Implementación de un laboratorio virtual de redes inalámbricas mediante el software de simulación de redes GNS3 y el sistema operativo Zeroshell en la Universidad de las Fuerzas Armadas ESPE Sede Latacunga

Masapanta Jaya, Jenny Lorena y Oña Cueva, Pablo Javier

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Monografía, previo a la obtención del título de Tecnólogo Superior en Redes y Telecomunicaciones

Ing. Caicedo Altamirano, Fernando Sebastián

10 de agosto del 2022

Latacunga

Reporte de verificación de contenidos

Firmado electrónicamente por: FERNANDO SEBASTIAN CAICEDO

Ing. Caicedo Altamirano, Fernando Sebastián
C.C: 1803935020
Tutor

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Certificación

Certifico que la monografía: "**Implementación de un laboratorio virtual de redes inalámbricas mediante el software de simulación de redes GNS3 y el sistema operativo Zeroshell en la Universidad de las Fuerzas Armadas ESPE Sede Latacunga**" fue realizada por los señores **Masapanta Jaya, Jenny Lorena** y **Oña Cueva, Pablo Javier,** la misma que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisada y analizada en su totalidad por la herramienta de prevención y verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se la sustente públicamente.

Latacunga, 10 de agosto de 2022

Firmado electrónicamente por:
FERNANDO SEBASTIAN CAICEDO ALTAMIRANO

Ing. Caicedo Altamirano, Fernando Sebastián

C. C: 180393502-0

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Responsabilidad de Autoría

Nosotros, **Masapanta Jaya, Jenny Lorena** y **Oña Cueva, Pablo Javier**, con cédulas de ciudadanía n°172632916-0 y n°1722418819, declaramos que el contenido, ideas y criterios de la monografía**: Implementación de un laboratorio virtual de redes inalámbricas mediante el software de simulación de redes GNS3 y el sistema operativo Zeroshell en la Universidad de las Fuerzas Armadas ESPE Sede Latacunga,** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Latacunga, 10 de agosto de 2022

Masapanta Jaya Jenny Lorena

C.C.: 1726329160

Oña Cueva Pablo Javier

C.C.: 1722418819

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Autorización de Publicación

Nosotros **Masapanta Jaya, Jenny Lorena** y **Oña Cueva, Pablo Javier**, con cédulas de ciudadanía n°172632916-0 y n°1722418819, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar la monografía: **Implementación de un laboratorio virtual de redes inalámbricas mediante el software de simulación de redes GNS3 y el sistema operativo Zeroshell en la Universidad de las Fuerzas Armadas ESPE Sede Latacunga,** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi/nuestra responsabilidad.

Latacunga, 10 de agosto de 2022

Masapanta Jaya Jenny Lorena

C.C:1726329160

Oña Cueva Pablo Javier

C.C:1722418819

Dedicatoria

El presente trabajo de titulación se lo dedico primeramente a mi familia, quienes con su esfuerzo y ayuda inmensa me han permitido obtener un logro más en mi vida y cumplir un objetivo propuesto, todo su apoyo moral e incondicional junto al sacrificio hecho, que hoy en día se ven reflejados en este trabajo de titulación. Agradezco a Dios por brindarme la salud y la sabiduría para adquirir un buen aprendizaje.

Para mí, este logro tiene un significado maravilloso en mi vida, me permitirá cumplir una meta muy anhelada en mi vida profesional.

Jenny Lorena Masapanta Jaya

El presente proyecto investigativo va dedicado principalmente a Dios por brindarme la vida, el don de la sabiduría, la dedicación y porque a pesar de las adversidades y obstáculos me han permitido superar con mucha firmeza haciendo que lo que he vivido nunca deje que las mismas me derroten

También el trabajo de titulación se la dedico encarecidamente a mi padre y a mi madre que me supieron forjar en mi educación, con valores, principios y conocimientos, además de que su grato esfuerzo y sacrificio que realizaron a fin de brindarme el enorme apoyo que constantemente necesite para lograr alcanzar mi meta tan importante en la vida.

Hago un reconocimiento y dedicatoria a todas aquellas personas que de alguna u otra manera estuvieron presentes en todas las instancias de mi vida y en especial a mi compañera de monografía y su familia que de alguna manera estuvieron día a día con su comprensión, apoyo y dedicación con el presente proyecto investigativo sea vea reflejado en su realización.

Pablo Javier Oña Cueva

Agradecimiento

Primeramente, agradezco a Dios por brindarme la vida y salud para seguir adelante, a mi familia por todo su amor, esfuerzos y sacrificio durante el estudio de mi carrera y mi vida profesional, gracias a ustedes he logrado llegar hasta aquí y poder convertirme en la persona que soy los amo mucho.

A la Universidad de las Fuerzas Armadas ESPE, por abrir sus puertas y poder adquirir mucho aprendizaje de todos mis docentes, a quienes con mucho gusto les agradezco por sus conocimientos impartidos. Ante todo, quiero expresar un agradecimiento a mi tutor de trabajo de titulación al Ing. Fernando Caicedo por su esfuerzo, paciencia, y motivación que me han instruido para alcanzar la meta propuesta.

Existen muchas personas a quienes de una u otra manera formaron parte de mi carrera y fueron apoyo incondicional, a las que me encantaría agradecer su amistad sincera.

Jenny Lorena Masapanta Jaya

Iniciare agradeciendo a Dios por la vida y la salud que nos ha regalado a lo largo de este tiempo para seguir adelante cumpliendo mis objetivos y metas propuestas.

Mis sentimientos de gratitud infinita dirigida hacia mis padres y familiares por ser un pilar fundamental en mi formación personal y de estudio, para lo cual agradezco por todo su amor, sacrificio y esfuerzo durante todos los años de estudio y dedicación con la vida académica.

Agradezco a la Universidad de las Fuerzas Armadas ESPE, por abrirme sus puertas hacia el conocimiento y poder adquirir su fructuosa sabiduría de todos mis docentes, a quienes con mucha gratitud y valor les agradezco por sus conocimientos impartidos hacia mí. También a mi tutor de proyecto el Ing. Fernando Caicedo que con su dedicación y motivación con en el ámbito académico me supo orientar y apoyar en todo momento para culminar mi carrera.

Pablo Javier Oña Cueva

ÍNDICE DE CONTENIDOS

Índices de figuras

Índice de tablas

Resumen

El presente proyecto tiene como objetivo la implementación de un laboratorio virtual de redes inalámbricas mediante el simulador de redes GNS3 con el uso de un router MikroTik y en conjunto con el sistema operativo ZeroShell en la Universidad de las Fuerzas Armadas Espe Sede Latacunga, en el campus Belisario Quevedo, donde se realiza la instalación y configuración del simulador de redes y el sistema operativo con el objetivo de desarrollar fichas de internet, los cuales son manejados por un usuario principal o también llamado Administrador, por lo tanto el administrador tiene el control total de toda la red generada dentro del portal cautivo o también conocido como Hotspot, el mismo que asigna o crea uno o varios usuarios, claves, un tiempo predeterminado de navegación en el mundo de la red y también el administrador facilita la cantidad de Mbit/s que designara a dicho usuario, todo este proceso es realizo por el sistema operativo de red ZeroShell y el simulador de red GNS# por medio del router MikroTik con el fin de generar fichas administrables y proceder a conceder el acceso a internet y que nos permita la comunicación entre los usuarios dentro del mismo laboratorio de comunicación de la universidad.

Palabras clave: Simulación de redes inalámbricas, Sistema operativo de red ZeroShell, Portal cautivo o Hotspot.

Abstract

The objective of this project is to implement a virtual laboratory of wireless networks through the GNS3 network simulator with the use of a MikroTik router and in conjunction with the ZeroShell operating system at the University of the Armed Forces Espe Sede Latacunga, on the campus Belisario Quevedo, where the installation and configuration of the network simulator and the operating system is carried out with the aim of developing internet cards, which are managed by a main user or also called an Administrator, therefore the administrator has total control of the entire network generated within the captive portal or also known as Hotspot, the same one that assigns or creates one or more users, keys, a predetermined time of navigation in the world of the network and also the administrator facilitates the amount of Mbit/s that will designate said user, this entire process is carried out by the ZeroShell network operating system and the GNS# network simulator by means of the MikroTik router in order to generate manageable files and proceed to grant access to the internet and allow us to communicate between users within the same communication laboratory of the university.

Keywords: Simulation of wireless networks, ZeroShell Network Operating System, Captive portal or Hotspot.

Capítulo I

Planteamiento del problema

Tema

Implementación de un laboratorio virtual de redes inalámbricas mediante el software de simulación de redes GNS3 y el sistema operativo ZeroShell en la Universidad de las Fuerzas Armadas Espe Sede Latacunga.

Antecedentes

En la década de 1990 se rompió el modelo de utilizar cables como medio de comunicación en todo el mundo. En los últimos años, las redes de área local inalámbricas (WLAN) se han vuelto más populares por su rendimiento y frecuencia de nuevas aplicaciones. (Lescano, 2017, pág. 15)

Las redes inalámbricas son una de las tecnologías de más alto crecimiento en los últimos años debido a su flexibilidad y los diversos campos de aplicación. Actualmente las redes wifi se las puede encontrar en domicilios oficinas pequeñas o grandes empresas, sin embargo, estas redes no tienen un control para el acceso, por lo cual se requiere de un sistema Hotspot. Está tecnología que todos conocen como Wi-Fi, basadas en los estándares de comunicación 802.11, crece cada día a través de la instalación de puntos de acceso inalámbrico particulares, corporativos y públicos, en donde facilita el trabajo para muchos de nosotros. (Tello Peña, 2017, pág. 8)

Por el interés del tema se han realizado proyectos, tales como se indican a continuación:

Experiencias como la de Lenin José Caiza Falconi (2018) de la Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica , Escuela de Ingeniería en Electrónica, Telecomunicaciones y Redes, ubicada en la ciudad de Riobamba-Ecuador, con su

trabajo de investigación con el tema: “ESTUDIO COMPARATIVO DE LA IMPLEMENTACIÓN DE UN PORTAL CAUTIVO MEDIANTE LAS TECNOLOGÍAS MIKROTIK Y CISCO PARA MEJORAR EL RENDIMEINTO DE UNA RED INALÁMBRICA EN MIPYMES” (Caiza Falconi, 2017) concluye al momento de su estudio comparativo entre las tecnologías MikroTik tiene una manera más simple y sencilla de elegir que tecnología adquirir, ya que tiene diversos factores decisivos como son los precios y las prestaciones. Por lo cual decidirse por uno de estos dispositivos sería beneficioso para poder manejar los recursos, no obstante, puede ser las disponibilidades de la red, su control, escalabilidad, capacidad de operación, rendimiento y accesibilidad al tipo de clientes que se maneja dentro de la red.

También se tiene la experiencia de Jefferson Joseph Delgado Proaño (2018) de la Universidad Politécnica Salesiana, Carrera de Ingeniería en Sistemas, ubicada en la ciudad de Guayaquil-Ecuador, con su trabajo de investigación con el tema:” REDISEÑO DE LA RED INALÁMBRICA E IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD UTILIZANDO MIKROTIK ROUTER BASADO EN UN SERVIDOR HOTSPOT APLICANDO LAS NORMAS IEEE 802.11 EN AL FUNDACIÓN DAMAS DEL HONORABLE CUERPO CONSULAR CENTRO MÉDICO SUR” (Delgado, 2018), concluye que la seguridad es muy primordial en toda la red inalámbrica y como medida de seguridad para usuarios administrativos se ejecutó un servidor radius para la autenticación en la red inalámbrica y el uso de un Hotspot para dar prioridades de acceso a internet ingresando las credenciales en u portar cautivo. En el mismo firewall de MikroTik se realizó diferentes reglas en cada una de las vlans tales como bloqueo de páginas, descargas de archivos específicos, las pruebas ejecutadas muestran la funcionalidad del servidor radius y el servidor Hotspot con los diferentes parámetros otorgados a los usuarios. Además, mediante un servidor log se lleva un registro de los usuarios autenticados y no autenticados siendo importante para realizar una auditoría de la red inalámbrica.

También se obtuvo la experiencia de Cristopher Geovanny Ligua Marcillo (2019) de la Universidad Estatal del Sur de Manabí, Facultad de Ciencias Técnicas Carrera de Ingeniería en Computación y Redes, ubicada en la cuidad de Manabí-Ecuador, con su trabajo de investigación con el tema: “DISEÑO DE UN HOTSPOT PARA EL MEJORAMIENTO DE ACCESO DE INTERNET PARA EL PARQUE CENTRAL DE LA PARROQUIA LA AMÉRICA DEL CANTÓN JIPIJAPA” (Ligua, 2019) concluye que el Hotspot es utilizado en ocasiones muy alta para navegación de internet dentro diversas acción de comunicación o información, y por otra parte es necesario la implementación del mismo para mejorar el rendimiento de acceso a internet dirigido a pueblos donde se puede brindar un servicio gratuito de navegación.

Por lo escrito anteriormente se deduce que al implementar un laboratorio virtual para el campus centro Latacunga de la Universidad de las Fuerzas Armadas ESPE, permitirá generar redes inalámbricas para el mejoramiento del uso de los laboratorios de la Universidad, al realizar la implementación de sistemas de apoyo al aprendizaje; en particular en los programas de formación técnica como las ingenierías y tecnologías ya que apoyarían y facilitarían un óptimo aprendizaje a los estudiantes y personal docente, en lo que existen prácticas con equipos y dispositivos en los laboratorios de Comunicaciones.

Planteamiento del problema

La Universidad de las Fuerzas Armadas ESPE tiene 99 años de historia considerada una de las más emblemáticas del país por tener una innovación y un gran aporte al desarrollo productivo del Ecuador. Fundada el 16 de junio del 1922 es distinguida por entregar soluciones prácticas para los alumnos y docentes de la universidad, contribuyendo a nuevas investigaciones que son desarrolladas por los docentes. El 26 de junio de 2013, el Consejo de Educación Superior del Ecuador aprobó los nuevos estatutos de la institución, mediante los cuales se aceptaba la fusión de los tres centros de educación superior de las Fuerzas Armadas (Escuela Politécnica del Ejército - ESPE, la Universidad Naval Rafael Morán Valverde -

UNINAV y el Instituto Tecnológico Superior Aeronáutico - ITSA), en la que a partir de ese momento pasa a denominarse Universidad de las Fuerzas Armadas - ESPE. (Wikipedia, 2021)

En el campus Espe Latacunga se encuentran los laboratorios pertenecientes a los departamentos de las diferentes carreras, donde se visualiza que el uso de los mismo no es aprovechado, por lo cual los laboratorios se han venido reforzando con el paso del tiempo, sin embargo, estos no cuentan con un sistema para prácticas de laboratorio relacionado a redes inalámbricas que permitan el desarrollo de habilidades de los estudiantes pertenecientes a la Universidad Espe-Latacunga.

Esto ha dado origen a que:

- Los estudiantes graduados de la carrera tengan dificultad e inconformidad en el ámbito laboral debido a la falta del desarrollo de sus habilidades prácticas en área de redes inalámbricas y la creación de laboratorios virtuales.
- Los estudiantes al realizar sus prácticas pre profesionales no obtienen los conocimientos necesarios para ejecutar sus habilidades en el área correspondiente, por lo que presentan falencias en la creación e instalación de un servidor Hotspot para el acceso de internet.

De no solucionarse lo expuesto se presentarán inconvenientes en el aprendizaje en el área de las redes inalámbricas, por lo cual el personal docente y alumnado no podrán realizar las practicas correspondientes a las asignaturas, al no contar con todo lo necesario para la creación de laboratorios o redes virtuales, por lo que no se podrá demostrar los conocimientos adquiridos durante todo el periodo escolar.

Por lo mencionado es importante que la Universidad de las Fuerzas Armadas Espe-Latacunga, integre las tecnologías computacionales y virtuales para desarrollar una conexión virtual educativa orientadas a las redes inalámbricas, en donde alumnos, maestros e investigadores pueden resolver problemas específicos de conectividad mediante Hotspot o compartir e intercambiar ideas sobre un experimento bajo un ambiente de trabajo grupal

virtualizado, siendo se va a implementar varios softwares de simulación para redes inalámbricas, creando así un laboratorio virtual con un servidor Hotspot, para la interacción del usuario con el laboratorio virtual.

Justificación

La Universidad de las Fuerzas Armadas ESPE-Latacunga es reconocida como un referente a nivel nacional y regional por trabajar de la mano del avance tecnológico, siendo así que el acceso a la información es parte fundamental dentro de la comunidad universitaria, generando así un amplio desarrollo de habilidades tanto físicas como virtuales en el área de las redes inalámbricas al implementar el servidor Hotspot para mejorar el acceso al internet dentro de los laboratorios.

Así como también ayuda a:

- Ampliar el conocimiento en el área de las redes inalámbricas, creando laboratorios virtuales utilizando servidores y sistemas operativos.
- Brinda un acceso a internet mejorado en cada laboratorio de comunicación para lo cual es fundamental el aprendizaje de cada estudiante perteneciente a la Universidad de las Fuerzas Armadas ESPE-Latacunga.
- Optimizar recursos y transmitir grandes cantidades de información con el acceso a internet.
- Desarrollar habilidades y destrezas de los estudiantes pertenecientes a la carrera de Tecnología Superior en Redes y Telecomunicaciones

Es por esto que el proyecto justifica que lo argumentado permite mejorar las habilidades de aprendizaje en las redes inalámbricas mediante servidores Hotspot, lo cual permitirá desarrollar las habilidades de los estudiantes en los laboratorios de comunicación, proporcionando así un amplio conocimiento en el área relacionada a redes y telecomunicaciones.

Se beneficiarán del presente proyecto investigativo, estudiantes, docentes y personal militar, puesto que contará con laboratorios virtuales en base a la implementación de un servidor Hotspot que servirá principalmente para brindar conectividad entre las distintas máquinas virtuales a implementar y un sistema operativo para tener un funcionamiento correcto.

Los resultados permitirán que la institución pueda cumplir con parámetros exigidos para su funcionamiento, de igual manera ayudará a mejorar la imagen institucional y sobre todo perfeccionar el conocimiento de los alumnos de la carrea de tecnología superior en Redes y Telecomunicaciones.

Por lo mencionado es importante que el campus Latacunga, disponga de laboratorios virtuales con servidores Hotspot, para el desarrollo de prácticas que faciliten al estudiante adquirir un amplio conocimiento y ejecute todas las habilidades en el área de las redes inalámbricas.

Objetivos

General

- Implementar un laboratorio virtual de redes inalámbricas mediante el software de simulación de redes GNS3 y el sistema operativo ZeroShell en la Universidad de las Fuerzas armadas Espe Sede Latacunga.

Específicos

- Investigar acerca del software GNS3 y el sistema operativo ZeroShell para la correcta implementación en el laboratorio.
- Instalar el software de simulación GNS3 y el sistema operativo ZeroShell en el laboratorio de comunicaciones de la ESPE-L.

- Simular dos redes inalámbricas Hotspot mediante la conectividad Wifi con los puntos de acceso a internet entre los dispositivos inalámbricos que sirvan para realizar las prácticas en los laboratorios de ESPE-L.

Alcance

El presente trabajo investigativo contiene un análisis técnico en el área de las redes inalámbricas utilizando software de simulación de redes GNS3 y el sistema operativo ZeroShell en los laboratorios de la Universidad de las Fuerzas Armadas Espe-Latacunga, basado en un estudio práctico que demuestre como estas tecnologías o herramientas de interacción académica pueden ayudar a solucionar los problemas que se presentan con respecto a las redes inalámbricas Wi-Fi o Hotspot.

Siendo así en el desarrollo de una herramienta para la educación virtual a distancia a través de internet. Se toma como caso de estudio un laboratorio de Comunicaciones, para ilustrar el potencial de esta aproximación en el trabajo experimental a través del uso de tecnologías modernas adaptadas a la necesidad que el eventual laboratorio necesita.

El laboratorio de comunicaciones de la universidad de las fuerzas armadas espe-campus Belisario Quevedo, se pretende instalar un prototipo de laboratorio virtual para lo cual se implementará sistemas operativos con el fin de recrear una simulación de red inalámbrica Hotspot, en donde el administrador tendrá el control total al momento de manejar la red, siendo el caso que se necesite el aumento de Mb con el objetivo de una navegación de red correcta

El sistema que se desarrolla en este trabajo, tiene como objetivo servir como apoyo de información y consulta para estudiantes interesados en temas relacionados a este proyecto.

Capítulo II

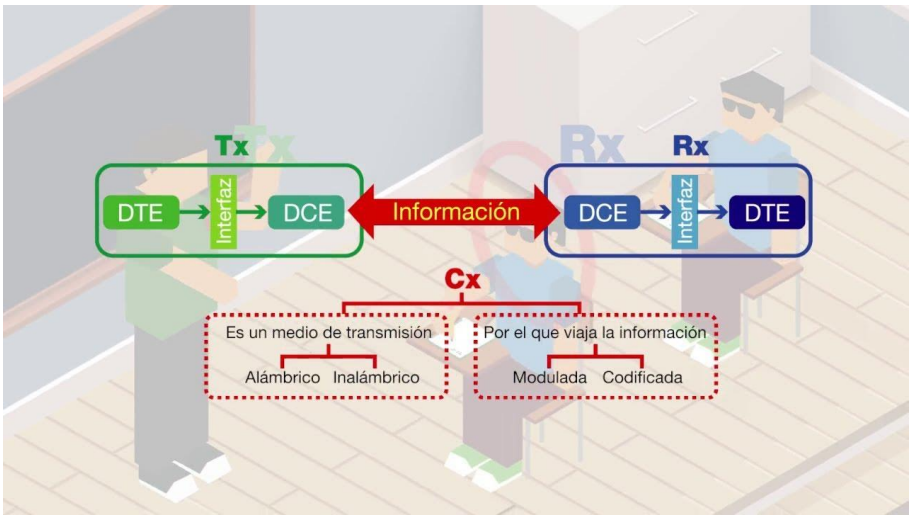
Marco teórico

Sistemas De Comunicación

Son un conjunto de medios, tecnologías, protocolos y facilidades en general, que tiene como objetivo transmitir, emitir y recibir señales de todo tipo, ya sea voz, datos, audio, video, etc. Para lo cual existen dos señales diferentes, como son digitales y analógicas.

Figura 1

Diagrama del sistema de comunicación



Nota. Se observa el funcionamiento del transmisor y receptor en un sistema de comunicación. Tomado de: (Udearroba, 2017)

El sistema de comunicaciones se detalla en tres elementos: un transmisor, el que generar la señal que puede combinar, de tal forma que esta pueda viajar por medio del canal permita ejecutar los procedimientos como lo es modulación, filtrado, codificación, etc. El medio de transmisión, es el canal mediante el cual la señal pasa por fibras ópticas, cables coaxiales, por medio del aire y finalmente el receptor, desempeña el procedimiento inverso del transmisor con el objetivo de reconstruir la señal y que esta sea idéntica a la original para adquirir la

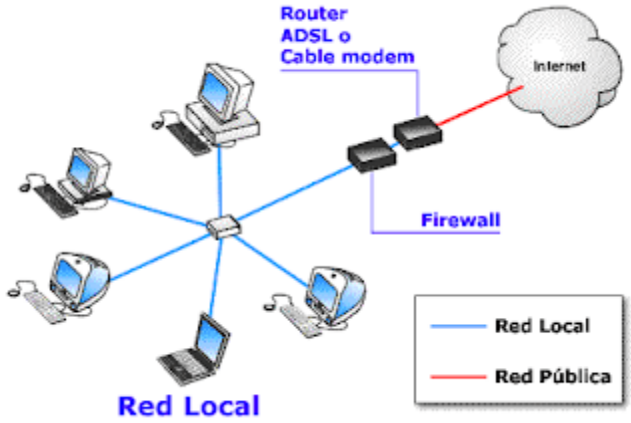
comunicación y el enlace de información completo. Habitualmente esto es necesario para el intercambio de información que se proporciona con la facultad de poder entenderse mutuamente entre ambas partes, ya sea entre las mismas personas, dispositivos electrónicos, sistemas de red. En donde la red es una estructura que para su estudio casi siempre se suele dividirse en componentes, como puede ser red de acceso, red de tránsito o núcleo de red, servidores, estaciones de trabajo y recursos periféricos y compartidos. (Tolomeo, 2017, pág. 1)

En los sistemas de telecomunicaciones se genera señales eléctricas, electromagnéticas u ópticas para la transmisión de información, por lo que se usa dos medios que se presentan a continuación (Parra, 2016):

Comunicación Alámbrica

Figura 2

Diagrama de la comunicación alámbrica



Nota. La figura muestra el funcionamiento de la comunicación alámbrica dentro de una red local. Tomado de: (sites, 2014)

La comunicación alámbrica está constituida por medio de cables, hilos de fibra óptica, que pueden ser de varios tipos, dependiendo de la capacidad para transportar información y de la resistencia que oponen a la interferencia (Linares, 2017).

Medios de transmisión de la comunicación alámbrica

a. **Cable de par trenzado:** está formado por 2 grupos de hilos a los cuales se les denomina como pares ya que estos están aislados entre sí y recubiertos de material plástico. Este cable es usado para la transmisión en distancias cortas, debido que en distancias largas la señal no transmite correctamente y se pierde información, las redes y el teléfono son quienes usan este tipo de cableado por la distancia corta (LAN) (Parra, 2016).
b. **Cable coaxial:** este tipo de cable es utilizado para transmitir señales eléctricas de alta frecuencia que contiene dos conductores separados por un aislante, una malla metálica externa la cual impide la interferencia, además de eso este tipo de cable se usan para transmitir a grandes distancias sin pérdida de información (Farrez, 2018).
c. **Fibra óptica:** este tipo de cable es un medio de transmisión de datos mediante impulsos fotoeléctricos, por medio de un hilo construido en vidrio transparente y otros materiales plásticos que cumplen la misma funcionalidad de transmitir luz, por lo que la información puede ser más rápido al momento de su envío y recepción (Parra, 2016).

Comunicación inalámbrica

La comunicación inalámbrica describe varias tecnologías que dependen de la señal inalámbrica para él envió de datos en remplazo del uso de medios físicos. El funcionamiento que realiza el emisor es de ondas electromagnéticas que, al transmitir la información codificada, el receptor recibe la información en ondas y está la decodifica y recepta la información, estas ondas viajan a través del aire como lo hace la radio, la redes wifi, bluetooth, etc. sin tener medios físicos. (Cuñas, 2017).

Que son las redes

Es un conjunto de equipos o dispositivos conectados entre sí; para el intercambio de recursos ya sea como hardware o software y de información habitual. Existen varios tipos de redes y las cuales una es; Las redes informáticas que se pueden clasificar según su tamaño; ósea la cantidad de equipos conectados que se puede tener en sí, velocidad de transferencia y alcance de la red que vendrían a ser las distancias geográficas que se tienen entre los dispositivos o los equipos utilizados. (Significados, 2017)

Redes de comunicaciones

Se denomina red de comunicaciones al sistema de equipos informáticos conectados entre sí; el enlace se lo hace por medio de dispositivos físicos que se envían y reciben mediante impulsos eléctricos, ondas electromagnéticas, no obstante, se busca el transporte de datos con la finalidad de compartir información, datos, y ofrecer varios servicios. (Rodriguez, 2017) Para lo cual la información se logra mediante la transmisión de forma analógica, digital o mixta.

Para realizar la red de comunicaciones se necesita de algunos componentes básicos de red, para simplificar y observar si logra formar una o varias redes se requiere de los siguientes elementos fundamentales como son los hardware, software y comúnmente los protocolos. (Rodriguez, 2017)

a. **Dispositivos de usuario final (Hosts):** en estos dispositivos se encuentran varios incluidos como: las computadoras, impresoras, escáneres, y finalmente los elementos que alcanzan a brindar diversos servicios directamente hacia el usuario.
b. **Dispositivos de red:** se debe tener en cuenta que son aquellos que logran conectar entre si hacia los dispositivos de usuario final, haciendo que funcione la intercomunicación entre sí.

En la comunicación de red se debe tener en cuenta los softwares, los cuales se basan en la comunicación de las redes; siendo el caso tienen dos importantes clasificaciones las cuales ayudan a comprender la red de comunicaciones. (Rodriguez, 2017)

- **Sistema operativo de red:** Este sistema platea la facilidad de la interconexión de los ordenadores para lograr acceder a los demás servicios y recursos. Esto necesita de un sistema operativo de red para su total operación y funcionalidad.
- **Software de aplicación:** El software coloca a todos los elementos que se manejan para que los usuarios puedan utilizar sus programas y archivos específicos. Por lo tanto, este software proporciona varias amplitudes, tanto como sea posible o lo requiera, esto puede incluir diversos procesadores de texto, paquetes integrados, sistemas administrativos de contabilidad, áreas afines, sistemas especializados y por consiguiente correos electrónicos. (Rodriguez, 2017)

Las redes de comunicación contienen, otro factor fundamental y esencial para su intercomunicación que es el material físico o tangible. Esto vendría a ser el hardware; En efecto está caracterizado por los siguientes componentes o dispositivos.

- **Tarjeta de red:** Es un componente que demuestra obtener los enlaces entre uno o varios dispositivos y su vez de la comunicación de los computadores y los medios de transmisión, es fundamental la intervención de una tarjeta de red o también llamada NIC (Network Card Interface), este tipo de tarjetas facilita el acceso de enviar y recibir paquetes de datos hacia otros usuarios o computadoras, siendo así se puede emplear un protocolo para su comunicación y se convierte esos datos en un código que pueda ser transmitido mediante (bits, ceros y unos). (Rodriguez, 2017)

Redes inalámbricas

Las redes inalámbricas son conexiones que, por medio de ondas electromagnéticas, realizan la transmisión y recepción de información o datos, dejando a un lado la conexión física del cableado de redes (ConceptoABC, 2022). Para la transmisión y recepción de datos se necesita que los dispositivos procedan a actuar como puertos, por lo cual, los vínculos entre computadoras y otros equipos informáticos no requieren la instalación de cableado, por lo que se asume un ahorro de dinero en infraestructura. (Merino, 2011)

Los dispositivos remotos son fácilmente de conectar dentro del área de la red, lo cual permite que varios terminales obtengan una comunicación sin tener la necesidad de estar conectado por medio de cables, en la siguiente figura 5 se muestra la representación de cómo trabajan las redes inalámbricas. (ConceptoABC, 2022)

Figura 3

Topología de una Red Inalámbrica

Nota. La figura demuestra la emisión de señal de una red inalámbrica a varios dispositivos, para la conexión a internet. Tomado de: (Duarte, 2015)

Características de las redes inalámbricas

Las redes inalámbricas proveen la conexión de ordenadores o laptop, por lo que tiene alcance, velocidad de transmisión, y seguridad siendo los factores claves para la elección del uso de las redes inalámbricas (Muñoz, 2018), existen dos amplias categorías de redes inalámbricas:

a. **Redes de larga distancia:** Son aquellas que se utilizan en distancias largas como su nombre lo indica, es decir puede ser de una ciudad a otra u otro país del mundo.
b. **Redes de corta distancia:** se usan para distancias cortas, como en edificios o casas donde la señal puede estar alrededor de donde esté instalada la red.

Funcionamiento de Una Red Inalámbrica

El funcionamiento de una red inalámbrica, permite conectar varias computadoras utilizando datos binarios, es decir la información se codifica en 2 dígitos entre ceros y unos. Lo que significa que los datos binarios se codifican transformándose en frecuencias de una onda de radio y son transmitidas a través de una antena, además de eso realiza la conversión de datos binarios a señales de radio, todo este proceso lo hace una tarjeta Ethernet, la misma que está integrada en su mayoría de dispositivos modernos.

Los datos enviados mediante una señal de radio por antena son recibidos en el ordenador por medio de la antena y la tarjeta Ethernet decodifican la señal a datos binarios nuevamente, para que la PC recepte la señal de mejor manera, todo este proceso permite obtener la red inalámbrica en funcionamiento para enviar y recibir datos o información por medio del aire sin el uso de cables. (Redes Inalambricas, 2022)

Figura 4

Tarjeta Ethernet

Nota. La figura indica un puerto de la tarjeta Ethernet que se conecta a una antena para el envío de la información. Tomado de: (Redes Inalambricas, 2022)

Rangos de frecuencia de las redes inalámbricas

Las redes inalámbricas tienen una característica u otra según el rango de frecuencia utilizado para transmitir. La transmisión puede cambiar entre las que se presenta a continuación: (ConceptoABC, 2022):

- **Ondas de radio:** emplea una transmisión de frecuencia de ondas electromagnéticas omnidireccionales. No requiere de antenas parabólicas.
- **Microondas por satélite:** se une dos o más estaciones terrestres (estaciones base). Como lo es, el satélite que recibe la señal en una banda de frecuencia, la amplifica y la retransmite en otra banda, la figura 5 representa la función que realiza la trasmisión de microondas por satélites

Figura 5

Diagrama de la transmisión de la señal microondas por satélite

Nota. En la figura se observa la transmisión de señal que realiza el satélite en formas de ondas de radio de alta frecuencia. Tomado de: (ConceptoABC, 2022)

- **Infrarrojos:** enlaza transmisores y receptores que modulan la luz infrarroja no coherente. Estos deben estar alineados directamente o con una reflexión en una superficie, en la figura 6 se visualiza la transmisión de señal por medio del infrarrojo.

Figura 6

Transmisión de señal del infrarrojo

Nota. La figura muestra cómo trabaja el infrarrojo al radiar una longitud de onda donde la luz es visible. Tomado de: (Google sites).

- **Microondas terrestres:** Es empleada por el uso de antenas parabólicas, contine una cobertura de kilómetros, con el inconveniente de que el emisor y el receptor deben estar perfectamente alineados (ConceptoABC, 2022), en la figura 7 visualizamos la radiocomunicación por medio del microondas terrestre.

Figura 7

Radiocomunicación por microondas terrestre

Nota. La figura presenta, indica la transmisión de datos o energía a través de radiofrecuencias con longitudes de onda tipo microondas. Tomado de: (ConceptoABC, 2022)

Tipos de redes inalámbricas

Las redes inalámbricas propagan la conexión a internet a través de los medios no físicos, usando varias tecnologías como las ondas electromagnéticas, radiación y medios ópticos para la transmisión de señal (Optical Networks, 2019).

Según su área de alcance.

Se clasifican de modo semejante a las redes alámbricas:

1. **WPAN.** Siglas de Wireless Personal Area Network (Red Inalámbrica de Área Personal), comprende un rango máximo de 10 metros, que sirve para uno o dos usuarios máximo, que se encuentren juntos. Este tipo de tecnologías incluye (concepto, 2021):

- **HomeRF**

  Estándar que permite la conexión de todos los teléfonos móviles de la casa y los ordenadores mediante un dispositivo central.

- **Bluetooth**

  Es un protocolo de comunicaciones que permite la transmisión inalámbrica de datos, como lo son las fotos, videos y música, entre distintos dispositivos que se encuentre a corta distancia, adicional a eso sigue la especificación IEEE 802.15.1 (Secarcam, 2016)

- **ZigBee**

  Es empleado en aplicaciones como lo es la domótica, que requiere comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo, requiere de las especificaciones IEEE 802.15.4 (Secarcam, 2016)

- **RFID**

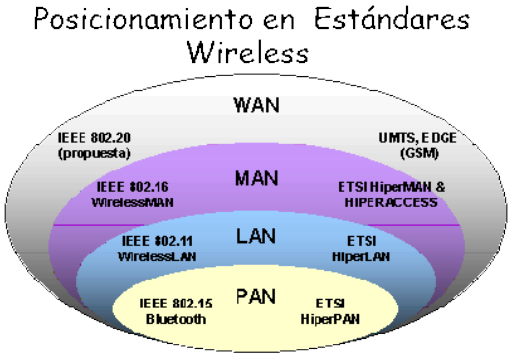
  Un sistema remoto de almacenamiento y recuperación de datos con el fin de transmitir la identidad de un objeto, idéntico a un número de serie único, por medio de ondas de radio (Secarcam, 2016).

2. **WLAN.** Sus siglas de Wireless Local Area Network (Red Inalámbrica de Área Local), es un estándar de comunicaciones en el cual se basan las tecnologías WiFi, que alcanzan una distancia mucho mayor en base a repetidoras, interconectando diversos tipos de aparatos mediante ondas de radio. (concepto, 2021)
3. **WMAN.** Siglas de Wireless Metropolitan Area Network (Red Inalámbrica de Área Metropolitana), una red mayor alcance, con una capacidad de cubrir hasta 20 kilómetros (concepto, 2021).

4. **WWAN.** Siglas de Wireless Wide Area Network (Red Inalámbrica de Área Amplia), utiliza las tecnologías de telefonía celular y microondas para transferir datos a largas distancias. Sus tipos de tecnología son GPRS, EDGE, GSM, 3G, 4G o 5G. (concepto, 2021)

Figura 8

Posicionamiento en estándares Wireless

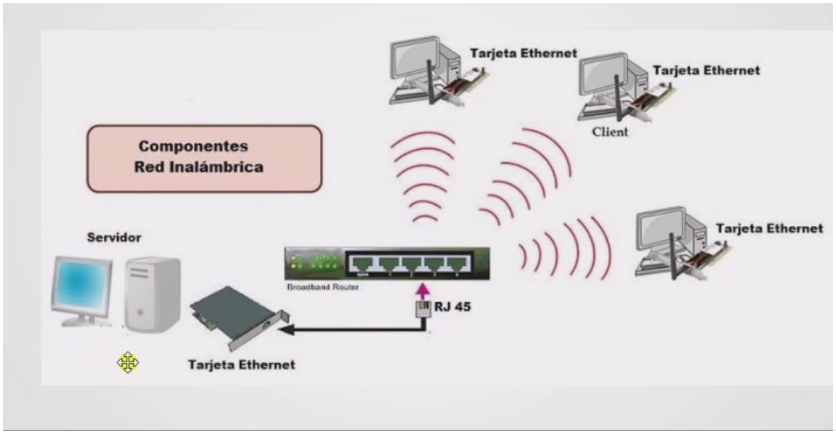


Nota. La figura muestra los estándares de los tipos de red inalámbrica que se maneja en la actualidad. Tomado de: (Secarcam, 2016)

Dispositivos de una red inalámbrica

Figura 9

Dispositivos de redes inalámbricas



Nota. La figura se observa los distintos componentes que se utilizan en la estructura de una red inalámbrica. Tomado de: (Redes Inalambricas, 2022)

a. **Dispositivos con capacidad inalámbrica.** este tipo de dispositivos para obtener conexión inalámbrica se debe tener un computador, teléfono, tableta o artefacto que contenga una antena capaz de percibir y emitir ondas electromagnéticas, con la capacidad de recibir y emitir señales de radiofrecuencia. Por lo cual se debe tener una tarjeta de red inalámbrica operativa. (concepto, 2021)

Figura 10

Dispositivos inalámbricos

Nota. En la figura presente se observa los distintos dispositivos que contiene tarjetas de red las cuales les permite obtener conexión a Internet. Tomado de: (HUEHUEH, 2015)

b. **Estaciones base.** Es una torre fija con capacidad para tener una comunicación baja, media o bidireccional, son moduladores que convierten la señal alámbrica en una señal inalámbrica transmitida por ondas de radio. (MÁSMOVIL, 2022)

Figura 11

Estación de base

Nota. La figura se observa cómo trabaja la estación base al enviar y recibir señales de radio con baja potencia. Tomado de: (EMF Explained, 2013)

c. **Repetidoras.** Dispositivos diseñados para percibir y reemitir una señal específica de ondas electromagnéticas, para da un reimpulso y permitirles para que pueda llegar más lejos o a lugares de otro modo inaccesibles (concepto, 2021).

d. **Enrutadores y puntos de acceso.** Los enrutadores “routers” son dispositivos que “traducen” la señal de Internet y la dirigen a los puntos de acceso, para que pueda ser distribuida por los diversos usuarios de una red. A los primeros se asignan una dirección IP, para el control y organización del acceso a los paquetes de datos y evitar pérdidas y solapamientos. (concepto, 2021)

e. **Router Inalámbrico.** Los routers inalámbricos son dispositivos de hardware los cuales proveen el servicio de internet para su conexión se usa el punto de acceso inalámbricos y un router, que conectan dispositivos de red con una frecuencia de radio dentro de las bandas de 900MHz y 2,4: 3,6: 5 y 60 GHz. (Cisco, 2020)

Figura 12

Red de infraestructura inalámbrica

Nota. En la figura se aprecia la función que tiene el router inalámbrico en un hogar o edificios, donde los dispositivos conectados tengan comunicación entre sí. Tomado de: (Miguel Angel, 2016)

Redes inalámbricas Wi-Fi

En las redes inalámbricas basadas en Wi-Fi, conectan los dispositivos en un solo enrutador, más no la conexión directa uno con otro.

Figura 13

Diagrama de la red inalámbrica Wi-Fi

Nota. En la figura se observa la conexión de dos router que trabajan como un conmutador que recibe señal desde un punto hacia otro punto principal. Tomado de: (Redes Inalambricas, 2022).

Las redes inalámbricas trasmiten señal y reciben la misma, para que todo esto suceda los dispositivos de una red no deben mezclarse con otros donde se utiliza el SSID (Service Set IDentifier) es un paquete de datos enviados por los dispositivos de una red inalámbrica. Este código alfanumérico contiene un máximo de 32 caracteres, para que los dispositivos inalámbricos intenten tener una comunicación entre sí, para lo cual deben compartir el mismo SSID. (Miguel Angel, 2016)

Señal Wi-Fi

La señal wifi usa ondas de radio para obtener una comunicación entre diferentes dispositivos como computadoras, teléfonos celulares, tablets o routers de red, donde el router inalámbrico contiene la interfaz de conexión por cable a internet u otra red Ethernet y a los dispositivos inalámbricos. La señal wifi trabaja con los estándares de red 802.11 al momento de transmitir la información. (NetSpot, 2022)

La intensidad de la señal wifi tiene una cantidad conocida como dBm (decibelios) relativos a una mili vatio que es representado por números negativos desde 0 – a 100. Los niveles de ruido afectan al funcionamiento del WiFi los mismo que también son expresado por dBm, aquí también se puede conocer el valor próximo a 0 indica altos niveles de ruido que se pueden producir, a continuación, se indica en la figura las diferentes intensidades de señal que utiliza el WiFi. (NetSpot, 2022)

Figura 14

Intensidad de la señal WiFi

Intensidad de la señal	Calificador	Usos adecuados
-30 dBm	Excelente	Esta es la máxima intensidad de señal alcanzable y será apropiada para cualquier situación de uso.
-50 dBm	Excelente	Este excelente nivel de señal es adecuado para todos los usos de la red.
-65 dBm	Muy bueno	Recomendado para smartphones y tablets.
-67 dBm	Muy bueno	Esta intensidad de señal será suficiente para voz sobre IP y streaming de vídeo.
-70 dBm	Aceptable	Este nivel es la intensidad mínima de la señal requerida para asegurar una entrega de paquetes fiable y le permitirá navegar por la web e intercambiar correos electrónicos.
-80 dBm	Malo	Permite la conectividad básica, pero la entrega de paquetes no es fiable.
-90 dBm	Muy malo	Un ruido que inhibe la mayoría de las funciones.
-100 dBm	Peor	Ruido total.

Nota. En la figura se muestra la intensidad de señal wifi en su diferente uso adecuado. Tomado de: (NetSpot, 2022)

Los Estándares de las Redes Inalámbricas

Los estándares de la red inalámbrica regulan la velocidad y el tipo de transmisión que se usan mediante los datos por las ondas de radio que se generan. El Instituto de Ingenieros Eléctricos y Electrónicos IEEE es una organización internacional, creada sin fines de lucro, son

líderes en el campo de las promociones de estándares nacionales e internacionales. (Redes Inalambricas, 2022)

La elaboración del estándar ‘’IEEE 802.11n’’ tiene velocidades de entre 150 y 600 Mbps, pero la nueva tecnología ac ‘’802.11ac’’ aumentan la velocidad teórica y periódicamente hasta los 1.300 Mbps. Usan bandas de frecuencias entre 2,5 y 5GHz (giga hertzios). Los dispositivos conectados a una red tienen compatibilidad con los estándares anteriores o posteriores y un adaptador inalámbrico, siempre van a escoger y usar, el de mayor velocidad, de acuerdo a las necesidades que se estén generando con respecto a la utilización de la red. (Redes Inalambricas, 2022)

Estándar de las redes inalámbricas WiFi

Las redes inalámbricas wifi operan en un conjunto de frecuencias de 2,4 GHz y 5 GHz, y otros dispositivos que trabajan en la misma frecuencia, como teléfonos celulares, walkie-talkies e incluso televisores, por lo que de igual forma se puede transmitir utilizando este tipo de estándares de red 802.11 (Miguel Angel, 2016):

a. 802.1x

La fabricación de esta estándar mejora la seguridad de todas las redes de área local al proporcionar un marco de autenticación que permiten a los usuarios o el administrador autenticarse ante una autoridad central que controle dicha conexión, como LDAP o Active Directory. Las tecnologías de acceso ‘’802.11’’, contienen un mecanismo eficaz y eficiente para el control del acceso a la red de área local inalámbrica (Redes Inalambricas, 2022).

b. 802.11a

Se creó una extensión del estándar 802.11 realizando por los ingenieros de la IEEE para las tecnologías de redes inalámbricas. El estándar ‘’802.11a’’ se utilizado en redes de áreas locales inalámbricas y acoge velocidades máximas de conexión de entre 54 Mbps en la banda de 5 GHz.

c. 802.11b

El estándar ‘’802.11b’’ se aplica a las redes de áreas locales inalámbricas y contiene una velocidad de conexión máxima de entre 11 Mbps con retroceso de hasta 5,5, 2 y 1 Mbps en la banda llamada ISM de 2,4 GHz.

d. 802.11g

Este tipo de estándar 802.11 permite que las velocidades de conexión máxima sean entre 54 Mbps mientras se pueda mantener la compatibilidad exclusiva con el estándar 802.11b en la banda de 2.4GHz.

e. 802.11i

El estándar 802.11 que proporciona seguridades eficientes que está disponible en extensiones ‘’802.11’’. La extensión elaborada proporciona métodos mejorados de encriptación y la integración del protocolo de autenticación ‘’IEEE 802.1x’’, como lo son los mecanismos de encriptación avanzados como la ‘’AES’’ o también identificado como (Advanced Encryption Standard), que serán para una implementación opcional y totalmente compatible con dicho estándar ‘’802.11i’’.

f. 802.11n

El estándar más usado y configurado actualmente el ‘’802.11n’’, Por que emplea múltiples antenas transmisoras y receptoras, permiten un mayor rendimiento y rango de datos en la red. Este tipo de estándar fue ratificado y modificado en el año de 2009. La fabricación del hardware estándar está disponible comercialmente y no es compatible con el dispositivo wireless PittNet. (Redes Inalambricas, 2022)

Figura 15

Estándar de las redes inalámbricas

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

Nota. En la figura de visualiza los tipos de estándares que se utilizan en las redes inalámbricas. Tomando de: (Oliveros, 2016)

g. 802.11ac

Su implementación dio inicio en el año del 2014, desde los componentes que se emplearon para el consumo menor de energía, por lo tanto, es preferible para dispositivos portables, es factible compartir datos comunes a usuarios diferentes, todo este proceso utiliza la banda 5 GHz, y el radio de alcance será menor, al momento del desarrollo de la práctica su alcance es mucho mayor usando la tecnología “Beamforming” la cual es la encargada de focalizar la señal de radio (ALvarez, 2015).

h. 802.11ah

Es un nuevo protocolo de redes inalámbricas que empezó a implementarse en el año 2016, este tipo de estándar inicio por los requerimientos de la tecnología, la información y la demanda en el mercado. Este estándar se diferencia a los demás por utilizar frecuencias menores a 1 GHz, y da paso a aumentar el rango de alcance de las redes, hasta un alrededor de 100 metros. Adicional a eso este tipo de estándar se lo usa en la práctica de

distribución en áreas rurales, utilizando torres de telefonía con sensores para repartir la señal. El estándar 802.11ah llevara un nombre Wi-Fi HaLow actualmente (ALvarez, 2015).

