
# Diseño e implementación de una red LAN para un laboratorio y un sistema de control de acceso a internet de forma inalámbrica hotspot en la Unidad Educativa Jorge Icaza.

Trávez Velasco, Kevin Santiago y Guamangate Umajinga, Silvia Maribel

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

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

Ing. Caicedo Altamirano, Fernando Sebastián

25 febrero del 2022

Latacunga

**DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA**

**CARRERA DE TECNOLOGÍA SUPERIOR REDES Y TELECOMUNICACIONES**

## CERTIFICACIÓN

Certifico que la monografía, "**Diseño e implementación de una red LAN para un laboratorio y un sistema de control de acceso a internet de forma inalámbrica hotspot en la Unidad Educativa Jorge Icaza.**" fue realizado por el señor **Trávez Velasco, Kevin Santiago** y la señorita **Guamangate Umajinga Silvia Maribel** la cual ha sido revisada y analizada en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto, cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Latacunga, 23 de febrero del 2022

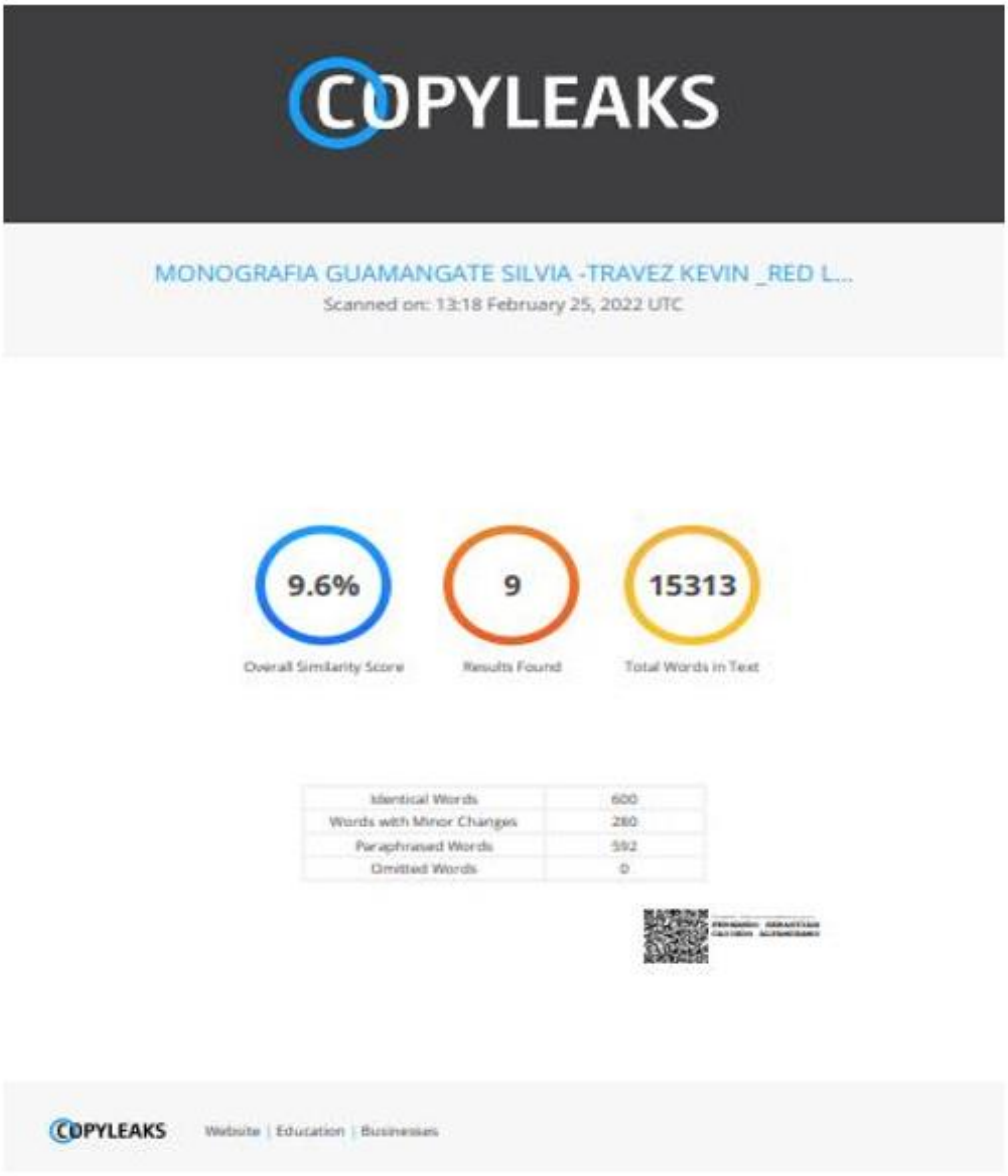
Firmado electrónicamente por:
FERNANDO SEBASTIAN
CAICEDO ALTAMIRANO

.....

Ing. Caicedo Altamirano, Fernando Sebastián

C.C.: 1803935020

**Reporte de verificación de contenido**




FERNANDO SEBASTIAN CAICEDO ALTAMIRANO

……..……..…

Ing. Caicedo Altamirano, Fernando Sebastián

C.C.: 1803935020

**DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA**

**CARRERA DE TECNOLOGÍA SUPERIOR REDES Y TELECOMUNICACIONES**

## RESPONSABILIDAD DE AUTORÍA

Yo, **Trávez Velasco, Kevin Santiago**, con cédula de ciudadanía **N° 0504067794** y **Guamangate Umajinga, Silvia Maribel,** con cédula de ciudadanía **N° 0504208109,** declaro que el contenido, ideas y criterios de la monografía**: Diseño e implementación de una red LAN para un laboratorio y un sistema de control de acceso a internet de forma inalámbrica hotspot en la Unidad Educativa Jorge Icaza,** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Latacunga, 25 de febrero del 2022

Trávez Velasco, Kevin Santiago

C.C.: 0504067794

Guamangate Umajinga, Silvia Maribel

C.C.: 0504208109

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA**

**CARRERA DE TECNOLOGÍA SUPERIOR REDES Y TELECOMUNICACIONES**

**AUTORIZACIÓN DE PUBLICACIÓN**

Yo **Trávez Velasco, Kevin Santiago** y **Guamangate Umajinga, Silvia Maribel,** Autorizo a la Universidad de las Fuerzas Armadas ESPE publicar la monografía: **Diseño e implementación de una red LAN para un laboratorio y un sistema de control de acceso a internet de forma inalámbrica hotspot en la Unidad Educativa Jorge Icaza.** en el repositorio institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Latacunga, 25 de febrero del 2022

Trávez Velasco, Kevin Santiago

C.C.: 0504067794

Guamangate Umajinga, Silvia Maribel

C.C.:0504208109

## Dedicatoria

Este trabajo de integración curricular dedico a mi madre por haberme inculcado valores y el significado de perseverancia hacia mis objetivos de vida, ha trabajado duro y sin importar las circunstancias ha sabido ofrecerme lo mejor de ella, para que yo pueda cumplir mis metas.

Por eso también doy mi trabajo a la Carrera de Redes y Telecomuniciones que, desde un inicio, ha abierto un gran interés de investigación.

**TRÁVEZ VELASCO, KEVIN SANTIAGO**

## Dedicatoria

El presente trabajo de titulación va dedicado con especial afecto y consideración a todas las personas que contribuyeron a mi formación profesional, en especial a mis padres y hermanos que me han inculcado valores y sobre todo a nunca rendirme.

**GUAMANGATE UMAJINGA, SILVIA MARIBEL**

**Agradecimiento**

Al cumplir una etapa académica maravillosa en mi vida quiero dar mis agradecimientos a mi familia por el apoyo moral y económico durante el desarrollo del proyecto, de forma especial a mi madre Emma Trávez y mi abuela Fanny Trávez. Sin ellas no lo habría logrado, son la motivación que tengo a diario para ser una mejor persona al igual que son el pilar fundamental para cumplir mis metas como profesional.

Gracias por la confianza y por brindarme ese apoyo incondicional durante toda mi vida.

**TRÁVEZ VELASCO, KEVIN SANTIAGO**

## Agradecimiento

Mi agradecimiento infinito a mis padres Nelson Guamangate y Elsa Umajinga por el apoyo incondicional brindado durante todos estos años, por ser ellos dos mi mayor inspiración, dándome así la fuerza para seguir caminando y lograr alcanzar esta meta anhelada. Dios los bendiga, les de salud y mucha vida para retribuirles un poco de lo que me han dado.

**GUAMANGATE UMAJINGA, SILVIA MARIBEL**

**Tabla de contenidos**

**Índice de figuras**

**Índice de tablas**

**Resumen**

En la actualidad tener acceso a internet es fundamental y más aún si se trata de una escuela o colegio ya que la iniciativa de investigación conlleva navegar en sitios informativos además de poder reforzar conocimientos mediante búsquedas en internet. Para lo cual el presente trabajo de integración curricular tiene como finalidad realizar una red LAN para el laboratorio de computación y un sistema inalámbrico Hotspot en la Unidad Educativa Jorge Icaza ubicada en la ciudad de Latacunga, en donde se realizó el cableado estructurado para lo cual se diseñó una red utilizando la herramienta Cisco Packet Tracer como simulador, con el objetivo de que las computadoras del laboratorio tengan servicio de internet por cable, así también se creó grupos de trabajo para organizar los equipos dentro de la red local y para el sistema Hotspot se utilizaron herramientas que permitieron realizar un análisis de cobertura para lo que los dispositivos fueron configurados e instalados en zonas estratégicas con el objetivo de que los estudiantes y docentes puedan tener acceso a internet con un ancho de banda controlado. Su funcionalidad se ejecutará de la siguiente manera: los usuarios deberán poseer un dispositivo electrónico por el cual accederán a nuestra red inalámbrica, los estudiantes accederán a la Red INVITADOS y les aparecerá un portal donde deberán colocar la contraseña para poder navegar en Internet y el mismo proceso con la red DOCENTES.

Palabras clave:

- **RED LAN**
- **HOTSPOT**
- **RED INVITADOS**
- **RED DOCENTES**

**Abstract**

Nowadays, having access to the internet is essential and even more so if it is a school or college since the research initiative involves browsing informative sites as well as being able to reinforce knowledge through internet searches. For which the present work of curricular integration has as purpose to realize a LAN network for the computer laboratory and a wireless Hotspot system in the Educational Unit Jorge Icaza located in the city of Latacunga, where the structured wiring was realized for which a network was designed using the tool Cisco Packet Tracer as simulator, with the objective that the computers of the laboratory have service of Internet by cable, Also, work groups were created to organize the equipment within the local network and for the Hotspot system, tools were used to perform a coverage analysis for which the devices were configured and installed in strategic areas so that students and teachers can have access to the Internet with a controlled bandwidth. Its functionality will be executed as follows: users must have an electronic device through which they will access our wireless network, students will access the GUEST network and a portal will appear where they must enter the password to be able to surf the Internet and the same process with the TEACHERS network.

Key words:

- **LAN NETWORK**
- **HOTSPOT**
- **GUESTS NETWORK**
- **TEACHERS NETWORK**

# Capítulo I

## 1 Marco metodológico de la investigación

### 1.1 Antecedentes

Silva Harol y Solorzano Miguel (2008), afirma que uno de los aspectos más importantes en el camino hacia el éxito radica en el manejo de la información llegando incluso a afirmarse que “quien maneja la información, maneja el poder”.

Las telecomunicaciones han cambiado drásticamente en estos últimos años, pasando de centrarse únicamente en la transmisión de la voz, a la ocupación actual de las redes que es la comunicación y transmisión de datos, imágenes, video, entre otros, aspecto que unido al avance de las tecnologías de las telecomunicaciones, exige que las empresas de cualquier sector, cuenten con sistemas de comunicación eficientes y de alta tecnología. Por esta razón, Diana Catherine Ledesma Mera, de la Universidad Politécnica Salesiana Sede Guayaquil en el año 2018 en su tema de titulación “Reestructuración de la Infraestructura de Red LAN Basado en las Normas de Cableado Estructurado, y la aplicación de Políticas de Seguridad para el control de acceso Mediante un Servicio Proxy Linux en la Unidad Educativa Hispanoamericano”, en donde realizo la reestructuración de la red LAN por lo que logró solventar los problemas de conexión a internet, facilitó la detección de fallas mediante la identificación y etiquetado de cada punto de red y brindó una mejor administración al disponer de un diseño lógico de la red actual, estos cambios se realizaron siguiendo los estándares TIA/EIA 568-B1 y TIA/EIA 606, brindando así también seguridad a los dispositivos de red y protección del cableado mediante la utilización de canaletas y mediante la implementación del servidor proxy en la institución, se establecieron políticas de seguridad que permitieron limitar el

acceso de contenidos web en los equipos utilizados por los estudiantes en el Laboratorio de Cómputo. (Mera, 2018, pág. 16)

Herrera Regalado José Aturo, de la universidad de Guayaquil en el año 2017 en su trabajo de titulación “Análisis Investigativo para la Implementación de un Sistema de Geolocalización Vía Wi-Fi dentro de la Reserva Forestal Senderos a través de la Aplicación de Hotspots”, en donde desarrollo un sistema para que los usuarios tengan acceso a Internet en el parque ecológico y adicionalmente ofrece un servicio de geolocalización para determinar el punto exacto de donde se encuentra en caso de extravío involuntario. Además permitió que los habitantes del estado de Guayaquil y turistas de otros lugares accedan universalmente a la tecnología de la información, mejoren su calidad de vida y completen la experiencia turística en las extensiones del parque ecológico Samanes y de acuerdo a la cartografía observada en el sitio se puede identificar que la factibilidad técnica es muy alta para este proyecto porque no existen bloqueos de señal y el terreno amplio es propicio para optimizar el alcance de los nodos antes mencionados y el incremento de señal. Llegando a la conclusión de que muchas necesidades de los usuarios o visitantes del parque serán cubiertas por en términos de tecnología y seguridad. (Regalado, 2017, pág. 14)

Como se puede evidenciar en los trabajos anteriormente descritos hay un gran interés en la implementación de laboratorios informáticos con acceso a Internet para las redes y telecomunicaciones, por lo cual es importante que la Unidad Educativa cuente con estos 2 sistemas de Redes y así permitir una mejor calidad de educación.

## 1.2 Planteamiento del problema

En el artículo que escribió Clay Alvino (2021), da a conocer un estudio en Ecuador sobre el acceso a internet el 45,5 % de la población ecuatoriana no poseen acceso a recursos tecnológicos y de igual manera al servicio, de esta forman la importancia que se está dando es libre acceso a internet ya que el 98% de los estudiantes ingresan desde cualquier dispositivo móvil. El acceso información a día de hoy en primordial por la constante evolución tanto tecnología como digital.

La UNIDAD EDUCATIVA “JORGE ICAZA” con sostenimiento fiscal, ubicado en la zona 3, correspondiente al Distrito Educativo 05D01 Latacunga, en la Ciudadela Maldonado Toledo, calle Tanicuchí y Salcedo, parroquia Eloy Alfaro, oferta la modalidad presencial, el cual ha prestado sus servicios de Nivel de Educación General Inicial, Básica y Bachillerato por más de 40 años. Su metodología de estudio ha estado basada en una oferta ordinaria, con modalidad presencial, jurisdicción intercultural, Régimen Sierra, jornada matutina y vespertina, por lo tanto, no cuentan con un laboratorio informático que brinde las capacidades necesarias de enseñar a los estudiantes la nueva era digital, trayendo así una serie de desventajas en la nueva modalidad de clases virtuales.

La escuela no cuenta con estos recursos ya que anteriormente recibían clases sin utilizar la tecnología por lo que la Institución pretende instalar un laboratorio informático que cuenta con 13 máquinas la cual no tienen ninguna infraestructura de conectividad.

Los estudiantes al igual que los docentes han sido afectados al no tener acceso a internet impidiendo aprendizajes y a su vez dificultando ir de la mano con la evolución de la tecnología ya que como estudiante se debe tener libre acceso a la información. Al

no tener una solución para dicho problema los alumnos no podrán desarrollar destrezas de investigación, tampoco recibir clases de materias sobre computación o informática dificultando tener una educación de calidad en donde se lleve a cabo la investigación de nuevos descubrimientos tecnológicos. Pero si la Unidad Educativa contase con un laboratorio informático y algún sistema que les permita el acceso a Internet permitiría un mejor desempeño académico tanto de estudiantes como de Docentes.

### 1.3 Descripción resumida del proyecto

El presente proyecto técnico se desarrolla en la Unidad Educativa Fiscal Jorge Icaza con el objetivo de realizar un diseño e implementar una red LAN para un laboratorio y un sistema de control de acceso a internet de forma inalámbrica hotspot. De esta manera los equipos y materiales a utilizar para el cableado estructurado de telecomunicaciones será mediante el análisis de normas así también del área de trabajo para la instalación de Access Point.

La implementación de la red LAN y el sistema Hotspot asegura que los estudiantes activen sus habilidades de investigación así como también los docentes puedan impartir clases dinámicas al igual que a mejorar la metodología de enseñanza.

Siguiendo el desarrollo, las simulaciones son parte fundamental para tener un punto de vista de la situación del área de trabajo, los equipos seleccionados al poseer software propio de configuración facilitan la manipulación entre los principales se destaca Winbox que permite la configuración de dispositivos MikroTik y UniFi que permite la configuración de puntos de acceso de equipos Ubiquiti.

## 1.4 Justificación e importancia

El enfoque en realizar una red LAN tiene como funcionalidad mejorar el laboratorio de computación para dar el uso adecuado a los computadores, porque al verificar el estado del laboratorio de manera técnica ninguna de las computadoras tenía conectividad a Internet.

El sistema Hotspot ha sido planteado porque en las unidades educativas se debe tener una cobertura inalámbrica de acceso a internet ayudando así tanto a docentes como a estudiantes a estar conectados a la información desde cualquier parte.

Con la implementación de dicho sistema inalámbrico al igual que la creación de una red LAN mejora la calidad de estudio y aprendizaje ya que al poseer todos acceso a internet se estaría fortaleciendo y motivando a realizar investigaciones en el mundo de la tecnología demás de aprovechar a su máximo el recurso que la unidad educativa está ofreciendo en la parte tecnológica. Por parte de la institución al querer mejorar su área tecnológica estaría beneficiando a los estudiantes de la próxima generación, los padres de familia también seriar beneficiados al saber que el lugar donde sus hijos se están formando académicamente este cuenta con acceso a la información para lo cual en punto general la institución subiría un peldaño en educación hacia los estudiantes. Al tener como objetivo siempre tener acceso a la información en el laboratorio e institución será de ayuda para aquellos estudiantes que en sus hogares no tengan internet para realizar sus tareas e investigaciones de esta manera también se estará mejorando la comunicación ya que la mayor parte siempre estamos conectados a internet para estar al tanto de noticias y en constante comunicación con amigos y familiares.

## 1.5 Objetivos

### *1.5.1 Objetivo General*

- Diseñar e implementar una red LAN para un laboratorio y un sistema de control de acceso a internet de forma inalámbrica hotspot en la unidad educativa Jorge Icaza.

### *1.5.2 Objetivos Específicos*

- Investigar las normativas de cableado estructurado y realizar un análisis técnico para seleccionar los equipos y materiales necesarios para la implementación de la red LAN y sistema Hotspot.
- Implementar la red LAN en el laboratorio aplicando normativas de cableado estructurado.
- Implementar el sistema Hotspot mediante el uso de puntos de acceso para garantizar la cobertura en toda el área de la institución.
- Verificar el correcto funcionamiento de la Red LAN y el sistema Hotspot utilizando herramientas de verificación como tester y mapas de calor.

## 1.6 Alcance

El proyecto de titulación se basa en la implementación de una Red LAN donde se aplicará estándares y normativas del cableado estructurado, de la misma manera que la adquisición de equipos nos ayude a mejorar el proyecto.

Se pretende mejorar el control para el acceso a Internet configurando un Portal Cautivo y teniendo una cobertura que abarque toda la institución a través de los puntos de acceso. Adicionalmente la configuración del Router es un elemento fundamental ya que los parámetros de conexión se establecen porque la institución no cuenta con una alta conexión a Internet. Los servicios deberán emparejarse y configurarse de manera óptima para resolver este problema.

# Capítulo II

# 2 Marco teórico

## 2.1 Redes de computadoras o Redes Informáticas

Al principio la computadora estaba aislada en la oficina, el lugar de trabajo, la escuela o el hogar. Luego se volvió liviana, es decir permitía a los usuarios del dispositivo intercambiar información y compartir recursos como una impresora, un disco y software de memoria, como el paquete de una base de datos de programación y sistemas de comunicación como un canal de conexión en red corporativa.

En la era anterior de Internet, que permitía a docenas de usuarios de la empresa usar un solo recurso de impresión en una red y un solo canal de comunicación para acceder a Internet. Una vez conectado a la World Wide Web, es posible acceder a diversas fuentes de información para transmitir mensajes de interlocutores en cualquier parte de la ciudad y del país o del mundo. (Sosa, 2011, pág. 56)

## 2.2 Tipos de Redes

La creación de redes es parte de las operaciones comerciales normales. Lo usamos todos los días para todo, desde imprimir documentos hasta conectarnos de forma remota a la información y los recursos informáticos de nuestra empresa. Así lo escribe José Poveda (2020) en su artículo.

### *2.2.1 Red de área personal (PAN)*

Este es el tipo más básico de red informática que existe. Una red PAN consta de un módem inalámbrico, una o dos computadoras, un teléfono, una impresora y una cantidad de dispositivos conectados limitados a un radio de diez metros. Las redes

personales normalmente se encuentran en oficinas pequeñas o áreas residenciales y se administran desde un solo dispositivo. Además, este tipo de red informática puede funcionar a través de Internet sin necesidad de cableado. (Poveda, 2020)

### *2.2.2 Red de área local (LAN)*

Las Redes de área local (LAN) se componen de espacios de trabajo interconectados para compartir información y equipos. Al igual que las redes anteriores, las redes LAN cubren un área geográfica limitada, como oficinas o un grupo de edificios. Sin embargo, difiere de las redes PAN en su amplio rango de comunicación, velocidad de transferencia de datos y cantidad de dispositivos que se pueden conectar. (Etecé, 2022)

### *2.2.3 Red de área amplia (WAN)*

Este tipo de red informática conecta diferentes dispositivos ubicados a largas distancias. De esta manera, pueden comunicarse de forma remota, independientemente de su distancia.

El ejemplo más común de una red WAN es Internet, que conecta millones de dispositivos en todo el mundo. Como tal, por su extensión, la gestión de este tipo de redes informáticas es pública y corresponde a diferentes administradores. (ENI Networks, 2019)

### *2.2.4 Red de área de almacenamiento (SAN)*

Las SAN están formadas por servidores, conmutadores y dispositivos de almacenamiento conectados mediante diferentes protocolos. Este tipo de red tiene una disponibilidad casi total, ya que almacena datos en bloques, lo que permite asignar los recursos de la manera más eficiente posible. (Bilegow, 2021)

### *2.2.5 Red virtual privada (VPN)*

Con este tipo de red, puede establecer una conexión segura con cualquier otra red a través de una red pública como Internet. Generalmente, las empresas utilizan este tipo de red informática para el acceso remoto a la red de área local de la empresa. De esta forma, un empleado puede trabajar desde cualquier parte del mundo utilizando los recursos tecnológicos de la empresa como si estuviera trabajando localmente. Por su seguridad, una VPN también sirve para evitar que las actividades y los datos de una empresa sean rastreados por terceros, cuestión de vital importancia debido a la conexión a través de una red pública, por ejemplo, como Internet. (Poveda, 2020)

## 2.3 Topologías de Red

José Dordoigne dice en su libro de Redes Informáticas que la topología de red se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse.

### *2.3.1 Topología lógica*

Indica cómo funciona una red real, es decir, podemos hacer que la topología física en estrella se comporte como un bus o como un anillo. (Dordoigne, 2020)

### *2.3.2 Topología física:*

Es la topología que forman las estaciones a nivel físico, estas pueden ser (Dordoigne, 2020):

#### 2.3.2.1 Topología de interconexión completa

- Todos los nodos comunicados con los otros.
- Cada nodo tiene una conexión hacia los otros nodos.

- Muchos enlaces, pero no se usan mucho.
- Es muy costoso

**2.3.2.2 Topología de red jerárquica árbol.** Una conexión en árbol es similar a una serie de redes en estrella interconectadas, excepto que no tiene un nodo central. En cambio, tiene un nodo troncal, generalmente ocupado por un concentrador o conmutador, desde el cual se ramifican otros nodos. Esta es una variante de la red de bus, donde la falla de un nodo no está relacionada con interrupciones de comunicación. (Corvo, 2019)

**2.3.2.3 Topología en bus.** Esta topología permite que todas las estaciones reciban la información transmitida, una estación la transmita y todas las demás estaciones la escuchen. Consiste en un cable con un terminal en cada extremo del que se suspenden todos los elementos de la red. Todos los nodos de la red están conectados a este cable: llamado “Cable Backbone”. (Dordoigne, 2020)

**2.3.2.4 Topología en anillo.** En esta topología de red, cada estación está conectada a la siguiente estación y la última estación está conectada a la primera estación. Cada estación tiene un receptor y un transmisor que actúa como repetidor, transmitiendo la señal a la siguiente estación. En este tipo de red, la comunicación se da a través de la transmisión de tokens o cookies, que pueden conceptualizarse como un cartero que pasa y que recolecta y entrega paquetes de información, evitando así que la información sea interceptada y perdida por colisión. (Noguera, 2019)

**2.3.2.5 Topología en estrella.** Una red en estrella activa con un nodo central activo a menudo tiene los medios para evitar problemas relacionados con los ecos. Se utiliza principalmente para redes de área local. La mayoría de redes de área local con enrutadores, conmutadores o concentradores siguen esta topología. (Orduño, 2021)

**2.3.2.6 Topología en malla.** La topología de malla es una topología de red en la que cada nodo está conectado a todos los demás nodos. De esta forma, es posible transportar mensajes de un nodo a otro utilizando diferentes caminos. Si la red está completamente conectada, no puede haber absolutamente ninguna interrupción en la comunicación. Cada servidor tiene su propia conexión con todos los demás servidores. (Dordoigne, 2020)

### *2.3.3 Medios de comunicación*

Hay diversos medios de transmisión, pero los más utilizados en redes de computadoras son los siguientes:

- Cable UTP categoría 5

Este es un cable que contiene 4 pares de hilos de cobre de par trenzado, sin malla y capaz de transmitir datos hasta 155 Mbps. El cableado UTP es la base de lo que llamamos cableado estructurado dentro de una empresa y como tal es una excelente comunicación dentro de un edificio. Se espera que durante los próximos cuatro o cinco años, este medio siga siendo el canal de comunicación por excelencia en un edificio. (Sosa, 2011)

- Fibra óptica

El cable de fibra óptica consiste en un conductor interno hecho de fibra de vidrio, llamado núcleo, y una cubierta hecha de fibra de vidrio, pero con un índice de refracción diferente, llamada cubierta. Aparte de ser el cable que transporta múltiples pares de fibras ópticas y es el medio de transmisión utilizado para la comunicación en un entorno WAN, aunque también se utiliza como backbone o enlace de alta velocidad para conectar las subredes de una empresa en locales donde puede demultiplexar e instalar fibra. (Castillo J. A., 2019)

- Sistema satelital

El sistema satelital es menos importante hoy en día para la transmisión de big data, sin embargo, su uso como medio de transmisión en redes informáticas se incrementará en los próximos años con la operación de satélites a baja altura. Su aplicación será principalmente para vehículos móviles que transporten equipos informáticos sobre los que se utilizará la denominada IP móvil. En cuanto a los satélites mexicanos ubicados a una altura de 36,000 km, creemos que debido a que se ha resuelto el problema de la gran transmisión de datos entre las ciudades de la República Mexicana, la red de fibra óptica de las empresas de servicios satelitales debe ser utilizada para brindar canales de comunicación a zonas del país que no están conectadas a redes de fibra óptica. (Sosa, 2011, pág. 46)

### *2.3.4 Familia de protocolos*

Un protocolo es el que permite la transferencia de datos entre computadoras dentro de una red, por lo que existen más de cien protocolos, pero el estudio se centrará más en el protocolo TCP/IP, en la siguiente tabla se encuentra una lista de los

protocolos más importantes y la utilidad de cada uno de ellos. (Manuel Ramirez, Carlos Polanco y Bernardo Farias, 2017)

**Tabla 1**

*Famila de protocolos*

| PROTOCOLO | UTILIDAD |
|---|---|
| HTTP | Acceso a páginas web |
| FTP | Transferencia de archivos |
| SMTP | Correo Electrónico |
| POP | Correo Electrónico |
| TELNET | Acceso a equipos remotos |

*Nota.* Cada Protocolo tiene una diferente utilidad.

Este protocolo permite la comunicación entre las computadoras de la red sin importar el sistema operativo de cada computadora. Se encarga de transmitir los datos en forma de paquetes y recogerlos en el orden en que son enviados.

TCP significa Protocolo de control de transmisión que garantiza que los datos enviados de un punto a otro no se pierdan y se reciban igual que cuando se enviaron. (Calderon, 2013)

#### 2.3.4.1 IPv4

Esta es la versión del protocolo IP más popular del mundo y, por lo tanto, más utilizado, la cantidad de direcciones IP que admite 2^32 o sea 4.294.967.296.

Este protocolo es la base de Internet, en la actualidad la direcciones en todo el mundo ya no satisface, y también hay desperdicio de direcciones, por lo que se creó una versión de lujo. (Manuel Ramirez, Carlos Polanco y Bernardo Farias, 2017)

#### 2.3.4.2 IPv6

Esta versión del protocolo fue creada para sustituir a IPV4. La versión 6 de este protocolo soporta un número de direcciones de 2^128 es decir 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones, dando así una solución al gran problema de la versión 4 del protocolo IP. (Calderon, 2013)

### *2.3.5 Seguridad de Redes Inalámbricas*

Las redes inalámbricas son muy populares en estos días y muy peligrosas en muchos casos, ya sea por cable o en la red, la información del usuario puede quedar expuesta y siempre se debe considerar la mejor protección. Esta tecnología también permite que terceros intercepten la información transmitida por el usuario más fácilmente que en las redes cableadas. (J.A.M.A, 2020)

**2.3.5.1 WEP.** Al existir muchos problemas de las redes inalámbricas con la seguridad, se implementó un tipo de seguridad llamado WEP, que significa Wire Equivalent Privacy, que resolvió estos problemas. En pocos años, este tipo de seguridad ha sido atacado por personas que quieren irrumpir ilegalmente en la red, presentando así vulnerabilidades en su seguridad a nivel empresarial, por lo que se considera poco confiable. Aun así, actualmente un gran porcentaje de las redes inalámbricas utilizan este tipo de seguridad debido a la facilidad de implementación, que se considera suficiente para los hogares. (Alex González Paz, David Beltrán Casanova y Ernesto Fuentes Gari, 2016)

**2.3.5.2 WPA.** Durante el desarrollo del estándar de seguridad inalámbrica 802.11i, se utilizó WPA como una mejora de seguridad temporal sobre WEP. La mayoría de las aplicaciones WPA modernas utilizan un clave pre compartido (PSK), comúnmente conocida como WPA Personal, y el Protocolo de integridad de clave transitoria o TKIP para el cifrado. WPA, al igual que WEP, después de haber sido sometida a pruebas de concepto y a demostraciones públicas aplicadas, resultó ser bastante vulnerable a la intrusión. Requiere un servidor configurado para realizar tareas de autenticación autorización y contabilidad. (J.A.M.A, 2020)

**2.3.5.3 WPA2.** Fue creado por IEEE según el estándar 802.11i, a diferencia de la mencionada seguridad creada por Wi-Fi Alliance y actualmente todos los dispositivos con tecnología inalámbrica deben contar con esta seguridad para poder ser aprobados por Wi-Fi Alliance y por lo tanto comercializados. Al igual que en la seguridad WPA, en WPA2 también puede utilizar el servidor de autenticación de usuarios en su versión Enterprise a nivel doméstico o de pequeña oficina en su versión Personal. (NetSpot, 2020)

**2.3.5.4 WPA 3.** La seguridad WPA3 está diseñada para ayudar a prevenir ataques. En lugar de depender de contraseñas compartidas, WPA3 registra nuevos dispositivos a través de procesos que no requieren el uso de una contraseña compartida. Este nuevo sistema, llamado Protocolo de aprovisionamiento de dispositivos Wi-Fi (DPP), funciona transmitiendo cómo acceder al sistema sin transmitir una contraseña a través de la red. (NetSpot, 2021)

## 2.4 Cableado Estructurado

El cableado estructurado debe soportar varios servicios de telecomunicaciones, principalmente datos y voz, integrados dentro de un edificio o campus. Una instalación de cableado estructurado está formada por cables, siendo el medio físico para la transmisión de datos y todos los demás elementos.

Esto nos permitirá conectar dispositivos a la red y, además, cumplir con los estándares de cableado establecidos. (Castillo M. , 2014)

**Tabla 2**

*Categorías del cableado*

| Categoría del Cableado | Velocidad de transmisión | Aplicaciones |
|---|---|---|
| Categoría 1 | Hasta 16 Kbps | Telefonía |
| Categoría 2 | Hasta 4 Mbps | Datos |
| Categoría 3 | Hasta 10 Mbps | Datos |
| Categoría 4 | Hasta 10 Mbps | Datos |
| Categoría 5 | Hasta 100 Mbps | Datos (Fast Ethernet) |
| Categoría 6 | Hasta 1 Gbps | Datos (Gigabit Ethernet) |
| Categoría 7 | Hasta 10 Gbps | Datos (Gigabit Ethernet) |

*Nota.* Cada categoría del cableado tiene una diferente velocidad de transmisión.

