UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

“DISEÑO Y GESTIÓN DE UNA RED INALÁMBRICA PARA LA ZONA CENTRAL DE SAN LUIS DE GUACHALÁ DEL CANTÓN CAYAMBE PARA BRINDAR EL SERVICIO DE INTERNET MEDIANTE LA TECNOLOGÍA 802.11AC, BASADA EN EL MODELO FUNCIONAL FCAPS DE LA ISO.”

AUTOR: NELSON ANDRES ACERO LANCHIMBA

DIRECTOR: MSC. CARLOS ALBERTO VÁSQUEZ AYALA

IBARRA – ECUADOR

2024

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO	
CÉDULA DE IDENTIDAD:	1727232223
APELLIDOS Y NOMBRES:	Acero Lanchimba Nelson Andres
DIRECCIÓN:	San Luis de Guachalá
EMAIL:	naasero@utn.edu.ec
TELÉFONO MOVIL:	0960135168

DATOS DE LA OBRA	
TÍTULO:	Diseño y gestión de una red inalámbrica para la zona central de San Luis de Guachalá del cantón Cayambe para brindar el servicio de internet mediante la tecnología 802.11ac, basada en el modelo funcional FCAPS de la ISO."
AUTOR :	Acero Lanchimba Nelson Andres
FECHA:	30 de enero del 2024
PROGRAMA:	PREGRADO
TITULO POR EL QUE OPTA:	Ingeniero en Electrónica y Redes en Comunicación
ASESOR /DIRECTOR:	MSc. Carlos Alberto Vásquez Ayala

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 30 días del mes de enero de 2024

EL AUTOR:

.....

Acero Lanchimba Nelson Andres

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

MAGISTER CARLOS VÁSQUEZ, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN

CERTIFICA:

Que, el presente trabajo de titulación **"DISEÑO Y GESTIÓN DE UNA RED INALÁMBRICA PARA LA ZONA CENTRAL DE SAN LUIS DE GUACHALÁ DEL CANTÓN CAYAMBE PARA BRINDAR EL SERVICIO DE INTERNET MEDIANTE LA TECNOLOGÍA 802.11AC, BASADA EN EL MODELO FUNCIONAL FCAPS DE LA ISO."** ha sido desarrollado en su totalidad por el Señor: **NELSON ANDRES ACERO LANCHIMBA** portador con número de cedula 172723223 bajo mi supervisión.

Es todo en cuanto puedo certificar en honor a la verdad.

Atentamente

Firmado electrónicamente por:
CARLOS ALBERTO
VASQUEZ AYALA

Ing. Carlos Vásquez, MSc

DIRECTOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

El presente trabajo va dedicado a mis Padres, Luis y Alicia quienes con esfuerzo y trabajo duro hicieron posible cumplir mis objetivos, superando los tropiezos presentados a lo largo de mi vida personal y profesional, este logro es tanto de ustedes como mío.

A mis hermanas Paola, Alison, Heidi por cuidarme y siempre estar pendientes de mí brindándome su apoyo incondicional.

A todos le agradezco de corazón muchas Gracias.

Nelson Andres Acero Lanchimba

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

Agradezco a mis padres Luis Acero y Alicia Lanchimba por darme vida por el apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles y por ayudarme con los recursos necesarios para estudiar.

A mi familia en general y a mi compañera de vida Paola por todo el apoyo brindado en todo momento a lo largo de la carrera universitaria

A mi director Ing. Carlos Vásquez, a mi Asesor Ing. Fabian Cuzme, por la ayuda y el tiempo brindado en el desarrollo del presente proyecto.

Al municipio de Cayambe por la colaboración brindada en su debido momento.

Nelson Andres Acero Lanchimba

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

El presente proyecto consiste en el diseño y gestión de una red inalámbrica para la zona central de la comunidad San Luis de Guachalá del Cantón Cayambe para brindar el servicio de internet mediante la tecnología 802.11ac basada en el modelo funcional FCAPS de la ISO, la cual permitirá el acceso al servicio de internet, ayudando a solucionar el problema de digitalización que tiene la comunidad, con ello mejorar la calidad de vida en aspectos de tecnología de información y comunicación. Mejorando así el trismo que tiene dicha comunidad. El Primer capítulo se detallará el planteamiento del problema, los objetivos. El alcance del proyecto y el motivo por que se realizara el proyecto de tesis, En el segundo capítulo se realizara un estudio del marco teórico de los temas que se tratara en el trabajo de grado, en el tercer capítulo se realizara el diseño de la red inalámbrica en base a criterios, se analizará el número de nodos, necesarios, el área de cobertura los canales de frecuencia en donde funcionara el radio enlace y la ubicación de los respectivos Access Points en dicho lugar, en el cuarto capítulo se gestionará la red en base a las políticas de Gestión ya existentes en el municipio de Cayambe con sus respetivas pruebas de funcionamiento tanto para el diseño de la red como para la Gestión.

ABSTRACT

This project consists of the design and management of a wireless network for the central area of the community San Luis de Guachalá of Cayambe Canton to provide internet service through 802.11ac technology based on the FCAPS functional model of ISO, which will allow access to internet service, helping to solve the problem of digitization that the community has, thereby improving the quality of life in aspects of information technology and communication. This will improve the community's situation. The first chapter will detail the problem statement, the objectives. The scope of the project and the reason why the thesis project was carried out, in the second chapter a study of the theoretical framework of the issues to be addressed in the degree work, in the third chapter the design of the wireless network based on criteria, the number of nodes will be analyzed, necessary, In the fourth chapter the network will be managed based on the management policies already existing in the municipality of Cayambe with their respective performance tests for both the design of the network and the management.

CAPITULO I: INTRODUCCION

Antecedentes

1.1 Tema

Diseño y Gestión de una red inalámbrica para la Zona central de San Luis de Guachalá del Cantón Cayambe para brindar el servicio de internet mediante la tecnología 802.11ac, basada en el modelo funcional FCAPS de la ISO.

1.2 Problema

En la actualidad la conectividad inalámbrica es la forma más fácil para establecer una conexión y poder comunicase, pero una red inalámbrica es vulnerable y complicado al momento de gestionar. El Gobierno Municipal de Cayambe tiene implementado redes inalámbricas las cuales proveen el servicio de internet a Instituciones Educativas Fiscales, sectores rurales y sectores urbanos, donde también se incluyen los parques principales de la ciudad de Cayambe. La topología que se utiliza en el Municipio de Cayambe es punto-multipunto para la transmisión y recepción de señales. Se utiliza repetidoras las cuales permitan la comunicación entre el punto central y los puntos de acceso, utilizando antenas que trabajen en bandas de frecuencia de 5GHz para la interconexión de la red inalámbrica.

La red inalámbrica del Municipio provee el servicio de internet a todas las comunidades del cantón Cayambe, pero no a la zona central de San Luis de Guachalá, dicho lugar no cuenta con un medio de comunicación con el municipio, debido a que no existe una propuesta de diseño de una red WLAN y no tener una antena de línea de vista directa con esta comunidad, a pesar de que existe una gran demanda de personas que visitan este lugar, además que cuenta con múltiples atractivos turísticos, en dicho lugar no se ha realizado un diseño de una red inalámbrica que cuente con un sistema de gestión para que brinde el servicio de internet.

Con el diseño de una red inalámbrica y la implementación de un sistema de gestión en la red inalámbrica en la Zona central de Guachalá se podrá gestionar y controlar el acceso a

internet, solucionando los posibles fallos que pueda existir en la red, se controlará el acceso de usuarios en horas en donde exista mayor demanda de usuarios que deseen acceder a la red. Instalación de nodos para mejorar la cobertura de red, con esto se conseguirá el acceso a la red inalámbrica con servicio de internet de manera rápida y segura, manteniendo una red estable, garantizando mayor disponibilidad de red y un alto rendimiento para los usuarios que visiten esta zona**.**

1.3 Objetivos

1.3.1 Objetivo general.

Realizar el diseño y Gestión de la red inalámbrica de la zona central de San Luis de Guachalá del cantón Cayambe, brindando el servicio de internet mediante la tecnología 802.11ac, usando el modelo funcional FCAPS de la ISO.

1.3.2 Objetivos específicos.

Diseñar una red inalámbrica WLAN, para brindar el servicio de internet a la zona central de la comunidad de San Luis de Guachalá.

Adaptar el nuevo diseño de la red a las políticas de Gestión ya existentes del modelo FCAPS en el municipio de Cayambe, selección de herramientas de gestión en software libre en base al estándar IEEE 29148.

Gestionar la red inalámbrica en base a las políticas de gestión, utilizando las herramientas de software libre y realizar de funcionamiento de la red inalámbrica.

1.4 Alcance

El presente proyecto tiene como finalidad el diseño de una red inalámbrica para lo cual se establecerá un estudio de las características que tiene el estándar IEEE802.11ac, fundamentos de redes inalámbricas, las áreas funcionales del modelo FCAPS (Gestión de Fallos, configuración, contabilidad, prestaciones y seguridad) de la ISO, se entenderá como trabaja el protocolo SNMPv2 en la capa aplicación, el intercambio de información entre gestores y agentes de las MIB para el diseño de la red inalámbrica.

Se analizará la situación geográfica de la comunidad San Luis de Guachalá y la infraestructura del municipio para determinar la mejor opción de enlace entre la zona central de la comunidad y un punto de acceso a la red del municipio, de forma inalámbrica mediante un radio enlace, debido a que no existe línea de vista, se realizará el cálculo del radio enlace en base a la trayectoria y los efectos a los que se encuentra expuesto, una vez analizado estos aspectos se seleccionará la antena más adecuada para levantar el radio enlace logrando así una transmisión de señales.

Una vez el enlace sea establecido se diseñará una red inalámbrica WLAN, en base a las necesidades de la zona central de la comunidad San Luis de Guachalá donde existe mayor número de usuarios, incluido usuarios locales y turistas que visitan este lugar. Para el diseño se analizará los canales de frecuencia, canales de operación, el ancho de banda, tasas de transferencia, área de cobertura, puntos con mayor afluencia de personas, números de APs y se establecerá los puntos de acceso de red necesarios para el cumplimiento de las necesidades actuales y futuras.

En base al análisis de puntos con mayor afluencia de usuarios, se establecerán políticas de gestión que ayude a controlar el acceso a la red evitando que esta colapse, además se utilizará el principio roaming con el objetivo de transferir el servicio de un

punto de acceso (AP) a otro punto de acceso (AP), cuando la potencia de la señal sea insuficiente, de esta manera no pierda conexión cuando el usuario se encuentre en movimiento.

Posteriormente se monitoreará la red en base a el estándar IEEE 29148 y se implementará sobre software libre una plataforma que cubra las 5 áreas funcionales del modelo FCAPS de la ISO.

Para cubrir la gestión de fallos (Fault Management) el modelo de gestión detectará un mal funcionamiento que exista en la red, aislará y resolverá los problemas que exista en la red, es necesario ser proactivo para minimizar los tiempos de reparación y maximizar los tiempos de medios entre fallos, para esto se utilizara el protocolo SNMP que permitirá controlar y medir el estado de la infraestructura de la red actual.

Para la Gestión de configuración (Configuration Management) se basará en la instalación y configuración de los sistemas de software que conforma el sistema de gestión, en esta fase se establecerá un ambiente amigable para el administrador, en donde se mostrará la topología, la distribución de los puntos y elementos de la red, permitiendo la supervisión y control de los equipos que conformen la topología de la red.

En la gestión de contabilidad (Accounting Management) se administrará la utilización de los recursos, en este proceso se distribuye los recursos de ancho de banda dependiendo de las necesidades que se van a utilizar por los usuarios, puntos de acceso y los servicios, los cuales ayudaran a reducir el coste operacional, logrando así proporcionar un servicio de calidad sin interrupciones.

En la gestión de prestaciones o gestión del rendimiento (Performance Management) implica monitorear la red para conocer el estado actual de la misma y así poder presentar informes ya sea de forma historial, estadística, textual, o resúmenes de la información que tiene en la base de datos, permitiendo así tener monitoreada la red constantemente, de manera que el administrador pueda solucionar los problemas de una manera más fácil en el menor tiempo posible y poder mejorar el rendimiento de la red.

En la gestión de seguridad (Security Management) se encargará del acceso a la plataforma de red en donde se protegerá la confidencialidad de los usuarios y brindar su respectiva seguridad.

Para las pruebas de funcionamiento en base a la cobertura de red se realizará en la zona central de la comunidad San Luis de Guachalá utilizando un mapa de calor para determinar la ubicación de los APs, manejando un software libre y para las pruebas del sistema de gestión se realizaran en un ambiente de trabajo controlado previo a una comparación y selección del software más idóneo que trabaje con el protocolo simple de gestión de la red (SNMPv2), lo que permitirá la transmisión de información entre gestores y agentes mediante el envío de mensajes SNMP y TRAPS. También se instalará un sistema de seguridad para controlar el acceso mediante un portal cautivo que funcionará como Gateway para el acceso al servicio de internet.

1.5 Justificación

El uso de las redes inalámbricas ha facilitado el uso del servicio de internet. El Plan Nacional de telecomunicaciones y tecnologías (2016-2021) promueve el uso de las tecnologías de la información y comunicación para establecer el camino hacia la sociedad de la información y el conocimiento en especial el acceso al servicio de internet que es utilizado como la principal herramienta de trabajo en instituciones Educativas e

Instituciones Públicas. El Gobierno Autónomo Descentralizado Intercultural Plurinacional (GADIP) del municipio de Cayambe forma parte de entidades públicas donde se promueven proyectos de innovación tecnológica para cumplir con proyectos que ayuden a la digitalización de la comunidad. (MINISTERIO DE TELECOMINICACIONES, 2016-2021).

El diseño de la red inalámbrica beneficiara tanto a la comunidad como a las personas que visiten este lugar como se indica en la constitución de la República del Ecuador tiene vigente desde el año 2008 en el Plan del Buen vivir en donde se trata los derechos de los ciudadanos en la tercera sección, Comunicación e Información: "Todas las personas, en forma individual o colectiva tienen derecho al acceso universal a las tecnologías de información y comunicación". Con la instalación de la red Inalámbrica y el uso del modelo de gestión. Además de contar con el servicio de internet, simplificara los procesos de monitorización, administración y protección de sus redes, el proceso de gestión que brinda el modelo funcional FCAPS ayudará a que el servicio de internet sea continuo, la red podrá cumplir su trabajo de manera más efectiva, con buena disponibilidad y un alto rendimiento en la red beneficiando al administrador de la red.

Con la implementación del modelo de gestión se plantea mejorar el acceso y la disponibilidad de la red además de brindar el servicio de internet a los usuarios, facilitando a los administradores de la red trabajar de manera más eficiente, reducir el tiempo en la resolución de fallas en la red optimizar los recursos económicos del municipio de Cayambe beneficiando a los usuarios que accedan a la red disponiendo de un servicio contante y de calidad.

CAPITULO II

MARCO TEORICO

Este capítulo abordará conceptos básicos referentes a las redes inalámbricas en general y a las redes de área local, se describirá y explicará las diferentes tecnologías inalámbricas, definiciones, principales características, diferencias, problemas de seguridad, administración y gestión de redes entre otras. Así como también los estándares IEEE 802.11ac y el modelo funcional FCAPS.

2.1 Redes Inalámbricas

Las redes inalámbricas es un conjunto de elementos que permiten la comunicación entre diferentes dispositivos sin la necesidad de un cable, este proceso se realiza mediante ondas electromagnéticas u ondas de radio, aún si se encuentran separados a una cierta distancia o incluso en movimiento, es una de las tecnologías más utilizadas en la actualidad, proporcionado libertad de movimiento en cualquier parte de un determinado lugar. En la actualidad las redes inalámbricas son una de las tecnologías más prometedoras y una de las principales ventajas de las redes inalámbricas respecto a las redes cableadas son sus costos debido a que se elimina el cable ethernet y para ampliar una red inalámbrica es mucho más económico y tiene una fácil instalación (Wireless Networks, 2015).

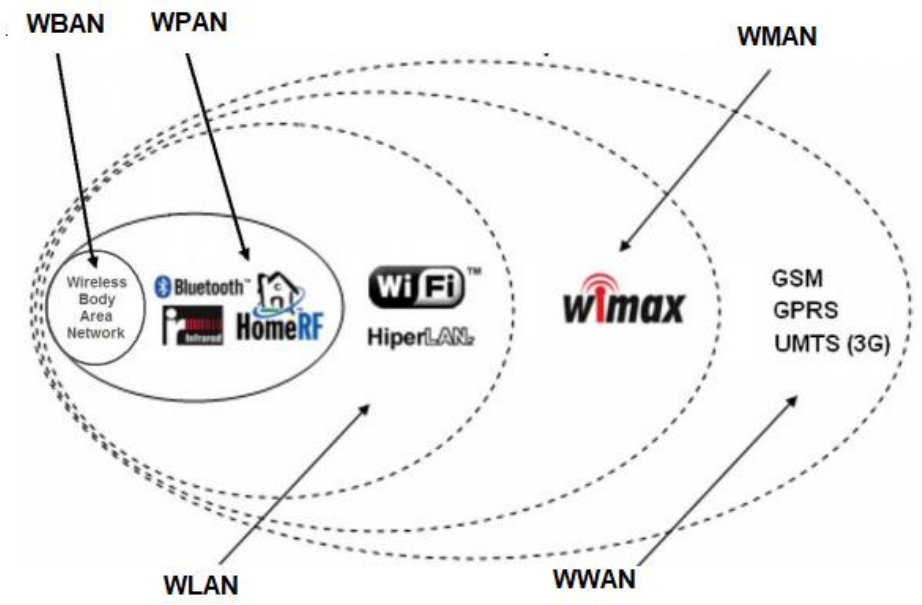
Según Salazar (2012), menciona que “Las redes inalámbricas permiten a los dispositivos remotos que se conecten sin dificultad, independientemente que estos dispositivos estén a unos metros o a varios kilómetros de distancia. Todo ello sin necesidad de romper paredes para pasar cables o instalar conectores. Esto ha hecho que el uso de esta tecnología sea muy popular, extendiéndose muy rápidamente.”

2.1.1 Tecnologías de Redes Inalámbricas

Las redes inalámbricas se pueden clasificar en diferentes tecnologías según su cobertura, por ejemplo: las redes inalámbricas de área corporal (WBAN), las redes inalámbricas de área personal (WPAN), las redes inalámbricas de área local (WLAN), las redes inalámbricas de área metropolitana (WMAN) y las redes inalámbricas de área amplia (WWAN), en la Figura 1 se puede observar la clasificación de las tecnologías inalámbricas.

Figura 1

Clasificación de las Tecnologías Inalámbricas



Fuente: Recuperado de (Salazar, 2012, pág 7)

2.1.1.1 Redes Inalámbricas de área corporal (WBAN)

Las redes Inalámbricas de área corporal por sus siglas en inglés (WBAN: Wireless Body Area Network) es una tecnología que ayuda en el ámbito de la salud y sanidad, su

objetivo es conseguir un mayor grado de interacción entre los usuarios y los servicios que implica la presencia de conexiones entre los dispositivos electrónicos y dispositivos de comunicación que el usuario puede ser integrado en su ropa o en su cuerpo, esto se refiere a que los sensores pueden ubicarse en el cuerpo como diminutos parches inteligentes o pueden ser implementados bajo la piel o en los músculos.

Las WBAN tienen plataformas básicas para sensores accesibles, diminutos y ligeros. Los dispositivos que trabajan en esta tecnología pueden ser equipos complejos como un teléfono celular o dispositivos simples como un auricular o un visor adaptado en unas gafas, normalmente tiene un alcance de uno o dos metros. (Wireless Networks, 2015).

2.1.1.2 **Redes inalámbricas de área personal (WPAN)**

Las redes Inalámbricas de área personal por sus siglas en inglés (WPAN: Wireless Personal Area Network), están diseñadas para interconectar de manera inalámbrica a equipos móviles sin la necesidad de cables, entre los diferentes dispositivos se encuentran: teléfonos móviles, laptops, impresora, cámaras de fotos, Smart TV, electrodomésticos o Asistentes Personales Digitales (PDAs), entre otros, su área se limitada a unos cuantos metros en donde el usuario puede moverse sin perder la conexión (Lorenzana, 2018).

Existen varios tipos de tecnología WPAN:

- Bluetooth es una de las más importantes debido a que tiene un alcance aproximado a treinta metros y una velocidad máxima de 1 Mbps, con un bajo consumo de energía.

- HomeRF por sus siglas en inglés Home Radio Frequency. Esta tecnología se basa en el teléfono inalámbrico digital mejorada. Tiene un alcance variado dependiendo

en el ambiente en que se encuentre puede alcanzar de 50 a 100 metros sin utilizar ningún tipo de amplificador, su velocidad puede llegar a 10 Mbps como máximo. Esta tecnología se abandonó en enero de 2003 debido a sus fabricantes.

- La tecnología Zigbee tiene un alcance máximo de 100 metros, puede alcanzar una velocidad de transferencia de hasta 250Kbps.y funciona en la banda de frecuencia de 2,4 GHz y en 16 canales.

- La Tecnología de Infrarrojos tiene un radio de unos pocos metros y una velocidad de unos pocos megabits, esta tecnología se utiliza más en domótica.

2.1.1.3 **Redes inalámbricas de área local (WLAN)**

Las redes inalámbricas de área local por sus siglas en inglés (WBAN: Wireless Local Area Network), se refiere a una red que cubre un área similar a la red local de una empresa, con un alcance aproximado de 100 metros, permitiendo que los usuarios terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí (Pillou, 2008).

Un ejemplo de esta tecnología es el Wifi o IEEE 802.11 son redes locales que están diseñadas para interconectar equipos informáticos en movilidad dentro de un edificio, enlaces de corta y media distancia con quipos fijos. Su alcance cubren distancias entre los 10 a 100 (Lorenzana, 2018).

2.1.1.4 **Redes inalámbricas de área metropolitana (WMAN)**

Las WMAN están diseñadas para la creación de enlaces a grandes velocidades y largas distancias, el estándar más significativo es WiMax por sus siglas en inglés (Worldwide Interoperability for Microwave Access) considerada como una alternativa de bajo costo para el reemplazo de cable MODEM y como una red de acceso

inalámbrico operando en un centro de negocios en una ciudad principal. La cual se estima alcanzara distancias aproximadas a 50 Km(Lorenzana, 2018).

Las redes WMAN permiten conexiones inalámbricas dentro de un área metropolitana ejemplo: campus universitarios, oficinas de edificios de una ciudad, etc. Según (Cerro, 2015) dice que "WMAN utiliza ondas de radio o luz infrarroja para transmitir los datos. Tienen un radio de acción mayor que el de las WLAN. Del orden de varias decenas de kilómetros. Lo suficiente para cubrir una población completa. Las WMAN pueden interconectar unas WLAN con otras".

2.1.1.5 Redes inalámbricas de área amplia (WWAN)

Las WWAN tienen el alcance más amplio de todas las redes inalámbricas, de esta manera todos los dispositivos móviles están conectados a una red inalámbrica extensa. Su infraestructura consta de antenas y torres ubicados en lugares altos estratégicos, para transmitir ondas de radio y ondas microondas con el fin de conectarse a diferentes redes de área local (Estrada, 2013). En esta tecnología se menciona 3 tipos de redes WWAN: Sistema Global para las comunicaciones Móviles (GSM), Servicio general de paquetes vía radio (GPRS) y el Sistema Universal de Telecomunicaciones móviles (UMTS).

Las WWAN es considerada una tecnología de tercera generación de la telefonía móvil debido a que tiene capacidades multimedia, capacidad elevada de acceso a internet lo que permite transmitir audio y video en tiempo real y una transmisión de voz equiparable a la telefonía móvil (Estrada, 2013).

2.2 Características de las Redes Inalámbricas

Las redes inalámbricas ofrecen múltiples ventajas sobre redes de área local convencionales, por ejemplo: Velocidad, Movilidad, Flexibilidad, Escalabilidad, y

costos reducidos en la instalación. Es una tecnología que ayuda a la solución de problemas de arquitectura en edificios históricos (Ramírez & Díaz, 2008).

A continuación, se describen las principales ventajas de las redes inalámbricas:

- Garantiza compatibilidad con el mayor número de dispositivos inalámbricos.
- Es rápida y fácil de instalar, elimina la necesidad de cablear atreves de paredes y techos.
- Las redes inalámbricas es un robusto estándar bien establecido que continúa creciendo y evolucionando.
- Tiene un alcance variado según el tipo de red puede ir de unos pocos metros a algunos kilómetros.
- Se puede elegir hubs inalámbricos que ofrezcan servidores DHCP incorporados, en lugar de un servidor DHCP independiente.
- Fácil interacción con las redes de área local cableadas
- En escalabilidad un buen hub inalámbrico puede soportar hasta 60 usuarios simultáneos, permitiendo expandir la red con mucha facilidad.
- Capacidad automática de conexión a la red de un punto a otro, transferir las comunicaciones sin interrupciones sin la necesidad de reconfigurar la dirección IP
- Una fácil configuración para acceder a la red.

Como en toda tecnología existen ventajas y desventajas a continuación se describen los principales inconvenientes de las redes inalámbricas (Salazar, 2012):

- La transferencia de datos se ve afectado por la interferencia de cambios climáticos como pueden ser: lluvia, neblina, fuertes vientos, etc.
- Los teléfonos inalámbricos que trabajan en la misma frecuencia también provocan interferencias.
- La velocidad de las redes inalámbricas es limitada, mientras que las redes cableadas tienen velocidades mucho más altas.
- Con respecto a la seguridad, por el hecho de emir su señal por aire existe posibilidades que una persona no autorizada pueda acceder a la red.

2.3 IEEE 802.11

El estándar IEEE 802.11 es un conjunto de estándares de comunicación del Instituto de ingenieros eléctricos y electrónicos, es un estándar internacional que define los protocolos a usarse en los niveles de la arquitectura del modelo OSI, la capa física y la capa de enlace de datos, dicho estándar norma muchas reglas de las redes inalámbricas de área local en las bandas de frecuencias 2,4 GHz, 5 GHz, y 60 GHz. (Lorenzana, 2018). según Pérez (2006) menciona que el estándar 802.11 “Son las reglas definidas por la IEEE sobre las tecnologías de redes inalámbricas, mismas que determinan los parámetros sobre la interfaz en el aire entre dos clientes o un cliente y una estación”.

Este estándar se encuentra basado en una arquitectura de tipo celular. Esta arquitectura se encuentra dividida en celdas donde cada una de ellas está controlada por

una estación llamada Punto de Acceso (AP), y estos Puntos de Acceso se encuentran conectados a un Sistema de Distribución (Lorenzana, 2018).

2.3.1 Principales estándares IEEE 802.11

El Instituto de Ingenieros Eléctricos y Electrónicos 802.11 ha generado una seria de estándares de redes inalámbricas desarrolladas por un grupo de trabajo del comité de estándares LAN/MAN (Herrera Ramírez, Díaz Ramírez, & Calafate, 2007). Estos estándares se detallan a continuación siendo los más populares.

El estándar IEEE 802.11 tenía velocidades de 1 y 2 Mbps que trabajaba en la banda de frecuencia de 2,4 GHz, presentaba dos tipos de modulación de frecuencia FHSS (Espectro extendido de salto de frecuencia) y DSSS (Espectro extendido de secuencia directa), de la misma manera la modulación del espectro infrarrojo. En octubre de 1999 nacieron las dos primeras modificaciones del estándar original de la IEEE 802.11: las variantes IEEE 802.11a e IEEE 802.11b.

El estándar IEE 802.11a es aplicada en la banda Unlicensed National Information Infrastructure (UNII) de los 5 GHz (de 5.150 MHz a 5.350 MHz y de 5.470 a 5.725 MHz). Este estándar utiliza la modulación OFDM, por lo que resulta más robusta ante las interferencias multitrayecto, mejorando el rendimiento en espacios interiores. Permite velocidades de hasta 54 Mbps, y el principal inconveniente es la incompatibilidad con los estándares 2,4 GHz y la perdida de absorción en obstáculos. Fuera de eso este estándar es similar al 802.11g (Radio Comunicaciones, 2006).

Por otro lado, el estándar 802.11b fue aprobado en el año 1999 y trabaja en la banda de 2,4 GHz, accediendo a una tasa de transmisión de 5,5Mbps y 11 Mbps de velocidad, utilizando el mismo método de acceso al medio que el estándar 802.11 en dicha época

se pensaba que no era posible superar los 6 Mbps con el protocolo UDP. Cuando apareció la modulación DSSS (Direct-Sequence Spread Spectrum) surgieron los primeros equipos que eran extensión de la modulación original. Con la reducción del costo y el aumento de la velocidad se logró un rápido crecimiento de la demanda y oferta (Herrera Ramírez et al., 2007).

En el año 2003 el estándar 802.11g fue diseñado como el sucesor de IEEE 802.11b con un mayor ancho de banda. En este estándar un punto de red puede soportar el estándar IEEE 802.11b y el estándar IEEE 802.11g, esto se debe a que las redes inalámbricas basadas en 802.11g utilizan la banda 2,4 GHz que utiliza la IEEE 802.11b, con una velocidad de transferencia máxima de enlace inalámbrico de 54Mbps dependiendo del entorno en el que se encuentre, si existe obstrucciones en la señal de radio de cobertura la señal se reducirá (Salazar, 2012).

El siguiente paso se dará con la norma 802.11n que sube el límite teórico hasta los 600 Mbps. Según (Herrera Ramírez et al., 2007) menciona que “El objetivo principal por el cual se aceptó la creación del estándar 802.11n es definir modificaciones en la capa física y la capa de control de acceso al medio para alcanzar una velocidad de procesamiento de dato de 100 Mbps en la capa MAC SAP (Media Access Control Layer, Service Access Point) situada en el tope de la capa de control de acceso al medio”. Teniendo en cuenta estos requerimientos se obtiene aproximadamente un flujo de 4 veces mayor respecto a los otros Estándares.

2.3.1.1. Comparación entre estándares

A continuación, en la Tabla 1 se muestra la comparativa de los principales estándares 802.11 con su respectiva frecuencia, ancho de banda, velocidad de transmisión, canal y el año de lanzamiento.

Tabla 1

Comparación Estándares 802.11

ESTANDAR	Frecuencia	Ancho de Banda	Velocidad de Transmisión	Canal	Año
802.11	2,4 GHz	20 MHz	2Mbps	DSS, FHSS	1997
802.11a	5 GHz	22 MHz	54 Mbps	OFDM	1999
802.11b	2,4 GHz	21 MHz	11 Mbps	CCK, OFDM	1999
802.11g	2,4 GHz	23 MHz	54 Mbps	DSSS, OFDM	2003
802.11n	2,4 GHz y 5Ghz	24 y 40 MHz	600 Mbps	OFDM	2009
802.11ac	5 GHz	20, 40, 80, 160 MHz	1,3 Gbps	OFDM	2013

Fuente: Elaborado por el autor

2.3.2 Arquitectura de la Red IEEE 802.11

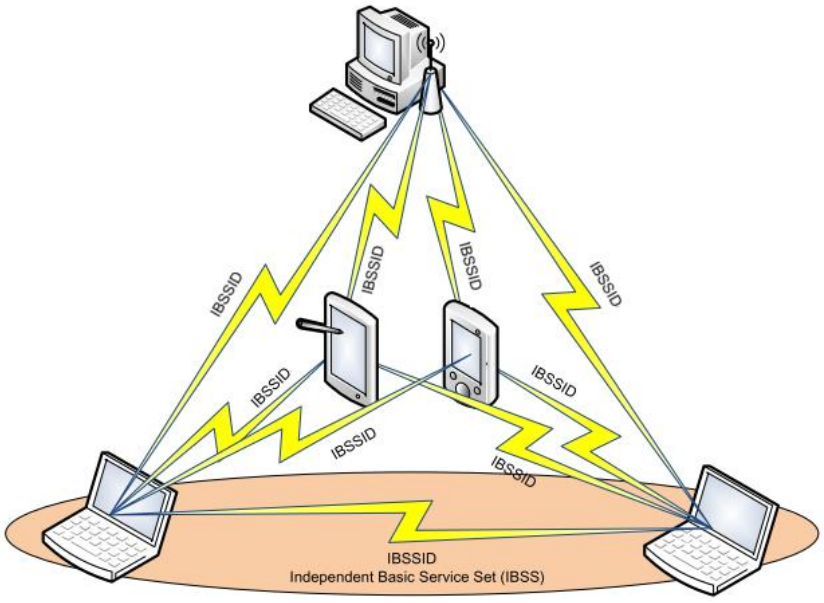
La Arquitectura de estándar IEEE 802.11 define dos modos de configuración para el funcionamiento de una red inalámbrica: el modo Ad-Hoc, en donde los dispositivos transmiten punto a punto y el modo infraestructura en donde los dispositivos se comunican a través de un punto de acceso que sirve de puente para otras redes, más conocida como punto a multipunto. La arquitectura de comunicación de una red especifica la funcionalidad del sistema y sus componentes de red (Lorenzana, 2018).

2.3.2.1 Modo Ad-Hoc

Una red Ad-Hoc inalámbrica es un tipo de red inalámbrica descentralizada. Esta red no depende de una infraestructura preexistente como routers o puntos de acceso, permitiendo a los equipos inalámbricos interconectarse entre sí, estableciendo conexiones punto a punto. Cada una de estas redes punto a punto se denominan conjunto de servicios básicos independientes por sus siglas en inglés (IBSS: *Independent Basic Service Set*), y las conexiones tendrán un identificador propio denominado Identificador de conjunto de servicio básico independiente por sus siglas en inglés (IBSSID: Independent Basic Service Set Identifier) como se muestra en la Figura 2 (Lorenzana, 2018).

Figura 2

Esquema de red modo Ad-Hoc



Fuente: Recuperado de (Lorenzana, 2018, pág. 37)

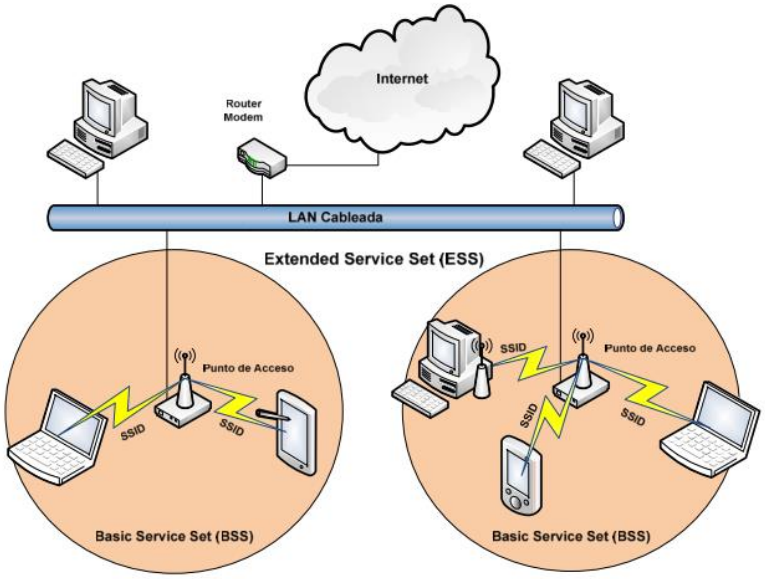
2.3.2.2 Modo Infraestructura

En el modo infraestructura, los equipos que conforman la red este modo se conectan entre sí a través de un Punto de Acceso, que, a la misma vez ofrece el acceso a una red cableada. Es la manera habitual de establecer una red inalámbrica. Al área de cobertura de un punto de acceso se le conoce con el nombre de (BSS) y se identifica mediante un nombre de red denominado (SSID).

La red se puede componer de varios Puntos de Acceso interconectados entre sí de forma cableada, lo que se conoce como una (ESS). Este conjunto de BSS pueden compartir un mismo SSID, denominándose en ese caso (ESSID), como se muestra en la Figura 3 (Lorenzana, 2018).

Figura 3

Esquema de red en modo Infraestructura



Fuente: Recuperado de(Lorenzana, 2018, pág 38)

2.3.3 Componentes de la Arquitectura

En la Arquitectura de Red existe diversos términos y componentes que se utilizan para realizar una conectividad de una red inalámbrica, a continuación se definirán cada uno de los componentes (Salazar, 2012):

Estación

Una estación conocida en inglés como (STA: Station) puede ser considerado una portátil, computadora de mesa, celular o cualquier dispositivo móvil, el cual posea la tecnología de transmitir información por el medio inalámbrico.

Punto de Acceso (AP)

Un punto de acceso por sus siglas en inglés (AP: Access Point), en ocasiones llamado Estación Base (SB: Base Station), son dispositivos que se usan para establecer conexiones inalámbricas entre 30 metros a 100 metros, formando una red inalámbrica externa conocida como (red local o red de internet) con el área de Red. Logrando eliminar las conexiones cableadas.

Conjunto de servicios básicos (BSS)

El Conjunto de Servicios Básicos por sus siglas en inglés (BSS: Basic Service Set) consiste en un punto de acceso, con el resto de las estaciones asociadas. Este punto actúa como maestro para controlar las estaciones dentro del conjunto de servicios básicos (BSS). El conjunto más simple se conforma de un punto de acceso (AP) y una estación (STA).

Conjunto de servicios extendidos (ESS)

El Conjunto de Servicios Extendidos por sus siglas en inglés (ESS: Extended Service Set) consiste en el conjunto de uno o más conjuntos interconectados de servicios básicos

que aparecen en un solo conjunto de servicios básicos a la capa de control de enlace lógico de cualquier estación asociada con un conjunto de servicios básicos.

Independiente conjunto de servicios básicos (IBSS)

Un Independiente Conjunto de Servicios Básicos por sus siglas en inglés (IBSS: Independent set of basic services) se refiere a todas las estaciones de conjunto de servicios básicos son estaciones móviles donde no existe ninguna conexión a red cableada, más conocida como red AD HOC la cual no tiene puntos de acceso, lo que significa que no puede conectarse a cualquier otro conjunto de servicios básicos (BSS).

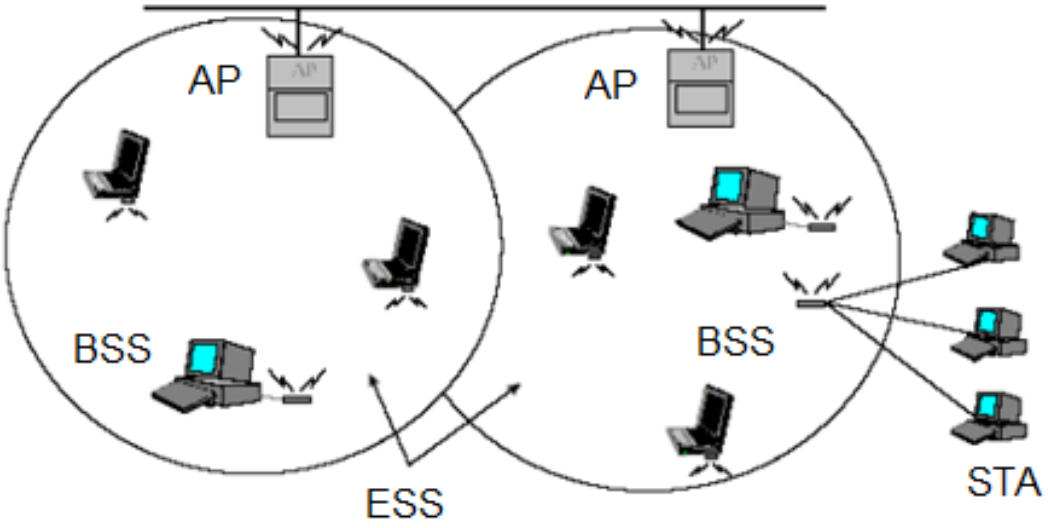
Sistema de distribución (DS)

Un sistema de distribución por sus siglas en inglés (DS: Distribution system) es un mecanismo por el cual diferentes puntos de acceso pueden intercambiar tramas entre sí o con las redes cableadas, si las hubiera. El sistema de distribución no es necesariamente una red y el estándar IEEE 802.11 no especifica ninguna tecnología en particular para el sistema de distribución (DS). En la mayoría de los productos comerciales se utiliza Ethernet por cable como la tecnología de red troncal.

En la Figura 4 se muestra un sistema de distribución de la arquitectura de red inalámbrica 802.11 con sus componentes antes mencionados.

Figura 4

Sistema de distribución



Fuente: Recuperado (IEEEStandards, 2016)

2.4 Estándar IEEE 802.11AC

En la actualidad estamos conectados de forma inalámbrica a través de muchos dispositivos portátiles como teléfonos móviles, impresoras y todo tipo de electrodomésticos, desde videoconsolas hasta cámaras digitales. Cada vez son más los dispositivos que se comunican sin cables y nos permiten navegar por Internet desde cualquier lugar. Todo el proceso de comunicación se basa en un protocolo estándar desarrollado para redes inalámbricas, denominado 802.11, comercializado como Wi-Fi (Peralta, 2014).

Este protocolo 802.11 ha evolucionado continuamente, hasta que en diciembre de 2012 se lanzó el estándar IEEE 802.11ac que es una propuesta de mejora a la norma IEEE 802.11n que se viene utilizando actualmente. El nuevo estándar inalámbrico 802.11ac tiene por objetivo garantizar una mayor velocidad a tu red inalámbrica, con un aumento en la eficiencia del 10 % y un consumo de energía menor, proporciona un

alcance mayor a velocidades Gigabit Ethernet (El nuevo estándar inalámbrico 802.11ac, s/f).

2.4.1 Migración del estándar 802.11n a 802.11 ac

Los sistemas de comunicación de telecomunicaciones del mundo se basan en protocolos y estándares con el objetivo de establecer normas y reglamentos para su correcto y eficiente funcionamiento. El estándar IEEE 802.11ac es una evolución lógica del estándar IEEE 802.11n debido a una modificación y mejora tecnológica del estándar (Ortiz, 2015).

Después de inspeccionar y estudiar los sistemas de transmisión 802.11n y 802.11ac; Se afirma que 802.11ac es mucho más rápido que 802.11n. La medición del rendimiento es el único indicador real del rendimiento de 802.11ac y se basa en tecnologías introducidas en 802.11n, como MIMO, formato de trama en cascada, canales más amplios y transmisión espacial adicional. Debido a todas estas posibilidades, la intensidad de la señal no es un indicador real del rendimiento de la WLAN (Fluke Networks, 2014). 802.11ac es compatible con versiones anteriores de 802.11n y 802.11a y funciona en entornos de modo mixto en la banda de 5G Hz (Ortiz, 2015).

El rendimiento del cliente 802.11ac puede verse afectado negativamente debido a las bajas velocidades de transferencia del cliente 802.11a/n. El estándar 802.11ac ofrece canales extendidos de 80 MHz y 160 MHz que permiten un mayor rendimiento. El uso de canales más anchos en 802.11ac aumenta el potencial de interferencia de los canales adyacentes y esto afecta negativamente el rendimiento (Ortiz, 2015).

2.4.2 Características principales

- Las tasas de transferencia mucho más altas, hasta 1,3 Gbps con tres transmisiones de 433 Mbps cada una. Por su velocidad, este estándar también se conoce como Wi-Fi 5G o Wi-Fi Gigabit. Un rango de cobertura más amplio, un máximo de 90-100 metros, es lo que suelen demandar los consumidores para este tipo de conexión (Peralta, 2014).

- Opera en la banda de 5 GHz, proporcionando más canales libres de interferencias y "menos población", por lo que ofrece una mayor estabilidad de conexión y un mayor radio de operación (Peralta, 2014).

- La nueva gama incorpora beamforming, una tecnología que permite a los routers y puntos de acceso dirigir las ondas de radio con mayor precisión, mejorando la recepción.

- Mayor ancho de banda de hasta 160 MHz (40 MHz en redes 802.11n), hasta 8 transmisiones MIMO (4 en 802.11n) y modulación de alta densidad, 256-QAM (64-QAM en 802.11n).

2.4.3 Aspectos técnicos del estándar 802.11 ac

Mayor densidad de codificación: Esto significa que se utiliza una mayor modulación, lo que permite enviar más datos, pero, por otro lado, es más susceptible a interferencias.

Mayor flujo de numero de datos: en el actual estándar 802.11n, se pueden transmitir hasta cuatro flujos de datos, lo que significa que la velocidad máxima se puede aumentar 4 veces. En el nuevo estándar, se pueden transmitir hasta 8 flujos simultáneamente. También se debe tener en cuenta que la tecnología para lograr esto dista mucho de ser simple y requiere hasta 8 antenas por punto de acceso (Ubierna, 2013).

Beamforming: la antena puede dirigir la potencia transmitida a la ubicación donde se encuentra el usuario, ajustándose dinámicamente a medida que el usuario cambia su ubicación en relación con el punto de acceso. Esto ayuda a evitar interferencias y mejora la cobertura.

Canales más amplios: los estándares Wifi-originales usaban canales de 20 MHz, en 802.11n permitían el uso de canales de 40 MHz, el nuevo 802.11ac tenía que usar canales de hasta 160 MHz para obtener el ancho de banda máximo. El principal problema con esto es que 160MHz es la frecuencia completa disponible y nos dará un canal para usar en todas las aplicaciones Wifi con problemas de interferencia (Ubierna, 2013).

MIMO multiusuario: varios usuarios pueden recibir información simultáneamente a toda velocidad. Esto hace posible utilizar el ancho de banda disponible de manera más eficiente y transmitir más información.

2.4.4 Modulación y Velocidad 802.11ac

La mayor ventaja para los administradores de redes puede ser la habilidad de manejar un mayor número de dispositivos sin degradaciones inaceptables en el rendimiento. Dado el hecho de que más usuarios están accediendo a la red inalámbrica con varios dispositivos (teléfonos, tabletas y otros dispositivos smarth), la actualización del AP a 802.11ac proporciona una mejora a un costo moderado. La ventaja de las características de 802.11ac permitirá que las soluciones Wi-Fi cumplan con la demanda actual de las aplicaciones en tiempo real de teléfonos de alta calidad y capacidad, tales como vídeo y voz (Avila, 2014).

El estándar 802.11ac logra su aumento de velocidad pura de varias maneras:

- Más unión de canales, aumentando el máximo de 40MHz en 802.11n y ahora hasta 80 y pronto 160 MHz.

- Una modulación más densa, ahora usando modulación de amplitud en cuadratura (QAM) de 256, comparada con 64 QAM de 802.11n.

- Un número más elevado de flujos espaciales. 802.11ac es compatible con ocho flujos espaciales, más que los cuatro de 802.11n.

- La simplificación de la capacidad de formación de haces de transmisión, que primero fue introducida con 802.11n. La nueva tecnología MU-MIMO o MIMO de varios usuarios, permite a un AP enviar tramas a varios usuarios al mismo tiempo en la misma frecuencia. Así que, por primera vez, un AP puede actuar algo así como un switch de Ethernet en lugar de un concentrador, asistiendo a más usuarios.

2.4.5 Transmisor y receptor 802.11ac

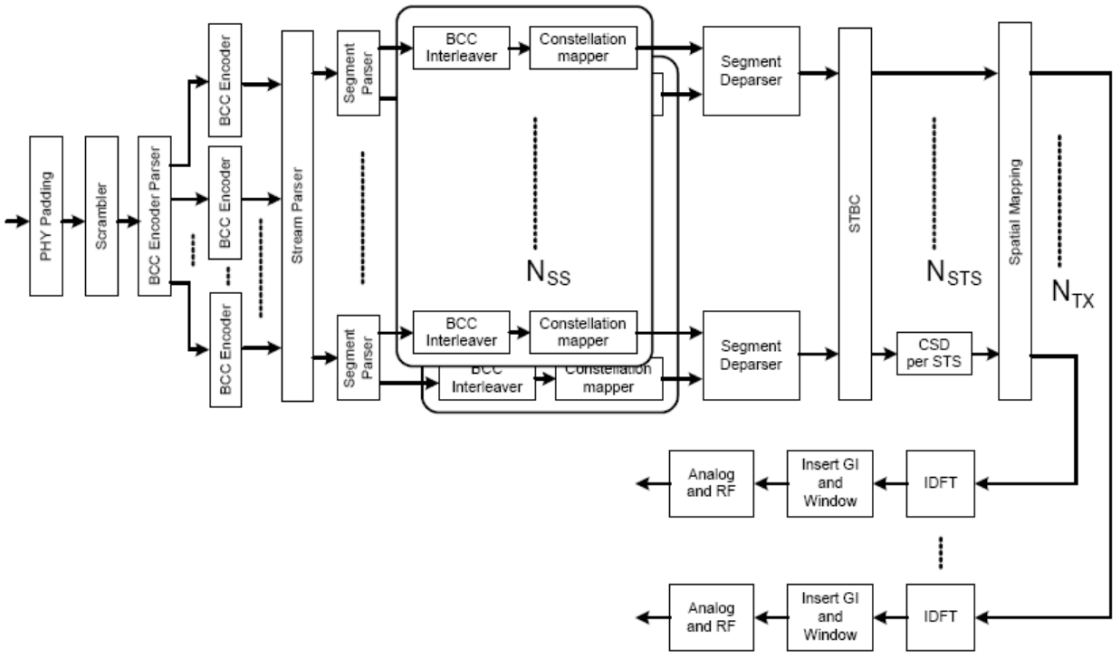
El transmisor 802.11ac, una mejora con respecto al 802.11n, tiene los mismos procedimientos de intervalo de protección, mapeo, encuadre y envoltura; Entonces el análisis de bloques es similar al anterior, pero con la diferencia que el número de cifrados BCC aumentó a 6 en lugar de 4 como en 802.11n, con este número de cifrados se obtiene una modificación diferente (Ortiz, 2015).

El número de bits utilizados para especificar el tipo de modulación ahora suma el número 8, por lo que las modulaciones incluidas en la transmisión son BPSK, QPSK, 16-QAM, 64-QAM y 256-QAM. Aparte de eso, el generador de polinomios, el codificador de errores, el cambio de bloque, el diseño, la verificación final, el mapa y el proceso de redirección son exactamente los mismos que en 802.11n. Para verificar esta

afirmación, se muestran la Figura 5 y la Figura 6, donde se resaltan los bloques que son parte esencial de un transmisor 802.11ac (Ortiz, 2015).

Figura 5

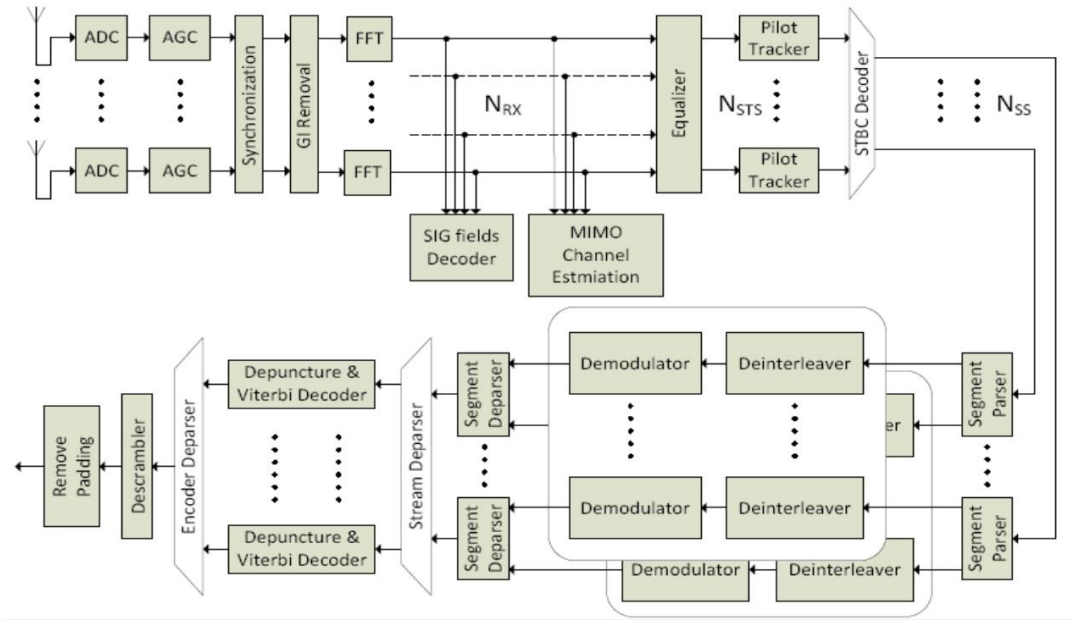
Transmisor 802.11ac por bloques.



Fuente: Recuperado de (Ortiz, 2015)

Figura 6

Receptor 802.11ac por bloques



Fuente: Recuperado de (Ortiz, 2015)

2.4.6 Redes Ideales IEEE 802.11ac

En la norma 802.11ac se usa la tecnología mejorada de MIMO que es MU-MIMO. La línea de vista es un factor importante, pero con la tecnología MU-MIMO, por medio de los rebotes se puede recuperar la señal en el receptor, más como se trata de efectivizar los parámetros en la recepción se debe tener línea de vista, adicionalmente a los parámetros como potencia, distancia y cobertura (Ortiz, 2015).

Para el caso de las redes 802.11ac los parámetros que se debe alcanzar en la simulación son:

- Cantidad de datos que se reciben en un segundo que es 1,3 Gbps.
- Ancho de banda del canal que es 40 MHz y 80 MHz.
- Modulación OFDM.

- Antenas MU-MIMO

2.4.7 Redes Reales IEEE 802.11ac

Como 802.11ac es el sucesor de 802.11n se deben tomar en cuenta los mismos parámetros en la parte real, de tal forma que para fines de estudio no exista discrepancias sobre los cálculos de tramas o bits, por tener diferentes valores de alcance, potencia y antenas. Los parámetros que se usarán son: La distancia máxima que se usará para fines de estudio es 1 km o menos (Ortiz, 2015).

La potencia que se estima usar para el caso real es 450mW o 600mW para el transmisor y 250mW en el receptor, ya que con estas potencias se garantiza una comunicación entre AP y estación. en el caso de 802.11ac se estima que las velocidades alcancen valores de 450 Mbps, en un ancho de banda de 40Mhz y máximo hasta 900 Mbps en un ancho de banda de 80 Mhz, este último solo para fines de simulación ya que en la realidad el ancho de banda de 80 MHz, todavía no se lo usa (Ortiz, 2015).

La compatibilidad del estándar 802.11ac no es un motivo de preocupación, ya que está diseñado de una manera profunda para entenderse de manera eficiente con dispositivos 802.11 a y 802.11 n existentes, al mismo tiempo al trasmitir más datos en un menor tiempo, el estándar 802.11ac ayudará a aumentar el rendimiento de la batería de los dispositivos móviles.

Mejoras con respecto a 802.11n

- El estándar IEEE 802.11ac Opera en la banda de 5Ghz, haciendo que las redes inalámbricas sean más robustas y no estén sujetas a la interferencia y ruido que presenta la banda 2,4GHz.

- El estándar IEEE 802.11ac tiene una velocidad teórica de 1,3Gbps mientras el estándar IEEE 802.11n ofrece velocidad de 600Mbps.

- Es compatible con versiones anteriores IEEE 802.11a, IEEE 802.11n, sin embargo, cuando se conecten su velocidad reducirá a las velocidades respectivamente, la compatibilidad con los estándares IEEE 802.11b e IEEE 802.11g el equipo 802.11ac debe ser dual esto quiere decir que trabaje en las bandas de frecuencia de 2,4GHz y 5GHz.

- El estándar IEEE 802.11ac puede tener 8 antenas de transmisión y recepción utilizando la tecnología MU-MIMO el cual activa las trasmisiones simultáneas para varios usuarios mientras que IEEE 802.11n incluye la capacidad MIMO esto solo beneficia a un solo dispositivo, tiene 4 antenas para trasmisión y recepción.

- El estándar IEEE 802.11ac incorpora la tecnología Beamforming, en donde la señal no sufre perdidas por los obstáculos como las paredes, mejorando la cobertura.

En la Tabla 2 se resume y se muestra una comparación de las características del estándar 802.11n vs 802.11ac.

Tabla 2

Comparación de las características del estándar 802.11n vs 802.11ac

Características	IEEE 802.11n	IEEE 802.11ac
Frecuencia de Operación	2.4GHz y 5GHz	5GHz
Canales	20, 40MHz	20, 40, 80 y hasta 160 MHz
Streams	1 a 4	1 a 8
MU-MIMO	No	Si
Máxima tasa de transferencia por radio (1x1)	150 Mbps	450 Mbps
Máxima tasa de transferencia por radio (3x3)	450 Mbps	1.3 Gbps

Fuente: Elaborado por el Autor

2.5 Radio enlaces

Hoy en día los sistemas inalámbricos se encuentran en la mayoría de los lugares en donde existe mayor afluencia de personas, en donde se deben transmitir dos portadoras modulares, una para la transmisión y otra para la recepción asignando un radio canal a las frecuencias, también conocido como radioenlace a cualquier interconexión entre dos terminales de telecomunicaciones realizado por ondas electromagnéticas, permitiendo la transferencia de información. Los sistema de comunicación fijos son puntos ubicados en la superficie terrestre, proporcionando una capacidad de información con beneficios en calidad y disponibilidad, estos enlaces pueden ser entre los 800 MHz y 43 GHz (Ruesca, 2016).

2.5.1 Funcionamiento de un Radio Enlace

Como su nombre lo indica, la base de un radioenlace es la comunicación mediante ondas de radio, que permite transmitir datos entre dos lugares con una determinada

distancia ya sea por pocos metros o decenas de kilómetros. Los radioenlaces de microondas se realizan cuando existe line a de vista entre el transmisor y el receptor, la línea de visión implica que la antena de uno de los extremos pueda verse con la antena del otro extremo. Para el diseño de un radio enlace de microonda se deben tomar en cuenta los siguientes pasos básicos (Martínez, 2018).

- Elevación del sitio en donde se van a instalar el respectivo transmisor y receptor.
- Relevamiento del perfil del área o terreno, estudio de la trayectoria y los efectos que podría estar expuestos,
- Pruebas posteriores a la instalación del radio enlace y su puesta al servicio con tráfico real.

Además de estos pasos, el sistema más básico de radioenlace está formado por 4 elementos principales como es transmisor, receptor, dos líneas de transmisión y dos antenas.

El Transmisor es el que produce una señal modulada de microondas de una determinada potencia y frecuencia, de una manera que ingrese a la línea de transmisión, emitiendo una señal al espacio libre

El receptor o antena receptora la cual debe apuntar el transmisor recoge la señal que se encuentra en el aire libre que emite su respectivo transmisor, la modula y la procesa y poder interpretar la información enviada.

2.5.2 Parámetros de Radio enlace

En cuanto a los parámetros de un sistema de radio enlace o radiocomunicación, varía según las especificaciones que utilizan los elementos en el proceso de comunicación,

esto quiere decir que existen diferentes tipos de comunicaciones según los terminales utilizados y la señal emitida (Peña, Joan Domingo Gámiz Caro, Juan Grau i Saldes, 2003).

