UNIVERSIDAD AUTONOMA DE BAJA CALIFORNIA

Facultad de Contaduría y Administración

Facultad de Ciencias Químicas e Ingeniería

Maestría en Tecnologías de la Información y Comunicación

Implementación de la tecnología WPA2 - Enterprise para la administración y seguridad de la red inalámbrica de la FCQI

TESIS

PARA OBTENER EL GRADO DE:

MAESTRO EN TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN

Presenta:

LUIS ALBERTO SAMANIEGO TAMAYO

Bajo la dirección de:

M.C. Carlos Francisco Álvarez Salgado

TIJUANA, BAJA CALIFORNIA, MÉXICO MAYO 2014

Índice

Índice de Figuras

Capitulo I. Introducción

Antecedentes

En los últimos años las tecnologías de red de alta velocidad y el desarrollo de muchas aplicaciones han cambiado de forma dramática cada vez que se acercan más a problemas de gran escala. Estas oportunidades que nos brinda la tecnología han dado lugar a la posibilidad de utilizar recursos geográficamente distribuidos como un único recurso de información, mientras el aumento de las oportunidades de compartir recursos ha evolucionado por la gran necesidad de enviar y recibir información.

Hoy en día estamos ante una novedosa forma de comunicación en un entorno globalizado debido al desarrollo de internet. Por ello, se ha hecho indispensable el aumento de la infraestructura tecnológica dentro de las empresas, tanto en la red convencional como en la red inalámbrica.

Una red de área local por radiofrecuencia o WLAN (Wireless Local Area Network – Red Inalámbrica de Área Local) puede definirse como una red local que utiliza tecnología de comunicación inalámbrica para enlazar los equipos conectados a la red, en lugar de los distintos cables que se utiliza en las LAN (Local Area Network – Red de Área Local) convencionales cableadas, o se puede definir de la siguiente manera: "Cuando no existe una conexión física entre las terminales". De igual manera una WLAN es un sistema de comunicación de datos flexible implementado como una extensión o una alternativa de una LAN cableada dentro de un edificio o campus universitario.

Las redes inalámbricas de área local, debido a sus múltiples aplicaciones y la facilidad que ofrecen para acceder a ellas, cobran cada vez una mayor importancia, en especial aquellas orientadas a usuarios móviles. En particular, las redes inalámbricas de área local se adaptan rápidamente como una

alternativa eficiente y confiable para todo tipo de organizaciones e instituciones académicas.

Cabe mencionar que son indudables los beneficios que estas innovaciones traen, principalmente para las organizaciones a nivel de competitividad y rentabilidad, para aumentar el rendimiento del manejo de la información haciéndola más accesible, no obstante, también se han convertido en un elemento de riesgo, debido a que se reportan en las redes de información situaciones de acceso no autorizado, modificación o eliminación de archivos confidenciales, caída inesperada e inexplicable de los servicios de red y de los servidores.

En la mayoría de los casos relacionados a estas fallas de seguridad, son ocasionadas por personas expertas en el manejo de las tecnologías de la información, que hacen uso de sus habilidades y conocimientos para infiltrarse a través de las redes informáticas, estas personas son identificadas a nivel mundial con denominaciones como *Hackers y Crackers*. Por otro lado, este tipo de fallas de seguridad también pueden ser causadas por las mismas personas encargadas de establecer dichas medidas de seguridad en la red de la organización, las cuales debido a algún descuido técnico en la red puedan ocasionar que esta tenga un mal comportamiento, por lo tanto, queda vulnerable a algún ataque.

También, las mismas tecnologías de la información y comunicaciones, debido a la rapidez con que son desarrolladas e introducidas al mercado o la complejidad de sus configuraciones, presenta ciertas vulnerabilidades que ofrecen una puerta de acceso a los intrusos.

Ante esta situación se hace necesario analizar los niveles de seguridad implementados en empresas de tecnología para apoyar el diseño y organización de mecanismos de seguridad que ayuden a mitigar los riesgos y las vulnerabilidades tecnológicas.

Las empresas no le dan la importancia debida a que dicha infraestructura está en peligro por las vulnerabilidades que presenta, por lo que es muy necesario implementar una configuración de control de acceso a la red que permita proteger la información de posibles ataques de personas ajenas a ella mediante suplantación de identidades falsas, de esta manera burlan el acceso a la red de la organización, lo cual podría provocar pérdidas financieras o espionaje corporativo. Para evitarlo se cuenta con estándares, protocolos y equipos que permiten construir soluciones de seguridad robustas.

El problema de la autenticación en redes inalámbricas de área local basadas en infraestructura, se suele resolver mediante servidores de autenticación o entidades, certificaciones ubicadas en el sistema de distribución, para lo cual se utilizan protocolos tales como el IEEE 802.1X. Aunque este protocolo no fue originalmente concebido para las redes inalámbricas, se ajusta muy bien a las necesidades de esta tecnología inalámbrica basada en las infraestructuras de un sistema de distribución, y en general a toda la red IEEE 802.X.

La gran mayoría de las organizaciones que utilizan una red de computadoras de acceso inalámbrico, cuentan con algún protocolo de seguridad para acceder a la red. Hoy en día, el protocolo de seguridad más común utilizado es el WPA2, el cual no es lo suficientemente robusto para proteger el acceso a internet a personas ajenas a esta organización. Este tipo de protocolo de seguridad es utilizado por la mayoría de las instituciones educativas, tal es el caso de la Facultad de Ciencias Químicas e Ingeniería (FCQI) de la Universidad Autónoma de Baja California (UABC).

La UABC nació formalmente el 28 de febrero de 1957, gracias a la promulgación de su ley orgánica, como respuesta a la labor que se desarrollaba mediante un grupo de profesionistas, empresarios, intelectuales y estudiantes en la entidad.

El 18 de febrero de 1974 es fundada la Escuela de Ciencias Químicas en el Campus Tijuana de la Universidad y durante 9 años se ofreció el programa de Químico. En el año de 1983 se aumentó la oferta educativa, donde se ofreció la carrera de Químico Industrial y la de Ingeniero Químico. En 1984, se estableció el programa de Maestría en Biofarmacia, y se cambió por esta razón de Escuela a la categoría de Facultad de Ciencias Químicas. En 1986 se estableció el programa de Químico Farmacobiólogo y cinco años más tarde la oferta educativa nuevamente crece y se diversifica, para dar inicio a las carreras de Ingeniero en Computación e Ingeniero en Electrónica en 1991. En ese mismo año, se modifica el plan de estudios del programa de posgrado, convirtiéndose en el primer programa que adopta la flexibilización curricular en donde se ofrecieron tres áreas terminales: Ecotoxicología, Síntesis Orgánica y Biofarmacia.

En 2002, la oferta educativa nuevamente crece, estableciéndose el programa de Ingeniero Industrial. Un año después el posgrado se da inicio al programa de Maestría y Doctorado en Ciencias e Ingeniería, ofrecido como programa institucional tanto en la Facultad de Ingeniería en el campus Ensenada como en Mexicali.

En 1974, la población estudiantil de la Escuela de Ciencias Químicas era de 14 alumnos. En la actualidad, la población estudiantil es de 2333 alumnos en los programas de licenciatura y 90 en el posgrado. La población estudiantil es atendida por una planta de 74 profesores de tiempo completo, 6 de medio tiempo y 58 de asignatura, lo que hace un total de 138 profesores. Las principales líneas de investigación son la de salud y la de medio ambiente, pero también existen otras líneas tales como: desarrollo tecnológico, fisicoquímica de materiales, control automático, telemática, sistemas electrónicos de comunicación y optimización de procesos. (UABC)

Planteamiento del problema

Durante hace ya varios años, la Facultad de Ciencias Químicas e Ingenierías cuenta con servicios de red inalámbrica, de los cuales, alumnos y maestros tienen acceso a estos servicios. La facultad de Ciencias Químicas e Ingeniarías, cuentan con diferentes puntos de acceso a la red inalámbrica en los diferentes edificios. Uno de los puntos que hace que esta red sea poco accesible, es que, ya que cuenta con diferentes puntos de acceso (AP's), cada uno de ellos utiliza contraseñas diferentes, lo cual, hace un tanto complicada la accesibilidad a la red inalámbrica para todos aquellos usuarios que necesitan mayor movilidad dentro de la facultad. Además, cada determinado tiempo se vuelven a cambiar las contraseñas para los accesos a la red, y es un tanto complicado para alumnos y maestros solicitar las claves de acceso o en el caso del administrador de la red, proveerlas.

Para la actualización de la red inalámbrica, se busca crear un control de acceso para los usuarios, como por ejemplo, el diseño e implementación de una red WLAN con sistema de control de acceso mediante servidores "AAA" (Authentication, Authorization, Account – Autenticación, Autorización, Conteo) en donde cada usuario tendrá asignado uno o más dispositivos para tener acceso a la red inalámbrica. Estos usuarios podrán acceder a los equipos de la red de acuerdo a su nivel de autorización. Esto permitirá tener un registro en una base de datos de los usuarios que entran y salen de la red, en donde se le garantiza al administrador de la red un mejor control sobre los usuarios.

Justificación

La implementación de la tecnología WPA2 – Enterprise permitirá a las personas autorizadas o registradas en la red un acceso seguro dentro de ella y proporciona una administración adecuada de los usuarios que ingresan a la misma, ya que gracias a la creación de usuarios para el acceso a la red, se genera el acceso sin importar en que Punto de Acceso se intenten conectar, de esta manera, garantiza un acceso adecuado para los usuarios en cualquier parte que se encuentren dentro del rango de la red inalámbrica de la facultad.

Además, el administrador de la red tendrá una adecuada administración sobre los usuarios que ingresen a la misma, gracias a que podrá clasificarlos y permitirles o no el acceso. El acceso a la red dependerá del tipo de dispositivo que intenten ingresar, ya que si el sistema de seguridad no reconoce el dispositivo por el cual el alumno o maestro desee ingresar, no le permitirá el acceso aunque proporcione un usuario y contraseña.

Objetivo General.

Implementar la Tecnología WPA2-Enterprise, para obtener una adecuada administración y seguridad de acceso a la red inalámbrica, así como agilizar el proceso de autenticación a los usuarios de la FCQI.

Objetivos específicos.

- Identificar las necesidades para la administración y seguridad de la red inalámbrica.
- Investigación y configuración de la herramienta para la implementación de la tecnología WPA2 - Enterprise.
- Instalación del servidor RADIUS.
- Configuración de AP's.
- Generar el certificado
- Creación de cuentas de usuarios temporales para la realización de pruebas.

Limitaciones de Estudio

Las limitaciones del presente estudio estarán determinadas por los siguientes aspectos:

Limitaciones de recursos financieros. En un determinado caso en el que se necesite equipo nuevo o especializado para realizar una tarea o proceso, se necesitaría apoyo financiero por parte de la facultad de Ciencias Químicas e Ingeniería.

Limitaciones de Información y de población. Esto abarca la complejidad para obtener la información necesaria referente al problema de investigación por parte del personal que elabora dentro de la facultad de Ciencias Químicas e Ingeniería, al igual de la disponibilidad tanto del personal como del alumnado de dicha facultad.

Capitulo II. Marco Teórico

Redes y Características

Una red es un conjunto de dispositivos (a menudo denominados nodos) conectados por enlaces de un medio físico. Un nodo puede ser una computadora, una impresora o cualquier dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red. (Forouzan, 2002)

Existen diversas formas en las que podrían organizar las redes, y la mayoría de las redes se encuentran en un constante estado de transmisión y desarrollo. Si la red de computadoras tiene solo una ubicación central o computadora anfitriona que realiza todas las tareas de procesamiento de datos desde uno o más lugares distantes o remotos, se trata de una red centralizada.

Si hay computadoras distantes, las cuales, procesan trabajos para usuarios finales, y también una computadora ubicada en un sitio central, entonces podemos tener los inicios de una red distribuida. Una red distribuida puede ser centralizada o dispersa; pero una red en la que no se realiza procesamiento distribuido solo puede ser centralizada, ya que todas las tareas de procesamiento de datos se efectúan en una computadora ubicada en un sitio central.

Una red de punto a punto es sin duda la más sencilla, ya que tiene solo una computadora, una línea de comunicaciones y otra terminal en el otro extremo del cable. Esta fue la primera forma de red existente.

Las redes multipuntos constituyeron originalmente una extensión directa de sistemas punto a punto en que en vez de haber una sola estación remota existen múltiples estaciones distantes. (Madron, 1992)

La transmisión de datos por medio de una red cableada se envía a través de un medio sólido, como por ejemplo un par trenzado de cobre, un cable coaxial o una fibra óptica.

Las características y la calidad de la transmisión están determinadas tanto por el tipo de señal, como por las características del medio. En el caso de los medios guiados, el medio, en sí mismo, es lo que más limitaciones imponen a la transmisión.

En los medios no guiados, las características de transmisión están más determinadas por el ancho de banda de la señal emitida por la antena que por el propio medio. Una propiedad fundamental de las señales transmitidas mediante antenas es la direccionalidad. En general, la señal desde la antena se emite y se propaga en todas las direcciones. A frecuencias más altas, es posible concentrar la señal en un haz direccional. (Stallings, Comunicaciones y Redes de Computadoras 7ma. Edicion, 2004)

Una Red local se denomina inalámbrica cuando los medios de unión entre las estaciones o dispositivos no son por medio de claves (Raya Cabrera & Raya Pérez, 2008).

Tecnologías Inalámbricas de Transmisión de Datos

Actualmente, existen cuatro técnicas para su utilización en redes inalámbricas que son: infrarrojos, radio en *UHF*, microondas y laser.

Todas las redes por infrarrojos usan un rayo de luz para transportar los datos entre dispositivos. Estos sistemas necesitan generar señales muy fuertes, debido a que las señales de trasmisión dispersas son susceptibles a la luz.

Una red basada en equipos de radio en *UHF* necesita para su instalación la obtención de una licencia administrativa. No se ve interrumpida por cuerpos opacos gracias a su cualidad de difracción.

Las microondas son ondas electromagnéticas cuyas frecuencias se encuentran dentro del espectro de las súper-altas frecuencias, utilizándose para las redes inalámbricas la banda ancha de los 18 – 19 Ghz.

Esta tecnología para redes inalámbricas es útil para conexiones punto a punto con visibilidad directa y se utiliza, fundamentalmente, para interconectar segmentos distantes de redes locales convencionales, en donde llegan a cubrir distancias de hasta 1000 metros. (Cabrera & Gonzalez, 2006)

Existen multitud de redes, cada una de ellas con unas características específicas que las hacen diferentes del resto. Podemos clasificar a las redes en diferentes tipos, según sus diferentes criterios:

- Redes dedicadas: Una red dedicada es aquella en la que sus líneas de comunicación son diseñadas e instaladas por el usuario o administrador, o bien, alquiladas a las compañías de comunicaciones que ofrecen este tipo de servicios, y siempre para su uso exclusivo.
- Redes compartidas: las redes compartidas son aquellas en las que las líneas de comunicación soportan información de diferentes usuarios. Se trata de todos los casos de redes de servicio público ofertadas por las compañías de telecomunicaciones bajo cuotas de alquiler en función de la utilización realizada o bajo tarifas por tiempo ilimitado. (Molina Robles, 2006)

Redes Inalámbricas

A lo largo de los años, las *redes inalámbricas de área local (Wireless Local Area Network – WLAN)* han evolucionado rápidamente y han hecho más fácil la conectividad entre diferentes dispositivos. No obstante, la seguridad en las redes inalámbricas ha sido un factor muy importante y delicado, ya que los datos viajan a través del espacio libre, y estos pueden ser interceptados por otros usuarios.