Ventajas de las redes inalámbricas

- Dado que las redes inalámbricas no utilizan medios cableados o físicos para establecer conexión entre dispositivos, tienen mayor libertad los equipos conectados a la red.
- Las tecnologías de red inalámbricas como el Wi-Fi, acceden a la conexión de un gran número de dispositivos móviles como teléfonos, tablets, impresoras y ordenadores.
- El mantenimiento de las redes inalámbricas es más factible y económico que en las redes cableadas, ya que se debe supervisar los aparatos transmisores de señal.
- Las redes inalámbricas son ideales en su instalación para espacios donde nonse puedo colocar correctamente. (ConceptoABC, 2022)

Desventajas de redes inalámbricas

- Algunas redes inalámbricas pueden llegar a realizar interferencias, lo que puede afectar la calidad de conexión a internet.
- Una de las desventajas primarias esta entre las redes inalámbricas vs las redes alámbricas, la red alámbrica no logra superar la velocidad de transferencia de datos de las redes alámbricas, mientras que una red inalámbrica alcanza hasta 55 Mbps, las redes cableadas logran tasas de velocidad de hasta 100 Mbps. (ConceptoABC, 2022)

Simulación y emulación de redes

La simulación y la emulación son dos formas de virtualización, y se aplica en el contexto de las redes de computadoras, describiendo sus características distintivas, ventajas y desventajas. Se investiga los principales simuladores y emuladores de redes, comparando las herramientas Packet Tracer y GNS3. (Gómez Carmona, 2017)

Diferencia entre emulador y simulador

La diferencia entre un emulador es que este trata de modelar una forma adecuada al dispositivo de tal manera que funcione como si se usara el dispositivo original, al contrario, un simulador funciona como su nombre lo indica “simula”, lo cual verifica el comportamiento de un programa. (Smith, 2014)

Simulación de las redes computacionales

La simulación es el estudio cuantitativo de un sistema real, en el cual se trabaja con un modelo simplificado que atrae los elementos, sucesos y magnitudes del modelo original. En este modelo realiza una representación numérica de la evaluación del sistema, durante un período de tiempo, en el cual se calcula varios parámetros representativos a partir de los datos recogidos, usando un programa de simulación. (Gómez Carmona, 2017, pág. 9)

Un simulador es una herramienta de software que quiere desarrollarse por una aplicación de software o dispositivo de hardware por medio de la imitación de sus funcionalidades. (Gómez Carmona, 2017)

La emulación de redes computacionales

La emulación es una copia del interior de un dispositivo, esto hace referencia al procesador, juego de instrucciones y periféricos hardware. El emulador configurara de una forma precisa el dispositivo de tal manera que funcionamiento sea idéntico a un aparato. Para realizar la emulación se debe tomar en cuenta el código de la maquina original para el desarrollo desde el emulador, con esto lograr interactuar con componente y aplicaciones reales dando referencia aun red real. Cabe mencionar que al emular esto no será perfecto debido ah que no emula al 100% en los aspectos de microprocesador o elementos adjuntos al sistema,

por lo que la emulación no es semejante al desarrollo de los dispositivos reales. (Gómez Carmona, 2017, pág. 10)

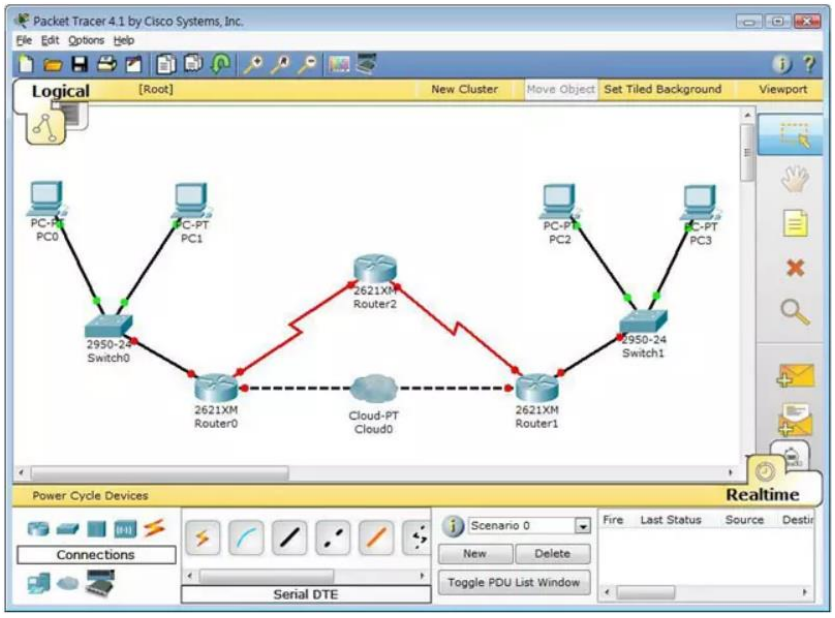
Existen varios simuladores y emuladores de red que son utilizados para la creación de topologías de redes:

a. Cisco Packet Tracer

Este simulador de redes es uno de los más completos, donde se realizan pruebas con sus propios dispositivos es decir los routers, switchs, hubs y servidores, los cuales permiten realizar todo tipo de virtualizaciones de redes, adicional a eso este simulador es usado por varios usuarios para el estudio y la obtención de un certificado en CCNA de cisco. (Velasco, 2014)

Figura 16

Simulación de topología de red



Nota. La figura presenta se refleja la una simulación de redes creada en Cisco packet tracer. Tomando de: (Velasco, 2014)

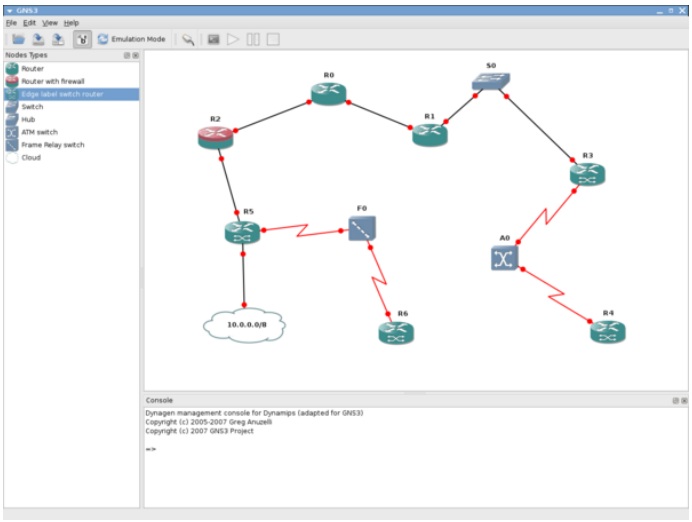
b. GNS3

Este simulador conocido como GNS3 o Graphial Network Simulator permite generar redes de código abierto, el mismo que es diseñado para simular redes complejas de la forma más parecida a un ambiente real. En GNS3 se utiliza módulos como Dynamips, Virtual Box y Qemu los cuales ayudan a obtener experiencias más reales posibles utilizando sus distintos dispositivos que contiene el mismo, adicional a eso es una herramienta multiplataforma con usuarios adaptados para Windows, Linux y Mac. (Velasco, 2014)

GNS3 consta de dos componentes de software. Software GNS3 todo en uno (GUI) y Servidor/Máquina Virtual GNS3. Esta es la interfaz gráfica de usuario (GUI) de GNS3 y la parte de software necesaria para su operación. Este paquete instala el software todo en uno en su PC local (Windows, MAC, Linux), con lo cual puede crear sus topologías utilizando el software incluido (Telectrónika, 2018).

Figura 17

Diagrama de una topología de red



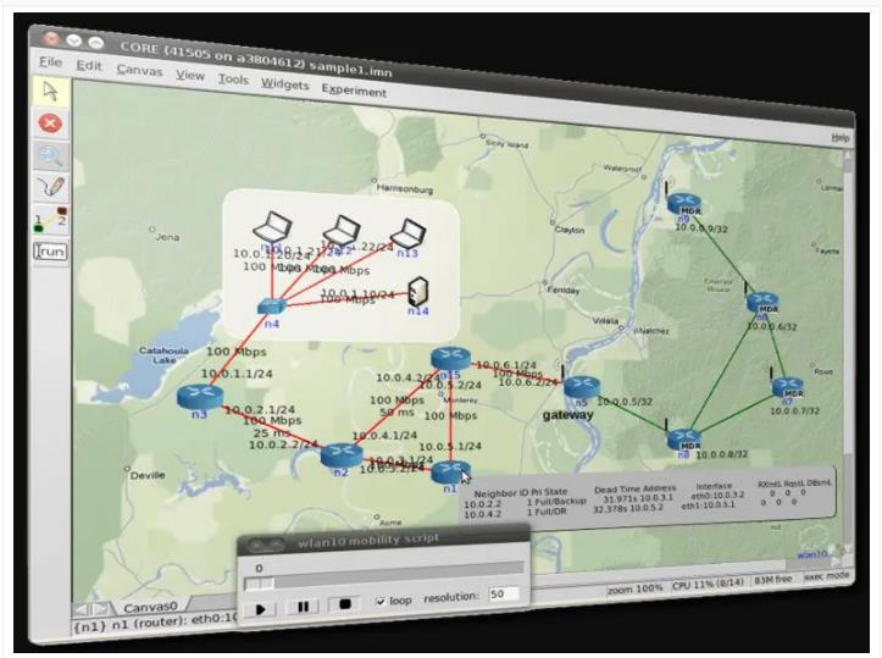
Nota. En la siguiente figura se visualiza la topología de red con la utilización de routers mikrotik, cloud, y conectores, los mismos que permiten desarrollar la simulación de redes en GNS3. Tomado de: (Velasco, 2014)

c. Common open research emulator (core)

CORE, es una herramienta que accede a emular las redes informáticas en una o varias máquinas, esta herramienta hace posible crear distintos escenarios y configurar diferentes dispositivos de red, por lo que nos permite conectar a escenarios reales. Esta herramienta contiene una interfaz gráfica de usuario o GUI la misma que nos permite diseñar topologías de red y configurar los equipos activos como routers, switchs, Access points, etc. (Julio, 2021)

Figura 18

Emulador Common open research emulator



Nota. La figura presenta como funciona el emulador Core el mismo que permite realizar topología de red informáticas para distintos escenarios. Tomado de: (Julio, 2021)

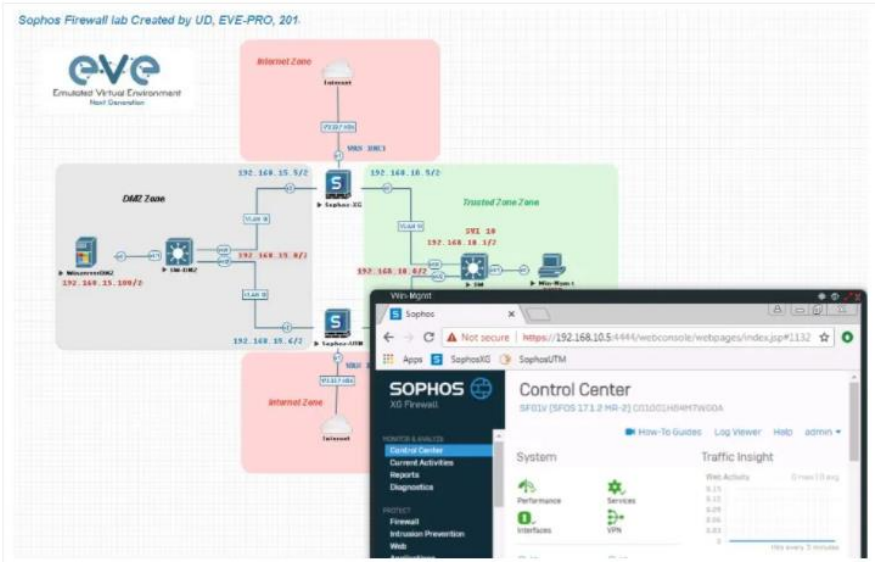
d. Eve-ng

El eve-ng es el primer software de emulación de red multiproveedor sin usuarios que accedan a profesionales en el área de redes conjunto con la seguridad en el mundo de las redes (Pomar, 2020). La gran diferencia de esta plataforma en otras es que

los laboratorios se pueden realizar a través de un simple navegador, adicional a eso el eve-ng dispone de una sencilla imagen. OVA, la cual se puede ejecutar en cualquier sistema operativo como lo es Windows, Linux o MacOS. (Julio, 2021)

Figura 19

Topologías del emulador EVE-NG



Nota. En la figura se observa la funcionalidad que realiza el even-ng para la creación de topologías de red, creada en un sistema operativo. Tomado de: (Julio, 2021)

Virtualización

La virtualización es un concepto del que ha estado en desarrollo durante varios años, pero parece que se ha encontrado la forma eficiente de ser explicada en pocas palabras por lo que consiste en instalar sistemas operativos de forma virtual con una base llamada anfitrión o host, por lo cual consiste en que se puede cargar diversos sistemas operativos los mismo que son aprovechados al máximo en hardware del equipo y la disponibilidad del host, conexión de red, puertos USB, unidades de almacenamiento y la capacidad de los procesadores. Al realizar la instalación de un sistema operativo en la maquina principal no surge ningún problema debido a que esto permite que el arranque de Windows mejore. (Limones, 2021)

Se asigna a cada máquina virtuales recursos de la maquina física es decir memoria RAM, procesadores, almacenamiento), con esto se puede instalar el sistema operativo a utilizarse como lo es Windows, Linux, Unix, Solaris, Zero Shell, etc.). Existen dos componentes fundamentales que permiten comprender el funcionamiento de la virtualización. (Limones, 2021)

Funcionamiento de la virtualización

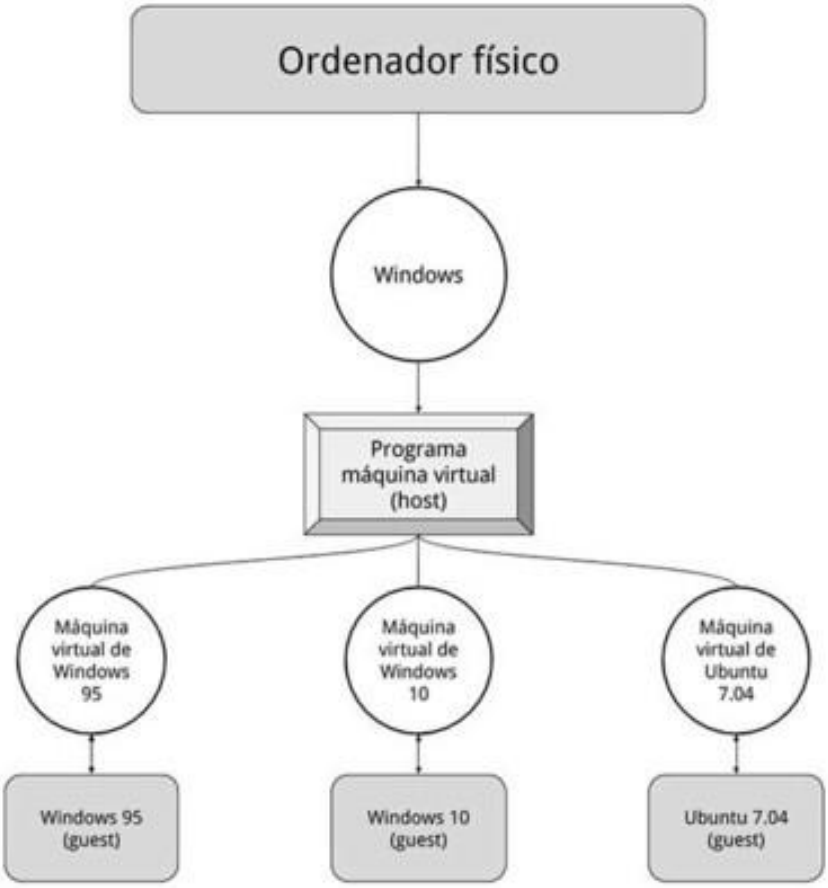
El software llamado hipervisor es el cual separa los recursos físicos del entorno virtual, además de eso este software tiene la capacidad de controlar los sistemas operativos en una computadora o también pueden instalarse en el hardware como un servidor. Los hipervisores adquieren recursos físicos y luego los divide a los entornos virtuales para que puedan ser usados, esto permite que la funcionalidad trabaje tanto en la parte virtual como en la pate física. (Red Hat, 2018)

Máquina virtual

Simulación creada por software para la implantación de sistemas operativos o aplicaciones, las mismas que adquieren recursos de la maquina física (Limones, 2021), por lo que al emular una computadora por completo se debe ejecutar el entorno de la aplicación basada en Java o basada en .NET Framework. La utilidad que tienen las máquinas virtuales es encender varios sistemas operativos a la vez, por lo que se adquiere los componentes virtuales reservados para la virtualización por lo que se usa recursos de la maquina física, adicional a eso también se debe tener una imagen ISO en vez deun lector Cd para la instalación de sistemas operativos. (Xataka, 2020)

Figura 20

Diagrama del funcionamiento de la máquina virtual



Nota. La figura muestra la emulación y la ejecución que realiza la máquina virtual con los sistemas operativos. Tomado de: (Ramírez, Maquina Virtual , 2020)

El uso de máquinas virtuales

- Permite compilar e implementar aplicaciones en la nube.
- Creación de copias de seguridad del sistema operativo.
- Acceder a datos infectados por virus o ejecutar una versión anterior de una aplicación con la instalación de un sistema operativo anterior.

- Ejecutar software o aplicaciones en sistemas operativos para los que no se habían diseñado inicialmente (Microsoft, 2022).
-

Máquinas virtuales de sistema

Las máquinas virtuales de sistema, son conocidas como máquinas virtuales de hardware que brindan el acceso a la maquina física donde se emplea varias máquinas virtuales, donde cada una de ellas desarrolla un sistema operativo. La capa que permite la virtualización se llama monitor virtual o hypervisor, este monitor se puede ejecutar directamente en el hardware o sobre el sistema operativo. (Microsoft, 2022)

Máquinas virtuales de proceso

Una máquina virtual de proceso o también conocida como máquina virtual de aplicación, por lo que esto se ejecuta con normalidad dentro de un sistema operativo donde solo soporta un solo proceso. El objetivo de estas máquinas es proporcionar un entorno de ejecución independiente al hardware y al sistema operativo, por lo que los detalles subyacentes permiten que el programa ejecute siempre sobre cualquier plataforma. (Microsoft, 2022)

Entre las máquinas virtuales más utilizadas están:

- Oracle VM VirtualBox
- VMware Workstation

a. Oracle VM VirtualBox

Es un software de virtualización con versiones x86/amd64, es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización. Por medio de este software es posible instalar sistemas operativos adicionales, conocidos como “sistemas invitados”, dentro de otro sistema operativo “anfitrión”, cada uno con su propio ambiente virtual. (Microsoft, 2022)

b. VMware Workstation

VMware Inc., (VM de Virtual Machine) filial de EMC Corporation que proporciona la mayor parte del software de virtualización disponible para ordenadores compatibles X86. Entre este software se incluyen VMware Workstation, y los gratuitos VMware Server y VMware Player. El software de VMware puede funcionar en Windows, Linux, y en la plataforma Mac OS X que corre en procesadores INTEL, bajo el nombre de VMware Fusion. (Microsoft, 2022)

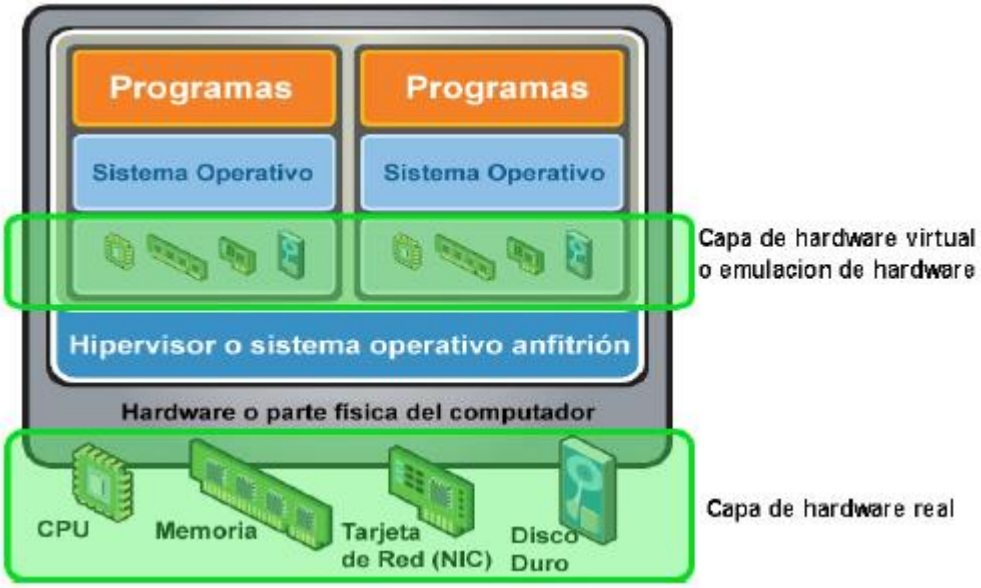
Cuando se ejecuta el programa, proporciona un ambiente de ejecución similar a todos los efectos a un computador físico (excepto en el puro acceso físico al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc. VMware es similar a su homólogo Virtual PC, aunque existen diferencias entre ambos que afectan a la forma en la que el software interactúa con el sistema físico. El rendimiento del sistema virtual varía dependiendo de las características del sistema físico en el que se ejecute, y de los recursos virtuales (CPU, RAM, etc.) asignados al sistema virtual. (Microsoft, 2022)

Hipervisores de la virtualización

Es el encargado de la creación de una capa virtual a la cual se le asigna dinámicamente los recursos necesarios en cada máquina virtual. Es importante que el funcionamiento de las máquinas virtuales sea el correcto tanto en el almacenamiento como en los componentes de red y así adquirir buenos resultados. (Limones, 2021)

Figura 21

Virtualización en software o hardware



Nota. En la figura se observa la capa software o hipervisor atrae recursos de la computadora física los mismos que son ejecutados en la capa donde se puede hallar el hardware (host) y el sistema operativo de una máquina virtual (guest). Tomado de: (Gracia, 2012)

Tipos de virtualización

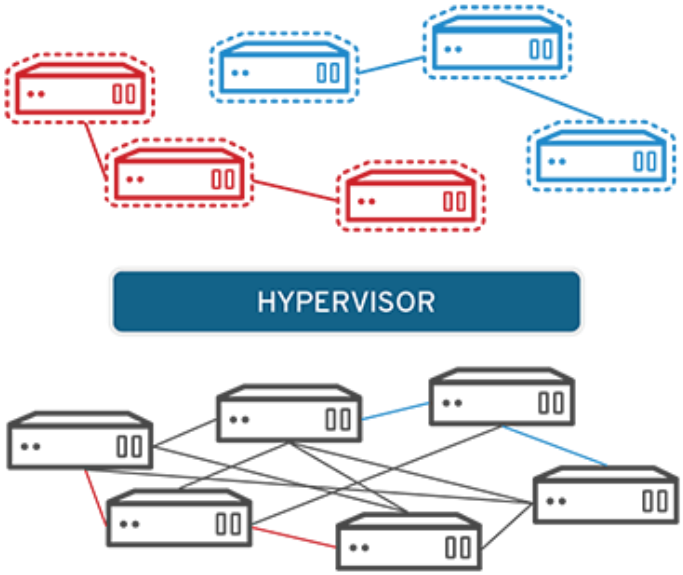
La virtualización está clasificada en los siguientes parámetros:

a. Virtualización de red.

La virtualización de funciones de red (NFV) separa las funciones clave de una red, como lo son los servicios de directorio, el uso compartido de archivos y la configuración de IP, para ser repartidas entre los entornos. La virtualización de redes, se empela con frecuencia en el ámbito de las telecomunicaciones, reduciendo así la cantidad de elementos físicos como son los conmutadores, enrutadores, servidores, cables y centrales, que se desarrolla para la creación de varias redes independientes. (Red Hat, 2018)

Figura 22

Diagrama de la virtualización de redes



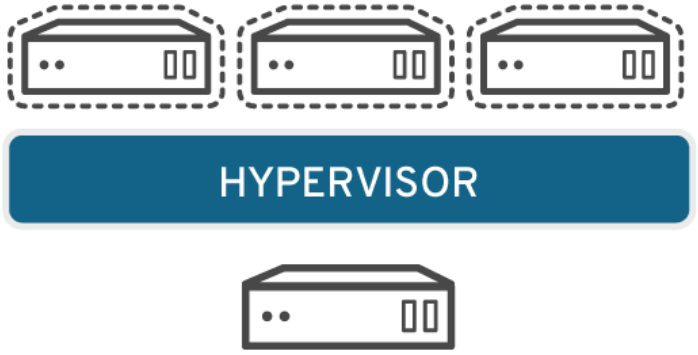
Nota. En la figura presente se visualiza cómo funciona el hipervisor de virtualización de redes. Tomado de: (Red Hat, 2018)

b. Virtualización de servidor.

Los servidores son ordenadores diseñados para procesar un gran volumen de tareas específicas de forma muy eficiente para que otros ordenadores portátiles o de escritorio, puedan ejecutar otros procesos, que implican dividir sus elementos que puedan ser usados para realizar varias tareas, permite ejecutar más funciones específicas. (Red Hat, 2018)

Figura 23

Hipervisor del servidor



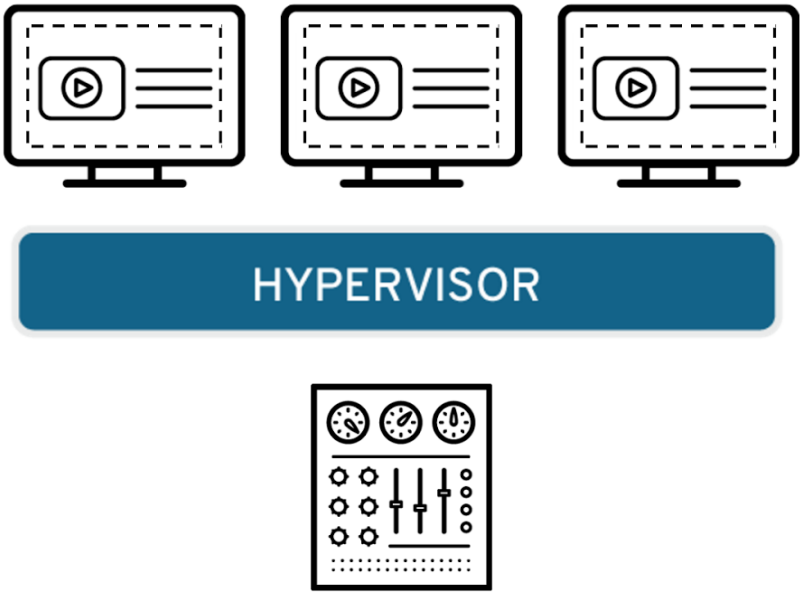
Nota. La figura presente se muestra cómo trabaja con varias tareas, donde sus elementos son usados correctamente. Tomado de: (Red Hat, 2018)

c. Virtualización de escritorio.

La virtualización de escritorios es la cual permite implementar muchos de estos en una sola máquina, sin embargo, la posibilidad de que un administrador central implementen entornos simulados de escritorio en cientos de máquinas físicas al mismo tiempo. A diferencia de los entornos de escritorio tradicionales que se instalan, configuran y actualizan físicamente en cada máquina, la virtualización de escritorios permite que los administradores realicen múltiples configuraciones, actualizaciones y controles de seguridad en todos los escritorios virtuales. (Red Hat, 2018)

Figura 24

Diagrama de la virtualización de escritorio



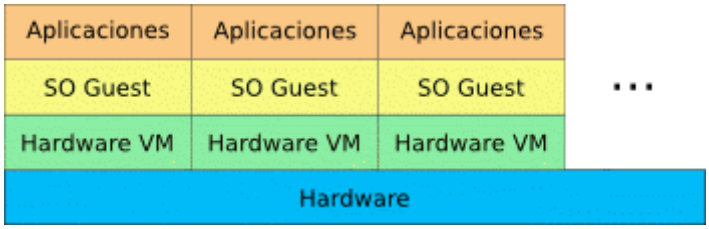
Nota. En la figura se demuestra como este tipo de hipervisor de escritorio realiza varias configuraciones y la seguridad de los escritorios virtuales. Tomado de: (Red Hat, 2018)

d. Virtualización de hardware.

Este es el tipo de virtualización más complejo de lograr. Consiste en emular, mediante máquinas virtuales, los componentes de hardware. De esta manera el sistema operativo no se ejecuta sobre el hardware real sino sobre el virtual. La gran ventaja de este enfoque es que pueden emularse distintas plataformas de hardware (por ejemplo, x86 sobre SPARC). Su principal desventaja es el alto costo de traducción de cada una de las operaciones de las máquinas virtuales a la máquina real, pudiendo obtenerse un rendimiento de 100 a 1000 veces menor. (Smaldone, 2008)

Figura 25

Virtualización de hardware



Nota. La figura presente se observa como maneja este hipervisor al implementar las máquinas virtuales. Tomado de: (Smaldone, 2008)

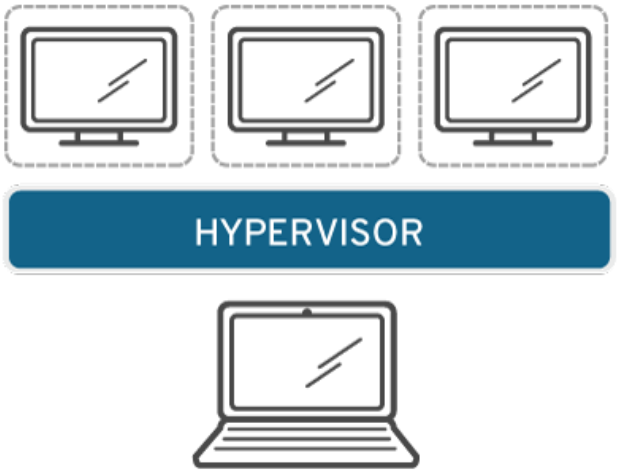
e. Virtualización de software.

Los sistemas operativos se virtualizan en el kernel, es decir, en sus administradores centrales de tareas. Es una manera más útil de desarrollar sus entornos de Linux y Windows, esta virtualización también nos permite ingresar más sistemas operativos:

- Reduce grandes gastos en sistemas de hardware.
- Aumenta la seguridad porque las instancias virtuales se pueden llegar a ser supervisadas y aisladas.
- Limita el tiempo que se destina a los servicios de TI, como las actualizaciones de software.

Figura 26

Diagrama del hipervisor del software



Nota. La figura muestra cómo funciona este tipo de hipervisor al momento de instalar los sistemas operativos, ya que esto ayuda a reducir recursos en hardware. Tomado de: (Red Hat, 2018)

El más usado es el virtualizador de servidor es la más utilizado, este tipo de virtualizador contiene requerimientos de uno o más servidores físicos, por lo cual el hipervisor cumple con ese propósito por lo que se menciona dos tipos de hipervisores a continuación. (Maldonado, 2019)

a. **Tipo 1:** se conectan directamente en el hardware, conocidos como Máquinas Virtuales (VMware, Microsoft y Citrix son los líderes del mercado en este aspecto).
b. **Tipo 2:** se hospedan en un sistema operativo ajeno (La KVM, Kernel based Virtual Machine de Red Hat es el producto más utilizado en este rubro) (Maldonado, 2019).

Ventajas y desventajas de la virtualización

a. Ventajas

- Se adquiere un mejor desempeño y eficiencia de los recursos y componentes de computación existentes.
- Mejora la seguridad de la máquina virtual., debido a que las máquinas virtuales están vulnerable a los ataques de malware o un glitch en el software.
- La virtualización de software es más económica, y requiere menos hardware que una máquina física.
- Las máquinas virtuales son confiables en el ámbito de recuperación ante desastres, respaldos y recuperación de capacidades (Maldonado, 2019).

b. Desventajas

- El rendimiento de las máquinas virtuales es un poco bajo que el servidor físico en el cual se instala la máquina virtual.
- Las maquinas físicas donde se realizan las máquinas virtuales es muy crítica, debido a que si presenta fallas en los componentes hardware esto podría afectar a la virtualización. (Limones, 2021)

Sistema operativo

El sistema operativo es un conjunto de programas que acceden a manejar la memoria RAM, discos, y los diferentes periféricos del ordenador, como lo es el teclado, mouse, impresora, tarjeta de red, etc. Cada periférico requiere de un drive o controlador que son realizados por los fabricantes de cada dispositivo. Existen varios sistemas operativos como lo es Windows. Linux, Mac OS, o también los que contiene los teléfonos o tablets los cuales son Android y iOS. (Dessallar inclusion, 2017)

Funcionamiento del sistema operativo

- Es el encargado de supervisar la memoria de acceso aleatorio y ejecutar las aplicaciones, designando los recursos necesarios (concepto, 2013-2022).
- Administra al CPU con un algoritmo de programación.
- Direccionar las entradas y salidas de datos a través de drivers por medio de los periféricos de entrada o salida.
- Administrar los archivos.

Características de un sistema operativo

- Es el intermediario entre el usuario y el hardware.
- Es indispensable para el funcionamiento de todos los computadores, tabletas y teléfonos móviles.
- Contiene seguridad y protege a los programas y archivos del ordenador.
- Permite administrar de manera eficiente los recursos del ordenador.
- Permite interactuar con varios dispositivos.
- Es progresivo, ya que existen constantemente nuevas versiones que se actualizan y adaptan a las necesidades del usuario (concepto, 2013-2022).

Tipos de sistema operativo

a. **Según el usuario pueden ser:** sistema operativo que permite que varios usuarios ejecuten simultáneamente sus programas; o monousuario, sistema operativo que solamente permite ejecutar los programas de un usuario a la vez.
b. **Según la gestión de tareas pueden ser:** sistema operativo que permite ejecutar un proceso a la vez; o multitarea, sistema operativo que puede realziar varios procesos al mismo tiempo.

c. **Según la gestión de recursos pueden ser:** sistema operativo que permite utilizar los recursos de un solo ordenador; o distribuido, sistema operativo que permite llevar a cabo los procesos de más de un ordenador al mismo tiempo (concepto, 2013-2022).}

A continuación, observaremos algunos de los sistemas operativos que se maneja en la actualidad:

- **Microsoft Windows.** El sistema operativo más utilizado en el mundo, en donde toda la información presentada es gráfica, permite realizar varias aplicaciones a la vez y contiene una forma fácil de realizar más rápido las tareas, al ser guiado paso a paso. Su característica de masivo hace que permanentemente sea repensado en función de hacerlo más intuitivo.
- **Mac OS X**. Sistema operativo de Apple, integrado totalmente con las plataformas de Apple como iCloud, iMessage, así como con las redes sociales Twitter y Facebook. Contiene el navegador propio de Apple, Safari, y se propone como competitivo a Windows en diversas áreas.
- **GNU/Linux**. Software libre más importante, que soporta el trabajo con más de un microprocesador y permite que toda la memoria pueda utilizarse como caché.
- **UNIX**. Sistema operativo multitarea, enfocado en la comunicación por correos electrónicos y en la conexión a redes y su acceso.
- **Solaris**. Sistema operativo certificado como una versión de UNIX, caracterizado por ser muy adecuado para el procedimiento simétrico por soportar un gran número de CPUs (Ejemplos, 2022).

Sistemas operativos de Red

Los NOS (Network Operating System) o sistemas operativos de red, un software utilizado para controlar la interconexión entre dos o varias computadoras en red, esto permite

que los usuarios interconectados para así poder distribuir información como archivos y programas entre el software y hardware. Las funciones de un sistema operativo de red incluyen paquetes de datos propios del sistema operativo del CP o servidores, lo cual funciona de forma integrada en el SO del ordenador. (ConceptoABC, 2019)

Figura 27

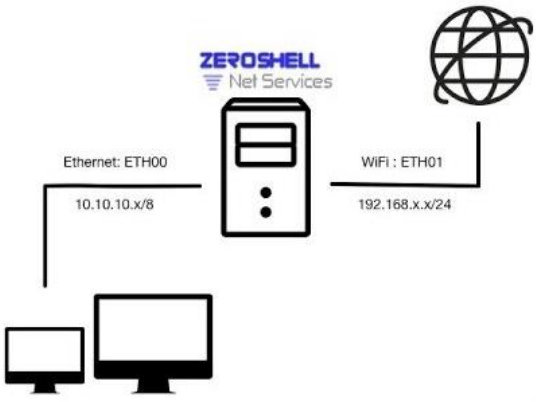
Diagrama del funcionamiento del S.O

Nota. En la figura se muestra como maneja el sistema operativo de red al tener interconexión entre varios dispositivos. Tomado de: (ConceptoABC, 2019)

Sistema operativo Zeroshell

Figura 28

Interfaz de la funcionalidad de Zeroshell



Nota. La figura se visualiza como trabaja el zeroshell al generar servidores de red sobre una máquina virtual. Tomado de: (Fulvio, 2018)

Zeroshell es una distribución basada en Linux dedicada a la implementación de dispositivos de enrutador y firewall completamente administrables a través de una interfaz web. Zeroshell está disponible para plataformas x86 / x86-64 y dispositivos basados en ARM como Raspberry Pi. Algunas características avanzadas de Zeroshell son: (Fulvio, 2018)

Equilibrio de carga y conmutación por error de varias conexiones a Internet, VPN de sitio a sitio y VPN de host a sitio, Acceso al portal cautivo para Internet Hotspot, Reglas de firewall que utilizan la inspección profunda de paquetes (filtros de capa 7 y nDPI), Calidad de los servicios y modelado del tráfico mediante la inspección profunda de paquetes, Proxy web transparente con antivirus y listas negras de URL, Autenticación y contabilidad RADIUS, Gestión de puentes y VLAN, Punto de acceso inalámbrico con soporte para múltiples SSID, Conexiones móviles, Seguimiento y registro de las conexiones de red. (Fulvio, 2018)

Zeroshell es una distribución Linux para servidores y dispositivos integrados destinados a proporcionar los servicios de red principal de una LAN, administrándose desde una interfaz web muy sencilla de utilizar.

Sistema operativo de RouterOS Mikrotik.

MikroTik RouterOS funciona como un Sistema Operativo para convertir un PC o una placa Mikotik RouterBOARD en un router dedicado. La ventaja fundamental que ofrece MikroTik es que va a funcionar exactamente igual que un router propietario, pero a un coste significativamente inferior. Además, es un software que ofrece gran flexibilidad para su configuración, con amplias posibilidades de actualización y, tal y como te estoy mostrando en estos tutoriales, te permite un mantenimiento fácil gracias a que tú eres el administrador principal. (Anrrango, 2014)

Figura 29

Dispositivo RouterOs MikroTik

Nota. En la figura se demuestra los dispositivos MikroTik para la configuración de redes. Tomado de: (Tezé, 2018)

Características del RouterOS MikroTik

Una característica a destacar de MikroTik es su sistema operativo o RouterOS; es un sistema operativo stand-alone basado en el kernel de Linux2.6, de gran potencia y capaz de ejecutar cualquier configuración de red, las configuraciones más populares son (Diego, 2018):

1. Firewall
2. Routing
3. Forwarding
4. MPLS
5. VPN
6. Wireless
7. HotSpot
8. Calidad de Servicio (QoS)
9. Web Proxy

Tecnologías y protocolos de red

- **DHCP.**

DHCP es un Protocolo de configuración dinámica de host, es usado la mayor parte por routers, domésticos o profesionales de una forma predeterminada para cualquier cliente por cableado o WiFi esto se desarrolla para adquirir una dirección ip por DHCP. Este tipo de protocolo de red contiene uno o varios cliente- servidor, por lo que genera de manera automática y dinámica las direcciones IP (Luz S. , 2022).

- **DNS.**

DNS (Domain Name System) un protocolo de red que funciona como resolución de nombres de dominio o lo que más comúnmente se conoce como direcciones IP. Este tipo de protocolo cumple la función de convertir un nombre de servidor a una dirección IP (Cloudflare, 2019). De acuerdo a lo definido los nameservers de dominio son el nombre de dominio tiene una zona DNS que lo vincula a los servidores DNS (Gustavo, 2022).

- **NTP.**

Se denomina (NTP) al protocolo de tiempo de red o (Network Time Protocol) y son los resultados del trabajo de desarrollo realizados por David L. Mills, quien es profesor de la Universidad de Delaware (Estados Unidos). Que forma parte de la familia de protocolos de Internet. Los NTP son un protocolo que tienen una función principal para sincronizar varios relojes de red de los sistemas informáticos usando un conjunto de clientes y servidores repartidos, con una precisión del orden de nanosegundos. Además, contienen indicaciones para especificar la precisión y las posibles fuentes de error del reloj del sistema local, así como las propiedades del reloj de referencia. (Digital Guide IONOS, 2019)

No obstante, también llamados enrutamiento de paquetes en redes con latencia variable. Como predecesores, se hacen menciones al mensaje ICMP Timestamp y al Time

Protocol, ya que sus funciones fueron incluidas en el Network Time Protocol. (Digital Guide IONOS, 2019)

- **Firewall.**

Un firewall o también llamado cortafuegos, es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente. Es decir, deciden si permiten o bloquean el tráfico específico en función de un conjunto definido de reglas de seguridad. Con esto quiero decir que es un sistema cuyas funciones es prevenir y proteger a vuestra red privada de varios intrusos o ataques de otras redes; en efecto bloqueándoles en su totalidad el acceso hacia la red. (Cisco, 2019)

Un firewall es un dispositivo que está formado por hardware o un software que nos permite gestionar y filtrar la totalidad del tráfico entre dos redes u ordenadores de una misma red. Si el tráfico de la red entrante o saliente cumple con una serie de reglas que vosotros podéis especificar, es probable que pueden acceder o salir de vuestra red u ordenador sin restricción alguna. Sin embargo, en caso de no cumplir las reglas el tráfico entrante o saliente será bloqueado el usuario que está perjudicando a la red. Por lo tanto, a partir de lo expuesto podemos comprobar que con un firewall excelentemente configurado podemos evitar intrusiones o malicias no deseadas en nuestra red y ordenador, por otra parte, también podemos bloquear cierto tipo de tráfico saliente de vuestra red. (Carles, 2013)

- **VLAN.**

Las VLAN o también llamadas Virtual LAN**,** permite crear redes lógicamente independientes dentro de la misma red física, utilizando los switches gestionables que soporten VLANs para segmentar adecuadamente la red. Es muy importante que los routers que se usen den soporte VLAN, caso contrario no se podra gestionar todas ni permitir o denegar la comunicación entre ellaa. (Luz S. D., 2021)

- **VPN.**

VPN son las siglas de Virtual Private Network*,* red privada virtual, la palabra clave aquí es virtual, pues es esta propiedad la que genera la necesidad de la VPN en sí, así como la que permite a las conexiones VPN ofrecerte los múltiples usos como conectarse a Internet, tu móvil, PC, televisión y demás dispositivos generalmente se comunican con el router o módem que conecta tu casa con tu proveedor de Internet, ya sea mediante cable o inalámbricamente. Los componentes son distintos si estás usando la conexión de datos de tu móvil (que incluye su propio módem y habla con la antena de telefonía) pero la esencia es la misma: tu dispositivo se conecta a otro, que le conecta a Internet. (Ramírez, Xataka, 2021)

- **RADIUS.**

Los servidores RADIUS son ampliamente utilizados por muchas instituciones que proporcionan conectividad WiFi con autenticación WPA2/WPA3-Enterprise, es decir, una autenticación donde tendremos un nombre de usuario/contraseña o certificado digital para autenticarnos en la red inalámbrica. También es ampliamente usado por los operadores para el acceso de Internet, por los servicios de VPN para autenticar de forma fácil y rápida a los diferentes clientes VPN con nombre de usuario/contraseña, e incluso para la autenticación por Ethernet usando el estándar 802.1X. (Luz S. , 2021)

- **LDAP.**

Con relación a ‘’LDAP’’ son las siglas de Protocolo Ligero de Acceso a Directorio, o también llamadas en inglés ‘’Lightweight Directory Access Protocol’’. Se denomina al conjunto de protocolos de licencias abiertas que son utilizados para acceder o ingresar a la información que está almacenada o guardada de forma centralizada en una red. Este tipo de protocolo se utilizan a nivel de aplicación para acceder y conceder a los servicios de directorio remoto. Un directorio remoto es un conjunto de uno o varios objetos que están organizados de forma jerárquica, tales como nombres, claves, direcciones y demás definiciones. Estos tipos de objetos estarán disponibles por unas series de clientes conectados mediante una red;

Normalmente es una conexión interna o LAN y proporcionarán las identidades a cada uno. Adicional tienen permisos para esos usuarios que los utilicen. (Castillo, 2019)

Las tecnologías y protocolos de red ‘’LDAP’’ está basado en el protocolo ‘’X.500’’ que esta designado para compartir directorios, y contiene esta información de forma jerarquizada. Es decir, mediante categorías para proporcionarnos una estructura intuitiva desde el punto de vista de la gestión por parte de los administradores que manejan la red. Es, por así decirlo, una guía telefónica; Dicho de otra manera, con más atributos y credenciales. En este caso y por definitiva utilizamos el término directorio para referirnos o indicar a la organización que tienen de estos objetos.

En definitiva, dichos directorios se utilizan básicamente y primordialmente para contener o almacenar información virtual de usuarios, para que otros usuarios accedan y dispongan de información acerca de los contactos que están aquí almacenados respectivamente. Pero en resumen es mucho más que esto, debido a que es capaz de comunicarse de forma remota con uno o varios directorios LDAP situados en servidores que pueden estar en el otro lado del mundo; Dando un ejemplo de un país europeo a uno latinoamericano. Por lo cual para acceder a la información disponible solamente deberían estar en red. De esta forma se crean una base de datos de información descentralizada y completamente accesible para todo tipo de usuario interconectado. (Castillo, 2019)

- **Portal Cautivo**

Un portal cautivo es una ventana que permite controlar y gestionar el acceso a redes WiFi a través de un proceso de autenticación o login. Mediante este sistema es posible recoger información sobre los usuarios a cambio de habilitar el acceso a una red WiFi de calidad. (Hotelero, 2012)

Por tanto, es una solución de las más completas del mercado, siendo su mayor ventaja la facilidad de uso, y que está basado en software libre. Una maravilla. Podemos instalarlo en cualquier equipo incluso aquellos con poca potencia. (Obasoftfp, 2015)

Hotspot o Portal Cautivo

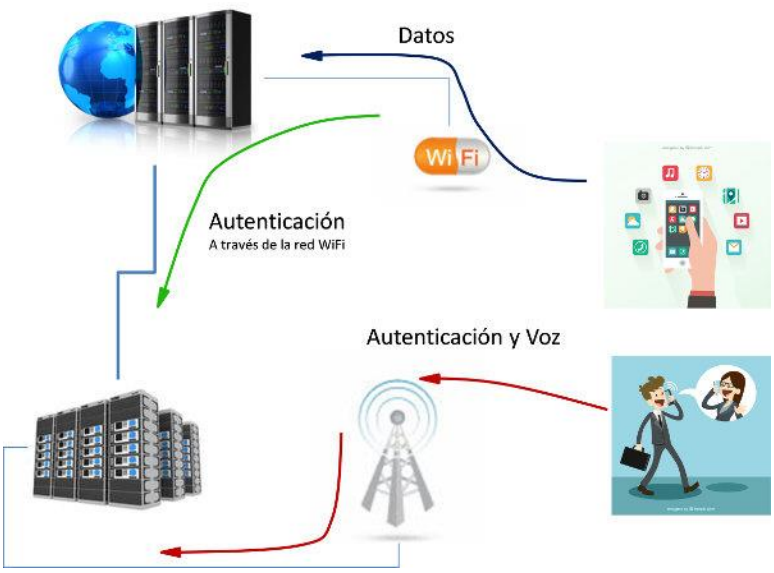
Un Hotspot o portal cautivo ofrece acceso a Internet a través de una red inalámbrica y un enrutador conectado a un proveedor de servicios de Internet. Los hotspots se encuentran en lugares públicos, como aeropuertos, bibliotecas, centros de convenciones, cafeterías, hoteles, escuelas, etcétera. Este recurso se ejecuta por medio de wifi, por lo que permite mantenerse conectado a Internet en lugares públicos. Puede brindarse de manera gratuita o cobrando una suma que depende del proveedor. (Prieto Fernández, 2018)

Por norma general, un Hotspot presenta al usuario una pantalla de bienvenida donde se tiene que hacer login con un usuario de forma gratuita, pagando o usando una cuenta temporal. Una vez realizado este pasó y en función de la configuración del Hotspot, el usuario podrá acceder a Internet.

