UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN

SEGURIDAD EN REDES INALÁMBRICAS DE ÁREA LOCAL (WLAN) - 802.11 b/g

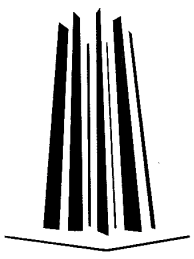
T E S I S

por

Pedro Bautista Fernández

Asesor: M. en C. Marcelo Pérez Medel

Para optar al título de
Ingeniero en Computación



Diciembre 2008

SEGURIDAD EN REDES INALÁMBRICAS DE ÁREA LOCAL (WLAN) - 802.11 b/g

Aprobado por:

_____

M. en C. Marcelo Pérez Medel, Asesor

Fecha de Aprobación _____

A mi mamá, mi primer maestra, quien me ha guiado por el camino de la felicidad y el amor, quien siempre ha estado a mi lado y siempre me ha apoyado.

A mi papá, a quien le he aprendido la dedicación, la constancia y el buen gusto por el conocimiento.

A mi hermana Cinthia, que aunque no todo salga bien ella siempre va a estar conmigo.

A mi hermana Dalia, que con su alegría hace que todo sea mejor.

A mi abuelita Beta, símbolo de la fuerza y capacidad.

Agradecimientos

A mi familia

Tíos, primos y sobrinos, gracias por dejarme formar parte de su vida y al igual ustedes formar parte de la mía.

A todos mis profesores

Desde el preescolar hasta el final de mi carrera que me brindaron su tiempo, paciencia y sobre todo su conocimiento, muchas gracias.

A mis amigos

Lilia, Cuca, Janik, Edgar, Moni, Kika, Mardol, Mario, Christian, Pedro, Alfredo, Lalo, Felpo, Hugo, Erus, Jan, Jaque, Sam, Armando, Bren, Luis, Benji, Ruth que hicieron que esta fase de mi vida tuviera otro sentido, gracias.

Agradezco a mis sinodales, quienes me apoyaron y realizaron la revisión,
haciendo posible la culminación de este trabajo:

Ing. Antonia Navarro González
Ing. Blanca Estela Cruz Luévano
Ing. José Manuel Quintero Cervantes
Mat. Luis Ramírez Flores

En especial quiero agradecerle a mi asesor de tesis, M. en C. Marcelo Pérez Medel por
su apoyo y paciencia para lograr este objetivo.

Índice

Índice de Tablas

Índice de Figuras

Introducción

El presente trabajo se ubica en el área de la administración de redes inalámbricas de computadoras de área local y tiene como objetivo crear una propuesta de solución para permitir implantar niveles de seguridad por medio de la asignación de políticas y con ello poder prestar un servicio "seguro" en comunicaciones de tipo inalámbricas de área local.

0.1. Definición del Problema

El uso de tecnologías de comunicación inalámbricas se ha incrementado considerablemente en la actualidad, puesto que en diversas instituciones tanto gubernamentales como privadas y académicas han sido muy bien adoptadas dichas tecnologías, ya que simplifica la estructura de una red tipo cableada e incluso ofrece una mayor movilidad del equipo, por ejemplo, un usuario con una computadora portátil en el rango de cobertura de la red inalámbrica y con un dispositivo de conexión puede estarse moviendo dentro de éste espacio y no perder la conexión, brindando así, movilidad a los usuarios.

En redes cableadas, de cualquier tipo, por UTP o fibra óptica, por ejemplo, para que un usuario tenga acceso a la red, debe conectarse físicamente por medio de un cable; en el caso de las redes inalámbricas con una simple tarjeta de conexión a redes inalámbricas y dentro del rango de cobertura, el usuario puede tener acceso a la red. Hay varias organizaciones donde el acceso y uso de la red inalámbrica es libre y no cuenta con ningún tipo de mecanismo de autenticación o seguridad, es decir, cualquier usuario, sea o no de la organización puede hacer uso de los servicio y recursos. El hecho de que la red sea de libre acceso, hace que los recursos y servicios pasen a ser de dominio público, dejando a la vista datos que pueden ser de uso exclusivo para la organización.

