UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

CARRERA: INGENIERÍA EN SISTEMAS

Proyecto Técnico previo a la obtención del título de: INGENIERO DE SISTEMAS

TEMA:

REDISEÑO DE LA RED INALÁMBRICA E IMPLEMENTACIÓN DE MECANISMO DE SEGURIDAD UTILIZANDO MIKROTIK ROUTER OS BASADO EN UN SERVIDOR HOTSPOT APLICANDO LAS NORMAS IEEE 802.11 EN LA FUNDACIÓN DAMAS DEL HONORABLE CUERPO CONSULAR CENTRO MÉDICO SUR.

AUTOR:
JEFFERSON JOSEPH DELGADO PROAÑO

DIRECTOR:
ING. DARIO HUILCAPI

Guayaquil, Ecuador
2018

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO

Yo, Jefferson Joseph Delgado Proaño, autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

.....
Jefferson Joseph Delgado Proaño
CI 0930249198

CESIÓN DE DERECHOS DE AUTOR

Yo Jefferson Joseph Delgado Proaño con documento de identificación N° 0930249198, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de grado intitulado: "REDISEÑO DE LA RED INALÁMBRICA E IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD UTILIZANDO MIKROTIK ROUTER OS BASADO EN UN SERVIDOR HOTSPOT APLICANDO LAS NORMAS IEEE 802.11 EN LA FUNDACIÓN DAMAS DEL HONORABLE CUERPO CONSULAR CENTRO MÉDICO SUR ", Mismo que ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....
Jefferson Joseph Delgado Proaño
CI 0930249198

CERTIFICACIÓN

Certifico que el presente proyecto técnico previo a la obtención del título Ingeniero de Sistemas fue realizado por el Sr. Jefferson Joseph Delgado Proaño bajo mi supervisión.

……

Ing. Darío Huilcapi Subía.

Tutor de Proyecto

DEDICATORIA

El presente trabajo se la dedico a Dios por poner en mi vida a personas que fueron fundamentales a lo largo de toda esta etapa universitaria.

A mi madre Emperatriz por su apoyo incondicional creyendo en mí en todo momento, por su preocupación de darme siempre lo mejor y también por darme la educación de enseñarme lo correcto. A mi mama Blanca que siempre estuvo pendiente en ayudarme y preocupándose por darme lo mejor junto a mis hermanos.

A mi tía Lucia que siempre estuvo pendiente y me apoyo en toda la carrera, siendo un ejemplo a seguir junto a mi tío Alberto que se mantuvieron en darme consejos sobre sus diferentes experiencias. A mi tía Paulina y Marisol que siempre estuvieron dándome su tiempo para cualquier consejo y ánimos.

A mi tío Vicente que siempre estuvo ahí como un padre, dándome consejos.

A mi novia Karem Valero, por su apoyo y paciencia en todo momento e inspirarme crecer como persona y profesionalmente. Gracias por creer en mí.

A mis hermanos, primos, tíos, amigos que siempre me dieron su aliento para salir adelante.

Jefferson Delgado Proaño

AGRADECIMIENTO

Primeramente agradezco a Dios por darme la fuerza para seguir adelante y permitir obtener nuevos logros en esta vida, logrando culminar sin ningún inconveniente mis estudios universitarios. También por una familia que siempre estuvo unida pendiente de mi bienestar, a mi madre Emperatriz sacrificándose en todo momento con consejos y apoyo, a mi madre Blanca por su apoyo incondicional y sacrificio siendo ellas los pilares fundamentales para seguir adelante. A mi tío Vicente y tías Lucia, Paulina, Marisol de una forma u otra forma estuvieron presente desde pequeño ayudándome y dándome su apoyo el cual el día hoy soy lo que soy por ellos.

A mi novia Karem Valero, siendo una compañera fiel el cual tuve su apoyo tanto en los buenos y malos momentos dándome motivación, consejos, y la oportunidad de aprender cosas nuevas junto a ella para seguir adelante.

Al tutor de mi proyecto técnico, Ing. Darío Huilcapi Subía no solo por la orientación del presente trabajo, sino también por sus conocimientos y experiencia trasmitida cuando tuve la oportunidad de ser su alumno.

Docentes y amigos que siempre estuvieron predispuestos a cualquier ayuda y aportaron a mi educación.

Al Ing. Rubén Rivera y Danny Valverde por su buena aportación de su experiencia laboral para fortalecer mis conocimientos. Al Ing. Christian Burgos por su experiencia y profesionalismo que me ha permitido culminar este proyecto en la fundación.

A la señora Esmeraldas de Parodi, coordinadora general del centro médico Sur de la Fundación Damas del Honorable Cuerpo Consular por permitirme la facilidad y la confianza de poder implementar el presente proyecto en las instalaciones de la fundación.

Dios los bendiga a todos

Jefferson Delgado

RESUMEN

El propósito de este proyecto consiste en rediseñar una red inalámbrica utilizando tecnología Mikrotik en el edificio principal de la Fundación Damas del Honorable Cuerpo Consular Centro Médico Sur. Para el acceso a la red inalámbrica se utilizó un portal cautivo siendo implementado en un servidor hotspot que permite almacenar la lista de usuarios doctores e invitados, mientras para los usuarios administrativo se utilizó la versión Ubuntu 16.04 para la instalación de un servidor Radius con la respectiva base de datos Mysql y poder llevar un registro de todos los usuarios administrativo que pertenecen a la fundación.

La instalación de cada punto acceso inalámbrico se determina según la influencia de usuarios, permitiendo realizar un análisis de propagación inalámbrica en cada access point para que pueda existir una óptima señal y cubrir las áreas requeridas. Cada access point o también llamado cap será administrado por un controlador llamado Capsman que permite gestionar de manera centralizada todos los caps usando comunicación segura DTLS, en el controlador se crea los ssid según el grupo el usuario asociado a una vlan que permite la segmentación del trafico inalámbrico.

Para los mecanismos de seguridad se utiliza las diferentes reglas en el firewall del servidor Mikrotik bloqueando páginas web, descargas, servicios, puertos y usuarios con el fin de tener una red segura.

Finalmente, una vez realizado las configuraciones tanto en el router, servidor Radius y access points se procede a instalar la red cableada para las conexiones de los switches con las Vlans establecidas en cada puerto, luego se conectan los Access points para brindar un acceso inalámbrico a los usuarios de la fundación permitiendo al departamento de sistemas tener un monitoreo y control centralizado de todos los usuarios.

ABSTRACT

The purpose of this project is based in the redesign of a wireless network in the main building of the Foundation "Damas del Honorable Cuerpo Consular" located in the south of the city. For access to the wireless network, was used a captive portal, being implemented in a hotspot server that allows storing the list of users doctors and guests, for the administrative users was used the version of Ubuntu 16.04 for the installation of a Radius server with the respective Mysql database in order to keep a record of all administrative users belonging to the foundation.

The installation of each wireless access point is established according to the influence of users, allowing a wireless propagation analysis in each access point so that an optimal signal can exist and cover the required areas. Each access point or also called cap will be managed by a controller called Capsman that allows to centrally manage all the caps using secure communication DTLS, in the controller the ssid is created according to the vlan.

For security mechanisms, the different rules are used in the Mikrotik server firewall blocking web pages, downloads, services, ports and users in order to have a secure network.

Finally, once the configurations have been made in the router, Radius server and Access point, it proceed to install the wired network for the connections of the switches with the Vlans established in each port, then the access points are connected to provide wireless access to the users of the foundation, allowing the systems department to have a centralized monitoring of all users.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

Actualmente las redes inalámbricas están presentes en todos los medios posibles, dando la oportunidad de que diversas empresas implementen nuevas tecnologías y crezcan con el tiempo, logrando así que personas tales como los usuarios de la Fundación Damas del Honorable Cuerpo Consular Centro Médico Sur requieran el uso del medio inalámbrico dentro de las instalaciones. Es por eso que la tarea más requerida es administrar la red Wifi, para tener un control de todos los equipos conectados y tener un registro de usuarios autorizados para asegurar el correcto uso de la red Wifi.

La Fundación Damas del Honorable Cuerpo Consular, en los años de estar presente en la ciudad tiene como propósito brindar atención médica a personas de bajos recursos mediante el cual doctores y personal administrativo usan dispositivos inalámbricos tales como celulares, tablets o laptops para conectarse a internet mediante una red Wifi, esto provoca una incorrecta asignación de ancho de banda entre la red siendo necesario segmentar mediante vlans cada grupo de usuarios con su propio SSID para asi otorgar diferentes reglas y permisos de acuerdo a las políticas establecidas de la fundación. Para el manejo centralizado de los access points se usa una aplicación que se ejecuta en el mismo Mikrotik el cual se lo conoce como Capsman, permitiendo la administración y configuración centralizada de los access point y así lograr proveer autenticación y control de acceso de alta concurrencia a determinada área. El propósito de este proyecto es permitir una seguridad óptima con el correcto uso del ancho de banda que se disponga y obtener la administración del uso de la red de los diferentes usuarios que trabajan en la fundación.

2. PROBLEMA

Actualmente en la ciudad de Guayaquil existen diferentes centros médicos que brindan servicios tales como consultas médicas, exámenes de rayos x, laboratorio y la Fundación Damas del Honorable Cuerpo Consular Centro Médico Sur, con la finalidad de brindar servicio inalámbrico a usuarios administrativo y doctores que permita tener conectividad a internet, requiere de buena cobertura inalámbrica en las instalaciones el cual preste las garantías suficientes como herramienta de trabajo.

El problema de lentitud en la red y el incorrecto uso del ancho banda se debe a que todos los usuarios se conectan mediante una clave compartida, clave que es empleada en los diferentes equipos inalámbricos que el usuario disponga, considerando que esa misma clave sea distribuida a usuarios externos o pacientes que utilizan el internet para otros asuntos, generando una lentitud mayor en la red lan de la Fundación, utilizado también por los departamentos administrativos en diferentes servicios como correos electrónicos, facturación, etc. Cuando se conoce cuál es el usuario conectado que consume bastante ancho banda no se puede limitar su velocidad ni bloquear al no existir una administración de la red Wifi.

2.1 Antecedentes

Actualmente la fundación no cuenta con un apropiado diseño de la red inalámbrica, por esta razón origina inconvenientes al personal de sistemas en el control de usuarios conectados. La creciente demanda del uso de las tecnologías de información y comunicación (TIC) que se viene dando en el progreso de las comunicaciones permite encontrar nuevas soluciones de conectividad para la red Wifi, es por eso que la fundación brinda internet a los usuarios a través de routers inalámbricos, los cuales poseen una seguridad inalámbrica poca robusta logrando así una desorganización y disminución en el ancho de banda.

Actualmente, se conoce los problemas que se presenta en no tener una protección hacia la red Wifi de una empresa, siendo crítico el tema de usuarios no autorizados que se conecten a la red inalámbrica y logren distribuir malware.

2.2 Importancia y alcances

En el rediseño de la red inalámbrica serán aplicados los estándares 802.11 para el correcto uso y seguridad de la red siendo fundamental en la fundación para llevar un control sobre el personal administrativo y doctores en la red wifi.

Con el avance de las redes inalámbricas principalmente en las redes Wifi en los últimos años, permite a la fundación maneras de interactuar con su personal administrativo, doctores e invitados implicando manejar riesgos como hackeo, virus a la estructura de la red e información.

Debido a estas amenazas se implementa el presente proyecto utilizando una autenticación mediante un portal cautivo para la validación de los usuarios administrativo con un Radius externo y para usuarios doctores e invitados se valida mediante la gestión del Hotspot, permitiendo tomar medidas de seguridad con el control y protección de la información y asi evitar posibles ataques y accesos no autorizados.

Así los usuarios beneficiarios del proyecto serán:

Fundación Damas del Honorable Cuerpo Consular:

La Fundación podrá tener un servicio que cumpla con las normas en redes inalámbricas facilitando a los usuarios el uso de dispositivos inalámbricos.

Coordinador de Sistema

Podrá conocer los usuarios que se conectan y tener un control de acceso de los dispositivos dándoles diferentes permisos a los grupos usuarios. También podrá tener un manejo centralizado mediante un controlador de Access Point.

Usuarios (Personal Administrativo, Doctores, Invitados)

El usuario podrá saber que se autentica en una red existente, y no correr el riesgo de conectarse a una Wifi clonada y poder ser hackeado.

2.3. Delimitación

El presente proyecto se implementa en la Fundación Damas del Honorable Cuerpo Consular ubicada en el Sur de Guayaquil, Avenida Domingo y Calle F.

Ubicación Geográfica

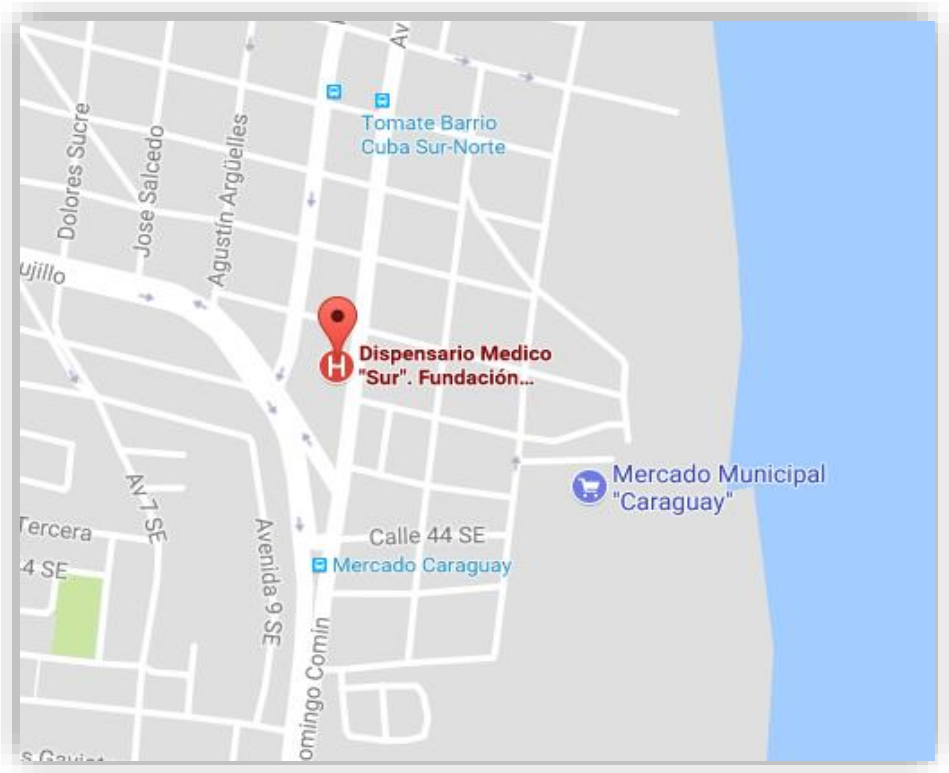


Figura 1 Ubicación geográfica del Centro Médico Sur

Fuente: Google Maps

Ubicación Satelital

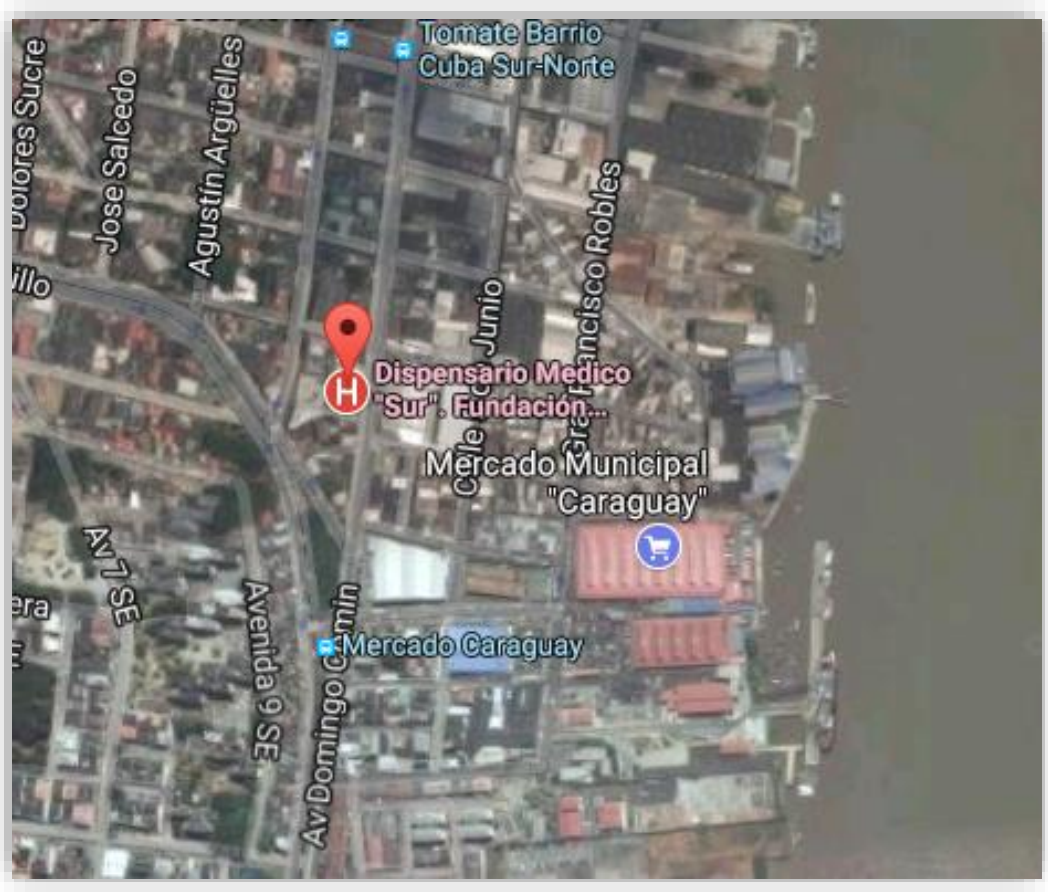


Figura 2 Ubicación satelital del Centro Médico Sur

Fuente: Google Maps

Para cada grupo de usuarios (administración, doctores, invitados) se segmenta mediante Vlans con un SSID, logrando así proteger la información de los usuarios y tener un mejor control con respecto al uso de la velocidad de navegación en los diferentes grupos de usuarios. En cada Vlans se hará el uso de calidad de Servicio (QOS) que permita administrar el ancho de banda tanto como administración, doctores e invitados.

Se crea Hotspot en las diferentes Vlans permitiendo el control de ingresos mediante usuarios únicos, agregando los perfiles de usuario para asignar sesiones máximas y tiempo de conexión.

3. OBJETIVO GENERAL Y ESPECÍFICOS.

3.1 Objetivo General

Rediseñar una red inalámbrica basado en parámetros de normas IEEE 802.11 con un nivel de seguridad óptimo, para los usuarios de la Fundación Damas del Cuerpo Consular.

3.2 Objetivos Específicos

- Administrar de manera centralizada todos los puntos de acceso con su respectiva configuración a través de un controlador inalámbrico de Access Points.

- Realizar un análisis para conocer la demanda de usuarios conectados y aplicaciones que se utiliza, mediante una entrevista al personal de sistemas.

- Administrar el manejo de políticas de seguridad para los usuarios de la red Wifi a través de HotSpot.

4. REVISIÓN DE LA LITERATURA O FUNDAMENTOS TEÓRICOS O ESTADO DEL ARTE

4.1 Redes Inalámbricas

Las redes inalámbricas se encuentran disponibles en todas las instalaciones ya sea para computadoras, celulares, equipos médicos entre otros dispositivos que soporten tecnología inalámbrica. Con el propósito de poder desarrollar este proyecto se explica los diferentes componentes básicos que son principales para tener una idea más clara del origen de la tecnología inalámbrica. Los componentes que se deben tomar muy en cuenta para una red inalámbrica son los estándares y compatibilidad la cual explica las normas convenientes para elaborar un diseño apropiado de una red y conocer la cobertura inalámbrica que se debe aplicar. En las tecnologías inalámbricas para tener una red segura se debe tomar en cuenta los mecanismos utilizados en las configuraciones del access point, el cual deberá ser administrado por un controlador de red inalámbrica.

4.1.1 Ventajas de las redes Inalámbricas

Existen ventajas como menciona (Cisco, 2012) donde la tecnología inalámbrica es un beneficio, estas implican:

- **Accesibilidad**

  Actualmente la tecnología Wifi está integrada en los celulares, televisores, tablets, computadores, dispositivos médicos, entre otros, siendo importante para el uso del internet al estar conectado a red inalámbrica. Desde diferentes puntos de acceso con una cobertura óptima se podrá tener un acceso inalámbrico que permita al usuario tener una conexión segura.

- **Movilidad**

  Proporciona al usuario la agilidad de mantenerse conectado a la red y las herramientas que necesita dando acceso a documentos, aplicaciones, servicios desde cualquier ubicación.

- **Escalabilidad**

  La red inalámbrica con el pasar del tiempo puede adaptarse a los cambios que se ejecutan en el medio físico incluso expandirse con nuevos dispositivos siendo más flexible que una red cableada.

- **Seguridad**

  La red Wifi ofrece estándares que facilita una estabilidad en la red para que la información trasmitida solo se comparta entre los equipos autorizados.

4.1.2 Tipos de redes inalámbricas

La comunicación entre dispositivos inalámbricos es incluida por un intercambio de datos entre los equipos que se están comunicando, por ese motivo no solamente existe la conexión entre dos equipos sino que también pueden existir varios equipos que intervengan en la compartición de datos. Los tipos de redes inalámbricas se pueden dividir en cuatros tipos según sus características, donde una de ella es el entorno geográfico el cual se utiliza la señal y el servicio. La figura 3 muestra sobres los tipos de redes inalámbricas.

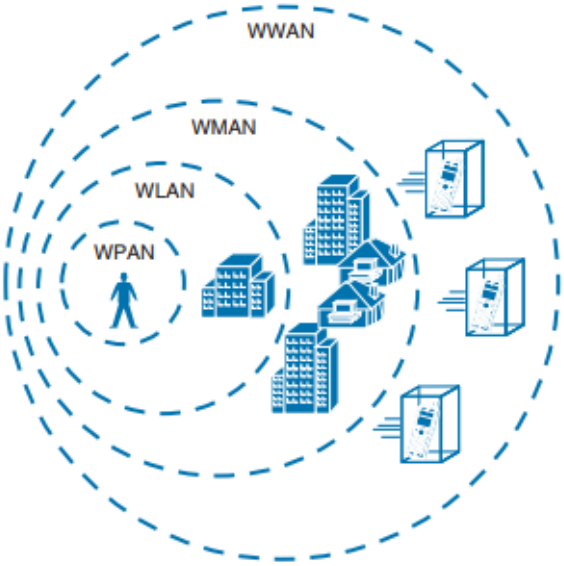


Figura 3 Tipos De Redes Inalámbricas

Fuente: (Hucaby, 2014)

4.1.2.1 Redes Inalámbricas de Área Personal

De acuerdo a (Hucaby, 2014)

"Las redes Inalámbricas de Área Personal (WPAN) trabaja con señales de baja potencia creando un rango cercano con una cobertura no mayor a 10 metros. Las tecnologías como Bluethooth y Zigbee se especifica como una red Inalámbrica Área Personal empleando el estándar IEEE 802.15 que trabaja en la banda ISM de la frecuencia 2,4 GHz"

4.1.2.2 Redes Inalámbricas Área Local

Según como menciona (Hucaby, 2014):

"Las redes inalámbricas de Área Local (WLAN) permite la interconexión de varios equipos inalámbricos que trabajen en la banda 2,4 y 5GHz empleando el estándar IEEE 802.11 con señales que lleguen a una cobertura de 90 metros aproximadamente"

4.1.2.3 Redes Inalámbricas Área Metropolitana

(Hucaby, 2014) Explica:

"Las redes inalámbricas de área metropolitana (WMAN) cubre en su mayor parte áreas geográficas mayor a la redes WLAN cubriendo un rango total de una ciudad entera utilizando como por ejemplo tecnología Wimax que emplea el estándar IEEE 802.17"

4.2 Estándar IEEE 802

IEEE (Institute of Electrical and Electronic Engineers) es un organismo encargado de los estándares que trabaja dentro de las diferentes tecnologías de las capas física y enlace del modelo OSI, implementado un proyecto llamado IEEE 802 que fue desarrollado en febrero de 1980 con el propósito de elaborar estándares donde exista una norma para las diferentes tecnologías que especifican acerca de LAN (redes área local) y MAN (redes área metropolitana), esto quiere decir que los equipos inalámbricos deberán cumplir con los estándares mencionados para que exista conexiones entre diferentes equipos así sea de diferentes marcas. En la Tabla 1 se detalla las categorías que actualmente existen en el Estándar 802.

Tabla 1 Estándares IEEE 802

Estándar	Tecnologías
802.1	Bridges MAC
802.3	Ethernet
802.11	Wifi
802.15	Bluetooth, Zigbee
802.17	Wimax
802.19	TV White Space Coexistence Methods
802.21	Mecanismos de servicios HandOver
802.22	Wireless Regional Área Network (WRAN)

Fuente: (IEEE G. P., 2017)

4.2.1 Estándares Redes Inalámbricas

En la actualidad en el ámbito de redes inalámbricas a nivel de área local se emplea un estándar conocido como IEEE 802.11 para las redes Wifi, también existen otras tecnologías más comunes como es la tecnología Bluetooth que usa el estándar 802.15 y la tecnología Wimax con la tecnología 802.17. Existen varios tipos de tecnologías inalámbricas, sin embargo el presente trabajo se basa en el estándar 802.11 que corresponde a la tecnología Wifi.

4.3 Estándares y Organismos Reguladores de tecnología Wifi

4.3.1 Estándar 802.11

La tecnología Wi-Fi en base del estándar 802.11 determina que los dispositivos inalámbricos utilicen los mecanismos establecidos para tener una conexión inalámbrica con otro dispositivo inalámbrico. Existen diferentes características como señales de radiofrecuencia, bandas, canales que trabajan facilitando un enlace inalámbrico robusto. En diferentes dispositivos inalámbricos se encuentran especificaciones técnicas tales como 802.11 a, b, g, n, ac (Hucaby, 2014) . En la tabla 2 se detalla los diferentes estándares entre sí.

Tabla 2 Estándar IEEE 802.11

Estándar	Año	Velocidad Máxima	Frecuencia	Compatible con versiones anteriores
802.11 a	1999	54 Mb/s	5GHz	No
802.11 b	1999	11 Mb/s	2,4 GHz	No
802.11 g	2003	54 Mb/s	2,4 GHz	802.11b
802.11 n	2009	600 Mb/s	2,4 GHz o 5 GHz	802.11a/b/g
802.11 ac	2012	1,3 Gb/s	5 GHz	802.11a/n
802.11 ad	2013	7 Gb/s	60 GHz	802.11 a/b/g/n/ac

Fuente: (Hucaby, 2014)

4.3.2 Wi-Fi Alliance

La Wi-Fi Alliance (Alianza Wifi) certifica los productos Wi-Fi ajustando a normas de redes inalámbricas establecidas por el Estándar 802.1, además la organización Wi-Fi Alliance es dueña de la marca que se la conoce como Wi-Fi, de modo que el logotipo de la compañía es utilizado en todos los equipos inalámbricos de diferentes marcas. (Wi-Fi, 2017)

4.3.3 ITU-R

La Unión Internacional de telecomunicaciones o también conocida como ITU-R cumple una función en las redes Wi-Fi, el cual es poder tener una asignación del espectro de radio frecuencia o RF de manera administrada con el objetivo de realizar diferentes estudios técnicos y evitar que existan interferencias en los diferentes tipos de sistemas de telecomunicaciones. (ITU, 2017)

4.4 Modo Operaciones IEEE 802.11

El Estándar IEEE 802.11 define dos modos de operaciones tales como:

- ✓ Modo AD-hoc (Red Descentralizada):

  Se lo conoce también como topología punto a punto, puesto que es un modo de operación que trabaja con una comunicación directa entre los clientes inalámbricos sin el uso de equipos intermedios de red tales como Access Point, por lo general es usado en espacios pequeños tales como oficinas o en hogares. En redes IEEE 802.11 se la conoce como Conjunto de Servicios Básicos Independientes (IBSS).

- ✓ Modo Infraestructura (Red Centralizada)

Este modo trabaja diferente al modo mencionado anteriormente, donde existe un equipo que permite administrar ya sea un access point o router, en el caso de un equipo cliente se desconecte de la administración del equipo centralizado este perderá comunicación. En redes IEEE 802.11 a esta configuración se la expresa como Conjunto de Servicios Básicos (BSS).

4.5 Vulnerabilidad de la redes

Actualmente en las diferentes empresas al ofrecer internet inalámbrico para los clientes o empleados se debe tener un acceso que garantice rapidez, seguridad y sea fiable al momento de tener un acceso entre los dispositivos inalámbricos, es por eso que es importante tener conocimiento acerca de las amenazas más concurrentes que en un futuro pueden afectar a la red inalámbrica. Existen muchas vulnerabilidades como una de ellas es tener una clave predeterminada, el cual un atacante con diferentes métodos de hackeo descifre la clave. Existen ataques a redes alámbricas y para redes inalámbricas no es la excepción puesto que ocasiona diversos problemas a la red y al usuario, modificando datos importantes en los equipos o provocando daños de software mediante virus o diferentes amenazas.

Las amenazas más conocidas según (Duarte, 2012)

- **Virus:** Son programas que alteran el funcionamiento de un programa, provocan daños en archivos personales o del propio sistema operativo.

- **Caballo de Troya (Trojan horse):** Es un programa que trabaja normalmente como cualquier otro programa pero ejecuta procesos peligrosos en segundo plano ocasionando robo de información sin ser detectado por cualquier mecanismo de seguridad.

- **Gusano:** Impide el trabajo al usuario ocasionando lentitud del sistema operativo, perdidas de información, a diferencia del virus el gusano se difunde entre los dispositivos conectados en la red.

- **SQL injection:** Este ataque puede producirse mediante ataque a portales cautivos mediante infiltración de programación maliciosa con el objetivo de manipular la base de datos de los usuarios que se autentican.

- **Phishing:** También conocida como Ingeniería Social, se trata de una persona externa de la red con el propósito de obtener información usando diferentes medios de comunicación que puede ser utilizado para producir el ataque, siendo información proporcionada de parte del mismo personal de la empresa.

- **Denegación de servicio (Denial-of-service):** Se lo conoce como ataque DOS, siendo un ataque destinado a los servidores de una empresa con el propósito de colapsar los procesos del servidor e impida trabajar normalmente.

- **Ataque del día cero (Zero-day exploit):** Este ataque es provocado por hackers que sacan ventaja de una vulnerabilidad ocasionada por una nueva actualización sea aplicaciones o sistema operativo, siendo desconocida por parte del usuario y el fabricante de software.

4.6 Mecanismo de Seguridad Wifi

En la actualidad con el avance de la tecnología y nuevos métodos de ataques, las redes inalámbricas son más vulnerables que las redes cableadas debido al uso del espacio libre como medio de trasmisión siendo compartido por cualquier

dispositivo, por eso es recomendable utilizar mecanismos de seguridad al momento de diseñar una red Wifi.

Uno de los mecanismos de seguridad incorporado en la red IEEE 802.11 es el proceso de autenticación según el tipo de seguridad de red inalámbrica que trabaja en la capa 2 del modelo OSI siendo importante para el proceso donde el equipo inalámbrico se identifica en la red, existen 2 tipos de autenticación:

- **Autenticación de sistema abierto**: La conexión será demasiado sencilla para los usuarios que dispongan de dispositivos inalámbricos, siendo usado este tipo de autenticación solo en circunstancias donde exista inconvenientes con la seguridad de la información de la red, esto podría ser en casos particulares como redes que otorguen acceso gratuito para clientes como hoteles, hospitales, centros comerciales.

- **Autenticación mediante clave compartida:** Este tipo de autenticación usan mecanismos de seguridad conocidos como WEP, WPA o WPA2 donde el cliente y el dispositivo inalámbrico que otorga servicio podrá conectarse mediante una clave y un cifrado de datos seguro. (Hucaby, 2014)

4.6.1 Protocolo WEP

Es un protocolo de seguridad obsoleto para una red inalámbrica al no ofrecer una garantía de seguridad en ninguna de las fases de autenticación, confidencialidad e integridad. La autenticación abierta entre el cliente y un access point no es segura, como solución se implementó en el año 1999 el protocolo WEP (Wired Equivalent Privacy) siendo uno de los primeros protocolos que serviría para encriptación logrando una conexión segura como era la conexión por cable. El Protocolo WEP utiliza algoritmo de cifrado RC4 para cifrar los datos con una clave secreta y el

mecanismo CRC-32 para integrar los datos que se trasmiten en la capa de enlace de datos que corresponde a la segunda capa del modelo OSI. (Hakima Chaouchi, 2007)

4.6.2 Protocolo WPA

WPA, fue la mejoría del Protocolo WEP, siendo el segundo protocolo de encriptación para las redes inalámbricas en base al estándar IEEE 802.11i del año 2003 logrando una conexión segura de diferentes equipos inalámbricos. El Protocolo WPA tiene dos maneras que sirve como servidor de autenticación la cual se la conoce como Modo Empresarial y Modo Personal.

- **Modo Enterprise:** Este modo es utilizado para empresas que cuentan con un gran número de usuarios y necesiten una administración centralizada del acceso para realizar procesos como autentificación, autorización y contabilidad aplicados en un servidor AAA como Radius.

- **Modo Personal:** Este modo es más simple utilizar, siendo implementado para redes pequeñas que utilizan una clave pre-compartida (PSK) por el administrador de la red y es proporcionada en los equipos clientes y Access Point. La seguridad depende de lo complejo y extensa sea la clave. (Hakima Chaouchi, 2007)

4.6.3 Protocolo WPA2

El protocolo WPA2 se creó para ratificar al protocolo 802.11i completo el cual logro ser un protocolo seguro con una versión certificada, por la importancia que tenía el protocolo 802.11i, Wi-Fi Alliance decidió nombrar al nuevo protocolo como WPA2. El protocolo WPA2 tiene algunas diferencias en ciertas características

como los tipos de cifrado el cual el actual protocolo usa cifrado AES mientras el anterior protocolo usaba cifrado TKIP.

4.6.3.1 Debilidad de WPA2

En Octubre 2017 el protocolo más seguro había sido hackeado por un ataque llamado Krack provocando que diferentes dispositivos inalámbricos puedan ser vulnerables y que la información que se trasmite con los Access Point sea manipulada siendo una vulnerabilidad critica. Este nuevo ataque se implementaba en código abierto ejecutándose en Sistemas Operativos tales como Linux, Android y OpenBSD. El ataque fue grave porque el protocolo WPA2 es utilizado en todos los dispositivos inalámbricos que tienen conexión a internet.

4.6.3.2 Solución al ataque WPA2

Al momento del ataque muchos equipos inalámbricos se consideraron desprotegidos al estar conectado en una red inalámbrica con seguridad WPA2, por tal motivo se pensaba que llegaba el fin del protocolo pero existían maneras de aún poder proteger los datos que se trasmiten inalámbricamente.

Según el experto (Serrano, 2017) en el tema de CiberSeguridad indico los siguientes puntos a tomar en cuenta para que el equipo inalámbrico no sea atacado.

- **Actualizaciones:**

  Al momento del ataque varias compañías que están relacionadas a equipos de redes inalámbricas lanzaron nuevos parches de seguridad para que la brecha del ataque sea cerrada, como por ejemplo una de las primeras empresas que lanzo los parches fue Microsoft para el Sistema Operativo

Windows 7,8 y 10 que aun cuenta con soporte técnico. Así mismo con el pasar de los días diferentes empresas se sumaron con nuevas actualizaciones para que diferentes equipos como celulares instalados con sistema Operativo Windows Phone, Ios y Android realicen la respectiva actualización.

- **Navegación segura:**

Enrique Serrano explica que otro método es el uso de encriptación en aplicaciones que cifran la información de extremo a extremo para así poder proteger los datos ya que los atacantes pueden desencriptar el protocolo WPA2 pero el cifrado de datos aun no es vulnerable. Una de la ventajas es que la aplicación popular de mensajería instantánea como whatsapp cumple con este método de encriptación y es utilizado por la mayor parte de los usuarios, así como WhatsApp trabaja con un método de encriptación también existen diferentes páginas web que ya el usan el protocolo HTTPS el cual es un protocolo seguro de transferencia hipertexto que utiliza un cifrado seguro basado en SSL/TLS, impidiendo que la información confidencial del usuario no sea manipulada por el atacante.

- **Cable de datos y paquete móvil:**

Una de las últimas opciones que Enrique Serrano menciona y que muy pocos usuarios usarían seria el uso de cable Ethernet a la PC y de los datos móviles en vez de la tecnología Wi-Fi.

4.6.6 Cifrado de Datos

Los protocolos de cifrado proporcionan de manera segura la información que se trasmite entre equipos inalámbricos y así evitar que la información sea descifrada

por un atacante. Los diferentes métodos de autenticación tanto WPA y WPA2 usan métodos de cifrados pueden generar una clave para las conexiones de los equipos

- **TKIP (Temporal Key Integrity Protocol)**

  Es un protocolo de encriptación antiguo aplicado junto a WPA para cifrar los datos de las redes inalámbricas. Actualmente no es un protocolo utilizado en los mecanismos de seguridad puesto que es obsoleto y con la creación de WPA2 perdió credibilidad. (Cisco Networking Academy, 2016).

- **AES (Estándar Cifrado Avanzado)**

  Con la creación del mecanismo WPA2 se evidenció la necesidad de reemplazar el antiguo método cifrado TKIP, por lo cual se creó el método AES basado en el estándar IEEE 802.11i siendo un método de cifrado más confiable y seguro. (Cisco Networking Academy, 2016).

4.6.7 802.1X

IEEE para administrar el acceso de redes inalámbricas implemento el estándar 802.1x utilizando certificados digitales para el acceso a la red a los usuarios. El proceso de autenticación y autorización trabaja de manera conjunta con el cliente, el punto de acceso y el servidor de autenticación. Cuando el cliente se conecta a la WLAN se le otorga un certificado digital al autenticarse y navegue en internet mediante la red inalámbrica. (GrandStream, 2015)

El protocolo 802.1x trabaja con un servidor RADIUS que sirve para autenticar los equipos inalámbricos y mediante el estándar 802.1x usa un protocolo extensible. La Figura 4 se muestra el proceso de operación que realiza el protocolo.

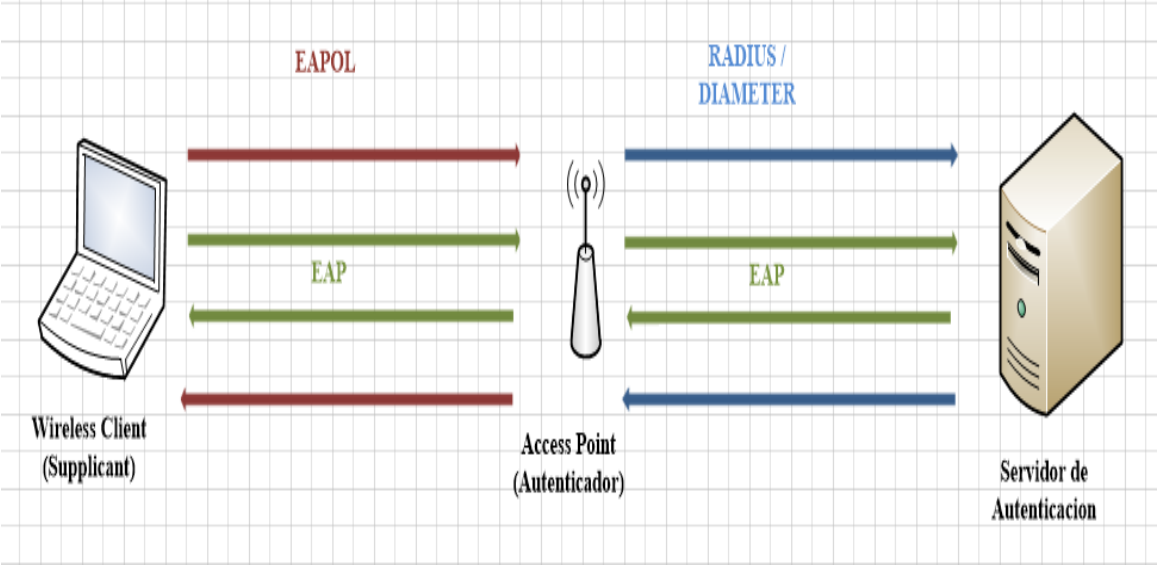


Figura 4 Proceso autenticación 802.1x

Fuente: (GrandStream, 2015)

El protocolo 802.1X cuenta con elementos que permiten realizar el proceso de autenticación, siendo el Suplicante (Cliente), Autenticador (Punto de acceso) y finalmente el Servidor de Autenticación como el servidor Radius o Diameter. El proceso del protocolo 802.1x como menciona (GrandStream, 2015) es:

- El proceso comienza cuando el cliente se conecta a la red inalámbrica e intenta autenticarse enviando un mensaje EAP.

- Estos mensajes se envían al Access Point siendo encapsulados por EAP (EAPOL).

- El Access Point al ser el autenticado este obtiene la solicitud del cliente con las respectivas credenciales.

- El Servidor de autenticación solicita las credenciales del cliente para confirmar si el cliente se encuentra registrado, siendo aprobado o denegado la solicitud para la conexión.

- Si el cliente fue aceptado, el Access Point modifica el puerto virtual a un estado autorizado que permite la conexión a la red

El método de autenticación EAP contiene varias variantes que son utilizadas en las redes inalámbricas, como se menciona en (Intel, 2017), estos pueden ser:

- ✓ **EAP-LEAP:** Es un Protocolo Ligero de Autenticación Extensible fabricado por la marca Cisco Systems, el cual trabaja con una autentificación parecida al protocolo WEP.

- ✓ **EAP-TLS: (**Seguridad de la Capa de Transporte) Este estándar es basado en certificados digitales en el lado cliente y servidor logrando ser un sistema de autenticación en la capa de transporte muy fuerte donde se utiliza túneles TLS encriptado.

- ✓ **EAP-TTLS** Es un protocolo nombrado Seguridad de la Capa de Transporte Tunelizada basándose en una mejoría de EAP TLS al no requerir certificados digital en el lado cliente sino en el lado servidor, en el cliente se utiliza cualquier método de autenticación siendo CHAP, PAP, MS-CHAP, EAP.

- ✓ **EAP-PEAP:** Es un Protocolo de Autenticación Extensible Protegido siendo creado recientemente, el cual es muy similar a EAP-TTLS donde no se requiere un certificado en extremo cliente. EAP-PEAP a diferencia de los demás tiene implementación de parte de CISCO y MICROSOFT logrando

que de igual manera a EAP-TLS solo necesite certificado en el lado servidor, abasteciendo a EAP antiguos. PEAP solo permite algunos métodos de autenticación como MS-CHAPv2 mediante el túnel TLS.

4.7 Sistema de Autenticación

El sistema de autenticación conocido como Protocolo AAA por sus siglas como Autenticación, Autorización y Auditoria, corresponde a una familia de protocolos que realizan las funciones mencionadas anteriormente , el cual permite tener un control de acceso en una red alámbrica e inalámbrica para tener una conexión segura en los usuarios conectados.

Para poder entender las funciones que cumple cada servicio, se hace una breve explicación según un artículo de la revista RedUsers. (RedUsers, 2013).

- **Autenticación:** En este proceso cuando un usuario está en el rango de cobertura de la red inalámbrica y se conecta al Access Point, deberá ingresar las credenciales según el mecanismo implementado, al hacer este proceso de conexión se valida al usuario y si es correcto se procede a la conexión entre los dos equipos inalámbricos.

- **Autorización:** En este proceso se refiere a los permisos otorgados por el servidor de autenticación que tendrá el usuario al conectarse a la red inalámbrica, siendo establecidos los privilegios que tendrá el usuario autenticado tales como el tipo de conexión, ancho de banda, límite de tiempo, asignación de calidad de servicio entre otros, en el caso de existir problemas, se rechaza el acceso.

- **Contabilización:** Al estar autenticado el usuario a una red tendrá un registro en el servidor de autenticación, tales como Radius, Diameter, Tacacs donde se realiza un seguimiento correcto de todos los datos del usuario.

4.8 Servidor Radius

Radius (Remote Authentication Dial In User Service) es un protocolo de autenticación que trabaja como cliente-servidor utilizando puertos 1812 en Protocolo UDP siendo el más utilizado como implementación AAA para usuarios que se conectan a una red inalámbrica. Fue implementado por la empresa Livingston Enterprise siendo publicado en el año 1997 en RFC2865 y RFC 2866.

Cuando un usuario ingresa la petición de autenticación, el servidor se encarga de verificar que la información ingresada está registrada, utilizando los diferentes esquemas de autenticación como son PAP, CHAP o EAP. El usuario al ser aceptado, tendrá asignado los recursos de red tales como la dirección IP y puerta de enlace. (Sun Microsystems, 2000)

4.8.1. Elementos de RADIUS

Los elementos básicos que componen un servidor RADIUS son los siguientes:

Protocolo: Define el formato de trama RADIUS usando los puertos; 1812 de autenticación y 1813 de auditoria.

Servidor: Encargado de mantener la información para la autenticación de usuarios y servicios de acceso de red siendo instalado en un ordenador u otra estación de trabajo.

Cliente: Las peticiones de NAS serán producirás cuando el Cliente NAS lo solicite.

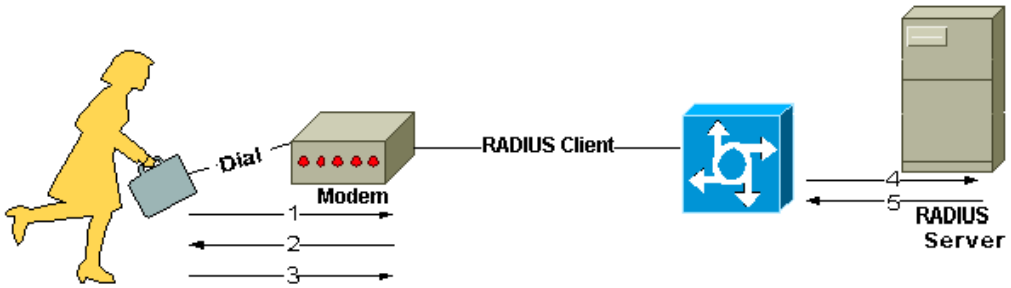


Figura 5 Funcionamiento Radius

Fuente: (Cisco, 2006)

4.9 FreeRADIUS

Alan DeKok y Miquel van Smoorenburg tuvieron la idea de crear un proyecto que pueda ser una alternativa diferente y libre en el ámbito de servidores RADIUS, es por eso que en el año 1999 comenzaron con la implementación del proyecto llamado FreeRADIUS, logrando actualmente ser un servidor ligero usado para administración de usuarios en diferentes infraestructura tales como redes inalámbricas y alámbricas.

