Análisis técnico y económico de la implementación de una red SDN en el backbone de la Sede Matriz de la Universidad de las Fuerzas Armadas ESPE

Rojas Rivera Diego Paúl

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Gerencia de Sistemas

Trabajo de titulación, previo a la obtención del título de Magíster en Gerencia de Sistemas

Msc. Galárraga Hurtado, Juan Fernando

15 de junio de 2022

TESIS DIEGO ROJAS FINAL.pdf

Scanned on: 0:48 December 7, 2022 UTC

Identical Words	242
Words with Minor Changes	40
Paraphrased Words	132
Omitted Words	1042

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnologia

Centro de Posgrados

Certificación

Certifico que el trabajo de titulación: "**Análisis técnico y económico de la implementación de una red SDN en el backbone de la Sede Matriz de la Universidad de las Fuerzas Armadas ESPE**" fue realizado por el señor **Rojas Rivera, Diego Paúl**; el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolqui, 09 de Diciembre del 2022

JUAN FERNANDO GALARRAGA HURTADO

Ing. Fernando Galárraga, Mgrt

Director

C.C: 1711464816

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Responsabilidad de Autoría

Yo **Diego Paúl, Rojas Rivera**, con cédula n° 1717947186, declaro que el contenido, ideas y criterios del trabajo de titulación*:* **Análisis técnico y económico de la implementación de una red SDN en el backbone de la Sede Matriz de la Universidad de las Fuerzas Armadas ESPE** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolqui, 09 de Diciembre del 2022

Rojas Rivera Diego Paúl

C.C.: 1717947186

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Postgrados

Autorización de publicación

Yo, **Diego Paul Rojas Rivera**, con cédula n° 1717947186, autorizo a la Universidad de las Fuerzas armadas, ESPE, a publicar el trabajo de titulación: **Análisis técnico y económico de la implementación de una red SDN en el backbone de la sede Matriz de la Universidad de las Fuerzas armadas, ESPE**, en el Repositorio Institucional, cuyo contenido, ideas y criterio son de mi responsabilidad.

Sangolquí, 9 de diciembre de 2022

Rojas Rivera Diego Paul

C.C.: 1717947186

Dedicatoria

Dedico esta tesis, que he realizado con tanto esfuerzo y dedicación, primero a Dios, quien con su luz y guía me ayudó en su realización. A toda mi amada familia y a los estimados docentes de esta prestigiosa universidad.

Agradecimiento

En primer lugar, a Dios por guiarme y permitirme alcanzar mis sueños, y a mi familia que ha sido incondicional en todo el proceso, sin ellos no habría sido posible cumplir este objetivo.

Un sincero agradecimiento a todos mis compañeros que durante estos años de estudio hicieron el camino más corto y por todo su apoyo, a todos los docentes y coordinación de la Maestría en Gerencia de Sistemas.

Índice de contenido

Índice de tablas

Índice de figuras

Resumen

Las redes de datos en instituciones educativas son un aspecto crítico debido a la cada vez mayor necesidad de seguridad de la información, costos reducidos y eficiencia. En la actualidad, la Universidad de las Fuerzas Armadas ESPE no cuenta con un protocolo robusto y seguro, y se identificó que requiere de una infraestructura centralizada que permita obtener flexibilidad, escalabilidad y mayor seguridad en su administración. En este contexto, las redes definidas por software SDN son una alternativa que ofrece estas mejoras sustanciales y a bajo costo. Por tales razones, el presente trabajo tuvo como objetivo analizar técnica y económicamente la implementación de una red SDN en el backbone de la sede matriz de la Universidad de las Fuerzas Armadas, a realizar mediante el diseño de una red simulada en Mininet que cumpla con los parámetros de seguridad necesarios, de un análisis económico de su implementación, de un análisis de costo/beneficio y de pruebas de conectividad y desempeño. El diseño metodológico utilizado es de investigación mixta aplicada, basado en un diagnóstico inicial de la situación en la red backbone de la institución, para luego implementar de forma simulada la red SDN, evaluando su conectividad y desempeño según métricas. Luego se elaboró un estudio económico para la evaluación integral de este tipo de red a nivel institucional. Como resultados, se obtuvo una red simulada SDN de tres capas (infraestructura, control y aplicación), con puertos en casa matriz y las cinco sedes de la institución educativa. Esta fue desarrollada en Mininet y con Floodlight v1.0, Eclipse IDE, OpevSwitch (OVS). Las pruebas realizadas con Wireshark con Openflow dissector demuestran que la red presenta una buena conectividad y desempeño. La implementación es factible en términos económicos con VAN de $17.713,14, TIR de 29,09%, ROI de 6,95 y costo/beneficio (C/B) de $1,07. Se determinó, por tanto, que la implementación de esta red es factible y favorable para el sistema de gestión de información en la ESPE.

Palabras clave: Red sdn, red backbone, gestión de datos, mininet, evaluación económica.

Abstract

Data networks in educational institutions are a critical aspect due to the increasing need for information security, reduced costs and efficiency. Currently, the Universidad de las Fuerzas Armadas ESPE does not have a robust and secure protocol, and it was identified that it requires a centralized infrastructure that allows for flexibility, scalability and greater security in its administration. In this context, software-defined networking (SDN) is an alternative that offers these substantial improvements at low cost. For these reasons, the objective of this work was to technically and economically analyze the implementation of an SDN network in the backbone of the headquarters of the University of the Armed Forces, to be done through the design of a simulated network in Mininet that meets the necessary security parameters, an economic analysis of its implementation, a cost/benefit analysis and connectivity and performance tests. The methodological design used is an applied mixed research, based on an initial diagnosis of the situation in the institution's backbone network, to then simulate the implementation of the SDN network, evaluating its connectivity and performance according to metrics. Then, an economic study was elaborated for the integral evaluation of this type of network at institutional level. As a result, a simulated SDN network with three layers (infrastructure, control and application) was obtained, with ports at the head office and the five sites of the educational institution. This was developed in Mininet and with Floodlight v1.0, Eclipse IDE, OpevSwitch (OVS). Tests performed with Wireshark with Openflow dissector show that the network presents good connectivity and performance. The implementation is feasible in economic terms with NPV of $17.713,14, IRR of 29.09%, ROI of 6.95 and cost/benefit (C/B) of $1.07. It was determined, therefore, that the implementation of this network is feasible and favorable for the information management system at ESPE.

Keywords: Sdn network, backbone network, data management, mininet, economic evaluation.

Capítulo I

Introducción

Antecedentes

En la actualidad tener una red segura, centralizada y escalable es un tema muy importante a considerar en la red de datos de una entidad, esto debido a que se tiene el temor que la misma puede ser vulnerable a ataques informáticos, problemas con la conmutación de datos ante una falla y la complejidad de implementar configuraciones y equipos en redes que no son escalables. Las entidades educativas deberían tomar en cuenta todos aspectos al momento implementar redes para la comunicación de los datos.

Existen diversas formas de implementar redes seguras, escalables y centralizadas, para ello nos enfocamos en las redes definidas por software (SDN por sus siglas en inglés).

Con las redes SDN, las redes estáticas pueden convertirse en redes inteligentes, mucho más flexibles y escalables, la programabilidad de la red compleja y la capacidad de modificar su comportamiento de forma automática en tiempo real, simplifica notablemente la complejidad y costes de la gestión de redes.

Planteamiento del problema

En la actualidad la mayoría de organizaciones cuentan con redes tradicionales como redes distribuidas dentro de su infraestructura; sin embargo, dichas redes no poseen seguridad centralizada en la transmisión de datos ni tampoco la escalabilidad y el modo de obtener el control de su red mediante un solo dispositivo, esto debido al desconocimiento de nuevas tecnologías que permiten realizar un control centralizado y optimizar de esta manera los recursos técnicos y económicos dentro de la organización.

Actualmente la red de backbone de la Universidad de las Fuerzas Armadas no cuenta con un protocolo robusto para la comunicación de datos, es necesario contar con una infraestructura centralizada que cuente con flexibilidad y seguridad en la administración de su red.

Justificación

Las entidades educativas debido a la criticidad de la información que manejan, requieren que sus redes tengan una alta disponibilidad, cuente con algoritmos de seguridad y se pueda tener el control de la red de una manera sencilla y focalizada en un solo punto.

El backbone de la Universidad de las Fuerzas Armadas cuenta con una red distribuida para la comunicación de los datos, estas redes ofrecen una mínima seguridad, soluciones complejas a escalabilidad y respuestas tardía ante fallas, para ello se propone utilizar una infraestructura robusta que contribuya en el mejoramiento de estos aspectos mediante la implementación de una red SDN.

Objetivos

Objetivo general

Analizar técnica y económicamente la implementación de una red SDN en el backbone de la Sede Matriz de la Universidad de las Fuerzas Armadas.

Objetivos específicos

- Realizar el diseño de una red SDN mediante simulación a través del software Mininet basado en Linux que cumpla con parámetros de seguridad y escalabilidad para la red de Backbone en la matriz de la Universidad de las Fuerzas Armadas.
- Realizar un análisis económico de la implementación de una red SDN basado en indicadores como el ROI, VAN, TIR.
- Analizar los resultados obtenidos y determinar el costo/beneficio de la implementación de la red SDN en la Universidad de las Fuerzas Armadas.
- Realizar pruebas de conectividad hacia 4 campus de la ESPE (Latacunga, Santo Domingo, Salinas y Shell) y evaluar el rendimiento de la red mediante indicadores latencia, throughput.

Hipótesis

¿Qué solución se puede implementar en el backbone de la matriz Universidad de las Fuerzas Armadas para fortalecer la comunicación de los datos?

Debido a que la matriz de la Universidad de las Fuerzas Armadas cuenta con una red distribuida es necesario implementar una infraestructura robusta en la red con el propósito de mejorar el rendimiento de la red con alta disponibilidad, algoritmos robustos de seguridad y obtener un control centralizado de la red.

Capítulo II

Marco teórico-referencial

Antecedentes

Las redes SDN han sido estudiadas durante los últimos años debido a su capacidad para aumentar la seguridad de manera eficiente y para mejorar el rendimiento general de las redes tradicionales. A continuación, se exponen las investigaciones más relevantes para el tema de este trabajo, las que ofrecen información relevante sobre SDN, su rendimiento y su aplicación en contextos académicos.

El trabajo de Cameselle (2021) consistió en el diseño de una herramienta centralizada que permita definir y aplicar políticas de seguridad a partir del uso de las redes SDN. Con ello se esperó que este sistema fuera capaz de establecer las políticas en la red a partir de procesos automatizados y distribuidos, de modo que no requiriese configuraciones manuales, reduciendo con ello errores y facilitando la distribución a todos los dispositivos. Esto permitió disponer de seguridad en la red completa y no solo en determinados nodos, además de proveer un sistema estable y con un buen rendimiento.

El sistema diseñado está compuesto por cuatro partes: la red física, la infraestructura de los controladores, la aplicación en los controladores y una aplicación de tipo externa, obteniendo con ello una estructura de tipo jerárquica en la que los niveles abstraen para avanzar al siguiente. El resultado es una herramienta que, a diferencia de otra tipo SDN-WAN, posee un sistema que se distribuye por los controladores y evita con ello los puntos de fallo únicos debidos al análisis de tráfico.

El trabajo de Ramos (2021) buscó evaluar el rendimiento de las redes SDN respecto de las tradicionales HDN en el contexto de una arquitectura de red académica avanzada. El rendimiento se evaluó considerando parámetros como el grado de retardo o velocidad de la red, el consumo de los recursos computacionales y la pérdida de paquetes. Para esto se

emularon ambos tipos de redes a partir de la topología de una red modelo (REUNA de Chile), implementando HDN con GNS3 y SDN con Mininet y otros.

Los resultados obtenidos indican que existe una correlación negativa entre la cantidad de instancias de control y el rendimiento de la red; esto es: la red SDN presenta un mejor rendimiento que HDN en una relación inversamente proporcional, dado que añadir más instancias de control a HDN implican menor rendimiento en la misma magnitud que una sola instancia hace eficiente a SDN. De esta manera, con el estudio se evidencia la mejora sustancial en rendimiento de una red cuando se aplica la arquitectura SDN.

El trabajo de Barroso (2018) consistió en la implementación de una red SDN en la Diputación de Cádiz, para lo cual trabajó en el diseño de la aplicación de gestión para la red con el uso de un controlador para imbuir los comportamientos requeridos en los nodos. La metodología utilizada correspondió al uso de los criterios establecidos en la norma UNE 157801:2007 para desarrollo de sistemas de información.

El trabajo de Herrera (2020) tuvo como objetivo optimizar una red académica GPON mediante un escenario SDM para obtener una mejora en el rendimiento de esta y en la calidad del servicio. Con ello se mejoraron los problemas de conectividad, la cobertura y el rendimiento general de la red existente, además del uso plausible de protocolos abiertos como OpenFlow. Para realizar esto, la investigación inició con la documentación sobre la red existente y su análisis para diagnosticar sus problemas; posteriormente se fundamentó teóricamente el problema; y, finalmente, se diseñó la red GPON mediante SDN. El resultado fue una red estructurada en red interna y en red externa, la primera compuesta por SDN-OLT, donde se ubica la administración.

El trabajo de Cuba (2015) tuvo por objetivo implementar una red SDN/OpenFlow para la red de un campus académico. Esto se realizó considerando el gran número de usuarios en este tipo de red, lo que implica un enorme tráfico que se traduce en la disminución de su eficiencia y su poca estabilidad y escalabilidad. Por tanto, a partir del uso de SDN se diseñó un controlador

para la red, de modo de mejorar con ello su escalabilidad y su rendimiento en esas condiciones de alto tráfico. El controlador diseñado fue de carácter OpenFlow escalable para tráfico unicast, probado sobre plataforma Floodlight, y fue implementado definitivamente por el módulo Clustering. Además, este puede funcionar conjuntamente con elementos Legacy y permite migración total de la red del campus a SDN.

El trabajo de Bone et al. (2021) tuvo por objetivo determinar los parámetros de aplicación de la arquitectura SDN en redes de tipo educativas enfocadas a entornos de investigación. Para esto, utilizaron una metodología de investigación cualitativa basada en un análisis documental, la que inicia con un análisis teórico y continúa con el análisis de los factores que impactan en las redes educativas una vez que se aplica SDN.

Como resultados, determinaron que en términos generales las redes universitarias o educativas en general deben cumplir con permitir el acceso a diversas TIC, deben permitir certificaciones digitales en línea, deben disponer de plataformas de aulas virtuales, bibliotecas, entre otras. De esta manera, es preciso que las redes de dichas instituciones cuenten con gestión automatizada (verificada y depurada según las particularidades requeridas), gestión de actualizaciones, seguridad, eficiencia, virtualización, entre otras. Para esto, los controladores SDN cumplen una función adecuada y permiten la migración o trabajo con controladores en redes SDN híbridas.

La tesis de magíster de Mantilla (2021) consistió en la evaluación de la calidad del servicio ante un ataque DoS en sistemas de *streaming* en redes SDN. Como resultado, se obtuvo que los ataques de spoofing a la red son los que más causan afectación a la calidad del servicio. Co los resultados pueden determinarse de manera más adecuadas algoritmos que permitan detectar y migrar ante ataques tempranamente.

Redes de datos

Las redes, desde sus orígenes, han evolucionado continua y rápidamente. En términos generales, las redes de datos constituyen una serie de dispositivos de red conectados entre sí

bajo determinada jerarquía. Estas permiten el flujo de los datos de un punto a otro a través de la conexión de usuarios y determinadas aplicaciones. Tradicionalmente, estas redes se programan para que los datos transferidos de un punto a otro lo hagan bajo los requerimientos de la institución, de modo que cada dispositivo debe considerar estos parámetros y ser programado en función de ellos para llevar a cabo su tarea (Parra et al., 2015).

Dentro de los objetivos que tienen las redes de datos en general, destacan:

- Compartir recursos, equipos, información y programas que se encuentran localmente o dispersos geográficamente.
- Brindar confiabilidad a la información, disponiendo de alternativas de almacenamiento.
- Obtener una buena relación costo / beneficio.
- Transmitir información entre usuarios distantes de la manera más rápida y eficiente posible (Joskowicz, 2008, p. 4).

Según Joskowicz (2008) algunos criterios de clasificación son:

- Según el tipo de transmisión de datos: Pueden ser redes de difusión (medio de transmisión compartido por todos los dispositivos de la red), o redes punto a punto (varias conexiones entre dos dispositivos).
- Según su tamaño o alcance: Entre estas se encuentran las redes LAN, WAN, PAN (de alcance limitado, de alcance amplio o de tipo personal, respectivamente). Se añaden también a estas las inalámbricas (WLAN).

Dentro del ámbito tradicional de redes, los controladores, entendidos como aquellos programas que permiten manejar, mantener y diseñar las conexiones entre las redes (Joskowicz, 2008), son programados dispositivo a dispositivo, de modo que cada uno de estos “sabe” cómo ejecutar la transmisión de la información de acuerdo a su programación. Esta programación en la actualidad se realiza a través del protocolo IPv4, aunque suele existir la

posibilidad en los computadores de migrar a IPv6 (Ramos, 2021). Sin embargo, como Parra et al., (2015) plantean, esto dificulta la operatividad de la red cuando los usuarios, dispositivos o requerimientos cambian constantemente, dado que a partir de esto se requieren modificaciones de la topología de la red o su extensión. Una estructura básica de red tradicional está formada por un dispositivo de red y se subdivide en plano de control y datos.

En una red sencilla, que ni siquiera posee controlador, puede observarse un funcionamiento altamente dependiente de la calidad de los enlaces. En caso de existencia de fallos, las tablas que dirigen la información o de encaminamiento son capaces de redirigir la información por distintas vías, pero esto puede traer muchos costos en eficiencia, sobre todo si los enlaces disponibles no son de calidad (Córdoba, 2019).

En estas redes, el plano de control es aquel en donde pueden almacenarse y ser ejecutados los parámetros de operación, mientras que el plano de datos es aquel donde los datos son conmutados y transferidos. En este sentido, para volver a las redes tradicionales más eficientes, puede pensarse en el traslado de todos los controladores de cada dispositivo hacia un punto centralizado, de manera que pueda controlar al mismo tiempo toda la red. Esto se consigue añadiendo a este tipo de controladores centrales la capacidad de gestionar la red en su totalidad de manera “inteligente”, lo que puede realizarse a través de su programación vía software (Córdoba, 2019). Esto tiene por nombre red SDN (Software Define Network), y se analiza a continuación.

Topología de red

La topología de una red refiere a la manera en la que se encuentran distribuidos los dispositivos. Una tipología típica consta de dos tipos de nodos distintos, unos externos o *Edge* y otros intermedios, que conmutan y transfiere los paquetes, o *Core* (Vázquez, 2011).

Red backbone distribuida

Una red backbone o troncal corresponde a la red que conecta, a su vez, a los routers que se encuentran interconectados, las cuales se utilizan comúnmente en instituciones; sin

embargo, pueden ser aplicadas como conexiones enormes interterritoriales. Estas utilizan cables de fibra óptica para la interconexión entre redes locales con redes amplias (LAN y WAN, respectivamente) (Jiménez, 2021).

Dado su coste, este tipo de redes son usualmente utilizadas por instituciones, funcionando adecuadamente en contextos como los académicos, que requieren de la interconexión de sus sistemas de red en distintas facultades y territorios. Así, para Jiménez (2021) existen diversos tipos de redes backbone:

- En serie: refiere a la red de tipo troncal que se forma por dispositivos en cadena; es de carácter básico, y utiliza gateways, switches o routers. Estas funcionan para pocos equipos y no presentan escalabilidad, de modo que no se utilizan frecuentemente.
- Distribuida: se basa en una estructura jerárquica de tipo escalable, en donde pueden encontrarse dispositivos de carácter intermedio que interconectan a otros, como switches. Dado que permite integrar nuevos dispositivos, suele ser más utilizada que la backbone en serie.
- Paralela: en este caso, los dispositivos presentan varias conexiones distintas entre ellos, por ejemplo, en el caso de routers de alto nivel y otros elementos de la red, de modo que permite reducir considerablemente los problemas al disponer de conexiones duplicadas, además de mejor rendimiento y velocidad.

Redes definidas por software (SDN)

El acelerado crecimiento de los sistemas informáticos y la necesidad de transportar datos de mayor tamaño por medio de la red ha dado paso a la conformación de nuevos elementos que se adapten a los requerimientos de la sociedad informática actual. Frente a este hecho surgen nuevas tecnologías que brindan a los usuarios mayores rangos de control, seguridad y operatividad; así surge la red SDN.

Una red SDN ser definida como un tipo de arquitectura nuevo de carácter dinámico que puede ser gestionada y adaptada, como la define la Open Networking Fundation (Open Networking Foundation [ONF], 2021). Tiene como característica fundamental el separar las funciones de transferencia de paquetes y de control, de modo que este último es completamente programable, con lo que es posible abstraer toda la infraestructura subyacente por las aplicaciones y servicios de red (Parra et al., 2015).

Una determinación de las fases de desarrollo de esta tecnología en redes es la planteada por Córdoba (2019) se basan en redes activas establecidas entre 1995 y 2000; seguido de la separación de plano control y datos (2001-2007) y el desarrollo *open Flow* e interfaz de programación API (2007-2010).

Las redes SDN surgen como una respuesta a una necesidad específica: generar una mejor respuesta, mayor velocidad, mejoras en costos, arquitectura ágil, lograr un mejor control de su funcionamiento a través de un ancho de banda que haga posible la implementación de diferentes tipos de servicios en la virtualidad (Sper, 2013).

Las SDN, tal como plantea Velásquez (2013), hacen posible establecer una diferenciación entre el software o plano de control y la máquina que conmuta los datos en la red. De esta manera se logra que las redes adquieran características que hacen posible una mejor programación, automatización y flexibilidad. Por esta razón ha adquirido gran relevancia ya que ayudan a generar soluciones efectivas a los problemas que se presentan en las redes.

Mientras que las redes tradicionales requieren de procesos de programación para poder procesar los datos, en las SDN, esto depende de una interfaz de programación con un software que permite regular la forma en que se comporta. Esto significa que la programación no es estática, se encuentra directamente conectada con los mensajes que son enviados al software, de tal manera que sea una forma de gestionar más dinámica.

Las SDN, desde el planteamiento de García et al. (2014) se configuran como un tipo de tecnología que establece una separación entre los datos y el control de los mismos. Con la

expansión de los dispositivos móviles, el proceso de virtualización de los servidores, así como los cambios en los patrones de tráfico de datos, las redes tradiciones se convierten en obsoletas y por lo tanto surgen las SDN, dentro un paradigma nuevo enfocado a la transformación de la arquitectura de las redes.

Los principios sobre los cuales se asientan las redes definidas por software, según explica Velásquez (2013) son los siguientes:

- Reduce costos operativos debido a que centraliza los aspectos fundamentales de los planos de control, administración y costos simplificando en diseño de la red.
- La nube se utiliza como un medio a través del cual es posible que la red sea flexible y adaptable, además reduce el tiempo de servicio y por lo tanto los costos de funcionamiento.
- Hace posible crear una plataforma en la cual se pueden configurar aplicaciones de red, servicios y nuevos sistemas de administración.
- Brinda los parámetros suficientes para estandarizar los procesos. De esta manera se puede brindar asistencia inter operativa y heterogénea.
- Contar con una red SDN incrementa de manera significativa los niveles de seguridad para el manejo de datos para la institución y para todos quienes acceden a las redes móviles.

