Evaluación del desempeño de los sistemas de autenticación del estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el protocolo de RADIUS

Álvarez Mise, Luis Fernando

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Trabajo de titulación, previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones

Ing. Romero Gallardo, Carlos Gabriel

26 de agosto de 2022

Resultados de la herramienta para verificación y/o análisis de similitud de contenidos

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Certificación

Certifico que el trabajo de titulación, **"Evaluación del desempeño de los sistemas de autenticación del estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el protocolo de RADIUS"** fue realizado por el señor **Álvarez Mise, Luis Fernando**, el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 26 de agosto de 2022

Firma:

Firmado electrónicamente por:
CARLOS GABRIEL
ROMERO GALLARDO

Romero Gallardo, Carlos Gabriel

C.C.: 1712198066

Departamento de Eléctrica, Electrónica y Telecomunicaciones
Carrera de Ingeniería en Electrónica y Telecomunicaciones

Responsabilidad de Autoría

Yo, **Álvarez Mise, Luis Fernando**, con cédula/cedulas de ciudadanía n° 1206681882, declaro que el contenido, ideas y criterios del trabajo de titulación: **Evaluación del desempeño de los sistemas de autenticación del estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el protocolo de RADIUS** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 24 de agosto de 2022

Firma:

Firmado electrónicamente por:
LUIS FERNANDO ALVAREZ MISE

Álvarez Mise, Luis Fernando
C.C.: 1206681882

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Departamento de Eléctrica, Electrónica y Telecomunicaciones
Carrera de Ingeniería en Electrónica y Telecomunicaciones

Autorización de Publicación

Yo, **Álvarez Mise, Luis Fernando**, con cédula de ciudadanía n° 1206681882, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Evaluación del desempeño de los sistemas de autenticación del estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el protocolo de RADIUS** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi/nuestra responsabilidad.

Sangolquí, 24 de agosto de 2022

Firma:

Firmado electrónicamente por:
LUIS FERNANDO ALVAREZ MISE

Álvarez Mise, Luis Fernando
C.C.: 1206681882

Dedicatoria

Dedico este trabajo de titulación a mis padres, que siempre me han brindado su apoyo incondicional para que pueda cumplir mis metas y sueños tanto personales como profesionales. A la memoria de mis abuelitas Elida Marieta y María Margarita con las que siempre podía contar y aunque ya no esté con ellas siempre siento su amor y apoyo.

Luis Fernando Alvarez Mise

Agradecimientos

Mi agradecimiento va hacia mis padres que gracias a su esfuerzo he podido estudiar en esta prestigiosa institución, además de siempre brindarme su apoyo y amor para seguir adelante. Agradezco también a la empresa Compu Seguridad por permitirme realizar este trabajo de titulación con ellos y recibirme de brazos abiertos en su grupo de trabajo. De igual forma agradezco a mi tutor Carlos Romero por brindarme sus conocimientos a lo largo del desarrollo de este trabajo y de mi vida profesional.

Luis Fernando Alvarez Mise

Índice de contenidos

Lista de tablas

Lista de figuras

Resumen

En los últimos años las redes de comunicación han ido evolucionando de manera rápida, así como la demanda de los usuarios, entonces como ISP (Internet Service Provider) lo que busca es poder brindar confidencialidad a su red interna inalámbrica para que esta sea segura y confiable. El uso que se da a la red en la empresa Compu Seguridad trae consigo muchos riesgos de seguridad, algunos de ellos se producen por la inexistencia o carencia de mecanismos de seguridad que son insuficientes para proteger el acceso a la información de los usuarios. Por este motivo el presente proyecto de investigación consiste en evaluar el desempeño de los sistemas de autenticación del estándar de seguridad IEEE 802.1X para finalmente realizar la integración de un portal cautivo bajo el protocolo de RADIUS (Remote Authentication Dial In User Service) y así brindar los servicios de red en la empresa Compu Seguridad. Dicha integración beneficiará a la empresa para mejorar la seguridad de su red de comunicación inalámbrica, ya que al ser un ISP se tienen que plantear políticas de seguridad, para mantener un control en el acceso a la red y de esta forma resguardar la información de la empresa y de sus usuarios. El estándar 802.1X indica los componentes operativos, los protocolos y la arquitectura que ayudan a la autenticación basada en puertos de los usuarios en una red. El objetivo del estándar 802.1X es controlar el acceso de los usuarios y proteger la transmisión no autorizada. La implementación del portal cautivo bajo el protocolo RADIUS se realizó sobre el equipo MikroTik RouterBOARD RB951Ui-2Hnd, el cual cumple con los servicios AAA (Authentication, Authorization and Accounting). Además, la red inalámbrica está desplegada por medio de cinco enrutadores dentro de la empresa por medio de una VLAN para brindar servicio de internet inalámbrico. Finalmente, se implementó un sistema de tarifación del servicio de internet que brinda el ISP para los clientes que soliciten el servicio, por medio de vouchers que entregan credenciales para ingresar a la red inalámbrica de la empresa de forma limitada.

Palabras claves: ISP, IEEE 802.1X, RADIUS, AAA, portal cautivo

Abstract

In recent years, communication networks have evolved rapidly, as well as the demand of users, so as an Internet Service Provider (ISP) what they are looking for is to be able to provide confidentiality to your internal wireless network so that it is safe and reliable. The use that is given to the network in the company Compu Seguridad brings with it many security risks, some of them are caused by the inexistence or lack of security mechanisms that are insufficient to protect access to user information. For this reason, the present research project consists of evaluating the performance of the authentication systems of the IEEE 802.1X security standard to finally carry out the integration of a captive portal under the RADIUS protocol (Remote Authentication Dial in User Service) and thus provide network services in the company Compu Seguridad. This integration will benefit the company to improve the security of its wireless communication network, since being an ISP, security policies have to be established, to maintain control over access to the network and thus safeguard the information of the company and its users. The 802.1X standard outlines the operating components, protocols, and architecture that support port-based authentication of users on a network. The goal of the 802.1X standard is to control user access and protect unauthorized transmission. The implementation of the captive portal under the RADIUS protocol was carried out on the MikroTik RouterBOARD RB951Ui-2Hnd equipment, which complies with the AAA (Authentication, Authorization and Accounting) services. In addition, the wireless network is deployed through five routers within the company through a VLAN to provide wireless internet service. Finally, a pricing system of the internet service provided by the ISP was implemented for customers who request internet service, through vouchers that provide credentials to enter the company's wireless network on a limited basis.

Key words; ISP, IEEE 802.1, RADIUS, AAA, captive portal

Capítulo I

Planteamiento del problema de investigación

Antecedentes

Al implementar una red inalámbrica o cableada, debe asegurarse de que se implementen las medidas de seguridad adecuadas. Una empresa, por ejemplo, a menudo tiene recursos valiosos almacenados dentro de bases de datos que están conectadas a la red. El uso de contraseñas para acceder a aplicaciones específicas generalmente no es lo suficientemente bueno para evitar que los piratas informáticos accedan a los recursos de forma no autorizada y, a veces, paralizante. Para proteger adecuadamente su red de intrusos, debe tener mecanismos que utilicen métodos de autenticación probados que controlen el acceso a la red.

El marco general para proporcionar control de acceso a las redes es lo que se conoce como un sistema de autenticación basado en puertos, al que algunas personas se refieren como 802.1X. El concepto principal de este tipo de sistema es bastante sencillo: simplemente verifica que las credenciales que proporciona un usuario indican que el usuario está autorizado para usar la red. Si es así, entonces les permite tener acceso a la red. Si no están autorizados, entonces no les permite tener acceso a la red.

Uno de los primeros trabajos completos acerca de los sistemas de autenticación del estándar 802.1X corresponde a Chen y Wang (2005) mencionaron la implementación de diferentes tipos de técnicas EAP (Extensible Authentication Protocol). Implementar estas técnicas es bastante complejo, pero en este artículo se muestra que con la ayuda de WIRE 1x se puede hacer fácilmente. Es una implementación de CÓDIGO ABIERTO del lado del cliente, porque si el lado del cliente es fuerte la comunicación es más segura. Estos WIRE 1x funcionan fácilmente con Windows y admiten casi todos los mecanismos de autenticación definidos en EAP. WIRE 1x también proporciona una forma segura de comunicación para el usuario que utiliza WLAN. Este documento define todos los componentes de WIRE 1x. También define algunas de las técnicas EAP como EAP- MD5 EAP-TLS EAP-TTLS EAP-PEAP y también se ha

derivado una tabla de comparación. También informa sobre diferentes bibliotecas de código abierto como Libnet, Openssl.

Un segundo estudio de Ali y Al-Khlifa (2011) muestran que el EAP admite una variedad de protocolos de capa de autenticación de capa superior, cada uno de los cuales tiene algunas ventajas y desventajas. Este documento ofrece una descripción general de los métodos de autenticación EAP más utilizados. La principal ventaja de esto es que con la ayuda de este estudio comparativo podemos elegir la técnica que es más confiable para la comunicación y cuál es peor. También explica estas técnicas en detalle para que el usuario pueda entenderlas fácilmente. Y finalmente se detalla una tabla comparativa usando diferentes técnicas como son MD5, PEAP, LEAP, FAST, TLS y TTLS.

Un tercer estudio realizado por Sang y Zhou (2012) muestran que en los últimos años se ha desarrollado un gran número de aplicaciones para WLAN. Pero también surgen diferentes tipos de problemas relacionados con la seguridad en WLAN. Para brindar seguridad, necesitamos un protocolo de autenticación seguro como PEAP. Este documento habla principalmente sobre el Protocolo de Autenticación Extensible Protegido (PEAP). También habla poco sobre EAP-MD5, EAP-TLS y EAP-TTLS. Pero su principal preocupación en PEAP es cómo se lleva a cabo su proceso de autenticación, cuáles son los defectos en EAP-PEAP y cómo podemos mejorar PEAP para que pueda superar estos defectos.

Un cuarto estudio realizado por Baek, Smith y Kotz (2013) describieron ocho propiedades deseadas para los protocolos de autenticación WLAN. Estudiaron diferentes tipos de protocolos de autenticación EAP: LEAP, Kerberos, EAP-TLS, Green pass, autenticación criptográfica basada en ID, EAP-TTLS y PEAP. En su investigación encontraron que LEAP, Kerberos no son lo suficientemente seguros debido a un ataque de diccionario. EAP-SRP y la privacidad basada en ID carecen de implementación actual para WLAN. EAP-TLS brinda una seguridad sólida si la red no se preocupa por la delegación y la privacidad de la identidad. Además, estos protocolos superan algunas de las dificultades de la autenticación del cliente en

EAP-TLS (es decir, requieren que el cliente posea un certificado emitido por CA, Certificate Authority). Los autores en este documento explican los protocolos con la ayuda de un diagrama de flujo entre el cliente y el servidor.

Y un quinto estudio realizado por Sukhija y Gupta (2014) describieron diferentes protocolos para asegurar la LAN inalámbrica. WEP no puede proporcionar seguridad contra varios ataques y amenazas. Luego apareció WPA, que es una solución temporal a las fallas de seguridad identificadas en WEP. Pero todavía es propenso a varios ataques como Beck-tews, ChopChop, etc. Por lo tanto, se introdujo WPA2 que proporciona una mejora sobre WPA. WPA2 proporciona un cifrado sólido mediante el uso de cifrado de bloque AES, pero sigue siendo vulnerable a los ataques debido al uso compartido de GTK entre los clientes y la transmisión de marcos de gestión y control sin cifrar. Además, WPA2 no admite hardware heredado a diferencia de WPA.

Justificación

El estándar IEEE 802.1X tiene por objetivo ser el proveedor de los diferentes equipos que requieran de una conectividad inalámbrica permitiendo así la movilidad de los usuarios, el mismo trabaja en la banda de frecuencia de las redes LAN cumpliendo con ciertas funciones como: describir las funciones y servicios que requiere un dispositivo que este dentro de esta red, definir el proceso de la MAC para poder dar soporte a los servicios de entrega de datos, definir las técnicas de señalización y funciones que van a ser controladas por la MAC y describir los procedimientos y requerimientos necesarios para poder dar privacidad a la información que se transmite dentro del medio inalámbrico (Hurtado, 2017).

El portal cautivo es una técnica de autenticación y seguridad de datos que hace que un usuario de una red deba pasar por una página web especial antes de poder acceder a Internet. El portal cautivo es en realidad un enrutador o una máquina de puerta de enlace que utiliza un navegador web como un medio o un dispositivo de autenticación seguro y controlado para proteger y permitir el tráfico hasta que el usuario se registre (Wahyudi, Luthfi, & Efendi, 2019).

Un Network Access Server (NAS) funciona como cliente de RADIUS. El cliente se responsabilidad de enviar la información del usuario a los servidores RADIUS designados y luego proceder con la respuesta que se obtiene. Los servidores RADIUS son los encargados de receptar las solicitudes de conexión que realizan los usuarios, luego lo autentica para finalmente devolver toda la información de configuración necesaria para que el cliente brinde el servicio a los usuarios (Willens, Rubens, Simpson, & Rigney, 2000).

Para la empresa Compu Seguridad es importante poder proveer una óptima administración de sus redes y el internet para poder asegurar la información y datos que son transmitidos por la misma, por ello optimizando el sistema de seguridad se tendrá un control de acceso total y utilización de los recursos de la red.

Mantener la confidencialidad de la información siempre será el punto de mayor nivel a tomar en cuenta por los usuarios, para ello es necesario establecer políticas de seguridad internas y de control de acceso a la información, esto es posible mediante protocolos y servidores de seguridad los cuales deberán cumplir los siguientes requisitos: estabilidad, confidencialidad y seguridad de la información.

Para brindar una solución óptima e inmediata que garantice el funcionamiento correcto de los equipos para que la información que viaja por los mismos sea segura y confiable es necesario disponer de la información que se tiene en la empresa, este es un recurso indispensable para realizar el trabajo de investigación.

Como ingenieros en Electrónica y Telecomunicaciones se debe dar soluciones a los posibles problemas que se puedan presentar en el campo de seguridad en redes ya que son de gran importancia hoy en día tanto para las instituciones públicas como privadas, involucrándose directamente para garantizar la confiabilidad de la transmisión de datos de los usuarios, tomando como punto de partida las políticas de seguridad que establece la norma del IEEE 802.1X.

Alcance del proyecto

El trabajo de titulación plantea evaluar el desempeño de los sistemas de autenticación del estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el protocolo de RADIUS, con la finalidad de optar por la autenticación más adecuado para brindar los servicios de red de la empresa Compu Seguridad y así desplegar una red inalámbrica más segura, confiable y de administración sencilla.

Para evaluar los sistemas de autenticación del estándar de seguridad IEEE 802.1X se realizó un cuadro comparativo con los métodos del protocolo de autenticación extensible (Extensible Authentication Protocol, EAP).

Para la integración del portal cautivo con la integración del protocolo RADIUS para autenticar, autorizar y contabilizar a los clientes de la red, se puede contar con software libre como es FreeRADIUS, Openwisp RADIUS, daloRADIUS, también hardware como Cisco, MikroTik, Linksys, entre otros. La empresa Compu Seguridad cuenta con el MikroTik RouterBOARD RB951Ui-2Hnd, el cual se utilizó para implementar el sistema.

Además, para brindar servicio de internet inalámbrico se configura una VLAN con diferentes enrutadores en cada piso de la empresa para complacer la demanda de conexión y se creará un sistema de prueba gratuita para los clientes que soliciten información de velocidad y capacidad del internet del ISP.

Objetivos

Objetivo general

Evaluar el desempeño de los sistemas de autenticación del estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el protocolo de RADIUS y así brindar los servicios de red en la empresa Compu Seguridad.

Objetivos específicos

- Desarrollar el estado del arte del estándar de seguridad IEEE 802.1X, el protocolo RADIUS y su integración en portales cautivos.
- Realizar un análisis comparativo de la autenticación del estándar de seguridad IEEE 802.1X.
- Realizar un análisis de la situación actual de la red inalámbrica de la empresa Compu Seguridad.
- Desarrollar un portal cautivo que permita iniciar sesión y conectarse a internet a los empleados de la empresa Compu Seguridad.
- Configurar los equipos de red inalámbrica de la empresa Compu Seguridad bajo el estándar de seguridad IEEE 802.1X.
- Evaluar los resultados obtenidos en la implementación de los sistemas de autenticación.

Organización

El presente trabajo de titulación esta desarrollado en cinco capítulos. El primer capítulo tiene como finalidad describir los antecedentes sobre los cuales parte este trabajo, se redacta la justificación y alcance del proyecto. Finalmente, se detallan el objetivo general y los objetivos específicos que se tomarán en consideración para desarrollar este trabajo de titulación.

En el segundo capítulo se desarrolla el fundamento teórico, el cual es necesario para que el lector pueda comprender el desarrollo de esta investigación. Asimismo, ayuda a entender el análisis, diseño e implementación que se utilizó para el sistema de seguridad de comunicación inalámbrica mediante el protocolo RADIUS.

En el tercer capítulo se encuentra el análisis de los mecanismos de autenticación del protocolo de autenticación extensible (EAP), el diseño y la implementación de un portal cautivo mediante el protocolo RADIUS para reforzar la seguridad de la red inalámbrica de la empresa Compu Seguridad.

El cuarto capítulo muestra los resultados obtenidos en este trabajo de titulación, como es la implementación de un portal cautivo mediante el protocolo RADIUS en la empresa Compu Seguridad.

Finalmente, en el quinto capítulo se obtienen las conclusiones, recomendaciones y trabajos futuros acerca de este trabajo de titulación.

Capítulo II

Fundamento teórico

Redes inalámbricas

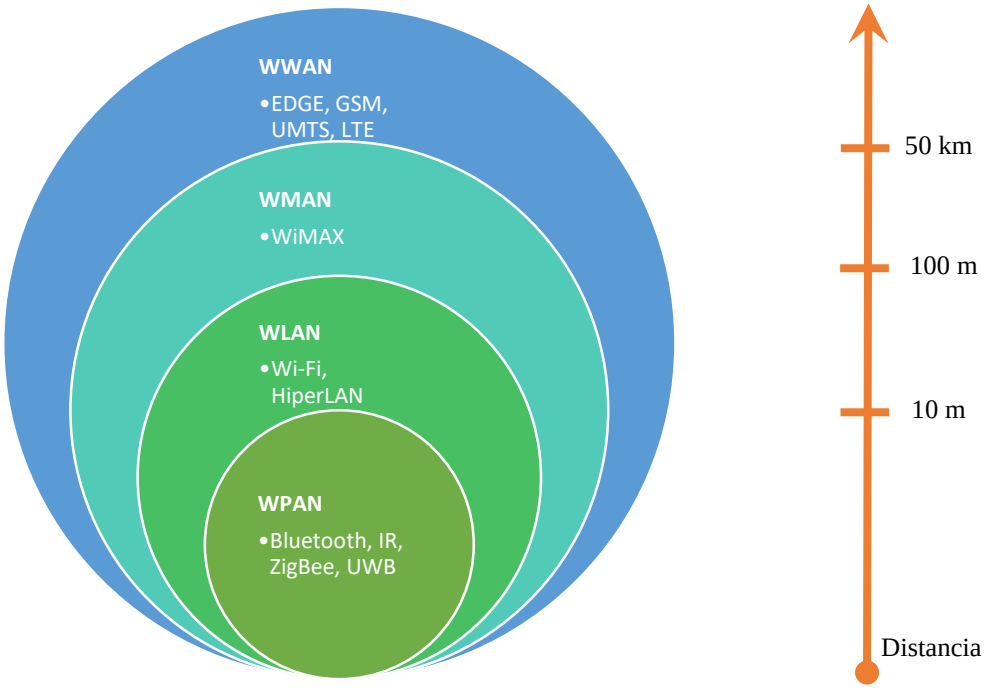
Las tecnologías inalámbricas, en el sentido más simple, permiten que uno o más dispositivos se comuniquen sin conexiones físicas, sin necesidad de cableado de red o periférico. Las tecnologías inalámbricas utilizan transmisiones de radiofrecuencia como medio para transmitir datos, mientras que las tecnologías alámbricas utilizan cables. Las tecnologías inalámbricas van desde sistemas complejos, como Redes de Área Local Inalámbricas (Wireless Local Area Networks, WLAN) y teléfonos celulares, hasta dispositivos simples, como auriculares inalámbricos, micrófonos y otros dispositivos que no procesan ni almacenan información. También incluyen dispositivos Infrarrojos (IR) como controles remotos, algunos teclados y ratones de computadora inalámbricos y auriculares estéreo de alta fidelidad inalámbricos, todos los cuales requieren una línea de visión directa entre el transmisor y el receptor para cerrar el enlace.

Las redes inalámbricas son muchas y diversas, pero con frecuencia se clasifican en cuatro grupos según su rango de cobertura: Redes Inalámbricas de Área Amplia (Wireless Wide Area Networks, WWAN), Redes Inalámbricas de Área Metropolitana (Wireless Metropolitan Area Networks, WMAN), WLAN y Redes Inalámbricas de Área Personal (Wireless Personal Area Networks, WPAN), ver Figura 1. WWAN incluye tecnologías de área de cobertura amplia como celular 2G, Paquete de Datos Digitales Celulares (Cellular Digital Packet Data, CDPD), Sistema Global para Comunicaciones Móviles (Global System for Mobile Communications, GSM), 4G y hasta 5G. WMAN incluye la tecnología de WiMAX. WLAN, incluye 802.11, HiperLAN y varios otros. WPAN representa tecnologías de redes de área personal inalámbricas como Bluetooth e IR. Todas estas tecnologías son "sin ataduras": reciben y transmiten información mediante Ondas Electromagnéticas (EM). Las tecnologías

inalámbricas utilizan longitudes de onda que van desde la banda de radiofrecuencia (radio frequency, RF) hasta la banda IR y por encima de ella.

Figura 1

Tipos de tecnologías inalámbricas según su rango de cobertura.



Nota. Adaptado de *Clasificación de las redes inalámbricas* (p. 7), por J. Salazar, 2015, TechPedia.

WPAN

Las redes inalámbricas de área personal (WPAN), actualmente tiene tres tecnologías que son Infrarrojos (IR), Bluetooth y ZigBee. Sin embargo, IR requiere una línea de visión directa y el rango es menor. Las WPAN se utilizan para transmitir información en distancias cortas (alrededor de 10 metros) entre un grupo privado e íntimo de dispositivos participantes. Una conexión realizada a través de una WPAN implica poca o ninguna infraestructura o conectividad directa con el mundo fuera del enlace. Esto permite implementar soluciones pequeñas, económicas y de bajo consumo para una amplia gama de dispositivos (Sharma & Dhir, 2014).

Tres organismos de normalización son los principales responsables de implementar las WPAN:

- Bluetooth: una tecnología WPAN ampliamente utilizada. El estándar IEEE 802.15.1 especifica la arquitectura y el funcionamiento de los dispositivos Bluetooth, pero solo en lo que respecta a la operación de la capa física y la capa de control de acceso al medio (MAC) (la arquitectura del sistema central). Las capas de protocolo más altas y las aplicaciones definidas en los perfiles de uso están estandarizadas por Bluetooth SIG (Special Interests Group).
- ZigBee: la tecnología ZigBee es más simple (y menos costosa) que Bluetooth. Los principales objetivos de las LR-WPAN (Low-Rate WPAN) como ZigBee son la facilidad de instalación, la transferencia de datos confiable, la operación de corto alcance, el costo extremadamente bajo y una duración razonable de la batería, manteniendo un protocolo simple y flexible. La tasa de datos sin procesar será lo suficientemente alta (máximo de 250 Kbit/s) para satisfacer un conjunto de necesidades simples, como juguetes interactivos, pero también es escalable para satisfacer las necesidades de sensores y automatización (20 Kbit/s o menos) usando comunicación inalámbrica.
- UWB (Ultra Wideband) sobre IEEE 802.15.3: UWB ha atraído mucho la atención recientemente como una comunicación inalámbrica de alta velocidad de corto alcance en interiores. Una de las características más emocionantes de UWB es que su ancho de banda supera los 110 Mbps (hasta 480 Mbps), lo que puede satisfacer la mayoría de las aplicaciones multimedia, como la entrega de audio y video en redes domésticas, y también puede actuar como un reemplazo de cable inalámbrico de bus serial de alta velocidad como USB 2.0.

WLAN

Las redes inalámbricas de área local (WLAN), permiten a los usuarios en un área local, como un campus universitario o una biblioteca, formar una red u obtener acceso a Internet. Una red temporal puede estar formada por un número limitado de usuarios sin necesidad de un punto de acceso; dado que no necesitan acceso a los recursos de la red (Sharma & Dhir, 2014).

Dos organismos de normalización son los principales responsables de implementar WLAN:

- IEEE802.11: Es una organización sin fines de lucro que brinda acciones para coordinar producir y promover estándares de redes de datos. Define el proceso mecánico de cómo se implementan las WLAN en los estándares 802.11 para que los proveedores puedan crear productos compatibles. Especifica la gestión de asociaciones de seguridad y la gestión de claves, así como el control de acceso, la confidencialidad de los datos y la integridad de los datos.
- The Wi-Fi Alliance: Básicamente, certifica a las empresas al garantizar que sus productos sigan los estándares 802.11, lo que permite a los clientes comprar productos WLAN de diferentes proveedores sin tener que preocuparse por ningún problema de compatibilidad.

Las redes WLAN, utilizan diferentes métodos de transmisión de datos, en el libro de Garg, 2010, expone tres métodos, los cuales son:

- Direct Sequence Spread Spectrum: DSSS utiliza un canal para enviar datos a través de todas las frecuencias dentro de ese canal. La codificación de código complementario (CCK) es un método para codificar transmisiones para velocidades de datos más altas, como 5,5 y 11 Mbps, pero aún permite la compatibilidad con versiones anteriores del estándar 802.11 original, que solo admite velocidades de 1 y 2 Mbps.

- Orthogonal Frequency Division Multiplexing: OFDM aumenta las tasas de datos mediante el uso de una modulación de espectro ensanchado.
- Multiple Input Multiple Output: transmisión MIMO, que utiliza DSSS y/o OFDM al difundir su señal a través de 14 canales superpuestos a intervalos de 5 MHz. Requiere varias antenas.

WMAN

La tecnología de las redes inalámbricas de área metropolitana (WMAN) permite la conexión de múltiples redes en un área metropolitana como diferentes edificios de una ciudad, lo que puede ser una alternativa o respaldo al tendido de cableado de cobre o fibra.

Un organismo de normalización es el principal responsable de implementar las WMAN. IEEE 802.16 WiMAX (Worldwide Interoperability for Microwave Access), es un estándar de banda ancha inalámbrica reciente que ha prometido un gran ancho de banda en transmisiones de largo alcance. Es una tecnología de radiofrecuencia que utiliza licencias y bandas sin licencia para proporcionar conexiones inalámbricas para implementaciones reales sin visibilidad directa con una velocidad de hasta 40 Mbps por canal y un radio de celda de hasta 10 kilómetros para situaciones de acceso fijo y portátil. En la línea de vista, WiMAX puede proporcionar una distancia de enlace de hasta 50 kilómetros (Salazar, 2015).

El estándar especifica la interfaz aérea, incluidas las capas de control de acceso al medio (MAC) y física (PHY). El desarrollo clave en la capa PHY incluye la OFDM, en la que el acceso múltiple se logra mediante la asignación de un subconjunto de subportadoras a cada usuario individual. En un sistema OFDM, los datos se dividen en múltiples subflujos paralelos a una tasa de datos reducida, y cada uno se modula y transmite en una subportadora ortogonal separada. Esto aumenta la duración del símbolo y mejora la solidez del sistema (Salazar, 2015).

WWAN

Las redes inalámbricas de área amplia (WWAN) se pueden mantener en grandes áreas, como ciudades o países, a través de múltiples sistemas satelitales o sitios de antena atendidos por un ISP.

CDPD: Cellular Digital Packet Data, es una técnica utilizada para transmitir pequeñas unidades de datos, comúnmente denominadas paquetes, a través de la red celular de manera confiable. Permite enviar y recibir datos desde cualquier lugar del área de cobertura celular en cualquier momento, de forma rápida y eficiente. La tecnología CDPD proporciona servicios de datos amplios, de alta velocidad, alta capacidad y rentables a los usuarios móviles. Con esta tecnología, tanto la voz como los datos se pueden transmitir a través de los canales celulares existentes (Rao, Bojkovic, & Milovanovic, 2010).

3G: Tercera generación es el término para la última generación de servicios móviles, que brindan comunicaciones de voz avanzadas y conectividad de datos de alta velocidad, incluido el acceso a Internet, aplicaciones de datos móviles y contenido multimedia. La Unión Internacional de Telecomunicaciones (ITU), trabajando con grupos de estándares de la industria de todo el mundo, ha definido los requisitos y estándares técnicos, así como el espectro para los sistemas 3G bajo el programa International Mobile Telecommunications-2000 (IMT-2000) (Rao, Bojkovic, & Milovanovic, 2010).

IEEE 802.11 – Wi-Fi

Wi-Fi se ha convertido en una necesidad en el mundo actual. Ha evolucionado hasta convertirse en un servicio fundamental, como la electricidad y el agua, que todos, sin pensarlo, esperan que esté disponible en todas partes, independientemente de si se trata de una escuela, un hotel, un restaurante, un estadio, un edificio de oficinas o incluso el transporte público.

Wi-Fi es una tecnología de red de área local inalámbrica (WLAN), esencialmente un reemplazo de Ethernet que permite que los dispositivos se conecten a Internet sin estar atados

por cables o alambres. Se basa en los estándares 802.11 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). La ausencia de alambres y cables amplía el acceso a lugares donde los alambres y cables no pueden llegar. Esto también reduce el costo de implementación de la red, ya que evita la excavación de zanjas y la perforación necesarias para crear conexiones físicas.

Los dispositivos habilitados para Wi-Fi pueden conectarse a Internet a través de un punto de acceso inalámbrico (AP). Los puntos de acceso tienen un alcance de entre 10 y 30 metros en interiores, y el alcance puede ser mucho mayor en exteriores. Cientos de millones de puntos de acceso Wi-Fi conectan miles de millones de computadoras, teléfonos inteligentes, televisores inteligentes, consolas de juegos, cámaras, impresoras, dispositivos de Internet de las cosas (IoT) y otros dispositivos de consumo a Internet para permitir que millones de aplicaciones lleguen a todos, en todas partes.

Uno de los principales catalizadores de la adopción generalizada de Wi-Fi es la decisión de los organismos reguladores de todo el mundo de poner a disposición bloques significativos de espectro exentos de licencia. A diferencia de las bandas con licencia, donde el protocolo de comunicación inalámbrica que se utilizará es obligatorio como parte del proceso de concesión de licencias, no se especificaron protocolos para estas bandas sin licencia. Este entorno no regulado creó oportunidades para que la industria desarrollara nuevos protocolos de comunicación inalámbrica para diversas aplicaciones, incluida la comunicación de computadora a computadora. Sin embargo, esto dio lugar a que varias empresas desarrollaran productos WLAN que eran incompatibles entre sí. Posteriormente se desarrolló el estándar IEEE 802.11 para garantizar la compatibilidad e interoperabilidad (Gulasekaran & Sankaran, 2022).

Los protocolos Wi-Fi se describen mejor como dos capas: capa de control de acceso medio (MAC) y capa física (PHY). La capa MAC gobierna el acceso al medio al hacer cumplir un conjunto de reglas que dictan cómo acceder al medio para transmitir o recibir datos. Además de esto, la capa MAC es responsable de la gestión de todas las conexiones, así como de la gestión del ahorro de energía. La capa PHY convierte los bits de datos recibidos de la capa

MAC en una forma de onda de radiofrecuencia (RF) para la transmisión y realiza el proceso inverso de convertir la forma de onda RF recibida en bits que se envían a la capa MAC (Gulasekaran & Sankaran, 2022).

IEEE 802.11b – Wi-Fi 1

La generación 1 de Wi-Fi opera en la banda de 2,4 GHz y se basa en el primer estándar 802.11 y la enmienda 802.11b publicada en 1997 y 1999, respectivamente. Utiliza tecnología DSSS y ofrece cuatro velocidades de datos diferentes de 1 Mbps, 2 Mbps, 5,5 Mbps y 11 Mbps. No se emplea ningún código de corrección de errores y el ancho de banda (BW, bandwidth) de transmisión ocupado es de 22 MHz. El encabezado PLCP tiene una longitud de 48 bits y hay dos variantes disponibles para el preámbulo PLCP: preámbulo largo y preámbulo corto. La velocidad de datos para las tramas de control ACK y CTS es obligatoria de 1 Mbps (Gulasekaran & Sankaran, 2022).

IEEE 802.11a – Wi-Fi 2

La generación 2 de Wi-Fi se basa en el estándar 802.11a lanzado el mismo año que 802.11b, pero los dispositivos de consumo tardaron algunos años más en adoptarlo debido al mayor costo de implementación. La capa PHY del 802.11a se basa en la tecnología OFDM, que es un esquema de modulación multiportadora. En la modulación multiportadora, la transmisión BW se divide en subcanales estrechos y el flujo de bits de información se divide en un número igual de flujos de bits paralelos. La frecuencia central de cada subcanal se llama subportadora. Cada flujo de bits modula una de las subportadoras y se suman las salidas moduladas en todos los flujos de bits. OFDM es una forma específica de modulación multiportadora, donde los subcanales se superponen a la mitad, pero son ortogonales, lo que da como resultado una alta eficiencia espectral. Para combatir la interferencia entre símbolos (ISI, inter symbol interference) debida a rutas múltiples, se agrega como prefijo a la forma de onda transmitida un prefijo cíclico (CP, cyclic prefix) o un intervalo de guarda (GI, guard interval) de duración mayor que la propagación del retardo del canal inalámbrico. La dispersión

del retardo del canal se define como la diferencia entre el componente de trayectos múltiples que llega más temprano y el componente de trayectos múltiples que llega más tarde. Aunque GI es una sobrecarga, simplifica significativamente el proceso de demodulación en el receptor. La modulación y demodulación multiportadora en OFDM se puede implementar utilizando operaciones eficientes de transformada de Fourier rápida inversa (IFFT, inverse fast Fourier transform) y transformada de Fourier rápida (FFT, fast Fourier transform) (Gulasekaran & Sankaran, 2022).

IEEE 802.11g – Wi-Fi 3

Aunque como tecnología, OFDM en Wi-Fi 2 demostró ser superior a DSSS en Wi-Fi 1, la adopción por parte del consumidor resultó ser muy lenta porque Wi-Fi 2 requería agregar una banda de radio de 5 GHz, que era costosa en ese momento. Para abordar la necesidad inmediata de menor costo y velocidades de datos más altas en la banda de 2,4 GHz, se introdujo el estándar 802.11g en 2003. La tercera generación de Wi-Fi basada en 802.11g agregó algunos cambios menores para la compatibilidad con 802.11b para hacer que el 802.11a OFDM PHY funciona en la banda de 2,4 GHz. Se requiere que todos los dispositivos Wi-Fi 3 sean compatibles con Wi-Fi 1 y empleen una velocidad de datos de 1 Mbps para todos los marcos de transmisión y marcos de administración. Wi-Fi 3 logró la compatibilidad con versiones anteriores al agregar un modo de protección en el que todas las transmisiones OFDM están protegidas con un intercambio de tramas RTS-CTS a una velocidad de datos de 1 Mbps, de modo que los dispositivos Wi-Fi 1 no interfieran. Un AP Wi-Fi 3 indica a todas las STA que deben emplear el modo de protección configurando el subcampo del modo de protección en 1 en ERP IE de la trama de beacon. Además, un AP indica a todas las STA que utilicen un intervalo de tiempo de 20 µs configurando el subcampo de tiempo de intervalo corto en 0 en el IE de información de capacidad de los beacon. Un AP Wi-Fi 3 anuncia el modo de protección y no permite un espacio de tiempo breve al detectar un AP Wi-Fi 1 en sus proximidades o si se conecta una STA Wi-Fi 1. Debido a su reutilización de Wi-Fi 2 en gran parte con solo cambios

menores, los dispositivos Wi-Fi 3 se comercializaron rápidamente y obtuvieron una tracción fenomenal entre los consumidores (Gulasekaran & Sankaran, 2022).

IEEE 802.11n – Wi-Fi 4

En 2009, se introdujo Wi-Fi 4 basado en 802.11n y admitió el funcionamiento en las bandas de 2,4 GHz y 5 GHz. Wi-Fi 4 aumentó significativamente la eficiencia espectral utilizando una nueva característica llamada multiplexación espacial basada en la tecnología MIMO OFDM. Es bien sabido que la eficiencia espectral de cualquier sistema de comunicación escala logarítmicamente con la relación señal-ruido (SNR, signal-to-noise ratio) en el receptor. Por lo tanto, un aumento exponencial en SNR (o potencia de transmisión equivalente) proporciona solo un aumento lineal en la eficiencia espectral. MIMO es una técnica alternativa para aumentar la eficiencia espectral al transmitir y recibir múltiples flujos de datos al mismo tiempo utilizando múltiples antenas. Wi-Fi 4 combina MIMO con OFDM para permitir una alta eficiencia espectral junto con resiliencia de trayectos múltiples. Wi-Fi 4 también agregó otras funciones de capa PHY, como transmisión de 40 MHz BW, GI corto y verificación de paridad de baja densidad (LDPC, low density parity check) para aumentar la tasa de datos y el rendimiento de corrección de errores. La capa PHY de 802.11n se denomina capa HT PHY, por lo que cualquier trama transmitida mediante la velocidad de datos de Wi-Fi 4 también se conoce como trama HT (Gulasekaran & Sankaran, 2022).

