UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

TRABAJO DE INTEGRACIÓN CURRICULAR

previo a la obtención del Título de:

INGENIERO EN TECNOLOGIAS DE LA INFORMACIÓN

TEMA: "Diseño de una infraestructura de red definida por software (SDN) para optimización de la red tradicional de una institución educativa del cantón Salinas con Mininet y Miniedit"

AUTOR:

Salinas Domínguez Isidro Ubaldo

PROFESOR TUTOR:

Ing. Shendry Rosero, MGTI.

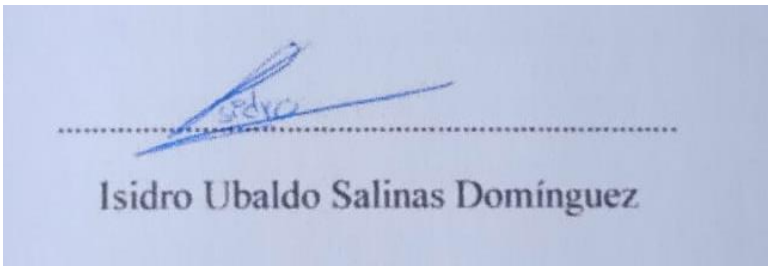
SANTA ELENA – ECUADOR

PAO: 2022-1

DECLARACIÓN

El contenido del presente proyecto de unidad de integración curricular es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

Atentamente,



DEDICATORIA

A mi mamá, Miriam Domínguez, y a mi tía, Sara Domínguez, por cumplir con el rol de padre y madre. Sin en el apoyo y respaldo de ellas durante todo el tiempo de carrera universitaria, este logro no podría ser una realidad. Mi motor de vida son ellas. Mi familia.

A mis mascotas, Murdock y Bobby, por acompañarme en el silencio de las noches de desvelo durante toda esta travesía.

Isidro Salinas Domínguez

AGRADECIMIENTO

A mis mejores amigos, Andrés Palacios, Jesús Tubay, Jean Marcos Aguilera, Raúl Villao, Jerson Barrio y Adriana López. Sin su apoyo, constantes aventuras, palabras, momentos tristes y alegres, no estaría completo. Agradecerles en la culminación de este proyecto no es suficiente por todo lo que han hecho por mí.

A la Ingeniera Alicia Andrade, por haberme inspirado en área de redes de comunicación de datos. Al Ingeniero Shendry Rosero, por su capacitación y paciencia como docente tutor.

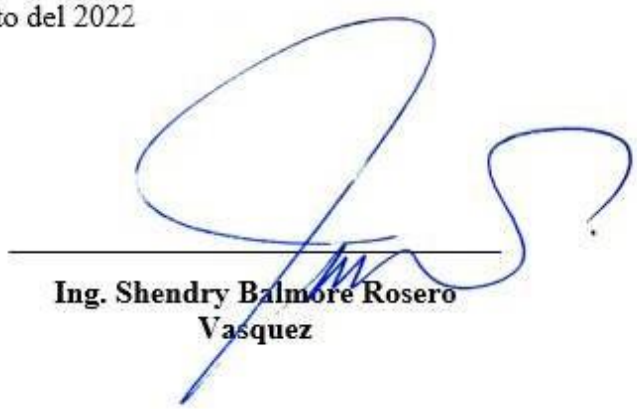
Gracias por haber hecho del 2021 el mejor año de todos. Fuiste parte de la aprobación del tema de este proyecto, y la primera en felicitarme con cariño desbordante. Gracias por haber sido mi consuelo, mi inspiración para buscar oportunidades laborales, y con ello ser mejor profesional.

Isidro Salinas Domínguez

APROBACIÓN DEL TUTOR

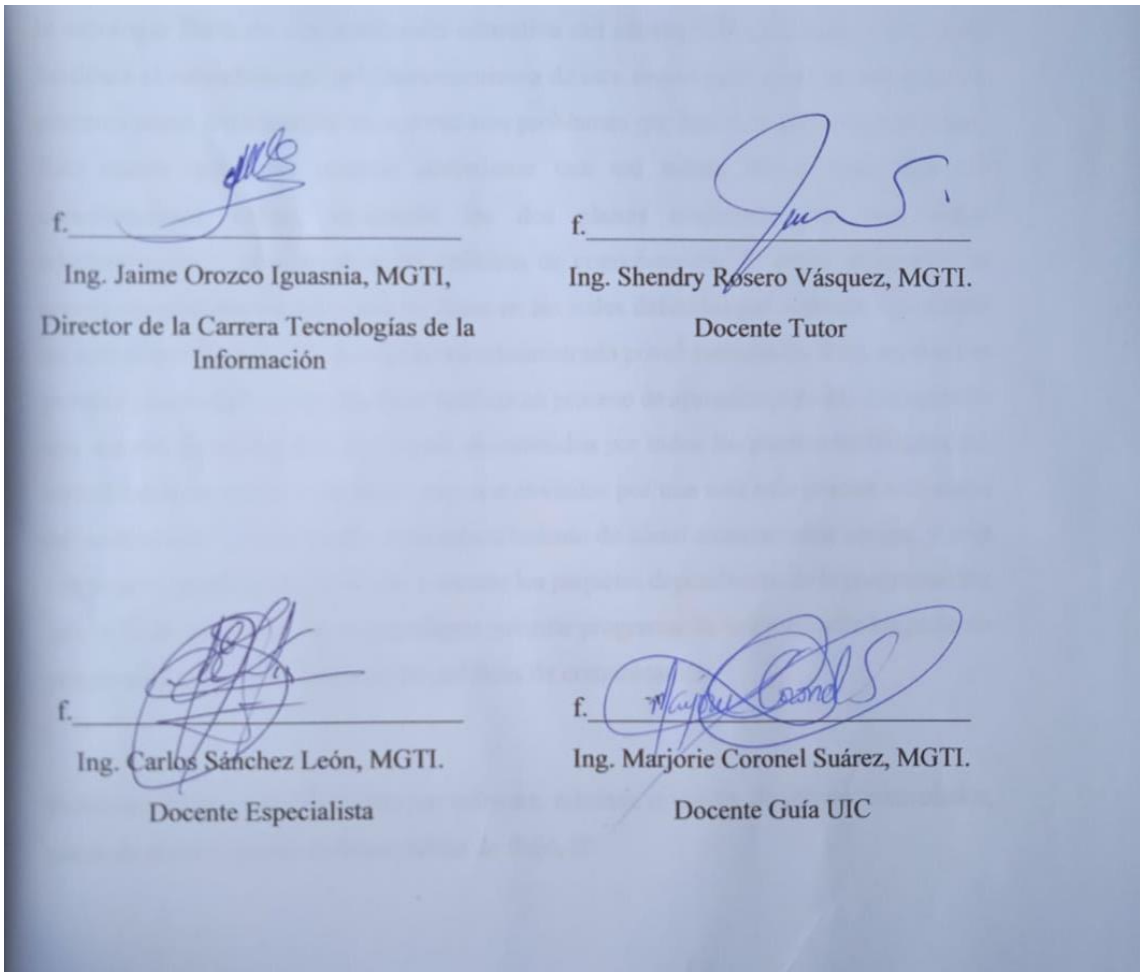
En mi calidad de Tutor/Tutora del trabajo de titulación denominado: **"Diseño de una infraestructura de red definida por software (SDN) para optimización de la red tradicional de una institución educativa del cantón Salinas con Mininet y Miniedit",** elaborado por la estudiante **Salinas Domínguez Isidro Ubaldo,** de la carrera de Tecnología de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, le apruebo en todas sus partes y autorizo al estudiante para que inicia los trámites legales correspondientes.

La libertad, agosto del 2022



Ing. Shendry Balmore Rosero Vasquez

TRIBUNAL DE GRADO



f._____

Ing. Jaime Orozco Iguasnia, MGTI,

Director de la Carrera Tecnologías de la Información

f._____

Ing. Shendry Rosero Vásquez, MGTI.

Docente Tutor

f._____

Ing. Carlos Sánchez León, MGTI.

Docente Especialista

f._____

Ing. Marjorie Coronel Suárez, MGTI.

Docente Guía UIC

RESUMEN

El trabajo propuesto como Proyecto de Unidad de Integración Curricular (Proyecto UIC) es una guía para poder realizar diseños de redes definidas por software (SDN) utilizando miniedit como herramienta topológica, mininet como como simulador de redes SDN y floodlight como controlador de red. El diseño SDN utilizado es un modelo adaptado de la topología física de una institución educativa del cantón Salinas-Ecuador. Está guía facilitará el entendimiento del funcionamiento de este nuevo paradigma de redes que se presenta como solucionador de una red con problemas que hacen frente a una red física. Esta nueva tecnología permite administrar una red entera física, como una red completamente virtual, separando los dos planos existentes para una mejor administración y programación de políticas de comunicación. El plano de control se separa completamente del plano de datos en las redes definidas por software, quedando un solo plano de control para toda la red administrado por el controlador. Esta separación permite a los switch o conmutadores realizar un proceso de aprendizaje único. Comparado con una red física, los paquetes ya no son enviados por todos los puertos habilitados del switch hasta encontrar su destino, sino son enviados por una sola ruta gracias a la orden del controlador. El controlador tiene conocimiento de cómo alcanzar cada equipo, y a su vez tiene la habilidad de conmutar y enrutar los paquetes dependiendo de la programación que se le dé, pues este nuevo paradigma permite programar la red mediante lenguaje de programación de alto nivel para las políticas de comunicación.

Palabras claves: redes definidas por software, mininet, miniedit, floodlight, controlador, plano de control, plano de datos, tablas de flujo, IP.

ABSTRACT

The work proposed as the Curricular Integration Unit Project (UIC Project) is a guide to be able to design software-defined networking (SDN) using miniedit as a topological tool, mininet as an SDN network simulator and floodlight as a network controller. The SDN design used is an adapted model of the physical topology of an educational institution in the Salinas-Ecuador canton. This guide will facilitate the understanding of the operation of this new paradigm of networks that is presented as a solver of a network with problems that face a physical network. This new technology allows you to manage an entire physical network, as a completely virtual network, separating the two existing planes for better management and programming of communication policies. The control plane is completely separated from the data plane in software-defined networking, leaving a single control plane for the entire network managed by the controller. This separation allows the switches or switches to perform a unique learning process. Compared to a physical network, the packets are no longer sent through all the enabled ports of the switch until they find their destination, but they are sent through a single route thanks to the order of the controller. The controller is aware of how to reach each device, and in turn has the ability to switch and route the packets depending on the programming given to it, since this new paradigm allows the network to be programmed using a high-level programming language for communication policies. communication.

Keywords: software defined networking, mininet, miniedit, floodlight, controller, control plane, data plane, flow tables, IP.

TABLA DE CONTENIDOS

INDICE DE FIGURAS

INTRODUCCIÓN

Las redes de comunicación de datos son de suma importancia en la actualidad, ya que por ellas es posible mantener una comunicación entre dispositivos ubicados en cualquier parte para obtener o compartir información. Por ello, la evolución e innovación constante de estas tecnologías es necesaria para garantizar una mejor experiencia en el envío de datos.

Las redes convencionales ofrecen la posibilidad de compartir información, pero dentro de la evolución de la tecnología, se ha presentado un nuevo paradigma de redes, uno que ofrece la posibilidad de manejar un solo plano de control para toda una red, haciendo que los switches realicen un proceso de aprendizaje único mediante el cual se convertirá en el camino para enviar los paquetes desde un origen a un destino.

Las redes definidas por software (SDN) permiten la programación de los paquetes al momento de conmutarlos o enrutarlos, a su vez, permite realizar una sola configuración dentro de un único dispositivo en lugar de estar visitando cada dispositivo existente en la infraestructura.

El proyecto constará de dos capítulos. El primer capítulo explicará la fundamentación, abarcando los antecedentes, descripción del proyecto, objetivos del proyecto, justificación, alcance, metodología del proyecto y técnica de investigación para la recolección de información de la institución educativa donde se representará la simulación de una red SDN partiendo desde el diseño de la red física tradicional propia de la institución.

Dentro del segundo capítulo se expondrá el componente práctico, detallando y explicando las herramientas que se utilizaron para poder realizar la simulación y demostrar la funcionabilidad de una la red SDN, donde podrá apreciar el tráfico que genera el protocolo openflow mediante el análisis con la herramienta de tráfico de red wireshark y a su vez la observación de la tabla de flujo de los conmutadores de red.

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1. Antecedentes

En las instituciones educativas por lo general la administración de los equipos se basa en una integración vertical, donde cada uno de sus dispositivos se controlan a sí mismos con su propio firmware instalado en su espacio de memoria [1]. Esta estrategia presenta complicaciones de configuración de la infraestructura, sea esta para seguridad, mantenimiento o cambios de protocolo para enrutamiento, ya que el encargado de administrar la red debería hacer las configuraciones de manera manual en cada dispositivo existente en la empresa con el riesgo de modificar una configuración previamente establecida. Si en la institución existe un problema en la red donde el administrador se encuentre alejado por una distancia excesiva del equipo que falla, para solucionarlo se debería acudir al lugar volviéndose una solución demorada y nada óptima.

La institución donde se llevará a cabo este proyecto de simulación de redes definidas por software tiene sede en la avenida Carlos Espinoza en el cantón Salinas, y por motivos de pandemia SARS-Cov-2, optó por mudar sus instalaciones en el año 2020 al sector siete esquinas del cantón La Libertad para continuar con su funcionamiento, hasta que la emergencia sanitaria disminuyera su impacto o los casos reduzcan. Fue fundada en el año 1976 llevando como nombre Frank Vargas Pazzos, pero por la Ley Orgánica de Educación Intercultural, art. 110, menciona que las instituciones únicamente pueden llevar el nombre de una persona fallecida [2], por esto, cambió su nombre a Salinas Innova School hasta la actualidad.

Al inicio no contaba con una red para administrar los diferentes departamentos que existían en sus instalaciones, no fue hasta el año 2003 donde integraron su primera intranet a través de un modem para comunicar sus computadoras mediante líneas telefónicas. A medida que la tecnología se actualizaba en Ecuador, el colegio de igual manera innovaba su infraestructura adaptando las tecnologías actuales como pantallas táctiles, proyectores, televisores, impresoras de red, computadoras y laptops modernas.

Los dispositivos operaban hasta el 2020 con redes tradicionales en la sede Salinas, mientras en la sede del cantón La Libertad, los equipos tuvieron que adaptarse a una nueva infraestructura, pero aun así operando bajo un paradigma de redes convencionales. La institución se encontraba en planes de retorno a sus instalaciones principales, pero no fue

hasta el presente año 2022 donde finalmente retornó. Se había tomado en cuenta adoptar una nueva infraestructura de red que administrará la institución, esta sería totalmente inalámbrica por las ventajas que ofrece ante una red cableada. La institución cuenta con tres laboratorios de informática, laboratorio de ciencias, rectorado, secretaría, y más de diez salones de clases funcionando bajo el paradigma de redes tradicionales.

La mayor desventaja que presentan las redes tradicionales es lograr que la infraestructura sea escalable y adaptable, donde al añadir un nuevo enrutador o conmutador para conectar computadora no represente una complejidad a la hora invertir en el presupuesto o la configuración sino que esta se vuelva rápida y eficaz para optimizar tiempo y aprovechar los recursos que existen dentro de la institución, por ejemplo, si una máquina nueva debe ser instalada, y la red se encuentra segmentada por VLANs, habría que acudir al switch donde se encuentra el departamento a ser asignada la máquina y verificar si hay interfaces disponibles en el switch correspondiente a la VLAN.

El administrador de la institución educativa en una entrevista (ver Anexo 1) mencionó que presentó problemas al tener una infraestructura física, ya que muchas veces tuvo problemas en la red por un cable en mal estado, de la misma manera se presenta este problema en la mayoría de las instituciones, incluso en organizaciones o empresas. Un cable en mal estado que conecta switch a un router para poder tener una tabla de enrutamiento a las demás redes o redes segmentadas es un error que conlleva su tiempo en solucionar, esto dependerá si la ejecución del "poncheo" de cable es correcto o si el conector RJ45 se encuentra en buen estado, y demás adversidades que se pueden presentar.

Que una red funcione de manera correcta, no significa que no se puedan realizar cambios para mejorar y quedar satisfecho con la infraestructura que se obtiene, al contrario, se debe cuestionar si es posible mejorar y optimizar para ofrecer un mejor servicio a los clientes y una mejor experiencia a la institución. El desarrollo continuo de nuevas tecnologías de red y su integración da lugar a mejores servicios de red, cómo aprovechar al máximo sus ventajas merece serias consideraciones [3]

Existe un amplio campo para el desarrollo de nuevos proyectos de investigación centrada en redes definidas por software, ya sea como herramienta para el desarrollo de nuevos servicios y aplicaciones de red, o como objetivo de estudios sobre nuevas redes, abstracciones y soluciones de implementación [4]. Se entiende que el camino de las SDN

no solo se estanca en un solo lugar, sino que tiene mucho más allá de lo que se puede apreciar, como soluciones definitivas para una calidad de servicio (QoS) aplicado a una necesidad primordial.

La arquitectura SDN tiene como principio fundamental la separación de planos de control y de datos y se basa en el protocolo OpenFlow para la comunicación entre el o los servidores controladores y los conmutadores [5]. OpenFlow es un protocolo que permite a un servidor decirles a los conmutadores de red adónde enviar paquetes que funciona dentro de un controlador de una SDN.

Entonces, aplicar una red definida por software en una institución educativa tiene varias ventajas desde el manejo de los conmutadores de red mediante un solo controlador funcionando con el protocolo OpenFlow para su debida administración separando plano de control y plano de datos haciendo que se maneje un solo plano de control para la red en general, así como también la reducción de configuración de equipos físicos o adquisición de nuevos equipos para agregar a la red.

OpenFlow se divide en tres planos: 1) Plano de datos que conmuta los paquetes a través de sus puertos. 2) Plano de control que controlar el encaminamiento de datos de la capa inferior. 3) Plano de aplicación que define las aplicaciones prácticas que necesita la red para poder encaminar eficientemente los paquetes de datos [1] permitiendo un uso más efectivo de los recursos de red de la institución.

1.2. Descripción del Proyecto

Se emulará una red definida por software para la institución educativa donde se explicarán las ventajas que presenta administrar una red mediante un solo dispositivo (controlador) que indica a los conmutadores qué salida tomar para el reenvío de paquetes evitando el tráfico de datos haciendo que solo los paquetes requeridos tengan primordial acceso, solucionar de manera eficaz los problemas que se presenten reduciendo el tiempo de demora, y teniendo un beneficio particular de ser escalable ante una infraestructura física. Eso permitirá que los administradores de red optimicen los procesos de la institución, ofreciendo una mejor experiencia a sus estudiantes, clientes y empleados.

La manera en la que se pretende realizar el presente proyecto es cumpliendo 5 etapas de la metodología PDIOO:

Etapa de planificación

En esta fase se lleva a cabo la identificación de todos los requerimientos de la red. Se analizan nuevas tecnologías y se determina la forma en que se pueden desarrollar para su uso en la red de la empresa. También habrá que tener en cuenta que se puede partir de cero o de una red en producción [6].

Etapa de diseño

En esta fase se ejecuta el planeamiento lógico y físico de la red. Hay que tomar la decisión de cuál va a ser la mejor distribución física de elementos, y a la vez, la mejor distribución lógica. Es la elaboración de un plano con la distribución lógica de la red [6]. El diseño en redes definidas por software partirá desde la red física tradicional, añadiendo sugerencias para que el nuevo modelo funcione.

Etapa de implementación

Se lleva a cabo la instalación de todo lo diseñado en la etapa anterior. Se hará estableciendo un plan de despliegue que incluirá los plazos de ejecución [6]. En la parte de implementación se pretende iniciar la emulación de la red definida por software partiendo del diseño establecido, omitiendo ciertos procesos que pueden ser erróneos u optimizados. Estos procesos sin optimizar serán tratados y corregidos en la etapa de optimización.

Etapa de operación

Se pone en funcionamiento y se prueba la red. Puede que se tenga que rediseñar algo debido a que no funcione o lo haga incorrectamente. Aquí se terminará por hacer la documentación definitiva del diseño de red, sus mapas lógicos y físicos, esquemas de direccionamiento, etc. [6]. En esta etapa se enviarán paquetes entre host y host, host y conmutadores, host y controlador para verificar que se genera tráfico de red y comprobar que esta funciona adecuadamente.

Etapa de optimización

Los posibles errores detectados son corregidos en esta etapa. Se reconfigura un dispositivo, se cambia de sitio, etc. También puede requerir un rediseño [6]. Los procesos y errores que no se optimizaron y solucionaron son analizados en esta etapa donde se

analiza qué decisión tomar, si es necesario crear o quitar equipos, si la infraestructura pensada es la correcta para aprovechar los recursos de la institución, entre otras.

Al ser un proyecto de simulación donde se tiene como finalidad presentar una nueva infraestructura de red donde se aplicarán redes definidas por software, se requiere utilizar herramientas especializadas para obtener un resultado que se acerca a la realidad de una red definida por software en total funcionamiento.

Virtualbox: es un potente producto de virtualización x86 y AMD64 / Intel64 para uso empresarial y doméstico [7].

Floodlight: es un controlador OpenFLow de clase empresarial basado totalmente en el lenguaje Java y que dispone de una licencia de Apache [8].

Mininet: red virtual realista, ejecutando kernel real, conmutador y código de aplicación, en una sola máquina (VM, nube o nativa), en segundos, con un solo comando [9].

Miniedit: interfaz gráfica idónea para experimentar con los conceptos de las SDN y OpenFlow [10].

OpenFlow: este protocolo define la comunicación entre un controlador SDN y el dispositivo y/o agente de red [11].

Wireshark: software de ayuda para la detección de tráfico de redes que verifica desde paquetes caídos hasta posibles paquetes con anomalías [12]

Este proyecto contribuirá a la línea de investigación virtualización, redes de comunicación, telecomunicaciones y soluciones informáticas, optimización de una infraestructura de red debido a que la propuesta tecnológica consiste en la simulación de una red de nueva generación con redes definidas por software.

1.3. Objetivos del proyecto

1.3.1. Objetivo general

Diseñar una infraestructura de red basándose en el paradigma de redes definidas por software mediante las herramientas Mininet, Miniedit, Floodlight Controller y el protocolo OpenFlow para la comprobación del tráfico de red generado por el plano de

control haciendo uso de la herramienta de análisis wireshark de una institución educativa perteneciente al cantón Salinas.

1.3.2. Objetivos específicos

- Implementar una máquina virtual con el sistema Floodlight en virtual box para posterior funcionamiento como controlador de red.
- Implementar un sistema de red basado en Mininet para utilización de las herramientas de diseño topológico Miniedit.
- Desarrollar una topología de red que se adapte a las instalaciones de la institución educativa con Miniedit
- Comprobar el plano de control generando tráfico de red enviando paquetes entre host para análisis con wireshark.

1.4. Justificación del proyecto

Este proyecto se basa en emular una red de una institución educativa aplicando conceptos, estrategias y protocolos basados en redes definidas por software, acogiendo los beneficios que trae este nuevo modelo que presenta un gran cambio en la evolución de la red, como el que supuso la sustitución por Ethernet e IP del modelo SNA (System Network Architecture) de IBM, pero con la diferencia de que la industria lo está asumiendo mucho más rápido. Debido a que al mantener la red y SDN libre permite que los desarrolladores puedan operar con total libertad en código abierto y así generar un sin número de soluciones, presentando como una de las principales a Openflow [13].

En una encuesta realizada por el portal Gigaom [14], los beneficios más relevantes que presentan las redes definidas por software son:

1. Habilitación de la programación de la red bajo demanda.
2. Aprovisionamiento acelerado de nuevos clientes y servicios.
3. Bajo costo de inversión.
4. Bajo costo de operación.
5. Simplificación en el despliegue y operación de la red.
6. Altos niveles de utilización de la red.
7. Fortalecimiento de la seguridad de la red

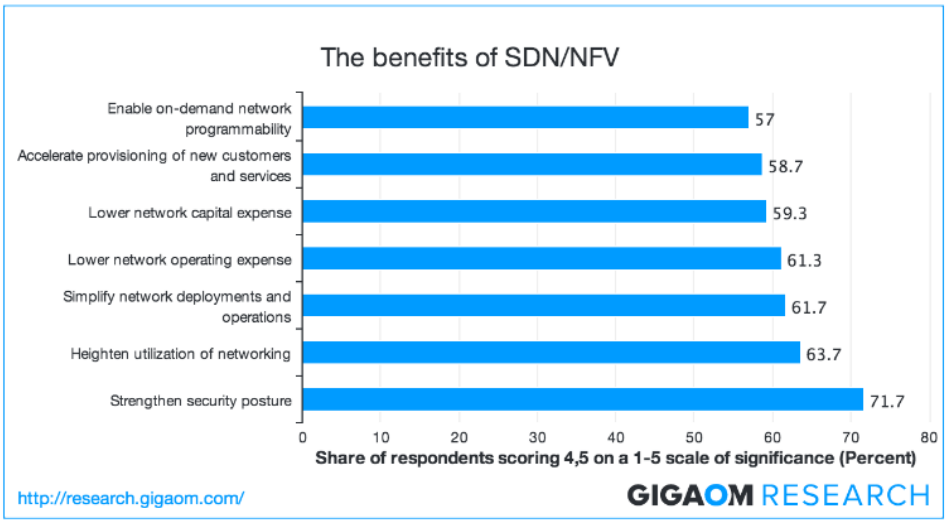


Figura 1. Beneficios de SDN

En la actualidad las instituciones educativas que pertenecen al cantón Salinas ya sean públicas o privadas, manejan una infraestructura de red donde cada equipo se administra de manera individual, es decir, las configuraciones deben ser realizadas dentro del mismo equipo. Un firmware para cada dispositivo físico. Una red que es administrada equipo por equipo funciona bien, pero se puede optimizar y mejorar, ya que, al ser definida por software, un solo controlador es el responsable de administrar toda la infraestructura y los equipos pertenecientes a esta, ordenando a los paquetes qué entrada y salida deben de tomar para llegar a su destino.

En la etapa de **planificación** permitirá seleccionar la tecnología a utilizar para crear el modelo que partirá de la red ya operativa de la institución con fines orientados a red definida por software, es aquí donde se identificarán factores escalabilidad, adaptabilidad, disponibilidad y redundancia, tráfico de red, entre otras. La etapa de **diseño** ofrece una vista de la red desde un punto lógico, un esquema o bosquejo de lo que sería la topología de red que se adecua a los recursos y la estructura del lugar, también ofrece el diseño de un esquema físico de donde irían situados los dispositivos de la red.

Dentro de la etapa de **implementación** se levanta la red para el debido funcionamiento, es aquí donde se inician las herramientas que se utilizarán para el nuevo modelo de red que se ofrecerá, situando los equipos requeridos en espacios con ventilación donde no exista el riesgo de sobrecalentamiento en caso de un modelo SDN físico. En la **operación** se puede establecer conexión con los demás equipos de la red y se podrá monitorear el tráfico que se genera a medida que se envían paquetes de un host a otro en diferentes

segmentos de red con herramientas como wireshark, también se podrá comprobar el consumo de ancho de banda.

En la última etapa de **optimización** se corrigen errores que se hayan presentado como mal asignación de direcciones IP en un segmento o si se puede se optimiza la red adaptando un nuevo diseño o mejorando el actual. En esta etapa se puede llegar a un acuerdo mezclando SDN y redes convencionales. Segmentar por VLANs una vez se haya realizado subnetting a una única IP que se dividirá en subredes para cada departamento. También se puede elegir otro tipo de tecnología o herramientas para concluir el levantamiento de la red de la institución.

Implementar una red definida por software en instituciones educativas traen consigo la ventaja de disminuir el presupuesto que se invierte en actualización, reparación, soporte, cableado, conectores y energía eléctrica para encender los equipos ya que varios dispositivos serían virtualizados, pero también y como punto más importante, mejora el tiempo de respuesta ante una escalabilidad limitada en redes tradicionales, pues no se adquirían nuevos equipos de capa 2 para poder levantar la red. La ventaja de usar la Mininet y Mininet es que se pueden crear diferentes topologías. Con OpenFlow se puede administrar una red de conmutadores donde se determina el mejor camino que deben seguir los paquetes que se están enviando (plano de control).

A partir de este proyecto, se dejan puertas abierta para seguir mejorando una red aplicando más herramientas de redes de nueva generación, como por ejemplo, que todos los equipos de una organización trabajen bajo un solo servicio que englobe radio, satélite, internet, etc., o mezclar conceptos de SDN y redes convencionales para aprovechar al máximo la tecnología de antes con la nueva generación de redes que se avecina.

El presente proyecto está direccionado al plan de creación de oportunidades del presidente de la república del Ecuador, Guillermo Lasso, haciendo énfasis en la directriz 1, lineamiento territorial A4, y en el objetivo 5, política 5.5.

Directriz 1: Soporte territorial para la garantía de derechos [15].

Lineamiento territorial A4: Fortalecer la conectividad y el acceso a las TIC como una vía para mejorar el acceso a otros servicios [15].

Objetivo 5: Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social [15].

Política 5.5: Mejorar la conectividad digital y el acceso a nuevas tecnologías de la población [15].

1.5. Alcance del proyecto

La emulación de una infraestructura nueva con redes definidas por software basadas en redes de nueva generación permitirá que la directiva de la institución educativa del cantón Salinas tenga una perspectiva nueva de cómo podría operar la red gestionada por un solo controlador evitando problemas de incompatibilidad de los mismos equipos o problemas físicos que se pudieran presentar dentro sus instalaciones. Además de dar un significado más amplio a la escalabilidad de red, donde para situaciones educativas o de investigación se podría generar un conmutador de red en el momento que se lo requiera.

Gracias a esta simulación se podrá considerar la implementación de manera oficial de una red definida por software por primera vez dentro de una institución educativa privada, convirtiéndose así en pionera de esta nueva tecnología para mejorar considerablemente la manera de transmitir datos al separar los planos de control y de datos, controlando un solo plano de control en toda la red, ordenando el mejor camino o ruta de entrada y salida para que los paquetes lleguen a su destino.

El proyecto para su ejecución consta de 5 etapas sugeridas por la metodología PDIOO:

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

La emulación también permitirá ver como se genera el tráfico de red con ayuda de la herramienta Wireshark como si se tratara de una red ya implementada dentro de la institución dando la oportunidad de estudio de los paquetes que viajan de un host a otro con la finalidad de aplicar calidad de servicio para los protocolos que sean primordiales y así no presentar latencia en la red en próximos estudios. De la misma manera se podrá comprobar el funcionamiento del plano de control de Floodlight.

Cabe recalcar que este proyecto no será implementado de manera oficial dentro de las instalaciones de la institución para reemplazo de la infraestructura de red con la que se

opera actualmente, sino crear una nueva perspectiva de funcionamiento de toda una red administrada por un solo equipo o controlador de red.

1.6. Metodología

1.6.1. Metodología de la Investigación

El presente proyecto se llevará a cabo aplicando una metodología de investigación de estudio exploratorio con el objetivo de examinar el tema propuesto para aclarar dudas sobre su implementación [44]. La red definida por software que se simulará basado en un infraestructura real y actual de la institución educativa del cantón Salinas no ha sido implementada por el departamento de TI. Por este motivo se realizará una investigación para la recolección de información entre el funcionamiento de una red tradicional ante una red nueva generación, más específico, una red definida por software, extrayendo información de referencias bibliográficas confiables y entrevista al encargado de la administración de la red de la institución a analizar.

Mediante la entrevista respectiva al administrador de red de la institución educativa, se planea obtener información si es posible reducir el tiempo de respuesta ante una escalabilidad de una red física comparada con una red definida por software, incluyendo el tiempo de demora de mantenimiento y actualización de los equipos que actualmente pertenecen y hacen funcionar la red. Estos puntos mencionados conllevan un tiempo de solución demorado para que una red tradicional pueda funcionar de manera eficiente. Por ello, para enriquecer la información a utilizar como el tiempo de adquisición de los equipos que se utilizan y el tiempo empleado para la configuración del mismo, se aplicará una metodología de la investigación de tipo diagnóstica [44].

Con la propuesta sugerida se busca resolver problemas de escalabilidad de la red evitando un tiempo de demora exagerado entre la adquisición, configuración y conexión del conmutador para fines de investigación o académicos.

1.6.2. Metodología del proyecto

Metodología de ciclo de vida de las redes mediante el modelo PDIOO

Para el desarrollo de este tema se plane utilizar el ciclo de vida de una red bajo el modelo PDIOO (planificar, diseñar, implementar, operar y optimizar) puesto que se puede adaptar a una red ya en funcionamiento o bien iniciar un nuevo diseño de red para estructurar de una manera lógica las diferentes tareas a llevar a cabo durante el ciclo de vida de la red.

El modelo ofrece 6 fases oficiales siendo la última la fase de "retirar". Esta fase se utiliza cuando la red ya no va a ser optimizada para dar un fin al ciclo de vida de la red. CISCO adapto este modelo agregando una fase antes de la fase de planificar para agregar una fase de "preparar". Dentro de este proyecto se ocuparán 5 fases primordiales descartando la fase 6 de "retirar" para dejar puertas abiertas a nuevas optimizaciones.

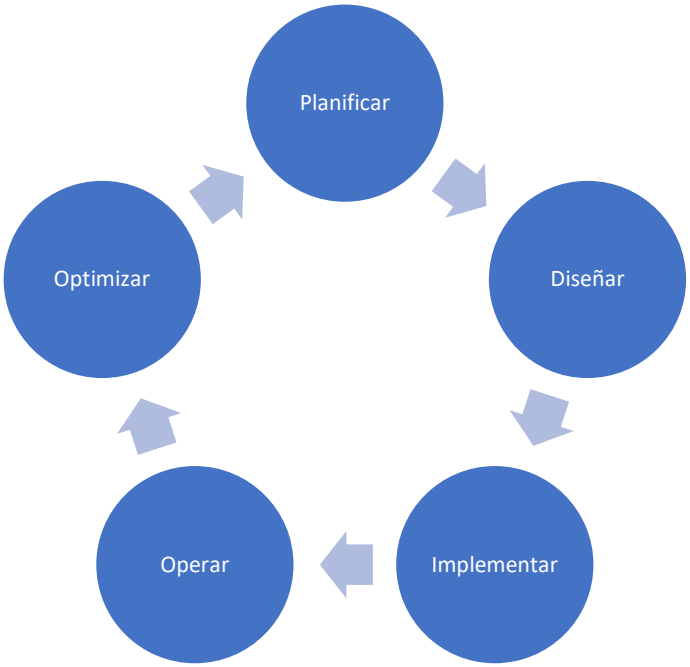


Figura 2. Modelo PDIOO Ciclo de vida de una red

Planificar: para la institución educativa se deberá analizar los equipos que se utilizan para el funcionamiento de la red, y seleccionar un dispositivo que actúe como controlador que esté en perfecto estado funcionando sin descanso como si de un servidor se tratará. Dentro del dispositivo seleccionado se instalará el software requerido para utilizar las herramientas mencionadas anteriormente.

Diseñar: el nuevo diseño de red definido por software partirá de la red actual de la institución. No se creará un nuevo diseño. Se adaptará la infraestructura física a una

infraestructura virtual sustituyendo equipos o agregando nuevos conmutadores sin necesidad de invertir en un presupuesto.

Implementar: teniendo el diseño lógico y/o físico de la red, se procederá a levantarla mediante una emulación donde se comprará la efectividad de las etapas anteriores y que esta funcione sin inconveniente con la posibilidad de lograr comunicar host entre ellos y al controlador. De presentarse algún error inesperado, se lo corrige en una próxima fase.

Operar: se comprueba la efectividad de la red que se instará en la institución educativa. Se revisará el tráfico de red generado haciendo un ping entre host y al controlador para evidenciar el viaje de los paquetes, tiempo de latencia, banda ancha consumida, protocolos en funcionamiento, anomalías, entre otras. El objetivo es que los paquetes puedan ser enviados y recibidos si presentar algún inconveniente.

Optimizar: los errores que se presentaron al levantar la red serán corregidos en esta etapa, como un posible mal diseño lógico, de ser necesario ser creará uno nuevo o se corregirá el ya antes planificado. Asimismo se optimizará la red como ofrecer ancho de banda a servicios necesarios, quitar o agregar elementos en caso de requerirse. Si los resultados obtenidos no son los esperados, se puede volver a la etapa de diseño.

1.6.3. Técnicas de investigación

Se describe la manera en que se obtuvo la información requerida para continuar con el proyecto detallando la técnica de investigación, población, muestra e individuo:

Técnica	Entrevista
Población	Institución educativa del cantón Salinas
Muestra	Departamento de TI
Individuo	Administrador de red

Entrevista	Se utilizará esta técnica como método de recolección de información mediante la resolución de un banco constituido por siete preguntas

Institución educativa	Será el lugar físico del cantón Salinas en el que se tomará el diseño arquitectónico para diseñar una infraestructura lógica y/o física para emulación del proyecto
Departamento de TI	Departamento seleccionado de la institución educativa del cantón Salinas donde se seleccionará un único individuo para obtener información del funcionamiento de la red
Administrador de red	Encargado de resolver problemas, actualizar firmware y brindar soporte y mantenimiento a los equipos de red. Individuo al que se le realizarán las preguntas.

1.6.4. Análisis de la información recolectada de la entrevista

Pregunta 1. ¿En qué año se implementó la primera red y cómo fue su funcionamiento?	
Resumen:	La primera red implementada dentro de la institución educativa fue una intranet. Los equipos lograban la comunicación entre ellos mediante un modem.
Conclusión	Para el año 2003 lograron la comunicación únicamente entre dispositivos perteneciente a la institución. Nacimiento de una red informática para optimización de la organización.

Pregunta 2. ¿En qué año implementaron redes tradicionales?	
Resumen:	En el 2010 fue la implementación de redes tradicionales. Funcionaba con enrutadores y conmutadores que segmentaban la red por departamentos,
Conclusión	Con la llegada de redes tradicionales, la institución educativa vio oportunidades de mejorar la red adquiriendo nuevos equipos para una infraestructura funcional y segura.

Pregunta 3. En la sede cantón Salinas, ¿todos los dispositivos se conectaban a la red?	
Resumen:	La institución contaba con ciertos dispositivos que se podían conectar a la red. Existían periféricos que portaban tarjeta de red y otros que no, como televisores.
Conclusión	Los dispositivos como periféricos de salida de proyección visual son requerimiento fundamental para impartir clases reemplazando proyectores por una mejor calidad de imagen.

Pregunta 4. ¿Presentaron problemas con la red al ser una red cableada?	
Resumen:	Existían ocasiones en los que un cable de red presentaba fallos por su mal estado, conectores RJ45 averiados por golpes por parte de los estudiantes de manera intencional y no intencional.
Conclusión	Uno de los principales problemas que presenta las redes cableadas es el descuido del medio por donde viaja la información que se comparte. Para este caso el cable de red

Pregunta 5. ¿Se presentaron problemas o demoras de configuración de la red?	
Resumen:	Existían problemas de demoras al ponchar un cable de red cuando los pines no encajaban de manera correcta con el conector RJ45 y el alcance del mismo cable.
Conclusión	Las redes cableadas presentan problemas en el medio de transporte de red si es que no se ejecuta un correcto poncheo con las normas requeridas.

Pregunta 6. ¿Cómo funciona la red de la sede del cantón La Libertad comparado con la red de la sede del cantón Salinas?	
Resumen:	La red de la sede del cantón La Libertad es una red inalámbrica administrada por mikrotik, y la red que funcionaba en el cantón Salinas era una red cableada en su mayoría.
Conclusión	La red inalámbrica implementada en la sede del cantón La Libertad funciona igual que una red tradicional sin resolver el problema de escalabilidad.

Pregunta 7. ¿Por qué optaron por redes inalámbrica para la sede del cantón Salinas?	
Resumen:	Para reutilización de los equipos que actualmente están operativos en la sede del cantón La Libertad y los beneficios que esta presenta ante una red cableada.
Conclusión	La reutilización de equipos evita la adquisición de equipo nuevo mitigando un presupuesto elevado, pero sigue sin resolver la escalabilidad siendo problema para el futuro.

CAPÍTULO II

2. La propuesta

2.1. Marco Contextual

2.1.1. Unidad Educativa Salinas Innova School

El colegio particular Salinas Innova School, más conocido por la comunidad estudiantil como Innova se encuentra ubicado en el cantón Salinas en la vía principal que conecta con el cantón La Libertad. Es conocido por su bachillerato internacional, un programa dirigido a los estudiantes de 16 a 19 años que cursan el Bachillerato en las instituciones autorizadas como Colegios del Mundo BI; con su programa y propuesta, pretende lograr un proceso de enseñanza-aprendizaje efectivo y eficaz que cumpla los estándares internacionales [16].

Cuenta con cursos extracurriculares para sus propios estudiantes en los que destacan el club de deportes y club de arte y música, además de un sistema educativo de blended learning, método que posee dos tiempos: 1) solo learning, y 2) group learning [17]. Los cursos se realizan para obtener el mejor rendimiento de los estudiantes, beneficiando a la institución por participar en eventos intercolegiales, cantonales, intercantonales y nacionales [17].

Estudiar dentro de la unidad educativa conlleva a pagar una mensualidad dentro de cada año que el estudiante pertenezca al colegio y ofrece media beca para estudiantes con promedios sobresalientes [17]. A causa de la pandemia del Covid-19, el exrector tuvo su deceso dejando así la unidad educativa a cargo de su hijo Julio Guamantica y su familia.