La forma en que se ofrecen los servicios por todas las organizaciones *debe estár determinada por medio de permisos y privilegios*. Para una organización, la información es su recurso primordial, que incluso puede determinar el éxito o fracaso de su negocio, es por ello que se debe tener cuidado con varios aspectos relacionados con los permisos hacia la información, por ejemplo, quién la administra, quién la manipula y quién la ve.

En la actualidad existen varias amenazas hacia las organizaciones por tratar de obtener o simplemente destruir la información, por tal razón debe de existir un método para poder *mantener segura la información*.

En el área de las redes de datos, si de por sí, son inseguras, las redes inalámbricas lo son aún más. Un factor que influye para decir esto es que, el medio de transmisión que ocupan estas redes es el "aire" y cualquiera puede hacer uso de él, incluso poner una máquina a la escucha del medio (*modo monitor*) y poder así, capturar todo el tráfico que pasa por el medio, de esta forma podría ver la información que se transmite. Es por ello que la seguridad de la información toma un papel trascendental con respecto al resguardo del activo más importante de una organización, la "información".

0.2. Objetivo General

Definir una metodología basándose en la aplicación de políticas y uso de mejores prácticas de modo que se puedan implantar niveles de seguridad altos en una organización para la comunicación en redes inalámbricas de área local utilizando algunos de los estándares definidos por los organismos reguladores.

0.2.1. Objetivos Específicos

- Desarrollo de políticas en las cuales se defina la forma en que la organización debe de manejar, administrar, proteger y asignar los recursos telemáticos para alcanzar un nivel de seguridad óptimo, fortaleciendo así el eslabón más débil de la cadena de seguridad de la información.

- Analizar las amenazas potenciales, ya sean tecnológicas o humanas que pongan en riesgo el funcionamiento o rendimiento de la red, ésto por medio de analizadores de tráfico o sistemas detectores de intrusos.

- Establecer las defensas necesarias para poder brindar un servicio seguro en una red inalámbrica, por medio de servidores de autenticación, uso de algoritmos de cifrado robustos, firewalls, VPN's, etc.

0.3. Organización del Documento

Éste trabajo cuenta con la siguiente estructura:

Capítulo 1 Introducción

Se dará una breve descripción de la problemática de la seguridad en la redes inalámbricas y la necesidad de implantar soluciones para un uso más seguro.

Capítulo 2 Redes Inalámbricas

Es el compendio de toda la teoría y principios básicos necesarios para introducirse en el universo de la telemática inalámbrica y poder así fundamentar la solución al problema de la seguridad en las redes de este tipo.

Capítulo 3 Estándar 802.11i

En este capítulo se describe principalmente el funcionamiento del 802.11i describiendo más que nada el incremento de la seguridad utilizando algoritmos de cifrado y técnicas basadas en claves más avanzadas.

Capítulo 4 InSeguridad en Redes Inalámbricas WLAN - 802.11 b/g

Aquí se describen los tipos de amenazas que pueden llegar a sufrir las redes inalámbricas e incluso el proceso de algunos ataques a esta tecnología, mostrando así que no hay un sistema completamente seguro y menos en esta tecnología.

Conclusiones

Con base en un ataque pasivo (*sniffing*), se muestra un análisis de lo capturado por una herramienta de monitoreo, demostrando así que probablemente la falta de cultura informática con respecto a esta tecnología sea la principal vulnerabilidad que tienen las redes inalámbricas de área local. Y finalmente, los comentarios generales a consecuencia de este trabajo.

Capítulo I

Redes Inalámbricas

A continuación analizaremos el preámbulo de lo relacionado con el tema del presente trabajo, para ello realizaremos un estudio sobre las principales tecnologías en cuanto a comunicaciones inalámbricas se refiere, tomando en cuenta los estándares definidos por los organismos reguladores como el IEEE [1] . Así mismo revisaremos las principales contribuciones en el área de la seguridad informática en comunicaciones inalámbricas de área local (WLAN).

Daremos inicio con el estudio de las tecnologías de red inalámbricas, haciendo énfasis en la familia de protocolos IEEE 802.11, ya que es el estándar con mayor madurez y difusión en cuanto a redes inalámbricas de área local se refiere.