IEEE 802.11ac – Wi-Fi 5

La quinta generación de Wi-Fi se introdujo en 2013 según el estándar 802.11ac y solo admite la banda de 5 GHz. Wi-Fi 5 es retro compatible con dispositivos Wi-Fi 4 y Wi-Fi 2. La capa PHY de Wi-Fi 5 se llama VHT PHY. Wi-Fi 5 amplió principalmente las ideas de MIMO y el aumento del ancho de banda en Wi-Fi 4 para aumentar significativamente la tasa de datos. Agregó soporte para anchos de banda en transmisión de 80 MHz y 160 MHz al tiempo que aumentó el NSS máximo a 8. También se agregó soporte opcional para modulación 256-QAM. La asignación de subportadora OFDM, las opciones de GI y las opciones de codificación en Wi-

Fi 5 son las mismas que en Wi-Fi 4. Las velocidades de datos compatibles con Wi-Fi 5 pueden llegar a los 433.3 MHz con BW de 80 MHz y hasta 866.7 Mbps con BW de 160 MHz. El NSS, BW, BW admitido y capacidades como LDPC, GI corto, transmisión de beamforming (TxBf) y MIMO multiusuario (MU-MIMO) se anuncian utilizando las capacidades VHT IE. Las nuevas tecnologías introducidas en Wi-Fi 5 son TxBf y MU-MIMO de enlace descendente (DL). Aunque técnicamente, 802.11n fue el primer estándar en introducir la función TxBf, no tuvo éxito debido a las múltiples variantes opcionales que generaron problemas de interoperabilidad entre los puntos de acceso y los proveedores de clientes. Estos errores se corrigieron en Wi-Fi 5 al admitir solo una variante de TxBf y garantizar la interoperabilidad a través de la certificación WFA (Gulasekaran & Sankaran, 2022).

IEEE 802.11x – Wi-Fi 6

Wi-Fi 6 es la sexta generación de Wi-Fi presentada en 2019 basada en el estándar IEEE 802.11ax. Mientras que las generaciones anteriores de Wi-Fi se centraron en aumentar las tasas máximas de datos, Wi-Fi 6 se trata principalmente de aumentar la eficiencia en una red con varios puntos de acceso (físicos y virtuales), varios clientes y cargas de tráfico variadas. La capa PHY de Wi-Fi 6 se llama PHY de alta eficiencia (HE, high efficiency) y se esfuerza por maximizar todas las métricas de eficiencia posibles en la capa PHY mientras mantiene la compatibilidad con versiones anteriores de Wi-Fi. Aunque mejorar la eficiencia es el objetivo principal, Wi-Fi 6 también aumenta la tasa de datos máxima al aprovechar la modulación 1024-QAM. Wi-Fi 6 aborda algunos problemas, como el alto tiempo de aire ocupado por el tráfico de administración, la baja eficiencia del tiempo de aire en marcos de datos cortos y el desperdicio de tiempo de aire debido a colisiones y retrocesos aleatorios (RBO, random backoff), que comúnmente se encuentran en implementaciones de alta densidad. En las primeras cuatro generaciones de Wi-Fi, compartir recursos en la dimensión del tiempo era la única forma en que múltiples clientes compartían el medio. Con la introducción de MU-MIMO en Wi-Fi 5, los flujos espaciales se convirtieron en otra dimensión

para que varios clientes compartieran el medio, pero esto se limitaba solo al tráfico de enlace descendente (DL). Hasta Wi-Fi 5, el AP no tiene control sobre la programación del tráfico de enlace ascendente (UL) y todos los clientes tienen que competir por el acceso al medio. Con la tecnología de acceso múltiple por división de frecuencia ortogonal (OFDMA, orthogonal frequency division multiple access) y la tecnología MU-MIMO, Wi-Fi 6 permite que el AP realice la asignación de recursos para el tráfico de enlace descendente y ascendente en tres dimensiones. Wi-Fi 6 también presenta nuevos mecanismos de ahorro de energía para que AP programe los tiempos de activación de la estación (STA), lo que reduce el consumo de energía de STA y las colisiones en el medio. Wi-Fi 6 presenta un nuevo modo de operación de múltiples puntos de acceso virtual (VAP, virtual access point) llamado enhanced multi-BSSID advertisement (EMA) para reducir la respuesta de la sonda y el tráfico de beacon en la operación de múltiples VAP o BSSID. Finalmente, para facilitar una mayor reutilización espacial en implementaciones de puntos de acceso de alta densidad, Wi-Fi 6 introduce colores BSS y reutilización espacial. En resumen, Wi-Fi 6 ofrece varias características nuevas con suficiente flexibilidad para abordar una amplia gama de casos de uso en diversas implementaciones (Gulasekaran & Sankaran, 2022).

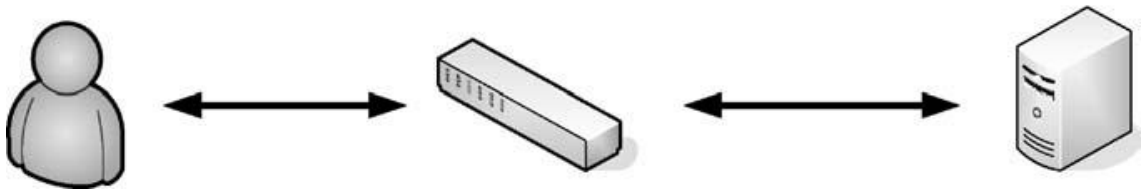
IEEE 802.1X

De manera muy simple, 802.1X es un protocolo de capa 2 que se utiliza para respaldar la determinación de si las credenciales proporcionadas por un dispositivo que desea conectarse a una red son suficientes para permitir la conexión (Brown, 2008).

Desde una perspectiva física, 802.1X consta de tres entidades: un dispositivo que intenta conectarse a una red, un segundo dispositivo que alberga el punto de conexión deseado y una base de datos que contiene información de credenciales utilizada para validar la conexión (Brown, 2008). Estos dispositivos se denominan suplicante, autenticador y servidor de autenticación, respectivamente. La Figura 2 ilustra las tres entidades.

Figura 2

Comunicación básica del 802.1X.



Nota. Adaptado de *802.1X Port-Based Authenticationation* (p. 4), por E. L. Brown, 2008, Auerbach Publications.

Estos tres dispositivos ejecutan tres conversaciones lógicas diferentes para realizar una autenticación. Dos de las conversaciones son intercambios físicos. El suplicante y el autenticador tienen una conversación física, y el autenticador y el servidor de autenticación tienen una conversación física. Ambas conversaciones pueden verse como transferencias de datos. Las conversaciones físicas en realidad apoyan el intercambio de información de credenciales entre el suplicante y el servidor de autenticación. Esta es la conversación completamente lógica.

Las tres conversaciones, y todos los protocolos empleados, se denominan comúnmente 802.1X; pero, en verdad, solo la conversación física entre el autenticador y el suplicante es 802.1X — EAPoL. La comunicación física entre el servidor de autenticación y el autenticador se realiza mediante el protocolo RADIUS. La conversación lógica entre el servidor de autenticación y el suplicante se lleva a cabo utilizando EAP y EAP-Methods (Brown, 2008).

¿Cómo funciona el 802.1X?

El suplicante y el autenticador conversan, y el autenticador y el servidor de autenticación conversan; pero el Suplicante y el Servidor de Autenticación nunca conversan directamente. Este es un concepto fundamental. El autenticador es siempre el destinatario, el traductor y el intermediario de todas las conversaciones entre los dos puntos finales. 802.1X es eficaz porque

no permite que un suplicante se comunique con la red antes de la autenticación. En realidad, existe una situación en la que un Suplicante no autenticado puede comunicarse con un dispositivo en la red. Esa situación tiene que ver con informar las condiciones ambientales y se discutirá en secciones posteriores. A todos los efectos prácticos, no se permite ninguna comunicación desde un dispositivo que intenta conectarse hasta que se haya completado el proceso de autenticación. Hay una gran cantidad de gofres en esa declaración, pero es correcta.

Cada endpoint, suplicante o servidor de autenticación, habla solo con el autenticador, y el autenticador reenvía la información de uno a otro. Cuando el Autenticador y el Suplicante conversan, está estrictamente dentro del protocolo EAPoL en la Capa 2. Esto impide que el Suplicante haga otra cosa que no sea conversar con el Autenticador y usar cualquier cosa que no sea ese protocolo para hacerlo. Todo lo que el Suplicante intente hacer fuera de ese protocolo se ignorará. Es posible configurar el proceso de autenticación para permitir un tráfico muy específico de la red al Suplicante en una instancia específica. Esto tiene como objetivo permitir que otro dispositivo residente en la LAN "despierte" a un suplicante y haga que el suplicante participe plenamente en el proceso 802.1X.

Debido a que 802.1X es un protocolo de capa de enlace, debería tener sentido que todo comience cuando se establece el enlace. Tan pronto como se establece el enlace, el autenticador exige credenciales de identidad en el enlace que se activó. Utiliza una trama EAPoL denominada Solicitud de identidad. Si hay un suplicante en el otro extremo del enlace, responderá con un paquete de respuesta. El autenticador aceptará la respuesta, la volverá a empaquetar y la reenviará al servidor de autenticación mediante el protocolo RADIUS. No se permitirá que se transmita nada desde el Suplicante; al menos, el Autenticador no responderá a nada más que a los paquetes EAPoL del Suplicante. El servidor de autenticación responderá al autenticador mediante el protocolo RADIUS. El autenticador volverá a empaquetar los datos del servidor de autenticación y los reenviará al suplicante mediante un paquete de protocolo

EAPoL, una identidad de solicitud. Este tipo de conversación continuará hasta que se complete el proceso de autenticación. En ese momento, el servidor de autenticación notificará al autenticador si se ha realizado correctamente o no. El autenticador pasará esta información al suplicante, pero también actuará en consecuencia. Permitirá que el suplicante ingrese a una VLAN autorizada o no. Es posible colocar suplicantes no autorizados, o dispositivos que no tienen suplicantes, en una VLAN especial llamada VLAN invitada.

Existen múltiples posibilidades para la asignación de una VLAN al dispositivo de conexión. Primero, hay una VLAN que está asociada con el puerto. Esta VLAN se define en la configuración del puerto de la misma manera que un puerto sin 802.1X habilitado tiene una VLAN configurada para ello. Esto es lo que se conoce como VLAN autorizada porque normalmente permitirá el acceso a algún tipo de recursos corporativos y, a menudo, es la VLAN a la que se asignará un suplicante autenticado. El Suplicante autenticado también puede tener una VLAN asignada a las credenciales en el servidor RADIUS. Esta VLAN se aplica dinámicamente después de una autenticación exitosa. La VLAN invitada se identificó en el párrafo anterior. Se puede configurar en un puerto que tenga habilitado 802.1X. Por lo tanto, existen varias posibilidades con respecto a la asignación de VLAN para un dispositivo que intenta conectarse a una red. Van desde ninguna VLAN hasta una elegida específicamente para el usuario en particular.

Las conversaciones lógicas entre el Suplicante y el Servidor de Autenticación carecen prácticamente de sentido para el Autenticador. Es decir: hasta que el Autenticador finalmente reciba un mensaje del Servidor de Autenticación indicando éxito o fracaso. Si se indica éxito, el autenticador realizará alguna actividad en función del mensaje de éxito y autorizará el puerto a una VLAN específica. Si se indica una falla, el Autenticador le dirá al Suplicante que se vaya y mantenga el puerto en un estado no autorizado. En algunas implementaciones, es posible que un suplicante que no se puede autenticar se coloque en una VLAN invitada.

EAPoL (Extensible Authentication Protocol over LAN)

EAPoL o protocolo de autenticación extensible a través de LAN es un protocolo de autenticación de puerto de red utilizado en IEEE 802.1X desarrollado para proporcionar un inicio de sesión de red genérico para acceder a los recursos de la red, que se usa entre el suplicante y el autenticador (Brown, 2008).

La especificación 802.1X creó la encapsulación EAPoL del paquete EAP como se definió inicialmente en RFC 2284. EAPoL consta de cuatro campos: Version, Type, Length (datos) y EAP Data. Actualmente, Version solo se establecerá en 1. Type identifica el tipo de función que se solicita. Length es la longitud de los datos, y EAP Data forman la trama EAP encapsulada en sí. La trama EAPoL se muestra en la Figura 3.

Figura 3

Trama EAPoL con datos EAP encapsulados.

Version (1 byte)	Type (1 byte)	Length (2 bytes)	EAP Data (0-n bytes)

Version:	01
Type:	Función solicitada
Length:	Longitud de los datos EAP
EAP Data:	Trama EAP

Nota. Adaptado de *802.1X Port-Based Authentication* (p. 46), por E. L. Brown, 2008, Auerbach Publications.

En total, hay cinco tipos de EAPoL posibles como se muestra en la Tabla 1.

- El tipo 0, EAPoL Data, es un marco EAP y no requiere procesamiento EAPoL. EAPoL simplemente lo pasa a la capa EAP. Este tipo generalmente se ve como una solicitud de identidad del autenticador o como una respuesta del suplicante. La mayoría de los paquetes de una conversación serán de este tipo.

Tabla 1

Tipos EAPoL.

Tipo	Descripción
0	EAP Data
1	EAPoL-Start
2	EAPoL-Logoff
3	EAPoL-Key
4	EAPoL- Encapsulated-ASF-Alert

- El tipo 1, EAPoL-Start, se utiliza para decirle al autenticador que debe iniciar el proceso de autenticación. Si el enlace ya está activo, el autenticador no iniciará el proceso.
- El tipo 2, EAPoL-Logoff, se usa para notificar al autenticador que el suplicante se va y devolver el puerto a un estado no autorizado.
- El tipo 3, EAPoL-Key, se utiliza para obtener o distribuir información de clave global entre el autenticador y el suplicante. El uso actual del paquete EAPoL-Key es inalámbrico (802.11). El proceso consiste en un protocolo de enlace de cuatro vías. Los estándares 802.11i definen el protocolo de enlace de cuatro vías de la siguiente manera: primero, se debe establecer una Asociación; segundo, la autenticación 802.1X normal debe tener éxito; tercero y cuarto, el intercambio de información clave debe realizarse entre el autenticador y el suplicante. El intercambio de información clave puede tener lugar una o más veces durante la vida útil de una conexión y puede ser iniciado por el suplicante o el autenticador.
- El tipo 4, EAPoL- Encapsulated-ASF-Alert, está diseñado para permitir que se produzcan "alertas" sin el requisito de autenticación. El requisito para que el dispositivo participe en 802.1X permanece, pero se permite declarar una emergencia sin requerir autenticación mediante el uso de este tipo de paquete.

EAP (Extensible Authentication Protocol)

EAP o protocolo de autenticación extensible es un protocolo simple con una sola función. Se utiliza para transportar y administrar información de autenticación entre el suplicante y el servidor de autenticación (Brown, 2008). Esto incluye la negociación de cómo se llevará a cabo la autenticación, qué método se utilizará, el intercambio de credenciales definido en el método y la declaración final de éxito o fracaso.

EAP fue creado para ser implementado en el protocolo Point-To-Point (PPP). PPP es un protocolo utilizado para la comunicación que tiene lugar en un enlace en serie. Las características PPP son fundamentales en el concepto de EAP. IEEE 802.1X aprovecha la topología de PPP y asume una arquitectura simple de un solo dispositivo que se conecta a un solo puerto en una red. Por lo tanto, 802.1X funciona en la Capa 2 del modelo OSI y se puede operar antes de permitir cualquier comunicación en el puerto (Stanley, Walker, & Aboba, 2005).

El flujo del 802.1X consiste en que el autenticador emite un paquete de Request-Identity. El suplicante emitirá un Response. El autenticador eliminará toda la encapsulación del paquete, volverá a encapsular el mensaje EAP y lo reenviará al servidor de autenticación. El servidor de autenticación procesará los datos y responderá. Esto continuará hasta que el servidor de autenticación declare Success o Failure (Ali & Al-Khlifa, 2011). Como se esperaba, el número y la sofisticación de los procesos EAP disponibles son muy limitados y la Tabla 2 define los códigos EAP.

Tabla 2

Códigos EAP.

EAP Code	**Número**
Request	1
Response	2
Success	3
Failure	4

Un mensaje EAP consta de cuatro campos: el EAP Code, el Identifier, el Length de los EAP Data y los EAP Data en sí. Los dos primeros campos son los únicos campos realmente pertinentes a EAP. El primero, EAP Code, identifica qué tipo de paquete EAP se está utilizando y el segundo se utiliza para garantizar la secuenciación correcta. La encapsulación EAP se muestra a continuación en la Figura 4.

Figura 4

Trama EAP.

Code (1 byte)	Identifier (1 byte)	Length (2 bytes)	EAP Data (0-n bytes)

Code:	01-04
Identifier:	Número de secuencia del paso de bloqueo
Length:	Longitud de los datos EAP
EAP Data:	Información de autenticación

Nota. Adaptado de *802.1X Port-Based Authentication* (p. 52), por E. L. Brown, 2008, Auerbach Publications.

Es responsabilidad del autenticador asegurarse de que haya recibido una respuesta a cada solicitud enviada al suplicante. Es posible que el autenticador envíe una solicitud y que el suplicante responda a una diferente. Esto se controla con un proceso de "paso de bloqueo", que es un método primitivo para garantizar un transporte confiable. Un proceso de paso de bloque es aquel en el que una acción realizada por un "líder" debe ser seguida exactamente por un "subordinado". En este caso, el proceso de paso de bloqueo es un indicador de que cada participante en la conversación está hablando de la misma información. Debido a que las solicitudes provienen del autenticador y las respuestas del suplicante, el autenticador siempre debe ser el que indique nueva información en este intercambio, y el suplicante solo puede responder a la solicitud de información actual (Brown, 2008).

El campo identifier se utiliza para implementar el paso de bloqueo. El autenticador establecerá el identificador en un valor específico. El suplicante se hará eco de este valor en su respuesta. El autenticador cambiará el valor del identifier para la próxima solicitud y el suplicante hará eco del nuevo valor en su respuesta.

EAP-Method

Un EAP-Method es la forma en que se realiza una autenticación en particular. En cierto sentido, un EAP-Method es una autenticación. Es un método particular que se utiliza para ejecutar una autenticación utilizando EAP como mecanismo de transporte (Brown, 2008). Los EAP-Methods se definen para varias formas de autenticación. Hay muchos métodos que se han definido. Algunos utilizan certificados, otros utilizan nombre de usuario/contraseña, y algunos son métodos de tunelización de información entre el suplicante y el servidor de autenticación. Por muy diversos que se vuelvan, todos y cada uno siempre estarán encapsulados en EAP entre el Suplicante y el Autenticador.

EAP es el protocolo utilizado para transportar el EAP-Method. El funcionamiento correcto del método está controlado por la información transportada y no por el protocolo del EAP-Method en sí. Sin embargo, el tipo de EAP-Method tiene significado en el número de intercambios entre el Suplicante y el Servidor de Autenticación. El número de intercambios y, hasta cierto punto, la dirección de los intercambios (pares de solicitud/respuesta) depende del método implementado. El Suplicante y el Servidor de Autenticación procesan estos datos de acuerdo con el algoritmo definido para el método particular elegido para la autenticación (Abo-Soliman & Azer, 2018).

La información del EAP-Method consta de tres campos: el código del EAP-Method, la longitud de los datos del EAP-Method y los datos del EAP-Method. Esto se ilustra en la Figura 5, con la definición de cada campo.

Figura 5

Trama EAP-Method.

EAP-Method Code (1 byte)	Length (2 bytes)	EAP-Method Data (0-n bytes)

Code: 01-255
Length: Longitud de los datos EAP-Method
EAP-Method Data: Información de autenticación

Nota. Adaptado de *802.1X Port-Based Authentication* (p. 54), por E. L. Brown, 2008, Auerbach Publications.

El Suplicante y el Servidor de Autenticación realmente negocian el EAP-Method, el campo Tipo, que se utilizará en el proceso de autenticación. El campo Tipo identifica la "desencapsulación de protocolo" de los datos contenidos en la porción de datos EAP del paquete. El tipo puede identificar una directiva/solicitud a la parte receptora o puede contener datos para ser utilizados por el método de autenticación. El EAP-Method es en realidad otro agujero en el suelo para introducir credenciales específicas (Brown, 2008). La Tabla 3 muestra los tipos actuales definidos.

Tabla 3

Tipos de EAP-Methods.

Tipo EAP-Method	**Número**
Identity	1
Notification	2
NAK (response only)	3
MD5-Challenge	4
One-Time Password (OTP)	5
Generic Token Card (GTC)	6
Expanded NAK	254
Experimental	255

Identity, tipo 1, se utiliza para transmitir información sobre las credenciales de cualquiera, o ambos, el Suplicante y el Servidor de Autenticación. Esto significa que la conversación entre el Autenticador y el Suplicante consistirá en respuestas e identidad de solicitud de EAP. Este es el escenario deseado, porque los intercambios de identidad significan que el proceso ha llegado al punto en el que se está intercambiando información de autenticación y conducirá al éxito o al fracaso.

Notification, tipo 2. El Servidor de autenticación envía un Tipo 2 al Suplicante y contiene información sobre el estado de la autenticación.

NAK, tipo 3. El suplicante envía un tipo 3, NAK, al servidor de autenticación cuando el Suplicante rechaza el método de autenticación propuesto.

One-Time Password (OTP), tipo 5, proporciona autenticación para el acceso al sistema (inicio de sesión) y otras aplicaciones que requieren autenticación segura contra ataques pasivos basados en la reproducción de contraseñas reutilizables capturadas.

Generic Token Card (GTC), tipo 6, se define para su uso con varias implementaciones de tarjeta de token que requieren la entrada del usuario. La Solicitud contiene un mensaje visualizable y la Respuesta contiene la información de la Tarjeta Token necesaria para la autenticación.

Expanded NAK, tipo 254, permite al Suplicante proponer un método de autenticación. El uso del Expanded NAK permite una convergencia más rápida para la selección de un método de autenticación.

Métodos de Autenticación del EAP

La autenticación del Protocolo de autenticación extensible (EAP) tiene varios métodos de autenticación disponibles, y la mayoría de ellos se basan en la Seguridad de la capa de transporte (TLS, Transport Layer Security). El método que se elija depende de los requisitos de seguridad y de si el método EAP es compatible con los suplicantes y el servidor de autenticación.

Actualmente hay más de 40 métodos EAP diferentes disponibles. Estos métodos EAP se pueden dividir en cuatro categorías diferentes: métodos legacy, métodos basados en certificados, métodos basados en contraseñas y métodos basados en contraseñas seguras. A continuación, en la Tabla 4 se enumeran los métodos de autenticación del protocolo EAP más comunes.

Tabla 4

Métodos de autenticación EAP.

Categoría	**Método**
Método Legacy o Método heredado	CHAP, EAP-MD5
Método basado en certificados	EAP-TLS, EAP-TTLS, PEAP
Método basado en contraseñas	EAP-LEAP, EAP-FAST
Método basado en contraseñas seguras	EAP-SPEKE

Métodos EAP legacy

Los métodos EAP legacy son los métodos EAP que se definieron por primera vez en RFC 3748 (Aboba, Blunk, Vollbrecht, Carlson, & Levkowetz, 2004) junto con EAP o antes de que se estableciera EAP. Los primeros métodos EAP se definieron para autenticar conexiones PPP.

CHAP. El método CHAP significa Challenge Handshake Authentication Protocol. CHAP está definido por RFC 1994 (Simpson, 1996). CHAP se usa para verificar la identidad de un par mediante el uso de un protocolo de enlace de 3 vías. El servidor de autenticación valida al par en el momento en que se realiza el enlace y también puede autenticar aleatoriamente al usuario mientras se realiza la conexión. El servidor de autenticación prueba la autenticidad del par enviando un mensaje de desafío al par. El par calcula un valor utilizando una función hash unidireccional y envía este valor al autenticador. El autenticador calcula su propio valor hash y compara este valor con el valor recibido del par. Si los dos valores coinciden, el par se autentica. Si los dos valores no coinciden, la conexión debe terminarse.

Una de las ventajas de CHAP es que evita el ataque de reproducción mediante el uso de un identificador que cambia gradualmente y un valor de desafío variable. El autenticador controla el tiempo entre desafíos y, por lo tanto, puede limitar el tiempo de exposición a un ataque. Otra ventaja de CHAP es que el método se basa en un secreto compartido, pero el secreto nunca se envía a través del enlace. Una tercera ventaja de CHAP es que se puede usar el mismo método para la autenticación mutua realizando el método en ambas direcciones usando dos secretos diferentes (Simpson, 1996).

Sin embargo, una de las mayores desventajas de CHAP es que el secreto debe estar disponible en ambos extremos en forma de texto sin formato. Esto significa que las bases de datos que cifran de forma irreversible los datos de la contraseña no se pueden utilizar para almacenar el secreto. Otra desventaja de CHAP es que no hay forma de establecer un PMK para el futuro cifrado de datos (Simpson, 1996).

EAP-MD5. El acrónimo, MD5, significa Message Digest 5. Este EAP-Method se basa en el uso del nombre de usuario y la contraseña para completar una autenticación (Orlando & Parsons, 2020). Es una implementación obligatoria dentro de EAP.

Por lo general, este protocolo se utiliza para autenticarse frente a una base de datos interna. El autenticador solicita la identidad del suplicante y la reenvía al servidor de autenticación. El servidor responde con un "Challenge". El Suplicante responde y la autenticación es exitosa o no.

EAP-MD5 utiliza un algoritmo hash para la autenticación en lugar de una contraseña cifrada. Los algoritmos hash no son reversibles como las contraseñas cifradas, por lo que no es posible descifrar el hash. En cambio, el suplicante debe conocer la clave para crear el valor hash esperado. Dado que el hash no se puede revertir, los mensajes no se pueden alterar y es una súplica autorizada (Tobar & Mora, 2016).

Métodos EAP basados en certificados

Los métodos EAP basados en certificados son aquellos métodos EAP que utilizan PKI o infraestructura de clave pública (Public Key) para la autenticación. PKI es un acuerdo que vincula las claves públicas a las identidades de los usuarios por medio de una autoridad de certificación o CA (certificate authority), que también se conoce como un TTP (Trusted Third Party). La vinculación se establece a través del proceso de registro y emisión realizado por software en la CA o bajo supervisión humana. La Autoridad de Registro o RA (Registration Authority) asegura que esta vinculación se realiza con éxito.

Para cada usuario, la identidad del usuario, la clave pública, su vinculación, las condiciones de validez y otros atributos se hacen infalsificables en los certificados de clave pública emitidos por la CA. La PKI típica consta de software de cliente, software de servidor, hardware (tarjetas inteligentes), contratos y garantías legales, y procedimientos operativos.

EAP-TLS. El acrónimo TLS es una abreviatura de Transport Layer Security. EAP-TLS es lo mismo que EAP-MD5, pero utiliza certificados digitales para autenticar al servidor y autentica directamente al suplicante con el servidor de acuerdo con su nombre de usuario y contraseña. El certificado digital debe ser autenticado por la Autoridad Certificadora (CA) (Brown, 2008).

EAP-TLS es el protocolo de autenticación EAP de LAN inalámbrica original. Aunque rara vez se implementa debido a una curva de implementación pronunciada, aunque todavía se considera uno de los estándares EAP más seguros disponibles y es compatible universalmente con todos los fabricantes de hardware y software de LAN inalámbrica. La autenticación de EAP-TLS, es fuerte debido a que del lado del cliente es necesario contar con un certificado instalado en él. Cuando los certificados del lado del cliente están alojados en tarjetas inteligentes, esto ofrece la solución de autenticación más segura disponible porque no hay forma de robar un certificado de una tarjeta inteligente sin robar la tarjeta inteligente en sí (Brown, 2008).

La mayor desventaja de este método, y otros de esta clase, es el costo requerido o la administración de certificados. Si los certificados no se compran de una autoridad reconocida por los dispositivos en la red, entonces se debe establecer un sistema privado. En cualquier caso, el costo de implementación, en dinero o experiencia, puede ser significativo. El entorno que implementa la autenticación basada en certificados se vuelve más complejo y requiere un mayor nivel de administración. Además, el uso de certificados generalmente autentica el dispositivo en el que reside el certificado y no al usuario (Vallejos, 2019). Para algunas organizaciones, esto frustra el propósito de implementar 802.1X.

EAP-TTLS. El acrónimo TTLS es una abreviatura de Tunneled Transport Layer Security. EAP-TTLS es un método EAP que proporciona una funcionalidad más allá de lo que está disponible en EAP-TLS.

En EAP-TLS, se utiliza un protocolo de enlace TLS para autenticar mutuamente un cliente y un servidor. EAP-TTLS extiende esta negociación de autenticación mediante el uso de la conexión segura establecida por el protocolo de enlace TLS para intercambiar información adicional entre el cliente y el servidor (Tobar & Mora, 2016). En EAP-TTLS, la autenticación TLS puede ser mutua; o puede ser unidireccional, en el que solo el servidor se autentica ante el cliente. La conexión segura establecida por el protocolo de enlace se puede utilizar para permitir que el servidor autentique al cliente utilizando las infraestructuras de autenticación existentes ampliamente desplegadas. La autenticación del cliente puede ser en sí misma EAP, o puede ser otro protocolo de autenticación como PAP, CHAP, MS-CHAP o MS-CHAP-V2.

Por lo tanto, EAP-TTLS permite que los protocolos de autenticación legacy basados en contraseñas se utilicen contra las bases de datos de autenticación existentes, al tiempo que protege la seguridad de estos protocolos legacy contra escuchas, intermediarios y otros ataques (Brown, 2008).

PEAP. El acrónimo de PEAP es Protected EAP y tal como sugiere el nombre, PEAP protege los intercambios EAP. Este proceso de autenticación se produce en dos partes. La

primera parte se utiliza para establecer un túnel entre el suplicante y el servidor de autenticación, y la segunda parte es la autenticación real de las credenciales (Brown, 2008).

El flujo de PEAP también es muy similar al de todos los demás métodos 802.1X. El autenticador emite una solicitud de identidad y el suplicante responde. El autenticador reenvía al servidor de autenticación; el servidor responde con un challenge que especifica un inicio PEAP. En ese momento comienza el establecimiento de un túnel TLS.

PEAP aprovecha TLS para crear un túnel seguro que luego se utiliza para transportar credenciales (Abo-Soliman & Azer, 2018). Un método EAP completamente diferente se encapsula dentro del túnel TLS.

Un punto que debe tenerse en cuenta para la implementación de PEAP es que se duplica el esfuerzo de autenticación. Primero, debe ocurrir el establecimiento del túnel TLS. Esto requiere intercambios entre el suplicante y el servidor de autenticación. Luego, la autenticación utilizando otro método EAP debe realizarse a través del túnel. Esto aumenta la complejidad de la autenticación, así como la duración y el volumen de tráfico requerido. Este método parecería ser una mala elección para los usuarios móviles en un entorno inalámbrico.

Métodos EAP basados en contraseñas

En el caso de los métodos EAP basados en contraseña, se utiliza una contraseña para autenticar al usuario y al servidor en lugar de un certificado de clave pública.

EAP-LEAP. LEAP es un método patentado de Cisco, con el acrónimo de Lightweight EAP, el cual se utiliza principalmente en entornos inalámbricos. El protocolo, como EAP-MD5 y EAP-TLS, deja la identidad en claro. Sin embargo, LEAP proporciona autenticación mutua entre el solicitante y el servidor de autenticación. Este protocolo se está eliminando gradualmente a favor de PEAP y EAP-FAST.

LEAP utiliza una versión modificada de MS-CHAP para autenticar tanto al cliente como al servidor. Por lo tanto, EAP-LEAP proporciona autenticación mutua. A diferencia de MS-CHAP, las claves de seguridad cambian dinámicamente con cada sesión de comunicación.

Esto ayuda a evitar que un atacante recopile los paquetes de autenticación necesarios para decodificar los datos.

Probablemente la mayor ventaja de EAP-LEAP es la baja sobrecarga asociada con este método EAP en particular. No hay que preocuparse por los certificados de clave pública, lo que reduce en gran medida la cantidad de problemas administrativos necesarios en la implementación. Además, el uso de un esquema de nombre de usuario/contraseña asegura que el usuario esté autenticado y no el dispositivo que se conecta a la red. Finalmente, el método es rápido y eficiente y requiere muy poco tiempo para la autenticación mutua.

La mayor desventaja de EAP-LEAP es que no proporciona un alto nivel de seguridad. A principios de 2004, Joshua Wright lanzó una herramienta llamada ASLEAP. ASLEAP se puede utilizar para explotar fallas en la seguridad de EAP-LEAP para obtener las contraseñas de usuarios desprevenidos de EAP-LEAP. Después de usar algún tipo de rastreador de paquetes, un pirata informático puede usar ASLEAP para realizar un ataque de diccionario muy simple para determinar la contraseña de los usuarios que se conectan a un punto de acceso de Cisco (Carballar, 2010).

EAP-FAST. FAST son las siglas de Flexible Authentication via Secure Tunneling. EAP-FAST fue diseñado por Cisco como reemplazo de EAP-LEAP después de que se demostró que EAP-LEAP era vulnerable a los ataques de diccionario. El objetivo de EAP-FAST era proporcionar un mayor nivel de seguridad que el logrado por EAP-LEAP y al mismo tiempo mantener la baja sobrecarga asociada con EAP-LEAP (Brown, 2008).

EAP-FAST es en realidad muy similar a EAP-TTLS. EAP-FAST se basa en el uso de TLS para establecer un túnel entre el cliente y el servidor que luego se puede usar para autenticar al cliente mediante el uso de un método de autenticación de contraseña heredado, como CHAP. La gran diferencia entre los métodos EAP basados en certificados y EAP-FAST es que EAP-FAST no requiere que el servidor tenga una certificación de clave pública

(Paredes, 2013). En su lugar, EAP-FAST utiliza un PAC (Protected Access Credential) para establecer el túnel TLS.

Una de las mayores ventajas de EAP-FAST es que proporciona una seguridad muy similar a la de EAP-TTLS o PEAP sin la sobrecarga asociada con el mantenimiento de un certificado de clave pública. Sin embargo, la seguridad asociada con PKI se debe en parte a la existencia de una CA a la que se puede contactar para verificar la autenticidad de un certificado en particular, y no hay una CA presente en este esquema en particular. Otra ventaja de este método es que admite la reconexión rápida.

Una de las mayores desventajas de este método en particular es que se necesitan muchos viajes de ida y vuelta para establecer la conexión inicial entre el usuario y el servidor. Otra desventaja de EAP-FAST es que cuando el aprovisionamiento automático de PAC está habilitado, EAP-FAST tiene una pequeña vulnerabilidad de que un atacante puede interceptar el PAC y usarlo para comprometer las credenciales del usuario.

Métodos EAP basados en contraseñas seguras

Los métodos EAP basados en contraseñas seguras permiten a los usuarios y servidores lograr la autenticación mutua mediante el uso de contraseñas simples que el usuario puede recordar fácilmente. La diferencia entre los métodos EAP basados en contraseñas seguras y los métodos EAP basados en contraseñas es que los métodos EAP basados en contraseñas seguras proporcionan una manera de usar contraseñas para la identificación sin transmitir ningún dato que pueda usarse posteriormente para determinar la contraseña, que es lo único que es necesario para la autenticación. En otras palabras, ambas partes pueden determinar que conocen un secreto con haber revelado alguna vez cuál es el secreto.

EAP-SPEKE. SPEKE es el acrónimo de Simple Password Exponential Key Exchange, es un método EAP propietario de Interlink Networks. El método SPEKE utiliza el conocimiento mutuo de una contraseña tanto en el autenticador como en el cliente para generar una serie de mensajes a intercambiar de contenido aparentemente aleatorio. Una vez que ambas partes

estén de acuerdo en que la contraseña es correcta, se compartirá una clave de sesión maestra entre los dispositivos para su uso posterior. La fuerza adicional de este método se deriva de un cálculo de clave pública que crea un gran número aleatorio módulo un número primo grande, dando efectivamente una función unidireccional debido a la dificultad relativa de realizar las funciones logarítmicas discretas requeridas para revertirla (Dantu, Clothier, & Atri, 2007).

Las ventajas del método SPEKE es que obtiene la seguridad de los métodos de encriptación de claves públicas para los procedimientos de autenticación y transferencia de claves sin el gasto y la complejidad de implementar certificados (Dantu, Clothier, & Atri, 2007). Además, el mecanismo no es tan sensible a los ataques de diccionario como otros métodos basados en contraseñas.