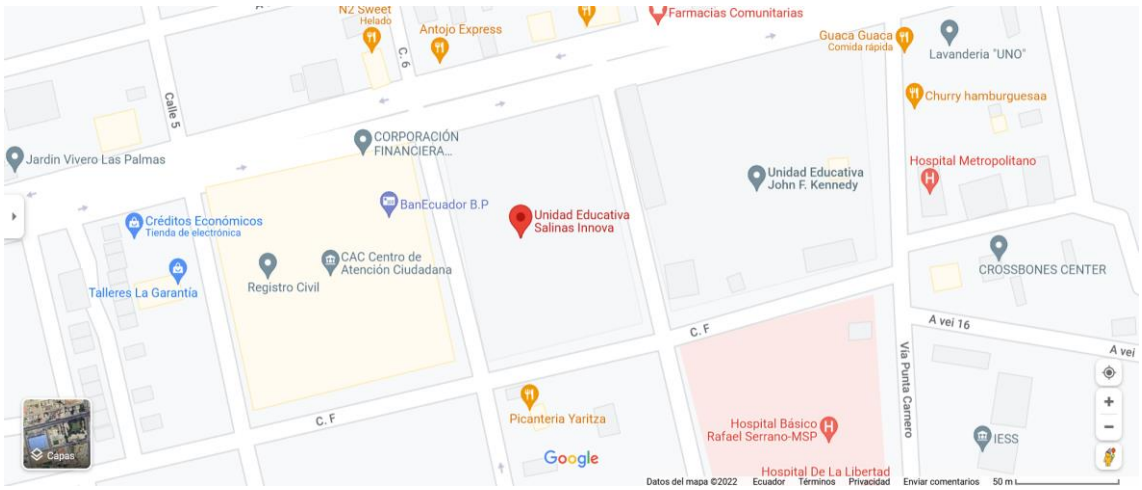


Figura 3. Ubicación de la institución educativa

MISIÓN

Brindar una educación de calidad con excelencia en los procesos académicos y administrativos, desarrollando programas internacionales con personal capacitado que aplica una formación constructivista desde un enfoque humanista, respondiendo a la filosofía de los colegios del mundo [17].

PRINCIPIOS

Formar jóvenes solidarios, informados y ávidos de conocimiento, capaces de contribuir a crear un mundo mejor y más pacífico, en el marco del entendimiento mutuo y el respeto intercultural [17].

2.1.2. Uso de redes convencionales

En el inicio las redes de telecomunicaciones se implementaban utilizando tecnologías basadas en técnicas de conmutación de circuitos [18]. En este tipo de redes, al retener un circuito dedicado para cada comunicación, se cuenta con retardo mínimo y fijo, y también se asegura que no pueda existir congestión para las comunicaciones ya establecidas [18].

Las redes basadas en técnicas de conmutación de paquetes se diseñan utilizando algoritmos estadísticos [18]. Estas redes son las más eficientes, y están adaptadas para bridar servicio a la mayoría de las aplicaciones, pero el retardo variable y la posible pérdida de información, pueden generar problemas al tráfico sensible a estos parámetros [18].

La red que funciona en la institución educativa se basa en redes tradicionales, es decir, una red que se comunican entre sí con dispositivos físicos que administran su propio plano de control y de datos, y si la organización quisiera cambiar o adaptar su red por consecuencia de alguna aplicación, nuevos dispositivos o cambio de topología, las redes tradicionales no pueden adaptarse a estas situaciones sin una reprogramación masiva del todos los dispositivos de la red [19]

2.2. Marco Conceptual

2.2.1. Redes Informáticas

Las redes de telecomunicaciones que transportan información de diversa índole, en su gran mayoría en un formato digital independiente de su naturaleza, han crecido de una manera muy rápida en las dos últimas décadas [20]. Este crecimiento trajo aparejado la utilización de velocidades muy elevadas, grandes anchos de banda y una variedad importante de medios físicos de transmisión [20].

Para hacer posible la comunicación entre computadoras de diferentes partes se requiere de un enlace que interconecte estos dispositivos, para ello las redes pueden clasificarse en PAN, LAN, MAN Y WAN [21]. Una red está constituida por equipos llamados nodos además de que las redes se categorizan en función de su amplitud y de su ámbito de aplicación [21].

2.2.2. Redes de Nueva Generación

Las Redes de Nueva Generación (NGN abreviado por su significado en inglés *Next Generation Networks)* probablemente se crean por medio de diferentes Tecnologías, por nombrar, la fibra óptica, satélites, por cable, Inalámbrica, fija y móvil, o a través del refuerzo de las líneas de cobre actuales [22]. Variedad de industrias ya han empezado a instaurar las NGN en las naciones desarrolladas, entre ellos Japón, la República de Corea y algunos estados de EEUU. y Europa Occidental. [22]

Las ngn buscan optimizar los conceptos de una red convencional. El portal SeverVoIP define a las ngn como aquellas basadas en paquetes que permite prestar servicios de telecomunicaciones con QoS garantizada, con movilidad y que permite la convergencia de servicios y aplicaciones [23]. Este modelo de arquitectura de Redes permite desarrollar toda gama de servicios IP multimedia; por ende, la función de NGN se basa en generar una evolución para pasar de un sistema de telecomunicaciones a otro [23]. Las ngn también tienen como propósito incluir todos los servicios como voz, video, multimedia, datos o cable en una sola red.

2.2.3. Redes Definidas por Software

El paradigma de las redes definidas por software se caracteriza por separar el plano de control y el de datos de los conmutadores de red para ser controlado por un único dispositivo que administra la red en general, es decir, un solo plano de control para toda la red y no uno por equipo como resuelven las redes convencionales, ofreciendo las ventajas de que sea una red flexible, programable, administrable y rentable [24].

Las SDN son tema de investigación que van tomando fuerza en los sectores laborales donde se requiere cada vez que la red sea escalable.

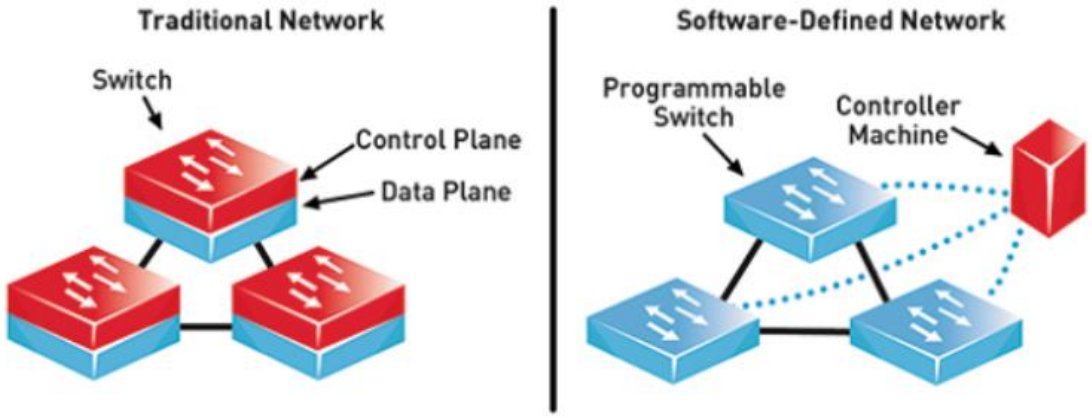


Figura 4. Imagen referencial de planos de control y datos de redes tradicionales y SDN

Las aplicaciones SDN proporcionan un control centralizado de la red políticas y reglas. Además, también ofrecen una variedad de funciones que permiten a los administradores resolver eficazmente problemas de red con métodos ML [25]. Al mismo tiempo, el control y la gestión del tráfico de red se implementan en función de sobre métodos ML en la arquitectura SDN [25].

2.2.4. Plano de Control

El plano de control SDN tendrá procesos fuertes después del desacoplamiento, y proporcionará mayor velocidad y flexibilidad en las instrucciones de enrutamiento y la energía administración de equipos de red como enrutadores e interruptores [25]. Es administrado por un único dispositivo que posee un software centralizado denominado controlador. Algunas de estas tablas son, la tabla de enrutamiento IP, la tabla MAC, la tabla ARP, la tabla STP [26].

2.2.5. Plano de datos

El plano de datos se refiere a todas las actividades que ejecuta un equipo para enviar la data mediante encapsulación de tramas, asociación de tramas con la tabla de envíos IP, filtrado de datos vía ACL o por security [26]. Reenvía los paquetes entrantes (es decir, el tráfico) en función de la decisión tomada por el plano de control [27].

2.2.6. Switch o conmutador

Es un dispositivo que nos permitirá interconectar los distintos equipos y nodos en una red, siempre cableada [28]. Mantiene una tabla de reenvío de puertos de Control de Acceso al Medio (MAC, Media Access Control) y realiza tres funciones importantes: 1) Busca el MAC de destino de cada cuadro cuando llega, 2) Reenvía un marco a uno o más puertos para la transmisión. 3) Evita entregas innecesarias [29].

2.2.7. Controlador de red

El controlador constituye un aspecto clave de las redes de sensores definidas por software, cuya función principal de este componente de la arquitectura SDN es la generación de las reglas para las tablas de flujo en los nodos [30]. Para esto, mantiene una vista actualizada del estado y topología de la red donde el controlador intercambia mensajes de supervisión con los nodos que le permiten adquirir información sobre los conmutadores vecinos y estado de los enlaces, entre otros [30].

El controlador de red es la aplicación que se comunica con los dispositivos y aplicaciones de red en una red definida por software [31]. Sirve como el núcleo de la red al conectar las capas de aplicaciones y de infraestructura, controlando el flujo de datos entre las API ascendente y descendente [31].

Puede detectar la capacidad de los recursos y los requisitos de la red desde una perspectiva global. Así, la introducción de SDN mejora el control de los recursos de red y permite la automatización de la gestión. su manejo de recursos logra un control unificado sobre múltiples tipos de recursos tales como computación, almacenamiento y redes, y satisface las necesidades de entrega de recursos en escenarios empresariales [25].

2.2.8. Floodlight

Floodlight es dos en uno, controlador más colección de aplicaciones que funcionan en Floodlight Controller, donde el controlador controla la red y las aplicaciones proporcionan funcionalidades comunes que los usuarios necesitan [32]. Floodlight es un controlador profundo basado en Java, con capacidad de actualización y expansión, siendo la principal razón por la que se lo utiliza como herramienta para pruebas y experimentos de ataque DDOS [32].

2.2.9. Mininet

El éxito de Mininet proviene de su capacidad para emular potencialmente grandes redes en una máquina, gracias a la virtualización ligera técnicas y una API simple pero poderosa [33]. Mininet fue diseñado para ejecutarse en una sola máquina, asume que todos los recursos son compartidos y directamente accesibles desde cada componente de un experimento [33]. Éste utiliza el kernel de Linux y otros recursos para emular elementos de la SDN como el controlador, los switches OpenFlow y los hosts [34].

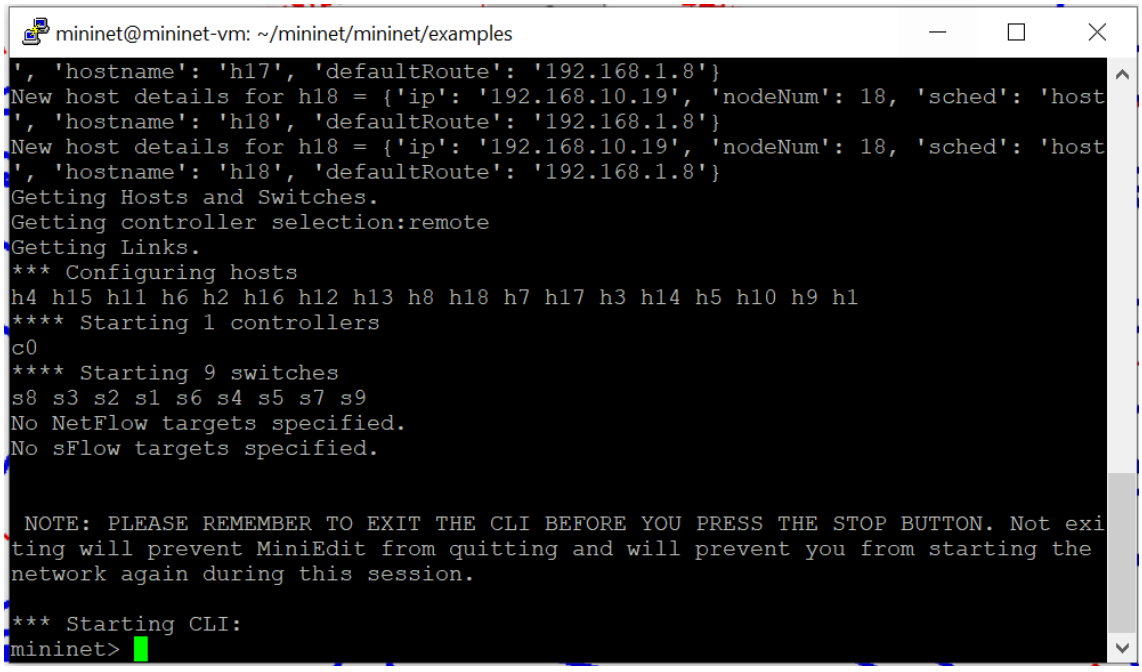


Figura 5. Acceso a mininet mediante putty

2.2.10. Miniedit

Miniedit es una extensión de Mininet, que nos permite crear redes de forma sencilla sobre un terminal gráfico alojado en el directorio examples [35]. Esta interfaz facilita la creación de redes, realizándose la programación de las mismas en un segundo

plano a priori oculto para el usuario, pese a ello esta plataforma presenta ciertas limitaciones en comparación con todas las capacidades que presenta el propio Mininet [35].

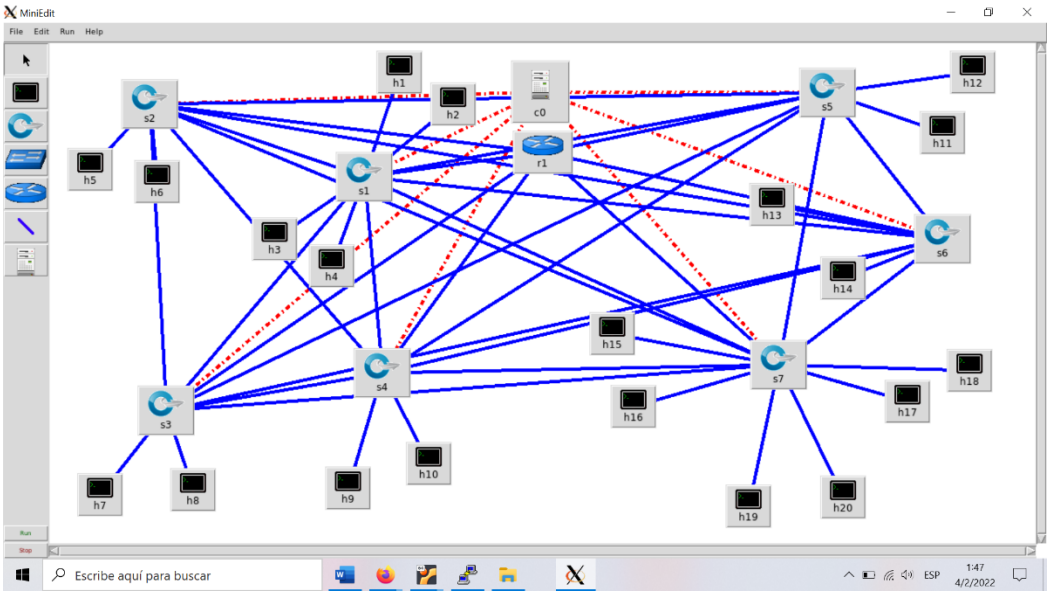


Figura 6. Vista de la topología desde miniedit

2.2.11. Protocolos

Los protocolos de red son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red [36]. Definen el formato y el orden de los mensajes intercambiados entre dos o más entidades que se comunican, así como las acciones tomadas al producirse la transmisión y/o recepción de un mensaje u otro suceso [37].

Los distintos protocolos de red se organizan en capas, es decir un protocolo en una capa determinada sólo puede comunicarse con el protocolo inmediatamente superior o inferior, si los hubiera, pero no con el resto [38].

2.2.12. Openflow

El protocolo OpenFlow fue originalmente propuesto como una alternativa para el desarrollo de protocolos experimentales en el campus de una universidad, en donde es posible probar nuevos algoritmos sin interrumpir o interferir con la normal operación del tráfico y surgió a raíz del proyecto de investigación “OpenFlow: Enabling Innovation in Campus Networks” en la universidad de

Stanford en el 2008 [39]. El protocolo OpenFlow ayuda que una red pueda ser gestionada en su totalidad mediante un servidor que les indica a los switches donde enviar el paquete [40].

La Open Networking Foundation (ONF) define a OpenFlow como el primer estándar para interfaces de comunicación definido entre los planos de control y de datos en una arquitectura SDN y permite acceso directo y manipulación del plano de datos de los dispositivos tales como switches y routers de una red [41]. Las tecnologías SDN basadas en el estándar OpenFlow permiten ofrecer un alto ancho de banda, adaptarse a los constantes cambios de necesidades del negocio y reducir significativamente la complejidad de la administración de la red [41].

2.3. Marco Teórico

2.3.1. Importancia del estudio del paradigma de redes definidas por software

Junto con la virtualización de servidores, muchas compañías también están utilizando una sola red para entregar todas las necesidades de red de voz, video y datos que tienen, teniendo la necesidad de proporcionar un nivel diferenciado de servicio para diferentes aplicaciones, lo cual es conocido como calidad de servicio (QoS) [42]. En la arquitectura de red tradicional, el aprovisionamiento de muchas herramientas QoS en la mayoría de los casos se realiza de manera manual, y el administrador de la red debe configurar el dispositivo de cada proveedor por separado y ajustar parámetros como el ancho de banda de la red y la calidad de servicio en cada sesión por aplicación, esto demanda tener el conocimiento de la configuración de cada dispositivo por cada proveedor que posea [42].

En la revista Conaic presentan un artículo donde menciona que las redes actuales no están preparadas para afrontar una serie de situaciones cada vez más comunes como: cambios de patrones de uso de la red debido a los usuarios móviles con nuevas aplicaciones, despliegue de nuevos servicios, y ampliaciones o cambios en la topología de red [19]. Se entiende dentro de este concepto que hasta el cambio físico de una red tradicional podría afectar la utilidad de esta.

2.3.2. ¿Por qué realizar un diseño SDN en una institución educativa particular del cantón Salinas?

Las SDN han transformado radicalmente la industria de las redes de comunicaciones gracias al despliegue, mantenimiento y gestión de servicios de red de forma dinámica y escalable, permitiendo al administrador de red operar a alto nivel desde un único punto lógico de control [43]. Este tipo de tecnologías suponen un cambio de paradigma en las arquitecturas de red y la industria de las redes de datos actuales, ya que sea parte de un modelo distribuido con hardware y software propietario de empresas como Cisco, Juniper, Avaya, HP, NEC, y organismos de estandarización clásicos (IETF, IEEE), a un modelo con un control centralizado utilizado por grandes empresas tecnológicas como Google o Telefónica y certificado por la Open Networking Foundation (ONF), empleando además hardware y software libre [43].

Se otorga mejor control de los equipos que estén conectados o bajo control del controlador floodlight, siendo capaz de administrar todos los dispositivos de red que tengan habilitado Openflow [42]. SDN brinda la oportunidad a los investigadores de desarrollar las líneas de investigación en el campo de la automatización de la red, seguridad de las redes de forma proactiva, convergencia en la red y desarrollo de aplicaciones proactivas de QoS [42].

La automatización de la gestión y provisión de la red, a través de SDN, es la siguiente fase en la virtualización de la infraestructura de tecnologías de la información y las telecomunicaciones ya que permite crea una red inteligente mucho más abierta, flexible, escalable y reprogramable [42].

2.4. Requerimientos

R01. Espacio para instalación del controlador Floodlight

Para realizar la instalación del controlador de red, se requiere implementar una máquina virtual donde se alojará el sistema. Los requisitos que se necesitan en la máquina virtual para esta instalación son:

Almacenamiento:	8 GB
RAM:	1 GB

Tipo:	Ubuntu
Sistema:	Floodlight-v1.1+Mininet.vmdk

R02. Espacio para instalación del sistema Mininet

Como se ha establecido en este proyecto, el sistema Mininet se instala de manera individual a Floodlight para hacer uso de su herramienta gráfica topológica Miniedit. Los requisitos que se necesitan en la máquina virtual para esta instalación son:

Almacenamiento:	8 GB
RAM:	1 GB
Tipo:	Ubuntu
Sistema:	Mininet-vm-i386.vmdk

R03. Adaptador puente para las máquinas virtuales

Al tratarse de una virtualización las máquinas requieren una configuración de red para que puedan intercomunicarse entre sí y obtener servicios de internet, para ello dentro de las configuraciones de red de cada máquina virtual el adaptador deberá estar funcionando como adaptador puente y así hacer uso de la misma red que se utiliza en el ambiente físico asignando así una IP propia del router.

R04. Topología de red

Dentro de la funcionalidad de la red se requiere un diseño de la estructura gráfica que formarán los equipos al conectarse al controlador de red, para ello la topología debe ser analizada con los nodos conectados directamente entre sí y al controlador. La finalidad de la topología es que todos los equipos puedan comunicarse aun perteneciendo a otro segmento o subred.

R05. Subnetting VLSM

El “Subneteo VLSM” es una técnica que consiste en dividir una dirección IP en subredes con el propósito de no utilizar direcciones IP innecesarias por segmento de red, sino la

cantidad justa que requiere. Se utiliza este método para dividir por red a los departamentos existentes en la institución y sus equipos correspondientes. De esta manera no se desperdician direcciones que podrían ser asignadas a futuros equipos.

R06. Conexión remota a Mininet

Para realizar la conexión remota a Mininet se deberá hacer uso de la herramienta Putty, de esta manera se podrá acceder a la herramienta topológica Miniedit y realizar diseños de topográficos en una venta auxiliar aparte, así las opciones de agregar y quitar equipos se tornan más sencillo.

R07. No se ocuparán equipos físicos

Este estudio únicamente será realizado en un ambiente simulado con virtual box, es decir, el controlador Floodlight y el sistema Mininet estarán virtualizados únicamente. Los hosts que se utilizan para realizar la prueba ping serán los que se generen en la topología de red con la ayuda de Miniedit. Los hosts generan su propio CLI para poder ejecutar ping.

R08. Levantamiento de servidor http de floodlight

Para observar como funciona el plano de control del controlador floodlight es necesario realizar el levantamiento del servicio http que el controlador tiene integrado. Se requiere ingresar el comando para posterior acceso mediante la IP asignada al controlador para observar topología, equipos y plano de control.

R09. Plano de control de datos

El plano de control de datos debe ser revisado para comprobar que el paradigma de redes definidas por software separa correctamente el plano de control y el plano de datos. Debe mostrar el puerto por donde ingresa y sale el paquete de un conmutador de origen y de la misma manera el puerto de ingreso y salida del conmutador de destino.

2.5. Componentes de la propuesta

2.5.1. Etapas del ciclo de vida de una red. Modelo PDIOO

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 [1]. La etapa de planificación recolectará la información necesaria de los recursos que se puedan necesitar o adquirir, así como recursos que ya posea la institución para evitar costos elevados al momento de levantar la red. Es aquí donde se toman decisiones como realizar el proyecto partiendo del diseño de la red ya establecida o por otro lado, iniciar un nuevo diseño con las tecnologías seleccionadas o realizar una infraestructura híbrida entre tecnología de red tradicional o nuevas tecnologías de redes.

Dentro de la metodología del proyecto usando el modelo PDIOO señalan ciertos factores a tomar en consideración para la planificación de la red que serán analizadas desde el punto de vista de una red definida por software [1]:

- Conexiones simultaneas de usuarios y/o máquinas
    - Se dejo establecido el número de equipos que existen en dentro de la institución como máquinas para administración de procesos contables o financieros pertenecientes a los departamentos existentes dentro de la institución. Asimismo equipos con fines educativos como los que se encuentran en laboratorios de computación, laboratorio de ciencias, biblioteca, entre otras.
    - En una red definida por software donde los conmutadores son virtuales, se planificó la posición de los departamentos y laboratorios para crear un switch donde los hosts reconocidos tengan comunicación entre sí y puedan intercambiar datos con ayuda del controlador.
- Aplicaciones que se van a utilizar en la red
    - Se tomó en consideración los tipos de aplicaciones que se utilizan para gestionar la institución educativa como los procesos de pago de mensualidades, matriculas, graduaciones, etcétera.
- Escalabilidad
    - Al ser una SDN la nueva tecnología para redes que se seleccionó, la escalabilidad queda cubierta para futuros problemas que puedan

presentarse como falta de conmutadores de red ofreciendo mayor cantidad de quipos al mismo costo incluso menor.

- Adaptabilidad
    - Como paso primordial para el funcionamiento de la SDN, se debe asegurar que el dispositivo donde se instalará el controlador funcione adecuadamente y floodlight no presente problemas de latencia por las características del equipo seleccionado.
    - Se debe optar por una planeación donde futuras tecnologías o tecnologías actuales puedan interactuar con la SDN.
- Servicios de red y tipo de tráfico
    - Se toma en cuenta el tipo de servicio de red que más utilizará la institución educativa como voz, videoconferencias, datos, entre otros servicios. Cabe aclarar que las SDN al pertenecer a las redes de nueva generación, es posible unificar todos los servicios en uno solo.
- Disponibilidad y redundancia
    - La red definida por software debe estar en capacidad de corregir fallos que se presenten en la red, y de igual manera debe ser accesible y fácil manejo para los administradores de network en caso de requerir la creación de otro conmutador si la red empieza a crecer.
- Coste y duración de recurso
    - Los costes que se deben tomar en cuenta para el levantamiento de la red deben ser destinado al alojamiento del controlador para que sea seguro y se prevengan cualquier tipo de daño físico que se pueda presentar.
    - El presupuesto para la integración de los conmutadores no representaría un problema ya que al ser virtualizados se pueden crear tantos como lo necesite la infraestructura.
- Requisitos
    - Se debe tomar en cuenta la seguridad de la red
    - Segmentos de red a utilizar
    - Tomar en consideración el número de host

Los equipos que posee la institución funcionan correcta y operativamente dentro de las instalaciones. El controlador será ubicado en el departamento de sistemas cerca de los laboratorios de computación y el laboratorio de ciencias. Los equipos tendrán

comunicación directa con el controlador de red para intercambio de datos entre toda la institución para el funcionamiento correcto.

Los recursos que posee la institución son:

1 ROUTER	**UBICADO EN EL DEPARTAMENTO DE SISTEMAS**
2 ROUTER INALÁMBRICO	Ubicado en rectorado y secretaría
3 SWITCH	1 en el primer laboratorio de computación ▪ Con 24 interfaces
	1 en el segundo laboratorio de computación ▪ Con 24 interfaces
	1 en el tercer laboratorio de computación ▪ Con 24 interfaces
85 COMPUTADORAS	36 computadoras en el primer laboratorio ▪ 16 con 8 GB de RAM ▪ 20 con 4 GB de RAM ▪ Procesador Intel Core i3 ▪ Procesador Intel Pentium
	14 computadoras en el segundo laboratorio ▪ 3 con 8 GB de RAM ▪ 11 con 4 GB de RAM ▪ Procesador Intel Core i7 ▪ Procesador Intel Core i3
	15 computadoras en el tercer laboratorio ▪ 3 con 8 GB de RAM ▪ 12 con 4 GB de RAM ▪ Procesador Intel Core i3 ▪ Procesador Intel Pentium
	28 computadoras. Una por cada curso ▪ 28 con 4 GB de RAM ▪ Procesador Intel Core i3 ▪ Procesador Intel Pentium
	1 computadora en el laboratorio de ciencias ▪ Con 8 GB de RAM ▪ Procesador Intel Core i3
	2 computadoras laptop en el área de financiero

	▪ Con 8 GB de RAM ▪ Procesador Intel Core i7 ▪ Procesador Intel Core i3
	3 computadoras en secretaría ▪ Con 4 GB de RAM ▪ Procesador Intel Core i3
	1 computadora en rectorado ▪ Con 8 GB de RAM ▪ Procesador Intel Core i7

El controlador donde se instalará floodlight deberá poseer características de 8 GB de RAM y procesador Intel Core i3 como detalles mínimos para su correcto funcionamiento y poder soportar la red que se creará en las siguientes etapas del modelo PDIOO.

2.5.3. Etapa de Diseño

En la segunda etapa del proyecto de redes definidas por software a simular es realizar un diseño que se adapte mejor a una infraestructura física de la institución educativa, para esto se tomará en consideración la mejor opción en topología de red que se deba usar como estrella, anillo, bus, árbol, híbrida, entre otras. De la misma manera se iniciará un análisis de la infraestructura física que maneja la institución para un mejor entendimiento a la hora de diseñar una infraestructura SDN lógica dentro del simulador minino con ayuda de miniedit.

Por último se compararán los diseños de una infraestructura de red tradicional física y una infraestructura de red definida por software lógica, señalando las ventajas y desventajas que presenta cada una y la debida conclusión. Como resultado final se espera que todos los hosts que se incluirán tengan comunicación entre sí como si fuera una red física.

Topología

La topología de red es la disposición en la que se encuentran los equipos y la forma geométrica en la que los nodos se comunican entre sí. Existen varios tipos de topologías de redes que se utilizan en instituciones dependiendo de la necesidad. Cada topología funcionará correctamente, pero presentará dificultad en casos de crecimiento de la red, latencia, equipos averiados, conexión, etcétera. En lo que cabe las SDN y al ser una red

conmutada, todos los nodos deben estar conectados entre sí para que el controlador elija el mejor camino por donde sea más efectivo hacer el envío de paquetes y dejar este camino establecido para próximos envíos.

Como cada switch debe estar conectado al controlador, estos serán los nodos por donde los paquetes de datos entrarán y serán reenviados dependiendo de la ruta que el controlador de red asigne, es por eso por lo que el diseño de la SDN será basado en una topología tipo árbol, siendo el padre de todos los nodos el controlador, ya que sin este el plano de control no estaría disponible.

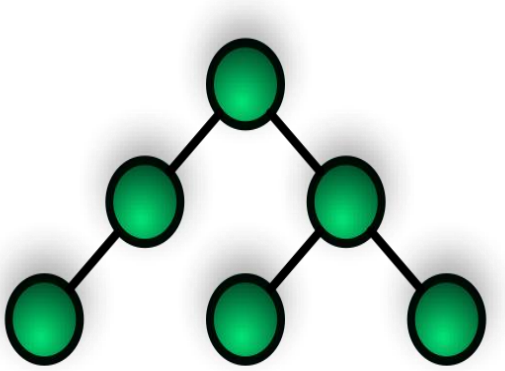


Figura 7. Topología de red tipo árbol

Análisis de la infraestructura de la red tradicional de la institución educativa

La institución educativa funciona con un modelo de red convencional, donde el plano de control y el plano de datos funcionan en el mismo conmutador o enrutador para hacer posible la transferencia de paquetes entre hosts. Esta institución posee equipos de red tales como routers y switches que levantan la red, ubicados principalmente en el departamento de sistemas, en la sección a la que pertenece el departamento de finanzas, el bloque de salones de clases #1 y en laboratorio de computación # 3. El diseño de la red tradicional fue pensado para segmentar mediante VLANs redes para estudiantes y docentes. Tres de los cuatro switches están conectados a una switch troncal siendo el encargado encaminar los paquetes al router con etiqueta de VLAN a la que pertenece el paquete para ser encapsulado, registrado y reenviado al destino.

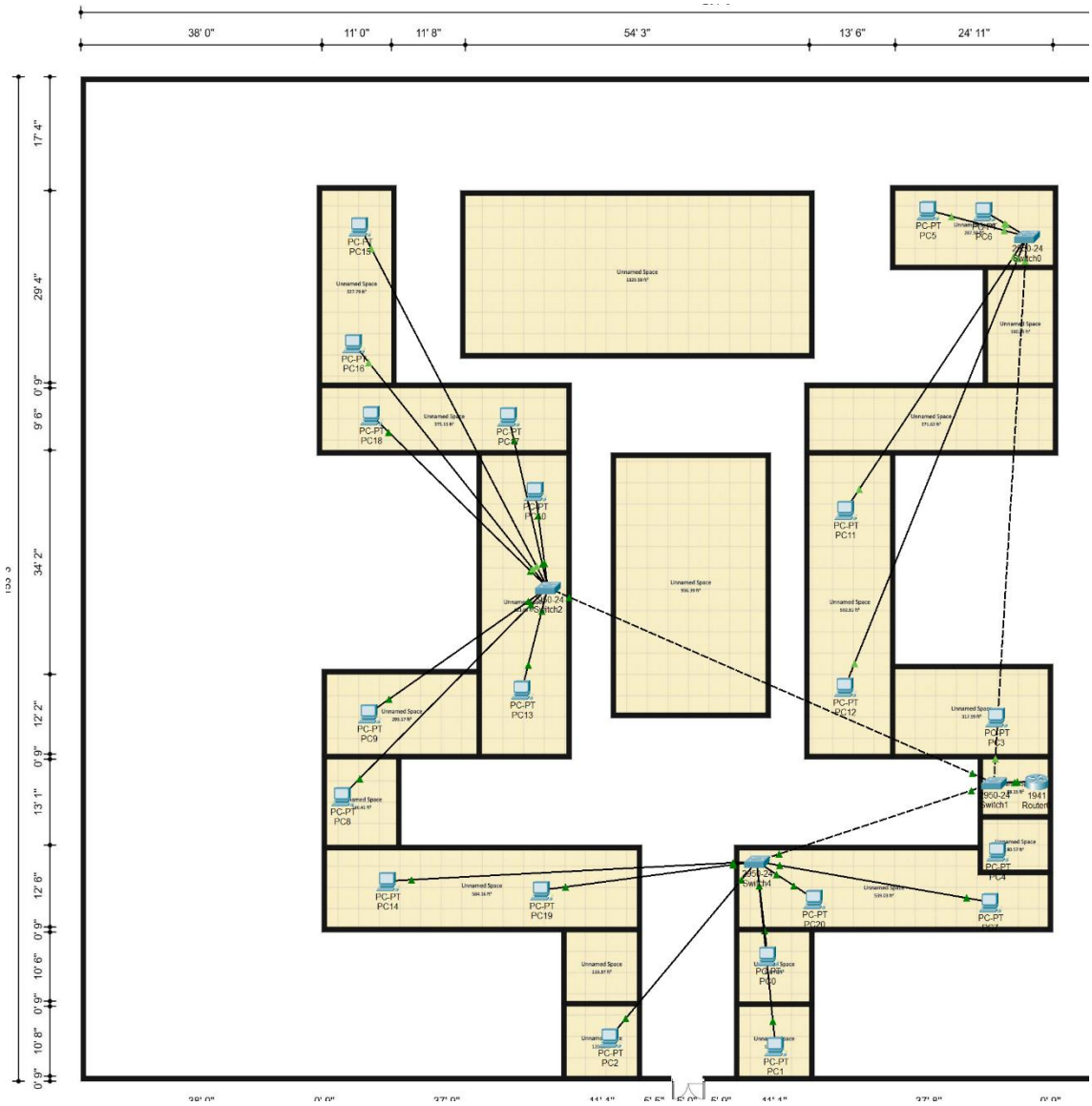


Figura 8. Infraestructura de red de la institución educativa

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

Como primer paso se debe crear una máquina virtual donde será instalada el controlador de red, para esto se debe acceder al link de descarga de la página oficial de floodlight: https://floodlight.atlassian.net/wiki/spaces/floodlightcontroller/pages/8650780/Floodlight+VM.

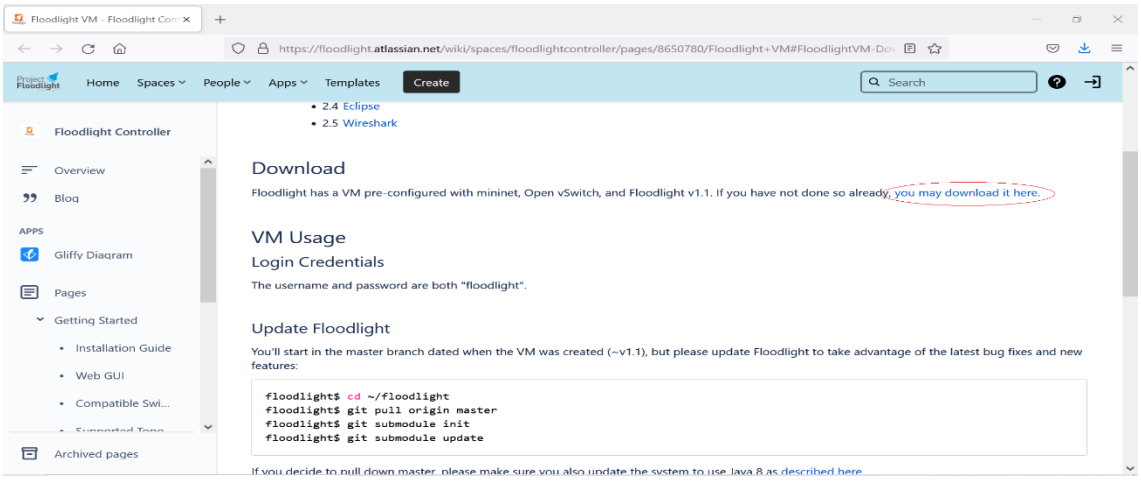


Figura 9. Sitio web para descargar floodlight

Se descargará un WinRAR que contiene comprimido un archivo .VMDK

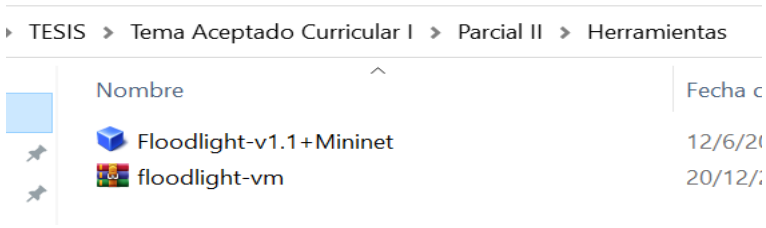


Figura 10. Archivos descargados desde el sitio web floodlight

Dentro de virtual box se establecerá el nombre del controlador, el tipo de sistema y su versión.

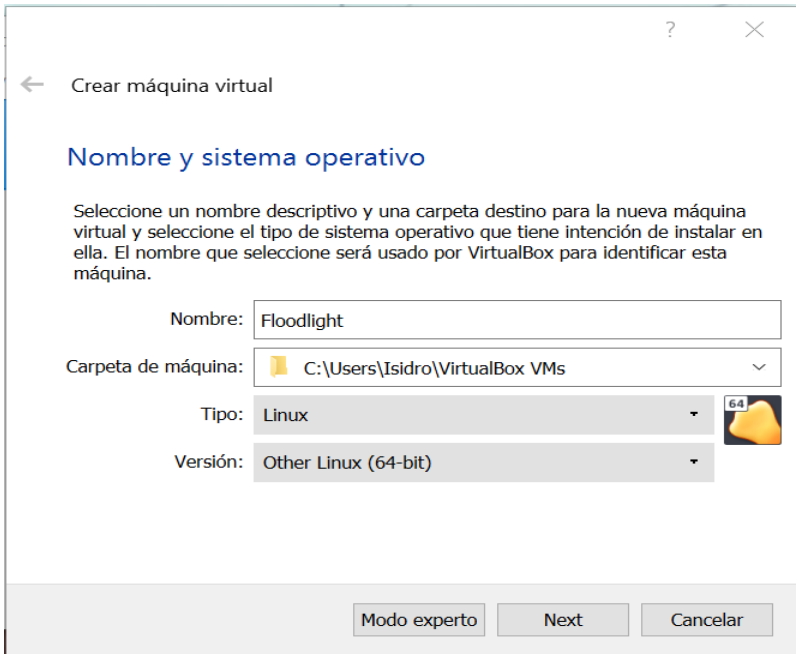


Figura 11. Instalación de Floodlight en VirtualBox

Se procede a asignar el tamaño de memoria RAM que ocupará el controlador. Para este proyecto se utilizó un 1 GB de RAM

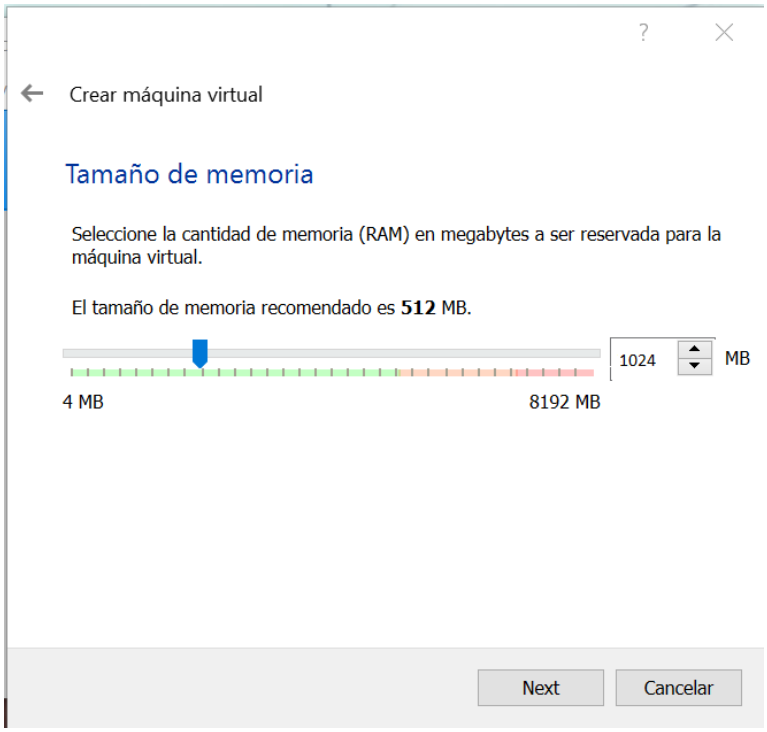


Figura 12. Asignación de memoria RAM para floodlight

Seleccionamos el disco de máquina virtual que contiene floodligh controller.

