Teste de Novos Tipos de Arquiteturas de Rede

Victor Schmeing Thomas, Carlos Adriani Lara Schaeffer

Ciência da Computação – Universidade de Passo Fundo (UPF) – Campus I Av. Brasil Leste, 285 – São José, Passo Fundo - RS

142008@upf.br, schaeffer@upf.br

Abstract. *This paper has the objective to investigate and compare the difference between the network architectures SDN (Software Defined Network) and IP (Internet Protocol) networks. Searching for networks and architectures that are alternatives to current ones, that can be used not only by the scientific community but by the population in general. Tests and comparisons were performed between the two networks as well as a more detailed view of the operation of an SDN network and the OpenFLow communication protocol. It was concluded that the SDN networks for their performance and scalability have a better performance than the current Ips networks.*

Resumo. *Este trabalho tem o objetivo de investigar e comparar a diferença entre as arquiteturas de rede SDN (Software Defined Network) e redes IP(Internet Protocol). Buscando por redes e arquiteturas alternativas às atuais, que possam vir a ser usados não apenas pela comunidade científica mas pela população em geral. Foram realizados testes e comparações entre as duas redes assim como uma visão mais detalhada do funcionamento de um rede SDN e do protocolo de comunicação OpenFLow. Concluiu-se que as redes SDN por sua performance e escalabilidade tem umn melhor desempenho que as redes Ips atuais.*

Introdução

A internet é, atualmente, o maior veículo de comunicação existente. Por consequência redes de computadores estão em todo lugar, desde a grande empresa até a sua própria casa. O problema é que a internet não foi pensada em dar suporte para o que temos hoje em dia.

A internet surgiu na década de 1960, com o objetivo de melhorar a comunicação do exército americano. Acontece que, na época não existia o que há hoje trafegando na internet. A internet não foi planejada á príncipio para trafegar aúdio, vídeo, ou fazer transações bancárias. Essas funcionalidades foram implementadas com o tempo e conforme a necessidade dos usuários.

Diante disso, surgiram novas propostas de rede como as SDN(Software-Defined Network) que são redes controladas por softwares (controladores SDN), em vez dos consoles de gerenciamento de redes e comandos que exigem um grande esforço operacional, tornando complexa a administração em larga escala.

Para compreender melhor por qual razão SDN tornou-se tão importante, precisamos olhar para o que existia antes do mundo SDN. As arquiteturas de rede

tradicionais têm limitações significativas enão estão preparadas para atender a uma demanda de tráfego tão grande e isso deve ser superado para atender as modernas exigências da tecnologia da informação (TI). A rede atual deve ser dimensionada para acomodar maiores cargas de trabalho com maior agilidade, tem de ser de fácil uso, além de manter o custo em um nível mínimo para que possa ser acessível a maioria das pessoas.

Diante dos avanços tecnológicos e de um mundo altamente competitivo em que é preciso estar em constante evolução, torna-se cada vez mais importante uma nova arquitetura de rede que possa atender a demanda das pessoas que buscam cada vez mais pela melhor qualidade de serviço, facilidade e preço acessível porém uma arquitetura de internet criada nos anos 60 não está mais a par de igualdade com as tecnologias apresentadas atualmente.

As redes definidas por software (SDN) expandiram muito nos últimos anos, deixando de ser apenas um tema de pesquisa em universidades para algo concreto, implementado e até mesmo usado em empresas. Nesse artigo é explorado o funcionamento das redes definidas por software, como ela se compara com a arquitetura de rede atual, são feitos alguns testes de comparação de performance e escalabilidade e quais vantagens e desvantagens esse tipo de rede traz.

Também mostramos nesse trabalho os detalhes dos planos das redes definidas por software como o plano de dados, controle, gerenciamento e como os protocolos de SDN podem dar mais flexibilidade e controle para a rede.

A relevância desta pesquisa contribui para estudos e conhecimento da área de redes de computadores como também para o conhecimento de novos tipos de rede e arquiteturas. A pesquisa também tem como objetivo mostrar uma comparação entre ambos os tipos de redes.

1. Problema

As redes atuais estão experimentando um uso de dados enorme através de vários tipos de dispositivos. Com uma demanda por mais recursos e largura de banda, uma sobrecarga de dados é uma constante preocupação para a área de redes. Para fazer alterações em tempo real em nível de aplicativo é preciso a capacidade de reduzir complexidade por automação, coisas que a estrutura de rede IP não fornece.

O modelo atual também não tem o mais eficiente uso de recursos e tempo, em vez disso redes IP tem configurações limitadas que engessam o usuário e levam a uma baixa eficiência de rede (ALGARNI, 2013). Com muitos recursos redundantes de rede as redes IPs pecam na eficiência dos recursos e na parte de automação que requer mudanças em tempo real, algo que a arquitetura de rede IP não é capaz de fornecer.

Entretanto uma SDN pode fornecer controle único sobre um grande fluxo de dados e uma estrutura de redes multifacetada, além de ter uma abordagem de fácil aceitação e amigável ao usuário. O novo modelo de infra-estrutura de software é relatado como sendo mais eficiente e menos provável de enfrentar dificuldades técnicas (ALGARNI, 2013).

2. Metodologia

A metodologia aplicada será a pesquisa bibliográfica e a experimentação prática através da criação de uma maquinas virtual, onde serão instaladas as seguintes configurações:

VirtualBox com uma imagem da máquina virtual(VM) Mininet.

