PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

CASO DE ESTUDIO PARA UNIDAD DE TITULACIÓN ESPECIAL

TEMA:

Propuesta de implementación de las tecnologías NFV y SDN y su utilización en la red de comunicaciones ***(CASO DE ESTUDIO UTM)***

Maritza Maribel Mendoza Zambrano

Quito – 2016

AUTORÍA

Yo, Mendoza Zambrano Maritza Maribel, portador de la cédula de ciudadanía No.1311496630, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se he respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

_____

Mendoza Zambrano Maritza Maribel

Contenido

1. Introducción

Uno de los principales retos y objetivos de todas las organizaciones es mantener sus servicios internos y externos disponibles todo el tiempo. Esto incluye la integración de diferentes mecanismos que garanticen la continuidad del servicio y que no tenga tiempos “muertos” y que en caso de que surjan fallos se tengan otras alternativas que no afecten las operaciones y entre en funcionamiento de manera automática brindando un servicio estable para los usuarios finales.

En el entorno de las redes de comunicaciones en la actualidad se está dando una conjunción excepcional de innovaciones tanto de arquitecturas como de tecnologías; en los actuales momentos las redes tienden a grandes exigencias para las cuales no fueron diseñadas, desarrolladas e implementadas inicialmente; de esta forma nace el reto de migrar el medio de comunicación para que proporcione mayor rendimiento en la misma.

Las tecnologías que se estudian en el desarrollo de la tesis son NFV (NFV, del inglés Network Functions Virtualization) y SDN (SDN, del inglés Software Defined Network) como sería su aplicación en la arquitectura de redes de comunicaciones del campus universitario, ayudando adecuar la arquitectura a nuevas necesidades.

La principal motivación para el desarrollo de esta tesis es la de proporcionar nuevas tecnologías para la universidad donde la investigadora presta sus servicios profesionales y que esta investigación sirva como guía para la Dirección de TICS (Tecnologías de la Información y Comunicación) aplicando dichas estrategias en entornos corporativos fortaleciendo la continuidad de las operaciones en cada uno de las unidades académicas y administrativas que la conforman.

El conjunto de las tecnologías Software Define Networking (SDN) y Network Function Virtualization (NFV solucionarían los grandes inconvenientes con los que cuentan las redes actuales; en los siguientes años estas redes harán revolucionar la forma de como operarlas, adaptándolas a los abruptos cambios de las muchas demandas del tráfico de la red.

2. Justificación

La presente investigación tiene como finalidad estudiar la arquitectura de red de comunicaciones de la Universidad Técnica de Manabí, realizando una evaluación de la actual arquitectura de red de comunicaciones identificando sus debilidades y su flexibilidad para integrar una nueva tecnología como son SDN, NFV.

La disponibilidad del servicio es un modelo de diseño de infraestructura de red, servicios y sistemas de información que aseguran en cierta medida la continuidad operacional en un período de tiempo determinado, es decir, la capacidad de brindar al usuario de forma ininterrumpida acceso a las aplicaciones o a los servicios de información a lo largo del tiempo. Es por ello que cuando el usuario no tiene acceso a dichos servicios, entonces se dice que no está disponible ([2]López Grande., 2105)

La tecnología Software Defined Networks SDN se enfoca mediante un software que a través de un controlador manejará todas las funciones de las capas de red en un dispositivo, ya que mediante esta tecnología las funciones serán manejadas de una forma fácil y ágil.

Por otro lado, la tecnología Network Function Virtualization (NFV) propone técnicas que se relacionan con virtualización a las estructuras de red, reemplazando los equipos físico conocido como hardware en el mundo de las tecnologías, por máquinas virtuales que pueden ejercer las mismas funcionalidad con las que operan estos equipos físicos, se espera que los diferentes procesos sobre servidores se ejecuten con alta capacidad, esto conlleva en ahorro económico y que estas tecnologías sean más sustentables.

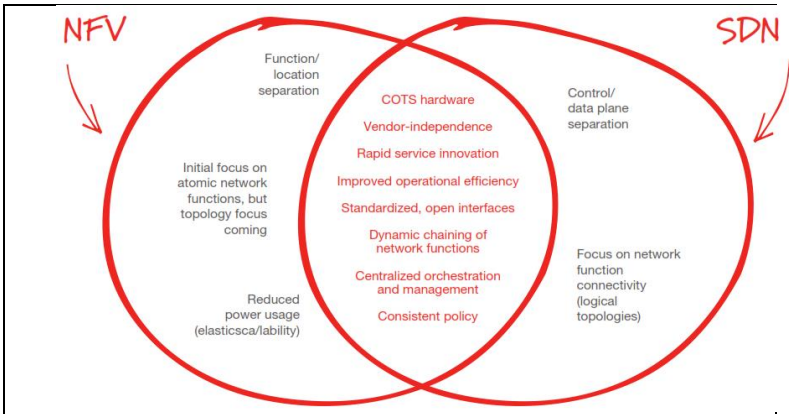


Figura 01: NFV vs SDN, ([3]Advisor, 2014)

En los actuales momentos la exigencias en las redes inalámbricas o alámbricas se debe a la diversa explosión de los dispositivos móviles, de aplicaciones así como la llegada de los servicios en la nube en los sistemas educativos generando visiones de arquitectura escalables dejando de lado a las arquitecturas tradicionales; la finalidad del estudio de este enfoque en las redes conlleva a que los medios comunicacionales tengan una mejor agilidad mediante el uso de herramientas basadas en software y virtualización.

3. Antecedentes

Las redes de comunicaciones han experimentado una transformación que ha permitido ofrecer todo tipo de servicios (voz, datos, televisión, etc.) sobre equipos que operan bajo la modalidad de conmutación de paquetes. Este cambio ha afectado tanto a las redes de cliente como a las redes de operadora, y su paradigma más difundido son las Redes de Nueva Generación.

En paralelo se ha producido un aumento constante de las velocidades de transmisión, tanto en los segmentos de acceso (cableado e inalámbrico) como en los de transporte. Y, sin embargo, paradójicamente, la arquitectura de servicio subyacente se ha mantenido inalterada en lo fundamental: las redes han seguido estando constituidas por nodos dotados tanto de funciones de

control, que permiten establecer el encaminamiento de los paquetes, como de funciones de datos, cuya misión es despacharlos. ([4]Ballesteros Martínez, 2015)

La Universidad Técnica de Manabí cuenta con un aproximado de 12001 estudiantes, 801 docentes y 526 empleados correspondientes al personal administrativo, lo que demanda contar con una infraestructura que soporte este gran número de usuarios en el uso de las redes de comunicaciones de la institución.

4. Objetivos

4.1. Objetivo General:

Estudiar y analizar las tecnologías SDN y NFV de tal forma que se comprendan ambos conceptos con sus ventajas y desafíos para la Universidad Técnica de Manabí.

4.2.Objetivos Específicos:

- Investigar el estado del arte de las tecnologías SDN y NFV.
- Realizar el análisis comparativo entre las tecnologías SDN y NFV.
- Evaluar técnica y económicamente los equipos y soluciones a utilizarse en el desarrollo de la investigación.
- Diseñar e implementar un caso práctico de SDN y NFV para la red de comunicaciones de la UTM.

5. Desarrollo del caso de estudio

En el presente capitulo se explica las tecnologías SDN y NFV, el estado del arte, sus ventajas, desafíos y analogías, además de su uso en las redes de comunicaciones para este caso de estudio.

5.1.Estado del arte de las tecnologías SDN y NFV

Las redes y comunicaciones hoy en día son parte fundamental en las empresas por su alta demanda de datos, voz y video que conlleva a tener una mejor gestión y control del ancho de banda y el ahorro de costos frente a los presupuestos del departamento de TIC. Estas nuevas soluciones permitirán la virtualización del hardware de red, separación de los planos de control y datos; ambas arquitecturas son fundamentales para construir una red definida por software, es decir que los elementos de red dejan de ser dispositivos hardware y se convierten en dispositivos de software.

En relación a lo antes mencionado se expone que la aparición de nuevos protocolos obliga a realizar cambios en las redes y la implementación de nuevos servicios como Cloud Computing, el Internet de las cosas, virtualización de redes. A todo esto, se menciona que la rápida evolución de la tecnología obliga a que las organizaciones independientes de su naturaleza generen nuevas inversiones en hardware y surgen estas soluciones de SDN y NFV que permitirán gestionar las redes de mejor manera.

5.1.1. Software Defined Networking en busca de la automatización de la red.

Dentro de los procesos que conllevan a desarrollar herramientas tecnológicas informáticas comunicacionales, estas han tenido que sortear todo un ejercicio innovador a soportar la demanda a la necesidad de cubrir el mercado de consumo, donde los equipos de red informático ha evolucionado en los últimos años de manera gravitante a su uso, lo que ha exigido vincular

escenarios de la estructura comunicacional de redes a través de un diseño arquitectónico que logre optimizar tal dispositivo, que sin lugar a dudas genera desafíos para toda una organización.

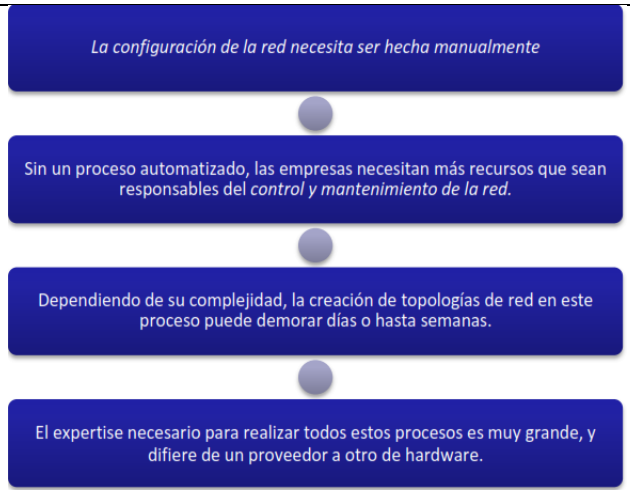


Figura 02: Desafíos de SDN, ([5]Frost & Sullivan CISCO, 2015)

El SDN que cumple el diseño de funcionamiento a través de las redes tecnológicas, conforme a su aplicación ha tenido que superar muchos desafíos en base a la aplicación del mismo; incluyendo a esto el tipo de hardware hacia la implantación de este sistema, donde la utilización del SDN alcance a cubrir toda una estructura diseñada sobre una arquitectura de red, cuyos beneficios todavía no han sido alcanzados de manera óptima por las organizaciones; teniendo en cuenta que la soluciones del Software Define Networkin, permite que toda una red comunicacional tecnológica de una organización surta un efecto orientador a este software, habilitando en su sistema de red beneficios en sus aplicaciones externas y posibilitando el uso de esta herramienta de manera muy fluida.

Esto es notorio que el área de las tecnologías informáticas ha traído cierta agilidad en los mecanismos informáticos de red en las empresas u organizaciones, sin embargo la parte

operativa en su red no alcanza a llenar todo el envío de su información, debido a que dentro del proceso TI el espacio de la nube tecnológica, permite una gran cantidad de tráfico de datos en el mismo sistema. Llevando todo esto a un reñido interés por las empresas latino americana en el año 2014.

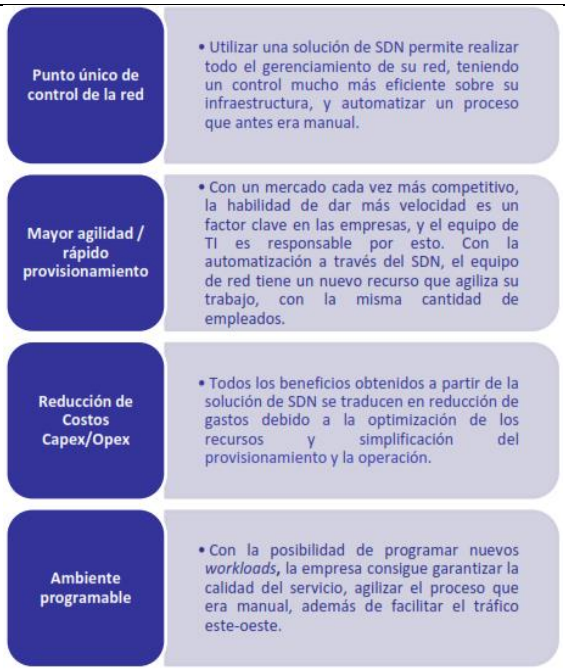


Figura 03: Impactos de SDN en la Infraestructura, ([5]Frost & Sullivan CISCO, 2015)

5.1.2. Virtualización de funciones de Red NFV

NFV, consiste en utilizar recursos de dispositivos genéricos o Centros de Procesamiento de Datos (CPD), para realizar funciones de red, que hasta ahora eran llevadas a cabo por equipos de red especializados. Con la utilización de hardware genérico se reducirá el coste y se aumentará la flexibilidad de la red por la naturaleza configurable que tiene el software. ([7]Huerta, 2015)

El NFV se lo considera con mayores ventajas a los nuevos modelos tecnológicos desarrollados para las computadoras desarrollando el uso del contenido del sistema hardware mediante previsores al uso del switch como distribuidor a los demás lugares de la carga de la nube informática, conectando el trafico virtual y físicos entre las demás máquinas.

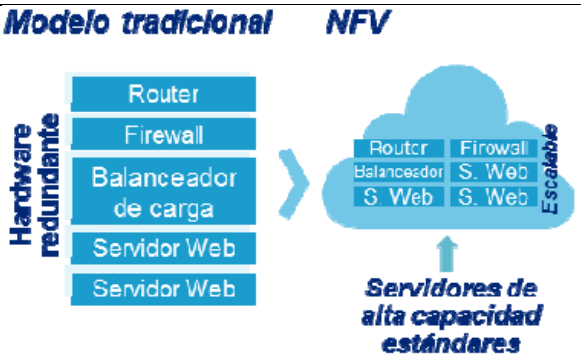


Figura 04: Modelo Tradicional NFV, ([7]Huerta, 2015)

5.1.3. Beneficios y desafíos de SDN y NFV

Beneficios de SDN

SDN apunta a separar la topología en dos sistemas que son, el plano de control y el plano de datos (forwarding). El plano de control provee la gestión de fallas y performance, gestiona la configuración de los nodos de la red y comprende la topología global de la red. Por otro lado, el plano de datos, es el responsable de conmutar el tráfico en la red. ([8]Trigo, 2014)

Los beneficios de implementar SDN en las empresas son varios como se mencionan a continuación. ([9]Adivisor-SDN, 2014).

Reducción de la complejidad

El Software define Netwokin SDN optimiza la gestión de la red virtualizada, en razón a que su aplicación, más allá de reducir el manejo manual de la red informática, disminuye toda inestabilidad a las actividades que se vienen realizando manualmente, que en muchas ocasiones los errores se producen por la configuración, lo que a través del desarrollo de esta herramienta SDN el suministro o distribución responden a ser más ágiles.

Reducción de costos

Considerando al SDN bajo un diseño de su infraestructura más abierta, fácilmente se puede prever su costo beneficio, a la diferencia que hasta la presente el gasto de la mano de obra especializada genera una diferencia determinante al número de profesionales; así como la independencia en la relación con los proveedores, es notorio que al modelo implementado al SND Y NFV los costos operacionales se verán muy reducidos generando mayor beneficios a sus administradores.