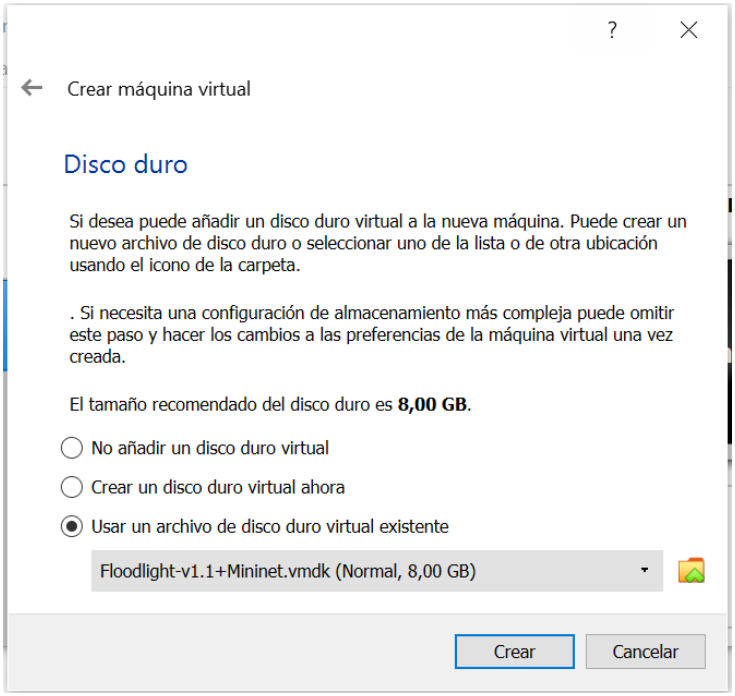


Figura 13. Asignación de tamaño de disco duro para floodlight

Una vez creada la virtual box se deberá establecer como puente para que el controlador pertenezca y sea asignada una IP de la red a utilizar.

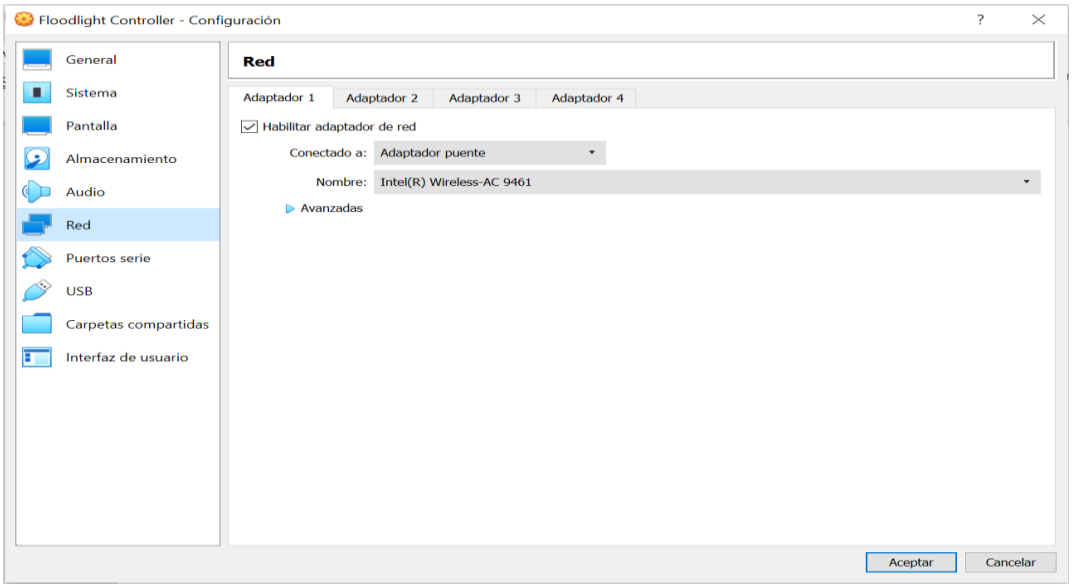


Figura 14. Configuración de red tipo puente para floodlight

Como último paso se deberá iniciar el controlador comprobando que esté asignada una IP de la red donde está instalado floodlight y no una IP nateada. Las credenciales por default tanto para usuario y contraseña es **floodlight**.

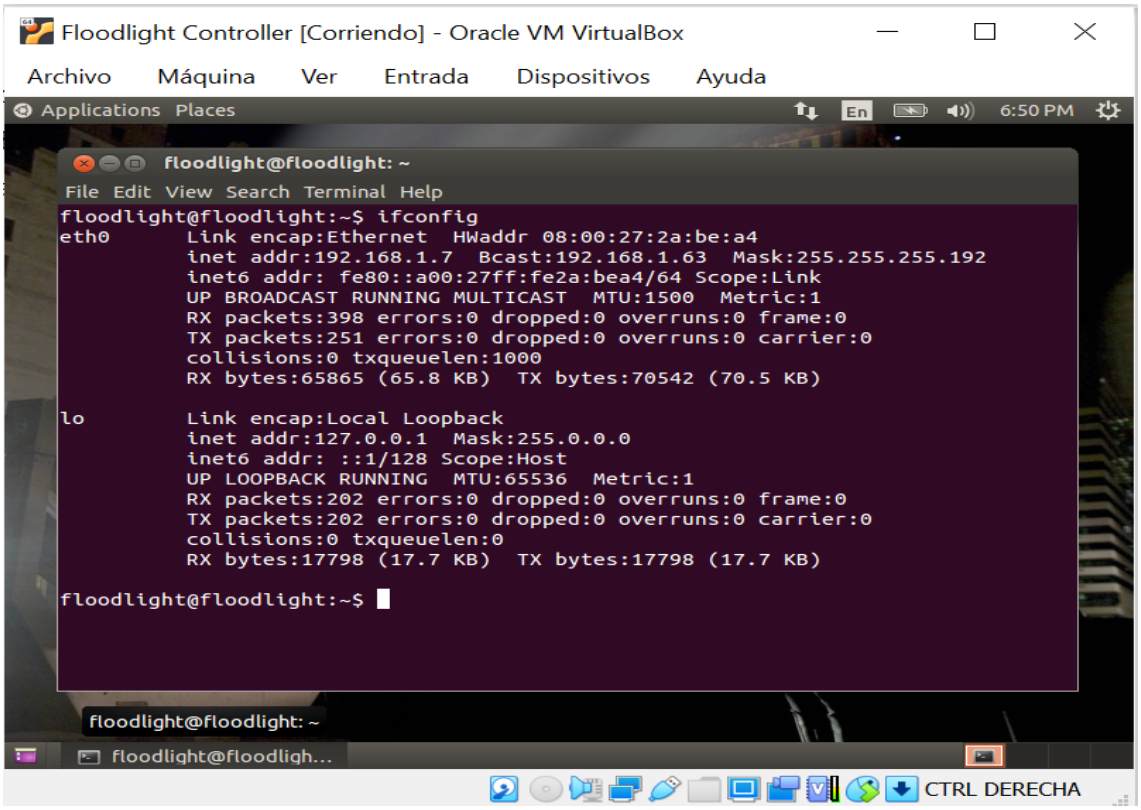


Figura 15. Verificación de IP tipo puente de floodlight

Instalación de mininet en una máquina virtual

Aunque floodlight posea mininet ya integrado como herramienta, se instalará mininet en una máquina virtual aparte para mejor manipulación de estas herramientas. Mininet instalada como máquina virtual deberá trabajar en conjunto con putty para funcionamiento remoto y xming para diseño de la red con miniedit.

Se debe descargar Mininet desde la página oficial http://mininet.org/download/ y seleccionar una versión para posterior trabajo.

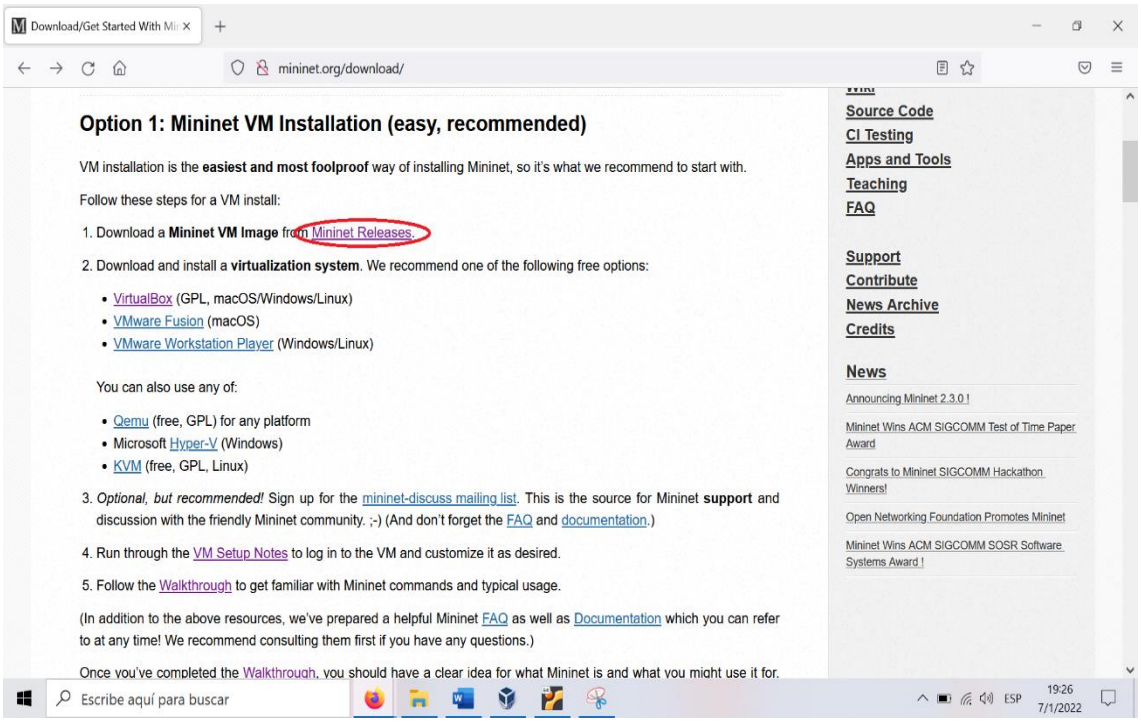


Figura 16. Sitio web para descargar mininet

La descarga se realiza en un comprimido de WinRAR que contine un archivo .VMDK

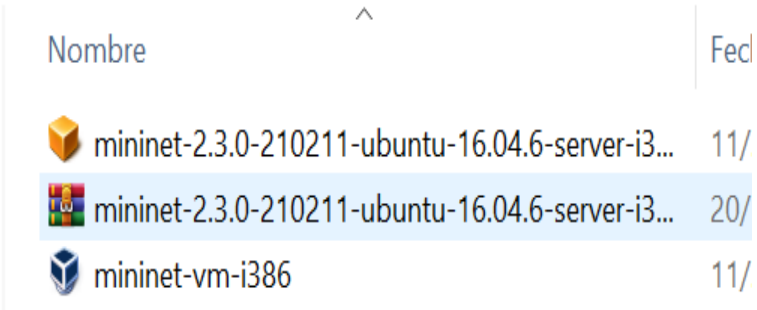


Figura 17. Archivos descargados desde el sitio web mininet

Se procede a crear la máquina virtual que contendrá mininet para diseñar la topología de red SDN. Se deberá establecer un nombre, el tipo de sistema y la versión.

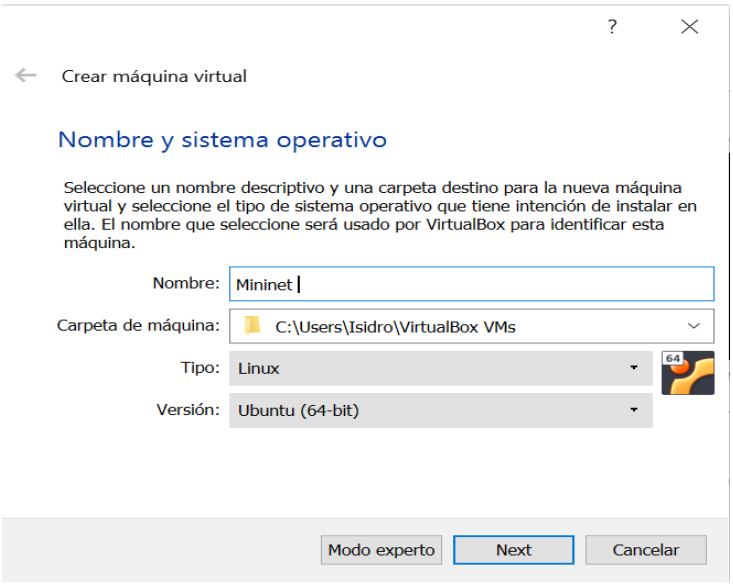


Figura 18. Instalación de Mininet en VirtualBox

Al igual que el controlador se asignará 1 GB de memoria RAM, siendo suficiente para que no presente errores.

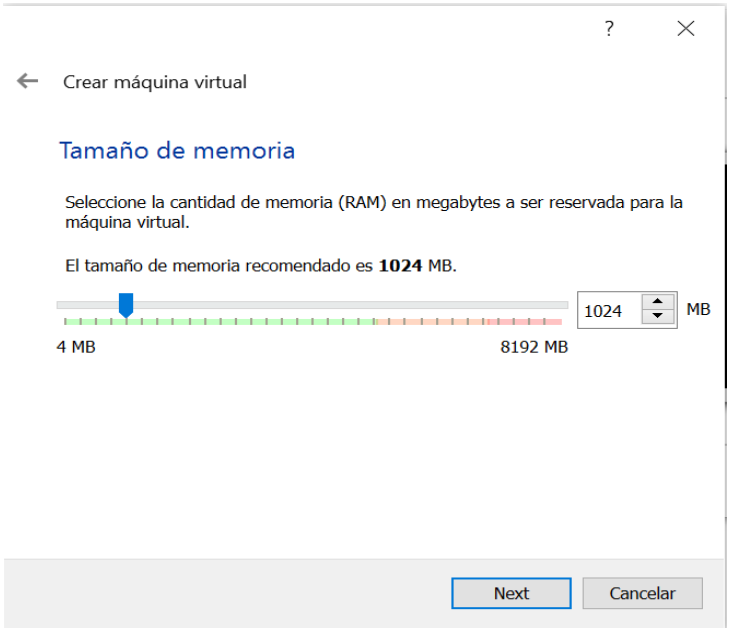


Figura 19. Asignación de memoria RAM para mininet

Ahora buscamos el directorio donde se encuentra el disco duro virtual de mininet y lo seleccionamos para poder iniciar la virtualización

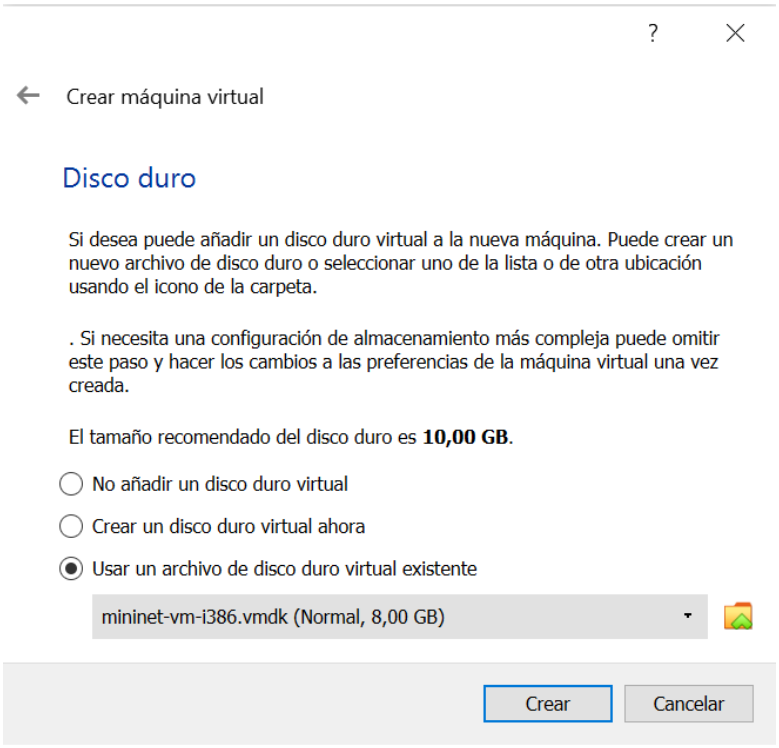


Figura 20. Asignación de tamaño de disco duro para mininet

A mininet también se lo debe configurar como adaptador puente para poder trabajar conjunto al floodlight y que estos se pueden reconocer.

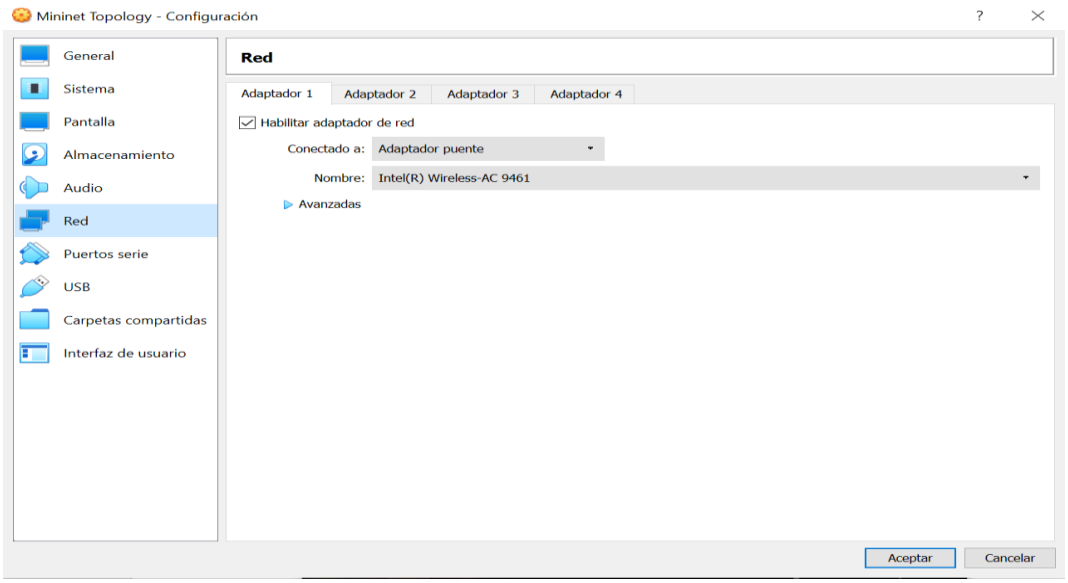


Figura 21. Configuración de red tipo puente para mininet

Como último paso de la instalación, se deber verificar que se le ha asignado una IP de la red en la que se encuentra. Las credenciales por default de mininet para usuario y contraseña es **mininet**.

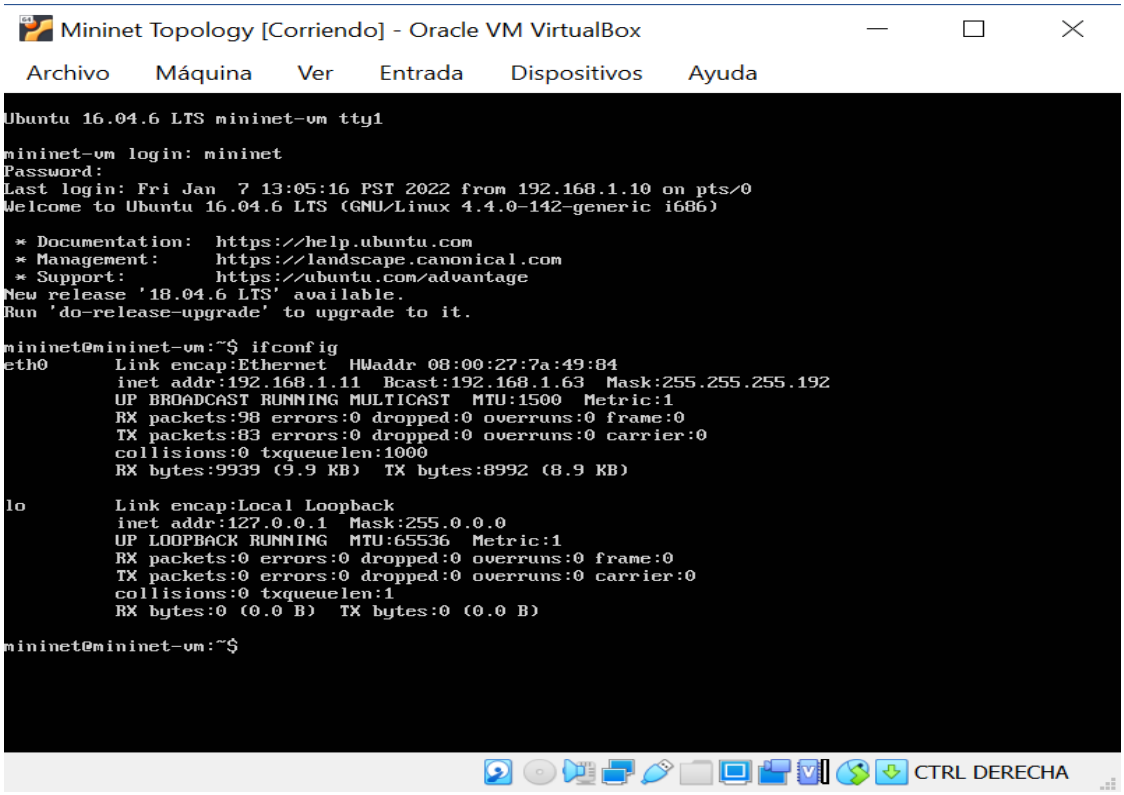


Figura 22. Verificación de IP tipo puente de mininet

Diseño de la infraestructura SDN

Para crear el diseño de la red se utilizará en controlador floodlight para operar una red OpenFlow, mininet como herramienta para administrar la red, miniedit y xming como herramientas gráficas para crear el diseño de la red, putty para establecer una conexión remota con mininet, y un navegador web para visualizar la interfaz gráfica del controlador.

Situado en la máquina virtual que contiene floodlight se deberá abrir un terminal para acceder al directorio floodlight/ mediante el comando **cd floodlight/**. Para levantar los servicios del controlador, una vez situados en el directorio floodlight ejecutar el comando **java -jar target/floodlight.jar.** Este comando permite abrir floodlight.jar escrito en lenguaje java.

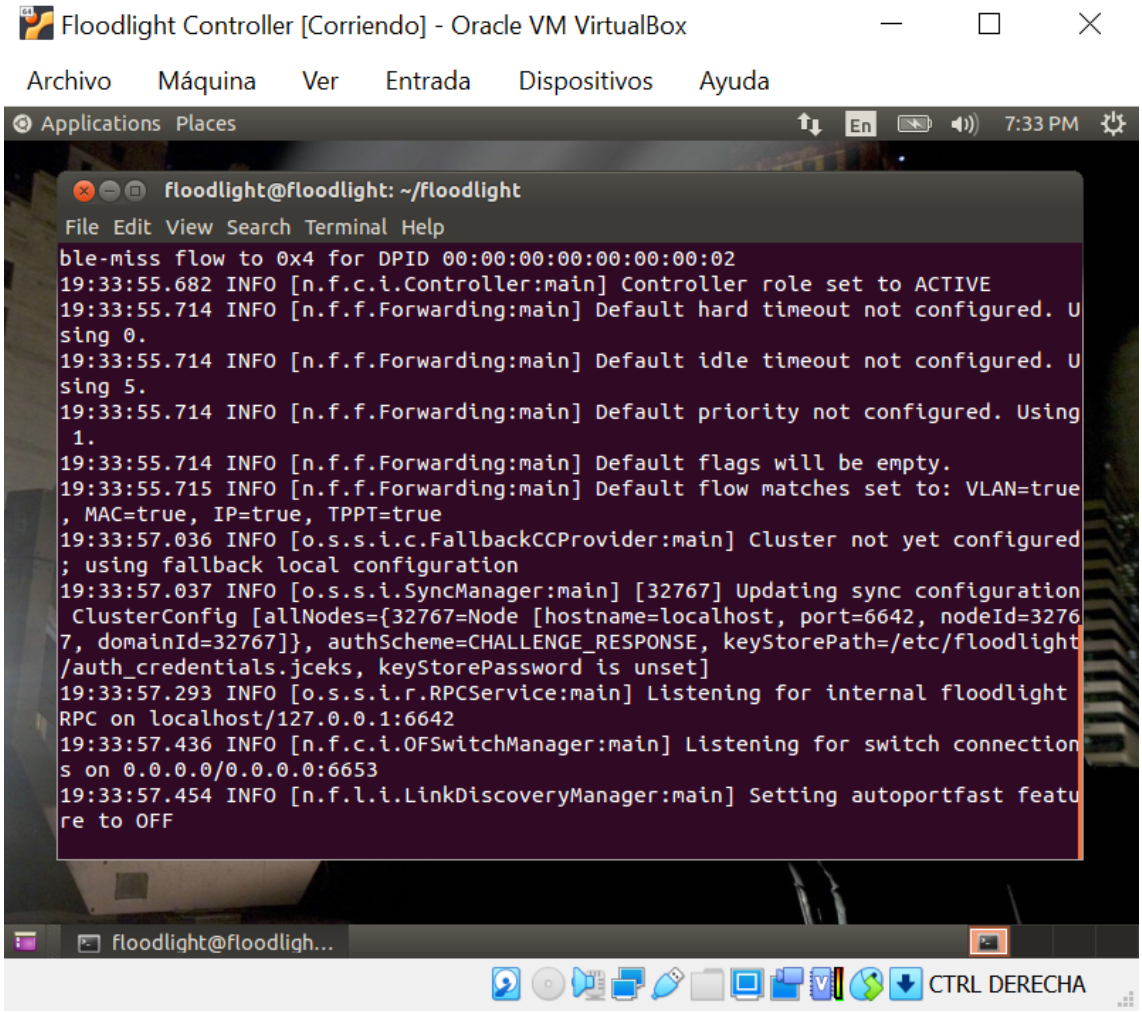


Figura 23. Levantamiento del controlador floodlight

La máquina virtual que contiene mininet deberá estar encendida para poder establecer una conexión remota con putty. La conexión remota se la realiza con la finalidad de manipular mejor las herramientas mininet y miniedit. Antes de establecer la conexión se debe habilitar la opción de x11forwarding que permite ejecutar aplicaciones gráficas de una máquina remota exportando la interfaz gráfica al escritorio de la computadora usada. Después de este paso se completa la conexión remota con la IP de la máquina virtual mininet.

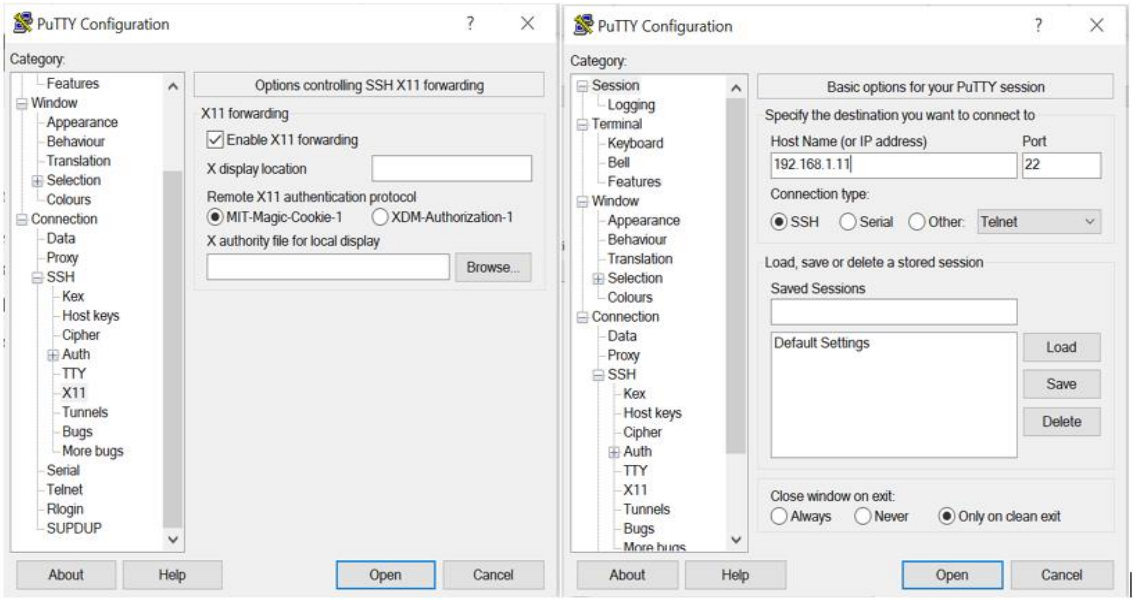


Figura 24. Conexión a mininet vía putty

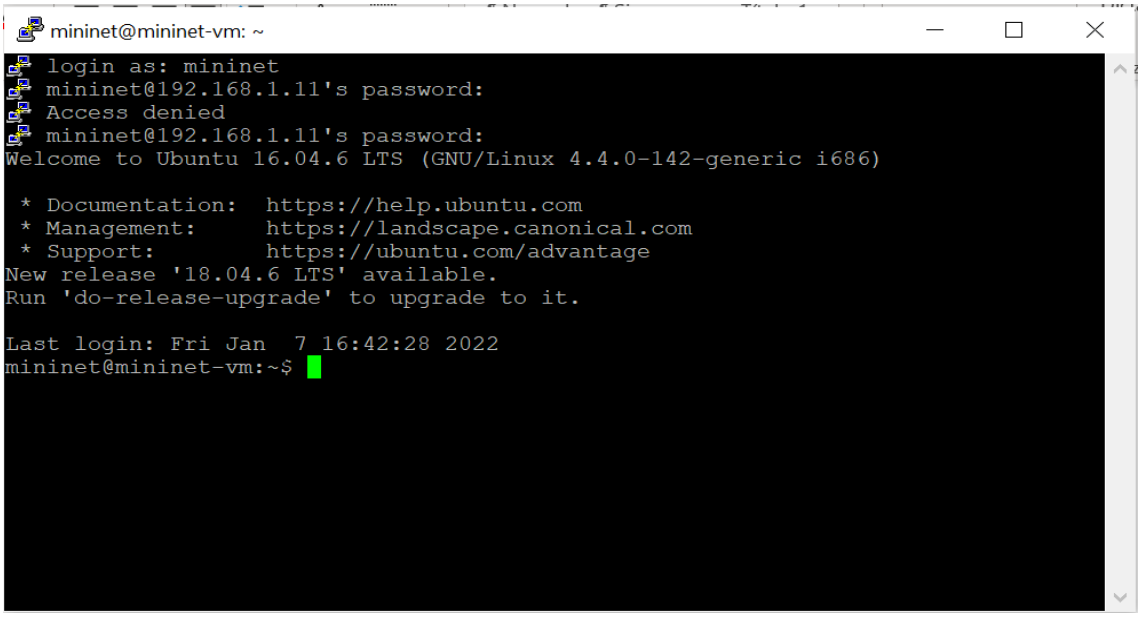


Figura 25. Acceso a mininet vía putty

La herramienta miniedit debe ser ejecutada dentro del directorio mininet/mininet/examples accediendo con el comando **cd mininet/mininet/examples.** Dentro del directorio se ejecuta el comando **sudo ./miniedit.py** y de manera instantánea se abrirá en xming el entorno gráfico para poder diseñar una topología de red seleccionando controlador, switches y hosts

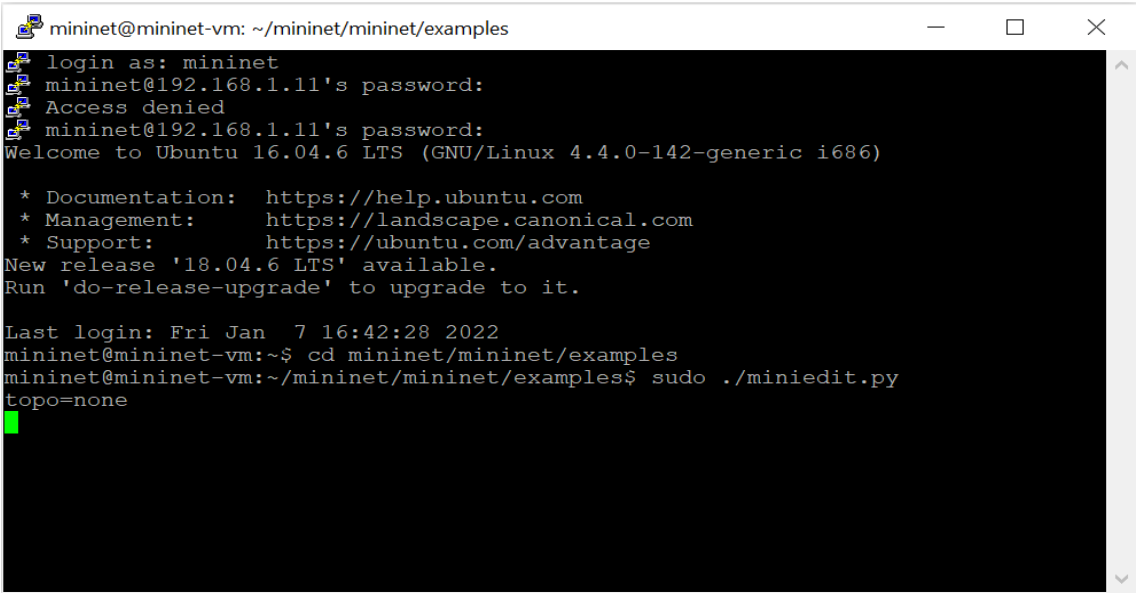


Figura 26. Acceso al directorio example de mininet y inicio de miniedit

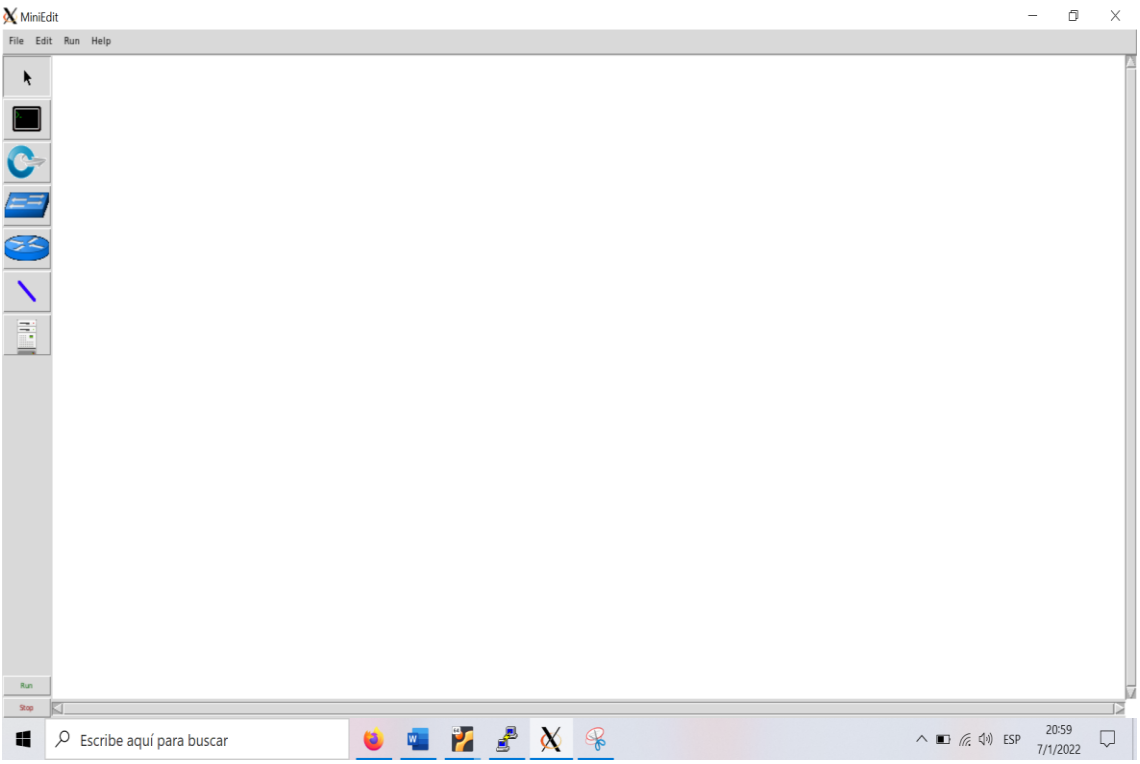


Figura 27. Interfaz de miniedit

Diseño de la infraestructura de red definida por software

Para la institución educativa se realizado el siguiente diseño de red, seleccionando los laboratorios de computación, laboratorio de ciencias, departamentos principales como financiero, secretaría y rectorado. De la misma manera se ubicó dos conmutadores más en puntos claves para poder tener red en los bloques principales donde se encuentran los

cursos más alejados del departamento de sistemas. En total se utilizó un controlador, nueve conmutadores de red, y para el estudio se asignó dos hosts por cada conmutador para establecer de manera eficaz conexión entre todos los hosts y así poder agregar más host sin correr riesgo de mala configuración.

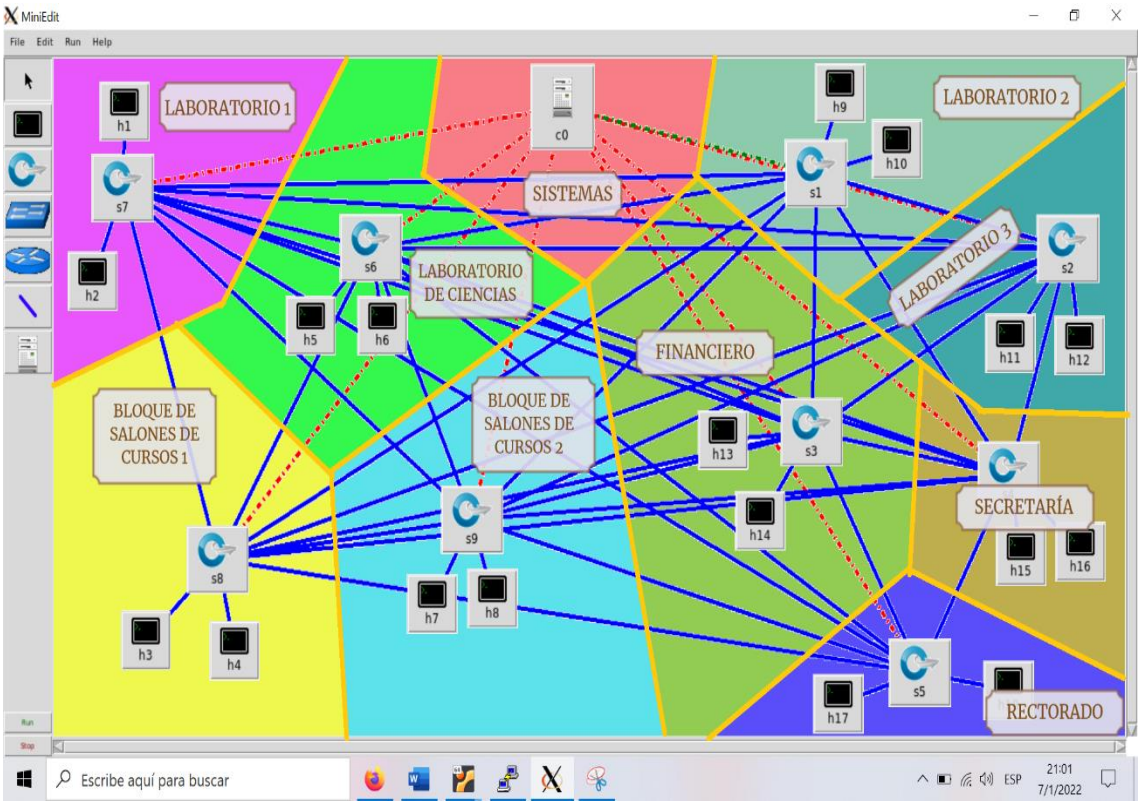


Figura 28. Primer diseño de red SDN para la institución educativa

El diseño muestra un recuadro de color rojo el departamento de sistemas donde será ubicado el controlador de red, y a los rededores los laboratorios de informática, laboratorio de ciencias, departamentos de financiero, secretaría y rectorado, y dos bloques de salones de clases. El propósito principal de este diagrama SDN es separar el plano de control y el plano de datos para que solo exista un proceso de reconocimiento de salida y forward que se registre en la tabla de flujo de datos del controlador, haciendo que el administrador de la red programe la comunicación de los datos en total libertad tomando en cuenta dirección MAC de origen y destino, dirección IPv4 o IPv6 de origen y destino o puertos UDP o TCP de origen y destino que comparad con las redes convencionales solo toman como criterio la dirección MAC o IP de destino.