Haremos un análisis más profundo en el funcionamiento de la capa de enlace, común para la mayor difusión en la actualidad, 802.11 b/g, describiendo las diferentes funciones de acceso al medio, ya que este esquema hereda el funcionamiento de las redes cableadas Ethernet, basado en un modelo de competición para el acceso al medio.

Posteriormente estudiaremos el resultado del grupo de trabajo 802.11i que tiene como propósito el especificar los requerimientos y procedimientos para proveer de confidencialidad e integridad al usuario al momento de transmitir información en medios inalámbricos, también veremos algunas características del IEEE 802.11 donde la seguridad definida es insuficiente, ya que los algoritmos para el cifrado de la información y los métodos de

[1] Para mayor información se puede consultar http://www.ieee.org.

autenticación utilizados son muy débiles.

1.1. Tecnología de Redes Inalámbricas

El término wireless hace referencia a todo tipo de comunicación donde no existen los cables, y en las que se utiliza en su mayoría algún tipo de modulación de ondas electromagnéticas y haciendo uso de un medio de transmisión como el aire.

Al igual que las redes cableadas las redes inalámbricas las podemos clasificar por la tecnología que utiliza o por el área geográfica que abarca su área de cobertura:

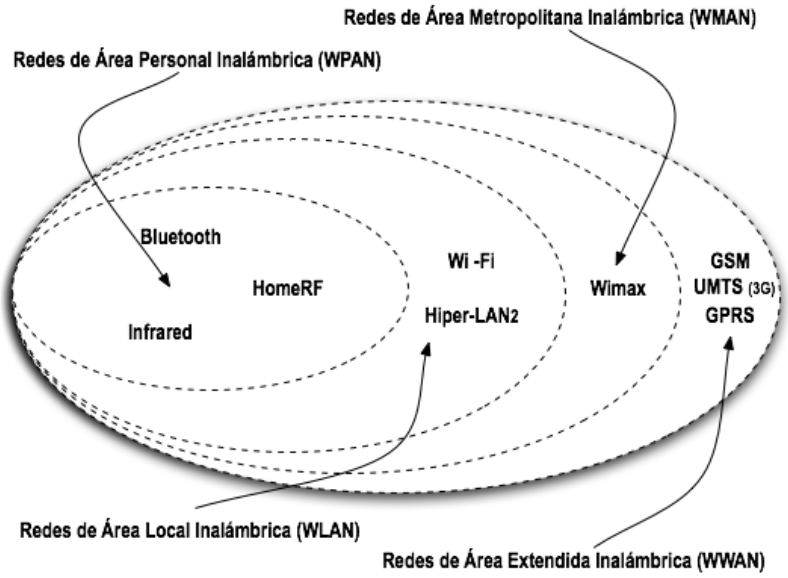


Fig. 1**:** Tecnologías Inalámbricas.

Ahora bien también existen diferentes tipos de Topologías en redes inalámbricas, donde ésta se define por medio de dos elementos, la estación cliente (STA) y el punto de acceso (AP). Existen dos topológias diferentes: El modo **Ad-Hoc** y el modo **Infraestructura**.

En una topología Ad-Hoc no existe un Punto de Acceso (AP) o nodo central, las estaciones se conectan directamente entre si (peer-to-peer), igual a una topología de malla en redes cableadas. Ver Fig. 2.

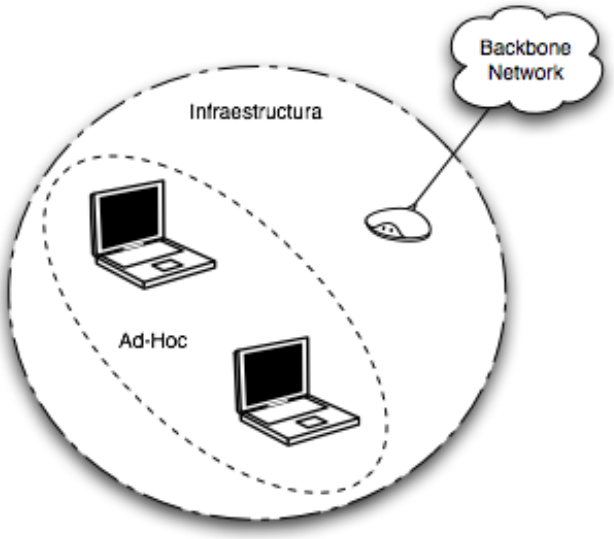


Fig. 2**:** Topologías en Redes Inalámbricas.

