ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"ESTUDIO COMPARATIVO DE LA IMPLEMENTACIÓN DE UN PORTAL CAUTIVO MEDIANTE LAS TECNOLOGÍAS MIKROTIK Y CISCO PARA MEJORAR EL RENDIMIENTO DE UNA RED INALÁMBRICA EN MIPYMES"

TRABAJO DE TITULACIÓN: **PROYECTO TÉCNICO**

Para optar al Grado Académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR: LENIN JOSÉ CAIZA FALCONI

TUTOR: ING. JORGE YUQUILEMA

Riobamba-Ecuador

2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

El Tribunal del Trabajo de Titulación certifica que: El trabajo de investigación "ESTUDIO COMPARATIVO DE LA IMPLEMENTACIÓN DE UN PORTAL CAUTIVO MEDIANTE LAS TECNOLOGÍAS MIKROTIK Y CISCO PARA MEJORAR EL RENDIMIENTO DE UNA RED INALÁMBRICA EN MIPYMES", de responsabilidad del señor Lenin José Caiza Falconi, ha sido minuciosamente revisado por los Miembros del Tribunal de Trabajo de Titulación, quedando autorizada su presentación.

	FIRMA	**FECHA**
Ing. Washington Gilberto Luna Encalada **DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	….....	.....
Ing. Franklin Moreno **DIRECTOR DE LA ESCUELA DE ELECTRÓNICA TELECOMUNICACIONES Y REDES**	….....	.....
Ing. Jorge Yuquilema **DIRECTOR DE TRABAJO DE TITULACIÓN**	….....	.....
Ing. Mónica Zabala MSc. **MIEMBRO DEL TRIBUNAL**	….....	.....

Yo Lenin José Caiza Falconi, soy el responsable de las ideas, doctrinas y resultados expuestos en este Trabajo de Titulación y el patrimonio intelectual de la misma pertenecen a la Escuela Superior Politécnica de Chimborazo.

Lenin José Caiza Falconi

DEDICATORIA

Dedico este trabajo primeramente a Dios que me ha bendecido todos estos años de arduo caminar estudiantil, a mi madre Luz América quien supo sacar adelante a toda una familia ella sola brindándonos amor incondicional y apoyo en todos los proyectos que me he propuesto, a mis hermanos que con su compañía alegran mi vida de manera especial a Juan Carlos que pese a sus adversidades siempre salió triunfante enseñándome a luchar por una meta y anteponerme sobre todos los obstáculos que se presenten y siempre levantarme con más fuerza después de cada caída.

Lenin José

AGRADECIMIENTO

Agradezco a Dios por darme la sabiduría necesaria para poder culminar de manera exitosa mis estudios, por guiar mis pasos y ayudarme a superar los obstáculos.

A mi madre Luz América que estuvo conmigo apoyándome en todo momento, brindándome sus consejos de vida y su amor incondicional, a mis familiares por estar en los momentos difíciles que se han presentado y a todas las personas que día a día me ayudaron a cumplir con mi meta.

De manera especial al Ing. Jorge Yuquilema y a la Ing. Mónica Zabala por su apoyo y predisposición para efectuar este trabajo.

Lenin José

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

ABREVIATURAS

AAA	AUTHENTICATION ATHORIZATION AND ACCOUNTIG
AES	ADVANCE ENCRYPTION STANDAR
AP	ACCESS POINT
BGP	BORDER GATEWAY PROTOCOL
CHAP	CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL
CPU	UNIDAD CENTRAL DE PROCESAMIENTO
CSMA/CA	CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE
DHCP	DYNAMIC HOST CONFIGURATION PROTOCOL
DNS	DOMAIN NAME SYSTEM
DHCP	DYNAMIC HOST CONFIGURATION PROTOCOL
DSSS	DIRECT SEQUENCE SPREAD SPECTRUM
EGP	EXTERIOR GATEWAY PROTOCOL
EIGRP	ENHANCEDINTERIOR GATEWAY ROUTING PROTOCOL
EAP	EXTENSIBLE AUTHENTICATION PROTOCOL
FTP	PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS
FDM	FRECUENCY DIVISION MULTIPLEXING
GBPS	GIGABITS POR SEGUNDO
GUI	GRAPHICAL USER INTERFACE
GHZ	GIGAHERTZ
HTTP	HYPERTEXT TRANSFER PROTOCOL
ICMP	INTERNET CONTROL MESSAGE PROTOCOL
ICV	VALOR DE IDENTIFICACION DE INTEGRIDAD
ID	IDENTIFICADOR

IDE	INTEGRATED DEVELOPMENT ENVIRONMENT
IEEE	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
IGRP	INTERIOR GATEWAY ROUTING PROTOCOL
IOS	INTERNET OPERATING SYSTEM
IP	PROTOCOLO DE INTERNET
IPv4	PROTOCOLO DE INTERNET VERSION 4
IPv6	PROTOCOLO DE INTERNET VERSION 6
IPREX	INSTITUTO DE PREPARACION PARA EXAMENES
IR	INFRAROJO
ISP	INTERNET SERVICE PROVIDER
ITU	UNIÓN INTERNACIONAL DE TELECOMUNICACIONES
LAN	LOCAL AREA NETWORK
LCP	LINK CONTROL PROTOCOL
MAC	MEDIA ACCESS CONTROL
MBPS	MEGABITS POR SEGUNDO
MIC	MESSAGE INTEGRITY CODE
MIMO	MULTIPLE INPUT MULTIPLE OUTPUT
MPLS	MULTIPROTOCOL LABEL SWITCHING
MTBF	MEAN TIME BETWEEN FAILURE
MTTR	MEAN TIME BETWEEN REPAIR
MIPYMES	MICRO PEQUEÑA Y MEDIANA EMPRESA
NCP	PROTOCOLO DE CONTROL DE RED
OS	OPERATING SYSTEM
OSI	OPEN SYSTEM INTERCONNECTION

OSPF	OPEN SHORTEST PATH FIRST
PC	PORTATIL COMPUTER
POE	POWER OVER ETHERNET
PSK	PRE-SHARED KEY
PPP	POINT TO POINT PROTOCOL
QoS	CALIDAD DE SERVICIO
RADIUS	REMOTE AUTHENTICATION DIAL-IN USER SERVICE
RAM	RANDOM ACCESS MEMORY
RTP	REAL TIME PROTOCOL
ROM	READ ONLY MEMORY
SSH	SECURE SHELL PROTOCOL
SSID	SERVICE SET IDENTIFIER
TACACS	TERMINAL ACCESS CONTROLLER ACCESS CONTROL SYSTEM
TCP	TRANSMISSION CONTROL PROTOCOL
TIC	TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN
VPN	VIRTUAL PRIVATE NETWORK
WIFI	WIRELESS FIDELITY
WLAN	WIRELESS LOCAL AREA NETWORK
WISP	WIRELESS INTERNET SERVICE PROVIDER
WAP	WIRELESS APPLICATION PROTOCOL
WEP	WIRED EQUIVALENT PRIVACY
WPA-PSK	WI-FI PROTECTED ACCESS

RESUMEN

En el presente trabajo se realizó un estudio comparativo entre las tecnologías Cisco y Mikrotik para la implementación de un portal cautivo con el fin de mejorar el rendimiento de red inalámbrica en una micro, pequeña y mediana empresa (MIPYMES). Se estudiaron características de los dispositivos existentes en el mercado, tomando en cuenta las necesidades de la infraestructura de red inalámbrica del instituto de preparación académica IPREX. Se realizó un análisis cualitativo, mediante la comparación de parámetros de evaluación subjetivos, obteniéndose como resultado que el dispositivo Mikrotik RouterBoard RB750G es el más adecuado para la implementación del portal cautivo con un 82% de promedio de los parámetros subjetivos frente al 75% obtenido por el dispositivo Cisco WAP 131Wireless-N Dual Radio Access Point, por lo cual se procedió con la implementación de la tecnología Mikrotik. Posteriormente se realizaron pruebas, análisis del tráfico de la red antes y después de la implementación del portal cautivo, obteniéndose como resultado una pérdida de paquetes de 24.581% sin portal cautivo vs 12.192% con portal cautivo, evidenciándose una mejoría del 12.389%; un jitter de 8.93ms sin portal cautivo vs 6.02 ms con portal cautivo, demostrándose una reducción de 2.90 ms; retardo de 122.3ms sin portal cautivo vs 46.9ms con portal cautivo, obteniendo una reducción de 75.4ms, y un 30 % total de optimización. Se observó una mejoría del 6% en la experiencia del usuario (MOS). Se concluye que la implementación de portal cautivo en la red inalámbrica de IPREX, con el dispositivo Mikrotik RouterBoard RB750G, es una solución fiable para el control de recursos y el número de usuarios. Se recomienda a IPREX considerar la implementación del servicio de internet mediante fibra óptica, con una disponibilidad mayor de 4Mbps de ancho de banda para mejorar la velocidad del internet y aumentar el número de usuarios del servicio de portal cautivo.

PALABRAS CLAVE: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <REDES DE COMPUTADORES>**,** <PORTAL CAUTIVO>**,** <MIKROTIK (TECNOLOGÍA)>**,** <PARÁMETROS DE CALIDAD>**,** <LATENCIA (JITTER)>, <RETARDO (DELAY)>, <PÉRDIDA DE PAQUETES>.

ABSTRACT

In the present work a comparative study was carried out between the Cisco and Mikrotik technologies for the implementation of a captive portal in order to improve the wireless network performance in a micro, small and medium enterprise (MIPYMES). Features of existing devices on the market were studied, taking into account the needs of the wireless network infrastructure of the IPREX academic preparation institute. A qualitative analysis was performed by comparing subjective evaluation parameters, resulting in the Mikrotik RouterBoard RB750G device being the most suitable for the implementation of the captive portal with an average of 82% of subjective parameters versus 75% obtained by The Cisco WAP 131Wireless-N Dual Radio Access Point device, which was followed by the implementation of Mikrotik technology. Subsequently, network traffic analysis was performed before and after the implementation of the captive portal, resulting in a loss of packets of 24,581% without captive portal vs 12.192% with captive portal, evidencing an improvement of 12.389%; A jitter of 8.93 ms without captive portal vs 6.02 ms with captive portal, demonstrating a reduction of 2.90 ms; Delay of 122.3 ms without captive portal vs 46.9 ms with captive portal, obtaining a reduction of 75.4 ms, and 30% total optimization. There was a 6% improvement in user experience (MOS). It is concluded that the implementation of captive portal in the IPREX wireless network, with the device Mikrotik RouterBoard RB750G, is a reliable solution for the control of resources and the number of users. IPREX is recommended to consider the implementation of the Internet service using fiber optics, with a greater availability of 4Mbps of bandwidth to improve the speed of the Internet and increase the number of users of the captive portal service.

KEYWORDS: < TECHNOLOGY AND SCIENCES OF ENGINEERING >, <COMPUTER NETWORKS>, <CAUTIVE PORTAL>, <MIKROTIK (TECHNOLOGY)>, <QUALITY PARAMETERS>, <JITTER>, <DELAY> <PACKAGE LOSSES>.

INTRODUCCIÓN

Las redes inalámbricas han alcanzado un papel importante en la vida cotidiana, debido a que facilitan la comunicación entre dispositivos móviles, esta evolución tecnológica permite a los usuarios interactuar entre sí, con la facilidad de poder comunicarse desde cualquier lugar. Dentro de las tecnologías inalámbricas más utilizadas se encuentra el WI-FI, cuya función es la interconexión de dispositivos electrónicos para intercambiar datos.

Las redes inalámbricas en un inicio estuvieron orientadas para uso empresarial, pero con la evolución de la tecnología móvil y el incremento de los usuarios las redes inalámbricas tomaron una expansión total lo cual permitió su utilización en lugares públicos y privados.

Hoy en día las instituciones adoptan estos mecanismos de comunicación con la finalidad de reducir los gastos y permitir la conexión de sinnúmero de dispositivos en la implementación de la red, por esta razón es de vital importancia contar con un sistema que garantice la seguridad de la información.

El portal cautivo es un sistema que controla el acceso de los usuarios, forzándolos a presentar las credenciales de identificación a través de una página web.

ANTECEDENTES

El portal cautivo se originó debido a la necesidad de administrar la seguridad en la red lo cual conllevo a el desarrollo de varios sistemas de control de tráfico http, en los últimos años la evolución de la tecnología ha permitido a los usuarios entrar a la red de forma segura y confiable, accediendo a los recursos de la misma solamente si se introduce correctamente su nombre y clave. Recientemente se agregaron muchas herramientas como lo son la funcionalidad inalámbrica, ancho de banda controlado, y calidad de servicio.

En el pasado las MIPYMES no contaban con una administración eficiente de los recursos de la red, lo cual ocasionaba problemas al momento de compartir la información. Hoy en día las MIPYMES han optado por incorporar técnicas que les faciliten la gestión de las redes garantizando seguridad en la transmisión y recepción de la información al usuario.

Para implementar este servicio en MIPYMES y realizar el estudio comparativo de las tecnologías de red inalámbrica se debe ubicar los puntos de acceso AP Mikrotik en lugares estratégicos del mismo para optimizar la zona de cobertura y poder gestionar el ingreso de usuarios a la red, para que puedan conectarse y tener acceso al servicio de internet durante un tiempo establecido.

En la actualidad la seguridad en las WLAN es de suma importancia para el administrador de red porque ayuda a se deben tomar precauciones con las características de las mismas para conservar la integridad, confiabilidad, seguridad y la utilidad máxima de la red. Tomando en cuenta estos parámetros es necesario emplear mecanismos para la gestión y el control de acceso para con los usuarios a través de la autenticación de los mismos.

El portal cautivo por hardware es aquel que está hecho mediante dispositivos físicos, los cuales han sido específicamente creados para su uso como portales cautivos, estos se agregan a la red de la misma manera que los dispositivos de networking. Mikrotik es una tecnología que apareció como un router basado en Linux que tenía iguales funcionalidades de los routers que se encontraban en el mercado, después se lanzaron soluciones para ISP llegando al año 1996 en el cual se introduce en el mercado de WISP donde fue tomando un gran crecimiento.

FORMULACIÓN DEL PROBLEMA

¿Es posible realizar el estudio comparativo de un portal cautivo mediante las tecnologías Mikrotik y Cisco para mejorar el rendimiento de una red inalámbrica en MIPYMES?

SISTEMATIZACIÓN DEL PROBLEMA

¿Es factible la implementación del portal cautivo en IPREX?

¿Es viable realizar una comparación de configuración del portal cautivo mediante las tecnologías Mikrotik y Cisco para la red inalámbrica?

¿Es posible mejorar el rendimiento de la red inalámbrica en IPREX?

¿Cuál es el comportamiento del portal cautivo implementado mediante Mikrotik?

JUSTIFICACIÓN DEL TRABAJO DE TITULACIÓN

JUSTIFICACIÓN TEORICA

El sector de las comunicaciones inalámbricas en el Ecuador ha sufrido una evolución significativa en los últimos años, lo cual hace necesario realizar investigaciones y análisis de las nuevas tecnologías y la manera de dar seguridad a las mismas de este modo surge esta iniciativa con el fin de analizar, implementar un portal cautivo el mismo que proveerá una solución a la seguridad de la red ya que para ingresar a la misma se deberá tener las respectivas IDs y contraseñas.

El presente proyecto ha sido basado en un estudio realizado en la Universidad Politécnica Salesiana Sede Quito por los tesistas Diego Mena y Jonathan Jara sobre “Análisis, Diseño y propuesta de implementación de un Portal Cautivo para la red inalámbrica de la Universidad

Politécnica Salesiana Sede Quito Campus Sur" obteniendo como resultado el análisis y funcionamiento de un portal cautivo optimizando el acceso de los usuarios en la red del Campus Sur.

El desarrollo del proyecto trata de realizar un estudio comparativo de la implementación de un portal cautivo mediante las tecnologías Mikrotik y cisco para mejorar el rendimiento de la red inalámbrica, con las condiciones físicas de la infraestructura que se tienen en IPREX ubicada en la ciudad de Riobamba, con el mismo se trata de solucionar la seguridad en la red de la Institución controlando el número de usuarios, ancho de banda asignados a los mismos dando a conocer las características de la tecnología que se utilizará en el presente trabajo de titulación.

La finalización del presente proyecto tecnológico dará como resultado la implementación de un portal cautivo mejorando el rendimiento de la red inalámbrica, realizando una comparativa de las tecnologías Cisco y Mikrotik en la implementación de portales cautivos en IPREX los cuales serán llevados a cabo bajo rigurosos procesos de seguridad y configuración de los dispositivos los mismos que se encuentran en constante competencia en el mercado de las comunicaciones inalámbricas.

JUSTIFICACION APLICATIVA

Actualmente la evolución de las comunicaciones inalámbricas en el Ecuador se centran en la implantación de redes públicas y comerciales del servicio de internet por parte de los proveedores de este servicio, instituciones públicas, privadas y muchos otros, ya que estas redes poseen ciertas inseguridades debido a que se encuentran en el espectro radioeléctrico se propone la implementación de un portal cautivo y la monitorización de la red lo cual nos permita gestionar a los usuarios que se conectan a la red y las características de su conexión.

Este proyecto surge debido a la necesidad de un estudio comparativo de las tecnologías pioneras en el mercado actualmente además de poder brindar seguridad a la red inalámbrica de la institución al restringir el acceso a usuarios no facultados al recurso de internet en la red inalámbrica mediante la utilización de portales cautivos. En el cual se utilizará los dispositivos de Mikrotik y Cisco, los cuales nos brindan muchos servicios y beneficios a la hora de gestionar los recursos de la red para esto se necesita primordialmente una clave de acceso y adicionalmente un control más riguroso sobre los usuarios que acceden a la misma, es ahí donde los portales cautivos cobran un interés especial.

Prever el volumen de tráfico de la red es difícil las tendencias de utilización cambian constantemente, la carga sube cuando menos lo esperamos, y los costes asociados pueden ser inmensos. Para mejorar el rendimiento de la red inalámbrica se tratará de gestionar de mejor manera los recursos disponibles en la red inalámbrica.

El beneficio principal que se obtendrá será el resultado de la comparación de estas dos tecnologías a la hora de implementar un portal cautivo y en la Mipymes será el tener una línea de seguridad enfocada a su red inalámbrica, como el bloqueo de usuarios no autorizados a acceder a la red lo que mejora el rendimiento y la calidad de servicio de la misma.

Este proyecto podrá ser implementado en otras redes inalámbricas de otros lugares que tengan las mismas características con algunos estudios y modificaciones a la configuración de los dispositivos Mikrotik y Cisco para que se adapte a la infraestructura a la que va a ser implementada.

OBTETIVOS

OBJETIVO GENERAL:

- Realizar un estudio comparativo de la implementación de un portal cautivo mediante las tecnologías Mikrotik y Cisco para mejorar el rendimiento de una red inalámbrica en MIPYMES.

OBJETIVOS ESPECIFICOS

- Investigar la información acerca del portal cautivo mediante las tecnologías Mikrotik y Cisco, sus características y aplicaciones requeridas de acuerdo con la red inalámbrica existente en la institución.
- Diseñar un modelo que permita determinar la tecnología más conveniente para la implementación del portal cautivo.
- Implementar el portal cautivo, utilizando las configuraciones de la tecnología más adecuada en IPREX.
- Evaluar los resultados de las pruebas realizadas al terminar la implementación para mejorar el rendimiento de la red inalámbrica.

MÉTODOS Y TÉCNICAS

MÉTODOS

La presente propuesta tecnológica de estudio comparativo de la implementación de un portal cautivo mediante las tecnologías Mikrotik y Cisco para mejorar el rendimiento de la red inalámbrica en IPREX es un trabajo de desarrollo el mismo que demanda además de un estudio a través de la aplicación de métodos, técnicas de investigación científica.

Para el estudio sobre la red inalámbrica y la implementación del portal cautivo es indispensable abordar una investigación descriptiva ya que se describirá el funcionamiento del hardware y las configuraciones del software además del estado actual de la tecnología inalámbrica presente en IPREX donde se desarrollará el diseño e implementación, esto permitirá obtener resultados más realistas.

Una vez concluido el estudio de la tecnología y sus características se pretende realizar un estudio comparativo de la implementación de un portal cautivo mediante tecnologías Mikrotik y Cisco para mejorar el rendimiento de una red inalámbrica, se debe realizar un análisis cualitativo que permita seleccionar la mejor tecnología.

Dentro de la implementación del portal cautivo se logrará optimizar el funcionamiento de la red inalámbrica además que se conseguirá analizar las características del mismo, para lo cual se describe un trabajo comparativo ya que permite obtener resultados de los recursos ocupados anteriormente por el portal cautivo implementado por tecnología Mikrotik y otro implementado con tecnología Cisco, estudiando el comportamiento de la red con el portal cautivo en funcionamiento.

La presente propuesta tecnológica posee una connotación de desarrollo transversal debido a que el diseño e implementación de un portal cautivo y monitorización de tráfico de red inalámbrico requiere de 4 etapas de desarrollo alcanzados en cortos ciclos de tiempo donde se efectuará cada una de las actividades descritas a continuación:

El ciclo de vida adoptado para la ejecución del proyecto de tesis es:

- Indagar la información y detalles del tema que permitan la elaboración del trabajo de titulación.
- Elegir la información segmentándola en fases que faciliten la configuración de un portal cautivo.
- Diseño e implementación de un portal cautivo tomando en cuenta las configuraciones existentes para cada tecnología.
- Pruebas y evaluación, en esta etapa se analizará el tráfico existente en la red inalámbrica con las dos tecnologías realizando una comparativa del rendimiento de la misma.
- Conclusiones y Recomendaciones

TÉCNICAS

Las técnicas de investigación que se emplearan son:

La Observación. - esta técnica nos permitirá observar detalladamente el funcionamiento de la red inalámbrica y registrar la información para su posterior análisis y aplicación de métodos correctivos para la implementación de un portal cautivo.

La Documentación. - la aplicación de esta técnica nos permitirá recopilar la información utilizando herramientas de software y hardware para llevar a cabo el análisis de los resultados obtenidos después de la implementación del portal cautivo y mejoramiento de la red inalámbrica.

CAPÍTULO I

1 MARCO TEÓRICO

El diseño e implementación de las redes de computadoras se ha realizado para brindar un sin número de servicios además de compartir información lo cual ayuda a optimizar el ambiente laboral y personal de los beneficiarios de la misma.

1.1 Redes Inalámbricas

Gracias al gran avance de la tecnología en los últimos años se han creado nuevos tipos de transmisión y comunicación de los datos que día tras día se enfocan más en lo inalámbrico.

Las redes inalámbricas están basadas en un medio de transmisión no guiado, lo cual quiere decir que no hace falta cables para poder realizar la comunicación en donde se usan ondas electromagnéticas, por lo que para poder transmitir y recibir información se hace necesario el uso de antenas.

Los usuarios se conectan a la red inalámbrica en donde encuentran datos, información y la mayoría de los recursos de la red, esto se lo logra sin necesidad de conectarse físicamente a la red ya que funciona como una red cableada la cual tiene varias ventajas como lo son la movilidad, un costo bajo de implementación, y una rápida instalación.

1.1.1 *Caracteristicas de una Red Inalámbrica*

Los usuarios corporativos y también los usuarios finales prefieren esta tecnología ya que las redes inalámbricas brindan las siguientes características:

- **Cobertura:** en este aspecto brindan servicio a donde el cable no puede llegar.
- **Escalabilidad:** la red inalámbrica no necesita de grandes cambios para la suma de nuevos usuarios, además que es adaptable a los distintos tipos de topologías que los usuarios requieran.
- **Flexibilidad de instalación:** la fácil conectividad que permiten estas redes inalámbricas es muy amplia llegando a espacios donde el cable difícilmente podría hacerlo.
- **Implementación a bajo costo:** en un principio la inversión que se requiere para la implementación de la red LAN puede ser costosa, pero a largo plazo los ahorros que generan son muy altos.

- **Movilidad:** el poder trabajar desde cualquier lugar en la empresa trae consigo un sinnúmero de beneficios lo cual mejora la productividad y el desempeño de los usuarios.
- **Facilidad y Simplicidad de instalación:** ya que al ser una tecnología inalámbrica no necesita de cableado para su funcionamiento evitando dañar la estética de la empresa lo cual genera una reducción en los tiempos de instalación.

1.1.2 Redes de Area Local Inalámbrica (WLAN)

Un área cubierta por una red que es igual a la red local de una organización es conocida como una WLAN, con aproximadamente una distancia de 100 metros de alcance lo cual permite que las terminales que están dentro de la zona de cobertura se puedan conectar entre sí. El brindar conectividad y flexibilidad a cambios de la red como el cambio de dispositivos o extensión de la misma es uno de los objetivos principales de la WLAN.

La facilidad de instalación y los beneficios en cuanto a gastos se refiere ya que se elimina en su mayoría el medio de transmisión cableado es su principal atrayente, aun así en cuanto a su velocidad que va entre los 2 Mbps y los 10 Mbps y la de una red convencional que puede llegar hasta los 100 Mbps las redes inalámbricas son una alternativa absoluta para lograr que una red convencional llegue a lugares a donde el cableado no lo permita por lo que se usaran es su mayoría como complementos de una red fija.

1.1.2.1 *Configuración WLAN*

Dependiendo de los requerimientos del sistema que deseemos implementar y las carencias que se vayan a cubrir el grado de dificultad de una red inalámbrica son distintas, para esto se puede usar varias configuraciones de red.

A. Peer to peer o red ad-hoc

Está conformada por dos terminales móviles equipadas con tarjetas de red inalámbrica las cuales están dentro de un rango de cobertura radioeléctrica esta es la configuración más básica lo cual hace que sea muy fácil de implementar y no necesita de administración de red.

B. Modo infraestructura

Tomando la configuración anterior como base se requiere aumentar el alcance de una red para lo cual se necesita un punto de acceso, la red inalámbrica con esta nueva unidad aumenta su alcance ya que la distancia máxima ya no es entre dos estaciones, es entre cada estación y el punto de acceso.

El punto de acceso tiene una gran ventaja ya que puede conectarse sin problema a otras redes y en especial a una red fija lo cual permite a los usuarios tener acceso a otros recursos, es necesario varios puntos de acceso para cubrir una zona específica.

C. Enlace entre varias LAN

Una de las configuraciones viables trae consigo antenas direccionales. Tomando en cuenta que varios sitios a conectarse se encuentran geográficamente distantes se usan antenas direccionales lo que permite un enlace entre redes alejadas considerablemente logrando interconectar redes locales.