Un problema de seguridad significativo para los sistemas en red es el acceso hostil, o al menos no autorizado, por parte de usuarios o software. La entrada ilegal de usuarios puede adoptar la forma de identificación no autorizada a una maquina o, en el caso de un usuario no autorizado, la adquisición de privilegios o la realización de acciones más allá de las que han sido autorizadas.

Todos estos ataques tienen relación con la seguridad de la red porque, efectivamente, la entrada al sistema puede lograrse por medio de una red.

Una de las amenazas a la seguridad más extendidas es el intruso (la otra es el virus), generalmente conocido como *Hacker o Cracker.* Existen tres clases de intrusos:

- Suplantador: un individuo que no está autorizado a usar la computadora y que penetra hasta los controles de acceso del sistema para obtener los beneficios de un usuario legítimo.
- Usuario fraudulento: Un usuario legítimo que accede a datos, programas o recursos a los que no está autorizado.
- Usuario Clandestino: Un individuo que toma el control de supervisión del sistema y lo usa para evadir los controles de auditoria y acceso o para suprimir información. (Stallings,

Fundamentos de seguridad en redes aplicaciones y estandares 2da.edicion, 2004)

Para proteger la información enviada mediante medios de comunicación inalámbrica, normalmente, se utilizan métodos de encriptación y autentificación (Mejía Nogales, Vidal Beltrán, & López Bonilla, 2006).

La autenticación es el proceso en que se determina que un individuo o, mejor aún, un dispositivo, es quien dice ser. El concepto de autenticación no está limitado a Wi-Fi o a las redes generales, por ejemplo:

- En un comercial de televisión, Hugo el loco, el dueño de una cadena de tiendas de aparatos electrónicos, proporciona una venta anual donde los precios son muy bajos. Al final del comercial, Hugo comenta a los televidentes: si mencionan "Hugo el loco me envió", entonces recibirá un descuento adicional especial.

El cifrado es la práctica de cambiar la información de forma que esté tan cerca como sea posible de ser imposible de leer son la información necesaria para descifrarla. Esta forma puede ser una clave secreta o código. Es una forma que se usa para generar un flujo de datos cifrados basado en una clave de cifrado. Estas claves se pueden medir en términos de longitud; en general, mientras más grande sea la clave, será más complicado y robusto el código. (Neil & Ron)

Estándar IEEE 802.11

En el año de 1997, surge el estándar IEEE (Institute of Electrical and Electronics Engineers) 802.11 con el fin de regular el diseño e implementación

de redes de comunicación, especialmente en las redes inalámbricas (Ocando & Ugas, 2005). De este estándar está basado el método de autenticación WPA2.

Arquitectura de Autenticación 802.1X

Esta arquitectura está compuesta por tres partes principales: Un solicitante, Un autenticador y un servidor de Autenticación. Cuando se aplica a la red inalámbrica, el solicitante reside en los dispositivos de cliente y el punto de acceso sirve como el autenticador. El solicitante, normalmente es un fragmento pequeño de software que se ubica en el sistema operativo o el controlador de dispositivos que proporciona el fabricante del adaptador del cliente. El punto de acceso actúa como el portero de la LAN, el cual, permite que el dispositivo del cliente obtenga el acceso a la LAN sólo después que el cliente ha sido autenticado.

El proceso de autenticación de 802.1X cuando se aplica a las WLAN funciona de la manera siguiente:

1. El cliente obtiene el acceso al medio inalámbrico a través de CSMA/CA y crea una asociación con un punto de acceso.
2. El punto de acceso acepta la solicitud pero coloca al cliente en una "área de espera" sin estar autenticado. Para el cliente sin autenticación, el puerto virtual, es decir, la puerta de enlace, hacia la LAN está bloqueada. El punto de acceso envía una solicitud de identificación al cliente.
3. El cliente responde con una identificación que tiene el nombre de usuario o un identificador especifico que no es secreto. Al recibir la respuesta de identificación, el punto de acceso reenvía esta respuesta a través del enlace cableado al servidor RADIUS.
4. El servidor RADIUS busca el ID del usuario en una base de datos.

5. Una vez que el ID del usuario ha sido identificado por el servidor RADIUS, comienza un proceso de interrogación al cliente, en donde el AP es el intermediario entre el servidor y el cliente. El cliente responde a estas preguntas hasta que llega el momento que el servidor RADIUS determina que el cliente es realmente legítimo.

Una vez que el cliente ha sido autenticado en la red a través del punto de acceso y el servidor RADIUS, y la red ha sido autenticada en el cliente, se abre el puerto virtual en el punto de acceso y el cliente puede comenzar a acceder a la red inalámbrica y cableada (Neil & Ron).

Descripción del protocolo RADIUS

Radius es un servicio o *daemon* que se ejecuta en una de las múltiples plataformas que permite (Unix, GNU/Linux, Windows, Solaris…) y que permanece de forma pasiva a la escucha de solicitudes de autenticación hasta que estas se producen. Para ello utiliza el protocolo UDP (y no TCP o SCTP que permitiría mayor control y seguridad en el transporte) y permanece a la escucha de los puestos 1812 o 1645 para la autenticación y 1813 o 1646 para el conteo. En un principio se utilizaban los puertos 1645 y 1646 para Radius, pero tras la publicación de la RFC 2864 se utilizan por acuerdo 1812 y 1813 debido a que el 1645 estaba siendo utilizado por otro servicio denominado "datametrics". Algunos servidores como FreeRadius utilizan el puerto UDP 1814 para la escucha de respuestas proxy Radius de otros servidores, pero esto no está contemplado en ningún RFC, y está en conflicto con el puerto utilizado por TDP Suite (Telocator Data Protocolo), (Garcia-Morán, Hansen, & Varón, 2009) protocolo de comunicaciones para localizadores o buscapersonas.

Radius está basado en un modelo de cliente – servidor, ya que Radius escucha y espera de forma pasiva las solicitudes de sus clientes o NAS, a las que responderá de forma inmediata. En este modelo de cliente es el responsable

del envío y de la correcta recepción de las solicitudes de acceso, y es el servidor Radius el responsable de verificar las credenciales del usuario y de ser correctas, de enviar al NAS los parámetros de conexión necesarios para prestar el servicio. (Garcia-Morán, Hansen, & Varón, 2009)

Tecnología WPA2 y el Protocolo RADIUS

El método de seguridad inalámbrica WPA2 *(Wi-Fi Protected Access 2),* deshabilita el SSID *(Service Set Identifier)* para evitar la conexión a usuarios no autorizados, el cual, filtra la dirección MAC *(Media Access Control)* para permitir el acceso solo a usuarios conocidos (P. Sarmiento, G. Guerrero, & Rey Argote, 2008), además de poder agregar métodos de encriptación y autentificación, lo que lo hace uno de los métodos más seguros.

El método de seguridad WPA2 Enterprise, conocido como "Clave Pre-Compartida" (P. Sarmiento, G. Guerrero, & Rey Argote, 2008), utiliza el protocolo RADIUS (*Remote Authentification Dial-In User Service*), que surgió inicialmente como una solución para la administración para el control de acceso a los usuarios que soportan su conexión mediante enlaces seriales y módems, el cual, facilita el control y supervisión de la seguridad, la autorización, la auditoria, verificación de nombres de usuario y contraseñas, así como una detallada configuración sobre el servicio que se pretende dar al usuario (Chaparro Bargas & Mejia Fajardo, 2006).

WPA2 – Enterprise (La combinación de la tecnología WPA2 y el Protocolo RADIUS)

El Modo Enterprise, permite a los usuarios conectarse a la red Wi-Fi con un nombre de usuario y contraseña y/o certificado digital. Ambos tipos de credenciales pueden ser cambiados en el servidor. Este modo, no solo ofrece a

los usuario una clave de cifrado dinámico y único, sino que también, impide los espionajes de usuario a usuario (Geier, 2011).

Cittix –Wifi es una herramienta desarrollada para el control de acceso a las redes inalámbricas. Es una herramienta de código abierto (open source) derivado de una de las distribuciones más utilizadas de Linux llamada "Debian", liberada bajo los términos de la licencia GPLv2 (Inc.).

Ciitix – Wifi trabaja en conjunto con FreeRADIUS, DaloRADIUS y OpenSSL para proporcionar un acceso a la red seguro y confiable, además de un entrono amigable y adecuado para una mejor administración de la red inalámbrica para un instituto u organización.

Ubuntu es un sistema operativo de Linux, el cual tiene mucho tiempo en el mercado. Este sistema operativo desde sus inicios ha contado con mucho soporte por usuarios alrededor del mundo, ayudando a que nuevos usuarios se integren a este poderoso sistema operativo ya sea solo para probar el sistema o para desarrollar aplicaciones y herramientas que los usuarios necesitan.

Ubuntu 12.03 LTS tiene gran número de aplicaciones muy útiles y fáciles de utilizar, además de interfaces graficas que llaman mucho la atención de los usuarios que intentan cambiarse a este sistema operativo. Cuenta también, con un enorme repertorio de aplicaciones de última generación, compatibilidad con miles de dispositivos y aplicaciones, así como también, robustez en su sistema contra virus y otros tipos de software mal intencionados para dañar información.

FreeRADIUS es el servidor RADIUS más popular del mundo, el cual es utilizado por gran número de organizaciones e institutos alrededor del mundo (Radius).

DaloRADIUS es una plataforma web RADIUS avanzada, destinada a la gestión de puntos de acceso (AP). Cuenta con gestión de usuarios, informes

gráficos y lleva una contabilidad de los usuarios que utilizan la red. DaloRADIUS está escrito en PHP y JavaScript. También, utiliza una base de datos de capa de abstracción que significa que es compatible con muchos de los gestores de bases de datos, entre ellos el popular MySQL, PostgreSQL, SQLite, MSSQL y muchos otros (Tal).

OpenSSL es una herramienta de código abierto que surge a partir de la colaboración de diferentes miembros alrededor del mundo, para implementar el protocolo *Secure Socket Layer* (SSL v2 / v3) y mejorarlo (Engelschall). SSL es un protocolo desarrollado por Netscape utilizado para transmitir información privada vía internet. SSL utiliza un sistema criptográfico que usa dos tipos de llaves para encriptar los datos, una llave pública conocida por todos y una llave privada o secreta que solo conocerá el que recibirá la información.

Capitulo III. Metodología

La metodología utilizada está basada en una investigación aplicada para un caso práctico, en la cual, la FCQI será el lugar en donde se aplicará esta investigación. Debido a una falta de administración hacía los usuarios de la red, el administrador de la red solicitó herramientas para dichas tareas de administración. También, sugirió implementar una nueva tecnología de autenticación para la red inalámbrica de la facultad.

Para cumplir con los requerimientos solicitados por el administrador de la red, es de suma importancia llevar a cabo procedimientos debidamente estructurados, para ello, se seguirán los siguientes procedimientos:

1. Recopilación de la información
2. Investigación de la herramienta
3. Desarrollo de prototipo
4. Implementación

Recopilación de la información

Hoy en día existen diferentes herramientas que ayudan a la administración y seguridad de una red. En los últimos años, muchas de las empresas gastan millones de dólares en dispositivos y software de protección para proteger sus redes inalámbricas contra intrusos, espías y robos de información, entre otros.

Muchas de las herramientas que se encargan de la seguridad en las redes inalámbricas son sumamente costosas, es por eso que se buscará una herramienta gratuita que ofrezca una serie de servicios para ayudar a la administración de las redes inalámbricas, en este caso, para la facultad de ciencias químicas e ingenierías.

Para poder seleccionar una herramienta que cumpla con las necesidades de seguridad y administración de la red inalámbrica de la facultad de ciencias químicas e ingenierías, es necesario realizar esfuerzos de investigación adecuados, que nos permitan una correcta y eficiente definición de requerimientos, especificaciones y funcionalidades de una red inalámbrica.

Para obtener la información adecuada respecto a las necesidades de la red, es necesario solicitar la información a la persona encargada de la administración, es decir, definir completamente la necesidad que existe para el manejo de la red, así como también, los tipos de mejoras, herramientas y necesidades que actualmente existen.

Investigación de la herramienta

Una vez obtenida la información sobre los requerimientos necesarios para un adecuado manejo y administración de la red inalámbrica, se llevará a cabo una investigación sobre algunas herramientas que ofrecen los servicios de administración de la red, que cuenten con la opción de la tecnología WPA2 – Enterprise, ya que esta tecnología de autenticación es la más segura actualmente.

Se buscará adaptar alguna herramienta de autenticación que sea de bajo costo o gratuita, pero que cumpla con las medidas de seguridad necesarias, para poder implementar la tecnología de autenticación WPA2 – Enterprise.

Desarrollo de Prototipo

Después de haber realizado el estudio de las herramientas de administración gratuitas más importantes, que más se adecuen a las necesidades de los usuarios y del administrador de la red, se llevará a cabo el desarrollo de un prototipo de red, para realizar las pruebas necesarias, de esta manera, se obtendrá la herramienta con un óptimo desempeño en el manejo y administración, y que cumpla con la mayoría de las necesidades que se requieren.

Para este prototipo de red, se requerirá de por lo menos dos equipos de cómputo y un dispositivo de red (AP), en donde una computadora se utilizará para simular un servidor que se comunicara con el AP, el cual, funcionará como un intermediario entre el usuario y el servidor.

Implementación

Cuando las pruebas realizadas en el prototipo de la herramienta seleccionada hayan terminado, se aplicará la misma arquitectura del prototipo en un edificio de la facultad de ciencias químicas e ingenierías, en donde se continuaran las pruebas pero en un ambiente real. Ya implementada la herramienta en un edificio y en base a los resultados obtenidos, los cuales se esperan ser positivos, se realizara la implementación en otro edificio y se continuará el monitoreo hasta cubrir por completo la facultad de ciencias químicas e ingenierías.

Una vez implementada, se llevará a cabo la administración y el monitoreo continuo, hasta determinar que han sido cumplidos los objetivos propuestos en la actualización de la tecnología de acceso a la red inalámbrica de la facultad de ciencias químicas e ingenierías.

En caso de que exista algún inconveniente durante la implementación de la tecnología WPA2 – Enterprise no visualizado durante el desarrollo del prototipo o mediante las pruebas realizadas durante el desarrollo, se volverán hacer las pruebas, esto es, se regresara el proyecto hasta la parte del desarrollo del prototipo, para asegurar que la herramienta funcione correctamente en la facultad de ciencias químicas e ingenierías.

Capitulo IV. Desarrollo

Instalación y configuración del sistema Ciitix Wi-Fi

Se comenzó utilizando una herramienta llamada Ciitix – WiFi, la cual, cumplía con algunas de las características necesarias (robustez en la seguridad, sistema basado en Linux, fácil de administrar, interfaz amigable) para implementarlo en el edificio 6I de la FCQI.

A continuación, se muestra la pantalla de inicio al arrancar el disco de instalación del sistema Ciitix – WiFi (Figura 1).

Figura 1. Pantalla de arranque de Cittix – WiFi.

Una vez instalado el sistema, nos muestra la siguiente pantalla del menú GRUB como se muestra en la Figura 2.