El propósito de la implementación FreeRADIUS es brindar un servidor accesible en su instalación teniendo la facilidad de dar soporte a los diferentes protocolos usados ya sea para base de datos o métodos de autentificación. Actualmente el proyecto incorpora bases de datos conocidas como LDAP, SQL que permite una administración correcta de usuarios y organizada para la autenticación, usando autenticaciones como EAP, EAP-TTLS y PEAP. FreeRadius trabaja en diferentes sistemas Operativos siendo estos: Linux (Debian, Ubuntu, Suse, Mandriva, Fedora Core, etc.), FreeBSD, MacOS, OpenBSD, Solaris, e incluso MS Windows por medio de cygwin. (FreeRadius, 2017)

4.9.1 Ficheros FreeRadius

El fichero “radiusd.conf” es un archivo del servidor radius donde se encuentra la información principal del servidor sea ficheros de log, parámetros de uso máximo, usuarios, grupos, también se encuentra ficheros que se utiliza para que el usuario pueda autenticarse y ser autorizado siendo estos las bases de datos como SQL, LDAP.

Tabla 3 Descripción de Ficheros

Fichero	Descripción
radius.conf	Fichero principal, donde se encuentran especificaciones y directivas del servidor.
eap.conf	Utilizado para configurar el tipo de EAP (extensible authentication Protocol)
users	Fichero donde se crea los usuarios para permitir el acceso.
clients.conf	Tiene la lista de clientes que están autorizados para usar los servicios de AAA proporcionados.

Fuente: (FreeRadius, 2017)

4.10 Hotspot

Un Hotspot o también conocido como portal cautivo es el acceso a internet utilizado en redes inalámbricas o alámbrica, por lo general es aplicado en redes Wi-Fi donde un access point incorpora hotspot conectado a un router de algún ISP que proporcione servicio de internet. Existen hotspot privados instalados en empresas para el personal y hotspot públicos instalados en lugares de mayor influencia de usuarios tales como hoteles, restaurantes, aeropuertos que ofrecen acceso inalámbrico a sus clientes, ya sea en las habitaciones, oficinas o en los pasillos.

El hotspot en lugares públicos se lo puede implementar como un servicio gratuito o pagado según el proveedor de internet. El usuario al intentar conectarse le aparecerá un portal cautivo o pantalla de bienvenida donde le pedirá un inicio de sesión, el inicio de sesión puede ser modo trial que solo deberá aceptar los parámetros que el proveedor indique o mediante una autenticación de usuario y contraseña para acceder a la red y tener navegación. Los portales cautivos se pueden clasificar de diferentes maneras, estos pueden ser mediante software o hardware.

El portal cautivo mediante software puede ser instalado gratuitamente o mediante pago en un servidor físico o máquina virtual según los requisitos técnicos que especifique el fabricante del portal cautivo, y así lograr trabajar adecuadamente. (WifiSafe, 2016)

Existe diferentes herramientas para portal cautivo tales como:

- WifiDog
- FirstSpot
- EasySpot
- OpenSplash
- ChilliSpot

El portal cautivo mediante hardware requiere de un equipo en específico con ciertos requerimientos que permita la administración de usuarios, siendo instalado entre el router de borde y el router de distribución. Al ser equipos de hardware, el portal cautivo viene incorporado con otras herramientas que pueden utilizarse.

Existen marcas que proveen este servicio en los equipos tales como:

- Cisco BBSM-Hotspot
- Nomadix Gatewy
- 4Ipnet Hotspot Gateway
- Mikrotik
- Ruckus

Tabla 4 Comparación de tipos Hotspot

Características	Diferencia	Similitud
Software	• Costo de implementación en Hardware al requerir otros equipos de red. • Costo de licencia en Hotspot de software pudiendo ser gratuito o de pago según la cantidad de usuarios.	• Incorpora interfaz gráfica • Seguridad basada en registros • Estadísticas de uso por usuario • Autenticación centralizada • Políticas por Usuario
Hardware		

Fuente: (WifiSafe, 2016)

4.11 Redes Virtuales (VLANs)

Vlan por sus siglas significa Virtual Local Area Network Red de Area Local siendo un método que se utiliza para segmentar redes LAN en la mayoría de switches. De esta forma se puede agrupar usuarios de la misma red física en diferentes tipos de redes virtuales, los usuarios de una red virtual podrán tener acceso a los recursos de la misma red virtual pero no tendrán acceso con usuarios de otra red virtual. Por lo general como método de seguridad es muy útil al momento de implementar en una red el uso de VLANs, permitiendo a los switches usar el protocolo más común IEEE 802.1Q conocido como dot1q el cual permite a

un dispositivo ser asignado según la etiqueta vlan. (Cisco Networking Academy, 2016)

4.11.1 Tipos Operaciones

Los puertos de un switch tienen dos maneras de operar:

- **Modo Acceso:** Permite la conexión de equipos finales, estos puertos solo trasmiten paquetes que operen con una sola Vlan, conocido como paquetes no etiquetados, a estos puertos se podrían conectar equipos como switches pero no es recomendable al no existir una escalabilidad correcta.

- **Modo Troncal:** Permite la conexión entre equipos de capa 2 como son los switches, permitiendo trasmitir los paquetes etiquetados con la agrupación de varias redes virtuales a un único enlace físico.

4.12 Firewall

En una red como mecanismo de seguridad debe existir un dispositivo de seguridad que se lo conoce como firewall, el cual permite monitorear y bloquear mediante reglas el tráfico origen y destino de una red, por lo general el firewall se utiliza como defensa perimetral de una red ubicándose entre el router de borde y la red externa siendo por lo general el internet.

Normalmente, un firewall se implementa según las políticas de seguridad de la empresa para realizar bloqueos a usuarios externos no autorizados evitando el robo de información, también este tipo de dispositivo se utiliza como medida de

protección con algunas reglas en la misma LAN para bloquear el tráfico saliente o entrante.

4.12.1 Firewall Mikrotik

Existen diferentes proveedores de hardware como Cisco, HP, Mikrotik que en los equipos de redes incorporan un firewall, es por eso que Mikrotik no es la excepción. El firewall de Mikrotik utiliza un sistema de seguridad que permite proteger al equipo y a la red de diferentes tipos de ataques sean provenientes de internet, análisis de puertos, acceso no autorizado o cualquier otro ataque sospechoso. Para comunicación entre router de diferentes redes, el firewall de Mikrotik puede cumplir funciones de ruteo configurado con servicios túneles VPN para una trasmisión de datos segura entre redes. (Mikrotik Documentation, 2017)

Existen 2 reglas comunes que son utilizadas en el firewall de MikroTik:

- **The matcher**: Las condiciones realizadas deben ser verificadas según los parámetros establecidos.

  Los parámetros que son analizados y comparados son:

  - Dirección MAC Origen.
  - Direcciones IP (network o list) y dirección tipo (broadcast, local, multicast, unicast).
  - Puerto o rango de puertos.
  - Opción de protocolos (tipo ICMP, campos de código, banderas TCP, opciones de ip).
  - Interface de salida y entrada del paquete.

- **The action**: Establece las condiciones y parámetros para ejecutar las acciones.

4.13 Mikrotik

En el año 1996 la marca Mikrotik fue fundada por Arnis Riekstins y Jhon Tully en la ciudad de Riga capital de Latvia, desde un principio la idea fue como proyecto de grado para la universidad, con el objetivo de elaborar un router basado en Linux con las mismas características que en ese entonces existía con routers de otras marcas. Con el pasar de los años dicho proyecto se convirtió en algo empresarial implementando routers y sistemas Wireless para proveedores de Internet (ISP). El sistema operativo Router OS, es un sistema estable y flexible para varias funcionalidades tales como firewall, Wireless, calidad de servicio, ruteo operando al siguiente año de haber comenzado la tesis.

. La compañía oficialmente se llama Mikrotikls Ltd pero por motivos comerciales se lo conoce internacionalmente como Mikrotik. Aparte de dar diferentes servicios también provee diferentes equipos y software para el mercado de telecomunicaciones. En algunos equipos también ofrece un sistema llamado SwOs que se enfoca en switches y para router conocidos como routerboards llamando al sistema operativo como RouterOS (Mikrotik, 2017). Actualmente Mikrotik compite con empresas conocidas mundialmente en el área de Networking tales como Cisco, D-Link, 3Com teniendo una ventaja por su precio accesible para diferentes usuarios.

4.13.1 RouterOS

El sistema operativo RouterOS funciona en una placa Mikrotik fabricado por la misma empresa e integrado en los diferentes equipos, la ventaja de Mikrotik también es que ofrece instalación de su sistema operativo en una PC como se realiza en el presente proyecto. El sistema operativo

RouterOS es basado en GNU/Linux ofreciendo servicios útiles para los ISP o administradores de redes como firewall, enrutamiento, wireless, calidad de servicio, etc. Se puede conocer más acerca del sistema gracias a que Mikrotik cuenta con su propia página de foro y una wiki donde detalla las diferentes funcionalidades de cada servicio, siendo útil y excelente aporte para los usuarios de networking.

RouterOS es obligado a lanzar nuevas versiones de diferentes servicios por su rápido crecimiento a lo largo de los años, actualmente Mikrotik cuenta con la versión 6.41 desde el 2013 que se implementó la v6.

4.13.2 Winbox

Mikrotik cuenta con una herramienta gráfica muy útil que permite gestionar un equipo Mikrotik conocida como WinBox, este programa puede funcionar en diferentes sistemas operativos conocidos como Windows, Linux, MAC. El ejecutable de instalación es descargado desde la página oficial de Mikrotik, una vez descargado se puede acceder a cualquier equipo Mikrotik solo con una dirección IP o mediante MAC (capa2) como se muestra en la Figura 6. (Mikrotik Documentation, 2017)

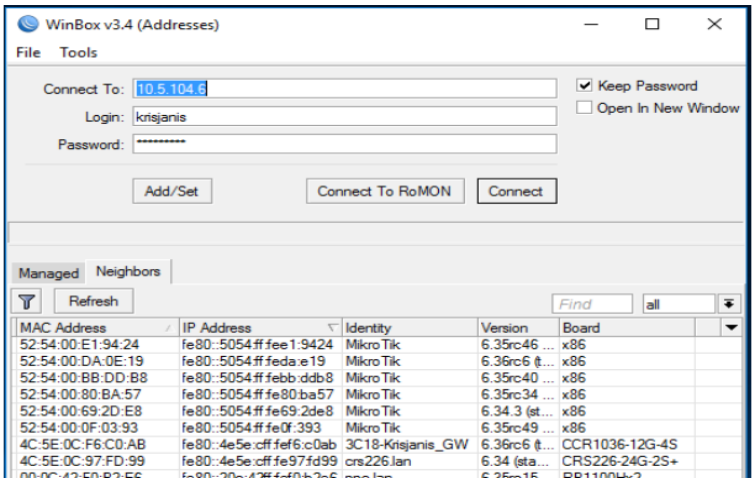


Figura 6 Winbox

Fuente: (Mikrotik Documentation, 2017)

4.13.3 Licenciamiento

En diferentes marcas se requiere licencia para una correcta activación y funcionalidad en los propios sistemas operativos, por eso Mikrotik cuenta con bajos costos en los diferentes niveles de licencia según el uso. Al efectuar la compra de un equipo, la licencia se encuentra incorporada pero en casos como la implementación en un CPU se requiere realizar la adquisición de la licencia. La compra de la licencia es original y nunca expiran siendo de un solo uso, permitiendo solo una vez la activación en cualquier equipo. (Mikrotik Documentation, 2015). Existen diferentes niveles de licencia como se explica en la Tabla 5, el precio de cada licencia puede variar.

Tabla 5 Característica Niveles Licencia

Nivel	**0**	**1**	**3**	**4**	**5**	**6**
Precio	No requiere	Registro	Depende Volumen	$ 45	$ 95	$ 250
Wireless AP	24h Gratis	-	-	Si	Si	Si
Interfaz Vlan	24h Gratis	1	Ilimitado	Ilimitado	Ilimitado	Ilimitado
Hotspot Activos	24h Gratis	1	1	200	500	Ilimitado
Cliente Radius	24h Gratis	-	Si	Si	Si	Si
User Manager Sesiones	24h Gratis	1	10	20	50	Ilimitado
Queues	24h Gratis	1	Ilimitado	Ilimitado	Ilimitado	Ilimitado

Fuente: (Mikrotik Documentation, 2015)

4.14 Distribución de Canales para Red Wifi

La saturación en el espectro radioeléctrico es provocada por el exceso del tráfico de trasmisión de los diferentes dispositivos inalámbricos conectados en una red Wifi. Esto ocasiona también una lentitud en la red pero al existir tecnologías tales

como b, g, n y usar la frecuencia correcta, los dispositivos conectados se adaptan a la velocidad soportada para poder tener una comunicación exitosa. La tecnología Wifi trabaja en la banda de 2.4Ghz que dispone de 11 canales separados por 5Mhz, por otro lado en la banda de 5Ghz al ser una nueva frecuencia los canales no están saturados, la única desventaja es que tiene un alcance menor por el simple hecho que la frecuencia es mayor. En la banda de 2,4Ghz al existir 11 canales existen solapamientos entre ellos, a excepción de tres canales que no existe solapamiento los cuales son 1, 6 y 11. En una red inalámbrica el mayor problema es la interferencia que existe entre los access points y es recomendable que para los access points del mismo rango de cobertura tengan diferentes canales. (HomeTech, 2016)

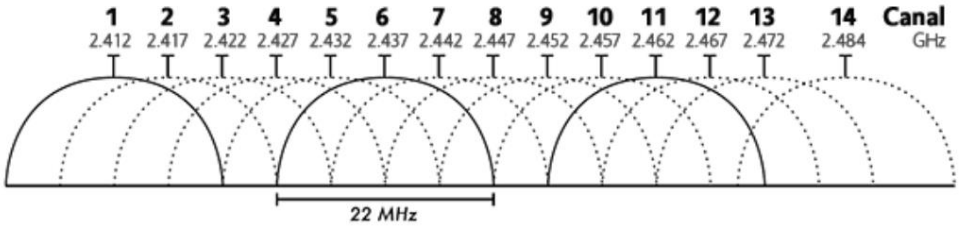


Figura 7 Canales de Wifi

Fuente: (HomeTech, 2016)

En la tabla 6 se muestra el número de canales con la respectiva frecuencia.

Tabla 6 Distribución de canales

Canal	Frecuencia (MHz)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462

Fuente: (Netspotapp, 2018)

4.15 Access Point

El Access Point es un dispositivo inalámbrico que trabaja en capa 2 del modelo OSI, permitiendo acceder a la red según la configuración establecida. Existen Access Point que tienen integrado su propia antena y otros que soportan antenas externas. Los AP (access point) son dispositivos que permiten la conexión inalámbrica de un dispositivo (computadora, tableta, smartphone) con una red. Para el uso de access point en la implementación de red Wifi, existen dos modos de operación:

- **Access Point Autónomo:** Requiere una configuración personalizada e independiente en cada access point instalado en la red.

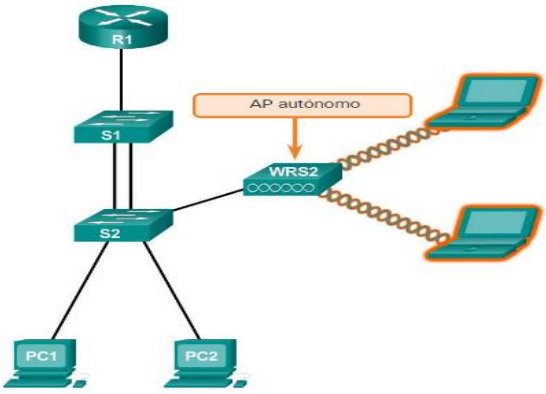


Figura 8 Estructura AP autónomos

Fuente: (Cisco Networking Academy, 2016)

- **Access Point Controlados:** A diferencia del modo autónomo, esta estructura utiliza un protocolo conocido como LWAPP que proporciona al WLC (Wireless LAN Controller) una administración centralizada de los Access Point.

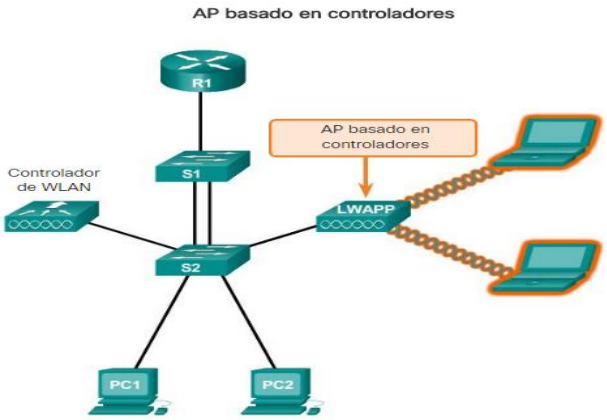


Figura 9 Estructura AP Controlados

Fuente: (Cisco Networking Academy, 2016)

4.17 Controlador Capsman

Mikrotik cuenta en su sistema operativo para redes wireless un controlador de access point que permite la gestión centralizada de todos access point conectados a la red. La única desventaja de este servicio es que solo tendrá el control de todos los access point de marca Mikrotik con tecnología wireless. En Mikrotik a estos equipos administrados por Capsman se los llama como CAP.

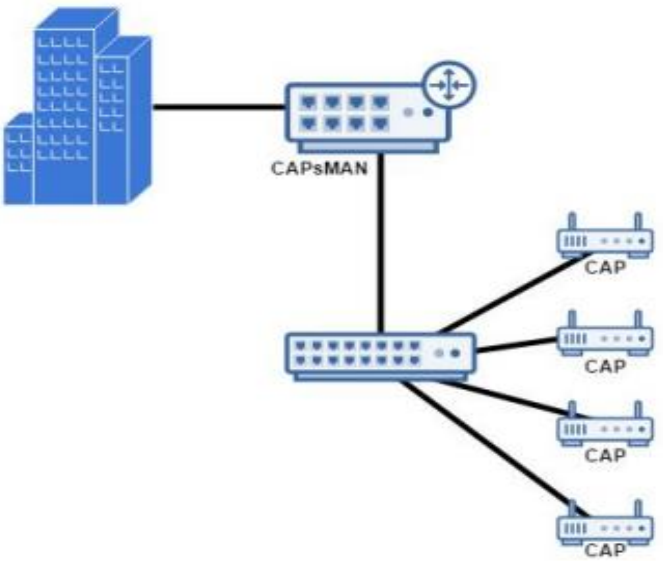


Figura 10 Estructura Capsman

Fuente: (Fassiano, 2015)

Para la gestión de access points por Capsman se debe realizar una serie de pasos para su funcionalidad y conectividad inalámbrica. Existen dos maneras de realizar la conexión del Capsman con el access point ya sea mediante el protocolo MAC o protocolo IP, esta conexión es protegida por DTLS. (Mikrotik Documentation, 2017)

5. MARCO METODOLÓGICO

5.1 Método de investigación

En el presente proyecto se utiliza el método de investigación cualitativo con el propósito de obtener información para conocer las necesidades de la red.

Para la implementación del rediseño de la red inalámbrica, al aplicar diferentes servicios se decidió por este método, al ser considerado un método de investigación que se enfoca al proyecto.

5.1.2 Método cualitativo

El método cualitativo permite la recopilación de información, en base a opiniones y punto de vista de las personas beneficiarias del proyecto que se desea realizar.

Según (Strauss & Corbin, 2002) “El método cualitativo no es un proceso numérico de interpretación de una recolección de información como se lo conoce al método cuantitativo, el método cualitativo es el propósito de interpretar un conjunto de datos obtenidos mediante entrevistas o datos que hayan sido interpretados por método cuantitativo como un informe de algún censo.”

Al usar el método cualitativo se obtiene el problema detallado con mejor exactitud, es por eso que en este proyecto a través de la entrevista proporcionada al Jefe de Sistemas y a la Administradora del centro médico se podra conocer información primordial.

5.1.3 Técnica de recolección de Información

Existen diferentes técnicas de recolección de información tales como: encuestas, observación, entrevistas, cuestionarios, diccionario. Para el presente proyecto se optó por la entrevista, por ser una conversación formal utilizando el formato de preguntas al Jefe de Sistemas y la Administradora de la fundación.

5.1.3.1 Entrevista

La entrevista se la determina como una conversación dirigida entre dos o varias personas, utilizando un formato de preguntas para obtener un resultado especifico.

Según (Dennis Chávez de Paz, 2008) aclara la entrevista como “La entrevista es coincidentemente con el cuestionario como técnicas de encuesta, siendo igual que la investigación científica un método de investigación social para tener en la etapa de recolección de datos un proceso diferente, con el uso de mecanismos como preguntas orales, escritas realizada a personas que participan en el problema.”

A diferencia de otras técnicas, la entrevista es más explícita en el método cualitativo ya que a medida que se van realizando la entrevista se puede realizar diferentes preguntas extras que permitan obtener información más esencial y lograr un análisis específico.

5.1.3.2 Tipo de preguntas

Preguntas abiertas: Son aquellas que se realizan al entrevistado y se obtiene una respuesta que especifica hechos o situaciones con información que son primordial.

Preguntas cerradas: Son aquellas las cuales de parte del entrevistado se obtiene respuestas con número finito siendo estos ninguno, uno o varias.

5.1.3.3 Procesos del análisis de los datos

La recolección de datos que se obtendrá para la implementación del presente proyecto es mediante una entrevista al Jefe de Sistemas y Administradora de la fundación.

Las preguntas que se realizan son de forma abiertas para poder conocer detalladamente los requerimientos, sin necesidad de escoger opciones y lograr respuestas requeridas y expresadas en libertad acerca de los problemas que presentan en la red.

Según (Acevedo Ibáñez, Alba , & López , 1986) para el proceso de una entrevista podemos interpretar lo siguiente:

1. Investigar los cargos las diferentes actividades que cumplen los entrevistados en la fundación.

2. Para establecer una organización correcta se debe preparar las preguntas y la información esencial.

3. Se debe establecer un tiempo limitado para la entrevista.

4. El lugar de la entrevista debe ser un lugar donde se pueda hacer la entrevista sin interrupciones.

5. Debe existir una planificación para que exista la reunión con su debida anticipación.

5.1.3.4 Análisis de las Entrevista

- **Análisis Entrevista al Jefe de Sistemas**

Luego de haber realizado la entrevista al Ing. Christian Burgos que ocupa el cargo de Jefe de Sistemas se pudo obtener datos técnicos acerca de la red inalámbrica, en base a las preguntas realizadas como indica el Anexo B, se logró obtener el siguiente resultado:

Según las respuestas obtenidas en la entrevista se pudo determinar que actualmente la red inalámbrica presenta algunos problemas al tener instalado router inalámbricos y al no tener una configuración adecuada en la red existe problemas en el alcance inalámbrico y el control de dispositivos inalámbricos conectados, es por eso que existe una necesidad prioritaria realizar un estudio del alcance que permita a los usuarios acceder a la red inalámbrica.

Para la implementación del proyecto el entrevistado indicó que existe prioridad en el edificio principal de la fundación por ser un área de influencia administrativa y por eso se desea contar con un servicio inalámbrico. Otros de los problemas que se identificó en la entrevista fue que no existe un control de usuarios conectados a la red inalámbrica ya que los usuarios se conectan por una clave única y al no tener control de ancho de banda le impide proporcionar la clave Wifi a todos los usuarios.

Un problema que también presenta es no tener un control de usuarios conectados provocando una complicación en saber que usuario está consumiendo bastante ancho de banda, por lo general se realiza un escaneo de la red con el programa Advanced IP Scanner pero solo se detecta el dispositivo inalámbrico sin poder bloquear al usuario. Al momento del escaneo de la red inalámbrico se encuentran conectados 25 usuarios, determinando que para el acceso inalámbrico según el grupo de usuarios se otorgue permisos con acceso total o acceso limitado en páginas web y ancho banda.

- **Análisis entrevista a la Administradora de la Fundación**

Luego de haber realizado la entrevista a la Ing. Letty Espinel que ocupa el cargo de Administradora del centro médico se pudo obtener información del uso de la red inalámbrica en el personal administrativo, doctores e invitados, obteniendo el siguiente resultado:

Se comprueba que existen problemas en la red inalámbrica para los usuarios al presentar problemas de lentitud por la saturación provocada en el uso de navegación indebida el cual no existe un control de acceso a páginas. Con el objetivo de realizar un control se tomó en cuenta que los doctores usan el internet para consulta de medicamentos y para el grupo de invitados pueden ser visitadores médicos o proveedores que requieren el uso de internet ya sea para

una presentación. Para el grupo de administración solo requieren el uso de whatsApp y por ser horario laboral no necesita otra aplicación.

5.2 Diseño Actual de la Red

En el siguiente diagrama se muestra el diseño lógico de la red actual del edificio en base al diseño del edificio principal de la Fundación Damas del Honorable Cuerpo Consular de Centro Médico Sur.

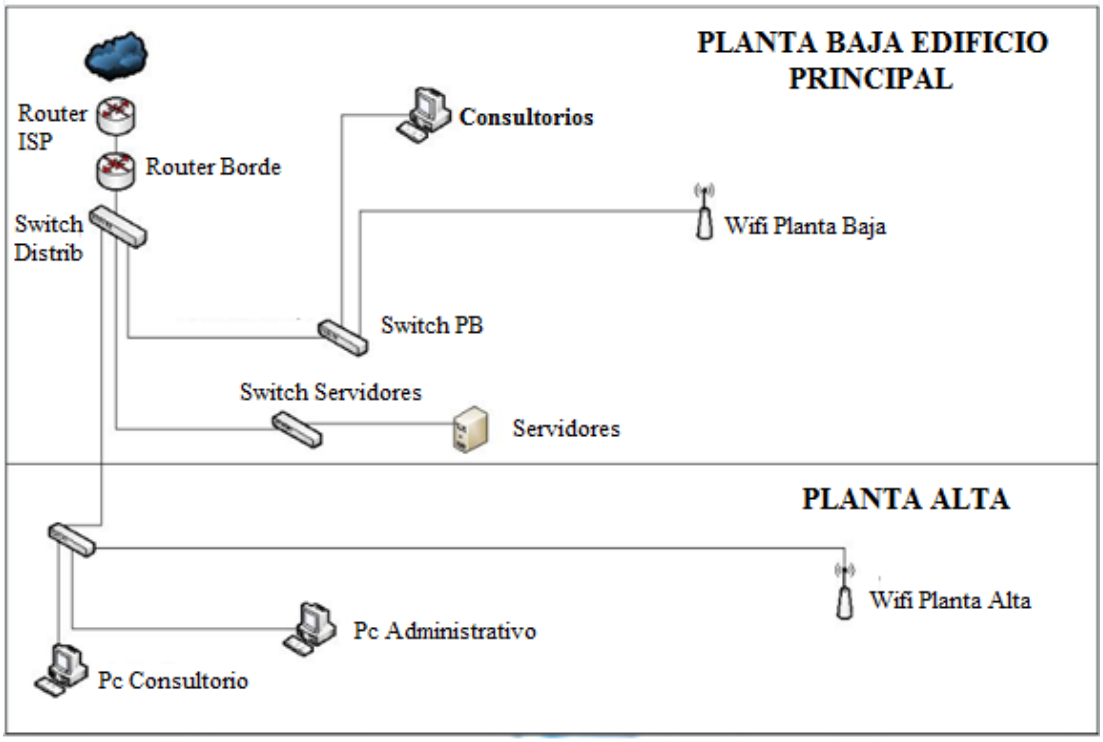


Figura 11: Diseño Lógico de la red

Elaborado por Autor

En base a una topología estrella, la Figura 11 muestra el diseño actual de la red inalámbrica en la planta baja y planta alta del edificio principal donde existe una mayor influencia de usuarios administrativos, doctores e invitados. El router del proveedor de internet se conecta a un router de borde de marca Mikrotik, y este al switch de distribución donde se conecta a los diferentes switches de acceso, para

conectarse a los router inalámbricos, el cual otorga señal inalámbrica a los diferentes usuarios.

La Fundación brinda internet a los usuarios a través de un router inalámbrico instalado en cada piso del edificio principal, el cual posee una infraestructura de seguridad inalámbrica con autenticación WPA2, también el no tener un control centralizado de algunos Access Point y una administración correcta de usuarios conectados, provoca una desorganización y disminución en el ancho de banda.

5.3 Diseño Propuesto de la red

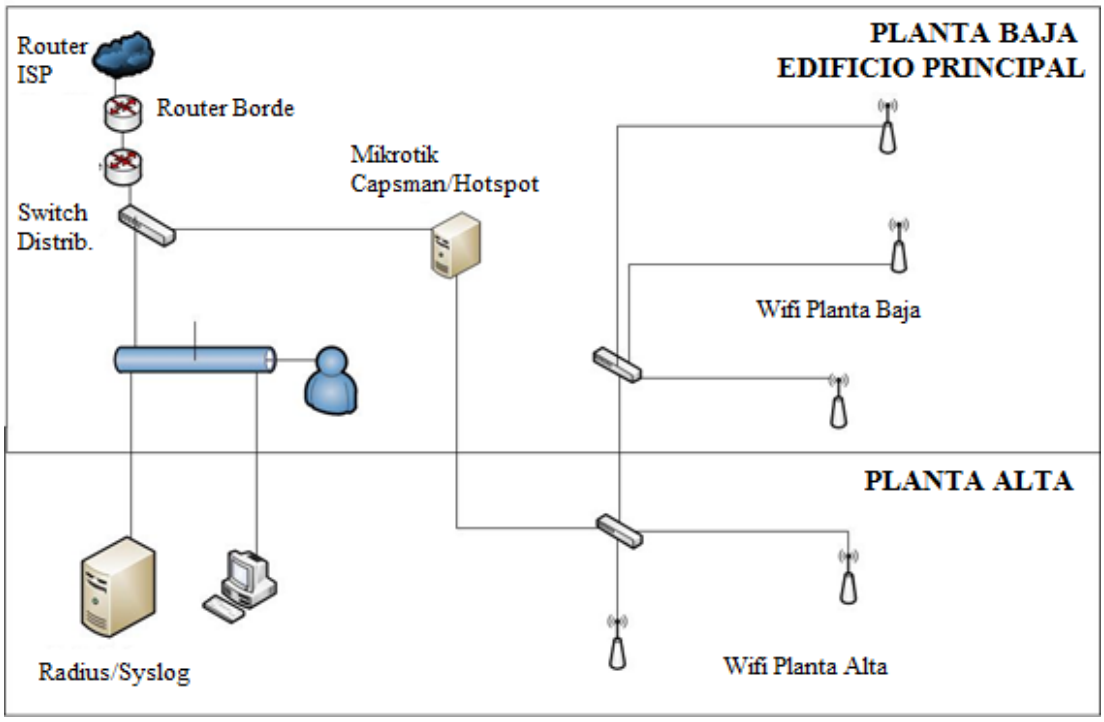


Figura 12 Diseño Lógico propuesto

Elaborado por Autor

El proyecto se realiza en el sistema operativo Mikrotik RouterOS basado en Linux, un sistema que se puede instalar en una maquina física o virtual. El portal cautivo servirá como una página de presentación implementado desde el servicio de hotspot del Mikrotik con un servidor Radius externo que permita una administración de los usuarios conectados a la red inalámbrica. El usuario

autenticado podra acceder a todos los servicios otorgados de internet con normalidad.

El uso del sistema operativo Mikrotik Router OS, no evita que se instalen otros servicios adicionales como firewall que posee funciones de seguridad para establecer reglas de acceso a internet.

Mediante la creación de Vlans se segmenta el tráfico para tener una red escalable y administrable. En el rediseño de la red inalámbrica se tendrá como equipo los access point que cuentan con la característica llamada multi-SSID el cual se asocian a una Vlan específica. En la tabla 7 se detalla brevemente los nombres de las VLANS que se crean.

Tabla 7 Asignación de Vlans con SSID

VLANS	
Vlan 15	Gestión de equipos
SSID con VLAN 16	Administrativo
SSID con VLAN 17	Doctores
SSID con VLAN 18	Invitados

Elaborado por: Autor

Como se detalla en la tabla 7 cada grupo de usuario tendrá acceso a los recursos de la vlan relacionada. El grupo 2 llamado Administrativo solo tendrá los permisos que se otorgue en la vlan 16 y así con las demás vlans. En el servidor de Mikrotik se instala el hotspot que permite el control de ingresos mediante usuarios únicos. Con la implementación del servidor Radius externo se tendrá el registro de los usuarios de administración y el hotspot de Mikrotik hará el respectivo login con los permisos respectivos. En cada Access Point se asocia las vlans que se enlazan con cada SSID creado.

Tabla 8 Tipos de Autenticación en VLANs

SSID	VLAN TAG	TIPO DE AUTENTICACIÓN
Admin_FDHCC	16	RADIUS
Doctores_FDHCC	17	HOTSPOT
Invitados_FDHCC	18	HOTSPOT

Elaborado por: Autor

En la Figura 13 se explica de forma gráfica brevemente lo anteriormente detallado

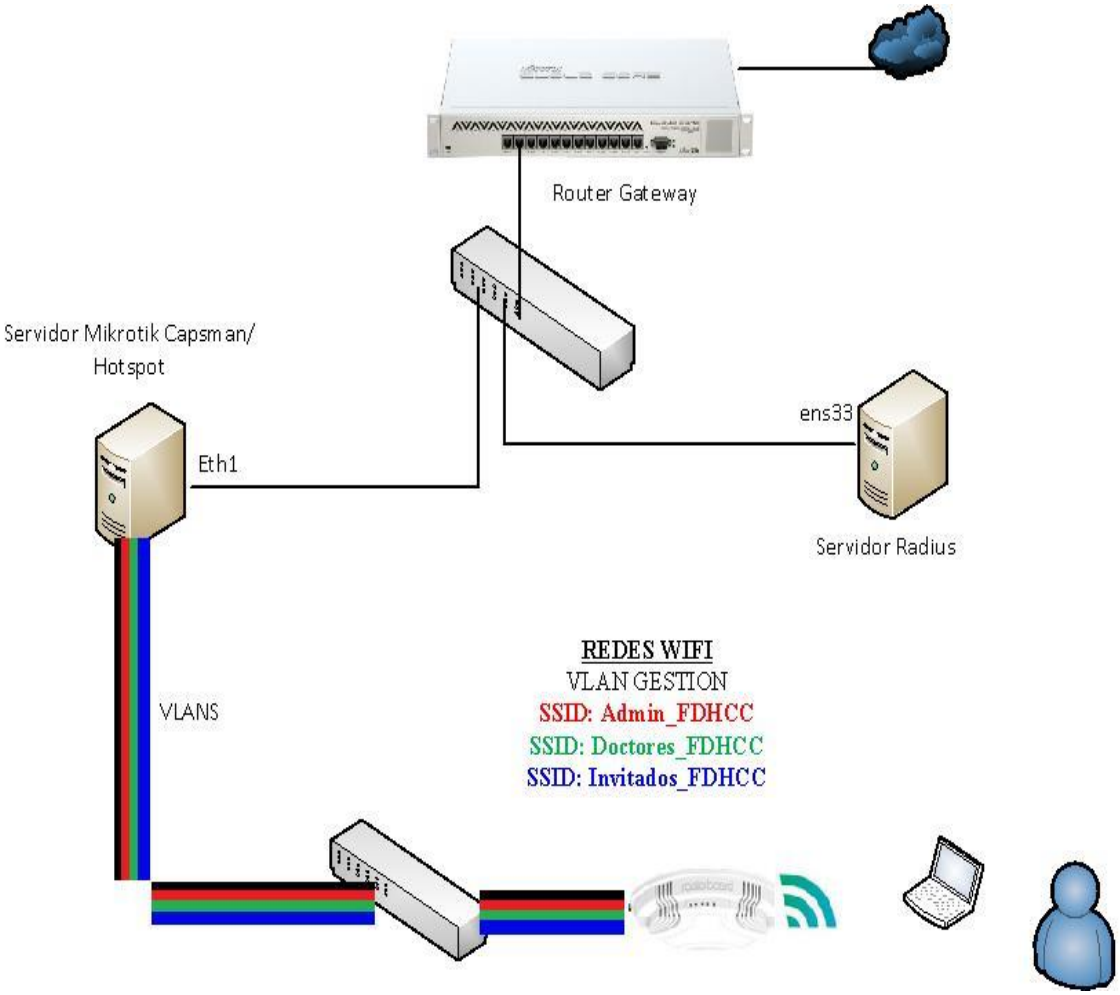


Figura 13 Diseño asignación VLANs

Elaborado: Autor

5.3.1 Esquema de Direccionamiento

Es necesario reservar algunas direcciones IPs de la LAN para asignar al servidor Mikrotik y al servidor Radius. En el análisis realizado del diseño de la red actual, se identificó que la red se encuentra con dirección 10.10.1.0/24 y para la red Wifi es entregada mediante dhcp de cada router una dirección IP 192.168.1.0/24 mediante dhcp.

En la Tabla 9 se detalla las direcciones asignadas para cada equipo en la red.

Tabla 9 Direccionamiento IP

VLAN ID	Dirección IP	Gateway	Usuarios
Vlan Gestión	10.10.15.0/28	10.10.15.1	Access Point, Radius, Capsman
	10.10.15.4-10.10.15.9	10.10.15.1	DHCP
15	10.10.15.2/28		Switch PA
15	10.10.15.3/28		Switch PB
15	10.10.15.10/28	10.10.15.1	CAP1-PB-Cosmetología
15	10.10.15.11/28	10.10.15.1	CAP2-PB-Nutricion
15	10.10.15.12/28	10.10.15.1	CAP3-PB-Sistemas
15	10.10.15.13/28	10.10.15.1	CAP4-PA-Sistemas
15	10.10.15.14/28	10.10.15.1	CAP5-PA-Auditorio
	10.10.1.131/24	10.10.1.111	Servidor Radius
	10.10.1.160/24		Servidor Syslog
Vlan 16	10.10.16.0/26	10.10.17.1	Administración
	10.10.16.2-10.10.16.62	10.10.17.1	DHCP
Vlan 17	10.10.17.0/26	10.10.17.1	Doctores
	10.10.17.2-10.10.17.62	10.10.17.1	DHCP
Vlan 18	10.10.18.1/28	10.10.18.1	Invitados
	10.10.18.2-10.10.18.14	10.10.18.1	DHCP

Elaborado: Autor

5.3.2 Comparación entre Access Point Mikrotik

El proyecto es basado en Mikrotik tanto en el router como en los Access Points, en la Tabla 10 muestra las comparaciones entre los access point según como indica el detalle técnico ubicado en el Anexo C.

Tabla 10 Comparación de Access Point Mikrotik

Descripción	RbCap2nd	RbWap2nd
Estándares Wifi	802.11b / g / n	802.11b / g / n
Usado en Instalaciones	Indoor	Outdoor
Nivel Licencia	4	4
Memoria RAM	64 Mb	64 Mb
Almacenamiento	17 Mb	17 MB
Ganancia Antena (dbi)	2	2
Alimentación	Poe en 802.3af / at	Poe en 802.3 af/t
Temperatura ambiente	-40C a + 70C	-40C a + 70C
Precio	$90	$100

Fuente: (Mikrotik, 2017)

Entre los modelos que se escogió de la marca Mikrotik, se optó por el Access Point Mikrotik RbCap2nd que es adecuado para lugares como hoteles, aeropuertos, hospitales adaptándose a las oficinas del edificio principal de la Fundación Damas Centro Médico Sur. (Mikrotik, 2017)

El RBcap2nd es un access point compacto que se adapta a cualquier ambiente de oficina y es fácil su instalación por su conectividad mediante energía POE (Power Over Ethernet), logrando así poder ser instalado en techo o pared que permite ser administrado por Capsman.

Según el fabricante Mikrotik indica que este equipo tiene una cobertura aproximadamente 40 metros con línea de vista. En la fundación se podría instalar un access point por piso pero se debe tener en cuenta la cantidad de usuarios conectados

y las paredes que obstaculizan la señal, es por eso que se instalan mínimo 2 access point por piso evitando el solapamiento de canales y tomando solo en cuenta a los canales 1, 6, 11 con sus respectivas frecuencias 2412, 2437 y 2462 MHz como indica la Tabla 6.

Los elementos que se utilizan en la red propuesta son:

- Servidor Radius en Distribución Linux Ubuntu 16.04 usando FreeRADIUS, Phpmyadmin, Mysql
- Servidor Mikrotik
  - Controlador Access Point (Capsman)
  - Hotspot
  - Firewall
  - VLANs
  - Calidad de Servicio (Qos)
- Access Point RbCap2nd
  - MultiSsid
  - VLANs
- Servidor Syslog

5.3.3 Análisis de la red Inalámbrica

Para el rediseño de la red inalámbrica es necesario realizar una recolección de información respecto al Wifi, tales como el análisis del espectro y en este proyecto se usa la herramienta propia del Mikrotik que permite conocer los canales y frecuencia utilizados.

Otra información requerida son los posibles obstáculos que provocan la interferencia en la señal, también el tráfico que demanda los usuarios al usar dispositivos inalámbricos.

5.3.3.1 Wireless Snooper

Esta herramienta permite saber el uso de frecuencias utilizados en el rango de cobertura donde se instalan los access point. Se puede ejecutar mediante comandos o interfaz gráfica proporcionando una información más específica tales como mac address del equipo que usa el canal.

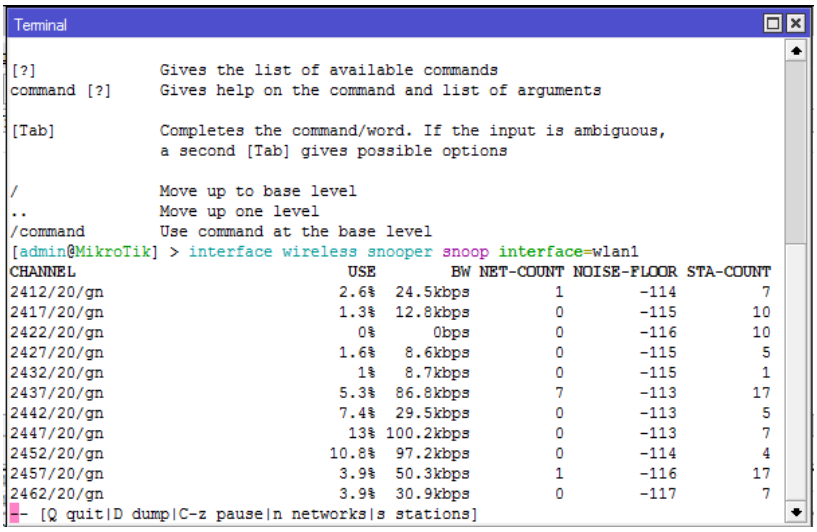


Figura 14 Escaneo wireless comando

Fuente: Winbox Mikrotik

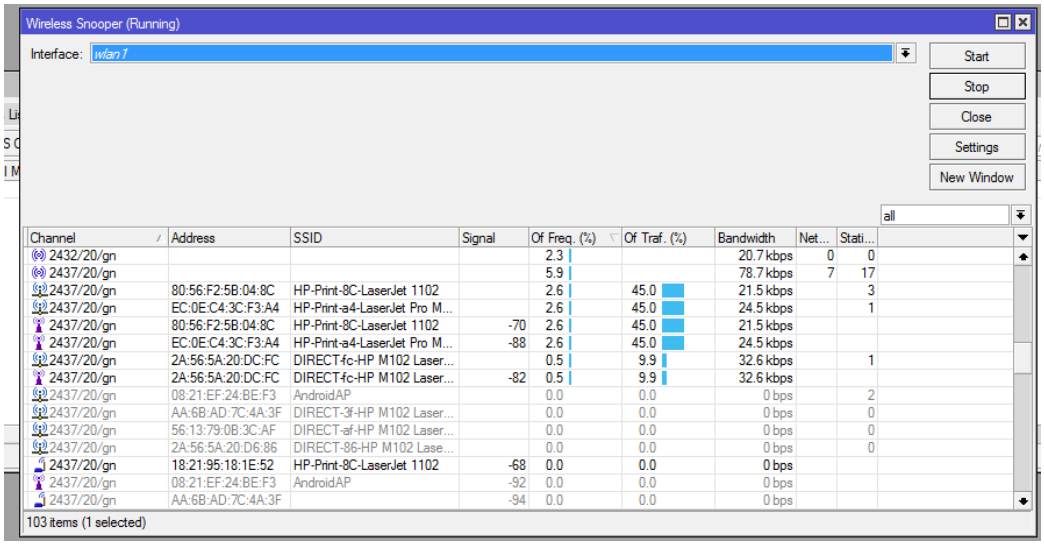


Figura 15 Escaneo Wireless

Fuente: Winbox Mikrotik

5.3.3.2 Análisis de Espectro

Otro método gráfico como escaneo de frecuencia es el comando **spectral-history** el cual escanea todas las frecuencias compatibles con la tarjeta inalámbrica del Mikrotik.

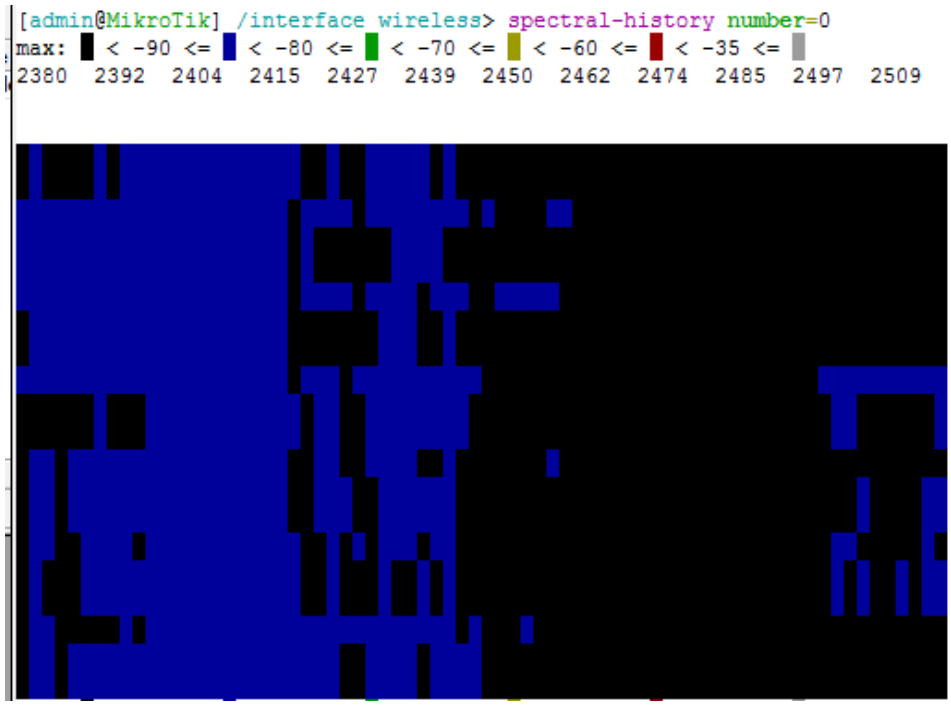


Figura 16 Análisis de Espectro

Fuente: Winbox Mikrotik

5.3.4 Cobertura inalámbrica de los Access Point

Para el rediseño de la red inalámbrica se propone la instalación de los Access point Rbcap2nd en los pisos del edificio principal de la fundación, con el uso del programa de planificación NetSpot se simuló el ambiente físico de la fundación para analizar la cobertura de los access point.

