de forma a este realizar o controle em caso de mobilidade do nó.

Na Figura 2.8 é possível verificar os dispositivos que arquitetura PMIPv6 e as funções desempenhadas no gerenciamento de mobilidade do protocolo.

Figura 2.8 Visão Geral do PMIPv6



Fonte: O Autor.

3

TRABALHOS RELACIONADOS

Este capítulo apresenta os trabalhos relacionados ao Wi-Flow. Ele está dividido em quatro subseções. A Seção 3.1 mostra alguns trabalhos relacionados ao gerenciamento de redes com SDN. A Seção 3.2 aborda artigos sobre gerenciamento de mobilidade em redes OpenFlow. Na Seção 3.3 são discutidos os trabalhos que abordam soluções para virtualização de rede. Na Seção 3.4 são apresentas as considerações finais deste Capítulo.

3.1 Gerência de Redes com OpenFlow

A solução proprietária de gerenciamento proposta pela fabricante Extreme denominada SDN Extreme, é baseada em uma versão do controlador OpenDaylight modificado pelo processo de Hardening[3] para conferir mais segurança ao controlador. A solução proposta visa ser uma plataforma de gerenciamento abrangente para toda a rede, incluindo sem fio, cabeada e centro de dados. Dentre as funcionalidades descritas estão o gerenciamento de mobilidade em redes sem fio, gerenciamento de rede cabeada, segurança baseado em controle de acesso a rede e aplicações de analise e monitoramento da rede (Extreme SDN Platform, 2016).

A solução apresenta boas idéias, mas como outras proprietárias mantêm elevador valor de aquisição, o que dificulta sua adoção. Já no contexto da pesquisa e inovação, mesmo guardando conceitos de arquiteturas abertas, como definida no paradigma SDN, a solução em sua essência mantém o seu perfil proprietário.

[3] Técnica usada para mapeamento de ameaças e vulnerabilidade e posterior inclusão de possíveis correções nos sistemas, preparando-os para determinadas tentativas de ataques.

A fabricante Brocade propõe o gerenciamento de redes SDN com a utilização do Brocade Controlador SDN (anteriormente chamado de controlador Vyatta). O Controlador SDN é uma versão comercial do controlador Opendaylight, adicionando aplicações prontas para o gerenciamento de redes virtuais, fluxos, funções de redes virtualizadas de forma a ajudar as instituições a diminuir a complexidade e reduzir os riscos operacionais (Brocade Controlador SDN, 2016).

A solução apresentada pela Brocade entrega uma interface Web que simplifica o gerenciamento de rede, pois oferece ferramentas para controle de fluxo, virtualização de redes, visualizador da topologia de rede, entre outros. Apesar de importante, entre os pontos negativos estão o alto custo de aquisição, pois trata-se de uma solução proprietária e a não entrega do gerenciamento de rede pleno, pois além de não contemplar a gerencia para redes sem fio e suporte à mobilidade, requisitos estes essenciais nas redes atuais, também não dá suporte ao gerenciamento de QoS, item importante para a entrega de uma melhor qualidade de experiência ao usuário final.

A solução proposta em (Huawei controlador Agile, 2016), visa prover o gerenciamento de redes com utilização do paradigma de SDN, de forma a disponibilizar uma rede flexível e de fácil administração. Para tanto a plataforma do controlador Agile fornece uma interface de gerenciamento, pela qual, é possível realizar o gerenciamento das redes virtuais, criação de regras fluxos, gerenciamento de redes sem fio e cabeadas de forma centralizada, controle de acesso baseado em usuários e dispositivo e gerenciamento de qualidade de serviço. No contexto das políticas de Qualidade de Serviço (QoS), segundo o fabricante, elas são configuradas atualmente de forma estática, não podendo adaptar-se a mudanças de localidade do usuário, ficando este sem a possibilidade de aliar prioridade de QoS ao serviço de mobilidade. Assim, o controlador Agile propõe que recursos e políticas de rede devem ser capazes de se reconfigurarem de forma a alocarem recursos e implementarem políticas dinamicamente durante migração dos usuários, de forma a manter a qualidade de experiência deles. No gerenciamento de redes heterogêneas, como as redes cabeada e sem fio, a proposta relata que para total integração no gerenciamento, as controladoras de rede sem fio serão descartadas e com uso da programabilidade inerente ao SDN, os pontos de acesso sem fim serão controlados pelos próprios switches de acesso. Para tanto, o controlador SDN Agile utiliza CAPWAP para se comunicar com switches de acesso. Isso permite que os pacotes

trocados entre o controlador e switches de acesso Agile possam atravessar dispositivos e redes de diferentes fornecedores de comutação, proporcionando flexibilidade na implantação da rede e também facilitando a implementação de convergência com e sem fio. As funcionalidades propostas pelo fabricante apontam para qualificar o controlador Agile como o mais completo das soluções analisadas, mas mesmo com todos estes benefícios, verificou-se que o custo de aquisição desta solução configura um grande impeditivo a ser avaliado. Outro ponto é que a fabricante também fecha a solução de forma a dificultar a pesquisa e inovação de maneira flexível, ficando o usuário restrito as aplicações desenvolvidas pelo fabricante.

3.2 Gerenciamento de Mobilidade

Esta subseção abordará trabalhos relacionados ao gerenciamento de mobilidade.

Em (Tantayakulet al., 2016) é proposto o gerenciamento de mobilidade baseado na rede com a utilização do paradigma de SDN. Na proposta (SDN Mobility), os autores defendem a não utilização de uma implementação baseada em protocolos legados como o PMIP e sim uma estratégia puramente baseada em SDN, que pode utilizar uma de suas características, a visão global da rede, para tratar e encaminhar fluxos de forma a entregar o serviço de mobilidade. Para avaliação da proposta foi criado um cenário emulado e realizado comparativo entre PMIPv6 padrão e a solução proposta, demonstrando ao fim que a solução SDN Mobility é mais vantajosa em termo de perdas de pacotes. Durante o processo de handover a proposta teve em medias duas vezes menos perdas de pacote que a implementação do PMIPv6. Um ponto observado é que para emulação da rede foi utilizado o mininet, aplicação que só prover suporte a redes cabeadas, não sendo, portanto, ideal para testes envolvendo mobilidade. Para simular o movimento dos MNs foi desenvolvido um código para realizar a conexão e desconexão do nó nos switches do mininet.

Em (Obele and Kang, 2009) é proposta uma arquitetura para handover proativo e com suporte gerenciamento de QoS fim a fim. Esta arquitetura é baseada em um servidor de informações, PIS (*Proxy Information Server*), que é consultado pelos ativos da rede a fim de auxiliar na mobilidade do terminal móvel. Para tanto, quando o cMAG (*current MAG*) verifica que o nível de sinal do terminal do usuário, MN (*Mobile Node*), está caindo, ele executa de forma proativa o procedimento de *handover*. Este processo consiste no envio de uma mensagem PBU (*Proxy Binding Update*) ao LMA (*Local Mobility Anchor*) que por sua vez realiza um consulta ao servidor PIS e de posse das informações obtidas realiza o *handover*. Com o inutuito de reduzir o tempo de migração do MN entre os MAGs, a sinalização de *handover* é enviada antes do MN realizar a migração efetivamente para outro MAG. As informações sobre QoSos requisitos de QoS do MN, são enviadas do MAG para o LMA por meio de mensagem PBU.

A proposta é comparada matematicamente com o PMIPv6 padrão usando as métricas tempo de handover em comparação ao atraso do enlace sem fio. Alguns pontos importantes não foram clarificados explicados neste trabalho. Por exemplo, os autores não apontam como o PBU foi alterado de forma a incluir informações referentes à Qualidade de serviço. Além disso, menciona-se a mensagem link going down do MIH (Media-Independent Handover), porém não é descrito como o framework foi inserido na proposta.

Em (Taghizadeh et al., 2011) os autores comparam quatro cenários na implementação do PMIPv6 intra e inter domínio: single domain, Hierarchical Multi-domain, Peer Multi-*Domain* e I-PMIP. As propostas são avaliadas pelo fator de latência de *handover,* adotando de modelos matemáticos. Os parâmetros variáveis utilizados são: distância entre o LMA e o MAG, distância entre os MAGs e as redes vizinhas e probabilidade de falha no meio sem fio. Os resultados da avaliação numérica apontam como proposta mais vantajosa a Peer Multi-domain, por suas características que lhe conferem grande potencial de ser implementado de modo distribuído.

No artigo (Kim et al., 2011) os autores denotam que a maioria dos protocolos de mobilidade são centralizados e com o crescimento do número de dispositivos conectados, estes protocolos deveriam possuir arquitetura distribuída. No artigo são propostos três alternativas de protocolos de gerenciamento de mobilidade, o PDMC

(*Partially Distributed Mobility Control*), o DDMC (Data-*driven Distributed Mobility Control*) e o SDMC (*Signal-driven Distributed Mobility Control*).

Na avaliação, estes protocolos são comparados com o PMIP em termos de *binding update* e custo de entrega de pacotes. Os resultados denotam que as três propostas distribuídas são melhores que a proposta centralizada do PMIP, e dentre todas, a melhor foi a SDMC.

Um ponto importante sobre esta avaliação é que, mesmo sendo uma comparação numérica importante, seria mais adequada a comparação com extensões do PMIP que permitam abordagem distribuída, como a versão vista em (Taghizadeh et al., 2011).

Em (Yapet al., 2010a) os autores discutem como as redes sem fio são fechadas e sem inovação e de certa forma parada no tempo. No artigo não é fornecido uma proposta para melhorar o *handover* com o uso do paradigma de SDN. Os autores admitem a existência de desconexão no *handover*, ficando as correções do problema por conta do desenvolvedor, onde este deverá criar aplicações NOX para gerenciamento de mobilidade.

O trabalho proposto em (Avelar, 2013) visa o provimento do gerenciamento de mobilidade com o uso do paradigma de SDN. Na proposta o autor baseia-se no protocolo PMIPv6 para criar o PMIPFlow, protocolo criado para realizar o gerenciamento de mobilidade baseado rede, de forma a não onerar o cliente no uso da mobilidade. No PMIPFlow o autor propõe também um mecanismo de antecipação de handover baseado em lógica fuzzy, que na avaliação executada mostrou-se muito efetiva na diminuição das quedas de conexões durante a troca de pontos de acesso. Apesar de sua contribuição, o PMPFlow como outras iniciativas também não trabalham aspectos de segurança e suporte a autenticação, requerimentos indispensáveis na entrega do serviço de rede sem fio nos dias atuais. Contudo, na implementação proposta, os pontos de acesso precisam embarcar parte do protocolo para desempenhar as funções especificas para o provimento da mobilidade. Outro pronto de entrave é que para implantação do protocolo Openflow nos pontos de acesso, foi utilizada uma versão de software switch que é executado no espaço do usuário, o que contribui para um desempenho ruim, em relação a vazão máxima, como visto na avaliação da proposta.

Esta seção discutiu os trabalhos relacionados ao Wi-Flow como forma de denotar a relevância desta proposta. Primeiramente, foram abordados artigos sobre o gerenciamento de mobilidade, porém nenhum deles propõem uma arquitetura que consolide o gerenciamento da mobilidade e o gerenciamento da qualidade de serviço e o uso do paradigma de SDN juntos.

Um dos pontos fundamentais deste trabalho, o uso de mecanismos de autenticação juntamente com a mobilidade, não é abordada em nenhum trabalho, apontando-se como uma lacuna importante a ser contornada. Desta forma, o provimento do gerenciamento da mobilidade com suporte a autenticação desta proposta contribui para a resolução deste entrave, de conciliar aspectos de segurança com gerencia de mobilidade.

3.3 Virtualização de Redes

Esta subseção abordará trabalhos relacionados ao estado da arte em virtualização de redes.

Em (R. Sherwood et al., 2009) os autores propõe o uso de um framework, chamado FlowVisor para o gerenciamento da virtualização de redes, de forma a agregar os benefícios inerentes a tecnologia de virtualização de redes, como prover as funcionalidades de isolamento da rede, priorização de serviços e facilidade de gerenciamento, por exemplo. Os autores apontam que FlowVisor é um controlador OpenFlow especial que atua como um proxy entre múltiplos controladores e os ativos openflow de forma a criar slices de recursos na rede e delegar cada slice para um controlador diferente.

Apesar de ter representado grande avanço para virtualização de redes com uso do paradigma SDN, o FlowVisor foi limitado a versão 1.0 da especificação do protocolo OpenFlow. Dessa forma, ele não trata novos *match* presentes nas versões atuais do protocolo OpenFlow, inclusive campos relacionados ao suporte a QoS não podem ser utilizados. Ainda em suas limitações, o FlowVisor tem uma arquitetura pouco escalável e que matem no próprio FlowVisor um ponto central de falha, onde caso este pare de funcionar todos os controladores e redes virtualizadas ficam

inacessíveis. A falta de atualização, sua arquitetura centralizada, que não leva em conta as redes distribuídas e a falta de suporte as novas versões do Openflow, foram pontos que levaram a sua descontinuação e o desenvolvimento de outras soluções, como o VTN empregado nesta proposta.

A proposta de (Nakauchi et al., 2011) é a utilização de uma plataforma de virtualização de redes cognitivas, denominada AMPHIBIA. Esta plataforma permite o gerenciamento de redes virtuais em ambientes heterogêneos, como redes sem fio e cabeadas. Esta funcionalidade permite a criação de slices fim-a-fim sobre o substrato físico de redes com e sem fio. O modelo descrito no artigo é bem completo, mas nenhuma avaliação foi realizada para comprovar sua eficácia. Apesar de proposto para redes heterogêneas, os autores apontam que as funcionalidades para o meio sem fio ainda não estão prontas. Dessa forma, o suporte fim-a-fim com QoS não pode ser empregado em sua totalidade.

Em (Yamasaki et al., 2011) os autores dissertam que as redes CAN (*campus area network*) utilizam VLANs (Virtual Local Area Network) para dispor de sua separação lógica. O uso deste mecanismo tem se tornado complexo à medida que as redes aumentam para atender a demanda crescente pelos recursos de rede. Neste contexto onde a complexidade da rede representa uma entrave para a segmentação baseada em VLANs, os autores buscam no paradigma de SDN uma solução que alie a programabilidade do Openflow com as VLANs tradicionais para criar um sistema escalável e fácil de configurar mesmo em redes complexas. O sistema pretendido transfere os conceitos das VLAN tradicionais para uma aplicação OpenFlow, as tags do 802.1Q são substituídas por GIDs (Group IDs), e a entidade gerenciadora de acesso, o AMF (Access Management Function), gerencia e controla o acesso dos usuários com o uso dos IDs de Grupo.

Na Tabela3 são sumarizadas as principais funcionalidade encontradas em cada trabalho e analisado e suas convergências e divergências em relação a proposta.

Tabela 3.1 Trabalhos Relacionados

Proposta	Finalidade	Ambiente de Avaliação	Interface de Gerenciamento de rede	Suporte à QoS	Suporte à Autenticação	Interface de Gerenciamento de rede Web	Controlador SDN	Gerenciamento de mobilidade	Virtualização de Redes	Custo da Solução
(Avelar, 2013)	Gerenciamento de mobilidade em SDN com antecipação de Handover.	WF	X	X	X	X	NOX	MM	X	BAIXO
(Brocade Controlador SDN, 2016)	Propõe o gerenciamento de redes com o uso da paradigma SDN, de forma a diminuir a complexidade e reduzir os riscos operacionais.	NA	IW	X	X	IW	ODL	X	GV/SV	ALTO
(Extreme SDN Platform, 2016)	Solução de gerenciamento baseado em controlador SDN e aplicações customizadas pela fabricante.	NA	IW	X	X	IW	ODL	MM	GV/SV	ALTO
(GT SciFi, 2012).	Gerenciamento Centralizado de pontos de acesso sem fio.	WF	IW	X	X	X	NUS	X	X	BAIXO
(Huawei controlador Agile, 2016)	Prover o gerenciamento de redes heterogêneas com utilização do paradigma de SDN.	WM	X	QO	X	IW	ODL	MM	GV/SV	ALTO
(Kim et al., 2011)	Comparação das emprego de propostas distribuidas para gerenciamento de mobilidade.	AM	X	X	X	X	NUS	MM	X	BAIXO
(Nakauchi et al., 2011)	Gerenciamento de redes virtuais em ambientes heterogêneos, com suporte a QoS e criação de slices fim-a-fim.	NA	X	QO	X	X	NUS	X	SV	BAIXO

(Obele and Kang, 2009)	Arquitetura para handover proativo e sensível à QoS.	AM	X	QO	X	X	NUS	MM	X	BAIXO
(R. Sherwood et al., 2009)	FlowVisor - Framework para gerenciamento de virtualização de redes com o uso do paradigma de SDN.	RC/WF/WM	X	X	X	X	FL/NOX	X	SV	BAIXO
(Taghizadeh et al., 2011)	Comparação de propostas PMIPv6 intra e inter domínio: single domain, Hierarchical Multi-domain, Peer Multi-Domain e I-PMIP.	AM	X	X	X	X	NUS	MM	X	BAIXO
(Tantayakul et al., 2016)	Gerenciamento de mobilidade baseado em SDN.	EM	X	X	X	X	RYU	MM	X	BAIXO
(Yamasaki et al., 2011)	Transfere os conceitos das VLAN para uma aplicação OpenFlow, as tags do 802.1Q são substituídas por GIDs, visando Gerenciar o acesso dos usuários com o uso dos IDs de Grupo.	RC/WF	X	X	1X/ED	X	NEC	X	SV	BAIXO
(Yap et al., 2010a)	Proposta de utilização de aplicações NOX para o gerenciamento de mobilidade.	WM/WF	X	X	X	X	NOX	MM	X	BAIXO
Solução proposta	Uma Arquitetura baseada em SDN para o Gerenciamento e Mobilidade em redes Wi-Fi com Suporte à Autenticação 802.1x.	WF	IW	QO	1X/ED	IW	ODL	MM	GV/SV	BAIXO

WF: 802.11 (WiFI)	GV: Gerenciamento de Virtualização Web	COD: CPqD OpenFlow1.3 softswitch e dpctl
RC: Rede cabeada	SV:Suporte a Virtualização de Redes	CI: Controlador interno do NS3
EM: Emulador	IW: Interface Web Para Gerenciamento	NOX: Controlador NOX
SM: Simulador	1X: Suporte a 802.1X	RYU: Controlador RYU
AM: Análise matemática	ED: Integração ao Eduroam	ODL: Controlador *OpenDayLight*
WM:Wimax	QO: Suporte à QoS	NUS: Não utiliza SDN
OF: Protocolo OpenFlow		FL:Flowvisor
MM:Suporte à Mobilidade	X: Não Possui	NEC Openflow Controller

3.4 Considerações Finais

Esta seção discutiu os trabalhos relacionados ao Wi-Flow, como forma de denotar a relevância da proposta.