1.2 Estándar Inalámbrico IEEE

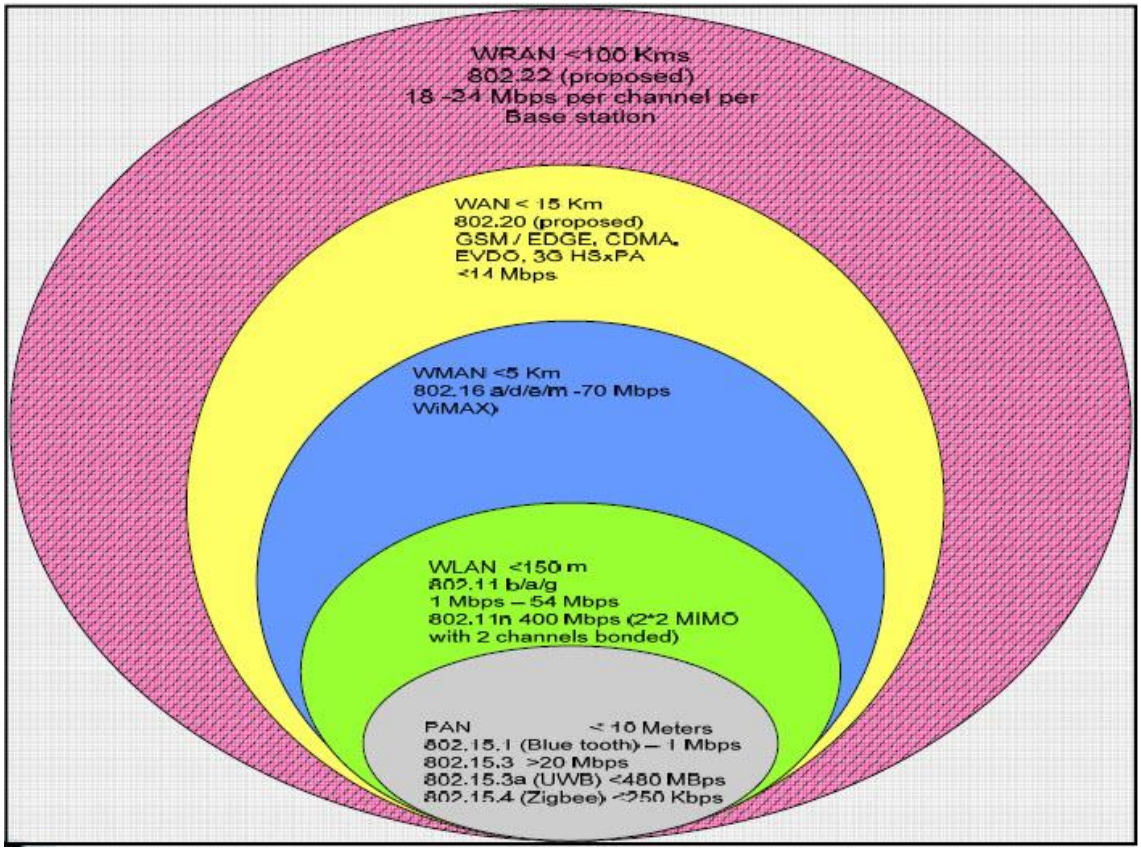


Figura 1-1: Estándares de comunicación inalámbrica

Fuente: http://nhprice.com/wp-content/uploads/2013/08/Wireless-Speeds.jpg

1.2.1 *IEEE 802.11*

La versión original consolidada en el año de 1997 se propaga mediante señales infrarrojas (IR) con velocidades de propagación teóricas que van de 1 a 2 Mbps a 2.4 GHz. Además, se define el protocolo CSMA/CA (Múltiple acceso por detección de portadora) como una técnica de acceso, el cual es usado para evitar las colisiones que se pueden ocasionar entre los paquetes de datos

enviados o recibidos. Este estándar ha sufrido varias modificaciones y mejoras obteniendo de este modo las siguientes:

- **802.11a**

Certificada en el año 1999 trabaja en la banda de 5 GHz y tiene 52 subportadoras (OFDM) con una velocidad de hasta 54 Mbps además posee 12 canales no solapados, utiliza los protocolos de la versión original brinda una gran ventaja ya que existe una menor interferencia.

OFDM: Admite la transmisión de grandes cantidades de información digital sobre una onda de radio ya que es una técnica de modulación FDM.

- **802.11b**

Su revisión fue ratificada en 1999, 802.11b adquiere una velocidad de hasta 11 Mbps utilizando el método de acceso del original CSMA/CA opera en la banda 2.4 GHz. Es una extensión del método de modulación DSSS lo cual ocasiono que los productos fueran actualizados de una manera rápida convirtiéndolo en la tecnología WLAN definitiva.

DSSS: El espectro ensanchado es modulado con este método para su propagación de señales digitales sobre ondas de radio.

- **802.11g**

Aprobada en el año de 2003, usa la banda de 2.4 GHz la misma que 802.11b pero tiene una velocidad real de transferencia de 25 Mbps y una velocidad teórica de hasta 54 Mbps de transferencia, es compatible con el estándar 802.11b ya que utiliza las mismas frecuencias por el proceso de diseño por el que paso para hacer compatibles a los dos estándares.

- **802.11n**

En enero de 2004, la IEEE anuncio la formación de un grupo de trabajo 802.11 para desarrollar una nueva revisión del estándar 802.11 la velocidad real de transmisión podría llegar a los 500 Mbps (lo que significa que las velocidades teóricas de transmisión serian aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b.

802.11n se construye basándose en las versiones previas al estándar 802.11 añadiendo MIMO (Multiple-Input Multiple-Output). MIMO utiliza múltiple transmisores y antenas receptoras permitiendo incrementar el tráfico de datos. (Claver y Martínez, 2014, https://repositorio.uade.edu.ar/xmlui/bitstream/handle/123456789/2454/Claver.pdf?sequence=1)

1.3 Seguridad en Redes Inalámbricas

Un punto crítico en una red es su seguridad debido a que el tipo de transmisión en las WLAN es por aire, la información es vulnerable ya que es receptada por cualquier equipo que esté al alcance del área de cobertura, logrando así tener acceso a la red lo que le permite generar el quebrantamiento, ataque, sustracción y manipulación de los datos que circulan en la red inalámbrica, dicha información pertenece a la empresa o a una persona con el único objetivo de perjudicar y dañar a la misma.

Una de las principales desventajas de utilizar una red inalámbrica es que está expuesta a amenazas y ataques:

- **Amenazas Estructuradas:** Lo realizan personas que no tienen experiencia en ataques informáticos, poseen herramientas para poder hackear una clave de acceso en su mayoría.
- **Amenazas No Estructuradas:** Estas amenazas son más técnicas ya que son realizadas por personas que tienen conocimientos en programación y que conocen en gran medida las vulnerabilidades de las WLAN´s, desarrollando scripts o programas para realizar el ataque.
- **Amenazas Internas:** Son generadas por el personal que cuentan con el acceso físico al servidor y están dentro de la red los cuales pueden exponer la red a posibles ataques externos.
- **Amenazas Externas**: Los ataques provienen de personas que no tienen acceso autorizado a la red inalámbrica y que son extrañas a la misma. (Mena y Jara, 2013, http://dspace.ups.edu.ec/bitstream/123456789/5348/1/UPS-ST001027.pdf)

Existen varios mecanismos de seguridad en las WLAN´s entre los cuales mencionaremos:

- **SSID (Service Set Identifier):** Es el nombre que está dentro de los paquetes de la red inalámbrica lo cual permite identificarla, el usuario debe poseer en su configuración el mismo SSID que el Access Point.

- **Filtrado de dirección MAC:** Una de las maneras de evitar la intrusión de usuarios no autorizados es aceptar las solicitudes de ciertos nodos de la red inalámbrica.

1.4 Protocolos de Encriptación

Son protocolos de abstractos que tienen funciones de seguridad en la cual se aplican métodos criptográficos que permiten incorporar varias características de seguridad.

1.4.1 ***WEP (Wired Equivalent Privacy).-***Es uno de los primeros protocolos de encriptación que constaban en el estándar IEEE 802.11, provee la confidencialidad, autenticación y control de los datos transmitidos en una red inalámbrica de igual manera que las LAN´s.

Usa el algoritmo de cifrado RC4 (Rivest Cipher 4), para cifrar los datos que se interconectan entre el punto de acceso y los clientes. RC4 brinda una clave de manera pseudo-aleatoria la cual tiene una extensión semejante al texto original, esta se crea utilizando una clave secreta que es dad por el usuario con una longitud de 40 o 104 bits.

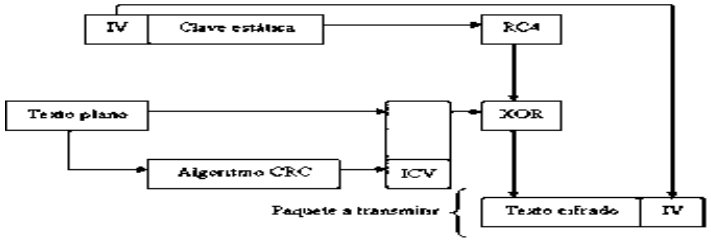


Figura 2-1: Funcionamiento del cifrado WEP

Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf

1.4.2 ***WPA (Wifi Protect Access)*:** Es una solución a las debilidades del protocolo WEP, la cual fue lanzada por la alianza WI-FI consiste en brindar diferentes claves a cada cliente lo que permite fortalecer la integridad de los datos. (García y Hytnen, 2006, An analysis of wireless security. Journal of Computing Sciences in Colleges)

El algoritmo que usa WPA es RC4 el mismo que en WEP, pero tiene una característica adicional la cual comprueba la integridad de los mensajes ICV, además que se cambió el código de detección de errores del protocolo WEP por MIC (Message Integrity Code).

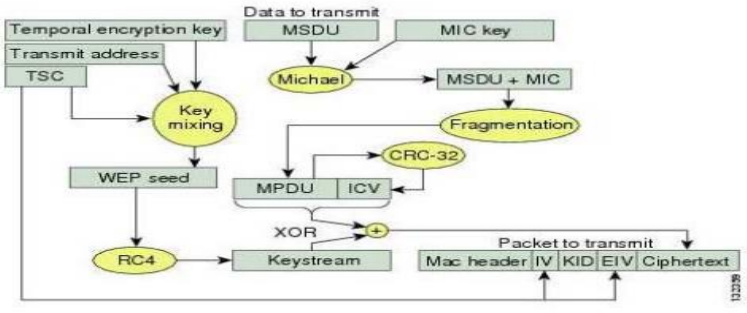


Figura 3-1: Funcionamiento del cifrado WPA

Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf

WPA funciona de dos maneras:

1.4.2.1 ***WAP-PERSONAL:*** este modo no usa un servidor de autenticación para su implementación en una infraestructura, está basada en la compartición de una clave (PSK) entre el Access Point y el usuario la misma que se usa como el inicio de la autenticación mas no para el cifrado de la información.

1.4.2.2 ***WAP-ENTERPRISE*:** Utiliza de manera general un servidor RADIUS el cual trabaja como un servidor de autenticación, requiere una implementación más compleja ya que brinda seguridad extra en la red inalámbrica.

1.4.3 ***WPA2 (Wifi Protect Access 2):*** Ratificado en el año de 2004 este estándar 802.11i se generó para corregir las vulnerabilidades que da el protocolo WEP. Es más seguro, pero no es compatible con el hardware anterior, WPA2 intercambia la clave de manera dinámica, un cifrado robusto y la autenticación del cliente.

Posee un nuevo algoritmo de cifrado AES (Advanced Encryption Standar). Es un algoritmo de cifrado de bloque simétrico ya que utiliza la misma clave para cifrar y descifrar. Usa el cifrado AES en lugar de MIC además de llaves de 128 bits con vectores de inicialización de 48 bits. (Luaces, 2013, seguridad en redes inalámbricas de área local WLAN, http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf)

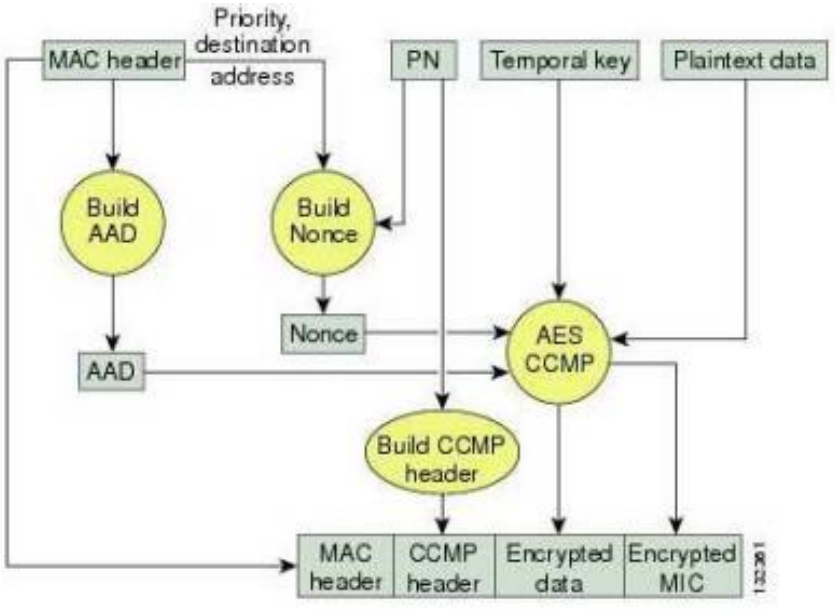


Figura 4-1: Funcionamiento del cifrado WPA2

Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf

1.4.4 ***Autenticación 802.1x:*** Este protocolo forma parte del estándar IEEE 802 para redes por medio guiado cableadas, el estándar 802.11i dispone a 802.1x como el protocolo usado

para la autenticación. Brinda un sistema de control de tráfico y gestión de claves para usuarios. El estándar 802.1x usa el protocolo EAP la cual le da una flexibilidad en la metodología de la autenticación.

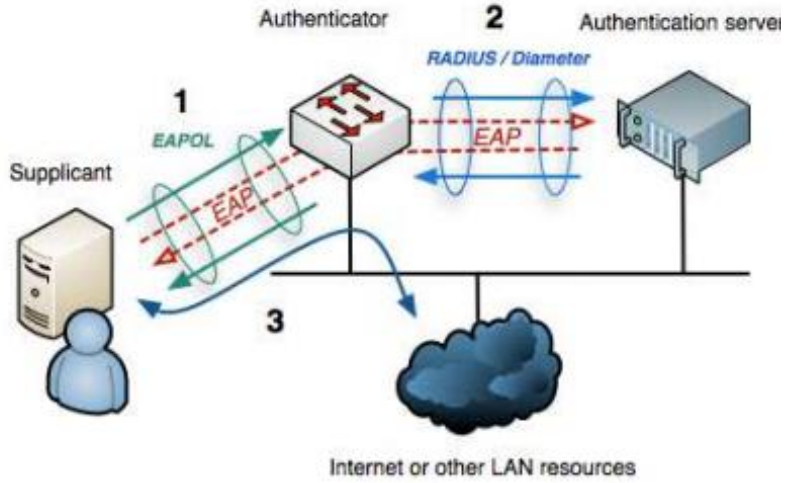


Figura 5-1: Arquitectura 802.1x

Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf

1.4.5 ***Autenticación EAP (Extensible Authentication Protocol):*** es una extensión del protocolo PPP (Point-to-Point Protocol) este protocolo adiciona seguridad a 802.11i ya que funciona como autenticador mutuo entre el usuario y el servidor, se acuerda una clave que se usara únicamente cuando la sesión este activa, se puede sumar varios esquemas de autenticación si se utiliza EAP.

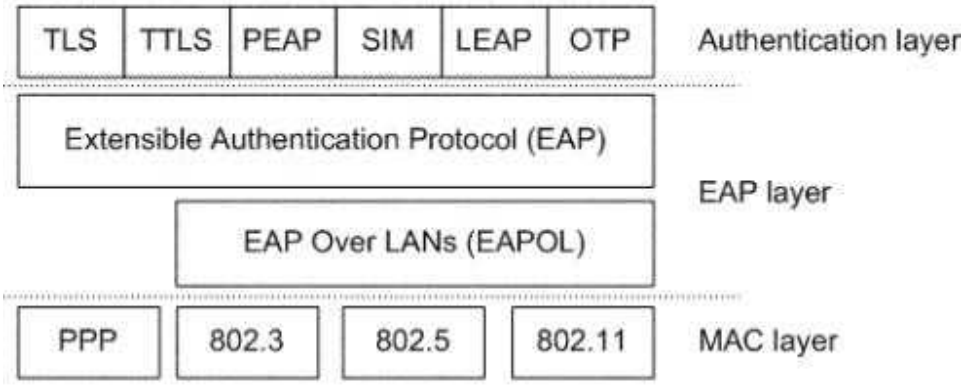


Figura 6-1: Protocolo EAP

Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf

1.5 Portal Cautivo

Proporciona una url a través de varios métodos (DHCP IPV4, DHCP IPV6) al cliente para acceder a la página de autenticación en donde coloca su número de usuario y password con la cual accede a las funciones de la red, es un método de seguridad que se puede aplicar únicamente a redes inalámbricas.

Figura 7-1: Portal Cautivo Mikrotik

Fuente: https://http2.mlstatic.com/S_381421-MLM20772652350_062016-O.jpg

1.5.1 *Tipos de Portales Cautivos*

Los portales cautivos se dividen en dos grupos principales los cuales son:

1.5.1.1 *Portal Cautivo por Sotware*

Son programas o aplicaciones los cuales fueron diseñados exclusivamente para implementarse como portales cautivos, los cuales están instalados en un servidor que se encuentra en la misma red.

Se enumeran a continuación los portales cautivos más usados:

- Wifidog (embedded Linux- Open WRT, Linux, Windows)
- PeperSpot (Linux)
- Chillispot (Linux)
- Easy Captive (Linux)
- Zeroshell (Linux)
- Easyspot (Linux), entre otros.

Figura 8-1: Portal Cautivo ChilliSpot

Fuente: http://www.chillispot.org/images/chillispot-20050511.png

1.5.1.2 *Portal Cautivo por Hardare*

Están diseñados principalmente para funcionar como portales cautivos están implementados por dispositivos físicos, tienen la misma función que los mencionados anteriormente se agregan a la red de la misma manera que los dispositivos de Networking.

A continuación, se mencionan los más utilizados:

- Cisco BBSM-Hotspot
- Nomadix Gateway
- Antamedia Hotspot Gateway
- Mikrotik RouterOS (5)

Figura 9-1: Portal Cautivo por Hardware

Fuente: http://slideplayer.com/24/7525637/big_thumb.jpg

1.5.2 *Funcionamiento de los Portales Cautivos*

Los portales cautivos se despliegan a través de un navegador web funcionan en todos los dispositivos con comunicación inalámbrica, se usan de manera global en redes inalámbricas abiertas es trascendental tener un control de acceso de los usuarios a nuestra red inalámbrica y por ende a la navegación web. (Fierro & Gonzales, 2001)

En primer lugar, el usuario busca la SSID en la cual desea conectarse luego de encontrarla se conectara y solicitara una contraseña que le asegure el acceso para validar el ingreso a la misma.

Seguidamente ya en la red inalámbrica no podrá navegar libremente en otras páginas ya que será re direccionado al portal cautivo y se verá imposibilitado de ocupar la información de la red hasta que se ingresen las credenciales de acceso.

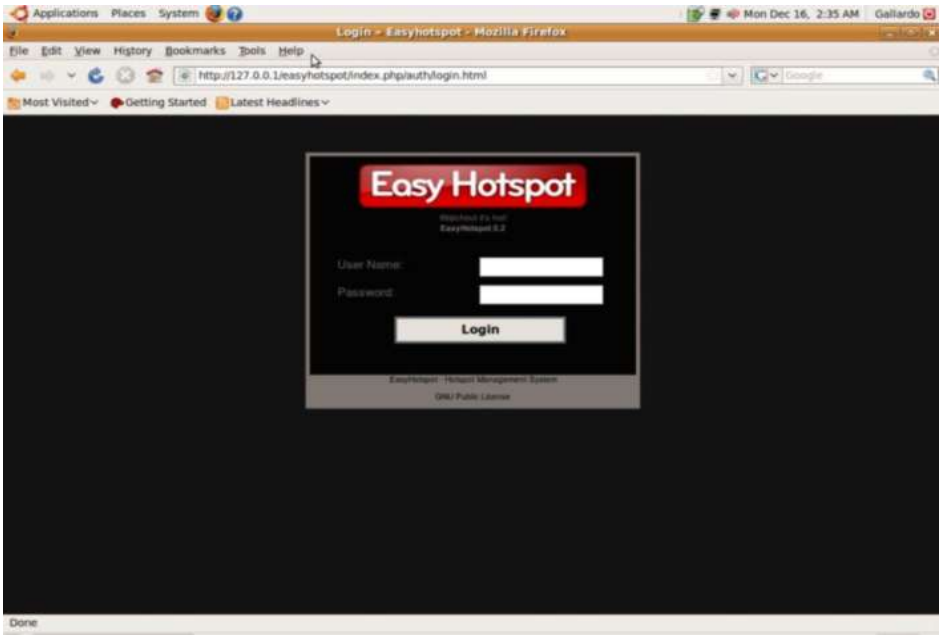


Figura 10-1: Petición de credenciales para el ingreso del usuario

Fuente: http://3.bp.blogspot.com/-cu8wUB5_FJc/Us5l5wLucrI/AAAAAAAAGAw/Zp9kuYSXBtY/s1600/easy5.png

Una vez ingresadas las credenciales serán verificadas por el portal cautivo el cual no dará paso al uso de la red inalámbrica hasta que se validen las credenciales de acceso del usuario.

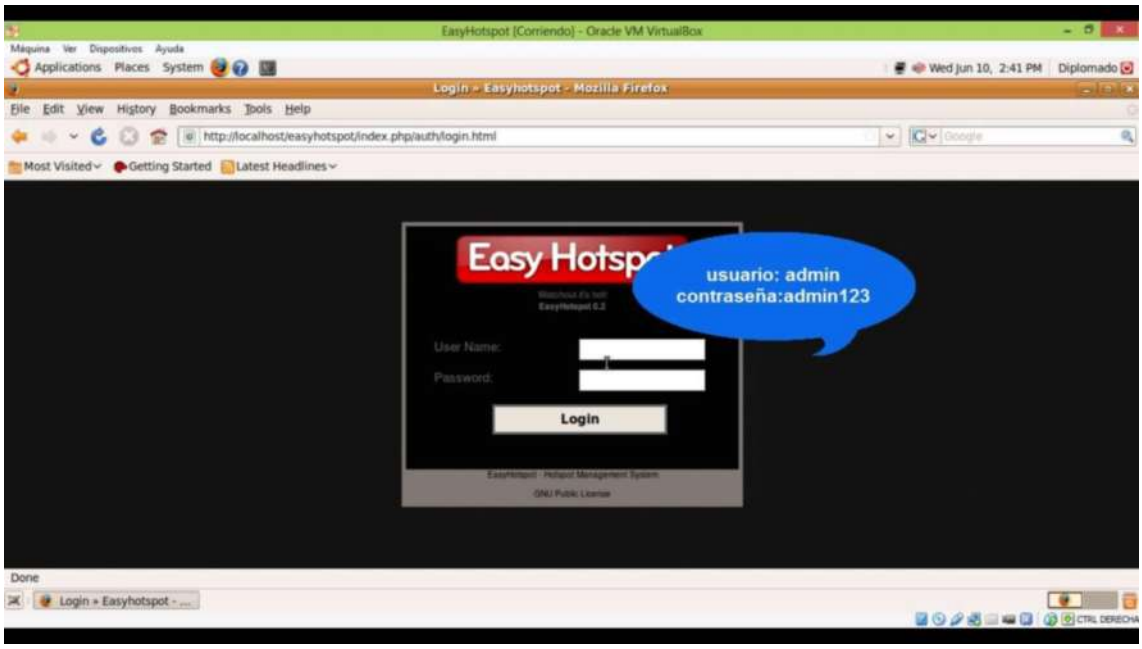


Figura 11-1: Ingreso de credenciales de usuario

Fuente: https://i.ytimg.com/vi/tYNOhR94uEo/maxresdefault.jpg

Al terminar el proceso de verificación hecho por el portal cautivo se direcciona a la página que ha sido configurada por el administrador lo cual le permite al usuario hacer uso del servicio de internet o información que se comparta en la red inalámbrica.

Uno de los beneficios que ofrece el portal cautivo es que vuelve a una red inalámbrica dinámica y funcional, al utilizar claves para los usuarios se controla el acceso de los mismos y aumenta la seguridad de acceso en la red. Si un usuario se ha conectado a la red, pero no posee una cuenta creada por el servidor del portal no podrá ingresar a ningún recurso ni mucho menos enviar tráfico a la red inalámbrica. (Maldonado, 2012, http://www.dspace.ups.edu.ec/bitstream/123456789/4167/1/UPS-ST000959.pdf)

Las ventajas que ofrecen los portales cautivos son muchas de entre la cuales se pueden resaltar:

- Usan Autenticación Centralizada.
- Se aplican políticas de acceso por usuario.
- Brinda estadísticas por usuario

Una de las desventajas de usar este tipo de solución es que si el dispositivo móvil no posee un navegador instalado no es posible la autenticación del usuario, los protocolos de aplicación no son cifrados, los usuarios que estén unidos a la red son visibles, aunque no estén con una sesión iniciada.

1.5.3 ***Protocolo AAA***

En seguridad informática, el protocolo AAA realiza tres funciones principales Autenticación, Autorización y Contabilización (Authentication, Authorization and Accounting). (García. Proyecto AAA.2008), provienen de una familia de protocolos que brindan los servicios detallados anteriormente.

Además, el protocolo AAA está preparado para autenticar a los usuarios, dando una respuesta a las solicitudes de autorización de los mismos y almacenar los datos, lo cual permitirá llevar un control de recursos a los que se ha tenido acceso.

1.5.3.1 Autenticación (Authentication)

Es la comprobación de una identidad reclamada de tal manera que haya una preexistente ya conocida por ambos (servidor, usuario), esta autenticación es dada a través de la presentación de un nombre de usuario y la verificación de la tenencia de la credencial lo cual permite comprobarla.

1.5.3.2 Autorización (Authorization)

Consiste en establecer si un determinado derecho, como el acceso a un recurso de la red se puede dar al usuario que presente una credencial, es la concesión de privilegios a un usuario basándose en su identidad y como se encuentra en el sistema.

1.5.3.3 Contabilizacion (Accounting)

Es el recolectar información sobre el uso de los recursos con el afán de realizar un estudio o análisis de cómo se han utilizado los mismo y las tendencias de los usuarios elaborando así un informe, facturación, auditoria o coste de asignación de los recursos usados.

1.5.4 ***Radius***

Radius (Remote Authentication Dial-In User Service) es un protocolo cliente/servidor, donde el cliente es un NAS (Network Access Server) y el servidor es un software el cual esta implementado en una máquina. (Lazo Nuttsy, 2012)

Utilizado para controlar el acceso a la red, opera como un servidor de autenticación de usuarios que ingresan de manera remota a un servicio de la red. (Aboba, 2003, Radius RFC 2869, http://www.faqs.org/rfcs/rfc3579.html)

Radius satisface 3 necesidades específicas Autenticación, Autorización y Contabilidad de uso.

