UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"IMPLEMENTACIONES DE SEGURIDAD EN REDES INALÁMBRICAS. CASO PRÁCTICO: RIU"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A:

ALFONSO CELESTINO MARTÍNEZ

DIRECTORA DE TESIS: M.C. MARÍA JAQUELINA LÓPEZ BARRIENTOS

MÉXICO, D.F. **2009**

Agradecimientos

A Dios, porque aceptar su existencia le da sentido real a mi vida, a mis logros, a mis sueños y a cada una de las actividades que hago.

A mi abuelita, qepd, por sus sabios consejos, enseñanzas, pero sobre todo por su vida ejemplar, llena de amor, humildad, lucha, tenacidad, integridad y sacrificio, que han resultado ser determinantes en la formación de mi carácter y en los objetivos alcanzados.

A mis padres, por la oportunidad que me dieron de conocer este mundo, por su protección y por las herramientas necesarias que me proporcionaron para abrirme camino en la vida.

A mis hermanos y hermanas, en especial a Miguel, Bruno e Isidoro que en algún momento su apoyo fue de vital importancia en este largo camino de mi formación escolar.

A mi Angelito del cielo, Guille, gracias por todo el amor que me brindas, eres mi fuente de inspiración y motivación.

A Lidia, mi madre adoptiva, sus consejos, su apoyo incondicional y sus "regaños" fueron fundamentales en mi vida universitaria.

A mis amigos y compañeros de la carrera, Isaías, Leonel y Enrique, que en todo momento conté con su amistad y ayuda, haciendo menos difícil mi vida en la ciudad y en la universidad, y por todos los momentos de alegría y de angustia que pasé con ustedes.

A Paty Chinos, por todas las oportunidades de desarrollo profesional proporcionadas, por su ejemplo de fortaleza y lucha ante las adversidades y por las facilidades brindadas para culminar con mi proceso de titulación.

A mi directora, por su tiempo, profesionalismo y dedicación en la revisión de mi proyecto de tesis.

A mis amistades de la ICM, gracias por su cariño incondicional, por sus enseñanzas, por sus consejos y por sus vidas ejemplares, he aprendido mucho de ustedes.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

INTRODUCCIÓN

Una de las innovaciones en redes de datos que actualmente está teniendo mucho auge, son las tecnologías de redes inalámbricas, principalmente las WLAN (Wireless Local Area Network, 'Redes Inalámbricas de Área Local') que si bien no son importantes por la mejora de ancho de banda como la Fibra Óptica, sí lo son por el medio de transmisión que utilizan, que es el aire, característica que le proporciona una serie de ventajas, sobre las redes cableadas en diversas situaciones, como rapidez de despliegue, costos de instalación, movilidad, entre varias más.

Pero junto a las ventajas que genera la transmisión aérea, las WLAN crean un problema muy grave, el de la seguridad. En este sentido cabe destacar que en una red cableada, existe una seguridad inherente que consiste en el hecho de que un intruso o atacante, para tener acceso a la red, necesariamente requiere de una conexión cableada, es decir, de un acceso físico a la red. A diferencia de las comunicaciones inalámbricas, donde estas barreras físicas no existen.

Las redes inalámbricas usan ondas de radio, cualquier persona dentro del área de cobertura, puede escuchar la comunicación. Se puede aumentar o disminuir el área de cobertura, aumentando o disminuyendo la potencia de transmisión de los APs (Access Points, 'Puntos de acceso'), pero resulta difícil establecer fronteras exactas y es inevitable mantener la señal únicamente en donde se requiera o se tenga control del espacio físico, este hecho hace a las redes inalámbricas vulnerables.

Otra vulnerabilidad surge como consecuencia de las escuchas espías (eavesdropping), para aquellos usuarios que no transmiten información confidencial no ven esto como un problema, sin embargo permitir las escuchas pasivas abre la posibilidad de una gran cantidad de ataques activos.

Desafortunadamente los problemas de seguridad de una WLAN no se limitan únicamente a usuarios inalámbricos, sino que una WLAN es por sí misma un riesgo para toda la infraestructura de red local si no se consideran las medidas de seguridad adecuadas. Un intruso puede acceder a la red local a través de la inalámbrica y causar daños a los sistemas internos o

simplemente contaminar de virus a la red. Las redes inalámbricas vulneran las medidas de protección tradicionales.

Por todo lo anterior resulta importante contar con información que permita establecer sistemas de redes inalámbricos de forma segura, confiable, eficiente; que proporcione los elementos a considerar y los pasos a seguir para su implantación.

Así, el objetivo de este trabajo, además de proporcionar una solución de seguridad específica, busca que se comprendan las amenazas de seguridad, las vulnerabilidades y los riesgos de ataques a la que están expuestas las WLAN; para ello se examinan las medidas de protección que propone el estándar, los objetivos de seguridad y riesgos que busca prevenir; para alcanzar el objetivo final que es la implementación de un conjunto de soluciones, entre las que se incluye la infraestructura de seguridad que permita operar una red inalámbrica robusta, confiable, escalable, funcional y fácil de administrar, específicamente la implementación de seguridad WPA/802.11i en la Red Inalámbrica Universitaria (RIU).

Otro de los aspectos importantes en este proyecto de tesis, es la propuesta del uso de software libre, que incluye el sistema operativo y la integración de todas las aplicaciones necesarias para lograr un sistema funcional.

Para ello, en el capítulo 1 se hace una descripción general de las WLAN basados en el estándar 802.11, sus componentes principales, las diferentes versiones que existen, su relación e integración con las redes tradicionales y las diferentes topologías que se pueden conseguir.

En el capítulo 2 se proporcionan términos básicos de seguridad, las amenazas a las que están expuestas las WLAN, las vulnerabilidades y las medidas para contrarrestar o mitigar los problemas.

En el capítulo 3 se presentan los diferentes protocolos de seguridad que define el estándar 802.11: WEP, que fue la solución original y sus deficiencias; WPA e IEEE 802.11i (WPA2) que buscan resolver los problemas de WEP.

En el capítulo 4 se analizan los tres elementos que juegan un papel importante en las especificaciones de seguridad tanto en WPA como en 802.11i: El estándar de control de accesos basado en puertos (IEEE 802.1X), el protocolo de autenticación EAP y RADIUS.

En el capítulo 5 se muestran los elementos necesarios para la implementación de una infraestructura de seguridad WPA/802.11i con el uso de software libre, también se presentan ejemplos de implementaciones mostrando las configuraciones necesarias para establecer cada uno de los tres mecanismos de autenticación EAP principales para WLAN: EAP-TLS, EAP-PEAP y EAP-TTLS tanto en el servidor de autenticación como en los dispositivo de los usuarios o “suplicantes”.

En el capítulo 6 se presenta un caso práctico. Se muestra la implementación del servidor AAA (Authentication, Authorization and Accounting, ‘Autenticación, Autorización y Contabilidad’) en la Red Inalámbrica Universitaria (RIU); en donde se establece WPA como protocolo de seguridad y EAP-PEAP como mecanismo de autenticación. Se proporciona los detalles de la integración de las diferentes aplicaciones para obtener un sistema funcional basado en software libre.

Finalmente, el presente trabajo muestra las conclusiones a las que se llegan después del estudio y el proyecto realizados.

CAPÍTULO 1

REDES INALÁMBRICAS IEEE 802.11

1. REDES INALÁMBRICAS IEEE 802.11

Para dar inicio con los temas relacionados con las redes WLAN es fundamental conocer los principios generales en los que basan su funcionamiento, familiarizarse con los términos que se manejan, conocer sus componentes físicos, su relación e integración con las redes tradicionales.

Actualmente las redes inalámbricas de área de local están teniendo un gran crecimiento en cuanto a su desarrollo y aceptación. El propósito principal de éstas es dar acceso y conectividad a las tradicionales redes cableadas como Ethernet, Token Ring, por lo que las WLAN más que una sustitución de las LANs convencionales son una extensión de las mismas que permiten el intercambio de información entre los distintos medios en una forma transparente al usuario. Se podría considerar que el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas.

Las redes inalámbricas son una alternativa para hacer llegar una red tradicional a lugares donde el cableado no lo permite. En general las WLAN se utilizan como complemento de las redes fijas.

Existen diferentes tecnologías de WLAN, pero los productos inalámbricos basados en la familia de estándares 802.11 son los que han dominado ampliamente el mercado y son los que se han elegido para su implementación por lo que en lo sucesivo sólo se enfocará el trabajo en este tipo de redes, así, en esta sección se realiza una descripción general de las redes inalámbricas 802.11.

El inicio de consolidación de las redes inalámbricas se presentó en junio de 1997 con la conclusión del estándar IEEE 802.11.

1.1. Relación de las WLAN y las tecnologías de redes LAN tradicionales

IEEE 802 es una serie de especificaciones para el establecimiento de tecnologías de redes de área local y redes de área metropolitanas basadas en el modelo OSI (Open Systems Interconnection, ‘Interconexión de Sistemas Abiertos’). Norma que fue ratificada en 1990.

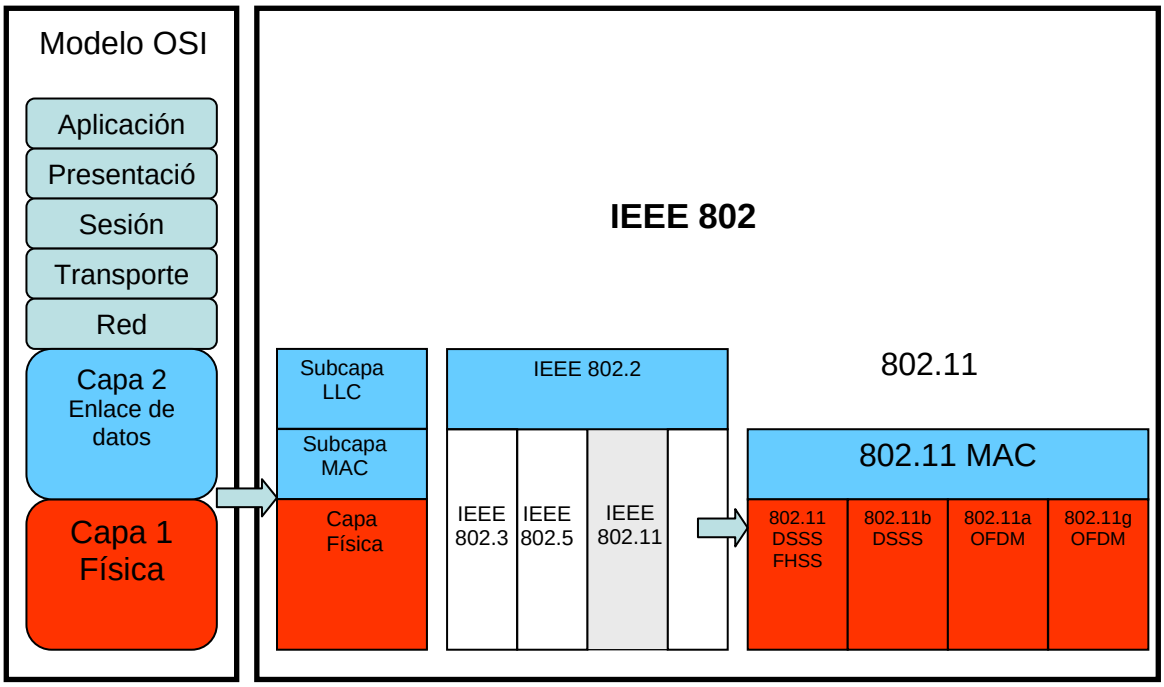

Figura 1.1. Comparación del estándar 802.11 con respecto al modelo OSI

El modelo OSI describe la forma de cómo la información en una computadora es transferida a una aplicación en otro equipo.

El modelo OSI organiza el proceso de comunicación en siete capas independientes (Física, Enlace, Red, Transporte, Sesión, Presentación y Aplicación), como se aprecia en la figura 1.1. La mayoría de las redes públicas y privadas de comunicaciones utilizan el modelo OSI como modelo de referencia.

Las tecnologías de redes LAN **IEEE 802** define únicamente los temas relacionados con las dos primeras capas del modelo OSI:

- **Capa de Enlace.**

  La IEEE 802 divide a la capa de enlace en dos subcapas: la subcapa LLC (Logical Link Control, 'Control de Enlace Lógico') y la subcapa MAC (Medium Access Control, 'Control de Acceso al Medio'). Como se observa en la figura 1.1, la subcapa LLC es definida por el estándar 802.2 y es común a toda la familia de redes 802, **tanto para las redes tradicionales (cableadas) como para las WLAN (802.11)**, el trabajo de esta subcapa es ocultar las

diferencias entre las variantes 802 con la finalidad de que sean imperceptibles para la capa de red, en cambio para el subnivel MAC cambia ya que define las técnicas de acceso, es decir cómo, cada terminal puede hacer uso del medio de comunicación común. Las primeras técnicas de acceso que especificó la IEEE fueron para las redes cableadas, por ejemplo para 802.3 define una tecnología conocida como CSMA/CD (Carrier Sense Multiple Access with Collision Detection, 'Acceso Múltiple por Detección de portadora con Detección de Colisión'), para las redes inalámbricas (802.11) se define una subcapa MAC propia, aunque en concepto es muy similar a la de 802.3, emplea una modificación del protocolo denominada CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*, 'Acceso Múltiple por Detección de Portadora con Evite de Colisión'). La tecnología CD detecta que se ha producido una colisión y retransmite los datos, mientras que la tecnología CA dispone de procedimientos para evitar que se produzcan colisiones.

La razón de que haya dos sistemas es que, cuando el medio es un cable, una terminal puede transmitir y recibir al mismo tiempo, por lo que puede detectar las colisiones. Por el contrario, en el medio radioeléctrico una terminal no puede transmitir y recibir al mismo tiempo por el mismo canal, por lo que, al no poder detectar las posibles colisiones, no hay más remedio que disponer de una técnica que las evite.

- **Capa Física.**

  El objetivo principal de esta capa es transmitir bits por un canal de comunicación, en el caso de las WLAN, el canal de comunicación es el espectro radioeléctrico y la capa física define las técnicas de transmisión y modulación de la señal.

Las características técnicas individuales en la serie 802 son identificadas por un segundo número. Por ejemplo, 802.3 que son las especificaciones que define la tecnología Ethernet y 802.5 definen la tecnología token ring.

1.2. IEEE 802.11

En 1997 la IEEE integró un nuevo miembro a la familia 802: el 802.11, que se ocupa de definir las especificaciones para las redes inalámbricas de área local, WLAN.

Las especificaciones base del estándar 802.11 define una capa MAC y dos capas físicas basadas en el uso de radiofrecuencia en la banda de 2.4 GHz. Ambas se diferencian en el método de transmisión de radio utilizado. Una emplea el sistema FHSS (*Frequency Hopping Spread Spectrum*, 'Difusión por salto de frecuencia') y la otra, el sistema DSSS (*Direct Sequence Spread Spectrum,* 'Difusión por Secuencia Directa'*)*, después surgió la técnica de transmisión OFDM.

Los dos estándares 802.11 originales tenían las desventajas de operar a velocidades muy bajas (1 y 2 Mbps), además los equipos tenían costos muy altos. Posteriormente surgieron nuevas capas físicas que mejoraron la velocidad de transmisión y empezaron a salir los primeros productos aceptados por el mercado.

- **IEEE 802.11b.** Sube la velocidad de transmisión a los 11Mbps. Agrega en capa física la técnica de transmisión HR/DSSS. Por este motivo se la conoció también como 802.11 HR (*High Rate*, 'Alta Velocidad').

- **IEEE 802.11a.** Esta norma se diferencia de 802.11b en el hecho de que no utiliza la banda de 2.4 GHz, sino la de los 5 GHz y que utiliza una técnica de transmisión conocida como OFDM (*Orthogonal Frequency Division Multiplexing*, 'Multiplexación Ortogonal por División de Frecuencia'). La gran ventaja es que se consiguen velocidades de 54 Mbps.

- **IEEE 802.11g.** Esta norma surgió en el año 2001 con la idea de aumentar la velocidad sin renunciar a las ventajas de la banda de los 2.4 GHz. Permite transmitir datos a 54 Mbps.

- **IEEE 802.11n.** En enero de 2004, se anunció la formación de un nuevo grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 600 Mbps. En enero de 2009 se aprobó el borrador 7.0. 802.11n puede trabajar en dos bandas de frecuencias: 2.4 y 5 GHz, por lo que 802.11n es compatible con dispositivos basados en todas las versiones anteriores de 802.11.

1.2.1. Compatibilidad entre 802.11 y Ethernet

La norma IEEE 802.11 se diferencia de la norma 802.3 únicamente de la subcapa MAC y de la capa física. Esto significa que una red inalámbrica y una red cableada son diferentes únicamente en la forma en cómo hosts o terminales acceden a la red; el resto es similar, por lo que una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales cableadas (802.3 o Ethernet).

1.2.2. Componentes de una red Inalámbrica

Los componentes principales de una red inalámbrica son los que se muestran en la figura 1.2 y que se describen a continuación:

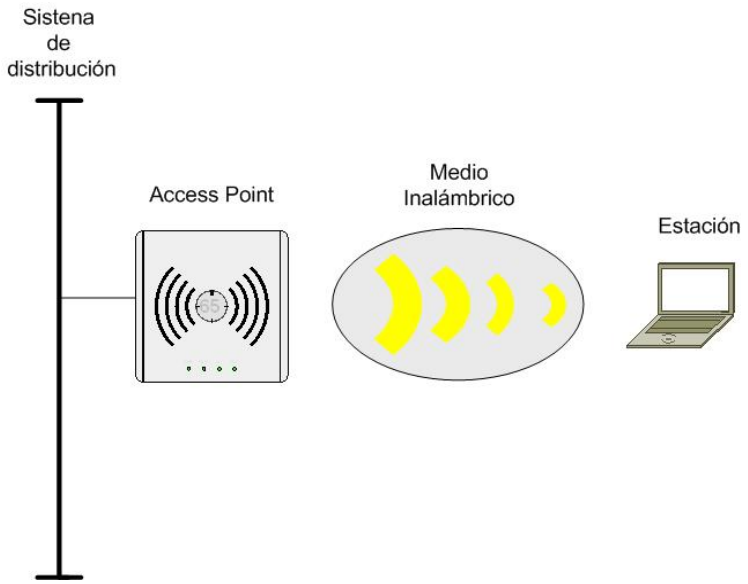

Figura 1.2. Componentes de una WLAN 802.11

1.2.2.1. **Sistema de distribución** (Distribution System, DS)

Cuando se requiere ampliar la cobertura de una red inalámbrica, se hace uso de más de un Access Point (AP). En este caso se requiere que las estaciones asociadas a distintos AP puedan interconectarse de forma transparente. El sistema que permite dicha interconexión es el **Sistema de distribución,** en el cual necesariamente debe existir una comunicación "*Inter-access point*". El estándar no especifica ninguna tecnología en particular para el sistema de distribución.

En la mayoría de los productos comerciales 802.11 el sistema de distribución es implementado como una combinación del proceso de "bridging" (reenvío de paquetes con base en la dirección MAC que realiza el access point) y el *medio de sistema de distribución* que es el *backbone* de la red usado para la retransmisión de paquetes entre los APs, que generalmente es Ethernet.

1.2.2.2. **Punto de acceso (**Access Point, AP)

Realiza las funciones de coordinación centralizada de la comunicación entre las distintas estaciones de la red, pero la principal función es la de "*bridging*" o *gateway* (pasarela) entre la red inalámbrica con la red cableada.

1.2.2.3. **Medio inalámbrico** (Wireless medium)

Los equipos inalámbricos emplean ondas de radio en sus comunicaciones, de esta manera, se puede llevar información de un punto a otro si necesidad de disponer de una instalación más que el aire. La capa física define diferentes formas de difusión y modulación de la información para su transmisión a través del aire.

1.2.2.4. **Estaciones** (stations)

Las estaciones son todos los equipos terminales con interfaces de red inalámbricos, comúnmente son computadoras portátiles, aunque esto no significa que las de escritorio no puedan tener acceso a la red inalámbrica, PDAs, celulares, etc.

1.2.3. Tipos o topologías de red

La topología de una red es la arquitectura de la red, la estructura jerárquica que hace posible la interconexión de los equipos. IEEE 802.11, contempla tres topologías distintas:

1.2.3.1. Ad hoc

Técnicamente conocido como **IBSS (***Independent Basic Service Set*, 'Conjunto de Servicios Básicos Independientes').

Permite exclusivamente comunicaciones directas entre los distintos terminales que forman la red. En este caso no existe ninguna terminal principal que coordine al grupo, no existe punto de acceso. Todas las comunicaciones son directas entre dos o más terminales del grupo. A la red *ad hoc*, también se le conoce como de "igual a igual" *(peer-to-peer* en inglés). Generalmente una red ad hoc está compuesta por un número pequeño de estaciones, para un propósito específico y por un periodo corto de tiempo. (véase figura 1.3).

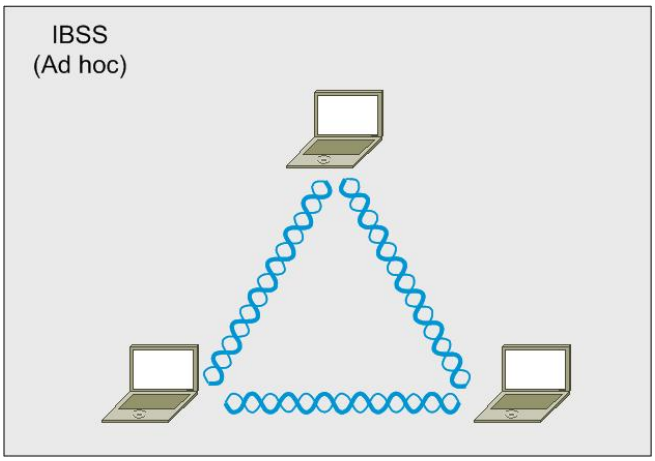

Figura 1.3. Modo Ad-hoc o peer to peer

1.2.3.2. Infraestructura

BSS *(Basic Service Set,* 'Conjunto de Servicios Básicos').
En esta modalidad se añade un AP, que va a realizar las funciones de coordinación centralizada

de la comunicación entre los distintos terminales de la red, como se ilustra en la figura 1.4.

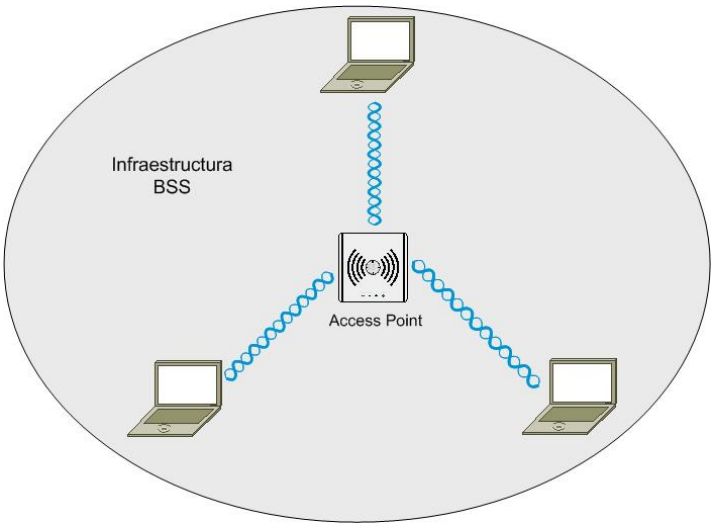

Figura 1.4. Modo infraestructura: BSS

ESS *(Extended Service Set,* 'Conjunto de Servicios Extendido').
Permite crear una red inalámbrica formada por más de un AP (véase figura 1.5). De esta forma se puede extender el área de cobertura de la red, quedando constituida por un conjunto de celdas pegadas unas a otras. Una red ESS está formada por múltiples redes BSS.

En las topologías BSS y ESS todas las comunicaciones pasan por los APs. Aunque dos terminales estén situados uno junto al otro, la comunicación entre ellos pasará por el punto de acceso al que estén asociados. Esto quiere decir que una terminal no puede estar configurada para funcionar en la modalidad *ad hoc* (IBBS) y de infraestructura (BSS) a la vez.

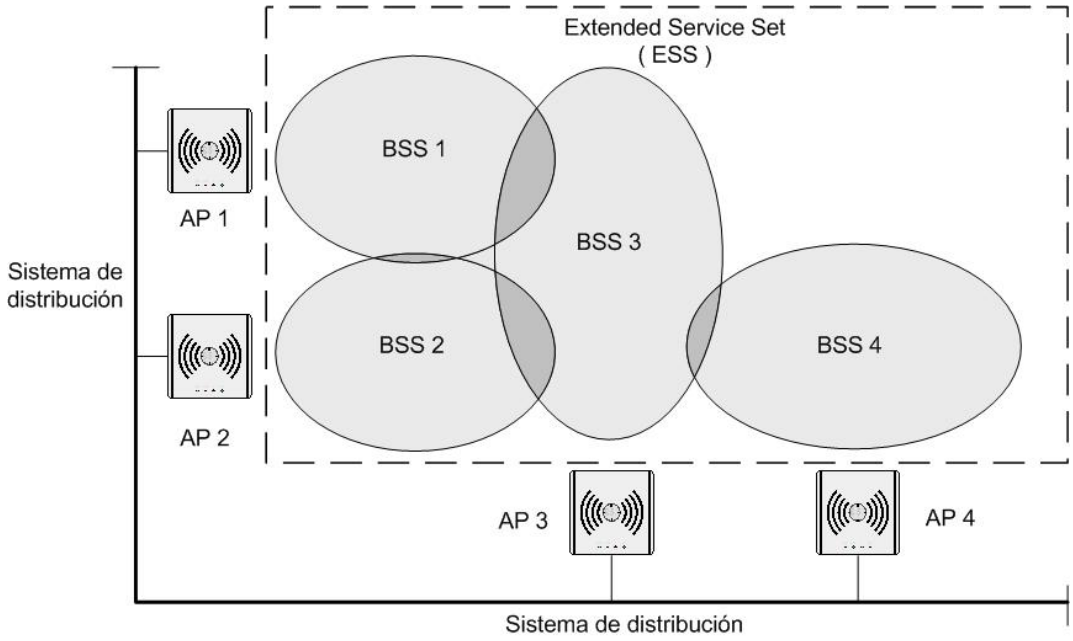

Figura 1.5. Modo infraestructura: ESS

1.2.3.3. Wirereless bridging

El **sistema de distribución** se conforma de dos elementos:

Bridging que es una las funciones del AP y **el medio de distribución** que es el *backbone de la red*. (Usualmente una Ethernet).

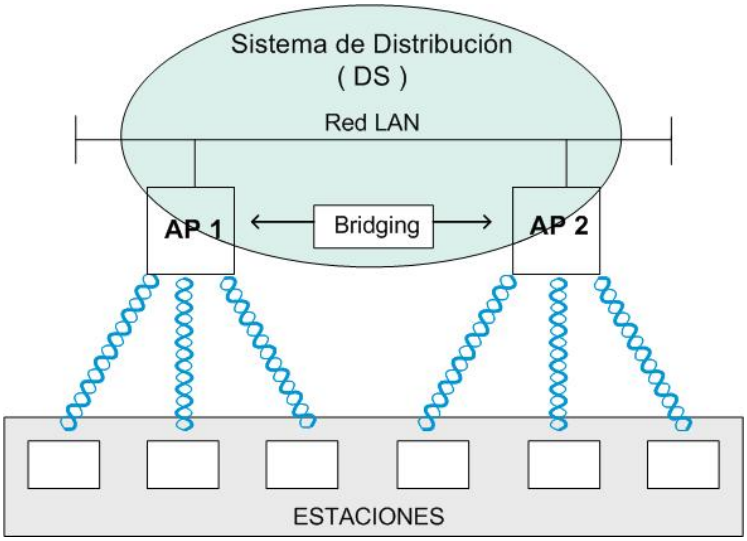

Figura 1.6. Sistema de distribución

Como se observa en la figura 1.6 existe un Sistema de Distribución (DS) también llamado Sistema de distribución inalámbrico (Wireles Distribution System, WDS). Las especificaciones del estándar también permiten que el medio de distribución sea inalámbrico. El WDS permite realizar enlaces entre dos LANs.

En este tipo de Red, se requiere incluir el uso de antenas direccionales. El objetivo de estas antenas direccionales es el de enlazar redes que se encuentran situadas geográficamente en sitios distintos tal y como se muestra en la figura 1.7. Un ejemplo de esta configuración lo tenemos en el caso en que tengamos una red local en un edificio y la queramos extender a otro edificio. Por lo que será necesario instalar una antena direccional en cada edificio apuntándose mutuamente.

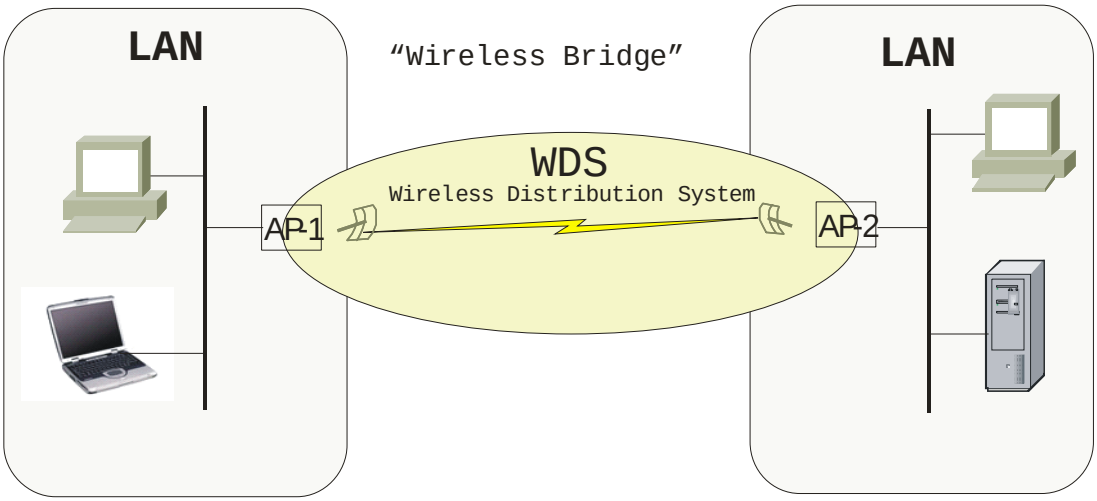

Figura 1.7. Topología building to building

CAPÍTULO 2

AMENAZAS Y VULNERABILIDADES EN LAS WLAN

2. AMENAZAS Y VULNERABILIDADES EN LAS WLAN

2.1. Introducción a la seguridad

Es necesario tener conocimiento acerca de las vulnerabilidades inherentes a la tecnología de redes inalámbricas, los riesgos y las amenazas a las que están expuestas, para establecer las medidas de protección con eficacia.

Implementar una infraestructura de seguridad fuerte requiere una estrategia: una definición de políticas que identifiquen las amenazas y que permita determinar las medidas a utilizar para mitigarlos. Si no se tiene conciencia de las amenazas y métodos de ataques, no será posible determinar el impacto que pudieran causar. Es necesario comprender los riesgos, para poder establecer medidas efectivas y contrarrestarlas.

2.1.1. Seguridad

No existe una definición única y exacta de seguridad, en términos generales se puede decir que la seguridad es una colección de soluciones que tiene por objeto proteger algún sistema de comunicaciones de datos o los datos mismos.

Más que tener una definición formal de seguridad, lo más importante es entenderla de acuerdo al contexto en el que se esté hablando, pero sobre todo entenderla en función de los objetivos o metas, tener claro qué es lo que se quiere proteger, contra quién se protege y porqué se protege.

2.1.1.1. Los objetivos de seguridad

Los objetivos de seguridad, también conocidos como servicios de seguridad más comunes en redes inalámbricas, se pueden clasificar de la siguiente manera:

- **Confidencialidad.** Proteger la información transmitida para que nadie pueda leerla o interpretarla más que para a quién va dirigida.

- **Integridad.** Proteger la información transmitida para garantizar su fiabilidad y evitar que no sea modificada o borrada.

- **Disponibilidad.** Que la información y los servicios de red estén presentes cuando los usuarios los requieran.

- **Control de Acceso.** Restringir y controlar los accesos de los usuarios a la red y a los recursos de red.

    - **Autenticación.** Implementar mecanismos para garantizar que un usuario o un equipo sea realmente quien dice ser.

    - **Autorización.** Restringir los privilegios para operar los recursos de red de acuerdo al nivel de autorización que tiene el usuario.

    - **Accounting.** Llevar un registro de las conexiones a la red de los usuarios.

Todos estos aspectos son importantes de considerar, el nivel de importancia dependerá de las características de la organización, de los servicios y aplicaciones que se ofrecerán sobre la red.

2.1.1.2. Los adversarios

Es importante conocer y entender las motivaciones de los adversarios, esto permitirá establecer y evaluar mucho mejor las defensas.

Los hackers pueden clasificarse en tres categorías de amenazas que pueden representarse como una pirámide, en donde en la parte inferior se encuentran los “script kiddies” quienes únicamente se limitan a ejecutar herramientas hacking existentes. En la parte intermedia de la pirámide el número de atacantes disminuye pero los conocimientos y la complejidad de las herramientas que usan aumentan, aquí se pueden encontrar herramientas que buscan romper los sistemas de cifrado. En la parte alta de la pirámide se encuentra un grupo reducido de hackers, pero emplean técnicas altamente sofisticadas.

En los sistemas de seguridad no hay ninguna distinción entre ataques accidentales y especializados. Cualquier visitante "extraño" en la red debe ser considerado como un potencial enemigo, sin tener en cuenta sus motivaciones o habilidades.

El trabajo de las políticas de seguridad es anticiparse a los posibles ataques, y el trabajo de los protocolos de seguridad es bloquearlos. Anticiparse a todas las opciones correctamente es uno de los retos de una buena seguridad. Sino, sucede lo que comúnmente se dice: "De nada sirve tener fuertemente bloqueado la puerta de una casa, si se tiene la ventana abierta".

Casi todos los ataques son efectuados por alguna de las siguientes motivaciones:

a) Diversión

La mayor parte de los ataques provienen de personas que se la pasan bajando y ejecutando programas o scripts, sólo por diversión. En la red existen una gran cantidad de programas fáciles de bajarlos, instalarlos y ejecutarlos, sin necesidad de tener conocimientos avanzados sobre seguridad y muchas de éstas herramientas trabajan de forma casi automática.

Aunque el mayor número de ataques son de este tipo, éstos son fáciles de bloquear. Incluso hasta con el más simple mecanismo de protección proporcionados puede bloquearlos. Pero desafortunadamente existen muchas redes inalámbricas "abiertas", completamente libres de algún mecanismo de seguridad donde es fácil para cualquiera, con una laptop y con una tarjeta inalámbrica, tener acceso a la red.

b) Beneficio o Venganza

Los ataques pueden ser realizados con la finalidad de alterar o dañar algún sistema por venganza. El robo de información para obtener algún beneficio, es otra de las motivaciones que orientan a los ataques.

Los ataques para obtener beneficio o por venganza tienen un objetivo específico y un blanco determinado. Antes de ser efectuados, hay a una planeación previa e inversión de tiempo y dinero, se investigan los métodos adecuados, posibles vulnerabilidades y se eligen las

herramientas correctas para llevarlo a cabo, sí el blanco tiene una red inalámbrica seguramente se iniciaría a buscar entrar por esta vía.

c) Ego

En la cúspide de la pirámide de amenazas se encuentran los hackers que actúan solamente por ego, conocidos como "ego hackers", que son los que más se asemejan a la idea que se tiene de un "hacker". Son personas motivadas solamente por demostrar su capacidad, buscan ser reconocidos como miembros de grupos de élite, dentro de los cuales se demuestran ataques exitosos realizados y se distribuyen nuevas técnicas o herramientas de ataque creadas. Entienden a detalle como funcionan los protocolos de seguridad del sistema que buscan atacar. Sus conocimientos y habilidades los ponen a la par con los investigadores de seguridad. Los investigadores de seguridad saben que están en competencia con este tipo hackers y muchas veces serán superados en encontrar alguna vulnerabilidad.

d) La ignorancia

La ignorancia también representa una adversidad a la seguridad en las redes inalámbricas, en las organizaciones donde no se consideran un procedimiento formal de implementación de WLAN pueden enfrentar amenazas, como por ejemplo de Rogue APs, que generalmente son instalados por empleados ingenuos, dentro del firewall de la organización, sin medidas de seguridad. Estos APs, sin intención maliciosa, se convierten en una puerta trasera a la red, exponiendo datos confidenciales y sistemas sensibles dentro de la red local, a los atacantes.

2.1.2. Amenazas y vulnerabilidades en las WLAN

Antes de presentar las amenazas y vulnerabilidades es necesario conocer las definiciones de estos términos que en ocasiones se consideran como sinónimos pero que son distintos, aunque son estrechamente relacionados y resulta a veces difícil de diferenciarlos.

Amenaza. Constituye un peligro potencial asociado con un fenómeno físico de origen natural o tecnológico que se puede presentar en un momento determinado y en un sitio específico

provocando consecuencias adversas, una amenaza es todo aquello que intenta o pretende destruir.

Vulnerabilidad. También se conoce como falla o brecha, representa el grado de exposición a las amenazas, son debilidades intrínsecas de un objeto o elemento.

Riesgo. Es el resultado de la probabilidad de ocurrencia de eventos peligrosos (amenaza) y de la vulnerabilidad de los elementos expuestos a tales amenazas. Los riesgos se pueden reducir sí se consideran medidas preventivas.

2.1.2.1. Clasificación general de amenazas o ataques inherentes a las WLAN

Las amenazas o ataques inherentes a las redes inalámbricas se pueden clasificar en dos grandes grupos como se describen a continuación:

a) Ataques pasivos

En este tipo de ataques, el intruso o usuario no autorizado no modifica la información ni interrumpe la comunicación. Hay dos tipos de ataques pasivos:

> **Eavesdropping**: El atacante "escucha" la comunicación, es decir monitorea la transmisión de datos entre los dispositivos inalámbricos en busca de información sensible como cuentas de usuario y contraseñas.
>
> **Análisis de tráfico:** Es una forma de ataque más inteligente que el anterior, se puede realizar un análisis profundo del tráfico y hacer búsquedas de patrones de cadenas.

b) Ataques Activos

Este tipo ataques involucran algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Los ataques activos pueden ser detectados, pero es posible que no puedan ser prevenibles. Pueden clasificarse de la siguiente forma:

Suplantación de identidad: El atacante se hace pasar por un usuario autorizado, para obtener accesos y privilegios.

Reenvío: El atacante, primero realiza un ataque pasivo, es decir monitorea la transmisión de datos, después retransmite paquetes como si fuera un usuario legítimo.

Modificación de mensajes: El atacante altera el mensaje de un usuario válido, ya sea borrando, agregando, cambiando o reordenando el mensaje.

Denegación del servicio: El atacante degrada o paraliza el servicio de la comunicación.

2.1.2.2. Vulnerabilidades

Se estudian las vulnerabilidades en las WLAN con base en lo que puede ocurrir ante los diferentes servicios de seguridad:

Vulnerabilidad en la confidencialidad

La confidencialidad es un requerimiento de seguridad fundamental, debido al medio de transmisión que utiliza las redes inalámbricas, resulta más difícil conseguir la confidencialidad en una WLAN que en una red cableada, en esta última un atacante requiere de un punto físico específico para tener acceso a la red, en cambio las señales de radio se propagan a través del espacio y el atacante solo requiere estar dentro de la zona de cobertura para tener acceso.

Los ataques pasivos eavesdropping representan una amenaza en las redes WLAN dicha amenaza se presenta porque las señales 802.11 cubre espacios más allá de donde se tenga control físico.
La facilidad con la se podría realizar un ataque eavesdropping, en el peor de los casos, se presenta cuando se omite la configuración de la funcionalidad de confidencialidad en los APs, por otro lado el estándar original 802.11 define WEP para garantizar la confidencialidad pero hoy día existe una infinidad de herramientas que permiten el rompimiento de WEP con gran facilidad.

Otro riesgo de pérdida de confidencialidad surge cuando un AP se conecta a un Hub, que es un dispositivo de red que reproduce todo el tráfico de broadcast a todos sus puertos, provocando que todo este tipo de tráfico sea retransmitido a su vez, por el AP por su interfaz de radio. Una forma de mitigar este problema es el uso de Switches en lugar de Hubs para conectar los APs.