Los cables o elementos que componen una red están diseñados para trabajar en una determinada categoría. Conociendo la tecnología, es posible saber si un elemento puede integrarse en una instalación de cableado estructurado estandarizado. Las categorías están numeradas según la velocidad admitida por el cableado. Cuanto menor sea este número, menor será la velocidad. (Castillo M. , 2014)

**Tabla 3**

*Características de cable UTP*

| Categoría | Topologías | Velocidad Max de Transferencia | Distancia Max. Entre Repetidores por Norma | Requerimientos Mínimos de materiales posibles a usar | Status |
|---|---|---|---|---|---|
| **Cat. 3** | Voz, Arcnet - 2Mbits, Ethernet - 10Mbits | 10Mbits | 100 M | Cable y conectores coaxiales o cable y conectores UTP de menos de 100 MHz. | Obsoleto |
| **Cat. 5** | Inferiores, Fast Ethernet | 100Mbits | 90Mts + 10Mts. En Patch Cord | Cable UTP y conectores Categoría 5 de 100 – 150 MHz | Sujeta a Descontinuar |
| **Cat. 5e** | Inferiores y ATM | 165Mbits | 90 Mts + 10 Mts. En patch cords. | Cable UTP/FTP y conectores categoría eran 5e de 150 – 350 MHz. | Actual |
| **Cat. 6** | Inferiores y Gigabit Ethernet | 1000Mbits | 90 Mts. + 10 Mts. En patch Cords, con cable de cobre Cat 6, 1Km en Fibra Multimodo, 2Km en Fibra Monomodo | Cable de cobre y conectores Categoriab6 y/o Fibra Óptica | Punta Tecnológica |

*Nota.* La tabla muestra los diferentes tipos de categoría de cables UTP

Los sistemas de cableado estructurado deben adaptarse a lo siguiente:

### *2.4.1 Cable de Par Trenzado*

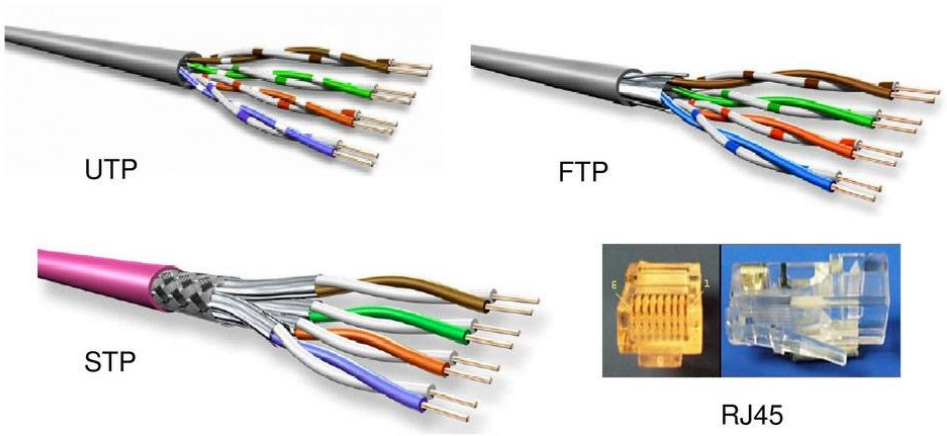
Dentro del cableado estructurado solo se utilizan cables de pares trenzados UTP Y FTP, para conexiones desde los conectores a rosetas. (Castillo J. , 2020)

### *2.4.2 Conector RJ-45*

El conector RJ45 es una interfaz física comúnmente utilizada para conectar redes informáticas con cableado estructurado. Tiene ocho pines o conexiones eléctricas, comúnmente usado como la punta de un cable de par trenzado. (Avalos, 2021)

**Figura 1**

*Elementos del cableado estructurado*




*Nota.* Existen diferentes elementos del cableado estructurado pero entre los importante para un Red es el cable UTP y RJ45. Tomado de *Redes de Datos (pag. 7), por J.A. Ferreyra, 2017, DocPlayer.*

### *2.4.3 Esquema General de Cableado Estructurado*

**2.4.3.1 Cableado Horizontal.** El cableado horizontal se refiere al cableado que se extiende desde el almacén del área de trabajo de telecomunicaciones hasta la sala de telecomunicaciones, es decir, el cableado que conecta el equipo en el mismo piso a un enrutador de fábrica. (Parra, 2017)

**2.4.3.2 Cableado Vertical.** Un sistema de cableado vertical o troncal proporciona conexiones entre los cuartos de servicio de entrada del edificio, los cuartos de equipos y el cuarto de telecomunicaciones, además, el backbone incluye una conexión vertical entre los pisos de los edificios hogar. (Parra, 2017)

### *2.4.4 Normas de Cableado Estructurado*

Cuando se trata de asegurar un proyecto de infraestructura, instalación o cableado, se basa en una serie de estándares de cableado estructurado, establecidos por las organizaciones involucradas en su desarrollo. (Wiki Pluz, 2018)

**Figura 2**

*Normativas del Cableado estructurado*


*Nota.* Existe diferentes normativas para cada proceso de cableado estructurado. Tomado de *Normas sobre el cableado Estructurado, por UNITEL,2020.*

**2.4.4.1 TIA (Telecommunications Industry Association).** Fue fundada en 1985 tras la disolución del monopolio AT&T. Es responsable de desarrollar estándares de cableado industriales voluntarios para varios productos de telecomunicaciones y tiene más de 70 estándares preestablecidos. (UNITEL, 2020)

**2.4.4.2 ANSI (American National Standards Institute).** Esta organización es responsable de supervisar el desarrollo de los estándares para productos, servicios, procesos y sistemas. ANSI también es miembro de la Organización Internacional para la Estandarización (ISO) y la Comisión Internacional de Ingeniería Eléctrica (IEC). (Parra, 2017)

**2.4.4.3 EIA (Electronic Industries Alliance).** Esta organización fue establecida por la asociación de empresas electrónicas y de alta tecnología en los Estados Unidos, su misión es promover el crecimiento del mercado y la competitividad de la industria de alta tecnología con los esfuerzos locales e internacionales. (UNITEL, 2020)

**2.4.4.4 ISO (International Standards Organization).** Esta organización fue fundada en 1947 a nivel mundial, con normas nacionales, con más de 10 países. (Parra, 2017)

**2.4.4.5 IEEE (Instituto de Ingenieros Eléctricos y de Electrónica).** Es el principal responsable de las especificaciones de Redes LAN como 802.3 Ethernet, 802.5 Token Ring, ATM y Gigabit Ethernet. (Wiki Pluz, 2018)

### *2.4.5 ANSI/TIA/EIA-568-B*

Tiene como objetivo definir estándares que permitan el diseño e implementación de sistemas de cableado estructurado para edificios de oficinas y entre edificios en campus universitarios. La mayoría de las normas se ocupan de las definiciones de tipos de cables, espaciamiento, conectores, arquitectura de cableado, normas para equipos terminales y características de rendimiento, requisitos de instalación de cables y métodos de prueba. (FIUBA, 2018)

- TIA/EIA 568-B1: Requerimientos generales

- TIA/EIA 568-B2: Componentes de Cableado de Par Trenzado Balanceado
- TIA/EIA 568-B3: Componentes de Fibra óptica.

### *2.4.6 ANSI/TIA/EIA-569-A*

Norma para telecomunicaciones y líneas espaciales entre edificios comerciales sobre cómo enrutar el cableado. (FIUBA, 2018)

### *2.4.7 ANSI/TIA/EIA-570-A*

Normas de Infraestructura Residencial de Telecomunicaciones. (Jose, 2012)

### *2.4.8 ANSI/TIA/EIA-606-A*

Norma para la gestión de infraestructuras de telecomunicaciones en edificios comerciales. (Jose, 2012)

### *2.4.9 ANSI/TIA/EIA-607*

Requisitos para la instalación de sistemas de puesta a tierra de telecomunicaciones en edificios comerciales. (Parra, 2017)

### *2.4.10 ANSI/TIA/EIA-758*

Cliente estándar Propietario del cableado externo de la fábrica de telecomunicaciones. (FIUBA, 2018)

## 2.5 Hotspot

Un hotspot es un punto de acceso a Internet a través de una red inalámbrica local y mediante el uso de un enrutador conectado a un proveedor de servicios de Internet.

Normalmente, su función principal es administrar clientes a través de puerto fijo, proteger su red a través de un sistema que le dice:

- Quién se conecta
- Cuando se conecta
- Cuánto tiempo esta
- Qué ancho de banda le doy
- Cuánto permito que pueda descargarse
- Reglas de Firewall

Para conectarse los usuarios pueden usar una computadora portátil, un teléfono inteligente o cualquier otro dispositivo móvil que permita el acceso a través de una conexión inalámbrica (Wi-Fi en general). Actualmente, hay dispositivos que combinan la funcionalidad de punto de acceso Wi-Fi y enrutador en un solo dispositivo.

Los hotspots se encuentran frecuentemente en los restaurantes, estaciones de tren, aeropuertos, bibliotecas, hoteles, hospitales, cafeterías, librerías, estaciones de servicio, supermercados, parques y campamentos, teléfonos públicos de pago y otros lugares públicos. (Gómez, 2020)

### *2.5.1 Hotspot Wi-Fi gratuito*

Hay varias formas de obtener Wi-Fi gratis. El primero es Wi-Fi gratuito que viene con otro servicio, como la membresía de un club o la reserva de hotel.

Por supuesto, no es completamente gratis porque hay que pagar por otra cosa. Además, estos proveedores pueden limitar el ancho de banda por usuario, lo que reducirá las velocidades de conexión.

La alternativa a un punto de acceso Wi-Fi gratuito es un sitio web comercial. Los sitios comerciales se pueden configurar con tarjeta de crédito o acceso con contraseña. Algunos de estos sitios también restringen el acceso a un pequeño grupo de páginas relacionadas. (Century Link, 2021)

### *2.5.2 Hotspot Wi-Fi Portátil*

Si necesita un punto de acceso en cualquier lugar, puede usar un punto de acceso Wi-Fi portátil. En lugar de buscar un lugar con acceso Wi-Fi, un punto de acceso Wi-Fi portátil te trae Internet. Este dispositivo contiene un enrutador móvil y se puede usar para conectar varios dispositivos al mismo tiempo sin descargar software adicional para el dispositivo.

Sin embargo, deberá traer otro dispositivo cargado (esto reduce la conveniencia de ser portátil). Además, la conexión a Internet puede ser más lenta. (Century Link, 2021)

### *2.5.3 Seguridad de Hotspot*

El Cifrado es una clave para la seguridad inalámbrica. Sin él, los hackers pueden capturar sus datos. Sin embargo, los datos no pueden ser cifrados a medida que fluye desde el hotspot Wi-Fi a su computadora. (Calero, 2017)

# Capítulo III

# 3 Desarrollo del proyecto

## 3.1 Levantamiento de infomación

### *3.1.1 Situación Actual*

**Edificio 1:** El edificio 1 está conformado de la siguiente manera:

- **Piso 3:** Están ubicados los cursos de 9no año Paralelo ‘A’ y ‘B’ y 10mo año Paralelo ‘A’ de Educación Básica con aulas de 8x6 m de ancho.
- **Piso 2:** Están ubicados los cursos de 10mo año Paralelo ‘B’ de Educación Básica, 8vo año Paralelo “A” y 7mo año, con aulas de 8x6 m de ancho.
- **Planta Baja:** Está conformada la parte administrativa (DECE, secretaria general, Colecturía, Laboratorio de Informática y Rectorado) y un aula del 8vo año Paralelo “B”.

### *3.1.2 Laboratorio de Informática:*

Se encuentra ubicado en la planta baja del edificio principal y contiene lo siguiente:

- 1 Router MikroTik y TP-LINK.
- 1 ordenador de escritorio destinado para uso del docente.
- 13 ordenadores de escritorio para uso de los estudiantes.
- 1 gabinete – Rack

## 3.2 Adquisición de Equipos

El principal objetivo de cada adquisición es saber la calidad y características de cada equipo.

**Tabla 4**

*Especificaciones de Routers*

| Routerboard Hap Lite | RB750Gr2 |
|---|---|
| **Arquitectura**: MIPS | **Arquitectura**: MIPS-BE |
| **Frecuencia de CPU**: 650 MHz | **CPU frecuencia nominal:** 720 MHz |
| **Cantidad de Núcleos de CPU:** 1 | **Número de núcleos de CPU**: 1 |
| **Sistema Operativo**: RouterOS | **Sistema operativo**: RouterOS |
| **Memoria RAM:** 32 MB | **Memoria RAM:** 64 MB |
| **Almacenamiento**: 16 MB | **Almacenamiento**: 16 MB |
| **Tipo de Almacenamiento**: DESTELLO | **Tipo de almacenamiento:** DESTELLO |
| **Puertos Ethernet**: 10/100 Mbps | **Puertos Ethernet:**10/100/1000 Mbps |

*Nota.* La adquisición de equipos se realiza en base a la calidad y especificaciones buscando un adecuado equipo para una Red LAN.

El router que se escogió es el RB750Gr2, la selección se hizo mediante un cuadro comparativo viendo así que el router tiene mejores especificaciones desde su Memoria RAM hasta su frecuencia nominal siendo recomendado para redes LAN.

**Tabla 5**

*Especificaciones Switch*

| Nombre | Switch Tenda 24 Puertos | Switch Tp-link 24 Puertos |
|---|---|---|
| **Estándares y Protocolos** | IEEE 802.3, IEEE 802.3u, IEEE 802.3x | IEEE 802.3i, IEEE 802.3u, IEEE 802.3x |
| **Capacidad de Switch** | 4.8 Gbps | 4.8 Gbps |
| **Montaje** | Soporte | Rack Montable |
| **Certificación** | CE, FCC, RoHS | FCC, CE, RoHS |
| **Memoria Búfer** | S/N | 2 Mb |
| **Medios de red** | CAT5 / 5e UTP o mejor | Cable 3, 4 5, 10BASE-T: categoría UTP (máximo 100m) |

*Nota.* Diferentes Modelos y especificaciones.

La selección de switch TP-link se realizó en base a las computadoras en funcionamiento de esta manera al tener 24 puertos y solo tener activas 10 pc se plantea que en un futuro se puedan completar las 20 mesas de trabajo y dar un funcionamiento total a las características de los equipos.

**Tabla 6**

*Materiales para el cableado estructurado*

| Cantidad | Material | Descripción |
|---|---|---|
| 14 | Canaletas 40x25 | Sin Divisiones, se puede pasar hasta 13 cables. |
| 10 | Cajetines dobles | Marca Dexson - Sobrepuesto |
| 300m | Cable Utp Cat. 5e | Marca HIKVISION |
| 20 | Jacks de red Hembras | Marca Nexxt |
| 100 | RJ45 | Cat 5e |

*Nota.* La tabla muestra los diferentes materiales y marca para el cableado estructurado.

**Tabla 7**

*Especificaciones Access Point*

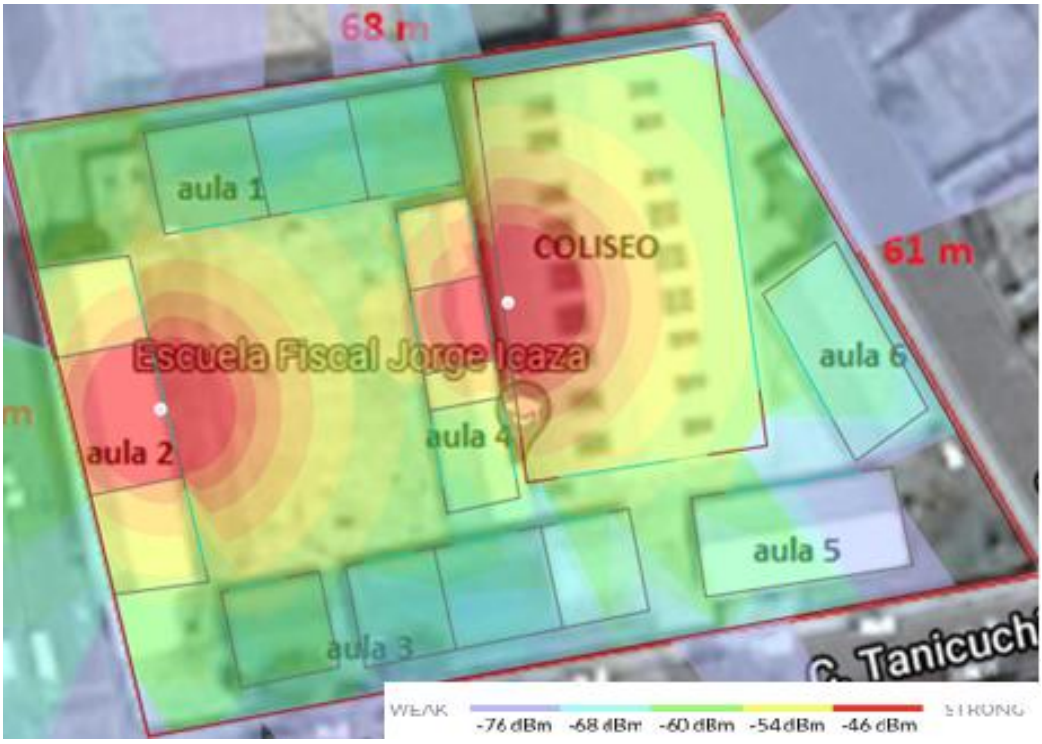
| Nombre | UAP-AC-LR Ubiquiti | EAP245 Tp – Link |
|---|---|---|
| **Potencia de transmisión** | 24dBm (2.4GHz)<br>22dBm (5GHz) | 20dBm (2.4GHz)<br>23dBm (5GHz) |
| **Antenas** | Dual-Band Antenna, Tri-Polarity, 2.4 GHz: 3 dBi<br>5 GHz: 3 dBi | Dual-Band Antenna 2.4GHz: 3x4dBi<br>5GHz: 3x4dBi |
| **Estándares Wi-Fi** | 802.11 a/b/g/n/r/k/v/ac | 802.11 ac/g/n/b/a |
| **Certificación** | CE, FCC, IC | CE, FCC, RoHS |
| **Seguridad inalámbrica** | WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES) | WEP, WPA/WPA2-Personal/Enterprise Encryption |
| **Clientes concurrentes** | 250 + | 100 |
| **Velocidad máxima de datos** | 450 Mbps (2.4GHz) + 867Mbps (5GHz) | 450 Mbps (2.4GHz) + 1300Mbps<br>(5GHz) |

*Nota.* La tabla muestra las características de entre dos Access Point.

La selección de Access Point a utilizar fue mediante la comparación de las características en donde el principal objetivo es cubrir el área de la unidad educativa teniendo en cuenta ese punto se opta por seleccionar el UAP-AC-LR ya que la potencia al igual que la frecuencia ayudan a abarcar la toda la institución

**Figura 3**

*Simulación del UAP-AC-LR Ubiquiti*




*Nota.* Esta figura muestra la simulación al utilizar dos Access Point UAP-AC-LR en la herramienta UniFi Design Center propia de la marca Ubiquiti.

### 3.3 Implementación red LAN

El laboratorio de la institución no cuenta con una buena conexión de electricidad, los cables se encuentran fuera de las canaletas y de las mesas de cada computador, por lo que primero se debe organizar bien los cables e identificar la conexión de la electricidad con cada mesa.

**Figura 4**

*Cableado de electricidad*

*Nota.* Los cables de electricidad no pueden estar fuera de las canaletas porque este podría ser peligroso para los estudiantes.

Después de identificar cada una de las conexiones se debe separar y cambiar el orden de las computadoras para que el laboratorio este mejor distribuido y este se vea más amplio.

**Figura 5**

*Ubicación de la mesas*


*Nota.* Las mesas están cerca de las ventanas, asegurando que en cada mesa quede un espacio para evitar contagios ante esta pandemia.

Previo a finalizar la organización de los cables de electricidad, se conecta correctamente a cada mesa comprobando que cada PC tenga electricidad, agregando

una canaleta más para las mesas faltantes y de este modo colocando cada cable en sus canaletas correspondientes para que de esta manera se vea mejor estéticamente.

**Figura 6**

*Cable de luz ubicada en su respectiva canaleta*

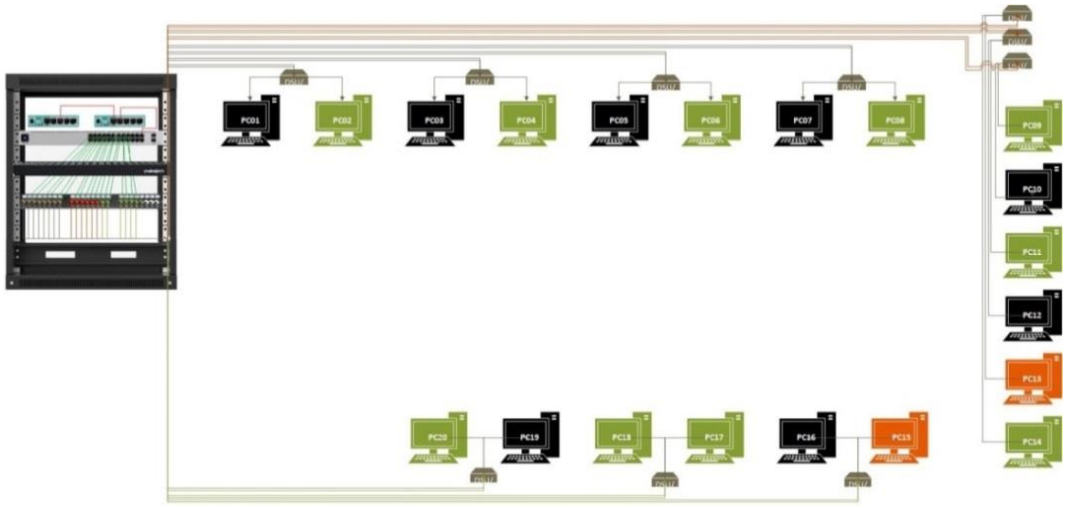
*Nota.* Algunas canaletas se encontraban en mal estado por lo que se cambió para evitar futuros problemas.

### *3.3.1 Implementación del Cableado Estructurado*

Al culminar la parte eléctrica se empieza con la parte del cableado estructurado de red. El laboratorio no cuenta con las herramientas necesarias por lo que se debe adquirir nuevos materiales y realizar un plano de la estructura.

**Figura 7**

*Diagrama de cableado*



*Nota.* La imagen muestra las PC, verdes están activas, negras mesa disponible y naranja PC con fallos.

Una vez hecha la planificación del cableado estructurado se empieza a ubicar las canaletas tomando en cuenta la Norma ANSI 569-B, la altura para la instalación debe ser de 1 m, aunque también puede considerarse una altura de 30 cm del piso.

**Figura 8**

*Aplicación de canaletas*

*Nota*. El cableado estructurado va encima del cableado eléctrico, no se podía cambiar nada, debido a que el cableado eléctrico ya estaba desde antes.

Previo a finalizar la instalación de las canaletas se procede a colocar los cajetines en lugares estratégicos cerca de los computadores 3 cm arriba de las canaletas en la mitad de dos mesas.

**Figura 9**

*Ubicación de cajetines*

*Nota.* Los cajetines deben quedar bien puestos a la pared por lo que se debe asegurar muy bien con tacos Fischer y tonillos.

Ya terminada la implementación de las canaletas y cajetines, se procede a pasar el cable por sus respetivas canaletas tomando en cuenta las recomendaciones de la Norma ANSI/TIA/EIA 569A, en las canaletas de mayor tamaño (40x25, 60x40, 100x45) se puede pasar hasta 13 cables UTP. Para llegar al gabinete se deberá coger la medida desde los cajetines y dejar 2 m de remanente en el gabinete.

**Figura 10**

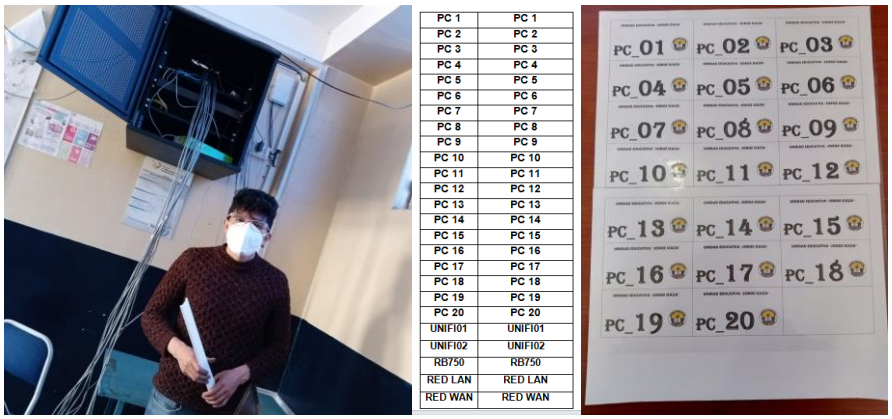
*Ubicación de los cables en las canaletas*

*Nota.* En las canaletas de mayor tamaño utilizar la banda adhesiva como ayuda de montaje, y fijar con tornillos.

Para continuar con el cableado estructurado se debe etiquetar los cables de manera que al llegar al gabinete se identifique del cajetín que llega, la norma ANSI/TIA/EIA-606 proporciona normas para la codificación de colores, etiquetado, y documentación de un sistema de cableado instalado. Este estándar menciona que los identificadores deben ser visibles durante la instalación y mantenimientos.

**Figura 11**

*Etiquetado de cables*




*Nota.* Las etiquetas deberán ser impresas o producidas por un elemento mecánico.

Una vez concluido el etiquetado del cableado y revisado que las canaletas estén aseguradas, es recomendable ubicar las mesas más atrás para facilitar el ponchado de cada cable con los jacks Rj45 Cat 5e que después serán ubicados en cada cajetín.

**Figura 12**

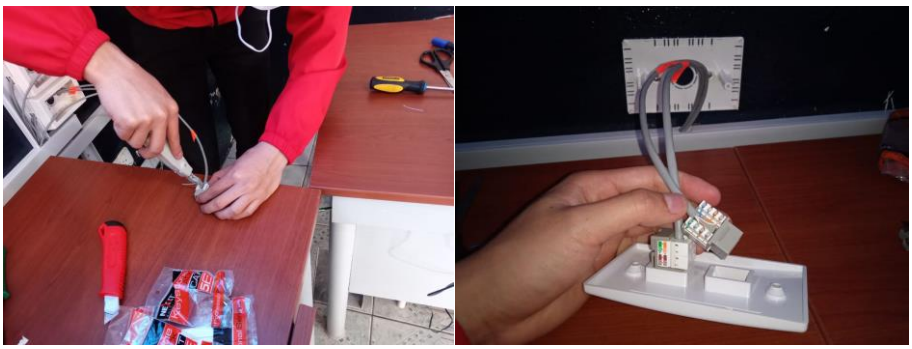
*Conexión de los jacks de red*

*Nota.* El remanente del cable de los cajetines deber ser 30 cm.

Para continuar la parte del Ponchado de jacks, se toma en cuenta la normativa de código de colores EIA/TIA 568-B, este será importante al momento de ponchar en el Patch Panel y no tener inconvenientes en la transmisión de datos.

**Figura 13**

*Código de colores para el Jack de Red*



*Nota.* Se utiliza la normativa ANSI/TIA/EIA 568B, utilizando el código de colores EIA/TIA 568-B.

Previo a finalizar el ponchado de jacks, se coloca en los cajetines correspondientes teniendo cuidado y revisando que el cable UTP no esté haciendo fricción para posteriormente asegurarlos con sus respectivos tornillos.

**Figura 14**

*Cierre de cajetines*

*Nota.* Para verificar que los jacks estén bien ponchados se debe hacer una prueba desde el Patch Panel.

### *3.3.2 Conexión del Patch Panel*

Antes de empezar esta conexión primero se debe organizar el gabinete y los cables que van dentro, porque estos no pueden quedar colgando o desorganizados.

**Figura 15**

*Organización e implementación del gabinete*

*Nota*. En el gabinete los cables todo debe encontrase etiquetado y ordenado para que se vea estéticamente bien.

El proceso de conexión del Patch Panel es similar al ponchado de un Jack, pero para empezar lo primero que se debe hacer es identificar el tipo de código de colores de los estándares del cable red que se va a utilizar. Hay que tomar en cuenta el tipo de colores que se utilizó en el Jack, en este caso sería EIA/TIA 568-B. Después de haber identificado se pela el cable UTP para luego separarlos y ordenarlos, así teniendo más facilidad de acoplarlo al Patch Panel.

**Figura 16**

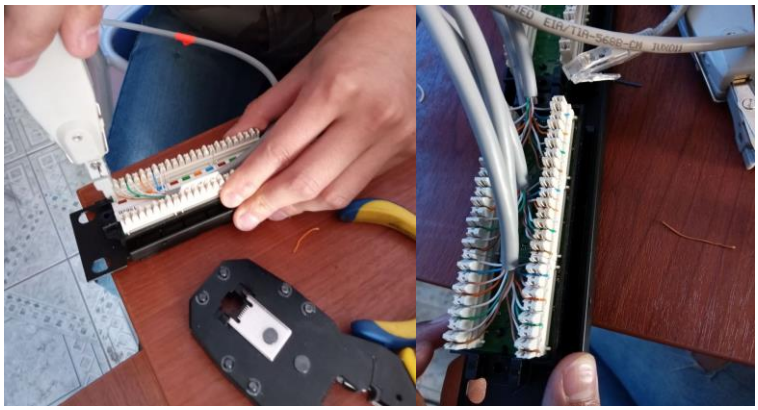
*Orden de cables e identificación de la normativa de Ponchado*

*Nota.* Para esto el cable se debe pelar 3 cm y se debe ir arreglando en el Patch Panel para que se pueda quedar firme.

Una vez ya ordenado los cables se realiza la conexión al Patch Panel siguiendo la normativa del orden de colores que se utilizara, que sería el mismo orden de conexión que se utilizó en el Jack de los cajetines. Para esto se necesitará una ponchadora de impacto que facilitará este proceso.

**Figura 17**

*Conexión según la Norma EIA/TIA 568-B*

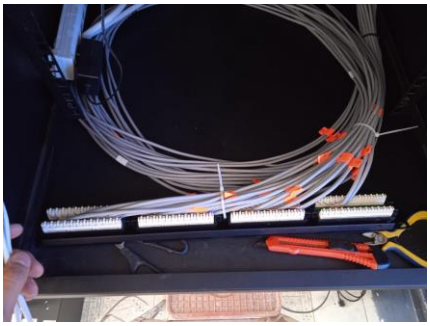


*Nota*. Para poder realizar la conexión en el Patch Panel es mejor empezar desde atrás hacia adelante.

Una vez culminado la parte del Patch Panel se ubica en el gabinete, asegurándolo con sus tornillos. Después se procede a ordenar los cables y verificar que ninguno quede colgado.

**Figura 18**

*Implementación del Patch Panel en el Gabinete*



*Nota*. Es recomendable usar velcro para que los cables no estén muy apretados.

### *3.3.3 Conexión del Patch Panel con el Switch*

Una vez culminado la conexión del Patch Panel, conectar el switch y realizar patchcords de 0.40 cm, mediante la normativa ANSI/TIA-568.

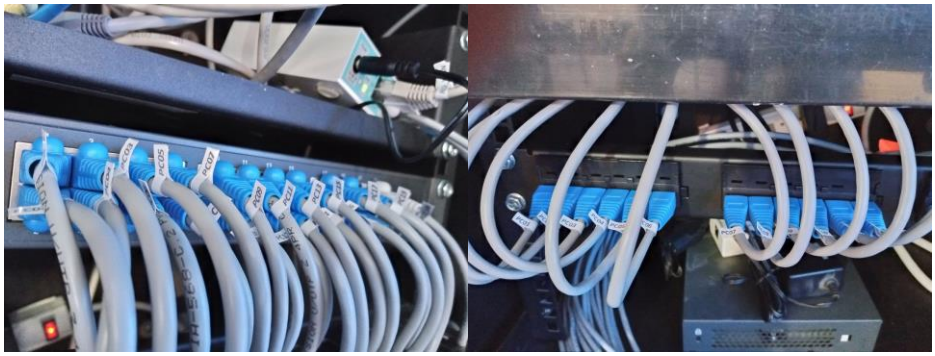
**Figura 19**

*Conexiones en el Switch desde el Patch Panel*

*Nota*. Es recomendable tener un organizador de cables para tener una mejor visualización y orden.

**Figura 20**

*Etiquetado de patchcords en el switch y Patch Panel*



*Nota.* Los cables en el gabinete siempre deberán estar etiquetados según la norma 606.

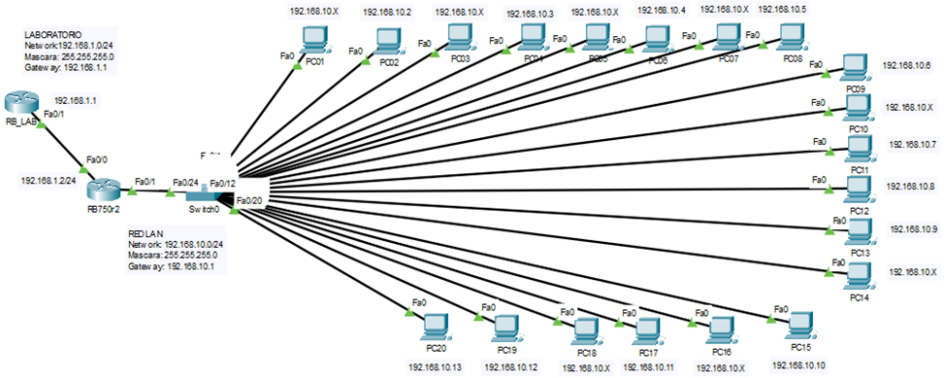
### *3.3.4 Configuración Router RB750r2*

El laboratorio de computación cuenta con 13 computadoras, pero solo 10 están en funcionamiento, se lleva a cabo una simulación en Cisco Packet Tracer donde consta con dos Routers, uno del proveedor del servicio de internet y el otro se utilizará como salida de internet al laboratorio.

El Switch tendrá activos 20 puertos Fast Ethernet porque existen mesas de trabajo con puertos disponibles, las computadoras que están activas se asignará una dirección IP estática, porque estas permitirán que las páginas web funcionen más rápido, por otra parte, los puertos disponibles tendrán IP dinámica de esta manera se tendrá acceso a internet sin necesidad de configurar una dirección IP.

**Figura 21**

*Simulación Red LAN*



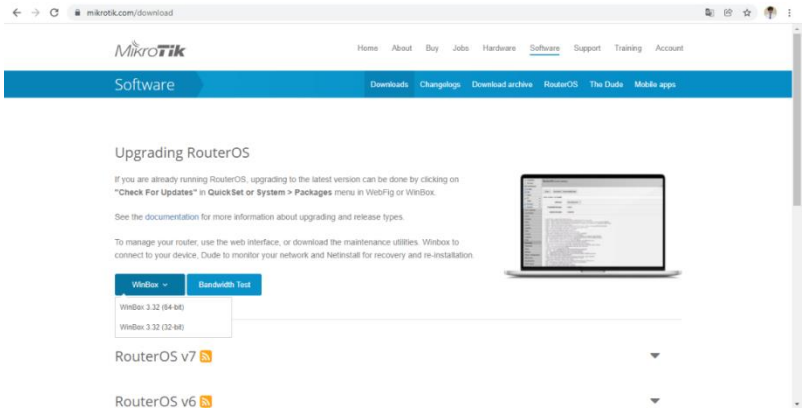

*Nota.* La simulación muestra una perspectiva del funcionamiento que tendrá el Laboratorio de Computación.

### *3.3.5 Descarga del Software Winbox*

Primero se descarga el instalador del software en el sitio web de MikroTik https://mikrotik.com/download, posee una breve introducción sobre las actualizaciones además de herramientas que ayudan al monitoreo de redes “Dude” y la recuperación y reinstalación de dispositivos MikroTik “NetInstall”.

**Figura 22**

*Página de Descarga Winbox*

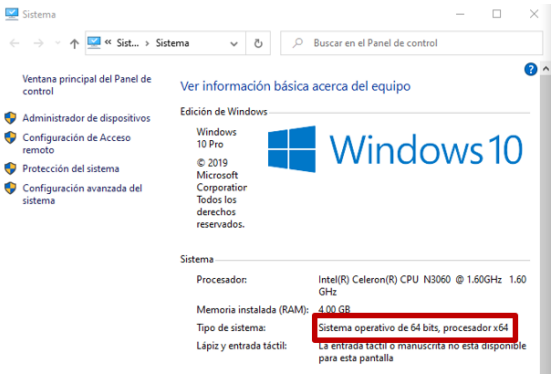



*Nota.* En la página MikroTik se puede seleccionar la arquitectura de 32-bit o 64-bit dependiendo del sistema operativo y procesador de la computadora.

Para verificar el tipo de sistema operativo que tienen la computadora se deben dirigir a Panel de Control > Sistema y Seguridad > Sistema. En información básica del equipo se constatará el software que se utilizará. Después en la página de MikroTik, iniciar la descarga.

**Figura 23**

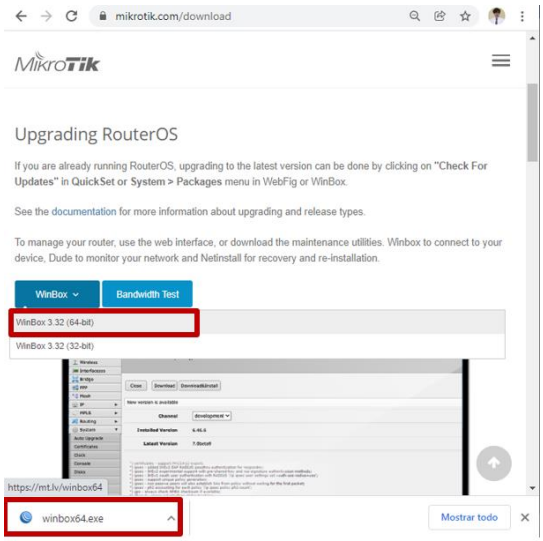
*Verificación del Sistema Operativo*




*Nota.* Verificar el tipo de sistema operativo para tener un software compatible.