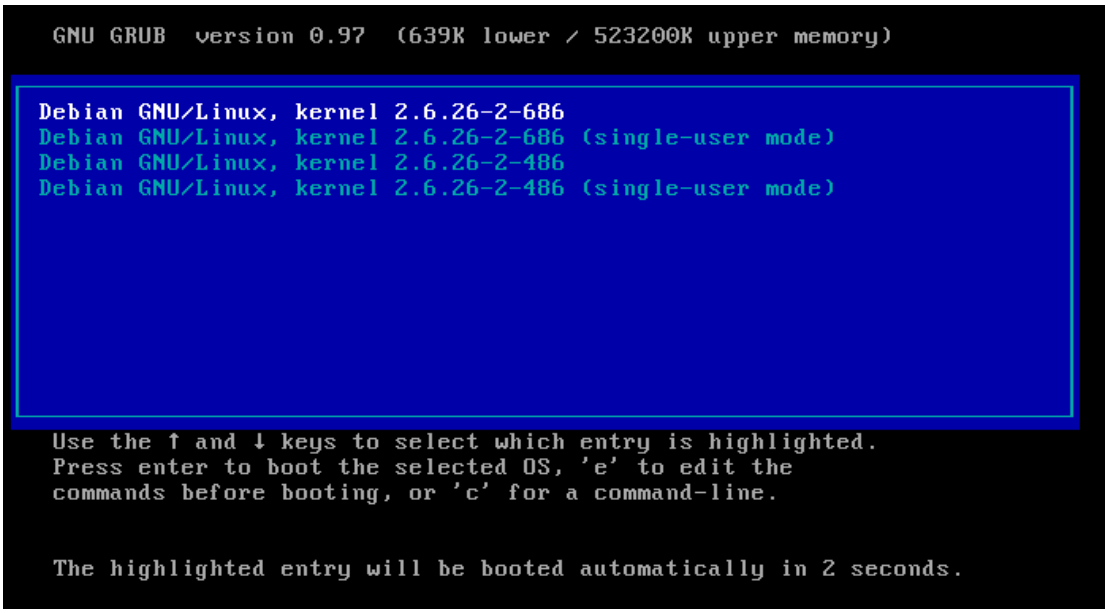

Figura 2. Pantalla de arranque del sistema GRUB.

Al iniciar el sistema, se muestra la ventana de inicio de sesión para el sistema (Figura 3), en donde se ingresa el usuario y la contraseña para acceder.

Figura 3. Pantalla de inicio de sesión de Ciitix – WiFi.

Después, muestra el escritorio del sistema de Ciitix – WiFi, en donde para empezar a configurar el servidor RADIUS se hace clic derecho en cualquier parte del escritorio y se selecciona la opción www Browser como indica la figura 4.

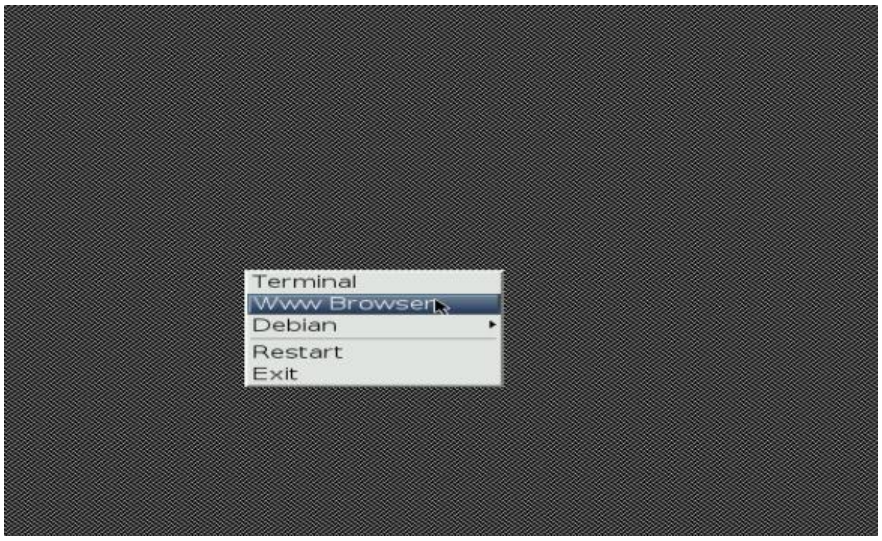

Figura 4. Seleccionar Www Browser para abrir un navegador.

Una vez realizado lo anterior, abrirá un navegador (Figura 5), en donde se configura el servidor RADIUS, para ello, se necesita ingresar un nombre de usuario y contraseña. El usuario es *administrator* y la contraseña es *radius,* estos datos los trae el sistema por *default*. Ya ingresados los datos en la pantalla se hace clic en el botón LOGIN para continuar.

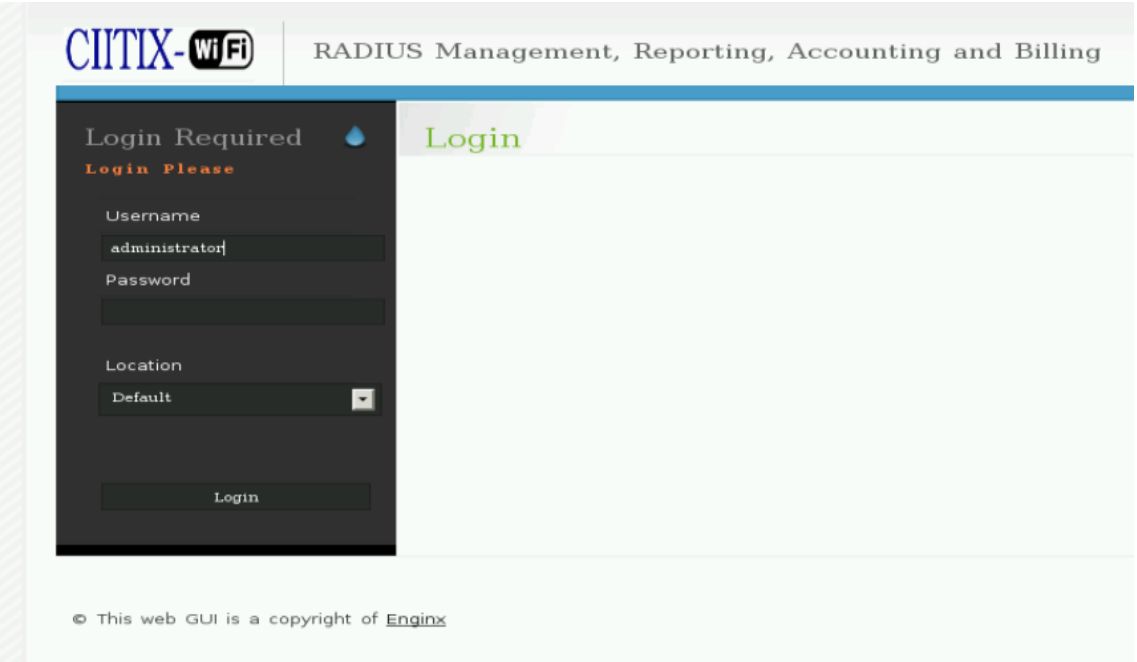

Figura 5. Pantalla de inicio de sesión para el servidor RADIUS.

Después, muestra las opciones como lo indica la Figura 6. A partir de aquí, se puede empezar la configuración del servidor RADIUS.

Figura 6. Pantalla de configuración del servidor RADIUS.

A partir de este punto, se procede a configurar el AP modelo WRT54G LINKSYS v5 con el que el servido RADIUS tendrá contacto, para esto, se podrá acceder al dispositivo mediante conexión alámbrica o inalámbrica.

Para acceder al dispositivo es necesario utilizar un navegador web e ingresar la dirección IP por default del AP, en este caso, la dirección IP es "192.168.1.1", el dispositivo solicitará un nombre de usuario y contraseña, se ingresan los datos y aparecerá una pantalla como lo muestra la Figura 7 a continuación.

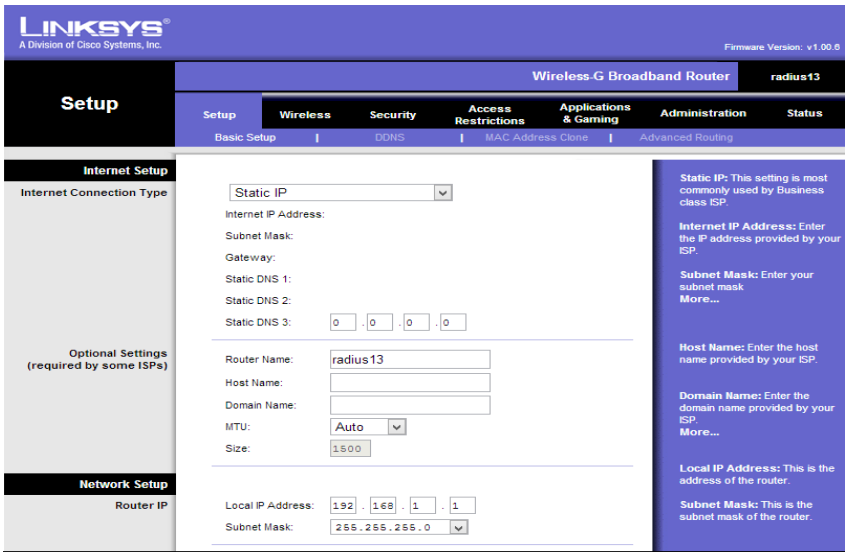

Figura 7. Pantalla inicial del AP.

Después, se ingresa a la pestaña de configuración de la conexión inalámbrica (Wireless) y posteriormente a la opción "Wireless Security" como se muestra en la Figura 8.

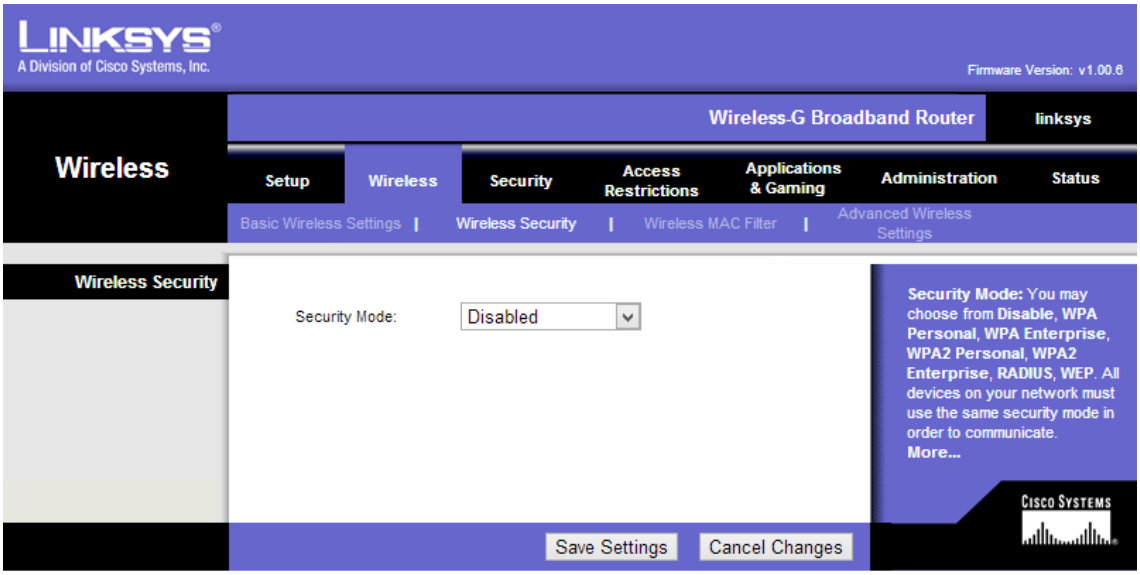

Figura 8. Pantalla de configuración de la seguridad inalámbrica.

A continuación, se da clic a la lista desplegable que muestra en la Figura anterior (Figura 30) y se selecciona la opción WPA2 – Enterprise dejando la configuración por default. Una vez realizados los pasos anteriores, podemos asignarle la dirección IP del servidor RADIUS con el cual se comunicará, así

como el puerto y una llave de intercambio, en este caso, la configuración quedará como se muestra en la Figura 9 y se guardan los cambios dando clic en el botón "*save settings*".

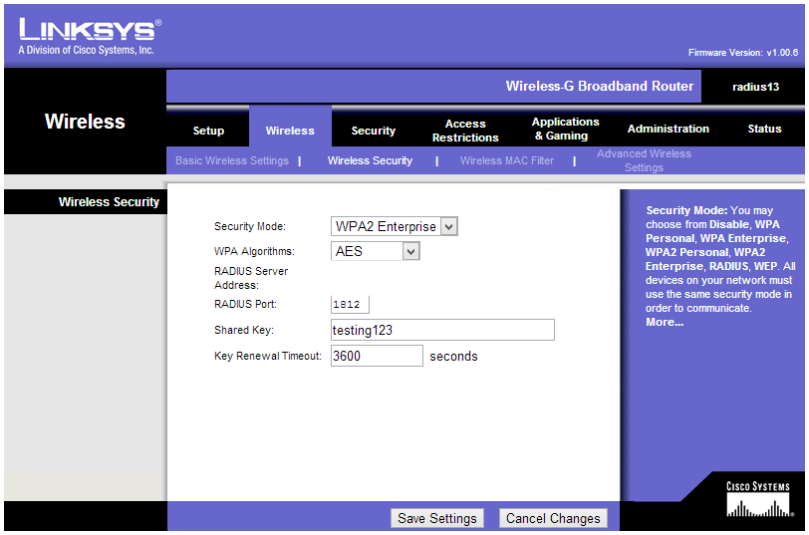

Figura 9. Pantalla de configuración, utilizando la seguridad WPA2 Enterprise.

Ya realizado lo anterior, es necesario mantener seguro el acceso al AP, para ello, se ingresa a la pestaña de administración (*Administration*) y se ingresa una contraseña en los campos "*password*" y "*Re-enter to confirm*" (Figura 10). Es recomendable crear una contraseña que contenga letras minúsculas y mayúsculas, así como símbolos y números para una robusta clave de acceso. Después, se guardan los cambios realizados dando clic al botón "*save settings*".

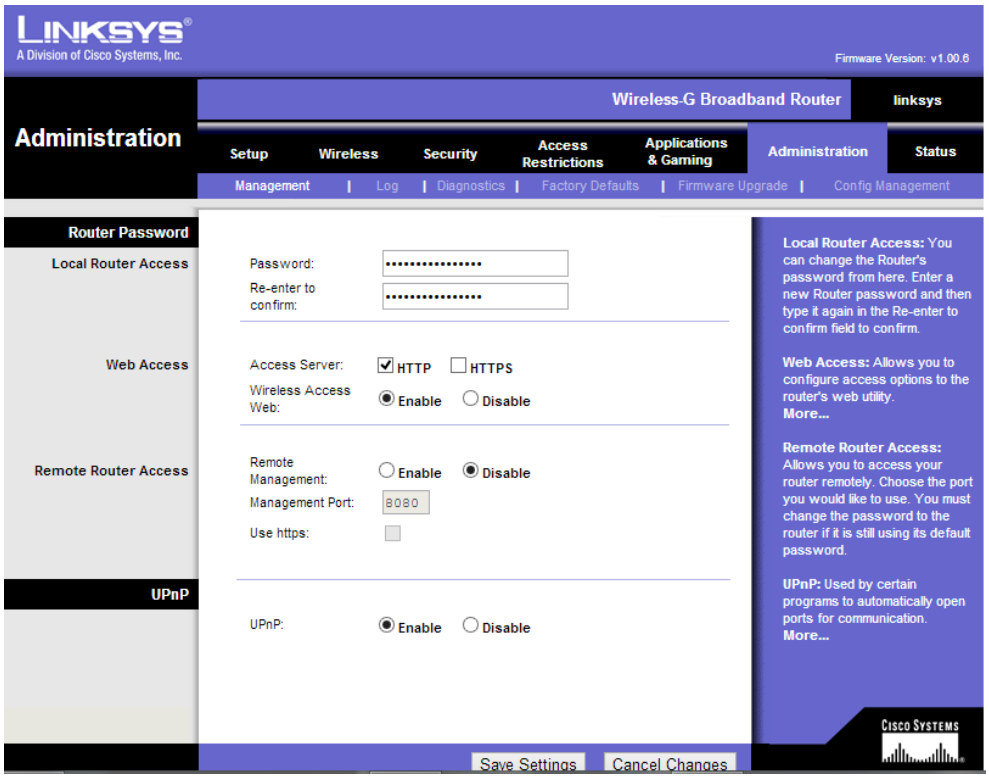

Figura 10. Pantalla de administración, agregando una contraseña de acceso.