La pérdida de confidencialidad conduce a los riesgos de ataques activos, debido a que los analizadores de tráfico inalámbricos son capaces de obtener nombres de usuario y contraseñas, el atacante puede suplantar usuarios válidos y conseguir acceso a la red local a través del AP y tener a la mano recursos y datos sensibles.

Otro problema muy cómun son los “rogue” APs, que pueden ser introducidos por usuarios con o sin intensiones maliciosas. Un rogue AP configurado de tal forma que parezca un Access Point legítimo puede fácilmente engañar a los usuarios inalámbricos, logrando capturar todo el tráfico de éstos usuarios y saltarse así todos algoritmos de seguridad implementados.

Por medio de los rogue APs también se puede lograr los accesos no autorizados a la red local, logrando saltarse todos los mecanismos de seguridad perimetral implementados. Y lo peor de todo, es que no son instalados precisamente por intrusos, sino por usuarios irresponsables quienes con el fin de aprovechar las ventajas de las WLAN instalan AP sin autorización del administrador de seguridad de la organización, y lo más grave es que lo hacen sin contemplar ninguna medida de seguridad en la configuración.

Vulnerabilidad en la integridad

El estándar original 802.11 no proporciona un mecanismo fuerte para proteger la integridad de los mensajes, el protocolo WEP usa CRC-32 para estas funciones, al que se le han encontrado deficiencias que permite que un atacante pueda borrar y/o modificar los datos en el sistema inalámbrico.

Vulnerabilidad en la disponibilidad

Existen dos formas de ataques de denegación de servicio (DoS) que pueden causar la pérdida de disponibilidad en una red inalámbrica: *Jamming y flooding.*

El jamming ocurre cuando un atacante emite deliberadamente señales RF desde un dispositivo inalámbrico, saturando el medio inalámbrico y como consecuencia provoca interferencia en la comunicación, aunque también puede ocurrir jamming sin intensiones maliciosas, cuando existen otros dispositivos que operan en la misma frecuencia, como por ejemplo los teléfonos inalámbricos o un horno de microondas. Un jamming puede provocar la degradación de la comunicación o hasta la ruptura total de la comunicación.

Un ataque flooding consiste en el uso de un software diseñado para emitir paquetes grandes, dirigidos al Access Point o a algún usuario inalámbrico particular, con lo que consigue inundar de paquetes y provocar así la degradación o la interrupción total de la comunicación.

Al igual que jamming, se puede provocar flooding sin intensiones maliciosas, cuando un usuario se adueña del ancho de banda al bajar archivos muy grandes, denegando el acceso a la red a otros usuarios. Por lo que se tiene que contemplar políticas que contemplen el control en el uso de ancho de banda.

Ambas amenazas son difíciles de contrarrestar, el estándar 802.11 no define ningún mecanismo de defensa.

2.1.2.3. Riesgos a la seguridad

Además de los riesgos que representan las amenazas y vulnerabilidades mencionadas en las secciones anteriores, existes otros, uno de los que requiere mayor consideración es la conexión a la red local de una organización desde una red inalámbrica pública, como las que existen en aeropuertos, hoteles ó cafés; que en la mayoría de los casos son redes abiertas que operan con pocas restricciones de seguridad. Un usuario móvil puede abrir un hueco de seguridad a su

organización al conectarse a una red pública a menos que se tenga implementado el uso de protocolos de seguridad a nivel de aplicación, como TLS u otras soluciones VPN, para proteger la comunicación de escuchas espías y de accesos no autorizados.

Se pueden mitigar los riesgos que representan las WLAN, aplicando una serie de políticas enfocadas a amenazas y vulnerabilidades específicas. Políticas de administración combinadas con políticas operacionales y técnicas pueden resultar efectivas para contrarrestar los riegos asociados con las redes inalámbricas. Seguir los pasos que se sugieren no garantiza una seguridad absoluta, pero sí pueden reducir considerablemente los riesgos, además el nivel seguridad que se necesite implementar está en función de la inversión económica y en el tiempo en la implementación, en la administración y operación del sistema, además de que implica cierta complejidad para los usuarios móviles finales en obtener la conexión. Cada organización requiere evaluar los riesgos y establecer un nivel de seguridad de acuerdo a sus necesidades y posibilidades.

Políticas de administración

Una política de seguridad en redes inalámbricas es la piedra angular para las medidas de administración y son muy importantes para tener un nivel adecuado de seguridad inicial. Una política de seguridad y la capacidad de hacerla cumplir son las bases para el establecimiento de las medidas operacionales y técnicas.

Políticas operacionales

Es importante también la definición de políticas sobre la protección de los dispositivos inalámbricos de forma física, proteger estos equipos de robos o daños resulta un poco más complicado que los dispositivos de red tradicionales que generalmente se cuenta con un “site” específico; en el caso de los equipos WLAN son esparcidos a lo largo de las áreas de la organización en las localidades en donde se requiera el servicio de acceso inalámbrico, tendrá un mecanismo específico de protección física.

Otro aspecto importante a considerar son los alcances físicos o señal de cobertura que alcanzarán los APs. Es difícil limitar las fronteras de los patrones de radiación, pero aumentando o disminuyendo las ganancias de las antenas, contemplar el uso de antenas direccionales y buscando una adecuada ubicación de los APs se puede conseguir aproximar un poco a las necesidades de cobertura.

Políticas técnicas

Consisten en las políticas sobre soluciones de hardware y software, establecimiento de configuraciones adecuadas, con las funcionalidades requeridas de cifrado, autenticación, sistemas de detección y prevención de intrusiones, implementación de VPN, PKI, Actualizaciones de software, parches, etc.

Algunas políticas generales

En una implementación de red inalámbrica, cada organización establecerá políticas específicas de acuerdo a sus necesidades y posibilidades, a continuación se presentan un conjunto de políticas generales que podrían considerarse en la construcción de una WLAN:

- Identificar los usuarios que serán autorizados de hacer de la red inalámbrica
- Identificar los tipos de accesos y servicios que serán proporcionados a través de la red inalámbrica
- Definir a las personas responsables de instalar y configurar los equipos inalámbricos.
- Definir los mecanismos para proporcionar seguridad física a los dispositivos inalámbricos.
- Determinar los servicios y el tipo de información que podrá ser manejado a través de la red inalámbrica, incluyendo las políticas de uso aceptable.
- Definir las configuraciones a implementar en todos los dispositivos inalámbricos para asegurar cierto nivel de seguridad.
- Describir las áreas o lugares en los que será permitido la instalación de red inalámbrica.

- Definir los procedimientos a seguir en caso de pérdida de los dispositivos inalámbricos y en casos de incidentes de seguridad.
- Definir sugerencia para minimizar el robo de dispositivos inalámbricos a los usuarios.
- Definir políticas de los mecanismos de cifrado a utilizar.
- Determinar las acciones a seguir para detectar los rogue AP y los dispositivos mal configurados.
- Determinar las frecuencias a las que operaran los AP.
- Definir las medidas a tomar en caso de no cumplir con las políticas establecidas.

Los administradores de red deben estar totalmente concientes de los riesgos de seguridad que representan las WLAN, buscar que se cumplan las políticas de seguridad y tener un procedimiento a seguir en caso de un ataque.

CAPÍTULO 3

SEGURIDAD EN LAS WLAN: IEEE 802.11i y WPA

3. SEGURIDAD EN LAS WLAN: IEEE 802.11i y WPA

Cuando se habla de seguridad en Redes Inalámbricas, generalmente se escuchan términos como WEP, 802.1X, 802.11i, WPA, WPA2, RSN, TSN, TKIP, AES, EAP, TLS, PEAP, etc., pero ¿Qué significan?, son términos que en este capitulo y el siguiente, se buscará dejar claro el papel que juegan dentro de la seguridad de las WLAN.

3.1. Wi-Fi e IEEE 802.11

IEEE 802.11 es un estándar de la IEEE que define los protocolos de comunicaciones en las capas Física y Enlace del modelo de referencia OSI para Redes Inalámbricas de Área Local (WLAN por sus siglas en ingles); 802.11 fue la versión original publicada en 1997, pero se han realizado mejoras en la velocidad de transmisión y actualmente se tienen las siguientes variantes: 802.11b, 802.11a, 802.11g y 802.11n.

IEEE 802.11 es un estándar muy extenso y complejo, a pesar de los esfuerzos del grupo de trabajo, existen áreas en las especificaciones del estándar que son ambiguas o parcialmente definidas, así también maneja un número de funcionalidades considerados como opcionales. Todo esto causa problemas de interoperabilidad entre los equipos de diferentes fabricantes. Para solucionar esta situación se formó la Alianza Wi-Fi, integrado por la mayoría de fabricantes creando la certificación “Wi-Fi”.

Para obtener la certificación Wi-Fi, el fabricante debe someter su equipo ante un conjunto de pruebas que la Alianza Wi-Fi ha definido, basados en el estándar. Evalúan únicamente un subconjunto de aspectos del estándar, principalmente los que puedan garantizar la interoperabilidad. Además el fabricante debe cumplir con algunos requerimientos adicionales al estándar. En resumen, Wi-Fi define un subconjunto de IEEE 802.11 con algunas extensiones. La figura 3.1 muestra esta relación.

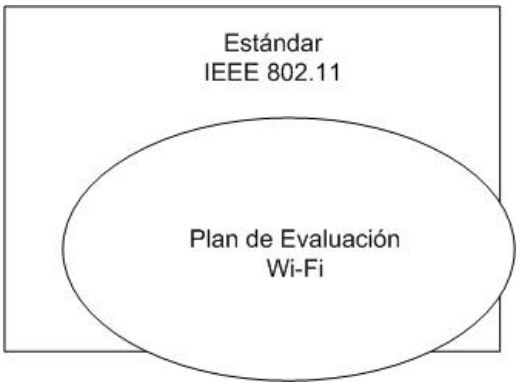

Figura 3.1. Relación entre Wi-Fi e IEEE 802.11

3.2. WEP

WEP (Wired Equivalent Privacy, 'Privacidad equivalente Alámbrica') es el sistema de seguridad original del estándar 802.11, pensado para proporcionar privacidad y confidencialidad a las comunicaciones inalámbricas equivalentes a las que existe en una red tradicional.

El protocolo WEP fue diseñado por la IEEE para proporcionar los siguientes tres servicios de seguridad básicas:

- **Autenticación.** El primer objetivo de servicio de seguridad WEP fue la autenticación, que consiste en verificar la identidad de las estaciones terminales; es decir proporciona un control de acceso a la red, denegando el acceso a una estación terminal que no se autentique correctamente.

- **Confidencialidad.** El segundo objetivo WEP fue proporcionar privacidad y/o confidencialidad a las comunicaciones inalámbricas de forma equivalente o similar a la que existe en una red tradicional, con el fin de evitar escuchas espías (ataques pasivos).

- **Integridad.** Otro servicio de seguridad WEP fue evitar la modificación de los mensajes (ataque activo) durante el tránsito entre las estaciones y el AP.

WEP no define mecanismos sobre autorización, auditoría, administración y distribución de las llaves entre otros servicios de seguridad necesarios.

3.2.1. Autenticación

El estándar 802.11 inicialmente define dos formas de autenticación:

- Sistema de autenticación abierta (Open System Authentication). Obligatorio
- Autenticación de llave compartida (Shared key authentication). Opcional

3.2.1.1. Autenticación abierta

El sistema de autenticación no maneja ningún mecanismo de autenticación, la forma en que las estaciones pasan a ser "autenticados" es proporcionando la siguiente información:

SSID (Service Set IDentifier) del AP. El SSID es un nombre que se les asignan a las WLAN para que las estaciones puedan distinguir entre una red y otra. Los APs envían mensajes de broadcast en texto plano anunciando su SSID, por lo que cualquiera puede conocerlo. En ningún momento se pensó usar el SSID como una funcionalidad de control de acceso.

Control de acceso por direcciones MAC. En algunas implementaciones de WLAN, los administradores definen una lista de direcciones MAC que corresponden a las interfaces inalámbricas de las estaciones a la que tendrán permitido el acceso (Filtrado por direcciones MAC). Las direcciones MAC se transmiten en claro, por lo que es muy fácil obtener una dirección válida y falsificarla.

En el sistema de autenticación abierta, los APs no se autentican con las estaciones, esto permite el riesgo de que estaciones se conecten a rogue APs, que son APs falsos con el mismo SSID.

3.2.1.2. Autenticación de llave compartida

Se pensó en este tipo de autenticación como una mejora del sistema abierto, pero es igual de insegura o hasta resulta peor usarlo.

Este tipo de autenticación utiliza una llave de cifrado secreta "pre-compartida" conocida como llave WEP que son compartidas por todas las estaciones y APs. La autenticación de llave

compartida se basa en el esquema simple de desafío/respuesta para asegurar que la estación conoce la llave WEP.

1. La estación inicia el proceso de autenticación enviando un mensaje de solicitud de autenticación.
2. El AP responde con un mensaje de desafío, que es un número generado aleatoriamente de 64 o 128 bits.
3. La estación cifra el desafío utilizando la llave WEP y envía el resultado de regreso al AP.
4. El AP descifra el desafío cifrado por la estación con la misma llave WEP, si recupera el mensaje original, significa que la estación conoce la llave WEP y por lo tanto tiene permitido el acceso, por lo que el AP confirma a la estación que la autenticación fue exitosa y le permite el acceso.

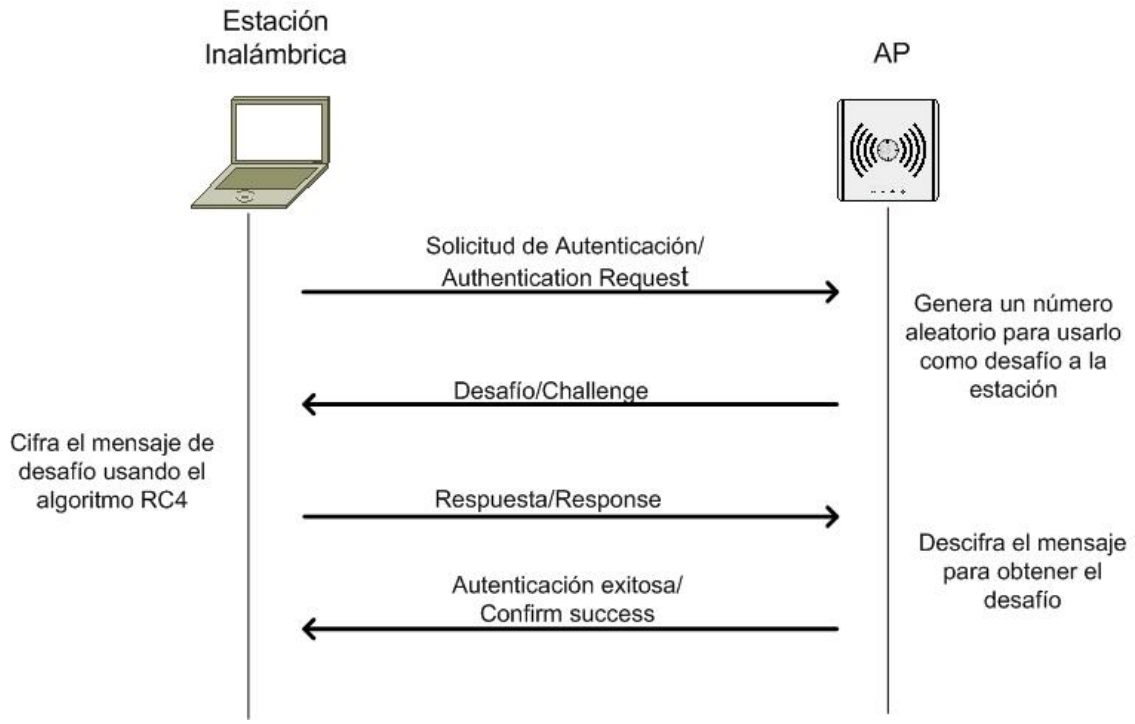

Figura 3.2. Autenticación WEP: Llave compartida

La autenticación de llave compartida también se le conoce como autenticación WEP. Utiliza el algoritmo RC4 para el cifrado de los datos. No existe la autenticación de los APs hacia las estaciones.

Los procesos de autenticación basados en los esquemas desafío/respuesta son susceptibles a ataques de “man in the middle” y ataques de fuerza bruta o de diccionario.

Una forma de vulnerar este mecanismo de autenticación consiste en que un atacante puede escuchar, capturar un mensaje desafío en texto claro y su correspondiente en forma cifrada; a partir del análisis de estas dos piezas de información se puede obtener la llave (key stream). Por este problema, es preferible mantener la autenticación abierta, porque una vez que se obtiene la llave WEP por la forma descrita anteriormente, el atacante además de que logra el acceso también compromete la privacidad y confidencialidad de la comunicación, ya que el protocolo WEP usa la misma llave para la autenticación y para el cifrado de los datos en la comunicación.

Otra limitación de la autenticación compartida es que la autenticación es sobre la identidad del dispositivo y no del usuario; una vez que una estación tenga configurada la llave secreta cualquier usuario que la tenga en sus manos será capaz acceder a la WLAN.

Otro inconveniente se presenta cuando los usuarios definen llaves WEP débiles o peor aún, en algunas implementaciones los administradores mantiene las llaves de *deafult* establecidas por el fabricante.

3.2.2. Cifrado/Privacidad

El protocolo WEP usa el algoritmo de cifrado de flujo RC4 para proteger la comunicación de las escuchas espías. WEP define un tamaño de llave de 40 bits, aunque algunos fabricantes soportan llaves de 104 bits, incluso de hasta 232 bits. El estándar también especifica el uso de un IV (Initialization Vector, ‘Vector de Inicialización’) de 24 bits, que se agrega a la llave WEP para conformar una llave RC4 de 64 bits que servirá como semilla para generar el *“key stream”*, véase figura 3.3. La llave RC4 será de 128 y 256 bits cuando la llave WEP es de 104 y 232 bits, respectivamente. Idealmente una llave más grande proporciona mayor protección, pero en el caso de WEP no es así, porque los problemas radican principalmente en la forma de usar el IV y de deficiencias del algoritmo de cifrado RC4.

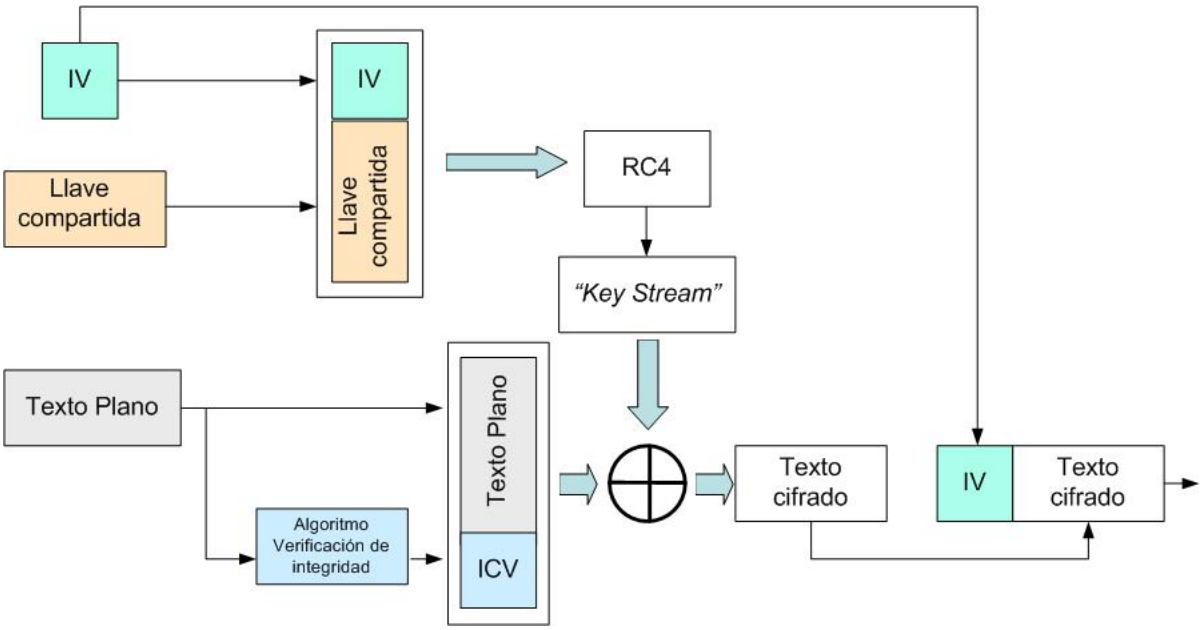

Figura 3.3. Cifrado WEP

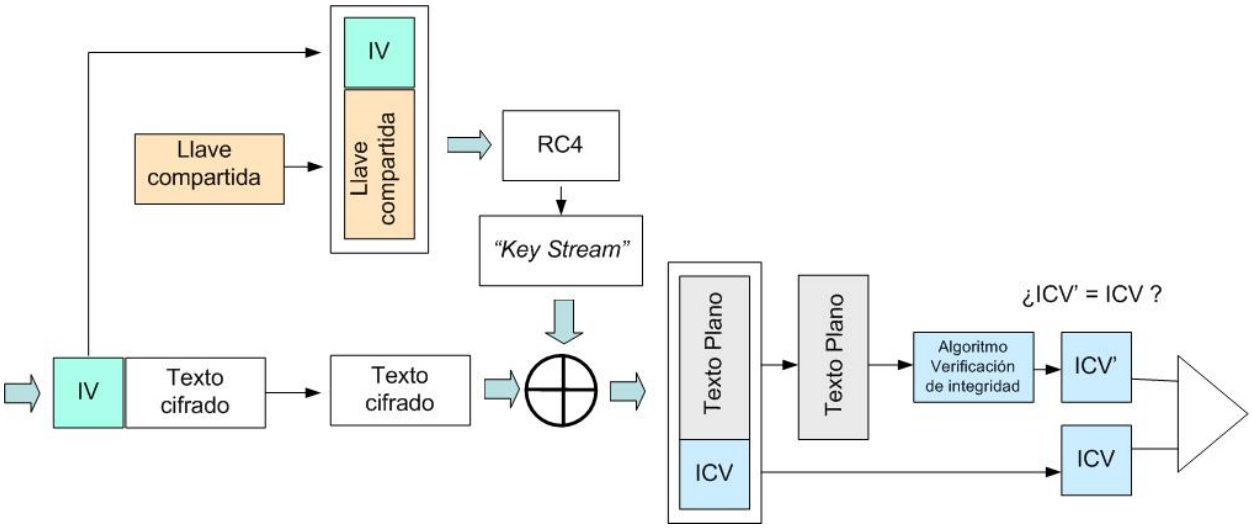

Figura 3.4. Descifrado WEP

Gran parte de los ataques a WEP se debe a las vulnerabilidades en el IV. Esta parte de la llave RC4 viaja en claro (como se observa en las figuras 3.3 y 3.4), con la captura y análisis de una cantidad relativamente pequeña de este tipo de tráfico, un atacante puede recuperar la llave; el espacio de combinaciones con 24 bits para los IV's es relativamente pequeño y la forma en que WEP implementa el algoritmo RC4. Además el estándar no define exactamente como establecer y cambiar los valores de los IV's, algunos fabricantes utilizan valores estáticos conocidos. Si dos mensajes tienen el mismo IV y se conoce el texto plano de uno de ellos, resulta trivial encontrar el texto plano del otro mensaje; es sencillo encontrar el primer mensaje con texto plano conocido

porque hay muchos de ellos con información de encabezados muy comunes conocidos u otros fáciles de adivinar; aunado al reducido tamaño de los IV's, ejemplo, pensando que el fabricante decide emplearlos usando números secuenciales, después de 17, 000,000 de paquetes se agotan todas las posibilidades y se empiezan a generar mensajes con IV's repetidos; en una red WLAN con tráfico, se logran agotar los IV's en unas cuantas horas. Incluso en el mejor caso de uso de los IV's que consiste en generar números aleatoriamente, por la paradoja del "*cumpleaños*", existe un 50% de probabilidad de que después de 2^{12} mensajes, dos IV's sean iguales.

3.2.3. Integridad

Para conseguir que los datos no sean alterados durante la transmisión entre las estaciones y APs, WEP calcula un valor ICV (Integrity Check Value) aplicando el algoritmo CRC-32 sobre el mensaje de texto plano. El mensaje de texto plano más su valor ICV son cifrados por el *key stream* generado por RC4 antes de ser enviado. En el receptor se sigue el proceso inverso; una vez recuperado el mensaje, se vuelve calcular su valor ICV' y se compara con el obtenido en el transmisor (ver Fig. 3.4). Si los valores son iguales el mensaje se considera que no sufrido alteración o no hubo ningún error durante la transmisión, en caso contrario, el mensaje se desecha.

Al igual que en el servicio de privacidad, la integridad 802.11 es vulnerable a cierto tipo de ataques, independientemente del tamaño de la llave. CRC-32 es blanco de varias amenazas de seguridad, entre las más importantes está el ataque de "bit-flipping", que ocurre cuando se logra saber qué bits cambian en el valor CRC-32 cuando se alteran ciertos bits en el mensaje.

3.2.4. Problemas con el estándar de seguridad 802.11

Se han descubierto muchas vulnerabilidades sobre la seguridad del estándar 802.11, estos problemas permiten que un usuario malicioso pueda ejecutar ataques ya sea pasivos o activos y lograr comprometer la red inalámbrica. A continuación se describen algunas de las deficiencias encontradas.

3.2.4.1. Carece de un mecanismo de administración de llaves

El hecho de que el protocolo WEP no defina especificaciones sobre el manejo y distribución de las llaves, genera una vulnerabilidad. Cuando una WLAN utiliza la misma llave por grandes periodos de tiempo, le permite a un atacante mayor posibilidades de encontrar la llave WEP por medio de captura y análisis de tráfico. Por otro lado, sí una estación inalámbrica fuera extraviado o robado, todo los dispositivos que emplean la misma llave quedan expuestos.

Además, la misma llave o grupo de llaves debe estar configurada en todas las estaciones y en todos los APs. Esta limitante complica la agilidad de respuesta ante incidentes que ponen en riesgo la WLAN, porque el administrador tendría que cambiar las llaves en todos los equipos tan rápido como sea posible, el problema es aún más grave debido a que se compromete también la privacidad y confidencialidad, por el hecho de usar la misma llave para el cifrado de datos. El administrador debe determinar la forma como generarlas, establecerlas y de distribuirlas;

3.2.4.2. Debilidades en los IV's

Como se vio anteriormente, los 24 bits para los IV's no son suficientes, además de que esta parte viaja junto con los mensajes en texto plano y como ya se ha comentado. Además como se observa en el diagrama, RC4 requiere que esta porción de la llave sea distinta, porque cuando se tiene IV's iguales, RC4 genera *key stream* idénticos, este inconveniente se convierte más grave aún porque el estándar no define como establecerlos, por lo que muchos fabricantes optaron por establecer valores constantes; incluso si se generan de forma aleatoria, un atacante le resultará relativamente fácil encontrar el *key stream* a partir de las deficiencias de los IV's.

3.2.4.3. Debilidad en la llave de cifrado

El tamaño de la llave WEP es muy pequeño para proporcionar el nivel de seguridad adecuado. Si un atacante conoce los 24 bits de cada llave y en combinación con las debilidades del algoritmo RC4, puede descifrar paquetes capturados interceptando y analizando una cantidad relativamente pequeña de tráfico.

3.2.4.4. Escasa protección en la integridad

El estándar 802.11 define el algoritmo CRC-32 para verificar la integridad de los paquetes. Es un buen mecanismo para detectar errores en la transmisión pero no proporciona un nivel fuerte de integridad, de hecho existen ataques que permiten modificar el resultado CRC-32 y el contenido del mensaje sin que sean detectados en el receptor, convirtiendo este tipo de ataques difíciles de detectar.

3.2.4.5. Nula protección contra reenvíos y disponibilidad

WEP no proporciona protección contra ataques de reenvío de paquetes, porque en su implementación no contempla ningún contador incremental, un *timestamp* o algo parecido que pueda detectar tráfico de paquetes reenviados. Además el estándar 802.11 no define ningún mecanismo de protección contra los ataques DoS.

Definitivamente WEP, ya no representa ninguna solución a los problemas de seguridad que representa las WLAN.

3.3. IEEE 802.11i

Debido a las limitaciones de seguridad que se encontraron en el protocolo WEP, el estándar IEEE 802.11 creó un nuevo grupo de trabajo llamado IEEE 802.11i, cuyo objetivo fue el de mejorar la seguridad de las redes inalámbricas y cuyas especificaciones finales fueron liberadas a finales de junio del 2004. El estándar **IEEE 802.1X** toma un papel importante en este nuevo sistema de seguridad.

Algunas características importantes:

- Especifica nuevas reglas para robustecer la seguridad en redes inalámbricas 802.11, fue ratificado en junio de 2004.

- Define un nuevo tipo de redes inalámbricas, el llamado RSN (Robust Security Network, 'Red de Seguridad Robusta). En muchos aspectos, este es lo mismo a las redes basadas en WEP, sin embargo para que los dispositivos inalámbricos pueden conformar un RSN, requieren de un número nuevo de capacidades. Debido a que mucha gente no va ha cambiar todos sus equipos inalámbricos de un día para otro, el IEEE 802.11i define TSN (transitional security network, ´Red de Seguridad de Transición'), que permite la interacción entre sistemas WEP y RSN.

- La mayoría de los equipos inalámbricos existentes no pueden ser actualizados a RSN, para hacerlo se requieren nuevos diseños en el hardware.

- Soluciona todas las deficiencias de WEP. Se divide en tres categorías:

    1. TKIP (Temporary Key Integrity Protocol, 'Protocolo de Integridad de Clave Temporal) es una solución rápida y a corto plazo que arregla todo las debilidades de WEP. TKIP puede ser usado con equipos 802.11 no recientes (después de actualizar firmware/driver). TKIP también utiliza un algoritmo de cifrado RC4, lo que implica nuevamente clave simétrica compartida entre la terminal y la estación base. En este caso las claves utilizadas (llamadas Temporal Key) son de 128 bits, que son actualizables cada cierto número de paquetes, y el vector de inicialización es de 48 bits, el cual es reiniciado a 0 cada vez que se fija una nueva clave temporal. TKIP proporciona integridad y confidencialidad.
    2. CCMP (Counter Mode with CBC-MAC Protocol) es un nuevo protocolo, diseñado desde cero. Usa el algoritmo de cifrado AES, el cual requiere mayor recurso de CPU que el algoritmo RC4 (usado en WEP y TKIP), por lo que para hacer uso de esta característica es necesario nuevo hardware. CCMP provee integridad y confidencialidad.
    3. 802.1X Control de Acceso a Red Basado en Puertos: Es usado para la autenticación, ya sea con TKIP o con CCMP.

3.3.1. Manejo de llaves 802.11i

Administración e intercambio dinámico de llaves:

Para realizar las tareas de cifrado e integridad, 802.11i define un sistema de derivación y administración de llaves (véase figura 3.5).

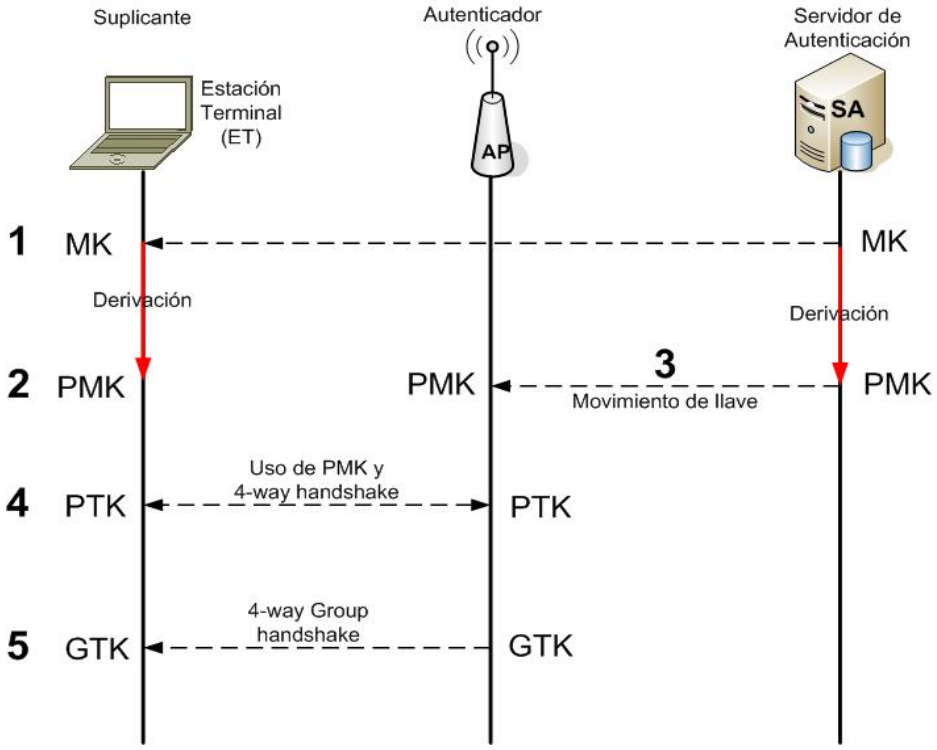

Figura 3.5. 802.11i: Administración y distribución de llaves

1. Después de una autenticación exitosa, el servidor de autenticación envía al suplicante el *master key(MK).* El MK solo es conocido por el suplicante y el servidor de autenticación.
2. Tanto el suplicante como el servidor de autenticación, generan una nueva llave conocido como *Pairwise Master Key (PMK),* a partir del MK.
3. El servidor de autenticación mueve la llave PMK al autenticador. Únicamente el suplicante y el servidor de autenticación pueden generar la PMK. La PMK es una llave simétrica que liga la sesión entre el usuario móvil y el AP o donde se encuentre alojado el autenticador.
4. la estación móvil y el AP usan la PMK y un 4-way handshake para generar la PTK que es una colección de llaves(véase la figura 3.6):

- *Key Confirmation Key (KCK).* Como su nombre lo indica, sirve para confirmar la posesión de la PMK y para ligar la PMK al AP.
- *Key Encryption Key (KEK).* Se utiliza para distribuir la colección Group Transient Key (GTK). Como se describe a continuación.
- *Temporal Key 1 & 2 (TK1/TK2).* Son usados para el cifrado.

5. Se utilizan la KEK y un 4-way group handshake para enviar la GTK del AP a la estación móvil. La GTK es una llave compartida entre todas las estaciones conectadas al mismo autenticador para cifrar el tráfico de multicast y broadcast.

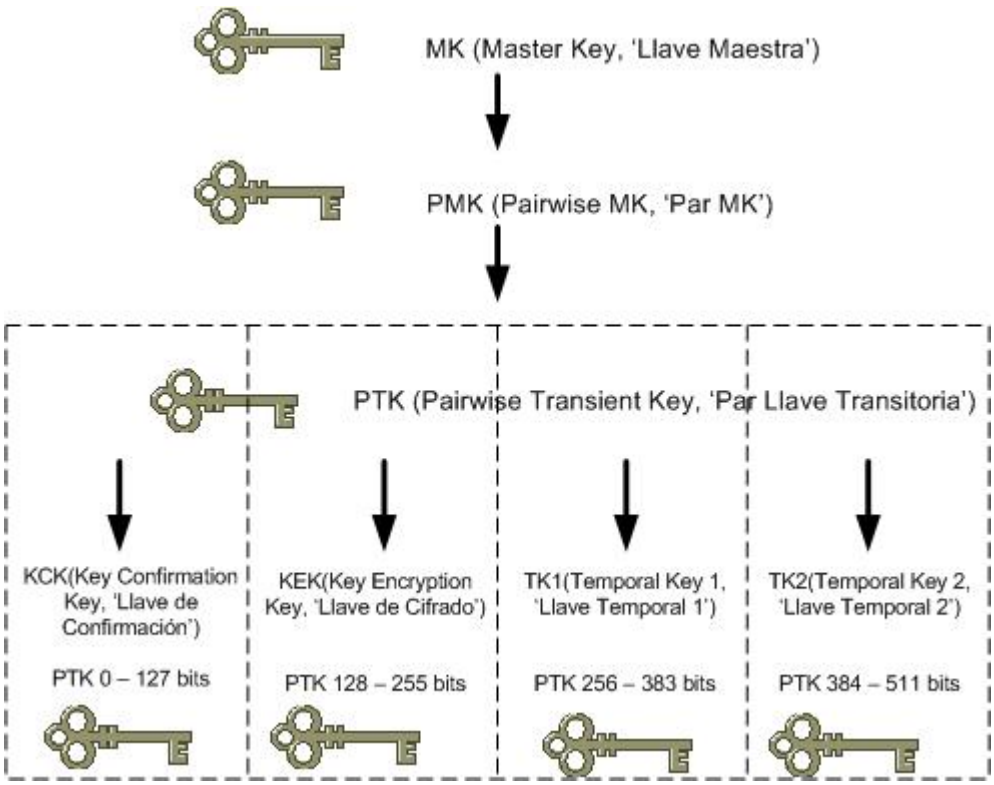

Figura 3.6. Jerarquía de llaves

3.3.2. WPA

Dada la magnitud de alarma que causó en los usuarios de equipos Wi-Fi saberse expuestos ante cualquier usuario malintencionado por el *rompimiento* de WEP, exigieron una solución rápida y que además fuera compatible con el hardware que ya poseían. Ante estas circunstancias, la mayoría de los fabricantes de equipos Wi-Fi conjuntamente con la IEEE, no quisieron esperar la

ratificación de IEEE 802.11i y la solución inmediata que ofrecieron fue WPA (Wi-Fi Protected Access, 'Acceso Wi-Fi protegido'), a mediados del 2003. En realidad WPA es un subconjunto de las especificaciones de 802.11i (se basó en el Draft 3 de 802.11i.), que puede ser adoptado únicamente actualizando el software de los equipos inalámbricos, a diferencia de 802.11i que necesariamente se requiere de cambios en el hardware. No obstante, ambas sistemas de seguridad son totalmente compatibles. WPA es básicamente TKIP + 802.1X.

3.3.3. TSN (WPA) / RSN (WPA2)

Actualmente los nuevos equipos, ya incorporan los esquemas de seguridad 802.11i, también conocido como WPA2 o RSN. Para obtener RSN, el hardware debe soportar y usar CCMP.

Los siguientes términos son equivalentes:

- TSN = TKIP + 802.1X = WPA(1)
- RSN = CCMP + 802.1X = WPA2 = 802.11i

Por otro lado también es común escuchar los siguientes términos relacionados con WPA:

- WPA-PSK
- WPA Empresarial o simplemente WPA.

WPA-PSK (Pre-shared Key, 'Llave pre-compartida')

En ambientes SOHO (Small Office/Home Office), pueden utilizar la opción de la llave compartida, que se conoce como WPA-PSK o WPA Personal, en el que se evita el uso de 802.1X.

La llave PSK de 256 bits, se genera a partir de una contraseña proporcionada o utilizando PBKDFv2 (RFC 2898), esta llave es utilizada como la MK.

WPA Empresarial

Por otro lado, cuando se incluye 8021.1X y por consecuencia el uso de EAP y de un servidor de autenticación, se conoce como WPA Empresarial o simplemente WPA.

Sí se usa AES como algoritmo de cifrado también se habla de

- WPA2-PSK
- WPA2 Empresarial o simplemente WPA2.

Este trabajo se enfoca a la seguridad WPA/WPA2 empresarial, que involucra el control de acceso basado en el estándar 802.1X. En lo sucesivo únicamente se utilizarán los términos WPA/WPA2 para referirse al tipo empresarial.

CAPÍTULO 4

CONTROL DE ACCESO: IEEE 802.1X, EAP Y RADIUS

4. CONTROL DE ACCESO: IEEE 802.1X, EAP y RADIUS

En este capítulo se describen los protocolos usados para implementar el acceso de seguridad de WPA y/o RSN (WPA2):

- IEEE 802.1X.
- EAP: Extensible Authentication Protocol.
- RADIUS: Remote Authentication Dial-In User Service.

Los primeros dos protocolos son obligatorios para WPA y RSN. WPA elige utilizar RADIUS, en tanto que para RSN es una opción.

4.1. IEEE 802.1X

Una de las funciones básicas necesarias para la seguridad, es el control de acceso. Las nuevas soluciones de seguridad se construyen con base en el estándar 802.1X.