**Figura 24**

*Descarga WinBox 3.32 (64-bits)*



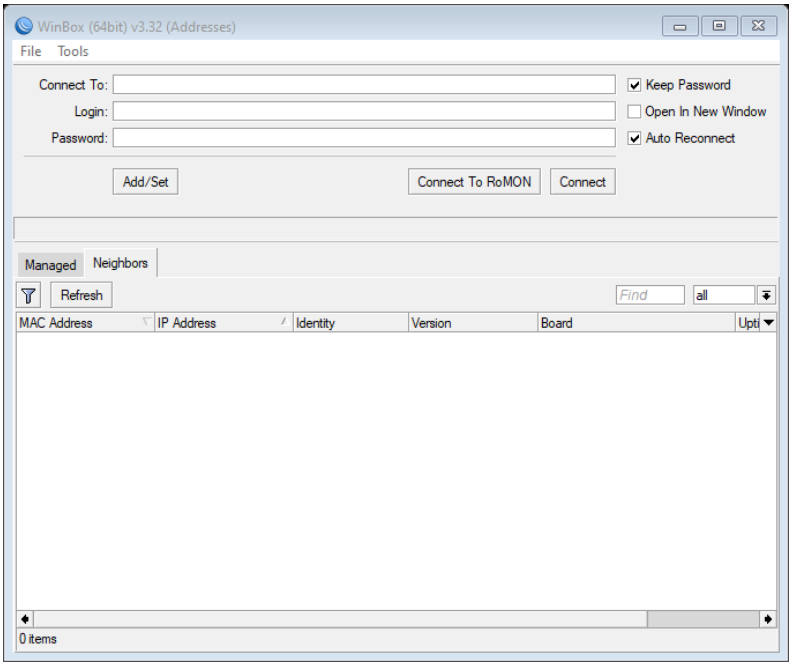

*Nota.* Verificar el tipo de sistema operativo antes de descargar el Software para prevenir posibles errores.

### *3.3.6 Ejecución WinBox*

Para ingresar por primera vez al software, dar doble clic en el icono que se descargó, una vez dentro la interfaz muestra de qué forma se puede ingresar ya sea mediante la dirección IP o MAC Address del equipo, además no tiene el nombre de acceso tampoco una contraseña.

**Figura 25**

*Ventana de inicio*

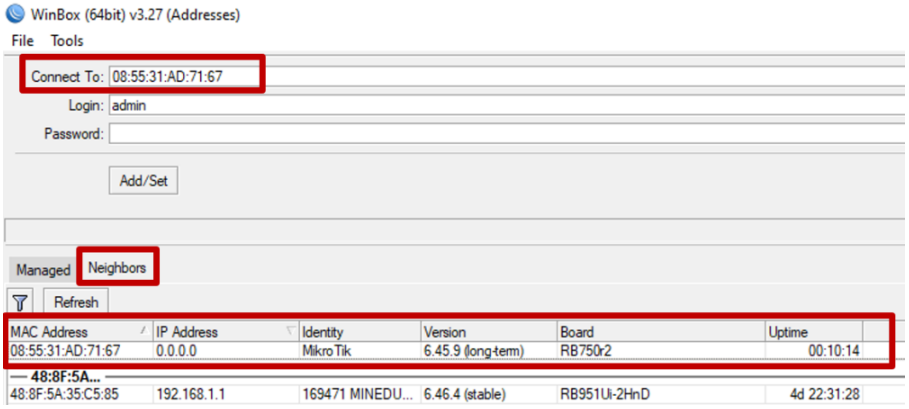



*Nota.* Esta ventana muestra los dispositivos a los que desea ingresar.

Para que el Software detecte el Router RB750r2 en la pestaña de Neighbors existe la opción Refresh, dar clic e inmediatamente aparecerá el dispositivo. Para acceder al Router se debe ingresar mediante el MAC Address, seguidamente dar clic en Connect una vez seleccionado el equipo.

**Figura 26**

*Acceso al Router RB750r2*

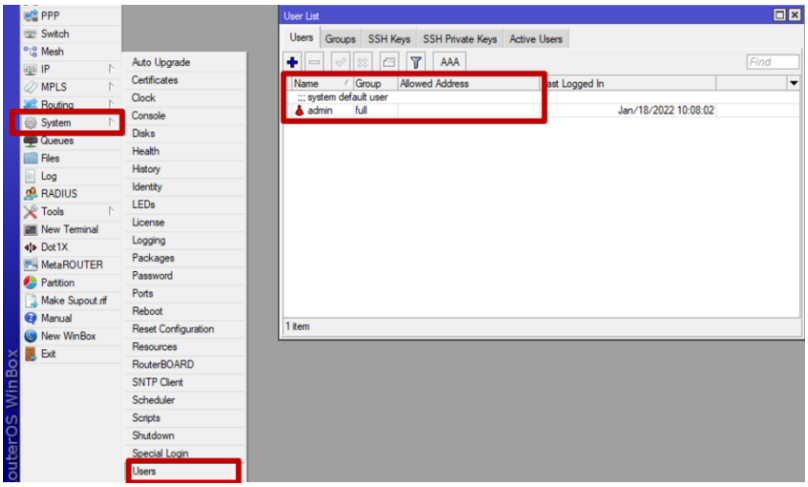



*Nota.* En la ventana muestra el Router que se va a configurar y también el otro Router que pertenece al proveedor de Internet.

Como medida de seguridad para el acceso a las configuraciones del Router en System, seleccionar Users y seguidamente se abrirá una ventana que tiene el usuario por defecto, dar doble clic y en el recuadro Admin colocar una contraseña, para que solo el personal designado pueda acceder a la aplicación.

**Figura 27**

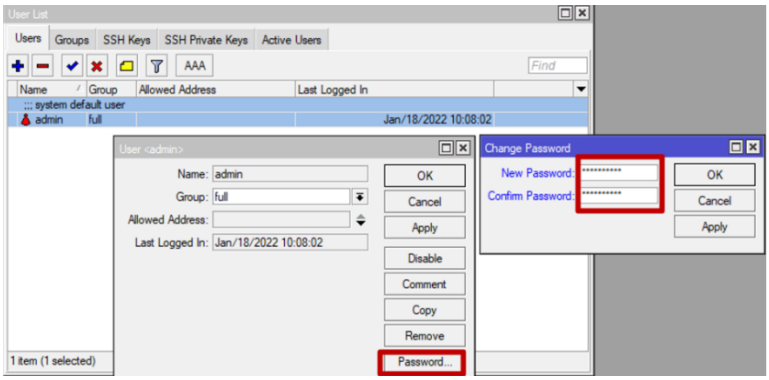
*Users List*




*Nota*. Esta ventana muestra el usuario Admin que tiene el Router MikroTik por defecto.

**Figura 28**

*Contraseña de acceso*



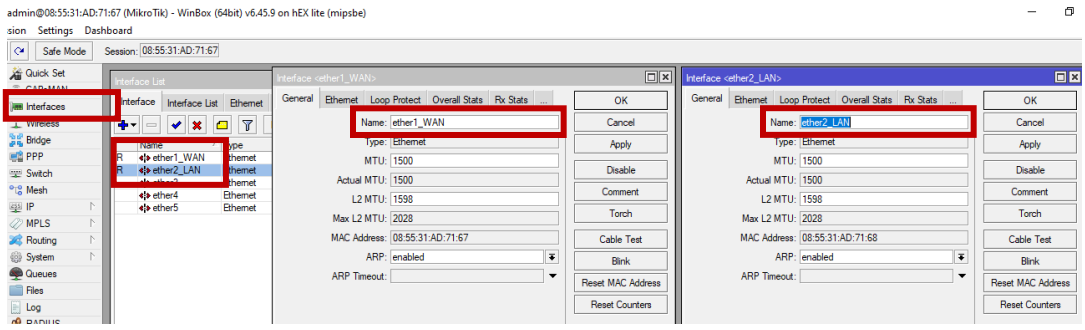

*Nota*. Para el acceso solo colocar una contraseña al usuario Admin.

### *3.3.7 Configuración Red LAN*

Primero se debe verificar el número de interfaces que tiene el Router para poder asignar las redes, dar doble clic en ether1 y se abrirá una nueva ventana, en la pestaña general se cambiará el nombre por ether1_WAN que se utilizará como entrada a internet de la misma forma en la interfaz ether2 se cambiará el nombre a ether2_LAN que se utilizará como salida a Internet, luego seleccionar Apply para aplicar los cambios.

**Figura 29**

*Asignación de nombres a las interfaces ether1 y ether2*



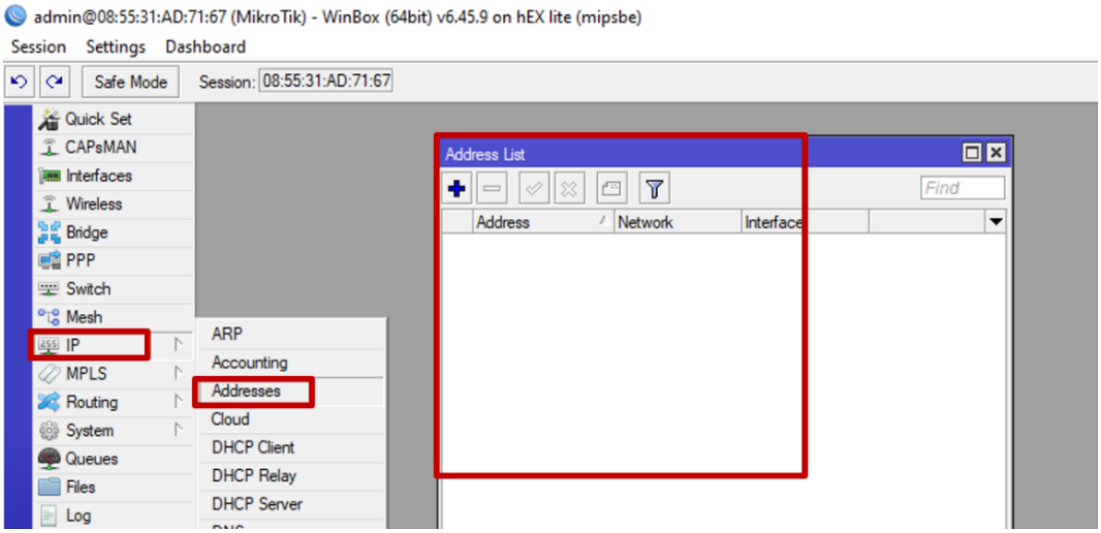

*Nota.* Cambiar el nombre de las interfaces ayudan a identificar los puertos del Router que se van a utilizar.

### *3.3.8 Asignación de Direcciones IP a las Interfaces*

Para la configuración hay que dirigirse a la barra lateral izquierda dar clic en IP y seleccionar Addresses, en la ventana pulsar en símbolo más que sirve para crear un listado de las direcciones IP, además muestra la red y la interfaz utilizada.

**Figura 30**

*Interfaz de Direcciones Ip*

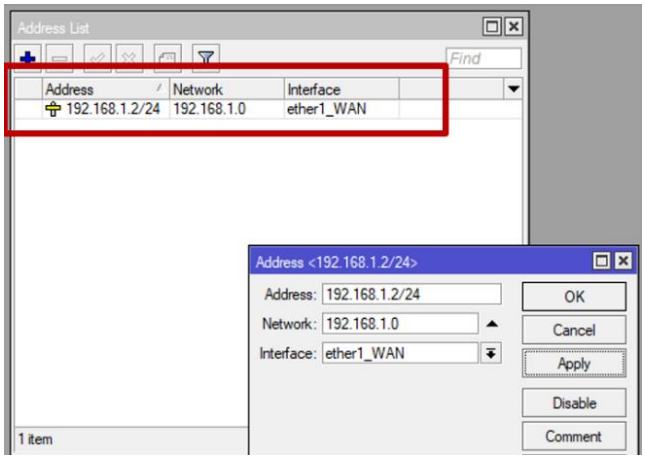



*Nota.* Aquí se guarda todas las direcciones IP asignadas.

A continuación, en la ventana Address se debe colocar la dirección IP 192.168.1.1/24 del servidor. La dirección IP que se utiliza como salida a internet es la 192.168.1.2/24 con dirección de red 192.168.1.0, luego en interfaz seleccionar el puerto ethe1_WAN, dar clic en Apply para guardar los cambios y OK para salir de la ventana. En la lista ya existe una nueva dirección IP creada como muestra en la figura 31.

**Figura 31**

*Asignación dirección IP Red WAN*

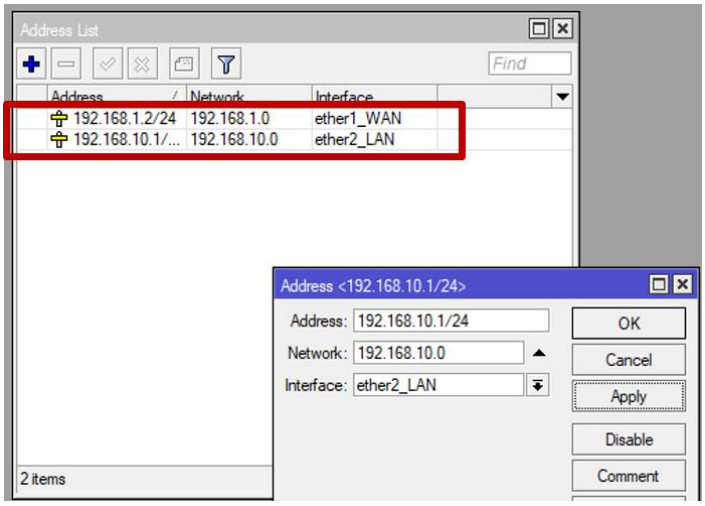



*Nota*. La dirección IP para la red WAN se creó correctamente.

Seguidamente, se configura la dirección IP para la red LAN del Laboratorio para esto usaran la IP inicial 192.168.10.1/24 con dirección de red 192.168.10.0 y en la interfaz seleccionar ether2_LAN. Aplicar los cambios y observar que se haya creado una nueva dirección.

**Figura 32**

*Asignación dirección IP Red LAN*



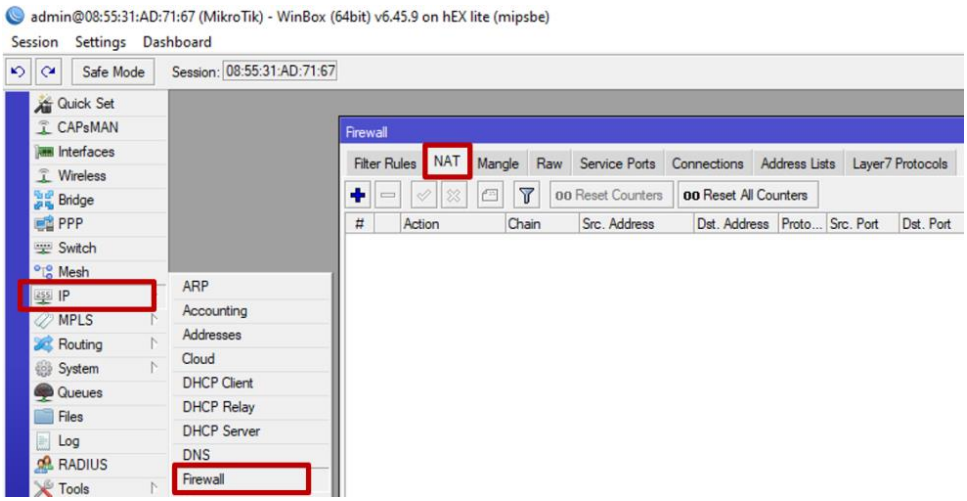

*Nota.* La dirección IP para la red LAN se creó correctamente.

### *3.3.9 Crear una NAT (Network Address Translation)*

Se dirigen a la opción IP, seleccionan Firewall que controla el acceso de una computadora a la red y de elementos de la red a la computadora, la NAT traducirá una dirección IP pública a una dirección IP privada y viceversa.

**Figura 33**

*Proceso para la configuración NAT*

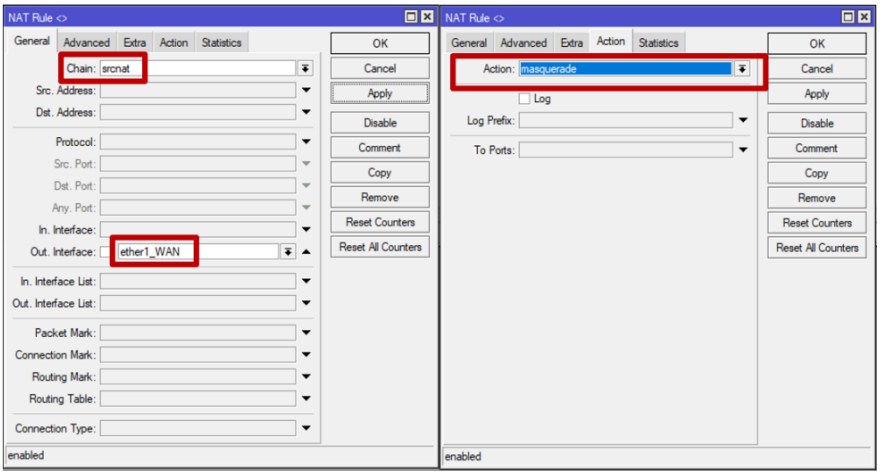



*Nota*. Es necesario crear una NAT por seguridad a la red.

A continuación, dar clic en el símbolo más para añadir una nueva regla, ahora dirigirse a la pestaña general y en el casillero Chain, seleccionar srcnat en Out. En la interface colocar el puerto ether1_WAN de salida a Internet. Después en la pestaña Action se colocará masquerade, que básicamente es enmascarar la dirección IP de los equipos de tu red interna.

**Figura 34**

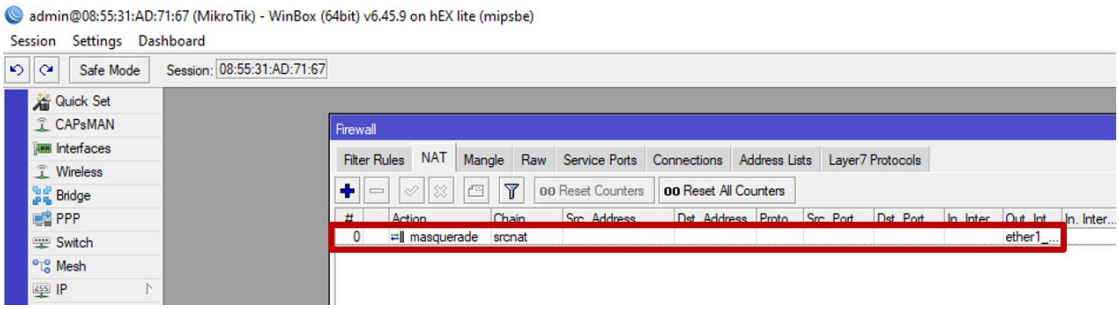
*Configuración NAT*




*Nota.* Seleccionar la interfaz de salida al puerto WAN que dará salida a Internet.

**Figura 35**

*Creación de la NAT*



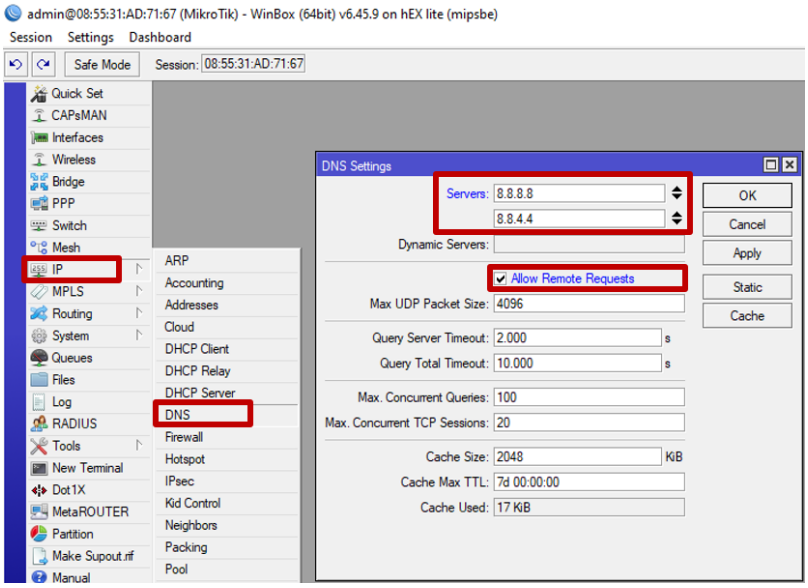

*Nota*. Verificar que la nueva regla se haya añadido a la lista.

### *3.3.10 Configurar un DNS Público*

A continuación, dirigirse a la opción IP y en la pestaña DNS dar clic, después en el casillero Servers colocar los DNS 8.8.8.8 y 8.8.4.4 de Google que ahora son mucho más seguros y privados. Con un Check mark seleccionar la opción “Allow Remote Requests” para que el Router atienda solicitudes remotas.

**Figura 36**

*Configuración DNS Google Public*




*Nota.* Aquí se pone los DNS o domino de los servidores de Google.

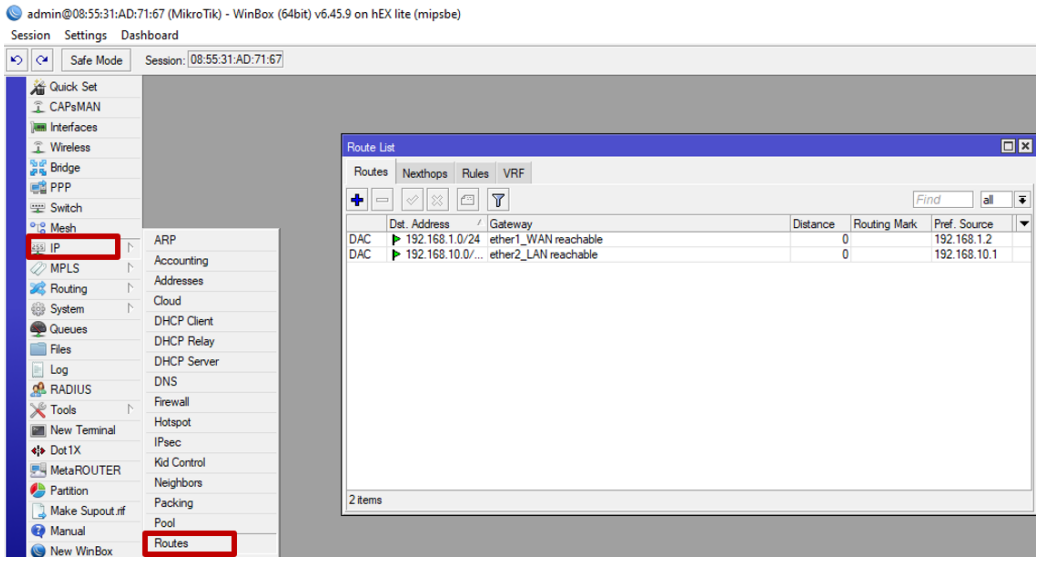
### *3.3.11 Configuración Ruta Estática*

Para esta configuración se debe acceder a IP, seleccionar la opción Routes, luego se abrirá una ventana en donde se podrá apreciar enrutamientos dinámicos conectados, para crear una ruta estática para la Red WAN hay que dar clic en el símbolo más.

Después en el casillero Gateway colocar la dirección IP 192.168.1.1 que es la puerta de enlace al servidor de Internet y automáticamente se conecta con el puerto ether1_WAN. Finalmente se creó la ruta a internet.

**Figura 37**

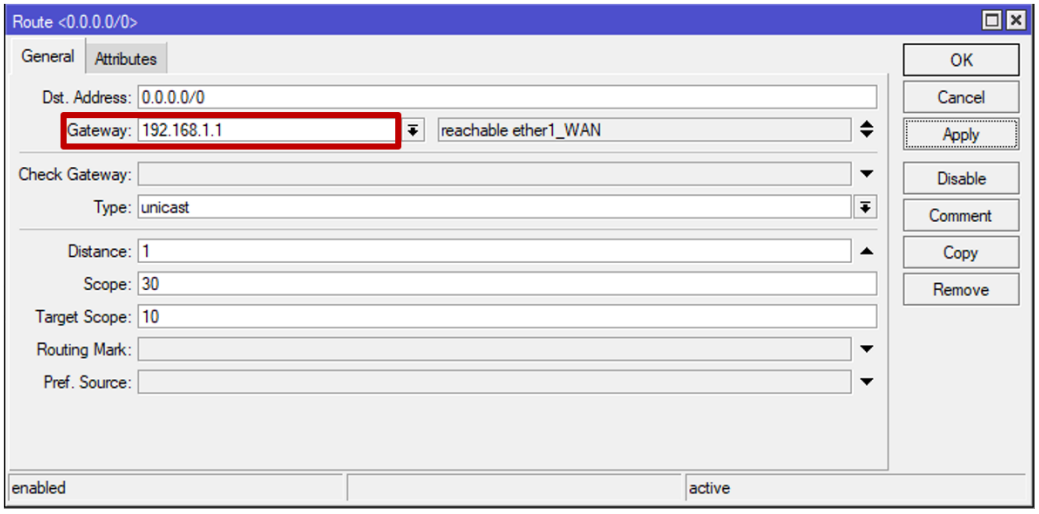
*Interfaz de la ventana de enrutamiento*




*Nota.* Aquí se puede observar la interfaz donde se pueden realizar enrutamientos estáticos.

**Figura 38**

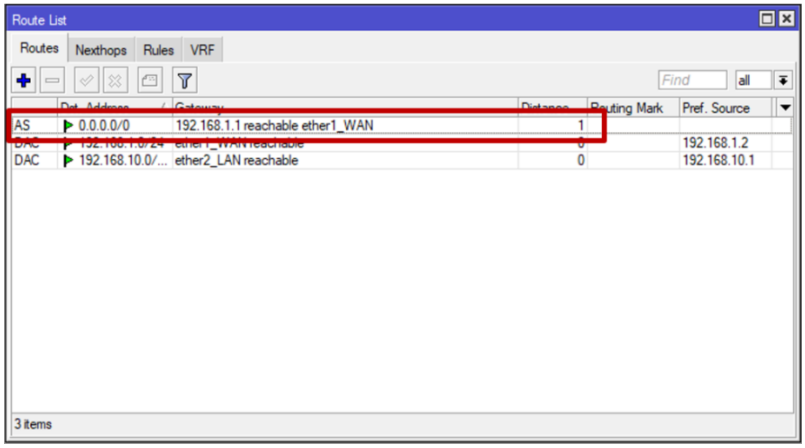
*Asignación IP puerta de enlace*




*Nota.* Aquí se coloca únicamente la dirección IP de la puerta de enlace y se deja los demás parámetros por defecto.

**Figura 39**

*Verificación del enrutamiento en el Route List*



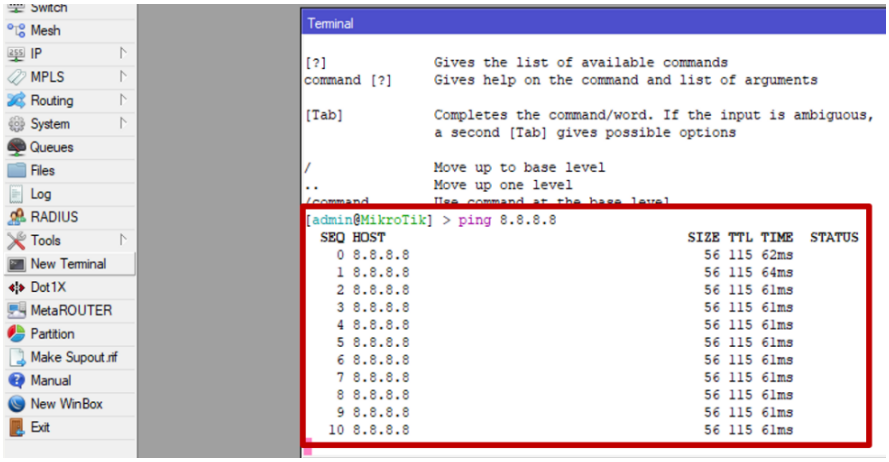

*Nota.* Aquí se puede constatar el enrutamiento estático en el puerto ether1_WAN.

### *3.3.12 Comprobación de Conectividad a Internet*

Posteriormente al terminar las configuraciones para la salida a internet por el ether1_WAN y la entrada a Internet por el ether2_LAN se realiza un ping hacia el servidor de Google 8.8.8.8 para verificar la velocidad de respuesta y la calidad de la red.

**Figura 40**

*Conexión al servidor de Google*



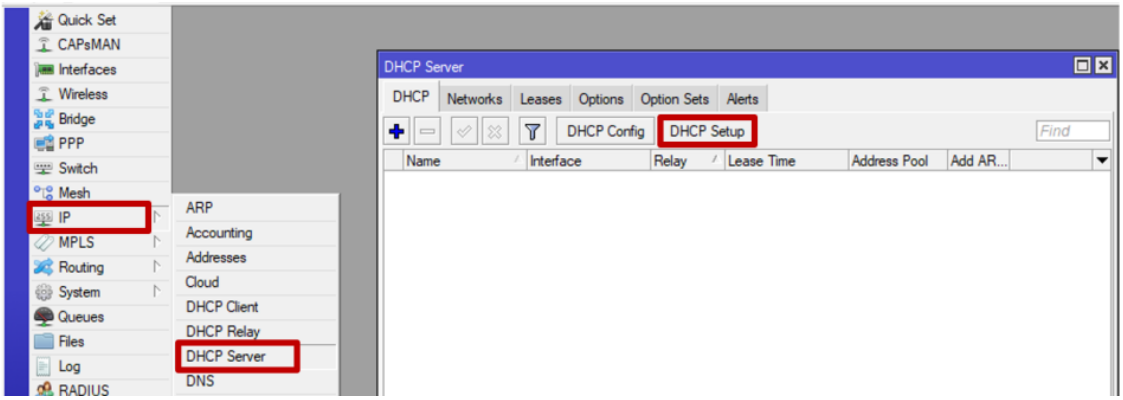

*Nota*. En la venta Terminal se pueden aplicar líneas de código para realizar configuraciones.

### *3.3.13 Configuración DHCP para la Red LAN del Laboratorio*

El DHCP permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y automáticamente. Para la configuración seleccionar IP, dar clic en DHCP Server y en la opción DHCP Setup, dar clic y se iniciara el proceso de configuración.

**Figura 41**

*Interfaz DHCP Server*

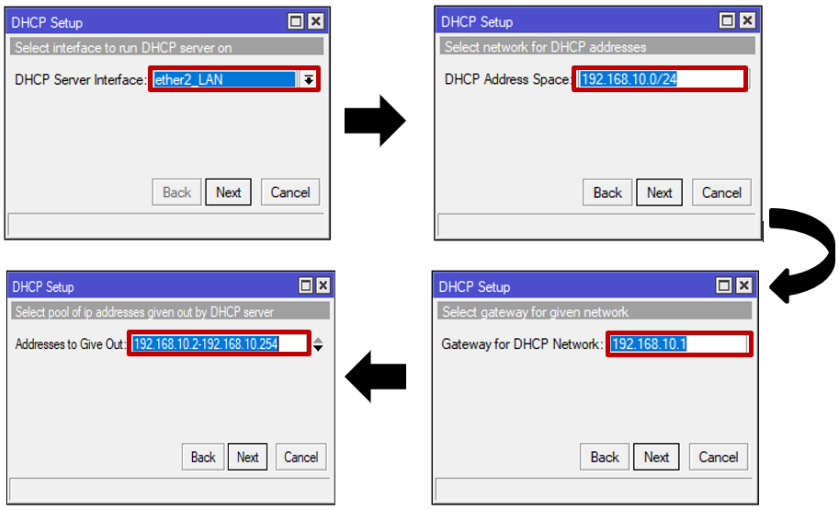



*Nota*. En esta ventana se realiza la configuración dinámica de host.

Después de presionar la opción DHCP Setup nos dirige a una ventana en donde se seleccionará ether2_LAN, en la siguiente ventana automáticamente muestra la dirección IP de la Red LAN que se había colocado en la asignación de IPs, posteriormente en la otra ventana muestra la puerta de enlace de red y en la última ventana da a conocer el rango de direcciones IP que se va a utilizar.

**Figura 42**

*Configuración de DHCP en la IP 192.168.10.0*

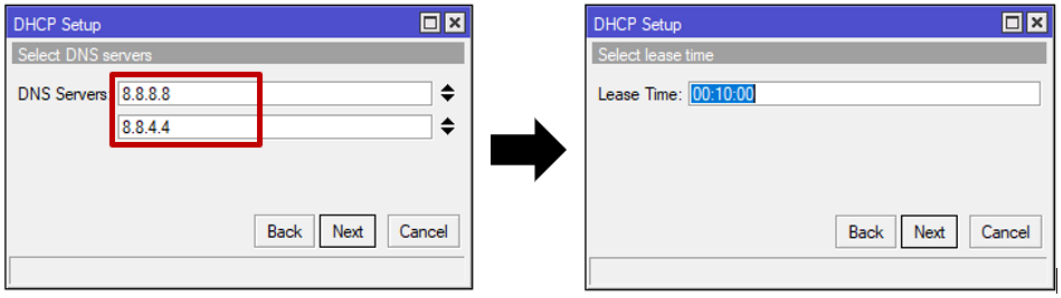



*Nota.* Aquí se selecciona la interfaz con la dirección IP que deseen que el software realice DHCP.

Después de haber configurado las direcciones IP en la ventana DNS Server de forma automática se coloca los DNS de Google que fueron configurados anteriormente.

**Figura 43**

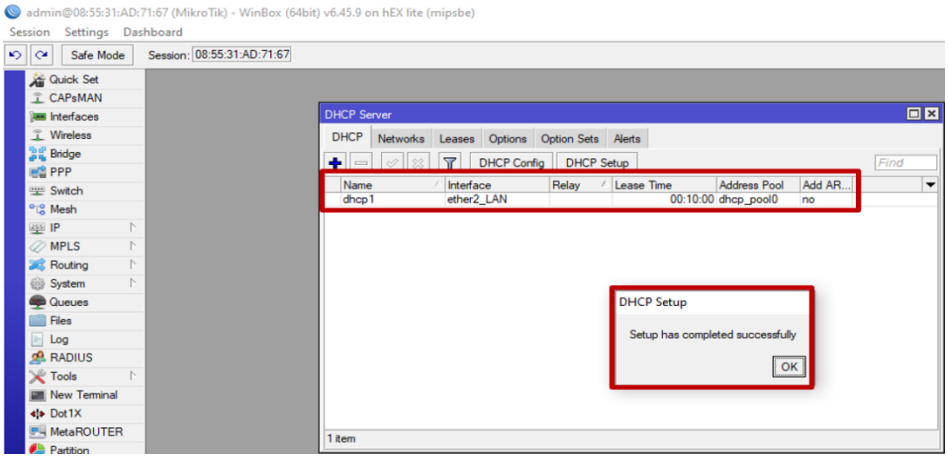
*Asignación DNS para la Red LAN*




*Nota*. En esta interfaz se coloca los DNS de Google y el tiempo de arrendamiento de DHCP se deja por defecto.

**Figura 44**

*Comprobación de la creación de DHCP red LAN*



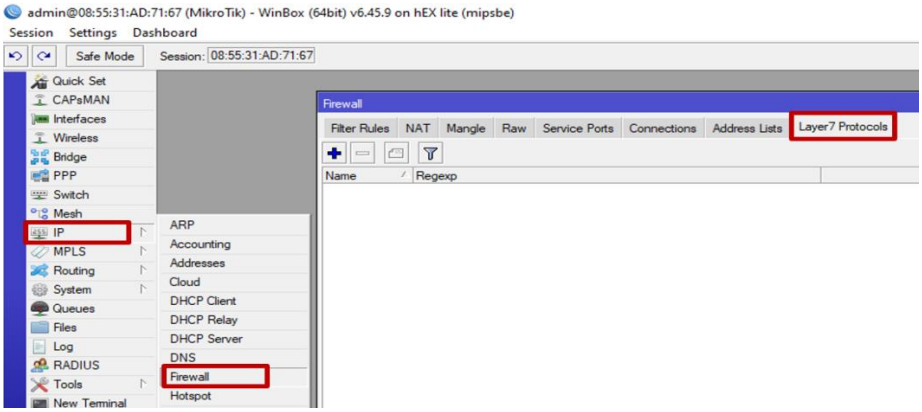

*Nota.* La interfaz LAN, se creó correctamente en el DHCP.