Según la ubicación la comunicación puede ser terrestre o Satélite.

- **Terrestre:** todos los terminales se sitúan en la tierra, por lo tanto, se crean radioenlaces terrenales.

- **Satélite:** mínimo uno de los repetidores se encuentra en satélite. Con ello, se generan radioenlaces espaciales o por satélite.

Según el terminal o usuario final puede ser servicio móvil o servicio fijo

- **Radioenlace de servicio móvil:** comunicaciones realizadas mediante terminales móviles.

- **Radioenlace de servicio fijo:** enlace creado entre puntos fijos situados sobre la superficie terrestre. Este sistema de comunicación realizada entre los 800 MHz y 42 GHz facilita una capacidad de información con características de calidad y disponibilidad determinadas.

Dependiendo de la señal emitida puede ser analógica o digital.

- **Analógica:** fueron las primeras señales que se emitían y se consiguen con la modulación en frecuencia.

- **Digital:** son más actuales que las analógicas y se crean mediante la modulación por conmutación de fase o por amplitud en cuadratura. Este tipo se señales

permiten la regeneración de los datos y constan de una mayor tolerancia frente a ruidos e interferencias.

2.5.3 Propagación de la señal

Respecto a la propagación de la señal, para una correcta transmisión de información, datos y voz, debe cumplir una de las condiciones más importantes en las comunicaciones inalámbricas, la línea de visión entre las antenas receptoras y transmisoras. Para ello, es necesario la definición correcta del rango de frecuencias a utilizar en el radioenlace. Esto es debido a que, las ondas emitidas pueden ser difractadas, refractadas, reflejadas o absorbidas por la atmosfera y los diferentes obstáculos que se encuentran en el recorrido que llevan los rayos desde el emisor hasta el receptor. Por lo tanto, se debe cumplir unas especificaciones mínimas establecidas para la propagación.

Las ondas de radio no viajan en una línea recta entre un punto y el otro, sino en una espiral llamada Fresnel. Por este motivo, se crean dos grupos según las frecuencias de las ondas a emitir. Por un lado, se encuentran en las frecuencias muy altas por sus siglas en inglés (VHF, Very High Frequency) que tienen un rango de frecuencia que va desde los 30 MHz hasta los 300 MHz y Frecuencias ultra altas por sus siglas en inglés (UHF, Ultra High Frequency) que tienen un rango de frecuencia que va desde 3 MHz hasta los 3 GHz, cuales presentan mayor tolerancia a los obstáculos y hacen posible los enlaces (casi con línea de visión) por sus siglas en inglés (nLOS, Near Line of Sight), lo cual define un trayecto parcialmente obstruido entre el emisor y el receptor de la señal (Peña, Joan Domingo Gámiz Caro, Juan Grau i Saldes, 20c3).

Zona de Fresnel

Se llama Zona de Fresnel al volumen de espacio entre el emisor de una onda magnética y un receptor, de manera que las ondas se desfacen superando el volumen de los 180 grados.

Una zona de Fresnel es una de una serie de zonas elipsoidales, de diámetro polar extenso, concéntricas, de espacio entre y alrededor de una antena que transmite y un sistema de antena que recibe. Se compone de múltiples zonas: a primera zona es el espacio elipsoidal a través del cual pasa la señal de línea de vista directa, la segunda zona rodea la primera zona, pero excluye la primera. En esta zona, la onda capturada por el receptor se desfasará más de 90°, pero menos de 270°, la tercera región rodea la segunda y las ondas desviadas capturadas por el receptor tendrán el mismo efecto que una onda en la primera zona. La onda sinusoidal tendrá un desfase mayor a 270°, pero menor a 450°, lo idealmente sería un desfase de 360° (Wix, 2015).

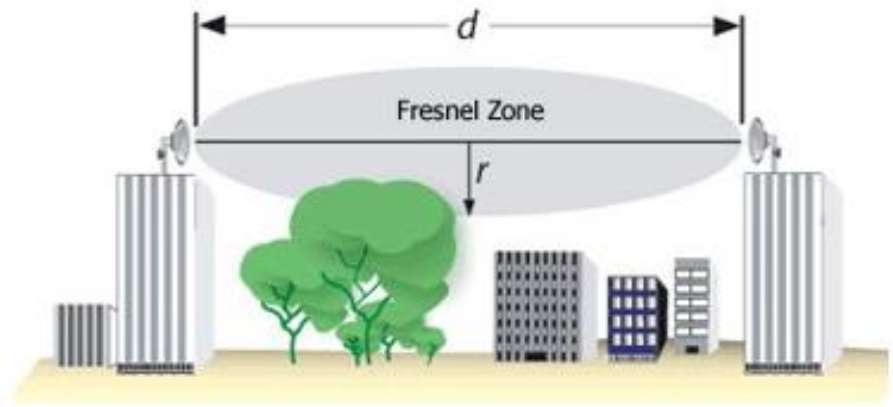
Para su cálculo se utiliza la siguiente formula

$$\boldsymbol{r1(m) = 17.32 + \sqrt{\frac{d\,(km)}{4f(GHz)}}}$$

En la Figura 7 se puede observar obstrucción que puede ocasionar un objeto en la zona de Fresnel.

Figura 7

Obstrucción en la zona Fresnel



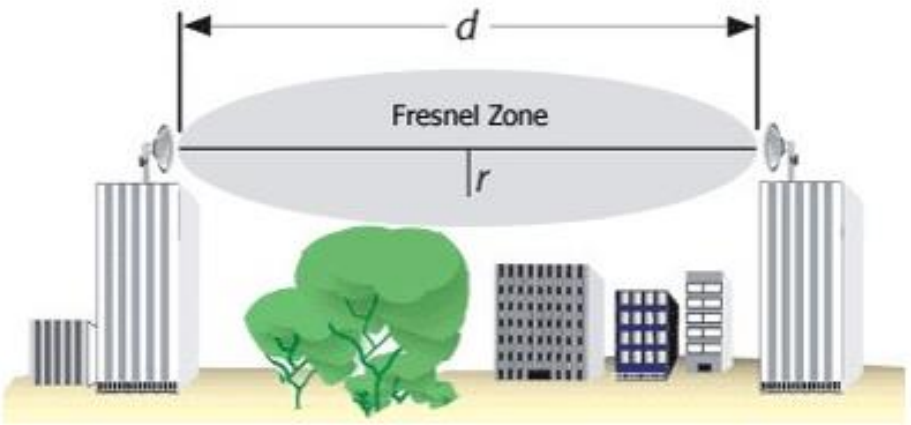
Fuente: Recuperado de (Peña, Joan Domingo Gámiz Caro, Juan Grau i Saldes, 2003)

En cambio, para los radioenlaces superiores a 900 MHz, es necesario realizar una propagación en línea de visión o visión directa por sus siglas en inglés (LOS, Line of Sight) es decir, sin obstáculos en la zona Fresnel.

En la Figura 8 se puede observar si la frecuencia del radio enlace aumenta ya no existe obstrucción en dicha zona.

Figura 8

Línea de vista no obstruida en la zona de Fresnel



Fuente: Recuperado de (Peña, Joan Domingo Gámiz Caro, Juan Grau i Saldes, 2003).

Entonces, los pasos a seguir para definir un radioenlace de una manera satisfactoria son:

1. Selección del lugar de instalación de los elementos. Se debe determinar, sobre todo, la ubicación de las antenas de transmisión y de recepción. Así como en caso necesario, las estaciones intermediarias.

2. Verificación del perfil del terreno en el que se va a configurar el sistema de comunicación. Es decir, se debe tener en cuenta el territorio donde se quiere realizar el radioenlace, ya que debe cumplir la línea de visión entre las dos antenas, así como la distancia de separación entre ambas.

3. Cálculos de la colocación del mástil de la antena, así como de la altura a la que instalar el elemento, con el fin de una correcta visualización.

4. Cálculos completos del radioenlace, teniendo en cuenta la trayectoria que van a llevar las ondas y los efectos a los que se exponen las mismas, ya sean consecuencias naturales o producidos por el ser humano (atenuación, interferencias…)

5. Pruebas posteriores a la instalación del sistema radioenlace, cuales verificarán la correcta implantación del sistema y puesta en marcha de este.

2.5.4 Tipo de Antenas

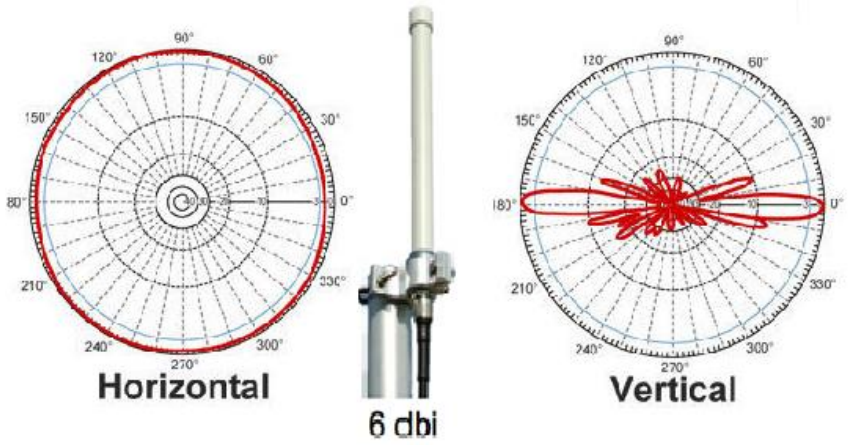
Las antenas forman parte fundamental de los dispositivos inalámbricos, debido a que se encargan de enviar y recibir las ondas electromagnéticas con los datos. Según la forma de señal que cubren, pueden clasificarse en tres tipos:

2.5.5 Antenas Omnidireccionales

Las Antenas Omnidireccionales radian al espacio señal de forma uniforme en todas direcciones. Es la única antena totalmente omnidireccional sobre un plano de 3 dimensiones. A medida que aumenta la ganancia de este tipo de antenas pueden lograr conexiones a mayores distancias, si bien la potencia se concentra cada vez más en el eje horizontal. La ganancia de la antena se puede definir como la eficiencia de la antena que se multiplica por la directividad y se expresa en decibelios, en la Figura 9 se muestra la antena omnidireccional con su patrón de radiación en plano horizontal y vertical (Ruesca, 2016).

Figura 9

Antena Omnidireccionales



Fuente: Recuperado de (Pietrosemoli, 2007)

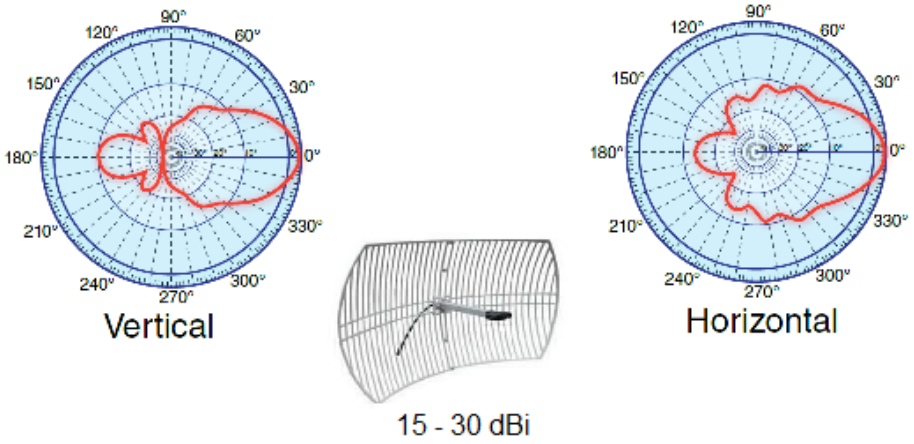
2.5.6 Antenas Direccionales o bidireccionales

Las antenas direccionales o bidireccionales concentran la señal en una sola dirección (o en dos direcciones, en las bidireccionales según sea el caso) cubren cierto ángulo alrededor de la dirección a la que se apunta. La ganancia de la antena depende del ángulo de la radiación, cuanto mayor sea la ganancia de la antena, menor será el ángulo de

radiación, por lo que resultará más difícil apuntar al otro extremo y mantener una conexión estable. Tienen forma de tubo. En su interior tienen unas barras de metal que cruzan el interior de ese tubo. en la figura 10 se muestra la antena omnidireccional con su patrón de radiación en plano horizontal y vertical (Ruesca, 2016).

Figura 10

Antena Direccional



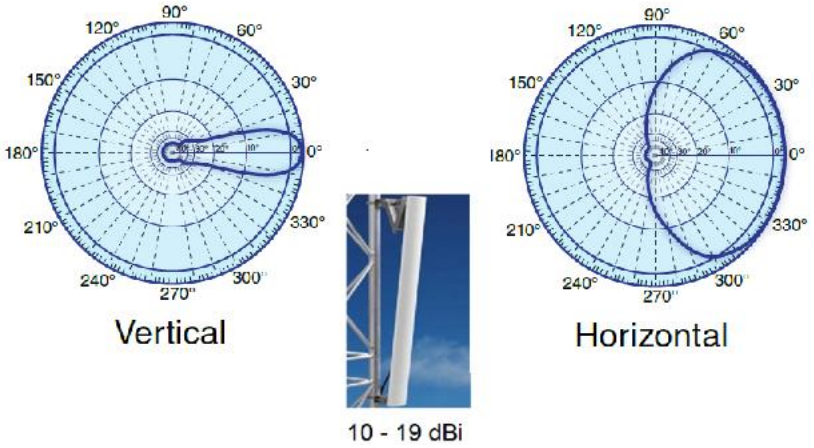
Fuente: Recuperado (Ruesca, 2016).

2.5.7 Antenas Sectoriales

Es un tipo mixto es decir la mezcla de antenas direccionales y antenas omnidireccionales, que intenta juntar lo mejor de los dos anteriores. Por una parte, emite una señal más amplia que una direccional, pero menor que la omnidireccional. Estas emiten un haz de luz más amplio que las direccionales pero no tan amplio como las omnidireccionales y su intensidad o alcance es mayor que una omnidireccional pero menor que una direccional En cuanto a la intensidad (alcance) es mayor que la omnidireccional, pero algo menor que la direccional en la Figura 11 se muestra la antena omnidireccional con su patrón de radiación en plano horizontal y vertical (Mensoza, 2017).

Figura 11

Antena Sectorial



Fuente: Recuperado de (Pietrosemoli, 2007).

2.6 Seguridad de Redes Inalámbricas

La seguridad de las redes inalámbricas es sumamente importante, debido a que una persona no autorizada pueda acceder a la red con el uso de un dispositivo móvil, computadora portátil, celular, o Tablet y lograr acceder a los archivos y utilizar este acceso para obtener información importante que se transmite por la red, la ausencia de seguridad inalámbrica es la principal razón que se puede ocasionar el robo de información (Alegsa, 2016).

Algunas recomendaciones que se deben aplicar en una red inalámbrica son: Cambiar frecuentemente la contraseña de acceso, cambiar el SSID por defecto de los puntos de acceso, desactivar la emisión de broadcast del SSID, inhabilitar DHCP, usar IP’s fijas y utilizar un mecanismo de encriptación.

2.6.1 Mecanismos de Seguridad

Los mecanismos de seguridad son protocolos de cifrado de datos para el estándar 802.11 estos mecanismos pueden ser WEP, WPA, WPA2 y WPA2 Empresarial estos se encargan de codificar la información que se transmite en la red y así proteger la confidencialidad e integridad de los datos de los usuarios.

WEP

Privacidad Equivalente al Cableado por sus siglas en Ingles (WEP: Wiring Equivalent Privacy) es un método original de seguridad del protocolo 802.11, el cual permite la autenticación de usuarios y la encriptación de datos. En la actualidad este método de seguridad está obsoleto debido a que presenta numerosas debilidades que le hace un método de seguridad no confiable (IEEE, 2012).

La autenticación WEP es un punto de acceso que debe autenticarse a una estación antes de asociarse a un AP, cabe recalcar que la autenticación con el método WEB son las estaciones y no los usuarios. Definiendo así dos tipos de autenticación

- (Open System Authentication) Sistema de autenticación abierta, es un protocolo original de 802.11 por esta razón el sistema autentica a cualquier usuario sin la necesidad de poseer la clave WEB correcta.

- (Shared Key Authentication) Sistema de Autenticación de Clave Compartida utiliza un mecanismo de desafío/respuesta, esto quiere decir una clave de 64bits o 128 bits, compartida por el punto de acceso y la estación, negando el acceso a todo aquel que no posea una clave.

WPA

Acceso protegido Wi-Fi por sus siglas en Ingles (WPA: Wi-Fi Protected Access) es un estándar basado en especificaciones de 802.11i en cual busca resolver deficiencias de la seguridad WEB, mejorando el cifrado de datos y brindando mecanismos de autenticación. El estándar fue propuesto por los miembros de Wi-Fi Alliance asociación que reúne a los grandes fabricantes para Redes Inalámbricas de Área Local, junto a IEEE para la seguridad de las WLANs (IEEE, 2012).

El cifrado WPA- Personal, utiliza un sistema de claves PSK o claves pre compartidas, situación en la que el usuario especifica la clave y el resto de los usuarios manejan la misma contraseña, simplificando el trabajo de recordarla. Ideal para empresas que manejen un servidor Radius, el cual permita autenticar a los usuarios con su respectiva contraseña, sin la necesidad de una contraseña global.(WatchGuard Technologies, 2019)

WPA2

Acceso protegido a Wi-Fi versión 2 por sus siglas en Ingles (WPA2: Wi-Fi Protected Access iversion 2) es la versión mejorada de WPA, proporciona seguridad adecuada para hogares y pequeñas redes inalámbricas, tiene un método de cifrado mucho más recomendado, tiene una mejor seguridad y un mejor rendimiento en la red. Al igual que WPA dispone de claves personales PSK y autenticación Radius. Con respecto a los pitaras informáticos u otras amenazas en línea WPA2 tiene una protección más adecuada frente a estos problemas (Capelle, 2019).

WPA2 Empresarial (Enterprise)

Una de las principales diferencias entre WPA2 y WPA2 Enterprise es el grado de sofisticación necesaria para configurar WPA2 Enterprise, este método de seguridad necesita un servidor de autenticación RADIUS más robusto en la administración de la

red. Si bien WPA2 Enterprise facilita un mayor grado de seguridad que WPA2, el tipo de fallos de seguridad contra los que protege el primero rara vez suceden en las redes de hogar y negocios pequeños (Capelle, 2019).

WPA2 o WPA Enterprise es una extensión de acceso protegido Wi-Fi, que requiere un servidor de autenticación como se mencionó anteriormente RADIUS, diseñado para redes corporativas que requieren seguridad adicional que las redes de clave pre compartidas normales no pueden proporcionar. La configuración de seguridad requiere un tipo de Protocolo de autenticación extensible (EAP) para la autenticación. EAP es un marco de autenticación, no un mecanismo de autenticación específico. Proporciona algunas funciones comunes y negociación de métodos de autenticación llamados métodos EAP (SILICON LABS, 2016).

802.1X

802.1X es un marco estándar IEEE para cifrar y autenticar a un usuario que intenta asociarse a una red cableada o inalámbrica. WPA-Enterprise usa el protocolo de integridad de clave temporal por sus siglas en Ingles (TKIP: Temporal Key Integrity Protocol) con cifrado de flujo RC4, mientras que WPA2-Enterprise agrega cifrado AES (Estándar de cifrado avanzado).

802.1X utiliza el Protocolo de autenticación extensible (EAP) para establecer un túnel seguro entre los participantes involucrados en un intercambio de autenticación. El Meraki admite múltiples tipos de EAP, dependiendo de si la red está utilizando un servidor de autenticación alojado por Meraki o un servidor de autenticación alojado por el cliente. Existe 7 beneficios de implementar la seguridad de Wi-Fi en modo Enterprise. El primero elimina los riesgos de seguridad de las contraseñas compartidas, el segundo pone un freno a personas que quieren entrar a la red, el tercero permite métodos de

seguridad mejorados, el cuarto los métodos de autenticación se pueden extender a la red cableada, la quinta las VLAN se pueden asignar dinámicamente, la sexta permite controles adicionales y la séptima admite protección de acceso a la red NAP (Punto de Acceso a la Red).

WPA Enterprise: 802.1x con servidor de autenticación, normalmente RADIUS. EAP*. Tiene una clave por usuario. EAP (Protocolo de autenticación cambia entre cliente y servidor de autenticación) existe 5 modos de EAP para WPA y WPA2:

- EAP-TLS (Transport Layer Security)
- EAP-TTLS
- PEAP (Protected EAP) 2 modos...EAP-MS-CHAPV2 y EAP-TLS
- LEAP
- EAP-SIM

Para configurar las diferentes seguridades que ofrece WPA2 empresarial se debe tomar en cuenta si la seguridad que se va a usar sea compatible con la red que se va a conectar.

2.6.2 RADIUS

RADIUS es un servicio de usuario de marcación de autenticación remota, es un protocolo de red: un sistema que define reglas y convenciones para la comunicación entre dispositivos de red, para usuarios remotos autenticación y contabilidad. Comúnmente utilizado por los proveedores de servicios de Internet (ISP), red celular proveedores y redes corporativas y educativas, el protocolo RADIUS cumple tres funciones principales. La primera autentica usuarios o dispositivos antes de permitirles el acceso a una red, la segunda autentica a esos usuarios o dispositivos para servicios de

red específicos y la tercera contabiliza y rastrea el uso de esos servicios (Copyright Network, 2014).

En el momento en que se creó RADIUS, los sistemas de acceso a la red se distribuían en un área amplia y eran administrados por múltiples organizaciones independientes. Los administradores centrales querían evitar problemas de seguridad y escalabilidad, y por lo tanto no querían distribuir nombres de usuario y contraseñas; en cambio, querían que los servidores de acceso remoto contactaran a un servidor central para autorizar el acceso al sistema o servicio solicitado. En respuesta al contacto del servidor de acceso remoto, el servidor central devolvería un mensaje de "éxito" o "falla", y las máquinas remotas se encargarían de hacer cumplir esta respuesta para cada usuario final (Urueña & Larrabeiti, 2005).

El objetivo de RADIUS es crear una ubicación central para la autenticación de usuarios, en la que los usuarios de muchos lugares pueden solicitar acceso a la red. La simplicidad, la eficiencia y la facilidad de uso del sistema RADIUS llevaron a su adopción generalizada por parte de los proveedores de equipos de red, en la medida en que actualmente RADIUS se considera un estándar de la industria y también está en condiciones de convertirse en un estándar del Grupo de trabajo de ingeniería de Internet (IETF) (Copyright Network, 2014).

El servicio RADIUS es un protocolo que ofrece múltiples ventajas tecnológicas para los clientes entre algunas de ellas se mencionan a continuación.

- Una solución abierta y escalable.

- Amplio soporte por parte de una gran base de proveedores.

- Modificación fácil
- Separación de los procesos de seguridad y comunicación.
- Adaptable a la mayoría de los sistemas de seguridad.
- Funciona con cualquier dispositivo de comunicación que admita el protocolo de cliente RADIUS.

2.6.3 Portal Cautivo

Un portal cautivo es una página web que el usuario puede acceder a través de un navegador web a una red de acceso público, este proceso de autenticación se debe realizarse antes de otorgar el acceso. Los portales cautivos suelen ser utilizados por lugares públicos, incluidos restaurantes, hoteles, centros de negocios, aeropuertos, trenes, centros comerciales, vestíbulos de hoteles, cafeterías, bibliotecas, parques y otros lugares que ofrecen puntos de conexión Wi-Fi gratuitos para usuarios de Internet. Si bien estos puntos de acceso ofrecen una opción interesante para mantenerse conectado, también pueden rastrear las actividades del usuario y compartir información del usuario o dispositivo con terceros, mediante el uso de rastreadores en su portal cautivo y sitios web de aterrizaje (Ali, Osman, Mannan, & Youssef, 2019).

En algunos portales cautivos, se muestran anuncios de los patrocinadores del proveedor y el usuario debe hacer clic en ellos o cerrar las ventanas en las que aparecen antes de acceder a Internet. Algunos portales cautivos requieren la entrada de una ID de usuario y contraseña previamente asignados antes de acceder a Internet. Tal autenticación puede desalentar el uso de puntos de acceso inalámbricos como sitios para realizar actividades delictivas. La mayoría de los servidores con portales cautivos

incluyen programas antivirus y cortafuegos para ayudar a proteger las computadoras de los usuarios de Internet y entre sí (Rouse, 2005).

Incluso cuando se usa un portal cautivo simple en una red de acceso público gratuito, algunas personas pueden conectarse repetidamente, usando la red de forma casi continua para descargar música, videos u otros archivos grandes. Esta actividad, llamada acaparamiento de ancho de banda, puede minimizarse mediante programación adicional en el portal cautivo. Dicha programación puede controlar la velocidad a la que se descargan archivos grandes, limitar el tamaño (en kilobytes o megabytes) de archivos que se pueden descargar, restringir el número de descargas que pueden ocurrir en una sola sesión o bloquear la conexión a sitios web comúnmente utilizados para descargar archivos grandes. Esto se llama limitación de ancho de banda o modelado de tráfico (Rouse, 2005).

2.6.3.1 Protocolos de control de acceso RADIUS.

El servidor RADIUS comprueba si la información es correcta a través de esquemas de autenticación como PAP, CHAP y EAP. Si la negociación es correcta el servidor aceptará la conexión y dará acceso al sistema del ISP, Asignando los recursos de la red como una dirección IP y parámetros de L2TP.

2.6.3.2 Protocolo de Autentificación por Contraseña (PAP)

PAP es un protocolo de autenticación en donde los usuarios deben ingresar un nombre de usuario y una contraseña antes de tener acceso al sistema, los mismos que son enviados a través de la red a un servidor, donde se comparan con una base de datos de las cuentas, es decir nombres y contraseñas de los usuarios.

PAP es un protocolo de autenticación en donde los usuarios deben ingresar un nombre de usuario y una contraseña antes de tener acceso al sistema, los mismos que

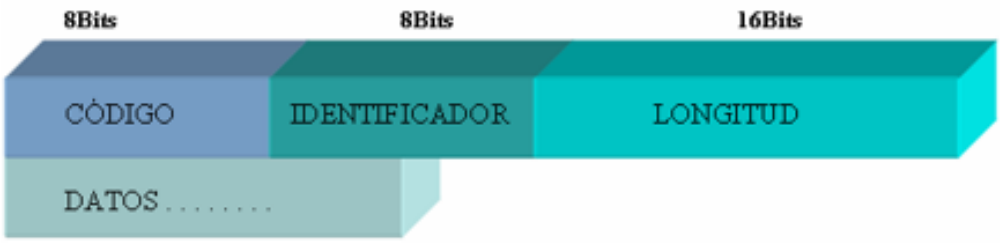
son enviados a través de la red a un servidor, donde se comparan con una base de datos de las cuentas, es decir nombres y contraseñas de los usuarios.

El protocolo PAP es un sencillo método para verificar la identidad de un usuario dentro de un grupo con una conexión punto a punto, en donde utiliza una negociación en dos sentidos en el enlace inicial. Por cada uno de los usuarios se envía un ID o contraseña, esperando una respuesta del otro usuario, si no se realiza este proceso la comunicación se dará por finalizada.

Este método de autenticación no tiene un sistema de seguridad adecuado, debido a que la contraseña es enviada en forma plana sin encriptación creando una vulnerabilidad al poderlas robarlas y reproducirlas fácilmente. A continuación, en la Figura 12, se presenta el formato de la Trama PAP.

Figura 12

Formato de la trama PAP



Fuente: Recuperado (Pablo & Cepeda, 2007,pág 19)

En el campo Código de 8 bits indica el paquete PAP en donde puede ser: Solicitud de autenticación, solicitud de ACK o solicitud Nak.

En el campo Identificador de 8 bits empareja los requerimientos con las respuestas.

En el campo longitud de 16 bits, indica la longitud total del paquete PAP, sea códigos, identificador, longitud y campo de datos.

En campo de datos puede tener varios tamaños que puede ir de cero a múltiples octetos, esta estructura dependerá de parámetros del campo del código.

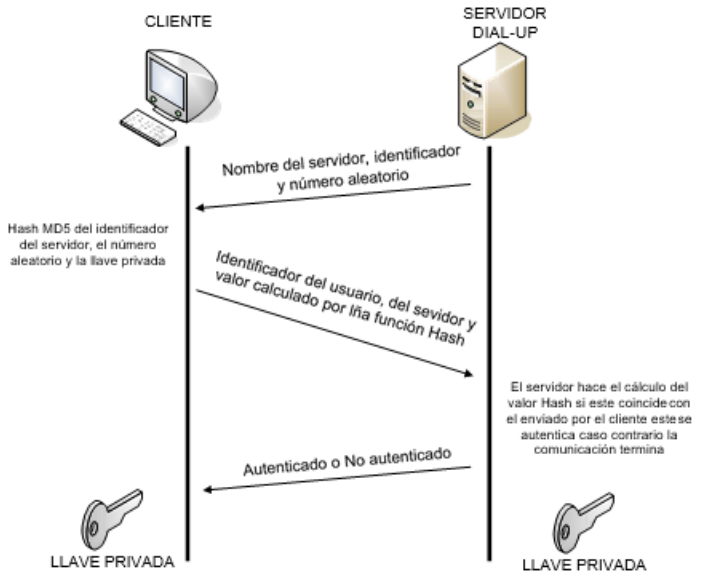
2.6.3.3 Protocolo de Autentificación por Reto (CHAP)

El protocolo CHAP esta aplicado para verificar la identidad de los usuarios de una comunicación punto a punto, utilizando una comunicación de tres líneas, usualmente se usa en una en el protocolo PPP en conexiones de un ISP a través de un modem.

Para el funcionamiento de este protocolo cuando se establece el enlace, el autenticador envía un reto a un usuario par, este usuario responde con un valor calculando una función hash de una vía. El autenticador revisa la respuesta, compara el valor utilizando a misma función hash, si el valor es correcto el autenticador responde con un ack, si no es correcto la comunicación termina. La función es utilizar un cambio constante en un tiempo aleatorio. En la Figura 13 se puede observar el proceso de autenticación CHAP de acceso remoto.

Figura 12

Autenticación CHAP para acceso remoto



Fuente: Recuperado de (Pablo & Cepeda, 2007,pág 21)

En este método de autenticación los extremos son los únicos que conocen la combinación secreta y no se intercambia en la autenticación. Generando un problema en la base de datos de encriptación, debido a que las combinaciones secretas no se guardan en dicha base.

A continuación, en la Figura 14 se muestra el formato de la Trama CHAP.

Figura 13

Formato de la trama CHAP.

Fuente: Recuperado de (Pablo & Cepeda, 2007, pág 21)

En el campo Código de 8 bits indica el paquete CHAP en donde el campo puede ser: Desafío, Respuesta, Éxito o Fracaso.

En el campo Identificador de 8 bits empareja los requerimientos con las respuestas.

En el campo longitud de 16 bits, indica la longitud total del paquete CHAP, sea códigos, identificador, longitud y campo de datos.

En campo de datos puede tener varios tamaños que puede ir de cero a múltiples octetos, esta estructura dependerá de parámetros del campo del código.

2.6.3.4 Protocolo de autenticación extensible (EAP).

Este protocolo permite que los módulos de autenticación de terceros puedan interaccionar con la implementación del protocolo punto a punto. Este protocolo amplio PPP proporcionando un mecanismo de soporte estándar, utilizando tarjetas testigo (inteligente), Kerberos, clave pública y S/Key para el esquema de autenticación. Los datos de autenticación no se incluyen en la información, pero va junto a ella. Esto ayuda a que los sistemas remotos de autenticación puedan negociar antes de recibir y pasar información(Urueña & Larrabeiti, 2005).

EAP surge como respuesta a la demanda continua de autenticar dispositivos, el cliente de acceso remoto y el autenticador negocian el esquema de autenticación exacto que se va a utilizar, ayuda a proteger las redes virtuales privadas (VPN) con los piratas informáticos que realizan ataques constantemente. EAP ofrece múltiples ventajas con respecto a los protocolos de autenticación PAP y CHAP (IBM Knowledge Center, 2005).

2.6.4 FreeRADIUS

FreeRADIUS es el servidor RADIUS de código abierto más popular y más ampliamente implementado en el mundo. Sirve como base para múltiples ofertas comerciales, y proporciona la autenticación, autorización, y las necesidades de contabilidad (AAA) de muchas compañías de Fortune 500 y proveedores de servicio de internet (ISP) de Nivel 1. También es ampliamente utilizado por la comunidad académica (es decir, eduroam, el servicio de acceso de roaming mundial desarrollado para la comunidad internacional de investigación y educación, utiliza el software FreeRADIUS).

La popularidad de FreeRADIUS se puede atribuir a la multitud de beneficios adicionales que ofrece, mucho más allá de los que se encuentran en la amplia variedad de otros servidores RADIUS. FreeRADIUS se basa en un protocolo de diseño escalable, modular y muchas en funciones, que proporciona los siguientes beneficios y ventajas a los administradores de red(Copyright Network, 2014).

2.7 Gestión de la Red

La gestión de red se define como el proceso de gestión de una red por fallas y rendimiento utilizando diversas herramientas y tecnologías para mantenerse al día con los requisitos comerciales. El objetivo de la gestión de red es lograr una red libre de

errores. En el entorno actual, se emplean múltiples herramientas de administración de red que hacen que todo el proceso sea complejo (OpManager & ManageEngine, 2019).

La evolución tecnológica está permitiendo la distribución, implementación de sistemas basada en la arquitectura cliente / servidor asociado con la eficiencia y bajos costos. Las Computadoras y las estaciones de trabajo interconectadas están sustituyendo el ordenador central. Las redes y los sistemas de procesamiento distribuido son cada vez más importantes y, de hecho, tienden a convertirse en un aspecto crítico en el mundo de los negocios. Dentro de una organización dada, la tendencia es hacia las redes más grandes y complejas que admiten más aplicaciones y más usuarios (Benítez, 2016).

Ha surgido la necesidad de una operación eficiente, libre de fallas, con la importancia de redes para las organizaciones. Las redes de computadoras están compuestas de diferentes Plataformas de hardware y software: recursos, servicios y varios protocolos. Una gran red no se puede armar y administrar por el solo esfuerzo humano. La complejidad de dicho sistema requiere herramientas automatizadas de administración de red para monitorear y administrar la utilización de recursos (Pérez et al., 2006).

2.8 Modelo de Gestión FCAPS de la ISO

La gestión de redes de telecomunicación se define como cualquier acción para planificar, instalar, mantener, explotar y administrar redes y servicios de telecomunicación, con el objetivo de preservar la calidad del servicio y maximizar su rendimiento. La gestión de red según el modelo ISO y se describen en cinco áreas funcionales: Gestión de Fallos (Fault), Gestión de la Configuración (Configuration), Gestión de la Contabilidad (Accounting), Gestión de las Prestaciones (Performance), y Gestión de la Seguridad (Security) (Benítez, 2016).

A continuación, se pasan a explicar cada una de ellas.

2.8.1 Gestión de fallos

La gestión de fallos es un conjunto de funciones que permiten detectar, aislar y corregir un funcionamiento anormal de la red de telecomunicaciones y de su entorno, con el objetivo de conseguir que siempre esté disponible. En esta definición, el fallo se refiere a toda desviación del conjunto de objetivos operacionales, servicios o funciones del sistema. Para mantener el funcionamiento adecuado de una red compleja, se debe tener cuidado tomando en cuenta que los sistemas en su conjunto, y cada componente esencial individualmente, funcionan correctamente. Cuando ocurre una falla, es importante, lo más rápido posible (University of Southern Indiana, 2008):

- Determinar exactamente dónde está la falla.
- Aísle el resto de la red de la falla para que pueda continuar funcionando sin interferencias.
- Reconfigurar o modificar la red de tal manera que minimice el impacto de operación sin el componente o componentes fallidos.
- Repare o reemplace los componentes fallidos para restaurar la red a su estado inicial.

El concepto fundamental de una falla es central para la definición de gestión de fallas. Las faltas deben distinguirse de los errores. Una falla es una condición anormal que requiere la atención (o acción) de la gerencia para repararla. Una falla generalmente se indica por la falla en el funcionamiento correcto o por errores excesivos. Por ejemplo, si una línea de comunicaciones se corta físicamente, no pueden pasar señales. O un

engarzado en el cable puede causar distorsiones brutales de modo que haya una tasa de error de bits persistentemente alta. Ciertos errores (por ejemplo, un error de un solo bit en una línea de comunicación) pueden ocurrir ocasional y normalmente no se consideran fallas. Por lo general, es posible compensar los errores utilizando los mecanismos de control de errores de los distintos protocolos (University of Southern Indiana, 2008).

2.8.2 Gestión de configuraciones

La gestión de la configuración consiste en la aplicación de operaciones administrativos y técnicos durante el desarrollo del sistema de información y su posterior mantenimiento proporciona las funciones con las que ejercer el control sobre los elementos de la red, identificarlos, recoger datos de estos y suministrar información a estos. Tiene el propósito de identificar, definir, proporcionar información y controlar los cambios que se realizan en la configuración del sistema.

La gestión de la configuración comprende a los grupos de funciones que deben encargarse de las siguientes tareas (Benítez, 2016):

Planificación de la red. Se encargará de determinar si existe la necesidad de aumentar la capacidad de la red y de introducir nuevas tecnologías.

Instalación. El sistema de gestión de red puede soportar la instalación de los equipos de la red de telecomunicación. Esa capacidad de soporte incluye la de ampliación o reducción de un sistema. Otra tarea que podría realizar sería la instalación de programas dentro de elementos de red desde los sistemas de base de datos. Además, se pueden intercambiar datos administrativos entre los elementos de red y el sistema.

Planificación y negociación de servicios. Esta función se refiere a la planificación de la introducción de servicios y los contactos con los clientes para establecer nuevos, cambiar características de servicios y desconectar servicios.

Provisión. La provisión consiste en el conjunto de procedimientos necesarios para poner en servicio un equipo, sin contar la instalación.

El administrador de la red debe poder rastrear el uso de los recursos de la red por usuario o clase de usuario por una serie de razones, que incluyen las siguientes:

- Un usuario o grupo de usuarios puede estar abusando de sus privilegios de acceso y cargando la red a expensas de otros usuarios.

- Los usuarios pueden estar haciendo un uso ineficiente de la red, y el administrador de la red puede ayudar a cambiar los procedimientos para mejorar el rendimiento.

- El administrador de la red está en una mejor posición para planificar el crecimiento de la red si la actividad del usuario se conoce con suficiente detalle.

2.8.3 Gestión de contabilidad

La gestión de la contabilidad permite la medición del uso de los servicios de red, la cantidad que se ha de cobrar al cliente por el mencionado uso y la determinación del coste que representa para el proveedor de servicios. Permite también la determinación de los precios de los servicios. El grupo gestión de la contabilidad comprende las siguientes funciones(Benítez, 2016):

Medición de la utilización. Un sistema de operaciones interno puede recoger datos de los dispositivos, que sirven para determinar los importes que deben cargarse a las cuentas de los clientes.

Tarificación o fijación de precios. Una tarifa es un conjunto de datos de un elemento de red, utilizados para determinar el importe del pago por los servicios utilizados. La clase de tarifa será definida en función del servicio, del origen y destino, del periodo de tarificación y de la categoría del día. Estos atributos pueden cambiar durante la comunicación.

Cobros y finanzas. Se encarga de la transferencia de datos financieros para la gestión de red, a efectos tales como los de administración de cuentas de clientes e información a los clientes sobre saldos, fechas de pago y recepción de pagos.

Control de la empresa. Estas funciones de gestión soportan el flujo de datos necesarios para actuar con diligencia sobre el flujo de fondos apropiado dentro de la empresa y entre la empresa y sus propietarios y acreedores. Este grupo soporta las responsabilidades fiduciarias de los directivos de la empresa.

Con el fin de conseguir dichos propósitos, se pueden realizar en esta gestión las siguientes tareas:

- Recopilación de datos de uso (medir y monitorizar).
- Definición de unidades a contabilizar.
- Mantenimiento de cuentas y logs.
- Asignación de costes a cuentas.

- Asignación y monitorización de cuotas.
- Estadísticas de uso.
- Políticas de cuentas y tarifas.

2.8.4 Gestión de Prestaciones

La principal diferencia entre este tipo de gestión con la de fallos, es que esta última pretende que la red funcione bien en el presente, mientras que el objetivo de la primera es garantizar la calidad de la misma en el futuro. La gestión de prestaciones proporciona funciones destinadas a evaluar e informar sobre el comportamiento de los equipos de telecomunicación y de los elementos de red y la efectividad de la misma. Su cometido consiste en reunir y analizar datos estadísticos, para supervisar y corregir el comportamiento y la efectividad de la red, del elemento o equipo de red y facilitar la planificación, la provisión, el mantenimiento y la medición de la calidad (Benítez, 2016).

El sistema de gestión recoge datos sobre la calidad de servicio (QOS, quality of service) de los elementos de red y contribuye a las mejoras de la misma. Para ello, se pedirán informes de datos de QOS a los distintos elementos, o bien se enviarán informes automáticamente con arreglo a un plan en casos de excepción. En cualquier momento, se puede modificar el plan y/o los umbrales vigentes. Los informes de los elementos de red sobre los datos referidos a la QOS pueden consistir en datos en bruto (datos recogidos durante la prestación de los servicios de telecomunicación) que luego se analizan, o bien en datos analizados por el propio dispositivo.

La calidad del servicio incluye la supervisión y el registro de parámetros relacionados con:

El establecimiento de la conexión. Por ejemplo, demoras en el establecimiento de la comunicación o peticiones de llamada logradas y fallidas, La retención de la conexión, la calidad de la conexión, la integridad de la facturación, el mantenimiento y el examen de ficheros cronológicos del estado de los sistemas.

La cooperación con la gestión de fallos, a fin de establecer posibles averías de un recurso, o con la gestión de la configuración, para cambiar los parámetros/límites de encaminamiento y de control de carga de enlaces, etc. La iniciación de llamadas de prueba para supervisar los parámetros de QOS.

2.8.5 Gestión de Seguridad

La gestión de seguridad se ocupa de generar, distribuir y almacenar claves de cifrado. Las contraseñas y otra información de autorización o control de acceso deben mantenerse y distribuirse. La gestión de la seguridad también se ocupa de supervisar y controlar el acceso a las redes informáticas y el acceso a toda o parte de la información de gestión de la red obtenida de los nodos de la red(Benítez, 2016).

Los registros son una herramienta de seguridad importante y, por lo tanto, la gestión de la seguridad está muy relacionada con la recopilación, el almacenamiento y el examen de registros de auditoría y registros de seguridad, así como con la habilitación y des habilitación de estas instalaciones de registro.

La gestión de seguridad proporciona instalaciones para la protección de los recursos de la red y la información del usuario. Las instalaciones de seguridad de red deben estar disponibles solo para usuarios autorizados. Los usuarios desean saber que las políticas de seguridad adecuadas están vigentes y son efectivas y que la administración de las instalaciones de seguridad es segura (University of Southern Indiana, 2008).

2.9 Arquitectura de la Gestión de Redes

La Gestión de redes consiste en la monitorización, el sondeo, configuración, evaluación, análisis y control de los recursos de una red para conseguir niveles de trabajo y adecuados a los objetivos de una instalación y una organización; mediante tareas de despliegue, integración y coordinación de hardware, software y elementos humanos.

El modelo de gestión de redes es usado para gestionar redes TCP/IP en donde se incluyen los siguientes elementos(Sosa, 2006):

- Estación de Gestión (Manager).
- Agente Administrador (Agente).
- Base de Información de Administrada (MIB).
- Protocolo de Administración de Redes

La estación de gestión (Manager) normalmente es un dispositivo independiente, que sirve como la interfaz entre el sistema de gestión y la persona que administra de la red.

El agente administrador (Agente), son elementos como: hosts, puentes, ruteadores y hubs, pueden ser equipados con agentes SNMP con el objetivo de poder ser administrados desde una estación administradora. El agente administrador responde a peticiones, para información y acciones desde la estación de gestión.

La colección de objetos se refiere a una base de información administrada. La MIB funciona como una colección de puntos de accesos en el agente para la estación de gestión, el cual es un estándar. Una estación de gestión realiza la función de supervisión tomando el valor de los objetos MIB. Una estación de gestión puede hacer una acción

al recurrir en un agente o puede cambiar la configuración en un agente modificando el valor de variables específicas.

Los estándares no especifican el número de estaciones de gestión o el radio de estaciones de gestión hacia los agentes. En general, es mejor tener dos sistemas capaces de realizar la función de estación de gestión, para proveer redundancia en caso de falla. Otra es una forma práctica de cuantos agentes puede manejar una simple estación de gestión.

2.9.1 SNMP (Protocolo simple de administración de red)

SNMP definido en la RFC 1157, muestra una manera de administrar y supervisar las redes de manera que se sea capaz de identificar y solucionar problemas existentes en la red, y poder expandir la red sin ningún problema. Dicho protocolo se encuentra implementado en la capa de aplicación, perteneciendo a los protocolos de TCP/IP. Puede administrar diferentes tipo de equipos por ejemplo: puentes, repetidores, terminales del código estándar Estadounidense para el intercambio de información y diferentes tipos de tecnología de interfaz como: punto apunto DS1, DS2, Frame Rele, Ethernet, Token-Ring entre otros (Sosa, 2006).

El protocolo usado para la administración de redes TCP/IP es el Simple Network Management Protocol (SNMP), el cual incluye las siguientes capacidades dominantes:

- Get: Permite a la estación de gestión recuperar el valor de los objetos en el agente.
- Set: Permite a la estación de gestión alterar el valor de los objetos en el agente.
- Trap: Permite a un agente notificar a la estación de gestión de eventos significativos.

Existen 3 versiones del protocolo: SNMPv1 (versión 1), SNMPv2 (versión 2) y SNMPv3 (versión 3). Las tres tienen el mismo principio, solo que SNMPv2 tiene algunas mejoras sobre la primera versión, y de la misma forma SNMPv3 tiene ciertas ventajas sobre la segunda versión.

2.9.2 CMIP (Protocolo de Administración Común de Información)

El protocolo de Administración Común de Información por sus siglas en inglés (CMIP: Common Management Information Protocol) es un estándar para la administración de redes a través de objetos manejados que suministran seguridad avanzada y reporteo de condiciones inusuales de la red. El protocolo CMIP fue establecido para simplificar y mejorar las insuficiencias y capacidades de administración del protocolo SNMP (Nuevas Tecnologias, 2010).

2.9.2.1 Protocolos de aplicación CMIP

Para comunicarse entre sí dos aplicaciones gestor y agente se utilizan unidades de datos del protocolo de aplicación por sus siglas en Ingles (APDU's: Application Protocol Data Units). CMIP está compuesto de los protocolos OSI que siguen:

- **ACSE**: Elemento de servicio de control de asociación por sus siglas en inglés (ACSE: Association Control Service Element) se utiliza para establecer y liberar asociaciones entre entidades de aplicación.

- **ROSE**: Elemento de servicio de operación remota por sus siglas en inglés (ROSE: Remote Operation Service Element) es el equivalente OSI a una llamada de un procedimiento remoto. ROSE permite la invocación de una operación en un sistema remoto. CMIP usa los servicios orientados a conexión proporcionados por ROSE para todas las peticiones, respuestas y respuestas de error.

Elemento de servicio de información de gestión común por sus siglas en inglés (CMISE: Common Management Information Service Element) proporciona los servicios básicos de gestión confirmados y no confirmados para reportar eventos y manipular datos de gestión. CMISE hace uso de los servicios proporcionados por ROSE y ACSE.

2.9.3 Comparación del protocolo SNMP Y CMIP

EL protocolo SNMP está basado en técnicas de sondeo, mientras que CMIP utiliza una técnica basada en eventos. Esto permite a CMIP ser más eficiente que SNMP en el control de grandes redes.

SNMP es un protocolo sin conexión mientras que CMIP es un protocolo orientado a conexión. Esto significa que la carga de proceso de SNMP es reducida, pero cuando se envía un mensaje nunca se puede asegurar que el mensaje llega a su destino, se puede considerar una mala gestión de la red. La seguridad de los datos no es prioritaria para SNMP.

CMIP permite, mediante una única petición, la recogida de gran cantidad de datos de los objetos gestionables, enviando información de retorno en múltiples respuestas. Esto no está permitido en SNMP.

SNMP está recomendado para la gestión inter-red en donde necesita el nombre de cada objeto, mientras que CMIP está especialmente preparado para gestionar grandes redes distribuidas, esto permite la implementación de comandos condicionales sofisticados.

CMIP realiza una distinción clara entre los objetos y sus atributos. SNMP no permite esto, lo cual hace imposible la reutilización de atributos y definiciones.

CAPITULO III

ANALISIS DE LA SITUACION ACTUAL Y REQUERIMIENTOS

Este capítulo hace referencia a la recopilación de información actualizada referente a la red inalámbrica del Gobierno Autónomo Descentralizado Intercultural y Plurinacional (GADIP) del Municipio de Cayambe y de la infraestructura tecnológica del mismo. Obteniendo la información de fuentes confiables para hacer uso de ella con responsabilidad, respetando la confidencialidad de esta. Además de permitir establecer requerimientos actuales y futuros a ser requeridos en el diseño de la red inalámbrica.

Además, se describe el diseño de la nueva red inalámbrica que se va a integrar en la actual red inalámbrica utilizando el estándar IEEE 802.11ac, el respectivo análisis de la topología actual, la zona de cobertura, ubicación de los nodos, puntos involucrados, dimensionamientos de red, enlaces, equipos, anchos de banda, velocidad de transmisión, la ubicación de dichos equipos, simulaciones en un software libre y los mecanismos de seguridad que se utilizara en el diseño de la red.

3.1 GADIP del Municipio de Cayambe

El GADIP de Cayambe, se encuentra ubicado en el centro de la ciudad de Cayambe, provincia Pichincha, entre las calles TERÁN Y SUCRE SO-54. Su edificación central cuenta con dos plantas como se muestra en la Figura 15. En las cuales se distribuyen varios departamentos que cumplen diferentes funciones, entre estos se encuentra la Dirección de Tecnologías de la Información (TICS), el que se encarga de brindar todos los servicios tecnológicos que requiere la institución para su buen desempeño diario en cada una de sus funciones.

El GADIP de Cayambe se encuentra en un proceso de conectividad como se indica en el Plan de Desarrollo y Ordenamiento Territorial Impulsado por el Gobierno

Autónomo Descentralizado y Plurinacional del Municipio de Cayambe, el cual permite a sus habitantes tener una ciudad digital con acceso a internet de manera Gratuita.

Misión: Fortalecer la participación ciudadana intercultural las potencialidades socioculturales, económico productivas, el desarrollo del intercultural, el manejo sostenible de los recursos naturales, mediante la implementación de infraestructura física, la provisión de bienes y servicios el ordenamiento y regulación territorial urbano y rural a fin de alcanzar una sociedad solidaria encaminada al Sumak Kawsay.

Visión: Una institución que lidera un modelo de gestión intercultural y plurinacional con una activa participación ciudadana y comunitaria atendiendo las necesidades individuales y colectivas de manera corresponsable con los actores sociales y demás niveles de gobierno construyendo una sociedad intercultural (GADIP-Cayambe, 2019)**.**

Figura 14

Vista frontal del GADIP Cayambe.

Fuente: Elaborado por el Autor

3.2 Antecedentes de la situación Demográfica Guachalá

Se realiza un estudio demográfico de la zona en donde se realiza el diseño de la red en este caso es la Comunidad San Luis de Guachalá perteneciente a la provincia de Pichincha Cantón Cayambe. La comunidad Guachalá está ubicada en la parroquia Cangahua, a una altura de 2.756 msnm y con un clima de 16 °C, se encuentra a una distancia de 6 km de la ciudad de Cayambe. Con una posición geográfica envidiable, se ubica en la Mitad del Mundo Latitud 0°0’0”, ha sido objeto de varias investigaciones de relevancia por su gran valor histórico – científico, una de ellas fue la Misión Geodésica de la Academia de Ciencias de París (Turismo, 2012).

En la figura 16 se muestra una vista del mapa Google Hearth de la Zona Central de San Luis de Guachalá ubicado en la Panamericana E35 Tronal de la Sierra.

Figura 156

San Luis de Guachalá

Fuente: Recuperado de Google Earth

Actualmente el Internet juega un papel esencial en las actividades sociales, culturales y económicas, por lo que el acceso a Internet se ha convertido en una necesidad más que

en una utilidad. Por esta razón los computadores portátiles, tablets y la mayoría de los teléfonos inteligentes incorporan interfaces Wi-Fi. Para las comunidades, proporcionar acceso a Internet mediante Wi-Fi fomenta el desarrollo económico y promueve el turismo en una variedad de lugares, como aeropuertos, centros de convenciones, estadios, centros comerciales y otros lugares públicos donde se reúnen los residentes y visitantes

3.2.1 Turismo en el Ecuador

El turismo es una actividad económica que ha crecido rápidamente en todo el mundo en las últimas décadas, permitiendo descubrir lugares únicos, culturas impresionantes, paisajes increíbles y vivir experiencias nuevas.

En los últimos años, uno de los sectores más afectados económicamente por la pandemia del COVID19 ha sido el turismo (Proaño, Cunalata y Maldonado, 2020). Según la Organización Mundial del Turismo (OMT), debido a que los viajes internacionales cayeron hasta un 78 % en 2020, lo que provocó el despido de millones de trabajadores del sector servicios y, según se informa, el total de llegadas de turistas cayó de 29 000 millones a 400 millones, lo que significa más de 450 mil millones de dólares en pérdidas. Esta pérdida económica ha provocado crisis económicas representativas, principalmente en países donde el turismo representa más del 15% del PIB (Ramón, Villacís y García, 2020).

Según el Ministerio de Turismo, en Ecuador, desde el primer trimestre de 2015 hasta el cuarto trimestre de 2019, la contribución del turismo receptor al PIB promedió 1,9, o alrededor de 490 millones de dólares estadounidenses. La situación en los países latinoamericanos es difícil porque nunca han enfrentado consecuencias a este nivel y

deben aprender y generar estrategias para restablecer y fortalecer la prestación de servicios. (MINTUR, 2019).

Gracias a la reactivación gradual que se está realizando en el país se ha logrado que entre enero y mayo de 2022 en el sector turístico se logró registrar ingresos por USD 939 millones, según el Servicio de Rentas Internas (SRI). Eso significa una recuperación de 28% frente a los primeros cinco meses de 2021, y de 34% en comparación con el mismo período de 2020, un año atípico por la pandemia. Si bien el sector registra recuperación en 2022, esta no alcanza niveles prepandemia. Entre enero y mayo de 2019, las ventas del sector fueron de USD 1.117 millones.

3.2.2 Área de Cobertura

Para el determinar el área de cobertura de la red WLAN se tomará en cuenta, los lugares en los que se garantizará la cobertura del servicio de Internet inalámbrico gratuito, son las áreas de la mitad del mundo, el reloj solar y los patios de comida de la comuna San Luis de Guachalá. En estos sitios se concentran las personas y se tienen las facilidades de comodidad y seguridad para que los habitantes y turistas hagan uso del servicio de Internet gratuito.

En las figuras se muestran los lugares que se pondrá a disposición el servicio de internet gratuito.

- Monumento Mitad del Mundo

Figura 167

Mitad del Mundo atractivo turístico

En la figura 17 se muestra imágenes de La Bola de Guachalá, es un monumento en honor a la línea ecuatorial, es en esta línea que divide la tierra en dos hemisferios iguales: Norte y Sur. Cualquiera que llegue a este lugar no puede evitar la tentación de pararse en ambos hemisferios al mismo tiempo.

Figura 178

Cartel informativo de distancia de Cayambe, de diferentes países

En la imagen 18 se muestra cartel informativo de distancia de Cayambe, de diferentes países escrito encima de una flecha de madera. El parque nacional Cayambe Coca en Ecuador.

La línea monumento, dos del ecuador empedró marcas de la estatua de los hombres el punto a través del cual el ecuador pasa, Cayambe, Ecuador.

Figura 189

Quitsato Reloj solar

En la figura 19 se muestra el monumento funciona tanto como un gran calendario, así como un reloj solar, convirtiéndose así, en el mejor sitio del mundo, para entender los movimientos aparentes del Sol, cómo funcionan las estaciones, la historia del calendario, el calendario agrícola y diferentes aspectos geográficos astronómicos. El Reloj Solar Quitsato es el primer y único Monumento de la Mitad del mundo, que se encuentra exactamente en la Línea Ecuatorial o Paralelo Cero.

3.2.3 Población en Guachalá

La comunidad San Luis de Guachalá cuenta aproximadamente con 1800 habitantes según el censo 2018- 2019, en sus 4 Barrios: La Bola, Santa Mónica, La Estación y San Isidro, el presente proyecto se enfoca en el barrio la Bola por ser conocida en la mitad del mundo en donde existe afluencia de personas de dicha comunidad y personas extranjeras.

Para determinar el número de usuarios en el lugar antes mencionado se planteó una observación de campo, el levantamiento de esta información se realiza una observación de los posibles usuarios de la comuna Guachalá que concurran diariamente a dicho lugar, de preferencia los viernes, sábado y domingo debido a que son los días con más afluencia de personas que pueden estar en la zona de cobertura. Los fines de semana son los días en donde la mayoría de las personas nativas y turistas concurren a este lugar donde puede hacer deporte, disfrutar de un plato típico, visitar los distintos tipos lugares turísticos.

El levantamiento de la información se realizará en 3 zonas diferentes en horarios Mañana 8am a 11am, Medio día 12:30pm a 2pm y en la Tarde 3pm a 5pm, estos horarios son de más afluencia de gente.

En las tablas 3,4,5 se muestra unos datos referenciales echas en los días mencionados en el transcurso de la semana de lunes a jueves la afluencia de personas es normal de 5 a 15 personas en los tres sectores.

Tabla 3

Número de usuarios por zonas (viernes).

Viernes

Horarios	8am - 11am	12:30pm-2pm	3pm-5pm
Zona 1	8	6	12
Zona 2	10	8	7
Zona 3	8	6	7
Total	26	20	26

Fuente: Elaborado por el Autor

Tabla 4

Número de usuarios por zonas (sábado).

Sábado			
Horarios	8am -11am	12:30pm-2pm	3pm - 5pm
Zona 1	20	15	20
Zona 2	15	8	12
Zona 3	14	25	20
Total	49	48	52

Fuente: Elaborado por el Autor

Tabla 5

Número de usuarios por zonas (domingo).