A diferencia de una red Ad-Hoc, en la de tipo infraestructura si existe un nodo central o Punto de Acceso (AP), donde toda la comunicación entre las estaciones circula por este dispositivo, la mayoría de las las redes inalámbricas que se van a encontrar van a ser de este tipo. El funcionamiento de esta topología es muy similar al de una topología estrella en una red cableada.

Desde la aparición de Internet las diferentes tecnologías de redes de área local, estuvieron marcadas por la presencia de cables entre cada uno de los nodos, desde redes con topologías tipo bus, anillo o estrella. La evolución de los sistemas de transmisión, ha permitido que estas redes migren a sistemas de transmisión inalámbricos.

Estos sistemas de red basados en un medio de transmisión inalámbrico han ofrecido una movilidad y flexibilidad no provista por otras tecnológias de red, dando lugar a que en los últimos 15 años estos sistemas hayan sobrepasado las expectativas.

Pero podemos decir que no todo es bueno en estos sistemas inalámbricos, puesto que

surge la incipiente preocupación de las organizaciones por la seguridad en el sistema, ya que por naturaleza se dice que las redes inalámbricas son inseguras y esto, por que el medio de transmisión (el aire) le pertenece a todos y cualquiera puede estar monitorizando, capturando y analizando el tráfico.

Los organismos reguladores, principalmente el IEEE consciente de la importancia de la seguridad en los sistemas inalámbricos, decidió crear un grupo de trabajo para el estudio y soporte de la seguridad en las redes inalámbricas bajo el 802.11. Este grupo de trabajo dió como resultado un nuevo estándar aprobado a mediados del 2004, dando lugar al no tan conocido 802.11i.

1.2. Estándar IEEE 802.11

El protocolo IEEE 802.11 es un estándar de comunicaciones del IEEE que define la capa física y de enlace para una trasmisión inalámbrica. Es un estándar publicado por el IEEE en 1997, y es conocido como IEEE.11-1997, este estándar permitía velocidades de transferencia de 1 y hasta 2Mbps, y trabaja en la banda ISM[2] a una frecuencia de 2.4GHz en la que no se precisa licencia, dos años más tarde se actualizaría dando lugar al IEEE 802.11-1999, de esta forma surgían nuevos estándares, por ejemplo, el IEEE 802.11b, el cual alcanza velocidades de 5 hasta 11Mbps que de igual forma trabaja en la banda de 2.4GHz. También se hizo una especificación sobre la frecuencia de los 5GHz. en la cual se hacían transferencias de hasta 54Mbps llamada IEEE 802.11a, pero resultaba incompatible con dispositivos del estándar 802.11b, por lo cual no tuvo mucho desarrollo. Posteriormente nace un estándar compatible con el 802.11b y lo mejor de todo es que contaba con la misma velocidad de transferencia que el 802.11a el cual fue nombrado como el 802.11g. Actualmente la mayoría de las redes inalámbricas existentes pertenecen a estos dos estándares, el 802.11b y el 802.11g. (En la actualidad se está desarrollando un estándar que teóricamente va a alcanzar velocidades máximas de transferencia de hasta 600Mbps el cual se espera para finales del 2008 y su nombre es IEEE 802.11n).

[2]Industrial, Scientific and Medical

A continuación describiremos algunos de los grupos de trabajo que han surgido a partir del 802.11 para poder tener un panorama más amplio en cuanto a redes inalámbricas se refiere.

	802.11a	802.11b	802.11g
Frecuencia de operación	5GHz	2.4GHz	2.4GHz
Velocidad Estándar	6 a 54 Mbps	1 a 11 Mbps	6 a 54 Mbps
Canales Disponibles	12	11	11
Modulación	OFDM	CCK	OFDM
Alcance	20 a 50 m.	35 a 180 m.	20 a 50 m.

Tabla 1.**:** Comparativa de las Variantes del Protocolo 802.11

802.11: Protocolo que proporciona de 1 a 2 Mbps. en el rango de frecuencia 2.4GHz, usando: FHSS[3] o DSSS[4] .