Características del Hotspot de Mikrotik, Diferentes métodos de autenticación de clientes usando una base de datos interna en el router ó un servidor RADIUS remoto, Almacenar los usuarios en base de datos local o en el servidor RADIUS externo, Walled-garden. Acceso a algunas páginas sin necesidad de autenticación, Gestión de ancho de banda por perfiles o usuarios individuales, Modificación de la pantalla principal de Login, donde podremos poner los datos que necesitemos, Cambio automático de la dirección IP de los clientes para el correcto funcionamiento. (Prieto Fernández, 2018)

Figura 30

Esquema de la conexión del Hotspot



Nota. La figura presenta muestra un diagrama de como la conexión del hotspot opera en varios dispositivos brindando WiFi para el traspaso de información de los usuarios. Tomado de: (tecnologia wireless, 2016)

Funcionamiento del Hotspot

Este dispositivo y/o aparato está conectado a una red o varias redes de internet y generan un campo de radio de wifi de una probabilidad de unos 15 metros al rededor. Dicho de otra manera, que todos los dispositivos que se encuentren dentro o alrededor de esta distancia no obstante podrán tener acceso a internet o la navegación con tan solo conectarse al Hotspot wifi de forma inalámbrica. Con la calidad y el rendimiento que esta provea.

Es decir que no tendrán que configurar ni conectar un montón de cables para establecer una conexión a internet. En la actualidad; existen uno o varios dispositivos Wi-Fis que cuentan con un mayor alcance, calidad, rendimiento y eficiencia debido a que poseen un mayor número de antenas, por lo cual esto no serían necesario quedarse muy cerca de estos dispositivos para que así puedan acceder al servicio de internet ilimitado de forma inalámbrica**.**

Incluso pueden comprar uno o varios dispositivos y/o apartados personales; Siendo así llevarlo contigo a donde quieran para que de esta forma puedan conectarse a internet desde casi cualquier sitio o lugar de trabajo y estudio. Adicionalmente también se pueden crear un punto de acceso wifi desde el pc para compartir internet con salida a otros dispositivos cercanos. (miracomosehace, 2020)

Tipos de wifi Hotspot

A continuación, en este nuevo apartado te hablaran con lujo de detalle sobre los tipos de puntos de acceso que existen en la actualidad y los cuales están siendo mayormente utilizados y configurados por los usuarios. En algunos casos te explicaremos cómo configurarlos, modificarlos y editarlos para que puedan utilizarlos sin ningún problemas o tipo de restricciones que eventualmente se suelen presentar en este tipo de modificaciones.

a. Hotspot gratis

Este tipo de dispositivos y/o aparatos; Habitualmente no es completamente gratuito**,** ya que para tener acceso tendrás que estar solicitando algún tipo de servicio como un alojamiento en un hotel o solicitando algún tipo de comida en algún restaurante. Por lo cual, es un servicio semi pago. En definitiva, el acceso estará garantizado siempre y cuando consumas un servicio en específico en algún puesto de ventas de productos.

En resumen, en algunas ocasiones tendremos que ingresar nuestro correo, número telefónico o algunos de los datos de nuestra tarjeta de crédito para poder acceder a la conexión que nos ofrece este dispositivo y así poder enlazarnos con la red de hotspot. (miracomosehace, 2020)

b. Hotspot portátil

En la actualidad existen varios y diferentes dispositivos que podemos adquirir en cualquier tienda, centro comercial y bodega de artefactos electrónicos cuyas funciones esa servir como una antena del router generando wifi que podemos tener siempre a nuestro lado para evitar y no quedarnos sin conexión a internet en donde quiera que vayamos a situarnos.

Una vez ya adquirido dicho dispositivo, simplemente deberían suscribirte a un servicio de internet de vuestra preferencia y con las características de nuestras necesidades para que este Hotspot tenga un plan de datos de calidad, eficiente y con rendimiento adecuado. De esta forma podremos estar conectados a este dispositivo en todo momento de forma inalámbrica ya sea a través de nuestro móvil, Tablet, computador o laptop. (miracomosehace, 2020)

Dispositivo móvil como Hotspot wifi

También tendrán la posibilidad de convertir nuestro móvil en un Hotspot wifi para permitir que otros dispositivos se conecten y tengan acceso a internet. Más adelante te explicaremos cómo funciona este proceso. (miracomosehace, 2020)

Para usar tu teléfono inteligente como un punto de acceso simplemente se debe seguir los siguientes pasos:

- Primero que nada, se debe ir a menú y seleccionar la opción "ajustes"
- Luego se tiene que presionar la opción "Conexiones inalámbricas"
- Una vez allí se verá una lista de opciones, entre ellas se debe seleccionar alguna que diga "puntos de acceso" o "zona wifi portátil"
- En el caso que sea la primera vez que se va a habilitar esta función, entonces se debe hacer algunos ajustes iniciales para que se pueda convertir el dispositivo móvil en una antena de wifi.

- Básicamente se tendrá que añadirle un nombre al móvil Android para diferenciarlo de los demás dispositivos. Te recomendamos colocarle un nombre que puedas recordar fácilmente.
- También tienes que añadir una nueva clave de acceso, ya que los otros dispositivos que deseen conectarse tendrán que ingresarla de forma correcta.
- Es recomendable crear una contraseña segura y fácil de recordar pero que cuente con números, letras y algunos caracteres especiales, de esta forma nos aseguraremos de que nadie pueda adivinar esta contraseña para acceder a nuestro móvil sin permiso. (miracomosehace, 2020)

Capítulo III

Desarrollo del tema

Materiales y Equipos

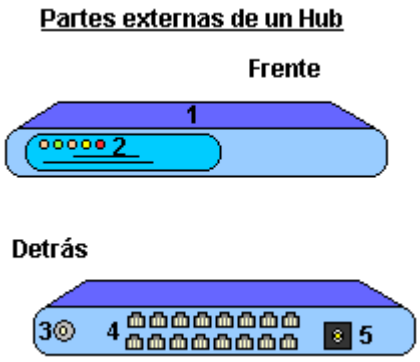
El proyecto tiene como objetivo usar materiales esenciales pero fundamentales para la creación del laboratorio virtual inalámbrico mediante la interfaz llamada portal cautivo o Hotspot. Los recursos didácticos son los medios o materiales de apoyo que se utilizan para medir los contenidos del aprendizaje significativo de nuevos o de refuerzo mediante la construcción del conocimiento por los propios estudiantes. Por definitiva logrando que los estudiantes tengan el interés por aprender y ser propios de su aprendizaje y poder mejorar el rendimiento académico. Para lo cual en el presente proyecto se detalla específicamente cada uno de los principales materiales, equipos y dispositivos que se deberían utilizar para lograr generar la red inalámbrica Hotspot en un laboratorio virtual.

Dispositivos de acceso a internet

Se realiza un análisis técnico con los diversos dispositivos que permiten la ejecución del acceso a internet por medio de las redes inalámbricas, por lo cual se desarrolló un cuadro comparativo que se presenta en la tabla 1.

Tabla 1

Cuadro comparativo de los dispositivos de red inalámbrica.

<table>
<tr><th colspan="2">Cuadro comparativo de los dispositivos de red</th></tr>
<tr><th>Características</th><th>Dispositivo</th></tr>
<tr><td colspan="2">HUB
-Permite la conexión en las estaciones de trabajo
(equipos clientes)
-Contiene varios puertos RJ 45 desde 4, 8, 16 y 32.
-Ayudan a la creación de redes con topología estrella.
-Son compatibles con los sistemas operativos de red.
-Permiten la repetición de la señal.
-Velocidad de la red LAN (10/100/100).
-Ancho de banda en enlaces de internet
(1Mbps hasta los 200Mbps)
-Permiten la conexión en cascada
(se puede conectar con otros Hubs por
medio del último puerto RJ45)
  </td></tr>
<tr><th>Características</th><th>Dispositivo</th></tr>
<tr><td colspan="2">Router inalámbrico
-Banda de 2.4 GHz y 5GHz
-Trabaja en el estándar Wifi 802.11ac
-Contiene antenas internas y externas,
con el objetivo de mantener la señal de red.
-Velocidad de 1.7 GBpd o 1700 Mbps
-Compatible con dispositivos móviles.
  </td></tr>
</table>

-Modem de 4G LTE incluido, xDLS, DOCSIS y fibra óptica. - Costo de entre 20 a 150 depende de la marca a usar.
Cuadro comparativo de los dispositivos de red
Características **Dispositivo**
ACCESS POINT **-**Velocidad de hasta 300Mbps -Frecuencia de 2.4 GHz y 5 GHz. -Estándar IEEE 802.11n, 802.11g y 802.11b -Trabaja por medio de ondas -Perfecto para crear redes WLAN. -Alcance de hasta 70m -Su costo puede llegar a ser muy alto. 
Características **Dispositivo**
REPETIDORES **-**Extiende su longitud de red más de los 500m. -Amplifica y regenera la señal. -Frecuencia de 2.4Ghz -Velocidad inalámbrica de 300Mbps. -Estandar WiFi IEEE 802.11b/g/n. 

Nota. La tabla presente muestra las especificaciones de los dispositivos de red.

Para el desarrollo de este proyecto se realizó el análisis técnico de los equipos por lo que se escogió el RouterTL-WR840N de la marca TP-LINK, debido a que contiene las

siguientes características que se indican en la tabla 2, el mismo que será configurado como un Access Point.

Tabla 2

Router Inalámbrico TP-LINK

ROUTER INALAMBRICO N	
MARCA TP-LINK	
-TL-WR840N 1 Puerto WAN de 10/100Mbps, 4 puertos LAN de10/100mbps -2 antenas fijan Omni Direccional -N 300Mbps en 2.4 GHz -Adaptador de corriente -Cable Ethernet RJ45 -Dimensiones de 7,2 * 5,0 * 1,4 (182 * 128 * 35 mm)	

Nota. La tabla presente muestra las especificaciones más relevantes del dispositivo, todo depende del tipo de proveedor donde sea adquirido. Tomado de: https://www.tp-link.com/ar/home-networking/wifi-router/tl-wr840n/ y (Intercompras, 2022)

Softwares y sistemas operativos

Se realizo el análisis investigativo de los distintos sistemas operativos de red y software de simulación de red, para el desarrollo del presente proyecto por lo que se seleccionó los siguientes a detallar en cada paso para la ejecución del portal cautivo.

Instalación del software Virtual Box

Paso 1. Virtual box es un software de virtualización, por lo que para su instalación de se requiere lo siguiente:

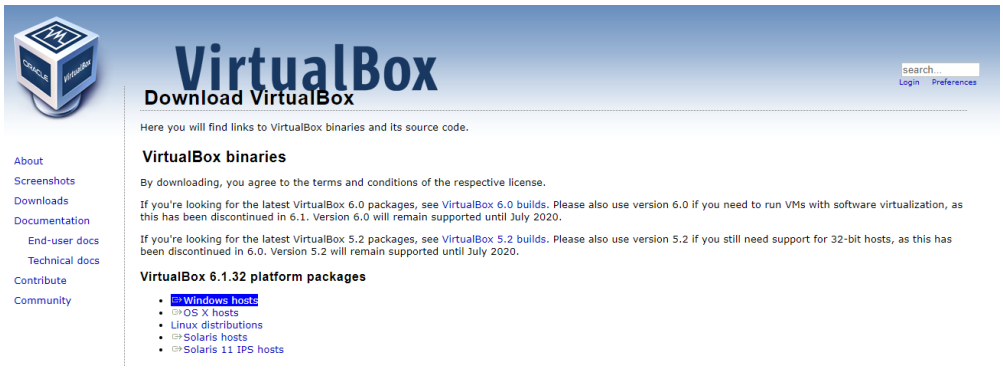
- Procesador x86 a 1GHz.

- Memoria RAM de 1GB.
- Disco Duro de 15 GB (swap incluida)

Este software será implementado dentro del sistema operativo Ubuntu por lo que para su ejecución se ingresó a la página oficial de Virtual Box, se adjunta el link de la descarga https://www.virtualbox.org/wiki/Downloads, luego se procede a seleccionar la plataforma en la figura 32 se observa la versión seleccionada la misma que es Linux, donde se empezó a descargar el software. Como consiguiente se inició ingresando los comandos correspondientes para la instalación de virtual box dentro del sistema operativo por lo que en la figura 32 se visualiza el comando" sudo dpkg -i Descargas/virtualbox-6.1_6.1.6-137129-Ubuntu-eoan_amd64.deb", luego de eso se ingresa la clave correspondiente que contiene el sistema operativo en el cual estamos instalando. En la figura 34 se muestra el comando de instalación de VirtualBox. Una vez culminado se pueda ingresar y empezar a desarrollar la máquina virtual para la configuración del sistema operativo Zersohell.

Figura 31

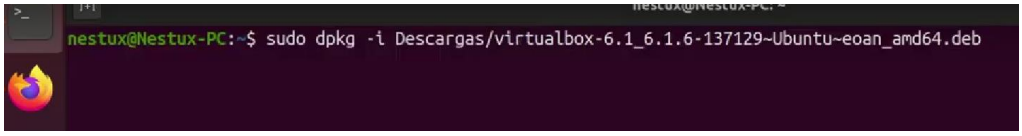
Diferentes plataformas de Virtual Box 6.1



Nota. En la figura se observa las diferentes plataformas en las cuales se puede descargar el software Virtual Box. Tomado de: https://www.virtualbox.org

Figura 32

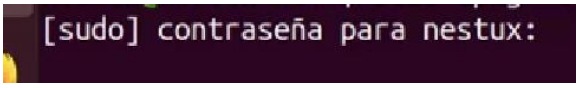
Archivo ejecutable de Virtual Box



Nota. Ingreso del comando de ejecución del archivo del software VirtualBox

Figura 33

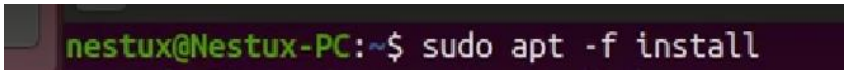
Ingreso de la contraseña



Nota. La figura muestra el ingreso de la contraseña que tiene el sistema operativo Ubuntu

Figura 34

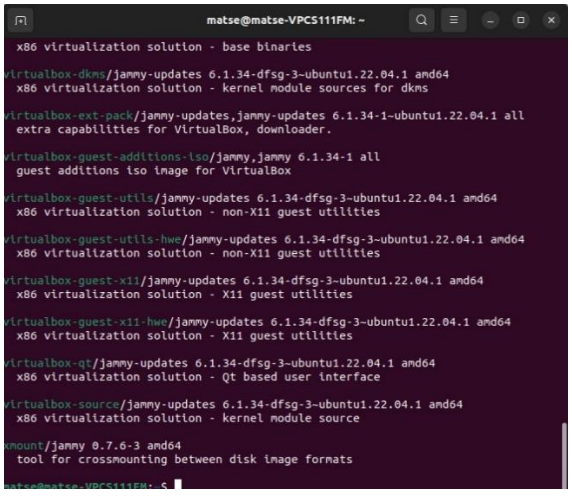
Comando de instalación de VirtualBox



Nota. En la figura se muestra el comando a ejecutar para la instalación.

Figura 35

Proceso de instalación de VirtualBox



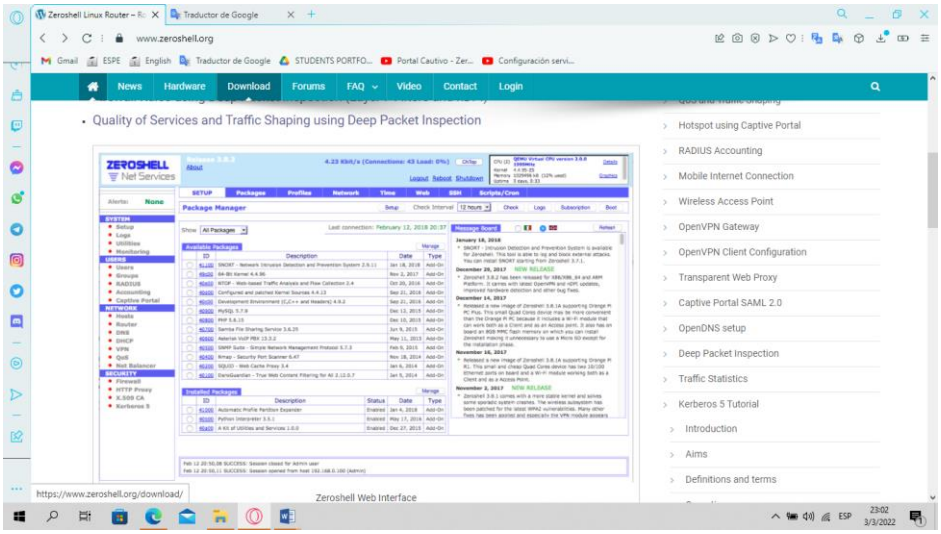
Nota. La figura presente indica el proceso de los update de la instalación del software VirtualBox.

Descarga del Sistema Operativo ZeroShell

Se procede a ingresar a la página oficial del sistema operativo ZeroShell en el siguiente enlace https://www.zeroshell.org, luego de eso se escoge la opción de Descarga, donde selecciona CEDIA, Ecuador donde una vez hecho clic se inicia con la búsqueda de la imagen ISO 3.9.5 para empezar a descargar, todo lo mencionado anteriormente se puede mostrar en las siguientes figuras 36,37 y 38.

Figura 36

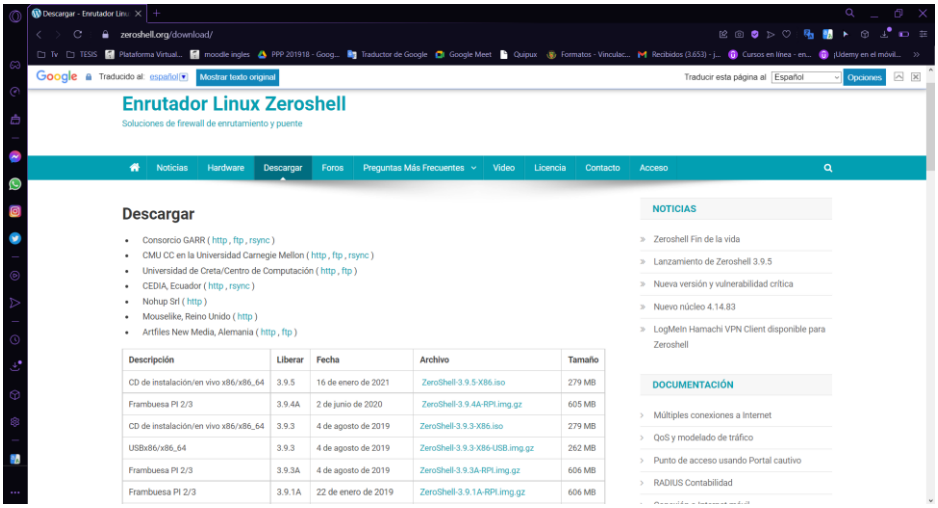
Página oficial del sistema operativo ZeroShell



Nota. En la figura se visualiza la página oficial donde descargaremos la imagen iso del sistema operativo. Tomado de: https://www.zeroshell.org

Figura 37

Versiones de la ISO del S.O ZeroShell



Nota. La figura muestra las diferentes versiones que contiene ZeroShell para la instalación de su imagen ISO. Tomado de: https://www.zeroshell.org/download/

Figura 38

Imagen ISO 3.9.5

Nota. En la figura se visualiza la imagen ISO a instalar al momento de su descarga se presenta como un archivo comprimido o WinRAR. Tomado de: http://mirror.cedia.org.ec/zeroshell/

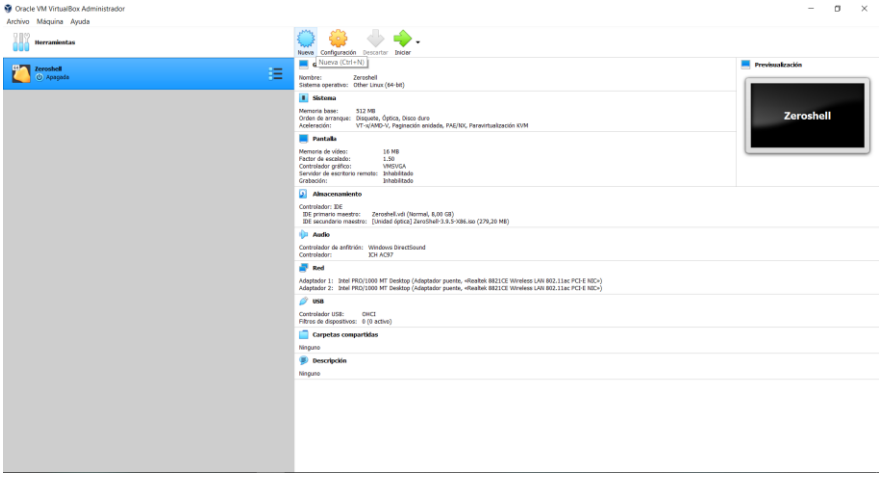
Instalación del sistema operativo ZeroShell en Virtual Box

Paso 1. Se inicia dando apertura al programa Virtual box, donde se desarrolló la máquina virtual con el sistema operativo Zero Shell por lo que se empieza realizando un clic en la opción “Nueva”, luego se visualiza varias ventanas de configuración las mismas que contiene datos diferentes como la colocación del nombre a la máquina virtual “ZeroShell”, el tipo “Linux” y la versión “Other Linux (64bits) en las siguientes figuras se indica lo mencionado 39, 40, l. A continuación, seguimos con siguientes pasos los cuales son el tamaño de la memoria RAM, la cual se deja por defecto si así lo deseamos, caso contrario lo podemos cambiar, se crea un

disco duro virtual, luego de eso seleccionamos el tipo de archivo haciendo clic en la primera opción. En las siguientes figuras 41, 42 y43 se observa lo mencionado.

Figura 39

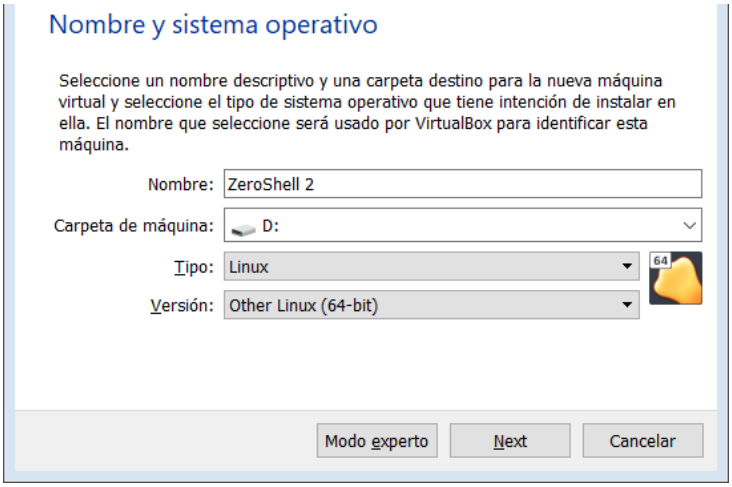
Ventana de la creación de la máquina virtual



Nota. La figura muestra la opción de crear la máquina virtual la cual contiene el Sistema operativo ZeroShell.

Figura 40

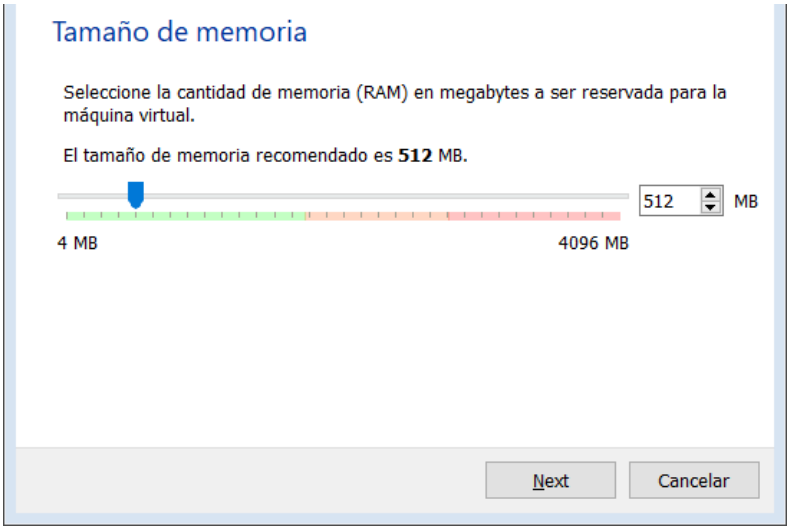
Ventana del Nombre y sistema Operativo



Nota. La figura presenta indica la colocación del nombre de la máquina virtual, la carpeta donde se guardará la información, adicional a eso se selecciona el tipo Linux y la versión Other Linux x64bits.

Figura 41

Tamaño de memoria RAM



Nota. En la figura se selecciona cantidad de memoria RAM que vamos adquirir de la maquina física para la creación de la máquina virtual.

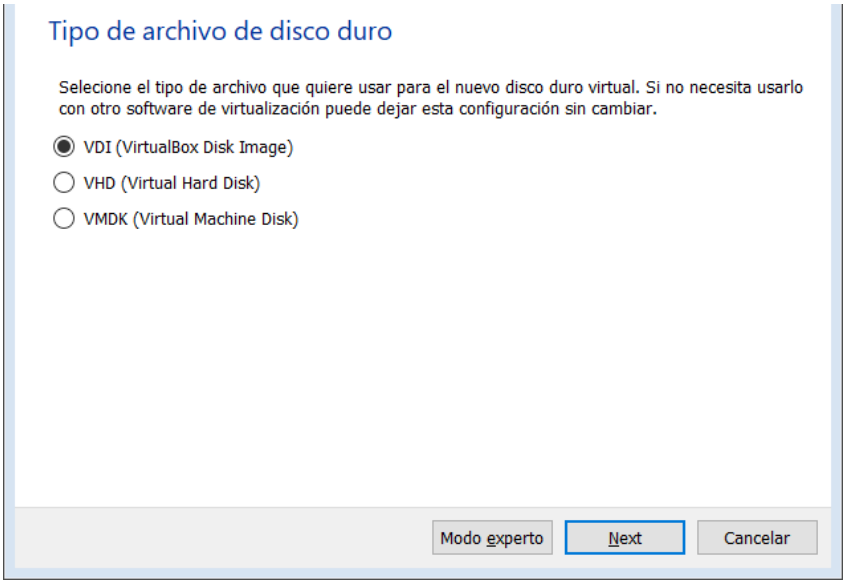
Figura 42

Creación del disco duro

Nota. En la figura presente nos indica que el tamaño del disco recomendado es 8,00 GB por lo que se selecciona la segunda opción de crear el disco.

Figura 43

Tipo de archivo de disco duro

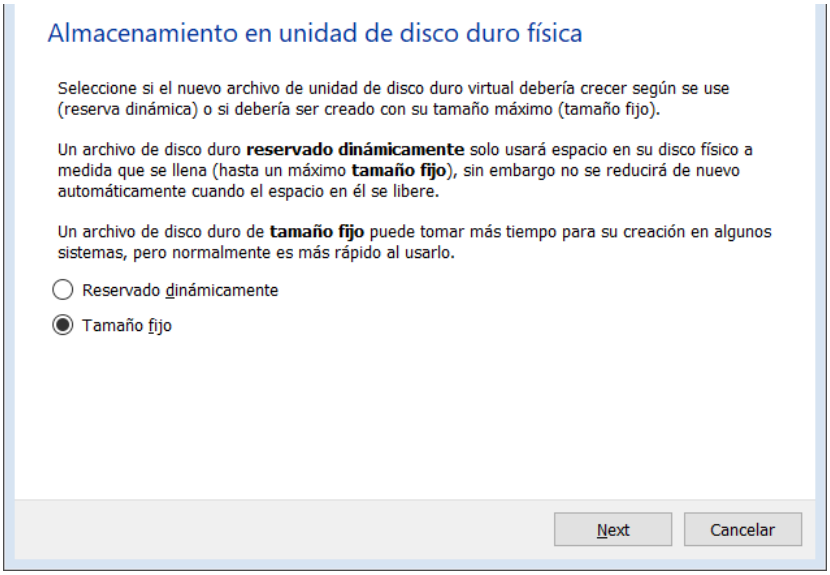


Nota. En la figura, muestra la selección del tipo de archivo que se desea usar en el nuevo disco duro virtual

Paso 2. Para la finalización la instalación de la máquina virtual se selecciona el almacenamiento con el tamaño fijo, luego de eso se procede a crear la carpeta de la máquina virtual una vez hecho todos los pasos correctos se hace clic en la opción de crear, en las siguientes figuras 44, 55 y 46 se observará todos los pasos a seguir.

Figura 44

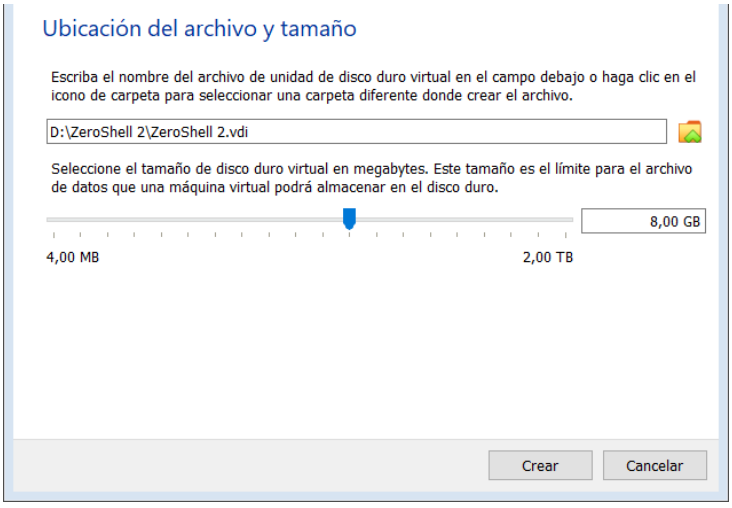
Almacenamiento en la unidad física



Nota. En la figura se observa el tamaño que va ocupar el disco duro de la maquina física con la intensión de que la máquina virtual al momento de ser creada con un tamaño estable.

Figura 45

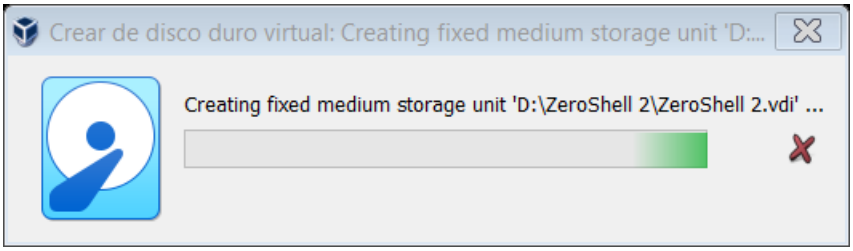
Ventana de la ubicación y tamaño de la máquina virtual.



Nota. En la figura se visualiza el último paso de la creación de la máquina virtual donde se verifica que los datos ingresados al inicio sean los adecuados para dar a la opción crear.

Figura 46

Ventana de la creación del disco virtual

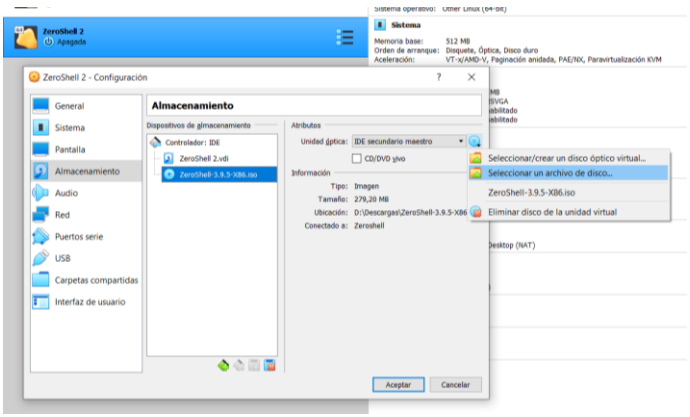


Nota. La figura indica, cómo se está creando la máquina virtual en el software Virtual Box.

Paso 3. Luego se desarrolla la integración de la imagen ISO en la máquina virtual por lo que se hace clic en configuraciones y se selecciona en almacenamiento donde se procede a instalar el archivo WinRAR una vez descargado se agrega al disco vacío en las figuras 47, 48. Se continua con la opción de red donde se configura los adaptadores 1 y 2 habilitando el primero en modo Wireless y el segunda en Ethernet, con el objetivo de tener una perfecta conexión a red, las siguientes figuras 49,50,51 y 52.

Figura 47

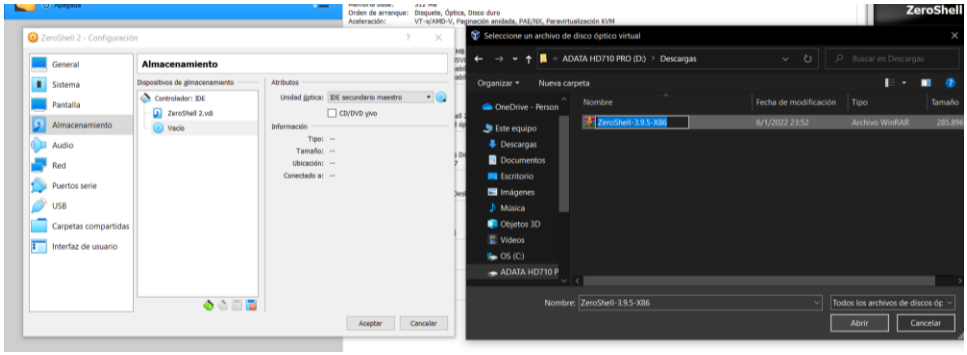
Zero Shell Configuración- Almacenamiento



Nota. En la figura se aprecia la ventana de almacenamiento donde se colocará la imagen ISO que contiene el sistema operativo a instalar.

Figura 48

Selección de la imagen ISO



Nota. En la presente figura se observa cómo se integra la imagen ISO del ZeroShell al disco vacío de la máquina virtual.

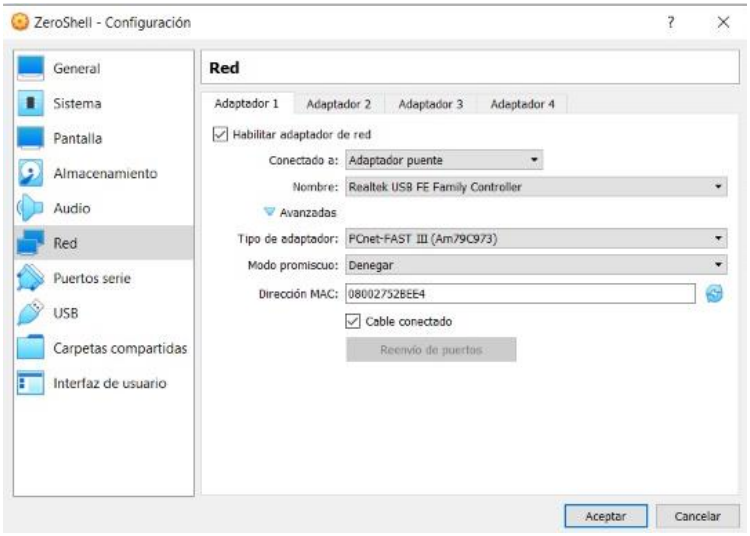
Figura 49

Conexión del Access point

Nota. La figura, muestra el Router Inalámbrico TP WR840N el cual es usado como Access point y se conecta cable al adaptador de red de la computadora.

Figura 50

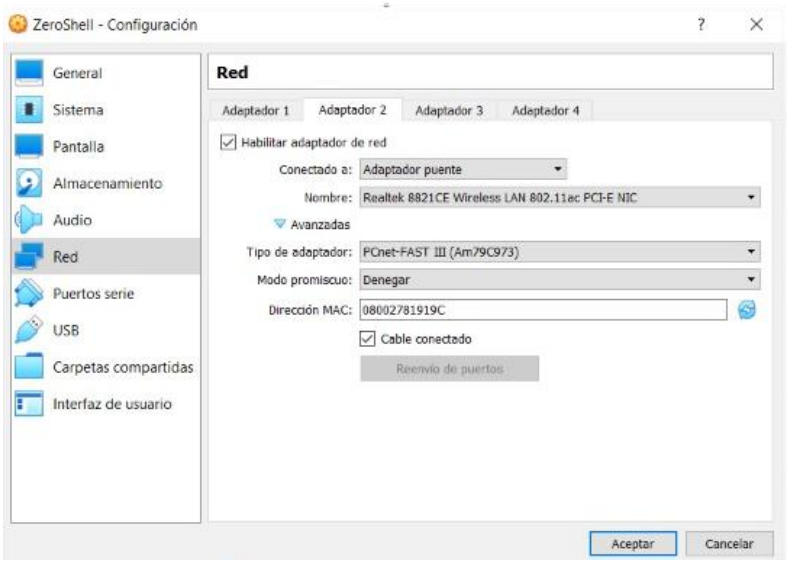
Adaptadores de red



Nota. En la figura, se visualiza la configuración de los adaptadores de red en el primero se coloca la conexión por cableado de red Ethernet.

Figura 51

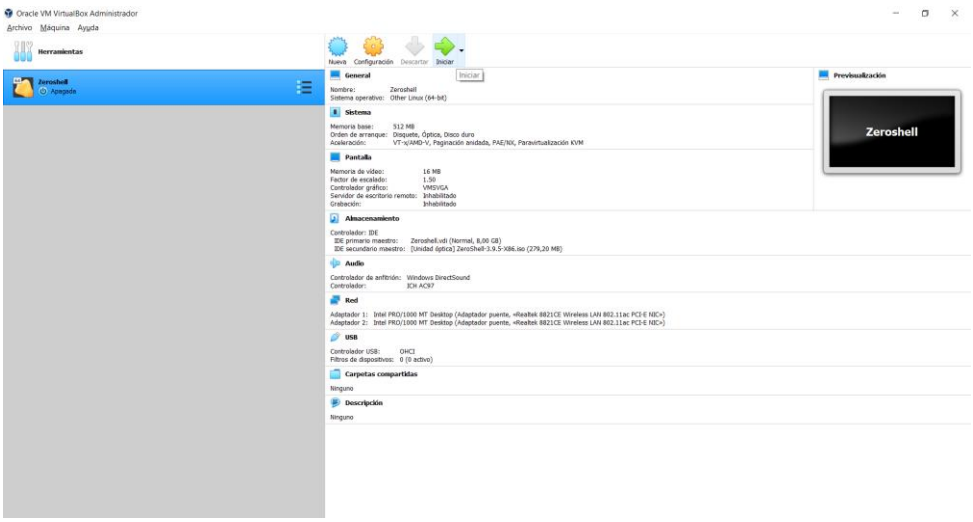
Adaptador de red



Nota. En la figura se indica el cambio del adaptador 2 en forma de WiFi o Wireless para la configuración de red.

Figura 52

Máquina Virtual ZeroShell



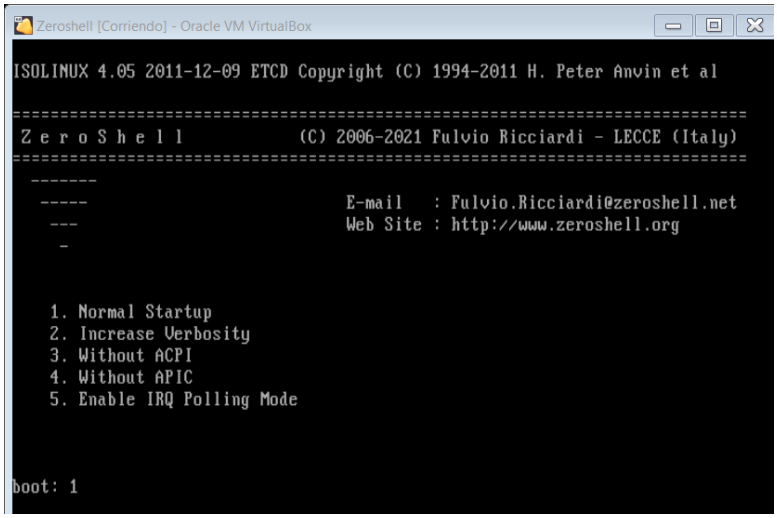
Nota. La figura muestra los cambios a realizar en la máquina virtual para continuar con la configuración del Hotspot.

Configuración del sistema operativo ZeroShell

Paso 1. Se realiza el inicio de la máquina virtual para proceder a la configuración del sistema operativo ZeroShell, por lo cual se selecciona “Normal Startup” y se coloca en el boot el número 1, y se observa como la configuración previa del fabricante se van integrando, en las figuras 53 y 54 se refleja toda la configuración que contiene el sistema operativo ZeroShell.

Figura 53

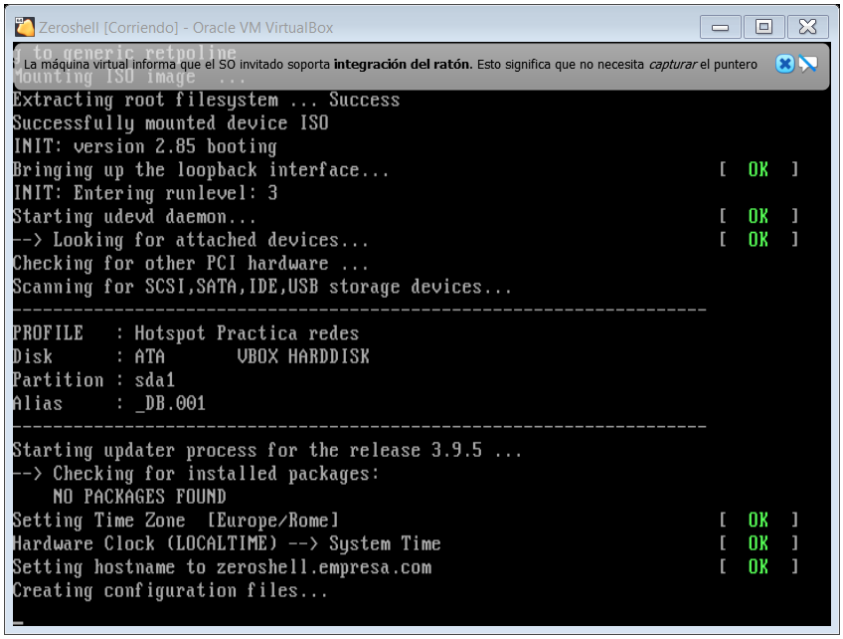
Ventana principal del sistema operativo Zero Shell



Nota. En la figura presente se muestra las opciones de arranque del Sistema operativo por lo que se selecciona la opción 1.

Figura 54

Configuraciones de fábrica del ZeroShell

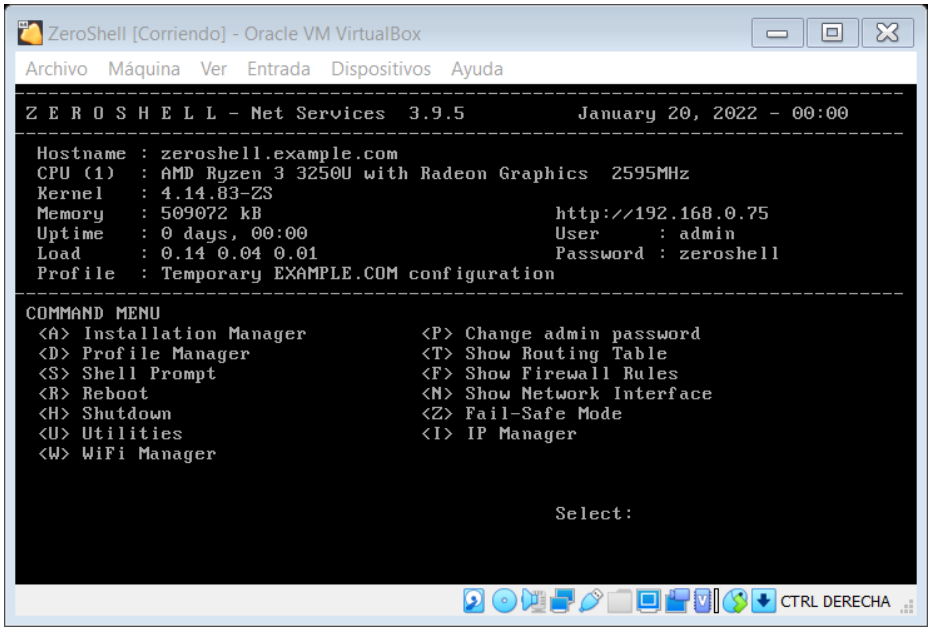


Nota. La figura se refleja las configuraciones automáticas que contiene el sistema operativo en la máquina virtual.

Paso 2. Se observa la configuración por defecto que luego será configurada, por lo que tenemos un menú de comandos el cual se escoge la opción “change admin password” y colocamos en select la letra P, luego de eso se nos presenta una nueva ventana donde se debe crear una clave o password para el sistema operativo. En las siguientes figuras 55 y 56 se observa la configuración de la clave y la selección de la letra P.

Figura 55

Menú de comandos de ZeroShell



Nota. En la figura se observa el menú de comandos donde se escoge la letra P

Figura 56

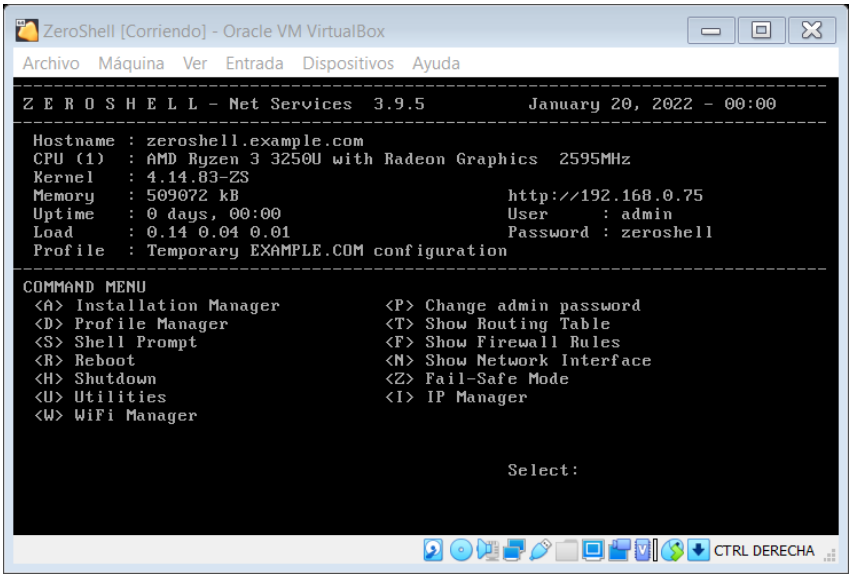
Ingreso del password en ZeroShell

Nota. La figura, muestra el ingreso del nuevo password para el sistema operativo ZeroShell.

Paso 3. En la pantalla principal se selecciona la opción “IP Manager” para poder ingresar y configurar una dirección IP en el sistema operativo, luego de se procede a visualizar la pantalla donde se elige la opción “Modify IP” para el ingreso y configuración de una dirección IP y la interfaz al sistema operativo y así tener una interfaz de red, en las siguientes figuras 57, 58 y 59 nos muestra el ingreso de la IP y el levantamiento de la interfaz.