Domingo			
Horarios	8am - 11am	12:30pm -2pm	3pm-5pm
Zona 1	20	15	10
Zona 2	16	12	6
Zona 3	12	25	20
Total	48	52	36

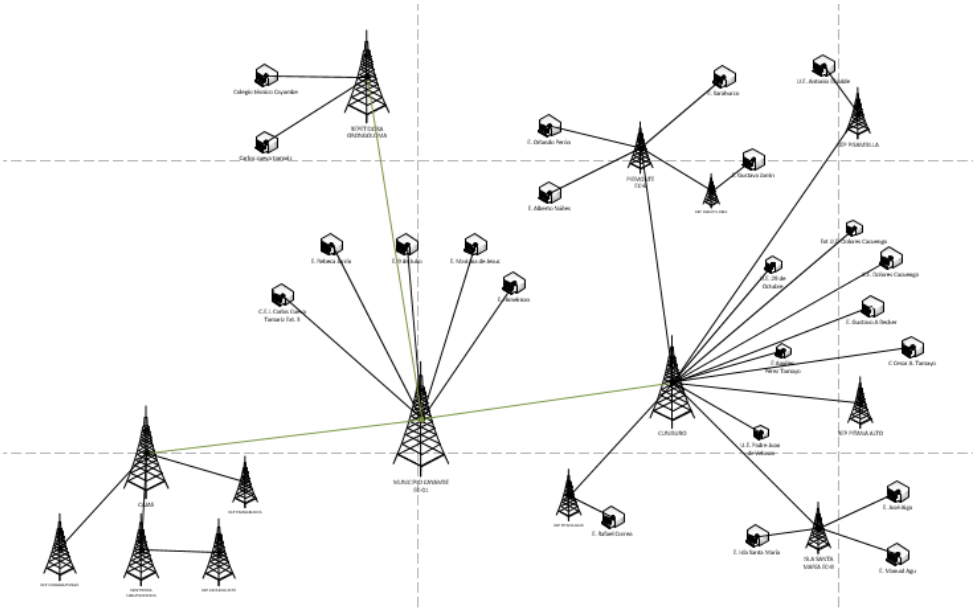
Fuente: Elaborado por el Autor

3.3 Topología de Red inalámbrica

Actualmente la red inalámbrica de Municipio de Cayambe cuenta con una topología tipo estrella, tiene una torre de aproximadamente 15 metros de altura con protección eléctrica e infraestructura metálica que se encuentra en el edificio del GADIP de Cayambe ubicado en la terraza de esta, este nodo conecta a múltiples Instituciones Educativas y parques públicos a cargo del municipio para brindar conectividad a Internet mediante la conexión Inalámbrica, como se muestra en la Figura 20.

Figura 19

Topología de la red Inalámbrica del Municipio de Cayambe.



Fuente: Recuperado de Microsoft Visio

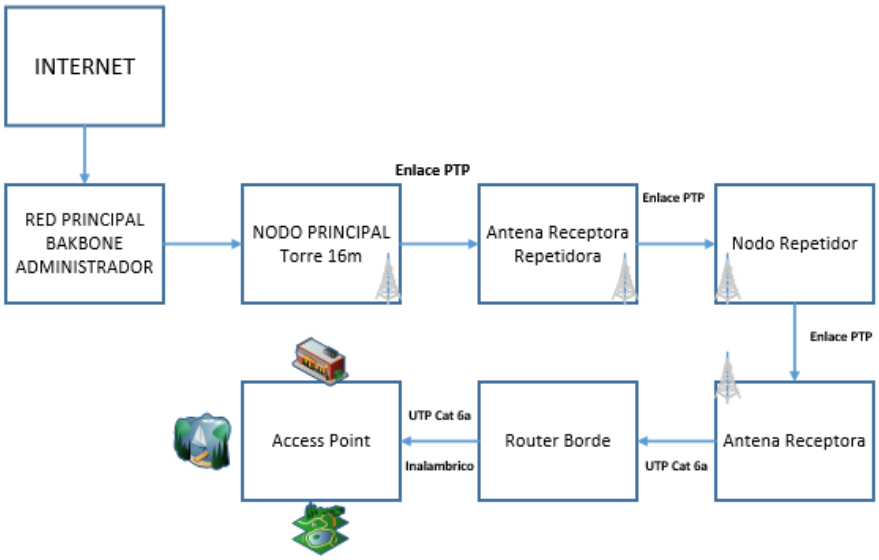
La topología cuenta con 3 repetidoras principales ubicadas en lugares estratégicos del cantón, una ubicada en el sector Cuniburo a 8.57 Km, otra en Orongoloma a Km y otra en Cajas a Km, ubicadas en las montañas más altas del cantón Cayambe pertenecientes a la provincia de Pichincha, cada una de estas conectan con repetidoras secundarios que brindan conectividad a varias Instituciones Educativas y comunidades pertenecientes al

cantón Cayambe. El GADIP cuenta con un ancho de banda de 100Mbps de los cuales 55Mbps son asignados a las escuelas y lugares públicos. Esta información fue adquirida por el administrador a cargo de la red. También se muestran los enlaces entre las repetidoras antes mencionadas, puntos de acceso (APs) y unidades educativas con sus respectivos equipos utilizados en cada uno de ellos.

3.4 Diagrama de Proceso de Red

Figura 20

Diagrama de proceso de red



Fuente: Elaborado por el Autor

Como se muestra en la Figura 21 se utilizará el siguiente diagrama para el diseño de la red, se iniciará a partir del nodo repetidor Cuniburo, es importante conocer la situación actual de la red el punto que se va a prestar el servicio de internet, coordenadas geográficas, datos de infraestructura, ancho de banda, usuarios directos e indirectos,

línea de vista y sus respectivas distancias. Se realizará una pequeña topología que mejor se adapte a las necesidades del entorno.

El diseño se tomará como punto de partida el GADIP del Municipio de Cayambe, tenido en cuenta que el enlace hacia la repetidora Cuniburo ya se encuentra en funcionamiento con un enlace punto a punto, en la repetidora Cuniburo se establecerá un enlace punto a punto hacia un nodo repetidor ubicado en un lugar que tenga line de vista entre la repetidora y la zona central Guachalá teniendo así conexión entre el municipio de Cayambe y la zona antes mencionada para esto se utilizara el software, Radio Mobile y Google Earth, los cuales ayudaran a analizar la zona de Fresnel y la ubicación de equipos, teniendo enlaces confiables que se puedan realizar sin problemas. Una vez establecido los enlaces se procede a realizar un diseño de una red WLAN que cubra los lugares de mayor afluencia de personas teniendo en cuenta que el acceso debe ser mediante un Portal Cautivo y todo esto gestionado por el administrador de la red utilizando FCAPS como modelo funcional.

3.5 Especificaciones técnicas para los enlaces

Para el diseño de la red es fundamental tener información de los puntos involucrados en cuanto a la infraestructura existente, las coordenadas geográficas y además el ancho de banda, para el cual se realizará una topología que se adapte a las necesidades de la red ya existente.

- El proyecto consiste en conectar mediante radio enlace a un nodo repetidor ubicado en un lugar estratégico para poder acceder a la zona a intervenir.

- La ubicación del nodo repetidor es de mucha importancia porque es el que permitirá crear un enlace entre el municipio y la zona central del sector de Guachalá de una manera eficiente, para lo cual se debe considerar varios factores importantes:

- Considerar el perfil del terreno, el cálculo de la altura adecuada a fin de conseguir una correcta ubicación del nodo, tomando en cuenta los posibles factores que interfieran y afecten la calidad de la señal.

- Considerar una altura adecuada que permita una visibilidad directa de transmisión entre los tres puntos involucrados. Este puede ser tanto para los enlaces punto a punto entre la repetidora Cuniburo hacia el nodo repetidor y el punto a punto entre nodo repetidor y la zona central.

3.5.1 Ubicación de Nodo repetidor

Para la selección del Nodo repetidor se tomó en cuenta muchos aspectos importantes referentes a demografía de lugar involucrado teniendo en cuenta que existe un problema de line a de visto por lo que se propone la implementación de un rebote que ayude a interconectar la zona central de Guachalá a la red del Municipio de Cayambe, a continuación, se describe el principal problema y se propone la ubicación del nuevo nodo repetidor.

Actualmente la Zona Central de Guachalá no cuenta con el servicio de internet, por motivo que no tiene line a de vista con ninguna repetidora a cargo del GADIP Cayambe, dicha zona es uno de los lugares más concurridos por ser la mitad del Mundo y no cuenta con acceso a internet, en la Figura 21 se puede observar el principal problema de línea de vista.

Figura 21

Problema de línea de vista en Guachalá

Fuente: Elaborado por el Autor

Como se muestra en la Figura 22, existe una gran cantidad de árboles que obstruyen la línea de viste al nodo Cuniburo para enlazar dichos lugares se necesitaría una torre con una altura considerable o ver la posibilidad de talar los árboles que tienen sus respectivos años de antigüedad, lo que conllevaría un mayor costo, permiso y tiempo para la implementación del proyecto, por lo cual planteó la propuesta de un nodo repetidor que será ubicado en un lugar estratégico para que ayude a conectar los lugares antes mencionados, se realizó la respectiva inspección y se presenta la mejor opción para el nodo repetidor que se muestra en la figura 23 a continuación.

Figura 22

Lugar para el nodo repetidor.

Fuente: Elaborado por el Autor

Como se muestra en la Figura 23 se consideró este lugar porque tiene línea de vista con los dos lugares involucrados y está a cargo de la comunidad, cuenta con una losa de hormigón aproximadamente de 40 metros cuadrados, además de la disponibilidad de energía eléctrica que alimentara los equipos sin costo de arriendo y sin ruido generado por antenas cercanas. Se instalará sobre un tubo galvanizado de 2 metros de altura el cual será empotrado sobre la loza de hormigón teniendo una altura aproximada de 6.5 metros de altura del suelo

3.6 Ubicación de equipos en la zona central Guachalá.

Para determinar la ubicación adecuada del equipo receptor se realizó una visita al lugar, se observa que existe un Infocentro que se encuentra a cargo de la comunidad beneficiada, en la parte central existe un poste con un reflector que ilumina la atracción principal, se necesitaría de un herraje con base para una caja en donde se pueda ubicar los equipos y otro herraje con una base de tubo galvanizado tipo L para la antena

receptora y el Access Point. La ubicación es idónea para colocar los equipos, al igual que el Access Point por su robustes, alcanza a cubrir las 3 zonas descritas anteriormente, garantizando la cobertura del todo el lugar al mismo tiempo de ser una red escalable por tener 3 puertos ethernet en el router de borde los cuales pueden ser utilizaos para ampliar la red utilizando equipos según las necesidades futuras.

Figura 234

Ubicación de equipos estación receptora

Fuente: Elaborado por el Autor

En la Figura 24 se puede observar un poste con un reflector en donde van a ser ubicados los equipos dentro de una caja térmica, la antena receptora junto a 3 Access Point de alta potencia.

3.7 Dimensionamiento de enlaces

Debido a que el diseño de red se basa en tecnología inalámbrica, el estudio que se hace en esta sección está enfocado concretamente a esta tecnología, pues existen estudios más rigurosos para el estudio de radio enlaces sin especificar el tipo de tecnología que se está empleando.

3.7.1 Línea de vista

El término línea de vista, a menudo abreviado como LOS (*Line of Sigh*t) representa la línea visual entre el receptor y transmisor. La verificación de la línea de vista entre el enlace permitirá saber qué tan confiable puede ser dicho enlace que se propone para unir los puntos a interconectar.

3.7.2 Zonas de Fresnel

Las ondas electromagnéticas al propagarse entre dos puntos determinados configuran un elipsoide cuya sección transversal aumenta a medida que el frente de ondas se aleja de los extremos. Este fenómeno es variable con la frecuencia y da lugar a la formación de las denominadas zonas de Fresnel.

3.7.3 Cálculo del presupuesto de potencia

El cálculo del presupuesto de potencia es el procedimiento que se utiliza normalmente para estimar de una manera rápida si un radio enlace funcionará correctamente.

La potencia disponible en un sistema inalámbrico puede caracterizarse por los factores como la potencia de transmisión, ganancia de las antenas, pérdidas en los cables, la sensibilidad del receptor. Que las señales puedan o no ser enviadas entre los radios dependerá de la calidad del equipamiento que se esté utilizando y de la disminución de la señal debido a la distancia, denominada pérdida en la trayectoria.

Además, cuando se calcula la pérdida en la trayectoria, se deben considerar varios efectos, algunos de ellos son la pérdida en el espacio libre, atenuación y dispersión. En primera instancia para que un enlace sea viable la potencia recibida debe ser superior a la sensibilidad del receptor, teniendo en cuenta la potencia transmitida, las ganancias y las pérdidas del enlace. Para calcular la potencia recibida se tiene la siguiente ecuación:

$$PRx = PTx + GTx - LCCTx - LP + GRx - LCCRx$$

Donde:

$\boldsymbol{PRx}$: Potencia recibida por el receptor

$\boldsymbol{PTx}$: Potencia de transmisión

$\boldsymbol{GTx}$: Ganancia de la antena de transmisión

$\boldsymbol{LCCTx}$: Pérdidas de cables y conectores en el sistema de transmisión

$\boldsymbol{LP}$: Pérdidas en espacio libre

$\boldsymbol{GRx}$: Ganancia de la antena de recepción

$\boldsymbol{LCCRx}$: Pérdidas de cables y conectores en el sistema de recepción

Potencia de Transmisión

La potencia del transmisor es la potencia de salida del equipo emisor, este valor se encuentra en las especificaciones del fabricante; su límite superior depende de las regulaciones de cada país. La potencia típica para equipos IEEE 802.11 varían entre 30 – 600 mW.

Pérdidas en los Cables

El cable que une los equipos de transmisión/recepción con las antenas agrega pérdidas al sistema. Las pérdidas dependen del tipo de cable y de la frecuencia de operación del sistema y normalmente se mide en dB/m o dB/pie.

Los valores típicos de pérdidas en los cables van desde 0,1 dB/m hasta 1 dB/m. Un cable siempre presentará pérdidas, independientemente del tipo y calidad del cable utilizado, por lo que el cable que une la antena hacia el equipo debe ser lo más corto posible. En general mientras mayor sea el diámetro del cable que se está usando menor será la atenuación con una misma longitud.

Perdida en Conectores

Los conectores en los cables coaxiales y los adaptadores (extensiones) incrementan las pérdidas de un sistema. Para cables coaxiales certificados se debe estimar 0.25 dB de pérdida por cada conector, este valor puede incrementar si los cables son fabricados por el usuario. Como regla general se considera un promedio de 0,3 a 0,5 dB por conexión.

Ganancia de las Antenas

Las antenas son dispositivos pasivos que crean el efecto de amplificación debido a su forma física. La ganancia de la antena se proporciona habitualmente en dB isotrópicos (dBi), es decir, la ganancia de potencia con respecto a un modelo teóricode antena isotrópica que radia la misma energía en todas las direcciones del espacio.

Pérdidas en el Espacio Libre

Se trata de las pérdidas de propagación que sufre la señal radioeléctrica en condiciones de espacio libre, sin ningún obstáculo en el camino, es decir, visión directa

entre las antenas. En esta magnitud no suelen incluirse otras pérdidas adicionales debidas a lluvia, absorción atmosférica, niebla, etc. Estas pérdidas están relacionadas directamente con la distancia del radio enlace y la frecuencia de funcionamiento mediante la siguiente expresión:

$Lp(dB) = 92{,}4 + 20log(\text{f}) + 20log(d)$

Donde:

f: Frecuencia de trabajo (GHz)

$\boldsymbol{d}$: Distancia total del enlace (Km)

Margen de Umbral

Permite relacionar la diferencia entre la potencia de recepción del enlace y el valorde sensibilidad mínimo del equipo:

$M_U = P_{Rx} - S$

En primera instancia se puede decir que $P_{Rx} > S$ para que funcione un radioenlace,ésta es una condición necesaria pero no suficiente debido a que no garantiza queel valor de M_U sea capaz de cubrir el desvanecimiento.

Comparación de Tipo de Antenas

A continuación, se hace una comparativa de los 3 tipos de antenas, según sus características y los requerimientos, elija la que se ajuste más a los requerimientos, en la tabla 6 se muestra las características más importantes.

Tabla 6

Comparación de antenas

	Direccional	**Omnidireccional**	**Sectorial**
Tipo de Enlaces	Punto a punto	Punto multipunto	Punto multipunto
Escalable	No	Si	Si
Ganancia	15 -30 dBi	6 dBi	19-20 dBi
Alcance	Largo	Corto	Medio

Fuente: Elaborado por el Autor

Para el diseño de la red inalámbrica se escoge la antena direccional porque son las que más se adaptan a las necesidades del diseño y cumplen con los requerimientos que son: soportar la comunicación punto a punto, quedaría con un enlace estable y a su vez permitir que la red pueda ser escalable a zonas más lejanas donde se encuentran otros lugares turísticos cuando se requiera ampliar el proyecto.

3.8 Requerimientos para enlaces punto a punto

Para calcular los enlaces es importante conocer las características de la tecnología a utilizar, comprender la velocidad del dispositivo a utilizar, la tasa de transferencia y su ancho de banda utilizable. El ancho de banda se refiere al caudal que se mide en Mbps, cabe recalcar que el ancho de banda se mide en MHz. Por lo que para un enlace punto a punto en el estándar 802.11ac para la onda 1 es 1300 Mbps, pero va a proporcionar más de 500 Mbps del caudal real y depende del equipo que se utilice y de algunos factores como la relación señal ruido. Y el resto estará (overhead) que necesita los radios para coordinar las señales.

Para el diseño de la red inalámbrica se debe tomar en cuenta ciertos parámetros mínimos que deben tener los equipos para los enlaces punto a punto en la tabla 7 se detallan las principales características que deben tener los equipos.

Tabla 7

Características de los equipos.

Parámetros	Característica
Estándar	802.11ac
Ancho del canal	20, 40, 80MHz
Velocidad de transmisión	500 Mbps
Frecuencia de operación	5.8GHz
Potencia de transmisión	23-30 dBm
Ganancia de transmisión	27-31 dBi
Ganancia de recepción	27-31 dBi
Distancia de enlace	5-10km

Fuente: Elaborado por el Autor

3.8.1 Comparación de antenas para enlaces punto a punto

Para garantizar un enlace estable de debe elegir la mejor opción, hacer una comparativa de diferentes marcas de antenas y elegir la que mejor se acople a las necesidades del enlace. A continuación, se muestra una Tabla 8 donde se hace la comparativa de 3 tipos de antenas.

Tabla 8

Comparación de antenas

Criterios	Mikrotik	Mikrotik	Ubiquiti AirMax
Modelo	SEXTANT G	RBLHGG-5HPacD2HPnD	RocketAC-R5AC-PTP
Radio incluido	No	Si	No
Estándar 802.11ac	Si	Si	Si
Ganancia	16dBi	27dBi	31dBi
Interfaz	Ethernet 10/100 Mbps	Ethernet 10/100 Mbps	Ethernet 10/100/1000 Mbps
Banda de Operación	2.4-5GHz	2.4-5GHz	2.4-5GHz
Memoria RAM	64 MB	256 MB	128 MB
Velocidad de transmisión	100Mbps	600 Mbps	500 Mbps
Consumo de energía	8W	18W	8.4 W
Material	Plástico	Plástico	Plástico estabilizado UV y aluminio
Compatibilidad de Estándares anteriores	Si	Si	Si

Fuente: Elaborado por el Autor

Para la selección de equipos se tomará las características de transmisión, por lo que en la tabla se menciona algunas características de tres fabricantes.

Principalmente, el equipo debe soportar el estándar IEEE 802.11ac que es la principal característica que debe cumplir por ser el estándar de diseño del proyecto. La mejor opción son las antenas Mikrotik RBLHGG-5HPacD2HPnD tiene una ganancia de 27 dBi, posee puertos 10/100 Mbps, velocidad de trasmisión 600Mbps, Una carcasa de plástico que reduce la interferencia al ruido. Además, cabe mencionar que el Municipio

de Cayambe trabaja con estos equipos en enlaces principales, otro aspecto importante es que el administrador ya tiene el conocimiento de cómo funciona y como operar estos equipos, tanto en rendimiento, escalabilidad, seguridad. Así como el factor económico.

3.8.2 Selección de antena para enlaces punto a punto

Antena Mikrotik RBLHGG-5HPacD2HPnD

Figura 24

Antena Mikrotik RBLHGG-5HPacD2HPnD

En la Figura 25 se muestra la robusta Antena RBLHGG-5HPacD2HPnD-XL también conocida como LHG XL 52 ac de MikroTik es una poderosa antena para enlaces Backbone PTP de alto rendimiento o ideal para Equipos Locales del Cliente (CPE) de larga distancia que opera en doble banda 2.4Ghz y 5GHz simultáneos y redundantes extremadamente potente para conexión de larga distancia sin tiempo de inactividad. En la tabla 9 se describe las características de un Antena RBLHGG-5HPacD2HPnD-XL

Tabla 9

Características de un Antena RBLHGG-5HPacD2HPnD-XL

Características	Especificación
Dimensiones	550 x 291 mm
CPU	Quad-core ARM Cortex A7, 716 MHz

Radio	LHG XL 52 ac
Protocolos compatibles	802.11 a/b/g/n/ac.
Rango de frecuencia	2412 - 2484 MHz 5150 - 5875 MHz
Ganancia	27 dBi
Sensibilidad de receptor	96 dBm
Tamaño RAM	256 MB
Potencia	29dBm en 2.4GHz y 30dBm en 5GHz.
Modo de Operación	CPE, Punto a Punto (PTP)
Temperatura	-40 C° a +70 C°
Apertura de Antena	27dBi apertura de 7° en 5GHz 18dBi apertura de 8° en 2.4Ghz
Entrada de PoE	802.3af/at
Sistema operativo	RouterOS
Voltaje	12 v – 57 v.

Fuente: https://i.mt.lv/cdn/product_files/LHG_XL_52_ac_191048.pdf

El radio LHG XL 52 ac incluido en la antena proporcionará una conexión de larga distancia sin tiempo de inactividad con su capacidad de doble banda. Se puede configurar fácilmente el canal de 5 GHz como el principal con velocidad de hasta 600 Mbps y utiliza el canal de 2,4 GHz como respaldo automático conexión con velocidad de hasta 260 Mbps o usar ambas conexiones al mismo tiempo para la carga equilibrio.

3.9 Cálculo de presupuesto de Potencia en los enlaces

3.9.1 Cálculo de presupuesto de potencia del enlace del nodo Cuniburo – Nodo Repetidor

Para obtener los valores aproximados de la distancia que existe entre los nodos se utilizó herramientas que existen en el software Google earth, para lo cual se usaron los datos de las coordenadas geográficas, altitud y longitud de los puntos involucrados.

Cálculo de pérdidas en el espacio libre (FSL)

Perdidas en el espacio libre para dos enlaces se podrá calcular utilizando la ecuación descrita a continuación.

$$\boldsymbol{FSL\ (dB)\ =\ 32.44\ +\ 20logf(Mhz)\ +\ 20logd(km)}$$

Donde:

L=perdidas en el espacio libre

F= frecuencia en MHz F=5800 (MHz)

D= la distancia en km D=4.42 (km)

$$\boldsymbol{FSL(dB)}\ =\ 32.44\ +\ 20log(5800(Mhz))\ +\ 20log(4.42(km))$$

$$\boldsymbol{FSL(dB)}\ =\ 32.44\ +\ 20\ *\ 3.7634\ +\ 20\ *\ 0.64$$

$$\boldsymbol{FSL(dB)}\ =\ 32.44\ +\ 75.268\ +\ 12.90$$

$$\boldsymbol{FSL(dB)\ =\ 120.616\ (dB)}$$

Cálculo del nivel de señal recibido en el receptor

El cálculo del nivel de señal recibido en el receptor se calcula mediante la siguiente ecuación:

$$\boldsymbol{PRx(dBm) = PTx(dBm) - LTx(dB) + GTx(dBi) - FSLx(dB) + GRx(dBi) - LRx(dB)}$$

Características de los equipos en Recepción y Transmisión:

- Potencia del transmisor **(PTxdBm)** = +30 dBm
- Pérdidas en los cables del Transmisor **(LTxdB)** = -3dB
- Ganancia de la antena en Transmisión **(GTxdBi)** = +27dBi
- Pérdidas en el Espacio Libre **(FSL)** = -120,358 dB
- Pérdidas en los cables en el Receptor **(LRxdB)** =-3 dB
- Ganancia de la antena en Recepción **(GRxdBi)** = +27 dBi
- Sensibilidad del Receptor **(SRxdBm)** =-96 dBm

$$PRx(dBm) = 30 - 3 + 27 - 120{,}616 + 27 - 3$$

$$PRx(dBm) = \mathbf{-42,616\ dBm}$$

Cálculo del margen de la potencia de recepción

El cálculo del margen de la potencia de recepción del enlace está dado por la siguiente ecuación:

$$\boldsymbol{M(dB) = PRx(dBm) - SRx(dBm)}$$

$$M(dB) = -42{,}616(dBm) - (-96(dBm))$$

$$M(dB) = \mathbf{53,384}\boldsymbol{dB}$$

3.9.2 Cálculo de presupuesto de potencia del enlace Nodo Repetidor-Guáchala

Para obtener los valores aproximados de la distancia que existe entre los nodos se utilizó herramientas que existen en el software Google earth, para lo cual se usaron los datos de las coordenadas geográficas, altitud y longitud de los puntos involucrados.

Cálculo de pérdidas en el espacio libre (FSL)

Perdidas en el espacio libre para dos enlaces se podrá calcular utilizando la ecuación descrita a continuación.

$$\boldsymbol{FSL\,(dB)\,=\,32.44\,+\,20logf(Mhz)\,+\,20logd(km)}$$

Donde:

L=perdidas en el espacio libre

F= frecuencia en Mhz F=5800 (Mhz)

D= la distancia en km D=0.41(km)

$$\boldsymbol{FSL(dB)}\,=\,32.44\,+\,20log(5800(Mhz))\,+\,20log(0.41(km))$$

$$\boldsymbol{FSL(dB)}\,=\,32.44\,+\,20\,*\,3.7634\,+\,20\,*\,-0.38$$

$$\boldsymbol{FSL(dB)}\,=\,32.44\,+\,75.268\,\,-\,7.74$$

$$\boldsymbol{FSL(dB)}\,=\,\boldsymbol{99.968\,(dB)}$$

Cálculo del nivel de señal recibido en el receptor

El cálculo del nivel de señal recibido en el receptor se calcula mediante la siguiente ecuación:

$$\boldsymbol{PRx(dBm)} = PTx(dBm) - LTx(dB) + GTx(dBi) - FSLx(dB) + GRx(dBi) - LRx(dB)$$

Características de los equipos en Transmisión y Recepción:

- Potencia del transmisor **(PTxdBm)** = +23 dBm
- Pérdidas en los cables del Transmisor **(LTxdB)** = -3dB
- Ganancia de la antena en Transmisión **(GTxdBi)** = +24dBi
- Pérdidas en el Espacio Libre **(FSL)** = -99,968 dB
- Pérdidas en los cables en el Receptor **(LRxdB)** =-3 dB
- Ganancia de la antena en Recepción **(GRxdBi)** = +24 dBi
- Sensibilidad del Receptor **(SRxdBm)** =-96 dBm

$$PRx(dBm) = 23 - 3 + 24 - 99{,}968 + 24 - 3$$

$$PRx(dBm) = \mathbf{-41,968\ dBm}$$

Cálculo de margen de la potencia de recepción

El cálculo del margen de la potencia de recepción del enlace está dado por la siguiente ecuación:

$$\boldsymbol{M(dB) = PRx(dBm) - SRx(dBm)}$$

$$M(dB) = -41{,}968(dBm) - (-96(dBm))$$

$$M(dB) = \mathbf{54,032}\boldsymbol{dB}$$

3.10 Simulación de radioenlaces

La simulación con la herramienta Radio Mobile del sistema de radioenlace permite probar si el despliegue del sistema inalámbrico con los equipos y condiciones especificados por el lugar de trabajo es óptimo, dependiendo de los resultados que proporcione la simulación, la instalación del sistema puede o no ser aprobada.

Este software de Radio Mobile utiliza mapas topográficos del área de diseño del sistema inalámbrico. Los datos de la simulación nos proporcionan el dispositivo utilizado y Google Earth la ubicación geográfica de cada punto para dar acceso a internet.

Para un enlace punto a punto, se definen el siguiente dispositivo preseleccionados a ser utilizado:

Antena LHG XL 52 ac y radio LHG XL 52 ac

Potencia de Trasmisión: 30 dBm

Sensibilidad del receptor: -96 dBm

Frecuencia de Operación: 5.15 - 5.85 GHz

Ganancia de la antena: 27 dBi

3.10.1 Simulación enlace entre el nodo Cuniburo- nodo repetidor

En la tabla 10 se muestra los parámetros de configuración en el simulador Radio Mobile

Tabla 10

Parámetros de configuración

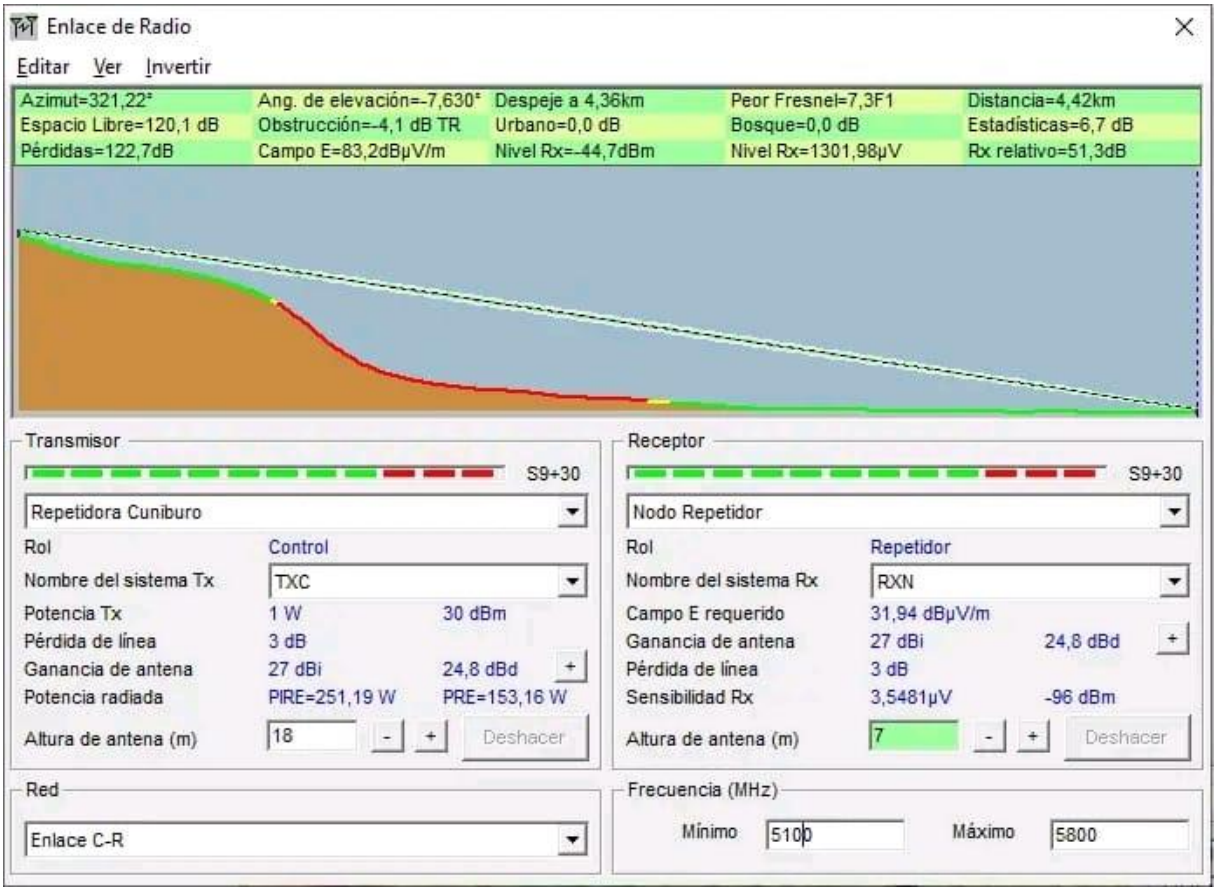
Nodo Cuniburo		**Nodo Repetidor**	
Característica	**Especificación**	**Característica**	**Especificación**
Latitud	0° 2'8.23"S	Latitud	0° 00'16.98"S
Longitud	78° 9'11.37"O	Longitud	78° 10'40.99"O
Elevación	3334 m	Elevación	2755m
Altura de torre	18 m	Altura de Torre	7m
SISTEMAS DE RADIO			
Tipo de Antena	RBLHGG-5HPacD2HPnD-XL	Tipo de Antena	RBLHGG-5HPacD2HPnD-XL
Ganancia de Antena Tx	27 dBi	Ganancia de Antena Tx	27 dBi
Tipo de Radio	LHG XL 52 ac	Tipo de Radio	LHG XL 52 ac
Potencia de Tx (dBm)	30 dBm	Potencia de Tx (dBm)	30 dBm
Sensibilidad de recepción Rx(dBm)	-96 dBm	Sensibilidad de recepción Rx(dBm)	-96 dBm
Frecuencia (GHz)	(5150-5875) GHz	Frecuencia (GHz)	(5150-5875) GHz

Fuente: elaborado por el autor

En la tabla 10 se muestra los parámetros del enlace entre los nodos de Cuniburo – Nodo repetidor, la estación trasmisora es el Nodo Cuniburo y la receptora es el nodo Repetidor. Además de los parámetros del enlace como potencia de trasmisión, ganancia de la antena, frecuencia de operación tanto del transmisor como receptor y elevación del terreno.

Figura 256

Perfil del enlace entre Cuniburo- Nodo repetidor



Fuente: Recuperado de Radio Mobile

En la figura 26 nos describe los resultados de la simulación, tales como, el ángulo de azimut que está orientada la antena que es de 321.22° en orientación del trasmisor, perdidas en el espacio libre de 120.9dB, distancia del enlace 4.42 Km, el ángulo de Fresnel es de 7.3F1. El enlace es óptimo esto es debido a que un parámetro importante en enlace es el Nivel Rx en dBm, cuanto menor sea ese valor mejor calidad tendrá el enlace, lo ideal es se encuentre entre -40 y -70 dBm, en por lo tanto tenemos un valor de -42,616 dBm que están en rango ideal y El margen de la potencia de recepción que permite conocer el valor de margen respecto de la sensibilidad del sistema receptor con que llega la señal recibida y tenemos 53.384 dB.

Para tener una visualización en Google earth nos vamos a opción de editar > exportar a… y escogemos la opción Google earth, en la siguiente figura 27 se muestra el enlace Cuniburo – Nodo repetidor.

Figura 267

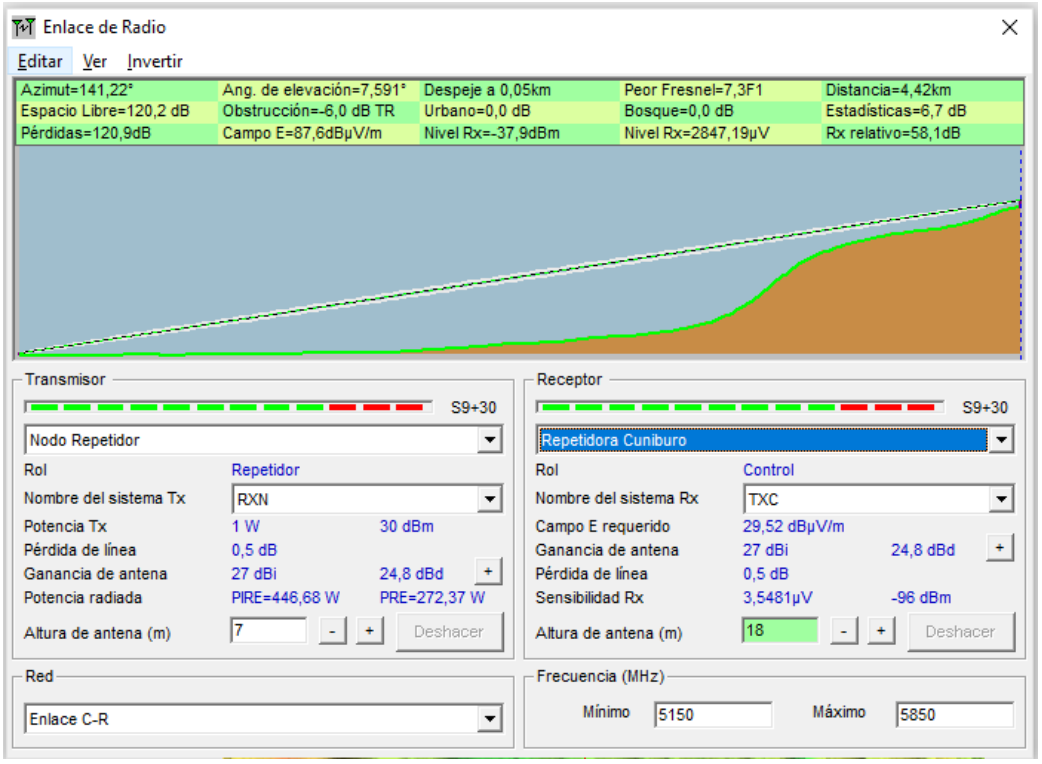
Enlace entre el nodo de Cuniburo – Nodo repetidor.

Fuente: Recuperado de Google Earth

Para una visualización del enlace y las zonas de fresnel se puede observar en la figura 27 mediante una simulación en el software google earth.

Figura 278

Enlace invertido entre de Nodo repetidor- Cuniburo.

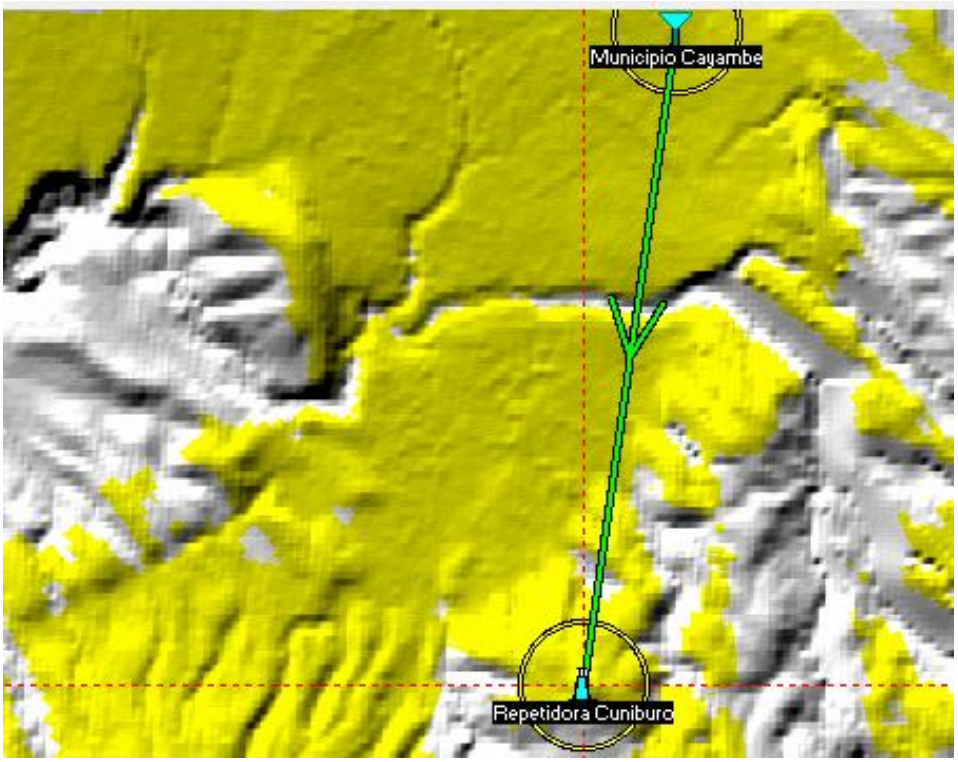


Fuente: Recuperado de Radio Mobile

Invirtiendo el enlace, el transmisor será el nodo repetidor y el receptor el nodo de Cuniburo, en la figura 28 se muestra el enlace invertido, por lo tanto, cambia el azimut, esto es debido a la orientación de los sistemas y los demás datos se mantienen.

Figura 289

Área de cobertura de los nodos Nodo repetidor- Cuniburo.



Fuente: Recuperado de Radio Mobile

En la figura 29 se muestra el área de cobertura del enlace Nodo repetidor- Cuniburo. Con la herramienta Radio Converge permite dibujar el área de cobertura de un enlace de radio y con la opción Single Polar se puede calcular el área de cobertura de una estación transmisora fija realizando un barrido en toda el área.

Comparación de datos calculados y simulación del enlace Cuniburo- Nodo repetidor.

En la tabla 11 se describe los cálculos matemáticos y la simulación en Radio Mobile del enlace Nodo repetidor- Cuniburo.

Tabla 11

Comparación de datos calculados y simulación del enlace Cuniburo- Nodo repetidor.

Enlace Cuniburo- Nodo repetidor.			
Características	**Datos calculados**	**Datos simulados**	**Margen de error**

Perdida del espacio libre (FSL)	120,616(dB)	120,1(dB)	0,516(dB)
Ninel mínimo de señal recibida en Rx (RSL)= Ganancia total – FSL	- 42,616(dBm)	-44.7(dBm)	2.08(dBm)

Fuente: elaborado por el autor.

En la tabla 11 se describe los resultados obtenidos de los datos calculados matemáticamente y en el software Radio Mobile, existiendo un margen de error debido a que en el software determina perdidas adicionales por múltiples trayectorias y obstáculos, además que en el simulador no existe el tipo de antena LHG XL 52 ac, por los que se debe elegir una antena similar en propagación de los lóbulos de radiación que es la Antena Corner, debido a estos factores es la variación de resultados.

3.10.2 Simulación enlace entre Nodo repetidor- Nodo Guachalá

En la tabla 12 se muestra los parámetros de configuración en el simulador Radio Mobile.

Tabla 12

Parámetros de configuración

Nodo repetidor		**Nodo Guachala**	
Característica	Especificación	Característica	Especificación
Latitud	0° 00'16.98"S	Latitud	0° 00'04.97"S
Longitud	78° 10'40.99"O	Longitud	78° 10'34.58"O
Elevación	2755m	Elevación	2751m
Altura de torre	7m	Altura de Torre	7 m
SISTEMAS DE RADIO			
Tipo de Antena	RBLHGG-5HPacD2HPnD-XL	Tipo de Antena	RBLHGG-5HPacD2HPnD-XL
Ganancia de Antena Tx	27 dBi	Ganancia de Antena Tx	27 dBi

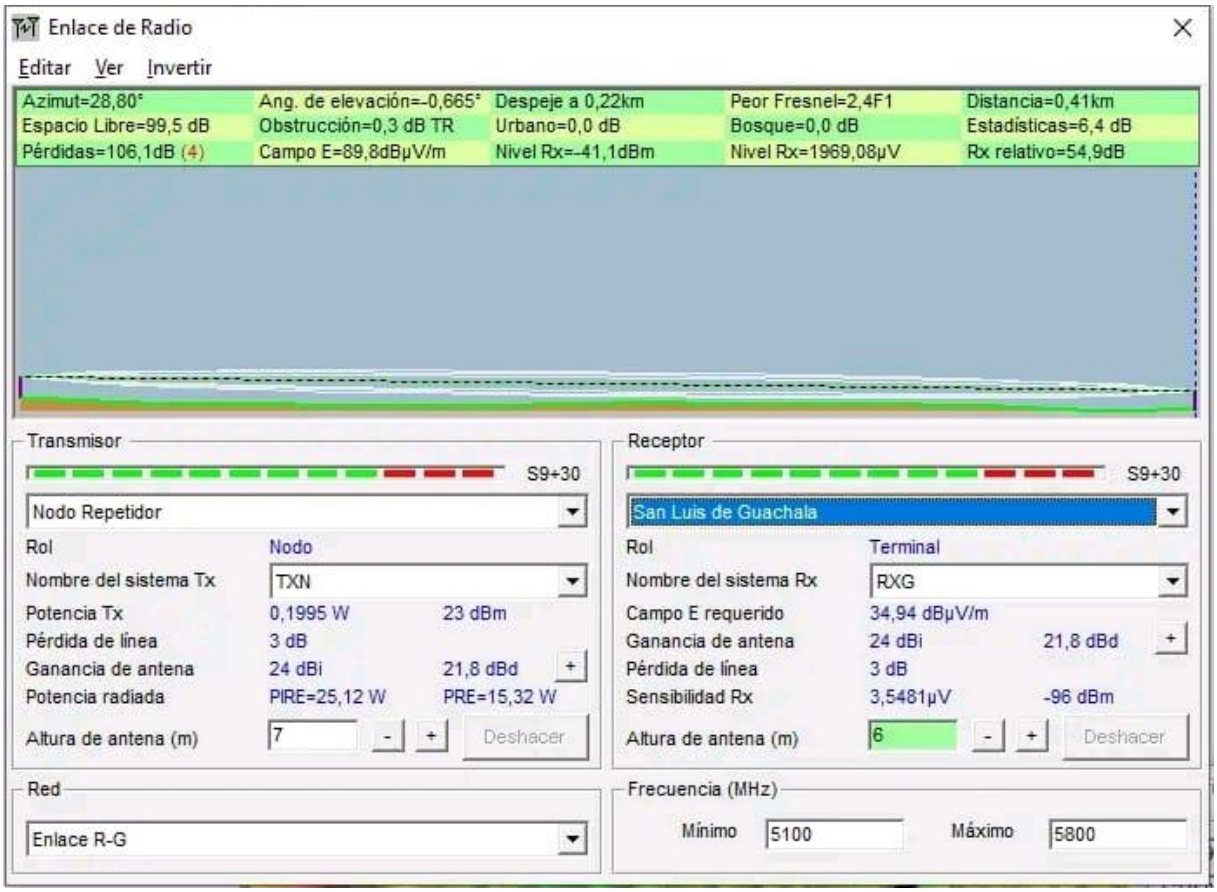
Tipo de Radio	LHG XL 52 ac	Tipo de Radio	LHG XL 52 ac
Potencia de Tx (dBm)	23 dBm	Potencia de Tx (dBm)	23 dBm
Sensibilidad de recepción Rx(dBm)	-96 dBm	Sensibilidad de recepción Rx(dBm)	-96 dBm
Frecuencia (GHz)	(5150-5875) GHz	Frecuencia (GHz)	(5150-5875) GHz

Fuente: elaborado por el autor

En la tabla 12 se muestra los parámetros del enlace entre el Nodo repetidor y el Nodo Guachalá, la estación trasmisora es el nodo repetidor y la receptora es el nodo Guachalá. Además de los parámetros del enlace como potencia de trasmisión, ganancia de la antena, frecuencia de operación tanto del transmisor como receptor y elevación del terreno.

Figura 29

Perfil del enlace entre el Nodo repetidor – San Luis de Guachalá



Fuente: Recuperado de Radio Mobile

En la figura 30 también describe los resultados de la simulación, tales como, el ángulo de azimut que está orientada la antena que es de 28.80° en orientación del trasmisor, perdidas en el espacio libre de 99.5dB, distancia del enlace 0.41 Km, el ángulo de Fresnel es de 2.4F1. El enlace es óptimo esto es debido a que un parámetro importante en enlace es el Nivel Rx en dBm, cuanto menor sea ese valor mejor calidad tendrá el enlace, lo ideal es se encuentre entre -40 y -70 dBm, en por lo tanto tenemos un valor de -44.3 dBm que están en rango ideal y El margen de la potencia de recepción que permite conocer el valor de margen respecto de la sensibilidad del sistema receptor con que llega la señal recibida y tenemos 71.7 dB.

Figura 30

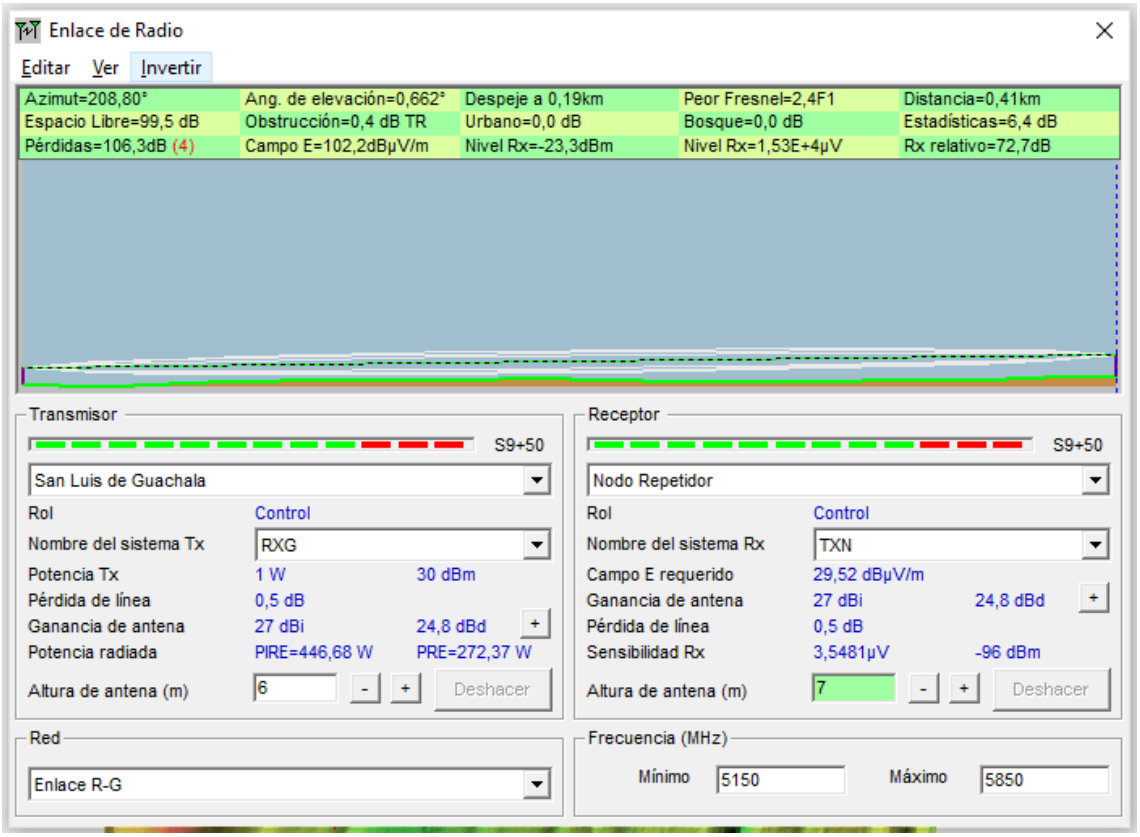
Enlace entre el Nodo repetidor – San Luis de Guachala

Fuente: Recuperado de Google Earth

Para tener una visualización en Google Earth nos vamos a opción de editar > exportar a… y escogemos la opción Google Earth, en la siguiente figura 31 se muestra el enlace Cayambe-Cuniburo.

Figura 31

Enlace invertido entre el nodo San Luis de Guachala – Nodo repetidor

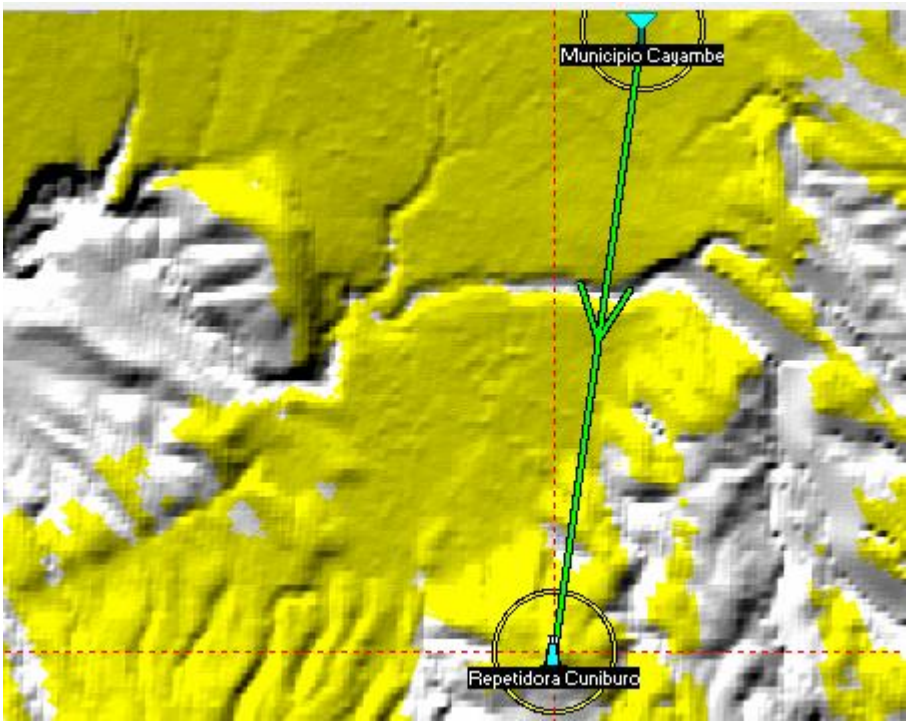


Fuente: Recuperado de Radio Mobile

Invirtiendo el enlace, el transmisor será el nodo Guachalá y el receptor el nodo repetidor, en la figura 32 se muestra el enlace invertido, por lo tanto, cambia el azimut, esto es debido a la orientación de los sistemas y los demás datos se mantienen.

Figura 32

Área de cobertura del nodo San Luis de Guachala – Nodo repetidor



Fuente: Recuperado de Radio Mobile

Con la herramienta Radio Converge permite dibujar el área de cobertura de un enlace de radio y con la opción Single Polar se puede calcular el área de cobertura de una estación transmisora fija realizando un barrido en toda el área. En la siguiente figura 33 se muestra el área de cobertura del enlace del nodo San Luis de Guachalá – Nodo repetidor.

Comparación de datos calculados y simulación del enlace del Nodo repetidor – San Luis de Guachalá.

En la tabla 13 se describe los cálculos matemáticos y la simulación en Radio Mobile del enlace del nodo San Luis de Guachalá – Nodo repetidor.

Tabla 13

Comparación de datos calculados y simulación del enlace del Nodo repetidor – San Luis de Guachala.

Enlace Nodo repetidor – San Luis de Guachala.

Características	Datos calculados	Datos simulados	Margen de error
Perdida del espacio libre (FSL)	99,968(dB)	99,5(dB)	0.468(dB)
Ninel mínimo de señal recibida en Rx (RSL)= Ganancia total – FSL	-41.968 (dBm)	-41.1(dBm)	0.868(dBm)

Fuente: elaborado por el autor.

En la tabla 13 se describe los resultados obtenidos de los datos calculados matemáticamente y en el software Radio Mobile, existiendo un margen de error debido a que en el software determina perdidas adicionales por múltiples trayectorias y obstáculos, además que en el simulador no existe el tipo de antena LHG XL 52 ac, por los que se debe elegir una antena similar en propagación de los lóbulos de radiación que es la Antena Corner, debido a estos factores es la variación de resultados.

3.11 Diseño de la Red WLAN

Para el diseño de la red WLAN se debe tomar en cuenta el área de Cobertura el número de usuarios, concentración de puntos de calor, equipos que soporten el estándar IEEE 802.11ac, la zona de cobertura, ubicación de los equipos, anchos de banda, velocidad de transmisión, la ubicación de dichos equipos, simulaciones en un software libre y los mecanismos de seguridad que se utilizara en el diseño de la red.

El turismo se ha convertido en una de las principales actividades económicas en todos los países del mundo, sobre todo en aquellos que poseen importantes testimonios culturales, hermosos paisajes o recursos geográficos y ecológicos. Ecuador tiene una variada oferta turística de naturaleza, cultura y aventura, en un espacio de territorio bastante cómodo para visitar en períodos de tiempo cortos.

Este proyecto se propone como un complemento a otros proyectos de promoción del turismo en el cantón y toda la zona norte del país, mediante la presentación de información turística del cantón al momento de acceder al servicio de Internet gratuito en los parques y plazas de la ciudad de Cayambe en este caso la comuna San Luis de Guachalá por ser uno de los atractivos turísticos más importantes de la zona. Pero no solo servirá para promover el turismo mediante al acceso a Internet a visitantes, sino también permitirá dar servicio de Internet gratuito a los habitantes de la ciudad, y cumplir con lo que dispone el Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD) en el inciso final del Art. 363: "Los gobiernos autónomos descentralizados dotarán servicios de banda libre para el uso de redes inalámbricas en espacios públicos."

3.12 Cálculo del Área de Cobertura

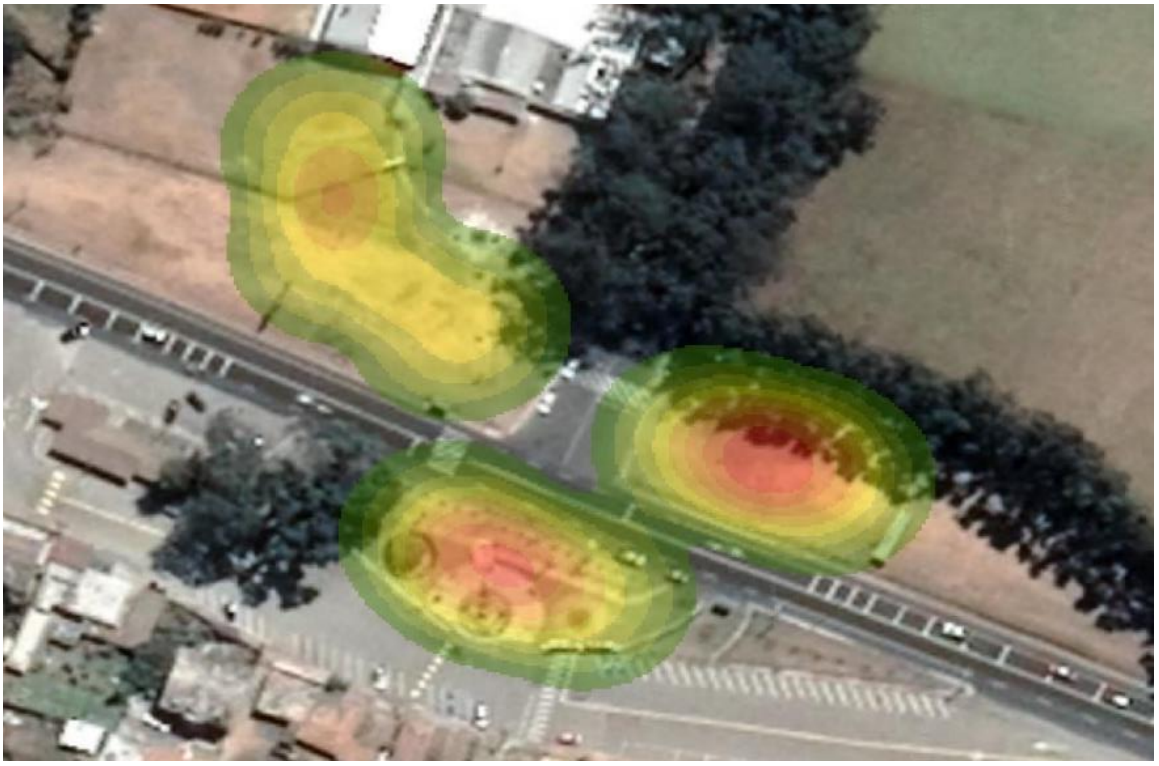
Para realizar el cálculo del área de cobertura se tomó en cuenta el número de usuarios, el cual se determinó mediante visitas de campo los días viernes, sábado y domingo, en donde se pudo observar que existen 3 puntos de mayor concentración de personas en la figura 40 se observar las 3 áreas de mayor afluencia de personas, la visita de campo permitió facilito la obtención de datos de los usuarios que harán uso del servicio, además de las estadísticas de turistas del Ministerio de Turismo. Para graficar los puntos de mayor concentración de personas se utilizará el software ArcGIS.