Primeiramente, foram abordados alguns artigos sobre o gerenciamento de redes e os trabalhos que se utilizam do paradigma de SDN para implementar a gerencia de redes. Foram apresentados também, alguns trabalhos que abordam gerenciamento de mobilidade em redes definidas por software, porém nenhuma delas propõe uma arquitetura com base num protocolo de mobilidade padronizado e suporte a autenticação 802.1X, não apresentam nenhuma proposta de otimização de handover com autenticação e não fazem avaliação de desempenho utilizando métricas de QoE em cenários com autenticação presente na troca de ponto de acesso (handover). Ainda na seção foi denotado que a solução de virtualização de redes utilizada no Wi-Flow permite, ao contrário de outras, a criação e administração e priorização de *slices* de rede pelo ambiente Web.

4

ARCABOUÇO DA SOLUÇÃO

A solução Wi-Flow, proposta nesta dissertação é composta de uma Interface Web, denominada WebFlow e dos seguintes módulos: Módulo de gerenciamento de fluxos, módulo de virtualização de redes, módulo de QoS e módulo de gerenciamento de mobilidade.

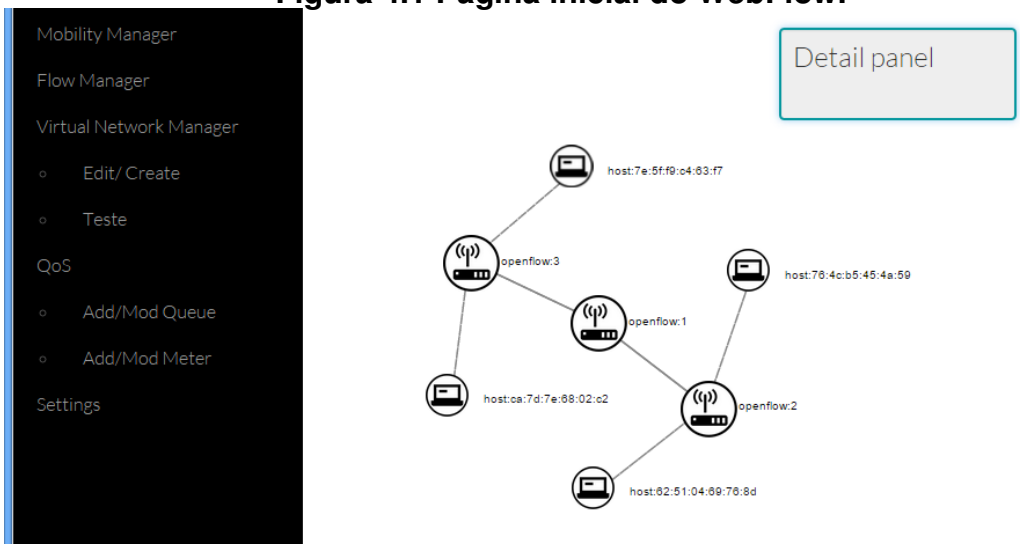
Neste capítulo apresentaremos o funcionamento dos módulos e as funções exercidas por eles no arcabouço da solução.

4.1 Interface de Gerenciamento WEB (WebFlow)

Para atingir um dos objetivos da proposta, o gerenciamento centralizado, foi desenvolvida uma interface Web para administração da rede (WebFlow), através da qual é possível realizar a gerencia tanto de redes cabeadas como sem fio.

A WebFlow fornece um gerenciamento holístico, pensado nos dois tipos de rede e entrega uma interface intuitiva e de fácil acesso, como visto na Figura 4.1.

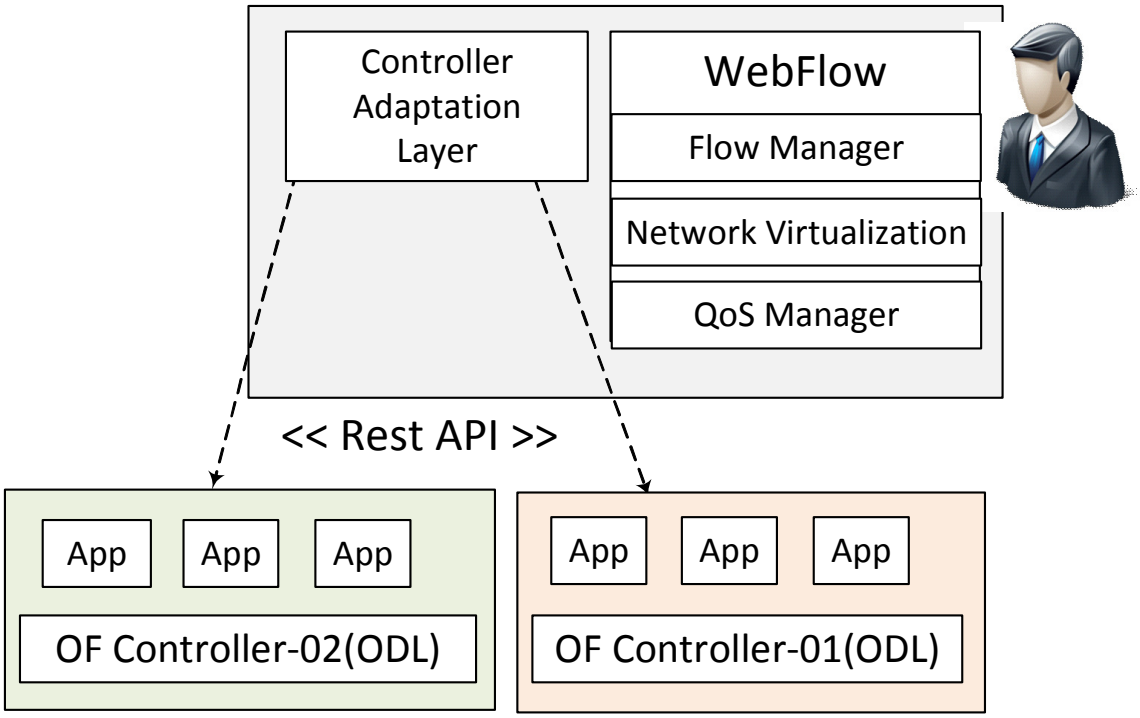
Figura 4.1 Página inicial do WebFlow.



Fonte: O Autor.

É a partir desta interface que se dá o acesso a todos os módulos de gerenciamento e controle. Comunicação da interface com os controladores SDN é realizada através de uma API REST disponível nos controladores, conforme apresentado na Figura 4.2.

Figura 4.2 WebFlow



Fonte: O autor.

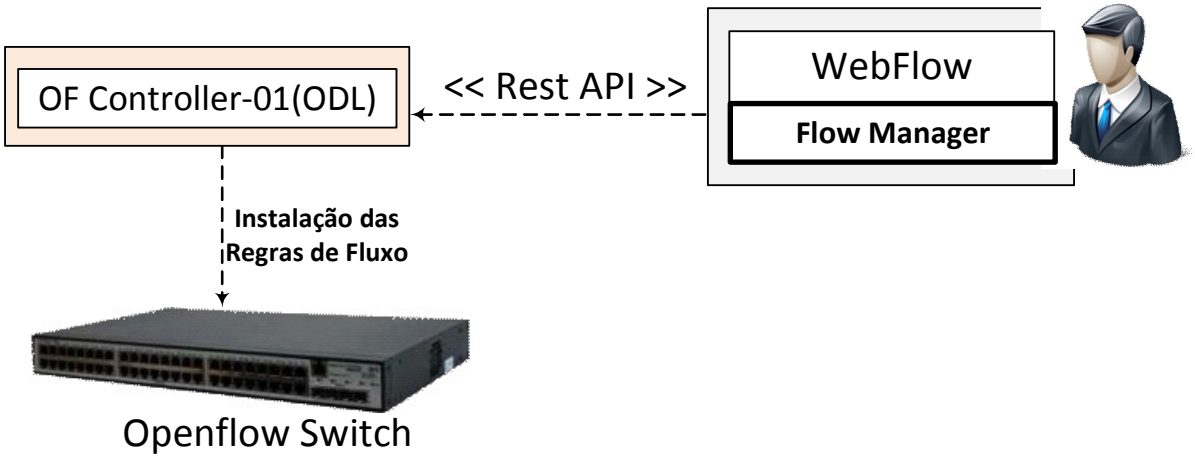
4.1.1 Módulo de Gerenciamento de Fluxos

O módulo de gerenciamento de fluxo foi desenvolvido para que o administrador possa realizar intervenções em tempo real em fluxos de rede para alterar seus comportamento e realizar operações diversas, como mitigar um ataque à rede local, espelhar tráfego para análise em tempo real, desviar fluxo variados por caminhos alternativos ou quaisquer manobras sobre o tráfego de rede.

A sequência seguida para a instalação de regras de fluxo é descrita na Figura 4.3, onde o módulo de gerenciamento de fluxo realiza uma chamada REST para o controlador e, nesta, envia os dados do fluxo a ser gerenciado. Com essas informações o controlador instala as regras de fluxo no ativo de rede em questão,

implementando assim alguma política ou modificação no comportamento do fluxo da rede.

Figura 4.3. Gerenciamento de Fluxos



Fonte: O autor.

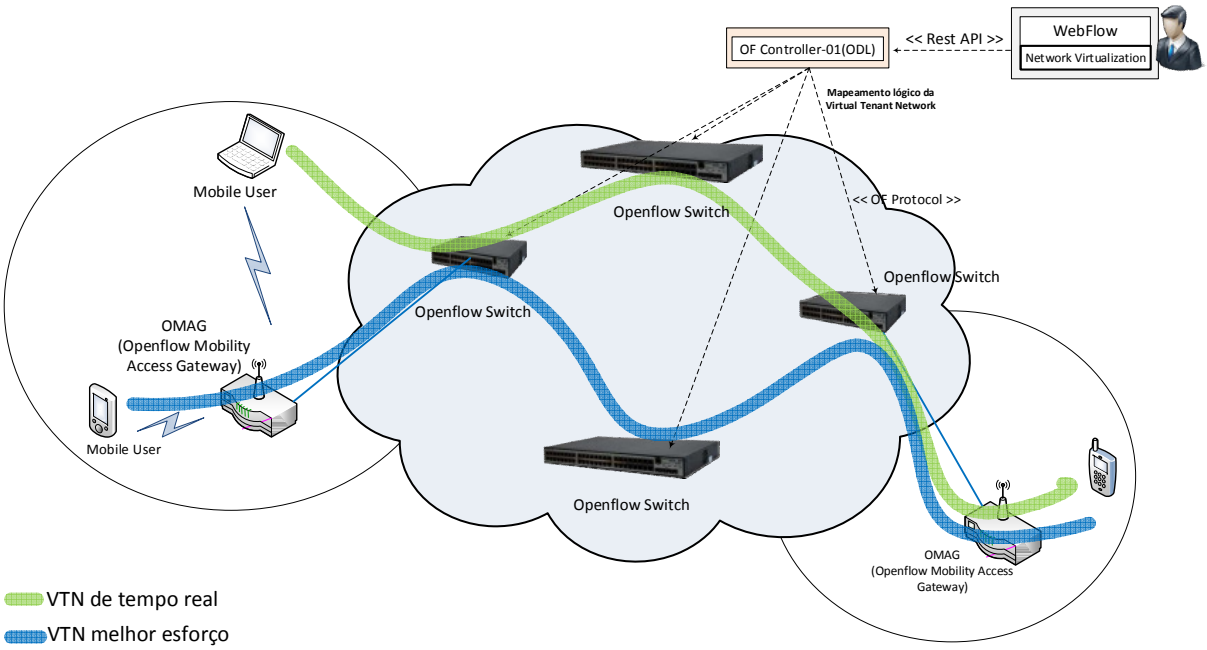
4.1.2 Módulo de Virtualização de Redes

O módulo de virtualização de redes foi desenvolvido de forma a ofertar características como escalabilidade, segurança, portabilidade, redução de custos, aumento da eficiência energética, diminuição da complexidade da rede e confiabilidade, baseando-se na separação completa do plano lógico do substrato físico por meio de redes multi-inquilinos (VTNs).

Com o uso da VTN os usuários podem criar e implantar qualquer rede lógica sem o conhecimento da topologia da rede física. Uma vez definida uma nova VTN (Rede Virtual), esta é mapeada automaticamente no substrato físico. O fluxo seguido para a criação da VTN é explanado na Figura 4.4, onde o módulo de virtualização de redes do WebFlow realiza uma chamada REST para o controlador e nesta envia os dados para criação da VTN (Nome da VTN, origem do trafego, destino do trafego). Utilizando-se do conceito de fundamental de SDN em que o controlador tem a visão global da rede, o usuário pode abstrair toda complexidade da topologia do substrato físico e de forma simples repassar ao controlador a função de instalar as regras de fluxo nos ativos de rede que compõe todo caminho origem e destino, de forma a promover o isolamento do fluxo autorizado a trafegar na rede multi-inquilino. A

Figura 4.4 apresenta hosts que utilizam duas redes virtuais criadas para fins diferentes e apesar de compartilharem um switch de ingresso e outro de egresso, seus tráfegos se mantêm isolados e sobre estas redes virtuais podem incidir diferentes priorizações mesmo sendo estes presentes num mesmo substrato físico.

Figura 4.4. Virtualização de redes



Fonte: O autor.

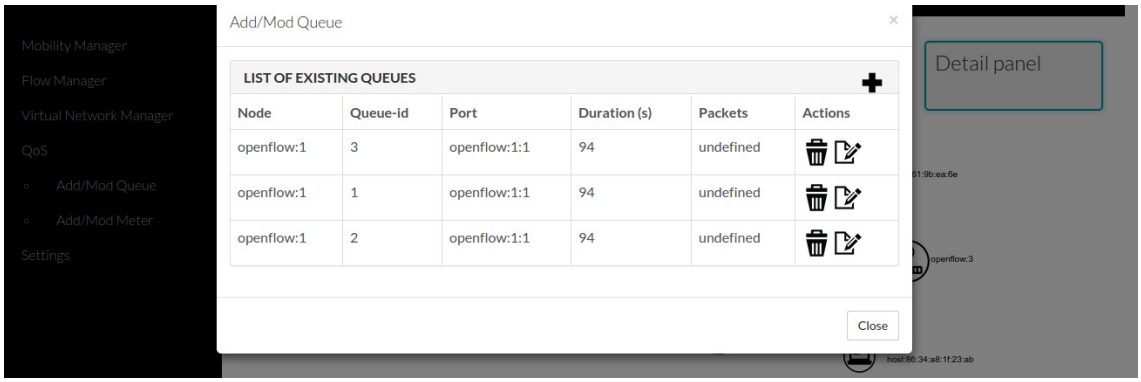
4.1.3 Módulo de QoS

A utilização das métricas de QoS na rede é fator essencial para o bom funcionamento de aplicações avançadas, como videoconferência, VoIP (voz sobre IP), que demandam grande largura de banda, e diferenciação do serviço de rede ofertado.

De forma sintética, o uso de QoS e uma boa estratégia de gerencia de tráfego de rede nos permite empregar a um determinado fluxo de dados, um nível de prioridade maior em detrimento as outros e com isso utiliza-se desta prioridade para encaminhar tal fluxo pela rede, aplicando-se a este requisitos de QoS. Neste sentido, o módulo de QoS, visa ofertar uma ferramenta que possibilita a formulação e implementação de mecanismos para gerenciamento de QoS de forma simplificada e da fácil uso por meio de uma interface Web.

Neste modulo é possível definir regras baseadas em filas e/ou meters para a criação de esquemas de qualidade de serviço complexos. Para tanto, na aba QoS presente no WebFlow existem dois sub-menus “Add/ModQueue” e “Add/Mod Meter”. A Figura 4.5 mostra a janela Add/ModQueue. Nela são listadas as filas instaladas nos switches. Neste exemplo, existem três filas instaladas no nó openflow:1, todas na porta 1 (openflow:1:1).

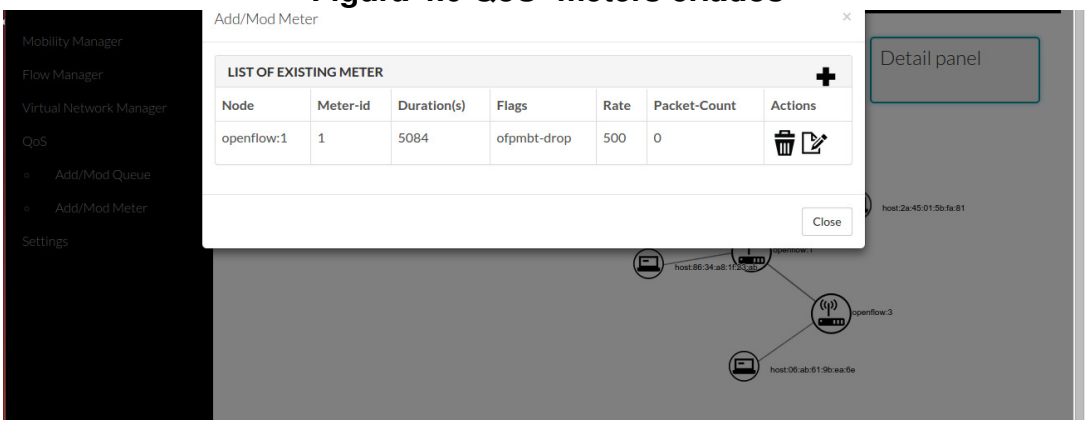
Figura 4.5 QoS - Filas Criadas



Fonte: O Autor.