El análisis de cobertura se realizó con el software Netspot en el sistema operativo Windows 8 de una laptop Gateway con tarjeta red Realtek.

Tabla 11 Mac Address de Access Points

Access Point	MAC ADDRESS
CAP1 PB COSMETOLOGIA	64:D1:54:12:62:E2
CAP2 PB NUTRICION	64:D1:54:0C:E7:80
CAP3 PB SISTEMAS 2	64:D1:54:0C:E7:C0
CAP4 PA SISTEMAS 1	64:D1:54:0C:E7:76
CAP5 PA AUDITORIO	64:D1:54:10:AC:5D

Elaborado: Autor

Las señales de potencia inalámbricas se miden en una unidad adimensional dbm con una referencia en vatios o el punto de referencia 0db o 1mw.

Planta Baja Edificio Principal

Figura 17 Cobertura Planta Baja

Fuente: Netspot Pro

Elaborado: Autor

Como se puede observar en la Figura 17, en los pasillos se muestra una potencia cercana a -80 dbm donde la señal de access point será baja, pero en la planta baja se coloca tres access point por ser un área de mayor influencia y se encuentra el área de administración.

Planta Alta Edificio Principal

En la Figura 18 se observa que existe dos access point en la planta alta, debido a que es un espacio de menos influencia pero se optó por colocar un access point en el auditorio donde son las reuniones del centro médico. La señal inalámbrica tendrá una intensidad baja (-81dbm) en el área de la salida de emergencia. En la parte central del piso se podrá conectar también al access point que se encuentra en la planta baja.

Figura 18 Cobertura Planta Alta

Elaborado: Autor

Fuente: Netspot Pro

5.3.5 Conexión de equipos

Para realizar el presente proyecto se configura primero el CPU con los servicios ya definidos tales como dhcp, vlans, bridge para trabajar como router de la red wifi ubicado en la sala de cómputo de la planta alta. Para poder gestionar los access point en el mismo CPU se activa el gestor Capsman con las debidas configuraciones como los datapath que indica el puerto vlan que se usa para la

gestión, los diferentes canales, ssid, security Profile para el ssid admin, roaming. Una vez configurado el gestor Capsman se asigna una dirección IP a los access point en la vlan de gestión y se activa el servicio de cap. Luego para la administración de usuarios se instala el servidor hotspot y también el servidor Radius creando los usuarios en las vlans respectivas, como método de seguridad se optó por usar firewall del Mikrotik , en el firewall se configura opciones como nat, address list, bloqueo de puertos, páginas web, bloqueo de descargas y bloqueo de usuarios mediante la Mac address. Finalmente se realiza la configuración en los switches creando las respectivas vlans y asignando una dirección ip para la gestión de los switches. Una vez configurado los diferentes equipos se realiza las conexiones, primero se conecta el puerto ether1 del CPU a la red LAN de la empresa, y así poder otorgar internet a la red Wifi implementada. Se usa el equipo RB750 que permite trabajar como switch. En el puerto eth2 del servidor Mikrotik se conecta hacia el eth1 del switch que gestiona la planta baja, en el eth3, eth4 y eth5 se conecta los cables del patch panel donde se conectan los Access Point. El puerto eth2 será el puerto troncal hacia el eth1 del switch planta arriba. En el switch de planta alta se usa los puertos eth2, eth3, eth4 para la conexión de los Access point. El servidor radius estará ubicado en otro segmento de red conectándose mediante ether1 del servidor Mikrotik a la red wifi.

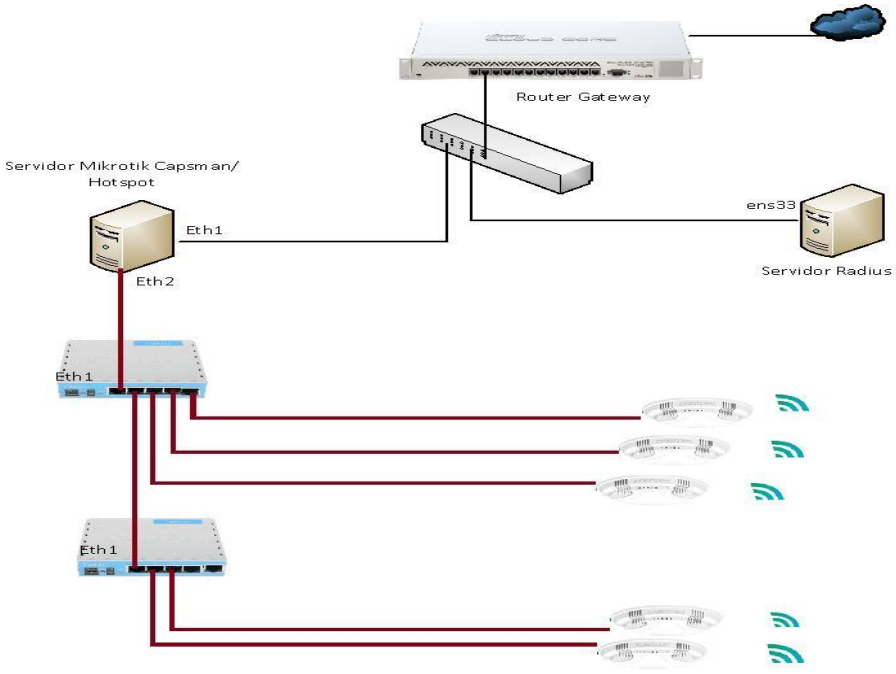


Figura 19 Interconexión de Equipos

Elaborado: Autor

5.4 Configuraciones

5.4.1 Requisitos Mikrotik

Una de las ventajas que se tiene al instalar el sistema operativo de Mikrotik en una PC Intel es la cantidad suficiente de procesamiento que pueda tener en dichas maquinas comparado a un equipo propietario de Mikrotik, Cisco, etc, por eso es recomendable al momento de la instalación del sistema operativo Mikrotik instalar en un disco vacío ya que se formatea cualquier partición que exista en el disco.

Los requisitos mínimos para que se pueda realizar la instalación en una PC son:

- Procesador: Intel x86 100Mhz
- Memoria RAM Mínimo: 64 Mb
- Disco Duro Mínimo: 1Gb
- Unidad de CD-ROM

5.4.2 Instalación Mikrotik Router OS

En la página de Mikrotik en www.mikrotik.com, la pestaña de software se descarga la imagen ISO, se debe tener en cuenta que al instalar en un CPU normal se debe descargar la imagen del grupo x86.

Figura 20 Descarga Imagen ISO

Fuente: (Software, 2018)

Al tener descargado la imagen iso, se empieza a grabar con el programa Rufus en un CD-ROM. Una vez quemada la unidad de CD-ROM con la imagen ISO, se comienza el proceso de instalación detectando el disco primario.

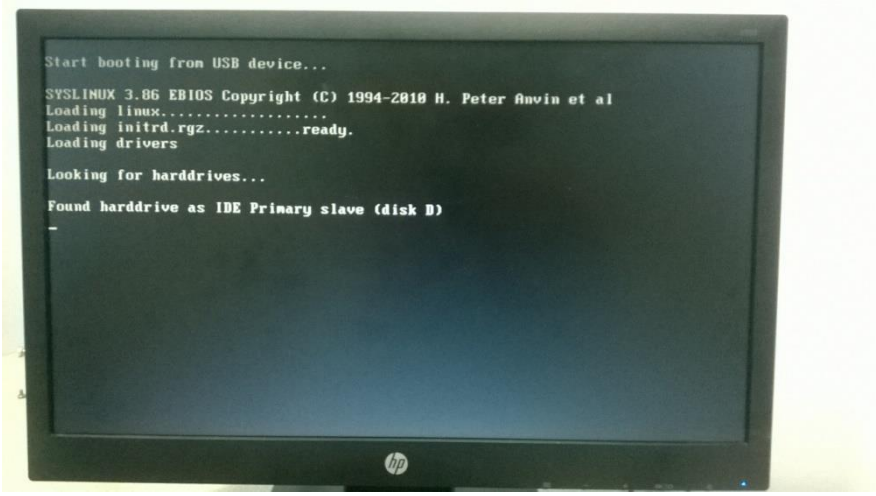


Figura 21 Reconocimiento Imagen Iso

Fuente: Mikrotik Router 6.41

Para el presente proyecto se requiere que el CPU donde se instale el sistema operativo tenga instalado dos tarjetas de red. Una vez que la instalación comienza se muestra la pantalla de todos los servicios el cual con la barra espaciadora se selecciona y con las teclas de flechas se desplaza en los diferentes servicios.

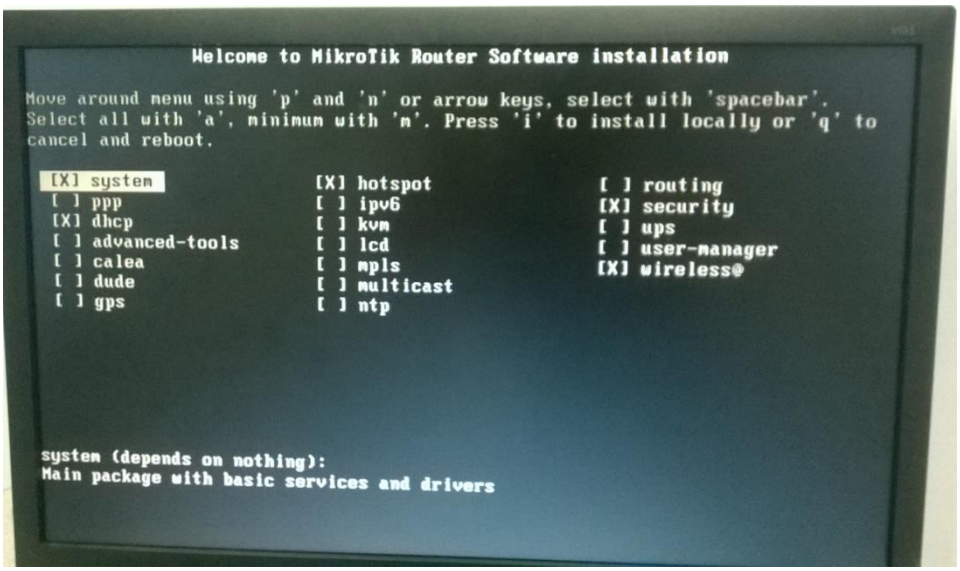


Figura 22 Instalación Servicios

Fuente: Mikrotik Router 6.41

Los servicios que se escogen para este proyecto son system, dhcp, hotspot, security y Wireless, a continuación se detalla algunos de ellos (Mikrotik Documentation, 2016).

- **System**: Contiene los servicios principales del Mikrotik siendo un paquete principal en toda instalación.

- **Ppp**: Contiene soporte para protocolos PPP, PPTP, etc.

- **Dhcp**: Contiene paquetes del Servidor y cliente DHCP.

- **Hotspot**: Instalación del paquete Hotspot.

- **Routing**: Contiene soporte para protocolos RIP, OSPF y BGP4.

- **Security**: Posee una conexión segura para Winbox y contiene protocolos como IPSEC, SSH.

- **User-manager:** Gestión de usuarios del propio Mikrotik con servicios como Radius.

- **Wireless**: En la nueva versión viene incluido en un solo paquete Wireless-cm2 que servirá para instalar CapsMan, Wireless-Rep y Wireless-Fp.

Una vez seleccionado los servicios necesarios se presiona la letra ‘i’ para comenzar la instalación de los paquetes seleccionados. Luego de la instalación se pide un reinicio como se muestra en la Figura 23

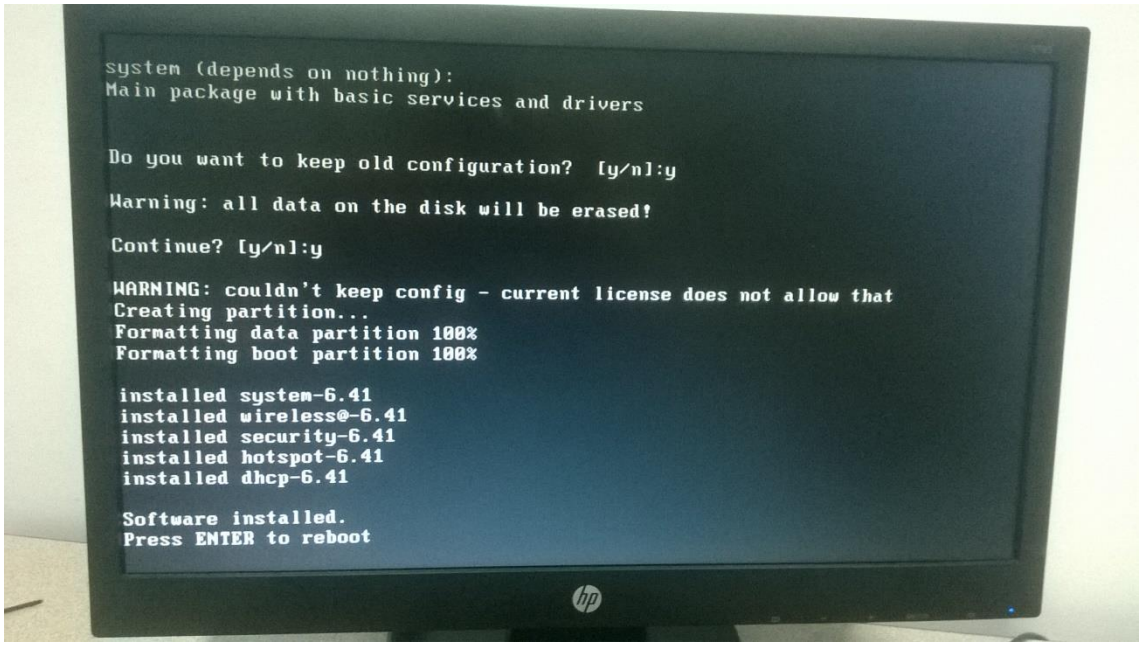


Figura 23 Instalación Mikrotik

Fuente: Mikrotik Router 6.41

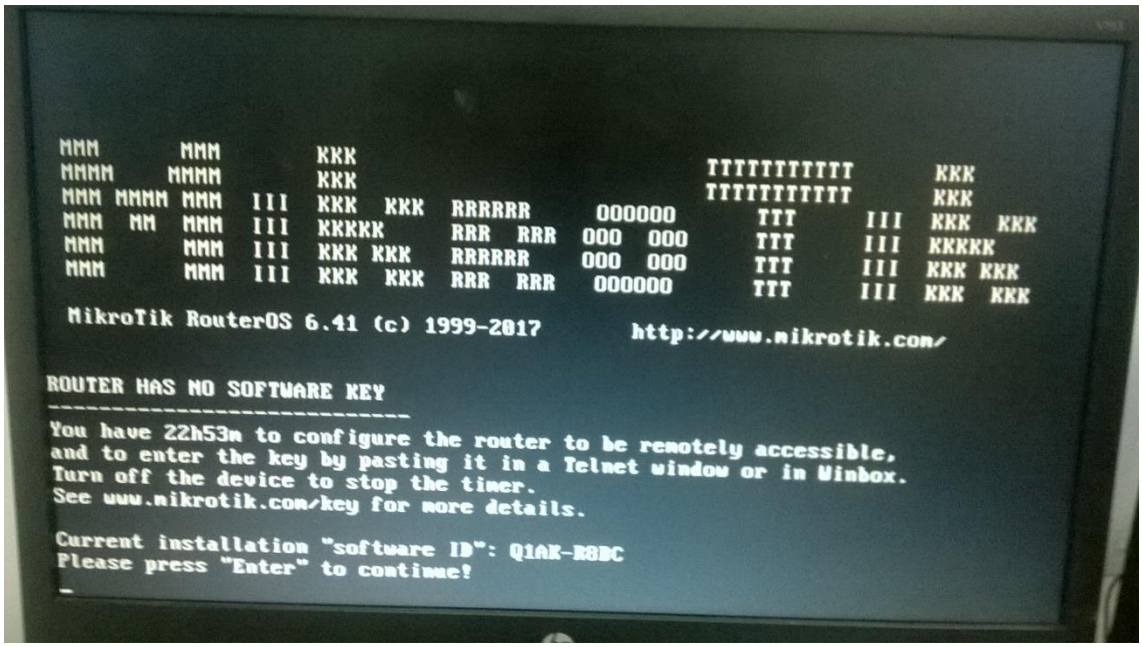


Figura 24 Notificación Instalación

Fuente: Mikrotik Router 6.41

Se accede al servidor Mikrotik ingresando el usuario admin sin contraseña, y así termina la instalación del servidor Mikrotik para poder administrarlo.

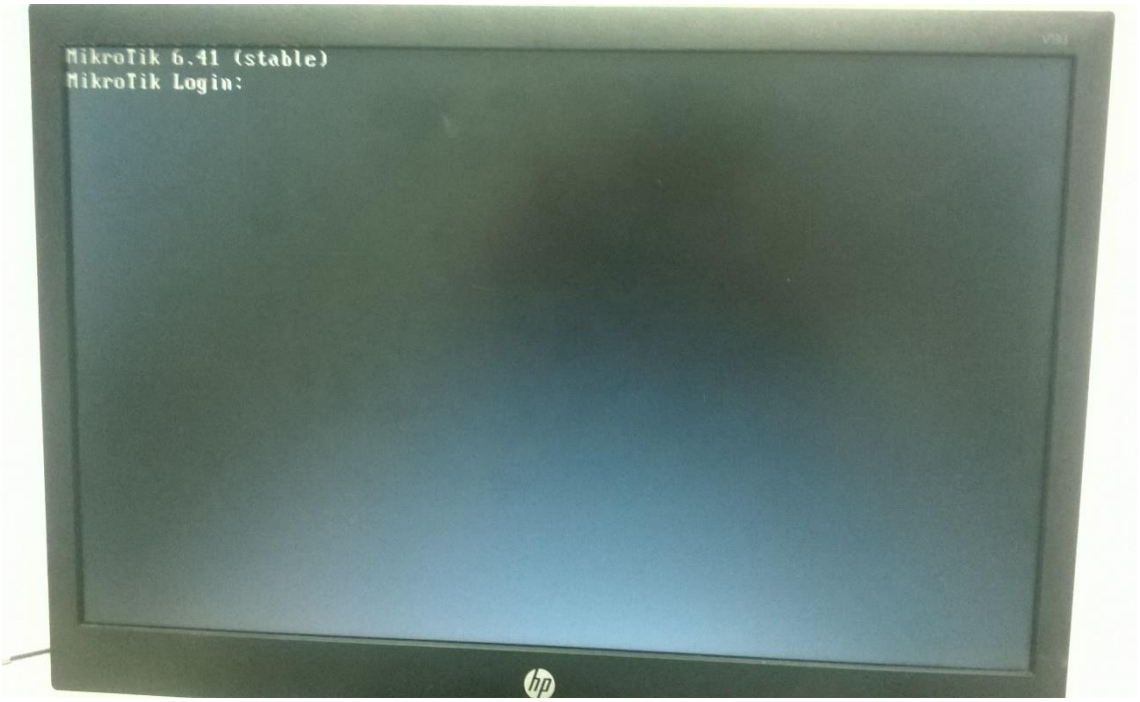


Figura 25 Login Servidor Mikrotik

Fuente: Mikrotik Router 6.41

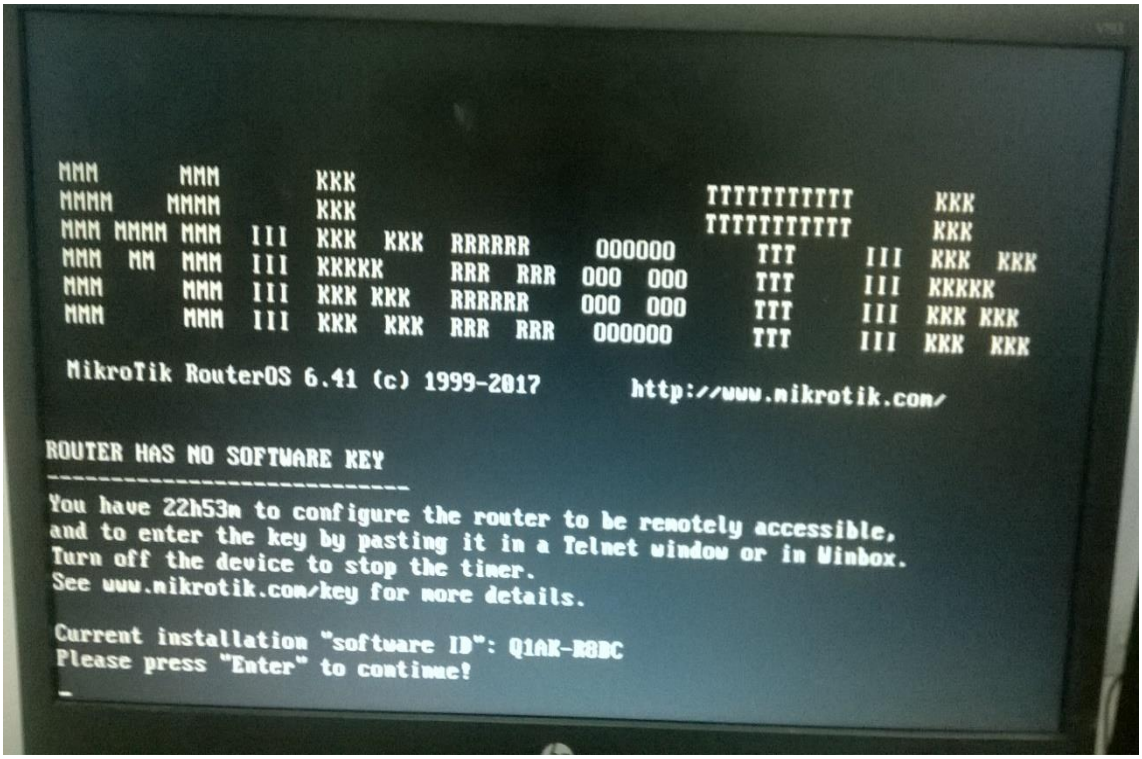


Figura 26 Inicio Servidor Mikrotik

Fuente: Mikrotik Router 6.41

5.4.3 Configuración Básica Servidor Mikrotik

Para realizar las diferentes configuraciones se usa una herramienta gráfica propia de Mikrotik llamada winbox. En la pestaña de software de la página de Mikrotik se encuentra la última versión del winbox para poder ser descargada. Una vez instalado en una laptop o PC se deberá conectar un cable UTP desde la tarjeta de red del equipo hasta el servidor Mikrotik.

Winbox muestra una pantalla inicial donde se debe ir al menú de neigbors para seleccionar el equipo Mikrotik a configurar. Para poder tener acceso al servidor Mikrotik por defecto se entra con IP 0.0.0.0 o mediante la MAC que se generó. Al momento de conectarse aparece una advertencia indicando el tiempo que se dispone para utilizar el router, por eso se debe activar la licencia.

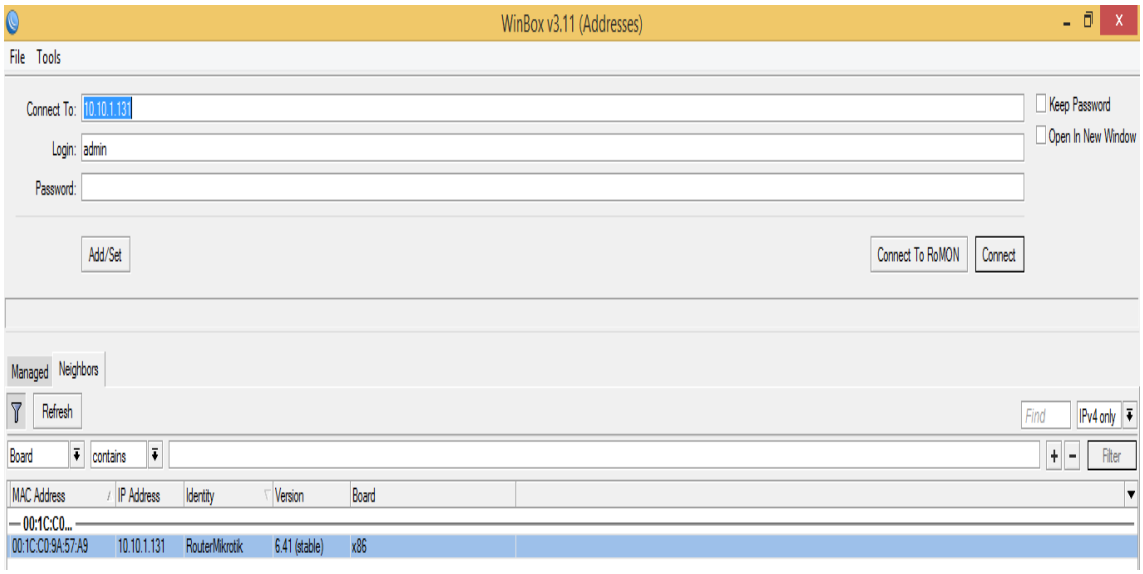


Figura 27 Winbox Inicio

Fuente: Winbox Mikrotik

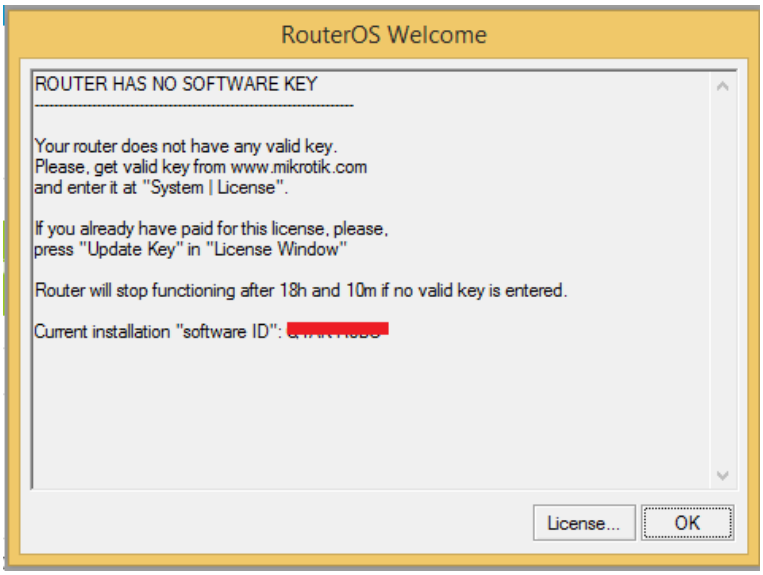


Figura 28 Licencia Gratuita

Fuente: Winbox Mikrotik

5.4.3.1 Licencia

Para solicitar una licencia para Mikrotik se debe comprar según el nivel que se requiere trabajar, en este caso para el presente proyecto se utiliza L4. Como primer paso se debe registrar en la página oficial de Mikrotik, luego se ingresa en la opción de Make a key from prepaid keys de la sección RouterOS Keys, una vez ubicado en la sección se ingresa el tipo de equipo en este caso como es un CPU, se coloca x86 system y también el software ID del Mikrotik.

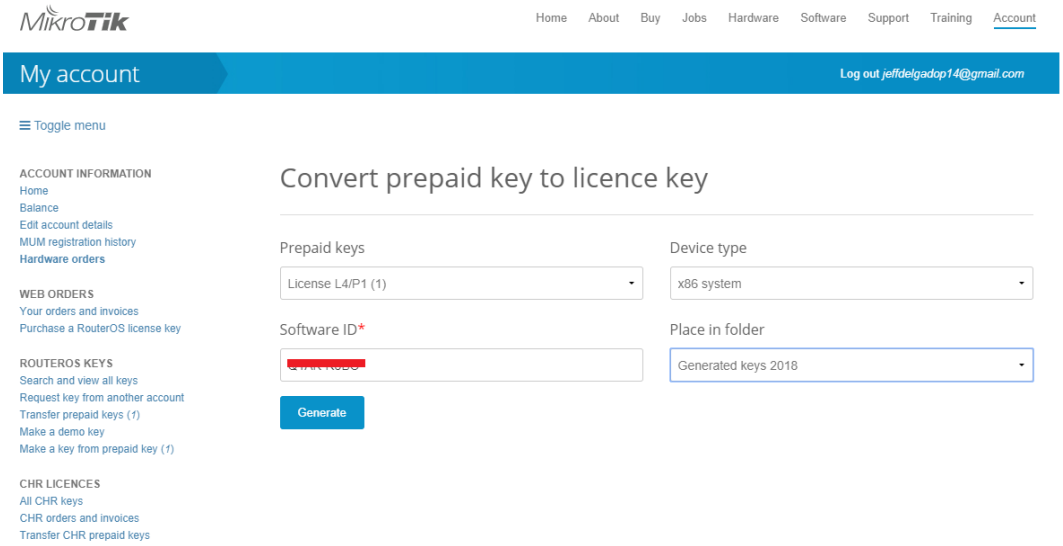


Figura 29 Preparación Licencia

Fuente: (Mikrotik, 2017)

Al generar la licencia, automáticamente se muestra una llave mediante claves, el cual se debe copiar y pegar en el terminal del router.

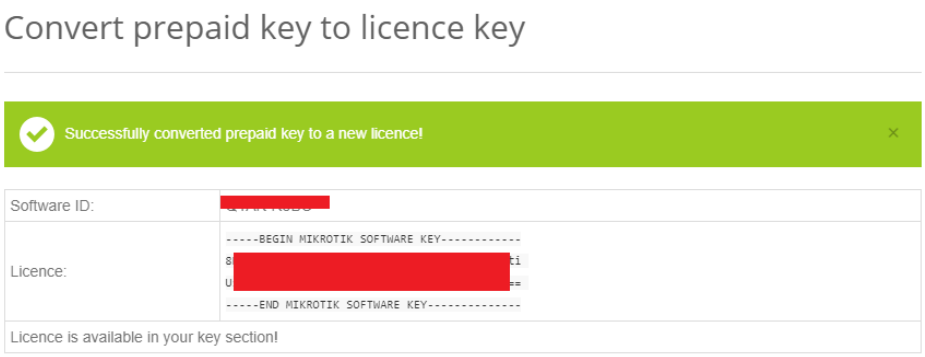


Figura 30 Activación Licencia

Fuente: Winbox

El router pide un reinicio del sistema para actualizar el nivel 4 de la licencia

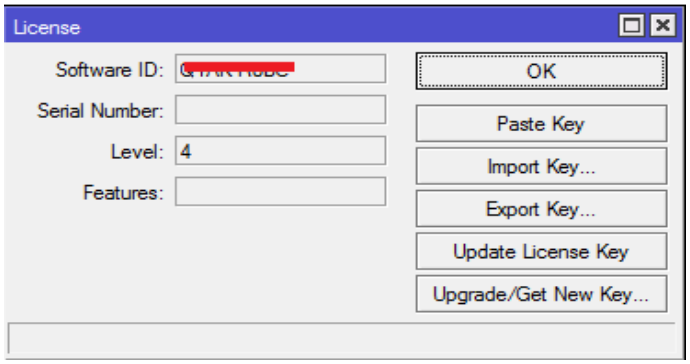


Figura 31 Comprobación Licencia

Fuente: Winbox Mikrotik

5.4.4 Configuración puerto WAN

Se renombra a la interfaz ether1 como WAN WIFI, así mismo al ether2 como LAN.

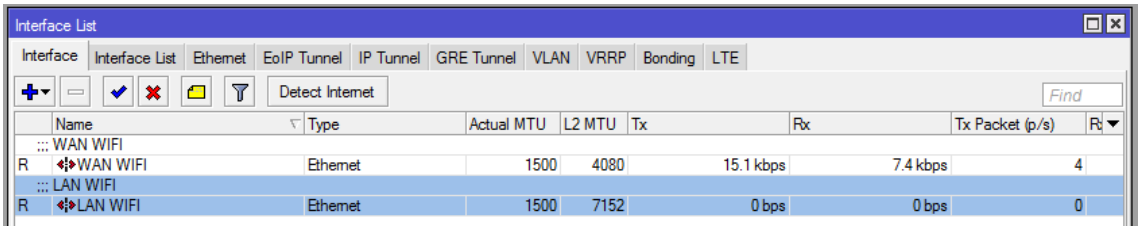


Figura 32 Interfaces Mikrotik

Fuente: Winbox Mikrotik

Se asigna la dirección IP al puerto WAN WIFI

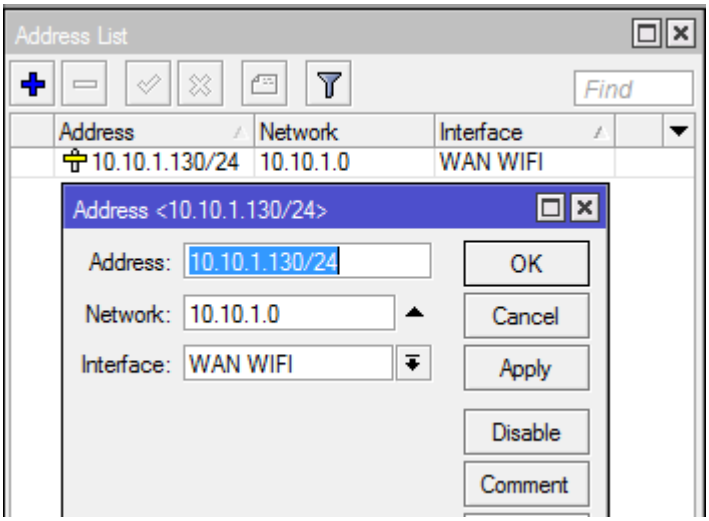


Figura 33 Dirección IP Puerto Wan

Fuente: Winbox Mikrotik

Se asigna DNS para dar acceso a internet, para el proyecto será necesario usar los dns del proveedor de internet pero como prueba usaremos los dns de google, también será necesario tener habilitado la función de DNS cache (Allow Remote Request) para entregar internet a la red lan y no solo al ether1

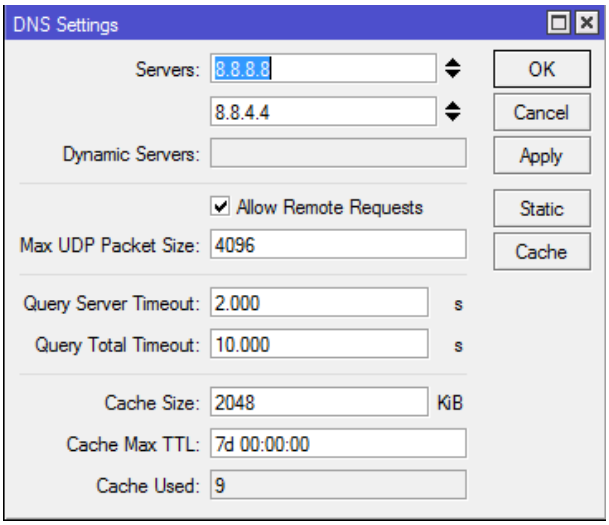


Figura 34 Asignación DNS

Fuente: Winbox Mikrotik

Se asigna el Gateway para la salida a internet, las iniciales que aparece en cada ruta significa lo siguiente.

AS: Active Static

DAC: Dynamic Active Connected

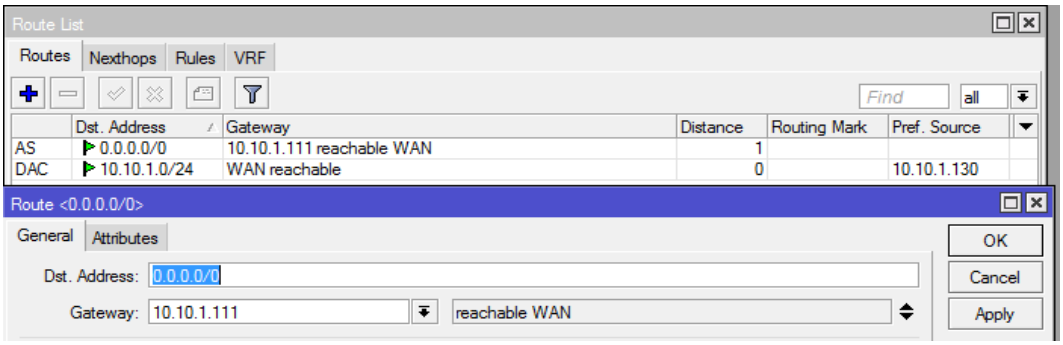


Figura 35 Gateway Mikrotik

Fuente: Winbox Mikrotik

Se prueba haciendo ping para verificar conexión

```
[admin@MikroTik] > ping www.google.com.ec
  SEQ HOST                                     SIZE TTL TIME   STATUS
    0 216.58.219.195                             56  54 119ms
    1 216.58.219.195                             56  54 120ms
    2 216.58.219.195                             56  54 129ms
    3 216.58.219.195                             56  54 126ms
    4 216.58.219.195                             56  54 104ms
```

Figura 36 Ping de prueba

Fuente: Winbox Mikrotik

5.4.5 Configuración Vlans

El sistema RouterOS de Mikrotik permite crear 4095 vlans por interfaz teniendo una id única. El puerto ether2 se conecta a un switch, lo cual se debe configurar como puerto troncal agregando las 3 vlans a la interface ether2 según detallado en la Tabla 7.

- Vlan 15: Gestión de Equipos
- Vlan 16: Red administración
- Vlan 17: Red doctores
- Vlan 18: Red invitados

Mikrotik automáticamente lo define como puerto troncal (Port Tagged) cuando se agrega varias vlans a una interfaz o bridge.

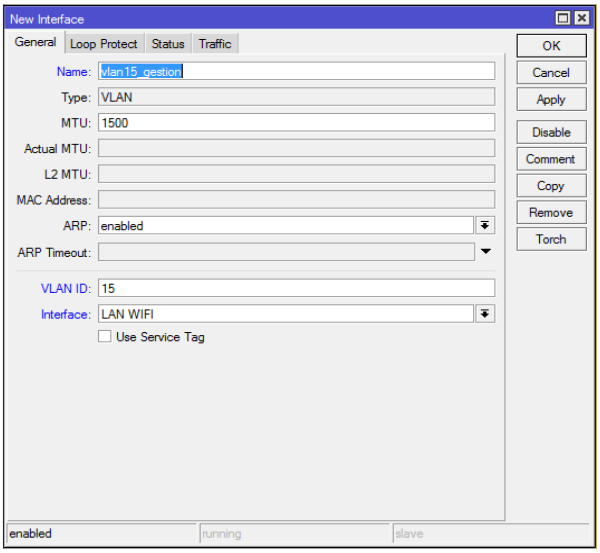


Figura 37 Creación Vlan 15

Fuente: Winbox Mikrotik

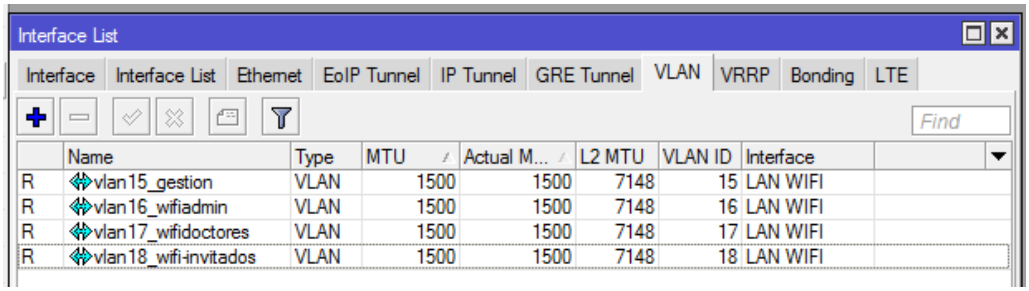


Figura 38 Interfaces VLAN

Fuente: Winbox Mikrotik

La Figura 39 se muestra la configuración de las vlans mediante comando

```
/interface vlan
add interface="LAN WIFI" name=vlan15_gestion vlan-id=15
add interface="LAN WIFI" name=vlan16_wifiadmin vlan-id=16
add interface="LAN WIFI" name=vlan17_wifidoctores vlan-id=17
add interface="LAN WIFI" name=vlan18_wifi-invitados vlan-id=18
```

Figura 39 Creación Vlans Comando

Fuente: Winbox Mikrotik

5.4.5 Bridge

Se crea bridge para cada vlan, el bridge puede unir diferentes tecnología en este caso es necesario crear bridge porque en este proyecto se trabaja con vlans por interfaces Ethernet y wireless.

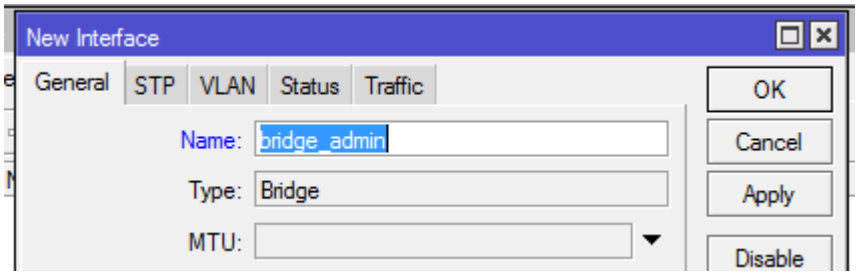


Figura 40 Creación bridge administración

Fuente: Winbox Mikrotik

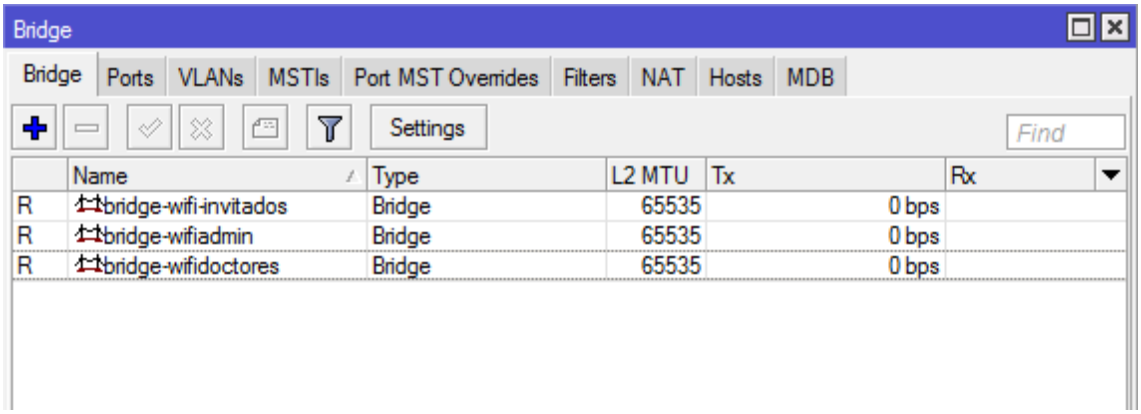


Figura 41 Bridges

Fuente: Winbox Mikrotik

5.5.5.1 Agregar puertos al bridge

Una vez creado las vlans y bridges se asocia a cada una de ellas. Al agregar puertos a un bridge se podrá definir que puertos pertenecen a la misma red.

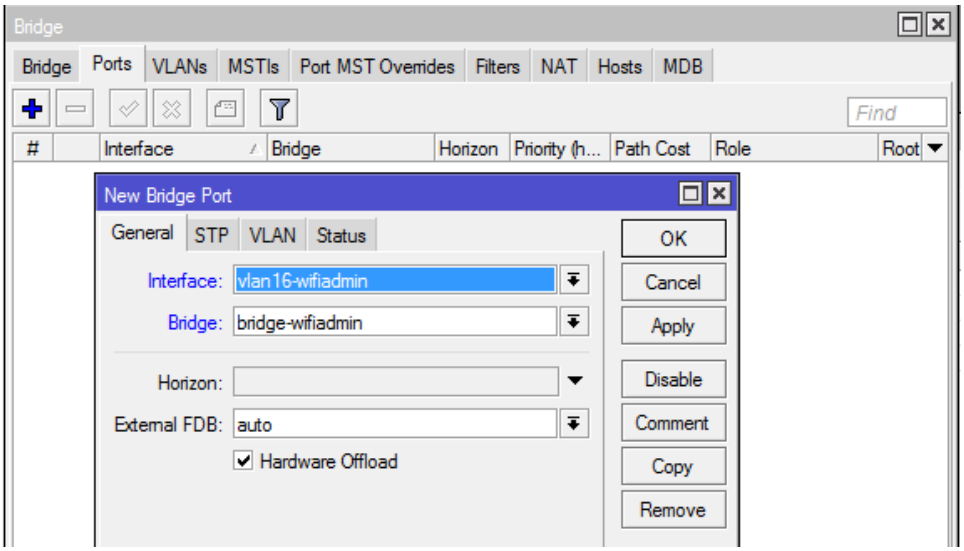


Figura 42 Puerto bridge admin

Fuente: Winbox Mikrotik

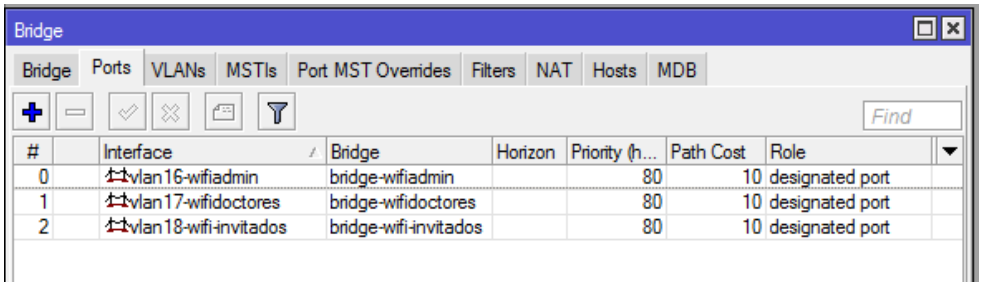


Figura 43 Puertos bridge

Fuente: Winbox Mikrotik

5.4.6 Direccionamiento IP y DHCP

Se asigna IP a cada interface Vlan como se muestra en la Tabla 9

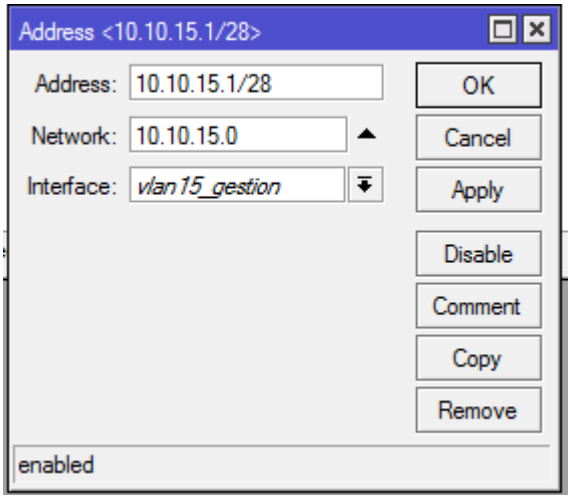


Figura 44 Dirección IP vlan 15

Fuente: Winbox Mikrotik

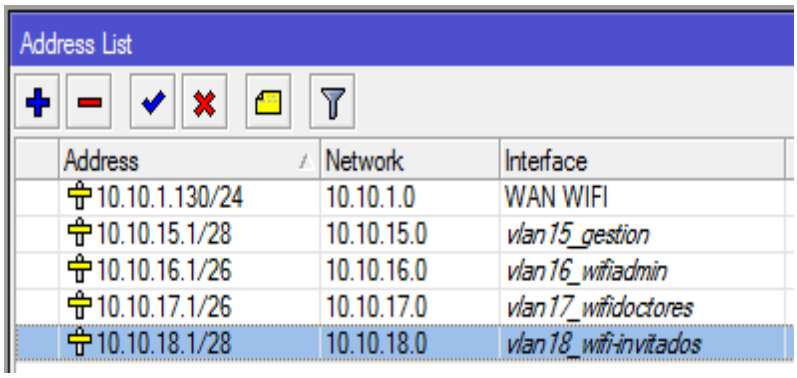


Figura 45 Direccionamiento IP

Fuente: Winbox Mikrotik

Se crea DHCP para otorgar de manera dinámica direcciones IP a las redes vlan de administración, doctores e invitados. Para la red de gestión solo se usa 5 direcciones IP dinámicamente para realizar las diferentes configuraciones necesarias del servidor, switch o access point.

