ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE DOS SOLUCIONES DE SEGURIDAD PARA UNA RED LAN INALÁMBRICA

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

JORGE ISAAC INSUASTI PROAÑO

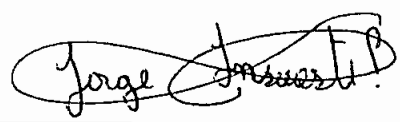
DIRECTOR: ING. PABLO HIDALGO

Quito, Noviembre de 2004

DECLARACIÓN

Yo Jorge Isaac Insuasti Proaño, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.



Jorge Isaac Insuasti Proaño

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Jorge Isaac Insuasti Proaño, bajo mi supervisión.

Ing. Pablo Hidalgo

DIRECTOR DE PROYECTO

AGRADECIMIENTO

A Dios, por haberme dado salud y tranquilidad.

A mi familia, por su apoyo incondicional.

A Shirma, por su amor y fortaleza.

A mis profesores, por su dedicada labor y confianza en la educación.

A mis amigos, por su compañía y ayuda en los momentos difíciles.

Al Ing. Pablo Hidalgo, por su guía dentro y fuera de las aulas.

A la Escuela Politécnica Nacional, por haberme echo crecer.

Gracias

PRESENTACIÓN

En la actualidad se vive una auténtica revolución de la tecnología inalámbrica. Cada vez más y más empresas están implementando redes LAN inalámbricas por las necesidades de movilidad que el negocio requiere. El *boom* inalámbrico se ha dado gracias a una reducción en los costos de los equipos y al aumento de la velocidad de transmisión, resultado de los avances en la investigación en esta tecnología.

Pero las redes inalámbricas traen consigo nuevos retos que deben superarse para que puedan convertirse en una solución óptima para el mercado.

El principal reto de las redes inalámbricas es la seguridad. La tecnología inalámbrica es por naturaleza insegura ya que las señales de datos viajan libremente por el aire y pueden ser interceptadas fácilmente afectando así la seguridad de toda la red.

Si no se afronta este reto de seguridad, las redes inalámbricas no serían prácticas para las empresas pues tendrían un agujero de seguridad y no se podría aprovechar toda la potencialidad de las mismas.

Por lo mencionado anteriormente nace la necesidad de proveer mecanismos de seguridad robustos que permitan tener autenticación, confidencialidad e integridad en los sistemas inalámbricos. Para cumplir con este objetivo el presente trabajo propone un estudio de los diferentes aspectos de la seguridad en redes inalámbricas y las principales soluciones disponibles actualmente en el mercado, para en base a ello desarrollar dos soluciones de seguridad para una red LAN inalámbrica.

Las soluciones seleccionadas están implementadas en función de los estándares disponibles actualmente en el mercado y utilizan toda la potencialidad de las herramientas que el fabricante (Cisco Aironet) ofrece para brindar seguridad a la red inalámbrica.

RESUMEN

El presente trabajo enfrenta el principal reto de las redes LAN inalámbricas, la seguridad. Para ello se inicia con una introducción al estándar IEEE 802.11 para abarcar el funcionamiento y los principales aspectos de las redes LAN inalámbricas (WLAN).

A continuación se realiza una introducción a la bases de la seguridad, donde se ubican conceptos de autenticación, integridad, confidencialidad y disponibilidad de los sistemas. También se tratan las principales herramientas existentes para brindar seguridad a los mismos como por ejemplo la encripción, las firmas digitales, los certificados digitales, los algoritmos de *hash,* etc.

Posteriormente se realiza un estudio de los principales mecanismos de seguridad existentes para WLAN's, específicamente WEP (*Wired Equivalency Protocol*), WPA (*Wi-Fi Protected Access*) y EAP (*Extensible Authentication Protocol*) con sus principales implementaciones comerciales. Se establecen comparaciones y las ventajas y desventajas de la implementación de los diferentes mecanismos en situaciones reales.

En base a este estudio, se realiza la implementación de las dos soluciones de seguridad, EAP (concretamente LEAP, Lightweight EAP) y WEP (con mejoras WPA), que se desarrolla con equipos CISCO para la infraestructura de red inalámbrica; esto es, puntos de acceso CISCO Aironet 340 y tarjetas inalámbricas CISCO Aironet PCMCIA 350 en los clientes. Además se considera el caso general de usuarios con sistema operativo Windows.

Para la implementación de la solución LEAP, se realiza la instalación y configuración de un servidor RADIUS, para lo cual se elige un software comercial, el Odyssey Server, que ofrece compatibilidad con LEAP y soporte para plataformas Windows. Ambas soluciones se someten a pruebas de funcionamiento para verificar su correcto desempeño y presentar las conclusiones finales.

ÍNDICE

CAPÍTULO 1

CAPÍTULO 1

1. DESCRIPCIÓN DE LA TECNOLOGÍA DE REDES INALÁMBRICAS

1.1. FUNDAMENTOS DE LAS REDES INALÁMBRICAS

Las redes inalámbricas tienen como objetivo realizar la interconexión de diferentes dispositivos a través de un medio de transmisión no guiado. Esto permite ofrecer conexión a sistemas que requieran movilidad o donde no sea posible llegar con un cableado físico.

La tecnología inalámbrica puede ir desde aplicaciones complejas como redes LAN inalámbricas WLAN (*Wireless Local Area Network*) o redes celulares, hasta aplicaciones sencillas como la conexión de periféricos de un computador. Además se tienen dispositivos infrarrojos como controles remotos, audífonos inalámbricos y todo objeto que requiera una línea de vista entre el transmisor y el receptor para el enlace.

Su principal diferencia con las redes alámbricas es que las señales se propagan libremente a través del área de cobertura. Por esto se deben tomar en cuenta ciertas consideraciones para el uso de esta tecnología.

1.1.1. CONSIDERACIONES AL USO DE LA TECNOLOGÍA INALÁMBRICA

La tecnología inalámbrica trae consigo varias consideraciones que se deben tomar en cuenta al momento de utilizarla [1]. Por su diferencia con las redes cableadas tradicionales se requiere replantear los conceptos tradicionales y establecer los nuevos retos que trae consigo esta tecnología. A continuación se presentan varias de estas consideraciones:

- El aire es un medio de transmisión muy contaminado, sometido a interferencias electromagnéticas de todo tipo que pueden disminuir la calidad de la señal.

- Debido a que las antenas emiten señales de radio en todas las direcciones a través de la red, se pueden producir choques con los elementos sólidos provocando que la señal se refleje y sea recibida varias veces pero por distintos caminos. Esto genera una interferencia en la recepción haciendo que la señal se desvanezca. Este efecto se conoce como desvanecimiento por múltiple trayectoria que se presenta en los sistemas inalámbricos. En la figura 1.1 se indica de forma gráfica este concepto.

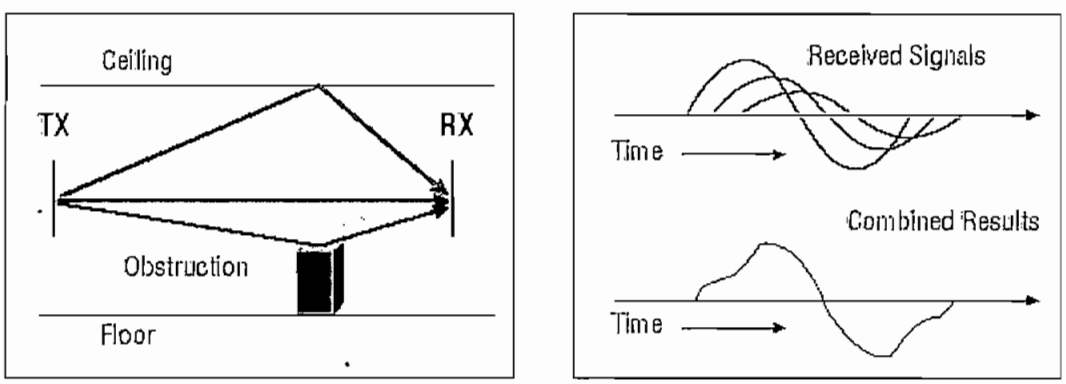


Fig. 1.1 Tipos de redes inalámbricas [13][1]

- Al propagarse libremente las señales de radio, éstas pueden ser fácilmente interceptadas y ver afectada la seguridad de los datos de la red.

- Se deben poder conectar varios tipos de dispositivos como computadoras portátiles, agendas electrónicas, impresoras inalámbricas, etc. a la red sin importar si el fabricante de estos equipos y el de la infraestructura de la red son los mismos. Esto implica una total interoperabilidad entre varias clases de sistemas y por supuesto el desarrollo de estándares.

[1] El número entre corchetes indica la fuente de la cual se tomó el gráfico, la misma que se especifica en la bibliografía del presente trabajo. Si no se tiene presente este número, significa que el gráfico fue creado por el autor.

- La cobertura cambia de sentido en la tecnología inalámbrica. En el caso de medios guiados se asegura la cobertura en un sitio colocando un punto de red, llevando físicamente el cable hasta el punto. En las redes inalámbricas la cobertura dependerá de las características de los equipos y de la arquitectura del lugar. La única forma de asegurarse que hay cobertura en un lugar es realizar pruebas y verificar que se tiene una adecuada potencia de la señal.

Ahora que se tiene presente las diferentes implicaciones del uso de la tecnología inalámbrica, se debe aclarar los tipos de redes inalámbricas y sus alcances.

1.1.2. TIPOS DE REDES INALÁMBRICAS

Existen distintos tipos de redes inalámbricas para diferentes campos de aplicación; generalmente son categorizadas de la siguiente manera [2]:

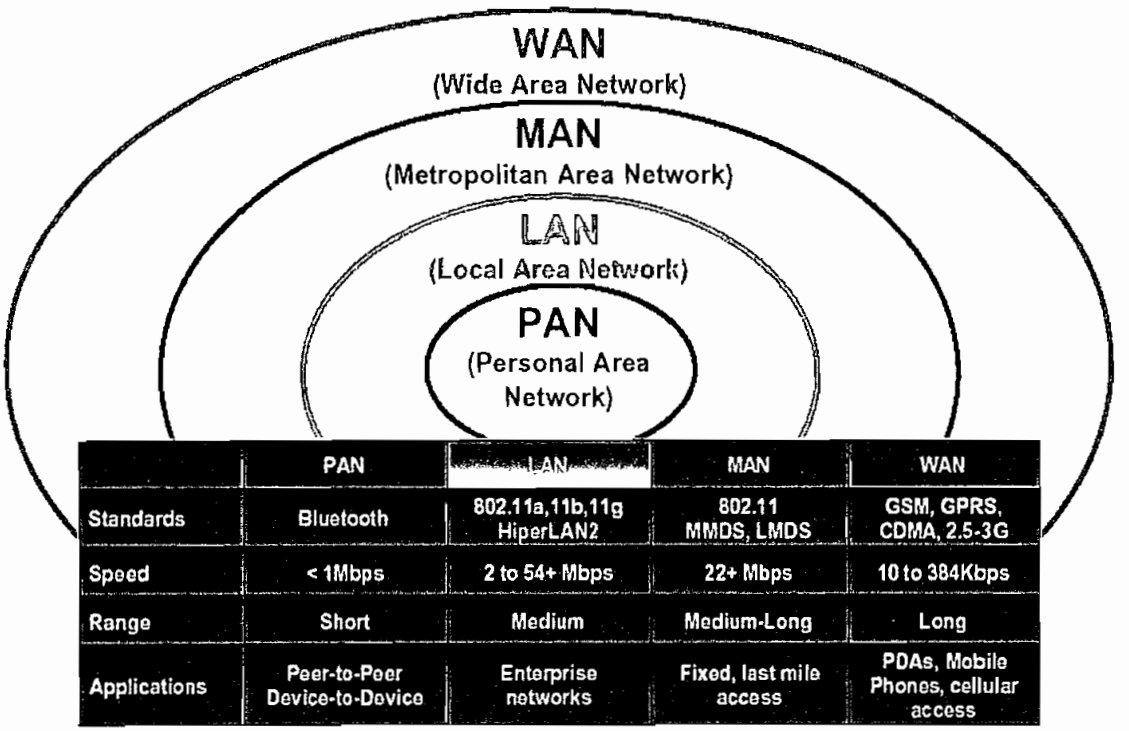
- WWAN = *Wireless Wide Area Networks*, Redes Inalámbricas de Área Extendida.

- WMAN = *Wireless Metropolitan Area Networks*, Redes Inalámbricas de Área Metropolitana.

- WLAN = *Wireless Local Area Networks*, Redes Inalámbricas de Área Local.

- WPAN = *Wireless Personal Area Networks*, Redes Inalámbricas de Área Personal.

En la figura 1.2 se muestra este esquema de clasificación de las redes inalámbricas.



	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a,11b,11g HiperLAN2	802.11 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G
Speed	< 1Mbps	2 to 54+ Mbps	22+ Mbps	10 to 384Kbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	Fixed, last mile access	PDAs, Mobile Phones, cellular access

Fig. 1.2 Tipos de redes inalámbricas [2]

1.1.2.1. WWAN, Redes Inalámbricas de Área Extendida

Son redes inalámbricas con un área de cobertura extensa que puede abarcar todo un país. Un ejemplo de este tipo son las redes de radio utilizadas para comunicación celular en ambientes urbanos con tecnologías como CDPD (*Celular Digital Packet Data)* y GSM (*Global System for Mobile Communications)*. Estas redes tienen velocidades entre los 10 Kbps y los 300 Kbps.

Fig. 1.3 Red Celular

1.1.2.2. WMAN, Redes Inalámbricas de Área Metropolitana

Tienen como objetivo cubrir ambientes urbanos. Generalmente se utilizan para proveer de enlace de última milla en las ciudades para evitar el tendido de cable. Ejemplo de este tipo de red es LMDS (*Local Multipoint Distribution Service*). Llegan a velocidades de hasta 22 Mbps.

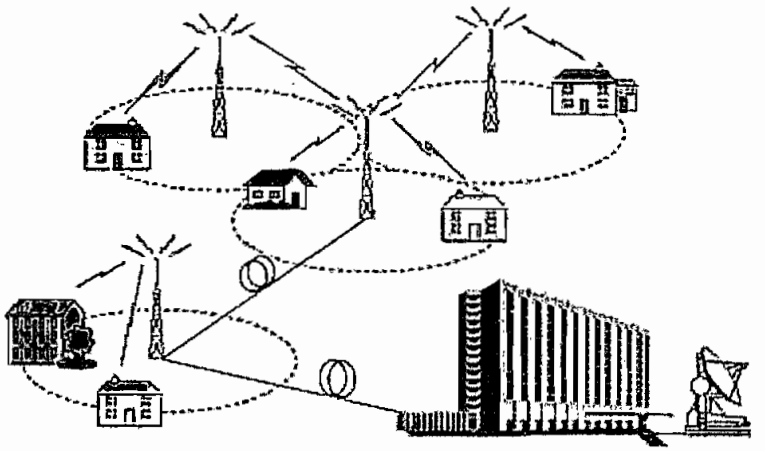


Fig. 1.4 Red LMDS

1.1.2.3. WLAN, Redes Inalámbricas de Área Local

Cubren áreas locales como edificios, oficinas, conectando las computadoras de los usuarios que tienen tarjetas de radio con antenas adecuadas para el manejo de las señales. El estándar más difundido para redes LAN inalámbricas es el IEEE 802.11. Actualmente las WLAN llegan incluso a los 108 Mbps.

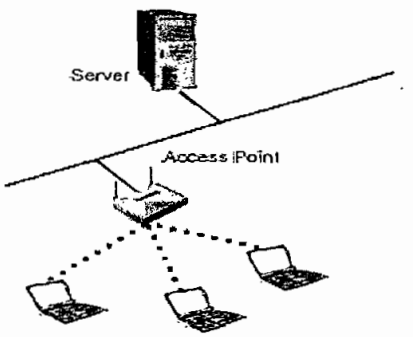


Fig. 1.5 Red LAN inalámbrica

1.1.2.4. WPAN, Redes Inalámbricas de Área Personal

Se refieren a la interconexión de sistemas de una computadora utilizando sistemas de radio de corto alcance. El más importante desarrollo en WPAN es el Bluetooth que permite la conexión inalámbrica de monitores, teclados, escáneres y *cualquier* periférico sin la necesidad de llenar de cables el sitio de trabajo. Las WPAN´s llegan a velocidades de 1 Mbps.

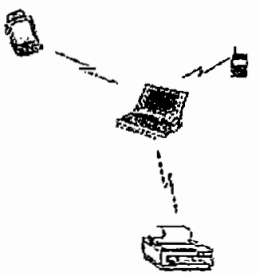


Fig. 1.6 Red WPAN

1.1.3. VENTAJAS Y DESVENTAJAS DE LAS REDES INALÁMBRICAS

Las redes inalámbricas proveen grandes ventajas con respecto a las redes cableadas, sin embargo esta tecnología también presenta ciertas limitaciones que deben ser consideradas. [3]

1.1.3.1. VENTAJAS

- La movilidad que ofrece a los usuarios es la razón principal de ser de las redes inalámbricas, la libertad de ir a cualquier sitio con una portátil y simplemente encenderla y estar conectado a Internet es muy apreciada. Además existen redes inalámbricas en lugares públicos como aeropuertos, restaurantes, bibliotecas donde se puede permanecer en línea gracias a una red inalámbrica.

- Ya no se requiere la instalación de un cableado para conectar las computadoras a la red. Esto permite tener bajos costos de mantenimiento y migración a otro sitio físico.

- Son una excelente opción en el caso de instalaciones temporales, ya que permiten interconectar diferentes dispositivos en tiempos record, sin mayor demora.

- Los cambios de topología son transparentes y se puede manejar redes pequeñas y grandes de igual forma.

1.1.3.2. DESVENTAJAS

- Su baja velocidad de transmisión ha sido siempre su principal desventaja. Como las redes inalámbricas se iniciaron a 11 Mbps los usuarios no se veían tan atraídos ya que tranquilamente podían tener Fast Ethernet a 100 Mbps en un lugar fijo. Sin embargo esto está cambiando con la aparición de nuevos estándares que van incrementando la velocidad. Hoy en día prácticamente la baja velocidad no es una desventaja pues se puede encontrar equipo inalámbrico que provee una velocidad de hasta 108 Mbps.

- Los altos costos de los equipos. Por la inversión que se debía realizar muchas empresas no se animaban a instalar una infraestructura inalámbrica en sus instalaciones. Pero en los momentos actuales gracias a los avances de la tecnología los fabricantes están desarrollando equipos a menores costos y muy pronto será común tener una red inalámbrica casera en el hogar.

- La seguridad es un miedo permanente de quienes utilizan redes inalámbricas. Es verdad que existe una inseguridad inherente con el uso de esta tecnología, sin embargo se han desarrollado mecanismos robustos que pueden garantizar que un usuario se sienta tan seguro como si estuviera en la red cableada tradicional.

- La incompatibilidad de equipos de diferentes fabricantes es un hecho al momento de implementar una WLAN. Para solucionar esto existen tablas de los fabricantes que indican con qué equipos del mercado pueden

trabajar, además, siempre se están actualizando los *drivers* y el *firmware*[1] de los equipos para permitir implementar mejoras y solucionar problemas de compatibilidad.

1.2. HISTORIA Y EVOLUCIÓN DE LAS REDES INALÁMBRICAS

El desarrollo de las redes inalámbricas se remonta a los logros del científico italiano Guillermo Marconi que basándose en los trabajos previos de Hertz y con gran inventiva patentó el telégrafo inalámbrico en 1897, en Inglaterra.

Su invento fue el desarrollo de un siglo de investigación científica y solucionó la necesidad de comunicación a grandes distancias. El éxito del telégrafo inalámbrico fue tal que en 1903 funda la *Marconi's Wireless Telegraph Company, Ltd*, la cual mantuvo un servicio de noticias entre Europa y los Estados Unidos. Se puede decir que nace la primera empresa de tecnología inalámbrica de la historia [4].

Ya en nuestros tiempos, en 1990 Motorola desarrolla uno de los primeros sistemas de redes inalámbricas comerciales con su producto Altair funcionando a una frecuencia de 1.8 Ghz.

Pero para empezar el verdadero desarrollo de la tecnología se debía superar varios problemas como los altos costos de los equipos, bajas velocidades de transmisión y licencias para el uso del espectro radioeléctrico. Solucionados estos problemas los fabricantes verían una verdadera oportunidad de negocio.

Con la liberación de la bandas ISM (Industrial, Científica y Medica) se produce el impulso que los fabricantes requerían para invertir en el desarrollo de esta tecnología. Es así que aparecen esfuerzos de varios fabricantes lo que lleva

[1] Microcódigo con el que trabajan los equipos

finalmente a que el IEEE (*Institute of Electrical and Electronics Engineers*) inicie en 1990 el proyecto del estándar 802.11 para redes inalámbricas.

Es en junio de 1997 que el estándar IEEE 802.11 se publica describiendo la capa de Control de Acceso al Medio (MAC) y la capa física (PHY) para conectividad inalámbrica para estaciones fijas, portables y móviles dentro de un área local.

El éxito del IEEE fue el crear un estándar base que puede albergar múltiples tipos de codificación física, frecuencias y aplicaciones, generando así un modelo a seguir por todos los fabricantes. Las velocidades originales del 802.11 eran de 1 y 2 Mbps a una frecuencia de 2.4 Ghz. Pero a finales de 1999 se publican 2 suplementos al estándar que son el 802.11a y el 802.11b que incrementan las opciones de velocidad.

El 802.11b extiende la velocidad hasta 11 Mbps a la misma frecuencia de 2.4 Ghz, en cambio el 802.11a extiende la velocidad hasta 54 Mbps pero a una frecuencia de 5 Ghz.

Pero el desarrollo de la tecnología continua y la necesidad de mayores velocidades lleva al desarrollo del estándar 802.11g publicado en junio del 2003 que define la operación hasta 54 Mbps pero a la frecuencia de 2.4 Ghz ofreciendo compatibilidad con 802.11b.

Finalmente se encuentra en desarrollo el estándar 802.11i, que pretende otorgar a los estándares 802.11 a, b y g características robustas de seguridad. Esto implica compatibilidad con el estándar 802.1x y total integración con AES (*Advanced Encryption Standard*).

Casi en paralelo al IEEE, la ETSI (*European Telecommunications Standards Institute*) desarrolló su estándar HIPERLAN *(High Performance Radio LAN*) para redes inalámbricas, publicándolo en 1996. HIPERLAN especifica su operación a 5 Ghz con velocidades sobre los 20 Mbps. Luego se desarrolla el HIPERLAN/2 para operar en la banda de los 5 Ghz con velocidad de 54 Mbps. Se diseña para

llevar celdas ATM[1], paquetes IP y voz digital, para lo cual provee calidad de servicio (QoS) y garantía de ancho de banda.

El uso de estos estándares HIPERLAN no se ha popularizado tanto como los estándares IEEE 802.11

1.3. TOPOLOGÍAS DE LAS REDES INALÁMBRICAS

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas, la una se conoce como administrada o de infraestructura y la otra como no administrada o "*ad hoc*" [5].

1.3.1. DESCRIPCIÓN GENERAL DEL FUNCIONAMIENTO DE LA TOPOLOGÍA DE INFRAESTRUCTURA

En la topología de infraestructura, se tiene una comunicación entre las estaciones inalámbricas mediante un concentrador inalámbrico llamado Punto de Acceso o *Access Point*. El *Access Point* (AP) también es el encargado de unir el mundo cableado con el inalámbrico y sirve como controlador central de la red LAN inalámbrica, coordinando la transmisión y recepción de múltiples dispositivos inalámbricos dentro de un área de cobertura específica. Si el área es extensa se utilizan varios puntos de acceso para cubrirla totalmente. En la figura 1.7 se muestra un ejemplo de esta topología.

El dispositivo que desea conectarse se conoce como "estación móvil" y primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante señalización de los puntos de acceso. La estación elige una red entre las que están disponibles e inicia el proceso de autenticación. Luego de comprobarse la identidad de los participantes comienza el proceso de asociación.

---

[1] *Asynchronous Transfer Mode*

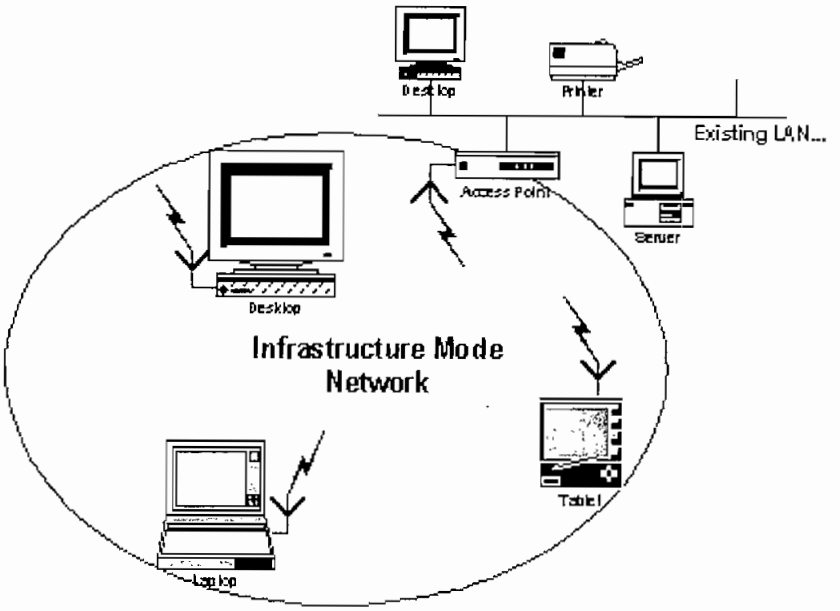


Fig. 1.7 Red de infraestructura [11]

La asociación permite que el punto de acceso y la estación intercambien información sobre el tipo de enlace para ponerse de acuerdo en los parámetros de comunicación que van a utilizar. Finalmente la estación puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

1.3.2. DESCRIPCIÓN GENERAL DEL FUNCIONAMIENTO DE LA TOPOLOGÍA *AD-HOC*

En la topología *ad hoc*, no se requiere un punto de acceso ni un control central, sino que más bien los propios dispositivos inalámbricos crean la red LAN enviándose mensajes directamente entre sí.

Un ejemplo práctico del uso de esta tecnología es cuando varios usuarios se reúnen en un cuarto no equipado con puntos de red o no se tiene cobertura de un punto de acceso y requieren intercambiar información. En la figura 1.8 se muestra un ejemplo de esta topología.

En la modalidad *Ad Hoc* sólo hay dispositivos inalámbricos presentes, por lo que la señalización debe ser controlada por las estaciones.

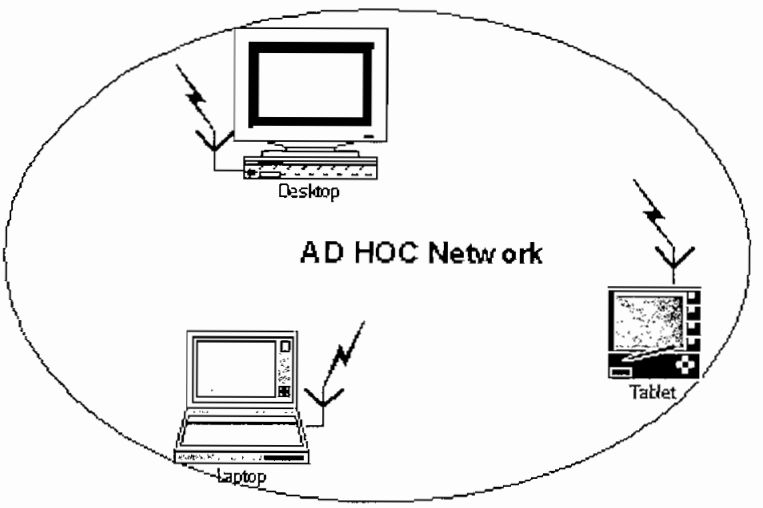


Fig. 1.8 Red ad hoc

1.4. ESTUDIO DEL ESTÁNDAR IEEE 802.11

Las principales ventajas de un estándar son:

- Incentiva la producción masiva de equipos al existir un patrón establecido, disminuyendo así los costos.

- Garantiza la interoperabilidad entre los distintos fabricantes.

Sin duda alguna el estándar 802.11 se ha consolidado en el campo de las redes LAN inalámbricas, siendo el más utilizado en hogares, en la pequeña y mediana empresa, en grandes corporaciones y llegando incluso a implementaciones públicas en hoteles, aeropuertos, cafeterías, universidades, bibliotecas, etc. Por esto es importante entender los principios de funcionamiento y el alcance del estándar IEEE 802.11 [6].

1.4.1. ALCANCE DEL ESTÁNDAR IEEE 802.11

El estándar define la operación inalámbrica para la conexión de estaciones fijas, portátiles y móviles dentro de un área local. Para esto especifica la capa física PHY y la capa de control de acceso al medio MAC. Por tanto IEEE 802.11 define la arquitectura ha utilizarse, su pila de protocolos, las técnicas de transmisión de radio utilizadas en la capa física, el protocolo de subcapa MAC, la estructura de las tramas y los tipos de servicios.

1.4.1.1. COMPONENTES Y TOPOLOGÍAS DEL IEEE 802.11

El IEEE admite 2 topologías: de infraestructura y *ad hoc*, que ya fueron tratadas en el punto 1.3. El estándar define el BSS Grupo de Servicios Básicos *(Basic Set Service*) que es un conjunto de estaciones que coordina su acceso al medio mediante el mismo procedimiento.

El *Set Service* se identifica de otro por su SSID (*Set Service Identifier),* que es como el nombre o dominio de la WLAN. El área que cubre el BSS se llama BSA Área de servicios Básicos (*Basic Service Area*). Si se tiene un único BSS en el que todos sus dispositivos son inalámbricos se tiene la topología *Ad hoc* o IBSS, un BSS independiente.

Para la topología de infraestructura el estándar puede conectar varios BSS mediante un DS Sistema de Distribución (*Distribution System*), con lo que forma un ESS Grupo de Servicios Extendidos.

Cada BSS tiene un Punto de Acceso que permite ingresar al DS. Así en el ESS se puede acceder a la red cableada e incluso al Internet a través de un portal[1] como lo indica la figura 1.9.

---

[1] Dispositivo de acceso a Internet

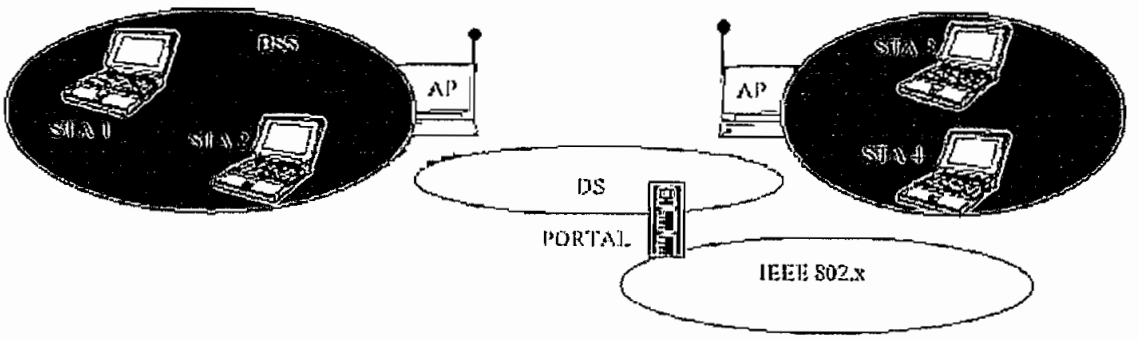


Fig. 1.9 ESS

1.4.2. PILA DE PROTOCOLOS DE 802.11

En la figura 1.10 se muestra una vista general de la ubicación 802.11 en la pila de protocolos. Se tiene como base la capa física que equivale a la descrita en el modelo OSI, ésta especifica las diferentes técnicas de transmisión permitidas.

Capas Superiores						
LLC						
Subcapa MAC						
Infrarrojos	FHSS	DSSS	OFDM 802.11a	HR DSSS	OFDM 802.11g	802.11

Fig. 1.10 Ubicación de 802.11en la Pila de Protocolos [6]

Luego se tiene a la subcapa MAC que define la forma en que se asigna el canal a los participantes. Finalmente se tiene las capas superiores que no son parte del 802.11 como la capa LLC.

1.4.3. CAPA FÍSICA DE 802.11

En la capa física se describen 6 técnicas de transmisión de radio, tres fueron introducidas en el estándar 802.11 original en 1997, éstas son Infrarrojos, FHSS

(*Frequency Hopping Spread Spectum*) y DSSS (*Direct Sequence Spread Spectum*). En 1999 se introducen 2 nuevas técnicas para aprovechar un ancho de banda mayor, OFDM (*Orthogonal Frequency Division Multiplexing*) y HRDSSS (*High Rate - Direct Sequence Spread Spectrum*).

La última técnica se publica en el 2001 y es una variación de OFDM en una frecuencia diferente. A continuación se realiza una breve descripción de estas técnicas.

1.4.3.1. Infrarrojos

Es una técnica de transmisión difusa con velocidades de 1 y 2 Mbps, con una longitud de onda de 0.85 a 0.95 micras. Para 1 Mbps se utilizan palabras de 4 bits a 16 bits que se codifican con el código de Gray[1], esto genera palabras de 16 bits con quince 0s y un 1, Para el caso de 2 Mbps se toman palabras de 2 bits y se codifican a 4 bits con tres 0s y un 1.

Este tipo de transmisión inalámbrica no se ha popularizado debido a que requiere tener línea de vista entre los sistemas pues no puede atravesar los objetos y a su pequeño ancho de banda.

1.4.3.2. FHSS

En la técnica de espectro disperso con salto de frecuencia (*Frequency Hopping Spread Spectrum*), la información se modula con un portador de señales que salta entre frecuencias diferentes en una secuencia específica, para esto utiliza un generador de números pseudoaleatorios para cambiar a un canal de transmisión.

Se tienen en total 72 canales con un ancho de banda de 1 Mhz que se encuentran en la banda ISM de 2.4 Ghz. El tiempo que una estación ocupa

[1] Codificación con el menor número de transiciones posibles

determinado canal de frecuencia puede variar pero siempre debe ser menor a 400 ms. Define velocidades de 1 y 2 Mbps.

Lo que se persigue con los saltos aleatorios de frecuencia es asignar de forma justa acceso a la banda ISM, con esto se logra además cierto nivel de seguridad, ya que no se sabe la frecuencia y el tiempo de permanencia en cada canal por lo que no se podrá escuchar la transmisión.

Por el salto aleatorio de frecuencias, FHSS es resistente a la interferencia, especialmente a la de otros equipos eléctricos, sin embargo su desventaja es su poco ancho de banda. Este esquema se utiliza en la tecnología Bluetooth.

1.4.3.3. DSSS

La técnica de espectro directo de secuencia expandida (*Direct Sequence Spread Spectrum*) utiliza 11 chips, que son bits de pequeño tiempo de duración para representar 1 bit utilizando la secuencia de Barker[1]. Luego se aplica una modulación por desplazamiento de fase BPSK[2] y DQPSK[3] a 1 Mbaudio[4] y transmite 1 bit por baudio en el caso de velocidad de 1 Mbps y a 2 bits por baudio cuando la velocidad es de 2 Mbps. Si uno o más bits se corrompen durante la transmisión, el dato original puede ser recuperado gracias a la redundancia en la transmisión lograda con los chips.

1.4.3.4. OFDM 802.11a

La Multiplexación por División de Frecuencias Ortogonales OFDM (*Orthogonal Frequency Division Multiplexing*) se diseñó para proveer alta velocidad de transmisión llegando hasta 54 Mbps.

---

[1] Codificación de estados con transiciones mínimas

[2] Modulación de fase con 2 estados

[3] Modulación de fase de 4 estados en cuadratura

[4] Número de símbolos por segundo

Funciona en la banda ISM de los 5 Ghz, en 52 frecuencias de las cuales 48 son para datos y 4 para sincronización, opera mediante la división de la señal de radio en varias subportadoras ortogonales que son transmitidas simultáneamente a diferentes frecuencias al receptor. Esto reduce el *crosstalk* o interferencia en las transmisiones.

1.4.3.5. HR-DSSS

La técnica de Espectro Disperso de Secuencia Directa de alta velocidad HR-DSSS (*High Rate - Direct Sequence Spread Spectrum*) utiliza 11 millones de chip/seg para alcanzar la velocidad de 11 Mbps a la frecuencia de 2.4 Ghz especificada en el estándar 802.11b. Sin embargo permite adaptarse de acuerdo al medio a velocidades menores de 5.5, 2 y 1 Mbps. Para llegar a la velocidad de 5.5 y 11 Mbps se aplica una secuencia de 1.375 Mbaudios con 4 y 8 bits por baudio respectivamente utilizando códigos de *Walsh/Hadamard*[1].

1.4.3.6. OFDM 802.11g

Esta técnica es similar a OFDM 802.11a, pero difiere en la banda utilizada, ya que funciona en los 2.4 Ghz con la misma funcionalidad OFDM pero en una banda más angosta.

1.4.4. CAPA DE ACCESO AL MEDIO 802.11

El problema de acceso al medio es más complicado en redes inalámbricas, en Ethernet por ejemplo, una estación espera a que el medio esté libre para transmitir, y si no se escuchan colisiones dentro de los primeros 64 bytes, se puede asegurar que los datos fueron entregados. Esto no se aplica en los sistemas inalámbricos. Se puede tener el problema de la estación oculta y expuesta. En el gráfico 1.11 se muestra el problema de la estación oculta, C

[1] Codificación por secuencias ortogonales.

transmite a la estación B, si A detecta el canal no escuchará nada y concluirá equivocadamente que puede transmitir sin problema a B.

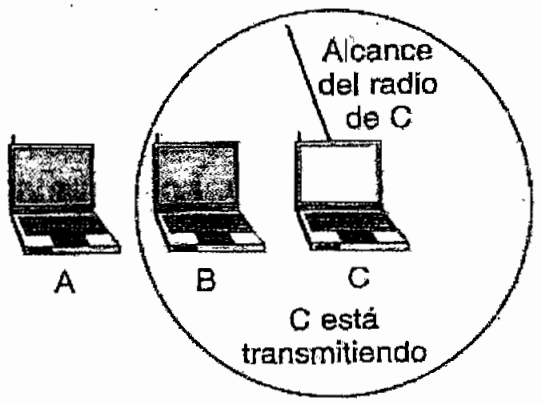


Fig. 1.11 Estación oculta [6]

Ahora por el contrario, en la figura 1.12 se muestra el problema de la estación expuesta, B desea transmitir a C, escucha el canal, pero al escuchar la transmisión de A hacia una estación D, concluye equivocadamente que C está ocupada.

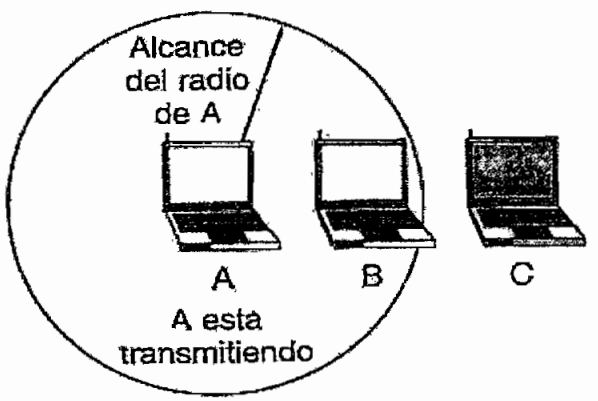


Fig. 1.12 Estación expuesta [6]

Además muchos sistemas inalámbricos son *semiduplex* por lo que no pueden transmitir y escuchar ráfagas de ruido al mismo tiempo en una sola frecuencia. Para solucionar estos problemas 802.11 define 2 modos de funcionamiento: PCF (Función de Coordinación puntual) y DCF (Función de Coordinación Distribuida).

1.4.4.1. Función de Coordinación Distribuida DCF

Cuando se emplea DCF no se tiene un control central, por lo cual es utilizado en redes *Ad Hoc*; DCF utiliza el protocolo CSMA/CA acceso múltiple con detección de portadora con prevención de colisiones.

CSMA/CA trabaja tanto en la detección del canal físico como del canal virtual. En el primer caso una estación que desea transmitir escucha el canal, si está libre transmite. Mientras transmite no escucha el canal y envía su trama completa, que podría perderse por interferencia.

Si el canal está ocupado, espera hasta que esté libre. Si se presenta una colisión las estaciones involucradas esperan un tiempo aleatorio con un algoritmo de retroceso exponencial binario que es el mismo de Ethernet y vuelve a intentarlo más tarde.

El otro modo de CSMA/CA utiliza la detección en el canal virtual. A continuación se muestra un ejemplo de esto en la figura 1.13. Se tienen 4 estaciones involucradas, A desea transmitir a B, C es una estación dentro del rango de A, y D es una estación dentro del alcance de B pero no de A. A decide enviar datos a B para lo cual le envía una trama RTS *(Request to Send)*.

Cuando B recibe la trama decide aceptar o negar la petición, si acepta envía una trama CTS (*Clear to Send)* hacia A. Al recibir A la trama CTS envía los datos y comienza su temporizador de ACK *acknolewdge*. B responde con otra trama ACK si los datos fueron recibidos. Si el temporizador de ACK termina antes de que el ACK regrese todo el protocolo se ejecuta de nuevo.

Ahora qué ocurre con las estaciones C y D. Como C está dentro del rango de A podría recibir también la trama RTS de A, cuando ocurre esto C se da cuenta de que se va a iniciar una transmisión y para evitar colisiones no transmite, imponiendo un tiempo de espera de acuerdo a la información del RTS recibido.

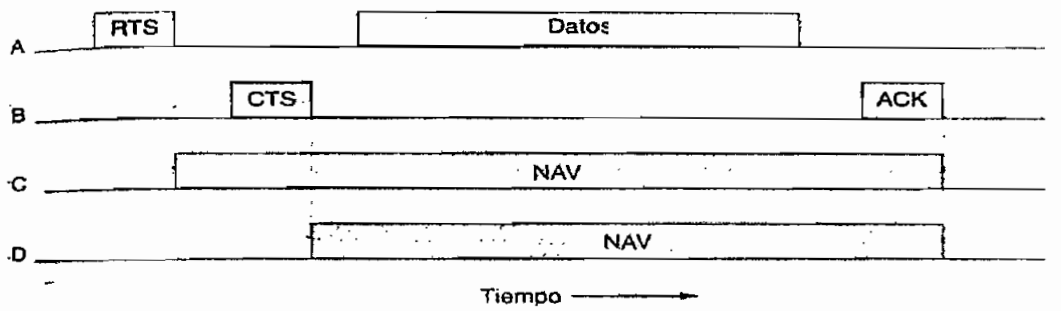


Fig. 1.13 CSMA/CA [6]

Este tiempo se representa por NAV (vector de asignación de red). Ahora D, que no escucha el RTS enviado por A, pero si el CTS enviado por B, también impone un NAV para si misma evitando transmitir y colisionar con los datos de A.

1.4.4.2. PCF Función de Coordinación puntual

En el modo PCF se tiene un control central de la estación base sobre toda su celda. La estación base realiza un sondeo a las estaciones para averiguar si tienen datos que transmitir. Como la estación base asigna los permisos de transmisión se evitan las colisiones.

El estándar define el mecanismo de sondeo pero no los periodos de sondeo y el orden del mismo. Las redes inalámbricas de infraestructura utilizan PCF aunque también pueden utilizar DCF y una combinación de las dos. Para el sondeo la estación base transmite una trama *beacon* de forma periódica, la cual contiene parámetros del sistema como secuencias de saltos (para FHSS), sincronismo de reloj, el SSID de la red, etc.

También se invita a nuevas estaciones a ingresar a la red, luego de lo cual se le asigna cierta frecuencia de sondeo otorgando una fracción del ancho de banda, lo cual permite establecer garantías de calidad de servicio.

1.4.5. ESTRUCTURA DE LA TRAMA 802.11

Se definen 3 tipos de tramas:

- ***Administración.***- Sirven para establecer asociación y desasociación de estaciones, para autenticación y negociación de parámetros.

- ***Control.***- Intercambio de datos de control

- ***Datos.***- Transportan los datos a través de la red

En la figura 1.14 se detalla la estructura de la trama de datos. El primer campo es el de control de trama que a la vez se subdivide en 11 campos como lo indica la tabla 1.1.

El campo siguiente es el de duración, que indica cuanto tiempo ocupará el canal la trama y su confirmación de recepción. Mediante este campo se maneja el mecanismo de NAV con tramas de control.

Luego vienen 4 campos de direcciones físicas que especifican la estación origen, el punto de acceso origen, el punto de acceso destino y la estación destino.

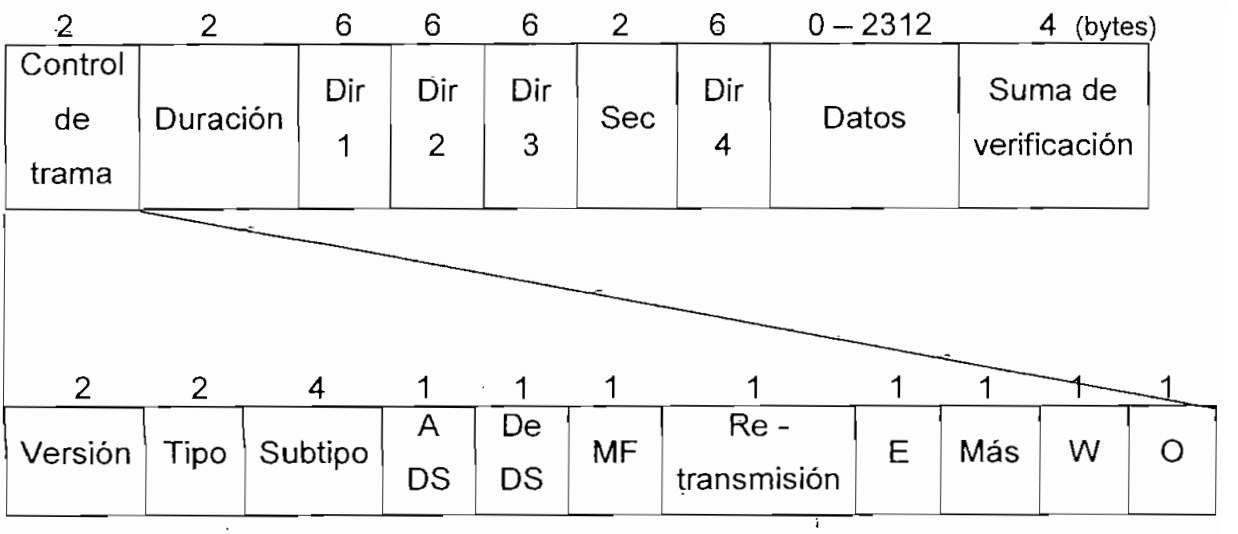


Fig. 1.14 Trama 802.11 [6]

Después de los tres campos de direcciones, de manera intercalada se encuentra el campo secuencia que permite numerar los fragmentos, consta de 16 bits, 12 de los cuales identifican la trama y los 4 restantes el fragmento.

Versión	Versión del protocolo
Tipo	Tipo de trama, administración, control o de datos
Subtipo	RTS, CTS, etc.
Hacia el DS	Trama dirigida al Sistema de Distribución
Desde un DS	Trama desde el Sistema de Distribución
Más Fragmentos	Indica que hay más fragmentos
Retransmisión	Marca que es una trama de retransmisión
Energía	Pone al receptor en estado de hibernación.
Más	Indica que el emisor tiene más tramas que enviar
WEP	Indica que en el cuerpo de la trama se ha utilizado WEP (*wired equivalency protocol*).
O	Indica que la secuencia de tramas debe procesarse en orden estricto.

Tabla 1.1 Campo control de Trama [6]

El campo de datos contiene la carga útil y puede llegar hasta los 2312 bytes [6]. Finalmente se tiene el campo de Suma de verificación para comprobar una correcta recepción de los datos.

Las tramas de administración tienen un formato parecido a las tramas de datos, se diferencian en que no tiene una de las direcciones de punto de acceso ya que estas tramas tienen sentido local dentro de la celda.

Las tramas de control son más pequeñas pues no tienen los campos de datos y de secuencia. En este tipo de tramas lo importante es saber el subtipo de trama, tales como CTS, RTS, etc.

1.4.6. SERVICIOS DE 802.11

El estándar define 9 servicios que la red LAN inalámbrica debe ofrecer, éstos se agrupan en dos categorías, servicios de distribución y servicios de estación.

1.4.6.1. Servicios de distribución

Son proporcionados por el AP y se encargan de la administración de estaciones dentro de la celda y su comunicación con estaciones de otras celdas. Se tienen 5 servicios de distribución que son los siguientes:

- **Asociación**.- Sirve para establecer la conexión entre el AP y las estaciones inalámbricas. Esto ocurre cuando una nueva estación ingresa a la celda o cuando se enciende la estación. Para empezar, anuncia su identidad y sus características como velocidades de transmisión soportadas, etc., así el AP puede admitir o denegar la asociación.

- **Disociación**.- Se produce cuando se rompe la conexión con el AP, debido a que la estación salió de la celda o a que fue apagada.

- **Reasociación**.- Se tiene cuando una estación cambia de una celda a otra, se asocia a otra estación base.

- **Distribución**.- Sirve para que le AP sepa donde enviar las tramas que arriban. Si son locales se envían por el aire y si son externas se envían por el cable.

- **Integración**.- Si las tramas deben ser enviadas por una red no 802.11, el servicio de integración maneja el direccionamiento y el formato para la traducción de 802.11 al estándar requerido.

1.4.6.2. Servicios de Estación

Se refieren a servicios solamente dentro de la celda, y son los siguientes:

- **Autenticación**.- Solamente se permite el acceso a estaciones autorizadas, por lo cual, primero deben autenticarse. El estándar 802.11 especifica el proceso de autenticación con el protocolo WEP que será descrito con detalle en el siguiente capítulo.

- **Desautenticación**.- Cuando una estación abandona la red se desautentica y luego se desasocia.

- **Privacidad**.- Este servicio permite privacidad de los datos que viajan en la red, para esto se utiliza esquemas de encripción.

- **Entrega de datos**.- Es el servicio esencial de transmisión y recepción de los datos.

1.4.7. DESCRIPCIÓN DEL ESTÁNDAR IEEE 802.11b

El 802.11 fue la base fundamental de los desarrollos de los fabricantes para productos de redes LAN inalámbricas. Sin embargo solo se especificaba la operación de 1 y 2 Mbps que con el paso de los años se volvió insuficiente.

Es por ello que en 1999 el IEEE libera el estándar 802.11b que extiende la velocidad hasta 11 Mbps a una frecuencia de 2.4 Ghz, aunque también permite el funcionamiento a 5.5, 2 y 1 Mbps.

Para que 802.11b llegue a la velocidad de 11 Mbps se desarrolló una nueva capa física para adherirla al estándar, ésta es HR- DSSS (*High Rate - Direct Sequence Spread Spectrum)* cuyas características fueron explicadas anteriormente.

Con este aumento de velocidad los fabricantes se lanzaron al desarrollo y fabricación de estos equipos, por lo cual el 802.11b es hoy en día el estándar más difundido en la industria.

1.4.8. DESCRIPCIÓN DEL ESTÁNDAR IEEE 802.11a

El estándar 802.11a se publica también en 1999 y extiende la velocidad hasta 54 Mbps pero a una frecuencia de 5 Ghz. Eso se logra utilizando la técnica OFDM (*Orthogonal Frequency Division Multiplexing)* descrita anteriormente. OFDM es más robusta que DSSS y permite llegar a la velocidad de 54 Mbps, además soporta las velocidades de 6, 9, 12, 18, 24,36 y 48 Mbps.

Su difusión no es tanta como 802.11b ya que los equipos requieren tecnología más cara y las necesidades de muchas empresas no sobrepasan los 11 Mbps de 802.11b. Sin embargo los precios de equipos 802.11a siguen bajando y llegará el momento en que la diferencia con 802.11b no sea tan significativa.

1.4.9. DESCRIPCIÓN DEL ESTÁNDAR IEEE 802.11g

Es el último desarrollo del IEEE, el borrador del 802.11g se publicó en el 2001 y fue ratificado en junio del 2003. Especifica el funcionamiento a 54 Mbps pero a la misma frecuencia de 802.11b de 2.4 Ghz, esto para establecer compatibilidad entre usuarios anteriores con 802.11b y usuarios nuevos con 802.11g.

La técnica de capa física utilizada es similar a OFDM de 802.11a, pero difiere en la banda utilizada, ya que funciona en los 2.4 Ghz, es OFDM en banda angosta.

Actualmente estos equipos están entrando en el mercado con bastante fuerza ya que permiten tener 54 Mbps con 802.11g para usuarios que requieran alta tasa de transmisión y 11 Mbps para usuarios que no requieran gran performance o que ya tengan instaladas tarjetas 802.11b. En la tabla 1.2 se muestra *un cuadro* comparativo de estas tecnologías.

Comparación de los estándares tecnológicos para redes LAN inalámbricas (WLAN)			
Estándar	802.11a	802.11b (base de usuarios más grande)	802.11g
Máxima Velocidad de datos	54 Mbps	11 Mbps	54 Mbps
Radiofrecuencia	5 Ghz	2.4 Ghz	2.4 Ghz
Distancia	25 a 75 pies	Más de 150 pies	100 a 150 pies
Compatibilidad con otros estándares WLAN	Incompatible con 802.11b o 802.11g	802.11g	802.11b
Problemas de Interferencia	Teléfonos inalámbricos a 5 Ghz	Hornos microondas, teléfonos inalámbricos a 2.4 Ghz, Bluetooth	Hornos microondas, teléfonos inalámbricos a 2.4 Ghz

Tabla 1.2 Cuadro comparativo de las tecnologías de redes inalámbricas de 802.11

1.4.10. APLICACIONES DE LAS REDES 802.11

En la actualidad las redes inalámbricas casi se encuentran en todas partes, en especial las redes 802.11 se han convertido en un complemento indispensable para las redes cableadas tradicionales. Los campos de aplicación de las redes 802.11 son muy diversos y se popularizan cada día más. Gracias a las redes inalámbricas, cada día se acerca más la computación ubicuota, donde la tecnología prácticamente rodea todo el entorno y pasa a formar una parte indispensable de la vida cotidiana. A continuación se describen los escenarios más comunes de aplicación de las redes inalámbricas.

1.4.10.1. Redes inalámbricas públicas

Para un cliente es muy importante saber que puede permanecer conectado mientras se encuentra en varios espacios públicos. Esto lleva a las empresas a ofrecer servicios de conexión inalámbrica gratuita para los usuarios que utilicen

sus instalaciones. En la figura 1.15 se muestran los escenarios más comunes para redes inalámbricas públicas.

- Muchos hoteles ofrecen a sus huéspedes la capacidad de conectarse a la red inalámbrica con sus equipos portátiles, esto es muy atrayente para personas de negocios que realizan viajes de trabajo o simplemente vacacionistas que tienen una *PDA*[1] y desean saber como están las cosas en el mundo.

- En restaurantes y cafeterías donde los usuarios buscan un lugar acogedor para trabajar.

- En muchos aeropuertos se está implementando redes inalámbricas en las zonas de espera de pasajeros. Esto con la finalidad de que las personas que esperan un vuelo puedan aprovechar mejor su tiempo.

- En bibliotecas y universidades es muy práctico tener acceso a la red desde cualquier sitio. Los estudiantes y profesores requieren realizar consultas rápidas, por ejemplo, acceder a bases de datos de información referente a proyectos o simplemente acceder a Internet.

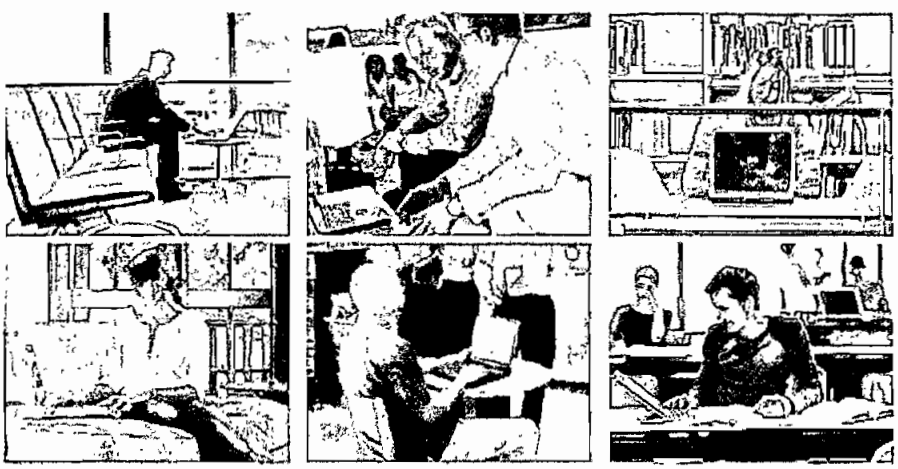


Fig. 1.15 Aplicaciones públicas de las redes inalámbricas de 802.11 [2]

[1] Asistente Digital Personal

[2] www.hp.com

1.4.10.2. Complemento de redes cableadas

Éste es uno de los campos de aplicación más difundido de las redes 802.11. En las empresas se tienen lugares como salas de reuniones, bodegas, áreas industriales donde el cableado no está disponible o donde simplemente no es sencilla la instalación de puntos de red.

Por ejemplo en la figura 1.16 se muestra la conexión de usuarios WLAN con servidores, impresoras y otros elementos de la red cableada.

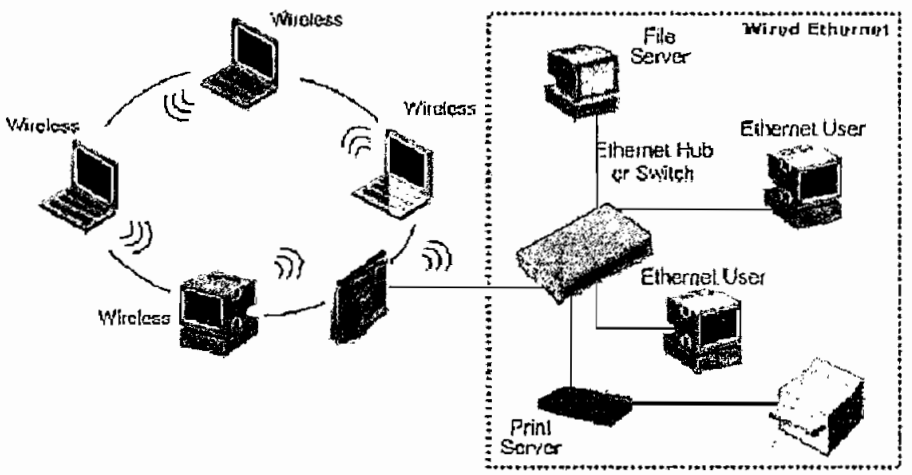


Fig. 1.16 Redes 802.11 como complemento de las redes cableadas tradicionales

En estos casos las redes 802.11 son el complemento perfecto para la red cableada tradicional, ofreciendo conectividad en esos lugares fácilmente. Así el personal puede movilizarse de su oficina a esos sitios con cobertura inalámbrica y mantenerse conectado con la misma funcionalidad de la red cableada.

1.4.10.3. Redes temporales

En algunas ocasiones se requiere instalar una red que va a ser utilizada solamente por una temporada y el resto de tiempo ya no es necesaria, además se requieren tiempos de instalación rápidos, esto se tiene por ejemplo en implementación de laboratorios temporales o en instalación de infraestructura de comunicaciones para eventos en coliseos, centros de exposiciones, etc.

Las redes cableadas no cumplen con estos objetivos. Instalar toda la infraestructura de cables no es sencillo, se requiere de tiempo, materiales y personal calificado, incrementando los costos de la solución. Además la red queda en desuso cuando ya no es necesaria.

En cambio al utilizar redes 802.11 se tiene un tiempo rápido de instalación y se evita gastar dinero en cableado. Además si la red es temporal simplemente se retiran los puntos de acceso dejando sin cobertura el sitio.

1.4.10.4. Redes Caseras

En la actualidad se está popularizando tener redes inalámbricas en los hogares, gracias a la reducción de los costos del equipo y a la proliferación de dispositivos con tarjetas inalámbricas como *PDA´s, laptops*, etc.

Por ejemplo se tiene el siguiente escenario, el padre de familia llega del trabajo con su *laptop*, los hijos trabajan en la PC del hogar que está conectada a Internet, y la madre de familia tiene una *PDA* para organizar sus actividades y obtener información importante de Internet.

Todos estos dispositivos podrían compartir el acceso a Internet en el hogar si se conectan mediante una red inalámbrica que los mantendría con conectividad de forma flexible.

1.4.10.5. Interconexión de edificios

Otro campo ocupado con éxito por las redes inalámbricas es la interconexión versátil de edificios, como sucursales de bancos, campus universitarios, etc. Las redes inalámbricas permiten instalaciones rápidas y económicas, generalmente son principalmente utilizadas como *backup* de enlaces de cable.

1.5. RETOS ACTUALES DE LAS REDES LAN INALÁMBRICAS

Como toda nueva tecnología, las redes inalámbricas se enfrentan a nuevos retos que deben ser superados para convertirse en una solución completa para el mercado.

Estos retos son verdaderas barreras que los especialistas tratan de derivar mediante el estudio de nuevas soluciones y estándares para las WLAN. Los principales retos a los que se enfrentan las WLAN son la seguridad, la movilidad y la configuración.

1.5.1. RETOS DE SEGURIDAD

La red cableada posee una seguridad inherente ya que un atacante necesita acceder a la red a través de una conexión por cable para realizar su cometido, esto implica acceso físico a la red que no es sencillo de obtener.

En cambio en las WLAN donde las señales viajan libremente por el aire, los datos pueden ser fácilmente interceptados. Por ello si la WLAN no provee de mecanismos de seguridad robustos a sus usuarios no podrían ser utilizadas ya que constituirían un agujero de seguridad para todo el sistema. En la figura 1.17 se muestra un ejemplo de ataque típico a las redes inalámbricas.

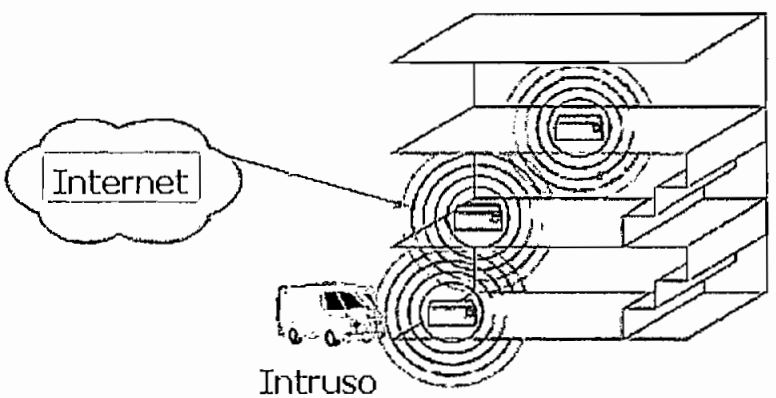


Fig. 1.17 Esquema de ataque a una red inalámbrica [11]

Las redes 802.11 proveen varios mecanismos de seguridad, el básico es el del SSID que los usuarios deben conocer para poder acceder a la red, sin embargo los AP envían en tramas de administración la información del SSID, razón por lo cual esto no es un gran alivio.

En el estándar 802.11 original se incluye WEP que provee autenticación y encripción mediante claves compartidas de 40 y 128 bits, el problema es que la clave es estática y se debe colocar en todos los usuarios de la red.

Finalmente el mecanismo más robusto de seguridad es el definido en el estándar 802.1x del IEEE que será tratado en el siguiente capítulo.

Es precisamente este reto que el presente trabajo pretende enfrentar ofreciendo mecanismos de seguridad robustos y sencillos de administrar e implementar.

1.5.2. RETOS PARA LOS USUARIOS MÓVILES

Si se tiene una red grande con varios AP para cubrir toda el área de servicio, una estación que se desplaza físicamente se desasocia del AP anterior y se asocia a un nuevo AP, la asociación entre la tarjeta NIC y el AP se debe mantener para tener conectividad en la red.

Esto implica un problema administrativo complejo pues el usuario debe cruzar límites de subredes o dominios de control administrativo. Si se tiene habilitado DHCP [1] y el usuario cruza un límite de subred, la dirección IP asignada originalmente a la estación puede dejar de ser adecuada para la nueva subred.

Si la transición supone cruzar dominios administrativos, es posible que la estación ya no tenga permiso de acceso a ciertas partes de la red dependiendo del tipo de usuario que sea.

---

[1] Asignación dinámica de direcciones IP

El problema va más allá de acceder a una WLAN empresarial, un usuario puede conectarse a una red inalámbrica en otra empresa, en sitios públicos e incluso en su propio hogar.

Por ejemplo un usuario deja su oficina y va a visitar otra compañía, primero al abandonar su sitio de trabajo se desasocia de la WLAN de su empresa, luego se dirige al Aeropuerto donde va a tomar el vuelo, pero en la sala de espera decide ultimar detalles del trabajo, entonces puede conectarse a esa WLAN pública y mediante Internet y una VPN[1] puede ingresar a la red de su empresa.

Finalmente llega a su destino y la empresa que visita puede tener una WLAN a la que seguramente podrá asociarse como invitado para proveerle acceso a Internet y no a la intranet de la empresa, con Internet podría nuevamente conectarse vía VPN a su empresa y empezar la reunión.

Para este ejemplo, la movilidad es una situación que debe pensarse muy detenidamente. La configuración puede ser un problema para el usuario móvil, ya que las distintas configuraciones de red pueden suponer un reto si la estación inalámbrica del usuario no tiene capacidad para configurarse automáticamente.