Para determinar la ubicación y número de equipos se realizó una simulación utilizando el software ArcGIS, utilizando los datos de la tabla del número de usuarios por zonas en donde se puede observar los puntos de mayor concentración de personas utilizando la tabla 3 del inciso 3.2.2 de población, en la figura 34 se muestra los 3 puntos

de mayor concentración en donde se ubicará puntos de acceso de alta potencia que cubran las 3 zonas mencionadas anteriormente.

Figura 334

Mapa de Calor de la Zona central Guachalá



Fuente: Elaborado por el Autor

En la figura 34 se muestra el mapa de calor se lo realizó en el programa ArcGIS en base a la afluencia de personas que visitan el lugar los fines de semana. Para ello se ingresó los datos de los puntos en coordenadas UTM en una hoja de Excel para tener más facilidad de importarlos en el programa ArcGIS y graficarlos. Lugo se utilizó la herramienta Kernel Density que se encuentra dentro de la extencion Spatial Analyst tools.

En base a este análisis del software y la visita de campo se toma la decisión de utilizar un Router de borde con 3 Access Points para cubrir las zonas de mayor afluencia.

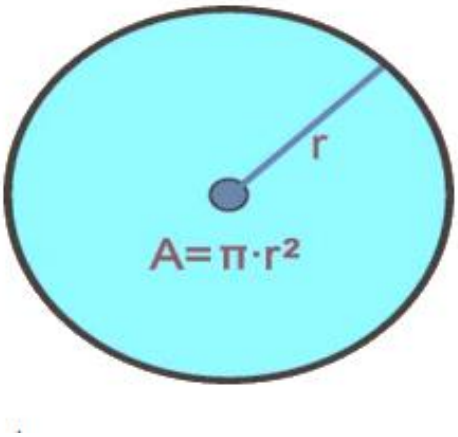
Como se puede observar en la figura anterior las 3 zonas de mayor afluencia de personas son especificas la Zona 1 es el principal atractivo por ser la mitad del mundo, la Zona 2 son las dos estatuas ubicadas en diferente hemisferio y la Zona 3 es un patio de comidas típicas del lugar.

3.12.1 Cobertura de los Access Point

Para encontrar el área de cobertura de un Access Point se debe tener en cuenta las especificaciones técnicas de una antena omnidireccional es de 30 a 60 metros, Para encontrar el área circular de la zona es como encontrara el área de un círculo donde se representa el lóbulo de radiación de una antena omnidireccional, en donde el Área es igual a la multiplicaron de Pi por el radio al cuadrado. Como se muestra en la Figura 35 a continuación.

Figura 345

Área de cobertura de un Access Point



Fuente: Kanaacademic.org

En la figura 35 se muestra la fórmula para calcular el área de cobertura de una determinada zona para el presente caso se utilizará un radio de 30 metros y un radio de 60 metros.

A= Área

r= Radio

Radio = 30 metros

$$A = \pi\, r^2$$

$$A = \pi\, (30m)^2$$

$$A = \pi\, (30m)^2$$

$$A = 2827{,}44$$

$$A = 2827m2$$

Radio = 60 metros

$$A = \pi\, (60m)^2$$

$$A = \pi\, (60m)^2$$

$$A = 11.309{,}76$$

$$A = 1.1310\text{m2}$$

3.12.2 Dimensionamiento del ancho de banda

Ancho de banda por aplicación

En el diseño de una red inalámbrica es fundamental desarrollar una planificación de red, analizando el tráfico que soportará la red, esto dependerá únicamente del ancho de banda que se requiera. Los diferentes tipos de tráficos que debe soportar la red inalámbrica son: Redes sociales Correo electrónico, Aplicaciones web, Video y audio en tiempo real.

El consumo de ancho banda para una red de invitados, correo electrónico, VoIP, navegar por Internet, música y redes sociales.

Tabla 14

Ancho de banda de aplicaciones

APLICACIONES	Ancho de Banda por usuario (kbps)	Ancho de Banda por 55 usuarios (bps)
Correo electrónico	100 kbps	5,5 Mbps
Navegación por internet	100 kbps	5,5 Mbps
Audio en tiempo real	160 kbps	8,8 Mbps
Redes Sociales	200 kbps	11 Mbps
Video en tiempo real	360 kbps	19,8 Mbps

Fuente: Recuperado de: https://www.usastreams.com/blog-streaming/1178/como-calcular-el-ancho-de-banda-que-necesito/

Estimación de Velocidad

Para determinar la velocidad aproximada que consumirá la red inalámbrica se dependerá del número de usuarios de la zona central Guachalá y valores mínimos que necesitan las aplicaciones, en la tabla 14 se analizara por ser una red abierta con un tiempo límite de conexión de 30minutos, teniendo en cuenta que cada usuario cuenta con un dispositivo móvil para conectarse a la red wifi gratuito. Para el cálculo de eficiencia de la red se tomará en cuenta los valores máximos de aplicaciones como YouTube y redes sociales por ser las más utilizadas por los usuarios actualmente, con capacidad de 200 kbps y 360 kbps respectivamente garantizando la eficiencia de la red para que el usuario pueda hacer el uso de las aplicaciones.

La velocidad total que se necesitara en la red se obtendrá multiplicando el número de usuarios por la velocidad, un valor redondeado de 55 usuarios por 360 Kbps da un

resultado de 19800 Kbps esto quiere decir que necesitara aproximadamente una velocidad de 19,80 Mbps (Megabits por segundo).

Factor de Simultaneidad

El factor de simultaneidad hace referencia al número de usuarios concurrentes intentando hacer el uso del ancho de banda, esto hace referencia a que no todos los usuarios utilizan el servicio al mismo tiempo de esta manera existe una pequeña posibilidad de que los usuarios utilicen el mismo servicio simultáneamente, por lo que se debe dimensionar la capacidad de los servicios en base a este factor.

El factor de simultaneidad expresa que proporción de usuarios utilizarán el servicio al mismo tiempo, y se determina con la siguiente formula: 1/n, donde n es el número de usuarios simultáneos. El factor de simultaneidad se utiliza con el mismo objeto de determinar la proporción de usuarios que acceden al servicio simultáneamente, sin embargo, en algunos casos se expresa de distintas formas.

$VT = VTT\ x\ Factor\ de\ simultaneidad$

VT: Velocidad del factor de simultaneidad.

VTT: Velocidad total de la red.

VT = 19,80Mbps x 30%

VT = 5,94 Mbps $Mbps$

Distribución de ancho de banda a la red WLAN

La distribución del ancho de banda para la zona Central Guachalá se realizará de manera dinámica para poder ocupar todo el recurso de red de una manera eficiente, se ha optado por realizar esto porque anteriormente basándose en el factor de simultaneidad existe una baja probabilidad del 30% de que todos los usuarios utilicen la red al mismo tiempo, al ser usuarios casuales.

El ancho de banda necesario para este punto es de 19Mbps, este será distribuido entre los usuarios que se conecten a esta zona para brindar el acceso a internet, el cual se irá dividiendo de acuerdo con el número de usuarios que se conecten, esto quiere decir que los 55 usuarios establecidos accederán eventualmente al servicio y harán uso de diferentes aplicaciones

3.12.3 Frecuencias y Canales para la red WLAN

El estudio de frecuencias es un factor importante, ya que a través de ésta se optimiza el rendimiento de la red, permitiendo la reutilización de frecuencias y disminución de interferencias.

Para la conexión inalámbrica de los usuarios a la WLAN y la interconexión de los nodos se utilizará el estándar IEEE 802.11 ac, más conocida como Wi-Fi 5G. Esta tecnología se presenta como una de las mejores opciones para la transmisión de datos en forma inalámbrica debido a las ventajas que ofrece, como son:

Uso de bandas de frecuencia sin licencia en 2,4 y 5 GHz con ciertas limitaciones de potencia.

Velocidades desde 1 hasta 600 Mbps, siempre teniendo en cuenta que el rendimiento neto obtenido está alrededor de un 50-70% de esos valores.

Tecnología con estándar ampliamente conocido y fácil de configurar, lo que favorece los bajos costos de los equipos y disponibilidad en el mercado.

La mayoría de los dispositivos (portátiles, teléfonos inteligentes, tablets, etc.) vienen equipados con tecnologías IEEE 802.11b, IEEE 802.11g y/o IEEE 802.11n, que utilizan la banda de frecuencias 2,4 GHz y son compatibles entre sí. Para el acceso de los usuarios a la WLAN se usará IEEE 802.11b/g/n en 2,4 GHz. Los equipos que trabajan en la banda de los 2,4 GHz, tienen 11 canales disponibles. Sin embargo, cada canal superpone al canal adjunto por lo que solamente se tienen tres de ellos que no se superponen.

En 5 GHz hay menos ruido e interferencias y mucho más espacio disponible en esta banda, lo que permite hasta 13 canales inalámbricos no superpuestos. Además, en IEEE 802.11n con canales de 40 MHz se puede transmitir muchos más datos, por lo que se usará IEEE 802.11ac en 5 GHz

En la tabla 15 se enlistan los canales disponibles en 2,4 GHz y 5 GHz para nuestro País.

Tabla 15

Canales disponibles en 2,4 GHz

Número de canal	Frecuencia (GHz)
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457

11	2,462

Fuente: Elaborado por el Autor

Tabla 16

Canales disponibles en 5 GHz

Banda	Número de canal	Frecuencia (GHz)
U-NII 1	36	5,180
	40	5,200
	44	5,220
	48	5,240
U-NII 2	52	5,260
	56	5,280
	60	5,300
	64	5,320
U-NII 3	149	5,745
	153	5,765
	157	5,785
	161	5,805
5.8 ISM	165	5,825

Fuente: Elaborado por el Autor

3.12.4 Distribución de canales

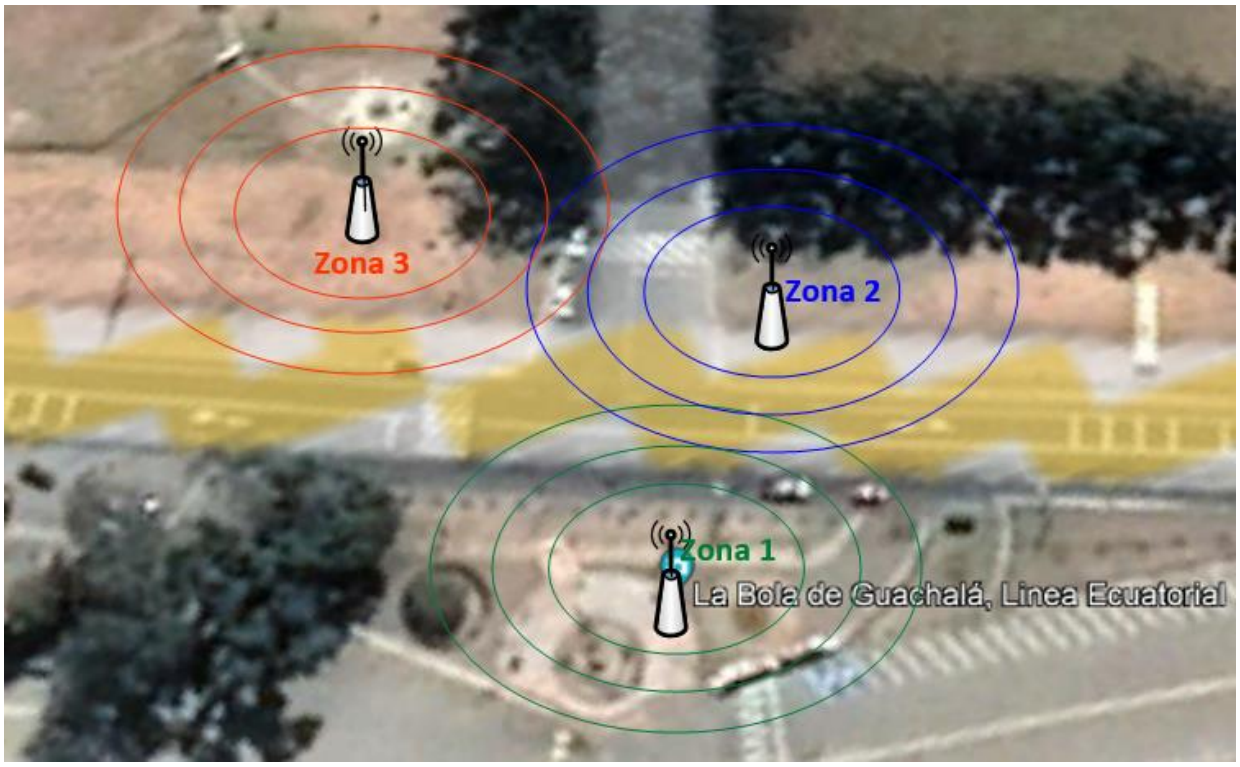
En la implementación de redes inalámbricas para que no exista interferencias en la comunicación por los mismos dispositivos se considera la configuración de canales específicos de trabajo 1, 6 y 11 en base a la distribución de los puntos de acceso con la finalidad que no exista problemas con el solapamiento de señales generando problema en los usuarios al querer hacer uso del internet.

En la Figura 36 se muestra la ubicación de Access Point y la descripción para diferenciar los diferentes canales de propagación que se configurara en cada uno de los Aps de acuerdo con el análisis de cobertura realizado.

- 2,4 GHz Canal 1 (Color Verde)
- 5 GHz Canal 36 (Color Verde)
- 2,4 GHz Canal 6 (Color Azul)
- 5 GHz Canal 52 (Color Azul)
- 2,4 GHz Canal 6 (Color Naranja)
- 5 GHz Canal 149 (Color Naranja)

Figura 35

Ubicación de Access Point



En la figura 36 se muestra la ubicación de los Access Point por canal en donde el primer AP corresponde a la zona 1 el cual se asignó el canal 1 en la banda de 2,4 GHz y en la banda 5GHz el canal 36, el segundo AP corresponde a la zona 2 el cual tiene asignado el canal 6 en la banda de 2,4 GHz y en la banda 5GHz el canal 52 y el tercer AP corresponde a la zona 3 que tiene asignado el canal 11 en la banda de 2,4 GHz y en la banda 5GHz el canal 149 respectivamente, esta distribución se hace con el fin de que no exista solapamiento de canales en los Aps mejorando el diseño de la red inalámbrica en la zona central de Guáchala.

3.12.5 Distribución de canales de los Aps

Tabla 17

Distribución de canales

# de AP	Nombre	Ubicación	Canal 2,4 GHz	Canal 5 GHz
AP 1	Alcaldía GADIP Cayambe	Monumento Mitad del mundo	1	36
AP 2	Alcaldía GADIP Cayambe	Patio de Comidas	6	52
AP 3	Alcaldía GADIP Cayambe	Estatuas - Reloj Solar	11	149

Fuente: Elaborado por el Autor

En la tabla 17 se muestra un resumen de la información mencionada anteriormente la asignación del nombre de AP, la ubicación y los canales tanto en la banda de 2,4 GHz y 5GHz.

3.13 Selección de Equipos para red WLAN

3.13.1 Selección de Access Point

Para garantizar la cobertura del área se debe elegir la mejor opción, hacer una comparativa de diferentes marcas de antenas y elegir la que mejor se acople a las necesidades del lugar. A continuación, se muestra una tabla 18 donde se hace la comparativa de Access Point antenas.

Tabla 18

Comparación de Access Point antenas

Criterios	Tp-link	Ubiquiti UniFi	Linksys
Modelo	EAP225-Outdoor	UAP-AC-M PRO	LAPAC1300CE
Estándar 802.11ac	Si	Si	Si
Banda de Operación	2.4-5GHz	2.4-5GHz	2.4-5GHz
Antenas	2.4GHz: 2x3dBi 5GHz: 2x4dBi	Triple Polaridad Antena Dual Band 3dBi	2.4G:5.17dBi 5G: 5.17dBi
Interfaz	1x Gigabit Ethernet Port	Ethernet 10/100 Mbps	1x Gigabit (PoE In)
Velocidad de transmisión	1200 Mbps 1167 Mbps	1750 Mbps	1300 Mbps
Consumo de energía	10.5W	9W	10W
Material	plástico	Plástico	Plástico
Compatibilidad	Si	Si	Si
Número de clientes	60	200	50
Alcance	200 metros	183 metros	
Precio Ecuador	109	379	279
Foto			

Fuente: Elaborado por el Autor

Se toma como mejor opción el Access Point Tp-Lik EAP225-Outdoor por tener las mejores características que se ajustan al rango y cantidad de usuarios simultáneos según el estudio de número de usuarios visto en el inciso 3.2.2, además del coste económico.

Tplink- EAP225-Outdoor

El Access Point AC de Tp-link ofrece una red Wi-Fi de alto rendimiento, seguridad avanzada, costo asequible, garantiza una velocidad y cobertura óptimas, ofrece una conexión estable es la solución ideal para ambientes residenciales como empresariales donde se conectan múltiples dispositivos al mismo tiempo. A continuación, en la tabla 19 se describe las características principales.

Tabla 19

Características principales

Característica	Especificación
Estándares Inalámbricos	IEEE 802.11a/b/g/n/ac
Frecuencia	2.4GHz, 5GHz
Potencia de Transmisión	CE: <20 dBm (2.4 GHz, EIRP), <27 dBm (5 GHz, EIRP) • FCC: <23 dBm (2.4 GHz), <22 dBm (5 GHz)
Tensión de entrada soportada	8 V - 30 V
Funciones Inalámbricas	Multiple SSIDs（Up to 16 SSIDs, 8 for each band） Enable/Disable Wireless Radio Automatic Channel Assignment Transmit Power Control （Adjust Transmit Power on dBm） QoS(WMM) MU-MIMO Airtime Fairness

Beamforming
Band Steering
Load Balance
Rate Limit
Reboot Schedule
Wireless Schedule
Wireless Statistics based on SSID/AP/Client

Fuente: Elaborado por el Autor

3.13.2 Selección del equipo de enrutamiento

El enrutador es uno de los componentes esenciales de la red y la elección adecuada ayudara a garantizar que la red ofrezca un servicio rápido, confiable y que se adapte a las necesidades del usuario. En la siguiente tabla 20 se muestra las características del enrutador

Tabla 20

Características del enrutador

Característica	Mikrotik	Mikrotik
Modelo	RB750Gr3	RB rb941
CPU	MT7621A	QCA9533
Memoria RAM	256 RAM y 16M Flash	32 RAM y 16M Flash
Puertos	5 puertos 10/100/1000	4 puertos 10/100
Sistema operativo	RouterOS	RouterOS
Consumo de energía	5W	3.5W
Dimensiones	113 x 89 x 28 mm	113 x 89 x 28 mm
Temperatura	-40°C a 60°C	-40°C a 60°C
Precio	$59.95	$24.95

Fuente: Elaborado por el Autor

Los enrutadores Mikrotik están especializados en interconectar redes con distinto prefijo en su dirección, su función es establecer la mejor ruta de los paquetes en la red. El Municipio de Cayambe viene trabajando con estos equipos mucho tiempo y certifican la operatividad y confiabilidad de esta marca.

Router MikroTik RB750Gr3

El MikroTik RB750Gr3 es un enrutador Gigabit Ethernet de cinco puertos para ubicaciones donde no se requiere conectividad inalámbrica. El dispositivo tiene un puerto USB de tamaño completo. Esta nueva revisión actualizada además de traer varias mejoras en el rendimiento. Es asequible, pequeño y fácil de usar, pero al mismo tiempo viene con una CPU dual core de 880 MHz muy potente y 256 MB de RAM, capaz de todas las configuraciones avanzadas que admite RouterOS. Mikrotik, s.f.)

Se admite el cifrado de hardware IPsec (~ 470 Mbps) y el paquete de servidor The Dude, la ranura microSD proporciona una velocidad de lectura y escritura mejorada para el almacenamiento de archivos y Dude. (Mikrotik, s.f.).

Figura 367

Equipo de enrutamiento Router RB750Gr3

Fuente: https://mikrotik.com/product/RB750Gr3#fndtn-gallery

En la figura 37 se muestra el equipo a utilizar como Router de borde en la red inalámbrica Wlan de la zona central de San Luis de Guachalá este dispositivo conectara la topología de enlaces y la red wlan además de funcionar como un Hostpot el cual controla el acceso de los usuarios.

Tabla 21

Características principales de Router.

Característica	Especificación
Frecuencia nominal de la CPU	880 MHz
Numero de núcleos CPU	Dual Core
Tamaño de RAM	256 MB
10/100/1000 puertos Ethernet	12
Número de puertos USB	1 tipo A
Tarjetas de memoria	1
Conector de alimentación	1
Tensión de entrada soportada	8 V - 30 V
Dimensiones	113x89x28mm

Sistema operativo	enrutador OS
Monitor de Voltaje	Sí
Monitor de temperatura de la CPU	Si
Sistema operativo	RouterOSv6 (64 bits)
Temperatura ambiente probada	-40°C + 60°C
Consumo máximo de energía	10W
Arquitectura	MMIPS

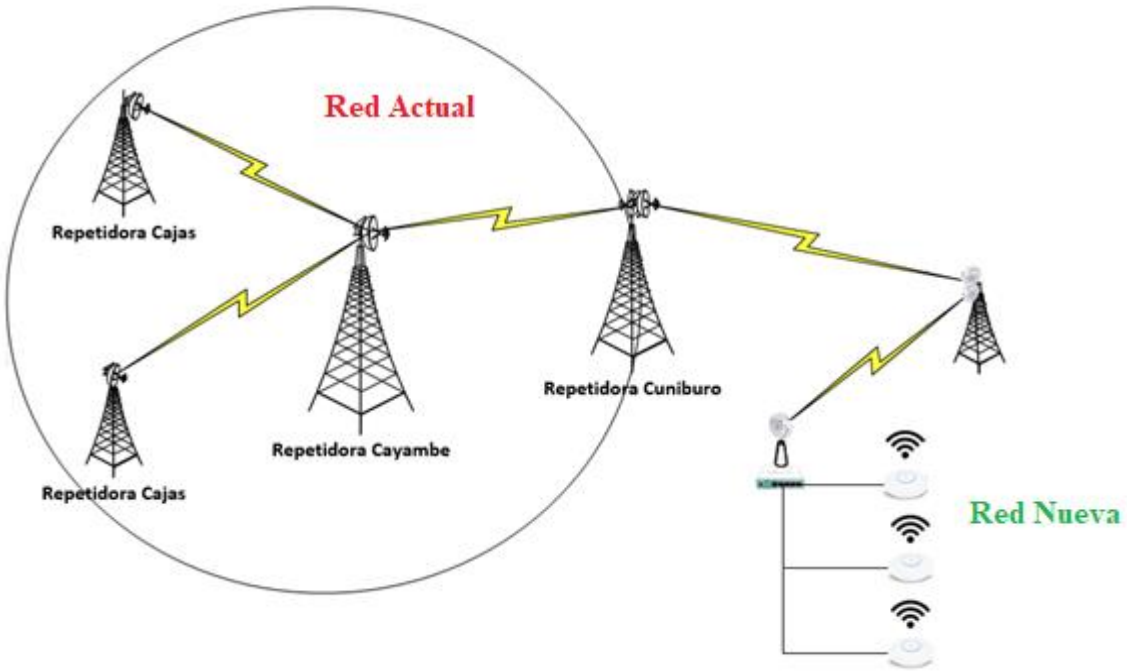
Fuente: Elaborado por el autor

En la tabla 21 se describe las características principales de Router.

3.14 Topología de la red Inalámbrica

Figura 378

Topología de la red Wlan



En esta topología se indica los equipos que se utiliza para la red inalámbrica como se puede observar en la figura 38, el portal cautivo Hotspot se encuentra configurado en el Router de borde en el nodo ubicado la comuna San Luis de Guáchala el cual tiene 5 puertos Ethernet 1 puerto Wan conectado a la antena receptora que se conecta al GADIP del Municipio de Cayambe, 3 puertos ethernet unidos en un Bridge a los puntos de acceso y un puerto libre para la red en caso de ser necesario, todos los equipos serán configurados con una dirección ip estática y ubicado en la un punto estratégico en la zona central de Guáchala, para los enlaces se utiliza antenas direccionales Mikrotik RBLHGG-5HPacD2HPnD que trabajan en la banda de 5GHz.

En la zona central de Guáchala se ubicarán 3 Access Point Tplink- EAP225-Outdoor mediante el cual el usuario final se podrá conectar a la red inalámbrica utilizando ya sea Tablet, laptops o teléfonos inteligentes.

3.14.1 Direccionamiento de los equipos de los enlaces

Tabla 22

Direccionamiento de los equipos de los enlaces

Enlace	Equipo	Dirección Ip	Mascara	Gateway
Cuniburo - Repetidor	Antena Mikrotik RBLHGG-5HPacD2HPnD	10.10.10.1/30	255.255.255.252	10.10.10.2
	Antena Mikrotik RBLHGG-5HPacD2HPnD	10.10.10.2/30	255.255.255.252	10.10.10.1
Repetidor-Guachalá	Antena Mikrotik RBLHGG-5HPacD2HPnD	10.10.10.5/30	255.255.255.252	10.10.10.6
	Antena Mikrotik RBLHGG-5HPacD2HPnD	10.10.10.6/30	255.255.255.252	10.10.10.5

Fuente: Elaborado por el autor

3.14.2 Direccionamiento de la red Wlan

Se estima tener 55 usuarios conectados a la red, 4 equipos para la comunicación de la red inalámbrica un router de borde y 3 Access Point, en base a esto se configurará los equipos utilizando un rango de Ips privadas de clase tipo C, esta distribución tiene 253 Ips disponibles, escalable a un futuro en caso de ser necesario.

192.168.10.0 Clase C: 255.255.255.0

Tabla 23

Direccionamiento Ip de la red Wlan.

Equipo	Dirección Ip	Mascara	Gateway
Portal Cautivo	192.168.10.1/24	255.255.255.0	192.168.10.1
TP-LINK-EAP225-Outdoor	192.168.10.2/24	255.255.255.0	192.168.10.1
TP-LINK-EAP225-Outdoor	192.168.10.3/24	255.255.255.0	192.168.10.1
TP-LINK-EAP225-Outdoor	192.168.10.4/24	255.255.255.0	192.168.10.1

Fuente: Elaborado por el autor

Las direcciones Ip se asignarán mediante DHCP desde la subred 192.168.10.10 hasta la 192.168.10.254.

3.15 Seguridad

La seguridad es indispensable en una red inalámbrica para la protección a los usuarios ofreciendo una conexión estable, confiable y segura. Al ser una conexión pública se debe enfocar en asegurar el correcto consumo de ancho de banda, proporcionar información de conectividad mediante una página de bienvenida y restricción de acceso a ciertos contenidos. Para esto se lo hace mediante un Hostpot.

Los requerimientos mínimos para la administración, gestión de red inalámbrica y usuarios se pueden observar en la tabla 23 siendo los siguientes

Tabla 24

Requerimientos mínimos para la administración

Requerimientos	Características

Sin autenticación de usuarios	Por ser una red inalámbrica para espacios públicos, se debe permitir que los usuarios se conecten por medio de un portal cautivo, donde se configure una página de bienvenida, la cual indique cuáles son los términos y condiciones para poder tener acceso al servicio que se va a ofrecer
Monitoreo y administración en tiempo real	Poder realizar configuraciones en tiempo real, monitorear el consumo de ancho de banda
portal cautivo	un portal cautivo para administrar el tiempo de conexión de los usuarios y el ancho de banda, ambos contenidos en la misma plataforma, para ahorrar recursos.
Fácil manejo	El GADIP Cayambe cuenta con un departamento de TICs, por esta razón se debe gestionar sin ningún problema la red y administrar para que la persona encargada de manejar la seguridad de la red pueda realizar sin ningún problema

Fuente: Elaborado por el autor

Para la para el sistema de seguridad se utilizó un Hotspot de la en la plataforma Mikrotik, esta plataforma cuenta con un host incluido el cual ayudará a la administración de los usuarios

3.15.1 Portal Cautivo

El portal cautivo permite forzar la autenticación de los usuarios redirigiéndolos a una página especial de autenticación o para aceptar los términos de uso, para poder tener acceso a la red. El portal cautivo es usado comúnmente para control de accesos a la red en los puntos de accesos inalámbricos de los, restaurantes, parques, y lugares turísticos.

Las características que Hotspot ofrece para la implementación de portales cautivos son:

Limitar el número de conexiones concurrentes de una misma IP, para evitar denegación de servicio por clientes que envían tráfico repetidamente sin autenticación.

Desconexión de usuarios que se mantienen inactivos por un número de minutos predefinidos.

Redirección de URL, para llevar a los usuarios a una página predefinida antes, durante y después de la autenticación.

CAPITULO IV

Implementación del Modelo de Gestión

En este capítulo se implementa el modelo de Gestión planteado y la herramienta de software escogida en el cuadro comparativo realizado en el capítulo III. Se aplica el protocolo SNMP v2, en el cual verificara su funcionamiento.

4.1 Establecimiento de las políticas de gestión de la red.

Se determina las políticas de gestión necearías basadas en las áreas funcionales del modelo FCAPS de la ISO que requiera el GADIP del Municipio de Cayambe de acuerdo con los requerimientos establecidos en el diseño de la red inalámbrica en el capítulo anterior.

4.1.1 Introducción

Una vez realizado el diseño de la red inalámbrica se realiza un análisis de la red para determinar las políticas de gestión que cubran las áreas Funcionales establecidas por el Modelo de Gestión FCAPS y en base a las necesidades de la nueva red diseñada, adaptar nuevas políticas al GADIP Cayambe; permitiendo el monitoreando constante, supervisión y control de los recursos existentes que brindaran el servicio de internet a la zona central Guachalá.

Las políticas que se establecerán a continuación no pertenecen a ninguna norma obligatoria es una guía que será utilizada por el administrador y las personas que están a cargo de la red inalámbrica, quienes con la ayuda del software de gestión implementado (Subcapítulo 3.20), cumple la función de mantener el correcto funcionamiento de la red cubriendo las áreas funcionales del Modelo FCAPS de la ISO, optimizando recursos y garantizando la disponibilidad del servicio a los usuarios.

4.1.2 Políticas de gestión para la red inalámbrica.

GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE		
POLÍTICAS DE GESTIÓN PARA LA RED INALÁMBRICA		
	**Versión:**	1.0.0
	Revisado por:	Ing. Daniel Veloz Administrador de la red Ing. Ronny Carbajal Jefe del Área de Hardware Y Software
	Aprobado por:	Ing. Cristian Peña Director del Departamento TIC's
	Desarrollado:	Andres Acero

1 Propósito

El propósito de este documento tiene el propósito de dar a conocer las políticas de gestión las que deberán ser atendidas por el administrador y personal a cargo de la red inalámbrica del departamento de las TIC's del GADIP Cayambe, con el fin de actuar ante eventos inesperados en la red inalámbrica, con el objetivo de mantener una red totalmente disponible, con un servicio de calidad y continuo hacia los usuarios.

2 Conceptos preliminares

- **Administración y Gestión de la Red Inalámbrica**

La Gestión de la red inalámbrica tiene como objetivo garantizar la operabilidad de la red utilizando mecanismos de software y hardware

- **Políticas de Gestión**

3 Generalidades

4 Niveles Organizacionales

- **Director de las TIC'S**

Autoridad del departamento de tecnología de información personal de nivel superior a cargo de la administración y toma de decisiones respecto a aprobación de políticas de gestión junto al encargado de la infraestructura de la red.

- **Infraestructura Tecnológica**

Autoridad encargada del área de redes de telecomunicaciones, manipulación y configuración de los dispositivos de la red inalámbrica, toma de decisiones en caso de no estar la autoridad de nivel superior para solucionar algún problema que ocurra en la red.

- **Soporte Técnico**

Personal encargado de la parte de software y hardware de la red del GADIP Cayambe, persona encargada de la toma de decisiones cuando sea requerido en la red.

- **Usuarios**

Los usuarios hacen referencia a las personas que tienen acceso los servicios brindados por la red inalámbrica como es el acceso al servicio de Internet.

5 Vigencia

El presente documento se de la administración y gestión de la red inalámbrica tendrá validez una vez sea aprobado por el administrador de la red, una de las autoridades del GADIP Cayambe. Este procedimiento deberá ser revisado y renovado según las exigencias de la entidad antes mencionada, de ser necesario realizar cambios en la infraestructura tecnológica de la red.

6 Referencia

Para la realización de este documento se toma en cuenta un formato a existente de proyectos anteriores (Torres Linda 2015 págs. 50-59) y al no haber un estándar definido

para la realización de las políticas de gestión se realizará en base a las áreas funcionales del modelo FCAPS de la ISO

1. **Política de Gestión de la Red Inalámbrica.**
    1.1. Objetivo de la Política de gestión.
    1.2. Compromiso de las Autoridades.
2. **Gestión de Fallos**
    2.1. Manejo de Fallos
    2.2. Envió de notificaciones
3. **Gestión de Configuración**
    3.1. Ingreso de Equipos
    3.2. Configuración de equipos
4. **Gestión de Contabilidad**
    4.1. Reportes
5. **Gestión de Prestaciones**
    5.1. Parámetros de Monitoreo
    5.2. Recopilación Datos estadísticos
6. **Gestión de Seguridad**
    6.1. Acceso al software de Monitoreo
    6.2. Acceso a los dispositivos de red
    6.3. Seguridad Portal Cautivo

7 Términos y Definiciones

GADIP Cayambe: Gobierno Autónomo Descentralizado Intercultural Plurinacional del Cantón Cayambe, encargado de promover el desarrollo económico, social, medio ambiente y cultural dentro de su jurisdicción.

Departamento TIC's: Departamento de Tecnología Información y Comunicación, encargado del desarrollo de tecnología dentro del GADIP Cayambe.

Red inalámbrica: La red Inalámbrica es la conexión de nodos que se da por mediode ondas electromagnéticas, sin necesidad de una red cableada o alámbrica. La transmisióny la recepción se realizan a través de puertos.

Dispositivos de red: Es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red.

SNMP: El Protocolo Simple de Administración de Red o (Simple Network Management Protocol) es un protocolo de la capa de aplicación TCP/IP que facilita el intercambio de información de administración entre dispositivos de red.

Fallo: Evento ocurrido en cualquier momento donde se genera un inconveniente o dañoen la red, donde el desempeño de la red reduce.

Notificación: Es usado por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación al NMS.

Reportes: Un reporte es un informe o una noticia. Este tipo de documento (que puede ser impreso, digital, audiovisual, etc.) pretende transmitir una información, aunque puede tener diversos objetivos.

Estadísticas: Se dedica a la descripción, visualización y resumen de datos. Los datos pueden ser resumidos en numérica o gráficamente.

Lineamientos: Leyes que se deben registrar los usuarios para un perfecto funcionamiento de la red inalámbrica.

Desarrollo de Políticas de Gestión para el GADIP del Municipio de Cayambe

<table>
<tr><td colspan="4"> 
</td></tr>
<tr><td>DOMINIO</td><td>1. Política de Gestión de la red inalámbrica</td><td>DESTINATARIO</td><td rowspan="2">Administrador y Usuarios</td></tr>
<tr><td>CONTROL</td><td colspan="2">1.1. Objetivo de las políticas de Gestión</td></tr>
</table>

Política. 1: Presentar la información necesaria sobre los requisitos necesarios para el buen desempeño de la red inalámbrica, al administrador y personal encargado de la administración de la red del GADIP Cayambe, determinando cualquier tipo de problema y dar solución en el menor tiempo posible a cualquier problema.

Política. 2: Relacionar la información necesaria al personal que aceden a los servicios de la red inalámbrica para su correcto funcionamiento.

Política. 3: Brindar a información necesaria con sus respectivas recomendaciones a los encargados de los equipos en los nodos de cliente final.

Para el cumplimiento de estos artículos, los formatos para documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.4 de este documento.

DOMINIO	1. Política de Gestión de la red inalámbrica	DESTINATARIO	Administrador y Usuarios
CONTROL	1.2. Compromiso de las Autoridades		

Política. 4: El Departamento de Tecnologías y Comunicación (TIC's) del GADIP del Municipio de Cayambe, como administrador de toda la red inalámbrica e inventor de las políticas de gestión aplicables, es responsable de monitorear y socializar los parámetros descritos en este documento para garantizar su correcto funcionamiento.

Política. 5: Los usuarios y beneficiarios de los servicios de las redes inalámbricas deben seguir las recomendaciones pertinentes del Departamento de Tecnología y Comunicaciones (TIC´s) del GADIP Municipio de Cayambe.

Para el cumplimiento de estos artículos, los formatos para documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.4 de este documento.

DOMINIO	2. Gestión de Fallos	DESTINATARIO	Administrador y Personal encargado
CONTROL	2.2. Manejo de Fallos		

Política. 6: Cuando ocurre una falla en una red inalámbrica, el administrador o responsable de administrar la red debe detectar la falla en el sistema de gestión para luego aislar y diagnosticar lo sucedido, posteriormente solucionarlo.

Política. 7: Ante la falla dentro de la red inalámbrica, el administrador o la persona responsable de la gestión debe encontrar la falla en el sistema de gestión, hacer una selección específica del problema que ha ocurrido y luego aislarlo. Corrigiendo el problema en el menor tiempo posible según los procedimientos que se basan en el manual de gestión de fallas.

Para el cumplimiento de estos artículos, los formatos para documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.4 de este documento.

GADIPCayambe SUMAK KAWSAYPAK
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE

DOMINIO	3. Gestión de Configuración	DESTINATARIO	Administrador
CONTROL	3.1. Ingreso de equipos		

Política. 8: Todos los dispositivos integrados en la red inalámbrica, sus funciones básicas deben ingresarse en la base de datos (Excel), lo que ayudará al administrador a encontrar fácilmente los dispositivos y operarlos.

Política. 9: Para el ingreso de los equipos a la base de datos se utilizará la nomenclatura establecida por el Departamento de Hardware y Comunicaciones del GADIP-Cayambe.

Para el cumplimiento de estos artículos, los formatos para documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.4 de este documento.

GADIPCayambe SUMAK KAWSAYPAK
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE

DOMINIO	3.Gestión de Configuración	**DESTINATARIO**	Administrador
CONTROL	3.2. Configuración de equipos		

Política. 10: Los equipos que se integrarán en la red inalámbrica debe tener una configuración básica que les permita operar en el entorno de red y realizar el rol asignado al administrador.

Política. 11: Un dispositivo que forma parte de una red inalámbrica, si es compatible con SNMP, debe ser configurado con las instrucciones apropiadas para ser completamente administrado.

Política. 12: Para monitorear el correcto funcionamiento de la red inalámbrica, cuando se realizan cambios o configuraciones a los equipos de la red, se debe actualizar la base de datos de información.

Política. 13: La persona responsable debe traer la documentación de la configuración inalámbrica existente.

Política. 14: Los administradores de redes inalámbricas deben realizar una copia de seguridad de la aplicación de administración cada 6 meses o cada vez que se realicen cambios para proteger el sistema en caso de pérdida o mala configuración.

Para el cumplimiento de estos artículos, los formatos para documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.4 de este documento.

DOMINIO	4. Gestión de contabilidad	DESTINATARIO	Administrador y personal encargado
CONTROL	4.1. Parámetros de monitoreo		

Política. 15: Los dispositivos de red inalámbrica monitoreados deben mostrar parámetros, al menos recursos y servicios locales, para demostrar su correcto funcionamiento.

Política. 16: Depende de la función del dispositivo que realices en él. En una red inalámbrica, los servicios y recursos se asignan en función del estado operativo actual del dispositivo.

Política. 17: El GADIP-Cayambe es una organización sin fines de lucro, por lo que este proceso no toma en cuenta la facturación por los servicios que brinda.

Para el cumplimiento de estos artículos, los formatos para documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.4 de este documento.

DOMINIO	5. Gestión de Prestaciones	DESTINATARIO	Administrador y personal encargado
CONTROL	5.1. Reportes		

Política. 18: Todos los reportes e informes se imprimen con la información solicitada por el administrador y con los requerimientos de la institución.

Política. 19: El software de administración The dude le permite monitorear su red inalámbrica con informes de estado diarios, mensuales y anuales.

Política. 20: Al final de cada mes, los administradores deben proporcionar un informe que confirme la disponibilidad de equipos y servicios.

Para el cumplimiento de estos artículos, los formatos para documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.4 de este documento.

DOMINIO	5. Gestión de Prestaciones	DESTINATARIO	Administrador y personal encargado
CONTROL	5.2. Monitoreo de trafico de red		

Política. 21: El rendimiento de los recursos y servicios utilizados por cada dispositivo que forma parte de la red inalámbrica se muestra en gráficos que muestran estadísticas e historial de su estado actual.

Política. 22: El ancho de banda de la interfaz se presentará en bit/s en la historia gráfica comparativa de transmisión y recepción

Para el cumplimiento de estos artículos, los formatos para documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.4 de este documento.

DOMINIO	6. Gestión de Seguridad	DESTINATARIO	Administrador y personal encargado
CONTROL	6.1. Acceso al Software de Gestión		

Política. 23: Las visitas al sistema de gestión solo se utilizarán para la responsabilidad de la gestión de redes inalámbricas.

Política. 24: El software de gestión permite 3 tipos de derechos de acceso al software, derechos de monitor write y derechos de administrador, dichos usuarios se clasifican según los procesos que cada persona puede realizar en el sistema de gestión a través del acceso remoto.

Política. 25: El encargado del monitoreo debe asegurarse de que el monitor de administración esté siempre activo para la administración continua de los dispositivos de red.

Para el cumplimiento de estos artículos, los formatos para documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.4 de este documento.

DOMINIO	6. Gestión de Seguridad	DESTINATARIO	Administrador y personal encargado
CONTROL	6.2. Acceso a los dispositivos de red		

Política. 26: Para cambiar o actualizar la configuración de los dispositivos de red, el acceso está limitado al administrador, de lo contrario, los cambios o actualizaciones correspondientes requieren la autorización del administrador.

Política. 27: El responsable de los equipos instalados en cada punto de la red inalámbrica. Al igual que la casa de Pilar, su centro de salud, etc., deben ser conscientes de su propia seguridad y poder implementar procesos para resolver problemas cuando sea necesario.

Para el cumplimiento de estos artículos, los formatos para documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.4 de este documento.

DOMINIO	7. Gestión de Cumplimiento	DESTINATARIO	Administrador y personal encargado
CONTROL	7.1. Cumplimiento de políticas		

Política. 28: Para eliminar los inconvenientes en el menor tiempo posible y brindar servicios de calidad al público, se debe seguir el manual de procedimientos que ofrece la red inalámbrica.

Política. 29: El departamento TIC será responsable de monitorear el cumplimiento de las políticas y lineamientos institucionales.

Para el cumplimiento de estos artículos, los formatos para documentación se encuentran detallados en el manual de gestión de configuraciones del subcapítulo 4.4 de este documento.

4.2. Comparación de tipos de Software para el monitoreo de gestión

Se realiza un estudio comparativo entre software de gestión de redes inalámbricas para determinar el mejor software en base a las características técnicas y específicas de cada software, permitiendo implementarlo como herramienta para el proyecto propuesto en base al estándar ISO / IEC / IEEE 29148-2018.

El software de monitoreo de red es un sistema integrado de monitoreo y análisis de red e infraestructura que proporciona monitoreo general de dispositivos de red (conmutadores, enrutadores, firewalls, puntos de acceso, etc.), representación gráfica y topológica de la infraestructura y análisis del consumo de tráfico de red.

En el medio hay innumerables tipos de software que tienen diferentes características y brindan diferentes servicios. Este documento realizará un análisis comparativo de los tres softwares de gestión para satisfacer completamente las necesidades sus herramientas sin problemas.

Para la elección del software de monitoreo donde se instalará el servidor Local que se encuentra en funcionamiento en el GADIP del Municipio de Cayambe se analizará según las especificaciones del estándar ISO / IEC / IEEE 29148-2018 y sus herramientas para cubrir las áreas funcionales del modelo de Gestión FCAPS de la ISO para administrar la red inalámbrica del GADIP Municipio de Cayambe

Tipos de software para la monitorización de la red Inalámbrica.

Se enumeran las características de los diferentes tipos de software de monitoreo de redes inalámbricas y se especifican los parámetros y requisitos de cada software de gestión.

MIKROTIK - THE DUDE

Mikrotik es un fabricante de equipos inalámbricos reconocido internacionalmente que desarrolla el software de monitoreo de redes inalámbricas The Dude, el software de monitoreo de gestión. Su licencia es gratuita, pero la funcionalidad es comparable a los productos comerciales. Se enfoca en la multitud experta en tecnología que prefiere la

facilidad de uso y una interfaz simple. Un inconveniente es la falta de alertas avanzadas y opciones de informes limitadas.

Características:

- **Sistemas operativos soportados:** Windows 10, Server 20019, (Linux, MacOS)
- **Interfaz de usuario:** La aplicación local/Los iconos del dispositivo / Representación gráfica de valores (gráfico de líneas) / árbol MIB / Tabla de valores /
  Mapas: interfaz gráfica de usuario
- **Idioma:** Español, Ingles
- **Protocolo de comunicación:** SNMP
- **MIB Manager:** Sí
- **Respuesta a la alarma:** Si
- **Local:** Reproducir un sonido, ejecutar un archivo externo, inicie sesión
- **Funciones:** Enviar un correo electrónico
- **Salida de valores:** Log (DB), gráfico (en la pantalla), los valores actuales (en pantalla)
- **Apoyo personalizado para Poseidón y Damocles:** No
- **Control de salida:** No
- **Funciones especiales:** Gestión de dispositivos WiFi por el mismo fabricante
- **Versión SW:** La v2.2 Amigo, Windows 10 Professional
- **Hardware:** Poseidon 3268, firmware ver. 3.0.1
- **Comunicación**: SNMP
- **Funciones Probado:** Adición de un dispositivo, alarma audible.

NAGIOS

Nagios es uno del software de código abierto más conocido y más utilizado para el seguimiento de las infraestructuras de TI. Nagios controla las estaciones de usuario final, servicios de TI, así como componentes de red activos. Su arquitectura es muy modular y adecuada para el despliegue en redes basadas en Multiplataforma. Hay una amplia y activa comunidad alrededor de Nagios que desarrolla muchos módulos adicionales o plug- ins.

Características:

- **Licencia:** Código abierto
- **Precio estimado:** gratuito, siempre y cuando cumpla con las condiciones de licencia
- **Sistemas operativos soportados:** Multiplataforma. NT servicio / demonio: Sí
- **Interfaz de usuario:** cliente Web
- **GUI:** Los iconos del dispositivo
- **Idioma:** ES, parcialmente personalizable
- **Protocolo de comunicación:** SNMP, SNMP Trap
- **MIB Manager:** No (sin embargo, es un componente estándar de Linux)
- **Respuesta de alarma:**
    - **Local:** Totalmente personalizable, colaboración ServiceDesk, etc.
    - **Funciones:** Totalmente personalizable
- **Notificación SMS:** Sí, mediante un componente especial
- **Salida de valores:** informes personalizables
- **Plug-ins personalizados**
- **Control de salida:** Sí
- **Funciones especiales:** Amplia gama de opciones de personalización, el apoyo para el desarrollo de componentes personalizados
- **Clientes objetivo:** Monitoreo de las redes comunitarias a gran escala
- **SW versión:** Nagios versión 3.0a3, Fedora 7 i386
- **Hardware:** Poseidon 3268, firmware ver. 3.0.3
- **Comunicación:** SNMP

- **Funciones Probado:** Adición de un dispositivo, valores que muestran

PANDORA

Pandora FMS Enterprise es un software de monitorización para empresas que le permite monitorizar desde 100 dispositivos a varias decenas de miles, unificando todos sus sistemas, redes y aplicaciones en una sola consola.

Monitorización de red unificada: A lo largo de los años hemos incorporado funcionalidades que otros fabricantes tienen en productos separados, ofreciendo bajo una única licencia un conjunto de soluciones de red homogéneo. Pandora FMS es realmente todo-en-uno.

Características

- Inventario remoto de software y licencias.
- Alta disponibilidad (HA). Gráficas de histórico hasta tres años.
- Monitorización de equipos Windows, Linux y Unix: con agentes o sin ellos.
- Polling SNMP v3 y gestión de traps SNMP completa.
- Explorador MIB integrado, con carga de MIBs personalizadas.
- Umbrales inteligentes, que aprenden de la red para autoconfigurarse.
- IPAM integrado para la gestión de direccionamiento IP (IPv4/IPv6).
- Netflow para la gestión de capacidad de la red y el rendimiento a bajo nivel.
- Sondas descentralizadas, para mayor flexibilidad y escalabilidad.
- Autodescubrimiento de redes a nivel 2 y 3.
- Detección de cambios en configuración de dispositivos de red.
- Informes avanzados de disponibilidad, SLA y gráficas de capacity planning, entre otras decenas de informes más.
- Cientos de dispositivos estándar listos para monitorizar en nuestra librería de módulos.

- Capacidad de lanzar miles de chequeos por segundo mediante sondas descentralizadas.
- Consola SSH y Telnet integrada.

Especificación de los Software basado en la estándar ISO/IEC/IEEE 29148

D2.1. Introducción

La especificación de requisitos de software ISO/IEC/IEEE 29148 permite la selección de software de acuerdo con los parámetros definidos en este estándar, lo que permitirá seleccionar el software más adecuado para el monitoreo de redes inalámbricas, de modo que el principal objetivo de rendimiento sea la gestión y el control. toda la red inalámbrica y con ello optimizar recursos y tiempo para poder brindar el soporte técnico necesario en caso de algún problema en la red.

a) Propósito.

El presente documento tiene por objeto determinar la mejor opción de la elección del software de monitoreo que se va a implementar para mejorar la gestión de la red Inalámbrica.

Este documento está dirigido a los administradores de red en GADIP del Municipio de Cayambe, se utilizará como una guía para determinar el software de monitoreo el cual debe cumplir con los requisitos operativos y de rendimiento de la red.

b) Ámbito del Sistema

El software de monitoreo de red inalámbrica utilizado brinda monitoreo de red a través del protocolo SNMP, permitiendo el acceso remoto a los puntos de acceso de cada institución, además de una conveniente administración y gestión, se generarán

notificaciones con mensajes de error enviados por el software, en caso de una falla en la red, independientemente de si está en dispositivos activos en cada configuración, los mensajes SNMP o alertas identificarán la falla, lo que determinará el nivel de error que determina la gravedad. aviso de. Una vez que se envíe este mensaje, se enviará al administrador de la red, quien notificará al software de cualquier problema. Es posible visualizar la topología de la red y las conexiones en ella.

Además, los parámetros básicos de la red inalámbrica, como la velocidad de transmisión y recepción de datos, ancho de banda, protocolo, si el dispositivo está activo, frecuencia y un gráfico que indica el espectro de radio, consumo de ancho de banda por punto de acceso.

c) Definiciones y Abreviaturas

SNMP: Protocolo simple de administración de redes. Es un protocolo que permite a los administradores de red administrar dispositivos de red y diagnosticar problemas de red.

Monitoreo: En la gestión de redes, se denomina monitoreo de redes al sistema de control continuo de las redes informáticas, que trata de detectar defectos y anomalías; si se encuentran daños, envíe un mensaje al administrador.

Protocolo: Un protocolo de red se usa en un contexto informático para nombrar las reglas y estándares que definen cómo deben comunicarse los diversos componentes de un sistema interconectado en particular. Esto significa que los dispositivos conectados a la red pueden intercambiar datos utilizando este protocolo.

IEEE.: Instituto De Ingeniería Eléctrica Y Electrónica.

Sistema operativo: Es el software básico de una computadora que provee una interfaz entre el resto de programas del ordenador, los dispositivos hardware y el usuario.

FCAPS: Siglas determinadas para describir las áreas funcionales de Fallos, configuración, contabilidad, prestaciones y seguridad del modelo de gestión de la ISO.

ISO: Responsable de coordinar el trabajo de otras organizaciones de estándares. Organización que desarrolló el modelo OSI para redes de datos.

GADIP: Descripción de la entidad Gobierno Autónomo Descentralizado Intercultural y Plurinacional.

Modelo de gestión: Reglas o procedimientos que se dan como base para mejor el entorno, tenido como objetivo principal administrar, controlar y monitorear a través de gestión en este caso la red inalámbrica.

Herramientas de gestión: Las herramientas utilizadas para el monitoreo de la red pueden variar según las necesidades del marco de implementación, por lo que pueden ser dispositivos que analizan las señales que pasan por la red o monitores.

d) Referencias

Para realizar el presente documento se ha tomado en cuenta las siguientes referencias obteniendo la información para determinar los requisitos adecuados para la selección del sistema operativo.

1. ISO/CEI/IEEE 29148:2018 Ingeniería de sistemas y software.
2. IEEE-STD-830-1998: Especificaciones de los Requerimientos del Software.
3. Castro Cuazapas , S. E., & Massa Manzanillas, A. f. (2010, Abril). Formulación de una guía metodológica para implementar una infraestructura

virtual con alta disponibilidad, balanceo de carga y backup, consecuente a un análisis y comparación de las soluciones de virtualización de servidores usando IEEE 830. CD-2856. Quito, Pichincha, Ecuador: Escuela Politécnica Nacional (Castro Cuazapas & Massa Manzanillas, 2010)

4. Ipiales Myrian (Mayo 2015) Administración de la Red Inalámbrica del Gobierno Autónomo Descentralizado de San Miguel de Ibarra a Través de la Plataforma Mikrotik Basada en el Modelo de Gestión FCAPS de la ISO.(Ipiales Myriam 2015).

e) Visión General

Este documento consta de dos partes, la primera parte incluye una introducción al software que se comparan y un análisis general de lo que se discutirá en la segunda parte, los requisitos de selección específicos describen los softwares de gestión.

4.2.1. Descripción General

El estándar IEEE-STD-830 creada en 1998 y actualizada al estándar ISO / IEC / IEEE 29148-2018 que especifica los requisitos que debe contener el software para su aplicación, permitiendo un análisis comparativo para la mejor elección software de gestión del sistema operativo que servirá de base para que la instalación del software de gestión y sus herramientas se realice en su totalidad y sin inconvenientes.

a) Perspectiva

El software de monitoreo de redes inalámbricas se puede utilizar en cualquier red con fines educativos. Es necesario implementar un sistema de control y gestión de datos en el que se pueda implementar el protocolo SNMP, que permitirá el acceso remoto a los puntos de acceso. con este

El software le permitirá obtener una imagen real de la red y cómo funciona para aumentar la eficiencia y eficacia de toda la red inalámbrica. Además, para el

cumplimiento, la eficiencia y la eficacia, genere mensajes de error para que estos mensajes generados puedan enviarse por correo electrónico a los administradores de red. Además, se deben determinar los parámetros clave de la red inalámbrica como SSID, tasa de baudios, ancho de banda y el mapa funcional que define el funcionamiento de cada parámetro.

b) Funciones

El software que se utilizara para la Administración y Gestión de la red Inalámbrica debe cumplir con las siguientes funcionalidades como son:

- Escalabilidad.
- Disponibilidad.
- Seguridad.
- Licencia.
- Interfaz de usuario
- MIB Manager
- Diseño de topología de red.
- Sistemas operativos compatibles.
- Interoperabilidad entre fabricantes y protocolos.
- Respuesta de Alarmas
- Notificaciones por correo electrónico

- Determinar los parámetros básicos de la red inalámbrica: velocidad de envío y recepción, ancho de banda, frecuencia, etc.

c) Características de los usuarios

El software de gestión que se seleccione debe ser familiar para el personal encargado de la administración que son los únicos usuarios del software de aplicación de gestión de la red inalámbrica del GADIP del Municipio de Cayambe y ser confiable y manipulable.

d) Restricciones

A El software utilizado debe ser compatible con el protocolo SNMPv2 y Managemet MIB, que define las variables que utiliza el protocolo SNMP para monitorear y controlar los componentes de la red.

Suposiciones y dependencias

- El software que se ejecuta en el sistema operativo es de uso gratuito.
- Aumento de puntos de acceso en la red.
- Reemplace el dispositivo con otro fabricante.

Requisitos Futuros

- Protocolo de acceso remoto cambiado a protocolo SNMPv3.
- Modifique el software SMS de su teléfono

4.2.2. Requerimientos específicos.

a)

REQ01: Administración

El sistema de control contará con una interfaz gráfica de fácil uso diseñada para los responsables de la gestión de redes inalámbricas con amplios conceptos informáticos.

b) Interfaz de Usuario

REQ02: Compatibilidad Sistema Operativo

El sistema operativo será totalmente compatible con la principal aplicación de gestión de proyectos actuales y sus herramientas internas.

REQ03: Compatibilidad herramientas de gestión.

El software de monitoreo además de la compatibilidad con las aplicaciones de gestión, el sistema operativo debe ser compatible con las herramientas para cubrir el alcance funcional del modelo ISO FCAPS, en este caso será compatible con la herramienta de análisis de tráfico.

REQ04: Compatibilidad software para documentación

El software de monitoreo debe admitir paquetes de documentos, por ejemplo: paquete de Office, paquete de Adobe Reader

REQ05: Soporte de Licencia

El software de gestión estará respaldado por una licencia que el dispositivo deberá garantizar su uso en caso de que no sea el sistema operativo libre.

REQ06: Soporte SNMP

El software de gestión tendrá que tener la opción de habilitar el protocolo simple de gestión (SNMP) de red para ser monitoreado y gestionado dentro de la red.

REQ07: Soporte VPN

El software de gestión admitirá y permitirá que se habiliten las redes privadas virtuales para permitir la administración remota gráfica del sistema operativo desde la administración fuera de la red local.

c) Interfaz Hardware

REQ08: Compatibilidad Hardware

El software de gestión para el monitoreo deberá ser compatible con las características físicas del Sistema Operativo.

d) Funciones

Funciones que deberá cumplir el Software de Monitoreo

REQ09: Soporte de Servidores Locales.