Control centralizado y más granular

La nueva arquitectura diseñada a través del SDN garantiza mayor agilidad y flexibilidad en las redes comunicacionales, debido al control centralizado de su infraestructura, lo que permite administrar y/ o diferenciar proveedores a través de un mismo gestor.

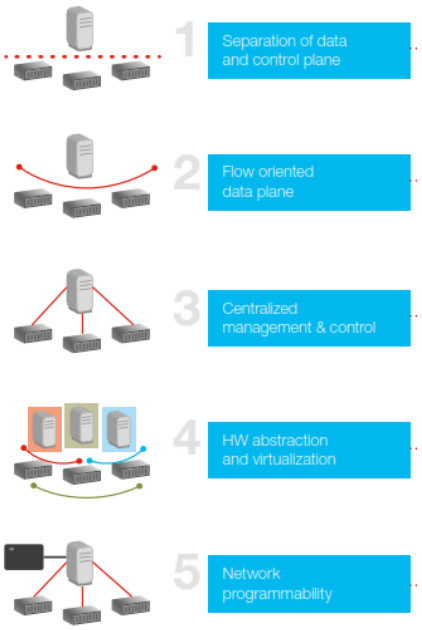


Figura 05: Control centralizado y más granular,

([9]Adivisor-SDN, 2014)

Disponibilidad, confiabilidad y seguridad

Las arquitecturas SDN, de acuerdo a su capacidad de definición pueden generar mayor disponibilidad, confiabilidad y seguridad en el desarrollo de esta herramienta, debido a que elimina la configuración manual en cada uno de sus elementos de red, reduciendo consecuencias negativas al servicio.

Agilidad en el desarrollo de aplicaciones

Las adecuaciones a la infraestructura de red, conforme al requerimiento del usuario final permiten un mayor flujo al manejo de las directrices al tráfico con adaptaciones flexibles en su aplicación; lo que permite que cualquier alteración se refleje directamente en la capa de red.

Las SDN trae varias ventajas en el ámbito de las telecomunicaciones, los resultados que permitirá es obtener redes flexibles sin complejidad que cumplirán los requerimientos de las

demandas existentes; todo esto genera un cambio en la arquitectura y los diversos elementos que conforman de red de comunicaciones pasando a tener en su método operacional de interfaces.

Beneficios de NFV

El NFV con el uso de dispositivos propios, generan beneficios distinguibles, tanto a la administración y al mantenimiento de la red.

Considerando que las inversiones en el mercado NFV crecerán de maneras significativas, cuya previsión se justificaría al hecho de que se está impulsando nuevas tecnologías como el hypervisor de soluciones de computación en la nube

NFV permite reducir el CAPEX Y OPEX, dentro de las inversiones de los equipos, consumo energéticos, logísticos y operacionales; siendo mayores los volúmenes de comprar para una misma infraestructura estándar, generando un mejor aprovechamiento en economía de escala, reduciendo los tiempos de mejoramiento de los hardware en su procesamiento y memoria.

Agilidad en la creación de servicios. - La agilidad que representa la creación de este servicio, por la transformación que surte efecto la aplicación de los interfaces, que respaldan esta herramienta el servicio en una capa o nivel superior; lo que potencializa mayores ingresos a la provisión de servicios a la red.

Mejor time-to-market.- La habilidad para aumentar o disminuir recursos informáticos de manera ágil y rápida. ([3]Advisor, 2014)

Eficiencias operativas: Indica el despliegue de VNF como software utilizando técnicas de administración en la nube que habilitan automatización escalable con un clic del “mouse” del operador (o cliente) o en respuesta a un estímulo analítico de red. La capacidad de automatizar la

incorporación, el aprovisionamiento y la activación en servicio de nuevas funciones de redes virtualizadas puede lograr ahorros significativos. ([10]4G Americas, 2014)

Agilidad de servicio, innovación y diferenciación: Al desplegar estas nuevas VNF, el tiempo de llegada al mercado de nuevos servicios de red puede verse significativamente reducido, y en respuesta a ello se aumenta la capacidad del operador de captar participación de mercado y desarrollar servicios diferenciadores. ([10]4G Americas, 2014)

Los beneficios que traerá NFV es la optimización de costos en la infraestructura al poder virtualizar los servicios y ofrecer un mejor rendimiento de las telecomunicaciones, reduciendo también el consumo energético. Se ofrece también mayor flexibilidad y movilidad permitiendo ajustar dinámicamente la capacidad de los procesos en función de la demanda de los recursos de la red.

Desafíos de implementar SDN y NFV

Los desafíos de implementar SDN Y NFV en la Universidad Técnica de Manabí y en cualquier empresa que desee implementar es analizar la infraestructura de la red, la estandarización de SDN utilizando la plataforma OpenDayLight que es open source, es patrocinada por varias empresas (Huawei, Cisco, Cyan, Ericsson, ZTE, Avaya, Ciena, Juniper Networks, HP Adva Optical, IBM, Coriant, entre otras), contar con el hardware para aprovechar la virtualización de NFV utilizando la plataforma Openstack.

La implantación del SDN a la necesidad de un cambio estructural organizacional al proveedor de servicio, no ha dejado de existir barreras; considerando, que el trabajar con personal bajo una misma rutina de sus procedimientos operacionales, de red planta externa- óptica o IP que nunca hablaban de controladores ni de protocolos, con el uso de este nuevo software, el reto a enfrentar

es al cambio y/o costumbre a cumplir con un tipo de arquitectura plana que beneficie a todo un sistema.

La adopción de las arquitecturas de SDN y NFV no es tarea fácil, estas tecnologías todavía son algo inmaduras, al no existir un modelo único, estas trabajan sobre entornos distribuidos y virtualizados; necesitándose contar con una buena conectividad, este elemento es crítico en las comunicaciones de estas dos tecnologías, y deben analizar latencia y el retardo de las comunicaciones.

El ingreso al nuevo mercado tecnológico para las redes definidas por el SDN, no deja de responder a un cambio de paradigma, donde la única forma de interacción es a través de protocolos e interfaces específicos de la industria, formando un grupo de siglas poco accesibles a este nuevo software.

La integración de NFV en nuestra plataforma actual con estándares virtuales y de diferentes fabricantes, que logre escalabilidad en la red cuando se gestionan múltiples aplicaciones, no están fácil logrando la estabilidad y la simplicidad en la red, pero sí permitirá un ahorro en costo de infraestructura, reducción del espacio a usar en hardware y optimización del consumo energético. Además, se debe tener en consideración la capacitación del personal la aplicación de SDN es compleja y el equipo TI no cuenta con los conocimientos necesarios y la institución debe asignar un presupuesto para la capacitación de los mismos.

Para la implementación de SDN, es necesario que la empresa desarrolle un plan que reducirá la complejidad de su uso y al mismo tiempo entender las necesidades del cliente; por lo que se hace necesario establecer cuidadosamente un socio no tan solo como proveedor de soluciones, sino que logre alcanzar el nivel de servicio ideal.

5.1.4. Arquitecturas y estrategias de seguridad en SDN y NFV

Siendo el SDN una red en arquitectura centralizada, lo que facilita una visión global de la red, a diferencia de las redes actuales, que se construyen sobre una visión de sistemas autónomos, separándolo de un todo en su estado general de la red. Por lo tanto las condiciones de su arquitectura y estrategia de seguridad en SDN permiten a los operadores, desde una misma base o dominio contar con una forma más eficaz de detectar y aislar las amenazas. Lo que permitiría actuar con un software que defina directamente los procesos de enrutamiento en un plan de datos de información tecnológica.

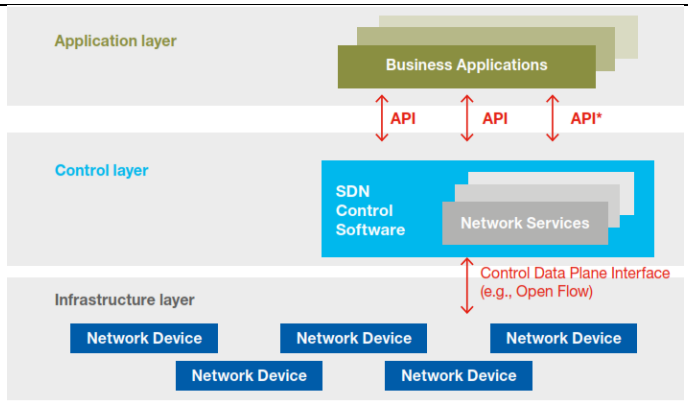


Figura 06: Arquitectura de SDN, ([9]Adivisor-SDN, 2014)

El NFV de acuerdo a su arquitectura de referencia que las entidades al servicio y proveedores cuya guía para definir protocolos y productos relacionados a NFV; esto se pueden sustentar en tres capas principales, considerando desde el nivel más bajo en la jerarquía, siendo:

- **Ambiente virtualizado (Hypervisor):** La plataforma que incluye los componentes físicos, como CPU, memoria y red, preceptuando la denominación Virtual Machine (VM).
- **Virtual Network Function (VNF):** La máquina virtual en función a una red específica como: NAT, FIREWALL Y DPI.

- **Orquestación:** Considerando que la distribución de las VNFs en toda la red corresponde a la conexión entre los ambientes físicos y virtuales, además de la integración de la capa tecnológica puesta al servicio.

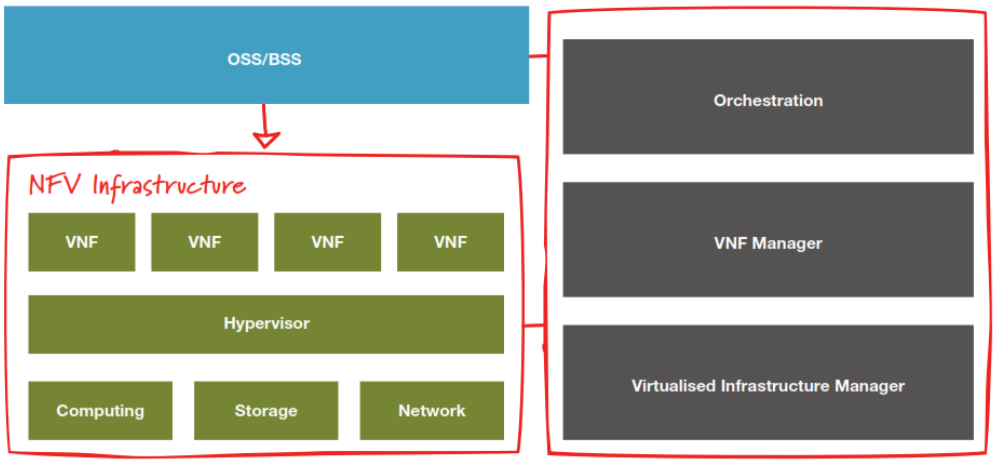


Figura 07: Arquitectura NFV FRAMEWORK, ([3]Advisor, 2014)

El SDN en ejercicio de una red informática, facilita la toma de decisiones inteligentes logrando así la flexibilidad, simplicidad operativa y una mayor seguridad a través de una infraestructura común, dependiendo de una configuración e integración adecuada, se puede asegurar un ambiente de SDN sin afectaciones a las demás capacidades.

SDN puede emular muchas de las funciones básicas de firewall. Los controladores pueden ejecutar secuencias de comandos (scripts) y comandos que pueden actualizar rápidamente las direcciones MAC e IP y el filtrado de puertos, lo que permite una respuesta rápida y cambios a las políticas y normas de tráfico. Esto también libera otros dispositivos de red de la carga de manejar grandes cantidades de tráfico. ([13]Shackleford , 2013)

SDN y NFV pueden aportar mucho al tráfico de red de la Universidad, pero al ser tecnologías nuevas y con estándar no definidos se debe aplicar políticas cuando se separa el plano de datos

del plano de control, si un hacker se apodera del plano de control toda la implementación se iría abajo. Otra ventaja en seguridad que puede aportar NFV es que al tener virtualizado los sistemas y las aplicaciones en caso de un ataque o fallas en el hardware se puede habilitar de manera inmediata solo con la imagen en el respaldo.

Entre las características de seguridad indispensables para cualquier solución de red basada en Cloud Computing destacan los sistemas IDS e IPS, cortafuegos o firewall y redes privadas virtuales ([14]POMEYROL, 2014)

5.1.5. Perfiles de usuarios de SDN

Fabricantes como, por ejemplo, VMware y Nuage Networks (propiedad de Alcatel-Lucent), se encuentran en el primer grupo, mientras que otros como NEC trabajan en un enfoque muy parecido al modelo de la Open Networking Foundation (ONF), que pone el énfasis en la centralización del control de red. HP es un ejemplo de compañía que está intentando cubrir el gap integrando su solución SDN con las herramientas de VMware. ([15]networkworld, 2014)

CISCO está siguiendo su propio camino, la compañía tiene varias soluciones que cataloga como SDN y algunas de ellas se ajustan a los dos enfoques, si bien su modelo difiere en que su Application Centric Infrastructure (ACI) deja parte de la funcionalidad de control en los switches y routers, y utiliza hardware dedicado. ([15]networkworld, 2014)

En el lado de la demanda, están emergiendo cuatro distintos tipos de usuarios de SDN. El primero son las organizaciones de muy gran tamaño. Google, por ejemplo, construye sus propios switches SDN y dispone de una red troncal de estas características que une sus centros de datos. Pero, obviamente, la gran mayoría de las empresas no pueden seguir su propio camino. ([15]networkworld, 2014)

Los proveedores de servicios de red forman una segunda categoría de consumidores de SDN. Muchos ya han lanzado ofertas SDN como servicio –bajo el modelo 'as a service'-, y es muy posible que esta sea la forma en que primero llegue a las empresas usuarias las redes definidas por software. ([15]networkworld, 2014)

Grandes firmas financieras como JPMorgan y Goldman Sachs representan una tercera clase de consumidores potenciales de SDN. Algunas de estas compañías han estado participando activamente en la agenda de la ONF, y muchas ya han realizado pruebas con estas tecnologías. Es probable incluso que estos grandes clientes financieros comiencen a desplegar SDN en producción durante 2015, y que sean las grandes cuentas en general las que lideren la demanda a corto plazo. ([15]networkworld, 2014)

Finalmente, en la última categoría de consumidores de SDN se integran el resto: compañías de todos los tamaños de todos los sectores. De ellas será el futuro de SDN, pese a que hasta el momento sean muy pocas las que ya hayan desplegado la tecnología. ([15]networkworld, 2014)

5.1.6. Establecer la infraestructura de red para NFV

La virtualización NFV introduce unas prácticas de soluciones de nube en las redes de los proveedores de servicios. Las funciones de red se virtualizan y automatizan para su ejecución en una infraestructura de servidor compartida que proporciona los recursos de red, computación y almacenamiento necesarios. No obstante, las funciones de red son más exigentes que la mayoría de las aplicaciones de TI, lo que significa que la virtualización NFV implica requerimientos específicos, entre los que se incluye: ([16]Lemke, 2014)

- **Dinamismo y capacidad de ampliación**. Es necesario que las infraestructuras de NFV sean dinámicas. Deben soportar aplicaciones con una gran capacidad de ampliación que

puedan responder a un entorno de servicios cambiante. Cuando se amplía una funcionalidad VNF o se traslada a una localización diferente, es necesario que las redes sigan operando sin una intervención manual. ([16]Lemke, 2014)