Las SDN centralizan la inteligencia en controladores basados en software que tienen un control integral de la red, el cual opera como conmutador lógico y único. Este aspecto es esencial para que las entidades que la implementan puedan operar de manera independiente sin tener que depender los proveedores para realizar cambios o solucionar un problema. García et al. (2014) plantean que otra de las características de las redes definidas por software es la simplificación de los dispositivos de red, ya que se limita el uso de protocolos y se generan instrucciones fáciles de seguir.

La red SDN se separa de manera eficaz en cuatro planos: forwarding, control, servicio y administración. De esta manera existe mayor flexibilidad y seguridad para el manejo de datos. En relación a estos Velásquez (2013) manifiesta que es fundamental que sean separados y definidos de manera precisa para una mejor comprensión de su funcionamiento. Los aspectos esenciales en forwarding se basan en el envío de paquetes en la red de forma optimizada; para control se realiza un análisis de topología y gestión del destino del flujo; en los servicios se toma decisiones y ejecución de operaciones con datos; en la administración se determina las instrucciones básicas del funcionamiento del dispositivo de la red.

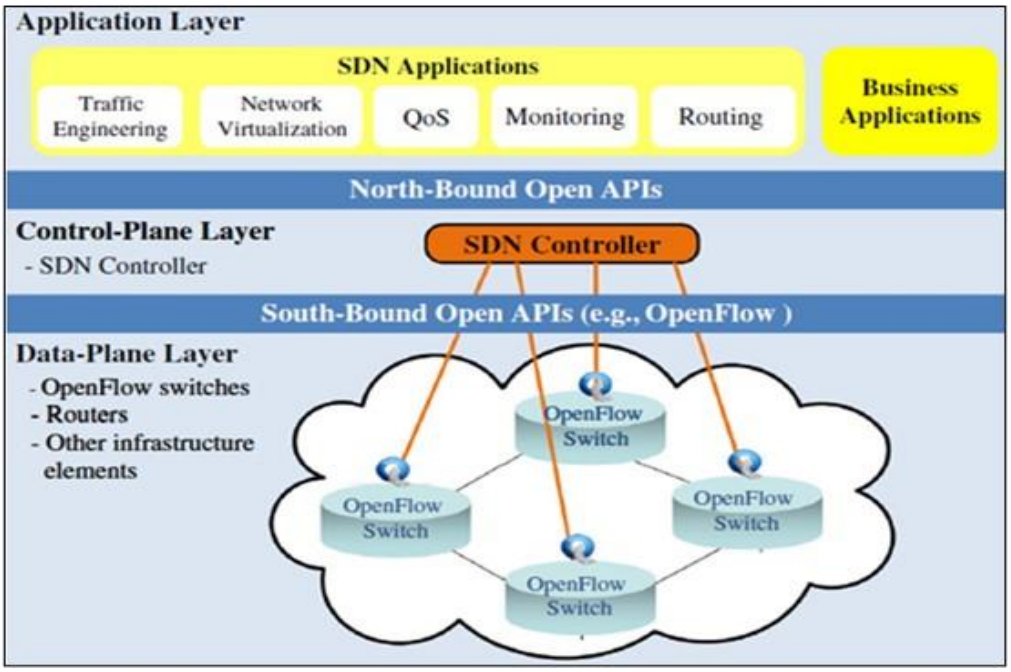
Las redes SDN tienen su principal fundamento en la multiplicidad de avances y desarrollos tecnológicos tanto a nivel de redes, dispositivos, fabricantes y softwares, lo que les otorga un mayor nivel de complejidad. En este sentido Dueñas et al. (2017) afirman que se trata de una solución adecuada para suplir la necesidad de incrementar el ancho de banda, transformar los patrones de tráfico y dar paso a la configuración de nuevos servicios.

Arquitectura

La arquitectura de la red SDN se encuentra conformada por tres componentes principales: infraestructura, control y aplicaciones (Figura 1).

Figura 1

Arquitectura de la Red SDN



Nota: Tomado de Pereira, G., & Gamess, E. (2017). Lineamientos para el despliegue de redes SDN/OpenFlow. *Revista Venezolana de Computación. 4(2)*, 21-33.

La infraestructura de la red (o plano de los datos) hace referencia a todos los dispositivos de red entre los que se encuentran: routers, switches, incluso se realiza una diferenciación entre elementos físicos como el hardware, y elementos virtuales, es decir el software.

- La capa de control corresponde al controlador (o múltiples controladores) que toma decisiones abordando a la totalidad de la infraestructura, de modo que la gestionan de forma adaptativa basados en la configuración básica que se detalla en las tablas de flujo.
- La capa de aplicaciones, por su parte, es aquella en la que se disponen el conjunto de programas que establecen comunicaciones directas con el o los controladores, de modo que permiten establecer requisitos y comportamientos deseados de la red

en su totalidad.

A continuación, se describen cada una de las capas.

Capa controlador. Es la capa fundamental dentro de la arquitectura SDN, dado que con ella se centralizan los componentes de la red y se gestionan, configurando los nodos de manera rápida y eficiente, a partir de lo que toma decisiones. Esta capa media entre los requisitos de funcionamiento de los usuarios (a través de software) y la infraestructura de los datos (García et al., 2014). Desde la perspectiva de Córdoba (2019), ante riesgos de seguridad es conveniente descentralizar en diversos equipos el control ejercido.

Esta capa se compone de interfaces abiertas, donde la primera interactúa con la capa de los datos. Se definen a partir de esto de manera direccional como interfaz southbound, que describe el relacionamiento por instrucciones APO hacia las capas inferiores, obteniendo con ello la relación control-datos; la interfaz northbound es aquella que realiza el intercambio entre controlador con la capa de aplicaciones; por último, las interfaces eastbound y westbound relacionan a los controladores entre sí (Hakiri, 2014, citado en Guanoluisa, 2019).

El controlador interpreta los requisitos establecidos bajo lenguajes como Phyton o C++, y es capaz de presentar el movimiento de la información en una matriz de tráfico. HyperFloy es un ejemplo de uso de varios controladores basado en OpenFlow, con el cual se puede desarrollar un número indeterminado de controladores en la red. Esto permite hacer un diseño escalable y controlar adecuadamente.

Capa de datos. Corresponde al conjunto de los dispositivos de la red SDN, ya sean físicos o virtuales, que se encargan de movilizar los datos dependiendo de las indicaciones recibidas de parte del controlador o controladores de la red. Estos se comunican con otras aplicaciones que se encuentran abstraidas a trapes de API de tipo northbound y abiertas, entre las que puede considerarse como ejemplo el protocolo OpenFlow, sobre el que se hablará más adelante (Pereira & Gamess, 2017).

Estas contienen planos de datos o forwarding planes, que son los que se encargan de movilizar y gestionar campos de cabecera de paquetes; y se compone también de otro plano de carácter operacional, que es el responsable de realizar las tareas de gestión y administración del funcionamiento. Estos dispositivos pueden ser switchs, elementos virtuales ofísicos de reenvío con forwarding planes y southbound (como OpenFlow).

Capa de aplicación. Este plano consiste en la actividad de las aplicaciones SDN y los requisitos establecidos mediante API que establece vínculos con la capa de control. Estas se definen según las necesidades de los usuarios, y son, en la actualidad, una gran variedad de API northbound, sistemas de archivos y lenguajes. Se consideran en ellas las aplicaciones de enrutamiento, cortafuegos, entre otras; estas permiten definir las políticas y las instrucciones específicas que terminan por definir el comportamiento de reenvío (Marrone et al., 2020).

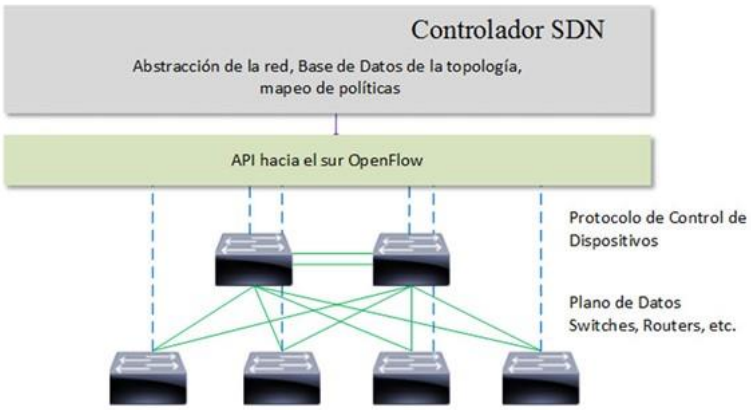
Modos de despliegue SDN

Según Skorupa y Fabbi (2013) para desplegar SDN efectivamente se pueden encontrar tres modelos generales:

- Basado en dispositivos: corresponde a una red de dispositivos o switches SDN de tipo físico que funcionan bajo las instrucciones de un controlador, y que es implementado rápidamente en un contexto nuevo de oficinas. Este tiene la siguiente estructura (Figura 2):

Figura 2

Despliegue SDN basado en dispositivos

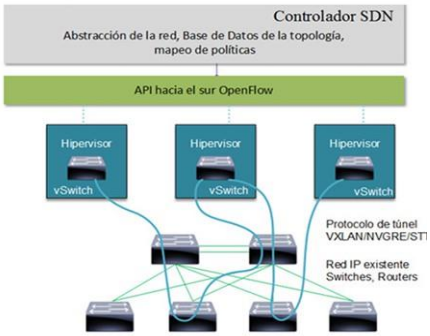


Nota: Tomado de Pereira, G., & Gamess, E. (2017). Lineamientos para el despliegue de redes SDN/OpenFlow. *Revista Venezolana de Computación. 4(2)*, 21-33.

Overlay: corresponde a un grupo de redes superpuestas en una infraestructura física que subyace, de modo que los nodos finales SDN corresponden a dispositivos de carácter virtual, parte de hipervisores que se dan en el entorno de virtualización de servidores. Así, no se altera la red física ni el plano de control que existe, ya que el controlador maneja el reenvío de tráfico de los switches lógicos. Para realizar esto, se establecen túneles overlay entre los nodos SDN lógicos. Esto se visualiza en la Figura 3.

Figura 3

Despliegue SDN overlay



Nota: Tomado de Pereira, G., & Gamess, E. (2017). Lineamientos para el despliegue de redes SDN/OpenFlow. *Revista Venezolana de Computación. 4(2)*, 21-33.

- SDN Híbrido: refiere a la coexistencia en un modelo de red tradicional y un modelo SDN, ubicado en el mismo entorno. Así, un Gateway de tipo SDN funciona bajo modelo overlay como en uno basado en dispositivos; o, bien, un Gateway SDN funcionando bajo protocolos tradicionales y otros protocolos OpenFlow. De esta manera, el Gateway se comunica con controlador o controladores SDN OpenFlow y Ethernet, funcionando bajo los dos esquemas.

Protocolos de comunicación SDN.

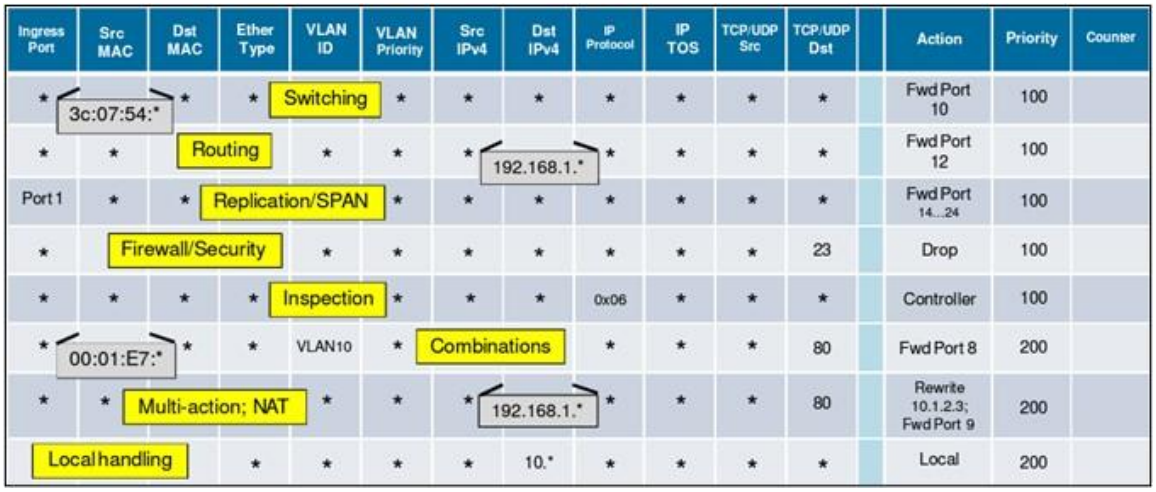
OVSDB. La instancia OVS corresponde a un servidor de base de datos y un Daemon de conmutador virtual (OVSDB-server y OVS-vswitchd respectivamente), donde los clústeres que corresponden a la gestión y al control son los administradores OVSDB y OpenFlow, que pueden estar en el mismo dispositivo o en dispositivos distintos (Iglesias, Álvarez, & Ramos, 2019). Para realizar particularmente la comunicación entre el controlador y el conmutador, el protocolo OVSDB se encuentra desarrollado para Open vSwitch. Este funciona con diferentes implementaciones de software y hardware de tipo OVS. Este gestiona operaciones como la creación de las interfaces o la configuración de parámetros de calidad del servicio.

OpenFlow. OpenFlow es un protocolo que permite aplicar SDN a nivel de software y de hardware, y el cual constituye la primera interfaz completa para SDN (Pereira & Gamess, 2017). Esto se realiza a partir de la estandarización de los mensajes que se intercambian entre controladores y conmutadores. En términos generales, los mensajes dan las instrucciones o parámetros sobre cómo debe funcionar la conmutación y definir estadísticas de los flujos que se dan (Iglesias et al., 2019).

Los protocolos se determinan en las tablas de flujos (ver ejemplo en Figura 4) que establecen cómo es el flujo de información; estas enseñan al conmutador qué hacer con los paquetes, de modo que cuando llega un nuevo flujo, el conmutador refiere a esta tabla de flujo. La entrada es usada para identificar los paquetes y procesarlos, dado que posee un grupo de campos de coincidencia, contadores, tiempos de espera o prioridad e instrucciones determinadas. OpenFlow 1.3 y en adelante presenta cuarenta campos de coincidencia (Figura 4).

Figura 4

Ejemplo tabla de flujo OpenFlow



Nota: Tomado de Pereira, G., & Gamess, E. (2017). Lineamientos para el despliegue de redes SDN/OpenFlow. *Revista Venezolana de Computación. 4(2)*, 21-33.

Cuando estos conmutadores están basados en software, pueden ser instalados en computadores normales de uso general, añadiendo y modificando sus funcionalidades (Krishna, 2016).

Arquitectura OpenFlow. La estructura de OpenFlow se basa en tres factores centrales:

- Red soportada por switches (plano de datos).
- El plano controlador que maneja los switches OpenFlow, ya sea con uno o más controladores.
- Canal de control seguro que permite la comunicación entre switches y controlador(es).

De este modo, los datos se reenvían entre los switches, basados en el protocolo OpenFlow, lo que es controlado por software en un controlador externo ubicado en un servidor. Así, cuando los dispositivos reciben datos, estos son evaluados según las tablas de flujo, buscando la primera concordancia y actuando según lo determinado en ella. Cuando no existen concordancias, el paquete es o bien enviado al controlador o es descartado (Pereira & Gamess, 2017).

Switches OpenFlow. Existen dos tipos de switches, los que son solo de tipo OpenFlow (OpenFlow only), y que como se deduce trabajan procesando paquetes solo bajo este protocolo; y también existe el switch OpenFlow híbrido, el cual tiene aplicación tanto bajo protocolo OpenFlow como bajo protocolos tradicionales.

Controladores SDN

En la arquitectura SDN, el núcleo central se ubica en la capa de control, la cual está fundamentalmente determinada por el controlador SDN, encargado de administrar los flujos de datos. Así, es mediante este controlador que se llevan a cabo las acciones en base a los requisitos establecidos, incluyendo estadísticas e información relativa a eventos.

Dado que OpenFlow es el modelo más utilizado, se describirán a continuación los controladores OpenFlow. Estos ofrecen la posibilidad de realizar tareas de gestión a través de

la propia interfaz de programación para los conmutadores. Corresponde a un sistema de softwares que gestionan el estado de la red (con bases de datos); realiza un modelo de datos que retiene las relaciones entre recursos, políticas y otros servicios (usualmente construidos bajo lenguaje Yang); proveen mecanismos de identificación de dispositivo, topología y servicios; otorgan control seguro sobre el protocolo de control de transmisión; y proveen un conjunto de APs (usualmente RESTful) (García et al., 2014).

Controladores SDN de código abierto. Al momento de implementar un sistema de red SDN, es importante definir adecuadamente el controlador según las características específicas de la red, como su tamaño o su costo. Pereira y Gamess (2017) plantean que existen controladores más robustos para redes grandes o medianas y otros mejor diseñados para redes de pequeño alcance. Como se plantea en Lasso y Puchaicela (2021), los desempeños de las redes tienen relación directa con los controladores SDN. A continuación, se describen algunos controladores utilizados comúnmente y que son de código abierto, esto en concordancia con Pereira y Gamess (2017) y Lasso y Puchaicela (2021):

- OpenDaylight: corresponde a un controlador de arquitectura modular que integra una máquina virtual propia (Java), de modo que puede desplegarse en entornos de cualquier tipo que presenten soporte Java (hardware y software).
- Floodlight: controlador de tipo OpenFlow que es extensible y que se basa igualmente en Java. De licencia Apache, este es desarrollado por una gran comunidad y patrocinado por Big Switch Networks.
- Ryu: corresponde en realidad a un framework SDN que utiliza componentes de APIs definidas y que permiten crear aplicaciones de control y gestionar las redes.
- ODL: programado en Java, tiene un tipo de arquitectura distribuida basada en OpenFlow, con protocolo northbound REST, XMPP o NETCONF. Con licencia EPL 1.0, funciona en plataformas Linux, Windows y MacOS.

Emulación con Mininet

Según Valencia et al., (2015) se debe evaluar previamente el funcionamiento de las redes es central para corregir errores previamente a su implementación. Para esto, existen distintos enfoques, dentro de los cuales se encuentran:

- Banco experimental de pruebas: uso de dispositivos físicos y herramientas como PlanetLab, OFELIA, entre otras. Con este enfoque, es posible crear y testear de manera realista la red diseñada, pero es costoso.
- Simulación: de menor costo, rapidez y flexibilidad, la simulación permite testear las redes, aunque sus resultados no logran ser precisos.
- Emulación: esta se diferencia de la simulación en que el testeo de la red se realiza en tiempo real, ejecutando programas y herramientas de igual manera reales que permiten emular, igualmente, su interacción en la simulación, de modo que sus resultados son más fiables (aunque el retardo de la red puede ser mayor o menor al tiempo efectivamente real).

Con la simulación de las redes es posible evaluar previamente el funcionamiento de un diseño de red y con ello verificar los posibles fallos y otros contratiempos. Esto permite reducir costos de instalación y mejoras, además de depurar los errores y realizar pruebas sin afectar la seguridad (Córdoba, 2019; Ruiz et al., 2019).

Mininet es un programa emulador que permite elaborar escenarios de redes de tipo virtual basado en GNU/Linux. En él pueden crearse los nodos de la red (ya sean switches, routers o controladores) y puede visualizarse su funcionamiento en un solo dispositivo en el que se encuentre el emulador (Duarte & Lobo, 2015). Dentro de este, Miniedit es el editor dentro del entorno que permite crear en un entorno gráfico las redes requeridas.

En Mininet los programas ejecutados realizan el trabajo de envío de paquetes a la velocidad que debiera hacerlo una red con las características particulares determinadas. El conmutador que procesa la información es prácticamente igual en términos de resultado a un

enrutador Ethernet real. De igual manera, hosts, enlaces y controladores tienen las mismas funcionalidades que los reales, con la diferencia de que todos son virtuales o software (Jiménez & Ramos, 2018).

Para Jiménez y Ramos (2018) algunas de las ventajas de realizar una simulación de redes con Mininet son:

- Simulación con rapidez.
- Uso de innumerables topologías.
- Pueden ejecutarse diversos programas en el emulador.
- Pueden personalizarse los paquetes (por ej. Programarse bajo OpenFlow).
- Posibilidad de ejecutar el emulador en varios dispositivos.
- Código abierto.
- Constante desarrollo.

Entre las desventajas que pueden identificarse, se encuentran:

- Dado el uso de núcleo Linux, no puede ejecutar programas de otras plataformas.
- Requiere del uso de controladores OpenFlow independientes.

Diseño metodológico

El presente trabajo tuvo por objetivo analizar técnica y económicamente la implementación de una red SDN en el backbone de la Sede Matriz de la Universidad de las Fuerzas Armadas. Para esto, se realizó el diseño de una red SDN mediante simulación a través del software Mininet basado en Linux con parámetros de seguridad y escalabilidad para la red de Backbone en la matriz de la Universidad de las Fuerzas Armadas; igualmente se realizó un análisis económico costo/beneficio de la implementación de una red SDN basado en indicadores ROI, VAN y TIR; y, además, se realizaron pruebas de conectividad hacia 4 campus

de la ESPE (Latacunga, Santo Domingo, Salinas y Shell) para evaluar el rendimiento de la red mediante indicadores latencia, jitter, throughput.

El enfoque de la investigación es de carácter cualitativo, cuantitativo y aplicado, dado que a partir del diagnóstico y caracterización de la situación actual mediante métodos cualitativos se realizó una propuesta aplicada y se evaluó tanto técnica como económicamente. De esta manera, se utilizó el enfoque cualitativo para fundamentar teóricamente el estudio y para caracterizar la situación actual de la red de la institución. Los análisis técnico y económico, por su parte, tuvieron un enfoque mixto (cualitativo y cuantitativo), por cuanto se desarrollaron mediante la observación y la evaluación en función de la medición de métricas determinadas y del análisis costo/beneficio de la propuesta desarrollada.

Los métodos utilizados se detallan a continuación en función de las etapas de desarrollo del trabajo:

Diagnóstico de situación actual

Para el diagnóstico de la situación actual se realizó una entrevista al encargado del Departamento de Informática de ESPE con el objetivo de conocer los siguientes factores:

- Estado actual del funcionamiento de la red en ESPE (topología y problemas).
- Requerimientos y problemas a mejorar en el desarrollo de la simulación.
- Funcionalidades.
- Disponibilidad de recursos.

De igual manera, se realizó un análisis documental para fundamentar teóricamente el trabajo y adecuar la propuesta al contexto de la institución.

Simulación

Para la simulación, se determinó como método el emulador Mininet basado en Linux y se establecieron los siguientes componentes para la simulación:

Herramientas de desarrollo. Máquina física para simulación 8GB RAM, procesador de 2 GH, máquina virtual Linux (Ubuntu, Red Hat u otra distribución), controlador SDN seleccionado y emulador Mininet (simulación mediante Miniedit / Phyton / línea de comandos).

Selección del controlador. Para seleccionar el controlador, se ha decidido comparar los tres más utilizados en la actualidad, idealmente con código abierto para adaptarlo completamente a las necesidades particulares de la institución.