Una vez concluido el proceso de configuración del AP, se dirige al sistema Ciitix, se abre una terminal y se teclea en la terminal la siguiente línea de código: "ifconfig eth0 192.168.1.254 netmask 255.255.255.0" coma se muestra en la Figura 11. Esto es para modificar y asignar la IP "192.168.1.254 que se usó como referencia en el AP en la Figura 10.

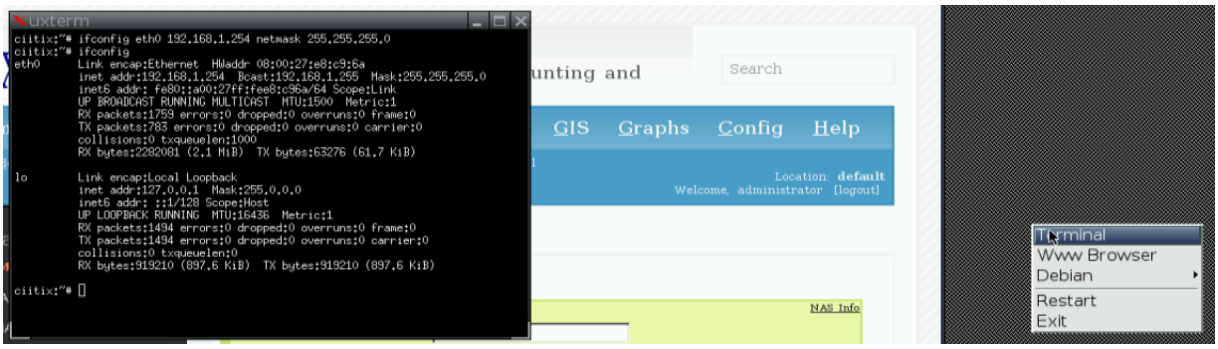

Figura 11. Pantalla en donde se accede a la terminar y se actualiza la IP.

Ya realizado lo anterior, se procede a agregar el dispositivo AP en el servidor. Primero se accede a la pestaña "*Management*", después se hace clic en la sub-pestaña "*NAS*" y por ultimo seleccionamos la opción que se encuentra abajo llamada "*New NAS*". A continuación, la Figura 12, muestra la configuración que se debe utilizar.

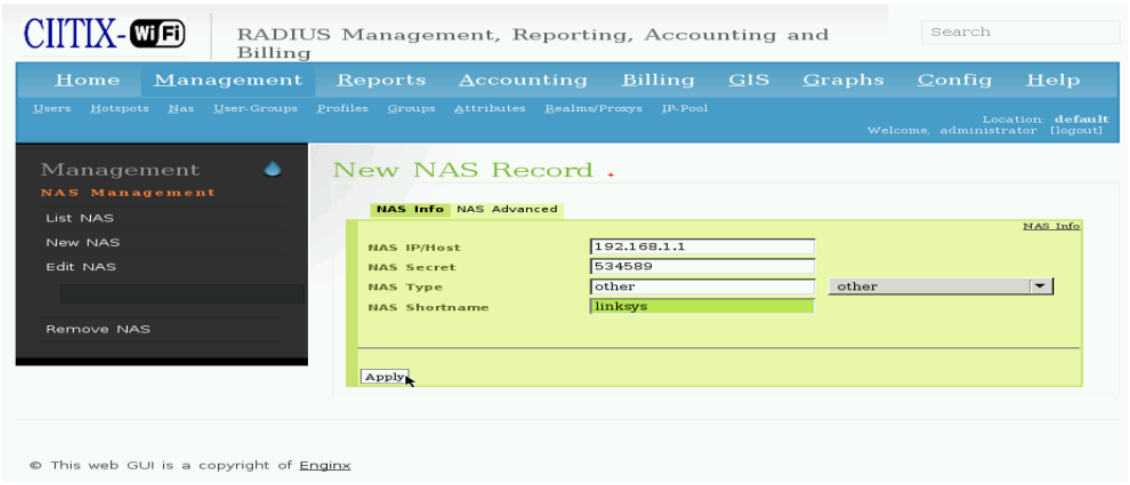

Figura 12. Pantalla donde se agrega un dispositivo AP.

Después de haber realizado todo lo anterior, se guardan los cambios realizados dando clic en el botón llamado "*Apply*".

Cuando los cambios estén hechos, es tiempo de agregar los usuarios que ingresaran a la red, solo ellos tendrán acceso a la red porque están dados de alta en el servidor. Para ello en la misma pestaña "*Management*" se le da clic a la sub-pestaña "*Users*", una vez dentro, se le da clic a la opción "*New User*" y se agregan los datos del usuario que se quiera registrar, después en la opción "*PassWord Type*" se selecciona la opción "*Cleartext-Password*", terminado esto, se da clic al botón "*Apply*" para guardar los cambios. En la Figura 13 se muestra un ejemplo de cómo se ingresan los datos.

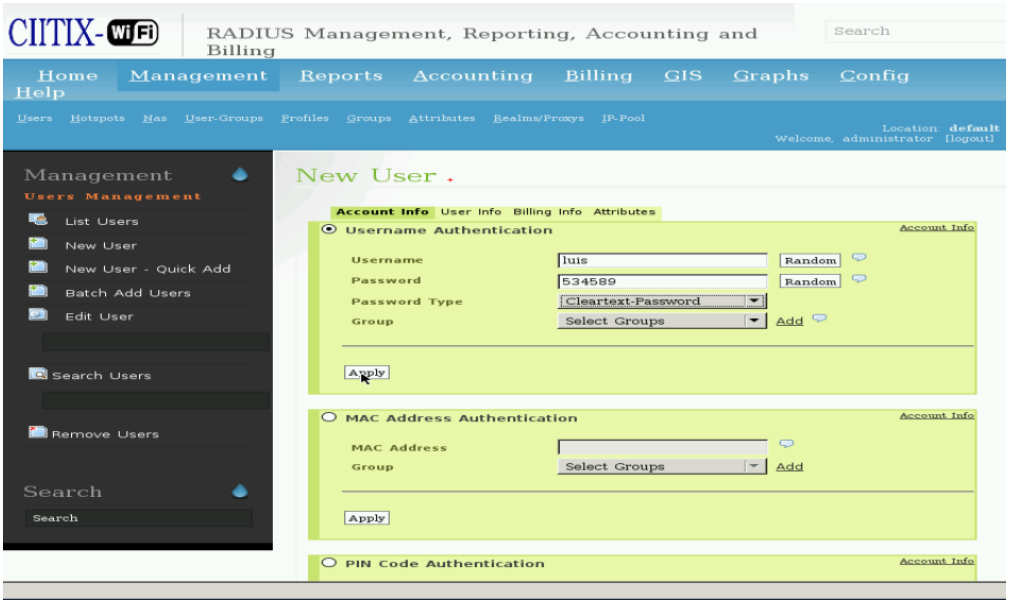

Figura 13. Pantalla donde se agregan nuevos usuarios.

Una vez concluido lo anterior, es necesario reiniciar el servidor Radius, esto se hace abriendo una terminal y tecleando la siguiente línea de código "sudo /etc/init.d/freeradius restart". La Figura 14, muestra un ejemplo de cómo se hará.

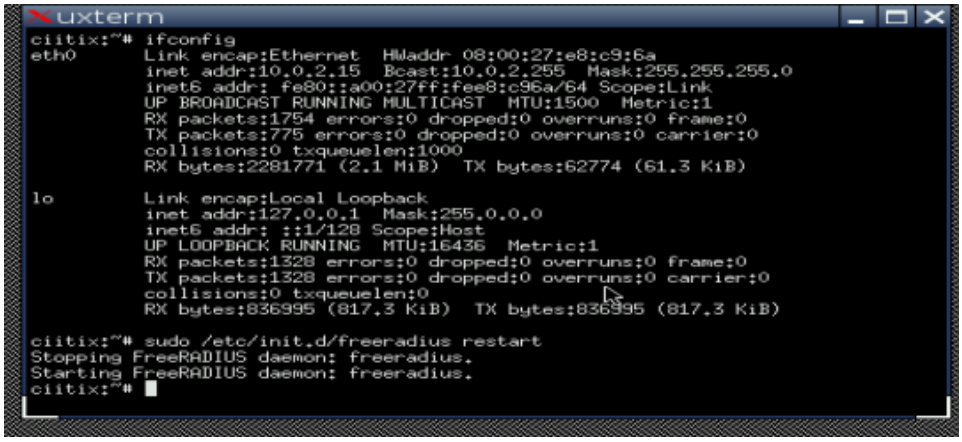

Figura 14. Pantalla de reinicio del servidor radius.

Después, es necesario copiar e instalar el certificado a los clientes de esta red, en este caso, a los dispositivos (computadoras) por medio del cual, los usuarios se conectaran a la red inalámbrica. Dichos certificados se encuentran en la siguiente ruta "/etc/freeradius/certs/client-certificates" dentro de ese directorio se encuentran los archivos "ca.der" y "server.p12". Para copiarlos será necesario algún dispositivo de almacenamiento (USB).

Para realizar dicha operación, es necesario abrir una terminal, una vez dentro de la terminal, se teclea la siguiente línea de código: “mount /dev/sda1 /mnt”. Esto le indicara al sistema que se montara el dispositivo “sda1” que se encuentra en la carpeta “/dev”, en la carpeta “/mnt”. Por lo tanto, para acceder al dispositivo se teclea la siguiente línea de código: “cd /mnt”. A continuación, la Figura 15 muestra un ejemplo. \

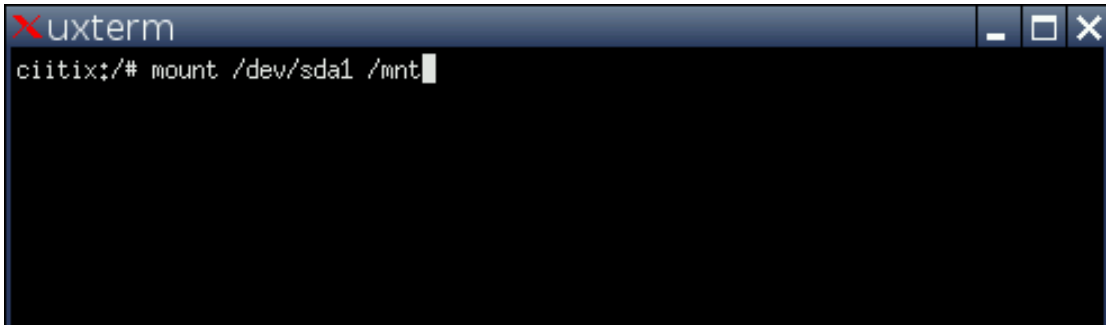

Figura 15. Montando el dispositivo USB en el sistema.

Una vez montado el dispositivo en el sistema, se procede a copiar los archivos anteriormente mencionados “ca.der” y “server.p12”. Para ello, existen formas distintas de copiar los archivos a la unidad de almacenamiento USB, en este caso se utilizara la siguiente:

1. Dirigirse a la ruta donde se encuentran los archivos con la siguiente línea de código: “cd /etc/freeradius/certs/client-certificates”.
2. Copiar los archivos a la unidad con la siguiente línea de código: “cp *.* /dev/sda1”.
3. Una vez copiados los archivos, se desmonta la unidad de almacenamiento con el siguiente código: “umount /mnt”.

A continuación la Figura 16, muestra un ejemplo de ello.

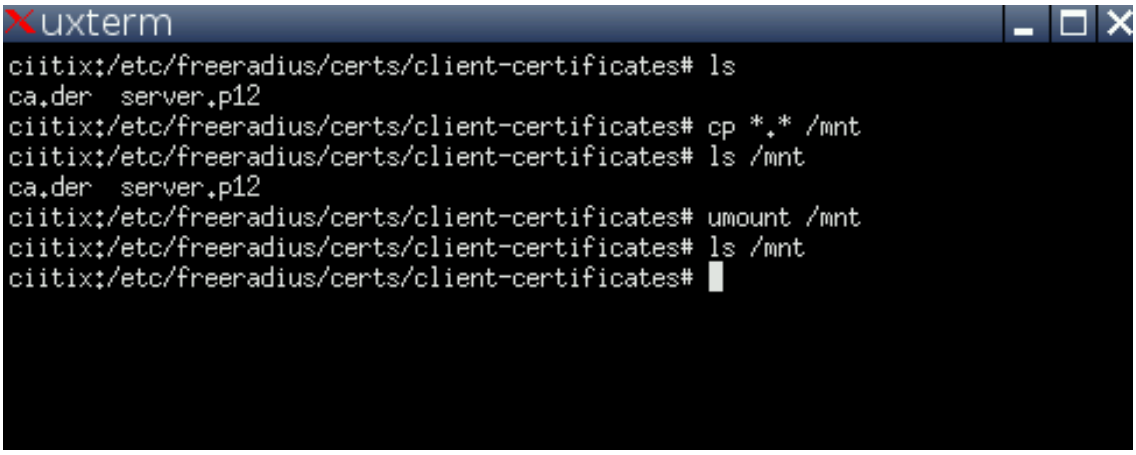

Figura 16. Muestra los pasos para copiar los archivos a la unidad USB. El comando "ls" muestra los archivos que se encuentran en la carpeta.

Instalación de los certificados en el cliente

Después, se extrae la unidad de almacenamiento y se inserta a la computadora del cliente, la cual, estará certificada para ingresar a la red. Los certificados deben ser instalados asegurándose de cumplir los siguientes pasos:

1. Insertamos la unidad de almacenamiento y se ejecuta el archivo "ca.der". una vez ejecutado, aparecerá la siguiente pantalla:

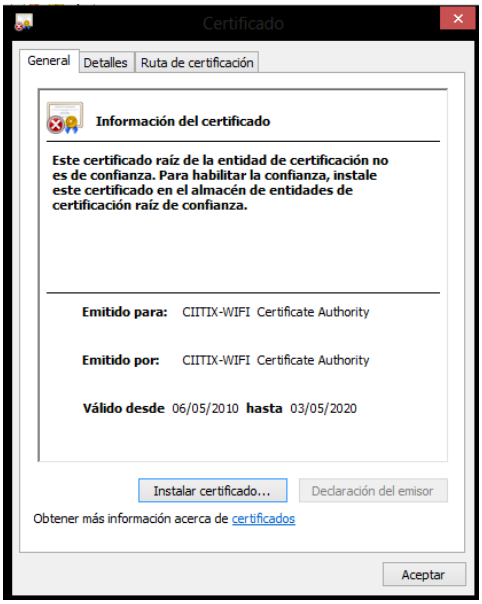

Figura 17. Pantalla del certificado.

2. Se hace clic en el botón “Instalar certificado”. Aparecerá una pantalla en donde indica para quien será instalado el certificado, en este caso, se instalará para el usuario actual y se le da clic al botón “Siguiente”.