1.5.4.1 *Cliente Radius*

NAS (Netwok Access Server) podría ser un AP, un switch, servidores de acceso remoto entre otros los cuales son dispositivos de comunicación que nos sirven como medios de acceso a la red sea esta cableada, inalámbrica, ADSL. Será el encargado de reenviar las peticiones de acceso y según la respuesta del servidor este dará autorización o no al acceso del usuario.

1.5.4.2 *Servidor Radius*

Es un software que está instalado en un sistema operativo y es el que administra el acceso de los usuarios a la red, recibe la autenticación y después de comparar las credenciales envía un mensaje negando o permitiendo el acceso, almacenando además los eventos de los procesos.

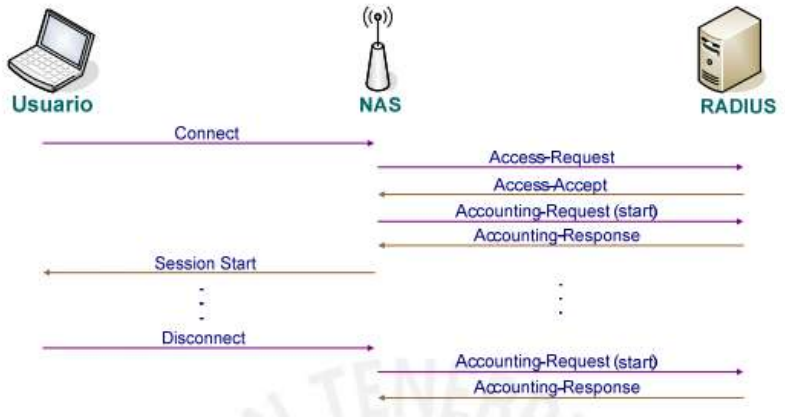


Figura 12-1: Intercambio de mensajes en RADIUS

Fuente: "Sistema de Autenticación" (TEC 2008)

1.5.4.3 TACACS+

Garantiza la transmisión al usar el protocolo TCP ya que es un protocolo de la capa de aplicación al enviar el paquete deja intacta la cabecera TACACS+ y cifra el cuerpo del mismo. Cada operación entre el cliente y servidor AAA usa una conexión dedicada TCP, para evitar tener carga en el servidor se puede realizar una sola sesión establecida la cual está vigente hasta que el dispositivo o el servidor estén funcionando. (CISCO, 2009)

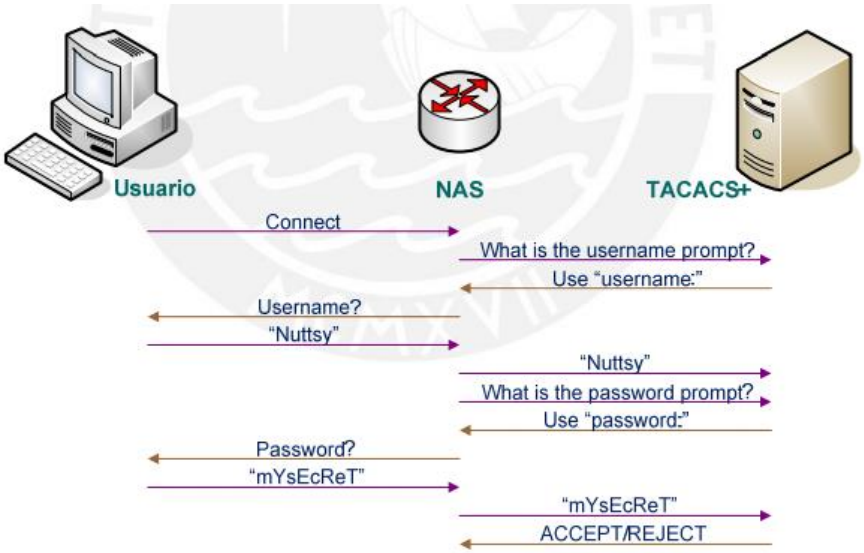


Figura 13-1: Autenticación TACACS+

Fuente: "Servidor TACACS+" (CISCO 2009)

1.5.4.4 PPP (Point To Point Protocol)

Brinda un estándar para transporta datagramas multiprotocolo a través de enlaces punto a punto. Este protocolo se compone de tres componentes principales:

1. Un método para encapsular datagramas multiprotocolo
2. Un protocolo de control de enlace (LCP) para establecer, configurar, y probar la conexión de enlace de datos.
3. Una familia de Protocolos de Control de Red (NCP) para establecer y configurar diferentes protocolos de capa de red. (Red de grupo de trabajo W. Simpson, Protocolo PPP1994, https://www.rfc-editor.org/rfc/rfc1661.txt)

1.5.4.5 EAP (Extensible Authentication Protocol)

Brinda su propio soporte para borrar la retransmisión y duplicados de datos, corre bajo un enlace de datos tales como capas soportan la autenticación de múltiples métodos. Puede ser usado en enlaces dedicados, así como circuitos conmutados ya sea por cable e inalámbricos.

1.5.4.6 *LDAP*

Trabaja a nivel de aplicación lo cual le otorga el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. (García, Proyecto Entorno AAA, 2008)

1.5.4.7 *MYSQL*

Es sistema de bases de datos relacionales rápido, sólido y flexible. (Angel Cobo. Tecnologías para el desarrollo de Aplicaciones Web.2005:340)

Permite soportar una gran cantidad de datos de manera práctica y eficiente cuando se tiene varias consultas. Debido a su acogida por parte de los informáticos y especialistas en esta rama MYSQL es uno de los gestores de base de datos más usado en la mayoría de empresas. Posee un gran número de ventajas entre las cuales se resaltan:

- Licencia Pública.
- Sistema cliente/servidor.
- Es compatible y portable a varias plataformas informáticas.
- Permite la unión con aplicaciones que trabajen con C y C++.
- Brinda soporte a la sintaxis con el lenguaje SQL

1.6 **Linux**

Es un sistema operativo de código abierto de la familia Unix esto significa que provee un ahorro en los costes de su instalación en los equipos ya que tiene distribución gratuita. Quien completa el completo funcionamiento del sistema operativo es el administrador (root), puede realizar las operaciones más convenientes en el sistema además que tiene acceso completo a los dispositivos de la máquina.

El usuario root debe tener un completo conocimiento sobre el sistema para realizar las configuraciones más convenientes en el mismo, debe conocer mejor que nadie sus equipos, sus aplicaciones y los usuarios, ya que así los mantendrá al día con los avances y las mejoras que presenta el sistema operativo.

1.6.1 ***Características***

- Multiusuario, ya que brinda un acceso a los recursos a varios usuarios.
- Multitarea, da al usuario la posibilidad de realizar varias tareas a la vez.
- Soporta diferentes tipos de arquitecturas.
- Soporta innumerables tipos de sistemas de archivos.
- Agiliza y mejora la utilización de la memoria en el sistema.
- Es compatible con Unix System y BSD en el código fuente.
- Soporta gran cantidad de protocolos y dispositivos de red.

1.7 **Router**

Es un dispositivo de enrutamiento de red ya que determina la mejor ruta para alcanzar otras redes, es el responsable de dirigir los paquetes destinados a redes locales y remotas. (Cisco, CCNA 2 V4.0. 2010)

1.7.1 ***Arquitectura Interna del Router***

El router funciona de igual manera que una Pc convencional esto quiere decir que incluye:

- Unidad de procesamiento central (CPU).
  Es aquí en donde se ejecutan todas las instrucciones del sistema en uso como lo son el inicio del sistema y las funciones de enrutamiento.
- Memoria de acceso aleatorio (RAM).
  La memoria RAM guarda la información, los datos y las instrucciones que debe ejecutar la CPU es donde se almacena el sistema operativo, los archivos de

configuración que se están ejecutando, las tablas de enrutamiento y los buffers de los paquetes.

- Memoria de solo lectura (ROM).

  Tiene la capacidad de almacenar la información de manera permanente, además utiliza un software incorporado en el circuito integrado el cual se lo conoce como firmware en donde se encuentran las instrucciones de inicio del router.

1.8 **Tecnología Mikrotik**

Mikrotik es una empresa de Letonia que desarrollo un software que gestiona placas conmutadoras llamadas RouterOS las mismas que se encuentran acentuadas en Linux lo cual da al usuario la posibilidad de conectarse, accesar a la configuración y administrar la red. Esta tecnología brinda la posibilidad de establecer VPNs, DHCP Server, QoS, Firewall, entre otros además de la implementación de Puntos de acceso inalámbrico

Poseen varios dispositivos de comunicaciones normalmente routers que han evolucionado con el pasar del tiempo con el fin de ir a la par con la resolución de necesidades y problemas que tienen sus clientes en cuanto a la administración de la red, son muy manejables ya que son menos costosos que los routers tradicionales. Siendo el preferido en empresas públicas y privadas especialmente en los proveedores de internet.

Figura 14-1: Logotipo de la empresa Mikrotik

Fuente: https://home-assistant.io/images/supported_brands/mikrotik.png

1.8.1 ***Características***

Las características que resaltan de Mikrotik según (PerúMikrotik, 2010) son:

- La conexión con el proveedor de internet es mejorada significativamente.
- Posibilidad de administrar el ancho de banda por usuario.
- Configuración por interfaz gráfica y comandos.
- Brinda la opción de bloquear páginas web no deseadas.
- Almacena contenido de la web como imágenes, archivos de actualización, descargas, etc., gracias a que tiene incorporado Webcache y Proxy (no almacena videos).

1.8.2 ***RouterOS Mikrotik***

Según (Parra Jorge.2014:13) RouterOS Mikrotik es un sistema operativo con aplicaciones de enrutador de software los cuales permiten funciones como firewall, VPN servidor y cliente, Ancho de Banda con calidad de servicio, y muchas otras características usadas para el enrutamiento y conexión de redes.

1.8.2.1 *Características*

Tiene soporte a varias aplicaciones de red las cuales son usados sin importar el tamaño de la misma tales como OSPF, BGP, VPLS/MPLS. RouterOS es un sistema versátil y estable que ofrece soporte para todas las interfaces de red.

1.8.2.2 *Estructura*

El router está basado en el Kernel de Linux, lo que le permite ejecutarse desde discos IDE o módulos de memoria flash haciéndolo actualizable gracias a su diseño modular guiándose en una interfaz gráfica de fácil uso amigables para el usuario.

1.8.2.3 *Routerboard Mikrotik*

Mikrotik ha desarrollado una plataforma de hardware a la cual ha llamado RouterBoard los mismos que funcionan gracias al sistema RouterOS, van desde pequeños CPEs inalámbricos hasta routers que contienen un núcleo de gran potencia cada uno con sus características y funcionalidades específicas de acuerdo a lo requerido por el usuario.

1.8.3 ***Dispositivos Mikrotik***

1.8.3.1 *Routerboard RB750G*

Es un router que lleva 5 puertos Gigabit ethernet autónomos con opciones de rendimiento para el cable ethernet, tiene un diseño compacto que se adapta en cualquier entorno.

Figura 15-1: Routerboard RB750G

Fuente: https://routerboard.com/rb750g

- Tamaño de memoria RAM 32 MB
- Puertos ethernet de alta velocidad
- Sistema Operativo RouterOS
- Nivel de licencia 4

1.8.3.2 *Routerboard RB750R2*

Es un router que se adapta a cualquier entorno debido a su diseño, es uno de los dispositivos MPLS más pequeños y baratos disponibles en el mercado hoy en día.

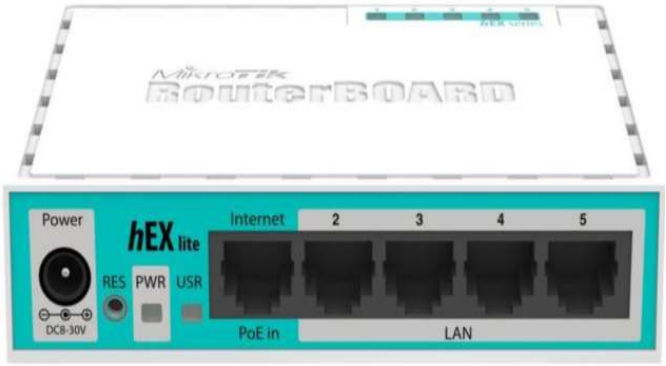


Figura 16-1: Routerboard RB750R2

Fuente: https://ftp3.syscom.mx/usuarios/fotos/RB750R22/RB750R2.jpg

- Tamaño de memoria RAM 64 MB
- 5 puertos 10/100 ethernet
- Sistema Operativo RouterOS
- Nivel de licencia 4

1.8.3.3 *Routerboard RB951Ui-2HnD*

Es el router ideal para casas y pequeñas oficinas ya que posee gran variedad de configuraciones que se adaptan a las necesidades requeridas además es portátil y fácil de instalar.

Tiene una gran variedad de usos en debido a su portabilidad y su facil manejo, es compacto y se adapta a cualquier tipo de entorno de trabajo.

Figura 17-1: Routerboard RB951Ui-2HnD

Fuente: http://www.techyshop.co.ke/wp-content/uploads/2015/10/MikroTik-RB951G-2HnD.jpg

- Memoria RAM 128 MB
- 5 puertos Fast Ethernet 10/100 Mbps
- Wi-fi con protocolo 802.11 b/g/n
- Sistema Operativo RouterOS
- Nivel de licencia 4

1.8.3.4 *Routerboard tipos de licencia*

Los dispositivos RouterBoard se encuentran con una licencia RouterOS preinstaladas es decir que si se adquiere un dispositivo no se puede hacer nada con respecto a la licencia adquirida. RouterOS y su sistema de licencias se basa en un número de ID de software que está ligado a medios de almacenamiento de los dispositivos.

```
[Admin @ RB1100]> / licencia del sistema de impresión
   software-id: "43NU-NLT9"
       nLevel: 6
     caracteristicas:
[Admin @ RB1100]>
```

Figura 18-1: Licencia de equipo RouterBoard RB1100

Fuente: https://wiki.mikrotik.com/wiki/Manual:License

1.8.4 ***Niveles de Licencia***

Mikrotik cuenta con una alta gama de licencias lo que le permite ofrecer distintas características en sus dispositivos en el mercado, de acuerdo a la necesidad de implementación el usuario debe tomar en cuenta que tipo de licencia es la que se adapta de la mejor manera a su proyecto.

A continuación, se mencionan las diferencias entre los niveles de licencia en RouterOS:

Tabla 1-1: Diferencias entre los niveles de licencia en RouterOS

Número de nivel	0 (modo de prueba)	1 (Free Demo)	3 (CPE WISP)	4 (WISP)	5 (WISP)	6 (controlador)
Precio	no hay llave	Se requiere registro	único volumen	$ 45	$ 95	$ 250
Soporte de configuración inicial	-	-	-	15 días	30 días	30 días
Cliente inalámbrico y el puente	juicio 24h	-	sí	sí	sí	Sí
RIP, OSPF, BGP protocolos	juicio 24h	-	sí	sí	sí	Sí
túneles EoIP	juicio 24h	1	ilimitado	ilimitado	ilimitado	Ilimitado
túneles PPPoE	juicio 24h	1	200	200	500	Ilimitado
túneles PPTP	juicio 24h	1	200	200	500	Ilimitado
túneles L2TP	juicio 24h	1	200	200	500	Ilimitado
túneles OVPN	juicio 24h	1	200	200	ilimitado	Ilimitado
interfaces VLAN	juicio 24h	1	ilimitado	ilimitado	ilimitado	Ilimitado
HotSpot usuarios activos	juicio 24h	1	1	200	500	Ilimitado
cliente RADIUS	juicio 24h	-	sí	Sí	sí	Sí
colas	juicio 24h	1	ilimitado	ilimitado	ilimitado	Ilimitado
proxy web	juicio 24h	-	sí	Sí	sí	Sí
Administrador de usuarios de las sesiones activas	juicio 24h	1	10	20	50	Ilimitado
Número de huéspedes KVM	ninguna	1	Ilimitado	Ilimitado	Ilimitado	Ilimitado

Fuente: https://wiki.mikrotik.com/wiki/Manual:License

1.8.5 *Winbox*

Es una aplicación de configuración del RouterOS ya que permite la administración de Mikrotik RouterOS utilizando una interfaz GUI sencilla.

1.8.6 *Beneficios de la tecnología*

- Permite el control de ancho de banda por usuario.
- Posee software de configuración Winbox de fácil uso.
- No se necesita de conocimientos previos para su implementación.
- Posibilidad de bloquear aplicaciones y páginas web no deseadas.

1.9 **Tecnología Cisco**

CISCO es una empresa multinacional estadounidense que es líder en las telecomunicaciones en todo el mundo, su recurso humano altamente calificado es una gran ventaja competitiva en el mercado además es una empresa muy cotizada debido a los avances tecnológicos que presenta cada año y además por sus programas de capacitación y certificación que ofrece a los usuarios.

Figura 19-1: Logotipo de la empresa CISCO

Fuente: http://showcaseguru.com/images/posters/cisco/cisco.gif

1.9.1 *Cisco Systems*

Hoy en día existen muchas empresas que elaboran y comercializan dispositivos y equipos de telecomunicaciones, pero según la mayoría de firmas internacionales CISCO es considerado como los mejores del mundo ya que cuenta con su propio código para las configuraciones lo que lo lleva a ser más confiable que la competencia existen varias tecnologías que brinda a los usuarios entre los cuales se destacan hubs, firewalls, teléfonos IP, routers, etc.

1.9.2 ***Router Cisco***

Es un equipo que se encarga de enrutar el tráfico existente en la red de la mejor manera, es el responsable de ayudar a las instituciones a encontrar un equilibrio entre las seguridades y la productividad de la red. Combina las fortalezas de un Firewall en lo que es la seguridad y las redes de última generación en donde se destaca la visibilidad y el control de las aplicaciones basadas en el comportamiento de las aplicaciones. (Vinocunga. Elizabeth. 2015:21)

1.9.2.1 *Características*

El router es la estructura básica de las redes, cuenta con las siguientes características:

- Soporta simultáneamente diferentes protocolos lo cual lo hace compatible con los demás dispositivos de red.
- Brinda una conexión ideal de LAN a WAN.
- Aísla las áreas en donde los mensajes pueden llegar a todos los usuarios de la red filtrándolo hacia el exterior de la red.
- Ofrece múltiples trayectorias a través de las redes, dando al usuario fiabilidad en la transmisión de los datos.
- Aprende las trayectorias de los paquetes de manera automática para después seleccionar las mejores.

1.9.3 ***Puntos de acceso inalámbricos***

1.9.3.1 *WAP 131 Wireless-N de doble radio access point con PoE*

Figura 20-1: Cisco WAP 131 Access Point

Fuente: https://www.cisco.com/c/en/us/products/wireless/wap131-wireless-n-dual-radio-access-point/index.html

- Conectividad inalámbrica Dual 2.4 y 5 GHz
- Es un punto de acceso autónomo
- Diseño simple integrado con soporte para su fácil instalación
- 1 gigabit Ethernet LAN con POE
- Instalación y configuración simple basada en red intuitiva

1.9.3.2 *WAP 150 AC Wireless/N de banda seleccionable con un solo punto de configuración*

Figura 21-1: WAP 150 AC Wireless Dual Access Point

Fuente: http://www.cisco.com/c/en/us/products/wireless/wap150-wireless-ac-n-dual-radio-access-point-poe/index.html

- Soporta hasta 1.2 Gbps con radio banda dual que aumenta el área de cobertura.
- Alimentación a través de ethernet POE
- Configuración en un solo punto no requiere controlador para su despliegue fácil y rentable de punto de acceso múltiple.
- Múltiples antenas internas.

1.9.3.3 *Punto de acceso WAP 321 Wireless-N de banda seleccionable con un solo punto de configuración*

Figura 22-1: Punto de Acceso WAP321 Wireless-N de banda seleccionable

Fuente: http://www.cisco.com/c/en/us/products/wireless/wap321-wireless-n-selectable-band-access-point-single-point-setup/index.html

- Conectividad inalámbrica 802.11n de banda seleccionable.
- Soporta conexiones de alta velocidad con interfaz LAN Gigabit Ethernet.
- Fácil configuración basada en asistente.
- Mayor seguridad incluyendo encriptación avanzada, autenticación segura, y la detección de punto de acceso.

1.9.3.4 *Punto de acceso WAP 351 Wireless-N dual radio*

Figura 23-1: Punto de Acceso Cisco WAP351 Wireless-N Dual Radio

Fuente: https://www.cisco.com/c/en/us/products/wireless/wap351-wireless-n-dual-radio-access-point-4-ports-switch/index.html

- Radio Dual 2.4 y 5 GHz conectividad inalámbrica.
- Fácil manejabilidad.
- Interruptor 5 puertos Gigabit Ethernet.
- Instalación simple y configuración intuitiva basada en web.

1.9.4 ***Características de la tecnología Cisco***

- Portal Cautivo seguro.
- Seguridad en la red.
- Inteligencia incorporada.
- Disponibilidad en la red.
- Gestión de la red y optimización de aplicaciones.
- Instalación Eficaz.
- Autenticación robusta.
- Calidad de Servicio Inteligente.
- Costo de la tecnología.
- Interfaz de usuario.

1.10 **Monitoreo de Red**

Monitoreo es un proceso que permite utilizar, recolectar y analizar la información con el fin de realizar un seguimiento y un control permanente del desempeño y la disponibilidad de los puntos críticos de una red a través de la detección de errores dentro de la misma.

1.10.1 ***Herramientas de Análisis y Monitoreo de Red***

1.10.1.1 *Wireshark*

Wireshark es un software de código abierto que permite analizar los paquetes de una red ya que intentará capturar y mostrar detalladamente los datos de los paquetes que se envían en la red. Es una herramienta que brinda un conjunto de características las cuales ayudan a examinar lo que está sucediendo dentro de la red.

Figura 24-1: Logotipo Wireshark

Fuente: https://i.ytimg.com/vi/GnCwRldX_bM/hqdefault.jpg

1.10.1.1.1 *Características de Wireshark*

- Reconocimiento de cientos de protocolos los cuales se actualizan conforme aparezcan nuevos protocolos.
- Análisis y captura sin conexión.
- Navegador estándar de paquetes de tres paneles.
- Es multiplataforma ya que se ejecuta en la mayoría de sistemas operativos.
- Interfaz gráfica que permite la navegación de los datos de la red.
- Filtros de pantalla potentes.
- Lee y escribe muchos formatos de archivos diferentes capturados.
- Soporte de descifrado para muchos protocolos de comunicación.
- La salida se puede exportar a XML, PstScript, CSV o texto sin formato, entre otros. (Wireshark, 2017, Wireshark features, https://www.wireshark.org/)

1.10.1.2 *The Dude Mikrotik*

The dude es una novedosa herramienta open source de monitorización de redes creada por Mikrotik la cual optimiza y mejora el control del sistema de red local ya que analiza los componentes de la misma, elaborando un mapa con la distribución de las conexiones y los dispositivos existentes. Incorpora un mapa del esquema de la red sobre la cual se está trabajando esto permite tener un acceso directo a cada elemento de la red y las funciones que posee dentro de la misma.

The dude posee un entorno gráfico amigable para el usuario y a la vez es un potente instrumento para la monitorización y administración de los elementos de la red. Existen modos de acceso al programa los cuales son, localmente cuando se encuentra físicamente donde esta implementado el equipo y de manera remota que se encuentre instalado como cliente del servidor The dude. (Claudio Víctor, 2009, http://repositorio.uta.edu.ec/handle/123456789/223)

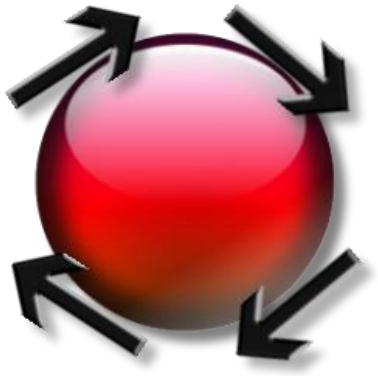


Figura 25-1: Logotipo The Dude Mikrotik

Fuente: https://wiki.mikrotik.com/images/9/93/Dude-icon.png

1.11 Access Point (AP)

Un punto de acceso inalámbrico es un dispositivo que tiene la función de interconectar otros dispositivos de comunicación inalámbrica para conformar una red inalámbrica, normalmente puede conectarse a una red cableada y transmitir los datos de la misma a la red inalámbrica. Se alcanza una red mayor interconectando varios WAP, además los AP poseen direcciones ip para poder ser configurados de acuerdo al uso que el usuario requiera.

1.11.1 ***Access point Ubiquiti Nanostation Loco M2*:** dispositivo de comunicación inalámbrica que trabaja a una frecuencia de 2.4 GHz que permite dar cobertura a zonas extensas.

CAPITULO II

2 MARCO METODOLÓGICO

2.1 Introducción

Para poder realizar el estudio comparativo se elaboró una investigación previa de las características de las tecnologías Cisco y Mikrotik y del funcionamiento del portal cautivo, lo cual permite elaborar un modelo comparativo de los dispositivos que tiene cada tecnología disponible en el mercado actualmente. Se realiza un análisis cualitativo de las características que poseen los dispositivos tomando en cuenta los requerimientos de la empresa, obteniendo como resultado la tecnología con el dispositivo más eficiente previo a la implementación del portal cautivo en IPREX.

Se optó por IPREX ya que es una institución que ha tenido un gran crecimiento en los últimos años y un aumento significativo en el número de usuarios en la red inalámbrica, la red es escalable ya que se adapta a futuros cambios que se presenten en la institución y la cobertura que ofrece la implementación del portal cautivo en la red inalámbrica es ideal. Se considera a las tecnologías Cisco y Mikrotik debido a que son actualmente las pioneras en el mercado de las redes de telecomunicaciones, los parámetros del análisis comparativo se seleccionaron tomando en cuenta el nivel de importancia que tienen al momento de implementar y controlar una red inalámbrica las cuales son seguridad, interfaz de usuario, gestión, compatibilidad y costos de la tecnología.

2.2 Estudio comparativo de las tecnologías Cisco y Mikrotik en la implementación de portales cautivos

El presente trabajo de titulación tiene como objetivo principal analizar en detalle cada uno de los dispositivos seleccionados en la implementación de portales cautivos, siendo las tecnologías Cisco y Mikrotik las escogidas para el estudio comparativo.

Se estudiarán las características de cada una de tal manera que se pueda valorar los recursos y prestaciones que ofrecen para la implementación de portales cautivos en las empresas e instituciones.

2.2.1 *Cisco*

Posee una alta gama de productos y servicios de las cuales se destacan para este estudio los routers y puntos de acceso que se usan en la implementación de redes inalámbricas dentro de una empresa.