El software de monitoreo permitirá el correcto funcionamiento para sistemas Operativos Linux y Windows.

REQ10: Protocolo de comunicación

El software debe permitir aplicar el protocolo SNMPv2 para la comunicación con los puntos de acceso de toda la red.

REQ11: Interfaz de usuario

El software de aplicación deberá tener representación gráfica de valores (gráfico de líneas), árbol MIB, Tabla de valores, Mapas: interfaz gráfica de usuario para facilitar la visualización de la administración de la red.

REQ12: Soporte de notificaciones

El Software permitirá la habilitación del servicio de notificación de alarmas a través de notificaciones dentro de las herramientas internas de la aplicación.

REQ13: Soporte acceso remoto

El software deberá permitir el ingresar de manera remota hacia la configuración de losequipos de red.

e) Requisitos de rendimiento

REQ14: Disponibilidad.

Siempre disponible ante cualquier actualización que exista por parte del proveedor delservicio.

REQ15: Interoperabilidad

Que permita la instalación de la aplicación de gestión en diferentes plataformas paraque no existan restricciones de funcionamiento.

REQ16: Escalabilidad.

El software permita agregar complementos para mejorar las funciones del software de gestión y administración.

f) Seguridad

REQ17: Acceso

Solo el personal administrativo debe tener acceso al software de monitoreo, ya que, si se envía un error al sistema, solo los responsables de administrar la red inalámbrica pueden recibirlo.

4.2.3. Selección del software de monitoreo

La elección del software de monitoreo se determinó de acuerdo con los requisitos propuestos, con base en el estándar IEE 830 actualizado al estándar ISO / IEC / IEEE 29148-2018, para lo cual la evaluación de los requisitos, las calificaciones necesarias y

las razones para elegir el software destinado a monitorear la red inalámbrica GADIP fueron determinadas por el Municipio de Cayambe

a) Establecimiento de valorización para los requerimientos

Cuando se han determinado la elección del software de monitoreo y los requisitos establecidos para la selección, es necesaria una evaluación adecuada de estos requisitos para determinar el mejor software para monitorear la red inalámbrica del GADIP del Municipio de Cayambe.

REQ01: Administración

0 No posee interfaz grafica

1 Posee interfaz vía remota

2 Posee interfaz grafica

REQ02: Compatibilidad con el Sistema Operativo

0 No tiene Compatibilidad

1 Tiene compatibilidad con algunas herramientas

2 Tiene compatibilidad completa

REQ03: Compatibilidad de herramientas de gestión

0 No tiene Compatibilidad

1 Tiene compatibilidad con algunas herramientas

2 Tiene compatibilidad completa

REQ04: Compatibilidad de software para la documentación

0 No tiene Compatibilidad

1 Tiene compatibilidad vía remota

2 Tiene compatibilidad completa

REQ05. Soporte de licencia

0 No tiene licencia para el S.O.

1 Licencia de software libre

2 Tiene licencia para el S.O.

REQ06: Soporte SNMP

0 No permite habilitación de SNMP

1 Si permite habilitación de SNMP

REQ07: Soporte VPN

0 No permite creación de redes privadas virtual en modo gráfico (VPN)

1 Permite la creación de redes privadas virtuales no en modo gráfico

2 Si permite creación de redes privadas virtual en modo gráfico (VPN)

REQ08: Compatibilidad con el Hardware

0 No opera en equipos de baja capacidad

1 Opera en equipos de baja capacidad

REQ09: Soporte de servicios locales

0 No permite la instalación de servicios locales

1 Permite la instalación de servicios locales

REQ10: Protocolo de Comunicación

0 No se puede modificar el idioma

1 Posee pocos cambios de idiomas

2 Posee todos los idiomas

REQ11: Interfaz del Usuario

0 No posee interfaz de usuario

1 Posee interfaz de usuario

REQ12: Soporte De Notificaciones por Correo.

0 No permite la configuración para la notificación por correo electrónico.

1 Permite adición de un servidor local

2 Permite la configuración para la notificación por correo electrónico

REQ13: Soporte de Acceso Remoto

0 No permite el acceso remoto

1 Permite el acceso remoto

REQ14: Disponibilidad.

0 Tiene una disponibilidad baja con sistemas Operativos Linux y Windows

1 Tiene una disponibilidad media con Windows y Linux

2 Tiene una disponibilidad alta con Windows

REQ15: Interoperabilidad

0 No Inter-opera con otros Sistemas operativos

1 Inter-opera con otros Sistemas Operativos

REQ16: Escalabilidad.

0 Software de monitoreo no escalable

1 Software de monitoreo escalable

REQ17: Acceso

0 No tiene Acceso de Seguridad a través de contraseña

1 Si Tiene el acceso de Seguridad a través de contraseña

b) Calificación para cada solución de software de gestión

Una vez determinados los requerimientos basados en el estándar ISO / IEC / IEEE 29148-2018, y estableciendo los valores para la selección, se analiza mediante la

siguiente tabla la calificación que determinará el software de gestión ideal que cumpla los requerimientos.

Tabla 25

Tabla de calificación de los diferentes

REQUERIMIENTOS	The Dude	Nagios	Pandora
REQ01	2	1	1
REQ02	2	2	1
REQ03	2	2	1
REQ04	1	1	1
REQ05	1	1	0
REQ06	2	1	1
REQ07	1	1	1
REQ08	1	1	1
REQ09	1	2	1
REQ10	1	0	1
REQ11	1	1	1
REQ12	1	1	2
REQ13	1	1	1
REQ14	1	0	2
REQ15	1	0	1
REQ16	1	1	1
REQ17	1	1	1
TOTAL	**23**	**18**	**20**

Fuente: Elaborado por el Autor

Respecto a los requerimientos específicos del estándar ISO / IEC / IEEE 29148-2018 y la tabla 25 de comparación de los tipos de software implementados, el mejor software para el manejo y control de la red inalámbrica en el proyecto propuesto para la red inalámbrica creada a cargo del GADIP del Municipio de Cayambe, es el software THE DUDE, debido a que las instalaciones y equipos del municipio se basa en MIKROTIK, que permitirá el mejor uso posible del software y también facilitará a los empleados el uso de la herramienta porque está dirigida a personas orientadas a la tecnología en lugar de aquellas que prefieren la facilidad de uso y una interfaz simple.

El software cumple con los requisitos de implementación del proyecto propuesto, tales como notificación de mensajes por correo electrónico, comunicación remota con puntos de acceso mediante el protocolo SNMP, actualización del software según las necesidades de la red mediante complementos, identificación de los parámetros básicos de las redes, representadas mediante diagramas de líneas, donde se indican el funcionamiento y el cumplimiento con las sus áreas funcionales Áreas Funcionales del modelo FCAPS de la ISO.

4.2.4. Implementación del modelo de gestión FCAPS en la red inalámbrica

La implementación del modelo de gestión FCAPS define los requisitos de software y hardware que abarcan las 5 áreas funcionales, identificadas por sus siglas y relacionadas con el sistema de gestión; compuesto por la aplicación de gestión The Dude como principal herramienta de monitorización, conjuntamente con el software de analizador de trafico Wireshark y herramientas que soporte los equipos Mikrotik, con el fin de que se cumpla los objetivos de gestionar la red inalámbrica en su totalidad.

4.2.4.1. Requerimientos para la implementación del modelo de gestión.

Al momento de implementar un modelo de gestión se deben tener en cuenta los requerimientos a nivel de hardware y software para que la aplicación de control realice el correcto seguimiento, control y procedimientos ante cualquier situación.

4.2.4.1.1. Requerimientos a nivel de software.

La instalación del software y las herramientas de gestión tiene en cuenta la situación de la red inalámbrica como del modelo de gestión FCAPS de la ISO, ayuda con la aplicación que se describe a continuación, sigue el proceso de supervisión y realiza una gestión centralizada de las funciones de la red inalámbrica del GADIP del Municipio de Cayambe.

a) Software de Gestión The dude.

La aplicación de gestión identificada para este proyecto fue Mikrotik The Dude, que fue el principal monitor de gestión con los siguientes aspectos esenciales:

- La mayoría de los dispositivos disponibles en la red inalámbrica son marcas Mikrotik compatibles.
- La aplicación proporciona acceso remoto centralizado a cada dispositivo utilizando sus herramientas integradas, asegurando un control y monitoreo continuo.
- Manipulación de herramienta fácil e intuitivo para el administrador.

b) Herramientas de gestión

Las herramientas de gestión que se describen a continuación se implementan en base a la interoperabilidad y se complementan con la aplicación The dude para crear un sistema de gestión que cubre las áreas funcionales del modelo ISO FCAPS.

ESTUDIO DE HERRAMIENTAS DE GESTIÓN COMPLEMENTARIAS.

Hay dos aspectos importantes a considerar al elegir herramientas de monitoreo para proporcionar un control integral de la red inalámbrica:

- ✓ Compatibilidad con los sistemas operativos donde está instalada la aplicación Dude Management
- ✓ Compatibilidad a la aplicación para cubrir las áreas funcionales del modelo de gestión ISO FCAPS.

Dude es una aplicación con herramientas integradas que cubren las siguientes áreas funcionales del modelo ISO FCAPS:

Gestión de fallos: Sistema de monitoreo de alarmas si y solo si la tarjeta gráfica de cada dispositivo es notificada en tiempo real a la red de control visual.

Gestión de configuración: Una opción de configuración centralizada para monitorear servicios y recursos usando el protocolo SNMP.

Gestión de contabilidad: Herramienta de verificación de ancho de banda, verificación de ancho de banda, monitoreo de recursos y servicios

Gestión de prestaciones: Archivos de informes e historial gráfico del estado de la red inalámbrica

Gestión de seguridad: Seguridad de acceso de usuario de derechos de administrador

Después de ver lo que se incluye en The Dude, puede ver que cubre estas áreas, pero algunas de las áreas que cubre son de bajo nivel y deben complementarse con herramientas compatibles, que se describen a continuación:

WIRESHARK

Es un analizador de redes es una herramienta poderosa que requiere un conocimiento sólido de los conceptos de estas mismas. Eso se traduce para las empresas de hoy en día modernas en comprender sobre protocolos HTTP y sus servicios, la pila de TCP / IP, analizar y comprender los encabezados de los paquetes que se reciben con muchos metadatos a veces complejos, así como el enrutamiento y como se entrelazan unos a otros, el reenvío de puertos y DHCP, por ejemplo (Altube Rafael, 2021):

- ✓ Permite seguir el rastro a los paquetes TCP stream, podemos ver todo lo relacionado con dicho paquete, el antes y el después, pudiendo aplicarles filtros personalizados a estos mismos sin perder el flujo.

- ✓ Permite ver estadísticas de los paquetes capturados incluyendo un resumen, jerarquía de protocolos, conversaciones, puntos finales y gráfica de flujos entre otros.

- ✓ Análisis fácil e informativo mediante resolución de nombres por mac, por red, etc… y re ensamblaje de paquetes.

- ✓ Cuenta con una herramienta de líneas de comandos para ejecutar funcionalidades llamada TShark.

VPN ACCESO REMOTO

Para tener control total de la aplicación de gestión, por la ubicación del servidor monitoriza constantemente la red las 24 horas del día, existen dos tipos de acceso remoto desde el cliente, el mismo que será controlado por el administrador de la red.

- ✓ Acceso remoto proporcionado por la aplicación de gestión Dude.

- ✓ VPN del cliente usando la aplicación Any Desk

ANY DESK

AnyDesk es un programa de software de escritorio remoto desarrollado por AnyDesk Software GmbH, Stuttgart, Alemania. Proporciona acceso remoto bidireccional entre computadoras y funciona con todos los sistemas operativos comunes.

.

HERRAMIENTAS MIKROTIK

Para complementar la aplicación de administración dude, Mikrotik ofrece varias herramientas propietarias para monitorear la red: Winbox (herramienta de configuración propietaria), rastreador de paquetes, etc.

A continuación, en la Tabla 26 se muestra las herramientas complementarias para cubrir en su totalidad las áreas funcionales del modelo FCAPS.

Tabla 26

Aplicaciones del sistema de gestión

Aplicación	Gestión Fallos	Gestión Configuración	Gestión Contabilidad	Gestión Prestaciones	Gestión Seguridad
The Dude	**X**	**X**	**X**	**X**	**X**
WIRESHARK	**X**		**X**		
VPN					**X**

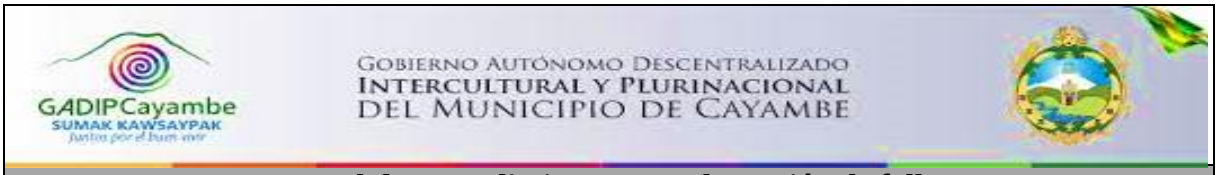
Fuente: Elaborado por el Autor

4.3.Manuales de Procedimiento

Durante el proceso de gestión, es importante recibir orientación para encontrar soluciones inmediatas, con procesos que ayude a resolver anomalías dentro de la red inalámbrica del GADIP del Municipio de Cayambe, por lo que en esta sección se describe un manual de procedimientos que cubre las áreas funcionales del modelo de gestión ISO FCAPS. El objetivo principal es gestionar la red usando la aplicación The dude y herramientas que complementen la gestión ayudando a que la red funcione sin problemas.

El presente manual es una guía general para saber cuándo utilizar las herramientas implementadas, no es una ley, sino una ayuda de rápido acceso para que los administradores, solucionando sin demora los problemas que se presenten dentro de la red inalámbricas del GADIP Cayambe. A continuación, se describen los procesos, los datos y las herramientas que se utilizan en cada manual de gestión que cubre las áreas funcionales FCAPS (Fallas, Configuración, Contabilidad, Prestaciones y Seguridad) del modelo OSI

4.2.5. Manual de procedimientos para la gestión de Fallos.



Manual de procedimientos para la gestión de fallos.			
Desarrollado:	Andres Acero		
Código:	PRO-001	**Destinatario**	Administrador Asistente de tecnología
Procedimiento:	Manejo de la gestión Fallos		

1.Objetivo

Iniciar el proceso de corrección de errores en la red inalámbrica en el menor tiempo posible, garantizando así la disponibilidad de la red inalámbrica sin inconvenientes para el usuario final.

2.Alcance

Este manual aplica para todos los puntos de red inalámbrica y todas las unidades de despliegue que brinden acceso inalámbrico a Internet, cubriendo áreas estratégicas; este procedimiento cubre los errores generales que ocurren en el funcionamiento de la red inalámbrica

Se anexará una base de datos de errores específicos que han ocurrido en el monitoreo hasta el momento; si se producen nuevos errores, sus nuevos procedimientos se documentarán para que se puedan prevenir de manera efectiva en el futuro.

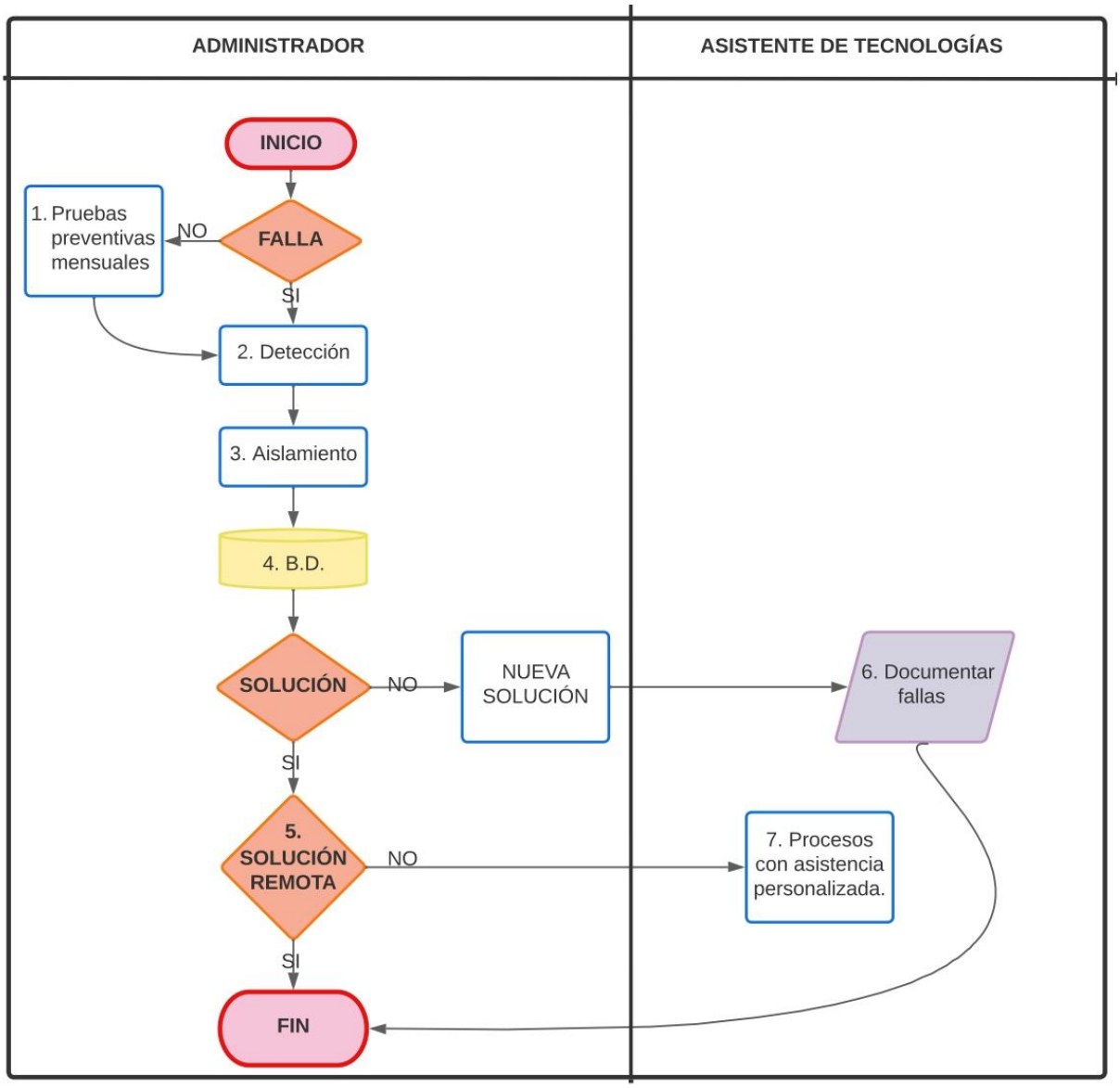
3. Abreviaturas y Definiciones

ABREVIATURAS	
TÉRMINO	**DEFINICIÓN**
TIC	Tecnología de la Información y Comunicación
GADIP	Gobierno Autónomo Descentralizado Intercultural y Plurinacional
SNMP	Protocolo Simple de Administración y Gestión

DEFINICIONES	
TERMINO	**DEFINICIÓN**

Base de Datos	Repositorio de información que contiene datos relacionados con el tema en discusión. Es un conjunto de datos pertenecientes a un mismo contexto que el sistema guarda para su uso.
Pruebas preventivas	Para detectar errores ocultos que normalmente no se pueden detectar, estas pruebas requieren interrupciones del servicio para prevenir los errores.
Vigilancia de alarmas	Mecanismo que posee The dude para presenta mediante notificaciones visuales los fallos en el instante que suceden.
Soluciones Remotas	Una vez que el error se identifica de forma centralizada mediante la herramienta winbox incluida en la aplicación de gestión The dude, se realiza una corrección remota.
Formularios	Son los informes que se presentan para el mantenimiento y protección de datos para la realización de los trámites y como tales se cumplen.
Diagnóstico	Cuando se monitorea un dispositivo de red inalámbrica, se detecta un diagnóstico que indica el tipo de error que ocurrió.

4.Diagrama de Flujos



5. Desarrollo de actividades

Procedimiento general para resolución de falla en la red inalámbrica GADIP-CAYAMBE

Actividad	Descripción	Responsable
Prueba preventiva	Permite el descubrimiento de defectos ocultos que normalmente pasarían desapercibidos y requieren	

	interrupciones del servicio para realizar controles preventivos como la conectividad. Como prueba preventiva, se toma las debidas precauciones a los usuarios y administradores de instituciones educativas información y recomendaciones necesarias para mantener el normal funcionamiento de la red.	Administrador de la red Inalámbrica Técnico de la Red Inalámbrica
Detección	Para detectar errores, el monitoreo de alarmas muestra mensajes visuales en la pantalla para informar al administrador que hay un evento o problema en la red **Alarma–Mensaje:** Envía un mensaje a la pantalla con el nombre del dispositivo, el estado del servicio y el tiempo requerido para el evento. **Alarma–Flash:** Titila la ventana The Dude en la barra del escritorio.	Administrador de la red Inalámbrica

	Alarma–beep: Envía un sonido de beep.	
Aislamiento	Se Aísla las fallas a través del mecanismo de la aplicación The Dude, codificada por colores para mostrar el estado del dispositivo: **GRIS:** Inestable, Servicios desconocidos **VERDE:** Activo, Servicios estables **ANARANJADO:** Inestable, Servicios inestables **ROJO:** Crítica, Servicios caídos **AZUL**: Inestable, Servicio en reconocimiento Si el fallo producido tiene un tiempo considerable sin solucionarlo se debe realizar una llamada de advertencia a los puntos afectados si existe un responsable. Cuando se descubre un problema específico, se	Administrador de la red Inalámbrica

	ingresará de forma remota a través de Winbox para resolverlo.	
Base de Datos	La base de datos de fallos almacena todos los fallos específicos encontrados en el monitoreo de la red y la base de datos de fallos puede proporcionar soluciones inmediatas detalladas en el ANEXO F	Administrador de la red Inalámbrica
Solución Remota	Para la solución de fallos de manera Remota la aplicación The Dude presenta dos opciones al administrador de la red: WinBox: Herramienta remota de configuraciones Terminal: Interfaz de línea de comandos del dispositivo	Administrador de la red Inalámbrica
Personalizada	La solución de fallos personalizada se realiza cuando el error no se puede resolver externamente con las herramientas de The Dude, esto se reporta enun documento generado para la documentación de la falla. Se detalla en el **ANEXO H.1:** Formulario de los Reportes Fallos. El problema es asistido por el asistente de tecnologías para solucionarlo. Al solucionar el problema se llenara el formulario del ANEXO H.2, para documentar la falla	Administrador de la red Inalámbrica

		Técnico de la Red Inalámbrica
Documentación de Fallos	Al solucionar el problema se llenará el formulario H.2 Se ingresara los datos de formulario H2 a la Base de Datos de problemas.	Administrador de la red Inalámbrica
FIN		

4.2.6. Manual de procedimientos para la gestión de Configuración.

GADIPCayambe SUMAK KAWSAYPAK
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE

Manual de procedimientos para la gestión de configuración.			
Desarrollado:	Andres Acero		
Código:	PRO-002	**Destinatario**	Administrador Asistente de tecnología
Procedimiento:	Manejo de la gestión de Configuraciones		

1. Objetivo

Presentar los procedimientos a seguir cuando se agrega un nuevo dispositivo a la red inalámbrica para que pase a formar parte de la administración y realice las funciones que se le asignan.

2. Alcance

Este manual se utiliza para agregar un nuevo dispositivo a la red inalámbrica, el proceso se aplica a todos los nuevos dispositivos conectados a la red inalámbrica, proporcionará el formato de grabación de datos del nuevo dispositivo agregado y el proceso de conexión es el siguiente para lograr la copia de seguridad del sistema de control y los dispositivos

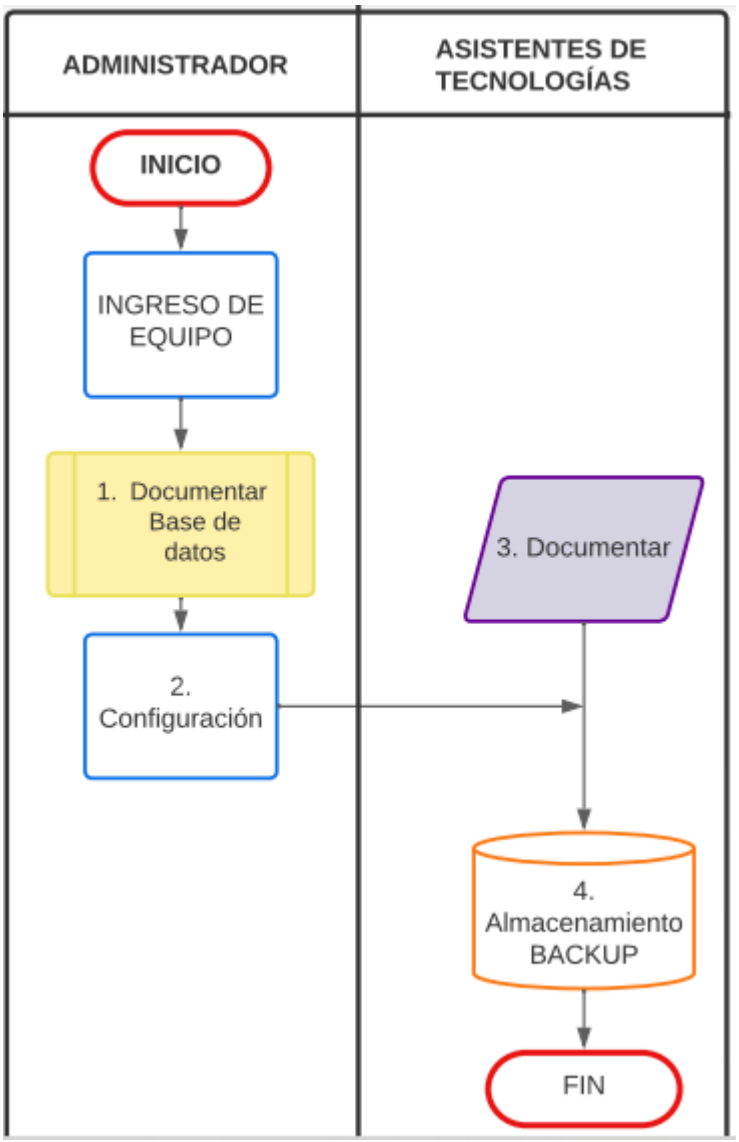
3. Abreviaturas y Definiciones

ABREVIATURAS	
TÉRMINO	**DEFINICIÓN**
IOS	Sistema operativo del dispositivo
SNMP	Protocolo simple de administración de red
MD5	Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico de 128 bits.
DES	Estándar de Encripcion de datos, es un algoritmo de cifrado Estándar
V3	Versión 3 de SNMP
V2	Versión 2 de SNMP

DEFINICIONES	
TERMINO	**DEFINICIÓN**
Proceso de adquisición del dispositivo	La institución cuenta con un mecanismo de adquisición de equipos, que incluye la emisión de pedidos anticipados con las características adecuadas al departamento responsable de la financiación.
Compra del dispositivo	Para adquirir un dispositivo, el personal del departamento de TICs debe justificar el uso del dispositivo para realizar la compra.
Implementación del dispositivo	Una vez adquirido el equipo, se procede a la implementación de los procedimientos descritos en este manual.
Nomenclatura para los dispositivos de la red	La nomenclatura es determinada por la Unidad de hardwarey comunicaciones del GADIP Cayambe, con el objetivo de identificar con facilidad los dispositivos en la red.
Recolección	La información del dispositivo se recopila para identificar el

	dispositivo y su configuración.
Proceso de configuración de la red	El administrador de la red asigna la configuración de red apropiada para que realice su función dentro de la red.
The Dude	Aplicación de gestión que permite la monitorización continua en tiempo real de los dispositivos.
Proceso de configuración de SNMP	La configuración de SNMP en los dispositivos es necesaria para que la aplicación The dude gestione el dispositivo dentro de la red inalámbrica.

4. Diagrama de Flujos



5. Desarrollo de actividades

Procedimiento para agregar un dispositivo en la redinalámbrica- GADIP-CAYAMBE para la gestión con The dude.

Actividad	Descripción	Responsable
Ingreso del equipo	Procedimiento para añadir un nuevodispositivo a la red inalámbrica: Proceso de adquisición del dispositivo Compra del dispositivo.Instalación del dispositivo	Administrador de la red Inalámbrica Técnico de la Red Inalámbrica
Documentación del equipo	En la documentación de los equipos se deberá ingresar el dispositivo a la base de datos de Inventario de Dispositivos se detalla en el **ANEXO E:** Base De Datos Para Los Equipos De Interconexión. Para el ingreso de los dispositivos de deberá tomar en cuenta la nomenclatura que maneja el departamento de Bodega del GADIP del Municipio de Cayambe. **Nomenclatura de los dispositivos** Tipo de Dispositivo • RB-Routerboard • SW-Switch • SR- Servidor • ANT- Antena **Recolección de datos** Las recolecciones de datos de los dispositivos de red serán agregados a la base de datos que contiene los siguientes parámetros de información: • Tipo de dispositivo • Nombre del Equipo • Dirección IP de Red • Marca	

	• Modelo • Número de Serie • Ubicación del Equipo • Fecha de Ingreso • Responsable	
Configuración	En la configuración se realiza el proceso para agregar un nuevo dispositivo a la red Inalámbrica del GADIP del Municipio deCayambe. **<u>*Configuración para añadir un nuevo dispositivo en la red.</u>** - Añadir/Añadir dispositivo/Ventana principal deconfiguración/general - Modificación de los parámetros: Nombre, Dirección, Tipo, Nombre de Administrador, Contraseña **<u>* Configuración del protocolo SNMP.</u>** *Dispositivo/Ventana General/Utilidades/winbox* ✓ IP/SNMP Setings /Enable:Habilitado **Ubicación:** Permite la ver la descripción de ubicación del dispositivo **Trap Comunity:** Muestra la Comunidad determinada para la gestión de los dispositivos **Trap versión:** v3 o v2, dependiendo del	Administrador de la red Inalámbrica/ Técnico de la Red Inalámbrica.

	dispositivo que soporta el Protocolo SNMP ✓ SNMP Comunities/ Agregar:nueva comunidad **Nombre:** Ingrese el nombre de lacomunidad de SNMP **Dirección IP:** Ingresar Dirección IP delservidor de Gestión **Seguridad:** Seleccionar el tipo deseguridad (Privada) **Protocolo de Autenticación:** MD5 pordefecto **Protocolo de Encriptación**: DES por defecto **Contraseña:** Ingresar la contraseña de laaplicación The Dude ***Proceso de modificación de laConfiguración del nuevo dispositivo.** Si se realiza algún cambio dentro de lared es necesario documentar el cambio enel de documentación de configuración de dispositivos este tendrá los siguientes parámetros: • Nombre del Equipo • Número de Serie • Dirección de Red • Fecha del cambio • Responsable	

	• Cambios Realizados • Observaciones. Estos cambios serán actualizados en el inventario de los dispositivos de red cada semana para mantener el buen funcionamiento de la red.	
Almacenamiento	Permite guardar los cambios o configuraciones realizadas dentro de la aplicación The Dude. **Barra de Herramientas/Exportar** Visualiza la pantalla para guardar una copia de seguridad, indicando la ubicación donde se guarda el documentoy el formato del documento **backup- 2015.06.18.xml.** **Barra de Herramientas/Importar** Permite abrir el documento de la copia de seguridad dependiendo de la fecha que sedesee abrir. Seleccionar el Documento/Abrir mostrara todas las configuraciones que se realizó esa fecha.	Administrador de la red Inalámbrica/ Técnico de la Red Inalámbrica.
	FIN	

4.4.3. Manual de procedimientos para la gestión de Contabilidad

Manual de procedimientos para la gestión de Contabilidad.			
Desarrollado:	Andres Acero		
Código:	PRO-003	**Destinatario**	Administrador
Procedimiento:	Manejo de la gestión de Contabilidad		

1. Objetivo.

Presentar el procedimiento a seguir para la configuración y monitoreo de recursos y servicios para mostrar el estado de los equipos de red inalámbricos.

2. Alcance.

Este manual es una guía para agregar recursos y servicios en un dispositivo de red inalámbrica que permite que la aplicación The Dude tenga monitorea continuamente la red, este programa funciona en todos los recursos y servicios, lo que le permite obtener informes sobre la situación actual del uso de los recursos para que la red brinde sus servicios a los usuarios.

3. Abreviaturas y Definiciones

ABREVIATURAS	
TÉRMINO	**DEFINICIÓN**
GADIP	Gobierno Autónomo Descentralizado Intercultural y Plurinacional
MAC	Control de Acceso al Medio, es un identificador de 48 bits

DEFINICIONES	
TERMINO	**DEFINICIÓN**
Reporte	Este tipo de documento indica los fallos o configuraciones que se realizó en determinado tiempo.
Parámetros de Monitoreo	Permite obtener datos específicos sobre el funcionamiento de cada dispositivo, permitiendo al administrador obtener información en tiempo real sobre el funcionamiento de la red

Compilación	Recolección de información de datos informáticos sobre el funcionamiento y configuración de los dispositivos de red.
Visualización del Reporte	Permite al administrador la visualización de los reportes que se generan, con las configuraciones o fallos ocasionados en cualquier dispositivo de la red.
Impresión del reporte	Permite tener un reporte físico sobre el estado de la red

4. Diagrama de Flujos

5. Desarrollo de actividades

Procedimiento para agregar un dispositivo en la red inalámbrica GADIP-CAYAMBE

Actividad	Descripción	Responsable
Configuración de Parámetros de Monitoreo	Este proceso permite el obtener reportes o historiales sobre el funcionamiento de la red. La aplicación The Dude muestra estos reportes o historiales sea diarios, semanales, mensuales ode un año de funcionamiento.	Administrador de la red Inalámbrica

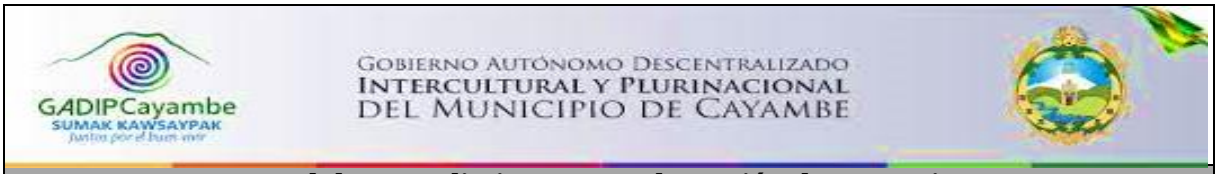
	<u>*Configuración de parámetros de Monitoreo The Dude.</u> **Menú Contenidos/ Admins** Presenta un reporte de los Administradores de la red Inalámbrica, del grupo que pertenecen cada administrador y un reporte del tiempo de conexión. **Menú Contenidos/ Devices** Visualiza un reporte con los datos dered, localización, servicios de cadadispositivo conectado, Lista, árbol,RouterOS, tipos y MAC mapping. **Menú Contenidos/ History Actions** Presenta un reporte de las funcionesque realiza el administrador duranteel inicio de sesión iniciada. **Menú Contenidos/ Links** Procede a indicar un reporte de los enlaces configurados dentro de la red y las características de cada uno de ellos. **Menú Contenidos/ Logs** ✓ Reporte diarios ✓ Reporte semanal ✓ Reporte anual **Menú Contenidos /Actions** Muestra el reporte de la acción generada en el monitoreo de la red Inalámbrica, indica parámetros detiempo, dirección y el evento que se realizó. **Menú Contenidos/ Logs / Evento** Emite	Técnico de la Red Inalámbrica

	el reporte del evento ocasionado en la red Inalámbrica, muestra parámetros de tiempo, dirección y la descripción del evento. **Menú Contenidos/ Logs / Syslog** Genera un reporte del evento ocurrido en la monitorización de lared, indica parámetros de Tiempo,Dirección IP y la descripción delevento, además identifica el eventomediante el código de colores dependiendo del fallo. **Menú Contenidos/ Network Maps** Muestra el reporte de los Mapas deRed que contiene un diagrama de redque permite el monitoreo. **Menú Contenidos/ Networks** Emite un reporte de los datos de segmentación de la red, generados en la red Inalámbrica. **Menú Contenidos/ Outages** Genera el reporte del estado de los servicios, dispositivos, el tiempo de conexión, la fecha de conexión y el estado.	
Monitoreo	En este proceso se muestra el monitoreo de los recursos físicos y lógicos de la red Inalámbrica en donde cada uno de ellos muestra mediante reportes el funcionamientoel monitoreo se realiza tanto	Administrador de la red Inalámbrica

	en el sistema de visualización como en la aplicación The Dude software de monitoreo. ***Monitoreo de la aplicación The Dude.** • Dispositivos de red • Enlaces • Diagramas de red • Estado de conexión de los dispositivos mediante el código de colores.	Técnico de la Red Inalámbrica
Determinación del Reporte o Historial	Se determina el reporte o historial en base al tiempo de funcionamiento quese quiera adquirir. **Aplicación The Dude indica el reporte de manera:** • Diario • Semanal • Mensual • Anual	Administrador de la red Inalámbrica Técnico de la Red Inalámbrica
Visualización del Reporte o Historial	La visualización del reporte o historial se puede obtener de la Aplicación The Dude. La aplicación The Dude indica mediante un documento .xml con la fecha que fue creado el reporte o historial.	Técnico de la Red Inalámbrica

Impresión del Reporte o Historial	Este proceso de debe determinará en caso de que sea necesaria la impresión. Es necesaria la impresión de reportes sobre el funcionamiento cada 6 meses. Y generar un reporte semanal para mantener el buen funcionamiento de la red.	Técnico de la Red Inalámbrica
FIN		

4.4.4. Manual de procedimientos para la gestión de Prestaciones



Manual de procedimientos para la gestión de Prestaciones.			
Desarrollado:	Andres Acero		
Código:	PRO-004	**Destinatario**	Administrador
Procedimiento:	Manejo de la gestión de Prestaciones		

1. Objetivo

Establecer procedimientos para el monitoreo de la red y los recursos utilizados para escanear el tráfico de la red con herramientas de monitoreo y generar informes o historial y estadísticas proporcionadas por la red.

2. Alcance.

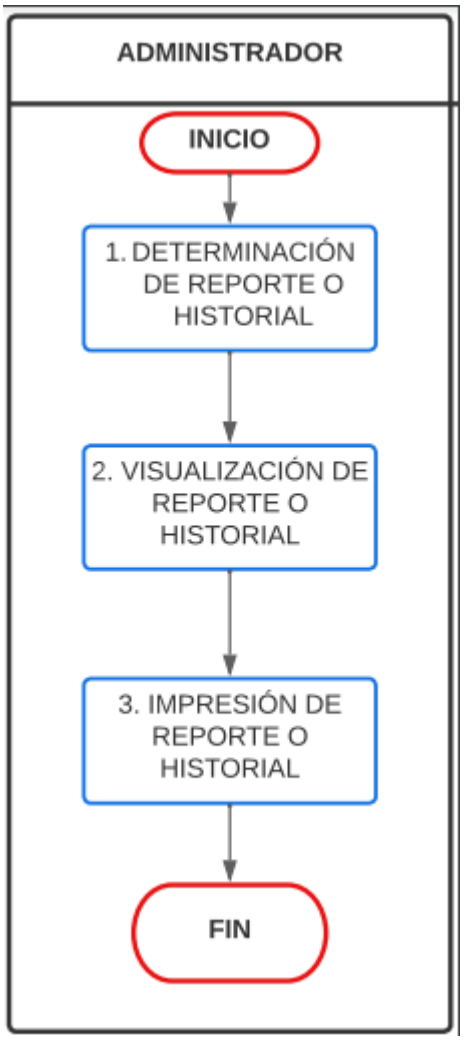
Este procedimiento aplica para usar herramientas de monitoreo que generan escaneos de tráfico de red y le permiten la presentación del análisis estadístico de recursos, servicios y parámetros de monitoreo en la red usando la aplicación The Dude.

3. Abreviaturas y Definiciones

ABREVIATURAS	
TÉRMINO	**DEFINICIÓN**
SNMP	Protocolo Simple de Administración y Gestión
TCP	Protocolo de Control de Transmisión
UDP	Protocolo Datagrama de Usuarios
ICMP	El Protocolo de Mensajes de Control de Internet
DNS	Sistema de Nombres de Dominio
CPU	Unidad Central de Proceso

DEFINICIONES	
TERMINO	**DEFINICIÓN**
Datos estadísticos	Permite que el administrador de la red analizar, comparar e interpretar los datos generados sobre el funcionamiento de la red inalámbrica.
Pruebas de Funcionamiento	Realiza funciones lógicas para determinar si los servicios y los recursos de red están activos, el monitoreo de sondeo le permite probar y sondear este recurso.
Tiempo de respuesta	El tiempo de respuesta es el tiempo que pasa desde que se envía una comunicación y se recibe la respuesta.
Gráficos Estadísticos	Los gráficos estadísticos le permiten comparar datos que se han recopilado y presentado en forma tabular. Resumir generando gráficos.

4. Diagrama de Flujos



5. Desarrollo de actividades

Procedimiento para obtener reportes e historiales que presentan el estado actual de la red inalámbrica GADIP-CAYAMBE

Actividad	Descripción	Responsable
Monitoreo	***Parámetros de Monitoreo de The Dude** Para la configuración de los parámetros de monitoreo, se configura las pruebas de función como SNMP, TCP, UDP, ICMP y DNS. Los cuales permiten la generación de los datos estadísticos representados	Administrador de la red Inalámbrica

	gráficamente para el administrador de la red.	Técnico de la Red Inalámbrica
Determinación de Herramientas	En la determinación de herramientas se tiene la aplicación The Dude que permite obtener gráficos estadísticos sobre los recursos y servicios de la red Inalámbrica delGADIP del Municipio de Cayambe. **<u>*The Dude:</u>** **Pruebas de Función** ***Contenidos/Probes/Añadir*** Realiza funciones lógicas para determinar si el servicio y los recursos de la red están activos o no, la supervisión de Polling permite verificar y sondear este recurso. ***Seleccionar el Dispositivo a verificar/Pestaña de Servicios*** ✓ ***Flag:*** *Asigna un color al estado (Codigo de colores para determinar Alarmas)* ✓ ***Tipo:*** *Parámetros de Monitoreo* ✓ ***Problema:*** *Visualiza estados como: Ok, Down, Estable, Inestable* ***Tiempo de respuesta:*** *Representa losdatos generados en milisegundos.*	Administrador de la red Inalámbrica/ Técnico de la Red Inalámbrica.
Visualización de	Los datos estadísticos que se generan se	

historiales y Datos Estadísticos	pueden obtener hasta de 1 año de funcionamiento del servidor, facilitando al administrador determinar el rendimiento de las características físicas de la red del GADIP del Municipio de Cayambe. **<u>*The Dude</u>** • 1 año • 1 mes • 1 día • 1 hora	
Impresión de los Datos	La impresión de los datos estadísticos se realiza dependiendo de las necesidades de la entidad. La impresión se deberá realizar cada 6 meses para verificación del funcionamiento del servicio y de los recursos. Se deberá realizar la verificación de los gráficos estadísticos cada semana paraobtener datos reales y determinar el funcionamiento de cada dispositivo.	Técnico de la Red Inalámbrica.
FIN		

4.4.5. Manual de procedimientos para la gestión de Seguridad

GADIPCayambe
SUMAK KAWSAYPAK
Juntos por el buen vivir

GOBIERNO AUTÓNOMO DESCENTRALIZADO
INTERCULTURAL Y PLURINACIONAL
DEL MUNICIPIO DE CAYAMBE

Manual de procedimientos para la gestión de Seguridad.			
Desarrollado:	Andres Acero		
Código:	PRO-005	**Destinatario**	Administrador Asistente de Tecnologías Personal encargado

Procedimiento:	Manejo de la gestión de Seguridad		

1. Objetivo.

Presentar el procedimiento a seguir para acceder a los dispositivos de la red inalámbrica, administrar el sistema y todas sus herramientas.

2. Alcance.

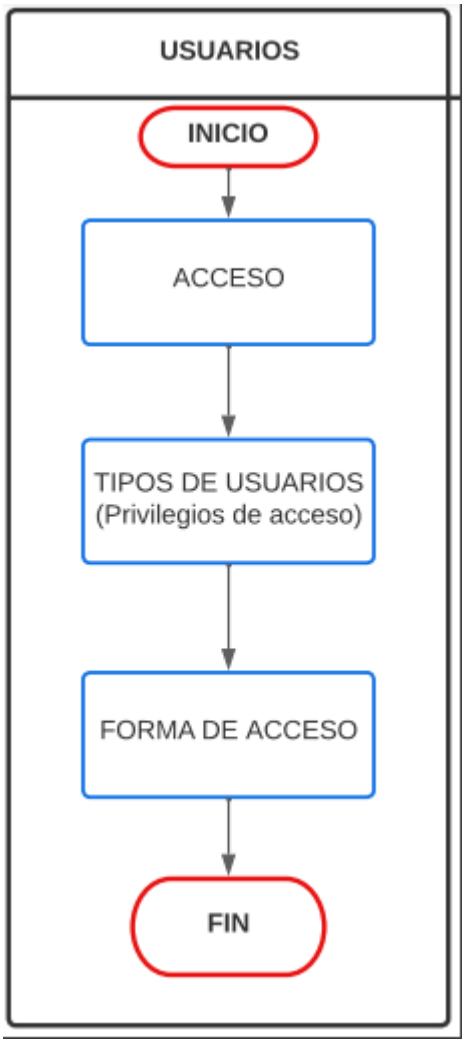
Este manual es una guía de procedimientos para acceder a los sistemas y dispositivos de gestión aplicables al sistema de gestión y en particular a la aplicación The Dude y a los dispositivos que forman parte de la red inalámbrica del GADIP Cayambe

3. Abreviaturas y Definiciones

ABREVIATURAS	
TÉRMINO	**DEFINICIÓN**
GADIP	Gobierno Autónomo Descentralizado Intercultural Plurinacional.
TIC´s	Tecnologías de información y comunicación
S.O.	Sistema Operativo

DEFINICIONES	
TERMINO	**DEFINICIÓN**
Tipo de Acceso	Tipo de acceso hace referencia a poder acceder a cada uno de los servicios configurados en el modelo de gestión de la red inalámbrica del GADIP del Municipio de Cayambe
Acceso Local	Acceda a la aplicación The Dude desde el misma lugar en donde se encuentra el departamento de las Tics.
Acceso Remoto	Es acceder desde cualquier otro sitio, siempre y cuando el cliente se encuentre con servicio de internet
Acceso Web	Es acceder mediante un navegador Web desde cualquier sitio siempre y cuando el cliente se encuentre conectado en el mismo segmento de red

4. Diagrama de Flujos



5. Desarrollo de actividades

Procedimiento para el acceso al sistema de gestión de la red inalámbrica GADIP CAYAMBE

Actividad	Descripción	Responsable
Acceso	En este proceso se indica el tipo de acceso para cada uno de los servicios configuradosen el modelo de gestión de la red Inalámbrica del GADIP del	Administrador de la red Inalámbrica

	Municipio de Cayambe estableciendo jerarquías y privilegios para el acceso al sistema.	Técnico de la Red Inalámbrica
Tipo de Usuario	**<u>Aplicación The Dude:</u>** **Administrador:** Es el usuario con mayor privilegio en el sistema de virtualización, capaz de configurar y modificar por completo la aplicación The Dude. Permite el Leer, escribir, local, remoto,web, agente, política, permite el administrar más de un panel para el monitoreo. **Asistente:** Es un usuario con privilegios de gestor con capacidad de solucionar los fallos dentro de la red mediante la aplicación The Dude con privilegios de Leer, Local, web, remoto, no le permite abrir más de un panel para el monitoreo.	Administrador de la red Inalámbrica/ Técnico de la Red Inalámbrica/ Usuario
Forma de Acceso	*<u>**Aplicación The Dude:**</u> **-Acceso Local-Servidor de Monitoreo** Ubicado en el Departamento de Tecnologíasde Información en el GADIP del Municipiode Cayambe el servidor de monitoreo con la aplicación The Dude y las herramientas preventivas para elfuncionamiento del sistema de gestión comoel ping, traceroute, WinBox y IPScanner.	Administrador de la red Inalámbrica/ Técnico de la Red Inalámbrica/ Usuario

	Inicio/The Dude/conectar **Modo:** Local **Nombre del Usuario:** Admin **Contraseña:** ***** **-Acceso Local- Remoto Servidor de Monitoreo** En el computador establecido como cliente se encuentra instalado The Dude donde se encuentra conectado en el mismo segmento de red, a través de la opción remota The Dude. **Modo:** remoto **Nombre del Usuario:** Admin **Contraseña:** ***** **Conectar a:** Dirección IP del Servidor de Monitoreo **Puerto:** 2210 **-Acceso Web local servidor Monitoreo** En el computador establecido se encuentra instalado The Dude donde se encuentra conectado en el mismo segmento de red, a través de un navegador Web. Ingreso al navegador (Firefox, Chrome, Internet Explorer,etc) **Barra de Direcciones:** IP del Servidor de Monitoreo:81 **User:** Admin **Password:** ***** **<u>*Servidor Monitoreo:</u>**	

	Usuario: Administrador **Password:** ********** **<u>*Portal Cautivo:</u>** **Administrador** **Usuario:** Portal **Contraseña: ********** **-Usuarios:** Para el uso del Portal Cautivo en el Parque deCayambe se estable: ✓ Presentar en Recepción del GADIP del Municipio de Cayambe la identificación cedula o pasaporte para personas extranjeras. ✓ Se creará el usuario con el nombre principal del usuario y como contraseña el número de cedula. ✓ Podrá ingresar al Portal Cautivo y hacer uso del servicio de internet gratuito. Conectar el dispositivo de acceso como Laptop, celular a la red GADIP-CAYAMBE ✓ Ingresar en el Navegador de su elección (Firefox, Chrome, Internet Explorer, etc) ✓ Seleccionar Añadir la excepción o Iral sitio no recomendado. ✓ Muestra la portada del Portal Cautivo, donde se ingresa el nombre	

	del usuario, y la contraseña el número de cedula del usuario. ✓ No cerrar la pantalla de sesión, para continuar con el servicio de internet.	
FIN		

4.4. Pruebas de Funcionamiento

El funcionamiento de cada área funcional del modelo de gestión se verifica a través de pruebas funcionales que demuestran la correcta funcionalidad del software The Dude.

4.4.1. Prueba de funcionamiento gestión de fallos

En la gestión de fallos de realiza las pruebas de funcionamiento en la aplicación The Dude donde se verificará la asignación de notificaciones en los dispositivos de red y él envió de las notificaciones el software de monitoreo al administrador de la red.

En la gestión de fallos el manejo de errores realiza pruebas funcionales en la aplicación The Dude, verifica la propagación de mensajes a los dispositivos de red y envía mensajes desde el software de monitoreo a los administradores de red.

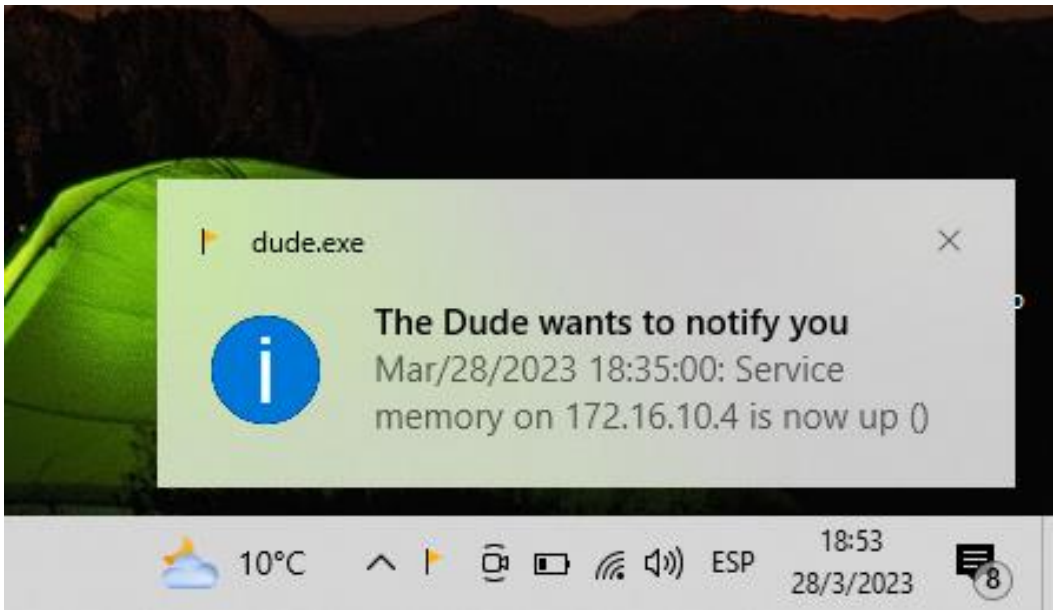
Estas pruebas funcionales demuestran el correcto funcionamiento de las configuraciones de notificación de fallos a través de mensajes de alerta a los administradores, lo que facilita a los técnicos la resolución inmediata de errores de red y el mantenimiento de operaciones dentro de red inalámbrica del GADIP del Municipio de Cayambe, brindando un buen servicio de calidad.

The Dude

La aplicación Dude tiene un sistema de notificación incorporado que se puede configurar en cualquier dispositivo de red conectado a la topología de red de la aplicación Dude.

Figura 38

Envió de Mensajes Emergentes y Mensaje Flash



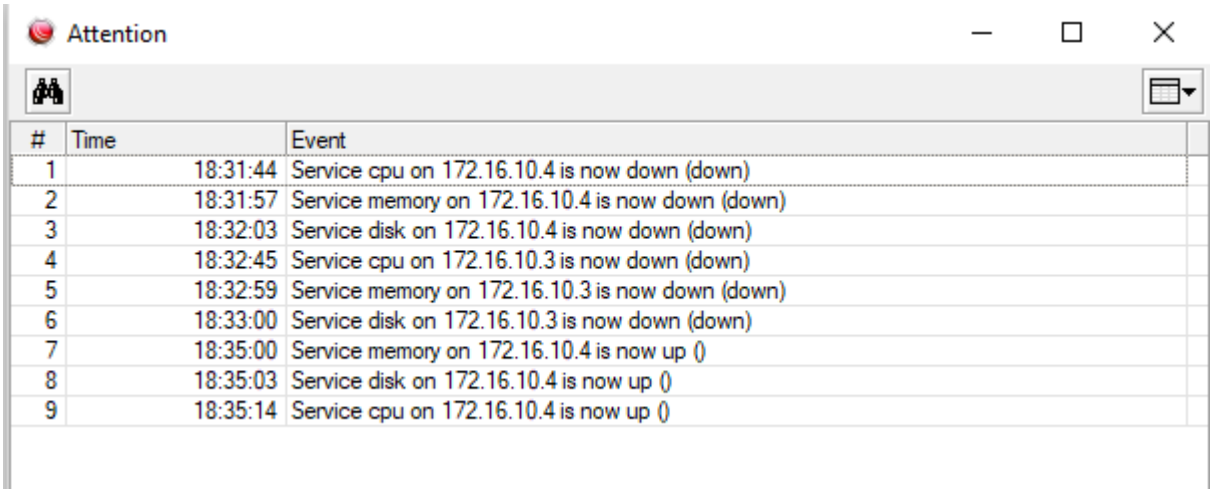
Fuente: (Aplicación The Dude)

En la Figura 39 muestra cada tipo de mensaje configurado en el dispositivo de red y muestra qué mensajes aparecen antes de que ocurra un error de red para que el administrador de la red inalámbrica.

Envió de Mensaje Pantalla Grande

Figura 39

Visualización de la notificación interfaz usuario



#	Time	Event
1	18:31:44	Service cpu on 172.16.10.4 is now down (down)
2	18:31:57	Service memory on 172.16.10.4 is now down (down)
3	18:32:03	Service disk on 172.16.10.4 is now down (down)
4	18:32:45	Service cpu on 172.16.10.3 is now down (down)
5	18:32:59	Service memory on 172.16.10.3 is now down (down)
6	18:33:00	Service disk on 172.16.10.3 is now down (down)
7	18:35:00	Service memory on 172.16.10.4 is now up ()
8	18:35:03	Service disk on 172.16.10.4 is now up ()
9	18:35:14	Service cpu on 172.16.10.4 is now up ()

Fuente: (Aplicación The Dude)

En la figura 40 se muestra las pruebas funcionales de la gestión de fallos generados por el software de la aplicación The Dude garantizan que los fallos se puedan resolver de manera inmediata utilizando las herramientas proporcionadas por la aplicación, lo que permite que los servicios de Internet funcionen sin inconvenientes.

Base de Datos Documentación de Fallos

Una base de datos de documentación de Fallos permite a los administradores de red almacenar copias de seguridad de los errores que ocurren en la red para que cualquier error pueda corregirse inmediatamente. Una base de datos de documentación de errores permite a los administradores de red almacenar copias de seguridad de los errores que ocurren en la red para que cualquier error pueda corregirse inmediatamente.

Figura 40

Base de Documentación de Fallos

BASE DE DATOS DOCUMENTACIÓN DE FALLOS					
FILTRO 1	FILTRO 2	FILTRO 3	FILTRO 4	FILTRO 5	FILTRO 6
N° REPORTE DEL FALLO	DESCRIPCIÓN DEL FALLO	FECHA	RESPONSABLE	LUGAR	OBSERVACIONES

Fuente: (Microsoft Excel 2019)

Una base de datos de documentación de fallos permite a los administradores de red examinar cada mensaje y asegurarse de que los errores resultantes se hayan resuelto, dando prioridad a la resolución inmediata de errores.

4.4.2. Prueba de funcionamiento gestión de configuraciones

En la gestión de configuración, la prueba funcional del software The Dude muestra una base de datos de dispositivos conectados a la red inalámbrica y una base de datos de dispositivos de red administrados y controlados en Microsoft Excel 2019 para la administración y control de todos los dispositivos conectados a la red.