### *3.3.14 Bloqueo Redes Sociales*

Para realizar la configuración de bloqueo de sitios Web en la red LAN del Laboratorio seleccionar IP, en la pestaña Firewall entrar a la opción Layer7 Protocols, para generar nuestra regla de bloqueo de páginas.

**Figura 45**

*Interfaz de Layer 7 Protocols*

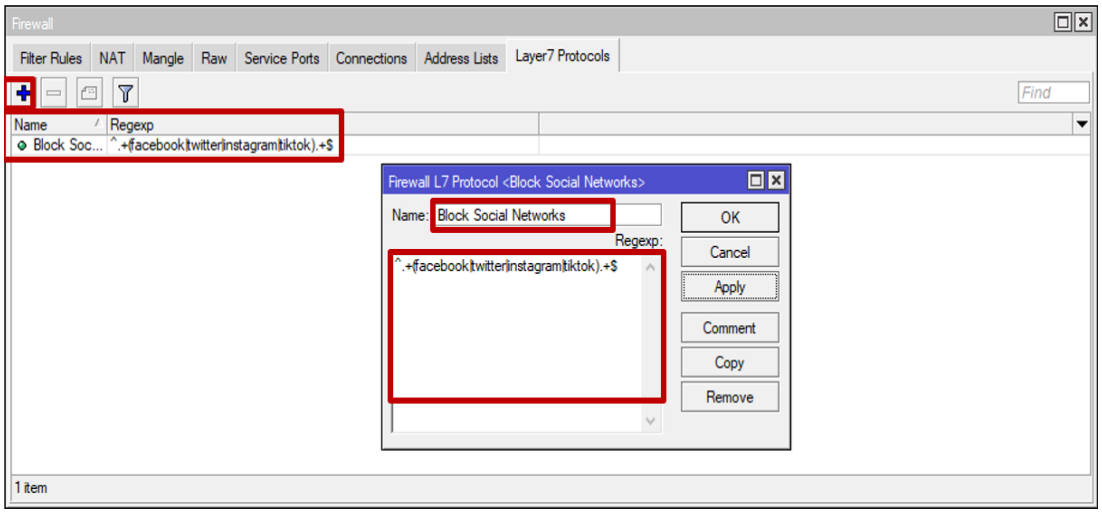



*Nota.* Aquí se puede crear una lista de páginas que se desea restringir el acceso.

A continuación, seleccionar el signo más para agregar una nueva regla de bloqueo, nombrar la regla como Block Social Networks. Para poder bloquear varios dominios se utiliza la siguiente línea de código: ^. +(facebook|twitter|instagram|tiktok). +$. Se debe aplicar los cambios y a continuación se creará la regla de bloqueo.

**Figura 46**

*Creación de bloqueo redes sociales*

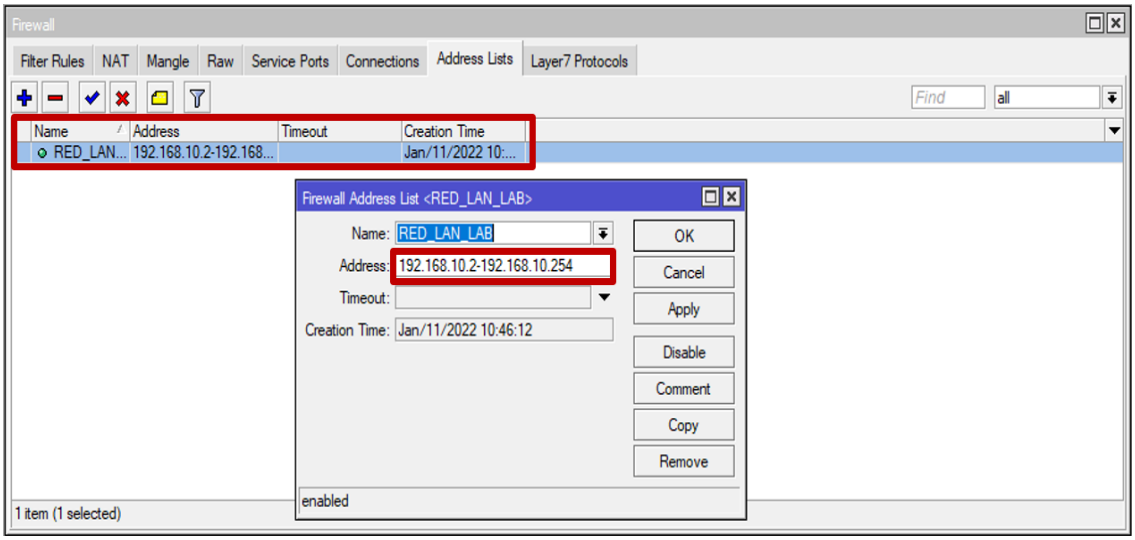



*Nota*. Aquí en El Layer7 se realiza el bloqueo de Páginas.

Una vez creada la regla de bloqueo pulsar en la pestaña Address Lists, dar clic en más y se desplegará una ventana donde se colocará un nombre para identificar la lista, después se coloca el rango de direcciones IP de la red LAN.

**Figura 47**

*Configuración lista de direcciones*



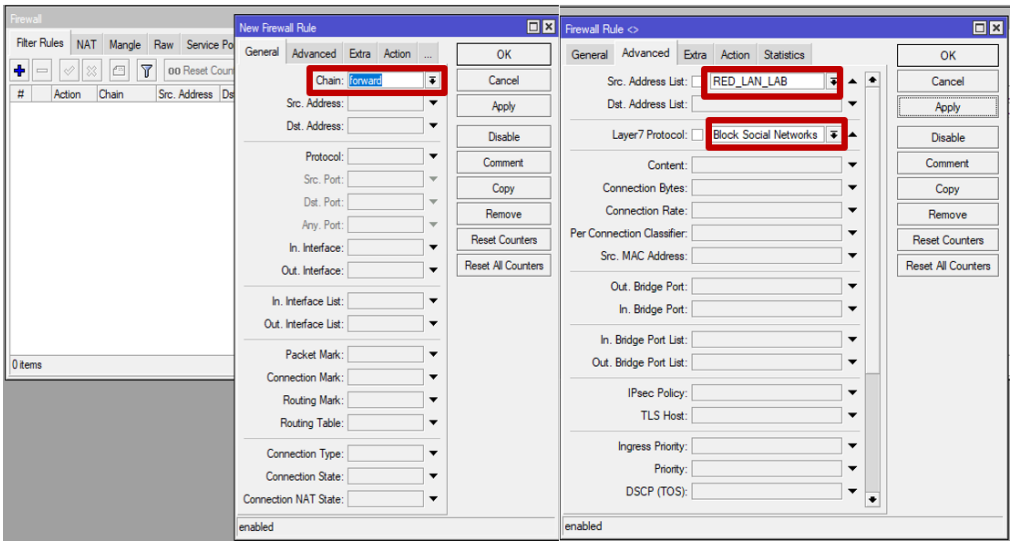

*Nota*. En esta ventana se coloca la primera hasta la última dirección IP valida de red.

Seguidamente en la pestaña Filter Rules se creará una regla y en la pestaña General Chain se escribirá forward que es cadena de reenvió. Ahora en Advanced se debe seleccionar la RED_LAN_LAB que se había creado, en Layer 7 Protocol se coloca el nombre de la regla de bloqueo creada. En la pestaña Action seleccionar drop que son paquetes descartados.

La regla de bloque de Redes Sociales se creará con acción de bloqueo como se muestra en la **Figura 48 y 49.**

**Figura 48**

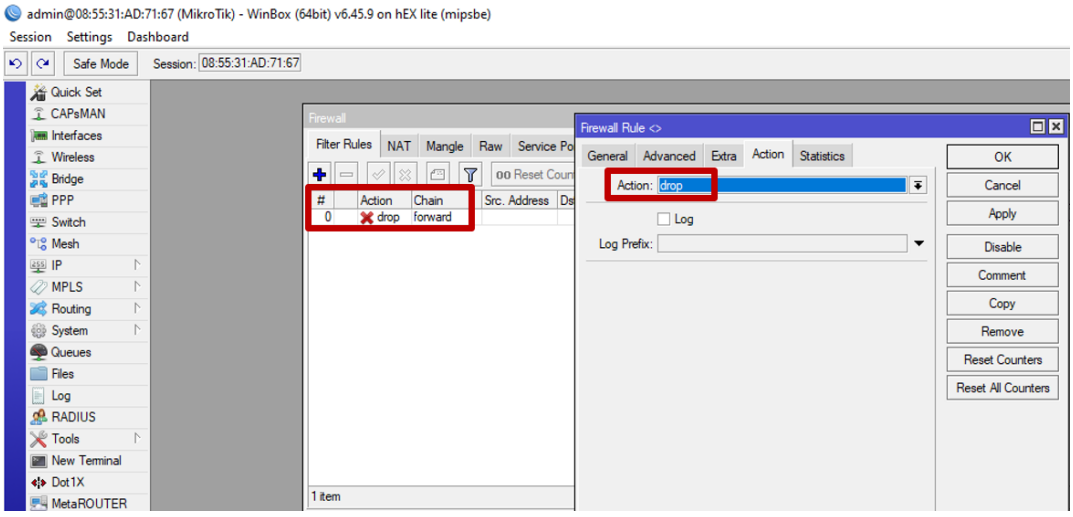
*Configuración con Address List y Layer 7 Protocol*




*Nota*. En esta ventana se coloca las configuraciones de bloqueo es decir los Firewall.

**Figura 49**

*Bloqueo Redes Sociales*



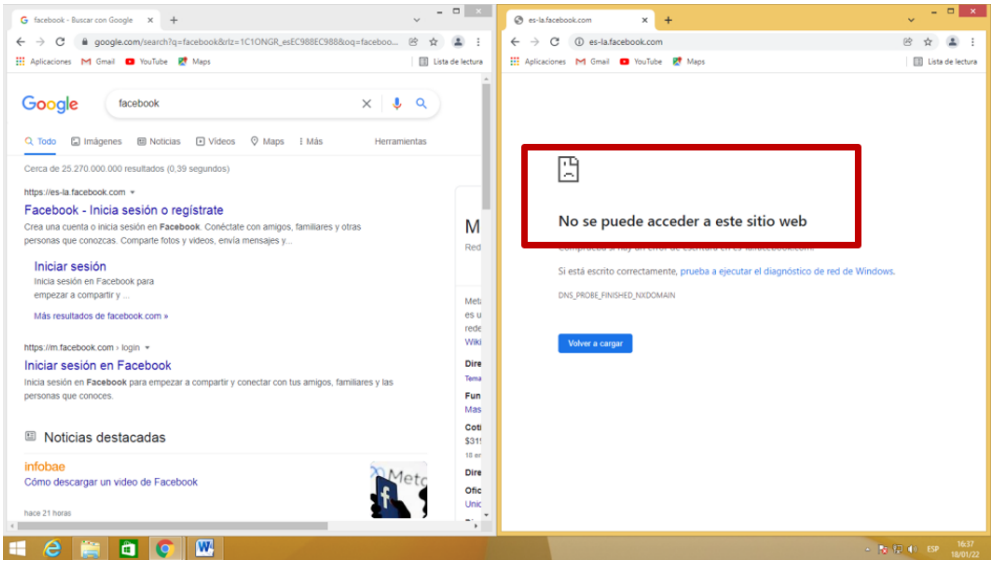

*Nota*. En la ventana Filter Rules se ve una “X” en la regla ya que esta con Action Drop.

### *3.3.15 Ejecución Bloqueo Redes Sociales*

Una vez aplicadas las configuraciones de bloqueo, ingresar a un navegador de preferencia, acceder a Google, escribir un nombre de la red social que se bloqueó (Facebook, Twitter, Instagram y TikTok) dar clic en el primer enlace y como se muestra en la figura 49 la página no carga además de mostrar un mensaje indicando que no se puede acceder a este sitio Web.

**Figura 50**

*Páginas Bloqueadas*



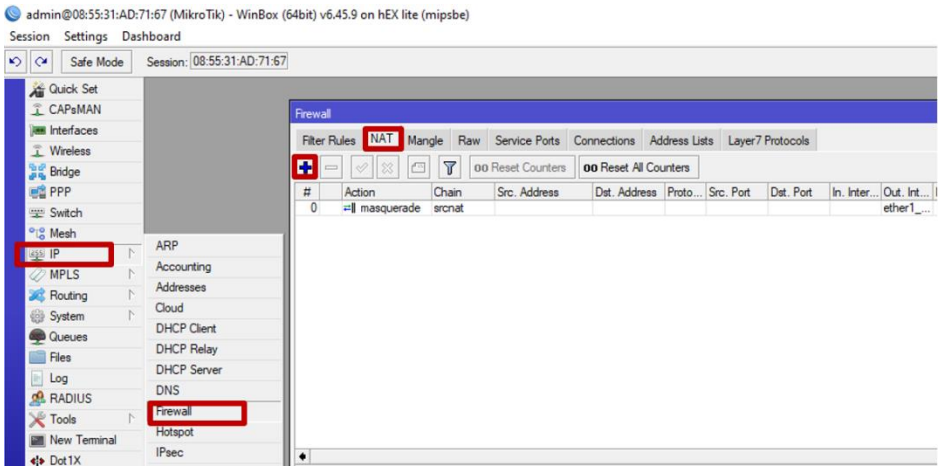

*Nota*. Únicamente los sitios que están dentro del Layer 7 Protocols están bloqueados, WhatsApp, Telegram entres otros se encuentran disponibles.

### *3.3.16 Bloqueo DNS Family Shield*

Para la configuración de una red familiar se utiliza el DNS Family Shield con acceso a Internet más rápido y seguro donde se tendrá un control de acceso así también bloqueando el acceso a contenido para adultos, para lo cual se debe dar clic en la opción IP y seleccionar Firewall luego en la pestaña NAT.

**Figura 51**

*Interfaz de creación de la regla de bloqueo*

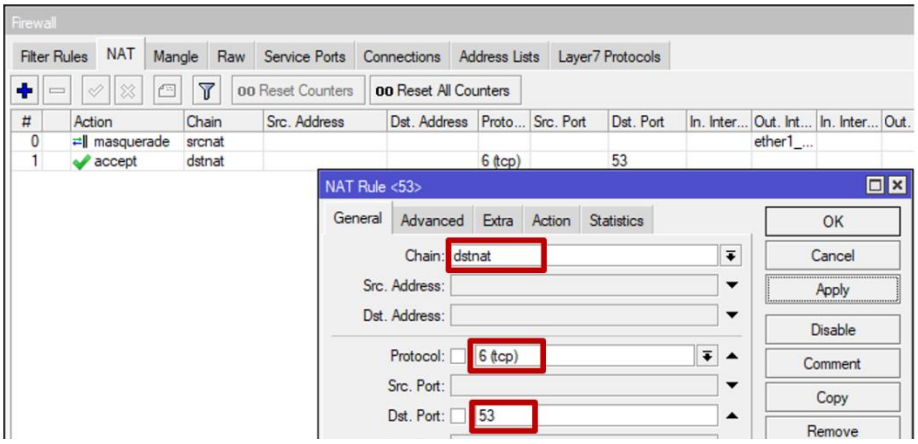



*Nota*. En esta ventana muestra las reglas de seguridad creadas.

A continuación, en la pestaña General en Chain colocar dstnat, después en el protocolo se debe seleccionar (tcp) que permiten la comunicación entre los ordenadores pertenecientes a una red y en Dst.Port asignando el puerto 53 que es utilizado para servicios DNS.

**Figura 52**

*Configuración General TCP*

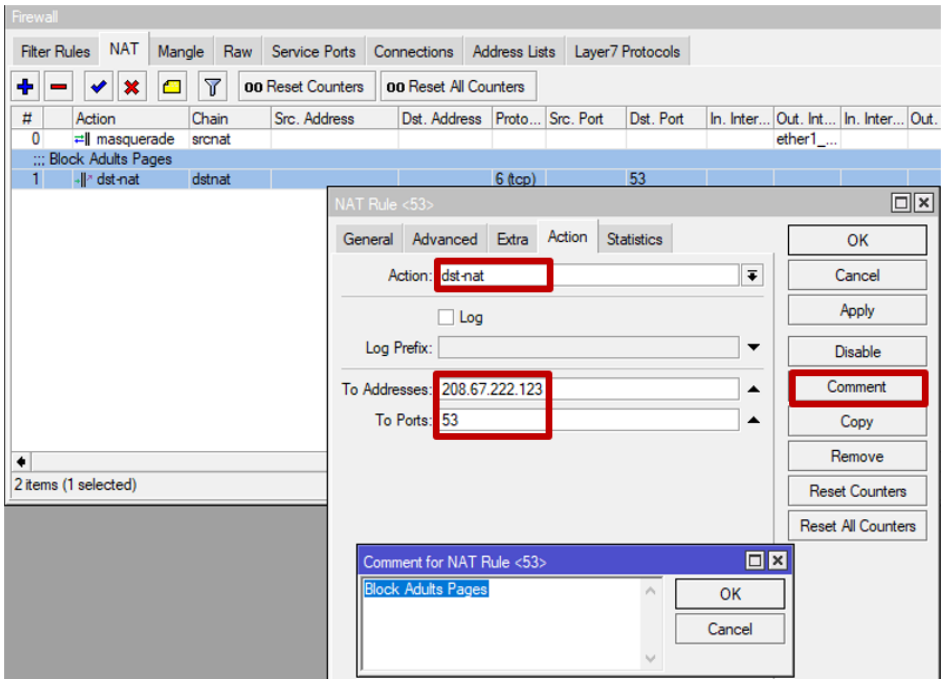



*Nota*. Esta ventana se utiliza para la configuración TCP.

Posteriormente en Action se colocará dns-nat en la ventana seleccionada, luego de eso se desplegará dos opciones para lo cual en Dirección se debe colocar el DNS Family Shield en el puerto 53. En cada regla se puede colocar un comentario para diferenciar de las demás reglas.

**Figura 53**

*Configuración de acción TCP*

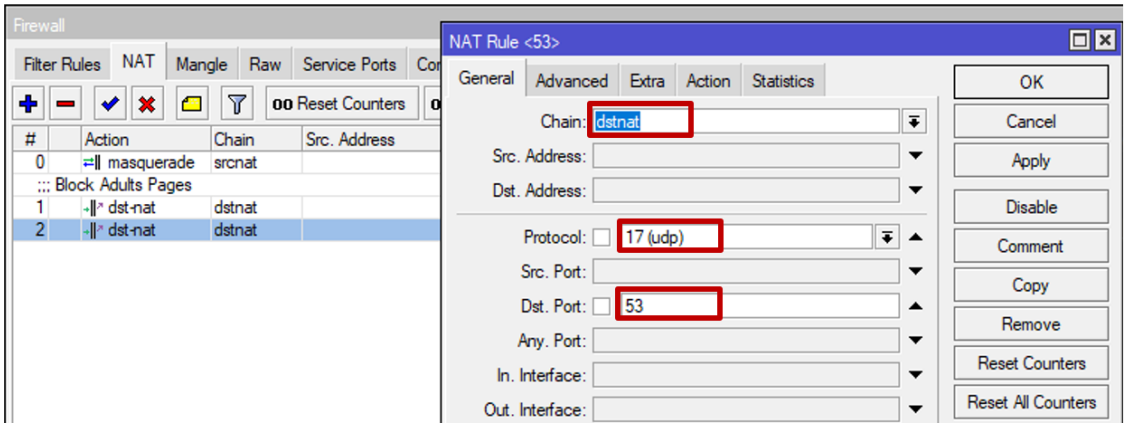



*Nota*. En la ventana se puede ver el Firewall activado en el protocolo TCP.

A continuación, en la pestaña General Chain seleccionar dstnat, en este protocolo se utiliza (udp) que sirve para realizar consultas DNS ahora en Dst. Port colocar el puerto 53 de servicios DNS. Después en Advanced se deberá colocar el Address List de la red LAN del Laboratorio, luego en Action colocar dst-nat y en dirección asignar 208.67.222.123 Family Shield en el puerto 53.

**Figura 54**

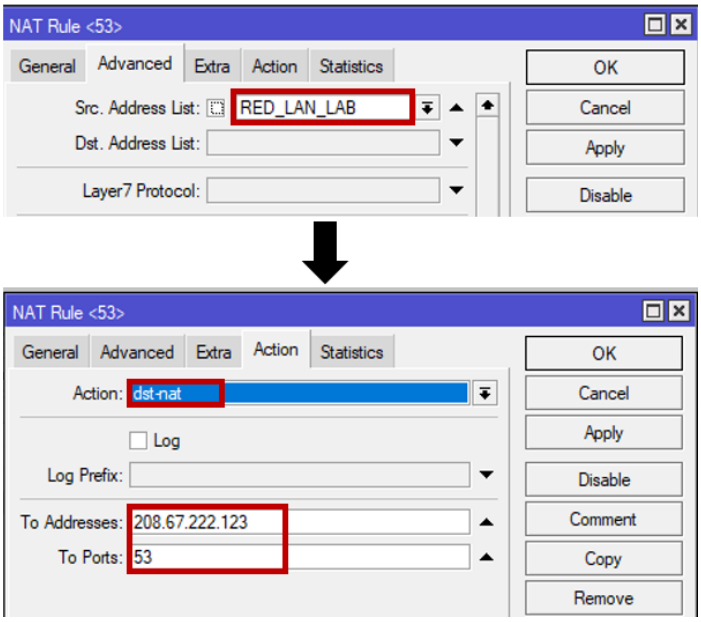
*Configuración General UDP*




*Nota*. Esta ventana se utiliza para la configuración UDP.

**Figura 55**

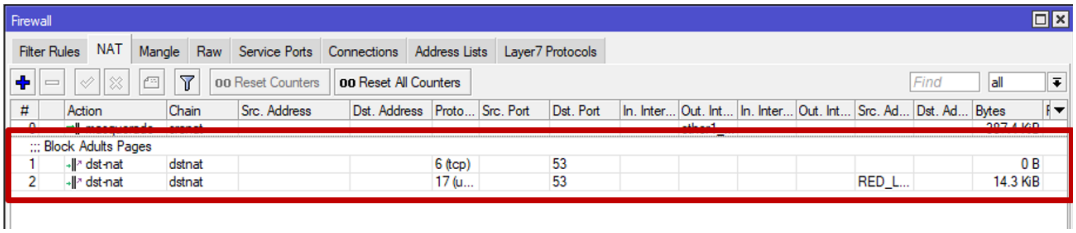
*Selección de Red y DNS Family Shield*




*Nota*. Se puede realizar una copia de la configuración de TCP y modificar el protocolo a UDP y seleccionar la Red LAN.

**Figura 56**

*Regla de bloqueo en TCP y UDP mediante DNS activada*



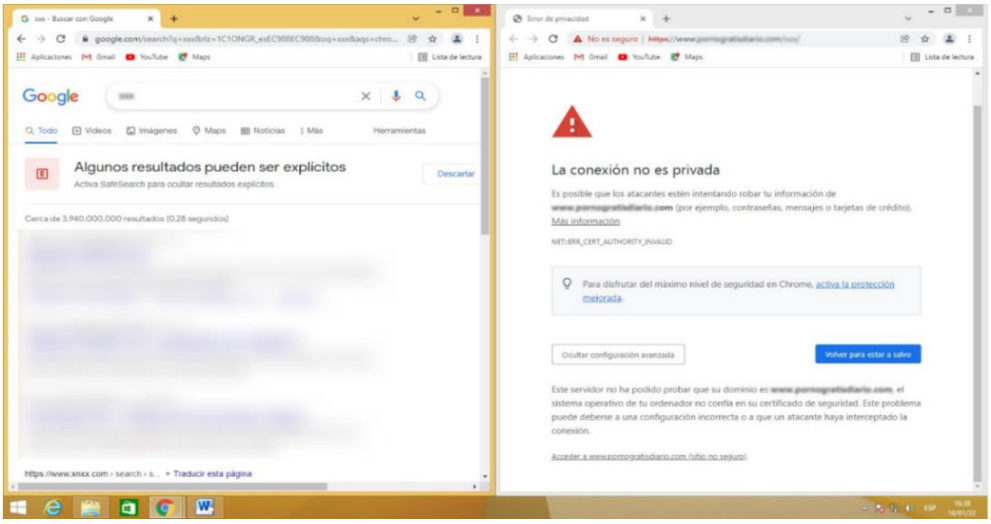

*Nota*. Con el comentario aplicado anteriormente, se puede ir separando fácilmente los diferentes tipos de configuraciones.

### *3.3.17 Ejecución Family Shield*

Ingresar a su navegador preferido, buscar un sitio que no sea familiar y al tratar de acceder a cualquier página web inmediatamente se restringe el acceso, también si se opta entrar con una configuración avanzada al sitio no seguro, nos redirige a la misma ventana de manera que está bloqueada por DNS.

**Figura 57**

*DNS Bloqueada*



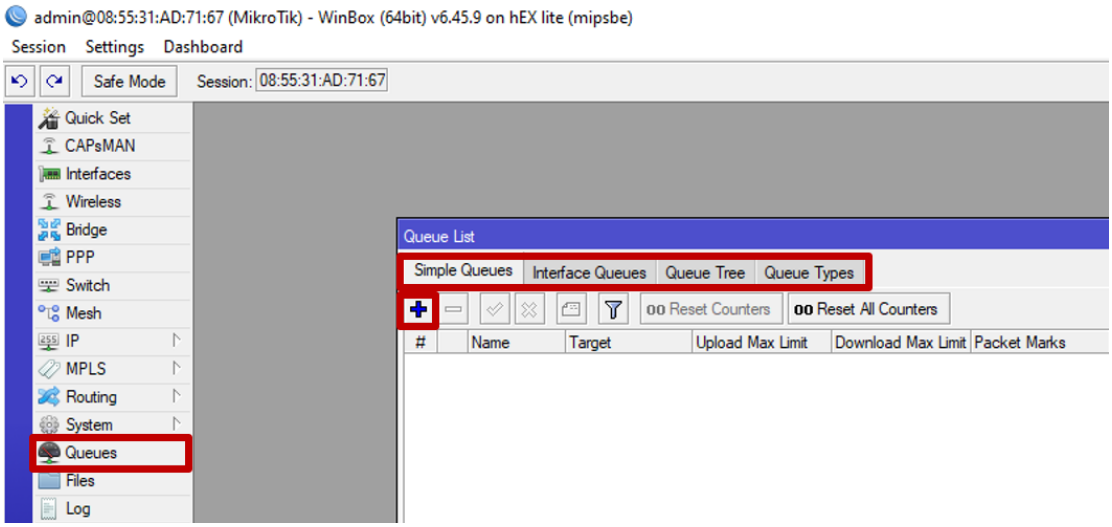

*Nota*. En estas ventanas muestra que al tratar de acceder a un sitio no adecuado el acceso no es permitido.

### *3.3.18 Limitar Ancho de Banda*

Para la configuración del ancho de banda del Laboratorio de computación se utiliza la opción de Simple Queues que nos ofrece MikroTik, para ello en el menú izquierdo dentro de Queues se creará una regla de prioridad por IP o a su vez por Target.

**Figura 58**

*Interfaz Queues*

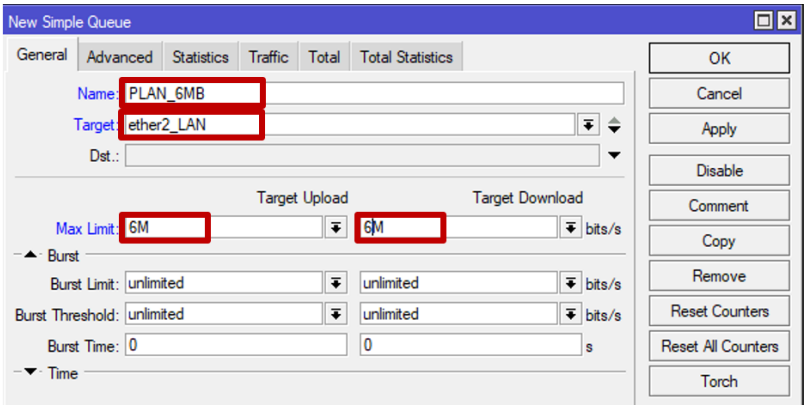



*Nota*. En esta ventana se puede limitar el ancho de banda mediante Interfaces, Queue Tree y configurar el tipo de Queue.

Posteriormente en la ventana Simple Queue en la opción General se realizará toda la configuración para eso en Name se coloca el nombre del plan y la cantidad de MB que se le asignará al puerto ether2_LAN. En la configuración de límite máximo tanto para descarga y subida de información se colocará 6MB de 9MB de la cantidad total del servicio de Internet.

**Figura 59**

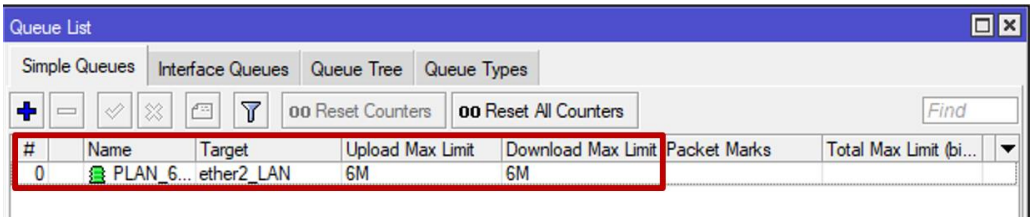
*Distribución 6MB para el Laboratorio de computación*




*Nota*. Ya que el ether1 tiene configurado la red LAN facilita controlar el ancho de banda de la red.

**Figura 60**

*Plan de 6MB activado*




*Nota*. La asignación de MB se realizó de acuerdo al número de computadoras.

### *3.3.19 Test de Velocidad LAN*

Para verificar el ancho de banda que tiene cada computadora del laboratorio se accede a un navegador y entrar al sitio https://fast.com/es/# las computadoras no llegaran a los 6MB configurados ya que es el Límite máximo que puede llegar la velocidad a internet, de tal manera que tiene un rango de velocidad entre 4Mbps a 5Mbps.

**Figura 61**

*Prueba de velocidad Internet*


*Nota*. En esta imagen se puede verificar que la PC02, PC04, PC06, PC08 y PC09 cuentan con una velocidad de internet no menor a los 4Mbps.

**Figura 62**

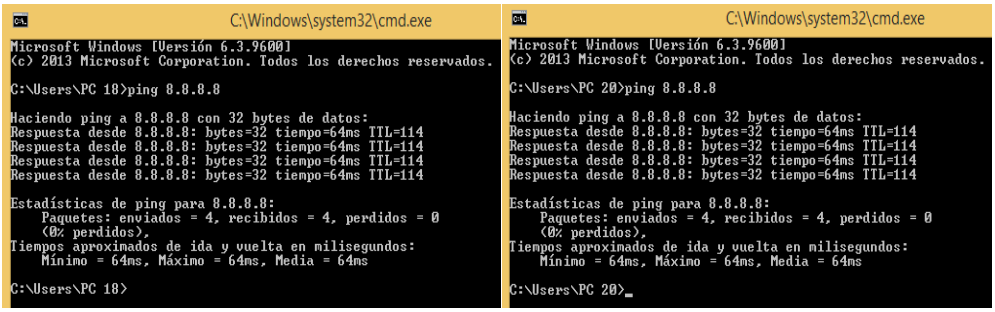
*Prueba de velocidad Internet*


*Nota*. En esta imagen se puede verificar que la PC11, PC14, PC17, PC18 y PC20 cuentan con una velocidad de internet no menor a los 5Mbps

A continuación, el resultado que muestra los pings en cada computadora indica que se enviaron cuatro paquetes de prueba de 32 bytes desde el host 8.8.8.8 y se devolvieron a este en un tiempo de 64 ms y TTL es el tiempo de vida, que indica la cantidad de saltos que le faltan al paquete ping antes de que se descarte.

**Figura 63**

*Verificación de Latencia mediante ping*




*Nota*. Como se puede observar en las imágenes se ha enviado 4 paquetes, se ha recibido 4 y se ha perdido 0.

## 3.4 Implementación Hotspot

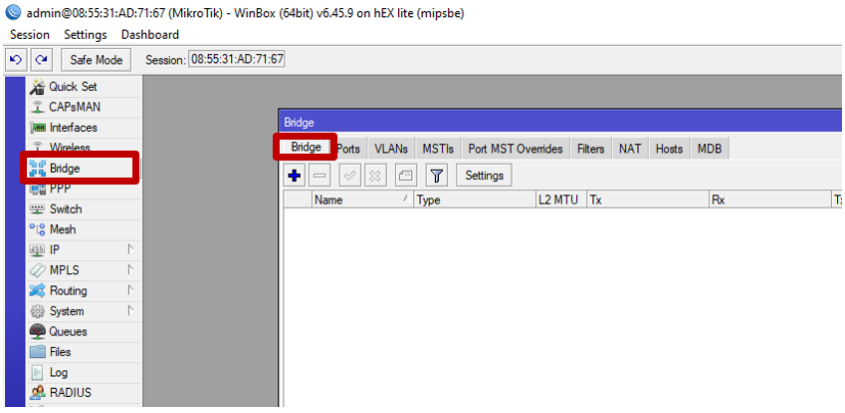
### *3.4.1 Configuración Bridge Router RB750r2*

Un bridge conecta segmentos de red formando una sola subred de esta manera las interfaces disponibles que tiene el Router son: ether3, ether4 y ether5 que serán utilizados para que los Access Point trabajen en la misma red.

En WinBox en la barra lateral seleccionar Bridge y crear una regla en el símbolo más como muestra en la **Figura 64 y 65.**

**Figura 64**

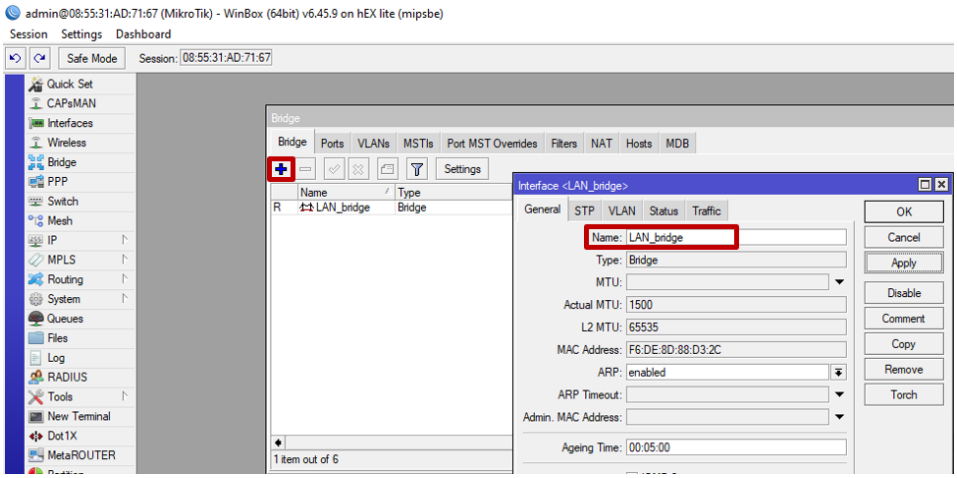
Interfaz Bridge o Puente de Red




*Nota*. En esta ventana se crea la regla la cual se usará para la unión de interfaces ethernet.