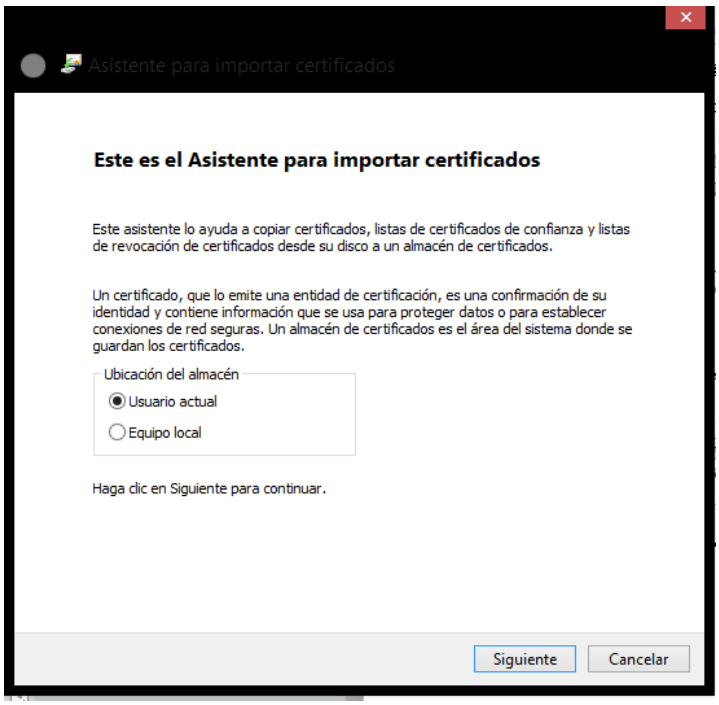

Figura 18. En este caso se selecciona “usuario actual”.

3. En la pantalla siguiente aparece donde se desea instalar el certificado, aquí se selecciona la segunda opción, se le da clic al botón “examinar” y por ultimo seleccionamos la carpeta “entidades de certificación raíz de confianza”, se le da clic al botón “aceptar” y luego clic al botón “siguiente”.

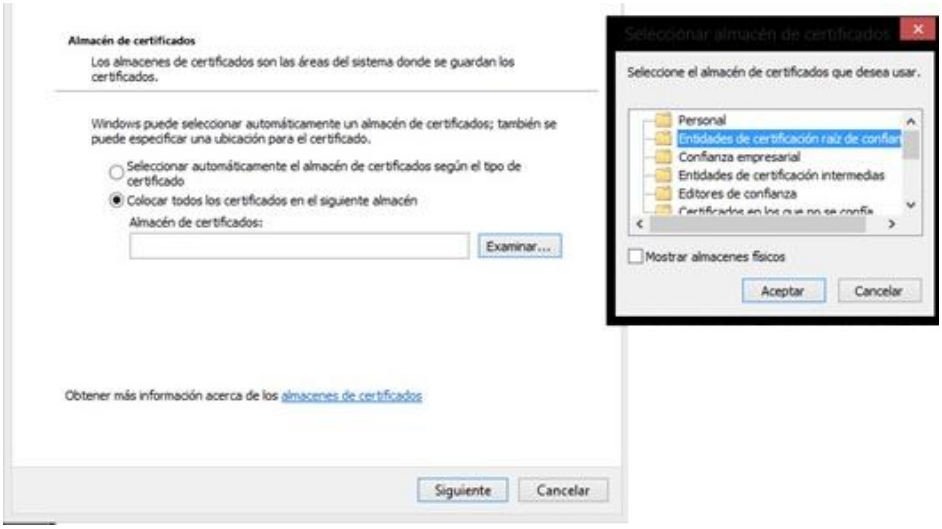

Figura 19. Ruta donde se instalará el certificado.

4. Después, aparecerá una pantalla de la finalización de la instalación, en donde se le da clic al botón "finalizar" para concluir con la instalación.

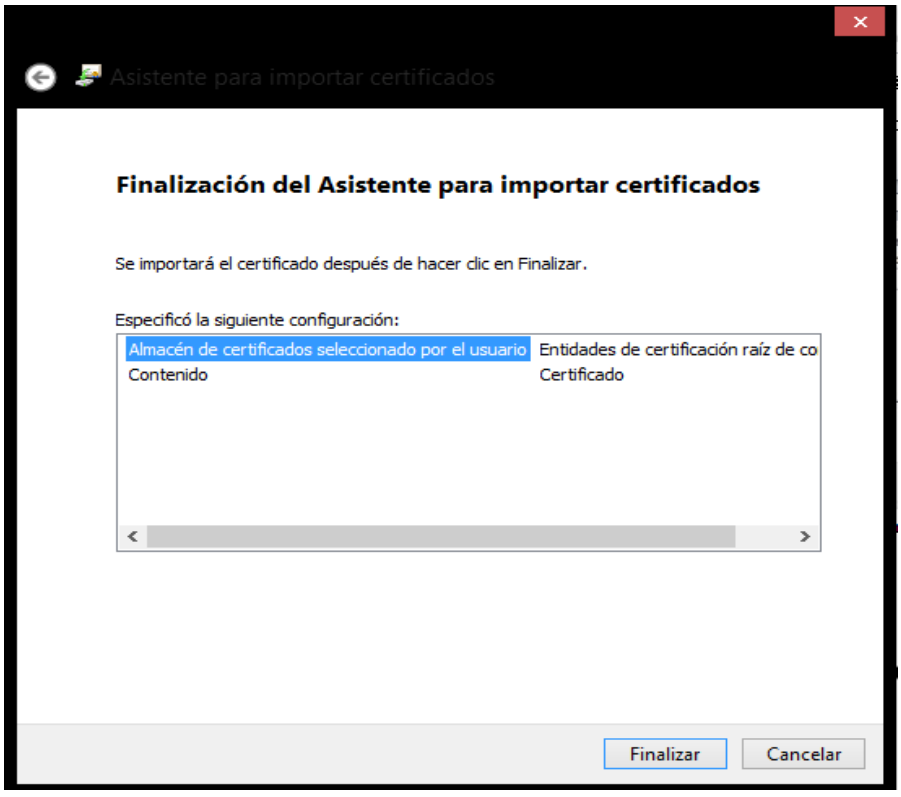

Figura 20. Pantalla de finalización de la instalación.

Una vez concluida la instalación del certificado, se procede a la instalación del archivo de intercambio "server.p12", para ello se deben de seguir los siguientes pasos:

1. En este paso se realizara lo mismo que el paso No. 2 visto anteriormente en la instalación del certificado.
2. Aquí , muestra una pantalla en donde pregunta sobre el archivo que se va a instalar, se deja la ruta por *default* y se continua dando clic al botón "siguiente" tal y como lo muestra la siguiente Figura:

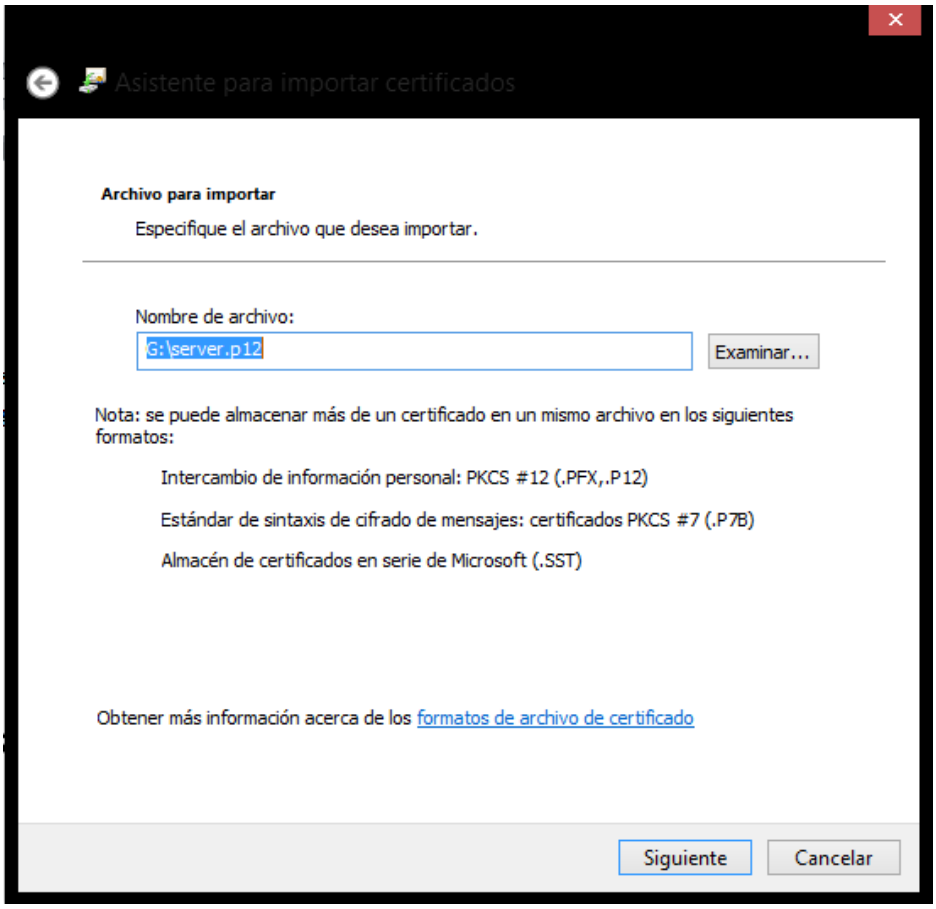

Figura 21. Pantalla de la ruta del archivo a importar.

3. A continuación, muestra una pantalla en donde solicita una contraseña para poder instalarse, se introduce la contraseña y se da clic al botón "siguiente". La Figura 21 da un ejemplo de ello.

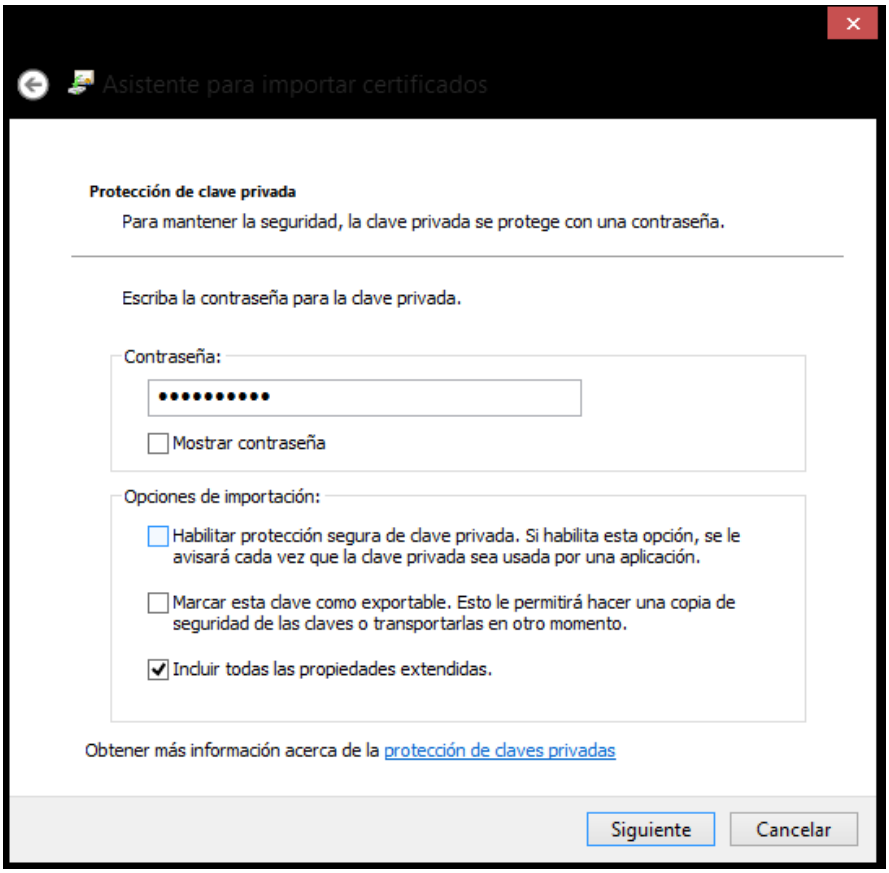

Figura 22. Pantalla de solicitud de contraseña para la instalación.

4. Aparecerá una pantalla en donde se siguen los mismos pasos vistos anteriormente en la instalación del certificado, paso No. 3.
5. Realizado lo anterior, concluimos la instalación dando clic en el botón finalizar.

Una vez instalado todo el sistema ciitix Wi-Fi y configurado, se comenzaron las pruebas para determinar si dicho sistema era el adecuado para la implementación de la tecnología WPA2 – Enterprise, el cual dio como resultado que era eficiente en tanto se utilice solamente esas herramientas, ya que al momento de intentar complementar el sistema con nuevas herramientas, el sistema no cumple con todas las librerías y dependencias necesarias para realizar dichas acciones.

Dado dicho problema se intentó agregar las direcciones para actualizar la distribución, agregando en el archivo "*source.list*" en la ruta "*/etc/apt/*" las siguientes direcciones de distribución:

```
deb http://http.us.debian.org/debian stable main contrib non-free
```

```
deb http://non-us.debian.org/debian-non-US stable/non-US main contrib non-free

deb http://security.debian.org stable/updates main contrib non-free
```

Una vez agregadas las direcciones, se guarda el archivo y dentro de una consola se ejecuta el comando "*apt-get update*", esto para actualizar las librerías del sistema y de esta manera tratar de instalar nuevas herramientas.

El resultado de dicha actualización fue que existían cientos de librerías con versiones un tanto antiguas y necesitaban muchas actualizaciones, además, muchas de las herramientas no serían compatibles debido a que ya eran obsoletas o habían sido remplazadas por otros archivos nuevos.

De esta manera, se determinó que el sistema no podía ser actualizado con nuevas herramientas en caso de necesitarlas por las personas encargadas de la administración de la red.

Dados los resultados anteriores, con el sistema Ciitix – WiFi, se dio a la tarea de implementar la tecnología WPA2 – Enterprise utilizando como base un sistema operativo Linux un tanto más reciente y estable, y que además, provee soporte hacia las aplicaciones que actualmente se están utilizando.

Ubuntu es un sistema operativo que a lo largo de los años ha sobresalido entre las diferentes distribuciones linux gracias su estilo tan simple de utilizarse, además de su interfaz gráfica intuitiva que favorece al usuario para el manejo de sus herramientas.

Además de la seguridad que ofrece este sistema operativo, Ubuntu cuenta con un soporte continuo en actualizaciones del sistema y herramientas, las cuales son de gran utilidad, haciendo de Ubuntu, un sistema muy completo, manteniendo a los usuarios actualizados al momento de instalar nuevas herramientas.

Para tener un ejemplo sencillo de como instalar el sistema operativo Ubuntu 12.10, véase la instalación del sistema operativo Ubuntu 12.10 en el apéndice A de este documento.

Instalación y configuración de las herramientas para la administración de la red inalámbrica

Con el sistema operativo Ubuntu instalado, se procede a la descarga de las herramientas para su instalación y configuración, en este caso, se hará uso de una terminal para realizar el proceso de descarga e instalación.

Primero se abre una terminal dando clic en el botón inicio de Ubuntu y a continuación, se teclea la palabra "terminal" y se da clic a la imagen con la pantalla negra. La figura 25 da un ejemplo de ello.

Figura 23. Proceso para abrir una terminal en Ubuntu.

A continuación, se abrirá una terminal, en donde se utiliza el comando "sudo su" para ingresar en la terminal como usuario root como lo muestra la Figura 26 a continuación.