Será usada uma VM Mininet por ela já ter instalado os protocolos OpenFlow e ser de fácil uso e de fácil criação de uma rede SDN.

Será usada uma topologia simples de um controller, um switch e dois hosts.

Na VM Mininet será executado o comando para se criar a rede com controller, switch e hosts e será usado XTERM para abrir o terminal dos hosts para assim executar os comandos criação de server TCP e pedido de request.

Um host servidor TCP: host em que ficará rodando o servidor TCP e que receberá o request de dados.

Um host Client: host que ficará encarregado de enviar o request ao servidor solicitando os dados.

Serão usados 2 computadores ligados a rede da Universidade para comparação de transferência de dados que transmitirão os dados via comando SCP.

Foi usado GNUplot para geração de gráficos.

3. IP ou SDN

Há sempre discussões sobre qual tipo de rede é melhor ou mais eficiente, SDN ou IP. Mesmo com ambas tendo suas vantagens e desvantagens, em maior parte a SDN é superior em relação a IP. ALGARNI (2013, p. 2) define as características principais de uma SDN como "*Key attributes of an SDN environment include its user friendliness, cost efficiency, and reduced complexity*". Isso faz com que seja mais fácil e agradável para os usuários que irão fazer uso da rede, como também mais rápido e de menor custo tornando muito mais acessível de se implementar esse tipo de rede para qualquer pessoa ou empresa.

As SDNs estão diretamente ligadas a simplicidade, adaptabilidade e escalabilidade em qualquer ambiente de rede (COSTANZO, 2012). Nesses aspectos as redes IP não são capazes de se igualar, e por isso, uma quantidade maior de provedores de internet estão usando e confiando mais em sdns. Não só pela sua adaptabilidade mas também por ser amigável aos administradores de sistemas que não precisam mais alternar switches ou fazer configurações manuais. Em vez disso, os administradores de sistemas SDN podem ter controle programável central sobre o tráfego de rede sem a necessidade de acesso direto ao hardware (COSTANZO, 2012).

Sdn fornece controle único sobre a infraestrutura de rede fazendo com que se reduza a complexidade de processos através de automações (COSTANZO, 2012). Isso é beneficial para as empresas porque elas são capazes que gerenciar mudanças em tempo real não só na camada de aplicação mas também na camada de usuário. Os administradores do sistema podem fazer essas mudanças a qualquer momento que for preciso independente da sua localização, isso é possível através da implementação de um sistema de acesso role-based que pode ser acessado remotamente.

Esse sistema é capaz de fornecer segurança e manter hackers e outros invasores de acessar a rede (Koldhofe et al). Infelizmente esses tipos de mudanças em tempo real e remotas não são possíveis em redes IP. Em redes IP os administradores do sistema tem que ter acesso direto ao painel de controle e fazer as políticas de configurações de modo manual para fazer quaisquer mudanças. Qualquer alteração de política de rede requer alterações de hardware o que deixa o sistema rígido e de difícil manutenção.

O SDN permite políticas ilimitadas e altera as políticas de detecção de intrusões, firewalls e balanceamento de carga com alterações no software, o que torna o gerenciamento de redes muito mais flexível.

Outra maneira em que as SDN superam as redes IP em performance é o fato de que ela permite aos administradores indicar serviços de rede sem conglomerar interfaces e especificações ao mesmo tempo (COSTANZO, 2012). Não só permite aos administradores escolher serviços específicos mas também permite eles controlarem os dois planos, já que as sdn são capazes de separar o plano de controle do plano de dados.

Ao separar os planos o administrador tem permissão de tomar decisões referente ao caminho dos dados (Koldehofe et al). Ao separar os dois planos, muitos afirmam que a rede é simplificada, fica mais rápida, menos propensa a ser sobrecarregada e se torna mais amigável ao usuário. Redes Ip são incapazes de fazer isso devido o fato que os dois planos são parte de uma única entidade (ALGARNI, 2013). As redes IPs não podem separá-los por isso não é possível fornecer permissão ao administrador para controlar os planos, isso pode gerar um overflow de dados e falhas na rede.

A SDN é conhecida por quão avançada e amigável ao usuário ela é mas outra vantagem que ela tem é o quão menos provável é de acontecer dificuldades técnicas. Devido aos administradores terem a capacidade de alterar diretamente o software, eles podem alterar as passagens de fluxo de dados garantindo que os pacotes de dados não fiquem em fila e degradem a performance da rede.

Ao garantir que os dados não bloqueem o caminho e nem sobrecarreguem a rede, é menos provável que as redes tenham problemas de funcionamento ou dificuldades técnicas. Outra vantagem é o seu custo. As SDNs são mais baratas que as redes IP por não precisar de tantas pessoas trabalhando nela(COSTANZO, 2012). As empresas podem cortar muito dos seus custos de engenheiros de sistemas e ter somente alguns administradores de sistemas.

Há muitas vantagens em se ter redes SDN em comparação com as redes IP, mas também há algumas desvantagens que não estão presentes nas redes IP. Embora seja superior para o administrador do sistema ter acesso remoto e controle sobre a SDN, ela tem alguns problemas de segurança que são combatidos pelas redes IP.