- **Conectividad en un entorno distribuido**. La función principal de la red en NFV - sea o no SDN - es proporcionar conectividad entre los Componentes de VNF (VNFC). La mayoría de las aplicaciones de NFV requieren conectividad a Nivel 2 o Nivel 3. Para algunas aplicaciones también puede ser necesario realizar el control de red a Nivel 1 y Nivel 0 (redes SDN de transporte). Las redes SDN proporcionan: ([16]Lemke, 2014)
    - Direccionamiento IP dinámico o estático
    - Direcciones IP flotantes
    - Servicios multicast / broadcast / anycast
    - Servicios de "middlebox"

Si bien las soluciones de nube de TI se aplican en la centralización y consolidación de los centros de datos, es necesario que los nodos de NFV se distribuyan cuidadosamente a lo largo del área de cobertura geográfica, para garantizar una alta disponibilidad y prestaciones y evitar unas conexiones de agregación y transporte ("backhaul") de tráfico innecesarias a centros de datos centralizados. ([16]Lemke, 2014)

- **Seguridad.** Un requerimiento fundamental de la infraestructura de cualquier operador es un alto nivel de seguridad ante cualquier ataque interno o externo. Por ejemplo, se deberá restringir la conectividad a aquellos elementos que se supone deben hablar entre sí, y sólo se deberá permitir el tráfico de datos autorizado (mediante cortafuegos y grupos de

seguridad). La funcionalidad VNF debe estar suficientemente aislada de cualquier vecino "ruidoso" por razones de seguridad y de prestaciones. ([16]Lemke, 2014)

- **Conexiones con las redes tradicionales.** La introducción de NFV será un proceso gradual y en varias etapas. La interconexión con las redes tradicionales será un elemento crítico para garantizar servicios ininterrumpidos durante la evolución hacia una infraestructura basada totalmente en NFV. ([16]Lemke, 2014)

- **Capacidad y prestaciones fiables.** Las soluciones de VNF soportan frecuentemente un tráfico de datos y de conexiones de medios de altas prestaciones. Debe tener disponible una capacidad de tráfico de paquetes y un ancho de banda suficiente, a través de la red de área extendida y entre los conmutadores virtuales, hipervisores y tarjetas de interfaces de red del servidor. ([16]Lemke, 2014)

Las funciones de red con requerimientos de prestaciones en tiempo real son también sensibles a la latencia y el jitter. Y es necesario que la red garantice la disponibilidad del servicio en caso de fallos o situaciones catastróficas o de fuerza mayor. ([16]Lemke, 2014)

- **Políticas de tráfico y funciones y responsabilidades cambiantes.** En esta época y con la actual tecnología cada servicio incluye su equipo de operación, software y hardware. NFV ofrece operar en una capa común, en el que no será necesario duplicar cada servicio. El enfoque de las tecnologías NFV y SDN es hacia las políticas de tráfico, que asegura una mejor automatización.

5.2. Análisis comparativo de SDN Y NFV

Mucho confunden el término de la NFV con el SDN, o Software Defined Networking o Redes Definidas por Software en español. SDN se centra en la separación de la capa de control de la red, para permitir la creación de redes virtuales, mientras que NFV se centra en la virtualización de las funciones de la red. ([17]Becares, 2014)

SDN y NFV son tecnologías diferentes, pero se complementan entre si y pueden trabajar de manera conjuntan en la infraestructura tecnológica de la Universidad Técnica de Manabí. El enfoque que tiene cada una de ellas es que trabajan con software en la creación de redes y de lo que se a visto en los otros apartados es el de tener redes escalables, agiles e innovadoras.

La función principal de SDN, es la de ayudar a hacer la red más fácil de usar y más programable y compatible con los nuevos protocolos de redes para hacer que su gestión sea más fácil y automática. De acuerdo con los expertos, lo mejor es combinar ambas tecnologías para el mejor funcionamiento de las redes. Y es que el SDN contribuye en la automatización de la red que permite tomar decisiones basadas en políticas para gestionar hacia dónde va el tráfico de red, mientras que la tecnología NFV se centra en los servicios y NV asegura que las capacidades de la red se alineen con los entornos virtualizados que están apoyando. ([17]Becares, 2014)

5.2.1. Características y puntos en común

Estas nuevas tecnologías NFV y SDN se confunden en su concepto, pero en realidad son muy independientes, estas se pueden combinar para separar entre el plan de control y datos, sean virtuales o no, facilite el mantenimiento de la red y procedimientos de operación.

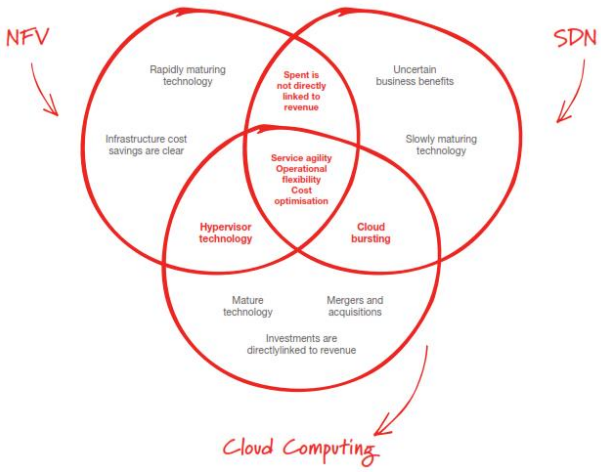


Figura 08: Arquitectura NFV FRAMEWORK, ([3]Advisor, 2014)

En las redes basadas en el software del futuro, Tecnologías de la SDN y NFV son complementarias que abordan distintos elementos de una solución basada en software. SDN aumenta la flexibilidad de la red a través de la gestión integral de la misma, permitiendo la rápida innovación y reduciendo los gastos de funcionamiento. NFV trabaja para disminuir el operador de red de CAPEX y OPEX a través de la reducción de costos de equipo y consumo de energía. ([18]pc-100, 2014). La combinación de ambos puede aportar un mayor potencial a la empresa que se decida por estas dos tecnologías.

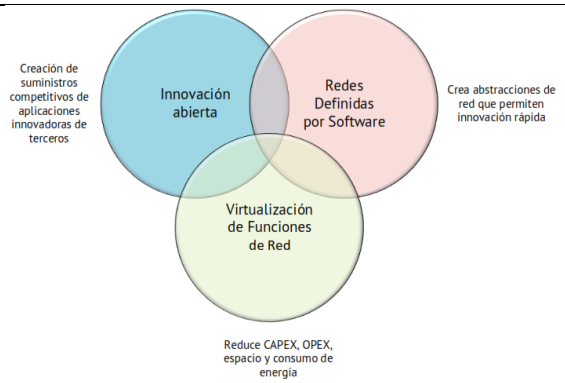


Figura 09: Funciones de Red de relación con la virtualización SDN, ([19]Pate, 2013)

SDN puede mejorar el rendimiento, simplificar la compatibilidad con implementaciones existentes, y facilitar los procedimientos de operación y mantenimiento. A diferencia de NFV que es capaz de soportar SDN, proporcionando la infraestructura sobre la que el software se puede ejecutar SDN. Por otra parte, las funciones de red de virtualización se alinean estrechamente con los objetivos SDN para utilizar los servidores de las materias primas y los interruptores. ([19]Pate, 2013)

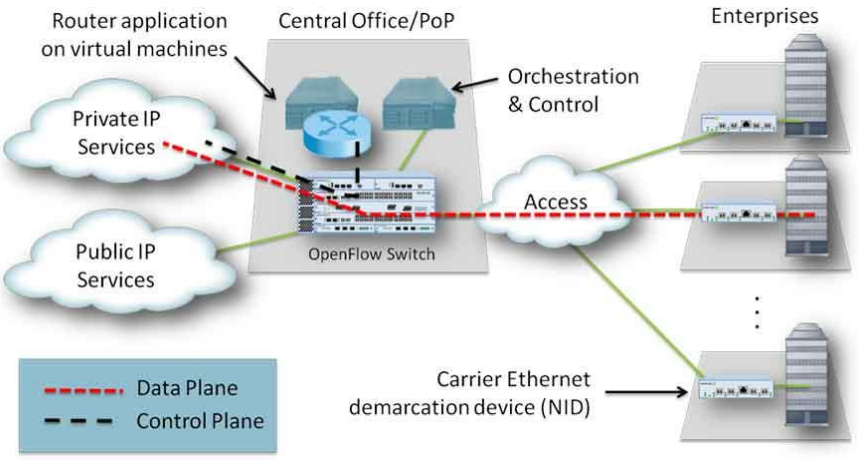


Figura 10: Managed Service Router Utilizando NFV y SDN, ([19]Pate, 2013)

La combinación de la SDN y NFV que se muestra en la Figura 10 proporciona una solución óptima: ([19]Pate, 2013)

- Un equipo de alto costo y dedicado se sustituye por el hardware genérico y software avanzado.

  El plano de control de software se mueve desde una ubicación de equipo de alto costo (en plataforma dedicada) a una ubicación optimizada (servidor de un centro de datos o POP).
- El control del plano de datos ha sido extraída y estandarizada, lo que permite a la red y la aplicación evolucionar sin la necesidad de actualizaciones de dispositivos de red.

5.2.2. Diferencias entre las dos tecnologías

La primera diferencia que se tiene es su origen NFV fue creada por proveedores de servicios de telecomunicaciones y su estandarización es liderado por ETSI, mientras que SDN fue creada por investigadores y fabricantes en un centro de datos.

Estas tecnologías funcionan en la red, mientras que SDN desacopla los planos de control y de datos es decir la inteligencia de red es centralizada, en tanto NFV se centra en la virtualización de red permitiendo el uso más eficiente de los recursos de hardware y licencias software.

NFV es más versátil para su implementación y ejecución, esta puede usar la red tradicional en hardware, mientras que SDN debe construir una nueva red donde el plano de datos y de control, estén separados.

Otra diferencia importante a la hora de hablar protocolos SDN es que utiliza openflow mientras NFV y la ETSI encargada de su estandarización todavía no han creado uno.

5.2.3. Resumen comparativo

Categoría	**SDN**	**NFV**
Razón de ser	Separación de control y datos, la centralización del control y capacidad de programación de la red	La reubicación de las funciones de red de aparatos dedicados a servidores genéricos
Localización del destino	Campus, centro de datos / nube	red de proveedor de servicios
Dispositivos de destino	servidores de conveniencia y conmutadores	servidores de conveniencia y conmutadores
Aplicaciones iniciales	La orquestación de la nube y las redes	Routers, firewalls, gateways, CDN, aceleradores WAN, la garantía de SLA
Nuevos protocolos	OPENFLOW	Ninguno todavía
Formalización	Open Networking Forum (ONF)	ETSI NFV Working Group

Tabla# 01: Cuadro comparativo de SDN Y NFV, ([19]Pate, 2013)

5.2.4. Calificación de posibles Beneficios de SDN

Descripción	Esencial	Importante pero no esencial	Útil, pero no importante	Para nada Importante
Uso optimizado de recursos	35.8%	42%	16%	3.7%
Innovación para redes y servicios	30.5%	46.3%	15.9%	2.4%
Implementación de hardware en menor costo	36.6%	39%	14.6%	4.9%
Reducción de costos operativos, especialmente para mantener equipos distribuidos.	41.5%	34.1%	18.3%	3.7%
Automatización u organización de servicios con más velocidad de servicios.	36.6%	39%	19.5%	3.7%
Coordinación de asignación de recursos de proveedores de servicios de red con redes IP/MPLS Y DC.	37%	38.3%	17.3%	4.9%
Rentabilización de servicios y nuevos servicios.	39.5%	35.8%	17.3%	2.5%

Tabla# 02: Estudio de Heavy Reading sobre operadores de redes, 2013.

5.3. Propuesta de implementación de caso práctico de SDN y NFV para la red de comunicaciones de la UTM.

En esta unidad se realizaron dos casos prácticos en escenario virtual tanto en SDN como en NFV.

5.3.1. Elección del escenario a recrear.

Para la recreación del escenario virtual se utilizará la herramienta MININET la cual permite crear redes virtuales a gran escala y de forma eficiente. En la cual se emulará una red la cual cuenta con dispositivos switches, routers y enlaces en un solo CORE de distribución de UBUNTU Linux dado que esta herramienta permite trabajar SDN y el protocolo openflow.

Características de MININET

- Proporciona una forma sencilla y económica, depara la ejecución de pruebas de red para el desarrollo de aplicaciones OpenFlow.
- Permite a los desarrolladores de múltiples tareas trabajar de forma independiente en la misma topología de manera simultánea.
- Soporta pruebas de regresión a nivel de sistema, que son repetibles y fácilmente envasados.
- Permite realizar pruebas de topología compleja, sin la necesidad de cablear una red física.
- Incluye un CLI que es consciente de la topología y OpenFlow, para las pruebas de toda la red de depuración o de funcionamiento.
- Soporta topologías personalizadas de manera arbitrarias, e incluye un conjunto básico de topologías parametrizadas.
- Es utilizable fuera de la caja sin necesidad de programación.

- También proporciona una API Python sencilla y extensible para la creación de redes y la experimentación (20]MiniNet, 2016)

5.3.2. Herramientas a utilizar

Virtual Box 5.0.2

SDNHUB con Ubuntu 14.04 con las siguientes herramientas incorporadas.

- Controladores SDN: OpenDaylight, Oñós, RYU, reflector, reflector-OF1.3, POX y Trema
- Ejemplo de código para un concentrador, conmutador de aprendizaje L2, control de tráfico y otras aplicaciones
- VSwitch abierta 2.3.0 con soporte para OpenFlow 1.2, 1.3 y 1.4, y el interruptor de LINC
- MiniNet 2.2.1 para crear y ejecutar Ejemplo de topologías
- Pirético
- Wireshark 1.12.1 con soporte nativo para el análisis de OpenFlow
- JDK 1.8, Eclipse Luna y Maven 3.3.3

5.3.3. Escenario de practica en SDN y NFV

Herramienta RYU.

Para el escenario de práctica se utilizará RYU para entender los componentes internos de RYU, los pasos para construir una nueva aplicación en la parte superior de RYU y se introducirá a la programación del controlador. RYU tiene soporte para varias versiones de OpenFlow, incluyendo OpenFlow versiones 1.0 y 1.3.

Lo primero, es ejecutar Mininet en una ventana del terminal con el comando ***$ sudo mn***, el cual inicia un entorno de emulación de red para emular 1 switch con 3 hosts como se muestra en la figura 11.

$ sudo mn --topo single,3 --mac --controller remote --switch ovsk

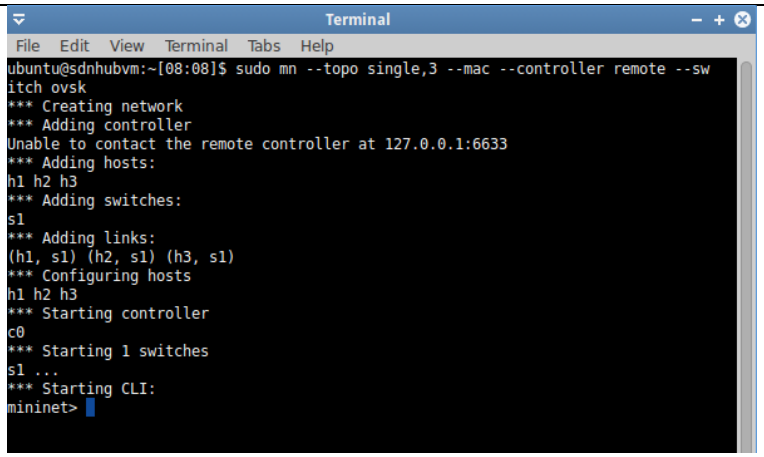


Figura 11: Creación de switch y hosts, ([19]Pate, 2013)

El comando anterior genera 1 switch que tiene soporte para OpenFlow ver 1.0 y 1.3. De acuerdo con sus necesidades, sin embargo, puede forzar un conmutador a soportar OpenFlow 1.3 ejecutando este comando:

sudo ovs-vsctl set bridge s1 protocols=OpenFlow13

El wireshark que forma parte de la VM puede analizar los mensajes de OpenFlow 1.3. Para iniciar wireshark y ver los mensajes de OpenFlow se ejecuta la terminal como se muestra en la figura 12.