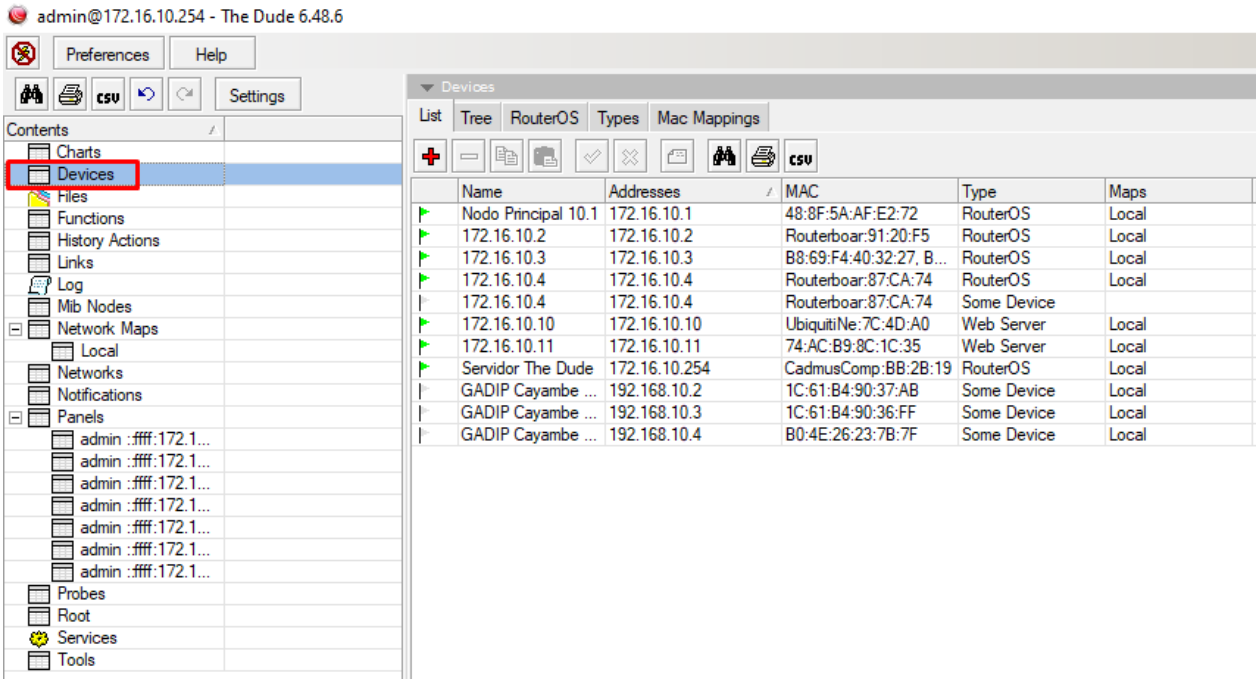
Aplicación The Dude

Permite enumerar automáticamente los dispositivos de red conectados en la topología de red de la aplicación, la figura 41 muestra la enumeración y las características clave de cada dispositivo, como dirección IP, dirección MAC, SSID, tipo de dispositivo y servicios configurados para cada dispositivo.

Inventario Automático de los Dispositivos

Figura 41

Base de datos de dispositivos



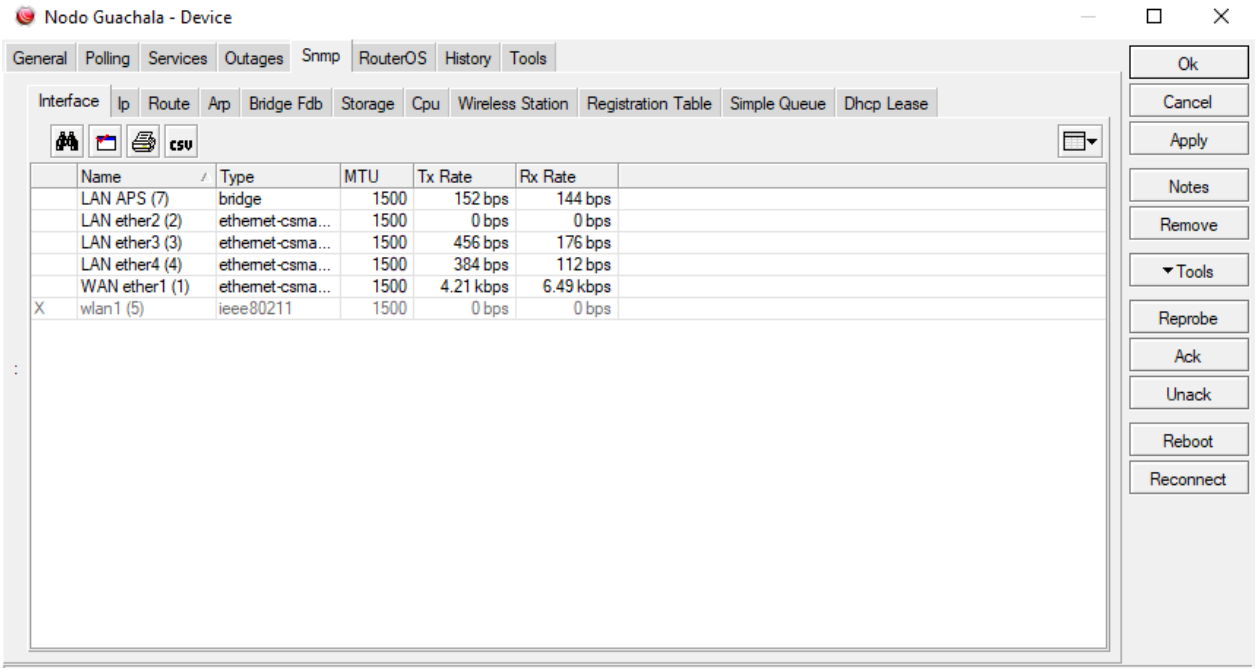
Fuente: (Aplicación The Dude)

Verificación del Protocolo SNMP

La configuración del protocolo SNMP permite a los administradores de red administrar de forma remota los recursos físicos de cada dispositivo, como se muestra en la Figura 42 que muestran los recursos físicos de cada dispositivo, la configuración general del dispositivo y los servicios que se pueden utilizar. para administrar los dispositivos de red.

Figura 42

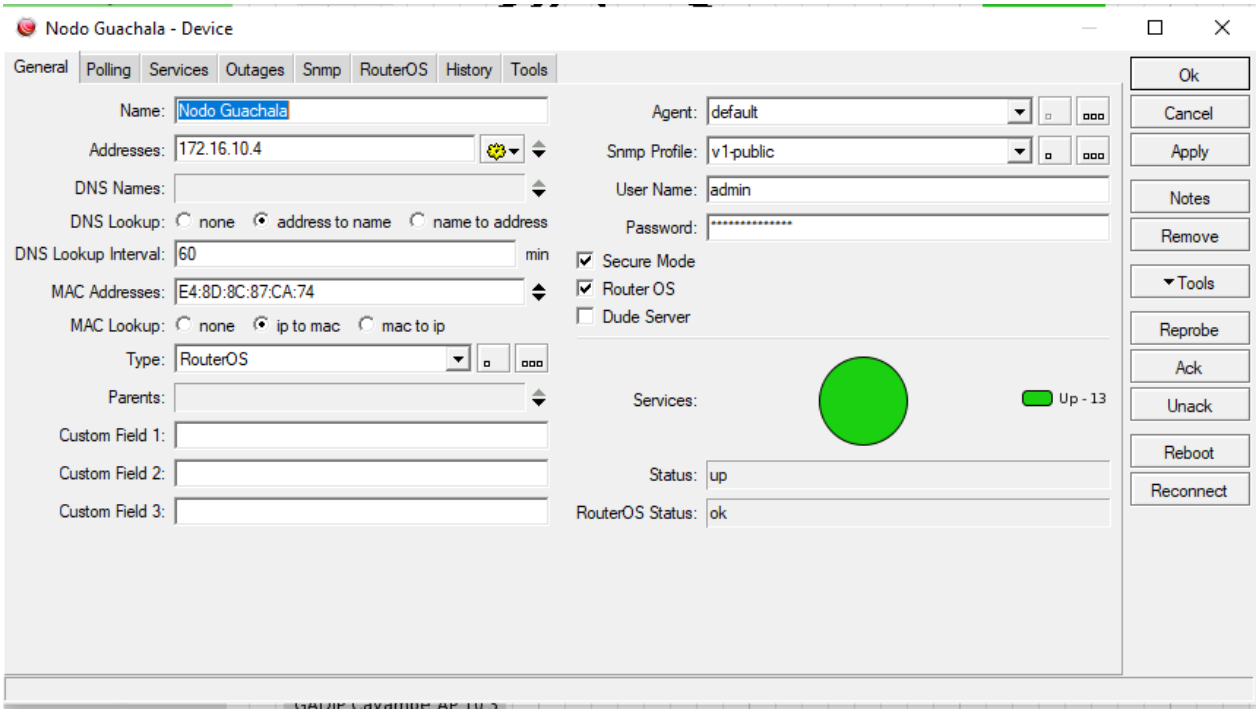
Activación SNMP dispositivo



Fuente: (Aplicación The Dude)

Figura 43

Verificación de SNMP



Fuente: (Aplicación The Dude)

Al verificar la configuración del protocolo SNMP en cada dispositivo de la red, permite el acceso a cada servicio que brinda y controla las partes físicas y lógicas del dispositivo, facilitando así la configuración remota de sus recursos.

Base de datos de inventario de equipos

Muestra el funcionamiento de la base de datos de gestión de inventario de dispositivos de red, los administradores pueden agregar nuevos dispositivos de red al inventario desde una interfaz gráfica dinámica que ayuda a ingresar automáticamente cada propiedad o parámetro en el inventario.

Figura 44

Inventario de Dispositivos de Red

Fuente: (Microsoft Excel 2019)

El inventario de dispositivos de red le brinda un control completo sobre sus dispositivos, lo que facilita encontrar cualquier dispositivo o configurarlos instantáneamente en función de los parámetros de red, como la dirección IP y la ubicación del dispositivo.

4.4.3. Prueba de funcionamiento gestión de contabilidad

En la gestión de Contabilidad se muestra las pruebas de funcionamiento, genera informes o historial de dispositivos de red y configuraciones realizadas en la aplicación The Dude.

Aplicación The Dude

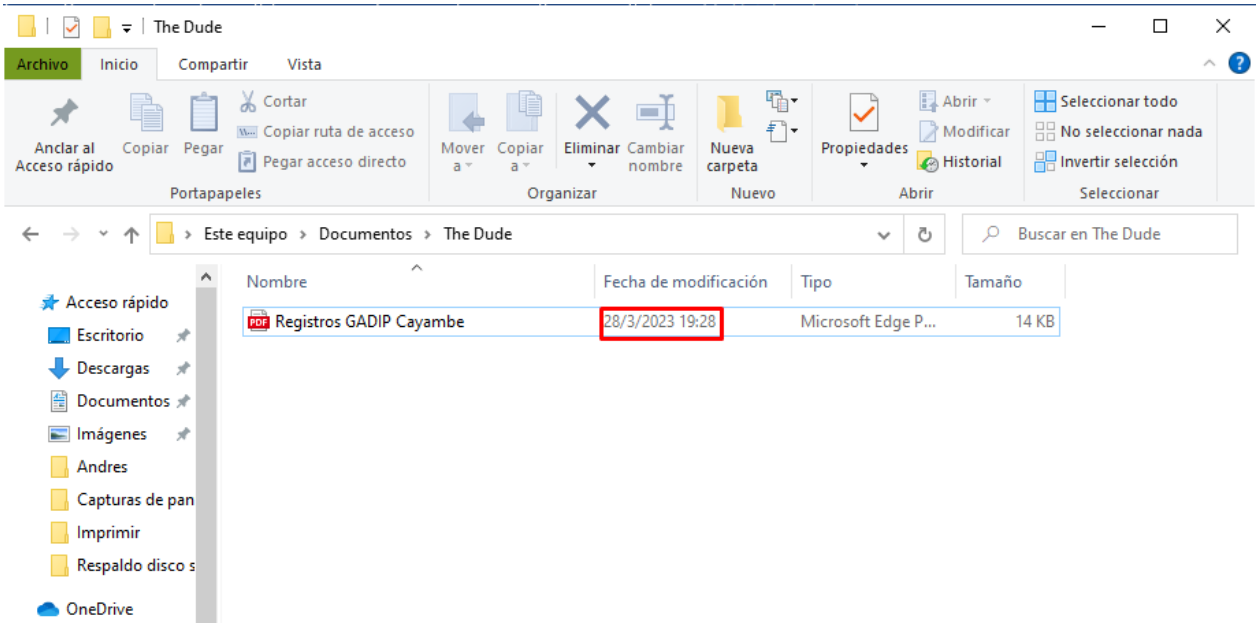
The Dude muestra el historial del dispositivo o la generación de informes, enlaces, configuraciones realizadas en la red, mensajes enviados, servicios configurados en cada dispositivo y descripciones generales de toda la red.

La figura muestra el historial de dispositivos de red y los informes generales de red, donde se representa como un archivo .pdf y la fecha de creación del informe.

Generación de Reportes o Historiales

Figura 45

Reportes del software The Dude



Fuente: (Aplicación The Dude)

4.4.4. Prueba de funcionamiento gestión de prestaciones

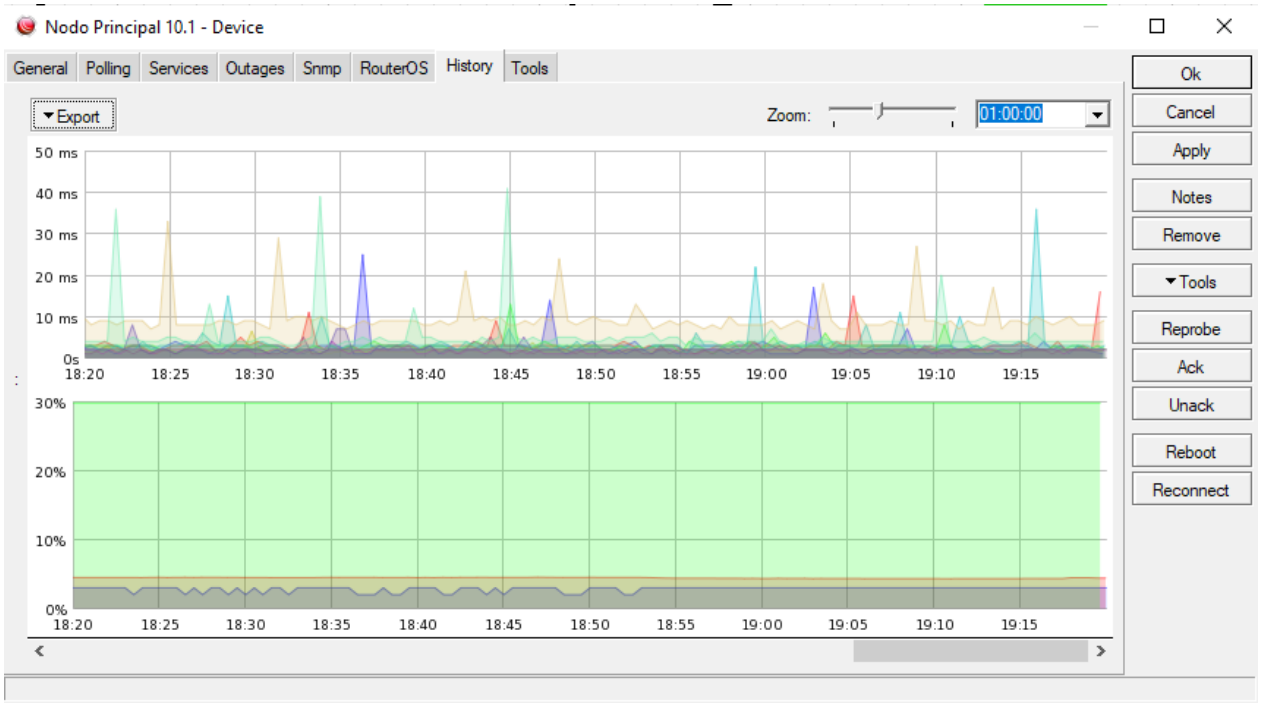
En la gestión de prestaciones se muestra un gráfico porcentual del rendimiento de varios dispositivos de red, como la memoria, el disco local y la tarjeta de red en la aplicación. Una prueba de rendimiento que genera datos estadísticos. The Dude representa un gráfico de las partes físicas y los recursos o servicios de cada entidad.

Aplicación The Dude

La Aplicación The Dude permite el generar y configurar los diagramas estadísticos sobre los recursos y servicios configurados en los dispositivos de red. En la **Figura 47 y Figura 48** muestra sobre el porcentaje restablecido en días, semana y mes del funcionamiento del dispositivo de red indicando sobre el correcto funcionamiento de los dispositivos de red.

Figura 46

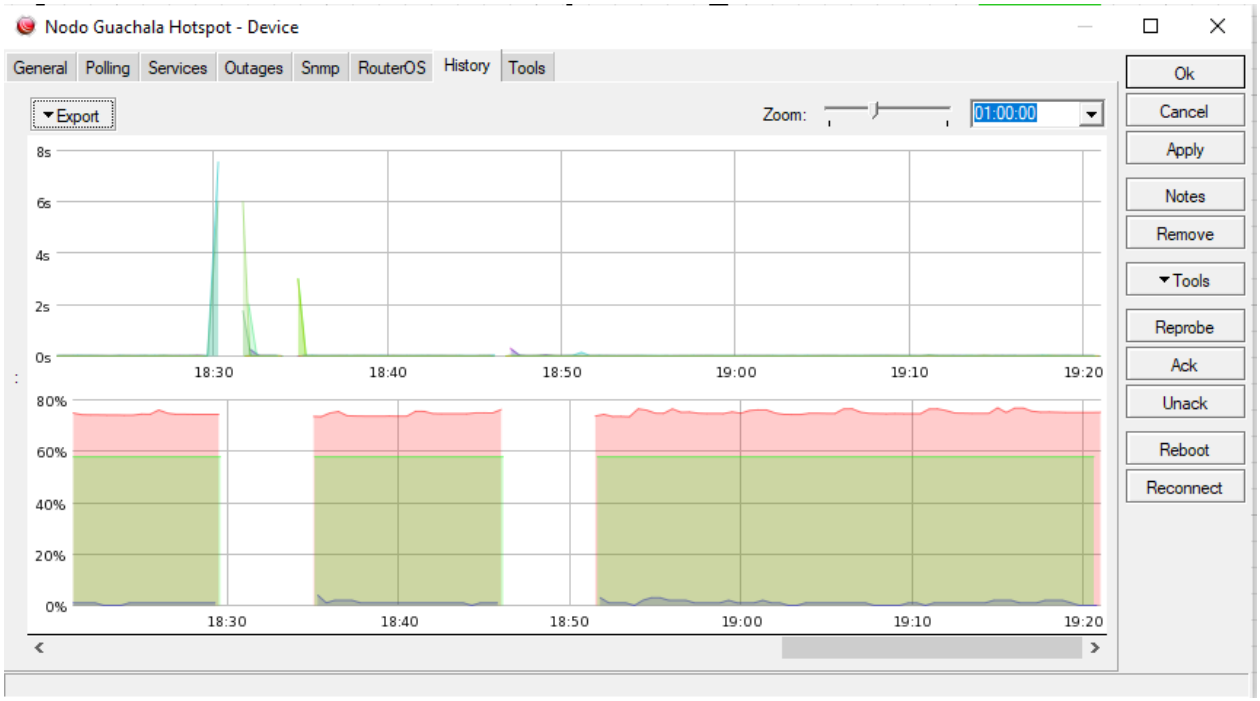
Diagrama estadístico Nodo Principal



Fuente: (Aplicación The Dude)

Figura 47

Diagrama estadístico Nodo-Guáchala



Fuente: (Aplicación The Dude)

Utilizando estadísticas gráficas, los administradores pueden obtener un porcentaje aproximado de dispositivos de red que están funcionando, indicando el rendimiento de cada recurso físico.

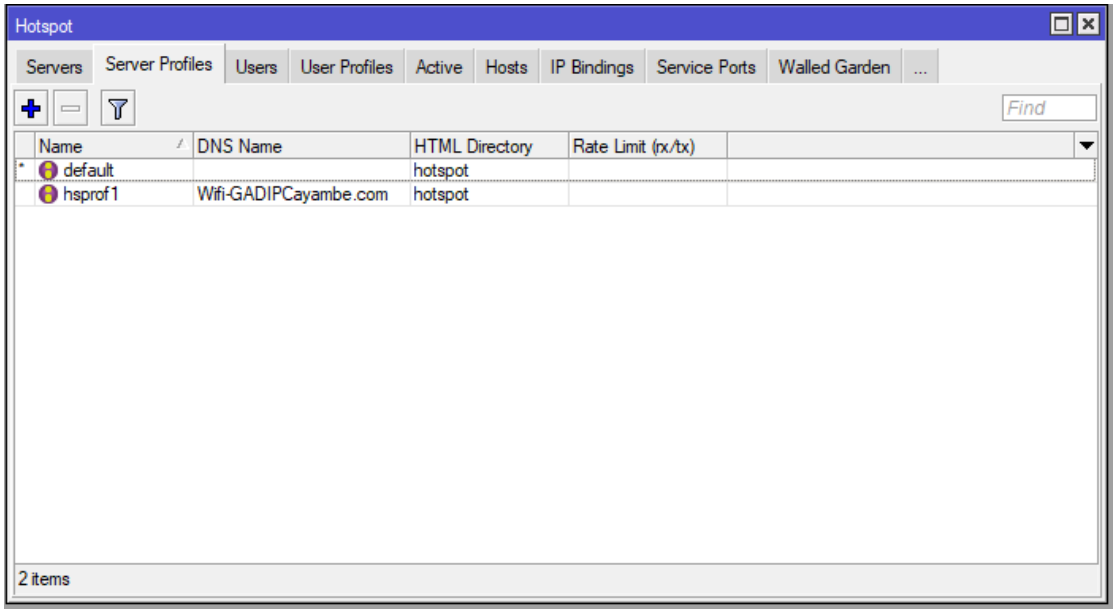
4.4.5. Prueba de funcionamiento gestión de seguridad

En la gestión de seguridad se establece la seguridad de acceso del personal técnico y deladministrador hacia la aplicación The Dude, y el sistema de Monitoreo y Portal Cautivo.

Como pruebas de funcionamiento se indica el funcionamiento del Portal Cautivo en el cual un usuario puede acceder al servicio de Internet Gratuito en la Zona central de Guáchala.

Figura 489

Administrador Hotspot



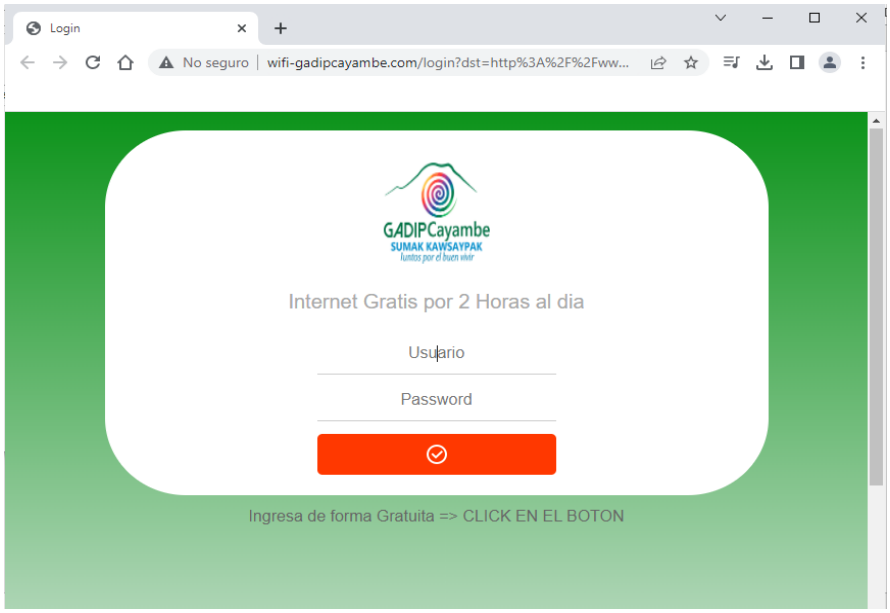
Fuente: (Sistema Operativo Mikrotik)

En la **Figura 49**, se muestra la página web donde el técnico administra los usuarios que se encuentran conectados a la red del Portal Cautivo Hotspot, indicando el tiempo de conexióny los datos establecidos para que pueda navegar en la Internet el usuario.

Ingreso al portal Cautivo Hotspot.

Figura 49

Página Web Portal Cautivo (Hotspot)



Fuente: (Sistema Operativo Windows 10)

En la Figura 50 se muestra la conexión y el ingreso como usuario para acceder al servicio de Internet gratuito.

El uso del Hotspot en la zona central de Guáchala permite a los usuarios acceder a la red sin saturación, lo que permite un servicio continuo e ininterrumpido, permitiendo a los usuarios utilizar el servicio con fines educativos, turísticos o personal.

5. CAPITULO V

Conclusiones y Recomendaciones

5.1. Conclusiones

La propuesta de la red inalámbrica presentada por el GADIP del municipio de Cayambe mejora algunos aspectos, permitiendo el desarrollo social y cultural dentro del lugar beneficiado teniendo en cuenta. Que el acceso universal a las tecnologías de la información y comunicación

Este proyecto, además de contar con enlaces que funcionan con el estándar 802.11 AC, también tiene una red doble. Velan diseñada con el mismo estándar para garantizar una buena conectividad e los usuarios.

Para el cálculo del ancho de banda se tomó en cuenta las aplicaciones que son más utilizadas como son redes sociales y videos de streaming. Por esta razón tanto las personas nativas y extranjeras suman un consumo aproximado de 25 Mbps como mínimo, para que una red funcione correctamente, siempre y cuando tenga un buen sistema de gestión

Como se sabe, la tecnología va avanzando a pasos agigantados. A pesar de esto, existen diferentes usuarios que no cuentan con la tecnología 5G en sus dispositivos móviles. Por este motivo en el proyecto se realizó un diseño en donde los Access Point tengan con doble banda, la 5G y la 2,4 Ghz. de esta manera, la red es más robusta, flexible y escalable.

La topología propuesta en este proyecto consta de un enlace de 4.5 km aproximadamente hacia un modo repetidor ubicado en un lugar estratégico dentro de la misma comunidad este nodo repetidor, ayudó a que exista conexión entre los nodos principales, a cargo del GADIP del municipio de Cayambe.

Para la simulación de los enlaces se utilizó la herramienta radio Mobile, la cual cuenta con. Múltiples herramientas que ayudan a ver tanto la latitud como la longitud y ver si un enlace es viable o no. De esta manera tuvimos un resultado de un 70%. De la zona despejada para realizar enlaces confiables y seguros.

En el presente diseño se utilizó el estándar 802.11ac. Debido a que la banda de 5 GHz es una banda libre y no existe mucha interferencia en Espectro electromagnético. En donde es de mucha importancia para la potencia de transmisión ganancia de la antena

En el presente proyecto para la parte de la gestión de la red mediante el modelo funcional FCAPS, se tomó en cuenta que ya existe un sistema. Implementado en el GADIP del municipio de Cayambe. Por lo cual se procedió a tomar las mismas. Áreas funcionales. pero aplicando nuevas políticas a los dispositivos que forman parte de esta nueva red.

A medida que las redes inalámbricas han ido creciendo, su gestión se ha vuelto más compleja, creándose procesos de planificación, seguimiento y control de redes, tal como lo define ISO en las áreas funcionales del modelo de gestión FCAPS para su uso en este proyecto.

5.2. Recomendaciones

este diseño sirve como modelo a aplicarse a los lugares en donde no existe el sistema de Internet, debido a que no existe una línea de vista directa, en el presente trabajo, se muestran los dispositivos que pueden ser utilizados para los enlaces punto a punto.

Hoy usar el mismo tipo de. Equipos para tener enlaces estables, asimismo utilizar equipos que tengan un buen rendimiento Para que en un futuro no exista por degradación de los equipos

Tomar en cuenta las leyes y normas que rigen en el país para la interconexión de los nodos. Llenar los formularios en el momento de implementar para que los enlaces estuviesen debidamente legalizados. Para la operación del servicio y así evitar sanciones por parte de los organismos de control.

Se recomienda tener un técnico capacitado para el monitoreo de la red. Él será el encargado de aplicar el sistema de seguridad y gestionar la red, según sea lo conveniente para que la red funcione correctamente.

al momento de conectarse, hay que tener en cuenta que el dispositivo del usuario sea compatible con la red 5G, de no tener un dispositivo con esta tecnología los equipos son doble banda y puede trabajar en la banda 2,4 Ghz sin ningún problema.

Si la demanda de usuarios en la red inalámbrica se incrementa, lo único que tendría que aumentar sería Hoy el ancho de banda. Esto se configuraría a través del administrador de la red. Cabe recalcar que los dispositivos Puntos de acceso (AP)pueden soportar Hoy, velocidades de hasta 300 Mbps. Hoy y puede soportar hasta 200 usuarios al mismo tiempo por cada equipo. Este proyecto consta de 3 Access Point.

Es importante que los equipos elegidos Hoy en el diseño, soporte en el protocolo SMTP. Para poder ser activados y monitoreados de esta manera, tener el control de la red. Y brindar un servicio de Internet de forma estable.

Hoy es importante que el equipo elegido en el diseño soporte el protocolo SMTP. Para poder. Ser monitoreados y de esta manera tener un control total de la red para brindar. Un servicio de forma estable.

5.3.Bibliografía

Alegsa, L. (2016). INFORMÁTICA Y TECNOLOGÍA. *Seguridad En Redes Inalámbricas*. Retrieved from http://www.alegsa.com.ar/Dic/seguridad_en_redes_inalambricas.php

Ali, S., Osman, T., Mannan, M., & Youssef, A. (2019). Captive portals. *On Privacy Risks of Public WiFi Captive Portals*. Retrieved from https://www.researchgate.net/publication/334248860_On_Privacy_Risks_of_Public_WiFi_Captive_Portals

Benítez, P. (2016). CAPÍTULO 2 : Introducción a la gestión. *MODELO FCAPS*, 4–18.

Campos, T. (2019). *ESTÁNDAR WIFI 802.11*. 29.

Capelle, C. (2019). Techlandia. Retrieved from WPA2 Personal contra Enterprise website: https://techlandia.com/wpa2-personal-contra-enterprise-info_206407/ Cerro, Y. (2015). Redes Inalámbricas.

Copyright Network. (2014). THE FREERADIUS TECHNICAL GUIDE. *RADIUS*, (C), 1–58. Retrieved from http://networkradius.com/doc/FreeRADIUS Technical Guide.pdf

Estrada. (2013). REDES INALAMBRICAS DE ÁREA EXTENSA (WWAN)WWAN Tienen el alcance más extenso. Retrieved from REDES INALAMBRICAS DE ÁREA EXTENSA (WWAN) website: https://redeswwan.wordpress.com/2013/06/09/redes-inalambricas-de-area-extensa-wwanwwan-tienen-el-alcance-mas/

Herrera Ramírez, E., Díaz Ramírez, A., & Calafate, C. T. (2007). Desarrollando el estándar IEEE 802.11n, un paso adelante en WLAN. *Group*.

IBM Knowledge Center. (25AD). Aplicacion, protocolos y servicios. Retrieved from Protocolo de autenticación extensible website:

https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_72/rzaiy/rzaiyeap.htm

IEEE. (2012). Familia IEEE 802.11. *Redes de Área Local Inalámbricas*, 66–73.

IEEEStandards. (2016). Topologias de una Red Inalámbrica. Retrieved from http://ieeestandards.galeon.com/aficiones1573328.html

Lorenzana, V. R. (2018). *Redes inalámbricas*.

Martínez, J. (2018). Qué es un radioenlace. *RADIOENLACE*. Retrieved from https://medium.com/@jlmartinez.es/qué-es-un-radioenlace-159ab9a66775

Mensoza, H. (2017). Antenas Sectoriales. *Antenas Sectoriales*, 2.

MINISTERIO DE TELECOMINICACIONES. (2016). *PLAN DE TELECOMUNICACIONES*. Nuevas Tecnologias. (2010). GESTION DE REDES. Retrieved from http://ntmoduloredes.blogspot.com/2010/02/protocolo-cmip.html

OpManager, & ManageEngine. (2019). Administración de Red. Retrieved from Software de monitoreo de red - ManageEngine website: https://www.manageengine.com/es/network-monitoring/network-management.html

Pablo, P., & Cepeda, C. (2007). *DISEÑO E IMPLEMENTACIÓN DE UN CLIENTE RADIUS EN LINUX*.

Peña, Joan Domingo Gámiz Caro, Juan Grau i Saldes, A. (2003). Diseño de un sistema de radioenlace para comunicaciones en el ámbito industrial. *Comunicaciones En El Entorno Industrial*, 369. Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81906/6/ggonzalezmeneTFG0618memoria.pdf

Pérez, C., Jesús, H. De, Salazar, G., Rocío, K., Inalámbricas, R., & Inalámbricas, R. (2006). Redes Inalámbricas 802.11n el Nuevo Estándar. *Conciencia Tecnológica*, 2–3.

Pietrosemoli, E. (2007). Redes Inalambricas. Retrieved from Antena y Cables website: https://slideplayer.es/slide/11180023/

Pillou, J. F. (2008). WLAN LAN inalámbrica.

Radio Comunicaciones. (2006). *Estándares inalámbricos (Pasado , presente y futuro de las redes wireless). 2006*.

Ramírez, J., & Díaz, J. V. (2008). Las redes inalámbricas, más ventajas que desventajas. *Ciencia Administrativa*, *2*, 85–89.

Rouse, M. (2005). Mobile Computing. Retrieved from Portal Cautivo website: https://searchmobilecomputing.techtarget.com/definition/captive-portal

Ruesca, P. (2016a). ANTENAS DIRECCIONALES. Retrieved from Teoria de Antenas website: http://www.radiocomunicaciones.net/radio/teoria-de-antenas/

Ruesca, P. (2016b). ANTENAS OMNIDIRECCIONALES. Retrieved from ANTENAS OMNIDIRECCIONALES website: http://www.radiocomunicaciones.net/radio/antenas-omnidireccionales/

Ruesca, P. (2016c). Radio comunicaciones. Retrieved from RADIO ENLACE website: http://www.radiocomunicaciones.net/radio/radio-enlace-que-es-un-radioenlace/

Salazar, J. (2012). Redes Inalámbricas. In *Redes* (Vol. 2). Retrieved from http://www3.uah.es/vivatacademia/ficheros/n54/redesinalam.PDF

SILICON LABS. (2016). WPA2 / WPA Enterprise. *WPA Enterprise*, 0–9.

Sosa, V. (2006). SNMP. *Protocolo SNMP*, *1*(versión 1).

Turismo. (2012). San Luis de Guachalá: historia, arte y cultura desde la mitad del mundo. Retrieved from http://turismo.mas.ec/sin-categoria/guachala-cayambe/

University of Southern Indiana. (2008). *Network Management*. *1*, 1–21. Retrieved from https://www.usi.edu/business/aforough/Chapter 20.pdf

Urueña, M., & Larrabeiti, D. (2005). *Contribución al diseño de arquitecturas distribuidas de nodos de red programables*. 250. https://doi.org/http://hdl.handle.net/10016/11415

WatchGuard Technologies. (2019). Establecer el Método de Autenticación Inalámbrica. Retrieved from WPA y WPA2 con Claves Precompartidas website: https://www.watchguard.com/help/docs/help-center/es-419/Content/es-419/Fireware/wireless/wireless_auth_method_set_c.html?TocPath=Inalámbrico%7CConfiguración Inalámbrica de Firebox%7CAcerca de la Configuración de Seguridad Inalámbrica%7C_____1

Wireless Networks. (2015). *INTRODUCCIÓN A LAS REDES INALÁMBRICAS*. 3–30.

Wix. (2015). RED DE MICROONDAS. Retrieved from Zonas de Fresnel website: https://yadira-19982012.wixsite.com/fashion-blog-es/single-post/2015/11/24/Zonas-de-Fresnel

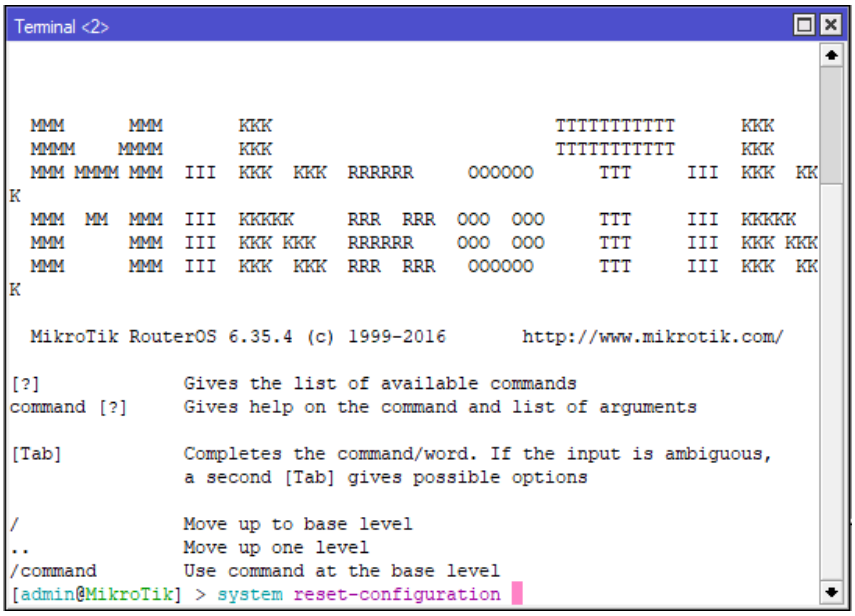
WNI México S.A. de C.V. (2012). El nuevo estándar inalámbrico 802.11ac. Retrieved from Wireless Solution website: https://www.wni.mx/index.php?option=com_content&view=article&id=75:80211ac&catid=31:general&Itemid=79

ANEXOS

6.1. ANEXO A: Manual de configuración enlaces Punto a Punto IEEE 802.11AC

Como primer paso reiniciamos el equipo a modo de fábrica con el comando **system reset-configuration**

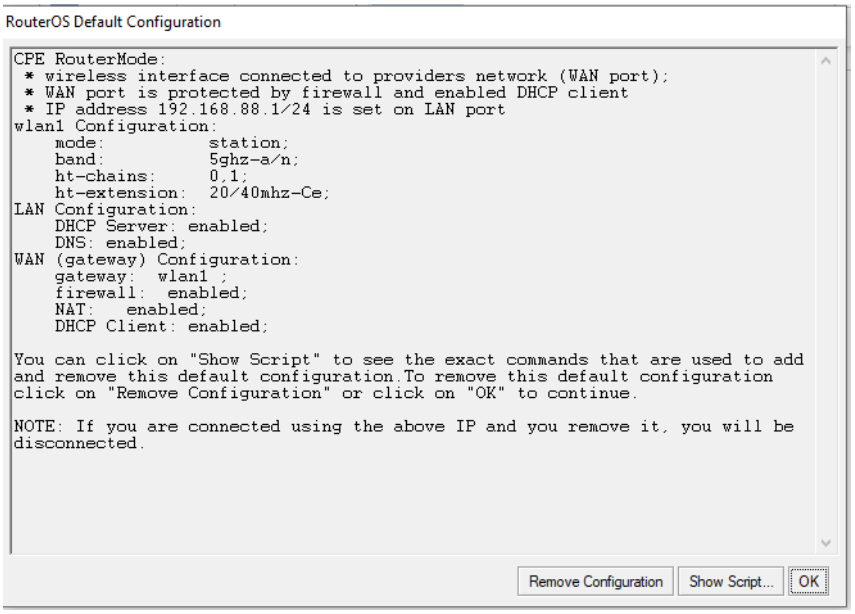
Figura A1



En la imagen A1 se muestra el reinicio del equipo a valores de fábrica confirmar escribimos la letra **y** para continuar

Una vez reiniciado el equipo aparece una ventana para confirmar si desea remover las configuraciones anteriores, para este caso damos clic en la opción remove configuration

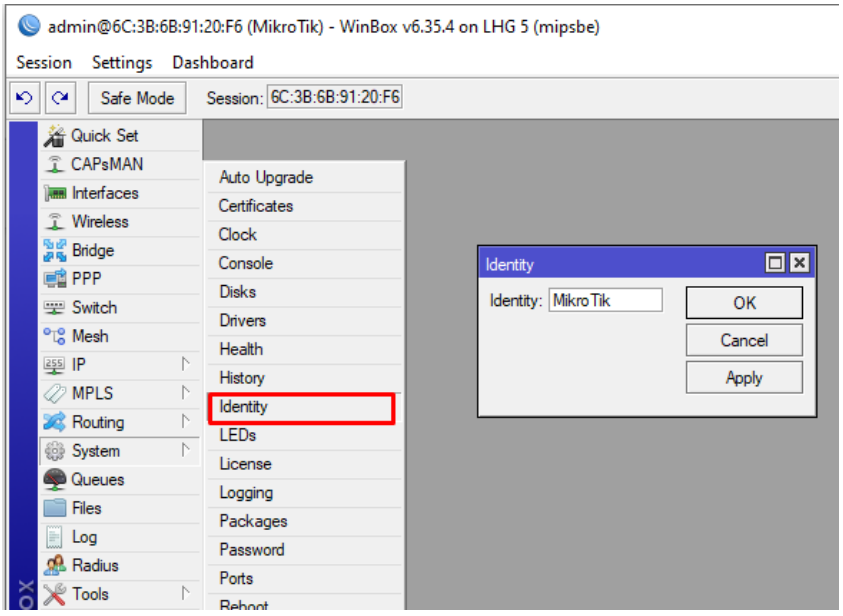
Figura A2



En la figura A2 se muestra el mensaje que envía el router al iniciar por primera vez y como primer paso vamos a poner un nombre que identifique el equipo emisor

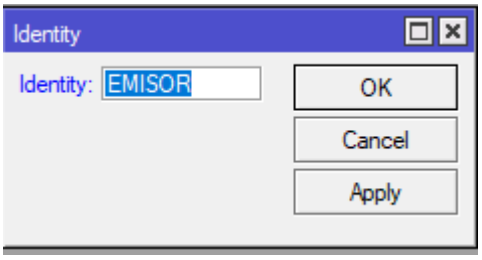
Para esto vamos a ingresar a la opción de system > identiti

Figura A3



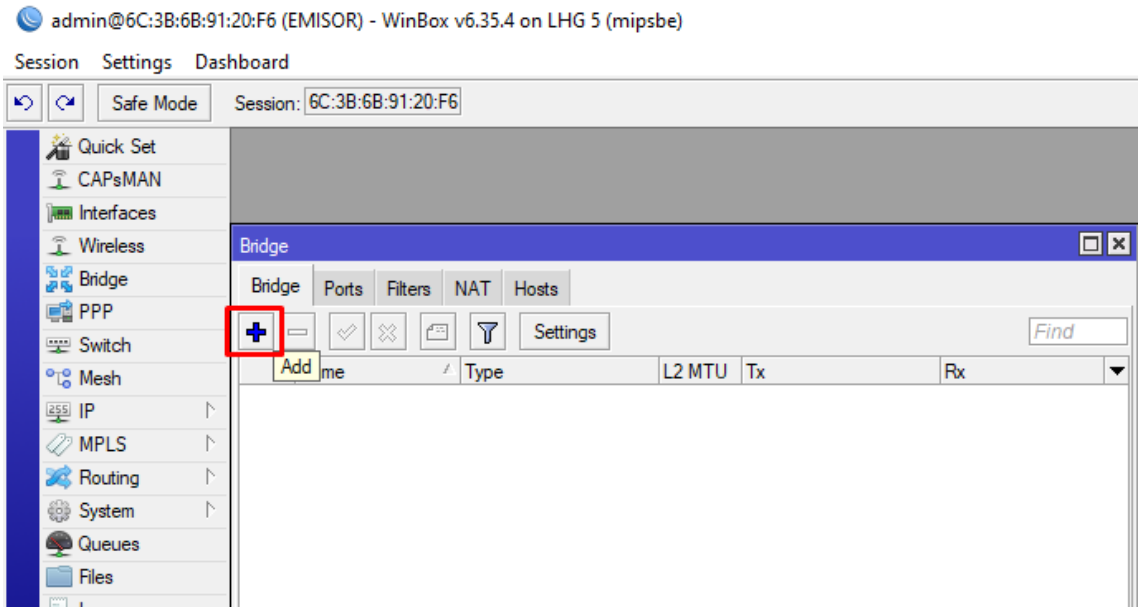
En la figura A3 se muestra la configuración en donde se le da un identi a a la antena, Escribimos el nombre del equipo emisor para el caso escribimos la palabra EMISOR

Figura A4



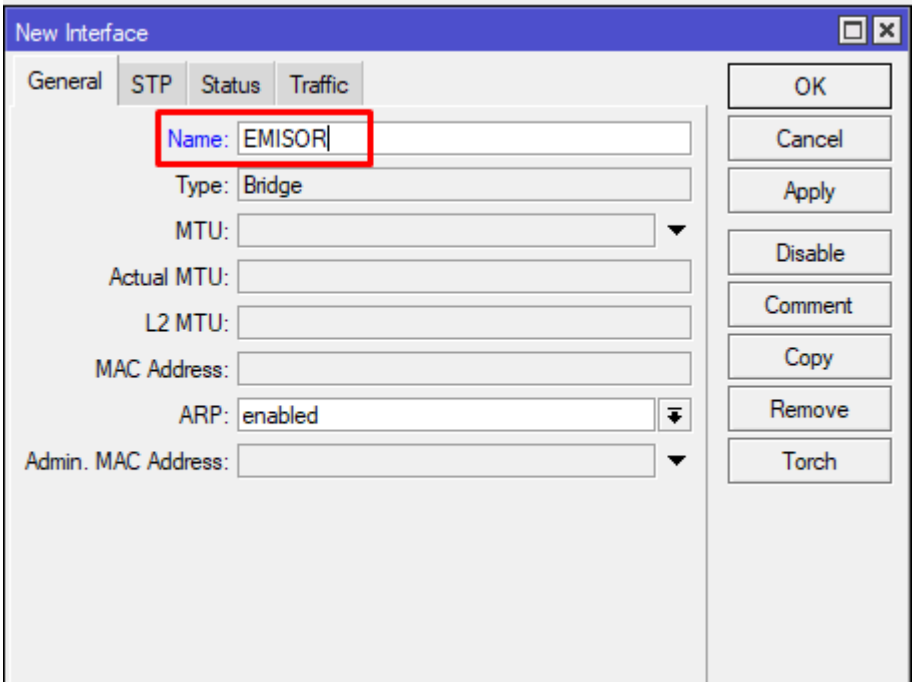
En la figura A4 se muestra cómo quedará nombrado el identity una vez ya identificado el equipo creamos un bridge

Figura A5



Colocamos el nombre de emisor

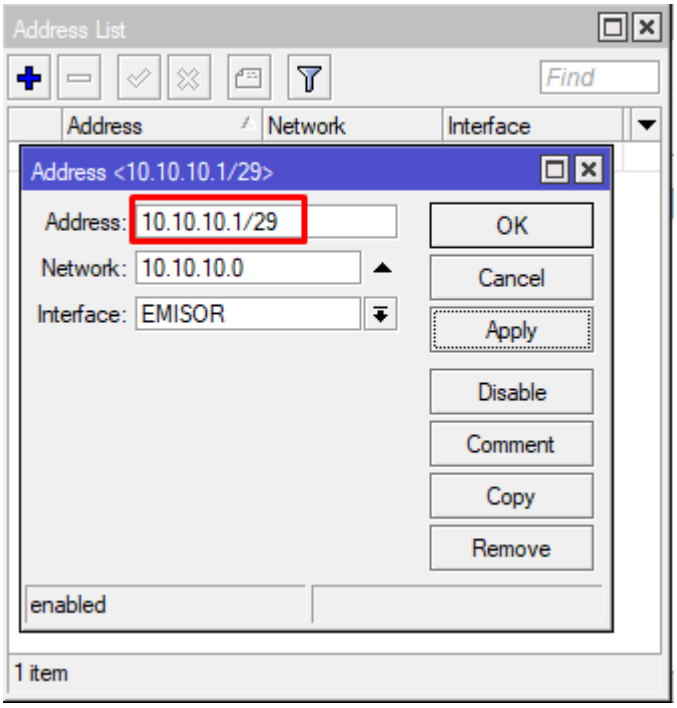
Figura A6



En la figura 55 se muestra la configuración del bridge creado en donde se asigna el nombre que tendrá la interfaz de la antena

La ip asignada es la 10.10.10.1/29 esta IP se la toma del direccionamiento IP realizado en el diseño

Figura A7

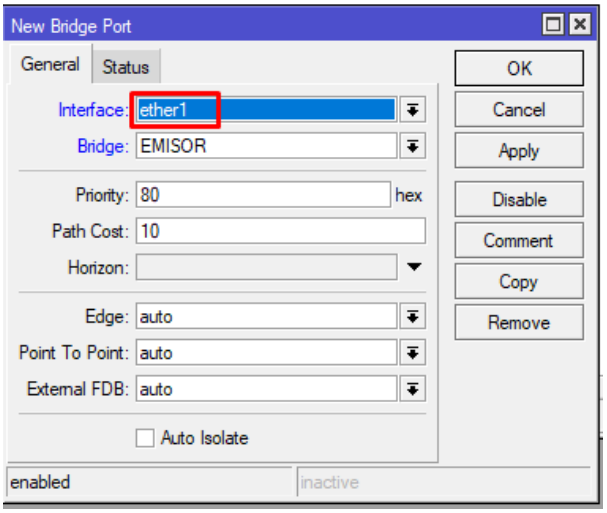


En la figura A7 se muestra la configuración de la dirección IP p para el emisor en este caso 10.10. 10. 1 máscara 29, una vez asignada la IP la máscara y la interfaz aplicamos y guardamos

Una vez asignada la IP la máscara y la interfaz aplicamos y guardamos

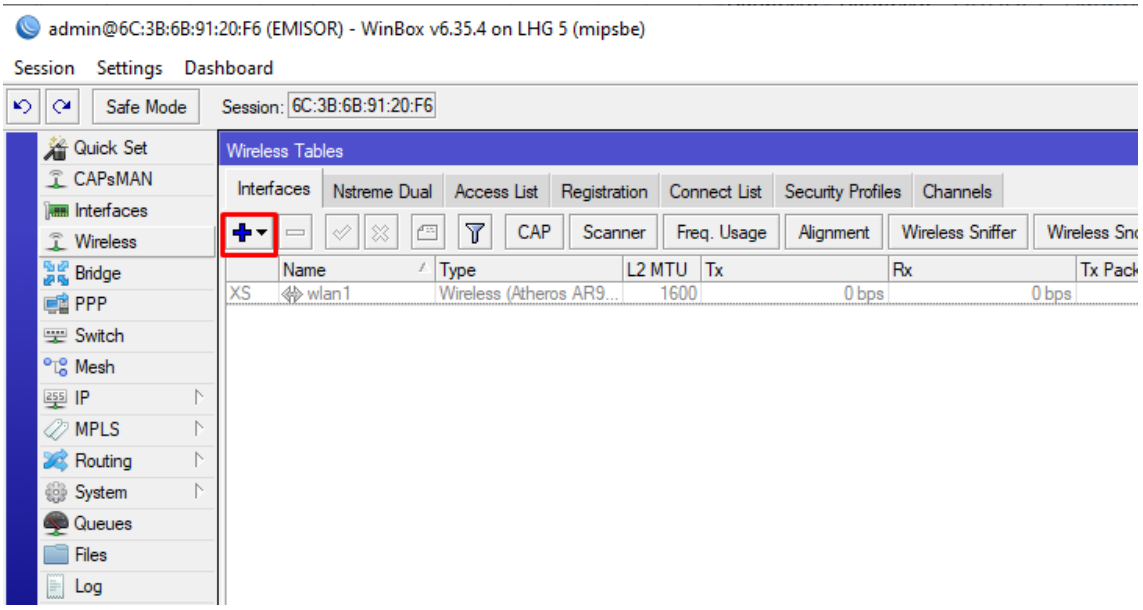
En la misma interfaz bridge se asignan los puertos de las interfaces la cableada y a inalámbrica.

Figura A8



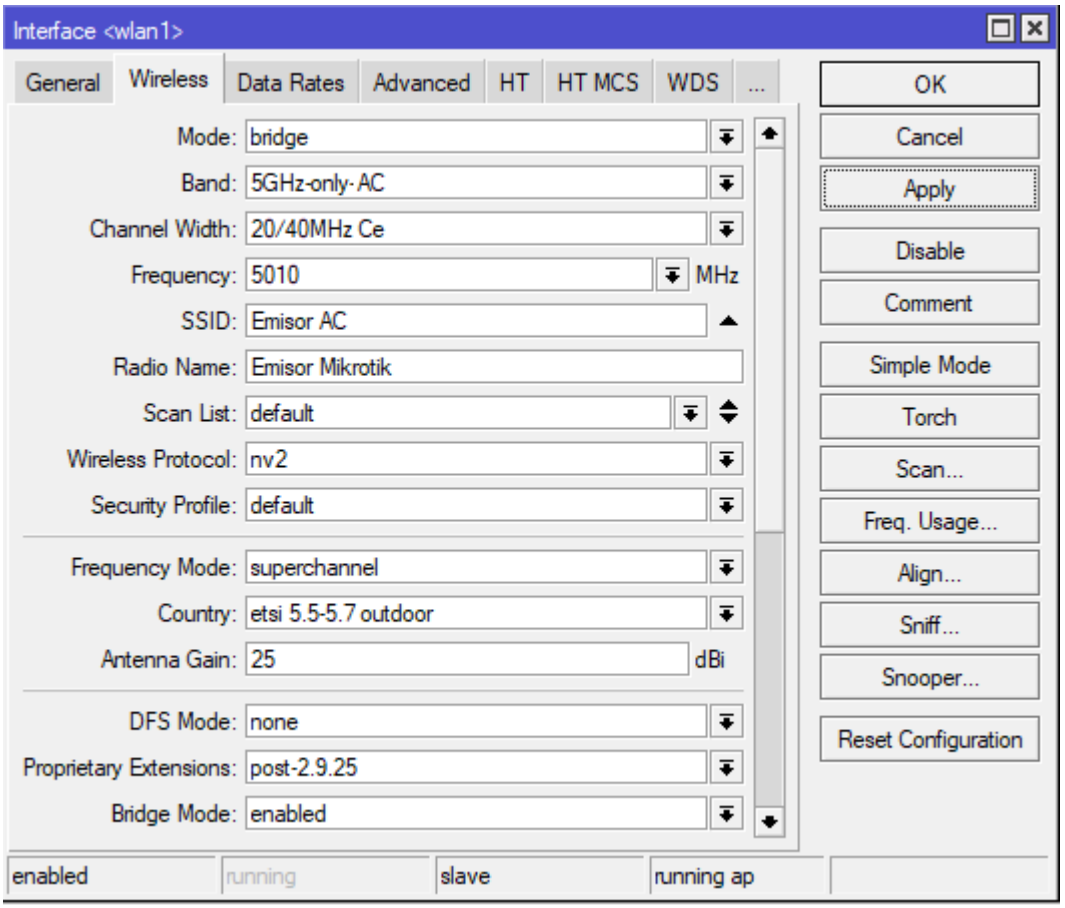
En la opción wireless se configurara la antena en modo AP

Figura A9



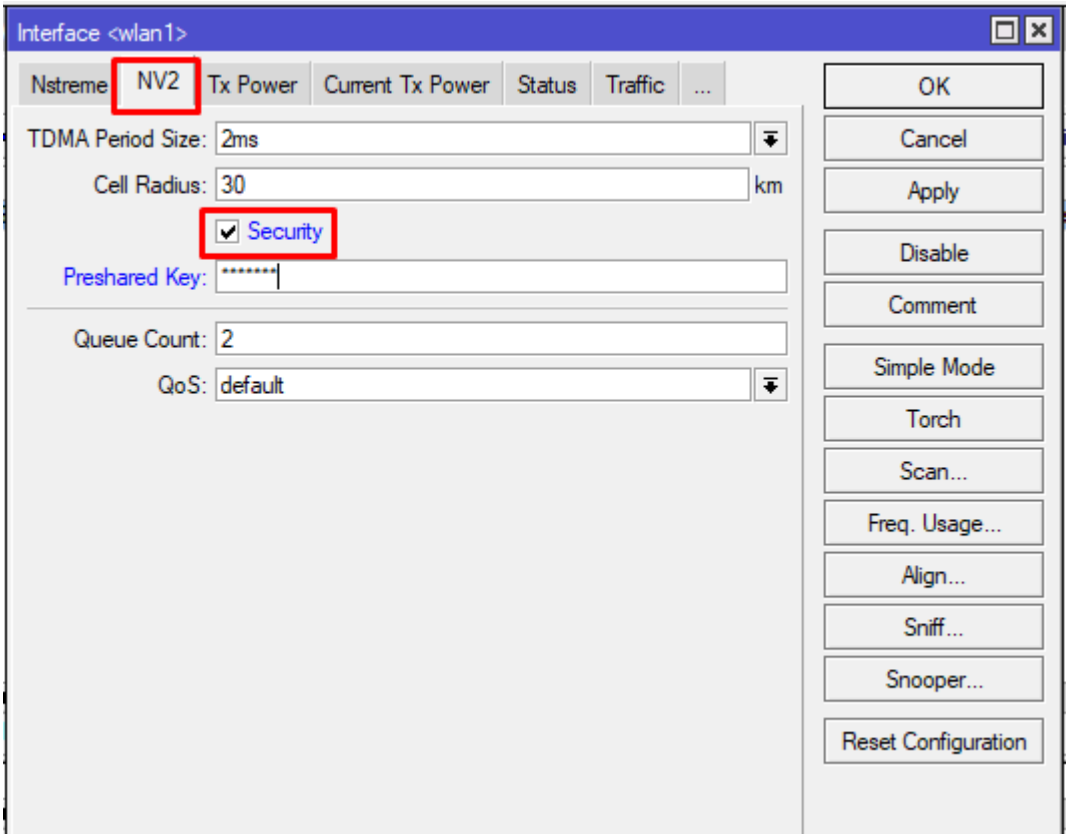
En la figura A9 se muestra la configuración de las interfaces, En la opción wireless presionamos la opción de agregar posteriormente aparecerá una pantalla en donde se configura el modo de trabajo la frecuencia el canal el emisor el Sid un protocolo de seguridad, la frecuencia en la que va a trabajar y la ganancia de la antena.