Comparación entre infraestructura de red convencional y SDN

Red convencional	Red definida por software
Funcionan mediante registro de tablas CAM	Funcionan mediante registro de tablas de flujo
Los conmutadores funcionan bajo el criterio de direcciones MAC	Los conmutadores de red realizan un proceso de aprendizaje
El plano de control funciona dentro de cada conmutador perteneciente a la red	Un solo plano de control funciona para toda la red de la institución dentro del controlador centralizado
El plano de control no puede ser manipulado por el administrador de red a menos que sea equipo por equipo.	El plano de control está presente y lista para ser administrada en el controlador
Los criterios de origen y destino como MAC, IP, puertos UDP o TCP no son considerados	Permite establecer políticas de conmutación tomando en cuenta más criterios
Los switches deciden de manera independiente como será enviada una trama de datos a los demás nodos de la red	Permite programar la red a conveniencia de como lo requiera la institución o la organización que lo implemente
Costo de mantenimiento de equipos puede llegar a ser elevado por equipo	El costo de mantenimiento no aumenta, incluso puede disminuir
Para que la red puede ser escalable, se debe invertir y adquirir más equipos con el riesgo de que estos no sean compatibles con los demás dispositivos	La escalabilidad no representa un problema, puesto que se pueden agregar conmutadores de red a disposición

Como punto débil de las redes definidas por software es que por ahora solo se puede trabajar con un solo controlador para administrar la red, y al existir un único controller, si este llegase a fallar debido a problemas físicos o lógicos, la red presentaría problemas hasta encontrar una solución. Por lo demás, la SDN ofrece tanto y más que una red tradicional.

Soporte y mantenimiento de una red tradicional

Las redes tradicionales tienen un precio alto para levantar con éxito una red donde los mayores precios apunta a la adquisición de los equipos de red como routers y switches, siguiendo en segundo puesto las herramientas que hacen posible está conectividad como lo son los cables de red, "ponchadoras", peladoras, conectores RJ45, testeadores y cobertores. Para la red de la institución analizada, el costo de levantar la red bordea un aproximado de $5000.

2.5.4. Etapa de Implementación

La tercera etapa para el desarrollo del proyecto corresponde a implementar el diseño de la red (etapa II) con las tecnologías seleccionadas dentro de la planificación de la red y el estudio de la red convencional que se realizó (etapa I). Una vez que el diseño está realizado, se deben configurar los conmutadores y el controlador para que estos puedan lograr la comunicación que se requiere para los hosts. Las herramientas que se utilizarán poseen una configuración ya establecida, como las IPs que se asignan a lo routers, ya que estás tienden a pertenecer a la red 10.0.0.0. De la misma manera hay que realizar el cambio del puerto de red del controlador previamente configurado a 5533.

Para esta primera implementación toda la red de la institución educativa será operada bajo la red **192.168.10.0** empezando desde la segunda IP asignable **192.168.10.2**, y el controlador con una IP proporcionada por el router**.** Se realizará esto para constatar que la red efectivamente funciona bajo las configuraciones efectuadas. Para el funcionamiento de la red será tomando en cuenta los conceptos de una red WAN y LAN, lo que quiere decir que las máquinas virtuales (floodlight y mininet) al estar configuradas como puente y poseer una IP proporcionada por el router será considerada como red WAN, mientras que la red que será asignada a los hosts se considerará como red LAN. La aplicación en un ambiente real conlleva el mismo concepto de funcionalidad.

En próximas etapas la red será segmentada para un mejor control de los departamentos principales, laboratorios y bloque de salones de clases (etapa V). A continuación se detallará una tabla con las IPs que serán asignadas a los diferentes host y controlador como información preliminar y tener así un mayor control.

Información preliminar de direcciones IP para la SDN				
Dispositivo	**Dirección IP**	**Red**	**Ubicación**	**Tipo de Red**
Controlador	192.168.1.7	192.168.1.0	Sistemas	WAN
Host 1	192.168.10.2	192.168.10.0	Laboratorio #1	LAN
Host 2	192.168.10.3	192.168.10.0	Laboratorio #1	LAN
Host 3	192.168.10.4	192.168.10.0	Bloque Cursos #1	LAN
Host 4	192.168.10.5	192.168.10.0	Bloque Cursos #1	LAN
Host 5	192.168.10.6	192.168.10.0	Laboratorio Ciencias	LAN
Host 6	192.168.10.7	192.168.10.0	Laboratorio Ciencias	LAN
Host 7	192.168.10.8	192.168.10.0	Bloque cursos #2	LAN
Host 8	192.168.10.9	192.168.10.0	Bloque cursos #2	LAN
Host 9	192.168.10.10	192.168.10.0	Laboratorio #2	LAN
Host 10	192.168.10.11	192.168.10.0	Laboratorio #2	LAN
Host 11	192.168.10.12	192.168.10.0	Laboratorio #3	LAN
Host 12	192.168.10.13	192.168.10.0	Laboratorio #3	LAN
Host 13	192.168.10.14	192.168.10.0	Financiero	LAN
Host 14	192.168.10.15	192.168.10.0	Financiero	LAN
Host 15	192.168.10.16	192.168.10.0	Secretaría	LAN
Host 16	192.168.10.17	192.168.10.0	Secretaría	LAN
Host 17	192.168.10.18	192.168.10.0	Rectorado	LAN
Host 18	192.168.10.19	192.168.10.0	Rectorado	LAN

Configuración previa al inicio de la simulación

En necesario configurar el controlador de red con el respectivo puerto, tipo de controlador, protocolo TCP para control de transmisión y la dirección IP que poseerá el controlador asignado por el router. El nombre del controlador puede ser cambiado. Esto para que los switches sepan donde enviar los paquetes de datos en caso de que la dirección MAC de destino no se encuentre registrada en sus tablas de flujo.

Puerto: **6653**	Tipo de controlador: **Remote Controller**	Protocolo: **TCP**	IP: **192.168.1.7**

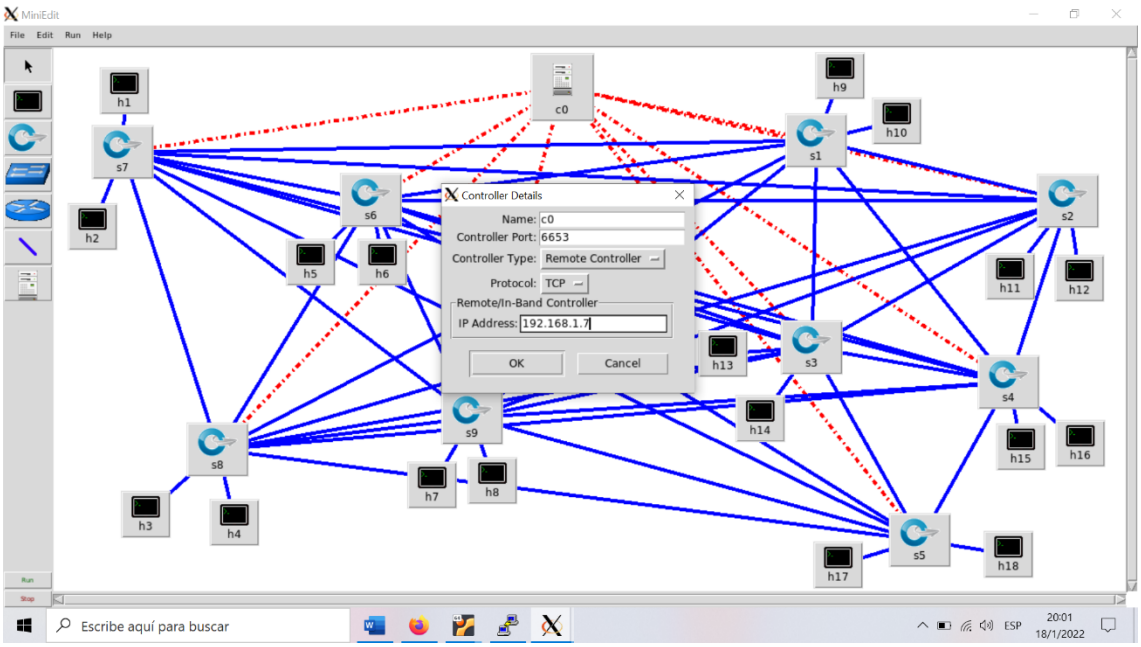


Figura 29. Configuración de IP del controlador en miniedit

Para los conmutadores se debe configurar el tipo de switch que es la manera en la que este debe operar dentro de la red. Para este caso se seleccionará **Open vSwitch Kernel Mode** para que permita una conmutación virtual con comunicación exitosa entre hosts mediante ping. Se realiza esto para conmutador agregado a la red.

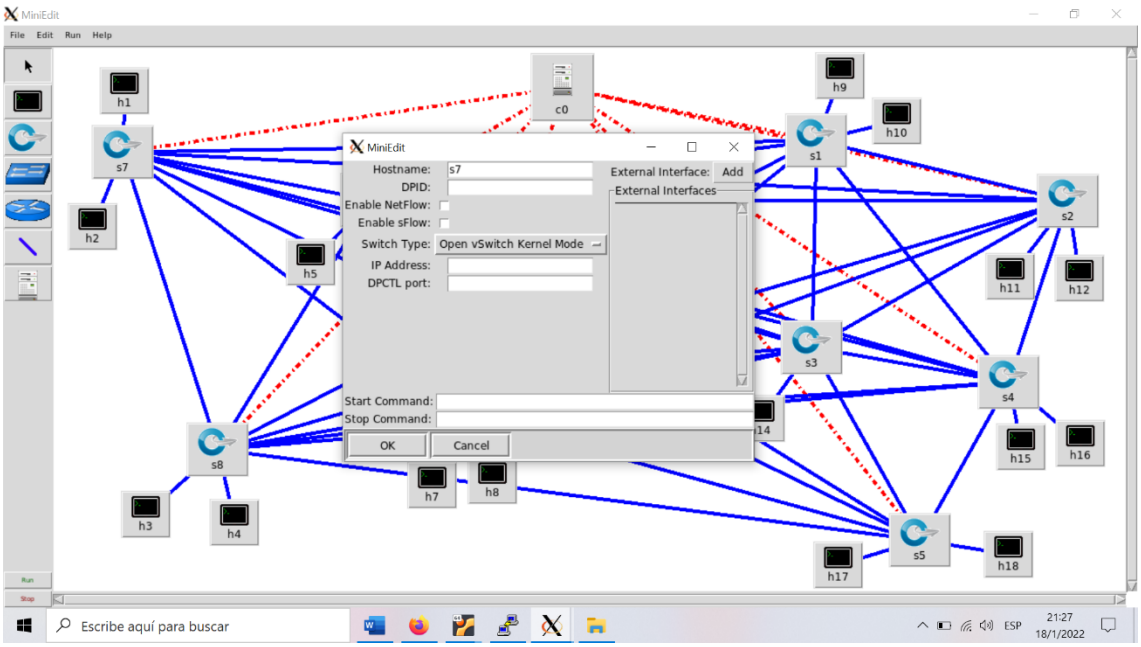


Figura 30. Configuración de switches

En los hosts se configura únicamente la dirección IP que tendrá cada una, iniciando desde la **192.168.10.2** hasta **192.168.10.19**. La dirección que posee el controlador de red, esta IP será el camino para comunicarse con el plano de control administrado por floodlight.

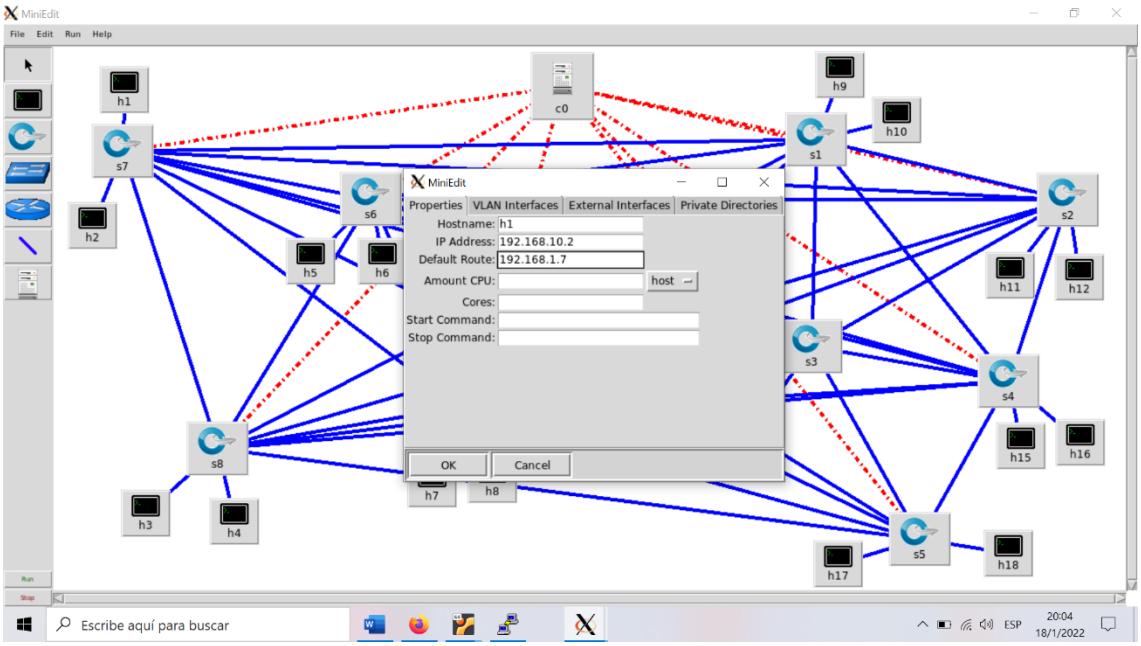


Figura 31. Asignación de IP en el host h1

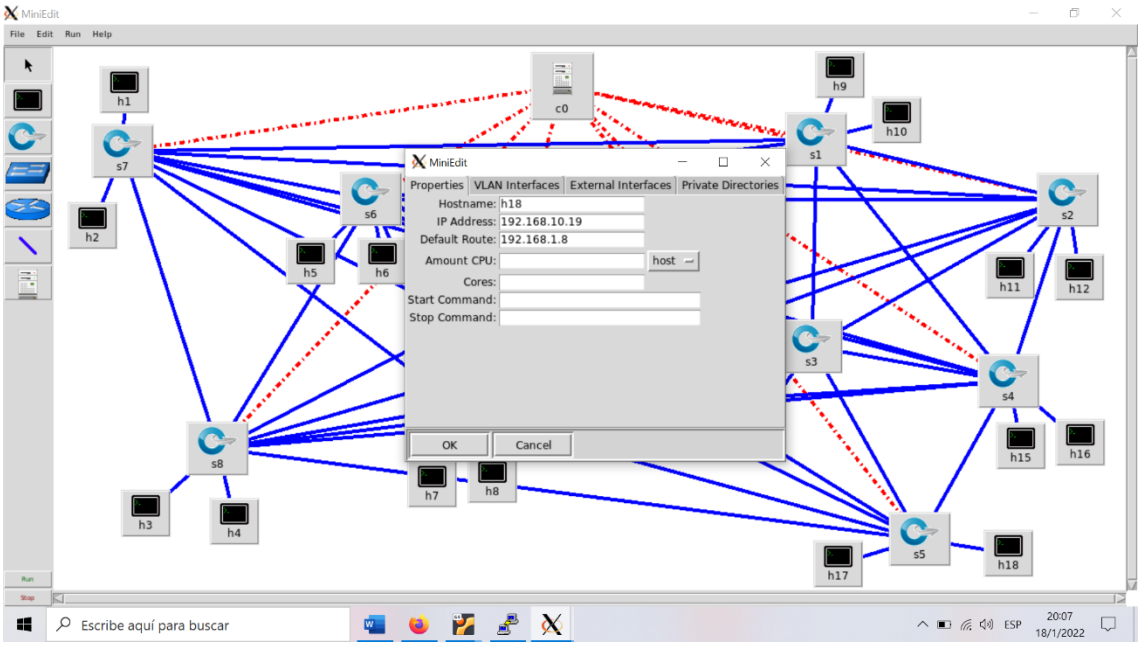


Figura 32. Asignación de IP en el host h18

Para acceder a las preferencias de miniedit seleccionamos la pestaña **Edit,** donde se marcará el recuadro de **Start CLI** para manejar mininet mediante línea de comandos. La configuración del switch como Open vSwitch Kernel Mode seleccionando OpenFlow 1.3 para que los paquetes de datos enviados encuentren un camino a seguir para llegar al destino dentro de la red.

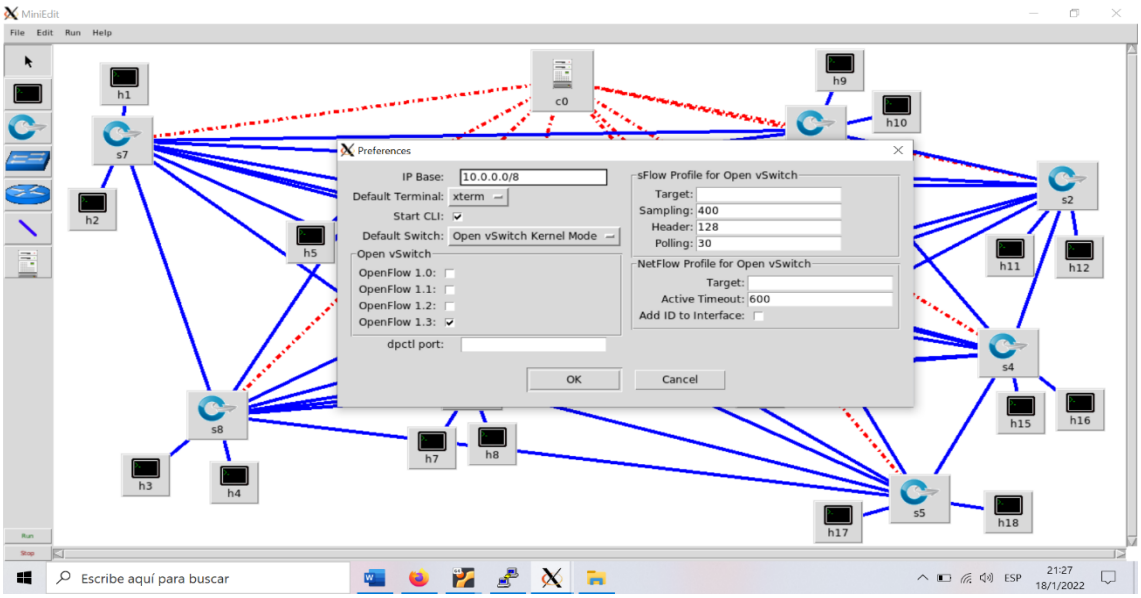


Figura 33. Configuración en las preferencias de miniedit

Inicio de la simulación SDN

La herramienta miniedit en su lado izquierdo de la interfaz, muestra dispositivos que se pueden usar para diseñar una red, compuesta por los siguientes elementos:

Puntero: selecciona, accede y mueve los dispositivos elegidos.

Host: computadora virtual donde se configura direcciones IP y VLANs

SwitchOpenFlow: dispositivo de red encargado de conmutar los paquetes

LegacySwitch: switch de una red convencional

LegacyRouter: router de una red convencional

Cable: conecta los equipos seleccionados para la red

Controlador: encargado de manejar el plano de control

Run: inicia la simulación con las configuraciones realizadas.

Stop: detiene la simulación de red para realizar cambios o salir.

Figura 34. Herramientas y dispositivos de miniedit

Una vez realizado todas las configuraciones anteriores y asignando las direcciones IP tanto para controlador y para los hosts, se presiona el botón **Run** para iniciar la simulación, seguido de esto no se podrá efectuar ningún cambió dentro del diagrama mientras se esté ejecutando y de manera inmediata en la terminar de la máquina virtual mininet donde se accedió de manera remota mediante putty, aparecerá mininet listo para controlar la red.

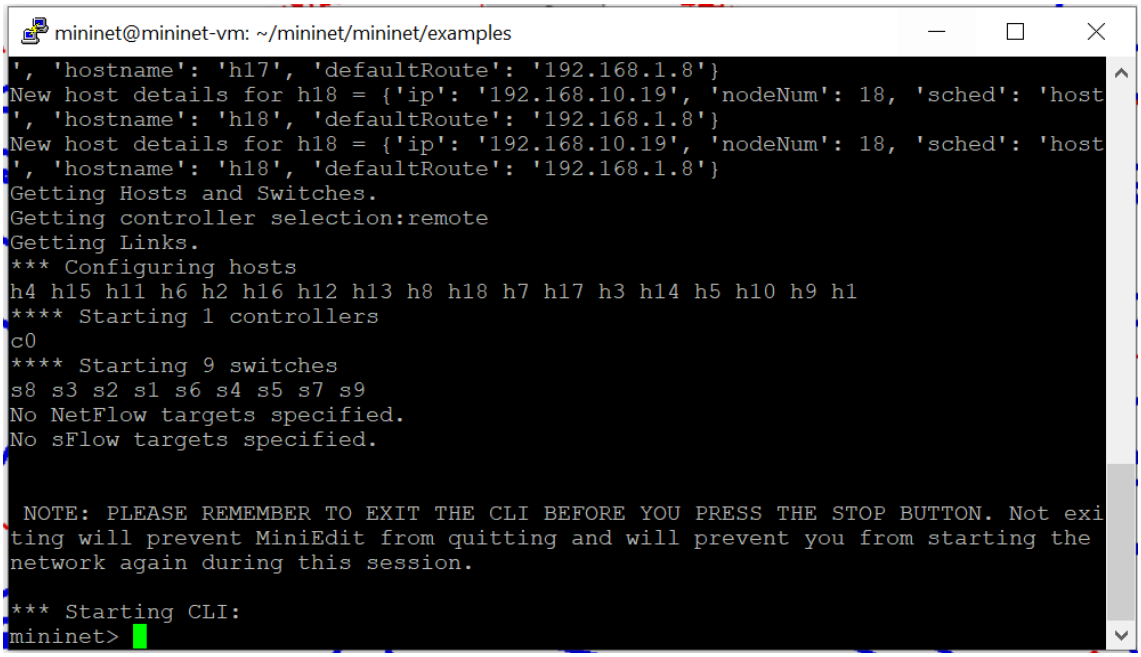


Figura 35. Inicio de la simulación de la topología de red SDN

Acceso al controlador floodlight desde el navegador

Se puede observar cómo funciona floodlight controller accediendo desde cualquier navegador hacia el servidor http de floodlight para la interfaz de usuario, para esto se debe colocar la IP del controlador seguido por el puerto 8080: **http://192.168.1.7:8080/ui/index.html.**

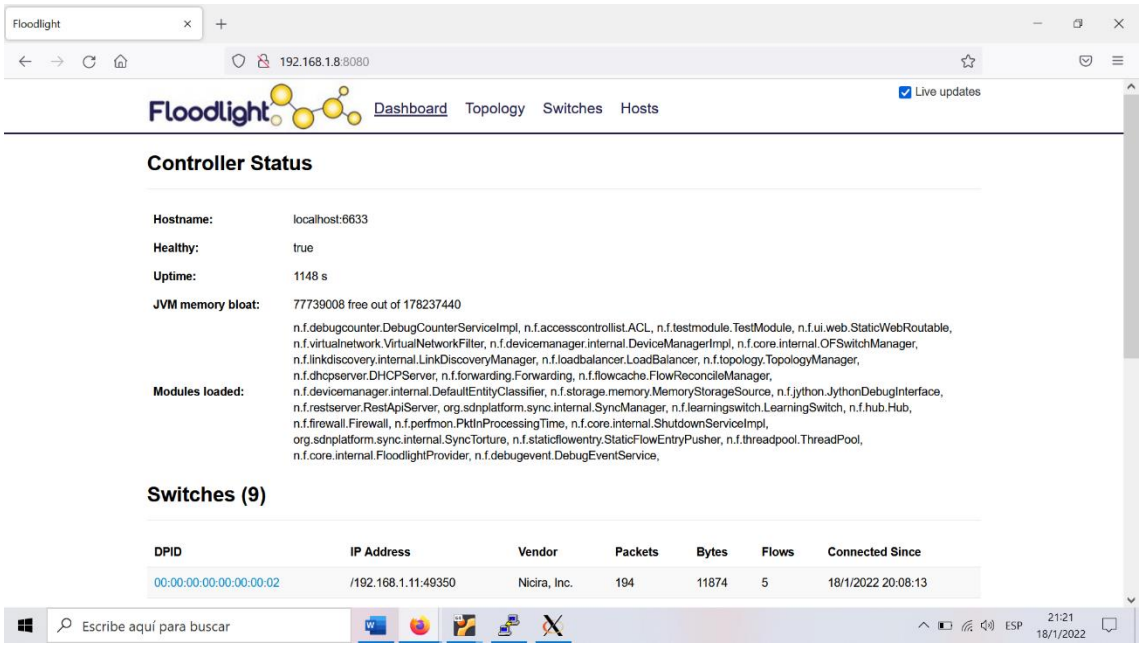


Figura 36. Servidor http de floodlight

A primera vista se observa una interfaz de usuario sencilla donde las manipulaciones por terceros no pueden realizarse, es decir, toda persona no autorizada al acceder al servidor http de floodlight no podrá ejecutar ningún cambio en la red o manipulación de los dispositivos. Se observa también cuatro pestañas: 1) dashboard 2) tolopogy 3) switches 4) hosts. Dashboard presenta el estado del controlador y los equipos de red utilizados. Topology muestra la topología de red desde el punto de vista de floodlight. Switches son los conmutadores de red utilizados. Hosts son los equipos o computadoras utilizadas.

Equipos de red generados

Una característica apreciada a primera instancia es que los hosts que se agregaron al diseño de la red no aparecen en la topología o en la pestaña de hosts, esto no quiere decir que no se han generado, sino que no están siendo utilizados. Para poder observar los hosts pertenecientes a cada conmutador es necesario realizar un ping (será demostrado en la siguiente etapa IV de operación).

Por otro lado los conmutadores sí son observados dentro de la pestaña switches. Se muestran los 9 switches utilizados en la red detallando el identificador de ruta de datos (**DPID**) la dirección IP a un solo plano de control (controlador), la compañía fabricante, los paquetes, bytes, flows y la fecha de funcionamiento.

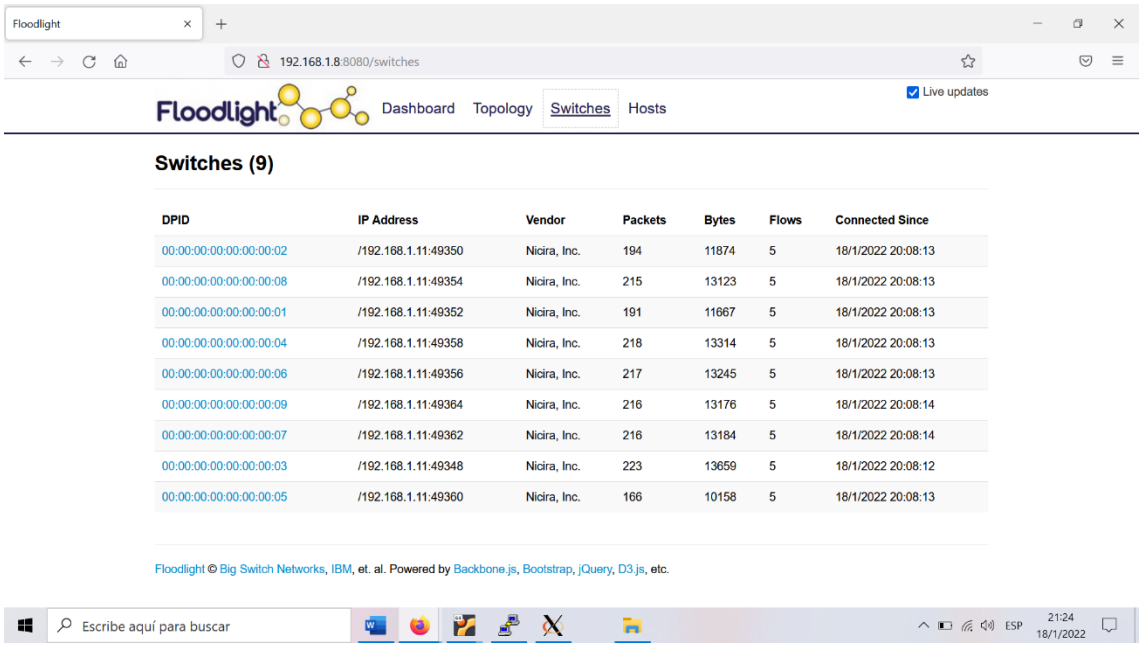


Figura 37. Sección de switches utilizados en el diseño de red SDN

Para los hosts se detallan la dirección MAC, dirección IP, el puerto utilizado del switch y la última conectividad. Como se mencionó en el primer párrafo de esta sección, los hosts no se muestran en la interfaz de usuario de floodlight hasta que se realice un ping.

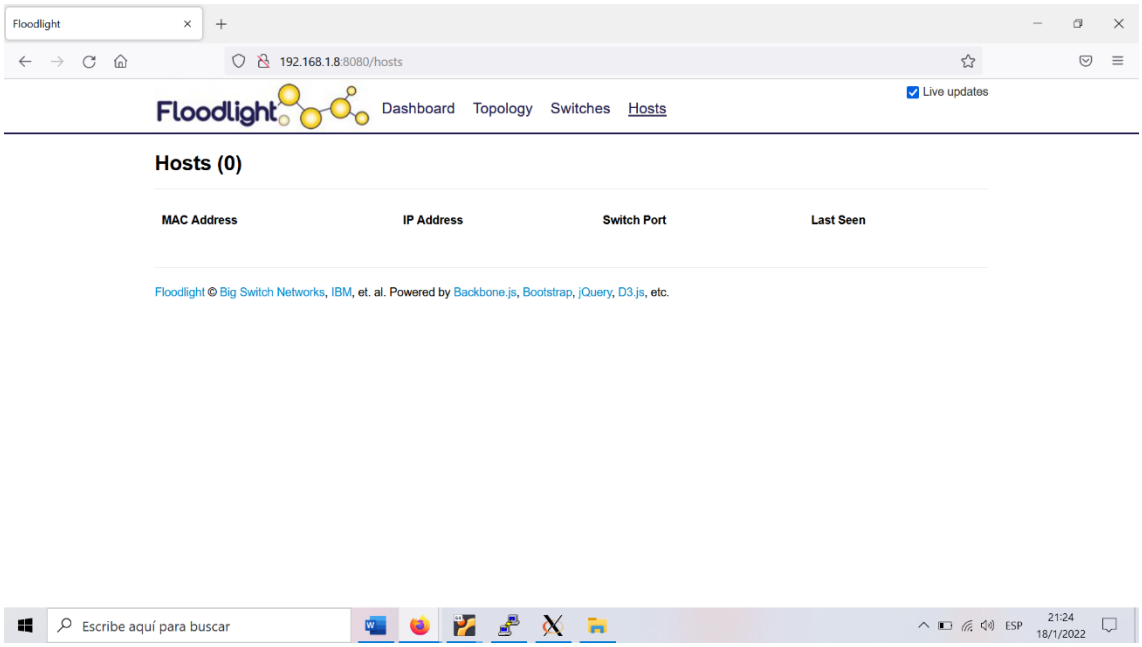


Figura 38. Sección de host utilizados en el diseño de red SDN

Topología vista desde floodlight

El diseño de la red en floodlight muestra todos los switches conectados entre sí y también el DPID. Los hosts también son visualizados en la topología una vez que se haya realizado ping entre los equipos. Se recalca que los cambios en la interfaz de usuario no posibles.

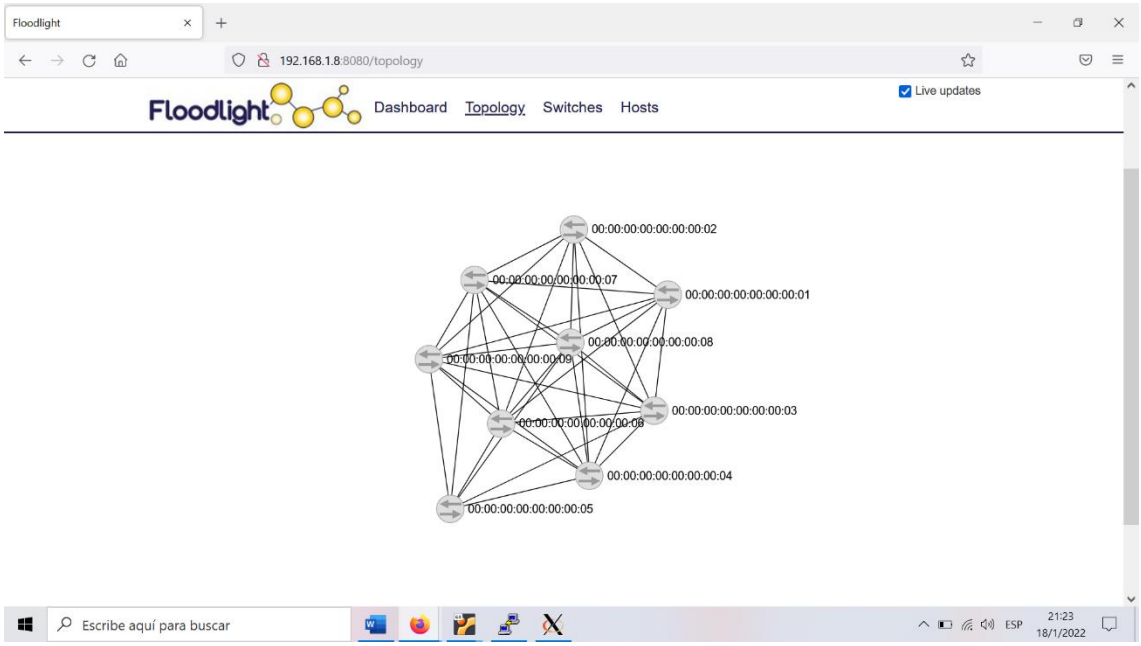


Figura 39. Sección de topología utilizado en el diseño de red SDN

2.5.5. Etapa de Operación

La cuarta etapa correspondiente a la metodología del proyecto aplicada, PDIOO, es la operación. Aquí se empezará a manipular la red para comprobar su efectividad a la hora del levantamiento, es decir, se procederá a inspeccionar la red revisando el tráfico que se genera con ayuda de wireshark para comprobar que la información generada como la IP de destino y origen, dirección MAC de destino y origen y puertos son los mismos que muestra el controlador floodlight y wireshark. Asimismo se demostrará el protocolo OpenFlow como protocolo de interacción para la red conmutada diseñada en la etapa II.

Para la evidencia de que los hosts de la red se generan en el servidor http de floodlight, se realizará un ping entre diversos hosts pertenecientes a diversos conmutadores, posterior a esto se demostrará la información del host en la pestaña hosts y en topology del controlador. De igual forma se explicará el funcionamiento de una red definida por software en el diseño de la red conmutada para la institución educativa: Unidad Educativa Salinas Innova School.

Comunicación entre host mediante ping

El comando ping ejecutado desde la terminal o CLI de mininet permitirá conocer si el estado de comunicación para la red es efectivo. Una vez el CLI de mininet esté ejecutándose deberá introducirse la línea de comando **h1 ping h10**, de esta manera es como en mininet se envía un ping a cualquier host a comunicar.

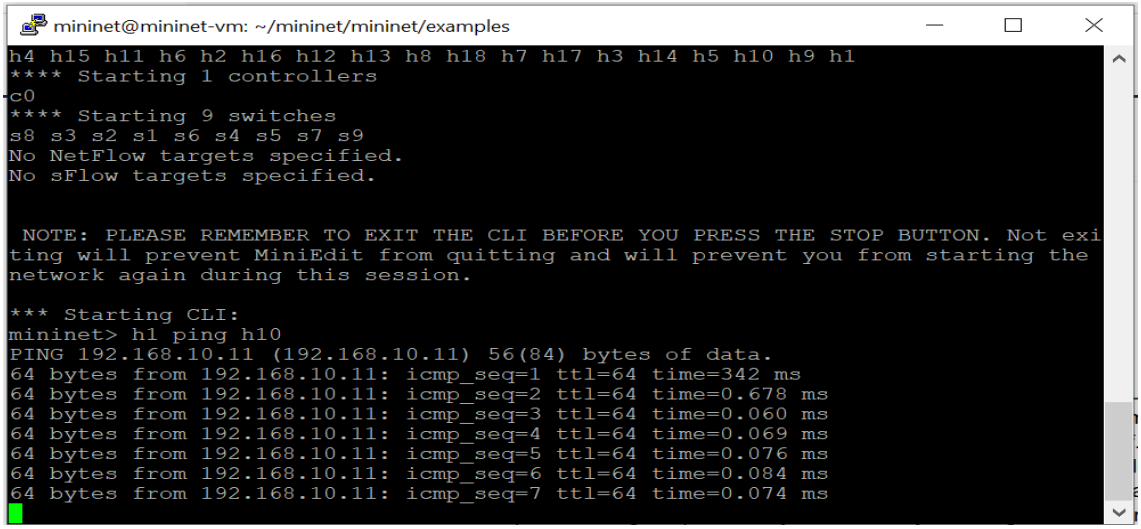


Figura 40. Ejecución de ping entre h1 y h10

Para que el comando ping funcione es necesario que dos hosts o computadoras estén habilitadas en la red, una de origen y otra de destino, y para este caso las máquina que intervienen son h1 con IP 192.168.10.2 y h10 con IP 192.168.10.11, por lo tanto estos dos hosts son los que aparecen en floodlight.

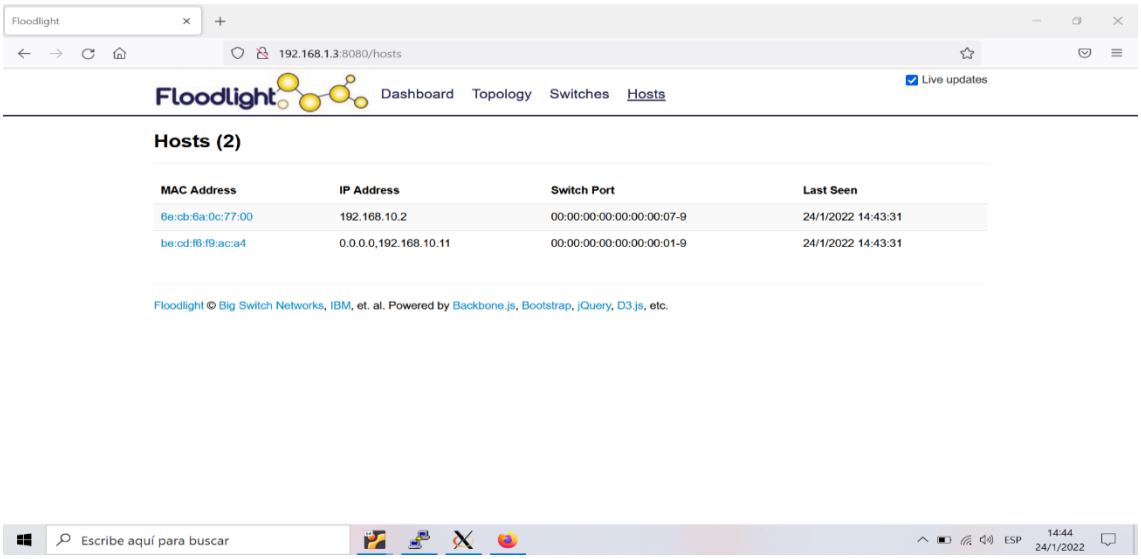


Figura 41. Hosts utilizados en el ping de prueba

Se realizarán tres ejemplos más de ping entre las máquinas para generar dentro de floodlight más hosts que se puedan apreciar dentro de la topología de red: h12 con IP 192.168.10.13 a h15 con IP 192.168.10.6 . De h2 con IP 192.168.10.3 a h9 con IP 192.168.10.10. Y h13 con IP 192.168.10.14 a h18 con IP 192.168.10.19.