$sudo wireshark &

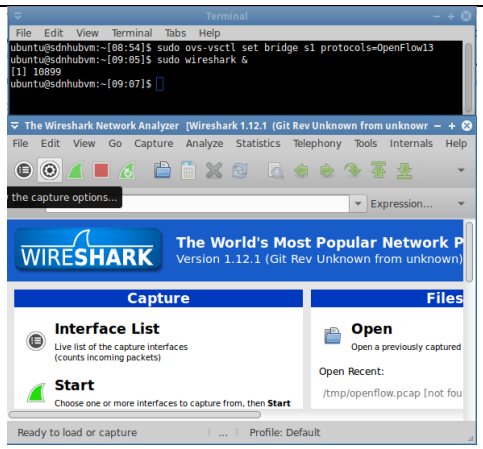


Figura 12: Ejecución de Wireshark, ([19]Pate, 2013)

A continuación, se inicia el controlador RYU. Asumiendo que la carpeta principal donde está instalado ryu es / home / ubuntu / ryu, El comando below inicia el controlador ejecutando la aplicación OpenFlow Protocol Handler y Simple Switch 1.3.

Dado que el conmutador admite OpenFlow 1.0 y 1.3, mientras que la aplicación sólo admite 1.3, el sistema se auto-negocia y decide continuar el OpenFlow 1.3.

cd /home/ubuntu/ryu && ./bin/ryu-manager --verbose ryu/app/simple_switch_13.py

loading app ryu/app/simple_switch_13.py

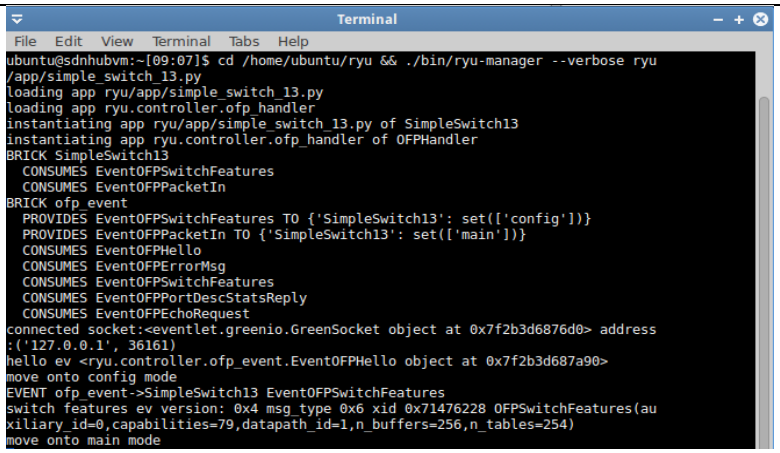


Figura 13: Inicie el controlador RYU

A continuación, se comprueba que los hosts de la topología mininet pueden llegar entre sí como se muestra en la figura 14 y se ejecuta el siguiente comando.

>hi ping h3

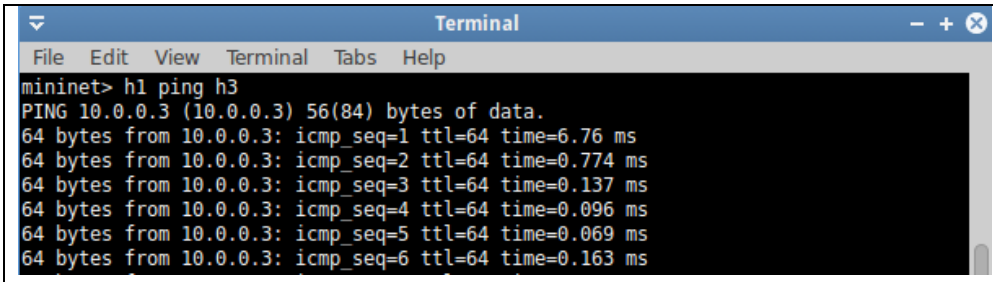


Figura 14: Comprobación de hosts

Estructura del Código RYU

El código del controlador principal se organiza bajo la carpeta / ryu / (En nuestro VM - / home / ubuntu / ryu / ryu /). A continuación, se expone las funcionalidades de los componentes claves. Es importante que se familiarice con ellos.

- App / - Contiene un conjunto de aplicaciones que se ejecutan en la parte superior del controlador.
- Base / - Contiene la clase base para aplicaciones RYU. La clase RyuApp del archivo app_manager.py se hereda al crear una nueva aplicación.
- Controlador / - Contiene el conjunto de archivos necesario para manejar las funciones de OpenFlow (p. Ej., Paquetes de interruptores, generación de flujos, manejo de eventos de red, recopilación de estadísticas, etc.).
- Lib / - Contiene un conjunto de bibliotecas de paquetes para analizar diferentes encabezados de protocolo y una biblioteca para OFConfig. Además, incluye analizadores para Netflow y sFlow también.

- Ofproto / - Contiene la información específica del protocolo OpenFlow y los analizadores relacionados para admitir diferentes versiones del protocolo OF (1.0, 1.2, 1.3, 1.4)
- Topology /: Contiene el código que realiza el descubrimiento de topología relacionado con los conmutadores OpenFlow y maneja la información asociada (por ejemplo, puertos, enlaces, etc.). Internamente utiliza el protocolo LLDP.
- Traductor de Google para empresas: Google Translator ToolkitTraductor de sitios webGlobal Market Finder.

Herramienta Floodlight

El controlador Floodlight Open SDN es un controlador OpenFlow con licencia Java de clase empresarial y con licencia de Apache. Es apoyado por una comunidad de desarrolladores que incluyen una serie de ingenieros de redes de gran cambio.

Características

- Ofrece un sistema de carga de módulos que lo hace fácil de ampliar y mejorar.
- Fácil de configurar con dependencias mínimas
- Soporta una amplia gama de switches OpenFlow virtuales y físicos
- Puede gestionar redes mixtas OpenFlow y no OpenFlow - puede gestionar múltiples "islas" de conmutadores de hardware OpenFlow
- Diseñado para ser de alto rendimiento - es multihilo desde el suelo hasta
- Soporte para la plataforma de orquestación OpenStack (enlace)

Práctica Floodlight

Para realizar la práctica en la máquina virtual se ejecuta los siguientes comandos, que se encuentran en este directorio:

#cd floodlight

Se realiza la ejecución directamente del archivo floodlight.jar una vez que ha ingresado al respectivo directorio como se muestra en la siguiente figura 15.

java –jar target/ floodlight.jar

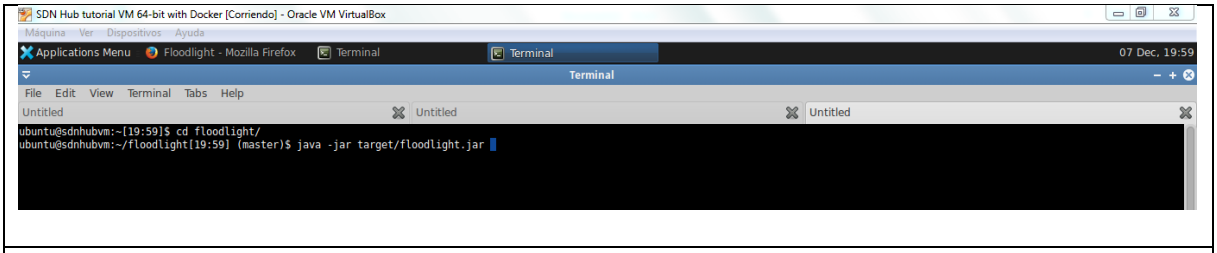


Figura 15: Ejecución de Floodlight.

Una vez que Floodlight se ejecutó, se lo adjuntó a una red OpenFlow. Una de las mejores herramientas para esto es Mininet, una herramienta de simulación de red, que se ejecuta con la siguiente línea según muestra la figura 16.

$ sudo mn --controller=10.0.2.15=<controller ip>,port=6653 --switch ovsk,protocols=OpenFlow13.

Realizar la creación de 1 switch y 4 hosts con la siguiente línea de comando su resultado se muestra en la figura 16.

Sudo mn –topo single,5 –controller=remote, 10.0.2.15, porty=6653 –switch ovsk, protocols=Openflow13

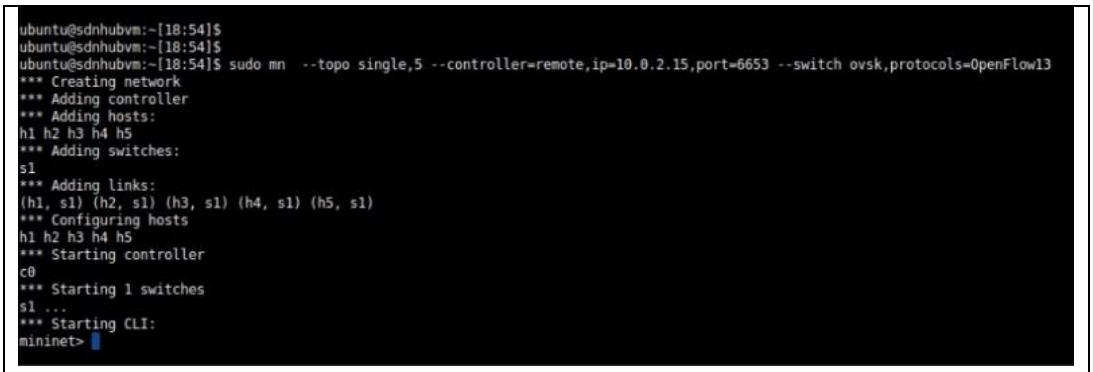


Figura 16: Ejecución de Floodlight creacion de redes.

Una vez creados los 5 hosts y el switch ejecutar la prueba de conectividad realizando un ping.

h1 ping s1, h2 ping s1, h3 ping s1, h4 ping s1.

Además verificar que existe conectividad, tal como se refleja en la figura 17.

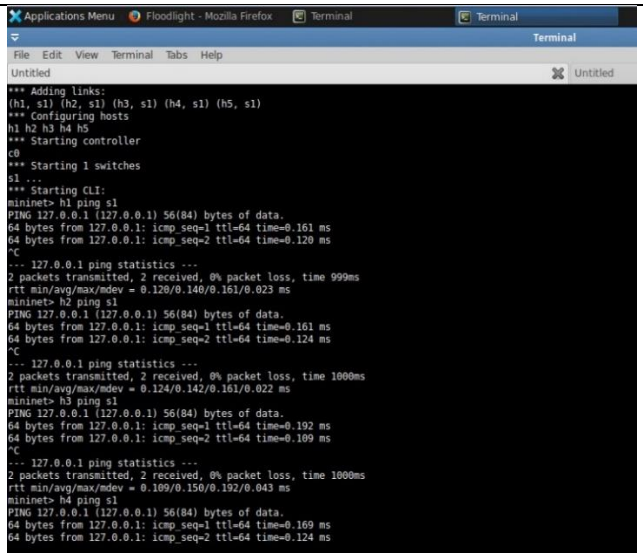
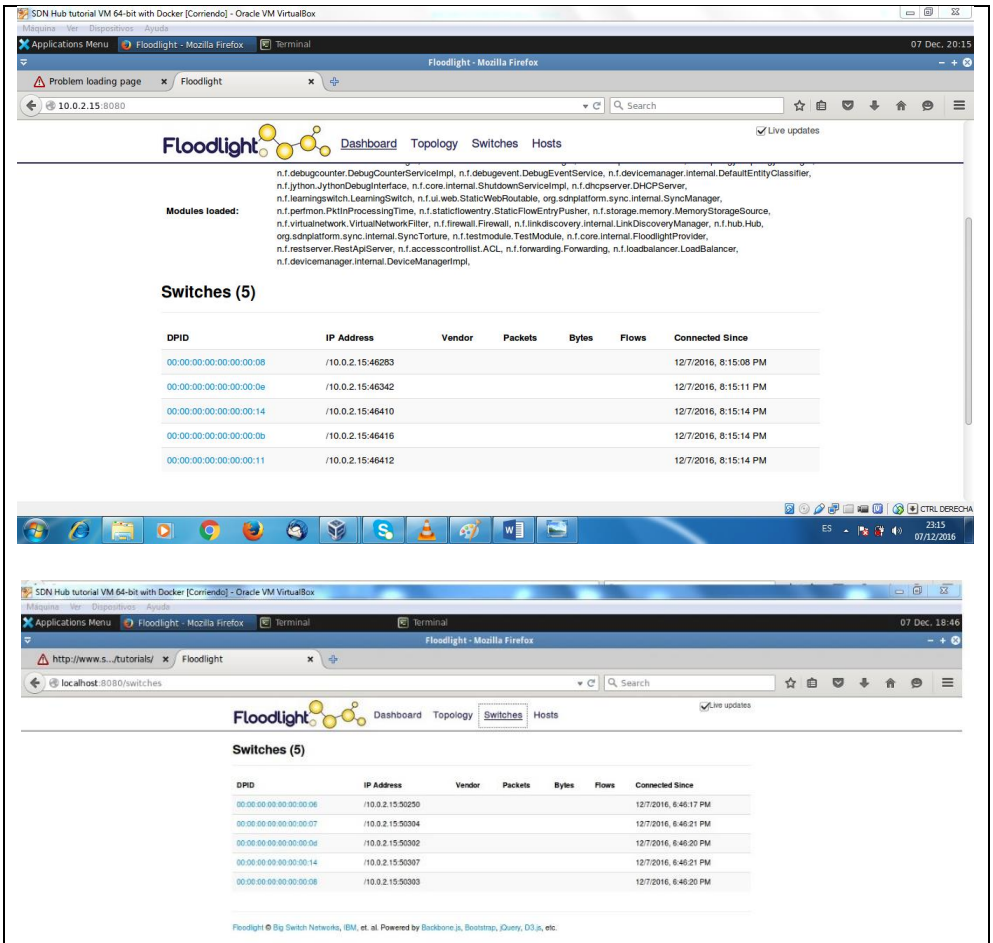


Figura 17: Pruebas de conectividad terminal mininet.

Se debe verificar que se puede ingresar de manera correcta a la interfaz Web Floodlight mediante el navegador, como se muestra en la figura 18:

http://10.0.2.15:8080/ui/index.html o http://localhost:8080/ui/index.html



Figuras 18: Administración de Floodlight

En las figuras 18 se muestran un entorno web para la administracion de esta herramienta floodlight con su respectiva hora de acceso y la IP asignada, en la parte superior se dirigen a los switches; donde muestra la topologia en la figura 19.