Se usa la opción “DHCP Setup” para hacer la respectiva configuración.

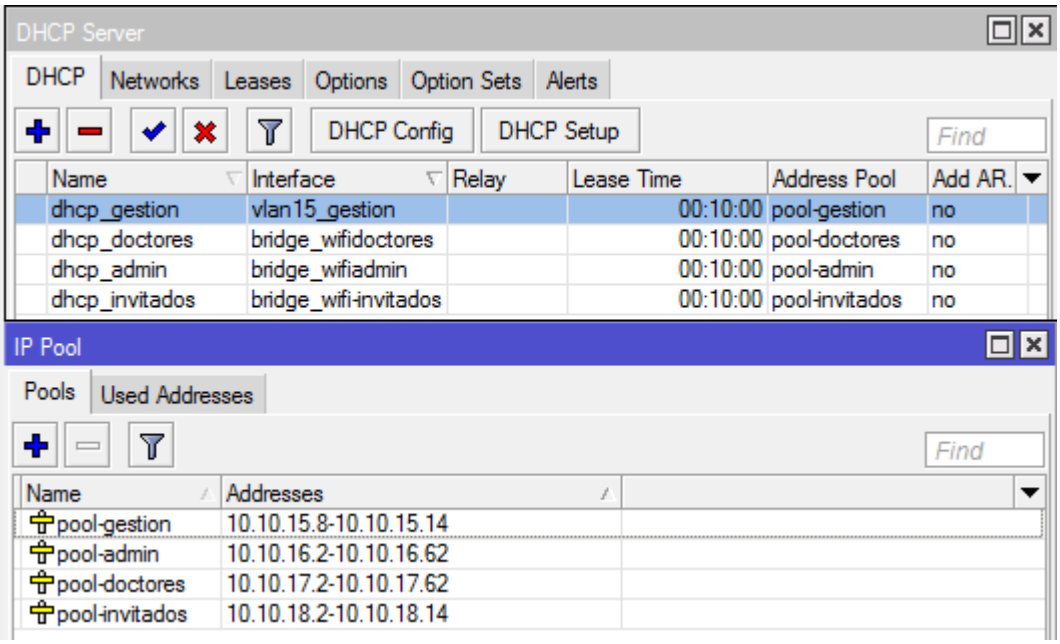


Figura 46 Creación Servidor DHCP

Fuente: Winbox Mikrotik

En IP -> Route se muestra el enrutamiento que hace cada Vlan

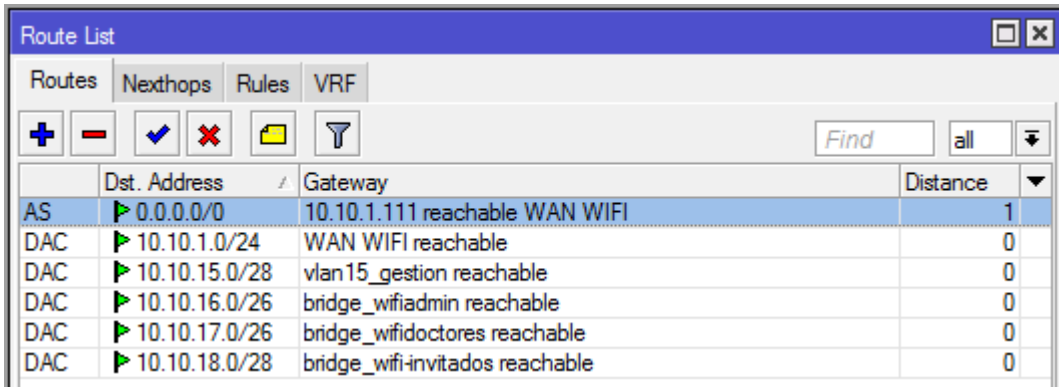


Figura 47 Gateway Vlans

Fuente: Winbox Mikrotik

5.4.7 Configuración Capsman y Access Point Rbcap2nd

La red inalámbrica la compone 5 access point marca Mikrotik el cual está configurado como modo cap (Controlled Access Point) siendo administrado por el Capsman (Controlled Access Point sytem Manager) soportando 32 interfaces para cada Access point.

Como requisito principal, Mikrotik indica que se debe tener actualizado la misma versión tanto en el Capsman como en el cap y habilitar en la opción de package List el paquete wireless, a continuación se detalla algunas características que menciona Mikrotik. (Mikrotik Documentation, 2017)

- Habilitar paquete wireless.npk
- Capsman opera desde la versión 6.22, actualmente la última versión es 6.41
- El Capsman no necesita interfaz inalámbrica, en cambio los CAP requieren mínimo una interfaz inalámbrica con Licencia L4

Para habilitar servicio Capsman, se usa el comando (Figura 48) o también mediante interfaz gráfica (Figura 49), en el menú principal se da click en la pestaña

Capsman -> Manager y se habilita el servicio CapsManager. Una vez activado el servicio se agregan automáticamente todos los cap habilitados.

```
/caps-man manager
set enabled=yes
```

Figura 48 Habilitación Capsman Comando

Fuente: Winbox Mikrotik

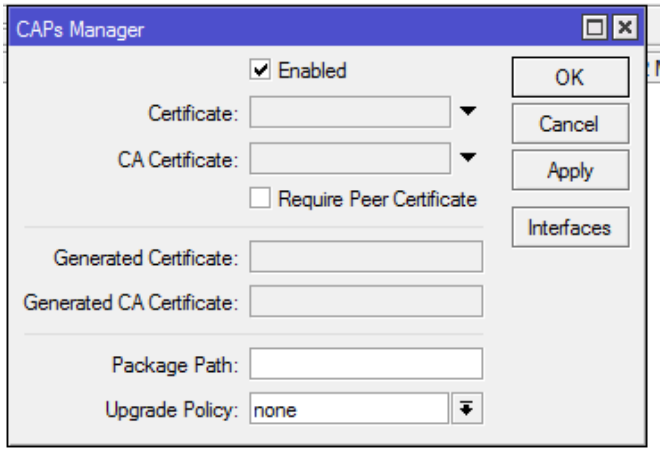


Figura 49 Habilitación Capsman Interfaz

Fuente: Capsman Mikrotik

El Capsman tiene algunos parámetros (Figura 50) que se usan en este proyecto, a continuación se explica la función de cada una de ellas

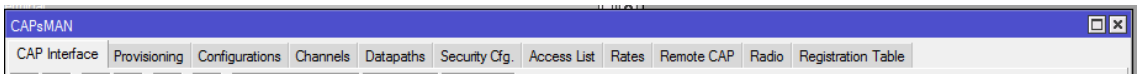


Figura 50 Parámetros Capsman

Fuente: Capsman Mikrotik

- **Provisioning:** Se define los caps que serán controlados por el Capsman con determinada configuración, se los puede agrupar por un cap especifico o un grupo de cap o en general.

- **Channels:** Se define las bandas y canales que se usa en los diferentes caps.

- **Datapaths:** Se determina en que puerto saldrá los datos, es configuración relacionada con el bridge donde se integra la interfaz de los CAPs, de esta forma se configura el reenvió de tráfico hacia el Capsman.

- **Security Cfg:** Se realiza configuraciones de seguridad tales como cifrado y autenticación.

- **Configurations:** Se define el SSID, canal, datapath, y seguridad ya creados en las otras pestañas.

5.4.7.1 Pestaña DATAPATH

Se crea los datapath para cada ssid, la opción de datapath en este proyecto se escoge la opción de bridge por usar vlans con tecnología inalámbrica y Ethernet.

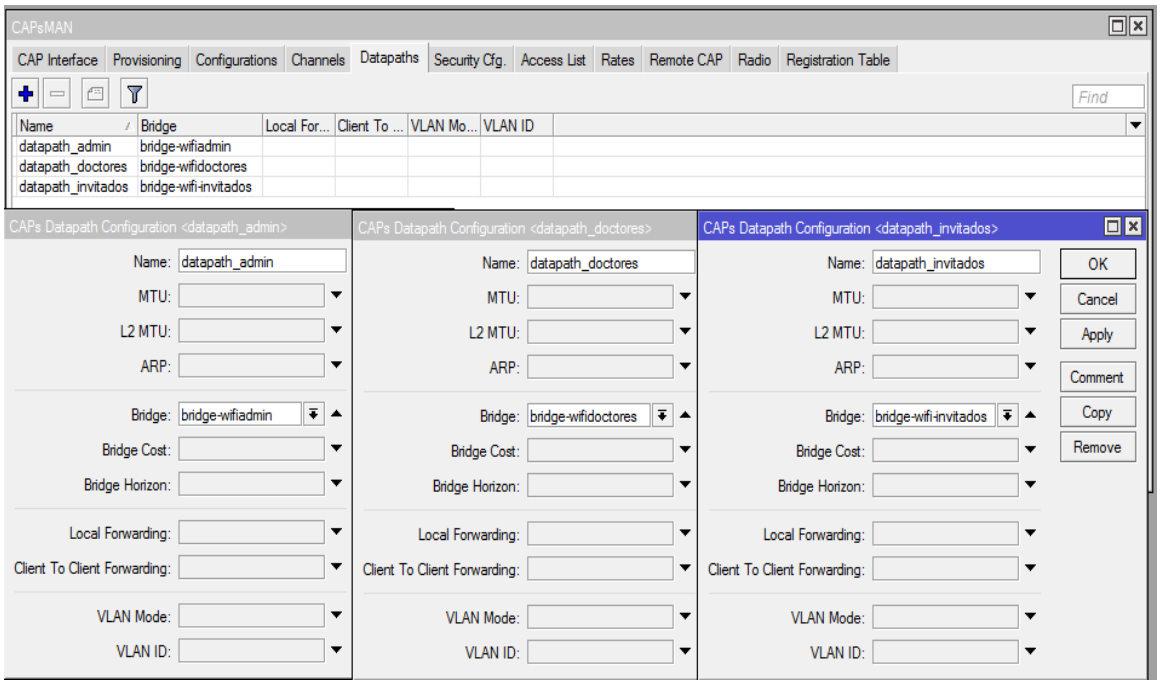


Figura 51 Pestaña Datapath

Fuente: Capsman Mikrotik

En algunas redes no es necesario que clientes de redes inalámbricas compartan información entre sí, en estos casos por seguridad es recomendable deshabilitar la opción Client to Client Forwarding.

5.4.7.2 Pestaña Canal

Como se explica en la tabla 6 es recomendable usar los canales 1, 6 y 11 para la frecuencia de 2,4 GHz. Se elige la banda 2ghz-b/g/n al existir dispositivos inalámbricos que no soportan todas las bandas.

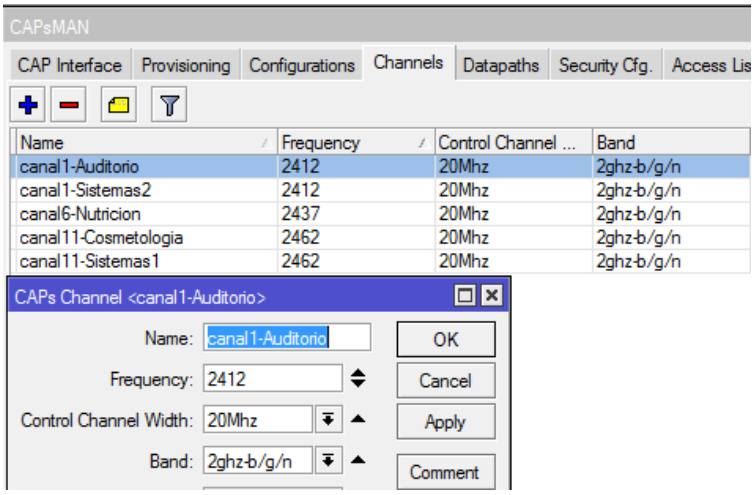


Figura 52 Pestaña Canal

Fuente: Capsman Mikrotik

La asignación de canales en cada access point se hace referencia a la ubicación de cada access point como se muestra la Figura 17 y 18.

Tabla 12 Asignación de canales a los AP

Equipos	Frecuencia 2.4 GHZ		Ubicación
	Canal	Ancho de banda	
CAP1	11	20Mhz	Cosmetología
CAP2	6	20Mhz	Nutrición
CAP3	1	20Mhz	Sistemas 2 PB
CAP4	11	20Mhz	Sistemas 1 PA
CAP5	1	20Mhz	Auditoria

Elaborado: Autor

5.4.7.3 Pestaña Seguridad

Se otorga la seguridad para la red administración creando un perfil de seguridad para añadir a los ssid. Mikrotik por defecto tiene la autenticación el método eap tls pero en el presente proyecto se procede la autenticación con un servidor Radius externo por eso se selecciona la opción de passthrough.

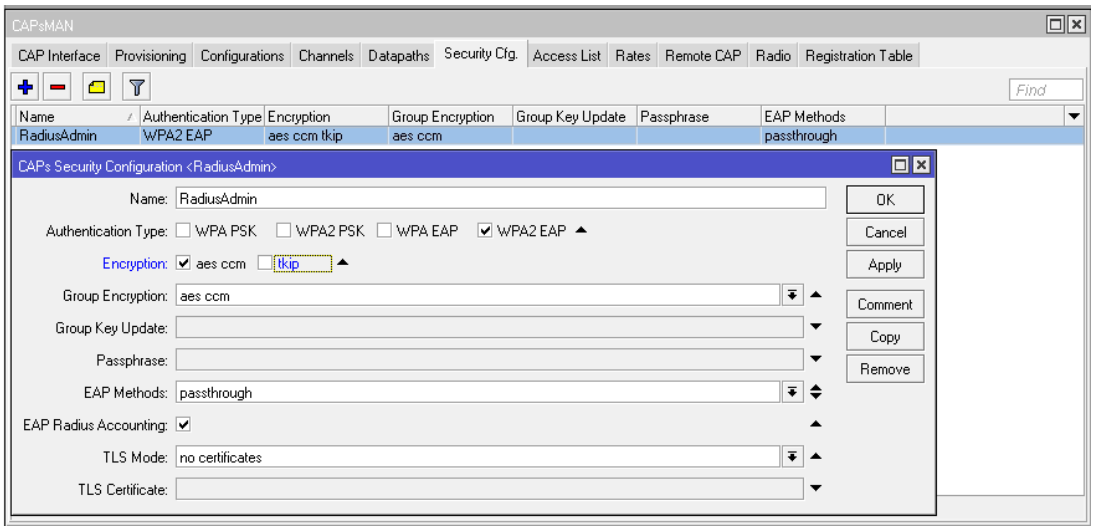


Figura 53 Pestaña Seguridad Admin

Fuente: Capsman Mikrotik

5.4.7.4 Pestaña Configuraciones

En esta pestaña se configura los ssid como indica la tabla 8 y se asocia al canal y datapath ya configurado. Es recomendable limitar el número de clientes por access point y exista un balanceo de estaciones.

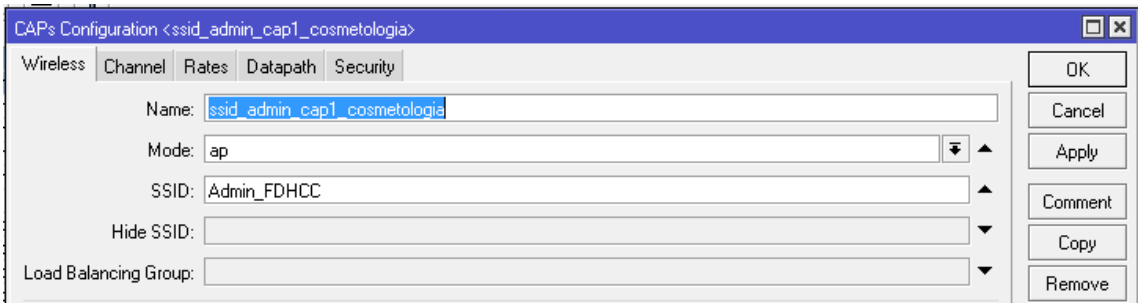


Figura 54 Creación SSID

Fuente: Capsman Mikrotik

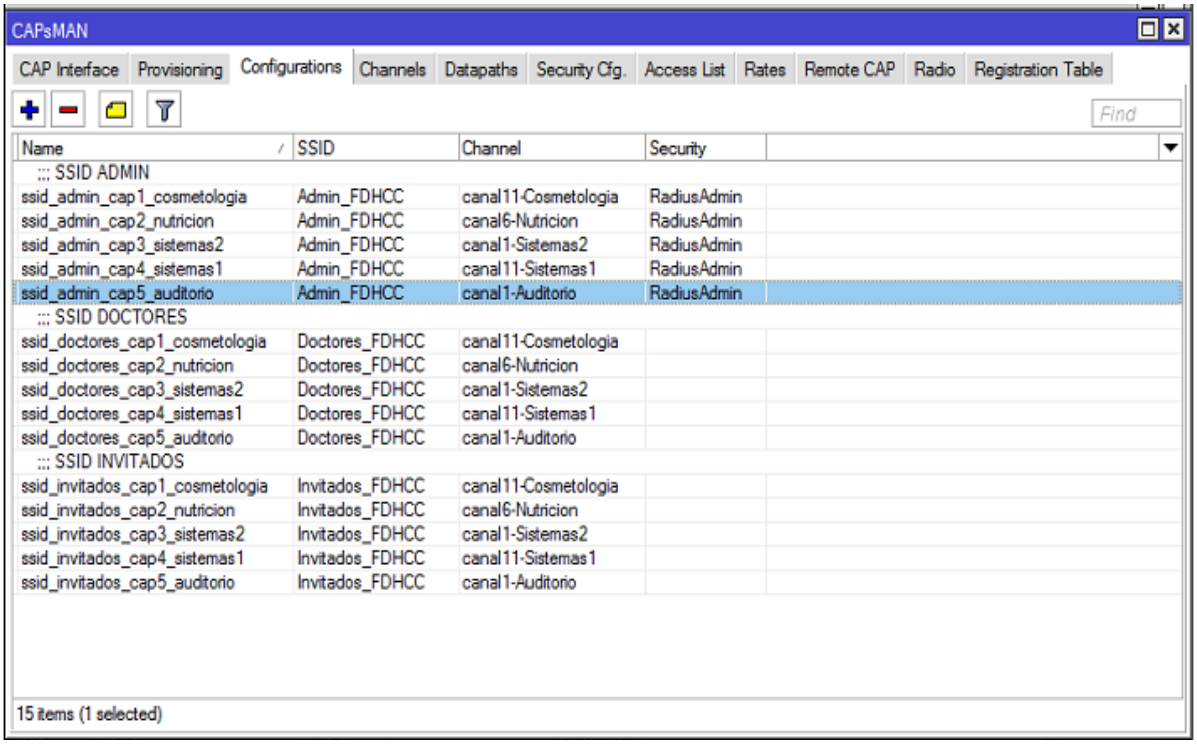


Figura 55 Pestaña Configuración

Fuente: Capsman Mikrotik

5.4.7.5 Pestaña Provisioning

En la pestaña de provisionamiento se establece las reglas con las configuraciones específicas para los diferentes cap, en este proyecto todos los cap tendran la misma configuracion excepto el canal.

Se explica brevemente las diferentes opciones que presenta esta pestaña.

- En la opción de Radio Mac por defecto se puede usar 00: 00: 00: 00: 00: 00 aplicando la configuración a todos los cap pero en este proyecto se coloca el radio name de cada cap y se asigna diferente configuración para cada cap.

- Se selecciona en action la opción de créate dynamic enabled que permite la creación dinámica de las interfaces y permanecer operativas.

- En la opción de Master y slave configuration se selecciona las configuraciones de ssid para los diferentes access points.

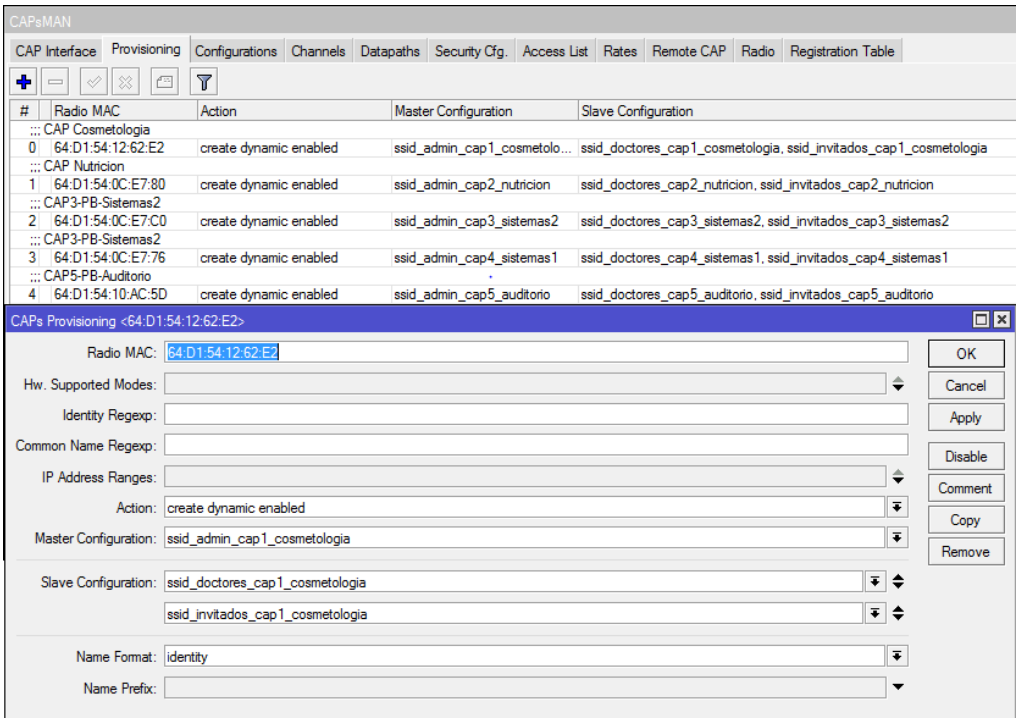


Figura 56 Provisioning

Fuente: Capsman Mikrotik

5.4.7.6 Configuración Roaming

Esta opción sirve para que un equipo inalámbrico no siga conectado a un access point con potencia baja teniendo un access point cercano con mejor potencia, configurando en access list para que se conecten al access point más indicado.

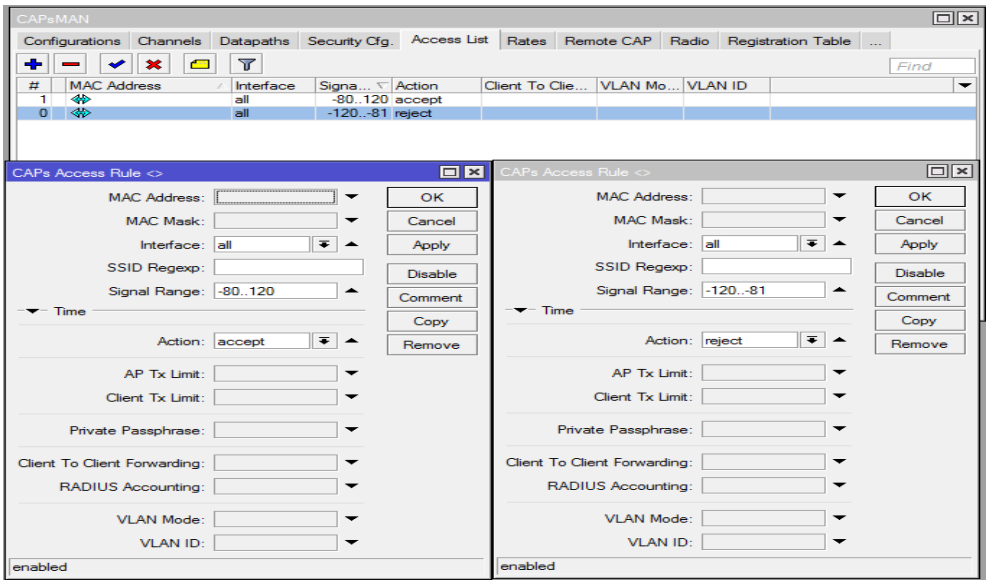


Figura 57 Access List Roaming

Fuente: Capsman Mikrotik

También se puede configurar mediante comandos

```
/caps-man access-list
add action=accept disabled=no interface=all signal-range=-80..120 ssid-regexp=\
    ""
add action=reject disabled=no interface=all signal-range=-120..-81 ssid-regexp=\
    ""
```

Figura 58 Access List Roaming Comando

Fuente: Capsman Mikrotik

El access list tiene lista negra que bloquea la conexión al access point y lista blanca que permite que dispositivo se pueda conectar.

5.4.7.7 Configuración CAP

Cada cap gestionado vía capa 2 o capa 3 por el Capsman tendrá desactivada la interface wireless, bloqueando realizar configuraciones de manera local. Se usa el protocolo DTLS entre la comunicación del cap con Capsman. Para la configuración inicial se conecta directamente en el puerto ether2 del servidor el access point. Desde el servidor se configura la identidad e IP de gestión del Cap.

En la opción IP -> Neighbors aparece una ventana donde muestra los equipos conectados al servidor. Una vez escogido el cap se selecciona la opción de mac telnet, entrando con el login por defecto admin

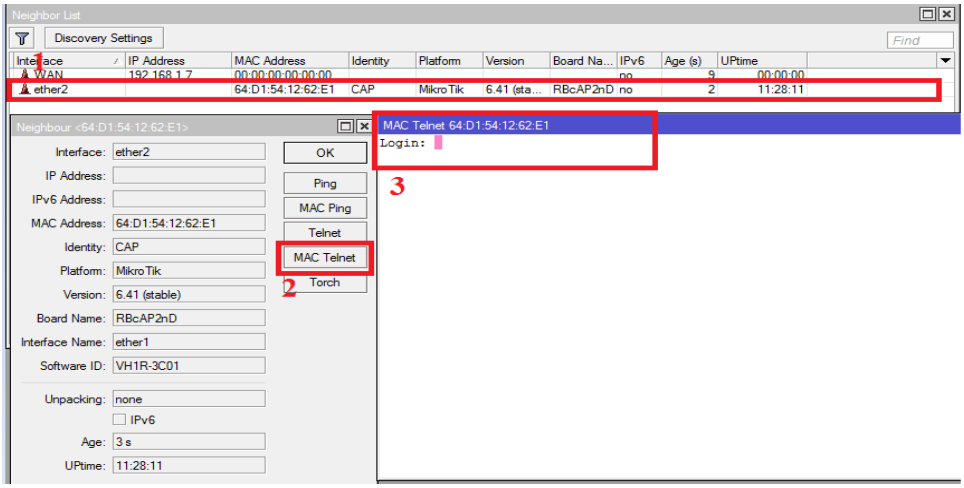


Figura 59 Conexión Telnet Cap

Fuente: Capsman Mikrotik

Una vez conectado se cambia el nombre del cap en este caso se configura el primer Access Point para planta baja

```
[admin@MikroTik] > /system identity
[admin@MikroTik] /system identity>> set name=CAP1-PB-Cosmetologia
```

Figura 60 Identity Cap

Fuente: Capsman Mikrotik

Se crea la vlan gestión para poder administrada con la ip de la red que se estableció en la Tabla 9

```
/interface vlan
add interface=ether1 name=vlan15_gestion vlan-id=15
```

Figura 61 Creación Vlan Cap

Fuente: Capsman Mikrotik

Luego se asigna el direccionamiento ip al primer cap, todos los access point tendrán ip en la vlan de gestión.

```
/ip address
add address=10.10.15.10/28 interface=vlan15 network=10.10.15.0
```

Figura 62 Dirección IP Cap

Fuente: Capsman Mikrotik

Para poder habilitar el modo cap se selecciona enabled y en este caso se elige que busque el Capsman por capa 2.

```
[admin@MikroTik] > interface wireless
set discovery-interfaces=vlan15 enabled=yes interfaces=wlan1
```

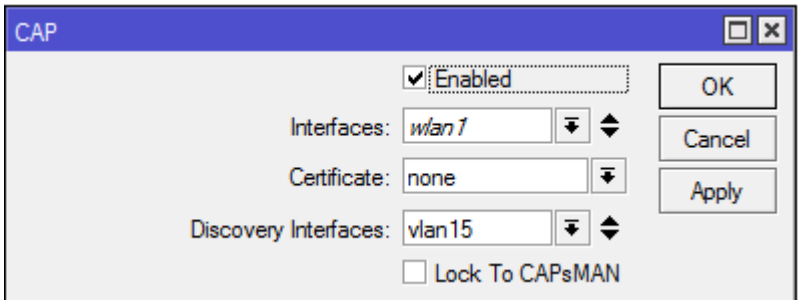


Figura 63 Habilitación Cap

Fuente: Capsman Mikrotik

Finalmente se comprueba que la interface del CAP sea gestionada por el Capsman, bloqueando la configuración localmente de la interface Wireless.

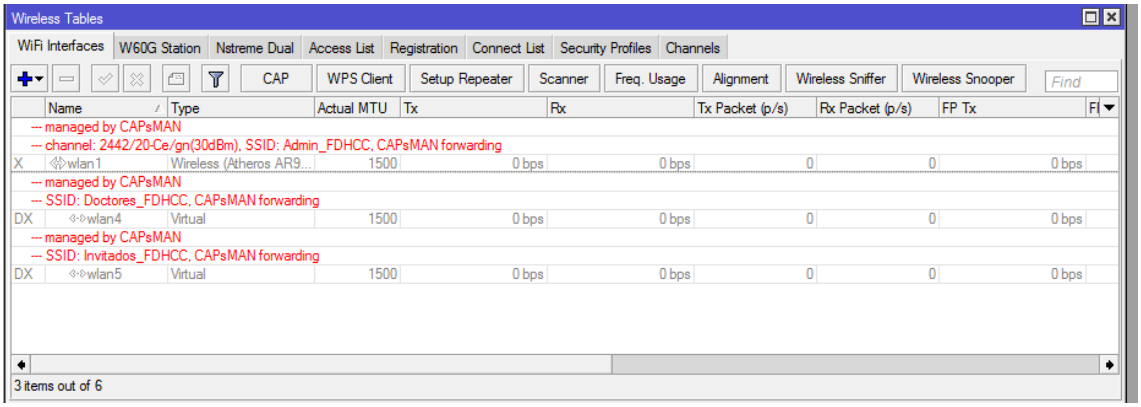


Figura 64 Conexión exitosa a Capsman

Fuente: Capsman Mikrotik

En la tabla de registro se puede ver todos los dispositivos conectados a los Access Point instalado, incluso se puede bloquear a un dispositivo el acceso a la red inalámbrica, únicamente copiando el registro de mac address en el Access List.

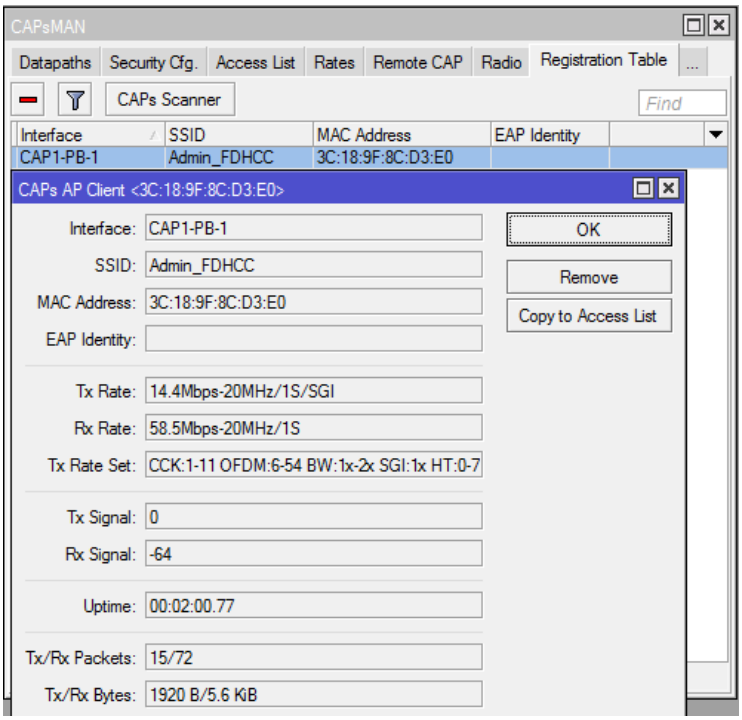


Figura 65 Registros de equipos clientes

Fuente: Capsman Mikrotik

Identificación CAP

Existen varios parámetros para identificar a cada Access point por el nombre, mac address, versión, serial, etc. También puede existir que trabajen en doble banda 2,4GH y 5Ghz

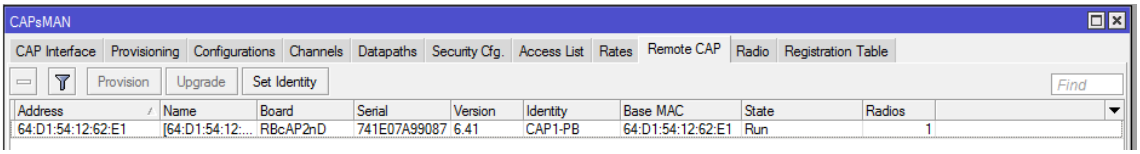


Figura 66 Identificación CAP

Fuente: Capsman Mikrotik

5.4.8 Radius

Para el presente proyecto se utiliza freeradius como servidor Radius, luego de realizar las configuraciones básicas de freeradius como direccionamiento IP, actualización del sistema e instalación de los diferentes paquetes se debe editar los diferentes archivos como clients.conf, nas.sql, sql.conf, etc.

5.4.8.1 Configuración Básica FreeRadius

Se utiliza el sistema operativo Linux por ser un sistema seguro y estable teniendo varias distribuciones, eligiendo la distribución Ubuntu 16.04 por ser un sistema LTS (Long Term Support). Ubuntu es basado en Debían, pero Ubuntu tiene una versión más actualizada para servidores, la versión 16.04 al ser una versión LTS permite tener actualizaciones y soporte hasta el año 2021 ya que una versión normal puede tener como máximo hasta 9 meses de soporte.

Para el presente proyecto se escogió la versión Ubuntu Server 16.04, orientado para servidores que permite tener una administración mediante interfaz de comandos como se muestra en la Figura 67. Los requisitos que se requiere para poder instalar la distribución Ubuntu son:

- Memoria RAM 512Mb
- Disco Duro Mínimo 5Gb
- Conexión a Internet

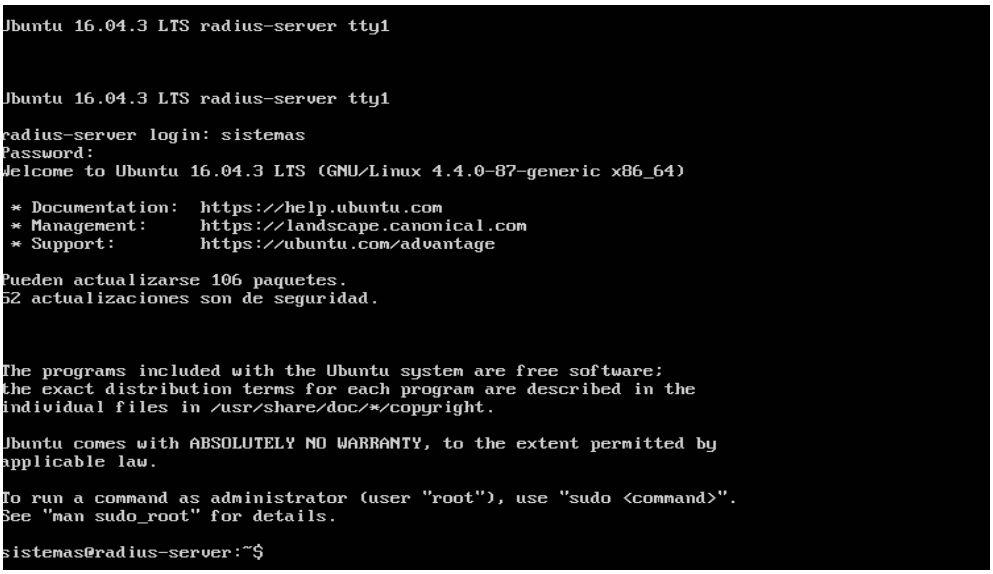


Figura 67 Interfaz de comandos Ubuntu Server

Fuente: Servidor Ubuntu 16.04

En el anexo D se realiza el proceso de instalación de la distribución Ubuntu, teniendo instalado los servicios LAMP, el cual significa la agrupación de servicios tales como Linux siendo el sistema operativo donde se ejecuta el FreeRadius, Apache server utilizado para el protocolo http, Mysql gestor de base de datos para el manejo de usuarios, y Php siendo un lenguaje de programación para páginas web dinámicas. En el caso de no tener instalado dicho servicios se tendrá que realizar la instalación de los paquetes manualmente.

Antes de realizar las configuraciones, se ejecuta un comando que permita instalar el entorno de escritorio en Ubuntu.

Figura 68 Instalación Interfaz Gráfica Ubuntu

Fuente: Servidor Ubuntu 16.04

Luego de ejecutar el comando para la instalación de la interfaz de escritorio, se podrá realizar las configuraciones básicas del servidor tales como direccionamiento Ip en modo root.

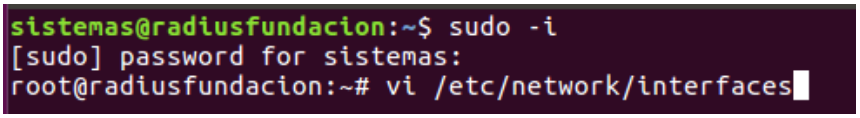


Figura 69 Comando interfaces

Fuente: Servidor Ubuntu 16.04

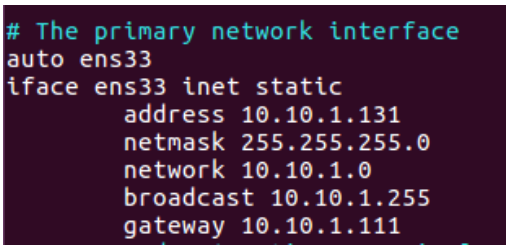


Figura 70 Configuración interface

Fuente: Servidor Ubuntu 16.04

Una vez configurado la dirección IP correspondiente al servidor se podrá realizar actualizaciones del sistema operativo y también descargas de paquetes tales como el paquete FreeRadius.

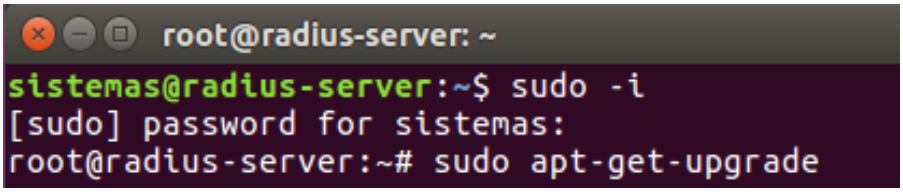


Figura 71 Actualización paquetes Ubuntu

Fuente: Servidor Ubuntu 16.04

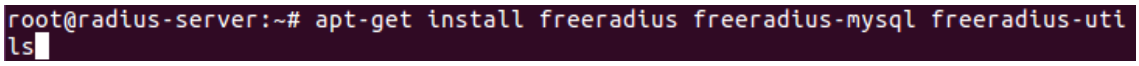


Figura 72 Instalación Paquetes FreeRadius

Fuente: Servidor Ubuntu 16.04

Al instalar el paquete FreeRadius se podrá crear localmente un usuario en la ruta **/etc/freeradius/Users,** para eso se usa el comando vi y como usuario de prueba se crea el usuario jdelgadop con contraseña sistemas.

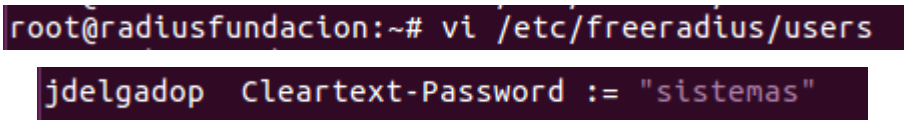


Figura 73 Creación usuario local

Fuente: Servidor Ubuntu 16.04

En el archivo clients.conf se añade los access points, en este proyecto los access point serán administrados por el controlador Capsman, el cual se debe colocar la dirección IP 10.10.1.130 con la contraseña para la comunicación con el Radius.

```
root@radiusfundacion:~# vi /etc/freeradius/clients.conf
```

```
client localhost {

        ipaddr = 127.0.0.1
        secret = fdhcc2017
}
```

```
client 10.10.1.130 {
        secret          = fdhccap
        shortname       = Admin_FDHCC
}
```

Figura 74 Cliente Radius

Fuente: Servidor Ubuntu 16.04

Se realiza una primera prueba verificando el funcionamiento del FreeRadius en modo debug, para eso se deberá primero detener el servicio y luego ejecutar el comando FreeRadius -X

```
root@radiusfundacion:~# service freeradius stop
```

```
root@radiusfundacion:~# freeradius -X
```

Figura 75 Prueba Freeradius

Fuente: Servidor Ubuntu 16.04

Al mostrar el mensaje “Ready to process requests” indica que todo está correcto

```
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on authentication address 127.0.0.1 port 18120 as server inner-tunnel
Listening on proxy address * port 1814
Ready to process requests.
```

Figura 76 Comprobación Freeradius

Fuente: Servidor Ubuntu 16.04

Ahora se verifica con usuario y contraseña creada localmente

```
root@radiusfundacion:/# radtest jdelgadop sistemas 127.0.0.1 0 fdhcc2017
Sending Access-Request of id 182 to 127.0.0.1 port 1812
        User-Name = "jdelgadop"
        User-Password = "sistemas"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=182, length=20
```

Figura 77 Prueba usuario Freeradius

Fuente: Servidor Ubuntu 16.04

5.4.8.2 FreeRadius con conexión Mysql

Se debe iniciar sesión como root y crear la base que se utiliza en el servidor, también se adiciona los privilegios a la base de datos para un usuario, el password por defecto puede ser la misma que se usó durante la instalación en la opción de Mysql.

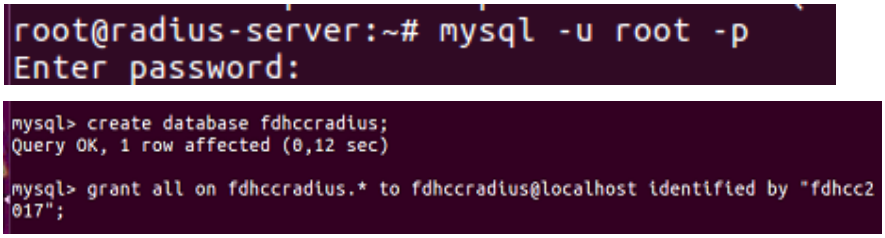


Figura 78 Configuración básica Mysql FreeRadius

Fuente: Servidor Ubuntu 16.04

Para la creación de las tablas de la base de datos se crea en base a los scripts que se encuentran en archivos schema.sql y nas.sql. En estas tablas se ingresan datos como usuario y contraseña, también el cliente radius, en este caso sería el Capsman.

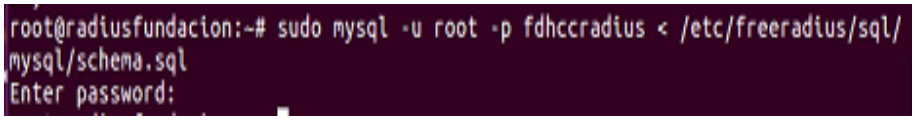


Figura 79 Creación tabla schema.sql

Fuente: Servidor Ubuntu 16.04

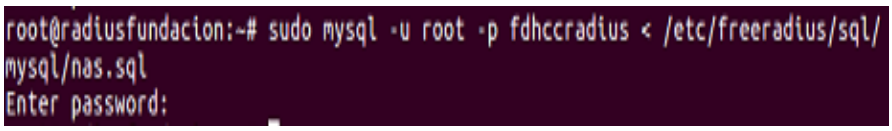


Figura 80 Creación tabla nas.sql

Fuente: Servidor Ubuntu 16.04

Para la comprobación, si la base de datos fue creada se ingresa al Mysql y se realiza las consultas con los comandos Mysql. En la figura 81 se muestra las bases de datos creadas, entre ellas la base fdhccradius que se creó para el proyecto.

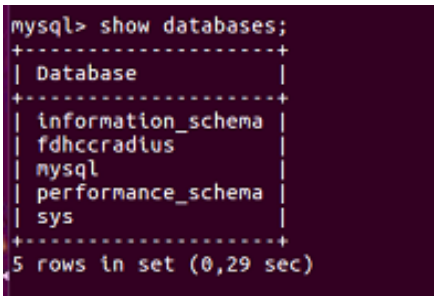


Figura 81 Consulta Base de Datos

Fuente: Servidor Ubuntu 16.04

Para usar la base de datos, se ejecuta el comando use con el nombre de la base de datos.

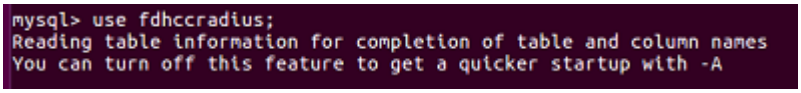


Figura 82 Elección Base Datos

Fuente: Servidor Ubuntu 16.04

Con el comando show table se verifica las tablas creadas en la base de datos

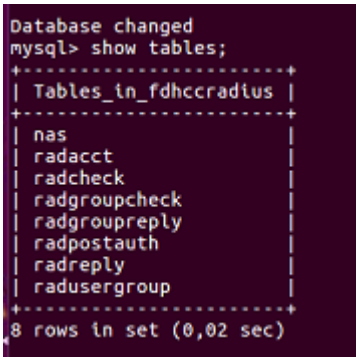


Figura 83 Comando show tables

Fuente: Servidor Ubuntu 16.04

Las diferentes tablas cumplen diferentes funciones para la gestión de usuarios.

Radacct Se crea una contabilidad de las sesiones iniciadas cuando el usuario se autentica, y también cuando finaliza.

Radcheck: Se crea el usuario con la contraseña.

Radusergroup: Se crea el grupo para asignarle al usuario.

Radreply: Se asigna atributos para los usuarios como tiempo de conexión.

Radgroupreply: Similar a radreply pero este asigna a un grupo de usuarios.

Nas: Cumple la misma función que clients.conf en freeradius, ingresando los clientes (Access Points).