Figura 57

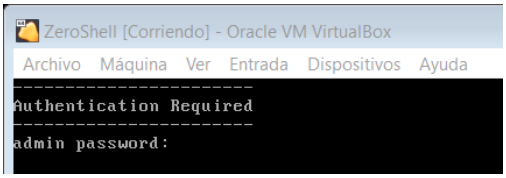
Menú de comandos



Nota. La figura se observa la pantalla principal de ZeroShell con el menú de comandos donde se escoge la opción de “IP Manager” la letra I.

Figura 58

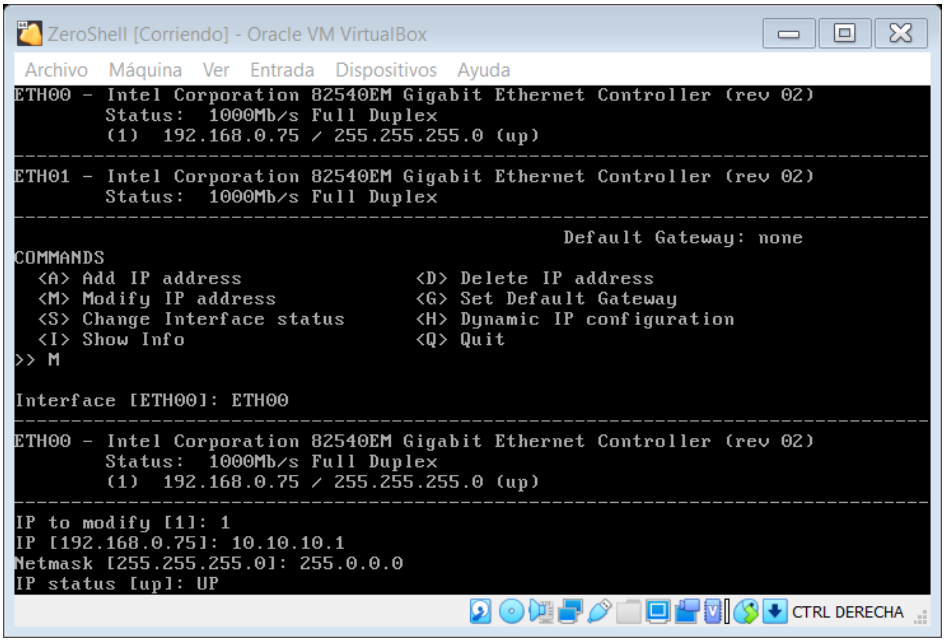
Autenticación requerida



Nota. La figura, indica que se debe ingresar la clave antes creada, para dar el paso a la siguiente ventana secundaria.

Figura 59

Ventana secundaria

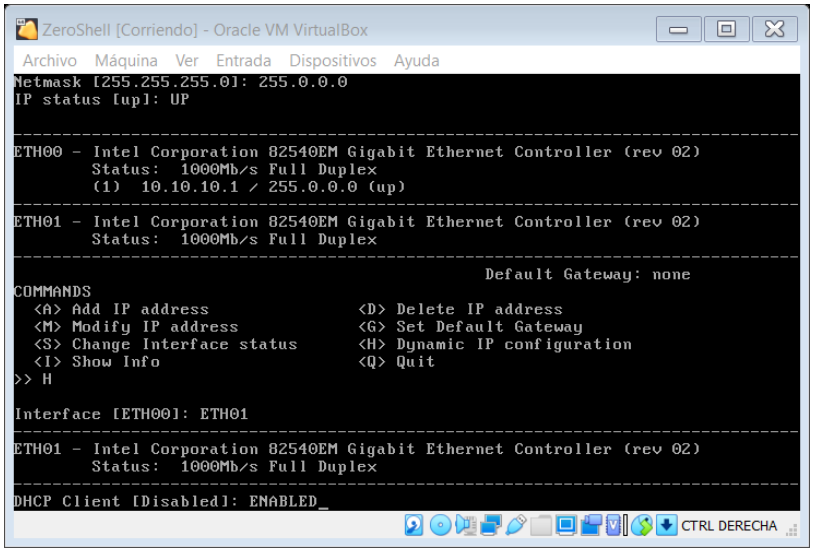


Nota. La figura, presenta la opción M de modificación de la dirección IP y su respectiva mascara y el levantamiento de la interfaz ETH00, ingresando el comando UP.

Paso 4. Configuración de la IP dinámica DHCP que permitirá el ingresar por la otra interfaz ETH01 al sistema operativo de ZeroShell, para proceder a configurar lo colocado como título de este proyecto, las figuras 60 y 61 se puede apreciar el ingreso de la IP y levantamiento de la interfaz

Figura 60

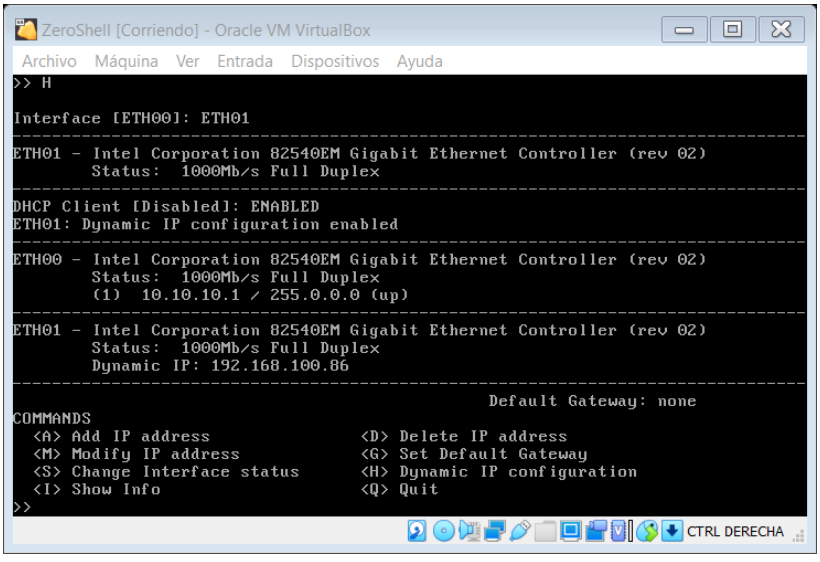
Ingreso de la IP Dinámica



Nota. En la figura se puede divisar que se selecciona la opción Dynamic IP configuration, es decir la letra H, esto permitirá el ingreso de la interfaz ETH01 con su respectivo comando ENABLED para levantar la interfaz de red.

Figura 61

Presentación de la interfaz y IP dinámica



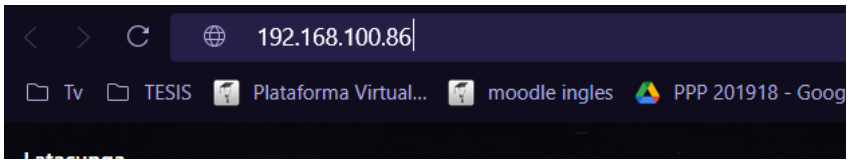
Nota. La figura, muestra la ventana secundaria donde ya se encuentran todas las IP ingresadas junto con la interfaz levantada.

Configuración del Hotspot en el sistema operativo ZeroShell

Paso 1. Se ingresa la dirección IP asignada en la configuración anterior por lo que se abre el navegador de preferencia y se ingresa la IP: 192.168.100.86, donde luego se abre una nueva pestaña donde se puede divisar la interfaz gráfica del sistema operativo ZeroShell, donde se ingresa el usuario “admin” y la clave “admin” para que agregar a la ventana principal donde se procederá a configurar el Hotspot, en las siguientes figuras 62 y 63 se presenta el ingreso al sistema operativo.

Figura 62

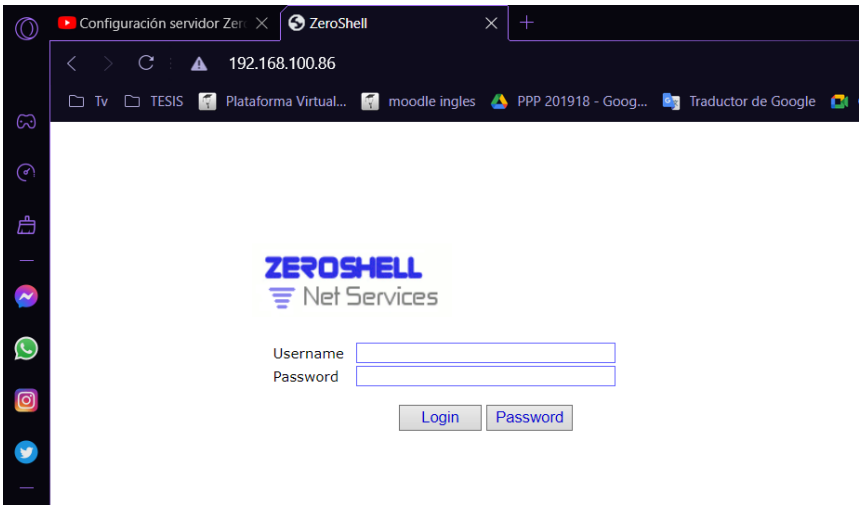
Ingreso de la dirección IP



Nota. En la figura se puede apreciar el ingreso de la IP dinámica en el buscador de nuestro navegador.

Figura 63

Ingreso al Net Services

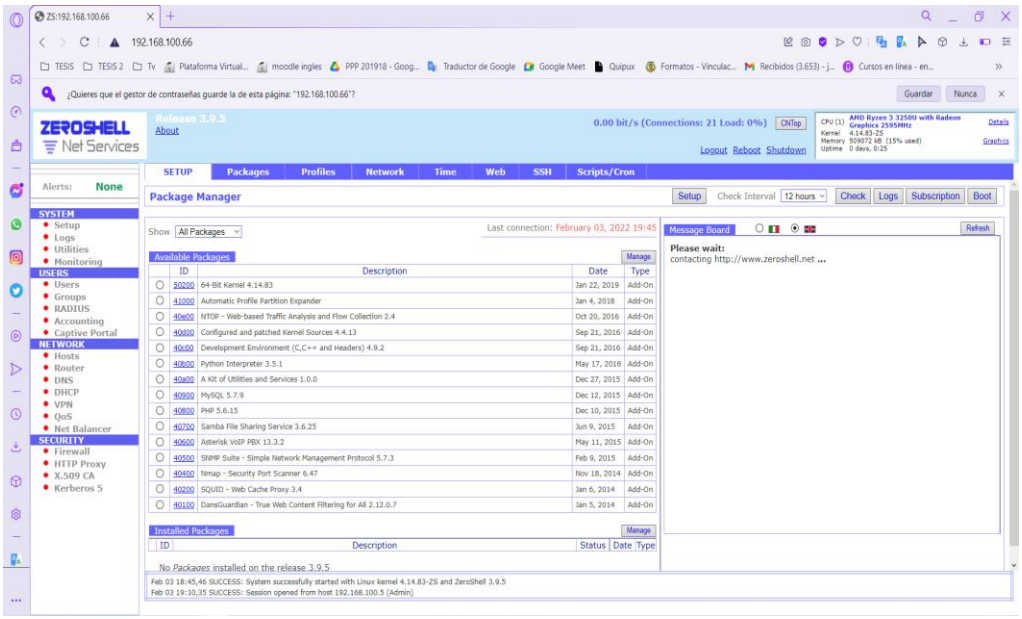


Nota. En la figura se muestra el ingreso al sistema operativo ZeroShell donde agregamos el usuario y la clave para proceder a entrar a la página principal.

Paso 2. Una vez ingresada a la página principal Net Services de ZeroShell donde se observa la pantalla de iconos del administrador de paquetes, donde se inicia a configurar, donde se selecciona las opcion SET UP que se encuentran en la parte izquierda, luego de eso se hace un clic sobre Profiles, luego un clic sobre el disco duro esto nos permitirá almacenar la interfaz del Hotspot. Realizamos un clic sobre la opción New Partition o nueva partición para crear dentro del disco lo que se escogió anteriormente, las siguientes figuras 64 y 65 reflejan la selección de disco duro. En la figura 66 se observa la ventana de la creación de la partición por lo que verificamos el tipo de archivo del sistema donde se elige la opción Extended 2 y se realiza un clic sobre el botón CRÉATE PARTITION.

Figura 64

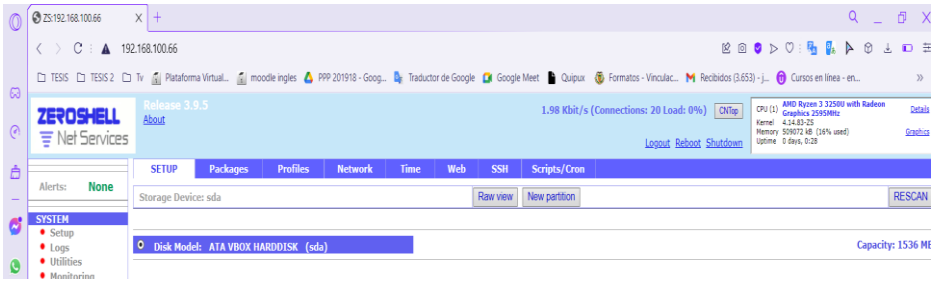
ZeroShell Net Services



Nota. En la figura se puede visualizar la página principal del sistema operativo ZeroShell, para proceder a ingresar al SET UP.

Figura 65

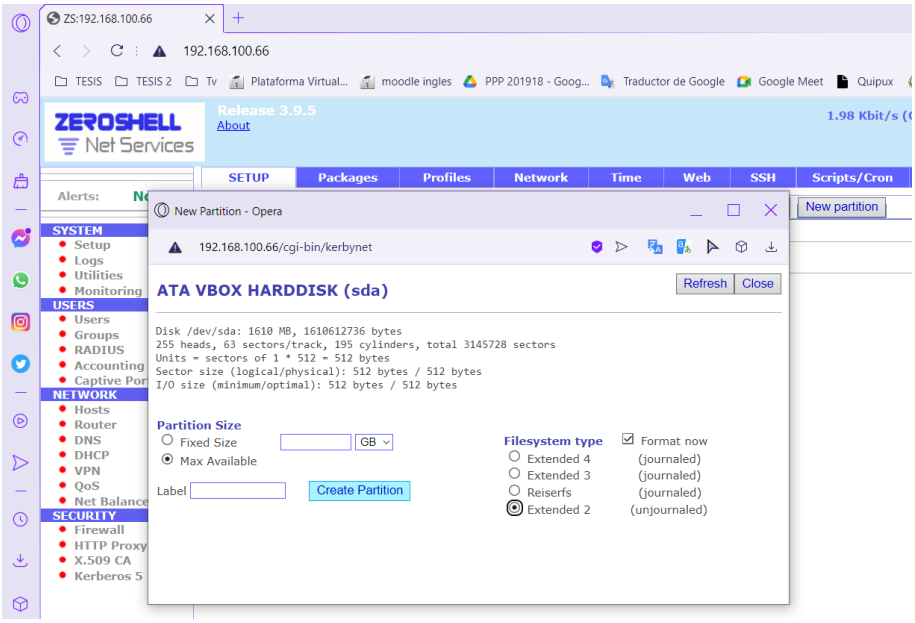
Ventana de configuraciones del disco duro



Nota. La figura, refleja la creación de perfiles y la selección del disco duro donde se va a implementar el Hotspot.

Figura 66

Ingreso a la ventana ATA VBOX HARDDISK



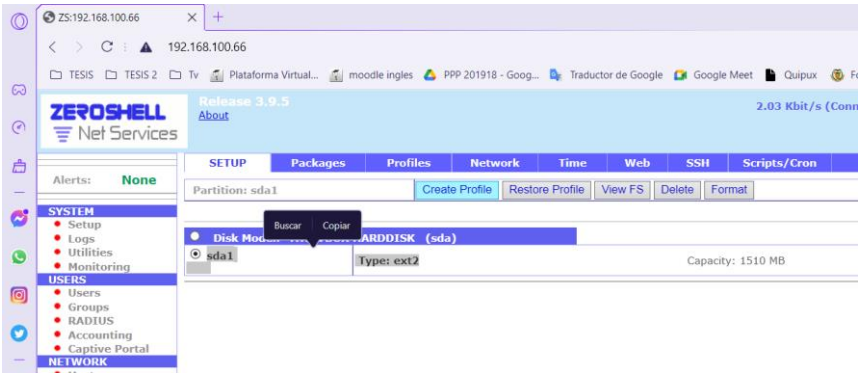
Nota. La figura, muestra la ventana de la creación de la nueva partición por lo que se elige en la opción en Filesystem type la opción Extender 2.

Paso 3. En la venta del Set Up se selecciona el disco dando un clic sobre el cirulo, luego de eso se procede a crear los perfiles dentro del disco, una vez que se abra la ventana se colcoa las configuraciones correspondientes como lo es el nombre del Hotspot, un correo electrónico,

el dominio, una clave, con esto crea el perfil, dando un clic para la salida de la ventana. Se verifica que los datos sean correctos en el perfil creado, luego se procede a activar dicho perfil para que se guarden todas las configuraciones, por lo que se hace un clic sobre el botón y se abre la ventana donde se muestran los datos para su verificación antes de la activación, en las figuras 67, 68, 69 y 70 siguientes se muestra las configuraciones realizadas en este paso.

Figura 67

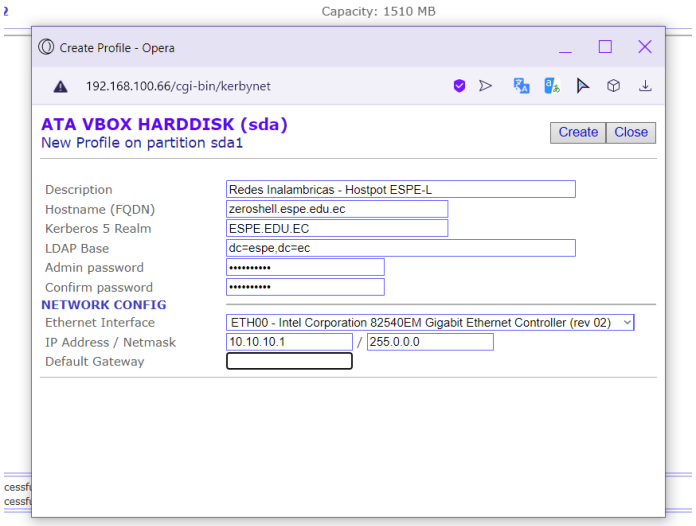
Creación del perfil en el sistema operativo ZeroShell



Nota. En la figura se divisa el disco que se escogió, para luego realizar un clic sobre la opción Create Profile.

Figura 68

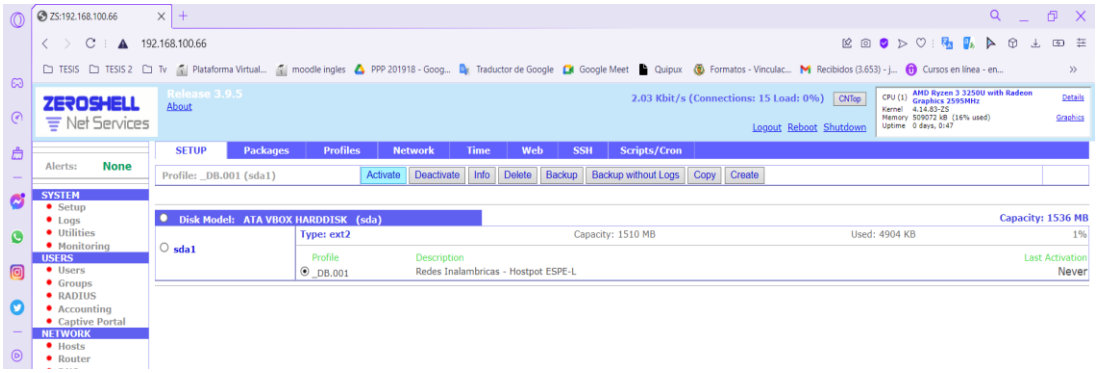
Configuración New Profile



Nota. La figura muestra todos los datos que se debe configurar para el Nuevo perfil del Hotspot.

Figura 69

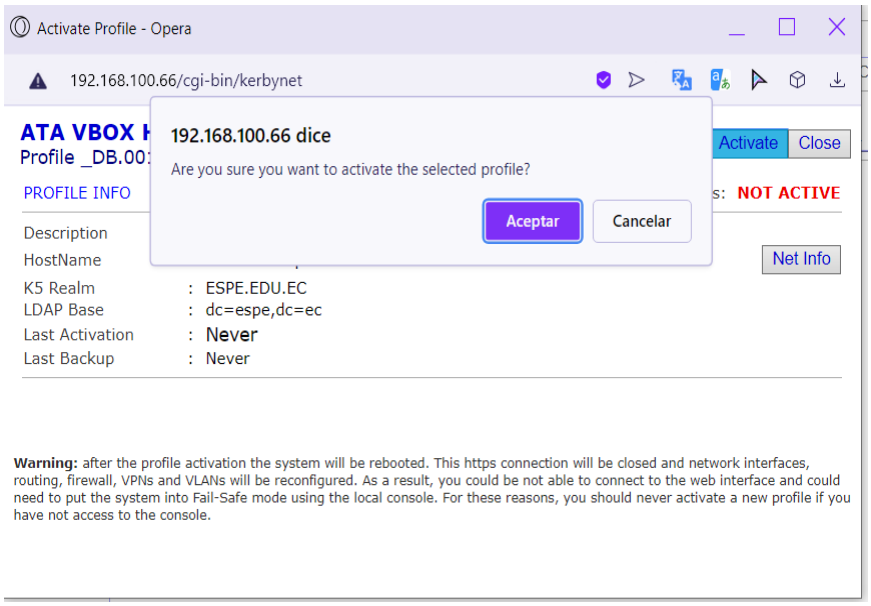
Activación del perfil



Nota. La figura nos indica la opción para activar el perfil creado en el disco duro.

Figura 70

Información del perfil



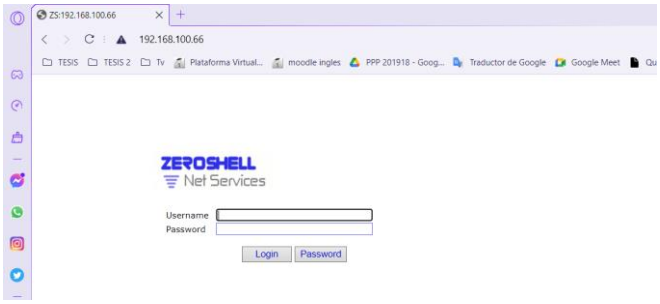
Nota. En la figura se visualiza la información del perfil previa a su activación del perfil.

Paso 4. Una vez realiza la configuración del perfil nuevo automáticamente el sistema operativo nos saca para volver a ingresar con el usuario y la clave, se debe tomar en cuenta que las configuraciones realizadas anteriormente se quedan guardadas al momento de ingresar nuevamente, se nos abre la ventana la cual indica que no se puede acceder al sitio web, por lo

que se vuelve activar las tarjetas red configuradas para con esto obtener conexión a internet. Las figuras 71 y 72 representan la interfaz del ZeroShell.

Figura 71

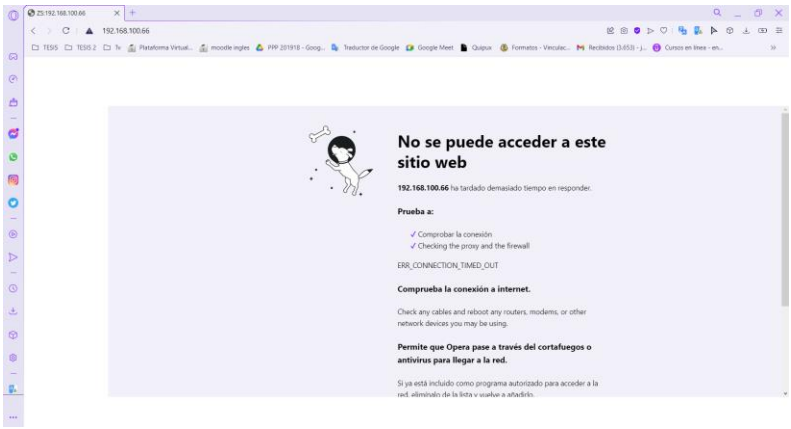
Página del navegador de ZeroShell



Nota. En la figura se aprecia el inicio para el Sistema operativo por lo que se ingresa usuario y clave ya asignada anteriormente.

Figura 72

Sin acceso al sitio web



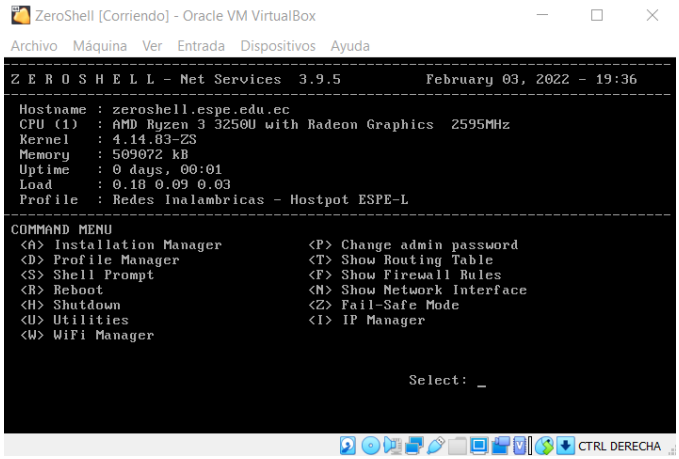
Nota. La figura indica que al momento del ingreso no se pudo acceder al sitio web por lo que se vuelve a conectar a la interfaz de red.

Paso 5. Se reinicia la máquina virtual que contiene el S.O ZeroShell y se puede divisar las configuración ya realizada anteriormente, una vez que se observa que el perfil esta con los datos ingresados, por lo que se ecoge la opción IP Manager (I), se presenta la nueva ventana

donde se ingresa la clave para acceder a las configuraciones realizadas y a los comandos donde se elige la letra (H) para el ingresa de la interfaz ETH01 y se procede a levantar con el uso del comando ENABLED y se puede observar las direcciones IP que se asignan a cada interfaz, esto se puede comprobar en las figuras 73,74 y 75.

Figura 73

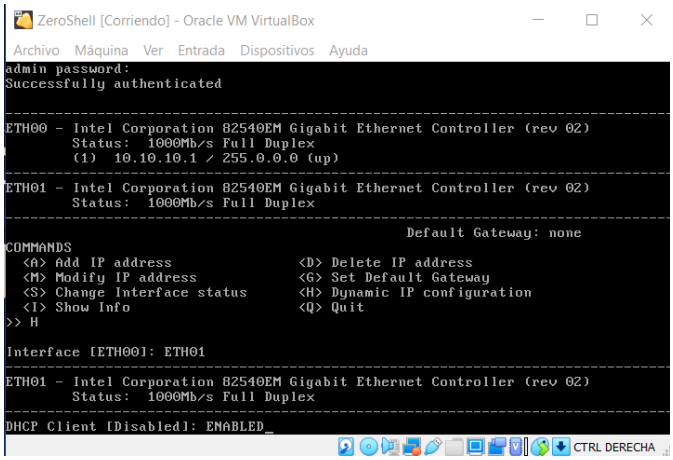
Pantalla del virtualizador



Nota. En la figura se observa las configuraciones que se realizó antes de que se vuelva a reiniciar, adicional a eso el menú de comandos se escoge la opción I para el ingreso de la IP.

Figura 74

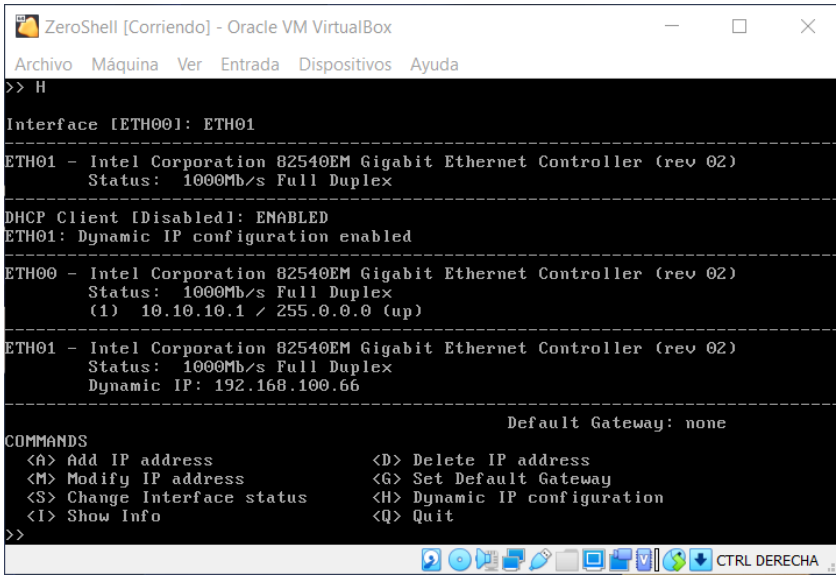
Ventana de interfaz de red



Nota. En la figura se puede visualizar el ingreso de la contraseña para la verificación de las interfaces de red, luego se procede a escoger el comando H para activar la interfaz ETH01.

Figura 75

Verificación De Direccionamiento IP

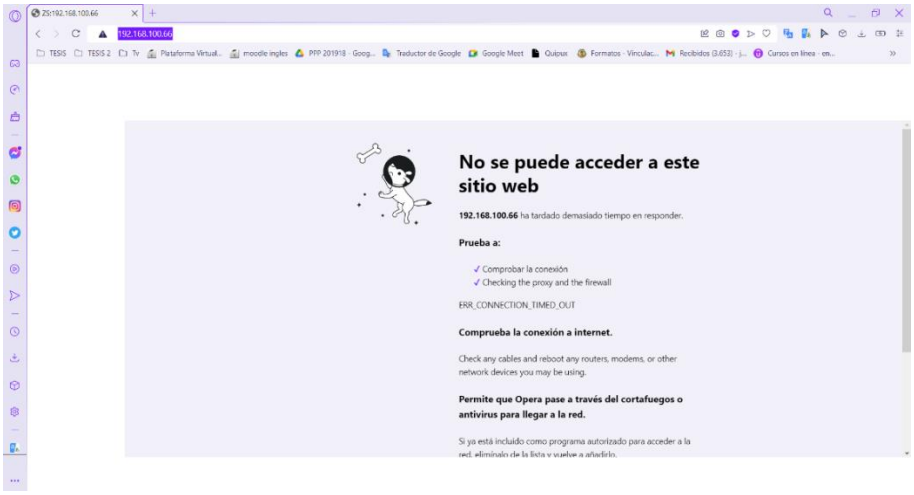


Nota. La figura se verifica y constata que las interfaces habilitadas en las configuraciones de red, tengan una dirección IP. La primera Tarjeta Ether00 tendrá una IP estática y en la otra tarjeta Ether01 tendrá una IP dinámica de nuestro servidor.

Paso 6. Una vez reiniciada y habilitada nuevamente el DHCP del Ether01 por lo que se procede a cargar la página nuevamente, donde se inició el proceso de operación con el net services del ZeroShell. Finalmente se carga la pantalla de dialogo por lo que escogemos la opción avanzada, para dar autorizaciones de aceptación de navegación en dicha página. Una vez cargada la página del net services se realiza el ingresar del usuario y contraseña correspondiente para seguir con las configuraciones del Hotspot, las figuras 76, 77 y 78 representan la configuración mencionada del Zeroshell.

Figura 76

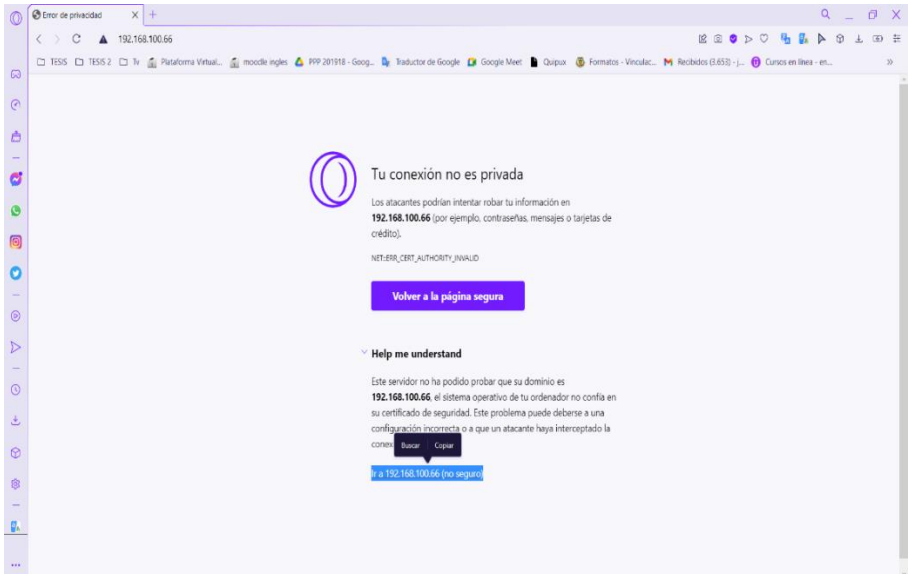
Refresh de la página oficial del net services ZeroShell



Nota. En la figura se observa la realización de volver a recargar o refrescar la página para proceder a ingresar al net services del ZeroShell.

Figura 77

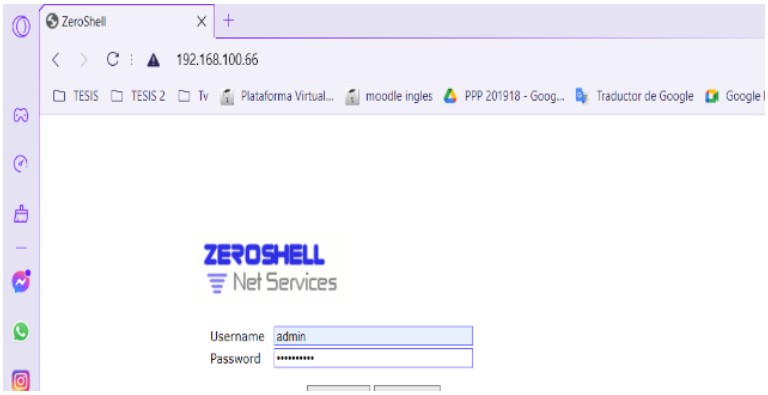
Aceptación de navegación modo segura



Nota. La figura indica el mensaje o la opción que ofrece la página al volver a carga que indica “help me understand” para abrir otra pestaña donde se ingresa al net services ZeroShell y continuar con el proceso de configuración.

Figura 78

Reingreso a los servicios del ZeroShell net services

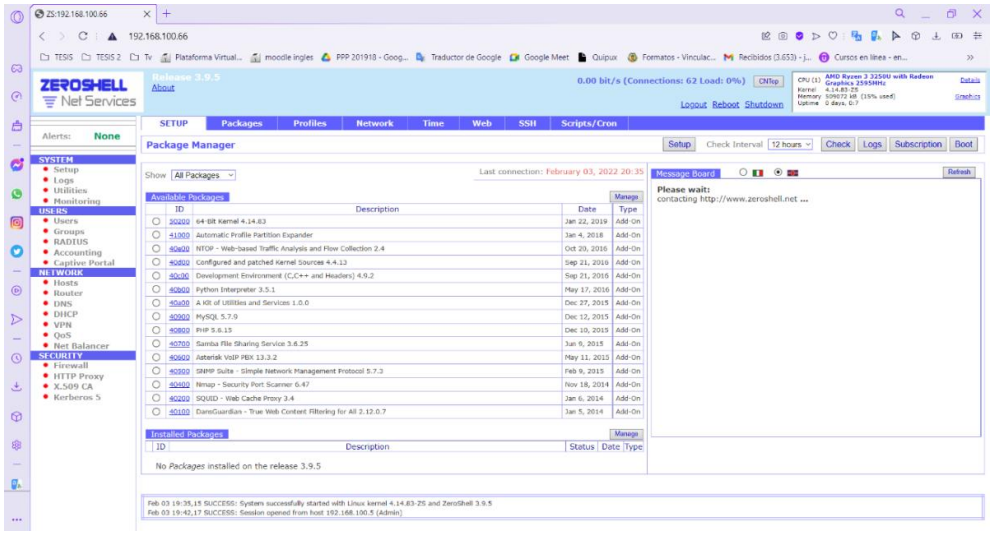


Nota. En la figura se observa la carga de la página principal del ZeroShell para proceder con la realización de la digitación del usuario y contraseña que nos solicita la página del ZeroShell para el net services.

Paso 7. Se observa que la pantalla principal del ZeroShell se ejecute correctamente, para lo cual se selecciona la pestaña network y se verifica que toda la interfaz Ether01 está habilitada con la dirección DHCP que se agrega por defecto a nuestro servidor de internet. Luego se lleva a cabo crear una interfaz de transmisión de datos para lo cual elige en la pestaña NAT y escoge la Ether01 para que se genere la transmisión deseada, en las figuras 79, 80 y 81 se visualiza lo mencionado en este proceso.

Figura 79

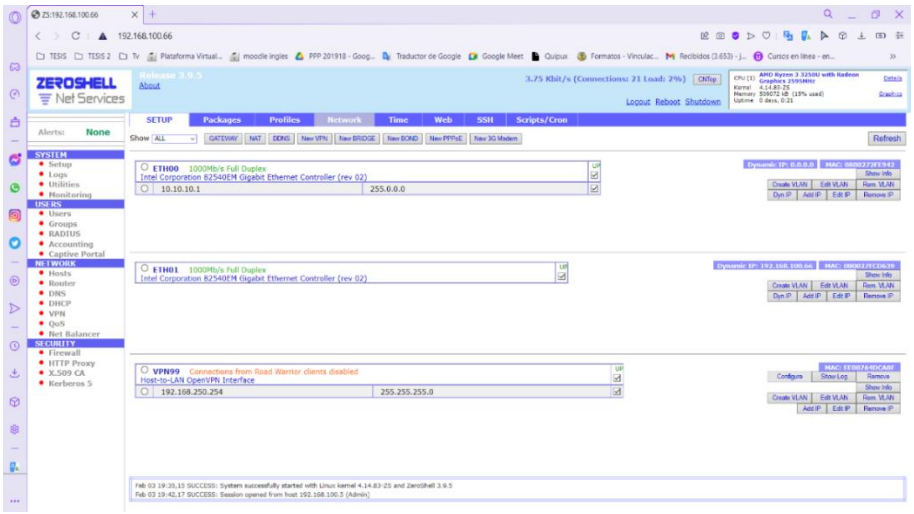
Página principal del ZeroShell net services



Nota. La figura indica la página principal de interacción del net services del ZeroShell. Para continuar con las configuraciones y cambios requeridos.

Figura 80

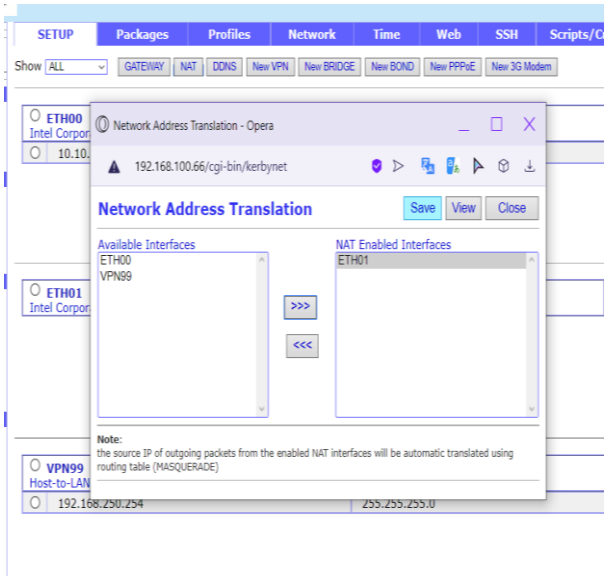
Verificación de la dirección IP por DHCP y red NAT



Nota. En la figura se verifica que la Ether01 este con la dirección IP asignada por el DHCP de nuestro servidor, y se procede a escoger la pestaña que dice NAT para la creación de una interfaz de transmisión.

Figura 81

Habilitación de la interfaz de transmisión

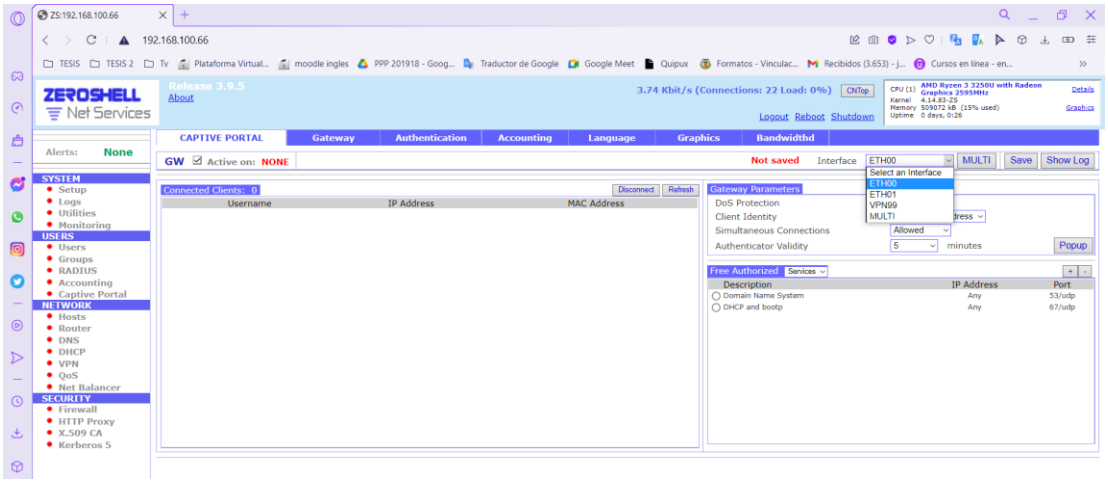


Nota. La figura la selección de la interfaz a la que se va asignar para que se genere la transmisión de datos para el Hotspot creado.

Paso 8. Ingreso al portal cautivo para la activación del mismo por lo que se selecciona la opción GW-Active on, esto levantara la interfaz de red del Hotspot, por lo que se escoge la interfaz ETH00 al realizar este proceso se genera el portal cautivo el cual tiene un enlace de red con la conexión de la misma, una vez realizado todo se guarda las configuraciones desarrolladas dando un clic sobre el botón Save. Antes de la configuración, un clic sobre la opción Authentication para proceder a realizar los cambios del encabezado en la parte de Web Login Page y el cambio de la imagen del portal cautivo se ingresa al botón imagen, donde se abre una ventana para colocar la imagen a nuestro criterio. Luego de realizar las configuraciones, se procede a guardar todo lo desarrollado en este paso se observa en las figuras 82, 83, 84 y 85.

Figura 82

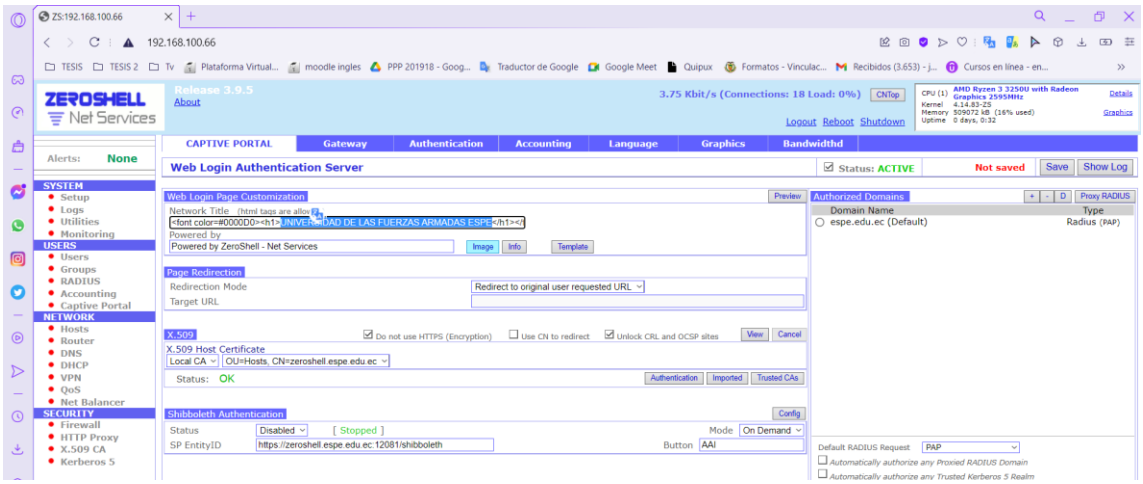
Portal Cautivo ZeroShell



Nota. La figura presenta la activación del portal cautivo y la selección de la interfaz de red que se usara en el Hotspot

Figura 83

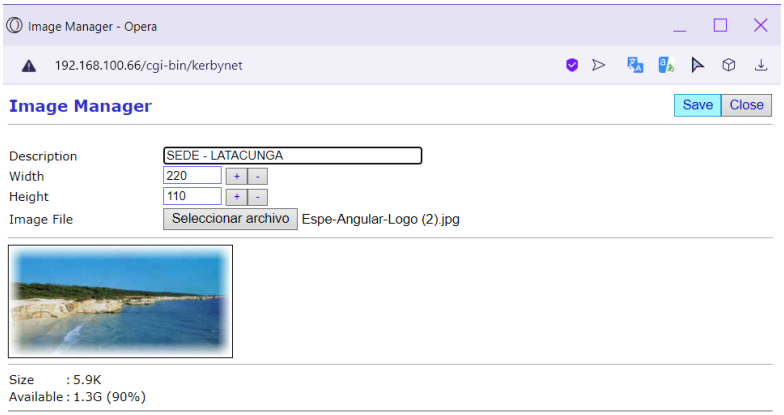
Ventana de Autenticación



Nota. En la figura se observa la configuración de la pestaña de autenticación realizando el cambio del encabezado en parte del Web Login Page.

Figura 84

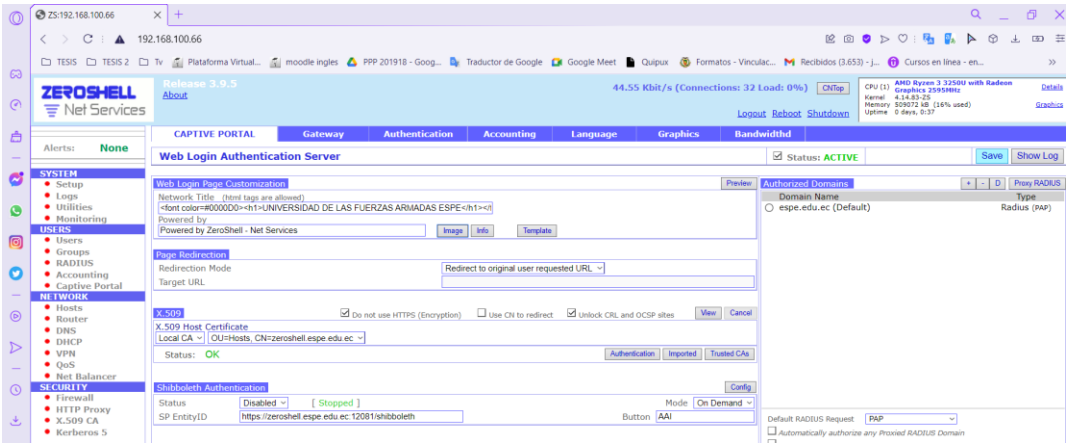
Ventana de manejo de imagen



Nota. La figura muestra las configuraciones del ingreso de los datos que contenga la imagen o logo tipo del portal cautivo.