Hay varias ventajas de usar EAP-SPEKE (Abo-Soliman & Azer, 2018). Probablemente, la mayor ventaja de EAP-SPEKE es que la información de la contraseña se puede intercambiar entre el usuario y el autenticador sin la amenaza de que un observador pueda obtener la contraseña. Para un observador externo, los mensajes parecen completamente aleatorios. Esto significa que el usuario solo tiene que recordar una pequeña contraseña para la autenticación. Otra gran ventaja de EAP-SPEKE es que no requiere el uso de certificados de clave pública, lo que significa que hay muy poca sobrecarga asociada con este método. Una ventaja final de este método es que admite el secreto directo, lo que significa que incluso si un observador obtiene la contraseña en una fecha futura. El observador aún no podrá descifrar el mensaje ya que la clave de sesión maestra se crea usando dos grandes números aleatorios además de la contraseña.

También hay varias desventajas de usar EAP-SPEKE. Aunque EAP-SPEKE no tiene la sobrecarga asociada con los métodos EAP basados en certificados, no admite la Re autenticación rápida. Esto significa que todo el proceso de autenticación EAP-SPEKE debe completarse cada vez que el usuario quiera conectarse al mismo servidor. Además, si alguien

puede obtener la contraseña, la contraseña es suficiente para hacerse pasar por otro usuario, incluso si la persona aún no puede descifrar los mensajes cifrados.

RADIUS

RADIUS es el “servidor backend” (Servidor de autenticación) en prácticamente todas las implementaciones de 802.1X. Las funciones de RADIUS cubren tres aspectos de seguridad, el cual se llama Protocolo AAA: Authentication, Authorization y Accounting, o bien autenticación, autorización y contabilización, respectivamente.

RADIUS opera en el modelo Cliente-Servidor donde el dispositivo de acceso a la red pasa información de autenticación en nombre de un cliente al servidor. La seguridad se conserva en este modelo mediante el uso de una contraseña secreta compartida codificada tanto en el dispositivo de acceso como en el servidor RADIUS. El servidor realizará la autenticación necesaria de un Suplicante, e informará al dispositivo de acceso del resultado, solo cuando el dispositivo de acceso haya proporcionado credenciales válidas a RADIUS (Brown, 2008). Esta funcionalidad básica funciona como se describe en el entorno 802.1X.

El autenticador y el servidor de autenticación, RADIUS, conversan utilizando el protocolo RADIUS. El protocolo utiliza un proceso de paso de bloqueo, similar al utilizado en EAPOL, para sincronizar la conversación entre el autenticador y el servidor de autenticación. Los paquetes RADIUS se componen principalmente de atributos. Cada atributo es un elemento de datos específico que utiliza el autenticador o se transmite al suplicante. Se han asignado más de cien atributos, pero solo una pequeña fracción de estos son pertinentes en una conversación basada en 802.1X.

Si una autenticación es un éxito, entonces el servidor RADIUS puede configurarse para proporcionar información al Autenticador que se utilizará para modificar dinámicamente una o ambas, la VLAN que se asignará y una lista de acceso. Esta información está contenida en dos atributos específicos que se pasan al autenticador fuera de un intercambio de método EAP.

Arquitectura, protocolo y flujo de paquetes RADIUS

El protocolo RADIUS utilizado para llevar la conversación entre el autenticador y el servidor de autenticación es muy similar en diseño a EAP. Al igual que EAP, RADIUS identifica la función a realizar a través de un elemento llamado Código y utiliza un proceso de sincronización de pasos de bloqueo mediante el uso de un elemento llamado Identificador (Hurtado, 2017). La Figura 6 ilustra el diseño del paquete RADIUS, junto con la descripción de cada elemento del protocolo.

Figura 6

Protocolo RADIUS.

Código (1 byte)	Identificador (1-byte)	Longitud (2 bytes)	Autenticador (16 bytes)	Atributos (0-n bytes)

Código:	Tipo de mensaje.
Identificador:	Código de paso de bloqueo para hacer coincidir las solicitudes con las respuestas.
Longitud:	Longitud del mensaje, incluido el encabezado.
Autenticador:	"Número aleatorio impredecible" utilizado para validar los intercambios de información.
Atributos:	Información de autenticación (método EAP).

Nota. Adaptado de *802.1X Port-Based Authentication* (p. 68), por E. L. Brown, 2008, Auerbach Publications.

Dentro del protocolo de RADIUS encontramos el elemento código que realiza la misma funcionalidad con RADIUS que el que realiza con EAP. Hay seis valores para este elemento que son pertinentes a 802.1X. El servidor RADIUS utiliza cuatro de los valores para las transmisiones al autenticador y el autenticador utiliza dos para comunicarse con el servidor. Los seis valores de Código que son pertinentes para la autenticación 802.1X se muestran a continuación en la Tabla 5.

Tabla 5

Códigos del protocolo de RADIUS.

Código	Descripción
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge

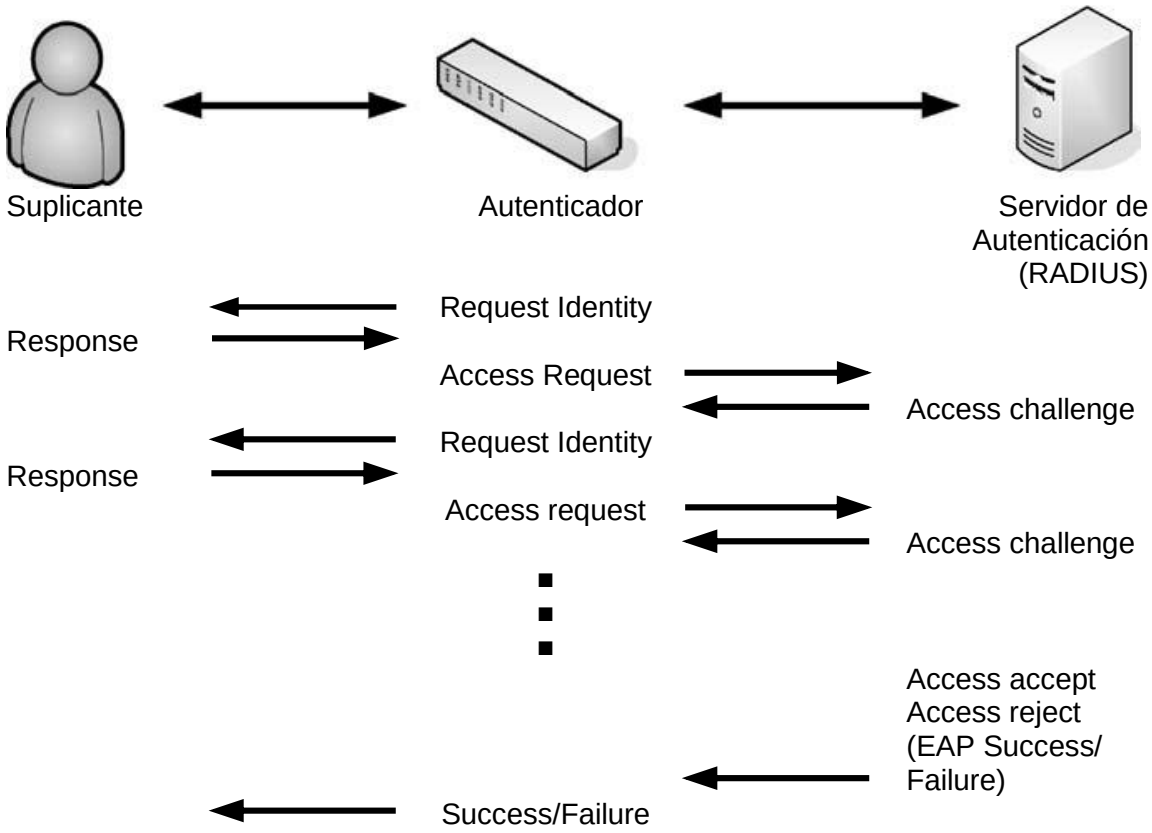
El servidor RADIUS tendrá una conversación "dual". Llevará a cabo una conversación entre el Autenticador y el Servidor de Autenticación utilizando el protocolo RADIUS y una conversación del método EAP con el Suplicante y el Autenticador. Recuerde que el Autenticador conversa físicamente con el Servidor de Autenticación mientras que el Suplicante conversa lógicamente con el Servidor de Autenticación, utilizando de puente al Autenticador. La Figura 7 resume este flujo del protocolo RADIUS.

Sistema AAA

El sistema AAA viene del acrónimo Authentication, Authorization and Accounting, fue emitido por el IETF (Internet Engineering Task Force) para proporcionar autenticación, autorización y contabilidad a cualquier sistema de redes. El sistema AAA está definido en el actual RFC2865 (Willens, Rubens, Simpson, & Rigney, 2000) y RFC2866 (Rigney, 2000), estos documentos incluyen: la administración de seguridad, configuración de claves entre el cliente RADIUS y el servidor RADIUS, configuración para cifrar información confidencial y usar los códigos de autenticación para probar la integridad de los paquetes de datos que transitan la red. El mecanismo principal del sistema AAA entre el usuario, un NAS y el servidor RADIUS, se muestran en la Figura 8.

Figura 7

Flujo que tiene generalmente el protocolo RADIUS.

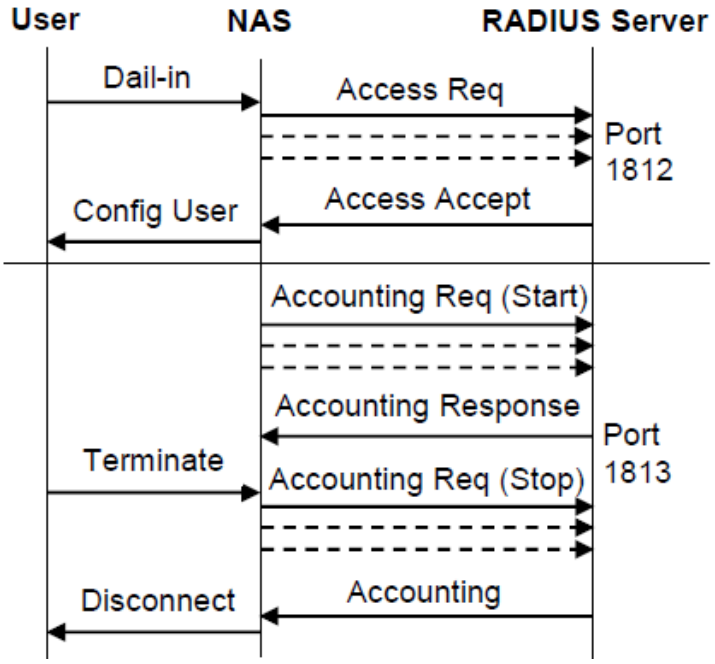


Nota. Adaptado de *802.1X Port-Based Authentication* (p. 69), por E. L. Brown, 2008, Auerbach Publications.

En la Figura 8, el NAS representa el protocolo AAA del cliente RADIUS en el flujo de trabajo (Setiawan, 2018). La línea de puntos representa la retransmisión provocada por el tiempo de espera. Para abreviar, no se muestran las retransmisiones del mensaje de respuesta enviado desde el servidor RADIUS al NAS. El protocolo RADIUS es escalable, el atributo tiene una longitud de variables y puede llevar información de autenticación, contabilidad y configuración detallada. En esta implementación, los nuevos atributos se pueden agregar para expandir el protocolo.

Figura 8

Flujo del sistema AAA.



Nota. Adaptado de "Wireless Network Security Information System on Banking Company with Radius Server Using Authentication, Authorization, Accounting (AAA)" (p. 256), por J. E. Setiawan, 2018, *International Journal of Computer Science and Software Engineering*, 7(11).

La Autenticación y Autorización del sistema de trabajo se da cuando el servidor de acceso a la red (NAS) autenticará a los usuarios a través de RADIUS, el NAS envía el paquete de solicitud de acceso al servidor RADIUS. Para este NAS, establece los atributos adecuados que describen la información que necesita sobre los servicios necesarios para el servidor y el usuario RADIUS. El atributo UserPassword de la contraseña en los usuarios se envía luego encriptado y no se envía en texto sin formato. NAS también produce un autenticador de solicitud único para solicitudes y restablece el identificador de NAS para que pueda conectarse respondiendo a la solicitud. Después de recibir una solicitud, este servidor RADIUS verifica la lista de clientes que están en la base de datos. Si la solicitud no proviene del usuario, las solicitudes no continúan y no se envía ningún mensaje de error. Si el usuario está vencido, el

servidor RADIUS para descifrar la contraseña del usuario (si corresponde) y este es el usuario verifica la base de datos en busca de entradas para preguntar a los usuarios y verifica si la contraseña del usuario es adecuada. Si no se encuentra el usuario, la contraseña no coincide o no se permite al usuario durante un tiempo.

Cuando NAS recibe una respuesta y de acuerdo con la solicitud que utiliza el identificador. Luego, el autenticador de respuesta de conteo de NAS recibe una respuesta de la misma manera que lo hace un servidor RADIUS y compara este valor con el autenticador de respuesta en el mensaje. Si coincide, la respuesta del servidor RADIUS se confirma y verifica. El proceso de combinación con el secreto compartido y este es el hash de la respuesta del Autenticador. El autenticador de respuesta se puede usar para verificar la verdad para autenticar el servidor RADIUS.

La Contabilidad se realiza casi igual que la autenticación y la autorización. Hay algunas diferencias. Contabilidad usando el puerto UDP 1813. También hay dos códigos de mensaje RADIUS y 12 atributos para Contabilidad. La contabilidad que comienza con el NAS envía un paquete con el código de solicitud de contabilidad que tiene el atributo Acct-Status-Type para iniciar el servidor RADIUS. En solicitud de inicio de contabilidad, atributo que contiene información sobre el usuario y los servicios utilizados. Todos los atributos que se pueden usar en la solicitud de acceso también se pueden usar en la solicitud de contabilidad con cinco excepciones. Este es el atributo User-Password, CHAP-Password, ReplyMessage, State y CHAP-Challenge.

Authentication. La autenticación de un sistema AAA debe confirmar si un usuario tiene derecho a acceder al sistema (Lu, Yeh, & Huang, 2018). Para ello en el servidor RADIUS deben constar las credenciales del usuario para que pueda ser autenticado.

Authorization. La autorización de un sistema AAA debe especificar los derechos/privilegios de acceso a los recursos para el usuario en particular, lo que también se denomina control de acceso (Lu, Yeh, & Huang, 2018). Si un usuario ha sido autenticado,

significa que sus credenciales están en el servidor RADIUS, por lo tanto, este puede tener restricciones en tasas de transmisión, tiempo de uso de la red, etc.

Accounting. La contabilidad de un sistema AAA debe cobrar a los usuarios por unidad de tiempo que consumen (Lu, Yeh, & Huang, 2018). Si la red es medida, se puede aplicar una tasación por el tiempo y las tasas de transmisión que requiera el usuario. Pero por otro lado, se puede utilizar esta información para controlar el uso que le dan los usuarios a la red.

Portal Cautivo

El portal cautivo es una técnica de autenticación y seguridad de datos que hace que un usuario de una red deba pasar por una página web especial, (normalmente como autenticación) antes de poder acceder a los servicios que ofrece el autenticador. El portal cautivo es en realidad un enrutador o una máquina de puerta de enlace que utiliza un navegador web como medio o dispositivo de autenticación seguro y controlado para proteger y permitir el tráfico hasta que el usuario se registra (Wahyudi, Luthfi, & Efendi, 2019).

Esto se hace para evitar la entrega de todos los paquetes de datos en cualquier forma a usuarios no autorizados hasta que el usuario abra un navegador web e intente acceder a Internet. En ese momento, el navegador será redirigido a una página específica especificada para autenticar, o simplemente mostrará la página de política aplicable y requerirá que el usuario la apruebe. Los portales cautivos a menudo se usan en redes inalámbricas (wifi, hotspot) y también se pueden usar para redes cableadas (Wahyudi, Luthfi, & Efendi, 2019).

¿Cuáles son los pasos que sigue un portal cautivo? Así funciona el portal cautivo como intermediario entre el usuario y el autenticador (Marques, Zúquete, & Barraca, 2019):

1. Los usuarios con clientes inalámbricos pueden conectarse a la red inalámbrica para obtener la dirección IP de DHCP.
2. Antes de la autenticación, todas las direcciones IP DHCP propagadas por el servidor anterior se redirigen al portal cautivo (autenticación basada en web).
3. Los usuarios conectados a la red pasarán por el portal Cautivo.

4. Una vez que el usuario haya terminado de iniciar sesión o registrarse, podrá utilizar la red de Internet proporcionada por el servidor.

La siguiente lista resume todos los problemas de seguridad planteados por la falta de seguridad de la capa de enlace causada por la actual explotación de puntos de acceso con Portales Cautivos (Marques, Zúquete, & Barraca, 2019):

- Los clientes pueden abusar de la red a través de túneles sobre protocolos que siempre están permitidos, como DNS.
- El tráfico de los clientes no está encriptado en la capa de enlace y, por lo tanto, puede ser capturado en texto claro por los espías del enlace de radio. Si bien parte del tráfico ya está encriptado en la capa de aplicación, este no es el caso para muchos protocolos de Internet.
- El tráfico hacia y desde los clientes no tiene autenticación de origen ni control de integridad y, por lo tanto, se pueden realizar ataques MitM y de suplantación.
- Los clientes y hosts, juntos, pueden ser engañados por puntos de acceso no autorizados, que pueden interferir con las actividades de los clientes.

Los problemas enumerados anteriormente son solo un ejemplo de lo que puede suceder cuando se usa un punto de acceso sin seguridad de capa de enlace. Sin dicha seguridad, tanto los clientes de la red como la propia red están abiertos a la inspección e inyección de tráfico.

HTML

El lenguaje de marcado de hipertexto (HTML, Hypertext Markup Language) existe desde principios de la década de 1990. Hubo un período en el que el mercado de los navegadores estaba muy disputado. Los principales competidores eran Microsoft y Netscape, y estas empresas competían agregando características únicas a sus navegadores web. La idea era que estas características serían tan convincentes que los desarrolladores web crearían su contenido para que funcionara solo en un navegador en particular, y este contenido sería tan convincente que los usuarios preferirían un navegador sobre otro y el dominio del mercado

seguiría. No funcionó de esa manera. Los desarrolladores web terminaron usando solo funciones que estaban disponibles en todos los navegadores o idearon soluciones elaboradas que usaban funciones más o menos comparables en cada uno (Freeman, 2011).

Las primeras versiones del estándar HTML no hicieron mucho para separar la importancia del contenido de la forma en que se presentó. Si deseaba indicar que un tramo de texto era importante, aplicó un elemento HTML que puso el texto en negrita. Correspondía al usuario hacer la asociación de que el contenido en negrita es contenido importante. El procesamiento automatizado de contenido se ha vuelto importante en los años posteriores a la introducción de HTML, y ha habido un esfuerzo gradual para separar la importancia de los elementos HTML de la forma en que se presenta el contenido en el navegador (Freeman, 2011).

El proceso para crear un estándar siempre es largo, especialmente para algo tan ampliamente utilizado como HTML. Hay muchas partes interesadas, y cada una quiere influir en las nuevas versiones del estándar para su beneficio comercial o punto de vista particular. Los estándares no son leyes, y los organismos de estándares temen la fragmentación por encima de todo, lo que lleva a una reconciliación que lleva mucho tiempo sobre cómo pueden funcionar las características y mejoras potenciales (Freeman, 2011).

El organismo de estándares para HTML es el World Wide Web Consortium (conocido como W3C). Tienen un trabajo difícil y se necesita mucho tiempo para que una propuesta se convierta en un estándar. Se necesita mucho tiempo para que se apruebe una revisión de la especificación principal de HTML (Hoy, 2012).

La consecuencia del largo proceso de estándares es que el W3C siempre ha estado siguiendo la curva, tratando de estandarizar lo que ya se ha convertido en una práctica aceptada. La especificación HTML ha sido un reflejo del pensamiento de vanguardia sobre el contenido web de hace varios años. Esto ha reducido la importancia del estándar HTML porque

la verdadera innovación estaba ocurriendo fuera del W3C, en parte en los navegadores y en parte en los complementos (Hoy, 2012).

HTML5

HTML5 (Figura 9) no es solo la última versión de la especificación HTML. También es un término genérico que describe un conjunto de tecnologías relacionadas que se utilizan para crear contenido web rico y moderno. Las tres tecnologías más importantes son la especificación principal de HTML5, las hojas de estilo en cascada (CSS, Cascading Style Sheets) y JavaScript.

Figura 9

Logo de HTML5 creado por la W3C.

La especificación principal de HTML5 define los elementos que usamos para marcar el contenido, indicando su significado. CSS nos permite controlar la apariencia del contenido marcado a medida que se presenta al usuario. JavaScript nos permite manipular el contenido de un documento HTML, responder a la interacción del usuario y aprovechar algunas características centradas en la programación de los nuevos elementos HTML5 (Freeman, 2011).

Algunas personas señalarán que HTML5 se refiere solo a los elementos HTML. Estas personas se están perdiendo un cambio fundamental en la naturaleza del contenido web. Las tecnologías utilizadas en las páginas web se han vuelto tan interconectadas que es necesario comprenderlas todas para crear contenido. Si usa elementos HTML sin CSS, crea contenido

que los usuarios encuentran difícil de analizar. Si usa HTML y CSS sin JavaScript, pierde la oportunidad de brindar a los usuarios comentarios inmediatos sobre sus acciones y la capacidad de aprovechar algunas de las nuevas funciones avanzadas que especifica HTML5 (Freeman, 2011).

Para lidiar con el largo proceso de estandarización y la forma en que el estándar va a la zaga del uso común, HTML5 y las tecnologías relacionadas se definen por una mayor cantidad de estándares pequeños. Algunas son solo un puñado de páginas enfocadas en un aspecto muy particular de una sola característica. Otros, por supuesto, siguen siendo cientos de páginas de texto denso que cubren franjas completas de funcionalidad (Freeman, 2011).

Capítulo III

Análisis, diseño e implementación del sistema

En este capítulo se realiza el análisis comparativo entre los métodos de autenticación más utilizados y comerciales del protocolo de autenticación extensible (EAP). Además, se detalla la situación actual de la empresa proveedora de servicio de internet Compu Seguridad. Información de importancia para realizar el análisis respectivo en la selección idónea del método de autenticación del EAP del estándar IEEE 802.1X. Obtenido el estándar a utilizar se realiza el respectivo diseño e implementación del sistema.

IEEE 802.1X

Las redes de área local inalámbricas (WLAN) se han vuelto cada vez más frecuentes en los últimos años. El estándar IEEE 802.11 es uno de los estándares más adoptados para el acceso inalámbrico a Internet de banda ancha. Sin embargo, las consideraciones de seguridad con respecto a los entornos inalámbricos son más complicadas que las de los entornos cableados. Debido a la naturaleza abierta de la radio inalámbrica, la red es más vulnerable. El estándar IEEE 802.11 (Bahn & Stanley, 2020) ha definido mecanismos básicos de seguridad para proteger el acceso a las redes IEEE 802.11. Sin embargo, todos han demostrado ser vulnerables.

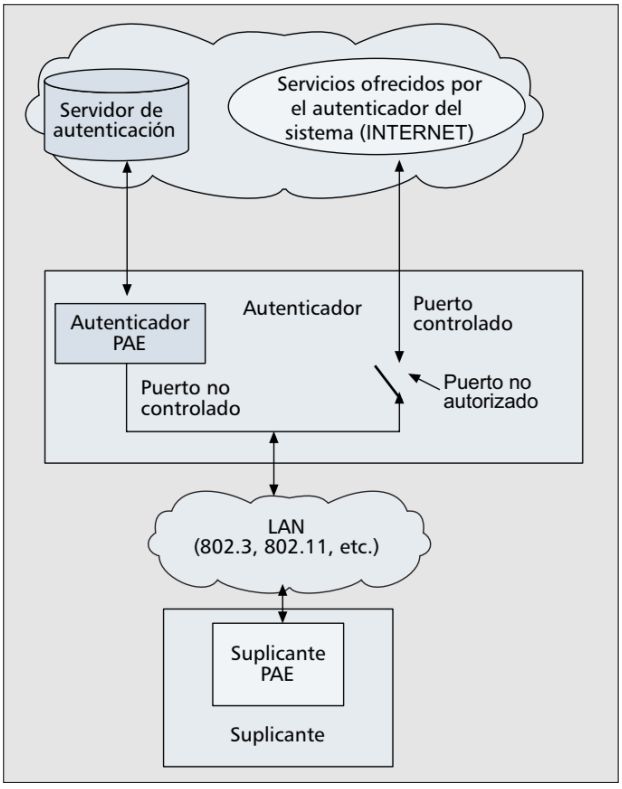
Para mejorar la seguridad en IEEE 802.11, se ha propuesto IEEE 802.1X (Orlando & Parsons, 2020) como su mejora de autenticación. El estándar IEEE 802.1X define un mecanismo para el control de acceso a la red basado en puertos. Se basa en EAP para proporcionar mecanismos de autenticación y autorización compatibles para dispositivos interconectados por LAN IEEE 802.

El estándar IEEE 802.1X ha sido bien definido. Actualmente, muchos fabricantes de puntos de acceso (AP) 802.11 también admiten 802.1X. Los AP compatibles con 802.1X se han implementado en muchas universidades, organizaciones y empresas. Para autenticarse mediante 802.1X, los usuarios finales también deben ser compatibles con 802.1X.

Como se muestra en la Figura 10, hay tres componentes principales en el sistema de autenticación IEEE 802.1X: suplicante, autenticador y servidor de autenticación. En una WLAN, el suplicante suele ser un nodo móvil. El enrutador generalmente representa un autenticador. Un servidor de autenticación, autorización y contabilidad (AAA) como el servidor RADIUS es el servidor de autenticación.

Figura 10

Suplicante, autenticador y servidor de autenticación en IEEE 802.1X.



Nota. Adaptado de “Extensible authentication protocol and IEEE 802.1x: Tutorial and Empirical Experience” (p.28), por J. Chen, & Y. Wang, 2005, *IEEE Communications Magazine*, 43(12).

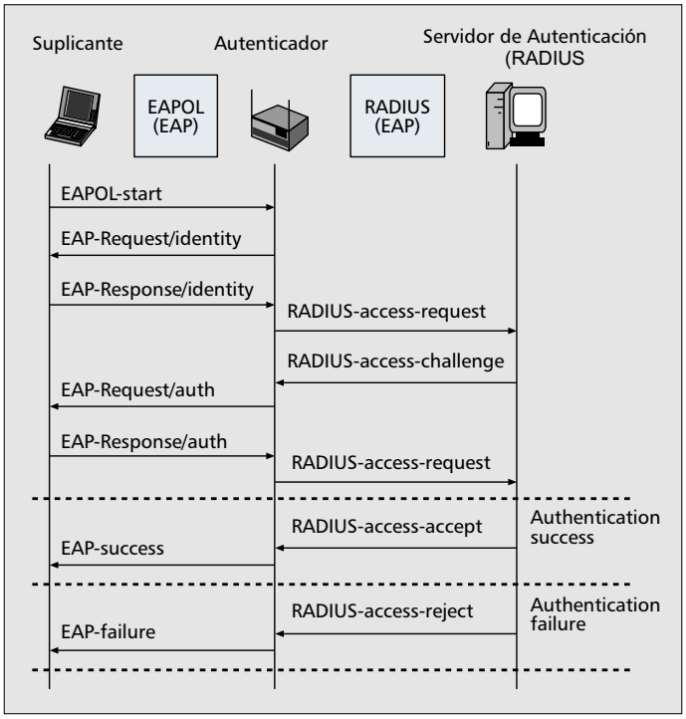
El puerto en 802.1X representa la asociación entre el suplicante y el autenticador. Tanto el suplicante como el autenticador tienen un PAE (port access entity o entidad de acceso al puerto) que opera los algoritmos y protocolos asociados con los mecanismos de autenticación. En la Figura 10, el puerto controlado del autenticador está en estado no autorizado, es decir, el puerto está abierto. Los mensajes se dirigirán solo al autenticador PAE, que luego dirigirá los

mensajes 802.1X al servidor de autenticación. El autenticador PAE cerrará el puerto controlado después de que el solicitante se autentique con éxito. Así, el solicitante puede acceder a otros servicios a través del puerto controlado.

Basado en EAP, el estándar IEEE 802.1X puede usar varios mecanismos de autenticación. El IEEE 802.1X también define EAP sobre LAN (EAPOL) para encapsular mensajes EAP entre el suplicante y el autenticador. El autenticador PAE transmite todos los mensajes EAP entre el solicitante y el servidor de autenticación. El 802.1X se utiliza para imponer el uso de un mecanismo de autenticación específico y para enrutar correctamente los mensajes de autenticación, mientras que los mecanismos de autenticación definen los intercambios de autenticación reales que tienen lugar. La Figura 11 muestra un intercambio de mensajes 802.1X típico.

Figura 11

Un flujo de mensajes típico del estándar IEEE 802.1X.



Nota. Adaptado de “Extensible authentication protocol and IEEE 802.1x: Tutorial and Empirical Experience” (p.28), por J. Chen, & Y. Wang, 2005, *IEEE Communications Magazine*, 43(12).

EAP y sus mecanismos de autenticación

Originalmente, EAP se desarrolló para su uso con conexiones de protocolo punto a punto o PPP y luego se adaptó para su uso en redes IEEE 802 cableadas y luego inalámbricas. En todas estas situaciones, es posible que un atacante obtenga acceso a los enlaces a través de los cuales se transmiten los paquetes EAP. Un atacante con acceso al enlace puede intentar descubrir las identidades de los usuarios, falsificar paquetes EAP, lanzar ataques de denegación de servicio, recuperar contraseñas usando un ataque de diccionario y convencer al par para que se conecte a una red no segura, así como otros tipos de ataques.

Para evitar este tipo de ataques, es extremadamente importante que el método EAP elegido pueda proporcionar una autenticación segura para que se pueda establecer una PMK (Pair-wise Master Key) segura entre el cliente o usuario y el punto de acceso a la red. Luego, el PMK se usa para la sesión de cifrado que usa TKIP (Temporal Key Integrity Protocol) o CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).

Actualmente hay más de 40 métodos EAP diferentes disponibles. Estos métodos EAP se pueden dividir en cuatro categorías diferentes: métodos legacy, métodos basados en certificados, métodos basados en contraseñas y métodos basados en contraseñas seguras. Pero, solo mencionaremos los que tienen mayor relevancia actualmente de cada uno de estos métodos, como son: CHAP, EAP-MD5, EAP-TLS, EAP-TTLS, PEAP, EAP-LEAP, EAP-Fast y EAP-SPEKE

CHAP

El método EAP-CHAP significa Challenge Handshake Authentication Protocol. CHAP está definido por RFC 1994 (Simpson, 1996). CHAP se usa para verificar la identidad de un par mediante el uso de un protocolo de enlace de 3 vías. El servidor de autenticación valida al par en el momento en que se realiza el enlace y también puede autenticar aleatoriamente al usuario mientras se realiza la conexión. El servidor de autenticación prueba la autenticidad del par enviando un mensaje de desafío al par. El par calcula un valor utilizando una función hash

unidireccional y envía este valor al autenticador. El autenticador calcula su propio valor hash y compara este valor con el valor recibido del par. Si los dos valores coinciden, el par se autentica. Si los dos valores no coinciden, la conexión debe terminarse.

Una de las ventajas de CHAP es que evita el ataque de reproducción mediante el uso de un identificador que cambia gradualmente y un valor de desafío variable. El autenticador controla el tiempo entre desafíos y, por lo tanto, puede limitar el tiempo de exposición a un ataque. Otra ventaja de CHAP es que el método se basa en un secreto compartido, pero el secreto nunca se envía a través del enlace. Una tercera ventaja de CHAP es que se puede usar el mismo método para la autenticación mutua realizando el método en ambas direcciones usando dos secretos diferentes (Simpson, 1996).

Sin embargo, una de las mayores desventajas de CHAP es que el secreto debe estar disponible en ambos extremos en forma de texto sin formato. Esto significa que las bases de datos que cifran de forma irreversible los datos de la contraseña no se pueden utilizar para almacenar el secreto. Otra desventaja de CHAP es que no hay forma de establecer un PMK para el futuro cifrado de datos (Simpson, 1996).

EAP-MD5

MD5 significa Message Digest 5 y fue desarrollado por RSA, se basa principalmente en una función hash unidireccional. Esencialmente, una función hash es una suma de control criptográfica. Una función hash unidireccional toma un mensaje de entrada arbitrariamente largo y produce una salida pseudoaleatoria de longitud fija llamada hash. Con un hash, es computacionalmente difícil encontrar el mensaje que produjo ese hash. Además, es casi imposible y difícil encontrar diferentes mensajes que generen el mismo hash.

MD5 toma un mensaje de entrada de longitud arbitraria y produce una salida de huella digital o resumen de mensaje de 128 bits. Al usar MD5, un servidor de autenticación puede autenticar a un usuario sin almacenar la contraseña del usuario en texto no cifrado. Cuando se crea una cuenta y un usuario ingresa su contraseña, el servidor de autenticación almacena el

hash generado por una función hash unidireccional que tiene la contraseña como mensaje de entrada. Cuando el usuario desea iniciar sesión en el sistema más tarde, el solicitante calcula el hash con la contraseña que el usuario ingresa ahora como la entrada de la misma función hash unidireccional. El hash se transmite a través de la red. Si el hash recibido es el mismo que el almacenado en el servidor de autenticación, el usuario está autenticado. Debido a que la contraseña no se almacena en texto no cifrado, la contraseña de usuario no se revelará, incluso cuando se revele el archivo de contraseñas.

El EAP-MD5 es uno de los tipos de EAP más populares porque es fácil de usar. Un usuario simplemente escribe el nombre de usuario. Luego se sigue un Challenge/Response para autenticar al usuario. El servidor de autenticación solicita la contraseña mediante el envío de RADIUS-Access-Challenge, como se muestra en la Figura 8. Luego, el hash de la contraseña se envía mediante EAP-Response/Auth, que se encapsula aún más mediante RADIUS-Access-Request. Esta es una opción simple y razonable para las LAN cableadas en las que existe un bajo riesgo de que los atacantes intercepten la transmisión. Sin embargo, en las LAN inalámbricas, los atacantes pueden rastrear fácilmente la identidad de una estación y el hash de la contraseña. Por lo tanto, MD5 es más vulnerable que otros métodos de autenticación. Uno de esos ataques es el ataque de repetición. Al utilizar el ataque de repetición, un atacante puede pretender ser un usuario autorizado para acceder a una red incluso cuando la contraseña está cifrada.

EAP-TLS

El EAP-TLS proporciona negociación de conjunto de cifrado protegido, autenticación mutua y administración de claves. Una vez completada la negociación EAP-TLS, los dos puntos finales (suplicante y los servicios ofrecidos por el autenticador) pueden comunicarse de forma segura dentro del túnel TLS cifrado. Por lo tanto, la identidad y la contraseña del usuario no serán reveladas. Debido a que TLS proporciona una forma de usar certificados tanto para el suplicante como para el servidor para autenticarse entre sí, un usuario, además de ser

autenticado, también puede autenticar la red. Por lo tanto, se podrían detectar puntos de acceso falsificados. Tanto el solicitante como el servidor de autenticación deben tener certificados válidos al usar EAP-TLS.

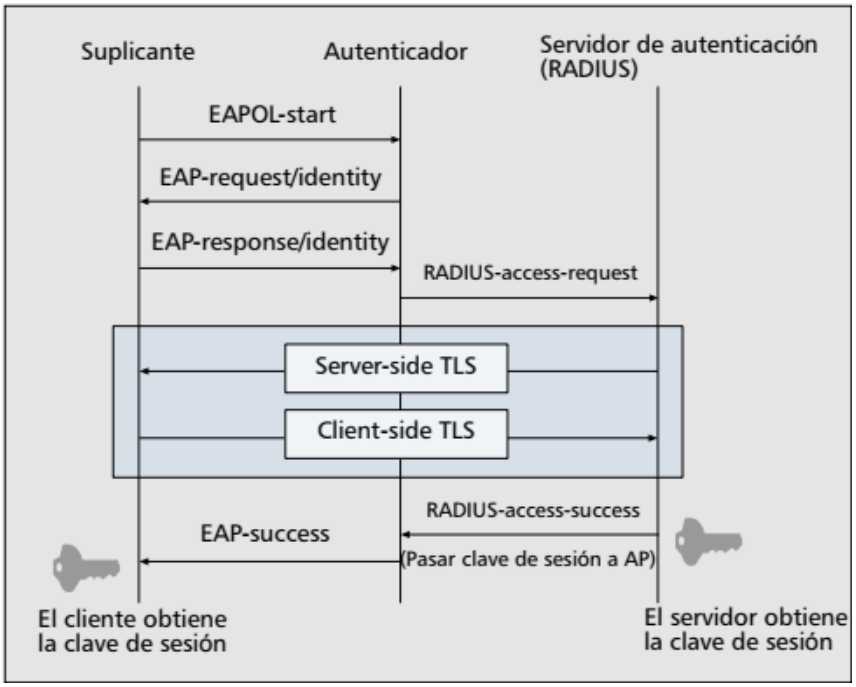
La Figura 12 ilustra el proceso de autenticación y los intercambios de mensajes de EAP-TLS en una WLAN. Después de que el autenticador recibe la identidad del suplicante en EAP-Response/Identity (flujo 3), inicia una RADIUS-Access-Request, que también lleva la identidad del suplicante, al servidor de autenticación. Luego, el servidor de autenticación proporciona su certificado al solicitante y solicita el certificado del solicitante. El solicitante valida el certificado del servidor y responde con EAP-Response que contiene el certificado del solicitante. El solicitante también inicia la negociación del material criptográfico. Después de que se valida el certificado del solicitante, el servidor responde el material criptográfico para la sesión. Las claves de sesión derivadas en ambos extremos se pueden utilizar para el cifrado de datos. Debido a que tanto el suplicante como los servidores de autenticación deben tener certificados válidos al usar EAP-TLS, hasta cierto punto, EAP-TLS es difícil de administrar.