Para la creación de usuarios en la base de datos se inserta el mismo usuario creado anteriormente, en la base de datos de forma manual.

```
mysql> insert into radcheck (username,attribute,value)VALUES ('jdelgadop','Passw
ord','sistemas');
Query OK, 1 row affected (0,08 sec)
```

Figura 84 Insertar usuarios base de datos

Fuente: Servidor Ubuntu 16.04

La figura 85 se muestra el comando para realizar una consulta de la información ingresada en la tabla radcheck.

```
mysql> select * from radcheck;
+----+-----------+-----------+----+----------+
| id | username  | attribute | op | value    |
+----+-----------+-----------+----+----------+
|  1 | jdelgadop | Password  | == | sistemas |
+----+-----------+-----------+----+----------+
1 row in set (0,02 sec)
```

Figura 85 Consulta tabla radcheck

Fuente: Servidor Ubuntu 16.04

```
mysql> describe radcheck;
+-----------+------------------+------+-----+---------+----------------+
| Field     | Type             | Null | Key | Default | Extra          |
+-----------+------------------+------+-----+---------+----------------+
| id        | int(11) unsigned | NO   | PRI | NULL    | auto_increment |
| username  | varchar(64)      | NO   | MUL |         |                |
| attribute | varchar(64)      | NO   |     |         |                |
| op        | char(2)          | NO   |     | ==      |                |
| value     | varchar(253)     | NO   |     |         |                |
+-----------+------------------+------+-----+---------+----------------+
5 rows in set (0,12 sec)
```

Figura 86 Consulta campos tabla radcheck

Fuente: Servidor Ubuntu 16.04

Para que exista conexión entre el Freeradius y la base de datos Mysql se debe modificar algunos archivos, a continuación se explica las modificaciones que se realizó a cada archivo.

- **Vi /etc/freeradius/sql.conf**

  Se coloca el usuario y contraseña de servidor Radius, y también se indica la base de datos donde se consulta los usuarios el servidor Radius.

Figura 87 Configuración archivo sql.conf

Fuente: Servidor Ubuntu 16.04

Para el uso de clientes remotos como el Capsman se habilita la siguiente línea

Figura 88 Habilitación clientes remotos

Fuente: Servidor Ubuntu 16.04

- **Archivo /etc/freeradius/sites-enabled/default // inner-tunnel**

  En el archivo default se descomenta la línea de SQL en las secciones de Authorize, Accounting y Session.

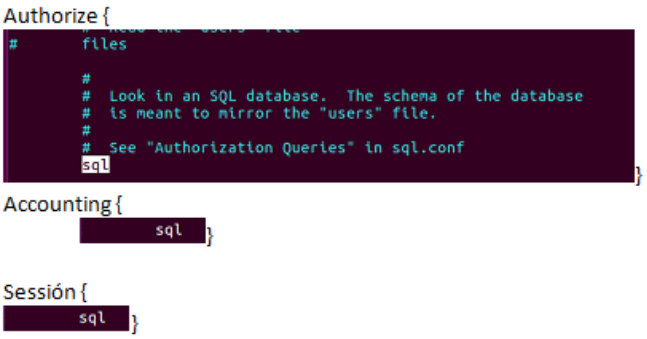


Figura 89 Autorización SQL Default

Fuente: Servidor Ubuntu 16.04

En el archivo virtual llamado inner-tunnel se descomenta **SQL** en la sección de authorize.

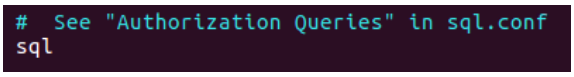


Figura 90 Autorización SQL inner-tunel

Fuente: Servidor Ubuntu 16.04

- **Archivo /etc/FreeRadius/radiusd.conf**

Este archivo sirve para activar el soporte de sql, para eso se descomenta las líneas:

- ✓ $Include sql.conf
- ✓ $INCLUDE sql/mysql/counter.conf
- ✓ $INCLUDE sqlippool.conf

Figura 91 Activación soporte Sql

Fuente: Servidor Ubuntu 16.04

Test FreeRadius

Para poder realizar el test de la base de datos se debe reiniciar el servicio freeradius para que se apliquen los cambios con el comando **service FreeRadius restart,** luego con el usuario creado en la base y colocando al final la contraseña del Radius se debe tener un mensaje de accept-accept por la solicitud de prueba que se requirió.

5.4.8.3 Cliente Radius

Luego de haber realizado las configuraciones respectivas del servidor Radius se define el cliente radius, como primer paso se debe crear el cliente Radius ubicado en el menú principal del servidor Mikrotik, definiendo el tipo de servicio que se usa en este caso se usa el hotspot y wireless. También se debe colocar la dirección IP del servidor Radius y la contraseña que se ingresó en el archivo de FreeRadius ya sea el de Nas o clients.conf

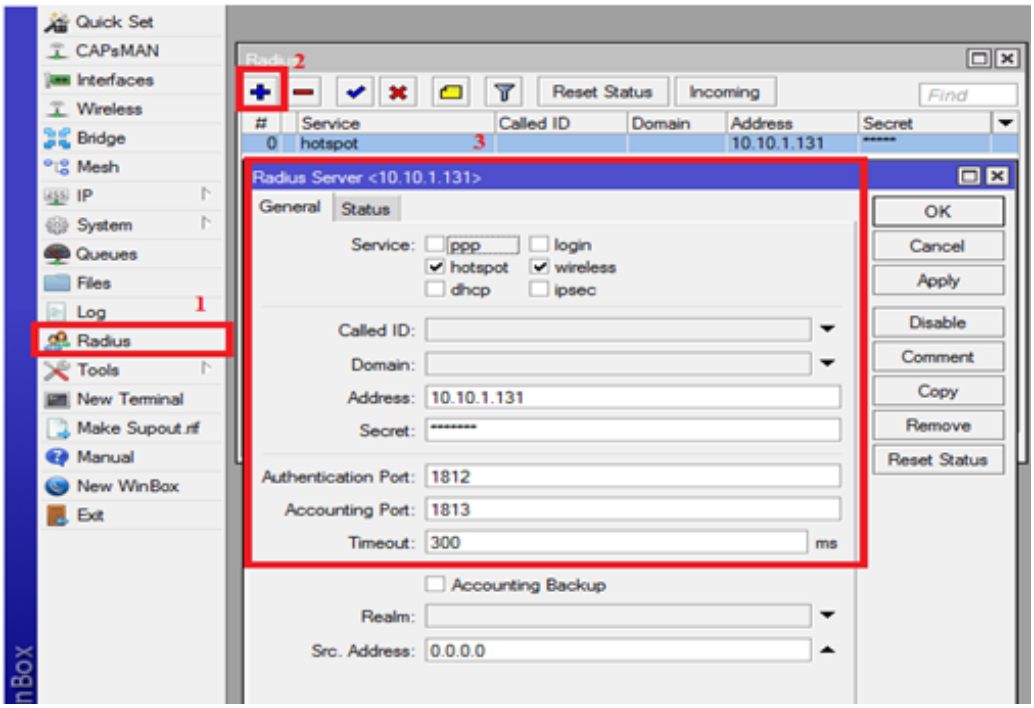


Figura 92 Cliente Radius Mikrotik

Fuente: Winbox Mikrotik

Se activa el puerto 1700 donde Mikrotik se comunica con el servidor FreeRadius para los paquetes de conexión o desconexión.

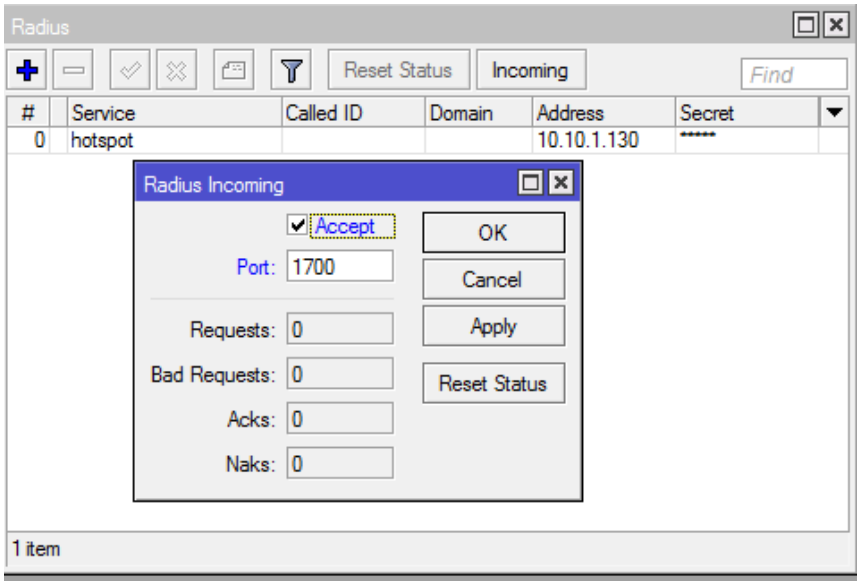


Figura 93 Radius Incoming

Fuente: Winbox Mikrotik

En el caso de que muestre un error al momento de autenticarse en el hotspot como RADIUS NOT RESPOND, se deberá verificar que con el mismo usuario no existan conexiones ya registradas, esto se puede deshabilitar mediante las pestañas del server DHCP o en la pestaña cookies del servidor hotspot.

5.4.9 Hotspot

El hotspot de Mikrotik tiene diferentes características que serán útiles para el presente proyecto, tales como prioridades de conexión, horarios de conexión para los diferentes usuarios, limitación de ancho de banda en las diferentes redes inalámbricas.

En una interfaz física se puede instalar un solo hotspot, es por eso que fue necesario la creación de varias vlans en el mismo Ethernet 2 del servidor Mikrotik, el cual permite la configuración de múltiples hotspot. En el menú principal se da click en la opción IP -> Hotspot el cual se abre la ventana de configuración del hotspot. Se comienza creando los servidores hotspot para cada Vlans, mediante la opción Hotspot Setup.

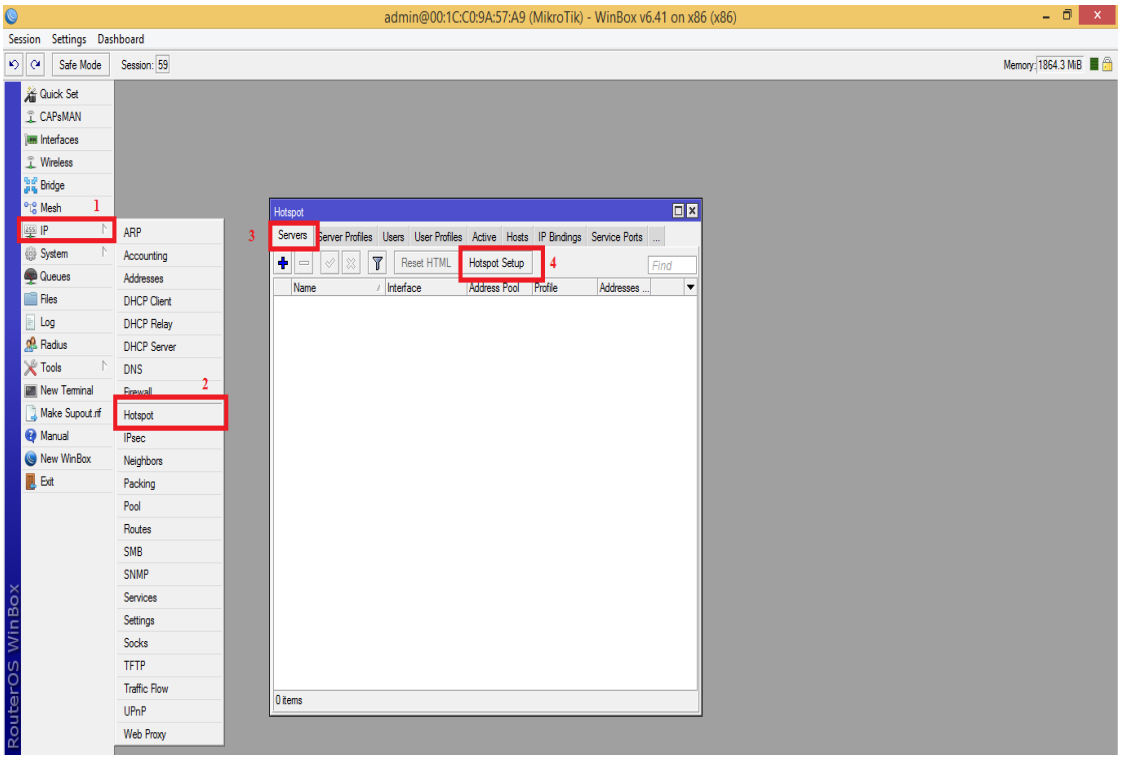


Figura 94 Hotspot Setup

Fuente: Winbox Mikrotik

Se asigna la interface bridge que se creó en cada vlan, para el presente proyecto se debe crear en el orden como se muestra en la Figura

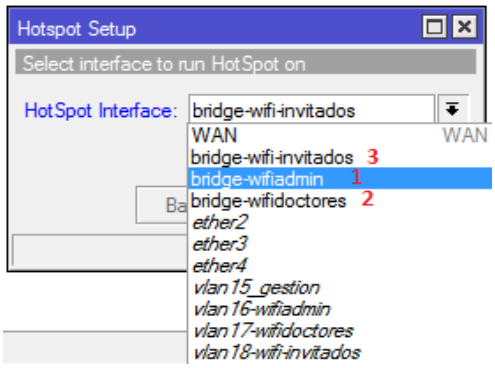


Figura 95 Interface Hotspot

Fuente: Winbox Mikrotik

Luego se asigna el Gateway del hotspot para cada usuario que se conecta, la opción de masquerade network se marca para que haga el respectivo enmascaramiento hacia internet por cada hotspot.

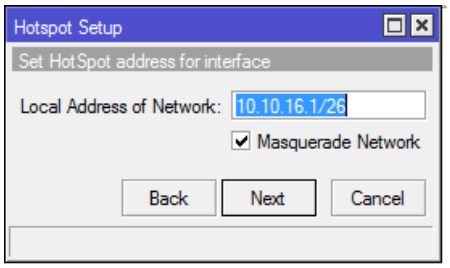


Figura 96 Gateway Hotspot

Fuente: Winbox Mikrotik

Se asigna el rango de IPs otorgado a los usuarios, en este caso se usa el mismo DHCP creado para cada una de las redes vlans.

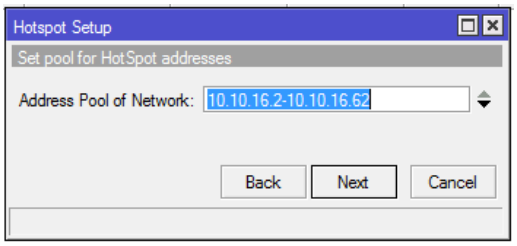


Figura 97 DHCP Hotspot

Fuente: Winbox Mikrotik

En la Figura 98 se muestra la asignación del dns name para el portal cautivo, este nombre dns aparece en el momento que un usuario se conecte a la red, el cual le pide un usuario y contraseña, en el caso de no ingresar un dns name el hotspot por defecto utiliza la dirección gateway de cada servidor.

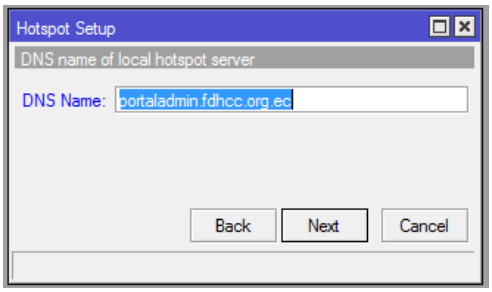


Figura 98 Dns name Hotspot

Fuente: Winbox Mikrotik

Una vez creado el servidor hotspot de la red administración, se procede a configurar también para las demás redes como se muestra en la Figura 99. En las configuraciones del servidor se deberá configurar dos opciones.

- **Addresses Per Mac:** En esta opción se define el número de direcciones mac que cuenta cada usuario, es decir el número de equipos conectados con el mismo usuario.

- **Profile:** Se define el perfil creado en la pestaña de perfil del servidor.

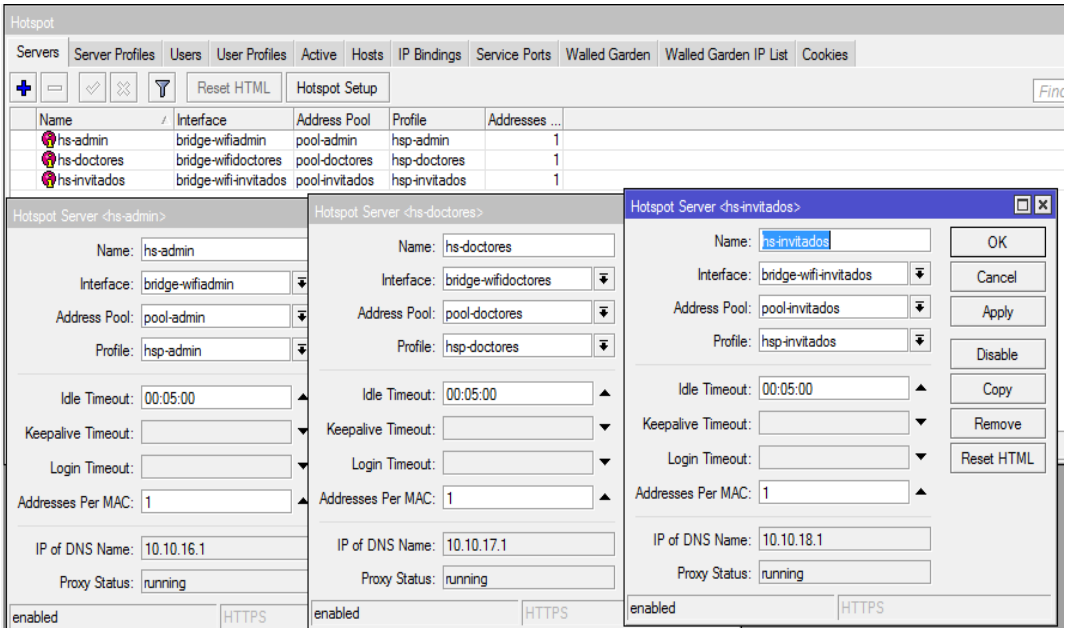


Figura 99 Server Hotspot

Fuente: Winbox Mikrotik

Antes de configurar los perfiles se personaliza la página de login que tendrá cada red inalámbrica, es por eso que en el menú principal del Winbox en la opción Files aparece las carpetas con el respectivo archivo HTML. En este caso se elaboró las páginas de inicio para cada red.

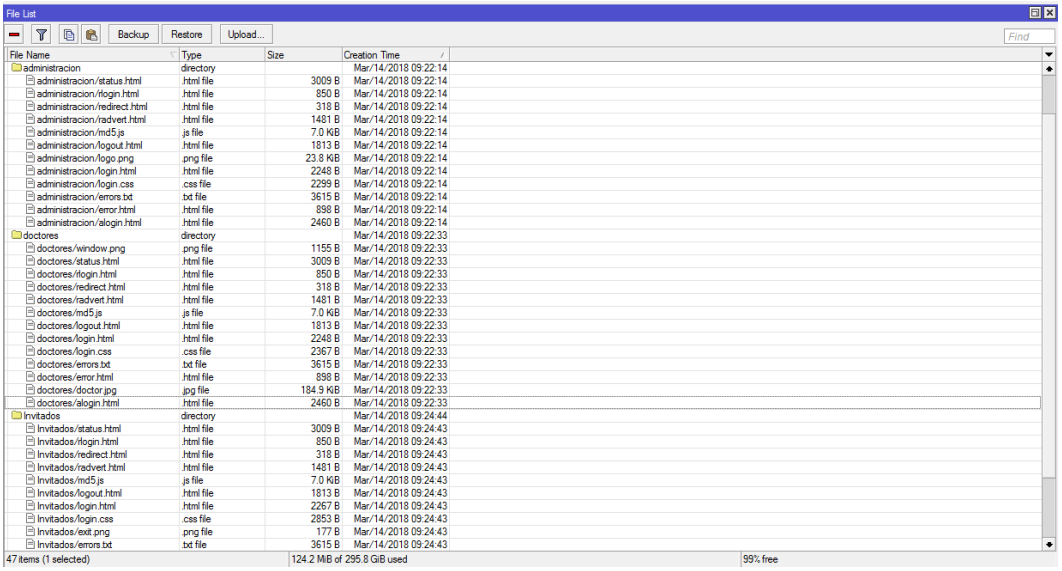


Figura 100 Html Hotspot

Fuente: Winbox Mikrotik

En la pestaña Server Profile, al crear el servidor hotspot automáticamente se crea el perfil de cada servidor, se da doble click en cada perfil y en la pestaña general de cada perfil se encuentra la opción HTML directory donde se debe seleccionar el inicio del portal cautivo que se encuentra elaborado en la carpeta File, el cual será presentado al momento de que un usuario intenta acceder a la red. También se muestra Hotspot Address, dns name configurado anteriormente para cada red.

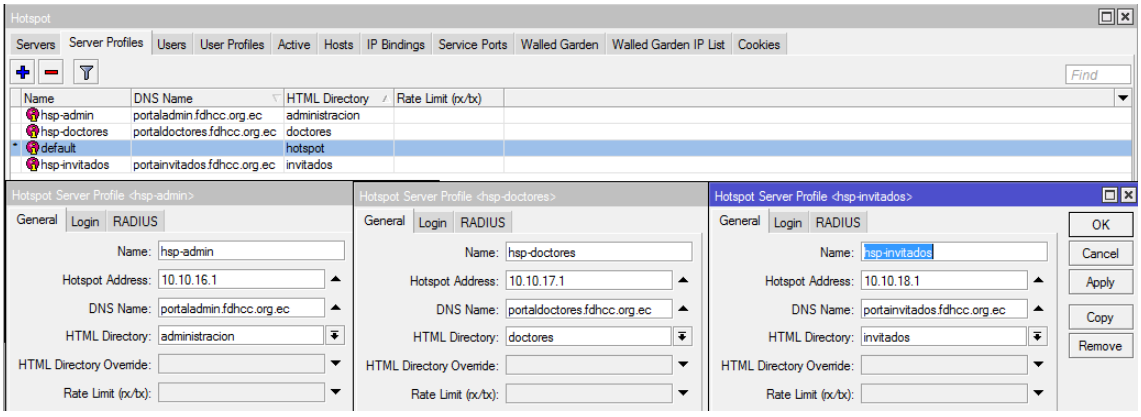


Figura 101 Server Profile Hotspot

Fuente: Winbox Mikrotik

Mikrotik por defecto tiene instalado un portal cautivo con su página de login, para este proyecto se usa páginas personalizadas creadas por diseño HTML.

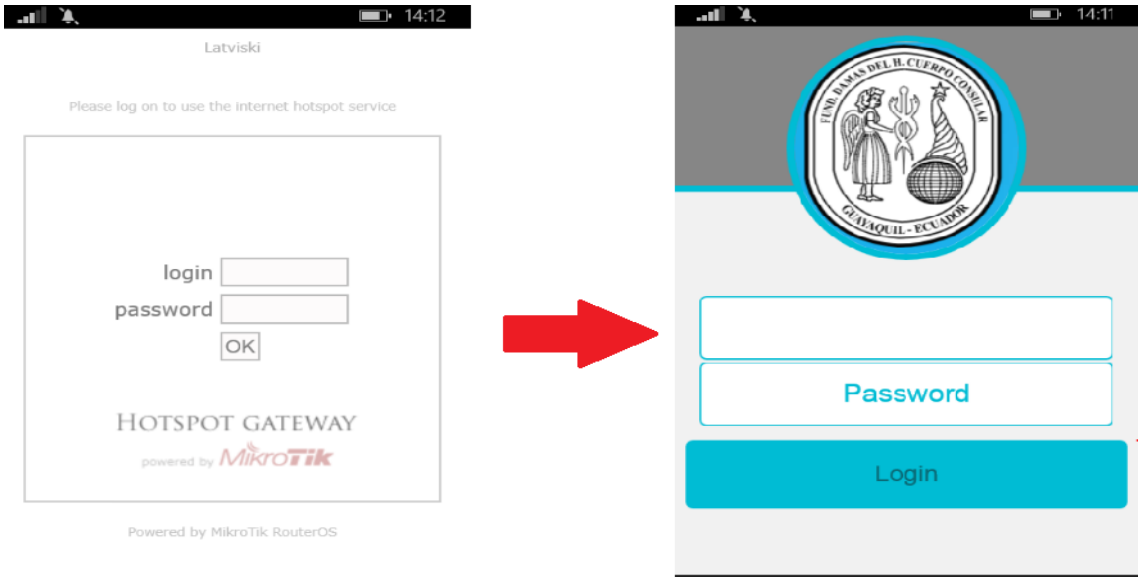


Figura 102 Login Hotspot

Fuente: Winbox Mikrotik

En cada perfil de servidor hotspot en la pestaña login se muestra diferentes métodos de autenticación.

- **HTTP PAP:** Es un método simple que pide autenticación por usuario y contraseña siendo fácil descifrar, usando programas como Wireshark que permite capturar paquetes.

- **HTTP CHAP:** Es un método igual que el anterior pero usando un algoritmo MD5 para cifrar los paquetes.

- **HTTPS**: La página de login utiliza el protocolo HTTP Secure

- **COOKIE**: Una vez que el usuario se autentique, en el servidor se almacena un cookie para que el usuario no vuelva a conectarse ingresando usuario y contraseña.

- **MAC**: En el servidor se registra la MAC para que el usuario con dicha MAC se conecte sin autenticarse.

- **TRIAL**: Por lo general este perfil se le otorga a usuarios invitados, con un tiempo de renovación para volver a conectarse o un tiempo que permanece conectado.

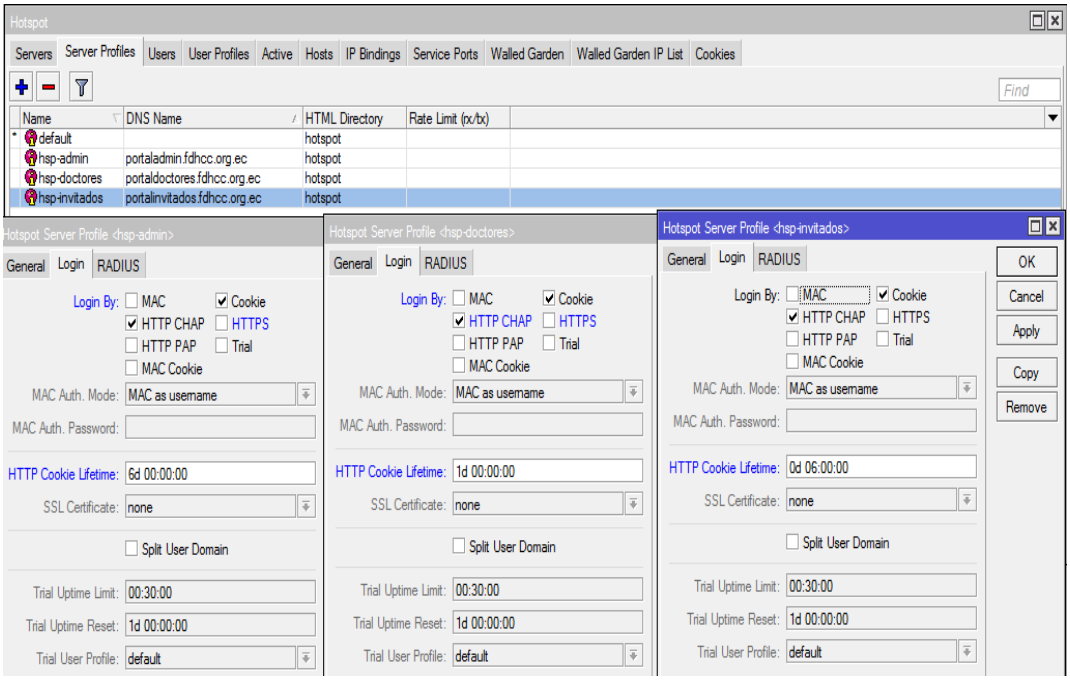


Figura 103 Server Profiles Login

Fuente: Winbox Mikrotik

Para cada servidor hotspot se define un tiempo que los cookies estarán almacenados, una vez agotado el tiempo se perderá la configuración y el hotspot volverá a solicitar usuario y contraseña.

En este caso para los usuarios de administración luego de 6 días les pedirá las credenciales siendo cada lunes de la semana en cambio a los usuarios de doctores les pedirá cada día y finalmente a los usuarios invitados cada 6 horas. En el presente proyecto no se utiliza el método trial ya que es basado solo para el personal de la

fundación. La Tabla 8 se indica que el servidor hotspot de administración tendrá una autenticación mediante el servidor Radius externo.

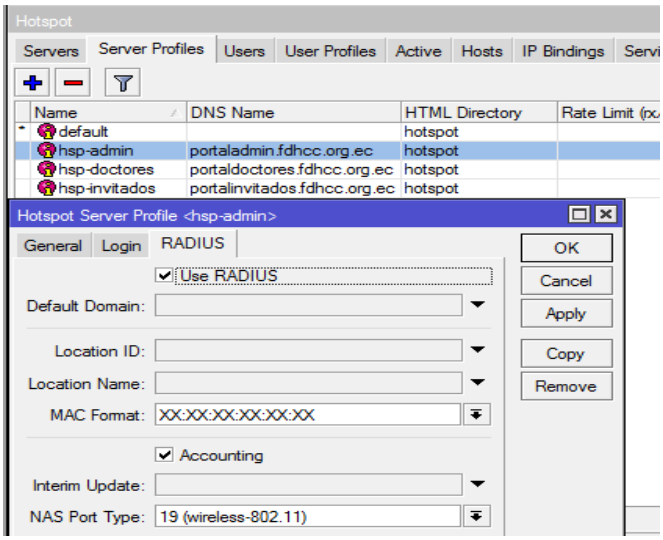


Figura 104 Autenticación Radius admin

Fuente: Winbox Mikrotik

5.4.10 Usuarios

Para la creación de los usuarios de administración se usa la herramienta phpmyadmin que permite gestionar la base de datos del servidor Radius mediante interfaz web, ingresando la dirección ip del servidor en un navegador.

Figura 105 Login phpmyadmin

Fuente: Phymyadmin

Para la creación de usuarios con su contraseña se debe ingresar los datos en la tabla radcheck.

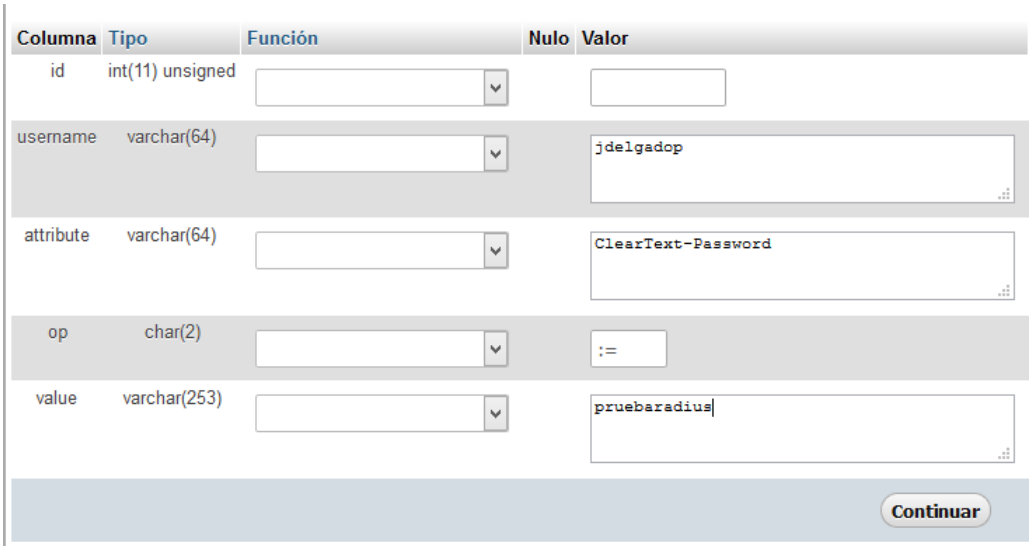


Figura 106 Creación Usuario phpmyadmin

Fuente: Phymyadmin

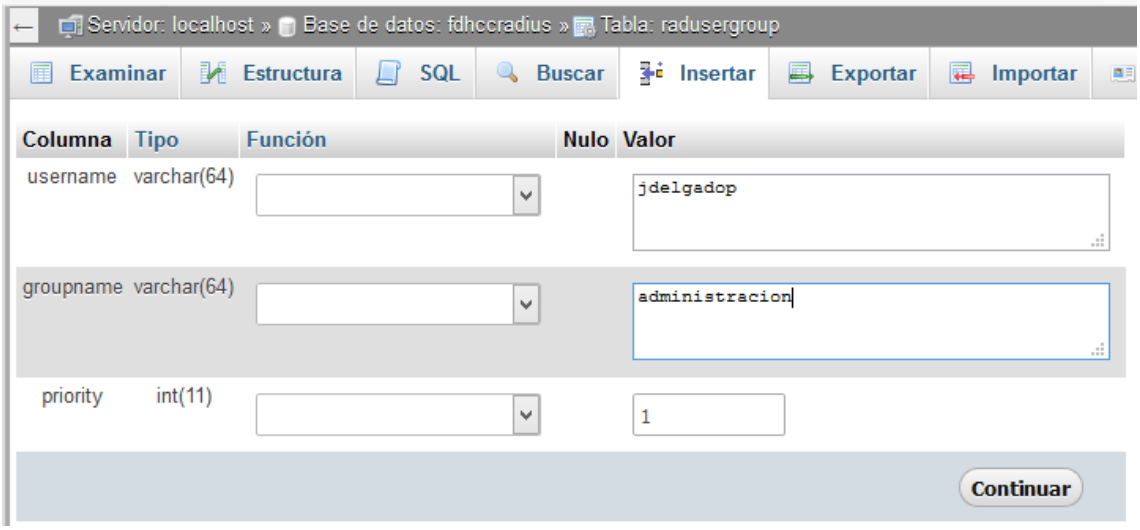


Figura 107 Creación Grupo phpmyadmin

Fuente: Phymyadmin

Luego de crear los usuarios para el grupo administración se crea a nivel local los usuarios doctores e invitados en el hotspot, por eso primeramente se crea un perfil de usuario, en estas opciones se tendrá diferentes características para los usuarios tales como control de tiempo, número de equipos conectados por usuarios,

en el caso de la limitación de velocidad no se toma en cuenta en el hotspot ya que se usa Simple Queue + PCQ.

El perfil de usuario ayuda agrupar los usuarios, en este caso los usuarios doctores e invitados tendrán ciertas características comparado a los usuarios administrativos.

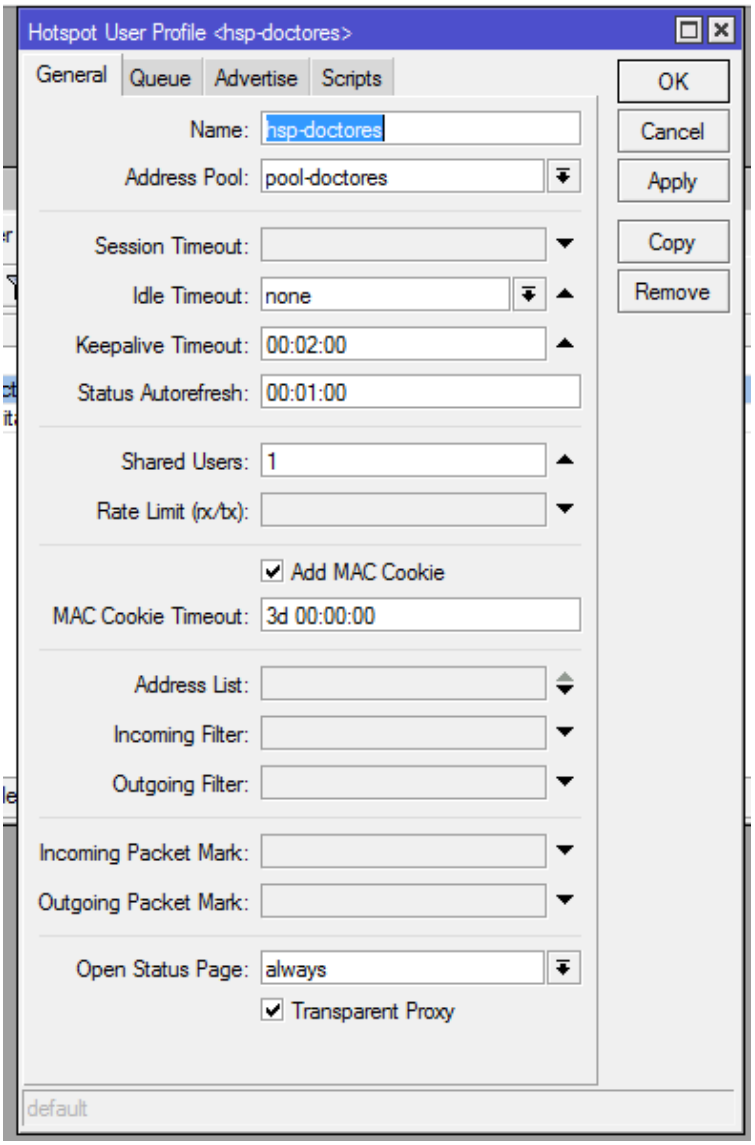


Figura 108 User Profile Hotspot

Fuente: Winbox Mikrotik

En la opción de User Profile se podrá configurar determinados tiempos tales como:

- **Session Timeout:** En este proyecto al momento de la implementación no se tomó en consideración pero esta opción sirve para darle cierto tiempo el acceso a internet, luego de un tiempo el usuario no tendrá conexión a internet

- **Idle Timeout:** Si un cliente no autorizado después del tiempo estipulado no se logra autenticar, el servidor hotspot lo desconecta de la red.

- **Shared Users**: Esta opción es importante ya que permite asignar a un usuario que se autentique en un solo dispositivo evitando que el usuario sea usado en otro dispositivo no autorizado

Usuarios Doctores e Invitados

Luego de haber creado el perfil de usuario se crea los usuarios tanto como para doctores e invitado, en el presente proyecto se crea el usuario para cada doctor con su respectiva contraseña. En la creación de cada usuario se puede asignar que dicho usuario solo se pueda conectar al hotspot teniendo una única dirección IP o el respectivo MAC Address del equipo inalámbrico.

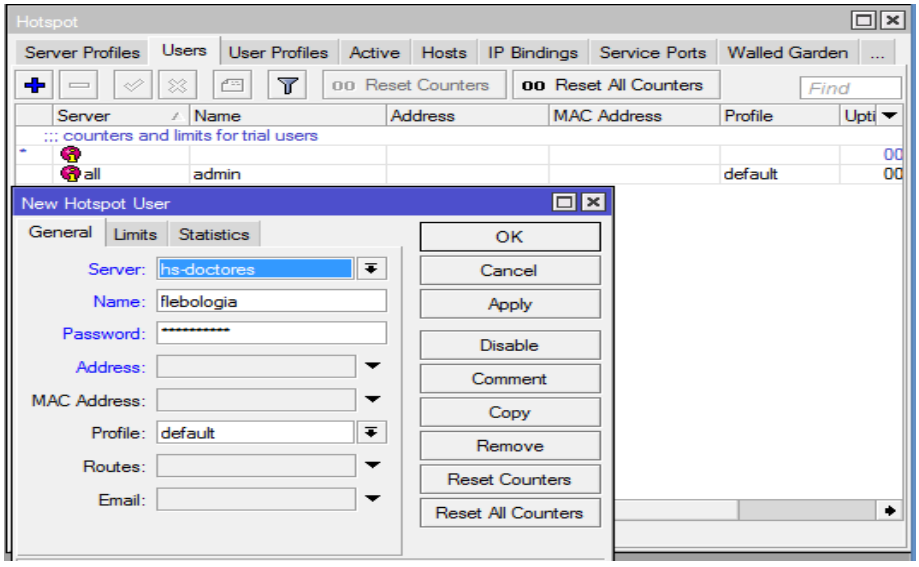


Figura 109 User Hotspot

Fuente: Winbox Mikrotik

Como monitoreo el servidor hotspot muestra una estadística de cuanto bytes el usuario ha usado en la conexión.

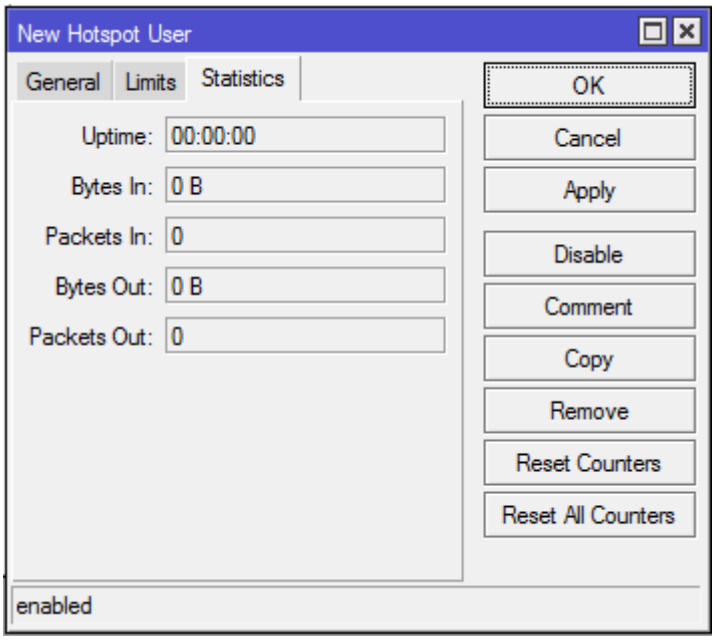


Figura 110 Monitoreo Usuarios Hotspot

Fuente: Winbox Mikrotik

Para terminar la sesión, el usuario en el navegador deberá ingresar al enlace el cual se conectan como por ejemplo portaladmin.fdhcc.org.ec/status y cerrar sesión dando click en log off.

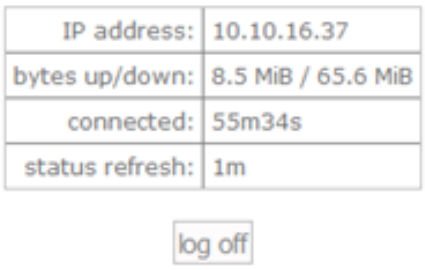


Figura 111 Log Off Hotspot

Fuente: Winbox Mikrotik

Existirán usuarios que no sigan el proceso, en esto caso desde el servidor Mikrotik en la pestaña de active y Host se podrá monitorear los usuarios conectados, si se desea desconectar a un usuario se selecciona el usuario y se lo desconecta con en el botón (-) de la parte superior. Se debe recordar que se debe eliminar de la pestaña de Cookie para que no vuelva a conectarse. La diferencia de las dos pestañas es que en la pestaña Active solo aparecen usuarios conectados satisfactoriamente con usuario y contraseña mientras en la pestaña Host aparecen usuarios que intentan acceder a la red pero no se han autenticado.

5.4.11 Walled Garden

Todos los usuarios que se conecten a la red inalámbrica podrán tener acceso a la página web de la fundación sin necesidad de autenticarse en el portal cautivo.

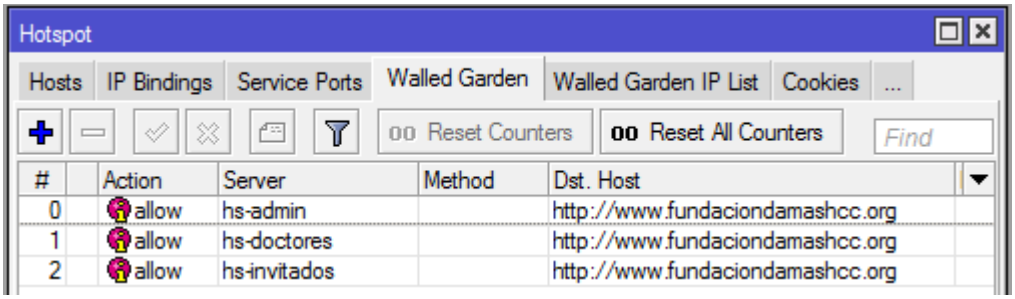


Figura 112 Walled Garden

Fuente: Winbox Mikrotik

5.4.12 IP Bindings

Existen usuarios tales como jefes o miembros del directorio de la fundación que no necesitan autenticación pero por registro será necesario que cuenten con un usuario. La pestaña de IP Bindings cuenta con diferentes acciones como bypass que permite navegación sin autenticación o el bloqueo del acceso a dispositivos inalámbricos con la dirección Mac.

Se tiene al usuario erivera que tiene como cargo Coordinadora General del centro médico sur y es miembro del directorio de la fundación por eso se le crea un usuario el cual se le asigna una dirección ip asociado a su mac address y en la pestaña de IP Bindings se le permite navegar sin necesidad de autenticarse.

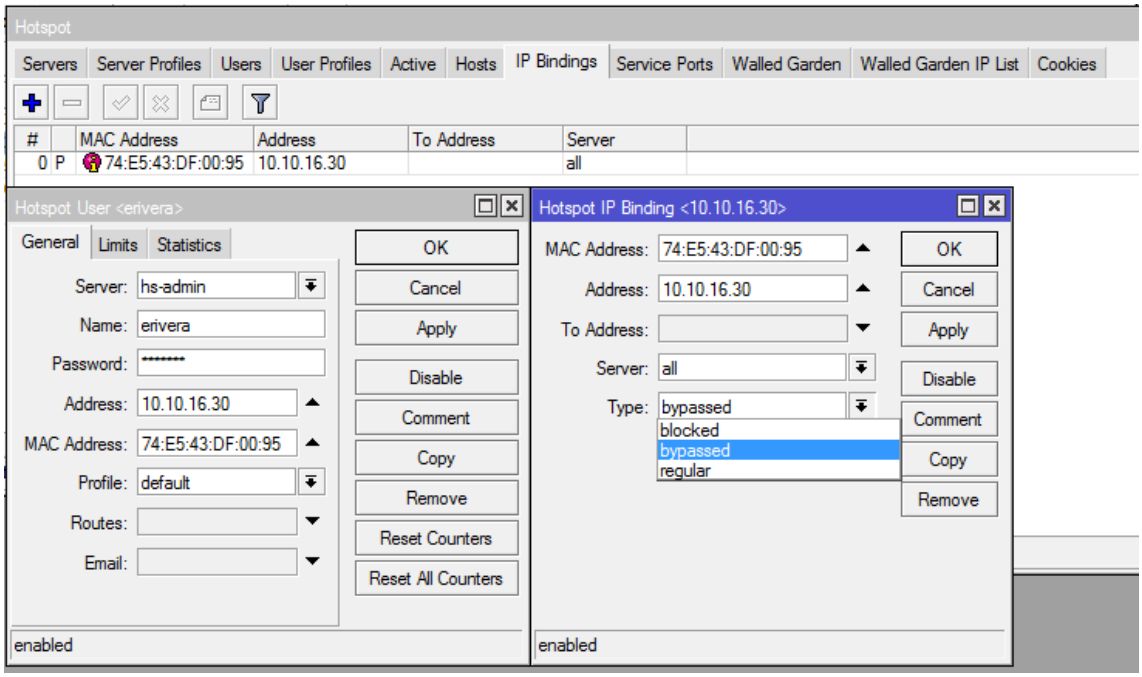


Figura 113 Ip Bindings hotspot

Fuente: Winbox Mikrotik

El usuario erivera solo podrá acceder a la red con la mac ingresada, en el caso que otro usuario intente acceder la red con el usuario erivera en otro dispositivo, se bloquea el acceso y se muestra un mensaje de error.