1.5.3. RETOS DE CONFIGURACIÓN

En los momentos actuales se tiene un verdadero abanico de soluciones WLAN, se tienen redes con seguridad, sin seguridad, con autenticación, sin autenticación, con encripción, sin encripción, etc.

La configuración de una WLAN de una empresa es muy diferente a la configuración de una WLAN de hogar. La diferencia empieza por el SSID de la WLAN y continúa con los parámetros de seguridad utilizados.

---

[1] Redes privadas virtuales

Podría ser necesario tener una configuración para el trabajo, donde la red funciona en modo de infraestructura, y otra configuración para el domicilio, donde funciona en modo *ad hoc*. Entonces, sería necesario elegir qué configuración se va a utilizar en función del sitio donde se encuentre.

Por ello los fabricantes deben proveer mecanismos para elegir diferentes perfiles automáticamente dependiendo de donde se encuentre el usuario, de tal forma que no sea un verdadero dolor de cabeza cambiar la configuración cada vez que el usuario se mueve de sitio.

CAPÍTULO 2

2. PRINCIPALES MECANISMOS DE SEGURIDAD EN LAS REDES LAN INALÁMBRICAS

2.1. ASPECTOS GENERALES DE LA SEGURIDAD EN REDES

La seguridad en las redes de datos ha sido uno de los aspectos más estudiados en los últimos tiempos. Cada día muchas empresas en el mundo son atacadas y ven afectada su seguridad lo que genera pérdidas económicas y de imagen a las mismas.

Los ataques son perpetrados por personas con conocimiento medio y alto de los sistemas, no es necesario ya ser un experto para realizar ataques sencillos. Una persona con un poco de tiempo, puede encontrar muchas herramientas disponibles en Internet para provocar muchos dolores de cabeza a los administradores de las redes corporativas. Además con los continuos estudios y desarrollos de los sistemas se encuentran nuevas vulnerabilidades, lo que hace que los sistemas de seguridad no sean estáticos, y por tanto caduquen y deban ser nuevamente replanteados y actualizados. Por esto un sistema que se consideraba seguro hace unos 5 años, hoy no lo es, ya que la seguridad es un proceso continuo de fortalecimiento del sistema.

2.1.1. IMPORTANCIA DE LA SEGURIDAD EN REDES

La seguridad de los sistemas de las empresas es de extrema importancia debido a los siguientes aspectos [7]:

- La información que poseen es de gran valor para su negocio, por ejemplo los bancos tienen información sobre la cantidad exacta de dinero que

corresponde a cada usuario, y si una persona maliciosa logra cambiar los datos provocaría una falta de credibilidad terrible en el banco.

- Un ataque puede provocar que una entidad deje de prestar un servicio debido al colapso del sistema. En el caso de empresas que proveen el servicio de Internet (ISP[1]), si su sistema sufre un ataque y dejan sin servicio a sus usuarios tendrían graves pérdidas económicas y generaría desconfianza en la misma.

- A la competencia le gustaría mucho conocer la información de la empresa, saber sus reportes financieros, ventas, cartera de clientes, proyectos, etc. Por ello de la seguridad depende que se mantengan las ventajas competitivas sobre las demás empresas.

Por todo esto, el campo de la seguridad en redes ha sido muy estudiado y se han fundado diferentes organismos encargados de realizar los diferentes estándares y mecanismos de seguridad, además de estudiar su continua mejora.

2.1.2. HISTORIA DE LA SEGURIDAD EN REDES

La seguridad de las redes es un tema relativamente nuevo [8]. Hace 30 años las computadoras no se conectaban en red de forma masiva, la tecnología no era muy difundida y lo que se tenía era acceso a *host* mediante puertos RS-232[2].

Luego con la aparición de las redes de conmutación de paquetes y sobretodo al uso de protocolos como TCP/IP (*Transmission Control Protocol / Internet Protocol*), los sistemas de red evolucionaron para ser más abiertos y su tecnología empezó a ser más conocida.

---

[1] *Internet Service Provider*

[2] Puerto de comunicaciones serial de 25 pines

Esto trae el problema de que los datos viajen por diferentes puntos que no están bajo el control de los clientes, es decir que los datos de las redes seguras, las LAN´s corporativas, viajen a través de redes inseguras, las redes WAN.

Además como la tecnología de redes empezó a ser más estudiada, nueva información estaba al alcance de los técnicos, originándose la aparición de los *hackers* que retan la seguridad de los sistemas y continuamente buscan vulnerabilidades simplemente por pasatiempo o para fines maliciosos.

Hoy en día las necesidades de comercio electrónico y el crecimiento de aplicaciones en Internet hacen que se encuentre un compromiso entre el rendimiento y la seguridad de la red. Por ello aparecen los *firewalls*[1], las VPN´s, las firmas y certificados digitales, y todos los diferentes mecanismos que en conjunto proveen de seguridad a un sistema completo.

Luego desde 1997 cuando se publica el estándar 802.11 hasta hoy en día la tecnología de redes inalámbricas ha revolucionado completamente el mercado de las redes de datos. Con un crecimiento muy grande son la mayor tecnología en expansión.

Por supuesto esto ha ido de la mano del desarrollo de nuevos sistemas de seguridad para redes inalámbricas de tal forma que puedan ser utilizadas con total confianza por las empresas.

2.1.3. FUNDAMENTOS DE LA SEGURIDAD

Un sistema de seguridad para ser completo y eficiente debe ser capaz de proveer 4 premisas básicas de seguridad: autenticación, confidencialidad, integridad y disponibilidad [9].

---

[1] Dispositivo que divide una red segura de una insegura

2.1.3.1. Autenticación

El objetivo de la autenticación es verificar la identidad del usuario, garantizar que es quien dice ser. No solo es suficiente con que un usuario se identifique, ya que éste puede estar suplantando la identidad de un usuario autorizado.

Se puede clasificar los métodos de autenticación de acuerdo a las credenciales que el usuario presenta, así se puede diferenciar aquellos que se basan en datos conocidos por el usuario (*password*), los que requieren que el usuario lleve un dispositivo (*token card*), y finalmente los métodos biométricos que se basan en rasgos físicos del usuario (retina del ojo).

2.1.3.2. Confidencialidad

La confidencialidad es garantizar la privacidad de la información, solamente los usuarios autorizados deben ser capaces de leer la información y nadie más. Esto se logra utilizando métodos de encripción en los datos para que viajen de forma segura a través de la red.

2.1.3.3. Integridad

La integridad se refiere a prevenir la alteración no autorizada de la información. Se debe verificar que los datos no fueron modificados por usuarios no autorizados o por algún accidente en la transmisión.

Para garantizar la integridad se utilizan los algoritmos de *hash*, que se aplican al grupo de datos y retornan un valor único correspondiente a esa combinación de datos, el valor resultante es el valor de *hash* y es transmitido junto con la información, en recepción se compara el valor de *hash* recibido con el valor de *hash* calculado con los datos recibidos.

2.1.3.4. Disponibilidad

Es el grado de confiabilidad del sistema, su resistencia a los ataques y su capacidad de recuperarse rápida y completamente después de éstos. Para garantizar la disponibilidad de un sistema se deben tomar medidas de seguridad físicas y técnicas en el sistema, por ejemplo no permitir el acceso de extraños a los cuartos de equipos, tener enlaces redundantes, etc. Estas medidas deben estar desarrolladas en la política de seguridad de la compañía, especificando procedimientos y responsables de las mismas.

2.1.4. AMENAZAS, ATAQUES Y VULNERABILIDADES

Una vez claras las ideas de un sistema seguro, se debe comprender los diferentes aspectos que se presentan en el mismo. Cuáles son los posibles ataques, qué amenazas posibles se presentan y las vulnerabilidades que posee.

2.1.4.1. Ataques

Los ataques son las técnicas utilizadas para explotar las debilidades de los sistemas. Pueden ser Pasivos y Activos.

a) Ataques Pasivos

Son ataques que no realizan una actividad evidente en el sistema, por lo general se utilizan para obtener información o para realizar tareas previas a un ataque activo. Son difíciles de detectar por su naturaleza.

Un ejemplo de estos ataques es el de *port scanning*, que es un escaneo de puertos abiertos, por ejemplo en un servidor, para buscar una puerta de entrada al mismo.

b) Ataques Activos

Realizan una actividad evidente en el sistema, son los que verdaderamente crean desastres y generalmente utilizan la información obtenida o los agujeros creados por los ataques pasivos. Por ejemplo luego de realizar el ataque pasivo de *port scanning* se puede ver los puertos abiertos para luego entrar en el servidor y realizar un ataque de negación de servicio, que ocurre cuando el servidor se satura de peticiones falsas.

2.1.4.2. Amenazas

Son todas las posibles situaciones que pueden afectar el normal funcionamiento del sistema. Se pueden tener amenazas de diversa índole; amenazas técnicas como proliferación de virus o fallas del sistema y amenazas no controlables como desastres naturales.

2.1.4.3. Vulnerabilidades

Son todas las debilidades que pueden presentar las redes y sistemas. Se pueden tener vulnerabilidades de tipo físico como poco control de acceso de personal al cuarto de equipos, vulnerabilidades en los diseños de software como agujeros de seguridad, puertas traseras, etc.

2.2. ENCRIPCIÓN, INTEGRIDAD DE MENSAJES Y CERTIFICADOS DIGITALES

Los diferentes mecanismos de seguridad existentes actualmente en el mercado se basan en los estándares y protocolos desarrollados por la IEEE y el IETF principalmente. Estos estándares y protocolos a su vez utilizan los sistemas de criptografía para el desarrollo de la seguridad, por lo cual es necesario tener una fuerte base sobre el funcionamiento y la implementación de los diferentes mecanismos de seguridad que provee la criptografía [10].

2.2.1. CRIPTOGRAFÍA

La clave para la seguridad de la información en la red es la criptografía. La criptografía es la encargada de estudiar los diferentes métodos de cifrado de mensajes, puede ser utilizada para implementar mecanismos de autenticación, integridad y confidencialidad de la información.

La encripción, que es el proceso usado por la criptografía para cifrar los mensajes, no es reciente, pues la humanidad la ha venido utilizando desde hace 4000 años. Uno de los primeros métodos de encripción que está documentado es atribuido a Julio Cesar, que se basaba en la sustitución de las letras de un documento por la tercera letra que le correspondiese en el alfabeto. Así la A se convertía en una D, la B en E, etc.

La encripción se basa en que el emisor emite un mensaje en claro, que es tratado mediante un cifrador con la ayuda de una clave, para crear un texto cifrado. Este texto cifrado, por medio del canal de comunicación establecido, llega al descifrador que convierte el texto cifrado, apoyándose en otra clave, para obtener el texto en claro original.

Las dos claves implicadas en el proceso de cifrado/descifrado pueden ser o no iguales dependiendo del sistema de cifrado utilizado.

La seguridad del sistema de encripción utilizado depende de lo secreta que sea la clave y de la longitud de la misma, por lo cual conocer el algoritmo de encripción utilizado no es relevante. Si un método de encripción es dependiente del algoritmo utilizado, se le considera un algoritmo restrictivo.

Es importante que los algoritmos utilizados no tengan debilidades serias o explotables, sin embargo todos los algoritmos pueden ser rotos por un método o por otro, lo importante es que no tenga debilidades inherentes que un atacante pueda explotar.

Ahora los tipos de encripción se pueden clasificar de acuerdo a las claves involucradas y al tipo de técnica de encripción utilizada.

2.2.1.1. Tipos de encripción por la técnica utilizada

Se tiene la encripción de flujo y la encripción por bloques:

a) Encripción de flujo

Estos algoritmos de encripción procesan el texto plano para producir un flujo de texto cifrado. La figura 2.1 muestra el funcionamiento de la encripción de flujo.

Los algoritmos de este tipo tienen muchas debilidades, la principal es el hecho de que los patrones en el texto plano se reproducen en el texto cifrado. Para demostrar esto se puede utilizar el sistema rudimentario de cifrado de la figura 2.2.

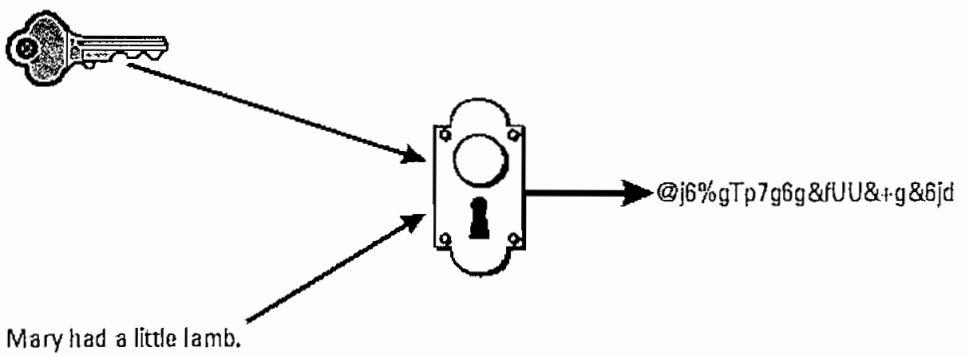


Fig. 2.1 Encripción de flujo [9]

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

Fig. 2.2 Sistema de cifrado simple [9]

Con este sistema se puede cifrar por ejemplo el siguiente mensaje:

Texto Plano: todos para uno y uno para todos

Texto Cifrado: ni4im j1l1 ohi s ohi j1l1 ni4im

Los patrones en el texto plano se reflejan en el texto cifrado. Las palabras y letras que se repiten en el texto plano se repiten en el texto cifrado. El conocer las palabras que se repiten hace fácil romper el código.

Otra debilidad de los algoritmos de encripción de flujo es que son vulnerables a ataques de sustitución, incluso sin necesidad de romper los códigos. En estos ataques se toma una porción vieja de código y se la inserta en un nuevo mensaje. Ejemplos de estos algoritmos son *Vernam* y RC4 (*Rivest Cipher 4*).

b) Encripción por Bloques

Los algoritmos de encripción por bloques se diferencian de los de flujo por que encriptan y desencriptan la información en bloques de tamaño fijo en lugar de hacerlo letra por letra. El algoritmo pasa un bloque de información del texto plano por si, para generar un bloque cifrado.

El bloque cifrado es relativamente más grande que el bloque original de información, en términos de *throughput* [1], si el bloque cifrado es el doble del bloque original, implica que el *throughput* disminuye a la mitad. Otra característica de los algoritmos de bloque es que no presentan un patrón detectable. En la figura 2.3 se muestra el funcionamiento del algoritmo de encripción por bloques.

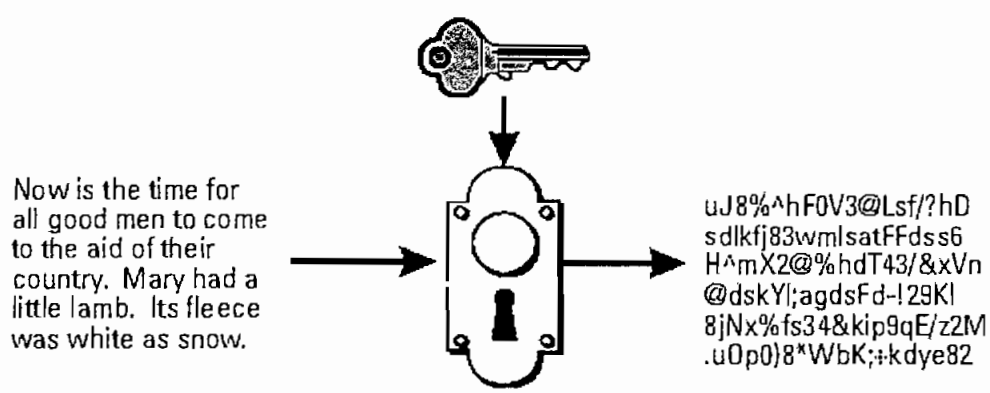


Fig. 2.3 Encripción por bloques [9]

[1] Datos efectivos transmitido por segundo

Ejemplos bien conocidos de este tipo de algoritmo son IDEA (*International Data Encryption Algorithm*) y DES (*Data Encryption Standard*).

2.2.1.2. Tipos de encripción por las claves utilizadas

Los algoritmos de encripción pueden utilizar una sola clave para encriptar y desencriptar la información, o pueden utilizar 2 diferentes claves, una para encriptar y otra para desencriptar.

a) Encripción Simétrica

Estos algoritmos utilizan una clave secreta o privada que los participantes comparten para intercambiar los datos encriptados. La misma clave sirve para encriptar y desencriptar los datos. Este proceso se muestra en la figura 2.4.

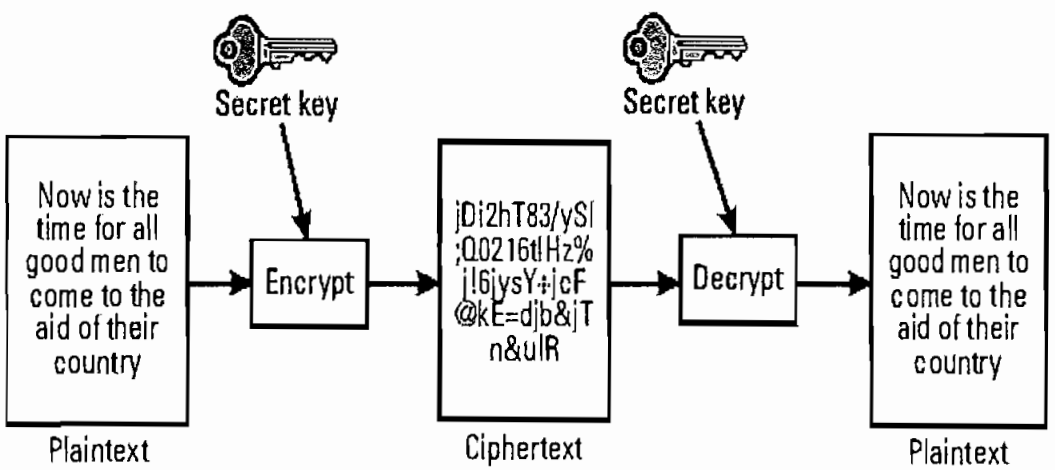


Fig. 2.4 Encripción Simétrica [9]

La fuerza de estos algoritmos depende de la longitud de la clave y de cuan secreta sea la misma, además los algoritmos de encripción de clave secreta son relativamente rápidos. Los algoritmos de clave secreta más importantes son: DES, IDEA, CAST y RC4.

a.1) DES

Fue desarrollado por IBM y adoptado por el Gobierno de los Estados Unidos como su estándar oficial para información no secreta. DES (*Data Encryption Standard)*, fue ampliamente adoptado por la industria como producto de seguridad.

DES consiste de un algoritmo y de una clave. La clave es una secuencia de 8 bytes, resultando una clave de 64 bits, pero como cada byte posee paridad, la clave efectiva se reduce a 56 bits.

La clave original de DES era de 128 bits pero la NSA, la agencia de seguridad nacional de los Estados Unidos no lo permitió e hizo que IBM la reduzca a 56, esto para que los mensajes encriptados con DES sean más fáciles de descifrar para la NSA.

Por ello DES tiene el problema de tener una clave muy corta, sin embargo IBM para solucionar este problema desarrollo el triple DES, que utiliza 2 claves en tres etapas de encripción.

a.2) IDEA

Internacional Data Encryption Algorithm, es un algoritmo de clave simétrica por bloques. Fue desarrollado por el *Swiss Federal Institute* a comienzos de los 90. Utiliza una clave de 128 bits, por lo que es más eficiente que DES. Como no fue desarrollado en los Estados Unidos, no posee restricciones de exportación.

a.3) CAST

Este algoritmo soporta claves de longitud variable, que pueden ir desde los 40 hasta los 256 bits. Utiliza bloques de tamaño de 64 bits, igual que DES. CAST fue desarrollado para ser de 2 a 3 veces más rápido que DES. Fue desarrollado por Carlisle Adams y Strafford Travares y patentado por *Entrust Technologies*. Existen versiones comerciales y no comerciales de CAST. Es utilizado en PGP (*Prety Good Privacy*).

a.4) RC4

Desarrollado por Ron Rivest de RSA. Es un algoritmo de cifrado de flujo con claves de longitud variable, especialmente la clave de 128 bits es muy efectiva. Existe una versión de exportación de clave de 40 bits que utiliza el *Internet Explorer* y el *Netscape.*

b) Encripción Asimétrica

Por muchos años la criptografía se basó en algoritmos de clave simétrica. En 1970 dos científicos de computación, Whitfiel Diffe y Martin Hellman de la Universidad de *Stanford* introdujeron el concepto de criptografía asimétrica que también se conoce como criptografía de clave pública. Este sistema utiliza 2 claves en lugar de una como lo hace la encripción simétrica, así se tiene una clave pública y una clave privada, se llaman así por que efectivamente una clave es publicada y la otra se mantiene en secreto. Así un mensaje que se encripta con la clave pública solo puede ser desencriptado con la clave privada. Y a la inversa un mensaje encriptado con la clave privada solo puede ser desencriptado con la clave pública como se muestra en la figura 2.5.

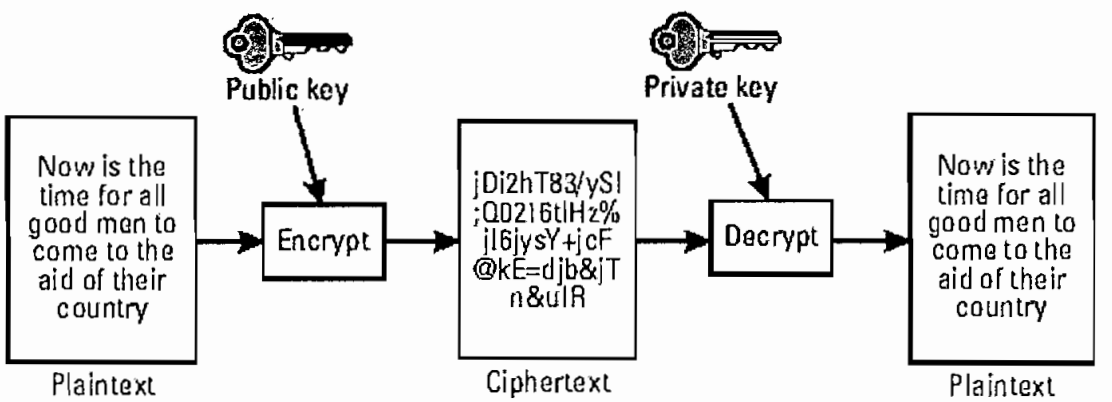


Fig. 2.5 Encripción Asimétrica [9]

Con la ayuda de la criptografía de clave pública es posible establecer comunicaciones seguras con cualquier entidad. Por ejemplo si A desea comunicarse con B, que es una persona totalmente desconocida y que se encuentra en un sitio geográfico remoto, el proceso es el siguiente. A envía su clave pública a B, con la cual, B encriptará los datos que vaya a enviar hacia A.

Cuando A recibe los datos, los desencripta con su clave privada, solo la clave privada de A puede desencriptar los datos encriptados con su clave pública. Ahora, si B envía su clave pública a A, entonces A puede encriptar datos para B con su clave pública, los datos solamente son desencriptados por B que tiene su clave privada.

No es importante si el intercambio de claves públicas de A y B se realiza en una red insegura, ya que el saber la clave pública no implica conocer algo de la clave privada. La seguridad solo se ve afectada si las claves privadas son comprometidas.

Los sistemas criptográficos asimétricos o de clave pública son más versátiles que los sistemas de clave compartida. Estos sistemas permiten la funcionalidad de autenticación, no repudio de los participantes y el uso de certificados digitales que serán tratados posteriormente.

Esto sistemas son más escalables para redes grandes que los sistemas simétricos. En la tabla 2.1 se resume las ventajas y desventajas de los sistemas de criptografía de clave pública.

Ventajas	Desventajas
Una clave secreta compartida no es necesaria	Recursos computacionales mayores
Permite Autenticación	Se requiere de una Autoridad Certificadora
Provee No - Repudio	
Escalable	

Tabla 2.1 Ventajas y Desventajas de los sistemas de criptografía de clave pública

Hoy en día existen 3 algoritmos de clave pública ampliamente utilizados, *Diffie*-Hellman, RSA y DSA.

b.1) Diffie-Helman

Este algoritmo fue desarrollado por Whitfiel Diffe y Martin Hellman en la Universidad de *Stanford*, y fue el primer algoritmo de clave pública utilizado. Se basa en la dificultad de procesar computacionalmente algoritmos discretos.

Es muy utilizado en el intercambio de llaves compartidas para establecer conexiones simétricas entre 2 entidades, muy utilizadas en protocolos de administración de llaves para *IPSec*[1].

Para una comunicación espontánea con *Diffie-Helman*, las dos entidades involucradas deben generar cada una un número aleatorio para servirles de clave privada. Luego intercambian sus claves públicas.

Una vez realizado el intercambio de claves públicas, cada entidad aplica su clave privada a la clave pública del otro para generar un valor idéntico en ambos lados, este valor es la clave compartida con la cual encriptarán e intercambiarán información.

b.2) RSA

Fue desarrollado por Ron Rivest, Adi Shamir y Len Adelman en el MIT (Instituto Tecnológico de *Massachusets*). RSA genera las claves multiplicando números primos muy grandes. Su fuerza radica en el hecho de que es muy difícil factorar 2 números primos muy grandes. RSA provee las facilidades para las firmas digitales que serán tratadas más adelante en este capítulo. Es utilizado en SSL (*Secure Socket Layer*) para iniciar la sesión y en seguridad para correo electrónico PEM (*Privacy- Enhanced Mail*).

b.3) DSS

Digital Signature Standard, utilizado para firmas digitales que serán tratadas posteriormente en este capítulo.

---

[1] IP Seguro

2.2.1.3. Ruptura del código

Desde que existen los sistemas de encripción, existe gente que trata de violarlos. Existen varios métodos que se han desarrollado para quebrar el cifrado, algunos son ingeniosos, otros son sofisticados y técnicos, mientras que otros son exclusivamente de fuerza.

A continuación se explican las principales técnicas utilizadas para romper la seguridad.

a) Conocimiento del texto plano

Se basa en conocer el texto plano encriptado en el mensaje cifrado. Conociendo ambos, el texto plano y el mensaje cifrado del mismo, el código puede ser roto por reingeniería y obtener la clave utilizada.

b) Eligiendo un texto plano

Se basa en la habilidad de los atacantes para conocer un texto encriptado, es decir "adivinar" el texto plano y proceder a encontrar la clave con el texto encriptado para descifrar el código. Con este método Estados Unidos rompió el código japonés en la Segunda Guerra Mundial.

c) Criptoanálisis

Técnicamente cualquier método utilizado para romper un código es criptoanálisis. Sin embargo el criptoanálisis se refiere a específicamente emplear análisis matemático para romper el código. Este método requiere de gran habilidad y sofisticación, por lo cual es utilizado por gobiernos y centros de estudio que poseen súper computadoras para realizar los análisis.

La principal agencia en el mundo que se dedica al criptoanálisis es la NSA (*National Securing Agency)* de los EUA, que cuenta con miles de profesionales y sofisticado equipo para realizar estos análisis matemáticos.

d) Fuerza Bruta

El método de fuerza bruta trata todas las posibles combinaciones de las claves o de los algoritmos para romper el código. Para realizar esta tarea se debe tener una tremenda capacidad de cómputo, pero si el algoritmo es sencillo y la clave no es muy larga se puede utilizar una PC común.

En cambio si el algoritmo es complejo y la clave es grande, se requiere poder computacional avanzado.

e) Ingeniería Social

Este método confía en romper el código obteniendo información de alguien que conoce el sistema de cifrado o la forma misma de romperlo. Para obtener la información se soborna o engaña a la persona para que la revele.

f) Otros

Existen otros tipos de ataques para romper la seguridad. Uno de ellos es el ataque de substitución. Un atacante inserta un mensaje previo, en un mensaje legítimo, por lo que no es necesario romper el cifrado.

Otra técnica más sofisticada es el ataque de sincronismo, teóricamente se puede romper el código conociendo los tiempos de encripción y desencripción de los datos, para esto se debe conocer bien el algoritmo que se está utilizando.

2.2.2. Integridad de Mensajes

Con la integridad de mensajes se espera prevenir o detectar la alteración de los mismos durante su transmisión. La técnica más empleada es la conocida como función *hash*.

La función *hash* toma un mensaje de cualquier longitud, lo procesa y obtiene como resultado un valor de longitud fija, el resultado se conoce como valor *hash*.

La longitud del mensaje original no afecta la longitud del valor *hash*. El valor *hash* es una suma de comprobación (*checksum*) criptográfica del mensaje, con el cual se comprueba si existió alteración durante la transmisión.

Por ejemplo al utilizar correo electrónico, la función *hash* se aplica al mensaje tanto en la transmisión como en la recepción. Si el mensaje es modificado durante la transmisión, el valor *hash* calculado en recepción no coincidirá con el valor *hash* calculado en la transmisión.

La función *hash* debe ser de una sola vía, es decir que no se puede recuperar el mensaje a partir del valor *hash*. Además la posibilidad de colisión de los valores *hash* debe ser pequeña. Una colisión ocurre cuando se obtiene el mismo valor *hash* para 2 o más mensajes únicos. El valor *hash* debe ser diferente para mensajes diferentes. A continuación se describen las principales implementaciones de algoritmos *hash*.

2.2.2.1. MD4

Desarrollado por Ron Rivest de RSA. MD4 es una función de una vía que procesa en tres rondas el mensaje de longitud variable y obtiene como resultado un valor *hash* de 128 bits. Un análisis del algoritmo demostró que no es de una vía por lo menos en las dos primeras rondas y que es susceptible de colisión.

2.2.2.2. MD5

Fue creado también por Rivest de RSA, como una mejora de MD4, de igual forma genera un valor *hash* de 128 bits procesando el mensaje. Este valor que es como una huella dactilar del mensaje sirve para procesar la integridad del mensaje.

Aunque MD5 es más seguro que MD4, también presenta algunas debilidades, también es susceptible de colisión, pero no por el algoritmo en sí, sino por la

limitación de la longitud del valor *hash* mismo. MD5 es muy utilizado en firmas digitales

2.2.2.3. SHA-1

Es un algoritmo de una sola vía utilizado para firmas digitales. Se deriva de SHA que fue desarrollado por la NIST (*National Institute of Standards and Technology*) de los EUA en 1994. Es ligeramente más lento que MD5, pero es más seguro. SHA-1 produce un valor *hash* de 160 bits, por lo cual es más resistente contra ataques de fuerza bruta que MD5.

2.2.2.4. RIPEMD

Es una función *hash* que fue desarrollada por el proyecto de la Comunidad Europea RIPEMD (*RACE Integrity Primitives Evaluation, Message Digest*). Existen varias extensiones de este algoritmo, de 128, 160 y de 256 bits.

2.2.3. FIRMAS DIGITALES Y CERTIFICADOS DIGITALES

Para tener un alto nivel de confidencialidad y poder confiar plenamente en la integridad de la información, las partes involucradas deben poder autenticar la identidad de la otra parte; con el uso de encripción de clave pública se garantiza la confidencialidad de la información pero no se puede asegurar la identidad de los participantes.

En el ejemplo presentado anteriormente de una comunicación con encripción de clave pública entre A y B, ninguna de las partes puede estar segura de la identidad del otro, cómo puede asegurar A que tiene la clave pública de B, y que por ejemplo una entidad X interceptó la clave pública de B y en su lugar envió su clave pública.

Este problema de autenticación fue por muchos años el mayor obstáculo para potencializar el uso de Internet para transacciones comerciales. Gracias al desarrollo de la tecnología de certificados digitales y firmas digitales ahora se puede realizar comercio electrónico con tranquilidad.

2.2.3.1. Firmas Digitales

Una firma digital permite al receptor autenticar la identidad del transmisor y verificar la integridad del mensaje. Para esto la firma digital utiliza encripción de clave pública y funciones de *hashing.* Para la autenticación el transmisor debe conocer de forma confiable cuál es la clave pública del transmisor, ya sea por conocimiento previo o por medio de un tercero confiable.

La firma digital se genera aplicando la función *hash* al mensaje y luego encriptando este valor *hash* con la clave privada del transmisor. El transmisor envía el mensaje en texto plano y la firma juntos al receptor. El receptor desencripta el valor *hash* con la llave pública del transmisor y verifica la integridad del mensaje. También se verifica la identidad del transmisor ya que solamente si el valor *hash* fue encriptado con la llave privada del transmisor entonces se puede desencriptar con la llave pública del mismo.

La figura 2.6 ilustra este proceso. La versatilidad de las firmas digitales radica en que son casi imposibles de falsificar y son fáciles de verificar.

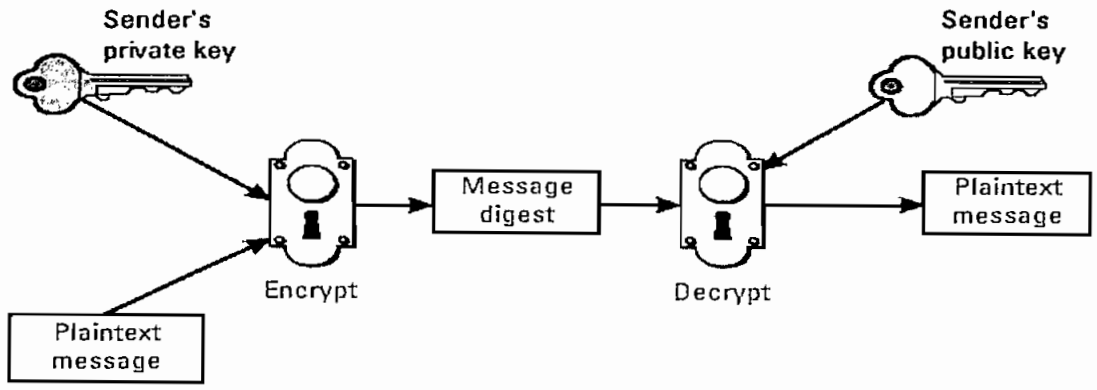


Fig. 2.6 Firma Digital [9]

Sin embargo existe un problema que queda pendiente, y es el de intercambiar las claves públicas y asegurar que pertenezcan a las entidades correspondientes. Este problema se soluciona con el uso de Certificados Digitales y Autoridades Certificadoras que serán tratados más adelante.

Existen 2 estándares actualmente en el mercado para firmas digitales, ambos se basan en el estándar X.509 de la ITU (*International Telecommunications Union*).

El primero fue desarrollado por RSA *Data Security* en 1977, que por supuesto, utiliza el algoritmo de clave pública RSA tanto para encripción como para autenticación.

El segundo estándar es el DSS (*Digital Signature Standard)* seleccionado por el NIST en 1994.

2.2.3.2. Certificados Digitales

Las firmas digitales se utilizan para verificar que el mensaje no haya sido alterado y autenticar la identidad del transmisor mediante su clave pública. Pero como se mencionó anteriormente existe un problema.

Se tiene nuevamente A y B que son dos entidades que desean intercambiar información de manera segura, A y B se encuentran en sitios remotos y no se conocen entre sí, el problema es cómo obtener la clave pública de A y de B para iniciar el proceso de comunicación de forma confiable y rápida.

La solución más práctica es publicar las claves públicas de las entidades en un sitio Web, por ejemplo B puede tener un sitio Web donde publica su clave pública para que cualquiera que lo requiera la pueda obtener.

Pero esto trae un problema más grave, por ejemplo A desea la clave pública de B, (Cb), para iniciar una comunicación segura, A ingresa el URL del sitio Web de B,

a continuación su navegador busca la dirección DNS de la página de inicio y envía una solicitud GET, como se muestra en la figura 2.7.

Por mala suerte un atacante X intercepta el mensaje y retorna una página Web falsa, probablemente una copia de la de B, pero con la clave pública de X, una Cx en lugar de Cb. Como A ya tiene lo que cree ser la clave pública de B, envía los mensajes encriptados realmente con la clave pública de X. Así X puede leer todos los mensajes que le envíen a B, e incluso modificarlos y encriptarlos con la clave pública de B para enviarlos a éste nuevamente.

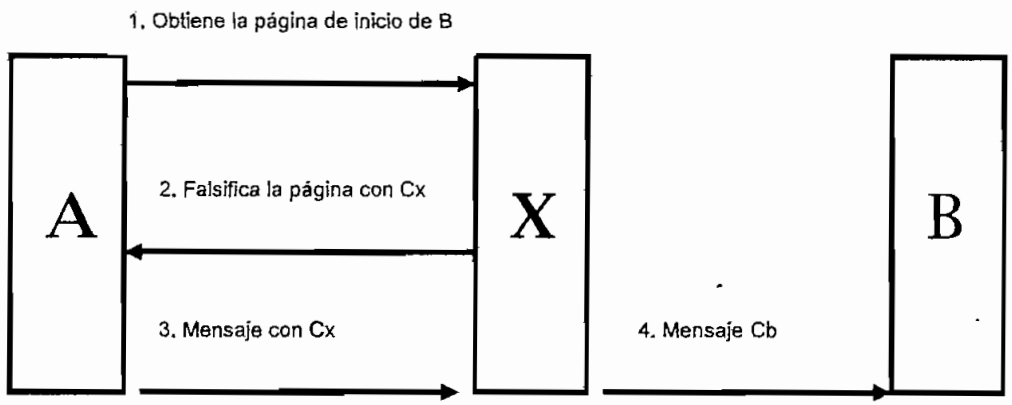


Fig. 2.7 Intercepción de la clave pública

Con este ejemplo se ve la necesidad de encontrar un mecanismo de intercambiar las claves públicas de manera segura y práctica.

Por ello nacen los Certificados Digitales. Un certificado digital es un documento digital emitido por una Autoridad Certificadora utilizando una infraestructura jerárquica de clave pública.

El certificado digital sirve para asociar un individuo o una entidad con su clave pública proveyendo los medios para una comunicación espontánea donde las partes no han tratado entre sí jamás. Permite tener un alto nivel de confidencialidad y autenticación de la identidad de los participantes. La Autoridad Certificadora (CA) que emite los certificados digitales debe ser una institución bien conocida y confiable, por ejemplo gobiernos y empresas de tecnología

importantes. La CA firma los certificados que emite con su clave privada. Esto provee confirmación independiente de que una entidad o individuo es en efecto quien dice ser.

El funcionamiento de los certificados digitales se puede entender mejor con un ejemplo práctico. Nuevamente se tiene 2 entidades totalmente desconocidas entre sí, A quiere enviar a B su clave pública, así B puede verificar la firma digital de A utilizando su correspondiente clave pública. Pero cómo se puede asegurar B que efectivamente va a obtener la clave pública de A y no la de un atacante X.

La respuesta es obteniendo la clave pública de A de un certificado digital firmado con la clave pública de la CA. A para obtener su certificado digital solicitó los servicios de una Autoridad Certificadora que realizó las investigaciones necesarias y físicamente entregó un archivo con el certificado digital firmado con su clave privada. Este certificado A lo presenta a B, B verifica el valor *hash* que se envía en el certificado, calculándolo nuevamente utilizando la clave pública de la CA que es bien conocida, así B verifica si el certificado digital es auténtico. A continuación en la figura 2.8 se muestra un ejemplo de un Certificado Digital, en este caso la CA es IBM.

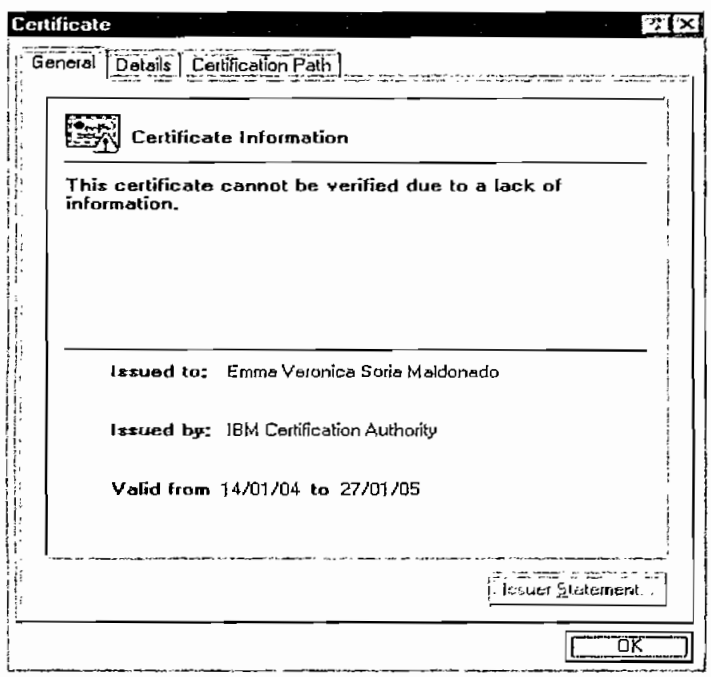


Fig. 2.8 Certificado Digital

Se podría pensar que se tiene el nuevo problema de conocer con seguridad la clave pública de la CA. Sin embargo la clave pública de las CA viene ya instalada en los *browsers* más conocidos como *Internet Explorer, Netscape*, etc., mediante convenios y sociedades de empresas de tecnología de software como Microsoft y Autoridades Certificadoras. Esta clave se incluye en los denominados certificados digitales raíces instalados ya en los *browsers*.

a) Estándar X.509

Ahora todo el mundo desea un certificado firmado por una autoridad certificadora bien conocida para poder establecer comunicaciones seguras, sin embargo, si los certificados tienen formatos diferentes, administrarlos y garantizar compatibilidad entre ellos sería muy complejo. Para ello la ITU desarrolló el estándar X.509 para certificados digitales que es ampliamente utilizado en Internet. Fue publicado originalmente en 1988 en su primera versión, actualmente se encuentra en vigencia la tercera versión que es la que se trata a continuación. El X.509 especifica la forma de describir los certificados digitales. Los campos principales que un certificado digital debe tener son los mostrados en la tabla 2.2.

Campo	Explicación
Versión	Versión del X.509
Número de Serie	Identificador único del certificado
Algoritmo de Firma	Algoritmo de firma del certificado
Emisor	El nombre de la Autoridad Certificadora
Validez	Fechas de inicio y fin del periodo por el cual el certificado es válido
Nombre del Sujeto	Nombre de la entidad a la cual pertenece el certificado
Clave Pública	La clave pública del sujeto y el ID del algoritmo utilizado para generarla
ID del Emisor	ID opcional que identifica de manera única al emisor del certificado
ID del Sujeto	ID opcional que identifica de manera única al sujeto del certificado
Extensiones	Varios
Firma	Firma del certificado con la clave privada de la Autoridad Certificadora

Tabla 2.2 Campos de un Certificado Digital

La información mostrada en el certificado es la esencial para que la otra parte conozca con quien está tratando.

Los certificados digitales se codifican con la ASN.1 (Notación de Sintaxis Abstracta 1), de la OSI, que especifica una notación y estructura específica.

A continuación en la figura 2.9 se muestra un certificado digital verdadero con sus principales campos.

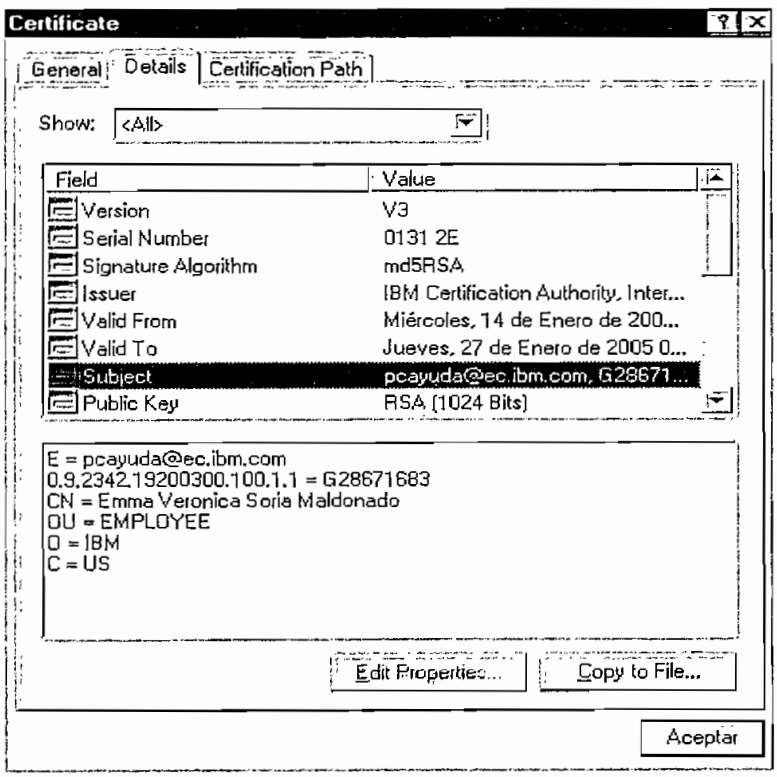


Fig. 2.9 Certificado Digital Verdadero

Para este certificado se puede apreciar que la información de los campos es la descrita en la tabla 2.3.

b) Limitaciones de un certificado digital

Hay algunos aspectos a considerar con el uso de certificados digitales. Por ejemplo los certificados digitales no son asignados de por vida a una entidad, tienen un tiempo de expiración.

El problema viene entonces con respecto a la no validez de los certificados expirados. Otro problema que se tiene es la revocación de certificados, supongamos que una compañía recibió su certificado de una CA sin mayor problema, pero qué ocurre si esa compañía quiebra y se liquida, se debe manejar la revocación del certificado, pues esa compañía ya no es una entidad confiable y que por tanto deba tener un certificado digital. Pero un certificado emitido tiene validez hasta que expire, por lo cual no existe un proceso inmediato para revocar o retirar esta certificación.

Campo	Explicación
Versión	Versión 3
Número de Serie	01 31 2E
Algoritmo de Firma	MD5 y RSA
Emisor	IBM *Certification Authority*
Validez	2004 – 01 – 14 hasta el 2005 – 01 – 27
Nombre del Sujeto	pcayuda@ec.ibm.com
Clave Pública (1024 bits)	3081 8902 8181 0090 321D 6FE0 7460 7F65 B221 F6F6 49E4 D068 57AA 0C95 BFE3 ECF6 2063 C7DD 5BFE 8162 E244 2A89 6B7B 20FC 0A0F 04ED 2D3F 918E 2E29 E404 D8CA D967 AF1F 2F0C 58BF 11E2 11F4 62C3 A374 C06F 2931 D9FA 7520 3F76 86EC E756 0948 8A3F 8D40 169D 292A 2CD8 0DE7 F7F8 AD24 F93A CCE6 7B6F 12DF 2E91 77DC 3F41 C01C 487E 1849 E0F8 4534 F302 0301 0001
ID del Emisor	ID opcional que identifica de manera única al emisor del certificado
ID del Sujeto	ID opcional que identifica de manera única al sujeto del certificado
Extensiones	Varios
Firma	Firma del certificado con la clave privada de la Autoridad Certificadora

Tabla 2.3 Campos de un Certificado Digital

Para solucionar este problema las CA emiten periódicamente listas de revocación de certificados CRL, los participantes utilizan la infraestructura de clave pública para mantener actualizadas sus CRL´s.

c) Autoridades certificadoras

Las Autoridades Certificadoras (CA) son entidades públicas o privadas que llenan la necesidad de tener una tercera parte que sea confiable para realizar el

comercio electrónico. La CA emite certificados digitales a toda entidad que lo requiera, para lo cual realiza una investigación minuciosa de la entidad para averiguar sus datos reales, una vez verificados la información, emite un certificado digital firmado con su clave privada.

Un certificado digital no es útil si la CA que lo emite no es una institución bien conocida y confiable, además si la otra parte no conoce con certeza la clave pública de la CA, no aceptará el certificado como válido.

La CA más importante en el mundo es *VeriSign* Inc, formada por *RSA Data Security.*, otras CA´s importantes son GTE, Baltimore y Microsoft. Todas estas CA´s mencionadas tiene su certificado raíz instalado en el Internet Explorer de Microsoft.

Se puede visualizar las CA´s de las que se conoce su clave pública en el Internet Explorer seleccionando *Tools* > *Internet Options* > *Content* > *Certificates* y luego seleccionando la pestaña de *Trusted Root Certifications Authorities*. Con lo que se visualizará la pantalla de la figura 2.10.

d) Infraestructura de clave pública

Si solamente existieran pocas CA que emitan certificados se tendría un claro problema de sobrecarga y puntos centrales de fallas. Una posible solución sería tener varias CA´s bajo una sola organización que compartan la clave privada.

Sin embargo, esto presenta un problema, debido a que las diferentes CA´s deben tener la clave privada, existirían varios servidores en el mundo con la clave privada por lo cual se tiene mayor probabilidad de que sea robada afectando así a toda la infraestructura.

Además se tendría discrepancias sobre quien debe actuar como CA, en algunos países se insistiría en que fuera el gobierno, pero en otros casos éste sería rechazado.

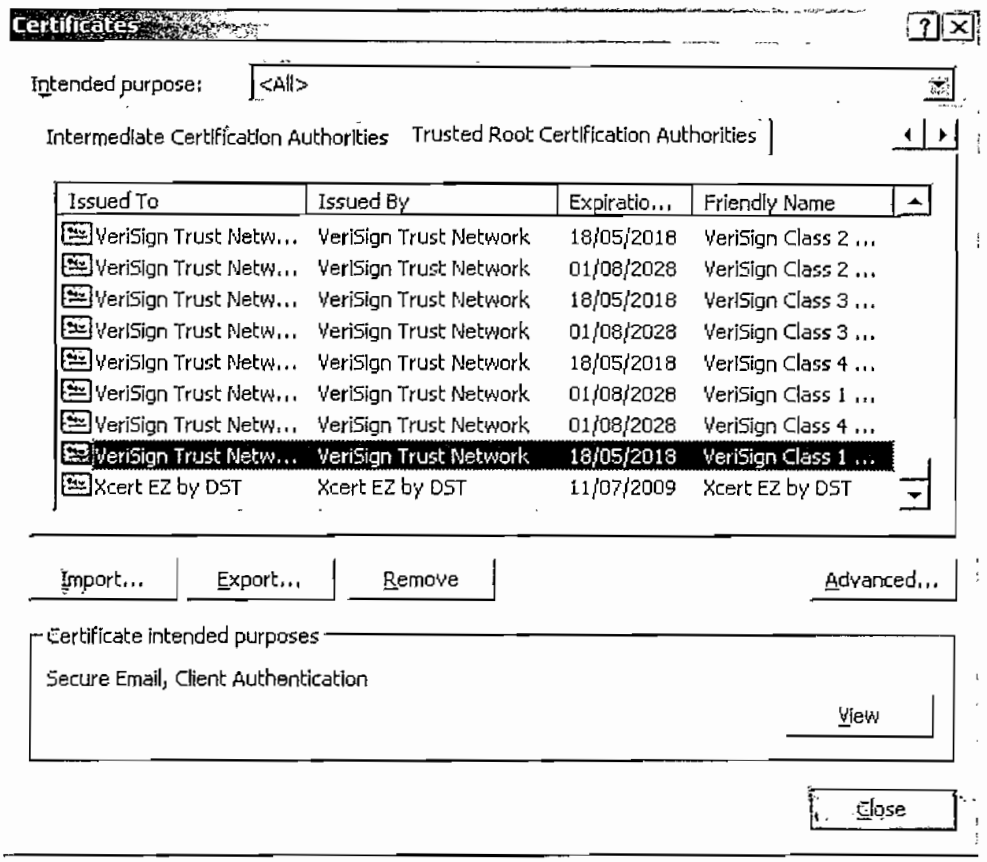


Fig. 2.10 Autoridades Certificadoras

Por estos problemas se ha desarrollado una forma diferente de establecer la certificación. Se conoce como PKI (*Public Key Infrastructure).* La PKI provee una estructura jerárquica de CA´s y define los estándares para los diferentes documentos y protocolos.

La PKI específica una jerarquía de CA´s. Se tiene una CA raíz que certifica a CA regionales llamadas Autoridades Regionales RA, que a su vez certifican a las CA´s verdaderas que emite los certificados digitales a las entidades. Cuando una raíz autoriza a una RA emiten un certificado aprobando la RA, incluyendo la clave pública de la RA. Igualmente una RA que autoriza una CA emite un certificado firmado con su clave privada a la CA en el que se incluye la clave pública de la CA.

Gracias a esto una entidad que requiera un certificado recurre a la CA más cercana autorizada por una RA, que a su vez está autorizada por una autoridad raíz. Esto hace que sea fácil y económico obtener un certificado digital para comunicaciones seguras. En la figura 2.11 se muestra un ejemplo de una PKI real.

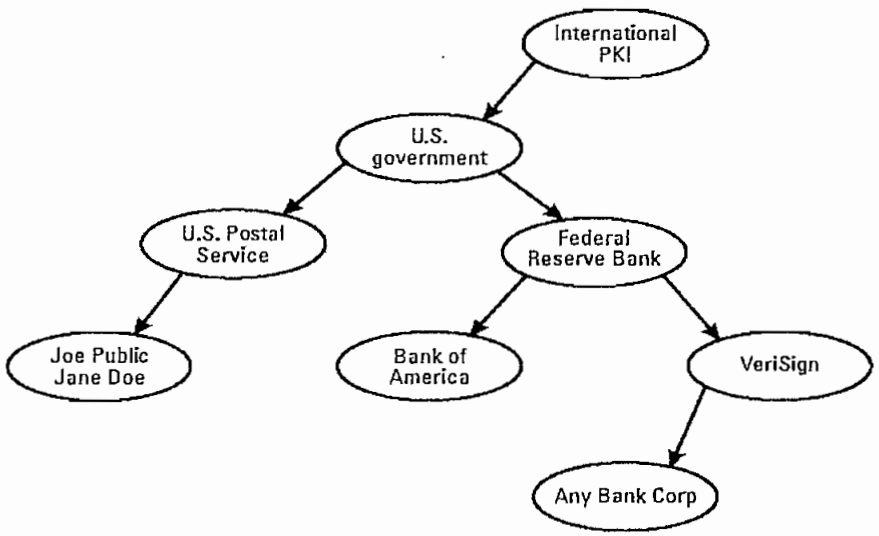


Fig. 2.11 PKI real [9]

2.3. ASPECTOS GENERALES DE LA SEGURIDAD EN REDES INALÁMBRICAS

Debido a las grandes ventajas de las redes inalámbricas, muchas empresas las han implementado como complemento de su infraestructura cableada instalada. Pero si no se tiene desarrollados los mecanismos de protección de la misma se deja un agujero de seguridad por donde se puede poner en riesgo la integridad de toda la red. La diferencia principal de las redes inalámbricas con las cableadas radica en el medio de transmisión que utilizan, esto implica que el concepto de cobertura de la red cambia ya que depende del alcance de la señal de radio, la misma que puede fácilmente salir del edificio y ser interceptada por un atacante con la utilización de un equipo no muy sofisticado *(PDA* con tarjeta inalámbrica y tiempo libre). Todo esto concluye en la necesidad de enfrentar uno de los mayores retos de las redes inalámbricas, la seguridad. Ya se ha visto los

principales aspectos de seguridad que debe cumplir un sistema, pero en el caso de redes inalámbricas se deben resaltar algunos aspectos importantes.

2.3.1. OBJETIVOS DE LA SEGURIDAD EN REDES INALÁMBRICAS

El objetivo de los mecanismos de seguridad en redes inalámbricas es proveer la misma confianza que se tendría en la red cableada. Para esto se debe entregar los tres servicios fundamentales de la seguridad en redes: Autenticación, Confidencialidad e Integridad (la disponibilidad depende más de la política de seguridad de la empresa).

2.3.1.1. Autenticación en Redes Inalámbricas

La autenticación debe ser de doble sentido, se debe poder verificar la identidad del usuario que se asocia a la red y la identidad de la red a la cual se asocia el usuario. Un atacante puede tratar de ingresar a la red mediante un dispositivo inalámbrico ubicándose cerca del edificio, o podría ubicar un AP ilegal de mayor potencia para que los usuarios se asocien a éste y le transmitan sus datos.

2.3.1.2. Confidencialidad en Redes Inalámbricas

Debido a que la señal de radio puede ser fácilmente capturada (inevitablemente por la naturaleza inalámbrica), se debe proveer mecanismos de privacidad para los datos que viajan en la señal. Esto se logra con mecanismos de encripción robustos.

2.3.1.3. Integridad en Redes Inalámbricas

En un ambiente inalámbrico los datos pueden ser interceptados y luego el atacante los podría modificar y enviar nuevamente a la red. Este tipo de ataque se

En la figura 2.29a se muestra un ejemplo de este tipo de autenticación, la clave compartida en este caso es 123.

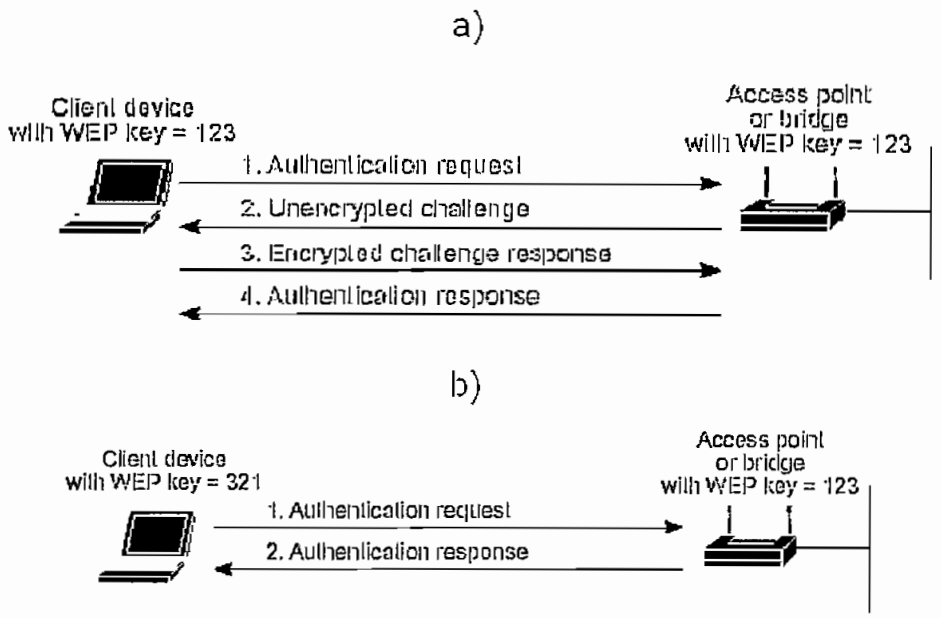


Fig. 2.29 a) Autenticación tipo Shared
b) Autenticación tipo Open [14]

Este tipo de autenticación presenta un problema. Si un atacante captura el texto plano del *challenge* y el texto encriptado con la clave secreta en respuesta, entonces puede descifrar la clave secreta mediante mecanismos inversos de encripción, logrando así la romper la seguridad de la WLAN.

c) Open System Authentication

En este tipo de autenticación se acredita a cualquiera que desea asociarse a la WLAN. Sin embargo no se le permite a la estación transmitir a menos que conozca la clave WEP compartida.

Este procedimiento se puede observar en la figura 2.29b. En este caso la clave WEP de la estación no corresponde a la del AP.

En la figura 2.30 se muestra el formato de una trama de autenticación. Este formato es utilizado para todos los mensajes de autenticación.

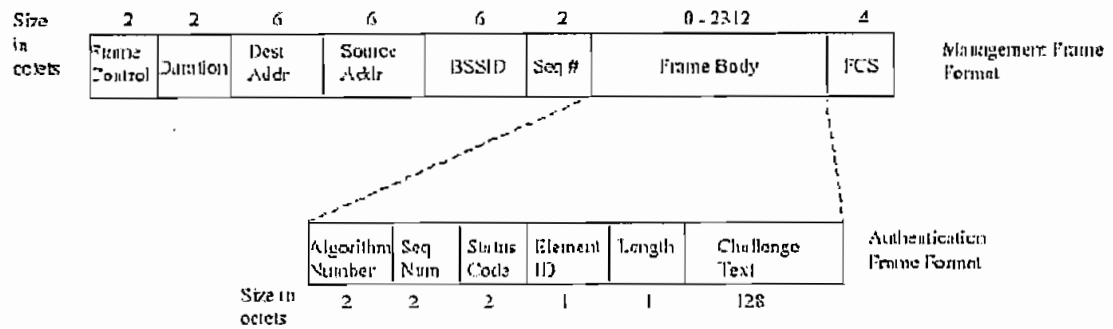


Fig. 2.30 Trama de Autenticación WEP [13]

Si el campo "*Status Code*" tiene valor '0' indica que la autenticación ha sido realizada con éxito, si no contiene un código de error.

- El campo "*Element identifier*" indica que la trama contiene el texto del *challenge*.

- El campo "*Length*" indica la longitud del texto de desafío y está fijado a máximo 128 bits.

- El campo "*Challenge text*" incluye el texto de desafío (challenge) aleatorio.

La tabla 2.4 muestra los posibles valores de los campos y cuándo está presente el texto del *challenge*, según el número de secuencia (Seq #) del mensaje.

Sequence Number	Status Code	Challenge Text	Se usa WEP
1	Reservado	No presente	No
2	Status	Presente	No
3	Reservado	Presente	Si
4	Status	No presente	No

Tabla 2.4 Valores de los campos de la trama de Autenticación [13]

2.4.1.5. Vulnerabilidades de WEP

a) Características lineales de CRC32

Esta vulnerabilidad fue demostrada teóricamente por Nikita Borisov, Lan Goldberg y David Wagner (Universidad de *Berkeley*).

Como se ha visto anteriormente, el campo ICV (*Integrity Check Value*) de una trama encriptada con WEP contiene un valor utilizado para verificar la integridad del mensaje.

Esto provee de un mecanismo de autenticación de mensajes a WEP, por lo tanto el receptor aceptará el mensaje si el ICV es válido. El ICV se genera simplemente haciendo un CRC (*Cyclic Redundancy Check*) de 32 bits, del *payload* de la trama. Este mecanismo tiene dos graves problemas:

- Los CRCs son independientes de la llave utilizada y del IV.
- Los CRCs son lineales: CRC (m (+) k) = CRC (m) (+) CRC(k).

Debido a que los CRCs son lineales, se puede generar un ICV válido ya que el CRC se combina con una operación XOR que también es lineal y esto permite hacer el *'bit flipping'* como se verá a continuación:

Un atacante debe interceptar un mensaje m (conocido o no) y modificarlo de forma conocida para producir m':

$m' = m (+) \Delta$

Como el CRC-32 es lineal, puede generar un nuevo ICV' a partir del ICV de m:

$IC' = IC (+) h (\Delta)$

ICV' será válido para el nuevo *cyphertext* c'

$c' = c (+) \Delta = k (+) (m (+) \Delta) = k (+) m'$

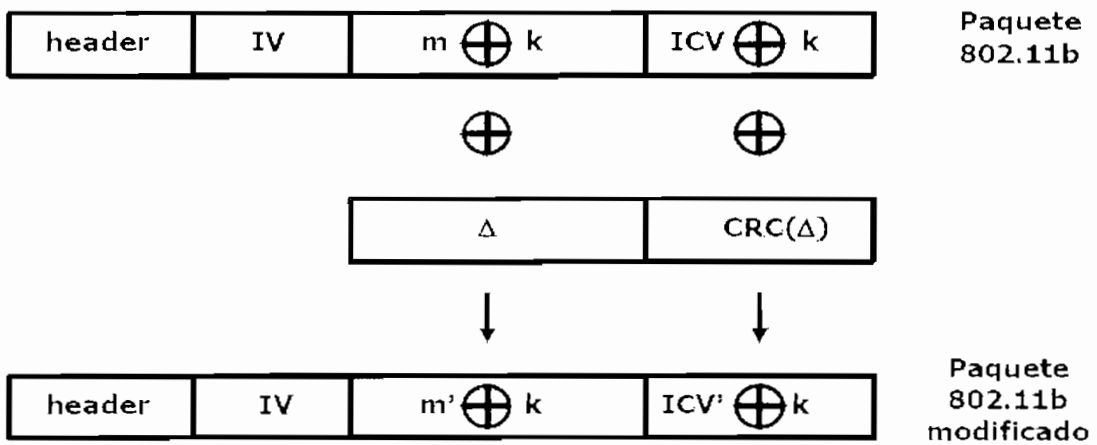


Fig. 2.31 Vulnerabilidad WEP

b) MIC Independiente de la llave

Esta vulnerabilidad fue demostrada teóricamente por David Wagner (Universidad de *Berkeley*). También conocida como "*Lack of keyed MIC*". El MIC[1] que utiliza WEP es un simple CRC-32 calculado a partir del *payload*, por lo tanto no depende de la llave ni del IV. Esta debilidad en la encriptación da lugar a que conocido el texto plano de un solo paquete encriptado con WEP sea posible inyectar paquetes a la red. Esto es posible de la siguiente manera:

El atacante captura un paquete c = m (+) k donde m es conocido (por ejemplo, el atacante envía un e-mail a la víctima)

El atacante recupera el flujo pseudo-aleatorio k = c (+) m para el IV concreto del paquete. El atacante inyecta un mensaje m' así:

ICV' = CRC32 (m')

El atacante ya puede ensamblar la parte encriptada del paquete:

[1] Mensaje de chequeo de integridad

c = (m'|ICV') (+) k

El atacante obtiene un paquete válido y listo para ser inyectado a la red:

Fig. 2.31 Vulnerabilidad WEP [10]

c) Tamaño de IV demasiado corto

Otra de las deficiencias del protocolo viene dada por la corta longitud del campo IV en las tramas 802.11b. El vector de inicialización (IV) tiene sólo 24 bits de longitud y aparece en claro (sin encriptar).