Tabla 1

Comparativa controladores SDN de código abierto

Característica	OpenDaylight [a]	Floodlight [a]	ONOS [a]	Ryu [b]
Lenguaje	Java	Java	Java	Phyton
Plataforma	Linux Windows Max	Linux Windows Mac	Linux Windows Mac	Linux
Tipo de arquitectura	Distribuida	Centralizada	Distribuida	Arquitectura completa de framework
Protocolos southbound / northbound	OpenFlow REST NETCONF	OpenFlow REST JavaRPC	OpenFlow Neutron	OpenFlow, NETCONF OF-config
Licencia	ELP	Apache	Apache	Apache

Nota: Tomado de Lasso, D., & Puchaicela, J. (2021). *Evaluación del rendimiento de un prototipo SDN (Software Defined Networking) bajo el protocolo OpenFlow utilizando herramientas OpenSource en un entorno virtualizado.* [Tesis de grado] Universidad Politécnica Salesiana. En http://dspace.ups.edu.ec/handle/123456789/19861; Pachés, A. (2020). *Estudio del controlador SDN Ryu sobre una Raspberry-Pi Model 4.* [TFG] Universitat Politecnica de Valencia. En https://m.riunet.upv.es/bitstream/handle/10251/152347/Juli%C3%A1n%20-

%20Estudio%20del%20controlador%20SDN%20Ryu%20sobre%20una%20Raspberry-Pi%20Model%204.pdf?sequence=1&isAllowed=y.

Se ha seleccionado el controlador Floodlight debido a las características particulares de la red de la institución, el cual se utilizará con la aplicación southbound OpenFlow, siendo igualmente utilizado este protocolo.

Análisis técnico

Para el análisis técnico de la simulación se considerarán pruebas de configuración y pruebas de desempeño. Para esto, se definieron métricas de evaluación determinadas para cada caso, esto con base en la investigación documental y de acuerdo al uso de Mininet como emulador. Así, las pruebas son las siguientes.

Pruebas de configuración. Las pruebas de configuración tienen por objetivo evaluar la correcta adecuación de las características establecidas al momento de realizar la simulación de SDN en Mininet. Así, entre estas se encuentran en la Tabla 2.

Tabla 2

Métricas de evaluación para pruebas de configuración

Métrica	**Determinación**
Conectividad entre nodos	Ejecución de *comandos ping, pingall,*
Intercambio de mensajes	Para el caso de OpenFlow, puede definirse con el uso de Wireshark.
Integración con elementos tradicionales	Valoración cualitativa.

Nota: Tomado de Gámez, L., Calderón, A., & Ballester, S. (2016). Evaluación de desempeño y configuraciones de las SDN mediante la simulación. *TONO vol. 13*, 29-33.; Oviedo, B., Zhuma, E., Guzmán, D., & Cáceres, C. (2020). Análisis del desempeño de redes definidas por software frente a redes con arquitectura TCP/IP. *RISTI*, 137-150.

Pruebas de desempeño. Se establecieron las siguientes métricas de evaluación de desempeño (Tabla 3).

Tabla 3

Métricas de evaluación para pruebas de desempeño

Métrica	Determinación
Latencia	Valores del parámetro RTT durante el intercambio de mensajes (mínimo, promedio, máximo y desviación estándar). Comando *ping* [a]
Pérdida de paquetes	Comando *ping* (pérdida de paquetes en función de la cantidad de paquetes intercambiados) [a]
Throughput	Comando *Iperf* [a]

Nota: Tomado de Gámez, L., Calderón, A., & Ballester, S. (2016). Evaluación de desempeño y configuraciones de las SDN mediante la simulación. *TONO vol. 13*, 29-33; Quintero, D., & Medina, J. (2020). *Evaluación del rendimiento de una red LAN y una red WAN tradicional bajo el estándar IEEE 802.3 y la norma RFC 3031 en un entorno simulado, aplicando procesos SDN.* [TFG] ITM. Disponible en https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/4692/DanielStiven_QuinteroLondo%c3%b1o_2021.pdf?sequence=1&isAllowed=y.

Análisis económico

El análisis costo/beneficio permite evaluar proyectos de inversión mediante la determinación de los costos y los beneficios asociados a este. A partir de este análisis es posible tomar decisiones de inversión adecuadas que permitan mantener la rentabilidad de los proyectos, considerando todos los beneficios (Aguilera, 2017). De esta manera, el análisis de costo/beneficio considera las siguientes etapas:

- Determinación de objetivos del proyecto
- Examen de requerimiento y limitaciones
- Definición monetaria de los costos de cada operación
- Determinar los costos y beneficios en el tiempo
- Actualizar el flujo de caja
- Determinar el numerador (beneficios) de la razón
- Determinar el denominador (costos) de la razón
- Analizar los otros indicadores para definir la factibilidad de la implementación
- Para realizar la evaluación económica de la propuesta, se utilizaron los siguientes indicadores.

En la siguiente tabla se presentan los indicadores de la evaluación económica de un proyecto:

Tabla 4

Indicadores de evaluación económica

Indicador	Definición / cálculo
ROI [b]	(Return On Investment) es el valor económico generado como resultado de la realización de diferentes actividades de marketing. Con este dato es posible medir el rendimiento obtenido de una inversión. Está dado por: $$ROI = \frac{(beneficio\ obtenido - inversión)}{inversión}$$
VAN [a]	El valor actual neto es un indicador financiero que sirve para determinar la viabilidad de un proyecto. Si tras medir los flujos de los futuros ingresos y egresos y descontar la inversión inicial queda alguna ganancia, el proyecto es viable. Está dada por: $$VAN = \sum_{t=0}^{N} \frac{FC_t}{(1+r)^t} - \text{Inversión}$$
TIR [a]	La tasa interna de retorno puede utilizarse como indicador de la rentabilidad de un proyecto: a mayor TIR, mayor rentabilidad; así, se utiliza como uno de los criterios para decidir sobre la aceptación o rechazo de un proyecto de inversión. Está dado por la tasa que iguala VAN a 0: $$\text{TIR} = \text{Tm} + (\text{TM} - \text{Tm})\frac{VAN\ Tm}{VAN\ Tm - VAN\ TM}$$

Nota: Tomado de Bargted, C., & Kettlun, A. (2016). *Indicadores de evaluación de proyectos.* Santiago: Universidad de Chile; Aguilera, A. (2017). El costo-beneficio como herramienta de decisión en la inversión en actividades científicas. *Cofin Habana. 11(2)*, En línea. Disponible en http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2073-60612017000200022.

Capítulo III

Simulación red SDN en Mininet

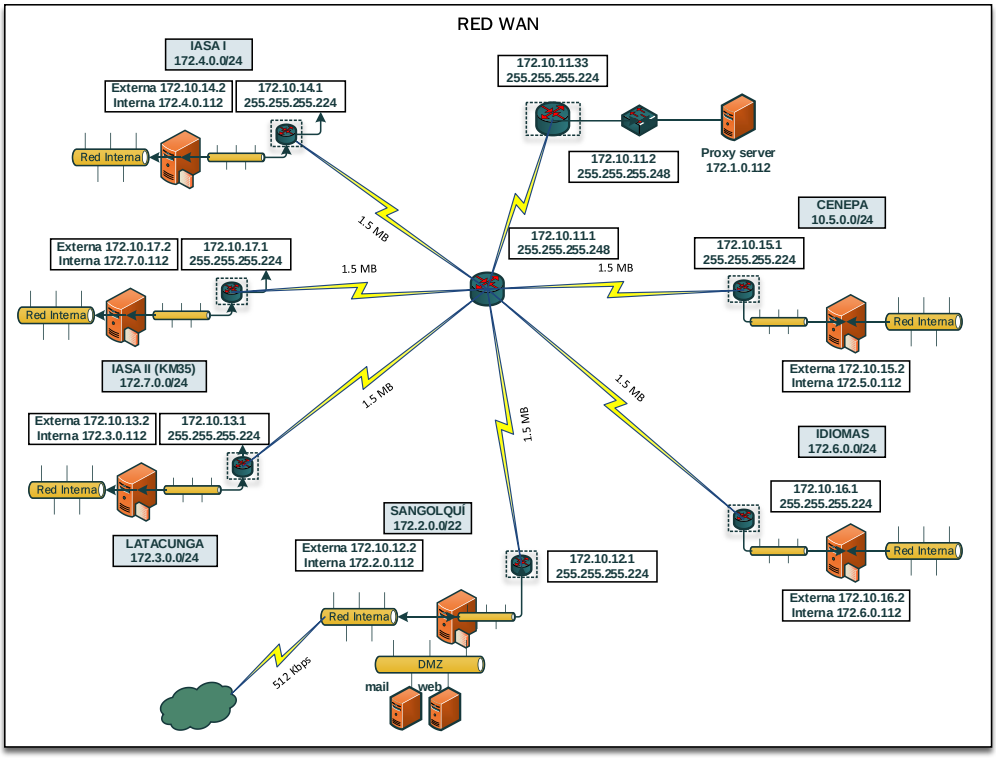
Análisis de infraestructura de red actual

Red WAN

Previo a la implementación de la tecnología o protocolo MPLS (*Multiprotocol Label Switching*), la Universidad de las Fuerzas Armadas aplica la red WAN, la cual cuenta con diversos equipos para el funcionamiento de la red actual, entre estos se encuentran el router para el balanceo de la carga, servidores DMZ, Firewall ASA, CORE antiguo, packet shaper, SW (6513 y 6506) y Standby. La topología de la red WAN con sus respectivas direcciones IP se muestra en la Figura 5.

Figura 5

Topología de la Red WAN – ESPE



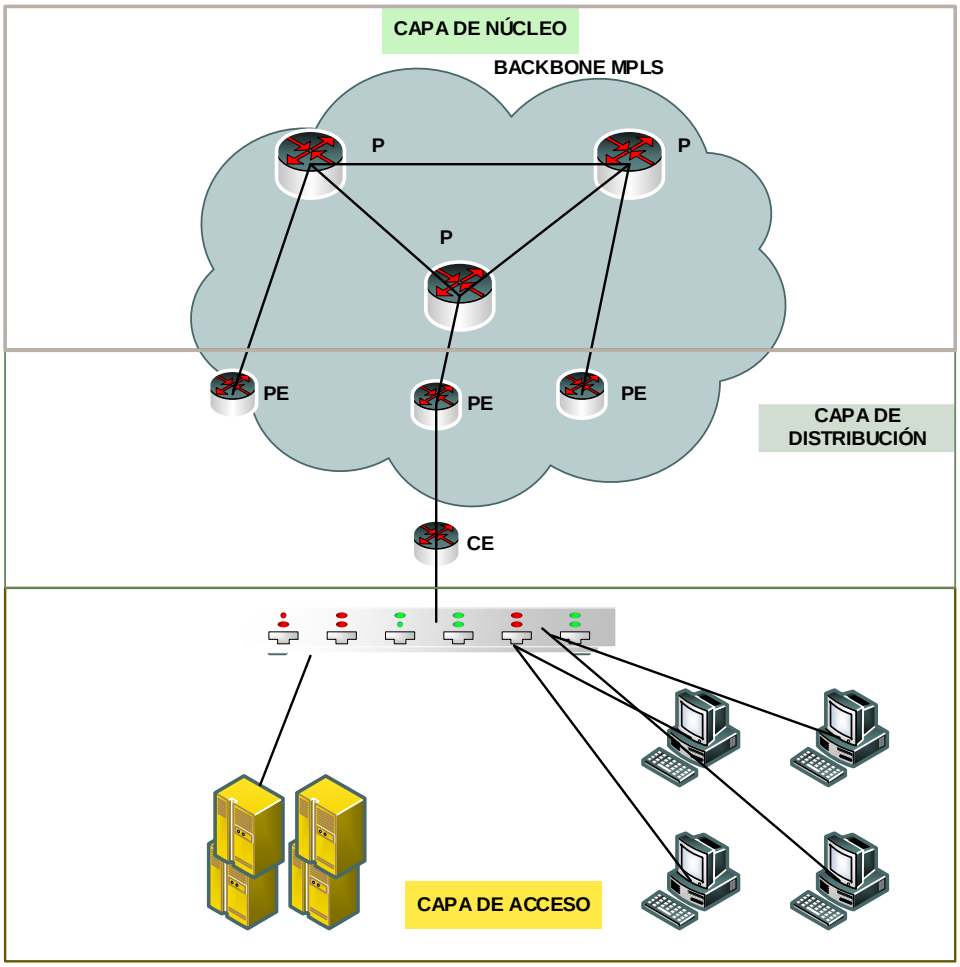
Nota: Tomado de ESPE (2020).

Red Backbone MPLS

Posteriormente, la institución implementó la tecnología basada en protocolo MPLS con el fin de mejorar el servicio, administrar y brindar seguridad. La red MPLS de la universidad está formada por tres capas como núcleo, distribución y acceso. La capa de núcleo (Backbone MPLS) conformado routers (P) para balancear la carga. La capa de distribución consta de LERs mientras que la capa de acceso está formada por toda la red LAN, lo cual se aprecia en la Figura 6.

Figura 6

Arquitectura de capas de Red MPLS – ESPE

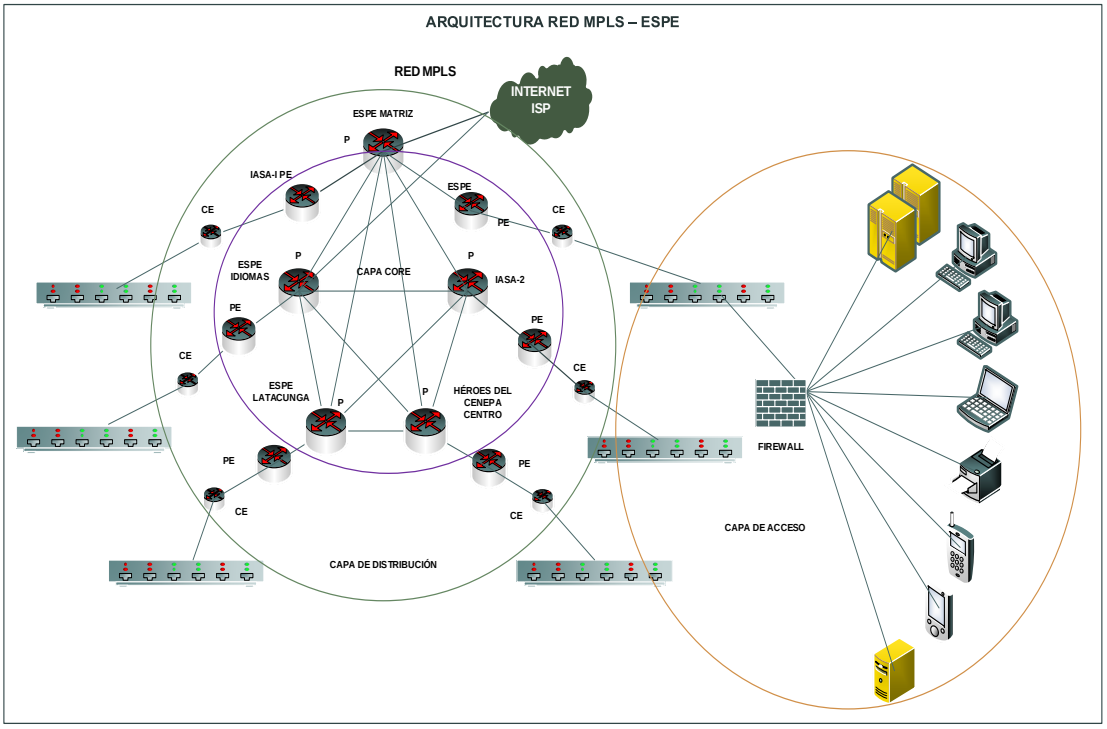


Nota: Tomado de ESPE (2020).

De igual modo se presenta la arquitectura de la red MPLS (Figura 7), es así que en la capa de core se observa los routers de la matriz, IASAI, IASA2, Idiomas, sede Latacunga, entre otros. Dentro de la capa de distribución está la capa core. En la capa de acceso se tiene un firewall para bloquear el acceso no autorizado y solo permitiendo el acceso autorizado para las sedes y extensiones de la institución.

Figura 7

Arquitectura de Red MPLS – ESPE



Nota: Tomado de ESPE (2020).

Además, se conoce que tienen varios switches de 3Com y CISCO para conectar y acceder a los servicios de la universidad. A continuación, se describe la cantidad de switches según capas de la red:

Switch de Core. 2 Switches Cisco Catalyst 6513-E.

Switch de Distribución. 1 Switch Cisco Catalyst 2960, 2 Switches Cisco Catalyst 6506-E, 1 Switch 3COM 5500.

Switch de Acceso. 21 Switches Cisco Catalyst 3960, 14 Switches Cisco Catalyst 2960, 39 Switches 4500, 6 Switches 5500, 5 Switches 4200, 2 Switches 3COM 4210, 5 Switches 4250, 2 Switches 3250, 1 Switch 2226, 3 Switches HP Procurve.

Cabe mencionar que la capa core cuenta con switches Cisco Catalyst 6513-E con tecnología *Virtual Switching System* (VSS) para la administración de la red en sistema de conmutación virtual. La capacidad de troughput es 720Gbps de cada chasis y cuando se combina llega a una capacidad máxima de 1400Gbps. Además, en switch CORE 6500 se realiza la virtualización de equipos en un solo switch, lo cual ayuda a conmutar, evitando el corte del servicio y ampliar el ancho de banda a 1,4 Tbps. Este switch se conecta mediante VSS, utilizando la tarjeta supervisora 720 10GE.

Las tarjetas de switch CORE se encuentran descritas en la Tabla 5.

Tabla 5

Tarjeta chasis de Switch CORE

Tarjeta	No.	Módulo	Puertos	Descripción
Chasis 1	1		24	Tarjeta de 24 puerto de 1Gbps
	2			Tarjeta controladora de red inalámbrica
	3			Tarjeta de administración de balanceo de carga
	4			Tarjeta supervisora 720 10GE
	5		48	Tarjeta de 48 puertos de 1Gbps
	6		16	Tarjeta de 16 puertos de 1Gbps
Chasis 2	1	3	24	Tarjeta de 24 puerto de 1Gbps
	2	7	5	Tarjeta supervisora 720 10GE
	3	9	48	Tarjeta de 48 puertos de 1Gbps
	4	10	16	Tarjeta de 16 puertos de 10Gbps

Nota: Tomado de ESPE (2020).

Para brindar servicio de la red cuenta con enlace de 1800 Mbps del proveedor Telconet, es decir, ayuda a brindar Internet a los equipos; incluso dispone de un router que tiene un

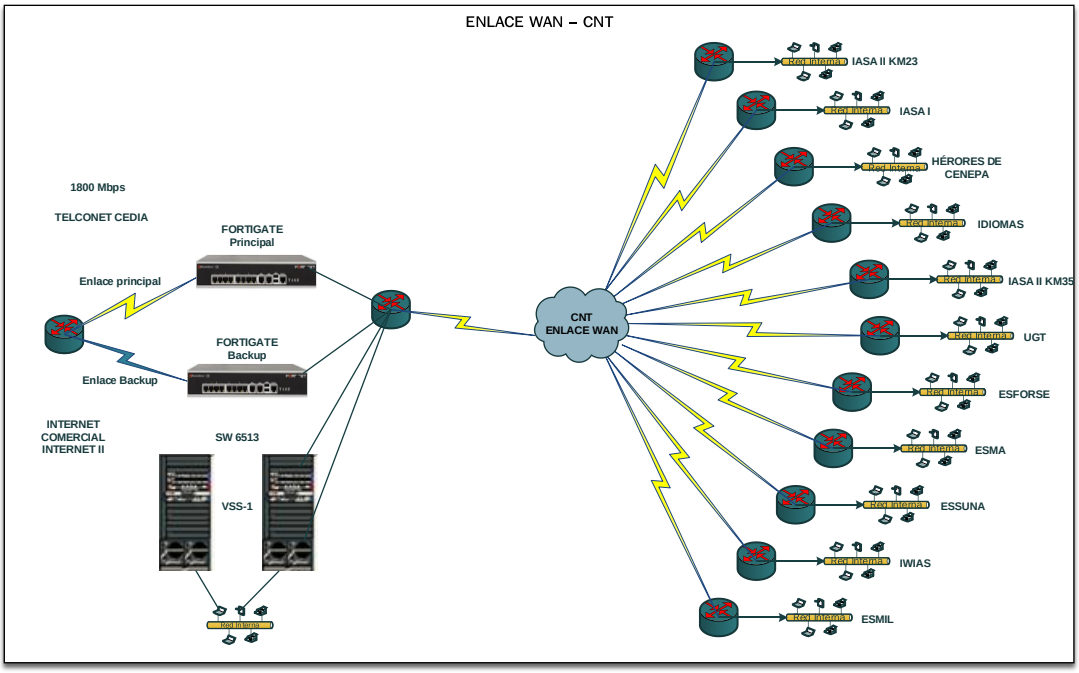
enlace principal y de refuerzo, estos se vinculan a los servidores internos y a FortiGate. El router se conecta a todas las sedes de la universidad, estos se detallan a continuación:

- Matriz
- Sede Latacunga
- Santo Domingo
- IASA I e IASA II (km 23 y 35)
- ESMIL
- Idiomas
- Héroes del Cenepa
- ESFROSE
- Salinas
- ESMA
- IWIAS
- ESUNA
- UGT

En la siguiente figura se observa las conexiones de punto a punto de la red MPLS de la universidad. Las sedes se conectan por medio del enlace WAN a la antena del proveedor CNT (Corporación Nacional de Telecomunicaciones) para brindar servicio de Internet.

Figura 8

Topología conexiones punto a punto Red MPLS – ESPE



Nota: Tomado de ESPE (2020).

Otro aspecto importante se relaciona con los costos del servicio de Internet para la red MPLS cuyo proveedor es Telconet, donde el costo de instalación es de $11.000 mientras que el costo mensual se ubica en $8.400, lo que significa un costo anual superior a los $100.000.

Red Inalámbrica Matriz- Espe

La matriz de la institución Superior cuenta con una red inalámbrica unificada, lo cual ayuda en la centralización del sistema para la administración automática, es así que se puede observar y monitorear los Access Point en tiempo real. Los Access Point se encarga de asignar de manera automática las frecuencias, potencias y cargas de los puntos de acceso.

La red inalámbrica tiene una velocidad de transmisión de 11 y 54 Mbps; incluyendo una capacidad máxima de 600 Mbps, para esto se tomó en cuenta el estándar 802.11n del Instituto de Ingenieros Eléctricos y Electrónicos – IEEE o por sus siglas en inglés *Institute of Electrical and Electronics Engineers*.

Los componentes de esta red son: un controlador de red inalámbrica Cisco WIS-M2, software de gestión (Cisco Prime Infrastructure) y Access Point de Cisco de numeración 3502, 3602 y 1552. La infraestructura de la red se detalla a continuación:

Controlador de Red Inalámbrica (Cisco WIS-M2). Este controlador es un módulo utilizado para el procesamiento y gestión de Access Point, así como la configuración y control de redes, lo cual es flexible y escalable, es decir, se puede agregar nuevos servicios (Figura 9).