El estándar 802.1X define un **Control de Acceso a Red Basado en puertos.**

El control de acceso a red basado en puertos utiliza las características físicas de los accesos a una infraestructura LAN IEEE 802 para proporcionar medios de autenticación y autorización a los dispositivos unidos a un puerto LAN que tiene características de conexión punto a punto, y bloquear el acceso a ese puerto en los casos en que la autenticación y la autorización fallan. Un puerto en este contexto es un simple punto de unión a la infraestructura LAN**.** En una red pueden existir varios puertos; por ejemplo, los puntos de conexión Ethernet de un switch.

802.1X plantea un escenario con tres entidades básicas:

- Supplicant (Suplicante). La entidad que solicita acceso a la red.
- Authenticator (Autenticador). La entidad que controla los accesos
- Authentication Server (Servidor de Autenticación). Entidad que toma la decisión de conexión o no.

El suplicante y autenticador se conocen como PAEs (Port Authentication Entities, 'Entidadades puertos de autenticación').

La figura 4.1 muestra un escenario de control acceso basado en el estándar 802.1X, de forma general el proceso consiste en los siguientes pasos:

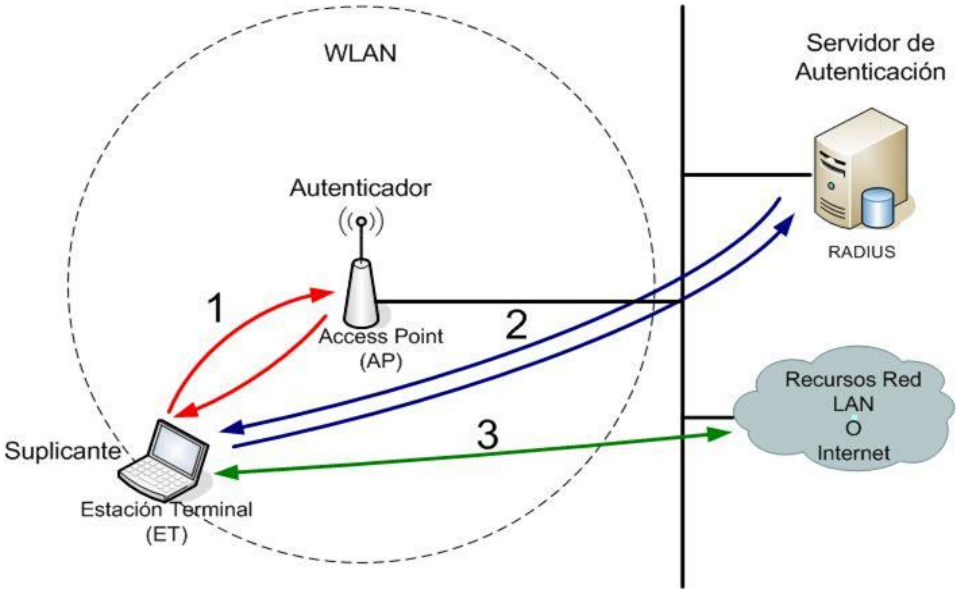

Figura 4.1. Control de acceso IEEE 802.1X

1. Cuando una Estación Terminal (ET) solicita acceso a los recursos de la Red LAN, El Acess Point (AP) pregunta por las credenciales de la ET. Antes de que la ET sea autenticada, sólo se le permite tráfico EAP; el puerto se mantiene "cerrado".

   La ET que solicita la autenticación, representa, o estrictamente hablando contiene el puerto *suplicante* que se ha definido anteriormente. El suplicante es el software o programa que se encarga de realizar y responder las peticiones. El AP contiene el autenticador 802.1X, el cual no necesariamente tiene que estar en el AP, puede ser un componente externo, como un Switch.

2. Una vez que se envían las credenciales, empieza el proceso de autenticación. El protocolo empleado entre el *suplicante* y el *autenticador* es EAP, en realidad EAPOL (EAP Over LAN), encapsulación de EAP en tramas Ethernet. El autenticador reencapsula los mensajes EAP en formato RADIUS y los reenvía al servidor de autenticación.

Durante la autenticación, el *autenticador* sólo reenvía los paquetes entre el *suplicante* y el servidor de autenticación. Cuando el proceso de autenticación termina, el servidor de autenticación envía un mensaje exitoso (o de rechazo si la autenticación falla). Si la autenticación fue exitosa el *autenticador* abre el puerto al *suplicante*.

3. Después de una autenticación exitosa, el *suplicante* tiene acceso a los recursos de la red LAN.

4.1.1. Autenticación basada en puertos

El autenticador opera con dos puertos, uno controlado y otro no. Ambos puertos son entidades lógicas o puertos virtuales y usan la misma conexión física a la LAN.

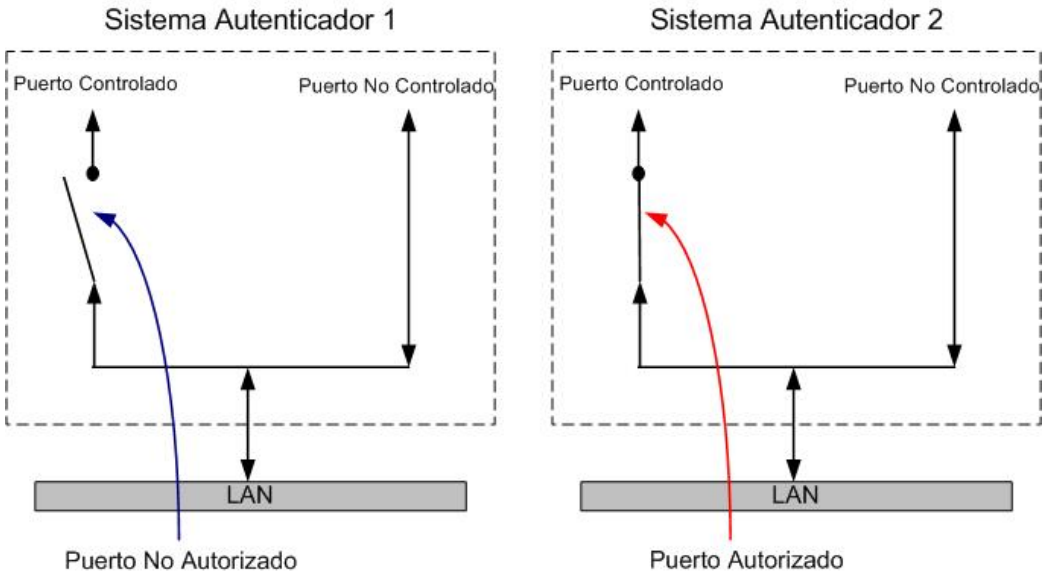

Figura 4.2. Estados de autorización del puerto controlado

Antes y durante la autenticación, el único puerto abierto es el no controlado. Este puerto sólo permite tráfico EAPOL. Si la autenticación resulta exitosa, se abre el puerto controlado y se obtiene el acceso a los recursos de red.

Existe una relación uno a uno entre un suplicante y un puerto, cada puerto tiene asociado un autenticador. Hay una relación muchos a uno entre los puertos y el servidor de autenticación. Un solo servidor de autenticación puede ser responsable de muchos puertos con sus respectivos autenticadores.

802.1X no fue diseñado con las redes inalámbricas en mente, pero el concepto de puertos físicos en una red Lan cableada se puede trasladar a conexiones inalámbricas. La necesidad principal de tener puertos seguros fue para proteger los puntos físicos de conexiones, localizadas en áreas no seguras. Por la naturaleza de las WLAN, físicamente no existen puntos específicos de conexión, en cualquier área donde alcance la señal se puede acceder a la red, siendo así 802.1X sumamente apropiado para las redes inalámbricas.

Los puertos 802.1X, en redes inalámbricas son las asociaciones entre las estaciones inalámbricas y el AP.

4.1.2. Arquitectura 802.1X y relación con los protocolos EAP y RADIUS

El autenticador realiza el proceso de autenticación sólo en la capa de enlace, no mantiene información de usuario. Todas las peticiones que entran las reenvía a un servidor de la autenticación, como un servidor RADIUS. El proceso de autenticación se lleva a cabo **lógicamente** entre el suplicante y el servidor de autenticación, el autenticador sólo actúa como intermediario o bridge.

La figura 4.3 (b) muestra la arquitectura lógica de los protocolos. Del suplicante al autenticador ("front end"), el protocolo es EAP over LANs (EAPOL). Del lado del "back end", EAP se lleva a cabo en paquetes RADIUS para el intercambio de mensajes (EAP over RADIUS). El suplicante realiza el intercambio EAP con el servidor RADIUS, aunque el puerto este desautorizado y no se requiere de una dirección IP.

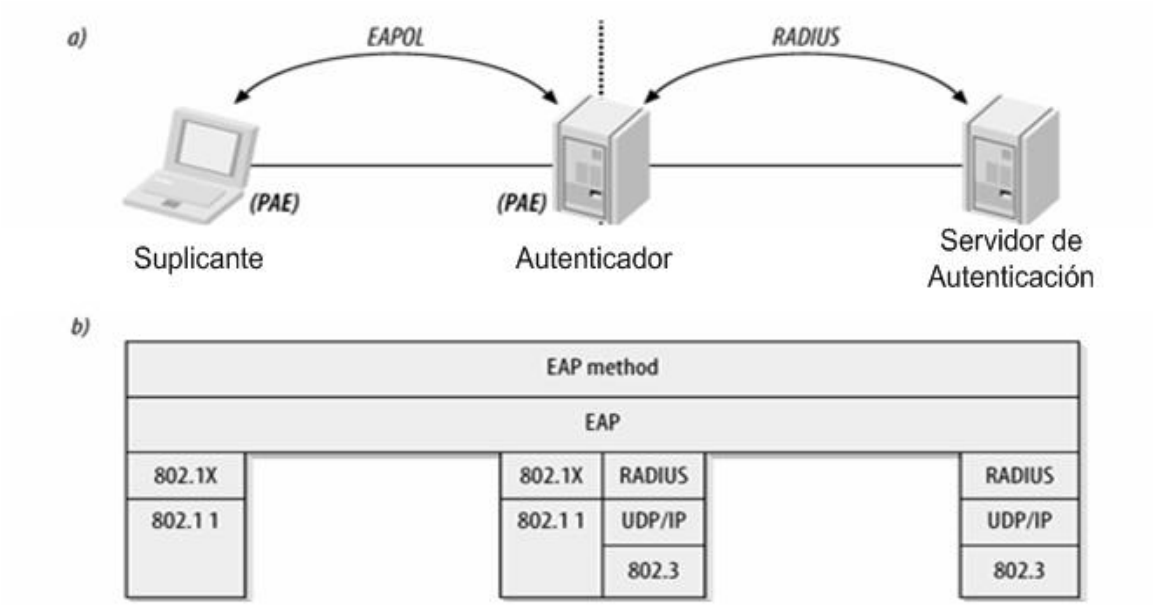

Figura 4.3. Arquitectura 802.1X

Una de las ventajas de usar RADIUS, es que soporta diferentes bases de datos de usuarios, además un servidor RADIUS puede servir como gateway para directorios LDAP, autenticación Unix como NIS o PAM, kerberos u otro servidor RADIUS.

4.2. EAP Extensible Authentication Protocol

Los protocolos EAP y RADIUS fueron desarrollados en el contexto de control de accesos remotos a través de las líneas telefónicas, por medio del protocolo PPP. Originalmente sólo existían dos mecanismos de autenticación, PAP y CHAP, ambos son muy simples, de manera que para proveer de métodos de autenticación más fuertes los miembros de la IETF diseñaron EAP.

El objetivo de EAP es permitir al suplicante demostrar su identidad al servidor de autenticación. Con la flexibilidad de EAP se consigue protocolos de autenticación arbitrarios y complejos entre el suplicante y el servidor de autenticación, conocidos como *métodos de autenticación EAP*.

EAP está definido en el RFC 3748. Fue diseñado para correr sobre cualquier nivel de enlace, y manejar diferentes métodos de autenticación, como se muestra en la figura 4.4.

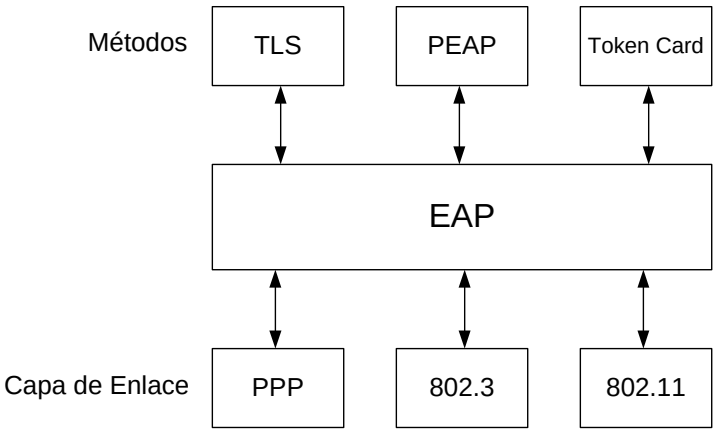

Figura 4.4. Arquitectura EAP

4.2.1. Formato de paquete EAP

Un paquete EAP consta de 4 campos como se aprecia en la figura 4.5, a continuación se describen cado uno de ellos:

Code: Este campo identifica el tipo de paquete EAP y se utiliza para interpretar el campo de datos (data) del paquete.

Existen 4 tipos de paquetes EAP:

- EAP-Request (01)
- EAP-Response (02)
- EAP-Success (03)
- EAP-Failure (04)

Identifier: Este campo se usa para identificar los mensajes de tipo *request* con su correspondiente mensaje de tipo *response*. En las retransmisiones se usa el mismo valor, pero se usa uno nuevo para nuevas transmisiones.

Length: Este campo contiene el tamaño total del paquete.

Data: Depende del tipo de paquete, es decir su interpretación depende del valor del campo *Code*.

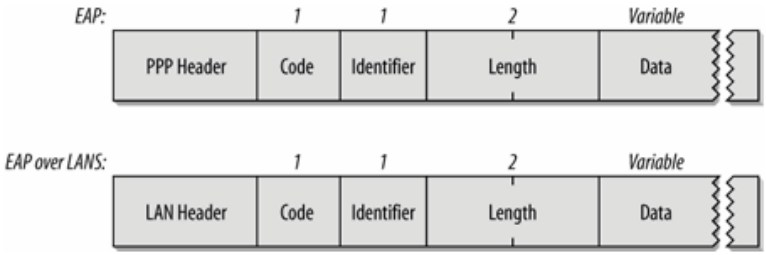

Figura 4.5. Formato de paquete EAP

4.2.1.1. Paquetes *EAP-Request* y *EAP-Response*

Figura 4.6. Paquetes: EAP-Request y EAP-Response

El campo *Code* se establece en 1 ó 2 para los mensajes de tipo request y response respectivamente, como se puede observar en la figura 4.6. El tipo de datos que transportan depende del valor que contiene el campo *Type.*

Type: Indica el tipo de mensaje Request o Respose.

Type-Data: Los datos son interpretados de acuerdo al valor del campo type.

Type (1) Identity: Los mensajes EAP-Request/Identity, EAP-Response/Identity se usan en la primera fase de autenticación EAP, o para realizar una autenticación sencilla, ya que como se verá más adelante, existen los llamados métodos de autenticación EAP.

Type (2) Notification: Se usa este tipo de paquetes para enviar y desplegar al usuario un mensaje ó notificación en modo texto.

Type (3) NAK : Un mensaje NAK se utiliza para comunicar que no existe soporte para un mecanismo de autenticación determinado.

Type (igual o mayor a 4) Métodos de autenticación EAP: EAP puede delegar la autenticación a otros protocolos más complejos, conocidos como métodos de autenticación EAP, cada uno de los cuales cuentan con sus propias técnicas para realizar la verificación de identidad. Dependiendo del método se asigna un valor igual o mayor 4 en el campo Type. En la tabla 1 se muestran algunos métodos de autenticación EAP más conocidos.

Type	Protocolo de autenticación	Descripción
4	MD5 Challenge	Autenticación Chap sobre EAP
6	GTC	Originalmente creados para ser utilizados con tarjeta token como RSA SecurID
13	EAP-TLS	Autenticación mutua con certificados digitales
21	TTLS	(Tunneled TLS)Protege métodos de autenticación con cifrado TLS
25	PEAP	(Protected EAP)Protege métodos EAP con cifrado TLS
18	EAP-SIM	Autenticación SIM a dispositivos móviles
29	MS-CHAP-V2	Autenticación Microsoft por cifrado de contraseña.

Tabla 1. Métodos de autenticación EAP más comunes

4.2.1.2. Paquetes EAP-Success y EAP-Failure

Una vez que finalizan los mensajes de intercambio de comprobación de identidad, el autenticador determina si la autenticación del usuario es exitosa (se le envía el mensaje EAP-Success) o si fue errónea (EAP-Failure). El campo *Code* se establece en 3 ó 4 para los mensajes de tipo success y failure respectivamente, como se muestra en la figura 4.7.

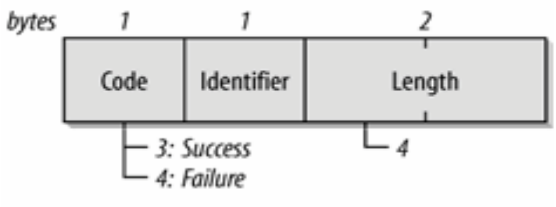

Figura 4.7. Paquetes: EAP-Success y EAP-Failure

4.2.1.3. Métodos de autenticación EAP

Una de las características importantes de EAP es que se trata solamente de un Framework, esto lo hace ser muy flexible y permite el diseño de nuevos métodos de autenticación conforme existen nuevas necesidades tal como se han presentado en las redes inalámbricas, resultando EAP ser fundamental en el desarrollo de nuevos protocolos.

Los primeros métodos EAP sólo buscaban conseguir un canal de comunicación con el servidor de autenticación; los métodos recientes sobre todo para redes inalámbricas, aparte del canal de comunicación buscan principalmente los siguientes tres objetivos:

- **Cifrado fuerte para la protección de las credenciales del usuario:** Todo tipo de datos que se transmite vía aérea tiene que ser protegida si es que estos se requieren que se mantengan seguro. La mayoría de los métodos EAP diseñados para redes inalámbricas emplean cifrado TLS para proporcionar protección a las credenciales de usuario.

- **Autenticación mutua:** La disminución de los precios de los APs ha propiciado los ataques de rogue AP que se utiliza para el robo de contraseñas, este hecho crea la necesidad de que además de la autenticación de usuarios, las estaciones inalámbricas deben ser capaces de validar la red a la que se conectan, es decir sí es realmente la que parece ser.

- **Generación de llave:** Un protocolo fuerte de seguridad requiere de llaves dinámicas y de algún mecanismo de cifrado para distribuirlas.

a) LEAP

El primer mecanismo de autenticación ampliamente utilizado fue propietario de Cisco, Lightweight EAP (LEAP). Usa dos veces MS-CHAP v1, primero autentica la red y después al usuario. Las llaves dinámicas son derivadas de los intercambios MS-CHAP. Fue una buena alternativa provisional, en lugar de manejar llaves estáticas con WEP, pero actualmente se le han encontrado varias debilidades y ya nos es recomendable su implementación.

b) EAP-TLS (Transport Layer Security)

El propósito de TLS es establecer un canal de comunicación confiable sobre redes inseguras, para evitar las escuchas espías.

TLS proporciona autenticación mutua a través del intercambio de certificados digitales. Un usuario tiene que enviar al servidor de autenticación un certificado para su validación, pero también el servidor tiene que proporcionar el suyo; al ser validado el certificado del servidor de una lista de autoridades certificadoras de confianza , el cliente puede estar seguro de que se está conectando a una red autorizada por una autoridad certificadora válida.

TLS es el primer método de autenticación para redes inalámbricas que cumple con los tres objetivos: canal seguro (cifrado), autenticación mutua y derivación de llaves para los protocolos de seguridad de la capa de enlace.

c) EAP-TTLS y EAP-PEAP

Implementar EAP-TLS requiere desplegar una infraestructura de PKI ó comprar un certificado para cada uno de los usuarios, a una autoridad certificadora. Esta solución no es viable por el momento para muchas organizaciones.

En lugar de manejar certificados para la autenticación de los usuarios, EAP-TTLS y EAP-PEAP maneja un *nombre de usuario* y una *contraseña*; pero sí se requiere un certificado para la autenticación del servidor con el que se consigue autenticar a la red.

Ambos protocolos trabajan de forma similar, en dos etapas:

> **Outer authentication:** En el primer paso establecen un túnel TLS usando rutinas similares a EAP-TLS, además con el certificado del servidor se realiza la autenticación de la red.

Inner authentication: En el segundo paso usan el túnel TLS para cifrar un protocolo de autenticación antiguos para la autenticación de los usuarios.

La ligera diferencia entre TTLS y PEAP es en la forma en que utilizan el túnel cifrado; TTLS lo usa para intercambiar directamente atributos (AVPs), PEAP en cambio lo usa para iniciar otro método EAP.

Métodos EAP no cifrados

Los primeros métodos de autenticación EAP no cifraban el canal de comunicación, los más comunes son los siguientes:

a) EAP-MD5 Challenge

El servidor envía un mensaje de invitación a la autenticación (*challenge message*), para que el usuario aplique el algoritmo MD5 y envíe su respuesta al servidor y éste al recibirlo recalcule el algoritmo para comparar si ambos valores son iguales. Si los valores obtenidos coinciden, el servidor manda un mensaje de aceptación, de lo contrario rechaza la autenticación. EAP-MD5 casi no es utilizado en redes inalámbricas por que no maneja llaves dinámicas.

b) EAP-GTC (Generic Token Card)

El servidor envía mensaje de texto como desafío (challenge) al usuario para la autenticación, quien responde con información generada por un Generic Token Card. El intercambio de credenciales se realiza en texto claro.

c) EAP-MSCHAP-V2

Microsoft CHAP version 2 (MS-CHAP-V2), inicialmente fue creado por Microsoft, está documentado en el RFC 2759. Es ampliamente utilizado como un protocolo “inner authentication”. EAP-MSCHAP-v2 puede ser utilizado por EAP-PEAP y EAP-TTLS

d) EAP-SIM

EAP SIM se define en el RFC 4186, permite la autenticación de usuario de telefonía celular por medio de la tarjeta SIM (Subscriber Identity Module).

4.3. Protocolo RADIUS

En esta sección se analiza como opera el protocolo RADIUS, su finalidad y sus características principales. Antes de iniciar se definen los siguientes términos relacionados con el tema:

4.3.1. Arquitectura AAA

AAA es un conjunto de especificaciones que define los servicios de Authentication, Authorization y Accounting en sistemas de redes IP. Esta arquitectura se basa en el uso de servidores AAA comunicándose mediante un protocolo estándar (no especificado), para realizar los servicios AAA.

Un servidor AAA debe ser capaz de recibir peticiones, examinar el contenido de dichas peticiones, determinar qué autorización se está pidiendo, recuperar las políticas que necesite de un repositorio, evaluar la petición y obtener la respuesta a la petición, o reenviar la petición a otro servidor AAA.

Como se mencionó anteriormente, el modelo AAA se enfoca en solucionar los tres aspectos de control de acceso de usuarios: Authentication, Authorization y Accounting. A continuación se describen en que consisten cada uno de éstos términos:

Authentication

Es el proceso de identificación de un usuario, es decir validar si realmente el usuario es quien dice ser, normalmente mediante un nombre de usuario y una contraseña, el conocimiento de la contraseña significa que el usuario es auténtico. Se basa en la idea de que cada usuario tendrá

una información única que le identifique o que le distinga de otros. También se pueden manejar certificados digitales, que evita el problema de la distribución de contraseñas.

Authorization

Es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido.

Accounting

Es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede así como los datos transferidos durante la sesión. Los datos registrados durante este proceso se utilizan con fines estadísticos, billing, análisis de tendencias, utilización de recursos, de planeamiento de capacidad y auditoría.

La arquitectura AAA busca proporcionar un diseño de cómo integrar las piezas AAA.

4.3.2. RADIUS (Remote Authentication Dial-In User Service)

RADIUS (Remote Access Dialin User Service) es el protocolo más utilizado en implementaciones AAA, es un protocolo de control de acceso ampliamente desplegado. Permite autenticar, autorizar y contabilizar (Accounting) usuarios que desean el acceso a un sistema o a un servidor central de red y puedan hacer uso de los servicios de red permitidos. Sin embargo no necesariamente con el protocolo RADIUS se pueden alcanzar los requerimientos de dicha arquitectura.

Originalmente RADIUS sólo era empleado en las conexiones remotas con ISPs, ya sea a través de módem, DSL o cablemódem; su uso se ha ampliado también en el control de acceso en redes locales Ethernet y en redes inalámbricas

El usuario que solicita la conexión envía sus credenciales que generalmente son un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de

Acceso a la Red) sobre el protocolo PPP o sobre la red local, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si el usuario es aceptado, el servidor autorizará el acceso a la red y le asignará los recursos de red permitidos.

Otra de las características importantes del protocolo RADIUS es la contabilidad (Accouting) que permite registrar sesiones, notificando cuando comienza y termina una conexión exitosa, información sobre los servicios de red asignados, cantidad de información de entrada y salida trasmitida, etc.; los datos se pueden utilizar con propósitos estadísticos.

RADIUS fue desarrollado originalmente por Livingston Enterprises, posteriormente se publicó como RFC 2138 y RFC 2139, actualmente obsoletos. Hoy en día existen muchos servidores RADIUS, tanto comerciales como de código abierto. Las funcionalidades varían entre uno y otro, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP y base de datos. Generalmente se utiliza SNMP para monitorear remotamente el servicio. Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo.

4.3.2.1. Estándares

El protocolo **RADIUS** actualmente está definido en los RFC 2865 (autenticación y autorización) y RFC 2866 (accounting).

Los RFCs correspondientes establecen los puertos UDP 1812 para las actividades de autenticación/autorización y 1813 para los procesos de accounting.

4.3.2.2. Características claves sobre el diseño de RADIUS

Algunas de las características más importantes del protocolo RADIUS son las siguientes:

a) Modelo cliente/servidor

Un NAS (Network Access Server, 'Servidor de Acceso de red') funciona como cliente de RADIUS; en IEEE 802.11X el NAS viene siendo el autenticador. El cliente es el responsable de reenviar la información del usuario a los servidores RADIUS designados, así también del reenvío a los usuarios las respuestas del servidor.

Los servidores RADIUS, en IEEE 802.11X son el servidor de autenticación, son los responsables de recibir las peticiones de conexión del usuario, de autenticar y de regresar toda la información de configuración necesaria al cliente para entregar los servicios autorizados al usuario.

NAS/Cliente → Autenticador
Servidor RADIUS → Servidor de Autenticación

Un servidor RADIUS puede actuar como cliente Proxy de otros servidores RADIUS o de otros tipos de servidores de la autenticación.

b) Seguridad en la comunicación

Las transacciones entre el cliente (NAS) y el servidor RADIUS son autenticados con el uso de un secreto compartido, que nunca se envía sobre la red. Además, cualquier contraseña de usuario se envía cifrada, para evitar la posibilidad de que alguien, al espiar la comunicación en una red insegura pueda determinar la contraseña de un usuario.

c) Mecanismos de autenticación flexibles

El servidor RADIUS puede soportar una variedad de métodos para autenticar a un usuario. La autenticación se puede realizar con PPP PAP, CHAP, UNIX login o con otros mecanismos de la autenticación.

d) Protocolo extensible

Todas las transacciones se realizan por medio de la tercia *Atributo-Longitud-Valor* de tamaños variables. Se pueden agregar nuevos valores de atributos sin alterar la implementación existente del protocolo.

e) Basado en el protocolo no orientado a conexión UDP

RADIUS emplea UDP por requerimientos de operación, además RADIUS tiene propiedades inherentes que son características de UDP: Si las peticiones al servidor primario de autenticación fallan deben ser redirigidas a un servidor secundario.

UDP reduce el tiempo de autenticación de los usuarios, que lo único que quieren es tener acceso a los recursos de red en el menor tiempo posible. Una de las propiedades de RADIUS es el de no guardar el estado de la conexiones, por lo que resulta natural emplear UDP, que también tiene esta característica.

UDP permite que RADIUS pueda servir múltiples peticiones a la vez, y cada sesión tiene todas las capacidades de comunicación.

La única desventaja al usar UDP es que se tiene que desarrollar y manejar contadores de tiempo para la retransmisión, es una desventaja mínima comparada con los beneficios antes mencionados.

f) AVPs (pares de atributo/valor)

RADIUS proporciona más de 50 AVPs con la posibilidad de que los fabricantes puedan crear pares específicos propietarios.

4.3.2.3. Formato de paquetes

RADIUS utiliza un formato de paquetes característico, que se conforma de cinco secciones (véase figura 4.8), que a continuación se describen.

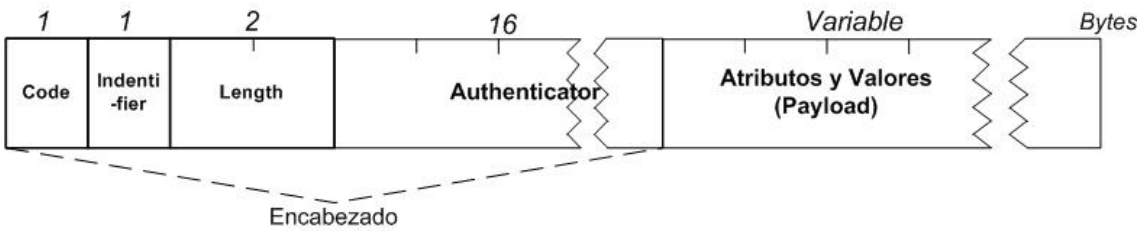

Figura 4.8. Estructura de un paquete de datos RADIUS

Code: El campo *code* permite distinguir el tipo de paquete RADIUS que está siendo transmitido, la tabla 2 muestra los tipos de paquetes que hay.

Tipos de paquetes válidos:

Código	**Nombre**	**Actividad**
1	Access-Request	Autenticación/Autorización
2	Access-Accept	Autenticación/Autorización
3	Access-Reject	Autenticación/Autorización
4	Accounting-Request	Accounting
5	Accounting-Response	Accounting
11	Access-Challenge	Autenticación/Autorización
12	Status-Server	Experimental
13	Status-Client	Experimental
255		Reservado

Tabla 2. Tipos de paquetes y sus códigos correspondientes

Identifier: Este campo sirve para ligar las peticiones con las correspondientes respuestas subsecuentes. El servidor RADIUS puede detectar una petición duplicada si el paquete del cliente tiene el mismo puerto, la misma dirección IP y el mismo identificador dentro de un periodo corto de tiempo.

Length: Este campo indica el tamaño total del paquete, es decir la suma de los tamaños de los campos: *Code, Identifier, length, Authenticator y Atributo*.

Authenticator: Este campo permite examinar y verificar la integridad del cuerpo (payload) del mensaje.

Tipos de paquetes

El tipo de paquete es determinado por el campo Code. Hay cuatro tipos de paquetes para las fases de Autenticación y Autorización:

- Access-Request
- Access-Accept
- Access-Reject
- Access-Challenge

Y dos tipos de paquetes para las transacciones de Accounting:

- Accounting-Request
- Accounting-Response

Access-Request

El paquete *Access-Request* se utiliza para solicitar los servicios de red. El NAS/cliente envía un paquete de este tipo al servidor RADIUS con una lista de los servicios solicitados. El aspecto importante en la transmisión es el campo *Code* que debe tener un valor de 1, el único valor válido para los paquetes de petición, la figura 4.9 muestra un paquete típico tipo Access-Request.

El payload del paquete Access-Request debe incluir el atributo username para identificar a la persona que intenta acceder al recurso de la red. También se debe incluir ya sea el atributo NAS-IP-Address o NAS-Identifier o ambos. Así mismo debe contener el atributo User-Password o CHAP-Password, pero no ambos. La contraseña de usuario debe ser hasheado con MD5.

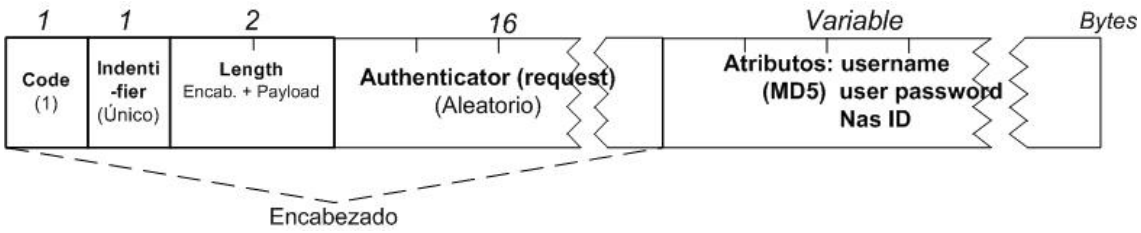

Figura 4.9. Un paquete típico Access-Request

Access-Accept

Los paquetes *Access-Accept* son enviados por el servidor RADIUS al NAS para notificar la aceptación de conexión solicitada por el usuario y proporciona la información específica de configuración necesaria de los servicios autorizados al usuario. La figura 4.10 ilustra un paquete típico tipo Access-Accept.

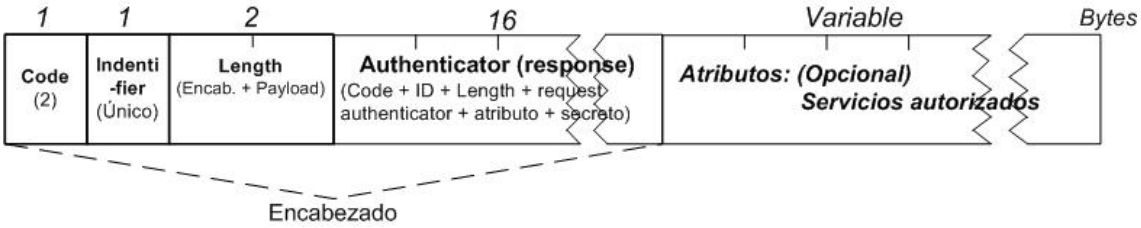

Figura 4.10. Un paquete típico Access-Accept

Access-Reject

El servidor RADIUS responde al NAS con paquetes de tipo ***access-reject***, el campo code establecido a 3 sí el usuario no está permitido o no tiene privilegios para acceder a los servicios solicitados. Puede incluir uno o más mensajes de texto a través del atributo reply-message para que el NAS le muestre al usuario, además puede hacer uso de los atributos proxy-message, únicamente tiene permitido éstos dos. Pueden aparecer ambos múltiples veces (véase figura 4.11)

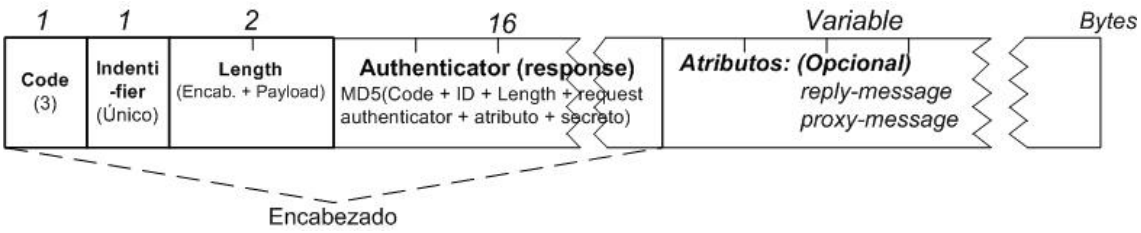

Figura 4.11. Un paquete típico Access-Reject

Access-Challenge

Si el servidor RADIUS desea más información del usuario, generalmente con la finalidad de robustecer los procesos de autenticación, envía al NAS un desafío requiriendo una respuesta, utilizando paquetes con el campo code establecido a 11, paquetes de tipo Access-Challenge.

El cliente (NAS), una vez que recibe un paquete de tipo Access-Challenge, responde con un nuevo paquete Access-Request con la información requerida por el servidor incluida.

Puede incluir uno o más mensajes de texto a través del atributo reply-message, puede incluir también los atributos: State, Vendor-Specific, Idle-Timeout, Session-Timeout and Proxy-State, en la figura 4.12 se presenta un paquete característico tipo Access-Challenge.

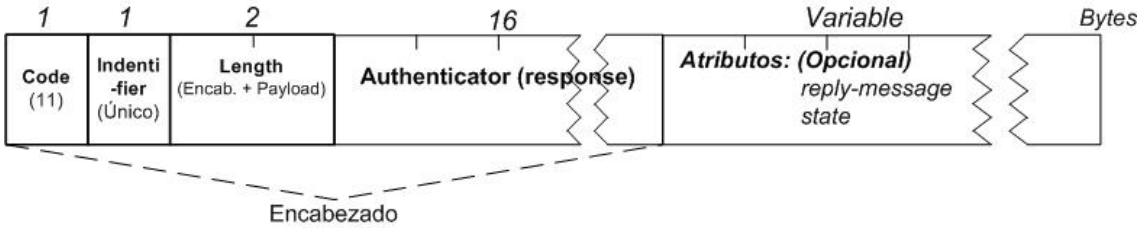

Figura 4.12. Un paquete típico Access- Challenge

Accounting-Request

Cuando el NAS acepta una conexión y cuando ésta termina, envía al servidor RADIUS un paquete con el campo *code* establecido a 4 que corresponde a un paquete de tipo *Accounting-Request.* Este paquete incluye información acerca del servicio entregado, el usuario a quien se le

proporcionó, datos estadísticos de uso como tiempo de conexión, cantidad de datos transferidos, lugar de conexión, entre otros datos.

Accounting-Response

Los paquetes *Accounting-Response* son enviados por el servidor RADIUS al cliente como reconocimiento cuando se recibe y registra con éxito una solicitud de contabilidad *(Accounting-Request)*, y no responde nada si falla.

4.3.2.4. Atributos y valores

Las transacciones RADIUS consisten en el intercambio de pares AVPs (Attribute-Values Pairs, 'Pares Atributo-Valor') entre el NAS/cliente y servidor; es decir, de atributos con sus respectivos valores.

Los atributos contienen información útil relacionada con los procesos de authentication, authorization y accounting, cada mensaje RADIUS puede llevar uno o más atributos.

Los atributos se trasmiten dentro de los paquetes RADIUS con un formato específico, como se indica en la figura 4.13:

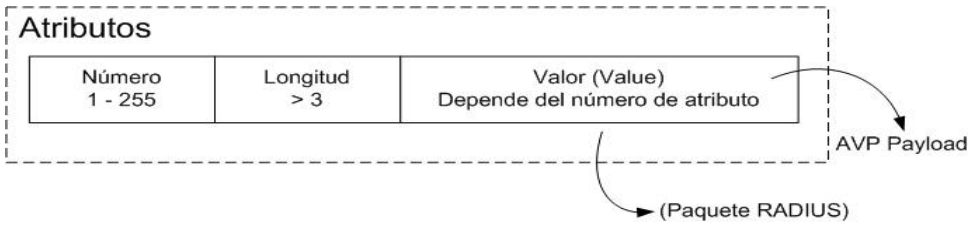

Figura 4.13. Formato estándar de los AVPs

Number: Este campo indica el tipo de atributo. El nombre de atributo no se incluye dentro del paquete, únicamente este número. Los números pueden ir de 1 a 255, el atributo número 26 sirve como gateway para que diferentes vendedores puedan incluir sus propios atributos.

***Length*:** Este campo contiene el tamaño del atributo, incluyendo la suma de los tres campos que lo conforman (tipo, longitud y valor)

Value: Contiene la propiedad o característica del atributo. Este campo es requerido, aunque el valor sea nulo, su tamaño es variable, depende de la naturaleza inherente del atributo.

Tipos de Datos

Los valores de los atributos pueden contener los siguientes tipos de datos:

Entero (INT). Datos que son representados por números enteros

Enumeración. (ENUM). Son datos de tipo entero relacionados con algún significado

Dirección IP (IPADDR). Es un número de 32 bits, diseñado para representar correctamente direcciones IP.

Cadena (STRING). Datos representados por cadena de caracteres imprimibles y leíbles.

Fecha (DATE). Es un número entero de 32 bits, representa el tiempo transcurrido en segundos desde el 01 de enero de 1972.

Binario (BINARY). Datos representados por 0 y 1.

Hay muchos atributos, la tabla 3 muestra los más comunes.