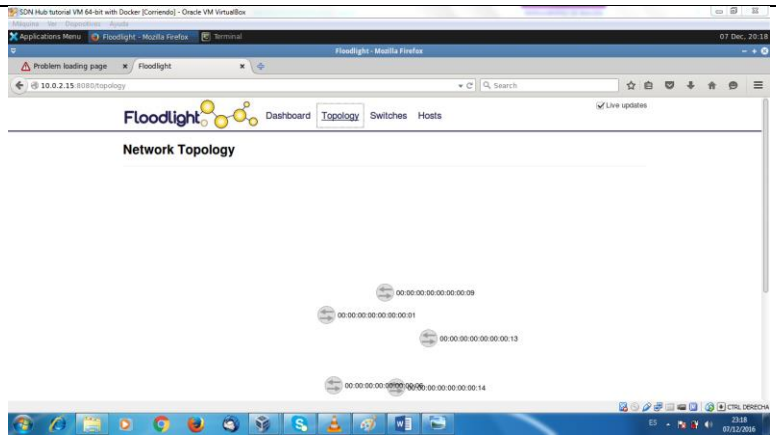


Figura 19: Administración de Floodlight.

Herramientas ONOS

ONOS, Open Network Operating System, es un controlador SDN de código abierto recientemente lanzado que se centra en los casos de uso de los proveedores de servicios. La plataforma está escrita en Java y utiliza OSGi para la gestión de funcionalidades. Similar a OpenDaylight, las características individuales se cargan utilizando el tiempo de ejecución de OSGi llamado Karaf. En la VM del tutorial del concentrador SDN le proporciona una versión pre-compilada de ONOS 1.1.0. Alternativamente, se pone a disposición un repositorio de contenedores de ONOS Docker. ([26] SDN, 2014)

Arquitectura

La plataforma es modular y construida con 1) los intentos de aplicación, y 2) el gráfico de topología de red como las abstracciones de nivel superior que las aplicaciones utilizan para programar el hardware subyacente. Estas intenciones se traducen a las reglas de OpenFlow que se programan en los conmutadores que usan el complemento southbound. A continuación, se muestra una arquitectura de alto nivel de ONOS. En la capa de aplicación superior, muestra la lista de aplicaciones de ejemplo incluidas en las versiones actuales. ([26] SDN, 2014)

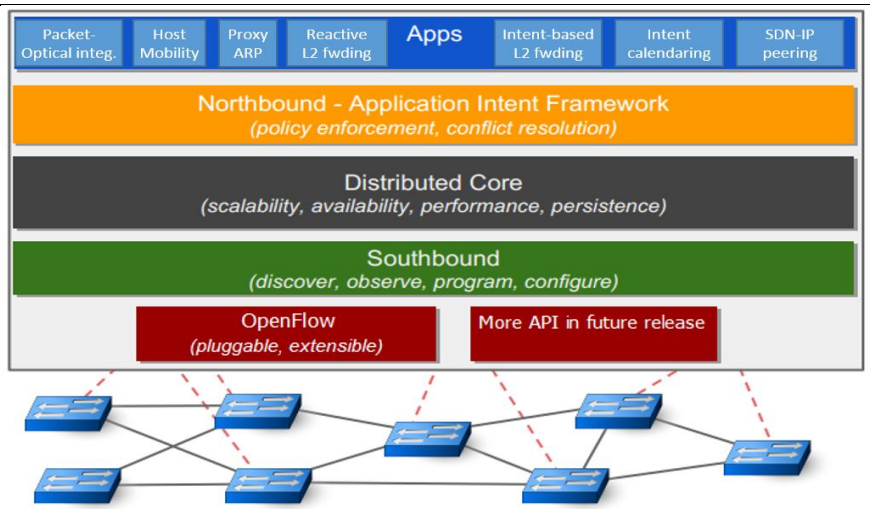


Figura 20: Arquitectura de ONOS. ([26] SDN, 2014)

Practica ONOS

Configurar las variables de entorno para la ejecución de ONOS y Karaf

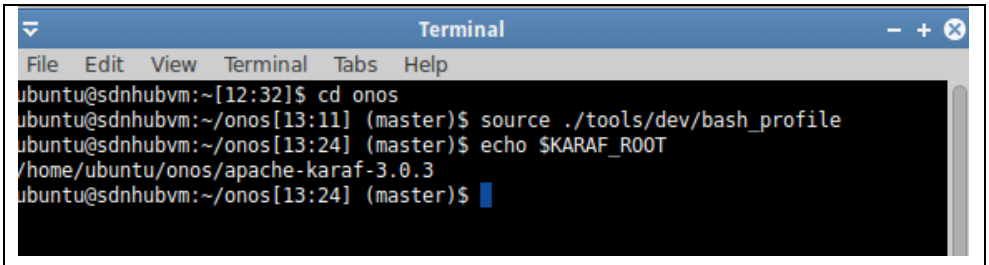


Figura 21: Configuración de ONOS.

Compilar el controlador utilizando los comandos:

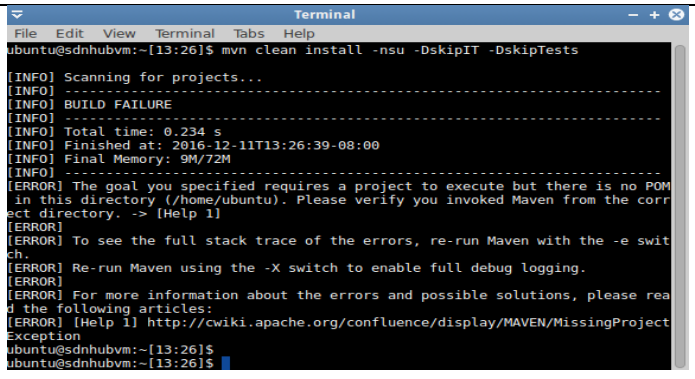


Figura 22: Configuración de ONOS controlador.

Ejecutar el controlador implica cargar los módulos necesarios. Como mecanismo de verificación, se visualiza el banner de ONOS impreso en la pantalla. En este punto, el controlador escucha en el puerto 8181 para UI, y los puertos [6633, 6635 y 6635] para OpenFlow figura 23.

ubuntu@sdnhubvm:~/onos[13:24] (master)$ karaf clean

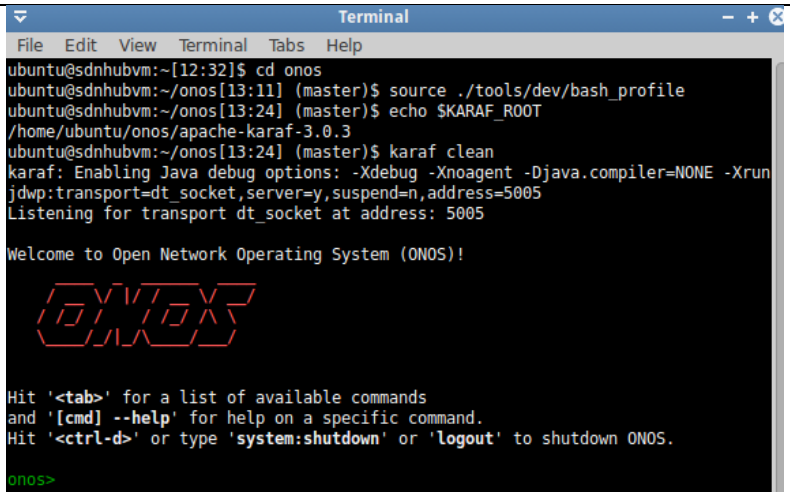


Figura 23: Controlador ONOS.

En la instalación de VM, se precargan ciertas características al incluirlo en ~ / onos / apache-karaf-3.0.2 / etc / org.apache.karaf.features.cfg archivo en la clave featuresBoot, ejecutando el núcleo ONOS en una sola instancia. Se debe comprobar que se cargaron todos los archivos ejecutando el comando en la consola Karaf:

onos> feature:list -i

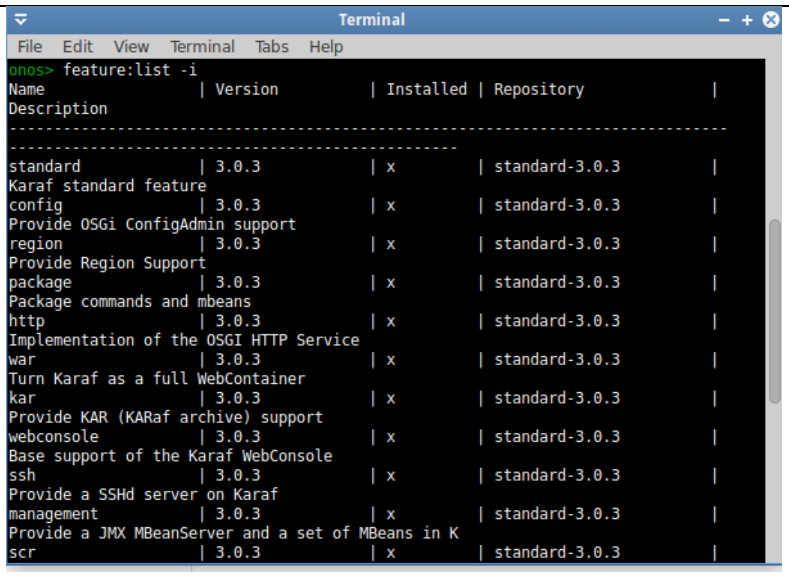


Figura 24: Comprobación archivos de ONOS.

Puesto que la característica OpenFlow y la función de reenvío iniciada, se puede conectar uno o más conmutadores al controlador y administrar el reenvío. En la VM de tutorial, puede iniciarse mininet para emular una red de conmutadores y hosts mediante este comando resultado en la figura 25:

sudo mn topo linear,2 mac switch ovsk,protocols=OpenFlow13 controller remote arp

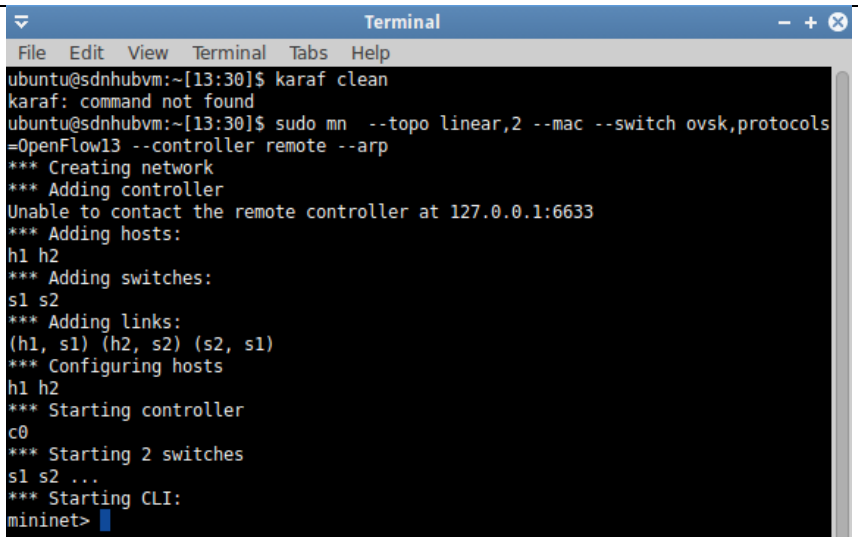


Figura 25: Emular una red de conmutadores.

mininet> h1 ping h2

PING 10.0.0.2 bytes of data.

Para controlar los hosts ya ejecutados por el controlador, utilizar el comando hosts de la consola Karaf:

onos> hosts

5.3.4. Escenario práctico de la herramienta SDN

5.3.4.1. Balanceo

En primera instancia de debe crear una topología de un swicth y 6 equipos, de los cuales 3 van a ser host y 3 servidores web; según muestra la figura 26:

sudo mn --topo single,6 --mac --controller=remote,ip=192.168.56.1,port=6633 -x

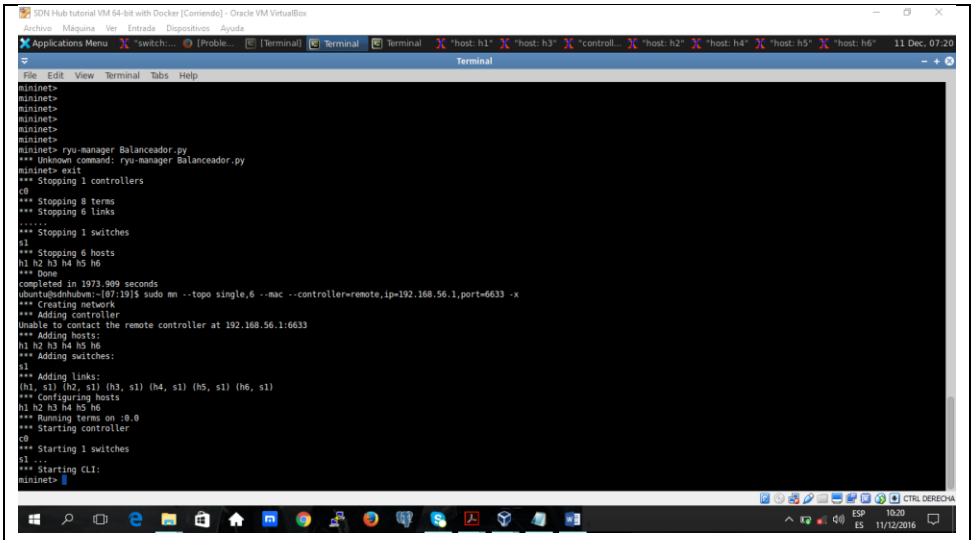


Figura 26: Creación de topología.

Luego asignar a lo hosts h4, h5 y h6 como server web, ver figura 27:

h4 python -m SimpleHTTPServer 80 &

h5 python -m SimpleHTTPServer 80 &

h6 python -m SimpleHTTPServer 80 &

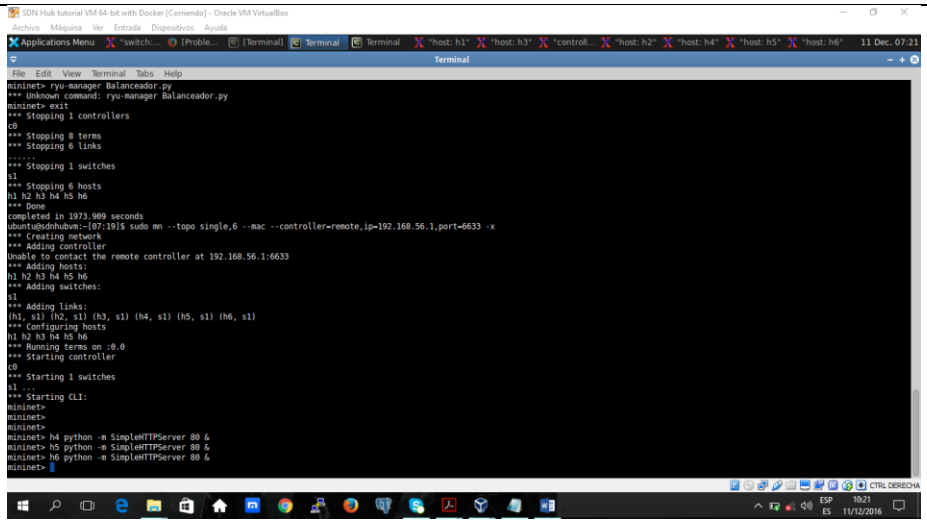


Figura 27: Designación de hosts.