O principal problema de segurança é o acesso remoto, isso significa que não importa os firewalls da rede se alguém conseguir hackear ele terá acesso as configurações da rede e poderá alterá-las a qualquer momento e também seria possível acessar qualquer arquivo protegido pela rede. As redes IPs não apresentam esses problemas porque para ter acesso a rede você tem que ter acesso ao hardware(Koldehofe et al). Por isso que apenas alguns indivíduos têm acesso ao hardware, fazendo com que o sistema seja mais seguro e menos provável de ser invadido.

Outro ponto positivo das redes IP é a disponibilidade de múltiplas camadas. Essas camadas não podem ser manipuladas e estão embutidas nos dispositivos de rede (COSTANZO, 2012). Isso faz com que não seja possível um mal funcionamento dos fluxos de dados devido a erros dos operadores. Mesmo que as SDNs permitam a manipulação dos fluxos de dados isso poderia gerar problemas de funcionamento na rede que causaria grande prejuízo na capacidade de enviar entre os hosts.

4. Plano de Rede

Redes consistem em uma arquitetura de camadas, que desempenham a parte principal na transferência de pacotes IP do destino a origem, que também é essencial para as SDN. Essa arquitetura consiste em um plano de controle, um plano de dados e um plano de gerenciamento.

O plano de controle é a camada mais importante de uma SDN. Contém controladores que encaminham as regras e políticas para as camadas de infraestrutura, e também controla como os roteadores interagem com os hosts. Ele tem a configuração do sistema, gerenciamento e troca de informações de roteamento contidas em uma Base de Informações(Information Base). Essas bases de dados contém tabelas de vários situações de roteamento com base em prioridades e preferências e também atualizam as tabelas de encaminhamento.

O plano de dados também conhecido como camada de infra-estrutura, representa os dispositivos de encaminhamento na rede. Ele analisa os cabeçalhos dos pacotes, gerencia encapsulamentos, ele basicamente gerencia o tráfego do usuário. Quando os pacotes são originados ou destinados de um roteador eles não passam por seu plano de dados apenas por seu plano de controle. Somente quando os pacotes estão sendo enviados através de um roteador intermediário é quando o plano de dados do intermediário está em uso. O plano de gerenciamento trabalha com o tráfego administrativo para poder gerenciar o tráfego de rede.

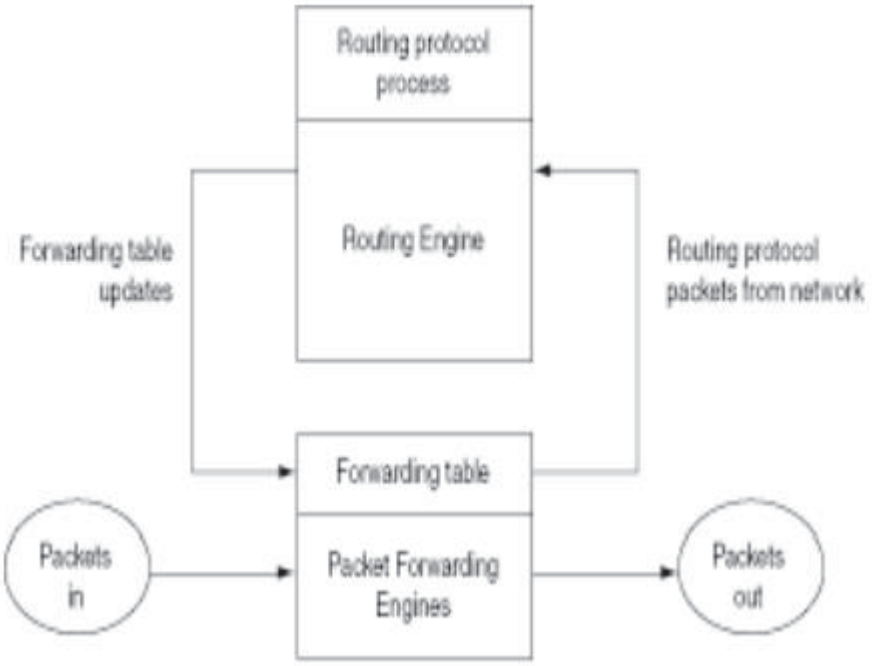


Figura 1. Plano de encaminhamento de um roteador(Algarni, 2013)

O plano de gerenciamento é a interface de comunicação entre uma SDN e o administrador da rede. Por meio dele é possível programar os equipamentos da rede como switchs e roteadores para desempenhar várias funções, além de obter informações sobre o estado da rede e notificações sobre eventos ou erros que possam ocorrerer. Essas funções são realizadas de forma facilitada devido às APIs (Application

Programming Interfaces) que fazem a comunicação entre o plano de gerenciamento e o controlador, além das linguagens de programação usadas nas aplicações desse plano, que fornecem várias abstrações. Isso facilita muito a programação das aplicações e o reuso de código, além de evitar erros e possíveis conflitos entre comandos vindos de várias aplicações diferentes.

5. SDN Controller

O SDN controller é uma entidade lógica centralizada encarregada de traduzir os requerimentos da camada de aplicação para os dispositivos da rede. O plano de controle é removido do switch e colocado no SDN controller. O controlador pode ser programado para fazer decisões de rota, ao invés de ter os algoritmos embutidos no switch. Assim ele permite controle e permite a plataformas inteligentes de rede a usar uma variedade de componentes tecnológicos.