.A adição de meter é realizado a partir do mesmo modulo de QoS, para tanto se faz uso da funcionalidade de “Add/Mod Meter” , como visto na Figura 4.6. Nela é possível visualizar os meters que estão instalados nos switches Openflow. No exemplo existe um meter no nó “openflow:1” do tipo drop com limitador de tráfego de 500 kbps.

Figura 4.6 QoS- meters criados



Fonte: O Autor.

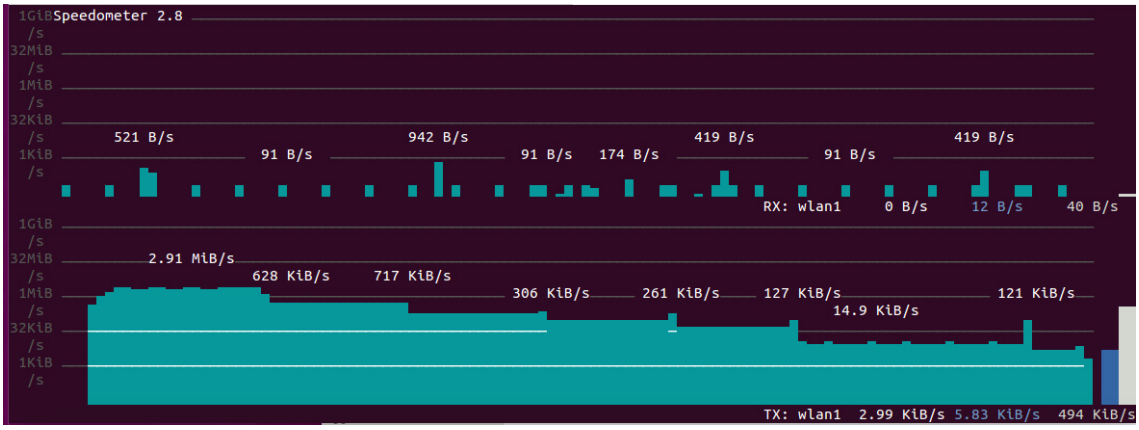
4.1.3.1 Redução de vazão com Medidor (meter)

Uma das contribuições desse trabalho foi a integração entre o Meter e o ambiente web que possibilita de forma simples e eficaz a elaboração de esquemas

para controle de qualidade de serviço ofertada. Através do meter é possível estabelecer valores máximos de vazão a serem utilizados por determinados fluxos de dados, os quais podem sofrer descarte de seus pacotes caso ultrapassem valores pré-estabelecidos. Este simples arranjo exemplificado aponta para soluções que possam realizar controles de forma a entregar uma qualidade de serviço de forma igualitária na rede, sem que algum usuário utilize dos recursos providos de forma a prejudicar todo o grupo de usuários da rede.

Um exemplo de um dos controles possíveis do meter pode ser verificado na Figura 4.7, onde o tráfego é modelado através do meter. Essa tela pertence ao aplicativo *speedometer*[4], que demonstra a vazão nas interfaces de rede do sistema. Na Figura 4.7, uma tráfego de vídeo é inserido com 3 Mbps, e aos poucos é reduzido usando-se o meter para realizar o controle da vazão máxima permitido para aquele fluxo. É possível ver na figura o tráfego pouco a pouco decaindo até a taxa de 512 kbps definida pela restrição de meter.

Figura 4.7 Reduzindo a vazão usando meter

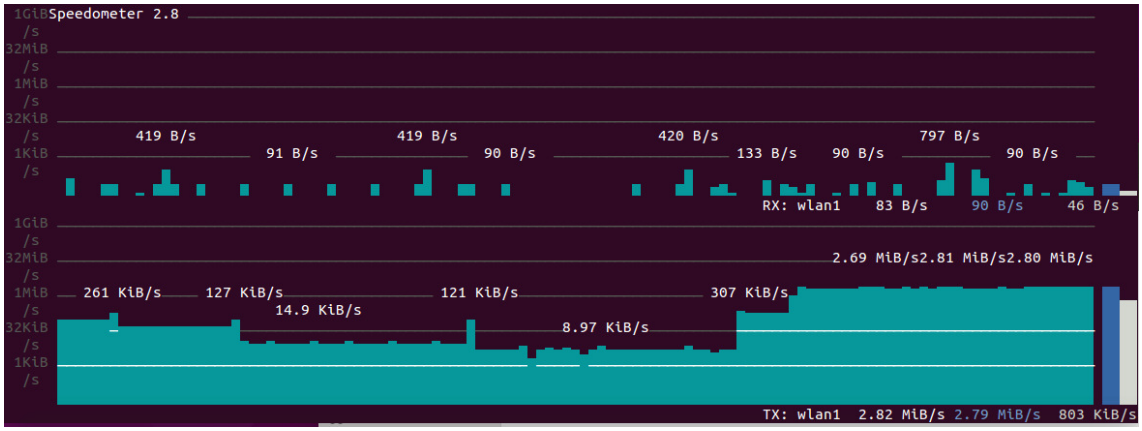


Fonte: O Autor.

A Figura 4.8 mostra a retomada da vazão usando quando é retirada a restrição de vazão máxima definida no meter. É possível observar que quando removida a regra de modelagem do tráfego do meter, a vazão volta ao normal imediatamente.

[4]https://excess.org/speedometer/

Figura 4.8 Retomando a vazão usando meter

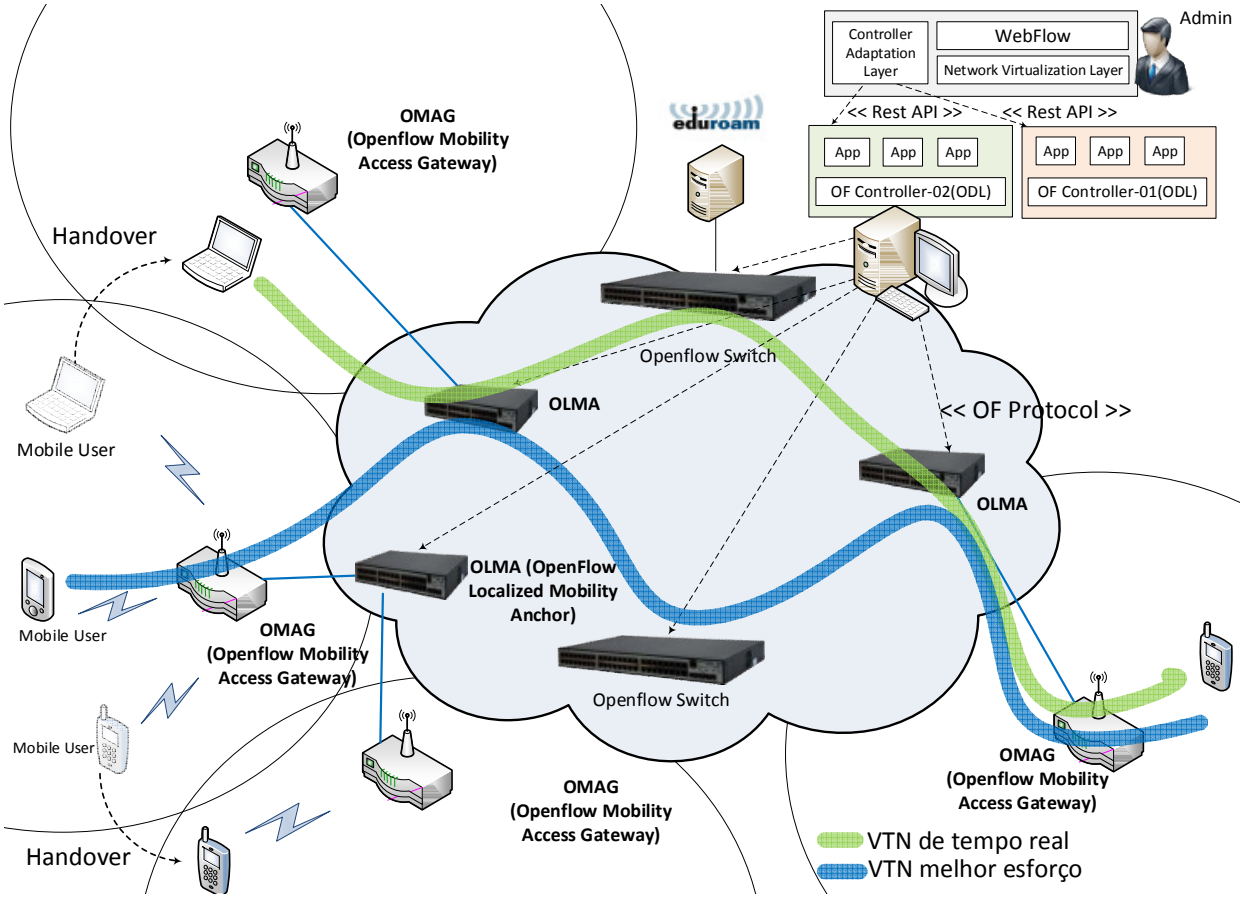


Fonte: O Autor.

4.2 Módulo de Gerenciamento de Mobilidade

A proposta Wi-Flow aproveita os benefícios do paradigma SDN e o emprega no módulo de gerenciamento de mobilidade, de forma a propor uma arquitetura para mobilidade, como visto na Figura 4.9.

Figura 4.9 Arcabouço Wi-Flow



Fonte: O Autor.

Os OMAGs, ou Openflow Mobility Access Gateway, mostrados na Figura 4.9, são as entidades responsáveis por monitorar e gerenciar a mobilidade dos usuários. No Wi-Flow, os OMAGs possuem duas representações, uma física e outra lógica.

A parte física do OMAG consiste de roteadores comerciais modificados. Nesses roteadores, o firmware original é substituído pelo OpenWRT[5], que é um sistema linux para dispositivos restritos, e é acrescentada uma versão espaço do kernel do Openflow. Foi escolhida a versão 1.3 do Openflow, pois as versões anteriores não dão suporte a funcionalidades como: QoS, IPv6 e Group Tables.

Os OLMAs ou Openflow Localized Mobility Anchor são os gateways dos OMAGs, eles gerenciam o tráfego. Além disso, mantêm estruturas de dados que permitem saber se o usuário está se movendo entre OMAGs diferentes (handover).

4.2.1 Wi-Flow Table Pipeline (WTP)

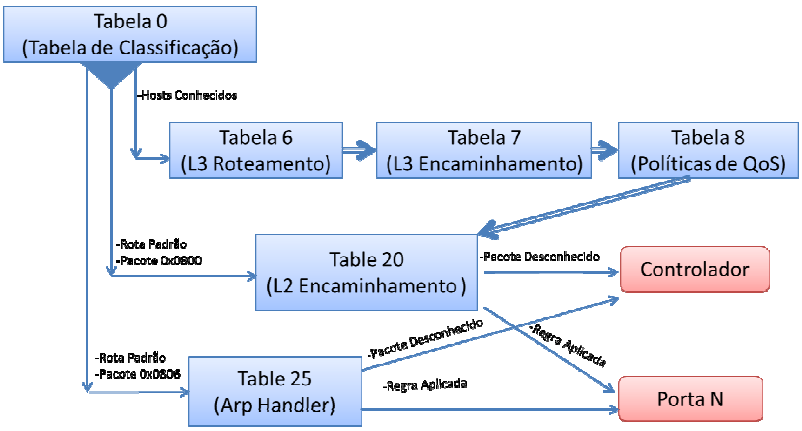
Todos os switches Openflow possuem várias tabelas. Cada tabela pode conter várias entradas de fluxo. As tabelas de fluxo foram especificadas no protocolo Openflow para elaboração de *pipelines* complexos, onde se pode atribuir diferentes funções às diversas tabelas de forma a tratar o fluxo de um processo estabelecido.

Os principais parâmetros das entradas de fluxo são os campos de *match*, a prioridade e o conjunto de instruções. Os campos de *match* dizem quais regras se aplicam aos fluxos de pacotes e as prioridades ordenam as regras na determinada tabela, e o conjunto de instruções dizem quais ações serão aplicadas naquela regra.

A WTP, apresentada na Figura 4.10, é um componente muito importante para o funcionamento do Wi-Flow. Quando o operador adiciona regras na rede, ele precisa estar ciente das funções de cada tabela, pois a inserção de regras de fluxos sem o conhecimento do pipeline estabelecido pode contribuir para ocorrência de conflitos entre regras de fluxo vigentes e as novas regras, o que pode gerar instabilidade nas funções da rede.

[5] Distribuição GNU/Linux para pontos de acesso sem fio - https://openwrt.org/

Figura 4.10 Organização da Wi-FlowTable Pipeline



Fonte: O Autor

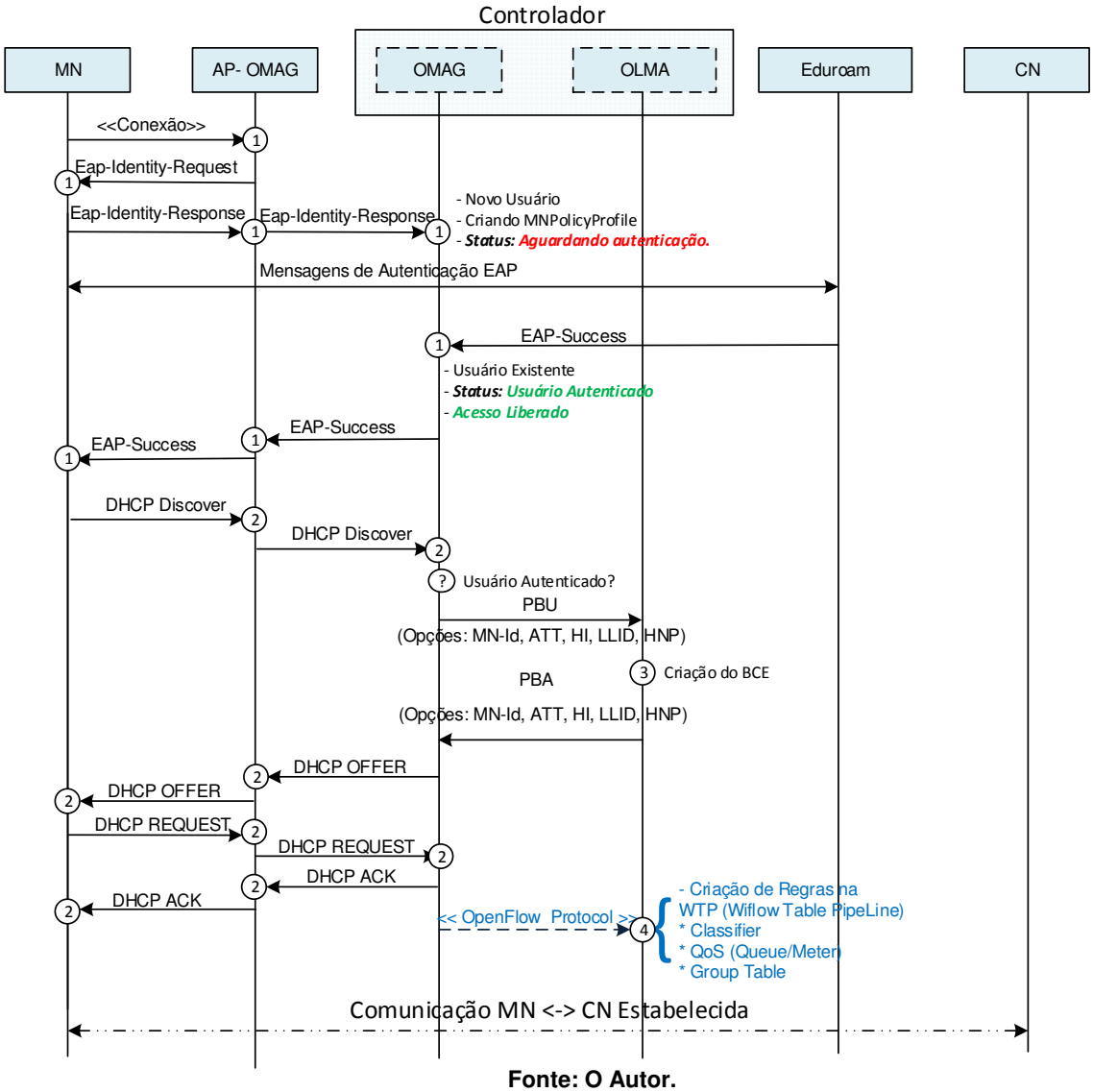
Na WTP, a tabela zero, funciona como tabela de classificação, todos os pacotes chegam primeiro na tabela zero e, a partir das regras nela instaladas, são distribuídos para as outras tabelas. Na tabela 6 é feito o roteamento dos pacotes, modificando-se os IPs; na tabela 7, o encaminhamento dos pacotes é feito modificando-se MACs. A tabela 8 é responsável pela funcionalidade de QoS como filas e meter. Nessa tabela, as regras associam os fluxos à determinada classe de QoS. Na tabela 20, todo o encaminhamento é feito via MAC. Nessa tabela, caso nenhum match ocorra, o pacote é enviado ao controlador. A tabela 25 é usada para tratamento de ARPs, caso não tenha regras para um determinado fluxo de ARP, esse pacote também é enviado ao controlador.

Este *pipeline* foi definido na proposta, de forma a orientar a criação de regras de fluxo em tabelas pré-definidas e agrupá-los para tratamento em grupo, o que otimizará o encaminhamentos dos pacotes.