Figura 9

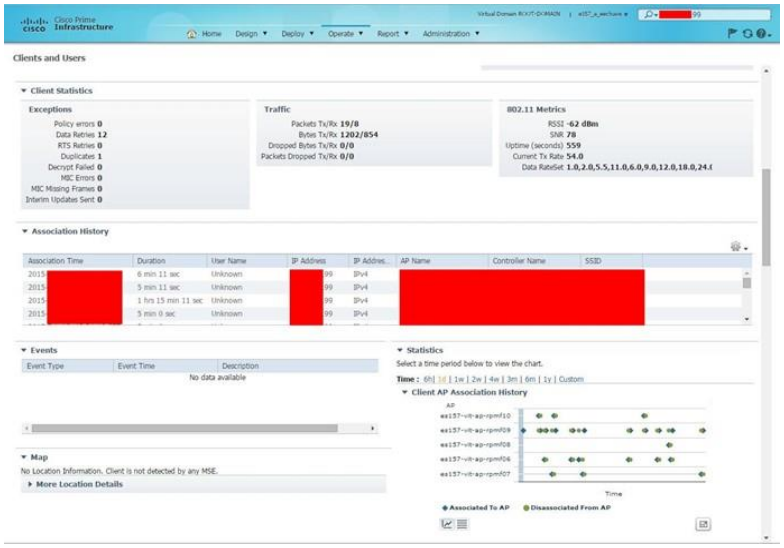
Controlador Cisco WIS-M2 – ESPE

Nota: Tomado de Cisco. (17 de Junio de 2019). *Módulo de servicios inalámbricos de Cisco 2 (WiSM2)*. https://www.cisco.com/c/en/us/products/interfaces-modules/wireless-services-module-2-wism2/index.html

Software de gestión de red (Cisco Prime Infrastructure). El software de gestión de modelo Cisco Prime Infrastructure ayuda a planificar, configurar los servicios de la red, revisar el estado de los dispositivos y canales, incluyendo la cantidad de usuarios conectados y su ubicación en tiempo real.

Figura 10

Software Cisco Prime Infrastructure – ESPE



Nota: Tomado de Cisco. (31 de Agosto de 2015). *Infraestructura Prime 3.0*. https://software.cisco.com/download/home/286285348/type/284272932/release/3.0.0

Access Point ligeros (Cisco 3502, 3602, 1552). Los equipos de Access Point modelo Cisco 3502, 3602 y 1552 ayudan a que los usuarios accedan a los servicios o recursos de la red, dando cobertura a las sedes y extensiones de la universidad (Figura 11)

Figura 11

Access Point Cisco – ESPE

3502 *3602* *1552*

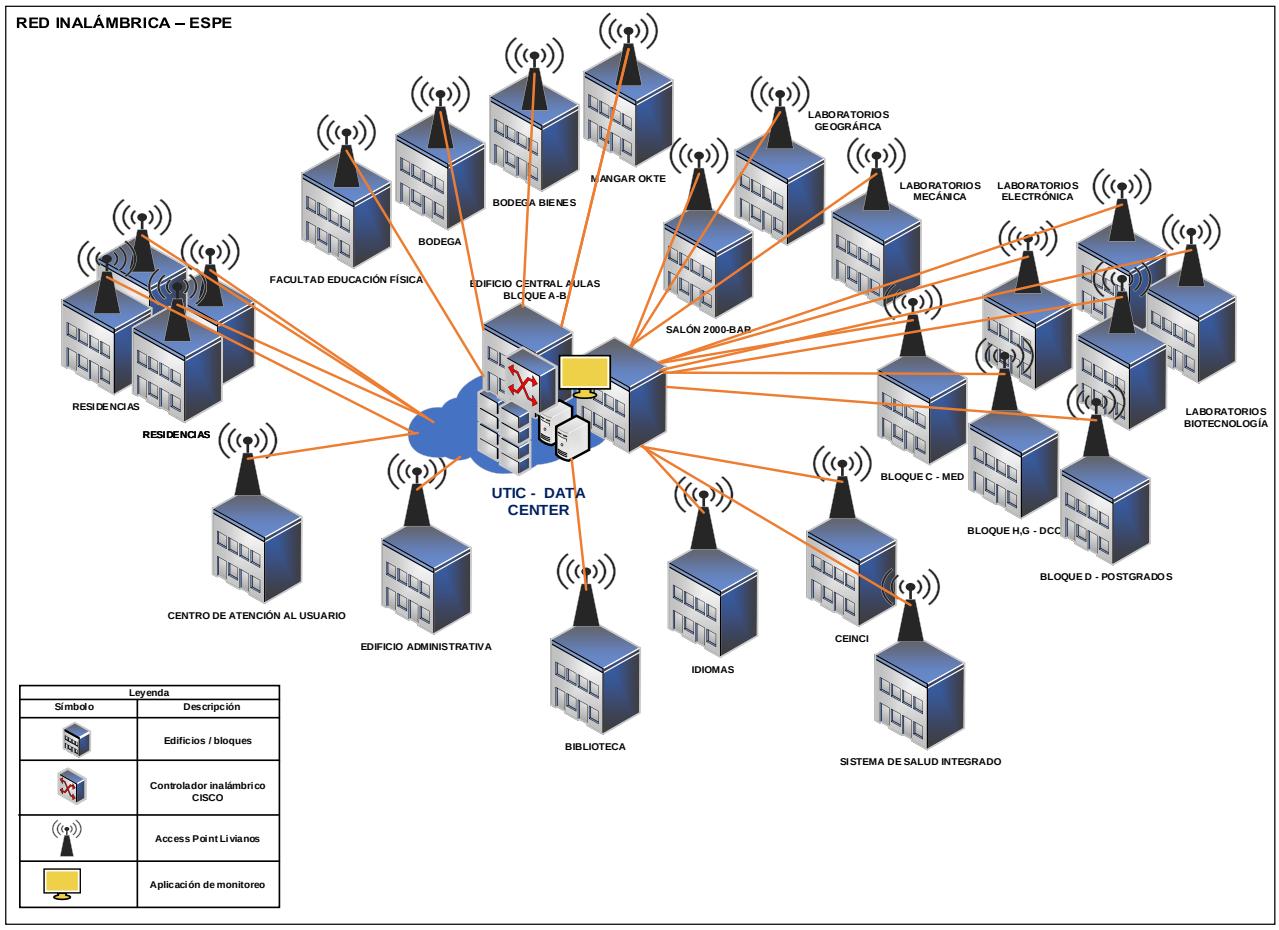
Nota: Tomado de Cisco. (25 de Noviembre de 2016). *Wireless*.

https://www.cisco.com/c/es_mx/support/wireless/index.html

Además, la red inalámbrica de la matriz – ESPE se encuentra formada por 26 edificios o bloques, 1 controlador inalámbrico Cisco, 127 Access Point livianos y 1 aplicación de monitoreo (Figura 12).

Figura 12

Red Inalámbrica – ESPE



Nota: Tomado de ESPE (2020).

Con los aspectos detallados de la infraestructura de la red de la Universidad de las Fuerzas Armadas – ESPE se conoció que hace falta implementar un protocolo más robusto para la comunicación de los datos, esto significa que no dispone de una infraestructura centralizada que ayude a contar con flexibilidad y la gestión de la red para brindar servicios en las distintas sedes y extensiones de la institución.

Simulación implementación SDN en la red backbone con Mininet

Requerimientos para la simulación

El sistema operativo utilizado es Linux, en particular la distribución Ubuntu 14.04. Los paquetes utilizados son:

Floodlight v1.0. Floodlight corresponde a un controlador tipo OpenFlow basado en Java, con licencia Apache y de código abierto. Su desarrollo es comunitario, y admite protocolos de OpenFlow 1.0 a 1.5 (UTA, 2015).

Los conmutadores que funcionan con este controlador son Open vSwitch (OVS) y Ofsoftswitch (virtual switches); Arista 7050, Brocade MLXe, Brocade CER, Brocade CES, Dell S4810 y Z9000, Extreme Summit x440, x460, x670, HP 3500, 3500yl, 5400zl, 6200yl, 6600, y 8200zl, y HP V2 line cards in the 5400zl and 8200zl, Huawei openflow-capable router platforms, IBM 8264, Juniper (MX, EX), NEC IP8800, PF5240 y PF5820, NetGear 7328SO y 7352SO y Pronto (3290, 3295, 3780). (hardware switches).

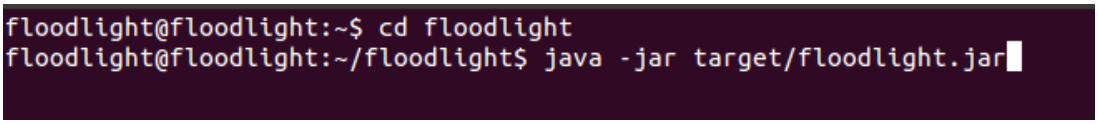
Para instalar en Ubuntu el paquete de Floodlight, debe ejecutarse el comando (HowtoInstall, 2021):

sudo apt-get update

sudo apt-get install floodlight

Figura 13

Ejecución de Floodlight



Nota: Tomado de UTA (2015).

Eclipse IDE. Para modificar aspectos del controlador Floodlight, se utilizó Eclipse, que corresponde a un entorno de desarrollo para programar de código abierto (Eclipse, 2021).

Para la instalación, es preciso contar previamente con Java Runtime Enviroment (JRE). Una vez comprobada la correcta instalación, es posible instalar desde paquete de instalador descargado o bien de la web o bien con el comando wget (Conpilar, 2021):

$ wget https://download.eclipse.org/oomph/epp/2020-06/R/eclipse-inst-linux64.tar.gz

Una vez descargado (en el directorio correspondiente a descargas), es preciso extraer el archivo tarball en ‘/ opt’ con el comando:

$ sudo tar -xf eclipse-inst-linux64.tar.gz -C /opt

Y, por último, se instala Eclipse con los comandos:

$ cd /opt/eclipse-installer

$ sudo ./eclipse-inst

Una vez realizado esto, aparece la ventana de instalación de Eclipse, en donde debe seleccionarse el paquete a instalar según el lenguaje y las necesidades de la programación. Aceptados las ventanas de licencia, se termina de realizar la instalación de la plataforma.

Figura 14

Instalación de Eclipse

Nota: Tomado de Conpilar. (12 de 03 de 2021). *Cómo instalar Eclipse IDE en Ubuntu 20.04*. ConpilarNews: https://conpilar.es/como-instalar-eclipse-ide-en-ubuntu-20-04/

Mininet. Emulador que permite elaborar escenarios de redes de tipo virtual basado en GNU/Linux. En él pueden crearse los nodos de la red (ya sean switches, routers o controladores) y puede visualizarse su funcionamiento en un solo dispositivo en el que se encuentre el emulador (Duarte & Lobo, 2015).

Para instalar Mininet en Ubuntu se debe descargar con el comando:

git clone https://github.com/mininet/mininet

Una vez descargado, debe ejecutarse el siguiente comando (HowtoInstall, 2021):

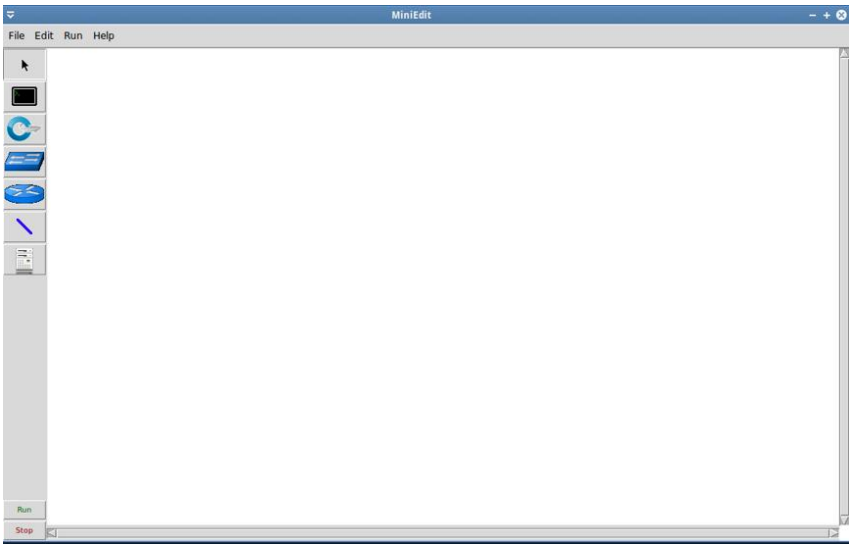
sudo apt-get update

sudo apt-get install mininet

El programa ejecutado en su interfaz gráfica se observa a continuación:

Figura 15

Interfaz gráfica de Mininet



Nota: Tomado de ProgramadorClic. (12 de 12 de 2021). *Instalación y uso de SDN-Mininet*. https://programmerclick.com/: https://programmerclick.com/article/49491544256/

Open vSwitch v2.3.1 (OVS). OVS es un servidor de base de datos y un Daemon de conmutador virtual (OVSDB-server y OVS-vswitchd respectivamente), en el cual los clústeres que refieren a la gestión y al control son los administradores OVSDB y OpenFlow. Estos pueden estar en el mismo dispositivo o estar en dispositivos distintos (Iglesias, Álvarez, & Ramos, 2019).

Para instalar OVS, se ejecutan los siguientes comandos (HowtoInstall, 2021):

sudo apt-get update

sudo apt-get install openvswitch-switch

Wireshark con OpenFlow disector. Corresponde a un analizador de protocolos de red ampliamente utilizado, que permite evaluar la red mediante inspecciones en vivo y fuera de línea, navegar por paquetes estándar, entre otras funciones (Wireshark, 2021).

Para instalar Wireshark deben ejecutarse los comandos (WebSetNet, 2020):

sudo add-apt-repository universe

sudo apt install wireshark

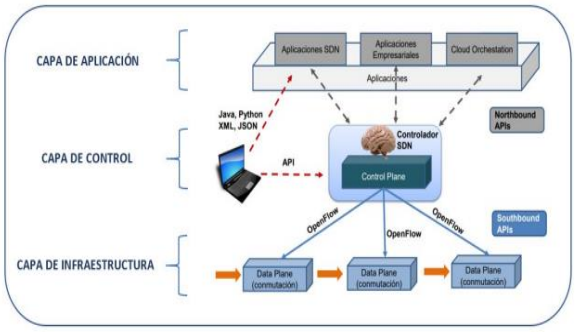
Es preciso tener habilitado el repositorio Universe en Ubuntu.

Topología de la red

La topología de la red SDN simulada en el backbone de la Sede Matriz de la Universidad de las Fuerzas Armadas presenta una arquitectura de 3 capas. Estas corresponden a la capa de infraestructura, es decir, el plano de datos (conmutación); la capa de control, en donde se ubica el controlador SDN y API; y la capa de aplicación, la que contiene las aplicaciones SDN, las empresariales y Cloud Orchestation.

Figura 16

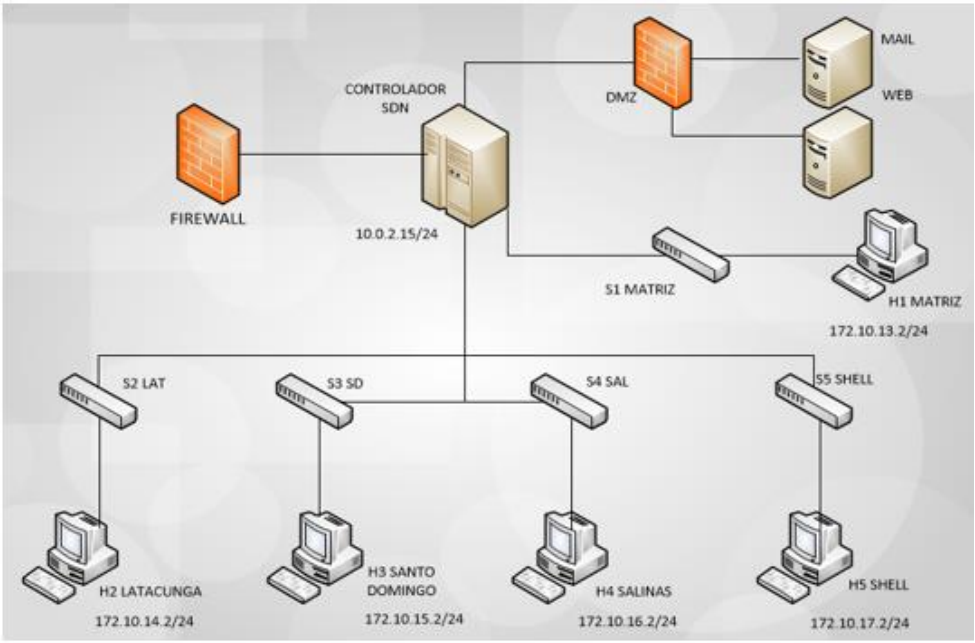
Arquitectura de la red simulada



La topología para la red SDN simulada a implementar en el backbone de la ESPE se presenta en la Figura 17.

Figura 17

Topología de la red



Nota: Cada uno de estos se identifica en la Tabla 6.

Tabla 6

Topología de la red. Nomenclatura

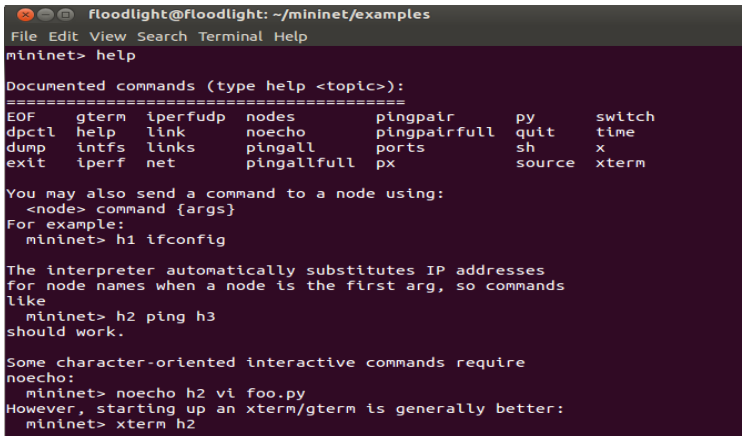
Nomenclatura	Descripción
s1Matriz	Switch correspondiente a la Matriz
s2LT	Switch correspondiente a la sede Latacunga
s3SD	Switch correspondiente a la sede Santo Domingo
s4Sal	Switch correspondiente a la sede Salinas
s5Shell	Switch correspondiente a la sede Shell
Controlador SDN	Corresponde al controlador ubicado en la Matriz
h1, h2, h3, h4 y h5	hosts
-------	Northbound APIs
——	Southbound APIs

Comandos disponibles en Mininet

Los comandos que se encuentran disponibles en Mininet corresponden a los que se presentan en la Figura 18. Estos han sido considerados para realizar las configuraciones y las pruebas de la red SDN simulada.

Figura 18

Comandos en Mininet



Configuración de equipos

Para configurar la red se utilizó el siguiente código en Python:

```
from mininet.net import Mininet
from mininet.node import Controller, RemoteController, OVSController
from mininet.node import CPULimitedHost, Host, Node
from mininet.node import OVSKernelSwitch, UserSwitch
from mininet.node import IVSSwitch
from mininet.cli import CLI
from mininet.log import setLogLevel, info
from mininet.link import TCLink, Intf
from subprocess import call
def myNetwork():
net = Mininet( topo=None,
```

```
        build=False,
        ipBase='10.0.0.0/16')
        info( '*** Adding controller\n' )
MatrizC0=net.addController(name='MatrizC0',
        controller=RemoteController,
        ip='10.0.2.15',
        protocol='tcp',
        port=6653)

info( '*** Add switches\n')
s5Shell = net.addSwitch('s5Shell', cls=OVSKernelSwitch)
s4Sal = net.addSwitch('s4Sal', cls=OVSKernelSwitch)
s3SD = net.addSwitch('s3SD', cls=OVSKernelSwitch)
s1Matriz = net.addSwitch('s1Matriz', cls=OVSKernelSwitch)
s2LT = net.addSwitch('s2LT', cls=OVSKernelSwitch)

info( '*** Add hosts\n')
h4 = net.addHost('h4', cls=Host, ip='172.10.16.2', defaultRoute=None)
h1 = net.addHost('h1', cls=Host, ip='172.10.13.2', defaultRoute=None)
h3 = net.addHost('h3', cls=Host, ip='172.10.15.2', defaultRoute=None)
h2 = net.addHost('h2', cls=Host, ip='172.10.14.2', defaultRoute=None)
h5 = net.addHost('h5', cls=Host, ip='172.10.17.2', defaultRoute=None)

info( '*** Add links\n')
net.addLink(s1Matriz, h1)
net.addLink(s2LT, h2)
```

```
net.addLink(s3SD, h3)
net.addLink(s4Sal, h4)
net.addLink(s5Shell, h5)
net.addLink(s1Matriz, s2LT)
net.addLink(s2LT, s3SD)
net.addLink(s3SD, s4Sal)
net.addLink(s4Sal, s5Shell)

info( '*** Starting network\n')
net.build()
info( '*** Starting controllers\n')
for controller in net.controllers:
        controller.start()

info( '*** Starting switches\n')
net.get('s5Shell').start([MatrizC0])
net.get('s4Sal').start([MatrizC0])
net.get('s3SD').start([MatrizC0])
net.get('s1Matriz').start([MatrizC0])
net.get('s2LT').start([MatrizC0])

info( '*** Post configure switches and hosts\n')
s5Shell.cmd('ifconfig s5Shell 172.10.17.1')
s4Sal.cmd('ifconfig s4Sal 172.10.16.1')
s3SD.cmd('ifconfig s3SD 172.10.15.1')
s1Matriz.cmd('ifconfig s1Matriz 172.10.13.1')
```

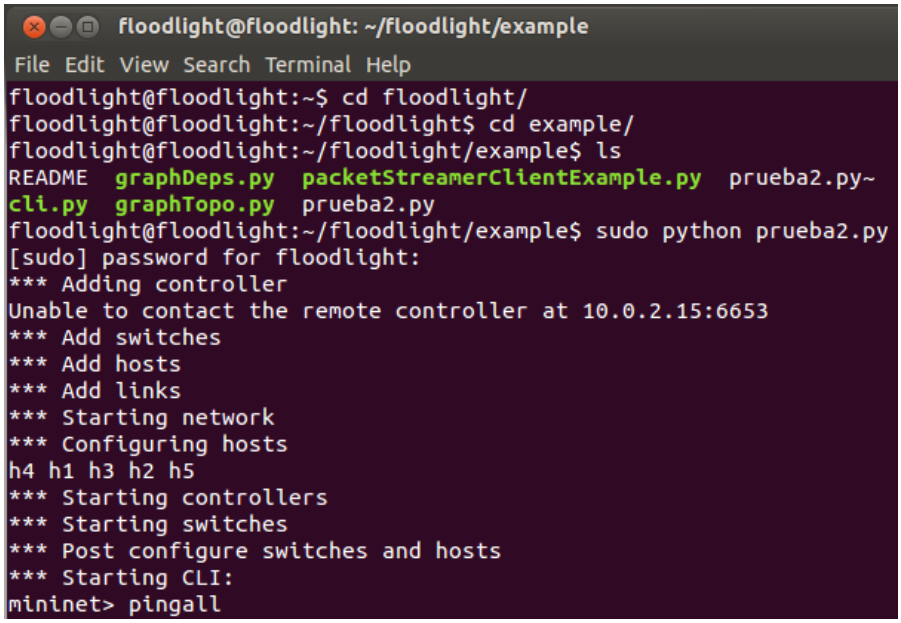
```
s2LT.cmd('ifconfig s2LT 172.10.14.1')


CLI(net)
net.stop()


if __name__ == '__main__':
        setLogLevel( 'info' )
        myNetwork()
```

Una vez implementada la red mediante código de programación se guarda el archivo con extensión .py en el directorio /home/floodlight/floodlight/example.