Para este cuadro de toma en cuenta la línea Cisco Small Business citados anteriormente por sus características de enrutamiento, su precio y en especial la más importante que es la integración de la opción del portal cautivo dentro del dispositivo lo cual permite una configuración e implementación más rápida del servicio.

2.2.1.1 *Cuadro comparativo de dispositivos Cisco existentes en el mercado*

Tabla 1-2: Tabla comparativa de dispositivos Cisco

Dispositivos	**Especificaciones**					
	Puertos	Tipo de Seguridad	Número de Usuarios Recomendados	Rendimiento Inalámbrico	Ganancia de la Antena	Precio
WAP 131Wireless-N Dual Radio Access Point	Ethernet 10/100/1000 compatible con 802.3 af/at PoE	WPA y WPA2	Hasta 32 usuarios conectados, 16 usuarios activos por radio	Velocidad de datos de 300 Mbps	3,4 dBi en 2,4 GHz 4,5 dBi en 5 GHz	$ 213,15
WAP 150 Wireless AC/N Dual Radio Access Point	Ethernet 10/100/1000 con soporte PoE 802.3 af/at	WPA, WPA 2	64 usuarios conectados	Velocidad de datos hasta 1,2 Gbps	3,61 dBi en 2,4 GHz 3,85 dBi en 5 GHz	$ 249,76
WAP 321 Wireless-N Selectable Band Access Point	Gigabit Ethernet compatibilidad para PoE 802.3 af	WEP, WPA, WPA2 incluida la autenticación de la empresa	64 usuarios conectados	Velocidad de datos igual a 300 Mbps	2 dBi cada antena	$ 280,56

Realizado por: Caiza José. 2017

De acuerdo con los requisitos de la empresa y a las características de los dispositivos se elige para este estudio a Cisco WAP 131Wireless-N Dual Radio Access Point que ofrece una alta gama de opciones y configuraciones que se adaptan perfectamente a los recursos que existen en la red, siendo el precio de compra el elemento más importante a la hora de escoger el dispositivo debido al presupuesto con el que se cuenta en la empresa.

2.2.2 *Mikrotik*

Es una empresa que fábrica equipos de hardware y software de telecomunicaciones, como compañía ha ido evolucionando a pasos agigantados de tal manera que en los últimos años ha desarrollado equipos hardware menos costosos y de gran rendimiento.

Para este estudio se consideran los equipos mencionados anteriormente ya que ofrecen múltiples opciones de configuración de portal cautivo integrado y su disponibilidad en el mercado.

2.2.2.1 *Cuadro comparativo de dispositivos Mikrotik existentes en el mercado*

Tabla 2-2: Cuadro comparativo de Dispositivos Mikrotik

Dispositivos	Especificaciones				
	Memoria RAM	Frecuencia Nominal CPU	Puertos	Nivel de Licencia	Precio
RouterBoard RB750G	32 MB	680 MHz	5 puertos 10/100/1000 Ethernet	4	$ 79,60
RouterBoard RB750R2 (Hex Lite)	64 MB	850 MHz	5 puertos 10/100 Ethernet	4	$ 120,40
RouterBoard RB951Ui-2HnD	128 MB	600 MHz	5 puertos 10/100 Ethernet	4	$ 150,60

Realizado por: Caiza José. 2017

Se elige al dispositivo RouterBoard RB750G para el estudio comparativo ya que tiene características que cumplen con los requisitos de red que presenta la empresa además que posee un precio que es muy accesible para su compra.

2.2.3 ***Parámetros de los equipos a comparar.***

Las mediciones descriptivas de una toda una población es considerada como parámetro, son datos imprescindibles que nos permiten evaluar una situación específica lo cual lleva a ubicarse en perspectiva. En este análisis se toma en cuenta parámetros de evaluación considerados

imprescindibles por su importancia a la hora de tomar una decisión para elegir una tecnología hacia su implementación en IPREX, se ha seleccionado como parámetros a las carácteristicas más importantes y comunes de las dos tecnologías y según la recomendación ITU-T Y.1271 que trata sobre los requisitos y capacidades de red generales, en donde se tiene:

2.2.3.1 *Seguridad*

En la actualidad es uno de los parámetros más importantes ya que se necesita que la red sea lo más segura posible para brindar confiabilidad en la información a los usuarios. Este parámetro puede ser medido tomando en cuenta el nivel de vulnerabilidad, donde el nivel de percepción bajo describe una red más vulnerable y el nivel de percepción muy alto describe una red invulnerable.

2.2.3.2 *Gestión de la tecnología*

La gestión de la red es un parámetro imprescindible ya que permite llevar un control eficaz de los recursos existentes en la red, controlando el ancho de banda que usa cada usuario y el número de clientes existentes. Para poder evaluar este parámetro se toma en cuenta el nivel de dificultad que existe al gestionar una red en donde el nivel de percepción bajo indica mayor dificultad y el nivel de percepción más alto describe un nivel de dificultad para la gestión muy bajo.

2.2.3.3 *Compatibilidad de la tecnología*

La compatibilidad de la tecnología con respecto a otras es un parámetro importante en la evaluación ya que permite conocer cómo trabaja junto a otras tecnologías. La valoración de este parámetro en el nivel de percepción bajo puede medir baja compatibilidad y el nivel de percepción muy alto está relacionado con el nivel de compatibilidad alta.

2.2.3.4 *Interfaz de usuario*

Es trascendental mencionar este parámetro que es el medio de comunicación entre el usuario y la tecnología. Este parámetro puede ser medido tomando en cuenta el nivel de percepción bajo como un interfaz de usuario complejo y el nivel de percepción muy alto describe un interfaz de usuario amigable de fácil uso.

2.2.3.5 *Costos de la tecnología*

Hoy en día este parámetro es significativo ya que nos indica el valor monetario que tiene la tecnología. Este parámetro es medido para esta evaluación en el nivel de percepción bajo indica

una valoración en el precio muy alta y el nivel de percepción muy alto describe un precio muy económico.

Según el proyecto "CENTRO VIRTUAL PARA EL DESARROLLO DE ESTÁNDARES DE CALIDAD PARA LA EDUCACIÓN SUPERIOR A DISTANCIA EN AMÉRICA LATINA Y EL CARIBE", el registro de autoevaluación se establece una escala cuantitativa del 1 al 4 en donde 1 se considera Bajo, 2 Medio, 3 Alto y 4 Muy alto se obtiene la siguiente tabla de ponderación :

Tabla 3-2: Tabla de ponderación

NIVEL DE PERCEPCION	VALORACION
Muy Alto	76-100
Alto	51-75
Medio	26-50
Bajo	1-25

Realizado por: Caiza José. 2017

2.2.4 *Comparación de las tecnologías Cisco y Mikrotik*

Para la realización de la tabla de valoración cualitativa se toma en cuenta la recomendación citada en la tabla anterior donde se menciona la escala cualitativa en donde la ponderación de 100 significa el 100% en la cual se obtiene la siguiente tabla de ponderización:

Tabla 4-2: Tabla de valoración cualitativa

Exelente	Muy Bueno	Bueno	Malo
100-76	75-51	50-26	25-1

Realizado por: Caiza José. 2017

Tabla 5-2: Tabla de valoración cualitativa del dispositivo Cisco WAP 131Wireless-N Dual Radio Access Point.

NIVEL DE	PONDE	Cisco WAP 131Wireless-N Dual Radio Access Point

PERCEPCION	RACION	SEGURIDAD	GESTION	COMPATIBILIDAD	INTERFAZ	COSTO
MUY ALTO	76-100 %	95		95	90	
ALTO	51-75 %		70			
MEDIO	26-50 %					
BAJO	1-25 %					25

Realizado por: Caiza José. 2017

Tabla 6-2: Tabla de valoración cualitativa de Mikrotik.

NIVEL DE PERCEPCION	PONDERACION	Mikrotik RouterBoard RB750G				
		SEGURIDAD	GESTION	COMPATIBILIDAD	INTERFAZ	COSTO
MUY ALTO	76-100 %	85	80	90		85
ALTO	51-75 %				75	
MEDIO	26-50 %					
BAJO	1-25 %					

Realizado por: Caiza José. 2017

En donde se obtiene como resultado:

Tabla 7-2: Tabla comparativa de los dispositivos Cisco y Mikrotik

PARÁMETROS	TECNOLOGIAS/DISPOSITIVOS	
	Cisco WAP 131Wireless-N Dual Radio Access Point	**Mikrotik RouterBoard RB750G**
SEGURIDAD	95 %	80 %

GESTION	70 %	80 %
COMPATIBILIDAD	95 %	90 %
INTERFAZ DE USUARIO	90 %	75 %
COSTO	25 %	85 %
TOTAL PROMEDIO	75 %	82 %

Realizado por: Caiza José. 2017

2.2.4.1 *Resultado del análisis comparativo*

En el estudio comparativo se determinó que entre las tecnologías Cisco con su router WAP 131Wireless-N Dual Radio Access Point y Mikrotik con su RouterBoard RB750G dio como resultado que en seguridad el dispositivo Cisco es mejor en un 15% que Mikrotik, y en general que el dispositivo Mikrotik ha obtenido un 82 % de las mediciones de los parámetros subjetivos vs Cisco que ha obtenido un 75 % en el promedio de las mediciones de los parámetros, se concluye que la tecnología Mikrotik es la más adecuada para implementar en la red de la institución IPREX debido a sus prestaciones y su funcionamiento siendo el parámetro más decisivo el costo de la tecnología. Es importante mencionar que para poder realizar este análisis comparativo se eligió minuciosamente 5 de los parámetros más importantes en las IT.

A continuación, se observa en detalle las razones por las cuales la tecnología Mikrotik es la adecuada para ser implementada:

- Interfaz de usuario amigable de fácil configuración.
- Costos mínimos en la implementación.
- Disponibilidad en el mercado.

2.3 **Diseño de la red de implementación**

2.3.1 ***Análisis de la situación inicial***

IPREX es una institución que brinda capacitación permanente a sus clientes en varias áreas de estudio además de cursos de preparación de rendición de exámenes para el ingreso a las universidades, por lo que el uso de la red inalámbrica dentro de la misma es muy solicitado por los estudiantes que se capacitan en la institución ya que requieren de un servicio de internet inalámbrico para consultas.

Actualmente la institución posee una red inalámbrica que ofrece el servicio de internet inalámbrico a muy pocas personas debido a que la red no es compartida y posee deficiencias al momento de transmitir la información mediante el modem que se tiene actualmente.

2.3.2 *Zona Geográfica*

IPREX es una de las instituciones enfocadas a la capacitación de estudiantes y profesionales que se especializan en Tecnología e Ingeniería más importantes de la ciudad de Riobamba, se encuentra ubicada en la calle Veloz 29-40 entre Juan Montalvo y Carabobo.

2.3.3 *Conceptos de diseño*

2.3.3.1 *Objetivos técnicos*

El objetivo técnico brinda un medio seguro, confiable y fiable para la transmisión de datos gracias al diseño de red de datos regida por estándares y normativas actuales con el fin de proporcionar conectividad a los usuarios.

2.3.3.2 *Escalabilidad*

Se elige la topología de árbol para su diseño ya que proporciona escalabilidad a la red permitiendo una ampliación de su capacidad de expansión. El proyecto inicia con 40 usuarios inalámbricos para quienes se ofrecerá un diseño que cumpla con los requerimientos de la institución respecto al escenario actual y futuro, la red se adapta fácilmente a nuevas tecnologías que se integren a la misma.

2.3.3.3 *Disponibilidad de la red*

Para elaborar una estimación de disponibilidad de red se toma en cuenta una medida estadística en un intervalo de tiempo y bajo condiciones de medición objetiva de las condiciones del servicio, el equipo implementado Mikrotik RB750G brinda un MTBF de 100000 horas y el administrador de la red reparara la falla de red en un tiempo máximo de 12 horas en IPREX centro.

- **MTBF=** 100000 h
- **MTTR=** 12 h

  Disponibilidad= $(\frac{MTBF}{MTBF+MTTR})$*100

  Disponibilidad= 99,99 %
- Desconexión por minutos

Tabla 8-2: Disponibilidad de la red

Disponibilidad	Por hora	Por día	Por mes	Por año
99,99 %	0.006 min	0,144 min	4,4 min	52,6 min

Realizado por: Caiza José. 2017

2.3.3.4 *Tipos de Seguridad*

2.3.3.4.1 *Seguridad lógica*

- **Portal Cautivo**

Provee un control de acceso de usuarios ya que para poder usar los recursos de la red debe disponer de un Id de usuario y contraseña.

- **Encriptación**

Dispone de una encriptación WPA-AES/WPA2-AES que ofrece mayor seguridad inalámbrica.

Implementación de políticas de seguridad para los usuarios.

2.3.3.4.2 *Seguridad física*

El router Mikrotik está ubicado en una zona específica dentro de la oficina principal de la institución y la antena repetidora está dentro de la institución asegurada con sus respectivos soportes.

2.3.3.5 *Adaptabilidad*

La tecnología Mikrotik trabaja bajo estándares internacionales lo cual permite que sea compatible con dispositivos de otras marcas, lo que genera una red que fácilmente se adapte a cambios tecnológicos.

2.3.4 ***Diseño lógico***

Actualmente en IPREX se presenta falencias en cuanto a seguridad en la red inalámbrica ya que no se tiene un control del número de usuarios que existen en dicha institución, por lo cual se puede optar por una solución que es la implementación de un portal cautivo para llevar un registro de cuantos usuarios hay en la red inalámbrica lo que también permitirá gestionar y asignar el ancho de banda que se dispone en la institución. A continuación, se visualiza el estado actual de la red:

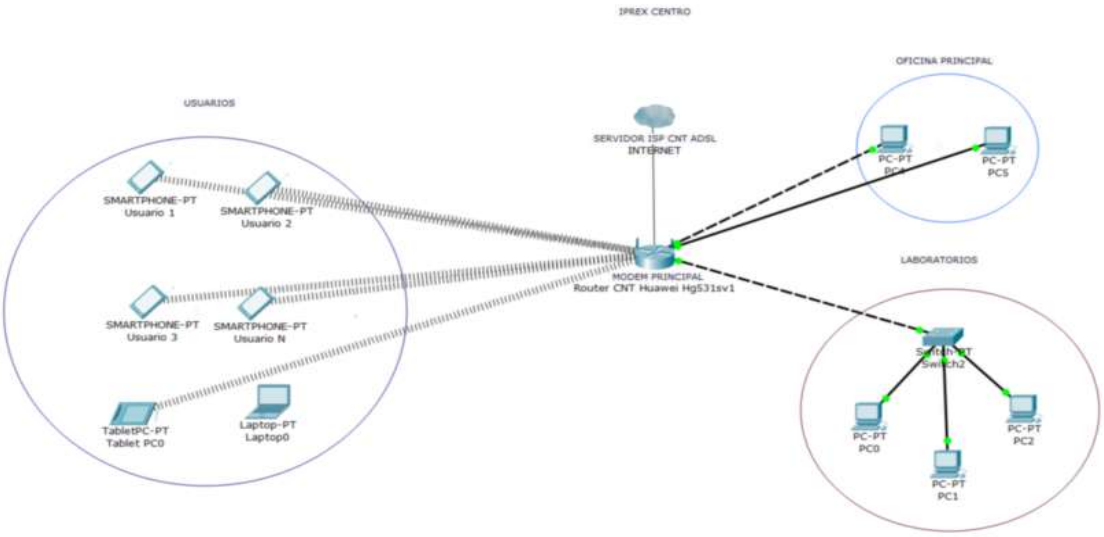


Figura 1-2: Red actual en IPREX

Realizado por: Caiza José. 2017

Para el diseño lógico de la red se eligió una red tipo árbol ya que ofrece muchas ventajas al momento de su implementación en IPREX lo que permite tener una red jerárquica, siendo el router Mikrotik el nodo central y la antena Nanostation m2 un repetidor que se encarga de brindar conectividad inalámbrica hacia los usuarios. Se presenta el diseño lógico de la red con la solución a este problema que es la implementación de un portal cautivo mediante la tecnología Mikrotik

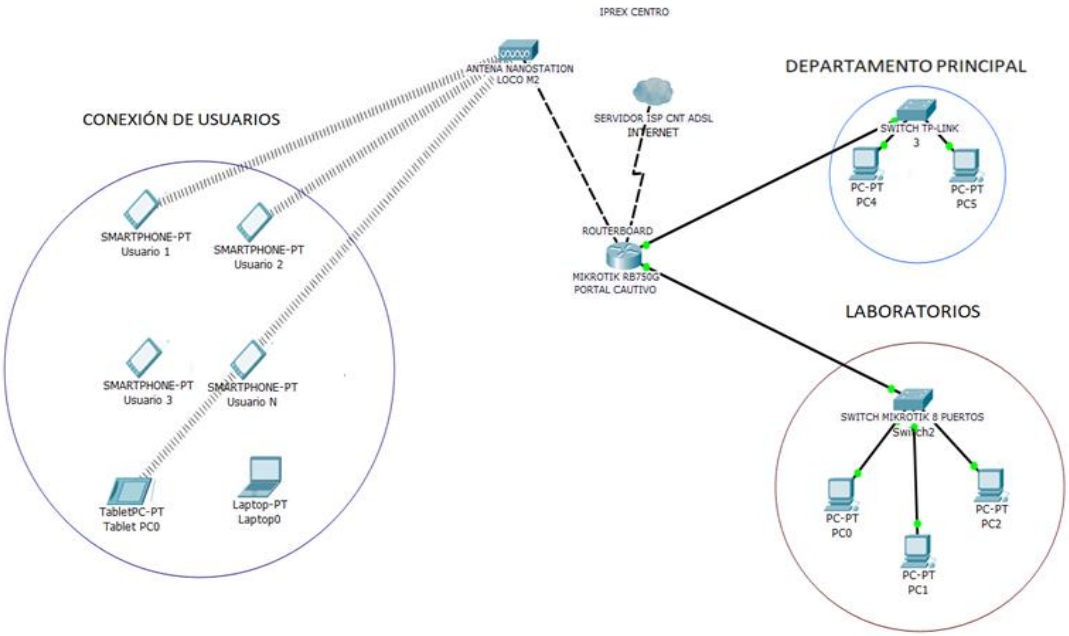


Figura 2-2: Topología de la red en IPREX

Realizado por: Caiza José. 2017

2.3.5 *Diseño físico*

2.3.5.1 *Descripción de los elementos a utilizar en la implementación de la red*

Para el mejoramiento de la red inalámbrica se opta por la implementación de un Portal cautivo mediante la tecnología Mikrotik que ofrece varias configuraciones que permiten el control de usuarios, ancho de banda, seguridad y además el costo de la tecnología la cual es mínima. Para poder implementar esta solución se necesita de dispositivos de comunicaciones que se describen a continuación:

2.3.5.2 *Requerimientos previo a la implementación del portal cautivo*

- Mikrotik RB750G
- Software Winbox.
- Access Point Ubiquiti Nanostation Loco M2
- PC

2.4 Implementación del portal cautivo mediante la tecnología Mikrotik en IPREX

2.4.1 *Implementación física*

La implementación del router Mikrotik RB750G se situó en la oficina central de la institución junto al laboratorio de clases y la antena repetidora Loco Nanostation en la parte más alta de la institución lo que permite un aprovechamiento de la cobertura de la misma.

Figura 3-2: Implementación física en la oficina central

Realizado por: Caiza José. 2017

2.4.2 *Implementación lógica*

Para esta implementación se toma en cuenta los requerimientos de la institución y el número de usuarios existentes, los pasos para la implementación del portal cautivo se encuentran detallados en el **ANEXO A**.

A continuación, se describe los pasos a seguir:

Paso 1.- Descargar el software Winbox que permite la configuración en un dispositivo Mikrotik en la página web oficial.

Paso 2.- Se ejecuta el software descargado.

Paso 3.- Se abrirá la interfaz en donde seleccionamos la pestaña que nos muestra los dispositivos Mikrotik conectados.

Paso 4.- Se da click izquierdo y se selecciona la opción en donde se encuentra la dirección MAC del dispositivo Mikrotik que se tenga ingresando así al interfaz de configuración.

Paso 5.- Se renombra las interfaces y se asigna nombres de acuerdo a los requerimientos que tenga el usuario en este caso se usara la interfaz del puerto 2 para la red de las oficinas centrales el puerto 3 para el portal cautivo y el puerto 4 para la interfaz de los laboratorios de la institución.

Paso 6.- Una vez configurados y cambiados los nombres de las interfaces se procede a darle direccionamiento ip correspondiente.

Paso 7.-Una vez creadas las interfaces con sus respectivas direcciones IP, se debe configurar los servidores DNS del proveedor de servicio de internet para tener acceso al servicio de internet.

Paso 8.-Configuración del Hotspot, se elige la pestaña IP>hotspot

- Se selecciona la opción Hotspot Setup
- Se sigue los pasos del asistente de configuración.

Paso 9.-Se procede a crear perfiles para el servidor de portal cautivo

- Para el acceso de usuario se habilita únicamente la opción HTTP CHAP para evitar que los datos queden guardados en los dispositivos clientes.
- Configuración de perfil de usuario es muy importante ya que en este apartado se configura el ancho de banda de subida y bajada para un plan específico que se va a brindar a los clientes.
- Se configura de acuerdo a los requerimientos de la institución.

Paso 10.-Creados los planes de servicio de internet se procede a crear a los usuarios con su ID y respectiva password de acceso

- Se asigna el plan 1 MB que consiste en 1024 Kb de bajada y 512 Kb de subida de datos a los usuarios y el plan 2 MB que consiste en 2048 Kb de bajada y 512 Kb de bajada de datos para la sección administrativa de la institución los cuales tienen habilitados todos los servicios que ofrece Mikrotik y se procede a guardar la configuración realizada.

CAPITULO III

3 MARCO DE RESULTADOS

3.1 Evaluación y comparación de resultados

3.1.1 *Simulación y análisis*

Para poder realizar las pruebas de la implementacion del proyecto se utilizó las siguientes herramientas:

3.1.1.1 Hardware

Servidor: Es una computadora Intel Core I7 con un sistema operativo que soporte los software necesarios para realizar el analisis de tráfico en la red.

Tabla 1-3: Caracteristicas de Laptop Toshiba

Características de la Laptop	
Marca	Toshiba Satellite S55t
Procesador	Intel Core I7
Ram	16 Gb
Sistema Operativo	Windows 10 X64 bits

Realizado por: Caiza José. 2017

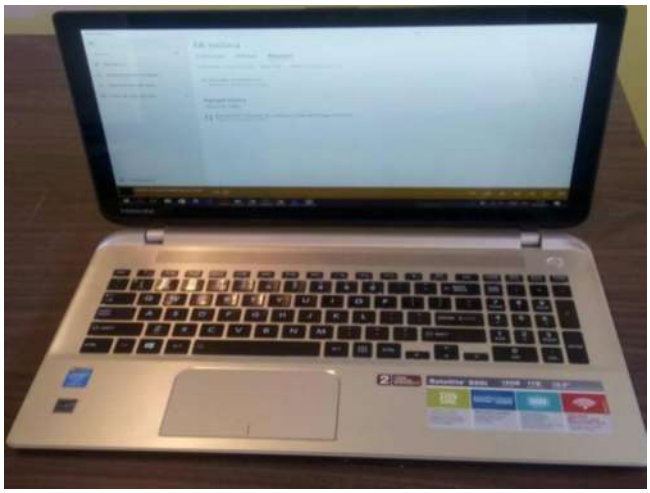


Figura1-3: Computadora Satellite S55t

Realizado por: Caiza José. 2017

3.1.1.2 Software

Wireshark es una herramienta de software libre que es fácil de usar e interpretar los datos que se obtiene en el análisis.

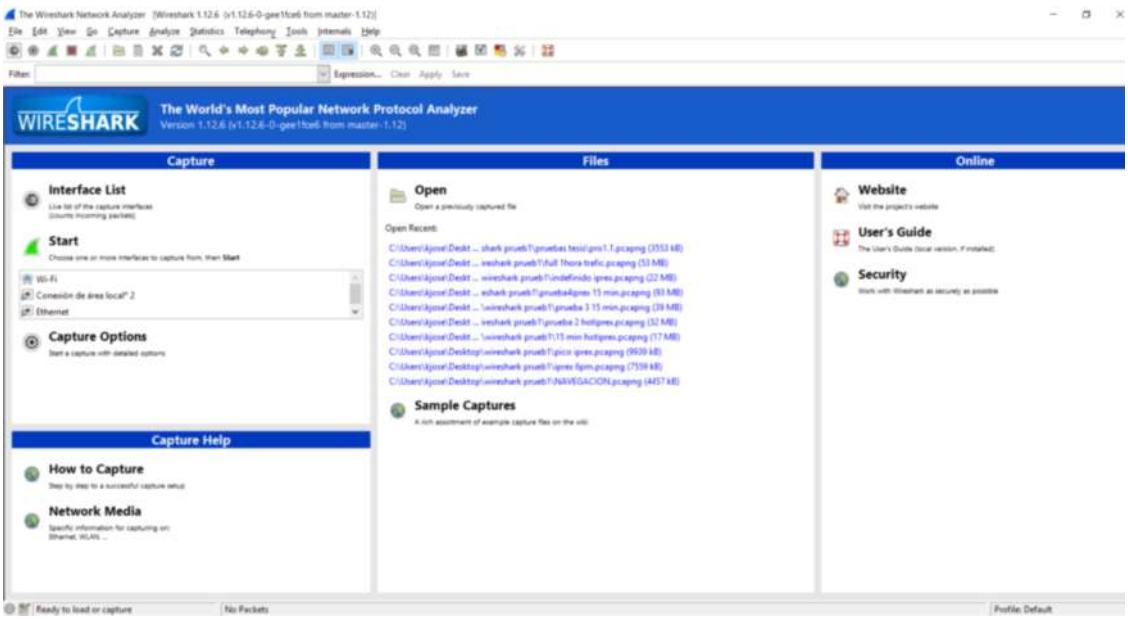


Figura 2-3: Software Wireshark

Realizado por: Caiza José. 2017

Cmd: Es una consola que permite ejecutar lineas de comandos especificos para realizar diferentes tareas dentro del sistema operativo Windows en este estudio ejecutó el comando ping que permite visualizar el retardo en el envío de paquetes en la red.

Figura 3-3: Consola de comandos CMD

Realizado por: Caiza José. 2017

3.2 Parámetros de calidad del servicio

Para realizar el análisis de tráfico en la red inalambrica se tomó en cuenta dos escenarios basándose en su implementacion, en cada caso se valoró parámetros importantes en la comunicación entre dispositivos los cuales han sido escojido debido a la importancia que tienen cada uno de ellos en el análisis de tráfico y son considerados métricas de gran importancia por las organizaciones reguladoras ITU-T Y LA IETF para la evaluación de la calidad de servicio las cuales son: jitter, pérdida de paquetes y retardo. Dichos parámetros permiten realizar un análisis minucioso de la red en tiempo real y poder detectar irregularidades en el funcionamiento de la red.

