UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

PROPUESTA DE IMPLEMENTACIÓN DE UNA RED SDN POR MEDIO DEL CONTROLADOR FLOODLIGHT Y MININET PARA LA INSTITUCIÓN UNIDAD EDUCATIVA AMERICANO

AUTOR

MELENDRES DEL PEZO STEVE MARTIN

PROYECTO DE UNIDAD DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

ING. CASTILLO YAGUAL CARLOS, MGT

Santa Elena, Ecuador

Año 2023

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino, Mgtr.
DIRECTOR DE LA CARRERA

Ing. Carlos Castillo Yagual, Mgtr.
TUTOR

Ing. Alicia Andrade Vera, Mgtr.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez, Mgti.
DOCENTE GUÍA UIC

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por MELENDRES DE PEZO STEVE MARTIN, como requerimiento para la obtención del titulo de Ingeniero en Tecnologías de la Información.

La Libertad, a los 27 días del mes de febrero del año 2023

Ing. Carlos Castillo Yagual, Mgt

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **MELENDRES DEL PEZO STEVE MARTIN**

DECLARO QUE:

El trabajo de Titulación, Propuesta de implementación de una red SDN por medio del controlador Floodlight y MiniNet para la institución Unidad Educativa Americano previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 27 días del mes de febrero del año 2023

Steve Martin Melendres del Pezo

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Propuesta de implementación de una red SDN por medio del controlador Floodlight y MiniNet para la institución Unidad Educativa Americano, presentado por el estudiante, Melendres del Pezo Steve Martin fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 4%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS

MELENDRES DEL PEZO STEVE - PROYECTO FINAL 22-02-2023

4% Similitudes

3% Texto entre comillas

1% Idioma no reconocido

Nombre del documento: MELENDRES DEL PEZO STEVE - PROYECTO FINAL 22-02-2023.pdf

ID del documento: fae423c5f8d044aa5ac5f9da0f8334f9fbc9ba56

Tamaño del documento original: 2,34 Mo

Autor: Steve Melendres del Pezo

Depositante: Steve Melendres del Pezo

Fecha de depósito: 22/2/2023

Tipo de carga: url_submission

fecha de fin de análisis: 24/2/2023

Número de palabras: 15.940

Número de caracteres: 105.591

Ing. Carlos Castillo Yagual, Mgt

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **MELENDRES DEL PEZO STEVE MARTIN**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, a los 27 días del mes de febrero del año 2023

Steve Martin Melendres del Pezo

AGRADECIMIENTO

Agradezco en primer lugar a Dios, por brindarme salud y fortaleza en aquellos momentos de dificultad y debilidad en esta etapa de mi vida.

A mis padres Jackeline del Pezo y Martin Melendres, que durante el transcurso de mi preparación profesional me han ayudado económicamente en mis estudios y por haber estado presente apoyándome siempre, guiándome y aconsejándome en todos los momentos en donde necesitaba ánimos para seguir adelante con mi carrera profesional.

A mis hermanos Geraldine, Ronny y Christopher, que me hacían sentir orgulloso de mi mismo a través de sus palabras, por estar siempre presentes, acompañándome y dándome su apoyo moral. A mis sobrinos Dante y Samira, que con sus travesuras y risas me alegraban el día.

A mi pareja Angee Rocafuerte, por motivarme y darme esperanzas diciéndome que lo lograría, por ayudarme hasta donde te era posible, muchas gracias corazón.

Y un especial agradecimiento al Ingeniero Carlos Castillo, por su paciencia y capacitación durante el desarrollo de este proyecto.

Steve Martin Melendres del Pezo

DEDICATORIA

Este proyecto va dedicado con mucho cariño y sentimiento a mi padre Martin Melendres, que me enseño que la mejor educación que se puede tener es la que se aprende uno mismo, a mi madre Jackeline del Pezo, quien me enseño que los sueños más grandes pueden alcanzarse sin prisa, pero sin pausa.

A toda mi familia por todo el apoyo incondicional, amor y confianza, que fueron de motivación para que fuese posible este momento, que es la culminación de mi carrera profesional.

Steve Martin Melendres del Pezo

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

Este trabajo se basó en una propuesta tecnológica de “Propuesta de implementación de una red SDN por medio del controlador Floodlight y MiniNet para la institución Unidad Educativa Americano. Fue desarrollado en dos capítulos. En el primer capítulo contiene temas como la fundamentación, antecedentes, descripción del proyecto, objetivos del proyecto, justificación, alcance, metodología, técnicas de recolección de datos de esta institución, en el cual se realiza la simulación un diseño de red SDN basado en el diseño de la red tradicional existente dentro de esta unidad educativa. En el segundo capítulo, se basó en el componente practico, mostrando las herramientas y componentes utilizados para la simulación de la red SDN, a la misma ves su funcionalidad, reglas de control de acceso para denegar el acceso entre Hosts, analizando el tráfico TCP con la herramienta de Wireshark, conectividad entre hosts. Dando como resultados obtenidos cumpliendo con los requisitos previstos.

Palabras claves: SDN, MiniNet, Floodlight.

ABSTRACT

This work was based on a technological proposal of "Proposal for the implementation of an SDN network using the Floodlight controller and MiniNet for the American Educational Unit institution". It was developed in two chapters. The first chapter contains topics such as justification, background, project description, project objectives, justification, scope, methodology, data collection techniques of this institution, in which the simulation of an SDN network design based on the design of the existing traditional network within this educational unit is performed. In the second chapter, it was based on the practical component, showing the tools and components used for the simulation of the SDN network, at the same time its functionality, access control rules to deny access between hosts, analyzing TCP traffic with the Wireshark tool, connectivity between hosts. The results obtained were the fulfillment of the expected requirements.

Keywords: SDN, MiniNet, Floodlight.

INTRODUCCIÓN

Este proyecto consistió en una propuesta tecnológica para la Unidad Educativa Americano. La institución se ha propuesto mantener actualizados y optimizar sus equipos informáticos, ya que en la actualidad sólo dispone de una red de datos con un diseño de red habitual que ha sufrido demoras, defectos de seguridad y gastos significativos, ya que ha reinstalado repetidamente sus equipos informáticos y no consiguen resultados que se esperaban.

Por esto es la importancia de examinar y concentrarse punto por punto para dar una propuesta capaz de fijar un nivel de desarrollo tecnológico, ampliando la capacidad y la productividad en la satisfacción de la misión delegada.

Una red convencional permite el intercambio de datos, sin embargo, en la actualidad existen nuevas tecnologías, como lo son las redes definidas por software, estas usan un solo plano de control para una estructura de red, dejando al switch de forma autónoma, lo que lo convierte en la ruta donde se enviaran los paquetes de origen a destino.

Las SDN, facilitan la programación de los paquetes conmutados, además se realizan las configuraciones en un solo dispositivo, con un control centralizado y programable, dejando a un lado la configuración por cada dispositivo en una estructura de red.

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1. Antecedentes

Tanto en empresas como en instituciones educativas, manejan el paradigma de un modelo de red tradicional integradas verticalmente, donde la gestión de los dispositivos se da de manera autónoma con su propio firmware instalado en su espacio de memoria[1]. En la actualidad la configuración de los equipos de red y nodos convencionales, ya no son adecuados ante el requerimiento a enormes cantidades de trabajos, esto debido a que hay que tener en cuenta que la distribución de redes de información y los servicios de capa superior demandan un número mayor de nodos a medida que se desarrollan exponencialmente[2].

La Unidad Educativa Americano ha tenido constantes problemas en su red, actualmente utilizan una red local con un diseño habitual, esto ha creado contratiempos y necesitan más velocidad de transferencia. Así mismo en su momento por elección de la administración de la institución se realizó una actualización de todo su hardware lo que supuso un gasto excepcionalmente importante y el problema no se solucionó del todo, además los especialistas de la institución, al darse cuenta de que este problema seguía siendo constante, optó por un sistema de alto coste que facilita la gestión de su información y proporciona mayor seguridad.

La SDN es un enfoque de construcción de estructuras de red que permite que una organización sea regulada u observada de manera astuta y unificada utilizando la programación. Esto ayuda a tratar la red de una manera exacta y completamente aislada de cualquier red actual. Como ventajas o beneficios que las SDN dan al cliente, podemos hacer referencia a que son más adaptables, versátiles, dan fondos de reserva de costes a largo plazo, utilizan la robotización, incrementan la seguridad y tienen una estructura básica[3].

Esta innovación se ha convertido en una estrategia prometedora para trabajar en la eficacia de la dirección en una red, el control de los flujos de datos, la calidad de servicio QoS y la seguridad. No obstante, la investigación sobre SDN se encuentra actualmente en una fase inicial y hay cuestiones que deberán explorarse adicionalmente. En particular, la búsqueda de cursos ideales para las aplicaciones que

requieren QoS y la seguridad, que abordan cuestiones importantes sobre las cuales la falta de atención ha sido completamente estudiada y focalizada debido a su desconcertante ejecución[4].

Yanko[5], nos muestra a través de su estudio, que a lo largo de los últimos años, que a pesar de los inmensos intereses en la exploración y los costes de aseguramiento del hardware, actualmente estructuran un obstáculo a la sección de nuevos tipos de innovación para mejorar los activos, lo que trae consigo una obstrucción a la destreza de la mejora, que hoy en día no es adecuada para satisfacer la necesidad y las expectativas de los clientes y el cambio del mercado, de esta manera trayendo la dependencia de los incluidos.

Benzekki[6], nos radica la importancia de evolucionar las estructuras de red, incitando al desarrollo a través de la programación de esta. Hoy en día, los responsables de las redes realizan las configuraciones, controlan y supervisan de manera manual y física los equipos, lo que supone un perjuicio en esta época informatizada, al no poder reaccionar de forma idónea ante las situaciones como el tráfico volátil en la red.

En 2018 Córdoba [7], planteo que desde una perspectiva, las condiciones para poder emplear SDN, que fueron las razones para ampliar las capacidades de la red, la dirección de paquetes controlados por aplicaciones, el panel de equipos, la naturaleza de la administración, la definición y la circulación absoluta de los acuerdos de seguridad. De la misma forma, algunos tipos de análisis están relacionados con el Internet de las cosas (IOT), la base de datos y la virtualización. El diseño de la SDN tiene como norma esencial la partición de los planos de control e información por lo que depende del protocolo OpenFlow para la correspondencia entre el servidor o servidores de control y conmutadores[8].

Estas son una parte de las cuestiones relacionadas con el plan y el diseño de su red, la misma que se utilizará como premisa para mostrar a través de un estudio de las mejoras que tiene otro modelo de red como SDN. Floodlight ofrece facilidades de implementación y mejoras en el desempeño del usuario en su labor. Además, es apto para ejecutar varios ciclos simultáneamente, es de ejecución superior y puede trabajar con redes híbridas Floodlight.

Al emplear redes SDN proporcionará la reserva de costes, la mejora de los activos, la seguridad de los datos y una red más sencilla que actuará como propuesta para la institución “Unidad Educativa Americano”.

En definitiva, se proponen las consecuencias de los distintos estudios de las clasificaciones referenciadas y de las partes de los trabajos explorados para realizar un modelo de red SDN con un controlador para su virtualización.

1.2. Descripción del Proyecto

La institución “Unidad Educativa Americano”, ha encontrado últimamente un enorme desarrollo en la cantidad de dispositivos y clientes vinculados a la red de la institución, haciendo que la necesidad de organizar y controlar los dispositivos de red e intercambio dentro del colegio, haga que el control de la organización y de sus dispositivos sea más difícil y tedioso.

Por lo cual en este proyecto se propone implementar una red SDN, para la administración, control, incorporación y la generación de redes virtuales utilizando el controlador de Floodlight por medio de la herramienta de MiniNet.

Para esta institución educativa se virtualizará una red SDN, donde se aprovecharán las ventajas de tratar con una red haciendo uso de un controlador que permitirá a los conmutadores saber que secuencia tomar para el envío de paquetes alejándose del tráfico de información o latencia, dirigiendo solo a los paquetes necesarios el acceso esencial, abordando con éxitos los problemas que surjan y disminuyendo el tiempo de aplazamiento, teniendo una ventaja especifica de ser versátil a una base actual.

Esto permitirá al responsable de la red mejorar los ciclos del establecimiento, ofreciendo un servicio y control eficaz a toda la institución.

Para el desarrollo de esta propuesta en la institución, constara de 5 etapas de la metodología PPDIOO, las cuales serán detalladas a continuación:

Etapa de Planificación

Se identificarán las deficiencias, requerimientos, tecnologías innovadoras, protocolos y controladores de red, con el objetivo de elaborar un plan de proyectos para el desarrollo de esta propuesta en la institución.

Etapa de Diseño

En esta etapa se diseñará el modelo de red definida por software (SDN), que se llevará a cabo a través de la estructura física de la red tradicional y el organigrama administrativo de la institución, agregando detalles y sugerencias para que el modelo a implementarse cumpla con las expectativas requeridas.

Etapa de Implementación

Se implementarán las instalaciones y configuraciones de la red SDN establecidas en la etapa de diseño, adjuntando la documentación de los procesos. Así mismo se iniciará la virtualización del modelo de red SDN, sin perjudicar ni vulnerar la red física en funcionamiento.

Etapa de Operación

En esta etapa se simulará y se harán pruebas necesarias del funcionamiento de la red, el monitoreo de sus componentes, su rendimiento y la identificación de procesos incorrectos. Además, se corrobora el ancho de banda, conexiones entre host, políticas de control de acceso, tráfico y envió de paquetes en la red. Con el objetivo de asegurar el funcionamiento correcto de la red definida por software (SDN) cumpliendo con los parámetros establecidos.

Puesto a que este proyecto de simulación es implementar un modelo de red SDN, es importante utilizar herramientas particulares para obtener un resultado que se acerque al funcionamiento total de una red definida por software. Las herramientas que se utilizaron para esta implementación fueron las siguientes:

Virtualbox: Potente producto de virtualización x86 y AMD64/Intel64 para uso empresarial y doméstico[9].

Floodlight: Controlador OpenFlow basado en java de clases empresarial con licencia de Apache[10], para trabajar con una cantidad creciente de switches, routers, switches virtuales y puntos de acceso (APs) que soporten el estándar OpenFlow[11].

Miniedit: Interfaz gráfica idónea para experimentar con los conceptos de las redes SDN y OpenFlow[7].

Mininet: Crea una red virtual realista, ejecutando código real de kernel, switch y aplicación, en una sola máquina (VM, nube o nativa), en segundos, con un solo comando[12].

OpenFlow: Protocolo estándar en las redes tradicionales definidas por software[13].

Wireshark: Es una herramienta multiplataforma de análisis de red, producto de la evolución de Ethereal[14].

El siguiente proyecto sigue a la línea de investigación relacionada con temas de infraestructura y seguridad de las tecnologías de la información, tecnologías verdes, virtualización y computación en la nube, seguridad de la información, el internet de las cosas a través de las redes de comunicación, sensores eléctricos y sistemas informáticos, sistemas de información geográfica, gestión de seguridad de la información que permitan generar información indispensable para la toma de decisiones[15].

1.3. Objetivos del proyecto

1.3.1. Objetivo general

Diseño de un modelo de red SDN, para la virtualización a través del controlador Floodlight en la Unidad Educativa Americano.

1.3.2. Objetivos específicos

- Definir los enfoques relacionados con la composición de redes SDN caracterizadas para la práctica de virtualización.
- Determinar los prototipos de software accesibles para la implementación de una SDN.
- Analizar los distintos tipos de controladores destinados a la virtualización de una red SDN.
- Plantear un modelo de red utilizando el controlador Floodlight.

1.4. Justificación del proyecto

La implementación de una red SDN es fundamental, pues al contrario que una red típica, las SDN ofrecen un desarrollo en la optimización de los activos, no suponen gastos significativos, adaptabilidad, versatilidad, automatización, niveles altos de seguridad y una gestión sencilla.

La implementación y la simulación de una red definida por software, hará posible acoplar las necesidades de la institución. Las capacidades de la red podrán ejecutarse

rápidamente cuando el usuario las necesite de forma precisa, manteniéndose libre de una disposición monótona.

Este modelo de red inteligente resumirá el trabajo del usuario en sí, no consume mucho tiempo ni medidas irrazonables de efectivo, se ejecuta con la administración de datos y en consecuencia este modelo es excelente para la Unidad Educativa Americano, a diferencia de la red tradicional actualmente existente.

La empresa Orbit Consulting Group[16], posteo en su página los aspectos más destacables de una red SDN, las cuales son:

1. Capacidad para administrar dinámicamente el ancho de banda según necesidades de cada recurso y tipo de usuario.
2. Mayor agilidad en el despliegue y control de redes.
3. Posibilidad de gestionar de forma centralizada todos los recursos de seguridad de la empresa.
4. Monitorización continua de redes y usuarios (huella digital).
5. Generación de Analíticas.

Actualmente los centros de educación en la provincia de Santa Elena, ya sean fiscales o particulares, cuentan con modelos de redes tradicionales en el que cada dispositivo se supervisa de forma independiente, por esto al referirse de redes definidas por software parte de un controlador primario y este se encargará de gestionar la infraestructura y sus dispositivos, agilizando la recepción de paquetes y dirigiéndolos a la ruta más rápidas para llegar a su destino.

De esta manera la primera etapa de **planificación,** permitirá la elección de la innovación tecnológica que se utilizará para hacer el modelo que se efectuará en la red ahora funcional del establecimiento para la programación de propósitos de redes SDN, donde se reconocerá la versatilidad, la flexibilidad, la accesibilidad y el tráfico de la red, entre diferentes elementos.

Así mismo la segunda etapa de **diseño,** nos da una perspectiva de la red de acuerdo con una representación relacionada, un plano o boceto de lo que podría ser la estructura de la red que se ajusta a los activos y la construcción del sitio, igualmente da el plano de un formato real de donde se encontrarían los dispositivos de la red en la institución.

En la tercera etapa de **implementación,** la red diseñada está preparada para su correcta ejecución, es en este punto donde se comienzan a colocar los dispositivos que se utilizarán para el nuevo modelo de red que se va a ofrecer a la institución.

En la cuarta etapa de **operación,** será posible realizar conexiones con diferentes dispositivos dentro de la red, examinar el tráfico producido a medida que se envían los paquetes empezando por un host y la utilización de la capacidad de transferencia de datos.

El proyecto está orientado al Plan de Creación de Oportunidades, haciendo énfasis en la directriz 1, lineamiento territorial A4, objetivo 5, política 5.5.

Directriz 1: Soporte territorial para la garantía de derechos[17].

Lineamiento territorial A4: Fortalecer la conectividad y el acceso a las TIC como una vía para mejorar el acceso a otros servicios[17].

Objetivo 5: Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social[17].

Política 5.5: Mejorar la conectividad digital y el acceso a nuevas tecnologías de la población[17].

1.5. Alcance del proyecto

El alcance de esta propuesta a la institución Unidad Educativa Americano, será el diseño y la implementación de una red definida por software (SDN), para acoplar las necesidades presentadas, el cual se hará la virtualización usando el controlador de Floodlight ideal para administrar mejor el funcionamiento de la institución.

Esto ofrecerá otro punto de vista a la institución de cómo podría funcionar una red supervisada por un único controlador manteniéndose alejados de los problemas de contradicción del propio dispositivo o de los problemas reales que pudieran surgir dentro de sus departamentos. Así como dar una importancia más amplia a la versatilidad de la infraestructura de red, donde por circunstancias de instrucción o investigación se podría efectuar un cambio de una estructura de red en el instante que se demande.

Para establecer los enlaces inalámbricos y la movilidad de los equipos, se determinaron conceptos básicos como la arquitectura SDN, el protocolo OpenFlow, el controlador Floodlight, VirtualBox, MiniEdit y MiniNet.

Para el desarrollo del proyecto, se realizarán 4 etapas de la metodología PPDIOO:

1. Etapa de planificación
2. Etapa de diseño
3. Etapa de implementación
4. Etapa de operación

La simulación de la red virtualizada permitirá observar el tráfico en la red en tiempo real a través del analizador de Wireshark, orientándose a la calidad de servicio para prevenir problemas de latencia a través del controlador Floodlight.

Es importante indicar que este proyecto no se llevará a cabo formalmente en las oficinas del establecimiento para suplantar a la estructura de red con la que trabaja habitualmente, por el contrario, será otro punto de vista para la ejecución de toda la red supervisada a través de un único PC.

1.6. Metodología

1.6.1. Metodología de la Investigación

El proyecto se realizará en base a la aplicación de la metodología de investigación de estudio exploratorio con el que se pretende analizar el tema propuesto para explicar cuestiones relacionadas con su desarrollo[18]. La institución Unidad Educativa Americano posee una estructura de red tipo hogar, por esto la red SDN estará simulada asemejada a una estructura de red real, generando una investigación para recoger datos sobre la presentación de una red convencional frente a una red SDN, obteniendo información de referencias bibliográficas sólidas y una entrevista al director de la institución.

A través de una entrevista con el director del establecimiento educativo, se quiere obtener datos en el caso de que sea factible disminuir el tiempo de reacción inmediata a una versatilidad en la red existente ante una red SDN, incluyendo el aplazamiento del tiempo de mantenimiento y actualización de hardware que hasta el momento tiene un lugar con el funcionamiento de la red.

Se trata de enfoques que conducen a un tiempo de disposición diferido para que una red convencional funcione de manera competente, de esta manera, para mejorar los datos que se van a utilizar, por ejemplo, la temporada de adquisición del hardware y el tiempo utilizados para su configuración, será aplicada a través de una metodología de la investigación de tipo diagnóstica[18].

La propuesta planteada trata de abordar los problemas de versatilidad de la red evitando los aplazamientos innecesarios entre la adquisición, el diseño y la asociación del conmutador con fines investigativos.

1.6.2. Beneficiarios del proyecto

Los beneficiarios del proyecto se encuentran clasificados en beneficiarios directos, conformados por la administración de la institución:

Beneficiarios	**Áreas**	**Numero de Personal**
B. DIRECTOS	Administración:	6
	Total:	6

Tabla 1. Beneficiarios del Proyecto

1.6.3. Variable

- La variable de este proyecto es la disminución del tiempo con respecto a la transmisión de paquetes de datos en la red de la institución Unidad Educativa Americano.

Con la iniciativa planteada y la información obtenida se pretende buscar una forma de disminuir el proceso de transmisión de datos, teniendo un mejor control a través de reglas de accesos creadas en MiniNet, también mejorando el ancho de banda por medio de la monitorización de Wireshark en tiempo real de la red y el controlador Floodlight para la creación de una red definida por software.

1.6.4. Técnicas de recolección de información

Se describe el modo en que se han obtenido los datos previstos para continuar con el proyecto, especificando el procedimiento técnico de la investigación, población e individuo:

Técnica	Entrevista
Población	Institución Unidad Educativa Americano
Individuo	Gerente General

Tabla 2. Descripción de procedimiento técnico

Entrevista	Como modo de recolección de datos de información, se hará uso de esta técnica, que tendrá un banco de 5 preguntas.
Institución Educativa	Lugar donde se desarrollará y se simulará el proyecto, ubicado en el cantón La Libertad,
Gerente General	Responsable de la administración de la institución, autoridad a quien ira dirigido la entrevista.

Tabla 3. Recolección de información

1.6.5. Metodología de desarrollo

La metodología PPDIOO fue escogida para llevar a cabo esta propuesta, debido a que puede acoplarse a una infraestructura de red funcional existente o iniciar un plan de

rediseño de la red para estructurar de forma legítima las distintas diligencias a realizar durante el ciclo funcional de la red.

Contienen 6 etapas oficiales, en donde la última etapa solo se aplica a partir de una red que ya nunca más será mejorada para terminar el ciclo de vida de esta. Por esto CISCO ajusto esta metodología añadiendo una etapa antes de la etapa de planificación para añadir una etapa de preparación.