4.2.2 Sinalização de Conexão

A sinalização de conexão, mostrada na Figura 4.11, possui quatro etapas: autenticação(1), mobilidade(2), fornecimento de IP(3) e implementação(4) de regras Openflow. Na autenticação, o usuário conecta-se à rede Eduroam fornecendo login e senha. No protótipo, a rede Eduroam usa o protocolo EAP com autenticação TTLS. A comunicação entre o cliente e o roteador é feita através do protocolo EAP e o protocolo RADIUS é usado para a troca entre o roteador e o servidor de autenticação.

Figura 4.11 Sinalização de Conexão



Fonte: O Autor.

A aplicação OMAG monitora toda a troca de mensagem entre cliente e servidor de autenticação. Após a confirmação da autenticação do usuário, inicia-se o processo de obtenção de IP. Nessa etapa terminal móvel troca mensagens com o servidor DHCP implementado no controlador. A obtenção de endereço é gerenciada pelo protocolo de mobilidade do OMAG. As mensagens PBU (Proxy Binding Update) e PBA (Proxy Binding Ack) são trocadas entre OMAG e OLMA com o objetivo de verificar permissões e possíveis ocorrências de Handover.

A implementação das regras Openflow nos switches é a última etapa do processo de conexão. Nessa etapa, as regras de roteamento, encaminhamento e aplicação de políticas de QoS são instaladas.

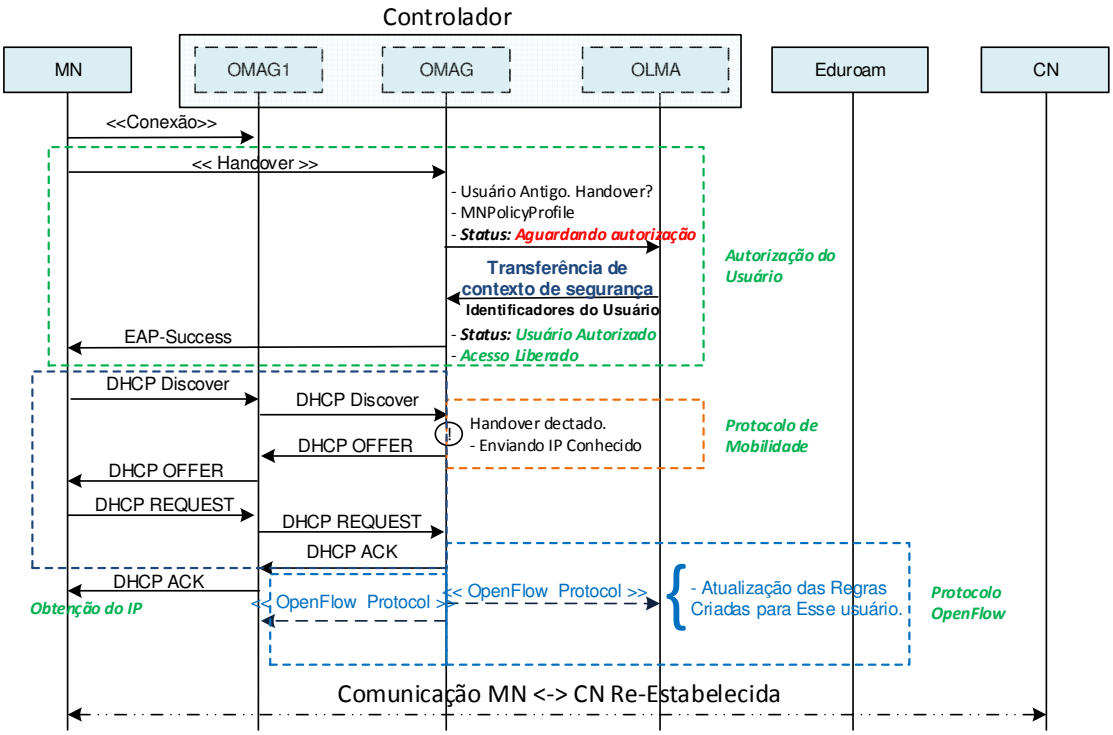
4.2.3 Sinalização de Handover

Uma das contribuições para o gerenciamento de mobilidade seguro foi a proposta de realizar o cache de autenticação, para tornar suave o handover.

A sinalização de handover, destacada na Figura 4.12, é semelhante à de conexão. A diferença é que quando o MN tentar migra do OMAG1 para o OMAG, o protocolo de mobilidade verifica que o usuário requisitante já estava conectado à outra rede, então o OMAG, consulta o OLMA para verificar se a solicitação tratar-se de uma handover. Em caso positivo, o OLMA verifica na estrutura de armazenamento, os identificadores utilizados na primeira conexão do MN solicitante, e autoriza a migração do cliente sem a necessidade de uma re-autenticação, pois a identificação é realizada a partir dos identificadores repassados por meio da transferência destes, dentro do mesmo contexto de segurança, conforme preceitua a RFC3374 (Context Transfer Problem Statement), o que corrobora para um handover suave, sem quebras decorrentes do tempo gasto no processo de re-autenticação.

Durante o handover o endereço obtido pelo usuário é o mesmo utilizado na rede anterior. Isso faz com que a quebra de conexão da camada 3 não ocorra, desse modo, mantendo a conexão nas camadas superiores.

Figura 4.12 Sinalização de Handover



Fonte: O Autor.

5

AVALIAÇÃO DOS RESULTADOS

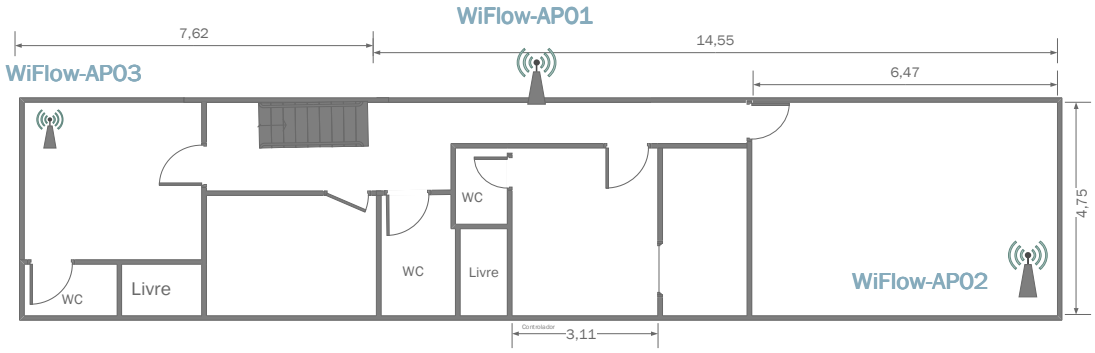
Neste capítulo realizamos a avaliação do Wi-Flow em um ambiente de teste experimental (testbed) montado para dissertação. Na Seção 5.1 é apresentado todo o ambiente de teste e as funções desempenhadas pelos equipamentos utilizados durante os experimentos.

Em seguida, na seção 5.2, são apresentadas métricas avaliativas utilizadas para avaliação. Na seção 5.3 são apresentados os resultados obtidos nas simulações com a utilização da gerência de mobilidade implementada na solução. Além disso, na seção 5.4 é realizada analise dos resultados e evidenciado as conclusões acerca das avaliações.

5.1 Ambiente de Testes

A Figura 5.1 mostra a planta baixa do ambiente onde o testbed foi implantado. O testbed possui três pontos de acesso Wi-Flow, que são roteadores sem fio com OpenvSwitch (OVS)(Openvswitch, 2015) instalado para suportar OpenFlow no nível do Kernel. O ambiente possui também um Wi-Flow Switch, que possui a função do LMA do protocolo PMIP, ou seja, funciona como ponto de ancoragem e saída dos APs. O Wi-Flow Switch é um roteador modificado para, assim como os Wi-Flow-APs, suportar o OpenFlow. O Controlador é o elemento mais importante da rede, ele controla toda a rede OpenFlow. O último elemento da rede é o Gateway, responsável por redirecionar o tráfego da rede OpenFlow para a Internet. Nos experimentos, o gateway também funciona como servidor de autenticação.

Figura 5.1 Ambiente do Testbed

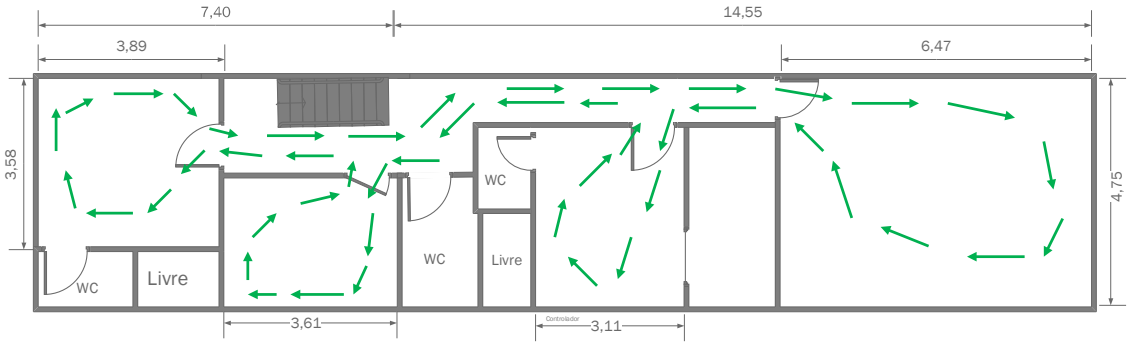


Fonte: O autor.

Todos os testes foram realizados com um usuário movendo-se a uma velocidade média de um metro por segundo (1m/s), equivalente a uma pessoa caminhando normalmente. Como o cenário possui cerca de 22 m, o usuário demora 22 segundos para ir de uma ponta à outra. Supondo-se que um usuário esteja na sala próxima ao AP03, ao andar até a sala do AP02, o usuário levou 22 segundos, em média, e cruzou o ponto de acesso AP01. A Figura 5.2 mostra o padrão de movimentação usado em todos os testes. Escolheu-se esse padrão para comparar de forma justa as diferentes soluções apresentadas. Um percurso completo da Figura 5.2 leva em média 120 segundos. Por isso, todos os testes foram ajustados para durarem 200 segundos.

Para cada teste foram realizados 30 repetições, como forma de obter resultados com relevância estatística.

Figura 5.2 Padrão de movimentação pelo ambiente

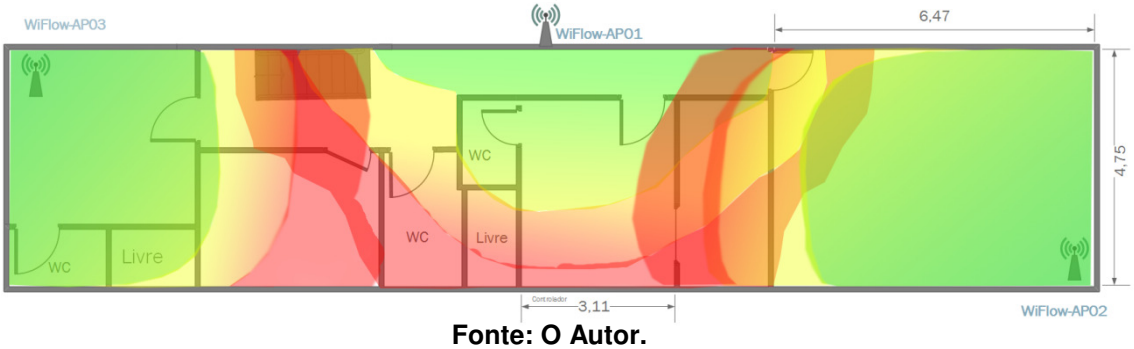


Fonte: O Autor.

A Figura 5.3 mostra o mapa de força de sinal dos três pontos de acesso sem fio. O mapa foi feito com auxilio da ferramenta *Heat mapper* da *Ekahau*, e mostra como está a distribuição do sinal no testbed. Quanto mais próximo do verde maior a

intensidade do sinal, quanto mais próximo do vermelho, menor a intensidade. As potências das antenas dos pontos de acesso foram levemente reduzidas, para permitir o cenário mostrado na Figura 5.3. Caso contrário, devido o espaço limitado, o usuário poderia se manter conectado mesmo estando no cômodo mais afastado. Como mostrado na Figura 5.3, quando o usuário migra de um cômodo ao outro ele é forçado a mudar de rede, do contrário a conexão é perdida.

Figura 5.3 Mapa de força de sinal do Testbed



Fonte: O Autor.

5.2 Métricas

É importante garantir QoS em qualquer que seja o tipo de rede, cabeada ou sem fio. No entanto, métricas de QoS não são o bastante para avaliar as redes do futuro. Com o intuito de resolver as limitações das tradicionais técnicas de controle de qualidade e desempenho da rede, no que diz respeito à percepção humana e aspectos subjetivos relacionados a conteúdos multimídia, uma nova abordagem vem sendo utilizada nas avaliações de novas arquiteturas. Os novos estudos de desempenho em sistemas multimídia têm como base as métricas de QoE.

Operações referentes ao controle de recursos da rede e, inclusive, mobilidade baseadas em métricas de QoE podem ser usadas para configurar e medir elementos de rede de forma a otimizar os recursos e garantir uma melhor percepção do conteúdo por parte dos usuários finais. Vários pesquisadores e organizações, como por exemplo, VQEG (Video Quality Experts Group), estão estudando formas de aplicar QoE em diferentes cenários fixos e móveis, porém essa metodologia continua sendo um desafio. Assim, as novas arquiteturas não estão sendo mais avaliadas apenas em termos de QoS, mas também quanto ao suporte à QoE. As métricas de QoE servem como extensão aos parâmetros de QoS, permitindo

avanços nas transmissões de aplicações de áudio e vídeo em redes IP e podem proporcionar melhorias nos protocolos. Neste contexto utilizaremos as seguintes métricas para avaliação da proposta:

- **Vazão:** Métrica de QoS obtida a partir da taxa de envio de dados por segundo, através desta métrica é possível durante o envio de um vídeo streaming, analisar o comportamento da taxa de envio durante o processo de handover do nó móvel e seu impacto na qualidade de serviço da rede;
- **Atraso(*delay*):** Métrica de QoS que mensura o tempo gasto pela rede para transportar um pacote do transmissor ao receptor. Em aplicações em tempo real, atrasos longos na rede podem inviabilizar a comunicação e contribuir para reduzir a qualidade de serviço da rede;
- **PSNR:** Peak Signal-to-Noise Ratio é uma métrica de QoE que representa a relação entre o sinal e o ruído ao comparar o frame original com o frame reconstruído, após o envio. Os resultados desta métrica mensuram de forma objetiva uma aproximação da percepção humana da qualidade de um vídeo;

5.3 Resultados obtidos

Nesta seção serão analisados os resultados obtidos nas avaliações dos cenários com base nas métricas de qualidade de serviço e qualidade de experiência, descritas anteriormente.

5.3.1 Vazão UDP com OVS e com CPQD

O primeiro teste foi realizado para verificar a diferença de desempenho existente entre a aplicação OpenFlow rodando no espaço do Kernel e no espaço do usuário. No primeiro caso, espaço do kernel, instalou-se o firmware OVS nos roteadores OpenFlow e no segundo caso, espaço do usuário, instalou-se o firmware disponibilizado pelo CPqD (CPqD, 2013), Nesse experimento, executou-se um fluxo

sintético UDP de 100 Mbps entre o gateway e o cliente estático já conectado. Esse tráfego sintético era o único fluxo na rede, portanto, não havia interferências internas.

A Tabela 5.1 mostra a estatística descritiva dos testes coletados. Ao todos foram feitas trinta repetições. A Tabela mostra que a vazão média do switch do CPQD corresponde apenas a 35% da vazão média alcançado pelo Switch OVS. Estes resultados obtidos pelo OVS influenciaram a decisão de adoção deste nos Wi-Flow-APs utilizados na proposta.

Tabela 5.1 Resultado sintético do teste de Vazão para 95% de IC.

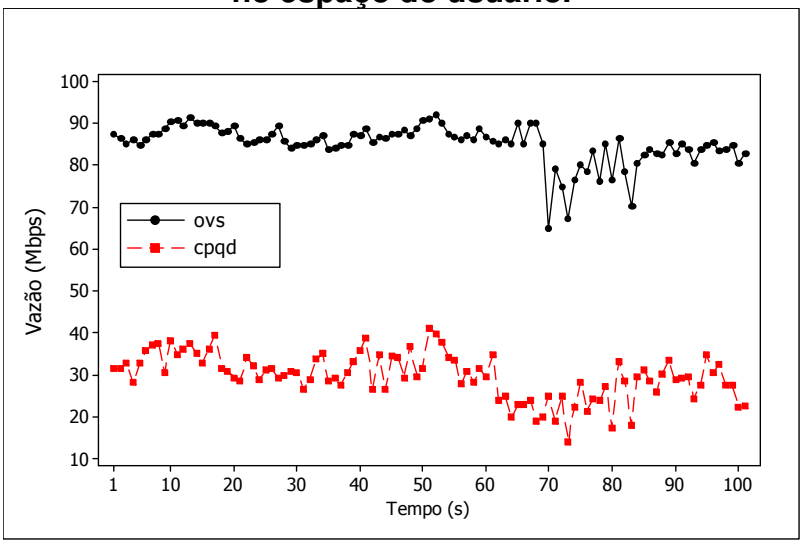
Vazão OVS x Switch CPQD						
Switch Openflow 13	**Espaço de Execução**	**Tipo de Teste**	**Protocolo de Transporte**	**Fluxo Sintético Enviado**	**Vazão Média alcançada**	**Intervalo de Confiança**
OpenVSwitch v2.4	Kernel	Vazão	UDP	100Mbps	85,087Mbps	95%
Switch CPQD	Usuário	Vazão	UDP	100Mbps	29,830Mbps	

Fonte: O Autor.