Se tomó en cuenta los parámetros que repercuten directamante en la calidad de servicio de acuerdo a un estudio anterior llamado "A Study on a QoS/QoE Correlation Model for QoE Evaluation on IPTV Service" donde se menciona lo siguiente:

Tabla 2-3: Parámetros de Calidad de Servicio y su grado de importancia

Número de Parámetro	Parámetro de Calidad de Sevicio	Grado de Importancia
1	Jitter	10.7 %
2	Pérdida de Paquetes	41.7 %
3	Retardo	10.6 %

Fuente: http://www.icact.org/upload/2010/0395/20100395_Abstract_B.pdf

A continuación se detalla las caracteristicas más importantes de cada parámetro y como se va a realizar la simulacion dentro del estudio:

3.2.1 *Jitter*

Es la variación de retardos de una misma comunicación la cual afecta el tiempo de respuesta de la transmisión. Considerando la recomendación ITU Y.1541 este parámetro no debe sobrepasar

los 50 milisegundos. De acuerdo a esto, se ha determinado una escala de valores de importancia que permite categorizar los parámetros de acuerdo a la métrica y la recomendación como se muestra a continuación:

Tabla 3-3: Valoración del procentaje del parámetro Jitter

VALORACIÓN	JITTER (ms)	PORCENTAJE
SOBRESALIENTE	0-10	20
MUY BUENA	11-20	40
BUENA	21-30	60
REGULAR	31-40	80
PÉSIMA	41-50	100

Realizado por: Caiza José. 2017

La cantidad de jitter que sobrepase los 50 milisegundos es igual a una calificación 100 % lo que quiere decir que no garantiza la calidad de transmisión de información ocasionando el deterioro de los datos transmitidos.

3.2.2 *Pérdida de paquetes*

No es más que el número de paquetes que se envían desde emisor y que no han alcanzado su objetivo de llegar al destino propuesto, esto se puede producir debido a un reducido ancho de banda, las condiciones físicas del cable de transmisión, la saturación de usuarios en la red, por fallo de enlaces o a causa de problemas físicos de los dispositivos de transmision y recepción de información. De acuerdo a la recomendación ITU-T Y.1541 establece un máximo del 10 % de pérdida de paquetes en una transmisión. Tomando en cuenta lo descrito anteriormente se ha determinado una escala de valores de importancia que permite categorizar los parámetros de acuerdo a la métrica y la recomendación como se muestra a continuación:

Tabla 4-3: Valoración del procentaje del parámetro Pérdida de Paquetes

VALORACIÓN	PÉRDIDA DE PAQUETES
SOBRESALIENTE	0-2
MUY BUENA	2-4
BUENA	4-6
REGULAR	6-8

PÉSIMA	8-10

Realizado: Caiza José. 2017

La cantidad de pérdida de paquetes que sobrepase el 10 % no garantiza la calidad de transmisión de información ocasionando el deterioro de la misma.

3.2.3 *Retardo*

Es el tiempo que un paquete tarda en llegar desde el emisor hasta su receptor. Este retardo es medido de manera unidireccional por equipos específicos o considerando el promedio de ida y vuelta Round Trip Time (RTT). Tomando en cuenta la recomendación ITU Y.1541 el máximo permitido para tener un servicio de buena calidad es de 100 milisegundos. Gracias al comando de consola ping se obtiene de manera inmediata el mínimo, máximo y el promedio del tiempo de ida y vuelta de un paquete en la red, se ha determinado una escala de valores de importancia que permite categorizar los parámetros de acuerdo a la métrica de la recomendación como se muestra a continuación:

Tabla 5-3: Valoración del procentaje del parámetro Retardo

VALORACIÓN	RETARDO (ms)	PORCENTAJE
SOBRESALIENTE	0-30	20
MUY BUENA	31-60	40
BUENA	61-90	60
REGULAR	91-120	80
PÉSIMA	121-150	100

Realizado por: Caiza José. 2017

El valor del retardo que sobrepase los 150 milisegundos equivale a 100% lo que quiere decir que no garantiza la calidad de servicio en la transmisión de datos.

3.2.4 *MOS (Mean Opinion Score)*

Es la percepción del usuario final referente a la calidad de servicio en el lado del usuario, lo que quiere decir que está definida como una medida subjetiva debido a que su determinación esta dada por tests que consisten en la visualización de muestras de servicio en la red por parte de los observadores, los mismos que califican la calidad del servicio recibido de acuerdo a una escala dada. El promedio que se obtenga de las calificaciones de cada observador viene a ser la puntuación de opinión media o MOS. De acuerdo a la recomendación ITU-T P.800 se ha

definido una escala de clases las cuales corresponden al nivel de calidad de servicio respecto a la calificación del observador obteniendo lo siguiente:

Sobresaliente= 5 Muy Buena= 4 Buena= 3 Regular= 2 Pésima=1

No obstante debido a que el MOS es mas una medida de calidad de experiencia, los valores que se obtengan estan relacionados directamente a los factores que influyen en la calidad de servicio, por lo tanto las medidas subjetivas correspondientes a la calidad de experiencia asi como las medidas objetivas correspondientes a la calidad de servicio permiten establecer un reconocimiento global del observador dentro de una red. Tomando en cuenta esto, se ha fijado una escala que contienen los valores de importancia que permiten clasificar al servicio de acuerdo a los porcentajes de la métrica, como a continuación se detalla:

Tabla 6-3: Valoración MOS

CALIFICACIÓN	MOS	PORCENTAJE
SOBRESALIENTE	5-4	100
MUY BUENA	3.9-3	80
BUENA	2.9-2	60
REGULAR	1.9-1	40
PÉSIMA	0.9-0	20

Realizado por: Caiza José. 2017

Los valores de los porcentajes de MOS que sean menores al 20 % equivalen a un ancho de banda de la red saturado y por ende una nulidad de calidad en cuanto a la experiencia en la navegación por internet.

3.3 Simulación del primer escenario sin la implementación del portal cautivo.

3.3.1 *Recolección de datos*

De acuerdo a la informacion detallada anteriormente sobre los modos de cómo están estructuradas las pruebas dentro de la implementación de la red, es preciso tener en cuenta que el número de pruebas a realizarse para cada implementación está dado por el tiempo de duración en el cual los estudiantes y docentes de IPREX salen a su respectivo cambio de hora, es decir un aproximado 10 minutos; por lo tanto la toma de datos en su total está compuesta de veinte pruebas. Por esta razón se ha considerado un estimado de diez pruebas del primer escenario la cual es la red ya existente en IPREX entre el servidor y el cliente, y 10 pruebas de la implementación del Portal Cautivo que viene a ser el segundo escenario, las mismas que se

realizan entre el servidor y el cliente también, lo cual permite obtener datos razonables los mismos que despúes de su análisis permitan una evaluación de la implementación y en consecuencia la determinación de la mejoría en la red inalambrica en la institución.

3.3.2 *Técnica de recolección de datos*

Se detalla a continuación la técnica que se usó para la recolección de datos tanto para la implementación tradicional como para la implementación del Portal Cautivo:

Se genera tráfico por cada usuario conectado en la red los cuales realizan solicitudes de diferentes servicios con varios protocolos de comunicación.

3.3.2.1 Jitter

La toma de medidas del jitter se realiza mediante el software Jperf el cual permite visualizar los protocolos existentes en una red, además de poseer una variada gama de opciones, una de ellas es el poder tomar mediciones del jitter generado en el tráfico de red inalámbrica. Para lo cual se efectuó la ejecución del software Jperf tanto en el cliente como en el servidor en donde se configuran los parámetros para la realización de las pruebas, el tiempo que dura la transmisión de los datos. Por ejemplo en el servidor una vez abierto el software se selecciona el protocolo UDP y en modo server durante un tiempo de 603.548 segundos que equivale a los 10 minutos con 3 segundos de la prueba, en el cliente se selecciona el protocolo UDP y el modo cliente que se conecta al servidor a través de la dirección 192.168.1.25 durante un tiempo de 603.548 segundos.

A continuación se muestra un ejemplo de la captura del Jitter que se realizó en la prueba 7.

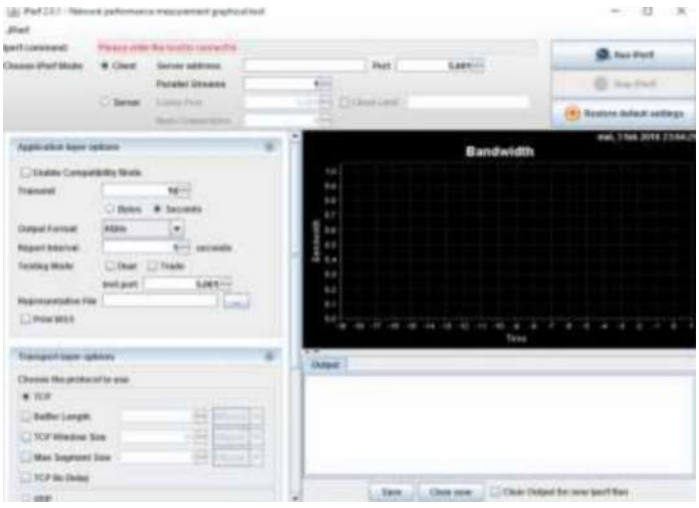


Figura 4-3: Prueba número 7 de Jitter

Realizado por: Caiza José. 2017

Despúes de haber configurado los parámetros que se necesitan para la medición del jitter se inicia la prueba tanto en el cliente como en el servidor simultáneamente en donde se recibe un jitter de 7.53 ms con un ancho de banda de 4 MB.

3.3.2.2 Pérdida de paquetes

Este parámetro es medido a través del software Wireshark el cual calcula la pérdida de paquetes tanto en el servidor como en el cliente donde se receptan los datos. Se puede apreciar a continuación los paquetes capturados en el tráfico de la red inalámbrica en la prueba número 5:

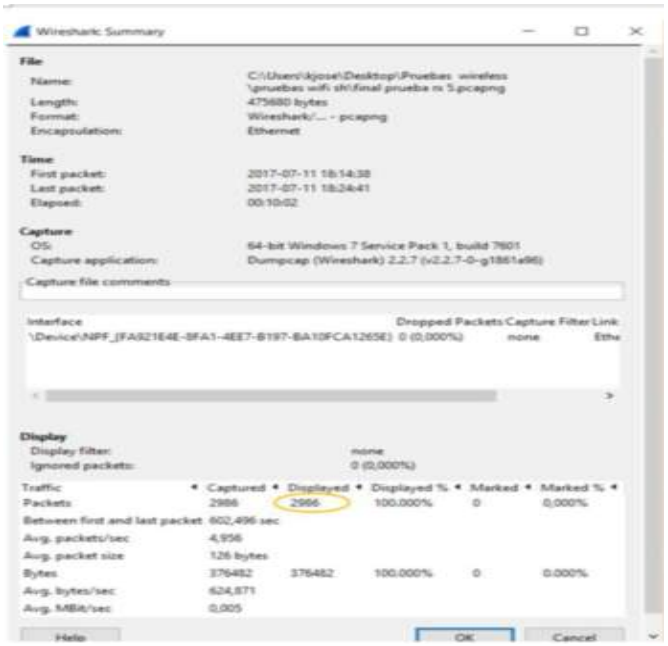


Figura 5-3: Resumen de paquetes recibidos por el cliente

Realizado por: Caiza José. 2017

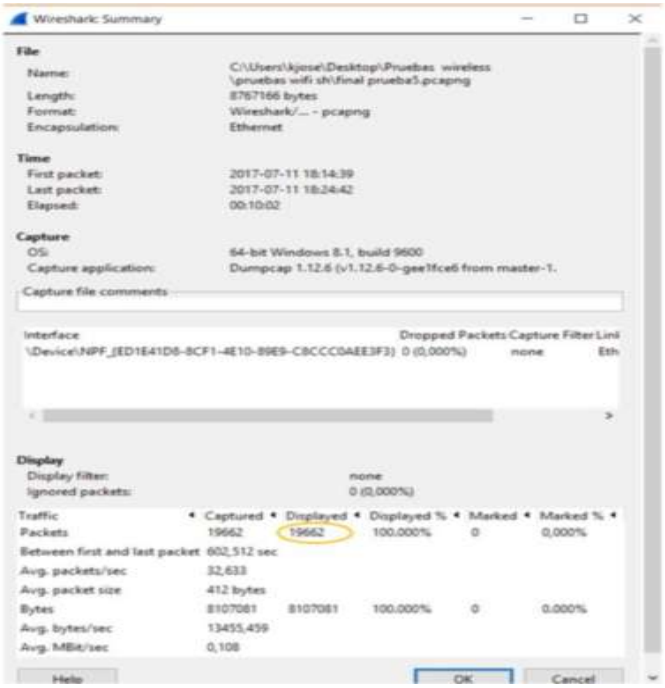


Figura 6-3: Resumen de paquetes enviados desde el servidor

Realizado por: Caiza José. 2017

Para determinar los paquetes que se han pérdido en el tiempo de captura se calcula a partir de la fórmula:

$$Pl(\%) = \frac{Pe - Pr}{Pe} * 100\%$$

En donde PI es la pérdida de paquetes, Pe los paquetes enviados por el emisor y Pr los paquetes recibidos por receptor, para esta prueba se obtiene una pérdida porcentual de 22.51% de total de paquetes pérdidos en toda la transmisión.

3.3.2.3 Retardo

Para poder realizar la captura de el retardo se procede a enviar paquetes ICMP de solicitud y respuesta desde el dispositivo cliente ejecutando cmd y el comando ping en donde se especifíca la dirección IP del servidor en este caso la dirección 192.168.1.25. A continuación se muestra la información brindada en la prueba numero 5:

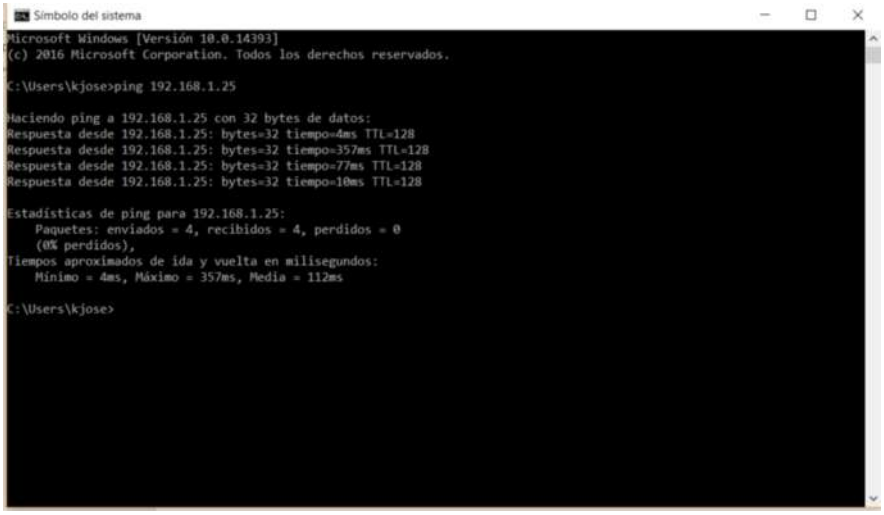


Figura 7-3: Prueba del retardo en Cmd

Realizado por: Caiza José. 2017

3.3.3 *Datos obtenidos de las pruebas*

3.3.3.1 Pruebas de la red sin la implementación del portal cautivo

Los resultados obtenidos se muestran en la tablas número 13-3 y 14-3.

Duración de la prueba: 10 minutos

Datos obtenidos de las pruebas de la pérdida de paquetes sin portal cautivo

Tabla 7-3: Medición de Retardo sin portal cautivo

Prueba	Retardo (ms)	Porcentaje (%)
1	49	40
2	74	60
3	98	80
4	34	40
5	112	80
6	15	20
7	60	40
8	190	100
9	283	100

10	308	100
Promedio	122,3	66

Realizado por: Caiza José. 2017

Tabla 8-3: Medición de Pérdida de Paquetes sin portal cautivo

Prueba	Paquetes mostrados por el emisor	Paquetes mostrados por el cliente
1	73606	56325
2	25358	18624
3	12158	9356
4	29277	22702
5	19662	15236
6	19005	14231
7	13469	9745
8	15603	11446
9	21720	16002
10	87945	68541

Realizado por: Caiza José. 2017

A continuación se muestra el resultado de la pérdida de paquetes en la tabla 8-3, la misma que se calculó mediante la fórmula de pérdida de paquetes:

$$Pl(\%) = \frac{Pe - Pr}{Pe} * 100\%$$

Tabla 9-3: Pérdida de paquetes de las pruebas realizadas sin portal cautivo

Prueba	Paquetes mostrados por el emisor	Paquetes mostrados por el cliente	Pérdida de paquetes (%)
1	73606	56325	23.48
2	25358	18624	26.55
3	12158	9356	23.04
4	29277	22702	22.45

5	19662	15236	22.51
6	19005	14231	25.12
7	13469	9745	27.64
8	15603	11446	26.64
9	21720	16002	26.32
10	87945	68541	22.06

Realizado por: Caiza José. 2017

Tabla 10-3: Medición del Jitter sin portal cautivo

Prueba	Jitter (ms)	Porcentaje de Ponderación
1	7.791	20
2	8.23	20
3	8.564	20
4	9.11	20
5	8.69	20
6	9.34	20
7	7.53	20
8	10.02	25
9	9.76	20
10	10.29	25
Promedio	8.93	21

Realizado por: Caiza José. 2017

Tabla 11-3: Medición de MOS sin portal cautivo

Prueba	MOS	Porcentaje de Ponderación (%)
1	4	100
2	5	100
3	5	100
4	4	100

5	3	80
6	4	100
7	3	80
8	4	100
9	4	100
10	3	80
Promedio	3,9	94

Realizado por: Caiza José. 2017

3.3.3.2 Resultados de las pruebas de la red sin la implementación del portal cautivo

Tabla 12-3: Resumen de la ponderación de porcentajes de los resultados obtenidos sin portal cautivo

Prueba	MOS (%)	Jitter (%)	Pérdida de Paquetes (%)	Retardo (%)
1	100	20	23.48	40
2	100	20	26.55	60
3	100	20	23.04	80
4	100	20	22.45	40
5	80	20	22.51	80
6	100	20	25.12	20
7	80	20	27.64	40
8	100	25	26.64	100
9	100	20	26.32	100
10	80	25	22.06	100
Total Promedio	94	21	24.581	66

Realizado por: Caiza José. 2017

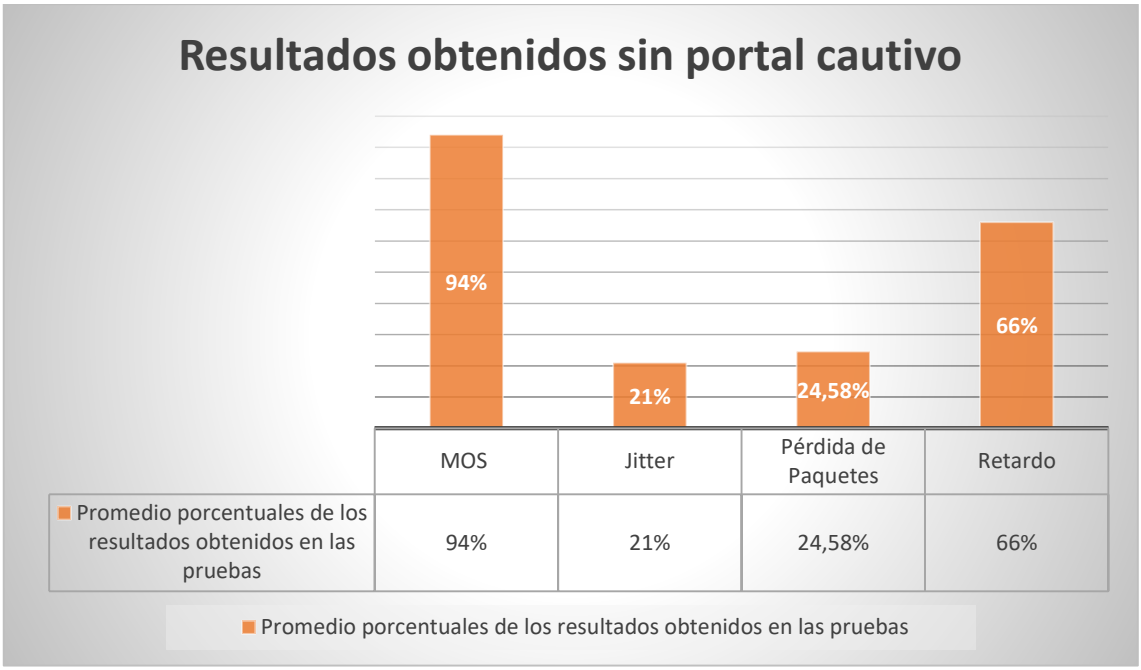


Gráfico 1-3: Resumen del promedio de datos porcentuales recolectados sin portal cautivo

Realizado por: Caiza José. 2017

Tabla 13-3: Resumen de resultados obtenidos en las pruebas sin portal cautivo del retardo y jitter.

Prueba	Jitter (ms)	Retardo (ms)
1	7.791	49
2	8.23	74
3	8.564	98
4	9.11	34
5	8.69	112
6	9.34	15
7	7.53	60
8	10.02	190
9	9.76	283
10	10.29	308
Total Promedio	8.93	122.3

Realizado por: Caiza José. 2017

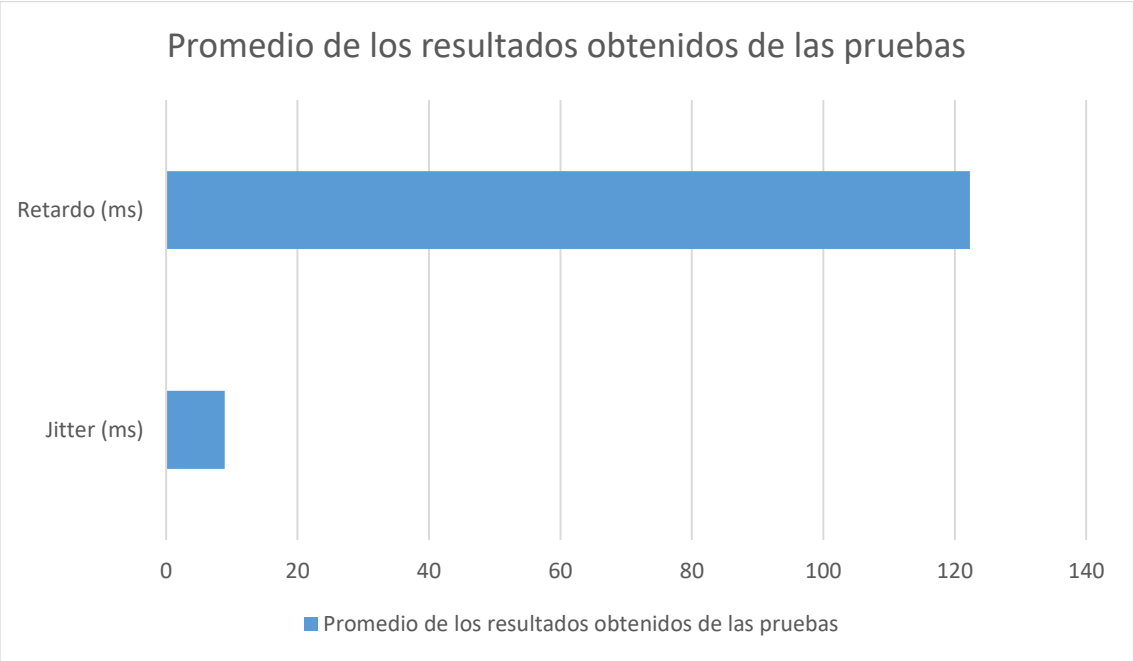


Gráfico 2-3: Resumen del promedio de datos recolectados sin portal cautivo del retardo y jitter.

Realizado por: Caiza José. 2017

Tabla 14-3: Resumen de resultados obtenidos en las pruebas sin portal cautivo del MOS y pérdida de paquetes.

Prueba	MOS	Pérdida de Paquetes (%)
1	4	23.48
2	5	26.55
3	5	23.04
4	4	22.45
5	3	22.51
6	4	25.12
7	3	27.64
8	4	26.64
9	4	26.32
10	3	22.06
Total Promedio	3.9	24.581

Realizado por: Caiza José. 2017

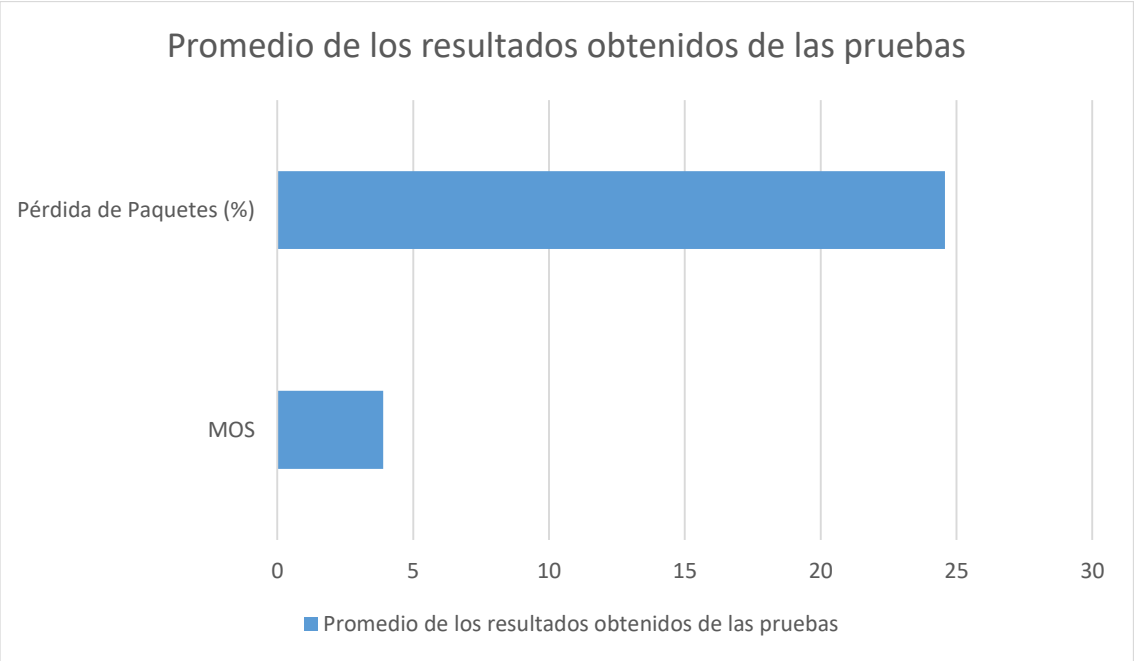


Gráfico 3-3: Resumen del promedio de datos recolectados sin portal cautivo del MOS y pérdida de paquetes.