Respecto al proyecto, solo serán implementadas y desarrolladas 4 etapas principales, dejando a las etapas 5 y 6 de retirar, para fines de optimizaciones en el futuro.

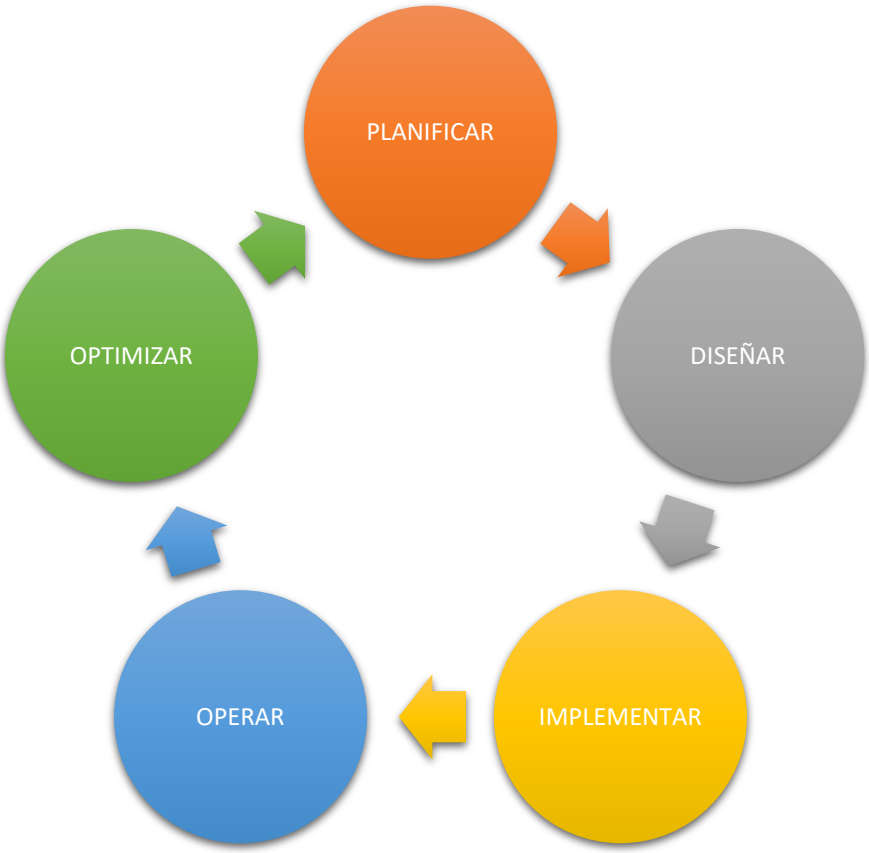


Figura 1. Etapas del Modelo PPDIOO

Planificar: Se analizará los dispositivos operativos para el funcionamiento correcto de la red y escoger a un único dispositivo con las mejores características para que se convierta en el controlador. Así mismo en el equipo escogido será la maquina anfitrión en donde se procederá a instalar el software sugerido en las herramientas anteriores comentadas.

Diseñar: El diseño de red SDN, estará orientada a su estructura de áreas de la institución. No se diseñará un nuevo modelo debido a que se ajustará al modelo de red existente y que pasará a ser una estructura de red virtualizada, añadiendo dispositivos sin necesitar recursos.

Implementar: Con el esquema de red lógico de la institución, se realiza la simulación para la comprobación de la efectividad de las etapas anteriores, así mismo verificar el comportamiento de la red y sus hosts. En caso de ocurrir algún tipo de error, será tratado en la siguiente etapa.

Operar: Se verificará el funcionamiento total de la red SDN implementada en la institución. También se evidenciará el tráfico de red en host y el controlador, en la transmisión de paquetes, problemas de latencias, velocidad de transmisión, conexiones entres hosts, reglas de control de acceso, ancho de banda y el tráfico de paquetes ICMP. El propósito de esta etapa se tratará de que la red SDN cumpla con los estándares establecidos.

1.6.6. Análisis e interpretación de la entrevista

La entrevista fue dirigida para el Ing. William Núñez, que ocupa el cargo de Gerente General de la institución "Unidad Educativa Americano", la entrevista fue de manera presencial en el Departamento Financiero, el cual nos respondió a las preguntas que fueron realizadas de acuerdo con el problema de red que presenta en la organización.

Se obtuvo como resultado de la entrevista puntos relativamente importantes, lo que se detallan a continuación:

- ✓ La institución realiza gastos en mantenimientos y en dispositivos nuevos, sin obtener una solución con el problema de tráfico de datos y seguridad en la red.
- ✓ Poseen una red tipo doméstica, lo cual no abastece a la institución.
- ✓ El grado de disparidad entre su arquitectura y sus dispositivos en su red, hacen que haya filtración de datos confidenciales.
- ✓ Es considerable cambiar a redes SDN, porque solo tener un switch Open Flow, gestionado por un solo controlador, aumenta el grado de seguridad, optimiza operaciones físicas y reduce gastos innecesarios.

CAPÍTULO II

LA PROPUESTA

2.1. Marco Contextual

2.1.1. Unidad Educativa Americano

La Unidad Educativa Americano es una institución creada recientemente en las instalaciones de lo que fue el colegio UPSE, ubicada en la provincia de Santa Elena, cantón La Libertad, fundada legalmente el 28 de junio del año 2022.

Una unidad educativa, comprometidas en la formación integral de los estudiantes, con habilidades académicas, humanas, sociales, artísticas y deportivas, tomando como base el desarrollo de sus valores y la solidaridad con la ciudadanía.

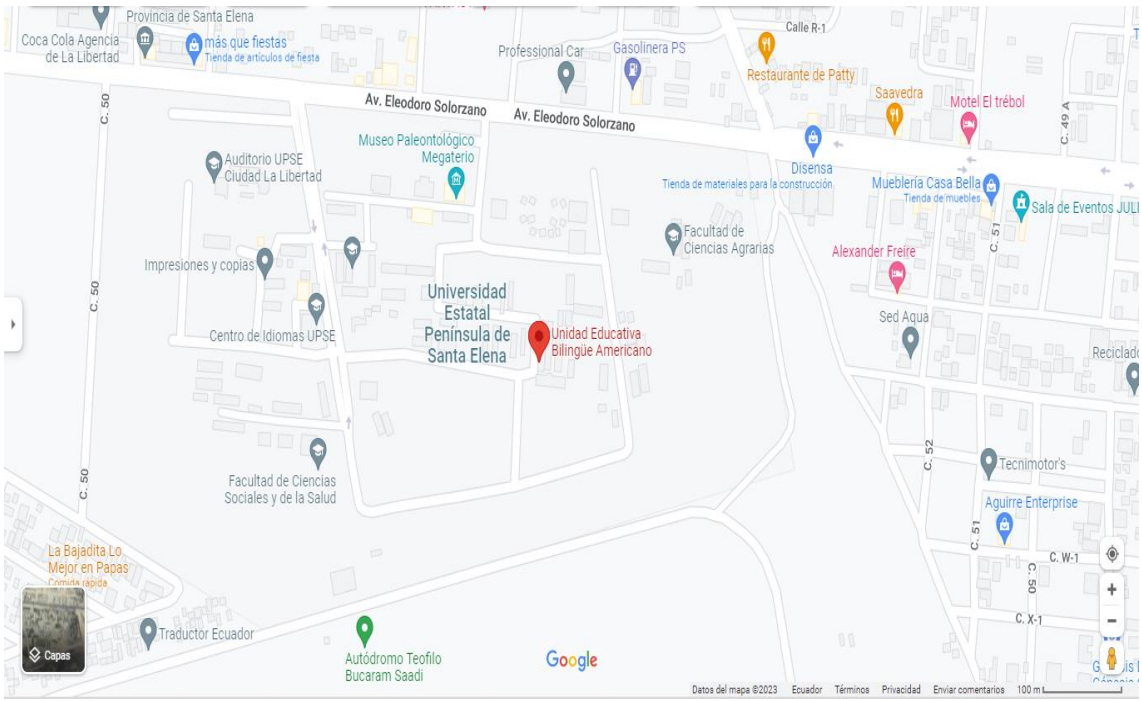


Figura 2. Ubicación de la Unidad Educativa Americano

VISIÓN

Ser reconocida en la provincia y el país como la Unidad de Educación Bilingüe, líder por su excelencia en sus programas académicos, humanístico, formado dentro de un

ambiente de mucha armonía, de seres humanos íntegros, capaces de generar cambios en el cuidado del medio ambiente.

MISIÓN

Somos una Unidad Educativa, humanística, comprometida con la formación integral de nuestros estudiantes formados para crear sus propias oportunidades, que contribuyan al desarrollo de la sociedad, competitiva y responsable.

2.1.2. Utilización de redes con arquitectura tradicional

Las redes con diseño convencionales son las que tienen en cuenta una dirección IP. Estas organizaciones son las más reconocidas en la actualidad y, en consecuencia, podría decirse que son las que más se llevan a cabo a nivel corporativo, el principal defecto de este tipo de redes es su administración, ya que es más complicada de ejecutar para el supervisor debido a sus disposiciones manuales y a su forma vertical integrada, diferentes desventajas de esta arquitectura de red convencional son los costes de ejecución y soporte, la vulnerabilidad de los datos y el tráfico en los procesos de transferencia de información[19].

La característica principal de estas redes es que cada uno de los dispositivos se controla a sí mismo, por ejemplo, cada uno de los dispositivos asociados sigue sus propias instrucciones y tiene su propio firmware introducido en el espacio accesible en su memoria [20].

Esto aumenta significativamente la complejidad de su trabajo y aumenta la posibilidad de errores sorprendentes en su ejecución, debido a este gran número de causas que se encuentran en las redes con diseño convencional, se podría decir que estas estructuras de redes avanzan a gran velocidad hacia creaciones de topologías de redes específicas que son más únicas y simultáneamente más programables, al igual que las redes definidas por software[21].

La Unidad Educativa Americano, tiene una arquitectura de red tradicional, donde todos los dispositivos se comunican con la red, los mismos que controlan el plano de control y datos, de este modo, para realizar cualquier ajuste que aborde un cambio, ya sea en caso de crear o rediseñar una topología, normas, añadir dispositivos o protocolos, el responsable de la red tendrá la obligación de realizar cambios físicos y configuraciones manuales en cada uno de los dispositivos accesibles, ya que este tipo

de arquitectura tradicional no pueden adaptarse sin una restructuración y reconfiguración en sus dispositivos conectados en su red[22].

2.2. Marco Conceptual

2.2.1. Redes informáticas

Se entiende por redes informáticas, redes de comunicaciones de datos o redes de computadoras a un número de sistemas informáticos conectados entre sí mediante una serie de dispositivos alámbricos o inalámbricos, gracias a los cuales pueden compartir información en paquetes de datos, transmitidos mediante impulsos eléctricos, ondas electromagnéticas o cualquier otro medio físico, los tipos de redes informáticas se clasifican según su aplicación y amplitud, como en redes PAN, LAN, MAN y WAN. De la misma forma están constituidas por nodos y elementos como servidores, clientes, medios de transmisión y equipo de hardware[23].

Una red informática es un conjunto de computadoras con sus periféricos de entrada y salida, cada una de estas computadoras está conectada a los llamados routers, también conocidos como enrutadores, estas redes informáticas pueden ser tanto inalámbricas o estar conectadas a través de cables de conexión, incluso pueden llegar a ser de tipo mixto, es decir una combinación de ambos tipos[24].

2.2.2. Redes Definidas por Software (SDN)

Las SDN facilitan la implementación y gestión de las administraciones de la organización de forma determinista, dinámica y versátil, evitando que el director de la organización supervise dichas administraciones a un nivel inferior, aparte constituyen una arquitectura de red cuya característica fundamental es desacoplar físicamente el plano de control (inteligencia) del plano de datos, derivando el control a una computadora (controlador) y esperando contar con dispositivos muy rápidos en las tareas de conmutación, aunque con limitada inteligencia[25].

Estas redes funcionan con un switch, en este existen dos partes diferenciadas, el plano de datos y el plano de control, el plano de datos corresponde a la parte del hardware, las tramas llegan al switch por cierto puerto y éste lo reenvía o distribuye por uno o varios puertos, este nivel de circuitos lo conforma el plano de datos, el plano de control es el cerebro del switch, es el que va a tomar esas decisiones para que esas tramas salgan por el puerto asignado, es decir, donde se decidirán y ejecutarán las decisiones de los protocolos que tengan implementados[19].

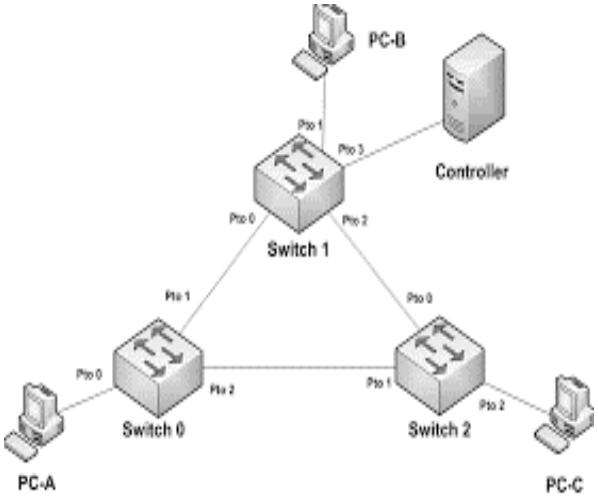


Figura 3. Arquitectura de una red SDN. [26].

2.2.3. Componentes de red SDN

A continuación, se muestra los componentes de las redes definida por software, que se dividen en tres capas:

- Capa de aplicación
- Capa de control
- Capa de infraestructura

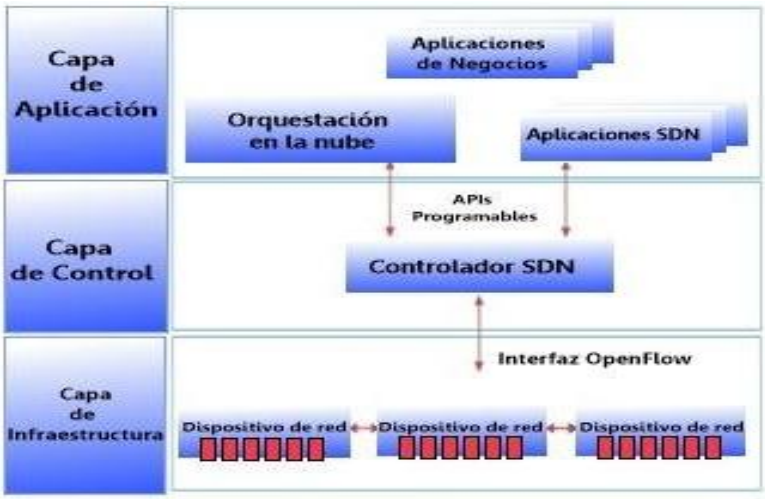


Figura 4. Componentes de una red SDN. [27].

Capa de aplicación: La capa Aplicaciones permite comunicar al controlador SDN, mediante las APIs hacia el norte, sus necesidades y el comportamiento que desean de la red, la interfaz de los controladores SDN hacia las aplicaciones es un conjunto de interfaces ya que la definición de aplicaciones SDN es muy amplia, cubriendo desde servicios de red, como QoS, a aplicaciones de negocio[28].

Capa de control: La capa intermedia la forma el Controlador SDN, quien tiene una visión global de la red, al igual que en un sistema operativo tradicional, la plataforma de control abstrae los detalles de bajo nivel de la conexión y la interacción con dispositivos de reenvío, es decir materializa las políticas de red[29].

Capa de infraestructura: Al igual que una red tradicional, la capa de infraestructura se compone de un conjunto de dispositivos, incluidos conmutadores y enrutadores que se vinculan entre sí, lo que genera una red sólida, la distinción fundamental es que los dispositivos típicos son piezas que representa un control considerable en él envió de paquete y no tiene un control exhaustivo[5]. Es la última capa de SDN donde se encuentran los dispositivos físicos o virtuales como (switch, routers) los cuales están conectados a través de una interfaz abierta que permite el switcheo y envío de paquetes en una conexión de red[30].

2.2.4. Herramienta de softwares para la virtualización

Hoy en día existen diferentes tipos de software para realizar la práctica de virtualización, en esta ocasión se mencionarán tres softwares utilizados en la práctica de redes SDN, los cuales son, Microsoft Hyper-V, VMware y Oracle VM Virtual box.

2.2.5. Plataforma Microsoft Hyper-V

Microsoft Hyper-V Server es un producto que permite la virtualización de servidores basada en hipervisor que permite a las organizaciones la consolidación de cargas de trabajo, mejorar el aprovechamiento del servidor y la reducción de costos. Microsoft Hyper-V Server contiene un hipervisor, modelo de controlador de Windows Server con capacidad de virtualización y componentes de apoyo como la conmutación por errores, sin embargo, no cuenta con el mismo conjunto de características y funciones de un sistema operativo Windows Server [31].

MS Hyper-V requiere un procesador con funcionalidad de virtualización asistida por hardware, lo que permite una base de código de virtualización mucho más compacta y la virtualización asociada. virtualización mucho más compacta y las consiguientes mejoras de rendimiento [32].

2.2.6. Plataforma VMware

Esta es una opción de virtualización realmente completa para alguna institución, aunque de código de pago, su coste por licencia es muy elevado, a excepción de otros tipos de software, consiste en unos de los sistemas de virtualización más populares

para la arquitectura x86, aparte es una infraestructura de virtualización que proporciona software para la virtualización desde entornos de escritorio hasta centros de datos, los productos disponibles se dividen en tres categorías: gestión y automatización, infraestructura virtual y plataformas de virtualización [33].

2.2.7. Plataforma Oracle VM Virtual box.

Virtual box es un hypervisor tipo 2 utilizado como herramienta de virtualización de hardware en servidores físicos, donde en una máquina física se comparte los recursos de hardware para instalar aplicaciones o sistemas operativos virtuales cada uno con su propio ambiente interacción, el cual actualmente es desarrollado por Oracle Corporation [34].

Permite la ejecución de una amplia variedad de sistemas operativos en las máquinas virtuales huésped sin que requiera los privilegios de administrador y permitiendo, si así se requiere, aislamiento total respecto al equipo anfitrión y la red de docencia [35].

2.2.8. Controladores de redes definidas por software (SDN)

Las SDN disponen de un componente clave, conocido como regulador o controlador, que tiene la capacidad de comunicar los requisitos previos procedentes de la capa de aplicación a los componentes de la red, por lo que se puede considerar que un controlador es el núcleo de toda la infraestructura, ya que se ocupa de los flujos y proporciona las órdenes importantes para que los diferentes componentes de la red accedan a ellos [10].

El controlador permite identificar los límites de los recursos y las necesidades de la organización desde un punto de vista generalizado, de este modo, la incorporación de redes SDN desarrolla aún más el control de los recursos de la red y potencia la automatización de la dirección[36].

Actualmente existen diferentes controladores OpenFlow y no Openflow, se mencionan de manera detallada los protocolos OpenFlow más utilizados.

2.2.9. Controlador OPEN DAYLIGHT

OPEN DAYLIGHT consiste es una plataforma modular accesible para automatizar y diseñar a medida redes de diverso alcance y escala, facilita el control programático con funciones de monitorización y administración centralizada de los dispositivos que

conforman la red, está basada en el entorno de programación java y funciona con Apache Maven como herramienta de autor de código abierto[37].

Apache Maven constituye la plataforma más implicada para los programadores en curso, se utiliza como instrumento de normalización, en otras palabras, se ocupa de la configuración de la ordenación, la agrupación y el establecimiento de las bibliotecas que posteriormente pueden ser supervisadas por los programadores[38].

2.2.10. Controlador ONOS

ONOS, controlador que funciona en la nube y es una de las etapas de código abierto más generalmente involucradas para la fabricación de SDN, mantiene configuraciones de red constantes, lo que elimina la necesidad de aplicar protocolos de intercambio y dirección dentro de la estructura de la red, además, facilita al cliente la creación eficaz de aplicaciones de red sin necesidad de cambiar los parámetros del plano de datos[39].

Fue creado para cubrir algunos requisitos de los operadores que buscaban soluciones de operador y que aprovechasen la economía del hardware y dieran la posibilidad de crear y desarrollar nuevos servicios de red dinámica con interfaces programables simplificadas[40].

2.2.11. Controlador Floodlight

Floodlight es un controlador OpenFlow que está basado en el lenguaje de programación Java, es uno de los más utilizados ya que contiene una máquina virtual que viene ya con configuraciones previas y con el software MiniNet integrado, Open Switch y Floodlight en su primera versión, también brinda a los usuarios maneras de ver la información sobre el estado del controlador y monitorización de los equipos remotos, además, permite conectar varios switches, hosts en la red, tablas de flujo y todo lo que contiene una topología de red[41], entre sus principales características se nombra las siguientes:

- Ofrece módulos de sistema de carga que son escalables y de fácil administración
- Configuración sencilla
- Es compatible con una gran cantidad de switches OpenFlow, virtuales y físicos
- Está creado para brindar un alto rendimiento, opciones de seguridad eficaces, y es tolerante a fallos
- Permite el uso de OpenStack.

2.2.12. MiniNet

MiniNet es un software que crea redes virtuales, utiliza switches, controladores y conexiones, es compatible con Linux y permiten usar el protocolo OpenFlow, este software es muy utilizado para desarrollar compartir y experimentar con otros sistemas de SDN, adicional es una buena herramienta para desarrollar, enseñar, investigar, crear y simular redes que serán de mucha ayuda en un entorno educativo o a nivel corporativo[12].

Tiene como característica principal que las configuraciones realizadas en una emulación pueden llegar a ser implementadas en una estructura física sin la necesidad de realizar grandes cambios, además MiniNet es una solución que está disponible de forma gratuita, además se puede disponer del código fuente[42].

2.2.13. MiniEdit

MiniEdit es una extensión de MiniNet, que nos permite crear redes de forma sencilla sobre un terminal gráfico alojado en el directorio examples, esta interfaz facilita la creación de redes, realizándose la programación de estas en un segundo plano oculto para el usuario, pese a ello esta plataforma presenta ciertas limitaciones en comparación con todas las capacidades que presenta el propio MiniNet[43].

MiniEdit permite tener una visión general de la red, puesto que muestra los elementos que la forman, por su parte, la ventaja de MiniEdit es que proporciona una visión de la red y hace que el aprendizaje sea más fácil sobre todo para los menos familiarizados con MiniNet[44].

2.2.14. Wireshark

Wireshark se define como un analizador de paquetes en la red, que captura paquetes de datos detallándolos de una forma más precisa, un dispositivo de medición para examinar lo que está pasando dentro de la red, también se distribuye en Licencia Pública General y Licencia de código abierto[45].

La herramienta implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para más de 1000 protocolos soportados, teniendo una interfaz intuitiva y sencilla permitiendo observar con facilidad las capas que conforman un paquete, entendiendo en si la estructura de los protocolos[46].

2.3. Marco Teórico

2.3.1. Implementación de redes SDN sobre redes convencionales en empresas

Tiempo atrás esta separación era increíble, sin embargo desde ese momento se empezó a fomentar en gran cantidad y variedad algunos dispositivos que pueden hacerlo, las redes no SDN o la ingeniería convencional era hasta ese momento la más fresca y satisfacía su capacidad de una manera correcta, sin embargo desde la llegada de SDN, la innovación empezó a seguir un camino alternativo, han pasado algo más de 10 años desde que se empezó a crear este tipo de innovación concentrada, esto es totalmente ideal ya que poco a poco las organizaciones y asociaciones están empezando a ver más interés en este tipo de innovación para aplicarla[47].