A Figura 5.4 mostra o resultado de uma instância dentre 30 repetições do experimento. Observa-se que com o OVS (espaço do kernel) o tráfego UDP atinge valores próximos a 90 Mbps. Por outro lado, o tráfego no espaço do usuário é bem inferior, atingindo apenas poucas vezes o valor de 40 Mbps.

Os resultados alcançados demonstram que a utilização do software switch openflow executado no espaço do usuário não entregaria a rede um desempenho aceitável, o que torna esta solução não aderente a um ambiente critico de produção. Diante desse contexto a opção do software switch em execução no espaço do kernel, mostrou-se a melhor alternativa para o desenvolvimento de uma solução aplicável em ambiente real.

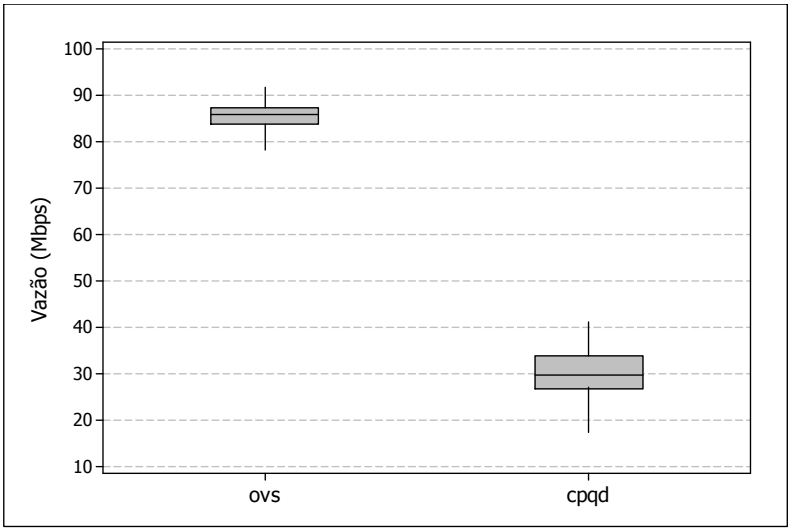
Figura 5.4 Diferença entre vazões com OpenFlow no Kernel versus OpenFlow no espaço do usuário.



Fonte: O Autor.

A Figura 5.5 apresenta o boxplot das vazões usando o OVS e o CPqD após 30 repetições do experimento. O boxplot apresenta os valores máximos e mínimos dos dados, bem como os percentis e a mediana no centro. Figura 5.5 corrobora o que foi apresentado na Figura 5.4, após várias repetições, a mediana dos resultados da vazão com OVS é estatisticamente superior ao CPqD. Em 30 repetições, a média da vazão do OVS é de 85,087 Mbps e do CPqD é de 29,830 Mbps.

Figura 5.5 Média dos valores de vazão com OVS e CPqD



Fonte: O Autor.

5.3.2 Mobilidade Com e Sem proposta de cache de Autenticação

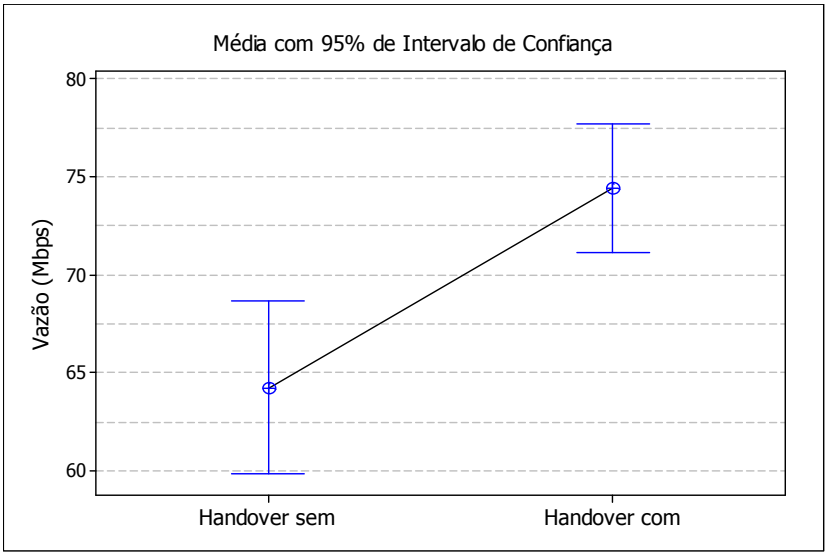
Os testes desta subseção foram realizados para verificar a existência de ganho na adoção de uma proposta de cache de autenticação para minimizar o tempo gasto na re-autenticação durante o *handover*, de forma a suavizar a perda de vazão na mudança de AP. Para os testes instalou-se o firmware OVS nos roteadores OpenFlow. Nesse experimento, executou-se um fluxo sintético UDP de 100 Mbps entre o gateway e o cliente em deslocamento seguindo o padrão de movimentação descrito na Figura 5.2.

Ao todo, foram feitas trinta repetições com a utilização da proposta de cache de autenticação e trinta repetições sem a adição da proposta e como resultado foi visto que a vazão média do switch do OVS utilizando-se da proposta de cachê representa um ganho 15,8%.

Na proposta de mobilidade com cache de autenticação, o tempo de re-autenticação do usuário é reduzido, assim não há quebras totais de conexão (quando a vazão chega à zero), diferentemente do experimento sem a proposta. O esquema empregado para a proposta baseia-se na seguinte processo: Ao identificar que há um procedimento de migração de ponto de acesso (*handover*) e de posse das informações da primeira autenticação guardadas na estrutura de armazenamento da aplicação, o controlador autoriza a migração do cliente sem a necessidade de uma re-autenticação. A identificação é realizada a partir das credencias armazenadas, o que colabora para um *handover* suave, com menor incidência de quebras decorrentes do tempo de re-autenticação. Ainda há queda na vazão, pois a re-associação, inerente à camada L2, não é instantânea, mas o ganho apresentado com a proposta mostra-se significativo.

A Figura 5.6 mostra a média da vazão em 30 experimentos. Sem a proposta, a média da vazão é de 64,24. Com a proposta esse valor aumenta para 74,43 Mbps, isso equivale a um ganho de 15,8%.

Figura 5.6 Vazão UDP com e sem a proposta de cache



Fonte: O Autor.

5.3.3 Avaliação do PSNR

O PSNR é uma métrica tradicional de QoE que estima a qualidade do vídeo em decibéis, comparando o vídeo original com o vídeo recebido pelo usuário. Para cada faixa de valores de PSNR, há uma qualificação para o vídeo que foi recebido pelo usuário. Veja a Tabela 5.2.

Tabela 5.2 - Valores de Classificação do PSNR

PSNR (dB)	> 37	31 – 37	25 – 31	20 – 25	< 20
QUALIDADE	EXCELENTE	BOM	ACEITÁVEL	POBRE	PÉSSIMO

Fonte: (Zinner et al. , 2010)

Os vídeos foram enviados um de cada vez. Durante a transmissão do vídeo, assim como no teste anterior, o usuário permanecia em constante movimento de um ponto de acesso para outro. Após o recebimento do vídeo foi utilizado a versão gratuita da ferramenta MSU (*Video Quality Measurement Tool*), (MSU Video Group, 2013), para avaliar e extrair as informações necessárias para avaliação do vídeo recebido. Utilizou-se o vídeo Bridge (Close, 2016) para avaliação.

A Tabela 5.3 mostra a estatística descritiva dos testes coletados. Ao todos foram feitas trinta repetições. A Tabela mostra que o valor médio do PSNR sem a

proposta foi de 26,7, considerado ACEITÁVEL de acordo com a Tabela 5.2, e com a proposta foi de 32,2, considerado BOM.

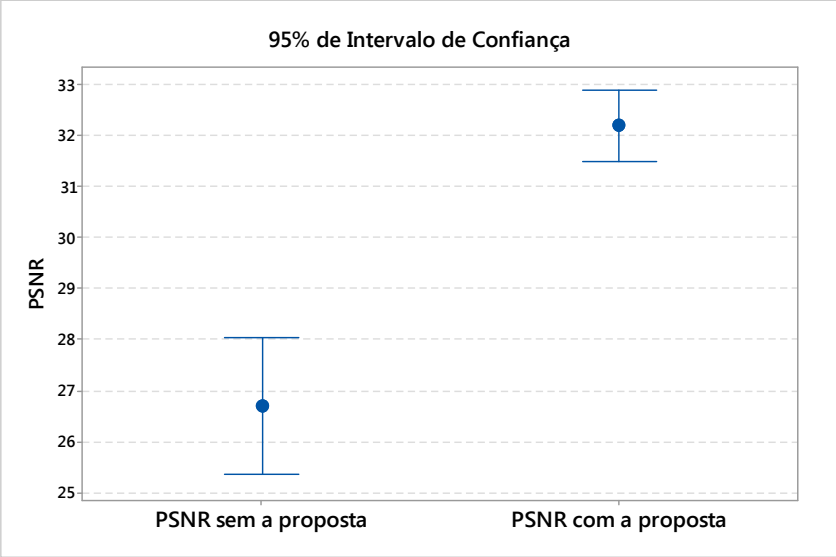
Tabela 5.3–Resultado teste de PSNR

Cenário	Repetições	Média	Erro Padrão Médio	Desvio Padrão	Valor mínimo	Mediana	Máximo	Tempo de Teste
PSNR sem a proposta	30	26,7	0,659	3,612	17	27	33	150s
PSNR com a proposta	30	32,2	0,344	1,883	29	32	35	150s

Fonte: O Autor

A Figura 5.7 mostra a comparação entre os intervalos de cada cenário, com 95% de confiança. É possível notar que com a proposta o PSNR é visivelmente superior ao cenário sem a proposta.

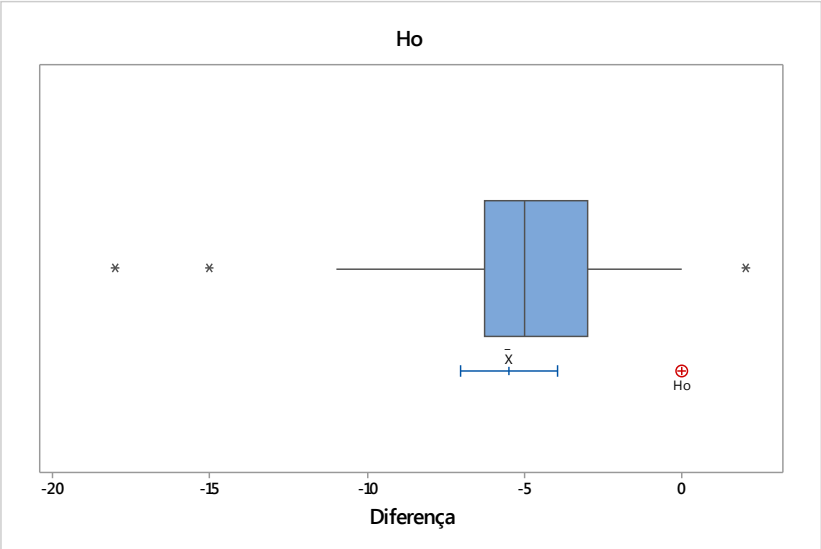
Figura 5.7 PSNR com e sem a proposta



Fonte: O Autor.

Apesar de visualmente ser perceptível a diferença entre os dados da Figura 5.7, é necessário embasar estatisticamente os resultados. Para isso, foi feito o teste T-Emparelhado nas duas massas de dados. A Figura 5.8 mostra o boxplot da diferença entre os cenários (com e sem a proposta). O símbolo H0 (Hipótese Nula) está bem distante do valor estimado de X. Isso significa que com 95% de certeza, que há fortes evidências para acreditarmos que os dados de PSNR com a proposta é superior aos dados de PSNR sem a proposta.

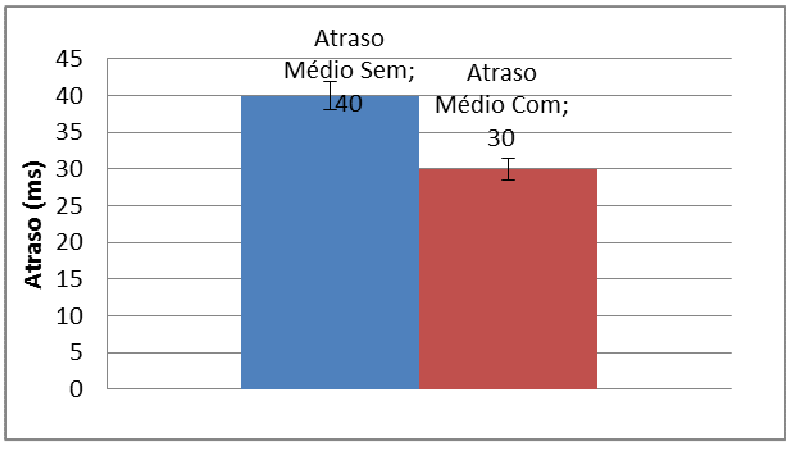
Figura 5.8 Boxplot da Diferença entre as propostas



Fonte: O Autor.

A Figura 5.9 mostra o atraso entre os frames dos vídeos. Quanto menor o atraso, melhor é a qualidade do vídeo recebido. Sem a proposta, o atraso médio em 30 repetições gira em torno de 40ms, e com a proposta de 30ms. Sem a proposta, as perdas de pacotes devido à mobilidade do usuário são mais acentuadas, com isso, o atraso médio da entrega dos pacotes é maior. Os resultados apresentados na Figura 5.9 foram calculados usando a ferramenta Evalvid (Evalvid, 2016)

Figura 5.9 Atraso na entrega dos frames



Fonte: O Autor.

A Figura 5.10 apresenta um frame original do vídeo usado na avaliação do PSNR. A apresentação dos frames fornece um respaldo visual para os resultados analíticos acima, permitindo comparar visualmente os desempenhos de diferentes

cenários. O vídeo utilizado dura 30 segundos e 2000 frames. Esse vídeo foi escolhido por durar mais do que os outros vídeos disponíveis em (Bridge, 2016). Como um percurso completo dura 120 segundos em média (ver Figura 5.2), o mesmo vídeo foi repetido 5 vezes, para simular um vídeo de 150 segundos.

Figura 5.10 Frame original do vídeo

Fonte: Bridge (Close)

A Figura 5.11 mostra um frame do vídeo capturado durante o *handover* sem a utilização da proposta de cache de autenticação. É possível ver que o frame está com uma qualidade bem inferior, se comparado com o frame original mostrado na Figura 5.10. Isso ocorre porque houve perdas de pacotes durante o *handover*, o que culminou na reconstrução incompleta do frame no receptor.

Figura 5.11 Frame no momento do *handover* sem a proposta

Fonte: Bridge (Close)

Por outro lado, a Figura 5.12 mostra o frame no momento do *handover* com a proposta. Percebe-se que nesse caso, o frame está com a qualidade melhor. Poucos pacotes são perdidos com a proposta, o que resulta em um frame mais completo. Embora não esteja tão nítido como no frame original, por ainda existirem perdas da camada L2, o vídeo resultante do cenário com a proposta é muito superior ao vídeo sem a proposta.

Figura 5.12 Frame no momento do *handover* com a proposta

Fonte: Bridge (Close)

5.4 Conclusões das análises

Neste capítulo foi verificado, após análise comparativa, que a utilização do OpenVswitch com suporte ao protocolo Openflow a nível de kernel, representou um ganho expressivo em relação ao desempenho de outras propostas que utilizam soluções de software switches executados no espaço do usuário.

Na análise da estratégia de gerenciamento de mobilidade com suporte a autenticação 802.1X, obtivemos o serviço de mobilidade e a continuidade de serviço ao usuário, bem como a garantia dos requisitos de tráfego de vídeo adequados em termos de métricas de QoS/QoE, demonstrando assim o êxito da proposta.

6

CONCLUSÃO E TRABALHOS FUTUROS

Este capítulo resume os principais pontos discutidos nessa dissertação. Para tanto Na Seção 6.1 são apresentadas as considerações finais do trabalho e na Seção 6.2 são discutidos os trabalhos futuros.

6.1 Considerações Finais

Este trabalho apresentou o Wi-Flow um arcabouço para o gerenciamento de redes heterogêneas com uso do paradigma de SDN. Discutiu-se sobre como o crescimento da complexidade e heterogeneidade das redes de computadores impactaria na sua administração e gerenciamento. Dessa forma, foi evidenciada a necessidade de arcabouços de gerenciamento para redes heterogêneas (Rede Sem Fio e Cabeada) que centralizassem e simplificassem a administração de ambientes tão complexos, provendo o atendimento de requisitos de qualidade de serviço, qualidade de experiência e segurança. No contexto de gerenciamento de mobilidade, foi discutido ainda, que há na literatura diversas iniciativas voltadas a prover o serviço mobilidade, no entanto os aspectos de segurança sempre são negligenciados, fato que contribui para a não utilização destas soluções em redes atuais, onde requisitos de segurança são essenciais.

Foi ainda apresentada a arquitetura da proposta Wi-Flow, e descrito todos os seus módulos (Gerenciamento de fluxos, de redes virtuais, QoS, topologia de rede e gerenciamento de Mobilidade).

Como resultados da avaliação da proposta, verificou-se o seu êxito na aplicabilidade do gerenciamento integrado da rede, bem como sua eficácia no serviço de mobilidade com suporte à autenticação, provendo assim as funcionalidades para o gerenciamento pleno, bem como a continuidade de serviço ao usuário móvel e a garantia dos requisitos de tráfego de vídeo adequados em termos de métricas de QoS/QoE.

6.2 Trabalhos Futuros

Essa dissertação possibilitou o surgimento de novas linhas para uma pesquisa adicional, com a finalidade de melhorar o gerenciamento de redes, segurança e o gerenciamento de mobilidade.