802.11a: Alcanza velocidades de hasta 54Mbps, ajustándose al estándar, y hasta el doble usando técnicas de desdoblamiento por el fabricante. Usa OFDM[5] , una técnica de multiportadora que permite mayores tasas de transferencia. Opera en el rango de frecuencias de los 5GHz. Sus principales inconvenientes son su incompatibilidad con 802.11b y 802.11g y que no incorpora mecanismos de calidad de servicio (QoS), entre otras.

802.11b: Es la implementación de 802.11 que mayor aceptación había tenido por los usuarios. Trabaja con frecuencias en el rango de los 2.4GHz, es decir en la banda reservada para usos industriales, científicos y médicos (ISM), y maneja distintas tasas de transmisión: 1Mbps, 2Mbps, 5.5Mbps y 11Mbps; además implementa DRS (Dynamic Rate Shifting) que ajusta la tasa de transmisión según las condiciones del entorno. Estos valores de tasa de transmisión los consigue gracias al uso de la modulación CCK (Complementary Code Keing) que da una mayor eficiencia que la antigua modulación

[3]Frequency Hopping Spread Spectrum
[4]Direct Sequence Spread Spectrum
[5]Orthogonal Frequency-Division Multiplexing

utilizada, el código Barker. A esto hay que añadirle el uso de la técnica de espectro ensanchado DSSS (Direct Sequence Spread Spectrum).

Los problemas que presenta esta tecnología es que tampoco presenta mecanismos de calidad de servicio, y se encuentra en una franja de frecuencias muy utilizada, por ejemplo teléfonos inalámbricos o dispositivos Bluetooth. Como principales ventajas cabe destacar el bajo costo de la tecnología que ha impulsado una fuerte implantación, que hace uso de una banda de frecuencias de uso gratuito y que se encuentra a nivel mundial.

802.11c: Define características de Punto de Acceso como puentes (bridges).

802.11d: Permite el uso de 802.11 en países restringidos por el uso de las frecuencias.

802.11e: Define el uso de QoS (Quality of Service).

802.11f: Define el enlace entre Estaciones y Puntos de Acceso en modo viajero (Roaming).

802.11g: Intenta aunar el comportamiento del 802.11a y la compatibilidad con el 802.11b, alcanzando tasas de hasta 54Mbps en la banda de frecuencias de 2.4GHz.

Es necesario destacar ciertos inconvenientes que pueden derivar de una tecnología inalámbrica. La eficiencia en cuanto al aprovechamiento del espectro para la transmisión de información es mucho más elevada en tecnologías cableadas, lo que provoca que el caudal ofrecido por tecnologías inalámbricas se encuentre a una gran distancia en cuanto a las redes basadas en cables.

802.11h: Superior al 802.11a permite asignación dinámica de canales (coexistencia con el HyperLAN[6]). Regula la potencia en función de la distancia.

[6]Para mayor información se puede consultar http://en.wikipedia.org/wiki/HIPERLAN

802.11i: Estándar que define fuertes mecanismos de cifrado y autenticación para complementar, completar y mejorar la seguridad en redes inalámbricas. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso de: *Temporal Key Integrity Protocol* (TKIP) y *Counter-Mode/Block Chaining Message Authentication Code Protocol* (CCMP). 802.11i también hace uso de un sistema de distribución de llaves para llevar el control de accesos a la red por medio del 802.11x . Todo esto es abordado en un capítulo destinado para este estándar.

802.11j: Estándar que permitirá la armonización entre el IEEE, el ETSI[7] HyperLAN2, ARIB (Association of Radio Industries and Businesses, Japan) e HISWAN (Hi Speed Wireless Area Network).

802.11k: Actualmente está en desarrollo. Proporciona información para hacer las redes inalámbricas más eficientes:

- Decisiones viajero (roaming).
- Conocimiento del canal RF.
- Nodos Ocultos
- Estadística de Clientes
- Transmisiones de Control de Energía (TPC).

802.11l: No se ocupa, por la similitud con el 802.11i.

802.11m: Trabajo propuesto para el mantenimiento de las redes inalámbricas.