Realizado por: Caiza José. 2017

3.3.3.3 Pruebas de la red con la implementación del portal cautivo

Los resultados obtenidos se muestran en las tablas número 21-3 y 22-3.

Duración de la prueba: 10 minutos

Tabla 15-3: Medición del Retardo con Portal Cautivo

Prueba	Retardo (ms)	Porcentaje (%)
1	7	10
2	9	10
3	55	40
4	96	70
5	71	50
6	84	60
7	62	50
8	9	10
9	5	10

10	71	50
Promedio	46,9	36

Realizado por: Caiza José. 2017

Tabla 16-3: Datos obtenidos de las pruebas de la pérdida de paquetes con portal cautivo

Prueba	Paquetes mostrados por el emisor	Paquetes mostrados por el cliente
1	22786	19468
2	22976	19986
3	18064	16232
4	18103	15989
5	22318	19412
6	25943	23002
7	32871	29100
8	21156	18173
9	19013	16992
10	24405	21478

Realizado por: Caiza José. 2017

A continuación se muestra el resultado de la pérdida de paquetes en la tabla 8-3, la misma que se calculó mediante la fórmula de pérdida de paquetes:

$$Pl(\%) = \frac{Pe - Pr}{Pe} * 100\%$$

Tabla 17-3: Pérdida de paquetes de las pruebas realizadas con portal cautivo

Prueba	Paquetes mostrados por el emisor	Paquetes mostrados por el cliente	Pérdida de paquetes (%)
1	22786	19468	14.56
2	22976	19986	13.01
3	18064	16232	10.14
4	18103	15989	11.67

5	22318	19412	13.02
6	25943	23002	11.33
7	32871	29100	11.47
8	21156	18173	14.10
9	19013	16992	10.63
10	24405	21478	11.99

Realizado por: Caiza José. 2017

Tabla 18-3: Medición de Jitter con Portal cautivo

Prueba	Jitter (ms)	Porcentaje de Ponderación (%)
1	7.35	15
2	6.88	15
3	5.92	15
4	5.26	15
5	6.84	15
6	4.965	10
7	5.48	15
8	7.62	15
9	4.13	10
10	5.74	15
Promedio	6.02	14

Realizado por: Caiza José. 2017

Tabla 19-3: Medición de MOS

Prueba	MOS	Porcentaje de Ponderación (%)
1	4	100
2	5	100
3	5	100
4	4	100

5	5	100
6	4	100
7	4	100
8	3	80
9	5	100
10	4	100
Promedio	4,4	98

Realizado por: Caiza José. 2017

3.3.3.4 Resultados de las pruebas de la red con la implementación del portal cautivo

Tabla 20-3: Resumen de Porcentajes de Ponderación de los resultados obtenidos de las pruebas con el Portal Cautivo

Prueba	MOS (%)	Jitter (%)	Pérdida de Paquetes (%)	Retardo (%)
1	100	15	14.56	10
2	100	15	13.01	10
3	100	15	10.14	40
4	100	15	11.67	70
5	100	15	13.02	50
6	100	10	11.33	60
7	100	15	11.47	50
8	80	15	14.10	10
9	100	10	10.63	10
10	100	15	11.99	50
Total Promedio	98	14	12.19	36

Realizado por: Caiza José. 2017

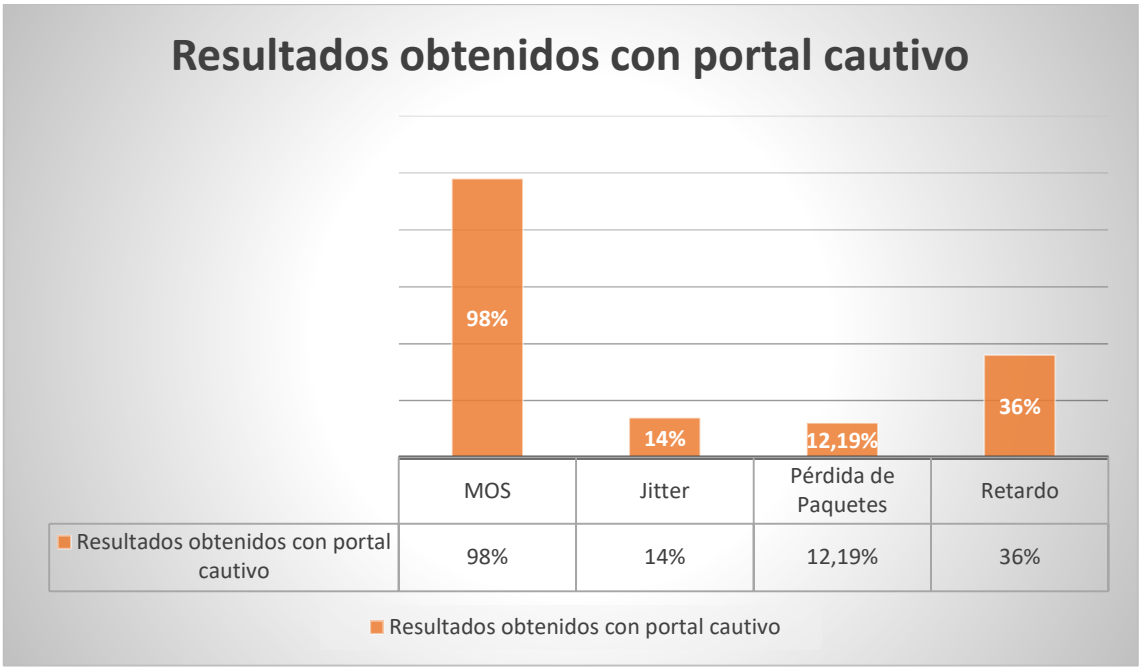


Gráfico 4-3: Resumen porcentual del promedio de datos recolectados con portal cautivo

Realizado por: Caiza José. 2017

Tabla 21-3: Tabla de resultados obtenidos de las pruebas con el Portal Cautivo del retardo y jitter.

Prueba	Jitter (ms)	Retardo (ms)
1	7.35	7
2	6.88	9
3	5.92	55
4	5.26	96
5	6.84	71
6	4.965	84
7	5.48	62
8	7.62	9
9	4.13	5
10	5.74	71
Total Promedio	6.02	46,9

Realizado por: Caiza José. 2017

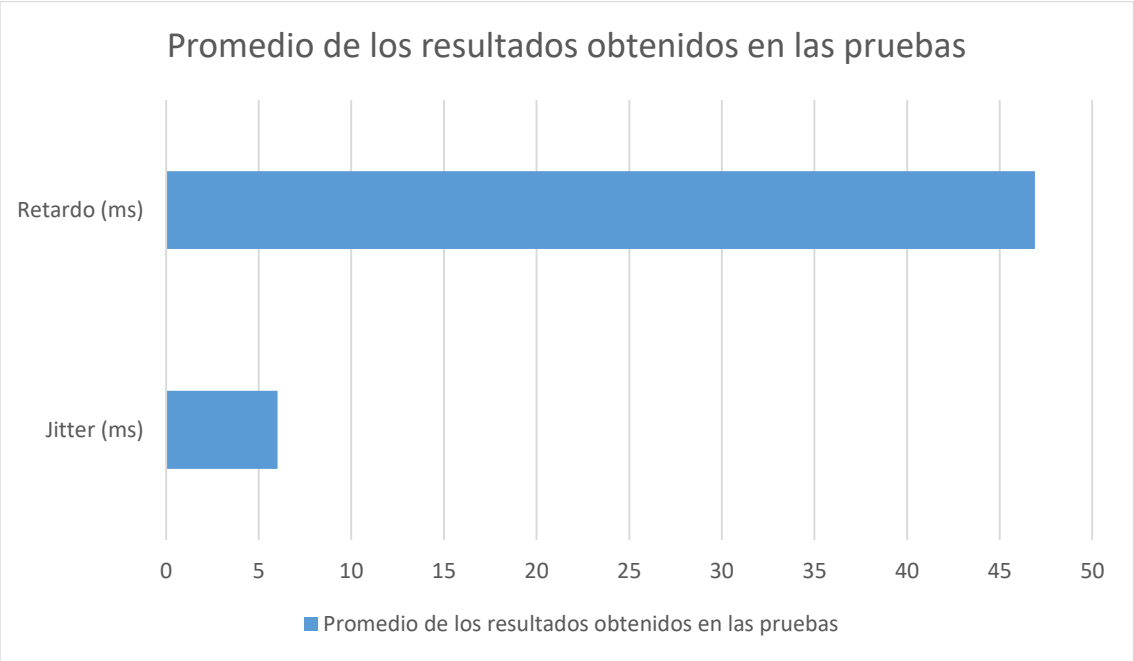


Gráfico 5-3: Resumen del promedio de datos recolectados con portal cautivo del retardo y jitter.

Realizado por: Caiza José. 2017

Tabla 22-3: Tabla de resultados obtenidos de las pruebas con el Portal Cautivo del MOS y pérdida de paquetes.

Prueba	MOS	Pérdida de Paquetes (%)
1	4	14.56
2	5	13.01
3	5	10.14
4	4	11.67
5	5	13.02
6	4	11.33
7	4	11.47
8	4	14.10
9	5	10.63
10	4	11.99
Total Promedio	4,4	12.19

Realizado por: Caiza José. 2017

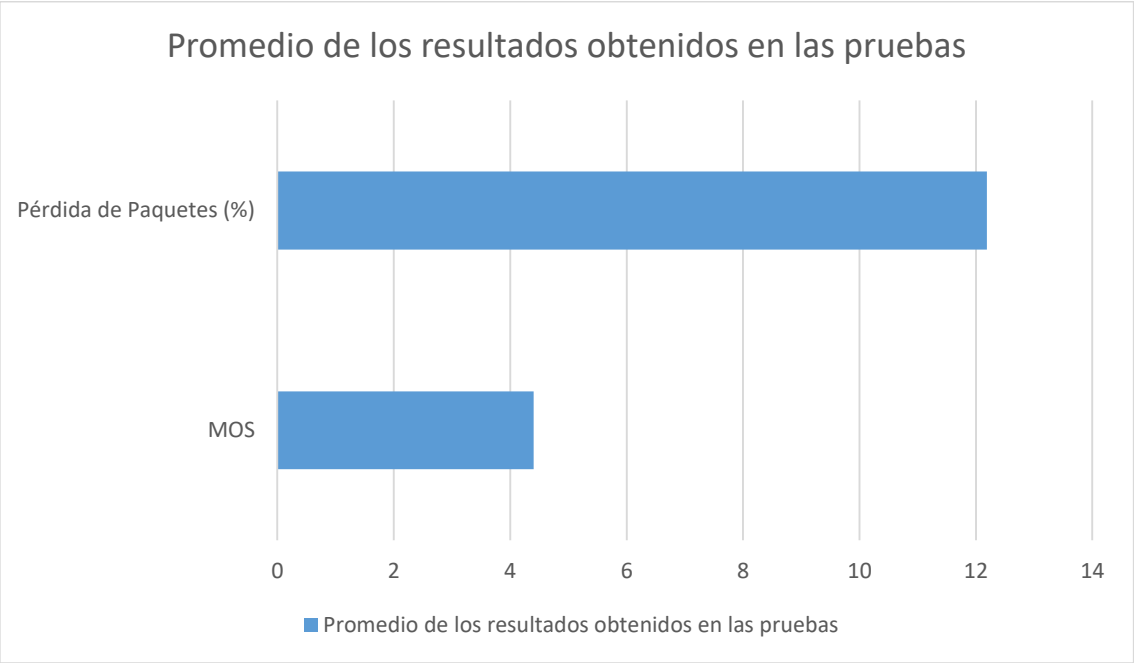


Gráfico 6-3: Resumen del promedio de datos recolectados con portal cautivo del MOS y pérdida de paquetes.

Realizado por: Caiza José. 2017

3.3.4 *Tabla comparativa de escenarios*

Comparación entre el escenario sin portal cautivo vs el escenario con la implementación del portal cautivo:

Tabla 23-3: Resumen de los datos comparativos en porcentajes de los escenarios

Parámetros (%) / Escenarios	Sin portal cautivo	Con portal cautivo
Pérdida de Paquetes	24.581	12.19
Jitter	21	14
Retardo	66	36
MOS (Mean Opinion Score)	94	88

Realizado por: Caiza José. 2017

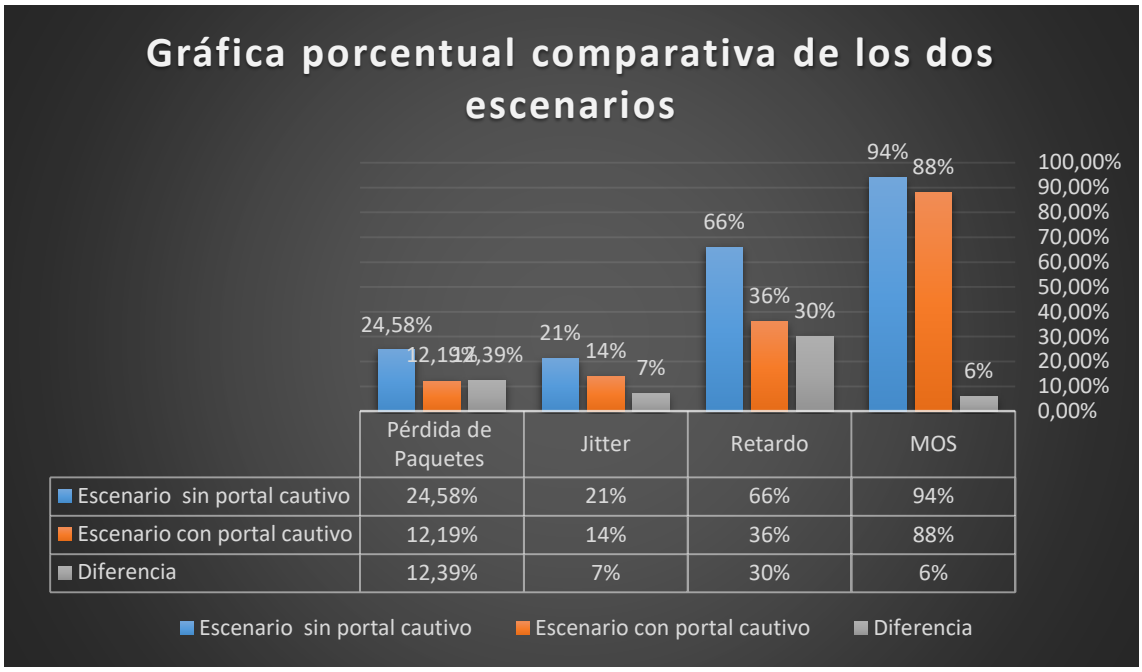


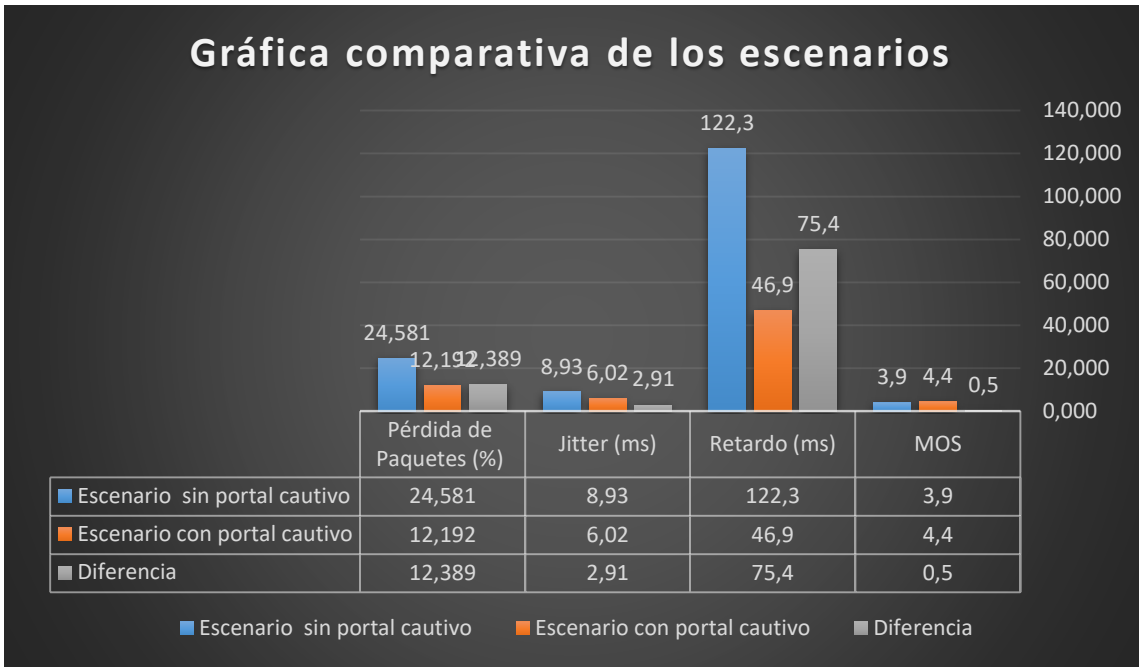
Gráfico 7-3: Gráfica comparativa de resultados porcentuales obtenidos en los dos escenarios

Realizado por: Caiza José. 2017

Tabla 24-3: Resumen de los datos comparativos de los escenarios

Parámetros / Escenarios	Sin portal cautivo	Con portal cautivo
Pérdida de Paquetes (%)	24.581	12.19
Jitter (ms)	8.93	6.02
Retardo (ms)	122.3	46.9
MOS (Mean Opinion Score)	3.9	4.4

Realizado por: Caiza José. 2017



	Pérdida de Paquetes (%)	Jitter (ms)	Retardo (ms)	MOS
Escenario sin portal cautivo	24,581	8,93	122,3	3,9
Escenario con portal cautivo	12,192	6,02	46,9	4,4
Diferencia	12,389	2,91	75,4	0,5

Gráfico 8-3: Gráfica comparativa de resultados obtenidos en los dos escenarios

Realizado por: Caiza José. 2017

3.3.4.1 *Análisis comparativo de resultados obtenidos en las pruebas*

Después de realizar la recolección de la información de las pruebas, se procede a elaborar un análisis comparativo de la medición de todos los parámetros obtenidos. En primera instancia se puede observar que en el parámetro de la pérdida de paquetes sin el portal cautivo se tiene un 24.581 % vs 12.192 % que se obtiene con la implementación del portal cautivo, donde se evidencia una mejoría del 12.389 %. Como segundo parámetro se tiene el jitter que en la implementación sin portal cautivo nos da un valor de 8.93 ms vs 6.02 ms con portal cautivo lo que da una diferencia de 2.90 ms. El promedio total del retardo medido en las pruebas sin portal cautivo se tiene 122.3 ms vs 46.9 ms con la implementación del portal cautivo obteniendo una diferencia de 75.4 ms y un 30 % total de mejoría lo cual describe un menor retardo en la implementación de la red con portal cautivo. En cuanto al MOS se puede observar una mejoría del 6 % en la experiencia del usuario con respecto al servicio brindado con la implementación del portal cautivo, cabe recalcar que las pruebas se realizaron en las horas en donde hay mayor trafico en la red. Con estos resultados se puede concluir que con la implementación del portal cautivo la red inalámbrica mejora significativamente.

CONCLUSIONES

Cumpliendo con los objetivos propuestos y las pertinentes evaluaciones de los resultados obtenidos se concluye lo siguiente:

1. Gracias al presente estudio comparativo de la implementación de un portal cautivo mediante las tecnologías Mikrotik y Cisco se puede concluir que los dispositivos Mikrotik ofrecen muchas prestaciones a un precio muy bajo lo cual hace que sea un factor decisivo al momento de elegir que tecnología adquirir.

2. Los dispositivos Mikrotik controlan de buena manera los recursos disponibles en la red, tienen un rendimiento igual similar a los dispositivos Cisco y a un bajo precio, los cuales son accesibles para cualquier tipo de cliente.

3. La configuración de un dispositivo Mikrotik es global es decir que la configuración que se realice en un dispositivo es escalable y puede trasladarse a cualquier otro modelo, la diferencia está en su capacidad de operación.

4. Para evitar la saturación en el funcionamiento del router Mikrotik se optó por adquirir una antena nanostation loco m2, que permite enviar la información de manera inalámbrica hacia los usuarios, además que mejora la capacidad de cobertura de la solución implementada.

5. La red inalámbrica de IPREX tiene una mejoría del 12.389 % en cuanto a la pérdida de paquetes, en el jitter presenta un 7%, una notoria mejoría del retardo con un 30% y el MOS de un 6% que representa un mayor rendimiento y aprovechamiento de los recursos de la red inalámbrica en el Instituto de preparación para Exámenes IPREX.

RECOMENDACIONES:

1. Se recomienda deshabilitar los adaptadores de red virtuales al momento de abrir la aplicación de Winbox, ya que se produce un error de comunicación entre el dispositivo Mikrotik y el computador.

2. Para mejorar la velocidad del internet y aumentar el número de usuarios del servicio de portal cautivo se recomienda a la empresa obtener el servicio de fibra óptica o a su vez adquirir un ancho de banda mayor a 4 Mbps, lo cual permitirá mayor rapidez en la transmisión de datos en la red inalámbrica.

3. Se recomienda al personal que labora en la oficina central de IPREX familiarizarse con la tecnología Mikrotik ya que serán los encargados de administrar el servicio de portal cautivo agregando a nuevos usuarios, debido a que no se dispone actualmente con un técnico de planta.

4. Para evitar el solapamiento de canales en la red inalámbrica es recomendable trabajar a 5 canales de separación, en esta implementación se usó el canal 6 para el envío de datos inalámbricos.

5. Para evitar generar interferencias en el espectro electromagnético es necesario configurar la potencia de transmisión de la antena nanostation loco m2 de acuerdo a la distancia que se necesite cubrir con el servicio.

BIBLIOGRAFÍA

ABOBA. *Radius RFC 2869* [en línea].United States of América,2003. pp: 2-15 [Consulta: 20 de Febrero del 2017]. Disponible en: http://www.faqs.org/rfcs/rfc3579.html

CLAUDIO TAPIA, Víctor Alfonso, *Monitoreo de los dispositivos y equipos de los clientes del proveedor de internet Speedy* [en línea]. (Tesis de pregrado). Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Escuela de Ingeniería Electrónica y Comunicaciones. Ecuador, 2009. pp: 20-24 [Consulta: 24 de Febrero del 2017]. Disponible en: http://repositorio.uta.edu.ec/handle/123456789/223

CLAVER, Martín Miguel; & MARTINEZ, Juan Facundo, *Análisis técnico comercial, de la implementación de accesos wifi como soporte de las redes móviles* [en línea]. (Tesis de pregrado) Universidad Argentina de la Empresa. Facultad de Ingeniería y Ciencias Exactas. Argentina, 2014. pp: 41-45 [Consulta: 25 de Febrero del 2017]. Disponible en: https://repositorio.uade.edu.ar/xmlui/bitstream/handle/123456789/2454/Claver.pdf?sequence=1)

GARCÍA & HYTNEN, "An analysis of wireless security" [en línea]. *Journal of Computing Sciences in Colleges.* United States of America, 2006. pp: 57-62 [Consulta: 26 de Febrero del 2017].