La inicialización de la simulación y construcción de la red se realiza abriendo un terminal y se ejecutan los comandos que se observan en la siguiente Figura.

Figura 19

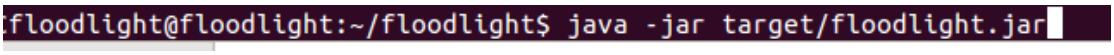
Inicialización de la simulación y construcción de la red



A continuación, se inicializa el controlador Floodlight con el comando: java -jar target/floodlight.jar

Figura 20

Inicialización del controlador Floodlight



Seguridad en la red SDN

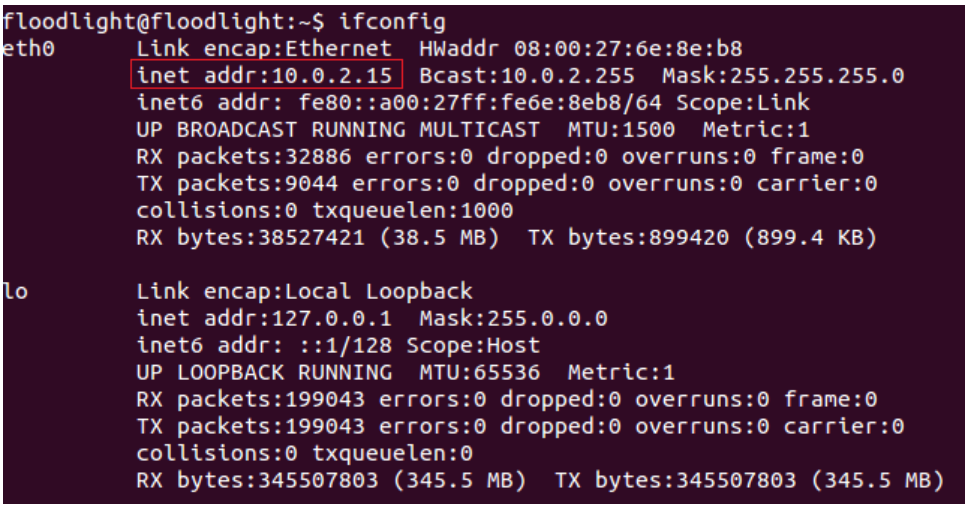
Existen varias formas de implementar seguridad en una red SDN, sin embargo, en este proyecto vamos a utilizar listas de acceso (ACL) y el firewall que viene embebido en el controlador SDN Floodlight.

Para empezar, vamos a implementar listas de acceso que nos permitan restringir la conectividad entre sedes de acuerdo a nuestras necesidades, a continuación, vamos a restringir la conectividad entre la sede de Salinas (h4) y la sede de Shell (h5)

Primero debemos identificar la ip con la que está configurado el controlador, mediante el comando ifconfig.

Figura 21

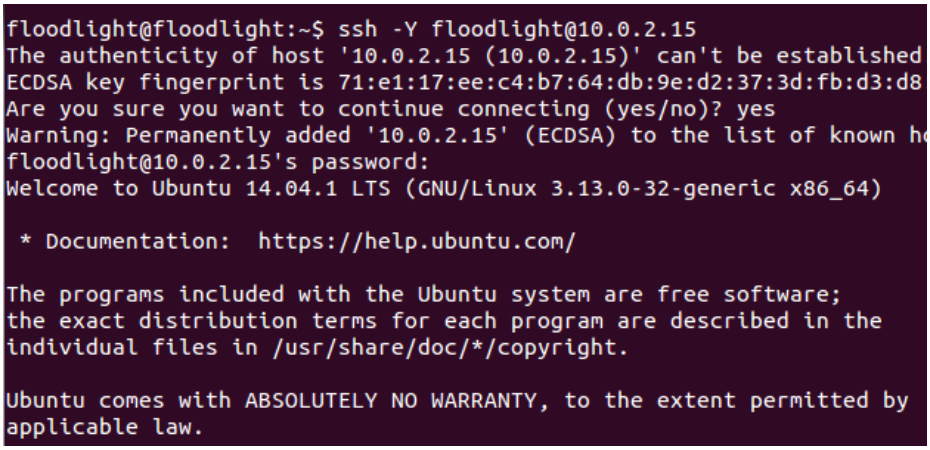
Verificación de ip del controlador



A continuación, verificamos la conexión con el controlador mediante el comando ssh -Y floodlight@10.0.2.15 como se muestra a continuación:

Figura 22

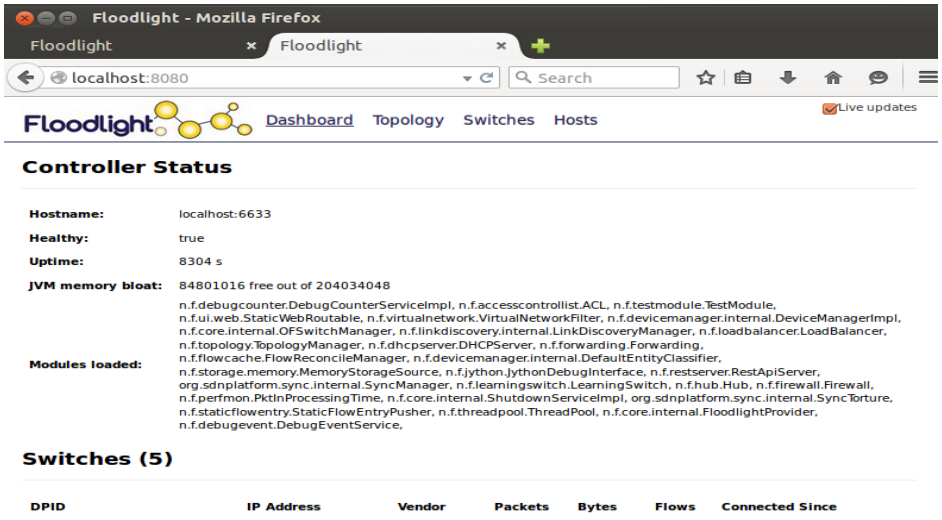
Conexión al servidor vía ssh



Una vez realizado esto, también es posible verificar la conexión con el controlador mediante web donde también podremos apreciar la topología, número de switch y número de hosts, para establecer conexión con el controlador mediante web abrimos un navegador y colocamos la siguiente URL: http://10.0.2.15:8080/ui/index.html

Figura 23

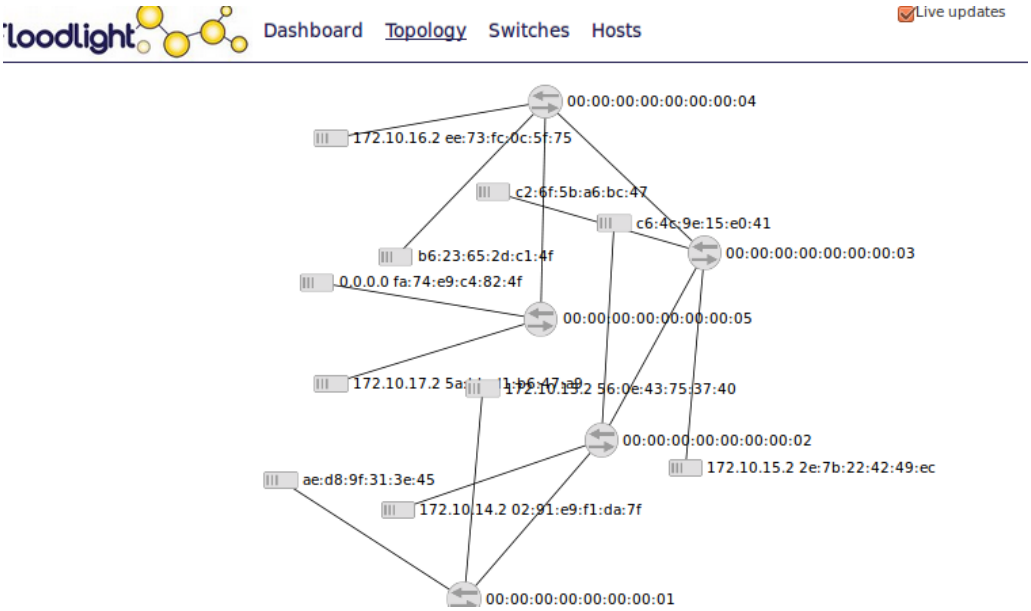
Conexión al controlador vía web



En la siguiente figura se despliega la topología de la red que se ejecuta en mininet, como se puede apreciar no es una topología clara por lo que se recomienda solo utilizarla como referencia.

Figura 24

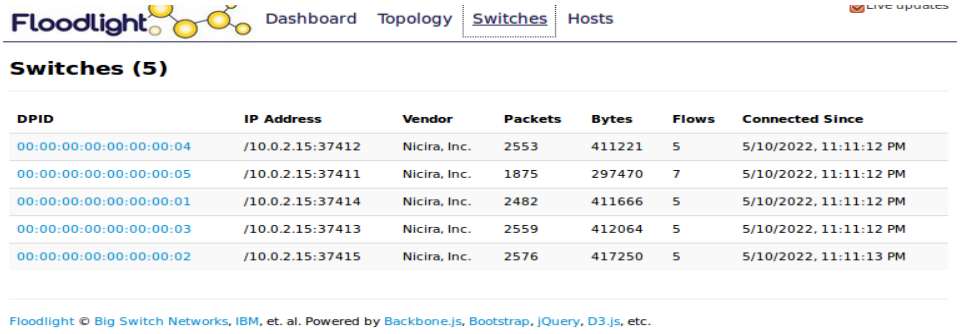
Topología de la red vía web



A continuación, en la pestaña switches podemos apreciar los 5 equipos de nuestro proyecto.

Figura 25

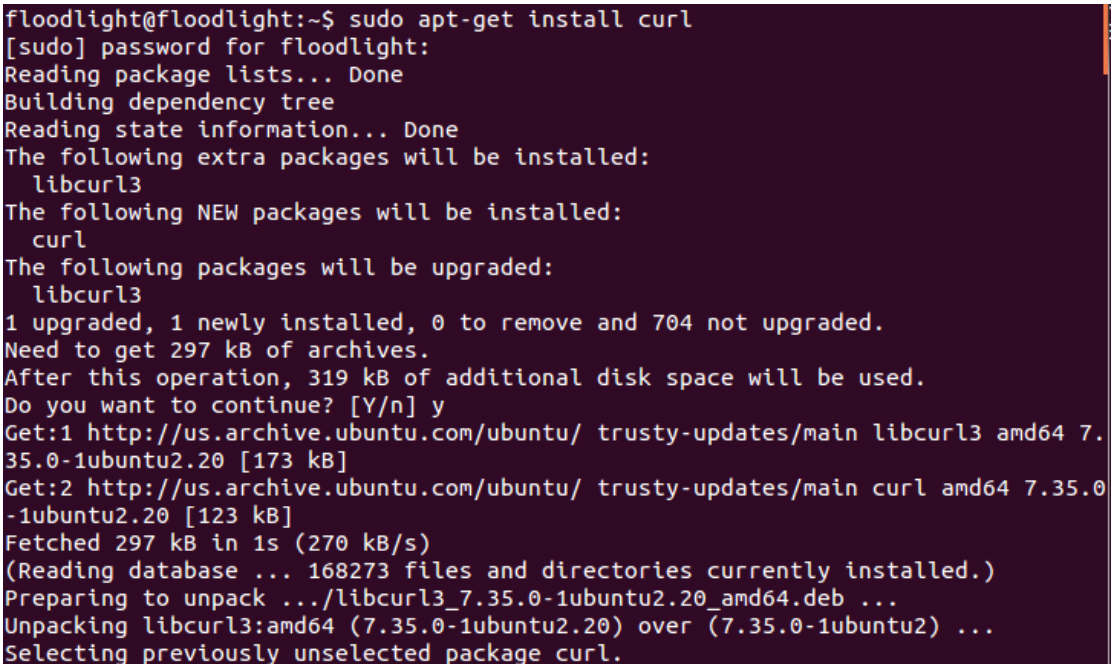
Estado de los switches vía web



Una vez que se estableció conexión con el controlador, se procede a instalar el código del complemento curl, la cual es una herramienta de línea de comandos para obtener o enviar datos utilizando la sintaxis de URL y se lo ejecuta de la siguiente manera:

Figura 26

Instalación herramienta curl



Esta funcionalidad de ACLs viene embebida en el controlador y a través de líneas de comandos podemos denegar o permitir la conexión entre ciertos host de una red dependiendo las necesidades que se presenten en un determinado escenario.

Otra forma de implementar seguridad en una red SDN es ejecutando el firewall propio del controlador SDN, para empezar, se debe habilitar el firewall ejecutando el siguiente comando: curl http://10.0.2.15:8080/wm/firewall/module/enable/json -X PUT -d ''

Capítulo IV

Análisis técnico

Pruebas

Una vez configurada e implementada de forma simulada la red SDN en el backbone de la ESPE, se llevaron a cabo pruebas de conectividad y pruebas de desempeño. Las primeras apuntaron a la evaluación de la configuración y seguridad de las redes entre todas las sedes y la casa matriz respecto de las sedes de la institución; las pruebas de desempeño buscaron evaluar la latencia, la pérdida de paquetes y la tasa de transferencia efectiva (throughput).

Pruebas de configuración

Una vez configurados los equipos de la red SDN simulada, fue preciso realizar pruebas de conectividad para verificar el funcionamiento y la seguridad de la red. Para esto, se evaluó la conectividad entre las sedes de la casa de estudios con el comando pingall entre la matriz y las distintas sedes. Esto se aprecia desde la Figura 27 a la Figura 31.