Entre as opções para trabalhos futuros, destacam-se algumas possíveis pesquisas:

- **Políticas dinâmicas de QoS:** No modulo de QoS implementado na proposta, a configuração de políticas de QoS é realizada de forma estática, não sendo estas adaptáveis ao estado da rede. Diante disso a Implementação de estratégia para configuração de políticas de QoS, com base na análise proativa do tráfego de redes Openflow, será um grande avanço no contexto de gerenciamento da qualidade de serviço prestada ao usuário.
- **Gerenciamento de Controle de Acesso com SDN:** Implantação de controle de acesso à rede (NAC - network Access control), com a utilização do paradigma SDN, para integração ao arcabouço de gerenciamento Wi-Flow.

REFERÊNCIAS

[1] Avelar, E. A. M. (2013). PMIPFlow: *Uma proposta para gerenciamento de mobilidade em redes definidas por software*. Master's thesis, Universidade Federal de Pernambuco.

[2] B. Raghavan et al., ‘‘Software-defined internet architecture: Decoupling architecture from infrastructure,’’ in Proc. 11th ACM Workshop Hot Topics Netw., 2012, pp. 43–48.

[3] Big Switch Networks (2012).Floodlight Controller: http://www.projectfloodlight.org

[4] Big Switch Networks (2011). Big Switch Controller. http://www.bigswitch.com/.

[5] Bridge (close) (2016). http://www2.tkn.tu-berlin.de/research/evalvid/cif.html

[6] Brocade Controlador SDN, (2016) Disponivel em: http://www.brocade.com/en/products-services/software-networking/sdn-controllers-applications/sdn-controller.html

[7] Chowdhury, NM MosharafKabir, andRaoufBoutaba. "A surveyof network virtualization." Computer Networks 54.5 (2010): 862-876

[9] CPqD (2013). OpenFlow 1.3 Software Switch. Disponível em: http://cpqd.github.io/ofsoftswitch13/.

[10] C. Rigney, S. Willens, A. Rubens and W. Simpson, “Remote Authentication Dial In User Service (RADIUS),” IETF RFC2865 (June 2000).

[11] Evalvid 2016. A Video Quality Evaluation Tool-set, http://www2.tkn.tu-berlin.de/research/evalvid/EvalVid/docevalvid.html

[12] Extreme SDN Platform (2016). disponível em: http://learn.extremenetworks.com/rs/extreme/images/SDN-BR.pdf

[14] Gundavelli S, Leung K, Devarapalli V, Chowdhury K, Patil B (2008) Proxy Mobile IPv6. IETF RFC 5213.

[14] Huawei controlador Agile (2016), Disponivel em: http://e.huawei.com/br/solutions/technical/sdn

[15] I.F. Akyildiz, J. Xie and S. Mohanty, A survey of mobility management in next-generation all-IP-based wireless systems, *IEEE Wireless Communications***11** (2004) (4), pp. 16–28.

[16] Internet Engineering Task Force (2010). Network-based Localized Mobility Management.http://datatracker.ietf.org/doc/charter-ietf-netlmm/.

[17] IEEE(2006), disponível em: http://www.ieee802.org/1/pages/802.1x.html

[18] J. Turner, D. Taylor, Diversifying the internet, in: Proceedings of theIEEE Global Telecommunications Conference (GLOBECOM'05), vol.2, 2005.

[19] K. Tantayakul, R. Dhaou and B. Paillassa, "Impact of SDN on Mobility Management," *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, Crans-Montana, 2016, pp. 260-265.

[20] Kim, J.-I., Jung, H., and Koh, S. J. (2011). Distributed mobility control for mobileorientedfuture internet environments. In ICT Convergence (ICTC), 2011 InternationalConference on, pages 342 –347.

[21] MSU Video Group (2013). Video Quality Measurement Tool. http://compression.ru/index_en.htm.

[22] NEC (2011a). Helios: An extensible C-based OpenFlow controller. http://www.nec.com/.

[23] NEC (2011b). Trema: Full-Stack OpenFlow Framework in Ruby and C. http://trema.github.com/trema/.

[24] Nicira Networks (2010). NOX: Network Operation System. http://noxrepo.org/wp.

[25] N.M.M.K. Chowdhury, R. Boutaba, Network virtualization: state ofthe art and research challenges, IEEE Communications Magazine 47(7) (2009) 20–26.

[26] N. McKeown, T. Anderson, H. Balakrishnan,G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. "OpenFlow: enabling innovation in campus networks". ACM SIGCOMM Computer Communication Review. April de 2008, Vol. 38, 2, pp. 69-74.

[27] Nakauchi, K., Ishizu, K., Murakami, H., Nakao, A., and Harada, H. (2011). Amphibia:A cognitive virtualization platform for end-to-end slicing. In Communications (ICC),2011 IEEE International Conference on, pages 1–

5. IEEE.

[28] Obele, B. and Kang, M. (2009). Mobility management: A proactive qos-aware proxymip with improved handover latency for end-to-end qos provisioning in a proxymip domain. In Advanced Communication Technology, 2009. ICACT 2009. 11thInternational Conference on, volume 03, pages 1867 –1869.

[29] ONF (2012). Software-Defined Networking: The New Norm for Networks. White paper, Open Networking Foundation. Disponível em: http://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wpsdn-newnorm.pdf

[30] OpenDaylight (2016). opendaylight controller : http://www.opendaylight.org/

[31] Opendaylight User-guide, 2015disponível em: https://www.opendaylight.org/sites/opendaylight/files/bk-user-guide.pdf

[32] OpenDaylight Consortium. http://www.opendaylight.org

[33] OpenFlow Specification 1.0 (2009). Disponível https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.0.0.pdf

[34] OpenFlow Specification 1.1 (2011). Disponível https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.1.0.pdf

[35] OpenFlow Specification 1.2 (2011). Disponível https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.2.pdf

[36] OpenFlow Specification 1.3 (2012). Disponível https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.0.pdf

[37] OpenFlow Specification 1.4 (2013). Disponível https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.4.0.pdf

[38] OpenFlow Specification 1.5 (2014). Disponível https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-switch-v1.5.0.pdf

[39] OpenvSwitch (2015). OpenFlow 1.3 kernel Switch. Disponível em: http://openvswitch.org/download/.

[40] Rice University (2011). Maestro: A System for Scalable OpenFlow Control. http://code.google.com/p/maestro-platform/.

[41] Stanford University (2011). Beacon: A Java-based OpenFlow Controller. https://openflow.stanford.edu/display/Beacon/Home.

[42] Stanford (2008). OpenFlow: Innovate in Your Network,disponível em: http://www.openflow.org/.

[43] Sherwood, R., Gibb, G., Yap, K., Appenzeller, G., Casado, M., McKeown, N., and Parulkar, G. (2009). *Flowvisor: A network virtualization layer*. OpenFlow SwitchConsortium, Tech. Rep

[44] Taghizadeh, A., Wan, T.-C., and Budiarto, . (2011). A comparative performanceevaluation of inter-domain network-based ip mobility solutions. In Proceedings of the7th Asian Internet Engineering Conference, AINTEC ’11, pages 136–139, New York,NY, USA. ACM.

[45] T. Benson, A. Akella, and D. Maltz,“Unraveling the complexity of network management,” inProc. 6th USENIX Symp.Networked Syst. Design Implement., 2009,pp. 335–348.

[46] T. Anderson, L. Peterson, S. Shenker, J. Turner, Overcoming theInternet impasse through virtualization, Computer 38 (4) (2005)34–41.

[47] Zinner, T. et al. Towards QoE management for scalable video streaming.21th ITC Specialist Seminar on Multimedia Applications-Traffic, Performance and QoE, IEICE, p. 64–69, 2010.

[48] Yamasaki, Y., Miyamoto, Y., Yamato, J., Goto, H., and Sone, H. (2011). Flexible access management system for campus vlan based on openflow. In Applications and theInternet (SAINT), 2011 IEEE/IPSJ 11th International Symposium on, pages 347–351.IEEE.

[49] Yap, K., Sherwood, R., Kobayashi, M., Huang, T., Chan, M., Handigol, N., McKeown,N., and Parulkar, G. (2010a). Blueprint for introducing innovation into wireless mobilenetworks. In Proceedings of the second ACM SIGCOMM workshop on Virtualizedinfrastructure systems and architectures, pages 25–32. ACM.

Apêndice

Este Apêndice aborda o arcabouço de ferramentas presente na interface WebFlow.

WebFlow (Ambiente Web para o Gerenciamento de redes)

A maioria dos ambientes de gerenciamento das redes openflow são proprietários, como o Vyatta da brocande. Os sistemas que possuem o código fonte aberto, geralmente, falham na usabilidade e são difíceis de configurar e gerenciar, como por exemplo, o Dlux, implementado para o controlador OpenDaylight. Com isso, o objetivo do WebFlow é fornecer um ambiente opensource para o gerenciamento de redes OpenFlow, que seja ao mesmo tempo completo e fácil de usar.

Das funcionalidades disponíveis no WebFlow tem-se a topologia de rede de todos os controladores conectados ao WebFlow, ver Figura 1. Além da topologia, o sistema mostra informações de cada nó, como identificação, no caso de switches OpenFlow e endereço MAC, no caso de hosts, objetivando auxiliar na administração da rede.

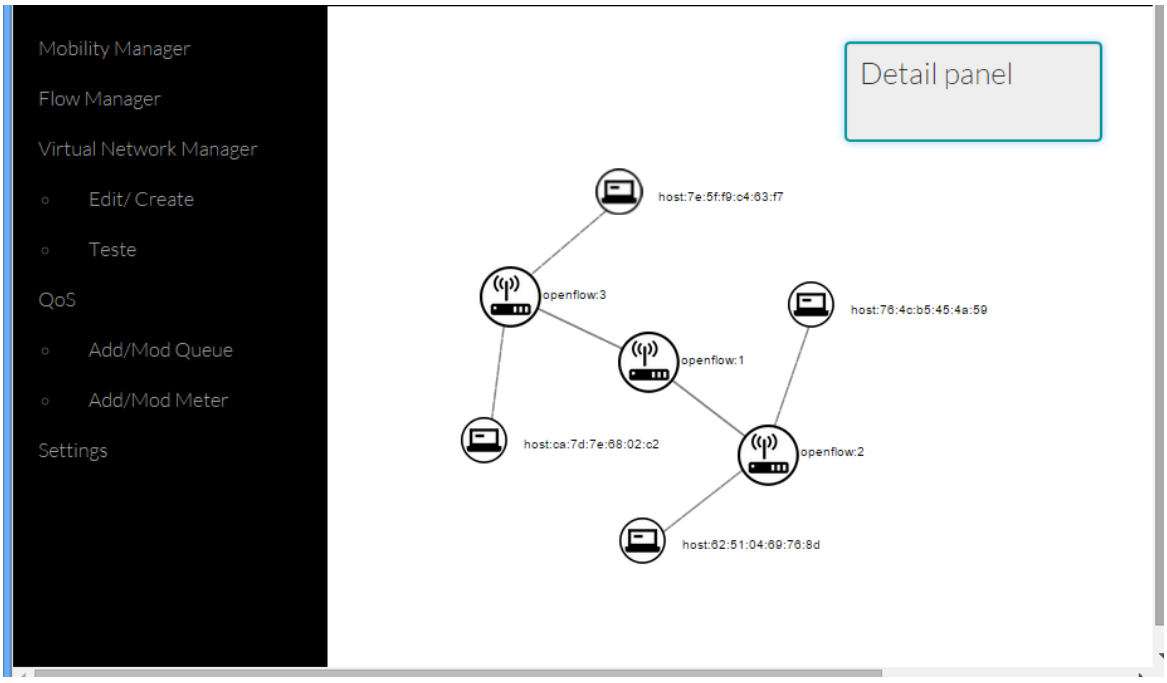


Figura 1 Página inicial do WebFlow.

Ainda na tela de topologia é possível detalhar informações dos nós clicando nos mesmos. A Figura 2 mostra o painel de detalhes que se abre ao interagir com um nó. Percebe-se que, para facilitar o gerenciamento, é possível adicionar regras de fluxo através desse painel, clicando-se em “Addflow” na seção Actions do painel de detalhes.

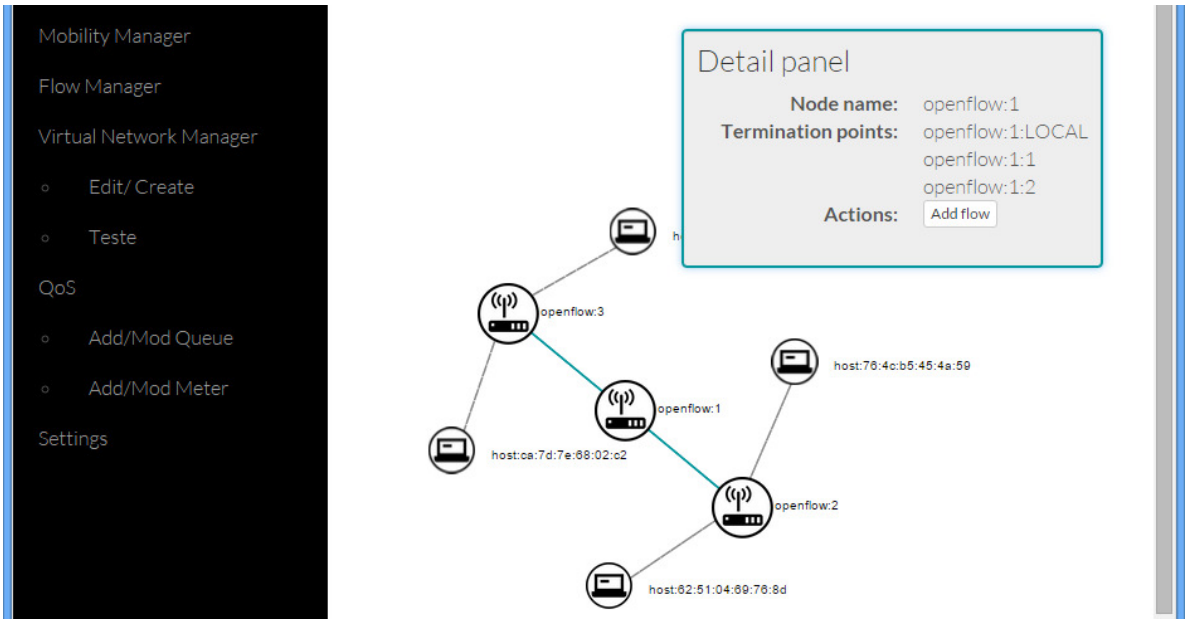


Figura 2 Detalhamento dos nós na tela de topologia.

Uma funcionalidade interessante do WebFlow é a possibilidade de verificar a localização dos nós em um mapa, como mostrado na Figura 3. Para apresentar os nós em um mapa, é preciso habilitar essa funcionalidade no aba settings, que será detalhado mais adiante.

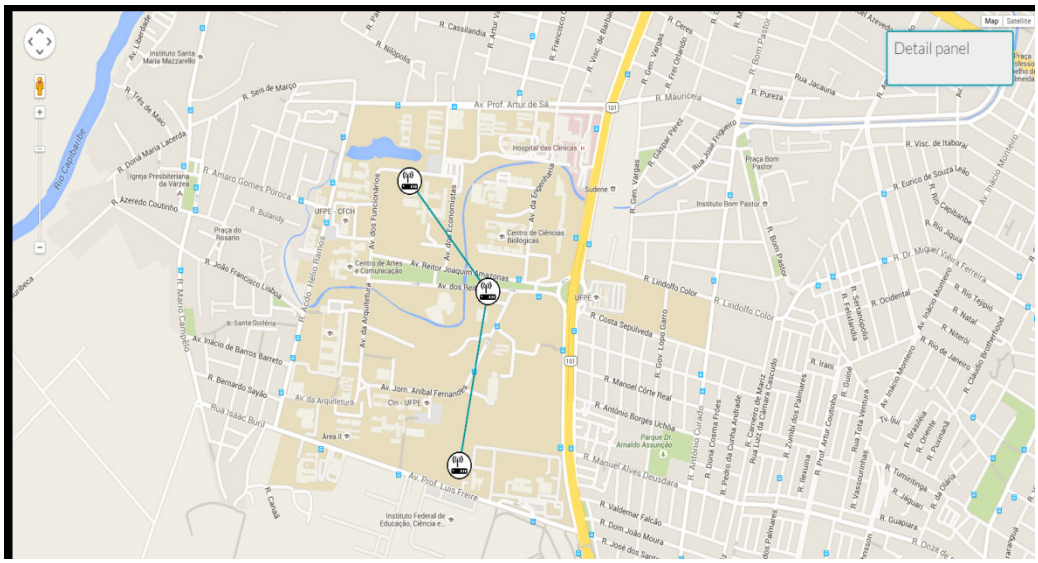


Figura 3 Mapa na tela de topologia

As funcionalidades do WebFlow são oferecidas através do menu localizada à esquerda da tela, são elas: *Mobility Manager*, *Flow Manager, Virtual Network Manager, Qualityof Service (QoS) e Settings*. A seguir, cada funcionalidade será detalhada.

- ***Mobility Manager***

No Eduflow, o gerenciamento de mobilidade possui todo um arcabouço formado por roteadores sem fio modificados; protocolos de mobilidade agindo na borda e no núcleo da rede; e gerenciamento próprio de QoS. Toda a inteligência da mobilidade está instalada no controlador OpenFlow. Portanto, suas operações não dependem do WebFlow. No entanto, como a mobilidade gera uma carga extra de sinalização, o operador/administrador pode optar por desabilitar essa opção para, por exemplo, reduzir o tráfego em momento de pico de atividade na rede. A Figura 4 mostra as opções disponíveis no gerenciamento de mobilidade. Na opção Mobile Handover a mobilidade está ativada e na opção manual permanece desativada.