Hay grandes organizaciones que han apostado proactivamente por un ajuste de su plan de organización e ingeniería, y ahora mismo cuentan con este tipo de innovación en sus asociaciones, entre estas organizaciones se encuentran Google, IBM, Microsoft, Cisco, Tech Mahindra[48].

Debido a la multitud de cambios que ha experimentado la innovación en los últimos tiempos, se podría decir que las SDN influyen en mayor medida en las grandes empresas debido a su capacidad de atracción en las configuraciones unificadas, lo que se traduce en menos costes de ejecución y mantenimiento, además, las SDN han despertado un extraordinario interés como objeto de estudio y mejora en diferentes áreas de la industria[49].

El diseño de estos dos tipos de redes es totalmente inesperado, a pesar de satisfacer una capacidad similar, se tiende a notar que la construcción funciona de manera diversa entre los dos tipos de arquitectura.

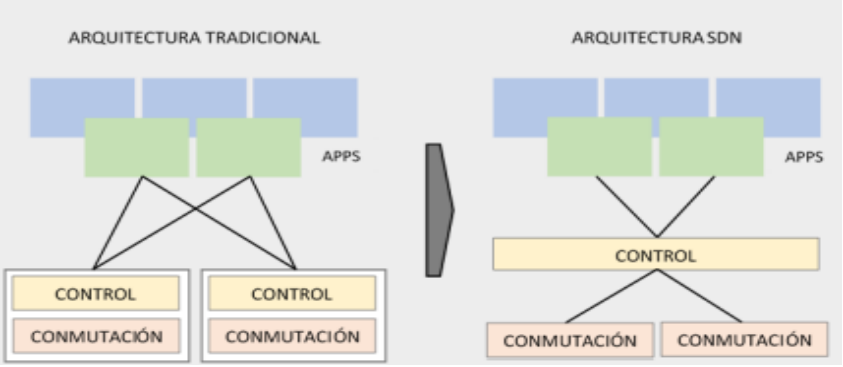


Figura 5. Arquitectura de redes tradicionales y redes SDN. [50].

Notamos en la figura que las redes convencionales se asocian particionando el plano de control, en consecuencia, los diseños deben ser individuales, mientras que la redes SDN se asocia de una manera más reunida.

2.3.2. ¿Aumenta las SDN la operatividad de la red en organizaciones?

SDN dispone de una infraestructura programable, por ejemplo, la posibilidad que ofrecen hoy en día los gadgets y diversas infraestructuras de programar y aplicar código programable a toda la infraestructura, sin SDN, la estructura de la red normal se describe como muy inflexible, ya que los dispositivos incorporan un sistema de trabajo que, por lo general, es restrictivo, con las SDN, todo el sistema organizativo puede personalizarse utilizando lenguajes de programación[51];

Son administrados centralizadamente, esto es fundamental debido a que la metodología normal enreda la red de un numero de dispositivos a medida que la organización aumenta de tamaño, ya que cada dispositivo debe colocarse físicamente y debe aplicarse la configuración de VLAN o las convenciones de dirección, aunque con una base concentrada es posible obtener una optimización dinámica y rápida[52].

La automatización en las redes realmente pretende que después de personalizarse con precisión y funcionar por su cuenta cuando haya una ocasión, pueda responder con astucia a las tareas preestablecidas que se le han encomendado, lo que con una red convencional podría requerir unas horas de trabajo en cambio con la automatización con SDN hay fondos de reserva de tiempo para la junta, ya que se ejecuta en un segundo plano[53].

Las SDN funcionan con código abierto, Open Source como se le conoce ordinariamente, lo cual es un buen beneficio ya que considera al comerciante no partidista, por ejemplo no están apegados a un vendedor similar, sin embargo pueden colaborar con varias marcas de dispositivos para ser compatibles[54].

2.3.3. ¿Por qué apostar por las redes SDN?

La necesidad de nuevas opciones y actualizaciones de la red actual para adaptarla a las necesidades futuras en una organización, se refiere a satisfacer los requisitos previos de comunicación de los medios de telecomunicaciones del público mundial es sin duda un gran reto para las redes tradicionales, de este modo, las ramas de TI de un sinfín de organizaciones y cooperativas de servicios en redes han empezado a destinar recursos a la utilización de las redes existentes[55].

Según Punt Informatic [56], este tipo de redes presentan una serie de ventajas interesantes para cualquier usuario u organización independiente, entre las que se incluyen las siguientes:

Flexibilidad: Son más adaptables por el hecho de que cuando una organización involucra la virtualización para su estructura de red, esta se puede ajustar a los diversos requerimientos de esta sin necesidad de adquirir nuevo hardware o gadgets, lo principal que se debe hacer es una reinvención del producto para que la organización refresque los avances realizados, las SDN tienen una administración concentrada y menos compleja, de igual manera se vuelven más efectivas que las redes con diseño convencional por el hecho de que su organización o los ejecutivos son de un punto similar, lo cual simplifica las cosas.

Ahorro de costos: En contraste con las redes de diseño convencional, las SDN por su administración unificada no necesitan gastos significativos, y esta es una de las ventajas por las que más personas y organizaciones se están decidiendo por el cambio de una organización habitual a una SDN.

Automatización: Debido a la deliberación de los planos de control e información, las SDN permiten un ajuste eficaz de la carga y la dispersión del tráfico para evitar la obstaculización de los puntos focales, lo que fomenta una mejor ejecución y utilización. Además, el establecimiento y diseño de estas redes están programados, lo que reduce los costes funcionales y de soporte, al tiempo que mejora las capacidades que se han introducido recientemente.

Seguridad: Las SDN se vuelven más vigorosas con la mecanización, asimismo desarrollan aún más la seguridad, ya que el envío de esta organización en marco hace que sea más sencillo determinar cualquier tipo de molestia desde un plano de control concentrado más rápido que las redes habituales así, uno de los puntos fuertes de este tipo de redes es que proporcionan seguridad con una precisión extraordinaria en aplicaciones, puntos finales y dispositivos BYOD, algo que una ingeniería de redes convencional sencillamente no puede ofrecer.

Utiliza Cloud Computing: Tal vez de la mayor transformación en la innovación es el almacenamiento distribuido, por lo que las organizaciones están empezando a ser entusiastas en la actualización de sus infraestructura con esta ayuda, para ello el diseño

debe ser virtualizado y supervisado a medio camino para que las nuevas administraciones se pueden establecer en la parte superior de la red[56].

Por su adaptabilidad y versatilidad, este tipo de redes permite a las organizaciones crear y transmitir aplicaciones y administraciones en un par de días en lugar de semanas o meses, que es lo que regularmente se tardaría en caso de aplicar una red con diseño habitual y, como es de conocimiento, la velocidad es lo más estimado en el negocio, la mayoría de las organizaciones buscan que sus estrategias se hagan en un tiempo base, para ellos la mejora del equivalente es clave e imperativa, lo que hace que sea profundamente solicitada por las asociaciones[57].

2.3.4. ¿En dónde aplicar redes definidas por software?

Teniendo en cuenta los amplios beneficios que existen en las redes SDN en contraste con las redes de diseño convencional, Digital Guide[58], hace referencia a las situaciones potenciales en las que se pueden introducir este tipo de redes:

Calidad de servicio (QoS): Es el control focal de todos los hubs de la organización, da simplicidad al director de la organización para saber cuánta velocidad de transferencia es utilizada por una asociación solitaria, con el objetivo de que pueda dar una reacción rápida. además, controla el tráfico de transporte de información para proporcionar a todos los miembros la velocidad de transferencia vital de forma constante.

Gestión de dispositivos: La aplicación de una tecnología uniforme, como OpenFlow, convierte a SDN en una respuesta con resultados extraordinarios cuando se utilizan terminales de distintos fabricantes en una.

Amplificación de las funciones de la red: La autonomía dada por la innovación SDN, además, se dirige a un acuerdo excelente en situaciones en las que las capacidades de la organización pueden ser alcanzados en cualquier momento y sin problemas, es más, la independencia de los productores de equipos se convierte en un beneficio concluyente para el cliente.

Enrutamiento de paquetes controlado por aplicación: Las SDN ofrecen el alojamiento fundamental para que las aplicaciones externas descubran cómo participar en la dirección de paquetes, por ejemplo, para alterar y cambiar los conmutadores de

la organización, la situación ideal para ello es que la unidad de control tenga el punto de conexión de comparación.

Políticas de seguridad: Esencialmente son dispuestas por la unidad de control focal, las mismas que permiten enviar reglas de seguridad a los switches de la organización de manera efectiva, las SDN trabajan con una convención OpenFlow, hay algunas que son viables con ellas y otras que son etapas que agregan aplicaciones en el entorno de la nube[58].

2.4. Requerimientos

A continuación, se muestra la tabla de requerimientos analizados para el desarrollo de este proyecto:

N.º	REQUERIMIENTOS	DESCRIPCIÓN
1	No se utilizará equipo de hardware	La propuesta estará desarrollada en un entorno de simulación desde virtual box.
2	Disponibilidad de espacio para Floodlight	Se requiere una máquina virtual para la instalación de Floodlight con 8GB de almacenamiento y 2GB de RAM
3	Conexión tipo adaptador puente	Deberá funcionar como adaptador puente para hacer uso de la red física con dirección IP asignada por el router.
4	Actualización de MiniNet en Floodlight	Mantener actualizado la herramienta de MiniNet dentro del controlador Floodlight para un mejor manejo.
5	Activación del servicio http de Floodlight	Para observar el plano de control de Floodlight se debe activar el servicio Http que por defecto ya viene instalado en la máquina virtual.
6	Diseño de topología de red	Se usará la herramienta de MiniEdit para desarrollar la estructura de red SDN a implementarse de acuerdo con los recursos de la institución.
7	Implementación de red SDN	Una vez diseñada la estructura de la red SDN, se procede con la creación de la red mediante comandos en MiniNet.
8	Reglas de control de acceso	Realizar las respectivas denegaciones entre hosts para evitar la conexión y visualización de equipos remotos entre sí.
9	Conectividad entre hosts	Se deberá verificar las conexiones entre los hosts, para comprobar la comunicación entre ellos mismos, aparte de los hosts que tienen establecidos con las reglas de control de acceso.

10	Medición de ancho de banda	Verificación de transferencia existente entre hosts transcurridos en segundos para determinar el ancho de banda
11	Medición de transferencia de paquetes	Realizar pruebas de transferencia de paquetes con el controlador Floodlight y sin el controlador.
12	Análisis de tráfico del protocolo ICMP	Capturar el tráfico ICMP que se genera entres los hosts con conexión y sin conexión.

Tabla 4. Tabla de requerimientos

2.5. Componentes de la propuesta

2.5.1. Aplicación de las etapas del ciclo de vida de una red del modelo PPDIOO

2.5.2. Etapa de planificación

"Se analizan nuevas tecnologías y se determina la forma en que se pueden desarrollar para su uso en la red de la empresa", [59]. Para ello, se procederá a recopilar los datos fundamentales sobre los activos necesarios a obtener, así como los activos que el establecimiento necesita a partir de ahora para evitar gastos significativos a la hora de montar la red, también se determinará cuál es el método más eficaz para llevar a cabo el proyecto teniendo en cuenta la estructura de la red establecida, si comenzar otro diseño con los avances elegidos o construir un estructura mixta entre la innovación habitual de la red o los nuevos avances de la redes.

Los dispositivos que actualmente posee la institución funcionan de manera correcta y estable dentro de su infraestructura, la maquina donde se situará el controlador será en el departamento de Inspección, los dispositivos se comunicaran con el controlador de red que permitirá el envío de datos para el correcto desarrollo de las operaciones de toda la institución.

Los dispositivos que la institución contienen son:

1 ROUTER	**UBICADO EN EL DEPARTAMENTO DE INSPECCIÓN**
1 SWITCH	En el departamento Financiero – Tiene 16 interfaces
6 COMPUTADORAS	1 en el departamento Inspección – Con 8Gb de RAM – Disco de 480 SSD, Disco externo de 1Tb HDD

	– Procesador Intel Core i3 – Windows 10 Pro 1 en el departamento Rectorado – Con 4Gb de RAM – Disco de 1Tb HDD – Procesador Intel Core i5 – Windows 10 Pro 1 en el departamento Vicerrectorado – Con 4Gb de RAM – Disco de 1Tb HDD – Procesador Intel Core 2 Duo – Windows 10 Pro 1 en el departamento Secretaría – Con 8Gb de RAM – Disco de 1Tb HDD – Procesador Intel Core i3 – Windows 10 Pro 1 en el departamento Financiero – Con 6Gb de RAM – Disco de 240 SSD, Disco externo de 500 Gb HDD – Procesador Intel Core i3 – Windows 10 Pro 1 en el departamento Medico – Con 4Gb de RAM – Disco de 1Tb HDD – Procesador Intel Pentium – Windows 10 Pro

Tabla 5. Dispositivos de la institución

Cuadro comparativo de controladores SDN

Características	Floodlight	ONOS	Opendaylight
Versión OpenFlow	Soporte OpenFlow: 1.0, 1.1, 1.2, 1.3, 1.4, 1.5	Soporte OpenFlow: 1.0, 1.3, 1.4	Soporte OpenFlow: 1.0, 1.3, 1.4
Interfaz	Web Gui, CLI	Web Gui, CLI	Web Gui, CLI
Licencia	Apache 2.0	Apache 2.0	EPL v1. O
Lenguaje	Java	Java	Java
Documentación	Muy buena	Muy buena	Muy buena
<Distribuido / Centralizado	Es centralizado	Es de distribución plana	Es de distribución plana
Consistencia	Ninguno	Muy alta	Muy débil
Seguridad	ACL Firewall Autenticación Autorización Detección de anomalías VLAN Recuperación de redes	Recuperación de fallos	Autenticación Autorización Limitación de red
Sistemas Operativos	Linux, MACOS, Windows	Linux, MACOS, Windows	Linux, MACOS, Windows
Código abierto	Si	Si	Si

Tabla 6. Comparación de los controladores SDN.

En la tabla se muestra las características de cada controlador, analizados en esta propuesta, en lo que se hace una comparación para definir cuál será utilizado de acuerdo a los recursos de softwares de la institución. Dando como resultado, la utilización del controlador de Floodlight, debido a que cumple con todos los requisitos para la implementación de la red SDN y se ajusta con los requerimientos de la institución Unidad Educativa Americano.

Para la instalación de Floodlight, tendrá que ser un equipo con características robustas, que será establecido como controlador, deberá contar mínimo con, 8Gb de RAM,

procesador Core i3, para que funcione debidamente y pueda ser de base para la implementación de la red que se será diseñada bajo las etapas del modelo PPDIOO.

2.5.3. Etapa de diseño

En esta etapa se plantea el diseño de red SDN para su virtualización, que resulte más adecuada a la estructura actual de la institución, también se pensará el tipo de topología más idónea que tendrá el diseño de la red.

Se hará una comparación entre la red tradicional de la institución con la red SDN, indicando las ventajas y desventajas de cada una, con la conclusión adecuada. Como resultado final se espera que, al incorporar nuevos hosts en la red definida por software, tengan comunicación entres si, asemejándose a una red física.

Topología

Los equipos informáticos están formados por diferentes dispositivos y la topología es la forma en que los dispositivos o equipos de la red están interconectados[60]. Actualmente hay diferentes tipos de topologías de redes, donde cada institución tiene definida de acuerdo con sus recursos de infraestructura, todas las topologías funcionan debidamente, sin embargo, carecen de problemas al momento de aumentar más equipos a la red, al haber problemas de latencia, conexiones fallidas, perdidas de paquetes o equipos averiados.

Por esto al tratarse de redes SDN, todos los hosts deben estar comunicados entre sí para que el controlador elija la forma más idónea de enviar paquetes y deje esta vía establecida para futuros envíos.

La topología escogida fue analizada de acuerdo a los requerimientos, disponibilidad de equipos y recursos económicos de la institución Unidad Educativa Americano, será de tipo lineal o bus, porque solo cuenta con un servidor, así sus nodos estarán conectados directamente a un único enlace si ninguna conexión entre otros nodos.

Es decir, físicamente cada nodo estará enlazado a un cable, facilitando la comunicación directamente con el controlador, permitiendo así que todos los dispositivos en la red puedan versen y comunicarse entre sí, tomando en cuenta las reglas de control de acceso en caso de algunas restricciones entre un nodo con otro nodo en la red.

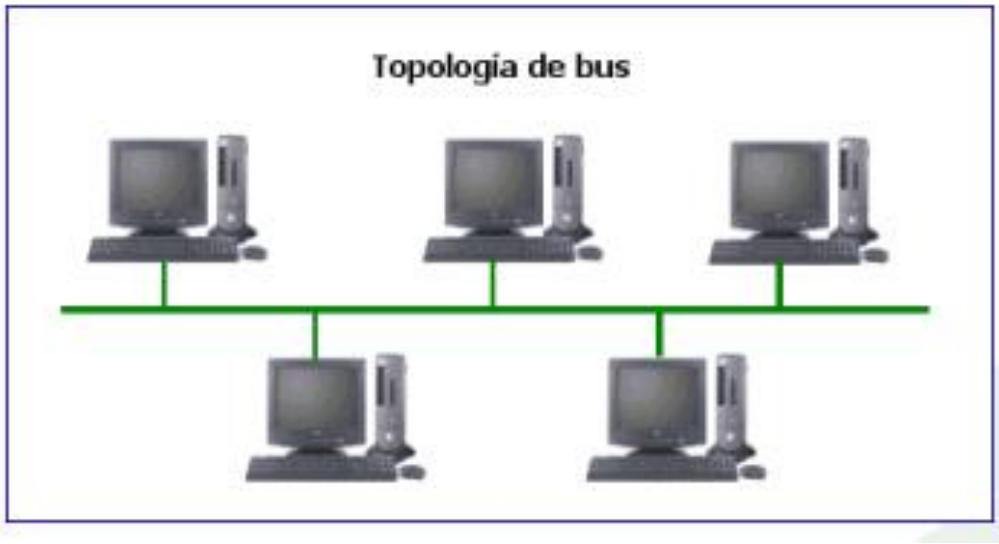


Figura 6. Topología de red tipo lineal. [61].

Instalación y configuración de las herramientas para el diseño de la SDN

Instalación del software Oracle VM VirtualBox

Se procede a abrir el archivo descargado de la página oficial de VirtualBox

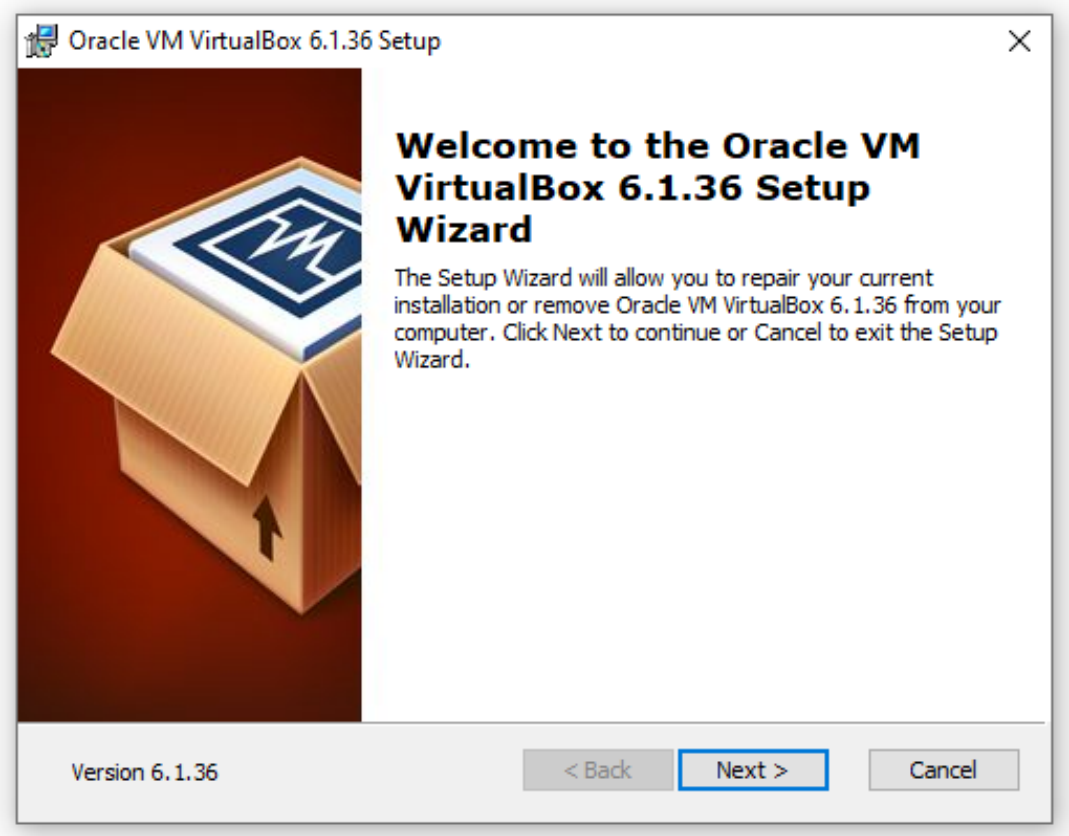


Figura 7. Instalación de Oracle VM VirtualBox

Una vez instalado Oracle VM VirtualBox en el equipo donde estará situado el desarrollo de esta propuesta, se crea una maquina con el nombre de Floodlight asignando el sistema operativo de Linux versión Ubuntu 64bits.

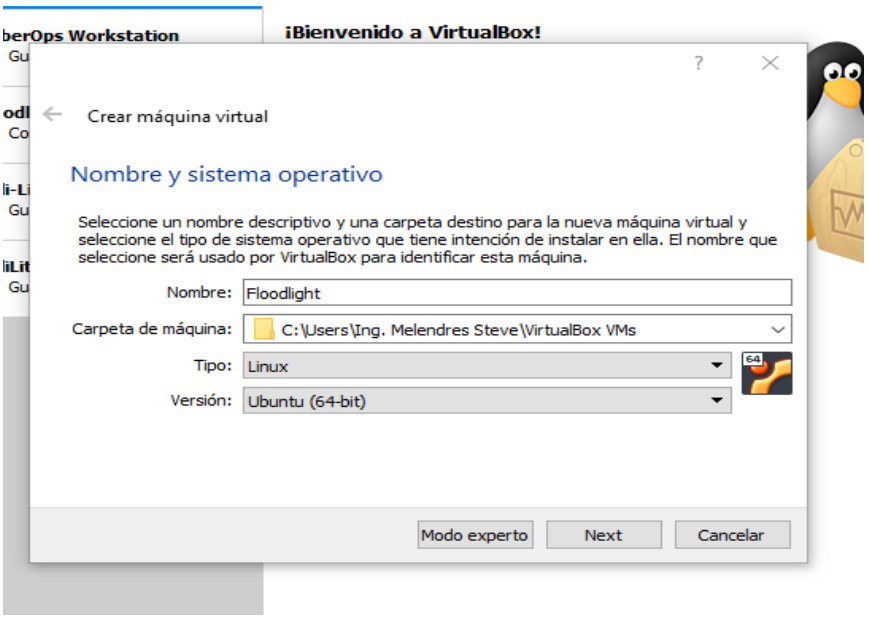


Figura 9. Creación de la máquina virtual Floodlight

Asignamos la cantidad de memoria RAM que tendrá el controlador, el cual se utilizará 2 GB de RAM para esta propuesta.