Figura 27

Prueba de conexión entre todas las sedes de la ESPE

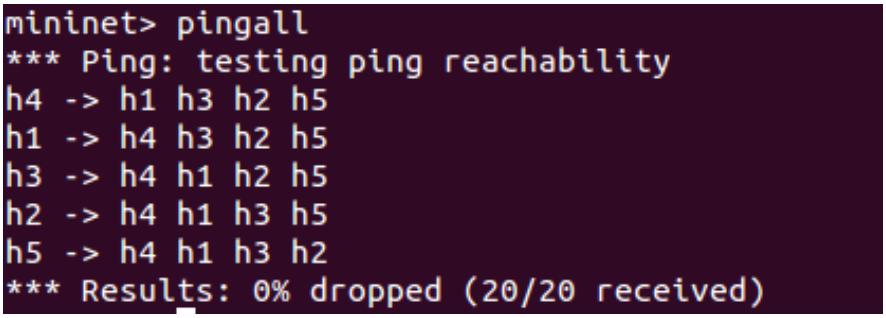


Figura 28

Prueba de conexión entre Matriz - Latacunga

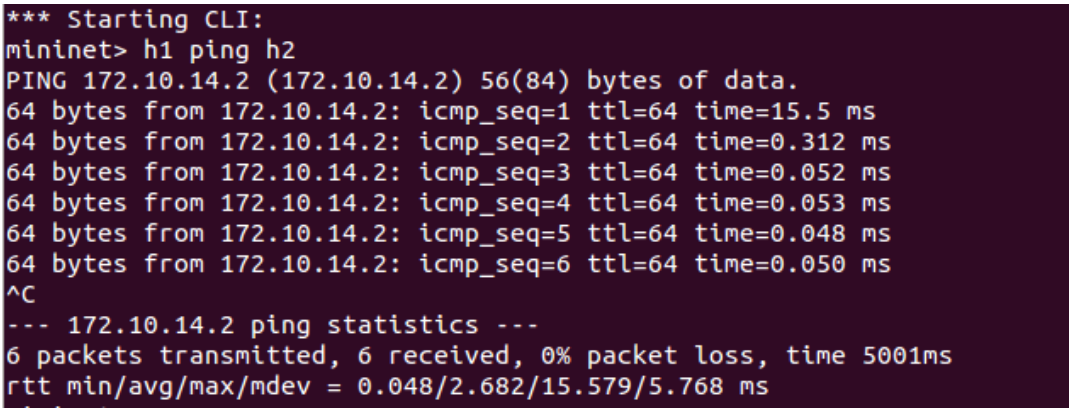


Figura 29

Prueba de conexión entre Matriz – Santo Domingo

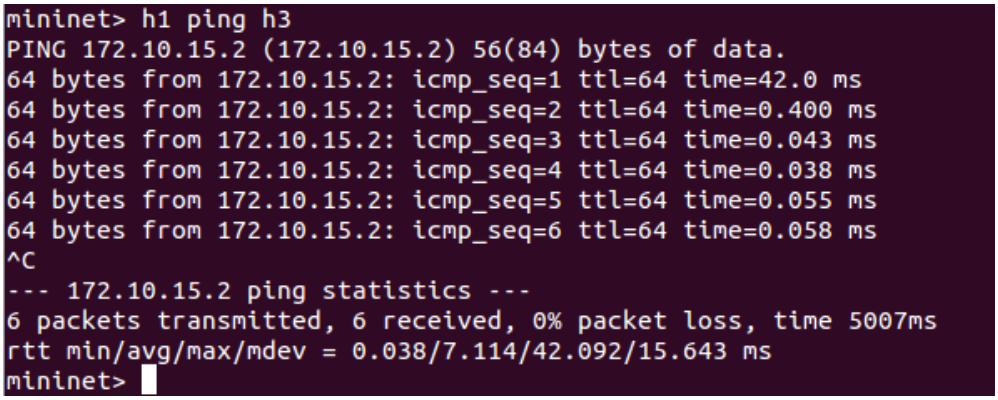


Figura 30

Prueba de conexión entre Matriz - Salinas

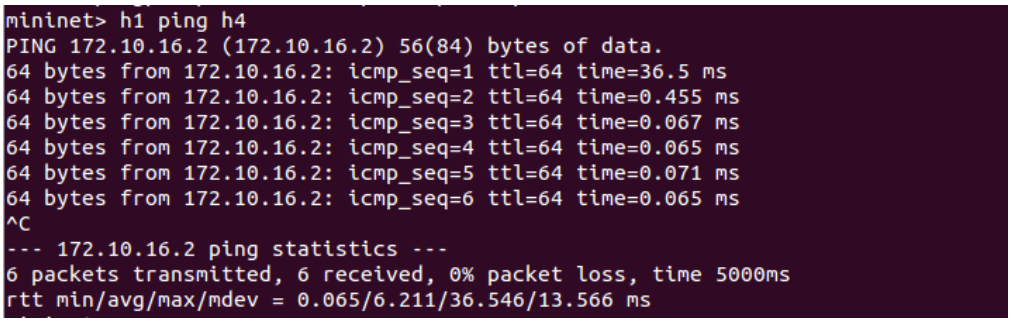


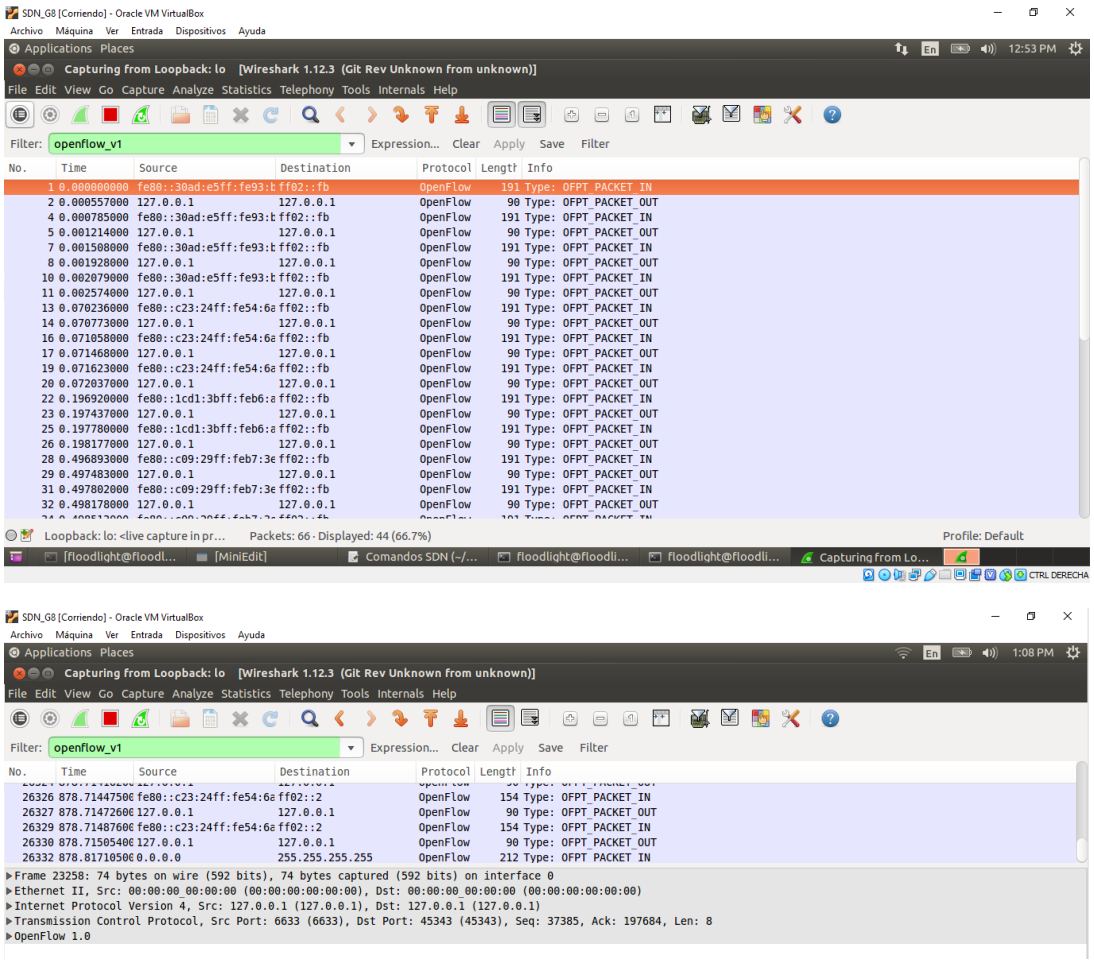
Figura 31

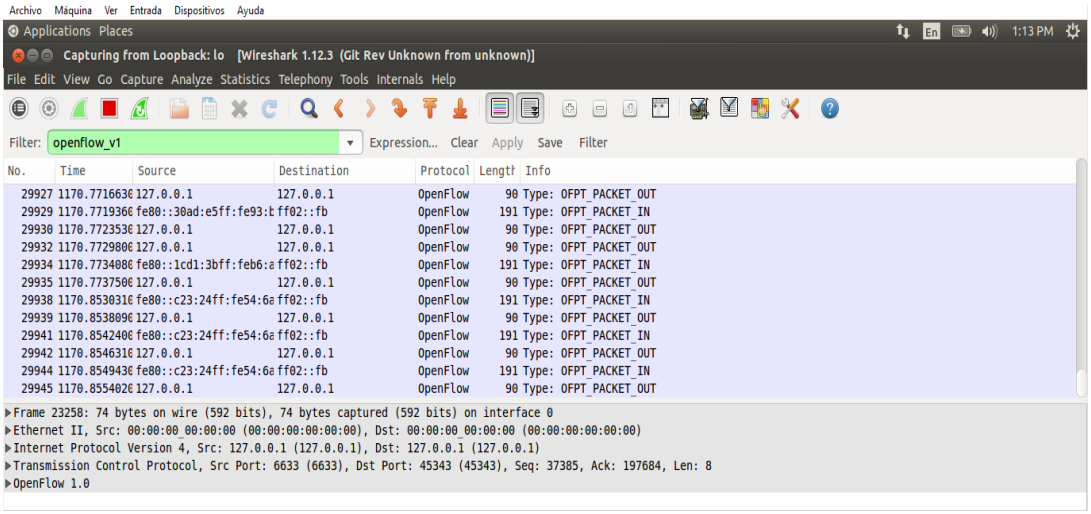
Prueba de conexión entre Matriz - Shell

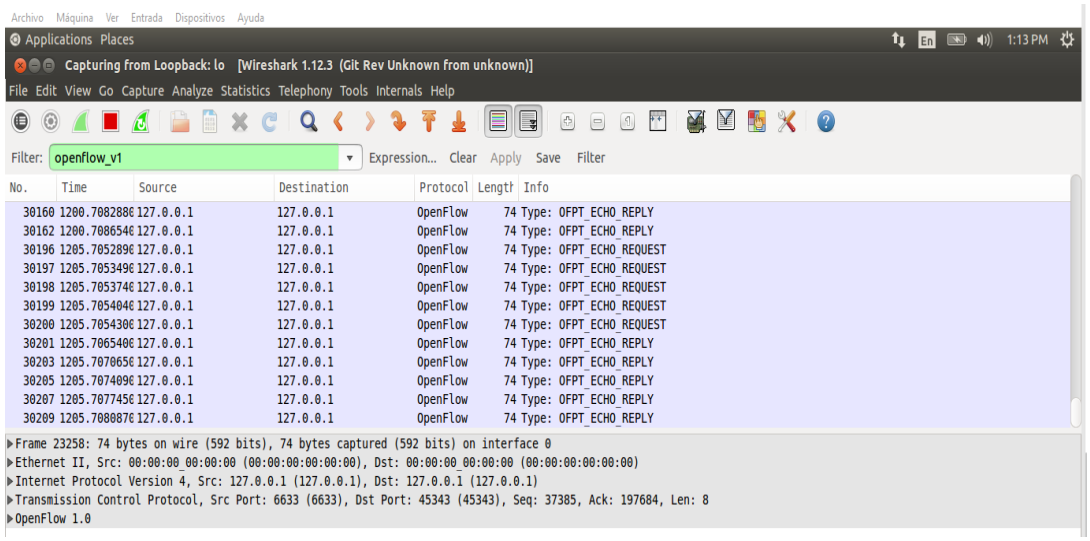
```
mininet> h1 ping h5
PING 172.10.17.2 (172.10.17.2) 56(84) bytes of data.
64 bytes from 172.10.17.2: icmp_seq=1 ttl=64 time=37.7 ms
64 bytes from 172.10.17.2: icmp_seq=2 ttl=64 time=0.547 ms
64 bytes from 172.10.17.2: icmp_seq=3 ttl=64 time=0.071 ms
64 bytes from 172.10.17.2: icmp_seq=4 ttl=64 time=0.054 ms
64 bytes from 172.10.17.2: icmp_seq=5 ttl=64 time=0.071 ms
64 bytes from 172.10.17.2: icmp_seq=6 ttl=64 time=0.056 ms
^C
--- 172.10.17.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5000ms
rtt min/avg/max/mdev = 0.054/6.420/37.722/13.999 ms
```

Figura 32

Filtro de ejecución Wireshark con conexión ssh.







Pruebas de desempeño

A continuación, se presentan los resultados de las pruebas de desempeño realizadas, las cuales consistieron en la evaluación de la latencia, la pérdida de paquetes y la transferencia efectiva.

Latencia. Para evaluar la latencia, se utilizó la información arrojada por el comando ping.

Tabla 7

Medición de latencia con el comando ping

Nodos	Mínimo	Promedio	Máximo	Desviación estándar
Matriz - Latacunga	0.048	2.682	15.579	5.768
Matriz – Santo Domingo	0.038	7.114	42.092	15.643
Matriz - Salinas	0.0695	6.211	36.546	13.566
Matriz - Shell	0.054	6.420	37.722	13.999

Pérdida de paquetes. A partir del uso del mismo comando ping se analizó la información respecto a la pérdida de paquetes

Tabla 8

Medición de pérdida de paquetes con el comando ping

Nodos	Cantidad de paquetes enviados	Cantidad de paquetes recibidos	% Pérdida de paquetes
Matriz - Latacunga	6	6	0
Matriz - Santo Domingo	6	6	0
Matriz - Salinas	6	6	0
Matriz - Shell	6	6	0

Throughput. El análisis de la tasa de transferencia tiene como objetivo evaluar el volumen de la información que es transferida por la red SDN simulada.

Figura 33

Matriz (h1) con los demás nodos

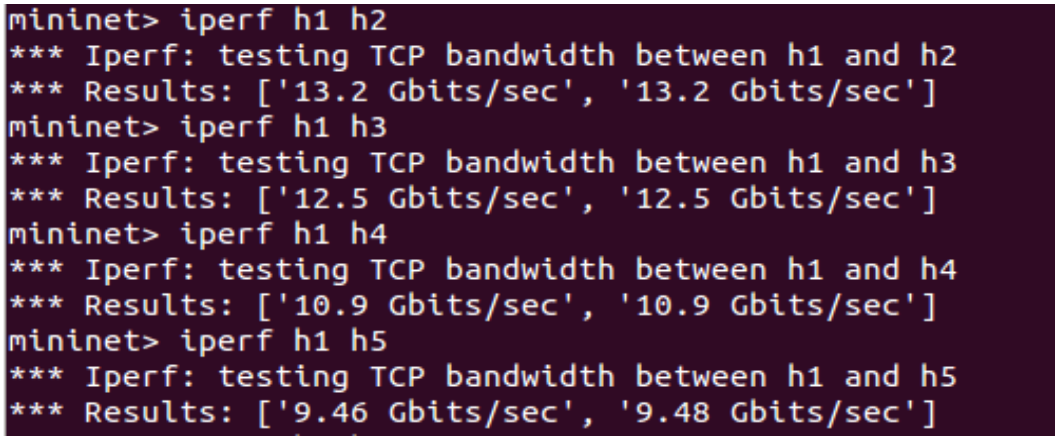


Figura 34

Latacunga (h2) con los demás nodos

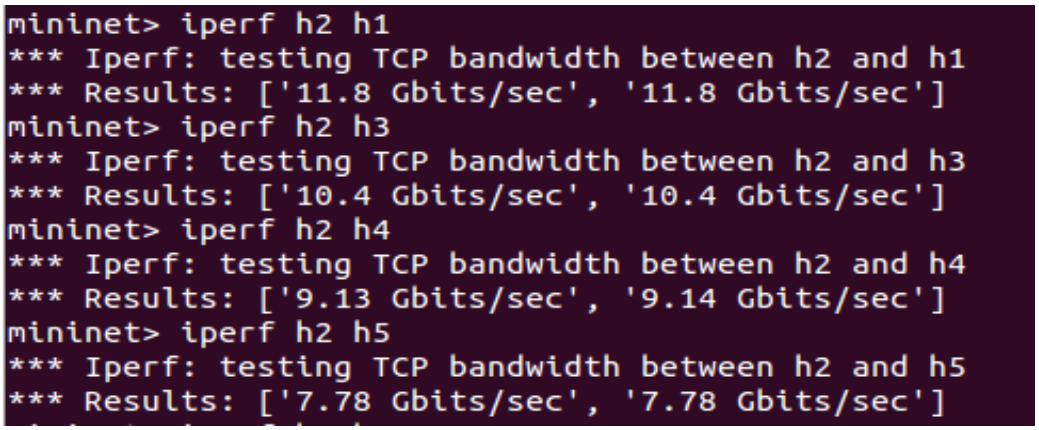


Figura 35

Santo Domingo (h3) con los demás nodos

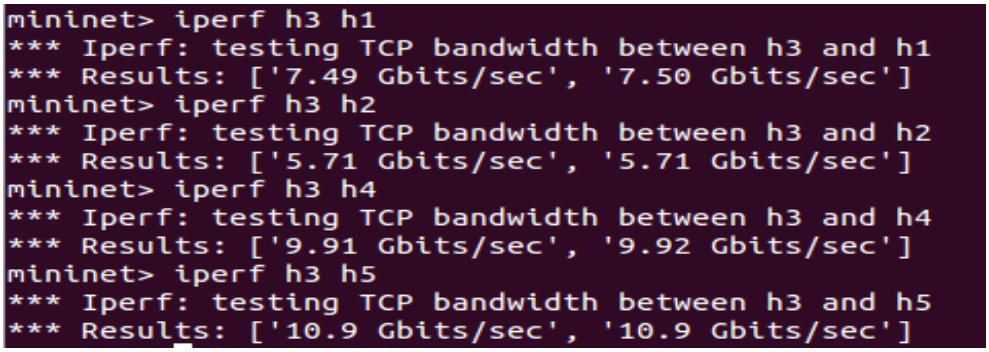


Figura 36

Salinas (h4) con los demás nodos

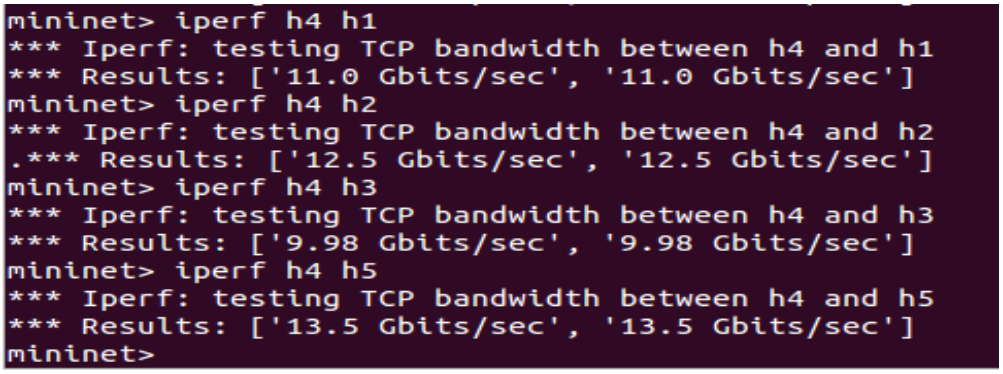
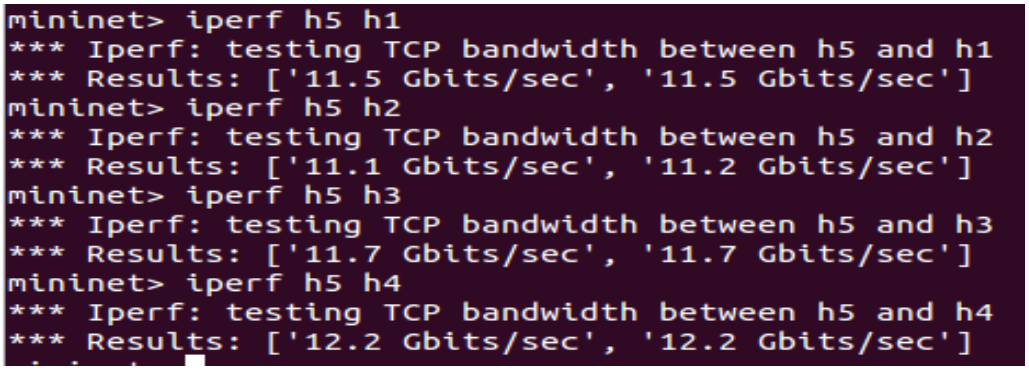


Figura 37

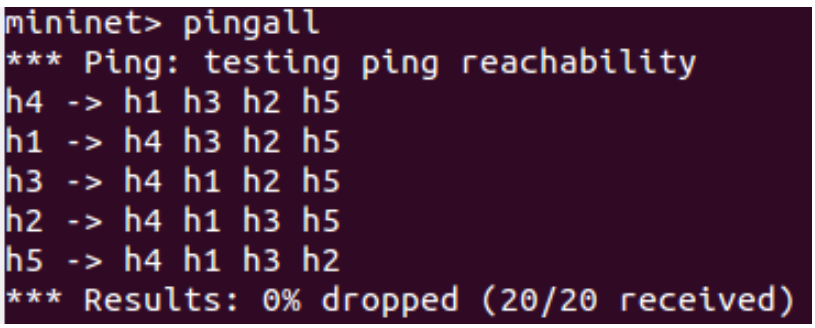
Shell (h5) con los demás nodos



Listas de Acceso (ACL). Se procede a realiza pruebas de conectividad entre todas las sedes antes de implementar las ACLs, en la Figura 39 se verifica conectividad exitosa entre sedes.

Figura 38

Prueba de conectividad antes de implementar ACLs



A continuación, se va a generar 2 ACL que impidan la comunicación entre distintas sedes, ACL #1 restringe la comunicación entre la Sede Salinas (h4) con la Sede Shell (h5), y la ACL #2 restringe la comunicación entre la Sede Latacunga (h1) con la Sede Shell (h5)

Para ejecutar la ACL #1, se ejecuta la siguiente línea de código que se muestra en la Figura 39, en donde interviene la ip origen (172.10.17.2/32), ip destino (172.10.16.2/32), la acción que se va a realizar en nuestro caso es denegar (DENY) el acceso.

Figura 39

ACL #1

```
floodlight@floodlight:~$ curl http://localhost:8080/wm/acl/rules/json | python -mjson.to
ol
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   399    0   399    0     0  12030      0 --:--:-- --:--:-- --:--:-- 12468
[
    {
        "action": "DENY",
        "id": 1,
        "nw_dst": "172.10.16.2/32",
        "nw_dst_maskbits": 32,
        "nw_dst_prefix": -1408626686,
        "nw_proto": 0,
        "nw_src": "172.10.17.2/32",
        "nw_src_maskbits": 32,
        "nw_src_prefix": -1408626430,
        "tp_dst": 0
    },
```

Para ejecutar la ACL #2, se ejecuta la siguiente línea de código que se muestra en la Figura 40, en donde interviene la ip origen (172.10.17.2/32), ip destino (172.10.13.2/32), la acción que se va a realizar en nuestro caso es denegar (DENY).

Figura 40

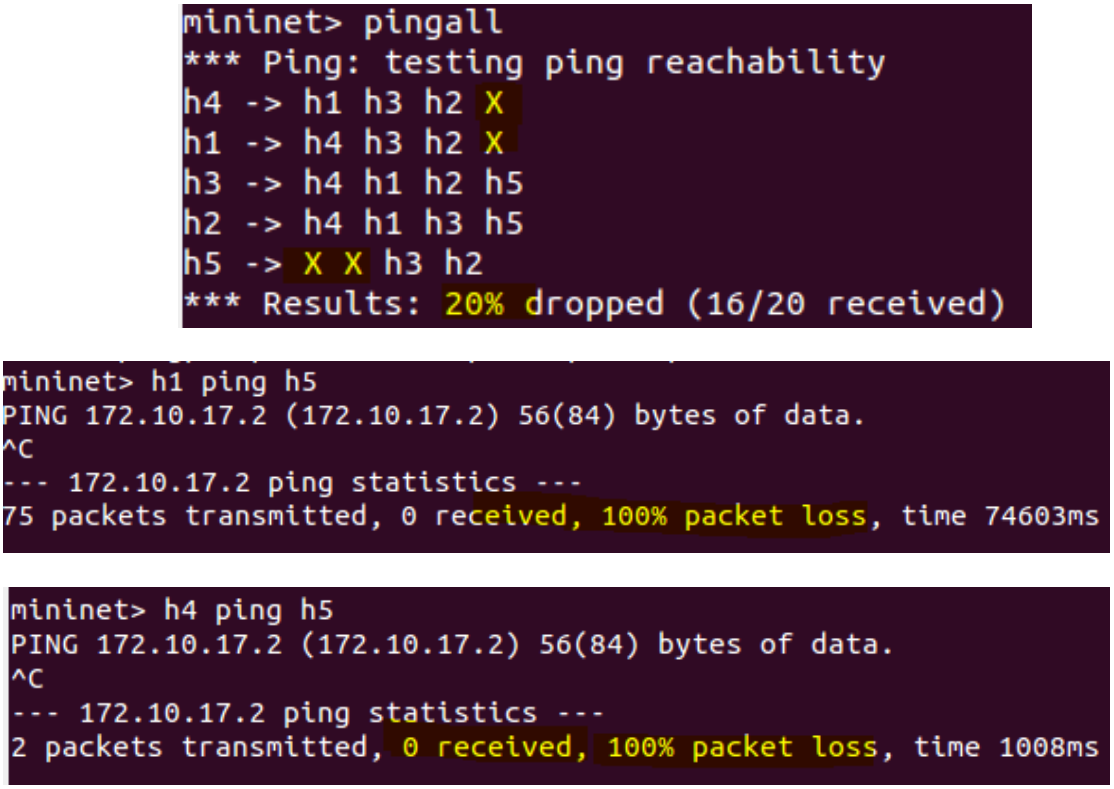
ACL #2

```
{
    "action": "DENY",
    "id": 2,
    "nw_dst": "172.10.13.2/32",
    "nw_dst_maskbits": 32,
    "nw_dst_prefix": -1408627454,
    "nw_proto": 0,
    "nw_src": "172.10.17.2/32",
    "nw_src_maskbits": 32,
    "nw_src_prefix": -1408626430,
    "tp_dst": 0
}
```

Una vez que se ejecutan las ACLs, nuevamente se realizan pruebas de conectividad entre sedes para verificar los resultados.

Figura 41

Pruebas de conectividad una vez ejecutadas las ACLs.

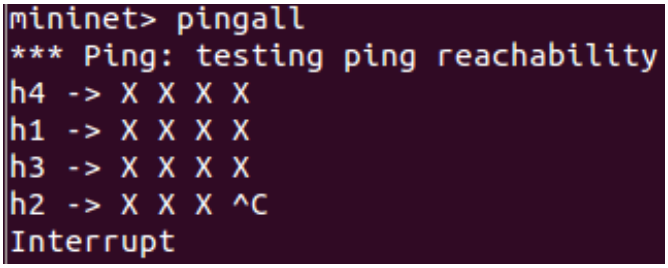


En la Figura 41 se puede visualizar que no se tienen conectividad entre h4-h5 y h1-h5, las listas de acceso funcionan de manera correcta. Elaboración propia.

Reglas de Firewall. Una vez que se habilita el firewall por defecto se deniega todo el tráfico de la red, únicamente permitirá el paso del tráfico que se haya permitido con reglas de firewall, por lo que al realizar pruebas de conectividad no se tiene comunicación entre ninguna sede como se muestra en la Figura 42.

Figura 42

Pruebas de conectividad con el firewall por defecto habilitado

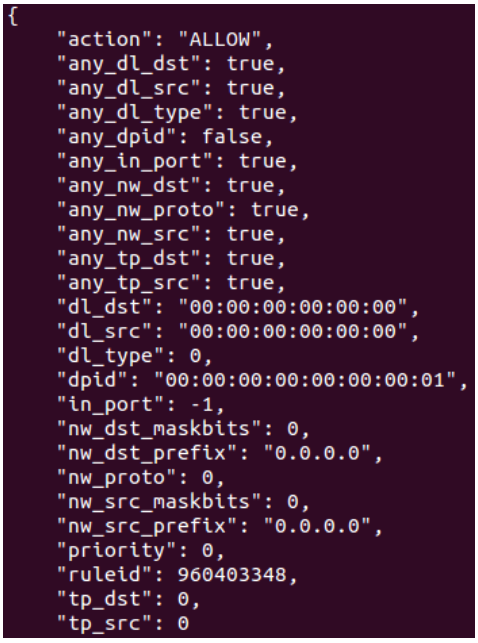


Para permitir la comunicación entre sedes se deben definir reglas para definir a través de que switch queremos que se permita el paso de tráfico, con esto se puede permitir o denegar la comunicación de toda una sede, por lo que vamos a ejecutar los siguientes códigos de comandos por cada switch que se tenga en la red de la siguiente manera:

Para el SW Matriz. curl -X POST -d '{"switchid": "00:00:00:00:00:00:00:01"}' http://10.0.2.10:8080/wm/firewall/rules/json

Figura 43

Regla de Firewall Sw Matriz

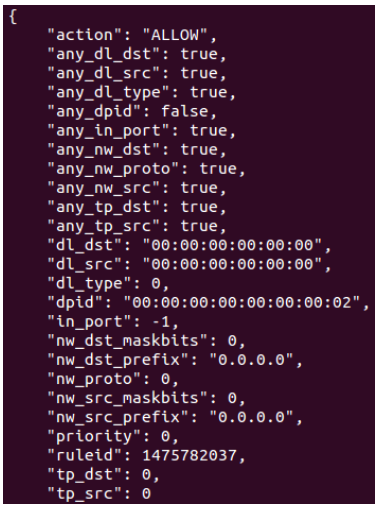


Para el SW Latacunga. curl -X POST -d '{"switchid": "00:00:00:00:00:00:00:02"}'

http://10.0.2.10:8080/wm/firewall/rules/json

Figura 44

Regla de Firewall Sw Latacunga



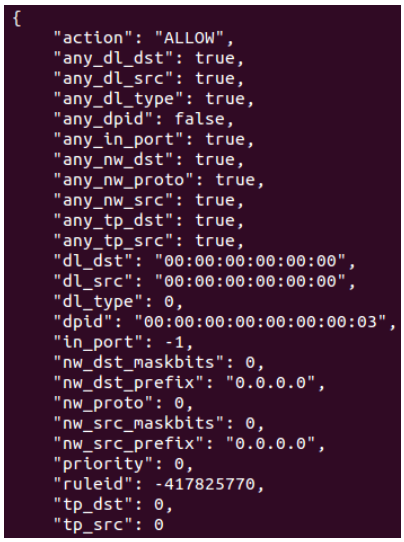
```
{
    "action": "ALLOW",
    "any_dl_dst": true,
    "any_dl_src": true,
    "any_dl_type": true,
    "any_dpid": false,
    "any_in_port": true,
    "any_nw_dst": true,
    "any_nw_proto": true,
    "any_nw_src": true,
    "any_tp_dst": true,
    "any_tp_src": true,
    "dl_dst": "00:00:00:00:00:00",
    "dl_src": "00:00:00:00:00:00",
    "dl_type": 0,
    "dpid": "00:00:00:00:00:00:00:02",
    "in_port": -1,
    "nw_dst_maskbits": 0,
    "nw_dst_prefix": "0.0.0.0",
    "nw_proto": 0,
    "nw_src_maskbits": 0,
    "nw_src_prefix": "0.0.0.0",
    "priority": 0,
    "ruleid": 1475782037,
    "tp_dst": 0,
    "tp_src": 0
```