Tipo de Atributo	Nombre	Descripción
1	User-Name	Contiene el Nombre del usuario
2	User-Password	Contiene la contraseña del usuario.
3	CHAP-Password	Se utiliza en un proceso de autenticación CHAP
4	NAS-IP-Address	La dirección IP del NAS (Cliente del servidor RADIUS)
8	Framed-IP-Address	Dirección IP que le será asignado al usuario.
18	Reply Message	Se utiliza para enviar un mensaje de texto al usuario.
26	Vendor-Specific	Este atributo permite a los fabricantes implementar y comunicar funcionalidades especiales en sus equipos.
27	Session-Timeout	Periodo de tiempo en segundos, antes de que termine la sesión de un usuario.
28	Idle-Timeout	Periodo de inactividad de un usuario antes de ser desconectado.
30	Called-Station-ID	La dirección MAC del NAS, por el cual el un usuario obtiene conexión.(En redes inalámbricas).
31	Calling-Station-ID	Dirección MAC del usuario.

Tabla 3. Atributos RADIUS más comunes

Atributos VSAs (Vendor-specific attributes, 'Atributos específicos del fabricante').

El protocolo RADIUS permite que los fabricantes puedan implementar sus propios atributos conocidos como VSAs. Los VSAs son encapsulados dentro del atributo estándar 26, llamado `Vendor-Specific,` como se observa en la figura 4.14.

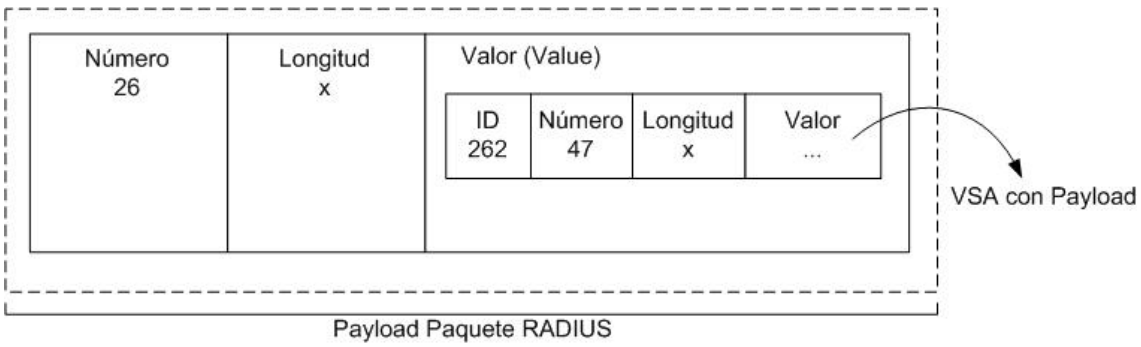

Figura 4.14. Encapsulado de un VSA dentro del atributo estándar 26

Vendor ID. Esta sección del VSA representa el identificador del desarrollador/diseñador/fabricante.

Vendor Type. Lo utiliza el fabricante para identificar con un número del 1-255 a los atributos que implementa.

Lenght. Contiene el tamaño completo del VSA. El valor mínimo es siete.

Value. Este campo es necesario que al menos sea de un Byte y contiene los datos específicos del atributo mismo.

4.3.2.5. Diccionarios

Los servidores RADIUS deben tener una forma de saber que número le corresponde a cada atributo y el tipo de dato que usa, tanto de los atributos estándar como de los VSAs. Estas definiciones se realizan en los archivos conocidos como diccionarios. La figura 4.15 muestra un ejemplo de un diccionario del fabricante Aruba

```
VENDOR          Aruba                       14823
BEGIN-VENDOR    Aruba

ATTRIBUTE       Aruba-User-Role                     1       string
ATTRIBUTE       Aruba-User-Vlan                     2       integer
ATTRIBUTE       Aruba-Priv-Admin-User               3       integer
ATTRIBUTE       Aruba-Admin-Role                    4       string
ATTRIBUTE       Aruba-Essid-Name                    5       string
ATTRIBUTE       Aruba-Location-Id                   6       string

END-VENDOR      Aruba
```

Figura 4.15. Diccionario del fabricante Aruba.

4.3.2.6. Realms

El servidor RADIUS puede identificar usuarios provenientes de diferentes organizaciones, utilizando nombres “realms”.

Los nombres realms pueden utilizarse como prefijos, es decir se colocan antes que el nombre de usuario separados comúnmente por alguno de los caracteres / o \ configurables.

Ejemplo:

UNAM\jperez

Otra forma de usar los nombres realms es como sufijo, es decir después del nombre de usuario separados por el carácter @.
Ejemplo:

rlopez@UNAM

4.3.2.7. Accounting

El Accounting consiste en recolectar información sobre actividades de los usuarios en la red, qué usuarios accedieron a la red, cuándo lo hicieron, dónde se conectaron, qué servicios se le concedieron, etc.

La información que genera el accounting también puede ser utilizada para propósitos estadísticos, por ejemplo saber cuantas conexiones se realizan en un tiempo determinado, la cantidad de datos trasmitidos, áreas con más accesos, tiempo de promedio de conexión, etc. Información de gran utilidad para determinar el nivel de los recursos utilizados y contar con elementos para decidir en qué momento los dispositivos de red deban ser escalados para cubrir con la demanda de recursos.

RADIUS cumple con todos los requerimientos de accounting del modelo AAA.

Formato de paquetes

Es el mismo formato descrito en la sección 4.3.1.3, obviamente el campo *code* sólo podría contener los dos tipos de paquetes para las transacciones de Accounting.

- Accounting-Request
- Accounting-Response

La tabla 4 enumera algunos de los atributos más comunes que se utilizan en los procesos de accounting.

Tipo	Nombre	Descripción
	Acct-Status-Type	Este atributo especifica si un usuario inicia o detiene una sesión
	Acct-Delay-Time	Especifica el periodo de tiempo en segundos en el que el cliente o NAS ha estado intentando entregar el paquete al servidor
	Acct-Input-Octets	Indica el número de octetos recibidos durante la sesión, se encuentra solamente en paquetes tipo Accounting-Request con el atributo Acct-Status-Type establecido en stop
	Acct-Session-ID	Este atributo permite identificar a una sesión de forma
	Acct-Session-Time	Indica el tiempo en segundos durante el cual el usuario estuvo conectado, esto significa que sólo se encuentra cuando el atributo Acct-Status-Type está establecido en stop
	Acct-Input-Packets	Indica el número de paquetes recibidos durante la sesión, se encuentra solamente en paquetes tipo Accounting-Request con el atributo Acct-Status-Type establecido en stop
	Acct-Output-Packets	Indica el número de paquetes enviados durante la sesión, se encuentra solamente en paquetes tipo Accounting-Request con el atributo Acct-Status-Type establecido en stop
	Acct-Terminate-Cause	Indica el motivo por el cual finalizó una conexión.

Tabla 4. Atributos RADIUS más comunes para el accounting.

4.4. EAPOL (EAP Over LAN)

EAP no es totalmente un protocolo IP, como se mencionó anteriormente fue utilizado originalmente en los accesos vía MODEM. IEEE 802.1X implementa EAP over LAN para el intercambio de tramas entre el suplicante y el autenticador que encapsula los mensajes EAP.

Los componentes de la trama son:

MAC header: En la figura 4.16 se muestra el formato EAPOL para 802.11 y 802.3 en donde se observa que los campos MAC difieren un poco.

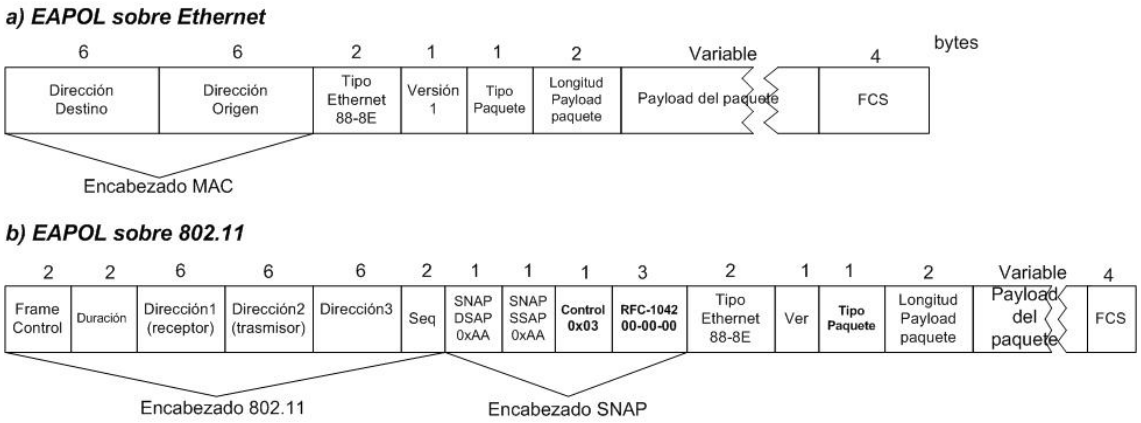

Figura 4.16. Formato de trama EAPOL

Ethernet Type: Como cualquier otra trama ethernet, contiene código que indica el tipo de trama, es este caso el 88-8E corresponde a una trama EAPOL.

Versión: Indica la versión de 802.1X, existen las versiones 1 y 2.

Packet Type: EAPOL es una extensión de EAP, además de los tipos de paquetes que existen, EAPOL agrega otros más, para adaptar EAP en el ambiente LAN (véase tabla 5).

Tipo	Nombre	Descripción
0000 0000	EAP-Packet	Contiene un paquete EAP
0000 0001	EAPOL-Start	Un suplicante puede enviar una trama EAPOL-Start, sin esperar por un desafío del autenticador, quien responderá con una trama EAP-Request/Identity
0000 0010	EAPOL-Logoff	El suplicante envía una trama EAPOL-Logoff para reestablecer el puerto en estado no autorizado, es decir termina la conexión.
0000 0011	EAPOL-Key	Se utiliza para el intercambio de información de la llave de cifrado.
0000 0100	EAPOL-Encapsulated-ASF-Alert	Se utiliza para manejar alertas, como traps SNMP, WPA/RSN no lo usa.

Tabla 5 Paquetes EAPOL para adaptar EAP en el ambiente LAN.

Packet Body Length: Indica el tamaño del cuerpo del paquete en bytes. Se establece en 0 cuando no existe ningún cuerpo del paquete.

Packet Body: Está presente en todas la tramas EAPOL, excepto en las tramas EAPOL-Start y EAPOL-Logoff. Puede contener un paquete EAP en EAP-Packet, un descriptor de llave en EAPOL-Key o una alerta en EAPOL-Encapsulated-ASF-Alert.

4.5. EAP sobre RADIUS

La autenticación EAP en paquetes RADIUS se especifica en el RFC 2869. Para conseguirlo, RADIUS se ha extendido a fin de permitir que el NAS pueda retransmitir mensajes EAP al servidor RADIUS. El NAS actúa como intermediario durante el proceso de autenticación, simplemente retransmitiendo los mensajes EAP entre el suplicante y el servidor hasta completar el proceso. En la siguiente sección, se muestra cómo se realiza la encapsulación.

4.5.1. 802.1X EN WLANs

802.1X proporciona una estructura o framework para la autenticación de usuarios en cualquier red LAN, incluyendo WLAN. Los puertos 802.1X, en redes inalámbricas es una asociación entre una estación inalámbrica y su access point. Si un intento de asociación resulta exitoso, 802.1X considerada activo el nivel de enlace de la comunicación. Una vez asociada, una estación puede iniciar el intercambio de tramas 802.1X para entonces realizar el proceso de autenticación.

La forma en que trabaja EAP y EAP sobre RADIUS encaja perfectamente en la arquitectura WPA/RSN.

WPA/RSN usa un atributo RADIUS de tipo Vendor-Specific llamado MS-MPPE-Recv-Key, implementado por Microsoft para enviar información de la llave master del servidor RADIUS al Autenticador, para el cifrado de paquetes en la comunicación entre el suplicante y el autenticador.

Usuarios remotos → Usuarios inalámbricos
NAS → Acces Point ó Switch controller
Servidor RADIUS → Servidor de Autenticación

Ejemplo de intercambio 802.1X en 802.11.

En la figura 4.17 se presenta un ejemplo de intercambio 802.1X en 802.11, se asume el uso de un servidor RADIUS como servidor de autenticación, por lo que se muestra la traducción que realiza el autenticador de EAP a RADIUS.

En este ejemplo también se muestra el uso de la trama EAPOL-Key que distribuye la llave para los protocolos de seguridad de la capa de enlace.

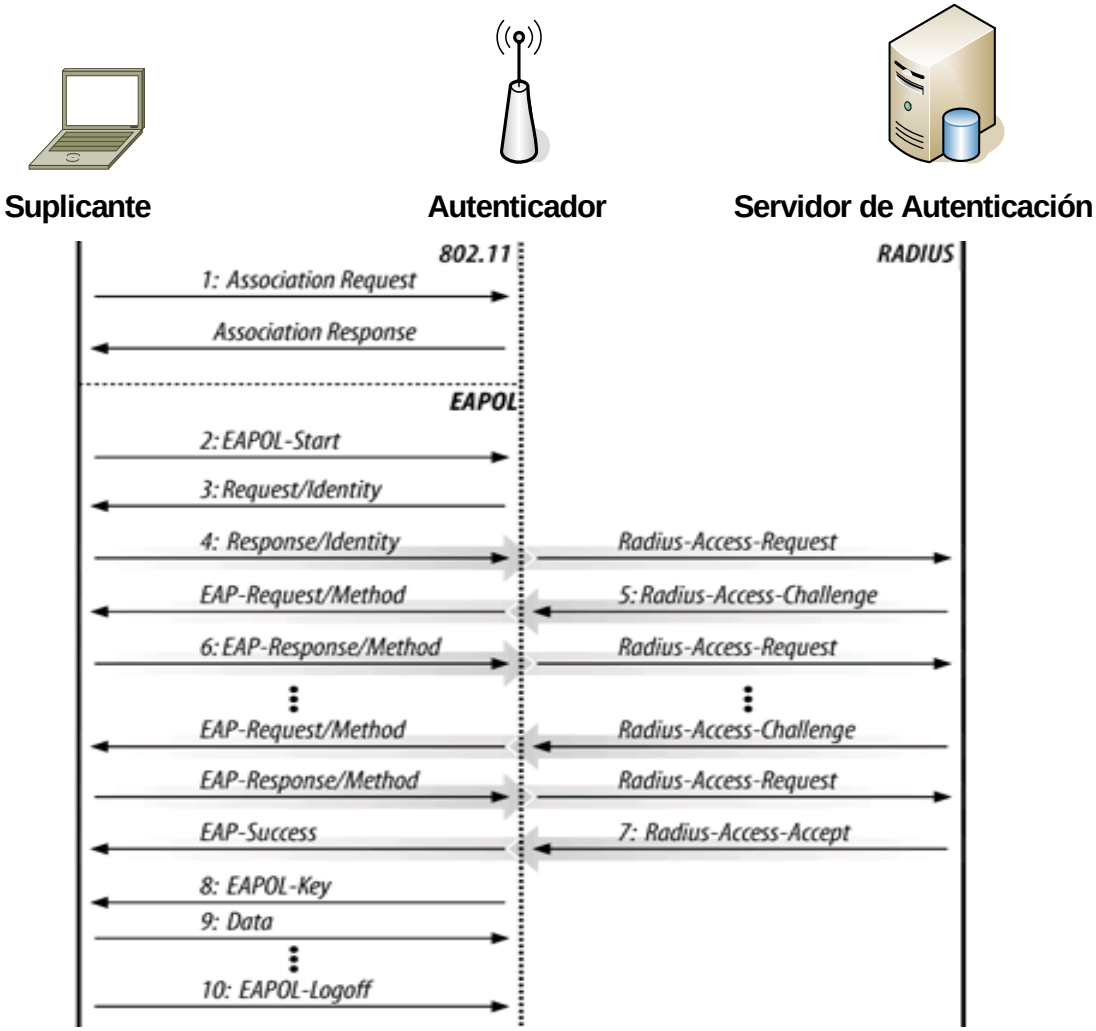

Figura 4.17. Intercambio 802.1X sobre 802.11

1. El suplicante se asocia a la red 802.11.

2. El suplicante inicia el intercambio 802.1X enviando un mensaje EAPOL-Start.

3. El autenticador (AP) emite una trama EAP-Request/Identity. Pueden enviarse tramas Request/Identity sin tener un EAPOL-Start. Tramas Request/Identity no solicitadas indican al suplicante que se requiere autenticación 802.1X.

4. El suplicante responde con una trama EAP-Response, que es reenviado al servidor RADIUS por el autenticador como un paquete Radius-Acess-Request.

5. El servidor RADIUS determina el tipo de autenticación requerida, y envía al AP un EAP-Request de acuerdo al método. EAP-Request se encapsula en un paquete RADIUS Access-Challenge. El AP reenvia el EAP-Request al suplicante. Los mensajes EAP-Request a menudo se denota como EAP-Request/Method donde Método se refiere al método EAP que se está usando. por ejemplo si se usa PEAP, el paquete de retorno se escribiría como EAP-Request/PEAP

6. El suplicante obtiene la respuesta del usuario y envía un EAP-Response de regreso. El autenticador traduce la respuesta en RADIUS Access-Request con la respuesta del desafio en el campo de datos. Los pasos cinco y seis se repiten tantas veces como sea necesario para completar la autenticación.

7. El servidor RADIUS usa paquetes Access-Accept para permitir el acceso, que el autenticador lo traduce en una trama EAP-Succes y autoriza el puerto.

8. Inmediatamente después de que se consigue una autenticación exitosa, el AP distribuye las llaves al suplicante usando mensajes EAPOL-Key.

9. Una vez que se instalan las llaves en el suplicante, puede empezar la transferencia de datos a la red. Es muy común que en este punto se realice la configuración de DHCP.

Cuando el suplicante termina el acceso a la red se envía un mensaje EAPOL-Logoff para regresar el puerto en estado desautorizado.

CAPÍTULO 5

IMPLEMENTACIONES DE SEGURIDAD 802.11i/WPA CON SOFTWARE LIBRE

5. IMPLEMENTACIONES DE SEGURIDAD 802.11i/WPA CON SOFTWARE LIBRE

En esta sección se presentan los elementos y procedimientos necesarios para obtener distintas soluciones de seguridad en redes inalámbricas de forma práctica, principalmente en la obtención de los diferentes mecanismos de autenticación.

Se muestran soluciones con configuraciones básicas en el servidor RADIUS para su implementación en redes pequeñas sin necesidad de entrar en mayores detalles en las configuraciones, y en el siguiente capítulo se presentan configuraciones avanzadas a través de un caso práctico.

WPA /WPA2

Para implementar WPA o WPA2 en una infraestructura AAA, es indistinto uno u otro, los cambios se realizan en el autenticador y en los suplicantes, pero ninguno en el servidor RADIUS. Es importante recordar que la mayor diferencia entre estos dos protocolos consiste en el algoritmo de cifrado. (Véase tabla 6)

Protocolo de seguridad	Algoritmo de cifrado
WPA	TKIP
WPA2	AES

Tabla 6. Protocolos de seguridad

Un aspecto a considerar para el despliegue de una red inalámbrica con seguridad basada en 802.11i/WPA son los equipos inalámbricos. Si los equipos van a ser nuevos, no habrá mucho problema, sólo será necesario evaluar que el equipo soporte 802.11i RSN que es totalmente compatible con WPA TSN. Para equipos adquiridos con anterioridad y que todavía están en operación, será forzosamente necesaria la actualización por software para que soporten WPA. La actualización a 802.11i RSN sólo es posible con el cambio del hardware.

A manera de ejemplo se presenta la configuración WPA en un AP Avaya, el procedimiento para obtener WPA2 es muy similar.

Alternativas de mecanismos de autenticación: EAP-TLS, EAP-PEAP o EAP-TTLS

En este capítulo se presentan los cambios necesarios en la configuración del servidor RADIUS para conseguir cualquiera de los métodos de autenticación más importantes en WLAN: EAP-TLS, EAP-PEAP y EAP-TTLS, además de las configuraciones necesarias en los suplicantes para cada uno de los distintos métodos de autenticación mencionados, la tabla 7 resume las soluciones de seguridad que se logran.

Para el autenticador, ya sea un AP o un switch controlador, la elección del mecanismo de autenticación es transparente, como se sabe, éste actúa como intermediario y solamente reenvía los paquetes entre el suplicante (equipo del usuario móvil) y el servidor de autenticación.

Protocolo de seguridad / **Método De Autenticación**	**WPA o TSN Cifrado: TKIP**	**802.11i o WPA2 Cifrado: AES**
TLS	WPA/TLS	WPA2/TLS
PEAP	WPA/PEAP	WPA2/PEAP
TTLS	WPA/TTLS	WPA2/TTLS

Tabla 7 Soluciones de seguridad en las WLAN

Escenario

En el caso del autenticador se utiliza un AP de la marca Avaya, AP-8, con soporte de seguridad WEP únicamente; se tuvo que actualizar para conseguir las funcionalidades de seguridad WPA, como ya se ha mencionado la ratificación del estándar de seguridad 802.11i o WPA2 se presentó a fines de junio de 2004, pero muchos fabricantes no quisieron esperar y a mediados del 2003 incluyeron en sus equipos el protocolo WPA basado en el Draft 3 de 802.11i, la mayoría de los fabricantes Wi-Fi tienen disponibles versiones de software para adquirir las facilidades de WPA en sus equipos que salieron al mercado antes del surgimiento de las especificaciones WPA.

Cualquier AP de la marca que sea con soporte “WPA/802.11i empresarial” debería funcionar en este escenario. Algunos de los fabricantes que se probaron con esta infraestructura son: Cisco, Foundry, Enterasys, Colubris y funcionaron perfectamente con el servidor de autenticación RADIUS (FreeRADIUS).

Es importante recordar también que los equipos inalámbricos pueden emplear WPA de dos formas distintas:

1. WPA PSK
2. WPA Empresarial

La forma PSK no requiere de la instalación de un servidor de autenticación para centralizar la administración de los usuarios, por lo que evidentemente el tipo de WPA al que se refiere el documento es el segundo y simplemente se menciona como ***WPA*** sin el término ***Empresarial***.

La figura 5.1 muestra los componentes principales para presentar las soluciones de seguridad en una WLAN antes mencionadas.

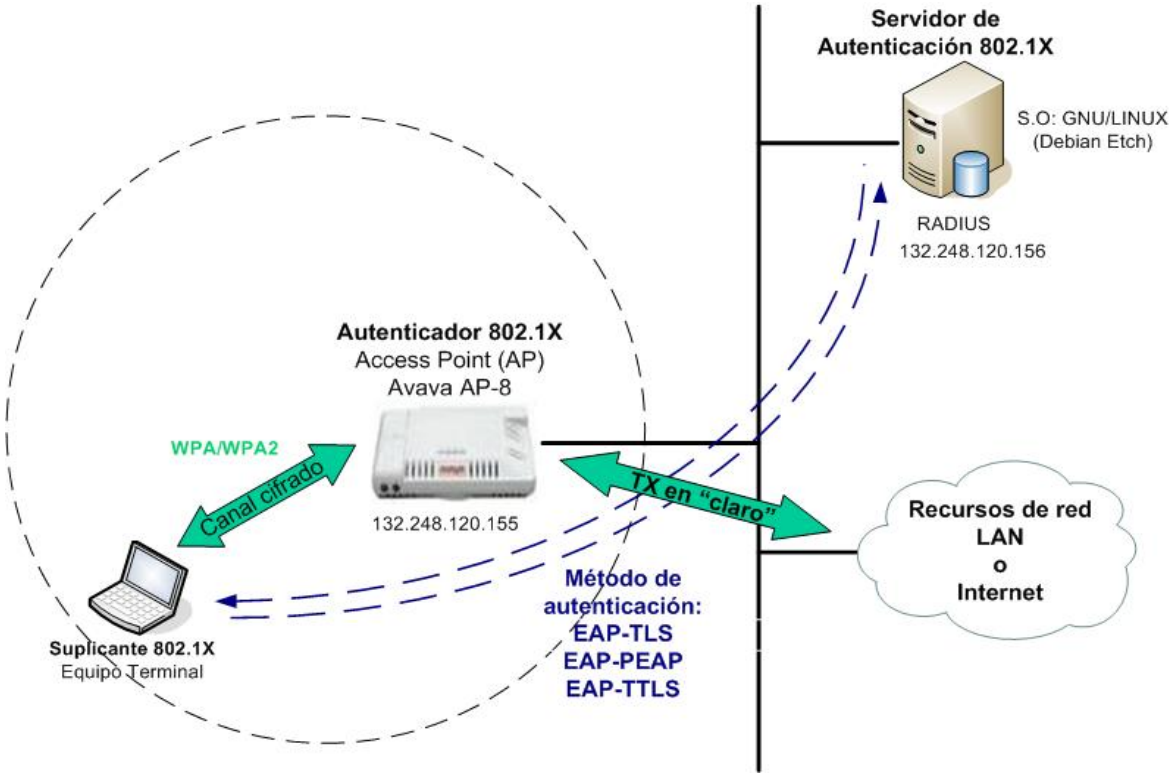

Figura 5.1. Escenario: implementación WPA/802.11i

5.1. Elementos necesarios para la solución 802.11i/WPA

Antes de llevar a cabo la implementación del sistema de seguridad, es importante identificar los elementos requeridos. Enseguida se describen dichas partes.

5.1.1. RADIUS como soporte 802.1X

Desplegar una infraestructura WPA/WPA2 Corporativo (específicamente la integración de un servidor de autenticación) no es tarea fácil. Sin embargo, el costo y esfuerzo se verá recompensado una vez que este se encuentre en operación.

El primer paso a seguir, es la elección del servidor de autenticación, en general se sugiere un servidor RADIUS. Se puede obtener un servidor RADIUS de diversas formas. Existen aplicaciones comerciales que trabajan en diferentes sistemas operativos. Hay también disponibles software libre para sistemas basados en Unix/Linux.

Las implementaciones libres de servidor RADIUS más conocidos son: FreeRADIUS, BSDRadius, GNURadius, JRadius, OpenRADIUS, entre otras. De todas ellas, la única que soporta, hasta el momento, el tipo de autenticación EAP (EAP-MD5, EAP-SIM, EAP-TLS, EAP-TTLS, EAP-PEAP y Cisco LEAP) es FreeRADIUS. Como WPA/WPA2 requiere método de autenticación EAP, se elige FreeRADIUS para la implementación en este proyecto.

5.1.2. Uso de una PKI (infraestructura de llave pública) o aplicaciones OpenSSL

Para el uso del método de autenticación EAP-TLS se necesita un certificado para el servidor y para cada uno de los usuarios de la red inalámbrica. Para aprovechar este mecanismo de autenticación es conveniente contar con una infraestructura de PKI para la emisión y manejo de certificados de llaves públicas, basados en el estándar X.509.

Establecer una PKI no es una tarea sencilla, se requiere todo un proceso y una planeación para su diseño, el alcance de este trabajo no contempla su implementación, en su lugar se usarán las herramientas de OpenSSL (Open Secure Socket Layer) para generar certificados, que permitirán

alcanzar el objetivo del uso de EAP-TLS; las librerías de OpenSSL permiten generar certificados *"auto firmados"* (self-signed), en lugar de solicitar la firma a una autoridad certificadora. El uso de las herramientas OpenSSL para manejar la autenticación EAP-TLS es recomendable sólo para redes pequeñas o caseras, para redes con cientos de usuarios no se tendría un control en la emisión, revocación y manejo de los certificados.

En los métodos de autenticación EAP-PEAP y EAP-TTLS (véase tabla 8) sólo es necesario el certificado para el servidor, en este caso se puede utilizar OpenSSL sin ningún problema o se puede comprar el certificado a una entidad emisora de certificados de confianza.

Formas de autenticación		
Método EAP	**Usuarios (Suplicante)**	**Serv. de Autenticación**
EAP-TLS	**Certificado**	**Certificado**
EAP-PEAP	Login/Password	Certificado
EAP-TLS	Login/Password	Certificado

Tabla 8. Mecanismos de autenticación

5.1.3. El autenticador 802.1X

El autenticador 802.1X es proporcionado por el fabricante de los equipos. Los APs recientes ya lo traen incorporados, o con una actualización por software se puede obtener. Actualmente muchos fabricantes ofrecen dos tipos de APs, los "thick" o "robustos" que son los tradicionales, en donde los APs hace las funciones de autenticación, cifrado, entre otras; por otro lado también existen los "thin" AP, que a diferencia de los APs "robustos" prácticamente sólo son antenas y operan junto con un Switch Controlador que coordina los APs y realiza las funciones que antes las hacía el AP, además de otras cosas; en este caso el autenticador 802.1X reside en el Switch, este tipo de soluciones es recomendado para redes de gran tamaño.

5.1.4. El suplicante 802.1X

Para hacer uso de WPA/WPA2, es necesario que los equipos de los usuarios móviles cuenten con el suplicante 802.1X, para la autenticación y control de acceso.

Microsoft Windows XP SP2 y Vista incluyen como parte del sistema operativo el suplicante 802.1X.

Para sistemas operativos Unix/Linux, existe el software libre llamado *WPA_Supplicant*.

El sistema operativo MAC OS también incluye en su sistema operativo, el suplicante 802.1X.

5.2. Preparación del servidor

El primer paso de la implementación de seguridad WLAN es preparar el servidor que contendrá las diferentes aplicaciones y se inicia con la elección del sistema operativo.

Elección del Sistema Operativo

Como se ha considerado una solución del proyecto basado en software libre, se elige un sistema operativo GNU/Linux que tiene la misma característica (software libre), para montar las aplicaciones.

Un sistema operativo GNU/Linux se compone principalmente de un núcleo (kernel) de Linux, un conjunto de herramientas GNU, un programa de instalación, un sistema de gestión de paquetes y muchos otros componentes de software, dichos elementos se pueden ajustar y configurar de acuerdo a diferentes necesidades y crear así un sistema operativo GNU/Linux, el hecho de que todos estos componentes son libres de usar y distribuir, desde 1993, muchas personas y empresas han creado una gran cantidad de distribuciones.

Todas las distribuciones incluyen el kernel de Linux desarrollado por Linus Torvalds y las herramientas GNU desarrollado por Richard Stallman, pero no necesariamente incluyen las últimas versiones de dichos componentes. Algunas distribuciones incluso hacen sus propios cambios en el núcleo. Cada distribución elige distintas aplicaciones de software, difieren en la forma en que dichas aplicaciones están configuradas y en la forma en que son instaladas y actualizadas, también difieren en muchos aspectos como su filosofía sobre el software propietario, prioridades entre facilidad de uso o eficiencia, entre estabilidad o última tecnología.

Algunas distribuciones son muy similares otras muy diferentes, la elección se hace dependiendo de las necesidades.

Actualmente hay muchas distribuciones disponibles, el siguiente sitio: http://www.distrowatch.com lista más 300 distribuciones activas, no tiene sentido comparar todas, en la tabla 9 se muestran algunas características de 8 de las más conocidas.

Distribución	**Primera Publica-ción**	**Distri – bución Base**	**No. Paquetes Precompila-dos (Aprox.)**	**Gestor de Paquetes**	**Propósito**	**Arquitecturas**
Debian	1993-08-16		25113	APT	general	x86, x86-64, IA-64, ppc, ppc64, sparc32, arm, hppa, mips, loongson, s390, s390x, alpha
Ubuntu	2004-10-20	Debian	26000	APT	Desktop/ Servidor	x86, x86-64, ppc
Slackware	1993-07-16	SLS	544	installpkg, upgradepkg	Desktop/ Servidor	x86, x86-64
Fedora	2003-11-05	RedHat	8000	yum	General	x86, x86-64, ppc, ppc64
Mandriva	1998-7-23	RedHat	20000	urpmi, rpmdrake	General	x86, x86-64
OpenSuse	1994-03-?	SUSE	22000	YaST, Zypper	Desktop/ Servidor	x86, x86-64, ppc
CentOS	2003-12-?	RHEL	1660	yum/up2date	Server	x86, x86-64, IA-64, s390, s390x, alpha
Gentoo	2002-3-?		80	Portage	General	x86, x86-64, IA-64, ppc, ppc64, sparc32, arm, hppa, mips, alpha

Tabla 9. Algunas características de las distribuciones GNU/Linux más conocidas

Se elige para este proyecto la distribución Debian, principalmente por las siguientes razones:

- Tiene uno de los mejores gestores de paquetes que es adoptada por muchas otras distribuciones, el APT.

- Es una distribución madura, es de las primeras que surgieron y actualmente ha logrado conformar una comunidad grande y fuerte.

- Es de las distribuciones con mayor número de paquetes.

- Es la que soporta mayor número de arquitecturas.

- Es una distribución de propósito general, pero gracias a la calidad de sus liberaciones se ha convertido en una distribución preferida para servidores.

Además Debian es conocido por su firme apego a la filosofía Unix y al software libre, es extremadamente estable, modular y rápido. También está muy bien documentado y traducido en muchos idiomas.

APT (Advanced Packaging Tool)
Es la herramienta de gestión de paquetes de Debian, es el mejor gestor de paquetes entre todas las herramientas GNU/Linux. La instalación y eliminación de software en Debian o en distribuciones que hacen uso del APT, es fácil y sin esfuerzo, y mucho más agradable que en la mayoría de las distribuciones que utilizan el formato RPM. Además soluciona de forma automática las dependencias que se presentan en la instalación de paquetes.

En resumen, el sistema operativo, la distribución y versión que se eligen para servidor son:

Sistema Operativo: **GNU/Linux**
Distribución: **Debian 4.0 "Etch**"

5.2.1. Consideraciones básicas de seguridad

Es importante contemplar aspectos básicos en la seguridad del servidor, porque de nada serviría implementar el último protocolo de seguridad si por un pequeño descuido, el servidor que aloja las aplicaciones quedara fuera servicio, se vea seriamente afectada la disponibilidad de la red inalámbrica.

a) Instalación únicamente del sistema base

La distribución Debian permite la instalación únicamente de un "sistema base", muy recomendado. Se realiza la instalación de las aplicaciones conforme se vayan requiriendo y de esta forma se evita tener programas innecesarios, algunos de ellos pueden tener huecos de seguridad, algunos otros "abren puertos" TCP/UDP no deseados, con lo anterior se reducen riesgos de seguridad al servidor.

Si se realiza la instalación sólo del sistema base, al ejecutar el siguiente comando en modo "superusuario", no se tiene que observar ningún servicio "escuchando" por algún puerto.

Con el siguiente comando, se puede verificar los servicios y los puertos "abiertos":

```
netstat –tulp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
State       PID/Program name
```

b) Espejeo o redundancia de disco duro

Algunas veces los discos duros llegan a fallar, por lo que resulta importante tener redundancia de disco duro, se recomienda la implementación de RAID1 durante la instalación, RAID1 permite realizar una réplica de los datos en un disco secundario, la distribución elegida, permite conseguir este objetivo de forma sencilla durante la instalación del sistema.

c) Seguridad física

El sitio físico donde permanecerá el servidor debe ser un espacio físicamente seguro, los accesos al lugar deben ser limitados y controlados, de igual forma los accesos al servidor tiene que ser restringidos, solamente usuarios autorizados tendrán accesos a él.

d) Respaldos

Los respaldos resultan invaluables en caso de que un desastre físico, accidente, ataque o por algún bug se llegara a alterar el correcto funcionamiento del sistema; se tiene que establecer una estrategia específica considerando los periodos para realizarlos, si van a ser respaldos totales, incrementales o diferenciales; definición de los dispositivos para almacenarlos; determinación de los lugares para resguardarlos y asignación de responsable(s) para realizarlos.

e) Particiones

Es recomendable que en los servidores se realicen particiones separadas al menos para: /, /boot, /usr/local, /var, /tmp y /home, si llegara a existir alguna falla en los sistemas de archivos de alguna partición, las demás particiones quedan libres de ese error, lo anterior disminuye los riesgos de pérdida total y acelera los tiempos de recuperación ante un desastre, además las particiones establecen una barrera lógica entre el espacio al que acceden los usuarios, el espacio al que accede el sistema y el espacio al que acceden las aplicaciones.

f) Firewall

Un firewall siempre es necesario para proteger un servidor en la red, todas las distribuciones GNU/Linux actuales traen integrados el módulo *netfilter* en el kernel o núcleo que permite la implementación de un firewall.

g) Accesos remotos inseguros

Telnet, rlogin, rsh, rcp y FTP son vulnerables a escuchas espías, se deben evitar ejecutar estas aplicaciones, en su lugar se pueden utilizar las siguientes aplicaciones:

- SSH como reemplazo de telnet, rlogin y rsh para los accesos o shell remotos.
- SCP como reemplazo de rcp y SFTP en lugar de FTP para las transferencias de archivos.

h) Contraseñas fuertes

Es importante establecer contraseñas fuertes, fáciles de recordar pero difíciles de adivinar. Hacer uso mínimo 8 caracteres, utilizando al menos uno de los siguientes: números, letras (mayúsculas y minúsculas) y caracteres especiales (ej. ¡@.?).

Ejemplo de una contraseña fuerte, difícil de adivinar y fácil de recordar:
Usuario: *root* (el usuario administrador en GNU/Linux)
Contraseña: *@dm!Nistrad0r*

5.2.2. Instalación de paquetes y librerías necesarias

Para evitar errores durante la compilación de FreeRADIUS es necesaria la instalación de las siguientes aplicaciones y librerías, además permite habilitar los módulos eap y ldap que son imprescindibles para la solución.

```
apt-get install build-essential
apt-get install snmp
apt-get install libperl-dev
apt-get install libltdl3-dev
apt-get install libssl-dev
apt-get install libgdbm-dev
apt-get install libldap2-dev
```

Instalación de SSH

Como se mencionó en la sección anterior, el servidor se mantiene en un espacio físico controlado, generalmente fuera del área de trabajo del administrador, haciendo necesarias las conexiones remotas para la administración del servidor, la aplicación recomendada para las tareas mencionadas es un servidor SSH (Secure Shell), además con la filosofía de instalar solamente las aplicaciones necesarias se tiene un sistema operativo en modo texto y es mucho más cómodo y eficiente trabajar en una consola remota que hacerlo directamente.

Con la ejecución del siguiente comando se instala el servidor OpenSSH, la implementación libre de SSH.

```
apt-get install ssh
```

Ahora se puede acceder al servidor desde un cliente SSH, es importante tener cuentas de usuarios con contraseñas fuertes.

Hasta el momento sólo se tiene el puerto 22 TCP abierto, es donde el servidor “escucha” las peticiones de conexiones remotas a través de SSH. Se comprueba lo anterior ejecutando el siguiente comando:

```
netstat –tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp6       0      0 :::22                   :::*                    LISTEN      2794/sshd
```

5.3. Implementaciones

5.3.1. OpenSSL

La versión estable disponible de OpenSSL, en el momento que se desarrolla este documento es la 0.9.8h, las fuentes se pueden conseguir en www.openssl.org.

5.3.1.1. Compilación de OpenSSL

La compilación de OpenSSL es muy fácil, tal como se muestra en la siguiente sintaxis. Es importante tener mucho cuidado en no sobrescribir el OpenSSL con alguna otra versión previamente instalada. Para evitar lo anterior es necesario especificar la ruta para la instalación.

Se mueven las fuentes al directorio /usr/src:

```
cd /usr/src/
```

```
tar xzvf openssl-0.9.8h.tar.gz
cd openssl-0.9.8h
./config shared –prefix=/usr/local/openssl
make
make install
```

Como la ruta de instalación no es una ubicación estándar, es necesario indicarle al sistema editando el siguiente archivo de configuración: /etc/ld.so.conf

En el archivo se agrega la siguiente línea:

```
/usr/local/openssl/lib
```

Enseguida se ejecuta el siguiente comando para que se tomen los cambios:

```
ldconfig
```

5.3.1.2. Configuración de OpenSSL

Una vez, que se haya instalado exitosamente OpenSSL, es necesario realizar algunos cambios a los archivos de configuración para facilitar la creación de los certificados, los datos que se insertan tienen que identificar a la organización.

El archivo que se va editar es el /usr/local/openssl/ssl/openssl.cnf.