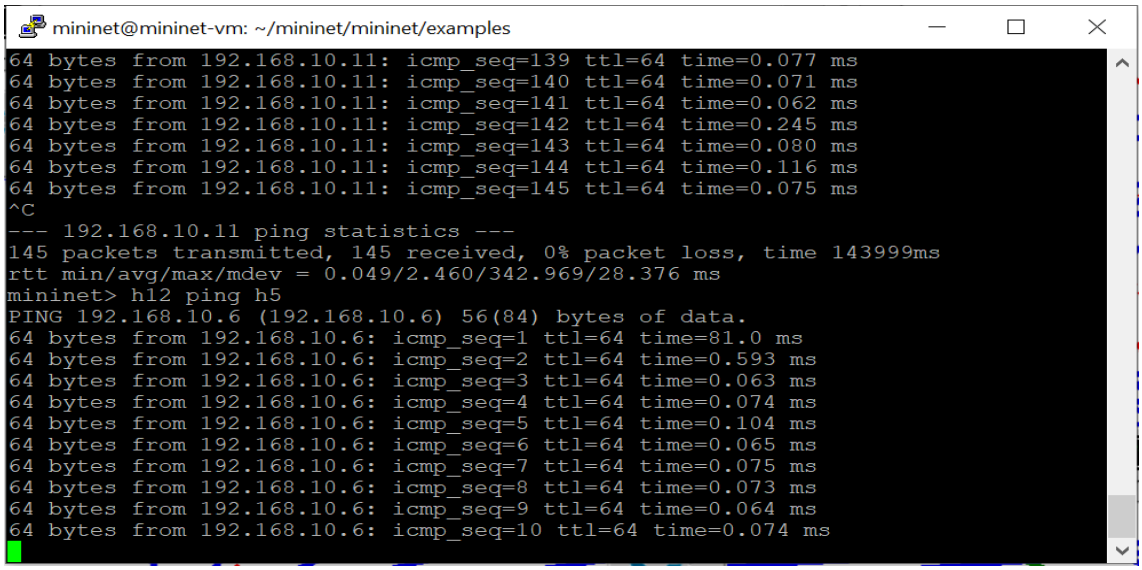


Figura 42. Ejecución de ping entre h12 y h5

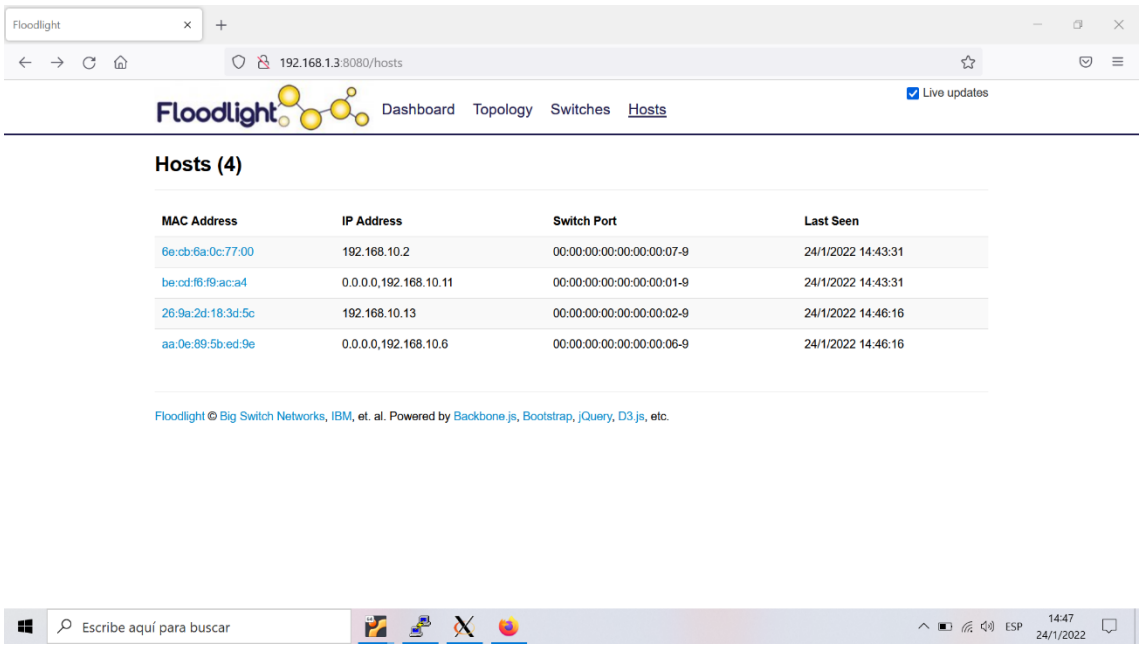


Figura 43. Hosts h12 y h5 generados en floodlight

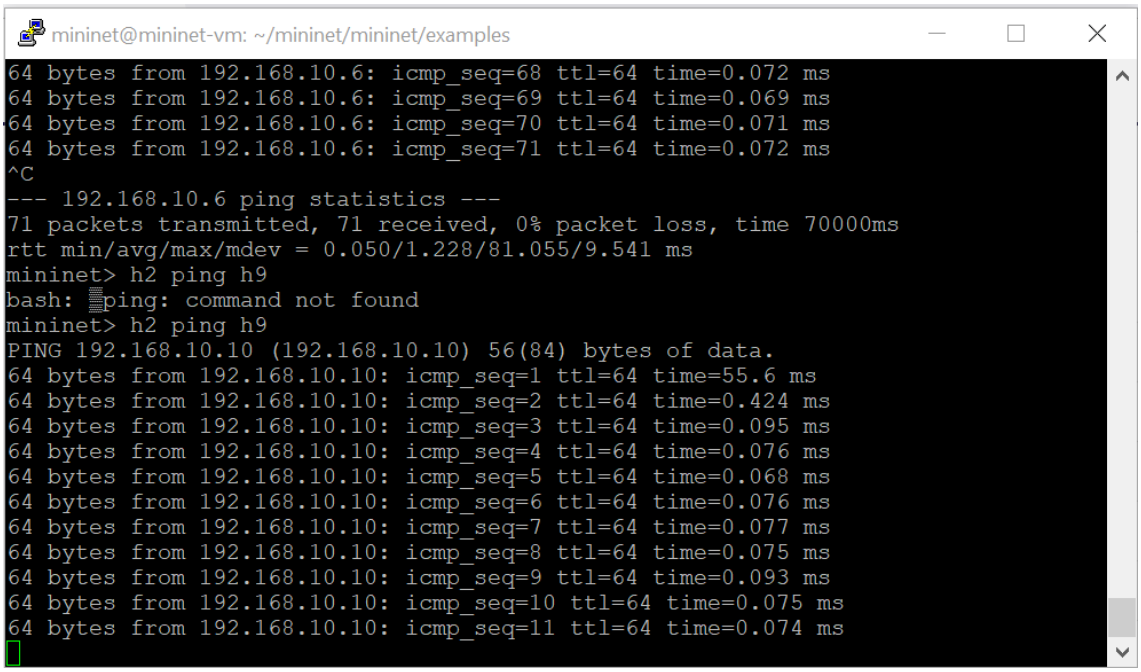


Figura 44. Ejecución de ping entre h2 y h9

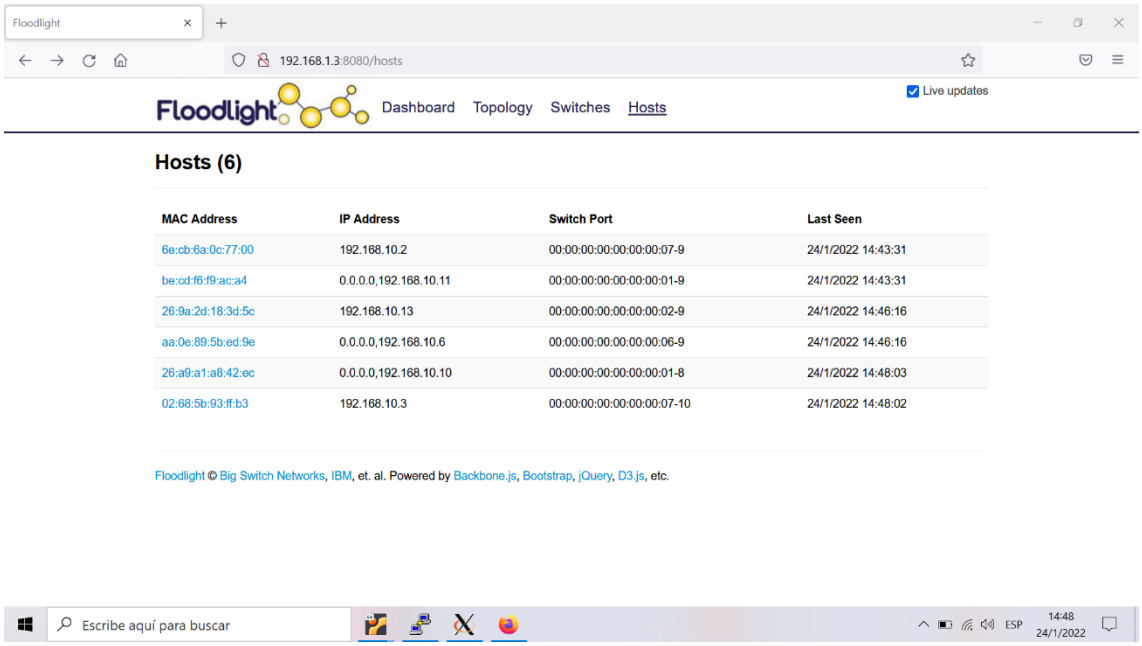


Figura 45. Hosts h2 y h9 generados en floodlight

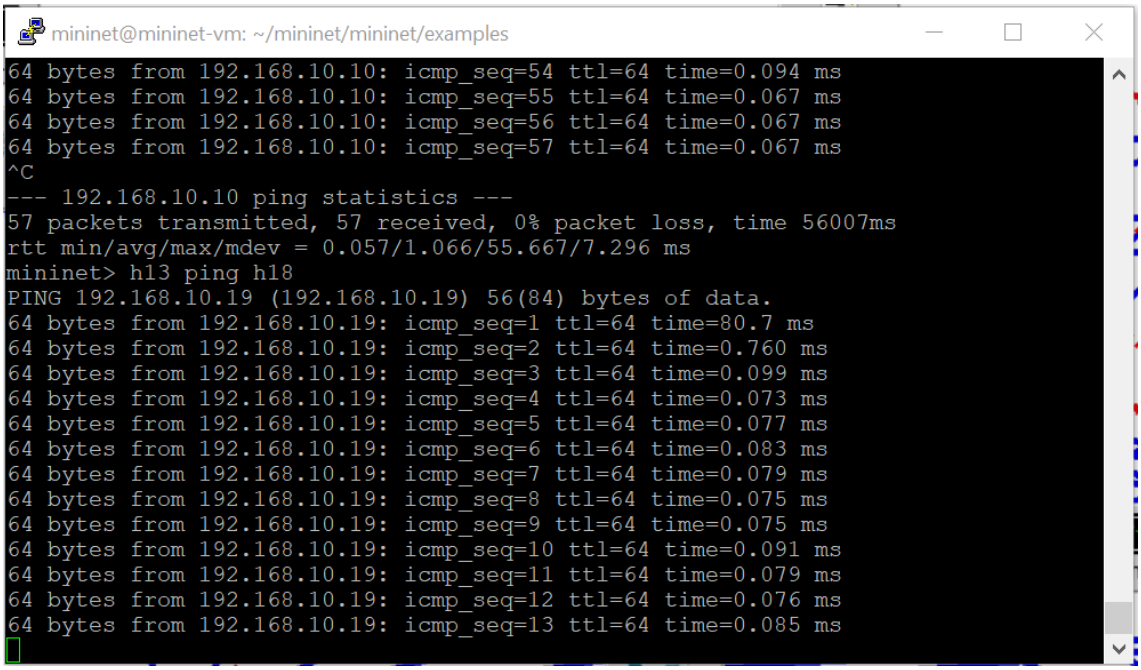


Figura 46. Ejecución de ping entre h13 y h18

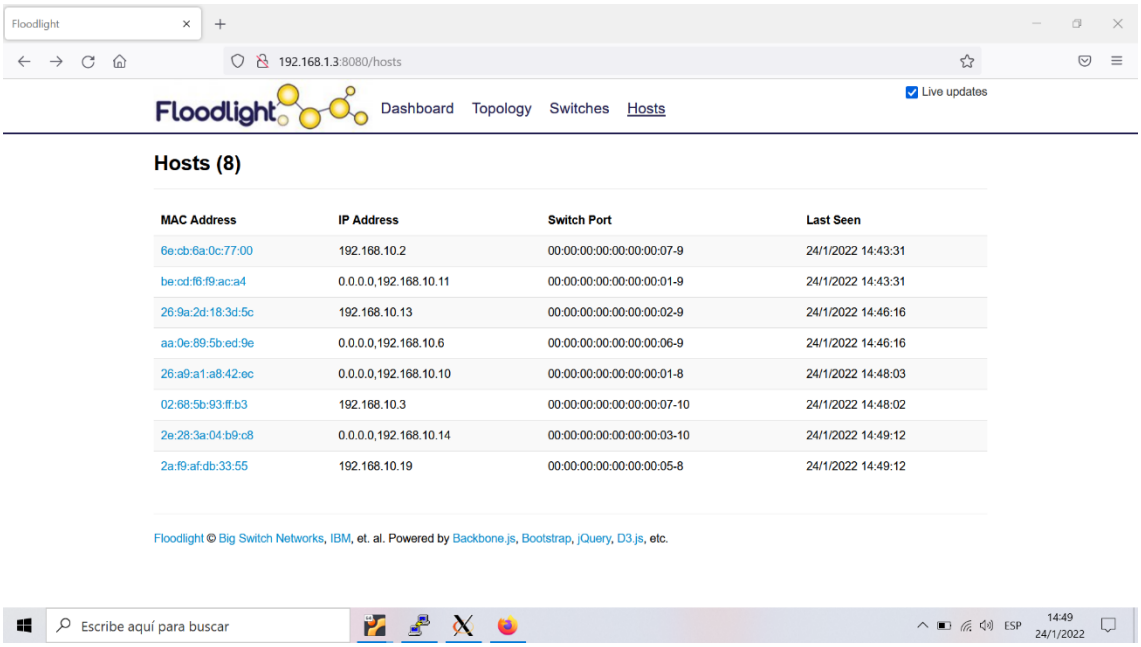


Figura 47. Hosts h13 y h18 generados en floodlight

Host en la topología de floodlight

Al realizar ping entre los hosts no solo se generan en la pestaña respectiva, sino también se puede apreciar en la topología y observar la conexión con sus debidos conmutadores. Los switches son las figuras redondas con flechas de izquierda a derecha conectados entre

sí , y los hosts son los rectángulos con tres líneas horizontales situadas del lado izquierdo conectados a los conmutadores

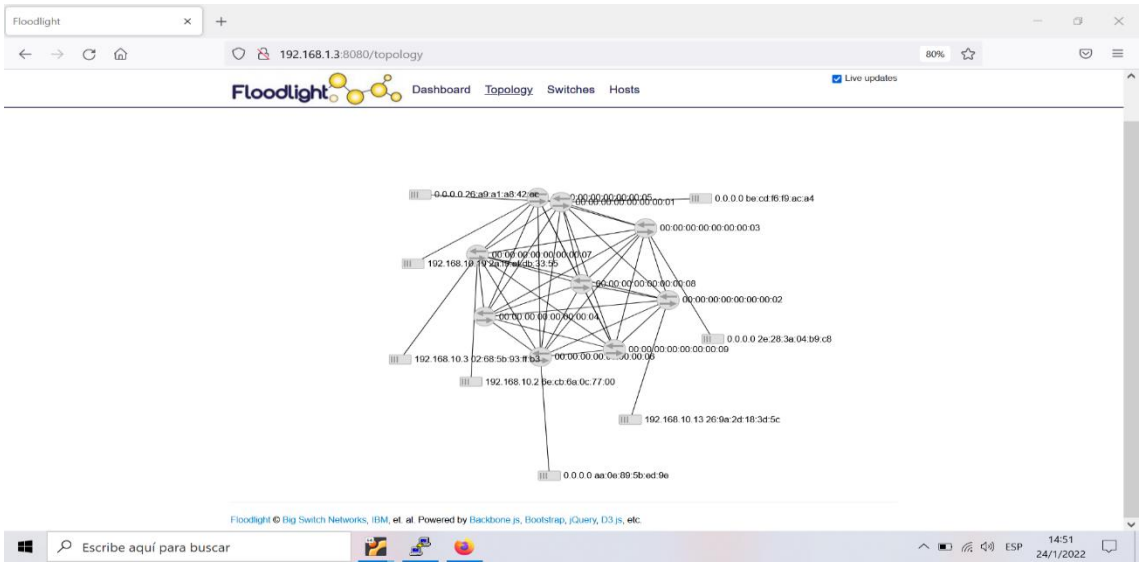


Figura 48. Topología SDN con los hosts utilizados

Funcionamiento de la red SDN y plano de control de floodlight

Una de las características principales de las redes definidas por software es que solo un plano de control funciona para toda la red administrada por el controlador, este se encargará de direccionar los paquetes a su destino en caso de que los switches no sepan a por donde enviarlos en una red conmutada.

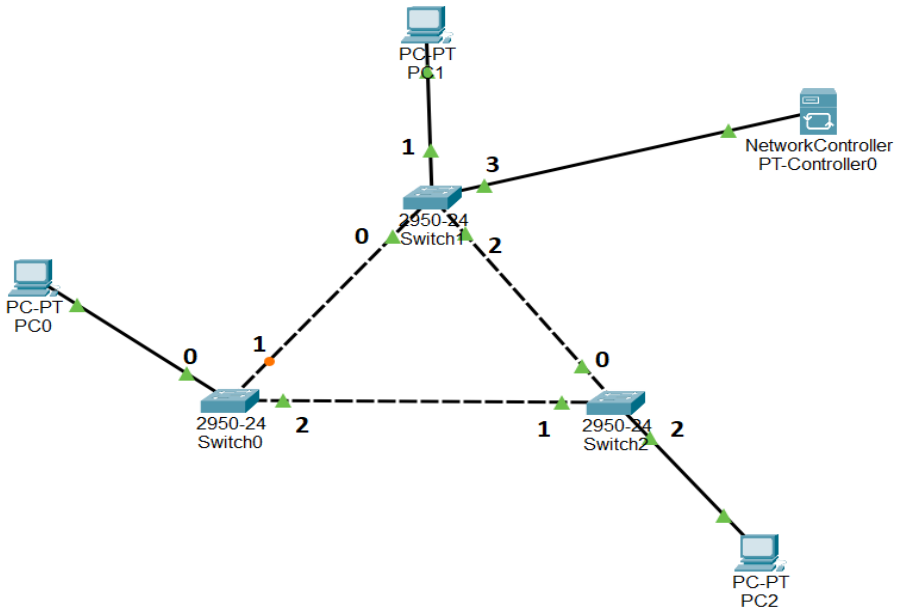


Figura 49. Funcionamiento de una red SDN

Supongamos que la PC 0 quiere enviar un paquete a la PC 1 en un ambiente donde los switches no poseen plano de control, sino es el controlador el único que maneja este plano para reenviar los paquetes. Para que la comunicación entre la PC 0 y PC 1 se realice, la PC 0 debe enviar el paquete al Switch 0 por el puerto 0. Como es el primer paquete que se está enviando, los switches no tienen registrado ninguna ruta dentro de sus tablas de flujo, por lo tanto el Switch 0 direcciona el paquete al controlador ya que los conmutadores lo reconocen. Una vez recibido la consulta por el controlador, este envía como respuesta al Switch 0 que para alcanzar a la PC B el paquete debe ser enviado por el puerto 1 con destino al Switch 1. Cuando se realiza esta entrada de flujo el Switch realiza un proceso de aprendizaje mediante un plano de control general.

En el momento en que el paquete llega al Switch 1 se realiza otra consulta al controlador para recibir instrucciones de cómo conmutar el paquete recibido, de la misma manera el Switch 1 recibe respuesta del controlador que el paquete debe ser reenviado por el puerto 1 con destino a la PC B, y asimismo el Switch 1 realiza un proceso de aprendizaje que los paquetes enviados desde el Switch 0 con destino a la PC B deben ser reenviados por el puerto 1. Para la respuesta de la PC B a la PC A se realiza el mismo proceso, ya que solo se ha registrado en las tablas de flujo lo que se debe hacer en caso de que la comunicación sea entre la PC A con destino a la PC B, pero no desde la PC B hacia la PC A. Para esto La PC B envía el paquete al Switch 1 y realiza la consulta al controlador hacia qué puerto debe enviar el paquete para que llegue a su destino.

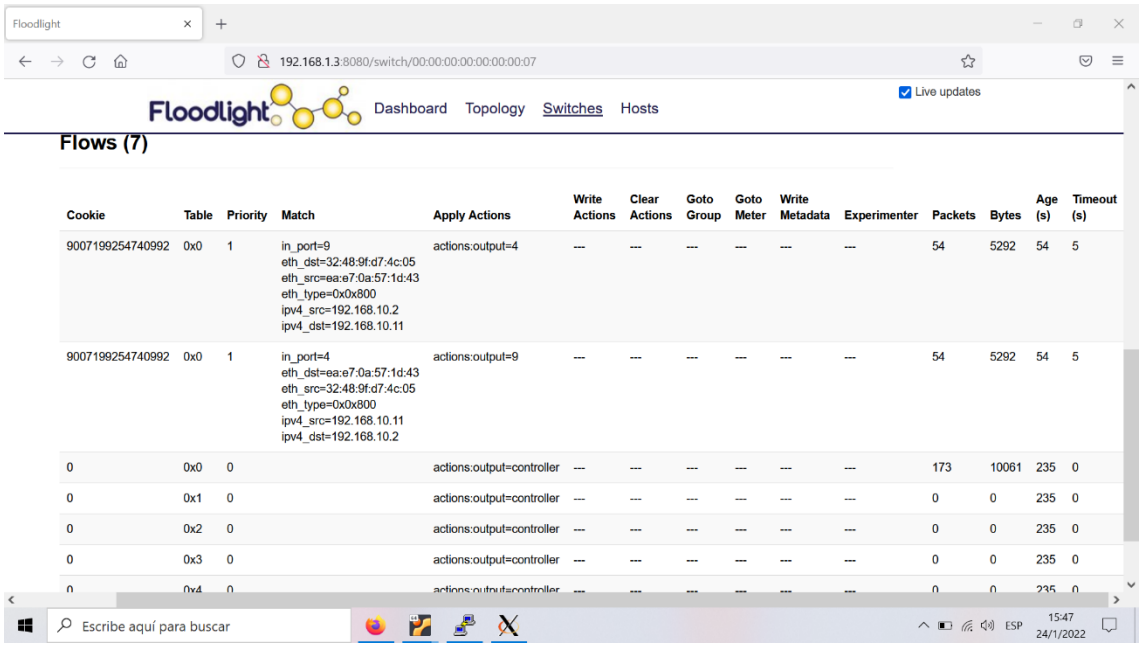
El controlador recibe esta información y da como respuesta que debe ser reenviado por el puerto 0 hacia el Switch 0. El Switch 0 vuelve a consultar cómo debe conmutar el paquete recibido desde el Switch 1 siendo la respuesta del controlador que debe ser reenviado por el puerto 0 hacia la PC A. De esta manera la comunicación desde la PC A hacia la PC B y la respuesta de haber recibido el paquete de la PC B hacia la PC A es como se realiza en una red definida por software. Desde este punto si las dos computadoras se quieren comunicar de nuevo, ya no será necesario enviar información al controlador sino se realiza de manera directa.

Plano de control en floodlight

Para el ejemplo se utiliza la comunicación entre el host h1 y h10 mediante ping. Se observa la tabla de flujo del switch s7 en su momento de aprendizaje. A primera vista se

observa que el paquete es “mactcheado” mediante la dirección MAC e IPv4 de origen y destino, seguido de esto se muestra el puerto por donde el host h1 envía el paquete hacia el switch s7 siendo este el puerto 9 para ser reenviado a su destino 192.168.10.11 mediante el puerto 4. Las respuestas que envíe el host h10 serán recibidos de manera contraría, es decir, entrarán por el puerto 4 y serán reenviados al puerto 9 con destino a 192.168.10.2.

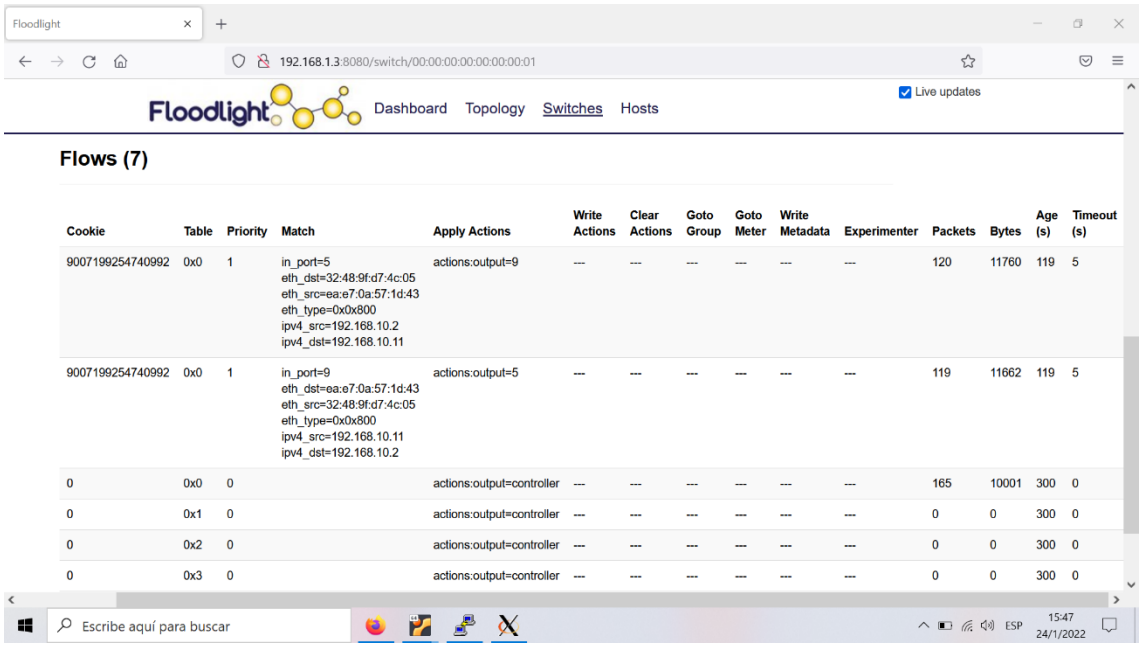
También presenta la prioridad que asignada al paquete, para este caso es prioridad 1 por tratarse de una interacción con otro host. Lo que se detalla más abajo son prioridad 0 porque no existen otros paquetes desde otros hosts que deban ser registrados en la tabla de flujo. En la columna **Apply Actions** a partir de la tercera fila se observa que los puertos de salida son direccionados al controlador.



Cookie	Table	Priority	Match	Apply Actions	Write Actions	Clear Actions	Goto Group	Goto Meter	Write Metadata	Experimenter	Packets	Bytes	Age (s)	Timeout (s)
9007199254740992	0x0	1	in_port=9 eth_dst=32:48:9f:d7:4c:05 eth_src=ea:e7:0a:57:1d:43 eth_type=0x0x800 ipv4_src=192.168.10.2 ipv4_dst=192.168.10.11	actions:output=4	---	---	---	---	---	---	54	5292	54	5
9007199254740992	0x0	1	in_port=4 eth_dst=ea:e7:0a:57:1d:43 eth_src=32:48:9f:d7:4c:05 eth_type=0x0x800 ipv4_src=192.168.10.11 ipv4_dst=192.168.10.2	actions:output=9	---	---	---	---	---	---	54	5292	54	5
0	0x0	0		actions:output=controller	---	---	---	---	---	---	173	10061	235	0
0	0x1	0		actions:output=controller	---	---	---	---	---	---	0	0	235	0
0	0x2	0		actions:output=controller	---	---	---	---	---	---	0	0	235	0
0	0x3	0		actions:output=controller	---	---	---	---	---	---	0	0	235	0
0	0x4	0		actions:output=controller	---	---	---	---	---	---	0	0	235	0

Figura 50. Tabla de flujo del switch s7. Ping h1 a h10

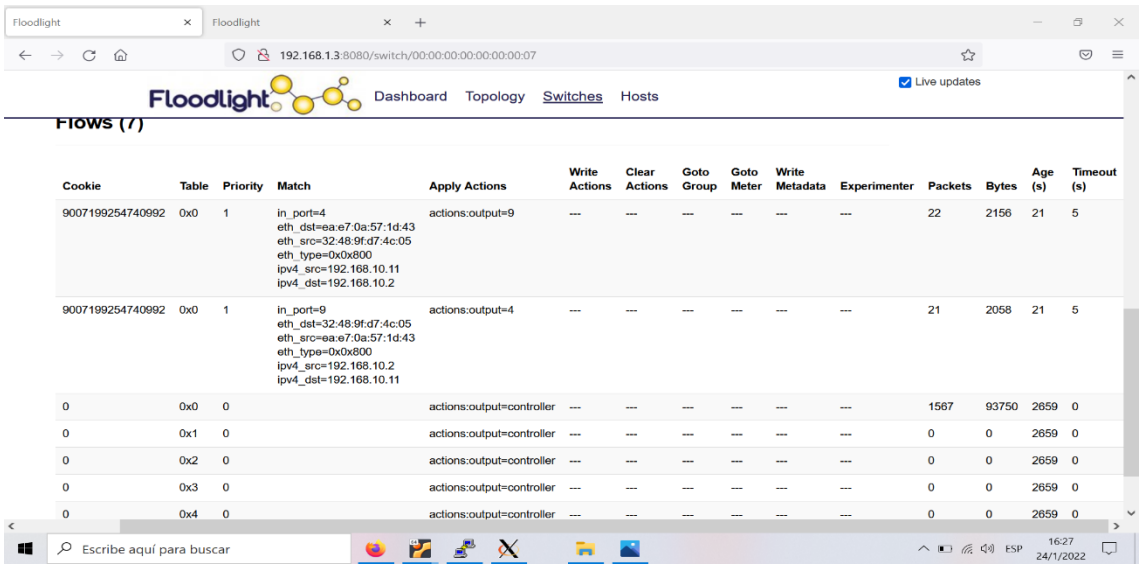
Se observa la tabla de flujo del switch s1 “matcheado” de igual manera con dirección MAC e IP de origen y destino, cambiando únicamente los puertos de entrada y salida. De este lado del switch puede ser confuso, pero la teoría es la misma. La respuesta que dará el host h10 a h1 entrará por el puerto 5 del switch s1 siendo su puerto de salida el puerto 9 con destino al switch s7.



Cookie	Table	Priority	Match	Apply Actions	Write Actions	Clear Actions	Goto Group	Goto Meter	Write Metadata	Experimenter	Packets	Bytes	Age (s)	Timeout (s)
9007199254740992	0x0	1	in_port=5 eth_dst=32:48:9f:d7:4c:05 eth_src=ea:e7:0a:57:1d:43 eth_type=0x0x800 ipv4_src=192.168.10.2 ipv4_dst=192.168.10.11	actions:output=9	---	---	---	---	---	---	120	11760	119	5
9007199254740992	0x0	1	in_port=9 eth_dst=ea:e7:0a:57:1d:43 eth_src=32:48:9f:d7:4c:05 eth_type=0x0x800 ipv4_src=192.168.10.11 ipv4_dst=192.168.10.2	actions:output=5	---	---	---	---	---	---	119	11662	119	5
0	0x0	0		actions:output=controller	---	---	---	---	---	---	165	10001	300	0
0	0x1	0		actions:output=controller	---	---	---	---	---	---	0	0	300	0
0	0x2	0		actions:output=controller	---	---	---	---	---	---	0	0	300	0
0	0x3	0		actions:output=controller	---	---	---	---	---	---	0	0	300	0

Figura 51. Tabla de flujo del switch s1. Ping h1 a h10

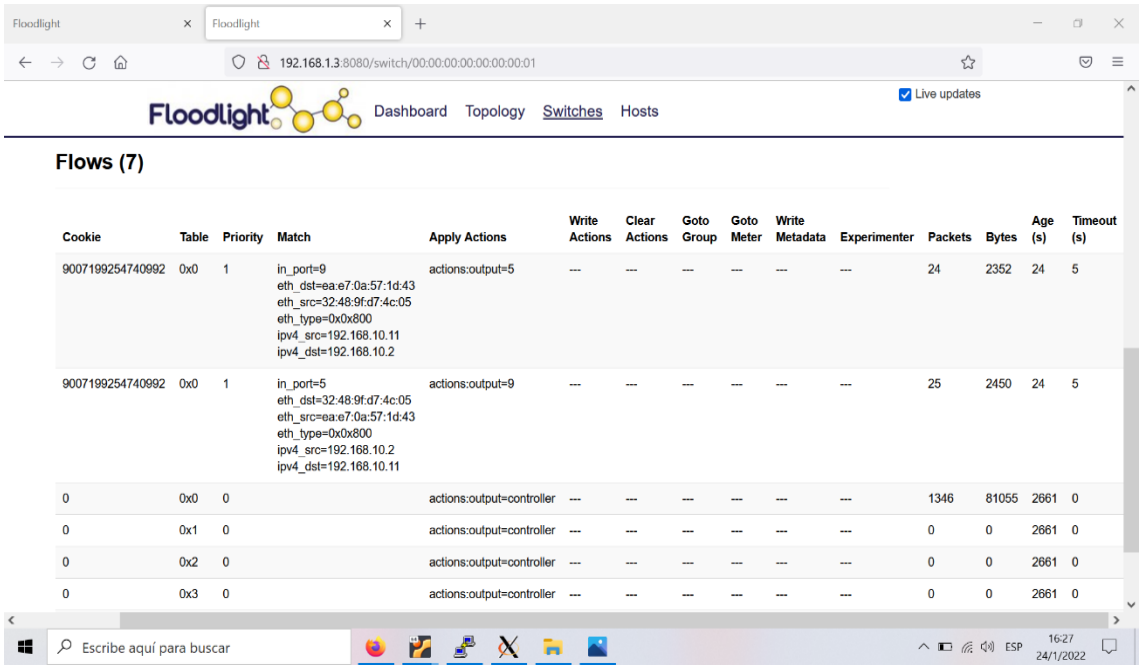
Para un mejor entendimiento se envía un ping desde el host h10 a h1, todo lo contrario. Dentro de la tabla de flujo de switch s7 se "matchea" el paquete con dirección MAC e IP de origen y destino, siendo el puerto de entrada al switch s7 el puerto 4 para ser reenviados por el puerto 9 del mismo switch. Cuando el host h1 quiera enviar una respuesta, esta entrará al switch s7 por el puerto 9 para ser reenviado al host h10 mediante el puerto 4.



Cookie	Table	Priority	Match	Apply Actions	Write Actions	Clear Actions	Goto Group	Goto Meter	Write Metadata	Experimenter	Packets	Bytes	Age (s)	Timeout (s)
9007199254740992	0x0	1	in_port=4 eth_dst=ea:e7:0a:57:1d:43 eth_src=32:48:9f:d7:4c:05 eth_type=0x0x800 ipv4_src=192.168.10.11 ipv4_dst=192.168.10.2	actions:output=9	---	---	---	---	---	---	22	2156	21	5
9007199254740992	0x0	1	in_port=9 eth_dst=32:48:9f:d7:4c:05 eth_src=ea:e7:0a:57:1d:43 eth_type=0x0x800 ipv4_src=192.168.10.2 ipv4_dst=192.168.10.11	actions:output=4	---	---	---	---	---	---	21	2058	21	5
0	0x0	0		actions:output=controller	---	---	---	---	---	---	1567	93750	2659	0
0	0x1	0		actions:output=controller	---	---	---	---	---	---	0	0	2659	0
0	0x2	0		actions:output=controller	---	---	---	---	---	---	0	0	2659	0
0	0x3	0		actions:output=controller	---	---	---	---	---	---	0	0	2659	0
0	0x4	0		actions:output=controller	---	---	---	---	---	---	0	0	2659	0

Figura 52. Tabla de flujo del switch s7. Ping h10 a h1

En la tabla de flujo del switch s1 está registrada la respuesta que se la dará al host h10. El puerto por el que se enviará la respuesta al switch h1 será el puerto 9 para ser reenviado por el puerto 5 hacia el switch s7 con destino al host h10.



Cookie	Table	Priority	Match	Apply Actions	Write Actions	Clear Actions	Goto Group	Goto Meter	Write Metadata	Experimenter	Packets	Bytes	Age (s)	Timeout (s)
9007199254740992	0x0	1	in_port=9 eth_dst=ea:e7:0a:57:1d:43 eth_src=32:48:9f:d7:4c:05 eth_type=0x0x800 ipv4_src=192.168.10.11 ipv4_dst=192.168.10.2	actions:output=5	---	---	---	---	---	---	24	2352	24	5
9007199254740992	0x0	1	in_port=5 eth_dst=32:48:9f:d7:4c:05 eth_src=ea:e7:0a:57:1d:43 eth_type=0x0x800 ipv4_src=192.168.10.2 ipv4_dst=192.168.10.11	actions:output=9	---	---	---	---	---	---	25	2450	24	5
0	0x0	0		actions:output=controller	---	---	---	---	---	---	1346	81055	2661	0
0	0x1	0		actions:output=controller	---	---	---	---	---	---	0	0	2661	0
0	0x2	0		actions:output=controller	---	---	---	---	---	---	0	0	2661	0
0	0x3	0		actions:output=controller	---	---	---	---	---	---	0	0	2661	0

Figura 53. Tabla de flujo del switch s1. Ping h10 a h1

Tráfico de red generado

Las redes definidas por software también generan tráfico de red, pero este tráfico está generado bajo el protocolo OpenFlow que utiliza el controlador para decirle a los conmutadores hacia dónde conmutar los paquetes. Para comprobar este tráfico se utiliza la herramienta wireshark. Se debe acceder a floodlight de manera remota con putty para mejor manejo del software al igual que se lo hizo con mininet para trabajar con miniedit. Las configuraciones son las mismas, se debe habilitar X11 para acceso remoto a entornos gráficos y luego realizar la conexión remota con la IP del controlador. Las credenciales son las mismas, floodlight como user y password. Al aparecer el CLI de floodlight se ejecuta el comando **sudo wireshark** para abrir la herramienta.

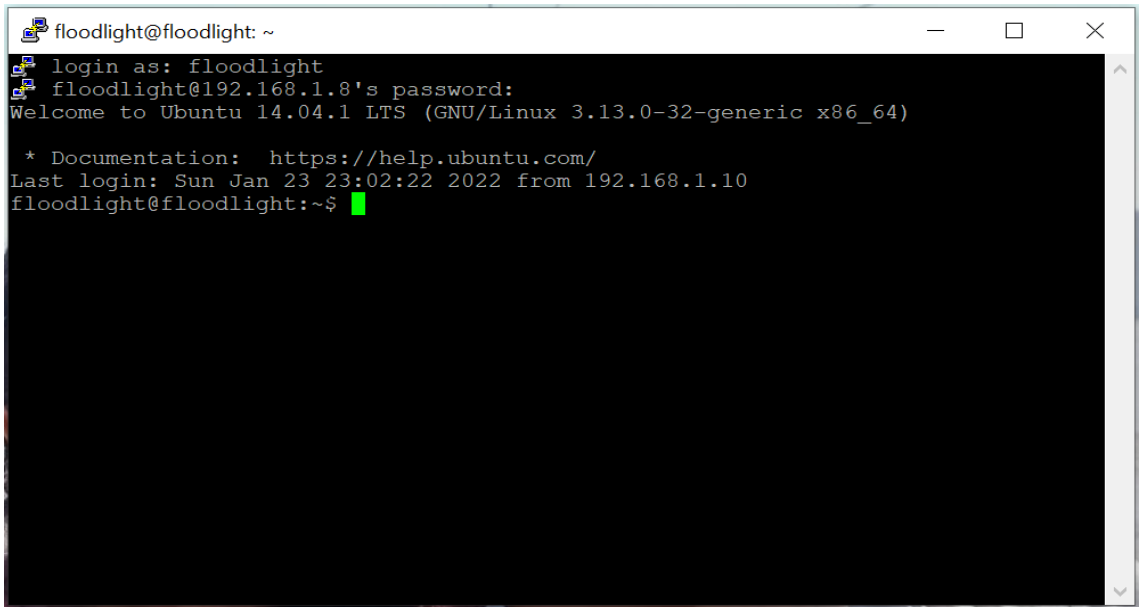


Figura 54. Acceso a floodlight vía putty

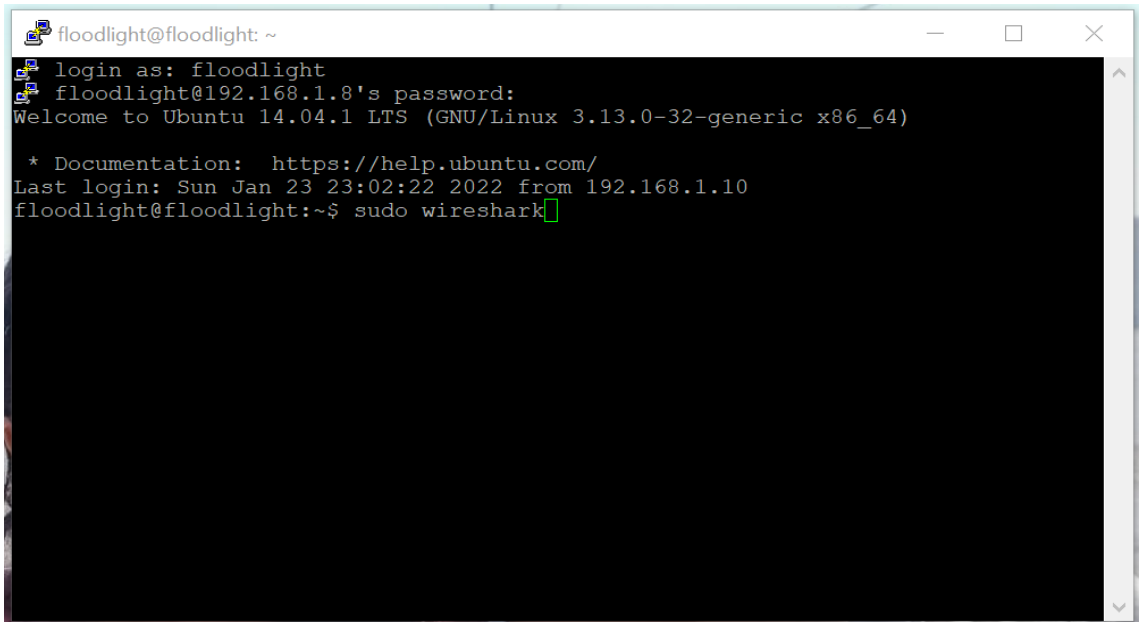


Figura 55. Ejecución de wireshark

Se abrirá wireshark ejecutado con privilegios elevados de super usuario. Wireshark sirve para inspeccionar el tráfico de red, para eso se debe elegir la interfaz a revisar. Presionando la lista de interfaces se observa que la primera interfaz es la eth0 con la IP del controlador 192.168.1.8. Esta será la interfaz por analizar.