Seguido se debe definir la versión de OpenFloW a utilizarse, figura 28.

ovs-vsctl set bridge s1 protocols=OpenFlow13

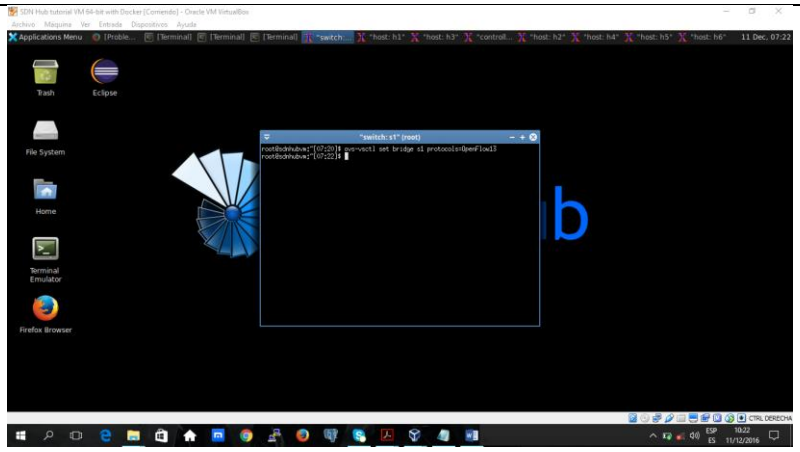


Figura 28: Designación de hosts.

Para realizar prueba y análisis de paquetes, con wireshark es necesario ejecutar el siguiente comando:

sudo wireshark &

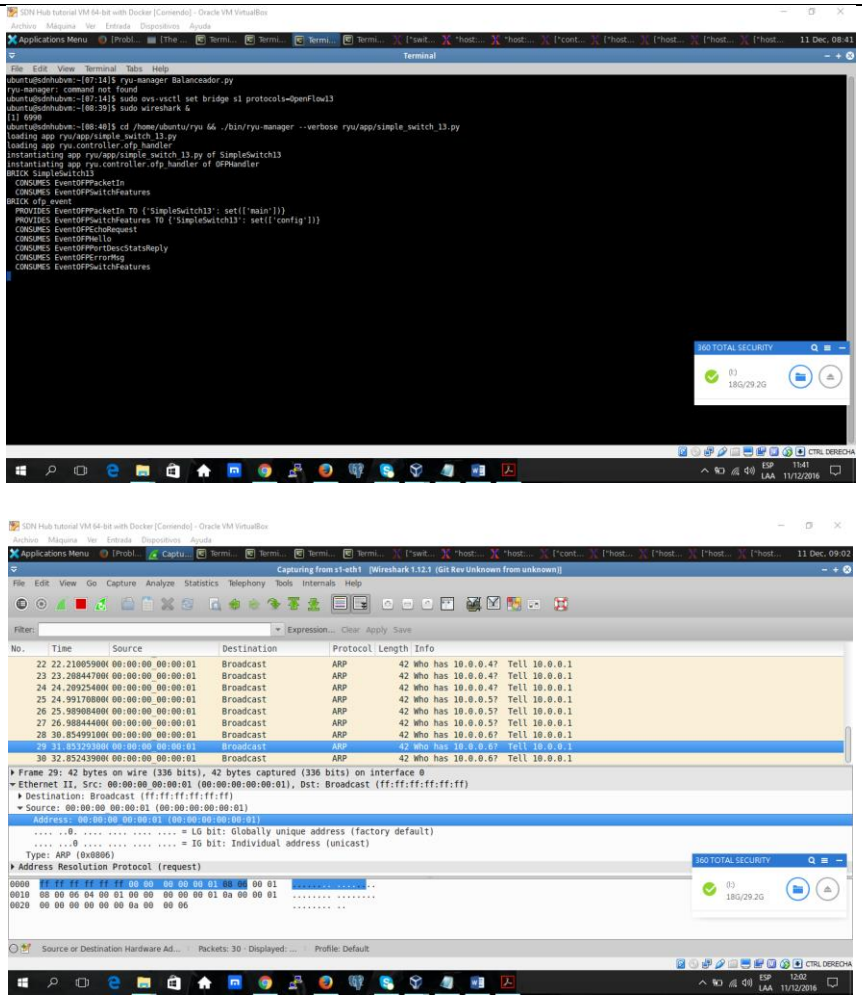


Figura 29: Ejecución de Wireshark.

Luego los profesionales en tecnologías deben realizar pruebas en el mininet sobre el balanceo con el comando resultado figura 30:

ryu-manager Balanceador.py

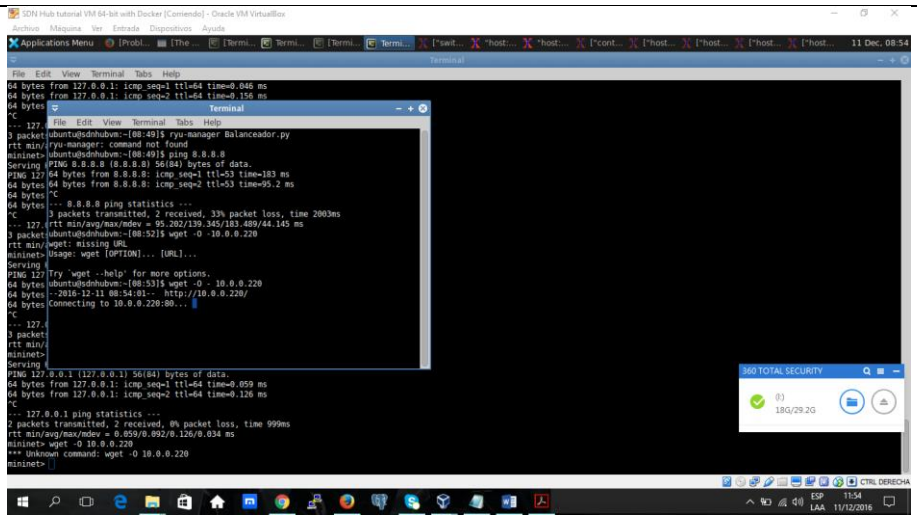


Figura 30: Pruebas de balanceo.

Finalmente es recomendable verificar el flujo de datos en el Swicth1 con el comando ovs-ofctl dum-flows s1

5.3.4.2 Calidad de servicio SDN

Continuando con la práctica crear la topología

sudo mn --mac --switch ovsk --controller remote –x

xterm c0

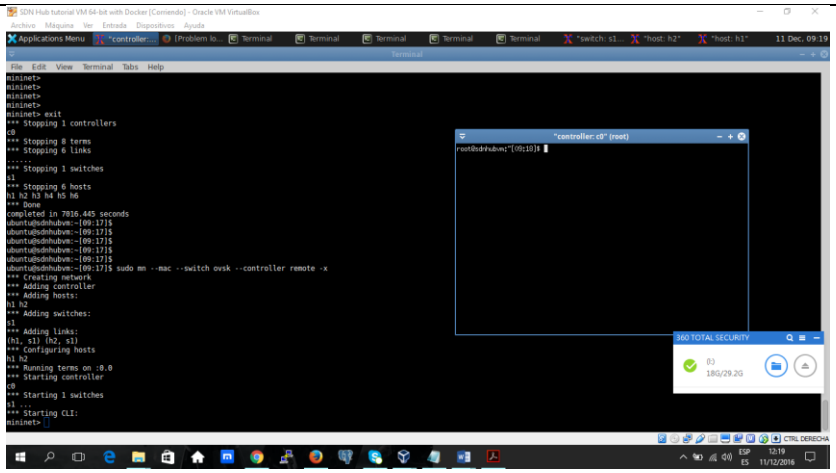


Figura 31: Creación de topología.

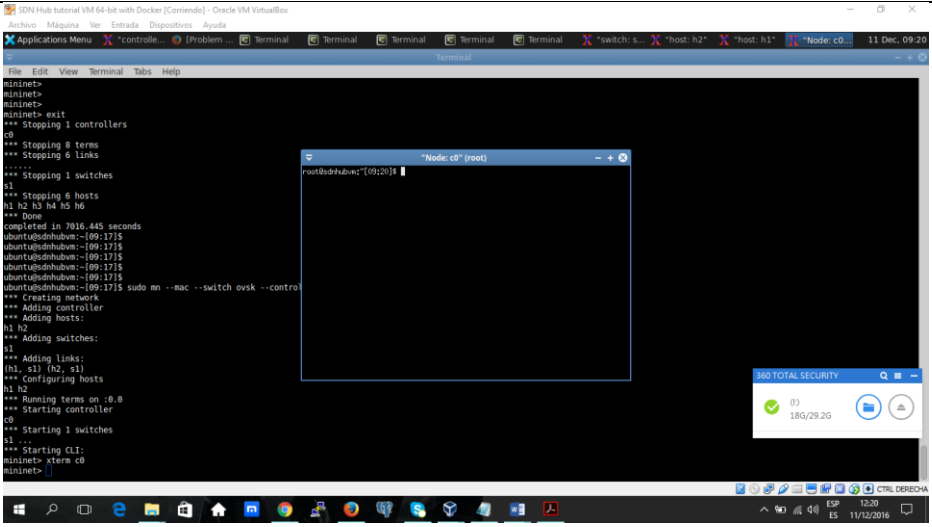


Figura 32: Creación de topología.

Seguidamente configurar el protocolo a utilizar y puerto figura 33 y 34

ovs-vsctl set Bridge s1 protocols=OpenFlow13

ovs-vsctl set-manager ptcp:6632

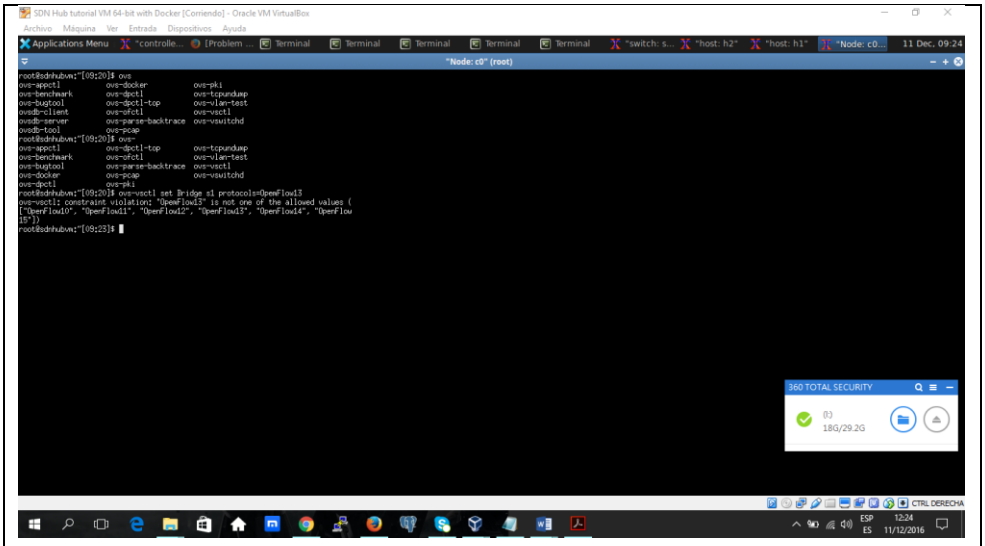


Figura 33: Configuración protocolo y puerto.

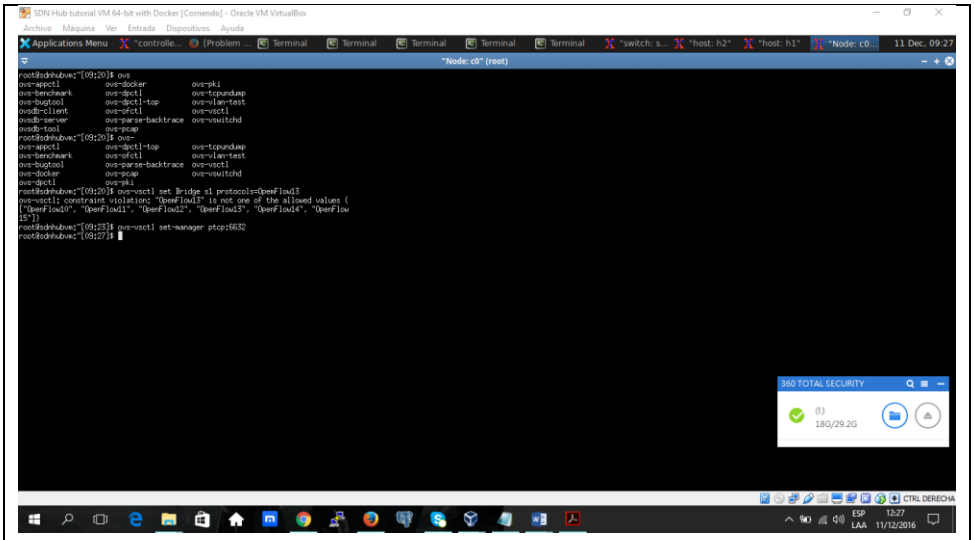


Figura 34: Configuración protocolo y puerto.

Es recomendable utilizar la librería que permite realizar la QoS figura 35 y 36.

sed '/OFPFlowMod(/,/)/s/)/, table_id=1)/' ryu/ryu/app/simple_switch_13.py > ryu/ryu/app/qos_simple_switch_13.py

cd ryu/; python ./setup.py install

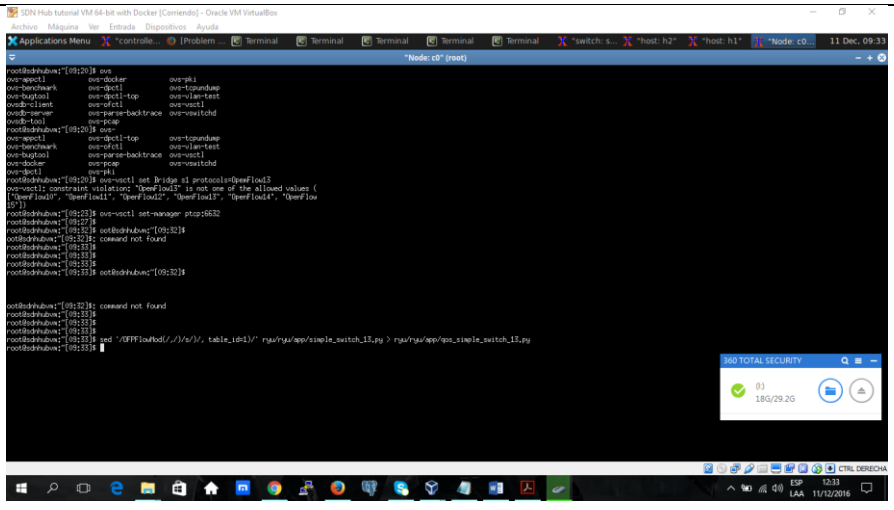
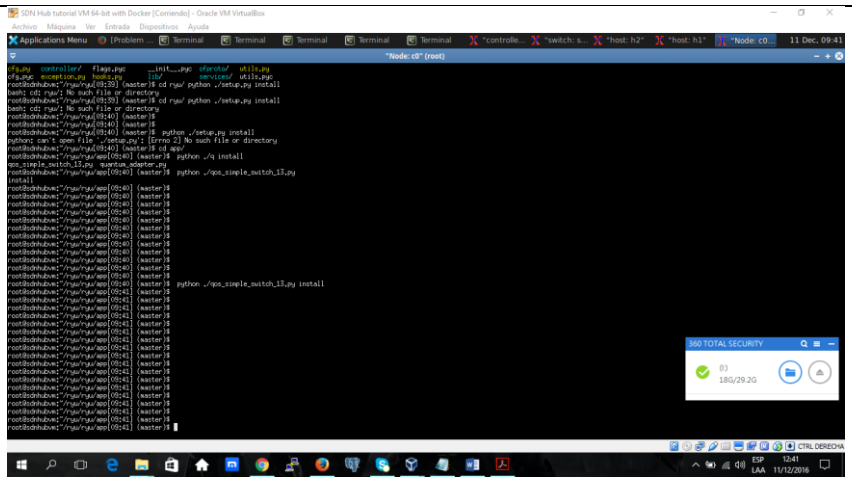


Figura 35: Librería para realizar QOS.