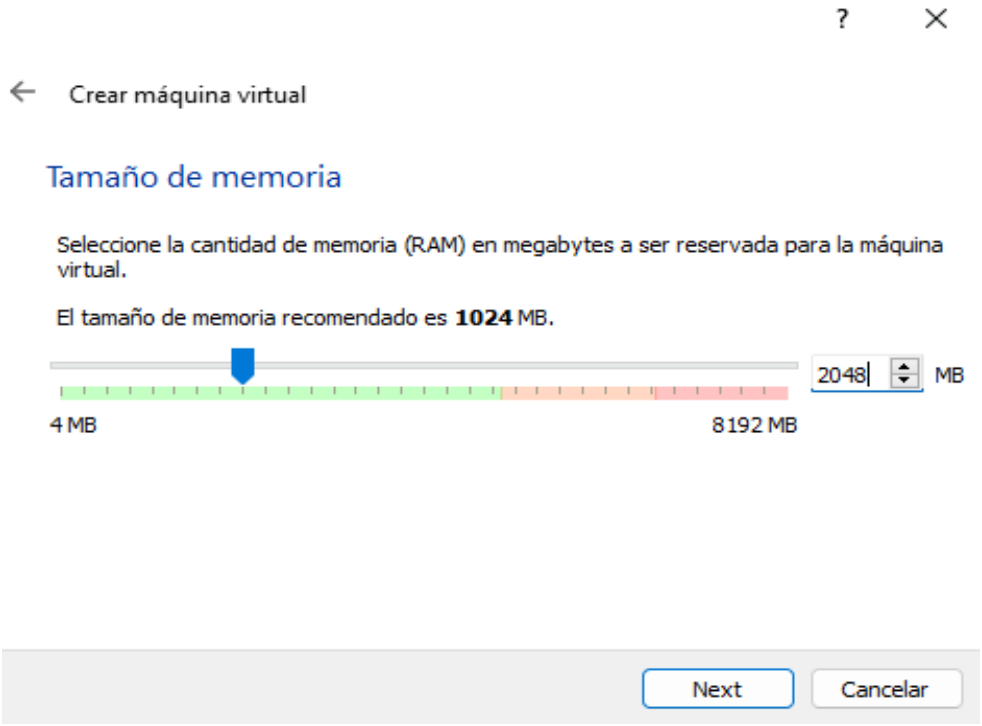


Figura 10. Fijando el tamaño de memoria RAM en Floodlight

Agregamos Floodlight Controller a través de su archivo .vmdk, descargado de su página oficial:

https://floodlight.atlassian.net/wiki/spaces/floodlightcontroller/pages/8650780/Floodlight+VM.

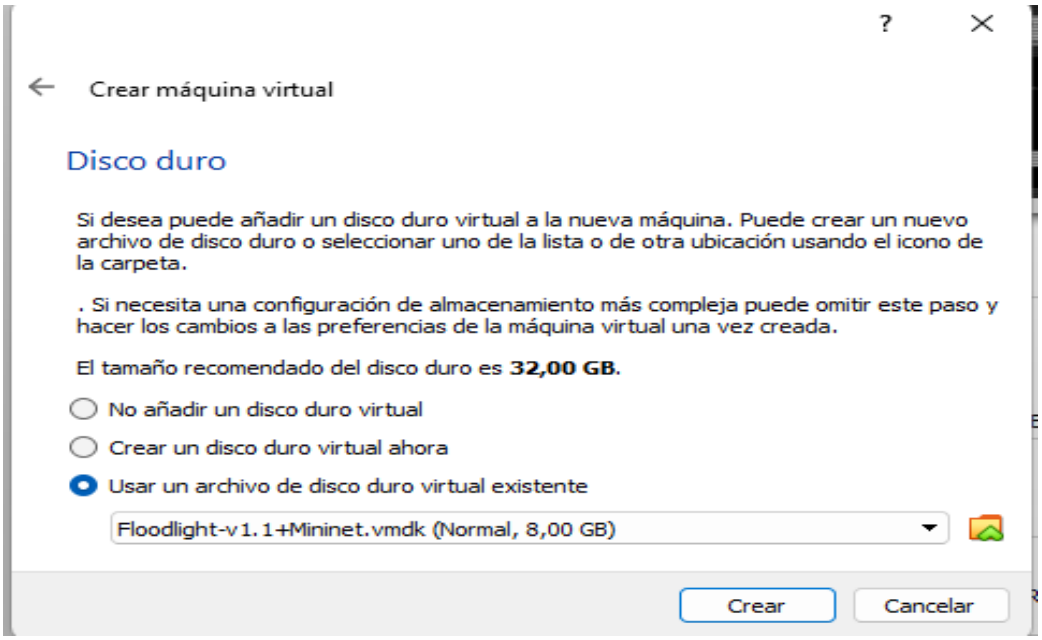


Figura 11. Asignación del tamaño en disco para Floodlight

Ya creada la máquina virtual, se deberá configurar como adaptador puente para que se conecte al dispositivo central que será de uso para esta propuesta.

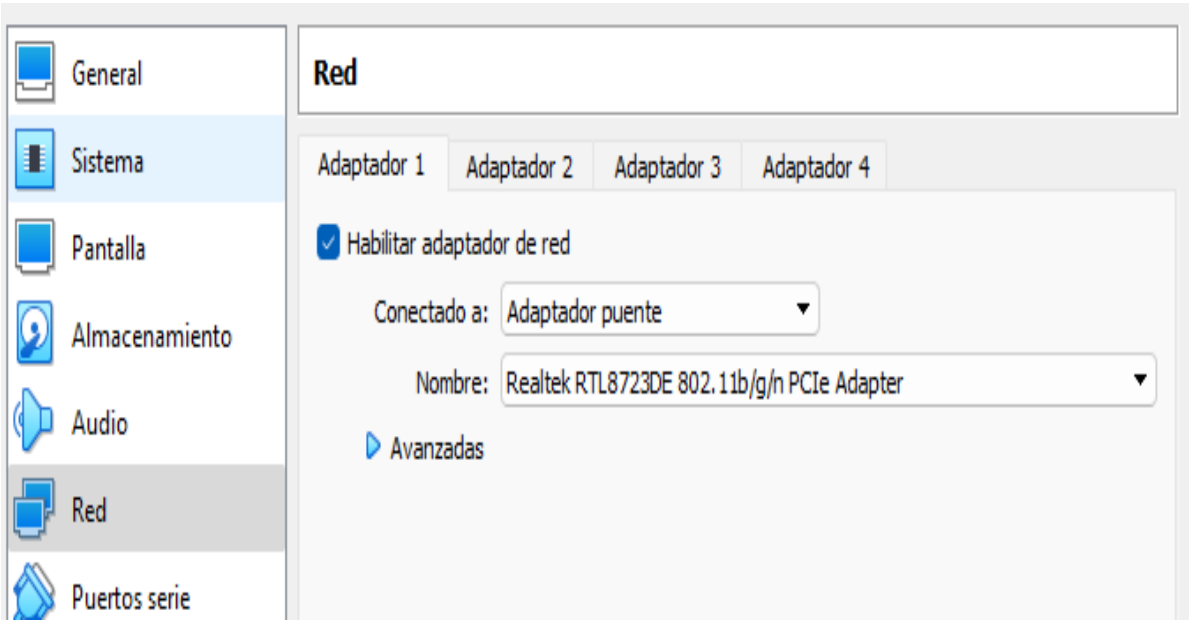


Figura 12. Asignación de red de Floodlight como adaptador puente

Por último, se inicia la máquina virtual ingresando con la contraseña default **Floodlight** y se verifica que la maquina este con una dirección IP de la red Central y no una IP default.

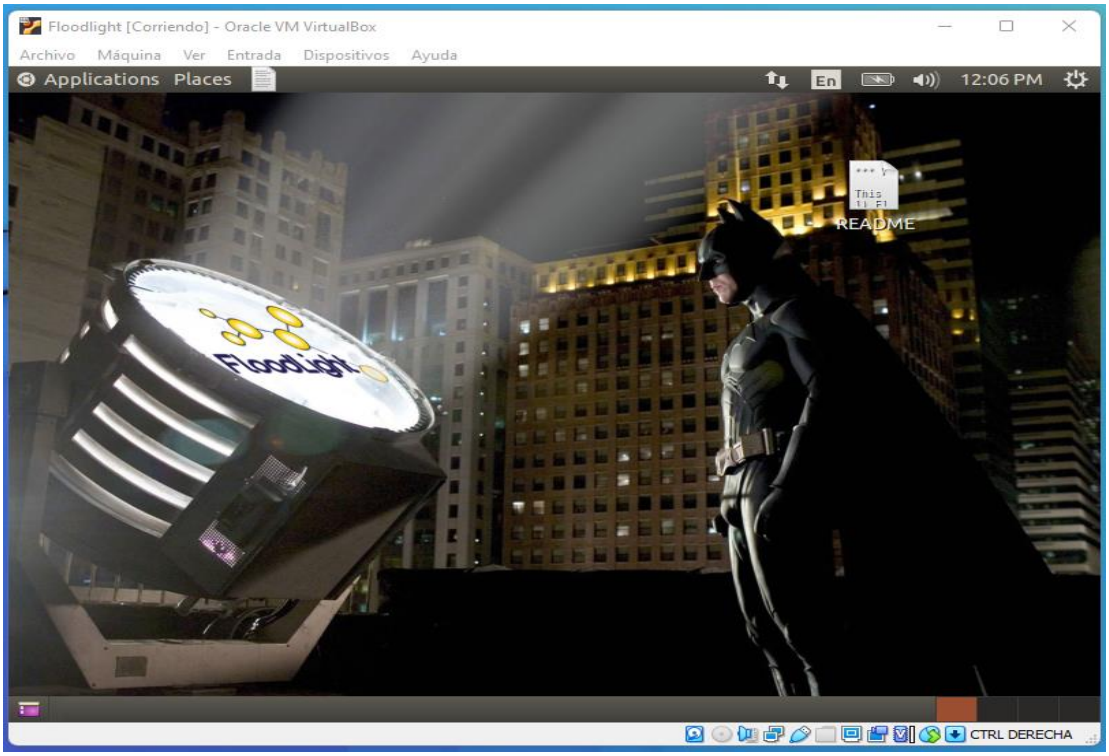


Figura 13. Pantalla de inicio de Floodlight

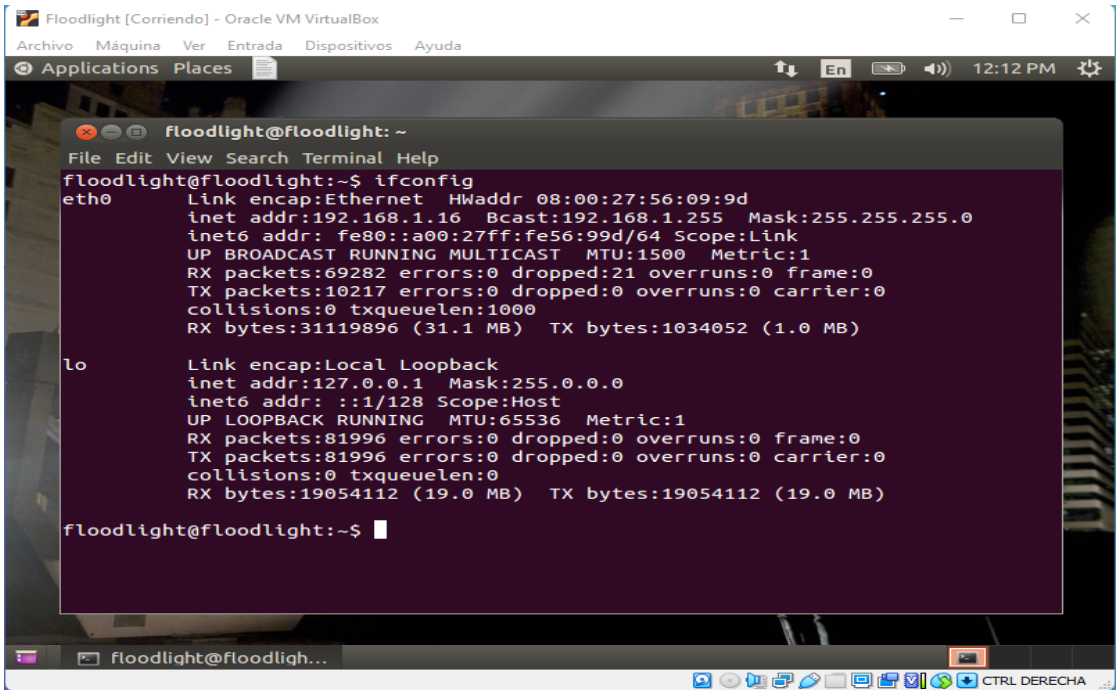


Figura 14. Verificación de IP como adaptador fuente en floodlight

Instalación de MiniNet en el controlador Floodlight

Floodlight ya incorpora esta herramienta, pero para su correcta instalación se deben realizar los siguientes pasos:

1) Es importante realizar una actualización de todo el framework del S.O UBUNTU, con el que se utilizará para esta propuesta. Para continuar con esta actualización se utilizarán las órdenes o comandos adjuntos en el terminal:

```
floodlight@floodlight:~$ sudo apt-get update
floodlight@floodlight:~$ sudo apt-get upgrade
floodlight@floodlight:~$ sudo apt-get dist-upgrade
```

Figura 15. Comandos de actualización para Ubuntu.

2) Terminada la actualización continuamos con la descarga e instalación del software Git, el cual permitirá descargar archivos en código fuente situados en repositorio, con el comando siguiente:

```
floodlight@floodlight: ~$ sudo apt-get install git
```

Figura 16. Instalación de Git a través de comando.

3) Descargamos el software de MiniNet a continuación con el comando:

```
floodlight@floodlight: ~$ git clone https://github.com/mininet/mininet.
```

Figura 17. Descarga de MiniNet

4) El comando anterior crea una carpeta alojada en el directorio “Home” de Ubuntu, nombrada como “MiniNet”, el cual está contenida por archivos y carpetas fundamentales para su correcta ejecución.

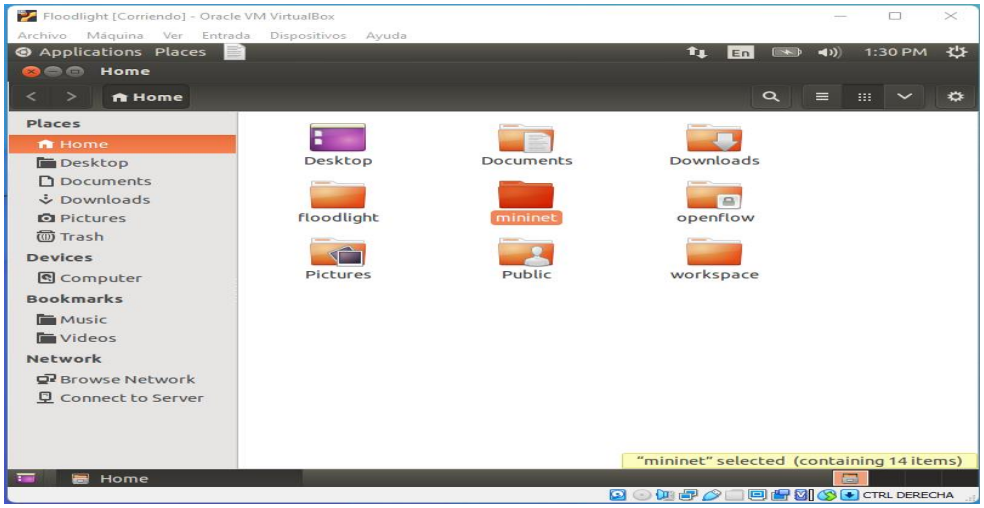


Figura 18. Instalación de MiniNet

5) El comando a continuación se ejecuta para comprobar la instalación correcta del software, el primero añadirá el controlador y hosts, el segundo mostrará si la conexión entre ellos existe:

```
floodlight@floodlight: ~$ sudo mn

mininet> pingall
```

Figura 19. Verificación de ingreso y ping en MiniNet.

6) La figura a continuación indica la instalación correcta de MiniNet, mostrando la creación del controlador y sus hosts con conexión.

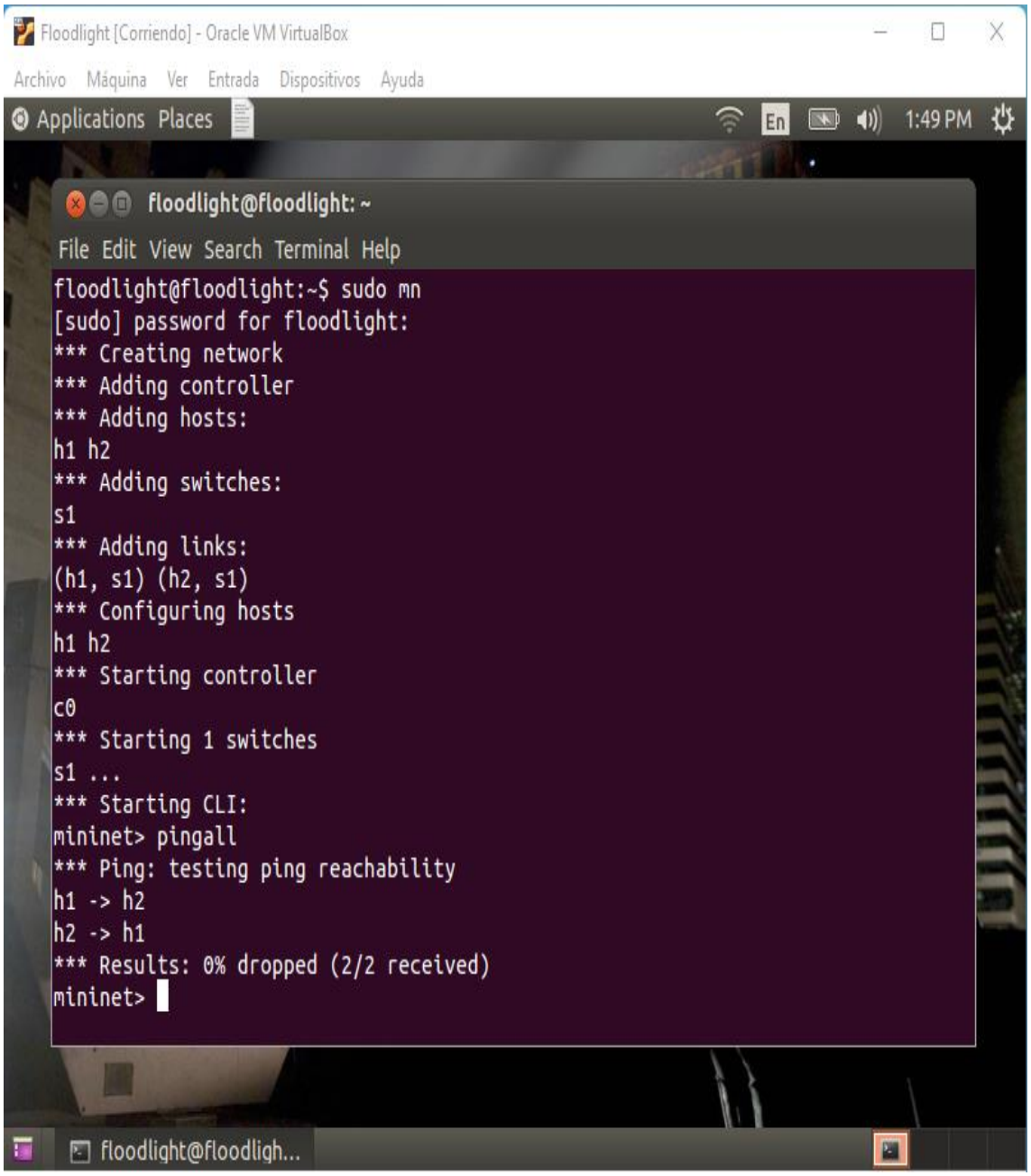


Figura 20. Verificación de instalación correcta de MiniNet

Comandos utilizados en MiniNet

En la siguiente tabla se muestran los comandos empleados en este trabajo de titulación y los más frecuentes en MiniNet.

Comandos	Descripción
Ping	Verifica la conexión de manera remota con otro dispositivo.
Ifconfig	Muestra la información base de la red.
Pingall	Muestra la conexión entre todos los dispositivos existentes en la red.
Xterm	Permite abrir un terminal para los dispositivos de forma específica.
Help	Muestra información de los comandos como una ayuda.
Nodes	Muestra los datos de un nodo simulado.
Dump	Muestra detalles como el puerto, dispositivos y datos de dirección IP.
Net	Muestra las conexiones y puertos entre los dispositivos.
Exit	Salir del programa.

Tabla 7. Comandos de MiniNet

Diseño de la red definida por software (SDN)

Para desarrollar el diseño de la red se empleará el controlador Floodlight para el manejo de una red Open Flow el cual estará visualizado en el navegador propio de este controlador, la red estará administrada por mininet y se usará MiniEdit para el diseño gráfico de cómo será la estructura de red a implementarse.

En Floodlight ejecutaremos un terminal para dirigirnos al directorio Floodlight con el comando **cd floodlight/**, luego se digitará el comando **java -jar target/floodlight.jar** para levantar los servicios de este controlador que permitirá visualizar, administrar la topología de nuestra red creada.

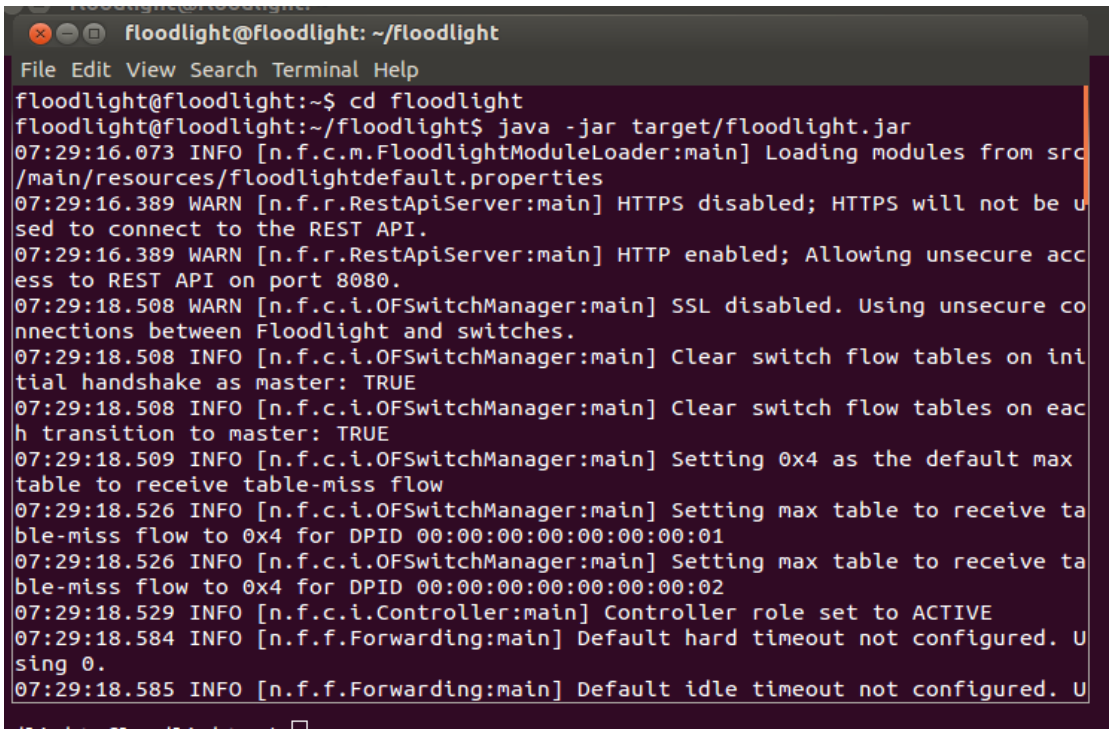


Figura 21.Levantamiento de servicios en Floodlight

En otro terminal abriremos la herramienta de MiniEdit dirigiéndonos al directorio de mininet/mininet/examples digitando el comando **cd mininet/mininet/examples**, ya ingresados al directorio ejecutamos el comando **sudo ./miniedit.py**, se nos abrirá en xming la interfaz gráfica para crear la topología de nuestra red.