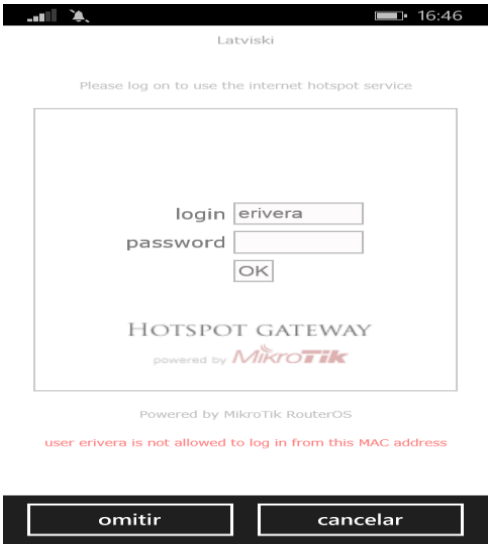


Figura 114 Denegación Acceso Usuario

Fuente: Navegador Windows Phone

5.4.13 Mecanismo de seguridad

5.4.13.1 Protección al router

Mikrotik por defecto tiene activado varios servicios y el usuario es admin sin contraseña. Lo primero que se realiza es desactivar los servicios de acceso, activando solamente el servicio winbox para la gestión y el puerto 80 para el monitoreo.

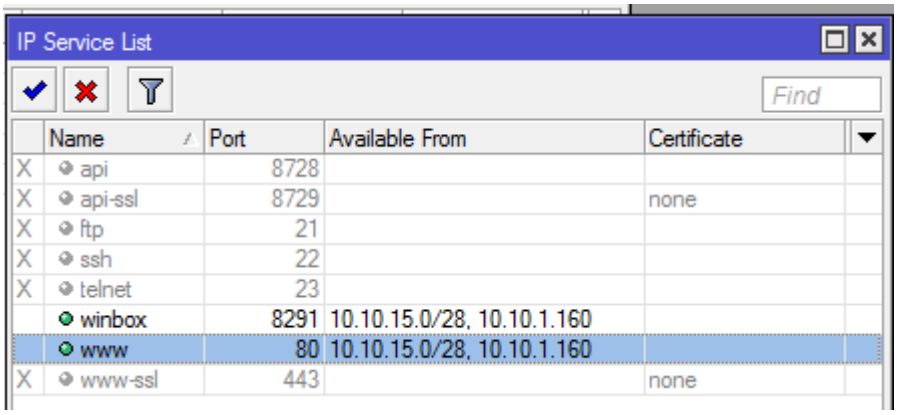


Figura 115 Servicios Mikrotik

Fuente: Winbox Mikrotik

5.4.13.2 Seguridad y configuración NAT

Algo muy importante para toda red y sobre todo en una red inalámbrica es su seguridad, uno de los mecanismos de seguridad que se optó para este proyecto es el firewall aplicando diferentes reglas. La primera configuración que se realiza en el firewall es crear reglas de NAT para poder tener salida al internet desde las diferentes redes Vlan. Se deberá realizar esta regla porque el router de borde no conoce la nueva red wifi, y tampoco existe un protocolo de enrutamiento.

En Firewall -> NAT-> + se crea las regla nat en el interfaz WAN WIFI el cual mediante ese puerto se conecta al Gateway. Mediante comandos se puede realizar el NAT como la Figura 116

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface="WAN WIFI"
```

Figura 116 Comando NAT

Fuente: Winbox Mikrotik

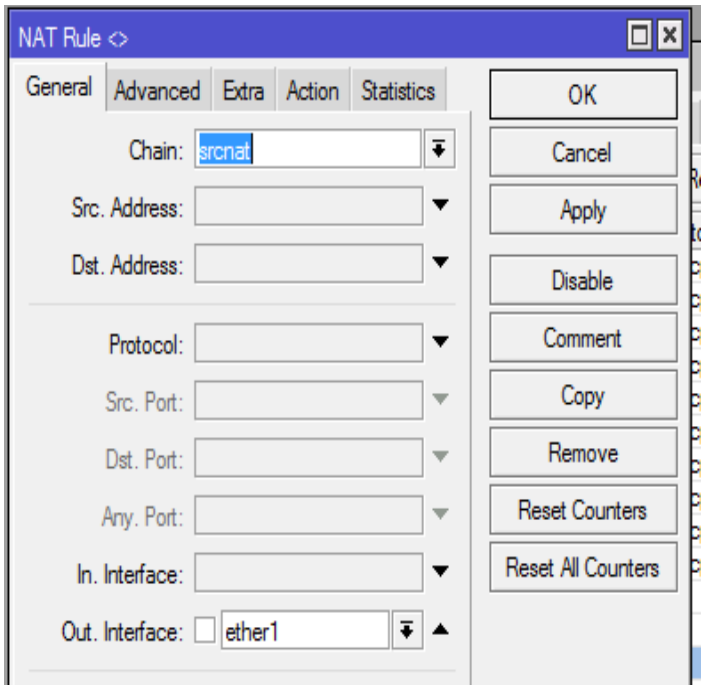


Figura 117 Chain srcnat

Fuente: Winbox Mikrotik

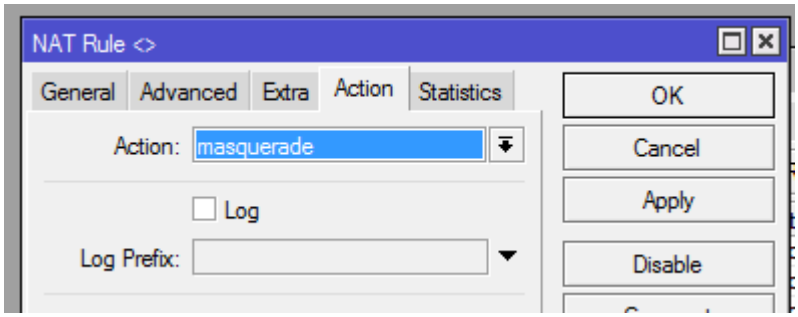


Figura 118 Action Masquerade

Fuente: Winbox Mikrotik

También se configura el enmascaramiento para las redes Vlan y para el acceso a internet.

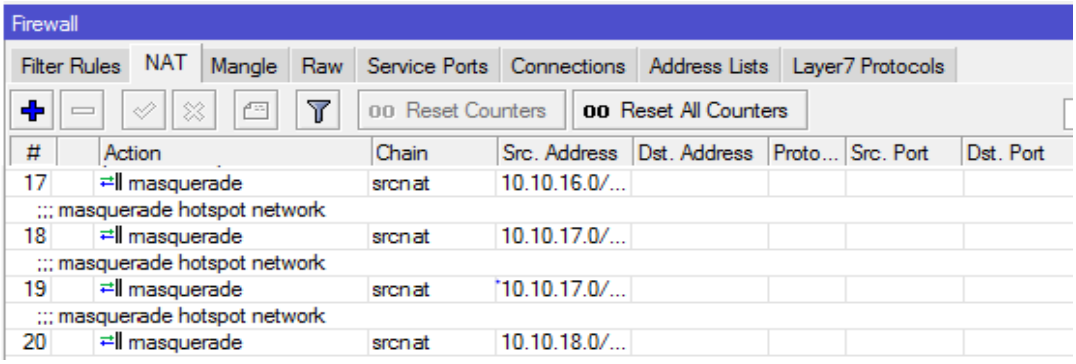


Figura 119 Nat Vlans

Fuente: Winbox Mikrotik

Una vez creado el NAT para cada red, se debe proteger al equipo Mikrotik de posibles ataques provenientes desde fuera de la red Wifi creando reglas que bloquean todo tráfico que recibe el Mikrotik.

Se permite las conexiones ya establecidas como el DNS

```
add action=accept chain=input comment="Permitir conexion" connection-state=established \
    in-interface="WAN WIFI"
```

Figura 120 Conexiones establecidas

Fuente: Winbox Mikrotik

En esta regla se permite las aplicaciones como el caso del servidor Radius tenga una conexión hacia la red LAN.

```
add action=accept chain=input comment="Permitir puertos aplicaciones" \
    connection-state=related in-interface="WAN WIFI"
```

Figura 121 Permiso Radius

Fuente: Winbox Mikrotik

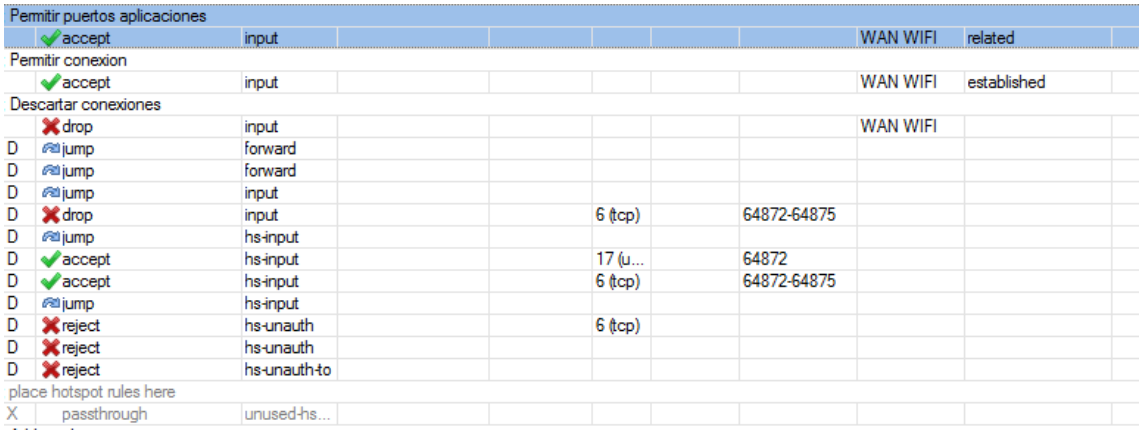
Finalmente todo lo que no esté como regla en el firewall será descartado.

```
add action=drop chain=input comment="Descartar conexiones" \
    in-interface="WAN WIFI"
```

Figura 122 Descartar conexiones

Fuente: Winbox Mikrotik

La Figura 123 muestra en modo gráfico las reglas creadas.



Permitir puertos aplicaciones								
	accept	input					WAN WIFI	related
Permitir conexion								
	accept	input					WAN WIFI	established
Descartar conexiones								
	drop	input					WAN WIFI	
D	jump	forward						
D	jump	forward						
D	jump	input						
D	drop	input			6 (tcp)		64872-64875	
D	jump	hs-input						
D	accept	hs-input			17 (u...		64872	
D	accept	hs-input			6 (tcp)		64872-64875	
D	jump	hs-input						
D	reject	hs-unauth			6 (tcp)			
D	reject	hs-unauth						
D	reject	hs-unauth-to						
place hotspot rules here								
X	passthrough	unused-hs...						

Figura 123 Reglas evitar ataques

Fuente: Winbox Mikrotik

5.4.13.3 Address List

Otra herramienta importante permitida del firewall de Mikrotik es crear un address list con el uso de firewall filter, esta herramienta ayuda a crear listas de direcciones IP y asignar reglas para diferentes acciones. Para tener un registro de cuantos equipos se conectan a cada ssid, mediante la creación de un address list se podrá tener un registro de equipos conectados a cada SSID, configurado mediante una cadena forward que indique la acción de agregar un address list con el nombre de equipos registrados Admin.

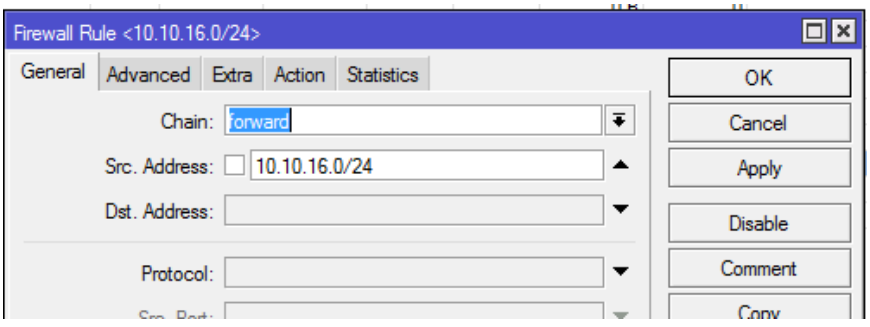


Figura 124 Address List admin

Fuente: Winbox Mikrotik

La figura 125 se indica la acción que toma cada regla.

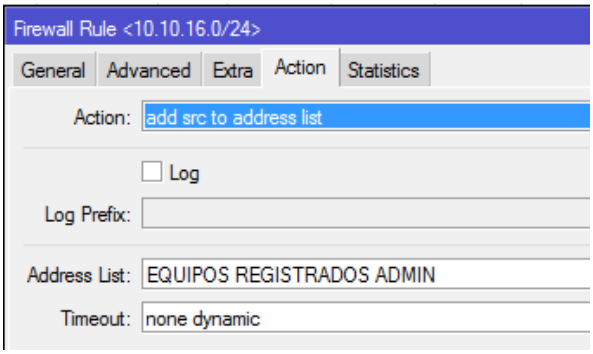


Figura 125 Acción Access List

Fuente: Winbox Mikrotik

Se debe crear para red Vlan un address list, y así se podrá tener detallado los equipos que se conectan en cada red.

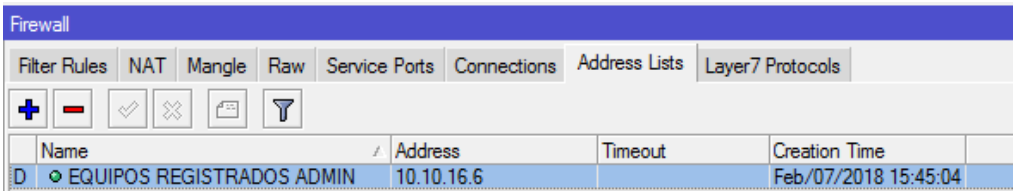


Figura 126 Pestaña Address List

Fuente: Winbox Mikrotik

5.4.13.4 Bloqueo Puertos

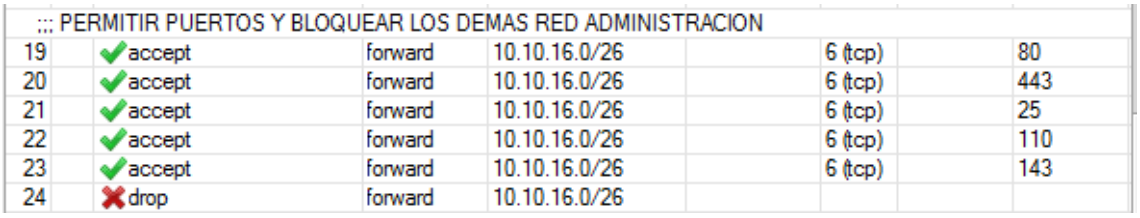
Para seguridad dentro de la red wifi se optó por permitir el uso a determinados puertos en cada red Vlan, definido de la siguiente manera.

Tabla 13 Bloqueo Puertos

Puertos	Administración	Doctores	Invitados
HTTP (80)	x	x	x
HTTPS (443)	x	x	x
SMTP (25)	x		
POP3 (110)	x		
IMAP (243)	x		

Elaborado: Autor

Red Administración

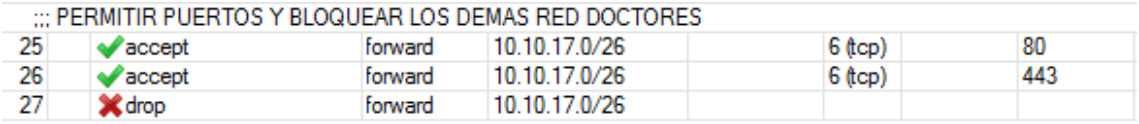


;;; PERMITIR PUERTOS Y BLOQUEAR LOS DEMAS RED ADMINISTRACION						
19	accept	forward	10.10.16.0/26		6 (tcp)	80
20	accept	forward	10.10.16.0/26		6 (tcp)	443
21	accept	forward	10.10.16.0/26		6 (tcp)	25
22	accept	forward	10.10.16.0/26		6 (tcp)	110
23	accept	forward	10.10.16.0/26		6 (tcp)	143
24	drop	forward	10.10.16.0/26			

Figura 127 Bloqueo Puertos Admin

Fuente: Winbox Mikrotik

Red Doctores



;;; PERMITIR PUERTOS Y BLOQUEAR LOS DEMAS RED DOCTORES						
25	accept	forward	10.10.17.0/26		6 (tcp)	80
26	accept	forward	10.10.17.0/26		6 (tcp)	443
27	drop	forward	10.10.17.0/26			

Figura 128 Bloqueo Puertos Doctores

Fuente: Winbox Mikrotik

Red Invitados

;;; PERMITIR PUERTOS Y BLOQUEAR LOS DEMAS RED INVITADOS						
28	accept	forward	10.10.18.0/28		6 (tcp)	80
29	accept	forward	10.10.18.0/28		6 (tcp)	443
30	drop	forward	10.10.18.0/28			

Figura 129 Bloqueo Puertos Invitados

Fuente: Winbox Mikrotik

5.4.13.5 Bloqueo Páginas Web

Tabla 14 Prioridades de acceso

Grupo de Usuario	Navegación	Facebook	YouTube	WhatsApp	Adultos
Administrativo	SI	NO	NO	SI	NO
Doctores	SI	NO	NO	SI	NO
Invitados	SI	SI	NO	SI	NO

Elaborado: Autor

Para realizar el bloqueo de las diferentes páginas se hará con el comando ip firewall filter como muestra la Figura 130, bloqueando mediante contenido a todas las redes.

```
/ip firewall filter
add action=drop chain=forward content=facebook src-address=10.10.16.0

[admin@MikroTik] /ip firewall filter> add action=drop chain=forward content=porn src-address=10.10.16.0
```

Figura 130 Comando Bloqueos Páginas

Fuente: Winbox Mikrotik

Como indica la Figura 131, para las redes sociales como youtube y facebook se realiza un bloqueo solo en horario de trabajo, en la misma regla creada se asigna el horario de bloqueo.

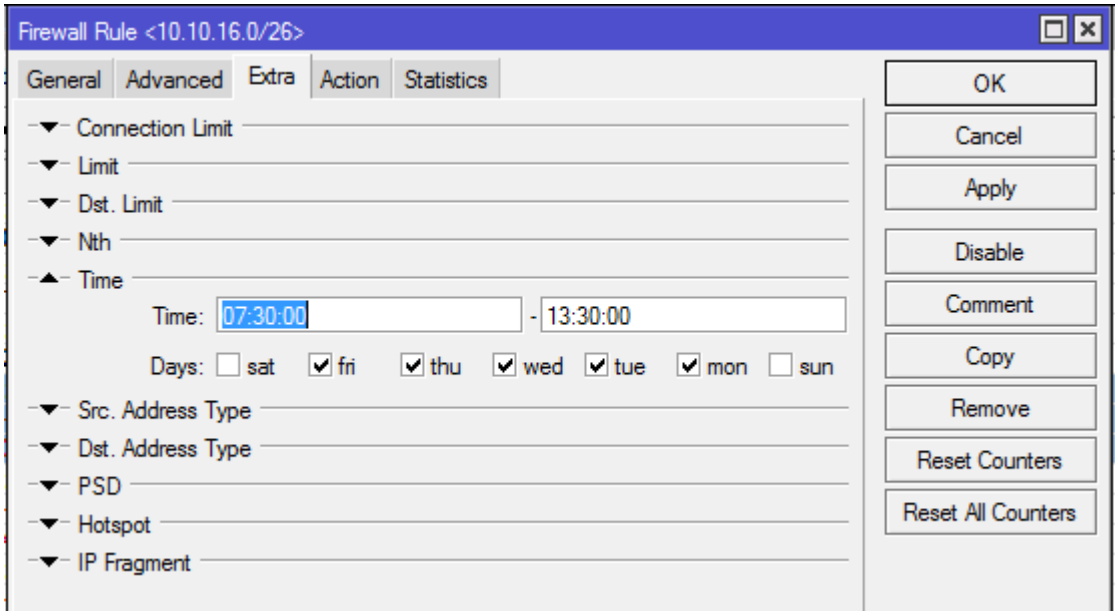


Figura 131 Tiempo Activo Bloqueo

Fuente: Winbox Mikrotik

5.4.13.6 Bloqueo Descargas

Para la opción de descarga se coloca la dirección ip en Dst address ya que son paquetes entrantes al router cuando se realiza una descarga.

```
/ip firewall filter
add action=drop chain=forward comment="Bloqueo Descargas ADMIN" content=.dat \
    dst-address=10.10.16.0/26
add action=drop chain=forward content=.exe dst-address=10.10.16.0/26
add action=drop chain=forward content=.iso dst-address=10.10.16.0/26
add action=drop chain=forward content=.cab dst-address=10.10.16.0/26
add action=drop chain=forward content=.gz dst-address=10.10.16.0/26
add action=drop chain=forward content=.mp3 dst-address=10.10.16.0/26
add action=drop chain=forward content=.mp4 dst-address=10.10.16.0/26
add action=drop chain=forward content=.mpeg dst-address=10.10.16.0/26
add action=drop chain=forward content=.flv dst-address=10.10.16.0/26
add action=drop chain=forward content=.swf dst-address=10.10.16.0/26
add action=drop chain=forward content=.avi dst-address=10.10.16.0/26
add action=drop chain=forward content=.wav dst-address=10.10.16.0/26
add action=drop chain=forward content=.wma dst-address=10.10.16.0/26
add action=drop chain=forward content=.wmv dst-address=10.10.16.0/26
add action=drop chain=forward comment="BLOQUEO DOCTORES" content=.dat \
    dst-address=10.10.17.0/26
add action=drop chain=forward content=.exe dst-address=10.10.17.0/26
add action=drop chain=forward content=.cab dst-address=10.10.17.0/26
add action=drop chain=forward content=.gz dst-address=10.10.17.0/26
add action=drop chain=forward content=.mp3 dst-address=10.10.17.0/26
add action=drop chain=forward content=.mp4 dst-address=10.10.17.0/26
add action=drop chain=forward content=.mpeg dst-address=10.10.17.0/26
add action=drop chain=forward content=.flv dst-address=10.10.17.0/26
add action=drop chain=forward content=.swf dst-address=10.10.17.0/26
add action=drop chain=forward content=.avi dst-address=10.10.17.0/26
add action=drop chain=forward content=.wav dst-address=10.10.17.0/26
add action=drop chain=forward content=.wma dst-address=10.10.17.0/26
add action=drop chain=forward content=.wmv dst-address=10.10.17.0/26
```

Figura 132 Bloqueo Descargas

Fuente: Winbox Mikrotik

5.4.13.7 Bloqueo Usuarios

Existen métodos para bloquear a usuarios el acceso a internet como por IP Bindings o firewall. En el firewall se ingresa el comando ip firewall filter que indica la acción de bloqueo a la mac-address correspondiente, para que no exista conflictos con las demás reglas del firewall siempre se coloca como primera regla los bloqueos hacia usuarios.