Figura#36: Librería para realizar QOS.

Ejecutar las librerías para aplicar QoS tal como se muestra en la figura 37.

ryu-manager ryu.app.rest_qos ryu.app.qos_simple_switch_13 ryu.app.rest_conf_switch

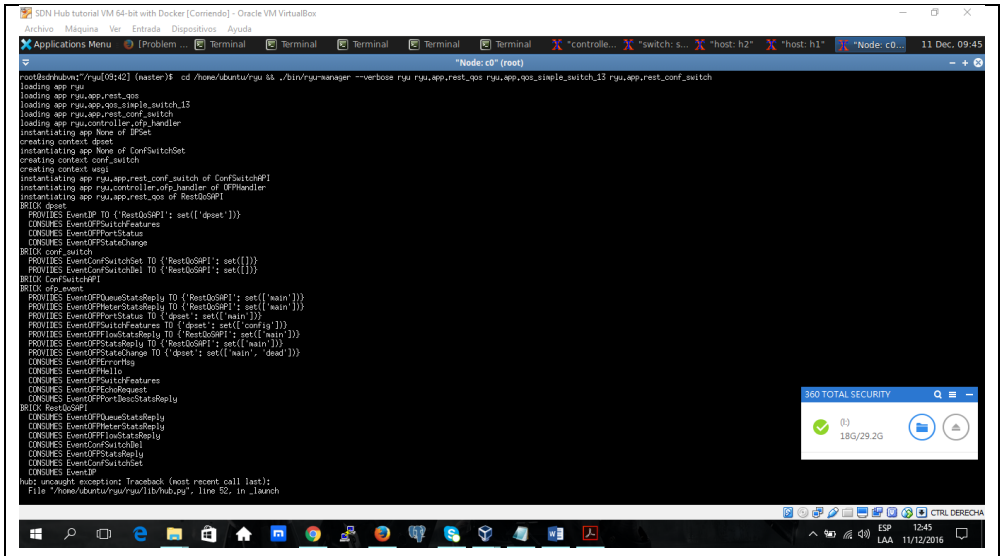


Figura 37: Ejecución de librerías QOS.

En pantalla observa un mensaje indicando la correcta ejecución de la aplicación de QoS

```
[QoS][INFO] dpid=0000000000000001: Join qos switch.
```

Figura 38: Ejecución de QoS.

Finalmente probar el tiempo de respuesta en la figura 38.

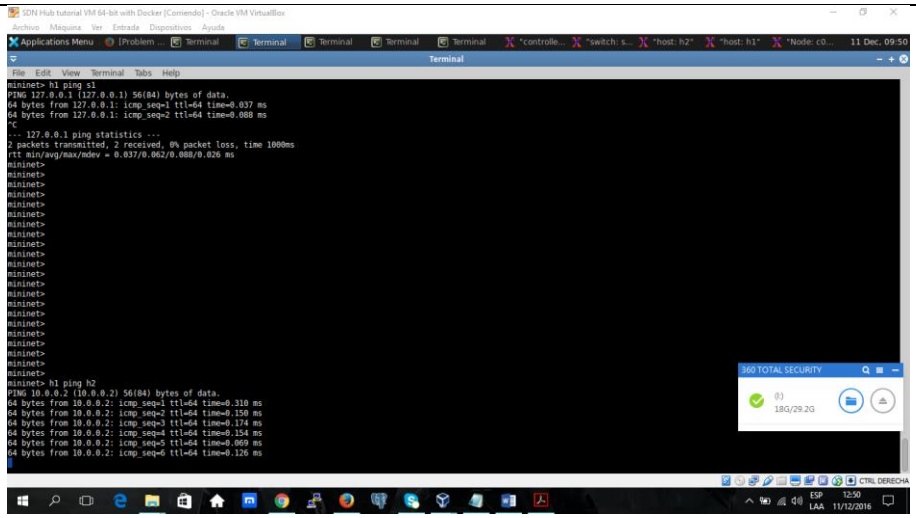


Figura 39: Pruebas y tiempos de respuestas.

5.3.4.3 Floodlight

Para este caso práctico es necesario utilizar Ubuntu 14.04 donde se encuentra incluido

- Floodlight v1.0
- Eclipse (w/Floodlight imported)
- Mininet v 2.2.0
- Open vSwitch v2.3.1
- Wireshark w/Openflow dissector

Para ingresar a Floodlight se tiene el usuario y contraseña con el mismo nombre del programa con minúscula.

Una vez realizado el escenario práctico de servicio, realizar una topología lineal, luego proceder a trabajar con la red creada, e ingresar al entorno de administración de floodlight, como se muestra en la figura 40.

Figura 40: Entorno de administración de Floodlight.

Inciar con la creación de los switch y los hosts, la topología a usar es lineal y la línea de comando a ejecutar es.

$ sudo mn –controller=remote, ip=127.0.0.1, port=6653 –topo=linear,4 –switch=ovsh, protocols=OpenFlow13 –mac

Luego ejecutar el comando pingall para verificar la conectividad figura 41 y 42.

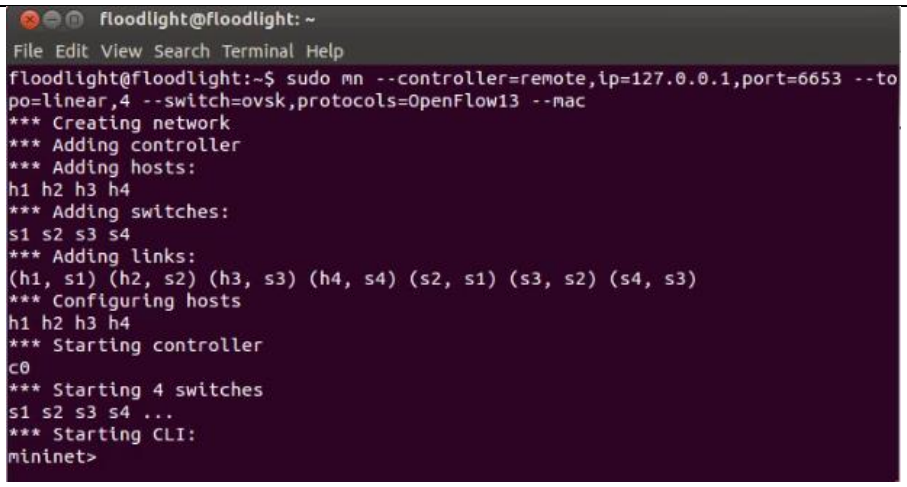


Figura 41: Creación de red, hosts, controlador en Floodlight.

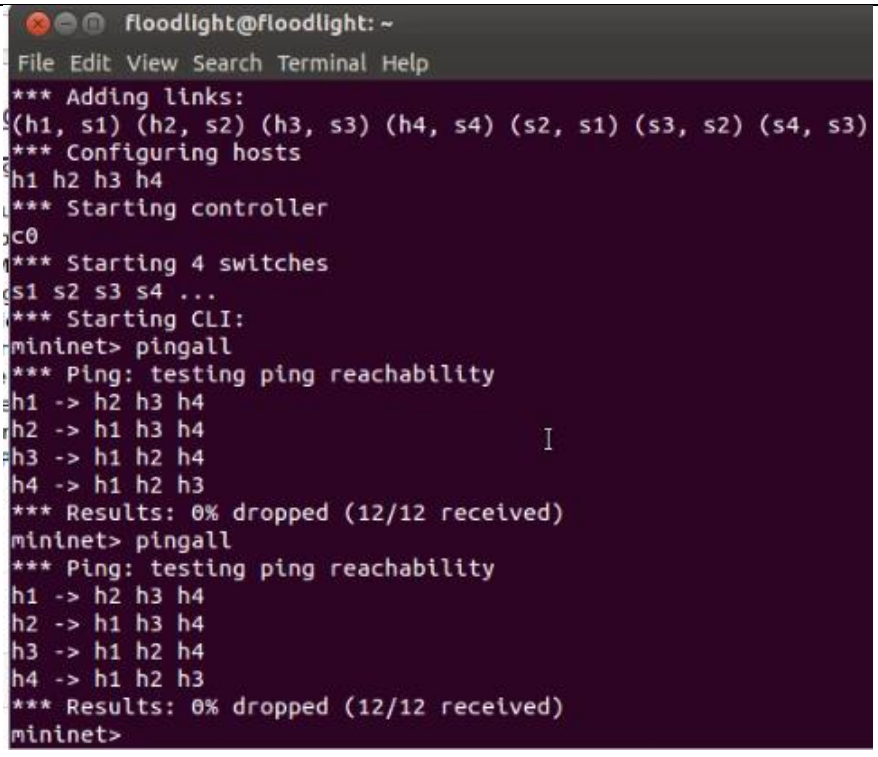


Figura 42: Prueba de conectividad en Floodlight.

Comprobar la conectividad en el entorno de administración de Floadlight mediante la opción "topología" figura 43.

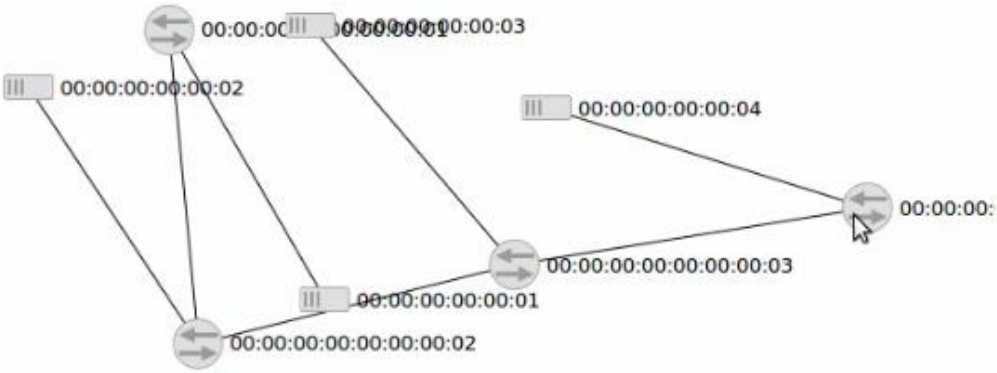


Figura 43: Diagrama en Floodlight.

Revisar la tabla de flujos ejecutando el comando ping entre los equipos y pingall para prueba de conectividad.

Ports (3)

#	Link Status	TX Bytes	RX Bytes	TX Pkts	RX Pkts	Dropped	Errors
local (s1)	DOWN	0	0	0	0	0	0
1 (s1-eth1)	UP 10 Gbps FDX	0	0	0	0	0	0
2 (s1-eth2)	UP 10 Gbps FDX	0	0	0	0	0	0

Flows (1)

Cookie	Table	Priority	Match	Apply Actions	Write Actions	Clear Actions	Goto Group	Goto Meter	Write Metadata	Experimenter	Packets	Bytes	Age (s)	Tim (s)
0	0x0	0		actions:output=controller	---	---	---	---	---	---	390	82758	170	0

Flows (7)

Cookie	Table	Priority	Match	Apply Actions	Write Actions	Clear Actions	Goto Group	Goto Meter	Write Metadata	Experimenter
0	0x0	0		actions:output=controller	---	---	---	---	---	---
9007199254740992	0x0	1	in_port=2 eth_dst=00:00:00:00:00:01 eth_src=00:00:00:00:00:02 eth_type=0x0x800 ipv4_src=10.0.0.2 ipv4_dst=10.0.0.1	actions:output=1	---	---	---	---	---	---
9007199254740992	0x0	1	in_port=1 eth_dst=00:00:00:00:00:03 eth_src=00:00:00:00:00:01 eth_type=0x0x800 ipv4_src=10.0.0.1 ipv4_dst=10.0.0.3	actions:output=2	---	---	---	---	---	---

Figura 44: Tabla de flujos tráfico en Floodlight.

5.4. Casos de uso de SDN y NFV, estrategias de despliegue y equipos que soporten esta tecnología.

5.4.1. Estrategias para impulsar el despliegue de SDN y NFV

Estrategia	**Descripción**
Costo reducción	Infraestructura de cloud computing Virtualización de funciones de red Reducir los costos de operación Escalabilidad Reduce los gastos de capital
Flexibilidad	Escala el servicio hacia arriba y hacia abajo rápidamente. Los recursos de red manipular de acuerdo a la demanda. Evitar bloqueo del proveedor. Introducir un nuevo servicio rápidamente
Agilidad	Responder rápidamente a los clientes a demanda. Optimización de la red y configuración en tiempo real. Sobre la marcha crear nuevos servicio.
Automatización	Administración de la red de manera simple Costos de operación reducidos Redefinición del modelo de prestación de servicios Aerodinamizado Funciones de control y operaciones integradas
Programación	Aplicaciones de software de red Infraestructura transparente de red APIs

Tabla 03: Estrategias de SDN Y NFV. Elaborado por autor

De acuerdo a la Tabla 03, las estrategias para impulsar SDN y NFV son:

- Conformar un equipo con las personas que laboran en la Dirección de Tics y que cuente con experiencia para el manejo de ingeniería, políticas, seguridad y gestión de las redes de datos. De esta manera, la Universidad Técnica de Manabí optimizará recursos, lo que permitirá satisfacer mejor las necesidades de su misión.
- Elegir un área física de redes de comunicaciones menos crítica dentro del campus universitario, en este caso se elegirá el Instituto de Ciencias Básicas donde esta tecnología es escalable y no afectara a la otra parte de la red de la universidad y con esto ganarías en experiencias.
- Realizar un informe de los resultados obtenidos durante un tiempo definido el cual pueda dilucidar las siguientes preguntas:
    - ¿Esta tecnología es la solución al problema actual?
    - ¿Es correcto realizar una inversión en implementar SDN en toda la red de comunicaciones del campus universitario?
    - ¿Se cuenta con el recurso económico y la infraestructura suficiente para mantener las redes definidas por software y la virtualización de funciones de red en la universidad?
- La última fase seria si las pruebas superan las expectativas y las tres preguntas planteadas anteriormente son aceptables y las lecciones aprendidas permiten ser una guía para implementar y tener la madurez necesaria para poder realizar el despliegue se debe hacer estas dos últimas preguntas.

¿Cómo va a afectar al rendimiento SDN entre las zonas más transitadas de la red?,

¿Hay otros retos fundamentales que esta tecnología pudiera resolver?

Porque si falla en la implementación no sólo están en riesgo la seguridad y el rendimiento de la red, sino también la capacidad de implementar la tecnología por completo.

5.4.2. Casos de usos en la utilización de redes definidas por software y virtualización de red.

Las tecnologías SDN y NFV están teniendo un gran impacto a nivel mundial, a pesar que aún son recientes; grandes empresas están estudiando y pensando en utilizarlas y dar solución de una manera diferente, rápida y eficaz.