O controlador então transmite a decisão para todos os dispositivos da rede com base no protocolo de comunicação OpenFlow. Os componentes tecnológicos são configurados com certos protocolos para ter uma sinergia com OpenFlow, isso permite aos serviços transferir dados aos switches e proteger qualquer pacote designado pela rede. O OpenFlow atualiza a tabela de fluxo dos switches que é usada pelos dispositivos da rede para mandar os pacotes de dados. Isso permite ao controlador gerenciar o fluxo de controle da rede e assim escolher o melhor caminho dependendo das condições da rede.

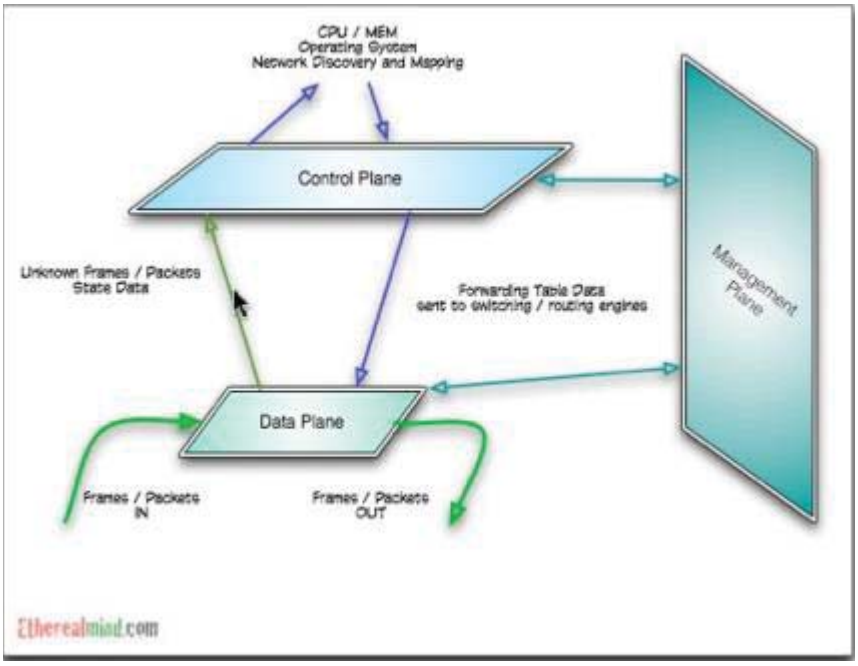


Figura 2. Plano de controle, gerenciamento e encaminhamento(Algarni, 2013)

5.1 Northbound Interface

São interfaces entre as Aplicações SDN e o SDN controller e fornece visão abstrata de rede, ou seja, ela é uma API que faz a comunicação entre o plano de gerenciamento e o plano de controle, permitindo que aplicações utilizadas por administradores de rede efetuem o controle e o monitoramento das funções da rede sem

ter que se preocupar com os detalhes da comunicação. Isso é possível também devido à Southbound Interface, descrita mais adiante.

O principal para essa interface é que um padrão seja estabelecido, de modo que seja gerada uma abstração que independa da linguagem de programação e do controlador. No entanto, estudiosos da área ainda não entraram em um consenso sobre o padrão a ser seguido. Cada controlador especifica sua própria API.

As funções principais de uma Northbound Interface são traduzir os requisitos das aplicações de gerenciamento em instruções de baixo nível para os dispositivos da rede e transmitir estatísticas sobre a rede, que foram geradas nos dispositivos da rede e processadas pelo controlador.

5.2 Southbound Interface

A Southbound Interface é responsável pela comunicação entre os elementos de controle e encaminhamento de dados. Essa é a principal separação entre os planos de controle e dados. Essa interface também é uma API e é por meio dela que os controladores da SDN podem comunicar os requisitos das aplicações para a rede, fazer controle de fluxo, firewall, reprogramar os equipamentos para que eles desempenhem inúmeras funções, sistemas de detecção de intrusos (IDS) e roteamento. Essa reprogramação é feita adicionando ou removendo regras das tabelas de fluxos.

Além disso, essa API é usada para os equipamentos de rede se comunicarem com o controlador. Isso ocorre em três casos:

- Envio de avisos de eventos caso ocorra uma mudança de porta ou enlace.
- Envio de estatísticas de fluxo geradas com o tempo e enviadas para o controlador, de forma a fornecer informações mais detalhadas sobre as características da rede para administradores da rede.
- Envio de pacotes para o controlador em dois casos: se os equipamentos do plano de dados não souberem o que fazer com um pacote, ou seja, quando não há uma regra definida para pacotes com alguma característica; ou quando alguma das regras instaladas no equipamento têm como comando “enviar para o controlador”.

Todos esses tipos de comunicação estão definidos na Southbound Interface mais utilizada, o OpenFlow.

6. Protocolo OpenFlow

OpenFlow é um protocolo de comunicações usado em SDNs que separa o plano de controle do plano de dados. Isso permite controle da rede e fluxo de tráfego de um único ponto. O plano de controle é referente ao mecanismo de roteamento. A criação de tabelas de roteamento e encaminhamento, filtragem, políticas e monitoramento do sistema são todos gerenciados pelo plano de controle. por outro lado, o plano de dados do roteador consiste em interfaces e mecanismos de encaminhamento de pacotes.

Na arquitetura atual o plano de controle preenche a tabela de fluxo que é usada pelo plano de dados para encaminhar os dados ao seu destino. Porém esse modo de funcionamento é rígido já que todos os dados entre dois hosts irão seguir o mesmo

caminho mesmo que seus requerimentos sejam diferentes, por exemplo, um é um pacote de dados de vídeo e o outro é de uma página comum.