**Figura 65**

*Configuración Bridge*

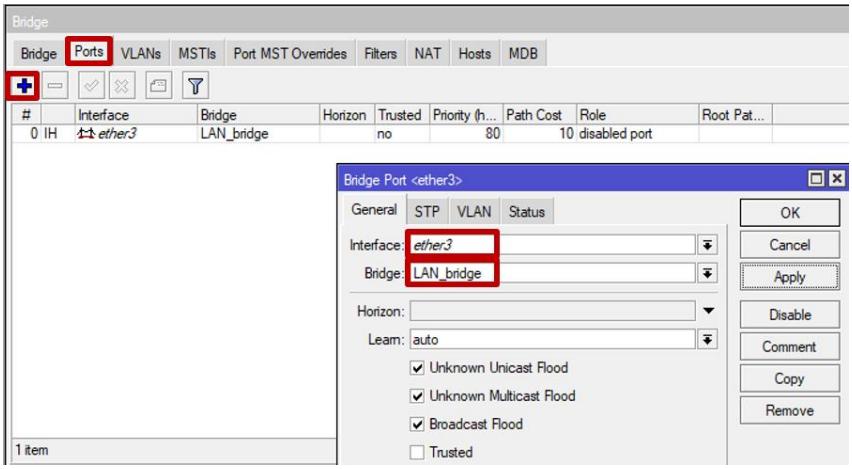



*Nota*. En la ventana se debe colocar el nombre del bridge de la red LAN del Hotspot.

Posteriormente, en la pestaña Ports cada interfaz ether3, ether4 y ether5 se le asignara la regla LAN_Bridge que fue creada anteriormente de esta manera las interfaces trabajaran en la misma red, una vez configurado el Bridge las demás opciones se las deja por defecto y se aplica los cambios para guardar la configuración.

**Figura 66**

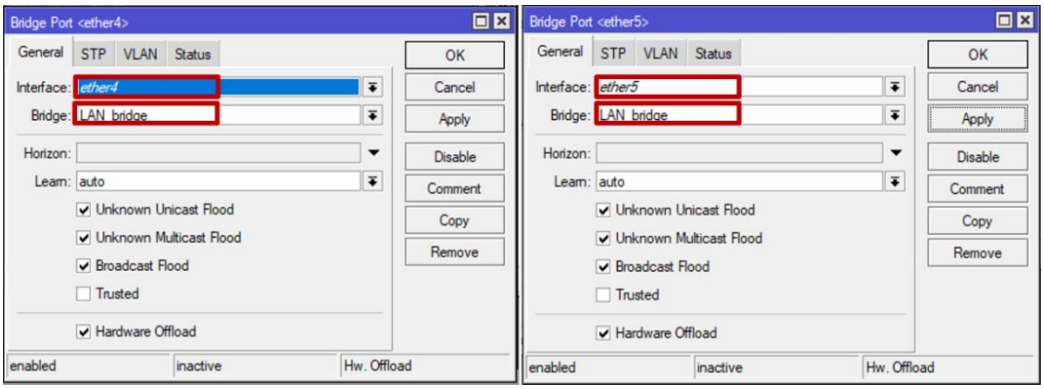
*Asignación de puertos al Bridge*




*Nota*. Esta ventana muestra que ether3 está en la LAN_bridge.

**Figura 67**

*Asignación de puertos al Bridge*

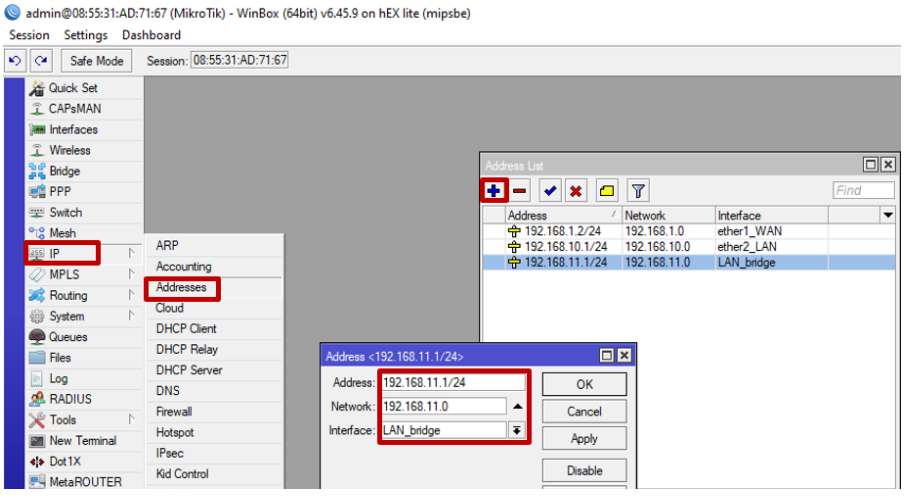



*Nota*. Aquí se puede observar que la ether4 y ether5 está configurada en LAN_bridge.

Posteriormente al Bridge se le asignará una dirección de red, en IP seleccionar Addresses y crear una nueva Red 192.168.11.0 con dirección IP 192.168.11.1/24 y en la opción interface se deberá colocar LAN_bridge en la cual están conectadas las tres interfaces anteriormente configuradas.

**Figura 68**

*Asignación de IP al Bridge*




*Nota*. En la ventana Address List se puede observar que LAN_bridge ya contiene una dirección IP.

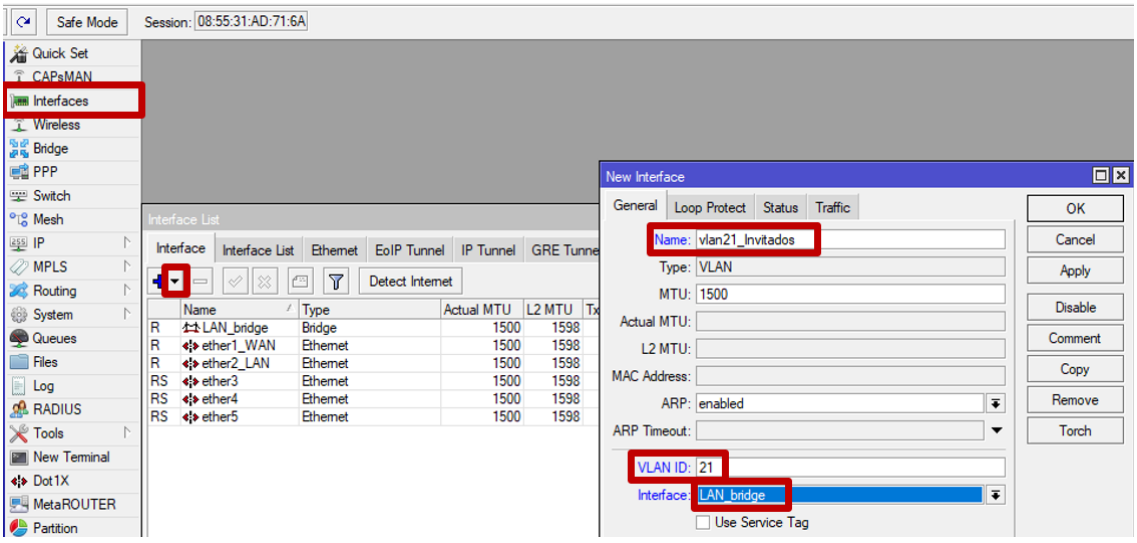
### *3.4.2 Configuración de Vlan*

Para esta configuración la red física que se creó en el Bridge se le aplicará el método de creación de redes lógicas, la primera Vlan para invitados que contiene la VLAN ID 21 que identifica la red virtual del dispositivo. La segunda Vlan pertenecerá a los docentes con una VLAN ID 22 y a la interfaz que debe pertenecer será la LAN_bridge.

A continuación, para acceder a la configuración de VLANs dar clic en Interfaces, una vez abierta la ventana Interface List se debe seleccionar la pequeña flecha que tiene el símbolo más, donde se desplazará una lista de opciones la cual se escogerá VLAN.

**Figura 69**

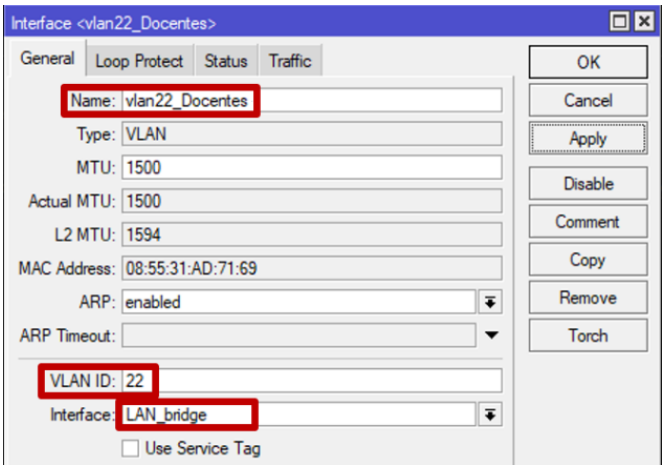
*Creación VLAN Invitados*




*Nota*. La VLAN invitados se encuentra configurado en la interfaz del bridge.

**Figura 70**

*Creación VLAN Docentes*

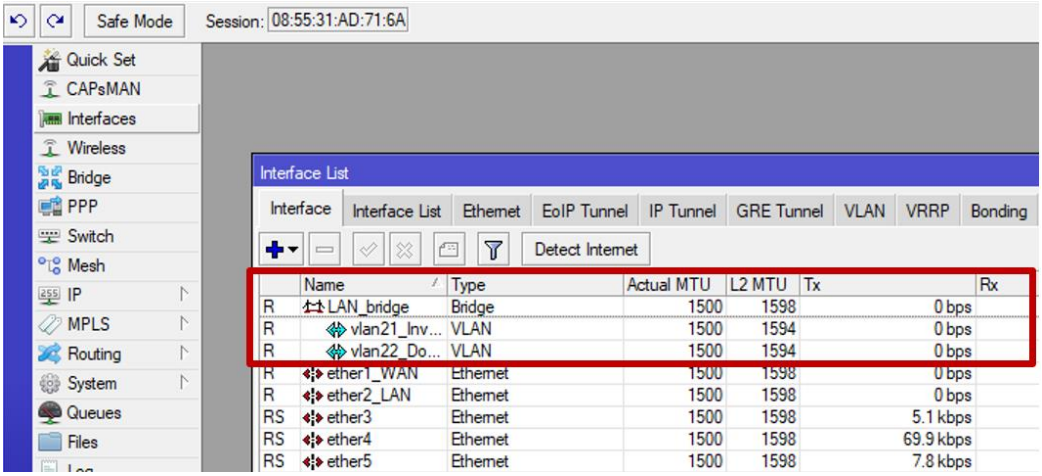



*Nota*. La VLAN Docentes se encuentra configurado en la interfaz del bridge.

Seguidamente para verificar la creación de las VLAN en la ventana de Interface List dirigirse a LAN_bridge y comprobar que efectivamente existan dos redes virtuales que poseen su identificador, además de estar en el mismo segmento de red al cual pertenece el Hotspot.

**Figura 71**

*Verificación VLAN en Bridge*



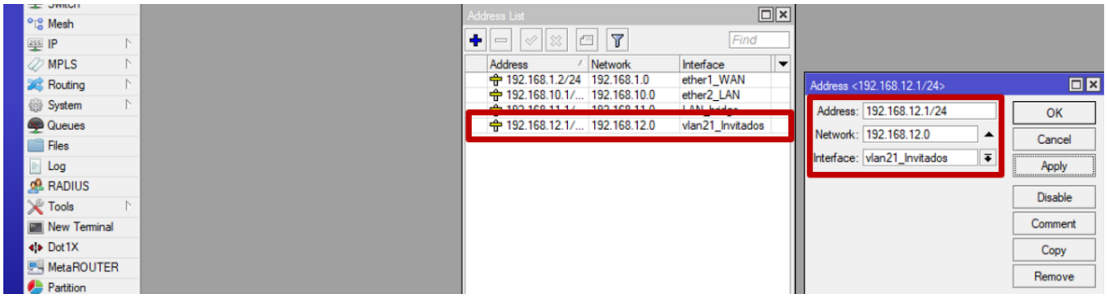

*Nota*. En la pestaña de interface se puede acceder y observar las VLAN creadas.

### *3.4.3 Asignación direcciones IP a VLANs*

Para la configuración de una dirección IP para la VLAN Invitados se usará la IP inicial 192.168.12.1/24 con dirección de red 192.168.12.0 y en la interfaz se selecciona vlan21_invitados, aplicar los cambios y ver que se haya creado una nueva dirección.

**Figura 72**

*Asignación IP VLAN Invitados*

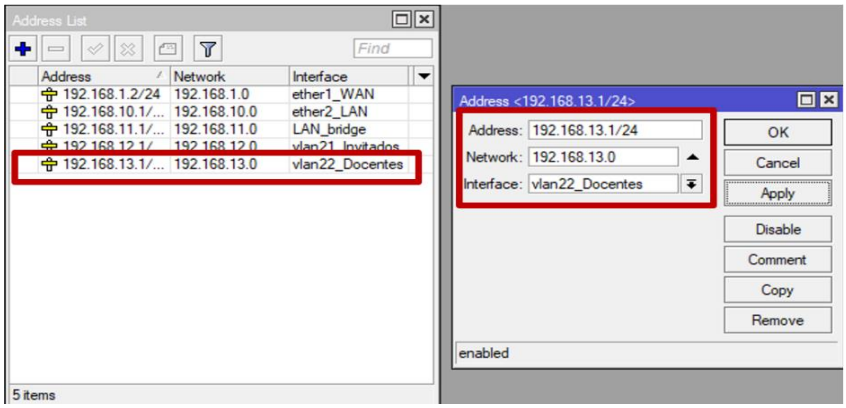



*Nota*. En la ventana Address List se ha creado una nueva IP para la Vlan 21.

A continuación, la VLAN Invitados deberá ser configurada con la IP inicial 192.168.13.1/24 con dirección de red 192.168.13.0 y en la interfaz seleccionar vlan22_Docentes, aplicar los cambios y verificar que se ha creado una nueva dirección.

**Figura 73**

*Asignación IP VLAN Docentes*



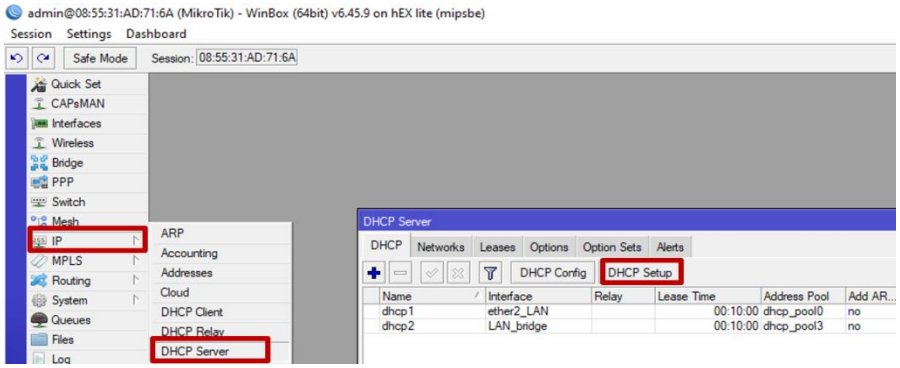

*Nota*. Aquí se muestra la dirección, red e interfaz donde fue creada la Vlan22.

### *3.4.4 Configuración DHCP a VLANs*

Para la configuración DHCP dirigirse a IP luego seleccionar DHCP Server y en la ventana que aparecerá presionar en DHCP Setup. En la nueva ventana seleccionar vlan21_invitados dar clic en Next y se mostrará la dirección IP de la Vlan configurada, en la siguiente ventana muestra la puerta de enlace de la Vlan que luego se asignará el rango de direcciones disponibles.

**Figura 74**

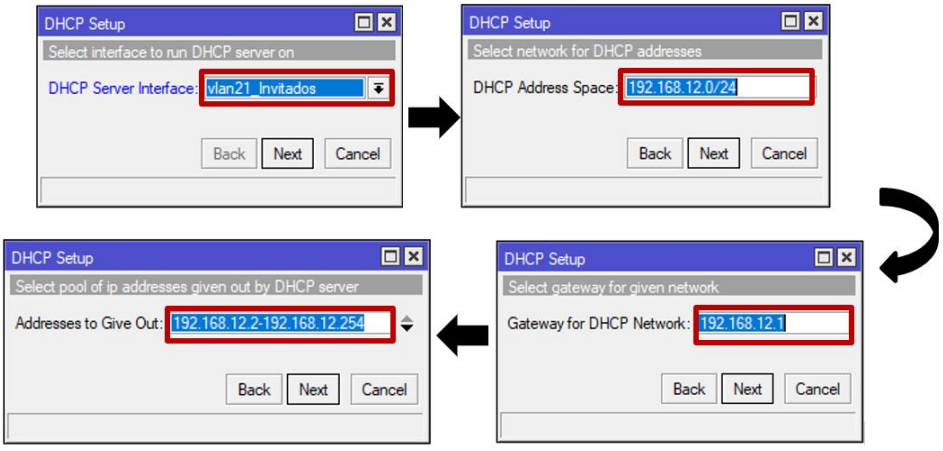
*DHCP Server*




*Nota*. Proceso de configuración Dynamic Host Configuration Protocol.

**Figura 75**

*Configuración DHCP VLAN Invitados*

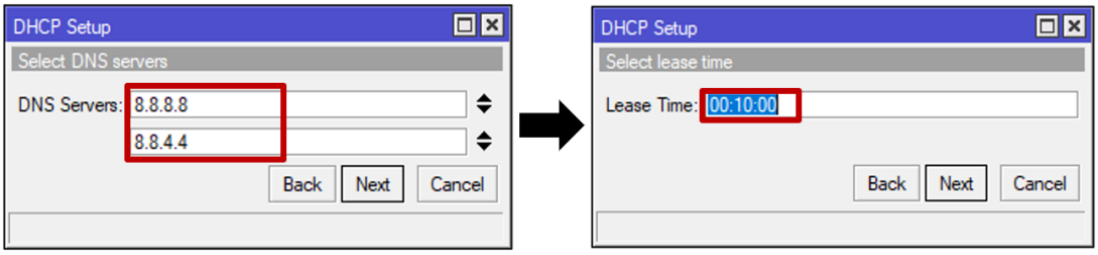



*Nota*. Proceso de configuración de la Vlan invitados mediante DHCP Server.

Posteriormente en el proceso de configuración de DHCP Setup se debe colocar los DNS correspondientes, en este caso se colocará los de Google. En la siguiente ventana muestra el tiempo de alojamiento normalmente se lo deja por defecto, finalmente la ventana muestra un mensaje diciendo la instalación se ha realizado con éxito. La lista de DHCP Server ya se encuentra activa para la vlan21_invitados.

**Figura 76**

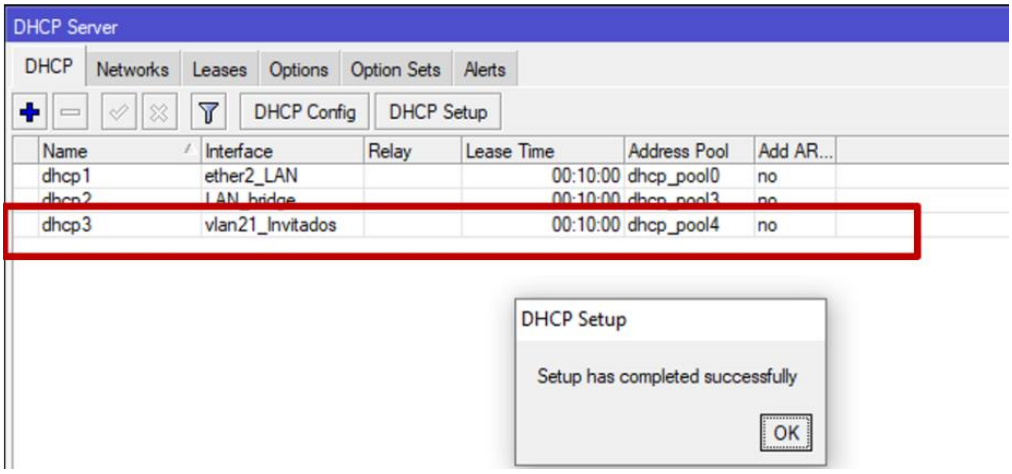
*DNS Vlan Invitados*




*Nota*. En esta ventana colocar también el DNS alternativo de Google.

**Figura 77**

*Verificación DHCP Invitados Activa*

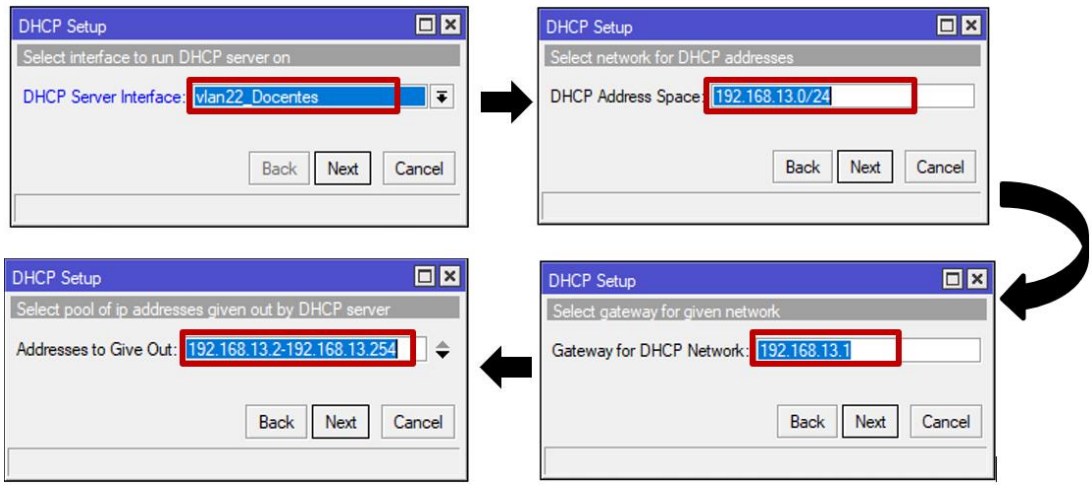



*Nota*. Esta ventana muestra que la configuración DHCP se ha realizado con éxito.

A continuación, la configuración de la Vlan Docentes se realizará de la misma forma. Se debe seleccionar vlan22_Docentes dar clic en Next y se mostrará la dirección IP de la Vlan configurada en Address, en la siguiente ventana muestra la puerta de enlace de la Vlan luego se asignará el rango de direcciones disponibles.

**Figura 78**

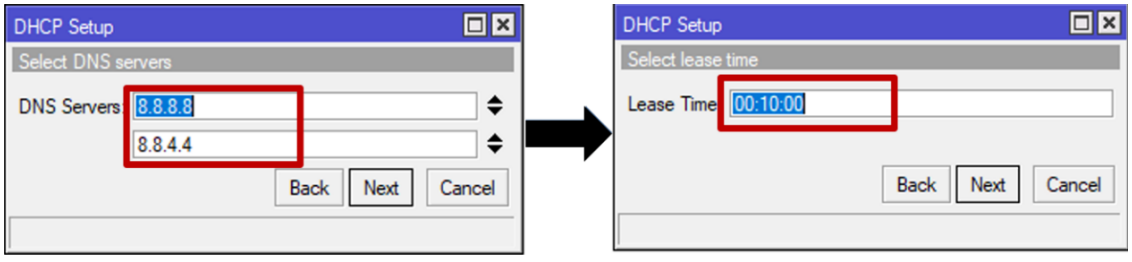
*Configuración DHCP VLAN Docentes*




*Nota*. Proceso de configuración de la Vlan Docentes mediante DHCP Server.

**Figura 79**

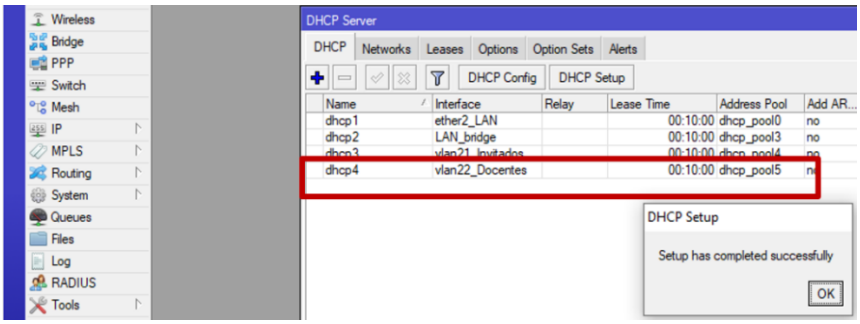
*DNS Vlan Docentes*




*Nota*. Aquí se coloca los DNS de Google y el tiempo dejar por defecto.

**Figura 80**

*Verificación DHCP Docentes Activa*



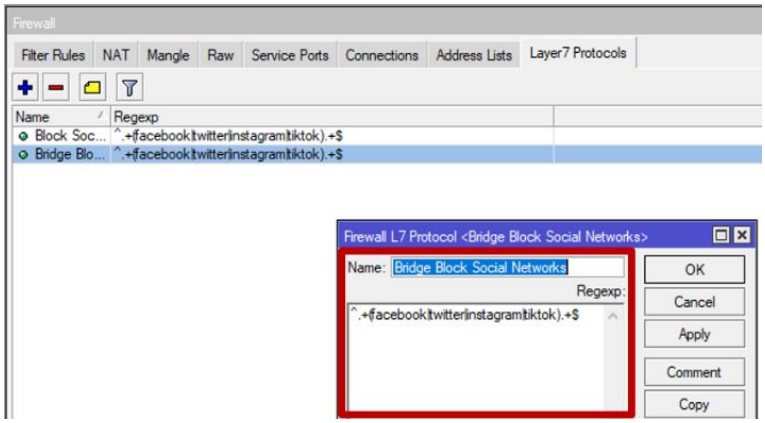

*Nota*: Esta ventana muestra que la configuración DHCP se ha realizado con éxito.

### *3.4.5 Bloqueo de Redes Sociales y Family Friendly VLANs*

Para la configuración dirigirse a IP dar clic en Firewall, en la pestaña Layer7 Protocols, crear una nueva regla que pertenecerá a Bridge donde están las Vlan. En el recuadro colocar la línea de código ^. +(facebook|twitter|Instagram|tiktok). +$ y aplicar cambios.

**Figura 81**

*Layer7 Protocols*

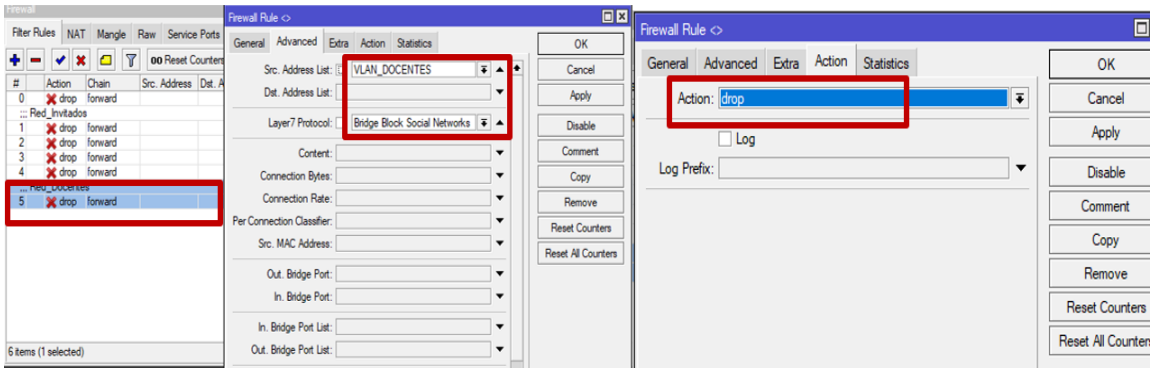



*Nota*. Se debe crear una nueva regla para diferenciar de la regla que pertenece a la red LAN.

Seguidamente en la pestaña Filter Rules crear una regla donde se seleccione la VLAN tanto para Invitados y Docentes, luego seleccionar la regla creada en Layer7 Protocols que pertenece al Bridge, en la opción Action seleccionar Drop que es descarte de paquetes.

**Figura 82**

*Bloqueo VLAN Docentes*

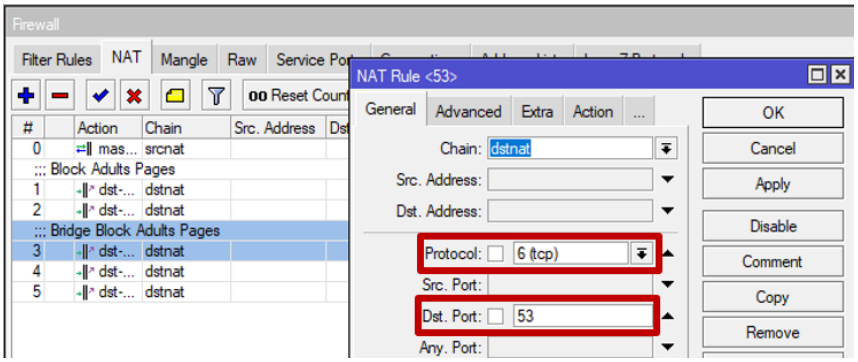



*Nota*. En la sección de Src. Address se puede denegar el acceso a la Vlan Invitados si fuese necesario.

A continuación, en la ventana de Firewall dar clic en NAT para crear una regla, en la pestaña General ir al apartado donde dice Chain, seleccionar dst-nat, en protocolo aplicar TCP para el puerto de destino asignar el puerto 53. En la pestaña de Action colocar dst-nat ahora en la dirección colocar el DNS Family Friendly y en el puerto colocar 53 que es utilizado para los servicios DNS.

**Figura 83**

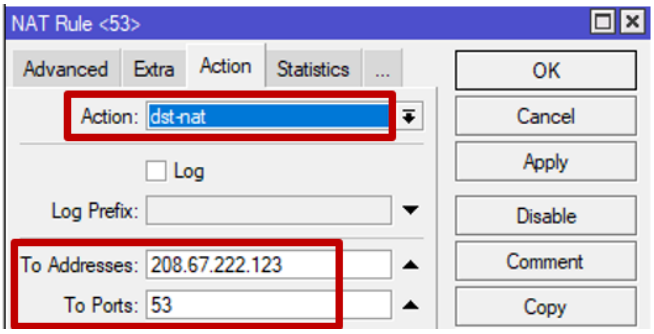
*Configuración TCP*




*Nota*. En las ventanas muestra el tipo de protocolo a utilizar además el puerto Dst.

**Figura 84**

*Configuración DNS Family Friendly*

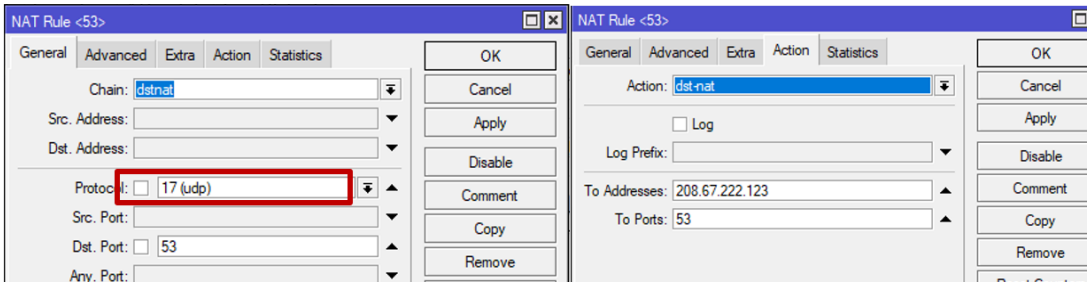



*Nota*. La ventana indica el DNS de bloqueo con su dirección Ip también el puerto del protocolo.

Posteriormente se utilizará UDP que es un protocolo sin conexión que se ejecuta sobre IP, se aplicará en el puerto 53, además en la pestaña Action colocar los DNS Family Friendly en el puerto 53. En configuración avanzada en Src. Address, seleccionar el ID de las Vlan Docentes e Invitados. Finalmente se crearán reglas NAT de Bloqueo con DNS.

**Figura 85**

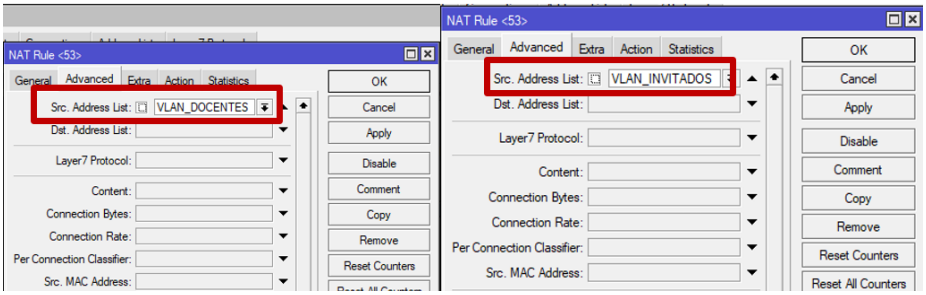
*Configuración UDP y DNS Family Friendly*




*Nota*. Esta ventana muestra el protocolo utilizado además la acción de la NAT.

**Figura 86**

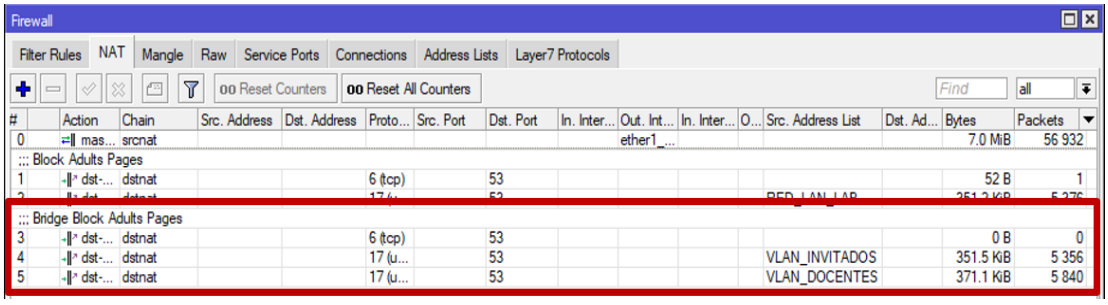
*Restricción DNS a VLANs*




*Nota*. Es necesario seleccionar únicamente las direcciones que se desea restringir el acceso ya que otras direcciones se utilizan con otros propósitos.

**Figura 87**

*Acceso Family Friendly activado*




*Nota*. Esta ventana indica que la Vlan Invitados como la de Docentes tiene acceso restringido a sitios web no apropiados.

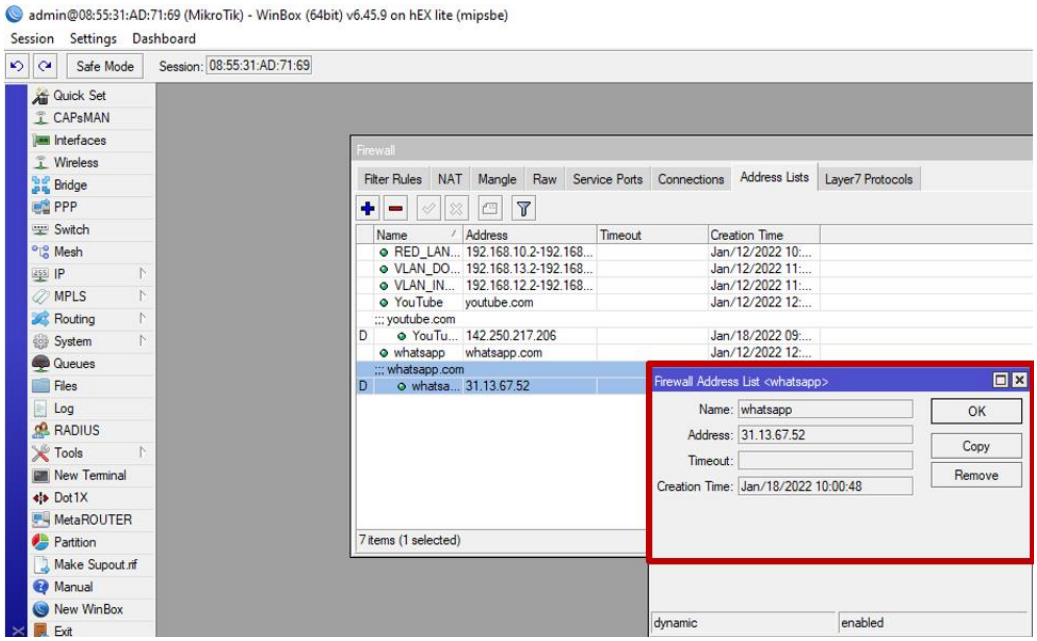
### *3.4.6 Bloquear todo y dejar Dominios Activados*

Para la configuración en IP se debe seleccionar Firewall una vez dentro de la ventana en la pestaña Address List se crearán dos reglas con los dominios de WhatsApp y YouTube para ello se debe dar clic en el símbolo más.