802.11n: Trabajo en proceso de desarrollo. Nuevo estándar de red inalámbrica.

- Construido desde cero. (No chips en modo turbo).

[7]Para mayor información visitar http://www.etsi.org/WebSite/homepage.aspx

- Se esperan velocidades de 100Mbps o más.
- Mejores distancias de operación.
- Posiblemente para finales del 2008.

802.11p: Trabajo en proceso de desarrollo. Usa la banda 5.9GHz y proporciona acceso inalámbrico en ambientes vehiculares, más que nada proporciona una estabilidad en la capa física a cambios muy repentinos, permitiendo tener un mejor enlace.

802.11q: Trabajo en proceso de dasarrollo. Proporciona soporte al desarrollo de VLANs.

802.11r: Trabajo en proceso de desarollo. r de *roaming*, manejando un cambio de código *("handoff")* rápido cuando hay un viajero *"roaming"* entre Puntos de Acceso.

802.11s: Estándar para redes malladas.

802.11T: Métodos para medir el rendimiento de la red Wireless Performance Prediction (WPP).

802.11u: Servirá para el funcionamiento con otras redes no 802, por ejemplo redes celulares.

802.11v: Administración de Redes Inalámbricas.

802.11w: Incrementa la seguridad en las tramas de administración.

1.3. IEEE 802.11 MAC - Nivel de Enlace

La capa de acceso al medio en 802.11 se encarga de proporcionar un servicio de datos fiable a los usuarios de esta capa (es decir, a los protocolos de capas superiores del modelo

OSI) al mismo tiempo permitir un acceso equitativo al medio inalámbrico compartido.

Para proporcionar un acceso fiable el estándar 802.11 define un protocolo para el intercambio de tramas de información. La secuencia mínima en este intercambio consistiría en el envío de una trama de información del origen al destino y un asentimiento (ACK - *Acknowledgment*) enviado por el destino en el caso de que la primera trama haya sido recibida correctamente. Todas las tramas a nivel de MAC incorporan un campo de control de errores (FCS - *Frame Check Sequence*, IEEE 32-bit CRC) que es comprobado en cada recepción. Si la fuente no recibe el asentimiento o el campo de control falla, la trama es reenviada. Aunque este mecanismo consume cierto ancho de banda, permite hacer frente a los posibles errores provocados por el medio inalámbrico.

Adicionalmente a este mecanismo básico de intercambio de tramas, existe una alternativa que proporciona una mayor robustez al protocolo y permite afrontar el problema de los "**nodos ocultos**". Este mecanismo es conocido por las tramas que utiliza RTS/CTS. Una estación que estuviese utilizando este mecanismo, debería mandar una trama RTS (*Request To Send*) al destino antes de transmitir cualqueir trama de datos (MSDU - *MAC Service Data Unit*). Una vez que el destino recibe esta trama correctamente entonces debe responder con otra trama llamada CTS (*Clear To Send*). A partir de este momento la fuente podría comenzar a mandar las tramas MSDU (ver Fig. 3).

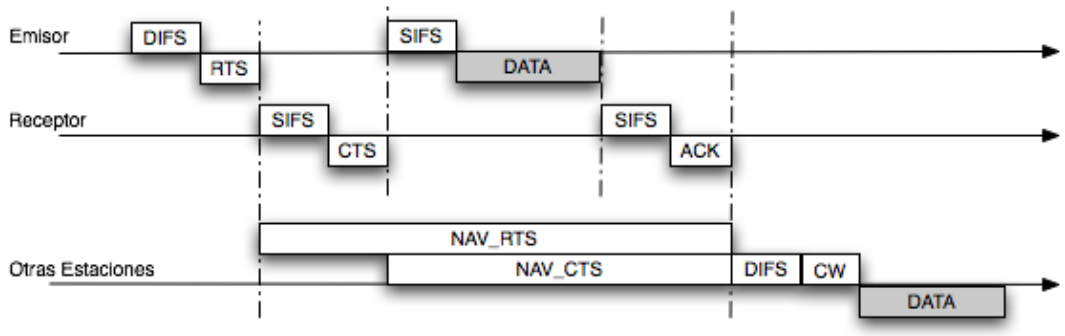


Fig. 3: Problemática RTS/CTS.