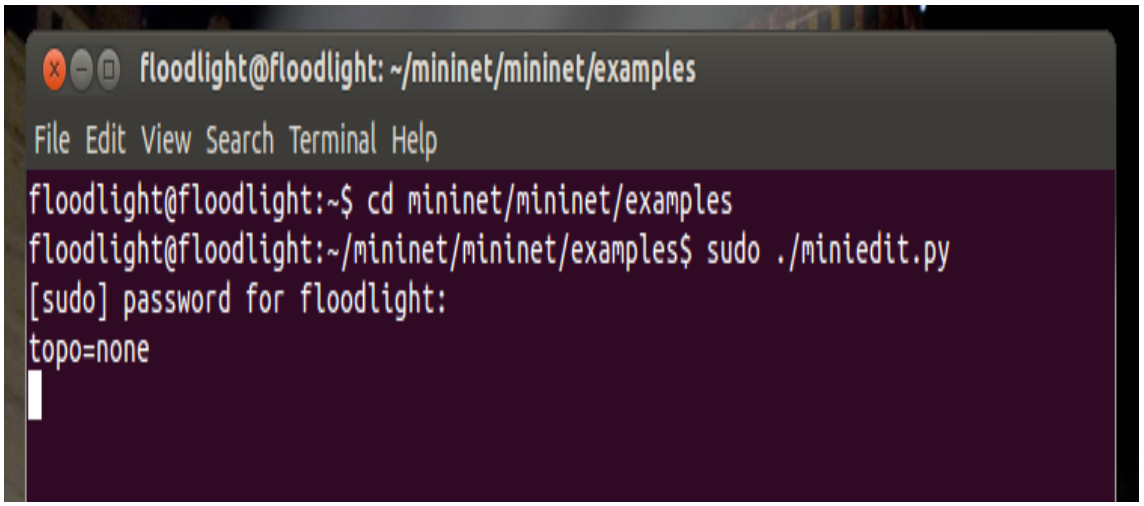


Figura 22. Acceso a la carpeta examples de mininet y ejecución de MiniEdit

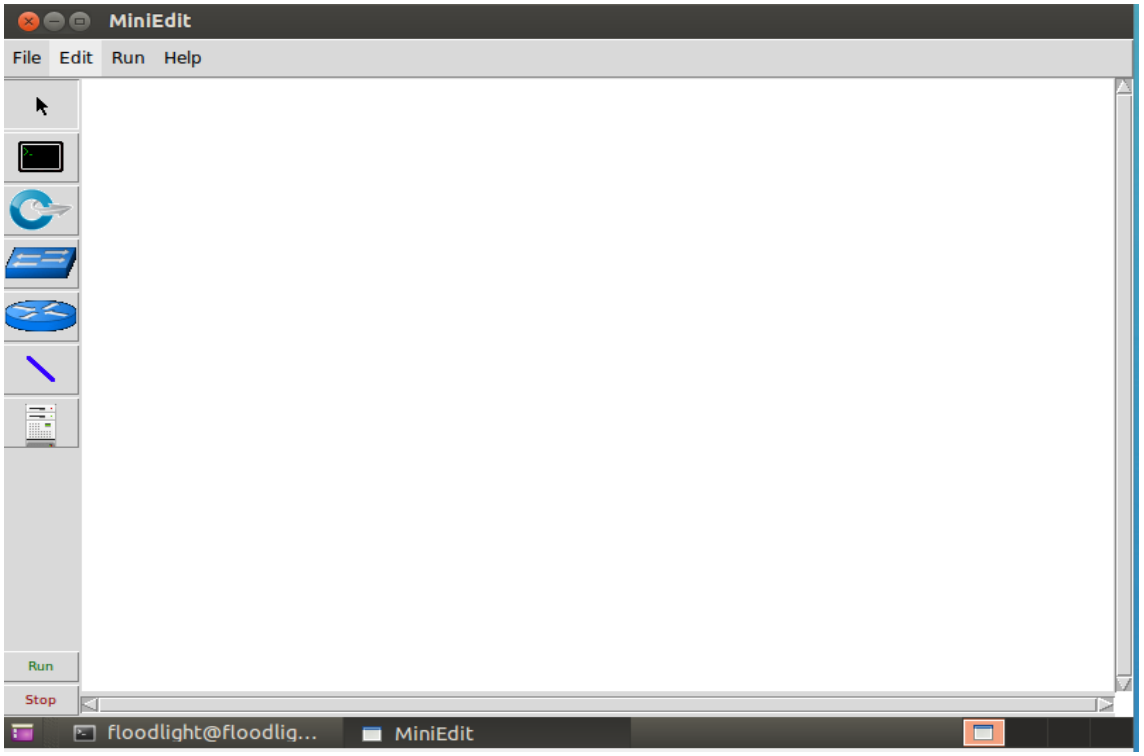


Figura 23. Entorno gráfico de MiniEdit

Una vez ingresado a la interfaz de MiniEdit, empezaremos a realizar el diseño de la red con sus respectivos dispositivos que poseen la institución.

Diseño de la topología de red SDN

En la actualidad existen algunas topologías de redes que MiniNet permite crear, tales como: lineal, malla, árbol, anillo y bus. En unas ya cuentan con su creación defecto en el software, y otras se puede desarrollar de forma manual y sencilla.

Para esta institución la topología escogida es de tipo lineal por motivo de que solo tienen un servidor existente, descartando la idea de incorporar más servidores en el futuro ya que no están en sus planes, sin embargo, la actualización de la estructura de red local que tienen a una estructura de red SDN, les permitirá ser escalable sin ningún problema al momento de incorporar nuevos servidores.

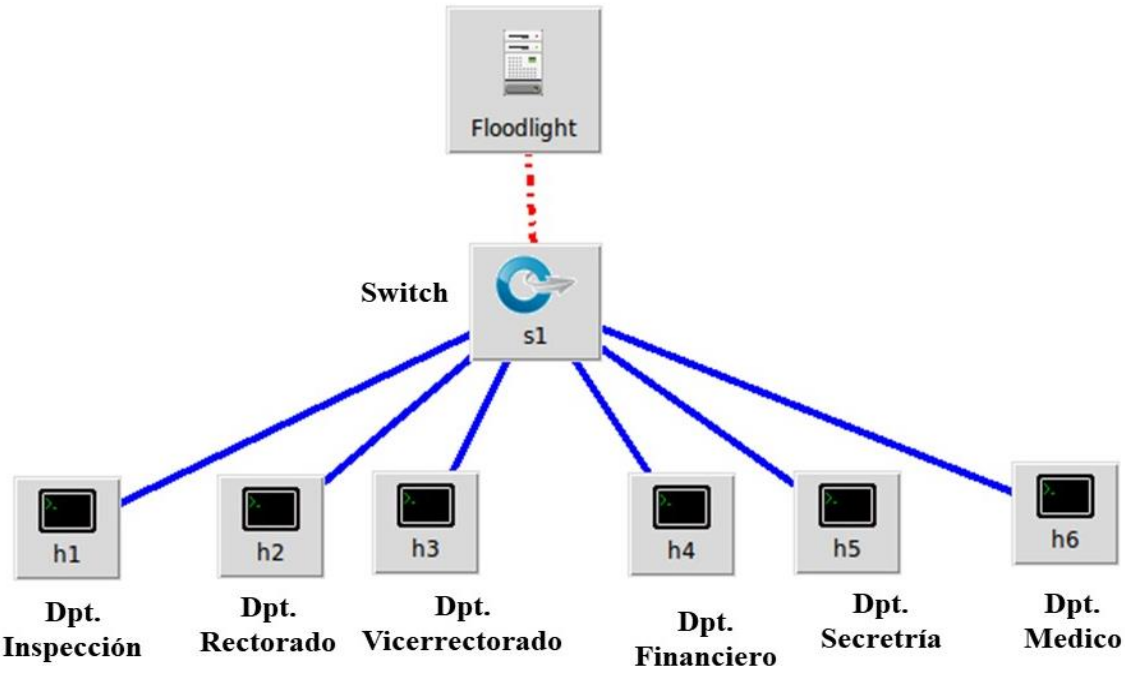


Figura 24.Creacion del diseño de red SDN para la institución

En la figura se muestra el diseño de la topología de la red a implementarse en la institución, así mismo se visualiza seis hosts con el nombre de cada departamento administrativo, los mismo que se encuentran conectados directamente a un switch enlazado al controlador de Floodlight.

Comparación entre estructuras de redes tradicionales y SDN

En esta tabla se muestran las diferencias existentes entre las redes que no son definidas por software y las que sí son definidas por software.

Redes SDN	Redes Convencional
Administración optimizada, rápida y dinámica.	Su administración demanda mayor tiempo y es estática.
Es escalable	No es escalable.
Sus tablas contienen apertura.	No tienen apertura las tablas de flujo
Operatividad centralizada.	Operatividad manual
Compatibilidad con dispositivos y software.	Limitaciones de compatibilidad en dispositivos y software.
Usa automatización	No usa automatización.
Bajos costos de operación	Altos costos de operación.
Accesibilidad por medio del hardware al plano de datos.	Accesibilidad por medio del software al plano de datos.

Tabla 8. Comparación entre SDN y no SDN

La desventaja de implementar redes SDN, es que la gestión de la red se puede hacer por un único controlador y esto hace que, si de algún modo sufriera una fallar debido a problemas físicos o u otros, la red tendría problemas convirtiéndose en una red inservible, hasta que se solucionen, sin embargo, las redes definidas por software, ofrece mucho más que una red convencional.

Asistencia y mantenimiento de una red tradicional

Las redes convencionales involucran un coste desorbitado para construir eficazmente una red , donde los grandes costes corresponden a la obtención de equipos de una red como conmutadores e interruptores, continuados en segundo lugar por los dispositivos que hacen posible esta red, por ejemplo, enlaces de red, ponchadoras, conectores RJ45, analizadores y protectores, en este caso para la Unidad Educativa Americano, se costeó el monto total del mantenimiento y soporte de su red, con una cifra considerada de $2000.

2.5.4. Etapa de implementación

Como la tercera etapa para la elaboración de la propuesta se refiere a la implementación de la configuración de la red en la etapa de **diseño**, con las innovaciones elegidas dentro de la estructura de la red y la investigación de la red tradicional que se llevó a cabo en la etapa de **planificación**.

Desarrollo de la topología lineal

A continuación, se muestra la tabla de direccionamiento IPs, que fueron asignados a los host y controlador, con sus respectivos departamentos, para así tener una buena gestión y control.

Áreas	Nombre	IP	Mac
Dep. Inspeccion - Controlador	H1	10.0.0.1	36:8c:ad:0e:4f:xx
Dep. Rectorado	H2	10.0.0.2	18:22:39:67:4a:xx
Dep. Vicerrectorado	H3	10.0.0.3	32:e5:26:44:2c:xx
Dep. Financiero	H4	10.0.0.4	3e:18:4b:24:80:xx
Dep. Secretaría	H5	10.0.0.5	ac:26:ef:19:52:xx
Dep. Medico	H6	10.0.0.6	62:ad:ef:4c:40:xx

Tabla 9. Tabla de direccionamiento de IPs.

Configuración previa antes de iniciar la simulación

La topología analizada y escogida para esta propuesta, se realizará en MiniNet, que nos facilita la creación de diseño de diferentes topologías adaptadas en el lenguaje Python.

Por último, se utilizarán los datos mostrados anteriormente en la etapa I y etapa II. Para el desarrollo de la topología tipo lineal, para eso se utilizará el siguiente comando en un terminal, el mismo que tendrá configurado el controlador con su puerto **6653**, controlador de tipo **Remote Controller**, protocolo **OpenFlow13**, IP **127.0.0.1**, **6** hosts, **1** switch y su topología **Topo Linear.**

```
sudo mn --topo linear,1,6 --controller=remote,ip=127.0.0.1,port=6653 –switch ovsk,protocols=OpenFlow13
```

Figura 25. Desarrollo de la topología lineal a través de código

El uso de este comando nos dejara añadir los hosts y switches permitiendo la conexión entre sí, al mismo tiempo creara una arquitectura de tipo lineal a través del controlador Floodlight. También se pondrá en marcha la simulación de la topología creada una vez digitalizado el comando.

Simulación de la red SDN

A continuación, se muestra la topología lineal creada a través del comando, ya en proceso de simulación con sus respectivos hosts y enlaces.

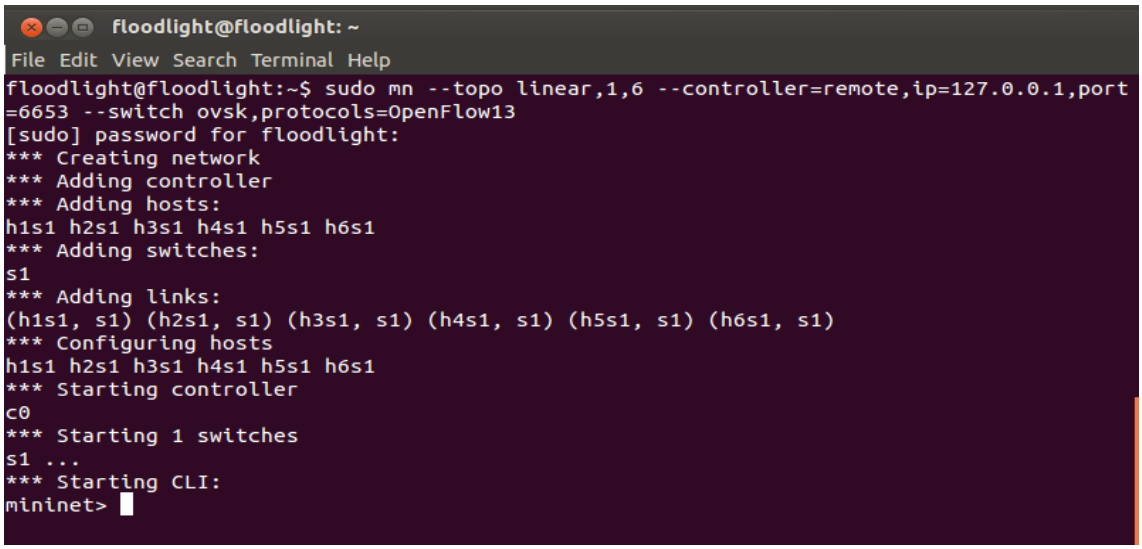


Figura 26. Creación del diseño de la topología lineal de la red SDN

Acceso a Floodlight Controller por el navegador

Para acceder al servidor http de Floodlight para visualizar su interfaz, nos dirigimos a nuestro navegador y colocamos la dirección IP con su puerto establecido para el controlador en este caso **http://127.0.0.1:8080/ui/index.html**, con el fin de ver como se desarrolla Floodlight Controller.

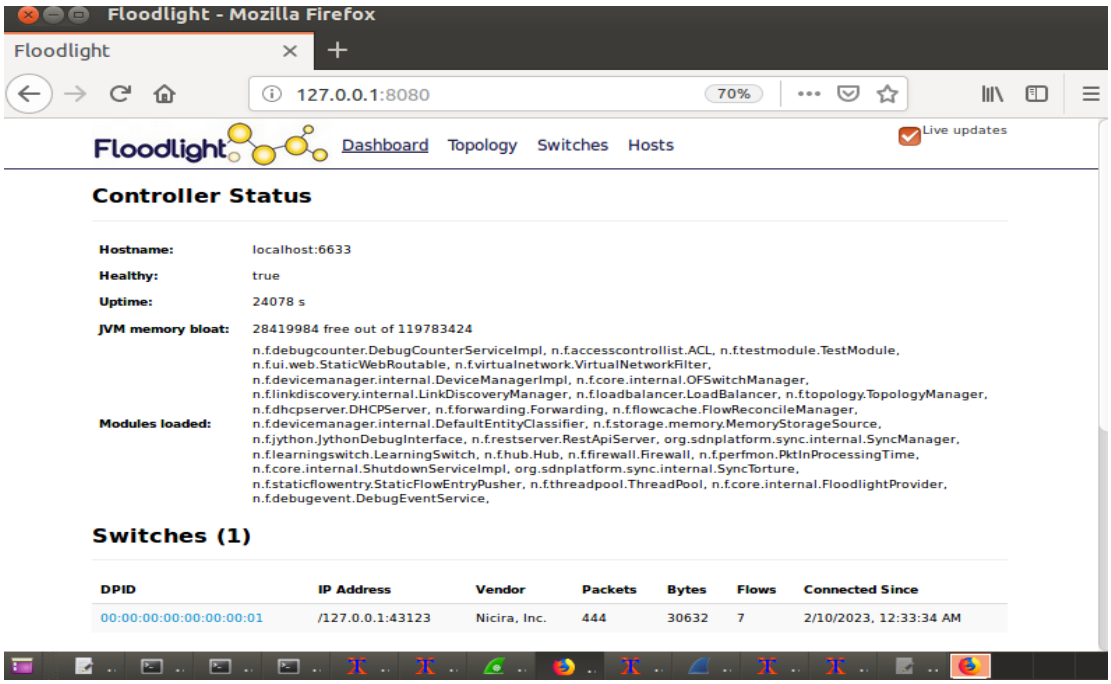


Figura 27. Acceso al servidor http de Floodlight

Muestra una interfaz de usuario desde el principio, donde los controles por parte de personas externas no están hechos, por ejemplo, cualquier persona que no tenga acceso al servidor http de Floodlight, no puede realizar ninguna mejora en la red ni controlar los dispositivos. También se pueden ver cuatro opciones de vista, el primer que es el dashboard que muestra cómo se está desarrollando el controlador y los dispositivos conectados, el segundo que es topology que visualiza la topología de una red de manera vista por Floodlight, el tercero que es switches que presenta los conmutadores que se están ocupando y el cuarto que es hosts que son los hardware o PCs usados en la red.

Dispositivos generados en la red

Al momento de levantar una topología de red, los hosts por defecto no aparecen ni en la opción de ver los hosts, sin embargo, al no visualizarse no significa que no se hayan añadido, solo no se están usando, para hacer que se logre visualizar los hosts creado en la topología de red, se requiere hacer un ping. En este caso se hará el respectivo ping en la etapa de operación.

También se puede observar que los conmutadores si se visualizan en el apartado de switches, en este diseño de red, solo se muestra un solo switch, mostrando la dirección IP, el vendor, los paquetes, los bytes, flows y el registro de fecha funcionarios.

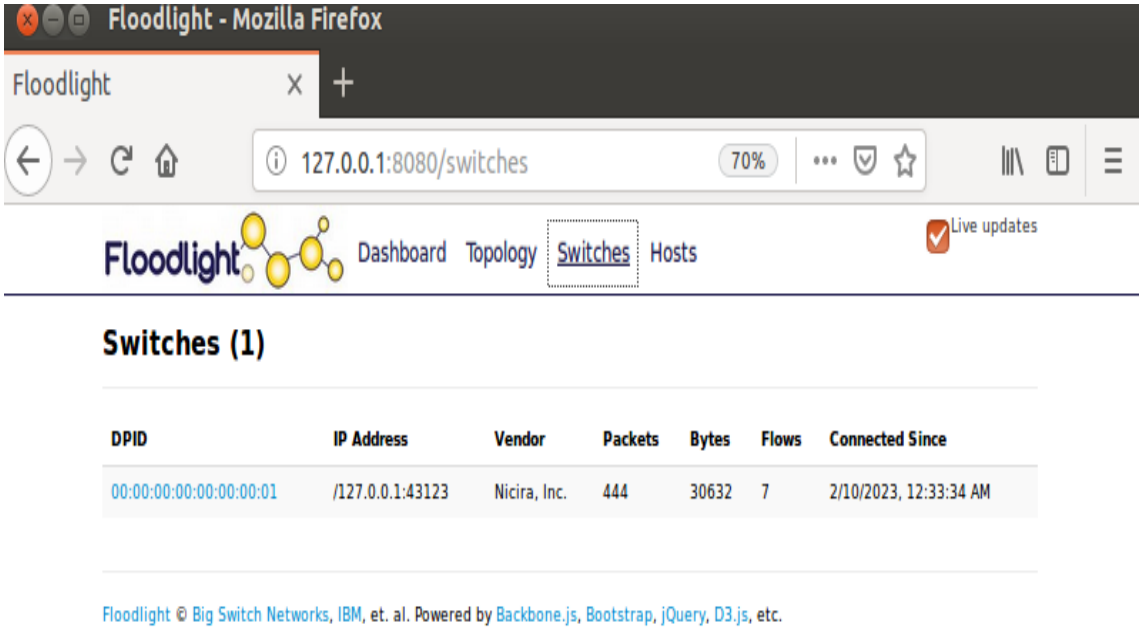


Figura 28. Pestaña de switches usados en el diseño de red SDN

En el apartado de los hosts nos muestran las direcciones MAC, IP Address, que puerto del switch está usando y el registro de conectividad, en este caso no se mostraran los hosts hasta cuando se haga un ping.

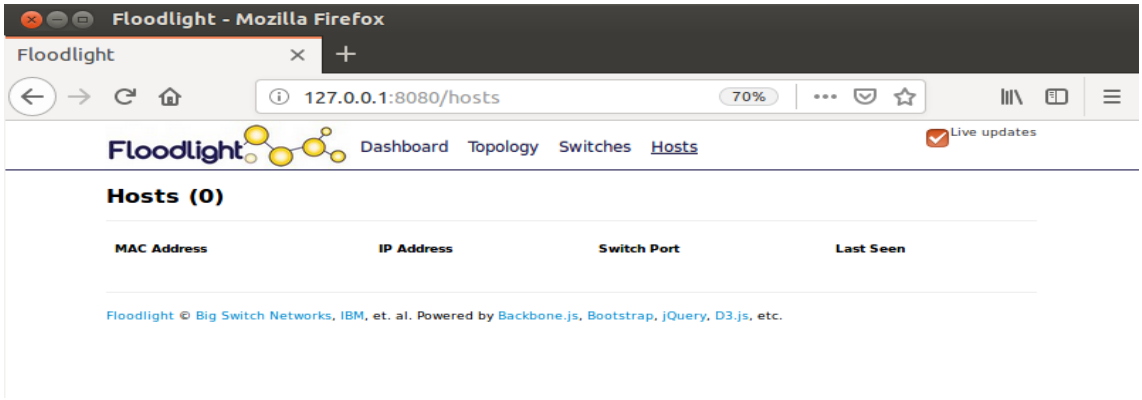


Figura 29. Pestaña de hosts usados para el diseño de red SDN

Topología de red visualizada desde Floodlight

La visualización del diseño de red en la interfaz http de Floodlight, nos muestra el switch utilizado conectado con los hosts visualizados ya realizado un ping con los dispositivos. Por último, se resalta que no es posible realizar cambios en la interfaz de usuario.