Matemáticamente sólo hay 2^{24} (16.777.216) posibles valores de IV. Aunque esto pueda parecer mucho, 16 millones de paquetes pueden generarse en pocas horas en una red inalámbrica con tráfico intenso:

Un punto de acceso que constantemente envíe paquetes de 1500 bytes (MTU) a 11 Mbps, acabará con todo el espacio de IV disponible después de $1500*8/(11*10^6)*2^{24}$ = ~1800 segundos, o 5 horas. Este tiempo puede ser incluso más pequeño si la MTU es menor que 1500 bytes.

La corta longitud del IV, hace que éste se repita frecuentemente y de lugar a la deficiencia del protocolo que se verá a continuación, basada en la posibilidad de realizar ataques estadísticos para recuperar el texto plano gracias a la reutilización del IV.

d) Reutilización de IV

Esta vulnerabilidad fue demostrada teóricamente por David Wagner (Universidad de *Berkeley*). Se basa en que WEP no utiliza el algoritmo RC4 "con cuidado": el

Vector de Inicialización se repite frecuentemente. Se pueden hacer ataques estadísticos contra *cyphertexts* con el mismo IV.

Si un IV se repite, se pone en riesgo la confidencialidad. Supóngase que P y P' son dos textos planos encriptados con el mismo IV. Supóngase que Z = RC4(*key*, IV); entonces los dos *ciphertexts* son:

C = P (+) Z y C' = P'(+) Z

Nótese que C (+) C' = (P (+) Z) (+) (P' (+) Z) = (Z (+) Z) (+) (P (+) P') = P (+) P' por lo que la XOR de ambos textos planos es conocida. Si hay redundancia, se pueden descubrir ambos textos planos. Si se puede adivinar un texto plano, el otro puede también ser descubierto estadísticamente de forma trivial, así que si RC4 no se usa con cuidado, se vuelve inseguro.

2.4.1.6. El definitivo rompimiento de WEP

En Agosto del 2001 Scott Fluhrer, Itsik Mantin y Adi Shamir publicaron un documento titulado debilidades en el algoritmo de programación de clave de RC4. Al final del documento los autores describen un ataque teórico a WEP. El ataque se basa en una debilidad encontrada en la manera que RC4 genera el *Keystream*.

Todo lo que se asume es la habilidad de recobrar el primer byte de los datos encriptados. Desafortunadamente 802.11 utiliza encapsulación LLC, por lo que el valor en texto plano de este primer byte es siempre 0xAA. Como se conoce este primer byte el *Keystream* puede ser deducido por una operación trivial XOR con el primer byte encriptado.

El ataque que describe el documento se centra en la forma en que las claves son escritas: (B+3):ff:N. Cada IV es utilizado para atacar un byte particular de la porción secreta de la clave RC4. Los bytes de la clave son numerados desde cero, por lo cual la debilidad del IV corresponde al byte cero de la clave secreta

que toma la forma 3:ff:N. El segundo byte debe ser 0xff; conocer el tercer byte de la clave es requerido, pero éste no necesita ser ningún valor específico.

Una clave WEP estándar es de cinco bytes numerados consecutivamente de cero a cuatro. El IV tiene el primer byte en el rango de tres a siete y el segundo byte de 255. Existen 5x1x256, es decir, 1280 posibles IVs débiles en una red WEP estándar. Es necesario notar que el número de claves débiles depende de la longitud de la clave RC4 utilizada, por lo cual a mayor longitud de clave, más IVs débiles existirán.

Aplicando la teoría de probabilidad los autores predijeron que cerca de 60 casos resueltos son necesarios para determinar un byte de la clave.

Poco después de la publicación de este trabajo Adam Stubblefield, Johon Loannidis y Avi Rubin aplicaron este ataque experimental en una red real, con efectos devastadores. En 60 casos resueltos usualmente determinaban un byte de la clave, y en 256 casos resueltos siempre encontraban la clave completa.

Esto implica que con 5 o 6 millones de paquetes encriptados con WEP capturados se puede descifrar la clave.

En el mismo mes en que se realizó esta prueba Jeremy Bruestle y Blake Hegerle lanzaron *AirSnort,* un programa de código abierto que puede recuperar la clave WEP. Con esto se facilitó que personas con conocimiento medio de seguridad en redes pudieran comprometer la seguridad de una WLAN. Es por esto que WEP por sí solo, es aplicable únicamente para pequeñas empresas y hogares.

2.4.1.7. Ventajas de WEP

- WEP es fácil de instalar.
- No requiere de una inversión adicional
- No necesita servidores de autenticación, certificados digitales y bases de datos de usuarios.

- Compatible con todas las plataformas de clientes.
- Compatible con casi todo el hardware de redes inalámbricas.

2.4.1.8. Desventajas de WEP

- Utiliza la misma clave para encripción y autenticación. Si se compromete la una se compromete también la otra.
- Mecanismo de autenticación, encripción e integridad con varias debilidades.
- No constituye una solución adecuada para WLAN´s corporativas.
- No protege de intrusión de usuarios internos, pues la clave es compartida por todos los usuarios de la WLAN.

2.4.2. WPA

WEP es un sistema muy débil ya que se puede conseguir la clave de cifrado monitorizando las tramas y procesándolas. Además la integridad se consigue utilizando simples técnicas de detección de errores (CRC) que no son eficientes para garantizar la integridad. Otro problema es que se tiene un punto simple de vulnerabilidad, ya que si la clave es robada se pone en riesgo la autenticación y la confidencialidad.

La *Wi-Fi Alliance*, como organización responsable de garantizar la interoperabilidad entre productos para redes inalámbricas de fabricantes diversos, ha definido una especificación de mercado basado en las directrices marcadas por el grupo de trabajo 802.11i denominada *Wi-Fi Protected Access* (WPA), junto con la correspondiente certificación de productos.

WPA aparece a finales del 2002 y es básicamente el pre-estándar de 802.11i que se espera este listo para finales del 2004. WPA está destinado a garantizar la seguridad en las especificaciones IEEE 802.11b, 802.11a y 802.11g.

En la tabla se muestra una comparación entre el WEP de 802.11 y WPA.

Comparación de características de seguridad proporcionadas por IEEE 802.11 y WPA				
Características			802.11	WPA
Cifrado	Sistema (Algoritmo) de Cifrado		WEP (RC4)	TKIP (RC4)
		Longitud	40 bits	128 bits
	Gestión claves	Generación clave	Estática, la misma para todos los dispositivos	Dinamica: por usuario, por sesion, por paquete
		Distribución clave	Manual, en cada dispositivo	Automatica, gestionada por 802.1x/EAP
Autenticacion		Entorno	Definido por 802.11	802.1x/EAP
		Metodo	Abierta/Clave compartida (autentifica el equipo)	EAP-TLS, PEAP, EAP-TTLS (autentifican al usuario)

Tabla 2.5 Campos de un Certificado Digital[1]

Lo que WPA ofrece es mejorar WEP considerablemente utilizando toda la tecnología desarrollada hasta el momento, para lo cual se vale de la definición de nuevas herramientas como el TKIP (*Temporal Key Integrity Protocol*), el MIC *(Message Integrity Check)* y estándares completos como el 802.1x y EAP.

El esquema de 802.1x y EAP será explicado en la siguiente sección en más detalle, por lo que se empezará la descripción del funcionamiento de TKIP.

2.4.2.1. PRIVACIDAD E INTEGRIDAD CON TKIP

Temporal Key Integrity Protocol (TKIP) amplía y mejora a WEP, solucionando sus vulnerabilidades. TKIP amplía la longitud de la clave de 40 a 128 bits y pasa de ser única y estática a ser generada de forma dinámica, para cada usuario, para cada sesión (teniendo una duración limitada) y por cada paquete enviado.
TKIP ofrece las siguientes 4 mejoras:

- Un código de integridad de mensaje criptográfico (MIC) y no un simple CRC.

[1] http://www.edubis.com

- Una nueva disciplina de secuencia del IV, para remover los ataques de retransmisión a WEP.
- Función de combinación de claves por paquete para eliminar la correlación de los IV.
- Mecanismo de generación de nuevas claves para que no existan ataques por su reutilización.

2.4.2.2. MIC

El *Message Integrity Check* o MIC sirve para garantizar la integridad del mensaje emitido. Debido a que un simple CRC no es suficiente ya que puede ser recalculado con facilidad, el MIC emplea un mensaje criptográfico que se añade a la información transmitida.

Este mensaje se conoce como *Message Authentication Codes* o *MAC´s*. El Algoritmo de integridad utilizado específicamente por TKIP es el algoritmo de *Michael* [1] que genera un bloque de 4 bytes a partir de la dirección MAC origen, MAC destino y los datos.

2.4.2.3. Reforzamiento del IV

Un problema del MIC es que no detecta si los paquetes han sido retransmitidos. Esto ocurre cuando un atacante almacena un paquete válido que estaba en vuelo y luego lo retransmite.

El estándar resuelve este problema asociando un número de secuencia de paquete con el MIC encriptado, y reiniciando la misma una vez que el MIC encriptado es reemplazado. Esta estrategia requiere que el transmisor se abstenga de enviar datos protegidos con MIC´s anteriores una vez que este finaliza el espacio de la secuencia. El transmisor tiene entonces 3 opciones:

---

[1] Algoritmo de integridad de mensajes propio de TKIP, diseñado para consumir pocos recursos computacionales

- Detener todas las comunicaciones en conjunto.
- Tratar de asegurar el MIC con una clave fresca.
- Enviar el tráfico siguiente sin protección.

El no adoptar una de estas 3 estrategias, pone en riesgo el tráfico ya protegido con la clave WEP. TKIP ya no sigue el diseño clásico. Para defenderse de las retransmisiones, TKIP reutiliza el campo IV como un número de secuencia de paquete.

Ambos, el transmisor y el receptor inicializan el espacio de secuencia a cero cuando una nueva clave TKIP es utilizada, y el transmisor incrementa el número de secuencia con cada paquete que envía. TKIP requiere que el receptor cumpla con la secuencia de IV apropiada en el arribo de paquetes. TKIP define un paquete como *out-of-sequence* si su IV es el mismo o menor que el paquete previo correctamente recibido. Si un paquete se recibe fuera de orden, entonces es descartado.

2.4.2.4. Combinación de claves

La característica de TKIP para generar una clave por paquete es necesaria para eliminar las vulnerabilidades del uso de RC4 en WEP.

En WEP, se construye una clave RC4 por paquete concatenando la clave base y el IV. La nueva construcción de la clave por paquete en TKIP se llama *Key Mixing Function* o función de combinación de claves. Funciona generando claves temporales con un periodo fijo de duración que son reemplazadas frecuentemente. Esta función fue desarrollada por *Doug Whiting* y *Ron Rivest.* Este proceso se divide en 2 fases.

En la fase 1 se combina la dirección MAC del transmisor y la clave WEP mediante iteraciones XOR para producir una clave intermedia. Como la dirección MAC es

única para cada dispositivo se garantiza que siempre se genere diferentes claves intermedias para cada dispositivo.

La fase 2 utiliza un pequeño cifrado con el Algoritmo de *Feistel*[1] para encriptar el número de secuencia de paquete con la clave intermedia, produciendo una clave por paquete de 128 bits.

2.4.2.5. Re-Keying

Este mecanismo consiste en generar continuamente claves nuevas para evitar que sean reutilizadas. Este mecanismo maneja tres tipos de claves: claves temporales (2), claves de encripción (2) y clave maestra.

La clave maestra se establece por el servidor de autenticación 802.1x o de forma manual. Se utiliza para encriptar la comunicación durante la generación del resto de claves. Las claves de encripción son mensajes seguros que se intercambian con la clave maestra para generar las claves temporales. En función de las claves de encripción se derivan 2 claves temporales, una de 128 bits para encripción, y otra de 64 bits para integridad.

2.4.3. 802.1x y EAP

Debido a las debilidades de WEP, los fabricantes empezaron a trabajar intensamente en el desarrollo de mecanismos de seguridad más robustos, para ofrecer mejores soluciones al mercado de las WLAN´s. El IEEE dirigió estos esfuerzos mediante las especificaciones del 802.1x, que se basó principalmente en el protocolo EAP. [13]

Con esta base, las diferentes industrias de tecnología empezaron la carrera por

---

[1] Algoritmo con estructura de transformación (L,R) -> (L,R, ⊕ f(R)), la función f se implementa con simples iteraciones XOR.

crear soluciones principalmente empresariales para la seguridad en WLAN´s. Empresas como Microsoft, CISCO y *Funk Software*, desarrollaron mecanismos propios con características particulares de seguridad y costos.

Por todo esto, el entendimiento de la arquitectura de seguridad del 802.1x, los protocolos que utiliza y las implicaciones de los diferentes tipos de EAP implementados, son de vital importancia para elegir una solución de seguridad para una WLAN.

2.4.3.1. EAP Extensible Authentication Protocol

La base fundamental del estándar 802.1x es EAP. EAP fue desarrollado por el IETF y está especificado en el RFC 2284. EAP inicialmente se utilizó en ambientes WAN con PPP (*Point to Point Protocol*) permitiendo varios tipos de autenticación de acuerdo a las necesidades.

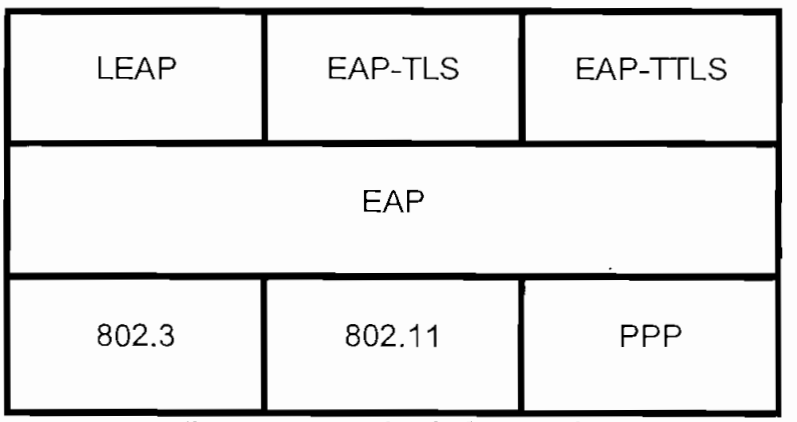


Fig. 2.32 EAP en la pila de protocolos

Gracias a que EAP es una simple encapsulación, que define el formato de las tramas para el intercambio de credenciales de las partes, puede utilizarse sobre cualquier tipo de capa enlace, y no solo con PPP. Esta característica es clave para que EAP haya sido elegido como base del estándar 802.1x. En la figura 2.32 se muestra la ubicación de EAP dentro de la pila de protocolos. Como se puede apreciar EAP se puede utilizar en cualquier red 802.3, en redes WLAN´s y en redes PPP.

Además permite gran flexibilidad en el método de autenticación que se puede utilizar.

a) Formato del paquete EAP

La figura 2.33 muestra el formato de paquete EAP. En el caso de PPP, los paquetes son transportados en tramas PPP, sin embargo, esto no es una restricción, ya que los paquetes EAP pueden ser transportados por cualquier tipo de tramas, por ejemplo en tramas 802.11.

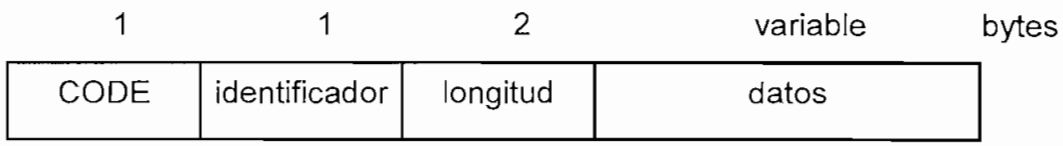


Fig. 2.33 Paquete EAP [13]

- *Code*.- Es el primer campo del paquete, es de 1 byte de longitud y define el tipo de paquete EAP para poder interpretar el campo de datos.

- Identificador.- Es de 1 byte de longitud, este contiene un entero sin signo utilizado para corresponder las peticiones con las respuestas. En la retransmisión de un paquete EAP, se utiliza el mismo identificador. En nuevas transmisiones se utiliza un nuevo identificador.

- Longitud.- Este campo tiene una longitud de 2 bytes. Contiene el número de bytes existentes en el paquete EAP, incluyendo los campos de *code*, identificador, longitud y datos. En algunos protocolos de capa de enlace es necesario un *padding* para completar la longitud requerida. EAP asume que todos los datos en exceso del campo longitud son *padding* de la capa de enlace y por tanto los descarta.

- Datos.- El último campo del paquete EAP es de longitud variable. Dependiendo del tipo de paquete, el campo de datos puede ser también de longitud cero. La interpretación de los datos depende del valor del campo *code*.

b) Peticiones y Respuestas EAP

El intercambio de EAP está compuesto por peticiones y respuestas. El autenticador envía peticiones a los sistemas que buscan acceso, y basado en las respuestas, el acceso puede ser otorgado o denegado.

El formato de estos paquetes se muestra en la figura 2.34.

1	1	2	1	variable bytes
CODE	identificador	longitud	Tipo	Tipo-Datos

1 *Request*

2 *Response*

Fig. 2.34 Paquete EAP Response y Request [13]

El campo *Code* es puesto en 1 para peticiones y en 2 para respuestas. Los campos Identificador y Longitud se utilizan de forma normal a la descrita anteriormente. El campo datos lleva la información utilizada en las peticiones y respuestas. Cada campo de datos lleva un tipo de datos específico, dividido en un código de identificador de tipo y en los datos asociados.

Tipo.- Este campo es de 1 byte de longitud e indica el tipo de petición y respuesta. Solamente un tipo puede ser utilizado en cada paquete. Con una excepción, el tipo de respuesta, siempre debe coincidir con el tipo de petición.

Esa excepción ocurre cuando la petición no es aceptada, y la contraparte envía un NAK para sugerir un tipo alternativo. Tipos mayores o iguales a 4 indican el método de autenticación.

Tipo-Datos.- Es un campo variable que debe ser interpretado de acuerdo a las reglas de cada tipo.

Código Tipo 1.- Identidad

El autenticador generalmente usa el tipo identificador para una petición inicial. Siempre el primer paso para la autenticación es identificarse.

Naturalmente la mayoría de implementaciones de EAP tiene el nombre del usuario para determinar la identidad del mismo. El campo de tipo de datos puede contener texto utilizado para colocar el usuario; la longitud de la cadena es calculada en base al campo longitud del mismo paquete EAP.

Algunas implementaciones de EAP pueden tratar de ocultar la identidad del usuario en la petición, incluso antes de enviar el *challenge* de autenticación. Si el usuario no existe, la autenticación se rechaza y no se realiza ningún procesamiento.

Código Tipo 2.- Notificación

El autenticador puede utilizar el tipo Notificación para enviar un mensaje al usuario. Así el sistema del usuario puede desplegar este mensaje. Los mensajes de notificación son utilizados para proveer mensajes al usuario del sistema de autenticación, como por ejemplo un *password* a punto de expirar.

Las respuestas deben ser enviadas como consecuencia de notificaciones de petición. En todo caso, éstos sirven como simple confirmación, y el campo de tipo de datos tiene longitud cero.

Código Tipo 3.- NAK

Son utilizados por el autenticador para sugerir a los usuarios un nuevo método de autenticación, el autenticador envía un *challenge* codificado por el código tipo. Si el usuario final no soporta el tipo de autenticación del *challenge*, éste puede utilizar un NAK. El campo de tipo de Datos del mensaje NAK incluye un byte que corresponde al tipo de autenticación sugerido.

Los tipos de autenticación utilizados dependen de cada fabricante o infraestructura, los más importantes son MD5, OTP, *Token Card*, LEAP, TLS y TTLS. Sus códigos tipos correspondientes se muestran en la tabla 2.5.

Código Tipo Número	Descripción
Código Tipo 4	*MD5 Challenge*
Código Tipo 5	*OTP One Time Password*
Código Tipo 6	*Generic Token Card*
Código Tipo 13	*EAP – TLS*
Código Tipo 17	*LEAP*
Código Tipo 21	*EAP - TTLS*

Tabla 2.5 Tipos de EAP y su código correspondiente [13]

Los mecanismos de MD5, OTP y *Token Card* son sencillos de implementar y muy populares en ambientes WAN. En cambio en ambientes WLAN los mecanismos más utilizados son LEAP, EAP–TTLS y EAP–TLS, por lo que serán tratados más adelante con mayor profundidad.

MD5 *Challenge.-* El mecanismo *Message Digest 5* es descrito en el RFC 1321. Es uno de los mecanismos más populares de autenticación, gracias a su fácil y rápida implementación. Con MD5 el cliente recibe un desafío (*challenge*) que debe ser codificado correctamente con una clave compartida, si esto ocurre el cliente es autenticado.

OTP *One Time Password.-* El OTP es un método de autenticación remoto de usuarios. En el esquema OTP el *password* nunca viaja por la red, evitando que sea capturado durante su transmisión. Además en cada conexión el usuario utiliza un *password* distinto (*password* que se usa una sola vez). Para conseguir esto OTP opera de la siguiente manera:

El servidor envía un requerimiento al cliente que consta de una semilla aleatoria y un número de secuencia de *password*. El cliente generador de OTP ingresa el valor aleatorio recibido y el *passphrase* en una función *hash* generando un

password. El *passphrase* corresponde a una cadena almacenada en un diccionario que se encuentra tanto en el servidor como en el cliente. Luego se envía esta información al servidor. Si un atacante intercepta el valor aleatorio, no es suficiente ya que no conoce el *passphrase*. Si intercepta un *password* de una sesión anterior es inútil pues el *password* solo sirve una vez.

Generic Token Card.- Es un tipo de autenticación OTP, con la diferencia que el *password* es generado por un hardware externo; este hardware es un tarjeta electrónica que tiene un algoritmo específico que se aplica al requerimiento del servidor que se le ingresa por teclado. Nunca devuelve el mismo resultado.

Ejemplos de estas tarjetas son *SecureID* de *Secure Dynamics* y *Cryptocard* de *Cryptocard Corp*. En la figura 2.35 se muestra una tarjeta *Cryptocard*.

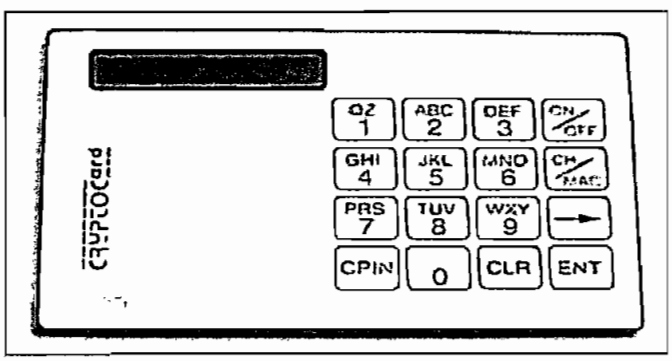


Fig. 2.35 Tarjeta Cryptocard

Con el uso de este hardware se evita que los diccionarios de *passphrase* estén almacenados en el cliente y el servidor, ya que la pérdida de confidencialidad de los mismos comprometería todo el sistema.

c) Éxito y Fracaso en autenticación EAP

Luego de que el intercambio de EAP termina, el usuario puede haber tenido éxito o fracaso en la autenticación. Una vez que el autenticador determina que el intercambio de credenciales está completo, éste envía una trama con un código de éxito (3) o de fracaso (4) al final del intercambio, como se indica en la figura

2.36. Muchas implementaciones permiten enviar varias peticiones antes de que la autenticación falle, esto para permitir al usuario aplicar las credenciales correctas.

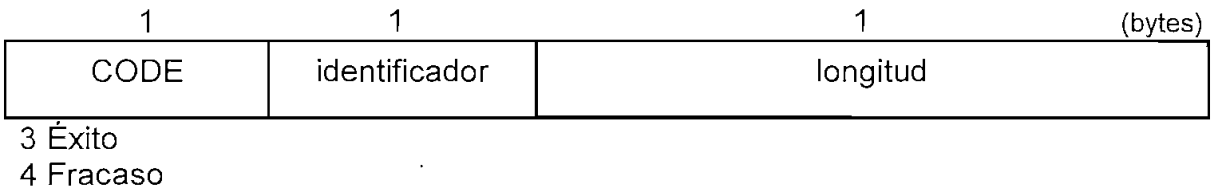


Fig. 2.36 Paquetes EAP Succes y Failure [13]

d) Ejemplo de intercambio de EAP

Un ejemplo de intercambio de credenciales EAP se muestra en la figura 2.37. Solamente se muestra el procedimiento de forma general pues las características particulares dependen de cada tipo de EAP. El intercambio de EAP es una serie de pasos empezando por una petición de identidad y terminando con un mensaje de éxito o fracaso de autenticación.

1. El autenticador envía un paquete de Petición / Identidad para identificar al usuario.

2. El sistema del usuario final toma la entrada, recolecta la identificación del usuario, y lo envía en un mensaje Respuesta / Identidad.

3. Con el usuario identificado, el autenticador envía el *challenge* de autenticación. En el ejemplo de la figura, en el paso 3, el autenticador envía un reto MD5 al usuario en un paquete Petición / MD5.

4. Pero el sistema del usuario final está configurado para utilizar *token card* como mecanismo de autenticación, así que éste responde con un paquete Response / NAK, sugiriendo el uso de *Generic Token Card* al autenticador.

5. El autenticador entonces envía un *challenge* en un paquete Petición / *Generic Token Card,* junto con la secuencia numérica de la tarjeta.

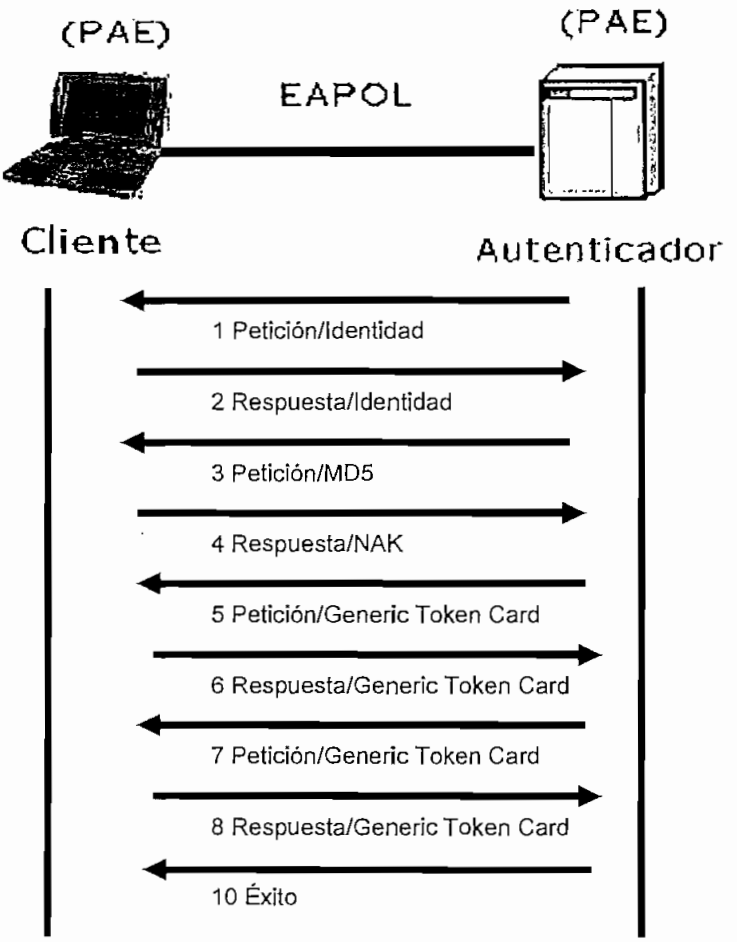


Fig. 2.37 Intercambio EAP [13]

6. El usuario escribe la respuesta, que luego es enviada en un paquete Respuesta / *Generic Token Card.*

7. La respuesta del usuario no es correcta, así que la autenticación no es posible. Sin embargo la implementación del autenticador EAP permite que el usuario realice varias peticiones, así que un segundo paquete Petición / *Generic Token Card* es enviado.

8. Una vez más el usuario escribe la respuesta, la misma que es enviada en un paquete Respuesta / *Generic Token Card.*

9. En un segundo intento, la respuesta es correcta, así que el autenticador envía un mensaje de Éxito.

2.4.3.2. IEEE 802.1x Autenticación basada en puerto

Estándar del IEEE publicado en el 2002. El nombre completo del estándar *es Port Based Network Access Control,* Control de acceso a red basado en puerto. Se basa en asignar puertos autorizados, mediante un autenticador y un servidor AAA, a los usuarios.

En el esquema WLAN los puertos son conexiones lógicas entre el AP y el cliente. A continuación se explica el funcionamiento de la infraestructura 802.1x y sus herramientas de implementación.

a) Arquitectura y Nomenclatura del IEEE 802.1x

El estándar define 3 componentes principales para el proceso de autenticación. El cliente (*suplicant*), el autenticador y el servidor de autenticación. El cliente es el usuario final que busca acceso a la red.

El autenticador controla el acceso a la red. Estas dos entidades se conocen como Entidades de Autenticación por puerto (PAE´s).

El autenticador solamente termina el intercambio de credenciales en la capa de enlace, éste no conoce ninguna información sobre el usuario, ni realiza ninguna validación sobre las credenciales.

Todas las peticiones son pasadas al servidor de autenticación, un servidor AAA (*Authentication, Authorization and Accounting*) cualquiera, el estándar no especifica alguno, sin embargo el más utilizado es el servidor RADIUS (*Remote Authentication Dial In User Service)* para el caso de WLAN´s.

Este servidor se encarga de la validación de las credenciales del usuario en base a información almacenada en bases de datos locales o remotas. La arquitectura y nomenclatura 802.1x se muestra en la figura 2.38.

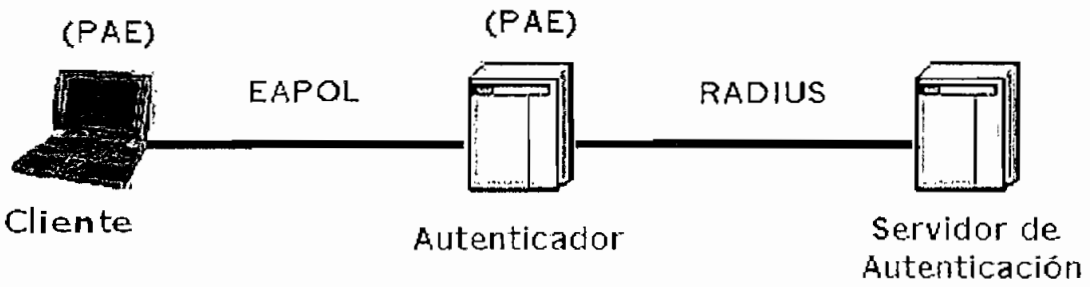


Fig. 2.38 Arquitectura y Nomenclatura 802.1x [13]

El proceso de autenticación se realiza de forma lógica entre el cliente y el servidor de autenticación, con el autenticador actuando solamente como un puente. Entre el cliente y el autenticador, se utiliza el protocolo *EAP over LAN* (EAPOL) o también conocido como *EAP over WLAN* (EAPW). Entre el autenticador y el servidor se utiliza el protocolo RADIUS, también conocido como *EAP over RADIUS*. Como se puede apreciar 802.1x es simplemente un marco de trabajo.

El mecanismo preciso de autenticación (LEAP, EAP- TLS, etc.) es implementado por el servidor, 802.1x provee los mecanismos para el intercambio de credenciales y la confirmación de acceso. Es por esto que cambiar el método de autenticación no requiere cambios complejos en los dispositivos de usuario o en la infraestructura de la red. Ahora que se conoce la arquitectura de trabajo de 802.1x, se debe describir el funcionamiento de los protocolos que ayudan a su implementación: EAPOL y RADIUS.

a) Encapsulación EAPOL

EAP es simplemente el encapsulamiento de EAP sobre los protocolos de red LAN como el 802.11. El formato básico de una trama EAPOL se muestra en la figura 2.39.

- Cabecera MAC.- Contiene las direcciones MAC origen y destino.

- Tipo de Ethernet.- Como cualquier tipo de trama Ethernet, el EAPOL tiene su código asignado que es 88 8EH.

- Versión.- Solo la versión 1 de EAPOL está estandarizada.

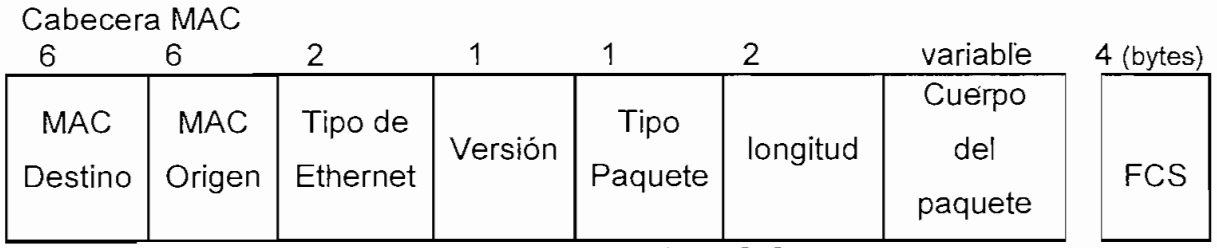


Fig. 2.39 Paquete EAPOL [13]

- Tipo de Paquete.- EAPOL es una extensión de EAP, y además de los mensajes descritos para EAP, EAPOL añade algunos mensajes para adaptar EAP a un ambiente LAN basado en puerto. En la tabla 2.6 se muestran los tipos de paquete y su descripción.

- Longitud.- Este campo de 2 bytes contiene la longitud del campo cuerpo del paquete en bytes. Es cero si el cuerpo del paquete no está presente.

- Cuerpo del paquete.- Este campo es de longitud variable, está presente en todos los paquetes EAPOL excepto en los mensajes de *Start* y *Logoff*. Éste encapsula un paquete EAP en tramas *EAP- packet*, las claves en tramas *EAP – Key* y una alerta en *EAPOL–Encapsulated ASF Alert.*

- FCS.- Es una suma de comprobación (CRC) de la trama en su totalidad.

b) Ejemplo de intercambio 802.1x

El intercambio EAPOL es similar al de EAP. Las principales diferencias son que el cliente puede generar tramas *EAPOL- Start* para disparar el intercambio EAPOL y también puede utilizar tramas *EAPOL – logoff* para desautorizar el puerto en el que la estación está utilizando la red.

Tipo de Paquete	*Nombre*	Descripción
0000 0000	*EAP-Packet*	Contiene y encapsula un paquete EAP.
0000 0001	*EAPOL - Start*	En lugar de esperar un *challenge* del autenticador, el cliente puede enviar una trama *EAPOL – Start* para forzar a iniciar el proceso de autenticación.
0000 0010	*EAPOL – Logoff*	Cuando un sistema ya no va a utilizar la red, envía un paquete *EAPOL- Logoff* para retornar el puerto a un estado sin autorización.
0000 0011	*EAPOL - Key*	Es utilizado para el intercambio de información criptográfica. En especial el intercambio de claves.
0000 0100	*EAPOL–Encapsulated ASF Alert*	El ASF *Alerting Standard Forum* ha definido una forma de enviar alertas, como *traps* SNMP, para ser enviados a un puerto no autorizado usando este tipo de paquete.

Tabla 2.6 Tipos de Paquetes EAPOL [13]

El caso más común de autenticación se muestra en la figura 2.40. En principio el puerto no está autorizado, así que el acceso a la red está bloqueado. Los pasos típicos para el intercambio EAPOL son:

- El cliente empieza el intercambio 802.1x con un mensaje *EAPOL- Start.*

- El intercambio normal de EAP comienza. El autenticador contesta con una trama *EAP – Request/ identity.*

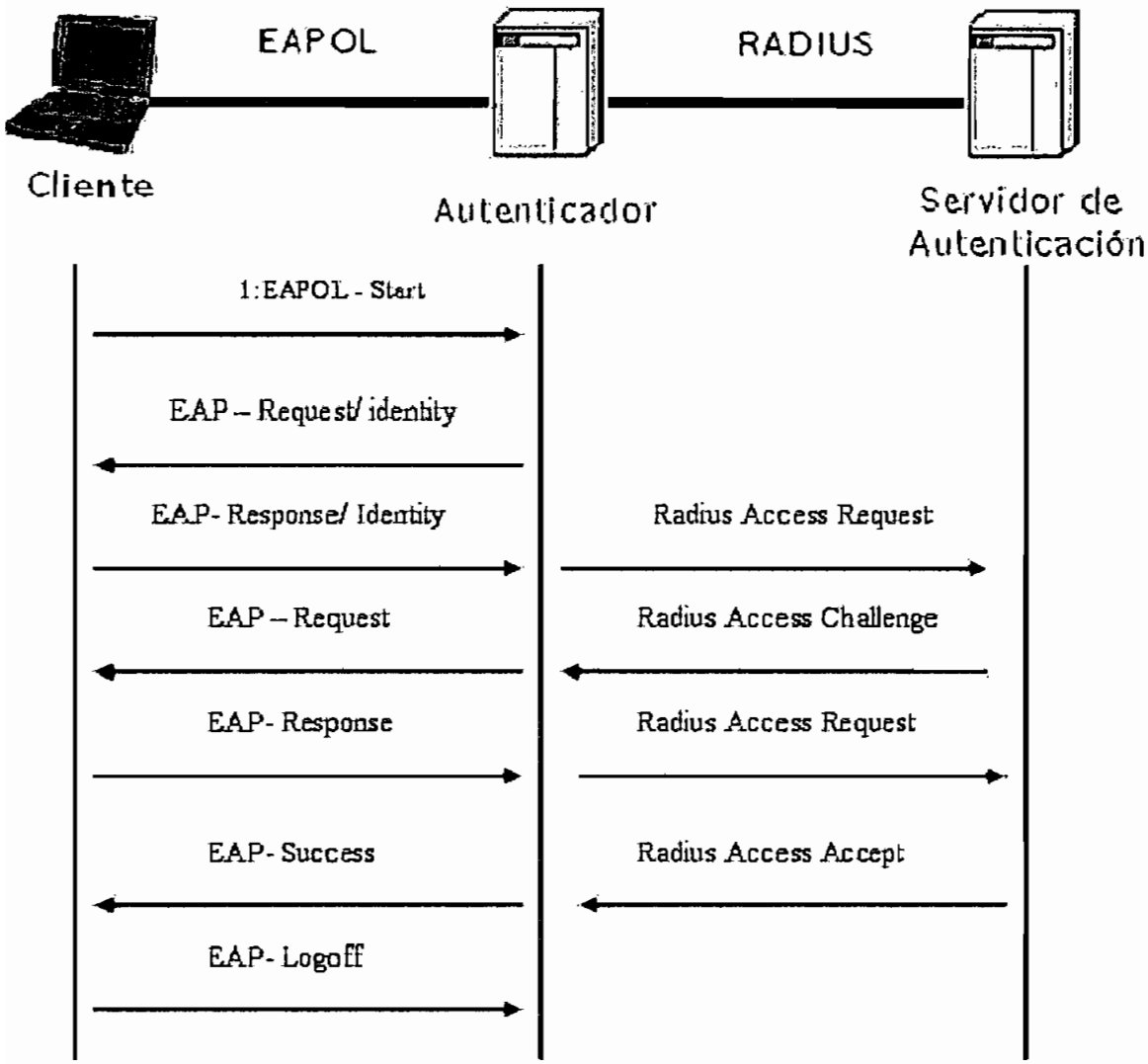


Fig. 2.40 Autenticación EAP [13]

- El cliente responde con un mensaje *EAP- Response/ Identity*, que es pasado al servidor RADIUS como un paquete *Radius Access Request.*

- El servidor Radius responde con un paquete *Radius Access Challenge*, enviado al cliente como un *EAP- Request* junto con información apropiada para el método de autenticación.

- El cliente captura la respuesta del cliente y envía un EAP-Response de retorno. La respuesta es traducida por el autenticador en un *Radius Access Request* con la respuesta al desafío en el campo de datos.

- El servidor RADIUS otorga acceso con un mensaje *Radius Access Accept*, con lo que el autenticador envía una trama *EAP-Success*. Entonces el Puerto es autorizado y el cliente puede empezar a utilizar la red. Todos los servicios de la red empiezan a funcionar en este punto como DHCP, DNS, etc.

- Si el cliente no fue autorizado a utilizar la red, éste envía un mensaje *EAP – Logoff* para poner el puerto de regreso a un estado no autorizado.

c) RADIUS

Es el servidor AAA (*Authentication, Authorization and Accounting)* ampliamente utilizado en ambientes de red. El protocolo es utilizado por dispositivos de red como *routers, switches*, puntos de acceso, etc. para comunicarse con un servidor de autenticación RADIUS. Está definido en el RFC 2865 *Remote Authentication Dial In User Service.* El éxito de este protocolo radica en las siguientes ventajas:

- Administración centralizada de sistemas complejos. Manejo de grandes infraestructuras de clientes.

- Protección contra *hackers* que intenten capturar las credenciales de los clientes autorizados.

- El soporte de RADIUS es general. Es consistente con todo el hardware y software de los dispositivos de red del mercado.

- Ofrece compatibilidad para varios tipos de autenticación, facilitando que los fabricantes puedan desarrollar sus mejoras sobre una base estándar.

- RADIUS es actualmente el estándar *de-facto* para autenticación AAA.

- Compatibilidad con sistemas antiguos (*legacy*).

c.1) Funcionalidades del Servidor RADIUS

RADIUS es ofrece administración centralizada de la Autenticación, Autorización y Registro de la actividad de los usuarios conectados en la red.

- Autenticación: Es el proceso mediante el cual se decide si el usuario es o no quien dice ser; así mismo se define si está autorizado o no para el ingreso a la red, esto se hace validando las credenciales del usuario.

- Autorización: En este proceso se define a qué recursos de red puede acceder el usuario y se limita el tiempo que puede estar conectado en la red.

- Registro de actividad: En este proceso se generan archivos (*Logs*) que graban los datos que describen cada conexión de red, es usado normalmente para facturación, diagnóstico y planeamiento de la expansión de la red.

Toda la información de seguridad de los usuarios está centralizada en uno o más servidores RADIUS; el sistema RADIUS soporta configuraciones de "múltiples sitios / sedes" y "múltiples dominios / organizaciones", así mismo soporta el "*Roaming*" de usuarios.

El servidor debe tener acceso a una base de datos con la información de cada usuario, perfiles de red para un usuario o grupo de usuarios, políticas de seguridad y el nivel de acceso a los recursos de la red y aplicaciones que le corresponden.

Estas bases de datos pueden estar almacenadas localmente en el mismo servidor RADIUS o estar ubicadas en servidores de bases de datos remotos.

La compatibilidad con el tipo de bases de datos depende de la implementación específica del servidor RADIUS. Por ejemplo existen servidores comerciales como el *Steel Belted Radius* 4.0 de la empresa *Funk Software* que ofrece compatibilidad con bases LDAP[1] y SQL. El servidor *Odyssey Server* de la misma empresa ofrece en cambio compatibilidad con la base de datos de Windows administrada en el *Active Directory*.

Cisco ofrece varios tipos de servidores RADIUS para plataformas Windows y Unix con su producto comercial ACS *Cisco Secure Access Control Server*.

El soporte del servidor RADIUS para los diferentes tipos de EAP existentes depende también de la implementación comercial del mismo. Por ejemplo el Servidor RADIUS de Windows 2003 Server da soporte principal a EAP – TLS, aunque también maneja otros tipos de EAP.

Al momento de elegir un servidor RADIUS se debe establecer la compatibilidad con el hardware de la WLAN. Para verificar esto se debe revisar la documentación del servidor y establecer claramente sus funcionalidades y soporte para el hardware inalámbrico.

c.2) Funcionamiento del servidor RADIUS

En el esquema de AAA de RADIUS los puertos de red de un dispositivo de acceso normalmente se encuentran en el estado "desautorizado" y sólo pueden pasar el tráfico explícitamente permitido por el RADIUS.
Típicamente este tráfico está limitado a las funciones de autenticación y el resto de aplicaciones quedan bloqueadas incluso los algoritmos de DHCP usados para

[1] Protocolo de Acceso Ligero a Directorio

la asignación de direcciones IP no se puede transmitir hasta que los datos del usuario sean validados.

Sólo cuando el usuario está validado el tráfico puede pasar libremente desde y hacia el usuario.

Muchos servidores RADIUS comerciales implementan funcionalidades adicionales que facilitan la administración de los usuarios. Puede definir atributos lógicos como los días de la semana donde el acceso es permitido, la duración de la conexión, el número de sesiones que se pueden abrir con el mismo nombre de usuario, etc.

c.3) Formato del paquete RADIUS

RADIUS define el formato de paquete que se utiliza para el intercambio de información de autenticación entre el autenticador y el servidor. Este encapsulamiento se conoce también como *EAP over RADIUS*. El formato se muestra en la figura 2.41.

1	1	2 (bytes)
Código	Identificador	Longitud
Autenticador		
Atributos		

Fig. 2.41 Paquete RADIUS [13]

El campo código establece el tipo de paquete, en la tabla 2.7 se muestran los valores correspondientes al tipo de paquete y su descripción.

El campo identificador es de un byte de longitud, permite al cliente RADIUS asociar la respuesta RADIUS con la respectiva petición.

El campo longitud de 2 bytes contiene la longitud de todo el paquete RADIUS, por lo que incluye la longitud los campos de Código, Identificador, Longitud,

Autenticador y Atributos. El campo autenticador es de 2 bytes de longitud. Este valor es utilizado para autenticar las respuestas del servidor RADIUS.

Valor	Paquete	Descripción
1	*Access-Request*	Petición de acceso de un cliente
2	*Access-Accept*	Petición aceptada
3	*Access-Reject*	Petición rechazada
4	*Accounting-Request*	Petición de Registro
5	*Accounting-Response*	Respuesta de Registro
11	*Access-Challenge*	Desafío de acceso para autenticación del cliente
12	*Status-Server* (experimental)	Reservado
13	*Status-Client* (experimental)	Reservado
255	*Reserved*	Reservado

Tabla 2.7 Valores del campo Code [13]

La sección de atributos se tiene cuando un número arbitrario de campos de atributos son almacenados. Por ejemplo en el caso más simple sería el *Username* y el *Password* del cliente.

c.4) Manejo de llaves

Una vez que la autenticación fue exitosa el servidor RADIUS debe manejar la generación y entrega de la clave criptográfica de sesión WEP para el cliente WLAN. Estas llaves son generadas de forma aleatoria mediante algoritmos

específicos de la implementación del servidor. Esta clave se entrega al AP que a su vez le envía al cliente en mensajes *EAPOL – Key*.

2.4.3.3. LEAP

LEAP (*Ligthweight EAP*) ó *EAP-Cisco Wireless* se basa en autenticación por nombre de usuario y *password*. Es un protocolo propietario de Cisco que cumple con el estándar 802.1x. Soporta plataformas Windows, Macintosh y Linux tanto para el servidor como para los usuarios WLAN.

a) Características técnicas

Al ser un protocolo propietario de Cisco, se requiere que toda la infraestructura de la WLAN sea Cisco, esto es AP´s y tarjetas inalámbricas. En el lado del cliente se debe tener un utilitario de software que maneje el proceso de autenticación, este utilitario puede ser propio del sistema operativo o software de CISCO como el ACU *Aironet Client Utility*. Para la implementación del servidor RADIUS se tienen 3 opciones:

- Servidor RADIUS Comercial, desarrollado por empresas de software privadas para diversas plataformas.
- Servidor CISCO ACS *Access Control Server*, propietario de CISCO para plataformas Windows y Unix.
- Servidor *FreeRadius*, software gratuito para plataformas Linux

El proceso de autenticación se realiza en base a *username* y *password*, datos que se almacena en la base de datos del servidor RADIUS. A continuación se describe el funcionamiento de LEAP.

b) Funcionamiento de LEAP

Una secuencia de intercambio de autenticación típica de LEAP consiste en los siguientes paquetes, encapsulados en los protocolos EAPOL y RADIUS descritos anteriormente.

1. El cliente (software utilitario) genera un *challenge response* a través del algoritmo de LEAP (conocido sólo por Cisco) con su *password*. Este *challenge response* es enviado junto con su *username* al AP mediante encapsulación EAPOL. Debe notarse que el *password* nunca se transmite sobre la red.

2. El AP envía esta solicitud al Servidor mediante encapsulación RADIUS.

3. El servidor recibe la petición y busca el nombre del usuario y su *password* en su base de datos, luego utiliza el algoritmo de LEAP y el *password* del cliente para generar su propio *challenge response*. Si el *password* enviado por el cliente y el de la base de datos del servidor son idénticos, el *challenge response* también será idéntico y el acceso será otorgado. El servidor envía la respuesta positiva al AP.

4. El AP pasa estos datos al cliente y le indica que la autenticación fue exitosa.

5. Ahora es el turno del cliente de autenticar la WLAN a la que se conecta. Envía un *challenge* de 8 bytes aleatorio al AP generado con su *password* y el algoritmo de LEAP.

6. El AP pasa estos datos del cliente al servidor.

7. El servidor genera la respuesta al *challenge* y envía la clave de sesión WEP para la encripción de los datos del usuario.

8. El cliente verifica el desafío para autenticar la red, si fue correcto, con la clave WEP enviada por el servidor empieza a transmitir sus datos al AP.

Como se puede apreciar el *password* no viaja por la red por lo que no puede ser interceptado y robado.

c) Ventajas de LEAP

- Fácil y relativamente rápido de implementar.
- Autenticación mutua, del usuario y la red entre sí.
- Se tiene gran soporte de CISCO, en software, hardware, documentación y corrección de problemas.
- Muy difundido y popular en el mercado.
- Al ser un protocolo propietario de Cisco, los algoritmos de generación del *challenge* no son públicos.
- No requiere de infraestructura de clave pública y de certificados digitales.

d) Desventajas

- Solo funciona sobre infraestructura Cisco pues es un protocolo propietario.
- Es susceptible de ataques de diccionarios como todo mecanismo de autenticación por *password*.

2.4.3.4. EAP - TLS

EAP - TLS está definido en el RFC 2716, es un protocolo desarrollado por Microsoft que permite a los usuarios autenticarse mediante el uso completo de

certificados digitales con el estándar X.509. Además el intercambio de credenciales se realiza sobre un túnel seguro mediante TLS (*Transport Layer Security)*, haciendo difícil que la información de autenticación del usuario sea capturada.

Fue diseñado para ser implementado en sistema operativo Windows XP que tiene un cliente de software para EAP-TLS, por lo que originalmente sólo se podía utilizar plataformas Microsoft para los certificados digitales. Sin embargo luego de la publicación del RFC, muchos fabricantes trabajaron en la implementación de EAP-TLS, a más de *Microsoft*, logrando un buen desarrollo por lo que actualmente se tiene una variedad de opciones para diferentes plataformas.

a) Características técnicas

EAP - TLS utiliza la infraestructura de clave pública para la autenticación mutua entre el usuario y la WLAN. Esto implica que tanto el cliente como el servidor deben tener certificados digitales autorizados debidamente instalados. El utilizar infraestructura de clave pública y certificados digitales implica mayor complejidad del servidor RADIUS y mayores costos de implementación y administración de la WLAN.

b) Funcionamiento de EAP - TLS

A continuación se describe el proceso de acceso a la WLAN mediante EAP - TLS que consta de 3 fases:

b.1) Fase de autenticación

La primera fase funciona siguiendo el estándar IEEE 802.1x, es decir, cuando el cliente entra en el área de cobertura del AP, éste le pide su identidad, y el cliente se la proporciona (de forma plana). Tras esta fase inicial se realiza el proceso de establecimiento de conexión TLS entre los extremos (el protocolo TLS se explica en el anexo 1), donde según el estándar tanto el cliente como el servidor se

autentican mutuamente mediante certificados X.509 y negocian los parámetros de configuración necesarios para establecer el canal de comunicación seguro.

Fig. 2.42 Canal Seguro TLS

Una vez terminada la negociación, se establece un canal TLS entre el cliente y el servidor de autenticación basado en la posesión por ambas partes de un secreto compartido (*Master Secret*) que posteriormente se utilizará para derivar la clave de sesión WEP.

b.2) Fase de autorización

En esta fase el cliente indica al servidor de autenticación cuál es el tipo de conexión que desea en cuanto al ancho de banda requerido y el tiempo que va a estar conectado, junto con los certificados que demuestran que está autorizado a realizar el uso de la red .

Entonces el servidor evalúa los certificados y comprueba su validez, si todo es correcto y el nivel de privilegios del cliente es el necesario, lo autoriza. Por el contrario lo desautoriza al cliente para acceder a la red si hay algún problema. Algo importante de diferenciar es que de esta forma no es necesario acceder a ninguna base de datos de usuarios para comprobar los permisos de los mismos, sino que sólo se necesita confiar en las entidades emisoras de dichos certificados de autorización.

Los parámetros del cliente se mandan en una estructura firmada, de manera que el servidor de autenticación pueda estar seguro de que nadie ha modificado estos parámetros. Además, toda la información relativa a la autorización del cliente, parámetros y certificados, se manda a través del canal TLS establecido anteriormente, de manera que solo pueden haber sido enviados por parte del cliente con el que se ha iniciado el proceso de conexión.

Dicha estructura contiene el certificado del cliente con el que se ha realizado la firma para que el servidor pueda verificar que la firma es correcta. En el mensaje mediante el cual el servidor le pide al cliente sus parámetros de conexión, se incluye un identificador de 4 bytes aleatorio, que posteriormente se utilizará para derivar la clave WEP junto con la dirección MAC del punto de acceso y la clave maestra de la conexión TLS anteriormente establecida.

b.3) Fase de distribución de clave

En esta fase del protocolo, únicamente participan el punto de acceso y el servidor de autenticación, y consiste en que este último le pase al primero un descriptor de la clave WEP que debe utilizar con el cliente, así como el tipo de servicio que el cliente espera que se le ofrezca.

Esta clave WEP la habrá generado el servidor, como resultado de una función de resumen digital MD5 aplicada sobre la clave maestra generada por EAP-TLS, la dirección MAC del punto de acceso, y los 4 bytes aleatorios generados por el servidor anteriormente.

Por su parte, el punto de acceso debe comprobar que en su situación actual puede soportar las necesidades del nuevo cliente, es decir, debe comprobar que la suma total del ancho de banda necesitado por todos los usuarios que actualmente hay conectados, junto con el requerido por el nuevo cliente, no sobrepase su capacidad. Adicionalmente comprueba que vaya a estar disponible el tiempo que el cliente requiere; informando al servidor de autenticación sobre la decisión que tome.

Tras estas fases, el proceso de conexión ha terminado, y si todo se ha realizado correctamente, el servidor de autenticación notifica al punto de acceso la autorización por su parte, a que el cliente haga uso de la red.

El punto de acceso traslada entonces al cliente esta decisión para que inicie la comunicación. El cliente, que habrá generado la misma clave WEP que obtuvo el punto de acceso, puede comenzar a hacer uso de la red, con la garantía de que

sus mensajes son sólo descifrables por el punto de acceso, dado que la clave WEP generada es distinta para cada usuario.

c) Ventajas de EAP - TLS

- Fuerte autenticación mutua basada en certificados X.509.
- La sesión TLS provee seguridad adicional en el intercambio de credenciales.
- Actualmente la solución más segura de seguridad para WLAN´s.

d) Desventajas de EAP – TLS

- La solución EAP –TLS es difícil de gestionar pues se requiere un Autoridad Certificadora para el soporte de los certificados X.509 y su respectiva instalación y mantenimiento en el servidor y clientes.
- Implica más costos de implementación y administración, debido a que el servidor RADIUS es más complejo y debe manejar TLS. Además los certificados del servidor y los clientes implican también costos adicionales.
- Al momento no es una solución muy popular para WLAN. Los administradores son reacios a su uso debido a la gran infraestructura que implica su implementación.

2.4.3.5. EAP- TTLS

Protocolo desarrollado por las empresas *Funk Software* y CERTICOM, permite a los usuarios autenticarse mediante nombre de usuario y contraseña, pero con intercambio de *password* vía un túnel seguro TLS. Para la autenticación solamente requiere que el certificado digital sea distribuido al servidor, y no a los

clientes, por lo que no es necesario mantener una infraestructura compleja de administración y distribución de certificados en los usuarios.

a) Características técnicas

Es un protocolo libre, que puede ser implementado en base a su RFC el 2716 por cualquier fabricante. Utiliza autenticación por *username* y *password* pero primero establece un túnel seguro entre el cliente y el servidor para el intercambio de esta información. Ofrece autenticación mutua, credenciales de seguridad y generación de llaves dinámicas por sesión.

Para la autenticación de los servidores RADIUS se requiere que tengan instalado un certificado digital debidamente autorizado por una Autoridad Certificadora. Para la autenticación por *password* permite el uso de CHAP, PAP, MS-CHAP y MS-CHAPv2.

b) Funcionamiento de EAP - TTLS

Funciona de forma similar a EAP-TLS, excepto que para la autenticación del usuario se la realiza mediante *username* y *password*. Para la autenticación del servidor se sigue utilizando cerificados X.509.

c) Ventajas de EAP – TTLS

- Es más sencillo de instalar y gestionar comparado con EAP-TLS, ya que no requiere Certificados en el Cliente.
- Permite compatibilidad con varios tipos de bases de datos.
- No existe peligro de ataques de diccionario, ya que las credenciales del usuario viajan sobre el túnel TLS establecido, incluso la identidad del mismo.

d) Desventajas de EAP – TTLS

- Requiere un certificado digital otorgado por una autoridad certificadora, correctamente instalado en el servidor, lo que implica mayores costos.

2.5. COMPARACIÓN DE LOS ESTÁNDARES DE SEGURIDAD PARA REDES INALÁMBRICAS

Una vez que se tiene claro el funcionamiento, ventajas y desventajas, así como la implementación de los más importantes mecanismos de seguridad en WLAN´s, se debe proceder a establecer una comparación entre los mismos. En la tabla 2.8 se muestra un cuadro comparativo de los mecanismos WEP (más mejoras WPA), LEAP, EAP- TLS y EAP – TTLS. De esta tabla se puede obtener algunas ideas importantes. EAP-TTLS y EAP-TLS implican el manejo de certificados digitales y el establecimiento de sesiones seguras TLS, lo cual implica mayor complejidad en el servidor RADIUS y mayores costos.

La solución WEP es la más económica de todas pues no requiere ningún hardware o software adicional, sin embargo, es la solución más débil de todas y solo se debe utilizar en pequeñas empresas y hogares. La solución LEAP es la más común para WLAN's de pequeñas y grandes empresas, gracias a que ofrece la mejor relación costo-beneficio para una WLAN segura.

Ahora que se tienen las ventajas y desventajas de los diferentes mecanismos de seguridad *en redes inalámbricas*, se puede elegir el adecuado para una solución práctica. El decidirse a utilizar un mecanismo específico de seguridad depende de varios factores, como por ejemplo: el tamaño de la WLAN, las necesidades de la empresa, el factor económico, etc. En fin, dependiendo de la necesidad específica, se debe elegir el método adecuado. En las conclusiones finales del presente trabajo se desarrolla un análisis sobre el tipo de mecanismo de seguridad más adecuado para cada escenario.

Tema	WEP	LEAP	EAP -TTLS	EAP – TLS
Solución de seguridad	Estándar	Propietaria (cisco)	Estándar	Estándar
Certificados en el Cliente	No	No	No	Si
Certificados en el Servidor	No	No	Si	Si
Intercambio de claves dinámicas	No	Si	Si	Si
Autenticación mutua	No	Si	Si	Si
Plataformas de cliente soportadas	Linux, Windows y Mac.	Linux, Windows y Mac.	Linux, Windows y Mac.	Linux, Windows y Mac.
Servidor de Autenticación implementado por	N/A	CISCO (Cisco vende el motor de LEAP a otras empresas de software)	*Funk y Meetinghouse*	CISCO, *Funk,* HP, *FreeRadius, Meetinghouse y Microsoft*
Protección de la identidad del cliente	No	No	Si (mediante TLS)	No
Nivel de solución empresarial	Pequeña	Mediana - Corporativa	Mediana - Corporativa	Corporativa
Costo de implementación, mantenimiento y administración.	Bajo	Medio	Medio - Alto	Alto

Tabla 2.8 Canal Seguro TLS

CAPÍTULO 3

3. SOLUCIÓN PARA UNA RED LAN INALÁMBRICA SEGURA DE PEQUEÑA ESCALA CON WEP

En este capítulo se presenta una guía de implementación de seguridad en una red LAN inalámbrica de pequeña escala utilizando el protocolo WEP. Para ello se describen los diferentes aspectos a considerar en la solución WEP, se define un escenario común para redes inalámbricas y se diseña la solución para su implementación.

3.1. GENERALIDADES DE LA SOLUCIÓN CON WEP

Para la implementación de seguridad en una WLAN con WEP se tienen presentes sólo 2 componentes: el *Access Point* y las tarjetas inalámbricas de los clientes, presentándose el escenario común de la figura 3.1.

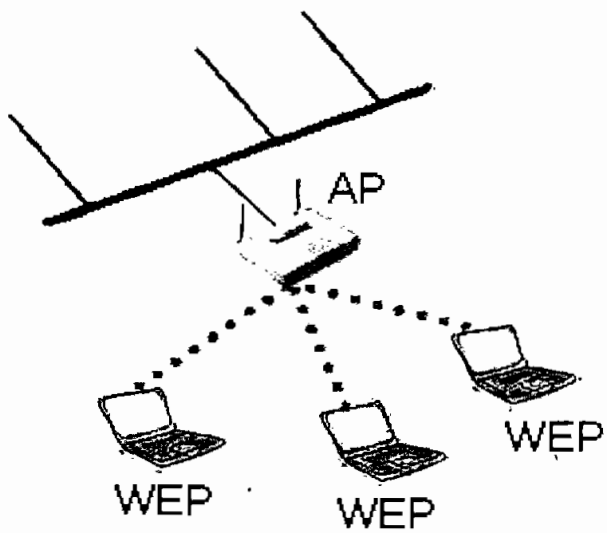


Fig. 3.1 Red WLAN con seguridad WEP

Los usuarios para asociarse a la red, simplemente necesitan sus tarjetas inalámbricas y el respectivo software de manejo de WLAN´s. Mediante este

software se deben configurar los parámetros de seguridad WEP que la red utiliza, como la clave compartida, tipo de autenticación, etc. Si los parámetros de seguridad WEP o la clave compartida del cliente no corresponden a los de la WLAN, no se podrá establecer la asociación.

Además para que WEP sea más fuerte contra ataques, se debe considerar el uso de las herramientas adicionales como el TKIP y el MIC (mejoras de WPA).

Sin embargo, la seguridad WEP por si sola no es suficiente ya que se deben implementar políticas de seguridad adicionales como accesos restringidos al AP, filtros MAC, etc.

3.2. DESCRIPCIÓN DEL PROBLEMA

Un escenario muy común es el siguiente. En una empresa mediana se desea proveer de cobertura inalámbrica a la recepción, oficinas y sala de reuniones, para así evitarse tender cableado en instalaciones que son alquiladas.

Además se tienen planes de movimiento de oficinas hacia un edificio propio, por lo que invertir en cableado no es una buena idea. La empresa también no desea invertir en gasto adicional para la seguridad de la WLAN.

Para la solución del presente problema se asume que se tiene el mapa de sitio de la figura 3.2, donde se aprecian las áreas que requieren cobertura (el área cero es una bodega de limpieza y no requiere de cobertura). Además se debe recalcar que las divisiones de oficinas son simplemente de madera y a una altura de 1.6 metros del suelo, por lo cual las señales RF no tendrán ningún problema en cubrir esta zona. En total el área a cubrir es de aproximadamente 5000 m^2.

Se tienen aproximadamente un total de 10 usuarios inalámbricos que podrían estar conectados al mismo tiempo a la red, utilizando principalmente correo electrónico, Internet y accediendo a carpetas compartidas en servidores.

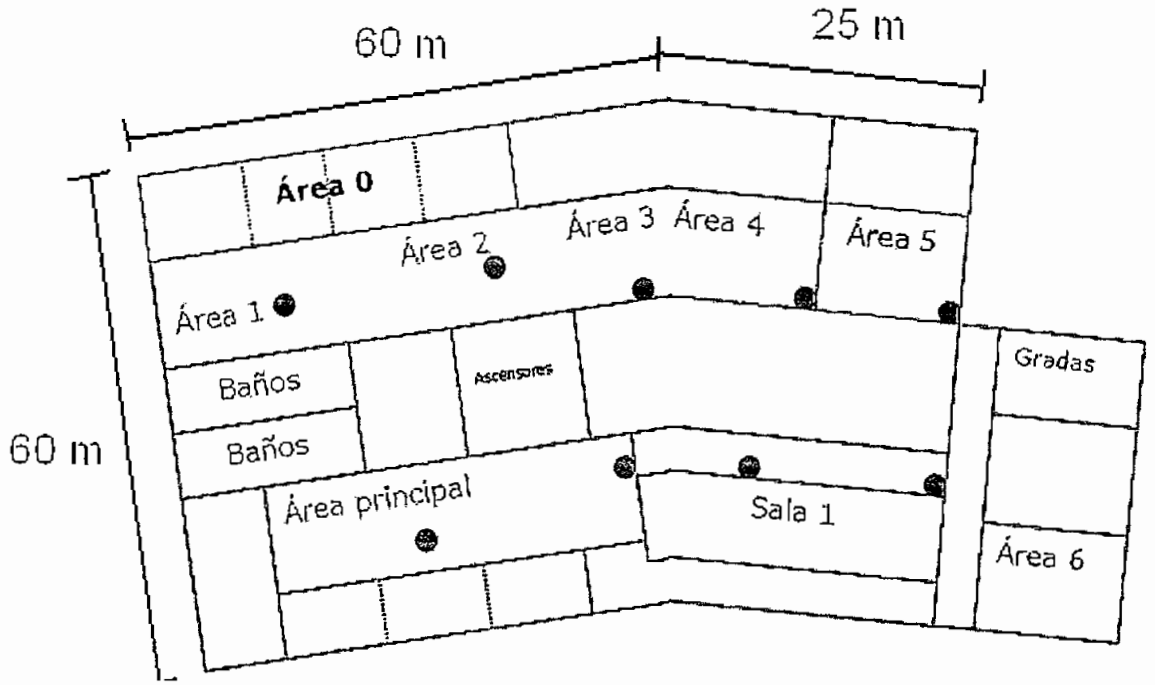


Fig. 3.2 Área que requiere servicio inalámbrico

En la figura 3.3 se presenta el diagrama de red de la WLAN, con su respectivo direccionamiento IP. En la figura se tienen las estaciones, el AP y el servidor *proxy*[1] de la red.