```
[lpina@CCR-GPON] >
[lpina@CCR-GPON] > ip firewall filter add chain=forward src-mac-address=aa:bb:cc:dd:ee:ff action=drop comment="bloqueo de prueba"
[lpina@CCR-GPON] >
```

Figura 133 Bloqueo Usuario

Fuente: Winbox Mikrotik

5.4.13.8 ARP

Según la Tabla 11, se indica la dirección IP de cada cap, para realizar el amarrado de Ip/Mac y evitar que el cap pierda la configuración por conflicto de IPs.

Se configura en la opción IP-> ARP y se procede a configurar la IP address con la MAC Address de cada cap.

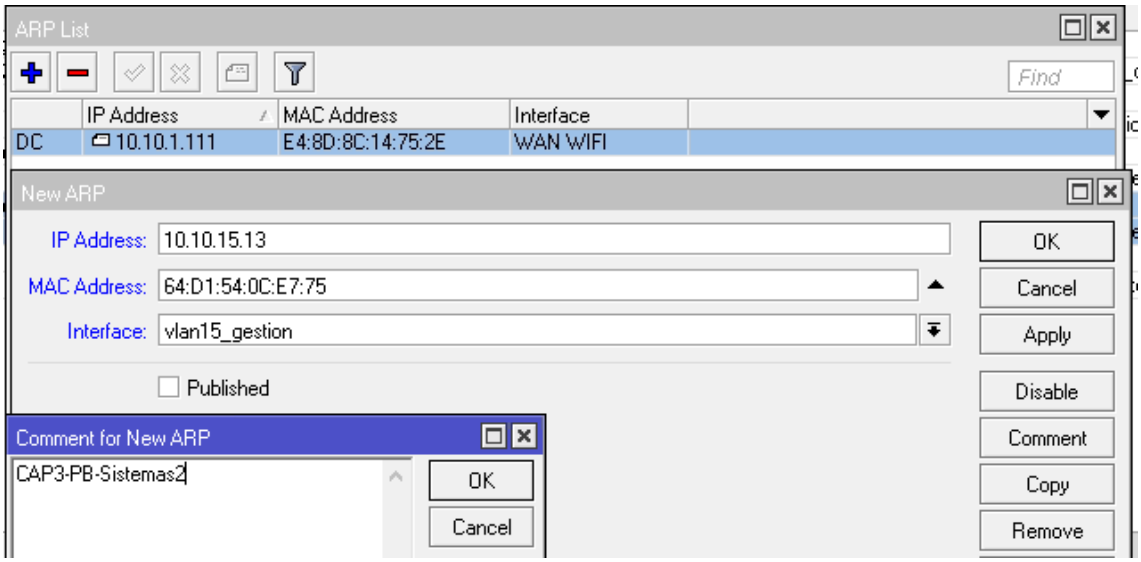


Figura 134 Tabla Arp

Fuente: Winbox Mikrotik

5.4.14 Calidad de Servicio

Para toda red inalámbrica es primordial el manejo del ancho de banda por medio de colas simples con algoritmo PCQ se puede llevar un control. Se crean reglas asignando a los dispositivos inalámbricos un ancho de banda equitativo entre todos los dispositivos conectados ya que no todos los usuarios navegan al mismo tiempo. Para el presente proyecto se asignó un ancho de banda según el grupo de usuario

Tabla 15 Asignación Ancho Banda

Grupo de Usuario	Ancho de banda Asignado
Administrativo	3 Megas
Doctores	2 Megas
Invitados	1 Mega

Elaborado: Autor

Como indica la tabla 15, si para usuarios administrativos se cuenta con 3 megas y tenemos 3 usuarios conectados, el Queues del servidor Mikrotik compartirá dicho ancho de banda en todos los usuarios, asignándole a cada usuario un ancho de banda 1024Kb.

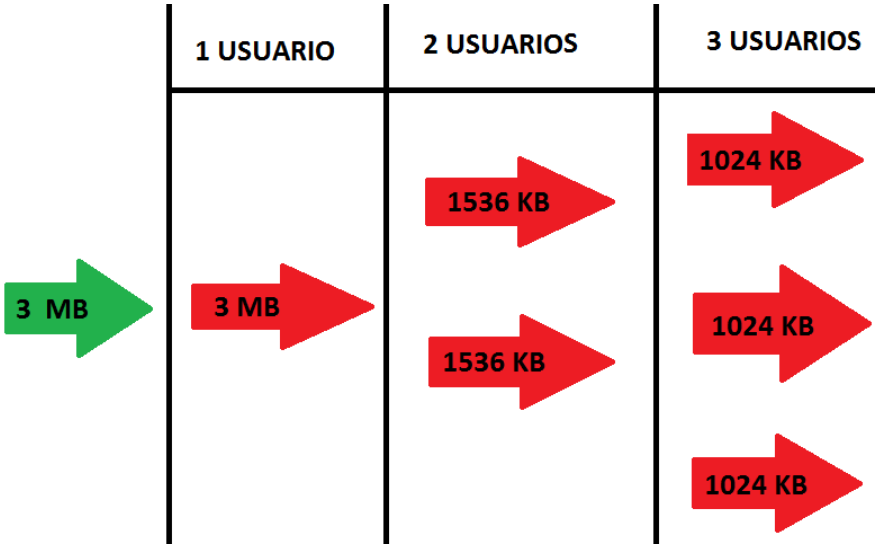


Figura 135 PCQ

Elaborado: Autor

Fuente: (Mikrotik Documentation, 2015)

Primero se crea reglas de descarga y subida. Para la opción de descarga se coloca Dst address ya que son paquetes entrantes al router, pero para la opción de subida sería lo contrario, seleccionando src address por ser todo lo que sale desde el router.

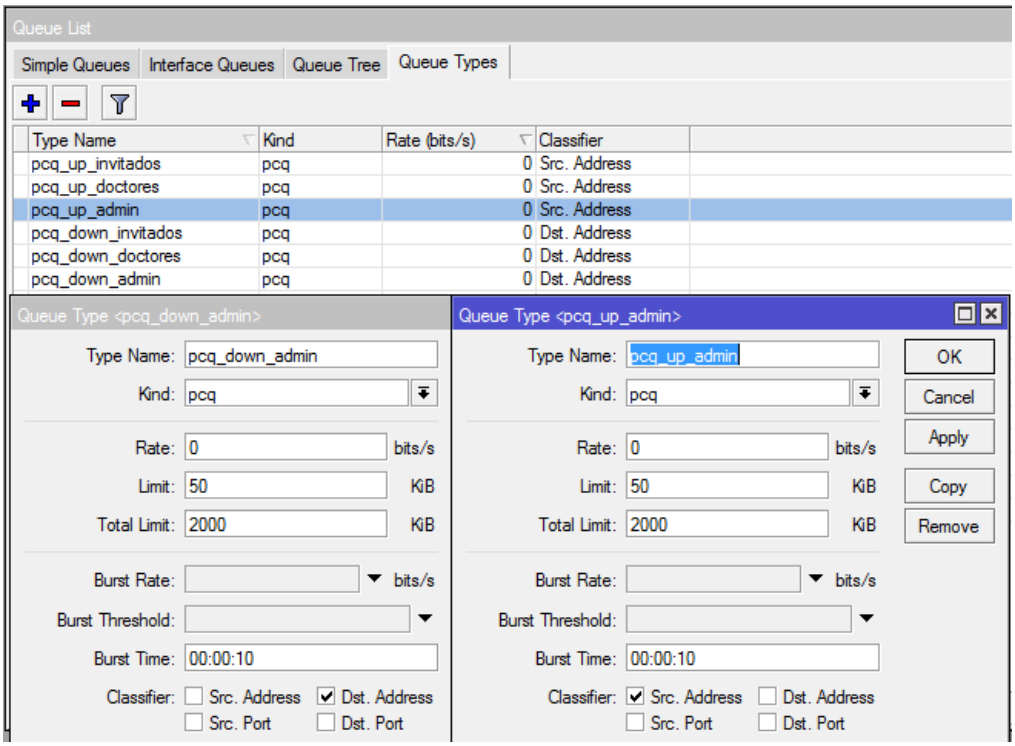


Figura 136 Queue Types

Fuente: Winbox Mikrotik

Se crea una cola simple indicando la interfaz que se desea regular, seleccionando en la opción de target, en este caso se debe hacer el mismo procedimiento para cada interfaz bridge. El Max Limit indica el ancho de banda total usado para cada red.

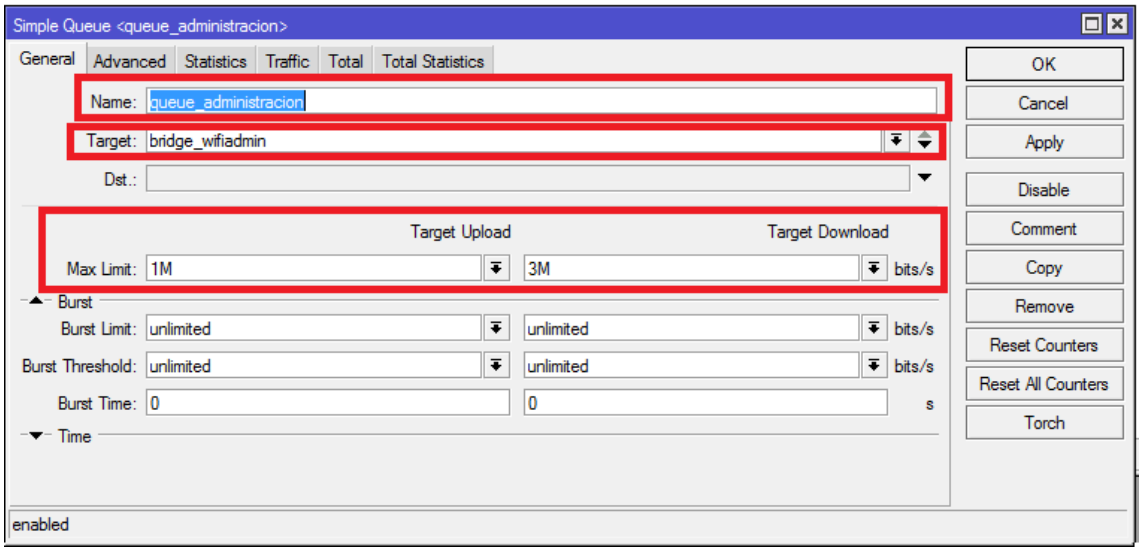


Figura 137 Simple Queue

Fuente: Winbox Mikrotik

Para calidad de servicio se puede usar QUEUE SIMPLE asignando a cada cliente un ancho de banda pero consume recursos del equipo y por eso se opta por balanceo PCQ, donde se podrá distribuir la velocidad de una manera igual y organizada a todos los usuarios conectados. Por ultimo en cada cola simple se escoge el tipo de cola creado.

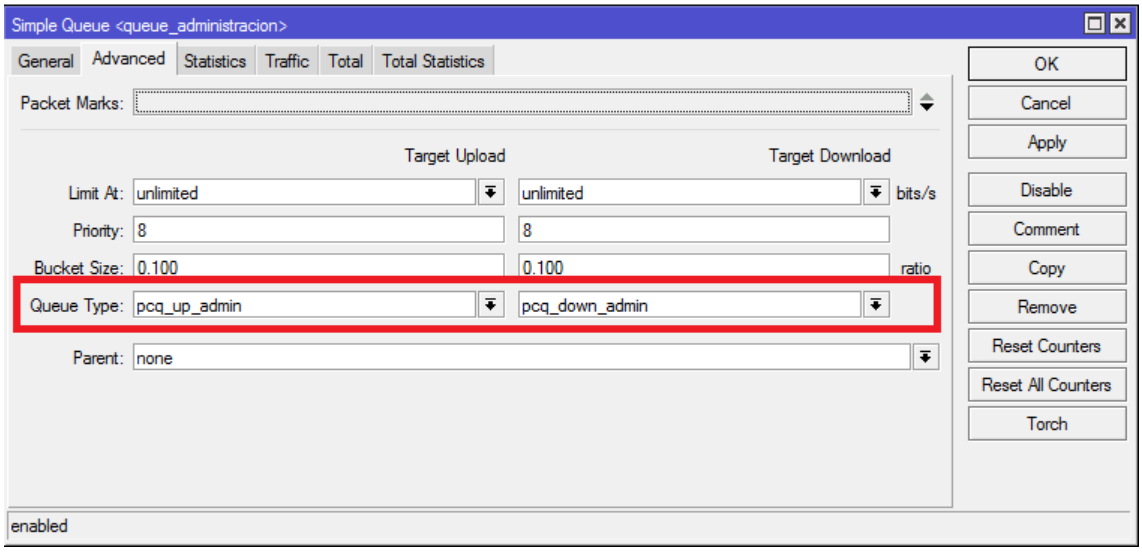


Figura 138 Simple Queue Advanced

Fuente: Winbox Mikrotik

En el caso de que existan usuarios que requieran otra cantidad de ancho de banda, se debe crear un diferente plan de velocidad asociando con un nuevo pcq creado con su respectiva mac address o dirección Ip.

5.5.15 Configuración Switch

La configuración será la misma para el switch de planta alta como planta baja, el esquema será como muestra la Figura 19. Los switches de Mikrotik trabajan en la capa de enlace de datos y por defecto usan protocolo RSTP.

Se crea las vlans para cada interfaz en la opción “interface” del menú principal y luego en la pestaña Vlan se asigna nombre, id de la Vlan y la interfaz correspondiente. Se configura el puerto ether 1 de cada switch en modo troncal y

para los puertos ether 2, 3, 4, 5 se configura en puertos híbridos permitiendo llevar Vlans troncales pero a la vez se puede tener un equipo en modo acceso.

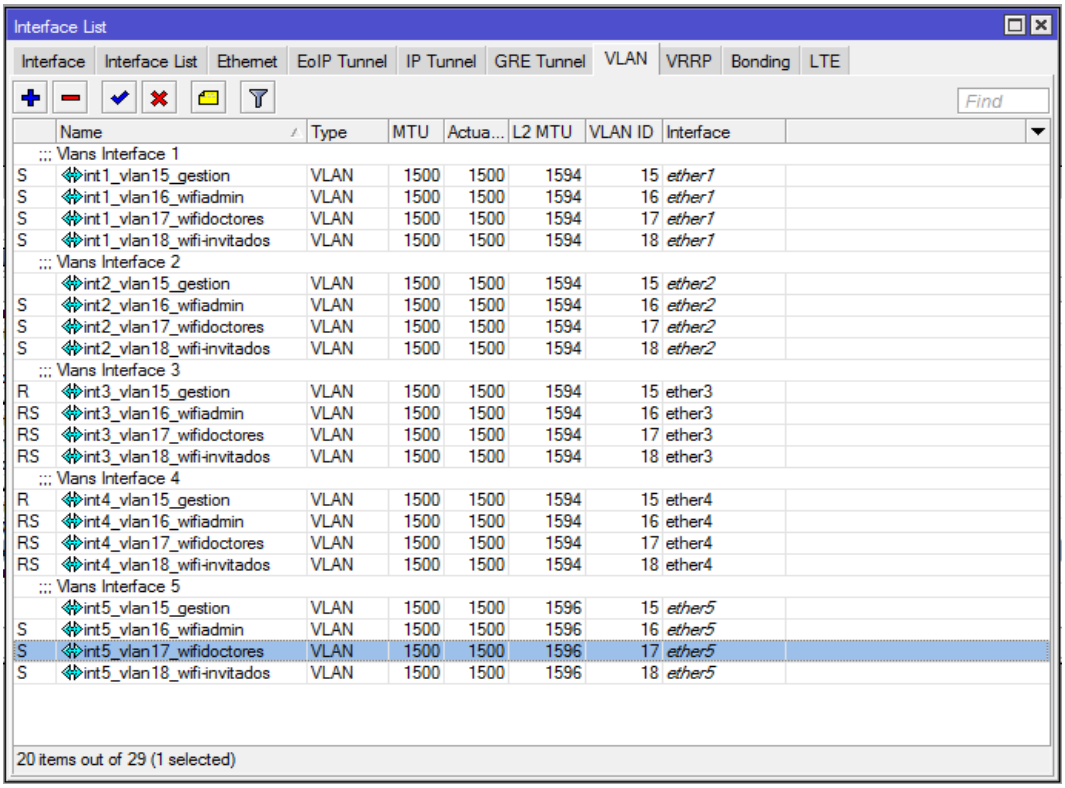


Figura 139 Creación Vlans

Fuente: Winbox Mikrotik

Una vez creada las vlans se crea bridges para cada una (Figura 140) y se asigna las interfaces de Vlan e interfaces Ethernet donde se conecta el tráfico sin etiquetar.

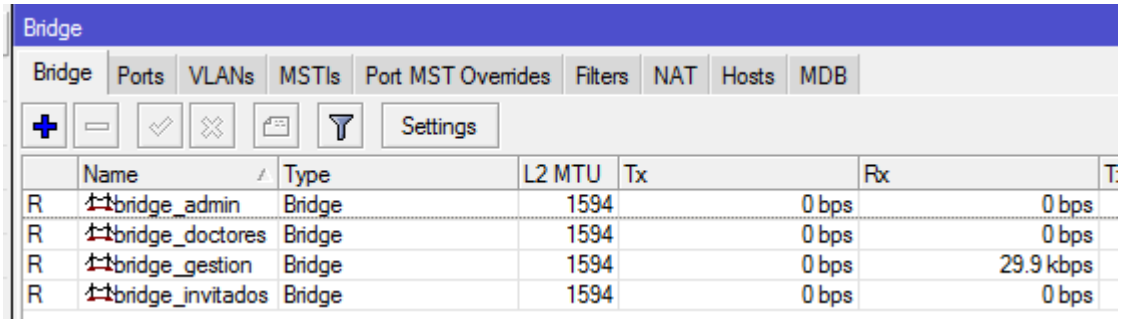
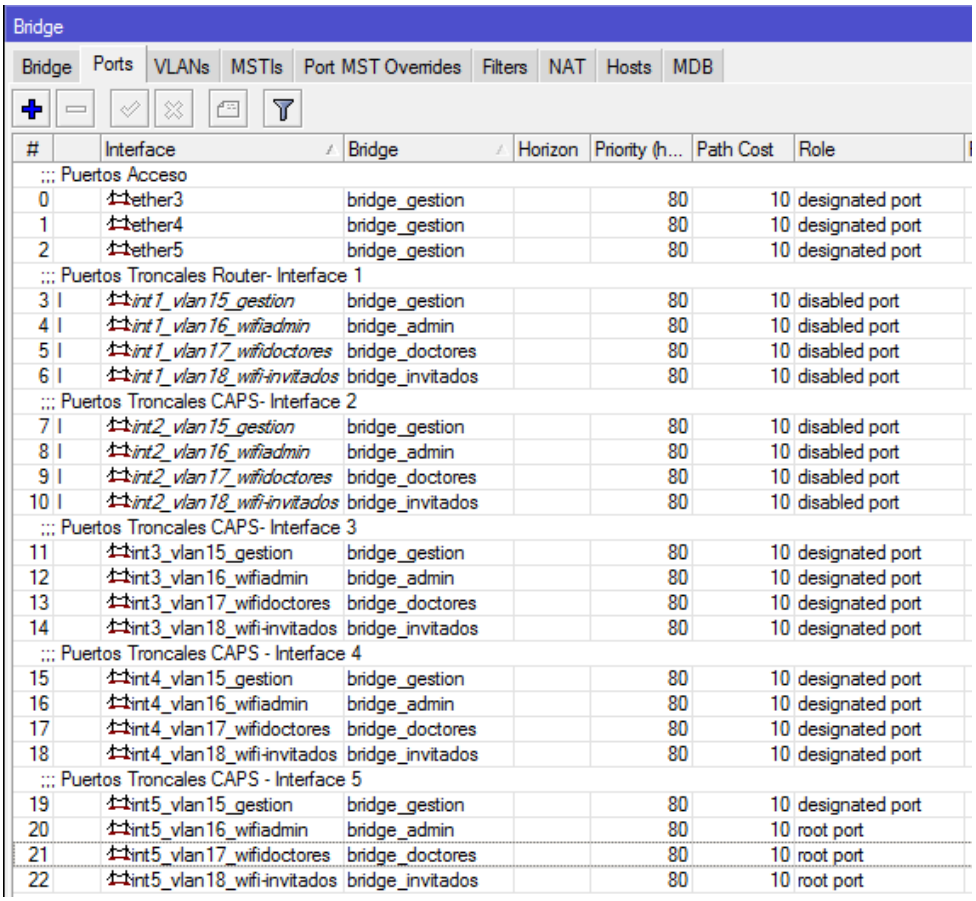


Figura 140 Creación Bridge

Fuente: Winbox Mikrotik



#	Interface	Bridge	Horizon	Priority (h...	Path Cost	Role
;;; Puertos Acceso						
0	ether3	bridge_gestion		80	10	designated port
1	ether4	bridge_gestion		80	10	designated port
2	ether5	bridge_gestion		80	10	designated port
;;; Puertos Troncales Router- Interface 1						
3	int1_vlan15_gestion	bridge_gestion		80	10	disabled port
4	int1_vlan16_wifiadmin	bridge_admin		80	10	disabled port
5	int1_vlan17_wifidoctores	bridge_doctores		80	10	disabled port
6	int1_vlan18_wifi-invitados	bridge_invitados		80	10	disabled port
;;; Puertos Troncales CAPS- Interface 2						
7	int2_vlan15_gestion	bridge_gestion		80	10	disabled port
8	int2_vlan16_wifiadmin	bridge_admin		80	10	disabled port
9	int2_vlan17_wifidoctores	bridge_doctores		80	10	disabled port
10	int2_vlan18_wifi-invitados	bridge_invitados		80	10	disabled port
;;; Puertos Troncales CAPS- Interface 3						
11	int3_vlan15_gestion	bridge_gestion		80	10	designated port
12	int3_vlan16_wifiadmin	bridge_admin		80	10	designated port
13	int3_vlan17_wifidoctores	bridge_doctores		80	10	designated port
14	int3_vlan18_wifi-invitados	bridge_invitados		80	10	designated port
;;; Puertos Troncales CAPS - Interface 4						
15	int4_vlan15_gestion	bridge_gestion		80	10	designated port
16	int4_vlan16_wifiadmin	bridge_admin		80	10	designated port
17	int4_vlan17_wifidoctores	bridge_doctores		80	10	designated port
18	int4_vlan18_wifi-invitados	bridge_invitados		80	10	designated port
;;; Puertos Troncales CAPS - Interface 5						
19	int5_vlan15_gestion	bridge_gestion		80	10	designated port
20	int5_vlan16_wifiadmin	bridge_admin		80	10	root port
21	int5_vlan17_wifidoctores	bridge_doctores		80	10	root port
22	int5_vlan18_wifi-invitados	bridge_invitados		80	10	root port

Figura 141 Puertos Bridge Switch Planta Alta

Fuente: Winbox Mikrotik

Se asigna la dirección IP correspondiente a cada switch, en el menú principal se da click en ip>address y se agrega una ip en la interface bridge de la Vlan gestión

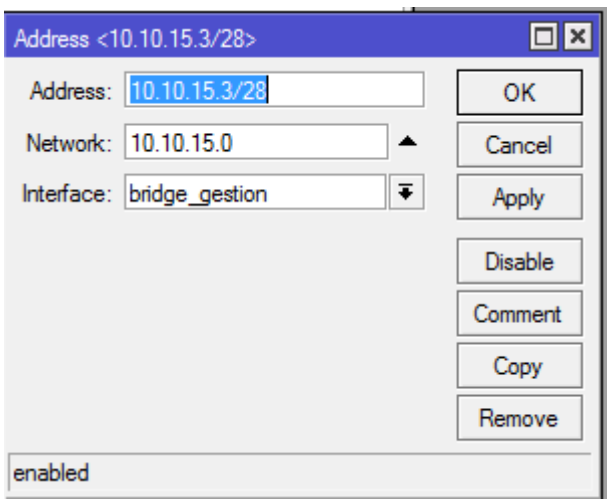


Figura 142 Asignación dirección IP Switch Planta Baja

Fuente: Winbox Mikrotik

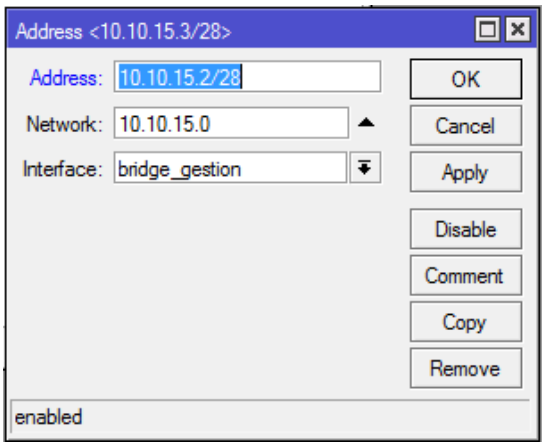


Figura 143 Asignación dirección IP Switch Planta Alta

Fuente: Winbox Mikrotik

5.5.15 Monitoreo

5.5.15.1 Syslog

Mikrotik incorpora un Sistema de log en sus equipos pero se almacenan temporalmente con el problema de que al reiniciar el equipo o pasado cierto tiempo estos se van borrando. Es por eso que se opta por usar un programa gratuito en Windows permitiendo almacenar los Logs.

Primero se debe configurar la dirección IP Servidor Syslog con el puerto 514 donde se envían los mensajes del Mikrotik para realizar los registros de las actividades.

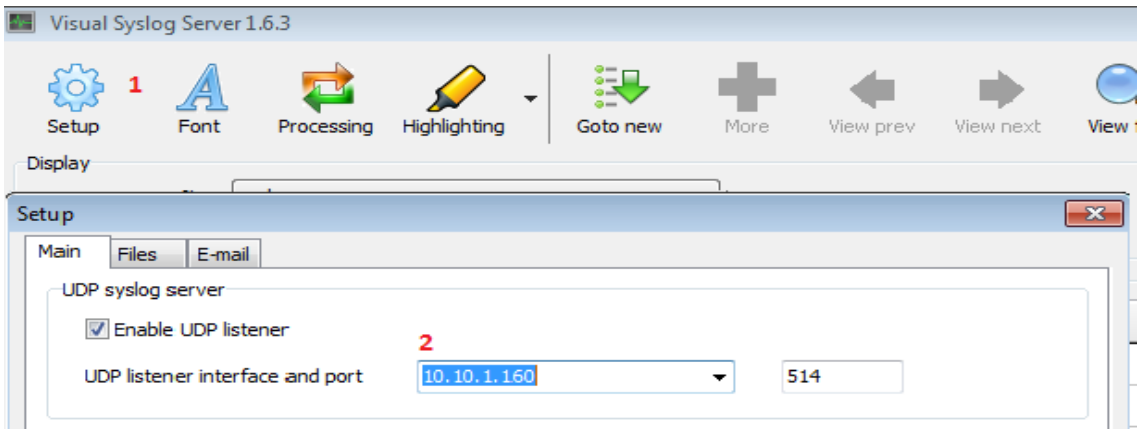


Figura 144 Configuración IP Syslog

Fuente: Visual Syslog Server

En el router Mikrotik en la sección system -> Logging se crea una acción en la Actions. En esta pestaña se indica la ubicación que guardará los log, en este caso se selecciona la opción remote y se indica la dirección IP del servidor Syslog (Figura), luego en la pestaña Rules se selecciona los topics que se desea que aparezca en el servidor Syslog. En el presente proyecto se escoge topics de hotspot debido a que este permite conocer todos los usuarios que se autentiquen por el servidor hotspot o Radius, así mismo para conocer la dirección ip que asignó al usuario, se agrega topics del servidor dhcp.

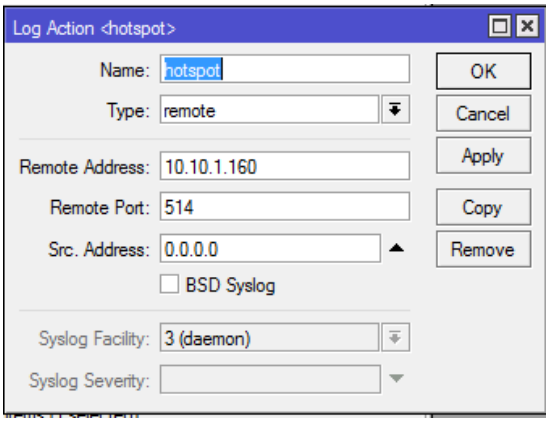


Figura 145 Acción Hotspot Syslog Server

Fuente: Winbox Mikrotik

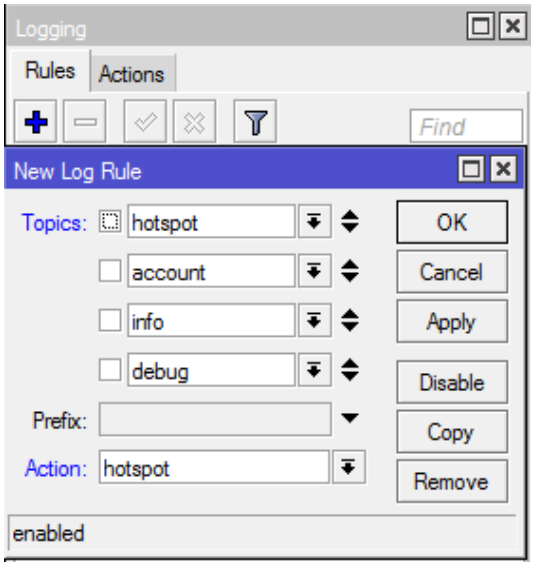


Figura 146 Regla Hotspot Syslog Server

Fuente: Winbox Mikrotik

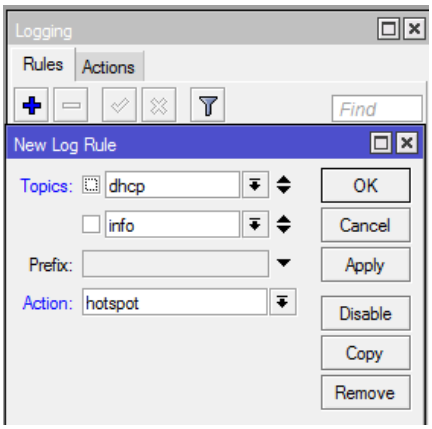


Figura 147 Regla DHCP Syslog Server

Fuente: Winbox Mikrotik

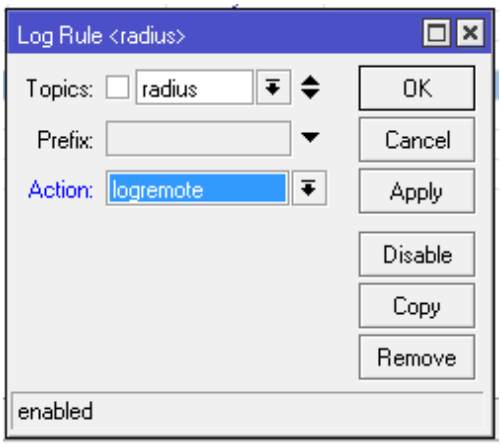


Figura 148 Regla Radius Syslog Server

Fuente: Winbox Mikrotik

5.5.15.2 Torch

Una herramienta que incorpora Mikrotik para utilizar como monitoreo es la opción de Torch que se encuentra en el menú principal de la opción de Tools. Esta herramienta muestra los detalles tales como conexión, protocolo, puertos y páginas web que visita en el momento el usuario.

En la Figura 149 se muestra detalles del tráfico que está saliendo por la Vlan de administración.

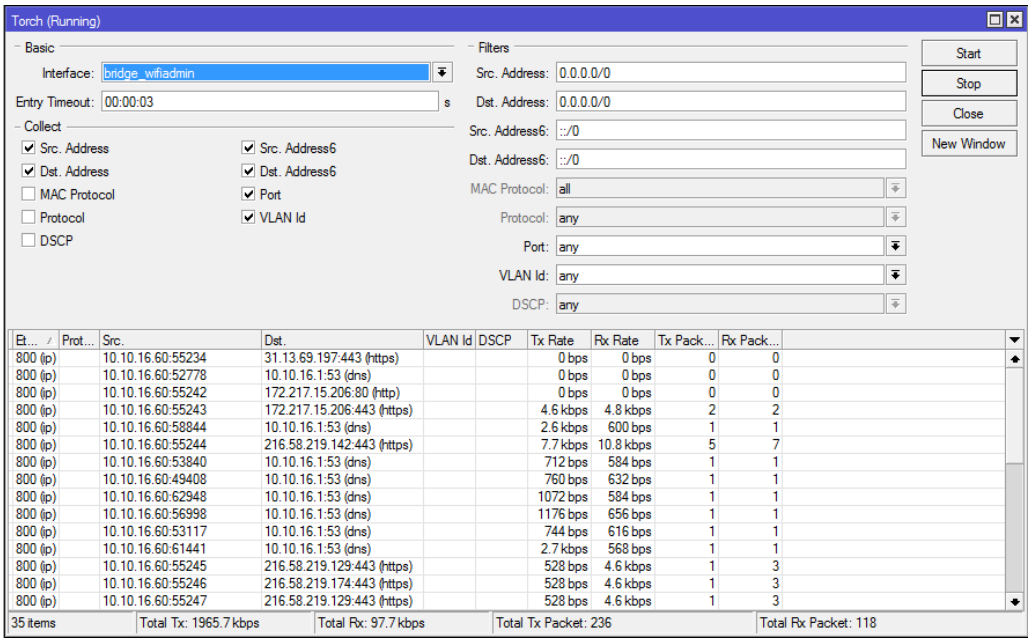


Figura 149 Herramienta Torch

Fuente: Winbox Mikrotik

6. RESULTADOS

Una vez que se realizó las diferentes configuraciones, en la pestaña Interfaces del Capsman se muestran todos los cap con sus ssid virtuales creados como se muestra la Figura 150.

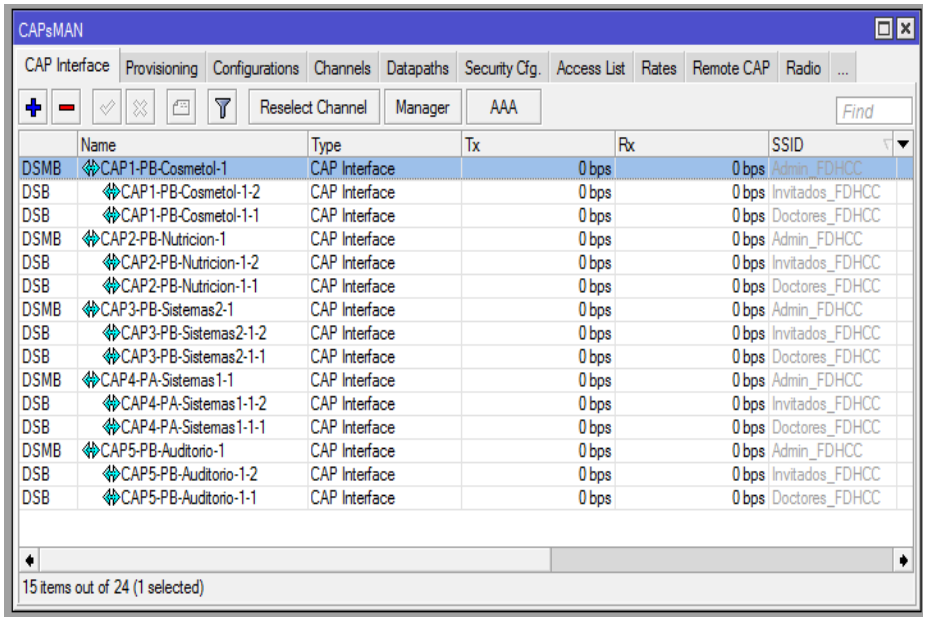


Figura 150 Interface Capsman

Fuente: Winbox Mikrotik

Se realiza la prueba con el usuario jdelgado desde un celular Nokia como muestra la figura 152, también se realizó la conexión en una laptop donde muestra las diferentes ssid, en la figura 151 se muestra que existe una conexión exitosa a la red. Los ssid como doctores e invitados tendrán una configuración abierta, pero para ssid admin tendrán una autenticación mediante el servidor Radius

Figura 151 Conexión SSID

Fuente: Windows 8

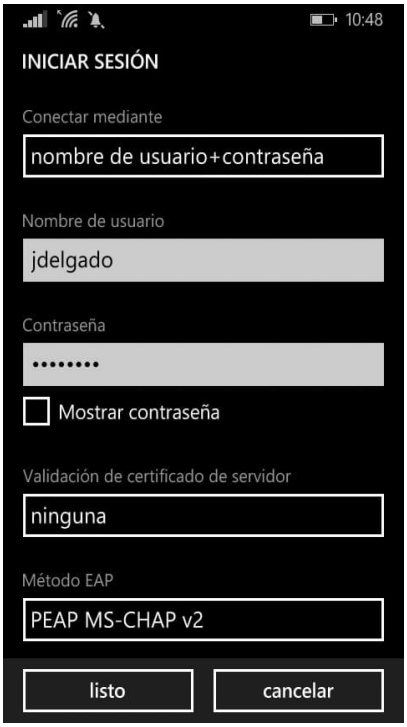


Figura 152 Autenticación usuario

Fuente: Windows Phone 8.1

En la figura 153 se comprueba que el servidor Radius está aceptando las peticiones del capsman al momento que un usuario se autentica en la red inalámbrica.

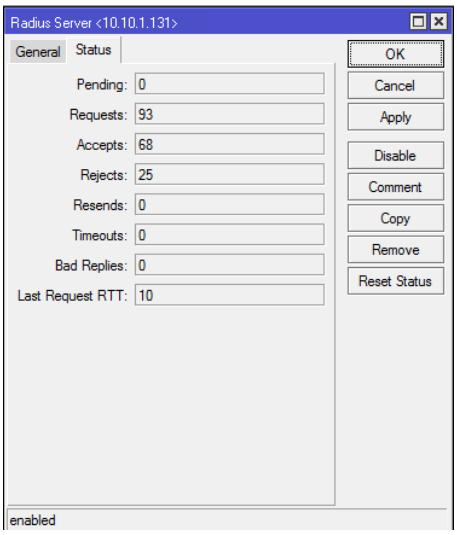


Figura 153 Estado Servidor Radius

Fuente: Winbox Mikrotik

- **Wifi analyzer Android**

En un teléfono Samsung J5 se instaló la aplicación wifi analyzer el cual permite conocer la intensidad de la señal, nombre de la red y canal que se trabaja.

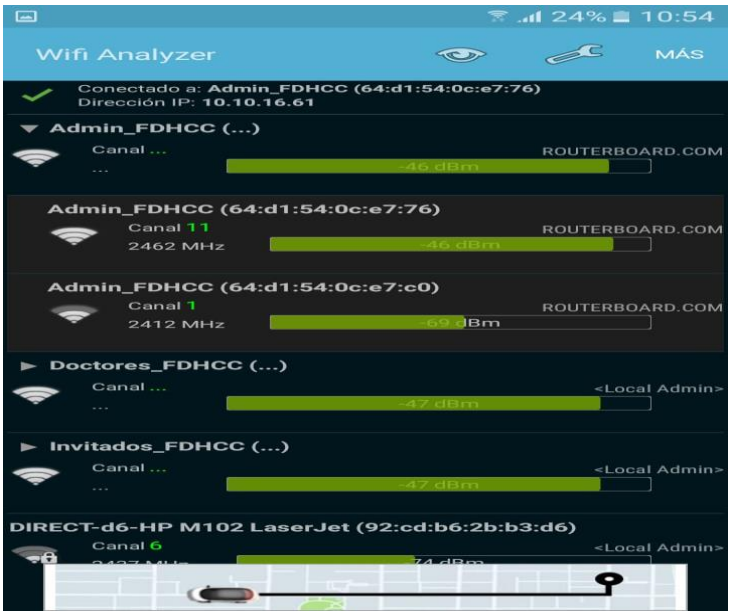


Figura 154 SSID Wifi Analyzer

Fuente: Wifi Analyzer

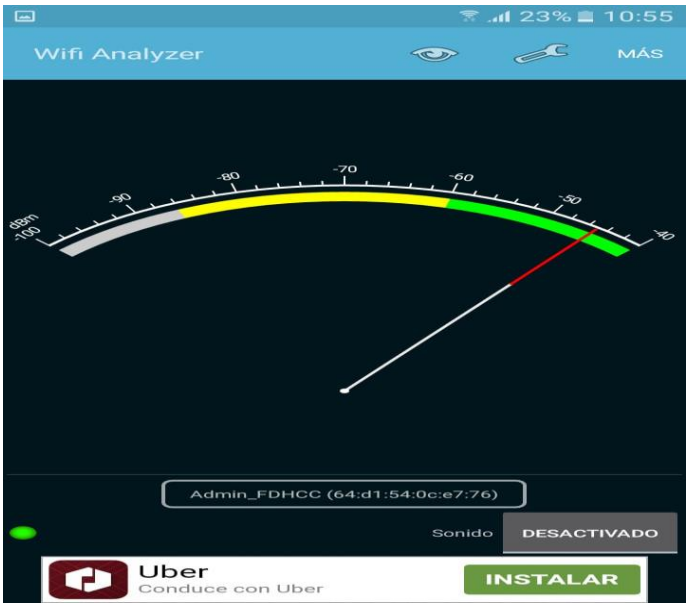


Figura 155 Medidor de Señal

Fuente: Wifi Analyzer

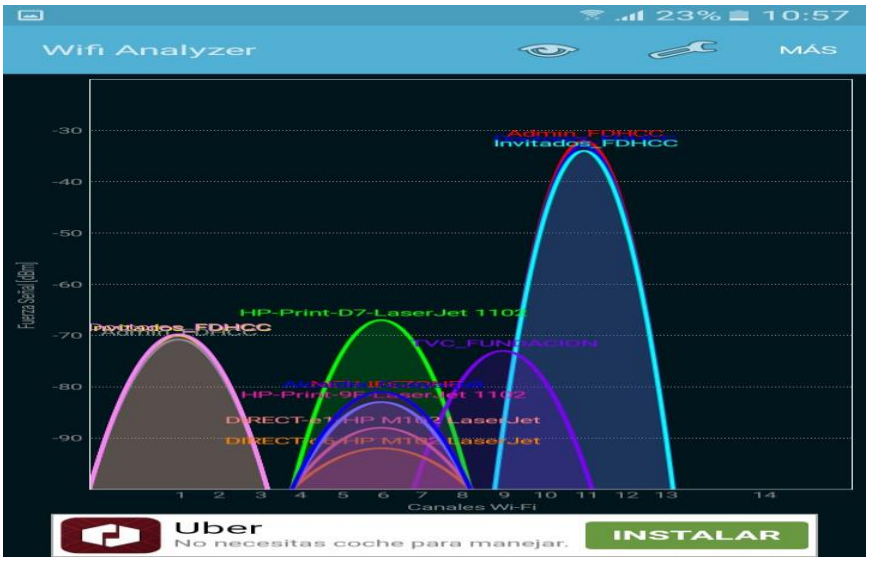


Figura 156 Canales Wifi

Fuente: Wifi Analyzer

Funcionamiento hotspot

Una vez autenticado en las diferentes redes, se muestra el hotspot donde hará la validación de las credenciales, en la red administración será mediante un servidor Radius, para las redes doctores e invitados los usuarios serán creados localmente en el servidor hotspot, así después de autenticarse el usuario podrá tener acceso a los servicios disponibles de la red inalámbrica

obteniendo automáticamente una dirección IP, si es un usuario no autorizado que no se autentica en un cierto tiempo el servidor hotspot lo desconecta automáticamente de la red.

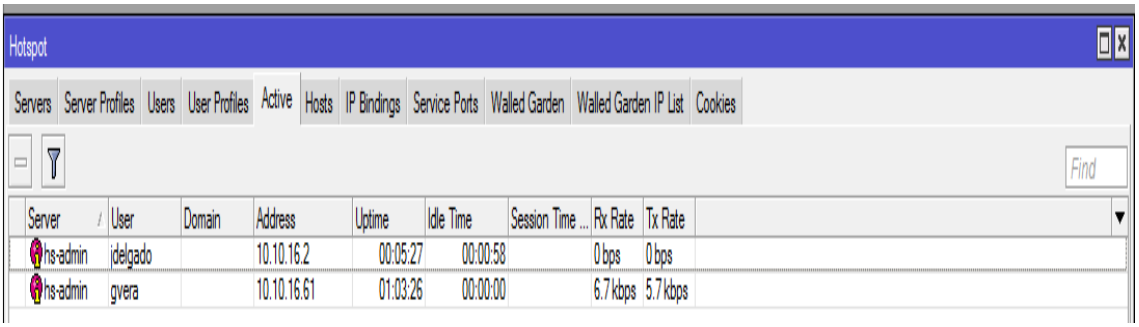


Figura 157 Prueba autenticación usuarios

Fuente: Winbox Mikrotik

Para cada red solo se permite el uso de un solo dispositivo como se muestra en la figura 158, si existe un intento de acceso con otro dispositivo con la misma credencial el hotspot muestra el error de sesión máxima.

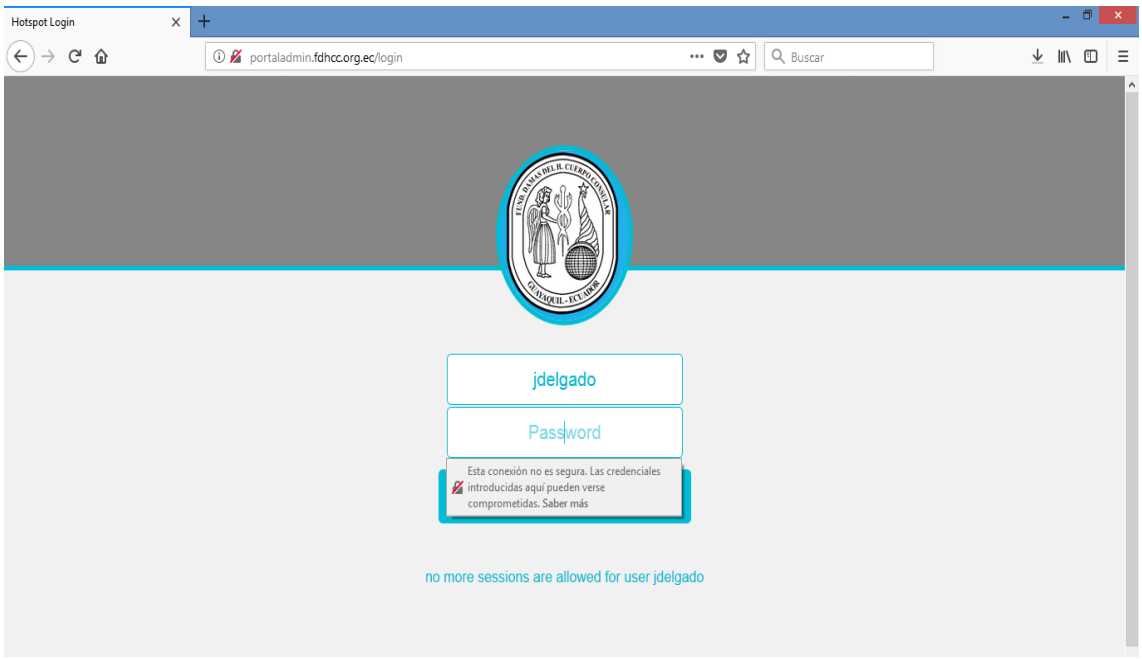


Figura 158 Sesiones permitida

Fuente: Hotspot Windows 8

Se verifica la funcionalidad que existe en la red como se muestra en la figura 159.

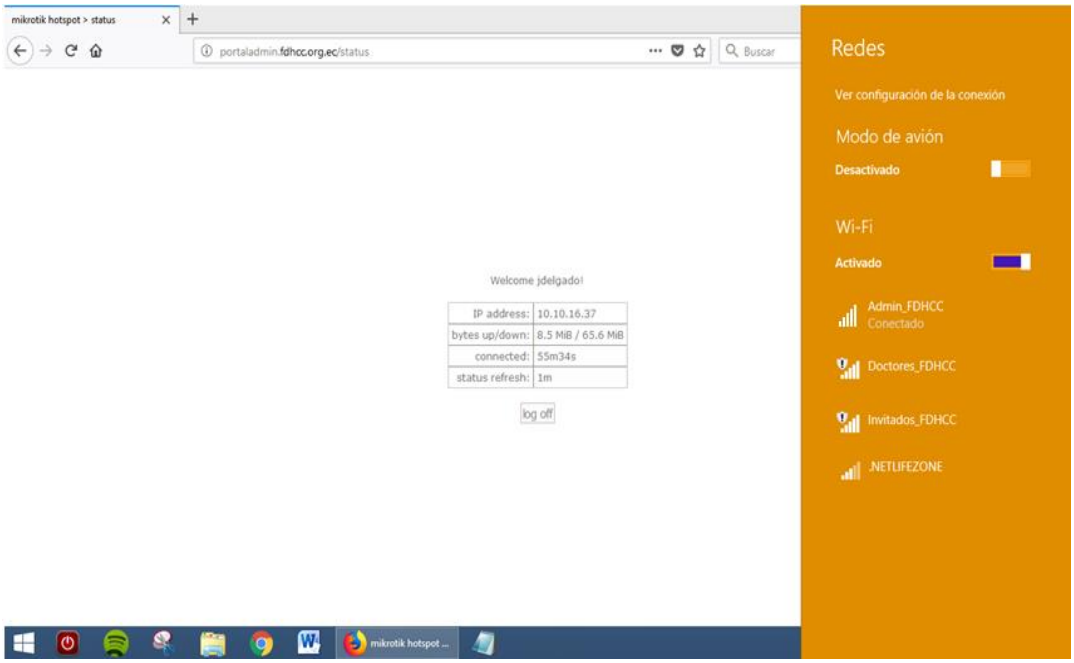


Figura 159 Funcionalidad Redes Wifi

Fuente: Windows 8

Para cada red se asignó un ancho, se verifica que en la red de administración al estar conectados 2 clientes en la misma red se le asigne la mitad del ancho de banda a cada uno. Se realizó la medición con la herramienta speedtest en un teléfono Nokia con sistema operativo Windows Phone y en una laptop con sistema operativo Windows 8.

Figura 160 Speedtest Nokia Lumia

Fuente: Windows Phone 8.1

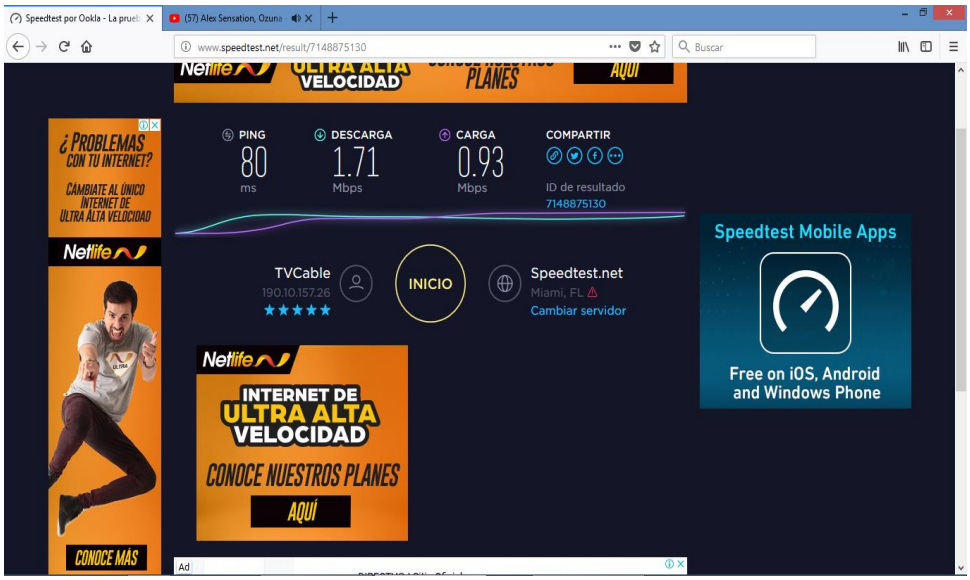


Figura 161 Speedtest Laptop

Fuente: Windows 8

En el servidor hotspot se puede observar el ancho de banda que está usando cada usuario conectado.

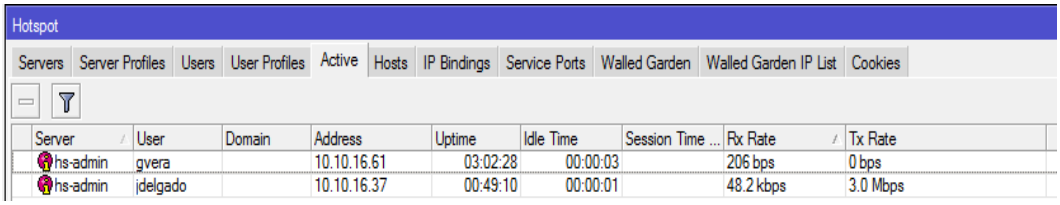


Figura 162 Hotspot Active

Fuente: Winbox Mikrotik

Para la prueba de bloqueo de páginas se modificó la hora de bloqueo en el servidor. Se verifica que para la red de administración a determinada hora no puede acceder a la página de Facebook.

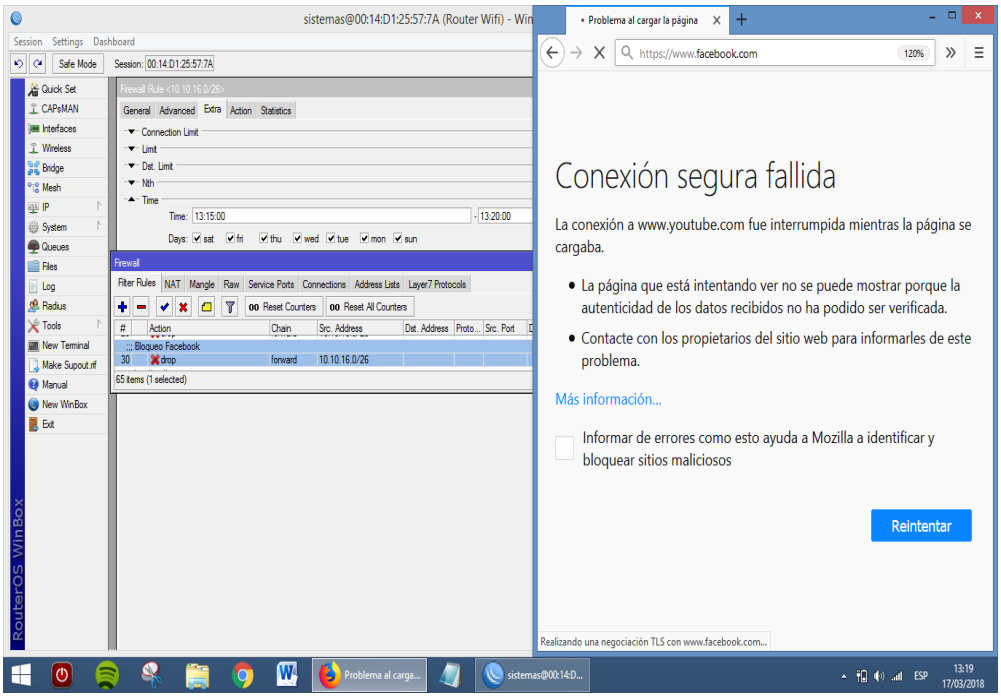


Figura 163 Regla Bloqueo Página Activa

Fuente: Winbox Mikrotik

Una vez que el tiempo de bloqueo expiró, la regla queda inactiva y el usuario podra navegar en la página de Facebook.

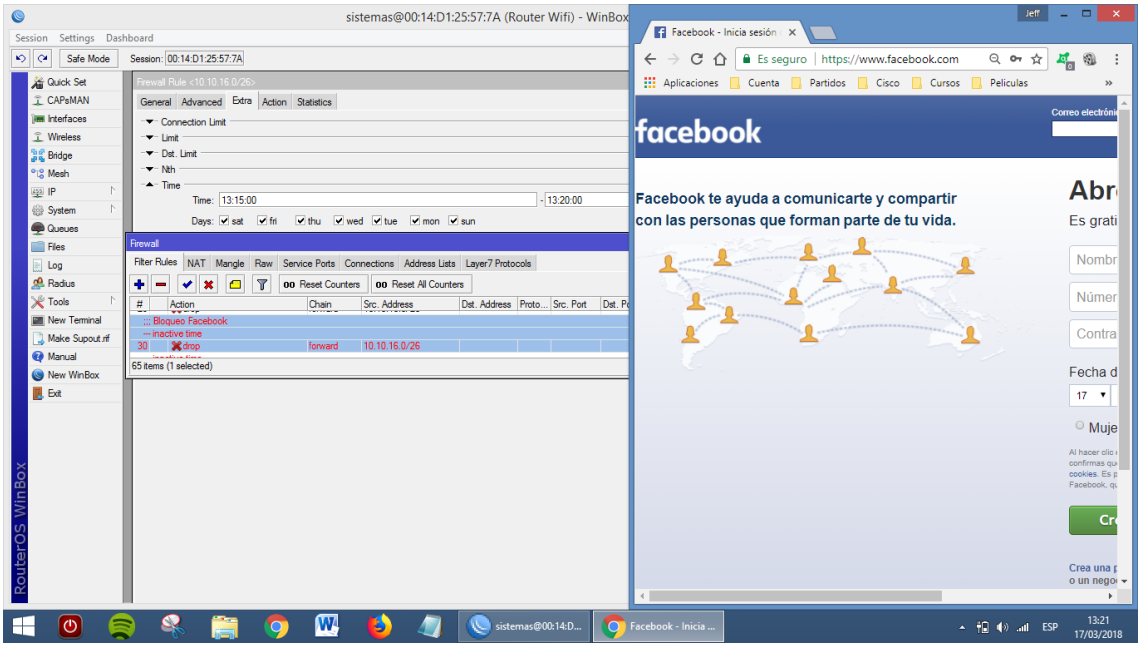


Figura 164 Bloqueo inactivo Página Web

Fuente: Winbox Mikrotik

Para evitar que la red inalámbrica se ponga lenta por descargas de archivos muy pesados se optó por bloquear las extensiones de algunos archivos. En la figura 165 y 166 fue negado al intentar descargar archivos como iso y rar.

-

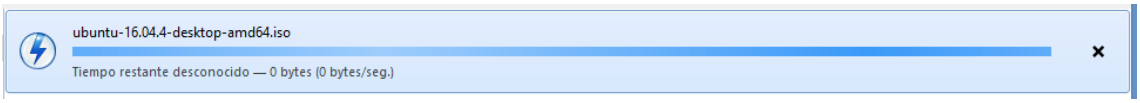


Figura 165 Bloqueo descarga archivo iso

Fuente: Windows 8

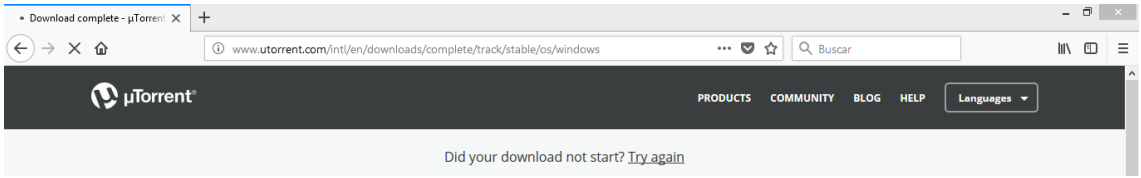


Figura 166 Bloqueo descarga archivo rar

Fuente: Windows 8

Gráfico consumo cliente

Para llevar un reporte de todas las interfaces se puede revisar el monitoreo que realiza el Mikrotik, desde la red de Gestión ingresando en un navegador la dirección IP como se muestra en la figura 167

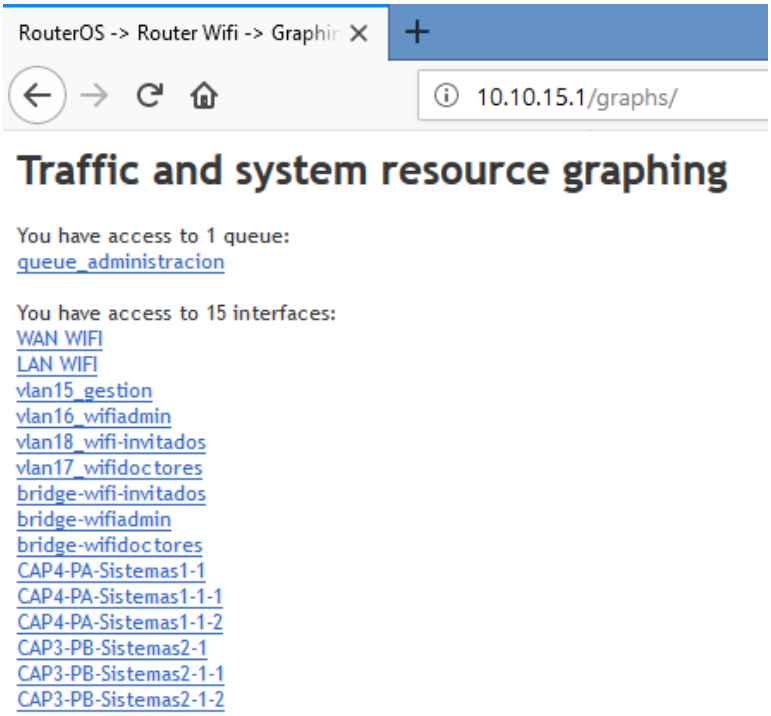


Figura 167 Interfaces Graphs

Fuente: Mozilla Firefox

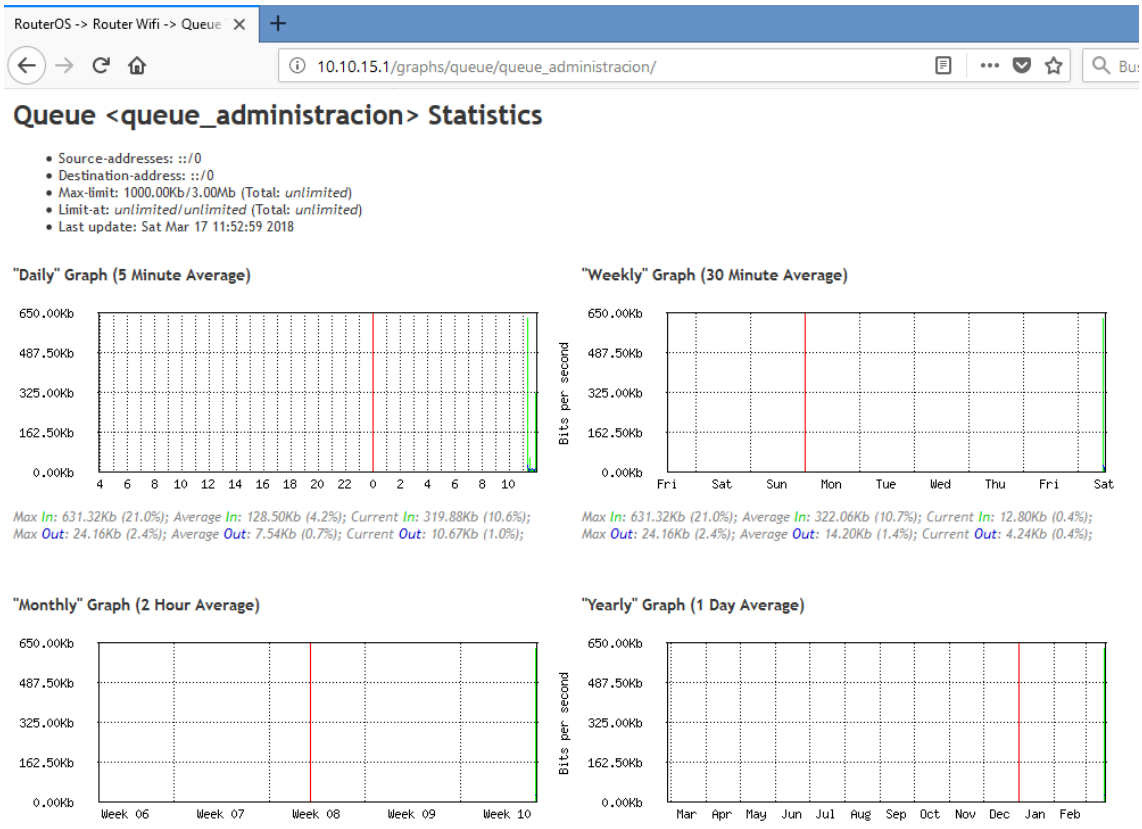


Figura 168 Monitoreo Graphs

Fuente: Mozilla Firefox

También se verifica los log que se generan en el servidor Mikrotik permitiendo conocer el usuario que se conectó con la respectiva dirección IP.

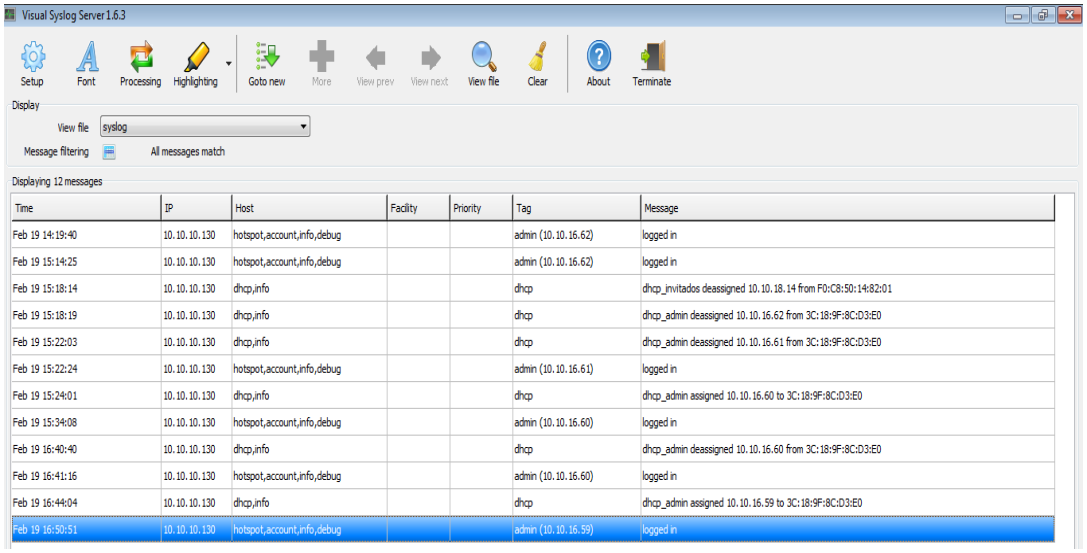


Figura 169 Log guardados Mikrotik

Fuente: Visual Syslog Server

7. CONCLUSIONES

La implementación del presente proyecto fue de beneficio para la Fundación en el tema económico al ahorrar un controlador y un router que permita gestionar los access point y el control de usuario sin necesidad de realizar la compra de un equipo de otra marca. En la entrevista realizada al Coordinador de Sistemas, mediante un software, se escaneo la red para determinar el número de equipos inalámbricos conectados y así concluir el uso de aplicaciones según un grupo de usuarios.

La seguridad es muy primordial en toda red inalámbrica y como medida de seguridad para usuarios administrativos se ejecutó un servidor radius para la autenticación en la red inalámbrica y el uso de un hotspot para dar prioridades de acceso a internet ingresando las credenciales en un portal cautivo. En el mismo firewall de Mikrotik se realizó diferentes reglas en cada una de las vlans tales como bloqueo de páginas, descargas de archivos específicos.