En la sección `[ CA_default ]` se cambia el periodo de validez de los certificados, ejemplo: 730 para 2 años.

```
Default_days    = 730                   # how long to certify for
```

En la sección `req_distinguished_name`, se realizan los cambios que se encuentran en negrita.

```
[ req_distinguished_name ]
```

```
countryName                     = Country Name (2 letter code)
countryName_default             = MX
countryName_min                 = 2
countryName_max                 = 2
stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = MEXICO
localityName                    = Locality Name (eg, city)
localityName_default            = DF #esta linea se agrega
0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = UNAM
organizationalUnitName          = Organizational Unit Name (eg, section)
organizationalUnitName_default  = DGSCA
commonName                      = Common Name (eg, YOUR name)
commonName_max                  = 64
emailAddress                    = Email Address
emailAddress_max                = 64
```

5.3.2. FreeRADIUS

Se pueden bajar las fuentes de FreeRADIUS de la página www.freeradius.org, se recomienda obtener la última versión, la 1.1.7 es la que se usa para este proyecto.

5.3.2.1. Compilación e instalación de FreeRADIUS

Se mueve el paquete al directorio `/usr/src`:

```
mv freeradius-1.1.7.tar.gz /usr/src/
```

Se accede a la carpeta /usr/src:

```
cd /usr/src
```

Se desempaqueta de la siguiente forma:

```
tar xzvf freeradius-1.1.7.tar.gz

cd freeradius-1.1.7
```

Se configura la instalación con las siguientes opciones:

`--prefix:` Establece la ruta en donde se instalará FreeRADIUS

```
./configure --prefix=/usr/local/radius
```

Con el siguiente comando se hace la compilación:

```
make
```

Finalmente se realiza la instalación:

```
make install
```

Las librerías se instalan en:

/usr/local/radius/lib

Se edita el archivo **`/etc/ld.so.conf,`** y se agrega la siguiente entrada:

```
/usr/local/openssl/lib
/usr/local/radius/lib
```

Para que se actualicen los cambios que se realizan en el archivo *ld.so.conf*, se ejecuta el comando:

```
ldconfig
```

5.3.2.2. Los archivos de configuración de FreeRADIUS

Los archivos de configuración se localizan en la siguiente ruta:

```
/usr/local/radius/etc/raddb
```

1. **radiusd.conf**

   Es el archivo de configuración principal de FreeRADIUS, contiene varias directivas que definen el comportamiento del servidor, apuntadores a otros archivos de configuración así como los módulos disponibles. Los cambios que se realizan en este archivo son mínimos.

2. clients.conf

Este archivo es responsable para determinar los clientes del servidor que podrán conectarse al servidor. En este caso clientes se refiere a los NAS (Autenticador) que pueden ser los Access Point o un Switch controlador. Existen dos formas de realizar las entradas, ya sea agregando todo un segmento de red o especificar únicamente a un cliente en particular con su dirección IP.

3. **users**

Este archivo contiene información de los usuarios que tendrán acceso al sistema, la forma en que serán autenticados y también se pueden agregar listas de atributos de autenticación. Para la entrada de usuarios inalámbricos con autenticación PEAP es muy sencilla, como se verá adelante; hay que recordar que el servidor RADIUS es utilizado para autenticar usuarios remotes vía MODEM, en donde es necesario asignar valores a ciertos atributos.

4. eap.conf

En este archivo de configuración se especifica el método EAP de autenticación a usar: EAP-TLS, EAP-PEAP o EAP-TTLS.

5.3.2.3. Configuración de FreeRADIUS

a) EAP-PEAP Básica

1. radiusd.conf

Los cambios que se realizan en este archivo son mínimos, únicamente verifique y/o modifique, lo que a continuación se indique, el resto de los parámetros permanece por default.

En la sección *mschap* descomente las siguientes directivas y asigne los valores indicados.

El protocolo MPPE definido en el *RFC3078* se encarga del envío PMK al AP.

```
mschap
{
        use_mppe = yes
        require_encryption = yes
        require_strong = yes
}
```

En la sección *authorize* y *authenticate* las directivas que se requieren generalmente ya se encuentran activas, en este caso no es necesario realizar alguna modificación, simplemente se verifican.

```
authorize
{
     preprocess
     mschap
     suffix
     eap
      files
}

authenticate
{

     Auth-Type MS-CHAP
      {
           mschap
     }
     eap
}
```

clients.conf

Se agregan los clientes (el AP es el NAS o cliente del servidor RADIUS), en este caso la dirección es 132.248.120.155.

Existen dos formas de agregar: incluyendo todo el segmento al que pertenece el AP o únicamente su dirección IP en particular:

Todo un segmento:

```
client 132.248.120.0/24
{
      secret     = secreto
      shortname  = wlan
}
```

Sólo la dirección IP:

```
client 132.248.120.155 {
        secret          = secreto
        shortname       = wlan
}
```

El valor de la directiva `secret,` también se usará en la configuración del autenticador.

users

Para el caso específico de la autenticación EAP-PEAP, las entradas de los usuarios es muy sencilla, simplemente se agrega un nombre de usuario y la contraseña, como se indica:

```
"usuario1" Cleartext-Password := "contraseña"
"usuario2" Cleartext-Password := "contraseña"
```

eap.conf

Se busca la directiva *`default_eap_type`* y se le cambia el valor por *peap:*

```
      default_eap_type = peap
```

En la sección *tls se* descomentan las líneas indicadas y se agrega la ruta donde se tiene el certificado del servidor.

En el apéndice C se muestra la forma de crear los certificados.

```
tls {
      private_key_password = wireless
      private_key_file = ${raddbdir}/miscerts/ServidorRADIUS.pem
      certificate_file = ${raddbdir}/miscerts/ ServidorRADIUS.pem
      CA_file = ${raddbdir}/miscerts/demoCA/cacert.pem
      dh_file = ${raddbdir}/certs/dh
      random_file = ${raddbdir}/certs/random
     }
```

Nota: En caso de que se utilicen los certificados que acompañan las fuentes de FreeRADIUS sólo se descomentan las líneas anteriores.

Finalmente se activa *EAP-PEAP*, quitando los comentarios a las líneas correspondientes de la sección *peap:*

```
       peap {
            default_eap_type = mschapv2
            }
```

No se realiza ninguna modificación con el resto de los parámetros

Y listo, se tiene un servidor RADIUS básico que es capaz de autenticar usuarios en una WLAN pequeña.

b) EAP-TLS

Para conseguir el método de autenticación EAP-TLS, los cambios se realizan únicamente en el archivo de configuración **eap.conf.**

En este caso, la directiva *default_eap_type* se le cambia el valor por *tls:*

```
default_eap_type = tls
```

La sección *tls* se mantiene igual

```
tls {
      private_key_password = wireless
      private_key_file = ${raddbdir}/miscerts/ServidorRADIUS.pem
      certificate_file = ${raddbdir}/miscerts/ ServidorRADIUS.pem
      CA_file = ${raddbdir}/miscerts/demoCA/cacert.pem
      dh_file = ${raddbdir}/certs/dh
      random_file = ${raddbdir}/certs/random
     }
```

Son todos los cambios que se requieren.

c) EAP-TTLS

Al igual que en los anteriores, los cambios solamente es en el archivo eap.conf:

```
default_eap_type = ttls
```

La sección *tls* se mantiene igual

```
tls {
      private_key_password = wireless
      private_key_file = ${raddbdir}/miscerts/ServidorRADIUS.pem
      certificate_file = ${raddbdir}/miscerts/ ServidorRADIUS.pem
      CA_file = ${raddbdir}/miscerts/demoCA/cacert.pem
      dh_file = ${raddbdir}/certs/dh
      random_file = ${raddbdir}/certs/random
     }
```

Se activa *ttls* quitando los comentarios de la sección de *ttls*

```
ttls {
      default_eap_type = md5
      }
```

5.4. Pruebas de las implementaciones

Para probar la implementación del Servidor de Autenticación se usa un AP avaya (el autenticador 802.1X) como se indico al inicio de este capítulo, en el apéndice A se muestra la configuración del AP Avaya con seguridad WPA y una Laptop con interfaz inalámbrica (suplicante 802.1X) que soporta los protocolos WPA y WPA2. Las configuraciones del suplicante 802.1X se muestran en el apéndice B.

a) WPA/EAP-PEAP

- Se establece la configuración EAP-PEAP en el servidor RADIUS como se indica en el inciso a) de la sección anterior.
- Se realiza la configuración de AP como se muestra en el apéndice A con una SSID “WLAN-PEAP”.
- Se genera e instala el certificado raiz (root) como se indica en los apéndices C y D.
- Se realiza la configuración EAP-PEAP en el suplicante (equipo del usuario inalámbrico) como se muestra en el inciso b) del apéndice B.
- En el equipo del usuario, se hace click con el botón derecho en el icono que aparece en la parte inferior derecha de la pantalla que corresponde a la interfaz de red inalámbrica y se elige *Ver redes inalámbricas disponibles.*

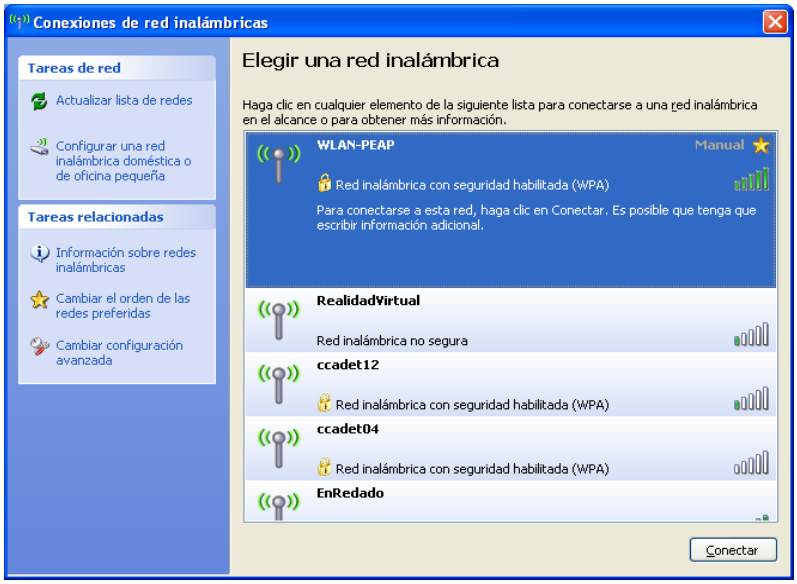

Figura 5.2. Redes inalámbricas disponibles.

- Se hace doble click sobre la red WLAN-PEAP (véase figura 5.2) y el sistema solicitará el nombre de usuario y la contraseña para la autenticación, como se muestra en la figura 5.3.

Figura 5.3. Conexión a la WLAN-PEAP.

- Después de que se proporcionan las credenciales (nombre de usuario y contraseña), el proceso pide validar el certificado del servidor, en este caso la "entidad emisora" es DGSCA, porque así se estableció en la generación de los certificados, si se compra el

certificado a una entidad emisora real, tendría que aparecer el nombre correspondiente (véase figura 5.4).

Figura 5.4. Validación de certificado.

- Si existe la entrada de la información del usuario en el archivo **users,** la conexión a la red inalámbrica se realiza de forma exitosa. La figura 5.5 indica que el equipo del usuario se encuentra conectado a la red inalámbrica.

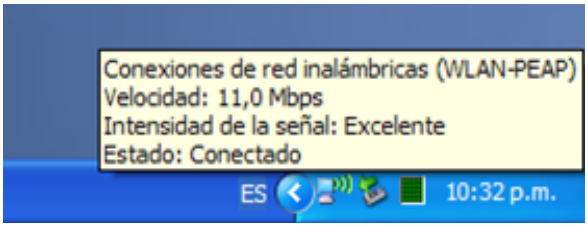

Figura 5.5. Estado conectado

b) WPA/EAP-TLS

- Se establece la configuración EAP-TLS en el servidor RADIUS como se indica en el inciso b) de la sección anterior.
- Se realiza la configuración de AP como se muestra en el apéndice A con una SSID “WLAN-TLS”.
- Se genera e instala los certificados raiz (root) y del usuario como se indica en los apéndices C y D.
- Se realiza la configuración EAP-TLS en el suplicante (equipo del usuario inalámbrico) como se muestra en el inciso a) del apéndice B.

- En el equipo del usuario, se hace click con el botón derecho en el icono que aparece en la parte inferior derecha de la pantalla que corresponde a la interfaz de red inalámbrica y se elige *Ver redes inalámbricas disponibles.*

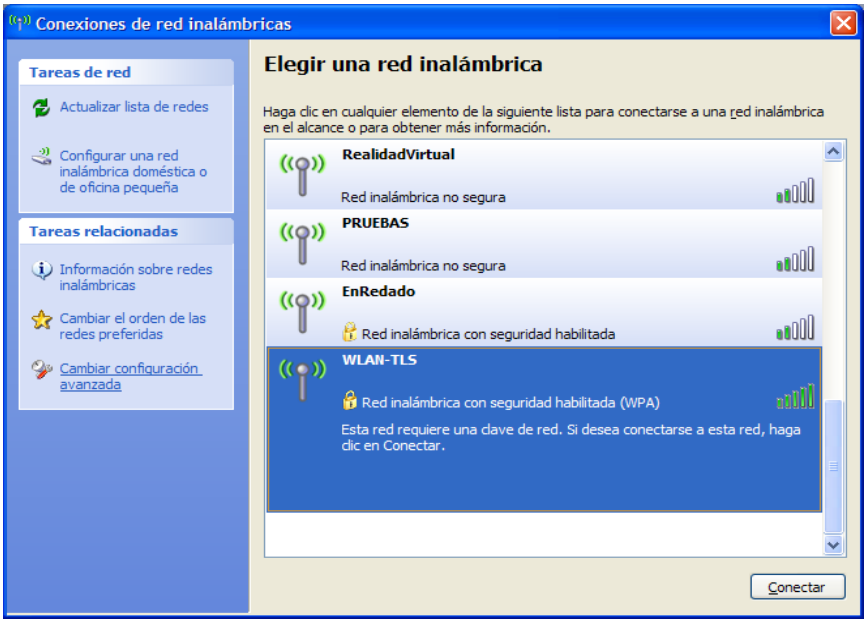

Figura 5.6. Redes inalámbricas disponibles.

- Se hace doble click sobre el nombre de la red que se ha configurado WLAN-TLS (véase figura 5.6) y se iniciará el proceso de conexión.
- Sí el certificado del usuario fue generado e instalado correctamente, la conexión se realiza de forma exitosa y transparente para el usuario.
- La figura 5.7 indica que el equipo del usuario se encuentra conectado a la red inalámbrica.

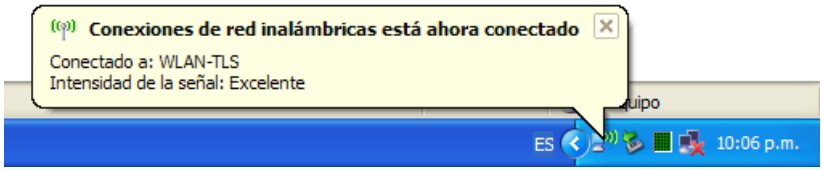

Figura 5.7. Conexión exitosa.

c) WPA/EAP-TTLS

- Se establece la configuración EAP-TTLS en el servidor RADIUS como se indica en el inciso c) de la sección anterior.
- Se realiza la configuración de AP como se muestra en el apéndice A con una SSID "WLAN-TTLS".
- Se genera e instala el certificado raiz (root) como se indica en los apéndices C y D.
- Se realiza la configuración EAP-TTLS en el suplicante (equipo del usuario inalámbrico) como se muestra en el inciso c) del apéndice B.
- La conexión es similar que en el caso de WPA/EAP-PEAP, el nombre de usuario y la contraseña tienen que estar dado de alta en el archivo users del servidor de autenticación.

Para obtener los protocolos de seguridad WPA2/EAP-PEAP, WPA2/EAP-TLS y WPA2/EAP-TTLS, los cambios se hacen solamente en el AP y en el suplicante, pero no en el servidor de autenticación. En el AP se elige el protocolo de seguridad WPA2 o 802.11i y en el suplicante se cambian los valores de los siguientes parámetros:

- *Autenticación de red:* WPA2 en lugar de WPA.
- *Cifrado de datos:* AES en lugar de TKIP.

CAPÍTULO 6

CASO PRÁCTICO: RIU

6. CASO PRÁCTICO: RIU

La dirección de Telecomunicaciones con el apoyo del departamento de seguridad en cómputo de la DGSCA (Dirección General de Sistemas y Cómputo Académico) tuvo la tarea de iniciar la implementación de la Red Inalámbrica Universitaria, a finales del 2005, en los diferentes campus de la UNAM.

Se establecieron una serie de requisitos, algunos de ellos que interesa a este proyecto fueron: una red inalámbrica segura, funcional, escalable y una administración centralizada.

Después de que se realizó el análisis de diseño y establecimiento de las diferentes políticas de seguridad, la red inalámbrica debía operar con los siguientes esquemas de seguridad:

- Protocolos de seguridad: WPA
- Mecanismo de autenticación: EAP-PEAP
- Diferentes niveles de acceso: *academicos, estudiantes y staff*.

En esta sección se describe la propuesta que se presentó como solución a los requerimientos de seguridad, escalabilidad y administración centralizada. Se consideró una infraestructura AAA compatible con las especificaciones de los protocolos de seguridad WPA/802.1i que se basan principalmente en el estándar 802.1X.

El componente principal es el servidor de autenticación. El protocolo ampliamente utilizado es el RADIUS, por lo que se elige un servidor RADIUS para dicha función.

La implementación se basa en el uso de software de libre, el sistema operativo y todos los elementos que integran la infraestructura:

- GNU/Linux como sistema operativo.
- FreeRADIUS como servidor de autenticación.
- Servidor MySQL como servidor de base de datos para los registros de las conexiones (Accounting).

- Servidor de directorio OpenLDAP como repositorio de usuarios.

WPA en lugar WPA2

WEP ya no es una solución confiable en la seguridad de las redes 802.11, por lo que de entrada fue descartado.

En la RIU se utiliza WPA, con la idea de migrar a WPA2 cuando la gran mayoría de los equipos de los usuarios cuenten con soporte, y como se mencionó anteriormente para la infraestructura AAA que se implementa en este proyecto, será transparente, por lo que no será necesario realizar cambios en su implementación para lograr seguridad 802.11i en la Red. Si en su momento se hubiera elegido WPA2, se dejaba a un gran porcentaje de los usuarios sin posibilidad de conexión.

EAP-PEAP en lugar EAP-TLS

Como se menciona en el capítulo anterior, para aprovechar al máximo el método de autenticación EAP-TLS es conveniente contar con una infraestructura de PKI para la emisión, revocación y manejo de certificados de llaves públicas, basados en el estándar X.509, establecer una PKI no es una tarea sencilla, se requiere todo un proceso y una planeación para su diseño, el alcance de este trabajo no incluye su construcción; más bien el proyecto propone el método de autenticación EAP-PEAP, que para la autenticación de los usuarios solamente se requiere de un nombre de usuario y una contraseña; y solamente se necesitan certificados para cada uno de los servidores de autenticación.

EAP-PEAP en lugar EAP-TTLS

Gran parte de los sistemas operativos de los usuarios es Microsoft Windows, principalmente XP y Vista y estos sistemas operativos incluyen el autenticador 802.1X con las opciones EAT-TLS y EAP-PEAP, en cambio, para conseguir el mecanismo de autenticación EAP-TTLS los usuarios

tendrían que instalar un software adicional, por lo que se prefiere aprovechar la ventaja que ofrece Microsoft Windows, que es el sistema operativo de la mayoría de los usuarios.

Cabe aclarar que ambos son igualmente seguros y eficientes ya que realizan las mismas funciones, aunque se lleven a cabo de formas distintas.

Tecnología ARUBA

De las diferentes pruebas que se realizaron a los diferentes fabricantes de equipos 802.1X, la tecnología Aruba fue seleccionada para la implementación de la red inalámbrica por aproximarse más a los requerimientos planteados en las evaluaciones.

El enfoque principal en este proyecto es en la infraestructura AAA, en el servidor de autenticación de la arquitectura 802.1X (véase figura 4.3), que por los motivos planteados en el capítulo anterior se elige FreeRADIUS como servidor RADIUS; por lo que no se presentan los detalles de la configuración del autenticador (Switch controlador ARUBA), sólo los aspectos generales que involucran la configuración de los protocolos de seguridad.

Escenario

En la figura 6.1 se muestra de forma general los diferentes elementos que conforma la solución total.

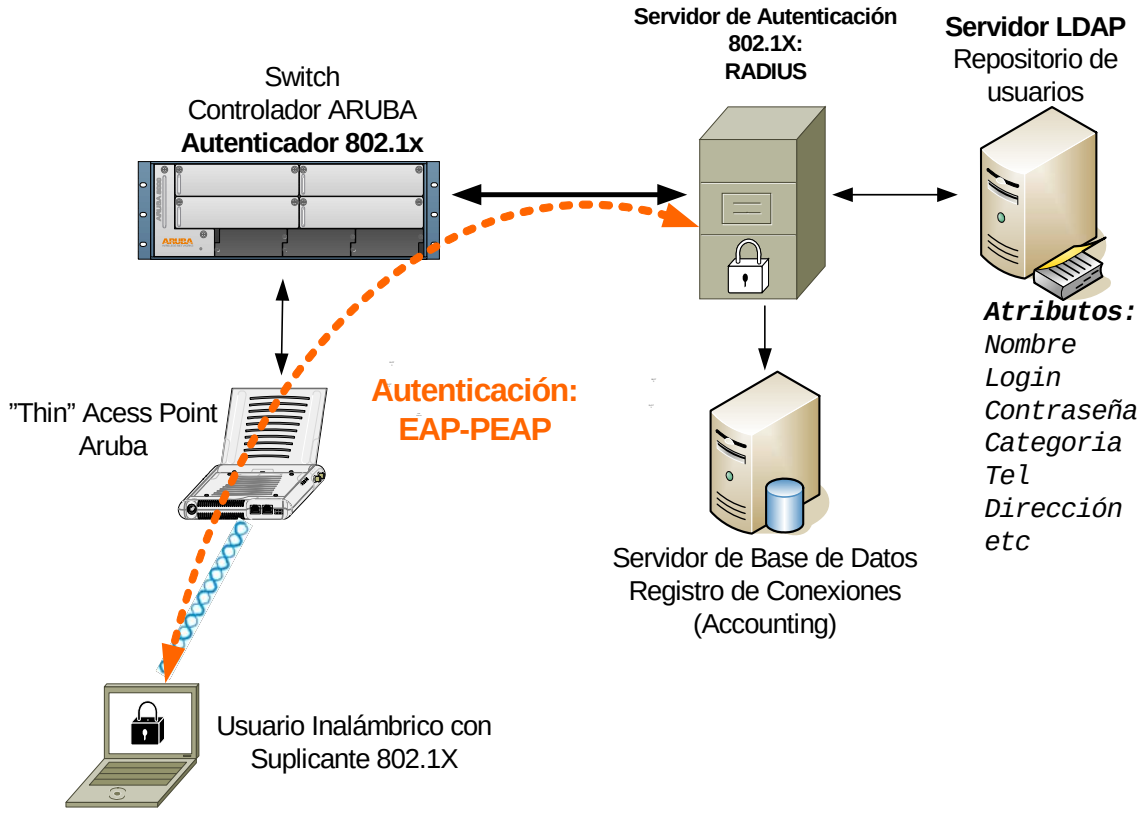

Figura 6.1. Solución de seguridad en la RIU

6.1. Infraestructura AAA basado en software libre

6.1.1. OpenSSL

Se siguen los pasos de instalación descritos en la sección 5.3.1 del capítulo anterior, como la solución utiliza el método de autenticación EAP-PEAP que sólo requiere certificado para el servidor de autenticación, el cual se adquiere a una entidad emisora de certificados no se va a utilizar OpenSSL para generar los certificados por lo que no es necesario modificar el archivo /usr/local/openssl/ssl/openssl.cnf. Las librerías SSL son indispensables para habilitar los módulos eap de FreeRADIUS; también se utilizará dichas librerías para generar una CSR (Certificate Signing Request, 'Solicitud de firma de certificado') requerido en la compra de un certificado a una entidad emisora de certificados real.

6.1.1.1. Solicitud de un certificado a una entidad emisora de certificados

En una red inalámbrica de grandes dimensiones como la RIU, no es recomendable el uso de certificados “auto firmados” para el servidor de autenticación, lo más conveniente es adquirirlo a una entidad emisora de confianza que existen en el mercado.

A continuación se muestra un ejemplo del proceso a seguir para solicitar un certificado:

1. Generación de la llave privada

```
/usr/local/openssl/bin/openssl genrsa -des3 -out nombreservidor.riu.unam.mx.key 1024
```

NOTA: Este archivo tiene que ser confidencial, solamente el servidor RADIUS tiene que conocer la ruta de su ubicación.

2. Obtención del Certificate signing request

```
/usr/local/openssl/bin/openssl req -new -key nombreservidor.riu.unam.mx.key -out
nombreservidor.riu.unam.mx.csr
```

```
país: MX
estado/provincia: MEXICO
localidad: DISTRITO FEDERAL
organización: UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
unidad organizativa: DIRECCION GENERAL DE SERVICIOS DE COMPUTO ACADEMICO
nombre común: nombreservidor.riu.unam.mx
```

3. Solicitud del certificado a la entidad emisora

La entidad emisora pide la “solicitud de firma de certificado” o el certificate signing request (CSR), en este caso específico a la DGSCA o a la organización que requiere el certificado, dicho archivo se generó en el paso anterior, a partir del CSR, la entidad emisora genera y firma el certificado.

4. Entrega del Certificado.

La entidad emisora entrega el certificado a la organización que lo solicita. En las secciones posteriores se indica dónde se tiene que colocar.

6.1.2. OpenLDAP

El servidor OpenLDAP se puede instalar con el apt de GNU/Debian, pero es recomendable usar siempre la versión más reciente, por lo que es preferible realizar la compilación de las fuentes.

OpenLDAP se puede obtener en la siguiente dirección:

http://www.openldap.org/software/download/

Las bases de datos *backend* más utilizados son:

- *bdb*. Se considera esta base de datos por defecto, sí se quiere deshabilitar se tiene que agregar en la configuración la cadena: `--disable-bdb`
- *ldbm*. Esta opción no se contempla, sí se quiere habilitar se tiene que agregar la cadena: `--enable-ldbm`

En esta implementación se hará uso de *bdb* como base de datos, por lo que se tendrá que instalar antes las librerías correspondientes de esta aplicación.

```
apt-get install libdb4.4-dev
```

6.1.2.1. Compilación e instalación de OpenLDAP

OpenLDAP permite conexiones seguras por medio de SSL, se habilita esta funcionalidad durante la instalación, pero para ello se requiere la instalación previa de OpenSSL.

Como se ha hecho con todos los paquetes, se mueve las fuentes OpenLDAP al directorio /usr/src.

```
cd /usr/src
tar xzvf openldap-version.tgz
cd openldap-version/
```

Configuración de instalación:

Para ver las opciones de configuración de la instalación, se ejecuta:

```
./configure --help
```

```
env        CPPFLAGS="-I/usr/local/openssl/include"                  LDFLAGS="-
L/usr/local/openssl/lib"     LIBS="-L/usr/local/openssl/lib"   ./configure   --
prefix=/usr/local/ldap    --enable-slapd  --enable-slurpd  --with-threads  --
enable-debug  --with-tls --enable-bdb  --enable-ldbm
```

LDFLAGS: Especifica las banderas para los enlaces con OpenSSL, que se instalaron en /usr/local/openssl.

LIBS:	Especifica librerías adicionales, en este caso OpenSSL
--prefix:	Especifica la ruta en donde se realizará la instalación
--enable-slapd:	Habilita la construcción del demonio del servidor LDAP
--enable-slurpd:	Habilita la construcción del demonio para replicación.
--with-threads:	Habilita la funcionalidad multihilo.
--enable-debug:	Activa el código de depuración.
--with-tls	Habilita el soporte TLS.
--enable-bdb:	Construye **slapd** usando como interfaz primaria de bases de datos Berkeley DB.
--enable-ldbm:	Construye **slapd** usando como interfaz primaria de bases de datos ya sea la de Berkeley DB GNU Database Manager.

Compilación e instalación:

```
make depend
make
make test
make install
```

Si no hubo errores en la compilación e instalación, OpenLDAP queda instalado en:
/usr/local/ldap.

6.1.2.2. Configuración de OpenLDAP

1. se edita el archivo de configuración principal: */usr/local/ldap/etc/openldap/slapd.conf*. Únicamente se agregan/cambian los parámetro indicados a continuación:

```
include         /usr/local/ldap24/etc/openldap/schema/core.schema
include         /usr/local/ldap24/etc/openldap/schema/RADIUS-LDAPv3.schema
include         /usr/local/ldap24/etc/openldap/schema/cosine.schema
include         /usr/local/ldap24/etc/openldap/schema/inetorgperson.schema
include         /usr/local/ldap24/etc/openldap/schema/nis.schema
include         /usr/local/ldap24/etc/openldap/schema/qmail.schema
…
database        bdb
suffix          "dc=unam,dc=mx"
rootdn          "cn=Manager,dc=unam,dc=mx"
…
rootpw          ponerUnPassword
…
directory       /usr/local/ldap/var/openldap-data
```

2. Se inicia el demonio del servidor, ejecutando el siguiente comando:

```
/usr/local/ldap/libexec/slapd
```

Se asegura que el servidor inició correctamente, con la ejecución del comando:

```
/usr/local/ldap/bin/ldapsearch -x -b '' -s base '(objectclass=*)' namingContexts
```

Si se observa el parámetro que se asigno a la directiva *suffix*, en el paso anterior significa que el servidor inicio correctamente, sino se verifica el archivo de configuración.

```
…
namingContexts: dc=unam,dc=mx
…
```

3. Se crea el arbol: ***unam.mx*.** En un editor de texto se crea el archivo *estructuraLDAP.ldif*, con el contenido siguiente:

```
dn: dc=unam,dc=mx
objectclass: dcObject
objectclass: organization
o: DGSCA,UNAM
dc: unam
```

```
dn: cn=Manager,dc=unam,dc=mx
objectclass: organizationalRole
cn: Manager
```

4. Se agrega la estructura:

```
/usr/local/ldap/bin/ldapadd -x -D "cn=Manager,dc=unam,dc=mx" -W -f
estructuraLDAP.ldif
```

La ejecución pedirá la contraseña que se asignó en el paso 1, a través de la directiva *rootpw*. Se tiene que asegurar que el archivo estructuraLDAP.ldif esté ubicado en la ruta actual.

Para verificar que la estructura fue agregada correctamente, se ejecuta:

```
/usr/local/ldap/bin/ldapsearch -x -b 'dc=unam,dc=mx' '(objectclass=*)'
```

Se muestra una salida similar a la estructura o árbol que se agregó.

```
# extended LDIF
#
# LDAPv3
# base <dc=unam,dc=mx> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# unam.mx
dn: dc=unam,dc=mx
objectClass: dcObject
objectClass: organization
o: DGSCA,UNAM
dc: unam

# Manager, unam.mx
dn: cn=Manager,dc=unam,dc=mx
objectClass: organizationalRole
cn: Manager

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

5. **Se crean los directorios que alojan a los usuarios.** En un editor de texto se crea el archivo *directorios.ldif*, con el siguiente contenido:

```
dn: ou=wireless,dc=unam,dc=mx
objectClass: top
objectClass: organizationalUnit
ou: wireless

dn: ou=usuarios,ou=wireless,dc=unam,dc=mx
objectClass: top
objectClass: organizationalUnit
ou: usuarios
```

Se agregan los directorios con el siguiente comando:

```
/usr/local/ldap/bin/ldapadd -x -D "cn=Manager,dc=unam,dc=mx" -W -f directorios.ldif
```

6. **Entrada de los usuarios al directorio.**

El directorio LDAP maneja varios atributos para almacenar la información de los usuarios pero los atributos esenciales para el servidor RADIUS son: **uid** que guarda el login o el nombre de usuario**, userpassword** que almacena la contraseña **y radiusGroupName** que permite hacer diferentes grupos**.**

Categorías o niveles de acceso

Se utiliza el atributo **`radiusGroupName`** para realizar las categorías de usuarios, en la RIU se manejan 3 categorías:

- *estudiantes*
- *academicos*
- *staff*

Una vez que un usuario es autenticado correctamente, el servidor RADIUS verifica el valor del atributo **radiusGroupName** en la base de datos LDAP y regresa el valor dentro del atributo **Aruba-User-Role** al switch controlador ARUBA con el que le indica la categoría a la que pertenece el usuario.

A manera de ejemplo, se muestra la entrada de un usuario, que pertenece al grupo *estudiantes*.

Se edita el archivo usuarios.ldif, con el contenido siguiente:

```
dn: uid=estudiante1,ou=usuarios,ou=wireless,dc=unam,dc=mx
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: radiusprofile
cn: estudiante1
sn: estudiante1
givenname: prueba
mail: estudiante1@unam.mx
telephonenumber: 56220000
homephone: 56220000
mobile: 56220000
uid: estudiante1
userpassword: estudiante1
radiusGroupName: estudiantes
```

Se agregan los usuarios, ejecutando el comando siguiente en un sola línea:

```
/usr/local/ldap/bin/ldapadd -x -D "cn=Manager,dc=unam,dc=mx" -W -f
usuarios.ldif
```

Los atributos *mail* y *radiusGroupName* requieren de los esquemas *qmail*.schema RADIUS-*LDAPv3*.schema, respectivamente.

Se obtienen de las siguientes ligas de Internet:

- qmail.schema

  http://www.grotan.com/ldap/

  Nota: En esta página también se encuentra RADIUS-LDAPv3.schema, pero no está actualizado.

- RADIUS-LDAPv3.schema

  http://www.whitemiceconsulting.com/node/42

Una vez que se consiguen los esquemas, se mueven al directorio /usr/local/ldap/etc/openldap/schema:

```
mv qmail.schema RADIUS-LDAPv3.schema /usr/local/ldap/etc/openldap/schema/
```

6.1.3. MySQL

La aplicación de FreeRADIUS realiza los registros de “accounting” en un archivo de texto plano.

Ejemplo: Registros de inicio y fin de conexión de un usuario en la Red Inalámbrica RIU:

Inicio de Conexión a la RIU

```
….
Thu Oct  9 00:05:58 2008
        NAS-IP-Address = 132.247.xxx.yyy
        Acct-Status-Type = Stop
        User-Name = "megabren"
        NAS-Port = 1
        NAS-Port-Type = Wireless-802.11
        Acct-Session-Id = " megabren0018DE7810AA-2483"
        Acct-Input-Octets = 0
        Acct-Output-Octets = 0
        Acct-Input-Packets = 0
        Acct-Output-Packets = 0
        Acct-Terminate-Cause = Idle-Timeout
        Framed-IP-Address = 10.3.2.248
        Calling-Station-Id = "0018DE7810AA"
        Called-Station-Id = "000B86033080"
        Acct-Session-Time = 187
        Acct-Delay-Time = 0
        Aruba-Essid-Name = "RIU"
        Aruba-Location-Id = "48.1.15"
        Aruba-User-Role = "ESTUDIANTE"
        Aruba-User-Vlan = 302
        Client-IP-Address = 132.247.xxx.yyy
        Acct-Unique-Session-Id = "5c6985aa82b3d762"
        Timestamp = 1223528758
….
```

FIN de Conexión

```
…
Thu Oct  9 00:31:03 2008
        NAS-IP-Address = 132.247.xxx.yyy
        Acct-Status-Type = Stop
        User-Name = "megabren"
        NAS-Port = 1
        NAS-Port-Type = Wireless-802.11
        Acct-Session-Id = "megabren0018DE7810AA-2483"
        Acct-Input-Octets = 0
        Acct-Output-Octets = 6961312
```

```
        Acct-Input-Packets = 0
        Acct-Output-Packets = 16593
        Acct-Terminate-Cause = Idle-Timeout
        Framed-IP-Address = 10.3.2.248
        Calling-Station-Id = "0018DE7810AA"
        Called-Station-Id = "000B86033080"
        Acct-Session-Time = 3498
        Acct-Delay-Time = 0
        Aruba-Essid-Name = "RIU"
        Aruba-Location-Id = "48.1.15"
        Aruba-User-Role = "ESTUDIANTE"
        Aruba-User-Vlan = 302
        Client-IP-Address = 132.247.xxx.yyy
        Acct-Unique-Session-Id = "5c6985aa82b3d762"
        Timestamp = 1223530263
…
```

La información útil para cuestiones estadísticas y de administración que se puede obtener de las bitácoras son:

- Fecha de inicio de conexión: **`Thu Oct 9 00:05:58 2008`** *(AcctStartTime)*
- Fecha de fin de conexión: **`Thu Oct 9 00:31:03 2008`** *(AcctStopTime)*
- Nombre de usuario: **`megabren`** *(UserName)*
- Dirección IP del usuario: **`10.3.2.248`** (*FramedIPAddress)*
- Dirección MAC del usuario: **`0018DE7810AA`** (*CallingStationId)*
- Categoría del usuario: **`ESTUDIANTE`** *(ArubaUserRole)*
- Vlan a la que pertenece el usuario: **`302`** (*ArubaVlan)*
- Localidad a la que pertenece el usuario: **`48.1.15`** (*ArabaLocationId)*
- Cantidad de información recibida: **`0`** (*AcctInputOctets)*
- Cantidad de información enviada: **`6961312`** (*AcctOutputOctets)*

En redes muy grandes, como el caso de la RIU se generan miles de entradas diariamente y se vuelve compleja la lectura de estos archivos, para facilitar el procesamiento y análisis estadísticos de los registros se introducen estos datos a una tabla de una base de datos, desde donde se puedan realizar consultas de cualquier tipo y desplegar la información de una forma clara , precisa y concisa.

Ejemplos de algunas consultas específicas que se podrían ejecutar a la tabla de registros son:

- Número de conexiones por día por AP

- Número de conexiones por usuario
- Rastreo de un usuario específico, ya sea por nombre de usuario por MAC
- Lugar (localidad) desde donde realiza la conexión
- Cantidad de información Recibida/transmitida por Switch o por usuario
- Tiempo de conexión del usuario.
- Etc.

Para conseguir lo anterior se implementa un servidor de base de datos y se integra al sistema, en este caso se elige MySQL en su versión libre para dichas funciones, por facilidad de implementación y porque existe amplia documentación en Internet sobre esta aplicación.

6.1.3.1. Instalación de MySQL

Se utiliza la aplicación *apt* de la distribución Debian para la instalación del servidor, además se instalan las librerías que requieren los módulos de FreeRADIUS para la conexión con la base de datos:

```
apt-get install libmysqlclient15-dev
apt-get install mysql-server-5.0
```

Durante la instalación que se realiza de mysql-server-5.0, también se instala un cliente que se utilizará como herramienta para el manejo y administración inicial del servidor:

Conexión al servidor a través del cliente “mysql”
Se ejecuta:

```
mysql –uroot -p
```

La aplicación proporciona un espacio interactivo desde donde se podrá realizar cualquier tarea de administración del manejador.