En el nombre colocar solo el nombre o también se puede colocar el ".com", automáticamente se colocará la dirección IP de los dominios que se deseen que estén activos.

**Figura 88**

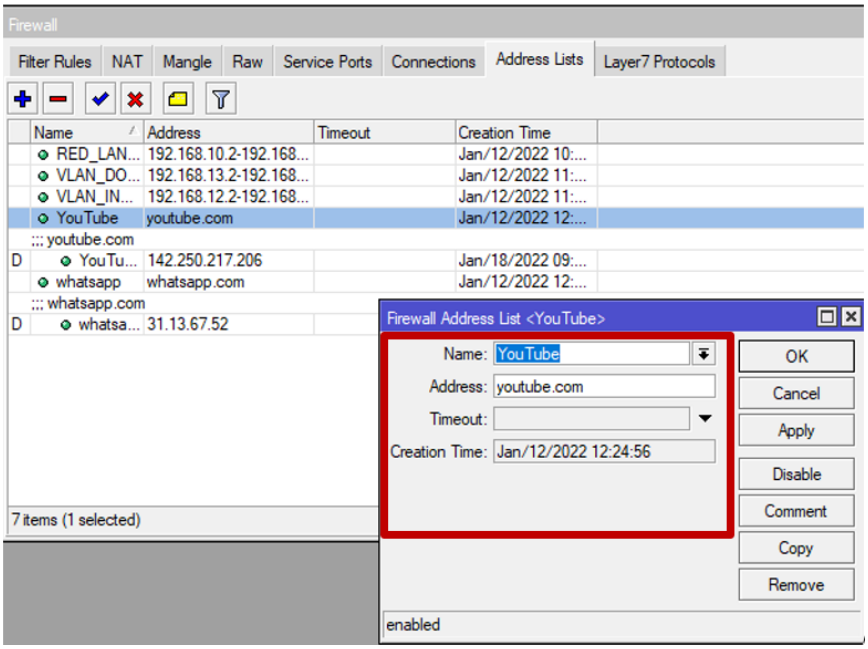
*Configuración Domino WhatsApp*




*Nota*. Como muestra el pequeño recuadro con solo poner el nombre ya se genera la dirección del domino.

**Figura 89**

*Configuración Domino YouTube*



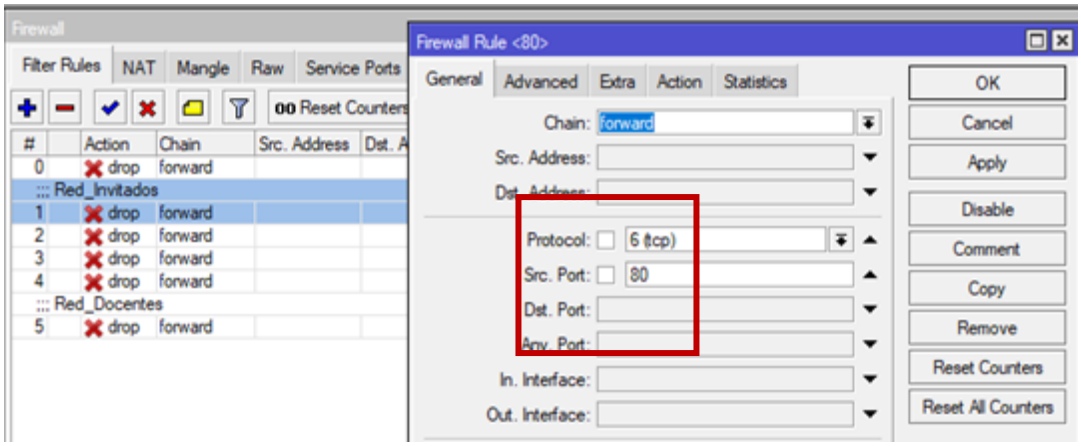

*Nota*. Como indica en recuadro también se puede poner el dominio con ".com" de igual manera funciona.

A continuación, se creará una nueva regla donde en Chain se debe colocar Forward, en protocolo se coloca TCP en el puerto 80, después en la ventana Advanced poner el domino configurado y en Dst. Address List seleccionar la VLAN que negara el acceso ahora en la pestaña Action poner Drop.

En la misma configuración dar clic en Copy y cambiar el puerto a 443 de esta manera se crearán dos reglas que filtrarán el tráfico web.

**Figura 90**

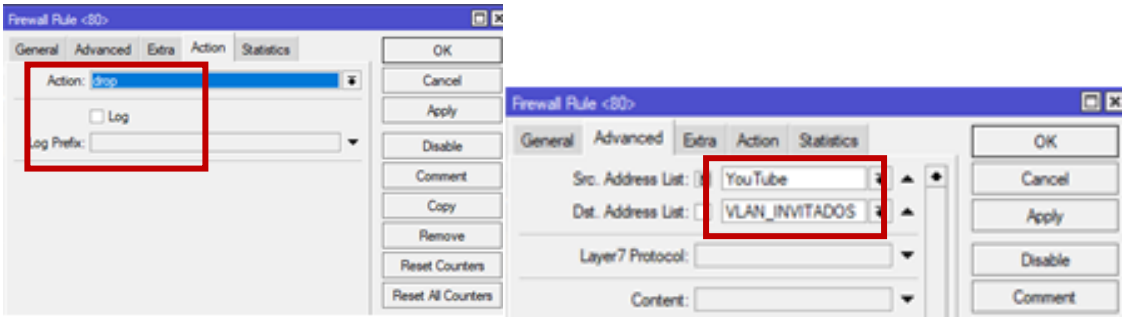
*Puerto 80 TCP*




*Nota*. La ventana indica la configuración TCP para la red invitados.

**Figura 91**

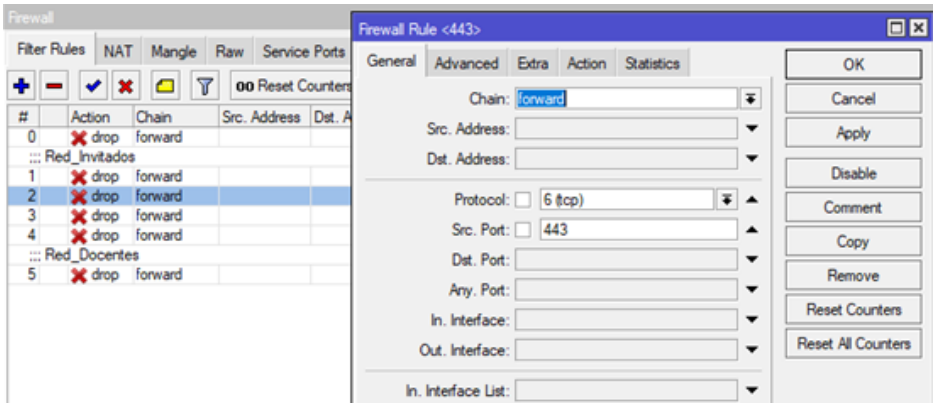
*Configuración Firewall Rule*




*Nota*. En esta venta se puede observar la configuración para el tráfico web del dominio de YouTube.

**Figura 92**

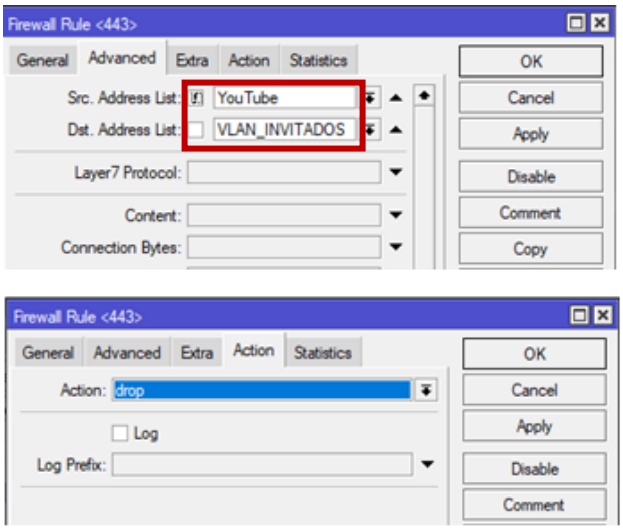
*Puerto 443 TCP*




*Nota*. La configuración indica el protocolo tcp en la segunda regla de la red invitados.

**Figura 93**

*Configuración Firewall Rule*

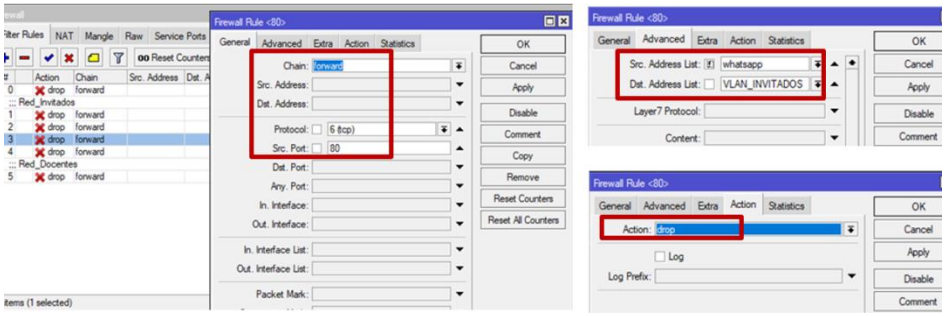



*Nota*. La regla funciona solo para la VLAN Invitados.

Posteriormente se realiza la configuración del dominio de WhatsApp para esto repetir los pasos anteriores, únicamente variar el domino ya que el Hotspot para Invitados solo posee acceso Limitado a dos sitios Web. De esta manera en la figura 96 muestra que las reglas para los dos dominios están activas.

**Figura 94**

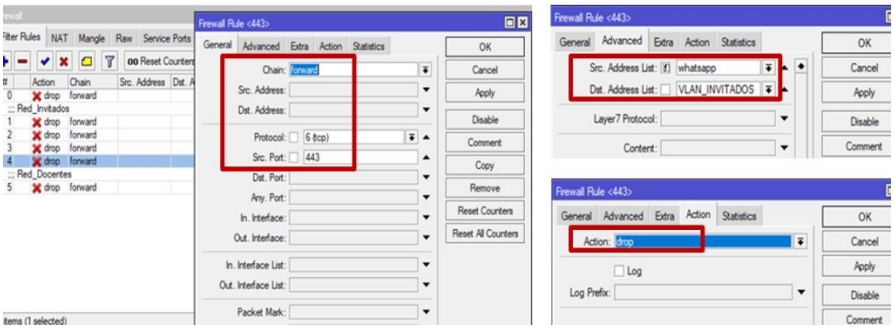
*Regla para WhatsApp Port 80*




*Nota*. La figura muestra el proceso para la configuración de acceso a WhatsApp.

**Figura 95**

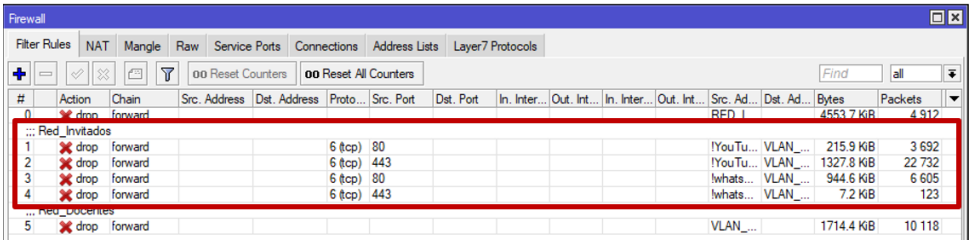
*Regla para WhatsApp Port 443*




*Nota*. La figura muestra que se deben aplicar configuraciones para dos puertos del protocolo TCP.

**Figura 96**

*Acceso solo a tráfico específico*



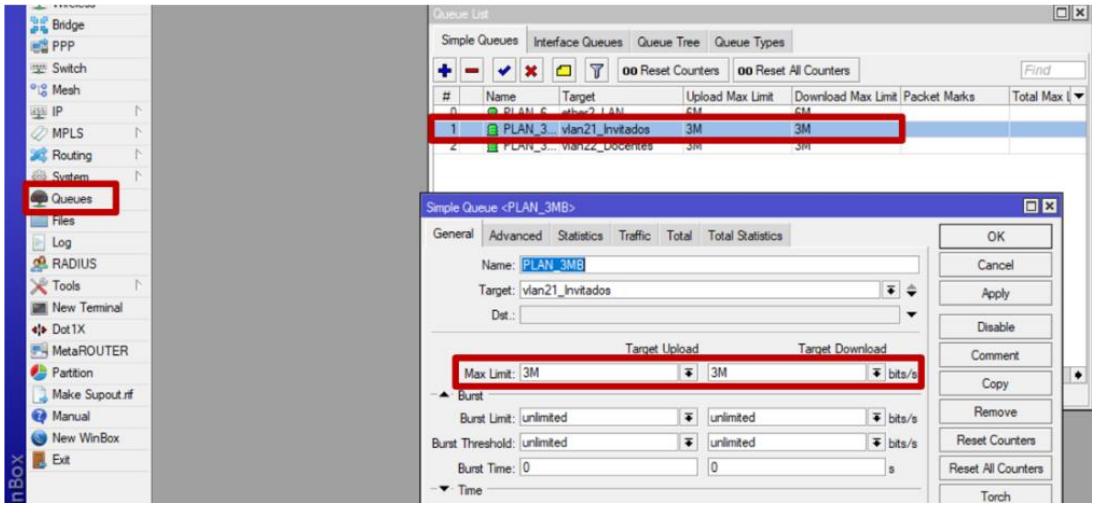

*Nota*. Esta ventana muestra que la Vlan Invitados solo tendrá acceso a YouTube y WhatsApp.

### *3.4.7 Limitar Ancho de Banda VLANs*

En la configuración para limitar el ancho de banda de internet seleccionar Queues, dar clic en el símbolo más y se abrirá un recuadro al que se colocará el nombre del plan. En la opción de Target seleccionar vlan21_Invitados después poner el límite máximo tanto para descarga como subida de datos.

**Figura 97**

*Configuración Vlan 21*

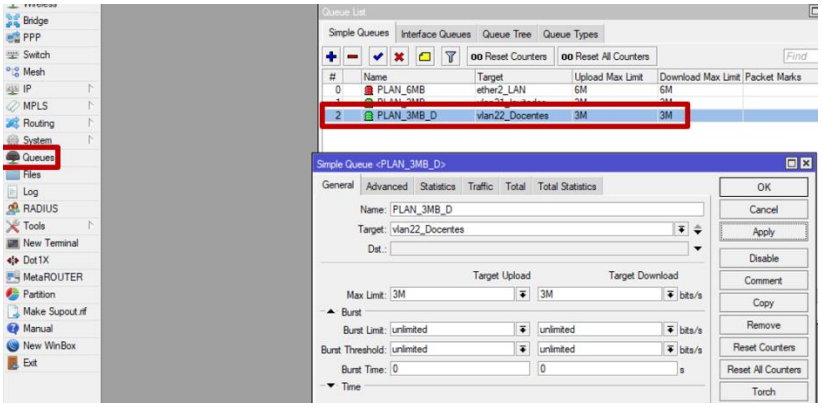



*Nota*. En esta ventana puede observar que en Simple Queues el segundo plan de Mbps este asignado a la Vlan Invitados.

Seguidamente para la configuración de la Vlan de Docentes presionar el símbolo más para crear una nueva regla, el nombre del plan será PLAN_3MB_D, en Target seleccionar la vlan22_Docentes que se creó en el Bridge y por último en límite máximo para descarga y subida de información se colocar 3Mbps.

**Figura 98**

*Configuración Vlan 22*




*Nota*. En esta ventana en Simple Queues List muestra el plan de 3Mbps aplicados en la Vlan Docentes.

### *3.4.8 UNIFI01 Primer Punto Estratégico*

Una vez ya listo el Laboratorio empieza la implementación de la red inalámbrica o Hotspot para esto se debe buscar puntos estratégicos donde puedan ir las Ap's. Una vez ya ubicados estos puntos se procedió a llevar cable UTP Cat5e desde el gabinete hasta el primer punto estratégico que en este caso es el edificio principal en el segundo piso (UNIFI01).

**Figura 99**

*Primer punto estratégico Edificio Principal*

*Nota*. El primer punto estratégico se encuentra en un lugar cerca de un campo semiabierto.

Posteriormente se debe llevar un cable de 30 metros desde el gabinete hacia el segundo piso. Al estar el cable en el exterior se deberá utilizar una manguera de electricidad para cubrir el cable, de igual manera se deberá adquirir grapas de interior del aula para que el cable no quede colgado.

**Figura 100**

*Transporte de cable hacia el primer punto estratégico UNIFI01*

*Nota*. Por seguridad del cable se utilizará una manguera de electricidad para evitar daños ya sea por animales o clima.

### *3.4.9 UNIFI02 Segundo Punto Estratégico*

Una vez ya identificado el segundo punto exacto se debe llevar 60 metros de cable UTP Cat5e hacia un aula cerca del punto estratégico para esto se debe por el techo cubierto de una manguera para más seguridad del cable, a lo que también se deberá reforzar con amarras para que este quede firme.

**Figura 101**

*Transporte de cable cerca del punto estratégico*

*Nota*. El segundo punto estratégico se encuentra a 80 metros desde el gabinete, pero un Adaptador POE solo puede dar alimentación a 40 metros distancia por lo que para llegar al punto se segmento en 2 partes.

Para llegar al punto estratégico se realizó una perforación en la pared del coliseo, donde 20 metros de cable fue pasado por una manguera desde el aula donde se encontraba el POE hasta el punto estratégico

**Figura 102**

*Transporte de cable desde Gabinete hacia punto estratégico*

*Nota*. En este punto la seguridad del cable es más esencial al estar por fuera del coliseo.

### *3.4.10 Ubicación de Jaulas de Protección para los Access Point*

Una vez ya pasado el cable a los dos puntos estratégicos se procede a ponchar el cable UTP, armar las antenas y a colocar las jaulas para que los Access Point tengan más protección al estar expuestos a los estudiantes.

**Figura 103**

*Implementación de Access Point y armado de jaulas*

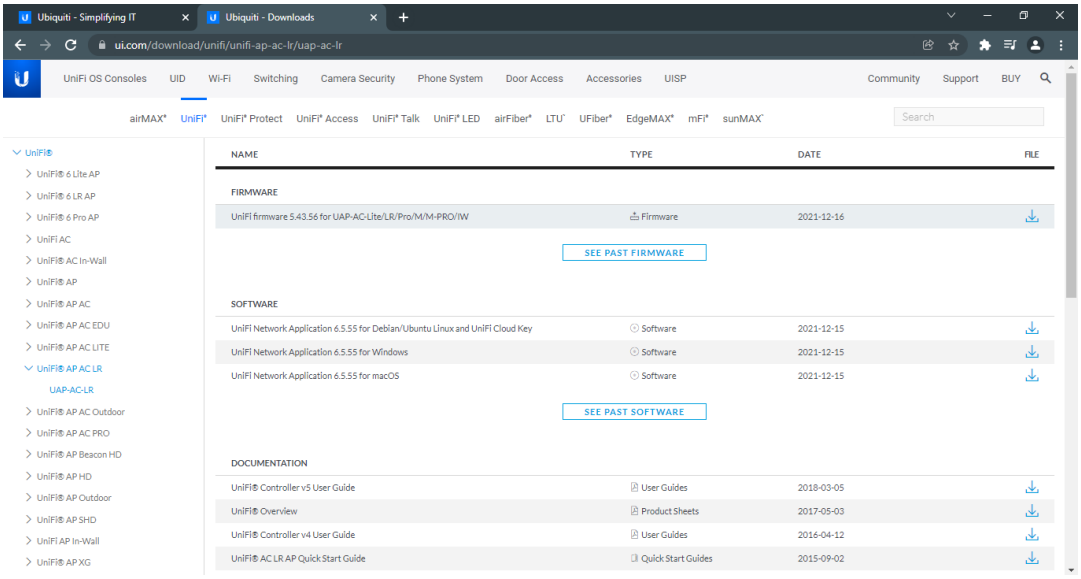
*Nota*. Las antenas fueron puestas en jaulas para tener mayor seguridad.

### *3.4.11 Instalación del Software UniFi*

Se necesita descargar el instalador del software el cual se lo puede encontrar en la página oficial de Ubiquiti https://www.ui.com/download/unifi/unifi-ap-ac-lr/uap-ac-lr en la parte izquierda se puede seleccionar los diferentes modelos de Access Point además cada uno cuenta con Firmware, Software y Documentación.

**Figura 104**

*Página de descarga UniFi*

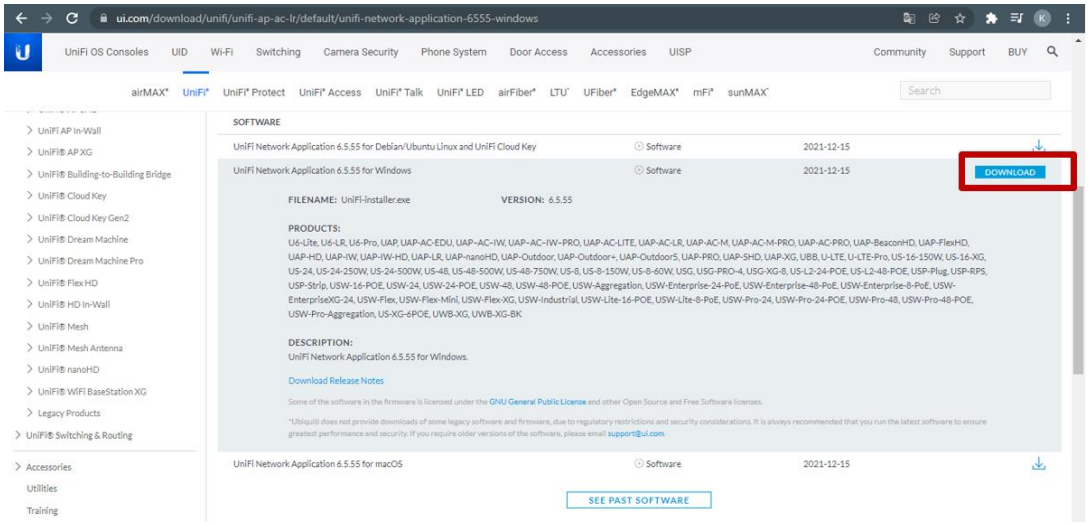



*Nota*. En la página de Ubiquiti existe el instalador para sistemas operativos libres, Windows y MacOS.

A continuación, al seleccionar el instalador para Windows se despliega información del software como es el nombre del archivo, la versión, los productos, cual software es compatible así mismo la descripción del mismo. Al iniciar la descarga se dirige a una venta donde se debe aceptar los términos y condiciones por parte de la página de Ubiquiti.

**Figura 105**

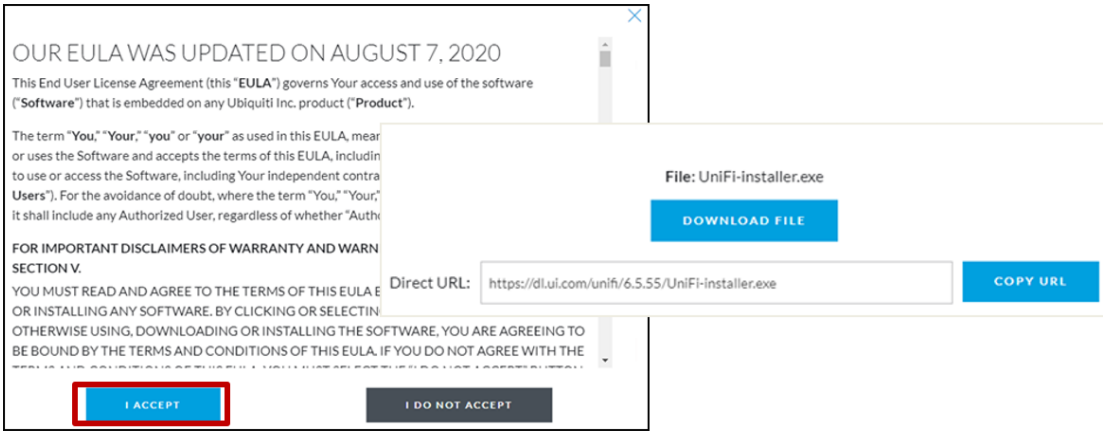
*UniFi Network Application 6.5.55 para Windows*




*Nota*. En la parte inferior de la ventana también se puede acceder a versiones anteriores del software.

**Figura 106**

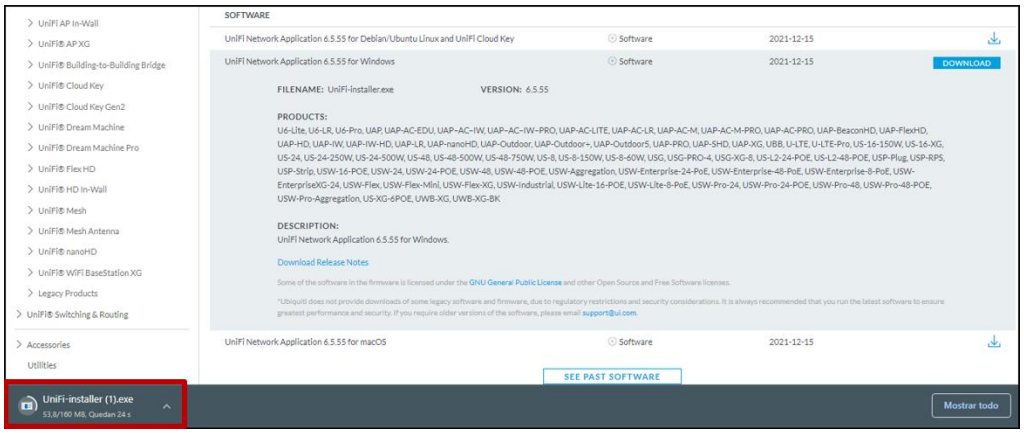
*Términos y Condiciones de Descarga*




*Nota*. Esta ventana muestra los términos y condiciones para la descarga, además que genera un link que se puede compartir.

**Figura 107**

*Descarga de UniFi v6.5.55*




*Nota*. El instalador pesa 160MB, se recomienda moverlo el archivo al escritorio para tener mejor control.

Seguidamente, se ejecutará el instalador como administrador de esta manera tendrá todos los permisos del equipo. Una ventana se abrirá en donde muestra las recomendaciones de instalación, luego de eso presionar en Install para que inicie el proceso de instalación.

**Figura 108**

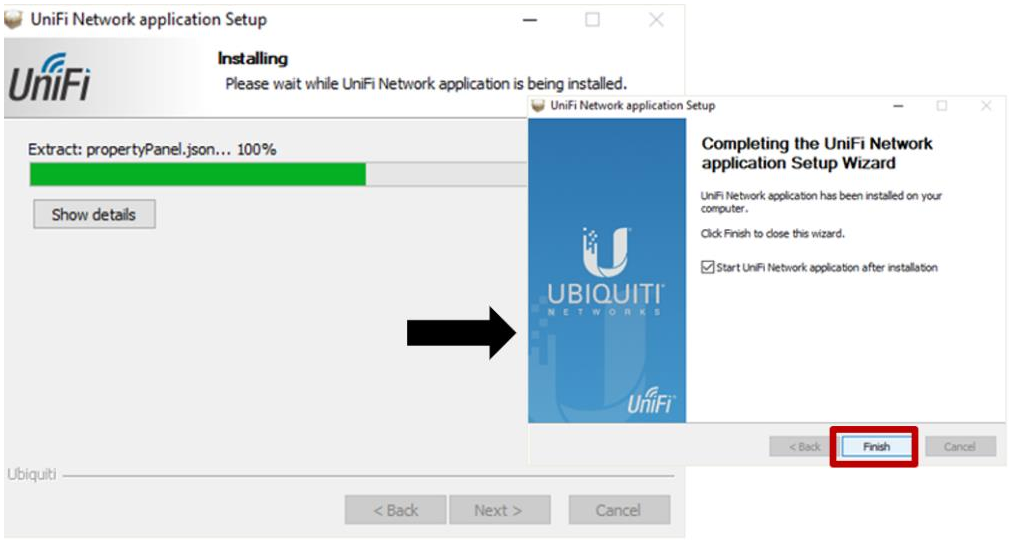
*Interfaz de bienvenida a VMware UniFi Network*


*Nota*. En esta ventana muestra recomendaciones de cerrar otras aplicaciones antes de comenzar la instalación.

En la siguiente parte, muestra el proceso de instalación lo cual puede durar de tres a cinco minutos, una vez que haya terminado la instalación en la siguiente ventana muestra un mensaje de si deseamos abrir el programa una vez terminado la instalación, se debe poner check en el casillero y presionar en Finish.

**Figura 109**

*Instalación UniFi Network Aplication*

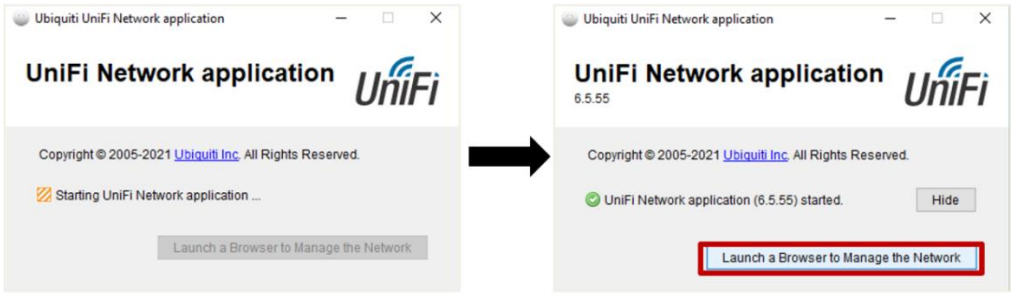



*Nota*. En la ventana final es opcional seleccionar sí que quiere abrir o no el programa al terminal la instalación.

A continuación, aparecerá una pequeña ventana que dirá iniciando la aplicación de red UniFi, al pasar un corto tiempo de 2 a 3 minutos aparecerá un icono en verde que muestra que la aplicación de red UniFi esta iniciada. Por último, se desbloqueará el botón iniciar un navegador para administrar la red.

**Figura 110**

*Ejecución UniFi Network Aplication*



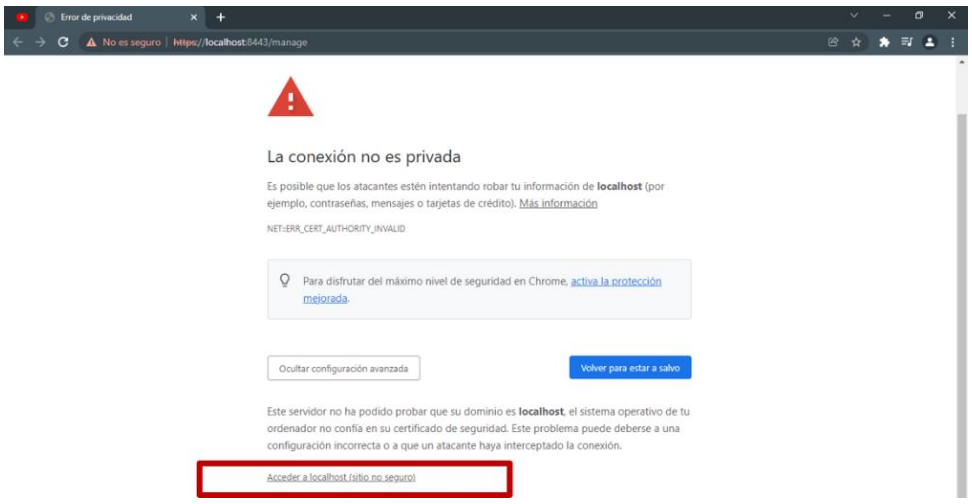

Nota: El launcher está listo para ser ejecutado en un navegador.

### *3.4.12 Configuración Básica UniFi*

El launcher redirige a una página de Google Chrome el cual está conectado a nuestro equipo en el localhost8443, la ventana muestra que la conexión no es privada para ello dar clic en configuración avanzada y se desplegará una opción que dirá Acceder a localhost (sitio no seguro).

**Figura 111**

*Página del localhost*

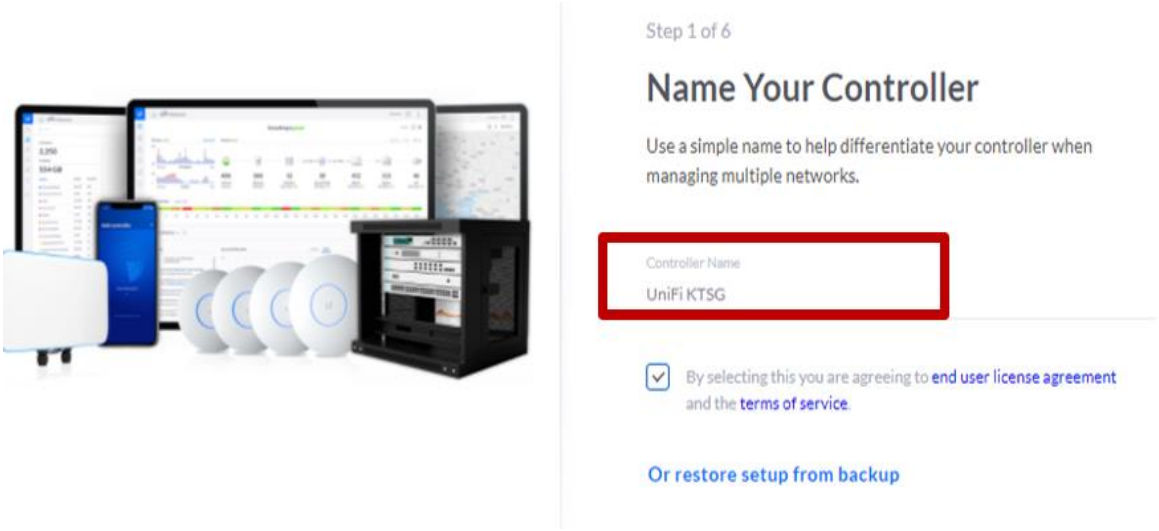



*Nota.* En esta ventana se deberá acceder de forma avanzada por seguridad a nuestra información.

A continuación, como primer paso se debe colocar un nombre al controlador, de esta manera se diferenciará de los demás. Se aceptará los términos y condiciones del servicio, finalmente se dará clic en siguiente.

**Figura 112**

*Nombre del controlador*

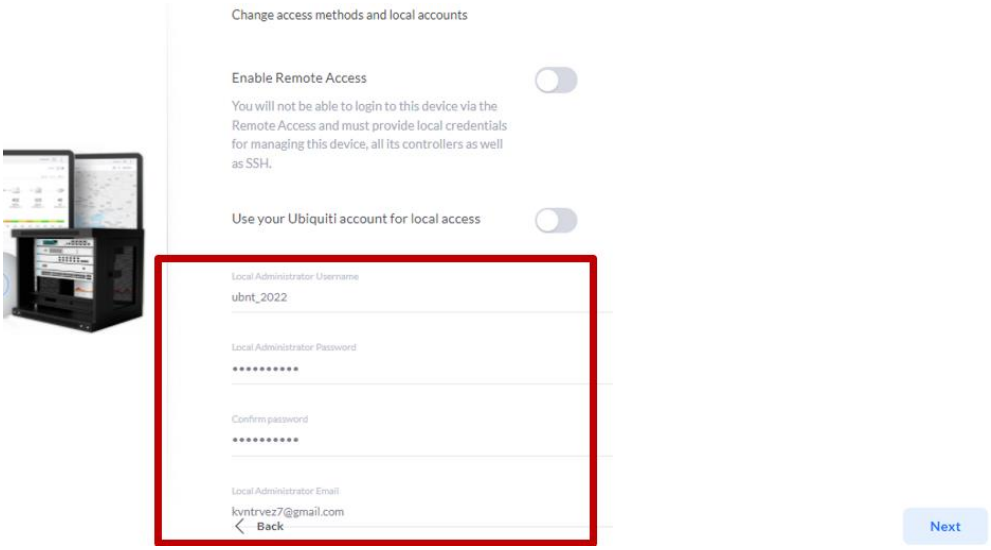



*Nota*. En esta parte del proceso se debe colocar un nombre para el controlador.