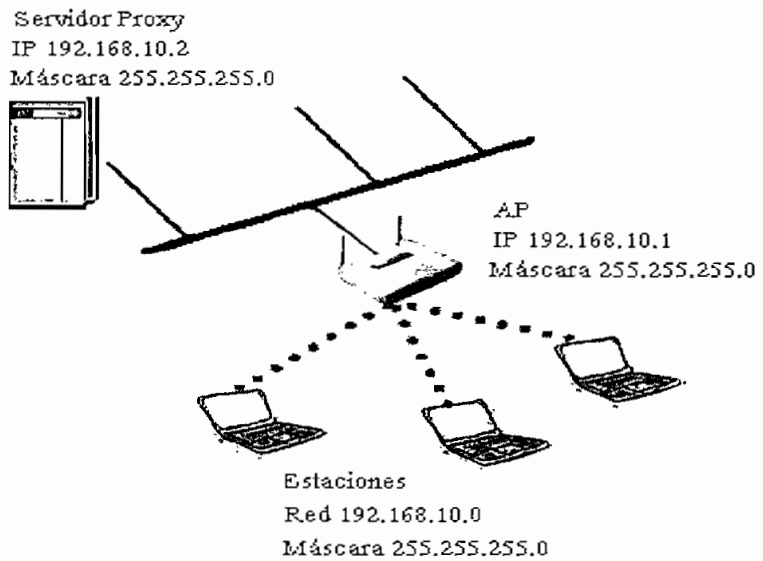


Fig. 3.3 Diagrama topológico de la red

[1] Servidor para acceso a Internet

De acuerdo a este escenario se deberá plantear la solución de conectividad.

3.3. BOSQUEJO DE LA SOLUCIÓN

La solución de seguridad con WEP requiere de la configuración de la clave secreta en el AP y en los clientes.

Además de esto se requieren establecer mecanismos de seguridad adicionales como accesos protegidos, filtros MAC, etc. Para la implementación se tiene un AP CISCO de la serie 340 con 2 antenas dipolares, como el que se muestra en la figura 3.4. Las características técnicas de este equipo se indican en el Anexo 2.

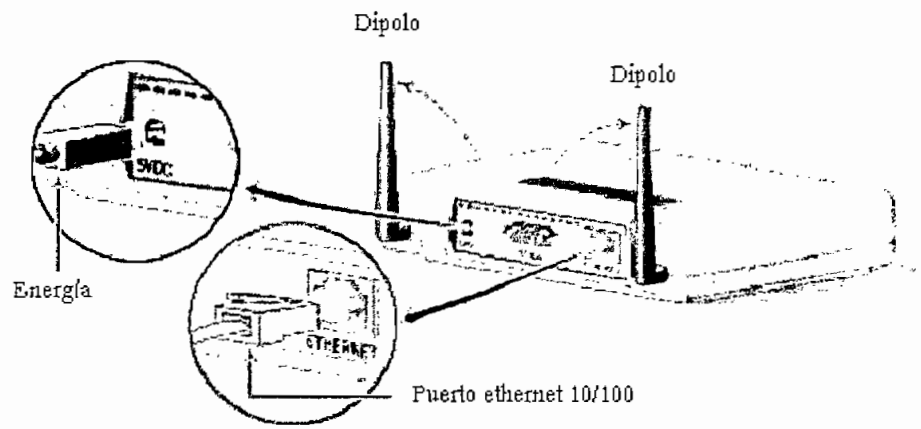


Fig. 3.4 AP 340 Aironet CISCO [14]

De acuerdo al Anexo 2, el AP 340 con sus 2 antenas dipolares de tipo omnidireccional[1] son suficientes para cubrir el área de cobertura requerida. En ambientes *indoor* la cobertura del equipo llega hasta los 300 m de radio.

[1] Propagación de las ondas de radiofrecuencia en todas las direcciones

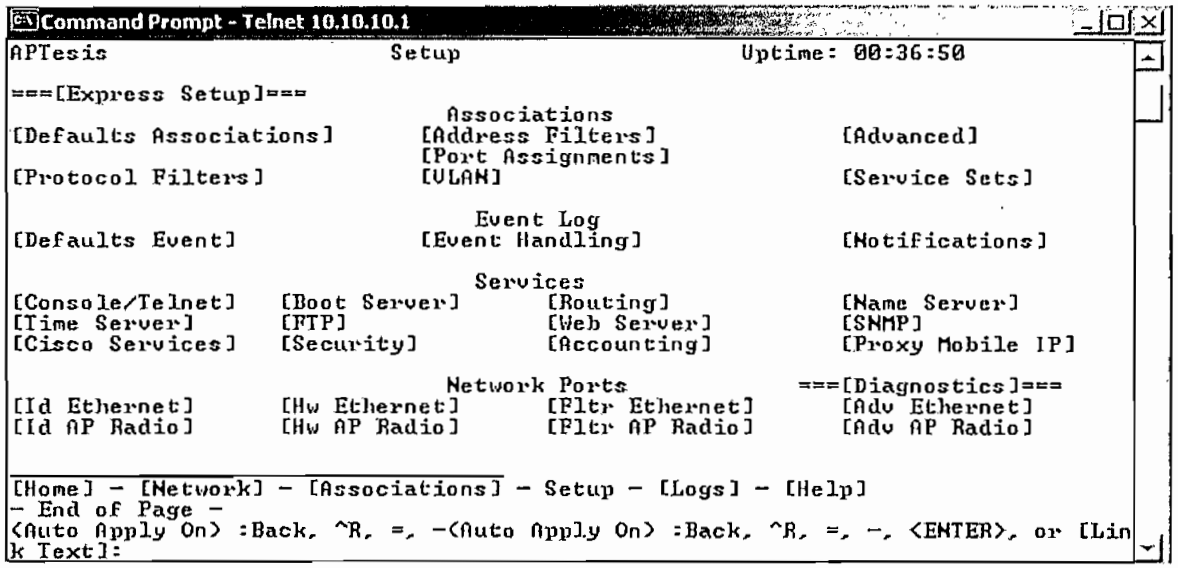


Fig. 3.11 Acceso vía Telnet al AP 340 Aironet CISCO

3.4.1.3. Acceso vía Web

Es la forma más interactiva y sencilla de configurar y realizar cambios al AP, principalmente por la interfaz interactiva que muestra al administrador y por la facilidad de acceso remoto que ofrece. Para acceder vía Web al AP se digita la dirección http://10.10.10.1 en un *browser* como el *Internet Explorer* de Windows, luego de lo cual se despliega la pantalla indicada en la figura 3.12.

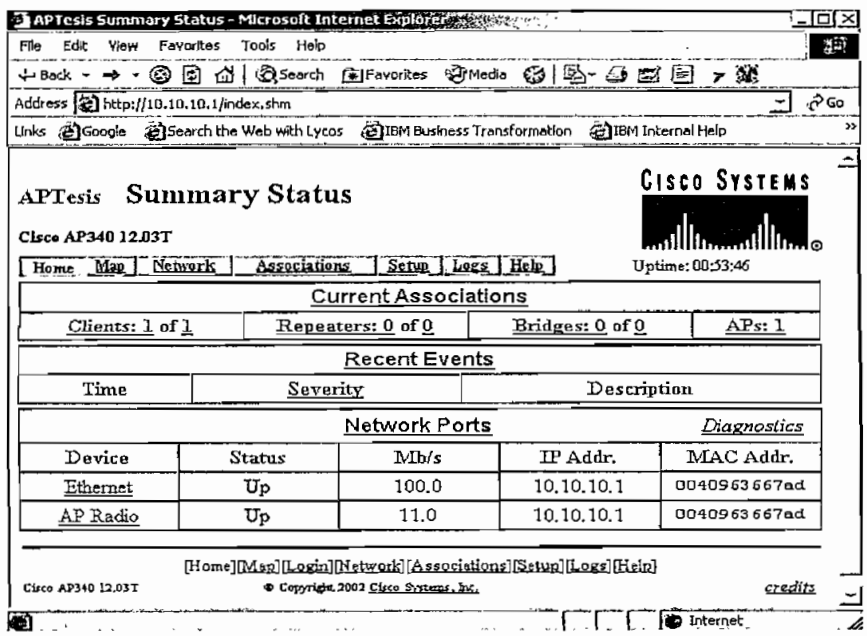


Fig. 3.12 Acceso vía Web al AP 340 Aironet CISCO

Se despliega la pantalla de inicio *Home* en la que se visualiza el estado del AP, un registro de eventos y el menú principal para acceder a las diferentes utilidades del software de configuración del AP. Gracias a la versatilidad de la configuración vía Web, los posteriores cambios se realizarán bajo este esquema.

3.4.1.4. Configuración Básica del AP CISCO 340 vía Web

Los parámetros básicos que se deben configurar en el AP son los siguientes:

- Nombre
- SSID
- Dirección IP, Máscara de red y *Default Gateway*
- Modo de Funcionamiento
- Comunidad SNMP

El nombre del AP es simplemente un parámetro de identificación del AP, y no influye en el funcionamiento o desempeño del mismo. Sirve simplemente para hacer más fácil la tarea de administración de la WLAN, ya que si se tienen varios AP's, el nombre puede tener información sobre el modelo, ubicación física, etc. En este caso el nombre del AP va a ser *AP340ecenter,* que hace referencia al modelo y ubicación del AP.

El SSID es el identificador de la WLAN, en este caso el SSID seleccionado es **1xWLAN.** La dirección IP del AP es la 192.168.10.1 con máscara de red de 255.255.255.0. El *default Gateway* es 192.168.10.2. Como se asigna una dirección IP estática al AP, el servicio DHCP se debe deshabilitar.

El AP puede funcionar en tres modos:

- AP raíz .- Concentrador de usuarios inalámbricos
- Repetidor.- Reenvía los paquetes que llegan a un AP raíz
- Cliente de supervisión.- Cliente de pruebas

Para que pueda dar cobertura a una WLAN el AP debe estar en modo raíz. La comunidad SNMP indica el grupo administrativo al cual pertenece el AP, en el problema actual la comunidad seleccionada es *root*.

Un resumen de estos parámetros de configuración se muestra en la tabla 3.3

Nombre del parámetro	Valor
System Name	*AP340ecenter*
Config Server Protocol (DHCP)	*None*
IP	*192.168.10.1*
Máscara	*255.255.255.0*
Default Gateway	*192.168.10.2*
SSID	*1xWLAN*
Role	*Access Point/Root*
SNMP Community	*root*

Tabla 3.3 Parámetros finales del AP

Para configurar todos estos parámetros se ingresa a *Setup* y luego a *Express Setup* del menú principal, con lo que aparece la pantalla de la figura 3.13. Aquí se cambian los parámetros predeterminados por los mencionados anteriormente, obteniendo como resultado la pantalla de la figura 3.14. Luego se da clic en *Apply* y los cambios se ejecutan.

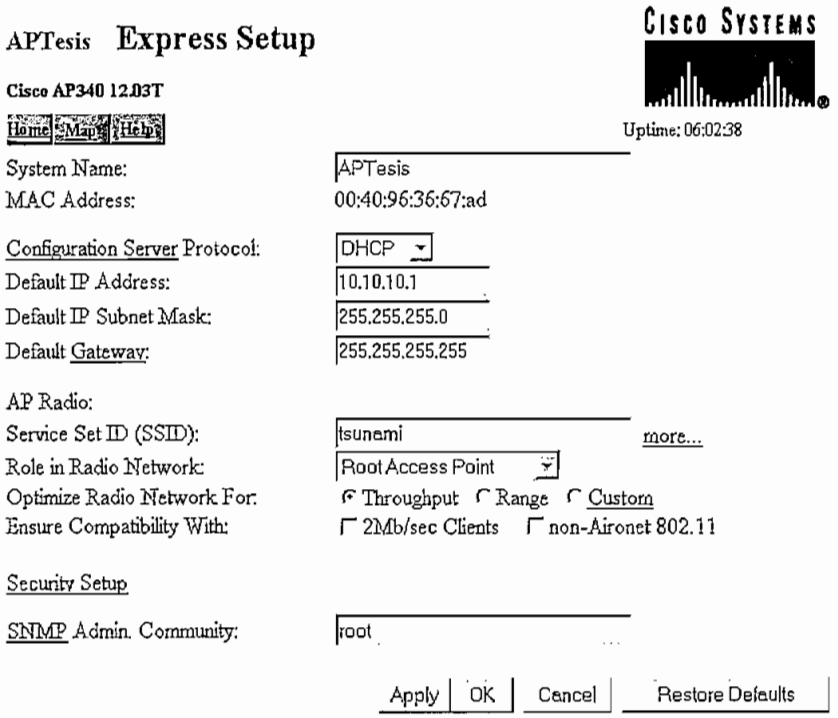


Fig. 3.13 Express Setup

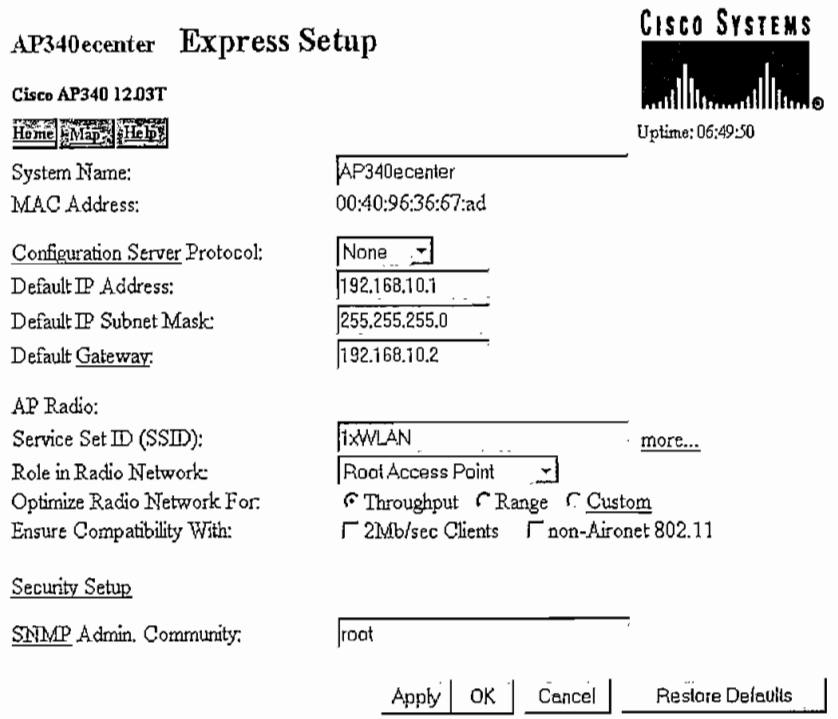


Fig 3.14 Express Setup modificado

3.4.2. ACTUALIZACIÓN DEL *FIRMWARE* DEL AP 340 CISCO

La actualización del *firmware* es importante debido a que se corrigen posibles agujeros de seguridad de versiones anteriores y además se añade nuevas funcionalidades al equipo. La última versión de *firmware* disponible para este equipo se la puede descargar del siguiente enlace del fabricante http://www.cisco.com/public/sw-center/sw-wireless.shtml. La versión más reciente de *firmware* es la 12.04.

La versión actual del AP se puede visualizar en la parte superior izquierda de la pantalla de configuración, en este caso la versión es la 12.03, tal como lo indica la figura 3.15.

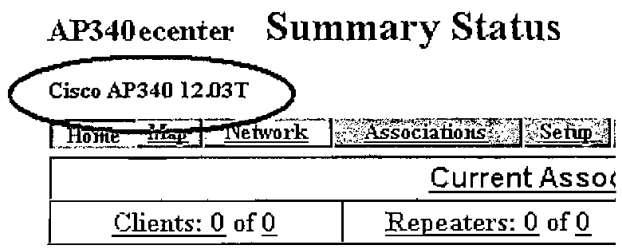


Fig. 3.15 Versión del Firmware del AP 340 Aironet CISCO

Cisco provee un utilitario para la actualización del *firmware* al cual se accede ingresando a *Setup -> Cisco Services -> Through Browser,* luego de lo cual se despliega la pantalla mostrada en la figura 3.16.

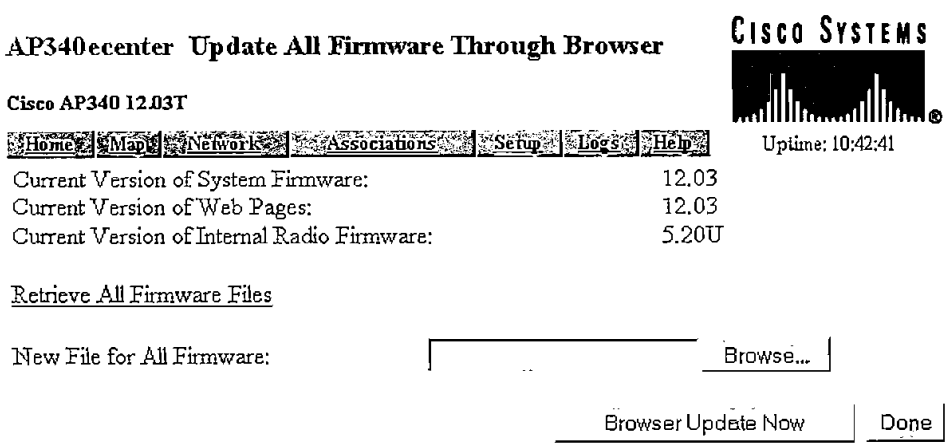


Fig. 3.16 Actualización de Firmware del AP 340 Aironet CISCO

Mediante la opción *Browse* se ubica el archivo con extensión .img que contiene el *firmware* actualizado y se da un clic en *Browser Update Now.* Este proceso se indica en la figura 3.17.

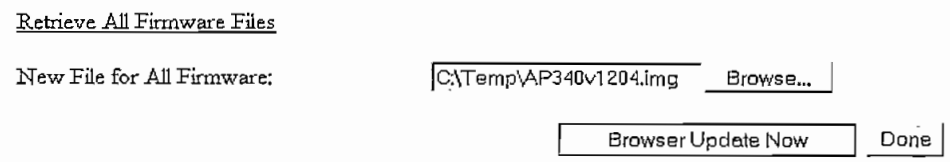


Fig. 3.17 Actualización de Firmware del AP 340 Aironet CISCO

Una vez finalizado el proceso, el AP reinicia con el nuevo *firmware* mostrando la pantalla *Home* de la figura 3.18.

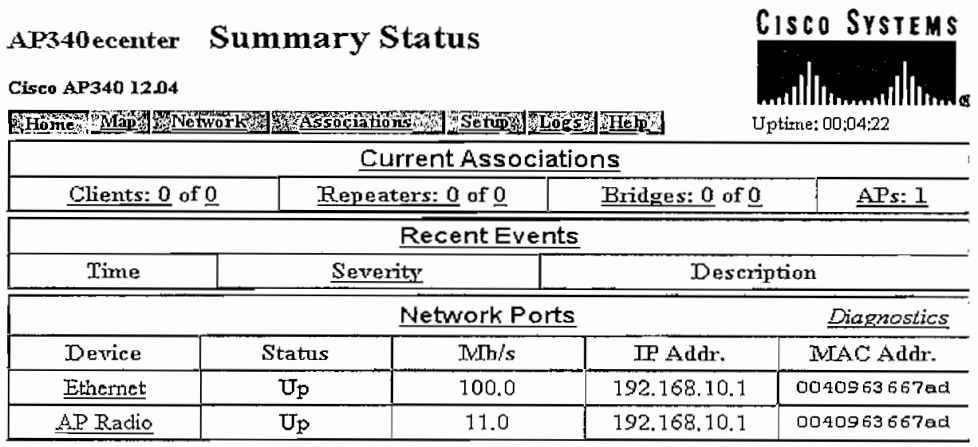


Fig. 3.18 Actualización de Firmware del AP 340 Aironet CISCO

Debe notarse que en la parte superior izquierda aparece 12.04 en lugar del 12.03 anterior. Una ventaja de la actualización del *firmware* es que no afecta la configuración del AP.

3.4.3. CONFIGURACIÓN DE MEDIDAS DE SEGURIDAD GENERALES EN EL AP340 CISCO

Se tiene que aplicar medidas de seguridad adicionales al mecanismo de autenticación, encripción e integridad que se está utilizando, estas medidas incluyen por ejemplo, restringir la configuración del AP solo para el *administrador*,

eliminar el *broadcast* del SSID, configurar filtros MAC, etc. A continuación se presenta la configuración de estas políticas de seguridad en el AP.

3.4.3.1. Creación de Usuarios para Acceso Restringido al AP

Cualquier persona puede ingresar vía consola al AP y realizar cambios, además, si se conoce la dirección IP del AP, también se puede acceder de forma remota vía Web y mediante Telnet. Para evitar esto se puede configurar usuarios con diferentes niveles de acceso al AP. Cada usuario tendrá su respectivo *password* para acceder mediante consola, Telnet y vía Web. Para crear usuarios se ingresa desde la página *Home* a *Setup -> Security -> User Information,* en la pantalla mostrada en la figura 3.19.

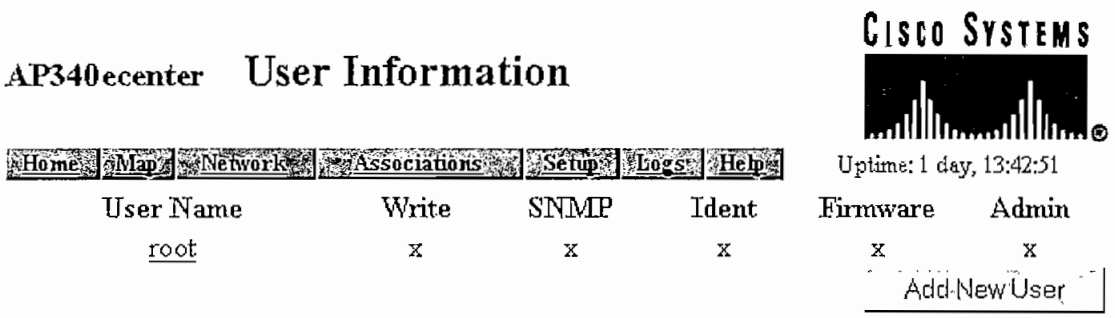


Fig. 3.19 Administración de Usuarios

El usuario predeterminado es *root* que tiene todos los permisos de configuración, estos permisos se pueden modificar dando un clic sobre el nombre del usuario en la pantalla mostrada en la figura 3.20.

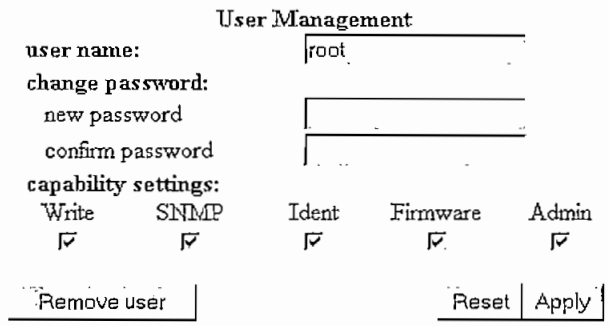


Fig. 3.20 Pantalla de configuración de Usuario

Este usuario no tiene definido un *password* por lo que se debe configurar uno, se llenan los dos espacios correspondientes con el *password* seleccionado y se aplican los cambios con *Apply.*

Ahora se debe añadir un usuario que solamente pueda ver la información del AP esto para fines administrativos, como por ejemplo ver estaciones asociadas, *logs*, etc. Se ingresa desde el *Home* a *Setup -> Security -> User Information -> Add New User,* a la pantalla de la figura 3.21, y en ella se habilita la opción admin tal como lo muestra la figura 3.22.

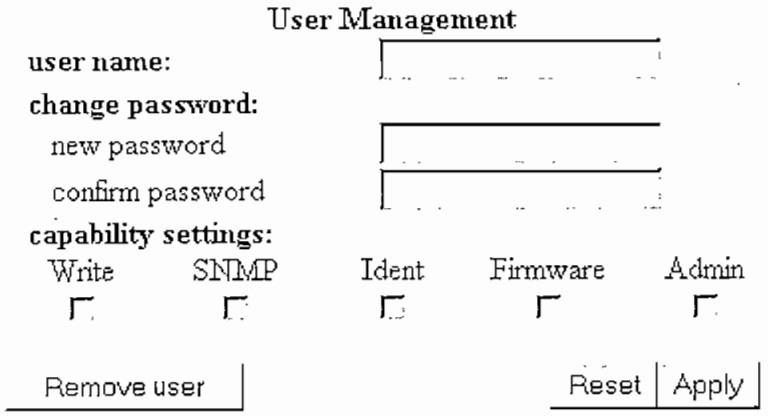


Fig. 3.21 Creación de un nuevo usuario

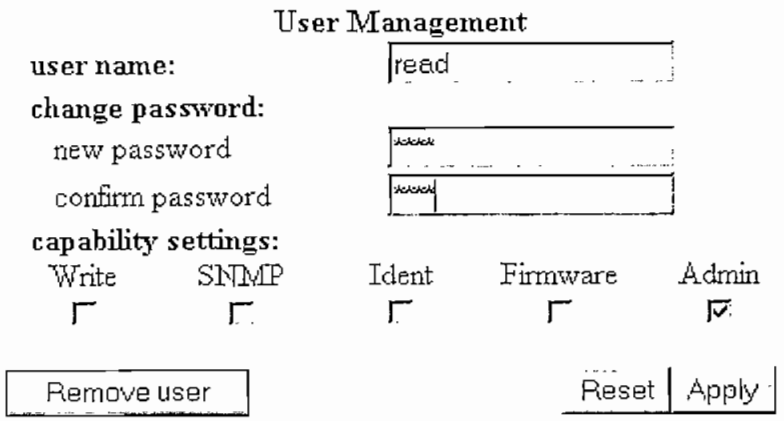


Fig. 3.22 Creación de un usuario con permisos de lectura

Una vez que se tienen creados los respectivos usuarios, se debe aplicar la política de acceso restringido, esto se realiza en la opción *Setup -> Security -> User Manager,* en la pantalla de la figura 3.23.

Fig. 3.23 Pantalla User Manager Setup sin acceso restringido

Para que se aplique la política de usuarios la opción *User Manager* debe estar en *enable*. La opción *Allow Read-Only Browsing without Login?* Se refiere a otorgar acceso de lectura sin necesidad de hacer *login*, ésta debe estar deshabilitada.

Finalmente la opción *Protect Legal Credit Page?* debe estar en *Yes* para protección de la página de créditos legales. Con esta configuración se tiene la pantalla de la figura 3.24.

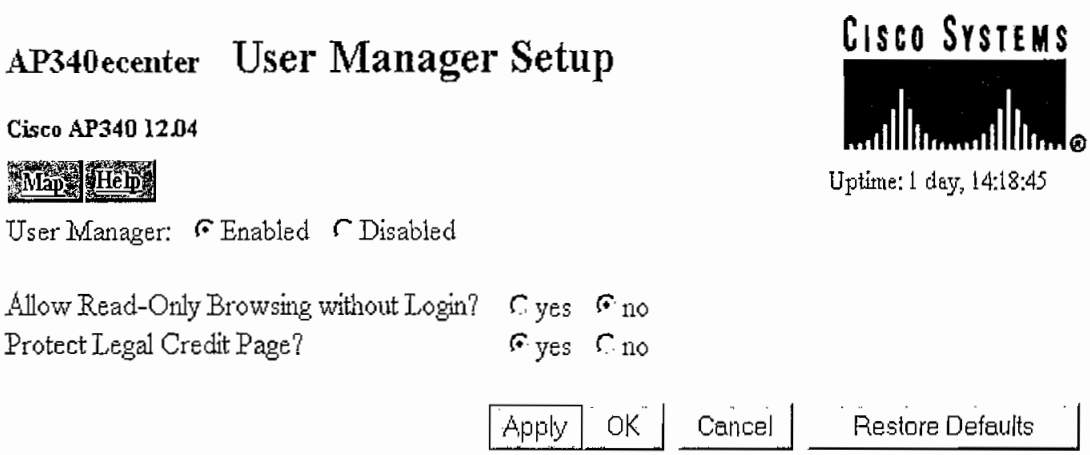


Fig. 3.24 Pantalla User Manager Setup con acceso restringido

Con esto termina la configuración de acceso restringido al AP.

3.4.3.2. Deshabilitación de SNMP y Telnet en el AP

Otra forma de obtener Acceso al AP y alterar su configuración es mediante SNMP y Telnet. Para asegurarse que la única forma de configurar el AP es vía Web, las opciones de SNMP y Telnet deben ser deshabilitadas.

Para deshabilitar SNMP se debe ingresar desde el *Home* a *Setup -> SNMP*, donde aparece la pantalla de la figura 3.25.

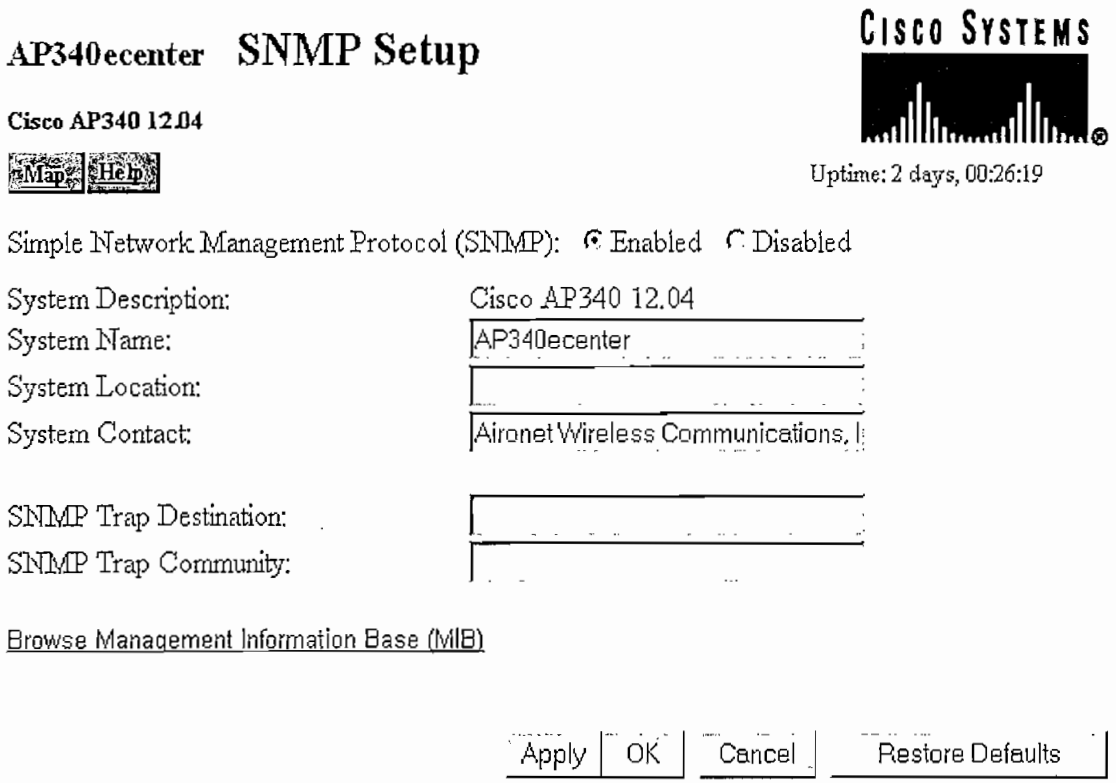


Fig. 3.25 Configuración de SNMP

Como se puede apreciar por defecto SNMP está habilitado, por lo cual se debe deshabilitar seleccionando *Disabled* en la opción *Simple Network Management Protocol (SNMP)* y aplicando el cambio con *Apply*.

La opción de Telnet se debe deshabilitar desde el *Home* ingresando a *Setup* -> *Console/Telnet*. Donde se despliega la pantalla de la figura 3.26.

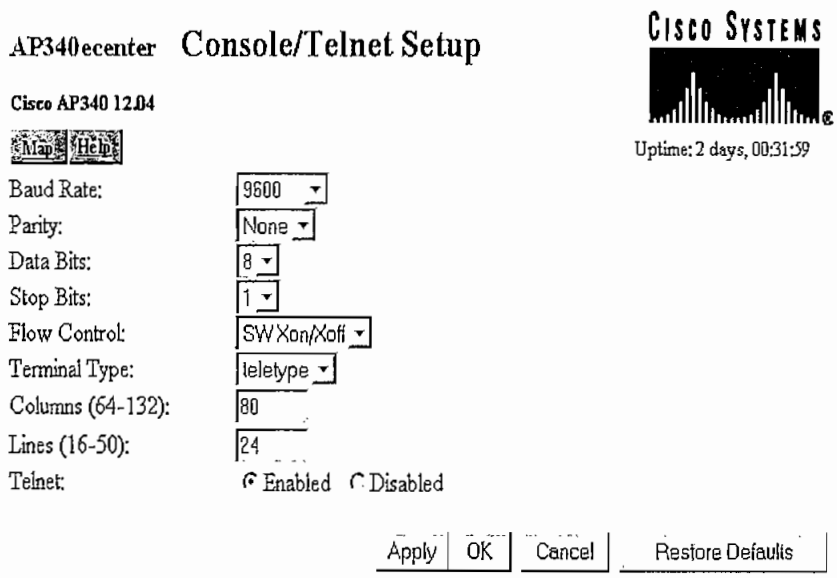


Fig. 3.26 Configuración de Telnet

En la última opción Telnet se debe elegir *Disabled* y aplicar los cambios con *Apply*.

3.4.3.3. Eliminación del *Broadcast* del SSID

El *broadcast* del SSID es una invitación para que usuarios extraños se asocien a la red, por ello se recomienda deshabilitar esta opción. Para esto se debe ingresar a la opción *Setup* y luego en la fila de *AP Radio* a *Hardware*, con lo que se presenta la pantalla de la figura 3.27. Por defecto el *broadcast* del SSID está habilitado, se debe elegir *No* y aplicar los cambios con *Apply*.

3.4.3.4. Filtrado en el AP 340 CISCO

Como se mencionó en el capítulo anterior, se pueden establecer 3 tipos de filtrado en el AP. El primero es el filtrado del SSID que ya está configurado. El segundo es el filtrado de MAC y el tercero es el filtrado de protocolos.

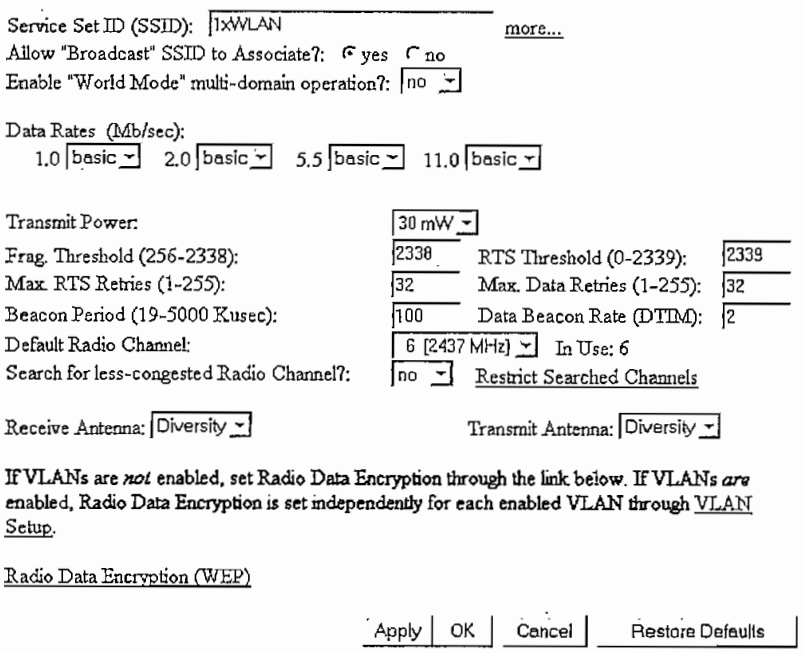


Fig. 3.27 Broadcast del SSID

a) Configuración de Filtrado de Protocolos en el AP 340 CISCO

Los clientes necesitan que todas las aplicaciones que corren en una red cableada, también funcionen en la WLAN, por ello no se aplica ningún filtro. Sin embargo éstos pueden añadirse ingresando a través de *Setup -> Protocol Filters*, a la pantalla de la figura 3.28. Luego se debe seleccionar *IP Protocol Filters* y aparece la pantalla de configuración de filtros mostrada en la figura 3.29. El filtro para VoIP viene predeterminado como ejemplo.

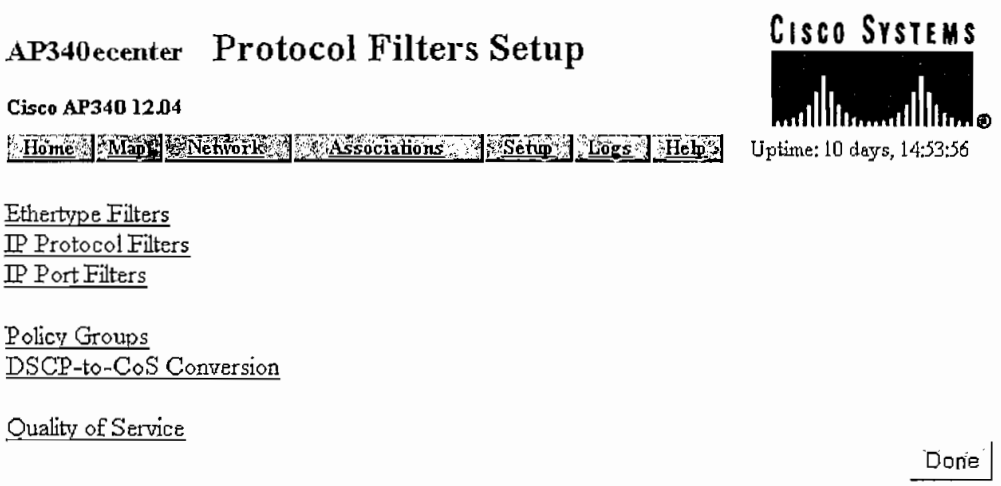


Fig. 3.28 Pantalla principal de configuración de Filtros

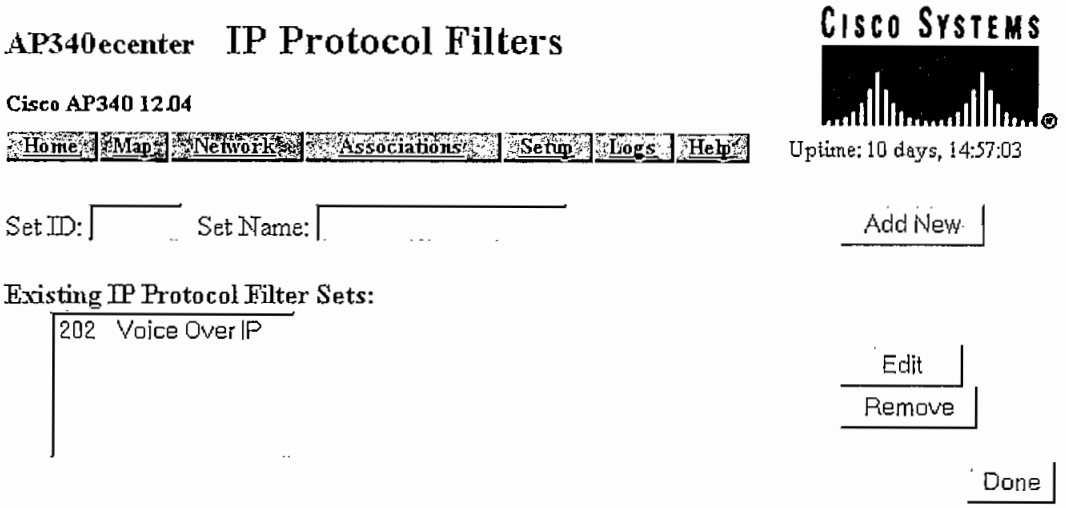


Fig. 3.29 Configuración de Filtros IP

b) Configuración de Filtrado MAC en el AP 340 CISCO

Para la configuración del filtrado MAC en el AP se debe ingresar a *Setup* -> *Address Filters*, luego de lo cual aparece la pantalla de la figura 3.30.

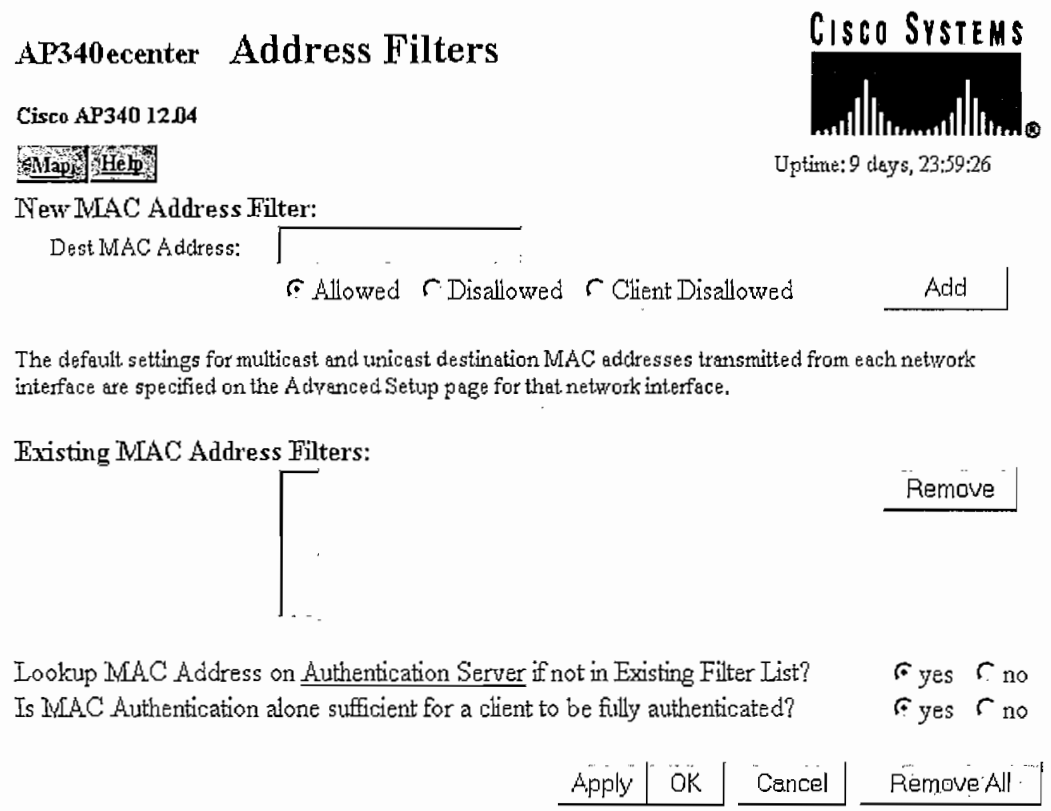


Fig. 3.30 Pantalla de configuración de Filtros MAC

En el campo *Dest MAC Address Filter* se ingresan las direcciones MAC de las tarjetas de los usuarios inalámbricos, con la opción *Allowed* y luego se presiona *Add.* Como el filtro se aplica directamente en el AP la opción *Lookup MAC Address on Authentication Server if non Existing Filter List?,* debe estar en *No.*

Además la autenticación por MAC autorizada no es suficiente por lo que la opción *Is MAC Authentication alone sufficient for a client to be fully authenticated?* también debe estar en no.

Realizados estos cambios la pantalla final se muestra en la figura 3.31. Luego se ingresa a la opción *Setup -> Service Sets*, donde aparece la pantalla de la figura 3.32. Aquí se selecciona el SSID de la red y se ingresa a la opción *Edit.*

Luego, debajo del tipo de autenticación que se esté utilizando *Open, Shared o EAP Network)* en la opción *Default Unicast Address Filter* se debe seleccionar *Disallowed*, tal como se indica en la figura 3.33 para el caso de autenticación *Open*; se aplican los cambios y está configurado el filtro MAC en la WLAN.

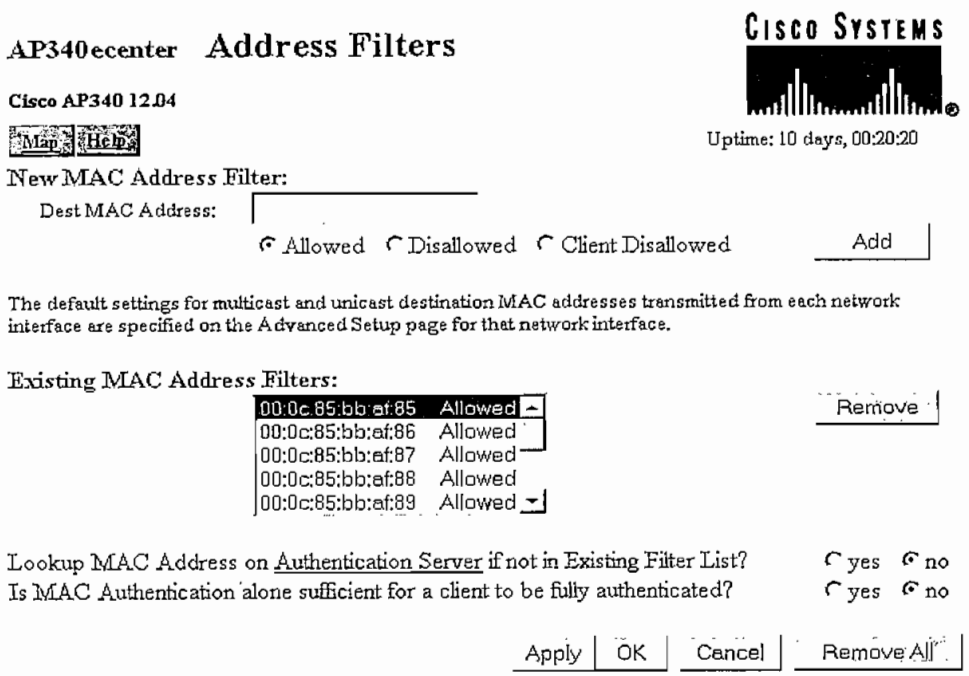


Fig. 3.31 Configuración de usuarios MAC autorizados

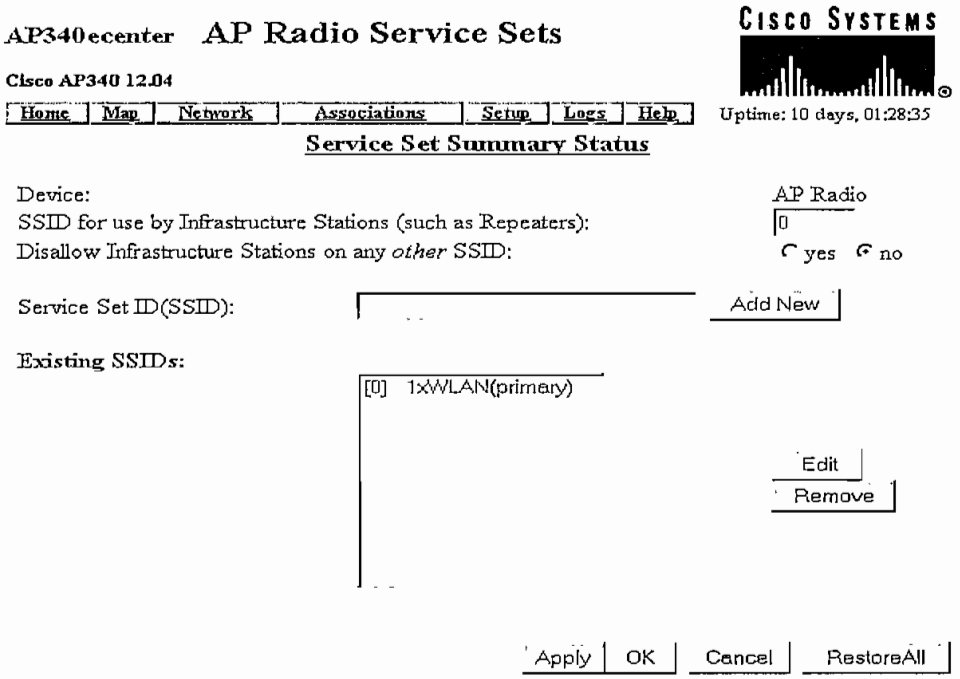


Fig. 3.32 Configuración de Específica por SSID del filtro

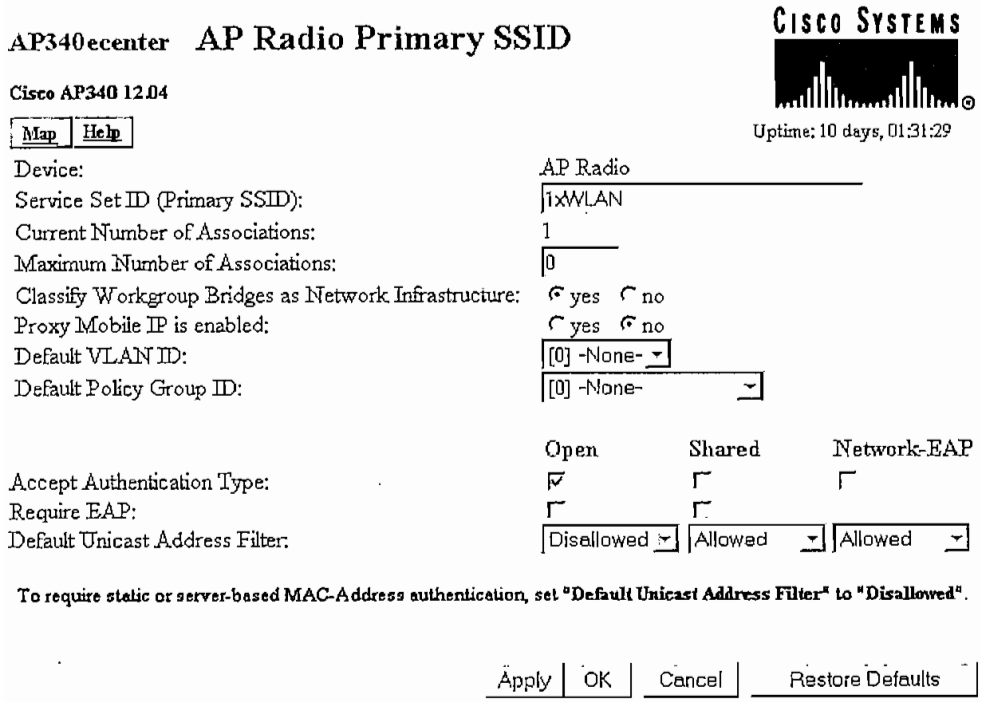


Fig. 3.33 Aplicación del filtro MAC para el tipo de autenticación

3.4.4. CONFIGURACIÓN WEP EN EL AP 340 CISCO

Una vez configurados todos los parámetros para el funcionamiento de la WLAN y las herramientas de seguridad adicionales, es momento de iniciar el desarrollo de la implementación de WEP como mecanismo de seguridad para la WLAN.

Para acceder a la utilidad de configuración WEP se debe ingresar a *Setup -> Security -> Radio Data Encryption (WEP)*, luego de lo cual aparece la pantalla de la figura 3.34.

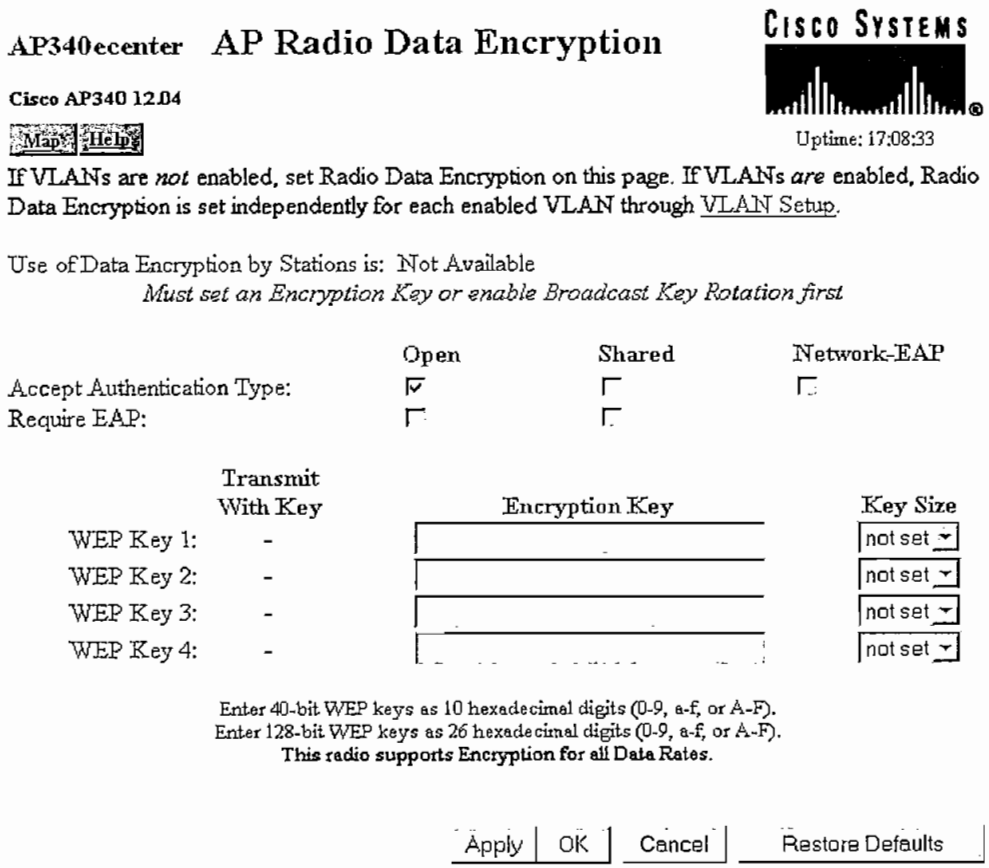


Fig. 3.34 Configuración WEP del AP 340 Aironet CISCO

Como se puede apreciar en la figura 3.34, la seguridad WEP viene deshabilitada de fábrica, por lo que cualquier usuario inalámbrico que conozca el SSID y robe un MAC autorizada podrá obtener acceso a la red, además, los datos de los usuarios no viajan encriptados y pueden ser interceptados fácilmente.

Para la configuración de WEP primero se deben generar 4 claves de 128 bits (se prefiere el uso de 128 bits al uso de claves de 40 bits) que equivalen a 26 números hexadecimales, y colocarlas en los respectivos espacios de *Encryption Key*, luego en los campos de *Key Size* para cada clave se debe elegir la longitud de 128 bits.

Las claves generadas deben ser aleatorias y no deben tener patrones característicos o fáciles de recordar. En la tabla 3.4 se muestran las claves seleccionadas que cumplen con estas condiciones.

Número de clave	Clave
Clave 1	7A8C6F91B549D7E37BA2F4D6AB
Clave 2	415778C6C6A5F91CBDC6FBBAFC
Clave 3	AB45DC87BD654CBDFC6CF91BA1
Clave 4	C548DA6F1B5C6A7D4C527B14FC

Tabla 3.4 Claves WEP seleccionadas

Luego en el parámetro *Accept Authentication Type* se tienen 3 opciones

- ***Open.***- El usuario requiere autenticarse con el método *Open,* para conectarse a la WLAN.
- ***Shared.***- El usuario requiere autenticación *Shared*, para conectarse a la WLAN.
- ***Network* – EAP.**- El usuario requiere autenticación EAP, para conectarse a la WLAN.

Por supuesto, de lo concluido en el capítulo 2, se debe seleccionar solo la opción *Open,* pues *Shared* implica mayor riesgo por la posibilidad de tener el texto plano y el texto encriptado del *challenge*, y en cambio la autenticación *Network–EAP* no está disponible en la solución.

Luego de configurados estos parámetros, la pantalla del utilitario queda como la que se muestra en la figura 3.35. Se aplican los cambios con *Apply*.

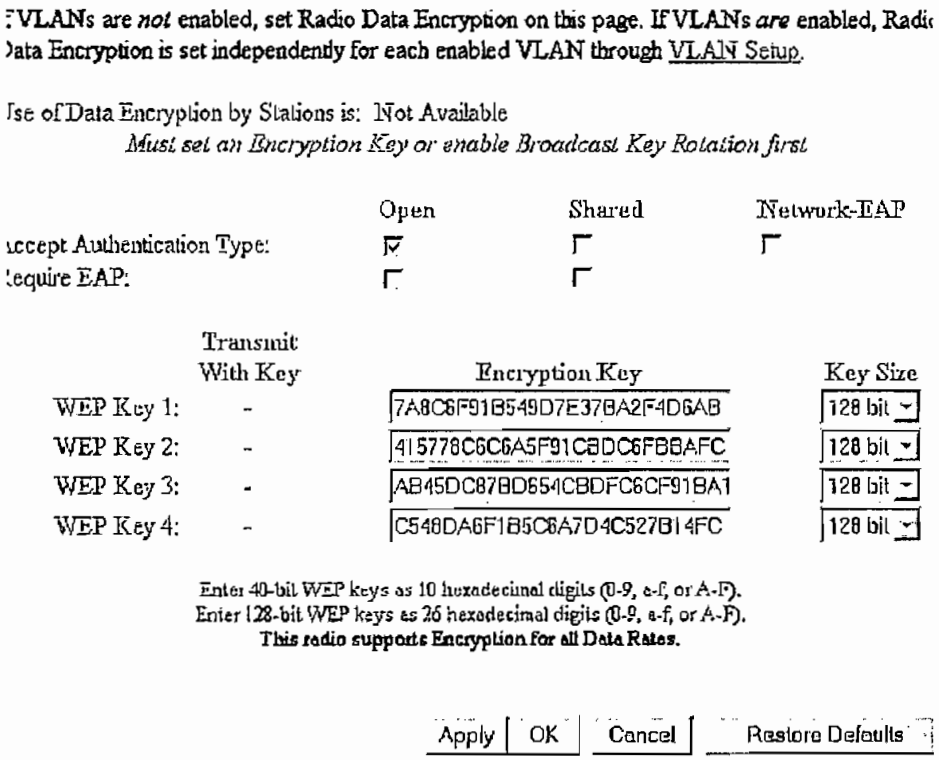


Fig. 3.35 Configuración WEP del AP 340 Aironet CISCO

Como resultado de estos cambios la pantalla aparece con una nueva opción, *Use of Data Encryption by Stations is,* como se muestra en la figura 3.36. Esta opción tiene las siguientes elecciones:

- *No Encryption.*- Los datos de los clientes no serán encriptados antes de su transmisión.
- *Full Encryption.*- Los datos de los clientes sí serán encriptados antes de su transmisión.
- *Optional.*- El cliente puede elegir si encriptar o no sus datos.

La opción a elegir es *Full Encryption* para que todos los datos sean encriptados obligatoriamente. Incluso si un cliente conoce la clave pero no está configurado para encriptar sus datos, el AP no le otorgará el acceso a la WLAN.

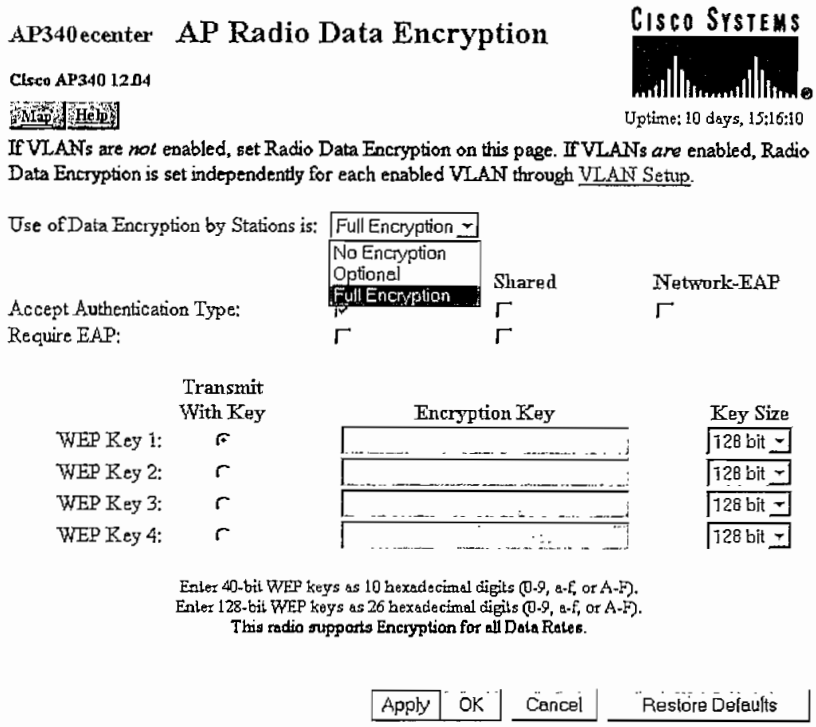


Fig. 3.36 Configuración WEP del AP 340 Aironet CISCO

Además aparece un campo *Transmit With Key*, que sirve para elegir una de las 4 claves para la encripción y autenticación. Se elige la clave 1. Finalmente se aplican los cambios y la pantalla final que se muestra es la de la figura 3.37. Además nótese que las claves ya no son visibles por seguridad.

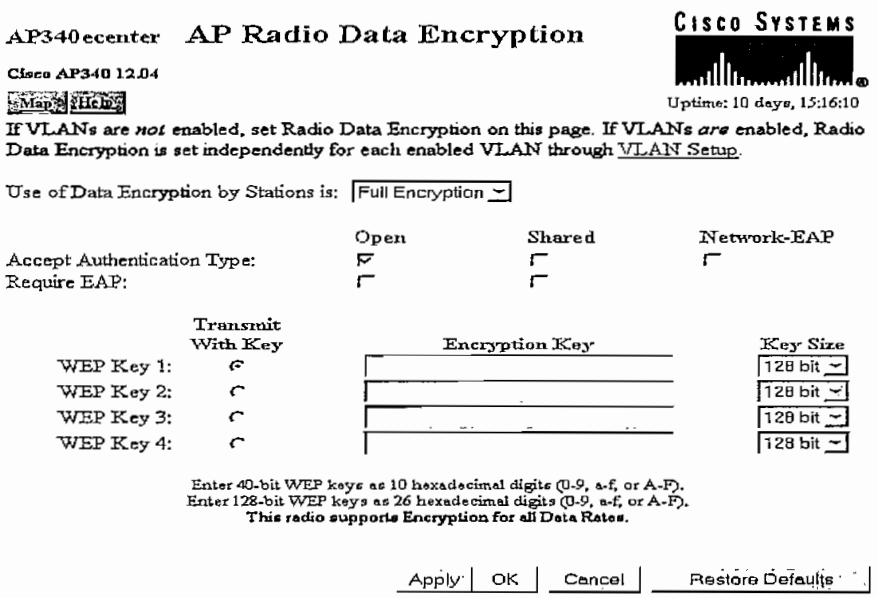


Fig. 3.37 Pantalla final de configuración WEP

Ahora que se tiene configurado el WEP básico, se deben añadir las propiedades de MIC y TKIP (las mejoras de WPA para WEP) para que el sistema sea seguro. Sin estas herramientas adicionales, WEP presenta las debilidades ya mencionadas en el capítulo 2 como IV demasiado corto, clave estática, etc., y no podría ser utilizado como mecanismo de seguridad confiable.

Para habilitar ambas opciones se debe ingresar a *Setup* y luego en las opciones de *AP Radio* en *Advance*, luego de lo cual, aparece la pantalla de la figura 3.38.