SDN y NFV son tecnologías con gran tendencia en networking, con una visión futura en la arquitectura de las redes a las necesidades tecnológicas, dependiendo de cómo evoluciona el ambiente informático.

El creciente interés por estas nuevas tecnologías, ha llevado a muchas empresas a implicarse en el tema de las virtualizaciones, ya que las funciones de estas redes permiten ser agiles y capaces de responder automáticamente a las necesidades del tráfico y los servicios que se ejecuten sobre esta.

La clave a la hora de confirmar SDN como elemento transformador está en sus casos de uso. Se muestra algunos de ellos: ([22]Fraile Herrera, 2015)

- Nicira (ahora VMware) encontró uno de ellos, la virtualización de red como forma de **agilizar la provisión y operación de entornos masivos** (grandes centros de proceso de datos como los de Google, eBay o Apple) con aplicaciones virtualizadas. Ahora VMware profundiza en la idea de llevar el *firewall* hasta la máquina virtual en escenarios donde la seguridad es crítica.

- Nuage (de Alcatel), tras ofrecer una solución también para la virtualización de red, ahora se enfoca en **llevar SDN a la WAN**. Su objetivo es ayudar a los operadores de telecomunicaciones a adaptar sus redes privadas de clientes a un entorno dinámico de provisión de servicios.
- HP por su parte ha apostado con su **App Store por el uso de SDN** en entornos de campus. Como adaptar de forma dinámica los requisitos de calidad de servicio en red de aplicaciones de mensajería como Lync, o segmentar redes físicas en redes virtuales o "*slices*". ([22]Fraile Herrera, 2015)

A continuación, algunas empresas que están incluyéndose en estas tecnologías.

INTEL

Intel ha anunciado que va a invertir 6,5 millones de dólares en la empresa Big Switch Networks, una joven compañía que ha apostado fuertemente por la arquitectura SDN (Software-Defined Networking). Sumando esta ronda de financiación a la que ya ha obtenido meses atrás, ha conseguido un total de 45 millones de dólares (Goldman Sachs, Index Ventures y Redpoint Ventures son los principales inversores). ([24]Fernández, 2013)
Big Switch Networks lanzó su primer paquete SDN a finales del año pasado. Esta arquitectura, basada en redes abiertas, virtualizadas y altamente programables para adaptarse a las necesidades puntuales, es el futuro de las comunicaciones y la conexión entre centros de datos o cualquier otra infraestructura de red. Es una tendencia que también se está expandiendo a todo el centro de datos como un conjunto unificado de recursos. ([24]Fernández, 2013)

El objetivo de SDN es asegurar redes más flexibles, dinámicas, escalables, fáciles de programar y, en definitiva más eficientes en materia de costes, algo que, debido al incremento

exponencial de la información que se maneja es de vital importancia para la continuidad de los negocios. ([24]Fernández, 2013)

CISCO

La virtualización no es un concepto nuevo, pero ahora se está aplicando a las funciones de red como los de conmutadores, enrutadores, y la miríada de dispositivos de red desplegados. La expectativa es de un considerable ahorro de costes y una gran reducción de la complejidad de la red. ([21]CISCO, 2015)

Los primeros días de la virtualización del servidor tuvieron un efecto dramático en la reducción del capital del servidor, gastos operativos, pero los costos operacionales se dispararon a medida que se procesos. Con el tiempo, estos costos fueron refrenados con una mayor integración de servidores e infraestructura de red y capacidades de software más avanzadas. ([21]CISCO, 2015)

HP VAN SDN controlador

El software del controlador de SDN HP Virtual Application Networks (VAN) proporciona un punto de control unificado en una red habilitada para SDN, lo que simplifica la gestión, el aprovisionamiento y la organización. Esto permite la entrega de una nueva generación de servicios de red basados en las aplicaciones para entornos de campus, centros de datos o proveedor de servicios. ([25]HP, 2015)

Interfaz programable abierta ([25]HP, 2015)

- El Software de controlador de SDN HP Virtual Application Networks (VAN) permite a HP y terceros desarrollar aplicaciones SDN utilizando una variedad de idiomas con una implementación rápida.

- El controlador permite la organización de las aplicaciones y la automatización de las funciones de red.
- El controlador HP VAN SDN es compatible con los protocolos OpenFlow 1.0, 1.3, SNMP y NetConf.
- Plataforma centralizada y resistente
- El Software de controlador de SDN HP Virtual Application Networks (VAN) ofrece automatización centralizada para redes habilitadas para SDN, incluyendo la detección de la topología de red y el reenvío de ruta más corta.
- El controlador de SDN VAN se integra con Intelligent Management Center (IMC) para la gestión completa de errores, configuración, rendición de cuentas, rendimiento y seguridad.

Altamente disponible y escalable ([25]HP, 2015)

- El Software de controlador de SDN HP Virtual Application Networks (VAN) está diseñado para proporcionar un controlador de alto rendimiento.
- El controlador está altamente disponible, en caso de fallo proporciona un funcionamiento continuado de la red.

Seguridad robusta ([25]HP, 2015)

- El Software de controlador de SDN HP Virtual Application Networks (VAN) utiliza una sólida autenticación y autorización de usuarios y aplicaciones.
- La arquitectura permite conexiones seguras entre conmutadores habilitados para SDN y el controlador.

6. Conclusiones y Recomendaciones

6.1 Conclusiones

- La investigación que se planteó en este proyecto fue estudiar y conocer las tecnologías SDN y NFV, las cuales ofrecen un abanico de posibilidades que forman un nuevo paradigma que habilita la programación de la red permitiendo programar los equipos de acuerdo a las necesidades de la organización, aunque son tecnologías muy jóvenes, tienen un gran potencial que con una buena planificación sustituirían a la red de comunicaciones actual de la Universidad Técnica de Manabí.
- Comparando las dos tecnologías en esta investigación se tiene como resultado que se complementan entre si y las cuales pueden trabajar de manera conjuntan en la infraestructura tecnológica de la Universidad Técnica de Manabí porque SDN contribuye automatización de la red que permite tomar decisiones basadas en políticas para gestionar hacia dónde va el tráfico de red, mientras que la tecnología NFV se centra en los servicios y asegura que las capacidades de la red se alinean con los entornos virtualizados.
- En los escenarios de práctica, se encontraron herramientas que permitan crear un entorno de redes definidas por software de las cuales se eligieron tres: Floodlight, RYU,ONOS estos sistemas funcionan perfectamente con Mininet, uno de los simuladores SDN más utilizados, se trabajó en diferentes escenarios para la creación de redes y controles, balanceo, calidad de servicio, finalmente se demostró que SDN permite un gran control del tráfico de red y de una forma centralizada mediante comandos en la terminal de Mininet y grafico en el panel de Floodlight obteniendo

como resultado flexibilidad y escalabilidad para la redes de comunicaciones de la universidad.

- Una vez analizados los casos de uso y las estrategias para impulsar estas tecnologías en la Universidad Técnica de Manabí; es importante realizar a través de fases todos los procesos descritos en este documento y contar con un equipo multidisciplinario para que de esta forma se logre el éxito deseado porque esta es una tecnología de gran alcance con una gran cantidad de beneficios.

6.2 **Recomendaciones**

De acuerdo a las conclusiones, se recomienda:

- SDN y NFV significa una revolución en el mundo de las redes de comunicaciones son tecnologías jóvenes y en constante actividad de desarrollo se cree que estas nuevas redes no sustituirán a las redes actuales a corto plazo, más bien se piensa que coexistirán aprovechando lo mejor de cada una de ellas para su aplicación en la Universidad, esto se debe realizar de manera bien planificada y con la adquisición de los equipos actuales que soporten esta tecnología.
- No cabe duda que estas dos tecnologías se complementan entre si y cambiaran la forma en que se administra las redes y comunicaciones, la universidad debe invertir en su talento humano de la Dirección de TICS formando equipos que tenga el conocimiento de implementar SDN Y NFV.
- En esta tesis se tuvo la oportunidad de aprender de estas nuevas tecnologías SDN y NFV que ha llevado a conocer, tanto desde un punto de vista teórico como práctico

tanto su funcionabilidad como beneficios. Los escenarios prácticos realizados con las herramientas Mininet, RYU, Floodlight, son una guía para su implementación se recomienda crear otros entornos virtualizados de escenarios de acuerdo a la necesidad de la organización.

- Que la Universidad Técnica de Manabí adquiera equipos que soporte SDN y NFV para poder aplicar esta tecnología en la institución, de acuerdo a las fases descritas en esta investigación, capacitar al personal de la Dirección de Tics en el uso de las diferentes herramientas para crear entornos de redes definidas por software y virtualización de funciones de red e implementarlos desde las redes menos críticas en el campus hasta las que cuentan con mayor flujo de datos.

7. Bibliografía:

[1]Mundo Contact,. (24 de 09 de 2014). Recuperado el 02 de 02 de 2016, de http://mundocontact.com/sdn-y-nfv-dos-tendencias-que-revolucionaran-las-telecomunicaciones/

[2]López Grande., C. E. (17 de 11 de 2105). *REVISTA TECNOLÓGICA.* Recuperado el 01 de 30 de 2016, de http://www.redicces.org.sv/jspui/handle/10972/2535

[3]Advisor. (10 de 2014). *NFV Los beneficios y los desafíos que acompañan el.* Recuperado el 02 de 02 de 2016, de http://www.br.promonlogicalis.com/globalassets/latin-america/advisors/pt/advisor-nfv---final---cuadros.pdf

[4]Ballesteros Martínez, E. (11 de 11 de 2015). *SDN, NFV y los fundamentos de las redes del futuro.* Recuperado el 01 de 02 de 2016, de http://www.aunclicdelastic.com/sdn-nfv-y-los-fundamentos-de-las-redes-del-futuro/

[5]Frost & Sullivan CISCO. (26 de 02 de 2015). *Software Defined Networking:.* Recuperado el 19 de 03 de 2016, de https://www.cisco.com/web/mobile/global/la/ofertas/fastit/pdfs/fs_white_paper_cisco.pdf

[6]Millán Tejedor, R. J. (03 de 2014). *Qué es… NFV (Network Functions Virtualization.* Recuperado el 19 de 03 de 2016, de http://www.ramonmillan.com/documentos/networkfunctionsvirtualization.pdf

[7]Huerta, F. (18 de 03 de 2015). *Predicciones de telecomunicaciones 2015.* Recuperado el 19 de 03 de 2016, de https://www2.deloitte.com/content/dam/Deloitte/es/Documents/tecnologia-media-telecomunicaciones/Deloitte_ES_TMT_Predicciones-telecomunicaciones-2015.pdf

[8]Trigo, G. (01 de 07 de 2014). *SDN y el cambio hacia las redes del futuro*. Recuperado el 21 de 03 de 2016, de http://www.auben.net/index.php/compania/novedades-y-eventos/167-sdn-novedades

[9]Adivisor-SDN. (01 de 06 de 2014). *SDN Cómo el nuevo universo trazado por las redes definidas por software impactará en los negocios.* Recuperado el 21 de 03 de 2016, de http://www.la.logicalis.com/globalassets/latin-america/advisors/es/advisor_sdn.pdf

[10]4G Americas. (20 de 11 de 2014). *www.4gamericas.org*. Recuperado el 14 de 04 de 2016, de http://www.4gamericas.org/es/newsroom/press-releases/nfv-controlando-las-redes-virtuales/

[11]Pautasio, L. (12 de 06 de 2014). *NFV y SDN, el desafío de comprar software*. Obtenido de http://www.telesemana.com: http://www.telesemana.com/blog/2014/06/12/nfv-y-sdn-el-desafio-de-comprar-software/

[12]Janz , C. (10 de 11 de 2015). *Cuatro beneficios que SDN aporta a la seguridad*. Recuperado el 22 de 04 de 2016, de http://www.telesemana.com: http://www.telesemana.com/blog/2015/11/10/cuatro-beneficios-que-sdn-aporta-a-la-seguridad/

[13]Shackleford , D. (08 de 07 de 2013). *Estrategias de seguridad de SDN para prevenir ataques a la red*. Recuperado el 22 de 04 de 2016, de http://searchdatacenter.techtarget.com: http://searchdatacenter.techtarget.com/es/reporte/Estrategias-de-seguridad-de-SDN-para-prevenir-ataques-a-la-red

[14]POMEYROL, J. (26 de 03 de 2014). *seguridad-en-la-nube*. Recuperado el 22 de 04 de 2016, de http://www.muyseguridad.net/2014/03/26/seguridad-en-la-nube

[15]networkworld. (12 de 09 de 2014). *SDN: perfiles de usuario y criterios de evaluación (1)*. Obtenido de http://www.networkworld.es: http://www.networkworld.es/sdn/sdn-perfiles-de-usuario-y-criterios-de-evaluacion-1

[16]Lemke, A. (08 de 12 de 2014). *Redes SDN: Llevar la funcionalidad NFV al siguiente nivel*. Recuperado el 25 de 04 de 2016, de https://techzine.alcatel-lucent.com/es/redes-sdn-llevar-la-funcionalidad-nfv-al-siguiente-nivel

[17]Becares, B. (31 de 03 de 2014). Recuperado el 25 de 04 de 2016, de http://www.channelbiz.es/2014/03/31/nfv-un-nuevo-concepto-y-un-futuro-para-las-redes/2/

[18]pc-100. (02 de 01 de 2014). *¿Cuál es la diferencia entre la SDN y NFV*. Recuperado el 25 de 04 de 2016, de http://www.pc-100.com/es/whats-the-difference-between-sdn-and-nfv/

[19]Pate, P. (30 de 03 de 2013). *NFV and SDN: What's the Difference?* Recuperado el 26 de 04 de 2016, de https://www.sdxcentral.com/articles/contributed/nfv-and-sdn-whats-the-difference/2013/03/

[20]MiniNet, e. (01 de 01 de 2016). *mininet.org*. Obtenido de http://mininet.org/overview/

[21]CISCO. (2015). *Guia de SDN Y NFV.* Recuperado el 11 de 11 de 2016, de https://www.cisco.com/c/dam/en/us/solutions/collateral/trends/sdn/executive-summary-cisco-2015-ebook.pdf

[22]Fraile Herrera, R. (02 de 09 de 2015). *Casos de uso de SDN: La búsqueda continúa.* Recuperado el 11 de 11 de 2016, de http://aunclicdelastic.blogthinkbig.com/casos-de-uso-de-sdn-la-busqueda-continua/

[23]diarioti. (28 de 08 de 2014). *Google explica las ventajas de haber incorporado SDN y NFV en su propia nube.* Recuperado el 11 de 11 de 2016, de http://diarioti.com/google-explica-las-ventajas-de-haber-incorporado-sdn-y-nfv-en-su-propia-nube/82876

[24]Fernández, P. (02 de 2013). *INTEL también se interesa por SDN.* Recuperado el 10 de 11 de 2016, de http://www.silicon.es/intel-tambien-se-interesa-por-la-arquitectura-sdn-32975

[25]HP. (2015). *HP J9863AAE: Licencia electrónica de uso de software HP VAN SDN Controller Base para 50 nodos.* Recuperado el 11 de 11 de 2016, de http://www.onlinecomputer.com.co/articulos/activos/catalogos/HP_VAN_SDN_Controler.pdf

[26] SDN, H. (2014). *ONOS Tutorial.* Recuperado el 09 de 12 de 2016, de http://sdnhub.org/tutorials/onos/