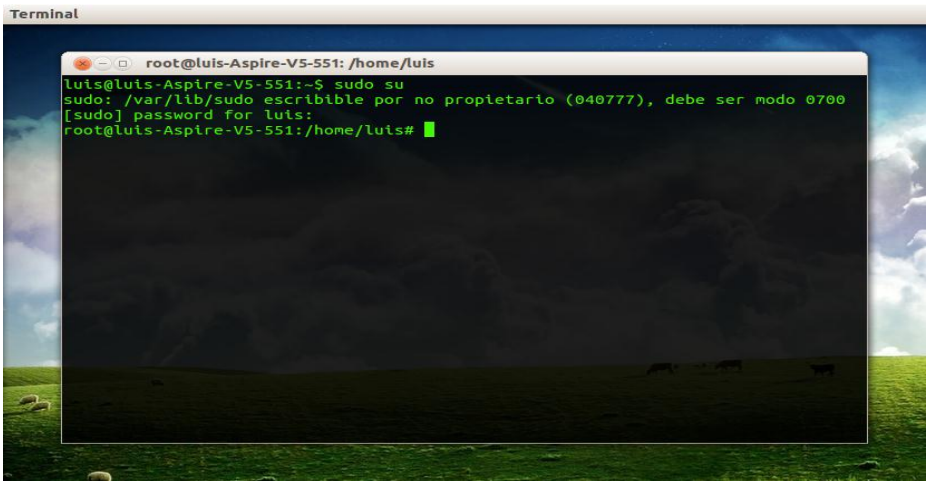

Figura 24. Ingresar como usuario root en la terminal.

Una vez iniciada la sesión como usuario root es momento de actualizar los repositorios de las cabeceras para el sistema mediante el comento “apt-get update”. Ya concluido el procedimiento, se procede a descargar e instalar freeradius junto con su paquetería mediante el comando “apt-get install freeradius freeradius mysql freeradius utils” tal y como lo muestra la Figura 27.

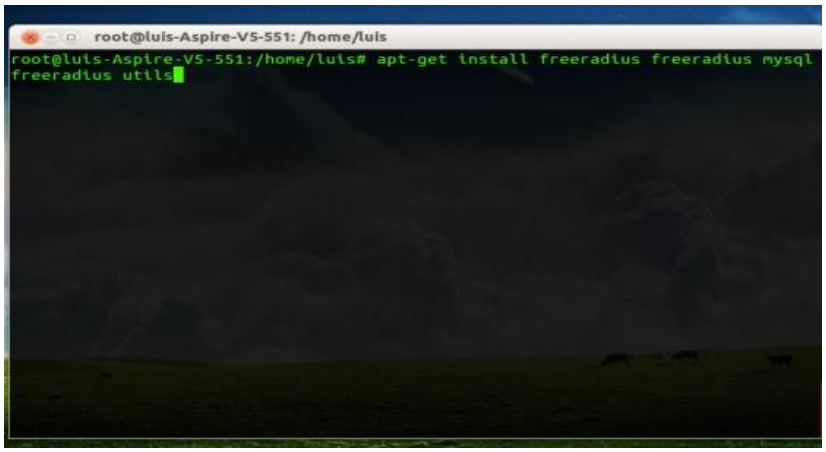

Figura 25. Comando de descarga e instalación para freeradius y su paquetería.

Cuando la herramienta haya terminado de descargarse, la terminal dará una alerta preguntando si se desea instalar la herramienta en donde se teclea la letra “S” y se da enter para proceder con la instalación.

Ya concluido el proceso de instalación de freeradius se continua con el proceso de configuración de la herramienta para que tenga contacto con la base de datos que se utilizara más adelante, para ello, editaremos el archivo “default” y el archivo “radius.conf”. En este caso, primeramente se edita el archivo default con el comando “nano /etc/freeradius/sites-enabled/default”, en este archivo se descomentarán las líneas “sql” de los apartados authorize y accounting.

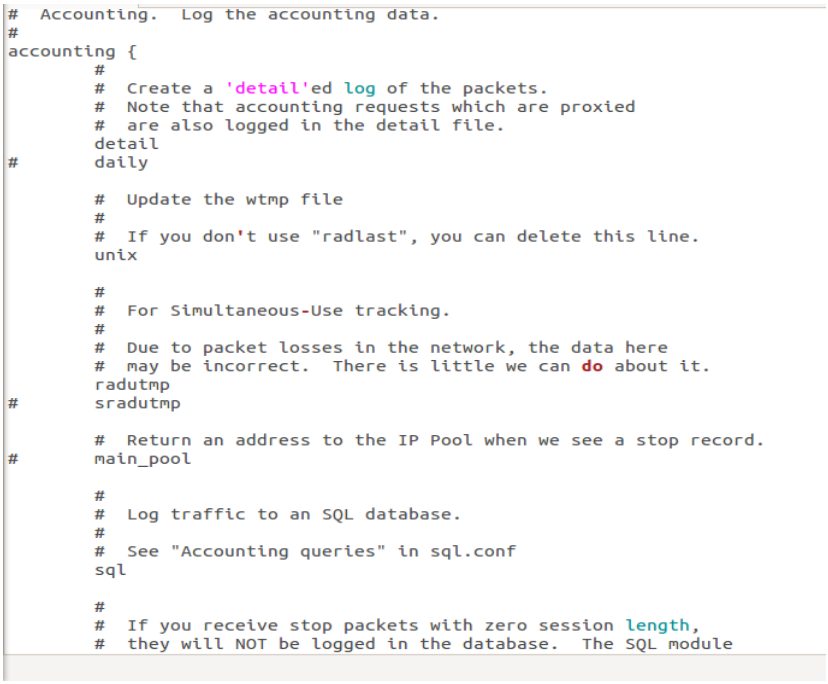

Figura 26. Se descomenta la línea sql del archivo default.

Después, se edita el archivo de configuración "radiusd.conf" mediante la siguiente línea de comando "nano /etc/freeradius/radiusd.conf", en donde se descomenta la línea "$INCLUDE sql.conf" tal y como se muestra en la Figura 29.

```
        $INCLUDE ${confdir}/modules/

        #  Extensible Authentication Protocol
        #
        #  For all EAP related authentications.
        #  Now in another file, because it is very large.
        #
        $INCLUDE eap.conf

        #  Include another file that has the SQL-related configuration.
        #  This is another file only because it tends to be big.
        #
        $INCLUDE sql.conf

        #
        #  This module is an SQL enabled version of the counter module.
        #
        #  Rather than maintaining seperate (GDBM) databases of
        #  accounting info for each counter, this module uses the data
        #  stored in the raddacct table by the sql modules. This
        #  module NEVER does any database INSERTs or UPDATEs.  It is
        #  totally dependent on the SQL module to process Accounting
        #  packets.
        #
#       $INCLUDE sql/mysql/counter.conf

        #
        #  IP addresses managed in an SQL table.
        #
#       $INCLUDE sqlippool.conf
}

# Instantiation
#
#  This section orders the loading of the modules.  Modules
```

Figura 27. Se descomenta la línea $INCLUDE sql.conf en el archivo radiusd.conf.

Una vez concluida la instalación de freeradius se continúa con la descarga de la herramienta para la gestión del servidor, para esto, es necesario ingresar a la página y descargar la herramienta como se muestra en la Figura 30 a continuación.

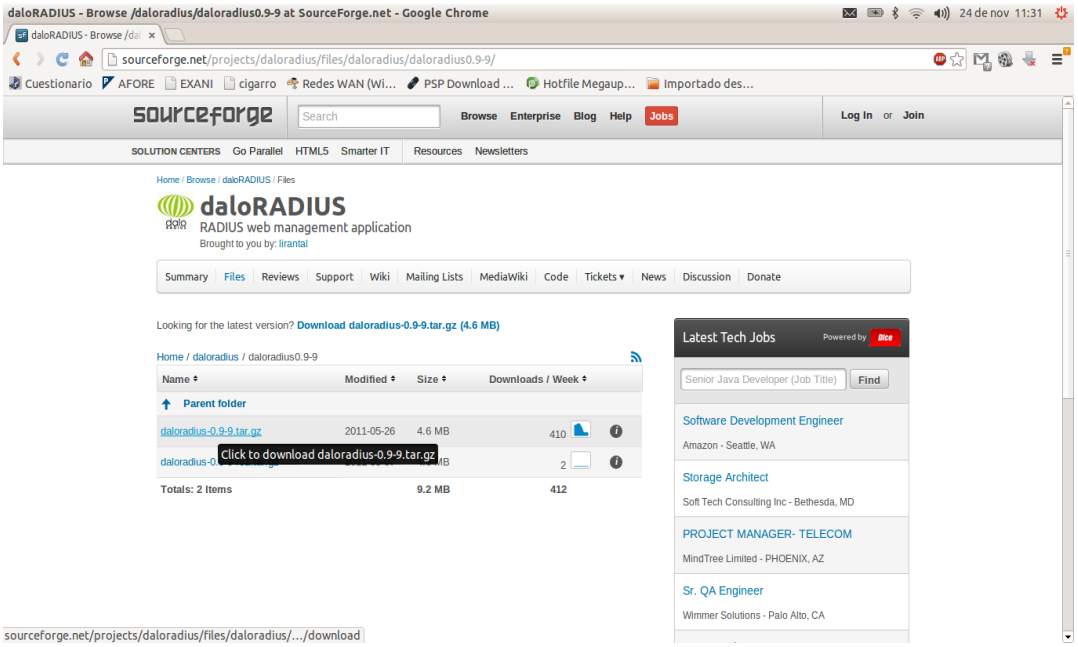

Figura 28. Página web de descarga para el gestor daloradius.

Ya descargada la herramienta, se procede a descargar las demás herramientas mediante una terminal utilizando la siguiente línea de comando, "apt-get install apache2 php5 php5-gd php-pear php-db libapache2-mod-php5 php-mail php5-mysql mysql-server". Después de haber terminado de instalarse, la terminal preguntara si se desea instalar las herramientas descargadas en donde al igual que la instalación de freeradius se teclea la letra "S" y se da enter para continuar.

Después de haber instalado las herramientas, se procede a descomprimir el archivo descargado de la página de daloradius, para ello se realizaran los siguientes pasos:

1.- Se descomprime el archivo descargado en la ruta "/var/www".

2.- Se ingresa en la carpeta mediante el comando "cd /var/www"

3.- Ejecutar el siguiente comando "chow n -R www-data:www-data daloradius".

4.- Se agregan permisos al archivo de configuración daloradius.conf.php mediante el siguiente comando "chmod 777 /daloradius/library/daloradius.conf.php.

5.- Editar el archivo daloradius.conf.php mediante el siguiente comando "nano daloradius/library/daloradius.conf.php" en donde quedara configurado de la siguiente manera:

```
$configValues['DALORADIUS_VERSION'] = '0.9-9';
$configValues['FREERADIUS_VERSION'] = '2';
$configValues['CONFIG_DB_ENGINE'] = 'mysql';
$configValues['CONFIG_DB_HOST'] = 'localhost';
$configValues['CONFIG_DB_PORT'] = '3306';
$configValues['CONFIG_DB_USER'] = 'root';
$configValues['CONFIG_DB_PASS'] = 'raton182';
$configValues['CONFIG_DB_NAME'] = 'radius';
$configValues['CONFIG_DB_TBL_RADCHECK'] = 'radcheck';
$configValues['CONFIG_DB_TBL_RADREPLY'] = 'radreply';
$configValues['CONFIG_DB_TBL_RADGROUPREPLY'] = 'radgroupreply';
```

```
$configValues['CONFIG_DB_TBL_RADGROUPCHECK'] = 'radgroupcheck';
$configValues['CONFIG_DB_TBL_RADUSERGROUP'] = 'radusergroup';
$configValues['CONFIG_DB_TBL_RADNAS'] = 'nas';
$configValues['CONFIG_DB_TBL_RADHG'] = 'radhuntgroup';
$configValues['CONFIG_DB_TBL_RADPOSTAUTH'] = 'radpostauth';
$configValues['CONFIG_DB_TBL_RADACCT'] = 'radacct';
$configValues['CONFIG_DB_TBL_RADIPPOOL'] = 'radippool';
$configValues['CONFIG_DB_TBL_DALOOPERATORS'] = 'operators';
$configValues['CONFIG_DB_TBL_DALOOPERATORS_ACL'] = 'operators_acl';
$configValues['CONFIG_DB_TBL_DALOOPERATORS_ACL_FILES'] =
'operators_acl_files';
$configValues['CONFIG_DB_TBL_DALORATES'] = 'rates';
$configValues['CONFIG_DB_TBL_DALOHOTSPOTS'] = 'hotspots';
$configValues['CONFIG_DB_TBL_DALOUSERINFO'] = 'userinfo';
$configValues['CONFIG_DB_TBL_DALOUSERBILLINFO'] = 'userbillinfo';
$configValues['CONFIG_DB_TBL_DALODICTIONARY'] = 'dictionary';
$configValues['CONFIG_DB_TBL_DALOREALMS'] = 'realms';
$configValues['CONFIG_DB_TBL_DALOPROXYS'] = 'proxys';
$configValues['CONFIG_DB_TBL_DALOBILLINGPAYPAL'] = 'billing_paypal';
$configValues['CONFIG_DB_TBL_DALOBILLINGMERCHANT'] = 'billing_merchant';
$configValues['CONFIG_DB_TBL_DALOBILLINGPLANS'] = 'billing_plans';
$configValues['CONFIG_DB_TBL_DALOBILLINGRATES'] = 'billing_rates';
$configValues['CONFIG_DB_TBL_DALOBILLINGHISTORY'] = 'billing_history';
$configValues['CONFIG_DB_TBL_DALOBATCHHISTORY'] = 'batch_history';
$configValues['CONFIG_DB_TBL_DALOBILLINGPLANSPROFILES'] =
'billing_plans_profiles';
$configValues['CONFIG_DB_TBL_DALOBILLINGINVOICE'] = 'invoice';
$configValues['CONFIG_DB_TBL_DALOBILLINGINVOICEITEMS'] = 'invoice_items';
$configValues['CONFIG_DB_TBL_DALOBILLINGINVOICESTATUS'] = 'invoice_status';
$configValues['CONFIG_DB_TBL_DALOBILLINGINVOICETYPE'] = 'invoice_type';
$configValues['CONFIG_DB_TBL_DALOPAYMENTS'] = 'payment';
$configValues['CONFIG_DB_TBL_DALOPAYMENTTYPES'] = 'payment_type';
$configValues['CONFIG_DB_TBL_DALONODE'] = 'node';
$configValues['CONFIG_FILE_RADIUS_PROXY'] = '/etc/freeradius/proxy.conf';
$configValues['CONFIG_PATH_RADIUS_DICT'] = '';
$configValues['CONFIG_PATH_DALO_VARIABLE_DATA'] = '/var/www/daloradius/var';
$configValues['CONFIG_DB_PASSWORD_ENCRYPTION'] = 'cleartext';
$configValues['CONFIG_LANG'] = 'en';
$configValues['CONFIG_LOG_PAGES'] = 'yes';
$configValues['CONFIG_LOG_ACTIONS'] = 'yes';
$configValues['CONFIG_LOG_QUERIES'] = 'yes';
$configValues['CONFIG_DEBUG_SQL'] = 'yes';
$configValues['CONFIG_DEBUG_SQL_ONPAGE'] = 'no';
$configValues['CONFIG_LOG_FILE'] = '/tmp/daloradius.log';
```

```
$configValues['CONFIG_IFACE_PASSWORD_HIDDEN'] = 'yes';
$configValues['CONFIG_IFACE_TABLES_LISTING'] = '25';
$configValues['CONFIG_IFACE_TABLES_LISTING_NUM'] = 'yes';
$configValues['CONFIG_IFACE_AUTO_COMPLETE'] = 'yes';
$configValues['CONFIG_MAINT_TEST_USER_RADIUSSERVER'] = '127.0.0.1';
$configValues['CONFIG_MAINT_TEST_USER_RADIUSPORT'] = '1812';
$configValues['CONFIG_MAINT_TEST_USER_NASPORT'] = '0';
$configValues['CONFIG_MAINT_TEST_USER_RADIUSSECRET'] = 'testing123';
$configValues['CONFIG_USER_ALLOWEDRANDOMCHARS'] =
'abcdefghijkmnpqrstuvwxyzABCDEFGHJKMNPQRSTUVWXYZ23456789';
$configValues['CONFIG_MAIL_SMTPADDR'] = '127.0.0.1';
$configValues['CONFIG_MAIL_SMTPPORT'] = '25';
$configValues['CONFIG_MAIL_SMTPAUTH'] = '';
$configValues['CONFIG_MAIL_SMTPFROM'] = 'root@daloradius.xdsl.by';
$configValues['CONFIG_DASHBOARD_DALO_SECRETKEY'] = 'sillykey';
$configValues['CONFIG_DASHBOARD_DALO_DEBUG'] = '1';
$configValues['CONFIG_DASHBOARD_DALO_DELAYSOFT'] = '5';
$configValues['CONFIG_DASHBOARD_DALO_DELAYHARD'] = '15';
```

Una vez configurado lo anterior, es necesario crear la base de datos en donde los datos se almacenaran, para ello se realizaran los siguientes pasos:

1.- Se ejecuta el siguiente comando en la terminal: "*mysqladmin -u root -p create radius".*

2.- Se ingresa a la siguiente ruta mediante lo siguiente: "*cd /var/www/daloradius/contrib/db"* y se ejecuta el siguiente comando "*mysql -u root -p nombre_BD < fr2-mysql-daloradius-and-freeradius.sql*".