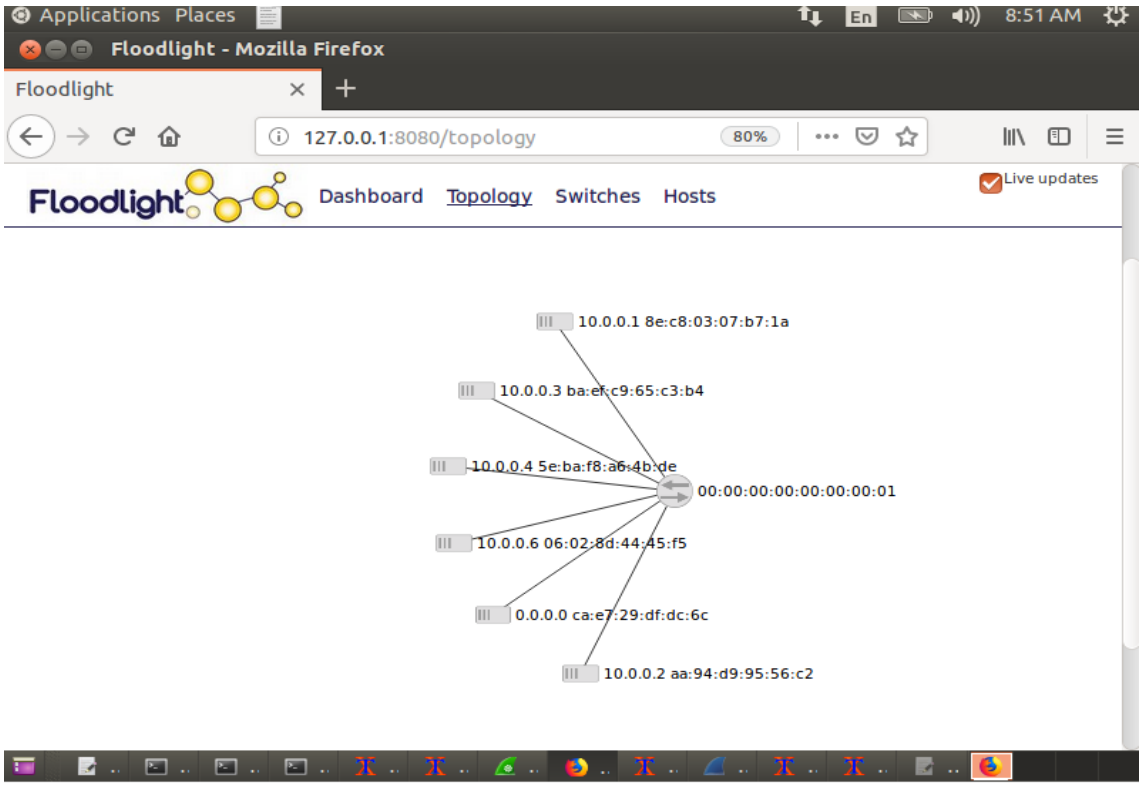


Figura 30. Visualización de topología de diseño de red SDN en la interfaz de Floodlight

Configuración de reglas de control de acceso

Se establece las reglas de control de acceso, para permitir que equipos remotos tendrán conexión y visualización entre sí, las reglas serán configuradas a través de los datos de direccionamiento MAC. Es de importancia analizar quienes tendrán permiso o a que equipo se le negara el acceso, debido a que la topología creada por el comando, dio por defecto que todos los equipos tengan conexión entre ellos.

Es por esto, que se analiza los puntos o estaciones, que no tendrán acceso en la topología diseñada, los cuales fueron los siguientes:

- ✓ H1 sin acceso a H4
- ✓ H4 sin acceso a H1
- ✓ H4 sin acceso a H6
- ✓ H6 sin acceso a H4

Para configurar e implementar estas reglas, se utilizó el comando siguiente

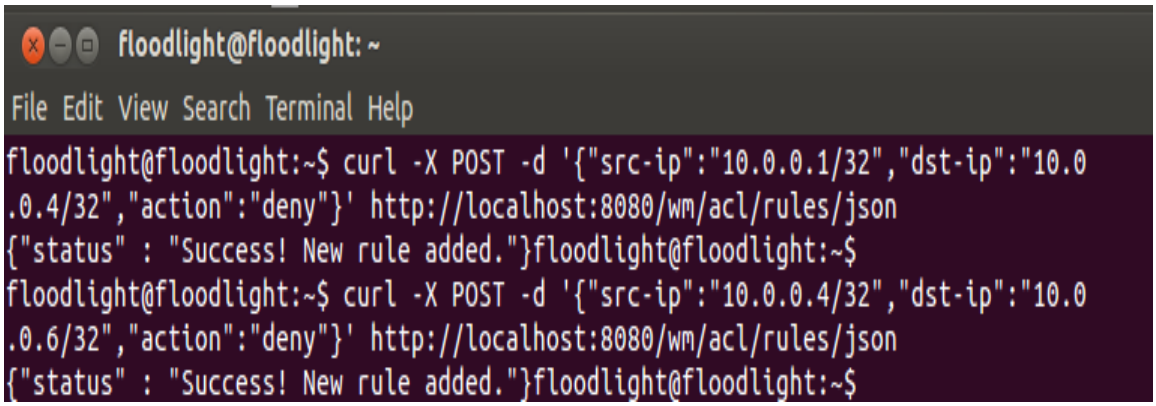


Figura 31. Creación de Reglas de control de acceso

Se observa en la figura, la denegación de acceso de la IP 10.0.0.1 que no tendrá visualización con la IP 10.0.0.4, de la misma forma la IP 10.0.0.4 no se visualizará con la IP 10.0.0.6, es decir, se bloqueara el enlace entre estos dos dispositivos.

De la misma forma, se verifica la correcta creación de reglas de control de acceso, a través del siguiente comando el cual nos permitirá visualizar las reglas creadas.

```
curl http://localhost:8080/wm/acl/rules/json | python -mjson.tool
```

Figura 32. Comando para visualizar las reglas de control de acceso

También podemos eliminar estas reglas una por una en caso de que se presente nuevas restricciones o acceso remoto entre los equipos para pruebas o análisis, y se la deshace con el comando a continuación.

```
curl -X DELETE -d '{"ruleid":"1" }' http://localhost:8080/wm/acl/rules/json
```

Figura 33. Comando para eliminar reglas de control de acceso

2.5.5. Etapa de operación

En esta etapa se realizarán todos análisis posibles, la simulación y los requerimientos necesarios con todos los parámetros anteriores que dará como resultado el trabajo propuesto.

Se asignarán las reglas de control de acceso, se analizará el ancho de banda que tienen entre los hosts, se hará pruebas de transmisión de paquetes con el controlador Floodlight y sin el controlador y por último se inspeccionará con la herramienta de Wireshark el tráfico de paquetes ICMP.

Se pretende demostrar como una red SDN, funciona con la asignación de reglas con control de acceso y sin control, para esto configuraremos la red SDN sin reglas de control de acceso, después se hará otra prueba con control de acceso asignado, así estudiaremos el comportamiento de esta red con las configuraciones establecidas.

En la configuración primaria sin aplicar control de acceso, se espera tener como resultado que los equipos remotos tengan comunicación y se visualizan entre ellos.

En la configuración secundaria se asignó control de acceso, se espera como un resultado el bloqueo de un host con otro, de acuerdo con lo decidido en las reglas de control acceso.

Resultados y análisis sin asignación de control de acceso

Se demuestra la vulnerabilidad que puede existir al no asignar reglas de control de acceso, se realizara a través de una prueba de conexión entre los dispositivos.

En este caso no serán habilitados las reglas. Para la conexión se coloca el comando **pingall** en la consola de MiniNet.

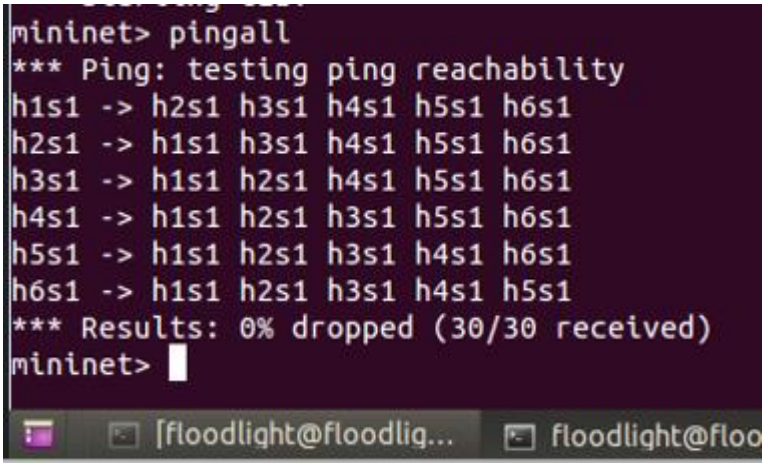


Figura 34. Prueba sin regla de control de acceso

Se observa en la figura, como los equipos están conectados y se visualizan entre sí.

Para una mejor seguridad en una topología de red, se deberá aplicar las reglas de control de acceso, como se observó en la figura todos sus dispositivos eran visibles y tenían conexiones entre ellos. En ningún caso sería aconsejable que dejara la configuración por defecto de estos principios, ya que podría estar dejando una vía de entrada para que aparezcan intrusos y vulneren los datos.

Además, como se mencionó en la **etapa de implementación**, una vez realizados pings entre todos los hosts, ya fueron visualizados por Floodlight Controller, en la trama de Hosts, en la siguiente figura se comprueba los hosts creados en la topología.

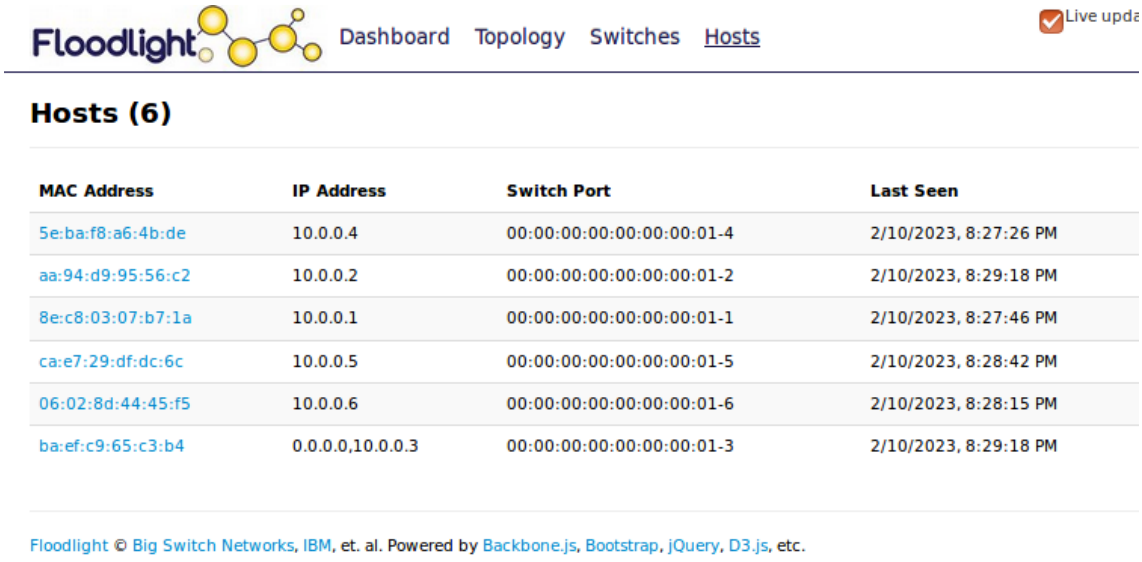


Figura 35. Hosts totales visualizados mediante ping

Resultados y análisis con asignación de control de acceso

Al implementar las reglas de control de acceso con el comando que se presentó anteriormente, se realiza la prueba con **pingall**, se observa como algunos dispositivos no tienen visibilidad ni conexión con otros. Las reglas ya fueron activadas en la etapa anterior, el acceso se desactiva a través del comando con reglas json.

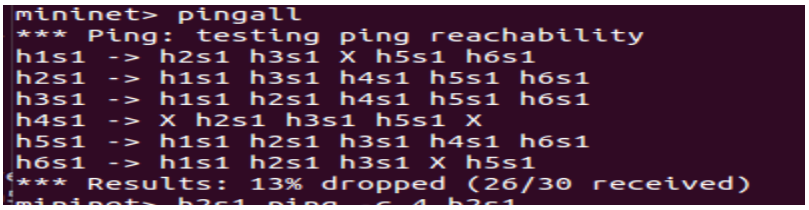


Figura 36. Prueba con control de acceso

En la figura se muestra como H1 no tiene acceso con H4, y H4 no tiene acceso con H6.

La incorporación de estas reglas impide que los interceptores lleguen al equipo, accedan a los datos y cambien o alteren los patrones en el hardware simulado. Estos resultados son muy positivos y así estaba previsto desde el principio de esta prueba. Las pruebas de control de acceso demuestran lo fundamentales que son para una empresa, debido a que fue factible valorar con eficacia y éxito las configuraciones en las que se permite o deniega el acceso al hardware simulado.

Comprobación de reglas de control de acceso

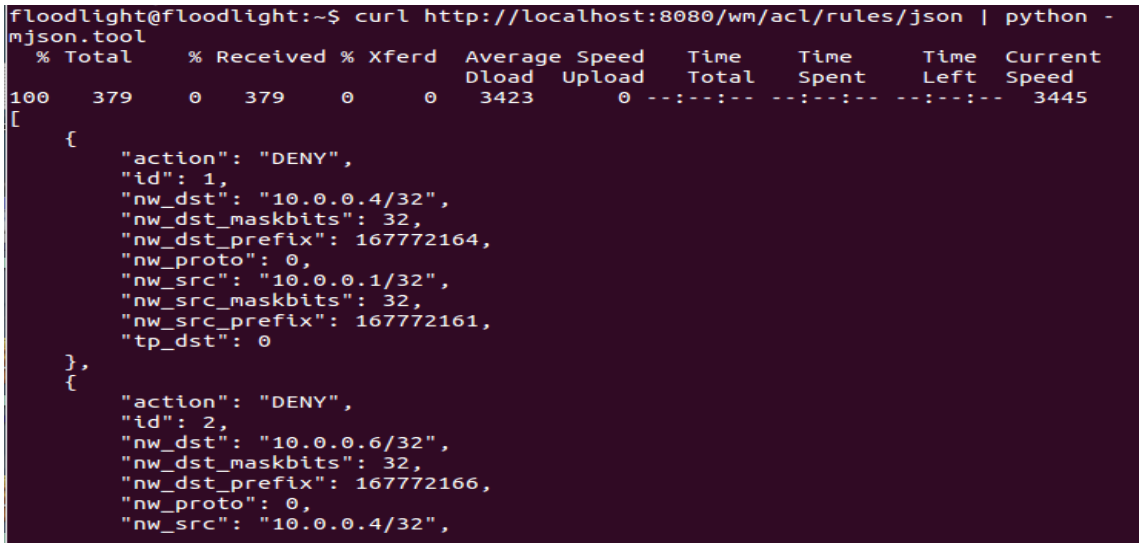


Figura 37. Reglas de control de acceso creadas

Se muestra en la figura la denegación de permiso entre los hosts, establecidos con anterioridad.

Comprobación de nodos enlazados

```
mininet> net
h1s1 h1s1-eth0:s1-eth1
h2s1 h2s1-eth0:s1-eth2
h3s1 h3s1-eth0:s1-eth3
h4s1 h4s1-eth0:s1-eth4
h5s1 h5s1-eth0:s1-eth5
h6s1 h6s1-eth0:s1-eth6
s1 lo:  s1-eth1:h1s1-eth0 s1-eth2:h2s1-eth0 s1-eth3:h3s1-eth0 s1-eth4:h4s1-eth0 s1-eth5:
h5s1-eth0 s1-eth6:h6s1-eth0
c0
```

Figura 38. Nodos enlazados en la red.

Gracias al comando net, nos proporciona la información de que nodo se encuentra, que no están conectados y cuales tienen conexión.

Información del switch

```
mininet> s1 ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:03:6a:07
          inet addr:192.168.1.5  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe03:6a07/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14533 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6814 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12850157 (12.8 MB)  TX bytes:767376 (767.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:110304 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110304 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:46022936 (46.0 MB)  TX bytes:46022936 (46.0 MB)
s1-eth1   Link encap:Ethernet  HWaddr 3a:a1:2d:ca:b6:e8
          inet6 addr: fe80::38a1:2dff:feca:b6e8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1555 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3532 (3.5 KB)  TX bytes:233619 (233.6 KB)

s1-eth2   Link encap:Ethernet  HWaddr 86:70:4d:eb:2d:96
          inet6 addr: fe80::8470:4dff:feeb:2d96/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1558 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3532 (3.5 KB)  TX bytes:234234 (234.2 KB)

s1-eth3   Link encap:Ethernet  HWaddr 6e:cb:1e:99:ae:a8
          inet6 addr: fe80::6ccb:1eff:fe99:aea8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1552 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3448 (3.4 KB)  TX bytes:230274 (230.2 KB)
s1-eth4   Link encap:Ethernet  HWaddr 56:0d:72:b4:59:fe
          inet6 addr: fe80::540d:72ff:feb4:59fe/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1557 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3350 (3.3 KB)  TX bytes:233869 (233.8 KB)

s1-eth5   Link encap:Ethernet  HWaddr 56:e0:ed:20:4c:e7
          inet6 addr: fe80::54e0:edff:fe20:4ce7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1570 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3448 (3.4 KB)  TX bytes:237549 (237.5 KB)

s1-eth6   Link encap:Ethernet  HWaddr ae:3b:9c:eb:39:2e
          inet6 addr: fe80::ac3b:9cff:feeb:392e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1554 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3350 (3.3 KB)  TX bytes:232139 (232.1 KB)
```

Figura 39. Información del switch

En la figura se observa toda la información detallada con sus enlaces del switch, obtenida de la topología de red diseñada por el comando.

Análisis y resultados del ancho de banda

En esta parte se hará las pruebas de ancho de banda, para empezar, se realizan las configuraciones en los hosts en el terminal de MiniNet, además se abrirá dos terminales en otra máquina virtual.

Se usará el nodo H1 y el nodo H3, para analizar el tiempo transcurrido y la transferencia de paquetes de datos entre nodos, se pondrá el comando iperf, para distinguir una evaluación de la velocidad que tiene la red y que dispositivo podría tener conflictos para alcanzar toda su capacidad

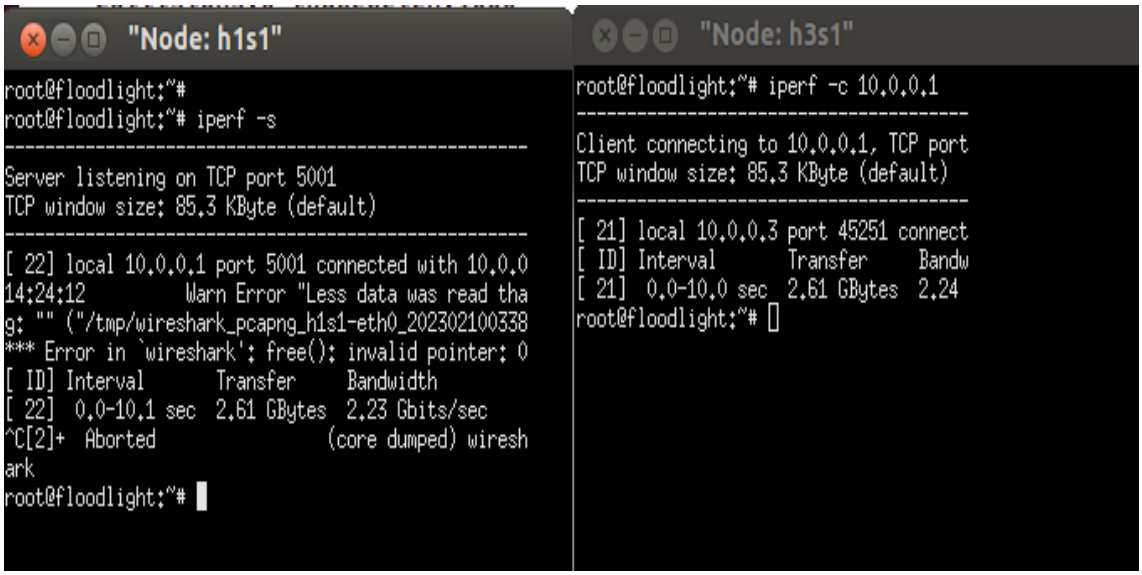


Figura 40.Prueba de ancho de banda

Tenemos la ventana del nodo H1S1 ejecutando el comando "**iperf-s"** y en la parte derecha tenemos la ventana del nodo H3S1, ejecutando el código **"iperf -c 10.0.0.2",** se demuestra la transferencia que existe entre el nodo H1 y el nodo H3, el tiempo transcurrido en segundos y el total de ancho de banda que arroja como resultado.

Pruebas de transferencia de paquetes

Para una comprobación más precisa, la figura adjunta muestra el tiempo transcurrido empleados en la transferencia de paquetes sin utilizar el controlador Floodlight.

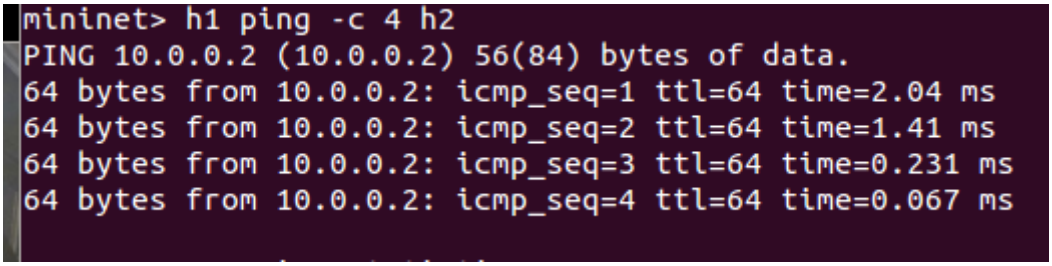


Figura 41. Transferencia de paquetes sin el controlador Floodlight

Se observa la velocidad de transferencia de cuatro paquetes enviados desde el host1 hacia el host2, ejecutados en MiniNet a través del comando ping en un entorno sin el controlador Floodlight.

A continuación, se muestra la transferencia de paquetes, ya levantando el servidor del controlador Floodlight, en la siguiente figura.

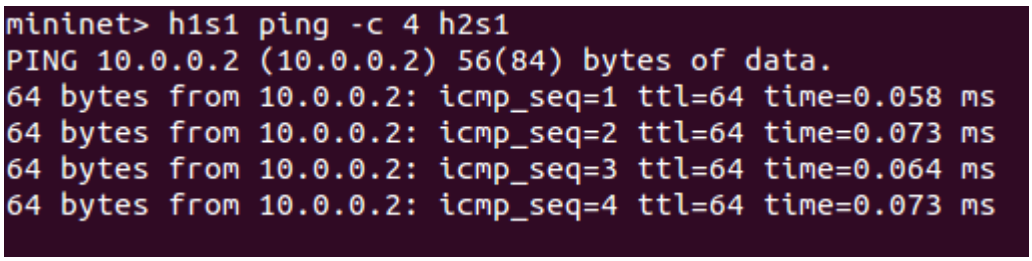


Figura 42. Transferencia de paquetes con el controlador Floodlight

Se observa la transferencia de paquetes realizados con el controlador de Floodlight, desde el host1 hacia el host2, mostrando que la transferencia y la velocidad al enviar estos paquetes son más reducidos, una gran diferencia a la figura anterior que no tiene activado Floodlight.

Análisis de tráfico ICMP con Wireshark

Para el análisis de tráfico ICMP, fueron hechos en dos casos diferentes:

El **primer caso** se realizó mediante un ping, enviando cuatros paquetes entre dos hosts que no tenían aplicadas las reglas de control de acceso, los hosts para realizar este análisis fueron **H1S1** y **H3S1**.

Para empezar, abriremos el analizador Wireshark desde la terminal del host H1S1, con el comando **Wireshark &**, el mismo nodo el cuál fue escogido para el análisis del tráfico ICMP en los dos casos.

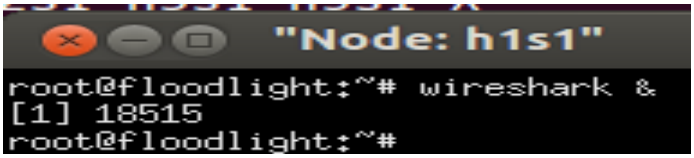


Figura 43. Accediendo a Wireshark desde el nodo host H1S1

Después de ejecutar el comando para inicializar Wireshark, se nos abre la interfaz, en donde empezamos a capturar el tráfico ICMP, por el host H1S1-eth0 y filtrando solo los paquetes ICMP.