EAP-TTLS

EAP-TTLS amplía EAP-TLS para intercambiar información adicional entre el cliente y el servidor mediante el uso del túnel seguro establecido por la negociación TLS. Una negociación EAP-TTLS consta de dos fases: la fase de protocolo de enlace TLS y la fase de túnel TLS. Durante la fase uno, se utiliza TLS para que el cliente autentique el servidor. Opcionalmente, el servidor también puede autenticar al cliente. Al igual que en EAP-TLS, la autenticación se realiza mediante certificados. También se establece un túnel TLS seguro después del protocolo de enlace de fase uno. En la fase dos, el túnel TLS seguro se puede utilizar para otros intercambios de información, como clave de autenticación de usuario adicional, comunicación de información contable, etc.

Figura 12

Flujo de mensajes de EAP-TLS.



Nota. Adaptado de “Extensible authentication protocol and IEEE 802.1x: Tutorial and Empirical Experience” (p.30), por J. Chen, & Y. Wang, 2005, *IEEE Communications Magazine*, 43(12).

En un entorno WLAN, el EAP-TTLS generalmente se usa de la siguiente manera. En la fase uno, TLS se usa como suplicante para autenticar el servidor de autenticación mediante un certificado. Una vez que se autentica el servidor de autenticación, el servidor de autenticación autentica al solicitante utilizando el nombre de usuario y la contraseña del solicitante en la fase dos. El nombre de usuario y la contraseña se transportan en los pares de valor de atributo (AVP) definidos por el servidor AAA, que generalmente es un servidor RADIUS. Los intercambios de mensajes están protegidos por el túnel TLS establecido en la fase uno. La autenticación del suplicante en la fase dos puede usar cualquier protocolo que no sea EAP. Debido a que solo el servidor de autenticación necesita tener un certificado válido, EAP-TTLS es más manejable que EAP-TLS.

PEAP

PEAP proporciona un túnel encriptado y autenticado basado en TLS. Por lo tanto, los mensajes EAP encapsulados dentro del túnel TLS están protegidos contra varios ataques. Similar a EAP-TTLS, PEAP también consta de dos fases. En la primera fase, se negocia y establece una sesión TLS. El cliente también autentica el servidor mediante un certificado. Opcionalmente, el servidor también puede autenticar al cliente. En la segunda fase, los mensajes EAP se cifran utilizando la clave negociada en la fase uno. La idea básica de PEAP y EAP-TTLS es idéntica. Sin embargo, PEAP solo puede usar protocolos EAP en la segunda fase, mientras que EAP-TTLS puede usar protocolos EAP o no EAP.

Cuando se usa PEAP en WLAN, normalmente, un servidor de autenticación es autenticado por un solicitante basado en el certificado del servidor. También se crea un túnel TLS seguro. A continuación, se autentica al solicitante mediante un nombre de usuario y una contraseña, que están protegidos por el túnel TLS.

EAP-LEAP

EAP-LEAP son las siglas de EAP-Light Extensible Authentication Protocol. EAP-LEAP es un método EAP patentado que fue desarrollado por Cisco Systems antes de la ratificación del estándar de seguridad IEEE 802.11i. LEAP utiliza una versión modificada de MS-CHAP para autenticar tanto al cliente como al servidor. Por lo tanto, EAP-LEAP proporciona autenticación mutua. A diferencia de MS-CHAP, las claves de seguridad cambian dinámicamente con cada sesión de comunicación. Esto ayuda a evitar que un atacante recopile los paquetes de autenticación necesarios para decodificar los datos.

Probablemente la mayor ventaja de EAP-LEAP es la baja sobrecarga asociada con este método EAP en particular. No hay que preocuparse por los certificados de clave pública, lo que reduce en gran medida la cantidad de problemas administrativos necesarios en la implementación. Además, el uso de un esquema de nombre de usuario/contraseña asegura

que el usuario esté autenticado y no el dispositivo que se conecta a la red. Finalmente, el método es rápido y eficiente y requiere muy poco tiempo para la autenticación mutua.

La mayor desventaja de EAP-LEAP es que no proporciona un alto nivel de seguridad. A principios de 2004, Joshua Wright lanzó una herramienta llamada ASLEAP. ASLEAP se puede utilizar para explotar fallas en la seguridad de EAP-LEAP para obtener las contraseñas de usuarios desprevenidos de EAP-LEAP. Después de usar algún tipo de rastreador de paquetes, un pirata informático puede usar ASLEAP para realizar un ataque de diccionario muy simple para determinar la contraseña de los usuarios que se conectan a un punto de acceso de Cisco (Carballar, 2010).

EAP-FAST

EAP-FAST son las siglas de EAP-Flexible Authentication via Secure Tunneling. EAP-FAST fue diseñado por Cisco como reemplazo de EAP-LEAP después de que se demostró que EAP-LEAP era vulnerable a los ataques de diccionario. El objetivo de EAP-FAST era proporcionar un mayor nivel de seguridad que el logrado por EAP-LEAP y al mismo tiempo mantener la baja sobrecarga asociada con EAP-LEAP.

EAP-FAST es en realidad muy similar a EAP-TTLS. EAP-FAST se basa en el uso de TLS para establecer un túnel entre el cliente y el servidor que luego se puede usar para autenticar al cliente mediante el uso de un método de autenticación de contraseña heredado, como CHAP. La gran diferencia entre los métodos EAP basados en certificados y EAP-FAST es que EAP-FAST no requiere que el servidor tenga una certificación de clave pública. En su lugar, EAP-FAST utiliza un PAC (Protected Access Credential) para establecer el túnel TLS.

Una de las mayores ventajas de EAP-FAST es que proporciona una seguridad muy similar a la de EAP-TTLS o PEAP sin la sobrecarga asociada con el mantenimiento de un certificado de clave pública. Sin embargo, la seguridad asociada con PKI se debe en parte a la existencia de una CA a la que se puede contactar para verificar la autenticidad de un certificado

en particular, y no hay una CA presente en este esquema en particular. Otra ventaja de este método es que admite la reconexión rápida.

Una de las mayores desventajas de este método en particular es que se necesitan muchos viajes de ida y vuelta para establecer la conexión inicial entre el usuario y el servidor. Otra desventaja de EAP-FAST es que cuando el aprovisionamiento automático de PAC está habilitado, EAP-FAST tiene una pequeña vulnerabilidad de que un atacante puede interceptar el PAC y usarlo para comprometer las credenciales del usuario.

EAP-SPEKE

EAP-SPEKE significa EAP-Simple Password-Authenticated Exponential Key Exchange. La base de EAP-SPEKE es un intercambio Diffie-Hellman. El intercambio Diffie-Hellman permite que el usuario y el servidor creen claves de cifrado sin que un observador pueda determinar cuáles son las claves.

El método EAP-SPEKE se basa en la exponenciación que involucra grandes números aleatorios y de módulo un gran número primo. El cálculo de valores exponenciales se considera una función unidireccional, ya que el proceso logarítmico para calcular los valores originales es muy complejo. Por lo tanto, alguien que es capaz de obtener el valor exponencial es incapaz de determinar la base o el exponente que se utilizó.

La autenticación se logra de la siguiente manera. Tanto el usuario como el servidor de autenticación generan un gran número aleatorio. El número aleatorio del usuario es a, y el número aleatorio de los servidores de autenticación es b. De esta forma cada uno de ellos solo conoce uno de los valores. Nadie conoce nunca los dos valores. Entonces, estos dos números aleatorios son similares a las claves privadas en TLS. La contraseña, es un secreto compartido conocido tanto por el usuario como por el servidor de autenticación. La contraseña es pequeña y fácil de recordar.

Hay varias ventajas de usar EAP-SPEKE. Probablemente, la mayor ventaja de EAP-SPEKE es que la información de la contraseña se puede intercambiar entre el usuario y el

autenticador sin la amenaza de que un observador pueda obtener la contraseña. Para un observador externo, los mensajes parecen completamente aleatorios. Esto significa que el usuario solo tiene que recordar una pequeña contraseña para la autenticación. Otra gran ventaja de EAP-SPEKE es que no requiere el uso de certificados de clave pública, lo que significa que hay muy poca sobrecarga asociada con este método. Una ventaja final de este método es que admite el secreto directo, lo que significa que incluso si un observador obtiene la contraseña en una fecha futura. El observador aún no podrá descifrar el mensaje ya que la clave de sesión maestra se crea usando dos grandes números aleatorios además de la contraseña.

También hay varias desventajas de usar EAP-SPEKE. Aunque EAP-SPEKE no tiene la sobrecarga asociada con los métodos EAP basados en certificados, no admite la Re autenticación rápida. Esto significa que todo el proceso de autenticación EAP-SPEKE debe completarse cada vez que el usuario quiera conectarse al mismo servidor. Además, si alguien puede obtener la contraseña, la contraseña es suficiente para hacerse pasar por otro usuario, incluso si la persona aún no puede descifrar los mensajes cifrados.

Análisis comparativo de los mecanismos de autenticación EAP

En la Tabla 6, se muestra un resumen de los mecanismos de autenticación EAP. Hay una serie de criterios que se pueden usar para comparar diferentes métodos EAP, pero el criterio más importante para este trabajo de investigación es si un método EAP cumple o no con la norma RFC 4017, titulada Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs (Stanley, Walker, & Aboba, 2005). Esta norma define los requisitos para los métodos EAP utilizados en las implementaciones de LAN inalámbrica IEEE 802.11.

Los métodos de autenticación EAP adecuados para su uso en la autenticación de LAN inalámbrica deben cumplir los siguientes criterios obligatoriamente:

- Generación de clave simétrica.

Tabla 6

Comparación de los mecanismos de autenticación.

	Legacy	**EAP-TLS**	**EAP-TTLS**	**EAP-PEAP**	**EAP-LEAP**	**EAP-FAST**	**EAP-SPEKE**
Autenticación mutua	No	Sí	Sí	Sí	Sí	Sí	Sí
Autenticación del servidor	No	Certificado	Certificado	Certificado	Claves de cifrado	PAC	Claves de cifrado
Autenticación del suplicante	Sí	No si el certificado está en el disco	No si el certificado está en el disco	No si el certificado está en el disco	Sí	No si el certificado está en el disco	Sí
Entrega de clave dinámica	No	Sí	Sí	Sí	Sí	Sí	Sí
Certificado de servidor	No	Requerido	Requerido	Requerido	No	Requerido	Requerido
Certificado de cliente	No	Requerido	Opcional	Opcional	No	Opcional	Requerido
Inmunidad en ataque de diccionario	No	Sí	Sí	Sí	No	Sí	Sí
Inmunidad en ataque MitD	No	Sí	Sí	Sí	No	Sí	Sí
Eficiente	Sí	No	No	No	Sí	No	Sí
Bajo costo	Sí	No	No	No	Sí	Sí	Sí
Amplio soporte de puntos de acceso	Sí	Sí	Sí	Sí	No	No	Sí
Reconexión rápida	No	Sí	Sí	Sí	No	Sí	No
Fortaleza general de la seguridad	Mala	Fuerte	Buena	Buena	Buena	Buena	Fuerte

- Clave segura. Un método EAP adecuado para su uso con IEEE 802.11 debe ser capaz de generar material de clave con 128 bits de fuerza de clave efectiva.
- Soporte de autenticación mutua.
- Equivalencia estatal compartida. El estado del método EAP compartido del par y el servidor EAP debe ser equivalente cuando el método EAP se completa con éxito en ambos lados.
- Resistencia a ataques de diccionario.
- Protección contra ataques man-in-the-middle.
- Negociación de ciphersuite protegido.

Los métodos de autenticación EAP utilizados para la autenticación de LAN inalámbrica deberían admitir las siguientes funciones:

- Fragmentación.
- Ocultación de la identidad del usuario final.

Los métodos de autenticación EAP utilizados para la autenticación de LAN inalámbrica podrían admitir las siguientes funciones:

- Unión de canales.
- Reconexión rápida.

Ya está muy claro en la lista de métodos EAP definidos en RFC 4017 que los métodos legacy no cumplen con los criterios más básicos establecidos para su uso con la comunicación inalámbrica. Todos los métodos legacy examinados, no brindan autenticación mutua, lo cual es muy importante para la comunicación inalámbrica. Además, se ha descubierto que todos estos métodos legacy son susceptibles a ataques de diccionario a menos que se utilicen contraseñas aleatorias extremadamente grandes. Por lo tanto, los métodos legacy no cumplen con RFC 4017 y no deben usarse para la autenticación de comunicaciones inalámbricas.

Los métodos de autenticación basados en certificados proporcionan autenticación mutua. Todos estos métodos son resistentes a los ataques de diccionario, ya que utilizan claves públicas y privadas sólidas que se almacenan en certificados de claves públicas. Todos estos métodos protegen contra ataques man-in-the-middle, y todos los métodos admiten la negociación de conjuntos de cifrado protegidos. Además, todos estos métodos EAP son compatibles con todas las funciones recomendadas y opcionales, como también la reconexión rápida. Por lo tanto, todos los métodos EAP basados en certificados cumplen totalmente con las especificaciones establecidas por RFC 4017.

Los métodos basados en contraseña también permiten la autenticación mutua. EAP-LEAP no es inmune a los ataques de diccionario, lo que se demostró utilizando la herramienta ASLEAP para obtener la contraseña de los usuarios que se conectan a un punto de acceso a la red. Por lo tanto, el método EAP basado en contraseña EAP-LEAP no cumple con RFC 4017. EAP-FAST, por otro lado, no es susceptible a ataques de diccionario. EAP-FAST no es susceptible a los ataques de intermediarios. EAP-FAST cumple con todos los requisitos obligatorios descritos en RFC 4017.

EAP-SPEKE cumple con todos los requisitos obligatorios especificados en RFC 4017. Sin embargo, EAP-SPEKE no brinda soporte para la reconexión rápida. Por lo tanto, EAP-SPEKE cumple con RFC 4017, pero no contiene todas las funciones definidas para su uso por un método EAP para la autenticación a través de una red inalámbrica.

La solidez de la seguridad de las credenciales hace referencia al nivel de seguridad que proporciona un método para la información secreta, como combinaciones de nombre de usuario y contraseña, claves de cifrado públicas y privadas y otra información segura. A partir de las descripciones de los métodos EAP, es fácil determinar que el nivel más alto de seguridad se obtiene con los métodos basados en certificados y, más específicamente, con el método EAP-TLS. Este método utiliza certificados de clave pública para autenticar tanto al usuario en el servidor de autenticación como al servidor de autenticación al usuario. El resto de

los métodos EAP basados en certificados solo requieren un certificado del lado del servidor. El método EAP basado en contraseña fuerte EAP-SPEKE y el método EAP basado en contraseña EAP-FAST brindan una seguridad que es ligeramente menor que la de los métodos EAP basados en certificados, pero sigue siendo muy sólida. Finalmente, los métodos EAP legacy brindan el nivel más bajo de seguridad de cualquiera de los métodos EAP.

Los métodos EAP legacy, junto con los métodos EAP basados en contraseña, son los métodos EAP más rápidos y eficientes que requieren la menor cantidad de viajes de ida y vuelta y la menor cantidad de operaciones para completar. El método EAP basado en contraseña segura, EAP-SPEKE, sería el siguiente método EAP más eficiente debido a los cálculos adicionales que se deben completar. EAP-FAST, EAP-TTLS y EAP-PEAP no son muy rápidos ni muy eficientes. Todos estos métodos requieren que se establezca un túnel TLS antes de que se pueda usar un método EAP heredado para autenticar al usuario. Esto requiere muchos viajes de ida y vuelta y no es muy eficiente. El método EAP menos eficiente es EAP-TLS, este método requiere que el protocolo TLS se use dos veces para autenticar el servidor al usuario y luego el usuario al servidor.

Si bien el costo de implementar métodos EAP legacy, basados en contraseñas y basados en contraseñas seguras es relativamente bajo, ya que estos métodos simplemente requieren paquetes de software, el costo de mantener un método EAP basado en certificados puede volverse costoso. Los métodos EAP basados en certificados utilizan una PKI que puede consistir en software de cliente, software de servidor, hardware, contratos y garantías legales, y procedimientos operativos. Esto se agrava en el caso de EAP-TLS, que requiere que cada cliente tenga un certificado de clave pública. Por lo tanto, EAP-TLS es, con diferencia, el método EAP más caro de implementar y mantener.

El hecho de que un método EAP admita o no la reconexión rápida es otra característica que se puede usar para comparar los métodos EAP. Los únicos métodos que admiten reconexiones rápidas son los métodos EAP basados en certificados y EAP-FAST, que también

es capaz de actuar como un método basado en certificados. Esta es una característica importante de estos métodos EAP en particular porque son los métodos EAP más lentos e ineficientes. Al proporcionar una reconexión rápida, estos métodos EAP esperan mejorar la eficiencia con la que los usuarios pueden conectarse a los servidores a los que se conectan una y otra vez. Esto también significa que la autenticación no toma tanto tiempo si la conexión se interrumpe por algún motivo.

Después de examinar las cuatro categorías diferentes de métodos EAP, está claro que el mejor método EAP para usar con redes inalámbricas depende de las prioridades del usuario. El usuario primero debe decidir qué características de un método EAP son las más importantes. El usuario también debe decidir qué características del método EAP son las menos importantes.

Situación actual de la empresa Compu Seguridad

La empresa Compu Seguridad (Figura 13) se encuentra situada en el cantón Buena Fe, provincia Los Ríos, perteneciente a la República del Ecuador. Su principal actividad económica es de Proveedor de Servicio de Internet por medio de fibra óptica y por antenas, para la ciudadanía del mismo cantón y de los sectores aledaños a los cuales no es posible tener FTTH (Fiber to the Home). Además, complementa su actividad económica con la venta e instalación de cámaras de seguridad, venta de equipos de computación, servicio IPTV, mantenimiento de equipos de computación, entre otros. A día de hoy cuenta con 20 empleados y más de 1500 clientes.

Figura 13

Logo de la empresa Compu Seguridad.

Equipamiento

La empresa Compu Seguridad cuenta con una infraestructura de red inalámbrica robusta para controlar y dar acceso a la misma, sin embargo, estos equipos están siendo desaprovechados, por lo que aún tienen falencias en rendimiento, disponibilidad y seguridad. Actualmente, la seguridad inalámbrica es como la de cualquier hogar convencional, por lo tanto, es vulnerable a ataques cibernéticos, teniendo acceso directo a información clasificada de la empresa.

Los equipos que conforman la infraestructura inalámbrica de la red se describen en la Tabla 7, que se muestra a continuación:

Tabla 7

Equipos WLAN de la empresa Compu Seguridad.

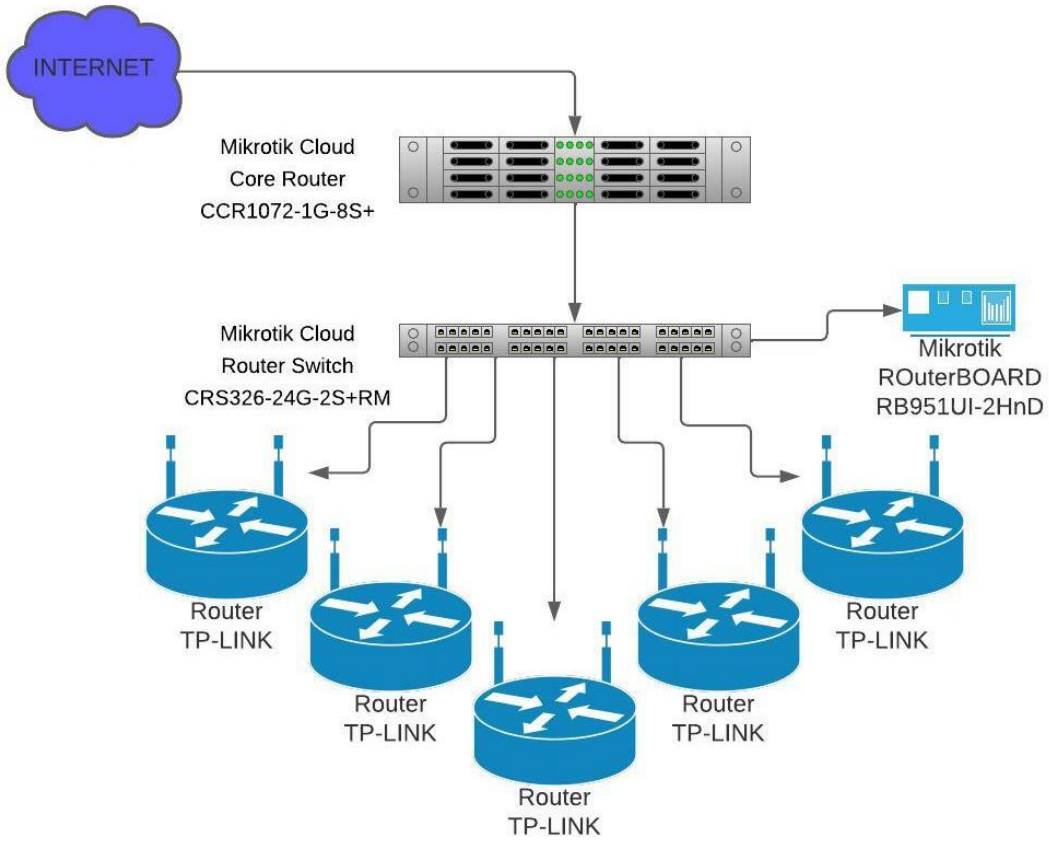
Cant.	Marca	Modelo	Estado	OS
1	MikroTik Cloud Core Router	CCR1072-1G-8S+	Funcional	RouterOS
1	MikroTik Cloud Router Switch	CRS326-24G-2S+RM	Funcional	RouterOS
1	MikroTik RouterBOARD	RB951Ui-2HnD	Funcional	RouterOS
3	TP-Link	TL-WR840N	Funcional	
2	TP-Link	Archer C20	Funcional	

Infraestructura de la red inalámbrica

Todos los servicios de red que provee la empresa Compu Seguridad (Figura 14) son a través del equipo de MikroTik Cloud Core Router CCR1072-1G-8S+, este llega a conectarse al MikroTik Cloud Router Switch CRS326-24G-2S+RM que distribuye el internet a los router inalámbricos TP-Link y al MikroTik RouterBOARD RB951Ui-2HnD que se lo utilizó como Hotspot durante unos meses y luego dejaron de usarlo, el mismo se encuentra conectado en la red, pero sin uso alguno.

Figura 14

Infraestructura de la red inalámbrica de la empresa Compu Seguridad.



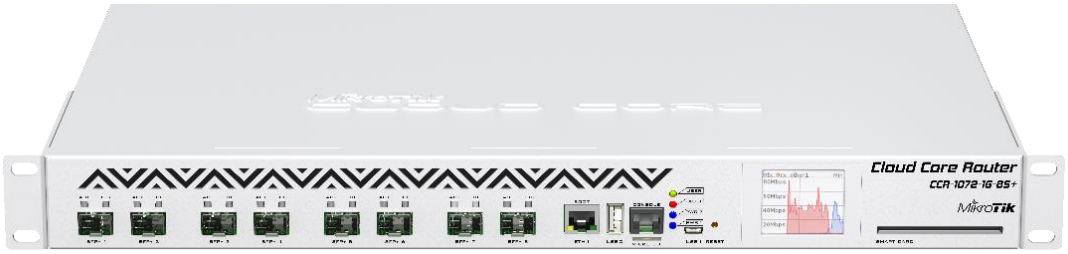
Descripción técnica de equipos

Para conocer la capacidad actual que tiene la infraestructura de red de la empresa Compu Seguridad, es necesario realizar una retroalimentación de los equipos que tiene. Por ello se describirán las características de sus equipos.

MikroTik Cloud Core Router CCR1072-1G-8S+. El CCR1072 (Figura 15), está alimentado por una CPU de 72 núcleos, cada núcleo tiene una frecuencia de reloj de 1 GHz y, para utilizar plenamente esta potencia, el CCR1072 está equipado con ocho puertos SFP + 10G conectados de forma independiente y un solo puerto Ethernet para fines de administración.

Figura 15

MikroTik Cloud Core Router CCR1072-1G-8S+.



Nota. Adaptado de *MikroTik Cloud Core Router CCR1072-1G-8S+*, por MikroTik (https://i.mt.lv/cdn/rb_images/1055_hi_res.png).

El router viene equipado con el sistema operativo RouterOS de nivel 6, cuenta con un CPU de 72 núcleos, 16 GB de RAM incorporada, una pantalla LCD a color, tiene dos fuentes de alimentación extraíbles, puertos microUSB, USB tipo A, una ranura para una microSD y dos ranuras M.2 para almacenamiento adicional. Se puede visualizar un resumen de sus especificaciones técnicas en la Tabla 8.

Tabla 8

Especificaciones técnicas del MikroTik Cloud Core Router CCR1072-1G-8S+.

Detalle	**Descripción**
Código de producto	CCR1072-1G-8S+
CPU	TLR4-07280
Núcleos CPU	72
Frecuencia del CPU	1 GHz
Dimensiones	443 x 315 x 44 mm
SO	RouterOS
Licencia	Nivel 6
RAM	16 GB
Almacenamiento interno	128 Mb
Tipo de almacenamiento	NAND
Temperatura de funcionamiento	-20°C a 60°C
Aceleración de hardware IPsec	Sí

MikroTik Cloud Router Switch CRS326-24G-2S+RM. Este es un conmutador Gigabit Ethernet de 24 puertos alimentado por SwOS/RouterOS con dos puertos SFP+, conectividad a velocidad de cable con varias funciones de conmutación nuevas (Figura 16).

Figura 16

MikroTik Cloud Router Switch CRS326-24G-2S+RM.

Nota. Adaptado de *MikroTik Cloud Router Switch CRS326-24G-2S+RM*, por MikroTik (https://i.mt.lv/cdn/rb_images/1301_hi_res.png).

Este switch tiene una función especial, la cual permite un arranque dual, para elegir el sistema operativo RouterOS o SwOS. Además, brinda la funcionalidad básica para un conmutador administrado, y más: permite administrar el reenvío de puerto a puerto, aplicar el filtro MAC, configurar VLAN, duplicar el tráfico, limitar el ancho de banda e incluso ajustar algunos campos de encabezado MAC e IP. Se puede visualizar un resumen de sus especificaciones técnicas en la Tabla 9.

Tabla 9

Especificaciones técnicas del MikroTik Cloud Router Switch CRS326-24G-2S+RM.

Detalle	**Descripción**
Código de producto	CRS326-24G-2S+RM
CPU	98DX3236
Núcleos CPU	1
Frecuencia del CPU	800 MHz
Dimensiones	443 x 144 x 44 mm
SO	RouterOS ó SwitchOS
Licencia RouterOS	Nivel 5

Detalle	Descripción
RAM	512 MB
Almacenamiento interno	16 Mb
Tipo de almacenamiento	FLASH
Temperatura de funcionamiento	-40°C a 60°C
Aceleración de hardware IPsec	No

MikroTik RouterBOARD RB951Ui-2HnD. El RB951Ui-2HnD (Figura 17) es un enrutador y punto de acceso (AP) inalámbrico de nueva generación, perfecto para SOHO (small office home office). Tiene un procesador Atheros de 600 MHz y más poder de cómputo. Cuenta con 128 MB de RAM, está equipado con cinco puertos Ethernet, de los cuales uno incorpora la función PoE para alimentar otros dispositivos compatibles, tiene un puerto USB 2.0 y una radio de 2,4 GHz con alta potencia de 1000 mW.

Figura 17

MikroTik RouterBOARD RB951Ui-2HnD.

Nota. Adaptado de *MikroTik RouterBOARD RB951Ui-2HnD*, por MikroTik (https://i.mt.lv/cdn/rb_images/902_hi_res.png).

Cumple con los estándares de red inalámbrica 802.11 b/g/n, aunque sus antenas estén integradas en el dispositivo MikroTik, esto no produce el menor inconveniente en el despegue de la red inalámbrica. El enrutador se basa en el firmware de nivel 4 de MikroTik RouterOS, lo que brinda facilidad de configuración y una multitud de funciones. Se puede visualizar un resumen de sus especificaciones técnicas en la Tabla 10.

Tabla 10

Especificaciones técnicas del MikroTik RouterBOARD RB951Ui-2HnD.

Detalle	**Descripción**
Código de producto	RB951Ui-2HnD
CPU	AR9344
Núcleos CPU	1
Frecuencia del CPU	600 MHz
Dimensiones	113 x 138 x 29 mm
SO	RouterOS
Licencia	Nivel 4
RAM	128 Mb
Almacenamiento interno	128 Mb
Tipo de almacenamiento	NAND
Estándares	802.11/b/g/n
Máx tasa de transmisión	300 Mbps
Temperatura de funcionamiento	-20°C a 60°C

TP-Link TL-WR840N. El TL-WR840N que se muestra en la Figura 18 es de TP-Link. Este dispositivo es una solución de alta velocidad que cumple con los estándares IEEE 802.11b/g/n. El TL-WR840N, está basado en la tecnología IEEE 802.11n, por lo cual proporciona un rendimiento inalámbrico de hasta 300 Mbps, lo que podemos decir que es suficiente incluso para los requisitos de redes domésticas más exigentes, y hasta llega a ser perfecto para soluciones SOHO.

Figura 18

TP-Link TL-WR840N.

Nota. Adaptado de *TL-WR840N | 300 Mbps Wireless N Router*, por TP-Link (https://www.tp-link.com/en/home-networking/wifi-router/tl-wr840n).

El enrutador tiene cuatro modos de funcionamiento diferentes. Se puede usar en una variedad de modos, incluido el modo de enrutador, el modo de punto de acceso, el modo extensor de rango y el modo WISP. Se puede visualizar un resumen de sus especificaciones técnicas en la Tabla 11.

Tabla 11

Especificaciones técnicas del TP-Link TL-WR840N.

Detalle	**Descripción**
Código de producto	TL-WR840N
Procesador	CPU de un solo núcleo
Dimensiones	182 x 128 x 35 mm
Estándares	WiFi 4: IEEE 802.11n/b/g 2,4 GHz
Máx tasa de transmisión	300 Mbps (802.11n)
Rango WiFi	2x arreglo de antenas
Modos de trabajo	Enrutador, punto de acceso, extensor de rango y WISP
Puertos Ethernet	- 1 x 10/100 Mbps WAN - 4 x 10/100 Mbps LAN
Temperatura de funcionamiento	0°C a 40°C

TP-Link Archer C20. El Archer C20 es el dispositivo que se visualiza en la Figura 19, su fabricante es TP-Link. Estos se encargaron de desarrollar un enrutador económico que satisface las necesidades de hogares y oficinas pequeñas, perfecto para SOHO. Este dispositivo cuenta con doble banda de tripe antena, es decir soporta las bandas de 2,4 GHz y 5 GHz, de esta forma evita interferencias causadas por otros dispositivos. Funciona con los estándares IEEE 802.11b/g/n/ac, proporcionando un rendimiento inalámbrico de hasta 433 Mbps para 802.11ac y 300 Mbps para 802.11n.

Figura 19

TP-Link Archer C20.

Nota. Adaptado de *Archer C20* | *AC750 Wireless Dual Band Router*, por TP-Link (https://www.tp-link.com/en/home-networking/wifi-router/archer-c20).

El router inalámbrico cuenta con tres antenas externas que mejoran la cobertura, incluso en áreas con obstáculos. El enrutador tiene tres modos de funcionamiento diferente, se puede usar el modo enrutador, el modo punto de acceso y el modo extensor de rango. A continuación, se puede visualizar un resumen de sus especificaciones técnicas que ofrece el fabricante en la Tabla 12.

Tabla 12

Especificaciones técnicas del TP-Link Archer C20.

Detalle	Descripción
Código de producto	Archer C20
Procesador	CPU de un solo núcleo
Dimensiones	230 x 144 x 35 mm
Estándares	IEEE 802.11n/b/g 2,4 GHz IEEE 802.11ac/n/a 5 GHz
Máx tasa de transmisión	300 Mbps (802.11n) 433 Mbps (802.11ac)
Rango WiFi	3x arreglo de antenas
Modos de trabajo	Enrutador, punto de acceso y extensor de rango
Puertos Ethernet	- 1 x 10/100 Mbps WAN - 4 x 10/100 Mbps LAN
Temperatura de funcionamiento	0°C a 40°C

Descripción de la problemática existente

En los últimos años las redes de comunicación han ido evolucionando de manera rápida, así como la demanda de los usuarios, entonces como ISP (Internet Service Provider) lo que busca es poder brindar confidencialidad a su red interna inalámbrica para que esta sea segura y confiable. El uso que se da a la red en la empresa Compu Seguridad trae consigo muchos riesgos de seguridad, algunos de ellos se producen por la inexistencia o carencia de mecanismos de seguridad que son insuficientes para proteger el acceso a la información de los usuarios. Al implementar una red inalámbrica o cableada, debe asegurarse de que se implementen las medidas de seguridad adecuadas. El uso de contraseñas para acceder a aplicaciones específicas generalmente no es lo suficientemente bueno para evitar que los piratas informáticos accedan a los recursos de forma no autorizada y, a veces, paralizante. Para proteger adecuadamente su red de intrusos, debe tener mecanismos que utilicen métodos de autenticación probados que controlen el acceso a la red.

El marco general para proporcionar control de acceso a las redes es lo que se conoce como un sistema de autenticación basado en puertos, al que algunas personas se refieren como 802.1X. El concepto principal de este tipo de sistema es bastante sencillo: simplemente verifica que las credenciales que proporciona un usuario indican que el usuario está autorizado para usar la red. Si es así, entonces les permite tener acceso a la red. Si no están autorizados, entonces no les permite tener acceso a la red.

En el levantamiento de la situación actual de la empresa, se identificó que se requiere un sistema centralizado, este permitirá acceder de maneras más eficiente a la red inalámbrica y tener un acceso controlado a la misma. De esta forma se mantendrán seguros los recursos que posee la empresa. Otro punto relevante a considerar es que el sistema deberá ser modular, es decir que se permita hacer cambios sin que estos afecten a los demás equipos que estén en el sistema de la red inalámbrica.

Con esta propuesta y tomando en consideración la infraestructura que tiene la empresa Compu Seguridad, se creará un servicio de autentificación AAA mediante el dispositivo MikroTik RouterBOARD RB951Ui-2HnD, el cual llevará la tarea de realizar un control de acceso seguro a la red y a su vez lleve un registro del desempeño de esta. El hardware y software que se obtiene del dispositivo de MikroTik garantiza el correcto funcionamiento del sistema inalámbrico. Además, es compatible con los demás equipos que ya cuenta la empresa.

Establecimiento de políticas de seguridad

Para establecer políticas de seguridad en este proyecto, se tomará de referencia al estándar ISO/IEC/IEEE 29148:2018 titulado como Ingeniería de sistemas y software — Procesos del ciclo de vida — Ingeniería de requisitos. Como su título lo indica, este estándar tiene relación a la ingeniería de requisitos, por lo tanto, se enfoca en los sistemas y productos de hardware y software a lo largo de su ciclo de vida. (International Organization for Standardization, 2018)

El estándar ISO/IEC/IEEE 29148:2018 define los procesos necesarios a implementar para que el sistema trabaje de manera adecuada durante su ciclo de vida útil. Dicho estándar provee reglas para la aplicación de los requerimientos y procesos relacionados con los requerimientos descritos en los estándares ISO/IEC/IEEE 12207 e ISO/IEC/IEEE 15288 (International Organization for Standardization, 2018). La Tabla 13, que se muestra a continuación, está basada en las consideraciones que plantea el estándar sugerido.

Tabla 13

Requerimientos iniciales del sistema, según estándar ISO/IEC/IEEE 29148:2018.