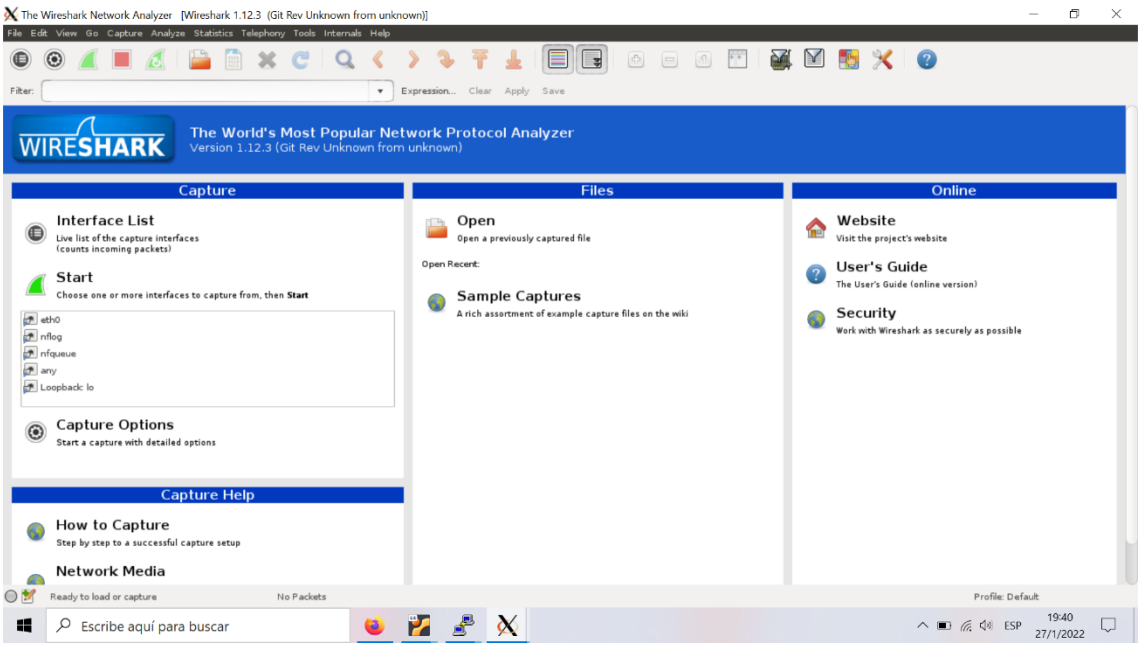


Figura 56. Interfaz de wireshark

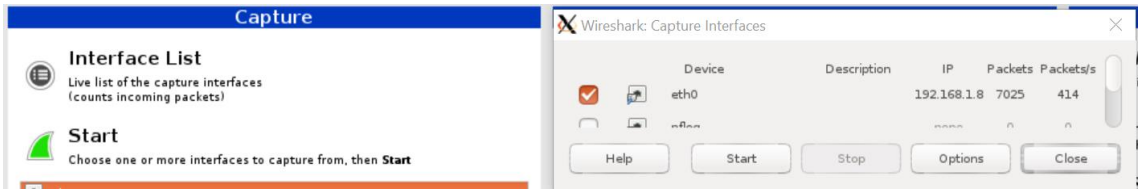


Figura 57. Selección de interfaces de red para analizar el tráfico de red

Una vez seleccionado la interfaz aparecerán varios protocolos que son ejecutados en la red. Para tener una mejor vista del protocolo OpenFlow se debe filtrar por este protocolo.

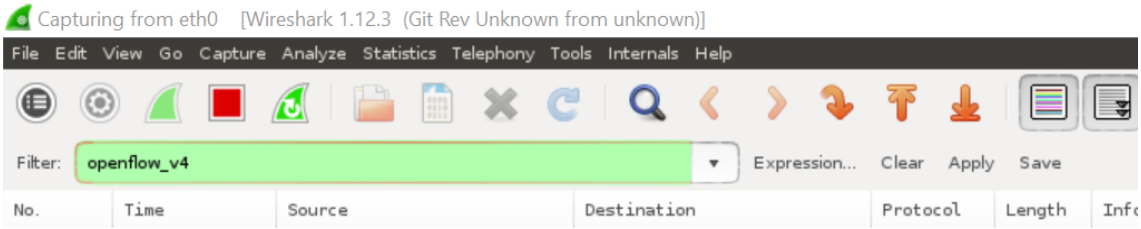


Figura 58. Filtro de paquetes por openflow

Ya filtrado aparece todo el tráfico OpenFlow que se está generando en esta red. Las dos IP que interactúan pertenecen a floodlight 192.168.1.8 y a mininet 192.168.1.11. Es por haber realizado previas configuraciones a las máquinas virtuales como conector puente. Son las dos únicas IP que se muestran por ser IP asignadas por el router y porque trabajan de manera independiente, mininet se comunica con floodlight, y floodlight con mininet.

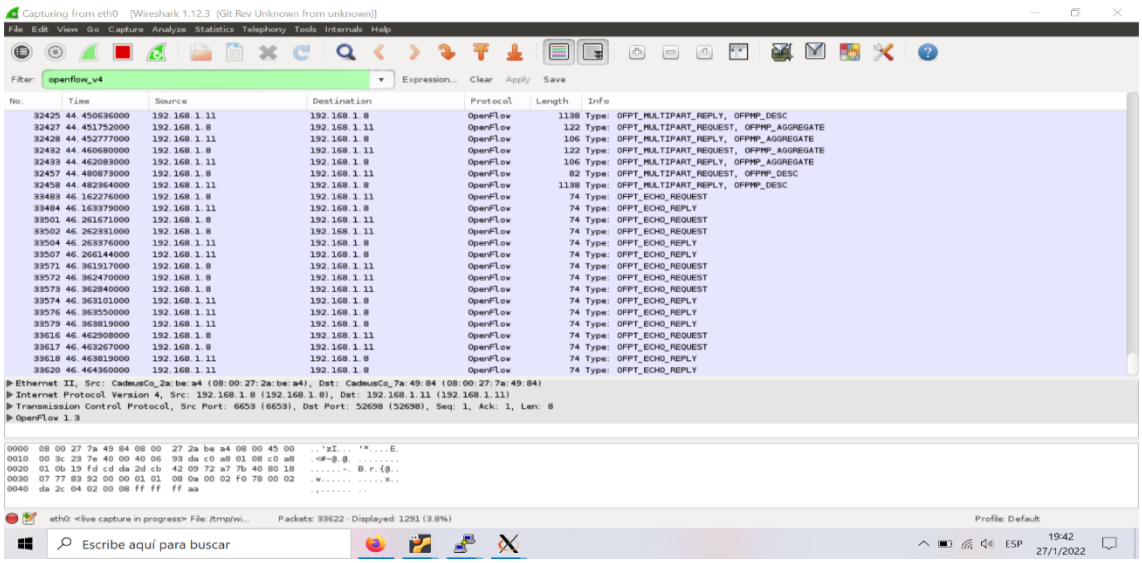


Figura 59. Tráfico de red del protocolo openflow

Al abrir una trama se observa lo que este contiene como los protocolos IPv4 y TCP. Las direcciones IP y los puertos que están interactuando son: como origen 192.168.1.11, 52704 perteneciente a mininet y de destino 192.168.1.8, 6653 perteneciente al controlador. Se presenta en este orden porque el paquete que se seleccionó es una respuesta de mininet hacia floodlight.

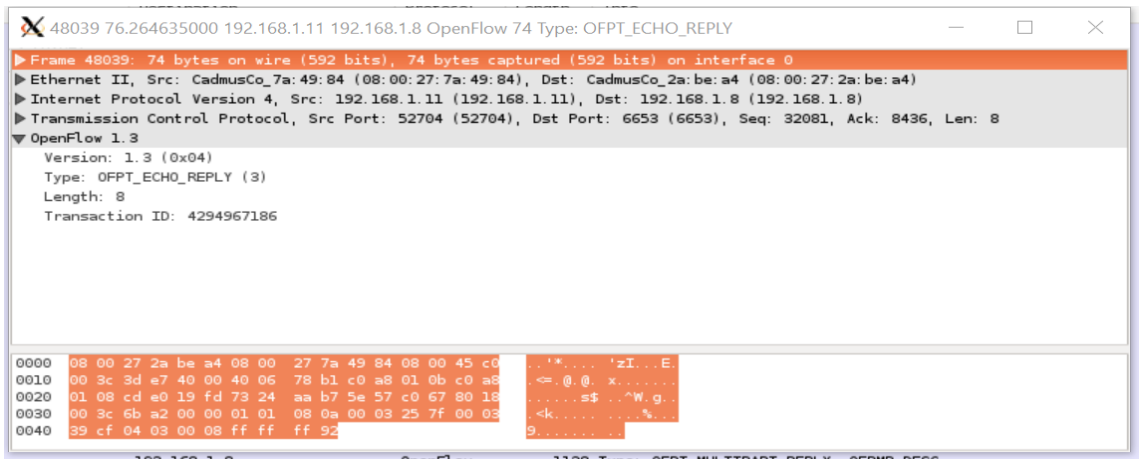


Figura 60. Trama abierta para la visualización del contenido

Tráfico de la red LAN

La red con la que funciona floodlight y mininet es (para entendimiento de este proyecto) WAN, y la red que generó mininet para control de floodlight es LAN. Para inspeccionar el tráfico de la red 192.168.10.0 se realizará un nuevo ping entre los hosts h4 y h10. Al realizar el ping, dentro de wireshark aparecen 4 tramas subrayadas generadas por el mismo protocolo OpenFlow. Estás 4 tramas son las que describen el proceso de enviar información y recibir una respuesta.

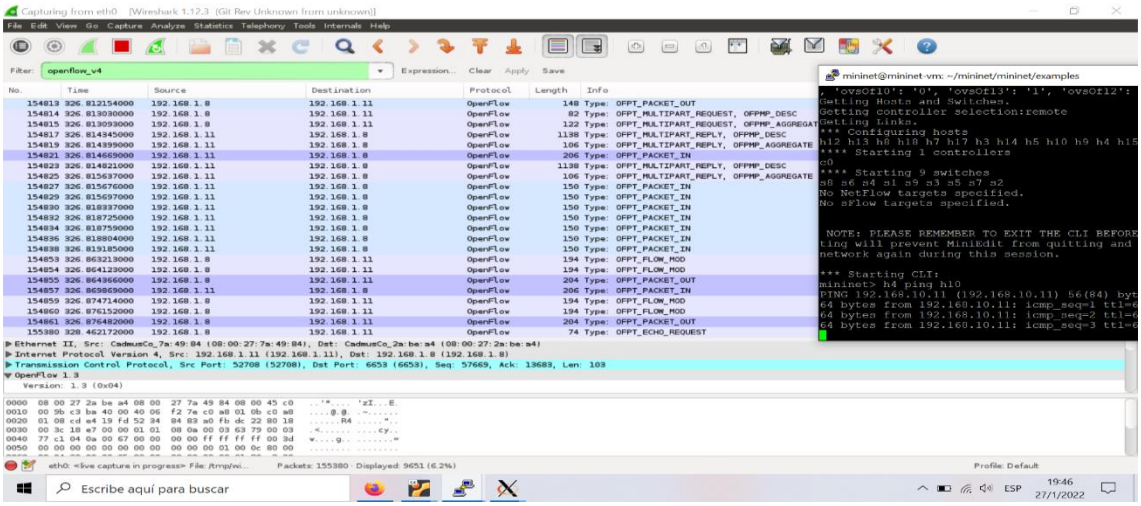


Figura 61. Tráfico de red generado al hacer ping entre h4 y h10

Al abrir la primera trama generada se muestra información del protocolo OpenFlow como la versión del protocolo y el tipo de paquete. Además se visualiza los datos que contiene este protocolo perteneciente a la red LAN "matcheado" por MAC de origen y destino, e IP de origen y destino.

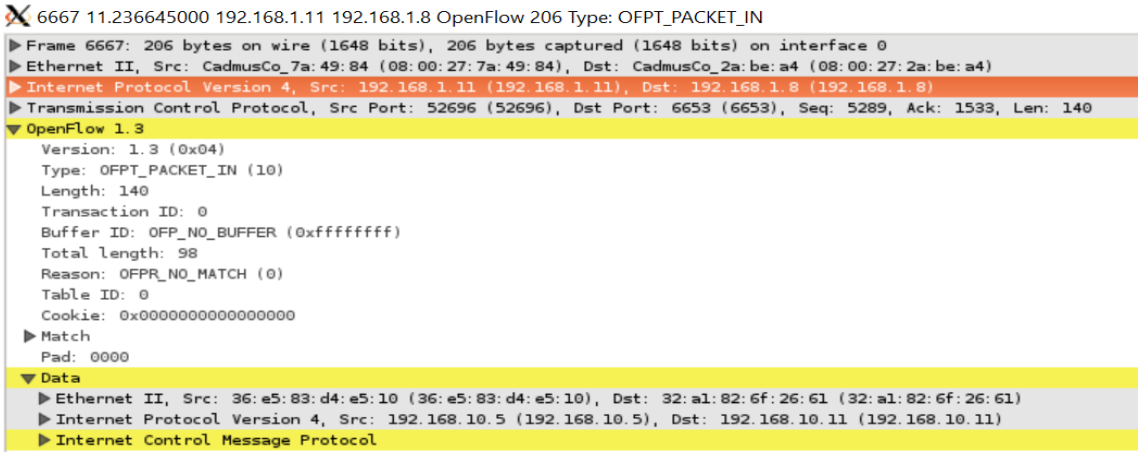


Figura 62. Primera trama abierta de la interacción entre h4 y h10

Por parte del “matcheo” de MAC se especifica que el destino es el host h10 siendo el origen el host h4. Tanto en el destino como en el origen el bit LG e IG permanecen iguales por ser una MAC alterada de administrativamente (LG) y por ser de unidifusión.

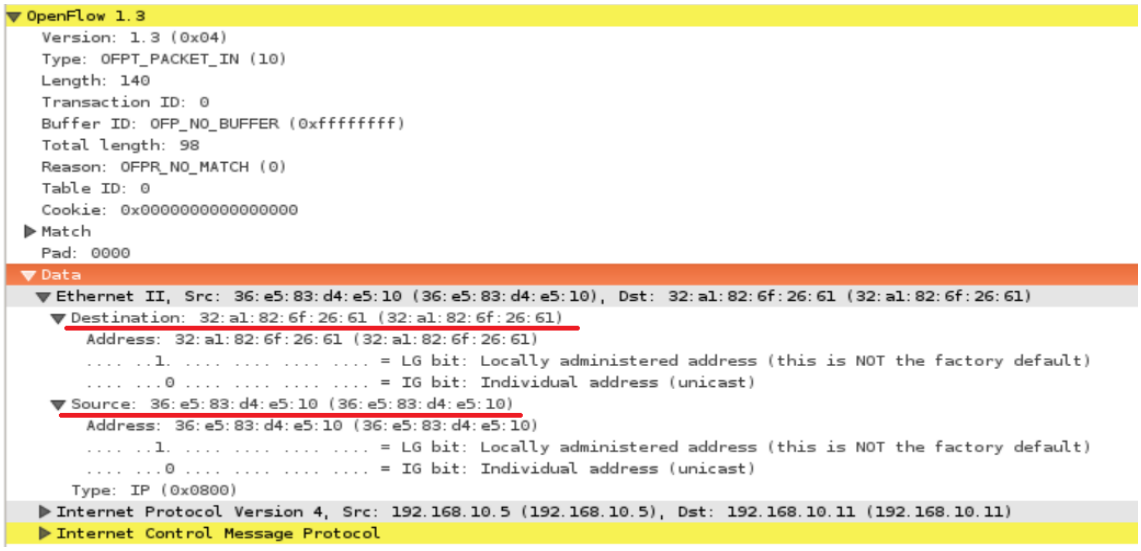


Figura 63. Matcheo de MAC entre h4 y h10

Por el lado del “matcheo” por IP, al abrir la cabecera se observa la dirección IP de origen y destino. Para este paso aún no se realiza el proceso de aprendizaje, esto es deducible porque no aparece la acción que debe realizar el conmutador, como por qué puerto debe ser redireccionado el paquete.

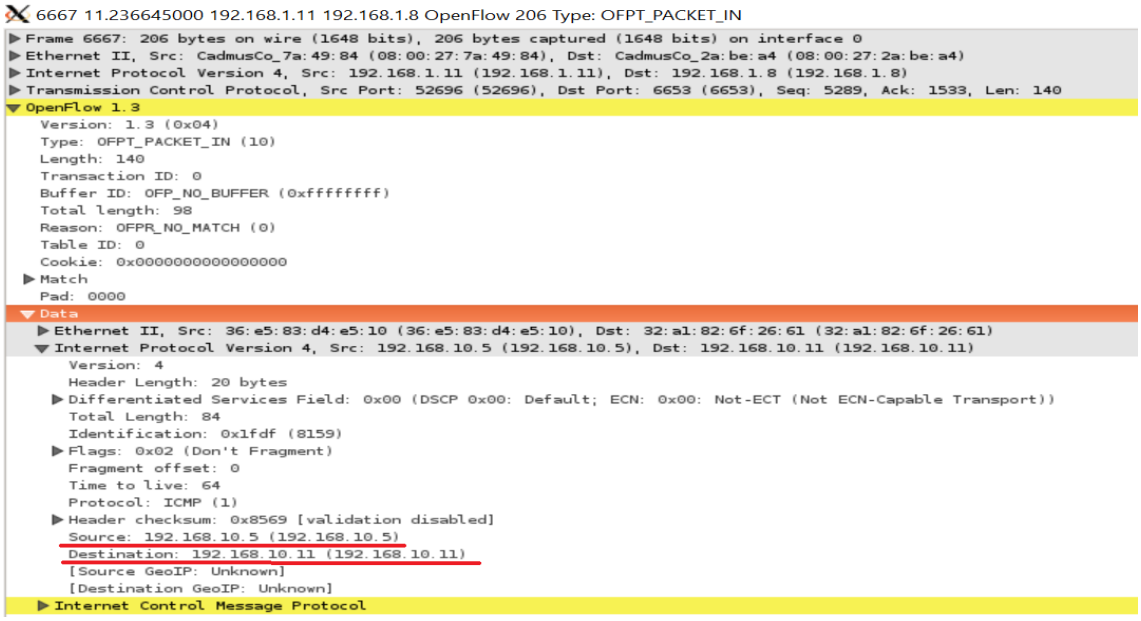


Figura 64. Matcheo de IP entre h4 y h10

Al abrir el siguiente paquete el proceso de aprendizaje es realizado diciendo que la acción que debe realizar el conmutador es reenviar el paquete del host h4 a través del puerto 10 para ser reenviado por el puerto 4 del switch s8.

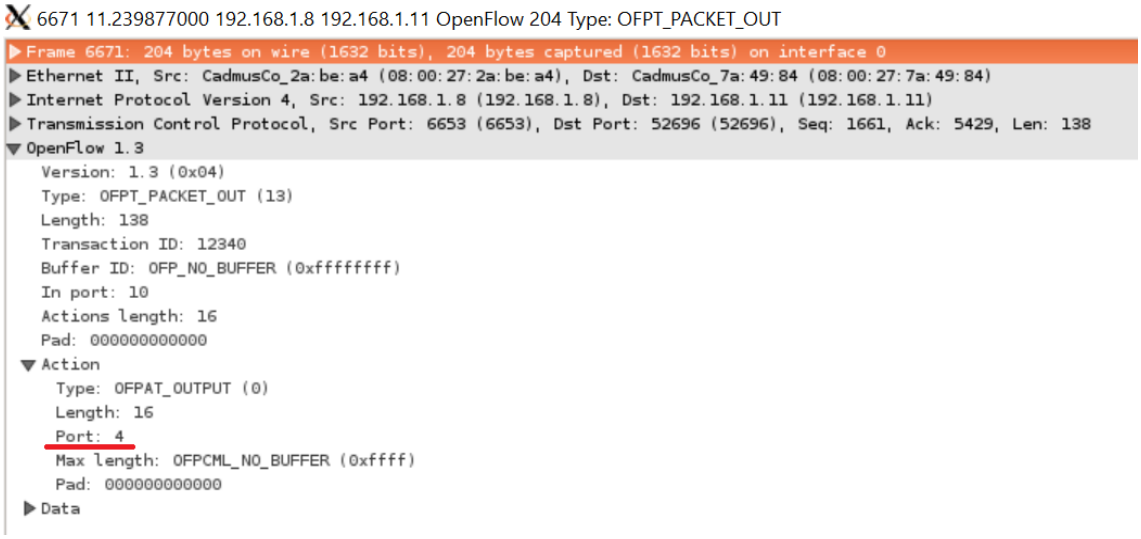


Figura 65. Proceso de aprendizaje del switch s8

El siguiente paquete que se abre es la respuesta del host h10 a h4 donde al igual que el primero es “matcheado” por dirección MAC de origen y destino. Ahora las direcciones se intercambian al ser una respuesta. Los conceptos de bit LG e IG son los mismos.

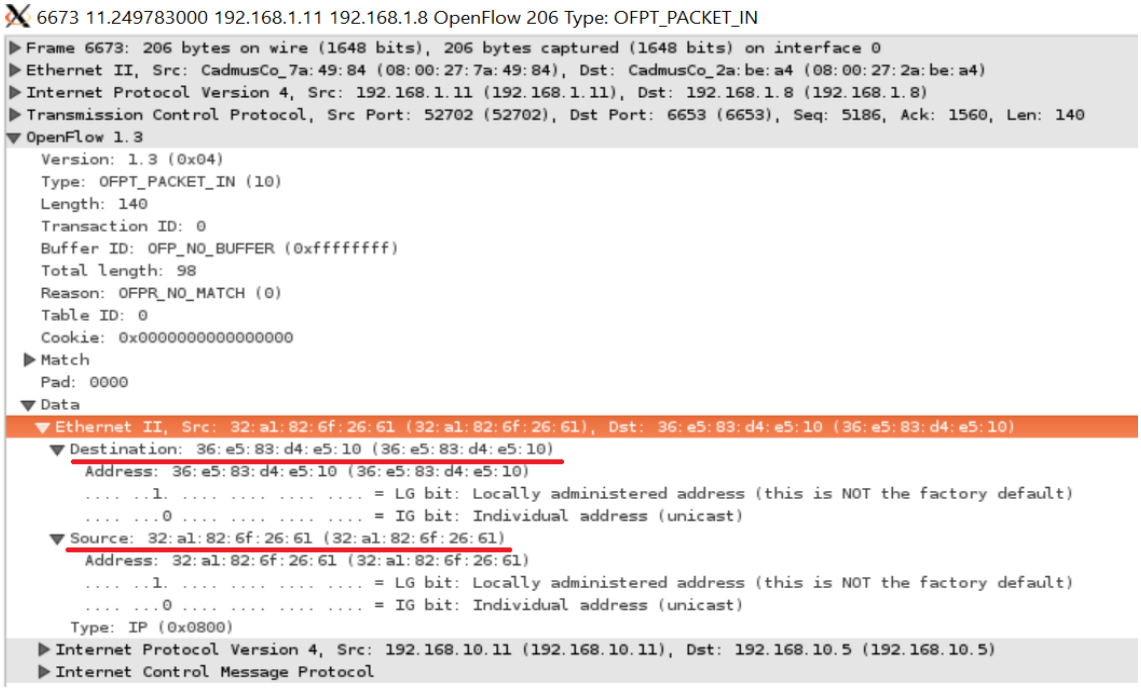


Figura 66. Respuesta de h10 a h4 matcheado por MAC

De igual forma el “matcheo” se presenta por IP de origen y destino, ahora intercambiados por tratarse de una respuesta del host h10.

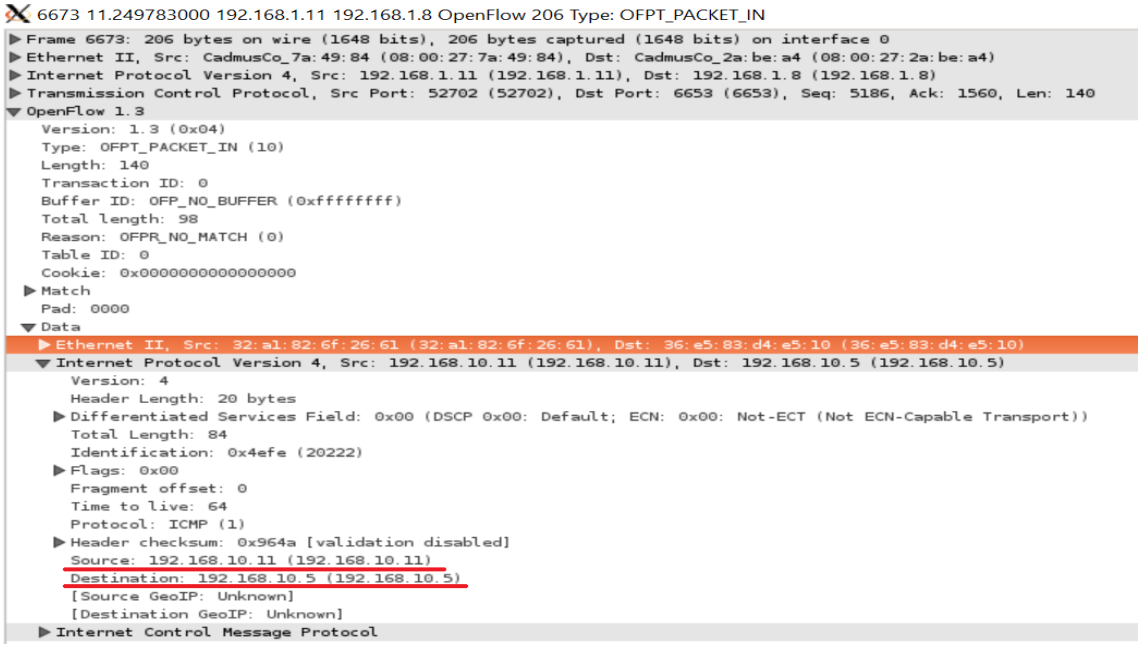


Figura 67. Respuesta de h10 a h4 matcheado por IP

Por el lado del switch s1, la acción que se está realizando es el aprendizaje por donde debe entrar el paquete para llegar al host h10, entrando por el puerto 9 y saliendo por e puerto 6. Esos puertos serán los mismo cuando se trate de enviar una respuesta o enviar un nuevo paquete al host h4.

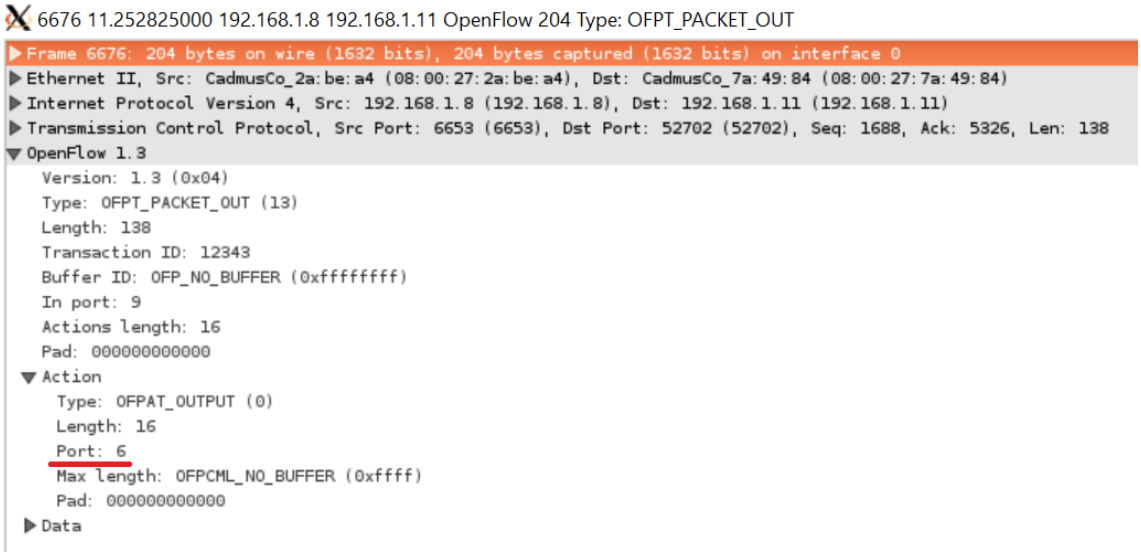


Figura 68. Proceso de aprendizaje del switch s1

La tabla de flujo que presenta floodlight coincide con el tráfico analizado con wireshark

Match	Apply Actions
in_port=10 eth_dst=32:a1:82:6f:26:61 eth_src=36:e5:83:d4:e5:10 eth_type=0x0x800 ipv4_src=192.168.10.5 ipv4_dst=192.168.10.11	actions:output=4
in_port=4 eth_dst=36:e5:83:d4:e5:10 eth_src=32:a1:82:6f:26:61 eth_type=0x0x800 ipv4_src=192.168.10.11 ipv4_dst=192.168.10.5	actions:output=10

Match	Apply Actions
in_port=6 eth_dst=32:a1:82:6f:26:61 eth_src=36:e5:83:d4:e5:10 eth_type=0x0x800 ipv4_src=192.168.10.5 ipv4_dst=192.168.10.11	actions:output=9
in_port=9 eth_dst=36:e5:83:d4:e5:10 eth_src=32:a1:82:6f:26:61 eth_type=0x0x800 ipv4_src=192.168.10.11 ipv4_dst=192.168.10.5	actions:output=6

Figura 69. Tabla de flujo de floodlight

Al igual que la diracciones MAC e IP de los host utilizados

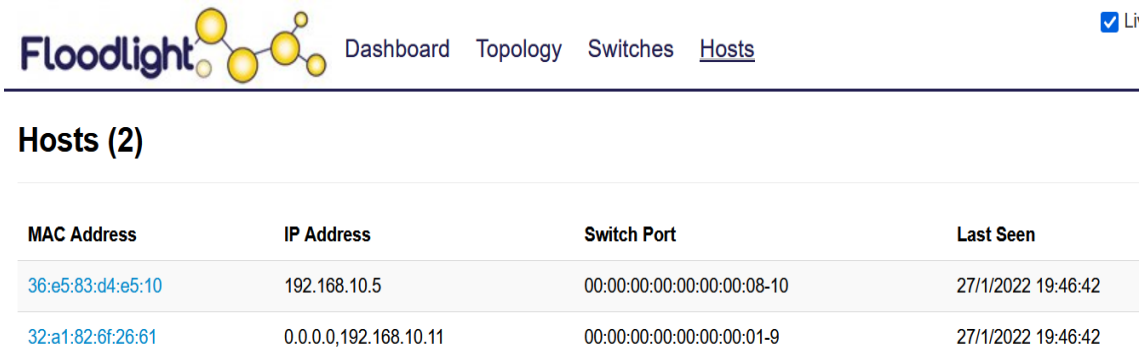


Figura 70. Hosts utilizados en el análisis

2.5.6. Etapa de Optimización

La última etapa del modelo PDIOO de la metodología de este proyecto culmina con la optimización de la red. Aquí se plantean nuevas ideas, se agregan o quitan dispositivos o cambiar el diseño de la red propuesto en la etapa II, en sí dependiendo de lo nuevo que se quiera implementar se puede volver a realizar la etapa I de planeación para seleccionar otra tecnología de red, la etapa II para cambiar el diseño, la etapa II para implementar,

sustituir o eliminar un dispositivo o configuración, y la etapa IV para seleccionar otras herramientas para controlar el tráfico de red. El diseño que se propuso en la segunda etapa fue una red conmutada que funcionaba sin estar segmentada, es decir, todos los hosts pertenecían a la misma red con una misma máscara o CIDR, que llevaba a una mala administración y direcciones IP malgastadas.

Para este nuevo paso se retomará desde la etapa II de diseño, la etapa III de implementación, y la etapa IV seguirá siendo controlada por la misma herramienta wireshark. La diferencia de este modelo es el retiro de dos switches sustituidos por un router ubicado en el departamento de sistemas, además de compartir un switch para sistemas y el laboratorio de ciencias al quedar juntos. De la misma manera un solo switch será compartido para los departamentos principales de secretaría, financiero y rectorado. Otra diferencia es la segmentación de red donde se aplicó subnetting VLSM para este propósito y así segmentar por subredes partiendo de la red 192.168.10.0/24 evitando el desperdicio de direcciones IP.

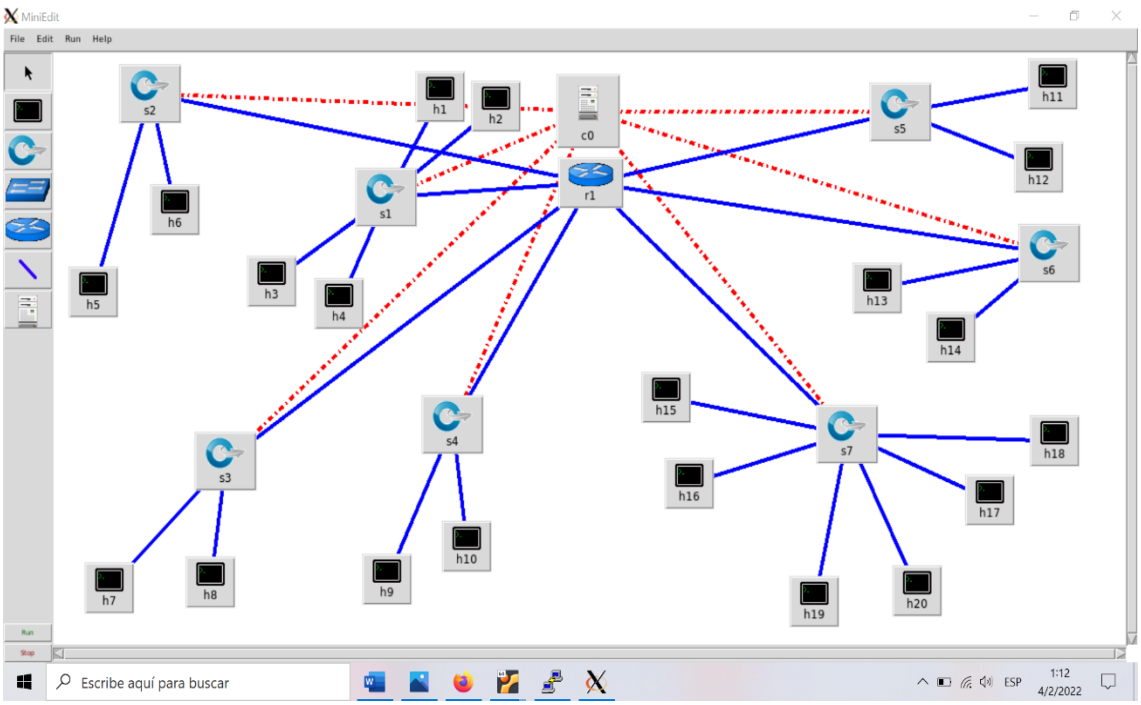


Figura 71. Nuevo diseño de red SDN para la institución educativa

Segmentación de red

VLSM es un proceso que se realiza para obtener subredes de una sola red variando la máscara de red para ocupar las direcciones necesarias para una sola sección evitando su

agotamiento. Para esto se debe tener un IP base o red general y empezar el proceso de subnetting. La IP a utilizar es **192.168.10.0/24.** Después se debe ordenar de mayor a menor la demanda de host por departamentos.

Laboratorio 1	30 hosts
Laboratorio 2	30 hosts
Laboratorio 3	30 hosts
Sistemas/Ciencias	14 hosts
Bloque de aulas 1	14 hosts
Bloque de aulas 2	14 hosts
Departamentos	14 hosts

Con los hosts ya ordenados se realiza el Subneteo empezando por el laboratorio 1 hasta departamentos. Para esto se utiliza la fórmula $\mathbf{2^m - 2 \geq host}$. $\mathbf{2^m}$ es base 2 elevado a un número desde el 0. Se resta $\mathbf{2}$ por ser una IP de red y otra IP de broadcast. Esto debe ser mayor o igual a la cantidad de $\boldsymbol{host}$ solicitados. Por ejemplo, Laboratorio 1 requiere 30 host, para esto hay que buscar un número elevado que la base 2 y restado 2 dé un aproximado a la cantidad de host requeridos: $\mathbf{2^5 - 2 = 30\ y\ 30 \geq 30}$ se cumple. Entonces 30 direcciones IP serán asignables a los hosts sin incluir red y broadcast. El resultado de la resta es la cantidad de IP que tendrá la subred. De ser el resultado mayor, las IP demás quedan reservados para la misma subred. Este mismo procedimiento se aplica para cada subred a crear.

Este caso en particular el resultado coincide con la cantidad de host requerida por subred, por lo tanto cada subred tendrá los hosts solicitados. Una vez aplicada la fórmula para cada subred, se empieza la segmentación de subredes empezando por la IP 192.168.10.0 para la subred 1, la IP de broadcast será la última IP de la subred, y la siguiente subred empezará una IP más a la IP de broadcast de la subred anterior teniendo en cuenta el resultado de las IP asignables para los equipos por cada subred. Esto cambiará la máscara para cada subred.

1) Laboratorio 1

   $2^m - 2 \geq host$

   $2^5 - 2 = 30 \geq 30$

   192.168.10.0

   192.168.10.1 – 192.168.10.30

   192.168.10.31

2) Laboratorio 2

   $2^m - 2 \geq host$

   $2^5 - 2 = 30 \geq 30$

   192.168.10.32

   192.168.10.3 – 192.168.10.62

   192.168.10.63

3) Laboratorio 3

   $2^m - 2 \geq host$

   $2^5 - 2 = 30 \geq 30$

   192.168.10.64

   192.168.10.6 – 192.168.10.94

   192.168.10.95

4) Sistemas/ciencias

   $2^m - 2 \geq host$

   $2^4 - 2 = 14 \geq 14$

   192.168.10.96

   192.168.10.97 – 192.168.10.110

   192.168.10.111

5) Bloque de aulas 1

   $2^m - 2 \geq host$

   $2^4 - 2 = 14 \geq 14$

   192.168.10.112

   192.168.10.113 – 192.168.10.126

   192.168.10.127

6) Bloque de aulas 2

   $2^m - 2 \geq host$

   $2^4 - 2 = 14 \geq 14$

   192.168.10.128

   192.168.10.129 – 192.168.10.142

   192.168.10.143

7) Departamentos

   $2^m - 2 \geq host$

   $2^4 - 2 = 14 \geq 14$

   192.168.10.144

   192.168.10.145 – 192.168.10.158

   192.168.10.159

La primera fila de IP de las subredes es la IP de red. El rango de IP's de la segunda fila de las subredes son las direcciones asignables para los hosts desde la primera hasta la última. La última IP de la tercera fila de las subredes es la IP de broadcast.

Tabla de direccionamiento IP

Host	IP	Mask / CIDR	Gateway	Ubicación	Switch	Router
h1	192.168.10.98	255.255.255.240/**28**	192.168.10.97	Sistemas/Ciencias	s1	r1
h2	192.168.10.99	255.255.255.240/**28**	192.168.10.97	Sistemas/Ciencias	s1	r1
h3	192.168.10.100	255.255.255.240/**28**	192.168.10.97	Sistemas/Ciencias	s1	r1
h4	192.168.10.101	255.255.255.240/**28**	192.168.10.97	Sistemas/Ciencias	s1	r1
h5	192.168.10.2	255.255.255.224/**27**	192.168.10.1	Laboratorio 1	s2	r1
h6	192.168.10.3	255.255.255.224/**27**	192.168.10.1	Laboratorio 1	s2	r1
h7	192.168.10.114	255.255.255.240/**28**	192.168.10.113	Bloque aulas 1	s3	r1
h8	192.168.10.115	255.255.255.240/**28**	192.168.10.113	Bloque aulas 1	s3	r1
h9	192.168.10.130	255.255.255.240/**28**	192.168.10.129	Bloque aulas 2	s4	r1
h10	192.168.10.131	255.255.255.240/**28**	192.168.10.129	Bloque aulas 2	s4	r1
h11	192.168.10.34	255.255.255.224/**27**	192.168.10.33	Laboratorio 2	s5	r1
h12	192.168.10.35	255.255.255.224/**27**	192.168.10.33	Laboratorio 2	s5	r1
h13	192.168.10.66	255.255.255.224/**27**	192.168.10.65	Laboratorio 3	s6	r1
h14	192.168.10.67	255.255.255.224/**27**	192.168.10.65	Laboratorio 3	s6	r1
h15	192.168.10.146	255.255.255.240/**28**	192.168.10.145	Departamentos	s7	r1
h16	192.168.10.147	255.255.255.240/**28**	192.168.10.145	Departamentos	s7	r1
h17	192.168.10.148	255.255.255.240/**28**	192.168.10.145	Departamentos	s7	r1
h18	192.168.10.149	255.255.255.240/**28**	192.168.10.145	Departamentos	s7	r1
h19	192.168.10.150	255.255.255.240/**28**	192.168.10.145	Departamentos	s7	r1
h20	192.168.10.151	255.255.255.240/**28**	192.168.10.145	Departamentos	s7	r1

Todos los switches van conectados al router del departamento de sistemas. En el router se habilitan varias interfaces dependiendo de la cantidad de switch que se conectan a él, por lo que no es necesario crear VLANs, sino reservar una interfaz para cada switch y asignar la debida dirección de Gateway a la interfaz según la ubicación del switch.

El funcionamiento es el mismo, el controlador es el encargado del plano de control y el que le dice al conmutador que camino tomar para llegar a su destino. El router cumple el rol de añadir un Gateway para conectar con las subredes.