Figura 85

Verificación de los datos en el portal cautivo



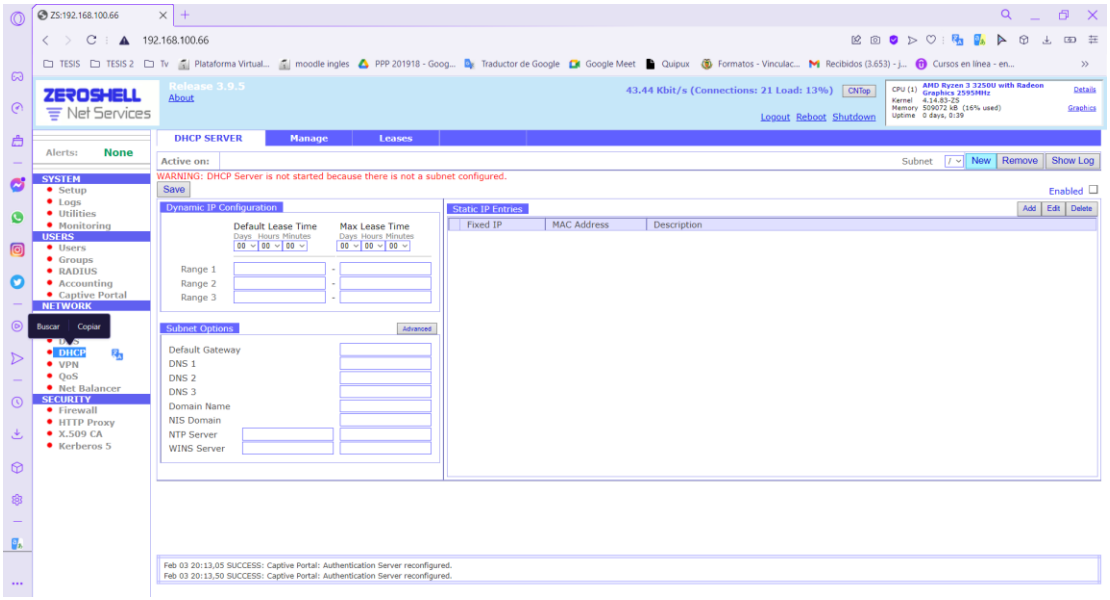
Nota. La figura representa la verificación de los datos que se ingresó para proceder a guardar todas las configuraciones.

Paso 9. Configuración del DHCP Servers que asigna una IP en las interfaces creadas por lo que se desarrollará los rangos entre 10.10.10.10 – 10.10.10.100 que tendrá la subred por lo que se esto se realiza en la IP creada anteriormente, se asigna el Gateway 10.10.10.1 y los

DNS1: 10.10.10.1, DNS2: 8.8.8.8 y DNS3: 8.8.4.4. Una vez realizada la configuración se hace un clic en el botón Save para guardar todo lo ingresado, en las siguientes figuras 86, 87 y 88, se aprecia lo menciona en este paso.

Figura 86

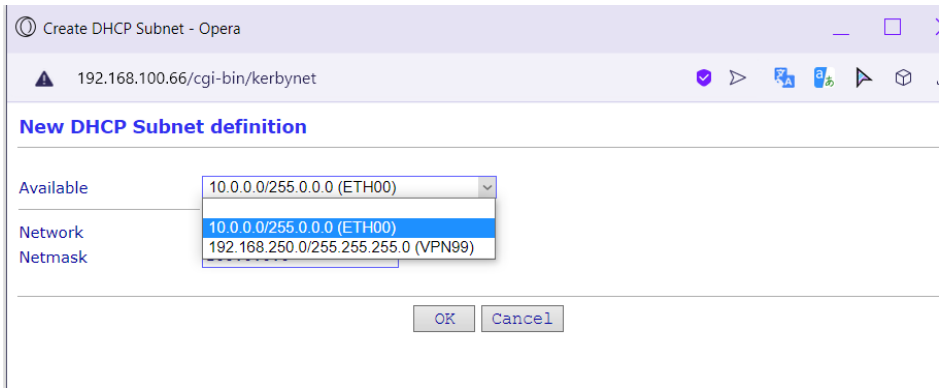
Pestaña del DHCP SERVERS



Nota. En la figura se aprecia la pestaña del DHCP SERVERS donde se hace un clic en el botón Nuevo para el ingreso de la configuración.

Figura 87

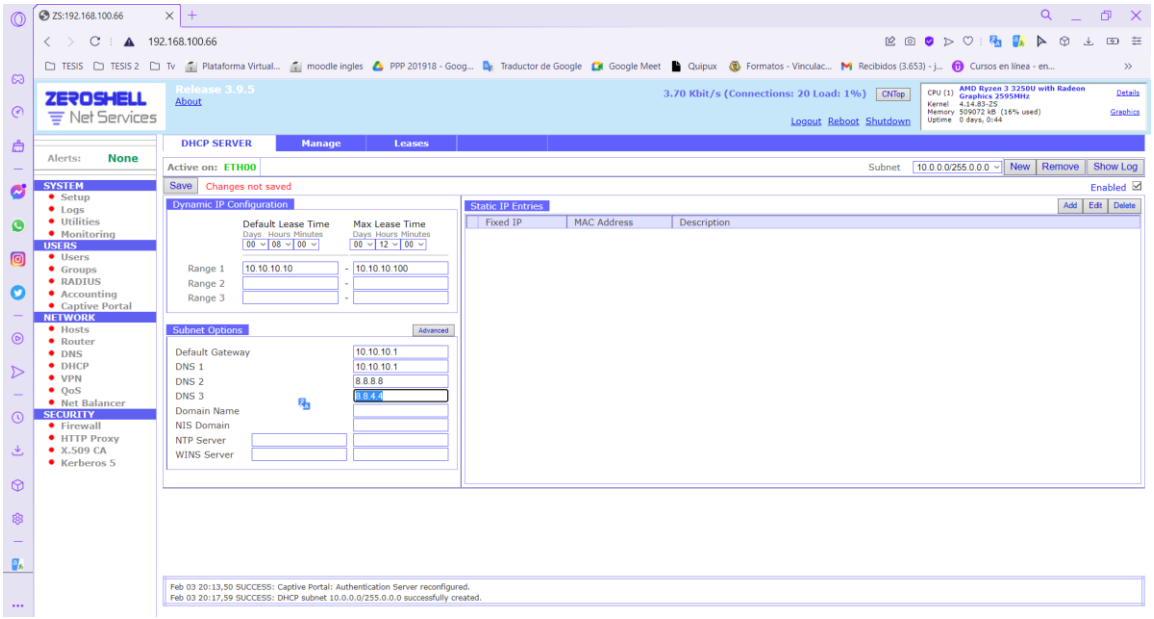
Nueva definición de subred DHCP



Nota. La figura se muestra el ingreso disponible del rango de la interfaz ETH00.

Figura 88

Configuración de la IP dinámica

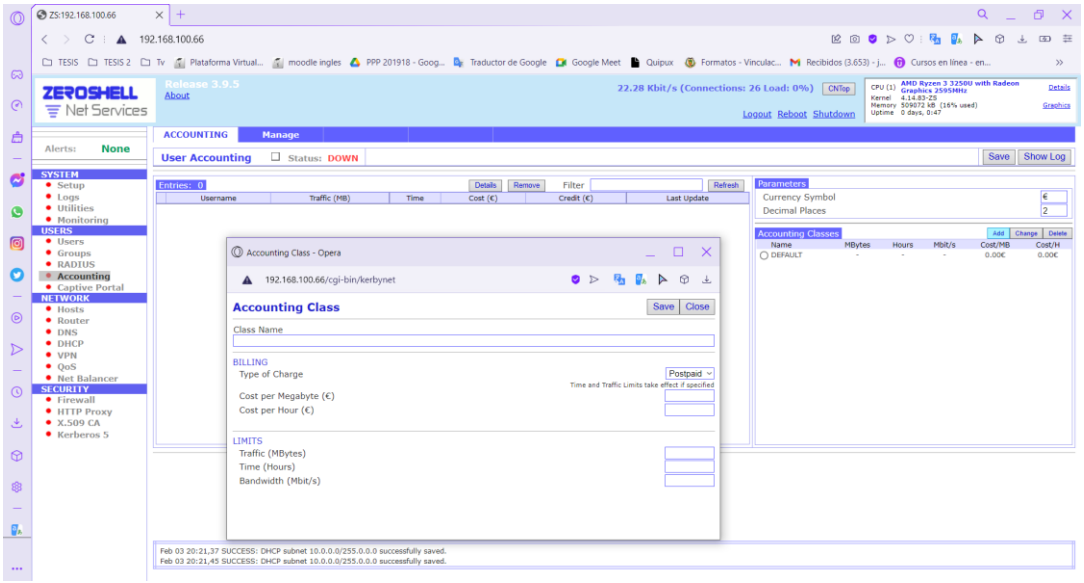


Nota. La figura indica el ingreso de los rangos de IP junto con la incorporación del gateway y los DNS del portal cautivo.

Paso 10. Ingreso a la Pestaña del Accounting donde se hace un clic en el botón Add que se encuentra en la parte derecha en la ventana de Accounting Classes, la cual abre una ventana de dialogo donde se configura los datos del nombre del portal cautivo, el formulario de facturación y los límites del tráfico de bytes y bits, una vez relizado todos los cambios se procede a cerrar la ventana y se verifica que todos s datos ingresados en el Accounting Class sean los correctos para continuar a activar la clase creada y guardar todas las configuraciones ingresadas, en las figuras 89, 90 y 91 se presencia todo lo hecho en este paso.

Figura 89

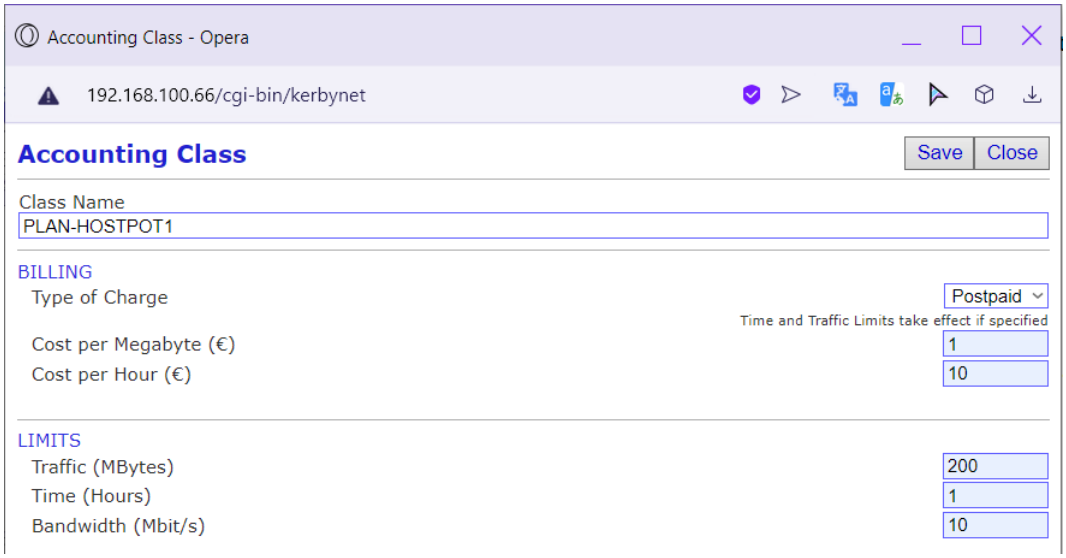
Pestaña de Accounting Class



Nota. La figura indica la creación de la nueva clase de contabilidad que se va a crear para el portal cautivo.

Figura 90

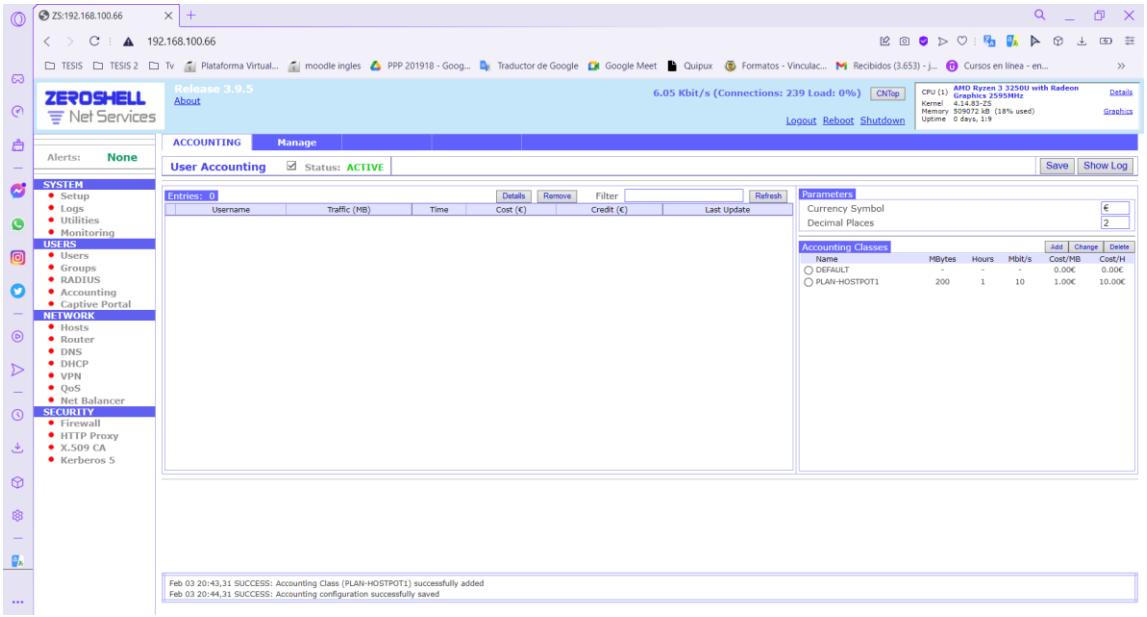
Clase de contabilidad



Nota. En la figura se aprecia la ventana del ingreso del nombre de la clase, la facturación y el límite de Mbytes, tiempo y Mbit.

Figura 91

Levantamiento del estado

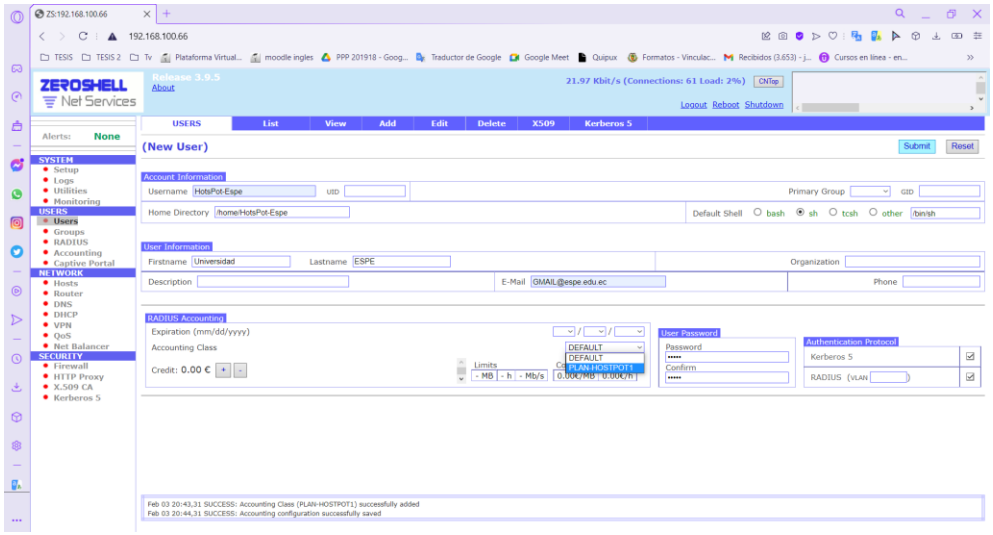


Nota. La figura muestra la clase creada en el accounting class, activación del levantamiento del estado y guardar todas las configuraciones realizadas.

Paso 11. Se procede a seleccionar la pestaña Users para dar un clic en la viñeta Add" agregar" para la creación de los nuevos usuarios que manejará el portal cautivo y con la cual se podrá accede a los servicios de internet, siendo así el formulario de creación de usuarios nos permite seleccionar el tipo de clase, el costo por el uso de navegación y el tiempo de utilización de la red Hotspot. Se crean contraseñas privadas para cada usuario, una vez realizado todas las configuraciones en el formulario de creación de usuarios se debe hace run clic en el botón Submit para confirmar los cambios ingresados, en las siguientes figuras 92,93 y 94 se muestra lo mencionado en este paso de la creación de usuarios.

Figura 92

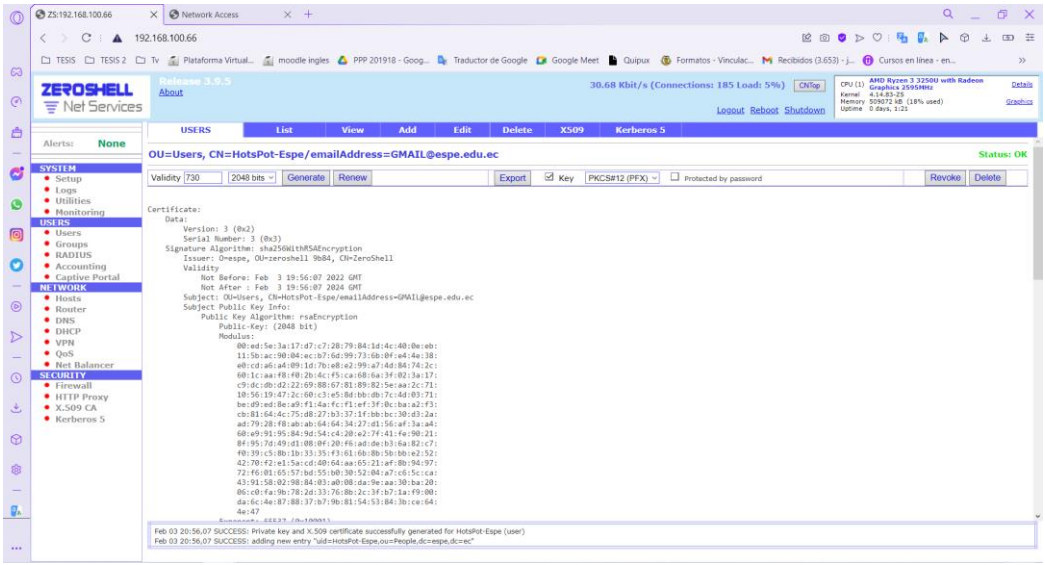
Pestaña de USERS



Nota. La figura indica la creación de usuarios agregando un nombre, e-mail y una contraseña para realizar un clic en el botón submit.

Figura 93

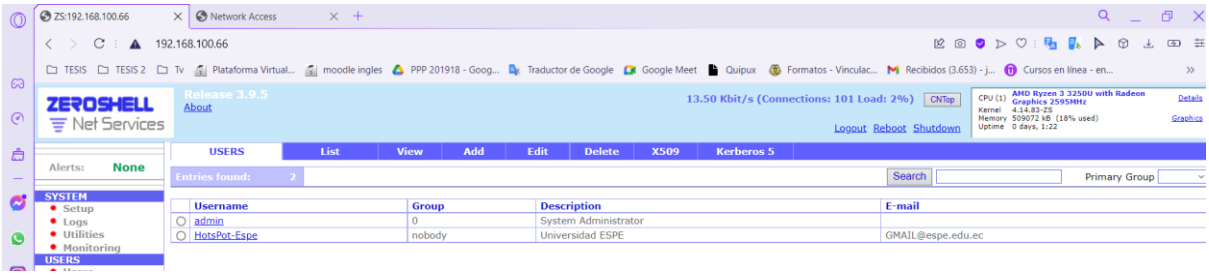
Verificación de datos ingresados



Nota. La figura muestra la verificación de los datos ingresados en el formulario de la creación de usuarios.

Figura 94

Viñeta de los usuarios creados

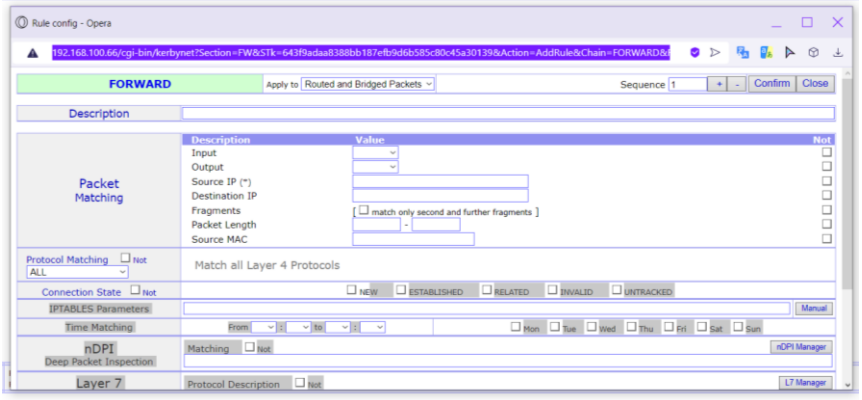


Nota. La figura se visualiza la cantidad de usuarios que se encuentran creados dentro del formulario.

Paso 12. Se continua con la configuración en este caso se ingresa al Firewall “cortafuegos o reglas de seguridad” donde se realiza un clic en el boton Add para desarrollar una nueva regla de seguridad, una vez hecho esto desplegará un formulario el cual se llenará con las reglas necesarias que tendrá nuestro Hotspot. Como primer dato a ingresar es seleccionar la interfaz a la que será asignada la regla, para luego digitar la dirección IP la cual afecta; siendo el caso se selecciona el tipo de protocolo el cual es TCP y el destino de puerto 443, si se desea crear una regla de deshabilitar una página web se debe escribir en el TextBox iptablets parameters la página que no desea que los usuarios ingresen. Adicional se escogerá el tipo de acción que tendrá la regla creada la cual es DROP y se elige la viñeta log, una vez configurado se procede a guardar dando clic en el botón Confirm, todo lo mencionado en este proceso se refleja en las siguientes figuras 95, 96 y 97.

Figura 95

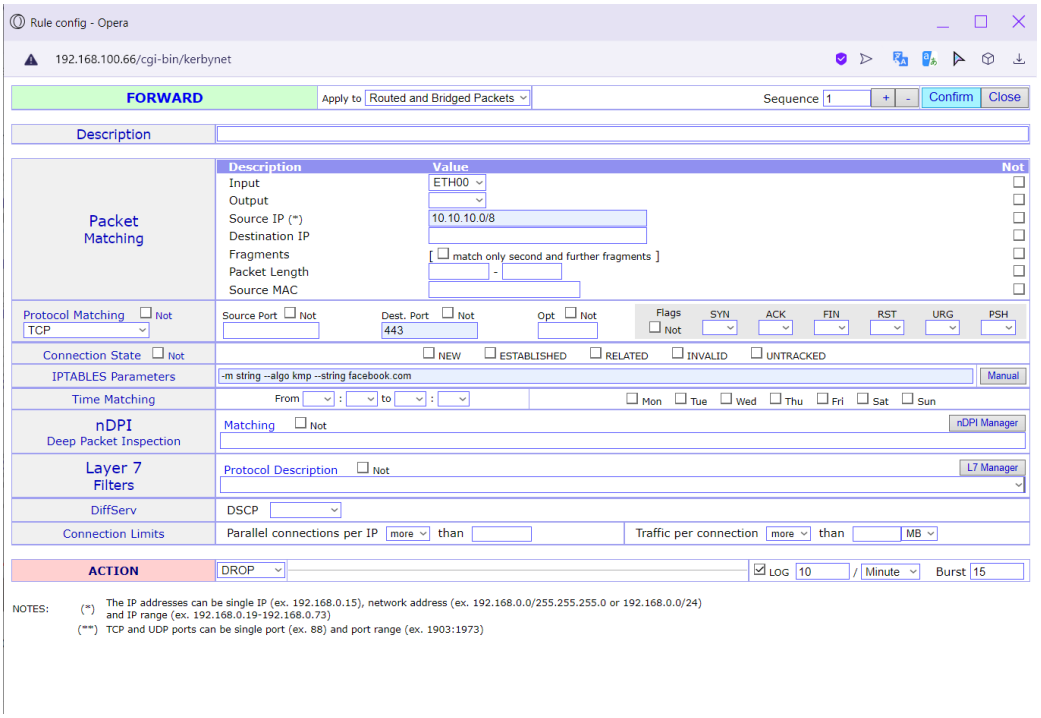
Ingreso a la configuración de reglas



Nota. La figura indica la apertura de la pestaña de configuración de reglas donde se ingresa los datos para la creación de las mismas.

Figura 96

Ingreso de los datos para el firewall



Nota. En la figura se aprecia la incorporación de los datos para las reglas que tendrá el portal cautivo al momento de su acceso a internet.

Figura 97

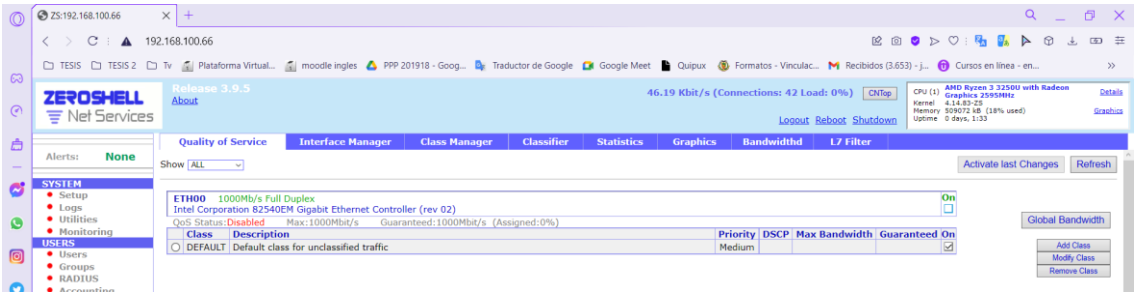
Activación de las reglas

Nota. En la figura se observa la activación de las reglas creadas con sus datos ingresados.

Paso 13. Configuración en la opción del QoS, donde se realiza un mejoramiento en el rendimiento como también la reducción de la calidad del servicio, a la cual el usuario tendrá el acceso para la navegación de internet. Por lo cual se escoge la interfaz que se le asigna a la calidad de servicios QoS, por lo tanto, se selecciona la interfaz ETH00 y la dirección IP 10.10.10.1, donde se procede a guardar dicho cambio en la opción actívate se nos desplegara un sms de confirmación de la confutación realizada, una vez hecho esto se activa QoS, y se procede a modificar la clase de la misma interfaz. Luego de eso se nos presenta una ventana de configuración de la clase, donde se secciona los parámetros locales y a la asignación de 1Mbits tanto se subida como de bajada, cuando ya esté realizado todo este proceso haremos clic sobre botón Save para guardar todas las configuraciones hechas, las figuras 98, 99, 100, 101 y 102 se muestra todo el proceso desarrollado en QoS

Figura 98

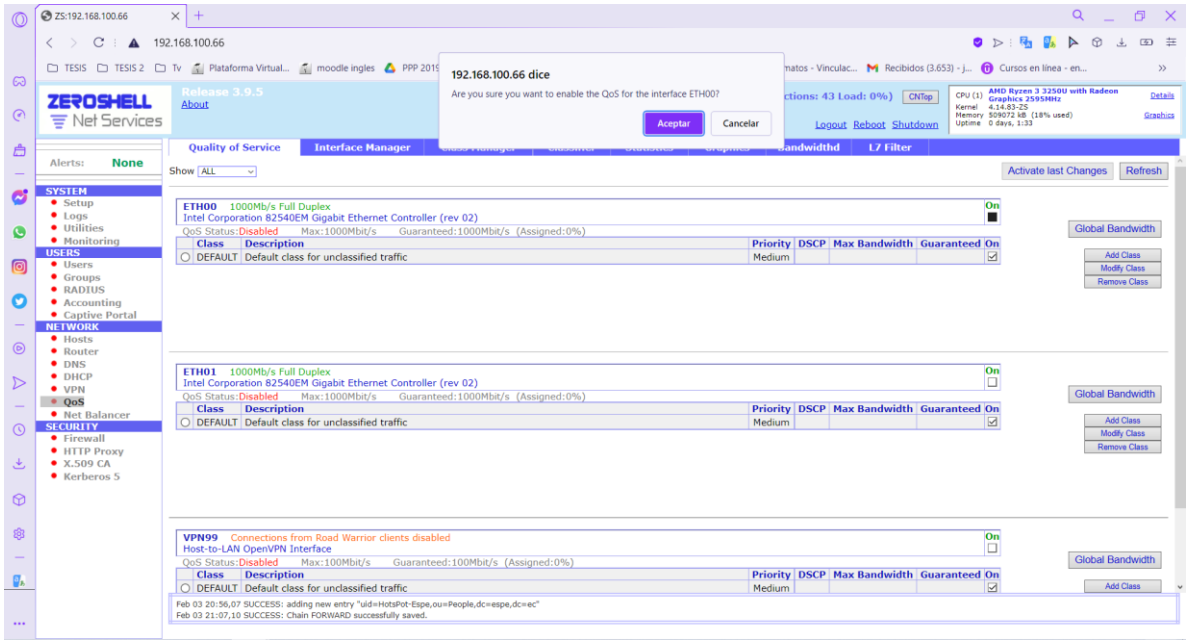
Ventana de la calidad de servicio



Nota. La figura refleja la calidad de servicio que se tiene al configurar el portal cautivo por lo que se active la interfaz ETH00.

Figura 99

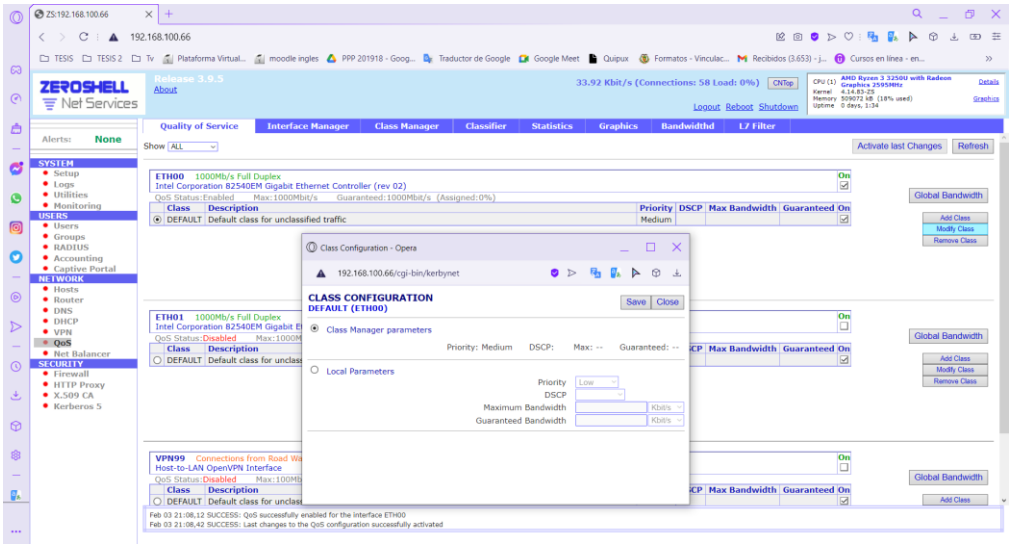
Solicitud de activación de red



Nota. En la figura se puede apreciar el mensaje de confirmación que se nos refleja al momento de activar la interfaz

Figura 100

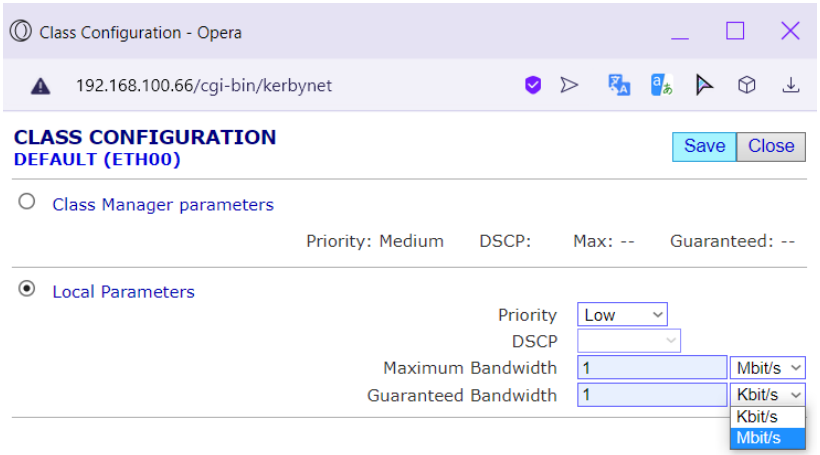
Configuración de clase



Nota. La figura indica el ingresa a la configuración de la clase en el botón Modify Class

Figura 101

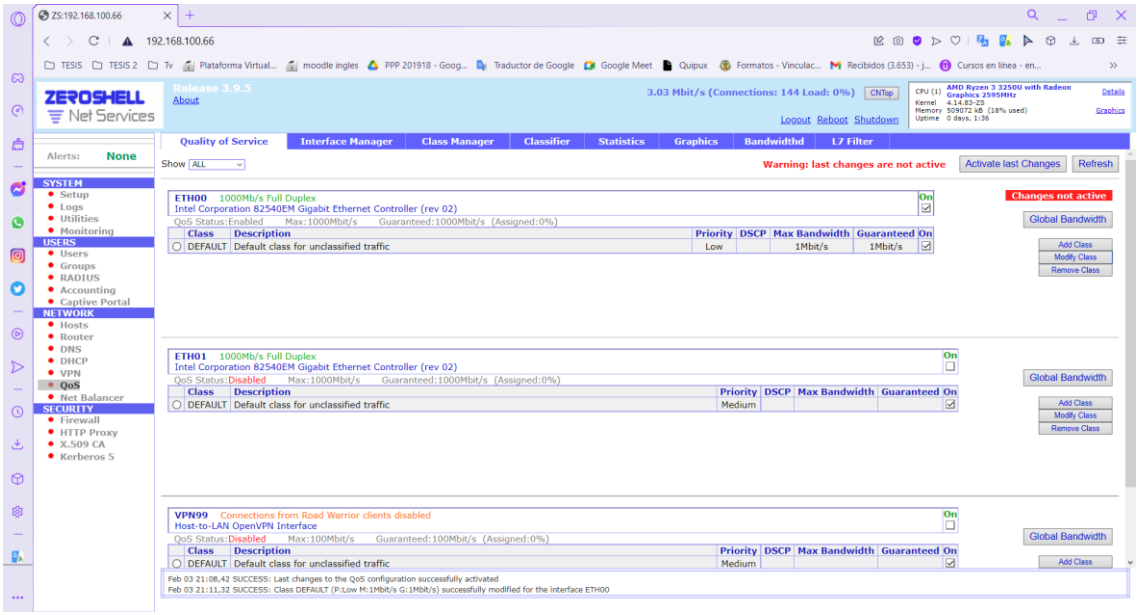
Ingreso de datos



Nota. En la figura se puede apreciar el ingreso de los datos en la opción local parámetros para luego procede guarde lo desarrollado.

Figura 102

Mensaje de activación

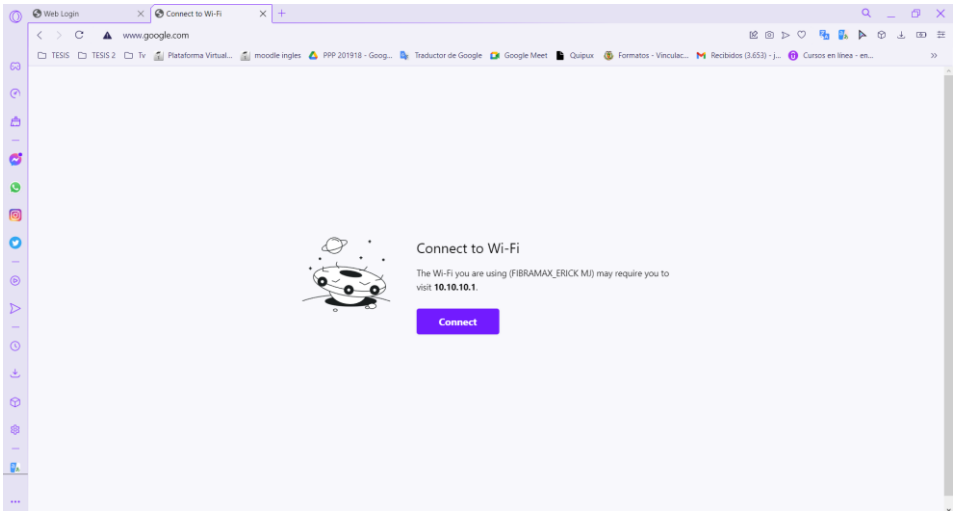


Nota. La figura muestra la activación de la clase configurando relajado en un sms de confirmación de activación del QoS.

Paso 14. Finalmente, para concluir con la práctica lo que procederemos a realizar es ingresar o refrescar la página web con la dirección IP 10.10.10.1 para que se nos conecte con el nuevo portal cautivo creado, por lo que una vez realizado este paso lo que se procederá a visualizar es el portal con la interacción de digitar el usuario y la contraseña. Siendo el caso de escribir mal no se podrá acceder a los servicios de navegación de internet y no se abre la pantalla de visualización de consumo de los servicios de internet. Para concluir si el usuario y la contraseña con las correctas lo que se realiza ahora es digitar una página web en el buscador del navegador y proceder a disfrutar de los de internet con los M/bits asignados, en las figuras 103, 104, 105, y 106 lo mencionado en este proceso.

Figura 103

Refresh o ingreso de la dirección IP del portal cautivo



Nota. En la figura se verifica y visualiza la pantalla de carga del portal cautivo con la dirección IP asignada para la misma.

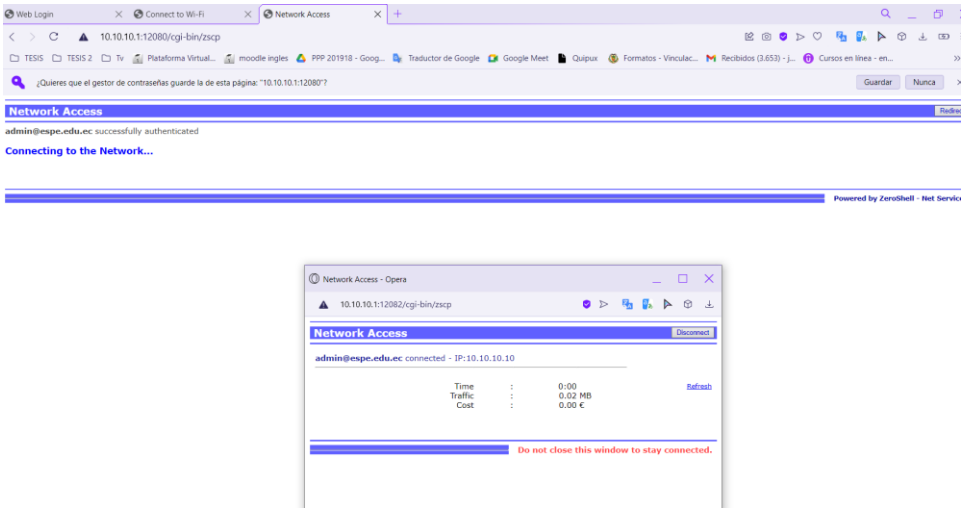
Figura 104

Digitación del usuario y contraseña correspondientes

Nota. La figura se aprecia del portal cautivo totalmente recargado y por la cual se procede a la digitación de usuario y contraseña designada para ese dispositivo.

Figura 105

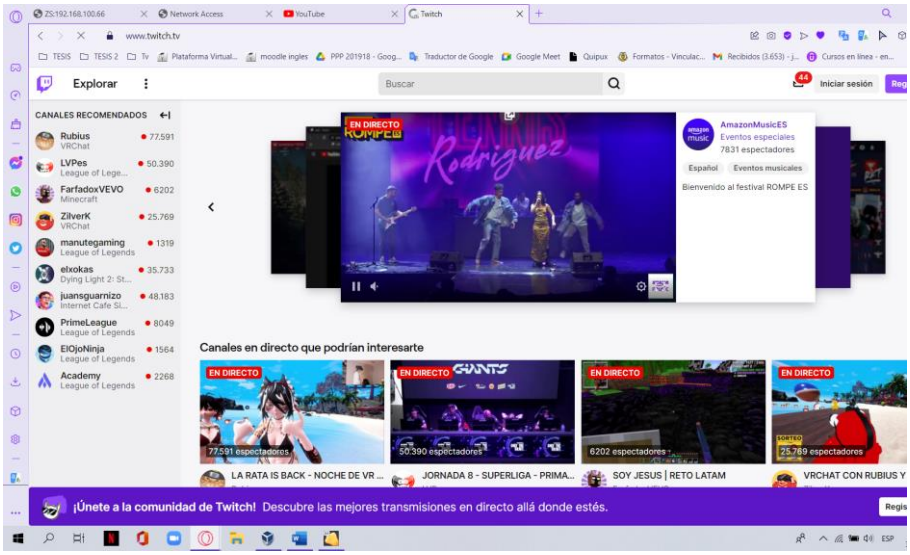
Pantalla de verificación de la navegación en el internet



Nota. En la figura se observa la pantalla de dialogo y de verificación del consumo con respecto a al tiempo, tráfico de datos y el costo que nos saldrá consecutivamente por la tardanza de en la navegación de internet.

Figura 106

Búsqueda y navegación del internet

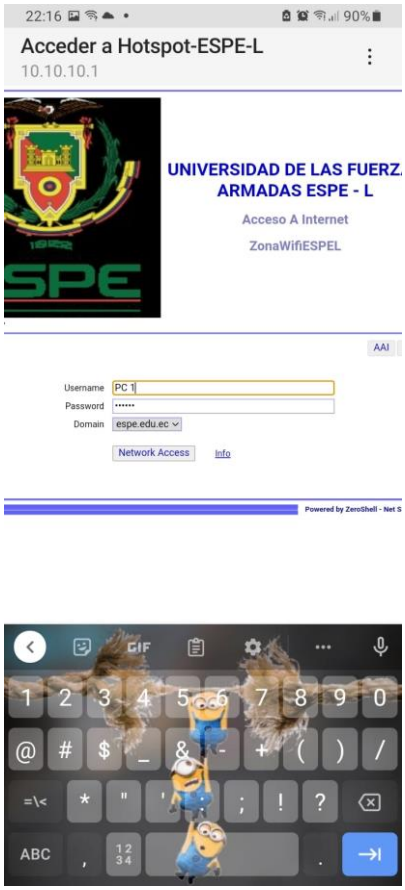


Nota. La figura muestra el pleno accionar de los datos a ingresar por el Hotspot y por el cual se está procediendo a navegar por una página de consumo alto de video y de carga.

Paso 15. Para culminar en las figuras 107, 108, 109, 110 y 111, se visualiza la revisión de la navegación de internet mediante el Hotspot creado lo que se realiza es ingresar en un dispositivo móvil o laptop los usuarios creados dentro del portal cautivo para lo cual se evidenciara que los usuarios y contraseñas sean las correctas para obtener el acceso correcto hacia el mundo del internet. Una vez realizado ese paso se procede a buscar una página web y disfrutar del ancho debanda y la calidad de servicio que nos ofrece nuestro Hotspot.

Figura 107

Digitación del usuario y contraseña correspondientes



Nota. La figura se aprecia del portal cautivo totalmente recargado y por la cual nosotros procederemos a la digitación de usuario y contraseña designada para ese dispositivo.

Figura 108

Acceso concedido al Hotspot y al internet

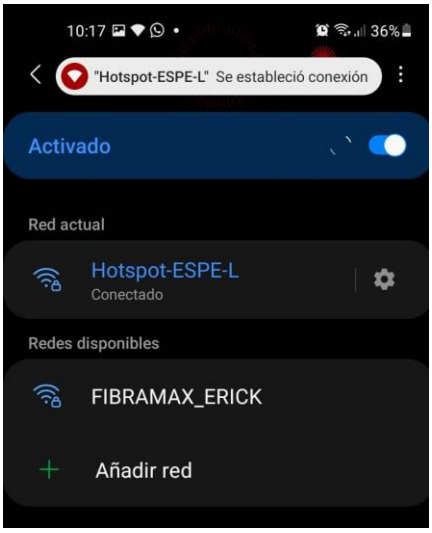


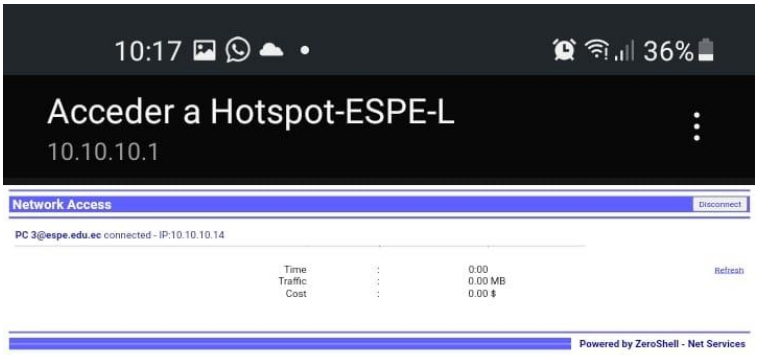
Figura 109

Verificación de conectividad, velocidad y dirección IP

Nota. En la figura se verifica la conectividad de internet con el Hotspot, adicional se visualiza la cantidad de velocidad que tenemos con respecto al resto de clientes, también se hace la comprobación de que dirección IP tiene asignada nuestro dispositivo.

Figura 110

Pantalla de verificación de la navegación en el internet



Nota. En la figura indica la pantalla de dialogo y de verificación de cuanto ese esta consumiendo con respecto a al tiempo, tráfico de datos y el costo que saldrá consecutivamente por la tardanza en la navegación de internet.

Figura 111

Búsqueda y navegación del internet

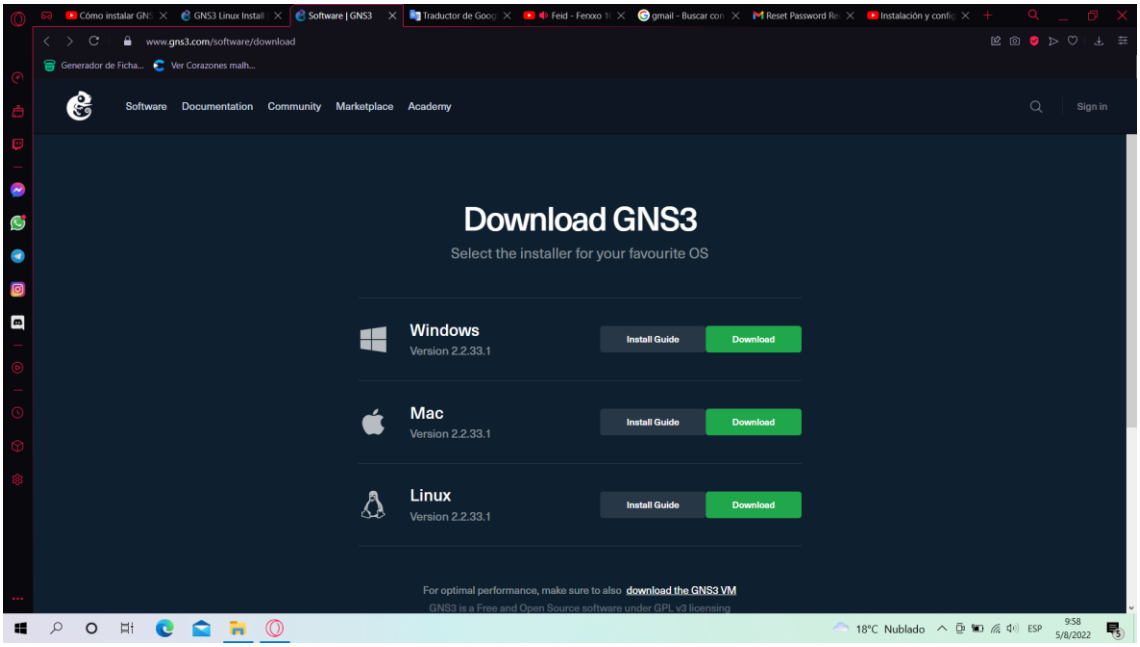
Nota. La figura muestra el pleno accionar de los datos a generar por el Hotspot y por el cual se procede a navegar por una página de consumo relativo y de carga inmediata para el usuario.