```
mysql>
```

Lo primero que se hace después de la instalación de MySQL es asignar una contraseña al usuario “*root”* de la aplicación.

Se asigna una contraseña al usuario “root”, con la siguiente instrucción:

```
mysql> set password for root@localhost = password('micontraseña');
flush privileges;
```

Una vez que se haya asignado la contraseña, para realizar la conexión se agrega el parámetro –p:

```
mysql -uroot -p
```

6.1.3.2. Creación de la base de datos *radius* y de las tablas

Se crea la base de datos “radius”:

```
mysql> CREATE DATABASE radius;
```

Se crean las tablas:

Se usa el esquema de tablas predefinida que acompaña las fuentes de FreeRADIUS. El archivo se localiza en:

```
/usr/local/radius/share/doc/freeradius/examples/mysql.sql
```

Este archivo contiene la estructura de las siguientes tablas:

```
radacct
radcheck
radgroupcheck
radgroupreply
radreply
usergroup
radpostauth
dictionary
nas
radippool
```

La tabla que interesa porque es la única relacionada con los registros de accounting es “radacct”.

Estructura de la tabla radacct:

```
CREATE TABLE radacct (
  RadAcctId bigint(21) NOT NULL auto_increment,
  AcctSessionId varchar(32) NOT NULL default '',
  AcctUniqueId varchar(32) NOT NULL default '',
  UserName varchar(64) NOT NULL default '',
  Realm varchar(64) default '',
  NASIPAddress varchar(15) NOT NULL default '',
  NASPortId varchar(15) default NULL,
  NASPortType varchar(32) default NULL,
  AcctStartTime datetime NOT NULL default '0000-00-00 00:00:00',
  AcctStopTime datetime NOT NULL default '0000-00-00 00:00:00',
  AcctSessionTime int(12) default NULL,
  AcctAuthentic varchar(32) default NULL,
  ConnectInfo_start varchar(50) default NULL,
  ConnectInfo_stop varchar(50) default NULL,
  AcctInputOctets bigint(12) default NULL,
  AcctOutputOctets bigint(12) default NULL,
  CalledStationId varchar(50) NOT NULL default '',
  CallingStationId varchar(50) NOT NULL default '',
  AcctTerminateCause varchar(32) NOT NULL default '',
  ServiceType varchar(32) default NULL,
  FramedProtocol varchar(32) default NULL,
  FramedIPAddress varchar(15) NOT NULL default '',
  AcctStartDelay int(12) default NULL,
  AcctStopDelay int(12) default NULL,
  PRIMARY KEY  (RadAcctId),
  KEY UserName (UserName),
  KEY FramedIPAddress (FramedIPAddress),
  KEY AcctSessionId (AcctSessionId),
  KEY AcctUniqueId (AcctUniqueId),
  KEY AcctStartTime (AcctStartTime),
  KEY AcctStopTime (AcctStopTime),
  KEY NASIPAddress (NASIPAddress)
) ;
```

Al inicio de la sección 6.1.3 se presentaron ejemplos de registros de inicio y fin de conexión que envía el controlador ARUBA (Autenticador) el servidor RADIUS en donde se observa que existen 4 atributos que no contempla la tabla. Los 4 atributos adicionales son propietarios del fabricante ARUBA.

ArubaLocationId
ArubaUserRole
ArubaUserVlan
ClientIPAddress

Se agregan estos cuatro registros a la tabla y se renombra a *conexiones*, queda de la siguiente forma:

```
CREATE TABLE conexiones (
  RadAcctId bigint(21) NOT NULL auto_increment,
  AcctSessionId varchar(32) NOT NULL default '',
  AcctUniqueId varchar(32) NOT NULL default '',
  UserName varchar(64) NOT NULL default '',
  Realm varchar(64) default '',
  NASIPAddress varchar(15) NOT NULL default '',
  NASPortId varchar(15) default NULL,
  NASPortType varchar(32) default NULL,
  AcctStartTime datetime NOT NULL default '0000-00-00 00:00:00',
  AcctStopTime datetime NOT NULL default '0000-00-00 00:00:00',
  AcctSessionTime int(12) default NULL,
  AcctAuthentic varchar(32) default NULL,
  ConnectInfo_start varchar(50) default NULL,
  ConnectInfo_stop varchar(50) default NULL,
  AcctInputOctets bigint(12) default NULL,
  AcctOutputOctets bigint(12) default NULL,
  CalledStationId varchar(50) NOT NULL default '',
  CallingStationId varchar(50) NOT NULL default '',
  AcctTerminateCause varchar(32) NOT NULL default '',
  ServiceType varchar(32) default NULL,
  FramedProtocol varchar(32) default NULL,
  FramedIPAddress varchar(15) NOT NULL default '',
  AcctStartDelay int(12) default NULL,
  AcctStopDelay int(12) default NULL,
  ArubaLocationId varchar(11) NOT NULL default '',
  ArubaUserRole varchar(30) NOT NULL default '',
  ArubaUserVlan int(4) default NULL,
  ClientIPAddress varchar(15) NOT NULL default '',
  PRIMARY KEY  (RadAcctId),
  KEY UserName (UserName),
  KEY FramedIPAddress (FramedIPAddress),
  KEY AcctSessionId (AcctSessionId),
  KEY AcctUniqueId (AcctUniqueId),
  KEY AcctStartTime (AcctStartTime),
  KEY AcctStopTime (AcctStopTime),
  KEY NASIPAddress (NASIPAddress)
) ;
```

Se crea la tabla con la ejecución de la instrucción:

```
mysql -uroot -p radius < tablasRiu.sql
```

Se crea un usuario con el que el servidor RADIUS realiza la conexión al servidor MySQL:

Para este ejemplo se usa:

Usuario: *wireless*
Contraseña: *UnPwdFuerte*

```
mysql -uroot -p
mysql>  GRANT  SELECT,INSERT,UPDATE  ON  radius.*  TO  'wireless'@'localhost
'IDENTIFIED BY 'UnPwdFuerte';
```

6.1.4. FreeRADIUS

6.1.4.1. Compilación e instalación

Se mueve el archivo al /usr/src y se desempaqueta:

```
mv freeradius-1.1.7.tar.gz /usr/src/
cd /usr/src
tar xzvf freeradius-1.1.7.tar.gz
cd freeradius-1.1.7
```

A diferencia de la instalación básica se establecen más opciones en la configuración de la instalación:

--prefix:	Establece la ruta en donde se instalará FreeRADIUS
--with-logdir:	Especifica la ruta donde se quiere guardar las bitácoras del servidor radius.
--with-radacctdir:	Especifica la ruta donde se quiere guardar los registros de accounting del servidor.
--with-ldap:	Establece el uso de los módulos de ldap
--with-rlm-ldap-include-dir y	
--with-rlm-ldap-lib-dir:	Especifican los directorios donde se tienen las librerías e includes ldap, respectivamente

Todo el comando se ejecuta en una sola línea:

```
./configure --prefix=/usr/local/radius --with-logdir=/var/log/radius --with-
radacctdir=/var/log/radius/radacct --with-ldap --with-rlm-ldap-lib-
dir=/usr/local/ldap/lib --with-rlm-ldap-include-dir=/usr/local/ldap/include
```

Se compila e instala con los siguientes comandos:

```
make
make install
```

Las librerías se instalan en:
/usr/local/radius/lib

Se edita el archivo **/etc/ld.so.conf,** y se agrega la siguiente entrada:

```
/usr/local/openssl/lib
/usr/local/radius/lib
```

Para que se actualicen los cambios que se realizan en el archivo *ld.so.conf*, se ejecuta el comando:

```
ldconfig
```

6.1.4.2. Configuración de FreeRADIUS

radiusd.conf

En este archivo se agrega la sección “ldap”, en donde se establecen los parámetros de conexión entre el servidor RADIUS y el servidor LDAP.

```
   log_auth = yes

   mschap
   {
            use_mppe = yes
            require_encryption = yes
            require_strong = yes
   }

ldap {
            server = "localhost"
            identity = "cn=Manager,dc=unam,dc=mx"
            password = wireless
            basedn = "ou=usuarios,ou=wireless,dc=unam,dc=mx"

            filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
            base_filter = "(objectclass=radiusprofile)"

            start_tls = no
      #     access_attr = "dialupAccess"

            dictionary_mapping = ${raddbdir}/ldap.attrmap
            ldap_connections_number = 5

            password_attribute = userPassword
            edir_account_policy_check=no
            groupname_attribute = cn
            groupmembership_filter                                          =
"(|(&(objectClass=GroupOfNames)(member=%{Ldap-
UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-UserDn})))"
            groupmembership_attribute = radiusGroupName
            timeout = 4
            timelimit = 3
            net_timeout = 1

      }
```

NOTA: Es importante comentar la línea `access_attr = "dialupAccess".` Todas las líneas que no se muestran en el párrafo o tienen que estar comentadas o eliminadas.

```
authorize
{
      preprocess
      mschap
      suffix
      eap
      files
      ldap
}

authenticate
{
      Auth-Type MS-CHAP
      {
            mschap
      }
      eap
}
accounting {
      detail
      unix
      radutmp
      sql
}
```

clients.conf

Se agregan los NAS o clientes del servidor RADIUS, en este caso la dirección IP de los controladores ARUBA, se muestran las dos formas de agregar: incluyendo todo el segmento al que pertenece el controlador o únicamente su dirección IP en particular:

Todo un segmento:

```
client xxx.yyy.zzz.0/24
{
      secret      = secreto
      shortname   = wlan
}
```

Sólo la dirección IP:

```
client xxx.yyy.zzz.aaa {
        secret          = secreto
        shortname       = wlan
}
```

users

En este archivo se asignan los diferentes niveles de acceso de usuarios, el servidor consulta a la base de datos LDAP, si el usuario en proceso de autenticación tiene el atributo de grupo “estudiantes” el servidor le asigna el role “ESTUDIANTE”, si tiene el atributo de grupo “academicos” el servidor le asigna el role “ACADEMICO” y si tiene el atributo de grupo “staff” el servidor le asigna el role “STAFF”, dicha información es procesada por el controlador ARUBA.

```
DEFAULT         Ldap-Group == estudiantes, Simultaneous-Use := 1
              Aruba-User-Role = "ESTUDIANTE",


DEFAULT         Ldap-Group == academicos, Simultaneous-Use := 1
              Aruba-User-Role = "ACADEMICO",

DEFAULT         Ldap-Group == staff, Simultaneous-Use := 1
              Aruba-User-Role = "STAFF",
```

eap.conf

Se busca la directiva *default_eap_type* y se le cambia el valor por *peap:*

```
default_eap_type = peap
```

En la sección *tls* en este caso, a diferencia de la configuración básica se utilizará un certificado emitido por una entidad certificadora real.

```
tls {
              private_key_password = wirelessriu
              private_key_file = ${raddbdir}/certs/nombreservidor.riu.unam.mx.key
              certificate_file = ${raddbdir}/certs/ nombreservidor.riu.unam.mx.crt
              CA_file = ${raddbdir}/certs/ nombreservidor.riu.unam.mx.crt

             dh_file = ${raddbdir}/certs/dh
             random_file = ${raddbdir}/certs/random

             }
```

Finalmente se activa *EAP-peap,* quitando los comentarios a las líneas correspondientes de la sección *peap:*

```
peap {
    default_eap_type = mschapv2
    }
```

sql.conf

En este archivo de configuración se definen los parámetros necesarios para la conexión con la base de datos "*radius"* en el servidor MySQL y define los *"queries"* que realiza a la base de datos. FreeRADIUS puede utilizar a un servidor MySQL ya sea para la autenticación, autorización y accouting de usuarios. Aquí se describirá sólo el uso que se hace para el accounting ya que para la autenticación y autorización se hace uso de la ayuda de la base de datos LDAP.

Se definen los parámetros para la conexión al servidor MySQL, los valores tiene que ser los que se usaron en la sección anterior:

```
server = "localhost"
login = "wireless"
password = " UnPwdFuerte "
radius_db = "radius"
```

Se especifica la tabla de accounting, acct_table1 se utiliza para almacenar todos los usuarios que iniciaron una conexión, independientemente de que el NAS no envíe los registros de fin de conexión; acct_table2 alojará los registros en los cuales hubo fin de conexión.

En este ejemplo, indicamos que los dos tipos de registros se almacenen en la misma tabla.

```
acct_table1 = "conexiones"
acct_table2 = "conexiones"
```

En una red inalámbrica grande como es el caso de la RIU, en donde existen muchos registros por segundo, es necesario mantener el servidor escuchando por varios sockets; la variable *num_sql_socks* permite definir este valor; 20 sockets ha sido suficiente hasta el momento en que se ha elaborado este documento.

```
num_sql_socks = 20
```

Se busca la sección *Accounting Queries,* en donde se localizan los queries que ejecuta el servidor Radius para poblar la tabla de accounting, en este ejemplo específico, la tabla se llama: *conexiones.*

```
accounting_onoff_query
accounting_update_query
accounting_update_query_alt
accounting_start_query
accounting_start_query_alt
accounting_stop_query
accounting_stop_query_alt
```

Se ha observado que los queries tipo *"start"*, realizan registros que no son tan útiles para cuestiones estadísticos, sobre todo en redes muy grandes, para la RIU, se deshabilita este tipo de queries (se comentan las líneas correspondientes a `accounting_start_query, accounting_start_query_alt`).

En este caso en particular, sólo se ha encontrado utilidad en los queries tipo *stop*. Se tienen que agregar los 4 atributos que se añadieron en la creación de la tabla *conexiones.*

Los queries quedan de la siguiente manera:

```
      accounting_stop_query = "UPDATE ${acct_table2} SET AcctStopTime = '%S',
AcctSessionTime = '%{Acct-Session-Time}', AcctInputOctets = '%{Acct-Input-
Octets}', AcctOutputOctets = '%{Acct-Output-Octets}', AcctTerminateCause =
'%{Acct-Terminate-Cause}',      AcctStopDelay      =      '%{Acct-Delay-Time}',
ConnectInfo_stop = '%{Connect-Info}' WHERE AcctSessionId = '%{Acct-Session-
Id}'  AND  UserName  =  '%{SQL-User-Name}'  AND  NASIPAddress  =  '%{NAS-IP-
Address}'"

      accounting_stop_query_alt = "INSERT into ${acct_table2} (AcctSessionId,
AcctUniqueId,   UserName,   Realm,   NASIPAddress,   NASPortId,   NASPortType,
AcctStartTime,       AcctStopTime,       AcctSessionTime,       AcctAuthentic,
ConnectInfo_start,   ConnectInfo_stop,   AcctInputOctets,   AcctOutputOctets,
CalledStationId,     CallingStationId,     AcctTerminateCause,     ServiceType,
FramedProtocol,      FramedIPAddress,      AcctStartDelay,      AcctStopDelay,
ArubaLocationId,      ArubaUserRole,      ArubaUserVlan,      ClientIPAddress)
values('%{Acct-Session-Id}', '%{Acct-Unique-Session-Id}', '%{SQL-User-Name}',
'%{Realm}',     '%{NAS-IP-Address}',     '%{NAS-Port}',     '%{NAS-Port-Type}',
DATE_SUB('%S',  INTERVAL  (%{Acct-Session-Time:-0}  +  %{Acct-Delay-Time:-0})
SECOND), '%S', '%{Acct-Session-Time}', '%{Acct-Authentic}', '', '%{Connect-
Info}',  '%{Acct-Input-Octets}',  '%{Acct-Output-Octets}',  '%{Called-Station-
Id}', '%{Calling-Station-Id}', '%{Acct-Terminate-Cause}', '%{Service-Type}',
'%{Framed-Protocol}',   '%{Framed-IP-Address}',   '0',   '%{Acct-Delay-Time}',
'%{Aruba-Location-Id}',      '%{Aruba-User-Role}',      '%{Aruba-User-Vlan}',
'%{Client-IP-Address}')"
```

El resto de las directivas quedan intactas.

6.2. Autenticador 802.1x: ARUBA

El objetivo principal de este documento es la implementación de una infraestructura AAA capaz de funcionar con cualquier marca o fabricante de equipos 802.11(b,a,g o n) por lo que no se muestran los detalles de la configuración específica que se tiene en el switch controlador Aruba para la RIU, sólo algunas características como funcionalidades que permiten conseguir una red inalámbrica con seguridad 802.11i/WPA así también las que proporcionan diferentes categorías de acceso.

Niveles de acceso

Los niveles de acceso se consiguen por medio de roles que agrupan políticas conformadas por una ó mas reglas de firewall.

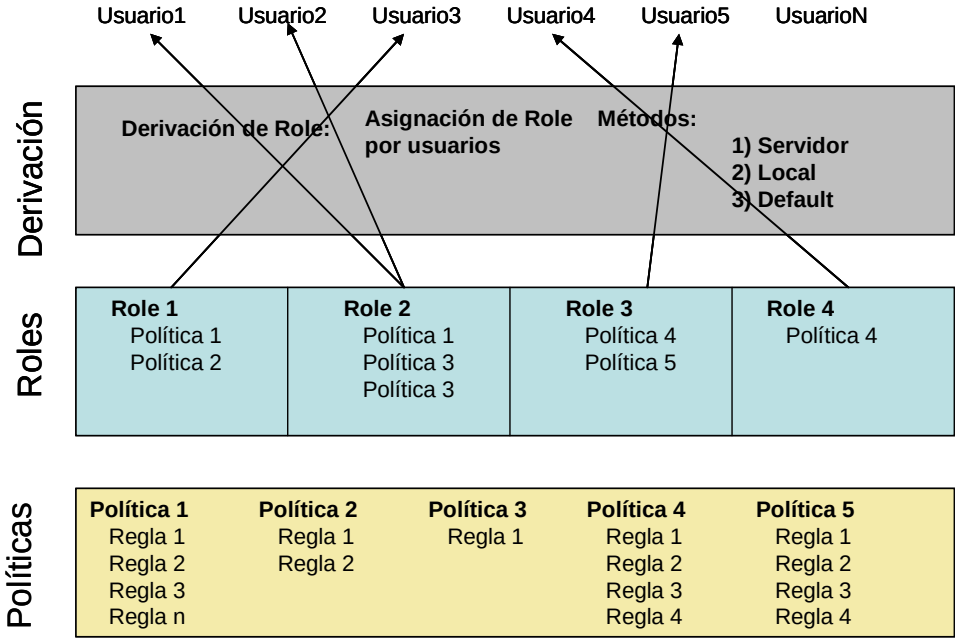

Figura 6.2. Conformación de las categorías de acceso

Las reglas de Firewall

Configuración de las reglas de firewall

- Las reglas pueden ser identificadas por nombre o por número.
- Formato de las reglas de firewall.

```
<Origen> <destino> <servicio> <acción> <acción extendida>
```

- Se pueden usar aliases para Origen, destino y servicio
    - Simplifica configuración repetitiva e incrementa legibilidad.

Aliases Pre-configuradas

Origen:

user

- Automáticamente representa la IP del usuario
    - Solamente se usa en las políticas de firewall

mswitch

- Representa la IP del switch controlador de Aruba.

Destino:

netdestination

- Host
- Rango de host
- Red

Servicio :

netservice

Ejemplos :

```
netservice svc-http tcp 80
```

- Define un servicio llamado “svc-http” que usa el puerto TCP 80

```
netservice svc-bootp udp 67 68
```

- Define un servicio llamado “svc-bootp” que usa los puertos UDP 67 y 68

```
netservice svc-esp 50
```

- Define un servicio llamado “svc-esp” que usa el protocolo IP número 50 (IPSec).

Acciones

- deny (drop en Web UI)
  - bloquea el tráfico.
- reject
  - bloque el tráfico y envía un mensaje ICMP al origen.
- permit
  - Permite el tráfico.
- src-nat
  - NAT/PAT tradicional.
- dst-nat
  - Cambia IP destino a la dirección de loopback del controlador.
  - Puede redirigir a puertos destino.
  - Se usa en el portal captivo para redirigir las sesiones http.
  - Puede captura los túneles VPN y terminarlas en el switch local.

Acciones avanzadas

- dot1p-priority. Asigna prioridad 802.1p
- log. Genera bitácora si la reglas es aplicada
- position. Se usa para insertar reglas dentro de las políticas.
- time-range. Se usa en políticas basadas en tiempo
- tos. Establecer prioridad de tráfico en el encabezado IP

Políticas

- Una política es un conjunto de reglas de firewall, que definen diferentes niveles de seguridad en los accesos a los recursos de red.
- Las reglas en una política deben ser escritas de la más específica a la menos específica.
- Las políticas deben ser escritas con aliases siempre que sea posible.

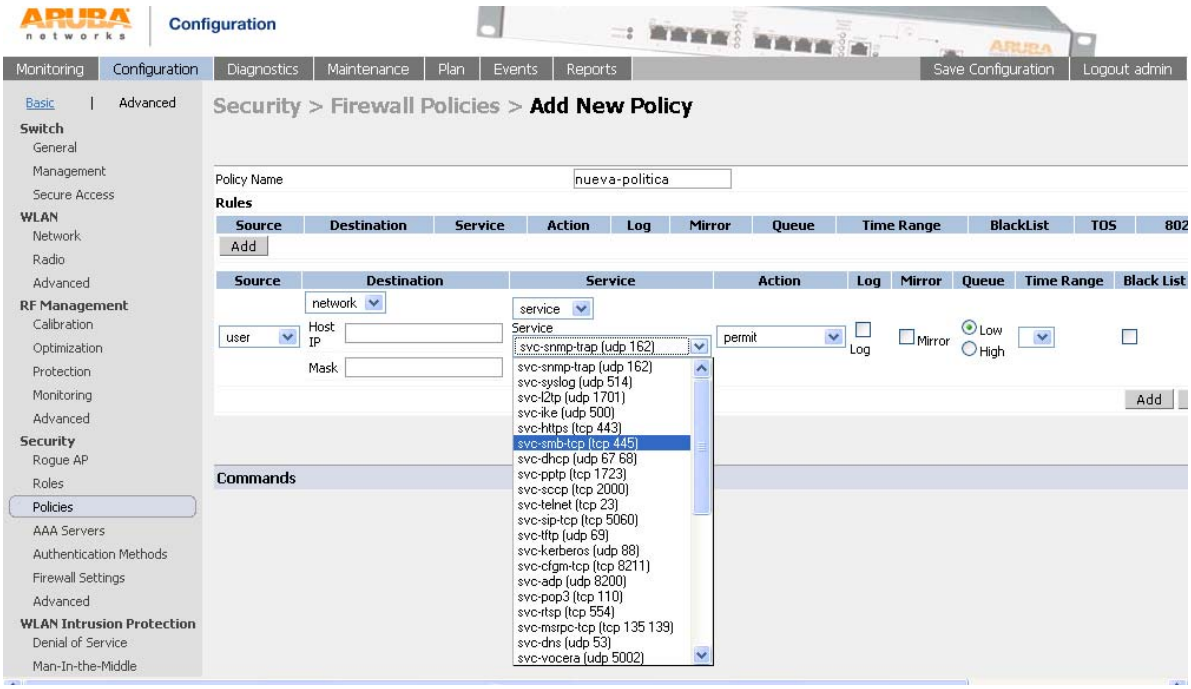

Figura 6.3. Creación de políticas

Roles

Los roles determinan derechos de acceso y obedecen a las políticas establecidas:

- Cada role tiene uno o más políticas de firewall aplicadas
- Las políticas de firewall son ejecutadas en orden
- La política final implícita es siempre “deny all”

Los roles definen los recursos a los cuales los usuarios tienen acceso.

Los roles pueden ser asignados de varias formas:

- Asignación default, de acuerdo al método de acceso (802.1x, VPN, WEP, etc.)
- Derivación por servidor.
    - Atributos RADIUS/LDAP
- Derivación Local
    - ESSID
    - MAC
    - Tipo de cifrado
    - Etc.

NOTA: El controlador Aruba siempre asigna un role a cada usuario que accede a la red inalámbrica.

Planeación de accesos basados en roles

Se pueden crear tantos roles como sean necesarios, algunos ejemplos de roles: *empleados, invitados, ingeniería, ventas, finanzas, staff, etc*.

Como ya ha se mencionado en secciones anteriores la RIU maneja roles diferentes de acceso: ESTUDIANTES, ACADEMICOS y STAFF.

Cómo se crea un role

Desde el CLI:

Se crea un role "ESTUDIANTE" y se aplica una política de firewall llamada "*estudiantes-acl*".

```
user-role ESTUDIANTE
     session-acl estudiantes-acl
```

Desde la Web UI:

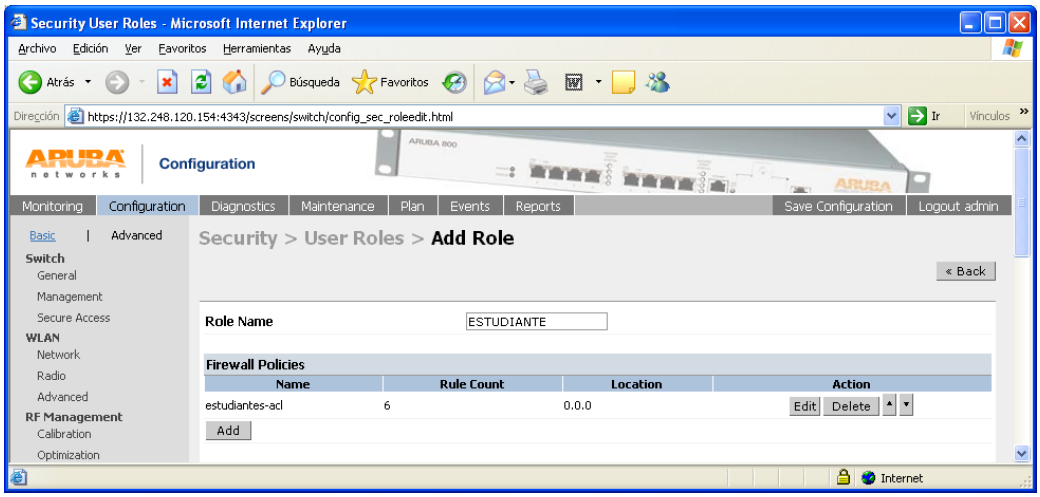

Figura 6.4. Creación de roles

Asignación de Roles por medio de un servidor RADIUS

La RIU usa la asignación de role por derivación de servidor. El servidor RADIUS se configura de tal forma que regresa un atributo con el nombre del role que le corresponde, tal como se dio de alta el usuario en la base de datos LDAP.

Existen dos formas de realizar la derivación, el primer es el que se emplea en la RIU:

- Si el servidor RADIUS regresa el nombre del role configurado en el switch controlador, se usa la siguiente derivación de regla:

```
aaa derivation-rules server NombreServidor
set role condition Class value-of
```

Donde `NombreServidor` es el nombre del servidor RADIUS

- Si el servidor RADIUS regresa un nombre distinto al de un role configurado en el switch controlador, se tiene que usar una derivación de regla distinta.