Figura A10



En la figura A10 se puede observar que el modo de trabajo será en modo bridge en la banda que trabajará será en la banda ac el canal de frecuencia es de 20 y 40 MHz la frecuencia para esta configuración se utilizó de 5010 el Sid se llama emisora c el radio se llama emisor marketing se utilizará el protocolo NB dos el modo de de frecuencia super channel, el country será el 5.5-5.7 outdoor y la potencia de la antena será de 25 dbi

Figura A11

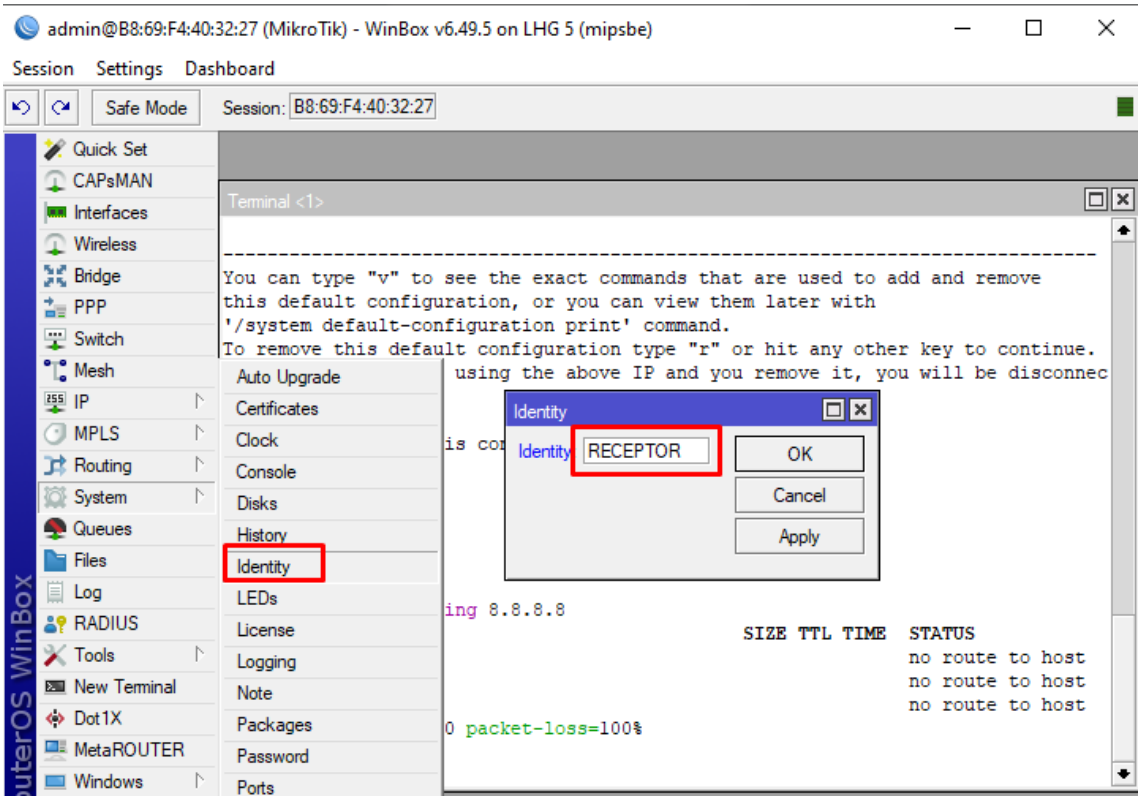


En la figura A11 se muestra la configuración del protocolo en web dos en donde se selecciona la opción Security y se coloca una contraseña para este caso es del 1 al 8

con eso se da por concluido la configuración de la antena emisora.

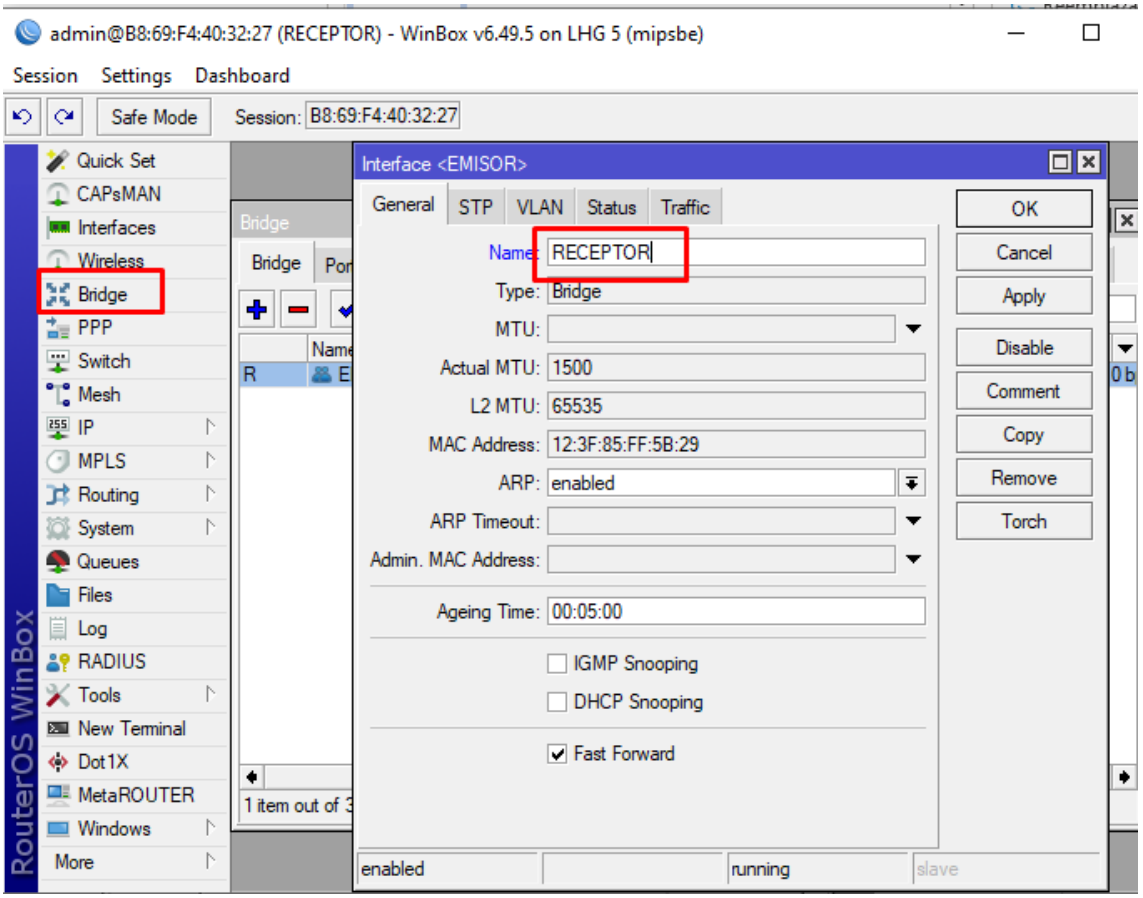
A continuación, se muestra la configuración de la antena receptora

Figura A12



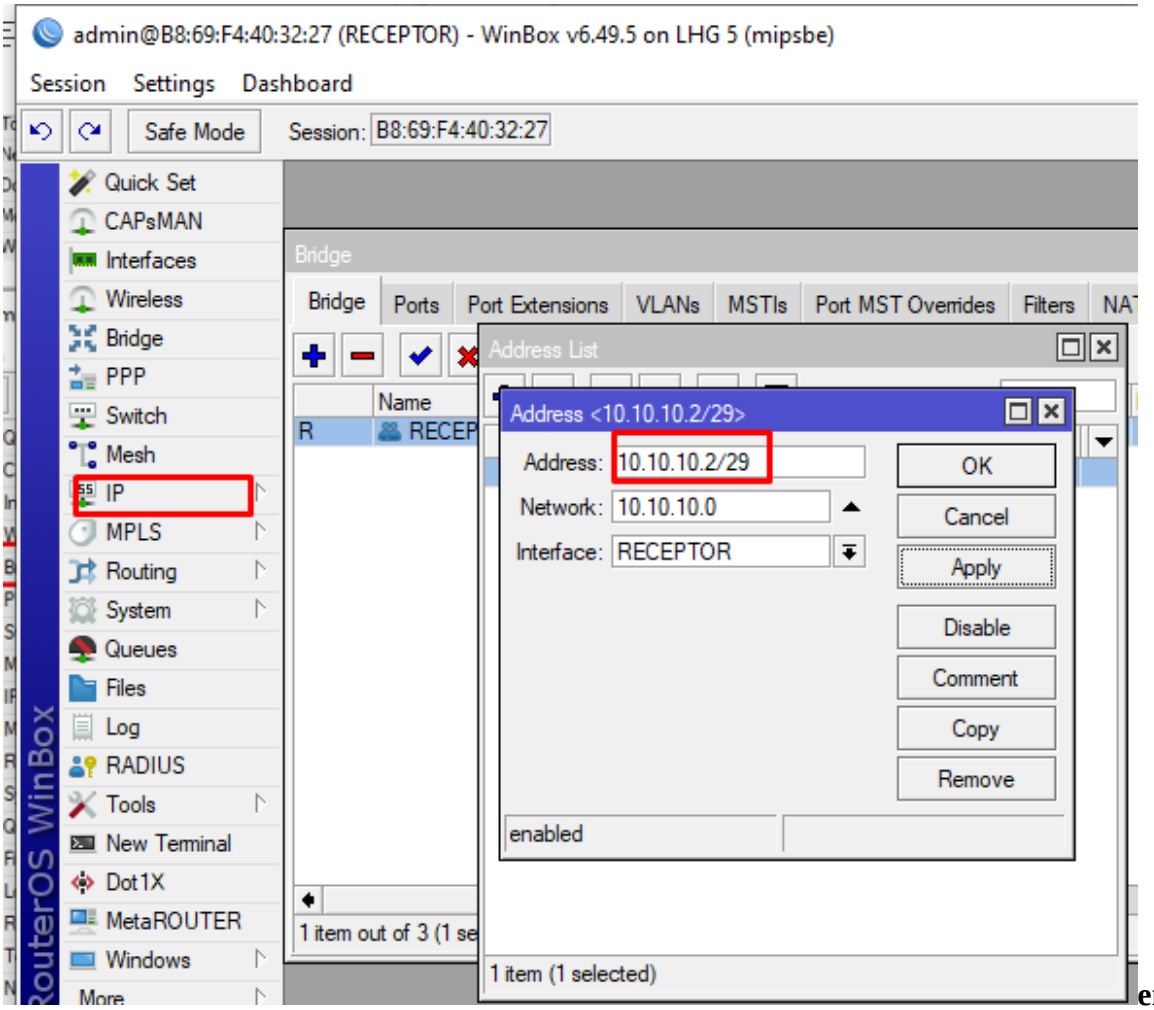
En la figura A12 se muestra la configuración de la antena emisora, como primer paso como en la antena emisora se procede a configurar un identi para poder identificar la antena.

Figura A13



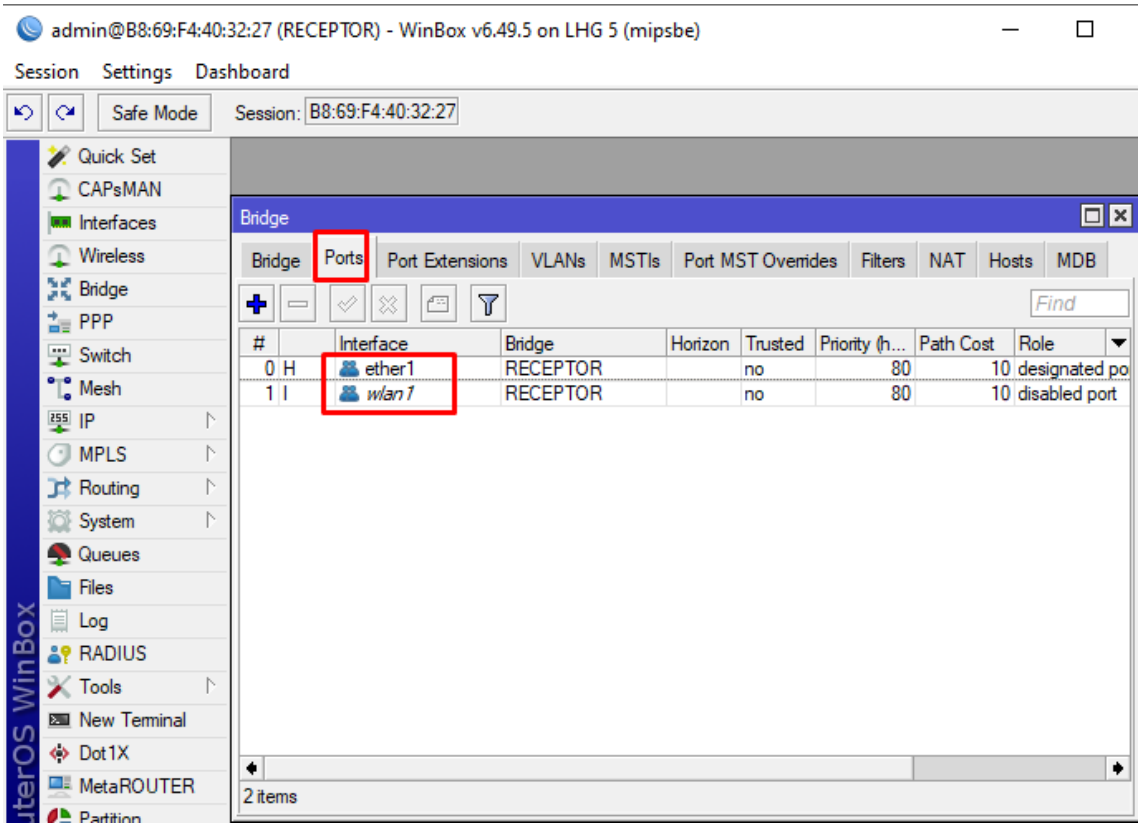
nunca en la figura A13 se muestra la configuración del bridge creado para la antena emisora se nombra como receptor guardamos la configuración con aplicar y ok

Figura A14



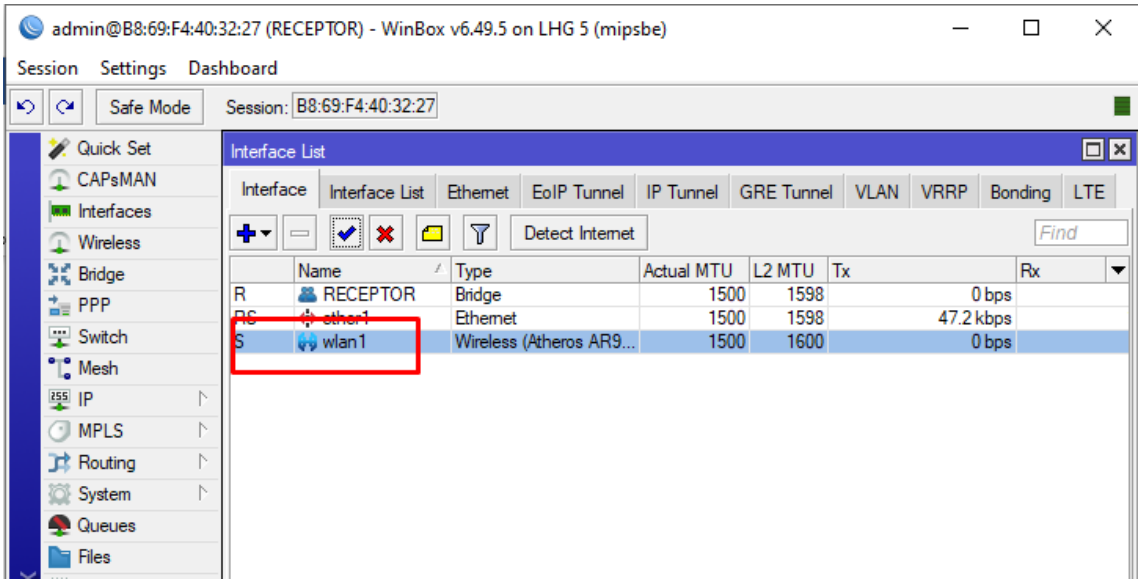
en la figura A14 se muestra la configuración de las direcciones IP en este caso se asigna la dirección 10.10. 10.2 máscara 29 para el equipo receptor y esto se asignado a la interfaz del bridge llamado receptor

Figura A15



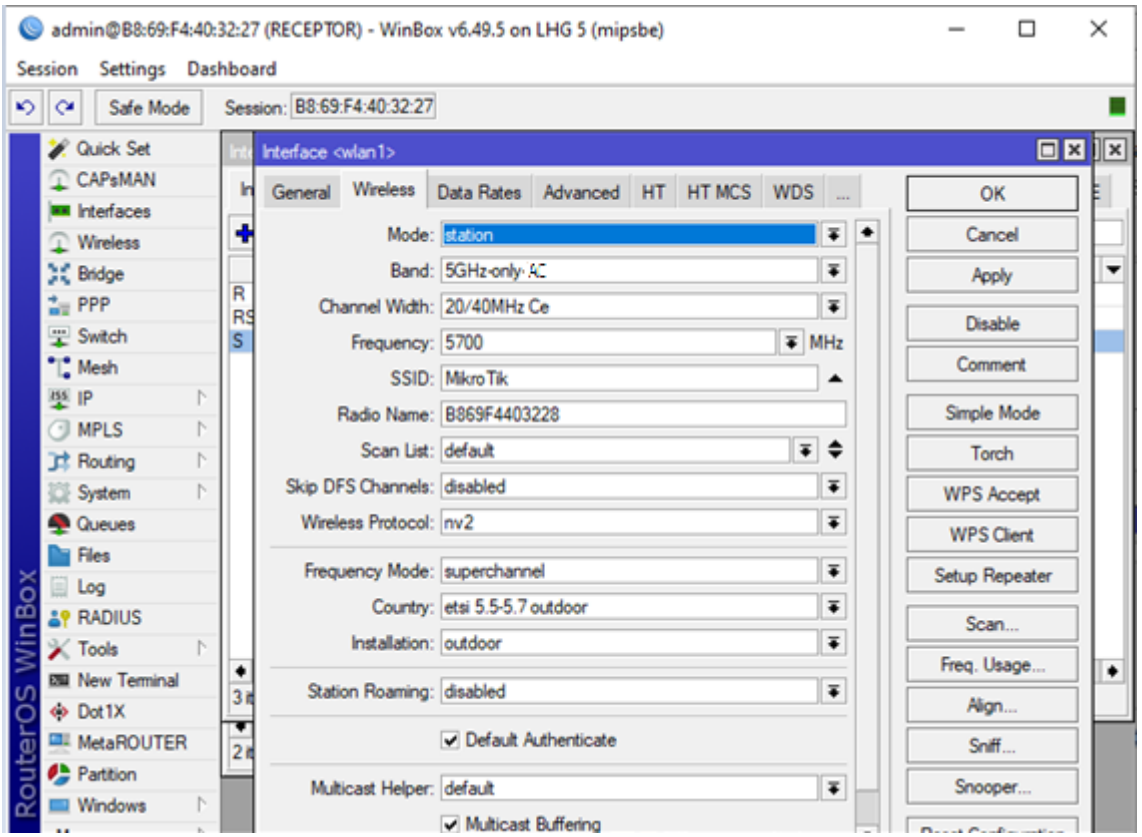
en la figura A15 se muestra la asignación de los puertos al bridge creado en este caso el bridge receptor

Figura A16



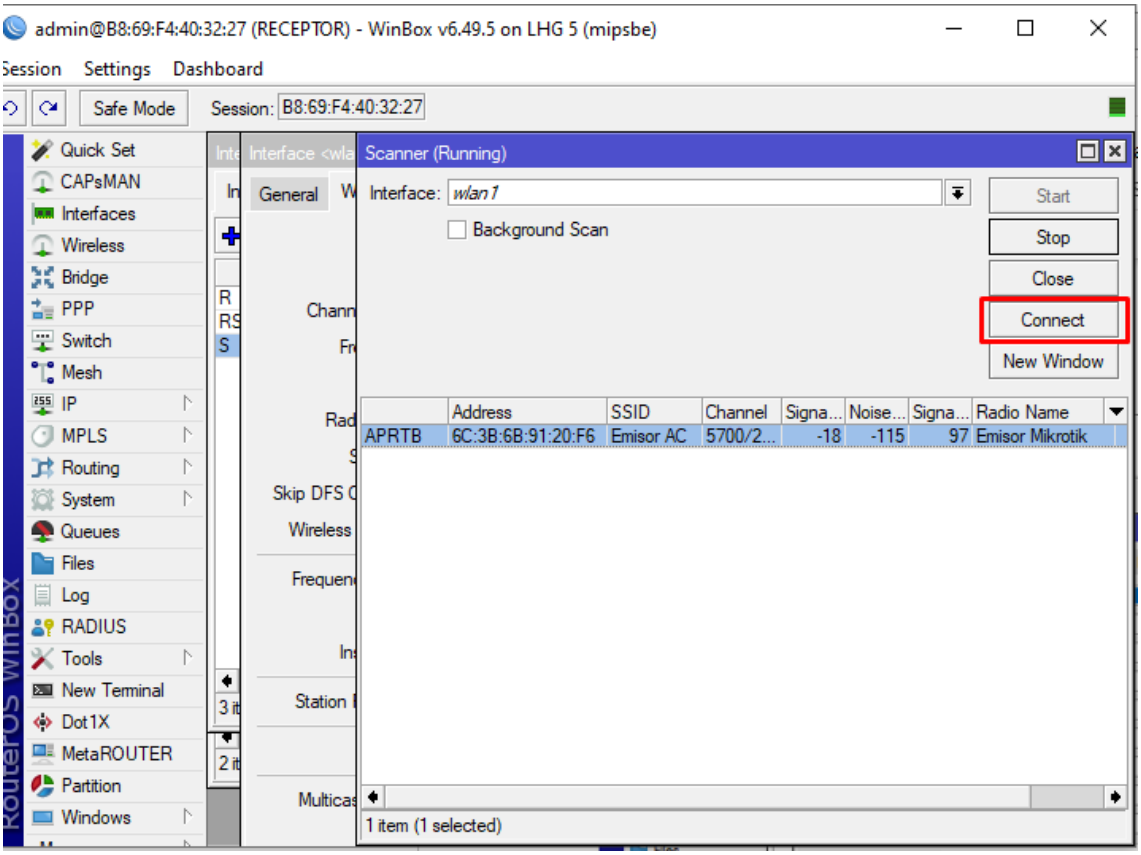
En la figura A16 se muestra la configuración del puerto doblan para el anclaje a la antena emisora

Figura A17



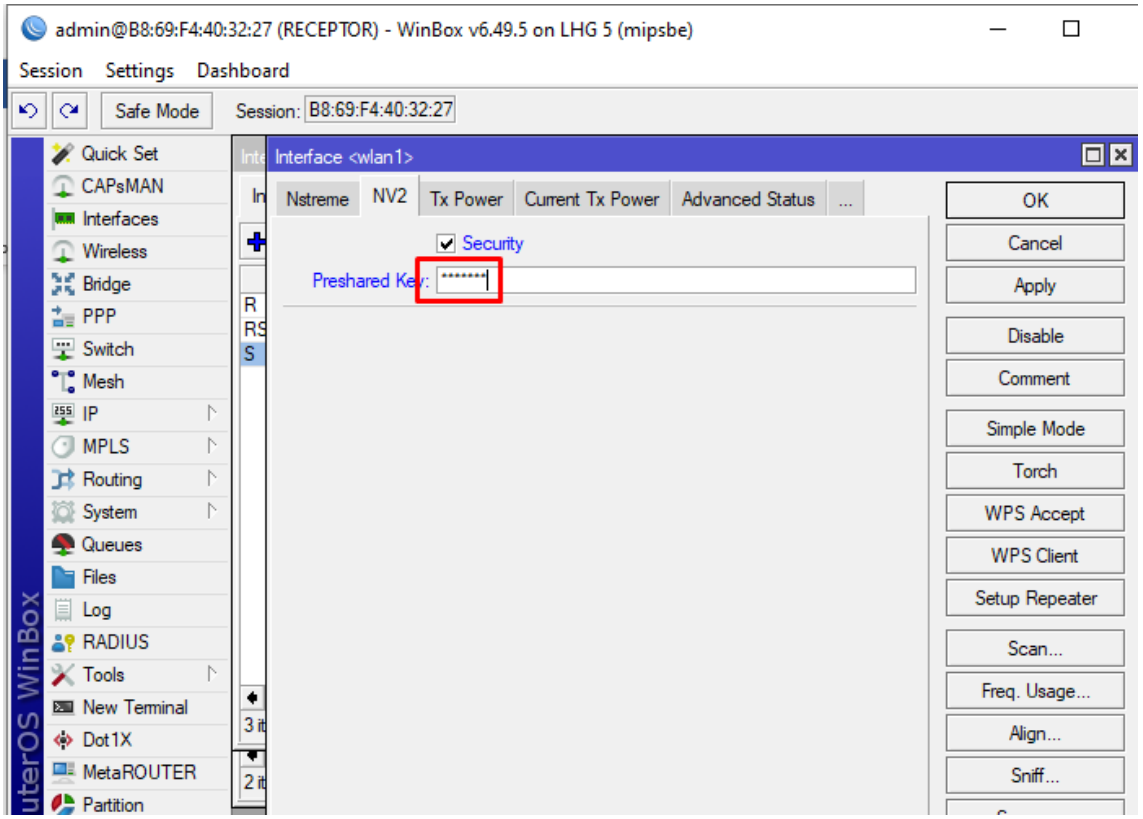
En la figura A17 se muestra la configuración de la interfaz antes de activada con el nombre estación banda de 5 GHz el canal frecuencia el essid el protocolo Nv2 dos y la frecuencia debe ser super channel

Figura A18



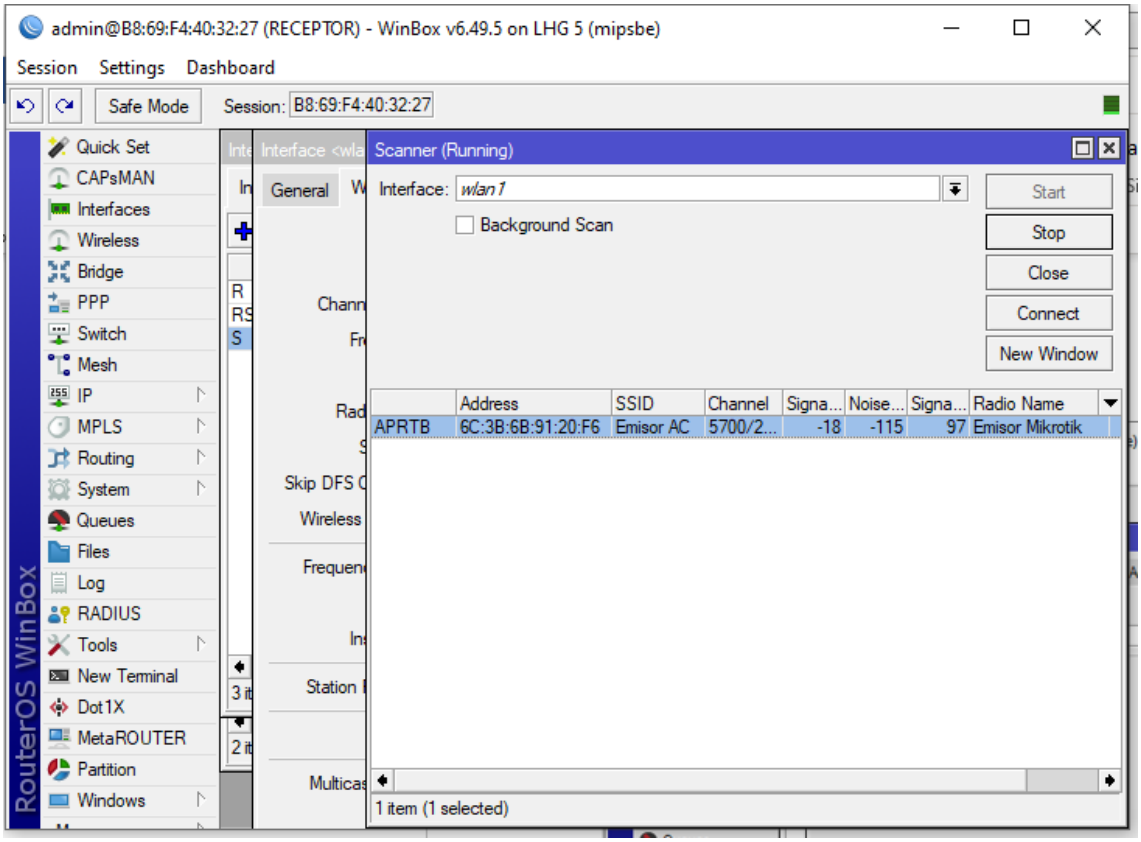
En la figura A18 se muestra la opción de escáner en donde aparece el Emisor AC con una potencia ideal para realizarse el enlace seleccionamos y presionamos el botón conectar

Figura A19



en la figura A19 se muestra la configuración del protocolo nv2 en donde se debe asignar la contraseña configurada en el emisor

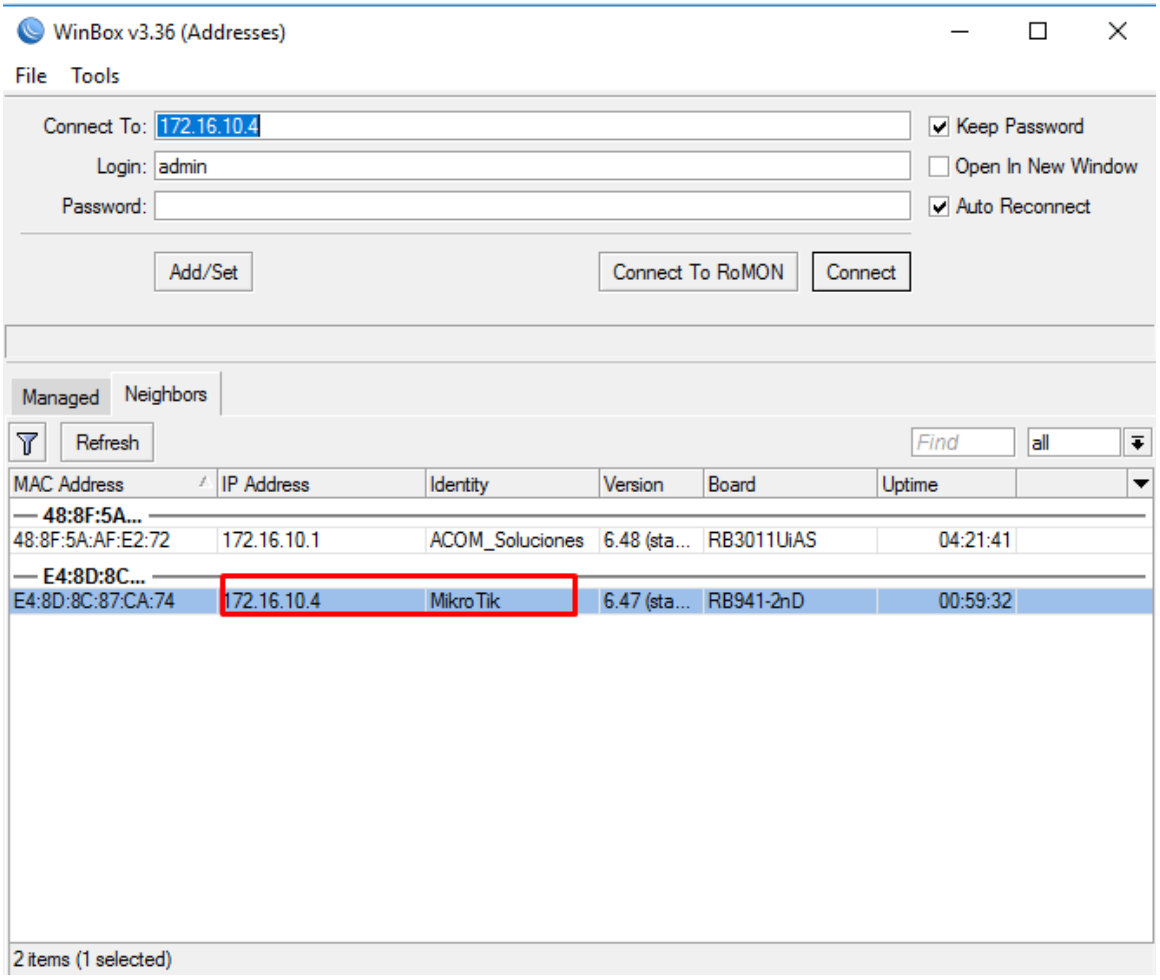
Figura A20



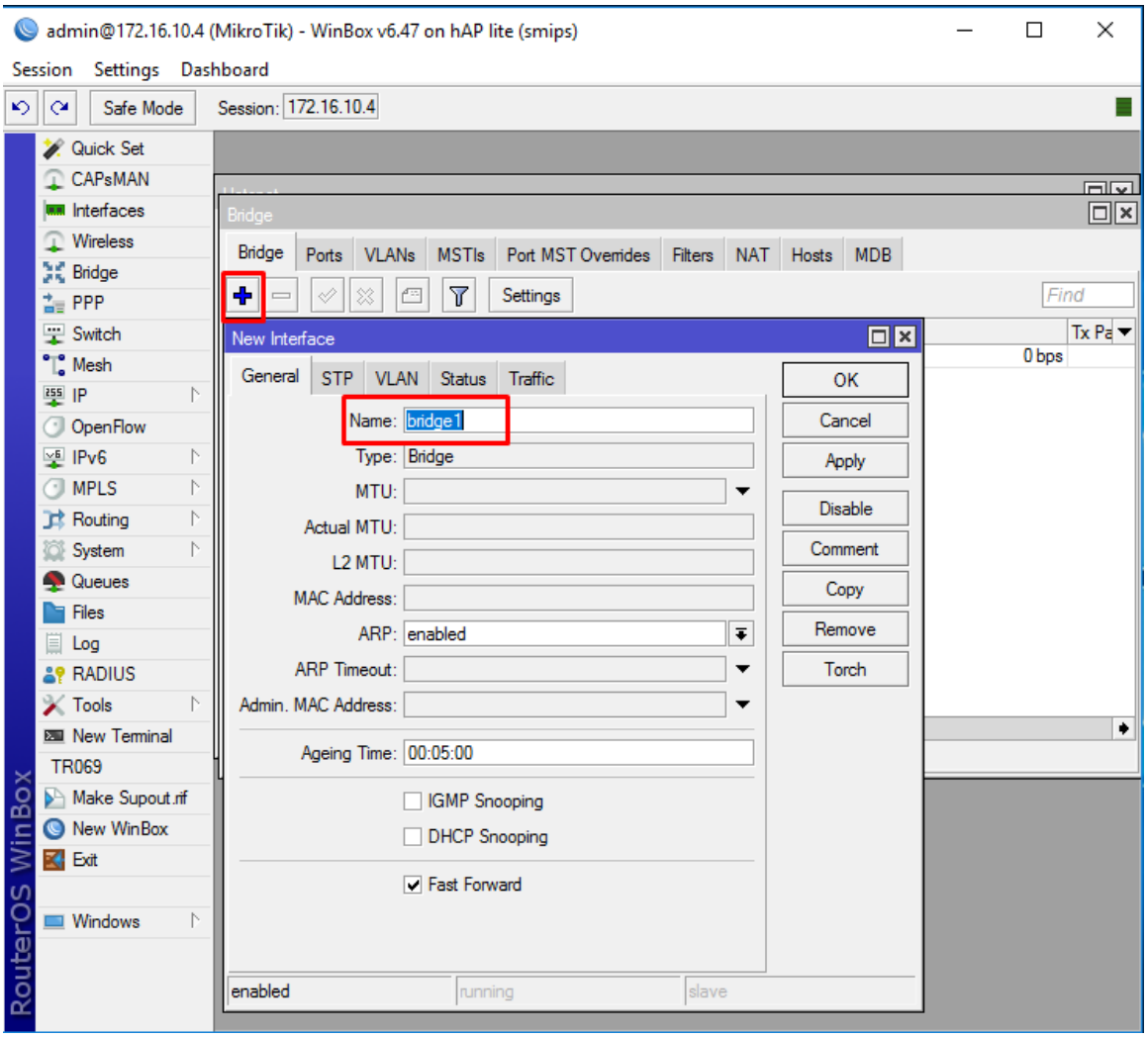
En la figura A20 se muestra la conexión exitosa entre las dos antenas, cabe recalcar que si no se configuró en la misma frecuencia o no se utilizó en la misma un canal de transmisión o contraseña incorrecta el enlace no se establecerá.

6.2. ANEXO B: Manual de configuración del portal Cautivo HOTSPOT RB Mikrotik

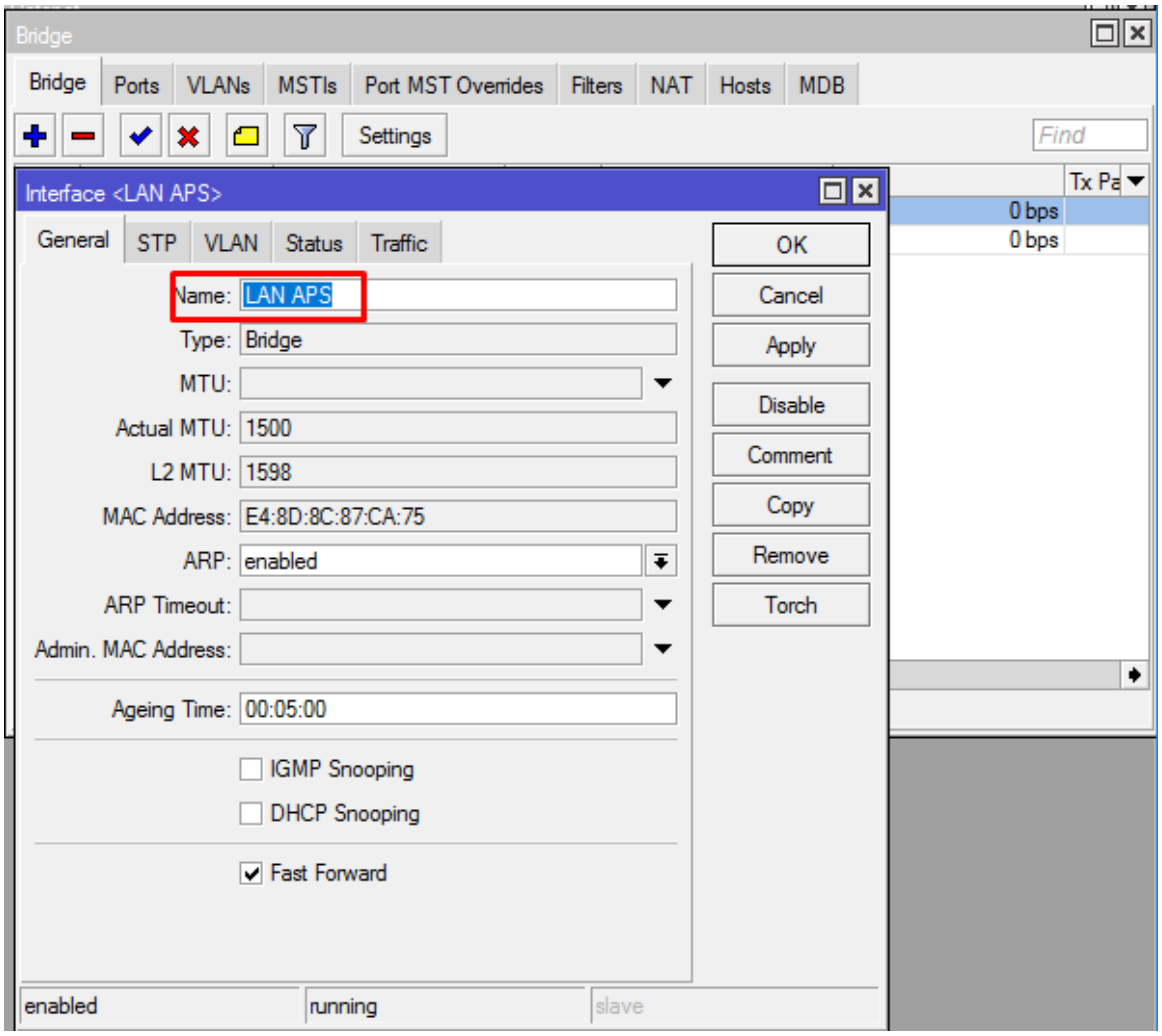
Para la instalación del Portal Cautivo Hotspot se debe verificar las capacidades del equipo seleccionado, para iniciar con la configuración se debe ingresar mediante la aplicación Winbox, utilizada anteriormente en las configuraciones de los enlaces punto a punto.



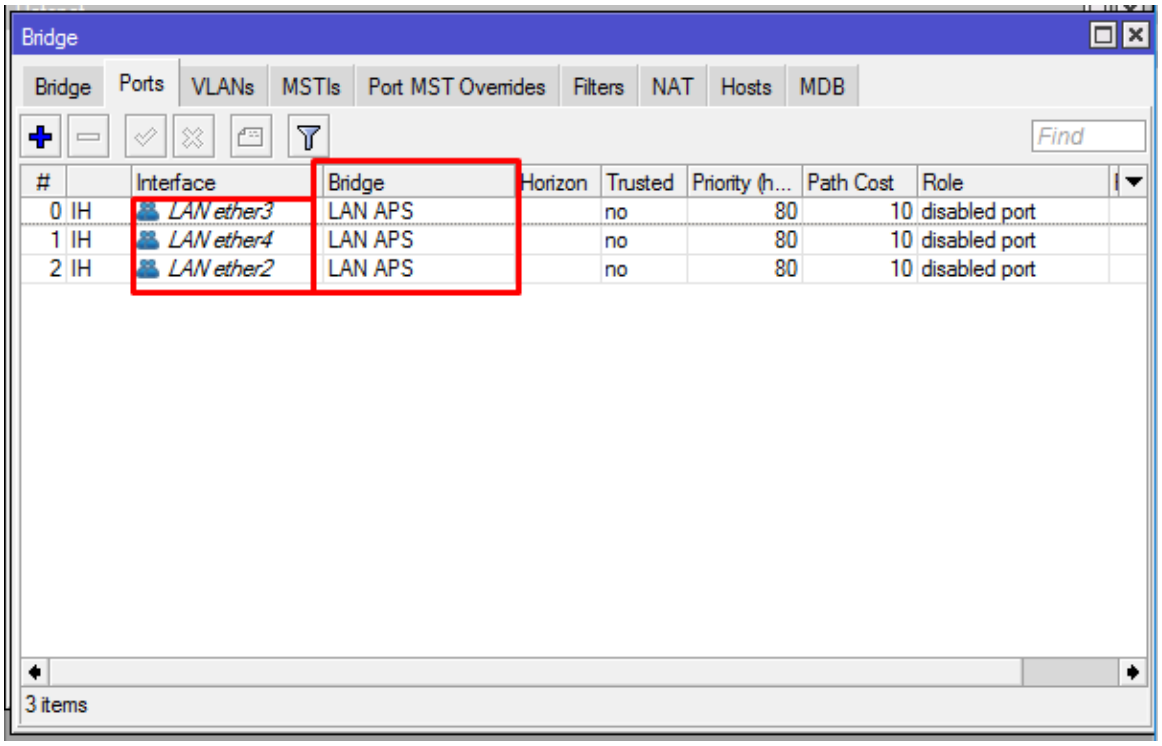
Para el ingreso se ocupa ya sea la dirección Mac o la ip asignada en el equipo para el caso se ingresará mediante la IP.



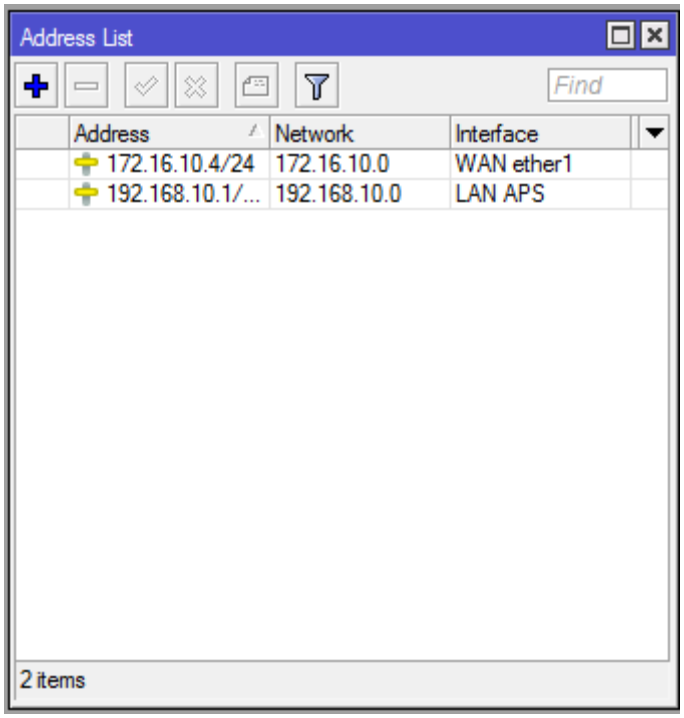
Una vez ingresado al Router se procede a crear un bridge, este bridge servirá para unir a los 3 cafés y puedan trabajar dentro de una misma interfaz, todo cambio deberá presionar el botón apply y posteriormente el botón ok.



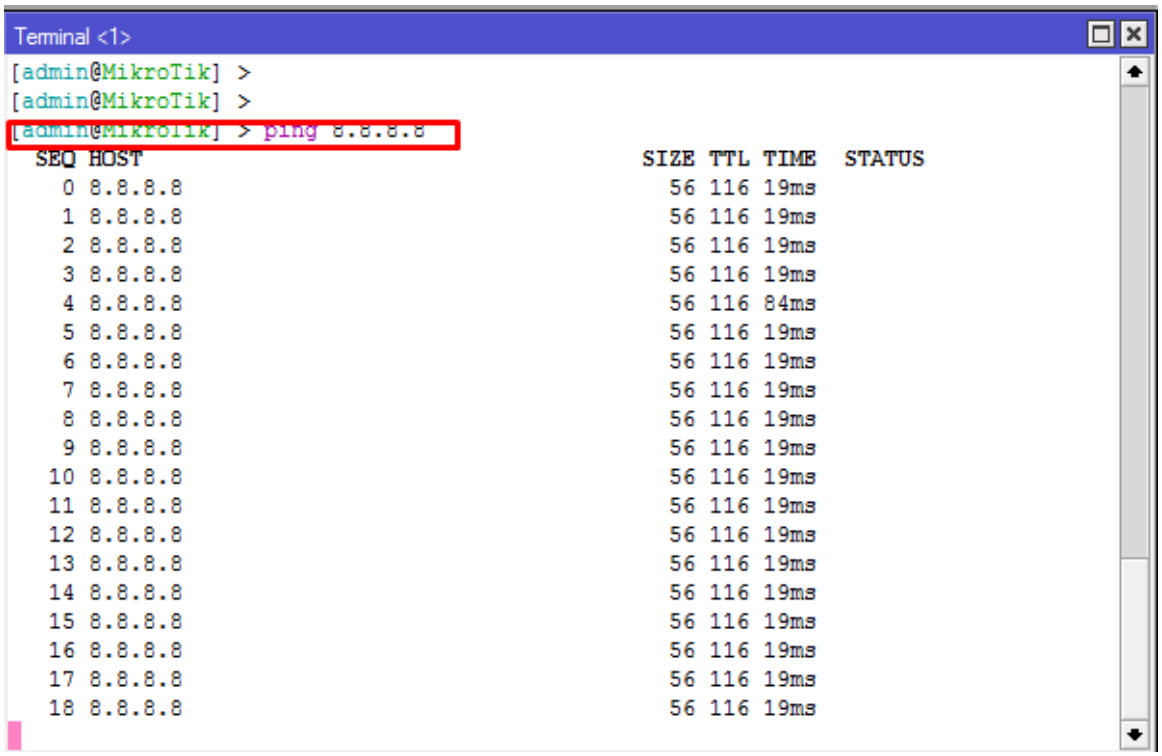
el nombre de este bridge se llamará LAN APS este bridge unificará a las 3 la del Router de borde se aplica y se guarda



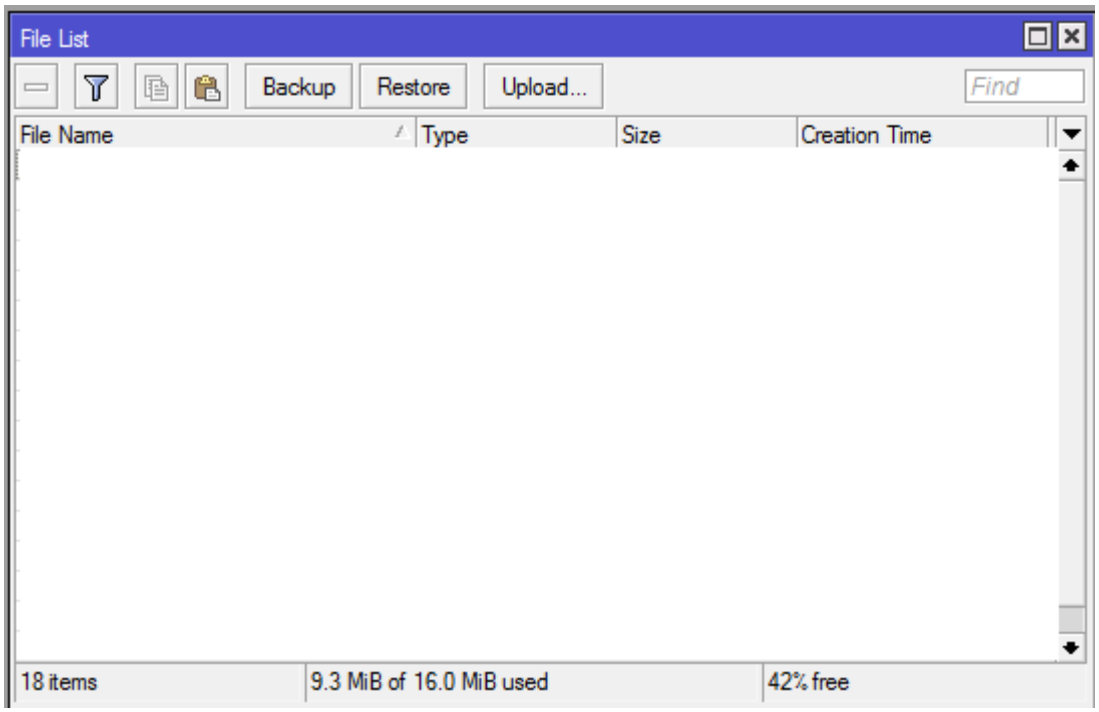
una vez ya creado el bridge se procede a asignar los puertos al bridge antes creado para el caso la LAN Ether, Ether 3 y Ether 4 pasarán a formar parte del bridge LAN APS



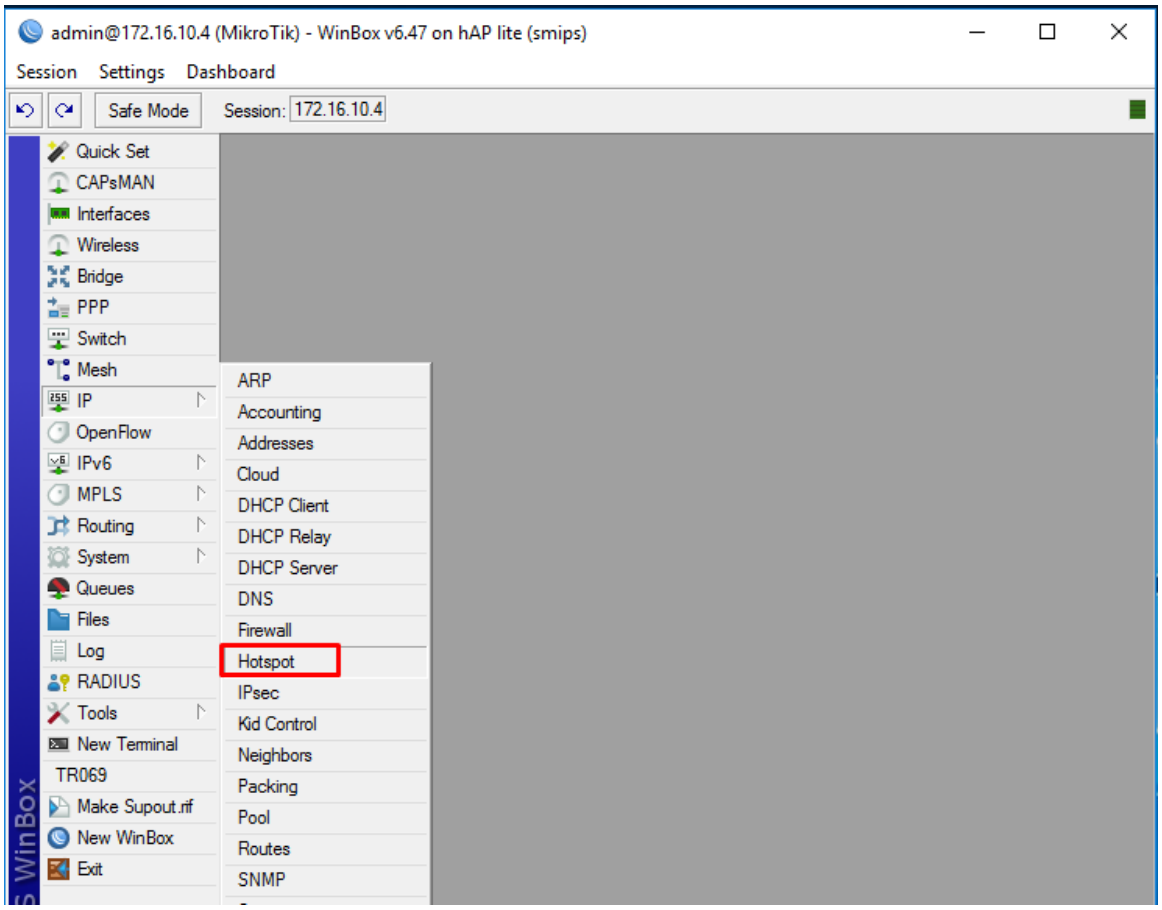
Se muestra la configuración de la IPs tanto para puerto Wan del ingreso a internet cómo del bridge Lan creado anteriormente, la WAN se asignó la IP 172.16 10.4 y para el bridge Lan se asignó el IP 192.168.10.1



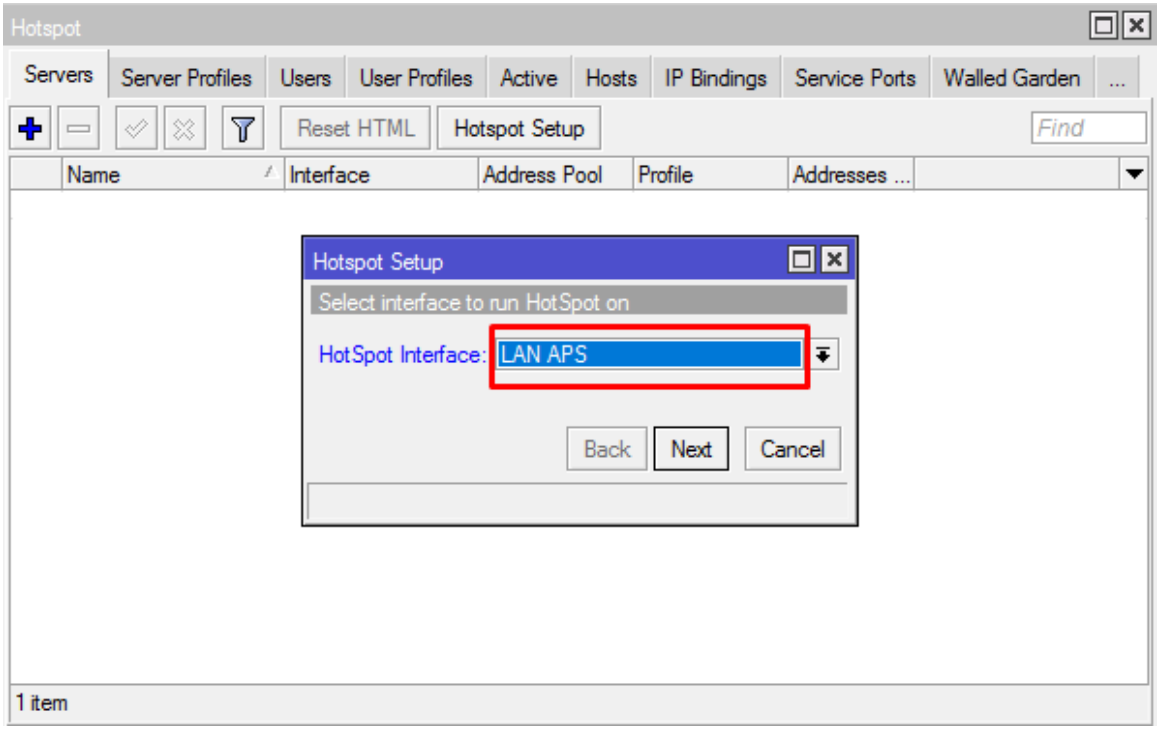
En la figura x se realiza un ping a la dirección IP de internet y para comprobar que se tiene acceso al servicio de internet.