3.- Después se ingresa a sql mediante el comando "*mysql -u root -p*" y ejecutamos el siguiente comando "*GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY 'raton182';"* y al terminar salimos con el comando "*quit*".

Después, se configura el archivo "eap.conf" que se encuentra en la ruta "/etc/freeradius" en donde en la línea No.30 se agrega lo siguiente: "default_eap_type = ttls", y en el módulo EAP-TLS solo se configuran los siguientes parámetros, quedando de esta manera:

```
tls {
                        #
                        #  These is used to simplify later configurations.
                        #
                        certdir = ${confdir}/certs
                        cadir = ${confdir}/certs
                        private_key_password = radius13
                        private_key_file = ${certdir}/cert-srv.pem
                        #  If Private key & Certificate are located in
                        #  the same file, then private_key_file &
                        #  certificate_file must contain the same file
                        #  name.
                        #
                        #  If CA_file (below) is not used, then the
                        #  certificate_file below MUST include not
                        #  only the server certificate, but ALSO all
                        #  of the CA certificates used to sign the
                        #  server certificate.
                        certificate_file = ${certdir}/cert-srv.pem

                        #  Trusted Root CA list
                        #
                        #  ALL of the CA's in this list will be trusted
                        #  to issue client certificates for authentication.
                        #
                        #  In general, you should use self-signed
                        #  certificates for 802.1x (EAP) authentication.
                        #  In that case, this CA file should contain
                        #  *one* CA certificate.
                        #
                        #  This parameter is used only for EAP-TLS,
                        #  when you issue client certificates.  If you do
                        #  not use client certificates, and you do not want
                        #  to permit EAP-TLS authentication, then delete
                        #  this configuration item.
                        CA_file = ${cadir}/cacert.pem

                        #
                        #  For DH cipher suites to work, you have to
                        #  run OpenSSL to create the DH file first:
                        #
```

```
#       openssl dhparam -out certs/dh 1024
#
dh_file = ${certdir}/dh
random_file = ${certdir}/random
```

Una vez configurados los archivos para el servidor radius, se sigue a configurar los archivos de configuración del servidor apache que se encuentran en la ruta "/etc/apache2". En esta ruta, se configurara el archivo "apache2.conf", se edita el archivo y en la parte final se agregaran las siguientes líneas de código:

```
# Include the virtual host configurations:
Include /etc/apache2/sites-enabled/
<Directory "/var/www/">
Options -Indexes
</Directory>
######################### DaloRadius ##############################
Alias /dalo "/var/www/daloradius/"
<Directory "/var/www/daloradius/">
        Options Indexes MultiViews FollowSymLinks
        Order allow,deny
        Allow from 127.0.0.1
        Allow from localhost
</Directory>
```

Después, se configuran algunos datos del gestor de certificados OpenSSL que se encuentra en la ruta "/etc/ssl" editando el archivo de configuración "openssl.cnf". Aquí se edita en la línea No.73 los días en que el certificado será válido, además de los datos que se agregaran por defecto al certificado, en este caso se agregaron los siguientes parámetros que a continuación se muestran:

```
[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = MX
countryName_min                 = 2
countryName_max                 = 2
```

```
stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = Baja California

localityName                    = Locality Name (eg, city)
localityName_default            = Tijuana

0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = UABC

# we can do this but it is not needed normally :-)
#1.organizationName             = Second Organization Name (eg, company)
#1.organizationName_default     = World Wide Web Pty Ltd

organizationalUnitName          = Organizational Unit Name (eg, section)
organizationalUnitName_default  = MTIC

commonName                      = Common Name (e.g. server FQDN or YOUR
name)
commonName_max                  = 64
commonName_default              = Luis Samaniego

emailAddress                    = Email Address
emailAddress_max        = 64
emailAddress_default            = luis.samaniego@uabc.edu.mx

# SET-ex3                       = SET extension number 3

[ req_attributes ]
challengePassword       = A challenge password
challengePassword_min           = 4
challengePassword_max           = 20

unstructuredName        = An optional company name
```

CREACION DE LOS CERTIFICADOS MEDIANTE EL SCRIPT “ca.all”

Cuando los datos del certificado hayan sido configurados según las necesidades del administrador de la red, es momento de generar un script para

generar con mayor facilidad los certificados que se emitirán a los usuarios que intenten ingresar a la red, para ello, es necesario regresarse a la ruta de los archivos de configuración del servidor radius e ingresar a la carpeta "/certs", en donde se encuentran los certificados por defecto que trae el servidor.

Dentro de la carpeta "/certs" se crea un nuevo archivo mediante el comando "nano ca.all" y se agregan los siguientes datos al archivo:

```
##########export PATH=${SSL}/bin/:${SSL}/ssl/misc:${PATH}

##########export LD_LIBRARY_PATH=${SSL}/lib

rm -rf demoCA roo* cert* *.pem *.der
mkdir demoCA
touch demoCA/serial
echo "02" > demoCA/serial

echo -e ""
echo -e "\t\t###################"
echo -e "\t\tcreate private key"
echo -e "\t\tname : name-root"
echo -e "\t\tCA.pl -newcert"
echo -e "\t\t###################\n"

openssl req -new -x509 -keyout newreq.pem -out newreq.pem -days 2 -passin pass:radius13 -
passout pass:radius13

echo -e ""
echo -e "\t\t###################"
echo -e "\t\tcreate CA"
echo -e "\t\tuse just created 'newreq.pem' private key as filename"
echo -e "\t\tCA.pl -newca"
echo -e "\t\t###################\n"

echo "newreq.pem" | /usr/lib/ssl/misc/CA.pl -newca

#ls -lg demoCA/private/cakey.pem

echo -e ""
echo -e "\t\t###################"
echo -e "\t\texporting ROOT CA"
echo -e "\t\tCA.pl -newreq"
echo -e "\t\tCA.pl -signreq"
echo -e "\t\topenssl pkcs12 -export -in demoCA/cacert.pem -inkey newreq.pem -out root.pem"
echo -e "\t\topenssl pkcs12 -in root.cer -out root.pem"
echo -e "\t\t###################\n"
```

```
openssl pkcs12 -export -in demoCA/cacert.pem -inkey newreq.pem -out root.p12 -cacerts -passin pass:radius13 -passout pass:radius13
openssl pkcs12 -in root.p12 -out root.pem -passin pass:radius13 -passout pass:radius13
openssl x509 -inform PEM -outform DER -in root.pem -out root.der

echo -e ""
echo -e "\t\t####################"
echo -e "\t\tcreating client certificate"
echo -e "\t\tname : name-clt"
echo -e "\t\tclient certificate stored as cert-clt.pem"
echo -e "\t\tCA.pl -newreq"
echo -e "\t\tCA.pl -signreq"
echo -e "\t\t####################\n"

openssl req -new -keyout newreq.pem -out newreq.pem -days 2 -passin pass:radius13 -passout pass:radius13
openssl ca  -policy policy_anything -out newcert.pem -passin pass:radius13 -key radius13 -extensions xpclient_ext -extfile xpextensions -infiles newreq.pem

openssl pkcs12 -export -in newcert.pem -inkey newreq.pem -out cert-clt.p12 -clcerts -passin pass:radius13 -passout pass:radius13
openssl pkcs12 -in cert-clt.p12 -out cert-clt.pem -passin pass:radius13 -passout pass:radius13
openssl x509 -inform PEM -outform DER -in cert-clt.pem -out cert-clt.der

echo -e ""
echo -e "\t\t####################"
echo -e "\t\tcreating server certificate"
echo -e "\t\tname : name-srv"
echo -e "\t\tserver certificate stored as cert-srv.pem"
echo -e "\t\tCA.pl -newreq"
echo -e "\t\tCA.pl -signreq"
echo -e "\t\t####################\n"

openssl req -new  -keyout newreq.pem -out newreq.pem -days 2 -passin pass:radius13 -passout pass:radius13
openssl ca  -policy policy_anything  -out newcert.pem -passin pass:radius13 -key radius13 -extensions xpserver_ext -extfile xpextensions -infiles newreq.pem

 openssl pkcs12 -export -in newcert.pem -inkey newreq.pem -out cert-srv.p12 -clcerts -passin pass:radius13 -passout pass:radius13
openssl pkcs12 -in cert-srv.p12 -out cert-srv.pem -passin pass:radius13 -passout pass:radius13
openssl x509 -inform PEM -outform DER -in cert-srv.pem -out cert-srv.der

echo -e "\n\t\t####################\n"
```

Una vez generado el script para generar los certificados, se ejecuta mediante la instrucción "./ca.all". Cuando el scritp empiece a ejecutarse, pedirá algunos parámetros para configurar los certificados, de los cuales, se puede dejar algunos de los parámetros por defecto, ya que se han configurado para cubrir las necesidades planteadas por esta implementación. Es necesario indicar hacia quienes van dirigidos los certificados y el script indicara cuando se está generando el certificado para el cliente y para el servidor.

Dentro de la misma ejecución del script, se irán firmando los certificados conforme avanza la creación de los mismos.

Después de que el script haya terminado de ejecutarse y creados los certificados, es necesario ingresar a la carpeta "demoCA" y copiar el archivo "cacert.pem" a la ruta "/etc/freeradius/certs", para ello se ejecuta el comando "cp cacert.pem /etc/freeradius/certs".

CONFIGURACION EN LA INTERFAZ GRAFICA DE DALORADIUS PARA INGRESAR LOS USUARIOS Y LOS AP's

Cuando todos los servicios fueron configurados de acuerdo a las instrucciones anteriores, se ejecuta el navegador web y se ingresa la barra de dirección del navegador la ruta "127.0.0.1/daloradius", en donde se procede a agregar los AP's y los usuarios que tendrán interacción con el servicio. Al momento de ingresar a la dirección mencionada con anterioridad, el navegador web muestra en la figura 31.

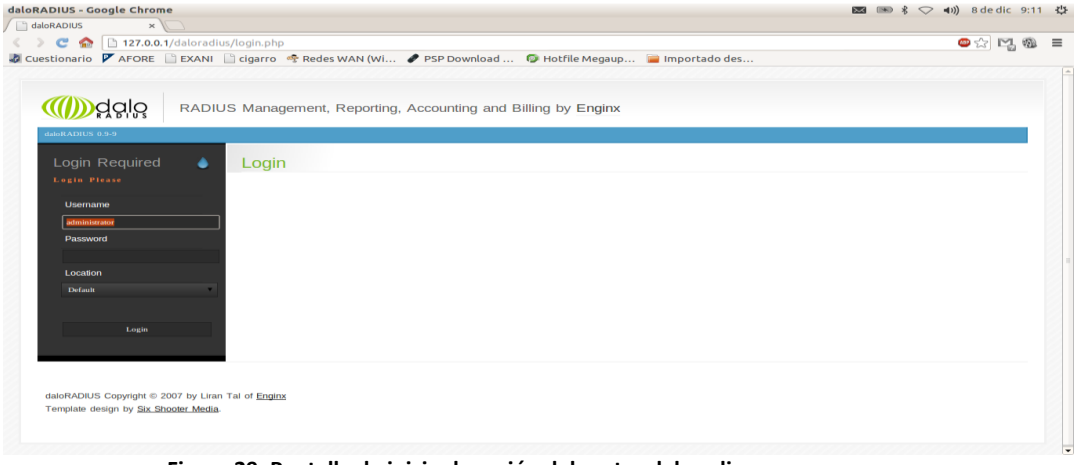

Figura 29. Pantalla de inicio de sesión del gestor daloradius.

La interfaz del gestor daloradius al momento de intentar ingresar, solicita un nombre de usuario y contraseña, en donde el usuario es “Administrator” y la contraseña es “radius”, después se teclea la tecla “enter” o se da clic en el botón “login”.

Una vez autenticado en el gestor daloradius, se deben de ingresar los datos de los AP's que se van a utilizar, así como también, los datos de los usuarios que van a ingresar a la red, para ello, se ingresa a la pestaña “Management”, después a la subpestaña “NAS” y por ultimo a la opción “new NAS” para ingresar los AP's, en donde una vez dentro, se muestra una pantalla como lo muestra la figura 32.

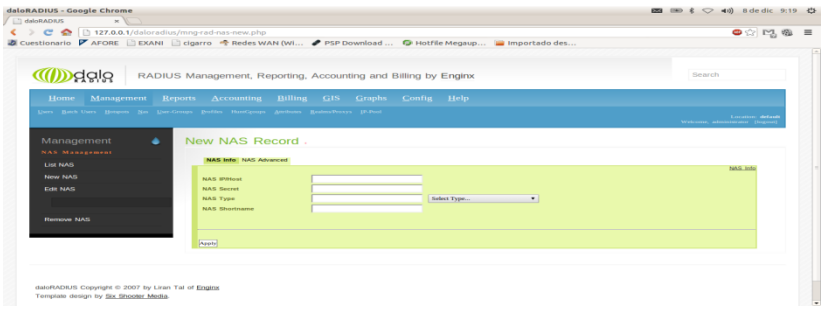

Figura 30. Ingresar un nuevo AP.

Dentro de la configuración del nuevo AP, se ingresan los datos solicitados por el gestor y se guardan los cambios dando clic en el botón “Apply”. Para confirmar que el AP fue agregado correctamente, se ingresa a la opción “List NAS” para revisar la lista de AP's que el servidor radius reconocerá.

De igual manera, los pasos para ingresar los nuevos usuarios es muy sencilla, basta con ingresar a la subpestaña “Users” y luego a la opción “New User”, en donde arrogara una pantalla como lo muestra la figura 33:

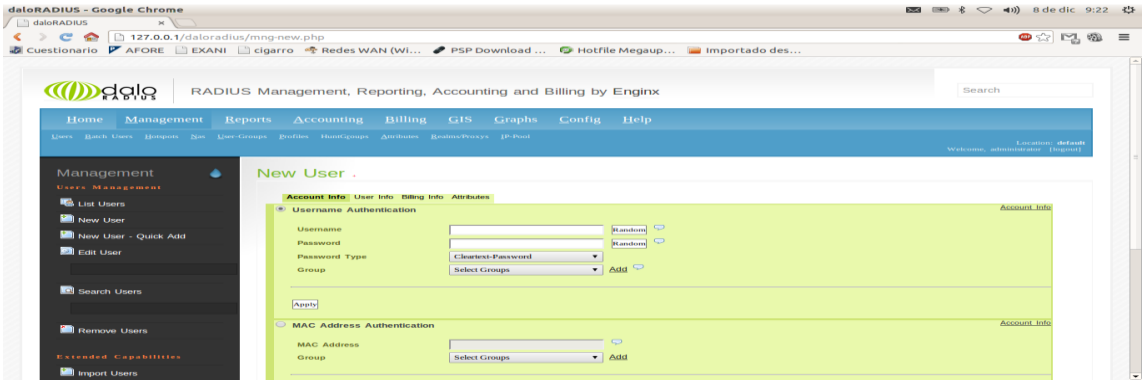

Figura 31. Pantalla de ingreso de nuevo usuario.