Todas las tramas, incluidas las RTS y CTS, contienen información sobre la duración

de la transmisión MSDU/ACK. De forma que basándose en esta información todas las estaciones presentes pueden actualizar un contador interno llamado NAV (*Network Allocation Vector*) y retrasar cualquier transmisión hasta que el contador expire. Aunque una estación oculta no pueda escuchar la trama RTS enviada por la fuente, será capaz de recibir la trama CTS con la que responde el destino de forma que pueda actualizar el contador NAV adecuadamente. Este mecanismo protege la transmisión entre estaciones frente a inesperadas transmisiones de estaciones ocultas.

El estándar 802.11 define dos funciones para el acceso al canal: Función de Coordinación Distribuida (DCF - *Distributed Coordination Function*) y Función de Coordinación Centralizada (PCF - *Point Coordination Function*). Podemos apreciar su posición dentro de la pila de protocolos TCP/IP en la Fig. 4. A continuación se describen ambas funciones.

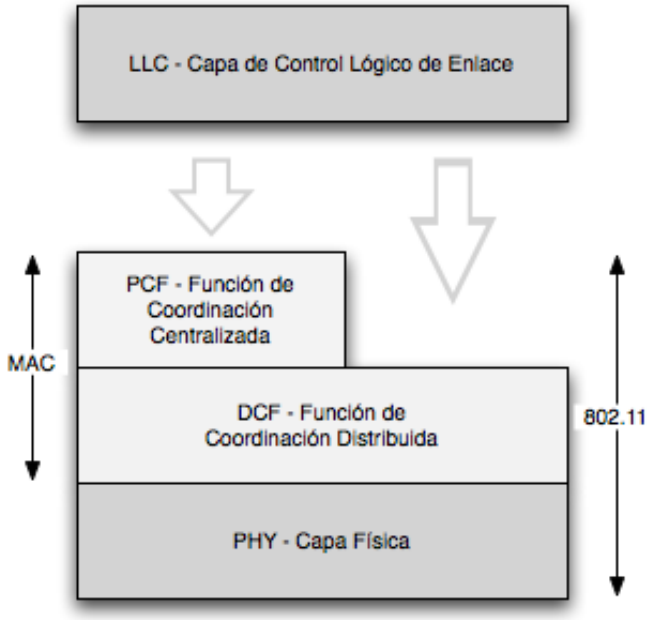


Fig. 4**:** Capas de la Pila de Protocolos TCP/IP definidas por el estándar 802.11.

1.3.1. Función de Coordinación Distribuida - DCF

Se trata de la función básica de acceso al medio definida por el 802.11. DCF proporciona un acceso compartido al medio entre dispositivos con la misma capa física mediante el uso de un protocolo basado en Acceso Múltiple con Detección de Portadora (CSMA - *Carrier Sense Multiple Access*) con evasión de colisiones (CA - *Collision Aviodance*). Todas las estaciones deben incluir obligatoriamente este mecanismo, a diferencia del mecanismo PCF que es opcional.

La detección de portadora se realiza a través de mecanismos físicos y virtuales. La detección física implica que cualquier estación antes de intentar una transmisión debe realizar una lectura de las condiciones del canal y comprobar que el medio está vacío por un periodo de tiempo (IFS - *Inter Frame Space*). La duración de este periodo varía pero la utilizada justo antes de una transmisión en condiciones normales es llamada DIFS (IFS de función de coordinación distribuida).

Para evitar una colisión entre dos estaciones que quieran transmitir simultáneamente, se utiliza un algoritmo de espera (*Backoff*) así como la espera de un periodo DIFS. Cuando existen peticiones de transmisiones pendientes y el medio se encuentra ocupado la estación esperaría hasta que el medio se encuentre vacío por un periodo DIFS. Entonces la estación escoge un número aleatorio entre un rango determinado y usará ese valor como espera adicional antes de transmitir. El rango para elegir esta espera aleatoria es llamado Ventana de Contienda (CW - *Contention Window*), que varía de acuerdo con el número de retransmisiones previas. Si se detecta que el medio pasa a estar ocupado durante el periodo de espera, el contador se detiene, y se reanudará una vez el medio vuelva a estar vacío después del periodo DIFS. En la Fig. 5 podemos comprobar el modelo de funcionamiento del mecanismo DCF.