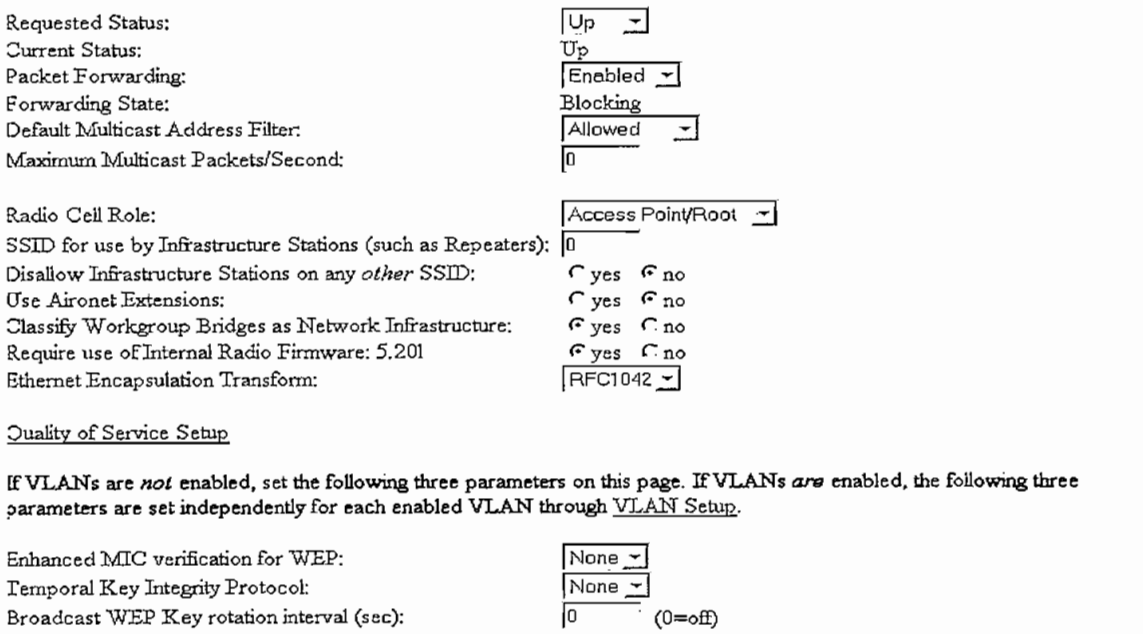


Fig. 3.38 Pantalla de configuración de seguridad adicional a WEP

Para poder habilitar las opciones de TKIP y MIC en el AP, primero se debe habilitar la opción *Use Aironet Extensions,* que le permite al AP manejar estas funcionalidades adicionales. Luego las opciones de *Enhanced MIC verification for WEP* y *Temporal Key Integrity Protocol:* deben estar en MMH y Cisco respectivamente, de acuerdo a la nomenclatura que utiliza Cisco. La pantalla final se muestra en la figura 3.39.

Con esto termina la configuración del AP, ahora los clientes deben tener la clave secreta 1 y una correcta configuración WEP para poder acceder a la WLAN.

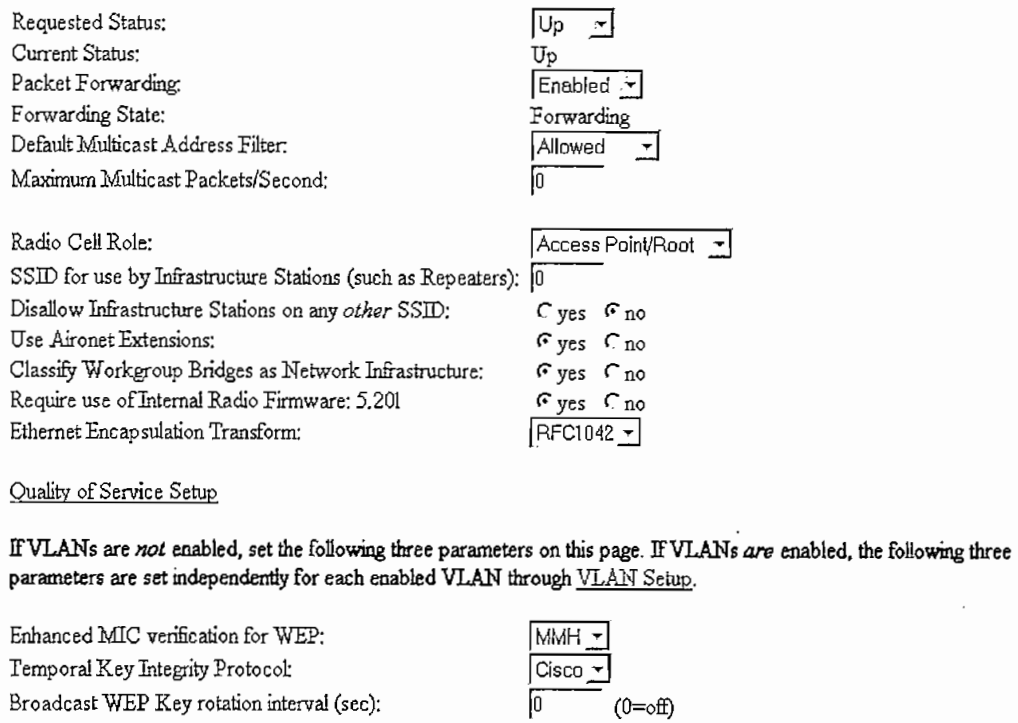


Fig. 3.39 Configuración MIC y TKIP

3.5. CONFIGURACIÓN DEL USUARIO CON TARJETA PCMCIA AIRONET 350 CISCO

3.5.1. INSTALACIÓN DE LA TARJETA INALÁMBRICA

La instalación de la tarjeta 350 *Aironet* en Windows XP, que es el caso común de sistema operativo en portátiles, es sencilla y rápida; simplemente se debe insertar la tarjeta en la ranura PCMCIA y el sistema operativo corre un programa de instalación automático en el cual sólo se debe especificar la ubicación del *driver* adecuado.

El *driver* actualizado para la tarjeta se puede descargar del siguiente enlace del fabricante: http://www.cisco.com/public/sw-center/sw-wireless.shtml.

3.5.2. INSTALACIÓN DEL SOFTWARE PARA EL CLIENTE INALÁMBRICO

Una vez que está instalado el hardware, es momento del software. Cisco ofrece el *ACU Aironet Client Utility*, que es el software del fabricante para manejar la configuración inalámbrica del cliente y su conectividad en la WLAN.
El ACU tiene las funcionalidades y ventajas siguientes:

- Manejo gráfico de la configuración de la WLAN.
- Provee herramientas de monitoreo de la calidad del enlace inalámbrico.
- Provee mecanismos de pruebas del enlace.
- Administración de varios perfiles de usuario para diferentes tipos de WLAN´s.
- Soporte a varios tipos de autenticación, como WEP, LEAP, EAP, etc.

El ACU más actualizado para el cliente inalámbrico se puede descargar del siguiente enlace del fabricante: http://www.cisco.com/public/sw-center/sw-wireless.shtml. En este caso es la versión V 5.05. En el Anexo 3 se presenta un manual de instalación del ACU V 5.05.

3.5.3. ACTUALIZACIÓN DEL FIRMWARE

Es el primer paso para la correcta configuración del cliente inalámbrico. La actualización del *firmware* provee de nuevas funcionalidades a la tarjeta inalámbrica y cubre agujeros de seguridad de versiones anteriores. La última versión de *firmware* para las tarjetas 350 Aironet se puede descargar del siguiente enlace del fabricante: http://www.cisco.com/public/sw-center/sw-wireless.shtml.

La versión más reciente es la 45c42530. Para proceder con la actualización se debe ingresar a la opción *Load Firmware*, desde la pantalla principal del ACU, como se indica en la figura 3.40.

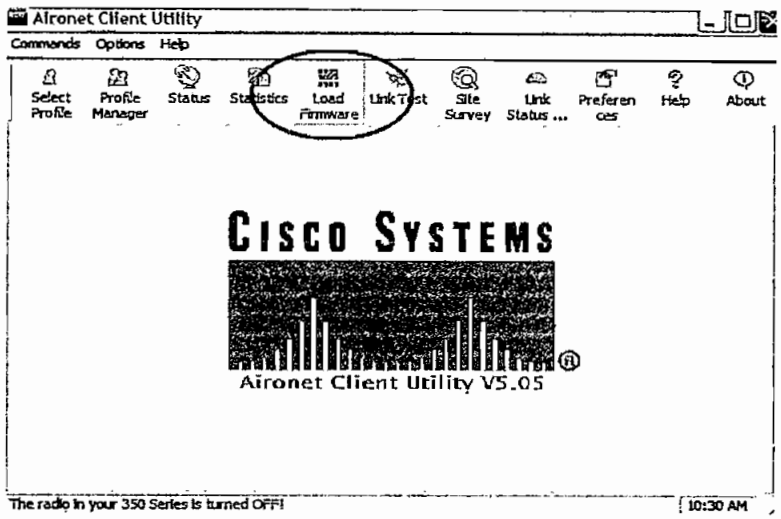


Fig. 3.40 Pantalla principal del ACU

Se ubica el archivo 45c42530.img y se lo carga, tal como lo muestra la figura 3.41.

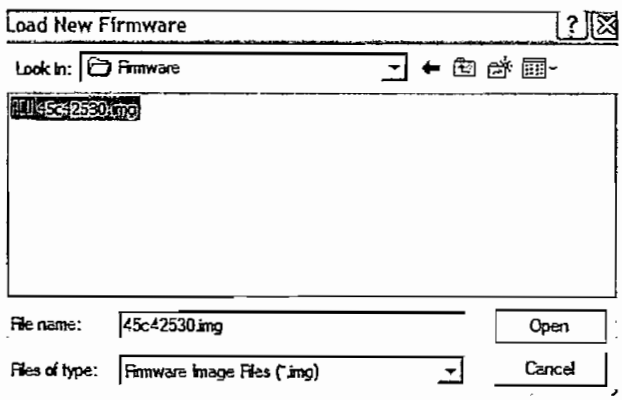


Fig. 3.41 Pantalla para cargar el firmware de la tarjeta

3.5.4. CONFIGURACIÓN DEL ACU PARA SEGURIDAD WEP

Ahora se tiene todo listo para iniciar la configuración de la WLAN y de su seguridad en el ACU. EL software de Cisco permite manejar perfiles de conectividad para aplicarse en diferentes ambientes inalámbricos, además se tiene la ventaja de que estos perfiles son exportables e importarles, es decir que basta con configurar un cliente de la WLAN completamente y luego exportar ese perfil para importarlo en el resto de usuarios inalámbricos, así ya no es necesario realizar nuevamente el proceso de configuración.

Para crear un perfil se ingresa a la opción *Profile Manager* en la pantalla principal del ACU. Aparece la pantalla de la figura 3.42.

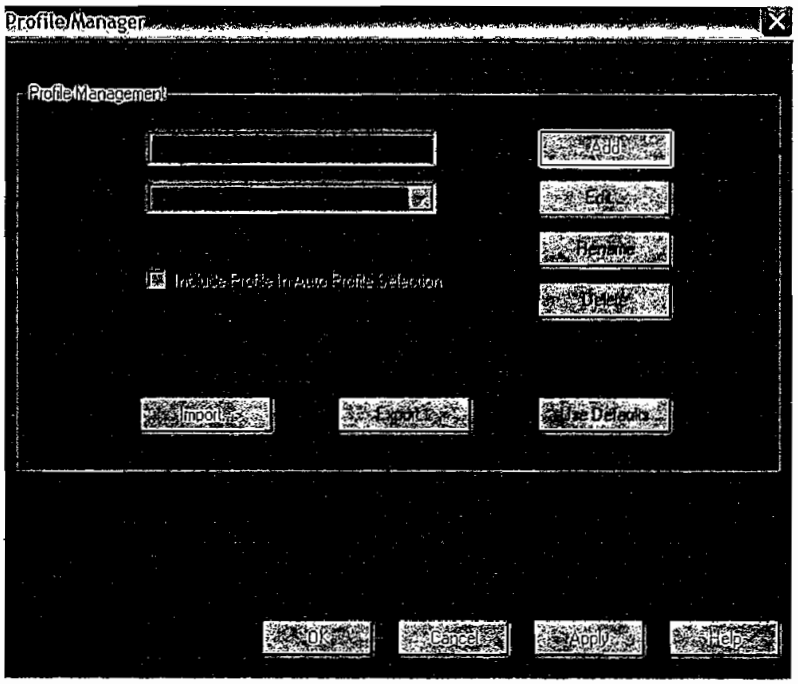


Fig. 3.42 Pantalla de Administración de Perfiles

Se da un clic en *Add* y se asigna un nombre al perfil, en este caso "usuarioWLAN", se da clic en *OK* para ingresar al perfil. Aparece la pantalla de la figura 3.43.

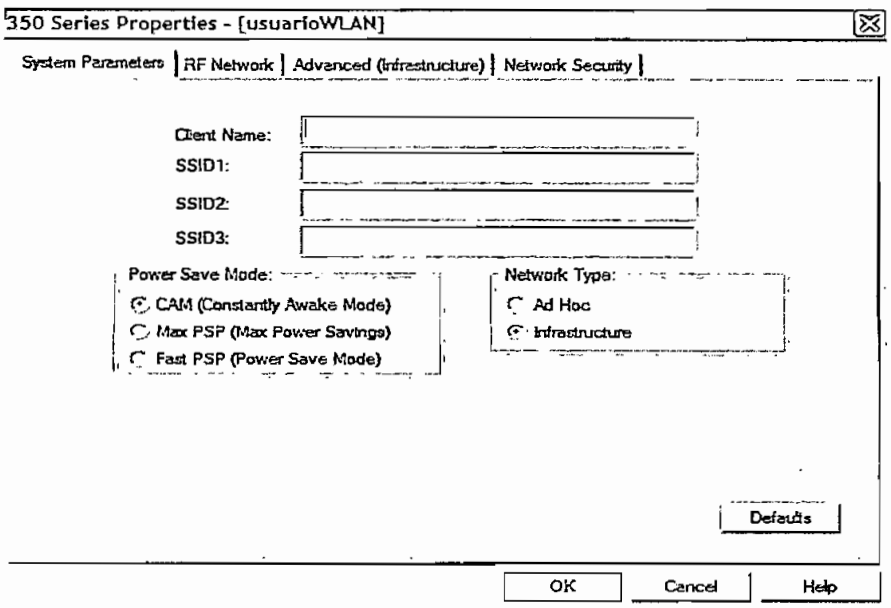


Fig. 3.43 Pantalla de System Parameters

En estas opciones, de la pestaña *System Parameters* se asigna un nombre al cliente, por ejemplo usuario1, luego se configura el SSID que es 1xWLAN, los demás son parámetros por defecto para el tipo de red. También se elige una WLAN de infraestructura y manejo de la energía tipo CAM (*Constantly Awake Mode*) que indica que las estaciones serán advertidas de eventos en la WLAN, el resultado final se muestra en la figura 3.44.

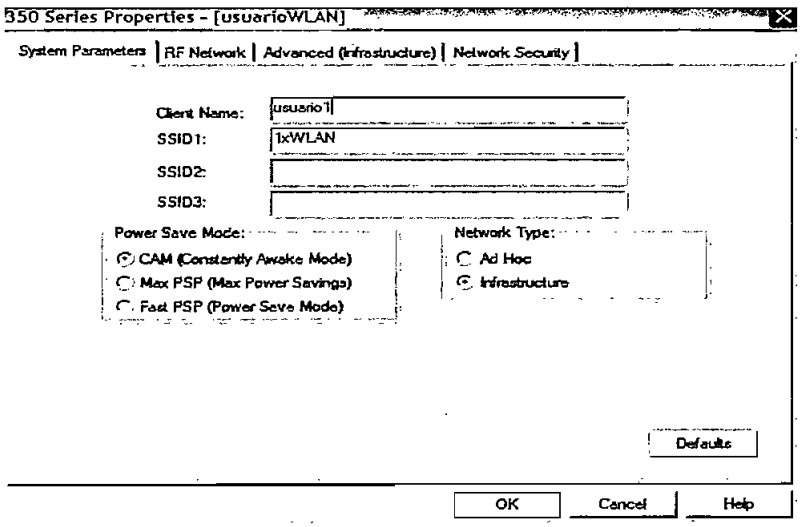


Fig. 3.44 Pantalla de System Parameters final

Ahora se debe seleccionar la pestaña de *Network Security* con lo que aparece la pantalla de la figura 3.45. Aquí se configura la seguridad WEP.

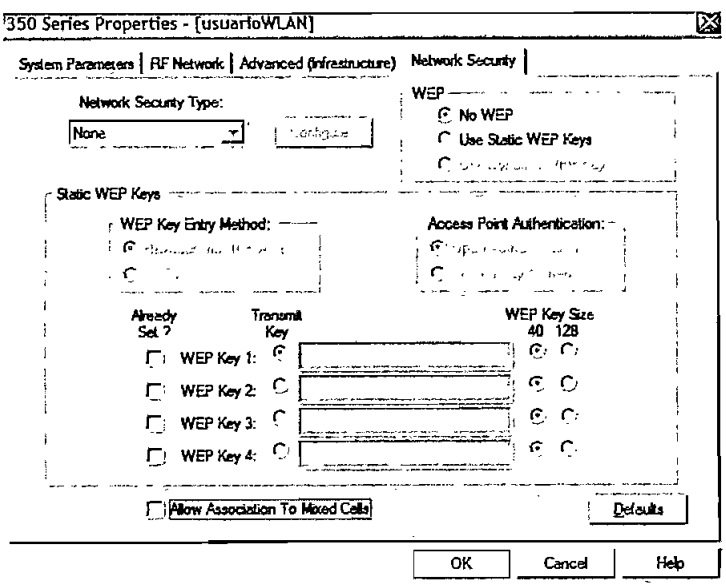


Fig. 3.45 Pantalla de Network Security

En las opciones WEP se debe elegir *Use Static WEP Keys*, con esto se habilitan los campos correspondientes a *Use Static WEP Keys*. Ahora en la opción *WEP Key Entry Method* se elige *Hexadecimal* para el modo de entrada de la clave y en *Access Point Authentication* el tipo de autenticación *Open*. Las mismas claves del AP de 128 bits deben ser configuradas en el mismo orden, luego se selecciona la primera clave como *Transmit Key*. La pantalla final se muestra en la figura 3.46.

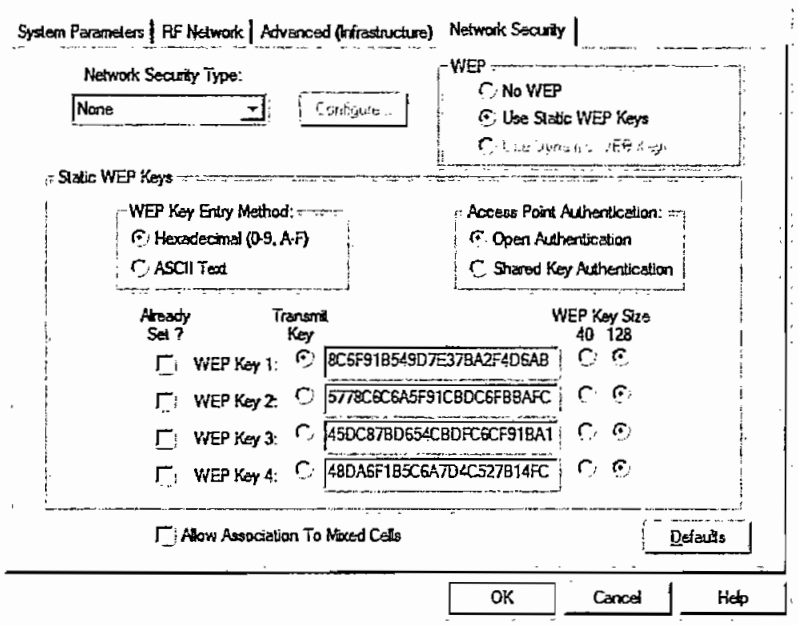


Fig. 3.46 Pantalla de final de Network Security

Se da un clic en *Ok* y se aplican los cambios. Una vez que se tiene el perfil correcto configurado se lo debe aplicar. Para esto se elige la opción *Select Profile* de la pantalla principal, luego de lo cual aparece la pantalla de la figura 3.47.

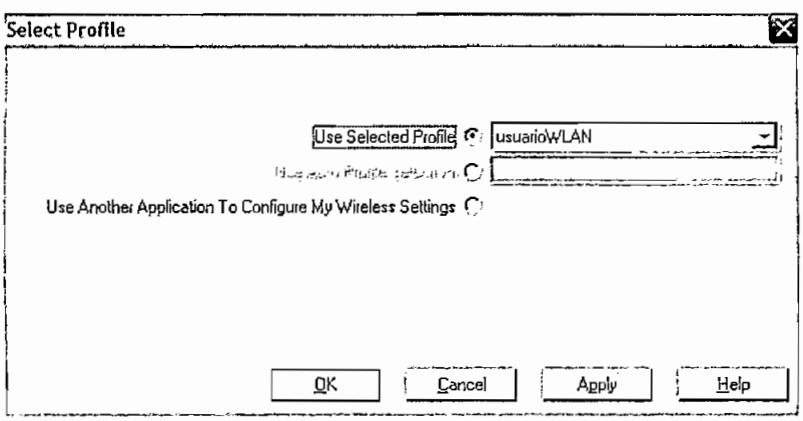


Fig. 3.47 Pantalla Select Profile

Se selecciona el perfil creado y se lo aplica con *Apply*. Una vez hecho esto, el sistema empieza el proceso de autenticación y se asocia a la red. La correcta asociación se puede visualizar en la parte inferior de la pantalla principal como lo indica la figura 3.48.

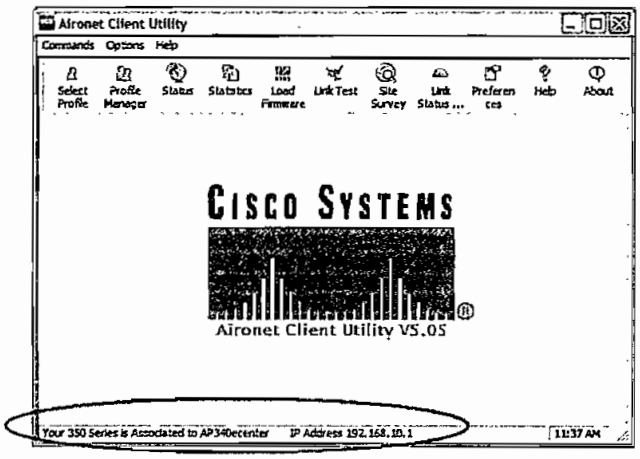


Fig. 3.48 Pantalla principal del ACU con la estación asociada

Se puede apreciar que el usuario está asociado al AP con el nombre AP340ecenter y con dirección IP 192.168.10.1. Con esto termina la configuración del cliente inalámbrico. El siguiente paso es la realización de pruebas de conectividad y de seguridad de la red inalámbrica.

3.6. PRUEBAS DE FUNCIONAMIENTO

Se deben realizar pruebas de funcionamiento para verificar el correcto desempeño de la WLAN y su seguridad. Esto implica que sólo los usuarios autorizados puedan acceder a la WLAN.

3.6.1. PROCESO DE AUTENTICACIÓN NORMAL

Si el cliente está correctamente configurado de acuerdo a la sección anterior, se autenticará sin ningún problema. Por ejemplo se tiene el cliente de pruebas descrito en la tabla 3.5

Parámetros de cliente de pruebas	
Nombre	usuario1
Autenticación	Open - WEP
IP	192.168.10.100
MAC	000c85bbaf85
Default Gateway	192.168.10.2
MAC	000c85bbaf85
Perfil	Correcto
Autenticación	*Open*

Tabla 3.5 Pantalla final de configuración WEP

Para la prueba de autenticación correcta se inserta la tarjeta PCMCIA en la ranura y el proceso empieza automáticamente. Se puede visualizar la correcta asociación a la red en la parte inferior de la pantalla principal del ACU, de igual forma que en la figura 3.48.

Además en las utilidades de red del sistema operativo Windows XP se puede visualizar el estado de la conexión de red mediante la tarjeta inalámbrica, tal como muestra la figura 3.49.

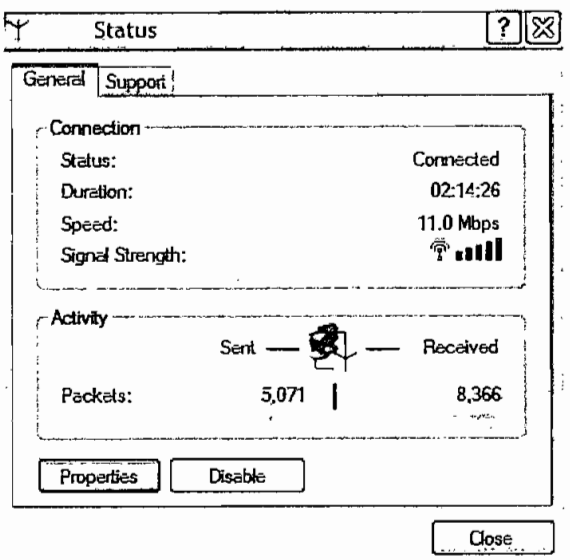


Fig. 3.49 Pantalla de estado de red de Windows XP

Una forma más amigable de verificar la asociación al AP es mediante la opción *Link Status Meter*, donde aparece la pantalla de la figura 3.50

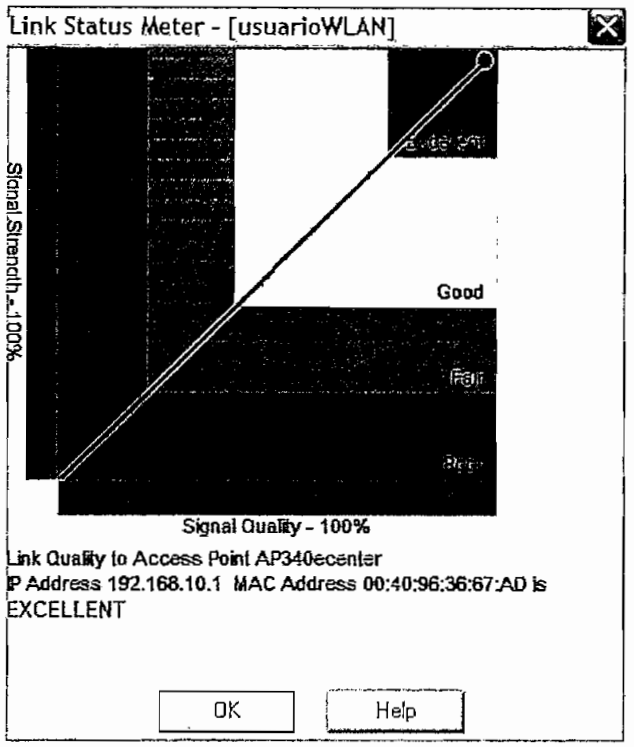


Fig. 3.50 Pantalla Link Status Meter

En esta pantalla se puede visualizar de forma gráfica el estado del enlace al AP, en el eje Y se muestra la potencia de la señal que depende principalmente de la distancia que se tenga con respecto al AP.

En el eje X se muestra en cambio la calidad de la señal que depende de la interferencia existente en el ambiente y del número de usuarios conectados en la red.

En este caso el enlace es excelente debido a que la estación se encuentra cercana al AP y solo existe un usuario conectado. La opción *Status* de la pantalla principal del ACU brinda mayor información sobre el enlace, ésta despliega la pantalla de la figura 3.51.

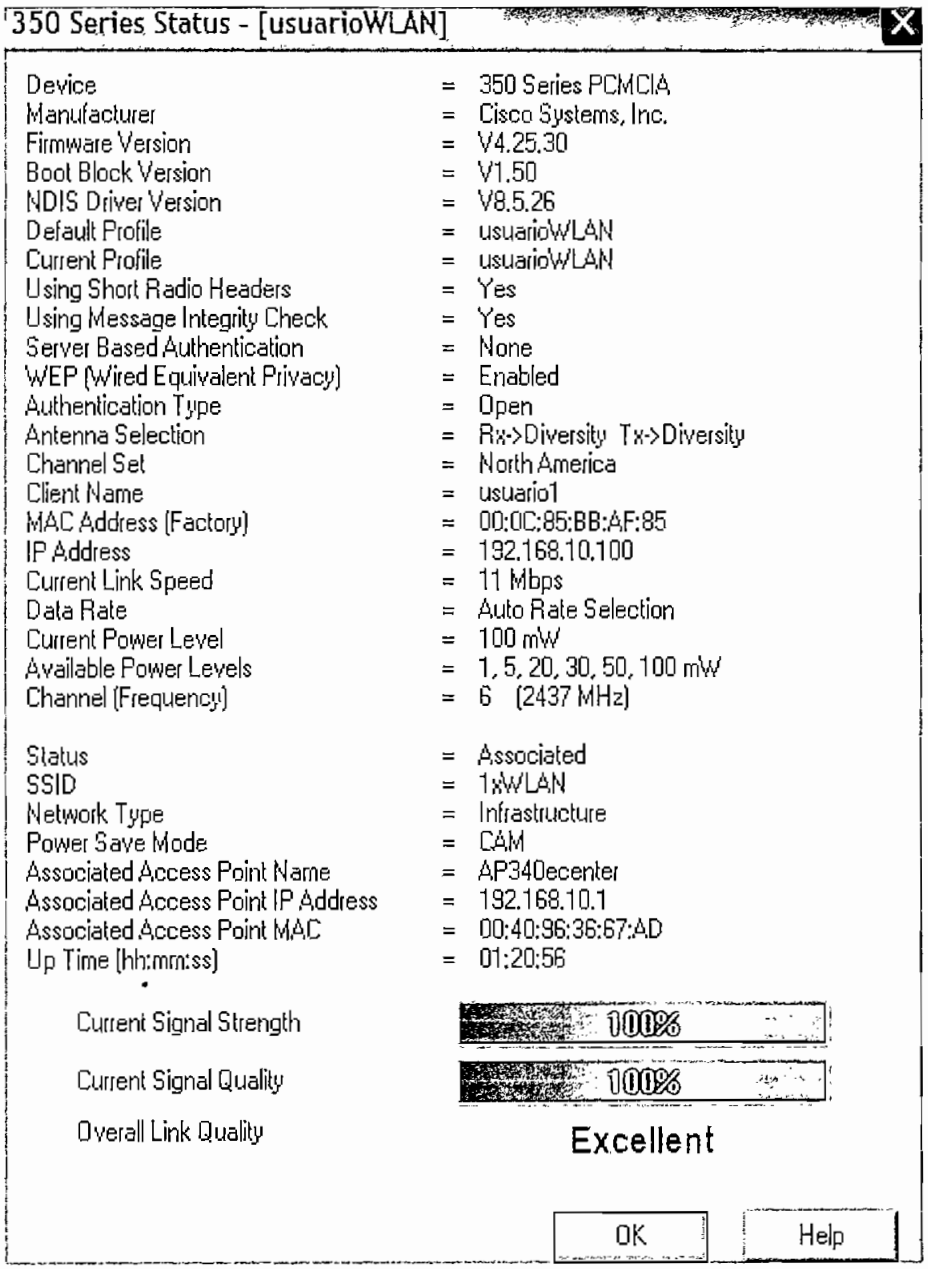


Fig. 3.51 Pantalla Status

Aquí se puede apreciar parámetros importantes como los que se resumen en la tabla 3.6.

Parámetros del Enlace	
Tarjeta inalámbrica	350 PCMCIA
Fabricante	Cisco Systems Inc.
Firmware de la tarjeta	V 4.25.30
Perfil utilizado	usuarioWLAN
Seguridad WEP	*Yes*
Autenticación	*Open*
MAC	000c85bbaf85
IP	192.168.10.100
Velocidad del enlace	*11 Mbps*
Potencia de la señal	*100 mW*
Frecuencia	*Canal 6 (2437 Mhz)*
SSID	*1xWLAN*
Tipo de red	*Infraestructura*
Nombre del AP	*AP340ecenter*
IP del AP	*192.168.10.1*
Mac del AP	*0040963667AD*
Tiempo total de actividad	*1:20:56*

Tabla 3.6 Parámetros del enlace obtenidos de la opción Status

En el AP también aparece el usuario asociado correctamente, tal como se muestra en la pantalla del *Home* en la figura 3.52.

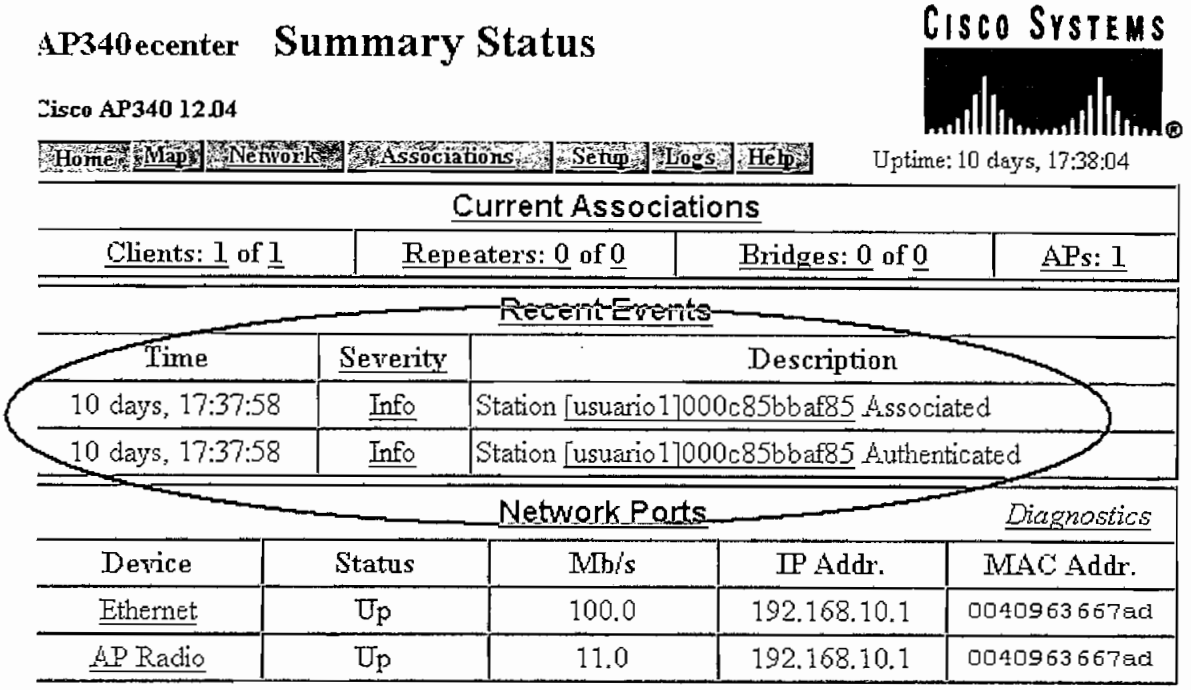
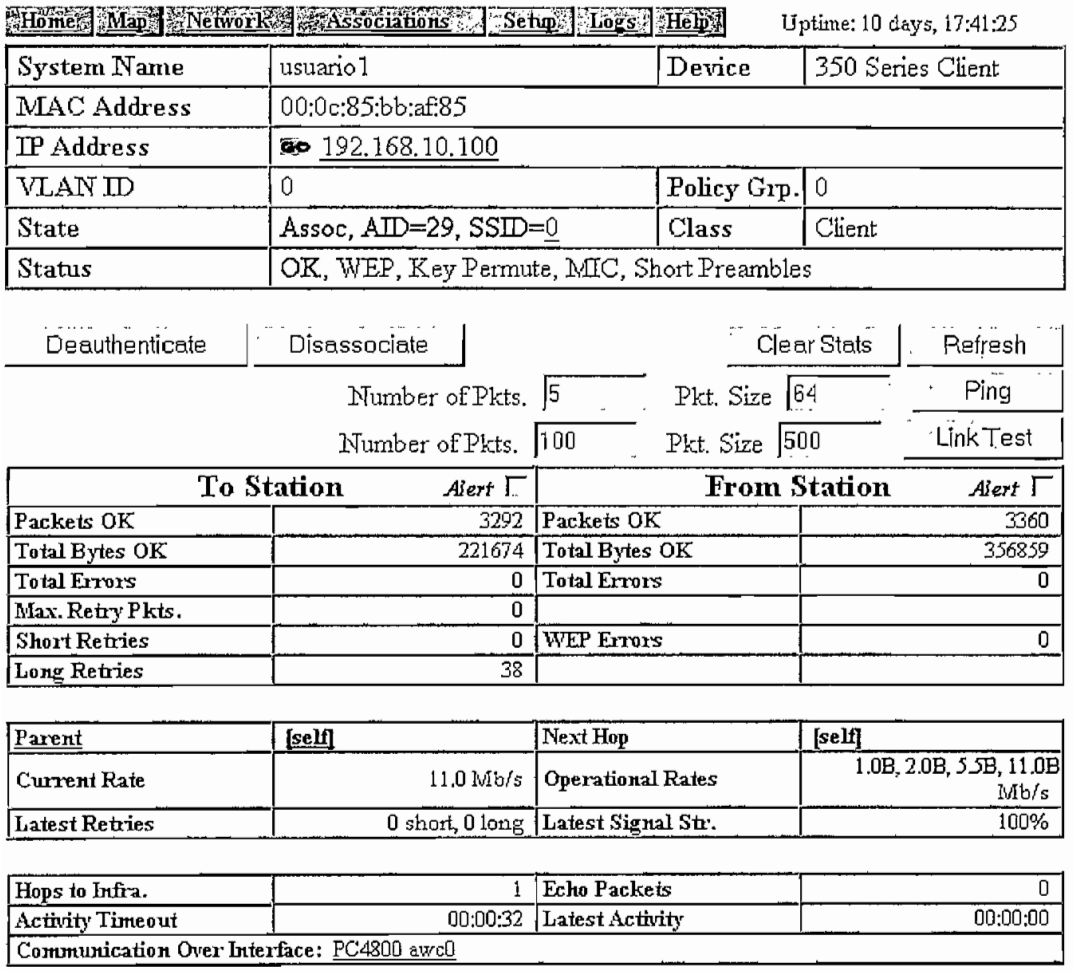


Fig. 3.52 Pantalla Home del AP con usuario1 asociado

En la pantalla anterior se presenta información sobre el usuario asociado, tal como el nombre, dirección MAC y hora de asociación. Para ver más información sobre el usuario se puede dar clic sobre el nombre del mismo, en este caso usuario1 y se despliega la pantalla de la figura 3.53 que tiene mayores datos sobre el cliente.

En esta pantalla se puede visualizar una estadística de los paquetes transmitidos y recibidos por el usuario. Además en la parte de *Status* se muestra un completo resumen del tipo de usuario. En este caso se indica que es un cliente que transmite con seguridad WEP, con MIC y que posee TKIP (*Key Permute*).

Como prueba de conectividad se puede realizar un *ping* a diferentes sitios de la red. Por ejemplo en la pantalla de la figura 3.54 se muestra el resultado de un *ping* hacia la dirección IP del AP 192.168.10.1 desde la estación del usuario.



Home | Map | Network | Associations | Setup | Logs | Help — Uptime: 10 days, 17:41:25

System Name	usuario1	Device	350 Series Client
MAC Address	00:0c:85:bb:af:85		
IP Address	192.168.10.100		
VLAN ID	0	Policy Grp.	0
State	Assoc, AID=29, SSID=0	Class	Client
Status	OK, WEP, Key Permute, MIC, Short Preambles		

Deauthenticate | Disassociate | Clear Stats | Refresh

Number of Pkts. 5 Pkt. Size 64 Ping

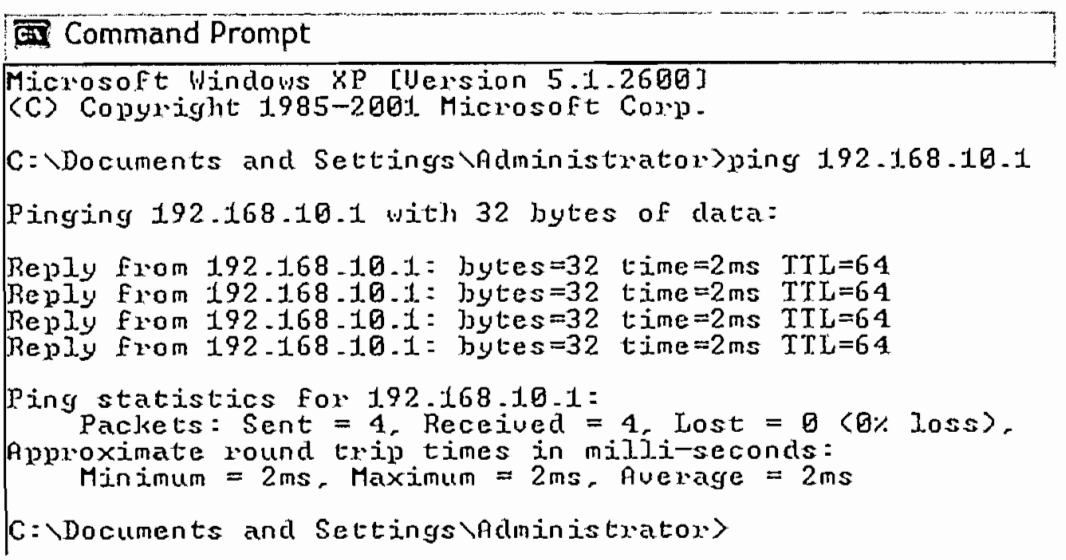
Number of Pkts. 100 Pkt. Size 500 Link Test

To Station	Alert	From Station	Alert
Packets OK	3292	Packets OK	3360
Total Bytes OK	221674	Total Bytes OK	356859
Total Errors	0	Total Errors	0
Max. Retry Pkts.	0		
Short Retries	0	WEP Errors	0
Long Retries	38		

Parent	[self]	Next Hop	[self]
Current Rate	11.0 Mb/s	Operational Rates	1.0B, 2.0B, 5.5B, 11.0B Mb/s
Latest Retries	0 short, 0 long	Latest Signal Str.	100%

Hops to Infra.	1	Echo Packets	0
Activity Timeout	00:00:32	Latest Activity	00:00:00
Communication Over Interface: PC4800 awc0			