INSTITUTO INTERNACIONAL PARA LA EDUCACIÓN SUPERIOR EN AMÉRICA LATINA Y EL CARIBE, *Guía-Autoevaluación de Programas de Pregrado*[en línea]. Ecuador, 2005. [Consulta: 4 Marzo del 2017]. Disponible en: http://www.uladech.edu.pe/images/stories/universidad/documentos/2012/Guia-Autoevaluacion-Programas-Pregrado-CALED.pdf

LUACES, J., *Seguridad en redes inalámbricas de área local WLAN* [en línea]. España, 2009 [Consulta: 22 de marzo del 2017]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf

LAZO GARCÍA, Nuttsy Aurora. *Diseño de la implementación de una red LAN y WLAN con sistema de control de Acceso mediante servidores AAA* [en línea]. (Tesis de pregrado). Pontificia Universidad Católica del Perú. Facultad de Ciencias e Ingeniería. Ingeniería de las Telecomunicaciones. Perú, 2012. [Consulta: 29 de marzo del 2017]. Disponible en: http://tesis.pucp.edu.pe/repositorio/handle/123456789/1445

MALDONADO, ÁNGEL, *Implementación de un portal cautivo que permita el control de acceso al servicio de internet a los estudiantes del colegio San Luis Gonzaga* [en línea]. (Tesis

de pregrado) Universidad Politécnica Salesiana. Escuela de Ingeniería de Sistemas. Ecuador, 2012. [Consulta: 4 de Abril del 20170]. Disponible en: http://www.dspace.ups.edu.ec/bitstream/123456789/4167/1/UPS-ST000959.pdf

MENA Y JARA, *Análisis Diseño y Propuesta de implementación de un portal cautivo para la red inalámbrica de la Universidad Politécnica Salesiana sede Quito* [en línea]. (Tesis de pregrado) Universidad Politécnica Salesiana. Escuela de Ingeniería de Sistemas. Ecuador, 2013. [Consulta: 25 de Abril del 2017]. Disponible en: http://dspace.ups.edu.ec/bitstream/123456789/5348/1/UPS-ST001027.pdf

MITTON, D., *Autenticación, Autorización y Contabilidad: Evaluación de Protocolo AAA* [en línea]. United States of America, 2001. [Consulta: 28 de Mayo del 2017]. Disponible en: https://www.rfc-editor.org/rfc/rfc3127.txt

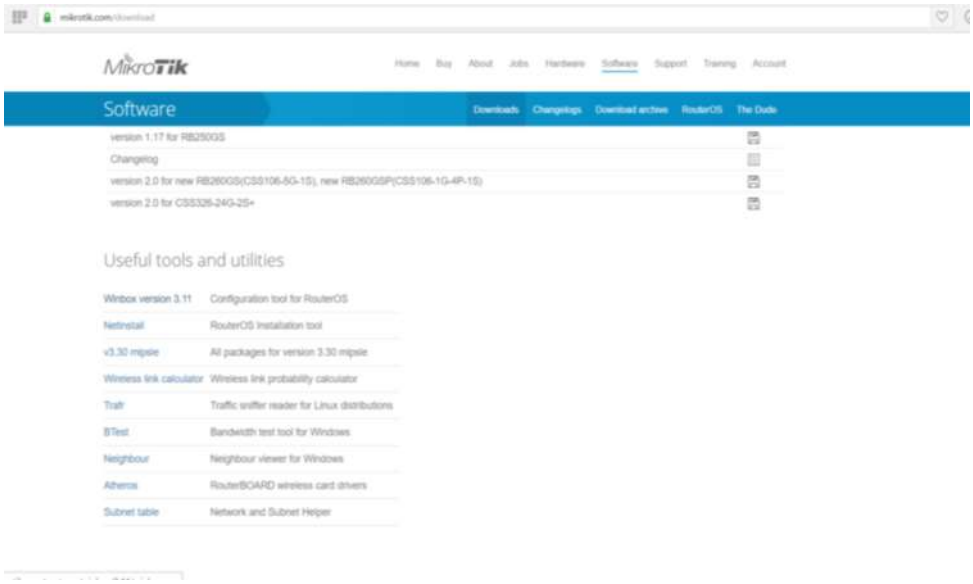
SIMPSON, W., *Red Grupo de Trabajo .Protocolo PPP.* [en línea]. United States of America, 1994. [Consulta: 29 de Mayo del 2017]. Disponible en: https://www.rfc-editor.org/rfc/rfc1661.txt)

WIRESHARK, *Wireshark features* [en línea]. United States of America, 2017. [Consulta: 02 de Junio del 2017]. Disponible en: https://www.wireshark.org/

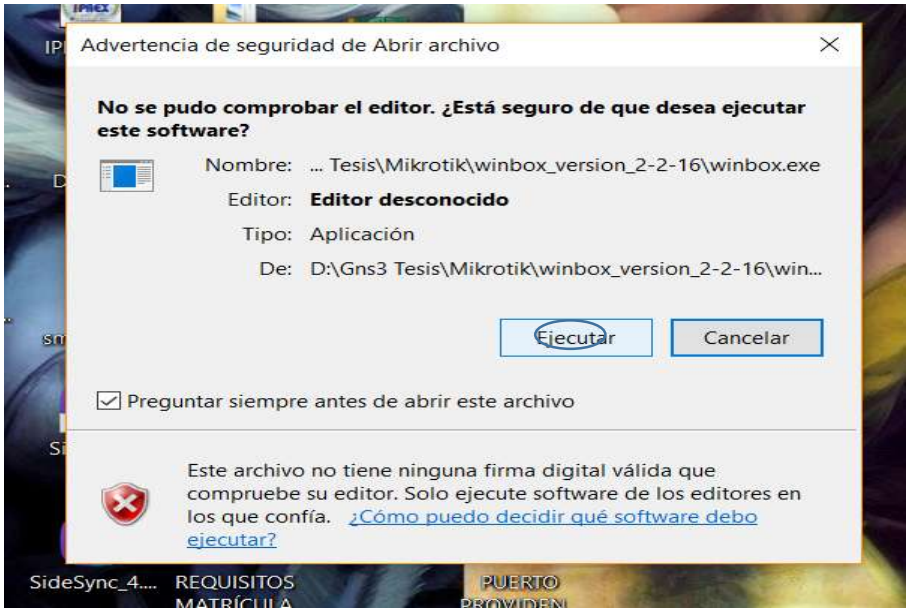
ANEXO A

Configuración del portal cautivo en Mikrotik

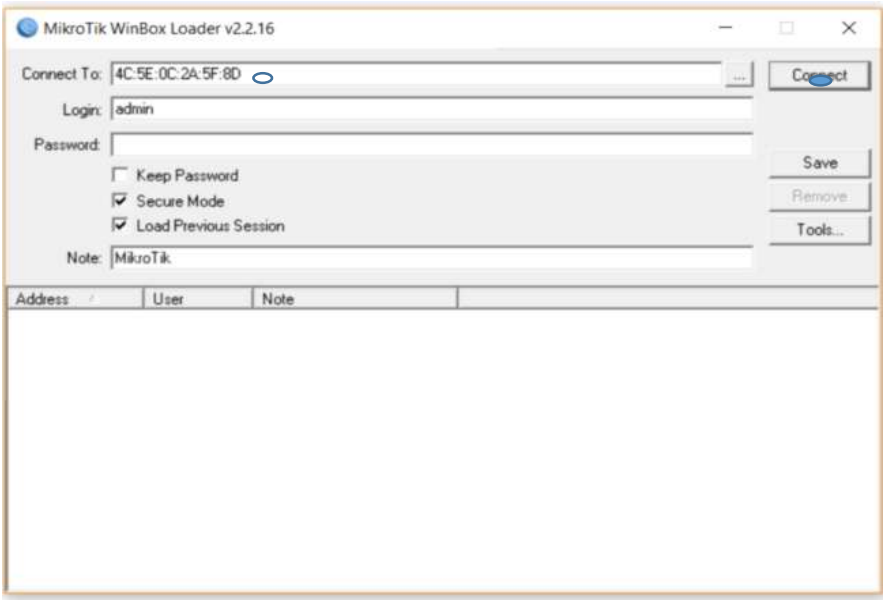
1.- Descargar el software Winbox que permite la configuración en un dispositivo Mikrotik en la página web oficial.



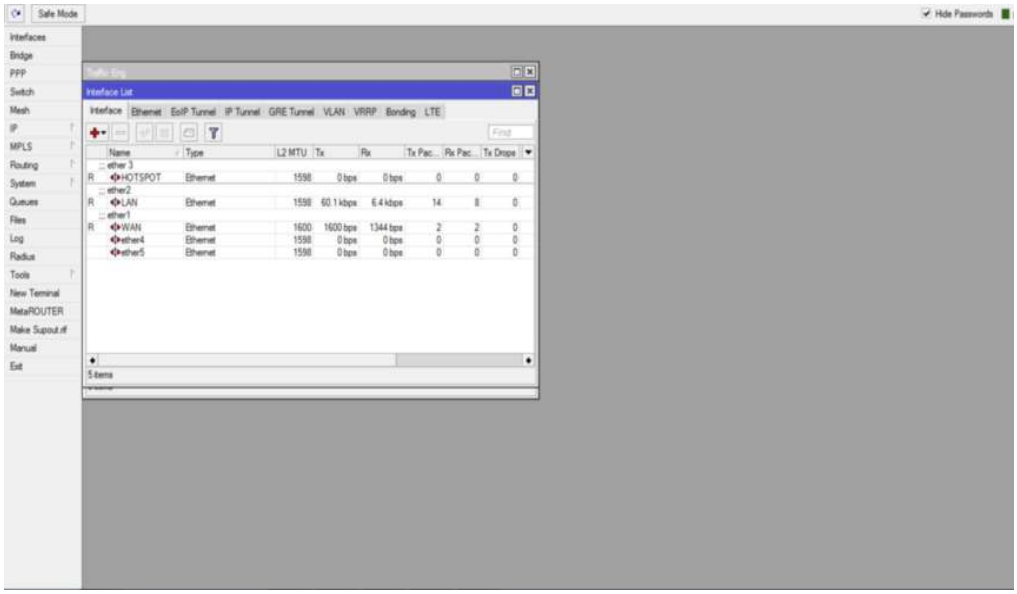
2.- Se ejecuta el software descargado.



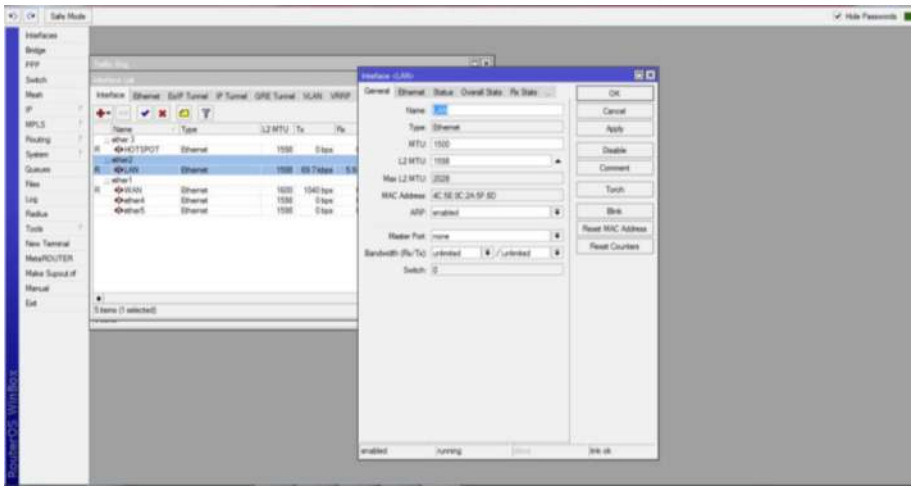
3.- Se abrirá la interfaz en donde seleccionamos la pestaña que nos muestra los dispositivos Mikrotik conectados.



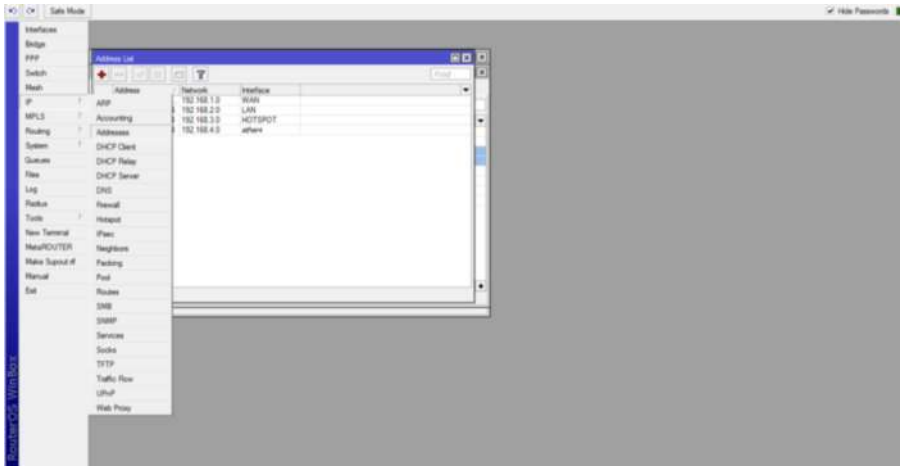
4.- Se da click izquierdo y se selecciona la opción en donde se encuentra la dirección MAC del dispositivo Mikrotik que se tenga ingresando así al interfaz de configuración.

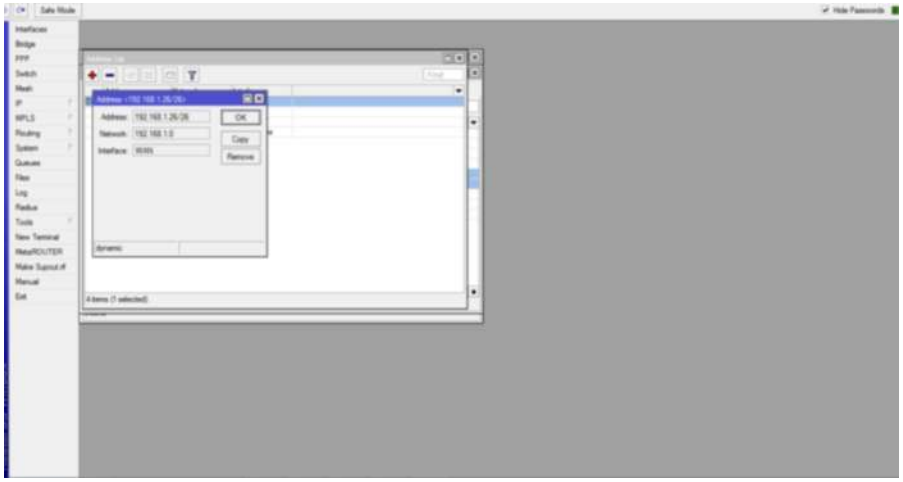


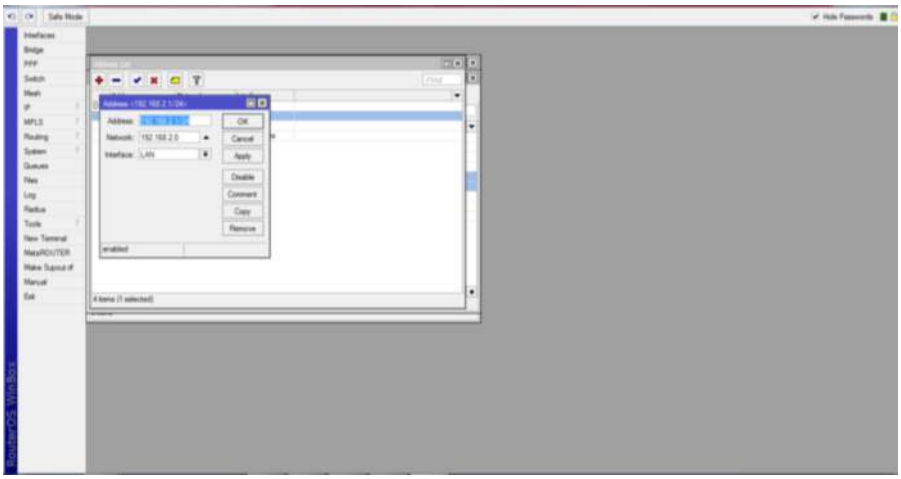
5.- Se renombra las interfaces y se asigna nombres de acuerdo a los requerimientos que tenga el usuario en este caso se usara la interfaz del puerto 2 para la red de las oficinas centrales el puerto 3 para el portal cautivo y el puerto 4 para la interfaz de los laboratorios de la institución.

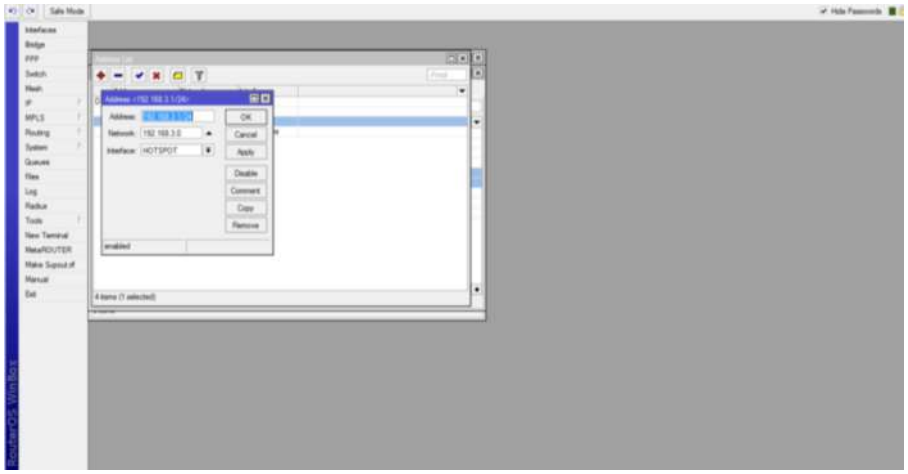


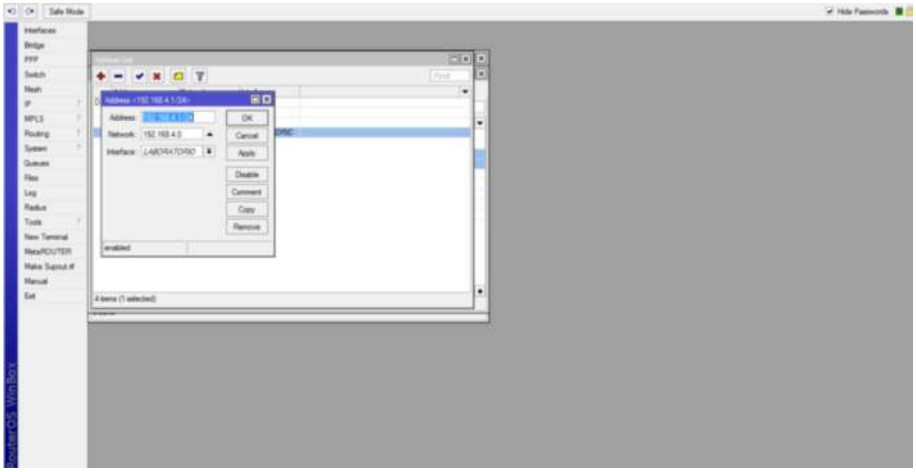
6.- Una vez configuradas y cambiados los nombres de las interfaces se procede a darle direccionamiento ip de la siguiente manera:



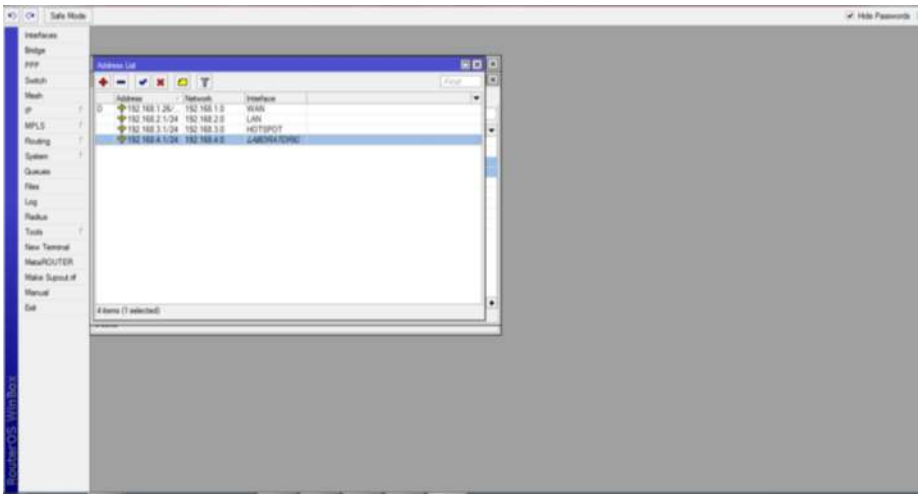




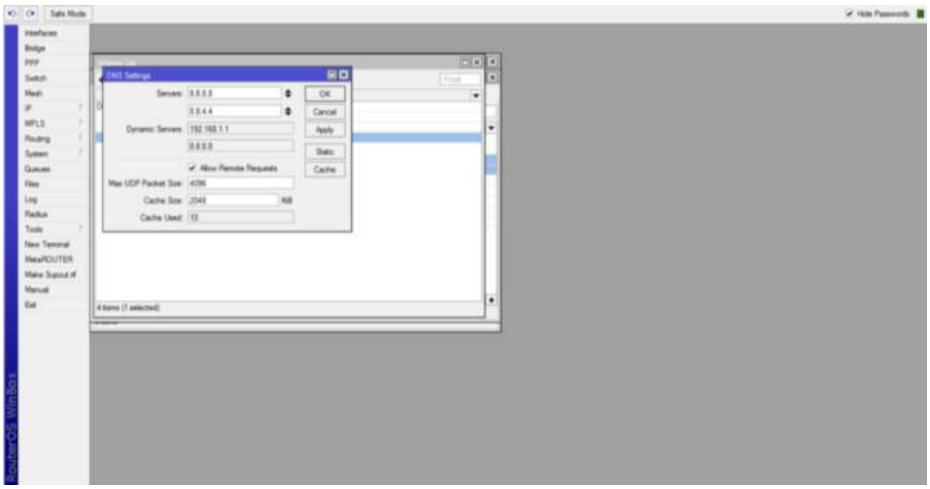




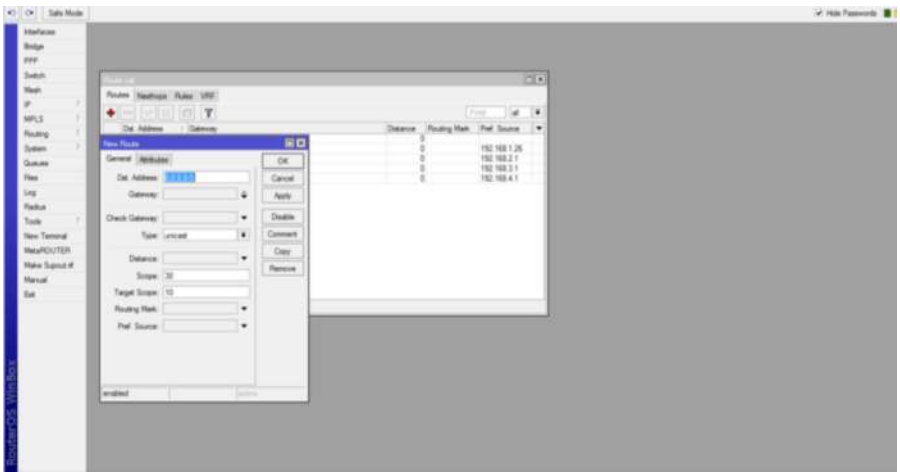
Se obtiene una configuración que se muestra a continuación:



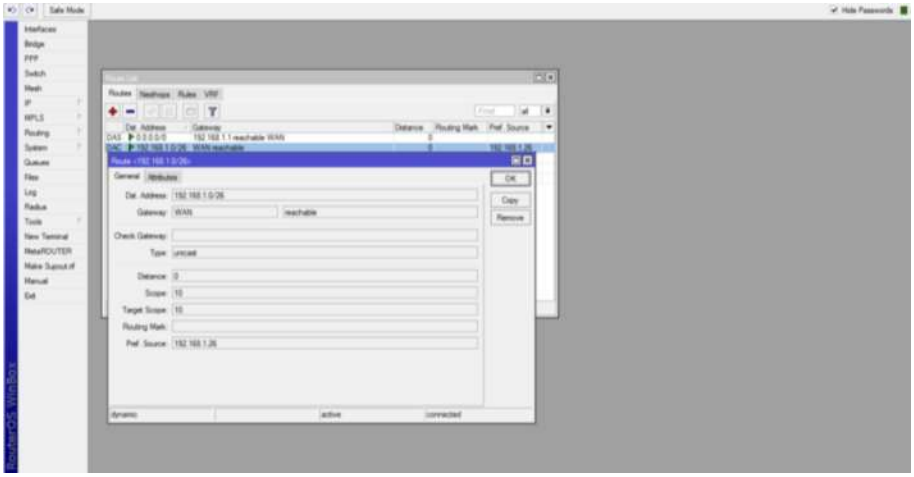
Una vez creadas las interfaces con sus respectivas direcciones IP, se debe configurar los servidores DNS del proveedor de servicio de internet para tener acceso al servicio de internet.



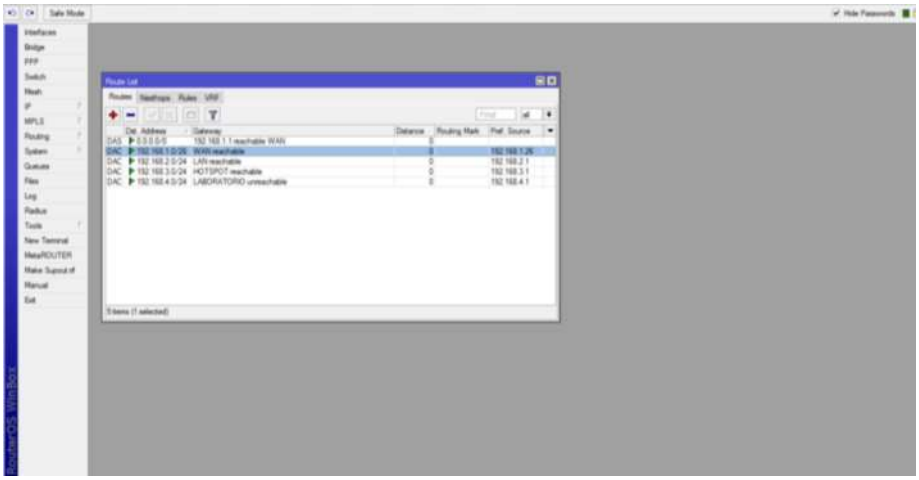
Se configura las interfaces necesitadas por el usuario para que la información pueda llegar a sui destino:



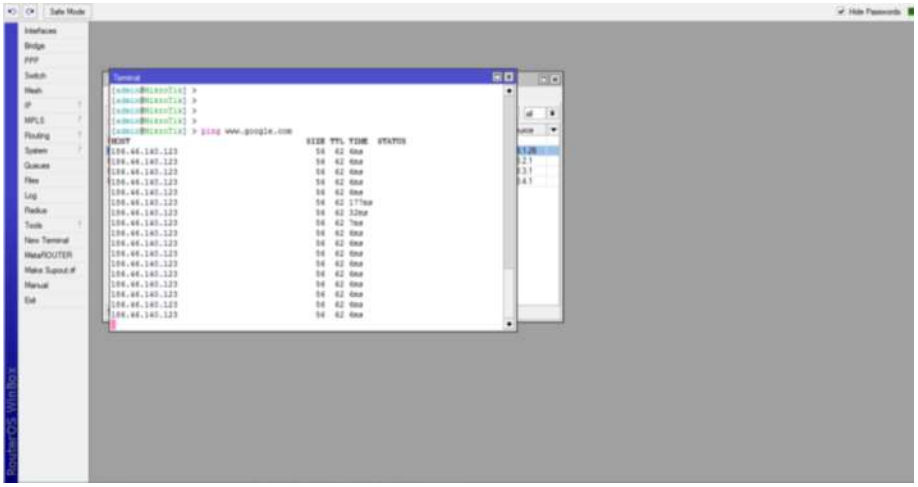
Se procede a configurar cada una de las interfaces de la siguiente manera:



Una vez terminado el proceso de configuración se obtiene que todas las rutas trazadas por el router hacia su destino llegan exitosamente:



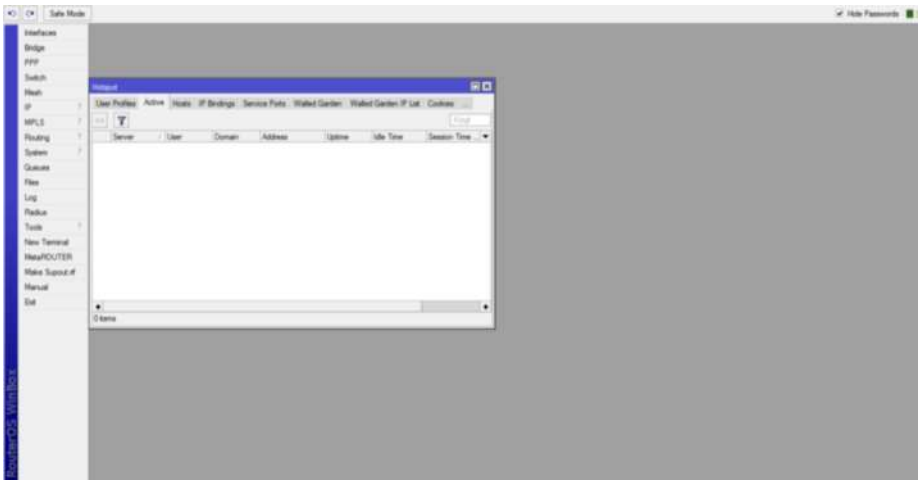
Terminado la configuración se procede a comprobar si existe servicio de internet en la red LAN



Se observa que la configuración a sido exitosa.