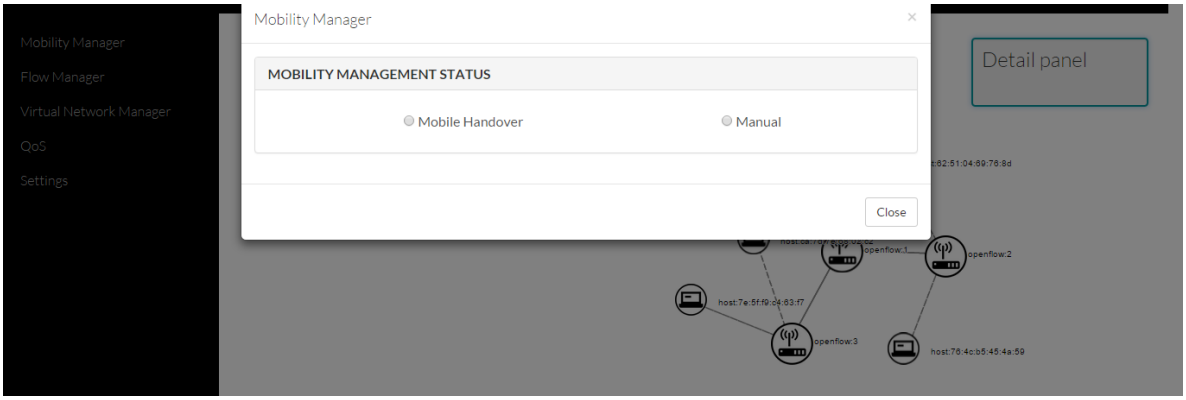


Figura 4 Configuração do gerenciamento de mobilidade

- ***Flow Manager***

Todo o gerenciamento de fluxo é feito nessa aba. Nela é possível adicionar, remover ou editar regras de fluxo. Ao clicar na aba é apresentada uma janela, Figura 5, listando os fluxos existentes em todos os switches.

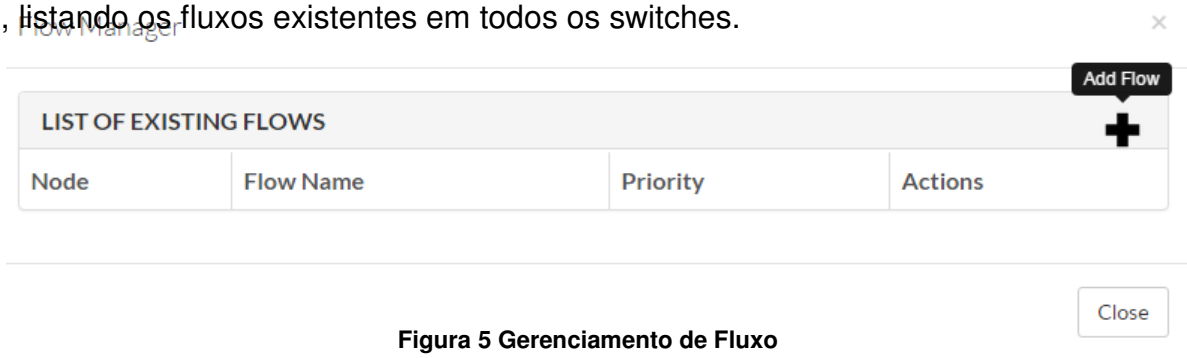
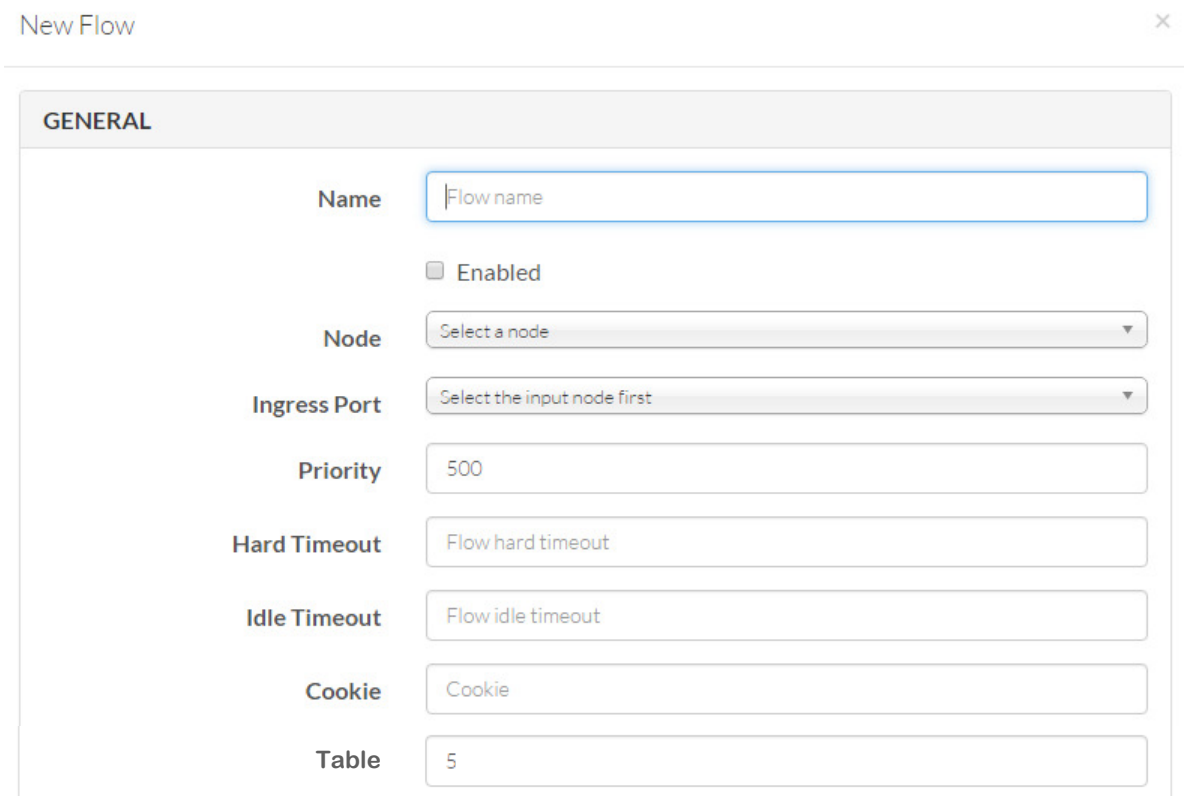


Figura 5 Gerenciamento de Fluxo

Ao clicar em AddFlow, uma nova janela é apresentada para adicionar uma nova regra de fluxo. A adição de regras é dividida em duas partes: os campos para match e as ações. O match é a descrição dos fluxos que se encaixam na regra e as ações dizem o que fazer com os fluxos que se encaixam nessa regra. A Figura 6 mostra os campos para match que podem ser usados para configurar as regras. Percebe-se que podem ser usados campos de quase todas as camadas da pilha TCP/IP.



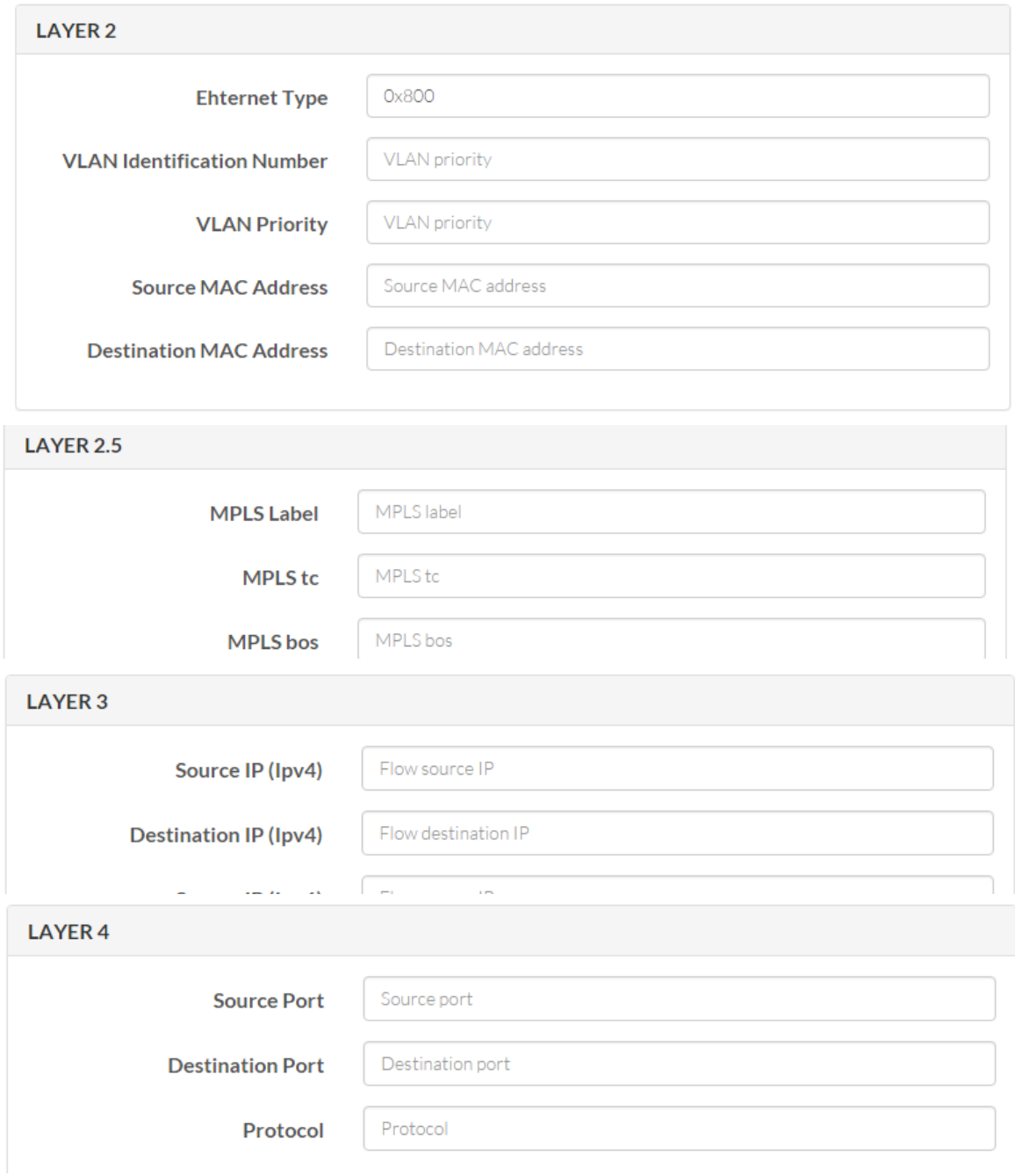


Figura 6 Adicionando um novo fluxo

As actions, ou ações, definem a instrução que deve ser tomada para determinada regras. Existem várias ações na especificação do protocolo Openflow 1.3, o WebFlow implementa todas elas. A Figura 7 mostra a seção de Ações do WebFlow. O operador pode adicionar quantas ações quiser. Elas são executadas

por ordem de inserção, ou seja, as primeiras a serem inseridas são também as primeiras a serem executadas.

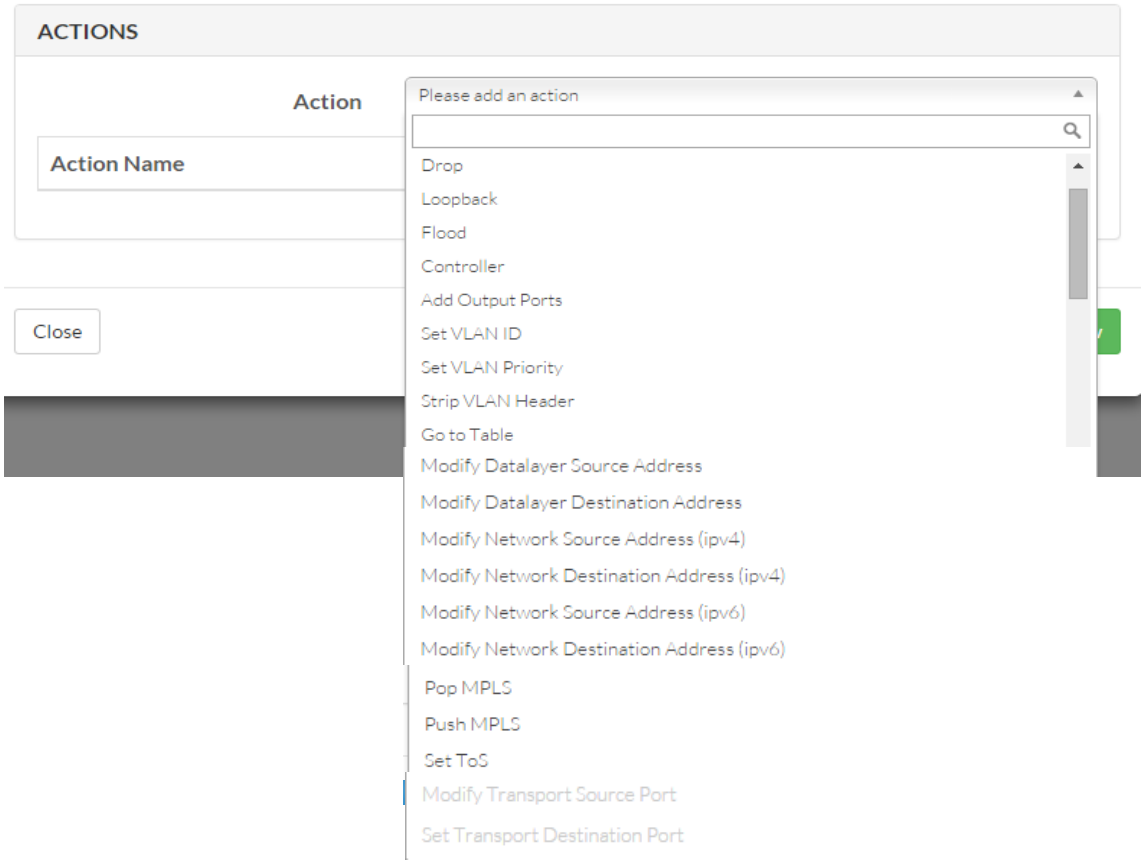


Figura 7 Adicionando uma ação à regra de fluxo

- ***Virtual Network Manager*:**

A criação de redes virtuais, que no OpenDaylight é chamada de VTN (Virtual Tenant Network), é uma das funcionalidades mais importantes que podem ser configuradas via WebFlow. Nela, é possível criar pontes virtuais de conexão entre hosts na mesma rede ou entre redes completamente diferentes.

A Figura 8 mostra uma ponte virtual (Virtual Bridge ou vBridge), chamada Teste, entre os hosts 63:51:04:69:76:8d (conectado ao nó “openflow:2”) e o host ca:7d:7e:68:02:c2 (conectado ao nó openflow:3). Fisicamente, os nós encontram-se separados, mas virtualmente, eles encontram-se juntos isolados pela VTN.

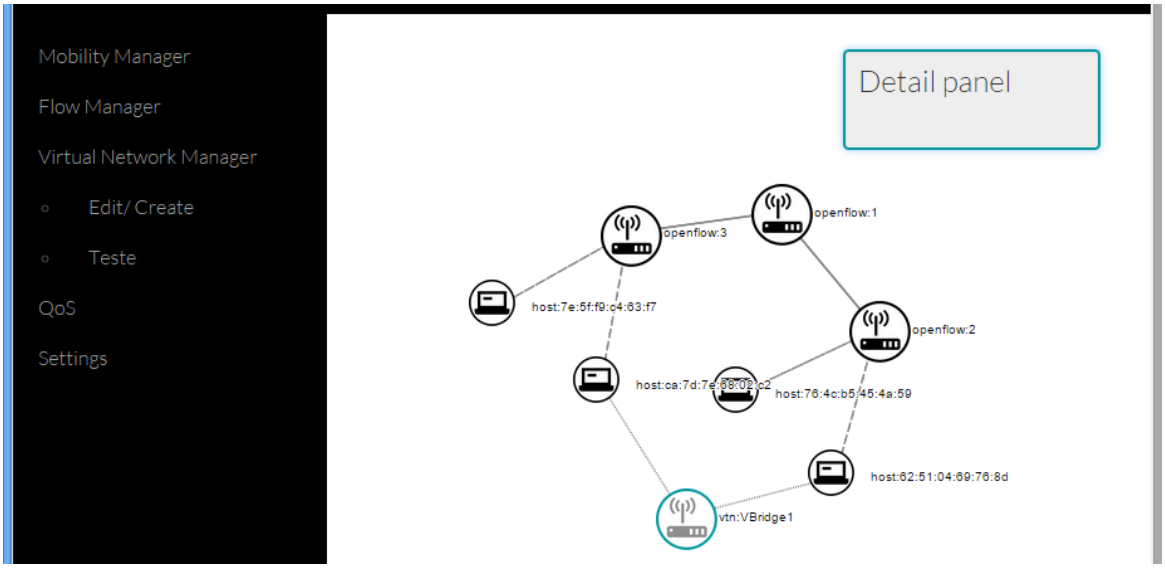
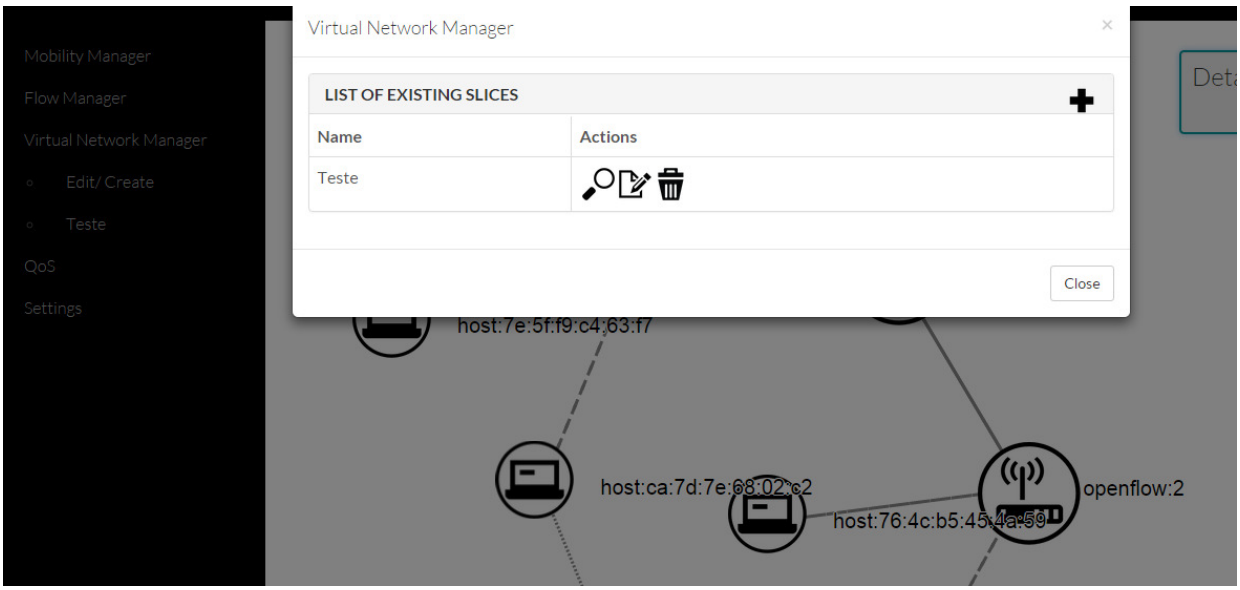


Figura 8 Redes Virtuais

A adição de VTNs é bem intuitiva, ao clicar na aba Virtual Network Manager, um sub-menu é apresentado mostrando as VTNs criadas e um item para Editar e Criar novas VTNs. A Figura 9 apresenta a janela de criação/edição de VTNs. Nela as VTNs criadas são listadas e podem ser editadas ou excluídas, conforme a necessidade do operador. As VTNs são visíveis na tela de topologia, assim como mostrado na Figura , apenas quando são selecionadas no menu.