Fig. 3.53 Pantalla de información sobre el usuario asociado



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=2ms TTL=64
Reply from 192.168.10.1: bytes=32 time=2ms TTL=64
Reply from 192.168.10.1: bytes=32 time=2ms TTL=64
Reply from 192.168.10.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\Documents and Settings\Administrator>
```

Fig. 3.54 Ping hacia el AP

Como se puede apreciar los tiempos de respuesta son de apenas 2 ms, un muy buen tiempo para una WLAN. Con esto se verifica una correcta conectividad de radio.

Ahora se puede realizar una prueba de conectividad hacia la LAN cableada desde la WLAN, para esto se realiza un *ping* desde la estación hasta el servidor *proxy* de la red con la dirección IP 192.168.10.2, obteniendo el resultado de la figura 3.55.

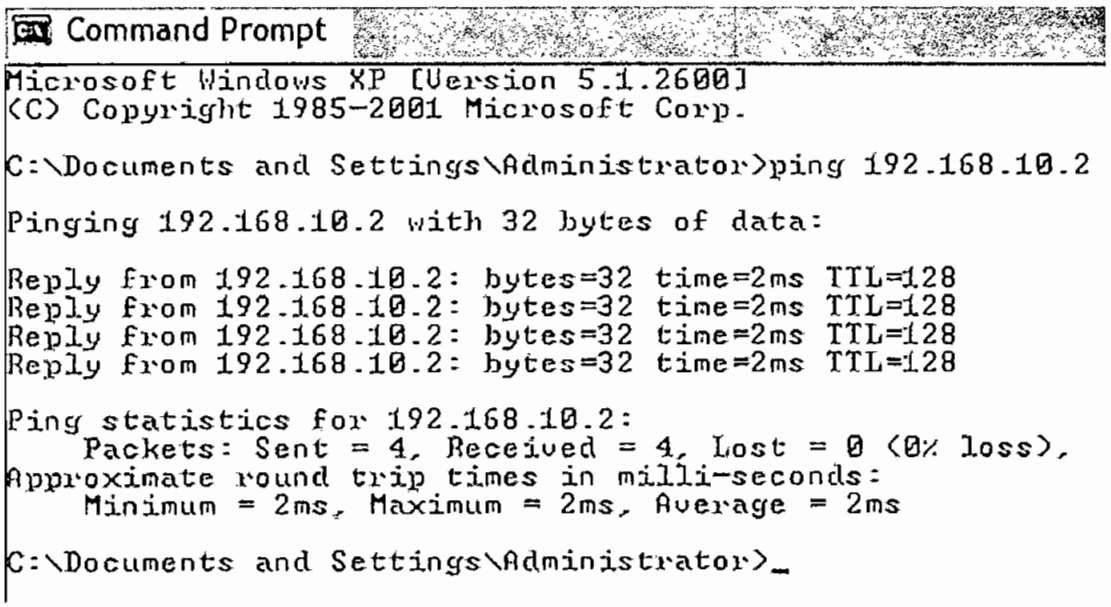


Fig. 3.55 Ping hacia el Servidor Proxy

Se puede apreciar que el resultado del *ping* es exitoso, obteniéndose respuesta desde el servidor *proxy* con tiempos de 2 ms.

3.6.2. USUARIO CONFIGURADO SIN AUTENTICACIÓN

En este caso se tiene un usuario que desea conectarse solamente conociendo el SSID y no las claves WEP. Es decir que su perfil, en la parte de *Network Security,* se encuentra configurado de la forma que indica la figura 3.56.

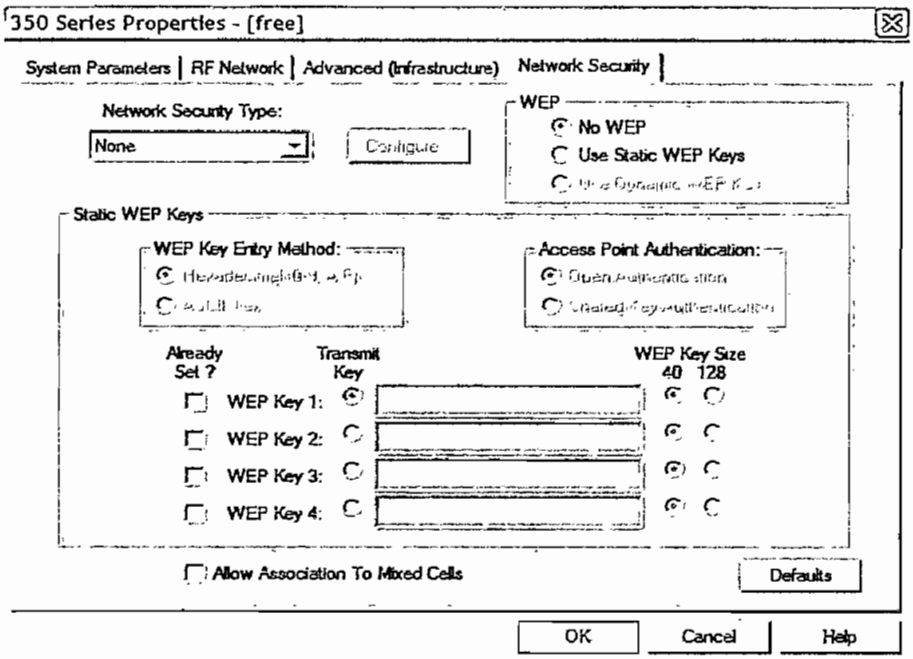


Fig. 3.56 Pantalla de Network Security sin WEP

Como el AP no permite asociarse a usuarios que no tengan configurado WEP y que no conozcan las claves WEP adecuadas, la pantalla de *Link Status Meter* del usuario en cuestión se verá como la mostrada en la figura 3.57.

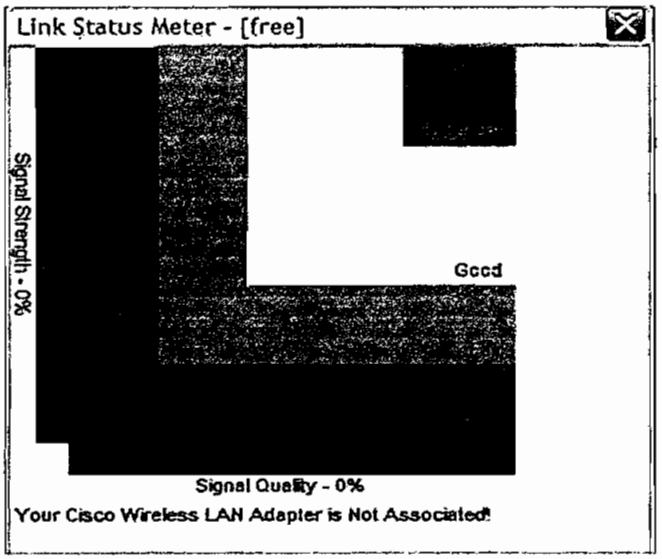


Fig. 3.57 Pantalla Link Status Meter que se muestra sin asociación

Como se puede apreciar no existe actividad en la WLAN pues no se le permite el acceso al usuario.

3.6.3. CLAVE WEP ERRÓNEA

Puede ocurrir que un usuario si está configurado para que utilice WEP, pero su clave de 128 bits no coincide con la del AP, por ejemplo se modifica la clave WEP correcta por una incorrecta que difiere solamente en el último hexadecimal, tal como se muestra en la tabla 3.7.

Número de clave	Clave
Clave 1 Correcta	7A8C6F91B549D7E37BA2F4D6AB
Clave 1 Incorrecta	7A8C6F91B549D7E37BA2F4D6AF

Tabla 3.7 Clave WEP correcta e incorrecta

Como se puede apreciar en la tabla 3.7 solo se cambia la última B por una F. Debido a esto la configuración WEP del usuario es la que se muestra en la figura 3.58.

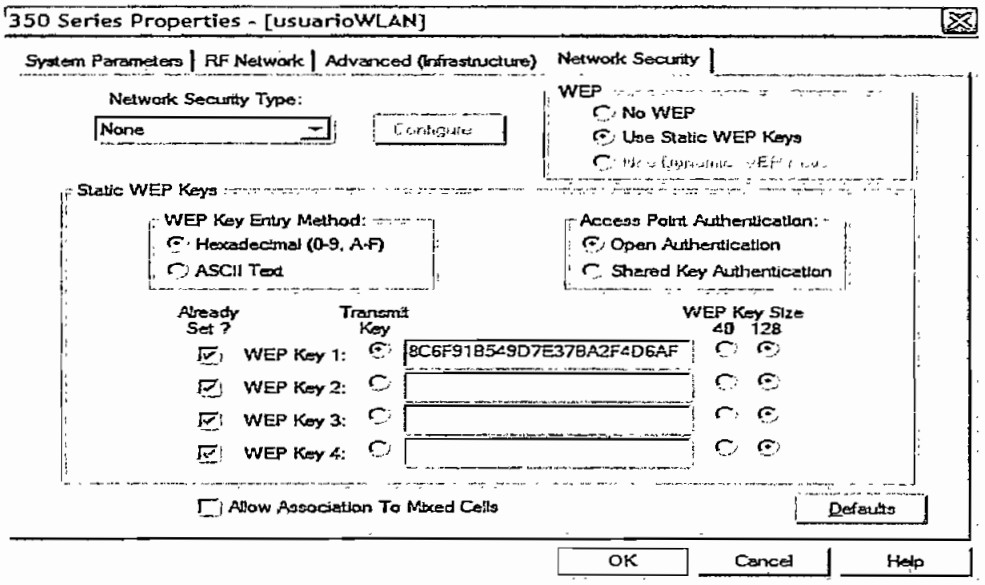


Fig. 3.58 Pantalla de Network Security con clave WEP incorrecta

Al aplicar esta configuración, el usuario parece autenticarse correctamente, incluso la pantalla de *Link Status Meter* es la misma que un usuario autorizado.

Sin embargo, a pesar de que el usuario parece asociado normalmente, el AP no le permite transmitir ni recibir datos en la WLAN. Se puede verificar esto intentando realizar un ping al AP, como lo muestra la figura 3.59.

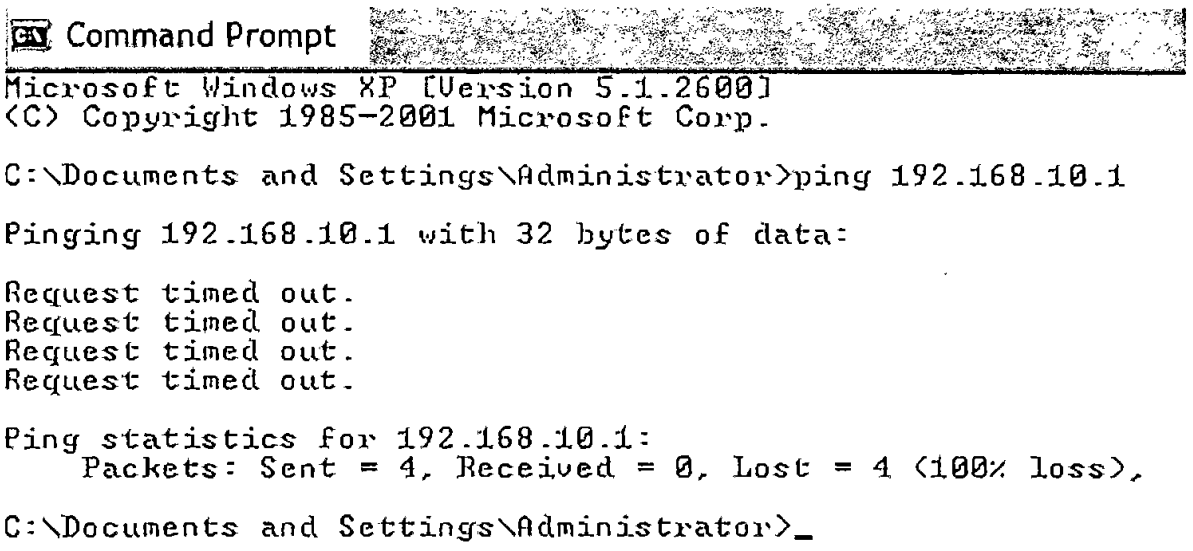


Fig. 3.59 Ping al AP

Como se puede observar en los resultados de la figura 3.59, el *ping* no es exitoso debido a que el usuario no tiene permisos en la WLAN.

3.6.4. CONFIGURACIÓN ERRÓNEA DE PARÁMETROS WEP

Ahora se tiene otro caso. Si el usuario tiene la configuración correcta de las claves WEP correspondientes, pero no el tipo de autenticación adecuado para la WLAN, tampoco se le otorgará acceso a la misma.

Por ejemplo, el tipo de autenticación en este caso es *Open,* pero si un usuario está configurado para utilizar autenticación de tipo *Shared*, tal y como se muestra en la figura 3.60, no obtendrá acceso a la WLAN.

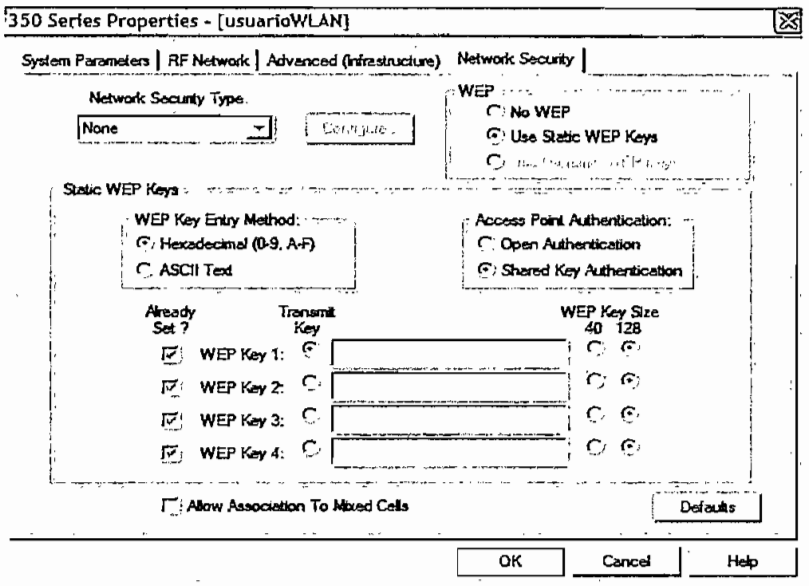


Fig. 3.60 Autenticación Shared

Al aplicar esta configuración el usuario no puede asociarse a la WLAN, por tanto se obtiene como resultado la misma pantalla de la figura 3.57 en la opción *Link Status Meter.*

AP340ecenter Summary Status

CISCO SYSTEMS

Cisco AP340 12.04

Home | Map | Network | Associations | Setup | Logs | Help

Uptime: 12 days, 13:19:45

Current Associations			
Clients: 0 of 1	Repeaters: 0 of 0	Bridges: 0 of 0	APs: 1

Recent Events		
Time	Severity	Description
12 days, 13:19:31	Warning	Station [usuario1]000c85bbaf85 Failed Authentication, status "Unsupported Authentication Algorithm"
12 days, 13:19:28	Warning	Station [usuario1]000c85bbaf85 Failed Authentication, status "Unsupported Authentication Algorithm"
12 days, 13:19:26	Warning	Station [usuario1]000c85bbaf85 Failed Authentication, status "Unsupported Authentication Algorithm"
12 days, 13:19:26	Warning	Station [usuario1]000c85bbaf85 Failed Authentication, status "Unsupported Authentication Algorithm"
12 days, 13:19:25	Warning	Station [usuario1]000c85bbaf85 Failed Authentication, status "Unsupported Authentication Algorithm"

Network Ports				Diagnostics
Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	Up	100.0	192.168.10.1	0040963667ad
AP Radio	Up	11.0	192.168.10.1	0040963667ad

Fig. 3.61 Actividad de usuarios con algoritmos de autenticación no soportados en la WLAN

Además en la pantalla *Home* del AP mostrada en la figura 3.61, se puede observar que existen intentos de asociación sin éxito debido a un algoritmo de autenticación no soportado por la WLAN. El AP presenta unos *Warnings* o alertas sobre estos sucesos. Estas alertas se pueden almacenar en un archivo de *logs* o de registros para su posterior análisis.

Estos *logs* son una buena manera de observar comportamientos extraños en la WLAN, verificar la actividad de los usuarios y prevenir ataques activos a la WLAN.

3.6.5. APLICACIÓN DEL FILTRO MAC

Finalmente se analiza el último cerco de seguridad de la WLAN. Si un usuario posee las claves WEP y la correcta configuración de seguridad exigida, no resulta suficiente, ya que debe tener una MAC autorizada para poder acceder a la WLAN.

Por ejemplo se tiene el usuario descrito en la tabla 3.8. Como se puede apreciar tiene los parámetros correctos para acceso a la WLAN y no tendrá ningún problema en la autenticación. Sin embargo se pregunta qué ocurre si su entrada MAC se elimina del AP en el listado de MAC autorizadas.

Parámetros de cliente de pruebas	
Nombre	usuario1
Autenticación	Open - WEP
IP	192.168.10.100
Default Gateway	192.168.10.2
MAC	000c85bbaf85
Perfil	Correcto
Autenticación	*Open*
Clave 1	7A8C6F91B549D7E37BA2F4D6AF

Tabla 3.8 Clave WEP correcta e incorrecta

Para eliminar su entrada en el AP se ingresa a *Setup -> Address Filters,* a través de la pantalla de la figura 3.62.

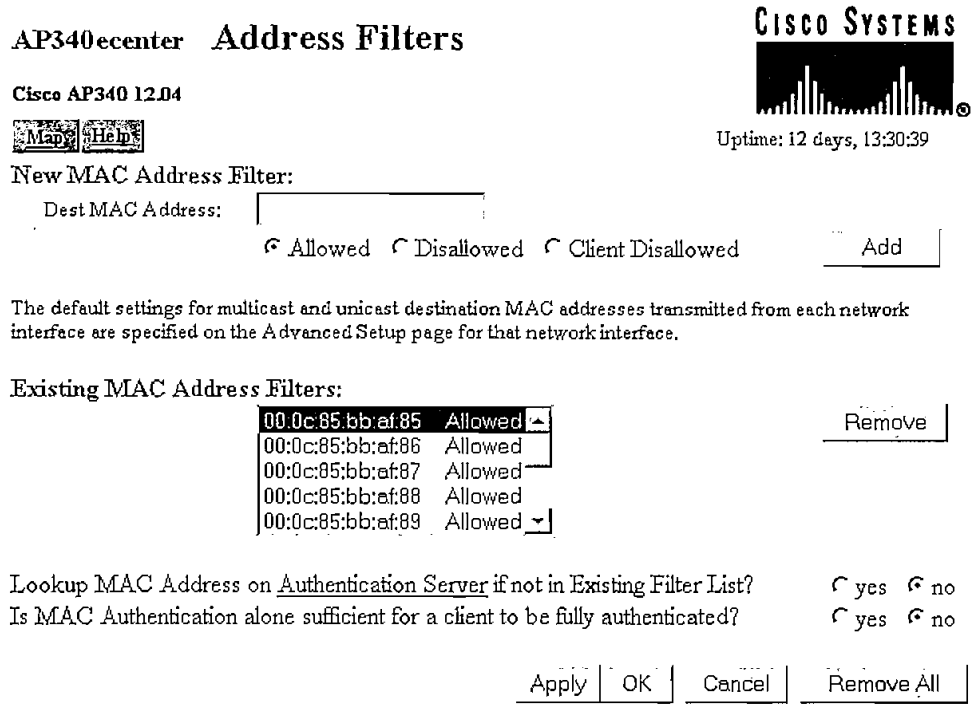


Fig. 3.62 Filtrado MAC en el AP

Se elige la entrada correspondiente a la MAC 000c85bbaf85 y se la elimina con *Remove*. El resultado se muestra en la figura 3.63. Se aplican los cambios con *Apply*.

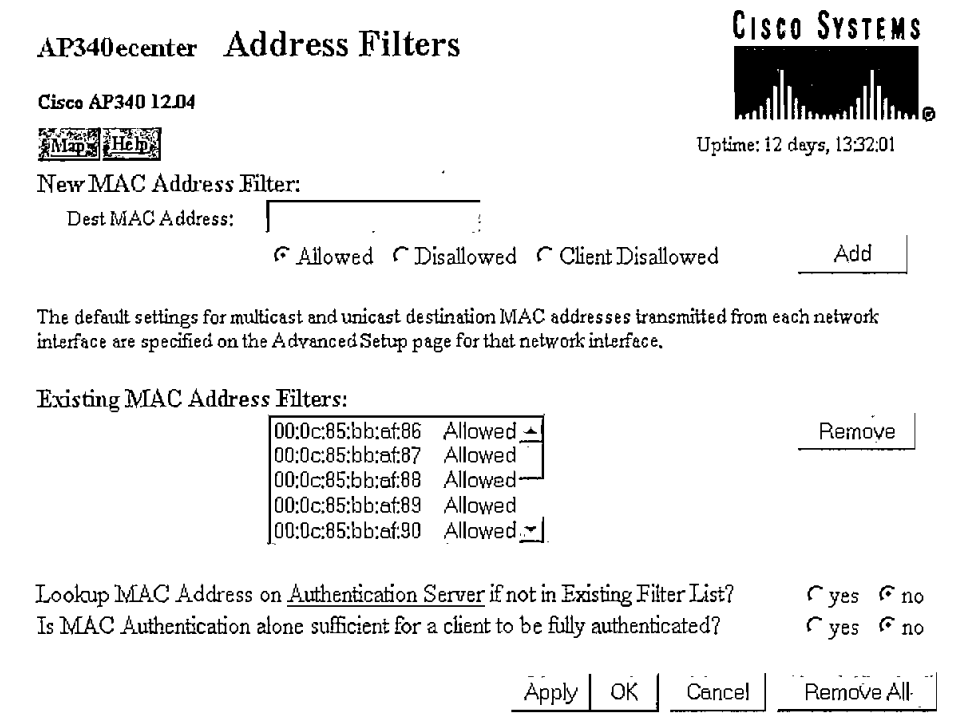


Fig. 3.63 Listado final de MAC's autorizadas en el AP

Ahora la MAC 000c85bbaf85 del cliente no es una entrada autorizada en el AP. El tratar de asociarse ahora es inútil, pues a pesar de tener los parámetros de seguridad correctos y conocer las claves WEP de la WLAN, su MAC no está configurada en el filtro del AP y por tanto no se le otorgará el acceso.

El resultado que se obtiene es la no asociación de la estación, que se puede apreciar en la pantalla *Link Status Meter* del usuario que es la misma que se muestra en la figura 3.57.

3.7. PRESUPUESTO REFERENCIAL

La solución con WEP no implica ningún gasto adicional en hardware en la implementación de seguridad, ya que solamente se realiza la configuración en la infraestructura inalámbrica instalada. Además el proceso de configuración WEP es sencillo y rápido.

Por todo esto la solución completa es muy económica y la implementación de la seguridad solo añade un costo de tiempo de configuración. En la tabla 3.9 se muestra un desglose del presupuesto final de la solución de una WLAN segura con WEP.

Se puede apreciar que la implementación de la seguridad implica solamente 2 horas técnicas de trabajo extra, una para el AP y una para los 10 usuarios inalámbricos. De esto se deduce que el costo de la seguridad es apenas un 3.5% de la solución total de la red inalámbrica para el problema planteado.

Esto por supuesto es muy atrayente para los clientes que desean reducir los gastos de implementación de esta tecnología. Además la solución presentada ofrece características fuertes de seguridad y el cliente puede estar tranquilo al utilizar su WLAN.

Ítem	Número de Parte	Descripción	Cantidad	Precio Unitario	Total
1	AIR-AP342EZR-A-K9	Access Point 802.11b, 100 mW, Dual RP-TNC, FCC, incluye 2 antenas dipolares.	1	950*	950
2	AIR-PCM352	Tarjeta PCMCIA 802.11b con antena integrada	10	110*	1100
3	Configuración del AP	Configuración básica del AP	1	40 (1 hora técnica)**	40
4	Configuración del AP	Configuración de seguridad WEP en el AP	1	40 (1 hora técnica)**	40
5	Configuración de usuario WLAN	Instalación de software y *drivers* en usuarios	10	40 (3 horas técnicas)**	120
6	Configuración de usuario WLAN	Configuración de seguridad WEP en usuarios	10	40 (1 hora técnica)**	40
				TOTAL	**2290**

* *Estos precios son ofertados actualmente por Cisco Systems Inc. e incluyen el 12% de IVA.*

** *Se considera el precio en función del número de horas técnicas requeridas, a un precio de 40 USD cada hora.*

Tabla 3.9 Presupuesto final para una WLAN con WEP

CAPÍTULO 4

4. SOLUCIÓN PARA UNA RED LAN INALÁMBRICA SEGURA DE PEQUEÑA ESCALA CON LEAP

En este capítulo se presenta una guía de implementación de seguridad para una red LAN inalámbrica de pequeña escala utilizando el protocolo LEAP. Para ello se describen los diferentes aspectos a considerar en la solución LEAP, se define un escenario común para redes inalámbricas y se diseña la solución para su implementación en los equipos.

4.1. GENERALIDADES DE LA SOLUCIÓN CON LEAP

Para la implementación de seguridad en una WLAN con LEAP se tienen presentes tres componentes:

- El *Access Point*
- Las tarjetas inalámbricas
- El Servidor RADIUS

Estos tres componentes se integran en el escenario de la figura 4.1.

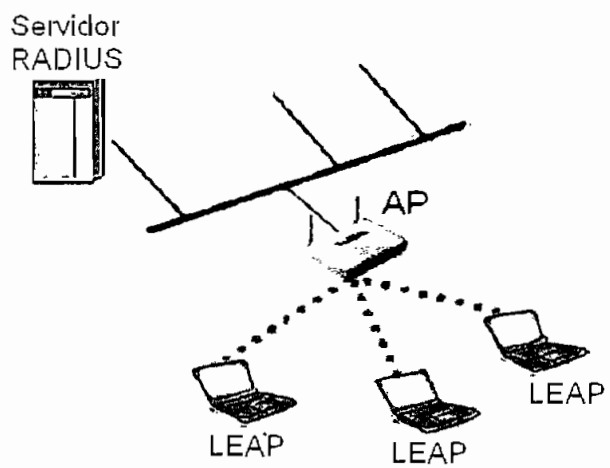


Fig. 4.1 Red WLAN con seguridad LEAP

El usuario para poder asociarse a la red necesita presentar sus credenciales al servidor RADIUS a través del AP; en el caso de LEAP, las credenciales son su nombre de usuario y una contraseña que también conoce el servidor.

Bajo este esquema de funcionamiento se requiere que el usuario tenga una configuración adecuada de LEAP y conozca sus credenciales para poder acceder a la WLAN.

Además el AP debe poder comunicarse de forma segura con el servidor RADIUS para poder intercambiar la información del usuario. A su vez, el servidor RADIUS debe manejar todas las peticiones del AP y conocer una base de datos consistente de todos los usuarios autorizados y sus respectivas credenciales. Como complemento de este esquema se pueden considerar todas las medidas de seguridad adicionales tomadas en cuenta en el capítulo anterior.

4.2. DESCRIPCIÓN DEL PROBLEMA

Se presenta el mismo problema planteado en la sección 3.3 del capítulo anterior. Una empresa mediana que desea tener conectividad con bajo costo y con un buen nivel de seguridad en su comunicación.

4.3. BOSQUEJO DE LA SOLUCIÓN

Para una solución con LEAP se deben establecer las características técnicas de los tres elementos a utilizarse. EL AP y las tarjetas inalámbricas son los mismos que se describen en el capítulo anterior. Esto es el AP 340 y las tarjetas inalámbricas 350 *Aironet* de Cisco.

Para el servidor se tienen tres opciones:

- Servidores *FreeRadius* sobre Linux.

- Servidores propietarios de Cisco sobre sistemas operativos de red como Windows 2000 Server.

- Servidores comerciales sobre varias plataformas.

Los servidores *FreeRadius* presentan el inconveniente de requerir una plataforma Linux completamente instalada y funcionando correctamente, esto implica contratar personal para soporte de los servicios y mantenimiento del hardware.

El servidor RADIUS más vendido de Cisco es el *Cisco Secure Access Control*, que funciona solo sobre plataformas de servidores como *Windows* 2000 *Server*. El inconveniente obvio es el costo de las licencias de estos sistemas operativos y la administración más compleja de los mismos. Además el software de Cisco no es exclusivo para servidor RADIUS, sino que también provee funcionalidades adicionales como concentrador de VPN´s, bases de datos, etc, por lo que su costo es elevado.

La solución más simple es el elegir un software comercial como el servidor *Odyssey Server* de la empresa *Funk Software*. Este software presenta las siguientes ventajas:

- Es exclusivamente un servidor RADIUS, por lo cual no se paga por servicios adicionales innecesarios.
- Puede instalarse sobre varias plataformas, incluso en sistemas operativos de estaciones como Windows 2000 y Windows XP.
- Ofrece compatibilidad con varios fabricantes de equipos y la empresa *Funk Software* brinda soporte sobre problemas comunes de configuración.
- Maneja varios esquemas de seguridad como LEAP, EAP – TLS, EAP – TTLS, etc.
- Permite autenticar a los usuarios directamente contra las bases existentes de Windows, evitando así manejar bases de datos externas en otros lenguajes.

- Tiene total compatibilidad con *Active Directory* de Windows por lo cual los usuarios del sistema pueden ser añadidos directamente como usuarios inalámbricos con sus respectivas credenciales.
- Por su interfaz gráfica es fácil e interactivo de configurar.
- Es fácil de instalar y ligero en ocupación de recursos del sistema.
- Ofrece una versión de prueba de 30 días para probar la funcionalidad del software.

Por todos estos aspectos mencionados anteriormente, la solución es utilizar el servidor *Odyssey Server*, específicamente la versión 1.10.00.297.

Ahora ya se tienen listos los 3 elementos para la implementación de la solución de seguridad con LEAP, se debe tomar en cuenta que los parámetros de la red son los mismos que se explican en la sección 3.3 del capítulo anterior.

4.4. CONFIGURACIÓN DEL SERVIDOR

Como se mencionó en el numeral anterior, el servidor RADIUS seleccionado es el *Odyssey Server*, específicamente la versión 1.10.00.297. Este servidor puede descargarse desde Internet del siguiente enlace del desarrollador: www.funk.com. Por tratarse de un software comercial tiene un costo económico que se presenta en el presupuesto de la solución al final de este capítulo. Sin embargo para propósitos de pruebas de compatibilidad ofrece una versión de prueba que dura 30 días que es la que se utiliza en la solución. La puesta a punto del servidor RADIUS comprende tres etapas: la instalación, la configuración LEAP y el manejo de usuarios autorizados.

4.4.1. INSTALACIÓN DEL SERVIDOR RADIUS ODYSSEY SERVER

Como se mencionó anteriormente, el servidor *Odyssey* ofrece una versión de prueba de 30 días que se puede descargar del Internet. El archivo que se

descarga del enlace del fabricante es un ejecutable de 6.1 MB compatible con los sistemas operativos Windows 2000 y Windows XP. [15]

En el caso del problema planteado el sistema operativo elegido es Wxp. Este archivo de instalación se lo puede observar en la figura 4.2.

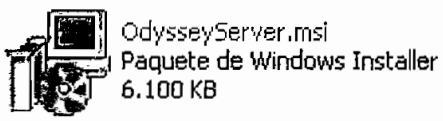


Fig. 4.2 Archivo de instalación del Servidor

Después de poner en ejecución el archivo que permite la instalación del *Odyssey Server* versión 1.10.00.297, se presenta en pantalla un mensaje que indica que se está preparando un asistente para la instalación, este mensaje se muestra en la figura 4.3.

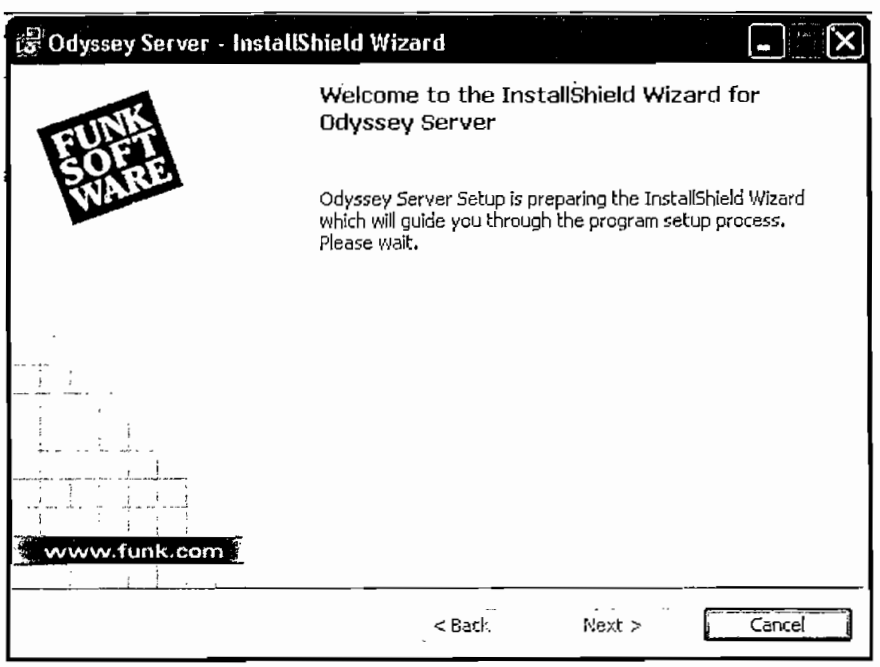


Fig. 4.3 Instalación del Servidor Odyssey

Después de unos segundos se presenta la pantalla que se muestra en la figura 4.4, para continuar con la instalación se da un clic en *Next.*

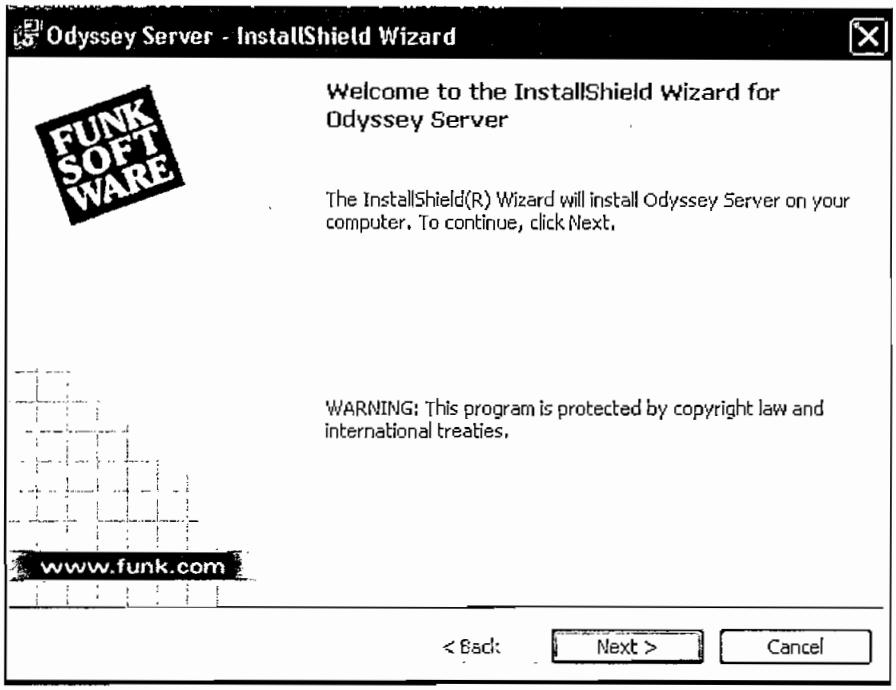


Fig. 4.4 Instalación del Servidor Odyssey

En la pantalla se despliega el mensaje de la figura 4.5, que indica la conformidad de la licencia de utilización del software, se aceptan los términos y se da un clic en *Next.*

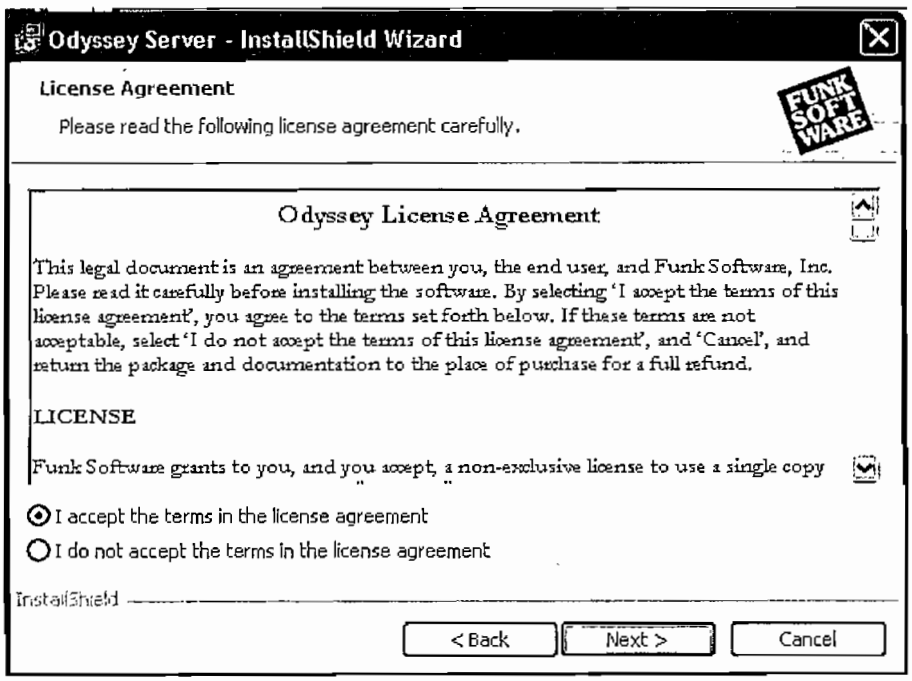


Fig. 4.5 Conformidad de términos de uso de la licencia

En la figura 4.6 se muestra la pantalla para ingreso de datos, como el *User Name, Organization* y *License Key*[1]. Luego de llenar estos datos se da un clic en *Next.*

Fig. 4.6 Datos del usuario del software

Luego, en la pantalla de la figura 4.7 se escoge las características del servidor que se instalará. Se selecciona la opción *Complete* y se da un clic en *Next.*

Fig. 4.7 Opciones del tipo de instalación del servidor

[1] En la opción *License Key* se selecciona la opción 30 *Day Install* ya que se trata de una *versión de prueba.*

Con esto termina la configuración de los parámetros de instalación, en la pantalla de la figura 4.8 se elige la opción *Install* y comienza el proceso de instalación.

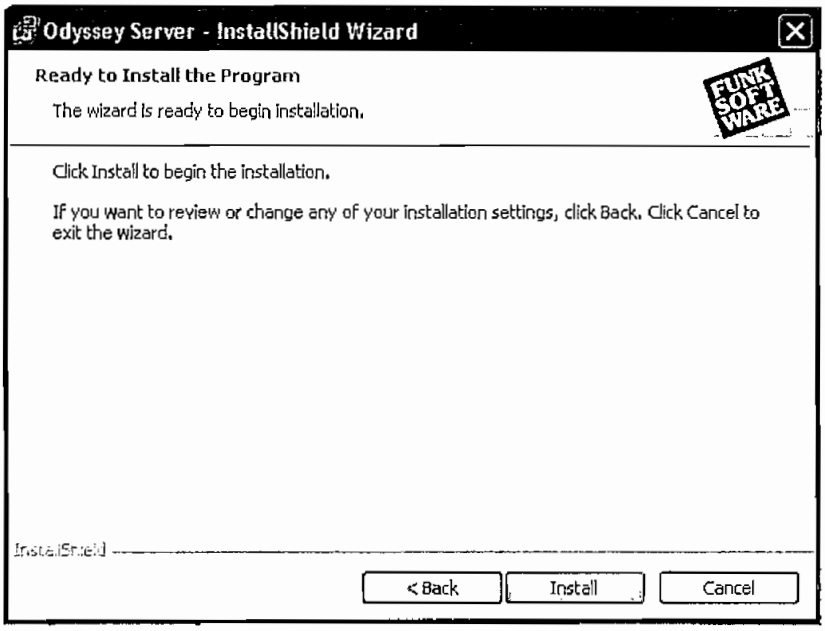


Fig. 4.8 Instalación del Servidor Odyssey

Finalmente aparece la pantalla de la figura 4.9 en la que se elige las opciones de ejecutar el servidor y ver el archivo de información general del servidor y luego se da un clic en *Finish*.

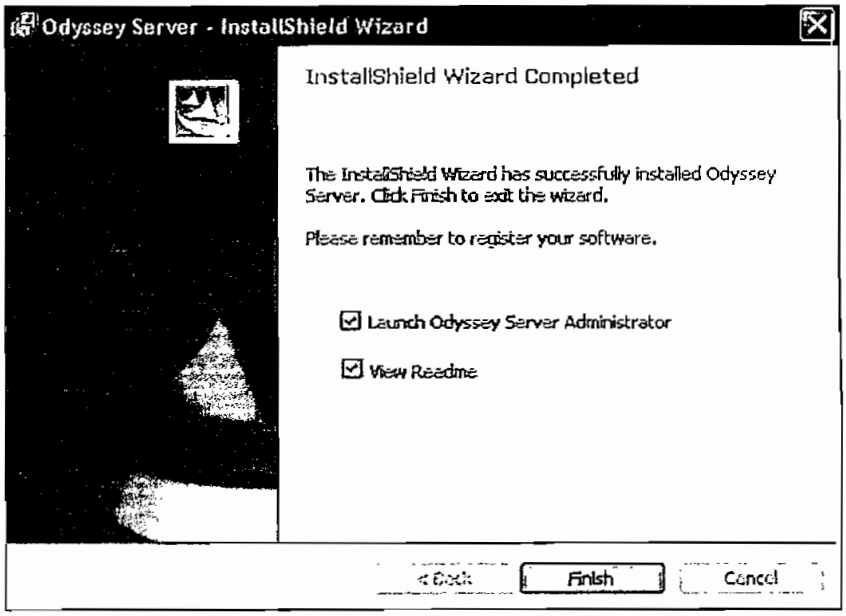


Fig. 4.9 Pantalla final de instalación del servidor

Luego se presenta en pantalla la consola de configuración del servidor que se muestra en la figura 4.10. Esta consola es la interfaz con el administrador para la configuración de los diferentes parámetros del servidor RADIUS.

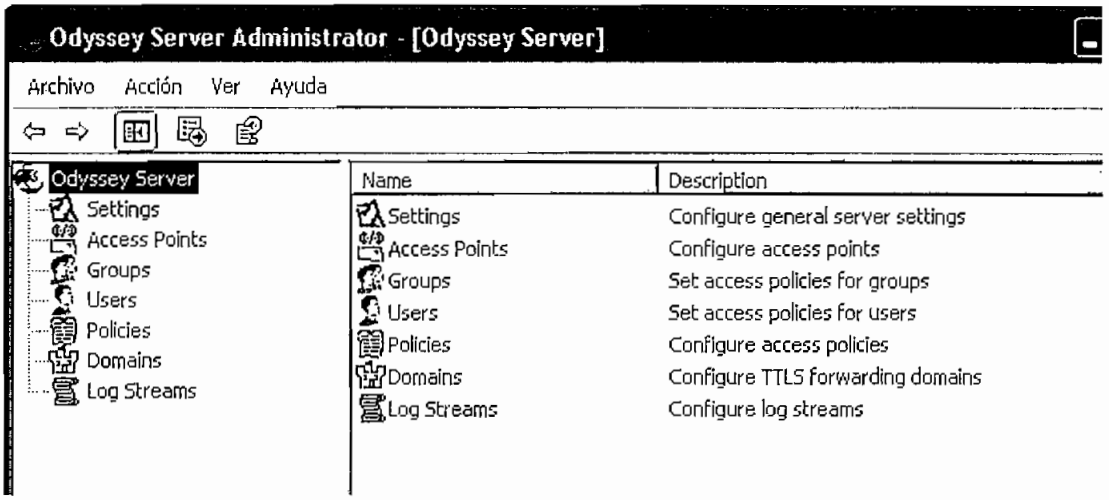


Fig. 4.10 Consola de configuración del servidor Odyssey

También se muestra el archivo *README.txt* del software en el que se puede observar las características fundamentales del servidor y su compatibilidad con el hardware del mercado. Verificar esto es muy importante ya que si no se ofrece soporte con la marca de infraestructura inalámbrica utilizada, el servidor no será útil. En la tabla 4.1 se muestra un resumen de la compatibilidad del servidor con diferentes marcas de AP´s y su correspondiente versión de *firmware*; en cambio en la tabla 4.2 se muestra la compatibilidad del servidor con diferentes marcas de tarjetas inalámbricas, con su correspondiente *driver* y *firmware*.

AP´s compatibles con el servidor *Odyssey*	
AP	***Firmware***
3COM	AP-800
ORiNOCO	AP-500
CISCO 340	11.07
CISCO 350	11.07
CISCO 1200	11.07
Intel 5000	-

Tabla. 4.1 AP´s compatibles con el servidor Odyssey

Tarjetas compatibles con el servidor *Odyssey*			
Tarjeta	***Firmware***	***Driver***	***Sistema Operativo***
3COM	-	4.0.4.00	XP
ORiNOCO Gold Card	8.10	7.41.0.36	XP,2000
CISCO 340	4.25.10	6.97	XP,2000
CISCO 350	4.25.23	6.97	XP,2000

Tabla. 4.2 Tarjetas inalámbricas compatibles con el servidor Odyssey [15]

4.4.2. CONFIGURACIÓN DEL SERVIDOR *RADIUS ODYSSEY*

La configuración del servidor es rápida y dinámica gracias a su completa interfaz gráfica mostrada anteriormente en la figura 4.10

Los parámetros fundamentales se configuran en las opciones *Settings,* en la pantalla de la figura 4.11.

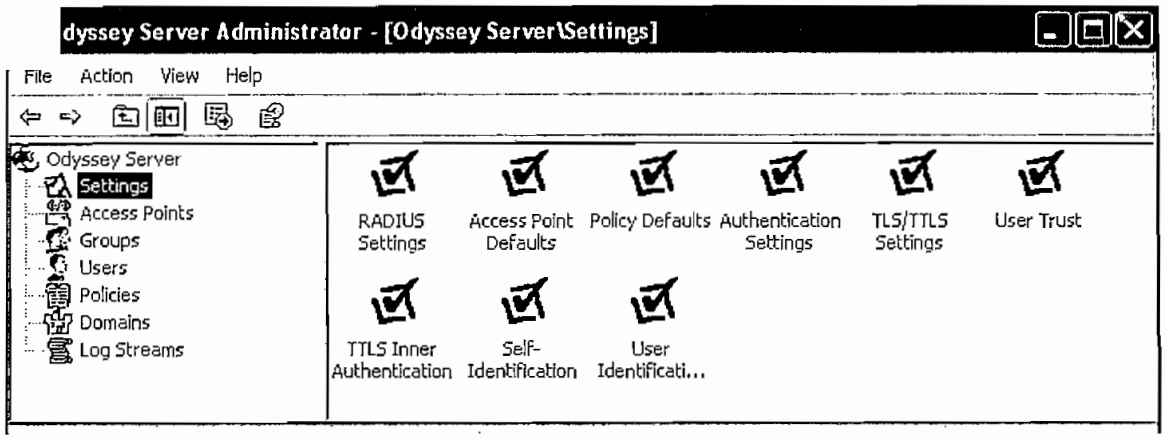


Fig. 4.11 Parámetros de configuración del servidor Odyssey

En el primer icono, el de *RADIUS Settings,* se especifica el puerto que el Servidor debe utilizar para la comunicación con el AP, el puerto estándar para RADIUS es el 1812, sin embargo es una buena política de seguridad utilizar otro puerto

disponible, ya que si un atacante logra realizar un escaneo de puertos al servidor y visualiza que el puerto 1812 está abierto, descubrirá que el servidor RADIUS de la empresa está instalado allí y tratará de obtener su valiosa información. Por ejemplo se puede seleccionar el puerto 516 que no está asignado a ninguna aplicación según el RFC 1700.

Para configurar este puerto se ingresa a la opción RADIUS *Settings* en la pantalla de la figura 4.12.

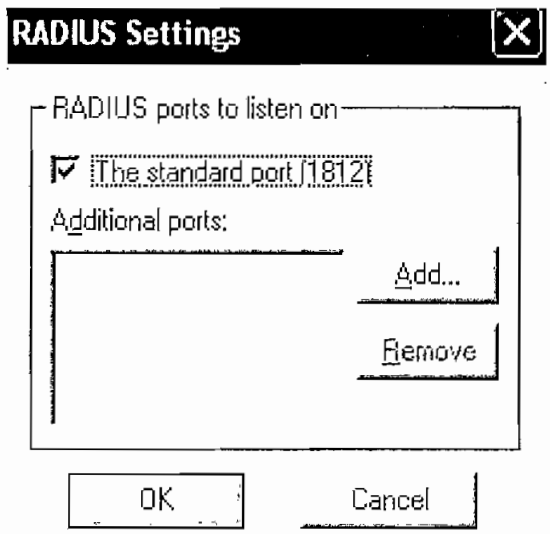


Fig. 4.12 Configuración del puerto del servidor Odyssey

Se deshabilita la opción del puerto estándar 1812 y se elige el puerto 516 en la opción *Add,* tal como lo muestra la pantalla de la figura 4.13. Se aplican los cambios con *OK.*

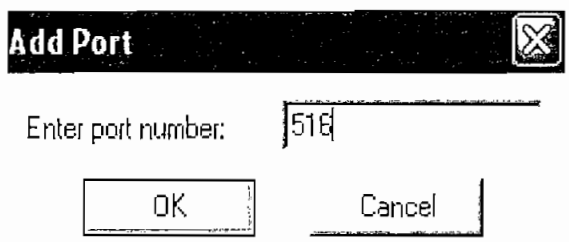


Fig. 4.13 Configuración del puerto del servidor Odyssey

Luego en el icono de *Access Point Defaults* se configura el AP por defecto con el que se comunicará el servidor. Se ingresa a esta opción y aparece la pantalla de la figura 4.14.

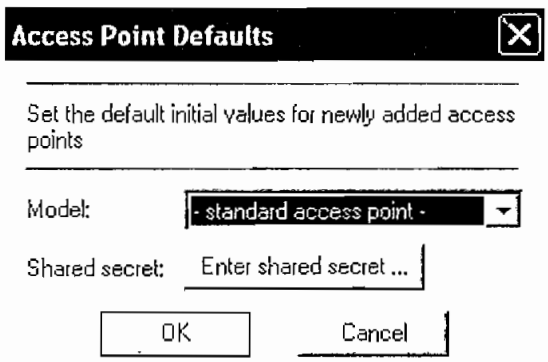


Fig. 4.14 Configuración del AP por defecto del servidor Odyssey

En el campo *Model* se elige la marca y modelo del AP, en este caso el AP 340 de Cisco, tal como lo muestra la figura 4.15.

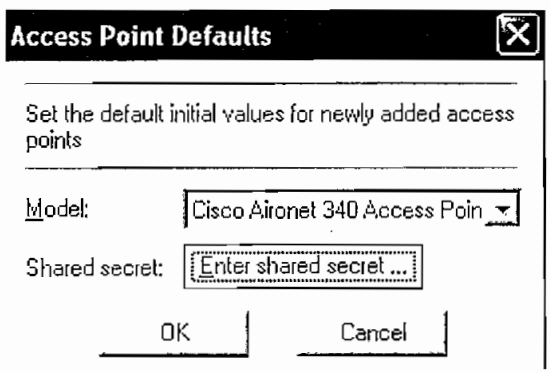


Fig. 4.15 AP por defecto del servidor Odyssey

En la opción *Enter shared secret* se ingresa una clave secreta que comparte el AP y el servidor, esta clave se utiliza para encriptar toda la información del usuario que viaja sobre la LAN cableada entre el AP y el servidor.

La clave puede ser de hasta 64 caracteres alfanuméricos, sin embargo una clave de gran longitud demoraría el procesamiento de la información y el proceso de autenticación del usuario podría durar varios minutos.

Por esto se elige utilizar la clave: q1w2ee. La configuración de la clave se puede apreciar en la pantalla de la figura 4.16.

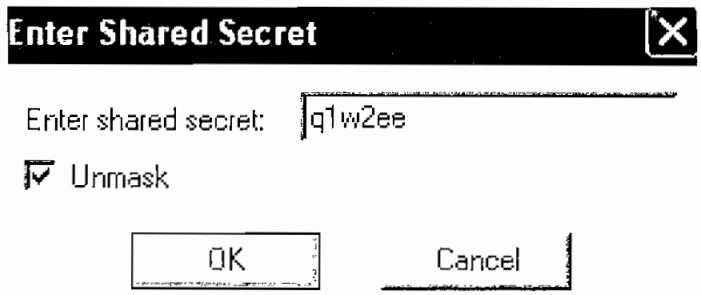


Fig. 4.16 Clave compartida entre el servidor y el AP

En el icono *Policy Defaults* de la pantalla de *Settings*, se configura la política por defecto que se debe aplicar a los nuevos usuarios que se añaden al servidor.

En la pantalla de la figura 4.17 se muestra la pantalla que se despliega al elegir esta opción. Como sólo se debe añadir usuarios autorizados al servidor, esta opción puede estar en *Allow,* que es permitir a todos los usuarios nuevos que se añaden al servidor el acceso a la WLAN.

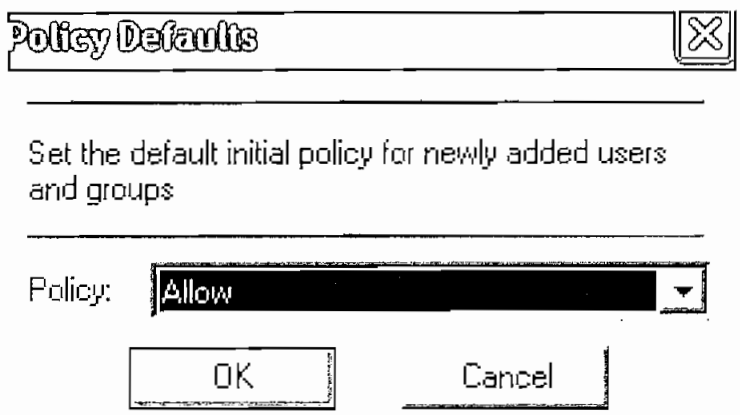


Fig. 4.17 Políticas por defecto que se deben aplicar los nuevos usuarios

En el siguiente icono, de *Autentication Settings*, se configura el método de seguridad implementado por RADIUS. Al elegir esta opción se despliega la pantalla de la figura 4.18.

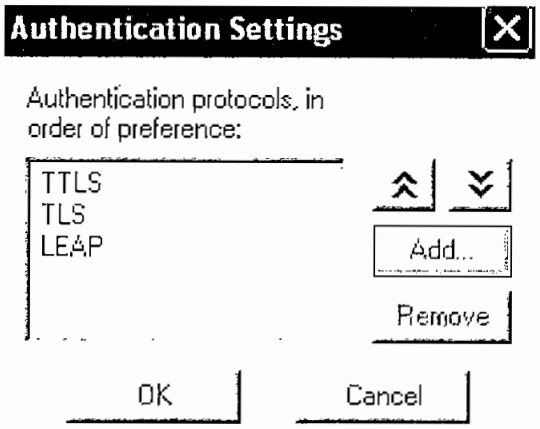


Fig. 4.18 Configuración del mecanismo de seguridad en el servidor Odyssey

En esta pantalla se puede apreciar que existen 3 métodos de autenticación soportados por el servidor: EAP- TTLS, EAP-TLS y LEAP. En la solución propuesta, sólo se debe permitir utilizar autenticación LEAP para el acceso a la WLAN, por lo cual los otros métodos deben ser removidos con la opción *Remove*. Así la pantalla final de *Authentication Settings* se muestra en la figura 4.19.

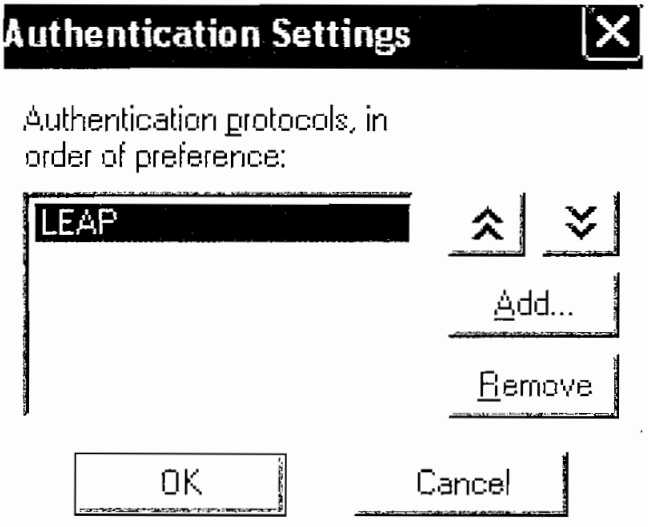


Fig. 4.19 Configuración de LEAP en el servidor Odyssey

El resto de opciones de la pantalla *Settings* son para configurar lo parámetros de EAP- TTLS y de EAP- TLS que no son necesarios ya que el servidor sólo utilizará LEAP para la autenticación de los usuarios.

4.4.3. ADMINISTRACIÓN DE USUARIOS EN EL SERVIDOR *RADIUS*

El servidor *Odyssey* permite integrarse al sistema de administración de usuarios *Active Directory* de Windows. Por ello no es necesario utilizar software adicional de bases de datos como SQL.

Al servidor se le pueden integrar los mismos usuarios del sistema de Windows, por lo cual si se desea crear un nuevo usuario inalámbrico se debe crear un usuario de Windows, asignarle su nombre de usuario y contraseña y luego añadirlo como usuario autorizado al servidor.

Para la creación de usuarios en Windows primero se debe ingresar a las opciones de administración del sistema. Para ello se da clic derecho sobre el icono de Mi PC y se selecciona Administrar, tal como se indica en la figura 4.20.

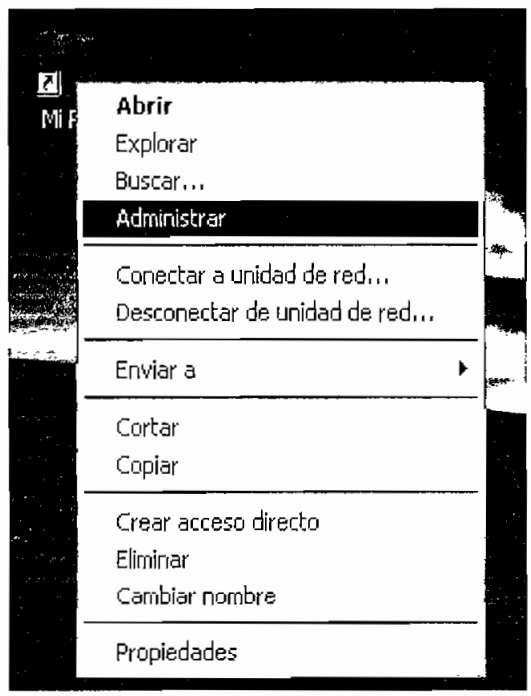


Fig. 4.20 Configuración de usuarios de Windows XP

Luego de esto se despliega la pantalla de la figura 4.21 en la que se muestra la consola de administración del equipo en su totalidad.

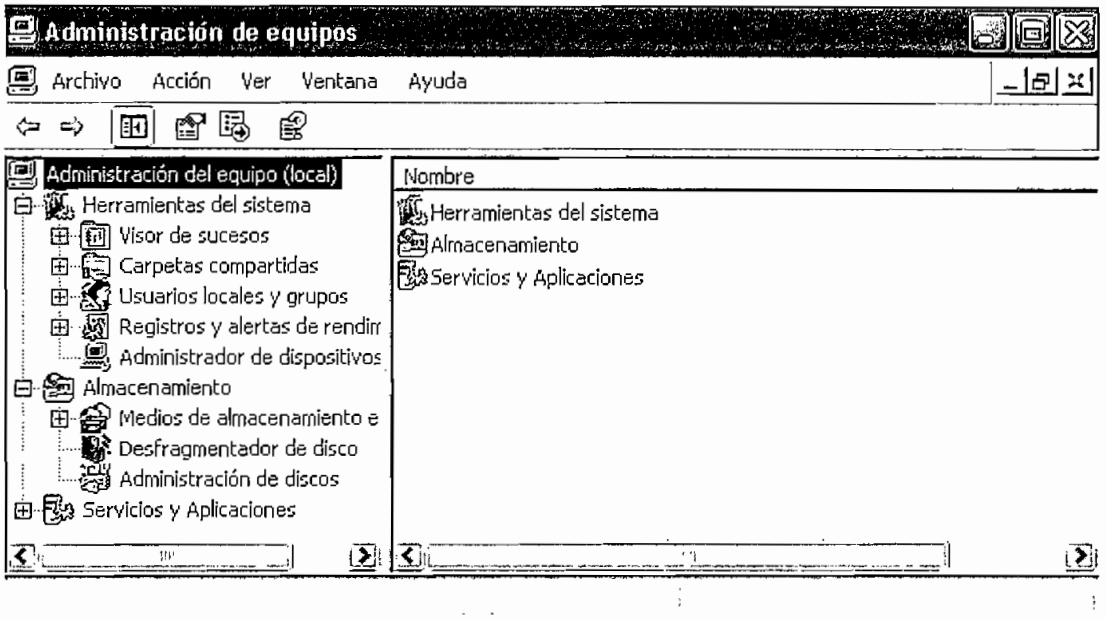


Fig. 4.21 Consola de administración del sistema WXP

Se elige la opción de Usuarios Locales y Grupos como se muestra en la figura 4.22.

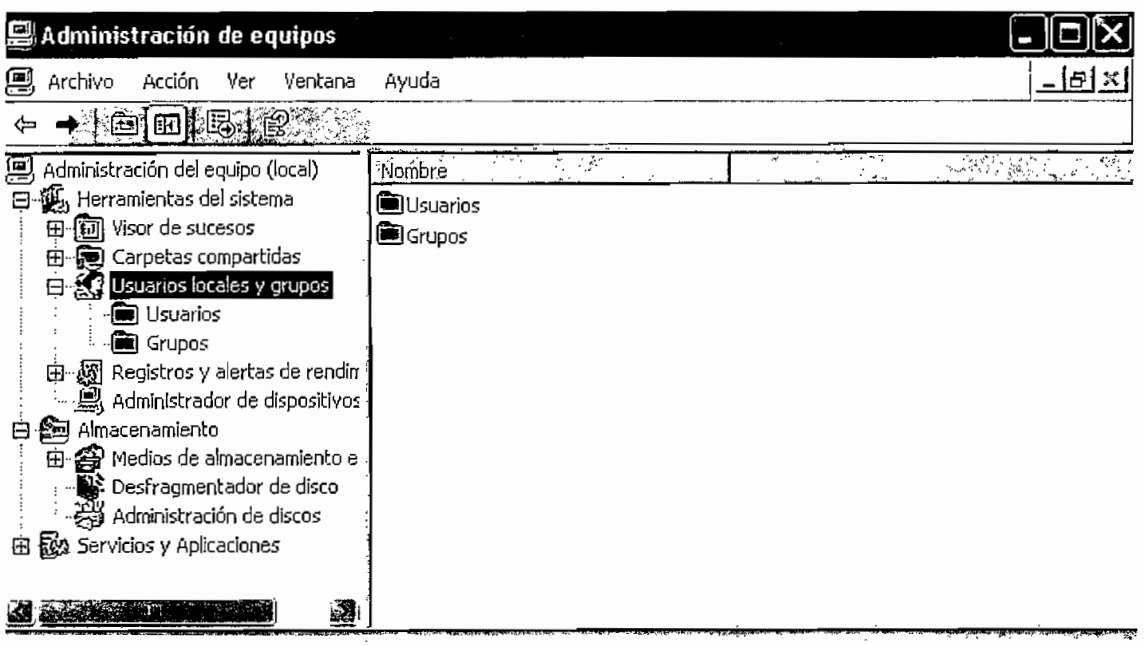


Fig. 4.22 Administración de usuarios del sistema WXP

Para añadir un usuario se debe realizar un clic derecho sobre la carpeta usuarios y èlegir la opción Usuario nuevo, como lo indica la pantalla de la figura 4.23.

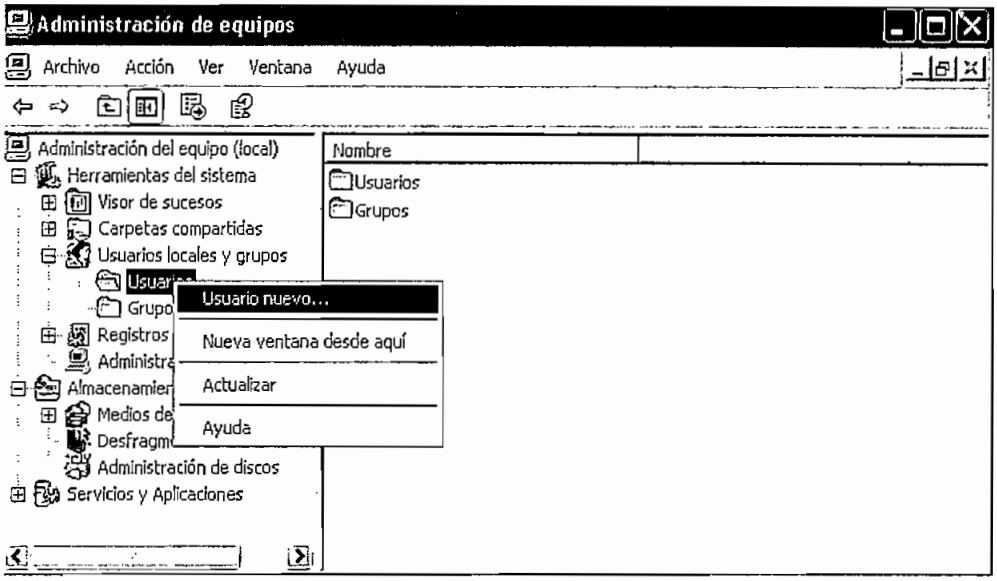


Fig. 4.23 Administración de usuarios del sistema WXP

Aparece después la pantalla de la figura 4.24 con los parámetros principales del usuario. En esta pantalla se llena el nombre, una breve descripción del usuario y su contraseña.

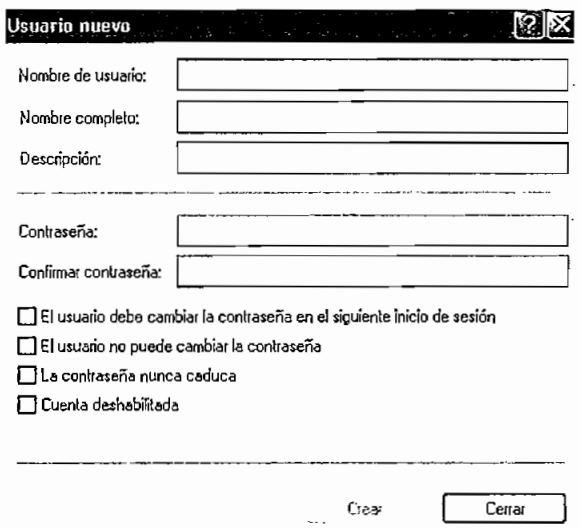


Fig. 4.24 Configuración de nuevos usuarios del sistema WXP

Además se tienen cuatro opciones adicionales para el usuario que son:

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión.- Esta opción no debe estar habilitada ya que el usuario puede cambiar a un contraseña fácil de recordar y por tanto no segura.

- El usuario no puede cambiar la contraseña.- Por la misma razón anterior esta opción debe estar deshabilitada.

- La contraseña nunca caduca.- Para evitar que un usuario se quede sin acceso debido a que su contraseña caducó, esta opción debe estar habilitada.

- Cuenta deshabilitada.- No se debe elegir esta opción, ya que crea la cuenta pero deshabilitada. Es decir que no puede utilizarse el usuario creado hasta que manualmente sea habilitado.

Finalmente se tiene el usuario1 configurado con su contraseña azsx01 como se muestra en la figura 4.25.

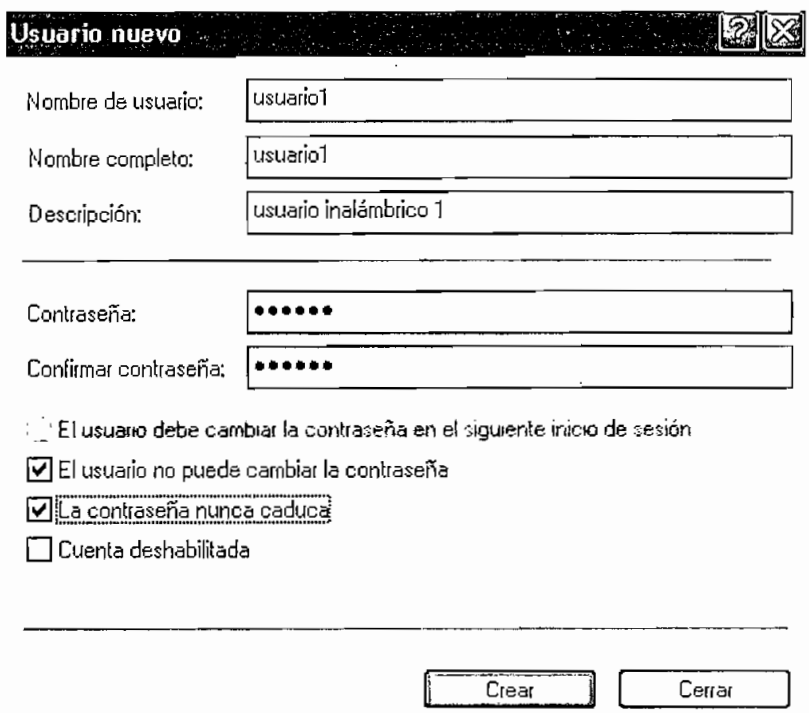


Fig. 4.25 Configuración de nuevos usuarios del sistema WXP

Con este procedimiento se pueden crear varios usuarios para acceso a la red inalámbrica, en la pantalla de la figura 4.26 se muestran los 10 usuarios creados para acceso a la WLAN según el planteamiento del problema.

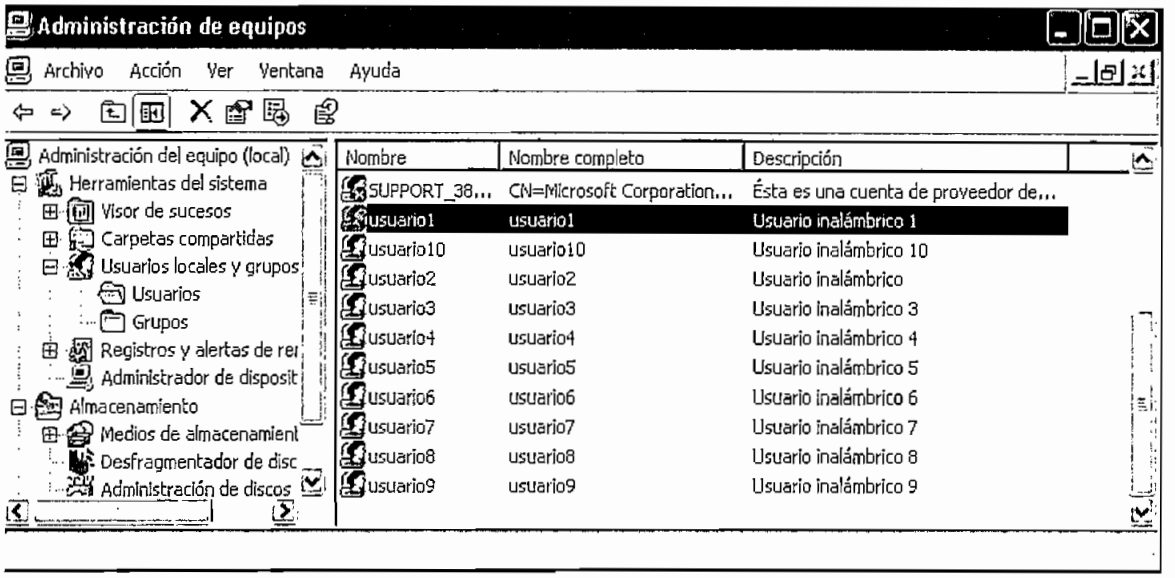


Fig. 4.26 Nuevos usuarios del sistema WXP

En la tabla 4.3 se muestran los usuarios creados con sus respectivas contraseñas de acceso.

Usuarios LEAP autorizados	
usuario1	azsx01
usuario2	azsx02
usuario3	azsx03
usuario4	azsx04
usuario5	azsx05
usuario6	azsx06
usuario7	azsx07
usuario8	azsx08
usuario9	azsx09
usuario10	azsx010

Tabla. 4.3 Nuevos usuarios del sistema WXP

Una vez que se tienen los usuarios creados se los debe añadir al servidor RADIUS para que puedan tener acceso a la WLAN. Para ello se ingresa a la opción de *Users* en la consola de administración del servidor, se da un clic derecho y aparece el mensaje *Add User,* tal como lo muestra la pantalla de la figura 4.27.

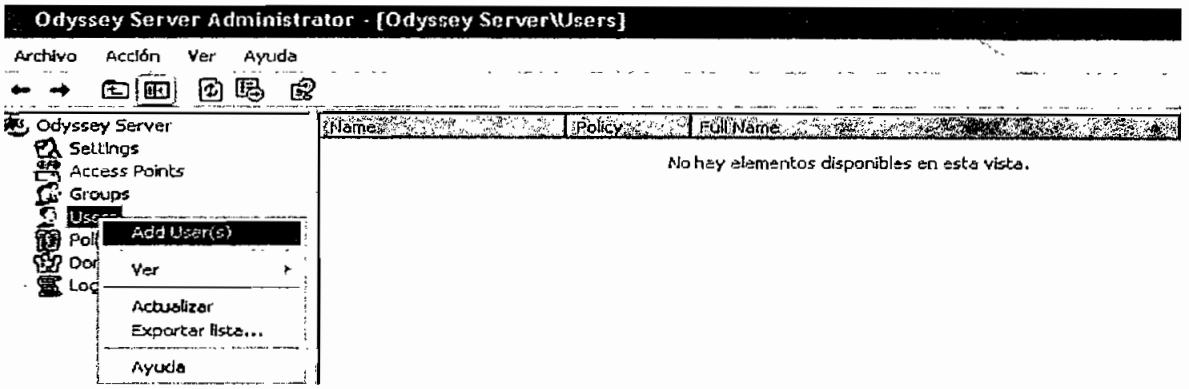


Fig. 4.27 Configuración de nuevos usuarios en el servidor Odyssey

Luego aparece la pantalla de la figura 4.28, en la que se muestran los usuarios inalámbricos creados anteriormente en el sistema. Se elige el primer usuario que es usuario1 y se lo añade con la opción *Add; e*ste procedimiento se sigue con los 10 usuarios creados en Windows y al final se tiene la pantalla de la figura 4.29 con todos los usuarios autorizados en la WLAN.

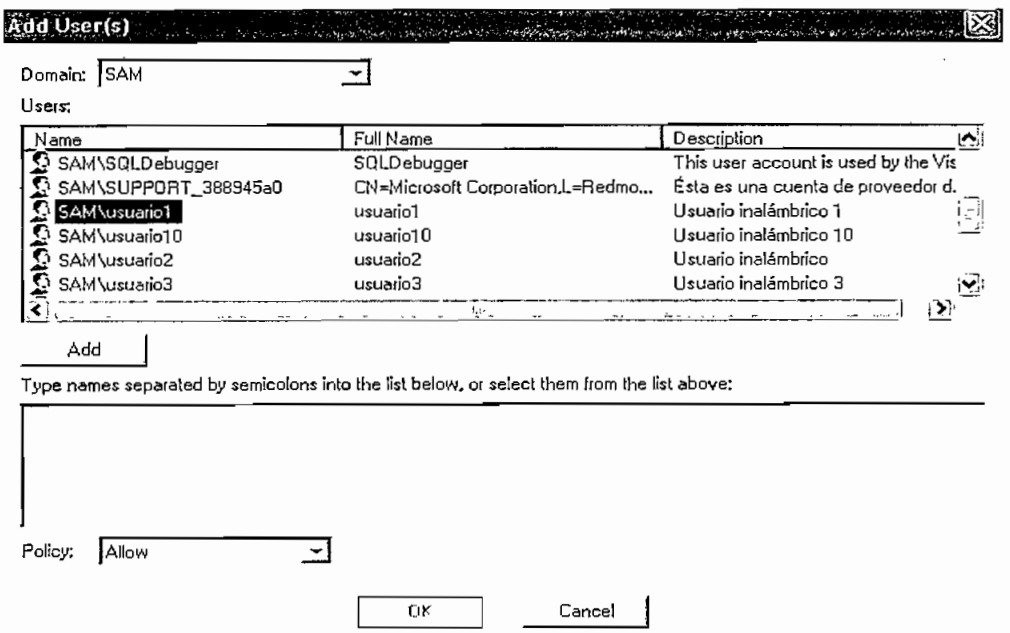


Fig. 4.28 Configuración de nuevos usuarios en el servidor Odyssey

Debe notarse que en el campo *Policy* se tiene la opción *Allow* que fue configurada por defecto en el servidor para permitir que los nuevos usuarios estén autorizados para acceder a la WLAN. Luego se aplican los cambios con *OK.*

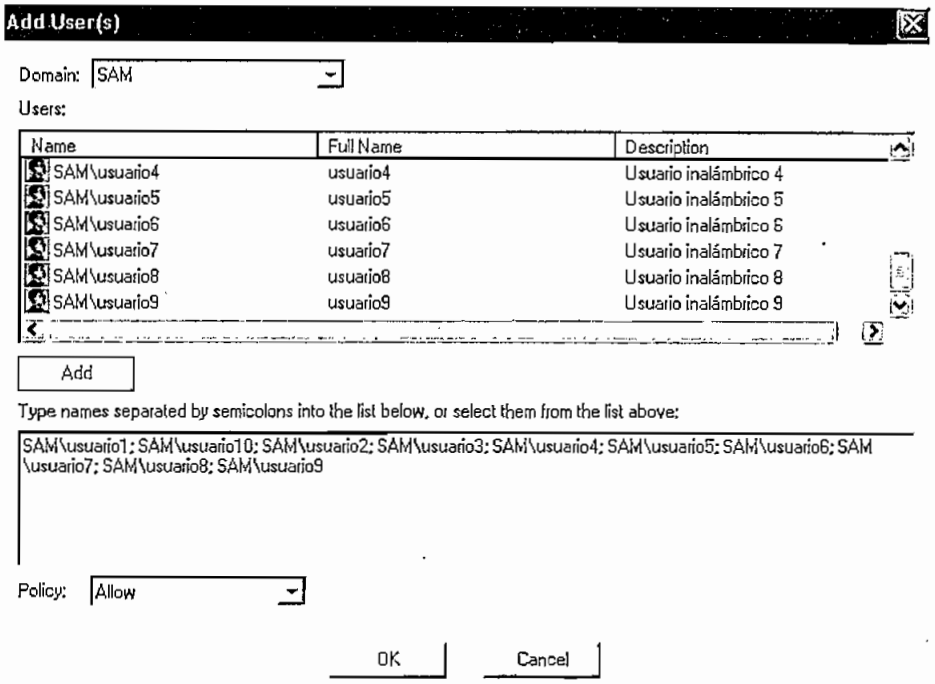


Fig. 4.29 Nuevos usuarios añadidos al servidor Odyssey

Finalmente en la consola de administración del servidor se muestran los usuarios autorizados, tal como lo muestra la pantalla de la figura 4.30.

Con esto termina la configuración del servidor *Oddysey*. Se tienen los parámetros RADIUS listos, los usuarios autorizados y el AP con el que se va a comunicar especificado. El siguiente paso es configurar el AP 340 de Cisco para que pueda comunicarse con el servidor e interactuar para la validación de las credenciales de los usuarios.

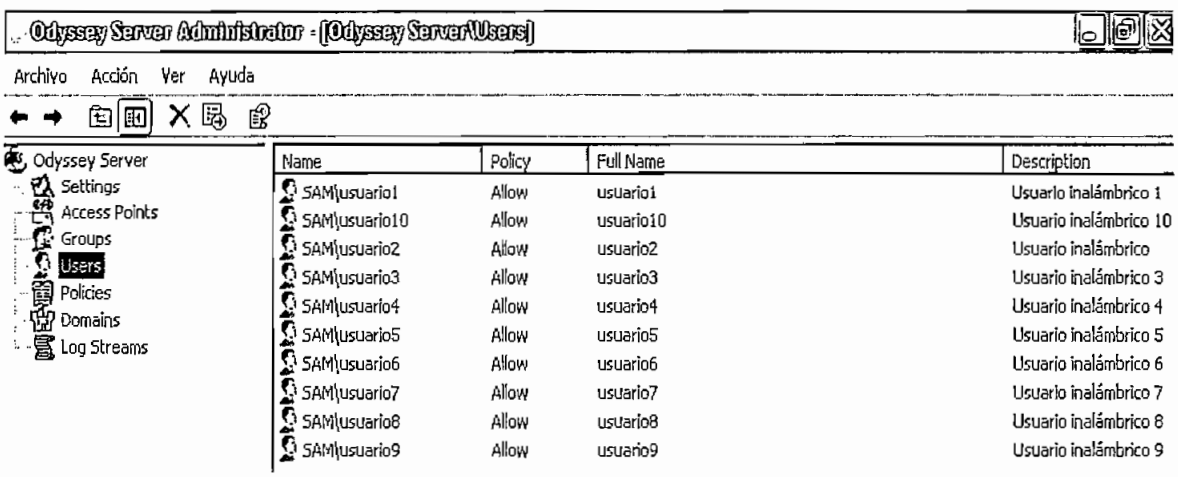


Fig. 4.30 Usuarios autorizados en el servidor Odyssey

4.5. CONFIGURACIÓN DEL AP AIRONET 340 CISCO

4.5.1. CONFIGURACIÓN BÁSICA DEL AP 340 CISCO

La configuración básica del AP se mantiene igual que la sección anterior, incluso la configuración de herramientas de seguridad adicionales como MIC y TKIP es la misma. La única variación que se tiene es en la aplicación del filtrado MAC que se muestra a continuación.

4.5.1.1. Configuración de Filtrado MAC, TKIP y MIC en el AP 340 CISCO para LEAP

Para la configuración del filtrado MAC en el AP se debe ingresar a *Setup -> Address Filters*, luego de lo cual aparece la pantalla de la figura 4.31.

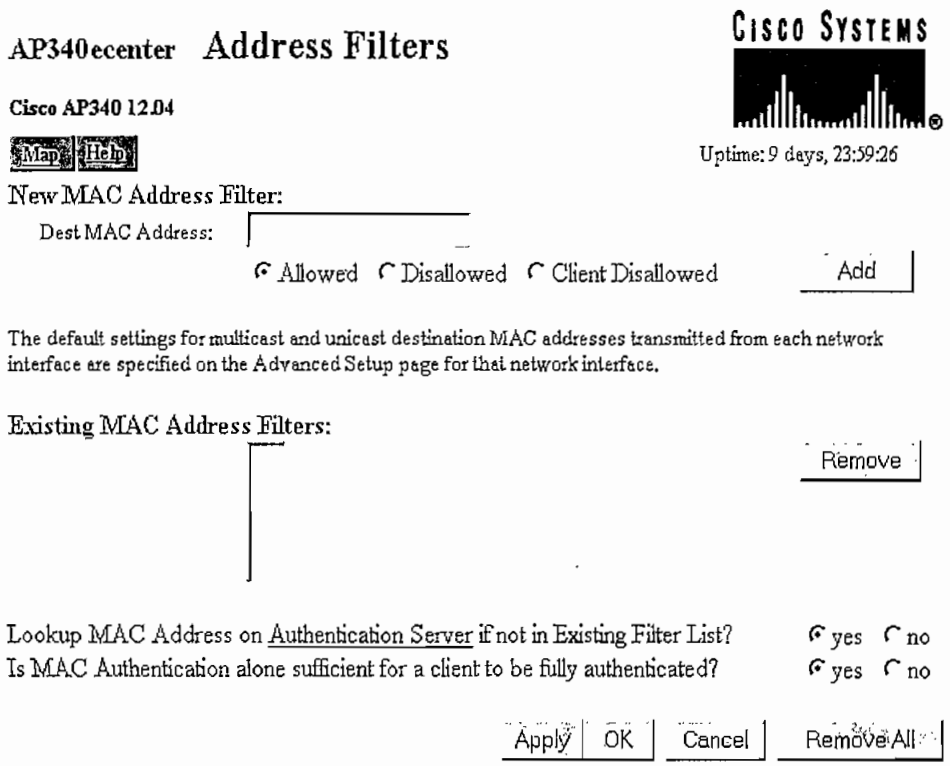


Fig. 4.31 Configuración de Filtros MAC

En el campo *Dest MAC Address Filter* se ingresan las direcciones MAC de las tarjetas de los usuarios inalámbricos, con la opción *Allowed* y luego se presiona *Add*. Como el filtro se aplica directamente en el AP la opción *Lookup MAC Address on Authentication Server if non Existing Filter List?,* debe estar en *No.*

Además la autenticación por MAC autorizada no es suficiente por lo que la opción *Is MAC Authentication alone sufficient for a client to be fully authenticated* también debe estar en no.