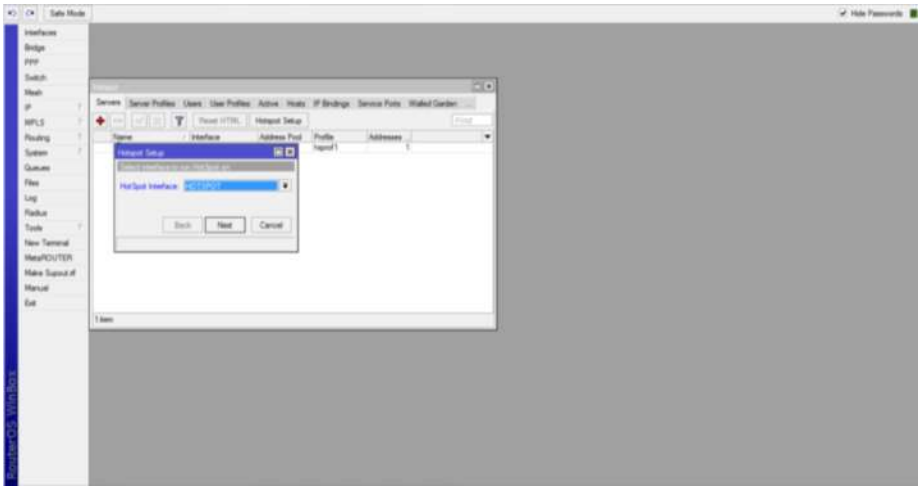
Configuración del hotspot

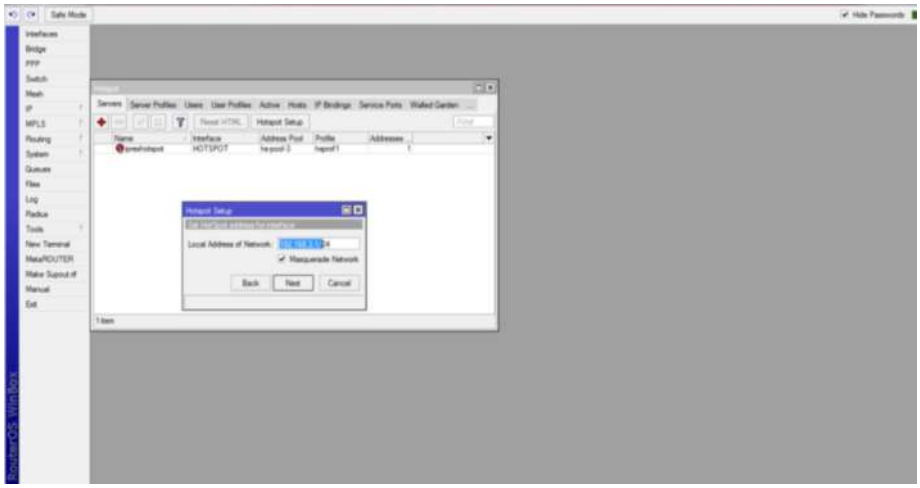
Se elige la pestaña IP>hotspot

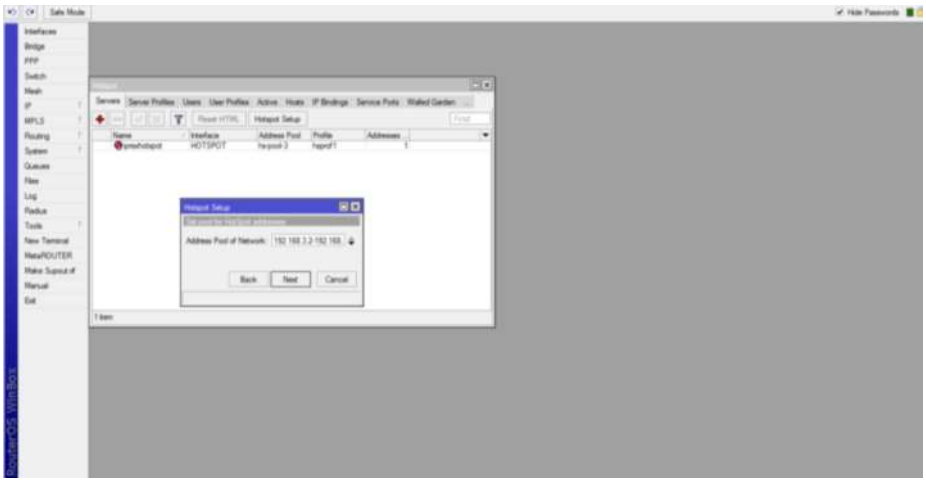


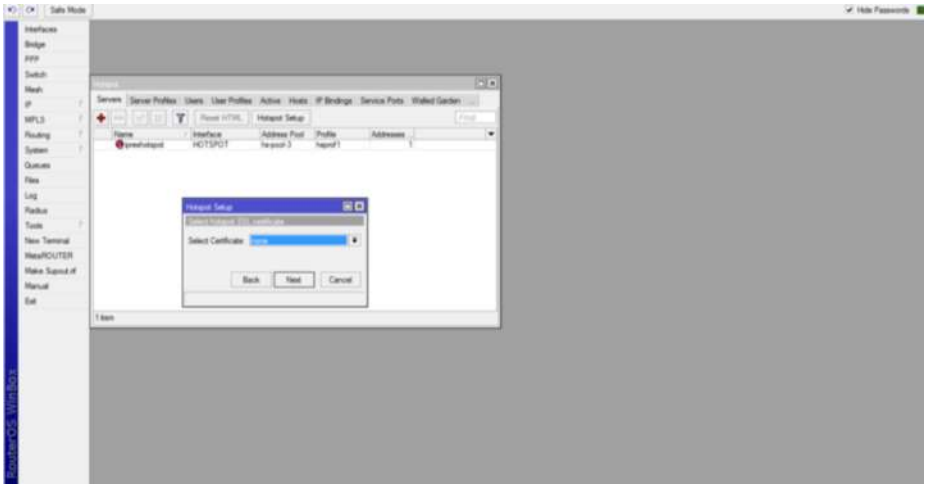
Se selecciona la opción Hotspot Setup

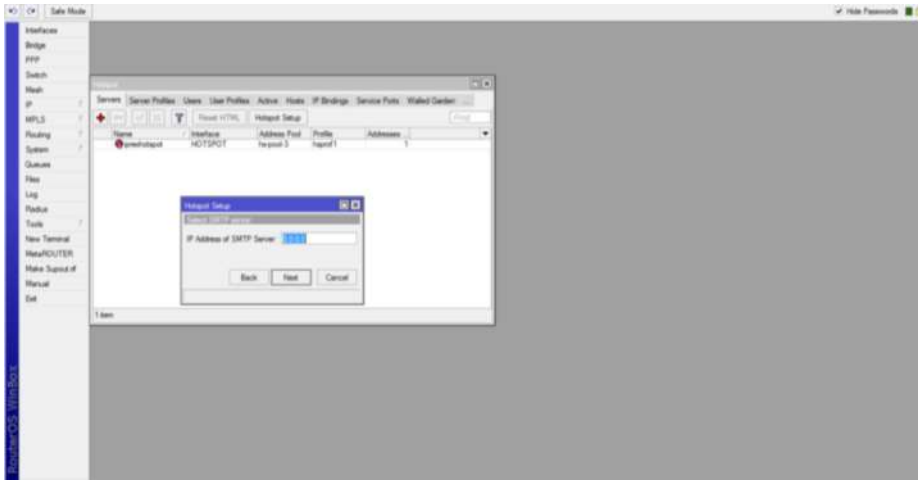
Se sigue los pasos del asistente de configuración.

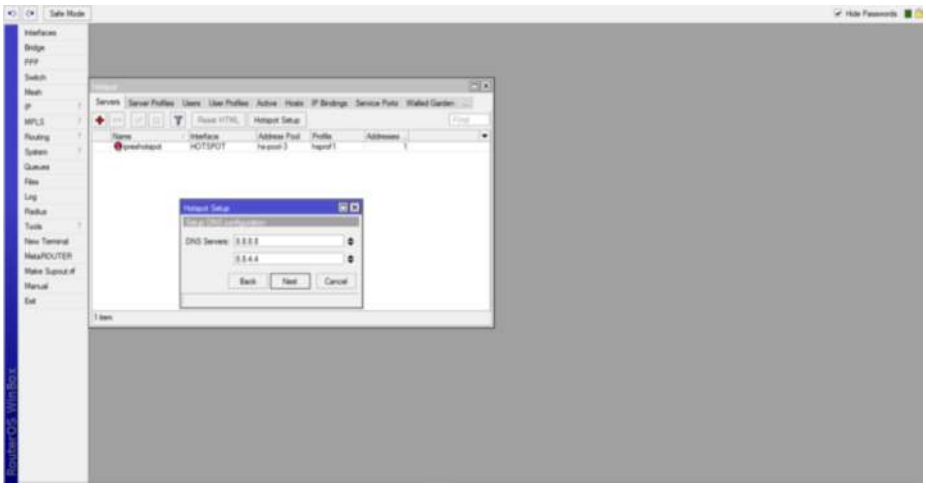


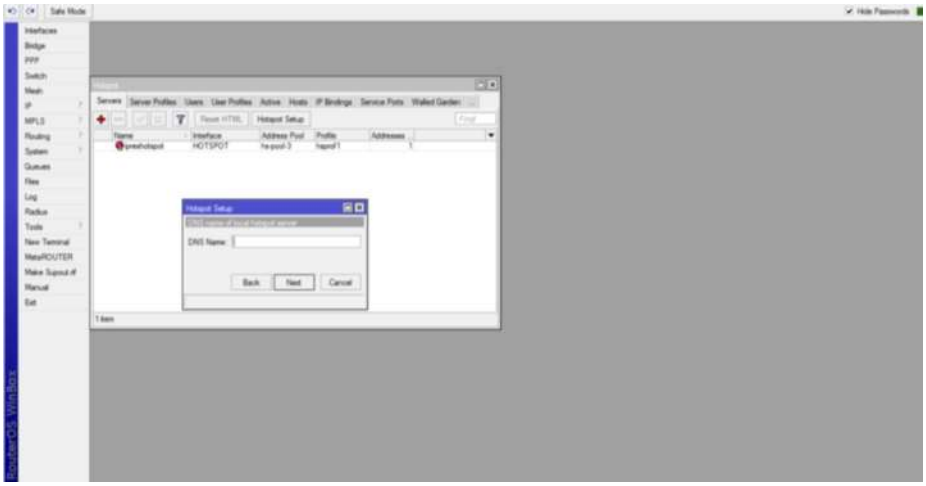




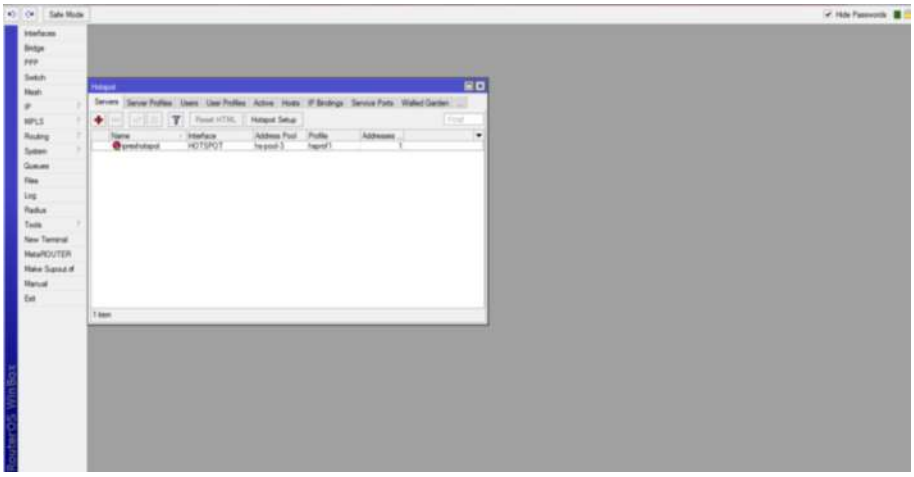


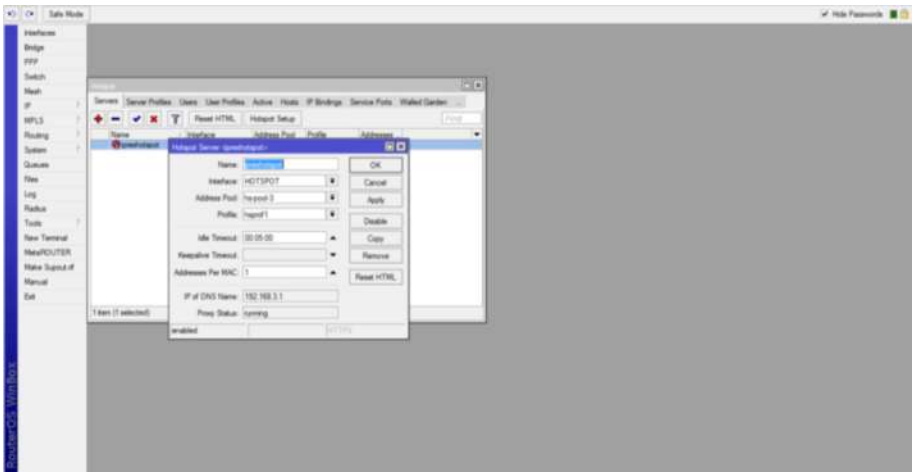




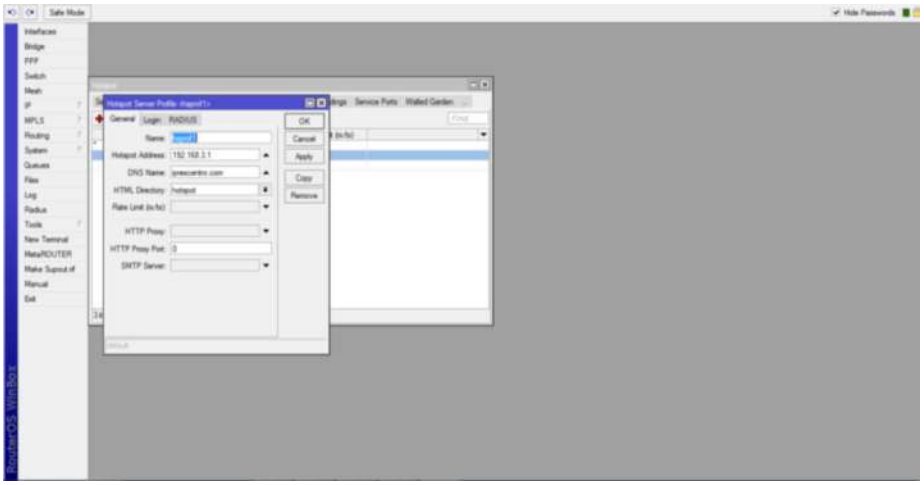


Terminada la configuración del asistente se obtiene:

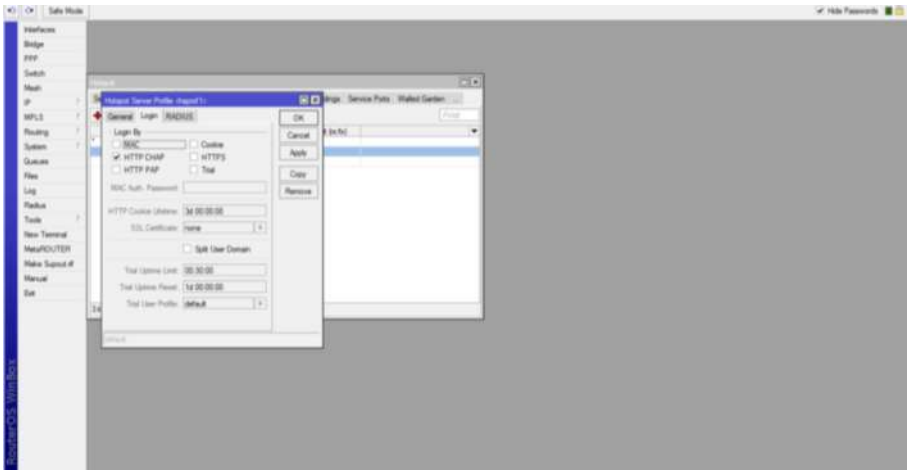




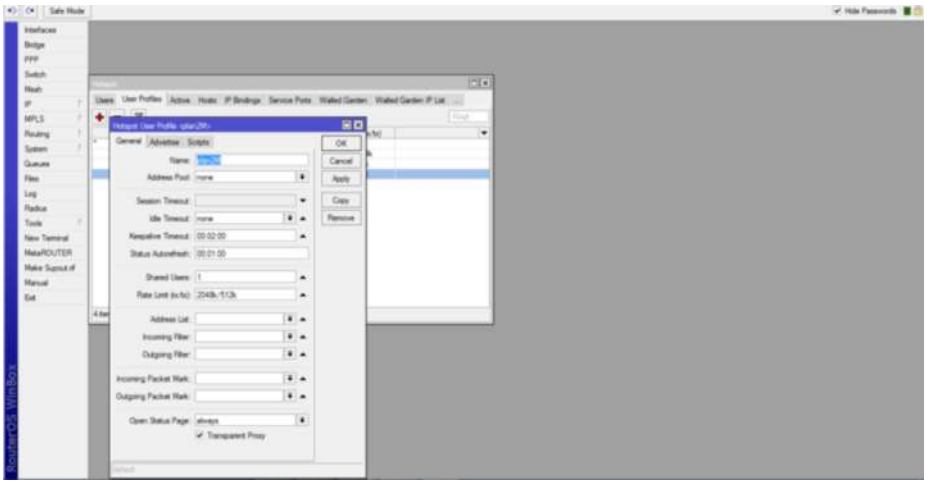
Se procede a crear perfiles para el servidor de portal cautivo



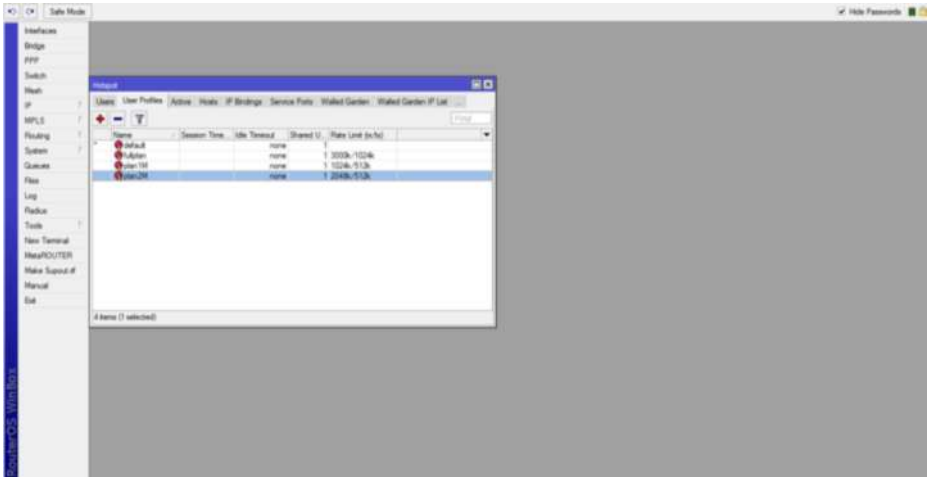
Para el acceso de usuario se habilita únicamente la opción HTTP CHAP para evitar que los datos queden guardados en los dispositivos clientes.



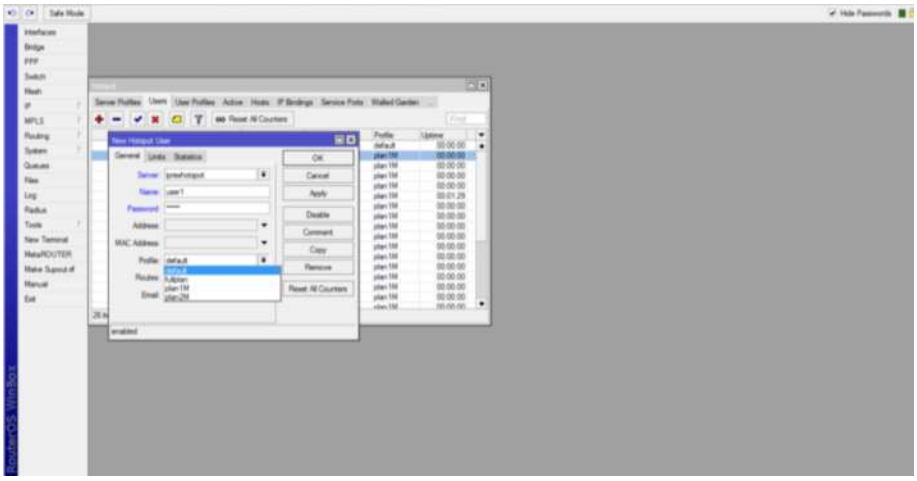
Configuración de perfil de usuario es muy importante ya que en este apartado se configura el ancho de banda de subida y bajada para un plan específico que se va a brindar a los clientes.



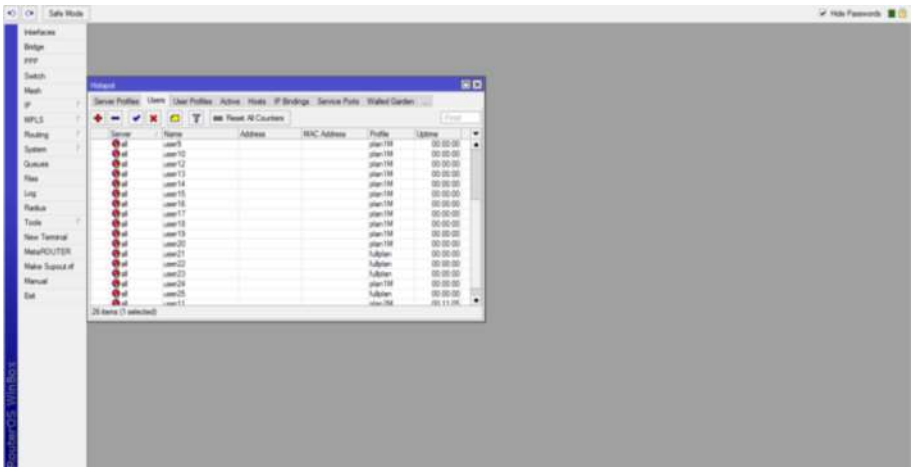
Se configura de acuerdo a los requerimientos de la institución.



Creados los planes de servicio de internet se procede a crear a los usuarios con su ID y respectiva password de acceso



Se asigna el plan 1 MB que consiste en 1024 Kb de bajada y 512 Kb de subida de datos a los usuarios y el plan 2 MB que consiste en 2048 Kb de bajada y 512 Kb de bajada de datos para la sección administrativa de la institución los cuales tienen habilitados todos los servicios que ofrece Mikrotik.

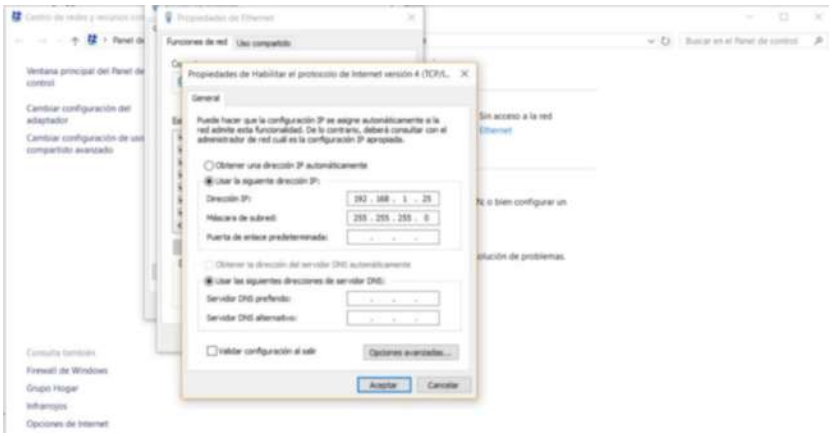


Terminada la configuración del router Mikrotik y el portal cautivo se puede elaborar una copia de seguridad para lo cual se selecciona la pestaña Files y después la opción backup se crea un archivo de respaldo el cual se copia y se guarda en una memoria flash.

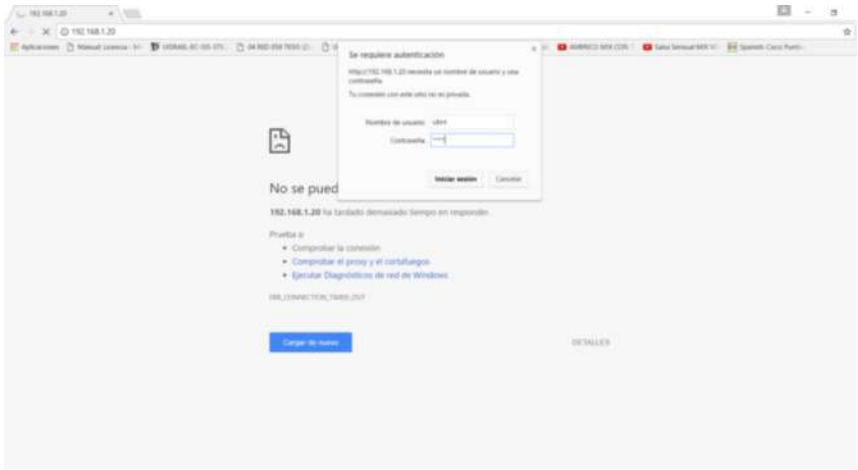
ANEXO B

Configuración de antena Loco Nanostation M2

1.- Asignación de ip fija al computador para poder ingresar a la configuración de la antena.

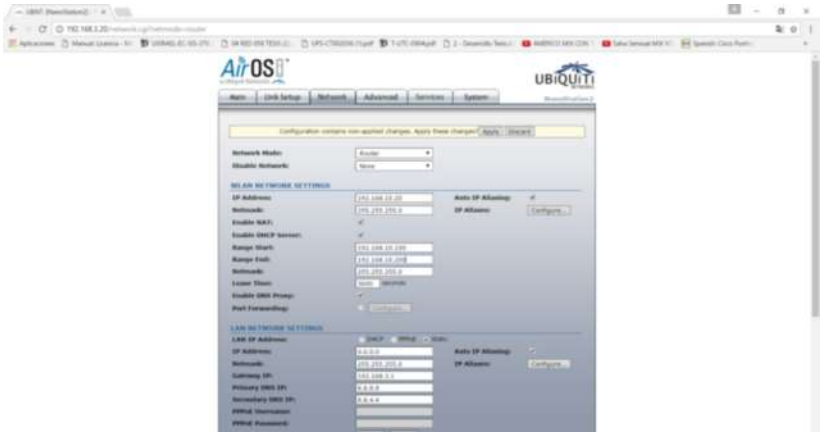


2.- Ingreso a un navegador de internet con la dirección 192.168.1.20 e ingresar nombre de usuario y contraseña.



3.- Configurar la antena como Access Point y configurar sin seguridad inalámbrica para que los usuarios tengan acceso a la red.

4.-Configurar Network y colocar en la opción Router lo cual permite que la antena pueda enviar la información de manera correcta hacia los usuarios.



5.- Por último, colocar el Gateway del router de donde sale la información.