Cuando se ingresa a agregar un nuevo usuario, el gestor solicita el nombre de usuario y la contraseña para el usuario que va a autenticarse al servidor, una vez ingresados se guardan los cambios dando clic en el botón "Apply" y se revisa que los cambios hayan sido satisfactorios dando clic en la opción "List Users" para mostrar una lista de los usuarios creados.

Después de que se agregan los usuarios y AP's, además de las configuraciones anteriormente realizadas, se procede a configurar los AP's para que tengan comunicación con el servidor RADIUS, para ello, se siguen los pasos mencionados anteriormente a partir de la figura 7.

Una vez configurados los AP's, se procede a la instalación de los certificados de usuario, utilizando los archivos "cert-clt.der y cert-clt.p12" anteriormente creados con el script "ca.all", en donde se deben de seguir las instrucciones que con anterioridad se muestran en la sección "Instalación de los certificados en el cliente", solo que esta vez, la contraseña para poder instalar el archivo "cert-clt.p12" es "radius13, tal y como se menciona en las instrucciones del script generado "ca.all".

Capitulo V. Resultados

Concluida la implementación de la tecnología WPA2 – Enterprise en la FCQI, fueron generados los usuarios con la finalidad de utilizar la red mediante las restricciones que ella presenta. Los certificados y llaves generadas al inicio del proyecto, tuvieron una caducidad de siete días para afirmar que los certificados caducaran y que los usuarios no pudieran ingresar a la red. Después, se generaron certificados nuevos para que los usuarios tengan el certificado por periodos de 1 año o más, tiempo con en el cual, el servidor estará funcionando día y noche con la finalidad de que los usuarios ingresaran a la red inalámbrica sin ningún problema. A continuación la figura 34 muestra un ejemplo de algunos usuarios creados en el gestor web "daloradius":

Figura 32. Lista de usuarios creado.

Los usuarios ingresaron sin importar el AP que deseaban ingresar, en donde, se instaló un AP en el edificio 6I y 6D de la facultad, un AP con el nombre de "radius13" y otro con el nombre de "radius13 CTC".

Dichos AP's están en contacto con el servidor para actuar como intermediarios entre el usuario y el servidor, en donde el usuario solo tiene contacto directo con el AP y no con el servidor, evitando así posibles ataques hacia el servidor RADIUS por parte de usuarios no identificados o externos a la facultad. Enseguida, la figura 35 muestra un ejemplo de la lista de AP's que se utilizaron:

Figura 33. Lista de AP's utilizados.

El administrador de la red tiene la capacidad de administrar los usuarios que ingresan a la red, ya que puede eliminar o agregar nuevos usuarios así como también la opción de agregar nuevos AP's para la extensión de la red dentro de la facultad, así como eliminarlos.

Los modelos de dispositivos que se utilizaron en la implementación fueron:

- WRT54G LINKSYS v5.
- APPLE AIRPORT 2da. Generación.

Durante los periodos de pruebas se eliminaron y crearon usuarios comprobando así la eficiencia del gestor web, las cuales fueron satisfactorias al confirmar que el la herramienta "daloradius" funciona correctamente administrando las cuentas de usuarios y de los dispositivos AP.

Capítulo VI. Conclusiones

La implementación de la tecnología WPA2 – Enterprise en conjunto con herramientas que ayudan a la administración y manejo, tanto como para la base de datos creada como para el servidor RADIUS, proveen al administrador de la red inalámbrica, una adecuada administración, así como una gran flexibilidad para el manejo de cuentas de usuarios y sus certificados, facilitando de esta manera las tareas del administrador y generando mayor confianza en la seguridad para negar el acceso a la red hacia personas ajenas de la facultad.

El uso de certificados para la identificación de los usuarios por el servidor, brinda gran confianza hacia el personal encargado de la administración y mantenimiento de la red, debido a que el servicio que otorga el servidor RADIUS es muy confiable y trabaja de manera rápida y eficaz al momento de reconocer los certificados, dando como resultado, un acceso seguro a los usuarios.

Recomendaciones

Las tecnologías de la información están en constante crecimiento gracias a las diversas necesidades de empresas y organizaciones que día con día solicitan la mayor seguridad posible para el manejo y envió de su información.

El papel que ejercen los administradores de red es parte fundamental para la seguridad de la información de la empresa, ya que se debe mantener actualizada la red con tecnología de seguridad resiente para proteger de esta manera el patrimonio informático de la empresa.

El manejo de un servidor RADIUS para la implementación de la tecnología WPA2 – Enterprise, requiere de un constante mantenimiento, para ello, es de gran prioridad mantener las herramientas, librerías y/o aplicaciones del servidor actualizadas, además, siendo el servidor el creador de los certificados y el que genere el acceso a la red inalámbrica, debe mantener la fecha y hora actualizada para prevenir inconvenientes al momento de generar los certificados, ya que la fecha de inicio de los certificados, será la misma que la fecha del servidor en donde se creó.

Durante el proceso de creación de nuevos usuarios, es importante agregar alguna descripción que identifique a la persona que se le otorgara el servicio de red inalámbrica para mantener una adecuada administración sobre las personas que podrán ingresar a la red, así como también, agregar comentarios a los AP's que están siendo administrados por el gesto web, describiendo el lugar en donde se encuentran y el SSID que provee cada uno de ellos.

Es recomendable llevar un control sobre los certificados impartidos a los usuarios además de las fechas en que fueron impartidos y su caducidad, para estar prevenido al momento que los certificados estén próximos a caducar y generar los certificados necesarios para los usuarios.

Además, debido a la gran cantidad de usuarios que puede llegar a tener el servidor, a causa de la gran cantidad de alumnos con los que cuenta la facultad, es de gran importancia tener un respaldo de toda la información o mejor aún, generar periódicamente una imagen del servidor, para que en caso de que exista alguna falla con el servidor, se pone en marcha el servidor de respaldo mientras el primero es llevado a mantenimiento.

Bibliografía

Cabrera, J. L., & Gonzalez, L. R. (2006). *redes locales 4ta. edicion.* madrid: alfaomega.

Chaparro Bargas, R. A., & Mejia Fajardo, M. (2006). Análisis de desempeño y evaluación de requerimientos AAA en el protocolo de seguridad sobre redes inalámbricas IEEE 802.11. *Redalyc*.

Engelschall, R. S. (s.f.). *http://www.openssl.org/*. Obtenido de http://www.openssl.org/: http://www.openssl.org/

Forouzan, B. A. (2002). *Transmision de datos y redes de comunicaciones 2da. edicion.* madrid: Mc Graw Hill.

Garcia-Morán, J. P., Hansen, Y. F., & Varón, A. R. (2009). *AAA / Radius / 802.1x Sistemas basados en la autenticacion en Windows y Linux/GNU.* Mexico: Alfaomega Ra-Ma.

Geier, E. (2011). *Deploying WPA2 Enterprise*. Obtenido de http://www.windowsnetworking.com/articles_tutorials/Deploying-WPA2-Enterprise-Wi-Fi-Security-Small-Businesses.html

Inc., G. (s.f.). *http://ciitix-wifi.sourceforge.net/*. Obtenido de http://ciitix-wifi.sourceforge.net/: http://ciitix-wifi.sourceforge.net/

Lazo García, N. A. (Julio de 2012). DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN Y WLAN CON. Lima, Perú.

Madron, T. W. (1992). *Redes de Area Local.* mexico: megabyte.

Mejía Nogales, J. L., Vidal Beltrán, S., & López Bonilla, J. L. (2006). Sistema de acceso seguro a recursos de información para redes inalámbricas 802.11. *Redalyc*.

Molina Robles, F. J. (2006). *Redes de area local 2da. edicion.* madrid: alfaomega.

Neil, R., & Ron, S. (s.f.). *802.11 (Wi-Fi) Manual de Redes Inalambricas.* Mc Graw Hill.

Ocando, A., & Ugas, L. (2005). Tecnologias para redes inalámbricas en las organizaciones del estado Zulica. *Redalyc*.

P. Sarmiento, O., G. Guerrero, F., & Rey Argote, D. (2008). Fundamentos prácticos de seguridad en redes inalámbricas. *Ingenieria e Invastigacion Vol. 28*.

Radius, N. (s.f.). *http://freeradius.org/*. Obtenido de http://freeradius.org/: http://freeradius.org/

Raya Cabrera, J. L., & Raya Pérez, E. (2008). *Redes Locales 3ra. Edicion.* Alfaomega RA-MA.

Sampieri, R. H., Collado, C. F., & Lucio, P. B. (2004). *Metodologia de la investigacion* (3ra. ed.). Mexico: McGraw-Hill.

Stallings, W. (2004). *Comunicaciones y Redes de Computadoras 7ma. Edicion.* Madrid: PEARSON.

Stallings, W. (2004). *Fundamentos de seguridad en redes aplicaciones y estandares 2da.edicion.* madrid: pearson.

Tal, L. (s.f.). *http://www.daloradius.com/*. Obtenido de http://www.daloradius.com/: http://www.daloradius.com/

Apéndice A

Instalación del sistema operativo Ubuntu 12.10

A continuación, se mostraran los pasos a seguir para instalar el sistema operativo Ubuntu 12.10:

1.- Se inserta el disco del Ubuntu y se arranca desde el CD, al hacer esto, arrojara la pantalla como muestra la figura 22.

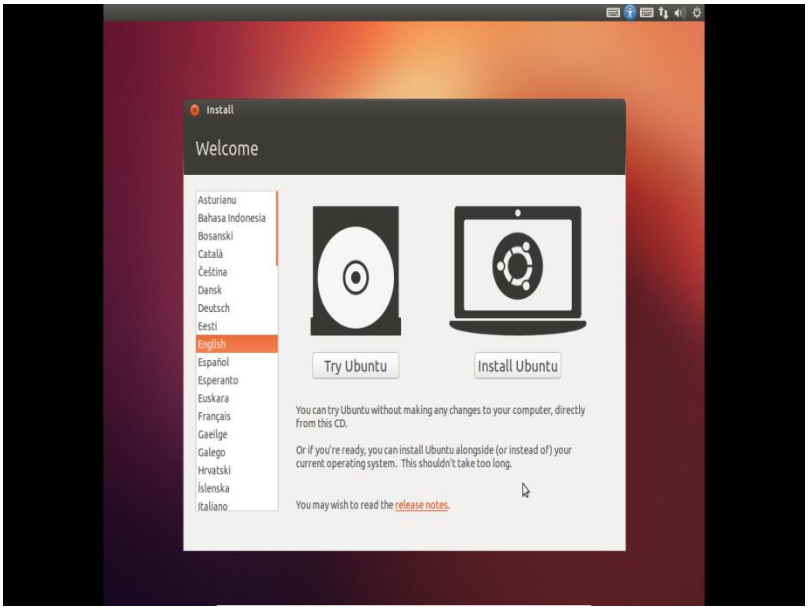

Figura 34. Pantalla de bienvenida de Ubuntu.

2.- En la Figura 22, la instalación del sistema muestra dos opciones, en donde se seleccionara la opción 2, ya que se instalara el sistema operativo y no se usara de forma Live, además, se puede seleccionar el idioma que se necesite, en este caso, se seleccionó el idioma Español.

3.- A continuación, muestra la siguiente pantalla, tal y como lo muestra la Figura 23, en donde se seleccionan los 2 check-boxs, esto es para obtener las

últimas actualizaciones del sistema, además de algunas paqueterías para la reproducción de archivos multimedia, los cuales se utilizaran más adelante.

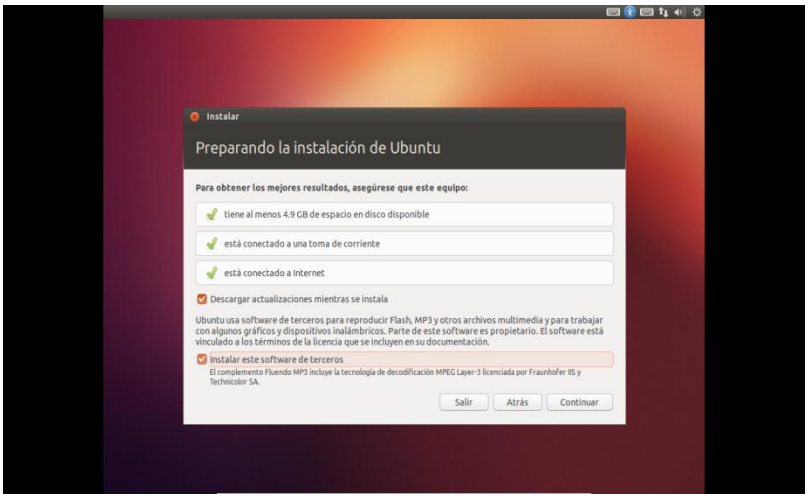

Figura 35. Pantalla de preparación de la instalación.

4.- Una vez seleccionadas las opciones indicadas en la Figura 23, se procede a hacer clic al botón continuar y seguir con la instalación del sistema. Durante la instalación, se les solicita alguna información sobre la zona horaria, el tipo de teclado y el nombre de usuario así como una contraseña, la cual se recomienda que tenga números y letras, en donde mínimamente el sistema nos indique que es una contraseña aceptable, tal y como lo muestra la Figura 24 a continuación.

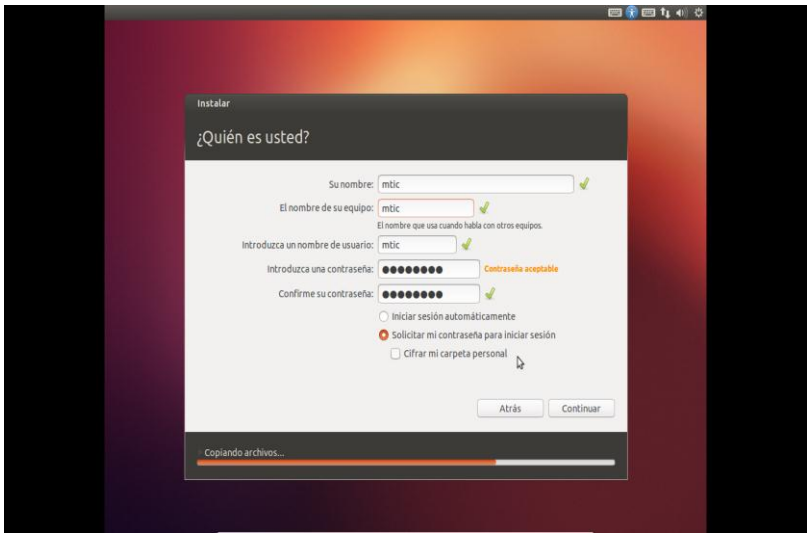

Figura 36. Pantalla de captura para el nombre de usuario.

5.- Ya terminado el proceso de instalación y configuración del sistema, la computadora se reiniciara y accederemos al sistema ya instalado, ingresando mediante el usuario y la contraseña. De esta manera, se concluye el proceso de instalación de Ubuntu.