Realizados estos cambios la pantalla final se muestra en la figura 4.32. Luego se ingresa a la opción *Setup -> Service Sets*, donde aparece la pantalla de la figura 4.33. Aquí se selecciona el SSID de la red y se ingresa a la opción *Edit.*

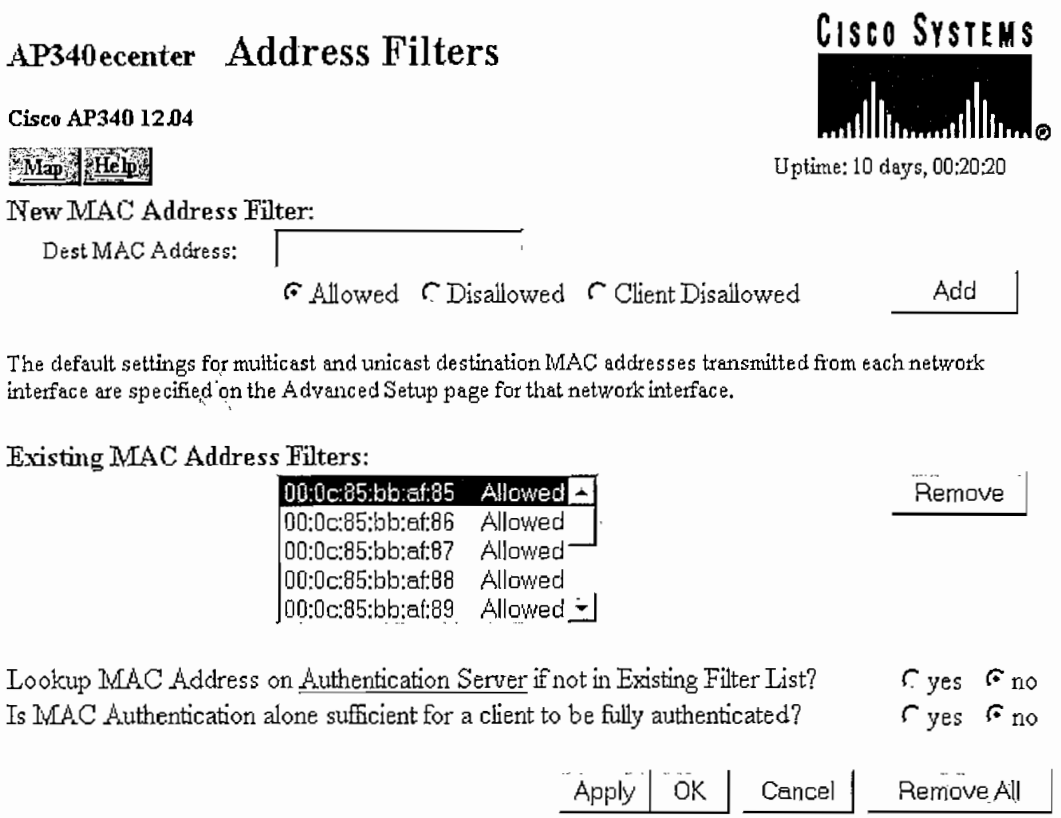


Fig. 4.32 Configuración de Filtros

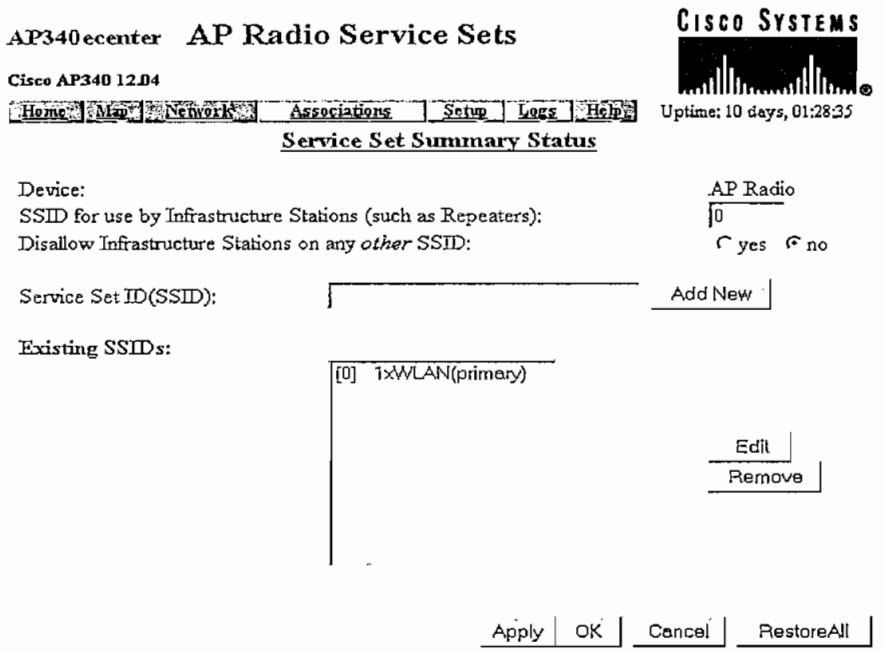


Fig. 4.33 Configuración Específica por SSID

Luego, aparece la pantalla de la figura 4.34. Hasta aquí se tiene el mismo proceso de filtrado MAC de WEP. Debajo del tipo de autenticación utilizado que es *EAP Network,* en la opción *Default Unicast Address Filter* se debe seleccionar *Disallowed*, tal como se indica en la figura 4.34, se aplican los cambios y se tiene configurado el filtrado MAC para LEAP.

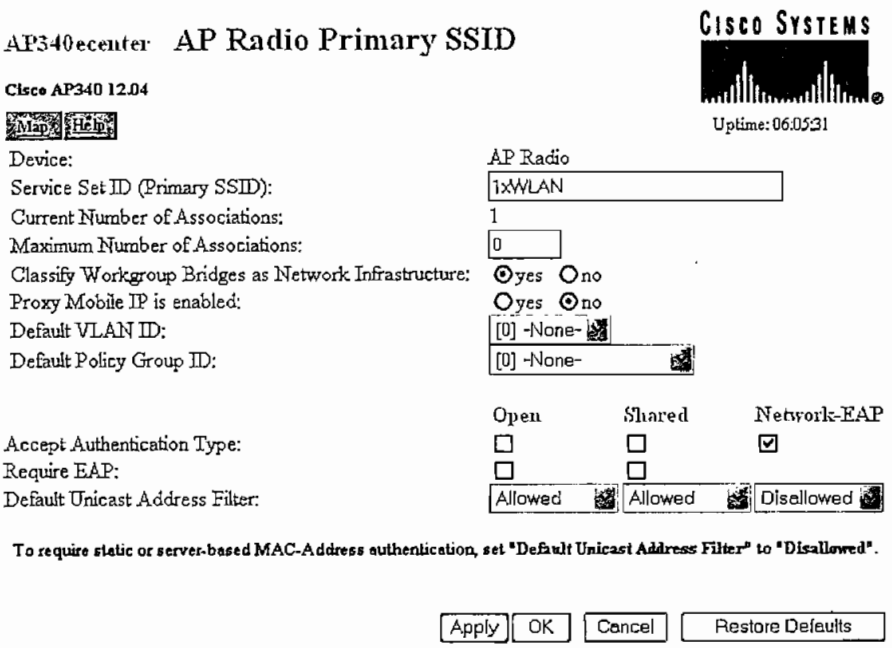


Fig. 4.34 Configuración de Filtros MAC

4.5.2. CONFIGURACIÓN LEAP EN EL AP 340 CISCO

Se debe acceder a la utilidad de configuración WEP, mediante *Setup -> Security -> Radio Data Encryption (WEP)*, luego de lo cual aparece la pantalla de la figura 4.35.

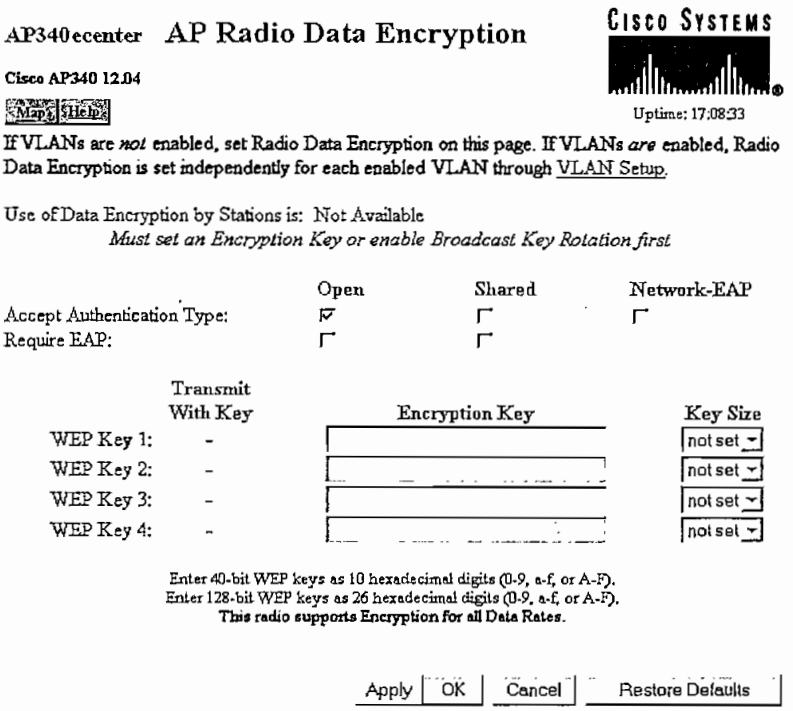


Fig. 4.35 Configuración WEP del AP 340 Aironet CISCO

Es recomendable configurar las claves WEP indicadas en el capítulo anterior ya que éstas serán utilizadas por el AP para emitir mensajes de administración; de igual forma la opción *Use of Data Encryption by Stations is* debe estar en *Full Encryption.*

La diferencia con WEP, es que en la opción *Accept Authentication Type* debe seleccionarse solamente *Network EAP* para que el único tipo de autenticación autorizado sea EAP, en este caso en particular LEAP. Finalmente la pantalla resultante se muestra en la figura 4.36. De forma similar a WEP, las herramientas de MIC y TKIP también deben configurarse. Para habilitar ambas opciones se debe ingresar a *Setup* y luego en las opciones de *AP Radio* en *Advance*, con lo que aparece la pantalla de la figura 4.37.

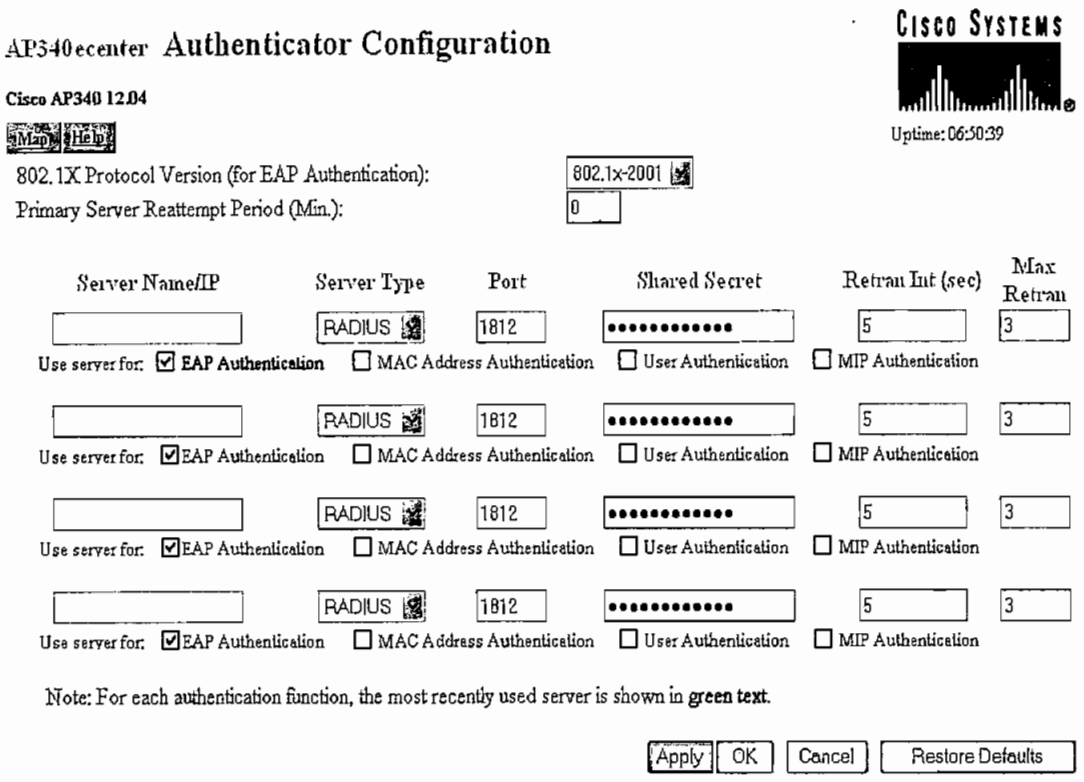


Fig. 4.39 Configuración del servidor RADIUS para el AP

Como se puede apreciar, se tienen 4 espacios para servidores RADIUS, esto es para ofrecer redundancia en caso de fallas y para tener varios tipos de EAP en la WLAN al mismo tiempo.

La opción *802.1X Protocol Version (for EAP Authentication)*, es para elegir el tipo de EAP con compatibilidad con el hardware de la red, por ejemplo si se tienen tarjetas inalámbricas antiguas con *firmware* obsoleto, esta opción permite elegir la compatibilidad de EAP con esos equipos.

En este caso, se realiza una actualización de *firmware* de las tarjetas para poder utilizar toda la potencialidad del hardware, por lo que en esta opción se debe elegir 802.1x-2001 que es la última versión compatible de funcionalidad EAP con el *firmware* actualizado.

La opción *Primary Server Reattempt Period (Min.)* es para establecer un período de reconexión al servidor primario en caso de fallas. En este caso solo se tiene un

servidor RADIUS por lo que esta opción se deja en cero. Por el mismo motivo solo se configura la primera posición para servidor RADIUS. En el campo *Server Name/IP* se coloca el nombre DNS del servidor o la dirección IP del mismo. Para que no exista demora en la resolución del nombre y prevenir fallos en DNS, es recomendable colocar directamente siempre la dirección IP; en la solución la IP del servidor es la 192.168.10.2.

En el campo *Server Type*, se tienen 2 opciones, servidor RADIUS y servidor TACACS, este último es un tipo especial de servidor AAA que tiene disponible Cisco. Para la solución actual se elige la opción RADIUS.

El campo *Port* es el número de puerto mediante el cual se comunican el servidor RADIUS y el AP. El puerto estándar para el protocolo RADIUS es el 1812, sin embargo para propósitos de seguridad es recomendable cambiar este número.

En el servidor se configuró el puerto 516 que está libre según el RFC 1700, por lo cual el mismo puerto debe colocarse en esta opción del AP.

El campo *Shared Secret* es una clave secreta compartida entre el AP y el servidor. Esta clave se utiliza para encriptar las credenciales del usuario que viajan a través de la LAN cableada entre el AP y el servidor.

El AP permite una clave de hasta 64 caracteres alfanuméricos, sin embargo no es recomendable utilizar toda la longitud posible ya que esto demora la comunicación entre el AP y el servidor por el procesamiento requerido. La clave establecida para el servidor y el AP es: q1w2ee.

El tiempo (en segundos) que el AP espera antes de que la autenticación falle se especifica en el campo *Retran Int.* Si el servidor no responde en este tiempo, el AP trata de contactarse con el siguiente servidor en la lista si el mismo se especifica. Como sólo se tiene presente un servidor, este tiempo no es importante y por tanto se lo deja con el valor predeterminado de 5 segundos.

El campo *Max Retran* especifica el número de intentos que el AP realiza antes de rendirse en la autenticación. Se mantiene el valor predeterminado de 3 intentos. En las opciones de *Use server for* solamente se debe seleccionar *EAP Authentication;* la opción de autenticación MAC se realizan en el AP, y las otras dos no son necesarias.

Los campos referentes a los otros 3 servidores se dejan con sus valores por defecto ya que sólo se tiene un servidor presente en la solución.

Con estos cambios la pantalla final de configuración EAP se muestra en la figura 4.40. Se aplican los cambios con *Apply.*

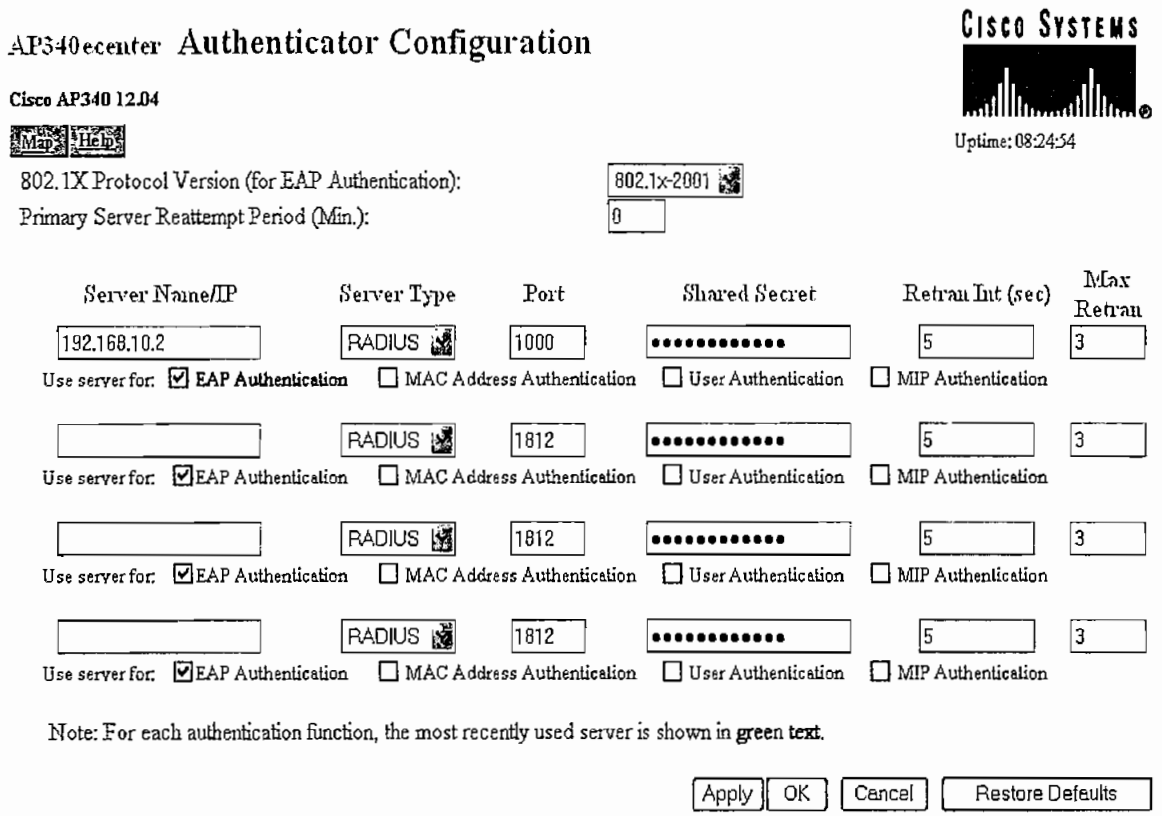


Fig. 4.40 Configuración final del servidor RADIUS para el AP

Con esto finaliza la configuración de EAP en el AP. Se debe aclarar que esta configuración es genérica para cualquier tipo de EAP ya que el caso específico de LEAP es manejado en el servidor RADIUS.

4.6. CONFIGURACIÓN DEL USUARIO CON TARJETA PCMCIA AIRONET 350 CISCO

La instalación de la tarjeta inalámbrica es sencilla, ya que el sistema WXP reconoce automáticamente el hardware. La instalación del software de Cisco de manejo de WLAN´s se explica en el anexo 3. Con estas premisas se empieza directamente con la configuración del software de manejo de WLAN´s para LEAP.

Lo primero es crear un nuevo perfil para el manejo de seguridad LEAP en el utilitario de configuración del fabricante, el ACU.

Para crear el perfil se ingresa a la opción *Profile Manager* en la pantalla principal del ACU, con lo que aparece la pantalla de la figura 4.41.

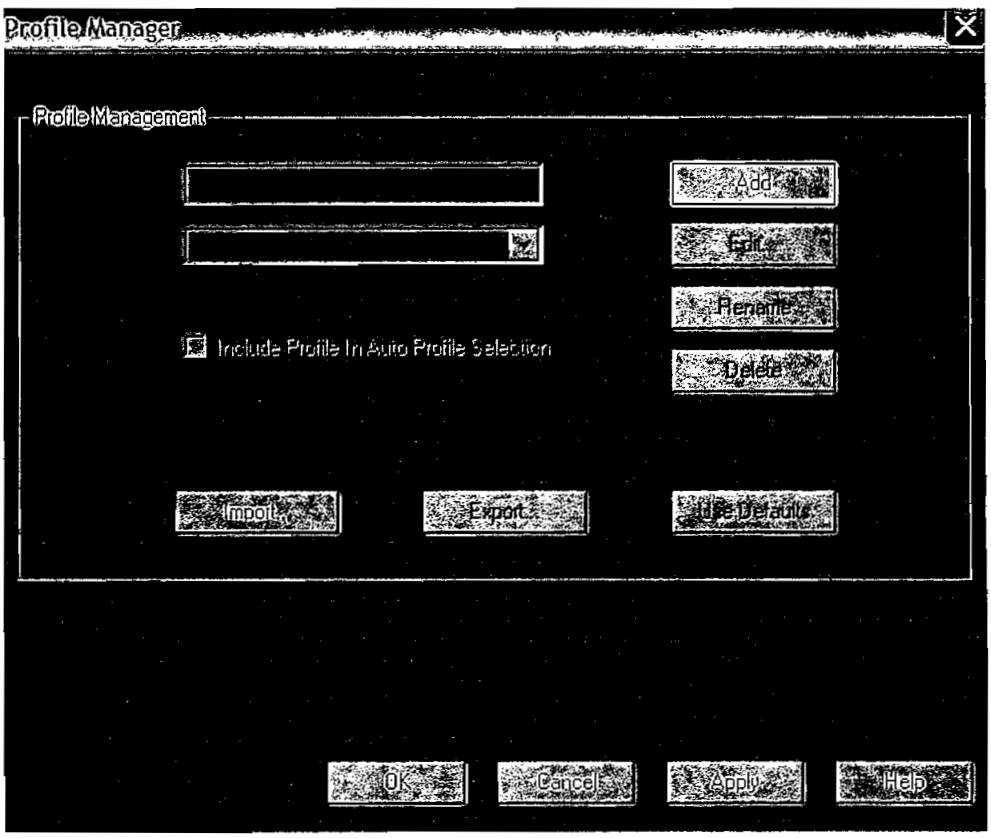


Fig. 4.41 Pantalla de Administración de Perfiles

Se da un clic en *Add* y se asigna un nombre al perfil, en este caso usuarioLEAP, se da clic en *OK* para ingresar a la configuración del perfil en la pantalla de la figura 4.42.

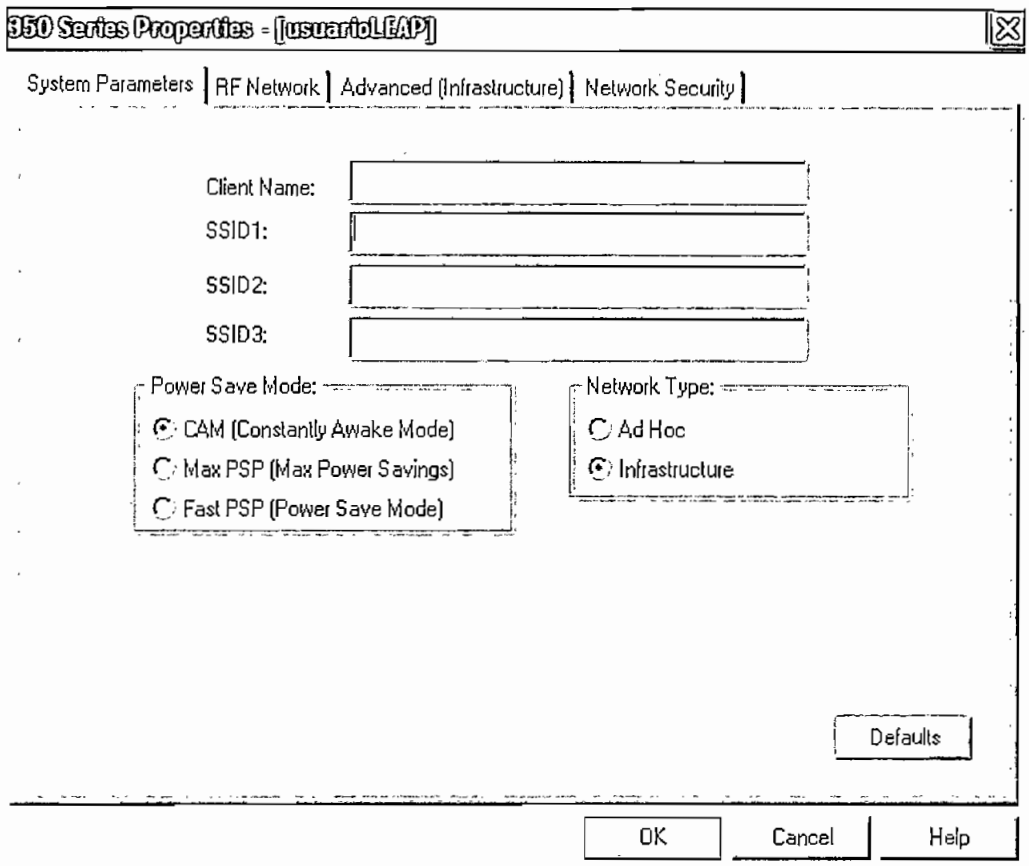


Fig. 4.42 Pantalla de System Parameters

Aparecen las opciones de *System Parameters,* aquí se asigna un nombre al cliente, por ejemplo usuario1, luego se configura el SSID que es 1xWLAN, los demás son parámetros por defecto para el tipo de red. Se elige una WLAN de infraestructura y manejo de la energía tipo CAM (*Constantly Awake Mode*) que indica que las estaciones serán advertidas de eventos en la WLAN. La pantalla final se muestra en la figura 4.43.

Hasta este punto la configuración es la misma que en el caso de WEP. La diferencia fundamental radica en los parámetros de la pantalla *Network Security* mostrada en la figura 4.44.

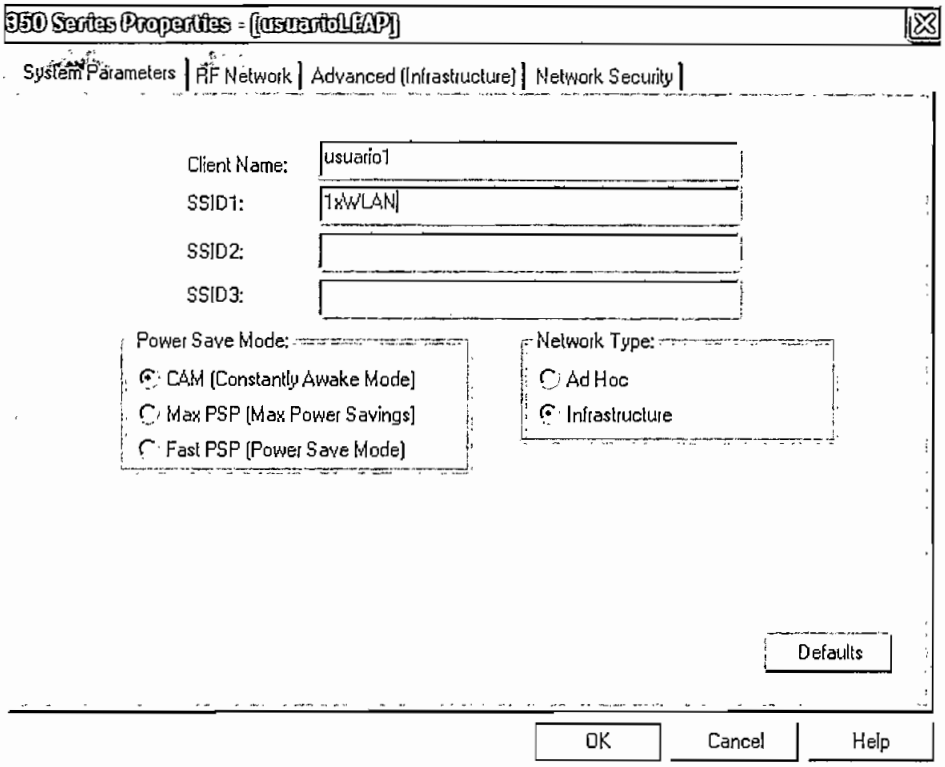


Fig. 4.43 Pantalla de System Parameters final

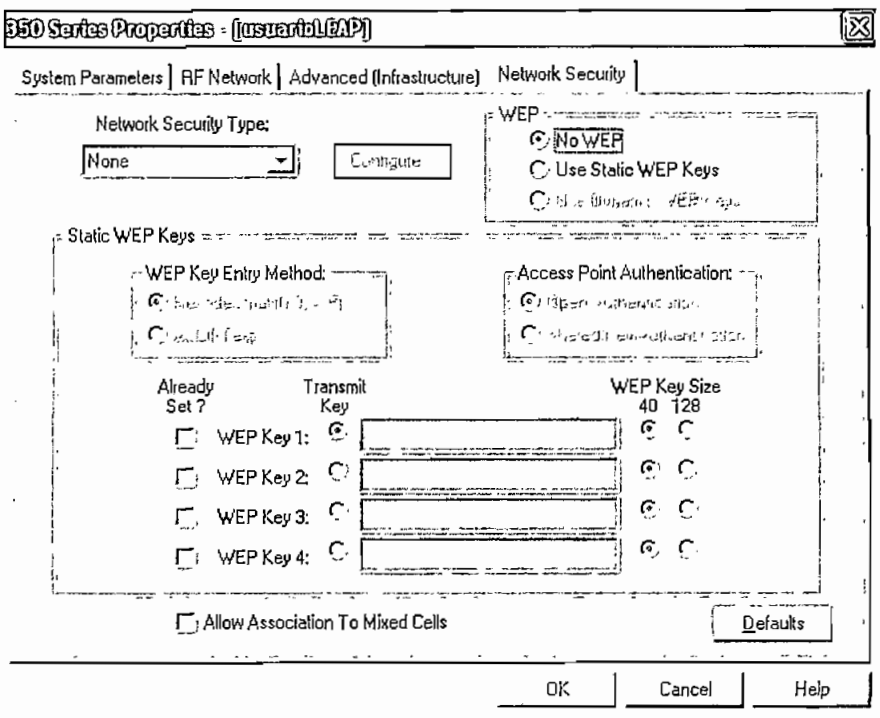


Fig. 4.44 Pantalla de Network Security

En la opción *Network Security Type* se debe elegir la opción LEAP, como se muestra en la figura 4.45, luego para la configuración específica del mecanismo de seguridad se debe ingresar en la opción *Configure,* en la pantalla de la figura 4.46.

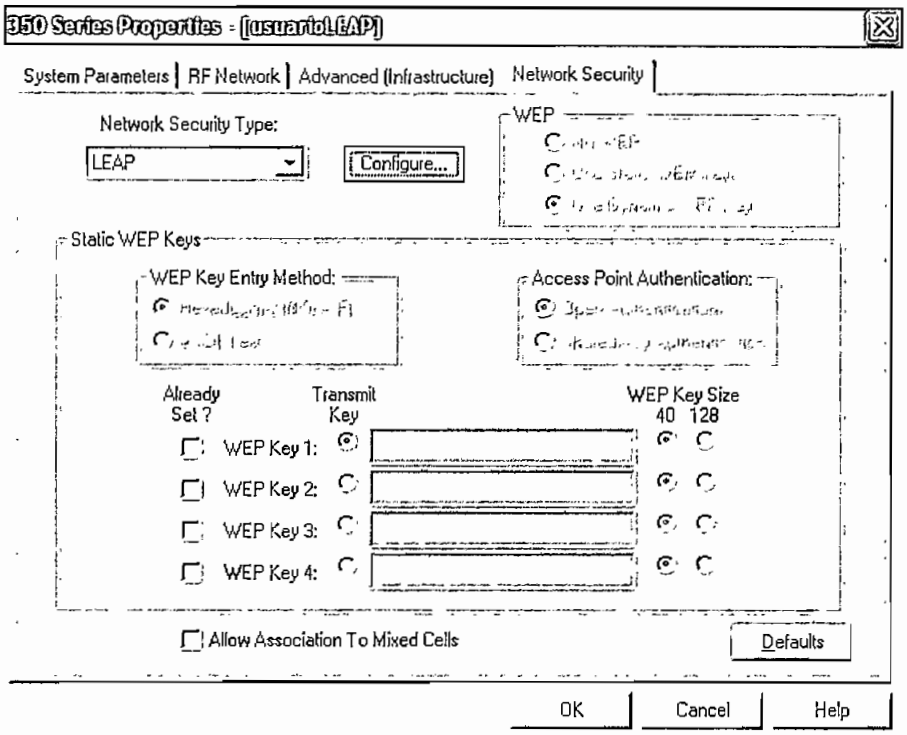


Fig. 4.45 Pantalla principal del ACU con la estación asociada

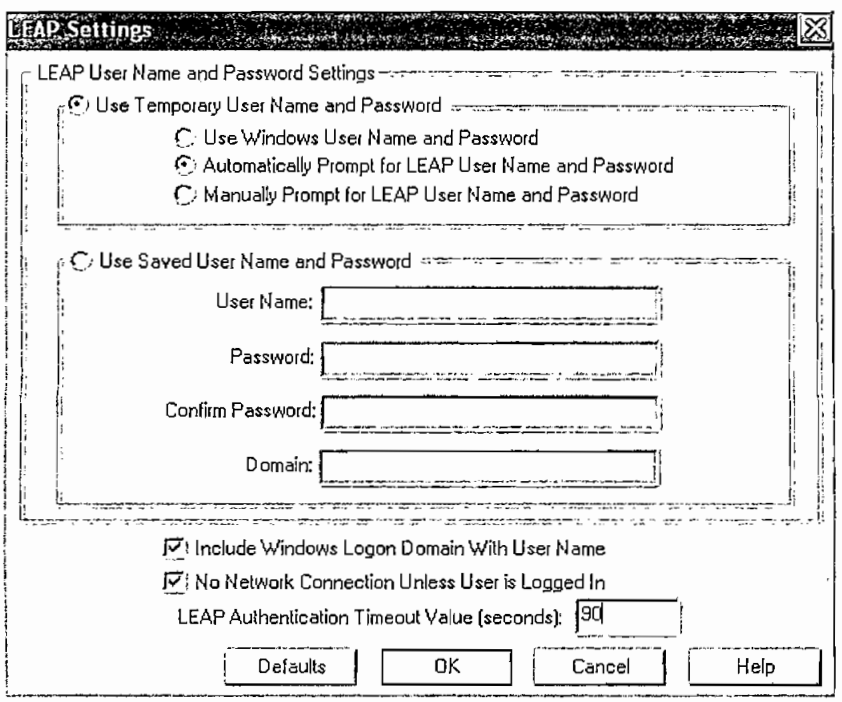


Fig. 4.46 Pantalla de final de Network Security

La pantalla de la figura 4.46 permite configurar la forma específica de presentar las credenciales en la WLAN. Se tienen 2 opciones, la primera es *Use Temporary Username and Password*, que consiste en utilizar un nombre de usuario y contraseña provisionales, aquí a su vez se tienen 3 sub-opciones que son:

- Utilizar las credenciales de usuario de Windows,
- Automáticamente solicitar las credenciales
- Manualmente colocar las credenciales para la validación en la red.

La otra forma de presentar las credenciales es más transparente para el usuario. Es la opción de *Use Saved Username and Password,* que implica almacenar un nombre de usuario y contraseña en la estación para que automáticamente se presente a la WLAN cuando sea necesario, así el usuario no tiene que escribir cada vez que sean requeridas sus credenciales.

Por comodidad de utilización de la WLAN, ésta es la opción más adecuada

Luego se tienen 2 opciones adicionales de configuración.

- La opción *Include Windows Logon Domain With User Name que* añade el dominio de la red de Windows al nombre de usuario. Esto se utiliza cuando se tiene presente un dominio de Windows y el servidor RADIUS integra el dominio en el nombre de usuario.
- La opción *No Network Conection Unless User is Logged In,* que sirve para evitar que se acceda a la WLAN sin que un usuario autorizado ingrese al sistema operativo.

Finalmente se tiene el parámetro *LEAP Authentication Timeout Value (seconds),* que permite especificar el tiempo de respuesta de la WLAN después de que el usuario presenta sus credenciales.

Por ejemplo si la red no está activa este parámetro indica que luego de 60 segundos de no obtener respuesta, el software emitirá un mensaje de fallo de autenticación.

En correspondencia a las necesidades del problema, los parámetros seleccionados para la presentación de las credenciales son los mostrados en la pantalla de la figura 4.47.

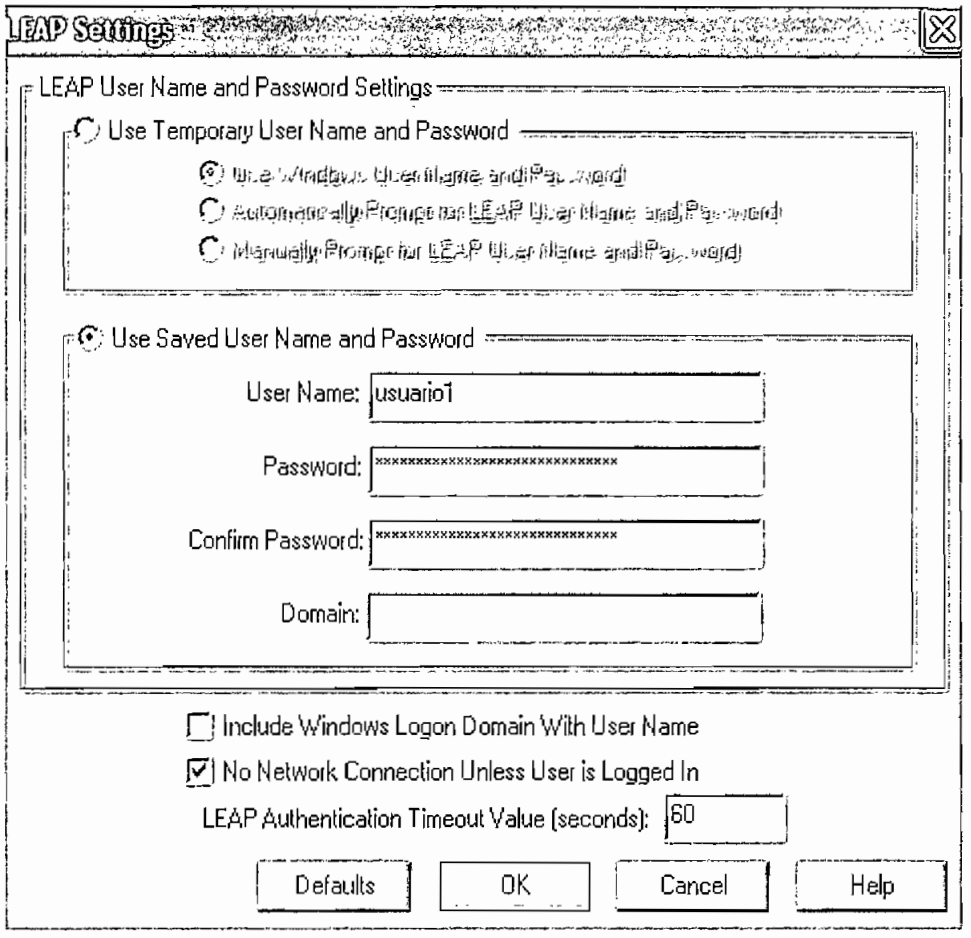


Fig. 4.47 Pantalla de final de Network Security

Para aceptar los cambios se da un clic en OK, luego se retorna nuevamente a la pantalla de la figura 4.48 y se aplican los cambios con un nuevo clic en OK.

Una vez que se tiene el perfil correcto configurado se lo debe aplicar. Para esto se elige la opción *Select Profile* de la pantalla principal, luego de lo cual aparece la pantalla de la figura 4.48.

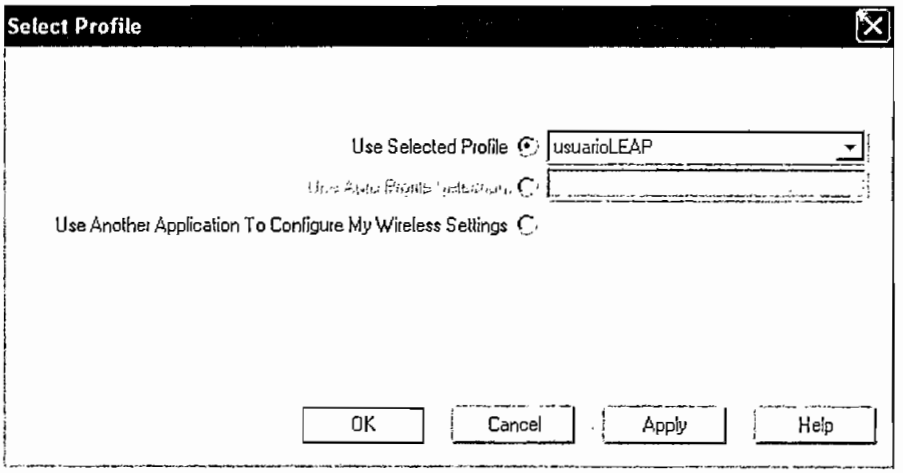


Fig. 4.48 Pantalla Select Profile

Se selecciona el perfil usuarioLEAP creado y se lo aplica con *Apply*. Una vez hecho esto, el sistema empieza el proceso de autenticación LEAP, esto se verifica con la presencia del mensaje de la figura 4.49.

Luego de la negociación de credenciales con el servidor la estación se asocia correctamente lo cual se puede visualizar en la parte inferior de la pantalla principal del ACU como lo indica la figura 4.50.

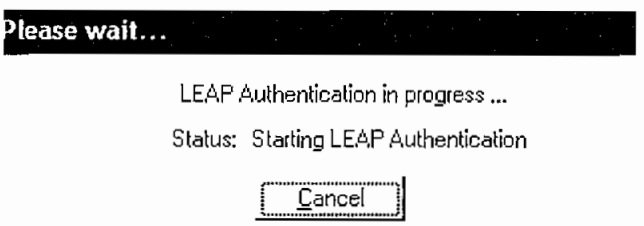


Fig. 4.49 Negociación de credenciales LEAP en proceso

Se puede apreciar que el usuario está asociado al AP con el nombre AP340ecenter y con dirección IP 192.168.10.1. Con esto termina la configuración del cliente inalámbrico con seguridad LEAP. El siguiente paso es la realización de pruebas de conectividad y de seguridad de la red inalámbrica.

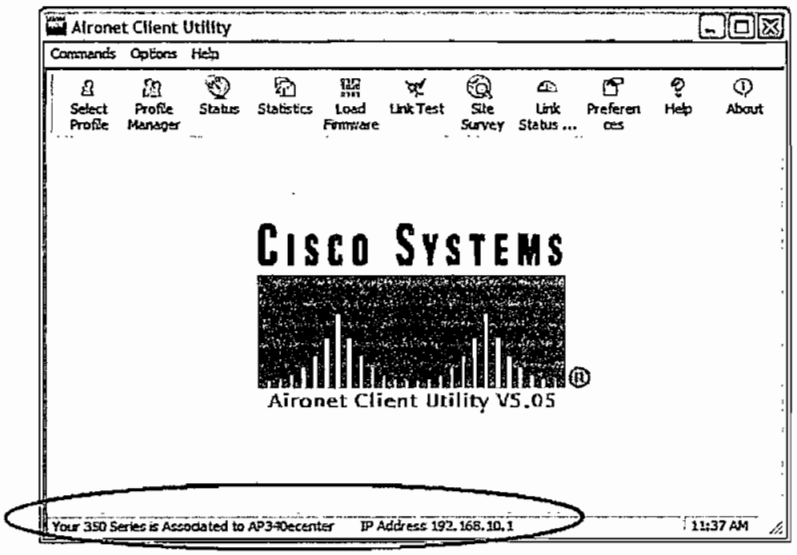


Fig. 4.50 Pantalla principal del ACU con la estación asociada

4.7. PRUEBAS DE FUNCIONAMIENTO

4.7.1. PROCESO DE AUTENTICACIÓN NORMAL

Para esta prueba de funcionamiento se tiene un usuario debidamente autorizado en el servidor RADIUS y con los parámetros de configuración LEAP correctos en el ACU. En la tabla 4.4 se muestra el usuario con sus datos respectivos.

Usuario LEAP autorizado	
Parámetro	**Valor**
Nombre	Usuario1
Contraseña	azsx01
IP	192.168.10.10
MAC	000c859a2120
Seguridad	LEAP
Perfil	usuarioLEAP

Tabla 4.4 Usuario inalámbrico de pruebas

El proceso de autenticación comienza automáticamente después de que el usuario conecta su tarjeta inalámbrica. El software de manejo de WLAN´s empieza la negociación de las credenciales del usuario con la red, esto se puede verificar con la presencia del mensaje de la figura 4.49 en la pantalla. La negociación demora aproximadamente 6 segundos, luego de lo cual el usuario se asocia a la red como lo muestra la pantalla principal del ACU en la figura 4.51 En la pantalla *Link Status Parameters* de la figura 4.52 también se puede observar que el usuario está correctamente asociado y activo.

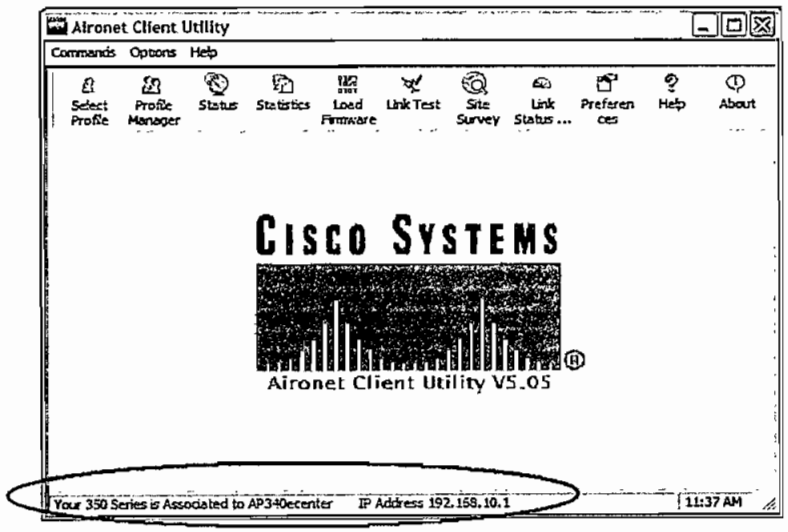


Fig. 4.51 Cliente asociado al AP con LEAP

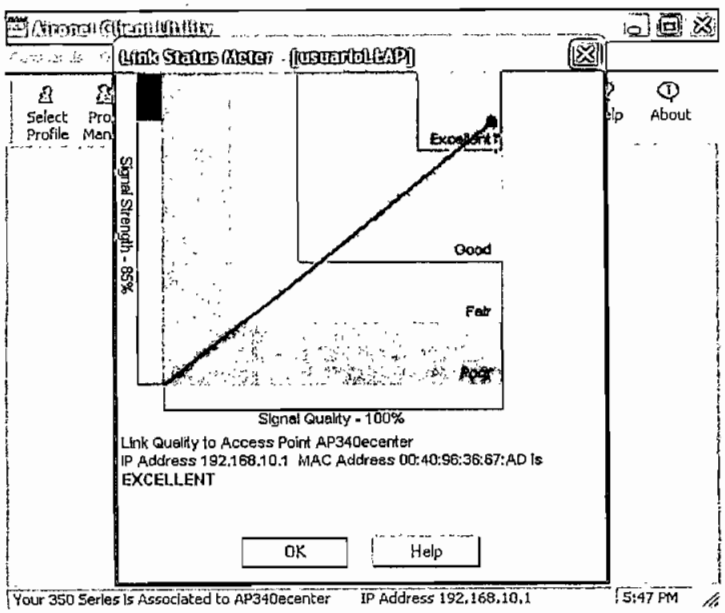


Fig. 4.52 Pantalla Link Status Parameters con la estación asociada

Para observar más información sobre el tipo de conexión que se establece, se puede ingresar a la opción *Status* del ACU, en la pantalla de la figura 4.53. Un resumen sobre los principales parámetros que se muestran en esta pantalla se presenta en la tabla 4.5.

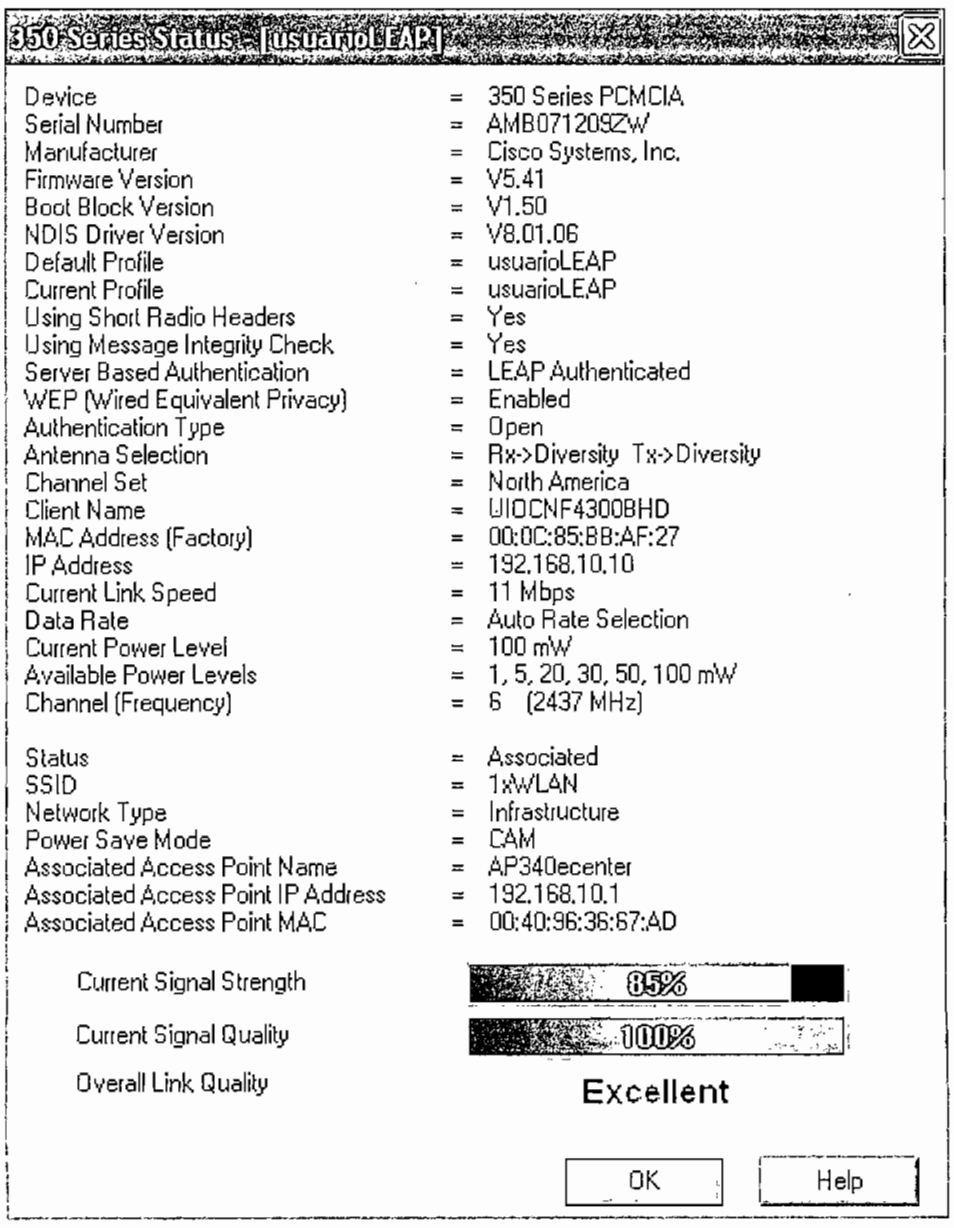


Fig. 4.53 Pantalla principal del ACU con la estación asociada

Parámetros del Enlace	
Tarjeta inalámbrica	350 PCMCIA
Fabricante	Cisco Systems Inc.
Firmware de la tarjeta	V 4.25.30
Perfil utilizado	usuarioLEAP
Seguridad WEP	*Yes*
Autenticación	*Open*
MAC	000c85bbaf27
IP	192.168.10.10
Velocidad del enlace	*11 Mbps*
Potencia de la señal	*100 mW*
Frecuencia	*Canal 6 (2437 Mhz)*
SSID	*1xWLAN*
Tipo de red	*Infraestructura*
Server Based Authentication	*LEAP Authenticated*

Tabla 4.5 Información sobre el enlace inalámbrico del usuario

El cliente también se muestra activo en la pantalla *Home* del AP, como lo muestra la figura 4.54.

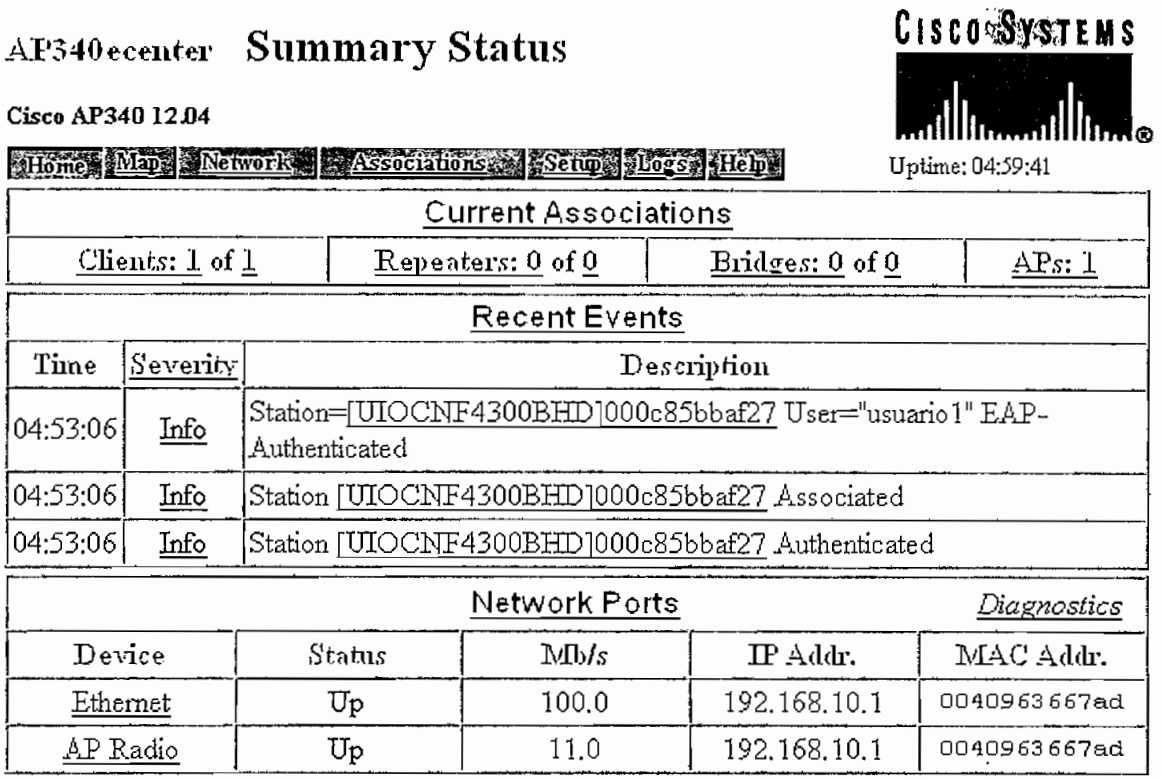


Fig. 4.54 Pantalla Home del AP con el usuario1 asociado

En el AP se presenta información sobre el tipo de usuario que está asociado y su nombre, en este caso usuario1, además se indica que fue autenticado mediante EAP, en particular con LEAP.

Para obtener mayor información sobre el usuario se puede dar un clic en el enlace del nombre del equipo del usuario o en su MAC, luego de lo cual se muestra la pantalla de la figura 4.55.

En la opción *Status* de esta pantalla se muestra la siguiente información: *EAP Authenticated, WEP, Key Permute, MIC, Short Preambles;*esta información indica que se trata de un usuario autenticado con EAP, con llaves WEP dinámicas y con integridad MIC.

La información *Short Preambles* también dice que la estación se conecta con la mayor velocidad posible.

Home | Map | Network | Associations | Setup | Logs | Help — Uptime: 04:59:30

System Name	UIOCNF4300BHD	Device	350 Series Client
MAC Address	00:0c:85:bb:af:27		
IP Address	192.168.10.10		
VLAN ID	0	Policy Grp.	0
State	Assoc, AID=29, SSID=0	Class	Client
Status	EAP Authenticated, WEP, Key Permute, MIC, Short Preambles		

Deauthenticate | Disassociate | Clear Stats | Refresh

Number of Pkts. 5 Pkt. Size 64 Ping

Number of Pkts. 100 Pkt. Size 500 Link Test

To Station		Alert ☐	From Station		Alert ☐
Packets OK	9864		Packets OK	9415	
Total Bytes OK	678690		Total Bytes OK	982643	
Total Errors	4		Total Errors	0	
Max. Retry Pkts.	4				
Short Retries	169		WEP Errors	0	
Long Retries	454				
MIC Packets	708		MIC Packets	706	
MIC Errors	0		MIC Errors	0	
			MIC Sequ. Errors	0	
			MIC Auth. Errors	0	

Parent	[self]	Next Hop	[self]
Current Rate	1.0 Mb/s	Operational Rates	1.0B, 2.0B, 5.5B, 11.0B Mb/s
Latest Retries	31 short, 9 long	Latest Signal Str.	100%

Hops to Infra.	1	Echo Packets	0

Fig. 4.55 Pantalla principal del ACU con la estación asociada

Como prueba de conectividad se puede realizar un *ping* a diferentes sitios de la red. Por ejemplo en la pantalla de la figura 4.56 se muestra el resultado de un *ping* hacia la dirección IP del AP 192.168.10.1 desde la estación del usuario.

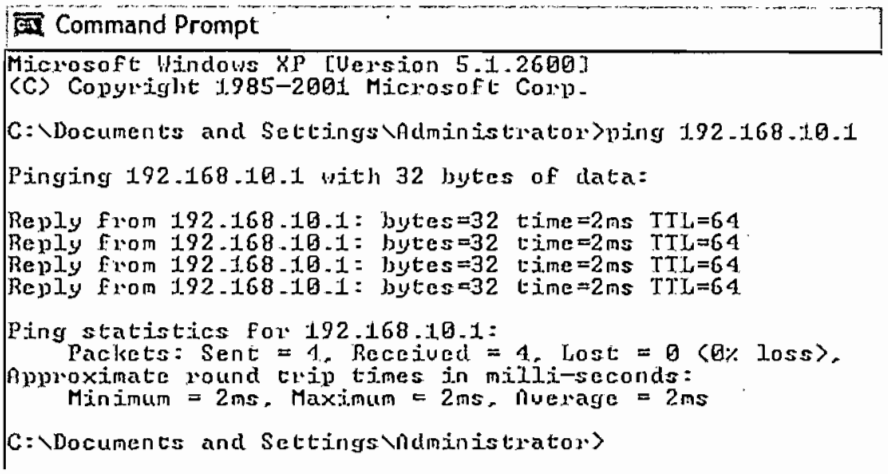


Fig. 4.56 Ping hacia el AP desde el usuario LEAP

Como se puede apreciar los tiempos de respuesta son de apenas 2 ms, un muy buen tiempo para una WLAN. Con esto se verifica una correcta conectividad de radio. Ahora se puede realizar una prueba de conectividad hacia la LAN cableada desde la WLAN, para esto se realiza un *ping* desde la estación hasta el servidor *proxy* de la red con la dirección IP 192.168.10.2, obteniendo el resultado de la figura 4.57.

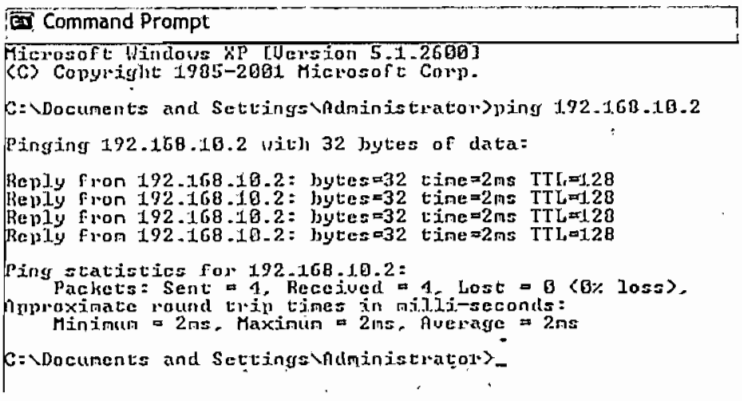


Fig. 4.57 Ping hacia el Servidor Proxy desde el usuario LEAP

Se puede apreciar que el resultado del *ping* es exitoso, obteniéndose respuesta desde el servidor *proxy* con tiempos de 2 ms.

4.7.2. CLIENTE SIN CONFIGURACIÓN DE SEGURIDAD

Ahora se tiene el caso en el que un cliente desea conectarse la WLAN pero no tiene configurado ningún parámetro de seguridad. Por ejemplo su configuración en las opciones de *Network Security* del ACU sería la que se muestra en la figura 4.58.

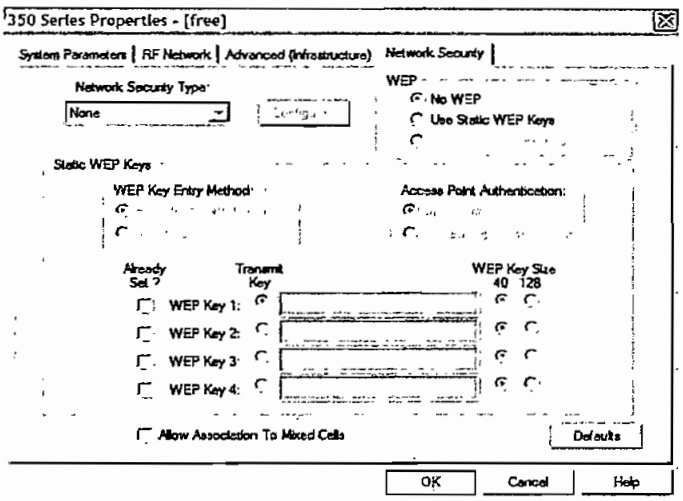


Fig. 4.58 Parámetros Network Security del cliente

Al aplicar esta configuración el usuario no se autentica y por tanto no se puede asociar a la red. Por este motivo la pantalla *Link Status Parameters* es la mostrada en la figura 4.59.

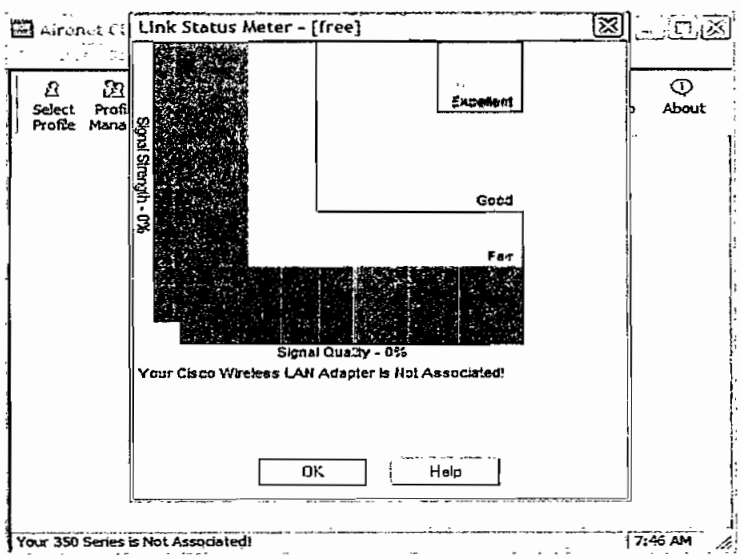


Fig. 4.59 Pantalla Link Status Parameters con la estación no asociada

4.7.3. CLIENTE CON NOMBRE DE USUARIO INCORRECTO

Ahora se tiene un usuario debidamente autorizado, con su MAC acreditada en el AP, con su nombre y contraseña establecidos en el RADIUS y sin ningún parámetro de configuración erróneo, como es el caso del usuario1.

Si al momento de ingresar su nombre de usuario se equivoca e ingresa por ejemplo usuariox en lugar de usuario1, el servidor RADIUS no otorgará el acceso a la WLAN a pesar de tener el resto de parámetros bien configurados.

Para realizar esta prueba se puede utilizar la opción *Manual LEAP Login* del menú *Commands* del ACU, como lo muestra la pantalla de la figura 4.60.

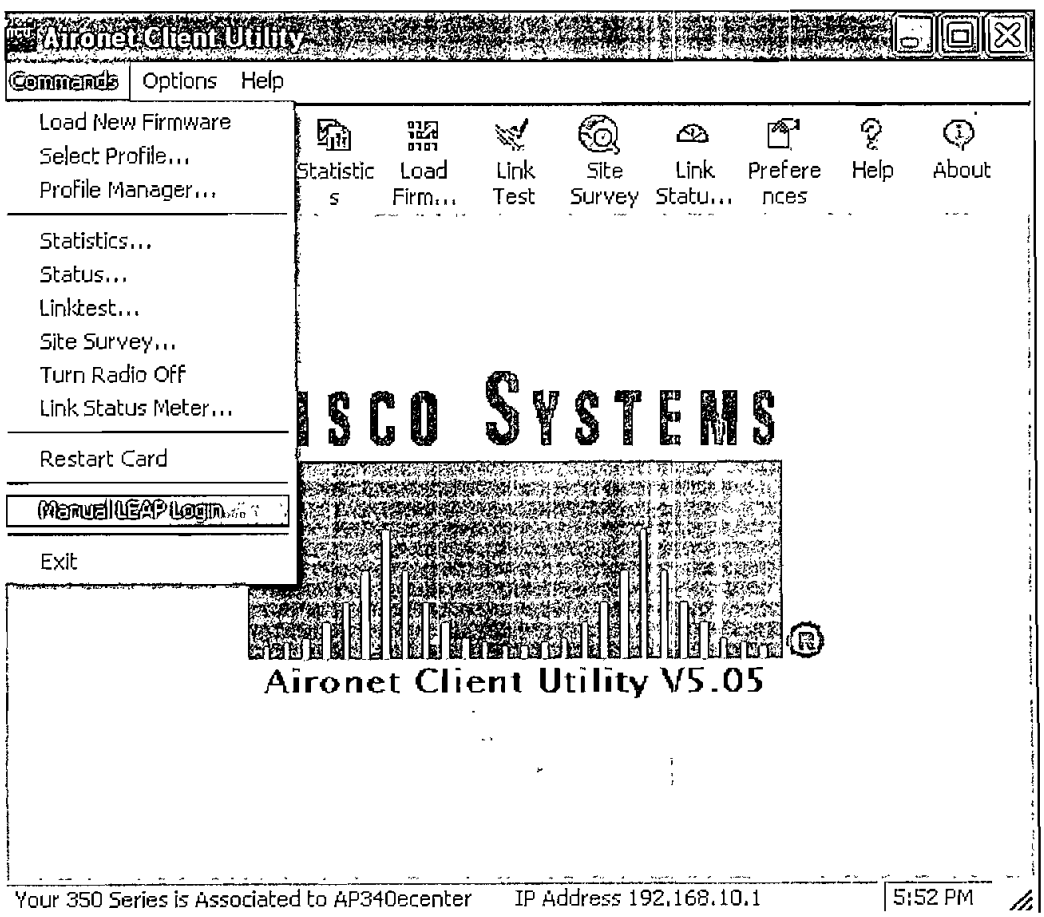


Fig. 4.60 Opción Manual LEAP Login

Luego de esto aparece la pantalla de la figura 4.61 en la que se puede ingresar manualmente el nombre de usuario y la contraseña para acceder a la WLAN. Además también se puede ingresar el dominio en caso de ser requerido. En este caso, en el campo *User name* se ingresa usuariox en lugar de usuario1.

Al aplicar con *OK* este nombre aparece el mismo mensaje de negociación de credenciales de la figura 4.49.

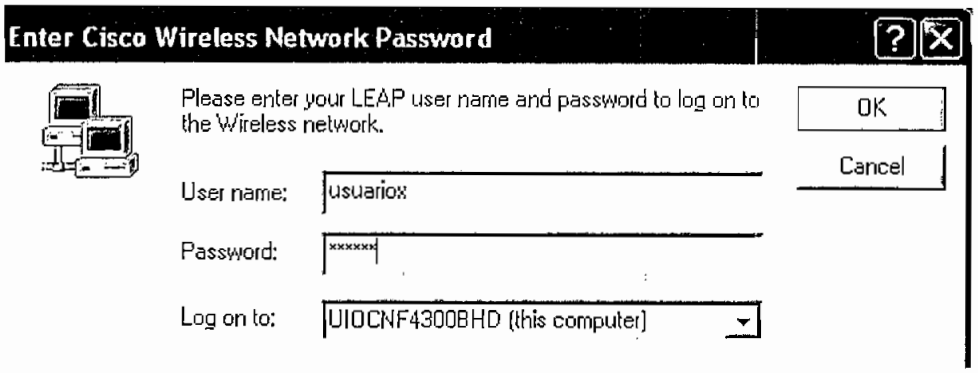


Fig. 4.61 Pantalla Manual LEAP Login del ACU

Luego de unos 8 segundos aparece el mensaje de la figura 4.62, el cual indica que no se logró autenticar al usuario debido a que su nombre o su contraseña no están correctos.

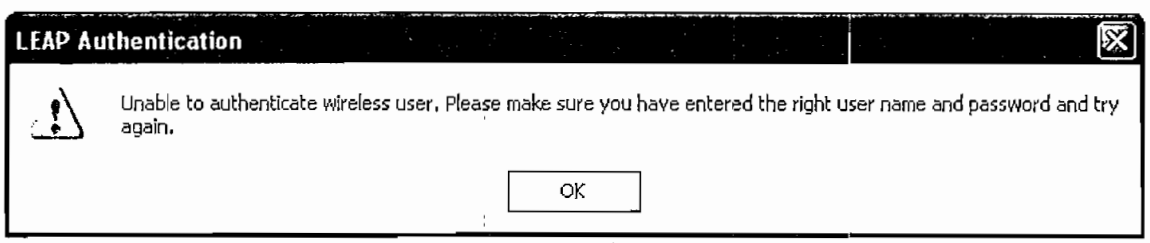


Fig. 4.62 Mensaje de error de autenticación LEAP

En el AP también se registra esta actividad; en la pantalla *Home* de la figura 4.63 se muestra una alerta (*warning*) en la que se indica que un usuario con el nombre usuario1x trato de autenticarse con EAP pero sin éxito.

Home | Map | Network | Associations | Setup | Logs | Help Uptime: 05:13:21

Current Associations

Clients: 1 of 1	Repeaters: 0 of 0	Bridges: 0 of 0	APs: 1

Recent Events

Time	Severity	Description
05:13:00	Warning	Station=[UIOCNF4300BHD]000c85bbaf27 user="usuariox" Failed EAP-Authentication
05:13:00	Info	Station [UIOCNF4300BHD]000c85bbaf27 Associated
05:13:00	Info	Station [UIOCNF4300BHD]000c85bbaf27 Authenticated

Network Ports *Diagnostics*

Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	Up	100.0	192.168.10.1	0040963667ad
AP Radio	Up	11.0	192.168.10.1	0040963667ad

Fig. 4.63 Pantalla Home del AP con registro de un intento fallido de autenticación

4.7.4. CLIENTE CON CONTRASEÑA INCORRECTA

Es un caso similar al anterior, pero en esta ocasión se prueba con el nombre de usuario correcto y la contraseña equivocada, es decir se aplica el nombre usuario1 pero con contraseña azsx0x en lugar de contraseña azsx01.

Se aplican estas credenciales con la opción *Manual LEAP Login* utilizada en el punto anterior, en la pantalla de la figura 4.64.

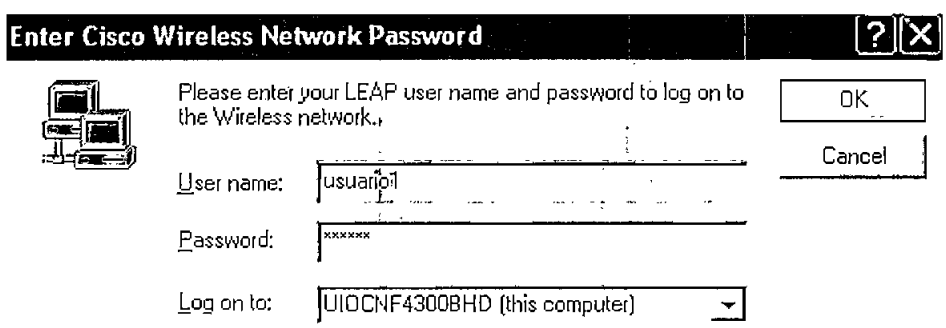


Fig. 4.64 Pantalla Manual LEAP Login del ACU

Una vez aplicadas estas credenciales aparece el mensaje de negociación de credenciales LEAP. Luego de 8 segundos aparece el mensaje de la figura 4.65 en la pantalla que indica que no se logró autenticar al usuario debido a que su nombre o su contraseña no están correctos.

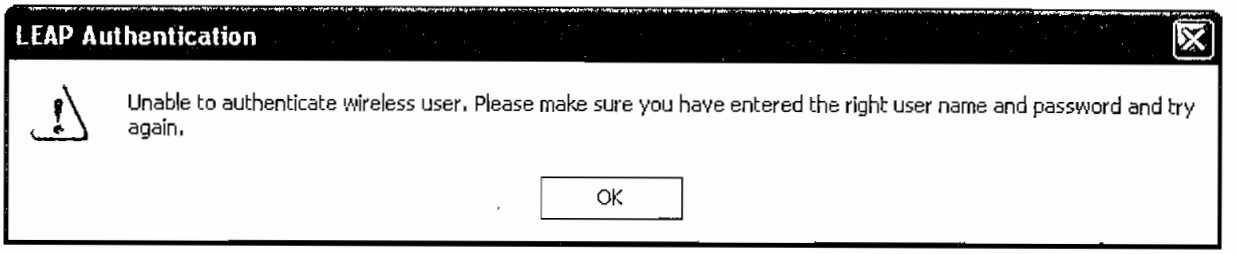


Fig. 4.65 Mensaje de error de autenticación LEAP

De igual forma que en el caso anterior, en el AP también se registra esta actividad; en la pantalla *Home* de la figura 4.66 se muestra la alerta en la que se indica que un usuario trató de autenticarse con EAP pero sin éxito.

Home | Map | Network | Associations | Setup | Logs | Help — Uptime: 05:22:04

Current Associations

Clients: 1 of 1	Repeaters: 0 of 0	Bridges: 0 of 0	APs: 1

Recent Events

Time	Severity	Description
05:21:27	Warning	Station=[UIOCNF4300BHD]000c85bbaf27 user="usuario1" Failed EAP-Authentication
05:21:27	Info	Station [UIOCNF4300BHD]000c85bbaf27 Associated
05:21:27	Info	Station [UIOCNF4300BHD]000c85bbaf27 Authenticated

Network Ports — *Diagnostics*

Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	Up	100.0	192.168.10.1	0040963667ad
AP Radio	Up	11.0	192.168.10.1	0040963667ad

Fig. 4.66 Pantalla Home del AP con registro de un intento fallido de autenticación

4.7.5. CLIENTE SIN MAC AUTORIZADA

Se tiene un usuario autorizado en el RADIUS y con una configuración LEAP correcta; sin embargo su dirección MAC no está autorizada en el filtro del AP. La tarjeta que se utiliza para esta prueba tiene la dirección MAC 000c859a2120 que no está autorizada para ingresar a la WLAN según el filtro que se muestra en la pantalla de la figura 4.67.

Al realizar la prueba de autenticación aparece el mensaje de negociación de credenciales LEAP. En esta ocasión el proceso demora más del promedio de 8 segundos, y en aproximadamente 15 segundos se despliega el mismo mensaje de fallo en la autenticación LEAP de la figura 4.65.

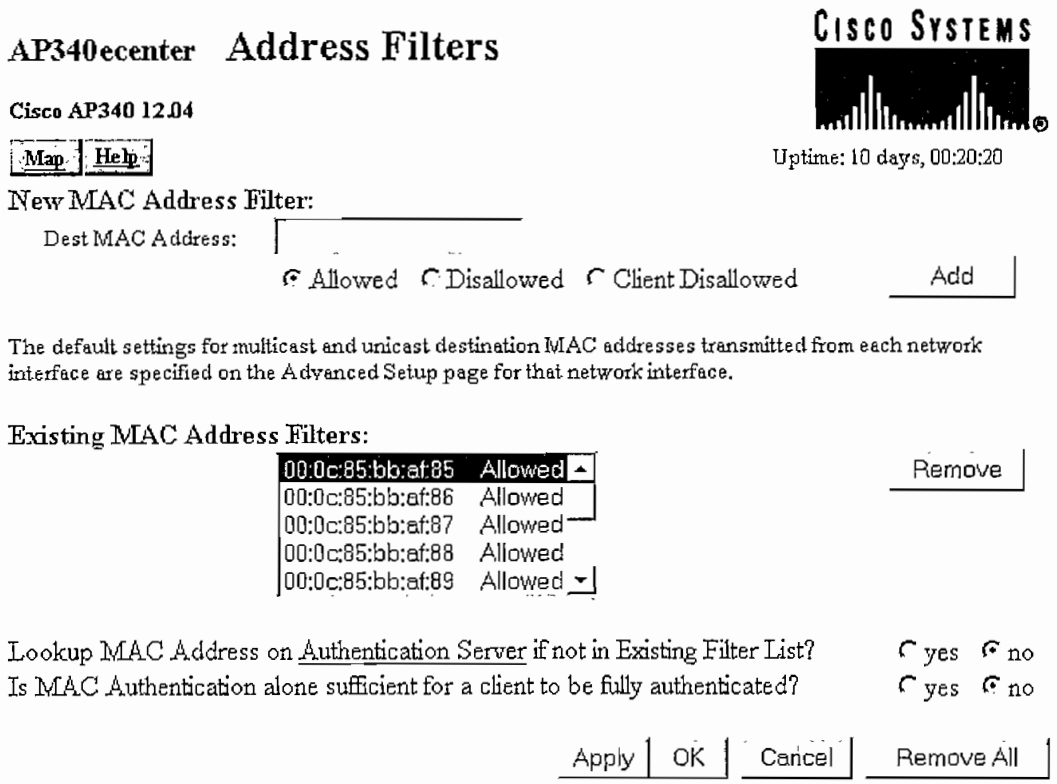


Fig. 4.67 Filtro MAC en el AP

Es el mismo mensaje de error de usuario o contraseña incorrectos, sin embargo el fallo en la autenticación no se debe a ello, sino más bien a que la MAC de la tarjeta utilizada no está autorizada para acceder a la WLAN. En el AP se puede

visualizar este proceso en mayor detalle. En la pantalla *Home* de la figura 4.68 se muestra que efectivamente el usuario fue autenticado y debidamente asociado a la WLAN ya que sus credenciales son correctas. Sin embargo luego de esto se procedió a validar la dirección MAC de la tarjeta del cliente y efectivamente se comprobó que no es una entrada autorizada en el filtro y por tanto el AP procedió a desautenticarla. Por este motivo el usuario no puede asociarse a la WLAN.

Home | Map | Network | Associations | Setup | Logs | Help — Uptime: 05:37:31

Current Associations

Clients: 0 of 1	Repeaters: 0 of 0	Bridges: 0 of 0	APs: 1

Recent Events

Time	Severity	Description
05:37:04	Info	Deauthenticating [UIOCNF4300BHD]000c859a2120, reason "Previous Authentication No Longer Valid"
05:37:04	Warning	EAP retry limit reached for Station [UIOCNF4300BHD]000c859a2120
05:35:34	Info	Station [UIOCNF4300BHD]000c859a2120 Associated
05:35:34	Info	Station [UIOCNF4300BHD]000c859a2120 Authenticated

Network Ports — *Diagnostics*

Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	Up	100.0	192.168.10.1	0040963667ad
AP Radio	Up	11.0	192.168.10.1	0040963667ad

Fig. 4.68 Pantalla Home del AP con registro de un intento fallido de autenticación

4.8. PRESUPUESTO REFERENCIAL

La solución de seguridad con LEAP es por supuesto más costosa que la solución con WEP, esto se debe principalmente a que se incrementa el valor de la licencia del software de servidor RADIUS. En la tabla 4.5 se muestra un desglose del presupuesto final de la solución de una WLAN segura con LEAP. Como se puede apreciar, el costo final de la solución LEAP es 4411 usd, casi el doble del la solución con WEP (2290 usd). No se toma en cuenta el costo del hardware del servidor ya que el mismo se puede instalar sobre una PC de la empresa que cumpla con los requerimientos mínimos.

Ítem	Número de Parte	Descripción	Cantidad	Precio Unitario	Total
1	AIR-AP342EZR-A-K9	Access Point 802.11b, 100 mW, Dual RP-TNC, FCC, incluye 2 antenas dipolares.	1	950*	950
2	AIR-PCM352	Tarjeta PCMCIA 802.11b con antena integrada	10	110*	1100
3	Configuración del AP	Configuración básica del AP	1	40 (1 hora técnica)**	40
4	Configuración del AP	Configuración de seguridad LEAP en el AP	1	40 (1 hora técnica)**	40
5	Configuración de usuario LEAP	Instalación de software y *drivers* en usuarios	10	40 (3 horas técnicas)**	120
6	Configuración de usuario LEAP	Configuración de seguridad LEAP en usuarios	10	40 (1 hora técnica)**	40
7	Servidor *Odyssey* de *Funk Software*	Licencia del servidor RADIUS	1	2000	2081
8	Configuración del servidor	Configuración LEAP en el servidor	1	40 (1 hora técnica)**	40
				TOTAL	**4411**

* Estos precios son ofertados actualmente por Cisco *Systems* Inc. e incluyen el 12% de IVA.

** Se considera el precio en función del número de horas técnicas requeridas, a un precio de 40 usd cada hora técnica.

Tabla 4.5 Presupuesto final para una WLAN con WEP

En el costo total, el precio de la licencia del servidor RADIUS implica cerca del 50 % del costo total de la solución final. Es por ello que se debe tener presente que para una red pequeña no se justifica el nivel de escalabilidad y la facilidad de administración que ofrece el método EAP en general.

En el caso particular del problema planteado, con una WLAN pequeña y con perspectivas de crecimiento, no se justifica realizar la inversión en EAP, ya que por el momento el número de usuarios es pequeño y no es necesario utilizar un método tan escalable de seguridad como lo es LEAP.

En las conclusiones finales del presente trabajo se presenta un análisis más detenido sobre el tipo de solución que se debe elegir para cada situación.

CAPÍTULO 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

5.1.1. *BROADCAST* DEL SSID

Los AP tienen predeterminada de fábrica la opción de emitir el SSID de la WLAN en *broadcast* y en claro hacia su entorno. Esto implica que el AP realmente está emitiendo una invitación para conectarse a su WLAN.

Muchos utilitarios de manejo de WLAN´s tienen la opción de realizar una búsqueda de redes activas detectando los mensajes de *broadcast* del SSID de los AP´s. El mismo utilitario *Windows XP* tiene esta opción. En función de lo mencionado anteriormente, es indispensable desactivar esta opción para mantener el compromiso de seguridad en la WLAN. Es necesario tener claro que mientras más información se proporcione sobre un sistema, más fácil será violentar su seguridad.

5.1.2. COMPATIBILIDAD

Un problema siempre presente en redes inalámbricas es la compatibilidad entre equipos de diferentes fabricantes. Funcionalidades como TKIP y MIC pueden ser soportadas por una marca y por otra no. Debido a esto es necesario elegir con precaución el *hardware* y el software a utilizarse en la WLAN.

Se tiene que recopilar información de manuales de los fabricantes y de diseños anteriores con equipos similares. No es buena idea dejarse llevar sólo por el precio, ya que por un costo adicional se puede tener garantía de compatibilidad,

actualizaciones de *firmware* y *drivers* gratis y un buen soporte, como es en el caso de equipos Cisco Aironet.

De ser posible, se deben realizar pruebas preliminares para verificar el desempeño y compatibilidad de los equipos de redes inalámbricas.

5.1.3. COSTOS Y APLICACIONES PRÁCTICAS DE WEP Y LEAP

Las soluciones para una red inalámbrica segura con WEP y LEAP tienen diferentes áreas de aplicación y por tanto una considerable diferencia económica en su implementación.

La solución WEP es sencilla y rápida de instalar ya que sólo implica la configuración de las tarjetas inalámbricas y del AP. Sin embargo este método no ofrece escalabilidad. Por ejemplo si se desea cambiar la clave WEP, se deben configurar todos los AP´s de la red, y realizar el cambio de clave en todos los usuarios inalámbricos.

Debido a esto, la solución WEP es para ambientes pequeños y medianos, por ejemplo en hogares, en oficinas y en pequeñas empresas. En estos sitios no se requiere métodos de seguridad que ofrezcan una gran escalabilidad y facilidades de administración ya que la infraestructura inalámbrica instalada no es muy grande. Además por el tamaño del negocio no se justifica la inversión en un mecanismo de seguridad tan resistente y escalable como lo es LEAP.

La solución LEAP, en cambio, es un método de seguridad muy escalable y de fácil administración. La distribución de claves es automática y se tiene un mecanismo central de administración de usuarios en el servidor RADIUS.

Por ejemplo, si se tiene un usuario autorizado que se desea dar de baja, simplemente se lo retira en el servidor y no es necesaria una actualización de toda la infraestructura inalámbrica instalada.

Por supuesto la escalabilidad ofrecida por LEAP implica un costo económico adicional considerable (cerca del 50 % más que WEP), tanto en instalación como en mantenimiento.