#	Requerimiento	Prioridad		
		Alta	**Media**	**Baja**
1	No exponer al sistema a altas temperaturas ni a humedad.	X		
2	Poseer una conexión estable a internet para el buen funcionamiento del servicio.	X		
3	Se deberá ingresar a la plataforma vía web o WinBox para poder configurar y gestionar el servicio.	X		
4	El sistema depurará a los usuarios que ya no pertenezcan a la empresa legalmente, así como también a los nuevos.	X		
5	La ubicación del sistema deberá encontrarse con los servidores de la empresa.	X		
6	Se requiere un software con soporte AAA (authentication, authorization, accounting)	X		
7	Se requiere compatibilidad entre la infraestructura con la que cuenta la empresa	X		
8	Se requiere que el sistema siempre este activo.	X		
9	Los empleados tendrán de una tasa de transmisión de datos de 5M y 10M para subida y descarga de datos, respectivamente.	X		
10	Los clientes dispondrán de una tasa de transmisión de datos simétrica de 25M, 35M y 60M, por 24 horas. Dependiendo del plan de internet que deseen contratar.	X		
11	Internet gratuito por 30 minutos al día con una tasa de transmisión de 2M y 5M de subida y descarga de datos, respectivamente.	X		

#	Requerimiento	Prioridad		
		Alta	Media	Baja
12	Solo el administrador del servicio podrá modificar, leer o eliminar datos de la base de datos.	X		
13	Solo se permitirá utilizar 1 dispositivo por usuario.	X		
14	Cada usuario dispondrá de un usuario y contraseña única.	X		
15	El tiempo de conexión al recurso estará asignado por el administrador de toda la red según sea necesario.	X		
16	Se requiere de un Hotspot amigable con el usuario	X		

Diseño del portal cautivo

El portal cautivo es una técnica de autenticación y seguridad de datos que hace que un usuario de una red deba pasar por una página web especial, (normalmente como autenticación) antes de poder acceder a los servicios que ofrece el autenticador. El portal cautivo es en realidad un enrutador o una máquina de puerta de enlace que utiliza un navegador web como medio o dispositivo de autenticación seguro y controlado para proteger y permitir el tráfico hasta que el usuario se registra (Wahyudi, Luthfi, & Efendi, 2019).

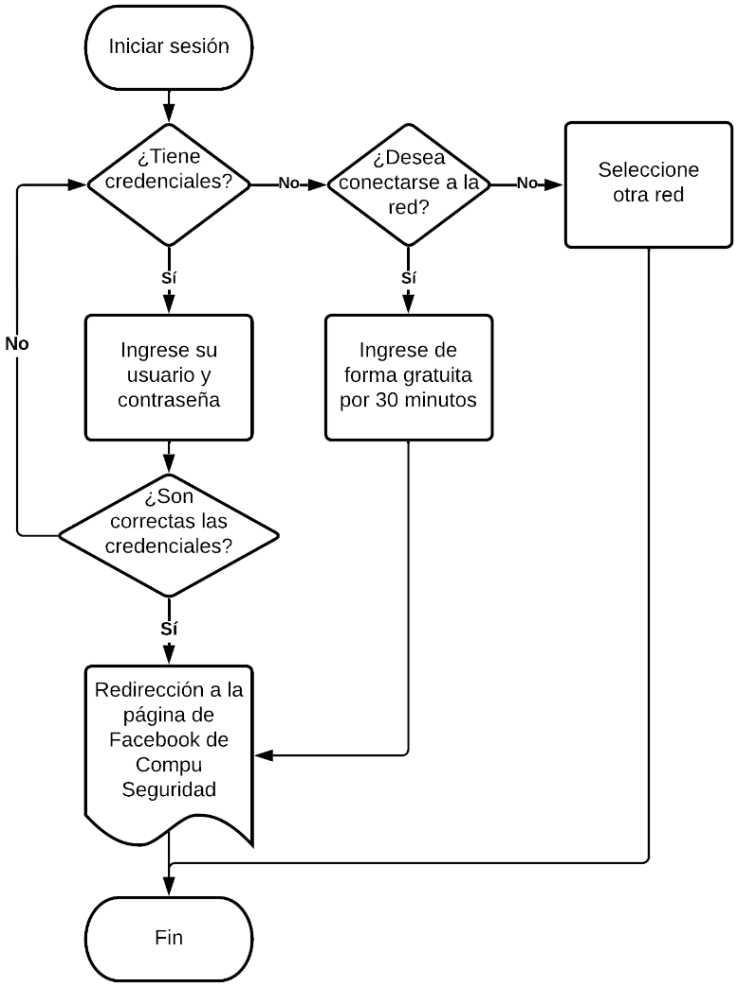
El Portal Cautivo de la empresa Compu Seguridad deberá estar diseñado para cumplir con todos los requisitos que permitan brindar mayor seguridad al momento de autenticarse en la red inalámbrica de la empresa. Asimismo, deberá ser entendible y simple para los usuarios nuevos que accederán. También, debe tener compatibilidad con los dispositivos de la infraestructura de red inalámbrica de la empresa y con los dispositivos de los usuarios que van a acceder.

El Portal Cautivo que se desarrollará en este trabajo de investigación para la empresa seguirá el diagrama de flujo de la Figura 20. En la página de inicio se mostrará un mensaje de bienvenida con el logo de la empresa, el usuario podrá ingresar su nombre de usuario y contraseña, si los tiene, de no tenerlos tendrá la opción de conectarse de manera gratuita por

30 minutos, una vez al día y con un ancho de banda limitado. Además, de información de contacto con el soporte técnico para obtener ayuda en cualquier momento.

Figura 20

Diagrama de flujos del portal cautivo.



El diagrama de flujo de la Figura 20, funciona como se indica a continuación. Primero, si el usuario se conecta a la red inalámbrica de la empresa se abrirá el navegador del dispositivo con la página de inicio de sesión del portal cautivo que podemos visualizar en la Figura 21, esta primero preguntará si tiene credenciales el usuario, de tenerlas debe ingresarlas. Luego el servidor de autenticación validará los datos y si son correctos el portal cautivo se redirigirá a la página de Facebook de la empresa Compu Seguridad y podrá tener acceso a internet, como observamos en la Figura 22.

Figura 21

Página de inicio de sesión del Portal Cautivo.

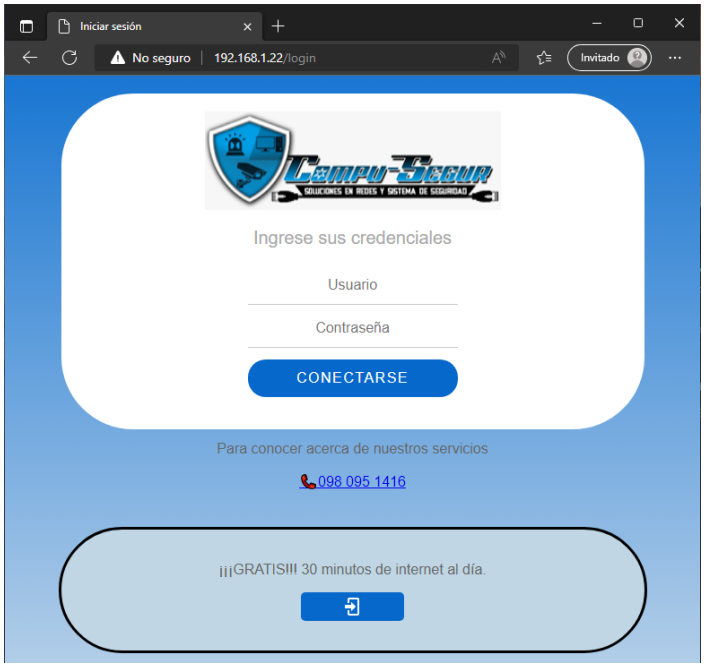


Figura 22

Redireccionamiento a la página de Facebook de la empresa Compu Seguridad.

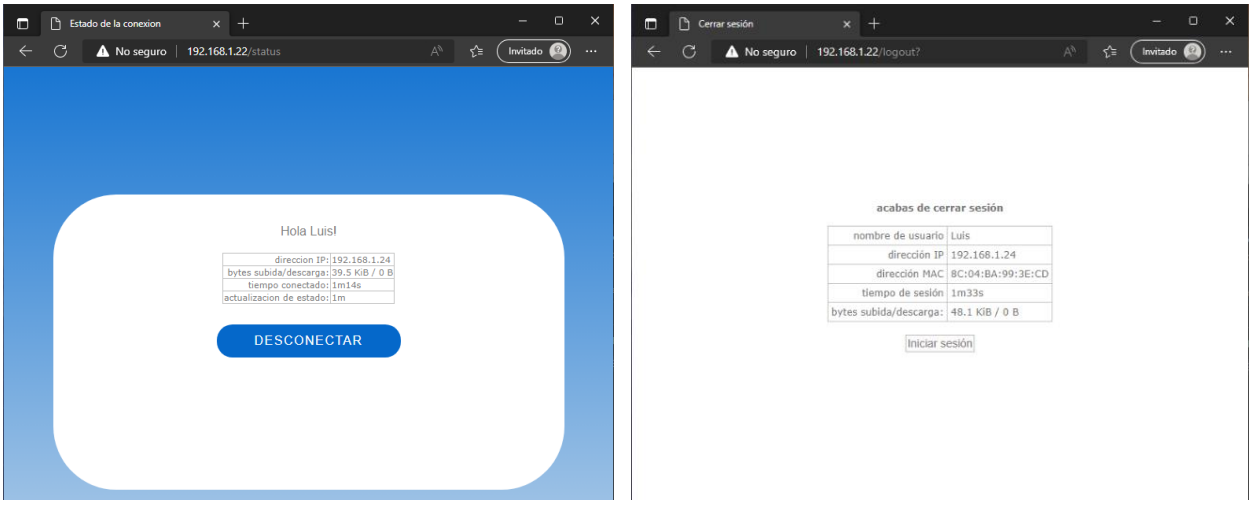
En caso, de que las credenciales ingresadas sean incorrectas o de no tener alguna, el usuario puede optar por la opción de acceder a la red inalámbrica de forma gratuita por 30 minutos, pero en este caso el ancho de banda será menor y podrá hacerlo solo una vez al día, ya que como su nombre lo indica es de manera gratuita, por lo tanto, los recursos son limitados, de hacerlo igualmente será redirigido a la página de Facebook de la empresa y empezará a disfrutar del servicio de internet.

Para crear el Portal Cautivo se tomó de referencia la plantilla que ofrece el dispositivo MikroTik RouterBOARD RB951Ui-2HnD, debido a que será el dispositivo que funcionará como servidor de autenticación y de esta forma se asegura que el sistema del Portal Cautivo tendrá la mejor compatibilidad con el sistema vigente en la empresa. Es indispensable tener conocimientos de HTML5 (HyperText Markup Language, versión 5), para poder trabajar en la plantilla obtenida. HTML5 es la revisión más reciente del estándar HTML desarrollado por el World Wide Web Consortium (W3C). Para publicar información para su distribución global, se necesita un lenguaje que universalmente todas las computadoras puedan entender, este lenguaje de publicación utilizado por la Web es HTML (Hoy, 2012).

Gracias a la plantilla obtenida del dispositivo MikroTik RouterBOARD RB951Ui-2HnD y bajo algunas modificaciones se obtuvo como resultado la Figura 18, este portal cautivo es compatible con las funciones de Hotspot de RouterOS, en donde con un solo click podemos aumentar o quitar funcionalidades del Portal Cautivo, como es el tipo de autenticación que solicitará el servidor de autenticación. Por ejemplo, que no solicite usuario y contraseña para ingresar a la red, sino solamente una contraseña o pin. También, puede quitar el ingreso gratuito a la red inalámbrica (modo trial). Adicionalmente, el usuario puede obtener las estadísticas de conexión que mantiene en la red con ingresar la dirección IP de la puerta de enlace a la que está conectado el dispositivo (Figura 23a), así mismo al desconectarse el usuario obtiene un resumen de las características de su tiempo y consumo de datos en la red (Figura 23b), y si es un usuario trial podrá visualizar el tiempo que le resta para utilizar la red.

Figura 23

a) Estado de la conexión actual, b) resumen del estado de conexión.



a) b)

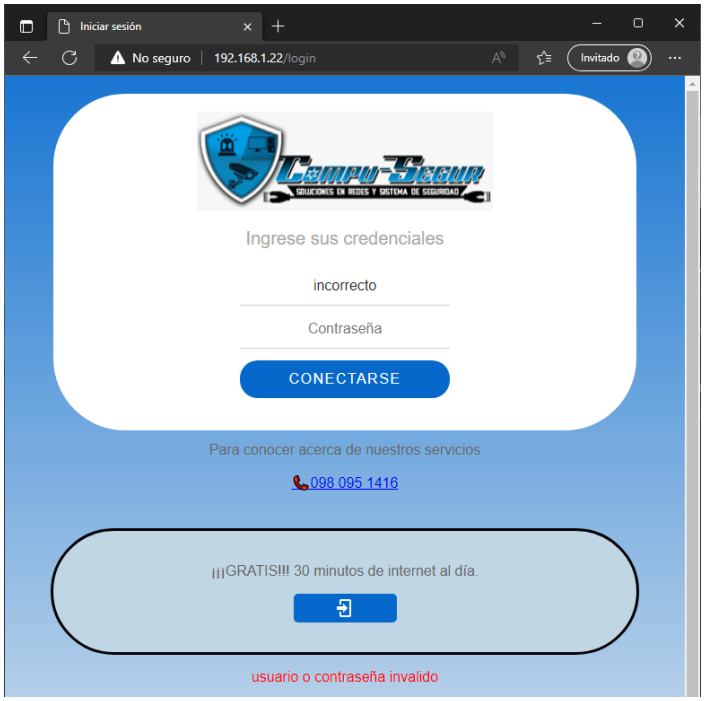
Finalmente, en el Portal Cautivo se complementó con una sección de errores que se muestran al usuario, los cuales son:

- Error interno. Nunca debería suceder. Si es así, se mostrará la página de error mostrando este mensaje de error.
- Error de configuración. Nunca debería suceder si el punto de acceso está configurado correctamente.
- Sin iniciar sesión. Sucederá, si el usuario solicita una página de estado o de cierre de sesión, pero en realidad no ha iniciado sesión.
- ippool-vacío. La dirección IP para el usuario debe asignarse desde el grupo de IP, pero no hay más direcciones en ese grupo.
- Apagando. Cuando se ejecuta el apagado, no se aceptan nuevos clientes.
- Límite de inicio de sesión por usuario. Si el perfil de usuario tiene un límite de usuarios compartidos, este error se mostrará después de alcanzar este límite.
- Nombre de usuario MAC incorrecto. Si el nombre de usuario parece una dirección MAC, pero no es una dirección MAC de este cliente, se rechaza el inicio de sesión.

- chap-desaparecido. Si se utiliza el método de inicio de sesión http-chap, pero el programa de punto de acceso no recibe la contraseña cifrada, se muestra este mensaje de error.
- Nombre de usuario no válido. Caso más general de nombre de usuario o contraseña no válidos. Ver Figura 24.
- MAC inválida. Los usuarios locales (en el servidor de punto de acceso) pueden vincularse a alguna dirección MAC. Si se intenta iniciar sesión desde una MAC diferente, se mostrará este mensaje de error.
- Límite de tiempo de actividad, límite de tráfico. Para usuarios de puntos de acceso locales en caso de que se alcancen los límites.
- tiempo agotado de RADIUS. El servidor RADIUS autentica al usuario, pero no recibe ninguna respuesta, se mostrará el siguiente error.

Figura 24

Mensaje de error "usuario o contraseña invalido" del Portal Cautivo.

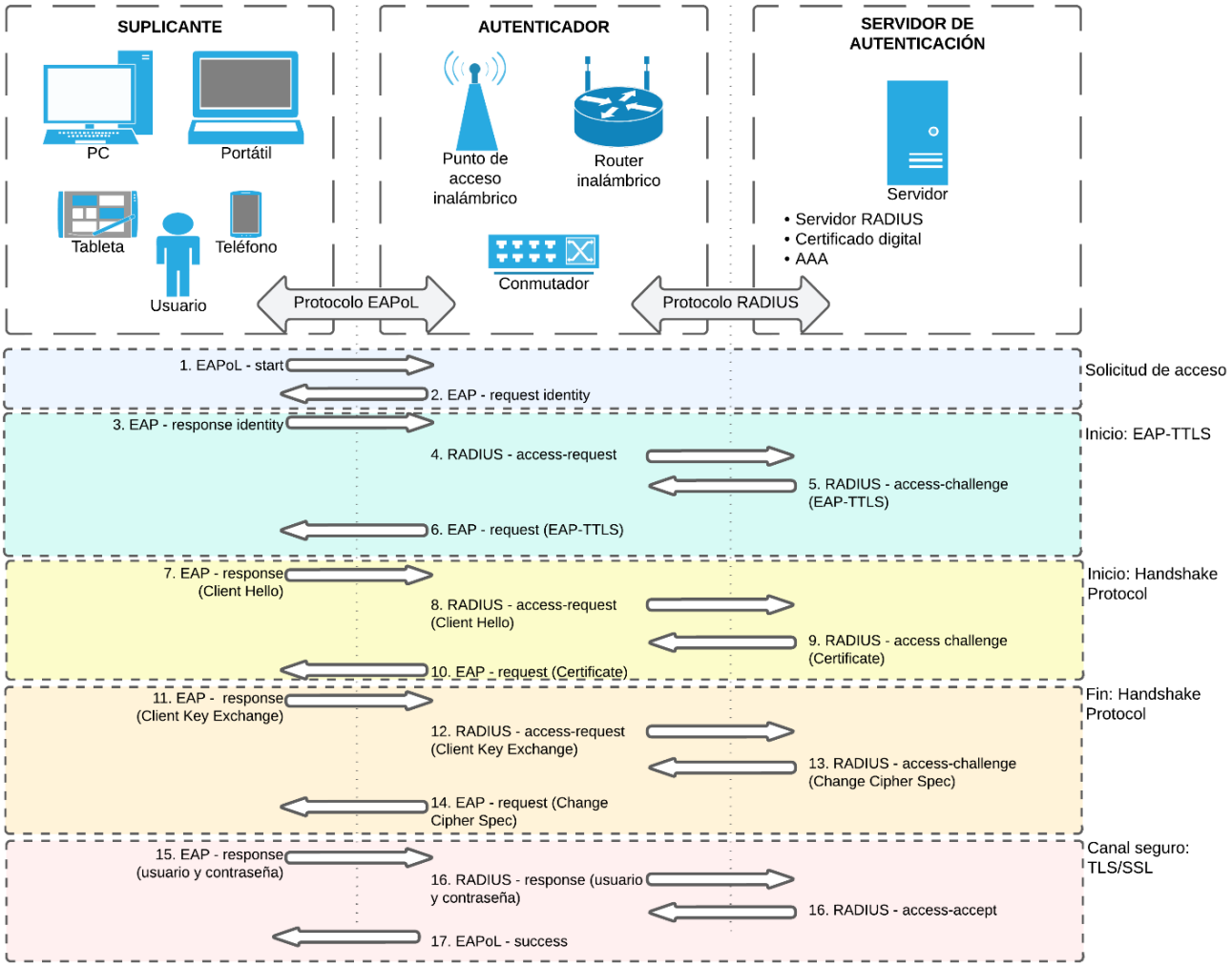


Diseño de la red inalámbrica

El diseño de la red inalámbrica para la empresa Compu Seguridad se basa bajo el sistema AAA (autenticación, autorización y contabilización) emitido por el IETF para el estándar IEEE 802.1X y tener total control sobre el acceso de red, el modelo usado en la implementación se muestra en la Figura 25. El diseño se lo realizó tomando en consideración todos los requisitos del estándar 802.1X usando como método de autenticación EAP-TTLS y con la reutilización de la infraestructura de red inalámbrica de la empresa.

Figura 25

Diseño de la red inalámbrica con el estándar 802.1X y autenticación EAP-TTLS para la empresa Compu Seguridad.



La infraestructura de red inalámbrica que se va utilizar es la misma que tenemos en la Figura 14, es la actual de la empresa Compu Seguridad, la cual está bien armada pero el inconveniente es que no está configurada correctamente. Debido a que la empresa es una ISP cuenta con buenos equipos de comunicación. Además, el despliegue de la red Wi-Fi dentro del edificio está bien distribuida. El inconveniente presentado se debe a la falta de conocimiento acerca de la seguridad inalámbrica.

El dispositivo MikroTik RouterBOARD RB951UI-2HnD, será el protagonista del sistema de portal cautivo con autenticación EAP-TTLS con protocolo RADIUS. El dispositivo cuenta con una licencia de nivel 4 del sistema operativo RouterOS, el cual nos permite realizar las actividades detalladas en la Tabla 14, a continuación:

Tabla 14

Características del RouterOS nivel 4.

Características	**4 (WISP)**
AP inalámbrico	Sí
Cliente inalámbrico y puente	Sí
Protocolos RIP, OSPF, BGP	Sí
Túneles EoIP	Ilimitado
Túneles PPPoE	200
Túneles PPTP	200
Túneles L2TP	200
Túneles OVPN	200
Interfaces VLAN	Ilimitado
Usuarios activos de Hotspot	200
Cliente RADIUS	Sí
Colas	Ilimitado
Proxy web	Sí
Sesiones activas del User manager	20
Número de agentes KVM	Ilimitado

Nota. Esta tabla muestra las características que ofrece el Nivel 4 de RouterOS. Adaptado de *Manual:License*, por MikroTik Documentation, (https://wiki.mikrotik.com/wiki/Manual:License).

User Manager

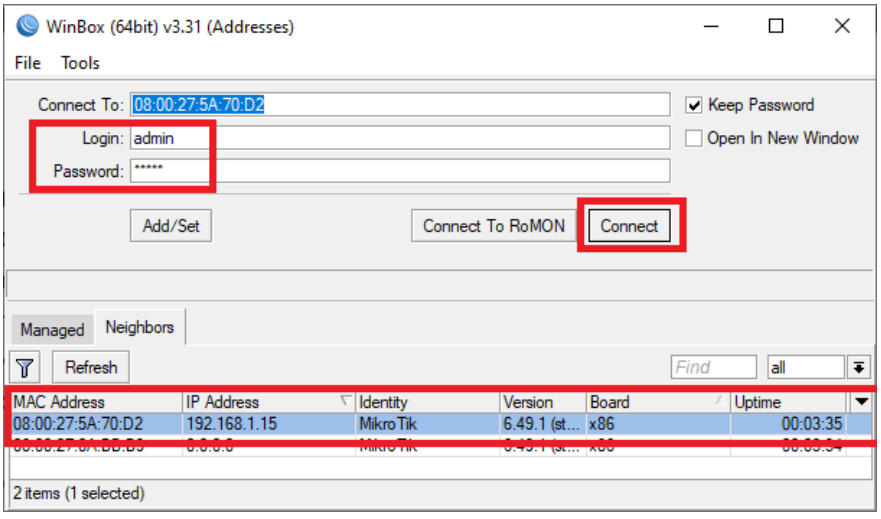
El servidor RADIUS dentro de las configuraciones del dispositivo de MikroTik RouterBOARD RB951UI-2HnD lo podemos encontrar como User Manager (UM). El UM es un sistema de administración que se puede usar en varias configuraciones, se puede utilizar para usuarios de Hotspot, PPP, DHCP, Wireless y RouterOS. User Manager es una aplicación de servidor RADIUS. El primer paquete de prueba de mensajería unificada se introdujo en la versión 4 de RouterOS. El paquete de administrador de usuarios es compatible con todas las arquitecturas de RouterOS, incluidas x86 y Cloud Host Router (Hari & Amin, 2022).

Lo primero que se debe hacer en un dispositivo de MikroTik con RouterOS de nivel 4 o superior, en el que se desee agregar un servidor RADIUS por medio de UM, es verificar que UM este instalado en el equipo. Para ello seguimos los siguientes pasos para verificar y descargar User Manager en un dispositivo MikroTik:

1. Con la herramienta WinBox de MikroTik ingresamos a las configuraciones del dispositivo. Para ello seleccionamos al dispositivo de MikroTik que vamos a acceder por medio de la dirección MAC o dirección IP, luego escribimos el usuario y contraseña, como observamos en la Figura 26.

Figura 26

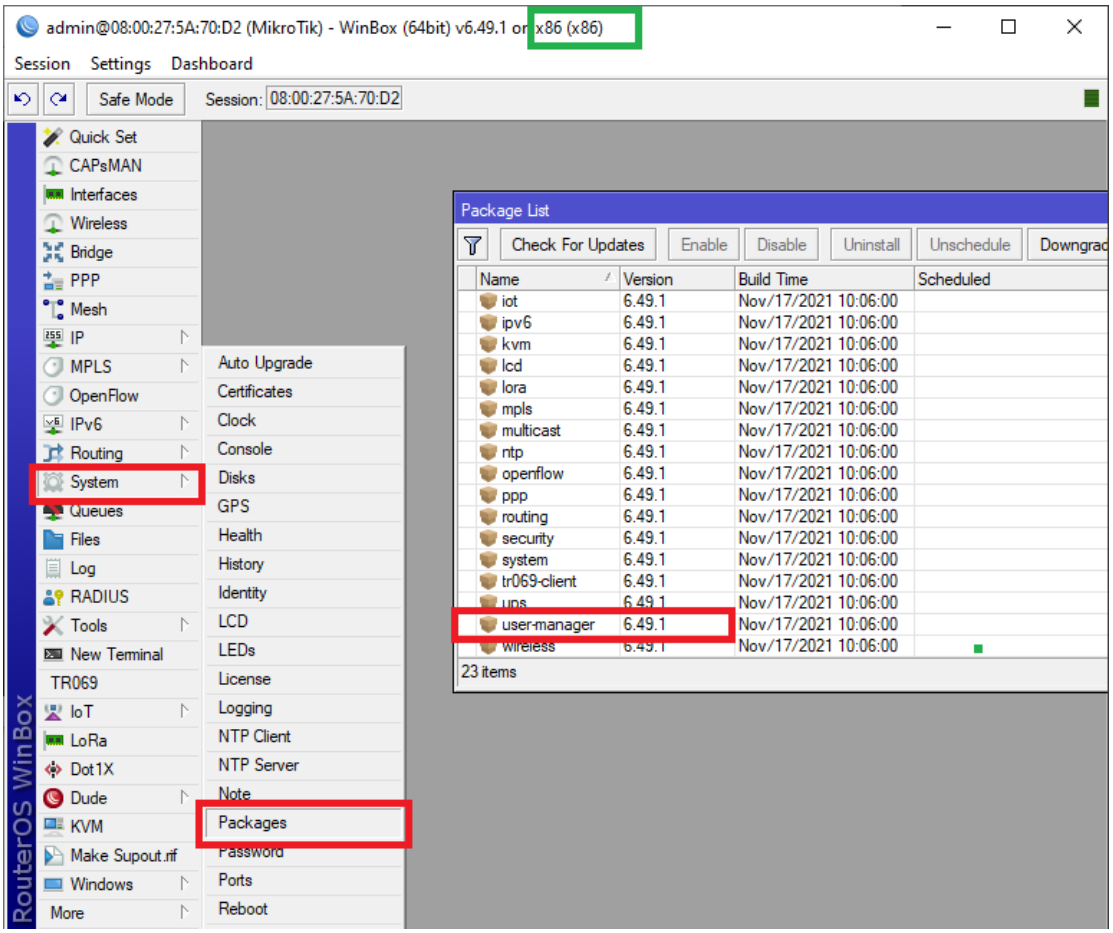
WinBox, ingreso a la configuración de los equipos MikroTik.



2. Dentro de las configuraciones del router seleccionamos System y Packages, como observamos en la Figura 27. Esto nos abrirá la lista de paquetes que tenemos instalado en nuestro dispositivo, en ella verificamos que se encuentre instalado el paquete user-manager.

Figura 27

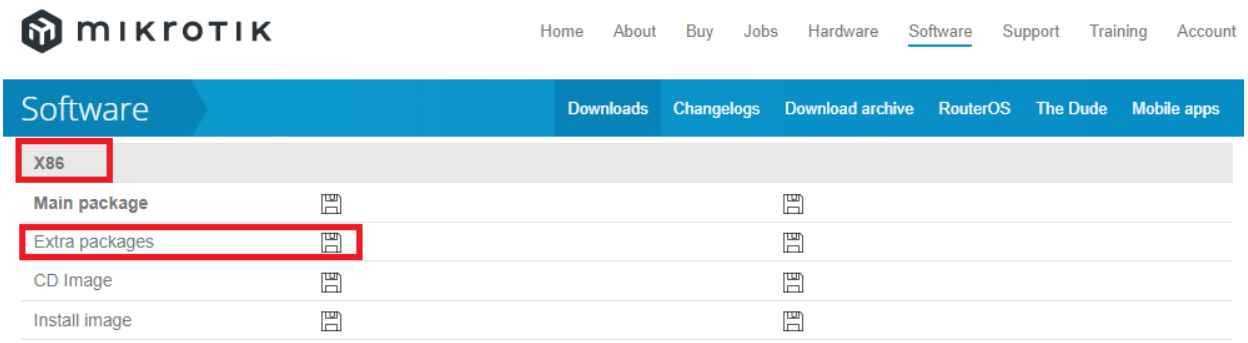
WinBox, ingreso de la lista de paquetes del dispositivo.



3. De no tener instalado el paquete user-manager, debemos descargarlo desde la página de MikroTik en el apartado de Software, ver Figura 28. Primero desde el WinBox verificamos la arquitectura que corre nuestro dispositivo, cuadro verde en la Figura 27, luego en la página de MikroTik descargamos el archivo Extra packages para nuestro dispositivo.

Figura 28

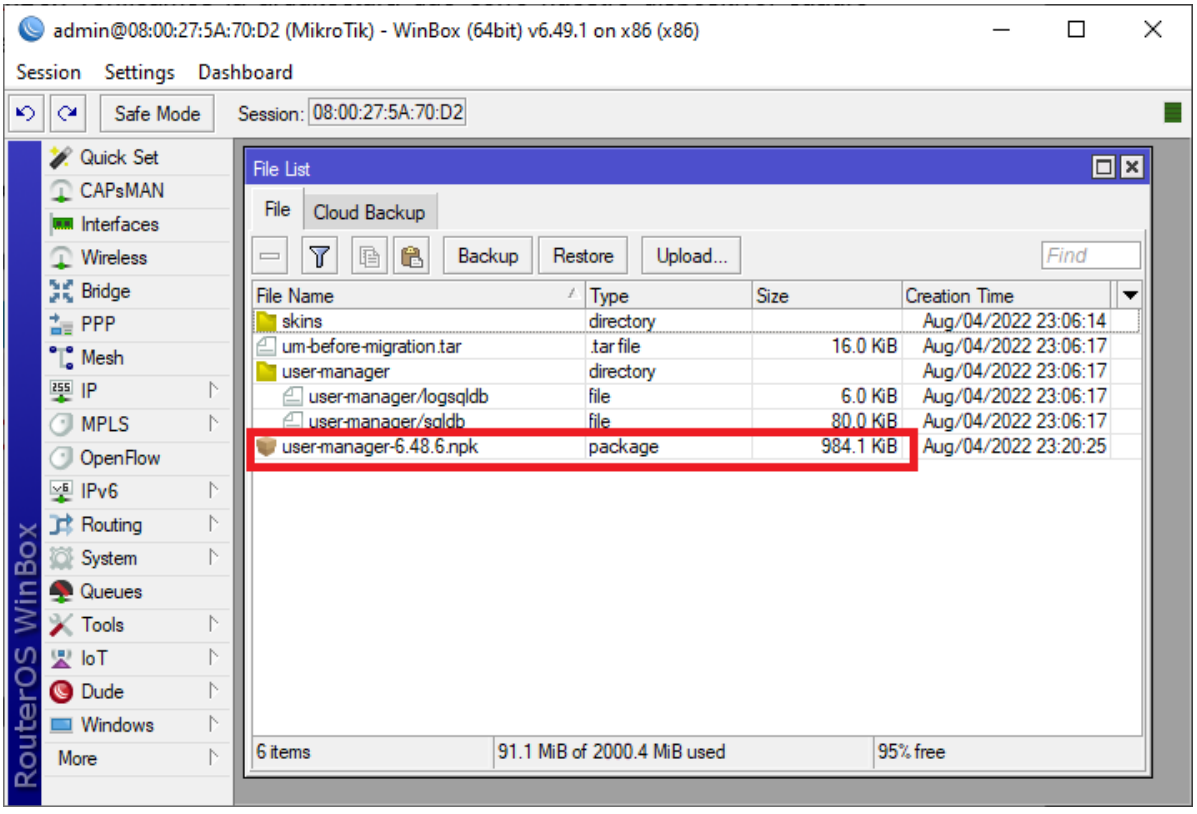
Descarga del paquete user-manager para RouterOS.



4. Una vez descargado, abrir el archivo comprimido y localizamos el paquete user-maganer, el cual debemos arrastrar hasta la carpeta files del WinBox como observamos en la Figura 29. Luego reiniciamos el equipo y al encenderse ya estará instalado el paquete.

Figura 29

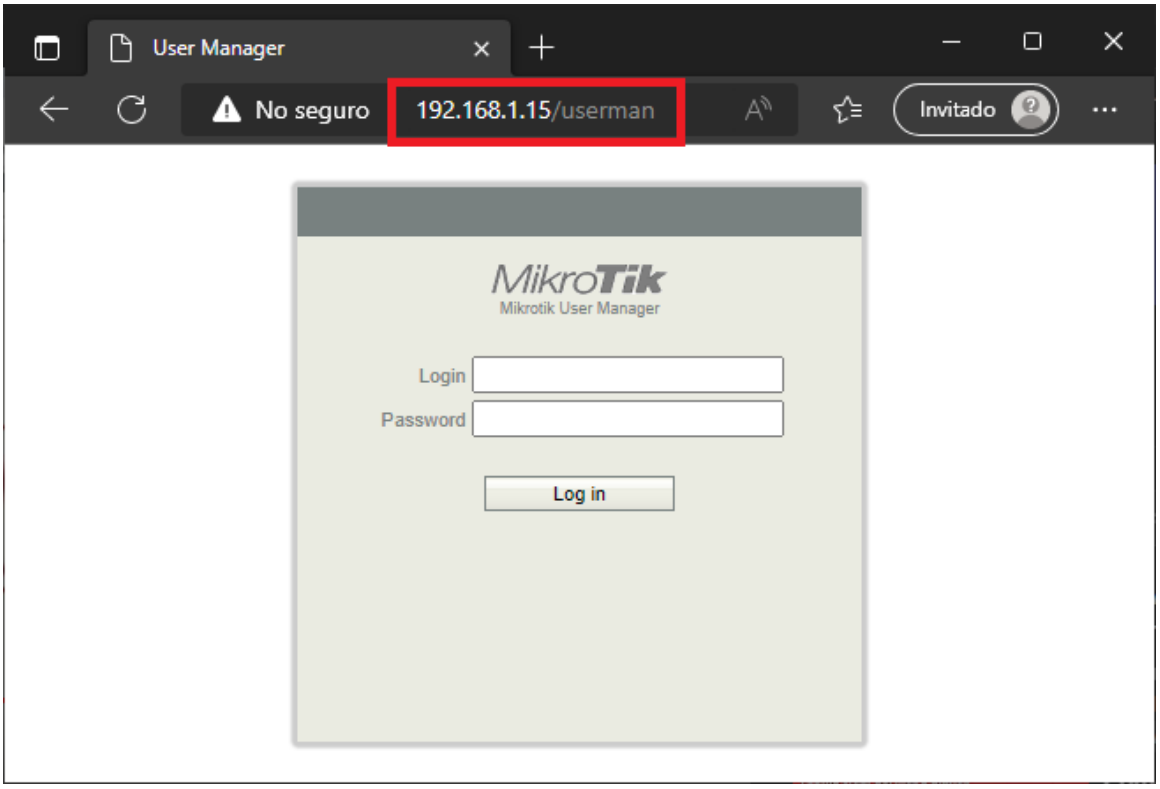
WinBox, instalación del paquete user-manager.



Para ingresar a User Manager debemos hacerlo desde el navegador con la Gateway de nuestro dispositivo agregando al final /userman, ver Figura 30. Ejemplo si nuestra Gateway es 192.168.1.1, para ingresar al UM debemos escribir en el navegador 192.168.1.1/userman.

Figura 30

Página de inicio de sesión del User Manager.