```
aaa derivation-rules server NombreServidor
set role condition Filter-ID equals alumno set-value ESTUDIANTE
```

Si esta regla encuentra en el atributo Filter-ID el valor “alumno”, asigna el role llamado ESTUDIANTE.

Configuración de los protocolos WPA/802.11i

Agregar un servidor RADIUS

Se accede a ***Security > AAA servers > Radius Servers > Add Radius Server***

Se agrega el nombre y la dirección IP del servidor en donde se encuentra instalado el servidor RADIUS, la llave secreta, tiene que ser la misma de la que se agrega en el archivo de configuración clients.conf y mantener los puertos 1812 y 1813 para la autenticación y accounting, respectivamente.

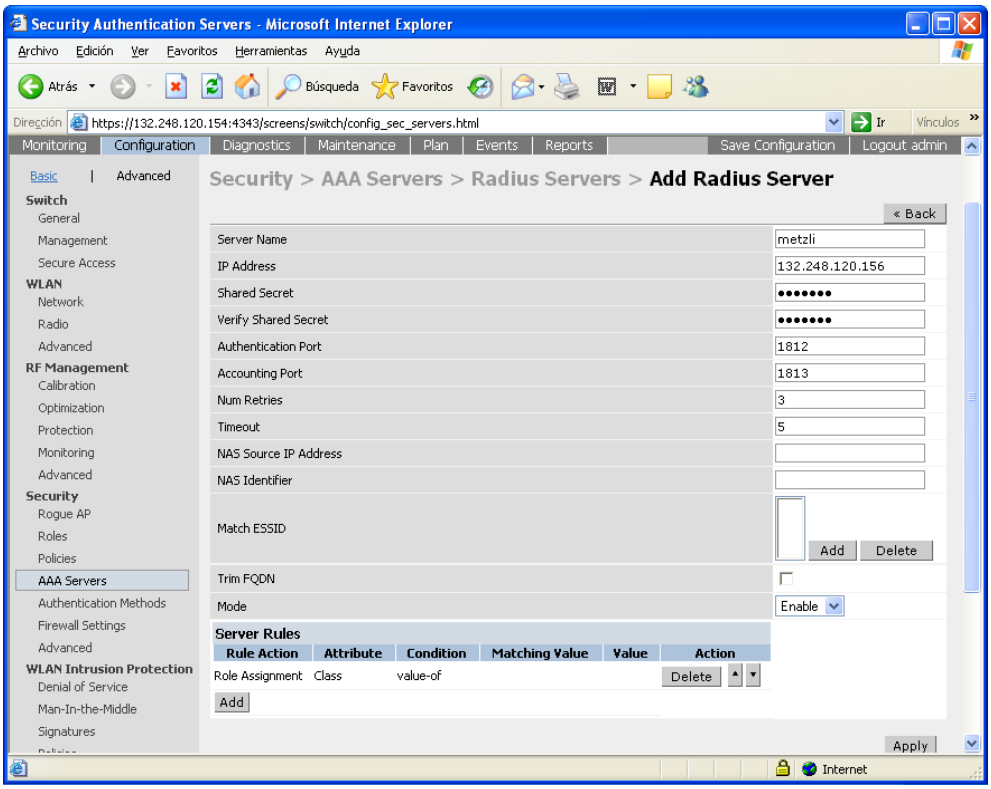

Figura 6.5. Configuración del servidor RADIUS

Selección de método de autenticación 802.1X

Se accede a ***Configuration → Security → Authentication Methods → 802.1x Authentication.***

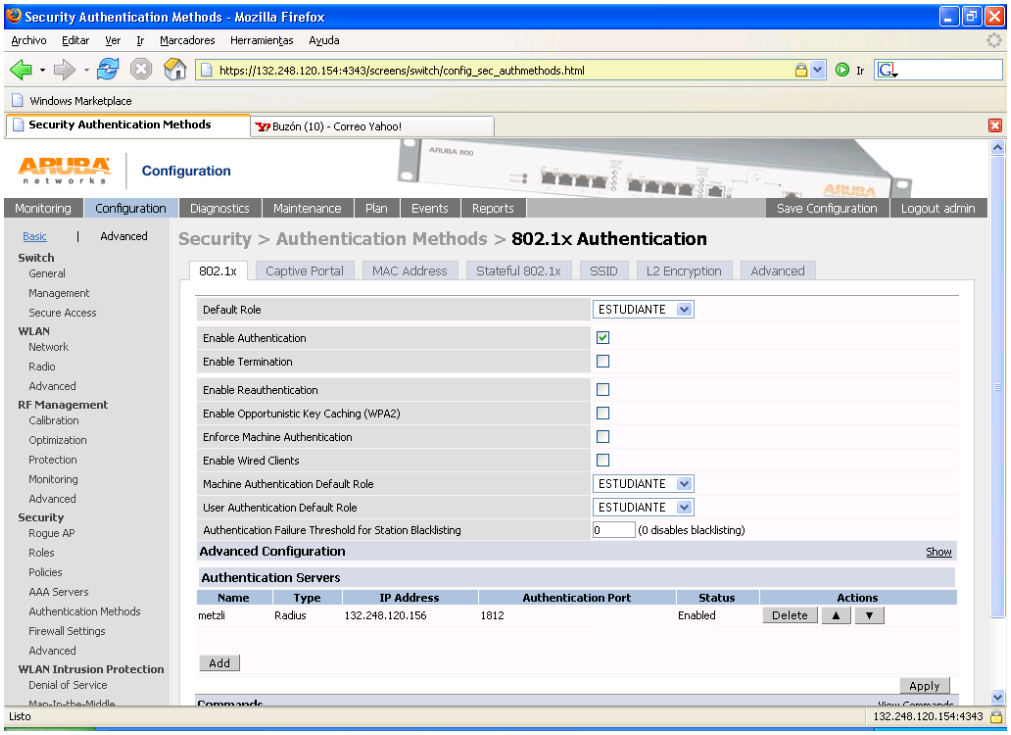

Figura 6.6. Selección del método de autenticación

Se asigna el role ESTUDIANTE como el role por default, si en el algún momento se agrega un usuario a la base de datos LDAP sin ninguna categoría o grupo, el servidor RADIUS no regresa ningún valor, por lo que el switch controlador le asignará el role ESTUDIANTE por default. Se agrega RADIUS como servidor de autenticación 802.1X.

Configuración WPA/WPA2

El controlador Aruba permite la creación de diferentes SSID's, cada de uno de los cuales puede ser configurado con distintos protocolos de seguridad, para la RIU, sólo existe una SSID (RIU) y por el momento se ha elegido WPA Corporativo, con la idea de pasar a WPA2 en un futuro, cuando se considere que todos los equipos de los usuarios soporten el cifrado AES.

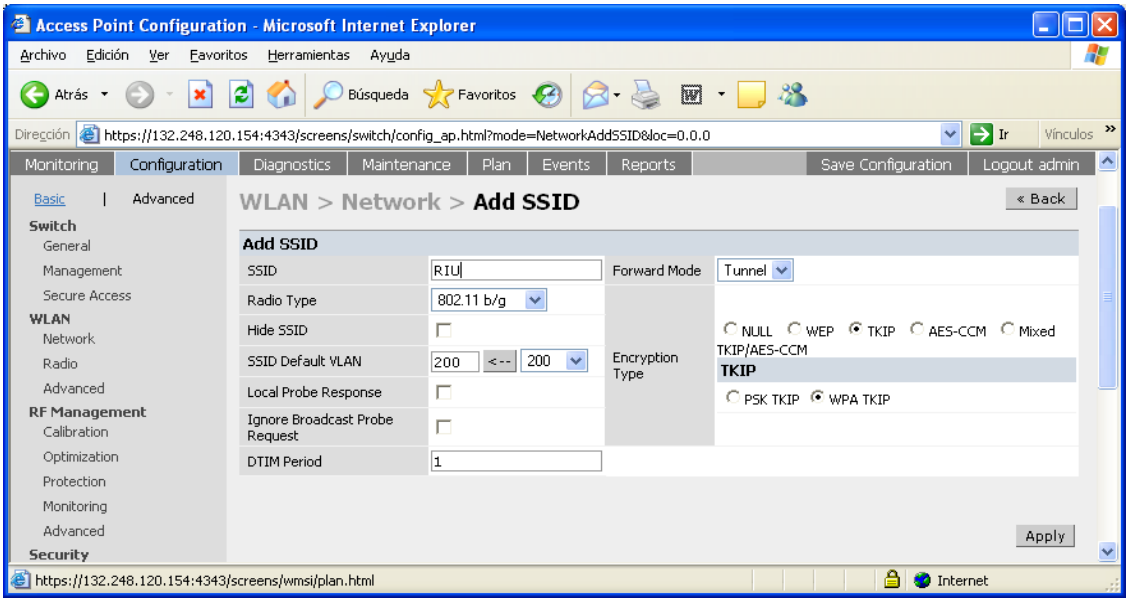

Figura 6.7. Configuración del SSID

Notas:

Las configuraciones en el controlador ARUBA anteriormente mostradas son a manera de ejemplo, sólo para mostrar las funcionalidades necesarias para conseguir la implementación de seguridad. La configuración real varía mucho y no es el objetivo de este trabajo.

El controlador ARUBA desconoce de los detalles EAP, es decir, es transparente el tipo EAP utilizado.

6.3. Suplicante 802.1x

En primer lugar, para que una estación o dispositivo pueda formar parte de una WLAN, tiene que contar con una interfaz de red inalámbrica 802.11, en su gran mayoría integrada en el equipo, pero también puede ser externa como una tarjeta PCMCIA o USB.

En los sistemas Windows XP SP2 y Vista al igual que el sistema operativo MacOS X tienen integrado el suplicante 802.1X. En los sistemas GNU/Linux algunas veces se tiene que instalar manualmente el suplicante; el más común es el *WPA_Supplicant*.

El los dispositivos de tipo *Handsets* como PDA's, celulares, etc. Una gran parte de ellos cuentan con una interfaz 802.11, pero desafortunadamente un gran número de ellos no soportan los protocolos *WPA Corporativo,* haciendo imposible su conexión a la RIU o a una red inalámbrica con seguridad WPA/802.11i.

6.4. Pruebas

Mucho tiempo antes del despliegue de la RIU, el diseño y la implementación del sistema de autenticación AAA estuvo listo, porque fue un componente muy importante para la evaluación de los diferentes fabricantes que participaron durante el proceso de selección de la tecnología adecuada. Los fabricantes que concursaron fueron: Aruba, Enterasys, Colubris y Foundry.

Los aspectos a evaluar que conciernen directamente a este proyecto fueron:

- Niveles de Acceso
- Soporte de todas las alternativas posibles de protocolos de seguridad en las redes inalámbricas 802.11.

Protocolo de seguridad / **Método De Autenticación**	**WPA ó TSN Cifrado: TKIP**	**802.11i ó WPA2 Cifrado: AES**
TLS	WPA/TLS	WPA2/TLS
PEAP	WPA/PEAP	WPA2/PEAP
TTLS	WPA/TTLS	WPA2/TTLS

Tabla 6.1 Soluciones de seguridad en las WLAN

Niveles de Acceso

Objetivo: Evaluar que sean asignados los atributos correspondientes a cada tipo de usuario definido.

Procedimiento: Se generan perfiles de usuario (ACADEMICO, ESTUDIANTE y STAFF. Se conecta a la red cada uno de ellos y se verifica que les sean asignados diferentes niveles de acceso, como por ejemplo:

- Rate-limit por tipo de usuario.
- Asignación de Vlan diferente a cada tipo de usuario.
- Permisos para uso de aplicaciones por tipo de usuario.

No todos los fabricantes lograron pasar esta prueba (se establecieron cartas de confidencialidad por lo que no esta permitido publicar los resultados), pero la falla fue responsabilidad de las marcas y no del servidor de autenticación.

Mecanismos de Autenticación

Objetivo: Evaluar que la integración del sistema AAA con los equipos inalámbricos de los fabricantes soportara cada una de las soluciones mostradas en la tabla 6.1.

Procedimiento: Se realizan las configuraciones al suplicante (equipo del usuario con interfaz inalámbrica con soporte de los protocolos WPA/WPA2) para establecer cada una de la opciones de seguridad mostradas en la tabla 6.1, de igual forma se realizan los cambios en el servidor de autenticación para usar uno u otro método de autenticación, así también el fabricante tiene que hacer los cambios pertinentes para realizar cada una de las pruebas.

La integración de servidor de autenticación con los equipos de los fabricantes para las pruebas de los mecanismos de autenticación, todos logran la conexión con éxito utilizando cada una de las opciones requeridas. Además de los fabricantes mencionados, las marcas Avaya y Cisco también logran pasar con éxito este tipo de pruebas, aunque dichas marcas no fueron parte del proceso de selección.

Equipo Utilizado en las pruebas:

2 Laptops con Windows XP
1 Laptop con Linux
1 Laptop con Windows 98
1 Tarjetas de red inalámbrica Orinoco (WEP-64)
1 Tarjeta de red inalámbrica Linksys (WEP-128)
1 Tarjeta de red inalámbrica Zonet (WPA)
1 PC con tarjeta inalámbrica y Win 98.
1 Servidor de Autenticación RADIUS
1 Servidor LDAP
1 Servidor MySQL
4 AP del fabricante a evaluar
1 Switch del fabricante a evaluar
1 Hub

Como se ha mencionado, la marca que se elige para el despliegue de la red inalámbrica fue Aruba y se mantuvo unas semanas en fase de prueba y en ese periodo no se presentaron problemas considerables en la integración con el servidor RADIUS.

CONCLUSIONES

CONCLUSIONES

En primer lugar con este trabajo se logra conjuntar información importante acerca de la seguridad de las redes inalámbricas por lo que resulta útil como material de apoyo o de consulta para todas aquellas personas que quieren iniciar o ampliar sus conocimientos en dicha área de las telecomunicaciones.

Además de la información teórica se presentan con detalle los elementos necesarios, las aplicaciones específicas, los procedimientos y las configuraciones necesarias para conseguir una implementación de seguridad en las WLAN mostrando cómo lograrlo utilizando alguno de los tres métodos de autenticación más importantes en redes inalámbricas: EAP-TLS, EAP-PEAP y EAP-TTLS, el escenario de implementaciones que se exponen funcionaron con todas las marcas de equipos 802.11 que se probaron antes del despliegue de la Red Inalámbrica Universitaria (RIU).

La solución que se propuso para la RIU, cumplió con el objetivo de establecer una red inalámbrica con los nuevos protocolos de seguridad que define el estándar 802.11, funcional, escalable y administración centralizada.

El sistema de seguridad que se propuso e implementó para la RIU es fácil de escalar, es decir, se contempló la migración posterior del protocolo WPA a WPA2, dicho cambio será transparente para el sistema, incluso los cambios serían mínimos si se pretendiera agrega equipos de otros fabricantes (Diferentes a la marca ARUBA).

En un futuro mucho más lejano será factible el uso del método de autenticación EAP-TLS, en este caso se requerirá algunos cambios en la configuración del servidor, pero muy ligeros.

Unas de las grandes ventajas de la solución es que permite una administración centralizada de la infraestructura lo que implica una administración entre otras cosas centralizada de los usuarios de la red inalámbrica, esto es una gran beneficio considerando el tamaño de la red inalámbrica, el tamaño de los espacios geográficos que pretende cubrir (Facultades, Institutos y Dependencias

de Ciudad Universitaria, todas las FES: Aragón, Iztacala, Acatlán, Zaragoza y Cuautitlán) así como el número de usuarios de la red inalámbricas.

El sistema de autenticación junto con el controlador ARUBA logró el objetivo de permitir diferentes categorías de usuarios con distintos niveles de acceso a los recursos de la red.

El sistema ha funcionado dentro de niveles aceptables considerando el tamaño de la Red.

Actualizaciones a nuevas versiones de las aplicaciones que conforman el sistema: empezando por el sistema operativo, las librerías OpenSSL, el servidor de aplicación FreeRADIUS, el servidor de directorios para el repositorio de usuarios OpenLDAP y la base de datos MySQL en donde se concentran los registros de accounting o contabilidad de conexiones en la RIU.

Implementación de cifrado TLS entre el servidor Radius (FreeRADIUS) y el servidor de directorios OpenLDAP.

Aprovechar la funcionalidad de redundancia de forma automática entre el servidor Radius con el servidor de directorios OpenLDAP y con la base de datos MySQL.

El sistema de autenticación fue implementado en base a software libre: desde el sistema operativo y todas las aplicaciones que lo conforman, lo que representa ahorros monetarios en pagos de licencia que significaría una solución con software comercial.

Obtención de estadísticas de forma sencilla, rápida y específica toda vez que los registros de conexiones se almacenan en un servidor de base de datos MySQL, dichas estadísticas resultan muy útiles para los administradores de la red, porque permite diagnosticar entre otras cosas la carga de usuarios en los diferentes puntos de acceso, el consumo de ancho de banda, etc.

Las tecnologías de redes inalámbricas 802.11 (b,a,g y n) se han consolidado fuertemente en el mercado y constantemente se está mejorando, lo anterior permite que la Red Inalámbrica Universitaria espere un largo periodo de vida, gracias además a la característica de escalabilidad que se contempló en un inicio.

Apéndice A

CONFIGURACIÓN DEL AUTENTICADOR 802.1X: AP AVAYA

Apéndice A. Configuración del autenticador: AP Avaya

Configuración

1. Se entra a la interfaz de configuración vía WEB.
2. Agregar parámetros del Servidor RADIUS.
   a. Dentro del menú principal, se accede a la parte de configuración, haciendo click sobre el botón *Configure* y posteriormente en la pestaña *RADIUS Profiles*.
   b. Se selecciona el perfil *autenticación EAP* y después se hace click sobre el botón *Edit.*(véase figura A.1).

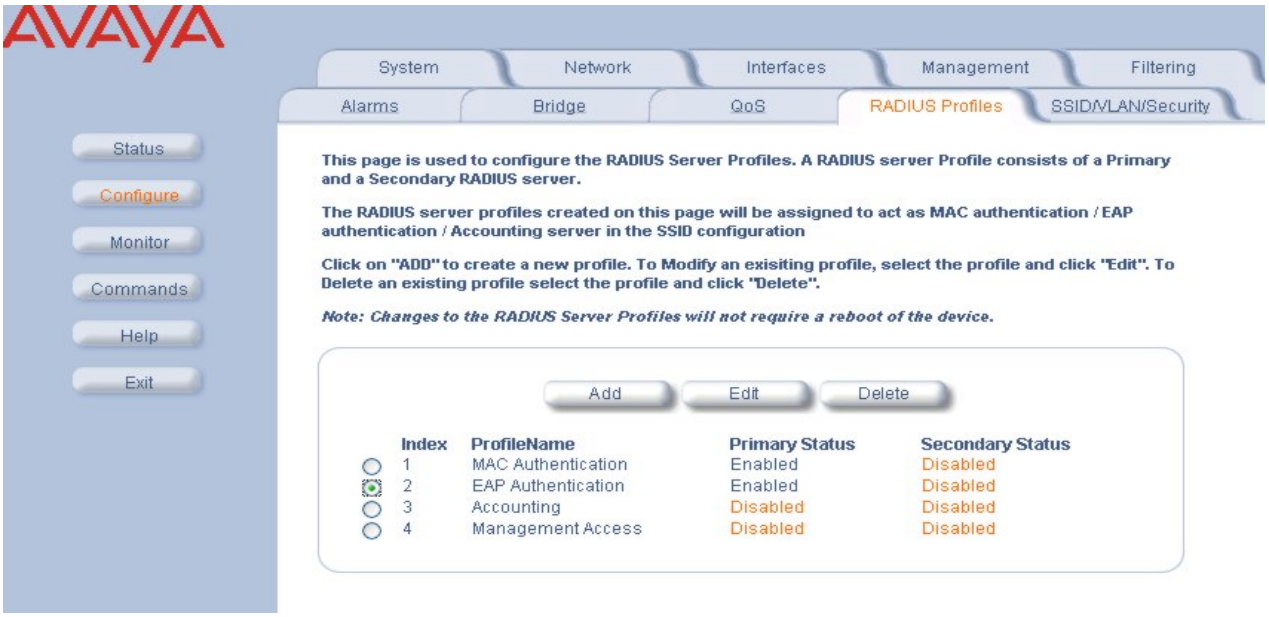

Figura A.1. Configuración: Autenticación EAP

   c. Se Coloca la dirección IP del servidor RADIUS, el puerto 1812 y una clave dentro del campo de *Shared Secret*, como se muestra en la figura A.2. La clave debe coincidir a la que se asigna a la variable "secret" del archivo de configuración *clients.conf*.

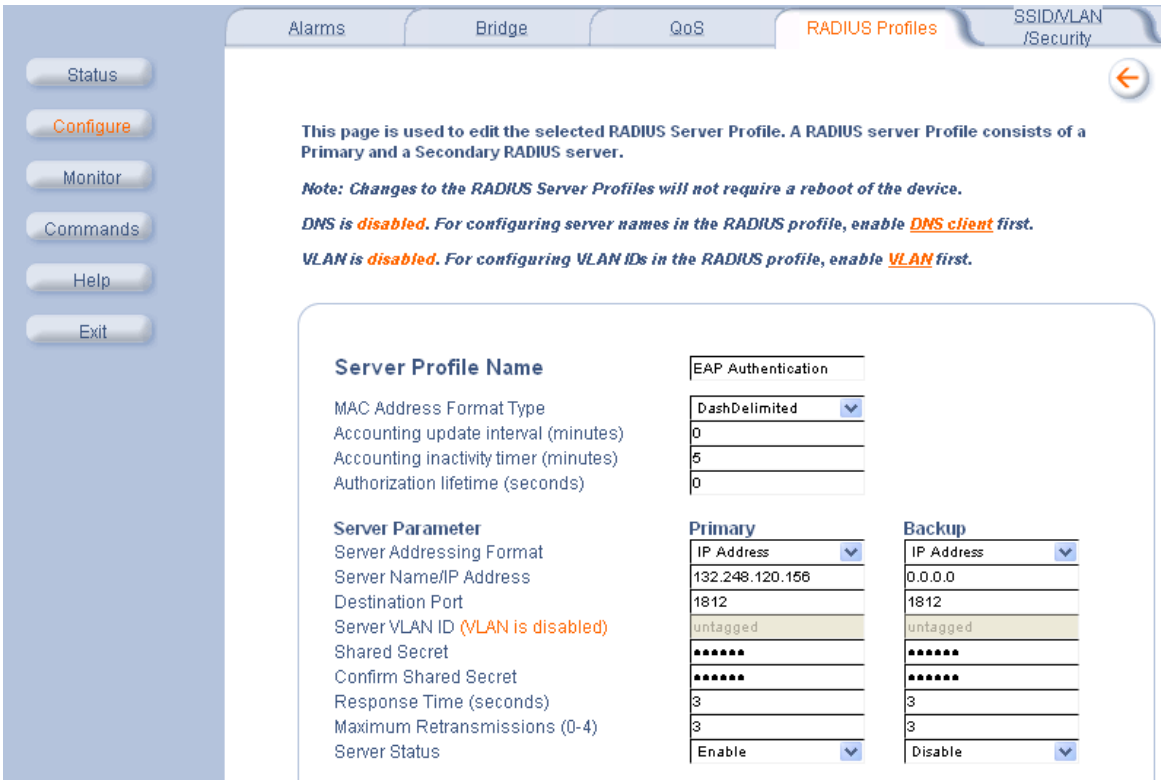

Figura A.2. Configuración: Servidor RADIUS

3. **Configuración de WPA-Corporativo**
   - **a.** Se entra a **Configure** >>**SSID/VLAN/Security>>Security profile,** como se observa en la figura A.3.

Figura A.3. Configuración: Perfil de seguridad

   - **b.** Se selecciona y edita un perfil o se puede agregar uno nuevo, en este ejemplo se edita el perfil 1.
   - **c.** Se elige únicamente la opción *WPA Station* (véase figura A.4).

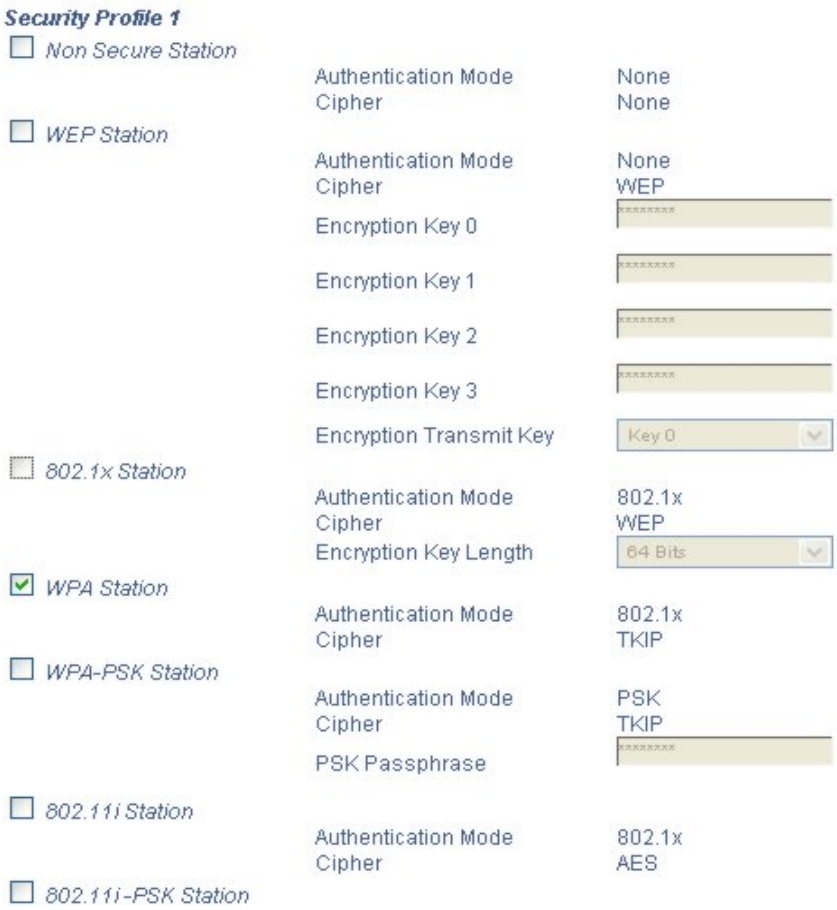

Figura A.4. Configuración: seguridad WPA

4. **Asignación de los perfiles de seguridad a una interfaz**
   - **a.** Se aplica las configuraciones anteriores a la interfase B del Access Point, que es la que se utiliza en este caso en específico.
   - **b.** Se selecciona la pestaña **Configure**>>**SSID/VLAN/Security**>>**Wireless-B**, como se indica en la figura A.5.Es importante asignar el perfil de seguridad (Security Profile) correcto, se recuerda que en este ejemplo se utiliza el 1. También hay que tener cuidado con el perfil de autenticación EAP.

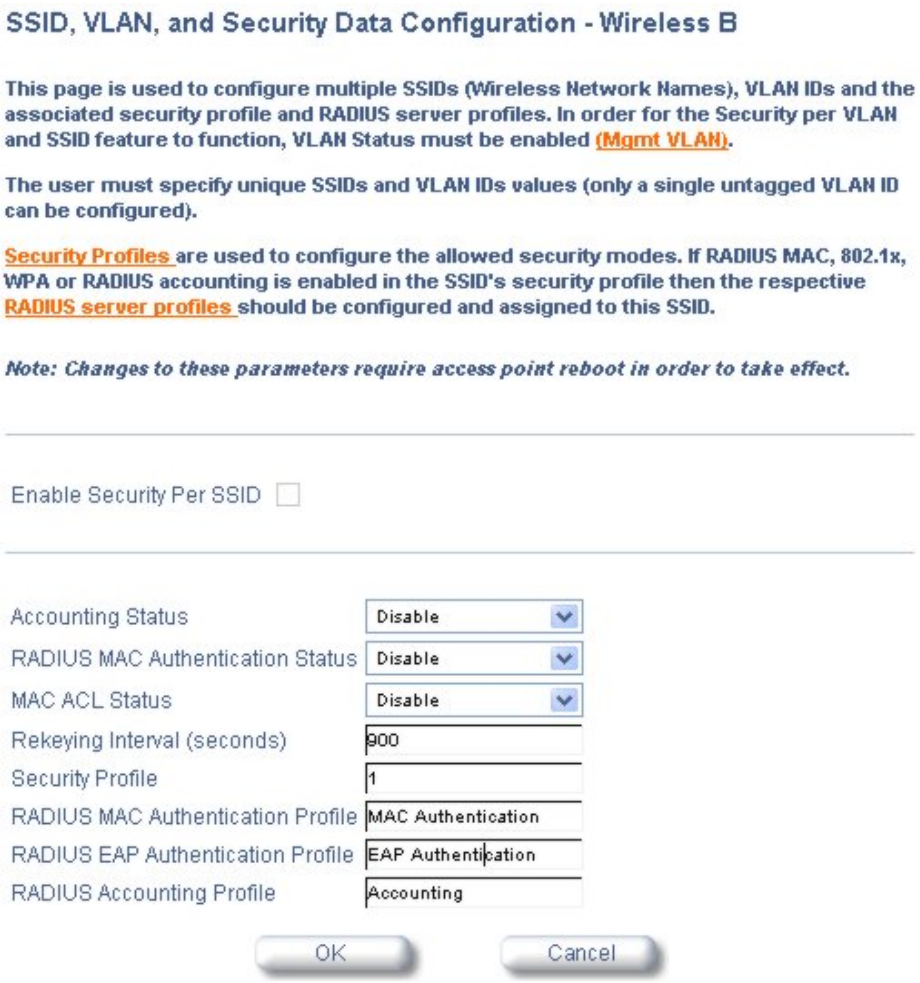

Figura A.5. Configuración: Asignación de perfiles.

5. **Reinicio del Acess Point**
   - **a.** Se selecciona **Commands >> Reboot** y se presiona el botón de **Reboot** para que los cambios hechos en el access point tomen efecto.
   - **b.** El Access Point ya es capaz de manejar WPA.

Apéndice B

CONFIGURACIÓN DEL SUPLICANTE O CLIENTE 802.1X

Apéndice B. Configuración del suplicante o cliente 802.1X

Los sistemas operativos Windows XP y Vista trae integrado el suplicante 802.1X, aunque varios fabricantes manejan software compatible con versiones de Windows anteriores.

Windows XP SP2

En esta sección se muestra como configurar el dispositivo inalámbrico (wireless NIC o tarjeta PCMCIA) el Windows SP2, para poder ser utilizado como cliente 802.1X.

El suplicante 802.1X de Windows XP SP2, maneja la opción de utilizar los mecanismos de autenticación EAP-TLS y EAP-PEAP.

a) Configuración EAP-TLS

Antes de iniciar con la configuración, es necesario la generación e instalación de los certificados: raíz (root.der) y el certificado del usuario como se muestra en la sección *5.3.5 Certificados.*

1. Se hace click con el botón derecho en el icono que aparece en la parte inferior derecha de la pantalla que corresponde a la interfaz de red inalámbrica y se elige *Propiedades.*

2. Se selecciona la pestaña de *Redes inalámbricas*, se hace click sobre el botón *agregar* para agregar y configurar una nueva red inalámbrica (véase figura B.1).

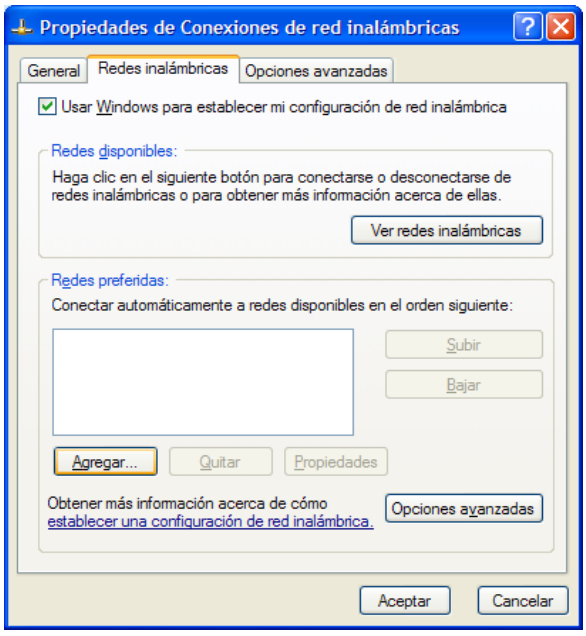

Figura B.1. Configuración dispositivo inalámbrico.

3. Se coloca el nombre o SSID de la red inalámbrica, WPA como Autenticación de red y TKIP como cifrado de datos, como se indica en la figura B.2.

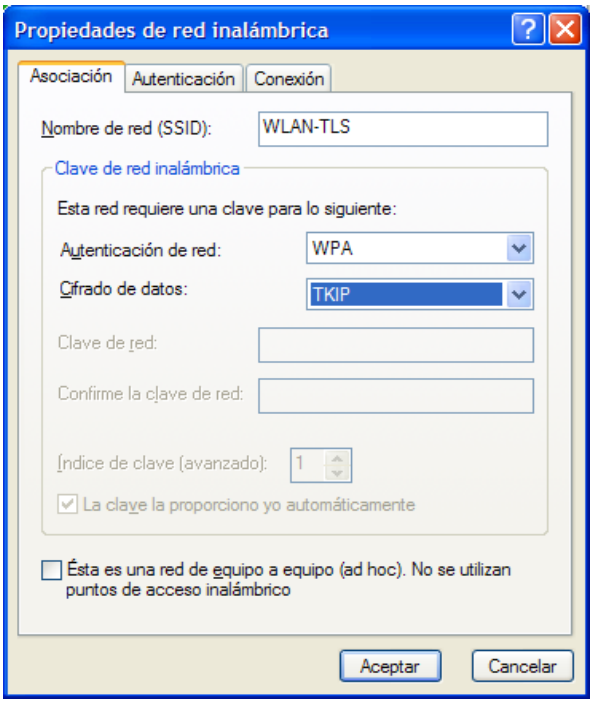

Figura B.2. Configuración: Tipo de autenticación y cifrado

4. A continuación se selecciona la pestaña de Autenticación y se elige la opción ***Tarjeta inteligente u otro certificado*** como tipo de EAP, como se muestra en la figura B.3.

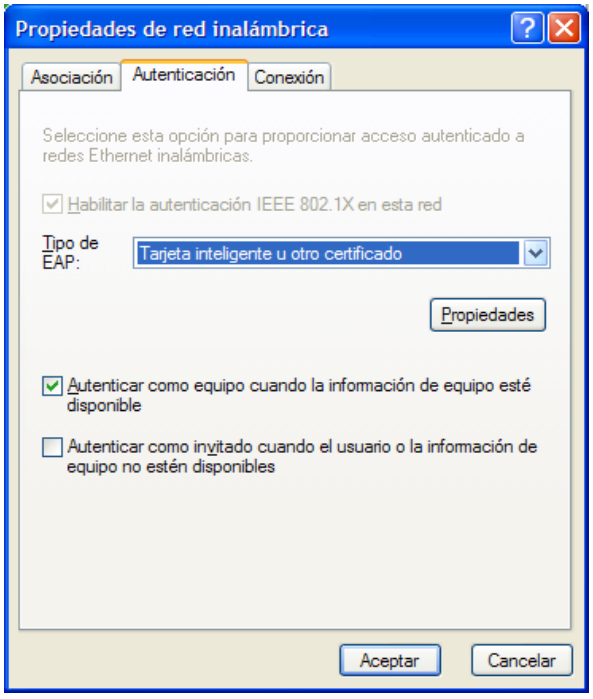

Figura B.3. Configuración: Selección tipo EAP-TLS

5. Posteriormente se hace click sobre el botón Propiedades y se selecciona a DGSCA como entidad emisora raíz de confianza (véase figura B.4)

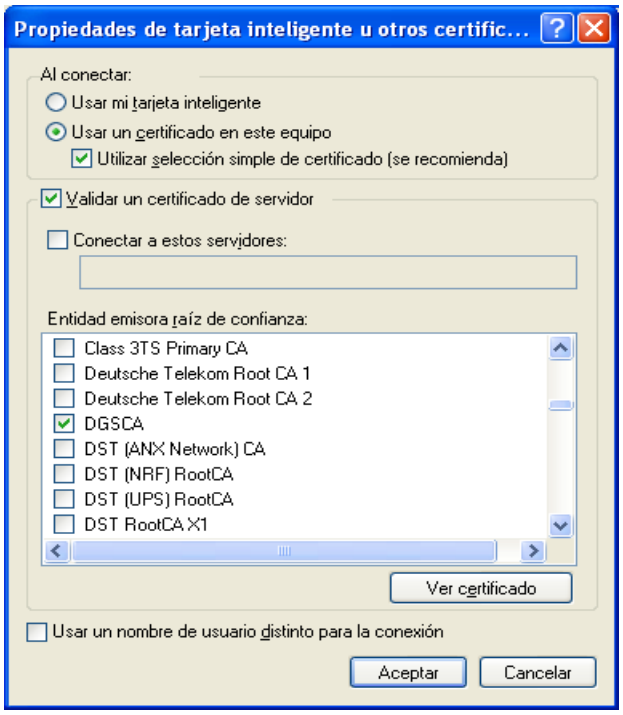

Figura B.4. Configuración: Selección certificado emisora raíz

6. Para finalizar, se hace click en el botón aceptar.

b) Configuración EAP-PEAP.

Antes de iniciar con la configuración, es necesario la generación e instalación del certificado: raíz (root.der) como se muestra en la sección *5.3.5 Certificados.*

1. Al igual que en el caso anterior, se hace click botón derecho en el icono que aparece en la parte inferior derecha de la pantalla que corresponde a la interfaz de red inalámbrica.

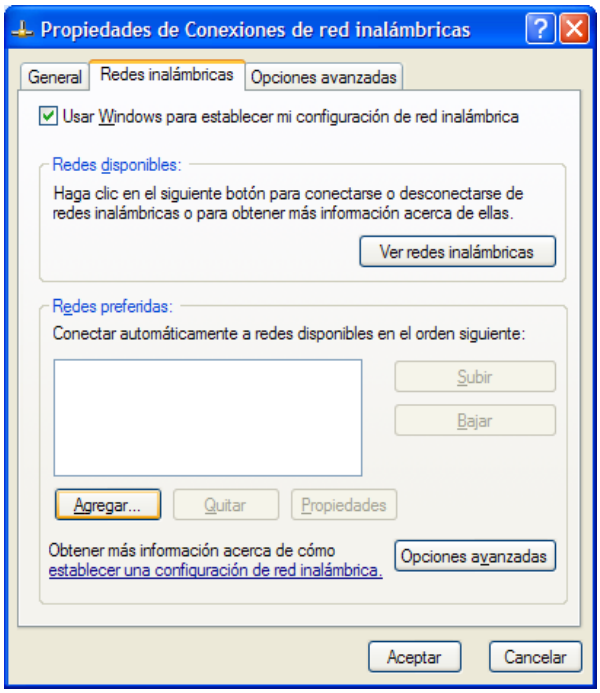

Figura B.5. Configuración dispositivo inalámbrico

2. Se selecciona la pestaña de *Redes inalámbricas*, se hace click sobre el botón *agregar* para agregar y configurar una nueva red inalámbrica, como se muestra en la figura B.5.
3. Se coloca el nombre o SSID de la red inalámbrica, WPA como Autenticación de red y TKIP como cifrado de datos, como se indica en la figura B.6.

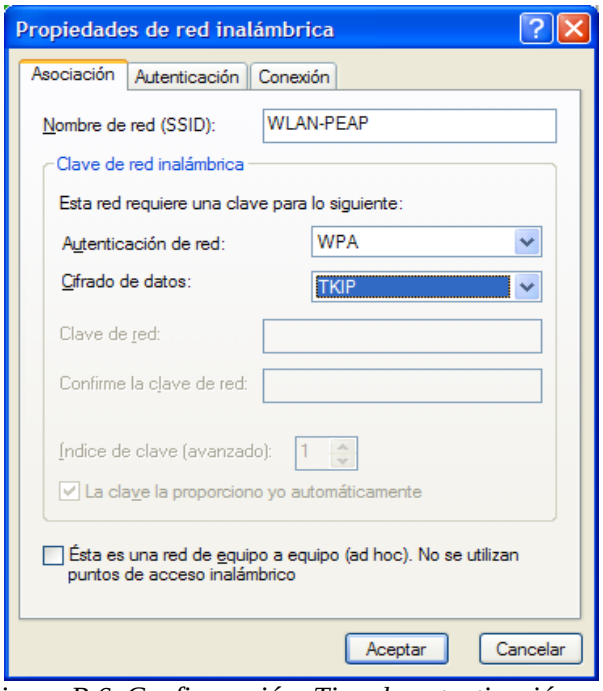

Figura B.6. Configuración: Tipo de autenticación y cifrado

4. A diferencia de la configuración EAP-TLS, en este caso se selecciona la opción "Protected EAP(PEAP)", como tipo EAP (véase figura B.7).

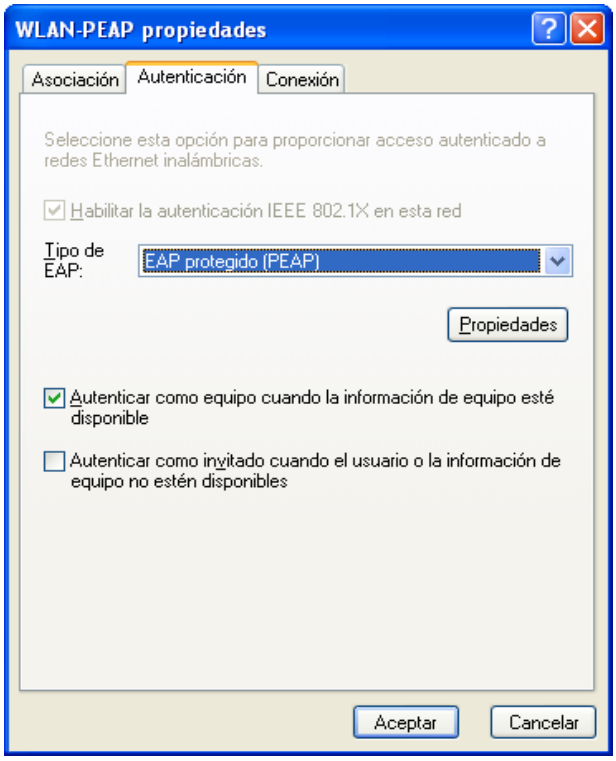

Figura B.7. Configuración: Selección tipo EAP-PEAP

5. Posteriormente se hace click sobre el botón Propiedades y se selecciona a DGSCA como entidad emisora raíz de confianza, como se muestra en la figura B.8.

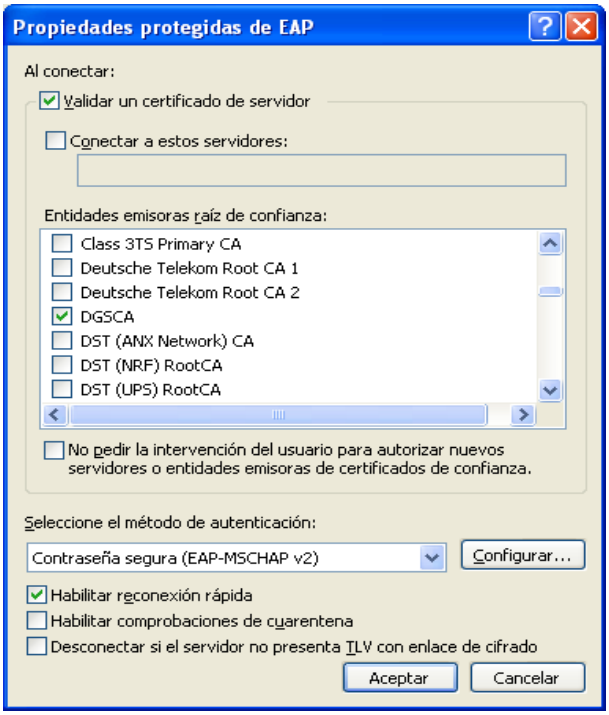

Figura B.8. Configuración: Selección certificado emisora raíz

6. También aparece un nuevo campo en la parte inferior del diálogo, que es para seleccionar el método interno de autenticación, en este caso se elige la opción *Contraseña segura (EAP-MSCHAP v2)*.

7. Finalmente se hace click sobre el botón *Configurar*. Aparece un diálogo (véase figura B.9) que permite elegir o no, usar el nombre de usuario y contraseña de Windows, para acceder a la red, en caso contrario el usuario tendrá que teclear un nombre de usuario y contraseña para entrar a la red.

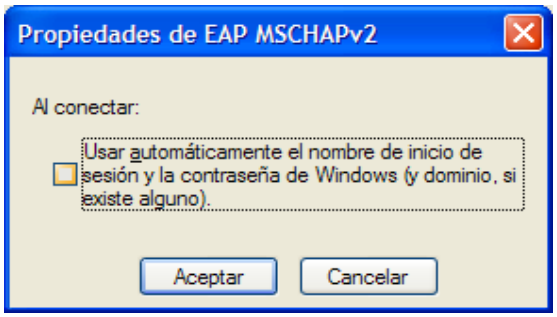

Figura B.9. Configuración: Usuario y contraseña

c) Configuración EAP-TTLS

Para conseguir la opción de autenticación EAP-TTLS, se instala la aplicación secureW2 Eap Suite, que es software libre (Open Source). Se puede obtener de la siguiente liga: http://www.securew2.com/

1. Una vez que se instala correctamente SecureW2 Eap Suite, se sigue los mismos primeros tres pasos anteriores, sólo que ahora en el cuarto paso aparecerá una opción más: **SecureW2 EAP-TTLS** (véase figura B.10)**,** que es la que se selecciona.

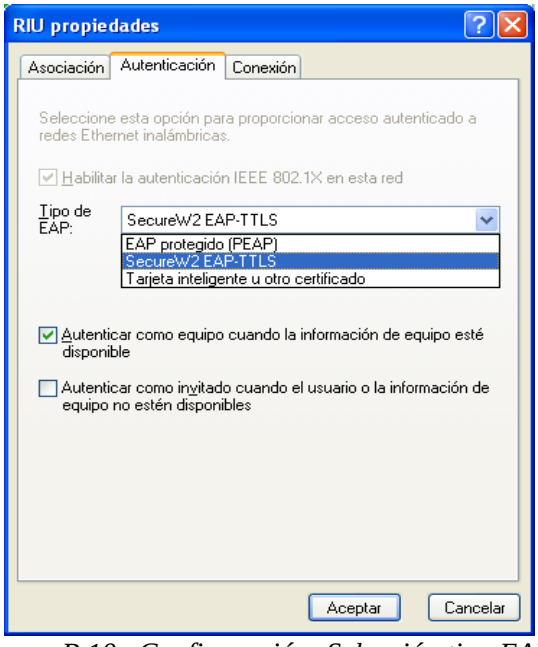

Figura B.10. Configuración: Selección tipo EAP-TTLS

2. Se hace click en propiedades e inmediatamente aparece un cuadro de diálogo solicitando introducir un perfil. Se introduce un nombre al perfil y luego se oprime *Configurar*.

Figura B.11. Configuración: Especificar una identidad externa

3. En la pestaña *Conexión* se especifica una identidad externa, de preferencia se coloca el login o nombre de usuario, como se muestra en la figura B.11. Se hace click en la pestaña *Certificados*, y se quita la opción *Comprobar certificadote servidor* (sólo en este caso, si el certificado del servidor es emitido por una entidad de confianza, se deja marcada esta opción, se elige y se agrega dicha autoridad de la lista que se despliega).

4. Se hace click en la pestaña *Autenticación* (véase figura b.12) y se agrega:

   Método Autenticación: **EAP**
   Tipo EAP: **Desafío-MD5**

Figura B.12 Configuración: Selección tipo EAP

5. En la pestaña *Cuenta de usuario* se introducen el login o nombre de usuario y la contraseña, como se indica en la figura B.13.

Figura B.13. Configuración: Nombre de usuario y contraseña

Apéndice C

GENERACIÓN, INSTALACIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

Apéndice C. Generación, instalación y administración de certificados

Generación de certificados

a) Primero se necesita crear un certificado raíz (root) para la entidad emisora de certificados, un certificado `self-signed`, es decir la entidad emisora se valida a si misma; lo anterior es un método aceptado para la creación de certificados root.
b) Una vez creado el certificado *root*, se tiene que generar un certificado para el servidor, en este caso para el servidor RADIUS.
c) Finalmente se crean los certificados para los usuarios.

FreeRADIUS incluye por default los certificados necesarios en la carpeta `/usr/local/radius/etc/raddb/certs`; para no confundirlos con los se van a crear, se crea el directorio `miscerts` en la misma ruta:

`/usr/local/radius/etc/raddb/miscerts.`

Nota. Los certificados que incluye FreeRADIUS funcionan sin ningún problema, pero contienen información que no corresponden a la organización, es este caso a DGSCA, por eso se muestra este procedimiento para generarlos de acuerdo a los datos de la institución.

Actualmente existen varios *scripts* creados para automatizar la ejecución de los comandos necesarios para la generación de los certificados usando OpenSSL. Los siguientes scripts fueron obtenidos de las fuentes de FreeRADIUS 1.1.7, con algunas ligeras modificaciones. El valor del parámetro *(pass*) para proteger los certificados es "*wireless"*. Si se instaló las librerías de OpenSSL en otra ruta diferente a /usr/local/openssl se tiene que modificar el parámetro *SSL*

Los scripts que se van a generar: CA.root, CA.server y CA.client se colocan en la carpeta *miscerts* y se les agrega los permisos de ejecución:

```
chmod u+x CA.root CA.Server CA.client
```

a) Generación del certificado raíz (root) para la "entidad emisora de certificados".

Se ejecuta el script CA.root:
`./CA.root`

El script crea el certificado root con auto-validación.

`Archivo CA.root`

```
#!/bin/sh –x
SSL=/usr/local/openssl
export PATH=${SSL}/bin/:${SSL}/ssl/misc:${PATH}
export LD_LIBRARY_PATH=${SSL}/lib
rm –rf demoCA

openssl req –new –x509 –keyout newreq.pem –out newreq.pem –days 730 –passin
pass:wireless –passout pass:wireless

echo "newreq.pem" | /usr/local/openssl/ssl/misc/CA.pl –newca > /dev/null
```

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

rm –rf newreq.pem
```

b) Generación de certificado para el servidor

Para efectuar la autenticación mutua entre el servidor RADIUS y el suplicante se debe tener un certificado de llave pública para el servidor de autenticación.

Antes de continuar con la creación del certificado del servidor, se copia el archivo `certs/demoCA/serial` a nuestro subdirectorio `miscerts/demoCA` que se creó durante la ejecución del script anterior.

Si se está ubicado en la ruta `/usr/local/radius/etc/raddb/miscerts`, se copia de la siguiente forma:

```
cp ../certs/demoCA/serial  demoCA/serial
```

Además, para la creación de los certificados para el servidor y para los clientes, es importante incluir el archivo `xpextensions` que acompaña las fuentes de FreeRADIUS al directorio miscerts/, desde donde se ejecuta los scripts, para que los certificados sea soportados correctamente en Microsoft Windows XP. En este caso en particular, como se desempaquetó el paquete en `/usr/src/`, el archivo se encuentra en:
`/usr/src/freeradius-1.1.7/scripts/xpextensions`

Si se está ubicado en la ruta `/usr/local/radius/etc/raddb/miscerts`, se copia de la siguiente forma:

```
cp /usr/src/freeradius-1.1.7/scripts/xpextensions .
```

Se ejecuta el script CA.server como sigue:

```
./CA.server <nombre-servidor>
```

Cuando pregunte por "common name" se teclea lo que se asigne como nombre del servidor <nombre-servidor> en la ejecución del script.

El script crea un certificado para el servidor y luego solicita ser firmado por la "autoridad emisora de certificados".

Archivo CA.server

```
#!/bin/sh –x
SSL=/usr/local/openssl

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

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


openssl req –new   -keyout newreq.pem –out newreq.pem –days 730 –passin
pass:wireless –passout pass:wireless
openssl ca  -policy policy_anything  -out newcert.pem –passin pass:wireless –
key  wireless  –extensions  xpserver_ext  –extfile  xpextensions  –infiles
newreq.pem

openssl pkcs12 –export –in newcert.pem –inkey newreq.pem –out $1.p12 –clcerts
–passin pass:wireless –passout pass:wireless
openssl  pkcs12  –in  $1.p12  –out  $1.pem  –passin  pass:wireless  –passout
pass:wireless
openssl x509 –inform PEM –outform DER –in $1.pem –out $1.der

rm –rf newcert.pem newreq.pem
```

c) Generación de certificados para los usuarios.

Se ejecuta el script CA.server como sigue:
`./CA.client <nombre-usuario>`

El script crea un certificado para un usuario y luego solicita ser firmado por la "autoridad emisora de certificados".

Lo mismo que en el script anterior, cuando pregunte por "common name" se teclea lo que se asigne como `<nombre-usuario>` en la ejecución del script.

Archivo CA.client

```
#!/bin/sh –x

SSL=/usr/local/openssl
export PATH=${SSL}/bin/:${SSL}/ssl/misc:${PATH}
export LD_LIBRARY_PATH=${SSL}/lib

openssl req –new –keyout newreq.pem –out newreq.pem –days 730 –passin
pass:wireless –passout pass:wireless
openssl ca  -policy policy_anything –out newcert.pem –passin pass:wireless –
key wireless –extensions xpclient_ext –extfile xpextensions –infiles
newreq.pem

openssl pkcs12 –export –in newcert.pem –inkey newreq.pem –out $1.p12 –clcerts
–passin pass:wireless –passout pass:wireless
openssl pkcs12 –in $1.p12 –out $1.pem –passin pass:wireless –passout
pass:wireless
openssl x509 –inform PEM –outform DER –in $1.pem –out $1.der

rm –rf newcert.pem newreq.pem
```

d) Creación de los certificados para la implementación de ejemplo:

Se crea un cerficado raíz (root) de la entidad emisora de certificados, un certificado para el servidor RADIUS, que se llama "ServidorRADIUS" y un certificado para el usuario "juanperez".

```
#cd /usr/local/radius/etc/raddb/miscerts
```

2. Se genera el certificado raiz (root):

```
/usr/local/radius/etc/raddb/miscerts# ./CA.root
```

Se acepta todo por default.

3. A continuación se genera el certificado para el servidor RADIUS:

```
/usr/local/radius/etc/raddb/miscerts# ./CA.server ServidorRADIUS
```

Cuando pregunta por "common name", se teclea `ServidorRADIUS`

4. Finalmente se puede crear los certificados para los usuarios, en caso de que se tenga una implemetación de autenticación EAP-TLS, en este ejemplo se crea el certificado para el usuario "juanperez".

```
/usr/local/radius/etc/raddb/miscerts# ./CA.client juanperez
```

Al igual que en el paso anterior, cuando pregunta por "common name", se teclea ***juanperez***

Se generan los siguientes certificados:

```
root.pem
root.p12
root.der
juanperez.pem
juanperez.p12
juanperez.der
ServidorRADIUS.pem
ServidorRADIUS.p12
```

ServidorRADIUS.der

Instalación y administración de los certificados

El sistema operativo Windows tiene la información de gran parte de las autoridades certificadoras raíz de confianza, pero en el caso particular de trabajar con certificados "autofirmados" mediante la ayuda de OpenSSL, se tiene que instalar el certificado raíz "root.der" de la entidad emisora de certificados, que se ha creado, para que durante el proceso de autenticación se pueda validar el certificado del servidor, y se pueda considerar como un certificado emitida por una autoridad certificadora raíz de confianza.