Com OpenFlow é possível programar a tabela de fluxo em diferentes switches, isso permite que o destino dos pacotes de dados seja definido pelo programa ao invés do plano de controle. Essa separação entre plano de controle e plano de dados permite que um programa decida o caminho a ser tomado na rede desde que o software seja instalado nos switches ou roteadores. Os dispositivos da rede podem funcionar com um único conjunto de instruções ao invés de vários padrões de protocolos.

O software OpenFlow é instalado na camada de controle e nos dispositivos de rede. O OpenFlow permite permite o controle com base em parâmetros e, como padrões de uso, permitindo respostas às alterações em tempo real nos níveis de sessão e usuário do aplicativo e a identificação do tráfego da rede com base em regras de correspondência predefinidas.

Uma entrada na tabela de fluxo tem três campos:

- Um cabeçalho de pacote que define o fluxo
- Uma ação, que define como os pacotes devem ser processados
- Estatísticas, que controlam o número de pacotes e bytes para cada fluxo.

As três ações principais que podem ser executadas em um pacote são:

- Encaminhar os pacotes deste fluxo para uma determinada porta.
- Encapsular e encaminhar os pacotes desse fluxo para um controlador.
- Descartar os pacotes do fluxo, usado para segurança.

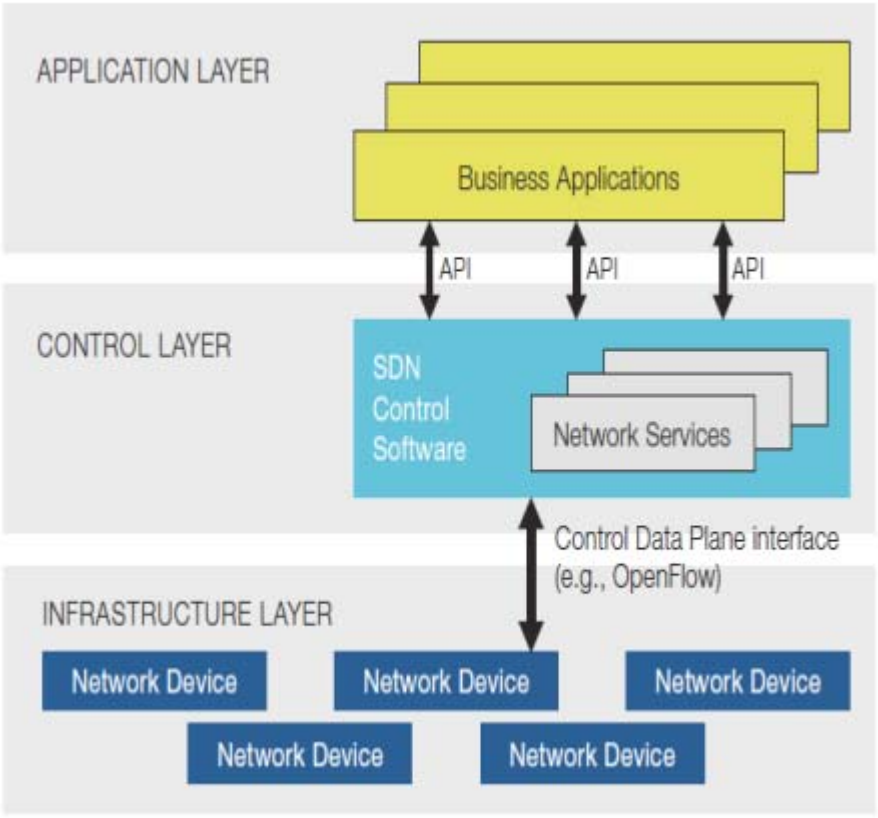


Figura 3. OpenFlow na camada de controle (Algarni, 2013)

OpenFlow pode ser implementado tanto fisicamente como em redes virtuais. Os dispositivos de rede atuais conseguem suportar o encaminhamento da tabela de encaminhamento assim como o encaminhamento definido pelo SDN com OpenFlow o que permite a implementação gradual de redes SDN.

7. Instalação

Para começar a instalação, primeiro será preciso baixar a VM mininet à partir do site http://mininet.org/download/ e importá-la para o VirtualBox. Depois da importação basta abri-la e logar com usuário e senha disponibilizados no site.