Configuración de los equipos

Al ser un nuevo diseño se deben volver a realizar las mismas configuraciones de las etapas anteriores teniendo en cuenta si la dirección IP del controlador ha cambiado por tratarse de una configuración de red en modo puente dentro de virtualbox. En este nuevo proceso la IP sí cambió, por ello se la actualiza y se vuelven a ingresar las mismas configuraciones como el puerto del controlador y el tipo como en la etapa III. En una red física la IP del controlador debe ser configurada como estática para evitar estos cambios.

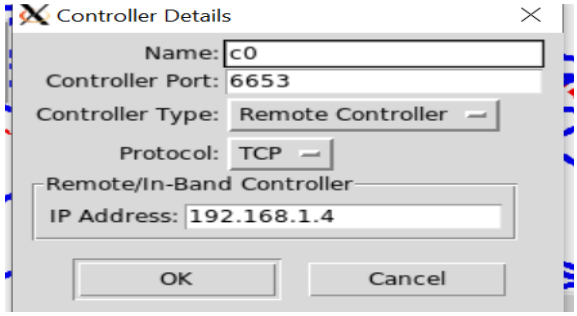


Figura 72. Reconfiguración de IP del controlador en miniedit

A diferencia de los pasos anteriores, para la configuración de los hosts a la dirección IP se le añade el CIDR correspondiente a la subred y su puerta de enlace predeterminada (Gateway). Se hace lo mismo con los demás hosts.

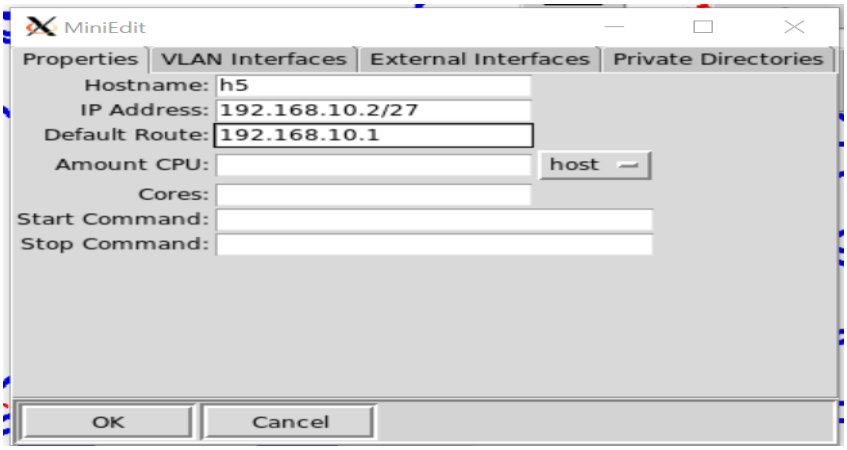


Figura 73. Configuración de IP subnetting h5

Para los switches se los configura nuevamente como Open vSwitch Kernel Mode

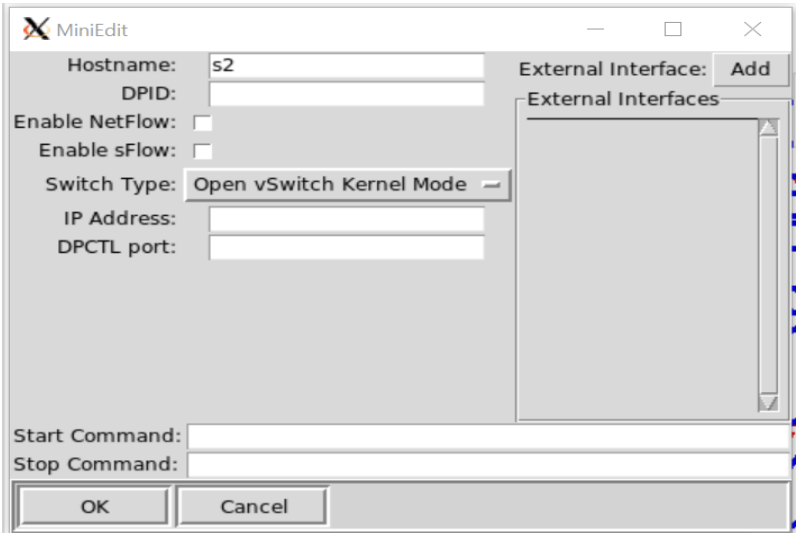


Figura 74. Reconfiguración de switches SDN

Dentro de las preferencias lo único que se cambia es la IP de base con la IP general de donde se desglosan todas las subredes "subneteadas": 192.168.10.0/24. El tipo de switch es igual Open vSwitch Kernel Mode, seleccionando CLI para abrir mediante consola con versión OpenFlow 1.3.

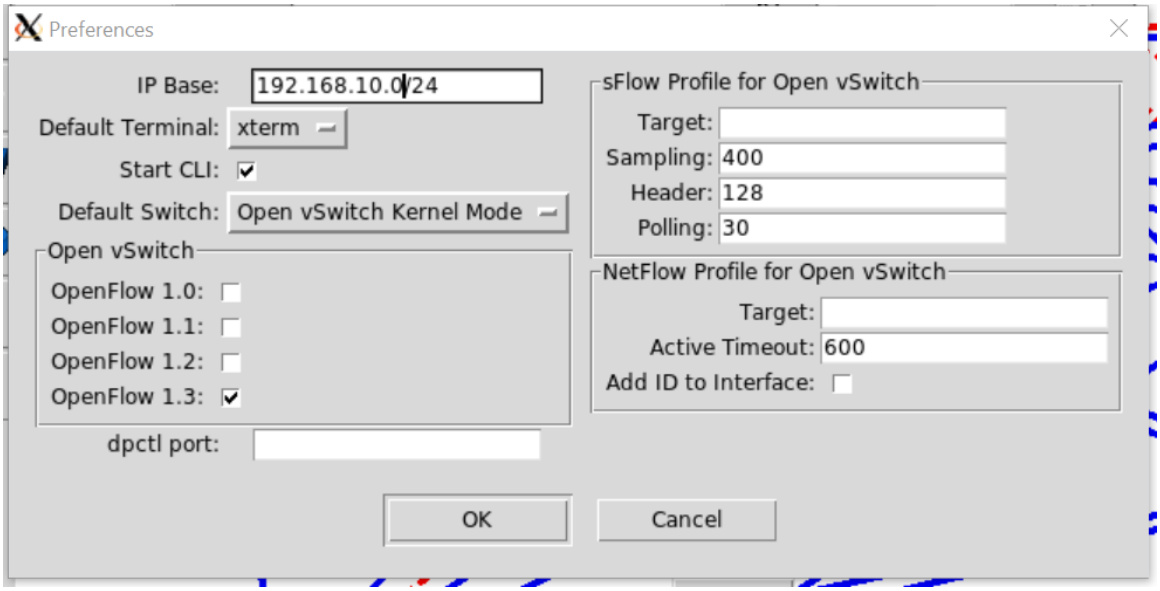


Figura 75. Configuración de IP base en las preferencias de miniedit

Al iniciar la simulación realizamos ping entre hosts de la misma subred para comprobar que las direcciones IP están correctas. Al ser de la misma subred no existe problema.

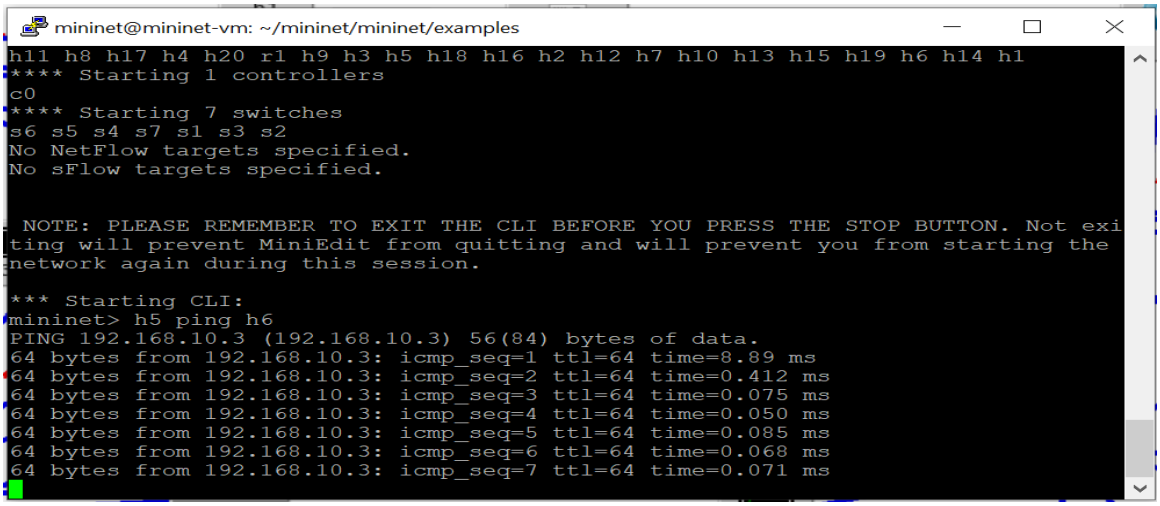


Figura 76. Ping entre dos hosts de la misma subred

Al realizar un ping a un host perteneciente a otra subred se obtiene como resultado que la red es inalcanzable ya que no está configurada una interfaz dentro del router que permita la comunicación entre subredes.

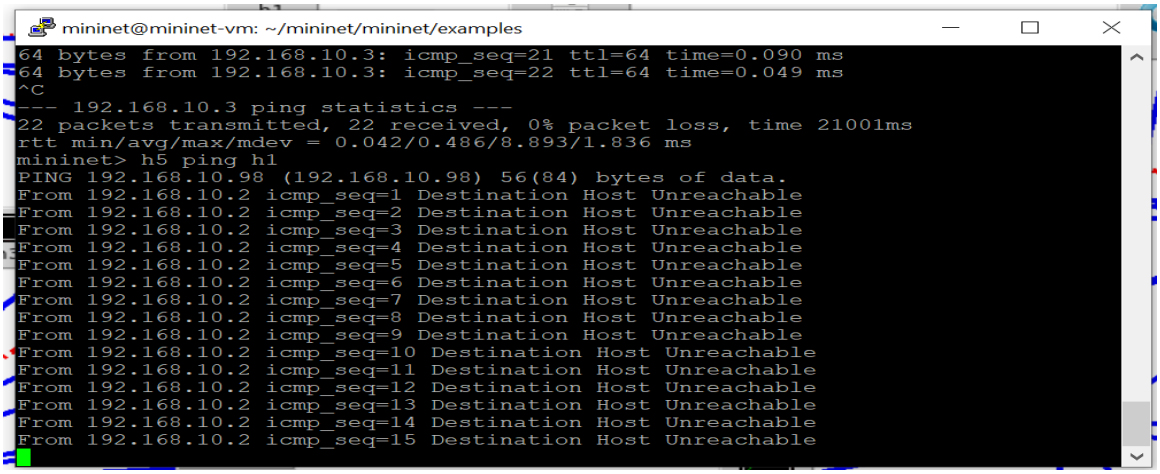


Figura 77. Ping entre subredes dirferentes

Para configurar las interfaces del router se presiona clic derecho al ícono del router en miniedit con la red ejecutándose. Seleccionar terminal para abrir una consola basada en lenguaje Linux.

Figura 78. Router de capa 3 en arquitectura SDN

Con el comando **ifconfig** se observan siente interfaces generadas desde r1-eth0 hasta r1-eth6 pero sin dirección IP asignadas.

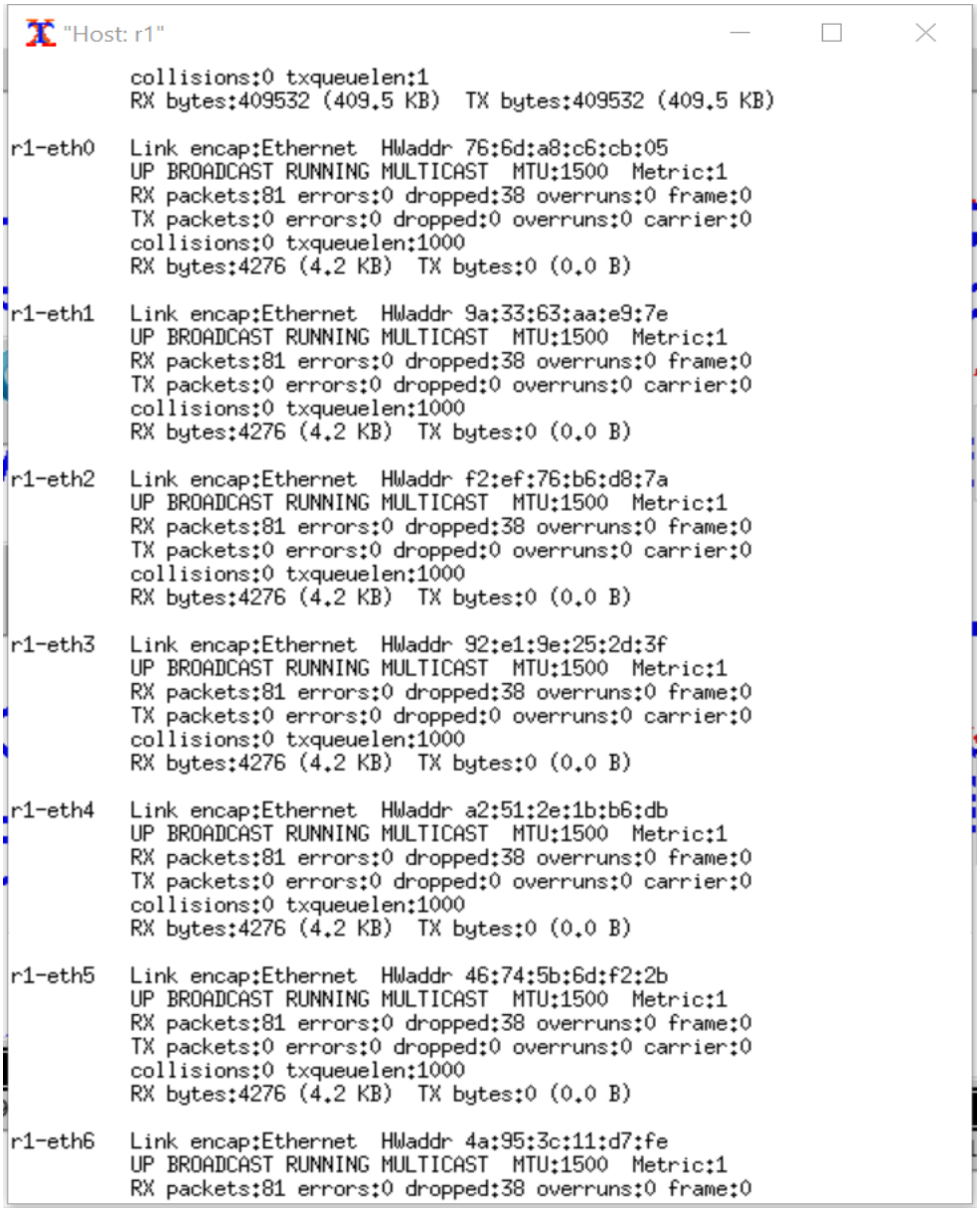


Figura 79. Presencia de interfaces de red en el router

Para añadir una dirección IP a las interfaces creadas dentro del router se debe introducir el comando **ip address add [ip/prefijo] dev [interfaz]** donde la IP es el Gateway, prefijo es el CIDR e interfaz es el nombre de la interfaz a utilizar. Se realiza esto para las siete interfaces.

Figura 80. Configuración de IP en las interfaces de red del router

Al ejecutar de nuevo **ifconfig** las interfaces tendrán asignadas las direcciones IP

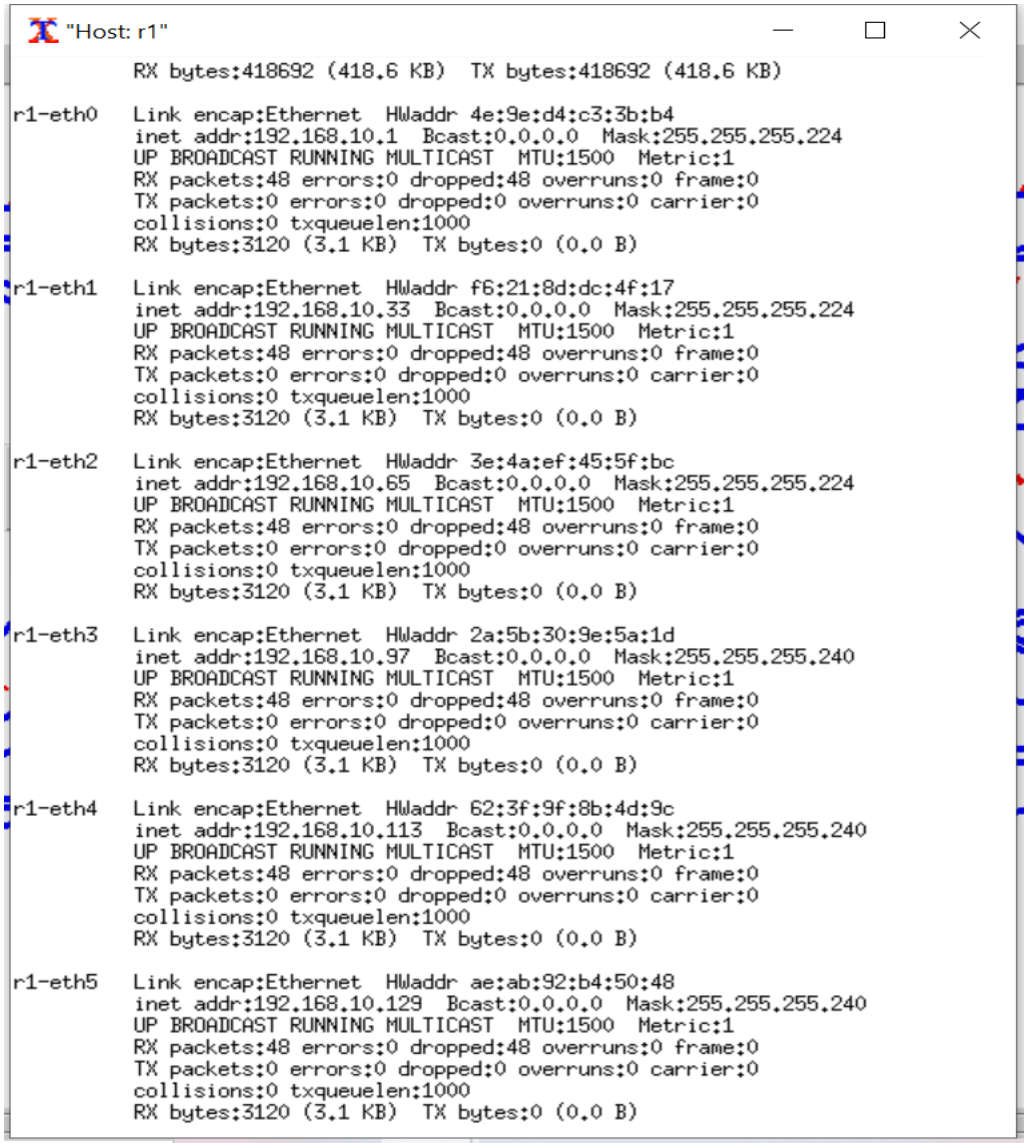


Figura 81. Verificación de IP asignadas

Se realiza un ping nuevamente ente subredes de h5 a h1 y con éxito la comunicación entre estos dos hosts se completa.

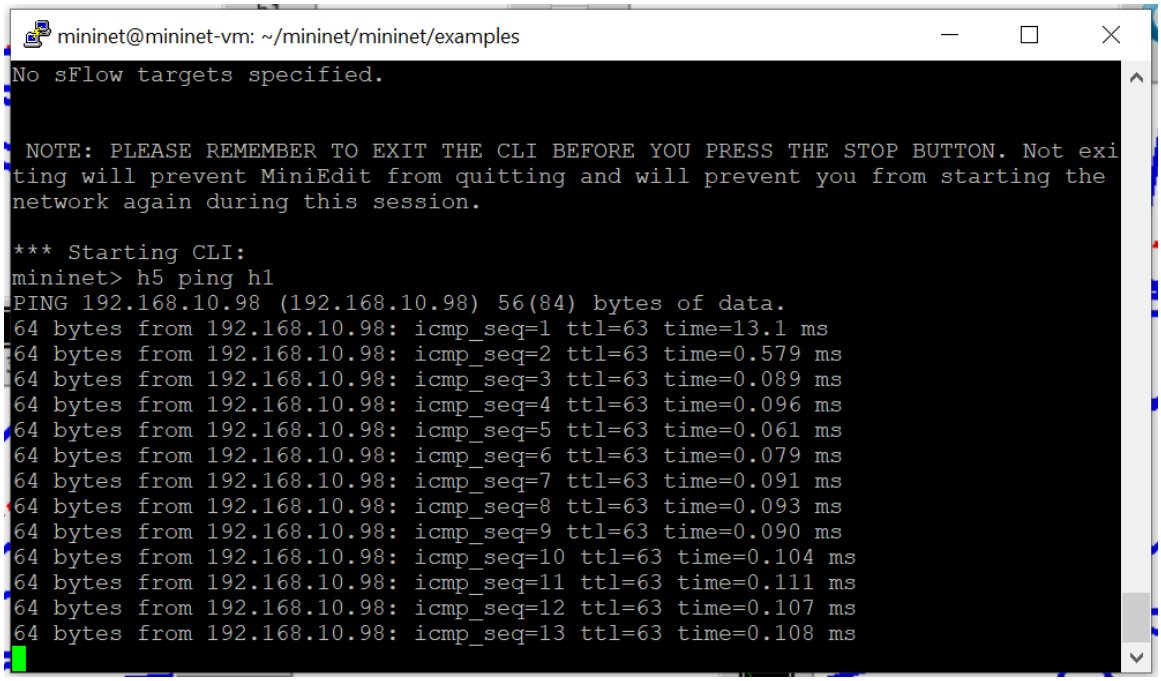


Figura 82. Ping efectivo entre subredes

Dentro del servidor http de floodlight en la pestaña de switches aparecen los siente conmutadores utilizados. El router es considerado como host por el funcionamiento del protocolo OpenFlow ya que se basa en encaminamiento para los switches y el controlador hace uso de este protocolo.

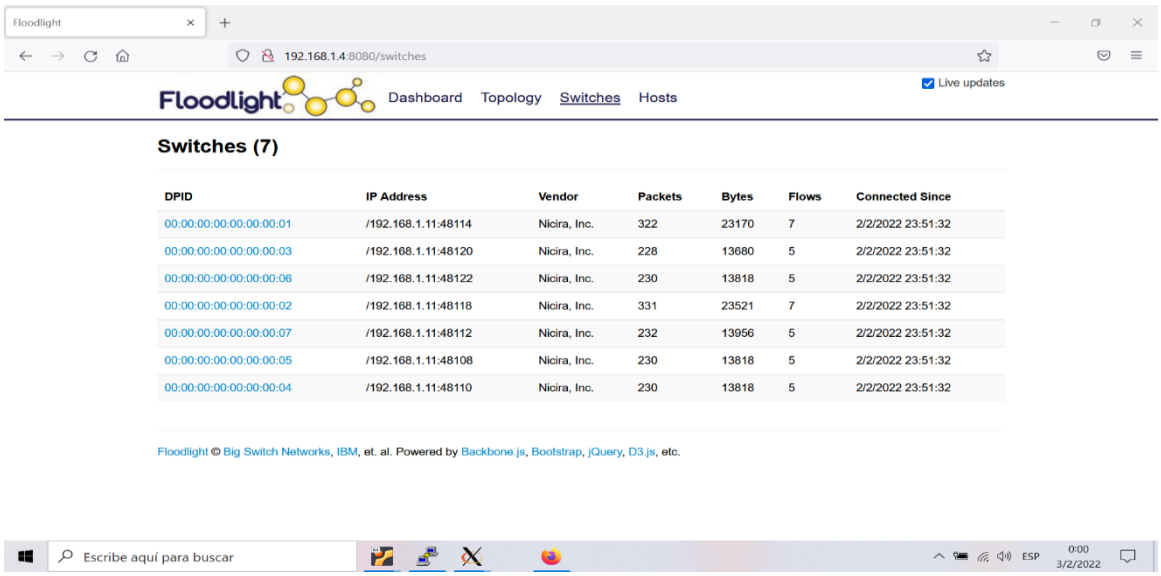


Figura 83. Conmutadores de red utilizados en el nuevo diseño SDN

El router aparece en la pestaña hosts como host por las direcciones IP que se le configuraron en las interfaces.

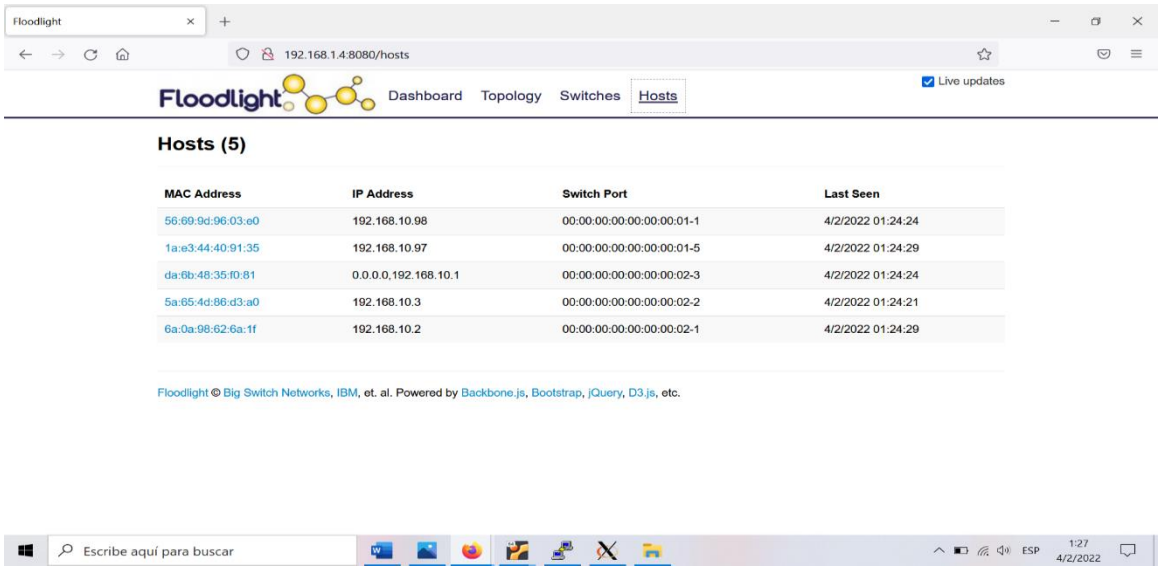


Figura 84. Aparición de las interfaces de red utilizadas en la pestaña hosts

En la topología de floodlight aparece el router como host del mismo switch al tener asignado una de las interfaces a la misma subred del host que mandó y recibió el ping. En esta optimización los switches no se muestran conectados entre sí ya que pasó de ser una red totalmente conmutada a una red segmentada. El controlador sigue teniendo control del plano de control.

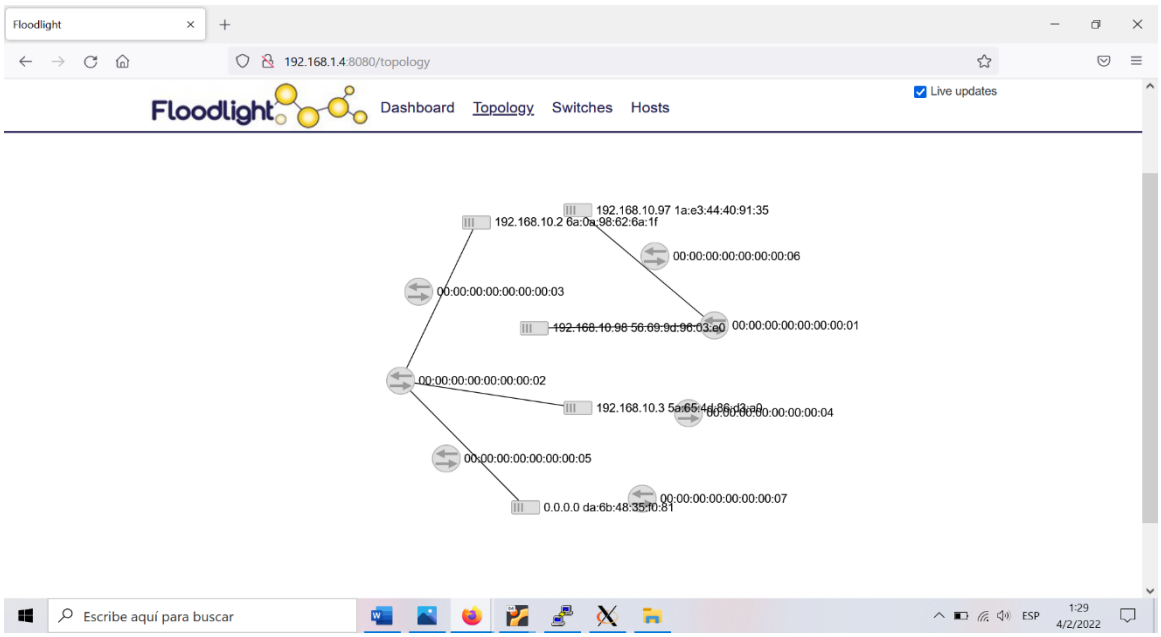


Figura 85. Nueva topología de red SDN

Para observar el funcionamiento del plano de control en este nuevo diseño, se realiza un nuevo ping desde el host h5 a host h15.

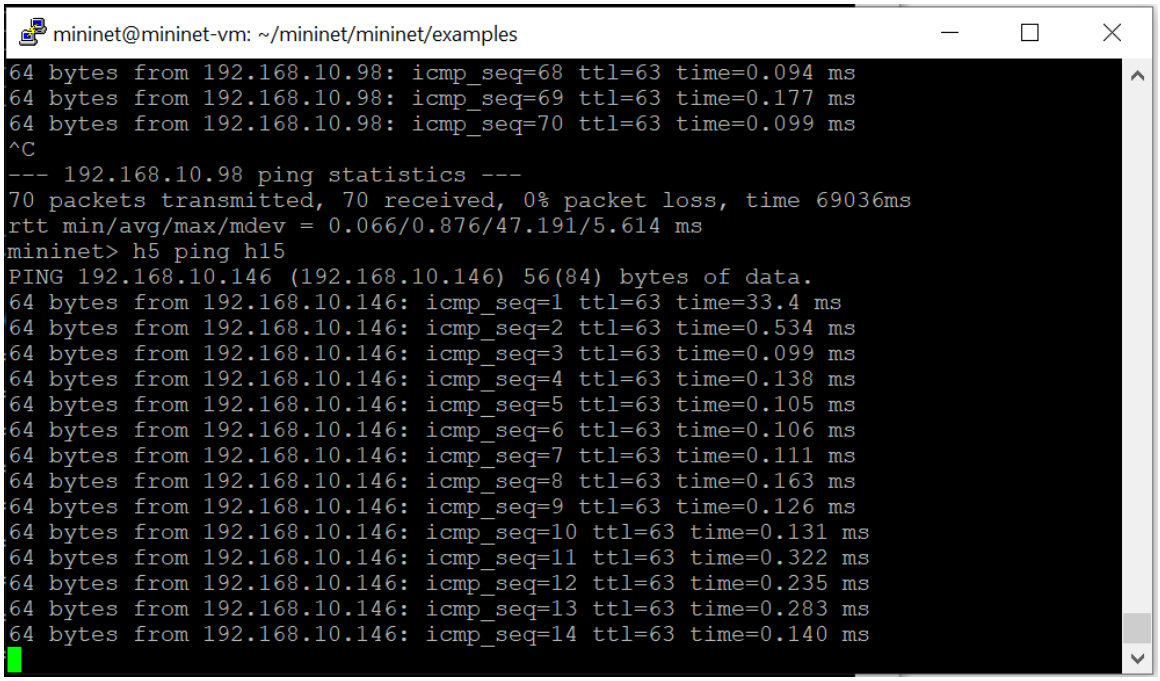


Figura 86. Nueva prueba para comprobación del tráfico de red

En la pestaña host se agrega la IP del host 15 y la IP de la interfaz que tiene asignada el Gateway de la misma subred.

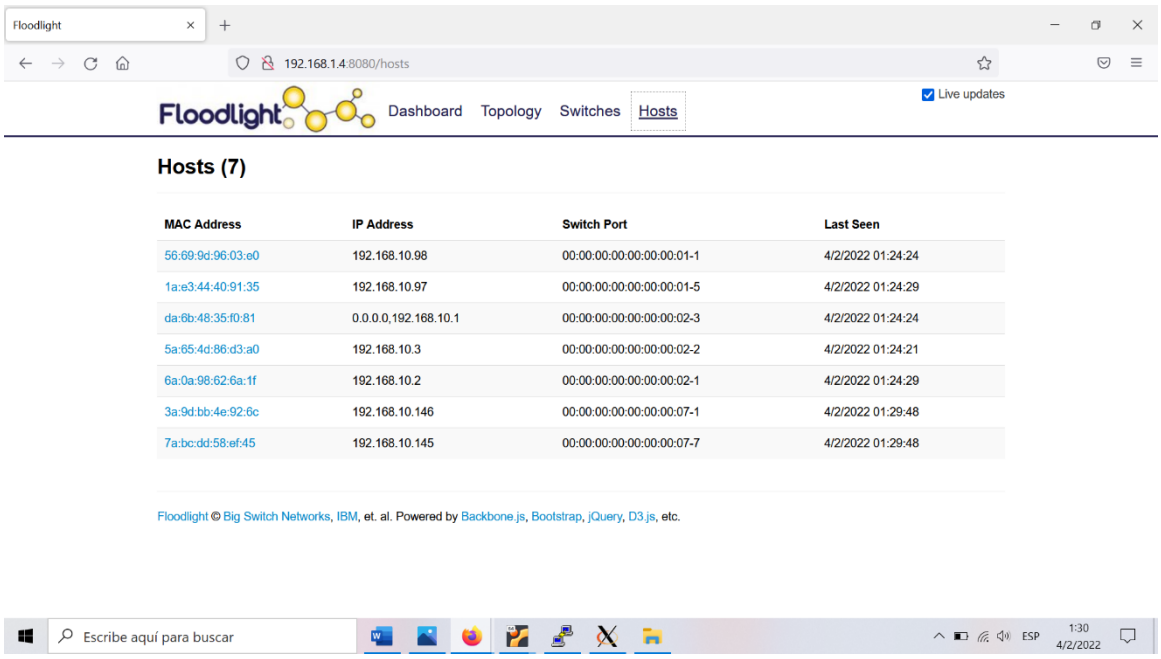


Figura 87. Dispositivos utilizados en la nueva prueba

Dentro de la topología de floodlight también se agrega con éxito los hosts (ip host h15 e interfaz del router perteneciente a la subred de h15).

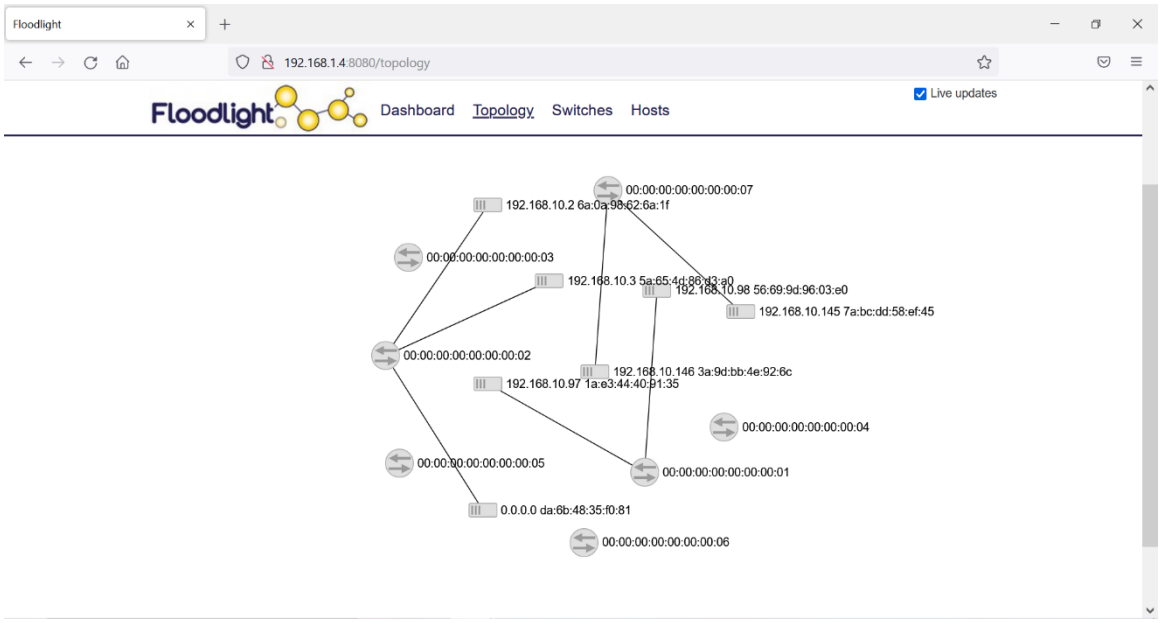
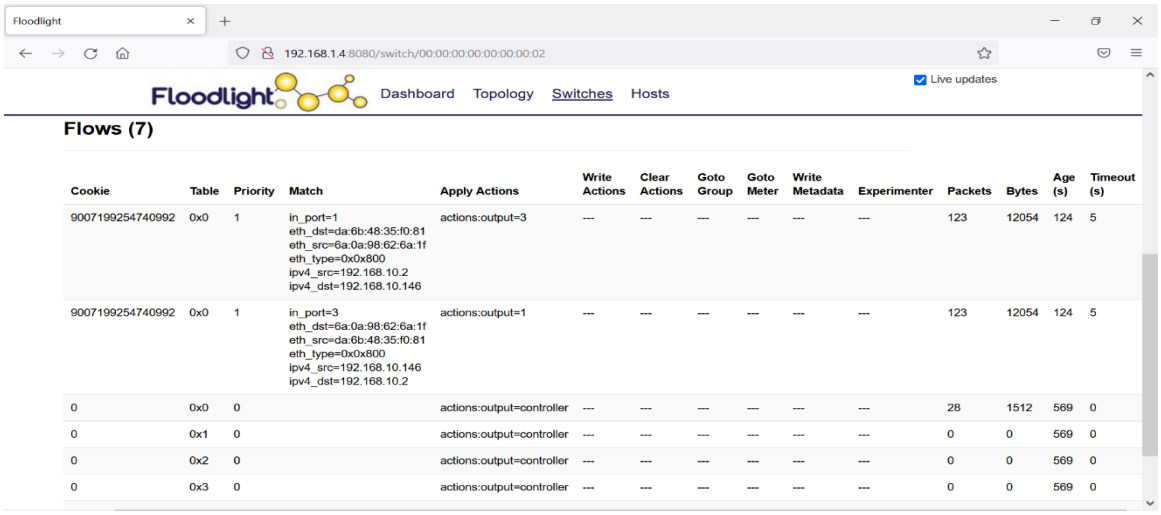


Figura 88. Detección de los dispositivos en la topología

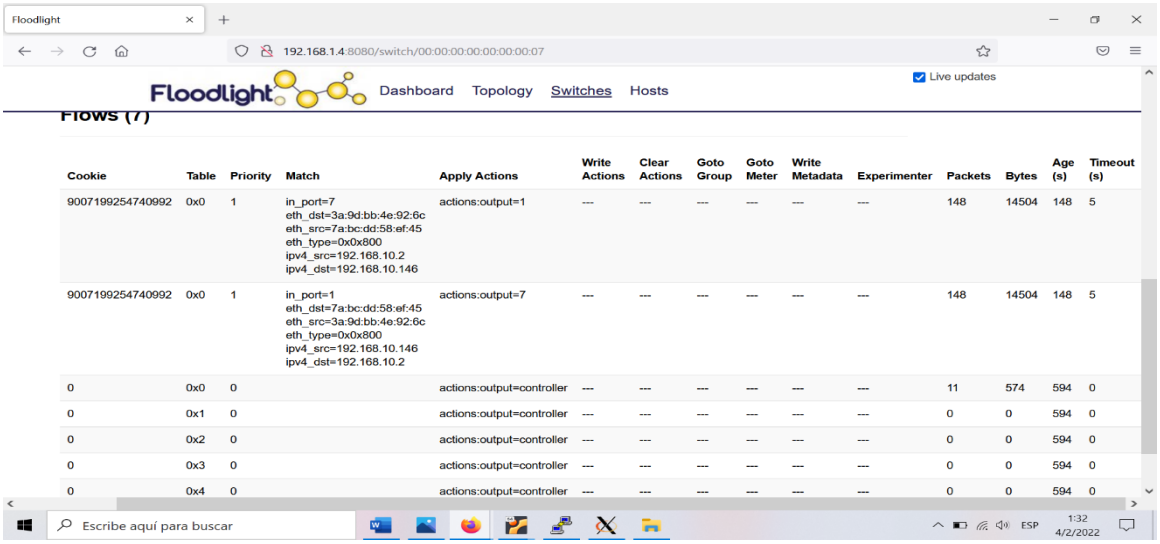
En la tabla de flujo del switch s2 al que pertenece el host h5 se muestra el mismo comportamiento, donde el paquete entra al switch por el puerto 1 y sale del switch por el puerto 3, y para recibir respuesta o un nuevo paquete realiza lo contrario. Lo diferente es que ahora el controlador le comunica al switch para que el paquete pueda llegar a su destino debe enviarlo a un intermediario (router). El router mediante sus interfaces reenvía el paquete por el Gateway de la subred de destino.