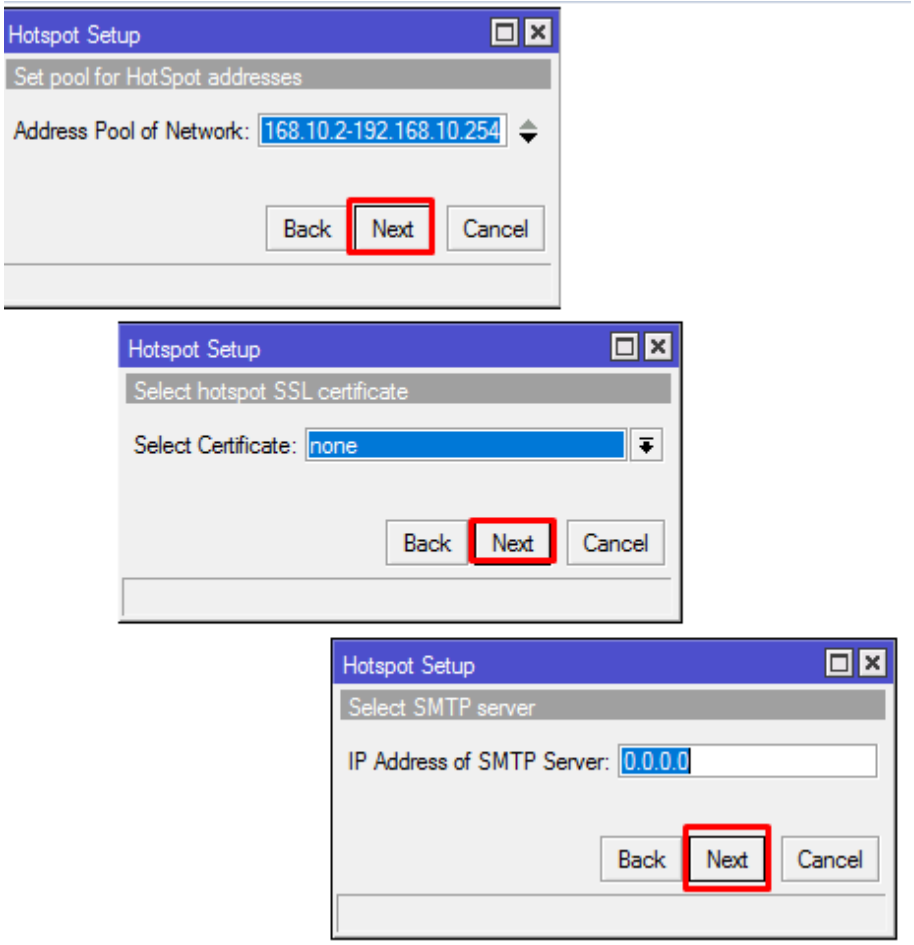
Antes de proceder con la configuración del portal cautivo se verifica que no existe en ningún archivo en la opción de filis dentro del router de borde, en caso de existir algún archivo se elimina cualquier tipo de archivo para que el hotspot que se cree no tenga ningún error



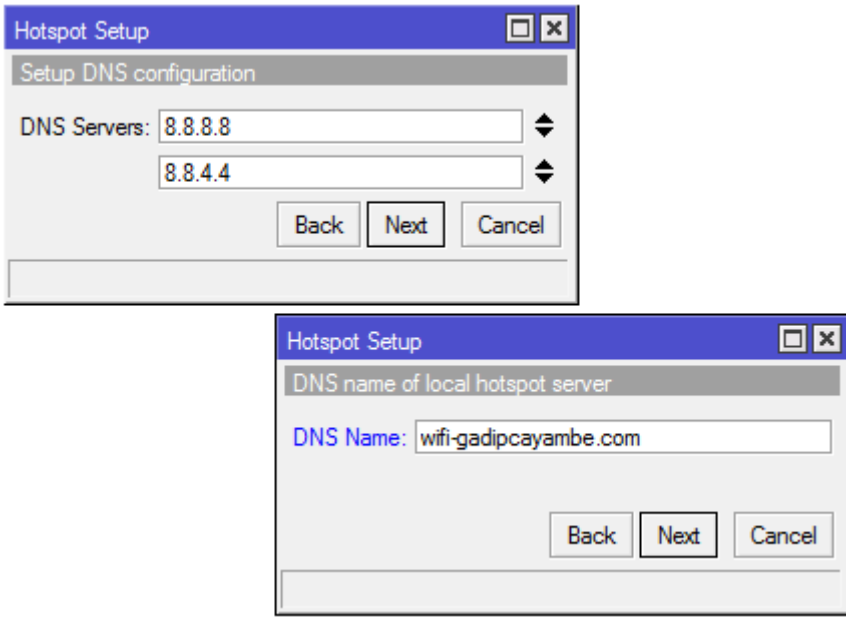
En la figura x se muestra la configuración a seguirse para crear el hostpot Ingresar a la opción IP posteriormente seleccionar la opción host



en la pantalla que aparece se selecciona la opción hotspot setup a continuación aparecerá una nueva pantalla en el cual seleccionaremos el bridge creado anteriormente seguido de eso presionamos el botón next.



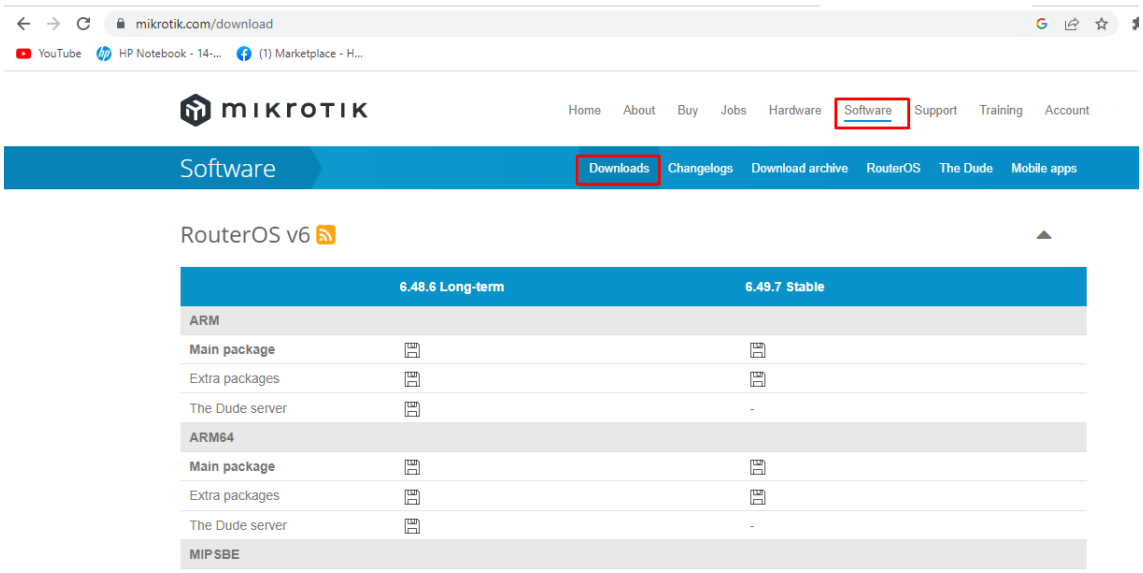
En la figura x se muestra los pasos siguientes en el cual se puede observar el Pool de direcciones Ip el cual será el configurado anteriormente para el bridge de los APS, tambien que no se utiliza ningún certificado SL ni tampoco un servidor SMTP.



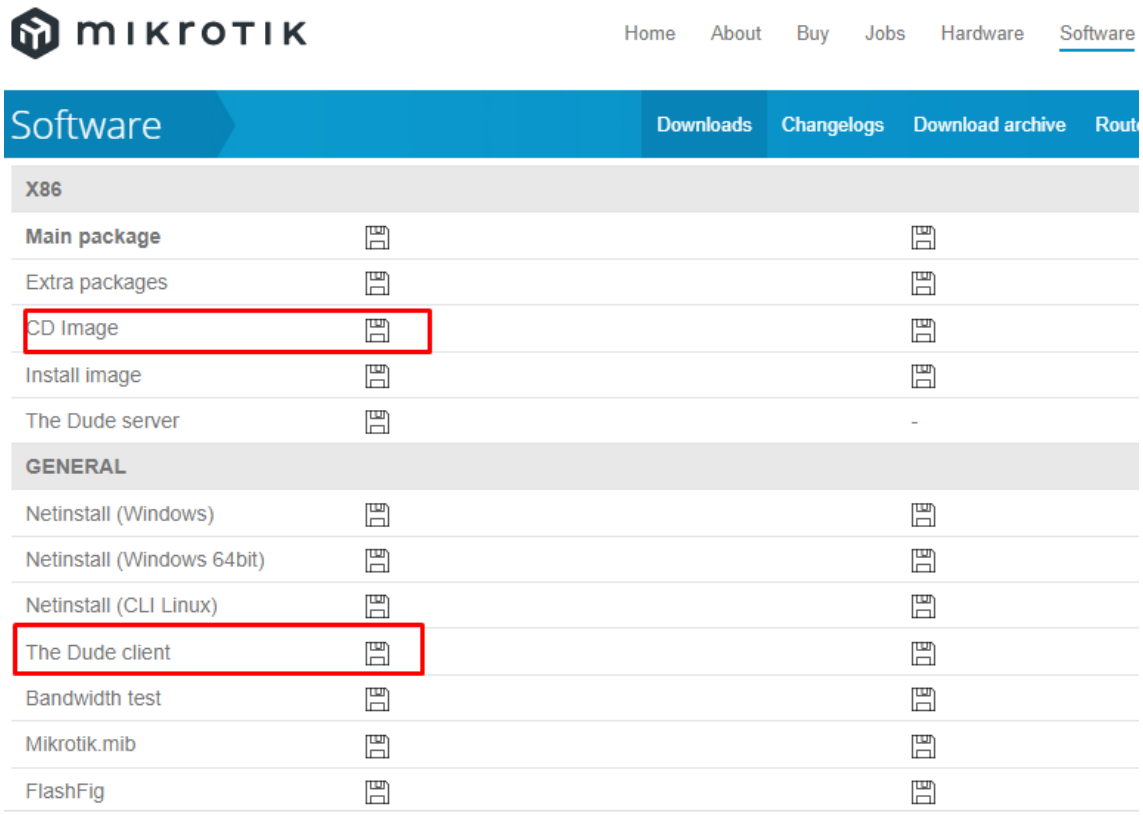
Para finalizar ingresamos los DNS del servicio de internet 8.8. 8.8 y el de NS secundario 8.8. 4.4 seguido de eso presionamos la tecla next, posteriormente aparecerá una pantalla en donde ingresaremos la dirección al cual re direccionará una vez que se conecte a la red wifi.

6.3. ANEXO C: Manual de instalación del Software THE DUDE

Para poder instalar el software dude ingresamos a la página oficial de Mikrotik, una vez ya en la plataforma nos dirigimos a la opción de software y descargas

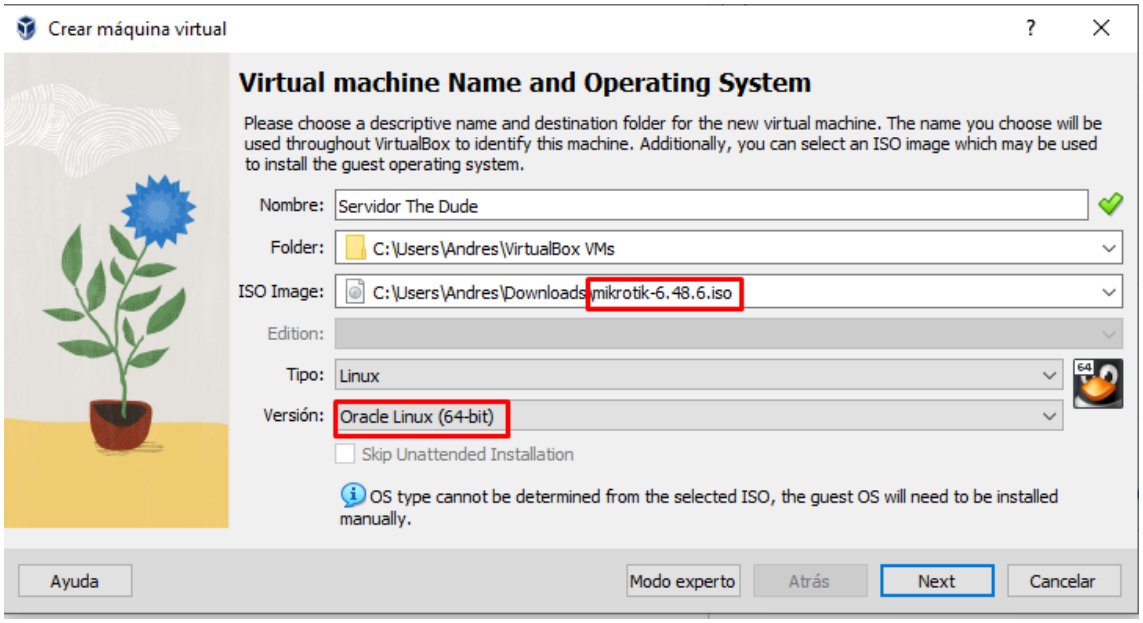


descargar lo que es el servicio de dude la herramienta cliente dude, tener en cuenta que cuando se descargue estos archivos sean de la misma versión, debido que existe conflictos cuando no son de la misma versión tanto en RouterOs v6 y RouterOs v7.



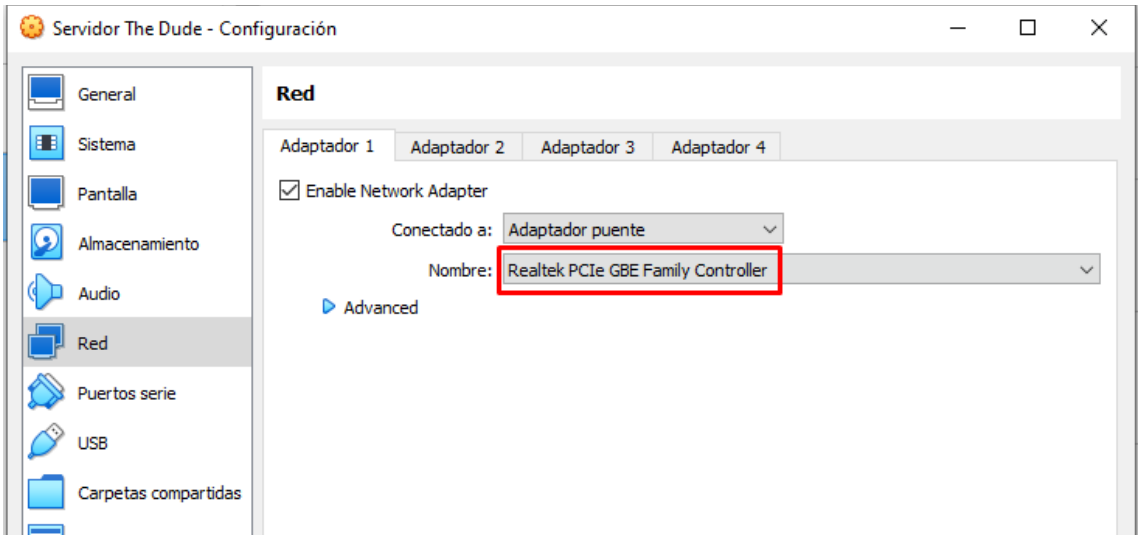
Una vez ya descargado los archivos procedemos a instalarlos en una máquina virtual

Agregar el nombre del servidor cargamos la ISO con la versión 6.48.6, Es importante poner en la versión de 64 bits.

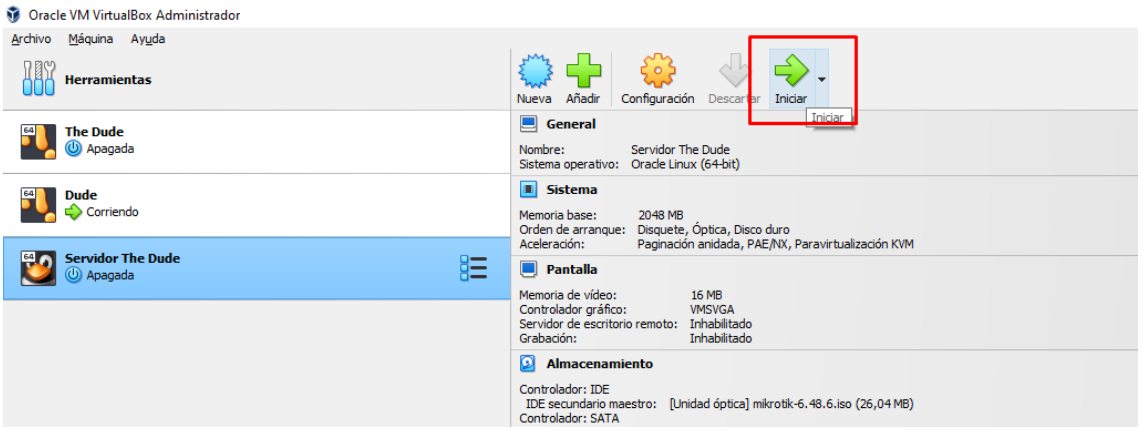


asignamos la memoria RAM y la memoria de almacenamiento, según los requerimientos.

Para la práctica estableceremos adaptador puente a la tarjeta ethernet.

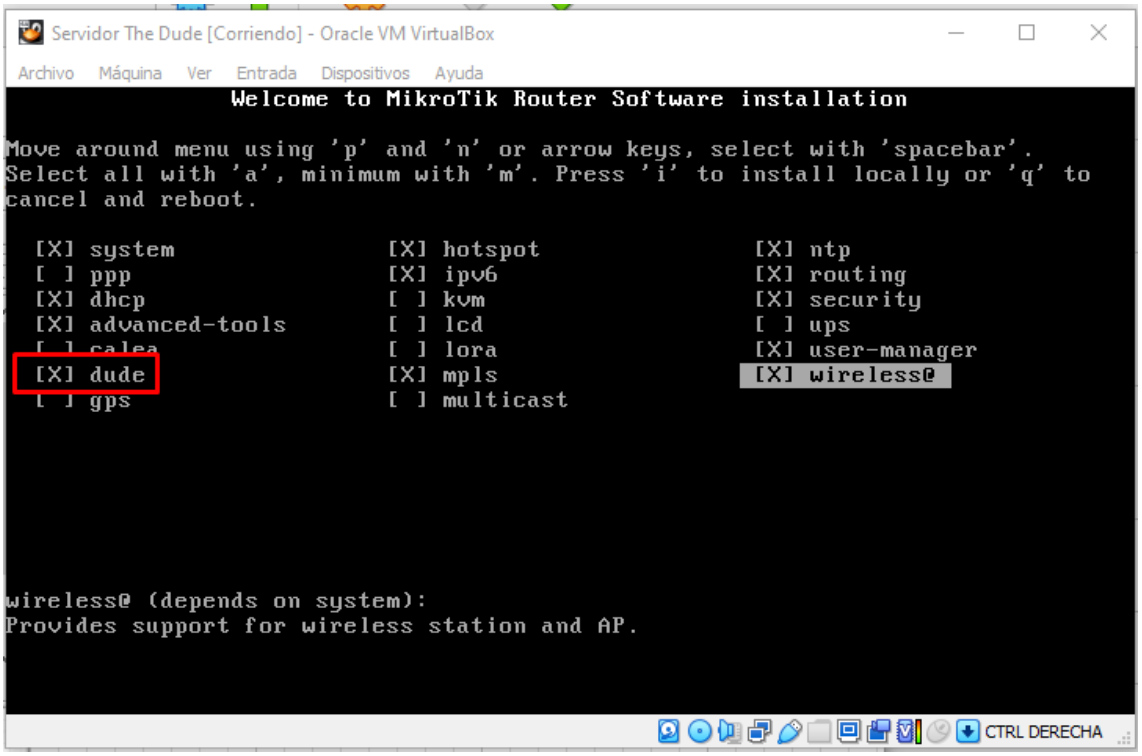


Iniciamos la máquina virtual

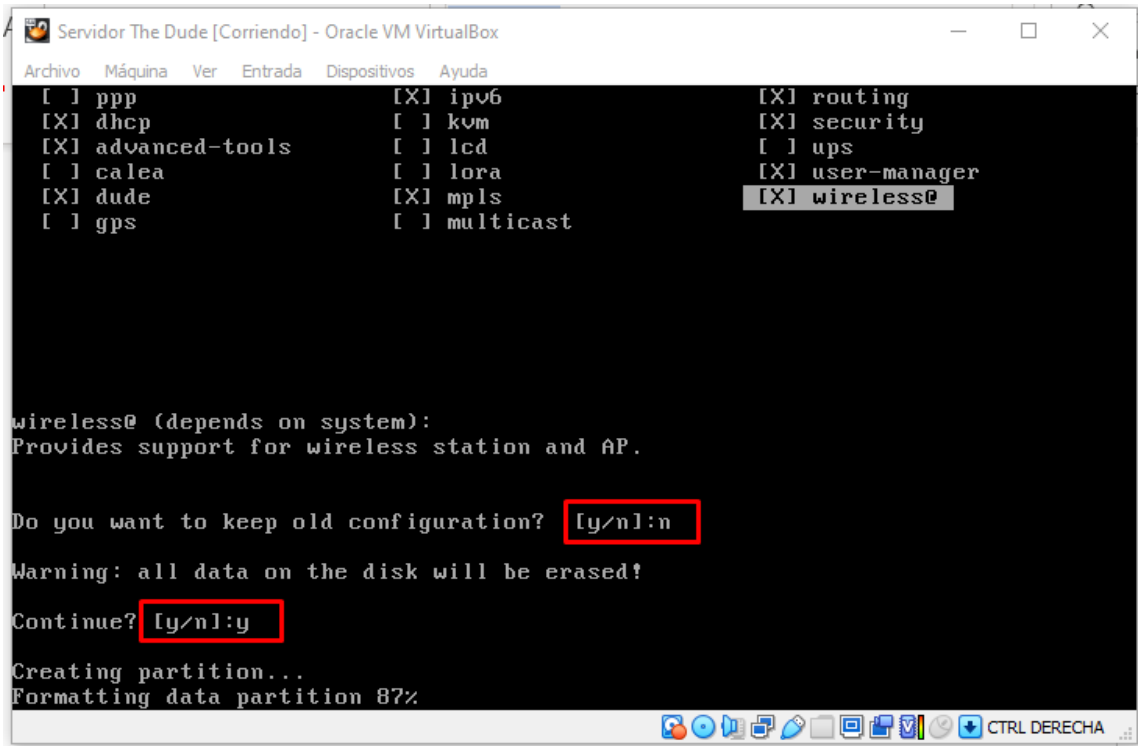


Una vez iniciada la máquina procederá a cargar el ISO MikroTik dude, a continuación, activaremos unas opciones extras que ayudará al mejor rendimiento del servidor para la gestión de la red.

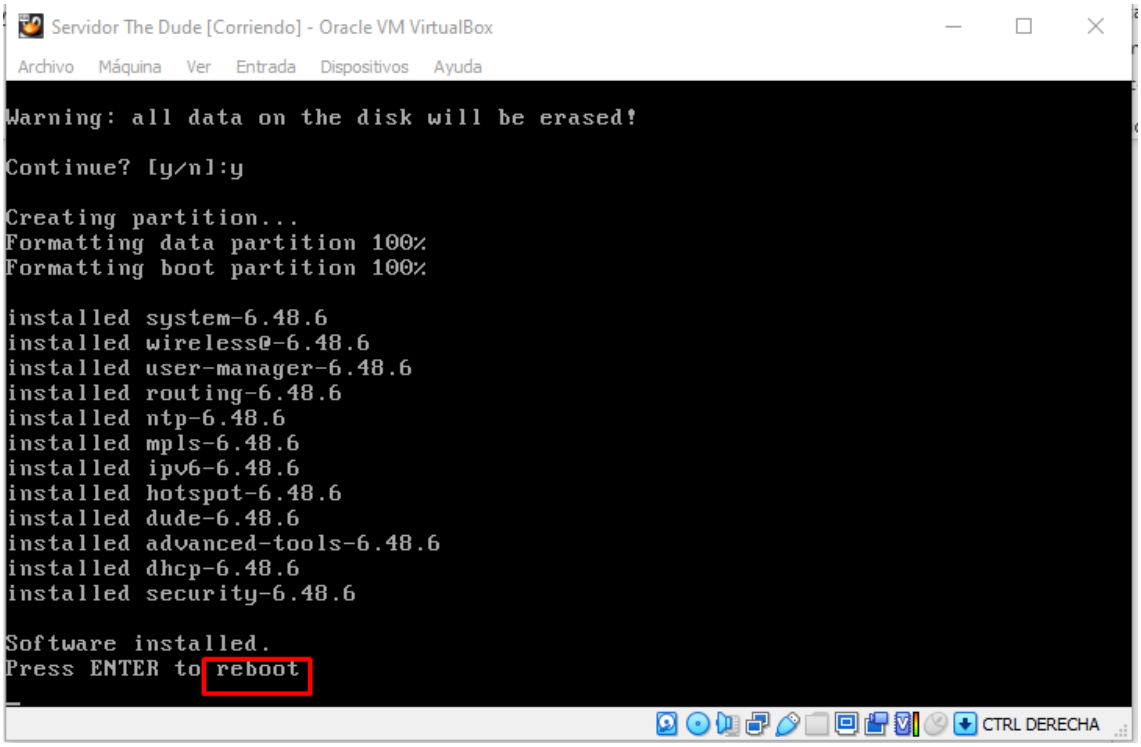
seleccionar las opciones como se muestra en la imagen, presionar la tecla i para instalar.



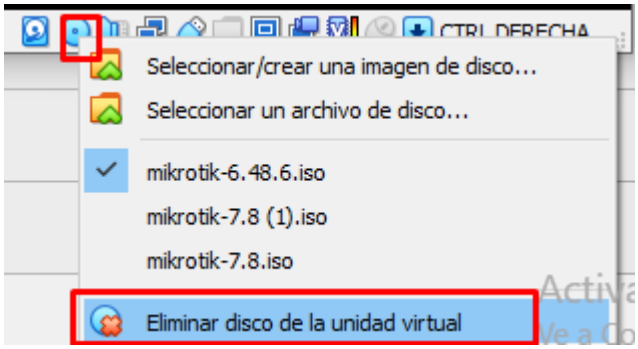
Antes de instalar el sistema pregunta si se desea conservar las configuraciones anteriores a la cuál presionamos la tecla n y después pregunta si s desea borrar el almacenamiento a la cual presionamos la tecla y.



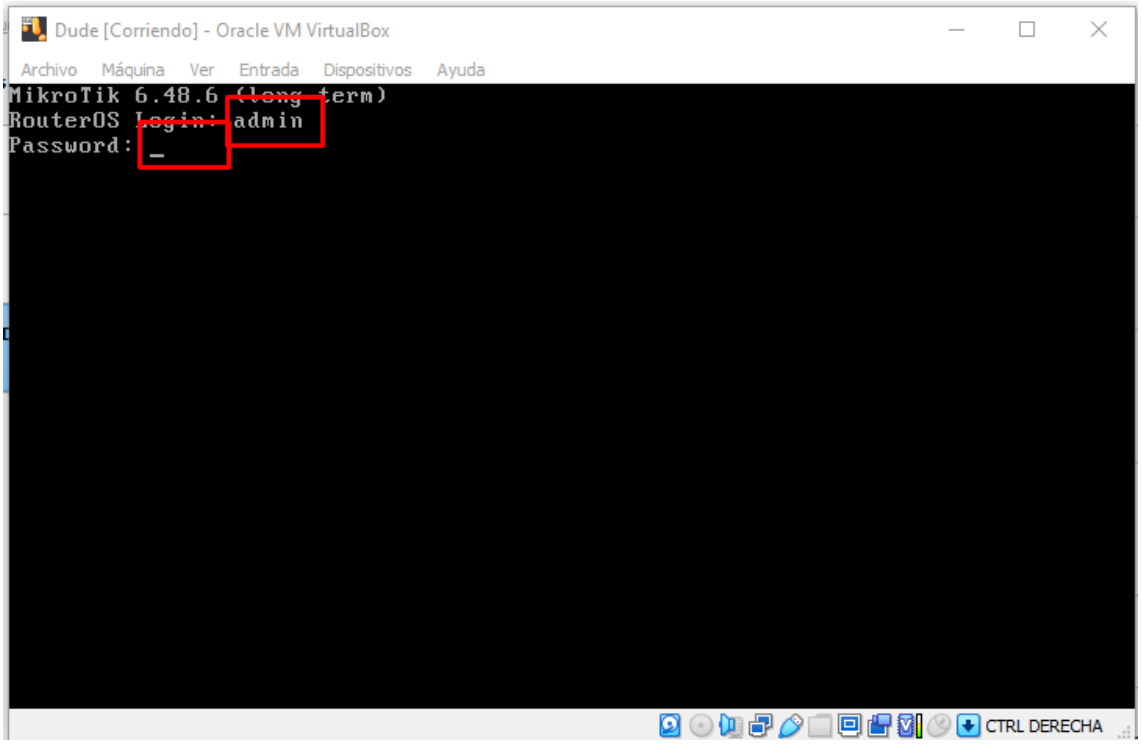
Una vez instalado el sistema deberá reiniciarse, para la cual se presiona la tecla enter.



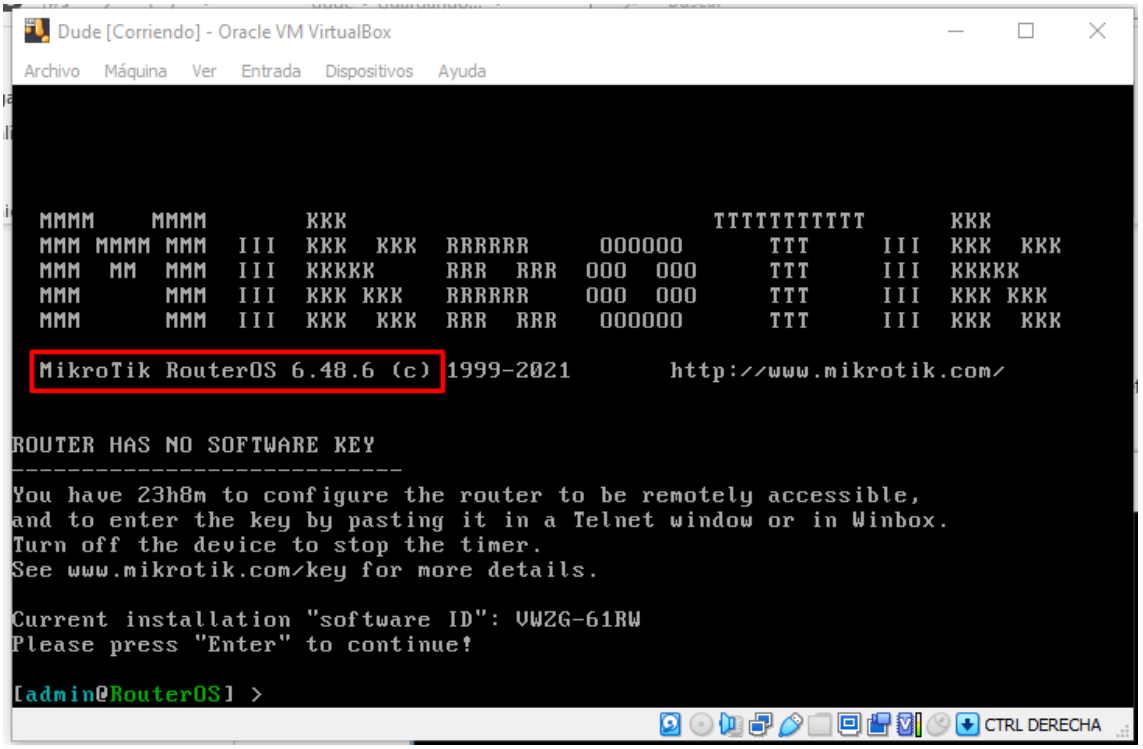
Una vez que el sistema se reinicia se procede a eliminar la imagen ISO, para que no vuelva a cargar el proceso de instalación.



Una vez que el sistema se reinicia cargará la página de logue, el usuario por defecto es admin y no posee contraseña.



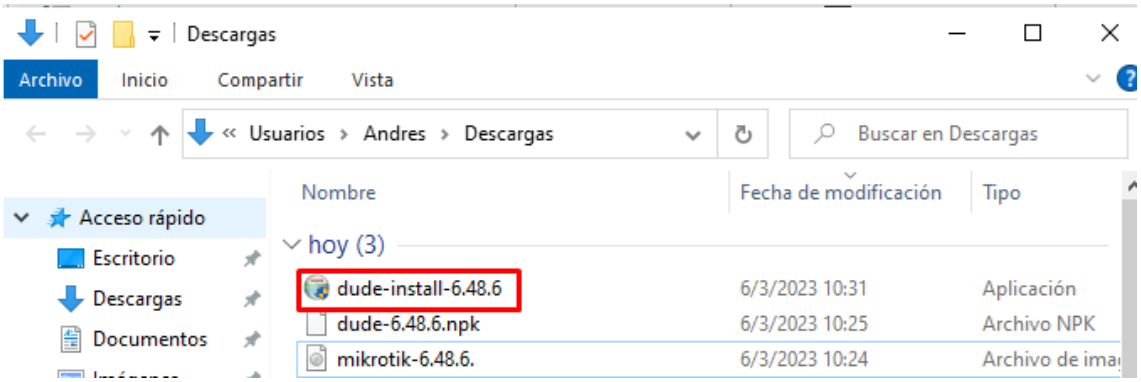
Con eso se tiene instalado el servidor dude para la configuración del cliente o gestor dude hay que tener en cuenta la versión ISO instalada.



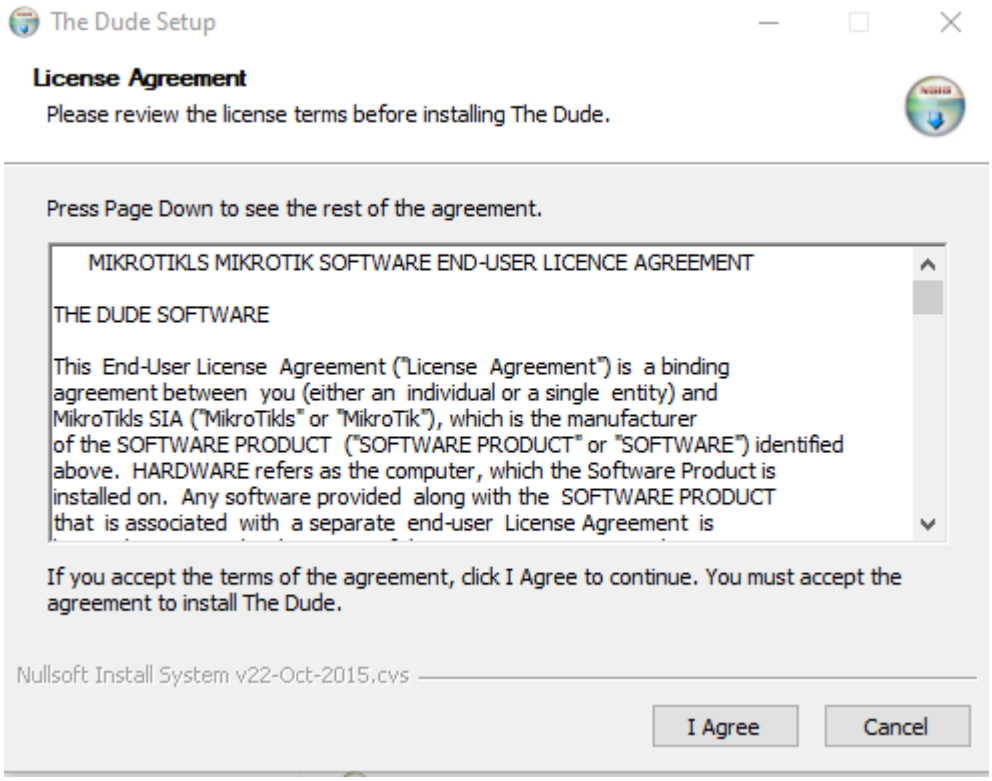
Instalación del gestor dude

Tener descargado el instalador del gestor dude con la versión del router os versión 6.48. 6.

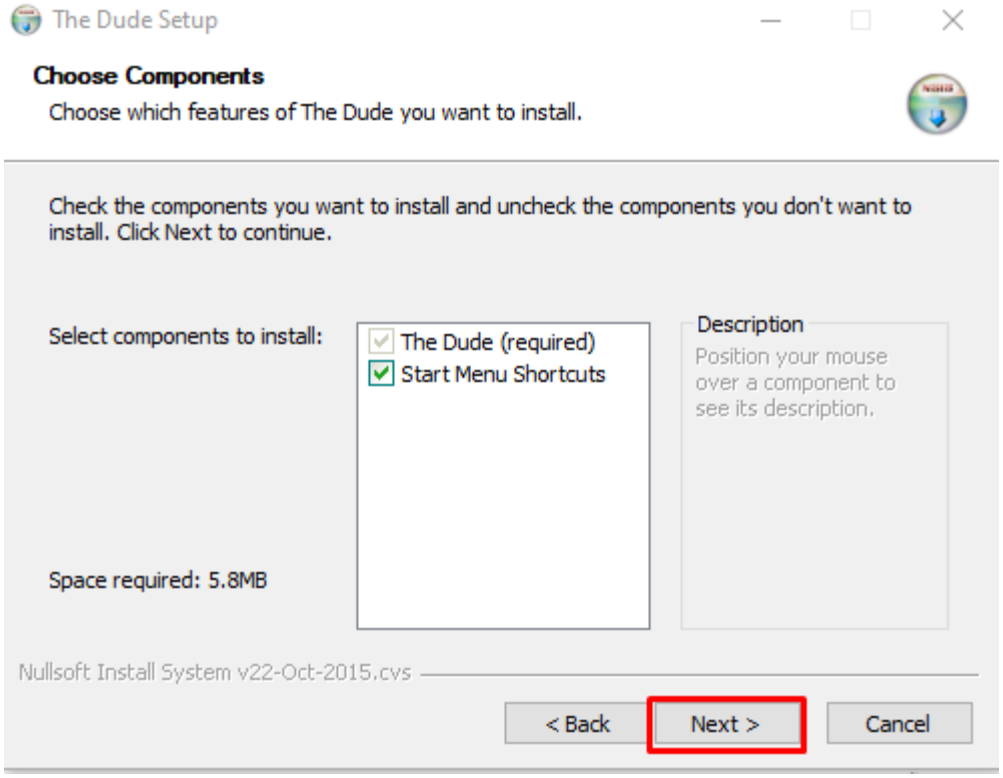
Este gestor se descarga de la página de mikrotik como se mostró en la instalación del dude



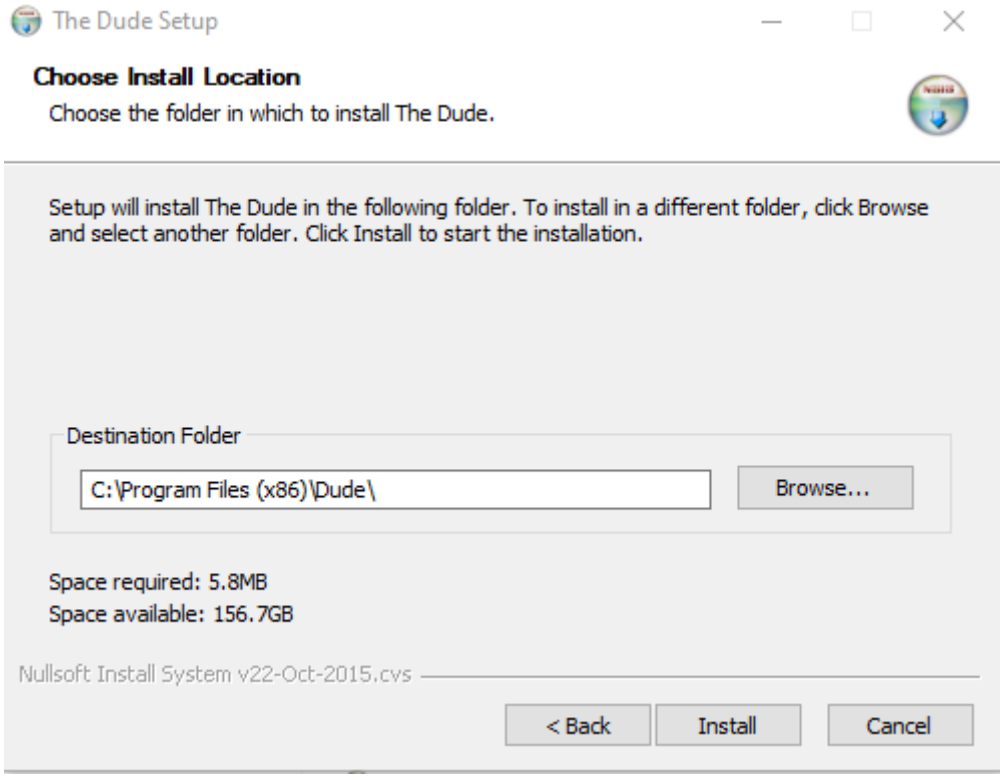
clic derecho sobre la aplicación para iniciar con la instalación. A continuación, iniciará el proceso de instalación para lo cual presionamos la tecla I Agree.



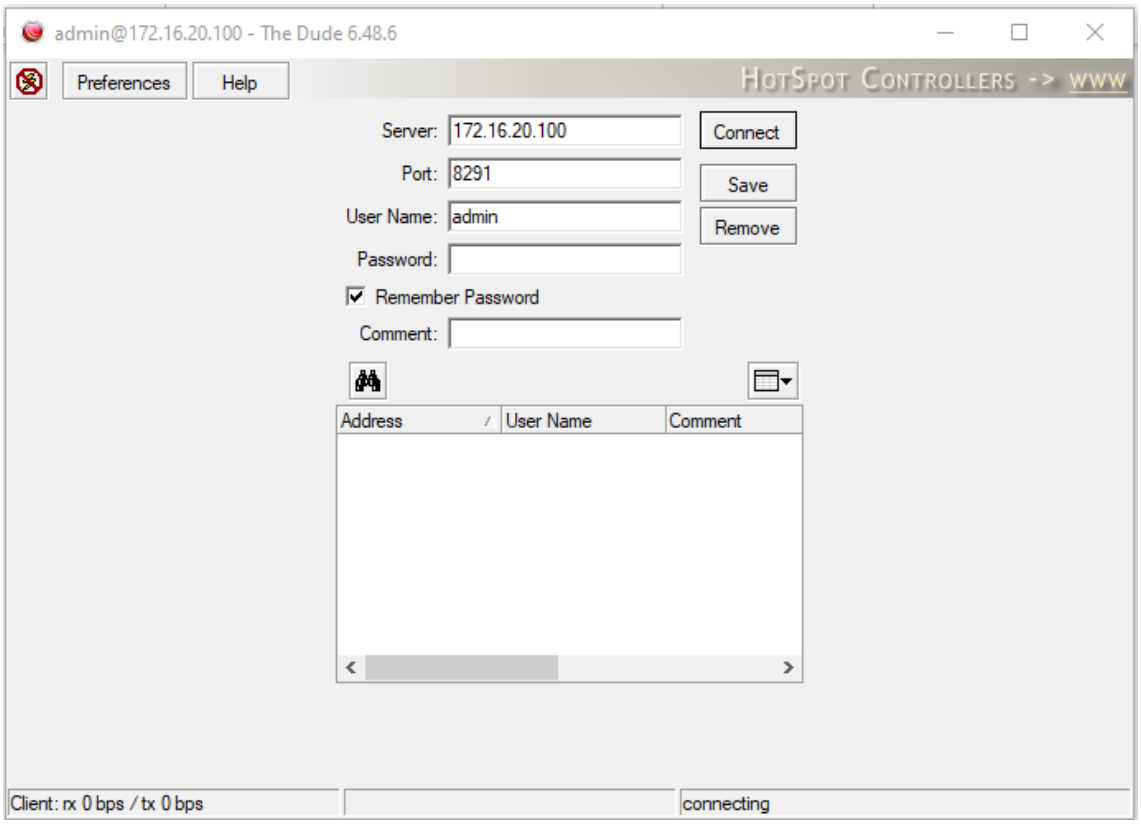
Fijar sé si está activado la casilla que inicie dude de no estarlo presionar la casilla



Y se procede con la instalación



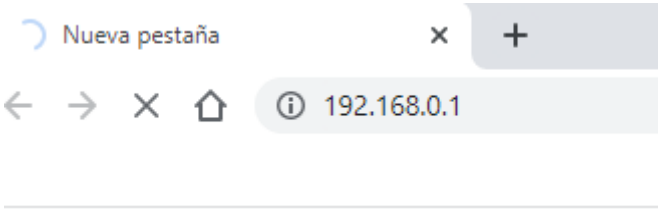
Una vez instalado el gestor aparecerá la pantalla de inicio en donde se ingresará la ip usuario y contraseña del servidor



6.4.ANEXO D: Manual de configuración del Access Point EAP225- Outdoor

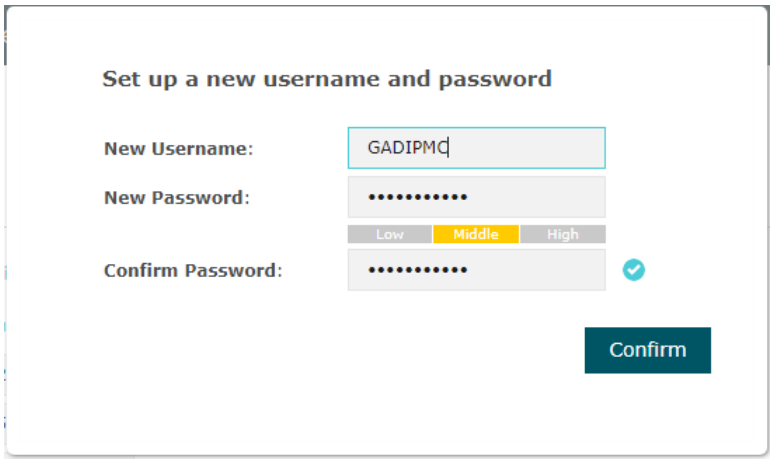
Para la configuración del Access Point EAP225 se ingresa por el navegador de por la dirección ip 192.168.0.1

Figura D1



Una vez ya en la interfaz principal procedemos a configurar el Usuario y contraseña del administrador

Figura D2



Se procede a configurar una ip estatica en la pestaña de Red, para el primer AP

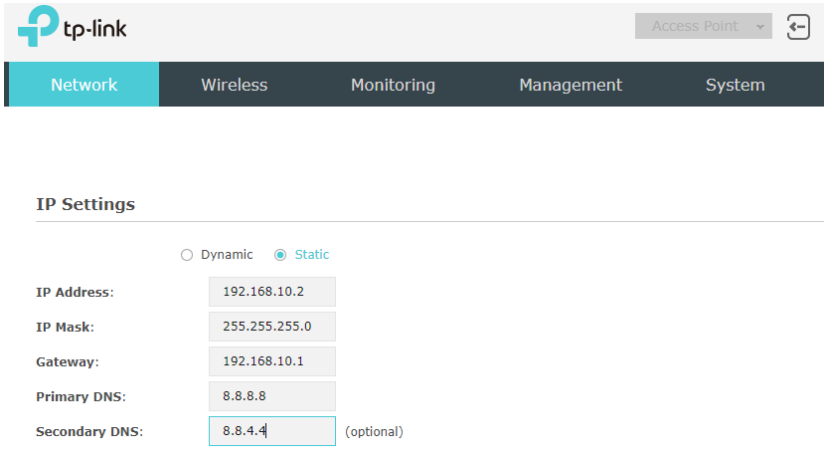
IP: 192.168.10.2

Mascara: 255.255.255.0

Puerta de Enlace: 192.168.10.1

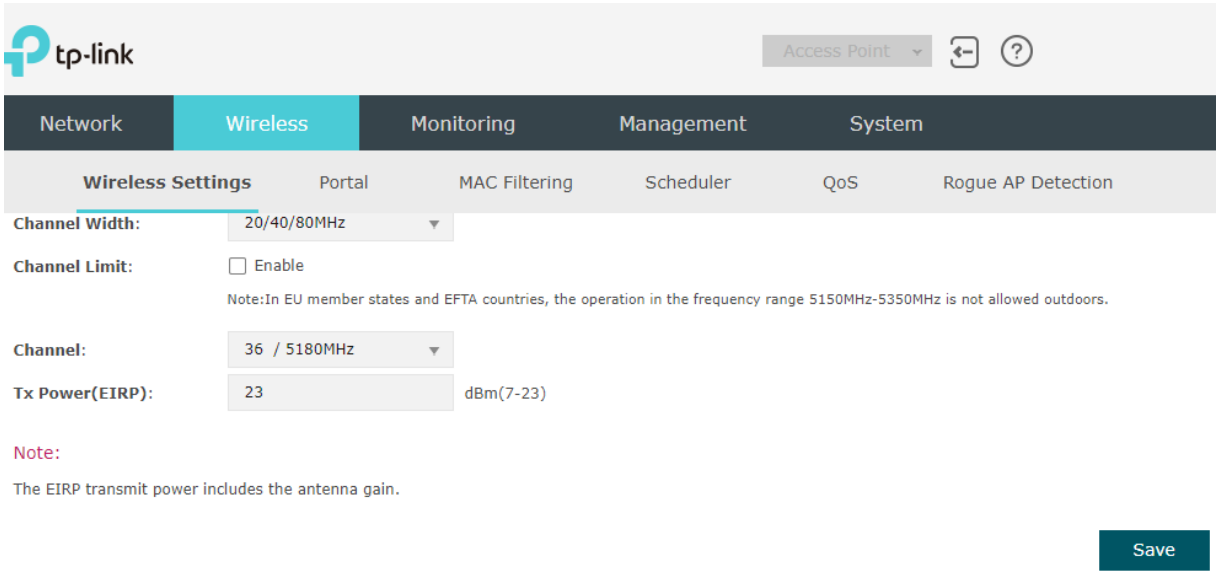
DNS: 8.8.8.8

Figura D3



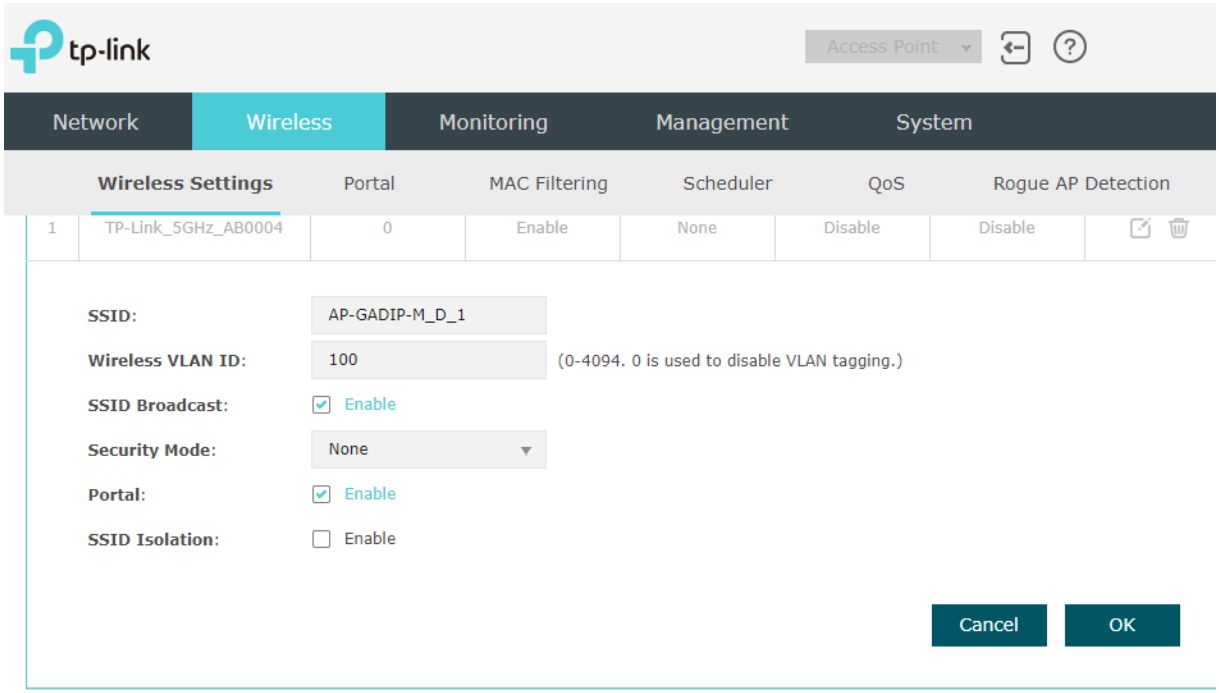
Se configura la frecuencia y se asigna los canales propuestos en el Ítem 3.12.3

Figura D4



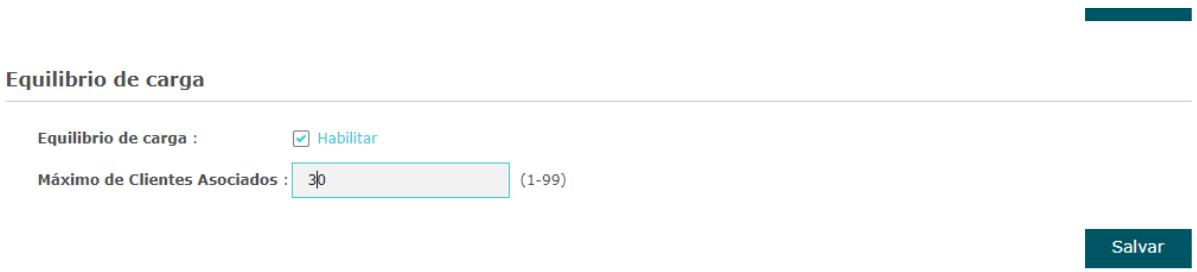
Se configura el SSDI de la red en este caso se asignó el nombre AP-GADIPCayambe y no debe tener ningún protocolo de seguridad.

Figura D5



Se configura el número máximo de usuarios que se conecte a este Access Point

Figura D6



Para la Gestión de la red inalámbrica es importante activar el protocolo SNMP para poder gestionar el equipo y poder monitorear todos sus recursos

Figura D7


tp-link
Access Point
Red
Inalámbrico
Supervisión
Gestión
Sistema
Registro del sistema
Servidor web
Acceso de gestión
LED
SSH
VLAN de administración
SNMP
Agente SNMP
Agente SNMP :
Habilitar
Contacto del sistema :
Nombre del sistema :
Ubicación del sistema :
Obtener comunidad :
public
Obtener fuente :
0.0.0.0
Establecer comunidad :
private
Establecer fuente :
0.0.0.0

6.5. ANEXO E: Base de Datos para los Equipos de Interconexión

Actualmente ya existe una base de datos se realizada en un trabajo de Grado titulado "ADMINISTRACIÓN Y GESTIÓN DE LA RED INALÁMBRICA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO (GADIP) DEL CANTÓN CAYAMBE BASADA EN EL MODELO FUNCIONAL FCAPS DE LA ISO".

En donde ya existe una base de datos realizada en Microsoft Excel y la utilización de la herramienta de programador, en la cual permite el manejar visual BASIC para realizar la interfaz. Esta base de datos se realizó para llevar un inventario de los dispositivos de red, permitiendo al administrador de la red tener un control total de todos los dispositivos de red y la ubicación exacta de cada uno de los dispositivos, se consideró los siguientes parámetros para el inventario de la red Inalámbrica del GADIP del Municipio de Cayambe.

- Tipo de Componente
- Nombre del equipo
- Dirección IP de red
- Marca y Modelo
- Número de Serie
- Ubicación del Equipo
- Fecha de Ingreso
- Responsable
- Teléfono del Contacto

6.6. ANEXO F: Base de Datos para los Fallos Ocasionados en laRed Inalámbrica Del GADIP del Municipio de Cayambe.

Actualmente existe una base de Datos con una interfaz de Visual Basic en un Microsoft Excel. Esta base de datos se realizó en un Trabajo de Grado anterior con autoría de “Linda Torres” esta base de datos se realizó para la documentación y reporte de los fallos ocasionados en la redInalámbrica del GADIP del Municipio de Cayambe, permitiendo al administrador de la red pueda manejar cualquier el tipo de fallos ocasionados y dar una pronta solución de manera que se garantice el correcto funcionamiento de la red, de esta manera los usuarios podrán acceder alservicio de internet constantemente sin interrupciones.

La base de datos para la documentación de fallos se determinó los siguientes parámetros para el documentar:

- Número del reporte del fallo
- Descripción del fallo
- Fecha
- Responsable
- Lugar
- Observaciones

6.7. ANEXO G: Recomendaciones para los usuarios del Portal Cautivo (Hotspot) de la zona central Guachalá

Para hacer uso del servicio de Internet gratuito en la zona central de Guachalá los usuarios deben seguir los siguientes Pasos:

GADIPCayambe
SUMAK KAWSAYPAK
Gobierno Autónomo Descentralizado Intercultural y Plurinacional del Municipio de Cayambe

RECOMENDACIONES A USUARIOS DEL SERVICIO GRATUITO DE INTERNET EN EL PARQUE CENTRAL DE CAYAMBE

1. Presentar en la recepción de documentos del GADIP del Municipio de Cayambe la cedula de identidad o pasaporte para personas extranjeras.
2. Se procederá a crear la cuenta de usuario y contraseña el técnico de la red Inalámbrica.
3. El nombre de usuario será el primer nombre y la contraseña el número de cedula de identidad.
4. Se le asignará un tiempo límite de uso del servicio de Internet al día.
5. Conectar el dispositivo móvil a la red con el SSID GADIP-CAYAMBE
6. Al ingresar en el navegador dar clic ***Accede a la Red***
7. El Hotspot tiene la opción de dar acceso a internet por 30 minutos en caso de no estar registrado en la base de datos del GADIP Cayambe.
8. Mientras no se cierre la sesión el tiempo seguirá corriendo.

6.8. ANEXO H: Formularios de Documentación

ANEXO H.1: Formulario de Reportes de Fallos

GADIPCayambe SUMAK KAWSAYPAK
GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PLURINACIONAL DEL MUNICIPIO DE CAYAMBE

REPORTE DE RED	**CODIGO: CTIC-FMT-001-SIE-PINT**		**N°: 00001**
	FORMATO ÚNICO DE REPORTES DE FALLOS		
INSTITUCIÓN EDUCATIVA:			
CANTÓN:		**FECHA:**	
PARROQUIA:		**HORA DEL REPORTE:**	
SECTOR:		**FECHA DE SOLUCIÓN:**	

DETALLE DEL EQUIPO

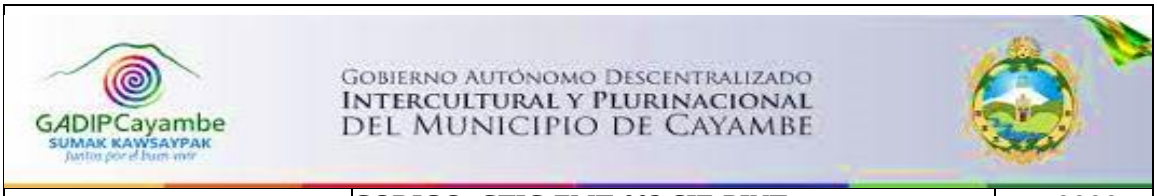
TIPO DE COMPONENTE	DESCRIPCIÓN	MARCA	MODELO

DETALLE DEL PROBLE:

……
……
……
……
……
……
……

……..	…….	…….
Firma de Representante	**Soporte Técnico**	**Aceptado a Satisfacción**

ANEXO H.2: Formulario de documentación de fallos



REPORTE DE RED	**CODIGO: CTIC-FMT-002-SIE-PINT**		**N°: 00001**
	FORMATO ÚNICO DE DOCUMENTACIÓN DE FALLOS		
INSTITUCIÓN EDUCATIVA:			
CANTÓN:		**FECHA:**	
PARROQUIA:		**HORA DEL REPORTE:**	
SECTOR:		**FECHA DE SOLUCIÓN:**	
TIPO DE ATENCIÓN:	**REMOTA**	**PERSONALIZADA**	

DETALLE DEL EQUIPO

TIPO DE COMPONENTE	DESCRIPCIÓN	MARCA	MODELO

DIAGNÓSTICO:

……
……
……
……

TRABAJO REALIZADO:

……
……
……
……

PROBLEMA SOLUCIONADO: SI ☐ **NO** ☐ **PARCIAL** ☐

CAUSAS:

……..	…….	……..
Firma de Representante	**Soporte Técnico**	**Aceptado a Satisfacción**