Seguidamente en el paso 2 se deberá configurar el acceso local y remoto avanzado, para ello se debe deshabilitar acceso remoto. Además, la opción que indica “use su cuenta de Ubiquiti” es para acceso local, pero como se está iniciando por primera vez y no tiene una cuenta, se deberá colocar información de acuerdo al usuario, contraseña y un correo electrónico.

**Figura 113**

*Configuración acceso local y remoto avanzado*

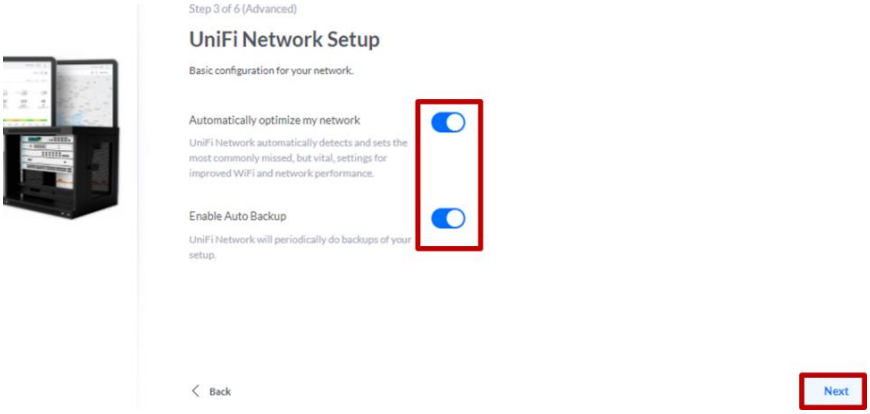



*Nota*. Esta ventana es para usuarios que no poseen una cuenta de acceso.

Después, en el paso 3 muestra la configuración de red UniFi que indica que si desea que la red se optimice automáticamente o si se desea habilitar la copia de seguridad automática. Habilitar las dos opciones y presionar en Next.

**Figura 114**

*Configuración Red UniFi*

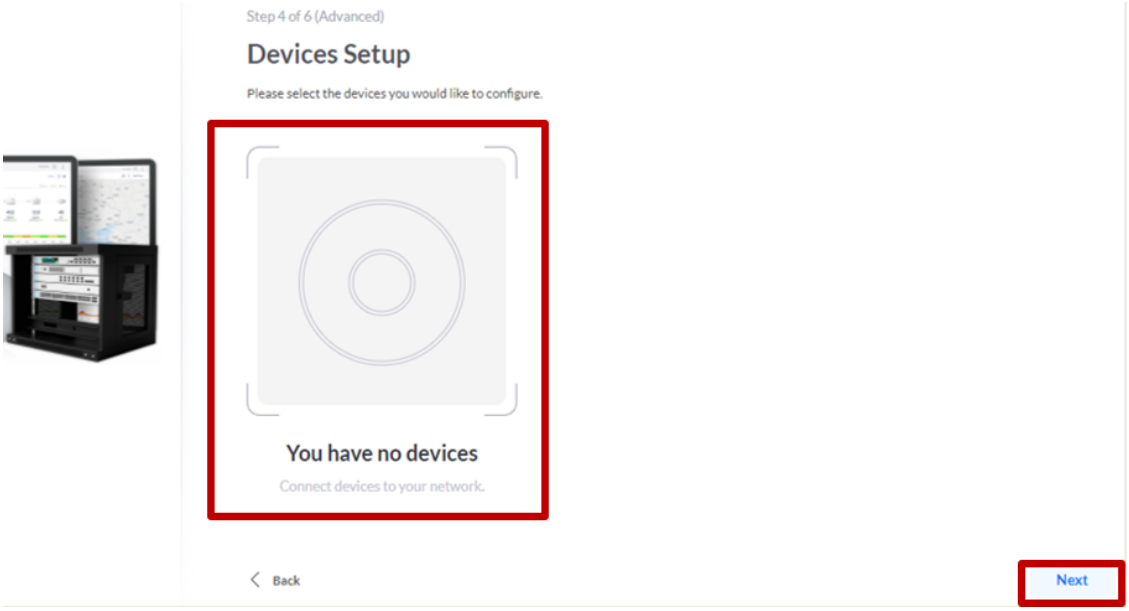



*Nota*. El mantener habilitado las opciones depende del usuario, ya que se puede realizar de forma manual dichas acciones.

En la siguiente ventana como paso 4, indica que se debe seleccionar el dispositivo que desea configurar. En caso de tener dispositivos conectados a la red mostrara, en este caso indica que no existe dispositivos.

**Figura 115**

*Configuración de dispositivo*



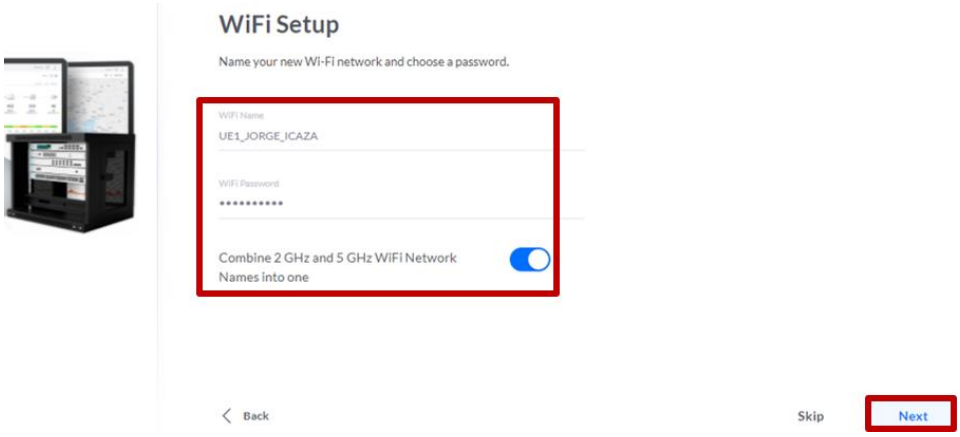

*Nota*. Los equipos no se muestran debido a que no están conectados a la Red.

Posteriormente, en el paso 5 se configura el nombre de la red Wi-Fi en este caso se colocará UE1_JORGE_ICAZA y una contraseña. En la parte final hay un mensaje que indica si se desea combinar 2GHz y 5GHz en la misma red.

La configuración Wi-Fi es opcional porque se puede saltar el paso al presionar clic en Next.

**Figura 116**

*Configuración Wi-Fi*

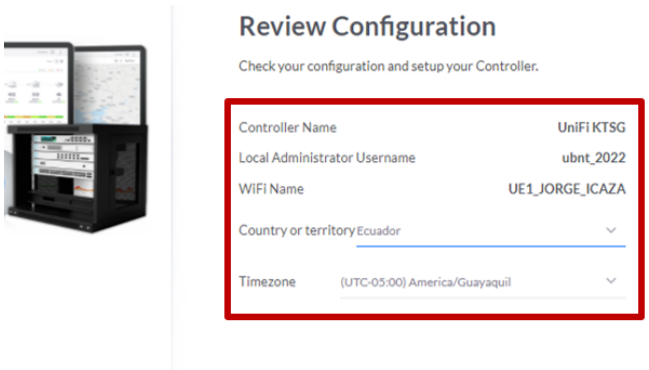



*Nota*. En esta ventana se crea una red Wi-Fi además de habilitar la opción combinada de frecuencias.

Ahora en el paso 6 muestra todas las configuraciones realizadas en los anteriores pasos como es el nombre del controlado, nombre del administrador local, nombre de la red Wi-Fi. Posteriormente se debe colocar el país y la zona horaria donde nos encontramos ubicados finalmente dar clic en Finish.

**Figura 117**

*Review Configuration*



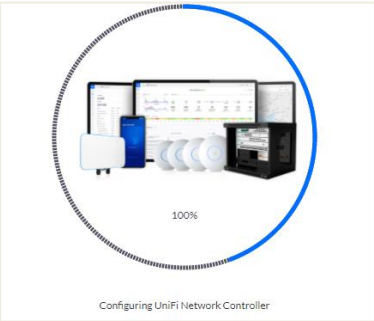

*Nota*. Aquí se puede realizar una revisión general de todas las configuraciones aplicadas.

Finalmente, en la siguiente ventana cargará el proceso de configuración del controlador de red UniFi. Una vez completada la carga se dirige a la interfaz de UniFi donde en la parte central muestra enlaces de los productos que se pueden configurar.

Además, un Ubiquiti Store https://store.ui.com/collections/unifi-network-wireless la barra lateral izquierda posee una lista de herramienta.

**Figura 118**

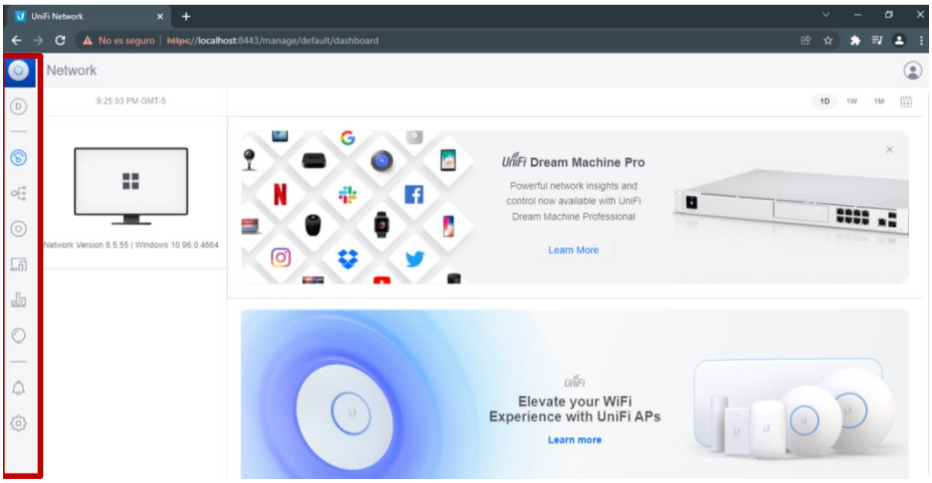
*Proceso final de configuración del controlador*




*Nota*. Aquí se estarán aplicando todas las configuraciones de manera que se debe espera a que este en un 100%.

**Figura 119**

*Interfaz UniFi*




*Nota*. En la ventana principal UniFi también muestra las herramientas de configuración.

### *3.4.13 Configuración Access Point*

Para la configuración primero dirigirse a la parte lateral en Unifi Devices a fin de que detecte los dos Access Point UAP-AC-LR para poder gestionar de manera fácil.

Seleccione el primer AP y se abrirá un pequeño recuadro en donde se colocará UNIFI_AP01 de nombre, seguidamente en la opción Network donde se configura una ruta estática con la dirección de la red Bridge en este caso la 192.168.11.11 con mascara 255.255.255.0, puente de enlace 192.168.11.1, DNS preferido y alternativo de Google 8.8.8.8 y 8.8.4.4, una vez realizado dar clic en aplicar cambios.

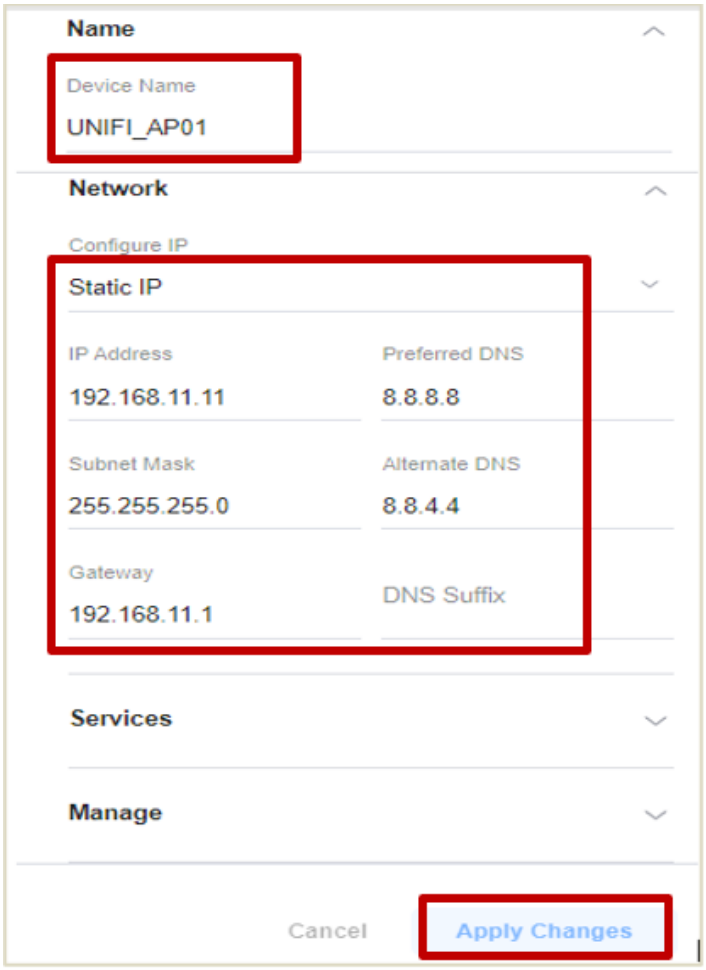
**Figura 120**

*Unidad de dispositivo*


*Nota*. En esta ventana se puede observar los cambios realizados en las configuraciones de UNIFI_AP01.

**Figura 121**

*Configuración UNIFI_AP01*

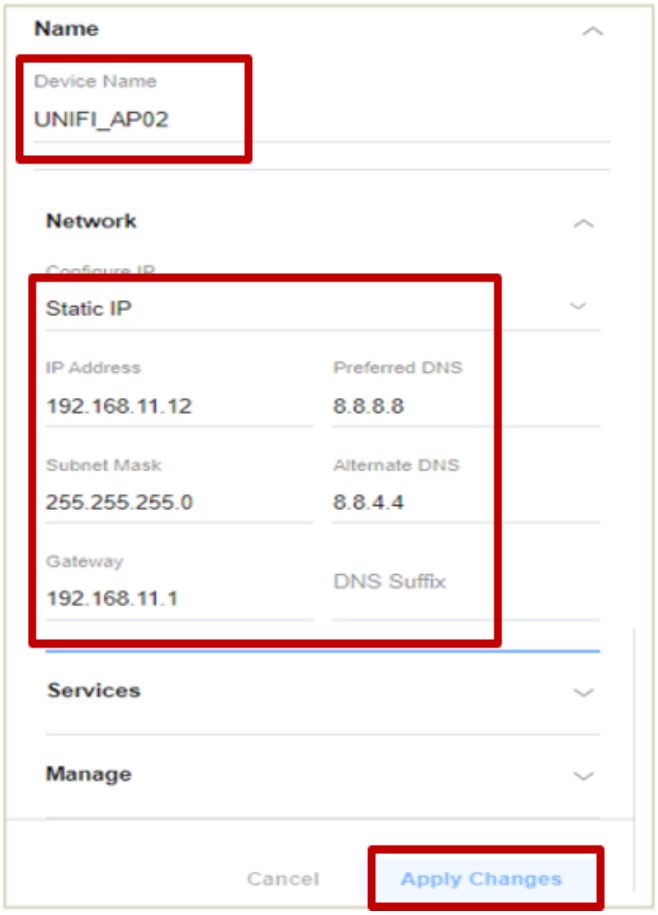



*Nota*. Esta ventana muestra las configuraciones de la IP estática y de los DNS de Google.

De la misma manera seleccionar el segundo AP donde se cambiará el nombre a UNIFI_AP02, después dirigirse a la parte inferior y en Network configurar una IP estática 192.168.11.12 con mascará 255.255.255.0, puente de enlace 192.168.11.1 con DNS de Google 8.8.8.8 y 8.8.4.4. Una vez realizada la configuración aplicar los cambios.

**Figura 122**

*Configuración UNIFI_AP02*



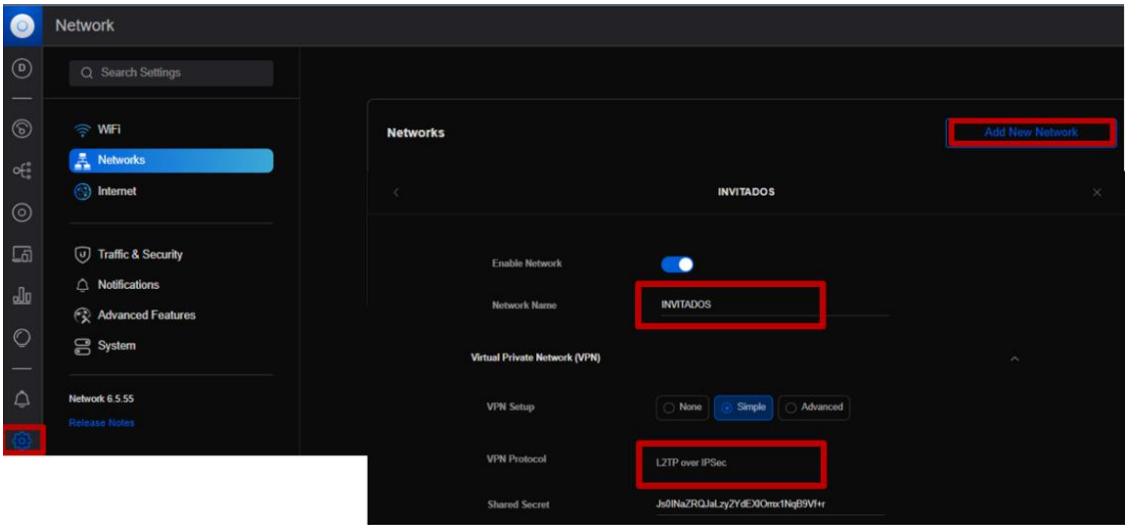

*Nota*. Esta ventana muestra las configuraciones de una IP estática y los DNS de Google.

### *3.4.14 Configuración Red Invitados y Docentes*

En esta configuración se debe ir a ajustes, seleccionar Networks dar clic en agregar una nueva red. Una vez dentro en nombre de la red colocar INVITADOS, en la parte de VPN seleccionar simple por que se trabajara con el protocolo L2TP over IPSec.

**Figura 123**

*Configuración red Invitados*

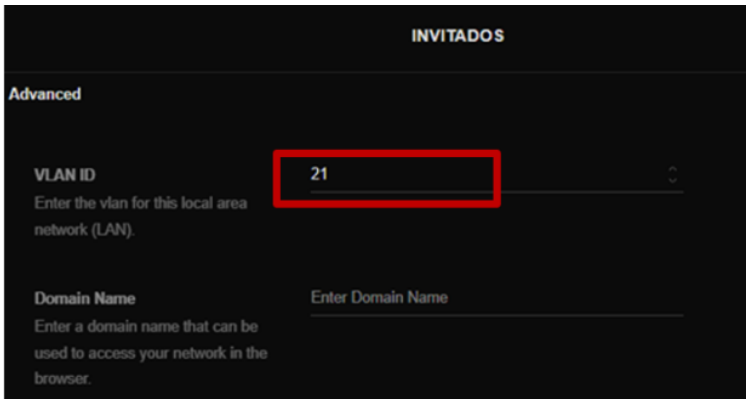



*Nota*. Esta ventana muestra el nombre de la red.

En configuración avanzada se debe ingresar el ID de VLAN en este caso la 21 que pertenece a Invitados, colocar los DNS de forma manual y dejar las demás opciones de forma predeterminada. Aplicar los cambios para que la configuración de la Red quede almacenada.

**Figura 124**

*VLAN 21*

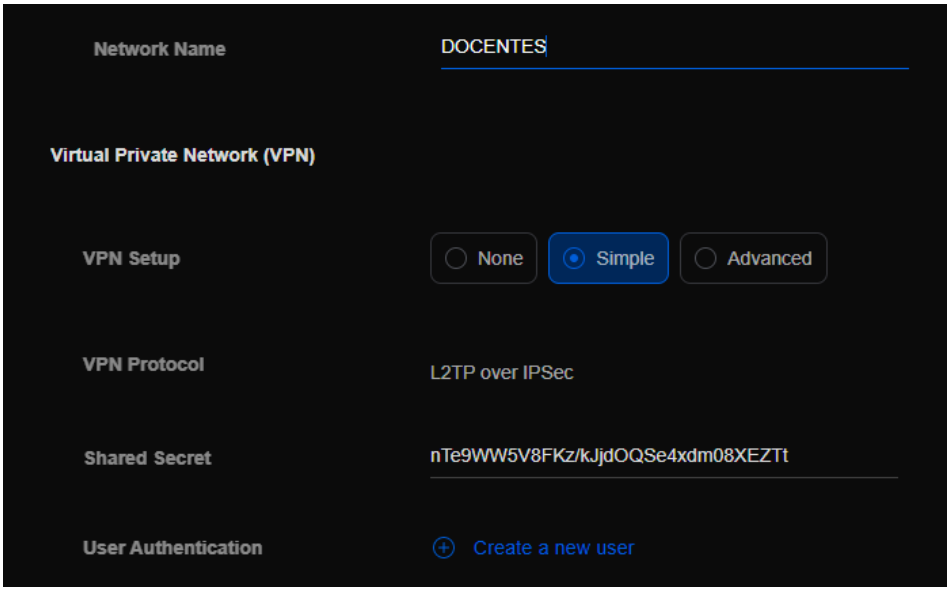



*Nota*. Esta ventana muestra la Vlan 21 creada para los Invitados.

Seguidamente se agregará una nueva red, para lo cual se realizará los mismos pasos anteriores para acceder a la configuración. Una vez dentro colocar el nombre de red DOCENTES, para esto se utilizará el protocolo VPN simple de L2TP over IPSec.

**Figura 125**

*Configuración red Docentes*

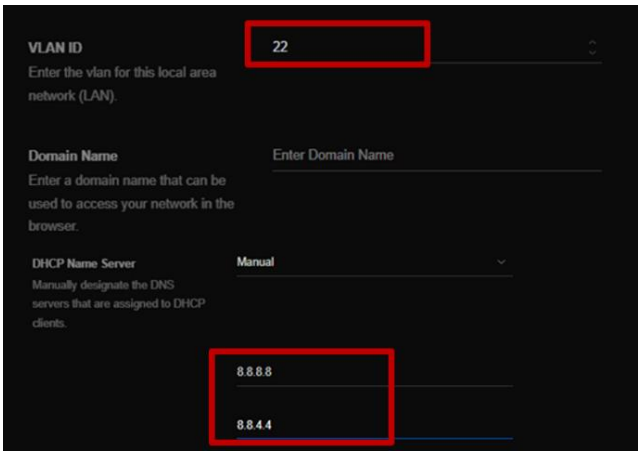



*Nota*. En esta ventana se puede observar la creación de la nueva red.

Finalmente, en configuración avanzada colocar el ID de VLAN 22 que pertenece a Docentes, colocar DNS de forma manual y dejar las demás opciones de forma predeterminada y aplicar los cambios para guardar la configuración de la Red.

**Figura 126**

*VLAN 22*



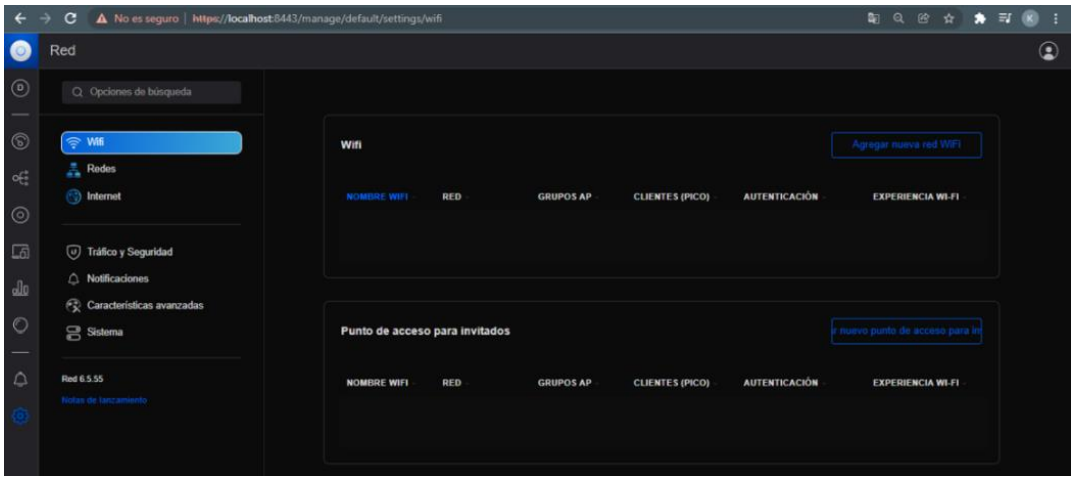

*Nota*. En esta ventana el ID 22 pertenece a la Vlan creada para los Docentes.

### *3.4.15 Creación Punto de Acceso Invitados*

Para la configuración dar clic en ajustes, seleccionar Wi-Fi enseguida se mostrará dos opciones una para crear una red Wi-Fi y la otra para Access Point, seleccionar crear nuevo punto de acceso para invitados para comenzar la configuración.

**Figura 127**

*Interfaz creación Punto de Acceso*

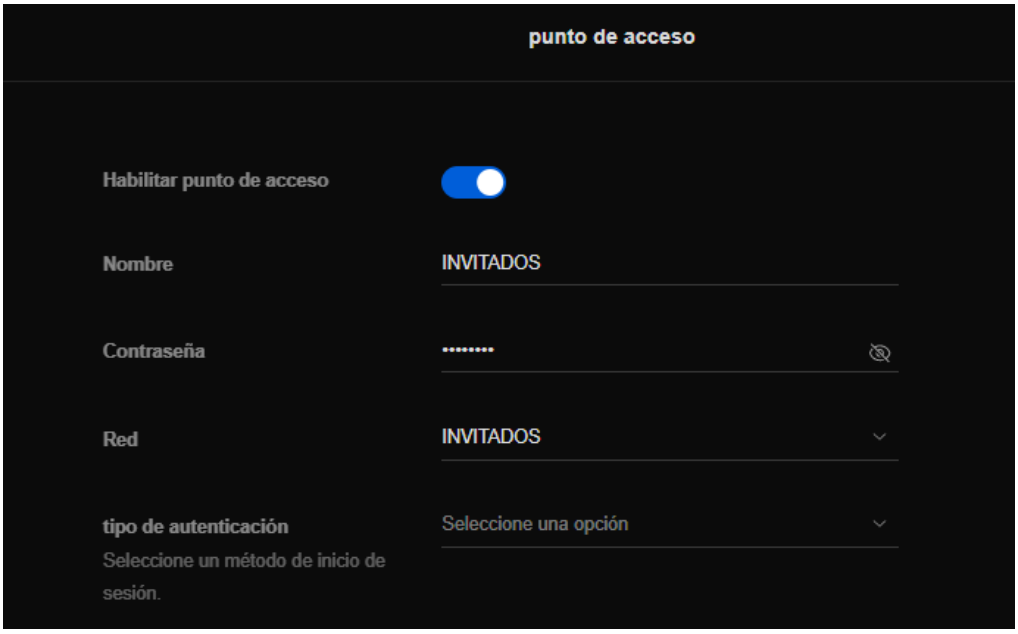



*Nota*. En esta ventana indica dos formas que se puede usar el Access Point Ubiquiti.

A continuación, colocar INVITADOS en el nombre del punto de acceso, en contraseña poner letras números y signos de ser posible. En red colocar INVITADOS de esta manera se estará conectando con la configuración de la Vlan 21, en tipo de autenticación dejar por defecto y activar el portal.

**Figura 128**

*Conexión a Vlan Invitados*



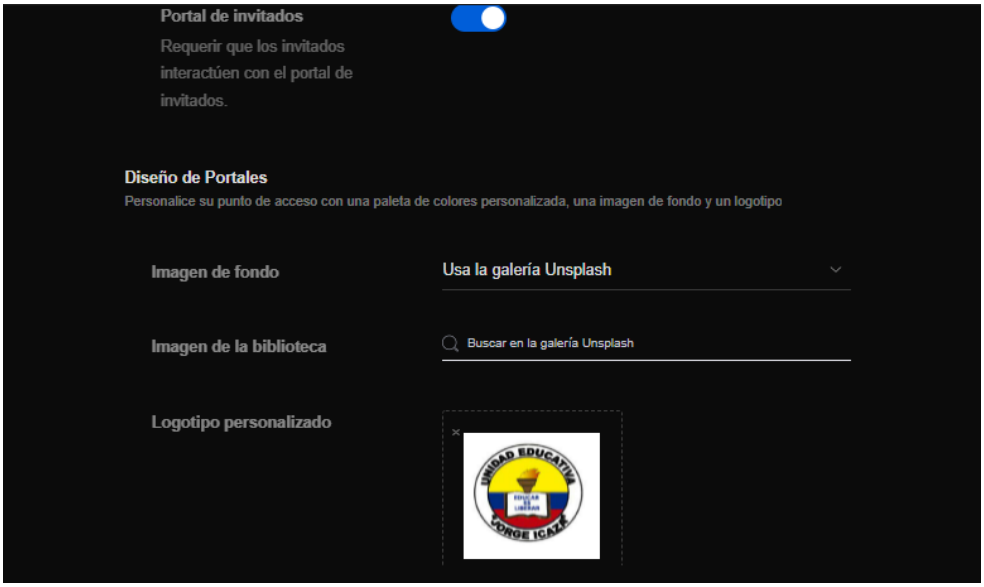

*Nota*. Aquí muestra el nuevo punto de acceso en la red para Invitados.

Al activar el portal para invitados se habilita el diseño de portales donde se colocará el escudo de la Unidad Educativa Jorge Icaza, además se puede modificar varios parámetros.

Posteriormente habilitar la opción donde los usuarios deberán aceptar los Términos de servicio antes de acceder a Internet y configura un mensaje de inicio donde se visualizará el siguiente texto “Bienvenidos”.

**Figura 129**

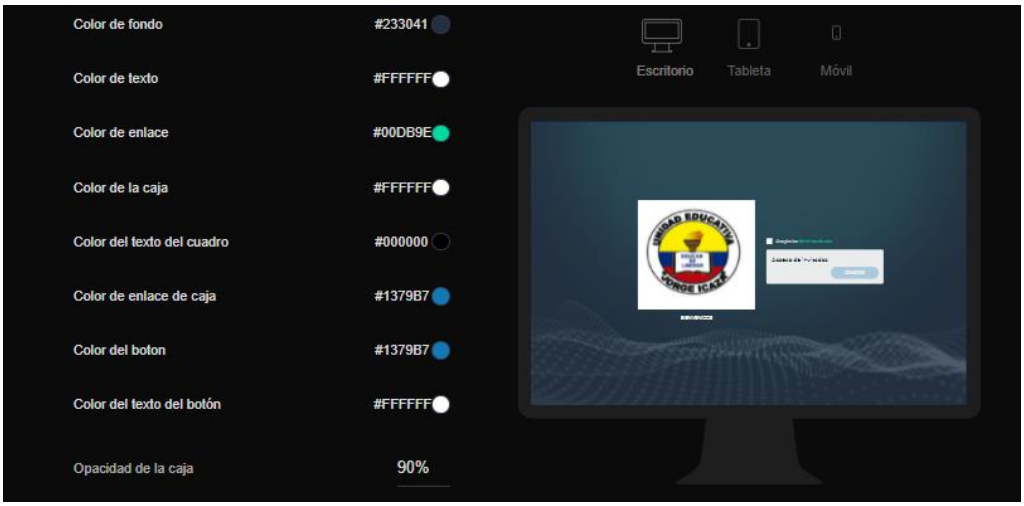
*Portal de invitados*




*Nota*. El portal sirve para que los usuarios interactúen antes de acceder a internet.

**Figura 130**

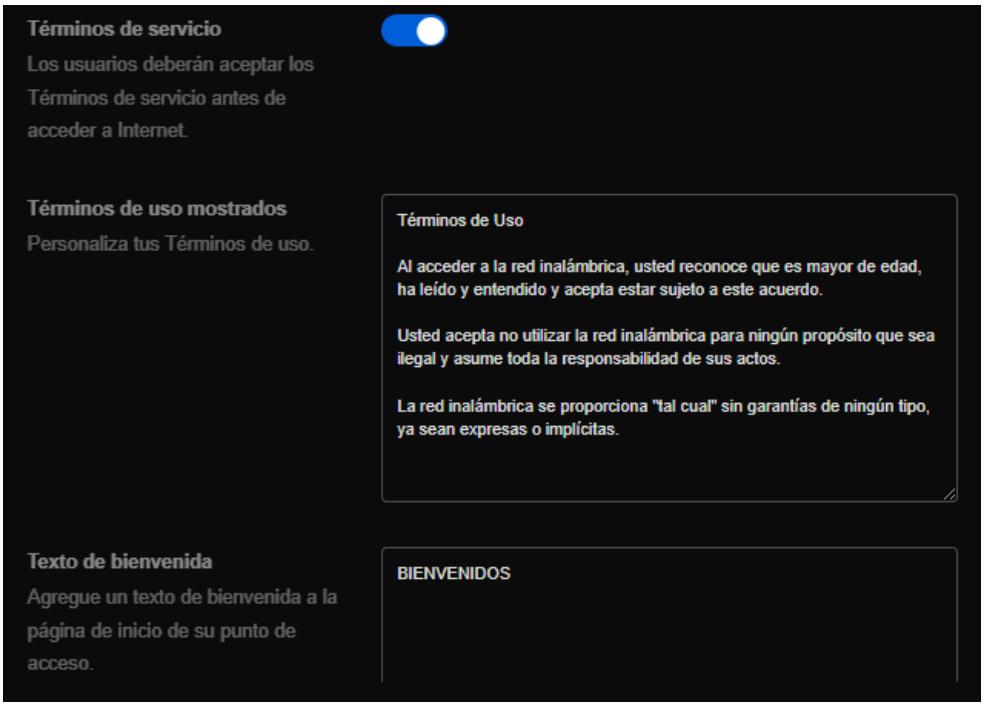
*Opciones de configurar el Portal*




*Nota*. Esta ventana muestra las opciones de configuración y la visualización del portal en Tablet y Móvil.

**Figura 131**

*Habilitar términos del servicio*



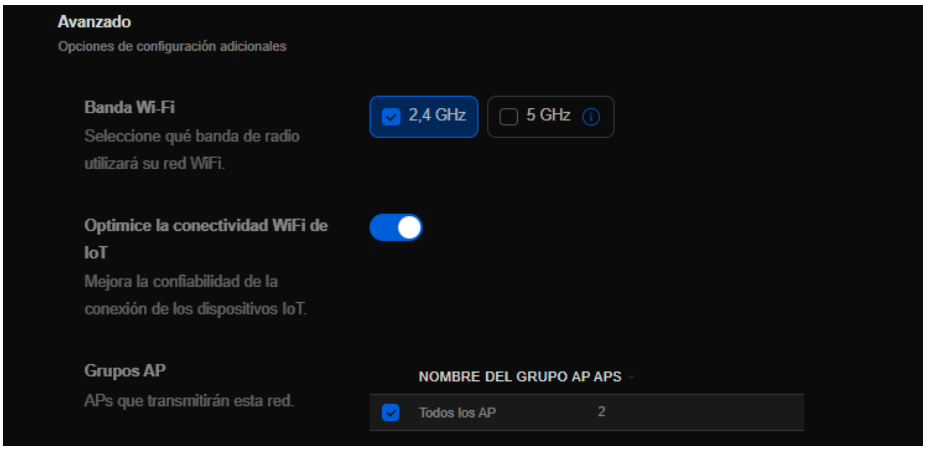

*Nota*. En el apartado términos de uso se establece condiciones para que los usuarios puedan acceder al servicio.