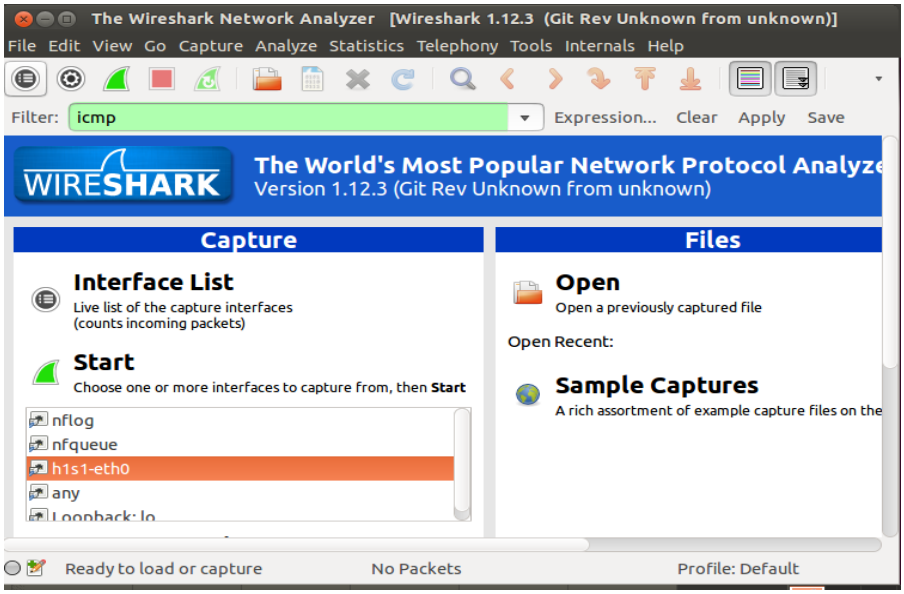


Figura 44. Interfaz de Wireshark

Se realizo el ping entre los hosts mencionados en MiniNet, enviando cuatro paquetes desde el host h1s1 al h3s1, con el comando **h1s1 ping -c 4 h3s1**.

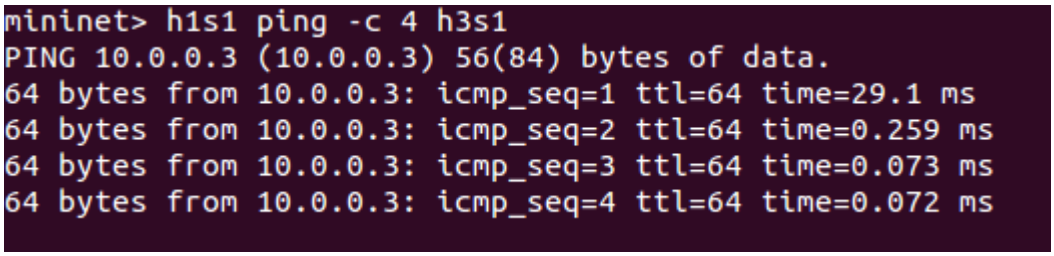


Figura 45. Ping entre los host h1s1 y h3s1

A continuación, se muestra en la figura, los paquetes enviados entre host sin reglas de control de acceso en la interfaz de Wireshark.

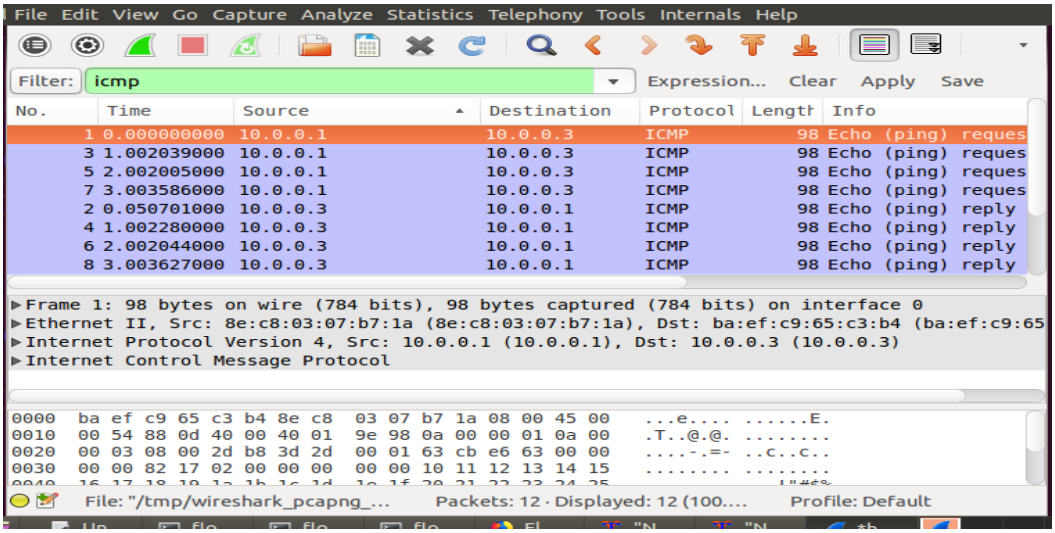


Figura 46. Tráfico de paquetes ICMP en hosts sin reglas de control de acceso

Como resultado se obtiene que fueron enviados cuatros paquetes y se recibieron cuatros paquetes entre el host H1 y el host H3 de forma correcta, por tanto, la dirección 10.0.0.1 del host H1, y la dirección 10.0.0.3 del host H3, se realizó un Echo (ping) request con el número de seq=1/256, un ttl=64, de la misma forma el host H3 responde con un Echo (ping) reply cuatro veces, también se muestra las capas por donde pasa el protocolo, se ubica en la misma capa del protocolo ICMP.

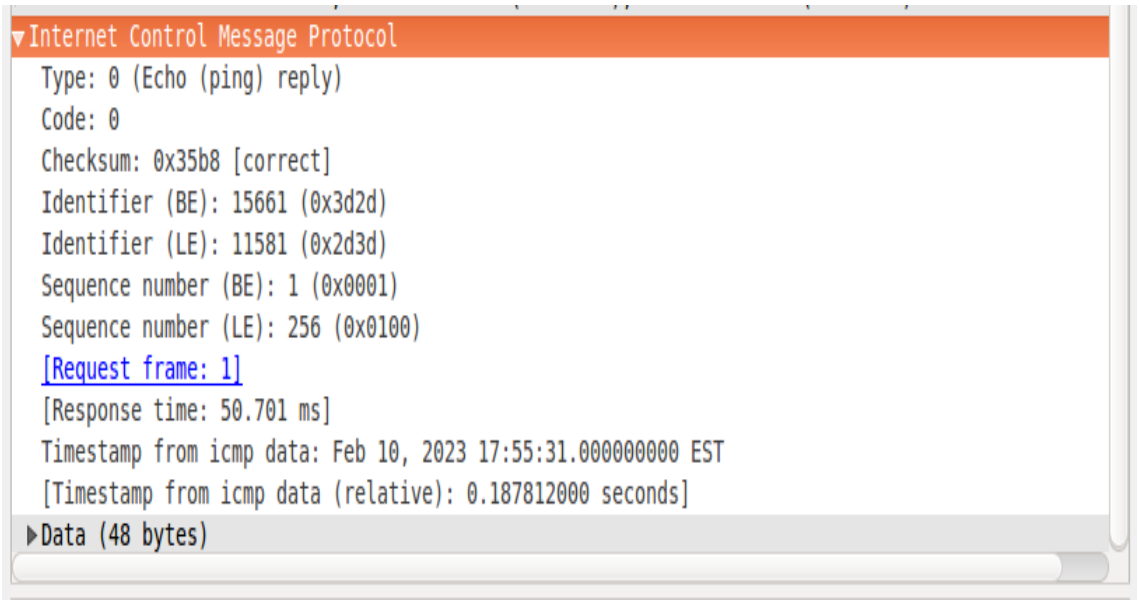


Figura 47.Información de la capa ICMP. Caso 1

Se observa que lo que se recibió es un mensaje de tipo de Echo reply, tipo 0, código 0, checksum correcto, los números identificadores y los datos, todos estos datos que representa en si la cabecera del protocolo ICMP.

El **segundo caso** se realizó mediante un ping, enviando cuatros paquetes entre dos hosts que, si tenían aplicadas las reglas de control de acceso, los hosts para realizar este análisis fueron **H1S1** y **H4S1**.

Se realizo el ping en MiniNet, enviando cuatro paquetes desde el host h1s1 al h4s1, con el comando **h1s1 ping -c 4 h4s1**.

```
mininet> h1s1 ping -c 4 h4s1
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.

--- 10.0.0.4 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3016ms
```

Figura 48. Ping entre los host h1s1 y h4s1

A continuación, se muestra en la figura, los paquetes enviados entre host con reglas de control de acceso aplicadas.

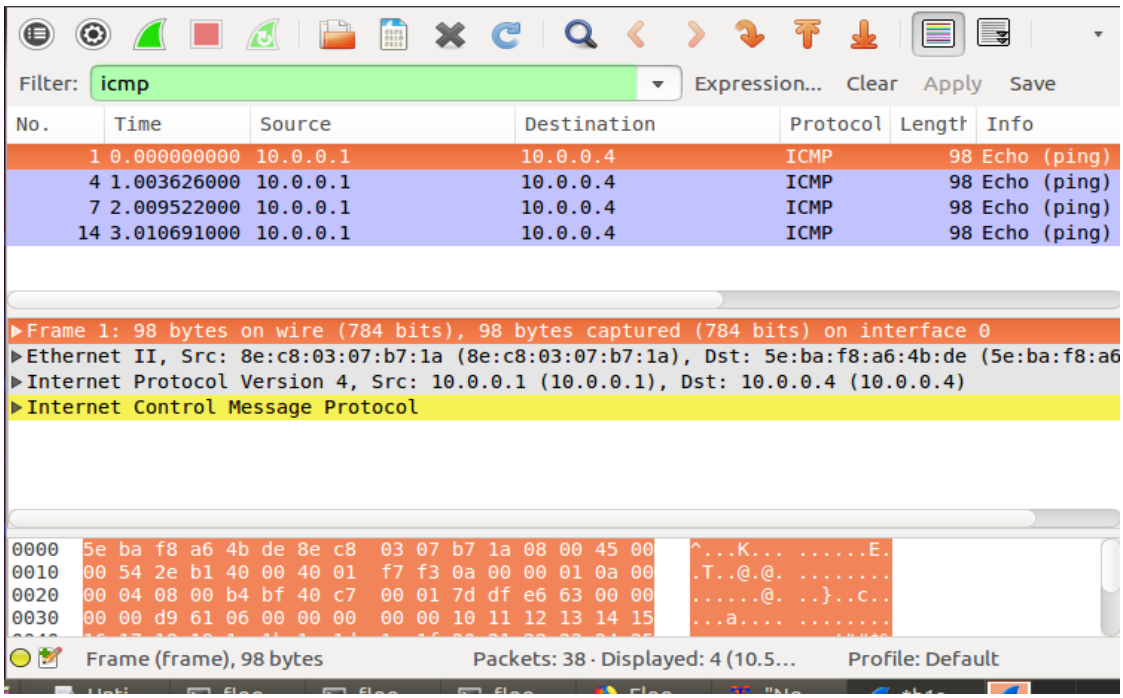


Figura 49.Tráfico de paquetes ICMP en hosts con reglas de control de acceso

Como resultado se obtiene, que fueron enviados cuatro paquetes, cero recibidos y cuatro perdidos, entre el host H1 y el host H4 de forma incorrecta, por tanto, la dirección 10.0.0.1 del host H1 y la dirección 10.0.0.4 del host H4, se realizó un Echo (ping) request sin encontrar respuesta, enviando cuatro paquetes al host H4.

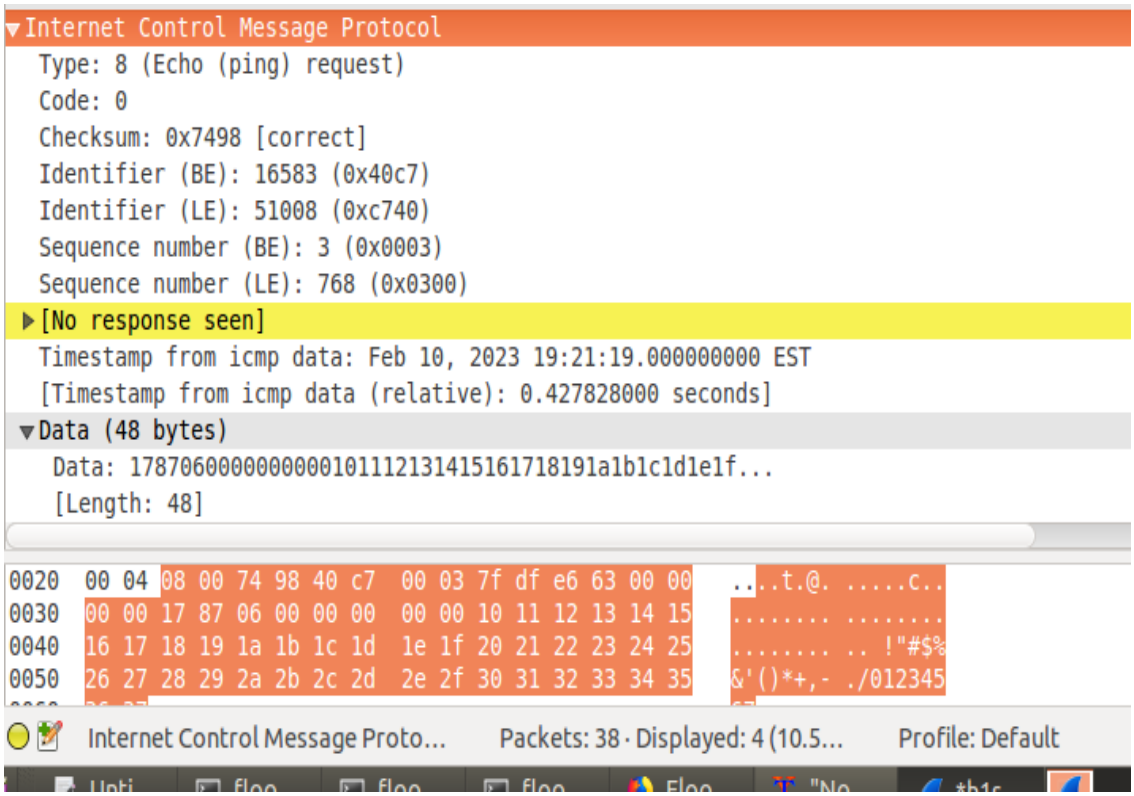


Figura 50.Información de la capa ICMP. Caso 2

Se observa que es de tipo 8, código 0 que es equivalente al mensaje de control de Echo request o petición de mensaje enviados, para recibir un Echo reply, en este caso no se recibió nada., debido a que el host H4 tiene denegado el acceso con el host H1, mediante las reglas de control de acceso.

Wireshark nos alerta de esto colocando de color amarillo en nombre de protocolo.

Resultados de las pruebas realizadas en la Etapa de Operación.

Los resultados en esta etapa final fueron los que se esperaban, en las pruebas de transferencias de paquetes y medición de ancho de banda, se pudo observar como el envío de estos paquetes se tornaron de forma lenta, al no tener activado el controlador Floodlight, también al activar este controlador junto a MiniNet, se observa que la distribución de transferencias de los paquetes de datos, arrojando un resultado de mejora en la velocidad, rendimiento, optimización de recursos de hardware y software. En cuanto al análisis de tráfico ICMP fueron exitosos, porque se pudieron verificar las tablas de control de acceso entre los hosts.

CONCLUSIONES

En esta propuesta tecnológica se comprobó que las redes definidas por software ofrecen notables resultados concebibles al ser implementadas en una organización, esto fue mediante a un análisis e investigaciones recolectadas de fuentes bibliográficas relacionados con el tema de composición de redes SDN.

El software de virtualización Oracle VM VirtualBox, el cual fue elegido para el desarrollo de la red SDN, funciono como se esperaba en el proceso de instalación de la máquina virtual con el controlador Floodlight, el mismo controlador, que ya venía con el software MiniNet integrado.

Mediante el controlador de Floodlight, resultó posible visualizar la disminución del tráfico de paquetes de datos generados en la red, debido a la asistencia con MiniNet, el cual se encargaba de distribuir el tráfico sin que no tenga el problema de saturación. Así mismo este controlador posee la capacidad de crear las reglas de control de acceso, las cuales fueron de importancia en este proyecto, porque si se dejaba sin reglas de control de acceso podría sufrir ataques de vulnerabilidad por terceras personas.

MiniNet y su administración no compleja, se caracteriza por ser unos de los softwares más sugerido para usuarios que no tienen experiencias, además permite la creación de redes con interfaz gráfica, esto proporciona al cliente una comprensión más fácil del uso del controlador.

Conforme a lo expuesto anteriormente, puede evidenciarse que al implementar la red SDN en la institución Unidad Educativa Americano, se consigue contrarrestar la congestión de la red local por sobrecarga de tráfico de paquetes, mejorando el rendimiento y el ancho de banda, esto fue posible mediante la aplicación de las reglas de control de acceso en las áreas, así mismo se pudo controlar el tráfico de paquetes ICMP por medio del analizador de paquetes Wireshark.

RECOMENDACIONES

Se recomiendo utilizar el software de virtualización a Oracle VM Virtual Box, por ser una plataforma totalmente gratuita que contiene herramienta de pago de otros softwares de virtualización y por su estabilidad con sistemas operativos de tipo en Linux o Ubuntu.

Utilizar el controlador Floodlight para llevar a cabo las pruebas necesarias para el correcto análisis que ofrecen algunos de sus componentes para el funcionamiento de redes definidas por software haciendo que, a través del control de acceso, garantice una mejor seguridad en los datos de forma simple con su interfaz excepcionalmente practico.

Hacer uso de la herramienta de MiniNet, su instalación es completamente sencilla y la ejecución de sus comandos principales, puede realizarse sin tener mucha experiencia con MiniNet, el más apropiado para prueba directas de ancho de banda, debido a que el mismo establece los límites de velocidad según los requisitos del cliente, mejorando en consecuencia la velocidad de manejo de la información sin importar la cantidad de ancho de banda recientemente utilizado.

Seguir explorando el tema de redes SDN, puesto que su ejecución en enormes o pequeñas instituciones son óptimas, en cualquiera de estas dos se ahorrará costes de implementación y administración, no obstante, esto mejora en ciclos e incrementa la ejecución con su administración unificada.

BIBLIOGRAFÍA

[1] userDataCenter, «REDES TRADICIONALES VS SDN DEFINIDAS POR SOFTWARE», 11 de marzo de 2020. https://blogs.salleurl.edu/es/redes-tradicionales-vs-sdn-definidas-por-software (accedido 28 de noviembre de 2022).

[2] Content Marketing, «Cómo resolver los problemas a los que se enfrentan las redes tradicionales», 13 de febrero de 2018. https://www.itreseller.es/content-marketing/2018/02/como-resolver-los-problemas-a-los-que-se-enfrentan-las-redes-tradicionales (accedido 28 de noviembre de 2022).

[3] I. Bernal y D. Mejía, «Las Redes Definidas por Software y los Desarrollos Sobre Esta Temática en la Escuela Politécnica Nacional», *Rev. Politécnica*, vol. 37, n.º 1, p. 43, 2016.

[4] A. Basit y N. Ahmed, «Path diversity for Inter-domain Routing security», *Proc. 2017 14th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2017*, pp. 384-391, mar. 2017, doi: 10.1109/IBCAST.2017.7868083.

[5] Y. A. Marín Muro, «Plataforma de pruebas para evaluar el desempeño de las redes definidas por software basadas en el protocolo Openflow», 20 de junio de 2016. https://dspace.uclv.edu.cu/handle/123456789/7255 (accedido 15 de julio de 2022).

[6] K. Benzekki, A. El Fergougui, y A. Elbelrhiti Elalaoui, «Software-defined networking (SDN): a survey», *Secur. Commun. Networks*, vol. 9, n.º 18, pp. 5803-5833, dic. 2016, doi: 10.1002/SEC.1737.

[7] S. Córdoba López, «Estudio de redes SDN mediante Mininet y MiniEdit», 23 de septiembre de 2019. https://riunet.upv.es/handle/10251/127877 (accedido 28 de noviembre de 2022).

[8] G. Cuenca Pérez y M. Flores Marín, «Redes definidas por software: Solución para servicios portadores del Ecuador», *INVESTIGATIO*, vol. 6, n.º 6, pp. 41-63, ago. 2021, doi: 10.31095/INVESTIGATIO.2015.6.2.

[9] Oracle, «Virtual Box». https://www.virtualbox.org/ (accedido 29 de noviembre de 2022).

[10] C. A. Carrillo Rodas, «Simulación de una red definida por software (SDN) para el control de acceso de los elementos de la red a nivel de capa 2.», 29 de junio de 2020. http://repositorio.ucsg.edu.ec/handle/3317/14837 (accedido 29 de noviembre de 2022).

[11] V. Moreno, «ESTUDIO DEL ESTANDAR OPENFLOW MEDIANTE CASO PRÁCTICO DE UTILIZACIÓN CON LA HERRAMIENTA VNX.», 2012. https://www.dit.upm.es/~posgrado/doc/TFM/TFMs2011-2012/TFM_Vanessa_Moreno_2012.pdf (accedido 29 de noviembre de 2022).

[12] Mininet, «Mininet: An Instant Virtual Network on Your Laptop (or Other PC) ». http://mininet.org/ (accedido 29 de noviembre de 2022).

[13] A. Rawal, «Introduction to OpenFlow Protocol », 7 de febrero de 2021. https://www.section.io/engineering-education/openflow-sdn/ (accedido 23 de noviembre de 2022).

[14] Alfon, «Análisis de red con Wireshark. Interpretando los datos.», 14 de febrero de 2008. https://seguridadyredes.wordpress.com/2008/02/14/analisis-de-red-con-wireshark-interpretando-los-datos/ (accedido 29 de noviembre de 2022).

[15] FACSISTEL, «LÍNEAS DE INVESTIGACIÓN». https://facsistel.upse.edu.ec/index.php?option=com_content&view=article&id=58&Itemi

d=463 (accedido 30 de noviembre de 2022).

[16] Orbit Consulting Group, «¿Cuáles son los beneficios de las Redes SDN (Software Defined Network)? », 30 de septiembre de 2022. https://www.orbit.es/cuales-son-los-beneficios-de-las-redes-sdn-sofware-defined-network/ (accedido 30 de noviembre de 2022).

[17] Secretaría Nacional de Planificación, «Plan de Creación de Oportunidades 2021-2025 de Ecuador», 2021. https://observatorioplanificacion.cepal.org/es/planes/plan-de-creacion-de-oportunidades-2021-2025-de-ecuador (accedido 30 de noviembre de 2022).

[18] D. López Pajares, «Nuevos conmutadores de red para redes integradas con SDN», 2021. https://ebuah.uah.es/dspace/handle/10017/51030 (accedido 30 de noviembre de 2022).

[19] L. K. Chalen Velez, «Diseño de un modelo de red definida por software para la virtualización a través del controlador FLOODLIGHT en la EMPRESA ELÉCTRICO HAZ S.A.», 2021. https://repositorio.ecotec.edu.ec/handle/123456789/224 (accedido 20 de enero de 2023).

[20] C. VALDIVIA MIRANDA, *Sistemas informáticos y redes locales*, 2.ª ed. Ediciones Paraninfo, SA, 2020.