Para el SW Santo Domingo. curl -X POST -d '{"switchid": "00:00:00:00:00:00:00:03"}'

http://10.0.2.10:8080/wm/firewall/rules/json

Figura 45

Regla de Firewall Sw Santo Domingo



```
{
    "action": "ALLOW",
    "any_dl_dst": true,
    "any_dl_src": true,
    "any_dl_type": true,
    "any_dpid": false,
    "any_in_port": true,
    "any_nw_dst": true,
    "any_nw_proto": true,
    "any_nw_src": true,
    "any_tp_dst": true,
    "any_tp_src": true,
    "dl_dst": "00:00:00:00:00:00",
    "dl_src": "00:00:00:00:00:00",
    "dl_type": 0,
    "dpid": "00:00:00:00:00:00:00:03",
    "in_port": -1,
    "nw_dst_maskbits": 0,
    "nw_dst_prefix": "0.0.0.0",
    "nw_proto": 0,
    "nw_src_maskbits": 0,
    "nw_src_prefix": "0.0.0.0",
    "priority": 0,
    "ruleid": -417825770,
    "tp_dst": 0,
    "tp_src": 0
```

Para el SW Salinas. curl -X POST -d '{"switchid": "00:00:00:00:00:00:00:04"}' http://10.0.2.10:8080/wm/firewall/rules/json

Figura 46

Regla de Firewall Sw Salinas


```
{
    "action": "ALLOW",
    "any_dl_dst": true,
    "any_dl_src": true,
    "any_dl_type": true,
    "any_dpid": false,
    "any_in_port": true,
    "any_nw_dst": true,
    "any_nw_proto": true,
    "any_nw_src": true,
    "any_tp_dst": true,
    "any_tp_src": true,
    "dl_dst": "00:00:00:00:00:00",
    "dl_src": "00:00:00:00:00:00",
    "dl_type": 0,
    "dpid": "00:00:00:00:00:00:00:04",
    "in_port": -1,
    "nw_dst_maskbits": 0,
    "nw_dst_prefix": "0.0.0.0",
    "nw_proto": 0,
    "nw_src_maskbits": 0,
    "nw_src_prefix": "0.0.0.0",
    "priority": 0,
    "ruleid": 1040543319,
    "tp_dst": 0,
    "tp_src": 0
```


Para el SW Shell. curl -X POST -d '{"switchid": "00:00:00:00:00:00:00:05"}' http://10.0.2.10:8080/wm/firewall/rules/json

Figura 47

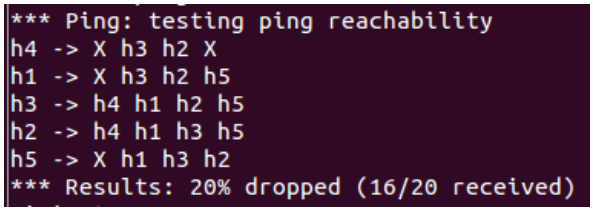
Regla de Firewall Sw Shell


```
floodlight@floodlight:~$ curl http://10.0.2.15:8080/wm/firewall/rules/json | python -mjs
on.tool
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2389    0  2389    0     0   174k      0 --:--:-- --:--:-- --:--:--  194k
[
    {
        "action": "ALLOW",
        "any_dl_dst": true,
        "any_dl_src": true,
        "any_dl_type": true,
        "any_dpid": false,
        "any_in_port": true,
        "any_nw_dst": true,
        "any_nw_proto": true,
        "any_nw_src": true,
        "any_tp_dst": true,
        "any_tp_src": true,
        "dl_dst": "00:00:00:00:00:00",
        "dl_src": "00:00:00:00:00:00",
        "dl_type": 0,
        "dpid": "00:00:00:00:00:00:00:05",
        "in_port": -1,
        "nw_dst_maskbits": 0,
        "nw_dst_prefix": "0.0.0.0",
        "nw_proto": 0,
```

Aplicando las reglas de firewall para el paso del tráfico nuevamente se tiene conectividad entre todas las sedes, excepto las que no tenían conectividad por las reglas de ACls generadas anteriormente

Figura 48

Pruebas de conectividad con las reglas de firewall



Análisis cualitativo

Las instituciones educativas, por el gran número de servicios que brindan y la cantidad de usuarios a los que atienden, son actividades complejas que requieren una gestión eficiente que garantice la calidad y la excelencia.

En la Universidad de las Fuerzas Armadas hay mucha información del personal y los estudiantes, contenidos de aprendizaje e investigación, número de procesos administrativos y académicos, convirtiéndolos en usuarios y dependientes de grandes centros de datos, centros de datos avanzados y conexiones y redes de alta velocidad, necesarias para poder mantener el alto nivel de servicio requerido por su comunidad.

Esto ha generado la necesidad de que las instituciones educativas deban crear y administrar redes de datos seguros, confiables y de alta velocidad para respaldar las operaciones de la universidad y todos sus servicios. Sumado a esta situación, el constante incremento en la cantidad y calidad de los servicios que brinda la universidad, ha derivado en el crecimiento y enorme complejidad de las redes de datos universitarios, haciendo que la universidad sea muy difícil de desarrollar y sin duda de operar y administrar.

Algunas cuestiones centrales para evaluar sobre las características y funcionamiento de las redes son la lentitud en la provisión de servicios o clientes nuevos, su complejidad, los

retardos en la provisión de servicios nuevos, la integración pronta de tecnologías nuevas, su conectividad, sus costos operativos y de equipamiento y la seguridad de las redes y sus vulnerabilidades.

Ventajas de la implementación

- El sistema hace posible el control y la administración dinámica de la red.
- Es posible programar mediante códigos la infraestructura de la red.
- Habilitación de la programación de la red bajo demanda.
- Alta velocidad en provisión de clientes y servicios nuevos.
- Baja inversión inicial.
- Bajos costos de operación.
- Despliegue y control de la red simplificados.
- Mayor seguridad y menores vulnerabilidades en la red.
- Alta usabilidad.

Capítulo V

Análisis económico

Análisis preliminar de los componentes

Dentro de los componentes para el trabajo, se ha considerado que la simulación requiere de las siguientes herramientas de desarrollo:

- Máquina física para simulación 8GB RAM, procesador de 2 GHz.
- Máquina virtual Linux (Ubuntu, Red Hat u otra distribución)
- Controlador SDN seleccionado.
- Emulador Mininet (simulación mediante Miniedit / Phyton / línea de comandos).

La topología de la red simulada cuenta con dos capas, el plano de datos (conmutación); la capa de control, en donde se ubica el controlador SDN y API. Esta se compone de 5 switchs (sede matriz y cuatro sedes).

Los equipos considerados para la implementación y que corresponden a la inversión inicial son:

- Cisco SF350-24P 350 Series 2 4-Port PoE+Managed 10/100/1000 Mb/s Ethernet Switch

Figura 49

Switch Cisco SF350-24P serie 350

Nota: Tomado de Cisco. (12 de 12 de 2021). *Switch administrado de 24 puertos 10/100 POE Cisco SF350-24P*.: https://www.cisco.com/c/es_mx/support/switches/sf350-24p-24-port-10-100-poe-managed-switch/model.html

- WD My Cloud Expert Series 2 8TB EX2 Ultra 2-Bay NAS Ser ver (2x14TB)

Figura 50

Switch SF350-24P

Nota: Tomado de Western Digital. (12 de 12 de 2021). *My Cloud Expert Series EX2 Ultra*. www.westerndigital.com: https://www.westerndigital.com/es-es/products/network-attached-storage/wd-my-cloud-expert-series-ex2-ultra#WDBVBZ0000NCH

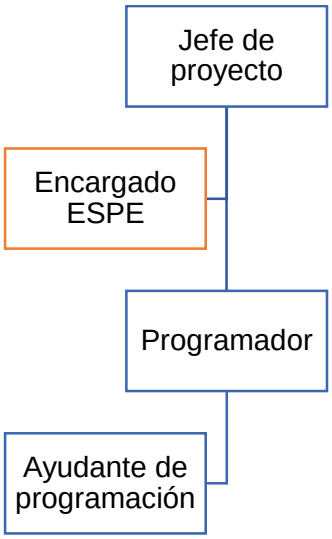
- Cableado
- Ordenadores

Definición de equipos de trabajo y personal a intervenir

El equipo de trabajo para el proyecto desarrollado consta con los siguientes roles:

Figura 51

Organigrama tentativo del equipo de trabajo



A continuación, se describen los cargos de cada uno de los integrantes del equipo de trabajo.

- **Jefe de proyecto:** Corresponde a un profesional del área de redes con experiencia en implementación y administración de redes institucionales. Tendrá como funciones el coordinar las actividades necesarias y el personal a cargo para implementar adecuadamente el proyecto en la institución, además de velar por la correcta ejecución presupuestaria. Los objetivos del cargo son llevar a cabo adecuadamente el proyecto de implementación de la red SDN en el backbone de las redes de la ESPE en función de la evaluación técnico económica desarrollada en este trabajo.
- **Programador:** Corresponde a un profesional del área de las redes que se encuentre capacitado en el uso de redes SDN y en su implementación. Tendrá como funciones configurar los equipos e implementar las redes en el backbone de la ESPE según las indicaciones del jefe de proyecto. El objetivo del cargo es llevar a

cabo adecuadamente la implementación efectiva de la red SDN simulada en este trabajo mediante la adecuada configuración de equipos y software.

- **Ayudante de programador:** Corresponde a un profesional o técnico en el área de redes que se encuentre capacitado para ayudar al programador en la implementación de la red SDN simulada en este trabajo. Tendrá como funciones ayudar a configurar y programar todos los componentes necesarios para la adecuada implementación de la red, según las indicaciones que el programador y el jefe de proyecto indiquen. El objetivo del cargo es prestar ayuda en la configuración y pruebas de la red SDN a implementar.
- **Encargado ESPE:** Profesional administrativo o técnico de la institución educativa que monitorea el desarrollo del proyecto y permite coordinar las actividades requeridas por el equipo de trabajo. Este profesional es externo al proyecto, y consta solo como soporte para el trabajo del jefe de proyecto, de modo que no debe incluirse en costos.

Aplicación pruebas sustantivas

Se aplicaron pruebas sustantivas relacionadas según configuración y desempeño, así como los indicadores financieros que forma parte de la evaluación económica. En la prueba sustantiva de la evaluación económica se consideraron los siguientes aspectos:

- Presentar la inversión inicial.
- Calcular los costos.
- Calcular los precios para obtener los ingresos.
- Elaboración y presentación del flujo de caja para diez años.
- Calcular y presentar resultados de los indicadores financieros como VAN, TIR, C/B y ROI.

Resultados

Informe sobre la estructura de sistemas de información. El proyecto desarrollado constituye, según la evaluación técnica económica realizada, una mejora sustancial para el sistema de gestión de información de la Universidad de las Fuerzas Armadas. La red SDN simulada se realizó en Mininet (Linux); se utilizaron herramientas como Eclipse IDE, Floodlight v1.0, y se basó en una arquitectura por capas, en la que constan las capas de infraestructura y administración.

En los principales resultados de evaluación técnica se encuentran las pruebas de configuración y de desempeño realizadas. Respecto a las pruebas de configuración, se evaluó la conectividad entre las sedes y la sede matriz y entre estas. Estas se realizaron con el comando pingall y ping, dando como resultado la conexión efectiva. Por otra parte, las pruebas de desempeño presentaron también resultados positivos; la latencia que se presenta (evaluada con el comando ping) tiene un promedio entre 2.682 y 7.114; la pérdida de paquetes es del 0 % en todos los casos; y la tasa de transferencia presenta valores positivos entre 5.71 Gbits/sec y 13.5 Gbits/sec.

Adicional para analizar el tema de la seguridad, se implementaron listas de acceso (ACLs) y reglas de firewall para permitir o denegar la comunicación entre determinados dispositivos o toda una sede.

Activos (equipos y materiales). Para la implementación de la red SDN en el backbone de la Sede Matriz de la Universidad de las Fuerzas Armadas se requiere una inversión en materiales y equipos de USD 6.959,82. Lo cual se aprecia en la Tabla 9:

Tabla 9

Inversión inicial red SDN

Descripción	Precio Unitario	Cantidad	Total
Cisco SF350-24P 350 Series 2 4-Port PoE+Managed 10/100 Mb/s Ethernet Switch	489,28	5	2.446,40
WD My Cloud Expert Series 2 8TB EX2 Ultra 2-Bay NAS Ser ver (2x14TB)	1.688,70	1	1.688,70
Cableado	324,72	1	324,72
Ordenadores	500,00	5	2.500,00
Total			**6.959,82**

Costos. De igual modo, se consideraron los costos relacionados con la mano de obra, servicio de Internet, capacitación, mantenimiento y depreciación de equipos. A continuación, se detalla los costos para el proyecto (Tabla 10 hasta Tabla 15):

Tabla 10

Costo mano de obra

Cargo	Cantidad	Sueldo Mensual	Sueldo Total	IESS Patronal 11,15%	Décimo Tercero	Décimo Cuarto	Valor mensual total	Valor Anual Total
Jefe de proyecto	1	1.260,00	1.260,00	140,49	105,00	35,42	1.540,91	18.490,88
Programador	1	980,00	980,00	109,27	81,67	35,42	1.206,35	14.476,24
Ayudante de programación	1	760,00	760,00	84,74	63,33	35,42	943,49	11.321,88
Total	**3**	**3.000,00**	**3.000,00**	**334,50**	**250,00**	**106,25**	**3.690,75**	**44.289,00**

Tabla 11

Costo servicio de Internet

Detalle	Unidad de medida	Cantidad	Costo Unitario	Valor total
Servicio de internet	unidad	12	8.400,00	100.800,00
Total				**100.800,00**

Tabla 12

Costo capacitación

Detalle	Unidad de medida	Cantidad	Costo Unitario	Valor total
Capacitación personal	unidad	1	1.500,00	**1.500,00**
Total				**1.500,00**

Tabla 13

Costo mantenimiento

Detalle	Unidad de medida	Costo	Porcentaje	Costo total
Mantenimiento de equipos	Unidad	6.635,10	15,071%	1.000,00
Total		**6.635,10**		**1.000,00**

Tabla 14

Costo depreciación

Activos Fijos	Costo	Vida útil	Año 1	Año 2	Año 3	Año 4	Año 5	Valor de salvamento
Cisco SF350-24P 350 Series 2 4-Port PoE+Managed 10/100 Mb/s Ethernet Switch	2.446,40	3	815,47	815,47	815,47			0,00
WD My Cloud Expert Series 2 8TB EX2 Ultra 2-Bay NAS Server (2x14TB)	1.688,70	3	562,90	562,90	562,90			0,00
Ordenadores	2.500,00	3	833,33	833,33	833,33			0,00
Total	**6.635,10**		**2.211,70**	**2.211,70**	**2.211,70**	**0,00**	**0,00**	**0,00**

Cabe mencionar que el costo de capacitación aplica únicamente para el primer año. Para la depreciación se consideró el método de línea recta, pues, se divide el costo y años de vida útil. En este caso, los equipos tecnológicos tienen tres años de vida. El costo total anual es de USD 150.842,18. El resumen del costo total se observa en la siguiente tabla.

Tabla 15

Costo Total

Detalle	Costo total
Mano de obra	44.289,00
Internet	100.800,00
Capacitación	1.500,00
Mantenimiento	1.000,00
Depreciación	2.211,70
Gastos financieros	1.041,48
Total	**150.842,18**

Además, se calculó la capacidad del proyecto para la puesta en marcha las actividades, considerando los costos y gastos, por lo que se utilizó el método de desfase mediante la siguiente fórmula:

$$\text{Capital de trabajo} = \frac{\text{Ca}}{365} * \text{n}_\text{d}$$

Donde:

Ca = Costo anual

nd = número días de desfase (30 días) o ciclo financiero para comenzar con las actividades

365 = Días del año

$$Capital\ de\ trabajo = \frac{150.842{,}18}{365} * 30$$

$$Capital\ de\ trabajo = 12.397{,}99$$

Para iniciar con el proyecto se requiere de USD 12.397,99, lo cual ayudará a cubrir los costos de la ejecución.

Inversión inicial. En la inversión total se suma los activos y el capital de trabajo, por ende, para el proyecto se necesita de USD 19.357,81.

Financiamiento. Para el desarrollo del proyecto del total de inversión se divide en un 43,18% (USD 8.357,81) con capital propio y el 56,82% (USD 11.000) mediante financiamiento. En este último caso se considera de un crédito bancario en BanEcuador debido a que se tiene tasas bajas en comparación que el resto de entidades, es decir, una tasa de interés anual de 10,21% (BanEcuador, 2021).

La amortización se aprecia en el apéndice 2 Las condiciones de crédito son: el monto del crédito es USD 11.000, tasa de interés anual del 10,21%, a 60 pagos mensuales (5 años). Con esto se obtiene una cuota mensual de USD 234,86. Las cuotas o pagos anuales se tienen en el apéndice 3 y el interés anual (gasto interés) están en el apéndice 4.

Proyección de costos fijos y variables. Para la proyección de los costos se utilizó la inflación anual de 0,60% del promedio obtenido del 2015 al 2020 (Instituto Nacional de Estadística y Censos, 2021).

Tabla 16

Proyección costos fijos y variables año 1 al año 5

Detalle	Año 1	Año 2	Año 3	Año 4	Año 5
COSTOS VARIABLES					
Costos directos	0,00	0,00	0,00	0,00	0,00
Subtotal	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
COSTOS FIJOS					
Mano de obra directa	44.289,00	44.552,52	44.817,61	45.084,27	45.352,52
Servicio de Internet	100.800,00	101.399,76	102.003,09	102.610,01	103.220,54
Capacitación	1.500,00				
Mantenimiento	1.000,00	1.005,95	1.011,93	1.017,95	1.024,01
Depreciación	2.211,70	2.224,86	2.238,10		
Gastos financieros	1.041,48	851,33	640,84	407,82	149,87
Subtotal	**150.842,18**	**150.034,42**	**150.711,57**	**149.120,05**	**149.746,93**
Total	**150.842,18**	**150.034,42**	**150.711,57**	**149.120,05**	**149.746,93**

Tabla 17

Proyección costos fijos y variables año 6 al año 10

Detalle	Año 6	Año 7	Año 8	Año 9	Año 10
COSTOS VARIABLES					
Costos directos	0,00	0,00	0,00	0,00	0,00
Subtotal	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**
COSTOS FIJOS					
Mano de obra directa	45.622,37	45.893,82	46.166,89	46.441,59	46.717,91
Servicio de Internet	103.834,70	104.452,52	105.074,01	105.699,20	106.328,11
Capacitación					
Mantenimiento	1.030,10	1.036,23	1.042,40	1.048,60	1.054,84
Depreciación					
Gastos financieros					
Subtotal	**150.487,17**	**151.382,57**	**152.283,30**	**153.189,38**	**154.100,86**
Total	**150.487,17**	**151.382,57**	**152.283,30**	**153.189,38**	**154.100,86**

Ingresos. Para obtener los ingresos es importante calcular el precio. Es así que se tomó en cuenta el costo individual derivado de la división entre el costo total y número de campus. Al costo individual se añadió un 2% de margen de utilidad. Para el precio se sumó el costo individual y margen de utilidad, siendo un valor de USD 30.771.80. Lo cual se aprecia en la Tabla 18.

Tabla 18

Precio

Costo total	No. campus	Costo individual (unidad)	Margen de utilidad		Precio por campus
150.842,18	5	30168,44	2,0%	603,37	30.771,80
150.842,18	**13,00**	**30.168,44**			**30.771,80**

Los ingresos se obtienen de la multiplicación entre precio por el número de campus, generando un beneficio al primer año de USD 153.859,02.

Flujo de caja. El flujo de caja se presenta en las Tablas 19 y 20 proyectada a 10 años. Para la proyección de ingresos se consideró el promedio del PIB del I y II trimestre del 2021, ubicándose en 1,50% (Banco Central del Ecuador, 2021). Mientras que para los costos se utilizó la inflación anual de 0,60% del promedio obtenido del 2015 al 2020 (Instituto Nacional de Estadística y Censos, 2021).

Tabla 19

Flujo de caja del año 0 al año 5

Detalle	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
INGRESOS						
Ingresos		153.859,02	156.166,90	158.509,41	160.887,05	163.300,35
(+) KTr (Valor total de capital de trabajo)						
Total Ingresos		**153.859,02**	**156.166,90**	**158.509,41**	**160.887,05**	**163.300,35**
Activos Fijos	6.959,82					
Capital de trabajo	12.397,99					
EGRESOS						
(-) Costo y gastos						
Costos de mano de obra		44.289,00	44.552,52	44.817,61	45.084,27	45.352,52
Servicio de internet		100.800,00	101.399,76	102.003,09	102.610,01	103.220,54
Capacitación		1.500,00	0,00	0,00	0,00	0,00
Mantenimiento		1.000,00	1.005,95	1.011,93	1.017,95	1.024,01
Depreciación		2.211,70	2.211,70	2.211,70		
Gastos financieros		1.041,48	851,33	640,84	407,82	149,87
Total Egresos		**150.842,18**	**150.021,26**	**150.685,17**	**149.120,05**	**149.746,93**

Detalle	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
(=) Utilidad antes de participación		**3.016,84**	**6.145,64**	**7.824,24**	**11.767,00**	**13.553,42**
(-) 15% participación utilidades		452,53	921,85	1.173,64	1.765,05	2.033,01
(=) Utilidad antes del impuesto		**2.564,32**	**5.223,80**	**6.650,60**	**10.001,95**	**11.520,41**
(-) 22% Impuesto a la Renta		564,15	1.149,24	1.463,13	2.200,43	2.534,49
Utilidad Neta del Ejercicio		**2.000,17**	**4.074,56**	**5.187,47**	**7.801,52**	**8.985,92**
Inversión	-19.357,81					
Depreciación		2.211,70	2.211,70	2.211,70		
Pago préstamo		1.776,79	1.966,93	2.177,43	2.410,45	2.668,40
Flujo de caja	**-19.357,81**	**2.435,08**	**4.319,33**	**5.221,74**	**5.391,07**	**6.317,51**

Nota: El flujo para el primer año es de USD 2.435,08.

Tabla 20

Flujo de caja del año 6 al año 10

Detalle	Año 6	Año 7	Año 8	Año 9	Año 10
INGRESOS					
Ingresos	165.749,86	168.236,11	170.759,65	173.321,04	175.920,86
(+) KTr (Valor total de capital de trabajo)					12.397,99
Total Ingresos	**165.749,86**	**168.236,11**	**170.759,65**	**173.321,04**	**188.318,85**
Activos Fijos					
Capital de trabajo					
EGRESOS					
(-) Costo y gastos					
Costos de mano de obra	45.622,37	45.893,82	46.166,89	46.441,59	46.717,91
Servicio de internet	103.834,70	104.452,52	105.074,01	105.699,20	106.328,11
Capacitación	0,00	0,00	0,00	0,00	0,00
Mantenimiento	1.030,10	1.036,23	1.042,40	1.048,60	1.054,84
Depreciación					
Gastos financieros					
Total Egresos	**150.487,17**	**151.382,57**	**152.283,30**	**153.189,38**	**154.100,86**

Detalle	Año 6	Año 7	Año 8	Año 9	Año 10
(=) Utilidad antes de participación	**15.262,69**	**16.853,54**	**18.476,35**	**20.131,66**	**34.217,99**
(-) 15% participación utilidades	2.289,40	2.528,03	2.771,45	3.019,75	5.132,70
(=) Utilidad antes del impuesto	**12.973,29**	**14.325,51**	**15.704,90**	**17.111,91**	**29.085,29**
(-) 22% Impuesto a la Renta	2.854,12	3.151,61	3.455,08	3.764,62	6.398,76
Utilidad Neta del Ejercicio	**10.119,16**	**11.173,90**	**12.249,82**	**13.347,29**	**22.686,53**
Inversión					
Depreciación					
Pago préstamo					
Flujo de caja	**10.119,16**	**11.173,90**	**12.249,82**	**13.347,29**	**22.686,53**

Nota: El flujo para el último año con USD 22.686,53.