Seguidamente se deberá aplicar configuraciones avanzadas donde la banda de radio de la red Wi-Fi es 2,4GHz. Se activará el protocolo de seguridad WPA-2/WPA-3 que proporcionará seguridad a posibles hackers.

En configuración del portal para la red invitados será con una caducidad de uso al cumplir 6 horas. Finalmente se aplicará los cambios y se creará el punto de acceso para Invitados.

**Figura 132**

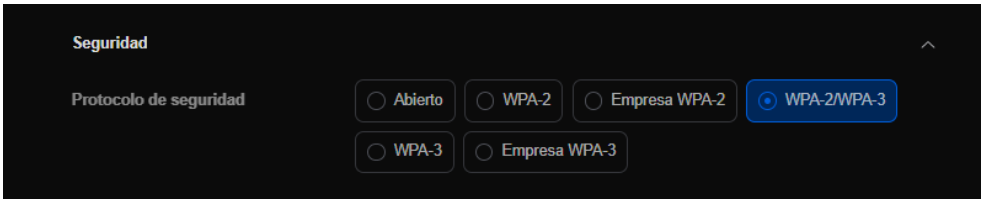
*Selección de la frecuencia*




*Nota*. En la imagen se puede observar la Banda de Wi-Fi es 2.4GHz en uso para mayor rango de la red.

**Figura 133**

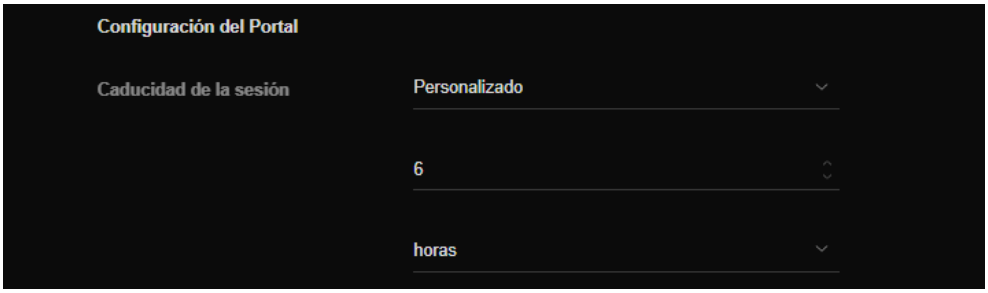
*Seguridad red Invitados*




*Nota*. Se activan dos protocolos porque existen dispositivos que solo soportan WPA2.

**Figura 134**

*Caducidad de sesión*



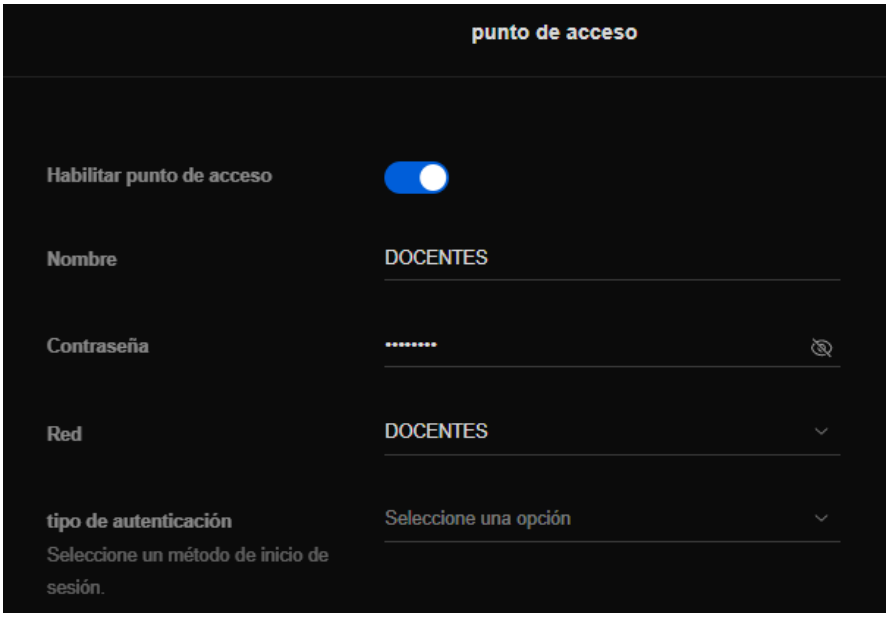

*Nota*. Se personaliza el tiempo de acceso a internet para que la red no se sature.

### *3.4.16 Creación Punto de Acceso Docentes*

La creación del segundo punto de acceso tiene como nombre de red DOCENTES con una contraseña que contiene letras y signos. En la red se deberá seleccionar DOCENTES la cual pertenece a la configuración de la Vlan 22, el tipo de autorización dejamos predeterminadamente.

**Figura 135**

*Conexión a Vlan Docentes*

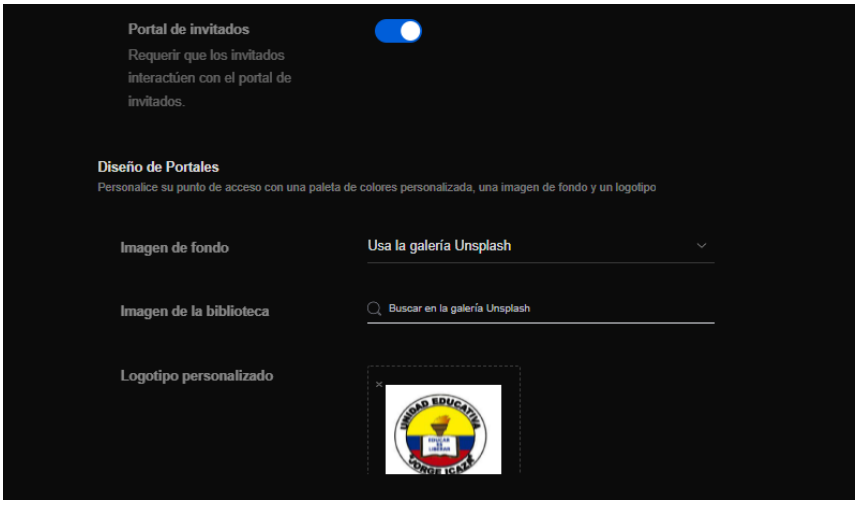



*Nota*. La ventana indica el nuevo punto de acceso para Docentes.

Una vez activado el portal de invitados se procede a colocar el logo de la institución, se activará los términos de uso del servicio y se escribe un mensaje que muestre “Bienvenidos” en el inicio del portal.

**Figura 136**

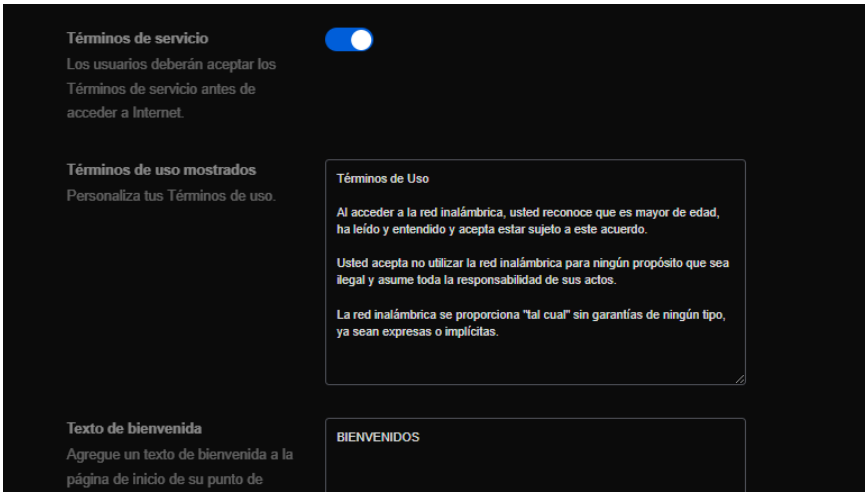
*Portal de Invitados Red Docentes*




*Nota*. La imagen indica el logo de la institución, es opcional colocar una imagen de fondo y de la biblioteca.

**Figura 137**

*Términos y Servicio de Docentes*




*Nota*. Aquí en términos de uso se establece condiciones para que los usuarios puedan acceder al servicio.

Finalmente, en la opción de Banda Wi-Fi seleccionar 2.4GHz por el rango de la red, también en grupos de AP activar con un check el UNIFI_AP01 y UNIFI_AP02 y guardar el grupo. Después activar el protocolo de seguridad WPA 2/WPA 3, la configuración de portal para los docentes tendrá un tiempo de caducidad.

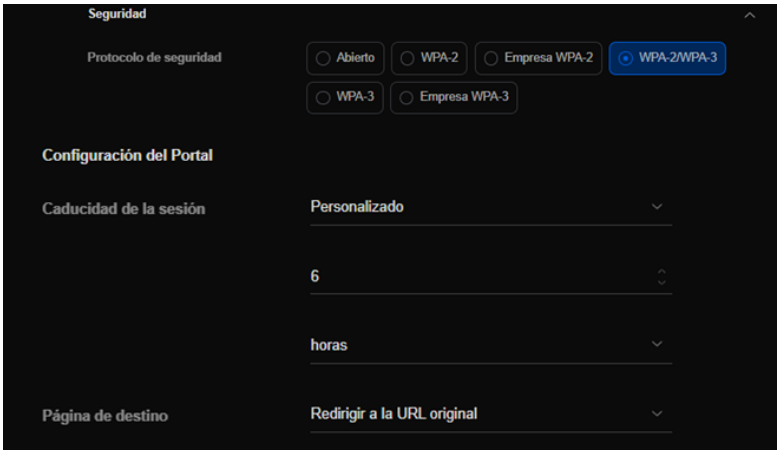
**Figura 138**

*Agrupación de Access Point*


*Nota*. Se activa el grupo para que los dos AP en el lugar que estén tengan la misma función.

**Figura 139**

*Seguridad y Caducidad de sesión*



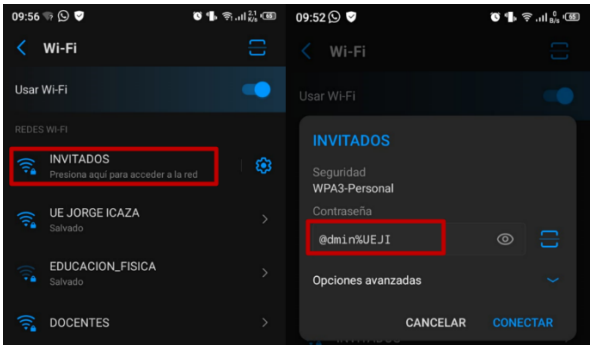

*Nota*. La cantidad de hora asignada para la red docentes se establece en base a la sección matutina y vespertina.

### *3.4.17 Prueba de Funcionamiento Hotspot*

Mediante un dispositivo móvil se procede a acceder a la red de INVITADOS, una vez seleccionado el recuadro colocar la contraseña de seguridad. Se conectará, pero no tendrá acceso a Internet porque primero se debe colocar la contraseña en el portal de invitados.

**Figura 140**

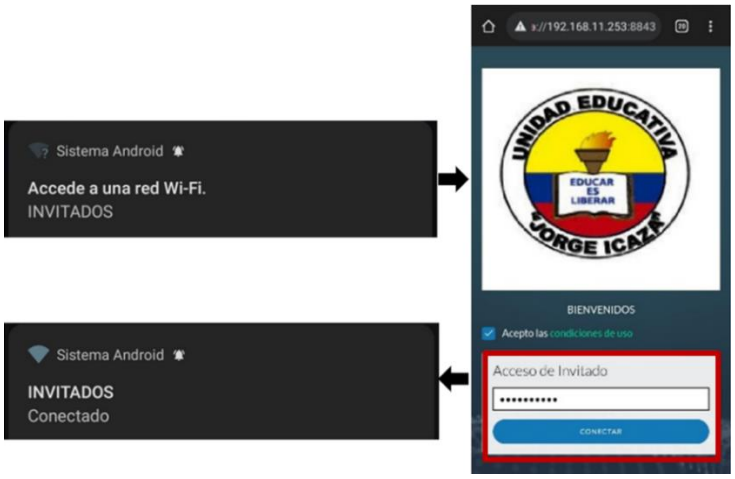
*Acceso a Internet mediante dispositivo Móvil*




*Nota*. En la ventana se deberá colocar una contraseña debido a que el protocolo de seguridad WPA3 necesita este tipo de seguridad.

**Figura 141**

*Portal de interacción*

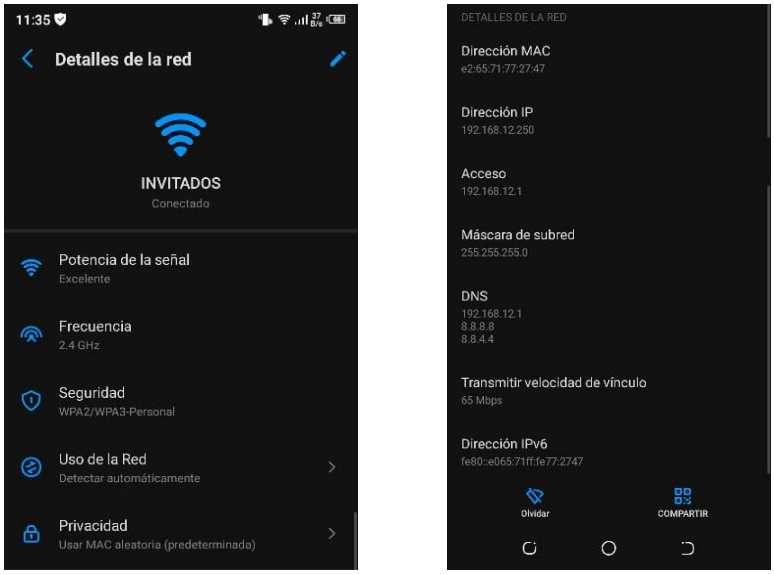



*Nota*. Para tener acceso a Internet obligatoriamente se deberá ingresar al portal cautivo.

En detalles de la red se puede observar una potencia excelente la frecuencia 2.4GHz, seguridad WPA2/WPA3 Personal, también la dirección IP es 192.168.12.250 que pertenece a la VLAN 21, IP de acceso 192.168.12.1, mascara 255.255.255.0 y DNS de Google.

**Figura 142**

*Detalles de la Red Invitados*

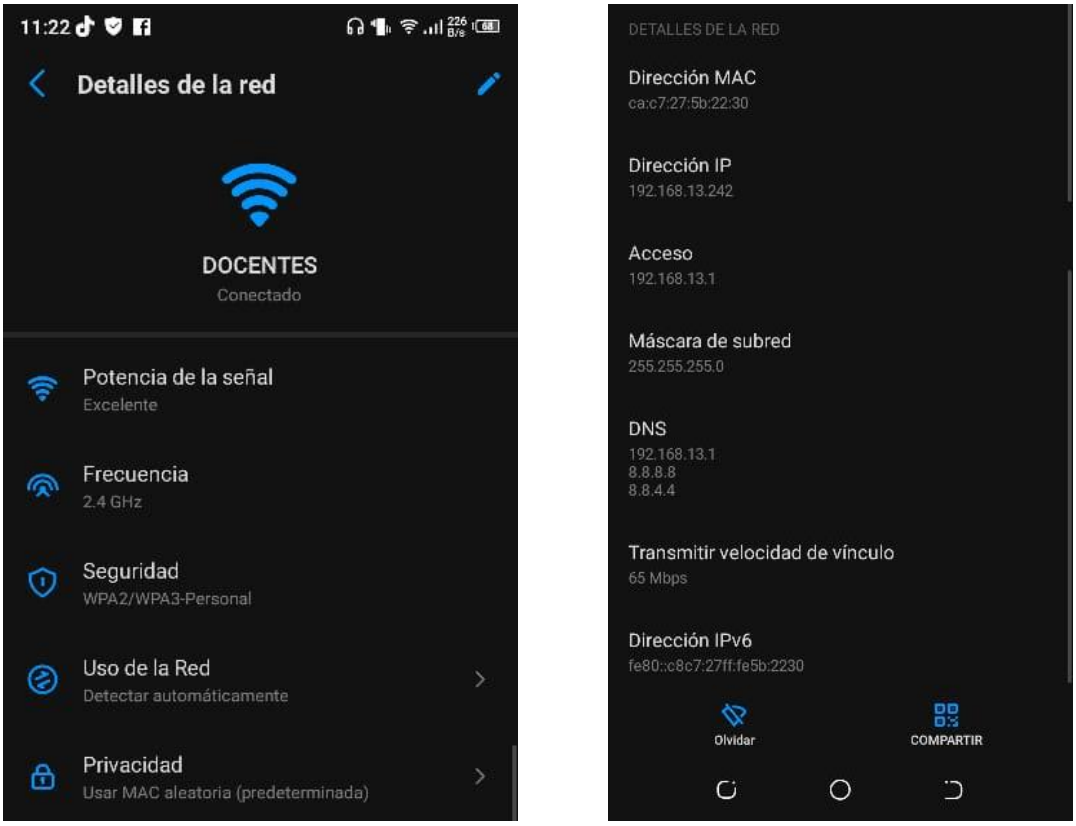



*Nota*. Los detalles que muestra la red Invitados contienen toda la configuración del Hotspot, además de la VLAN 21 creada para los estudiantes.

Seguidamente se verificará la red para los Docentes, para poder acceder a internet se debe interactuar con el portal. En detalles la red se encuentra con una potencia de señal excelente, frecuencia 2.4GHz, seguridad WPA2/WPA3 Personal también en dirección IP esta 192.168.13.242 que pertenece a la VLAN 22 en acceso está el Gateway del puente de enlace, mascara de red 255.255.255.0 y los DNS de Google.

**Figura 143**

*Detalles de la Red Docentes*




*Nota*. La potencia de señal depende de que tan lejos se encuentra el dispositivo de la red.

Finalmente, los dos puntos de acceso creados tienen un plan de 3Mbps para lo cual se procede a ingresar a un navegador y acceder al sitio web https://fast.com/es/ donde se puede ver la velocidad de internet.

**Figura 144**

*Test de Velocidad en VLANs*


*Nota*. Como muestra la imagen la velocidad que tiene la red es 2.8 Mbps con 5ms de descarga y 43ms de Carga.

### *3.4.18 Verificación de funcionabilidad*

Al terminal el proyecto se realizó diferentes pruebas mediante el tester verificando que todo quede funcional desde los patchcords tanto del gabinete como de las computadoras sin ningún inconveniente.

**Figura 145**

*Pruebas de funcionabilidad por medio del tester*


*Nota*. El tester es capaz de detectar cables sin conectar, el método más factible.

### *3.4.19 Análisis del sistema Hotspot*

El análisis se lleva a cabo con el software NetSpot que permite gracias a sus herramientas colocar puntos e ir verificando el nivel máximo de la señal, el canal en que se encuentran trabajando los Access Point y la seguridad que posee.

**Figura 146**

*Cobertura de la Escuela*


*Nota*. Los diferentes colores en el mapa de calor muestran el nivel de señal en cada parte de la escuela

**Tabla 8**

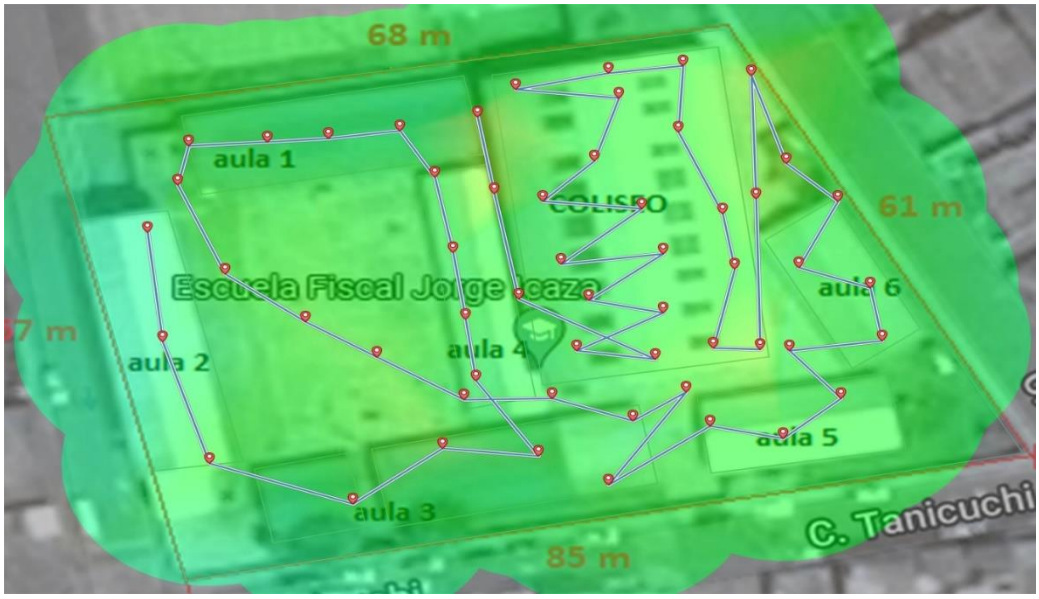
*Datos del Nivel de señal*

| N. | Nombre de Red | Dirección Mac | Canal | Modo PHY | Seguridad | Nivel de señal máximo | Vendedor |
|---|---|---|---|---|---|---|---|
| **1** | INVITADOS | 24:5A:4C:21:DD:2F | 11 | n | WPA3 | -57 | Ubiquiti |
| **2** | INVITADOS | 24:5A:4C:21:DD:03 | 1 | n | WPA3 | -52 | Ubiquiti |

| N. | Nombre de Red | Dirección Mac | Canal | Modo PHY | Seguridad | Nivel de señal máximo | Vendedor |
|---|---|---|---|---|---|---|---|
| **3** | DOCENTES | 2A:5A:4C:21:DD:2F | 11 | n | WPA3 | -50.7 | Ubiquiti |
| 4 | DOCENTES | 2A:5A:4C:21:DD:03 | 1 | n | WPA3 | -46.3 | Ubiquiti |

**Figura 147**

*Velocidad de subida*




*Nota*. Los puntos rojos son la ubicación de donde se realizó las pruebas de señal.

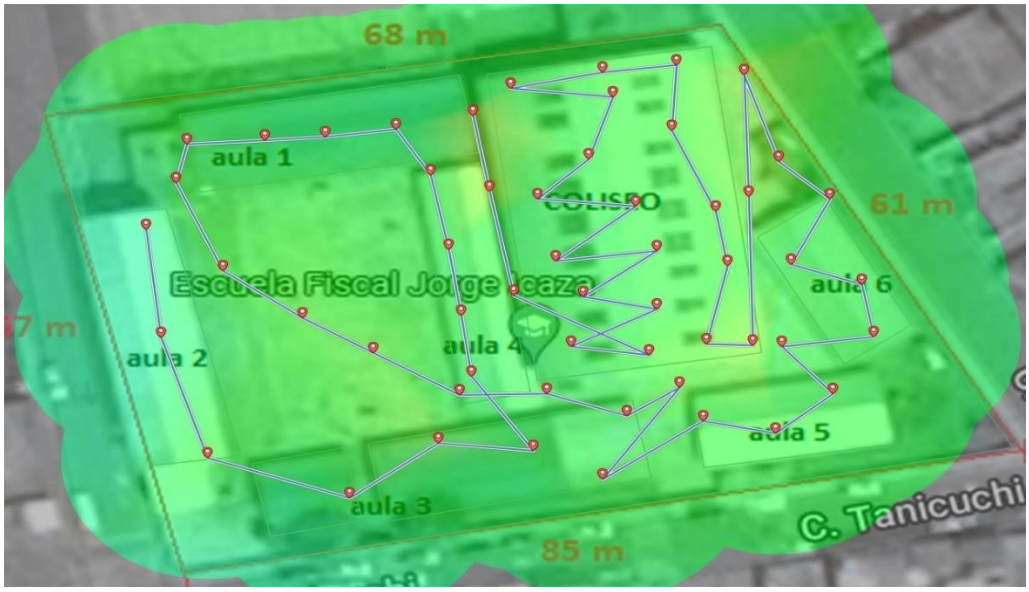
**Tabla 9**

*Datos de la Velocidad de carga*

| N. | Nombre de Red | Dirección Mac | Canal | Modo PHY | Seguridad | Vel. de Carga | Vendedor |
|---|---|---|---|---|---|---|---|
| 1 | INVITADOS | 24:5A:4C:21:DD:2F | 11 | n | WPA3 | 2.6 Mbps | Ubiquiti |
| 2 | INVITADOS | 24:5A:4C:21:DD:03 | 1 | n | WPA3 | 2.7 Mbps | Ubiquiti |
| 3 | DOCENTES | 2A:5A:4C:21:DD:2F | 11 | n | WPA3 | 2.4 Mbps | Ubiquiti |
| 4 | DOCENTES | 2A:5A:4C:21:DD:03 | 1 | n | WPA3 | 2.9 Mbps | Ubiquiti |

**Figura 148**

*Velocidad de descarga*




*Nota***.** Los diferentes colores muestran la cantidad de megas que llega a cada espacio.

**Tabla 10**

*Datos de la velocidad de descarga*

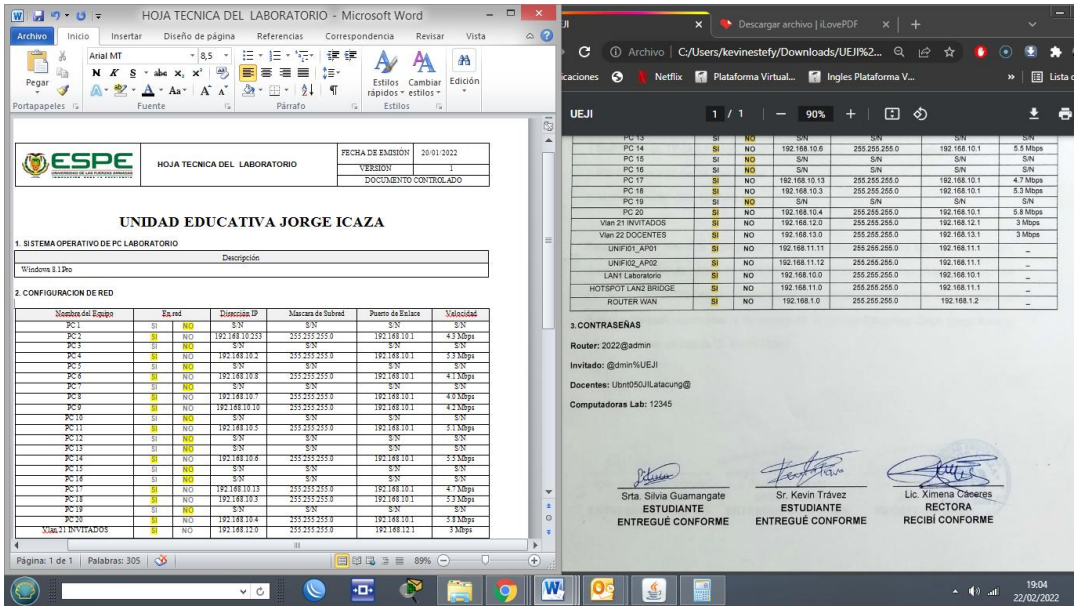
| N. | Nombre de Red | Dirección Mac | Canal | Modo PHY | Seguridad | Vel. de Descarga | Vendedor |
|---|---|---|---|---|---|---|---|
| 1 | INVITADOS | 24:5A:4C:21: DD:2F | 11 | n | WPA3 | 2.5 Mbps | Ubiquiti |
| 2 | INVITADOS | 24:5A:4C:21: DD:03 | 1 | n | WPA3 | 2.7 Mbps | Ubiquiti |
| 3 | DOCENTES | 2A:5A:4C:21: DD:2F | 11 | n | WPA3 | 2.8 Mbps | Ubiquiti |
| 4 | DOCENTES | 2A:5A:4C:21: DD:03 | 1 | n | WPA3 | 2.9 Mbps | Ubiquiti |

## 3.5 Hoja técnica

Este documento cuenta con información que ayuda a identificar de forma rápida las configuraciones que tienen las computadoras del laboratorio así mismo de los equipos como son: Router y Access Point.

**Figura 149**

*Hoja técnica de direccionemiento IP*




*Nota*. La hoja técnica detalla cada dirección IP que se aplicaron en la Red LAN y Hotspot.

# Capítulo IV

# 4 Conclusiones y recomendaciones

## 4.1 Conclusiones

- Se puede concluir en base a la Investigación realizada que, las normativas del cableado estructurado definen un grupo de cables, conectores, canalizaciones y dispositivos que conforman la infraestructura de telecomunicaciones los cuales ayudan a realizar implementaciones de manera óptima y verificada en una red de área local. El análisis de los equipos fue mediante comparaciones de datasheet, que son documentos que especifican las características, entre los equipos utilizados se pueden destacar las marcas Ubiquiti, TP-Link y MikroTik.
- Por cuanto se puede decir, que la implementación de la Red LAN se realizó mediante la normativa ANSI/TIA 568B. Esto indica los requisitos y componentes para el cableado estructurado de telecomunicaciones. Además, para que el sistema funcione las configuraciones se aplicó en un router MikroTik RB750r2 que permite mediante su interfaz tener el control de la red y una fácil manipulación.
- De igual forma se puede concluir que la implementación del sistema Hotspot en la institución, se realizó mediante 2 Access Point Ubiquiti UAP-AC-LR ubicados en el edificio central y el coliseo trabajando con una frecuencia de 2.4GHz. La configuración del mismo cuenta con dos vlan’s para Invitados y Docentes de igual manera posee ancho de banda limitado además de tiempo límite de acceso a la red.
- Finalmente, para comprobar su funcionalidad del cableado estructurado se utilizó un tester, donde al ser conectado a cada extremo del cable de red este nos daría una secuencia de conectividad, también mediante el comando ping en cada equipo se obtuvo una respuesta del servidor de Google. De igual forma

para el sistema inalámbrico Hotspot con la herramienta NetSpot se analizó la red de toda el área de la institución indicando con el mapa de calor su cobertura total.

## 4.2 Recomendaciones

- Una vez concluida el presente trabajo de titulación, se pone a consideración del lector y la comunidad educativa investigar sobre otros aspectos relacionados con las normativas del cableado estructurado, porque debido a que pasa el tiempo la tecnología va cambio por ende las normativas empezaran a cambiar.
- A continuación, se enumeran una serie de recomendaciones cuya implementación son vitales para mantener en buen estado la Red LAN implementada en el Laboratorio, no manipular demasiado los equipos, ni los cables de red que al estar expuestos tienen más probabilidad de llegar a estropearse y mantener el gabinete siempre cerrado a menos que sea necesario.
- En base a los resultados recogidos en la presente investigación y al aporte bibliográfico de este texto monográfico, se recomienda a la institución no manipular los equipos que están expuestos en los puntos estratégicos a que estos podrían llegar a maltratarse por ende dejaría de tener su funcionalidad correctamente.

**Bibliografía**

Alex González Paz, David Beltrán Casanova y Ernesto Fuentes Gari. (Diciembre de 2016). Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202016000400017

Alvino, C. (5 de Mayo de 2021). *Branch*. Obtenido de https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-ecuador-en-el-2020-2021/

Avalos, Y. (2021). *HENTEL.* Obtenido de Yanez Avalos Cia. Ltda.: https://drive.google.com/file/d/0BxZ_p2wlJYeCZ01SMjRxOUZ3TVE/view?resourcekey=0-tquAPtIX4UNH_DS5gLQOmw

Bilegow, S. J. (Agosto de 2021). *TechTarget.* Obtenido de https://www.computerweekly.com/es/definicion/Red-de-area-de-almacenamiento-o-SAN

Calderon, Y. T. (Febrero de 2013). Obtenido de http://132.248.9.195/ptd2013/febrero/0689006/0689006.pdf

Calero, B. X. (2017). *Implementación de un HOTSPOT con servidor RADIUS en la Biblioteca de la Ciudad.* Ambato.

Castillo, J. (12 de Septiembre de 2020). *Profesional Review.* Obtenido de https://www.profesionalreview.com/2020/09/12/cable-par-trenzado-caracteristicas/#:~:text=El%20cable%20par%20trenzado%20es,llevar%20mayor%20cantidad%20de%20datos.

Castillo, J. A. (15 de Febrero de 2019). *Profesional Review.* Obtenido de https://www.profesionalreview.com/2019/02/15/fibra-optica-que-es/

Castillo, M. (2014). *Instalaciones de telecomunicaciones.* Editex.

*Century Link*. (21 de Noviembre de 2021). Obtenido de https://espanol.centurylink.com/home/help/internet/wireless/what-is-a-wi-fi-hotspot1.html

Corvo, H. S. (23 de Octubre de 2019). *Lifeder.* Obtenido de https://www.lifeder.com/topologia-de-arbol/

Dordoigne, J. (Noviembre de 2020). Redes Informáticas. ENI. Obtenido de http://ual.dyndns.org/biblioteca/redes/pdf/unidad%2003.pdf

*ENI Networks.* (12 de Agosto de 2019). Obtenido de https://www.eninetworks.com/blog-que-es-una-red-wan/

Etecé, E. (17 de Febrero de 2022). *Concepto.* Obtenido de https://netcloudengineering.com/funcionamiento-redes-lan/

*FIUBA.* (2018). Obtenido de http://materias.fi.uba.ar/6679/apuntes/CABLEADO_ESTRUC.pdf

Gómez, I. M. (13 de Mayo de 2020). *TeamVOX*. Obtenido de https://teamvox.com/que-es-un-hotspot-y-como-funciona/

Harol Silva y Solorzano Miguel. (2008). *Sistema del Cableado Estructurado.* Barranquilla.

J.A.M.A. (13 de Julio de 2020). *TL*. Obtenido de https://tutorialesenlinea.es/40-protocolos-de-seguridad-en-redes-inalambricas.html

Jose. (7 de Septiembre de 2012). *Slideshare.* Obtenido de https://es.slideshare.net/Dolphinus/normas-para-cableado-estructurado

Manuel Ramirez, Carlos Polanco y Bernardo Farias. (2017). *Universidad Técnica Federico Santa Maria.* Obtenido de http://profesores.elo.utfsm.cl/~agv/elo322/1s13/project/reports/SEGURIDAD.pdf

Mera, D. C. (Septiembre de 2018). Obtenido de https://dspace.ups.edu.ec/handle/123456789/17336

*NetSpot*. (2020). Obtenido de https://www.netspotapp.com/es/blog/wifi-security/wifi-encryption-and-security.html#WPA

*NetSpot*. (2021). Obtenido de https://www.netspotapp.com/es/blog/wifi-security/what-is-wpa3.html

Noguera, B. (9 de Octubre de 2019). *Lifeder.* Obtenido de https://culturacion.com/topologia-de-red-malla-estrella-arbol-bus-y-anillo/

Orduño, M. R. (17 de Marzo de 2021). *ALEPH.* Obtenido de https://aleph.org.mx/cual-es-el-funcionamiento-de-la-topologia-de-estrella

Parra, Y. (2017). *DOCPLAYER.* Obtenido de https://docplayer.es/user/2684814/

Poveda, J. M. (30 de Enero de 2020). *INTERNEXA*. Obtenido de https://www.internexa.com/blogs/empresas-y-gobierno/conectividad/conoce-los-tipos-de-redes-informaticas/

Ramírez, I. (3 de Julio de 2020). *Xataka*. Obtenido de https://www.xataka.com/basics/que-se-diferencia-seguridad-wifi-wpa3-wpa2

Regalado, J. A. (2017). Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/27183/1/HERRERA%20REGALADO%20JOS%C3%89%20ARTURO%20final.pdf

Sosa, C. R. (2011). Redes de computadoras. MÉXICO: IPN.

*UNITEL.* (Noviembre de 2020). Obtenido de https://unitel-tc.com/normas-sobre-cableado-estructurado/

*Wiki Pluz.* (2018). Obtenido de https://sites.google.com/site/pluzwiki/normas-de-cableado-estructurado

# ANEXOS