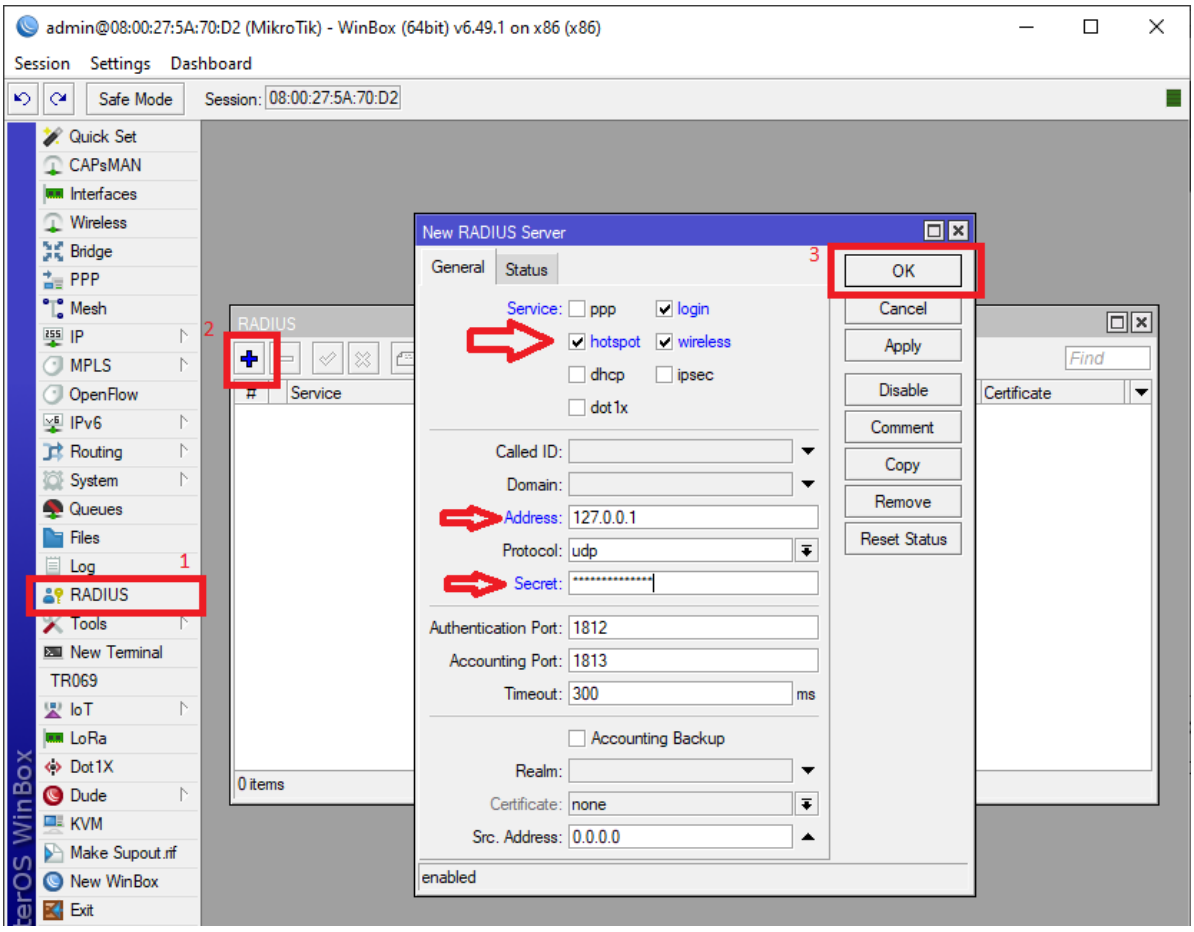
Si se ingresa por primera vez al User Manager debemos ingresar en Login “admin” y Password dejar en blanco. Esto se debe a que nunca se ha hecho la configuración del dispositivo y las credenciales que entrega MikroTik por defecto, son estas. Por lo tanto, hay que tomar en cuenta que un paso primordial es cambiar el usuario y contraseña del User Manager para evitar manipulaciones del mismo.

Antes de continuar con el paquete User Manager, debemos primero configurar dentro WinBox al equipo como servidor RADIUS. Para ello nos dirigimos a la opción RADIUS en el panel de la izquierda, nos mostrará una ventana en la que agregaremos un nuevo servidor RADIUS dando click en el “+”. En esta nueva ventana seleccionamos los servicios de hotspot,

login y wireless, ya que son los servicios que usaremos para este servidor RADIUS. En Address ingresamos la dirección IP de loopback que es 127.0.0.1, ya que nuestro equipo será el servidor de autenticación o servidor RADIUS. Finalmente, ingresamos una contraseña secreta en Secret, la cual nos entregará un paso más de seguridad para configurar el servidor RADIUS en el User Manager y por último le damos click en Apply y Ok, ver Figura 31.

Figura 31

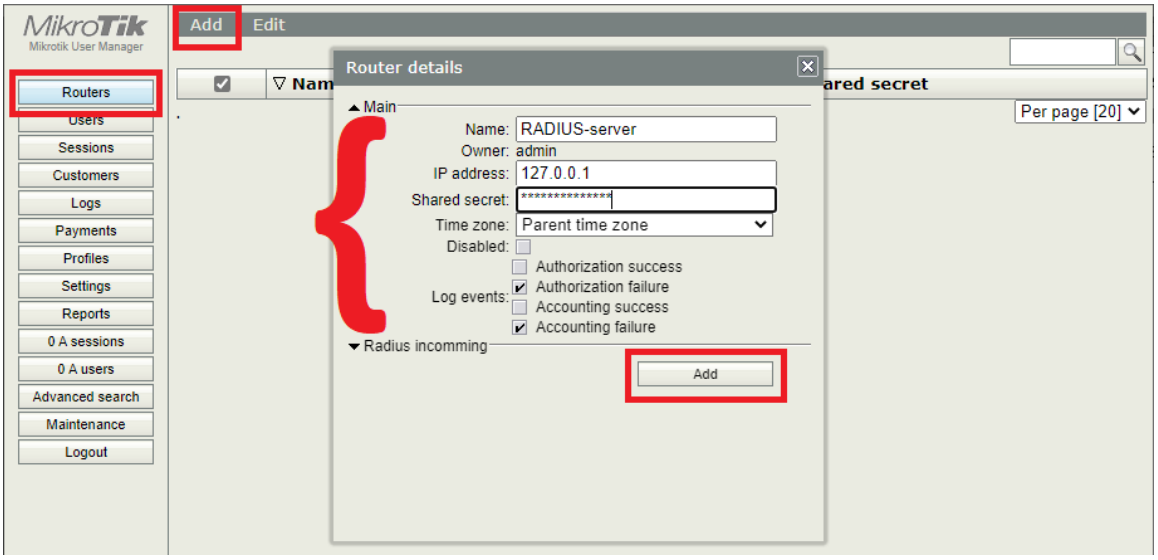
WinBox, configuración del servidor RADIUS.



Ahora sí, nos dirigimos al User Manager y seleccionamos la opción Routers en el panel de la izquierda, damos click en Add y completamos con la información que ingresamos en WinBox, ver Figura 32. Con esto se encuentra activado el protocolo RADIUS en el equipo de MikroTik, pero eso no significa que ya esté completamente configurado.

Figura 32

User Manager, configuración del servidor RADIUS.



Creación de perfiles

Configurado el servidor RADIUS dentro del User Manager de MikroTik procedemos a crear los perfiles de usuario que fueron mencionados en la Tabla 13 de las políticas de seguridad para la empresa Compu Seguridad. Para ello primero creamos las limitaciones de tiempo del uso de la red y velocidad de transmisión para cada tipo de usuario, lo cual observamos en la Tabla 15.

Tabla 15

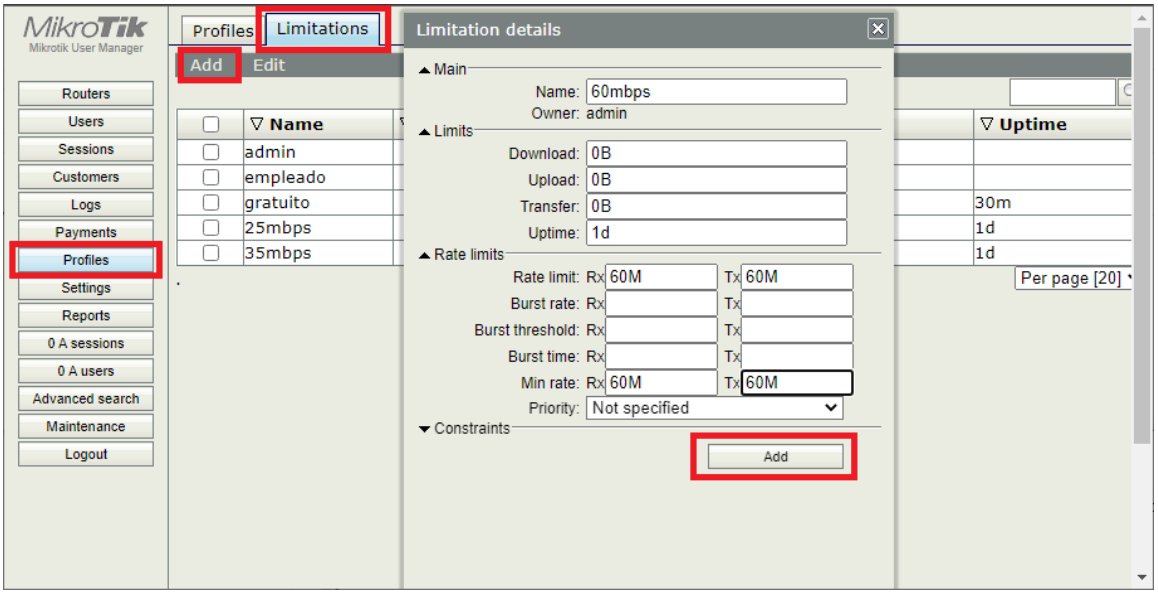
Límite de tiempo y tasa de transmisión para los usuarios de la red inalámbrica.

Tipo de usuario	Tiempo de uso	Tasa de transmisión Rx/Tx
Administrador	Ilimitado	50 Mbps / 100 Mbps
Empleado	Ilimitado	5 Mbps / 10 Mbps
Gratuito	30 minutos	2 Mbps / 5 Mbps
Plan 25 Mbps	24 horas	25 Mbps / 25 Mbps
Plan 35 Mbps	24 horas	35 Mbps / 35Mbps
Plan 60 Mbps	24 horas	60 Mbps / 60Mbps

Desde UM nos dirigimos a la opción Profiles del panel de la izquierda, en el menú superior seleccionamos Limitations y damos click en Add para agregar las limitaciones mencionadas en la Tabla 14, ver Figura 33.

Figura 33

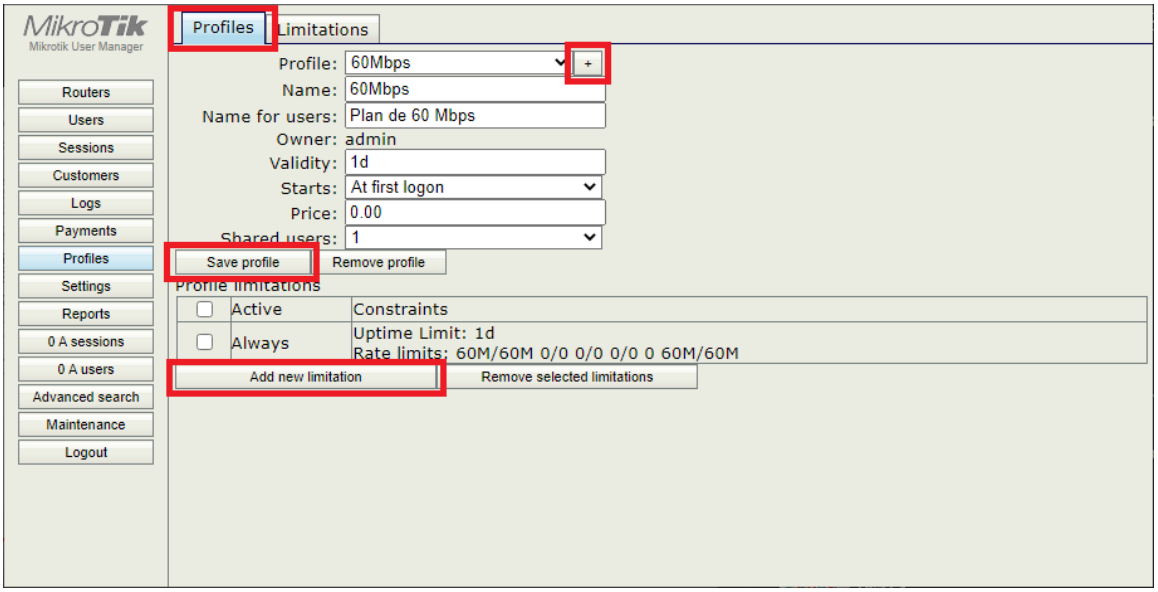
User Manager, creación de limitaciones.



Luego procedemos a crear los perfiles de usuario, para ello en la misma página damos click en Profiles en el menú superior. Para añadir un nuevo perfil de usuario damos click en el "+" que tenemos a lado de Profile. Procedemos a escribir el nombre del perfil, escribimos el tiempo de validez del usuario, seleccionamos cuando dispositivos pueden acceder por usuario y como se especificó en la Tabla 14, solo puede acceder un dispositivo por usuario. Finalmente agregamos la limitación correspondiente al perfil y procedemos a guardar los cambios, como podemos observar en la Figura 34.

Figura 34

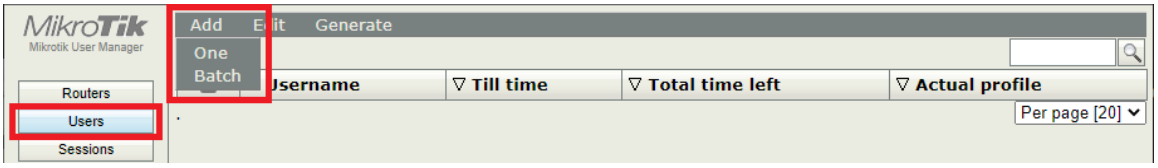
User Manager, creación de perfiles de usuario.



Ahora crear y administrar usuarios que puedan acceder a la red inalámbrica, nunca fue más fácil. Para ello desde User Manager, en el panel de la izquierda seleccionamos la opción de Users, aquí tenemos dos opciones para crear nuevos usuarios, podemos crear un solo usuario (One) o crear un grupo de usuario (Batch), ver Figura 35.

Figura 35

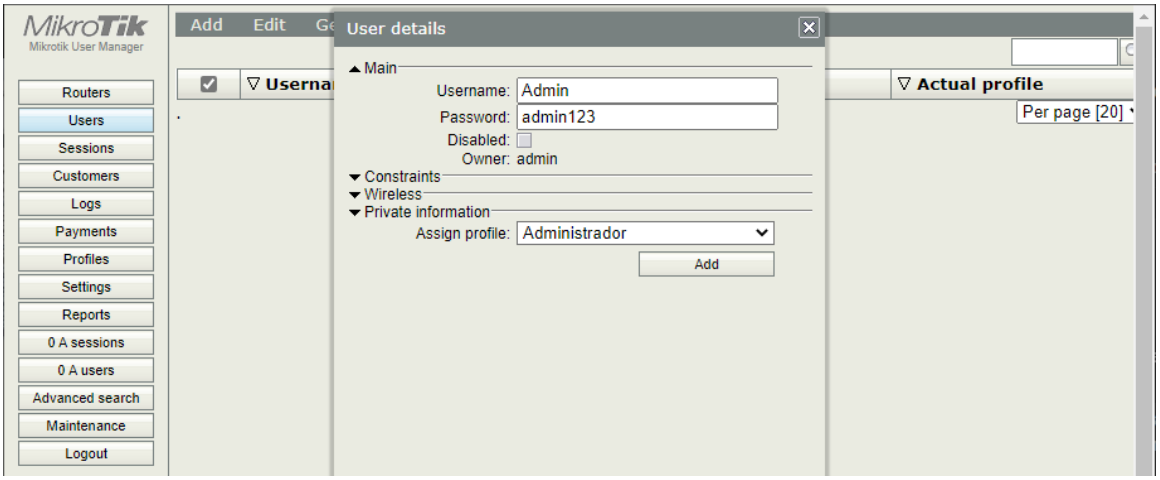
User Manager, creación de usuarios.



Para crear un solo usuario seleccionamos en el menú superior la opción Add y luego damos click en One, nos aparecerá una ventana de User details, desde la cual ingresamos los datos del usuario de la red inalámbrica, como usuario, contraseña y le asignamos el perfil de usuario que tendrá en la red, ver Figura 36.

Figura 36

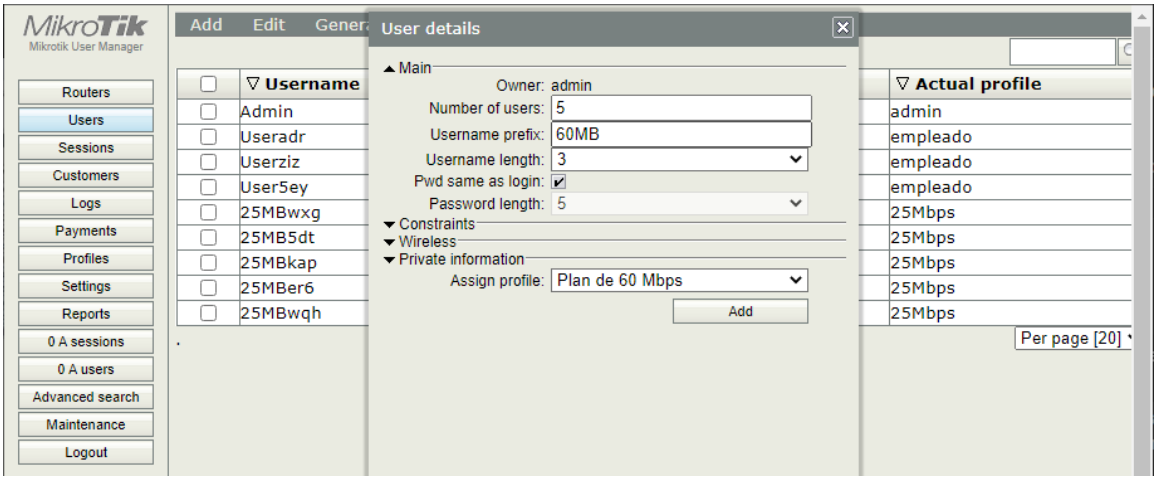
User Manager, creación de un solo usuario.



Si deseamos crear un grupo de usuario de forma más simple, seleccionamos la opción Batch. Se nos abrirá una ventana que nos permitirá decidir cuantos usuarios deseamos crear, si deseamos ingresar un prefijo al nombre de usuario, cuantos caracteres adicionales contendrá el nombre de usuario, de cuantos caracteres aleatorios será la contraseña del usuario, si la contraseña del usuario será la misma que el usuario y finalmente asignamos el perfil de este grupo de usuario, ver Figura 37.

Figura 37

User Manager, creación de un grupo de usuarios.



Vouchers

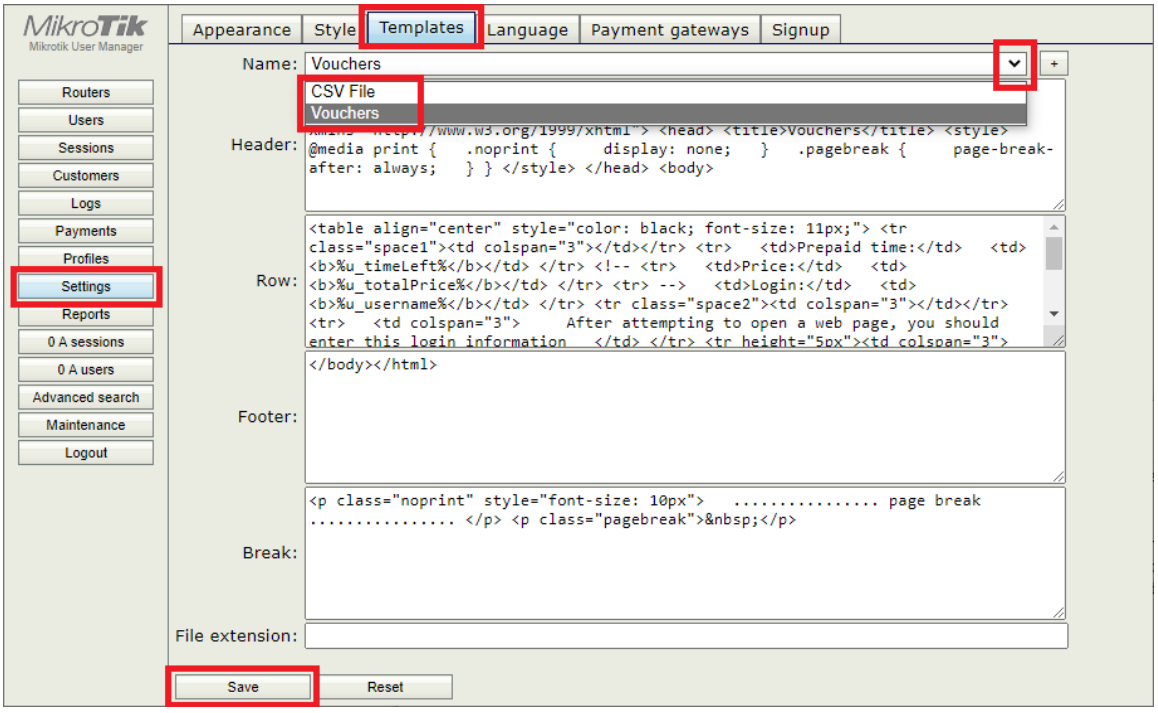
Una herramienta imprescindible que tiene User Manager es la creación de Vouchers, por medio de archivo CSV o HTML. Un Voucher sería un cupón con el nombre de usuario y contraseña que permitirá ingresar a la red inalámbrica, pero UM permite seleccionar uno, varios o todos los usuarios para obtener una lista de Vouchers.

Para ello la creación de los Vouchers UM, tiene unas plantillas que se pueden editar para agregar información relevante del dueño de la red inalámbrica. Además, existen páginas web que se especialización en la creación de Vouchers en CSV y HTML para User Manager, páginas como kangndo.com, mikrotikthemes.airpoint.club, binaryheartbeat.net, entre otras.

Para cambiar el modelo de Vouchers, desde UM nos dirigimos a la opción Settings del panel de la izquierda, seleccionamos Templates y aquí elegimos si deseamos cambiar el modelo de CSV o HTML (Vouchers), ver Figura 38.

Figura 38

User Manager, configuración de Vouchers.



Para generar los Vouchers nos dirigimos a Users en el panel de la izquierda del User Manager, seleccionamos las credenciales de los usuarios que deseamos que aparezcan en la generación del Voucher, luego en el menú superior seleccionamos Generate y damos click en Vouchers, así como se visualiza en la Figura 39. Obtenemos como resultado la plantilla de vouchers de la Figura 40.

Figura 39

User Manager, generación de Vouchers.

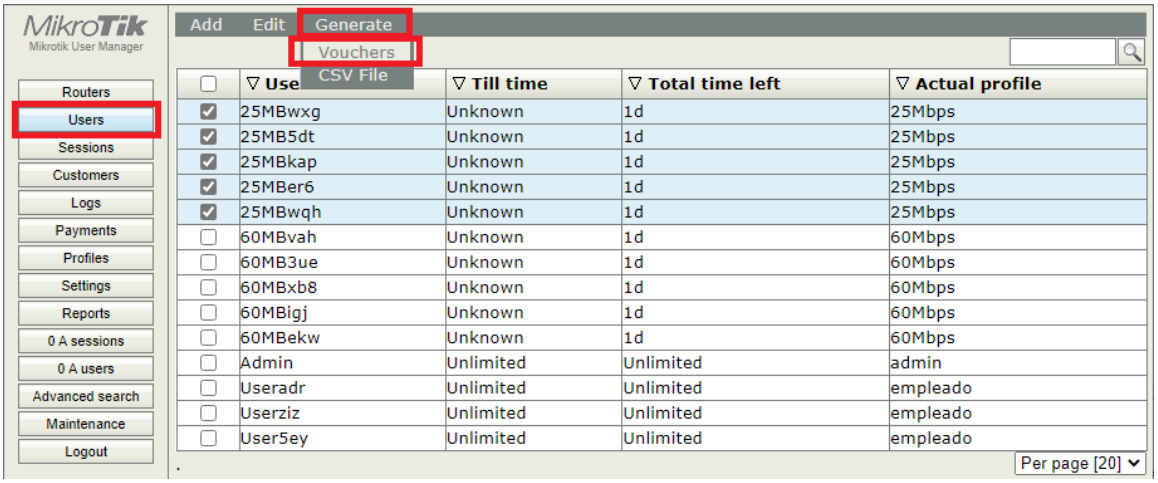
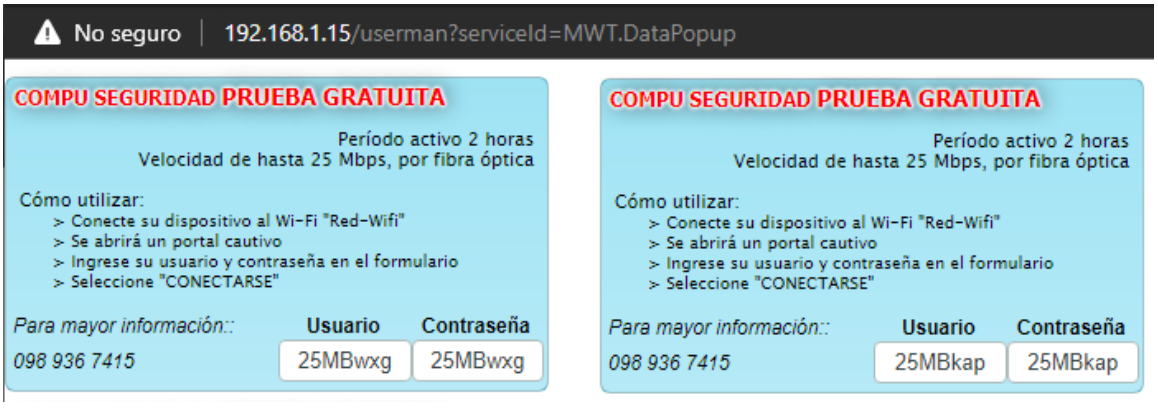


Figura 40

Vouchers de la empresa Compu Seguridad.



En la Figura 40, observamos toda la información que podemos colocar dentro de un Voucher, pero sin olvidar el nombre de usuario y contraseña para poder acceder a la red inalámbrica. Cabe destacar que este modelo de voucher es modificado, no es igual al de la plantilla que

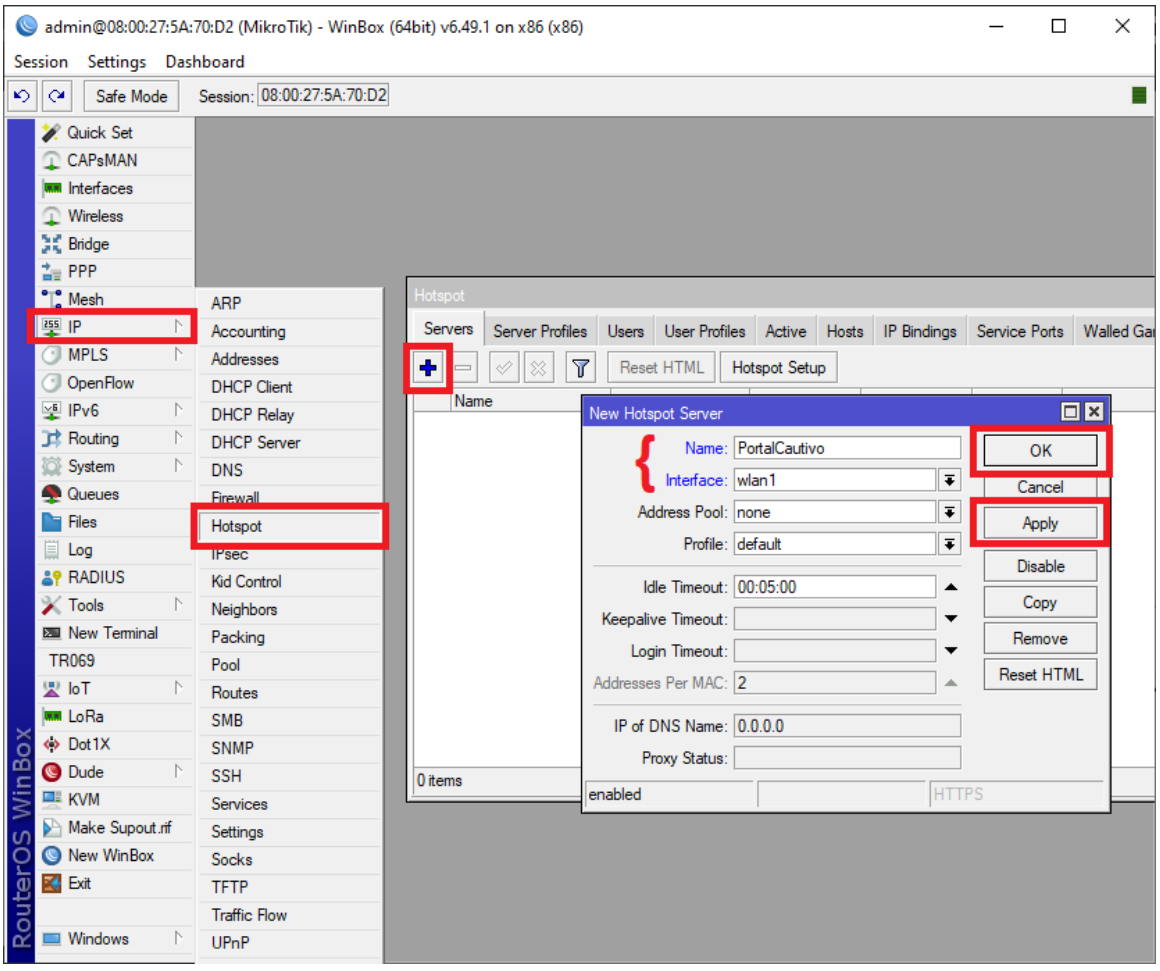
ofrece User Manager. El voucher es generado como un archivo HTML y fácilmente se lo puede imprimir para repartirlos o guardarlo en PDF.

Hotspot

RouterOs, ofrece la creación de un Hotspot y para configurarlo es necesario abrir WinBox y seleccionar la herramienta IP, seguido de Hotspot, nos aparecerá la ventana de Hotspot y damos click en el “+”. Se abrirá una nueva ventana de creación de un servidor Hotspot, aquí escribimos el nombre del servidor y seleccionamos la interface del dispositivo MikroTik que tendrá activo el Hotspot, como este trabajo de titulación trata de una red inalámbrica seleccionamos la interfaz Wi-Fi, wlan1. Como podemos observar en la Figura 41.

Figura 41

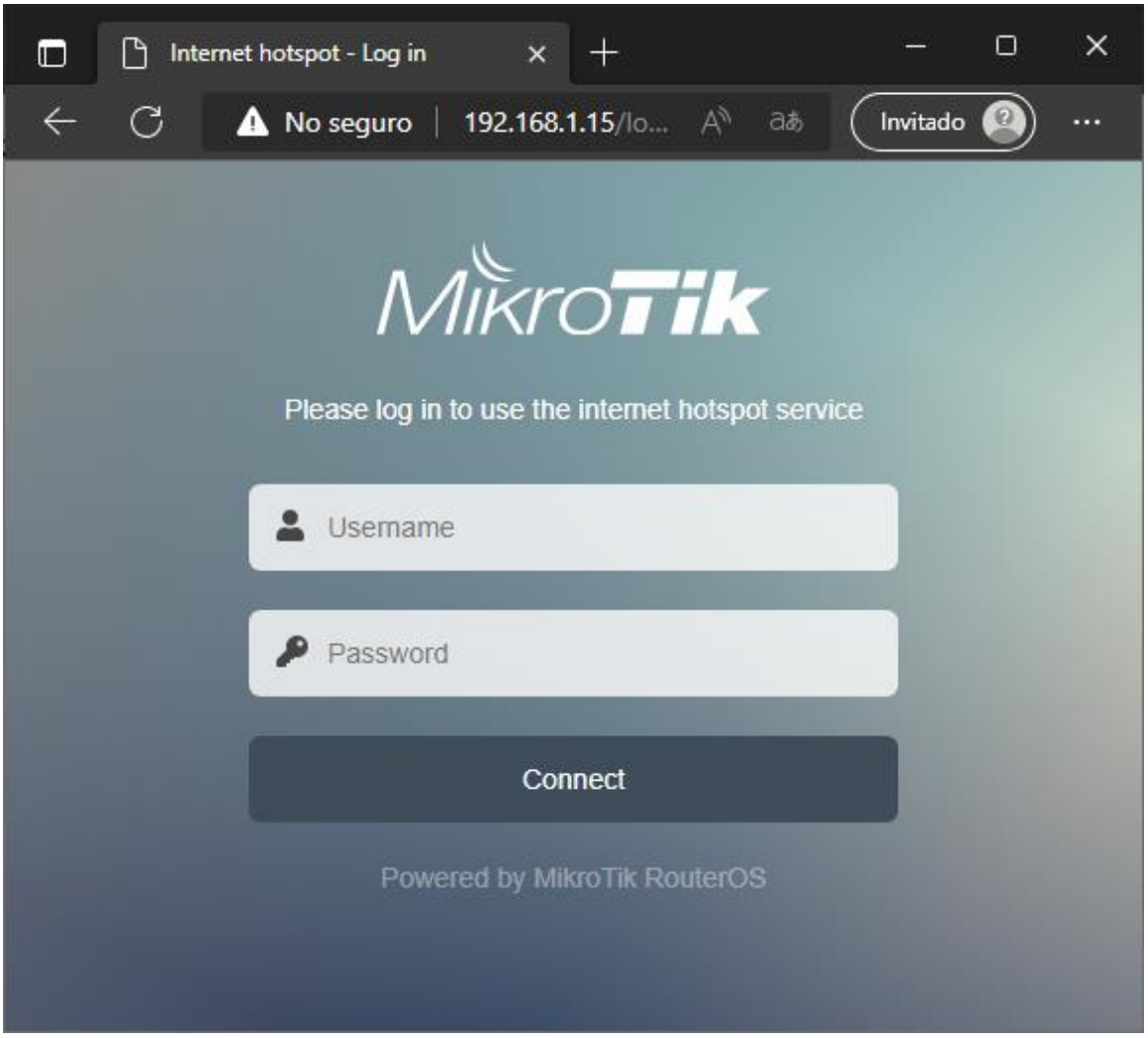
WinBox, configuración de un servidor Hotspot.



Al crear este servidor Hotspot, si nos conectamos a través de la red inalámbrica del dispositivo MikroTik, nos aparecerá el portal cautivo de la Figura 42. Además, el portal captivo se conectará con la autenticación por defecto de RouterOS que es CHAP, la cual está basada en el método EAP legacy, la cual carece de seguridad. También, hay que tomar en cuenta que no está enlazado con el servidor RADIUS User Manager, por lo que los usuarios creados en UM, no tendrán ninguna validez.

Figura 42

Hotspot por defecto de MikroTik.

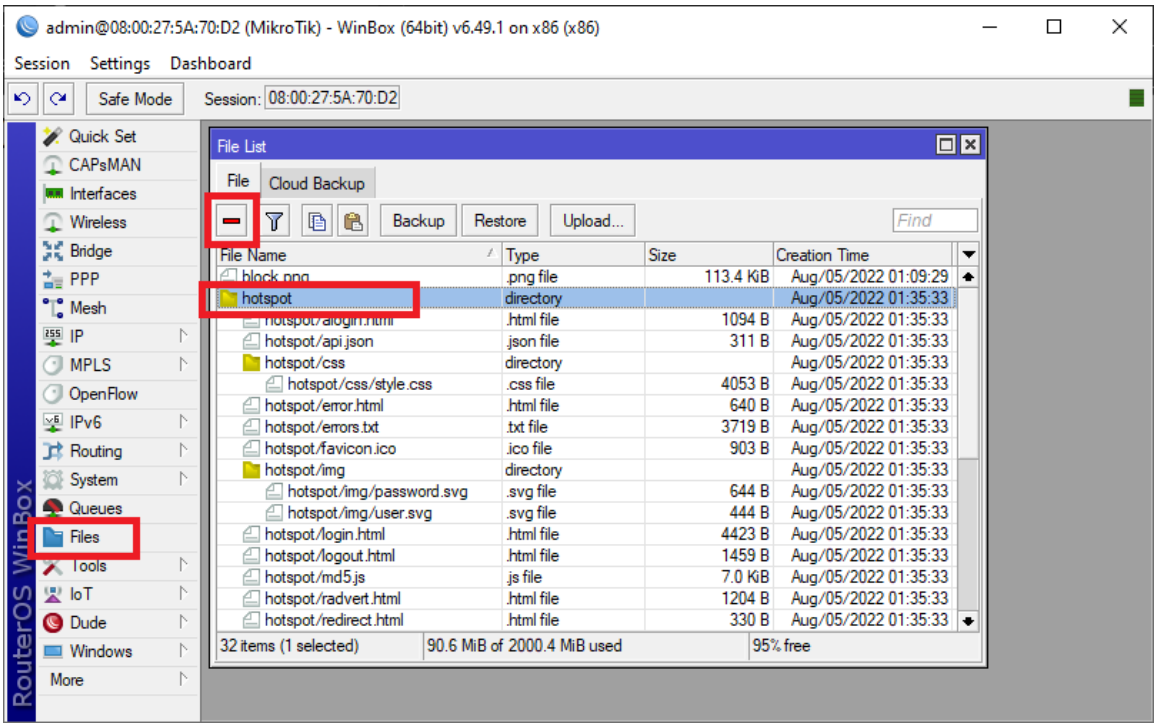


Para cambiar el Hotspot por defecto de MikroTik y cargar un diseño de autoría propia. Primero se debe dar click en Files del panel de la izquierda de WinBox, localizamos la carpeta

hotspot y procedemos a eliminarla, ver Figura 43. Una vez eliminada, para cargar el nuevo hotspot basta con arrastrar la carpeta que contengan los archivos de HTML. Luego ingresar a la red inalámbrica para comprobar que se haya cargado el nuevo hotspot, de no obtener resultado, intente reiniciando el dispositivo.