Indicadores financieros. Se analizó el Valor Actual Neto (VAN), Tasa Interna de Retorno (TIR), Costo – Beneficio (C/B) y Rendimiento sobre la Inversión (ROI).

VAN. Previo a calcular el Valor Actual Neto se obtuvo la tasa de descuento (TMAR) de la sumatoria de la tasa pasiva, riesgo país e inflación.

Tabla 21

Tasa de descuento

Tasa de descuento (TMAR)	
Tasa pasiva	5,91%
Riesgo país	8,47%
Inflación	0,60%
TMAR	**14,98%**

Nota: Tomado de Banco Central del Ecuador. (30 de noviembre de 2021). *Información Estadística Mensual No. 2037 - Noviembre 2021*. https://contenido.bce.fin.ec/home1/estadisticas/bolmensual/IEMensual.jsp; Instituto Nacional de Estadística y Censos. (30 de noviembre de 2021). *Inflación (Índice de Precios al Consumidor)*. https://www.ecuadorencifras.gob.ec//indice-de-precios-al-consumidor/

Con la tasa de 14,98% se calcula los flujos actualizados, lo cual se tiene en la Tabla 22.

Tabla 22

VAN

Años	Flujo de caja	(1+i) n	Flujos actualizados
0	-19.357,81		
1	2.435,08	1,15	2.117,92
2	4.319,33	1,32	3.267,45
3	5.221,74	1,52	3.435,62
4	5.391,07	1,75	3.085,04
5	6.317,51	2,01	3.144,34
6	10.119,16	2,31	4.380,50
7	11.173,90	2,66	4.207,08
8	12.249,82	3,05	4.011,46
9	13.347,29	3,51	3.801,56
10	22.686,53	4,04	5.619,97
TOTAL, FLUJO			**37.070,95**

$$VAN = Flujos\ actualizados - Inversión$$

$$VAN = 37.070{,}95 - 19.357{,}81$$

$$VAN = 17.713{,}14$$

El VAN es de USD 17.713,14, el cual es positivo, esto significa que el proyecto de inversión es aceptable.

TIR. Para calcular el TIR se va tener como referencia el porcentaje del TMAR que es el 14.98%. En la Tabla 23 se presenta los resultados de la Tasa Interna de Retorno:

Tabla 23

TIR

AÑO	FNC	VAN CON Tm	VAN CON TM
		28%	**29%**
0	-19.357,81	-19.357,81	-19.357,81
1	2.435,08	1.902,40	1.887,66
2	4.319,33	2.636,31	2.595,59
3	5.221,74	2.489,92	2.432,46
4	5.391,07	2.008,33	1.946,78
5	6.317,51	1.838,64	1.768,47
6	10.119,16	2.300,83	2.195,87
7	11.173,90	1.984,88	1.879,65
8	12.249,82	1.700,00	1.597,39
9	13.347,29	1.447,12	1.349,23
10	22.686,53	1.921,62	1.777,75
Total		**872,26**	**73,05**
Tm	28%		
TM	29%		
VPN_m	872,26		
VPN_M	73,05		
TIR	**29,09%**		

$$\text{TIR} = 0{,}28 + (0{,}29 - 0{,}28)\frac{872{,}26}{872{,}26 - 73{,}05}$$

$$\text{TIR} = 29{,}09\%$$

Para aceptar la inversión el valor del TIR debe ser mayor al valor del TMAR, La TIR es de 29,09%, el cual es mayor al porcentaje del TMAR (14.98%), por ende, el proyecto de inversión es aceptable.

Costo/Beneficio. Para el costo – beneficio se consideró los ingresos y egresos (costos), actualizando los mismos con la tasa de descuento de 14,98%. Esto se observa en la Tabla 24

Tabla 24

Costo/Beneficio

Años	Ingresos	Ingresos Actualizados	Egresos	Egresos Actualizados
1	153.859,02	133.819,54	150.842,18	131.195,63
2	156.166,90	118.135,97	150.034,42	113.496,92
3	158.509,41	104.290,51	150.711,57	99.159,96
4	160.887,05	92.067,73	149.120,05	85.334,05
5	163.300,35	81.277,44	149.746,93	74.531,67
6	165.749,86	71.751,78	150.487,17	65.144,68
7	168.236,11	63.342,51	151.382,57	56.996,99
8	170.759,65	55.918,81	152.283,30	49.868,34
9	173.321,04	49.365,16	153.189,38	43.631,27
10	175.920,86	43.579,59	154.100,86	38.174,28
Total	**1.646.710,26**	**813.549,04**	**1.511.898,43**	**757.533,80**

$$C/B = \frac{Ingresos\ Actualizados}{Egresos\ Actualizados}$$

$$C/B = \frac{813.549{,}04}{757.533{,}80}$$

$$C/B = 1{,}07$$

Se obtuvo un C/B de 1,07; siendo mayor a 1, por ende, se deduce que por cada dólar invertido se obtiene una ganancia de 0,07 centavos.

ROI. En la Tabla 25 se presenta el ROI para diez años:

Tabla 25

ROI

Años	Ingresos	Inversión	ROI
1	153.859,02	-19.357,81	6,95
2	156.166,90	-19.357,81	7,07
3	158.509,41	-19.357,81	7,19
4	160.887,05	-19.357,81	7,31
5	163.300,35	-19.357,81	7,44
6	165.749,86	-19.357,81	7,56
7	168.236,11	-19.357,81	7,69
8	170.759,65	-19.357,81	7,82
9	173.321,04	-19.357,81	7,95
10	175.920,86	-19.357,81	8,09

$$ROI\ (primer\ año) = \frac{153.859{,}02 - 19.357{,}81)}{19.357{,}81} = 6{,}95$$

Para el primer año, el ROI es de 6,95, es así que se obtendrá un beneficio adecuado por la inversión realizada.

Respecto de la evaluación económica, se calcularon indicadores que permitieron determinar cómo es factible la implementación de la red SND en el backbone de la Universidad de las Fuerzas Armadas. Para esto, se calculó la inversión inicial, que asciende a USD 19.357,81. El análisis de costo/beneficio arrojó como resultado un índice de 1.07, que indica que por cada dólar que se invierte en el proyecto se obtiene un beneficio de 0.07 centavos. El VAN es de USD 17.713,14, siendo positivo y pudiéndose considerar con ello que el proyecto es factible. La TIR es del 29,09 %. Así, se determinó como factible en términos económicos la implementación del proyecto, siendo una mejora sustancial con respecto a la situación actual sin implementación.

Hallazgos de aspectos técnicos

Los hallazgos identificados en el proceso de diagnóstico refieren, por una parte, a aspectos técnicos relacionados con la red. En primer lugar, se evidenció una infraestructura descentralizada, con lo cual mantener el control de la seguridad en la red es más complejo.

Dado que en la actualidad la información es uno de los principales activos que manejan las compañías y organizaciones, la seguridad es fundamental. Para el caso particular de una casa de estudios, la mayoría de los procesos e información que estas manejan se encuentran digitalizados, lo que implica que la actividad crítica de la organización se centra en la gestión de la información. De base, una red WAN y el protocolo MPLS para la red backbone, cuenta con una arquitectura basada en capas (núcleo, distribución y acceso)

El protocolo MPLS, por su parte, presenta algunas desventajas que constituyen un hallazgo: presenta elevados costos de inversión. De igual manera, la red se presenta con falencias en su flexibilidad y escalabilidad, lo que dificulta la gestión y la compatibilidad con tecnologías tanto tradicionales como emergentes.

Conclusiones

Respecto del análisis económico realizado, se determinó que la red SDN simulada para el backbone de la Universidad de las Fuerzas Armadas es factible económicamente con una inversión de $19.357,81, presentando los indicadores TIR de 29,09%, VAN $17.713,14 y ROI de 6,95 (primer año). Esto indica que la implementación de la red es factible económicamente y que representa una optimización respecto de la actual gestión de datos.

Se ha determinado que el análisis de costo/beneficio realizado indica que es favorable para la institución actualizar e implementar un sistema de red SDN, ya que se constató que este es de USD 1,07. Esto, además de ser económicamente factible, permitirá manejar con mayor seguridad la red, controlar y administrar de manera eficiente mediante la seguridad centralizada y obtener un sistema escalable y flexible para integrar nuevas tecnologías a medida que surjan.

Respecto a la factibilidad técnica ofrecida por la red SDN, se conoció que presentó un buen desempeño en las pruebas realizadas. Respecto de la conectividad, esta se comprobó entre las cuatro sedes y la casa matriz, presentándose adecuada en todos los casos. El desempeño, por otra parte, se mostró adecuado; la latencia obtuvo valores promedio entre 2.682 y 6.420, con desviaciones estándar de entre 5.768 y 15.643. La pérdida de paquetes presentó en todos los casos analizados un 0%, mientras que la tasa de transferencia de datos fue igualmente adecuada. Por lo tanto, también es factible a nivel técnico.

Aun cuando se presentan amplias ventajas, la tecnología de red SDN tiene algunas desventajas y riesgos asociados a su novedad. En primer lugar, cabe mencionar que algunas herramientas se encuentran aún en desarrollo, y, con ello, no se comprende su funcionamiento. Esto se resuelve de manera empírica a medida que se utilizan las herramientas y se incursiona en nuevas funcionalidades. Por otra parte, el conocimiento de los administradores y de los profesionales del área es un ámbito en el que se presentan déficit que, dada la novedad de la tecnología, se van resolviendo conforme se avanza en su implementación masiva. Algunas de

las áreas en que se ha identificado la exigencia de mejorar y/o ajustar los servicios de estas redes son los gastos que implica el cambiar el hardware y el software, la deficiente interoperabilidad con otros sistemas existentes, algunas características y funciones que se muestran inconsistentes y la falta de confiabilidad y problemas de desempeño. Todos estos riesgos pueden ser solventados con un estudio acabado del funcionamiento de las redes y de su rendimiento; y siendo, por esto, más favorable su implementación por los beneficios que puede generar.

Recomendaciones

A partir de la simulación y el análisis técnico económico realizado y los resultados obtenidos, se pueden plantear las siguientes recomendaciones:

Se recomienda implementar la red SDN simulada en la Universidad de las Fuerzas Armadas debido a los beneficios que esta representa y debido a su factibilidad económica, con lo que la gestión de la información puede ser más eficiente y segura. De igual manera, se recomienda implementar un sistema de gestión de información, que comprenda un seguimiento y evaluación continuos del funcionamiento.

Las redes SDN son una tecnología relativamente nueva que está en constante avance y redescubrimiento. Por tan razón, es posible que el funcionamiento de esta presente brechas respecto de algunos rendimientos y/o costos de implementación debido a la necesidad de adaptar el hardware. Para esto, es importante que los administradores de la red estén constantemente evaluando su desempeño y verificando la interoperabilidad entre la red y otros servicios y tecnologías.

Por otra parte, es preciso que los mismos administradores se capaciten y actualicen con regularidad los conocimientos sobre la red, de manera de prever posibles fallos o vulnerabilidades. La seguridad centralizada es efectiva para controlar adecuadamente una red

institucional, de modo que su implementación y administración adecuadas puede mejorar sustancialmente la eficiencia del sistema de gestión de información de la universidad.

Trabajos futuros

Es importante continuar estudiando el desempeño que tiene este tipo de red y, sobre todo, la interoperabilidad de esta con otros servicios web o aplicativos que surgen constantemente y que pueden presentar problemas de compatibilidad. Con esto se puede fortalecer aún más la seguridad de la red y reducir considerablemente sus vulnerabilidades.

Bibliografía

Aguilera, A. (2017). El costo-beneficio como herramienta de decisión en la inversión en actividades científicas. *Cofin Habana. 11(2)*, En línea. Disponible en http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2073-60612017000200022.

Banco Central del Ecuador. (30 de noviembre de 2021). *Información Estadística Mensual No. 2037 - Noviembre 2021*. https://contenido.bce.fin.ec/home1/estadisticas/bolmensual/IEMensual.jsp

BanEcuador. (5 de Noviembre de 2021). *Tasas de interés*. https://www.banecuador.fin.ec/tasas-de-interes/

Bargted, C., & Kettlun, A. (2016). *Indicadores de evaluación de proyectos.* Santiago: Universidad de Chile.

Barroso, J. (2018). *Estudio de las redes definidas por software (SDN) y desarrollo de un prototipo para la Diputación de Cádiz.* [TFG] Universidad de Cádiz. En https://rodin.uca.es/handle/10498/22568.

Bone, M., Rodríguez, J., Sosa, S., & Núñez, L. (2021). Aplicaciones de SDN en infraestructura de redes educativas. *Ciencia Digital 5(1)*, 219-231. DOI: https://doi.org/10.33262/cienciadigital.v5i1.1539.

Cameselle, A. (2021). *Definición de un sistema de gestión de políticas de seguridad utilizando redes SDN.* [Trabajo de fin de máster] Universidad de Vigo. En http://castor.det.uvigo.es:8080/xmlui/bitstream/handle/123456789/571/TFM_Adrian_Cameselle_Martin.pdf?sequence=1.

Cisco. (31 de Agosto de 2015). *Infraestructura Prime 3.0*. https://software.cisco.com/download/home/286285348/type/284272932/release/3.0.0

Cisco. (25 de Noviembre de 2016). *Wireless*. https://www.cisco.com/c/es_mx/support/wireless/index.html

Cisco. (17 de Junio de 2019). *Módulo de servicios inalámbricos de Cisco 2 (WiSM2)*. https://www.cisco.com/c/en/us/products/interfaces-modules/wireless-services-module-2-wism2/index.html

Cisco. (12 de 12 de 2021). *Switch administrado de 24 puertos 10/100 POE Cisco SF350-24P*.: https://www.cisco.com/c/es_mx/support/switches/sf350-24p-24-port-10-100-poe-managed-switch/model.html

Conpilar. (12 de 03 de 2021). *Cómo instalar Eclipse IDE en Ubuntu 20.04*.: https://conpilar.es/como-instalar-eclipse-ide-en-ubuntu-20-04/

Córdoba, S. (2019). *Estudio de redes SDN mediante Mininet y MiniEdit.* [TFG] Universitat de Valencia. En https://riunet.upv.es/bitstream/handle/10251/127877/C%c3%b3rdoba%20-%20Estudio%20de%20redes%20SDN%20mediante%20Mininet%20y%20MiniEdit.pdf?sequence=1&isAllowed=y.

Cuba, G. (2015). *Diseño e implementación de un controlador SDN/OpenFlow para una red de campus académica.* [Tesis de grado] Pontificia Universidad Católica del Perú. En https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/7149.

Duarte, G., & Lobo, R. (2015). Emulación de escenarios virtuales en una SDWLAN (Software Defined Wireless Local Area Network) de un campus universitario. *Ingeniería al Día*, 69-85.

Dueñas, C., Marín, Y., & Enriquez, H. (2017). Red SDN vs Red Tradicional. *ResearchGate*, 1-7.

Eclipse. (12 de 12 de 2021). *Eclipse IDE for Java Developers*.: https://www.eclipse.org/downloads/packages/release/kepler/sr1/eclipse-ide-java-developers

Gámez, L., Calderón, A., & Ballester, S. (2016). Evaluación de desempeño y configuraciones de las SDN mediante la simulación. *TONO vol. 13*, 29-33.

García, A., Rodríguez, C., Calderón, C., & Casmartiño, F. (2014). Controladores SDN, elementos para su selección y evaluación. *Telem@tica, 13*(3), 10-20.

Guanoluisa, E. (2019). *Diseño de la arquitectura de una red SDN mediante el protocolo OpenFlow con simulación en el software Mininet para la infraestructura de una pyme.* [Tesis de grado] UDLA. En https://repositorioslatinoamericanos.uchile.cl/handle/2250/2795725.

Herrera, A. (2020). *Diseño y optimización de una red GPON a través de una red SDN para la Facultad Técnica para el Desarrollo.* [Tesis de grado] Universidad Católica de Santiago de Guayaquil. En http://201.159.223.180/handle/3317/15577.

HowtoInstall. (12 de 12 de 2021). *Cómo instalar floodlight en Ubuntu*.: https://howtoinstall.co/es/floodlight

HowtoInstall. (12 de 12 de 2021). *Cómo instalar mininet en Ubuntu*.: https://howtoinstall.co/es/mininet

HowtoInstall. (12 de 12 de 2021). *Cómo instalar openvswitch-switch en Ubuntu*.: https://howtoinstall.co/es/openvswitch-switch

Iglesias, D., Álvarez, F., & Ramos, A. (2019). Combinación de mecanismos MPLS en una arquitectura SDN. *Revista Telem@tica. 18(1)*, 1-10.

Instituto Nacional de Estadística y Censos. (30 de noviembre de 2021). *Inflación (Índice de Precios al Consumidor)*. https://www.ecuadorencifras.gob.ec//indice-de-precios-al-consumidor/

Jiménez, J. (25 de Mayo de 2021). *Qué es backbone o red troncal y para qué se utiliza*.: https://www.redeszone.net/tutoriales/redes-cable/backbone-red-troncal-tipos/

Jiménez, P., & Ramos, A. (2018). *Desarrollo de prácticas de laboratorio de SDN en Mininet.* [Trabajo de diploma] Universidad Central "Marta Abreu" de las Villas. En https://dspace.uclv.edu.cu/handle/123456789/10059.

Joskowicz, J. (2008). *Redes de datos.* [Documento de trabajo] Universidad de la República. Instituto de Ingeniería Eléctrica. En https://www.researchgate.net/profile/Jose-

Joskowicz/publication/266907714_REDES_DE_DATOS/links/544e350a0cf26dda088e75f1/REDES-DE-DATOS.pdf.

Krishna, H. (2016). Providing end-to-end bandwidth guarantees with openflow.

Lasso, D., & Puchaicela, J. (2021). *Evaluación del rendimiento de un prototipo SDN (Software Defined Networking) bajo el protocolo OpenFlow utilizando herramientas OpenSource en un entorno virtualizado.* [Tesis de grado] Universidad Politécnica Salesiana. En http://dspace.ups.edu.ec/handle/123456789/19861.

Mantilla, C. (2021). *Análisis del Impacto de un Ataque DoS en la Calidad de Servicio de Sistemas Streaming Multimedia en Redes SDN.* [Tesis de maestría] Escuela Politécnica Nacional. En https://bibdigital.epn.edu.ec/bitstream/15000/21663/1/CD%2011143.pdf.

Marrone, L., Rodríguez, D., Talay, C., & González, C. (2020). Explorando las redes definidas por software (SDN). *XXII Workshop de Investigadores en Ciencias de la Computación (WICC 2020, El Calafate, Santa Cruz).* (págs. 100-104). Santa Cruz: Red de Universidades con Carreras en Informática. UNLP.

Open Networking Foundation [ONF]. (08 de 08 de 2021). *Software-Defined Networking (SDN) Definition*.: https://opennetworking.org/sdn-definition/?nab=0

Oviedo, B., Zhuma, E., Guzmán, D., & Cáceres, C. (2020). Análisis del desempeño de redes definidas por software frente a redes con arquitectura TCP/IP. *RISTI*, 137-150.

Pachés, A. (2020). *Estudio del controlador SDN Ryu sobre una Raspberry-Pi Model 4.* [TFG] Universitat Politecnica de Valencia. En https://m.riunet.upv.es/bitstream/handle/10251/152347/Juli%C3%A1n%20-%20Estudio%20del%20controlador%20SDN%20Ryu%20sobre%20una%20Raspberry-Pi%20Model%204.pdf?sequence=1&isAllowed=y.

Parra, R., Morales, V., & Hernández, J. (2015). Redes definidas por software: beneficios y riesgos de su implementación en universidades. *Revista CONAIC 2(3)*, DOI: https://doi.org/10.32671/terc.v2i3.153.

Pereira, G., & Gamess, E. (2017). Lineamientos para el despliegue de redes SDN/OpenFlow. *Revista Venezolana de Computación. 4(2)*, 21-33.

ProgramadorClic. (12 de 12 de 2021). *Instalación y uso de SDN-Mininet*. https://programmerclick.com/: https://programmerclick.com/article/49491544256/

Quintero, D., & Medina, J. (2020). *Evaluación del rendimiento de una red LAN y una red WAN tradicional bajo el estándar IEEE 802.3 y la norma RFC 3031 en un entorno simulado, aplicando procesos SDN.* [TFG] ITM. Disponible en https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/4692/DanielStiven_QuinteroLondo%c3%b1o_2021.pdf?sequence=1&isAllowed=y.

Ramos, J. (2021). *Evaluación del rendimiento de una red avanzada tradicional y una red avanzada SDN.* [Tesis de grado] Universidad Nacional Agraria de la Selva. En http://repositorio.unas.edu.pe/handle/UNAS/1937.

Ruiz, Y., Ramos, A., Iglesias, D., & Álvarez, F. (2019). Escenarios SDN en Mininet. *II Convención Científica Internacional* (págs. 1-15). Universidad Central "Marta Abreu" de las Villas.

Skorupa, J., & Fabbi, M. (2013). Ending the Confusion about Software-Defined Networking: A taxonomy. *Gartner Research*.

cobitSper, C. (2013). Software Defined Network: el futuro de las arquitecturas de red. *Data Center*, 42-45.

Tootoonchain, A., & Ganjali, Y. (2010). HyperFlow: A Distributed Control Plane for OpenFlow. *INM/WREN*, https://www.semanticscholar.org/paper/HyperFlow%3A-A-Distributed-Control-Plane-for-OpenFlow-Ganjali-Tootoonchian/b46e192c84945528f6029138fdb26a9629f2dc6c?p2df.

UTA. (08 de 03 de 2015). *Floodlight SDN Controller*.: http://190.15.141.68/index.php/uta/floodlight-controller

Valencia, B., Santacruz, S., Becerra, L., & Padilla, J. (2015). Mininet: una herramienta versátil para emulación y prototipado de redes definidas por software. *Entre Ciencia e Ingeniería. 9(17)*, 62-70.

Vázquez, J. (2011). *Diseño y Desarrollo de una Aplicación Para el Estudio Comparativo de Topologías de Red.* [Trabajo de fin de grado] Universidad Carlos III Madrid. En https://e-archivo.uc3m.es/handle/10016/12615.

Velásquez, W. (2013). Emulación de una red definida por software utilizando MiniNet. *Academia*, 1-8.

WebSetNet. (5 de 09 de 2020). *Instalar y usar Wireshark en Ubuntu Linux*.: https://websetnet.net/es/install-and-use-wireshark-on-ubuntu-linux/

Western Digital. (12 de 12 de 2021). *My Cloud Expert Series EX2 Ultra*.: https://www.westerndigital.com/es-es/products/network-attached-storage/wd-my-cloud-expert-series-ex2-ultra#WDBVBZ0000NCH-EESN

Wireshark. (12 de 12 de 2021). *About Wireshark*.: https://www.wireshark.org/