Instalación de GNS3 en el sistema operativo Ubuntu

Paso 1. Se inicia con ingreso a la página oficial de software GNS3 en el siguiente link: https://docs.gns3.com/docs/getting-started/installation/linux/ , una vez ahí se busca la versión de Linux, donde se despliega una ventana con los comandos a ejecutar dentro de la terminal de Ubuntu. Por lo que se procede a colocar los comandos dentro del terminal para la respectiva instalación. A continuación, se indica las figuras 112 y 113 lo mencionado en este paso.

Figura 112

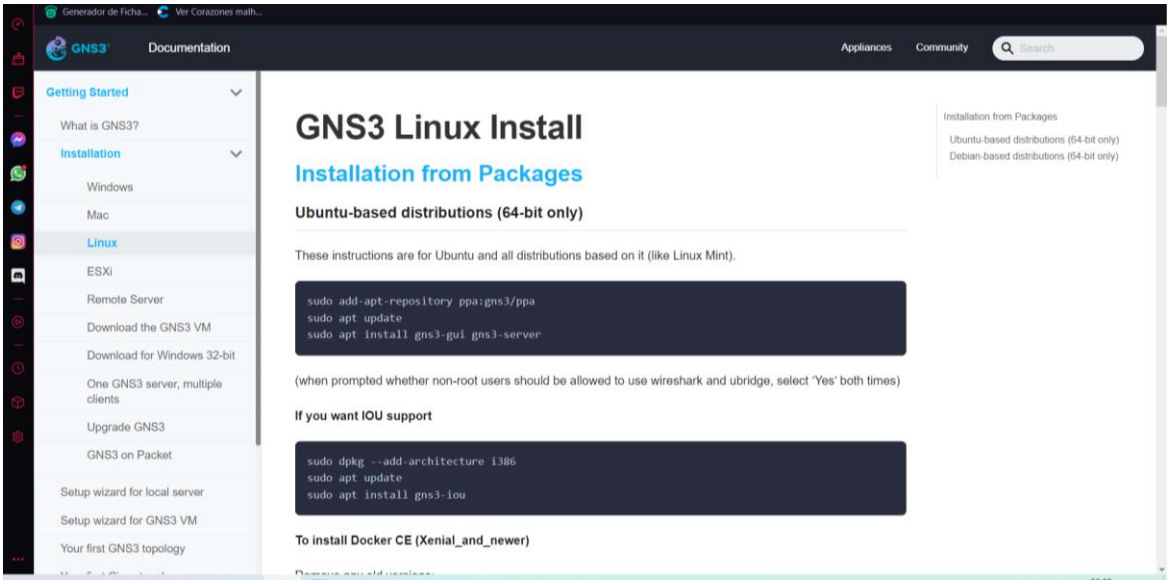
Página oficial del Software de simulación GNS3



Nota. La figura presente contiene la página oficial del software de simulación GNS3, el cual nos permita ser ejecutado dentro del sistema operativo para la respectiva configuración a realizar.

Figura 113

Instructivo para la instalación de gns3 dentro de linux



Nota. En la figura se visualiza el instructivo con los comandos que se interesará dentro de la terminal de Linux.

Paso 2. Proceso de instalación dentro del sistema operativo Ubuntu por lo que se requiere del instructivo con los respectivos comandos a ingresar dentro del terminal de Linux. Iniciamos agregando el comando de para agregar el repositorio ya que esto permite tener facilidad la instalación de GNS3, el ingreso de todos los paquetes que contiene el software de simulación conjuntamente con sus respectivas claves, versiones anteriores y los grupos que contiene gns3 para el correcto funcionamiento dentro de Linux, en las figuras 114, 115, 116, 117 y 118 se visualiza lo mencionado en este proceso.

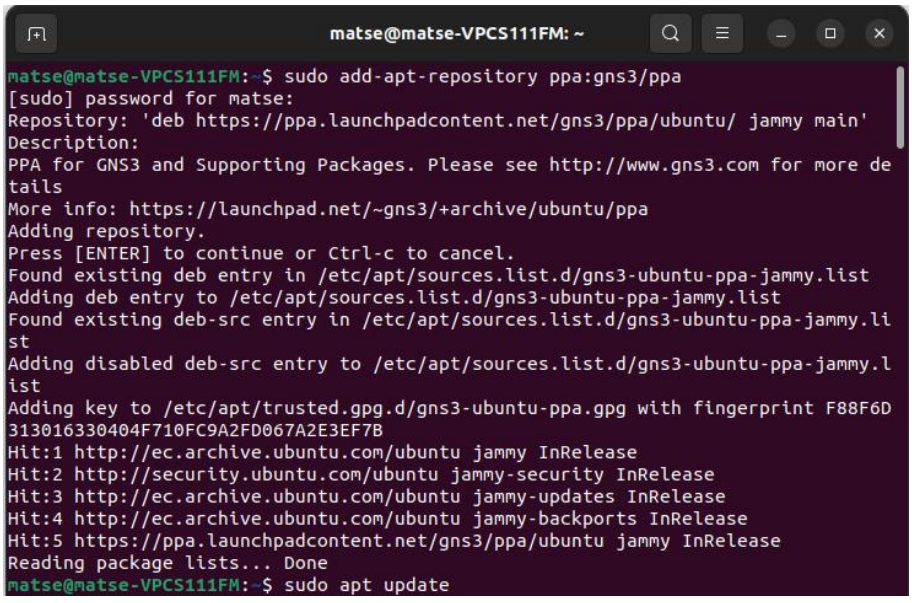
Figura 114

Instalación de gns3 dentro del sistema operativo Ubuntu

Nota. La figura se observa cómo se realizó la instalación colocando dos computadoras la una la instalación del software y la otra contiene el instructivo con el objetivo de ir siguir paso a paso la instalación.

Figura 115

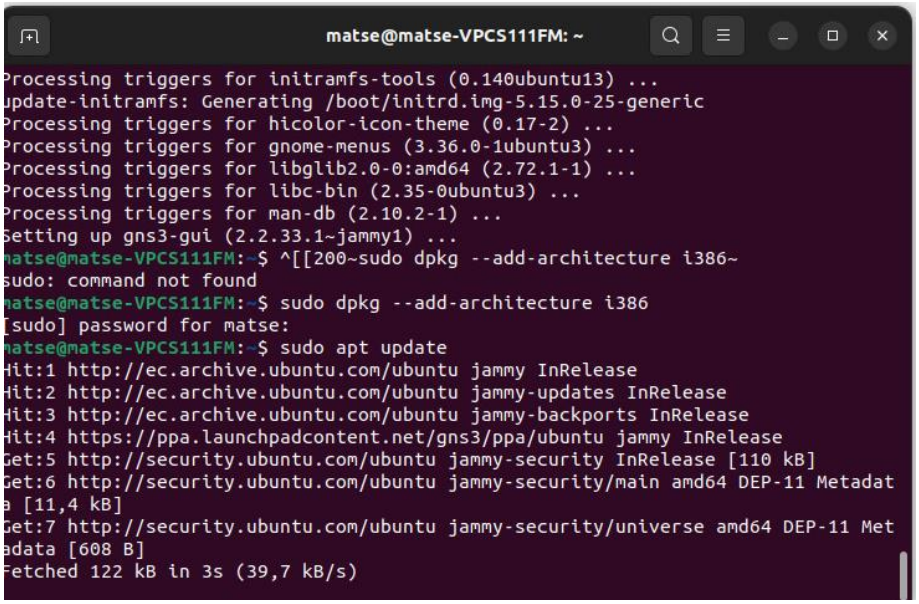
Ingreso del comando para el repositorio de GNS3



Nota. En la figura se muestra el comando “sudo add- apt-reposiroty ppa:gns3/ppa “ para el ingreso del repositorio de GNS3.

Figura 116

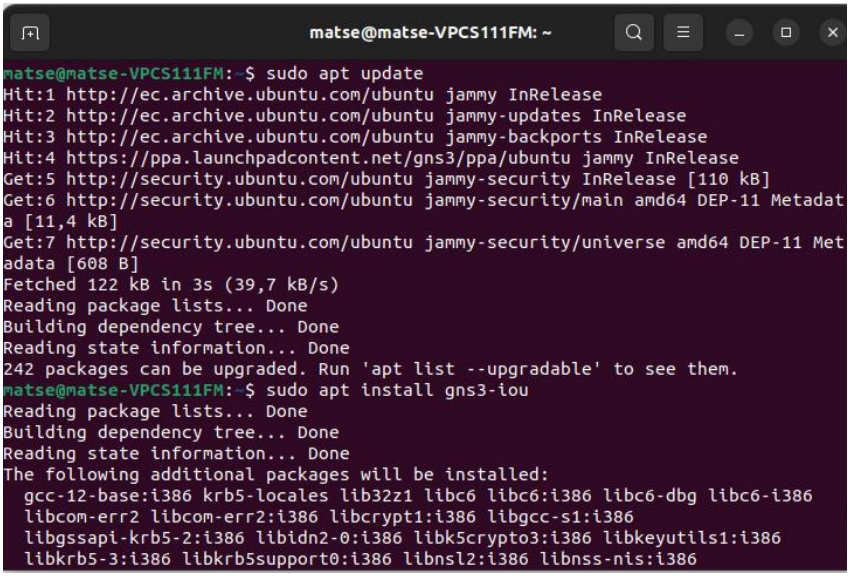
Ingreso de la arquitectura de GNS3



Nota. La figura muestra el ingreso de los comandos de actualización y arquitectura del software gns3.

Figura 117

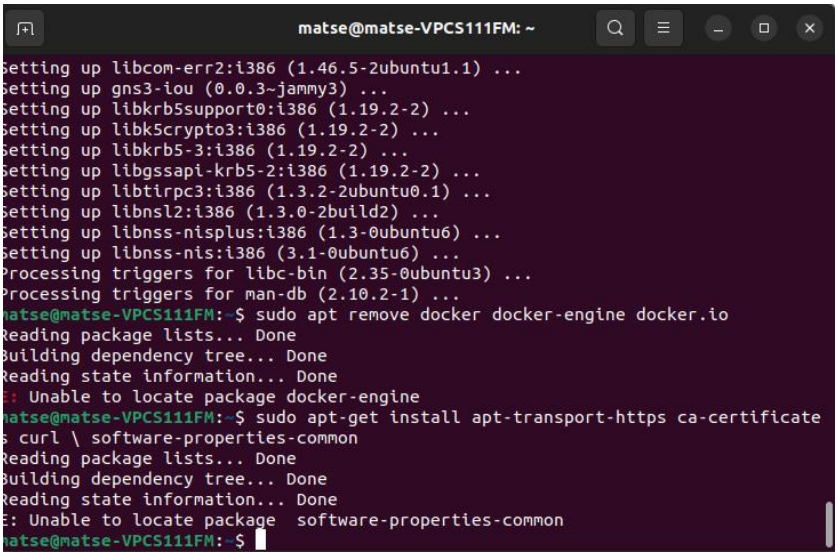
Instalación del software de simulación GNS3



Nota. En la figura se observa el comando para la instalación de GNS3 por lo que ingresamos el siguiente “sudo apt install gns3-iou”

Figura 118

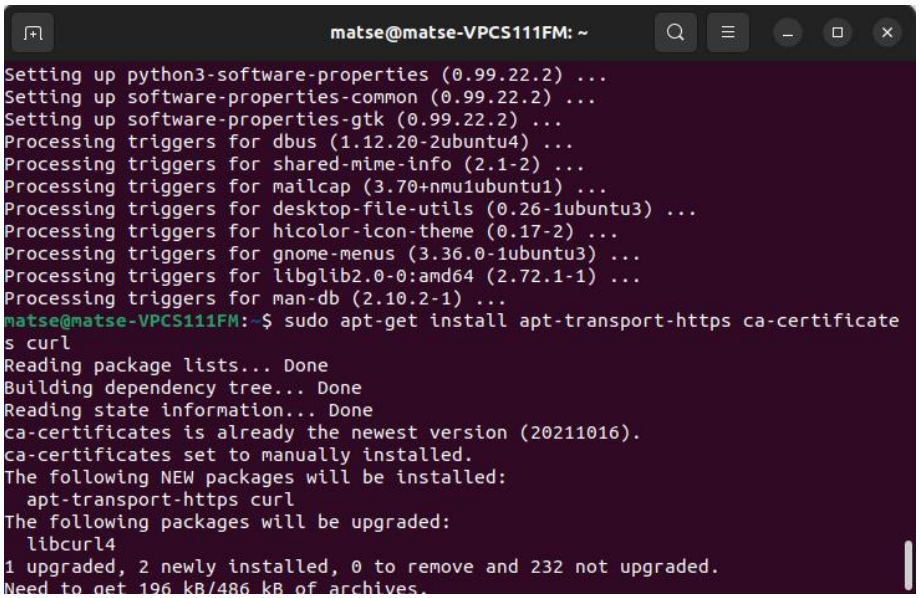
Ingreso del Docker de GNS3



Nota. La figura presente indica la instalación del Docker el cual nos permite automatizar un despliegue de aplicaciones dentro de los contenedores de software.

Figura 119

Instalación de la certificación de GNS3



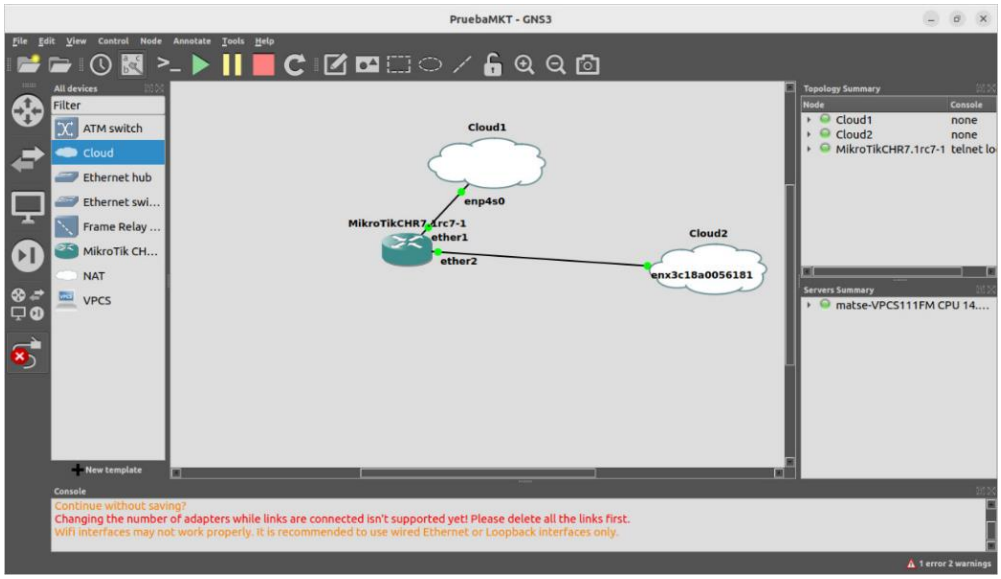
Nota. La figura muestra el comando para el ingreso de la certificación de GNS3.

Configuración del Portal cautivo en el RouterOS MikroTik

Paso 1. Se inicia desarrollando la topología usando un router y dos nubes (acceso a internt), la una será el ingreso por LAN (el cual será conectado a la red de área local) y la otra es la salida por WAN (que permite conectarse a una red de área amplia), esto permite que al momento configurar los puertos de red ethernet 00 y ethernet 01, contengan tarjetas de red correspondientes, esto se observa en la figura 120. En la figura 121 se visualiza el arranque del router para proceder a la respectiva configuración.

Figura 120

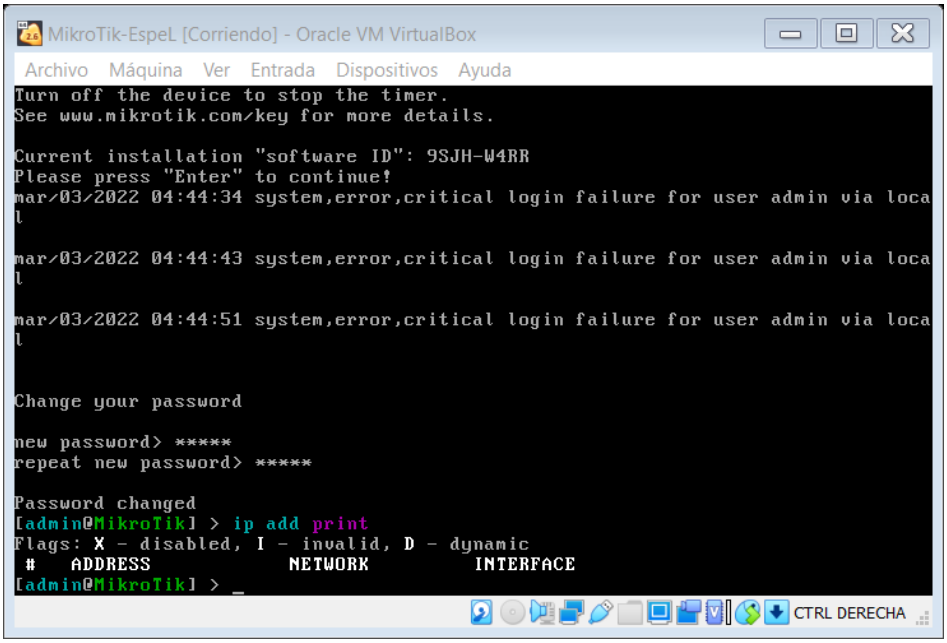
Topología de red Hotspot



Nota. EN la figura se observa el desarrollo de la topología a usarse para la creación del portal cautivo

Figura 121

Ventana principal del software de simulación RouterOs MikroTik

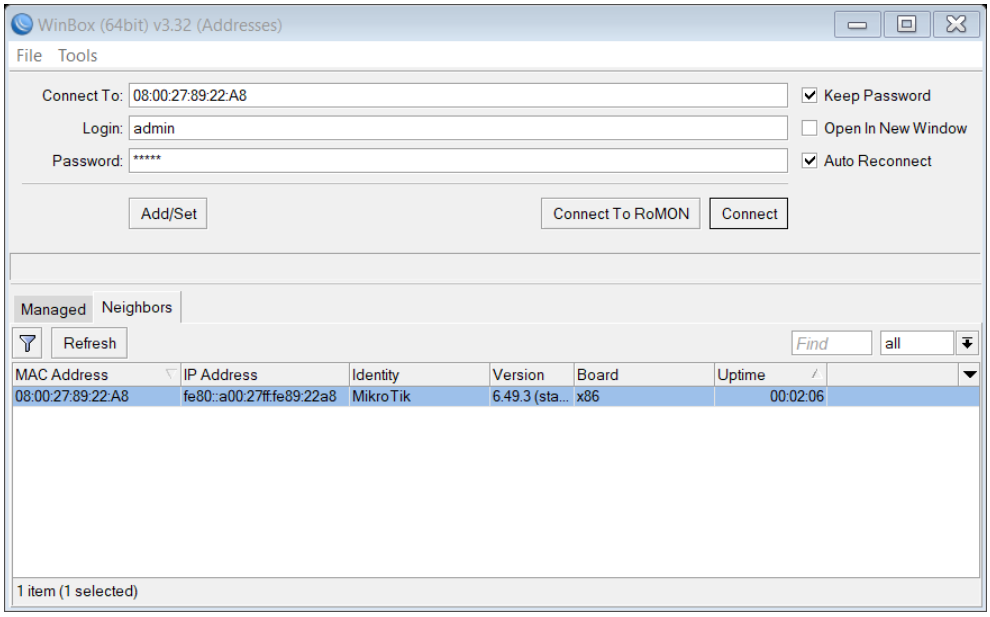


Nota. En la figura presente se muestra las opciones de arranque del software de simulación MikroTik, en donde digitaremos el password y el comando de visualización de las direcciones IP en las interfaces.

Paso 2: Como segundo paso se procede a dar inicio de la aplicación Winbox para continuar con la configuración del software de simulación Router Mikrotik, por lo cual una vez iniciada lo que se observa es la dirección MAC de nuestra tarjeta de red configurada en nuestra máquina virtual, por lo que selecciona con un clic izquierdo sobre la misma y luego digitando en el Login “admin” y en el password “admin” para después proceder a dar un clic izquierdo en el botón que dice “Connect” para conectar e iniciar las configuraciones en el sistema. Para lo cual una vez iniciada lo que se visualiza es una ventana de verificación de una licencia en donde le daremos clic izquierdo en el botón “OK”, en las figuras 122 y 123, se muestra lo mencionado en este desarrollo.

Figura 122

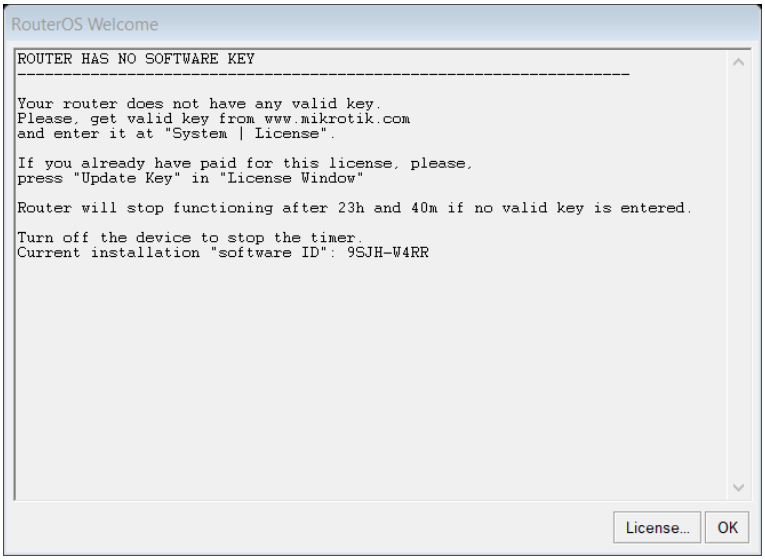
Ventana de configuración del Winbox



Nota. La figura, certifica que una dirección MAC por la cual se va ingresar y configurar.

Figura 123

Ventana de verificación de licencia del RouterOs

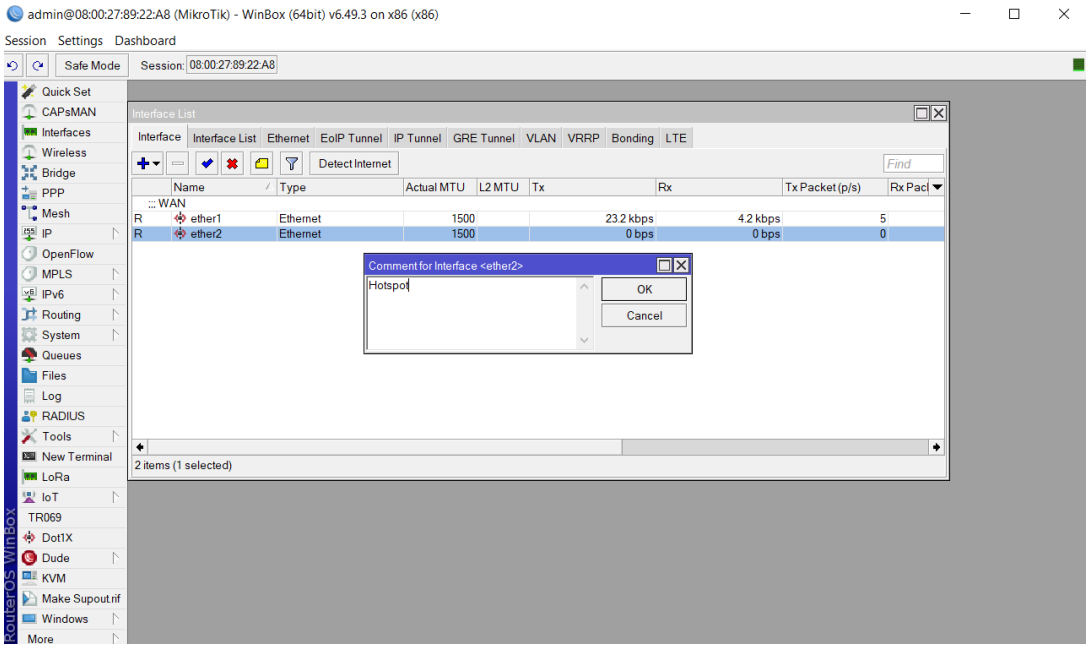


Nota. En la figura se observa de la verificación de si se tiene o no una licencia con respecto al RouterOs MikroTik.

Paso 3. Se coloca notas sobre las interfaces para poder reconocerlas más adelante; En la Ether1 se agrega el nombre “WAN” y en la Ether2 se coloca el nombre “Hotspot”. Luego lo que procede es crear un DHCP Client como se evidencia en las siguientes figuras124, 125, 126 y 127.

Figura 124

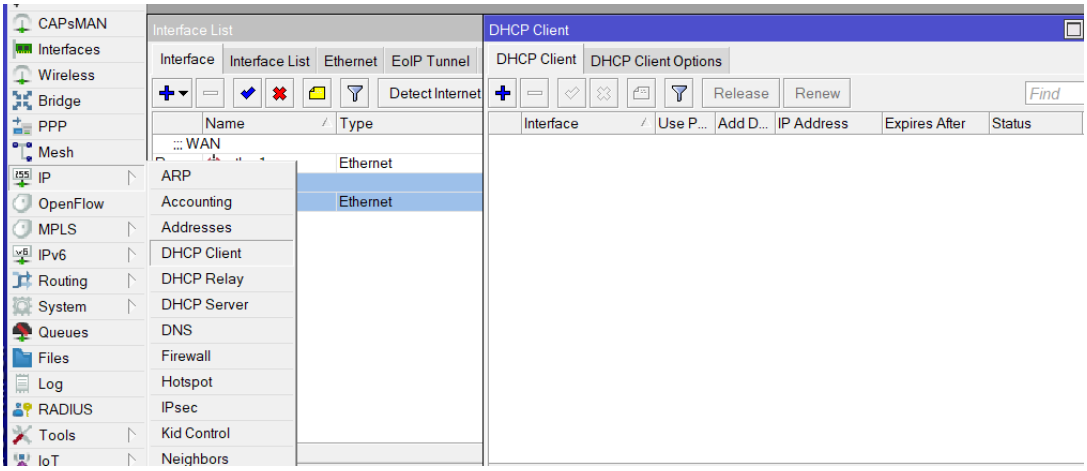
Creación de notas en las interfaces de red



Nota. La figura, muestra de la forma de cómo crear notas para las interfaces de red y que nombre a cada una de ellas.

Figura 125

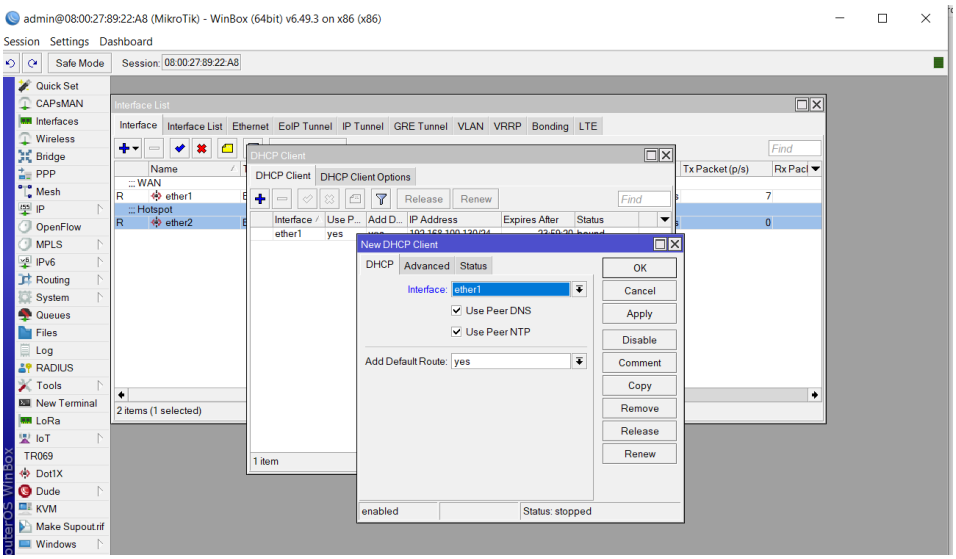
Forma de selección de un DHCP Client



Nota. En la figura se observa cómo realizar la creación de un DHCP Client.

Figura 126

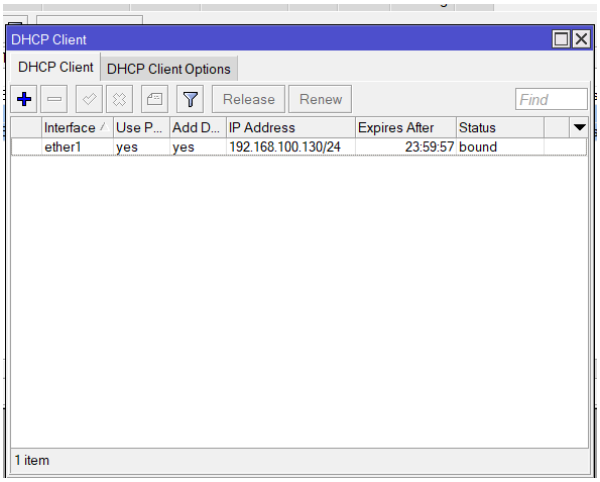
Creación de un DHCP Client en la interfaz



Nota. La figura indica la forma correcta de la creación de un DHCP Client y a la vez de la correcta asignación de la interfaz el enrutamiento de la misma.

Figura 127

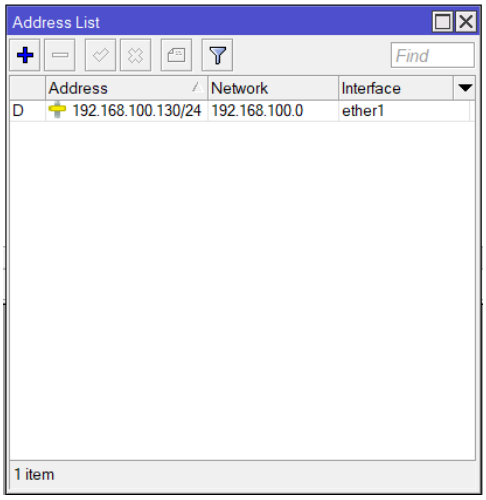
Visualización de la creación del DHCP Client



Nota. En la figura se verifica la correcta creación del DHCP Client y en la cual se evidencia los datos asignados hacia la misma.

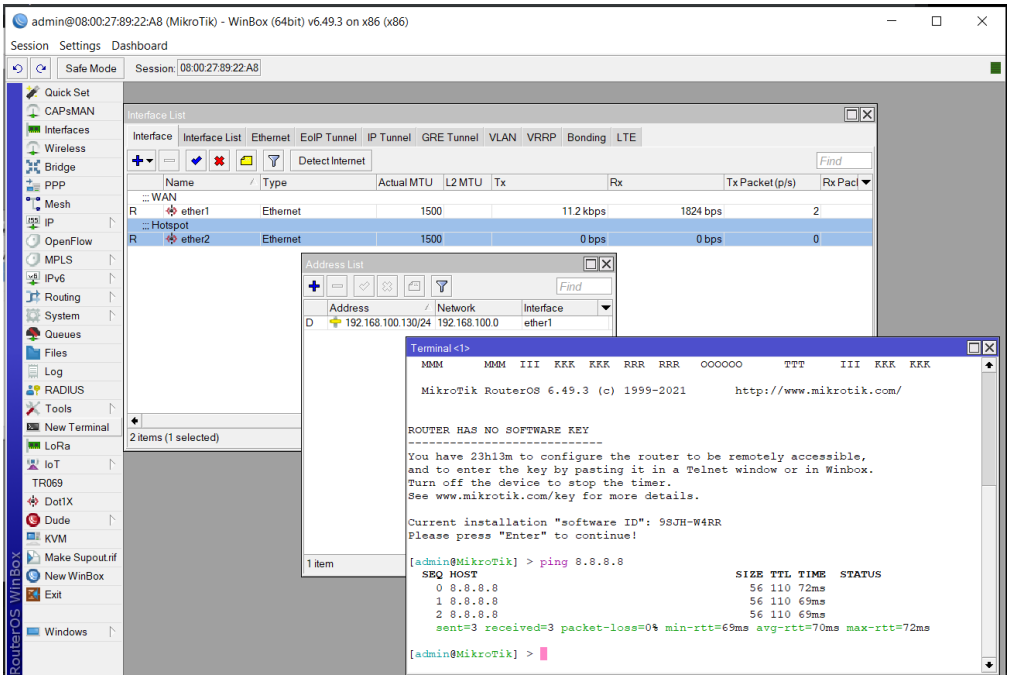
Paso 4. Se realiza la verificación de la conectividad con los servidores públicos de Google, para lo cual se visualizar dentro del CMD del sistema mismo si existe conectividad o no, colocando en la pantalla del terminal “ping 8.8.8.8” para testear y observar que sucede. Pero antes que eso debemos identificar que exista una dirección IP dentro de la lista de las interfaces dado mediante la conectividad DHCP de nuestro router del domicilio en las figuras 1285 y 129 se presencia lo desarrollado en este paso.

Figura 128 *Observación de Dirección IP dado por DHCP*



Nota. La figura certifica la existencia de una dirección IP Dinámica por la cual procederá a pasar o enviar datos hacia nosotros y generar la navegación de internet.

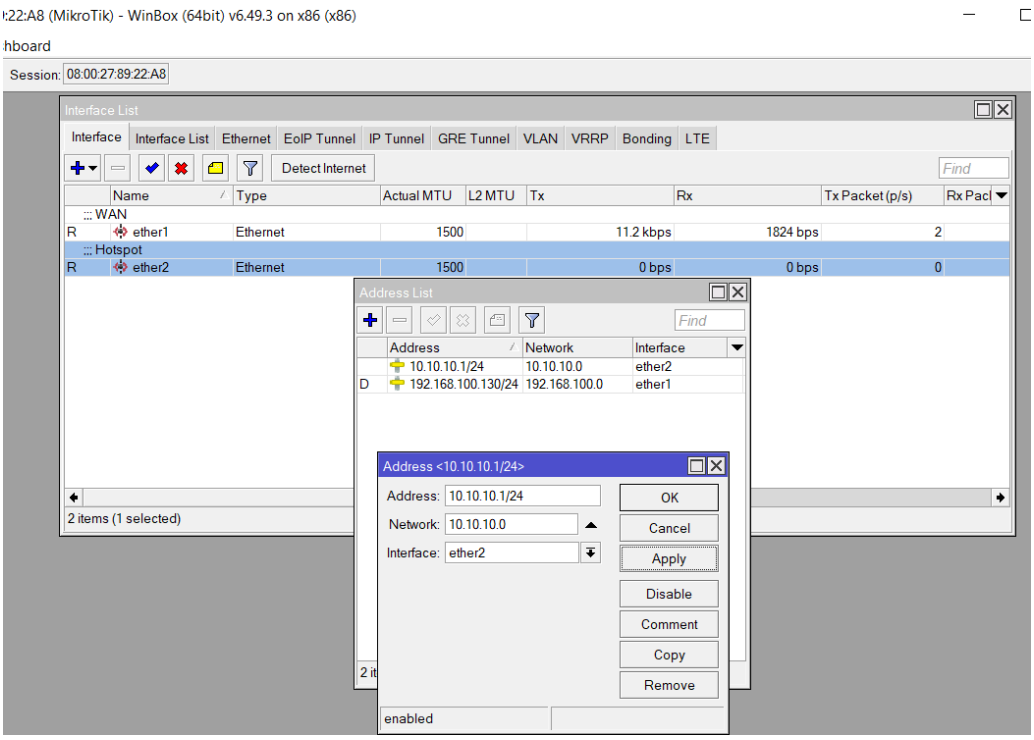
Figura 129 *Testeo de Ping con el servidor público de Google*



Nota. En la figura se observa la existencia de conectividad que existe con el servidor público de Google, efectuando un ping hacia la misma.

Paso 5. En la figura 130, se desarrolla la creación de un direccionamiento IP para lo cual se digita la siguiente IP “10.10.10.1/24” y se selecciona la interfaz Ether2. Luego se procederá a dar un clic izquierdo en el botón “OK”.

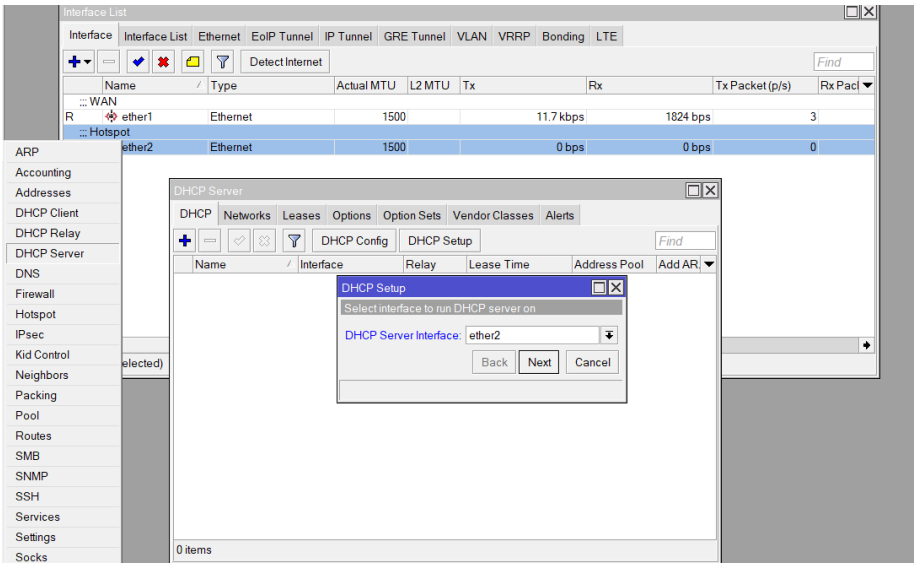
Figura 130 *Creación de una nueva dirección IP*



Nota. La figura evidencia la creación de una dirección IP y de la asignación hacía que interfaz será designada dicha IP.

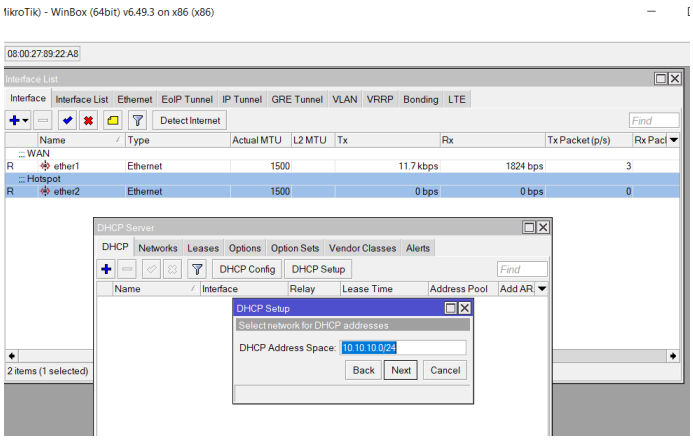
Paso 6. Luego lo que proceden a realizar es la creación de un nuevo DHCP Server con la asignación hacia la Ether2, la dirección IP creada anteriormente, el Gateway que es proporciona por defecto en la configuración, el DNS Server se elige el que es dado por defecto, el tiempo será el por defecto; Listo lo que resta por hacer es la verificación de la creación del DHCP Server y observar que todo está correctamente como se desea tener, en la figuras 131, 132, 133, 134, 135, 136 y 137 se aprecia lo aplicado en este paso.

Figura 131 *Selección de interfaz y Creación de un nuevo DHCP Server*



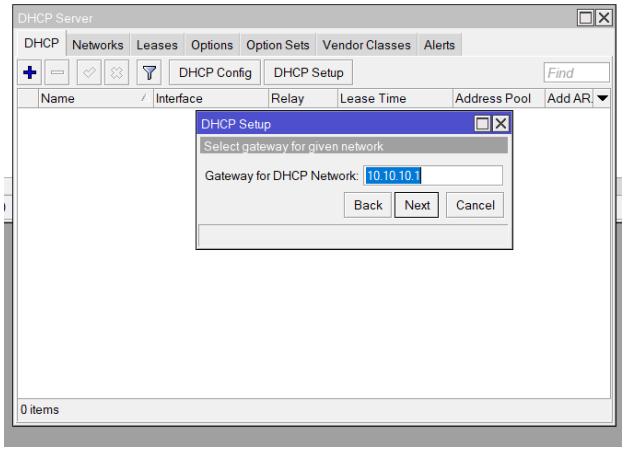
Nota. En la figura, se visualiza la selección de interfaz a la cual será asignada nuestro nuevo DHCP Server.

Figura 132 *Selección de dirección DHCP a la red*



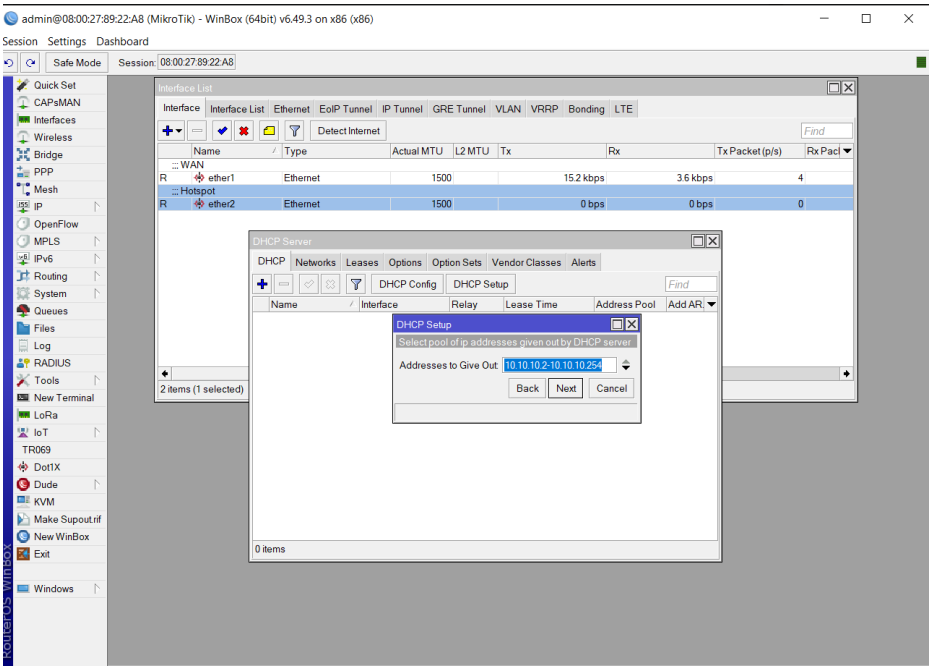
Nota. La figura, evidencia de la selección de la dirección IP escogida para la red DHCP de nuestro nuevo Server.

Figura 133 *Selección del Gateway para la red DHCP*



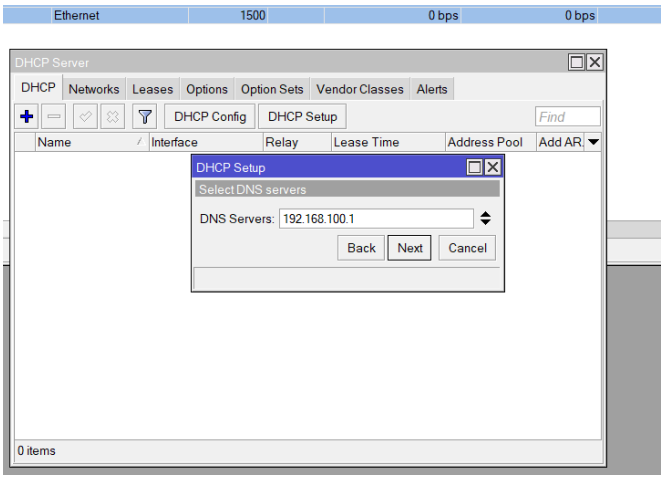
Nota. En la figura se observa cual es el Gateway que llevara el DHCP Server.

Figura 134 *Selección del rango de IP's para el DHCP*



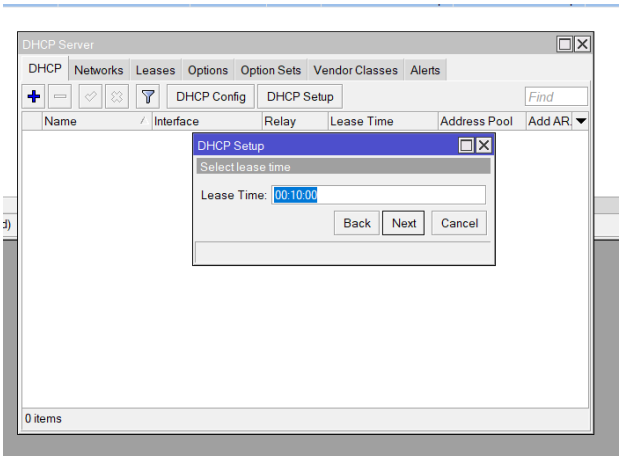
Nota. La figura se verifica el rango de IP's que tendrá el DHCP Server y por la cual se generaran automáticamente en nuestros dispositivos cuando se conecten.

Figura 135 *Selección del DHCP Server*



Nota. En la figura certifica la selección del DNS Server para lo cual será la que da por defecto la configuración.

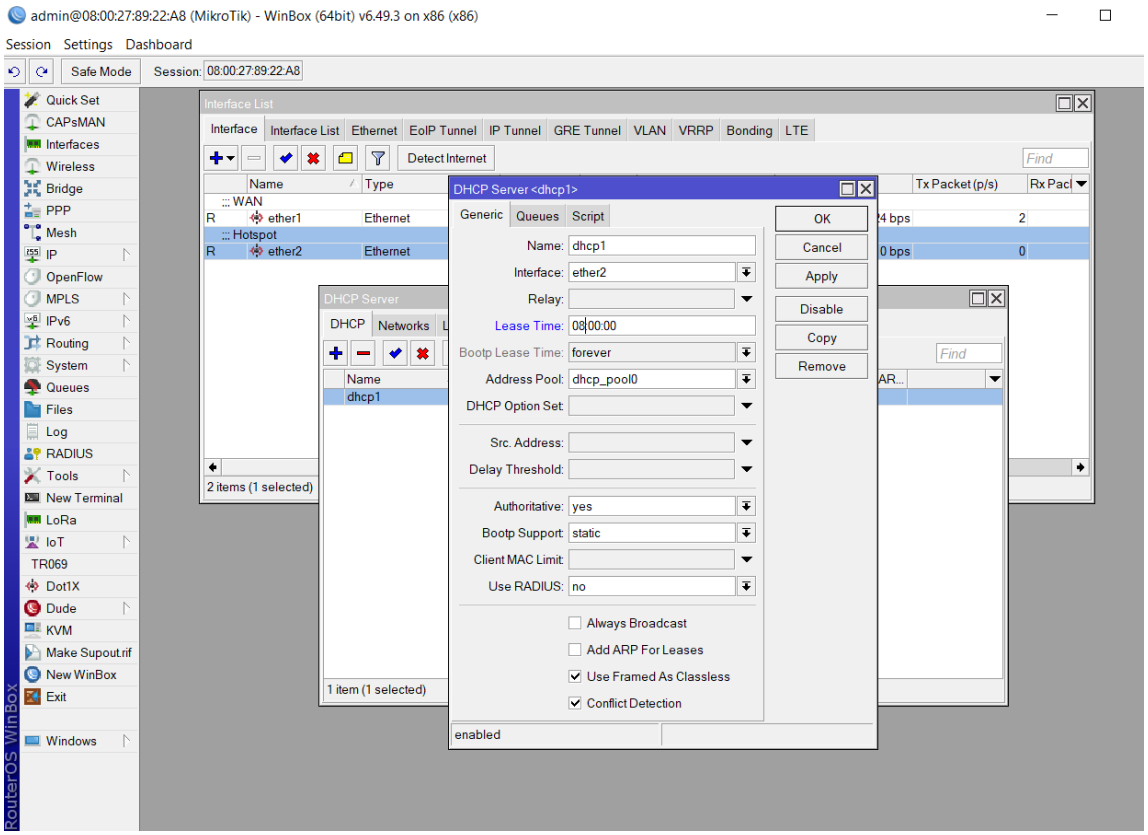
Figura 136 *Selección del tiempo de arrendamiento*



Nota. En la figura se observa el tiempo que se escoge para la parte de arrendamiento de nuestro servicio con respeto al Hotspot.