8. Testes

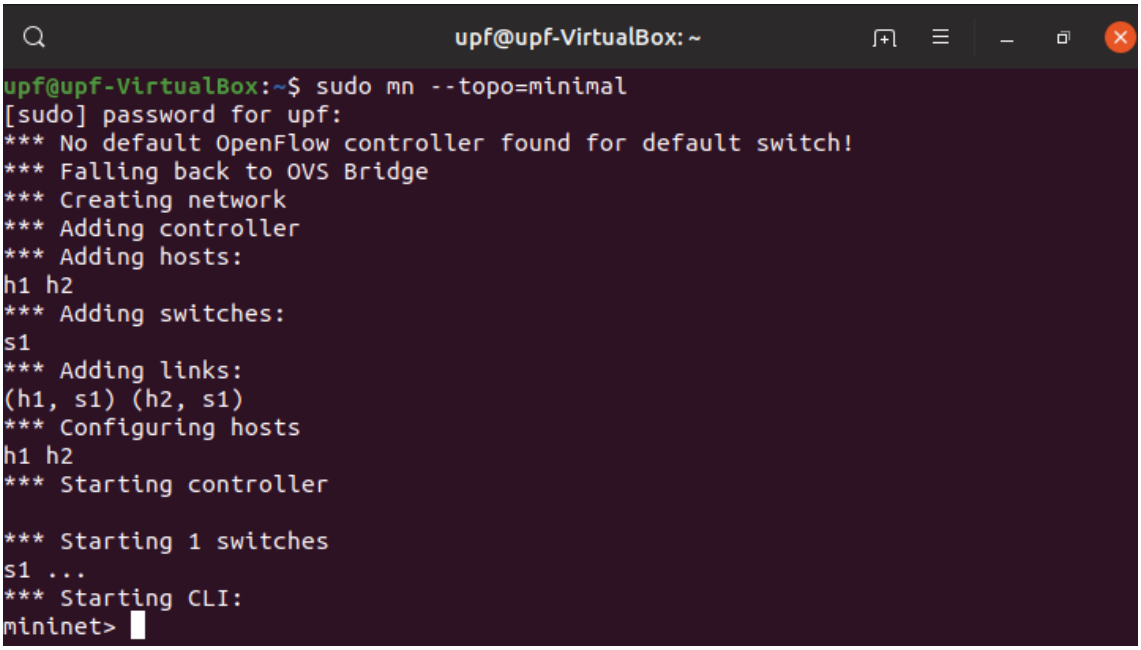
Para os teste na VM foi utilizada uma VM Mininet, por já ter os binários e ferramentas do OpenFlow já pré-instalados assim como algumas configurações de kernel para suportar redes de maior porte.

Para se chegar ao resultado e poder comparar tanto a escalabilidade como a performance de rede entre uma rede SDN e uma rede internet comum foram utilizados computadores do laboratório de informática da Universidade de Passo Fundo. Em relação aos testes foi utilizado uma rede SDN simples com um controller, um switch e dois hosts. Foi usada essa topologia de rede pelo motivo de se ter uma rede que se assemelhasse a rede física para que não houvesse muitas discrepâncias.

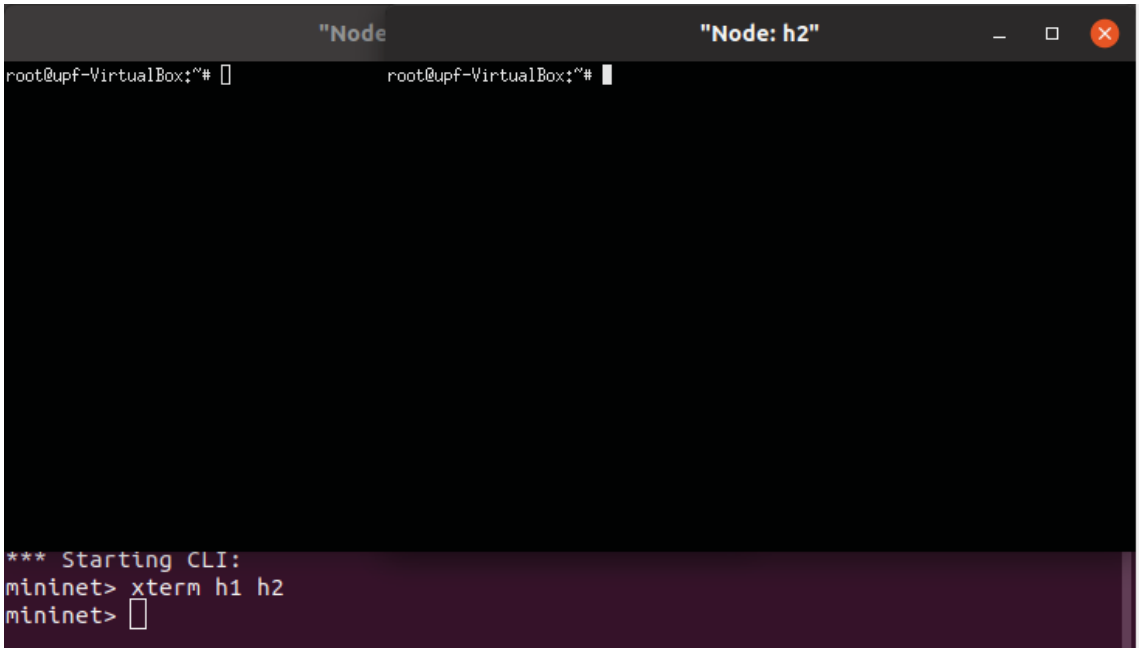
Primeiro foi criada a rede SDN e então foram abertos os terminais de cada host e foi feito um server TCP que receberia o pedido de transferência e um cliente enviaria.

8.1 Resultados da Rede SDN

Depois de seguir os passos de configuração disponíveis no site, basta apenas digitar o seguinte comando: *sudo mn --topo=minimal*.

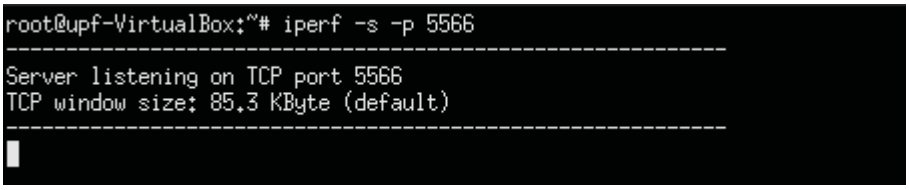


Isso criará uma rede SDN com um controlador, um switch e dois hosts. Em seguida executar o seguinte comando: *xterm h1 h2*.