Para la autenticación EAP-TLS, es necesario que los usuarios instalen en su equipo móvil el certificado que los permita autenticar a la red inalámbrica, en este ejemplo se instalará el certificado del usuario Juan Pérez (juanperez.p12).

En primer lugar, se copian ambos certificados al equipo del usuario (véase figura C.1).

Figura C.1. Certificados que serán instalados

a) Instalación del certificado raíz: *root.der*

1. Se hace doble click sobre el archivo *root.der*, aparecerá una ventana con información de alerta, como se inidica en la figura C.2, de que el certificado raíz de la entidad emisora no es de confianza.

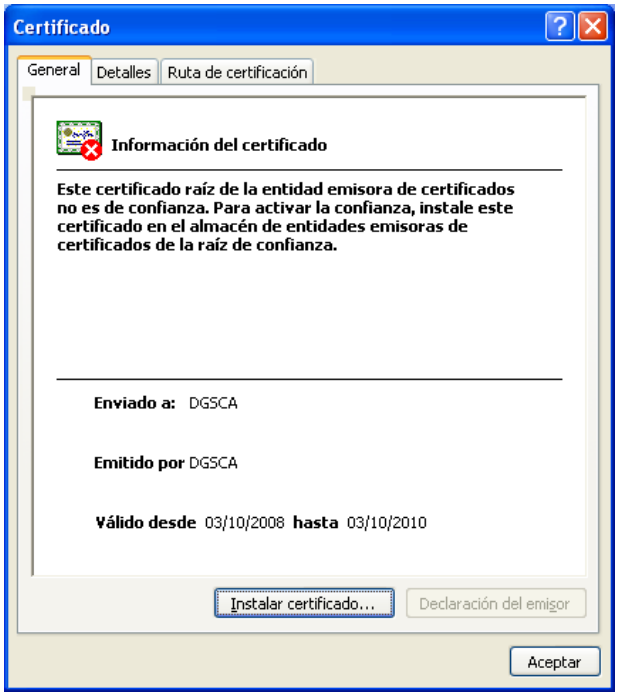

Figura C.2. Información del certificado

2. A continuación se hace click sobre el botón *Instalar certificado…*, se abrirá un asistente de instalación en la que se hace click sobre el botón *Siguiente>*, para abrir la ventana como la que se muestra en la figura C.3.

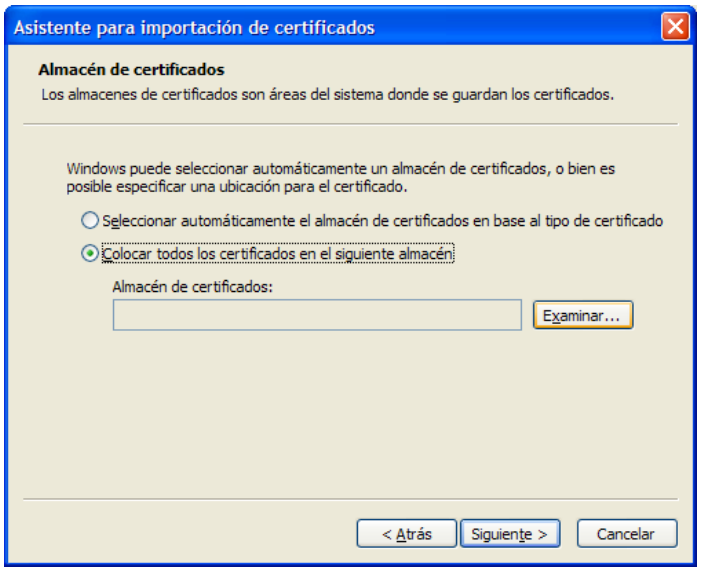

Figura C.3. Asistente de instalación

3. Se selecciona la opción *Colocar todos los certificados en el siguiente almacén* y se hace click sobre el botón *Examinar…*, para abrir el explorador como se muestra en la figura C.4.

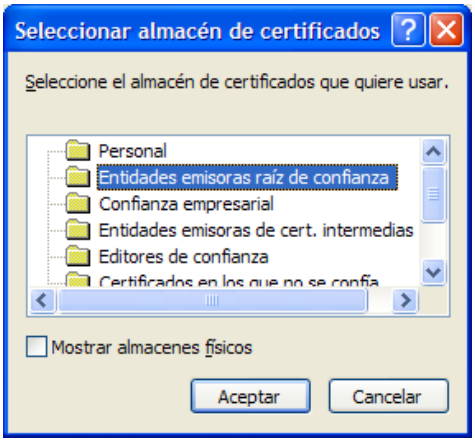

Figura C.4. Seleccionando directorio donde se colocará el certificado

4. Se elige la carpeta *Entidades emisoras raíz de confianza* y se oprime el botón *Aceptar*. Una vez seleccionada el almacén del certificado, se hace click sobre el botón *Siguiente* y aparecerá una ventana como la figura C.5.

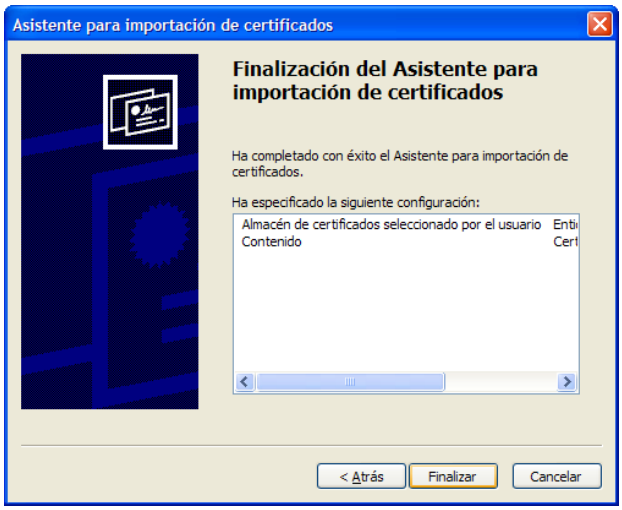

Figura C.5. Fin de la instalación

5. Se oprime el botón *Finalizar* para terminar la instalación y aparece otra advertencia de seguridad en donde alerta que si se instala el certificado raíz, Windows confiará automáticamente en cualquier certificado emitido por esa autoridad de certificados (véase figura C.6).

Figura C.6. Advertencia

6. Se hace click sobre el botón *yes* y el certificado queda instalado.

b) Instalación del certificado de usuario

1. Se hace doble click sobre el archivo *juanperez.p12*, aparecerá el asistente de instalación, en la que oprimimos el botón siguiente para continuar con la instalación.

2. Aparece un cuadro de dialogo solicitando el nombre del archivo, el asistente coloca el nombre y la ubicación del certificado de forma automática, simplemente se hace click sobre el botón *Siguiente*, como se muestra en la figura C.7.

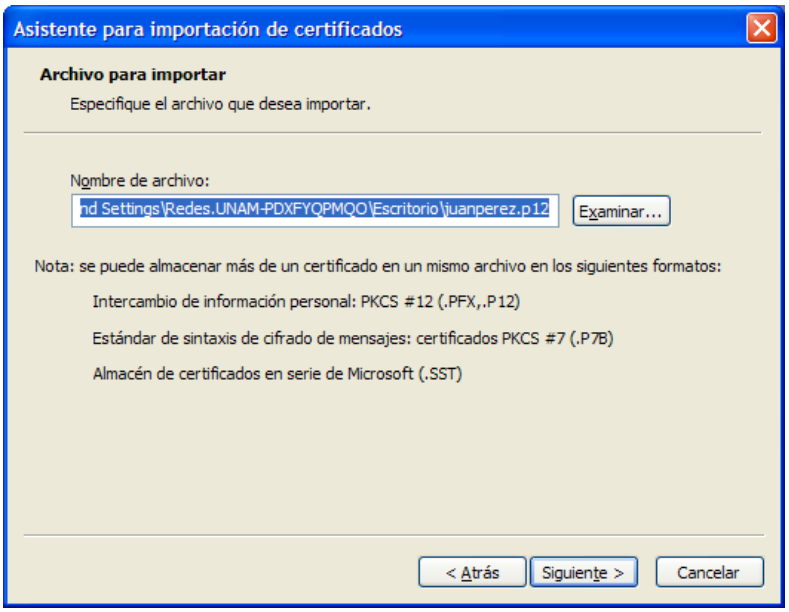

Figura C.7. Iniciando la instalación del certificado de usuario

3. La instalación solicita la contraseña, como se indica en la figura C.8, que protege la llave privada, en este caso es *wireless* y se estableció dentro de los scripts que se utilizaron en la creación de los certificados.

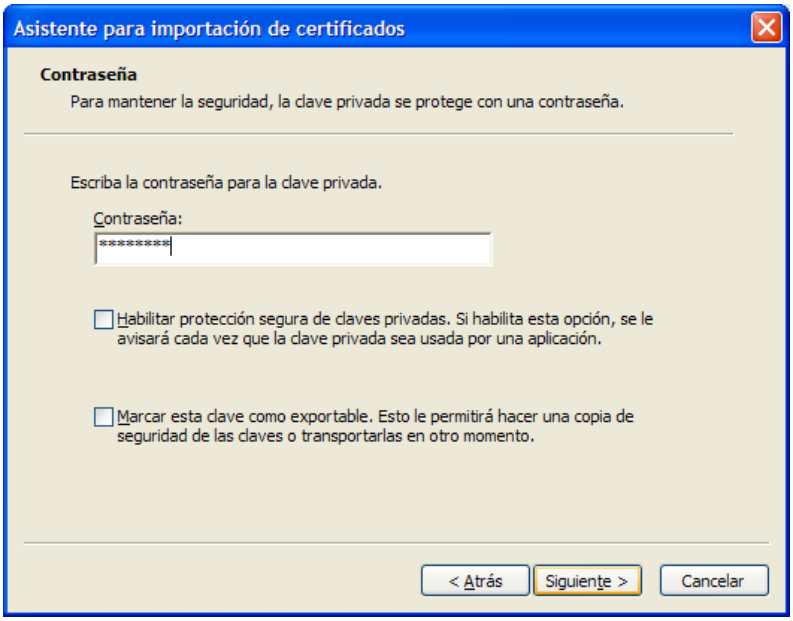

Figura C.8. Proporcionando contraseña de protección de la llave privada

4. Una vez que se teclea la contraseña y se hace click sobre el botón *Siguiente*, se abre una ventana como la mostrada en la figura C.9.

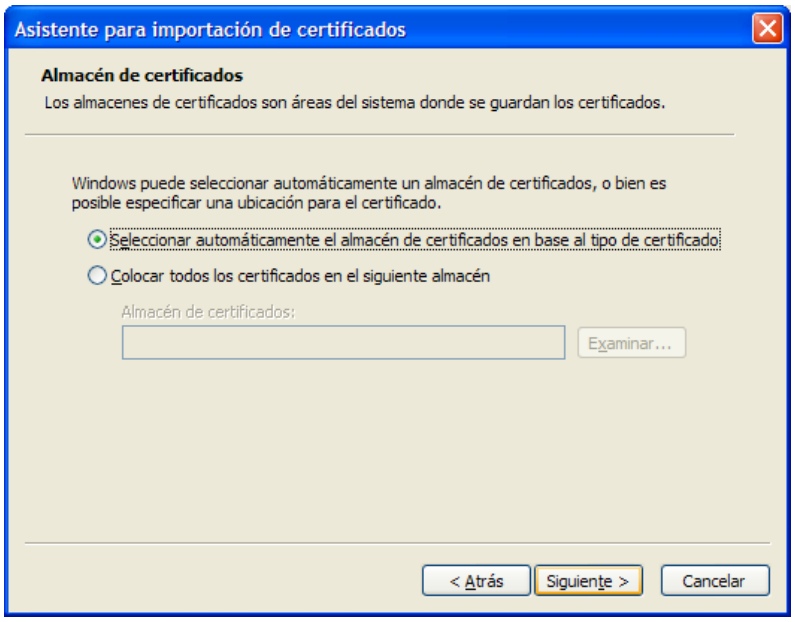

Figura C.9. Selección automática de almacenamiento del certificado

5. Se selecciona la opción *Seleccionar automáticamente el almacén de certificados en base al tipo de certificado*, y se hace click sobre botón *Siguiente.*

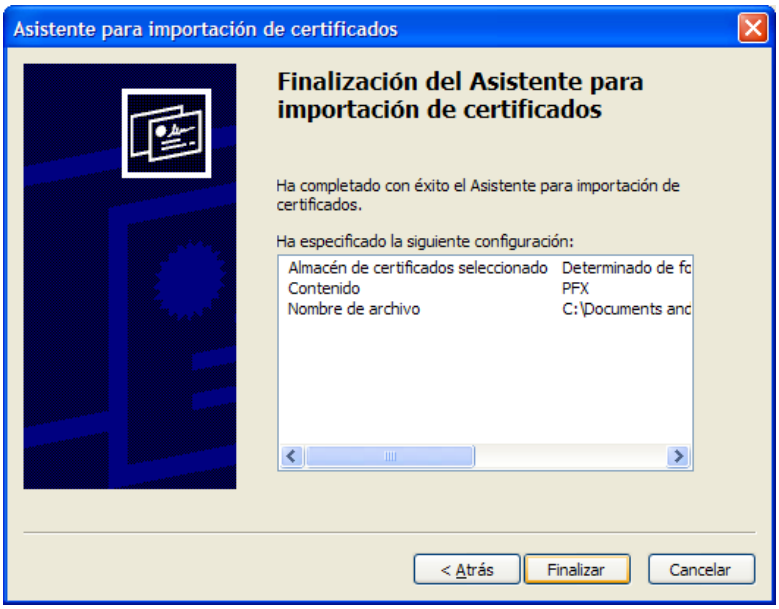

Figura C.10. Finalizando la instalación

6. Se finaliza la instalación al oprimir el botón *Finalizar.*

c) Administración de los certificados

Los certificados se pueden administrar por medio de la aplicación Microsoft Management Console (MMC), principalmente si en algún momento se requieran removerlos (certificados).

1. Se hace click en **Inicio**, en **Ejecutar**, y se escribe **mmc**, a continuación click en **Aceptar** (véase figura C.11).

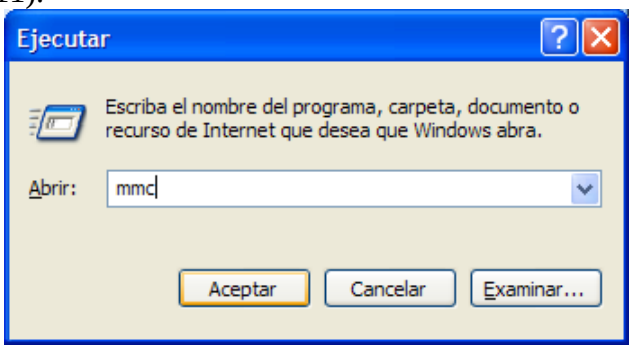

Figura C.11. Iniciando mmc

2. En el menú **Archivo**, se hace click en **Agregar o quitar complemento** y después sobre el botón **Agregar**, como se indica en la figura C.12.

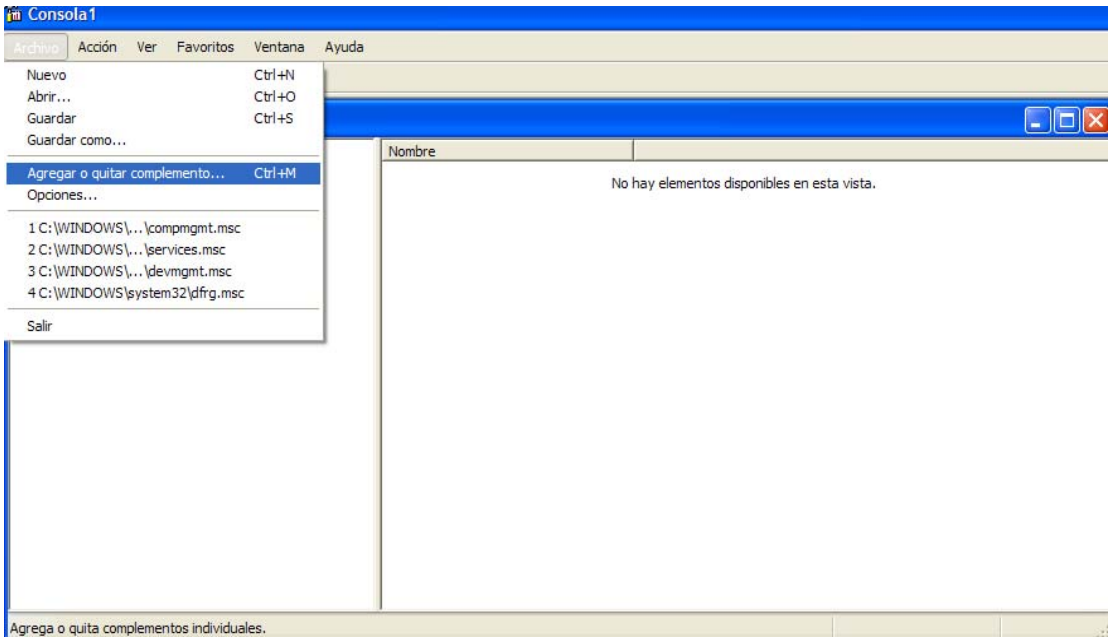

Figura C.12. Agregando un complemento

3. En la lista de **Complementos**, se hace doble click en certificados (véase figura C.13).

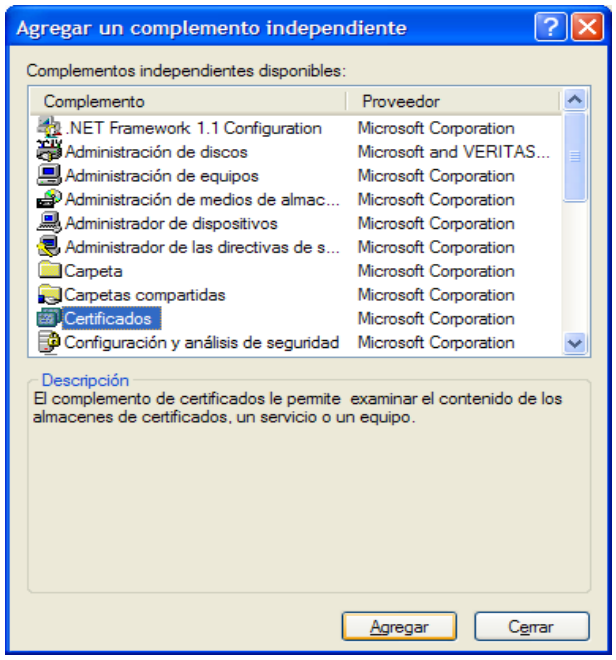

Figura C.13. Elección del complemento a agregar

4. Se selecciona la opción *Mi cuenta de usuario,* como se nuestra en la figura C.14, y se hace click en Finalizar, luego en Cerrar y Finalmente en Aceptar.

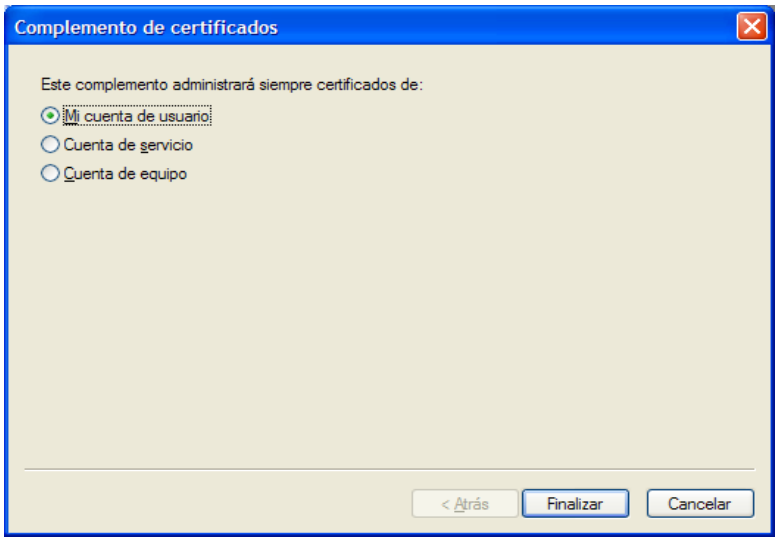

Figura C.14. Selección de tipo de administración

5. Sí se selecciona la carpeta Personal, se puede ver el certificado del usuario Juan Pérez, como se puede notar en la figura C.15.

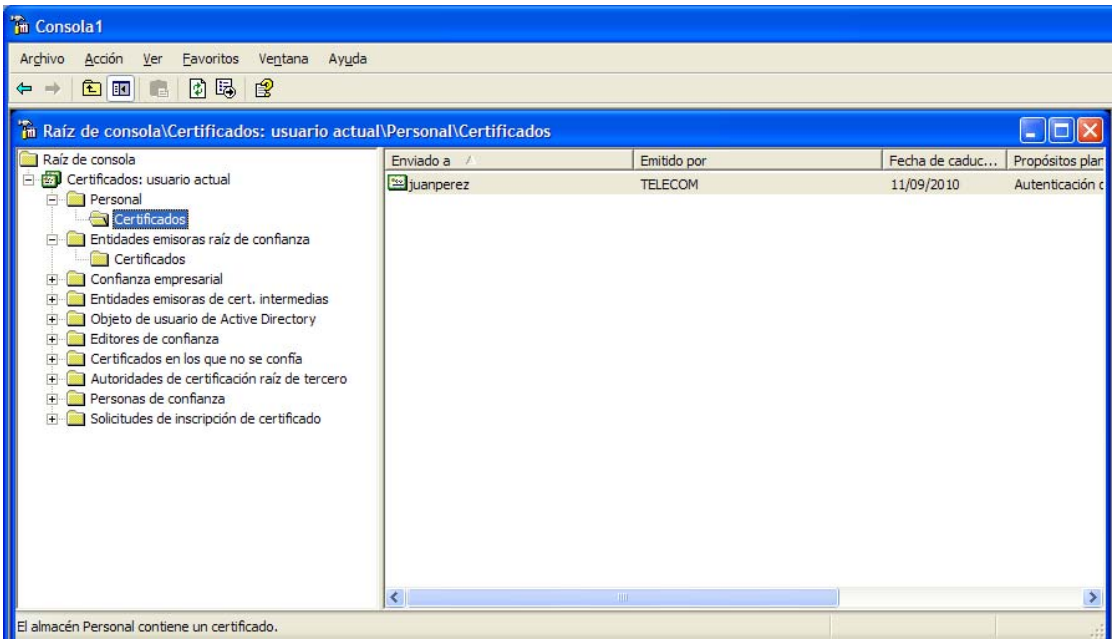

Figura C.15. Certificados personales instalados

6. Sí se selecciona la carpeta Entidades emisoras raíz de confianza, se puede ver el certificado raíz que se agregó (véase figura C.16).

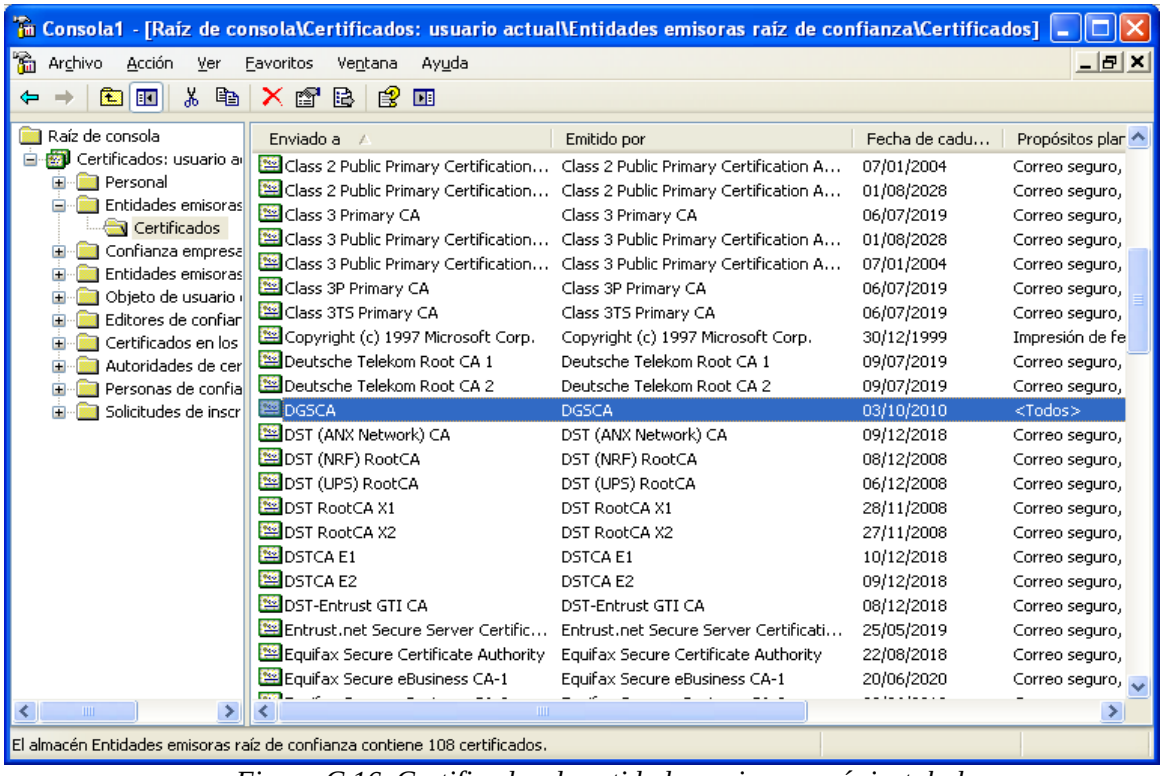

Figura C.16. Certificados de entidades emisoras raíz instalados

GLOSARIO

AAA
Authentication, Authorization and Accounting, 'Autenticación, Autorización y Contabilidad'**.** Generalmente se le denomina así al conjunto de protocolos que realiza las funciones de: Autenticación, Autorización y Contabilidad (Accounting).

AES
Advanced Encryption Standard, 'Estándar de Cifrado Avanzado'. Es un esquema de cifrado por bloques usado en criptografía simétrica, también se conoce como Rijndael. Puede utilizar claves de 128, 192 y 256 bits.

AP
Access Point, 'Punto de Acceso'. Es el dispositivo de la red inalámbrica que se encarga de controlar las comunicaciones de todos los equipos que forman la red, además sirve de puente con la red cableada.

Broadcast
El envío de paquetes de datos a todos los destinatarios posibles en la red.

BSS
Basic Service Set, 'Conjunto de Servicios Básicos'. Modalidad de comunicación en redes 802.11, en donde las conexiones inalámbricas se realiza a través de un AP

CBC-MAC
Cipher Block Chaining Message Authentication Code, 'Encadenamiento de Cifrado por bloques - Código de Autenticación de Mensaje'. Es una técnica para la construcción de un código de mensaje de autenticación de un sistema de cifrado por bloques.

CCMP
Counter Mode with CBC-MAC Protocol, 'Modo Contador con CBC-MAC'. Protocolo de seguridad en las WLAN diseñado desde cero. Usa el algoritmo de cifrado AES

CRC
Cyclic Redundacy Check, 'Comprobación Cíclica de Redundancia'. Son datos adicionales que se adjuntan al final de la información para comprobar que no ha habido errores en la transmisión. Los datos CRC son el resultado de realizar ciertas operaciones matemáticas a la información original.

DoS
Denial of Service, 'Denegación de Servicio'. Es un ataque a un sistema o a una red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

DSSS
Direct Sequence Spread Spectrum, 'Espectro Expandido por Secuencia Directa'.
Es la técnica de modulación utilizada por los sistemas IEEE 802.11b para transmitir datos hasta a 11 Mbps.

EAP
Extensible Authentication Protocol, ‘Protocolo de autenticación extensible’. Es un framework de autenticación muy utilizado en las redes inalámbricas, provee diferentes mecanismos de autenticación, conocidos como métodos EAP.

EAP-GTC
EAP Generic Token Card, ‘ EAP Tarjeta Token Genérico’. Método de autenticación que hace uso de un Generic Token Card para la identificación del usuario.

EAP-MD5 Challenge
Método de autenticación simple, aplicando el algoritmo MD5 a un mensaje de desafío.

EAP-MSCHAP-V2
EAP-Microsoft CHAP version 2. Inicialmente fue creado por Microsoft, ampliamente utilizado como un protocolo “inner authentication”. Puede ser utilizado por EAP-PEAP y EAP-TTLS

EAPOL
EAP Over LAN, ‘EAP sobre LAN’. Encapsula los paquetes EAP sobre una red LAN, por ejemplo: Ethernet.

EAP-SIM
Permite la autenticación de usuario de telefonía celular por medio de la tarjeta SIM (Subscriber Identity Module, Módulo de Identidad del Suscriptor).

EAP-TLS
EAP - Transport Layer Security, ‘Seguridad En la Capa de Transporte’. Método de Autenticación EAP mutua con certificados digitales, establece un canal de comunicación confiable.

ESS
Extended Service Set, 'Conjunto de Servicios Extendido'. Permite crear una red inalámbrica formada por más de un AP

Ethernet
Son las redes LAN más comunes en redes de área local, definida por el estándar IEEE 802.3.

FHSS
Frequency Hopping Spread Spectrum, ‘Espectro Expandido por salto de frecuencia’. Es la técnica de modulación usada en un principio por los sistemas IEEE 802.11. Transmite a 1 Mbps, fue sustituido por DSSS para alcanzar los 11 Mbps.

Firewall
Proporciona servicios de control de acceso, filtrado de paquetes que permite aislar la red de tráfico no deseado.

FreeRADIUS
Software de código abierto que permite la implemetación de un servidor RADIUS.

GNU
GNU's Not Unix. Conjunto de aplicaciones basadas en software libre, que puede ser copiado y distribuido libremente, junto con el núcleo Linux, se consigue el sistema operativo de software libre *GNU/Linux* tipo Unix.

Hacker
Persona que entra ilegalmente en sistemas y redes de computadoras para robar, alterar o borrar información.

IBSS
Independent Basic Service Set, 'Conjunto de Servicios Básicos Independientes'. Conexiones uno a uno de dispositivos inalámbricos.

IEEE
Institute of Electrics and Electronics Engineers, 'Instituto de Ingenieros Eléctricos y Electrónicos. Es un organismo de estandarización, principalmente de redes de área local.

IEEE 802.11
Define las especificaciones para las redes inalámbricas de área local, WLAN.

IEEE 802.11i
Es el nuevo estándar de seguridad de las redes 802.11 cuyo objetivo fue solucionar los problemas del protocolo WEP.

IEEE 802.11X
El estándar 802.1X define un Control de Acceso a Red Basado en puertos.

LAN
Local Area Network, 'Red de Área Local'. Es una clasificación de las redes según el área geográfica que abarca, una red LAN tiene una extensión reducida.

LDAP
Lightweight Directory Acces Protocol, 'Protocolo de Acceso a Directorios Ligero'. Es un protocolo de tipo cliente-servidor que proporciona un servicio de directorio.

LEAP
Lightweight EAP, 'EAP Ligero'. Mecanismo de autenticación propietario de Cisco, fue una buena alternativa provisional, en lugar de manejar llaves estáticas con WEP, actualmente ya nos es recomendado.

LLC
Logical Link Control, 'Control de Enlace Lógico'. Una de las dos subcapas en que se divide la capa de *Enlace* del modelo de referencia OSI. Proporciona servicios a la capa de red.

MAC
Medium Access Control, 'Control de Acceso al Medio'. Una de las dos subcapas en que se divide la capa de *Enlace* del modelo de referencia OSI. Entre otras cosas, define como los dispositivos de la red acceden al medio.

MIC
Message Integrity Code, 'Código de Integridad de Mensaje'. Mecanismo que evita que un atacante capture información cifrada, la altere y la reenvíe en redes inalámbricas.

Modelo TCP/IP
Transmission Control Protocol/Internet Protocol, **'**Protocolo de Control de Transmisión/Protocolo de Internet'. Es el estándar histórico y técnico de Internet. Fue desarrollado por el Departamento de Defensa de EE.UU. Para obtener una red de comunicación que pueda seguir funcionando ante cualquier catástrofe, incluso ante una guerra nuclear. Es una un pila de protocolos.

NAS
Network Access Server, 'Servidor de Acceso de red'. Funciona como cliente de un servidor RADIUS; en IEEE 802.11X el NAS viene siendo el autenticador.

OFDM
Orthogonal Frequency Division Multiplexing, 'Multiplexado Ortogonal por División de Frecuencia'. Es una técnica de modulación usado por los sistemas IEEE 802.11a que permite alcanzar velocidades de transmisión hasta los 54 Mbps

OpenLDAP
Software de código abierto que permite la implemetación de un servidor LDAP.

OpenSSL
Es un conjunto aplicaciones y librerías de código abierto que permite implementer los protocolos SSL y TLS.

OSI
Open System Interconnect, 'Inteconexión de Sistemas Abiertos'. Es un modelo de referencia, escribe las reglas o la manera de como la información en una computadora es transferida a una aplicación residente en otro equipo. Organiza las funciones de las redes en 7 categorías llamadas "capas".

PDA
Personal Digital Assistant, 'Asistente Digital Personal'. Son computadoras de "mano", pueden realizar muchas de las funciones que una computadora de escritorio.

PEAP
Protected EAP, 'EAP Protegido'. Protege métodos EAP con cifrado TLS, maneja un *nombre de usuario* y una *contraseña* para la autenticación del usuario y un certificado para la autenticación del servidor con el que se consigue autenticar a la red.

PKI
Public Key Infraestructure, 'infraestructura de clave pública'. Es el conjunto de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones como el cifrado, la firma digital o el no repudio de transacciones electrónicas. También se usa este término para referirse a una autoridad emisora de certificados.

RADIUS
Remote Authentication Dial-In User Service, 'Servicio de Autenticación Remota de Usuario Teléfonico'. Es un protocolo de control de acceso muy utilizado en las implementaciones AAA.

RAID
Redundant Array of Independent Disks, 'conjunto redundante de discos independientes'. El término hace referencia a un sistema de almacenamiento que emplea múltiples discos duros entre los que distribuye o replica los datos. Dependiendo de la configuración o nivel RAID, se pueden conseguir uno o varios de los siguientes beneficios: mayor integridad, mayor tolerancia a fallos, mayor rendimiento y capacidad, que sí se usara un solo disco duro.

RAID 1
Crea una copia exacta o espejo de los datos en dos o más discos, busca garantizar la disponibilidad, por que existe una tolerancia a falla de algún disco, al disponer de la misma información en cada uno de ellos.

RC4
Rivest Cipher version 4. Es un algoritmo de cifrado diseñado por la empresa RSA, basa su funcionamiento en permutaciones aleatorias.

Rogue AP
Es un AP instalado en una WLAN, pero que no esta autorizado, generalmente no cumple con las políticas de seguridad establecidas permitiendo que cualquier dispositivos inalámbrico tenga acceso a la red.

RSN
Robust Security Network, 'Red de Seguridad Robusta'. Redes inalámbricas con seguridad WPA2.

Script kiddie
Así se le llama a la persona que usa programas, scripts, exploits, troyanos, etc. creados por terceros para romper la seguridad de un sistema. Generalmente presumen de ser un hacker cuando en realidad no posee un grado relevante de conocimientos.

Servidor
Se trata de un software que ofrece servicios remotos a sus usuarios. También se le conoce asi al propio equipo donde está instalado el software servidor. Los dispositivos de los usuarios contacta con el servidor gracias a otro software llamado cliente.

Sniffer
'Husmeador'. Es una aplicación que permite capturar tramas en las redes cableadas o inalámbricas.

SQL
Structured Query Language, 'Lenguaje de consulta estructurado'. Es un lenguaje de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones sobre las mismas. Permite el manejo de álgebra y cálculo relacional permitiendo realizar consultas para

recuperar de forma sencilla información de interés de una base de datos, así como hacer cambios sobre la misma

SSID
Service Set IDentifier, 'Identificador del Conjunto de Servicios'. Es un nombre que se les asignan a las WLAN para que las estaciones puedan distinguir entre una red y otra.

SSL
Secure Sockets Layer, 'Capa de Conexión Segura'. Es un protocolo desarrollado por Netscape para codificar la información entre un explorador y un servidor WEB, garantizando la privacidad, autenticidad e integridad de la información intercambiada.

TCP
Transmission Control Protocol, 'Protocolo de Control de Transmisión'. Es un protocolo de la capa de transporte de la pila de protocolos TCP/IP. Proporciona un transporte confiable, control de flujo y es orientado a conexión.

TKIP
Temporary Key Integrity Protocol, 'Protocolo de Integridad de Clave Temporal'. Protocolo de seguridad en las WLAN diseñado de forma rápida para solucionar las debilidades de WEP, utiliza el algoritmo de cifrado RC4

Token Ring
Es una tecnología de red LAN con topología lógica en forma de anillo, en donde la información circula en u sólo sentido de éste.

TSN
Transitional Security Network, 'Red de Seguridad de Transición'. Redes inalámbricas con seguridad WPA (1), es decir TKIP + 802.11X.

TTLS
Tunneled TLS. Protege métodos de autenticación con cifrado TLS, maneja un *nombre de usuario* y una *contraseña* para la autenticación del usuario y un certificado para la autenticación del servidor con el que se consigue autenticar a la red.

UDP
User Datagram Protocol, 'Protocolo de Datagrama de Usuario'. Es un protocolo de la capa de transporte de la pila de protocolos TCP/IP. Proporciona una comunicación muy sencilla entre las aplicaciones de dos equipos, no es orientado a conexión, pero es mucho más rápido que TCP.

VPN
Virtual Private Network, 'Red Privada Virtual'. Es una red privada que se construye dentro de una infraestructura de red pública o no segura (WLAN), también permite establecer conexiones seguras a la redes locales a través de Internet.

WDS
Wireles Distribution System, ‘Sistema de distribución inalámbrico’. Permite realizar enlaces entre dos redes locales (*building to building*) con la tecnología IEEE 802.11.

WEP
Wired Equivalent Privacy, ‘Privacidad equivalente Alámbrica’. Fue el sistema de seguridad original del estándar 802.11, con la finalidad de proporcionar privacidad equivalente a la que hay en una red alámbrica.

Wi-Fi
Wireless Fidelity, ‘Fidelidad Inalámbrica’. Es la certificación que avala el grupo Wi-Fi Alliance, que define un subconjunto de IEEE 802.11 con algunas extensiones.

WLAN
Wireless Local Area Network, Red de Área Local Inalámbrica’. Es el acrónimo con el que se hace referencia a las redes de area local inalámbricas. Las redes IEEE 802.11 son un ejemplo de este tipo de redes.

WPA
Wi-Fi Protected Access, ‘Acceso Wi-Fi protegido’. Es un subconjunto de las especificaciones de 802.11i, que surgió como solución deWEP inmediata, es básicamente TKIP + 802.1X.

WPA Empresarial
Una solución WPA empresarial incluye 8021.1X y por consecuencia el uso de EAP y de un servidor de autenticación.

WPA-PSK
Pre-shared Key, ‘Llave pre-compartida’. También se conoce como WPA Personal se utiliza ambientes SOHO (Small Office/Home Office), usa la opción de la llave compartida evitando el uso de 802.1X

BIBLIOGRAFÍA Y MESOGRAFÍA

Bibliografía y mesografía

Edney, Jon y Arbaugh, William A; Real 802.11 Security: Wi-Fi Protected Access and 802.11i; Addison Wesley; Julio 2003

Gast, Matthew; 802.11 Wireless Networks: The Definitive Guide**;** O'Reilly; Abril 2005

Hassell, Jonathan. RADIUS; O'Reilly; Octubre 2002

Vladimirov, Andrew A.; Gavrilenko, Konstantin V. y Mikhailovsky Andrei A.; Wi-Foo: The Secrets of Wireless Hacking; Addison Wesley; Junio 2004

Carballar, José A.; Wi-Fi: Cómo construir una red inalámbrica; Alfaomega; 2004

Carter, Gerald; LDAP System Administration; O'Reilly; Marzo 2003

Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

802.1X Port-Based Authentication HOWTO
http://tldp.org/HOWTO/html_single/8021X-HOWTO/

http://www.openldap.org/doc/admin24/

http://freeradius.org/

http://www.openldap.org/

http://www.openssl.org/

http://www.debian.org/index.es.html

http://dev.mysql.com/doc/

http://www.linuxforums.org/reviews/overview_of_the_ten_major_linux_distributions.html

http://polishlinux.org/choose/comparison/