Figura 137

Verificación de nuestro Nuevo DHCP Server

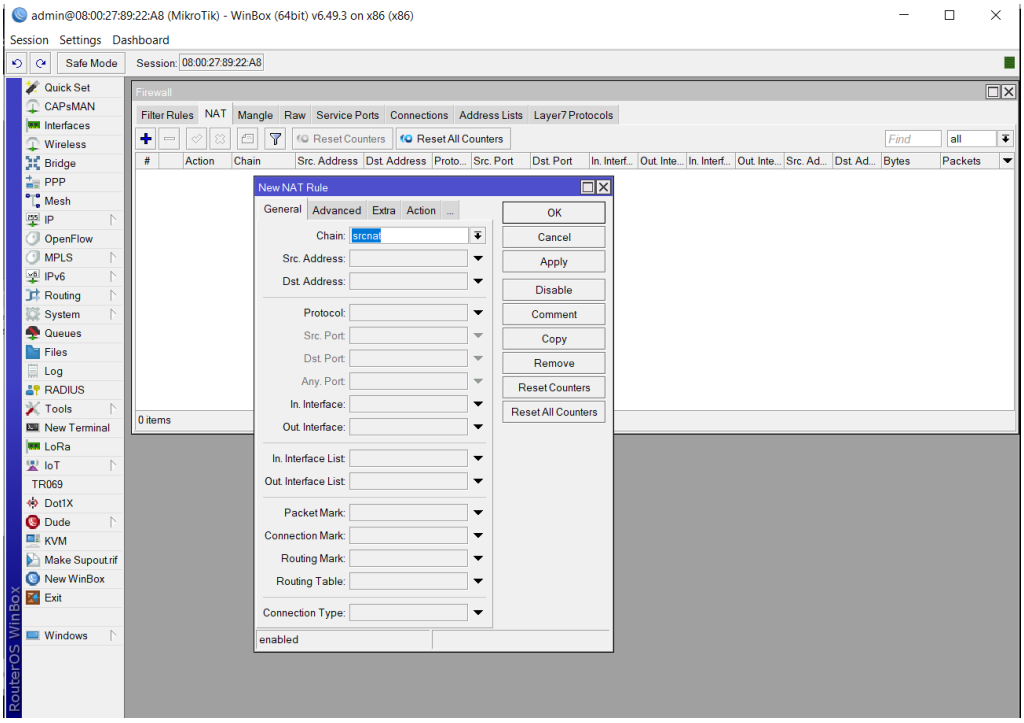


Nota. En la figura muestra la creación del nuevo DHCP Server, con las respectivas configuraciones.

Paso 7. Creación de intercambio de paquetes entre las dos redes anteriormente creadas pero que están asignadas mutuamente, para lo cual se necesita ir a la barra de opciones que dice Firewall y después a la pestaña que dice NAT y proceder con la creación de nuestra nueva regla. La opción a escoger será la siguiente “srcnat” e iremos a la viñeta que dice Action para seleccionar “masquerade” y finalizaremos dando un clic izquierdo en el botón “OK”, las siguientes figuras 138, 139 y 140 muestran lo realizado en este paso.

Figura 138

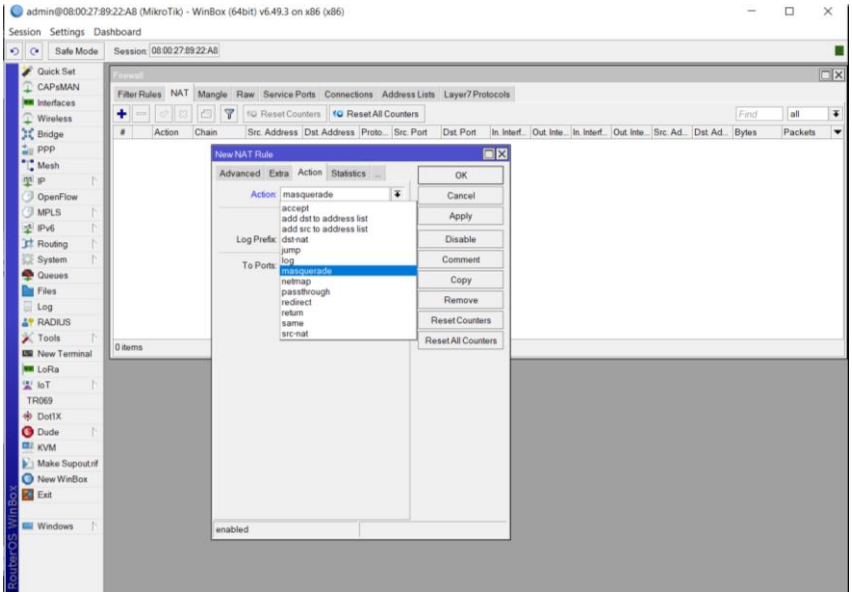
Creación de reglas en NAT



Nota. La figura certifica la forma correcta de cómo se debe crear una nueva regla NAT al seleccionar “srcnat”.

Figura 139

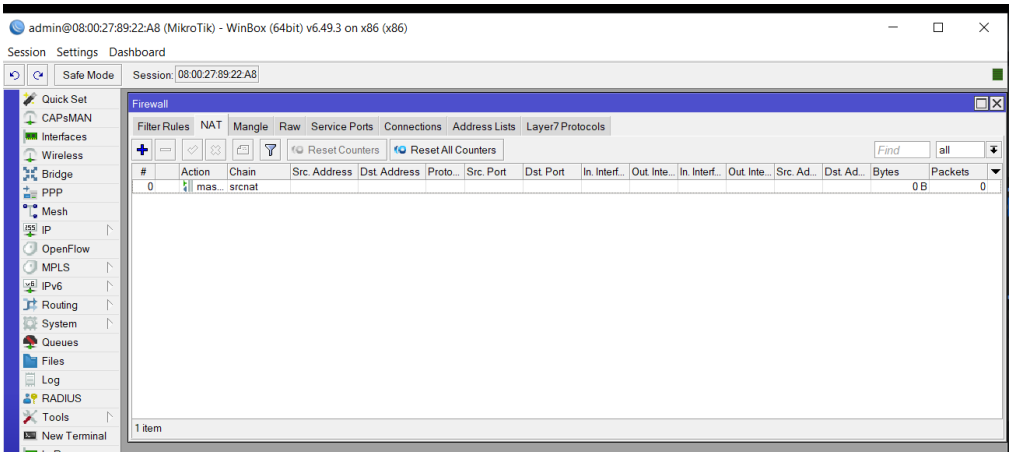
Selección de la acción que realizará la nueva regla



Nota. En la figura selecciona de la acción que se debe mostrar en la nueva regla opte, y por la cual será seleccionada la accion de “masquerade”.

Figura 140

Verificación de la Nueva regla creada

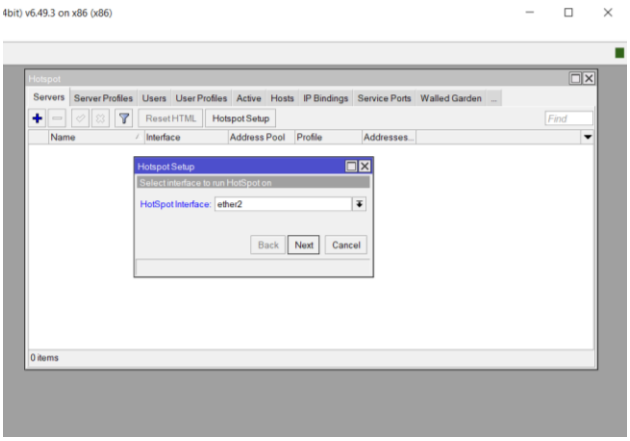


Nota. La figura indica el firewall creado correctamente dentro de sistema operativo Zeroshell.

Paso 8. Realizar es la creación de nuestra nueva red Hotspot para lo cual se procede a dar un clic izquierdo en la barra de opciones la que nos dirá Hotspot y la selección de cada una de las configuraciones que indica dicho apartado, por lo cual la interfaz hacia el Hotspot a escoger será la “Ether2”, luego la dirección de red local será la creada anteriormente, el rango de IP’s será obviamente el que se muestra por defecto la configuración, en el certificado lo que se elija es la que dice “none”, la dirección IP del servidor SMTP será la que viene por defecto, en el DNS Server se selecciona las que son públicas para Google como son “8.8.8.8” y la “8.8.4.4”. Además, para el nombre del DNS no se escoge nada y queda en blanco para que no exista un conflicto después, Finalmente se escoge un nombre para el usuario el cual es “admin” y una contraseña “admin” y finalmente se hace un clic izquierdo en el botón Ok, para concluir con la creación de nuestro nuevo Hotspot, las siguientes figuras 141, 142, 143, 144, 145, 146, 147. 148 y 149, lo mencionado en este paso de configuración del portal cautivo.

Figura 141

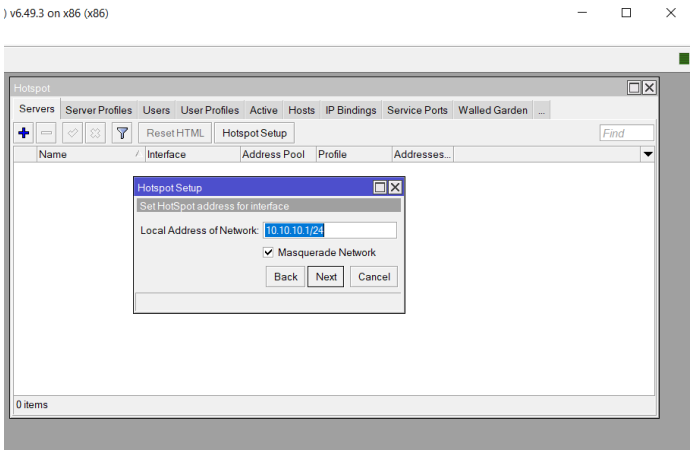
Asignación de la interfaz con relación al Hotspot



Nota. La figura muestra la correcta selección del puerto al que se va asignar al nuevo Hotspot y la cual se escoge la interfaz “Ether2”.

Figura 142

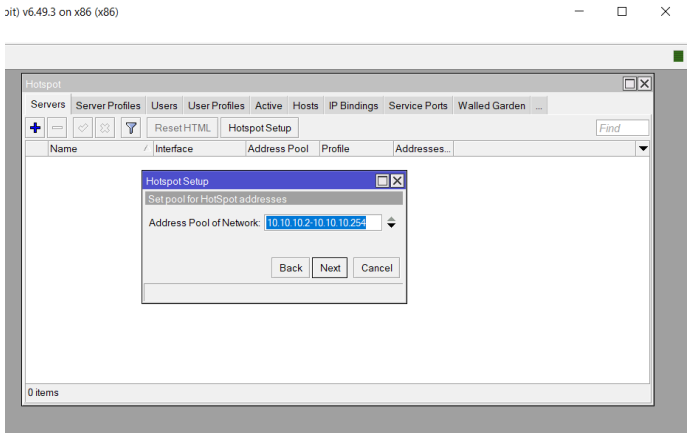
Selección de la dirección de red local



Nota. La figura se observa la selección de la dirección de red local que se escoge para el Hotspot.

Figura 143

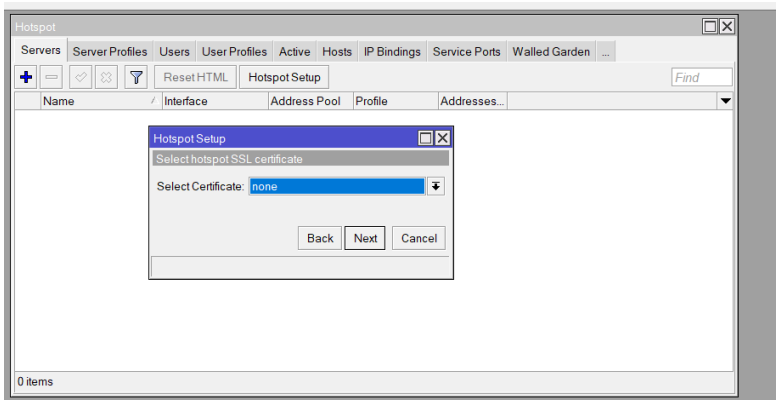
Selección de los Rangos de IP's de la red



Nota. La figura se evidencia el rango de IP's que se tomara en cuenta en la creación de del Hotspot y la cual tendrán nuestros dispositivos cuando se enlacen con la misma.

Figura 144

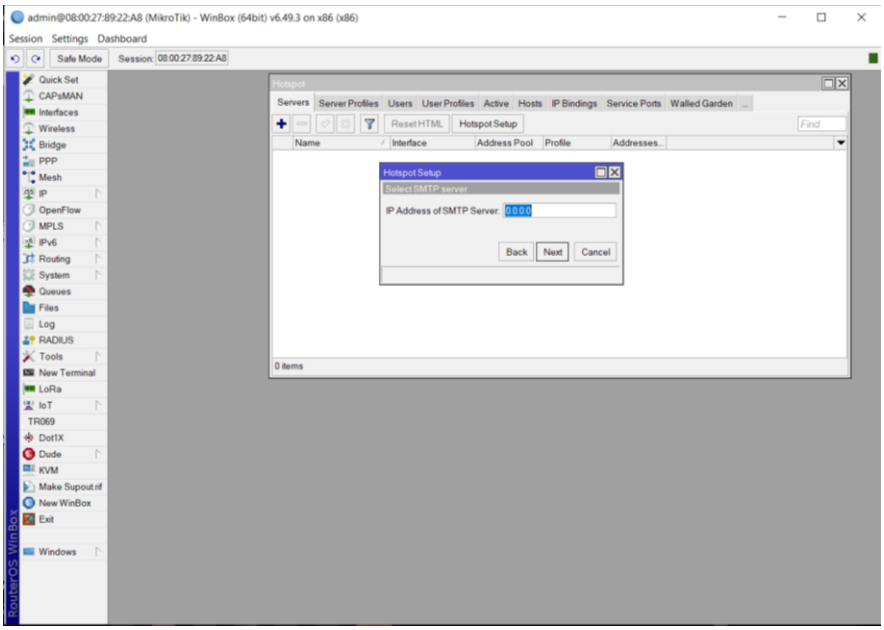
Selección del certificado del Hotspot



Nota. En la figura se visualiza la selección de “none” porque no está asignado o no se desea el certificado referente al Hotspot.

Figura 145

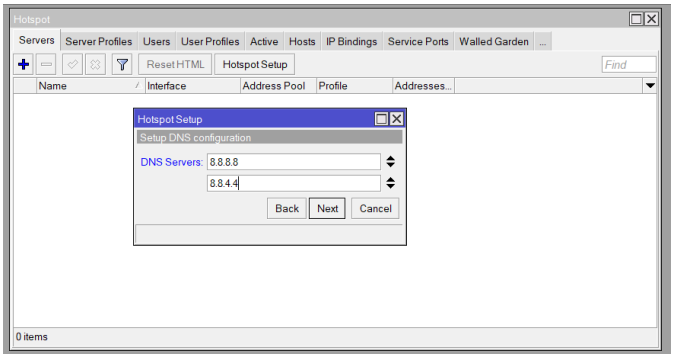
Selección de Dirección IP del servidor



Nota. La figura se ve la no selección de una dirección IP con respecto al servidor por lo cual se la dejara la que viene por defecto.

Figura 146

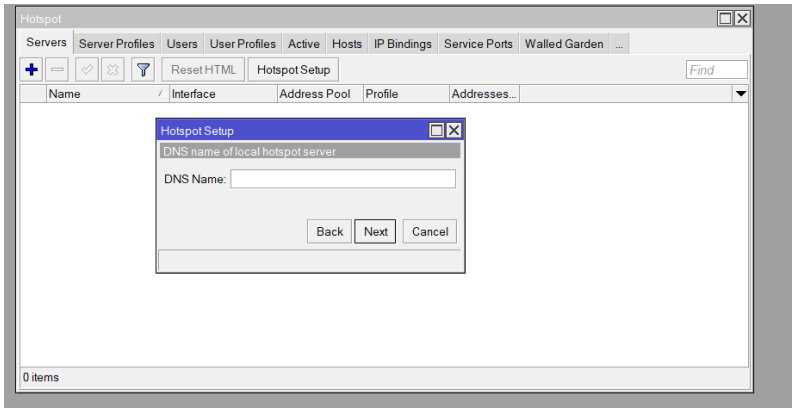
Digitación del DNS Server



Nota. En la figura se realizarla digitación del DNS Server para lo cual será la siguiente “8.8.8.8” y “8.8.4.4”.

Figura 147

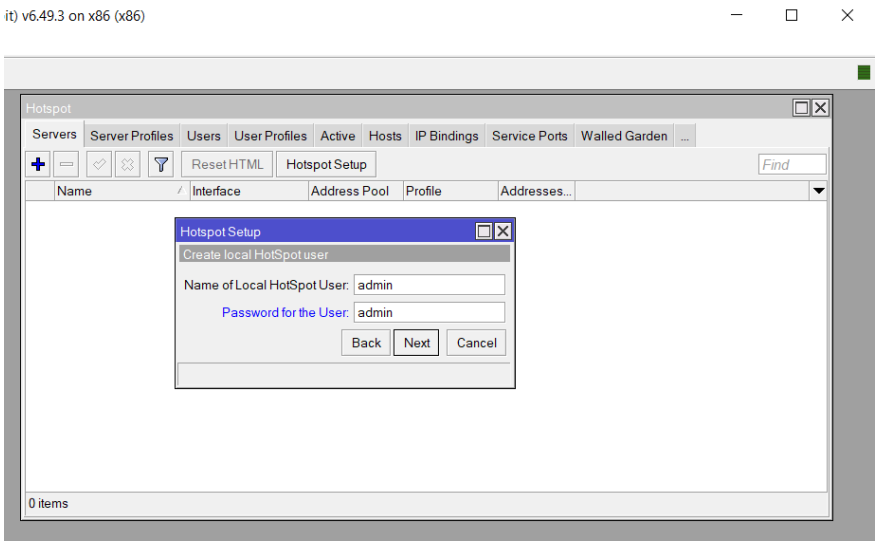
Digitación de Nombre al DNS



Nota. La figura se observa que no existe ninguna digitación con respecto a la asignación de algún nombre en el DNS.

Figura 148

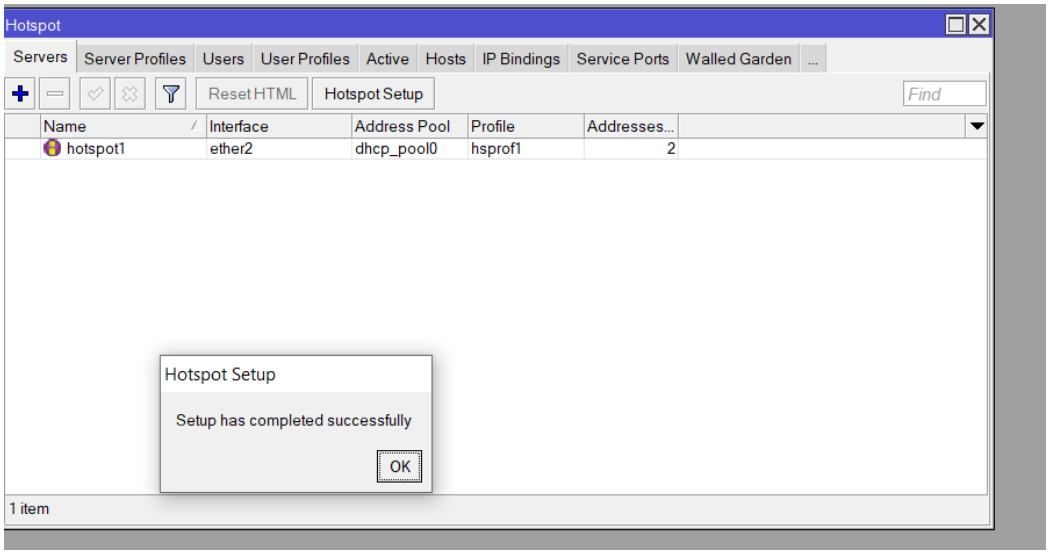
Digitación de un Nombre y Contraseña al Hotspot



Nota. En la figura realizaremos la digitación de un nombre y contraseña para proceder con el ingreso hacia la interfaz de red. La cual el nombre es “admin” y contraseña “admin”.

Figura 149

Verificación del Nuevo Hotspot ha sido completado

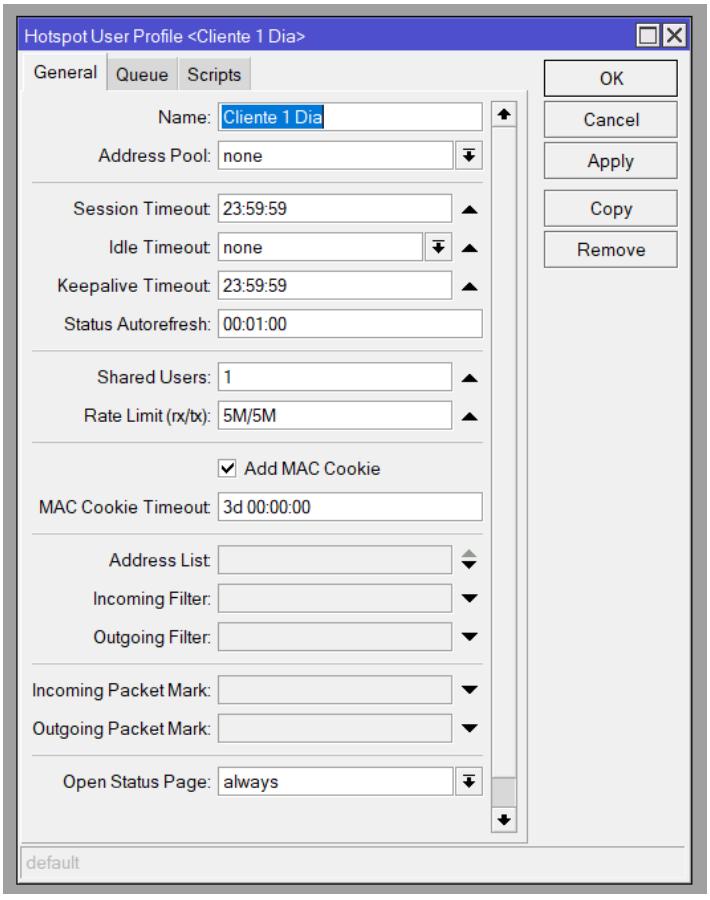


Nota. La figura muestra la notificación de que ha sido creado con éxito el nuevo Hotspot con todas sus configuraciones anteriormente.

Paso 9. Se realiza la creación de los usuarios y contraseñas para el respectivo ingreso ordenado hacia la navegación dentro del Hotspot, para lo que se procede a dar un clic izquierdo en la pestaña que dice “User Profile” y realizar el llenado de los datos que ahí solicita como un nombre, tiempo de arrendamiento, velocidad que se le asignara a cada usuario y listo, clic izquierdo en el botón “OK” para confirma dicha creación.

Figura 150

Creación de los perfiles de usuario

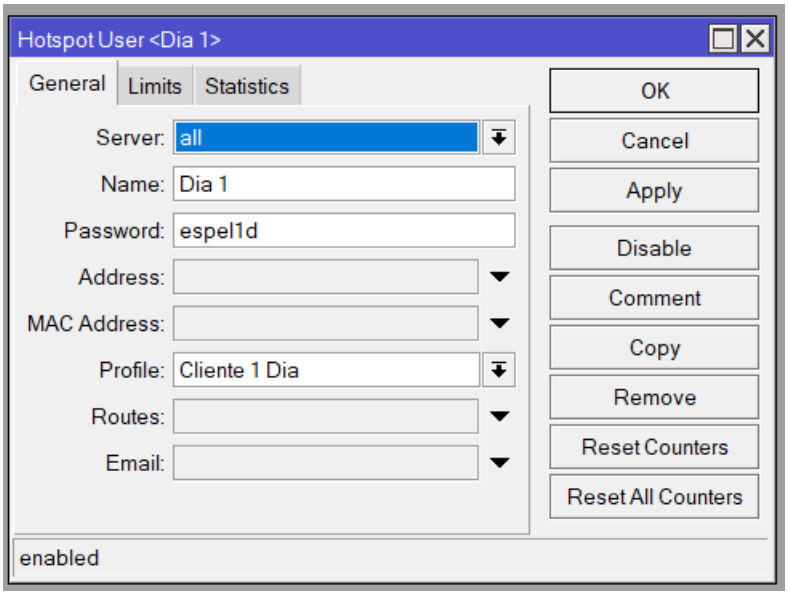


Nota. En la figura se muestra la forma correcta de la creación de un perfil de usuario para nuestra red Hotspot, con la respectiva limitación de tiempo y la cantidad de megabytes

Paso 10. Se desarrolla la asignación de los perfiles creados a los usuarios por generar donde se dirige a la pestaña “User” para crear el usuario que será definido con los parámetros anteriormente seleccionado. En el primer usuario se agrega el nombre de “Dia 1”, luego se procede asignar el perfil “Cliente 1 Dia” y una contraseña la cual será “espel1d”, se procede a darle un límite de acuerdo al tiempo que se le asigno al perfil de usuario. Para poder visualizar la clave que se está digitando, dar un clic izquierdo en la barra de opciones que dice “Settings” y luego en la opción que dice “Hide Passwords” para poder visualizar la contraseña digitada. Este proceso lo repetiremos un sin número de veces de acuerdo con la cantidad de perfiles que se van a creado, para proceder con la asignación y el orden correcto de navegación en nuestro Hotspot, en las siguientes figuras 151, 152, 153 y 154 se visualiza lo realizado en este proceso.

Figura 151

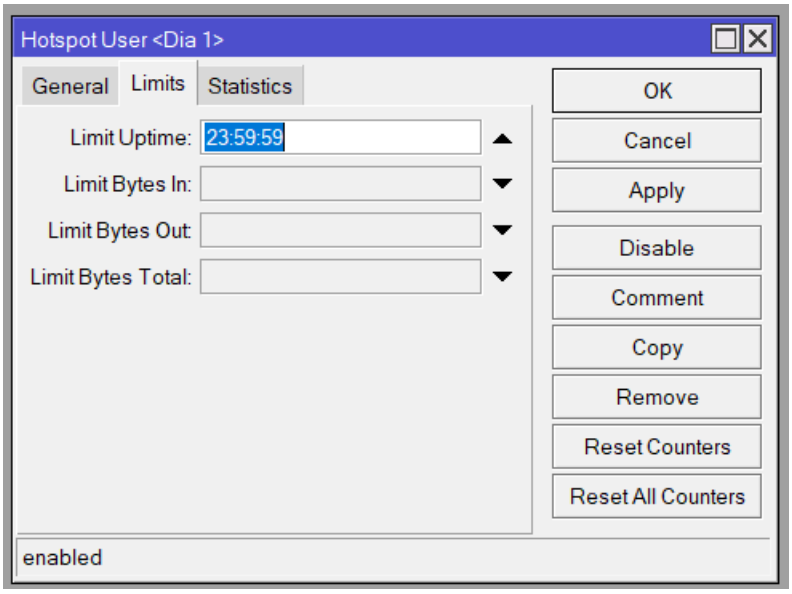
Creación y asignación de los perfiles de usuario



Nota. La figura se mira la correcta creación de un usuario con su respectiva asignación de perfil y digitación de clave personal.

Figura 152

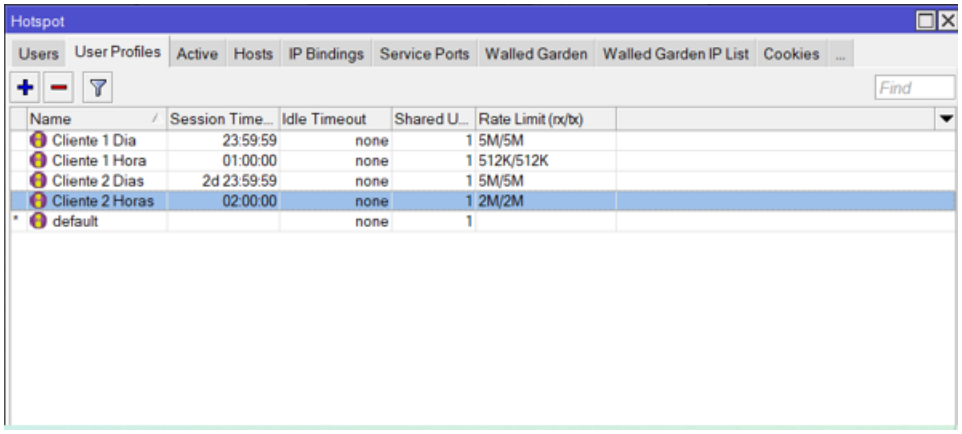
Asignación del tiempo limite



Nota. La figura se indica la asignación del tiempo límite que debe tener el usuario el mismo que coincidí con el perfil seleccionado.

Figura 153

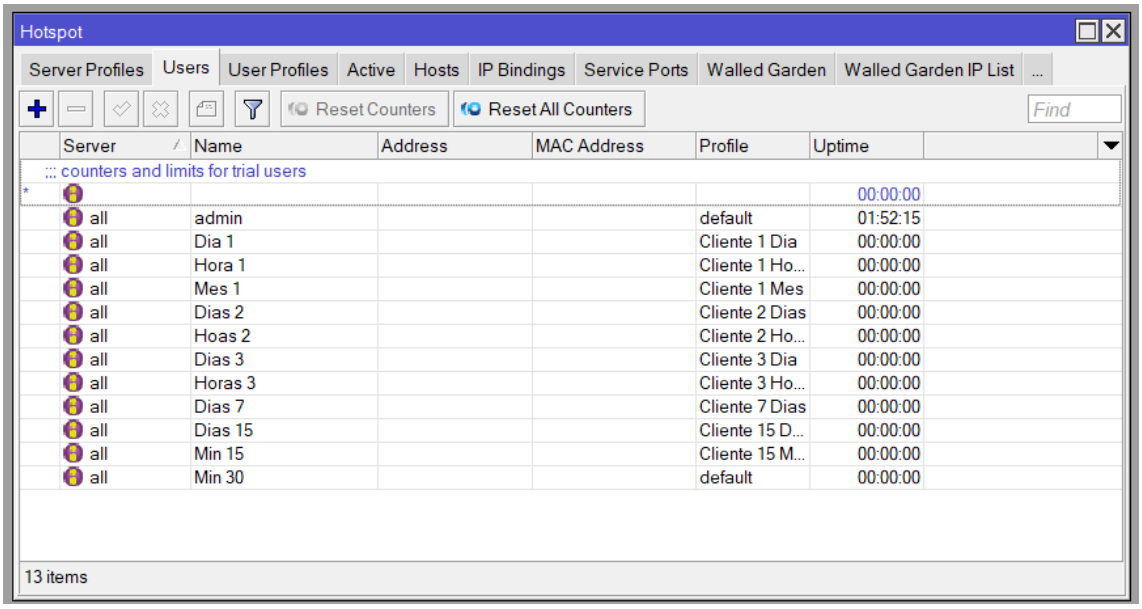
Verificación de los perfiles creados



Nota. En la figura, muestra los perfiles de usuario creados, con el tiempo de navegación y el ancho de banda que consume.

Figura 154

Verificación de los usuarios creados

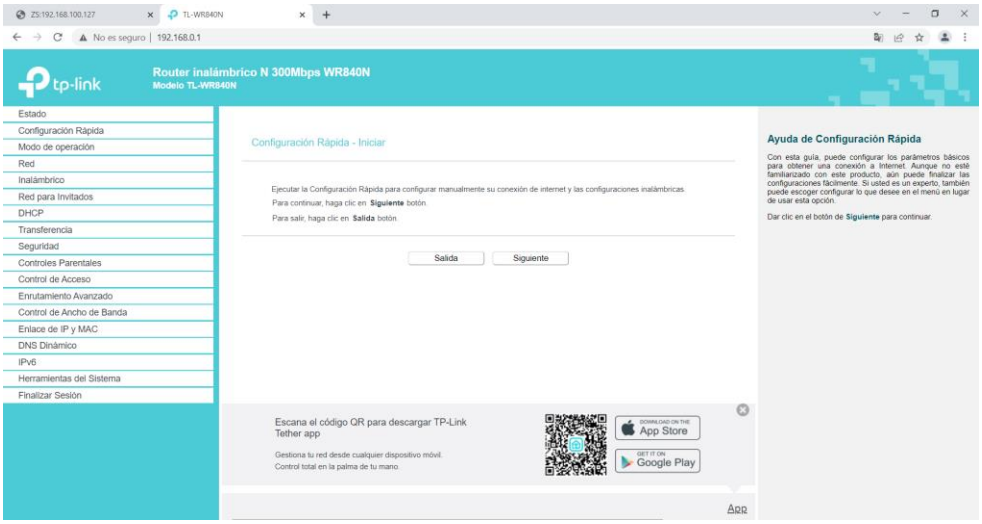


Nota. La figura nos muestra la cantidad de usuarios que fueron creados.

Paso 11. Se realiza la configuración del dispositivo router de marca TP-Link, para lo cual se procede a conectar el router con el computador mediante un cable UTP Cat6 al puerto Rj45 que se encuentra en el adaptador y se ingresa a las configuraciones del sistema colocando la siguiente IP en el navegador “192.168.0.1”; De usuario por defecto nos dará “admin” y de contraseña “admin”. Una vez dentro del sistema del TP-Link, se procede a realizar es la configuración a modo Access Point y eventualmente se cambia el nombre del equipo, la región, el tipo de seguridad y la clave para el acceso hacia el Tp-Link. Finalmente, lo que resta por hacer es aceptar los términos y condiciones que nos dará por efecto el sistema y damos un clic izquierdo en el botón “Reboot” para reiniciar y guardar los cambios efectuados dentro del sistema de configuraciones del Tp-Link. Y listo se puede conectar con facilidad al Hotspot y usar el ancho de banda designado para el mismo en las figuras 155, 156, 157, 158, 159 y 160 se indica lo desarrollado en este paso.

Figura 155

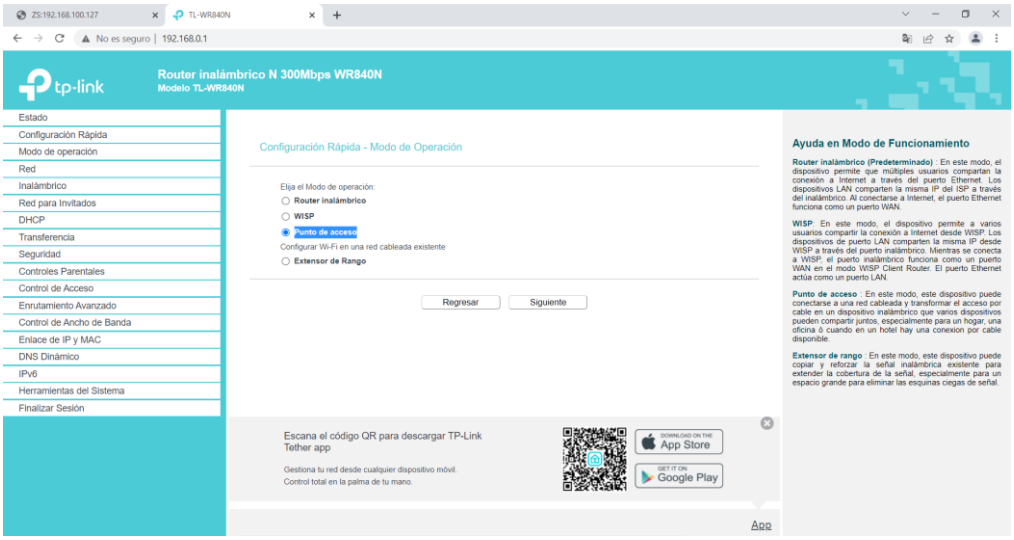
Acceso y configuración al Router TP-Link



Nota. En la figura se indica el acceso hacia el router TP-Link y el modo de configuración rápida.

Figura 156

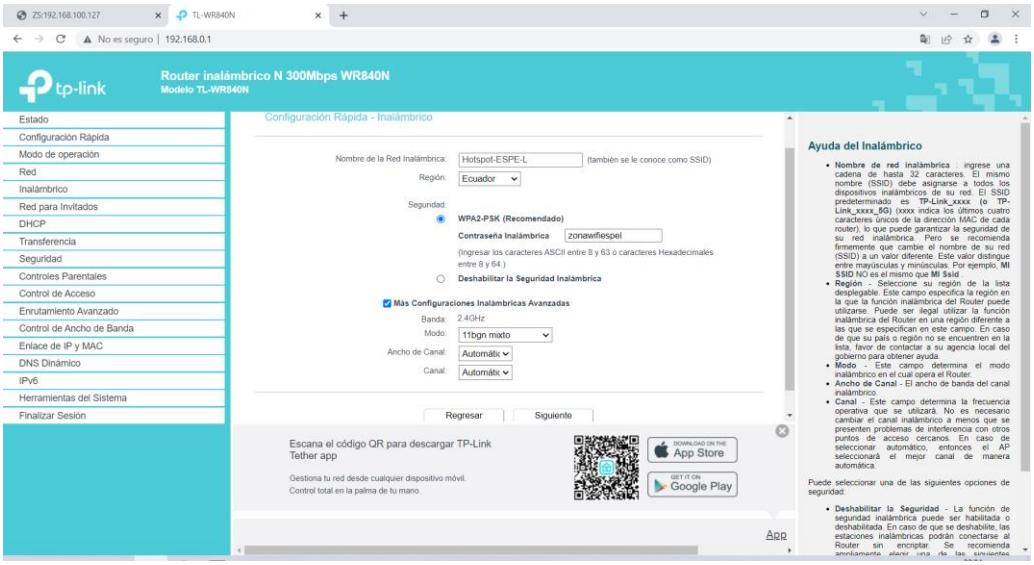
Selección del modo de operación del Router TP-Link



Nota. La figura muestra el modo de trabajo que contiene el router TP-Link para lo cual se selecciona el modo Access Point o Punto de acceso.

Figura 157

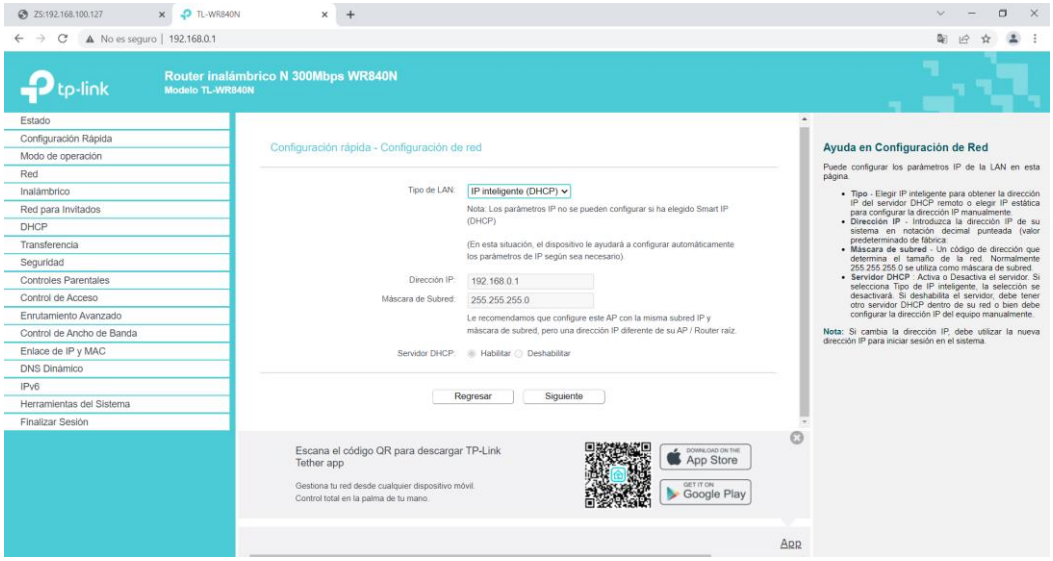
Configuraciones básicas del reconocimiento y acceso al TP-Link



Nota. En la figura se observar los cambios básicos y necesarios que se debe hacer con respecto al TP-Link y la red inalámbrica, para el ingreso y la navegación en el mismo.

Figura 158

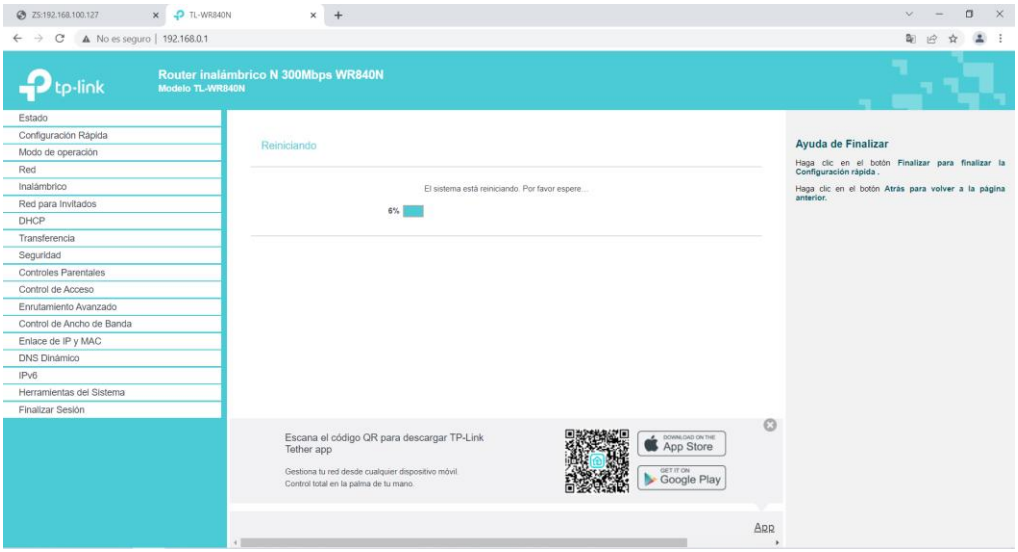
Selección de la forma de configuración de red



Nota. La figura indica la selección sobre la configuración de red que se escogio para nuestro TP-Link.

Figura 159

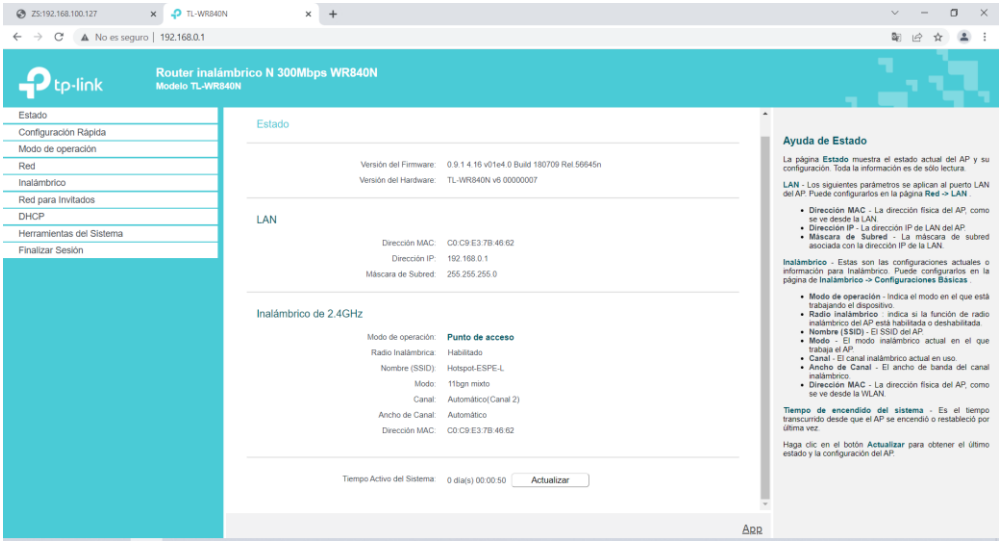
Reinicio o Reboot del sistema TP-Link



Nota. En la figura se verifica el reinició o reboot hacia el dispositivo TP-Link, para guardar y confirmar los cambios realizados en la misma.

Figura 160

Verificación del estado de red LAN e Inalámbrica del Router TP-Link

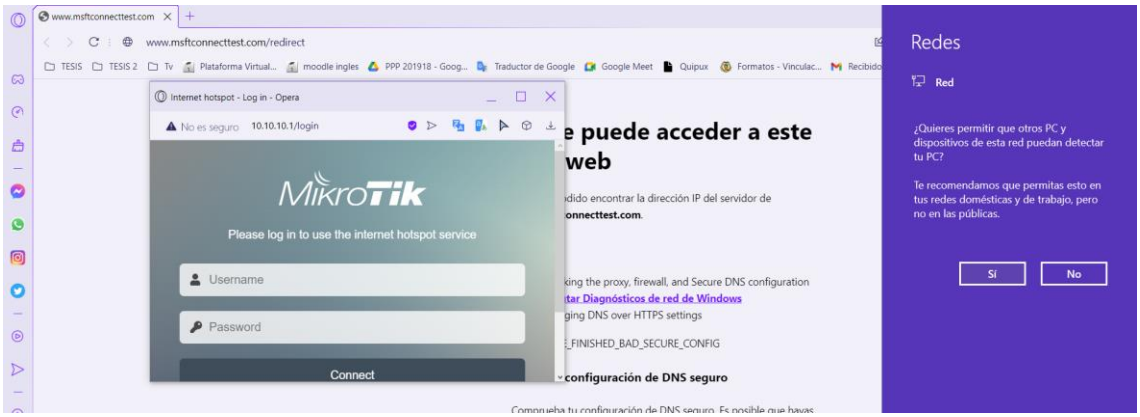


Nota. La figura de logra observar y constatar acerca de las configuraciones anteriormente realizadas y verificar sobre el estado de red en modo LAN e Inalámbricamente.

Paso 11. Una vez encendido el router TP-Link lo que se procede abrir múltiples ventanas de conectividad una de esas es el portal cautivo creado mediante el Hotspot y para la cual se debe digitar correctamente el usuario-username y la contraseña-password. Se ingresa el usuario que es “admin” y la contraseña que es “admin”, para generar el enlace de internet hacia los demás clientes que se conectaran después respectivamente con sus usuarios y contraseñas asignados. Una vez ingresado los datos lo que resta por hacer es navegar por la red, y proceder a buscar cualquier tipo de página web o plataforma que solicite transferencia de banda ancha en las siguientes figuras 161, 162, 163, 164 y 165se indica lo mencionado en este paso.

Figura 161

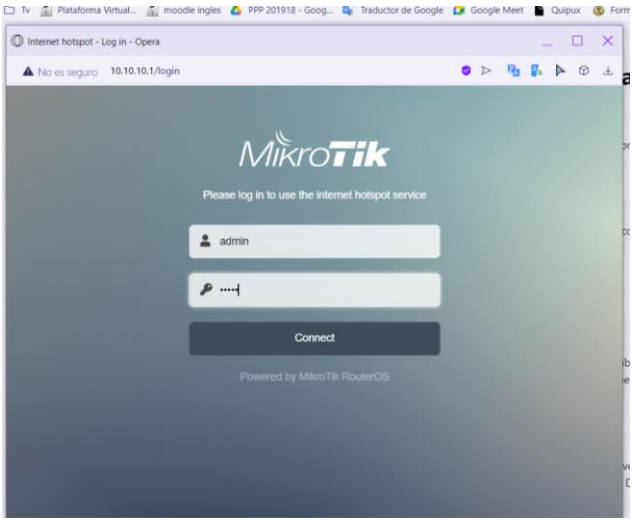
Apertura de ventanas de conectividad



Nota. En la figura se visualiza lo que se genera automáticamente la apertura de ventas de diálogo con respecto a la conectividad de del Hotspot.