Por estas razones la solución de una red inalámbrica segura con LEAP está dirigida a medianas y grandes empresas donde se manejan redes inalámbricas de mayor tamaño. Inclusive se puede tener el caso de redes inalámbricas distribuidas geográficamente, en las que se requiere que los usuarios puedan asociarse utilizando siempre sus mismas credenciales.

En definitiva la respuesta a la interrogante de qué protocolo de seguridad utilizar en la red inalámbrica? es: "depende". En la tabla 5.1 se muestra un resumen comparativo de los entornos de seguridad de WEP y LEAP.

Parámetro	WEP	LEAP
Nivel Escalabilidad	bajo	Alto
Facilidad Administración de Usuarios	NO	SI
Costo de Instalación	Bajo	Alto
Costo de Mantenimiento	Alto	Bajo

Tabla. 5.1 Comparación WEP - LEAP

5.1.4. *LOGS* Y SU IMPORTANCIA

Los *logs* o archivos de registro de eventos, son una buena herramienta para detectar actividad sospechosa en la WLAN y para obtener información sobre la utilización de la WLAN. En función de los *logs* se pueden tomar medidas para precautelar la seguridad de la WLAN y para mejorar el rendimiento. Ya en la práctica, en lo que se refiere a seguridad, lo que se debe buscar en los *logs* es eventos fallidos de autenticación que indicarían que un *hacker* está tratando de

encontrar vulnerabilidades en la red o que un usuario está mal configurado. En la tabla 5.2 se muestra una parte del archivo de eventos del servidor RADIUS Odyssey.

Número de Evento	Fecha, Hora y Descripción del evento
1	Sep 26 16:12:46 2004: No server certificate or invalid server certificate; TLS and TTLS disabled.
2	Sep 26 16:12:46 2004: No server certificate or invalid server certificate; TLS and TTLS disabled.
3	Sep 26 16:12:46 2004: Odyssey Server starting.
4	Sep 26 16:33:57 2004: User explicitly allowed; 'usuario1' accepted.
5	Sep 26 17:51:02 2004: User explicitly allowed; 'usuario1' accepted.
6	Sep 26 17:51:02 2004: User explicitly allowed; 'usuario1' accepted.
7	Sep 26 17:56:21 2004: User explicitly allowed; 'usuario1' accepted.
8	Sep 26 17:56:53 2004: User explicitly allowed; 'usuario1' accepted.
9	Sep 26 18:06:44 2004: User explicitly allowed; 'usuario1' accepted.
10	Sep 26 18:07:13 2004: User explicitly allowed; 'usuario1' accepted.
11	Sep 26 18:07:37 2004: User explicitly allowed; 'usuario1' accepted.
12	Sep 26 18:07:48 2004: User explicitly allowed; 'usuario1' accepted.
13	Sep 26 18:11:18 2004: User is not in any allowed group; 'usuariox' rejected.
14	Sep 26 18:15:23 2004: User explicitly allowed; 'usuario1' accepted.
15	Sep 26 18:15:31 2004: User explicitly allowed; 'usuario1' accepted.

Tabla. 5.2 Archivo log del servidor RADIUS Odyssey

Se puede apreciar en la entrada 4, que el día 26 de septiembre del 2004 a las 16:33, se asoció el cliente con nombre "usuario1". En el registro también se indica que el cliente tenía las credenciales correctas y por tanto fue aceptado (*accepted*).

Por el contrario en la entrada 13 se aprecia que el día 26 de septiembre del 2004 a las 18:11, ocurrió un intento de asociación a la WLAN por parte de un cliente con nombre de usuario "usuariox". Sin embargo las credenciales no fueron las correctas y por tanto el usuario fue rechazado (*rejected*).

Con un análisis sencillo de la información de los *logs* se puede detectar la actividad sospechosa y por tanto tomar las medidas respectivas.

5.1.5. LA SEGURIDAD COMO PROCESO DINÁMICO

La seguridad en redes inalámbricas no es un proceso estático que termina con la implementación de un determinado mecanismo de seguridad. El proceso debe ser continuo y dinámico, con pruebas de funcionamiento periódicas y actualización permanente de las medidas de seguridad del sistema. Incluso se debe tomar en cuenta el cambio total de mecanismo de seguridad debido a la aparición nuevas vulnerabilidades o al desarrollo de mejores estándares.

Por ejemplo WEP, que hasta hace unos 4 años era considerado un mecanismo que brindaba suficiente seguridad a las WLAN´s, hoy ya no lo es. Si no fuera por las nuevas herramientas desarrolladas continuamente como TKIP, EAP, etc, las WLAN´s no habrían podido seguir siendo utilizadas.

Los administradores tienen un gran compromiso en mantener actualizados sus sistemas de seguridad y someterlos periódicamente a pruebas que verifiquen que el sistema efectivamente sigue siendo seguro.

5.1.6. TKIP

TKIP es el desarrollo principal de la *Wi-Fi Alliance* en materia de seguridad. Gracias a este esfuerzo de los fabricantes se logró que WEP pueda seguir siendo utilizado corrigiendo sus vulnerabilidades.

Las vulnerabilidades en el diseño de WEP en comparación con TKIP son:

- Clave secreta demasiado pequeña (64 bits).
- La integridad solo se verifica con un simple CRC.

- Clave estática, la misma para todos los dispositivos.
- Vector de inicialización (IV) demasiado corto y vulnerable de predicción.

TKIP corrige esto mediante:

- Clave secreta más grande de 128 bits
- Integridad de mensaje criptográfica con la clave compartida y no con un simple CRC.
- Clave dinámica, por paquete enviado.
- Vector de inicialización más grande (48 bits) y con disciplina de secuenciamiento.

Gracias a estas mejoras, WEP con mejora TKIP, ha podido seguir siendo el mecanismo de seguridad más utilizado en ambientes caseros y pequeñas empresas.

5.1.7. SERVIDOR RADIUS

Para el caso de una empresa grande, se tiene seguramente una infraestructura de servidores bastante completa. Por ello no es difícil implementar el servicio RADIUS en una de sus infraestructuras para propósitos de seguridad WLAN. El costo adicional de mantenimiento y administración no sería significativo y por tanto una empresa grande puede decidirse fácilmente por mecanismos de seguridad 802.1x.

5.1.8. EXPANSIÓN DE LAS REDES INALÁMBRICAS

Gracias a los avances en materia de seguridad inalámbrica, las WLAN´s han podido seguir siendo utilizadas con gran confiabilidad. Sin embargo el

desconocimiento de las nuevas herramientas de seguridad y la falta de políticas de administración básicas, a hecho que las empresas se sientan desconfiadas de utilizar esta importante tecnología. En la actualidad esto está cambiando, la información sobre la tecnología inalámbrica está mas a la mano y los beneficios que ofrece llegan a ser indispensable para las necesidades de negocios.

5.2. RECOMENDACIONES

5.2.1. POLÍTICA DE SEGURIDAD

Si bien el objetivo principal del presente trabajo no es definir formalmente la política de seguridad de la red inalámbrica, se han desarrollado y analizado varios aspectos que se deben ser considerados en la misma. En la tabla 5.3 se presentan algunas recomendaciones que deben ser tomadas en cuenta en la política de seguridad de la WLAN.

5.2.2. FILTRADO DE PROTOCOLOS

El filtrado de protocolos permite o niega el uso de un protocolo específico a través del AP. Además, estos filtros se aplican independientemente en las 2 interfaces del AP, en la interfaz LAN de radio y en la interfaz LAN cableada.

Esto permite por ejemplo, filtrar SNMP en la interfaz de radio para evitar que los usuarios inalámbricos puedan usar SNMP con el AP, pero no se impide que se pueda hacer SNMP al AP desde la LAN cableada.

El filtrado de protocolos a más de servir como una medida de seguridad en la WLAN, también sirve para manejar el desempeño de la red. Por ejemplo si se tienen demasiados usuarios en la WLAN y se desea que no se sature la red con protocolos que inunden la red de tráfico, se los puede deshabilitar.

№	Política	Objetivo
1	Eliminación del *broadcast* del SSID	Evitar que el SSID de la red se propague por el área de cobertura, invitando a estaciones extrañas a asociarse.
2	Filtrado MAC	Permitir que solamente el *hardware* autorizado tenga acceso a la WLAN.
3	Actualización periódica de *drivers* y *firmware* de los equipos	Añadir nuevas funcionalidades a los equipos y cubrir agujeros de seguridad.
4	Restringir el acceso de configuración de los equipos	Impedir que personas extrañas puedan acceder a los equipos y realizar cambios en su configuración.
5	Política de contraseñas fuerte	Para evitar que los usuarios utilicen contraseñas fáciles de recordar o que sean referentes a la empresa
6	Filtrado de protocolos	Para que solamente el tráfico autorizado puede estar presente en la WLAN.
7	Limitar el área de cobertura	Asegurarse de que solamente el área necesaria tenga cobertura inalámbrica y así evitar que en áreas exteriores las señales se propaguen.
8	Registro consistente de usuarios autorizados	Permanentemente poseer una lista de acceso actualizada con los usuarios autorizados.
9	Pruebas periódicas de funcionamiento y seguridad	Establecer cronogramas de pruebas de funcionamiento de la WLAN para tratar de descubrir posibles nuevas vulnerabilidades.

Tabla. 5.3 Recomendaciones para una política de seguridad en la WLAN

Por ejemplo, es muy práctico deshabilitar el uso del protocolo NetBios[1] en la WLAN ya que inunda la red con *broadcast*. A continuación se muestra el

[1] Protocolo de Microsoft que permite compartir archivos en red, entre otras tareas; su característica principal es que emite mensajes de *broadcast* antes de establecer las sesiones entre los usuarios.

procedimiento para establecer este filtrado. Primero se debe ingresar a la opción *Protocol Filters Setup* de la pantalla de *Setup* en el AP, tal como lo muestra la figura 5.1. Luego se muestra la pantalla de la figura 5.2. En esta pantalla se tienen 3 tipos de filtros:

- *Ethertype Filters* .- Filtros a nivel de capa de enlace, por ejemplo ARP[1]
- *IP Protocol Filters* .- Filtros de capa de red, por ejemplo ICMP[2]
- *IP Port Filters* .- Filtros a nivel de capa de transporte, como el NETBIOS Session Service

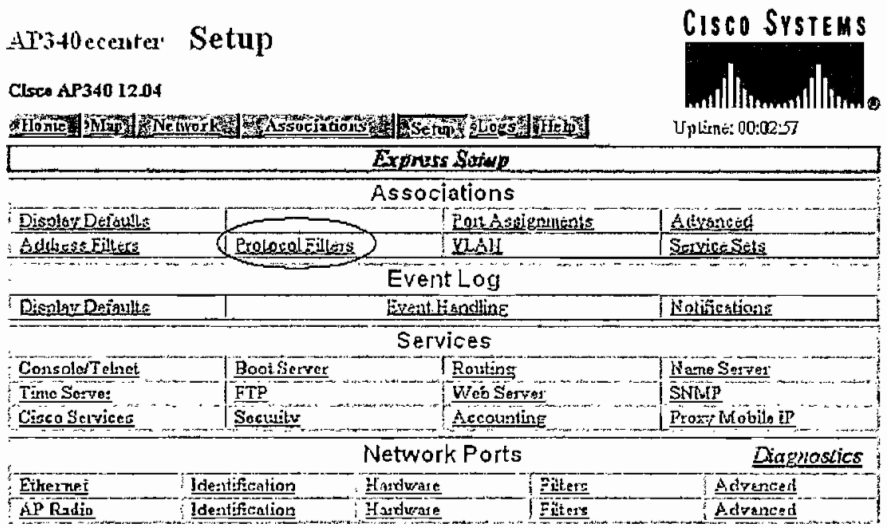


Fig. 5.1 Opción de filtrado de Protocolos en el AP

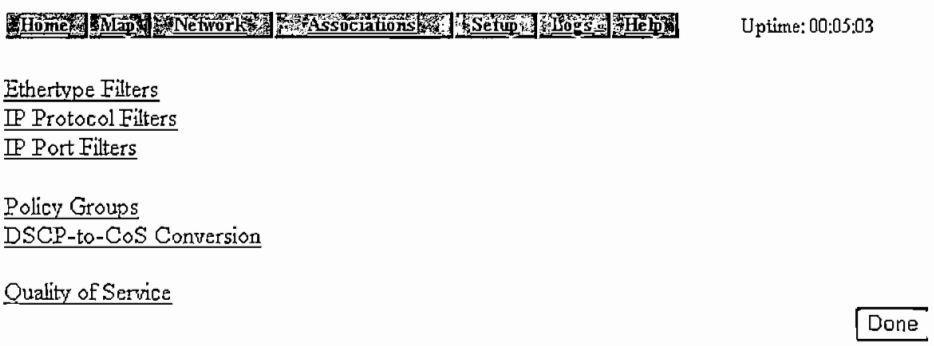


Fig. 5.2 Pantalla principal de filtrado de protocolos en el AP

[1] *Address Resolution Protocol,* resuelve la dirección MAC en función de la dirección IP
[2] *Internet Control Message Protocol,* permite enviar mensajes de prueba a las estaciones y recibir su eco.

Se elige la opción *IP Port Filters* para configurar el filtro de sesiones *Netbios*. A continuación se despliega la pantalla de la figura 5.3 en la que se ingresa un identificador del filtro y su nombre, en esta caso se elige el identificador *10* y el nombre *netbios*. Se continúa la configuración con la opción *Add New*. A continuación aparece la pantalla de la figura 5.4.

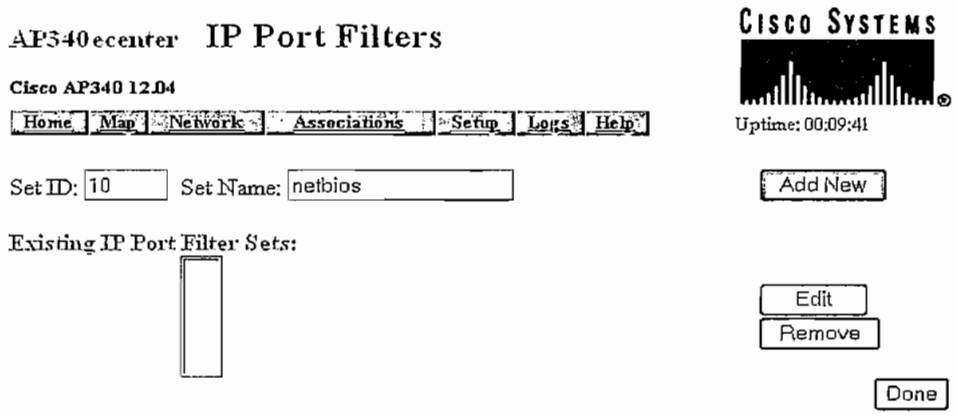


Fig. 5.3 Configuración de filtrado netbios

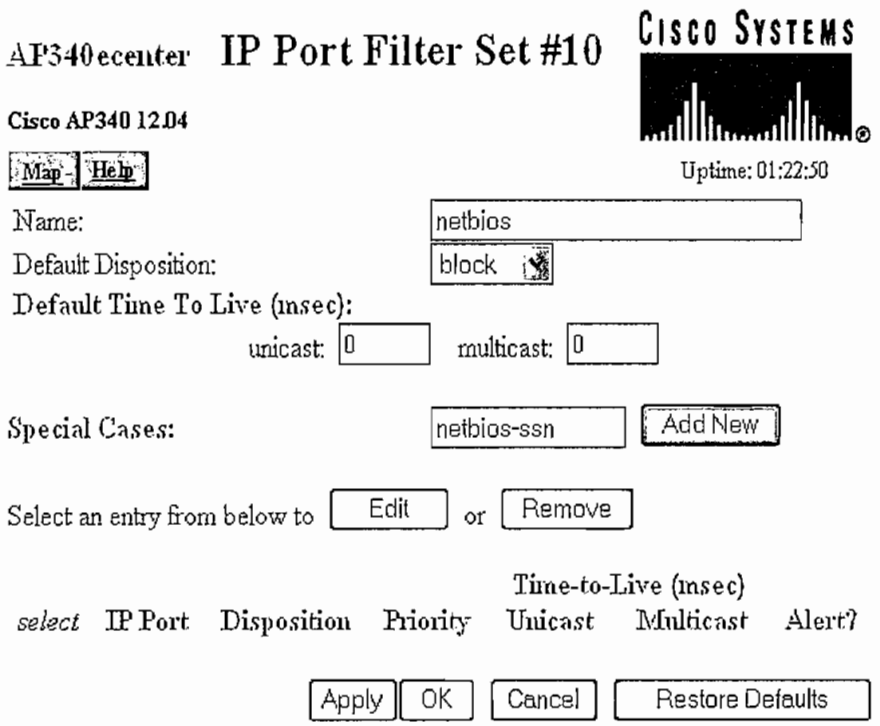


Fig. 5.4 Configuración específica del filtro nuevo

En la opción *Default Disposition* se elige *block* para que el tipo de tráfico definido no pueda pasar por el AP. En los campos *unicast* y *multicast* se configura el *Default Time to Live* que es el tiempo en milisegundos que los paquetes se mantienen almacenados en el *buffer* del AP antes de que éstos sean descartados.

En el campo *Special Cases* se debe colocar el número de puerto que utiliza el protocolo que se desea filtrar o el nombre ISO[1] del mismo. En el caso de las sesiones *Netbios* el puerto es el 139 y el nombre ISO es *netbios-ssn*. Para continuar se da un clic en *Add*. Luego se despliega la pantalla de la figura 5.5.

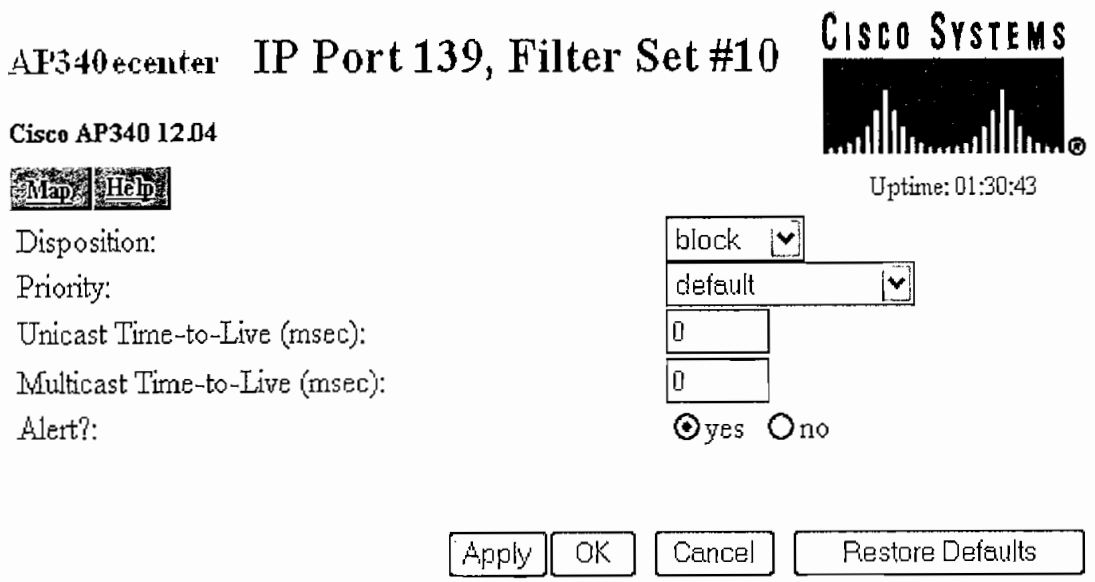


Fig. 5.5 Configuración específica del filtro Netbios

En esta pantalla se vuelve a configurar los parámetros ya mencionados anteriormente y además el tipo de prioridad. Este parámetro se lo deja en la prioridad por defecto.

También se puede elegir la opción de que el AP emita una alerta cada que el filtro se aplica. Finalmente se guarda el filtro con *OK*.

---

[1] *International Standard Organization*

5.2.3. FACILIDADES ADMINISTRATIVAS

Un factor fundamental al momento de decidir la marca de equipos que se utilizará en la WLAN, es la facilidad de administración que los mismos ofrecen. La marca Cisco Aironet, utilizada en las implementaciones inalámbricas del presente trabajo, brinda opciones de administración y configuración sencillas y muy prácticas.

Por ejemplo el hecho de poder importar y exportar el perfil de configuración de un usuario inalámbrico, evita que los parámetros de la red como su SSID, clave WEP, etc, tengan que ser configurados nuevamente en los nuevos usuarios.

Otra facilidad de administración que ofrece Cisco Aironet es la posibilidad de obtener un archivo de configuración del AP para luego aplicarlo a otro AP. Esto es muy práctico en casos en los que se requiera expandir el área de cobertura de la WLAN con otro AP, así ya no es necesario configurar todos los parámetros del nuevo AP. Por lo tanto se recomienda tomar en cuenta las facilidades administrativas de los equipos antes de decidirse por una marca.

5.2.4. DISEÑO WLAN Y SIMULACIÓN

Es común en el desarrollo de diseños WLAN realizar simulaciones previas a la implementación de una determinada solución. Se debe poner especial énfasis en el área de cobertura, desempeño y seguridad de la WLAN.

Existe bastante *software* en el mercado que permiten desarrollar una simulación completa y cercana de la realidad. Sin embargo esto no implica que las pruebas de campo con equipos temporales no se deban desarrollar. Por ejemplo en las simulaciones pueden no ser contemplados problemas como fuentes externas de interferencia, sobrecarga de tráfico de la red, ataques de negación de servicio frecuentes, etc.

En definitiva la única forma de asegurar un adecuado desempeño y seguridad de la WLAN es realizando pruebas prácticas y continuas.

5.2.5. SOLUCIONES CON OTROS FABRICANTES

La infraestructura que ofrece CISCO para redes inalámbricas es bastante completa y robusta, pero también puede ser más costosa que otras marcas. Es posible encontrar desempeño adecuado y precio más económico con otras marcas. Por ejemplo el fabricante D-Link ofrece tarjetas inalámbricas PCMCIA 802.11b a 40 usd, aproximadamente la tercera parte del costo de una tarjeta Cisco Aironet.

Por supuesto, la decisión final depende de varios factores a parte del económico, por ejemplo la confiabilidad, el desempeño, la cobertura, etc.

5.2.6. EL FUTURO DE LA SEGURIDAD INALÁMBRICA: 802.11i

Para finales del presente año se espera que esté listo definitivamente el estándar 802.11i es el esfuerzo final para brindar seguridad a las WLAN´s.

Ofrecerá total integridad con 802.1x y encripción más robusta con AES. Como trabajo futuro se puede plantear la implementación de 802.11i en una WLAN y verificar que los equipos cumplan con el estándar y por supuesto que funcionen todas sus herramientas de seguridad.

ANEXO 1

Transport Layer Security

A.1 TLS

Transport Layer Security (TLS) es un protocolo que asegura la privacidad en la comunicación entre diferentes aplicaciones a través del Internet. TLS se define en el RFC 2246.

Cuando un cliente y un servidor desean comunicarse, TLS asegura que ningún tercero pueda capturar y entender la información. TLS es el sucesor de *Secure Sockets Layer (SSL).*

TLS se compone de 2 capas funcionales: *TLS Record Protocol* y *TLS Handshake Protocol.*

- *TLS Record Protocol* provee conexiones seguras mediante la utilización de mecanismos de encripción simétricos como *Data Encryption Standard* (DES). Las claves para la encripción simétrica son generadas de forma única para cada conexión y se basan en una negociación secreta realizada por la capa *TLS Handshake Protocol.* La conexión establecida es confiable ya que se provee mecanismos de integridad como MD5.

- La capa TLS *Handshake Protocol* permite al servidor y al cliente autenticarse entre sí y negociar el algoritmo de encripción y las claves criptográficas antes de empezar el intercambio de información. La autenticación puede ser opcional pero generalmente es requerida para al menos una de las partes. La negociación de las claves compartidas es segura para evitar que pueda ser interceptada.

Para el caso específico de redes inalámbricas el establecimiento del túnel seguro con TLS se describe a continuación.

1. Primero el servidor y la estación deben autenticarse mutuamente, para lo cual ambos presentan sus certificados digitales debidamente firmados por una autoridad certificadora y se autentican mediante un algoritmo de clave pública como RSA.

2. Como la estación conoce la clave pública del servidor, y a su vez el servidor conoce la clave pública de la estación, empieza el intercambio de información necesario para establecer el algoritmo de encripción utilizado y la llave simétrica que deberán utilizar ambas entidades para el intercambio de datos posterior. Este intercambio está protegido mediante encripción asimétrica o de clave pública.

3. Una vez que ambas entidades han negociado el algoritmo de encripción y la clave secreta, empieza el intercambio de información que es protegido mediante la clave secreta compartida.

El proceso de autenticación y encripción utilizando certificado digitales ya es descrito en el capítulo 2 del presente trabajo. Sin embargo la generación de la clave secreta es un proceso diferente.

A.1.1 Generación de la clave de sesión

El cliente y el servidor generan por su cuenta una serie de números aleatorios, el cliente además genera una clave *pre-master secret* inicial, igualmente de forma aleatoria. El cliente y el servidor intercambian esta información mediante sus respectivas claves públicas.

Luego cada entidad por su cuenta aplica la función pseudo aleatoria PSF (*Pseudo-Random Function*) definida en el RFC 2236 a los 3 valores intercambiados, generando así la clave *Master Secret* para la sesión.

Nuevamente se utiliza la función PSF para aplicarse sobre la clave *Master Secret* y los valores aleatorios del servidor y el cliente para generar la clave secreta de la sesión TLS. Es importante notar que el servidor y el cliente encuentran la clave secreta de sesión independientemente del otro y por tanto no viaja sobre el sistema. En la figura a.1 se muestra este procedimiento.

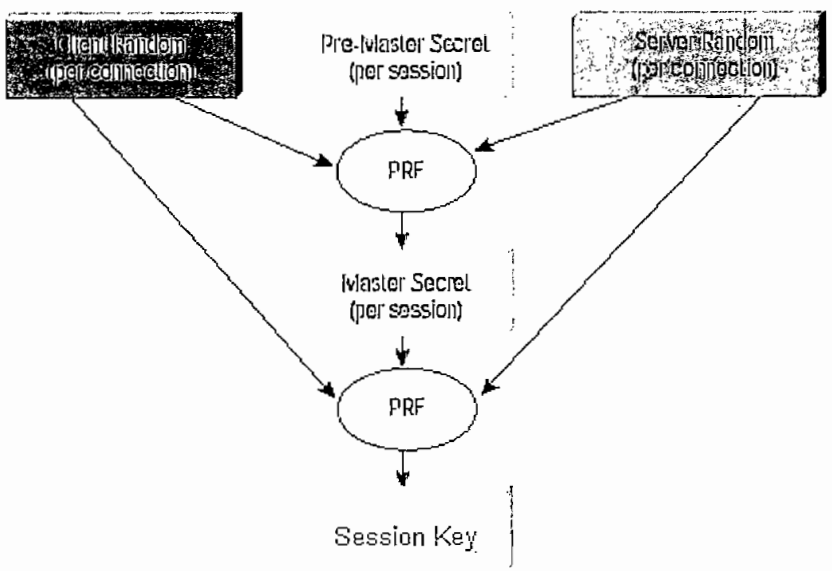


Fig. A.1.1 Generación de la clave compartida para TLS

ANEXO 2

Características técnicas del AP Cisco Aironet 340

Access Point Specifications

Table 1-1 lists specifications for the access point.

Table 1-1 Access Point Specifications

Category	Specification
Physical	
Size	6.30 in. (16 cm) W x 4.72 in. (12 cm) D x 1.45 in. (3.7 cm) H
Status indicators	Three indicators on the top panel: Ethernet traffic, status, and radio traffic
Connectors	On the back panel: An RJ-45 jack for 10/100 Ethernet connections; a nine-pin serial connector; a power connector (plug-in AC adapter) for a regulated 5V input (340 series only)
Voltage range	24 to 60 VDC (regulated 5 VDC for 340 series only)
Operating temperature range	32 to 122°F (0 to 50°C) for 340 and 350 series –4 to 131°F (–20 to 55°C) for 350 series metal case 32 to 104°F (0 to 40°C) for power injectors
Weight	Less than 1 lb (0.45 kg) for 340 and 350 series 1.43 lbs (0.64 kg) for 350 series metal case
Radio	
Power output	100, 50, 30, 20, 5, or 1 mW for 350 series 30, 20, 5, or 1 mW for 340 series (Depending on the regulatory domain in which the access point is installed)
Frequency	2.400 to 2.497 GHz (Depending on the regulatory domain in which the access point is installed)
Range	Indoor: 150 ft at 11 Mbps (100 ft for 340 series only) 350 ft at 1 Mbps (300 ft for 340 series only) Outdoor: 800 ft at 11 Mbps (400 ft for 340 series only) 2000 ft at 1 Mbps (1500 ft for 340 series only)
Modulation	Direct Sequence Spread Spectrum
Data rates	1, 2, 5.5, and 11 Mbps

ANEXO 3

Procedimiento de instalación

del *Aironet Client Utility*

A.3 Procedimiento de instalación del *Aironet Client Utility*

Para comenzar la instalación del *Aironet Client Utility (ACU)* versión 5.05.001 se ejecuta el archivo de instalación mostrado en la figura A3.1 que viene incluido en el CD de documentación y *drivers* junto con la tarjeta inalámbrica Cisco 350. Si se tiene el caso en el que la versión del ACU que viene en el CD sea anterior, se puede descargar la versión actualizada del siguiente enlace del fabricante: http://www.cisco.com/public/sw-center/sw-wireless.shtml

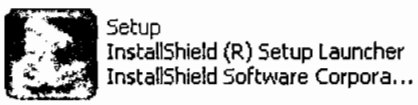


Fig. A3.1 Icono de instalación

El proceso instalación comienza y en la pantalla se muestra el mensaje de la figura A3.2 en el que se indica que se está preparando el asistente para la instalación.

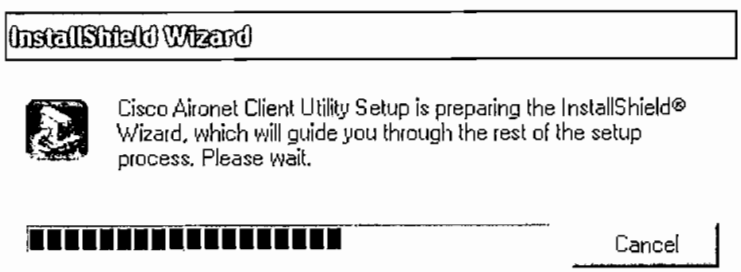


Fig. A3.2 Preparación de la instalación

Una vez listo el asistente se muestra la pantalla de la figura A3.3 en la que se indica que el proceso de instalación va a empezar. Para continuar se da un clic en *Next*

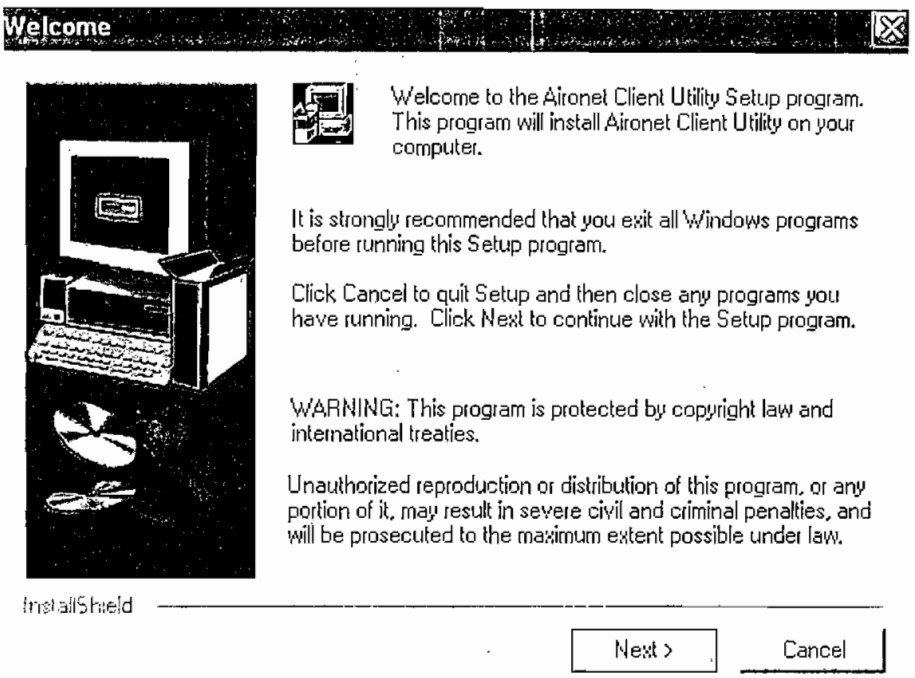


Fig. A3.3 Advertencia de instalación

A continuación se muestra la pantalla de la figura A3.4 en el que se tiene la opción de elegir el tipo de instalación que se requiere. Se tienen 3 opciones:

- LEAP.- Instala todas las funcionalidades de LEAP, además se tiene la sub-opción Allow Saved LEAP User Name and Password que añade la característica de utilizar un nombre de usuario y contraseña almacenados en disco, sin que sea necesario que el usuario ingrese sus credenciales cada vez que tenga que asociarse a la WLAN.

- Create ACU Icon in your Desktop.- Coloca un acceso directo al ACU en el escritorio de Windows.

- Allow Non-Administrator users to use ACU to modify profiles.- inhabilita a usuarios que no sena administradores cambiar los perfiles de configuración.

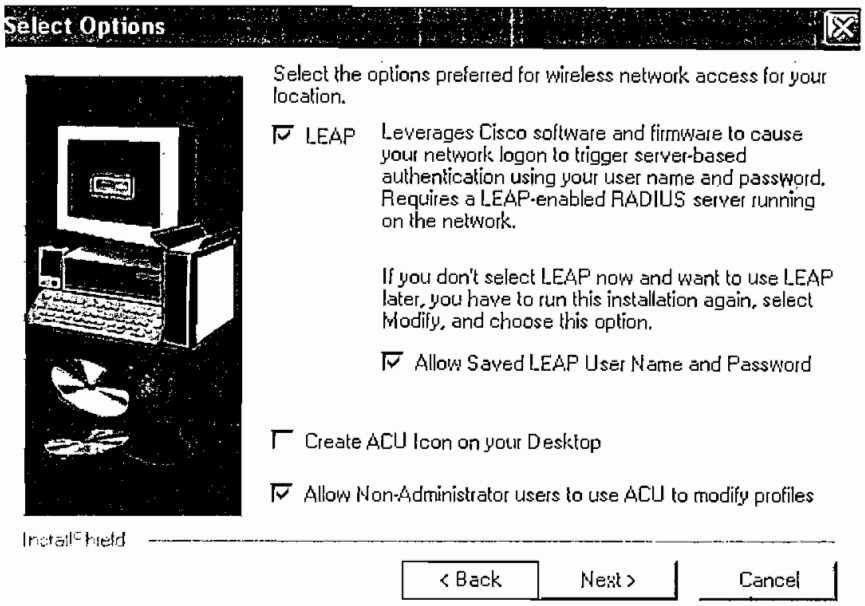


Fig. A3.4 Opciones de Instalación

Luego aparece la pantalla de la figura A3.5, en la que se debe elegir la carpeta de archivos donde se instalará el software. Es recomendable permitir que se cree la carpeta por defecto. Para continuar se da un clic en *Next.*

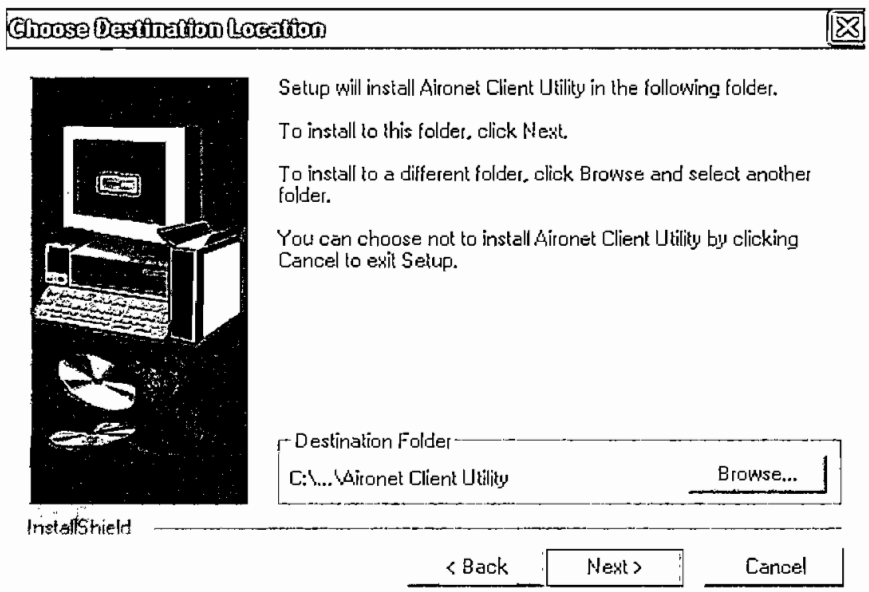


Fig. A3.5 Directorio de instalación

En la pantalla e la figura A3.6 se elige la ubicación del acceso al ACU en el menú de Windows. Por defecto se instala en Programas. Se da un clic en *Next* para continuar.

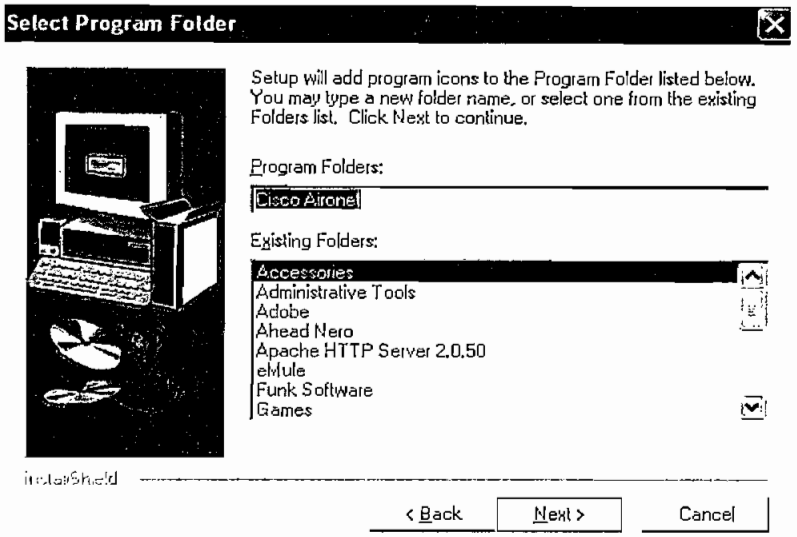


Fig. A3.6 Ubicación en el menú de programas

Finalmente se han seleccionado todas las opciones del ACU, el programa empieza la instalación de archivos, tal como lo muestra la pantalla de la figura A3.7.

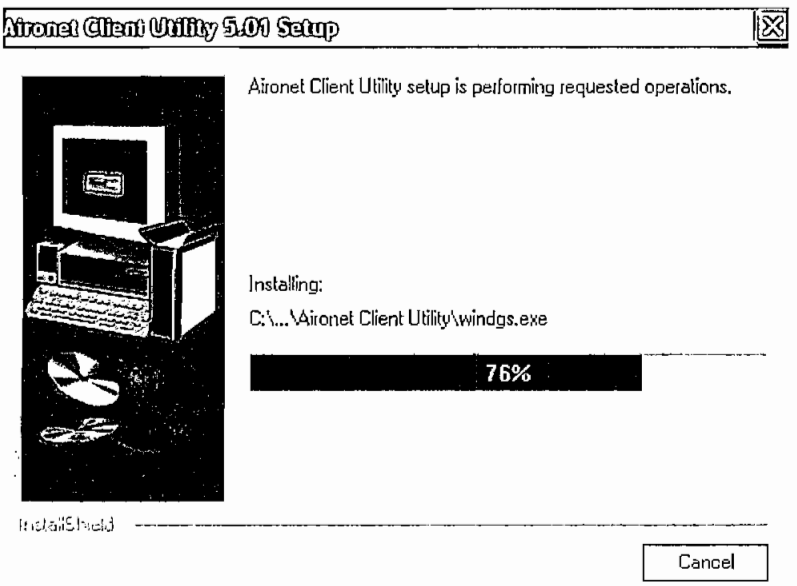


Fig. A3.7 Progreso de la instalación

Luego aparece la pantalla de la figura A3.8 en la que se solicita reiniciar el equipo para finalizar la instalación. Se elige la opción *Yes, I want to restar my computer now.*

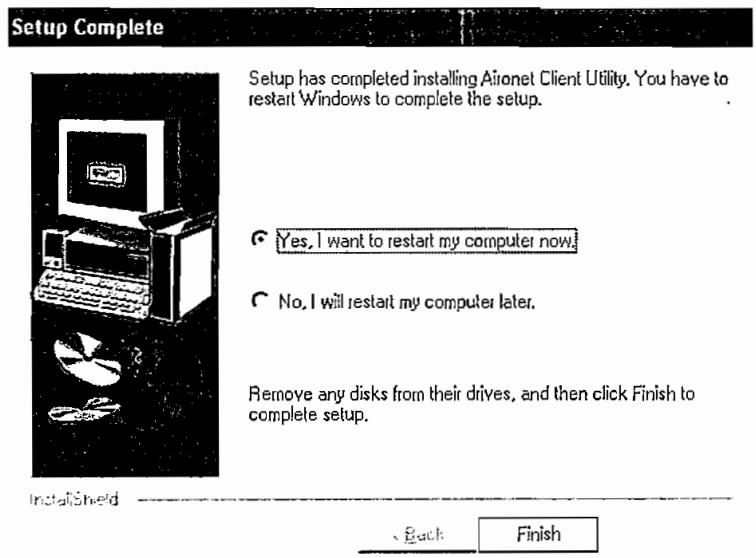


Fig. A3.8 Finalización de la instalación

Una vez reiniciado el equipo la instalación está completa y el ACU está listo para funcionar. Se da u clic en el acceso al programa y aparece la pantalla principal del ACU que se muestra en la figura A3.9.

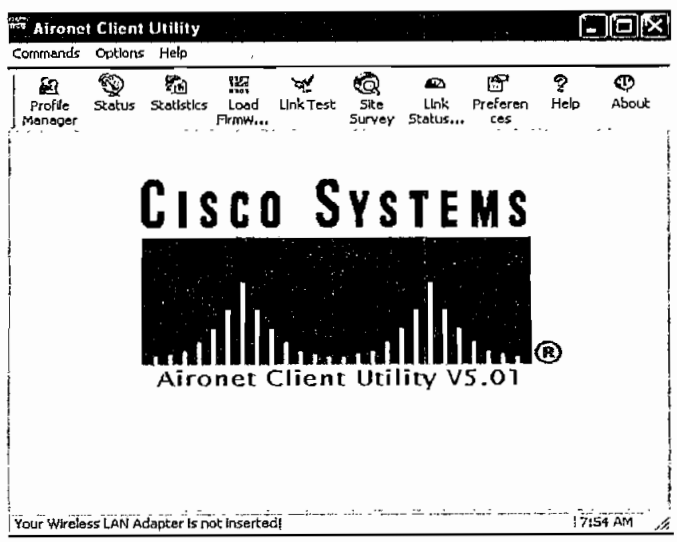


Fig. A3.9 Pantalla principal del ACU

GLOSARIO

AAA.- Abreviatura de Autenticación, Autorización y *Accounting*,

- Autenticación es el proceso de identificación de un individuo, normalmente mediante un nombre de usuario y contraseña. Se basa en la idea de que cada individuo tendrá una información única que le identifique o que le distinga de otros.

- Autorización 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 con éxito. 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, de planeamiento de capacidad, *billing*, y auditoría.

AES.- También conocido como "Rijndael", algoritmo de encriptación simétrica de 128 bits desarrollado por los belgas Joan Daemen y Vincent Rijmen. En Octubre de 2000 era seleccionado por el Instituto Nacional de Estándares y Tecnología (NIST) norteamericano como estándar de cifrado reemplazando a DES.

Ataque de Diccionario.- Método empleado para romper la seguridad de los sistemas basados en *passwords* (contraseñas) en la que el atacante intenta dar con la clave adecuada probando todas (o casi todas) las palabras posibles o recogidas en un diccionario idiomático. Generalmente no se introducen

manualmente las posibles contraseñas sino que se emplean programas especiales que se encargan de ello.

Bluetooth.- Estándar de comunicación inalámbrica que utiliza FHSS, capaz de transmitir a velocidades de 1 Mbps a una distancia de 10 metros entre aparatos (normalmente portátiles, impresoras, monitores, teclados, ratones, etc....) que implementen esta tecnología ya que su *FHSS/Hopping Pattern* es de 1600 veces por segundo, lo que asegura transmisiones altamente seguras.

Código Malicioso.- Es un término genérico utilizado para describir el software malicioso tales como: virus, troyanos, etc.

Crosstalk.- Ruido (interferencia) que fluye entre los cables de comunicación o dispositivos.

Desvanecimiento por múltiples trayectorias.- La variación de la señal causada cuando las señales de radio toman varios caminos desde el transmisor al receptor.

Denegación de Servicio (DoS).- O ataque DoS. Se trata de una ofensiva diseñada específicamente para impedir el funcionamiento normal de un sistema y por consiguiente impedir el acceso legal a los sistemas para usuarios autorizados.

IPsec - IP Security.- Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtuales (VPNs), soporta dos modos de encriptación: Transporte y Túnel. El primero sólo encripta la parte relativa a los de datos (payload) de cada paquete, pero deja la cabecera intacta. Por su parte, el modo Túnel, más seguro, ya que encripta todo.

LDAP - Protocolo de Acceso Ligero a Directorio, Protocolo para el acceso a directorios jerárquicos de información. Basado en el estándar X.500, pero significativamente más simple por lo que también se le denomina x.500-lite, se diferencia de éste porque soporta TCP/IP, necesario para cualquier tipo de acceso a Internet. Aunque no está ampliamente extendido, debería poderse implementar en la práctica mayoría de aplicaciones que se ejecutan virtualmente sobre plataformas informáticas para obtener información de directorios tales como direcciones de correo y llaves públicas. Ya que es un protocolo abierto, no afecta el tipo de servidor en el que se aloje el directorio.

Punto de acceso.- Dispositivo que transporta datos entre una red inalámbrica y una red cableada (infraestructura).

Puerta Trasera.- No se trata de un virus, sino de una herramienta de administración remota. Si es instalada por un hacker tiene la capacidad de dar a un atacante privilegios como administrador. Puede incluso buscar *passwords* y datos confidenciales y enviarlos vía mail a un área remota.

Roaming.- Movimiento de un nodo inalámbrico entre dos celdas. El *roaming* se da normalmente en infraestructuras de redes construidas con varios puntos de acceso.

Sniffers.- Programa y/o dispositivo que monitoriza la circulación de datos a través de una red. Los *sniffers* pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información. Los *sniffers* no autorizados pueden ser extremadamente peligrosos para la seguridad de una red ya que virtualmente es casi imposible detectarlos y pueden ser emplazados en cualquier lugar, convirtiéndolos en un arma indispensable de muchos piratas informáticos. Algunas herramientas *sniffers* conocidas son: *WepCrack, Airsnort, NetStumbler*, entre otras.

SSL - *Secure Sockets Layer.*- Aprobado como estándar por el IETF, es un protocolo desarrollado por Netscape para la transmisión privada de documentos vía Internet cliente/servidor. Trabaja empleando una llave privada de encriptación de datos que es transferida a través de la conexión SSL. Los navegadores Netscape y Explorer soportan SSL, y muchas páginas Web emplean el protocolo para obtener información confidencial del usuario, como números de tarjeta de crédito, etc.

TLS - *Transport Layer Security.*- Protocolo que garantiza la privacidad y la seguridad de datos entre aplicaciones cliente/servidor que se comunican vía Internet.

BIBLIOGRAFÍA

[1] Apuntes de clase de Redes LAN, Ing. Pablo Hidalgo.

[2] CWNA Study Guide – CISCO.

[3] EL AUGE DE LAS REDES INALÁMBRICAS (WLANs), José Manuel Hidrobo. Ingeniero de Telecomunicación, Antena de Telecomunicación / Diciembre 2002.

[4] *Is Wireless (Data) Dead?,* Randy H. Katz. University of California, Berkeley, 1997.

[5] Tecnologías para redes LAN inalámbricas y Windows XP, Por Tom Fout, *Microsoft Corporation*, Julio de 2001.

[6] TANENBAUM, Andrew. Redes de Computadoras, Cuarta Edición. Prentice Hall. México. 2003.

[7] Apuntes de Clase, Seguridad en Redes, Ing Nelson Ávila.

[8] http://oreilly.wirelessdevnet.com/

[9] CANAVAN, John. *Fundamentals of Network Security*, Primera Edición. *Artech House*, New York. 2001.

[10] http://siberiano.aragon.unam.mx/index.html

[11] *DRAFT Wireless Network Security 802.11, Bluetooth™ and Handheld Devices,* NIST, *Special Publication* 800-48.

[12] *IEEE Institute of Electrical and Electronics Engineers. IEEE Standard for Local and Metropolitan Area Networks: IEEE Standard for Wireles LAN Medium Access (MAC) and Physical Layer (PHY) Specifications.* IEEE 802.11. Junio 1997.

[13] 802.11 *Wireless Networks, The Definitive Guide*, Matthew S Gast, O Reilly, Abril 2002.

[14]http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspt/ap350hig/ap350ch3.pdf

[15] OdysseyServer 1.1 *Administration Guide, Funk Software Inc.*