Figura 43

Cambio de hotspot desde WinBox.



Creación de certificados

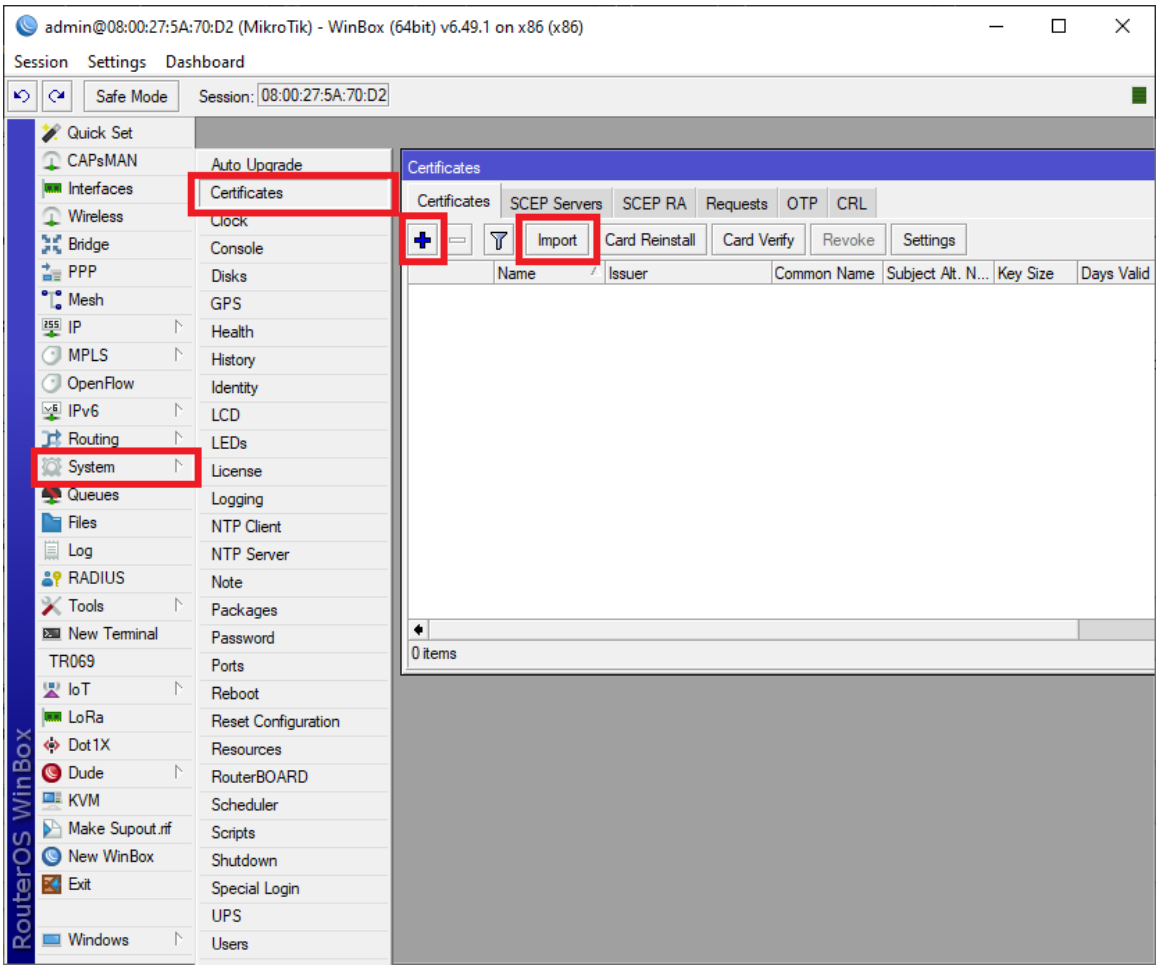
El sistema de autenticación de la red inalámbrica de la empresa Compu Seguridad debe ser EAP-TTLS y por ello se necesita crear dos certificados, el uno es por una entidad de certificación de confianza (CA, Certificate Authority) y el otro es un certificado auto firmado para el servidor RADIUS.

Para crear estos certificados existen un sin número de herramientas. Una de ella es la proporcionada por RouterOS, Certificates. Se puede hacer uso de esta herramienta desde el CLI del dispositivo o a través de WinBox.

Si deseamos crear los certificados por medio de WinBox, primero debemos dirigirnos a la opción System en el panel izquierdo y seleccionar Certificates, se nos abrirá la ventana que contiene los certificados del dispositivo. Además, aquí podemos crear o importar certificados que hayamos creado con otra herramienta, como podemos ver en la Figura 44.

Figura 44

WinBox, certificados del dispositivo.

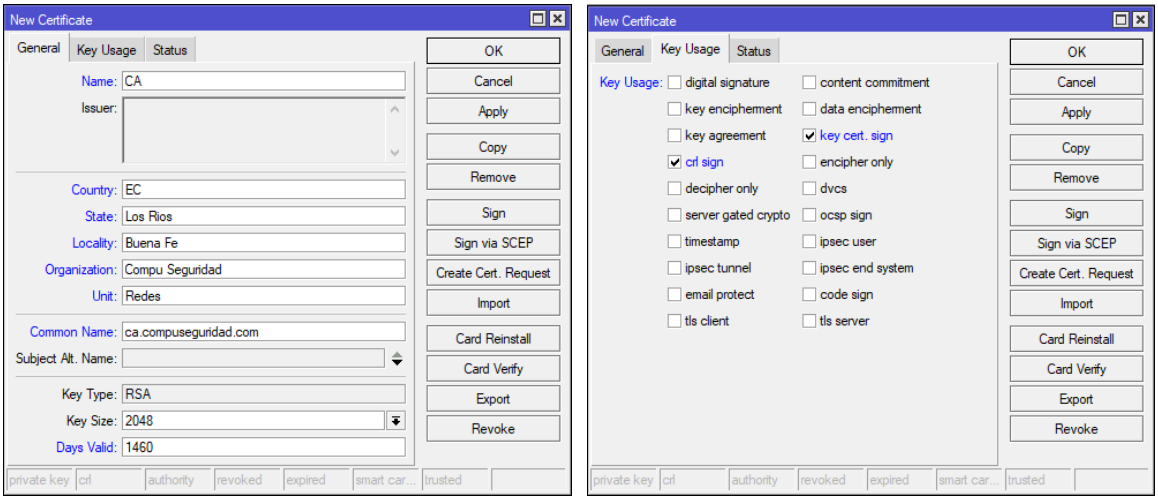


Para crear el certificado de autorización CA, creamos uno nuevo en la herramienta Certificates de RouterOS, llenamos los datos generales del certificado, como nombre, país, provincia, ciudad, organización, unidad, nombre común, tamaño de la llave y días de validez del certificado, como podemos observar en la Figura 45a. Lo más importante al momento de crear un CA, son las llaves que utiliza, para ello nos dirigimos a la pestaña de Key Usage y

seleccionamos las llaves “key cert. sign” y “crl sign”, las cuales nos permitirán señalar al certificado como una autoridad certificadora, con la capacidad de poder firmar otros certificados, ver Figura 45b. Finalmente, procedemos a firmar el certificado para el mismo, dando click derecho sobre él y seleccionando Sign, de esta forma se convertirá en un certificado de confianza.

Figura 45

Creación del CA. a) datos generales y b) llaves usadas.



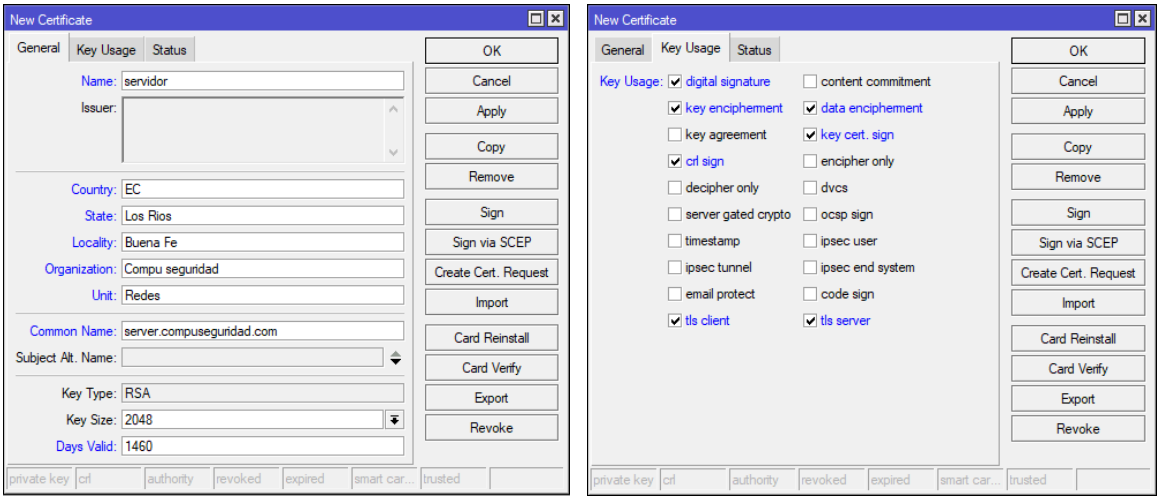
a) b)

Para crear el certificado del servidor RADIUS, de igual forma que en la creación del CA primero creamos un nuevo certificado con la herramienta Certificates de RouterOS, en la primera pestaña llenamos los datos generales y en la segunda pestaña de Key Usage, seleccionamos las opciones de digital signatura, key encipherment, data encipherment, key cert. sign, crl sign, tls client y tls server, tal cual como nos muestra la Figura 46b.

Finalmente, debemos firmar el certificado del servidor con la CA creada anteriormente y luego procedemos a convertir el certificado del servidor en un certificado de confianza, para ello debemos abrir el CLI de RouterOS y escribir “certificate”, seguido de “set [find name=certificado] trusted=yes”.

Figura 46

Creación del certificado para el servidor, a) datos generales y b) llaves usadas.



a) b)

RADIUS con EAP-TTLS

Para configurar el Hotspot con el diseño de la red inalámbrica desarrollado en la Figura 25. Primero abrimos la configuración de Hotspot, nos dirigimos a la viñeta Server Profiles, abrimos el perfil default, dándole doble click. Se nos abrirá la configuración del perfil del servidor Hotspot, aquí debemos seleccionar la opción de HTTPS y procedemos a seleccionamos el certificado SSL que creamos para el servidor, como muestra en la Figura 47.

Además, podemos habilitar la opción de Trial, la cual activará en el Portal Cautivo la opción de poder acceder a la red de forma gratuita por 30 minutos al día, tomar en cuenta que se debe seleccionar un perfil de usuario para este modo Trial, el cual deberá limitar la tasa de transmisión de datos para que los usuarios gratuitos no ocupen toda la capacidad de la red.

Finalmente, para habilitar User Manager con Hotspot debemos dar click en la pestaña RADIUS, habilitar el uso de RADIUS y escribir en Default Domain la dirección IP de Loopback, ya que el servidor RADIUS está en la misma interface inalámbrica del dispositivo de MikroTik, ver Figura 48.

Figura 47

Configuración del hotspot para autenticación EAP-TTLS.

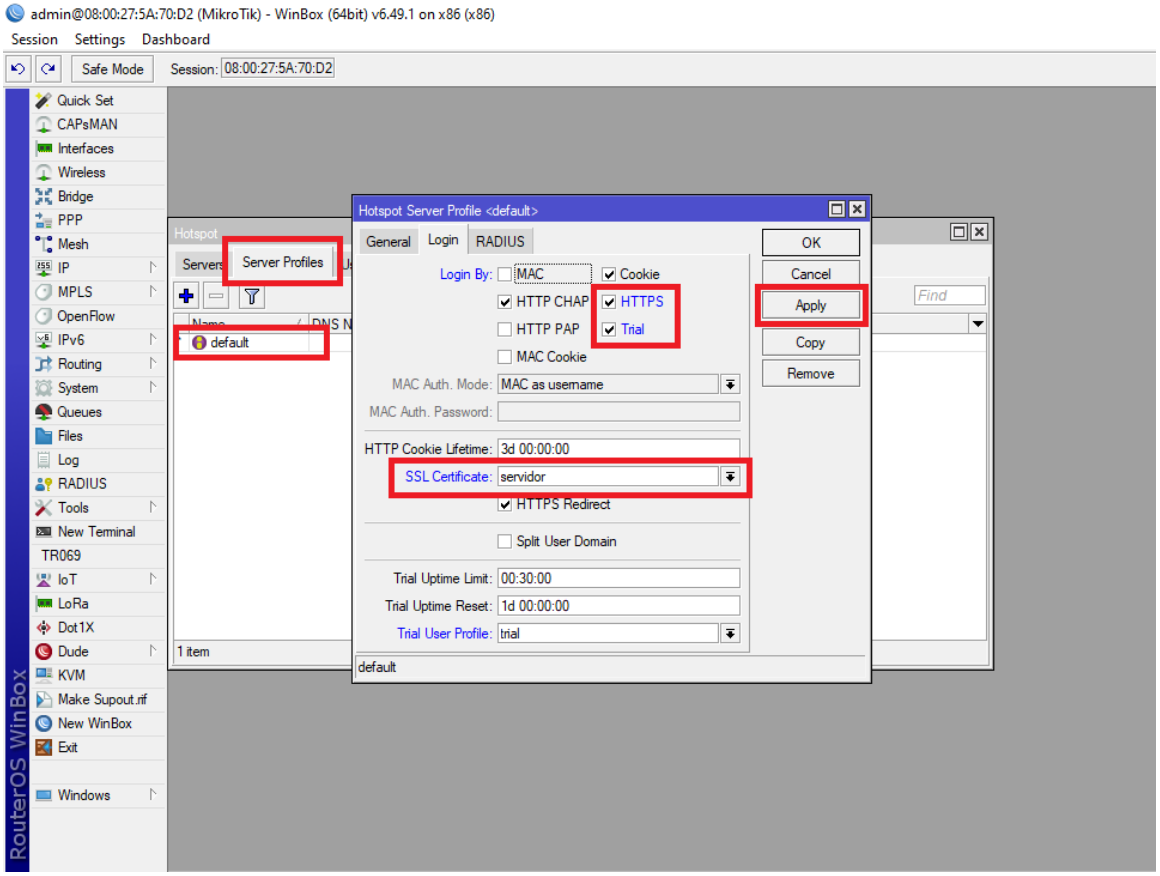
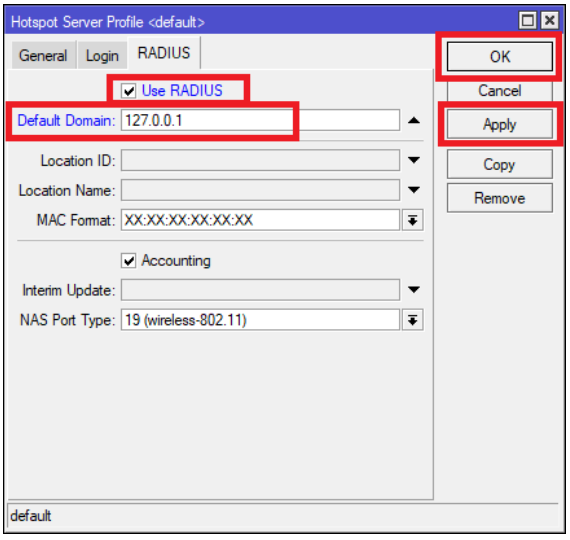


Figura 48

Configuración del hotspot para autenticación EAP-TTLS.



Una vez aplicado los cambios del perfil del servidor hotspot ya tendremos funcionando nuestro Portal Cautivo con autenticación EAP-TTLS y con el protocolo RADIUS con la ayuda del User Manager como sistema AAA para autenticar, autorizar y contabilizar a los usuarios que ingresen a la red inalámbrica de la empresa Compu Seguridad.

Capítulo IV

Análisis de resultados

Puesta en marcha el sistema de red inalámbrico con portal cautivo y autenticación EAP-TTLS de la empresa Compu Seguridad es necesario realizar un análisis y verificación de los resultados obtenidos en la implementación para comprobar si la red cumple con el diseño y las políticas de seguridad establecidas.

Análisis del proceso de autenticación EAP-TTLS

Para realizar el análisis y verificación del proceso de autenticación EAP-TTLS, es necesaria la utilización de la herramienta Wireshark. Wireshark es un analizador de paquetes de red, se podría pensar en un analizador de paquetes de red como un dispositivo de medición que se usa para examinar lo que sucede dentro de una conexión de red, pero en un nivel más alto (Chappell, 2010).

El proceso a seguir es establecer una conexión segura para que exista intercambios de paquetes entre el suplicante, el autenticador y el servidor de autenticación, y de esta forma capturarlos con Wireshark desde el suplicante.

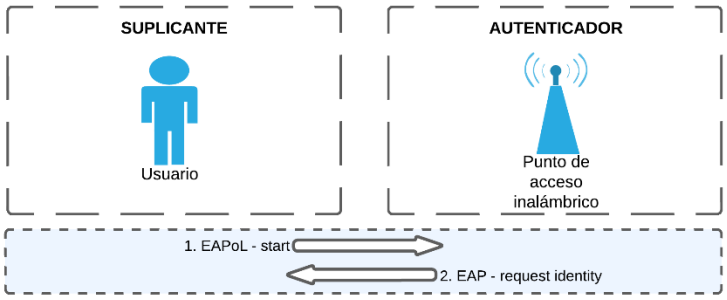
Como observamos en la Figura 25, la comunicación que se entabla entre el suplicante y el autenticador es a través del protocolo EAPoL, la cual encapsula los paquetes EAP y esta a su vez es encapsulada en paquetes RADIUS desde el autenticador para transmitirlos al servidor de autenticación o servidor RADIUS. Cuando la autenticación de EAP-TTLS es exitosa, los paquetes transmitidos a través del suplicante, autenticador y servidor de autenticación son extensos, por esta razón se analizarán las fases de comunicación para facilitar su comprensión.

Fase 1. Solicitud de acceso

En esta primera fase se analiza el intercambio de paquetes que existe entre el suplicante y el autenticador, durante la solicitud de acceso. Podemos visualizar la transmisión de paquetes en la Figura 49.

Figura 49

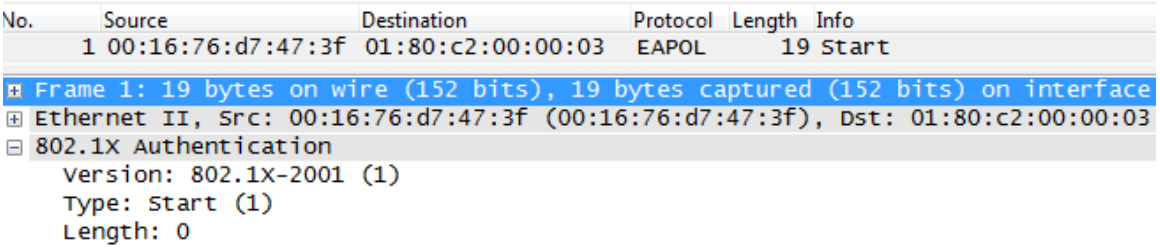
Solicitud de acceso en la autenticación EAP-TTLS.



- El proceso de conexión es iniciado por el suplicante, el cual envía un paquete EAPoL – start, para solicitar acceso a la red, ver Figura 50.

Figura 50

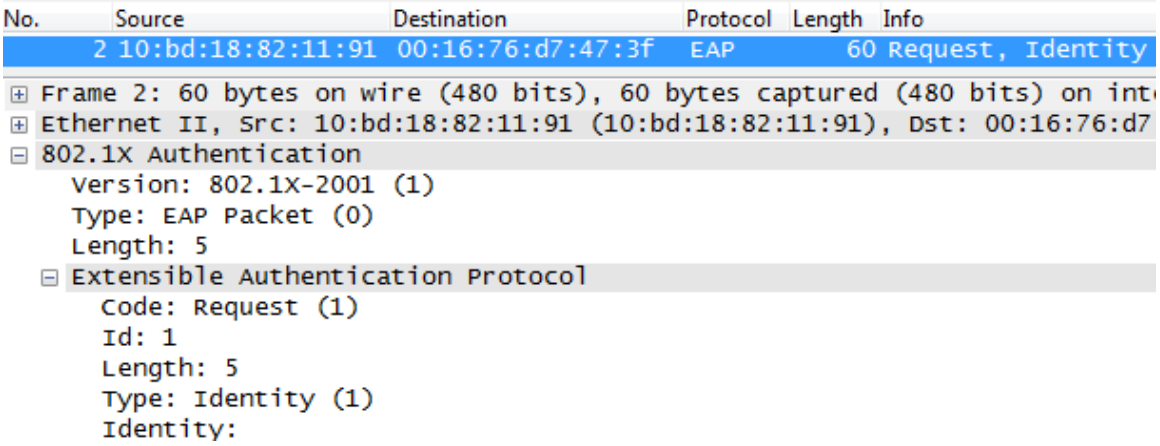
Paquete EAPoL – start.



- El autenticador responde con un paquete EAP – request identity, el cual le indica al suplicante que dispone del servicio y que le envíe sus credenciales, ver Figura 51.

Figura 51

Paquete EAP – request identity.

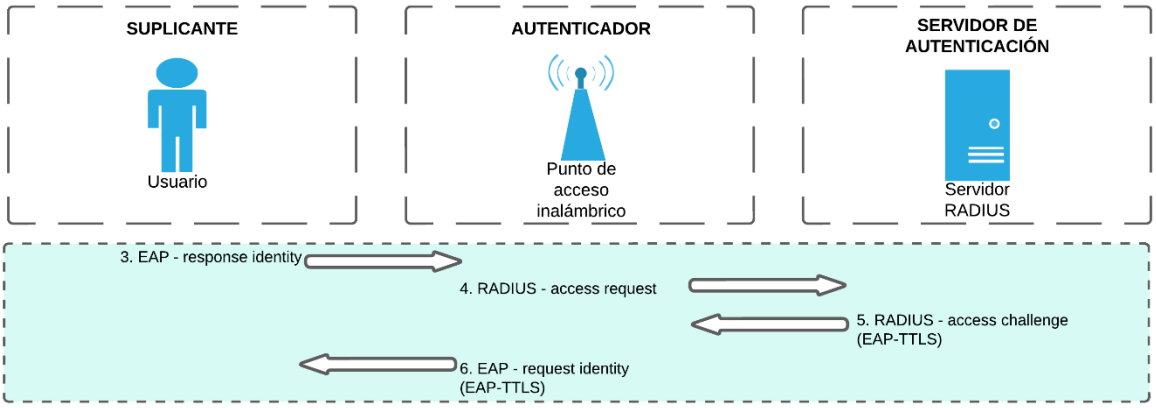


Fase 2. Inicio EAP-TTLS

Durante la fase 2, existe el envío de paquetes entre el suplicante y el autenticador, el autenticador y el servidor de autenticación y viceversa, como podemos observar en la Figura 52. En esta fase entre el autenticador y el servidor de autenticación definen el método a emplearse para autenticarse el usuario, en este caso es el EAP-TTLS.

Figura 52

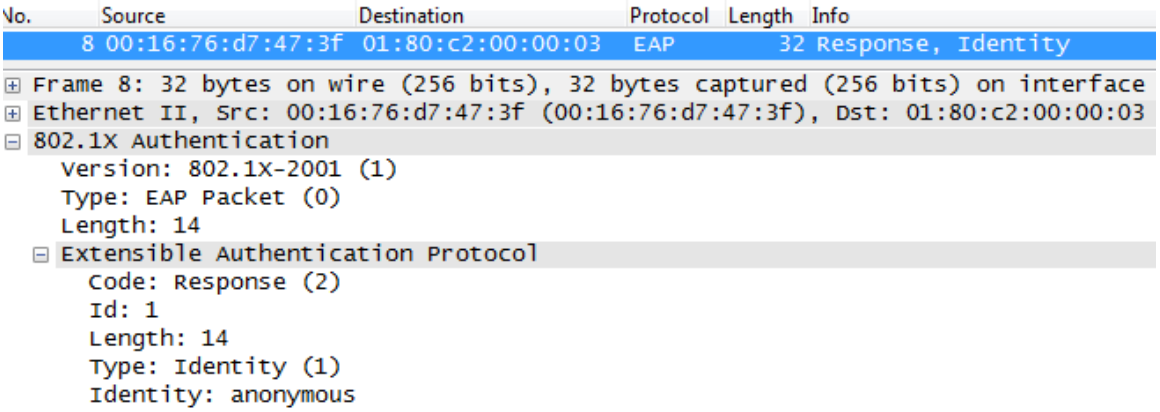
Inicio de la autenticación EAP-TTLS.



- Primero el suplicante envía el paquete EAP – response identity, que contiene una identidad anónima para proteger sus verdaderas credenciales ante cualquier intento de robo de usuarios y contraseñas, ver Figura 53.

Figura 53

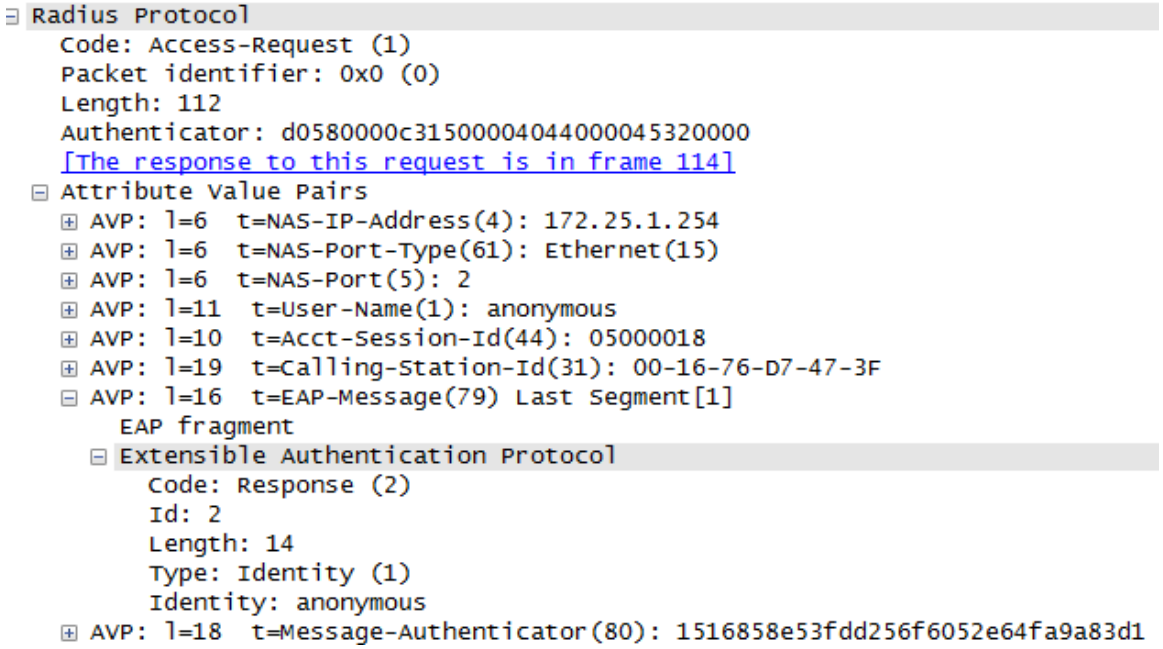
Paquete EAP – response identity.



- El autenticador recibe y encapsula el paquete recibido desde el suplicante con la identidad anónima en un paquete RADIUS – access-request y lo reenvía al servidor. Además, este nuevo paquete incluye información de dirección IP, NAS, puerto y credenciales del autenticador. En la Figura 54 observamos la captura del paquete realizada con Wireshark.

Figura 54

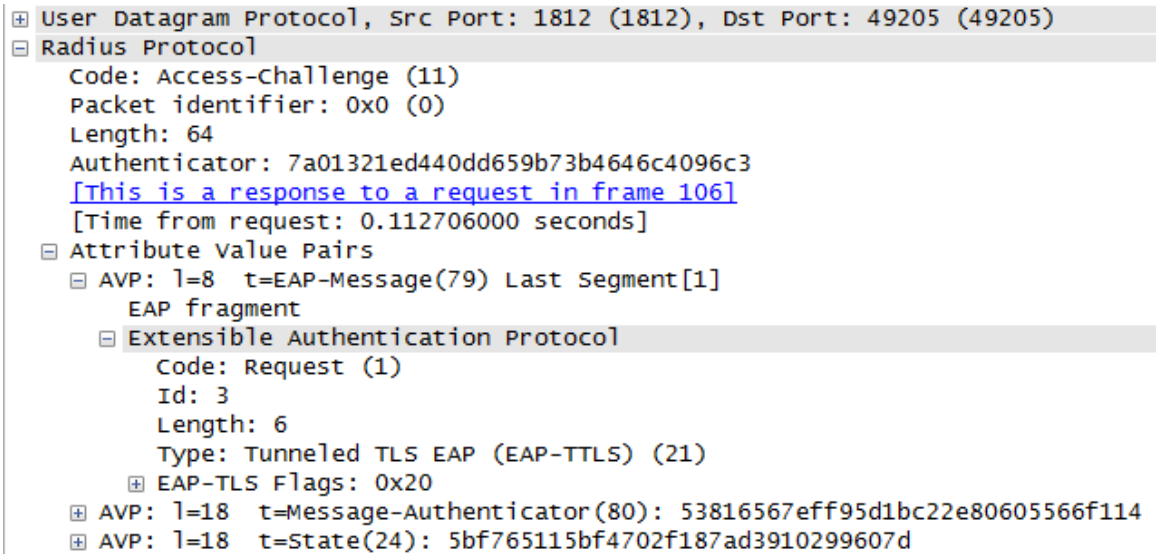
Paquete RADIUS – access-request.



- El servidor de autenticación recibe la información por proporcionada por el autenticador. Luego procede a verificar si la credencial recibida es válida, de serlo este envía un paquete RADIUS – access-challenge al autenticador, para indicarle al suplicante que da inicio el proceso de inicio de sesión y se establece un túnel cifrado TLS EAP con autenticación EAP-TTLS, ver Figura 55.

Figura 55

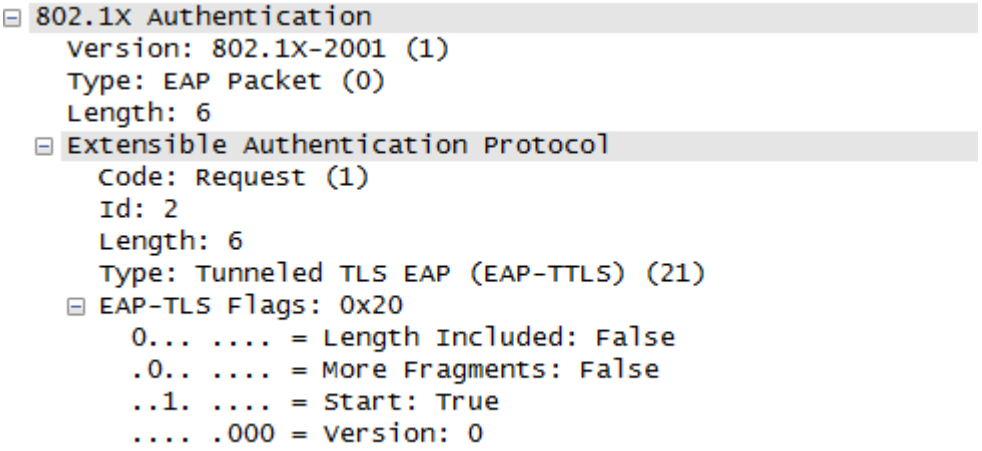
Paquete RADIUS – access-challenge (EAP-TTLS).



- El autenticador encapsula en un paquete EAP y retransmite la información brindada por el servidor de autenticación hacia el suplicante, en un paquete EAP – request, ver Figura 56.

Figura 56

Paquete EAP – request.

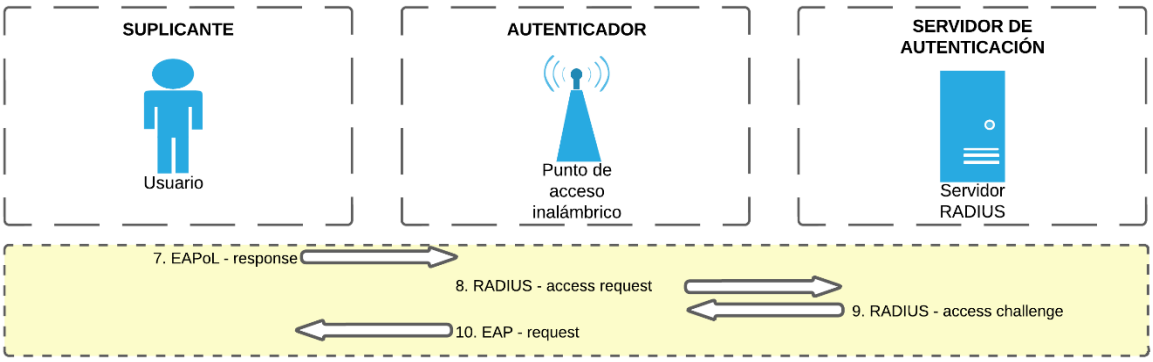


Fase 3. Inicio del protocolo Handshake

Para la fase 3, tenemos el inicio del protocolo Handshake, por lo que, entre el suplicante, autenticador y servidor de autenticación se estable un canal seguro TLS, de esta forma se tiene un intercambio de información seguro, ver Figura 57.

Figura 57

Inicio del protocolo Handshake en la autenticación EAP-TTLS.



- El suplicante da inicio al intercambio de paquetes con un EAP – response, el cual contiene el mensaje Client Hello, ver Figura 58.

Figura 58

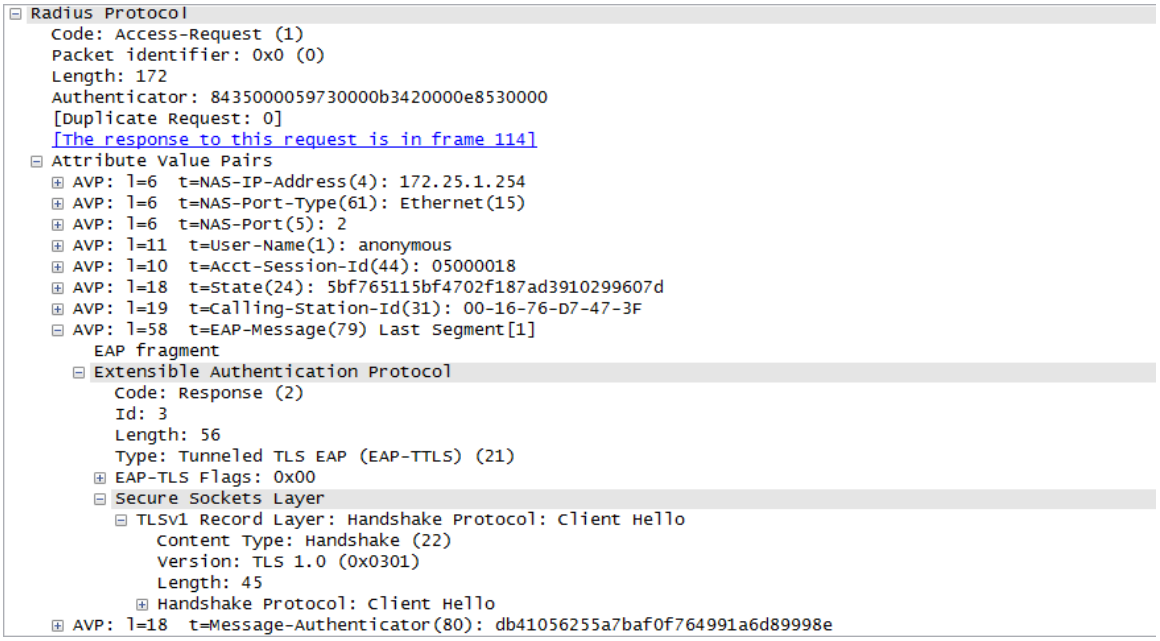
Paquete EAP – response (Client Hello).