Figura 162

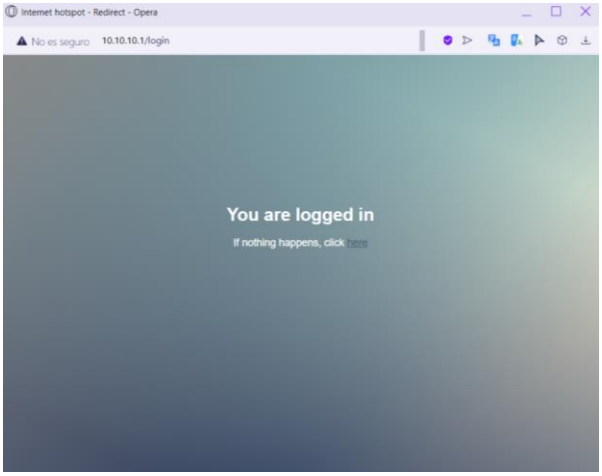
Ingreso del usuario y contraseña principal



Nota. La figura, muestra el ingreso del usuario y contraseña de nuestro principal perfil que navega la navegación con respeto a los demás clientes.

Figura 163

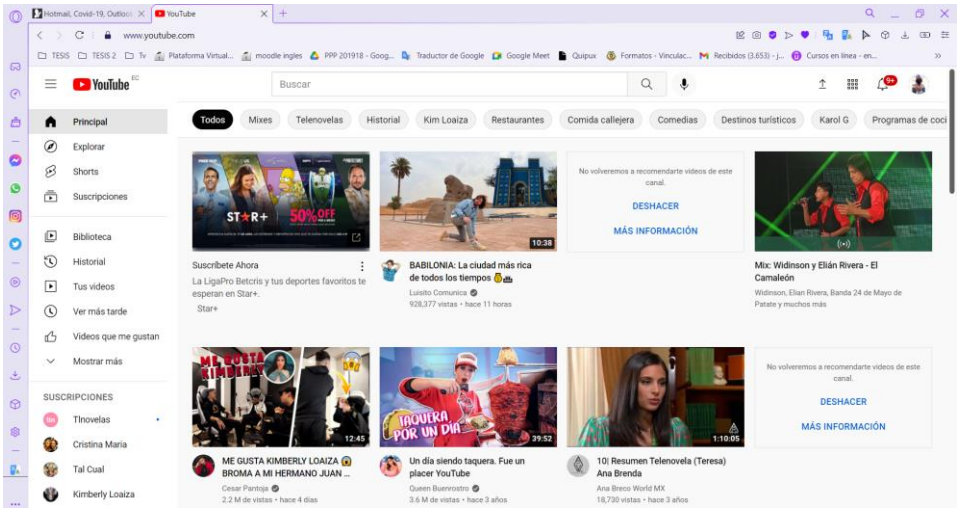
Venta de verificación de conectividad completada con éxito



Nota. En la figura indica la notificación que la conectividad se realizó con total éxito y está listo para la navegación de internet.

Figura 164

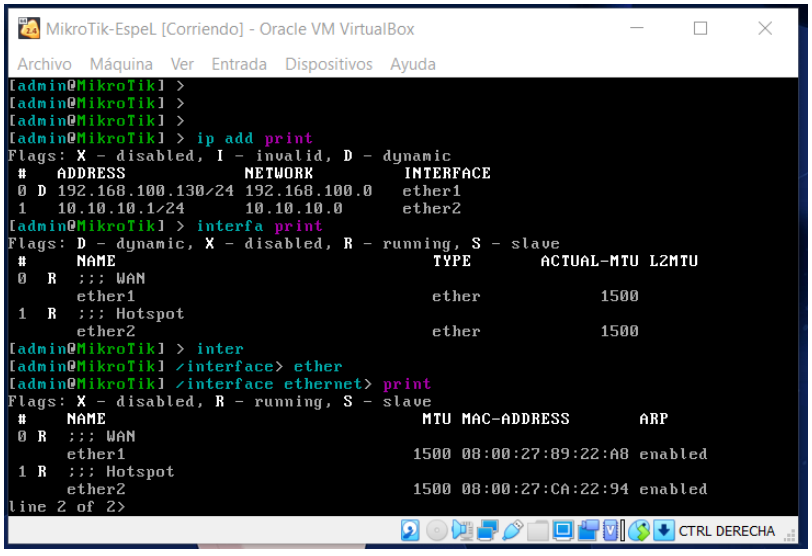
Navegación a internet



Nota. La figura evidencia la navegación de internet por lo cual está generando el ancho de banda designado con el usuario.

Figura 165

Verificación de las configuraciones en el RouterOs MikroTik

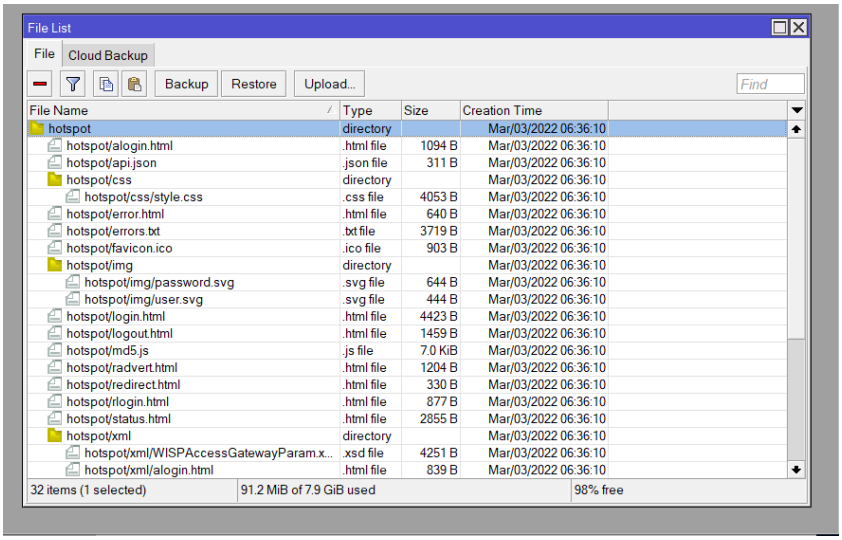


Nota. En la figura se podrá observar de todas las configuraciones realizadas dentro del software de simulación RouterOs MikroTik.}

Paso 12. Finalmente, para mejorar la estética ya la visualización de nuestro portal cautivo lo que se realiza es el cambio de entorno de trabajo para lo cual se debe eliminar la carpeta que dice “Hotspot” en el apartado que dice “File List” en la barra de opciones de nuestro software. Una vez realizado dicho paso se inicia con la búsqueda de la página principal de descarga del MikroTik y se selecciona la plantilla. Luego con un clic izquierdo y se da inicio a la descarga y descomprimimos el formato WinRAR a una carpeta normal, se hace un copiado y pegado de dicha carpeta descomprimida en el apartado que dice “File List” como reemplazo del antiguo archivo existente ahí mismo. Y listo el nuevo portal cautivo con las interacciones que el mismo nos ofrece y las visualizaciones que el mismo portal cautivo adquiere a continuación las figuras 166, 165, 167, 168, 169, 170 y 171 se muestra lo escruto en este paso.

Figura 166

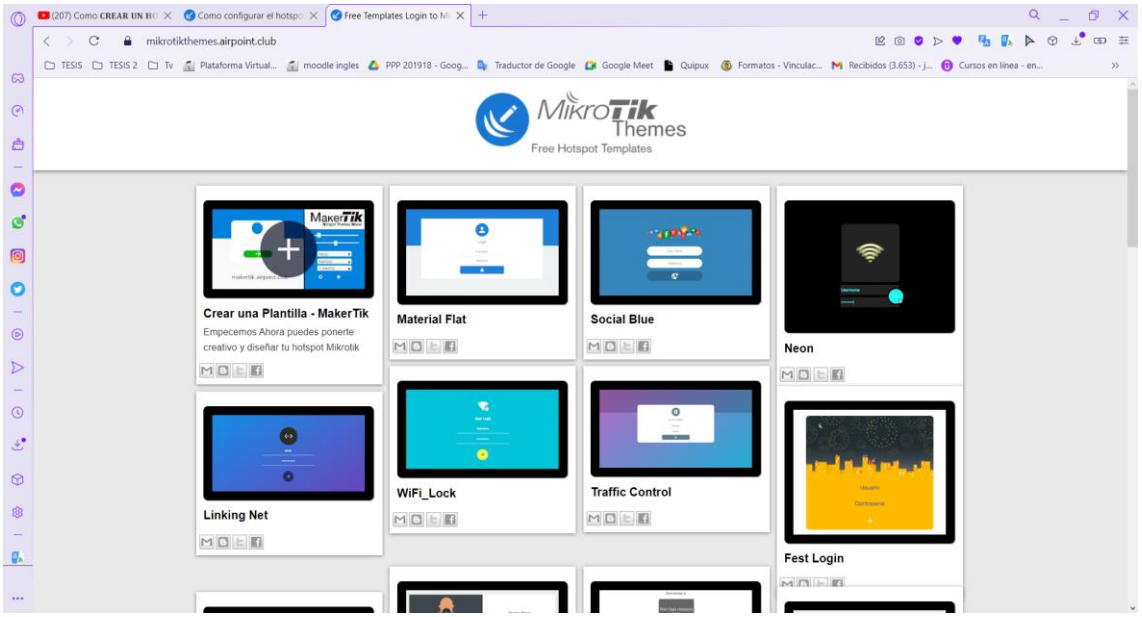
Búsqueda y eliminación del antiguo portal cautivo “Hotspot”



Nota. En la figura se visualiza la búsqueda y la eliminación de nuestro antiguo portal cautivo y la cual será reemplazado con el nuevo descargado.

Figura 167

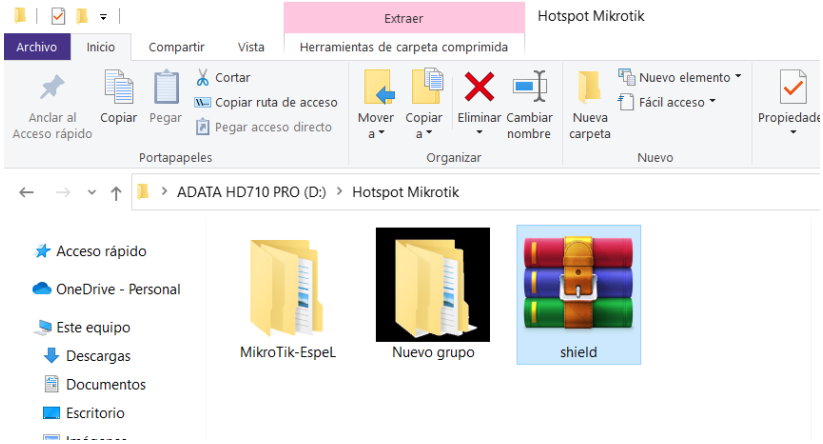
Búsqueda, selección y descarga del nuevo portal cautivo



Nota. En la figura se observa las plantillas existentes en la página oficial de descarga el software de simulación RouterOs MikroTik.

Figura 168

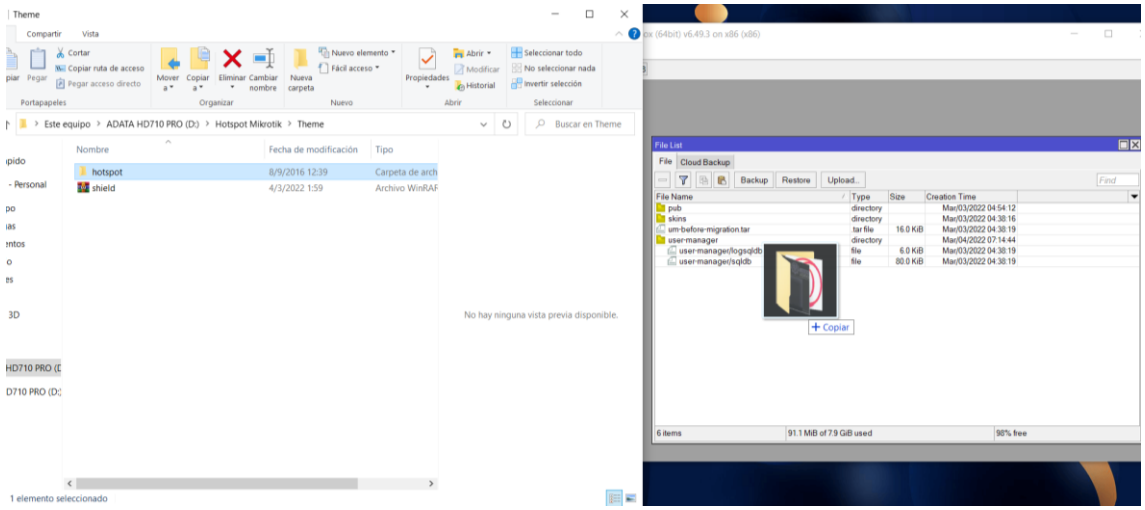
Descompresión del archivo WinRAR del portal cautivo nuevo



Nota. La figura muestra la descompresión del archivo WinRAR que se descarga por defecto para agregar a nuestro nuevo portal cautivo a la interfaz de Hotspot.

Figura 169

Agregación del nuevo portal cautivo al sistema MikroTik



Nota. En la figura se indica de la forma correcta de cómo se debe copiar y pegar un archivo en el sistema de simulación RouterOs MikroTik.

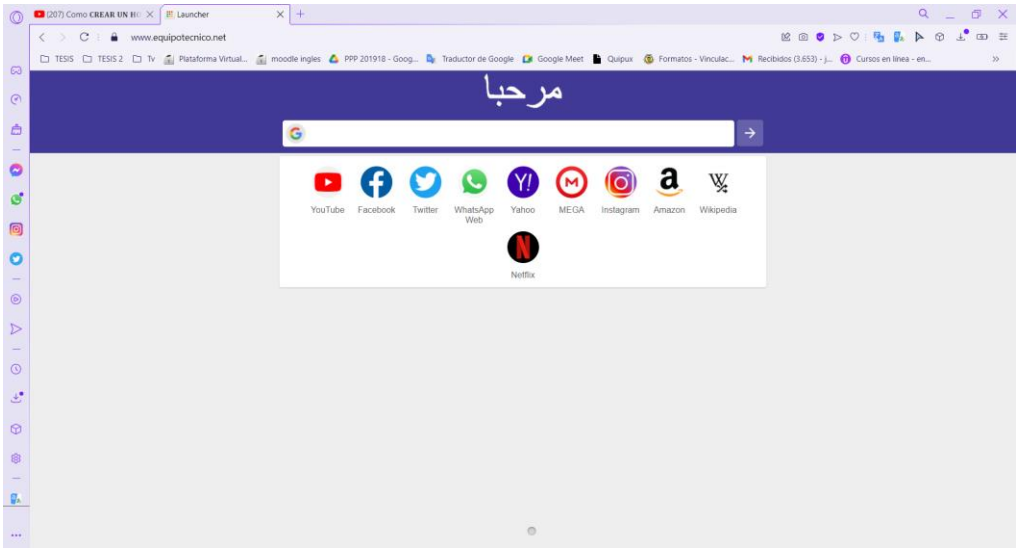
Figura 170

Nuevo portal cautivo agregado al sistema RouterOs MikroTik

Nota. La figura muestra el nuevo portal cautivo y que está vigente actualmente en el software de simulación RouterOs MikroTik.

Figura 171

Interfaz de navegación



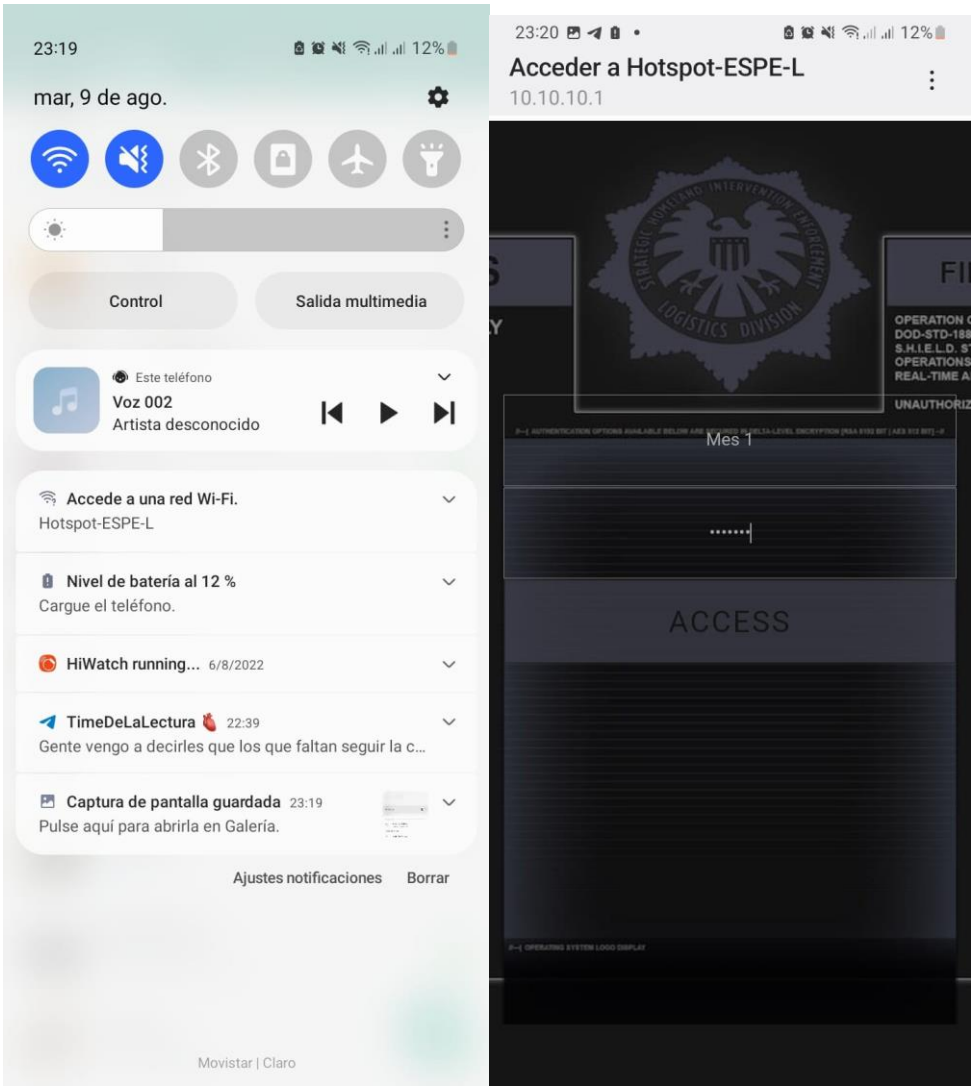
Nota. En la figura se logró con éxito la interfaz que viene integrado con el nuevo portal cautivo descargado y por la cual se inicia navegar o buscar a las redes sociales.

Simulación del portal cautivo para el acceso a usuarios

Se desarrollo las pruebas de comprobación del acceso al portal cautivo creado por medio del simulador de red GNS3 y software ejecutable Winbox, donde se pudo visualizar que, al concitarse los usuarios, ingresando por las fichas de internet creadas, dichos usuarios navegan en internet consumiendo un minino y máximo de Kbps hasta Mbps.

Figura 172

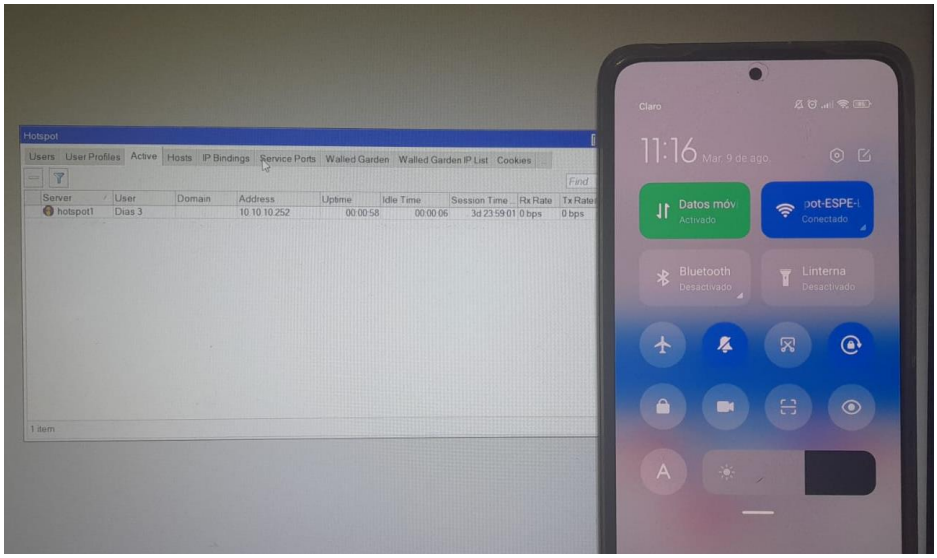
Verificación de la conectividad al portal cautivo



Nota. La figura indica el ingreso del usuario a la interfaz del portal cautivo creado a través del simulador de red GNS3 y el software Winbox.

Figura 173

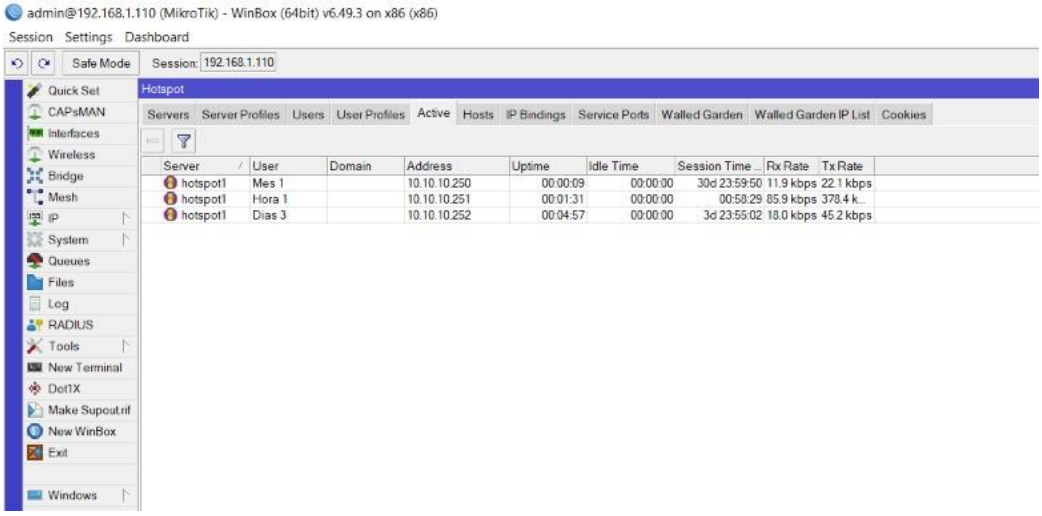
Comprobación de la conectividad del usuario



Nota. La figura muestra el manejo de los usuarios desde el Winbox

Figura 174

Visualización de los usuarios activados dentro del portal cautivo



Nota. En la figura se puede observar los dispositivos activos al Hotspot, por lo que el administrador puede ver el tiempo y la cantidad de bits.

Figura 175

Fichas de acceso a internet

Nota. En la figura se observa la creación de una de las fichas con su respectivo usuario y contraseña para el acceso al portal cautivo.

Implementación del proyecto

Se solicito el ingeniero a cargo del laboratorio de comunicaciones, se permitan implementar los equipos, simulador de red y los sistemas operativos de red, con el objetivo de cumplir con el proyecto de la implementación de un laboratorio virtual con el uso de las redes inalámbricas.

Figura 176

Instalación en el laboratorio de comunicaciones

Nota. En la figura se realizó la implementación del simulador gns3 y el ingreso de la iso del router MikroTik

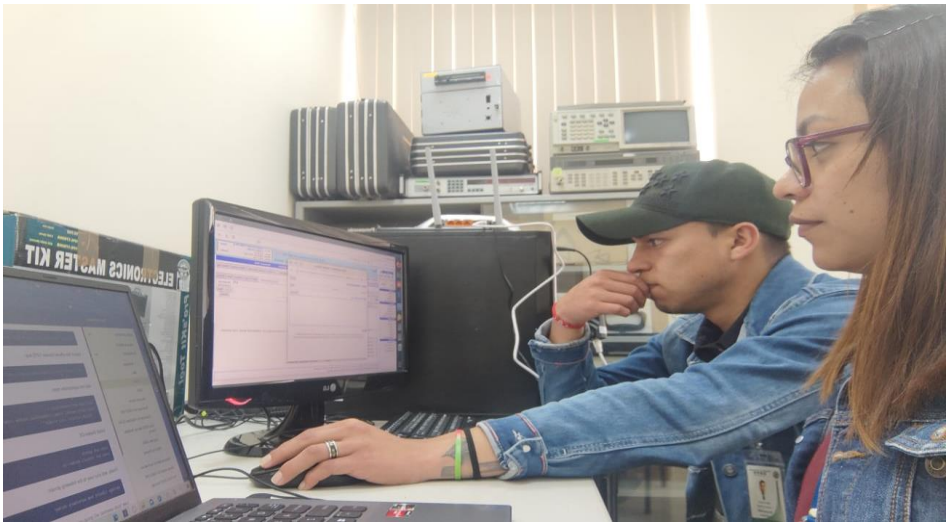
Figura 177

Configuración para el portal cautivo o Hotspot.

Nota. Configuración del software ejecutable Winbox para el portal cautivo de GNS3

Figura 178

Implementación del portal cautivo Zeroshell



Nota. La figura indica el proceso de la configuración del portal cautivo del sistema operativo Zeroshell.

Capítulo IV

Conclusiones y recomendaciones

Durante el tiempo que se realizó la presente monografía se establecieron las siguientes conclusiones y recomendaciones para el proyecto de Implementación de un laboratorio virtual de redes inalámbricas mediante el software de simulación de redes GNS3 y el sistema operativo ZeroShell en la Universidad de las Fuerzas Armadas Espe Sede Latacunga.

Conclusiones

- Tal como se ha investigado sobre las tecnologías de acceso a internet como lo es el portal cautivo, lo cual permitió realizar el análisis técnico de forma eficiente de los diferentes dispositivos que se pueden implementar o usar como un Access Point, el mismo que permite configurar el Hotspot para cumplir con los objetivos planteados.
- De acuerdo con los objetivos planteado se implementó el sistema de acceso Hotspot a través del sistema operativo Zeroshell y software de simulación de red GNS3, en el laboratorio de comunicaciones, el mismo que permite que los estudiantes puedan realizar las practicas referentes al ámbito de redes y telecomunicaciones, por medio de accesos inalámbricos dando así un resultado eficiente a los conocimientos.
- Se plantearon dos escenarios el uno MikroTik mediante el simulador GNS3 y el segundo en sistema operativo de red Zeroshell se simulo el acceso de diferentes clientes al sistema y se verifico que su acceso es satisfactorio con sus credenciales previamente realizas dentro del portal cautivo.

Recomendaciones

- Proponer realizar una investigación amplia de que trata y cómo funciona el portal cautivo o Hotspot, conjuntamente con los software y sistema operativos de red que se va a utilizar dentro del desarrollo de la práctica de laboratorio.
- Se sugiere que cuando se trabaja con emuladores y simuladores evitar el uso de máquinas virtuales ya que estas generan problemas en las interfaces de red, por lo que es recomendable instalar el simulador de red GNS3 dentro del sistema operativo Ubuntu con esto reducir las fallas posibles, adicional a eso poder tener amplitud al momento de desarrollar la máquina virtual Zeroshell.
- Se recomienda a los estudiantes de la cerrera de redes y telecomunicaciones apliquen los conocimientos adquiridos durante los periodos académicos para que este presente proyecto se realice correctamente al momento de ponerlo en práctica de laboratorio.

Glosario

ZeroShell: es una distribución libre para servidores y dispositivos embebidos o integrados, cuyo objetivo es ofrecer los principales servicios que una LAN requiere.A modo de ejemplo: DHCP. DNS. Firewall. VLAN. VPN. RADIUS. LDAP. Portal Cautivo

MikroTik: es un fabricante de hardware y software de routers.

GNS3: GNS3 es un simulador gráfico de red lanzado en 2008, que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales.

HOTSPOT: Un hotspot es un lugar físico donde la gente puede acceder a Internet, normalmente mediante una red WI-FI. La red que crea un hotspot WiFi incluye principalmente un módem y un router inalámbrico

PORTAL CAUTIVO: Un portal cautivo es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal.

WLAN: Una red de área local inalámbrica, también conocida como WLAN, es una red inalámbrica de comunicación para distancias cortas y funciona mediante ondas de radio o infrarrojas.

IEEE 802.11: El estándar 802.11 es una familia de normas inalámbricas creada por el Institute of Electrical and Electronics Engineers. 802.11n es la forma más apropiada de llamar a la tecnología Wi-Fi, lanzada en 2009.

FIREWALL: Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.

SERVIDOR RADIUS: Los servidores RADIUS son ampliamente utilizados por muchas instituciones que proporcionan conectividad WiFi con autenticación WPA2/WPA3-Enterprise, es decir, una autenticación donde tendremos un nombre de usuario/contraseña o certificado digital para autenticarnos en la red inalámbrica.

TIC: Tecnologías de la información y las comunicaciones es un término extensivo para la tecnología de la información que enfatiza el papel de las comunicaciones unificadas

ONDAS ELECTROMAGNÉTICAS: La radiación electromagnética es un tipo de campo electromagnético variable, es decir, una combinación de campos eléctricos y magnéticos oscilantes, que se propagan a través del espacio transportando energía de un lugar a otro.

VELOCIDAD DE TRANSMISIÓN: La velocidad de transmisión de datos mide, el tiempo que tarda un host o un servidor en poner en la línea de transmisión el paquete de datos a enviar. El tiempo de transmisión se mide desde el instante en que se pone el primer bit en la línea hasta el último bit del paquete a transmitir.

REDES INALAMBRICAS: El término red inalámbrica se utiliza en informática para designar la conexión de nodos que se da por medio de ondas electromagnéticas, sin necesidad de una red cableada o alámbrica. La transmisión y la recepción se realizan a través de puertos.

Bibliografía

ALvarez, D. (29 de julio de 2015). *NorficPC*. Recuperado el 26 de abril de 2022, de https://norfipc.com/redes/tipos-redes-estandares-wi-fi-diferencias.php

Anrrango, R. (27 de agosto de 2014). *Configurarmirkotik*. Recuperado el 15 de febrero de 2022, de configurarmikrotikwireless

Bercial, J. (24 de abril de 2020). *GEEKNETIC*. Recuperado el 15 de febrero de 2022, de https://www.geeknetic.es/VirtualBox/que-es-y-para-que-sirve

cableado estructurado. (01 de febrero de 2021). Recuperado el 15 de febrero de 2022, de https://www.casadelcable.com/https-blog-casadelcable-com-blog-que-es-el-cable-utp-categoria-5e/

Cabrera, P. (15 de Octubre de 2019). *Red de Comunicación ¿Qué es? #ISC #IngenieríasUninter*. Recuperado el 02 de Agosto de 2022, de https://blogs.uninter.edu.mx/ESCAT/index.php/red-de-comunicacion/

Caiza Falconi, L. J. (enero de 2017). *ESTUIDIO COMPARATIVO DE PORTAL CAUTIVO.* Recuperado el 20 de Octubre de 2021, de http://dspace.espoch.edu.ec/handle/123456789/8441

Calao Ballesteros, A. M. (19 de Enero de 2015). *DISEÑO E IMPLEMENTACIÓN DE UN LABORATORIO VIRTUAL DE.* Recuperado el 08 de Julio de 2021, de https://repositorio.unicordoba.edu.co/bitstream/handle/ucordoba/488/Laboratorio%20Virtual%20De%20Cinematica.pdf?sequence=1&isAllowed=y

Campoy, C. (09 de agosto de 2016). *Xerinfor*. Recuperado el 15 de febrero de 2022, de https://xerinfor.com/smartblog/8_Qué-es-y-cómo-funciona-un-router-inalámbrico.html

Carles, J. (06 de julio de 2013). *Geekland*. Recuperado el 15 de febrero de 2022, de https://geekland.eu/que-es-y-para-que-sirve-un-firewall/

Castillo, J. A. (5 de enero de 2019). *PROFESIONAL REVIEW*. Recuperado el 15 de febrero de 2022, de https://www.profesionalreview.com/2019/01/05/ldap/

Cisco. (12 de Marzo de 2019). *¿Qué es un firewall?* Recuperado el 03 de Agosto de 2022, de https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Cisco. (2020). Recuperado el 15 de febrero de 2022, de https://www.cisco.com/c/es_mx/products/wireless/wireless-router.html#~preguntas-y-respuestas

Cloudflare. (junio de 2019). *Cloudflare*. Recuperado el 26 de abril de 2022, de https://www.cloudflare.com/es-es/learning/dns/what-is-dns/

Computerworld. (12 de Marzo de 2021). *Cada vez existen más zonas en Ecuador que cuentan con servicios de redes inalámbricas*. Recuperado el 09 de Julio de 2021, de http://www.computerworld.com.ec/actualidad/tendencias/567-cada-vez-existen-más-zonas-en-ecuador-que-cuentan-con-servicios-de-redes-inalámbricas.html

concepto. (2013-2022). Recuperado el 15 de febrero de 2022, de https://concepto.de/sistema-operativo/

concepto. (16 de julio de 2021). (Etecé, Editor) Recuperado el 01 de febrero de 2022, de https://concepto.de/red-inalambrica/

ConceptoABC. (2019). Recuperado el 15 de febrero de 2022, de conceptoabc

ConceptoABC. (2022). Recuperado el 01 de Febrero de 2022, de https://conceptoabc.com/redes-inalambricas/

Cuñas, D. (2017). *Area tecnologia*. Recuperado el 26 de abril de 2022, de https://www.areatecnologia.com/informatica/tecnologia-inalambrica.html

Delgado, J. (20 de Agosto de 2018). *UPS-GT002232.* Recuperado el 20 de Octubre de 2021, de https://dspace.ups.edu.ec/bitstream/123456789/15961/1/UPS-GT002232.pdf

Dessallar inclusion. (2017). Recuperado el 15 de febrero de 2022, de https://desarrollarinclusion.cilsa.org/tecnologia-inclusiva/que-es-un-sistema-operativo/

Diego, L. (06 de octubre de 2018). *CQNET*. Recuperado el 15 de febrero de 2022, de https://www.cqnetcr.com/blog/que-es-mikrotik/

Digital Guide IONOS. (30 de julio de 2019). Recuperado el 01 de febrero de 2022, de https://www.ionos.es/digitalguide/servidores/configuracion/que-es-el-dhcp-y-como-funciona/

Digital Guide IONOS. (13 de Marzo de 2019). Recuperado el 15 de Febrero de 2022, de https://www.ionos.es/digitalguide/servidores/know-how/que-es-el-ntp/

Duarte, G. (Abril de 2015). *DefiniciónABC*. Recuperado el 15 de Febrero de 2022, de https://www.definicionabc.com/tecnologia/red-inalambrica.php

Ejemplos. (2022). Recuperado el 15 de febrero de 2022, de https://www.ejemplos.co/cuales-son-los-sistemas-operativos/

EMF Explained. (2013). Recuperado el 15 de febrero de 2022, de http://www.emfexplained.info/spa/?ID=24794

Farrez, H. (2018). *Tecnologia de la comunicacion*. Recuperado el 25 de abril de 2022, de https://sites.google.com/site/teccomunicacionmei/home/comunicacion-alambrica-e-inalambrica

Fulvio, R. (11 de Marzo de 2018). *Zeroshell End of Life*. Recuperado el 01 de Julio de 2021, de https://zeroshell.org

Gil Cevallos, M. J. (23 de Septiembre de 2013). *INTEGRACIÓN DE LA MATERIA LABORATORIO DE TELEMÁTICA PARA LA FACULTAD TÉCNICA USANDO EL SIMULADOR GRÁFICO DE REDES GNS3.* Recuperado el 28 de Julio de 2021, de http://repositorio.ucsg.edu.ec/bitstream/3317/1354/1/T-UCSG-PRE-TEC-ITEL-6.pdf

Gómez Carmona, J. (20 de Junio de 2017). *Diseño y elaboracion de los manuales de practica de laboratorio de redes utilizando el emulador GNS3.* Recuperado el 01 de Febrero de 2022, de https://dspace.uclv.edu.cu/bitstream/handle/123456789/7888/Joaquín%20Gómez.pdf?sequence=1&isAllowed=n

Gracia, L. (31 de Agosto de 2012). *Un poco de java*. Obtenido de https://unpocodejava.com/2012/08/31/que-es-la-virtualizacion/

Guevara, J. (10 de abril de 2018). *Hetpro*. Recuperado el 26 de abril de 2022, de https://hetpro-store.com/TUTORIALES/senal-digital/

Gustavo, B. (09 de Febrero de 2022). *Hostinger Tutoriales*. Recuperado el 15 de Febrero de 2022, de https://www.hostinger.es/tutoriales/que-es-dns

Herramientas, W. (19 de Abril de 2017). *El protocolo UDP*. Recuperado el 03 de Agosto de 2022, de https://neo.lcc.uma.es/evirtual/cdd/tutorial/transporte/udp.html

Hotelero, S. (12 de Mayo de 2012). *CERIUM*. Recuperado el 15 de febrero de 2022, de https://www.cerium.es/que-es-portal-cautivo-hotspot-hotel/

HUEHUEH. (14 de agosto de 2015). Recuperado el 15 de febrero de 2022, de https://deralaja.wordpress.com/2015/08/14/ondas-y-comunicaciones-satelites-wimax-wi-fi-li-fi-y-bluetooth/

Intercompras. (2022). Recuperado el 15 de febrero de 2022, de https://intercompras.com/p/router-inalambrico-tp-link-tl-wr841n-n-300mbps-chipset-atheros-antenas-76265

Julio. (25 de marzo de 2021). *apuntesjulio*. Recuperado el 15 de febrero de 2022, de https://apuntesjulio.com/emuladores-de-redes-informaticas/

Lescano, F. (11 de Julio de 2017). *SISTEMA DE COMUNICACIÓN UTILIZANDO TECNOLOGÍA WIRELESS.* Recuperado el 08 de Julio de 2021, de https://repositorio.uta.edu.ec/bitstream/123456789/405/1/Tesis_t626ec.pdf

Ligua, C. (26 de febrero de 2019). *UNESUM-ECU-REDES-2019-28.* Recuperado el 20 de octubre de 2021, de http://repositorio.unesum.edu.ec/bitstream/53000/1582/1/UNESUM-ECU-REDES-2019-28.pdf

Limones, E. (05 de Mayo de 2021). *OpenWebinars*. Recuperado el Febrero de 01 de 2022, de https://openwebinars.net/blog/virtualizacion-que-es-para-que-sirve-y-ventajas/

Linares, S. (23 de Junio de 2017). *Prezi*. Recuperado el 8 de junio de 2022, de https://prezi.com/luzznggdtxfk/comunicaciones-alambricas-e-inalambricas/

Luz, S. (20 de septiembre de 2021). *Redes Zone*. Recuperado el 20 de febrero de 2022, de https://www.redeszone.net/tutoriales/servidores/que-es-servidor-radius-funcionamiento/

Luz, S. (25 de mayo de 2022). *Rede Zone*. Recuperado el 19 de abril de 2022, de https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/

Luz, S. D. (12 de agosto de 2021). *Redes Zone*. Recuperado el 15 de febrero de 2022, de https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

Maldonado, D. (26 de agosto de 2019). *icorp*. Recuperado el 15 de febrero de 2022, de http://www.icorp.com.mx/blog/que-es-virtualizacion/

MÁSMOVIL. (2022). Recuperado el 15 de febrero de 2022, de https://blog.masmovil.es/glosario/definicion-estacion-base/

Merino, M. Y. (2011). *Defenición.DE*. Recuperado el 15 de Febrero de 2021, de https://definicion.de/red-inalambrica/

Microsoft. (2022). Recuperado el 15 de febrero de 2022, de https://azure.microsoft.com/es-es/overview/what-is-a-virtual-machine/#resources

Miguel Angel, A. G. (16 de junio de 2016). *cesian*. Recuperado el 15 de febrero de 2022, de http://www.cesian.edu.mx/blog/como-funciona-un-red-inalambrica-de-internet/

miracomosehace. (11 de mayo de 2020). Recuperado el 15 de febrero de 2021, de https://www.google.com/search?q=que+es+un+hotspot&client=opera-gx&ei=lRQTYrOjC6iawbkPk8mvmAs&oq=que+es+un+hots&gs_lcp=Cgdnd3Mtd2l6EAMYADIFCAAQgAQyBQgAEIAEMgUIABCABDIHCAAQgAQQCjIECAAQCjIECAAQCjIECAAQCjIECAAQCjIECAAQCjIECAAQCjoECAAQQzoICAAQgAQQsQM6DggueIAEE

Muñoz, J. (16 de abril de 2018). *Mercasat*. Recuperado el 15 de Febrero de 2022, de https://www.mercasat.es/blog/caracteristicas-de-las-redes-inalambricas-fundamentales-para-la-domotica/

Netc. (05 de junio de 2019). Recuperado el 15 de febrero de 2022, de https://www.netec.com/post/maquinas-virtuales-que-son-y-cuales-son-sus-tipos

NetSpot. (2022). Recuperado el 15 de febrero de 2022, de https://www.netspotapp.com/es/wifi-signal-strength/wifi-signal-strength-and-its-impact.html

Obasoftfp. (7 de octubre de 2015). Recuperado el 01 de febrero de 2022, de https://obasoftfp.wordpress.com/2015/10/07/zeroshell-una-solucion-ideal-para-la-empresa/

Oliveros, D. (Dirección). (2016). *Redes Inalambricas* [Película]. Recuperado el 15 de febrero de 2022, de https://www.youtube.com/watch?v=EQZLmBWJSiA

Optical Networks. (31 de octubre de 2019). Recuperado el 15 de febrero de 2022, de https://www.optical.pe/blog/tipos-de-redes-inalambricas/

Parra, K. (21 de enero de 2016). *slidshare*. Recuperado el 01 de agosto de 2022, de https://es.slideshare.net/Koldoparra/tecnologas-y-sistemas-de-comunicacion-57315855

Pomar, M. A. (30 de Enero de 2020). *José Maria González*. Recuperado el 15 de febrero de 2022, de https://www.josemariagonzalez.es/vmware-nsx/eve-emulated-virtual-environment.html

Prieto Fernández, R. (17 de Abril de 2018). *Cómo configurar un Hotspot con MikroTik y RouterOS*. Recuperado el 01 de Julio de 2021, de

https://www.raulprietofernandez.net/blog/mikrotik/como-configurar-un-hotspot-con-mikrotik-y-routeros

Ramírez, I. (31 de Enero de 2020). *Xataka*. Recuperado el 01 de Febrero de 2022, de https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas

Ramírez, I. (29 de enero de 2021). *Xataka*. Recuperado el 15 de Febrero de 2022, de https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

Red Hat. (02 de marzo de 2018). Recuperado el 15 de febrero de 2022, de https://www.redhat.com/es/topics/virtualization/what-is-virtualization

Redes Inalambricas. (2022). Recuperado el 01 de febrero de 2022, de https://www.redesinalambricas.es

redesgaby. (05 de diciembre de 2014). Recuperado el 15 de febrero de 2022, de http://redeesgabi.blogspot.com/2014/12/simulador-y-emulador.html

Rodriguez, A. (05 de |Marzo de 2017). *Definición de red de comunicaciones*. Recuperado el 02 de Agosto de 2022, de https://es.slideshare.net/punk-andii/definicin-de-red-de-comunicaciones

Rus, C. (05 de abril de 2021). *Xataka*. Recuperado el 15 de febrero de 2022, de https://www.xataka.com/otros-dispositivos/modem-router-punto-acceso-diferencias-cada-uno-cual-mejor-para-cada-usuario

Secarcam. (02 de mayo de 2016). Recuperado el 15 de febrero de 2022, de https://secarcam.webcindario.com/?p=707&lang=es

Sena, M. (12 de Julio de 2019). *¿Cuáles son los retos de las redes inalámbricas en América Latina?* Recuperado el 09 de Julio de 2021, de https://gblogs.cisco.com/la/en-msena-cuales-son-los-retos-de-las-redes-inalambricas-en-america-latina/

Significados. (11 de Marzo de 2017). *Significado de Redes*. Recuperado el 31 de Julio de 2022, de https://www.significados.com/redes/

sites. (2014). Obtenido de https://sites.google.com/site/teccomunicacionmei/home/comunicacion-alambrica-e-inalambrica

Smaldone, J. (20 de septiembre de 2008). *Blog*. Recuperado el 15 de febrero de 2022, de https://blog.smaldone.com.ar/2008/09/20/virtualizacion-de-hardware/

Smith, J. (2014). *RedesHakne*. Recuperado el 15 de Febrero de 2022, de https://redeshakne.blogspot.com/p/simulacion-y-emulacion-de-redes.html

tecnologia wireless. (11 de julio de 2016). Recuperado el 15 de febrero de 2022, de comunicacionesinalambricashoy

Telectrónika. (29 de Abril de 2018). *GNS3 Guía Introductoria: Características y Requerimientos Mínimos*. Recuperado el 01 de Julio de 2021, de https://www.telectronika.com/articulos/ti/que-es-gns3/

Tello Peña, R. P. (23 de Marzo de 2017). *Planteamiento de conexión alternativa a red móvil para acceso de conectividad a datos basado en el estándar 802.11.* Recuperado el 08 de Julio de 2021, de http://repositorio.puce.edu.ec/bitstream/handle/22000/12497/Caso%20de%20Estudio%20Unidad%20de%20Titulacion%20Ruben%20Tello%20%281%29.pdf?sequence=1&isAllowed=y

Tezé. (04 de febrero de 2018). *Wilsonlandia*. Recuperado el 15 de febrero de 2022, de https://wilsonlandia.net/mikrotik/que-es-mikrotik-para-que-sirve/

tiendamia. (2022). *tiendamia*. Recuperado el 04 de agosto de 2022, de https://tiendamia.com/ec/producto?amz=B08DHLCLCY&pName=Extensor%20WiFi%20TP-Link%20N300%20(RE105),%20amplificador%20de%20señal%20de%20extensores%20WiFi%20para%20el%20hogar,%20extensor%20de%20alcance%20WiFi%20de%20banda%20única,%20amplificador%20de%20Inter

Tolomeo, P. (13 de Junio de 2017). *Sistemas De Comunicaciones .* Recuperado el 31 de Julio de 2022, de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/861/A6.pdf?sequence=6

Udearroba. (05 de octubre de 2017). Recuperado el 23 de octubre de 2021, de https://www.youtube.com/watch?v=HTUjQh44GfE

Velasco, R. (20 de Marzo de 2014). *RZ redes zone*. Recuperado el Febrero de 01 de 2022, de https://www.redeszone.net/2014/03/20/lista-de-simuladores-de-redes-para-virtualizar-nuestra-propia-red/

Wifisafe Spain S.L. (2013-2020). Recuperado el 01 de febrero de 2022, de https://www.wifisafe.com/blog/funcionamiento-de-las-redes-inalambricas

Wikipedia, L. E. (08 de Junio de 2021). *Universidad de las Fuerzas Armadas de Ecuador*. Recuperado el 28 de Julio de 2021, de https://es.wikipedia.org/wiki/Universidad_de_las_Fuerzas_Armadas_de_Ecuador

Xataka. (31 de enero de 2020). Recuperado el 15 de febrero de 2022, de https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas

Zeroshell. (2018). Recuperado el 15 de febrero de 2022, de https://www.zeroshell.org

Anexos