[21] E. H. Pérez, *Tecnologías y redes de transmisión de datos*. Editorial Limusa, 2003.

[22] G. Cornetta, «Internet de las cosas: la hoja de ruta hacia un mundo conectado en red y sus implicaciones en el sector educativo», mar. 2016, Accedido: 23 de febrero de 2023. [En línea]. Disponible en: http://opendata.dspace.ceu.es/handle/10637/8064

[23] Editorial Etecé, «Redes Informáticas», 5 de agosto de 2021. https://concepto.de/redes-informaticas/ (accedido 20 de enero de 2023).

[24] M. Lederkremer, «Redes informáticas», *RedUsers*, 2019.

[25] I. Bernal y D. Mejía, «Las Redes Definidas por Software y los Desarrollos Sobre Esta Temática en la Escuela Politécnica Nacional», *Rev. Politécnica*, vol. 37, mar. 2016, Accedido: 13 de febrero de 2023. [En línea]. Disponible en: https://revistapolitecnica.epn.edu.ec/ojs2/index.php/revista_politecnica2/article/view/610/pdf

[26] M. Ramírez Giraldo y A. M. López Echeverry, «Redes de datos definidas por software-SDN, arquitectura, componentes y funcionamiento», *J. Cienc. e Ing.*, vol. 10, n.º 1, pp. 55-61, 2018, Accedido: 23 de febrero de 2023. [En línea]. Disponible en: http://jci.uniautonoma.edu.co/2018/2018-7.pdf

[27] E. R. Pérez Tardío, «Un acercamiento a las Redes Definidas por Software. Arquitectura y beneficios.», julio de 2018. https://www.researchgate.net/publication/326271018_Un_acercamiento_a_las_Redes_Definidas_por_Software_Arquitectura_y_beneficios (accedido 14 de febrero de 2023).

[28] A. García Centeno, C. M. Rodríguez Vergel, C. Anías Calderón, y F. C. Casmartiño Bondarenko, «Controladores SDN, elementos para su selección y evaluación.», *Rev. Telem@tica*, vol. 13, n.º 3, pp. 10-20, dic. 2014, Accedido: 13 de febrero de 2023. [En línea]. Disponible en: https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/164/153

[29] D. R. Rodríguez Herlein, C. A. Talay, C. N. González, y L. A. Marrone, «Explorando las redes definidas por software (SDN)», *SEDICI*, pp. 100-104, 2020, Accedido: 13 de febrero de 2023. [En línea]. Disponible en: http://sedici.unlp.edu.ar/handle/10915/103546

[30] E. B. Avendaño, D. R. Bautista, A. Coronel, y F. Cuesta Quintero, «Smart farm: Defining of infrastructure based on internet of things, IpV6 and software defined networks», *RISTI*

- *Rev. Iber. Sist. e Tecnol. Inf.*, n.º 17, pp. 183-197, ene. 2019, Accedido: 13 de febrero de 2023. [En línea]. Disponible en: https://www.researchgate.net/publication/331178386_Smart_farm_Defining_of_infrastructure_based_on_internet_of_things_IpV6_and_software_defined_networks

[31] G. A. Huaillas García, «Virtualización de Servidores con Hyper-V para la Gestión de la Continuidad del Servicio en la Red de Agencias MIBANCO», 2018. https://repositorio.ucv.edu.pe/handle/20.500.12692/36395 (accedido 22 de febrero de 2023).

[32] Z. H. Shah, «Windows Server 2012 Hyper-V : Deploying the Hyper-V Enterprise Server Virtualization Platform», *Packt Publ.*, p. 686, 2013, Accedido: 22 de febrero de 2023. [En línea]. Disponible en: https://www.vmware.com/

[33] VMware, «A Performance Comparison of Hypervisors», 2022.

[34] E. Buitrago y Y. Urrego, «Implementar una infraestructura de virtualización del sistema uno 8.5, a través del software virtual box, para la empresa Energizando Ingeniería y Construcción S.A.S.», 2016. http://hdl.handle.net/20.500.12622/4055 (accedido 22 de febrero de 2023).

[35] F. J. Ribadas-Pena, R. Anido-Bande, y V. M. Darriba-Bilbao, «DSBOX: herramienta docente para el diseño y simulación de entornos de red virtualizados», *Actas las XXII JENUI*, pp. 335-342, jul. 2016, Accedido: 22 de febrero de 2023. [En línea]. Disponible en: https://upcommons.upc.edu/handle/2117/90479

[36] M. F. Bone Andrade, J. D. Rodríguez Vizuete, S. M. Sosa Calero, y L. A. Núñez Freire, «Aplicaciones de SDN en infraestructura de redes educativas», *Cienc. Digit.*, vol. 5, n.º 1, pp. 219-231, ene. 2021, doi: 10.33262/cienciadigital.v5i1.1539.

[37] Open Daylight, «The linux foundation projects», 2021. https://www.opendaylight.org/#more (accedido 25 de enero de 2023).

[38] C. Yagüe, «Qué es Apache Maven», 29 de abril de 2019. https://openwebinars.net/blog/que-es-apache-maven/ (accedido 25 de enero de 2023).

[39] ONOS, «Open Network Operating System», 2021. https://opennetworking.org/onos/ (accedido 25 de enero de 2023).

[40] D. Casado Jiménez, «SIMULACIÓN DE UNA RED SDN DE VIDEOVIGILANCIA IP BASADA EN GNS3», 9 de septiembre de 2020. https://riunet.upv.es/bitstream/handle/10251/152379/Casado - Simulación de una red SDN de videovigilancia IP basada en GNS3..pdf?sequence=1&isAllowed=y (accedido 13 de febrero de 2023).

[41] Floodlight, «Project Floodlight», 7 de febrero de 2016. https://floodlight.atlassian.net/wiki/spaces/HOME/overview?mode=global (accedido 25 de enero de 2023).

[42] E. J. MARTÍNEZ COPETE, «ESTUDIO DEL FUNCIONAMIENTO DE LA HERRAMIENTA MININET», p. 116, 2015.

[43] B. Valencia, S. Santacruz, L. . Becerra, y J. . Padilla, «Mininet: una herramienta versátil para emulación y prototipado de Redes Definidas por Software», *Entre Cienc. e Ing.*, vol. 9, n.º 17, pp. 62-70, 2015, Accedido: 25 de enero de 2023. [En línea]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-83672015000100009&lng=en&nrm=iso&tlng=es

[44] M. Betegón García, «Estudio de técnicas de Ingeniería de Tráfico basadas en SDN (Study of SDN Traffic Engineering techniques)», junio de 2018.

https://repositorio.unican.es/xmlui/bitstream/handle/10902/14193/409476.pdf?sequence=1&isAllowed=y (accedido 13 de febrero de 2023).

[45] R. C. Martínez Zeas y M. Lituma Orellana, «Análisis y captura de paquetes de datos en una red mediante la herramienta Wireshark», 2011. http://repositorio.uisrael.edu.ec/handle/47000/168 (accedido 14 de febrero de 2023).

[46] S. A. ALVERNIA ACEVEDO, «WIRESHARK: COMO HERRAMIENTA DE APOYO PARA EL ANALISIS DE TRAFICO MALICIOSO EN UNA RED DE AREA LOCAL», 11 de febrero de 2016. http://repositorio.ufpso.edu.co/jspui/handle/123456789/996 (accedido 14 de febrero de 2023).

[47] E. Viales Zúñiga, «Uso de las Plataformas Educativas Virtuales de acuerdo a los lineamientos sugeridos por el Ministerio de Educación Pública y su repercusión en el aprendizaje significativo en la especialidad de Informática en Redes en el desarrollo de las habilidades apre», 2021. https://repositorio.ulatina.ac.cr/handle/20.500.12411/205 (accedido 23 de febrero de 2023).

[48] A. Pisano, «Internet de la cosas», noviembre de 2018. http://repositorio.udesa.edu.ar/jspui/handle/10908/16159 (accedido 23 de febrero de 2023).

[49] J. O. Sambrano Velasco, «Implementación de Redes SDN-WAN y evaluación de resultados sobre aplicaciones de uso recurrente en usuarios a travez de distintos proveedores de servicios de internet (ISP's)», 14 de diciembre de 2020. http://repositorio.espe.edu.ec/bitstream/21000/23406/1/T-ESPE-044177.pdf (accedido 23 de febrero de 2023).

[50] R. A. Ríos, «Conceptualización de SDN y NFV», *Maskay*, vol. 6, n.º 1, pp. 29-34, 2016, Accedido: 23 de febrero de 2023. [En línea]. Disponible en: http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-67122016000100029&lng=es&nrm=iso&tlng=es

[51] S. Rendón Bernot, «Enrutamiento de paquetes en Redes Definidas por Software mediante Aprendizaje Automático», p. 55, 2020.

[52] J. A. Maya Lamilla, «Ventajas y desventajas del paradigma de las redes definidas por software (SDN)», 2021. http://dspace.utb.edu.ec/handle/49000/10536 (accedido 23 de febrero de 2023).

[53] S. Pérez, H. Facchini, F. Hidalgo, G. Cangemi, y A. Dantiacq, «ESTUDIOS SOBRE SIMULACIÓN Y ANÁLISIS COMPARATIVO ENTRE REDES DE DATOS SDN Y REDES DE DATOS TRADICIONALES», *CeReCoN (Centro Reg. UTN en Comput. y Neuroingeniería)*, 2021, Accedido: 22 de febrero de 2023. [En línea]. Disponible en: https://www.researchgate.net/publication/354586961

[54] J. F. Guano Viscarra, «Prototipo de una SDN utilizando herramientas open-source», 22 de mayo de 2017. http://bibdigital.epn.edu.ec/handle/15000/17327 (accedido 22 de febrero de 2023).

[55] M. Sánchez López, «Análisis de redes SDN utilizando Mininet e implementación de un Deep Packet Inspector», julio de 2015. https://wpd.ugr.es/~jorgenavarro/thesis/2015_TFG_ManuelSanchez.pdf (accedido 22 de febrero de 2023).

[56] Punt Informatic Becomit Company, «Beneficios de las red definida por software sdn», 2018. https://puntinformatic.com/beneficios-de-la-red-definida-por-software-sdn/ (accedido 25 de enero de 2023).

[57] N. Coniglio Perdomo, L. S. Martínez Cuello, y G. M. Rodríguez Fontan, «ElastiCDN»,

2019. https://dspace.ort.edu.uy/handle/20.500.11968/3946 (accedido 1 de marzo de 2023).

[58] Digital Guide Ionos, «SDN: gestión de redes por software», 12 de junio de 2019. https://www.ionos.es/digitalguide/servidores/know-how/software-defined-network/ (accedido 25 de enero de 2023).

[59] Digital Books, «Gestión de redes telemáticas», 2022. https://reader.digitalbooks.pro/content/preview/books/37922/book/OEBPS/Text/chapter1.html (accedido 15 de febrero de 2023).

[60] E. W. Amaya Carrión, «Redes de computadoras. Introducción a las redes, necesidad de una red, tipo y equipos de redes, topología de una red, diseño de redes, instalación y administración de redes LAN», 28 de agosto de 2018. http://repositorio.une.edu.pe/handle/20.500.14039/4118 (accedido 15 de febrero de 2023).

[61] TICO María y Borja, «Red en bus o red lineal», 2023. https://sites.google.com/site/ticomariayborja/tipologias-de-red/red-en-bus-o-red-linial (accedido 22 de febrero de 2023).

ANEXOS

1. Solicitud dirigida a la institución para el desarrollo de la propuesta tecnológica.

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍA DE LA INFORMACIÓN

UPSE

ING. JOSÉ SANCHEZ AQUINO, MGT.

DIRECTOR DE LA CARRERA DE TECNOLOGIAS DE LA INFORMACION

C E R T I F I C O

Que el Sr. **STEVE MARTIN MELENDRES DEL PEZO,** portador de la cédula de ciudadanía No. **2450030065,** consta matriculado con No. 12018060313 en el **Octavo Semestre** de la **Carrera de Tecnologías de la Información,** en el periodo académico **2022-2** y asiste normalmente a clases en la modalidad presencial.

Además cabe indicar, que se encuentra registrado en la Unidad de titulación en la materia de Unidad Integración Curricular II, para el cual desarrolla un proyecto de trabajo de titulación denominado **"PROPUESTA DE IMPLEMENTACIÓN DE UNA RED SDN POR MEDIO DEL CONTROLADOR FLOODLIGHT Y MININET PARA LA INSTITUCIÓN UNIDAD EDUCATIVA AMERICANO"**, el mismo que deberá ser presentado y sustentado para la aprobación de la asignatura y a la vez es requisito previo a la obtención del título de Ingeniero en Tecnologías de la Información.

Es todo cuanto puedo certificar en honor a la verdad.

La Libertad, 24 de enero del 2023

Atentamente,

Ing. José Sánchez A, Mgt.

DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

UPSE DIRECCIÓN CARRERA TECNOLOGÍAS DE LA INFORMACIÓN

AMERICANO UNIDAD EDUCATIVA

GERENTE

Fecha: 24/01/2023

Hora: 4:00 pm.

Campus matriz, La Libertad - Santa Elena - ECUADOR
Código Postal: 240204 - Teléfono: (04) 781 - 732

UPSE ¡crece sin límites!

www.upse.edu.ec

Anexo 1. Carta AVAL emitida por la Carrera de Tecnología de la Información.

2. Autorización de la institución Unidad Educativa Americano para la elaboración de la Propuesta Tecnológica.

AMERICANO
UNIDAD EDUCATIVA

CARTA AVAL

Ing. José Sánchez A, Mgt
DIRECTOR DE LA CARRERA
TECNOLOGÍA DE LA INFORMACIÓN.
FACULTAD SISTEMAS Y TELECOMUNICACIONES
UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA.

YO, **Ing. William Amador Núñez De La Cruz, Gerente General** de la **Unidad Educativa Americano**, previa a la solicitud presentada por el **Sr. Melendres Del Pezo Steve Martin con** número de cédula **Nº 2450030065 de La Facultad De Sistemas y Telecomunicaciones de la Carrera de Tecnología De La Información** de la **Universidad Estatal Península de Santa Elena** se autoriza para que desarrolle el trabajo de titulación denominado **"PROPUESTA DE IMPLEMENTACIÓN DE UNA RED SDN POR MEDIO DEL CONTROLADOR FLOODLIGHT Y MININET PARA LA INSTITUCIÓN UNIDAD EDUCATIVA AMERICANO"** y que los resultados de dicho trabajo de investigación sean publicados en el repositorio del portal WEB de la UPSE.

Particular que informo a usted para los fines pertinentes.

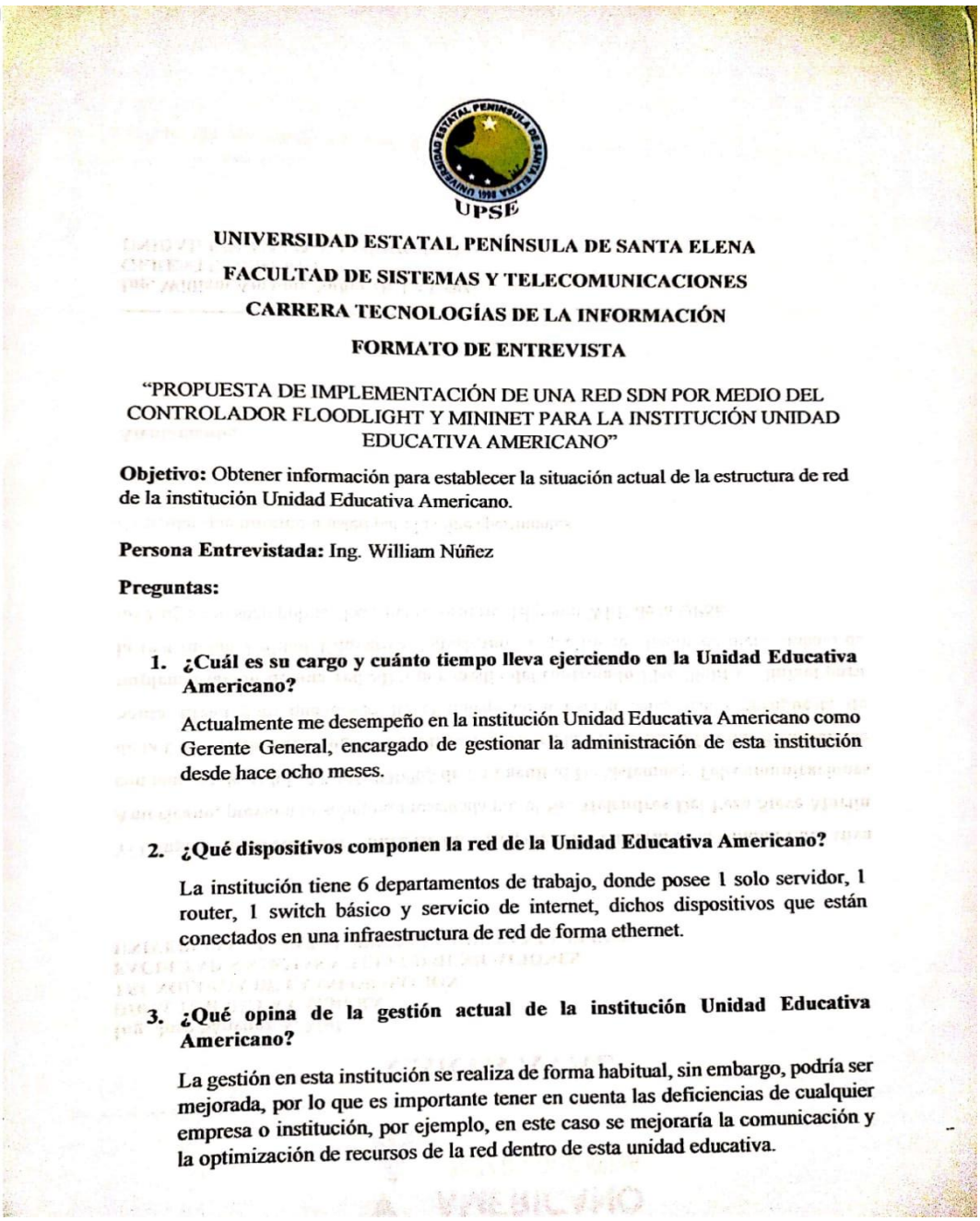
Atentamente,

Ing. William Amador Núñez De La Cruz
GERENTE GENERAL
UNIDAD EDUCATIVA AMERICANO

UPSE
CARRERA TECNOLOGÍAS DE LA INFORMACIÓN
RECIBIDO
HORA
09 FEB 2023
FIRMA AUTORIZADA

Anexo 2. Carta AVAL emitida por la institución Unidad Educativa Americano

3. Preguntas realizadas al gerente general de la institución Unidad Educativa Americano.



UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA TECNOLOGÍAS DE LA INFORMACIÓN

FORMATO DE ENTREVISTA

"PROPUESTA DE IMPLEMENTACIÓN DE UNA RED SDN POR MEDIO DEL CONTROLADOR FLOODLIGHT Y MININET PARA LA INSTITUCIÓN UNIDAD EDUCATIVA AMERICANO"

Objetivo: Obtener información para establecer la situación actual de la estructura de red de la institución Unidad Educativa Americano.

Persona Entrevistada: Ing. William Núñez

Preguntas:

1. **¿Cuál es su cargo y cuánto tiempo lleva ejerciendo en la Unidad Educativa Americano?**

   Actualmente me desempeño en la institución Unidad Educativa Americano como Gerente General, encargado de gestionar la administración de esta institución desde hace ocho meses.

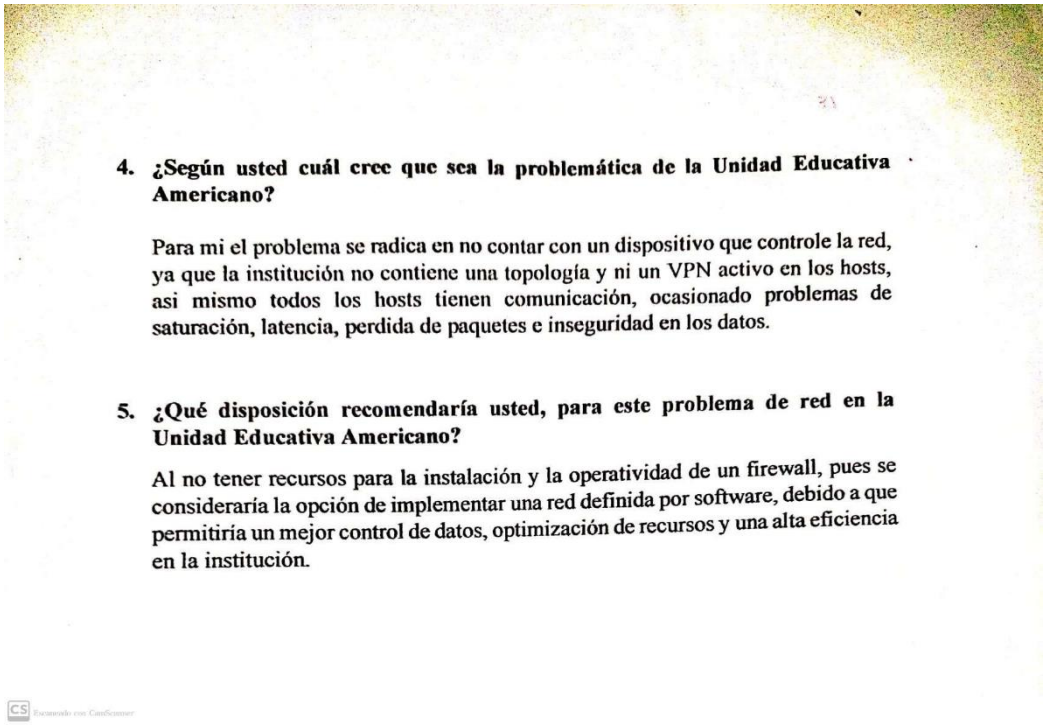
2. **¿Qué dispositivos componen la red de la Unidad Educativa Americano?**

   La institución tiene 6 departamentos de trabajo, donde posee 1 solo servidor, 1 router, 1 switch básico y servicio de internet, dichos dispositivos que están conectados en una infraestructura de red de forma ethernet.

3. **¿Qué opina de la gestión actual de la institución Unidad Educativa Americano?**

   La gestión en esta institución se realiza de forma habitual, sin embargo, podría ser mejorada, por lo que es importante tener en cuenta las deficiencias de cualquier empresa o institución, por ejemplo, en este caso se mejoraría la comunicación y la optimización de recursos de la red dentro de esta unidad educativa.

Anexo 3. Preguntas realizadas en la entrevista, Parte 1



4. **¿Según usted cuál cree que sea la problemática de la Unidad Educativa Americano?**

Para mi el problema se radica en no contar con un dispositivo que controle la red, ya que la institución no contiene una topología y ni un VPN activo en los hosts, asi mismo todos los hosts tienen comunicación, ocasionado problemas de saturación, latencia, perdida de paquetes e inseguridad en los datos.

5. **¿Qué disposición recomendaría usted, para este problema de red en la Unidad Educativa Americano?**

Al no tener recursos para la instalación y la operatividad de un firewall, pues se consideraría la opción de implementar una red definida por software, debido a que permitiría un mejor control de datos, optimización de recursos y una alta eficiencia en la institución.

Anexo 4. Preguntas realizadas en la entrevista, Parte 2

4. Entrevista realizada al gerente general de la institución Unidad Educativa Americano.

Anexo 5. Entrevista con el gerente general de la institución

5. Preparación del ambiente para llevar a cabo la virtualización de la red SDN.

Anexo 6. Máquina del departamento de inspección, donde estará ubicado el controlador Floodlight

Anexo 7. Manipulación de dispositivos, router y switch