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 56
  Extensible Authentication Protocol
      Code: Response (2)
      Id: 2
      Length: 56
      Type: Tunneled TLS EAP (EAP-TTLS) (21)
    EAP-TLS Flags: 0x00
    Secure Sockets Layer
      TLSv1 Record Layer: Handshake Protocol: Client Hello
          Content Type: Handshake (22)
          Version: TLS 1.0 (0x0301)
          Length: 45
        Handshake Protocol: Client Hello
```

- El autenticador encapsula el mensaje con el protocolo RADIUS – access-request y lo renvía al servidor de autenticación, ver Figura 59.

Figura 59

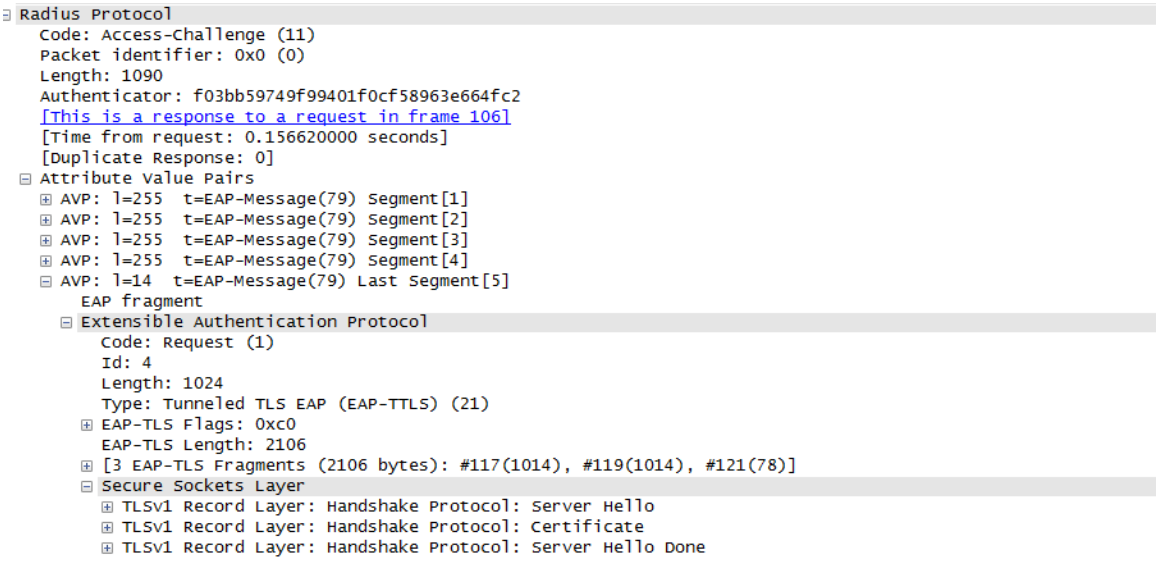
Paquete RADIUS – access-request (Client Hello).



- El servidor de autenticación responde el mensaje con un paquete RADIUS – access-challenge, que contiene un EAP – request, con el mensaje Server Hello, el certificado de servidor y el mensaje Server Hello Done, ver Figura 60.

Figura 60

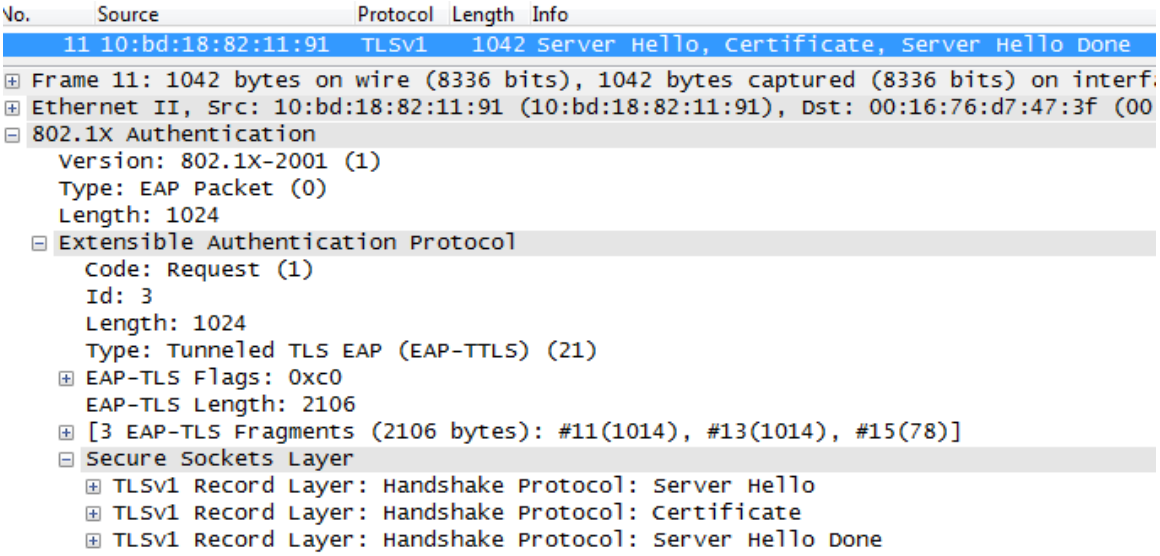
Paquete RADIUS – access-challenge (Certificate, Server Hello Done).



- El autenticador capta el paquete del servidor que incluye el mensaje Server Hello, el certificado digital del servidor y el mensaje Server Hello Done, para transmitirlo al suplicante en un paquete EAP – request, ver Figura 61.

Figura 61

Paquete EAP – request (Certificate, Server Hello Done).

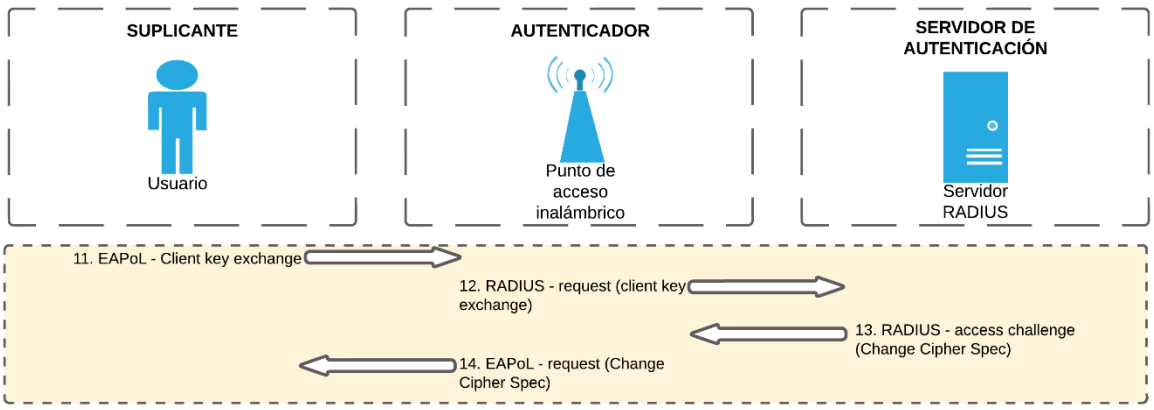


Fase 4. Fin del protocolo Handshake

Durante la fase 4, se crea un túnel encriptado TLS para la transmisión de credenciales en el inicio de sesión del suplicante hacia el autenticador.

Figura 62

Fin del protocolo Handshake en la autenticación EAP-TTLS.



- El suplicante al recibir el mensaje Server Hello Done, este verifica la validez del certificado del servidor con la lista de CA de confianza instaladas en el dispositivo. Comprobado el certificado, el suplicante envía el mensaje Client Key Exchange en conjunto con Change Cipher Spec con la encapsulación EAP – response, a través del túnel cifrado EAP-TTLS hacia el autenticador, como podemos observar en la Figura 63.

Figura 63

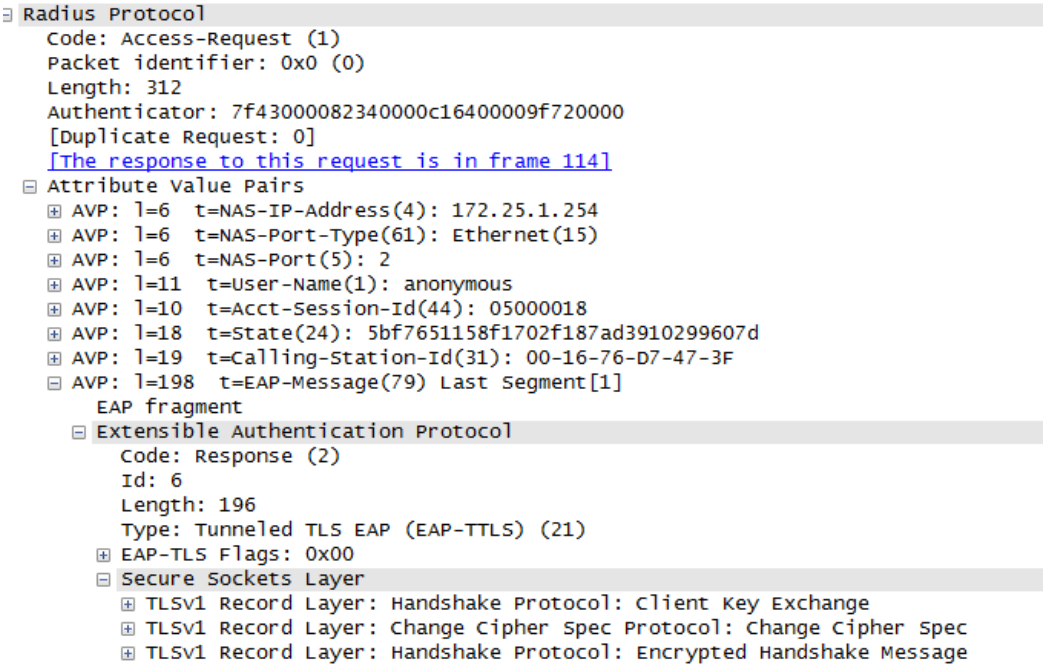
Paquete EAP – response (Client Key Exchange).

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 196
  Extensible Authentication Protocol
      Code: Response (2)
      Id: 5
      Length: 196
      Type: Tunneled TLS EAP (EAP-TTLS) (21)
    EAP-TLS Flags: 0x00
    Secure Sockets Layer
      TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
      TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
          Content Type: Change Cipher Spec (20)
          Version: TLS 1.0 (0x0301)
          Length: 1
          Change Cipher Spec Message
      TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
          Content Type: Handshake (22)
          Version: TLS 1.0 (0x0301)
          Length: 40
          Handshake Protocol: Encrypted Handshake Message
```

- El autenticador actúa como intermediario, por lo que recibe y encapsula el mensaje Client Key Exchange en un RADIUS – access-request, y lo envía a través del túnel cifrado EAP-TTLS hacia el servidor de autenticación, como podemos observar en la Figura 64.

Figura 64

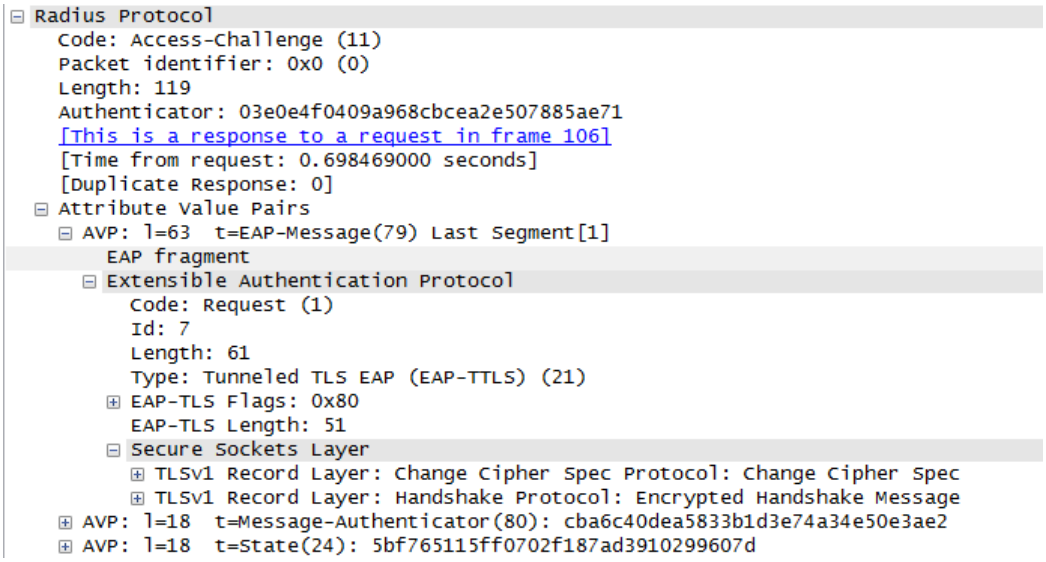
Paquete RADIUS – access-request (Client Key Exchange).



- El servidor de autenticación por medio de la encapsulación RADIUS – access-challenge, responde al autenticador con el mensaje Change Cipher Spec, ver Figura 65, el cual indica la finalización del túnel cifrado.

Figura 65

Paquete RADIUS – access-challenge (Change Cipher Spec).



- El autenticador continúa reenviando los paquetes del servidor de autenticación hasta el suplicando, para ello encapsula el mensaje Change Cipher Spec en un EAP – request, ver Figura 66.

Figura 66

Paquete EAP – request (Change Cipher Spec).

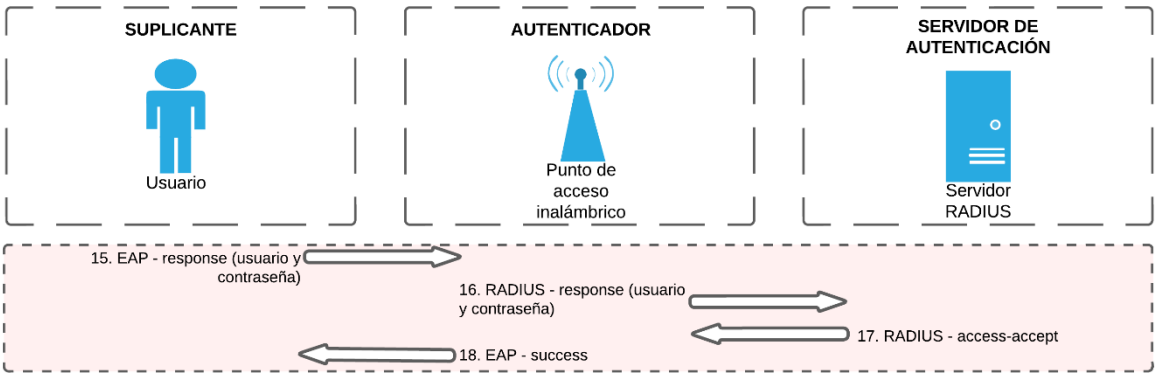
```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 61
  Extensible Authentication Protocol
      Code: Request (1)
      Id: 6
      Length: 61
      Type: Tunneled TLS EAP (EAP-TTLS) (21)
    EAP-TLS Flags: 0x80
      EAP-TLS Length: 51
    Secure Sockets Layer
      TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
```

Fase 5. Transmisión de credenciales

Finalmente, en la fase 5 se realiza la transmisión de credenciales a través de un túnel encriptado EAP-TTLS, desde el suplicante, pasando por el autenticador para llegar hasta el servidor de autenticación. En la Figura 67 podemos visualizar los paquetes que viajan a través de la red.

Figura 67

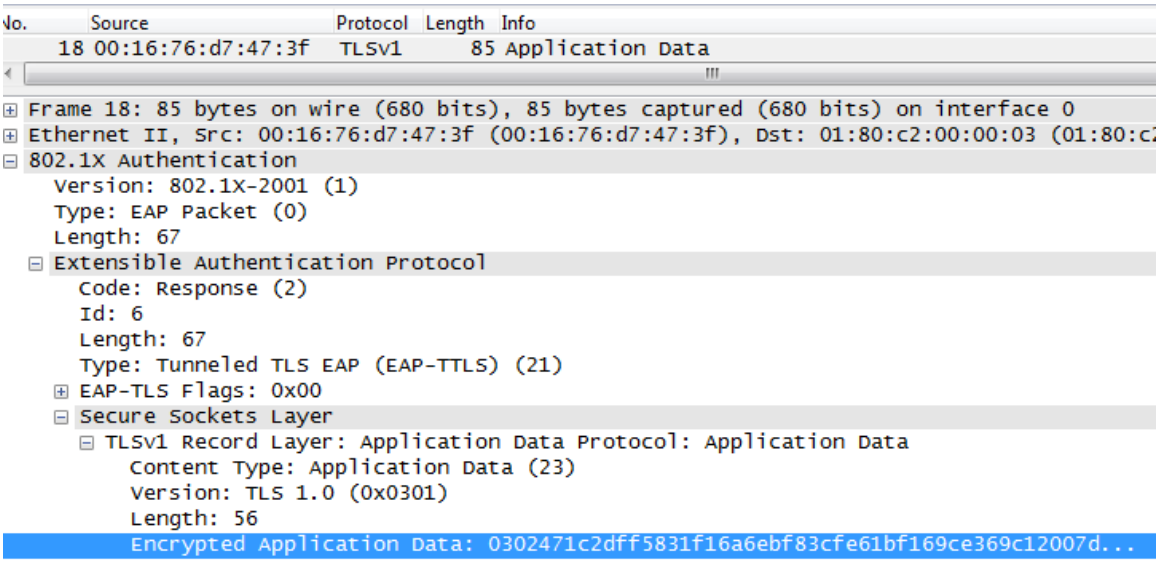
Transmisión de credenciales en la autenticación EAP-TTLS.



- El suplicante al recibir el mensaje de Change Cipher Spec, encapsula el usuario y contraseña en un EAP – response y se los envía al autenticador, ver Figura 68.

Figura 68

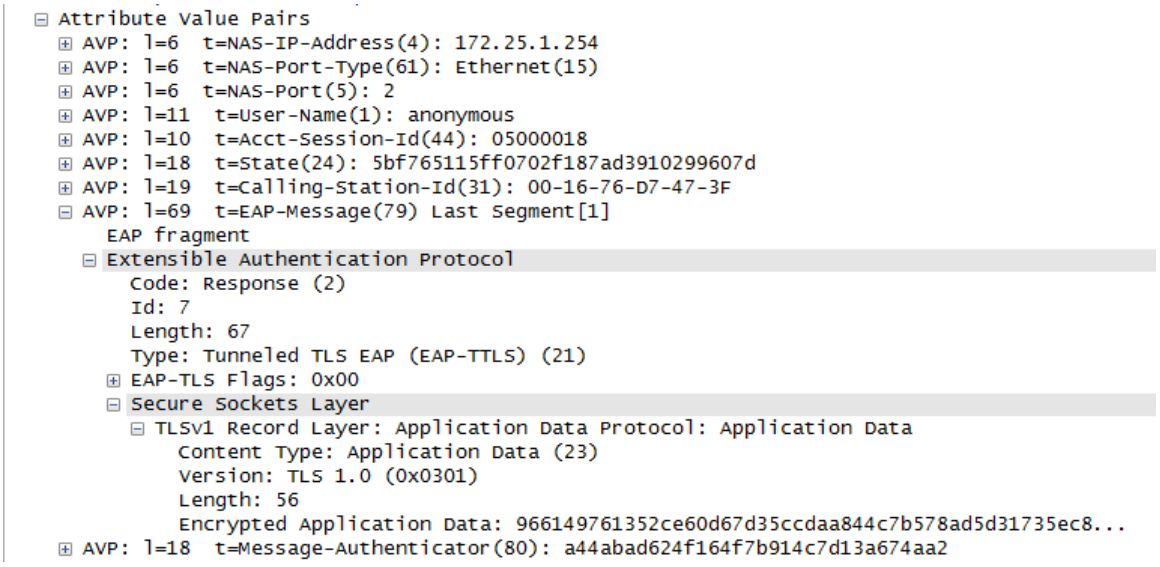
Paquete EAP – response (usuario y contraseña).



- El autenticador, igual que en fases anteriores reenvía las credenciales encriptadas al servidor de autenticación, ver Figura 69.

Figura 69

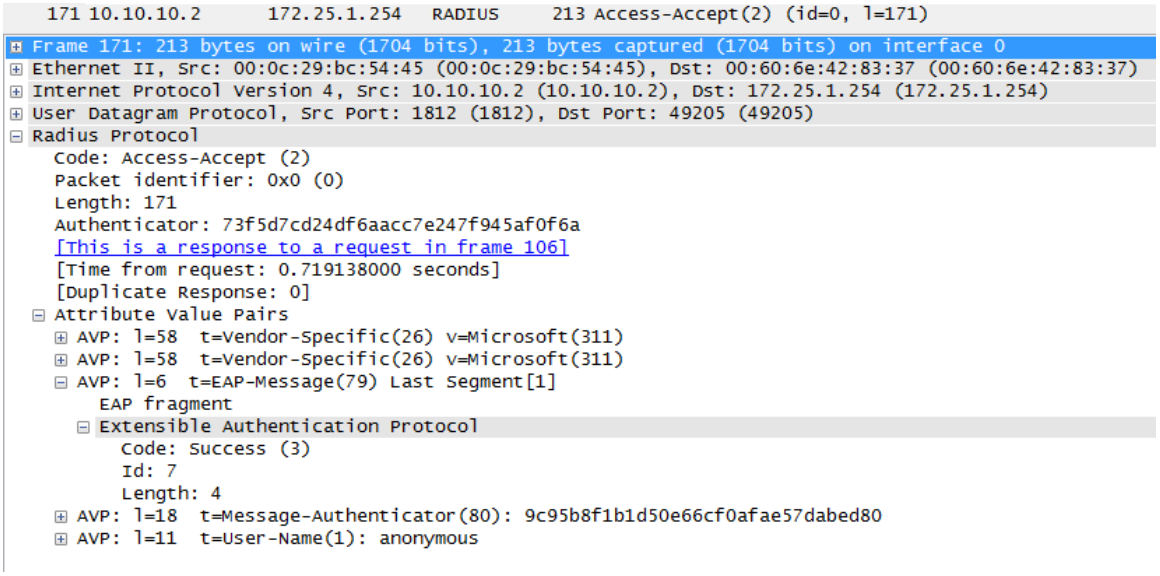
Paquete RADIUS – access request (usuario y contraseña).



- Una vez el servidor de autenticación verifica las credenciales en el User Manager y confirma que son válidas, este envía el último paquete RADIUS – access-accept al autenticador para que permita el acceso a la red, ver Figura 70.

Figura 70

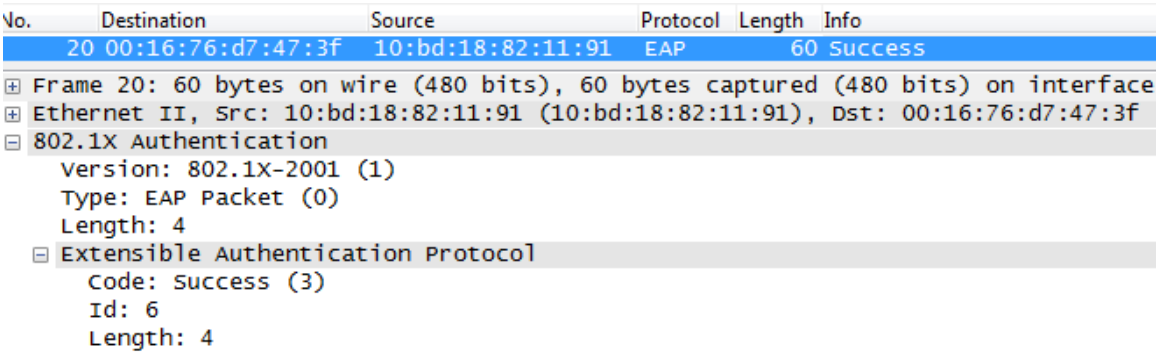
Paquete RADIUS – access-accept.



- Por último, el autenticador encapsula un mensaje EAP – success y se lo envía al suplicante para informarle que la autenticación ha sido exitosa y que habilitó el puerto de acceso a la red, ver Figura 71.

Figura 71

Paquete EAP - success.



Análisis de resultados de la implementación del sistema

Las pruebas realizadas para evaluar el desempeño del mecanismo de autenticación EAP-TTLS bajo el estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el protocolo de RADIUS y del sistema AAA, para brindar los servicios de red inalámbrica en la empresa Compu Seguridad, se realizaron empleando los sistemas operativos con los que cuenta actualmente la empresa que son Windows 10, Android e iOS. Adicionalmente, para comprobar el correcto funcionamiento de la autenticación EAP-TTLS en conjunto con el portal cautivo y el servidor RADIUS se utilizó Wireshark para la captura y análisis de paquetes de red.

La utilización del dispositivo MikroTik RouterBOARD RB951Ui-2HnD como servidor de autenticación o servidor RADIUS, fue la principal elección sobre otros sistemas de licencia gratuita como FreeRADIUS, debido a que la empresa Compu Seguridad ya contaba con este dispositivo y no le daban un uso especifico en la red. Además, hay que tomar en cuenta que si se utilizaba FreeRADIUS se necesitaba conectar un ordenador extra a la red, lo que conlleva mayor utilización de recursos.

MikroTik, a comparación de otras herramientas de software para simular RADIUS, presenta una interfaz gráfica fácil de entender por cualquier administrador de red. Además, para las personas que les gusta programar también se puede configurar a través de interfaz de línea de comandos (CLI, command-line interface).

Capítulo V

Conclusiones y recomendaciones

Conclusiones

El estudio del desempeño de los sistemas de autenticación EAP (Extensible Authentication Protocol) del estándar de seguridad IEEE 802.1X de este trabajo de investigación, ha permitido identificar una serie de criterios que se pueden usar para comparar diferentes métodos EAP. Estos criterios fueron identificados con la ayuda de la norma RFC 4017 EAP Method Requirements for Wireless LANs desarrollada por la IETF (Internet Engineering Task Force). Y así tuvo lugar el desarrollo de un análisis comparativo de los métodos EAP en función de la seguridad, resistencia a ataques informáticos, ocultación de identidad en la red, reconexión rápida, costos computacionales, entre otros criterios.

Analizando la situación inicial de la infraestructura inalámbrica en la empresa Compu Seguridad, se determinó un alto nivel de vulnerabilidad, teniendo como seguridad inalámbrica una configuración de LAN de hogar. Para un ISP (Internet Service Provider), estas vulnerabilidades son blanco perfecto para ataques cibernéticos, los cuales pueden acarrear varias pérdidas de datos y económicas.

Mediante el estado del arte de este trabajo de investigación se logró determinar las políticas de seguridad más relevantes para un ISP. Con la implementación del estándar de seguridad 802.1X y el sistema AAA en una WLAN, se puede mejorar el nivel de autenticación, tener un control sobre los usuarios que acceden a la red y crear políticas de seguridad que restrinjan el uso de la infraestructura inalámbrica. Con la finalidad de controlar la información que viaja por la red interna de la empresa Compu Seguridad.

Para la empresa Compu Seguridad se determinó que el método más adecuado de autenticación es el EAP-TTLS. Este mecanismo de autenticación es compatible con todos los dispositivos y la infraestructura interna de red inalámbrica. Este método EAP crea un canal

seguro entre los suplicantes y el servidor RADIUS mediante certificados digitales, los cuales garantizan que los datos brindados en el proceso de autenticación se mantengan cifrados.

Se diseño e implementó en la empresa Compu Seguridad un sistema de autenticación EAP-TTLS, mediante el estándar de seguridad IEEE 802.1X para la integración de un portal cautivo bajo el sistema AAA y así brindar los servicios de red. La infraestructura de red inalámbrica de la empresa fue reutilizada y configurada para mejorar los protocolos de seguridad de la red.

El servidor de autenticación o servidor RADIUS que se utilizó en la empresa Compu Seguridad fue a través del dispositivo MikroTik RouterBOARD RB951Ui-2HnD, el cual mediante la herramienta User Manager (UM) se aplicó los criterios de un sistema AAA que son autenticar, autorizar y contabilizar a los usuarios que se conectan a la red interna de la empresa.

Se definieron los permisos de usuario dependiendo del nivel dentro de la empresa y del uso que le dará a la red. Así fue como se limitó el uso de tiempo, de tasa de transmisión, de dispositivos que pueda conectar a la red y de expiración de credenciales.

Se realizó el portal cautivo a partir de la plantilla que entrega el dispositivo MikroTik RouterBOARD RB951Ui-2HnD, agregando información de importancia para la empresa y haciendo anuncios de los servicios que brinda esta. Asimismo, se utilizó la plantilla de vouchers del dispositivo de MikroTik para generar boletos con credenciales para poder ingresar a la red.

Finalmente, se evaluó el diseño y se analizó el correcto funcionamiento de la red inalámbrica con autenticación EAP-TTLS bajo el protocolo IEEE 802.1X, con la incorporación de un portal cautivo. Se utilizó herramienta Wireshark para capturar los paquetes que viajan entre el suplicante, autenticador y servidor de autenticación, y compararlos con la literatura del protocolo RADIUS. Obteniendo como resultado al sistema de red funcionando perfectamente.

Recomendaciones

Se recomienda realizar una capacitación a los técnicos de redes de la empresa Compu Seguridad, en los temas de Cyber Ops, protocolos de redes inalámbricas y fundamentos de RouterOS.

Se recomienda realizar verificaciones periódicas de los dispositivos que se conectan a la red inalámbrica, para determinar anomalías que se pueden presentar en el sistema.

Se recomienda tener el software de los diferentes dispositivos actualizados, con la finalidad de poder parchar vulnerabilidades que se pueden presentar.

Si se va a aumentar la infraestructura de la red inalámbrica se recomienda analizar el datasheet de los dispositivos que se desean adquirir, para comprobar que sean compatibles con el sistema implementado.

Tener en cuenta el tiempo de validez de los certificados digitales, ya que, si se pasa el tiempo de vida útil, se vuelven obsoletas y podrían corromper al sistema.

Se recomienda socializar el nuevo sistema implementado en la empresa con todos los trabajadores de la misma. Así mismo realizar una campaña para los clientes, que estos conozcan las nuevas características inalámbricas en las oficinas.

Trabajos futuros

Durante el desarrollo de este proyecto de titulación surgieron varias vías de investigación. Tal como desarrollar un sistema de autenticación EAP basado en contraseñas seguras.

Evaluar el desempeño de servidores de autenticación gratuitos y con licencia, mediante la aplicación de un sistema AAA para una red inalámbrica.

Referencias

Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., & Levkowetz, H. (2004). *Extensible Authentication Protocol (EAP).* Internet Engineering Task Force. doi:10.17487/RFC3748

Abo-Soliman, M. A., & Azer, M. A. (2018). Tunnel-Based EAP Effective Security Attacks WPA2 Enterprise Evaluation and Proposed Amendments. *Tenth International Conference on Ubiquitous and Future Networks, 1*(1), 268-273. doi:10.1109/ICUFN.2018.8437043

Ali, K., & Al-Khlifa, A. (2011). A Comparative Study of Authentication Methods for Wi-Fi Networks. *Third International Conference on Computational Intelligence, Communication Systems and Networks*, 190-194. doi:10.1109/CICSyN.2011.49

Baek, K.-H., Smith, S., & Kotz, D. (2013). A Survey of WPA and 802.11i RSN Authentication Protocols. *Dartmouth Computer Science*, 1-25.

Bahn, C., & Stanley, D. (2020). *IEEE 802.11-2020 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* IEEE Standars Association. Obtenido de IEEE 802.11-2020 - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: https://standards.ieee.org/ieee/802.11/7028/

Brown, E. L. (2008). *802.1X Port-Based Authentication.* Boca Ratón: Auerbach Publications.

Carballar, J. A. (2010). WI-FI. Lo que se necesita conocer. Madrid: RC Libros.

Cepeda, C., & Proaño, P. (2007). *Diseño e implementación de un cliente radius en linux.* Quito: Escuela Politécnica Nacional. Obtenido de https://bibdigital.epn.edu.ec/handle/15000/550

Chappell, L. (2010). *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide.* San Jose: Protocol Analysis Institute, Inc.

Chen, J.-C., & Wang, Y.-P. (2005). Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience. *IEEE Communications Magazine, 43*(12), 26-32. doi:10.1109/MCOM.2005.1561920

Dantu, R., Clothier, G., & Atri, A. (2007). EAP methods for wireless networks. *Computer Standards & Interfaces, 29*(3), 289-301. doi:10.1016/j.csi.2006.04.001

Freeman, A. (2011). *The Definitive Guide to HTML5.* New York: Apress. doi:10.1007/978-1-4302-3961-1

Garg, V. (2010). *Wireless Communications & Networking.* San Francisco: Elsevier.

Gulasekaran, S. R., & Sankaran, S. G. (2022). *WiFi 6: Protocol and Network.* Norwood: Artech House.

Hari, F., & Amin, M. (2022). Design and Implementation of Hotspot Network Login Authentication Using QR Code Based on Mikrotik. *Jurnal Komputer, Informasi Dan Teknologi, 2*(1), 229-238. doi:10.53697/jkomitek.v2i1.835

Hoy, M. B. (2012). HTML5: A New Standard for the Web. *Medical Reference Services Quarterly, 30*(1), 50-55. doi:10.1080/02763869.2011.540212

Hurtado, G. (2017). *Estudio comparativo entre servidores Mikrotik y Cisco bajo el estándar de seguridad 802.1x para servicios de red en la empresa Guano.Net.* Riobamba: Escuela Superior Politécnica de Chimborazo. Obtenido de http://dspace.espoch.edu.ec/handle/123456789/6851

International Organization for Standardization. (2018). *ISO/IEC/IEEE 29148:2018.* Obtenido de https://www.iso.org/standard/72089.html

Lu, P. J., Yeh, L.-Y., & Huang, J.-L. (2018). An Privacy-preserving Cross-organizational Authentication/Authorization/Accounting System using Blockchain Technology. *IEEE International Conference on Communications (ICC), 1*(1), 1-6. doi:10.1109/icc.2018.8422733

Lubbers, P., Albers, B., & Salim, F. (2011). *Pro HTML5 Programming.* New York: Apress.

Marques, N., Zúquete, A., & Barraca, J. P. (2019). Integration of the Captive Portal paradigm with the 802.1X architecture. *arXiv, 1*(1), 1-28. doi:10.48550/arXiv.1908.09927

Orlando, C., & Parsons, G. (2020). *IEEE 802.1X-2020 Port-Based Network Access Control.* IEEE Standars Association. Obtenido de IEEE 802.1X-2020 - Port-Based Network Access Control: https://standards.ieee.org/ieee/802.1X/7345/

Paredes, M. (2013). *Implementación de un plan piloto de seguridad bajo el protocolo IEEE 802.1x para el departamento de gestión tecnológica del Ministerio de Telecomunicaciones y Sociedad de la Información.* Quito, Universidad de las Fuerzas Armadas ESPE. Obtenido de http://repositorio.espe.edu.ec/handle/21000/7286

Rao, K., Bojkovic, Z. S., & Milovanovic, D. A. (2010). Wireless Networking Standards (WLAN, WPAN, WMAN, WWAN). En *Wireless Multimedia Communications* (págs. 99-166). Boca Raton: CRC Press. doi:10.1201/9781420008227

Rigney, C. (2000). *RADIUS Accounting.* RFC 2866. doi:10.17487/RFC2866

Salazar, J. (2015). *Redes Inalámbrica.* Praha: TechPedia.

Sang, S.-J., & Zhou, J.-W. (2012). Analysis and improvements of PEAP protocol in WLAN. *nternational Symposium on Information Technologies in Medicine and Education*, 918-922. doi:10.1109/ITiME.2012.6291453

Setiawan, J. E. (2018). Wireless Network Security Information System on Banking Company with Radius Server Using Authentication, Authorization, Accounting (AAA). *International Journal of Computer Science and Software Engineering, 7*(11), 255-259.

Sharma, K., & Dhir, N. (2014). A Study of Wireless Networks : WLANs , WPANs , WMANs , and WWANs with Comparison. *International Journal of Computer Science and Information Technologies, 5*(6), 7810-7813. Obtenido de https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.661.5914

Simpson, W. (1996). *PPP Challenge Handshake Authentication Protocol (CHAP).* Internet Engineering Task Force. doi:10.17487/RFC1994

Stanley, D., Walker, J., & Aboba, B. (2005). *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs.* Internet Engineering Task Force. doi:10.17487/RFC4017

Sukhija, S., & Gupta, S. (2014). Wireless Network Security Protocols: A Comparative Study. *International Journal of Emerging Technology and Advanced Engineering, 2*(1), 357-364. Obtenido de https://ijetae.com/files/Volume2Issue1/IJETAE_0112_61.pdf

Tobar, Y., & Mora, G. (2016). *Implementación de un servidor radios en windows server para centralizar la administración de nuevos access points en las oficinas remotas de galpones y huertos del gobierno autónomo descentralizado del Guayas.* Quito: Universidad Politécnica Salesiana. Obtenido de https://dspace.ups.edu.ec/handle/123456789/13235

Vallejos, E. (2019). *Diseño de sistema de seguridad a nivel de capa de enlace de datos en redes cableadas mediante el estándar IEEE 802.1X En La LAN de la Universidad Técnica del Norte.* Ibarra: Universidad Técnica del Norte. Obtenido de http://repositorio.utn.edu.ec/handle/123456789/9106

Wahyudi, E., Luthfi, E., & Efendi, M. (2019). Wireless Penetration Testing Method To Analyze WPA2-PSK System Security And Captive Portal. *Jurnal Explore STMIK Mataram, 9*(1), 1-7. doi:10.35200/explore.v9i1.32

Willens, S., Rubens, A., Simpson, W., & Rigney, C. (2000). *Remote Authentication Dial In User Service (RADIUS).* RFC2865. doi:10.17487/RFC2865

Apéndices