Se centralizó todos los access point mediante el servicio Capsman que permite agregar el access point con la mac registrada en la tabla ARP junto con la dirección IP y asi el controlador solo administre los cap registrado con dicha mac. Se colocaron en total 5 access point de la marca Mikrotik siendo fácil su instalación que permita acoplarse al ambiente de la fundación.

Las pruebas ejecutadas muestran la funcionalidad del servidor radius y el servidor hotspot con los diferentes parámetros otorgados a los usuarios. Además, mediante un servidor log se lleva un registro de los usuarios autenticados y no autenticados siendo importante para realizar una auditoría de la red inalámbrica.

8. RECOMENDACIONES

Una de las recomendaciones puntuales es realizar el debido mantenimiento y actualizaciones del sistema operativo Mikrotik, ejecutando siempre un backup para que no exista la perdida de configuración.

Durante el análisis de la red y la implementación que se realizó, se optó por generar una nueva topología para la red inalámbrica, por eso se recomienda que para cualquier cambio se actualice los datos que se elaboraron en el proyecto técnico ya que facilita rápidamente cualquier problema que se presente en la red.

A medida que los años van pasando la tecnología Wifi va creciendo, es por eso que sería muy importante realizar instalación de algunos access point en los edificios que no cuenten con una buena señal inalámbrica, estos nuevos access point solo requieren que exista comunicación con el Capsman para tener la configuración respectiva. En el caso que no requiera mediante cables la comunicación entre el Capsman y el cap, se podría realizar mediante comunicación inalámbrica.

Debido a la importancia de la tecnología wifi en la sociedad, se recomienda una nueva red con su respectiva Vlan para dar servicio inalámbrico a pacientes que visiten el centro médico pero se sugiere que se asigne un ancho de banda y se instale algunos Access point extra para que no exista congestión.

Se recomienda verificar si no existe lentitud en la red mediante monitoreo, y revisar que usuario está provocando el congestionamiento para poder desconectarlo de la red y bloquearlo mediante la mac address si no pertenece al personal de la fundación o darle ciertos privilegios a ese usuario si pertenece al personal.

9. REFERENCIAS BIBLIOGRÁFICAS

Acevedo Ibáñez, A., Alba , F., & López , M. (1986). *El proceso de la entrevista.* Obtenido de https://books.google.com.ec/books?id=V-Wi4_aHmKAC&printsec=frontcover&dq=proceso+de+entrevista&hl=es-419&sa=X&ved=0ahUKEwjU07WX7tLYAhWPl-AKHaaEAUIQ6AEIKDAA#v=onepage&q=proceso%20de%20entrevista&f=false

Cisco. (2006). *How Does RADIUS Work?* Obtenido de https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

Cisco. (2012). Obtenido de https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/wireless/pdfs/brochure_wireless.pdf

Cisco. (s.f.). *Cisco*. Obtenido de https://www.cisco.com

Cisco Networking Academy. (2016). *CCNA R&S: Scaling Networks.* Obtenido de www.netacad.com

Dennis Chávez de Paz. (2008). *CONCEPTOS Y TÉCNICAS DE RECOLECCIÓN DE DATOS EN LA INVESTIGACIÓN* . Obtenido de https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080521_56.pdf

Duarte, E. (2012). *Las 12 Amenazas Más Peligrosas En Internet.* Obtenido de http://blog.capacityacademy.com/2012/06/21/las-12-amenazas-mas-peligrosas-en-internet/

Fassiano, J. (2015). *MUM Mikrotik Argentina.* Obtenido de https://mum.mikrotik.com/presentations/AR15/presentation_2731_1447746341.pdf

FDHCC. (s.f.). *Fundacion Damas del Honorable Cuerpo Consular*. Obtenido de http://www.fundaciondamashcc.org/

FreeRadius. (2017). *FreeRadius About.* Obtenido de http://freeradius.org/about/

FreeRadius. (2017). *WikiSite.* Obtenido de http://wiki.freeradius.org/Home

GrandStream. (2015). *802.1x Authentication Guide.* Obtenido de http://www.grandstream.com/sites/default/files/Resources/802_1X_Guide.pdf

Hakima Chaouchi. (2007). *Wireless and Mobile Network Security.*

HomeTech. (2016). *Diseñar una Red Wifi.* Obtenido de http://www.hometechcolombia.com/boletines/PDF/DisenarRedWiFi.pdf

Hucaby, D. (2014). *CCNA Wireless 640-722.* (C. Press, Ed.)

IEEE. (s.f.). *Institute of Electrical and Electronics Engineers.* Obtenido de https://www.ieee.org

IEEE, G. P. (2017). Obtenido de http://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68

Intel. (2017). *802.1x Overview and EAP Types.* Obtenido de https://www.intel.com/content/www/us/en/support/articles/000006999/network-and-i-o/wireless-networking.html

IT, G. (s.f.). *Glosario IT.* Obtenido de http://www.glosarioit.com

ITU. (2017). *Historia de ITU-R.* Obtenido de https://www.itu.int/en/history/Pages/FocusOnRadiocommunication.aspx

Mateo, D. M. (Diciembre de 2004). *Soluciones de seguridad en redes Inalambricas.* Obtenido de http://www.astic.es/sites/default/files/articulosboletic/mono04.pdf

Mikrotik. (2017). Obtenido de RBcap2nd: https://mikrotik.com/product/RBcAP2nD

Mikrotik. (2017). *About US.* Obtenido de https://mikrotik.com/aboutus

Mikrotik. (2017). *Product Mikrotik.* Obtenido de https://mikrotik.com/product

Mikrotik. (2018). Obtenido de https://mikrotik.com

Mikrotik Documentation. (2015). *Manual License.* Obtenido de https://wiki.mikrotik.com/wiki/Manual:License

Mikrotik Documentation. (2015). *Manual Queues PCQ.* Obtenido de https://wiki.mikrotik.com/wiki/Manual:Queues_-_PCQ

Mikrotik Documentation. (2016). *Manual Packages*. Obtenido de https://wiki.mikrotik.com/wiki/Manual:System/Packages

Mikrotik Documentation. (2017). *Manual Winbox.* Obtenido de https://wiki.mikrotik.com/wiki/Manual:Winbox

Mikrotik Documentation. (2017). *Manual:CAPsMAN.* Obtenido de https://wiki.mikrotik.com/wiki/Manual:CAPsMAN

Mikrotik Documentation. (2017). *Manual:IP/Firewall/Filter.* Obtenido de https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter

NAS-HSM. (s.f.). Obtenido de http://academyxperts.com/index.php/cursos/certificaciones-academy/nas/nas-hsm

Netacad. (s.f.). *Cisco Networking Academy.* Obtenido de https://www.netacad.com/es/

Netspotapp. (2018). *Wifi channel scanner.* Obtenido de https://www.netspotapp.com/es/wifi-channel-scanner.html

RedUsers. (Febrero de 2013). *Seguridad en Redes: Autenticacion con servidores AAA.* Obtenido de http://www.redusers.com/noticias/seguridad-en-redes-autenticacion-con-servidores-aaa/

Serrano, E. (Octubre de 2017). ¿Cómo puedo proteger mi conexión a internet tras la ruptura del protocolo WPA2? *Diario El Confidencial*.

Software, M. (2018). *Download Software.* Obtenido de https://mikrotik.com/download

Strauss, A., & Corbin, J. (2002). *Bases de la Investigación Cualitativa.* Universidad de Antioquia.

Sun Microsystems. (2000). *Radius extesions*. Obtenido de https://www.ietf.org/rfc/rfc2869.txt

Wi-Fi, A. (2017). Obtenido de https://www.wi-fi.org/who-we-are

WifiSafe. (2016). *Controlador HotSpot*. Obtenido de https://www.wifisafe.com/blog/categoria/controlador-hotspot/

WikiMikrotik. (2017). *WikiMikrotik*. Obtenido de Mikrotik Documentation: https://wiki.mikrotik.com

10 ANEXOS

ANEXO A: Equipos Instalados

Figura 170 Ubicación Servidor Mikrotik

Fuente: Fundación Damas del Honorable Cuerpo Consular Centro Médico Sur

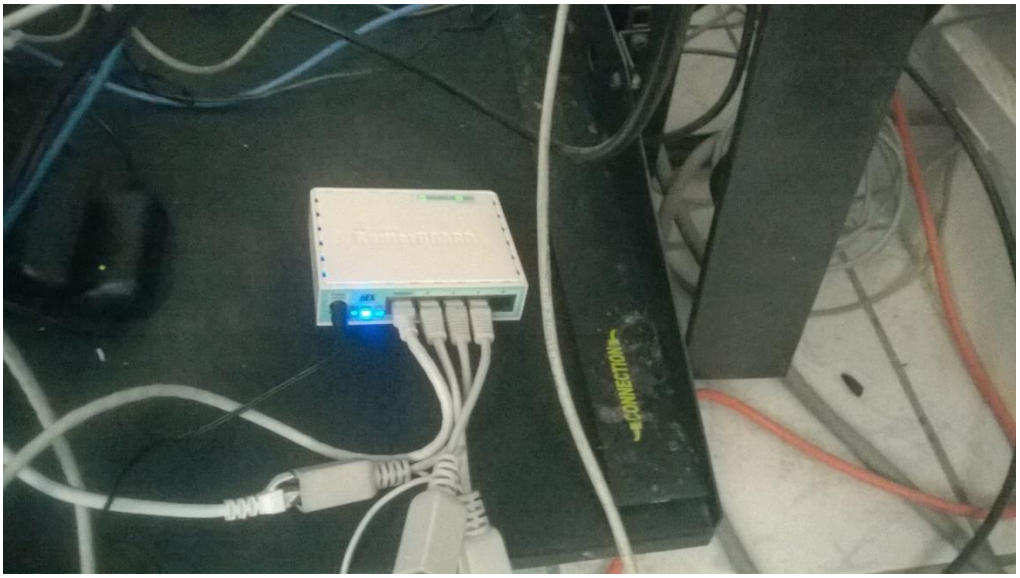


Figura 171 Switch Planta Baja

Fuente: Fundación Damas del Honorable Cuerpo Consular Centro Médico Sur

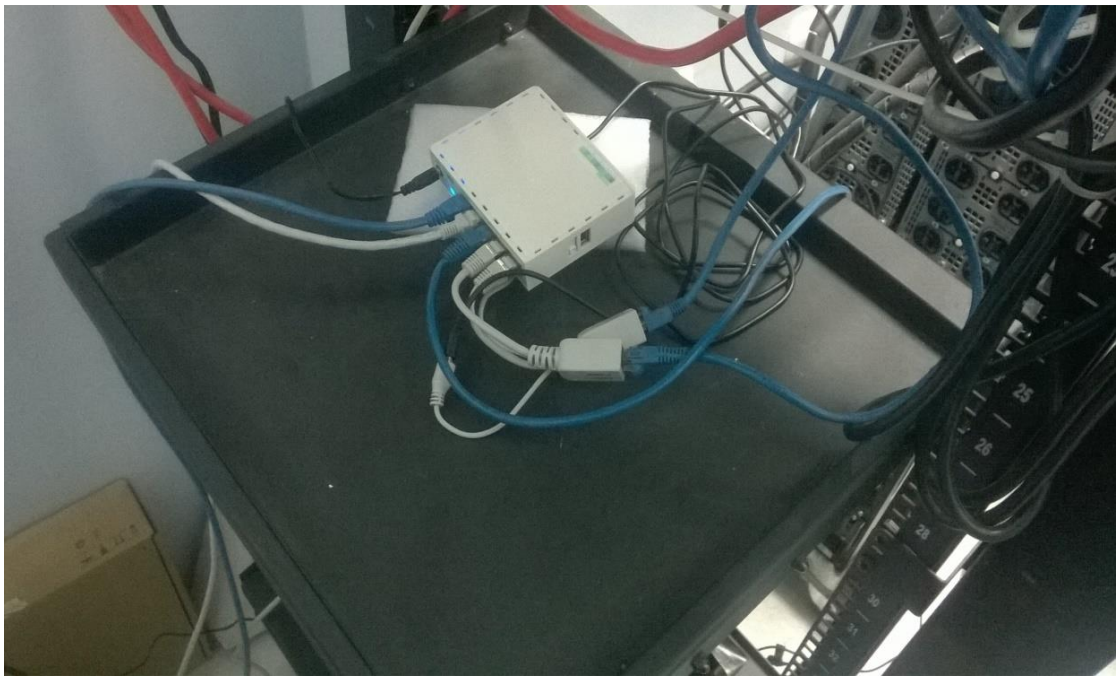


Figura 172 Switch Planta Alta

Fuente: Fundación Damas del Honorable Cuerpo Consular Centro Médico Sur

Figura 173 Access Point Cosmetología

Fuente: Fundación Damas del Honorable Cuerpo Consular Centro Médico Sur

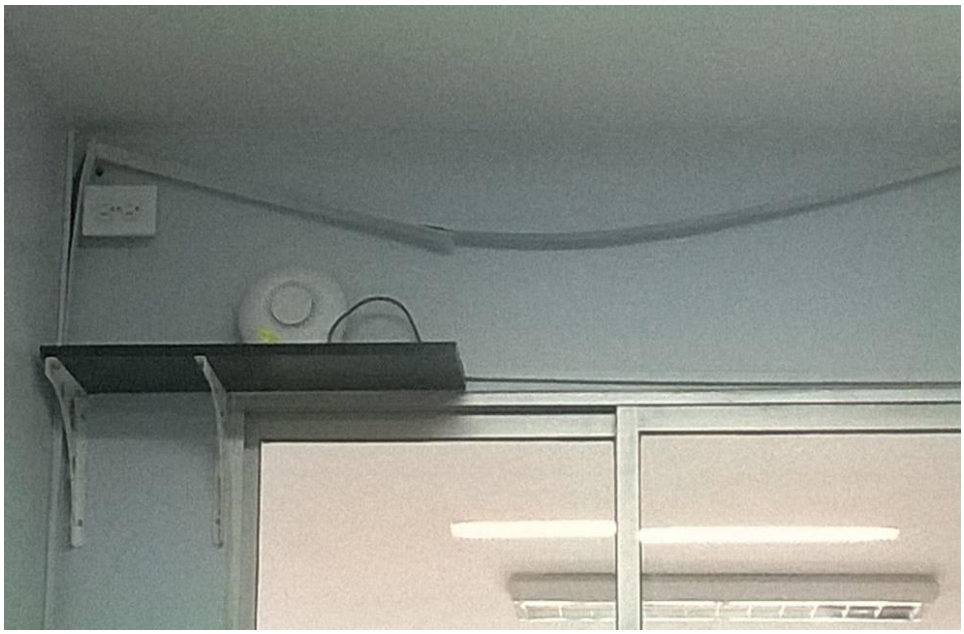


Figura 174 Access Point Nutrición

Fuente: Fundación Damas del Honorable Cuerpo Consular Centro Médico Sur

Figura 175 Access Point Cuarto de Rack Planta Baja

Fuente: Fundación Damas del Honorable Cuerpo Consular Centro Médico Sur

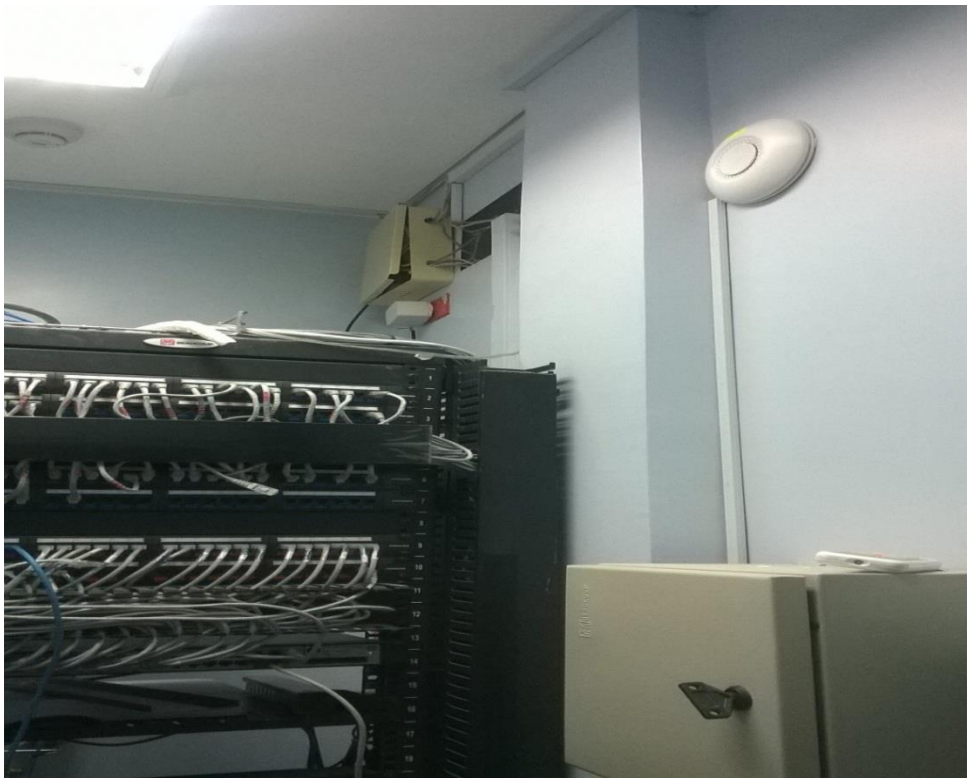


Figura 176 Access Point Cuarto de Rack Planta Alta

Fuente: Fundación Damas del Honorable Cuerpo Consular Centro Médico Sur

ANEXO B: Entrevista a Jefe de Sistemas y Administradora Centro Médico

JEFE DE SISTEMAS

1) **¿Ha presentado algún problema en la red inalámbrica?**

   "El alcance de los router inalámbricos y usuarios piden contraseña y al no tener control de ancho de banda le impide proporcionar la clave Wifi."

2) **¿Qué edificio y áreas del edificio se desea alcanzar con cobertura inalámbrica?**

   "El edificio que tenga mayor influencia de usuarios administrativo en este caso el Edificio Principal en la sala de espera principal de la Planta Baja y la Planta Alta."

3) **¿Existe un control de usuarios conectados a la red Wifi?**

   "Actualmente no, solo el usuario pide la contraseña y el personal de sistemas mismo le ingresa la contraseña."

4) **¿Qué página o aplicaciones deberían tener acceso los usuarios?**

   "Se debería agrupar usuarios con acceso total en este caso administrativo solo con bloqueo YouTube. Para doctores navegación controlada con un límite de navegación y bloqueo a YouTube, Facebook."

5) **Se maneja una lista de dispositivos inalámbricos registrados ¿Qué tan complicado es identificar un dispositivo inalámbrico que no forma parte de la red de la fundación?**

   "Se usa el programa Advanced IP Scanner que es una herramienta de escaneo para detectar que equipo está conectado y poder lograr identificar que usuario usa ese equipo"

6) **¿Cuantos usuarios por lo general se encuentran conectados al realizar un escaneo?**

"Aproximadamente 25 usuarios en hora pico que es en la mañana"

7) **¿Existe configuración centralizada de los Access Point?**

"No porque los que dan acceso a internet son router inalambricos y cada router proporciona su propia red"

8) **Desde su punto de vista? Cual la ventaja y desventaja del uso wifi**

"Una de las ventajas seria tener la movilidad en el edificio y la desventaja el no tener cobertura inalambrica"

9) **¿Qué le parece sobre la implementacion de un control de usuarios?**

"Es una buena herramienta para el control de acceso para los usuarios y tener un buen control y seguridad"

ADMINISTRADORA CENTRO MÉDICO

1) **¿Qué problema presenta con la red inalámbrica?**

   "Existe conexión lenta y hay momentos que no hay servicio inalámbrico"

2) **¿Qué tipos de aplicación utiliza los usuarios al momento de conectarse a la red Wifi?**

   "Por lo general el personal administrativo WhatsApp y para doctores por lo general requieren internet para el uso de navegación en google para consulta de medicamentos."

3) **¿Con que frecuencia usa el internet los doctores?**

   "Al momento de consultas para buscar medicamentos nuevos con las características"

4) **¿Los sitios que visitan por lo general realizar descargas o transferencias de archivos?**

   "Por lo general no, existen invitados como visitadores médicos, proveedores que requieren descargar archivos para una presentación."

5) **¿Cuándo no tiene conexión como lo resuelve?**

   "Normalmente se usa los mismos datos móviles"

6) **¿Que opina acerca de implementar una medida de seguridad para proteger la navegación a Internet?**

   "Excelente ya que el personal no tiene conocimiento de informática y puede entrar a páginas que piensa que son seguras pero contienen algún tipo de virus"

ANEXO C: Detalles Técnicos Access Point Mikrotik

Specifications

Product code	RBcAP2nD
CPU	QCA9533 650 MHz
Memory	64 MB
Storage type	Flash
Storage size	16 MB
Ethernet	One 10/100 Mbit/s Fast Ethernet port with Auto-MDI/X
Wireless	Wireless Built-in 2.4 GHz 802.11b/g/n, dual chain
Power options	Passive PoE input 11-57 V
Consumption	4W
Dimensions	⌀ 185mm, height: 31mm
Operating temperature	-40°C ~ +70°C tested
LEDs	5x LEDs, 1x user LED
License level	4
Operating system	RouterOS
Antenna gain	2 dBi

Wireless specifications

Rate	Tx	Rx
1MBit/s	22	-96
11MBit/s	22	-89
6MBit/s	20	-93
54MBit/s	18	-74
MCS0	20	-93
MCS7	16	-71

Figura 177 Detalles Técnico RbCap2nd

Fuente: (Mikrotik, 2018)

Mikrotik Wap2nd

Specifications

Product code	RBwAP2nD (white), RBwAP2nD-BE (black)
CPU nominal frequency	650 MHz
CPU core count	1
Size of RAM	64 MB
10/100 Ethernet ports	1
Wireless	Built-in 2.4 GHz 802.11b/g/n, dual-chain
Antenna gain	2 dBi
Antenna beam width	360°
Wireless chip model	QCA9533
PoE in	Yes
Supported input voltage	11 V - 57 V (Passive PoE and 802.3af/at with unshielded cable)
Dimensions	185 x 85 x 30 mm
License level	4
Operating System	RouterOS
CPU	QCA9533
Max Power consumption	4 W

Figura 178 Detalles Técnico RbWap2nd

Fuente: (Mikrotik, 2018)

ANEXO D: Instalación Ubuntu Server 16.04 LTS

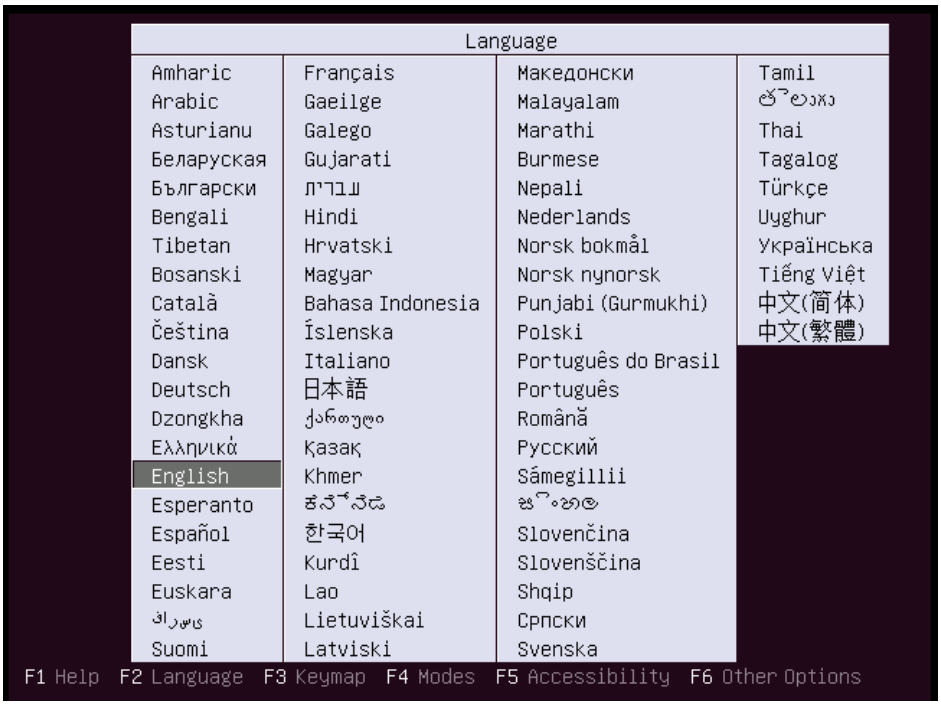


Figura 179 Selección de Idioma

Fuente: Sistema Operativo Linux Distribución Ubuntu 16.04

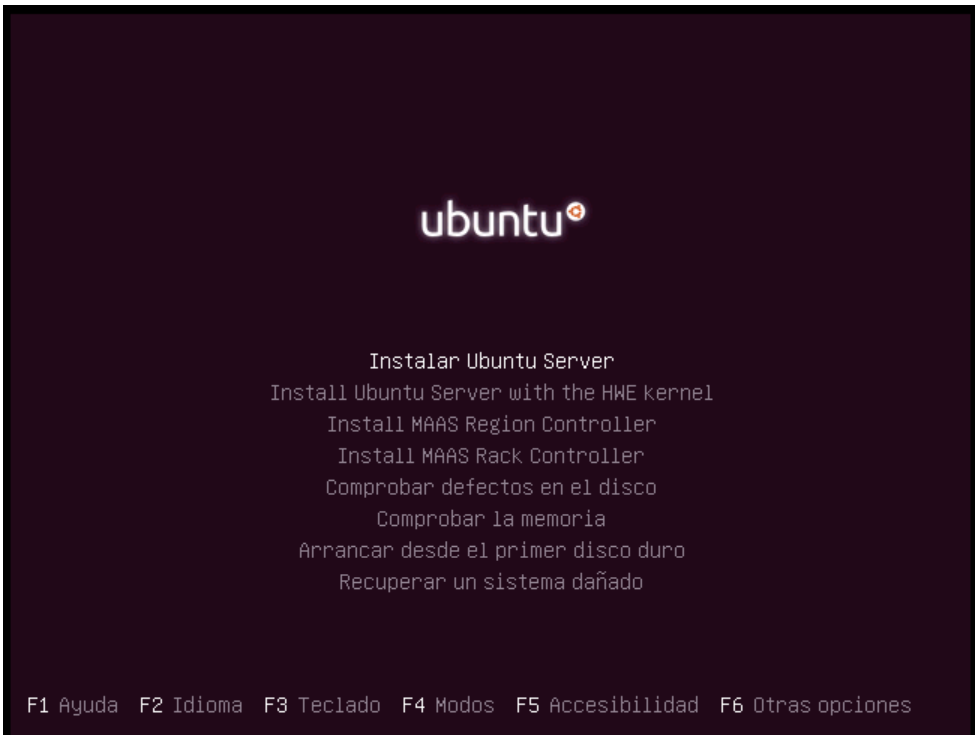


Figura 180 Instalación de Ubuntu

Fuente: Sistema Operativo Linux Distribución Ubuntu 16.04

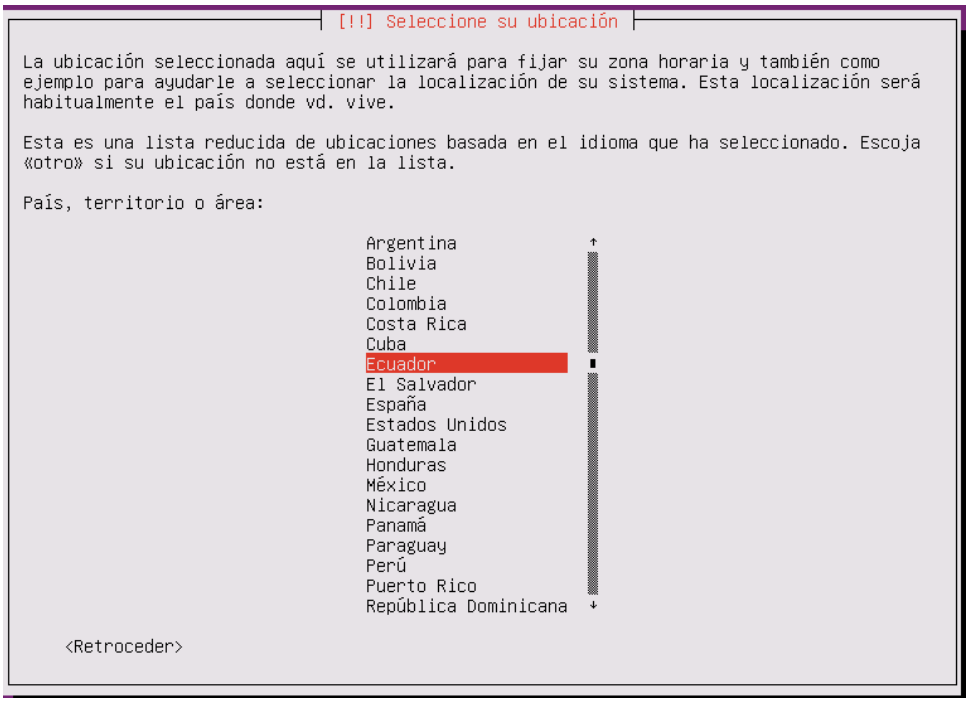


Figura 181 Selección de País

Fuente: Sistema Operativo Linux Distribución Ubuntu 16.04

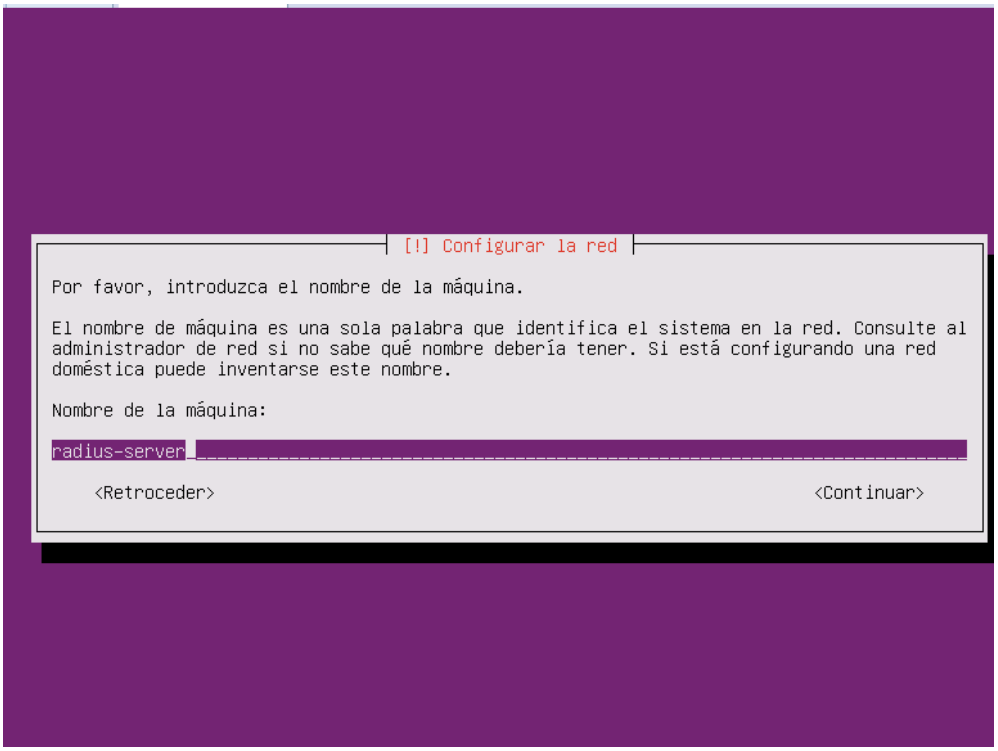


Figura 182 Nombre de la maquina

Fuente: Sistema Operativo Linux Distribución Ubuntu 16.04

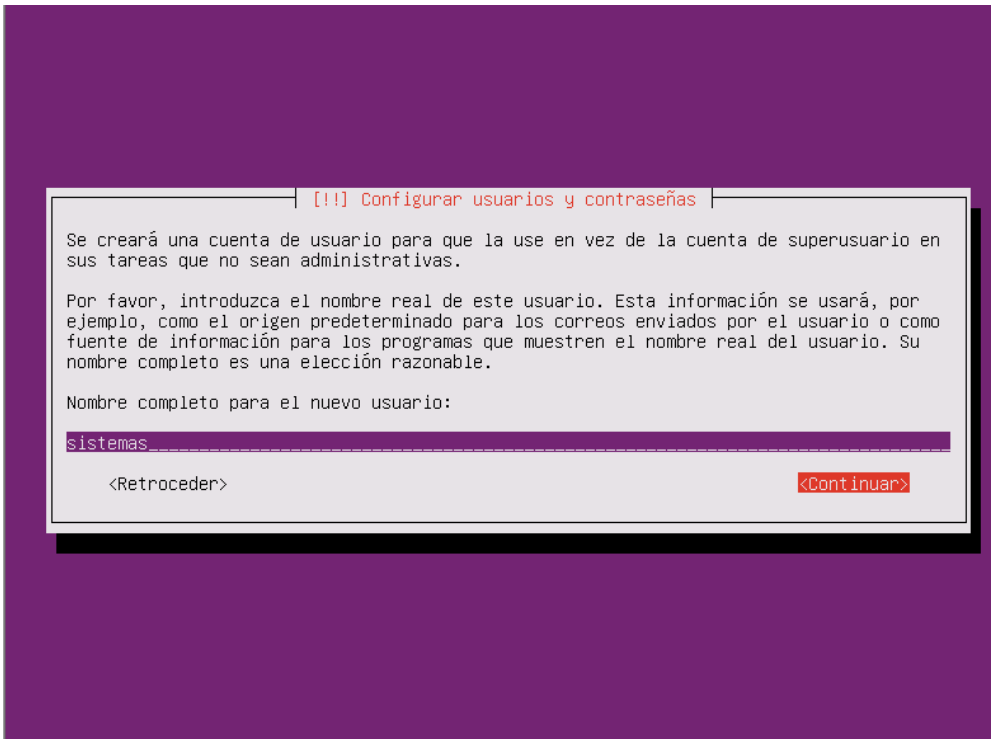


Figura 183 Creación Usuario

Fuente: Sistema Operativo Linux Distribución Ubuntu 16.04

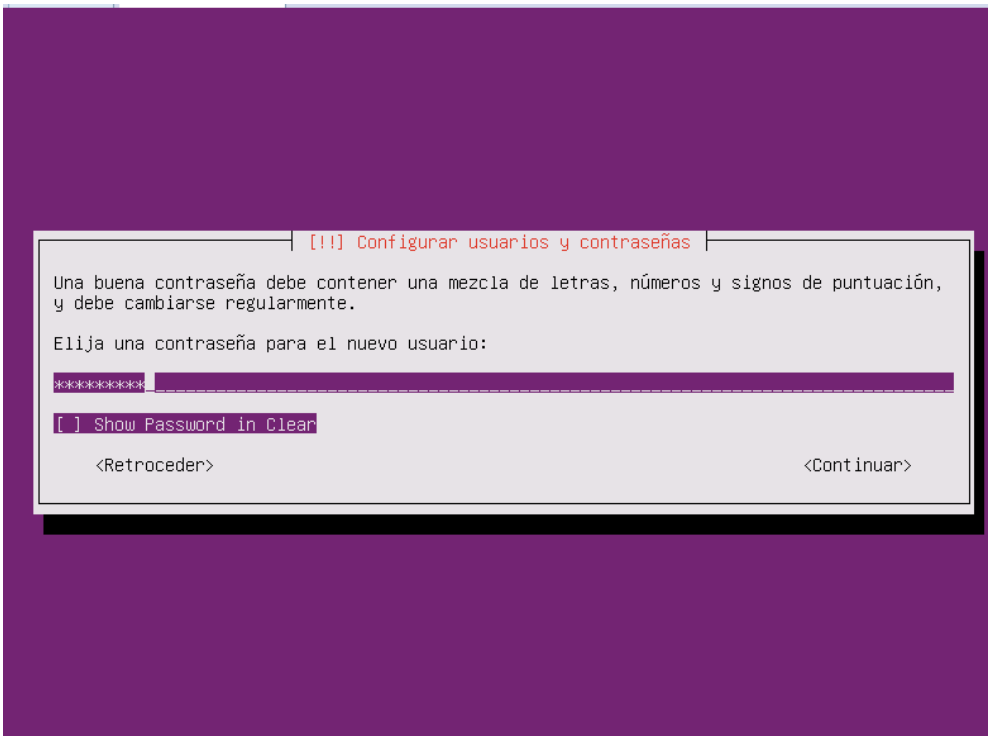


Figura 184 Configuración Contraseña

Fuente: Sistema Operativo Linux Distribución Ubuntu 16.04

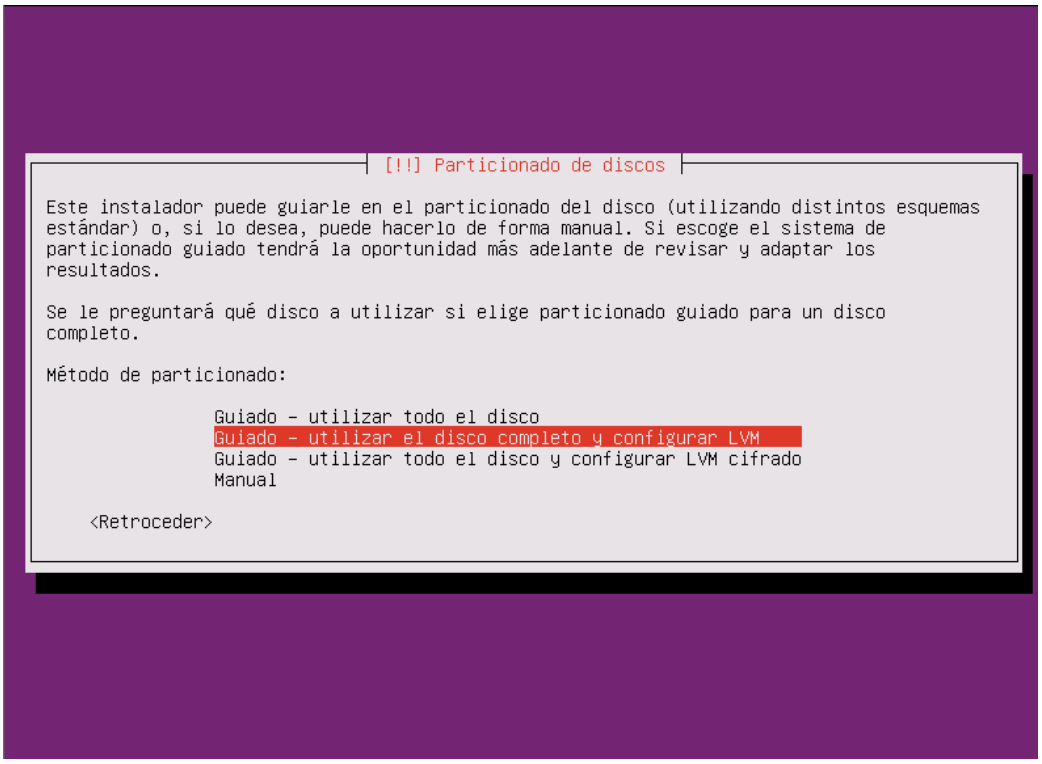


Figura 185 Partición de disco

Fuente: Sistema Operativo Linux Distribución Ubuntu 16.04

Figura 186 Disco Partición

Fuente: Sistema Operativo Linux Distribución Ubuntu 16.04

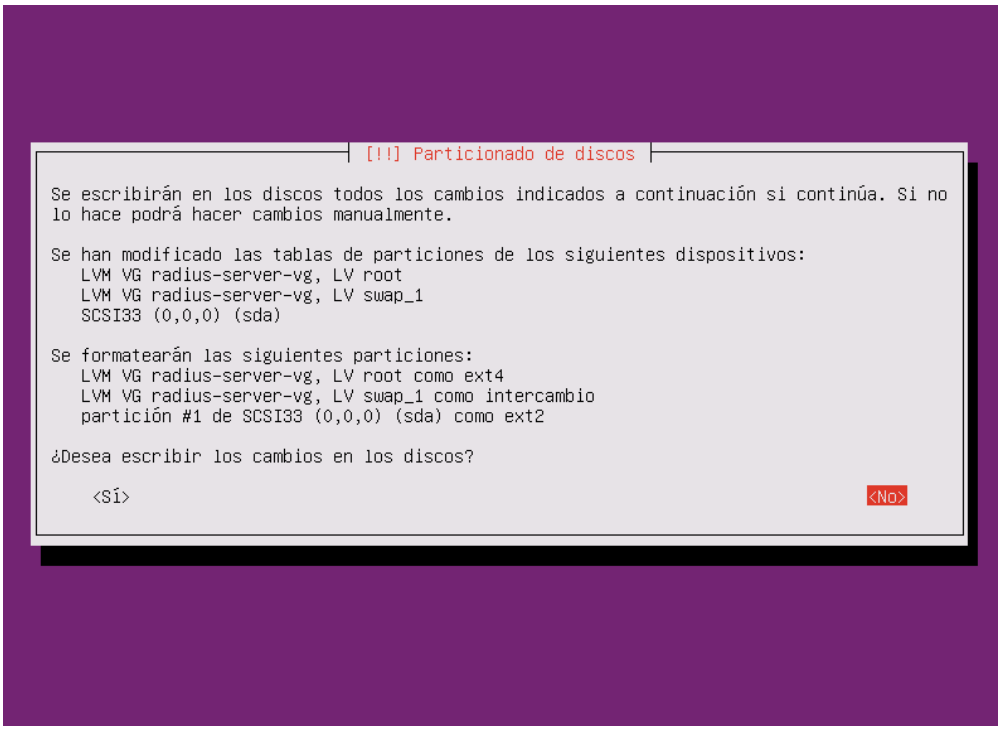


Figura 187 Inicio de Partición de Disco

Fuente: Sistema Operativo Linux Distribución Ubuntu 16.04

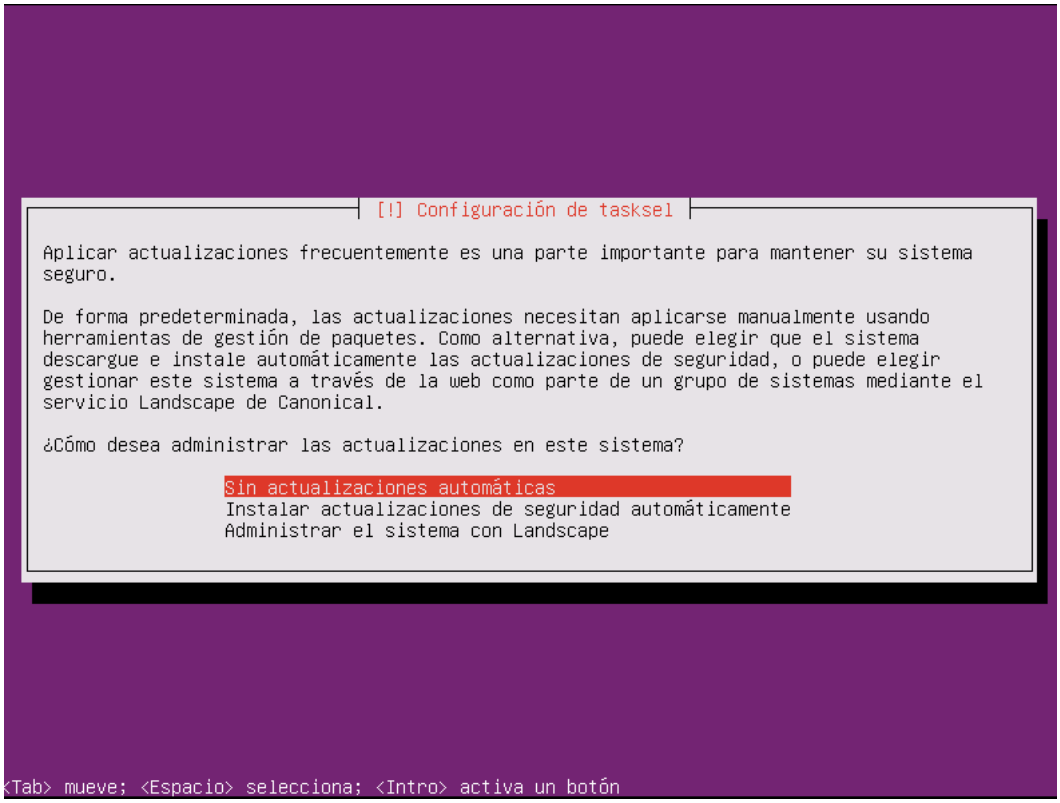


Figura 188 Configuración de actualizaciones

Fuente: Sistema Operativo Linux Distribución Ubuntu 16.04

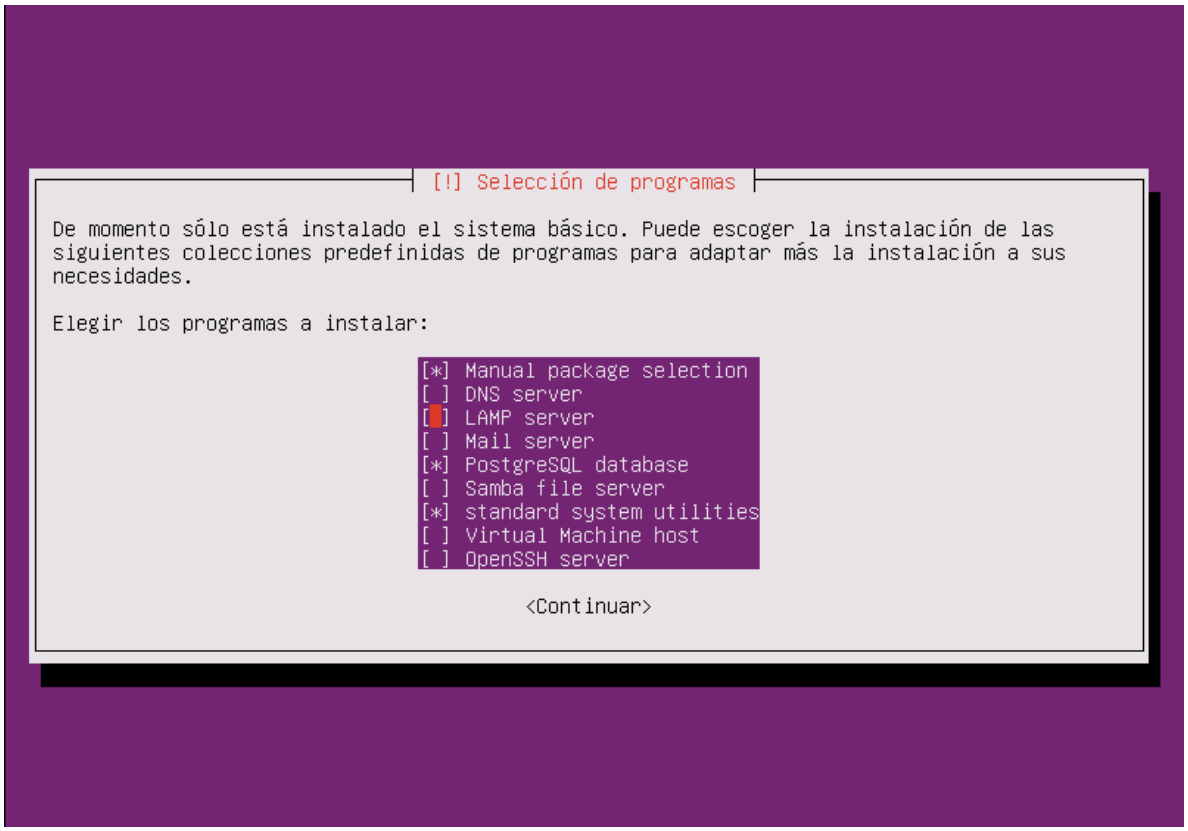


Figura 189 Selección de programas

Fuente: Sistema Operativo Linux Distribución Ubuntu 16.04

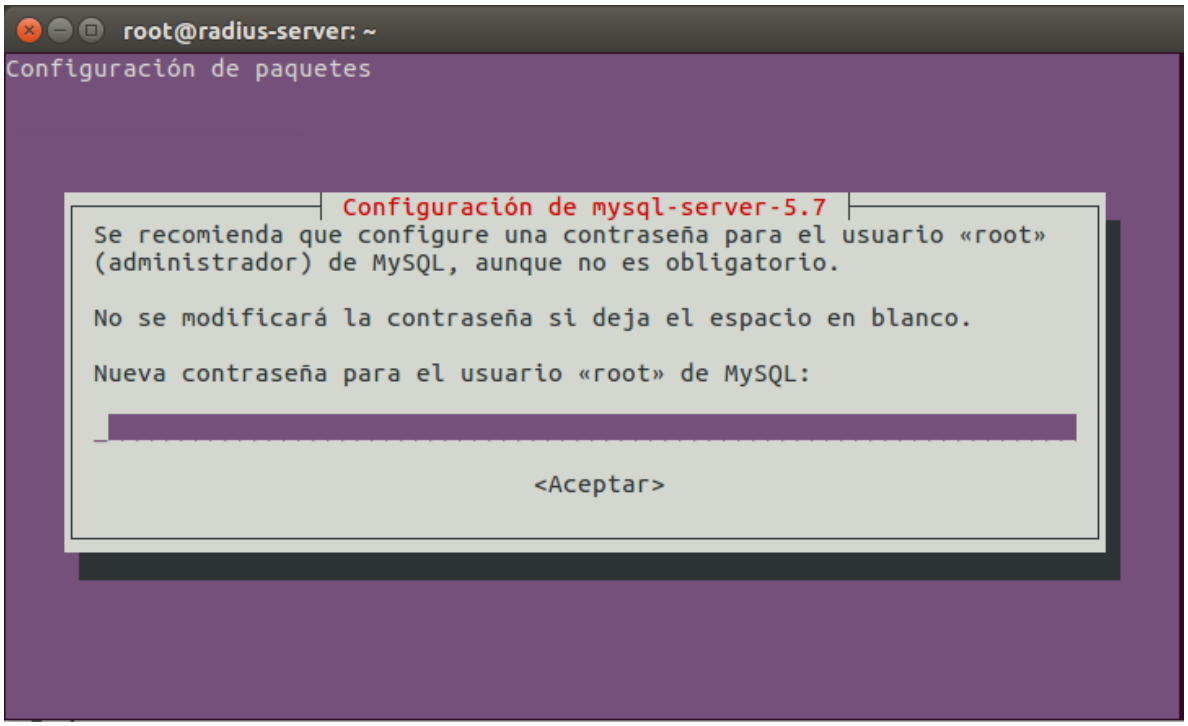


Figura 190 Contraseña Mysql

Fuente: Sistema Operativo Linux Distribución Ubuntu 16.04