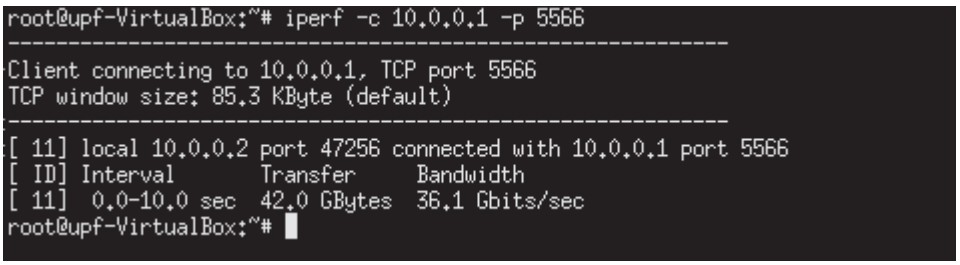


Assim que esse passos forem seguidos basta apenas executar os comandos para fazer o server e o cliente.

Comando de criação de server:



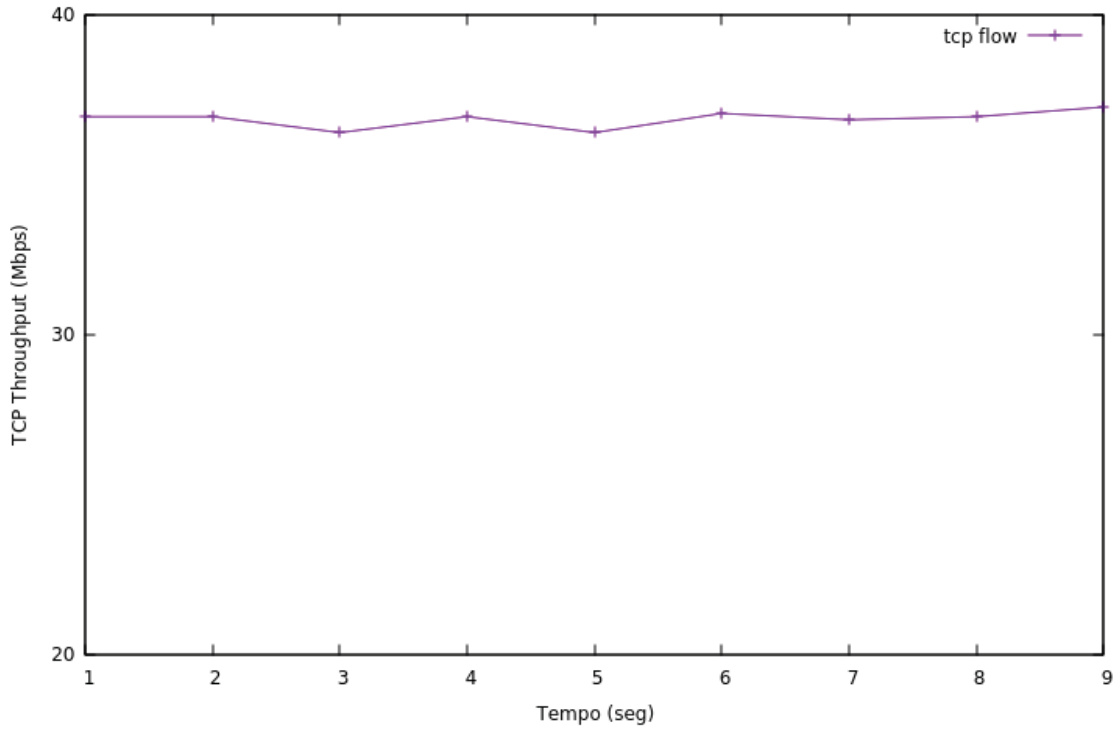
Comando de pedido de client:



Com isso é possível fazer a transferência dos dados entre os hosts. E usando a linha de comando todos os resultados detalhados foram enviados para um arquivo que foi formatado para que fosse possível a geração de um gráfico de Throughput da rede.

Foi usado o GNUplot para a geração do gráfico de rede de Throughput.

Gráfico 1. Gráfico de Throughtput de rede



Depois de várias transferências feitas para se ter certeza do resultado, foi feita uma média das quantidades tranferidas, média de banda e o tempo médio que levou cada transferência.42,600MB 4525MB 12,3

Média Quantidade transferida (GB)	Média de Banda (Gb/seg)	tempo médio em segundos
42,6	36,2	12,3

É possível verificar que mesmo uma simples rede SDN pode suportar uma grande quantidade de tráfego de rede sem problemas assim como uma quantidade de banda de internet consideravelmente alta.

8.2 Resultados da Rede Física

Para se chegar ao resultado e poder comparar tanto a escalabilidade como a performance de rede entre uma rede SDN e uma rede internet comum foram utilizados computadores do laboratório de informática da Universidade de Passo Fundo, ligados a rede de internet da própria Universidade. Foram feitas múltiplas transferências entre os hosts para poder se fazer uma média entre os resultados.

Para as transferências da rede física foram usados apenas dois computadores, isso se deve a dificuldade de se fazer uma rede IP de maior porte por falta de recursos, custos e escalabilidade. Em ambos os computadores foram usados o sistema operacional Ubuntu, a para as tranferências foi usado apenas o comando SCP, pelo motivo de não ser permitida a criação de servers FTP nos computadores do laboratório por motivos de segurança.