Cookie	Table	Priority	Match	Apply Actions	Write Actions	Clear Actions	Goto Group	Goto Meter	Write Metadata	Experimenter	Packets	Bytes	Age (s)	Timeout (s)
9007199254740992	0x0	1	in_port=1 eth_dst=da:6b:48:35:f0:81 eth_src=6a:0a:98:62:6a:1f eth_type=0x0x800 ipv4_src=192.168.10.2 ipv4_dst=192.168.10.146	actions:output=3	---	---	---	---	---	---	123	12054	124	5
9007199254740992	0x0	1	in_port=3 eth_dst=6a:0a:98:62:6a:1f eth_src=da:6b:48:35:f0:81 eth_type=0x0x800 ipv4_src=192.168.10.146 ipv4_dst=192.168.10.2	actions:output=1	---	---	---	---	---	---	123	12054	124	5
0	0x0	0		actions:output=controller	---	---	---	---	---	---	28	1512	569	0
0	0x1	0		actions:output=controller	---	---	---	---	---	---	0	0	569	0
0	0x2	0		actions:output=controller	---	---	---	---	---	---	0	0	569	0
0	0x3	0		actions:output=controller	---	---	---	---	---	---	0	0	569	0

Figura 89. Tabla de flujo de la nueva prueba s2

Al abrir la tabla de flujo del switch s7 se presentan los puertos que utiliza el switch para transmitir la información. Para enviar una respuesta o un nuevo paquete entra al switch por el puerto 7 con salida hacia el router por el puerto 1. Para recibir es realizado de la manera contraria.



Cookie	Table	Priority	Match	Apply Actions	Write Actions	Clear Actions	Goto Group	Goto Meter	Write Metadata	Experimenter	Packets	Bytes	Age (s)	Timeout (s)
9007199254740992	0x0	1	in_port=7 eth_dst=3a:9d:bb:4e:92:6c eth_src=7a:bc:dd:58:ef:45 eth_type=0x0x800 ipv4_src=192.168.10.2 ipv4_dst=192.168.10.146	actions:output=1	---	---	---	---	---	---	148	14504	148	5
9007199254740992	0x0	1	in_port=1 eth_dst=7a:bc:dd:58:ef:45 eth_src=3a:9d:bb:4e:92:6c eth_type=0x0x800 ipv4_src=192.168.10.146 ipv4_dst=192.168.10.2	actions:output=7	---	---	---	---	---	---	148	14504	148	5
0	0x0	0		actions:output=controller	---	---	---	---	---	---	11	574	594	0
0	0x1	0		actions:output=controller	---	---	---	---	---	---	0	0	594	0
0	0x2	0		actions:output=controller	---	---	---	---	---	---	0	0	594	0
0	0x3	0		actions:output=controller	---	---	---	---	---	---	0	0	594	0
0	0x4	0		actions:output=controller	---	---	---	---	---	---	0	0	594	0

Figura 90. Tabla de flujo de la nueva prueba s7

El tráfico de red que se genera pertenece al protocolo OpenFlow entre la máquina virtual que posee el controlador floodlight y la máquina virtual que posee mininet. Estás IP siguen siendo asignadas por el router donde se realizan las pruebas.

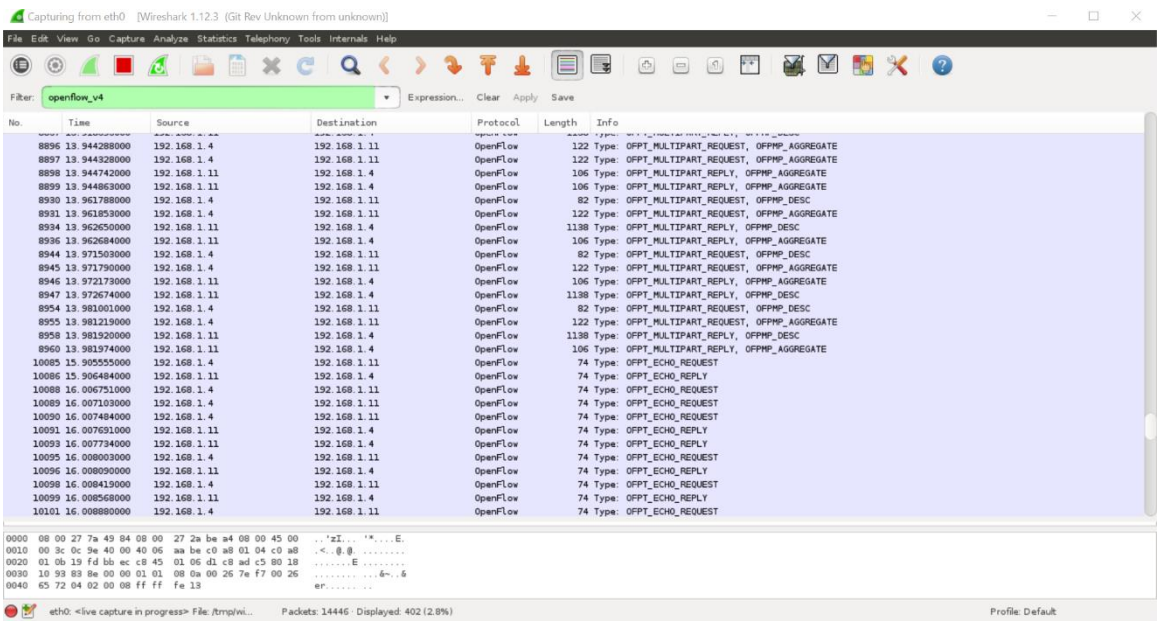


Figura 91. Tráfico de red generado en la nueva prueba

Con el mismo ping utilizado entre h5 y h15 se comprueba el tráfico que se genera en la nueva red LAN. Aparecen 8 paquetes sombreados.

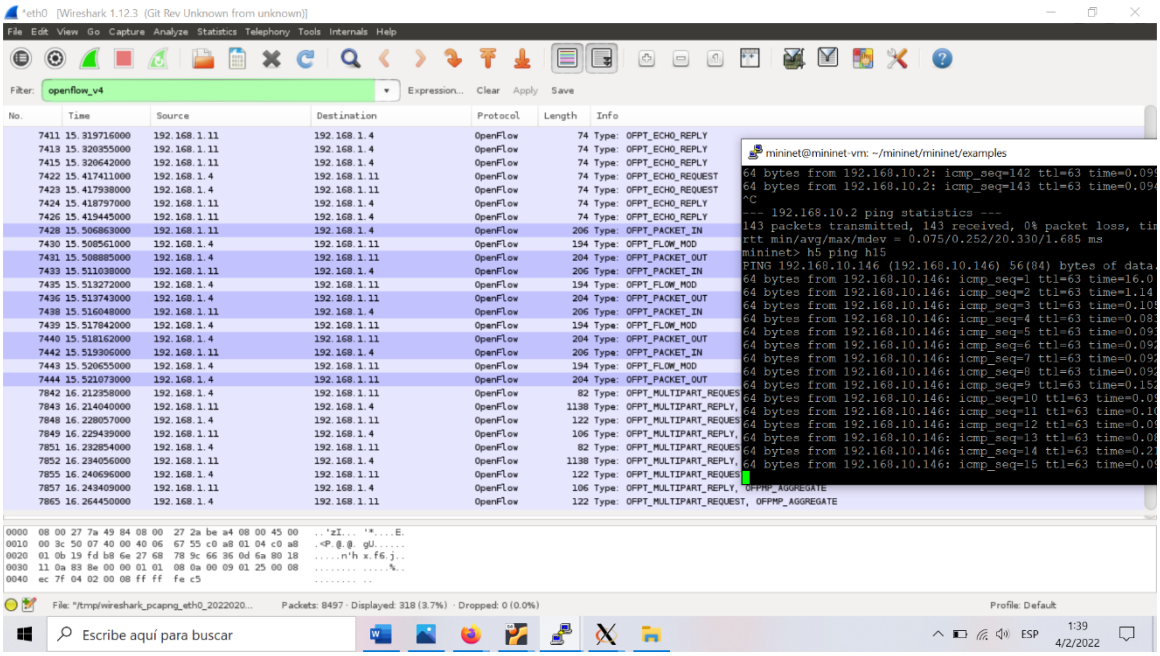


Figura 92. Aparición de las tramas al hacer ping entre dos subredes

El primer paquete contiene la información y la manera de cómo es "matcheado". Se observa que utiliza la dirección MAC de origen y destino, asimismo la dirección IP de origen y destino.

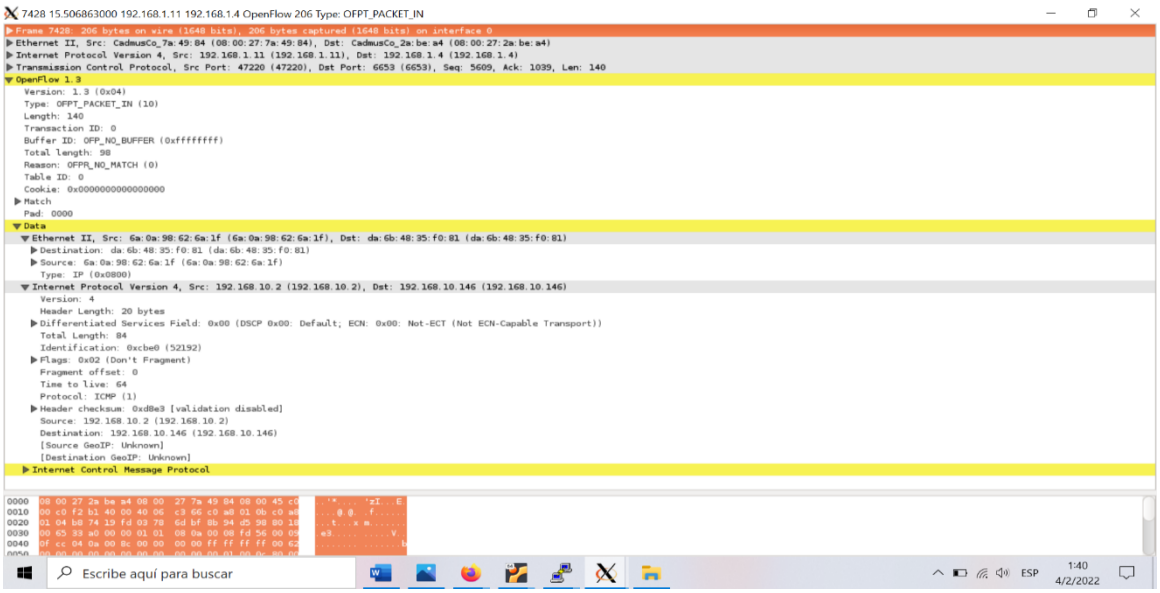


Figura 93. Matcheo de MAC

El siguiente paquete al abrir detalla la acción que está tomando una vez el controlador haya indicado qué puerto debe tomar para que el paquete pueda llegar a su destino. La entrada del paquete hacia el switch es por el puerto 1 con salida esta vez hacia el router por el puerto 3.

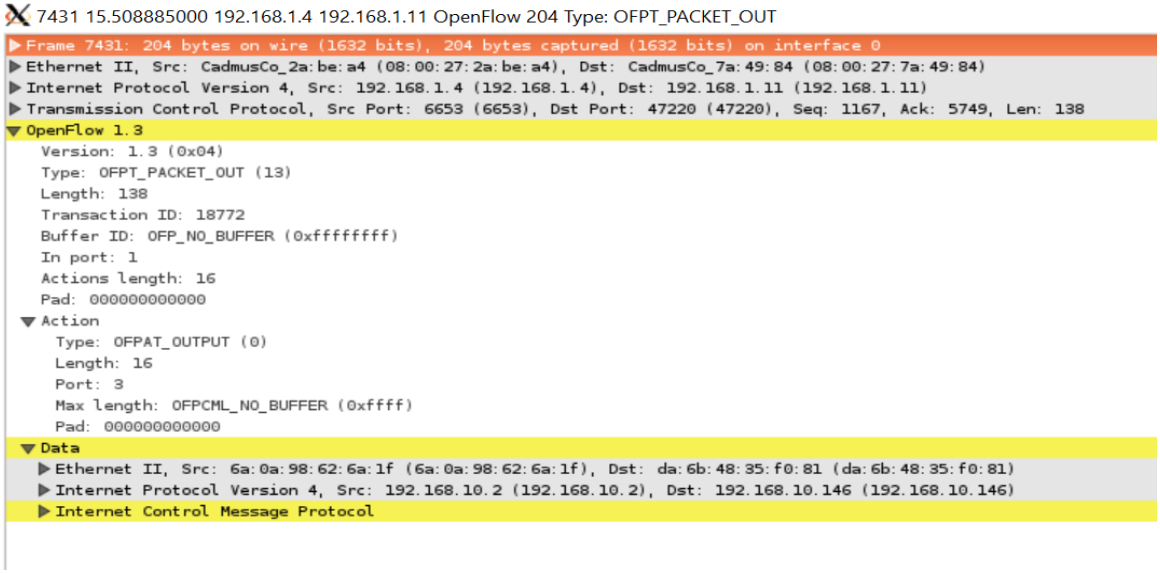


Figura 94. Acción que debe tomar la trama para llegar a su destino

Otro de los paquetes abiertos indica que el router ha reenviado el paquete mediante sus interfaces siendo recibido por el switch de destino por el puerto 7, hacia el host h15 mediante el puerto 1.

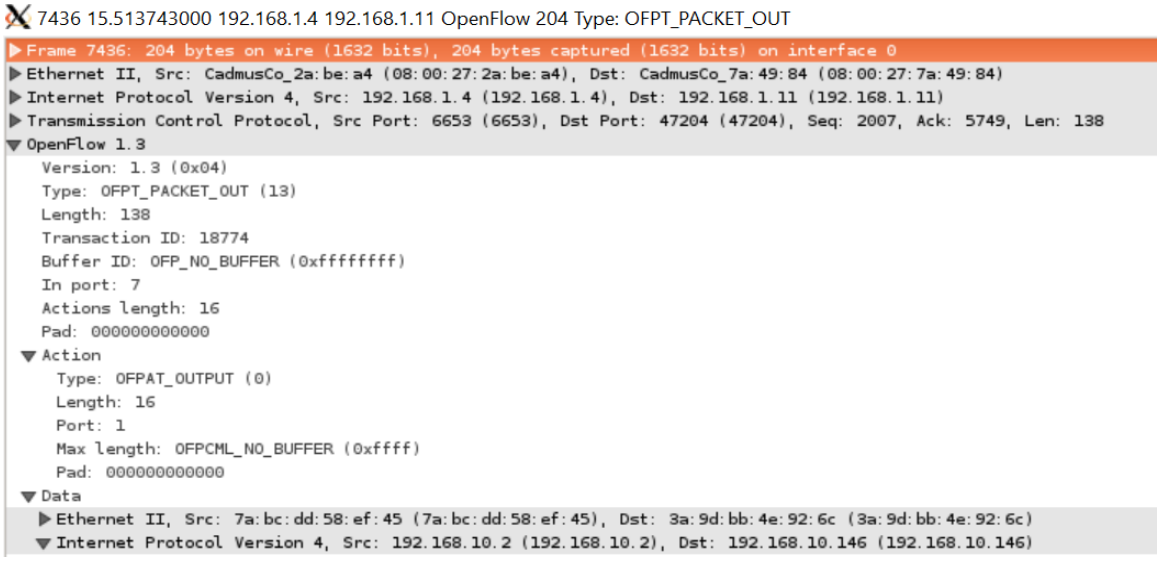


Figura 95. Recibimiento de la trama por el switch de destino

Se prepara la respuesta del host h15 hacia el host h5. “Matchea” de igual manera con dirección MAC de origen y destino, y dirección IP de origen y destino.

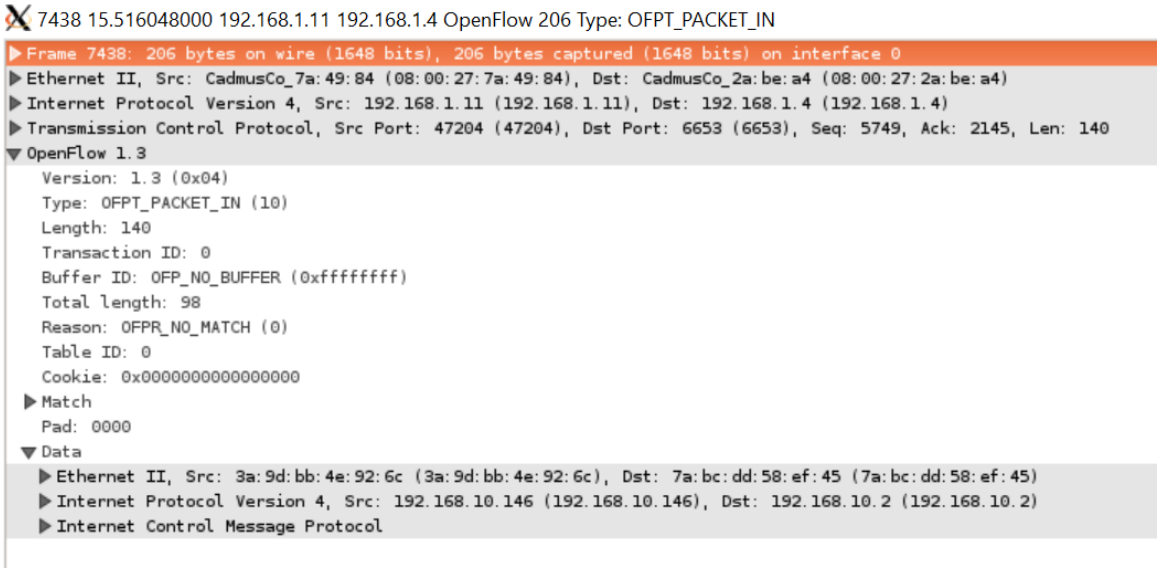


Figura 96. Respuesta de h15 a h5

La respuesta del host h15 llega al switch mediante el puerto 1 con salida hacia el router por el puerto 7.

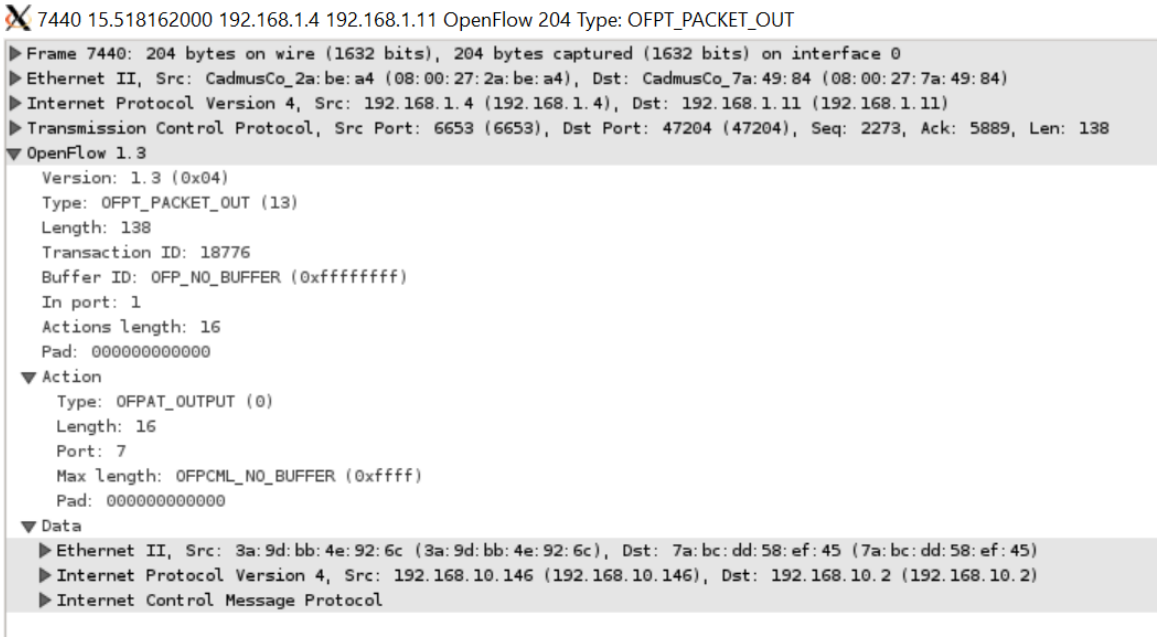


Figura 97. Salida de la trama de respuesta al router

Una vez que el router haya direccionado el paquete entrando por la interfaz de la subred de origen hacia la interfaz de la subred de destino, llega al switch s2 entrando por el puerto 3 para ser reenviado hacia el host h5 por el puerto 1.

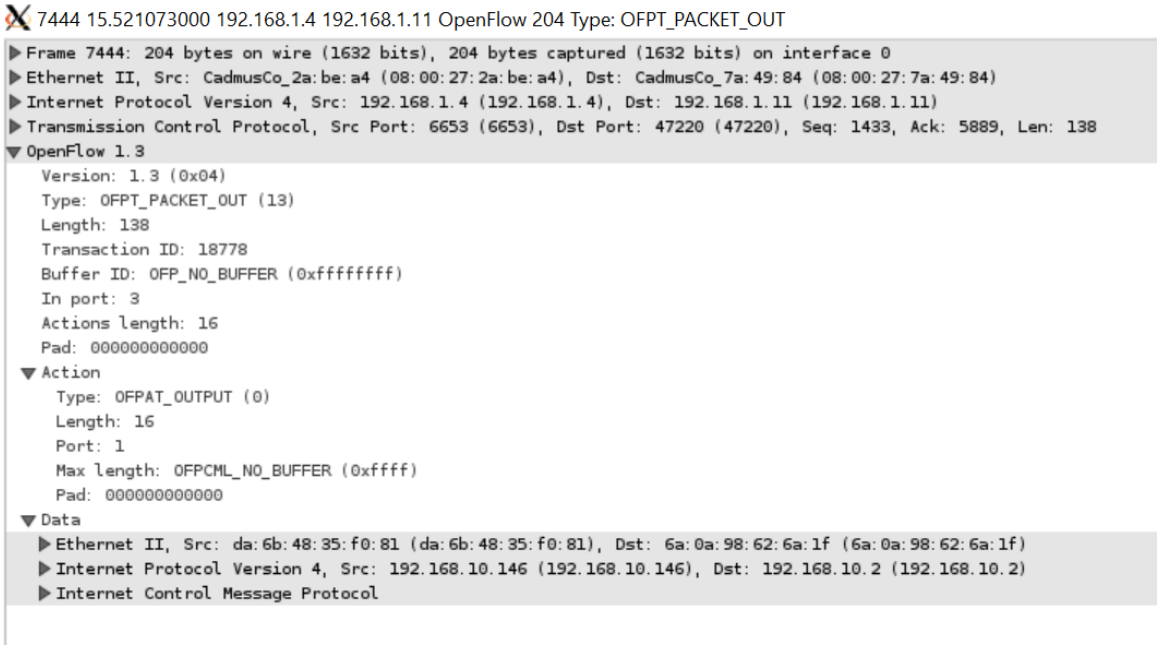


Figura 98. Llegada de la trama de respuesta

CONCLUSIONES

- La creación de máquinas virtuales separando mininet del controlador floodlight facilitó el entendimiento de la comunicación de estas dos herramientas al momento de interactuar entre sí bajo la misma red.
- El tiempo de transmisión del ping en una red física tiene un promedio de demora de 1,25 ms por cada 4 paquetes enviados en una primera prueba. En la segunda prueba realizada se obtiene un promedio de 2,25 ms por cada cuatro paquetes enviados. Para la tercera prueba se obtuvo un promedio de 1 ms de demora por cada cuatro paquetes enviados, obteniendo una media de velocidad de transmisión de 1,5 ms.
- Dentro de la red virtual la transmisión del ping tiene un promedio de demora de 9,528 ms por cada 4 paquetes enviados en una primera prueba. Dentro de la segunda prueba se obtuvo un promedio de 3,305 ms por cada 4 paquetes enviados. En la última prueba el promedio es de 0,085 ms por cada 4 paquetes enviados, obteniendo una media de velocidad de transmisión de 4,306 ms.
- El resultado de demora de la transmisión del ping en la red virtual es causado por el envío del primer paquete con un tiempo promedio entre las tres pruebas realizada de 16,655 ms (primera prueba: 37,5 ms + segunda prueba: 12,4 ms + tercera prueba: 0,067 ms), mientras que los siguientes paquetes enviados alcanzan una velocidad de transmisión menor a 1 ms. Aproximadamente 0,205 ms.
- Mientras los paquetes sean enviados uno tras otros sin ser detenidos dentro de la red virtual, alcanzarán una mayor velocidad de transmisión.

RECOMENDACIONES

- Se recomienda establecer una configuración de red conectado a “Adaptador sólo-anfitrión” en casos de presentar conflictos en una configuración NAT o tipo puente dentro de las máquinas virtuales a causa de las políticas de la red en la que se trabajará.
- Se recomienda ejecutar un ping en una red física LAN segmentada para analizar el tiempo de demora que presenta el ping hasta llegar a su destino realizando tres o más pruebas por cada cuatro paquetes enviados.
- Se conseja realiza pruebas del tiempo en que demora llegar el ping a su destino en un diseño de red únicamente con el controlador quitando el router para comprobar si existe alguna diferencia de tiempo en el enrutamiento de los paquetes.
- Incluir un segundo controlador para observar el comportamiento de la red y comprobar si existe mayor o menor latencia en el envío de los paquetes de datos configurando el ancho de banda en el próximo diseño.
- Realizar un nuevo diseño de red programando el controlador con otros criterios como dando prioridad a una VLAN determinada o funcionabilidad de la red con direcciones IPv6.

BIBLIOGRAFÍA

[1] userDataCenter, «laSalle,» laSalle, 11 Marzo 2020. [En línea]. Available: https://blogs.salleurl.edu/es/redes-tradicionales-vs-sdn-definidas-por-software. [Último acceso: 1 Noviembre 2021].

[2] R. Correa Delgado, Reglamento General a la Ley Orgánica de Educación Intercultural, Quito, 2014.

[3] Q. Y. Zhang, X. W. Wang, M. Huang, K. Q. Li y S. K. & Das, «Software defined networking meets information centric networking: A survey,» 7 Agosto 2018. [En línea]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8410516. [Último acceso: 2 Noviembre 2021].

[4] D. Guades, L. F. Menezes Vieira, M. Menezes Vieira, H. Rodrigues y R. Vinhan Nunes, «ResearchGate,» 16 Mayo 2014. [En línea]. Available: https://www.researchgate.net/profile/Dorgival-Guedes/publication/260346033_Redes_Definidas_por_Software_uma_abordagem_sistemica_para_o_desenvolvimento_de_pesquisas_em_Redes_de_Computadores/links/0c96053765194dafd6000000/Redes-Definidas-por-Software-uma-ab. [Último acceso: 2 Noviembre 2021].

[5] J. C. Chico, D. Mejía y I. Bernal, «Escuela Politécnica Nacional,» 2013. [En línea]. Available: http://ciecfie.epn.edu.ec/wss/VirtualDirectories/80/JIEE/historial/XXV/Redes/Memorias-360-369.pdf. [Último acceso: 2 Noviembre 2021].

[6] Á. L. Calvo García, Gestión de redes telemáticas, Málaga: IC Editorial, 2014.

[7] Oracle, «VirtualBox,» [En línea]. Available: https://www.virtualbox.org/. [Último acceso: 4 Noviembre 2021].

[8] UTA, 8 Marzo 2015. [En línea]. Available: http://190.15.141.68/index.php/uta/floodlight-controller. [Último acceso: 4 Noviembre 2021].

[9] Mininet, «Mininet,» Mininet, [En línea]. Available: http://mininet.org/. [Último acceso: 4 Noviembre 2021].

[10] S. Córdoba López, Estudio de redes SDN mediante, Valencia: Universidad Politécnica de Valéncia, 2019.

[11] A. Rawal, «Section,» Section, 2021 Febrero 2021. [En línea]. Available: https://www.section.io/engineering-education/openflow-sdn/. [Último acceso: 4 Noviembre 2021].

[12] R. Altube, «OpenWebinars,» OpenWebinars, 07 01 2021. [En línea]. Available: https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/. [Último acceso: 11 05 2022].

[13] W. Velásquez Vargas, «Emulación de una red definida por software utilizando MiniNet,» Escuela Técnica Superior de Ingenieros en Telecomunicaciones, Madrid, 2013.

[14] M. Leary, «GIGAOM,» GIGAOM, 19 Marzo 2014. [En línea]. Available: https://gigaom.com/report/sdn-nfv-and-open-source-the-operators-view/. [Último acceso: 12 Noviembre 2021].

[15] S. n. d. planificación, «Plan de creación de oportunidades 2021-2025,» Secretaria nacional de planificación, Quito, 2021.

[16] R. Hernández Sampieri, C. Fernández Collado y L. Pilas Baptista, Metodología de la investigación, Ciudad de México: McGraw Hill Education, 2014.

[17] E. G. FARO, «Grupo Faro,» Grupo Faro, 05 07 2020. [En línea]. Available: https://grupofaro.org/bachillerato-internacional-en-ecuador/. [Último acceso: 24 05 2022].

[18] Unidad Educativa Salinas Innova School, «Unidad Educativa Salinas Innova School,» Unidad Educativa Salinas Innova School, 5 Abril 2021. [En línea]. Available: https://ueinnovaschool.edu.ec/wp/. [Último acceso: 20 Junio 2022].

[19] A. D. M. C. A. S. P. L. C. J. A. M. C. V. &. G. A. A. Valdez, «Calidad de servicio en redes de telecomunicaciones,» *Extensionismo, Innovación y Transferencia Tecnológica*, vol. 4, pp. 278-293, 2018.

[20] R. Parra Loera, V. M. Morales Rocha y J. I. Hernández Hernández, «Redes Definidas por Software: beneficios y riesgos de su implementación en Universidades,» *Tecnología Educativa Revista CONAIC*, vol. 2, nº 3, pp. 48-54, 2015.

[21] V. C. M. P. S. J. C. C. M. &. A. G. Alberto, «Calidad de servicio en redes de telecomunicaciones,» *EXTENSIONISMO, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA*, vol. 4, pp. 278-293, 2018.

[22] J. &. A. P. Dordoigne, Redes Informáticas, Eni, 2016.

[23] D. D. Rojas Mesa, Análisis evolutivo de las redes desde la conmutación de circuitos hasta la actualidad de las redes de nueva generación (NGN) en Colombia, Bogotá: Universidad Nacional Abierta y a Distancia, 2022.

[24] F. Matango, «ServerVoIP,» ServerVoIP, 29 Agosto 2016. [En línea]. Available: http://www.servervoip.com/blog/redes-de-nueva-generacion/. [Último acceso: 7 Junio 2022].

[25] M. F. B. V. J. D. R. C. S. M. S. &. F. L. A. N. Andrade, «Aplicaciones de SDN en infraestructura de redes educativas,» *Ciencia Digital*, vol. 5, nº 1, pp. 219-231, 2021.

[26] Y. L. Y. Z. X. G. G. Z. W. &. S. Y. Zhao, «A survey of networking applications applying the software defined networking concept based on machine learning,» *IEEE Access*, vol. 7, pp. 95397-95417, 2019.

[27] J. Espinoza, «Medium,» Medium, 20 Julio 2021. [En línea]. Available: https://jesuseduardoespinoza.medium.com/el-controlador-y-los-planos-de-control-serie-sdn-1-1ed7a20ccf16. [Último acceso: 7 Junio 2022].

[28] A. A. B. A.-H. A. &. A. M. Malik, «Software-defined networks: A walkthrough guide from occurrence To data plane fault tolerance,» PeerJ Preprints, 2019.

[29] J. A. Castillo, «ProfesionalReview,» ProfesionalReview, 21 Febrero 2020. [En línea]. Available: https://www.profesionalreview.com/2020/02/21/switch-conmutador/#Que_es_un_Switch_o_conmutador_de_red. [Último acceso: 8 Junio 2022].

[30] L. E. Tabasco Vasallo, Análisis de la virtualización de conmutadores virtuales en redes empresariales, Santa Clara: Universidad Central "Marta Abreu" de las Villas, 2019.

[31] L. R. F. F. J. A. &. C. C. A. Amondaray, «Redes de Sensores Inalámbricos Definidas por Software,» *Revista Ingeniería Electrónica, Automática y Comunicaciones,* vol. 41, nº 2, pp. 39-50, 2020.

[32] Citrix, «Citrix,» Citrix, [En línea]. Available: https://www.citrix.com/es-mx/solutions/app-delivery-and-security/what-is-software-defined-networking.html. [Último acceso: 21 Junio 2022].

[33] M. A. G. B. &. A. S. Khan, Data visualization of software-defined networks during load balancing experiment using floodlight controller, Singapore: Springer, 2020, pp. 161-179.

[34] G. T. A. S. D. G. F. T. T. &. L. C. Di Lena, «Distrinet: A mininet implementation for the cloud,» *ACM SIGCOMM Computer Communication Review,* vol. 51, nº 1, pp. 2-9, 2021.

[35] B. S. P. S. B. S. L. Y. &. P. A. J. J. Valencia Suárez, «Mininet: una herramienta versátil para emulación y prototipado de Redes Definidas por Software,» *Entre Ciencia e Ingeniería,* nº 17, pp. 62 - 70, 2015.

[36] S. Córdoba López, Estudio de redes SDN mediante Mininet y MiniEdit, Valencia: Universitat Politècnica de València, 2019.

[37] L. Fernández, «RedesZone,» RedesZone, 24 Mayo 2022. [En línea]. [Último acceso: 8 Junio 2022].

[38] J. &. R. K. W. Kurose, Redes de computadoras, vol. 5, Pearson educación, 2010.

[39] B. Pascual Rueda, Desarrollo de un recolector de datos de monitorización para, Madrid: Universidad Autónoma de Madrid, 2018.

[40] A. V. Núñez Ramires, RED DEFINIDA POR SOFTWARE (SDN) EN BASE A UNA INFRAESTRUCTURA, Ambato: UNIVERSIDAD TÉCNICA DE AMBATO, 2015.

[41] E. Uscocovich Ruiz, Diseño de una red definida por software (SDN) basada en el protocolo openflow para pequeñas empresas, Guayaquil: Universidad de Guayaquil, 2022.

[42] ONF, «Software-Defined Networking:,» Open Networking Foundation, 2012.

[43] J. D. Chafloque Mejia, Propuesta de diseño de una red de datos de área local bajo la arquitectura de redes definidas por software para la Red Telemática de la Universidad Nacional Mayor de San Marcos, Lima: Universidad Nacional Mayor de San Marcos, 2018.

[44] D. López Pajares, Nuevos conmutadores de red para redes integradas con SDN, Madrid: Universidad de Alcalá, 2021.

ANEXOS

Anexo 1: Certificado Antiplagio

La Libertad, 5 de agosto de 2022

CERTIFICADO ANTIPLAGIO
SRV-2022-032

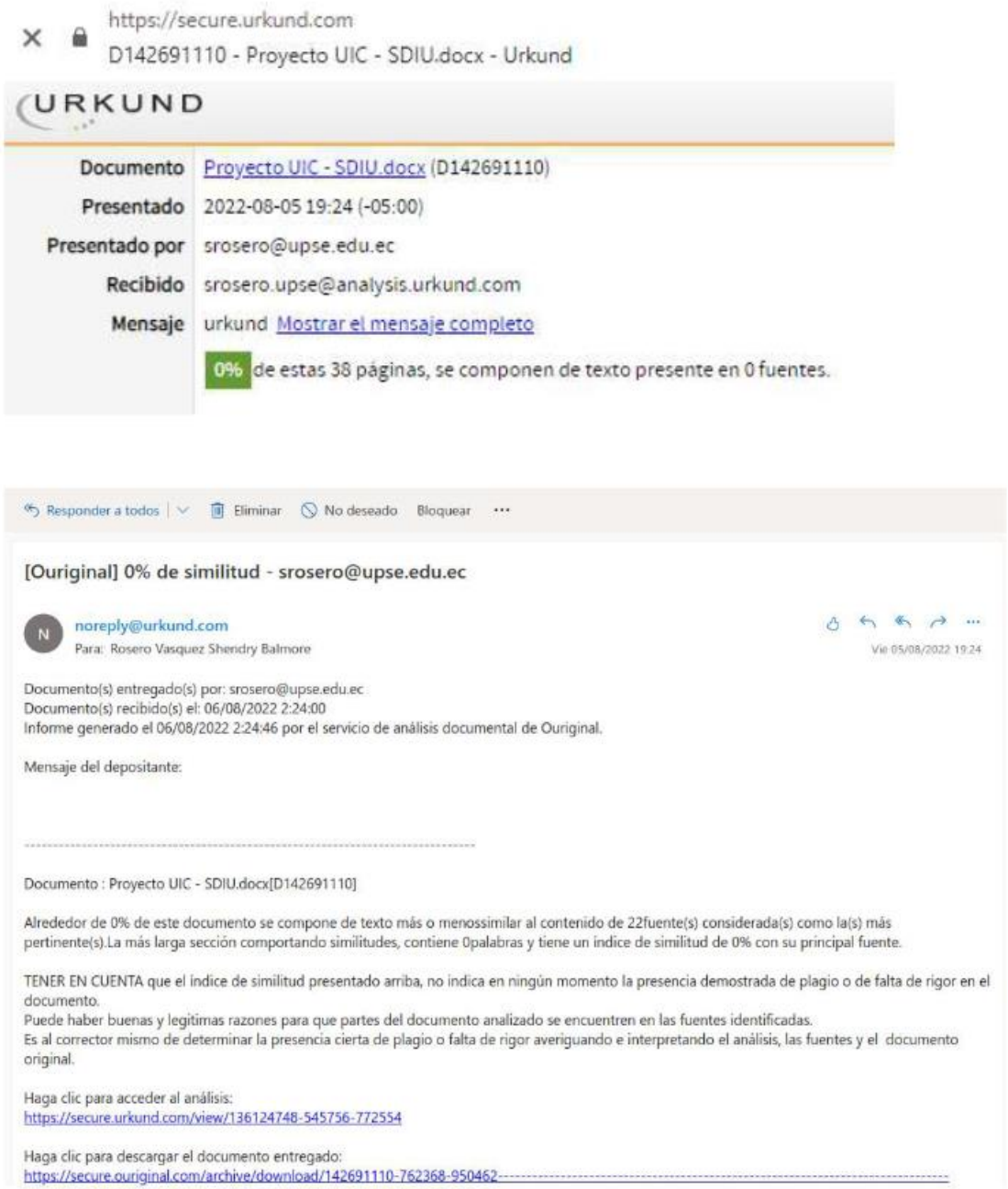
En calidad de tutor del trabajo de titulación denominado "**DISEÑO DE UNA INFRAESTRUCTURA DE RED DEFINIDA POR SOFTWARE (SDN) PARA OPTIMIZACIÓN DE LA RED TRADICIONAL DE UNA INSTITUCIÓN EDUCATIVA DEL CANTÓN SALINAS CON MININET Y MINIEDIT**", elaborado por el estudiante, **SALINAS DOMÍNGUEZ ISIDRO UBALDO**, egresado de la Carrera de Tecnologías de la Información, de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniero en Tecnologías de la Información y la Comunicación, me permito declarar que una vez analizado en el sistema anti plagio URKUND, y luego de haber cumplido los requerimientos exigidos de valoración el presente proyecto ejecutado se encuentra con 0% de la valoración permitida, por consiguiente se procede a emitir el presente informe.

Adjunto reporte de similitud.

Atentamente,

Ing. Shendry Rosero V. Ms.CC
TUTOR

Figura 99. Certificado Antiplagio 1



https://secure.urkund.com
D142691110 - Proyecto UIC - SDIU.docx - Urkund

URKUND

Documento	Proyecto UIC - SDIU.docx (D142691110)
Presentado	2022-08-05 19:24 (-05:00)
Presentado por	srosero@upse.edu.ec
Recibido	srosero.upse@analysis.urkund.com
Mensaje	urkund Mostrar el mensaje completo

0% de estas 38 páginas, se componen de texto presente en 0 fuentes.

Responder a todos | Eliminar | No deseado | Bloquear | ...

[Ouriginal] 0% de similitud - srosero@upse.edu.ec

N noreply@urkund.com
Para: Rosero Vasquez Shendry Balmore
Vie 05/08/2022 19:24

Documento(s) entregado(s) por: srosero@upse.edu.ec
Documento(s) recibido(s) el: 06/08/2022 2:24:00
Informe generado el 06/08/2022 2:24:46 por el servicio de análisis documental de Ouriginal.

Mensaje del depositante:

Documento : Proyecto UIC - SDIU.docx[D142691110]

Alrededor de 0% de este documento se compone de texto más o menossimilar al contenido de 22fuente(s) considerada(s) como la(s) más pertinente(s).La más larga sección comportando similitudes, contiene 0palabras y tiene un índice de similitud de 0% con su principal fuente.

TENER EN CUENTA que el índice de similitud presentado arriba, no indica en ningún momento la presencia demostrada de plagio o de falta de rigor en el documento.
Puede haber buenas y legítimas razones para que partes del documento analizado se encuentren en las fuentes identificadas.
Es al corrector mismo de determinar la presencia cierta de plagio o falta de rigor averiguando e interpretando el análisis, las fuentes y el documento original.

Haga clic para acceder al análisis:
https://secure.urkund.com/view/136124748-545756-772554

Haga clic para descargar el documento entregado:
https://secure.ouriginal.com/archive/download/142691110-762368-950462----------

Figura 100. Certificado Antiplagio 2