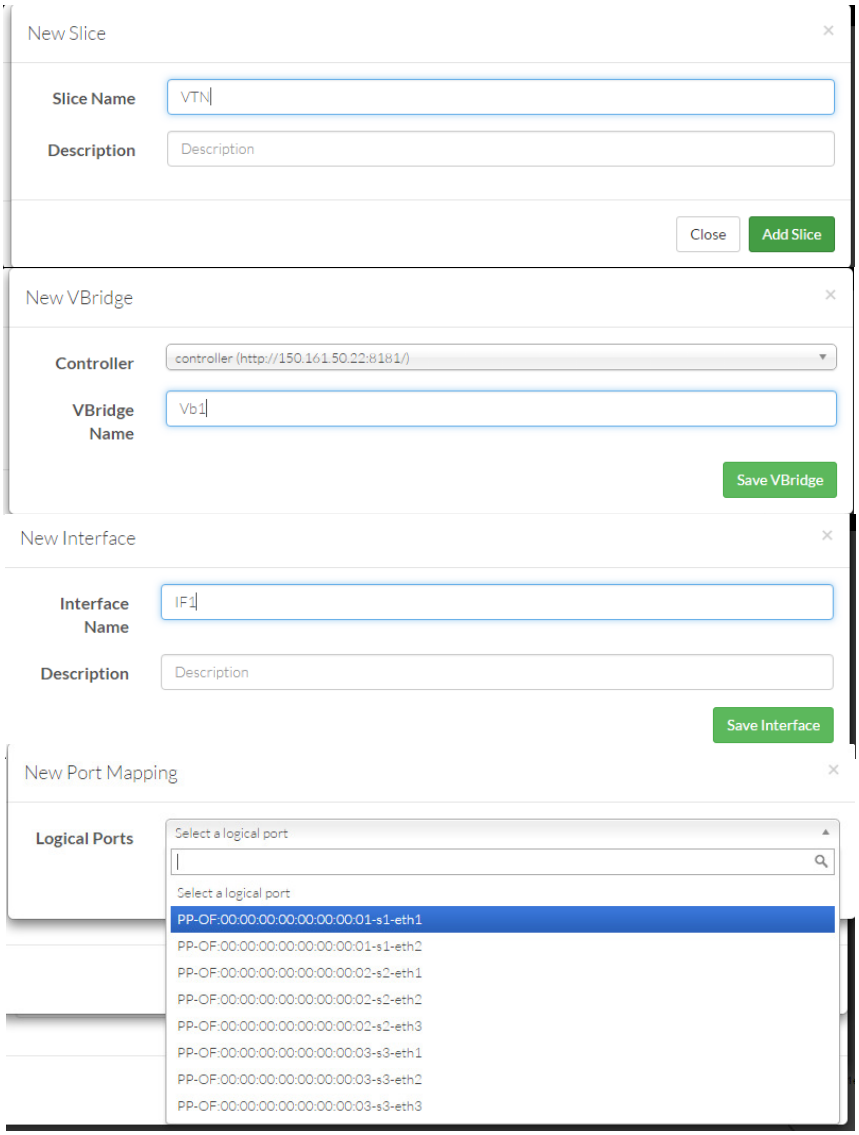


Figura 9 Criação de VTNs

- ***Qualityof Service (QoS):***

É possível também aplicar serviços diferenciados com o WebFlow usando a aba QoS. Nela existem dois sub-menus “Add/ModQueue” e “Add/Mod Meter”. A Figura 10 mostra a janela Add/ModQueue. Nela são listadas as filas instaladas nos switches. No exemplo da Figura 10, existem três filas instaladas no nó openflow:1, todas na porta 1 (openflow:1:1).

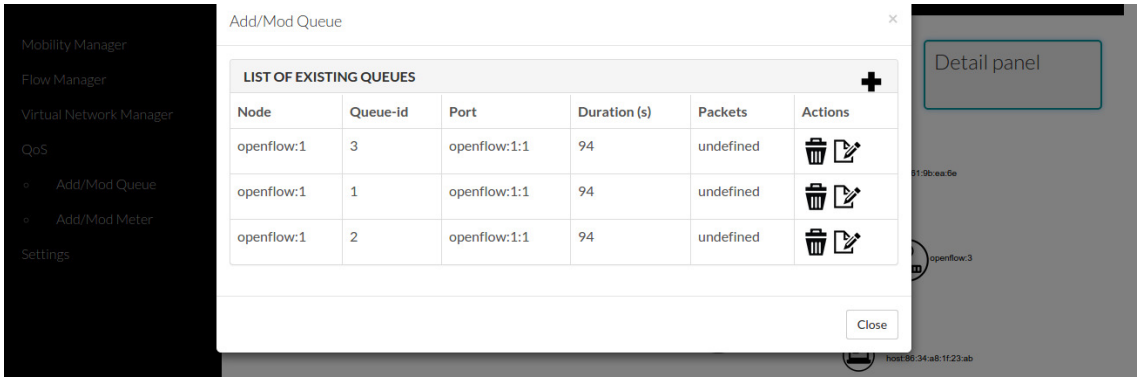


Figura 10 Tela de regras de QoS

Ao clicar em adicionar Queue (sinal de mais no canto direito da tela da Figura 10), a janela da Figura 11 é apresentada. Nela as informações que precisam ser inseridas para a criação de fila são: o ID da fila, o nó o qual será instalada, a porta e a taxa máxima garantida.

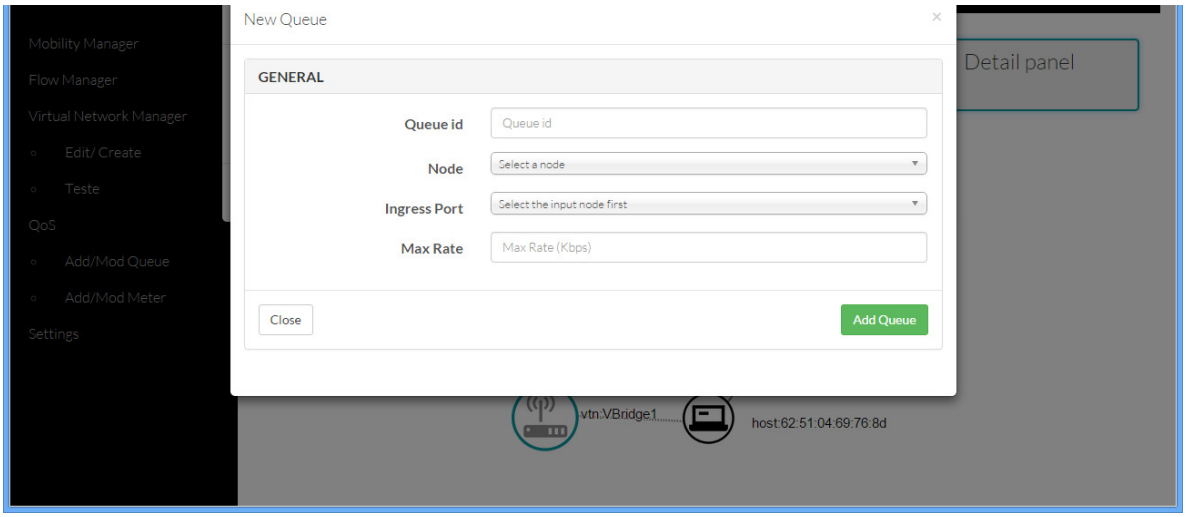


Figura 11 Tela de regras de QoS

O meter é adicionado de forma semelhante. Ao clicar no sub-menu “Add/Mod Meter” a tela mostrada na Figura 12 é apresentada. Nela é possível visualizar os meters que estão instalados nos switches Openflow. No exemplo da Figura , existe um meter no nó “openflow:1” do tipo drop com limitador de tráfego de 500 kpbs.

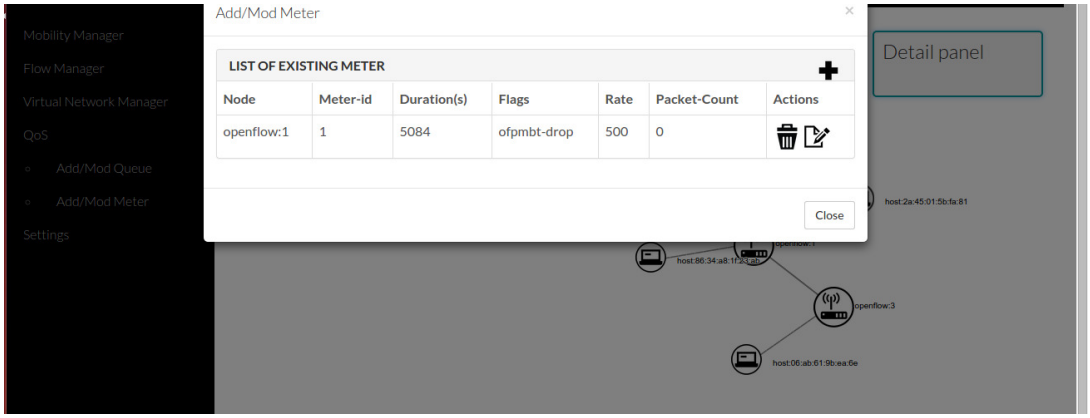


Figura 12 Tela de listagem de meters

A Tela da Figura 13 mostra com é feita a adição de um novo meter. Nela é possível ver que ele é adicionando usando os campos identificador do meter, Nó onde será instalado, Tipo de Flag (meter-kpbs ou meter-ppbs), Rate (limitador) e o tipo de ação, no caso drop.

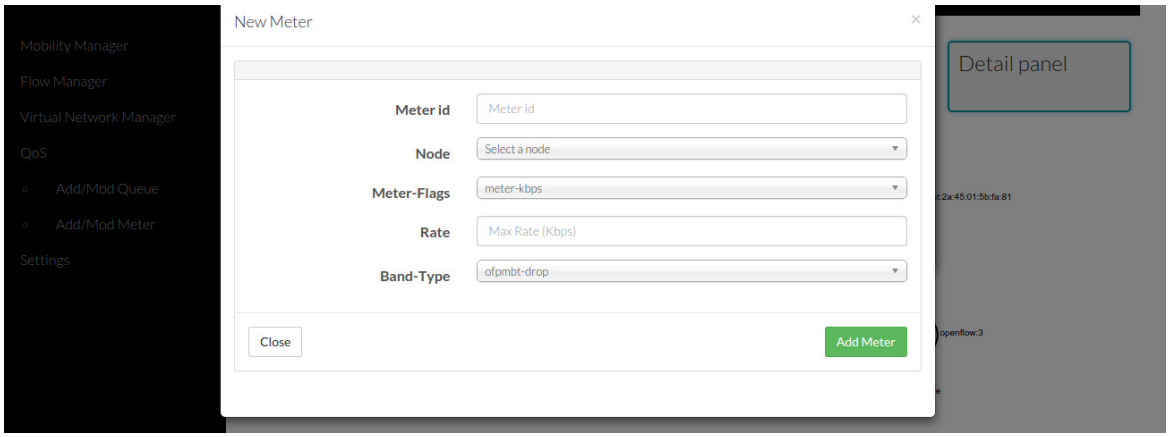


Figura 13 Tela de listagem de meters

- ***Settings*:**

Modifica configurações do WebFlow, como Mapa dinâmico, configurações dos controladores e coordinator (Serviço responsável pela criação de slices de rede). A Figura 14 mostra os principais campos de configuração do ambiente. Na aba “Server Settings”, as configurações do coordinator são adicionadas. Os controladores são adicionados logo abaixo. O WebFlow suporta apenas um coordinator, porém um coordinator pode prover as funcionalidades de VTN para diversos controladores.

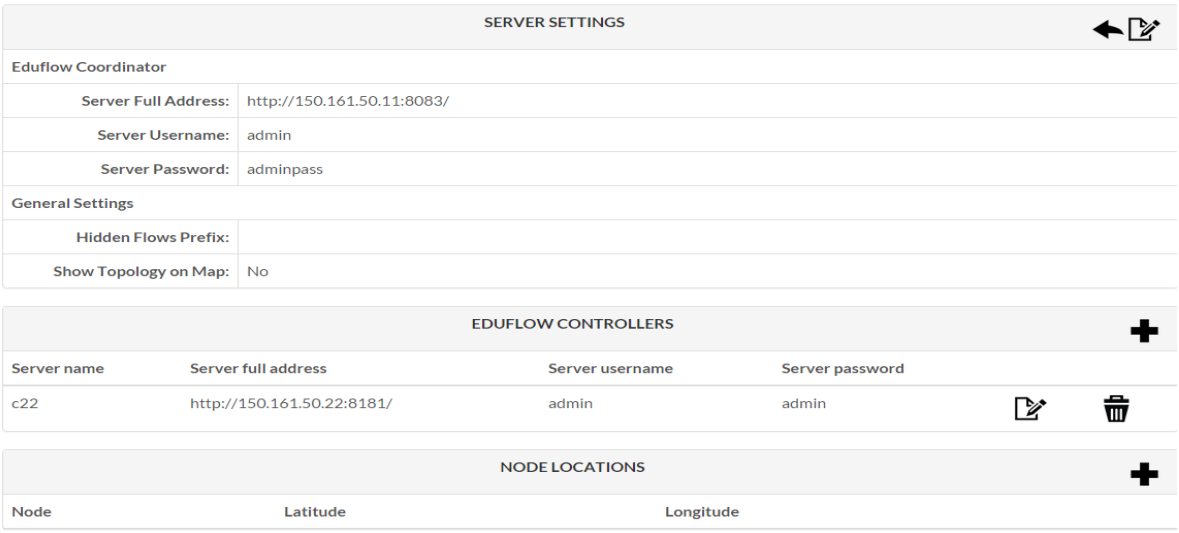


Figura 14 Tela de configuração do WebFlow

A última seção da Figura 14 é a adição de localização dos nós na tela de topologia. Nela, ao clicar no botão de adição de localização, abre-se a janela apresentada na Figura 15. É possível adicionar localizações através de informações de latitude e longitude ou usar o mapa para obter essas informações automaticamente.

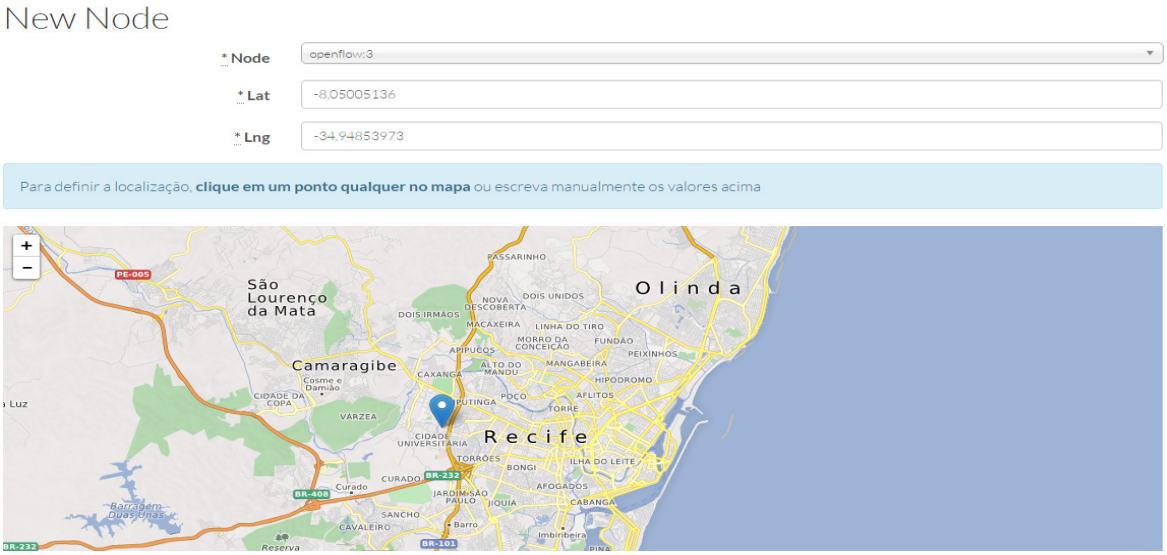


Figura 15 Adição de localização de nós.