Os arquivos enviados eram arquivos de 3 tipos diferentes e tamanhos diferentes para que fosse possível obervar que todos os arquivos foram enviados e recebidos da mesma maneira independente de tipo ou tamanho. Foram feitas várias tranferências desses arquivos e foram tiradas as médias de tempo e velocidade de envio.

Tamanho do arquivo	Extensão	Média de Tempo (seg)	Média de velocidade de envio (MB/s)
853MB	.ova	9	89,5
1669MB	.mp3	19	87,9
1485MB	.mp4	16	88,6

Com isso podemos reparar que se comparado com a rede SDN a rede IP tem uma drástica redução em velocidade de transferência, uma grande parte dessa diferença de performance se deve ao fato das redes SDN usarem tabelas de fluxo o que garante um rápido envio de pacotes entre hosts e servidores com isso ganhando muita performance. Também foi percebido a facilidade de se criar e configurar uma rede SDN em comparação as redes IP. Em poucos minutos pode-se criar a rede e configuração de switchs e roteadores como pode ser feita através de software, torna o trabalho mais fácil.

Outro fator são os custos de uma rede IP em compração com a rede SDN, pela rede SDN ser programável serão necessários menos funcionários para atender a pedidos e falhas da rede, diminuindo também os custos de manutenção. O maior problema encontrado nas redes SDN são falhas que podem ocorrer por erros de programação e problemas de segurança em relação a acesso remoto. Esses problemas não são encontrados em redes IP por se tratarem de redes físicas, em que é preciso ter acesso a hardware.

9. Discussão e Resultados

Com base nesse estudo e teste somos capazes de observar que uma rede SDN tem uma eficácia e performance bastante elevada e muito superior à arquitetura de rede IP. Podemos com base nos resultados afirmar que uma simples rede SDN mesmo sem balanceamento de carga, redirecionamento de pacotes ou outros softwares programados em seus switchs e controllers é muito mais eficiente, tem uma melhor performance e não sofre tanto com problemas de escalabilidade quanto uma rede IP já que em pode-se criar uma rede SDN em pouco tempo e com muito menos recursos. Pelos resultados é possível observar que mesmo uma simples rede SDN consegue suportar uma banda de internet muito alta, com grande quantidade de tráfego.

10. Referências Bibliográficas:

ARQUITETURA. www.gta.ufrj.br, 2019. Disponível em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2015_2/SDN/architecture.html>. Acesso em dia 16/06/2019.

SOFTWARE-DEFINED NETWORKING (SDN) DEFINITION. opennetworking.org, 2019. Disponível em: <https://www.opennetworking.org/sdn-definition/>. Acesso em dia 16/06/2019.

ALGARNI, Manal. Software-Defined Networking Overview and Implementation. Disponível em https://pdfs.semanticscholar.org/a956/f70380eef049403e7c61d6314fdd351db6a0.pdf. Acesso em: 16/06/2019.

SOFTWARE-DEFINED NETWORKING (SDN). searchnetworking.com, 2019. Disponível em: <https://searchnetworking.techtarget.com/definition/software-defined-networking-SDN> Acesso em dia 16/06/2019.

MCKEOWN, Nick. OpenFlow: Enabling Innovation in Campus Networks. Disponível em http://ccr.sigcomm.org/online/files/p69-v38n2n-mckeown.pdf. Acesso em 16/06/2019.

COSTANZO, Salvatore. Software Defined Wireless Networks (SDWN):

Unbridling SDNs. Disponivel em https://www.ewsdn.eu/files/Presentations/EWSDN%202012/1_1_Software_Defined_Wireless_Networks.pdf. Acesso em 16/06/2019.

CANINI, Marco. A NICE Way to Test OpenFlow Applications. Disponivel em https://pdfs.semanticscholar.org/6cfa/183c061337d171c86bf67500df1e0132e059.pdf?_ga=2.1347249.1284496872.1557240947-10596962.1557240947. Acesso em 16/06/2019.

DIEKMANN, Cornelius. Software Defined Networking. Disponivel em https://www.net.in.tum.de/pub/mccn/2013/slides_sdn.pdf. Acesso em 16/06/2019.

REDES DEFINIDAS POR SOFTWARE. www.cisco.com, 2019. Disponivel em: < https://www.cisco.com/c/pt_br/solutions/software-defined-networking/overview.html> Acesso em 16/06/2019.

WANG, Kuang-Ching. Software Defined Networkingand OpenFlow for Universities: Motivation, Strategy, and Uses. Disponivel em https://www.internet2.edu/presentations/fall11/20111003-wang-openflow.pdf. Acesso em 16/06/2019.

LIYANAGE, Madhusanka. Securing the control channel of software-defined mobile networks. Disponivel em https://ieeexplore.ieee.org/document/6918981?tp=&arnumber=6918981&url=http:%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6918981. Acesso em 16/06/2019.

MININET. www.minet.org, 2019. Disponivel em: <www.mininet.org> Acesso em 16/06/2019.

SOFTWARE-DEFINED NETWORK. www.wikipedia.org, 2019. Disponivel em: <https://en.wikipedia.org/wiki/Software-defined_networking> Acesso em 16/06/2019.

SDN ARCHITECTURE OVERVIEW. www.opennetworking.org, 2019. Disponivel em: <https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/SDN-architecture-overview-1.0.pdf> Acesso em 16/06/2019.