La evasión de colisión se consigue a través del mecanismo de detección de portadora virtual. Cada estación mantiene un contador interno llamado NAV, el cual indica cuándo es que el medio se encuentra ocupado. El valor de la duración se incluye en cada

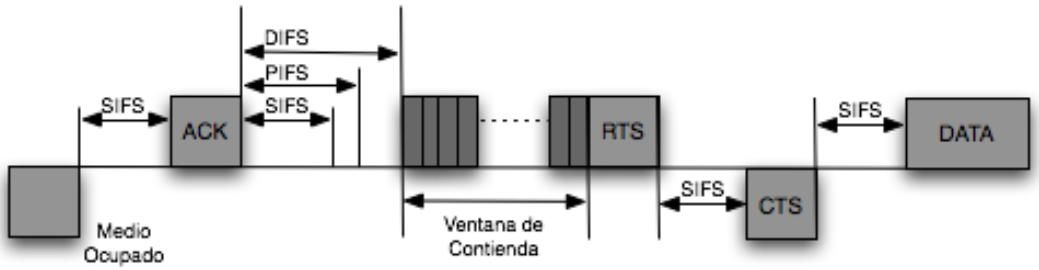


Fig. 5**:** Modelo de Funcionamiento de DCF.

trama transmitida por cada estación, el cual indica cuánto tiempo durará la transmisión, incluyendo los asentimientos y fragmentos. Todas las estaciones que se encuentran próximas reciben esta trama y usan este valor para actualizar su contador NAV. De forma que cuando una estación quiera comenzar una transmisión, en primer lugar comprueba que el contador NAV está a cero.

Una vez que una estación consigue acceso al medio, ésta puede transmitir la trama de información (MSDU). Entonces espera por un periodo de tiempo llamado SIFS (IFS corto) para transmitir el asentimiento (ACK). La duración del periodo SIFS es más corta que en el caso de DIFS, lo que proporciona a la trama de asentimiento la mayor prioridad para acceder al medio. De esta manera se asegura que ninguna otra estación podrá comenzar una transmisión antes que el asentimiento. Si esto no es recibido justo después de un periodo SIFS, se intenta una retransmisión hasta que el número de retrasmisión supera el determinado umbral o tiempo de vida de la MSDU expira. En este caso la trama de información MSDU sería descartada o desechada.

Las tramas de información pueden ser fragmentadas para aumentar las probabilidades de éxito en la transmisión. Sin embargo, dado que cada fragmento MSDU debe ser asentido individualmente, la fragmentación aumenta considerablemente la sobrecarga para la MSDU. En la Fig. 6 podemos ver un ejemplo del mecanismo de acceso DCF.

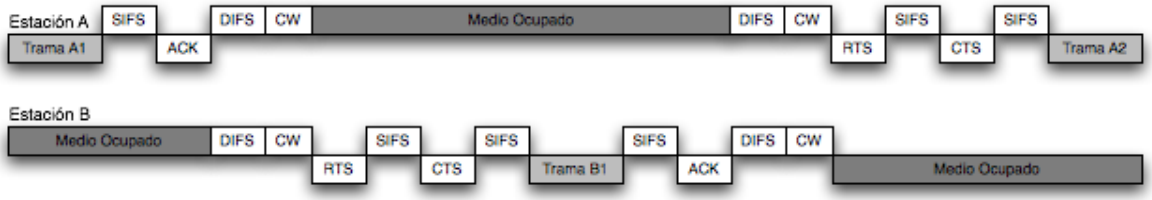


Fig. 6**:** Ejemplo de Funcionamiento de DCF.

1.3.2. Función de Coordinación Centralizada - PCF

El estándar 802.11 define un segundo mecanismo de acceso llamado PCF, pero que al contrario que DCF es opcional, y los productos 802.11 no están obligados a implementarlo. El PCF está diseñado para ofrecer soporte de servicios con restricciones temporales (soporte de calidad de servicio). Un nuevo elemento llamado punto de coordinación (PC - *Point Coordinator*) será el responsable de priorizar el acceso al medio de determinadas estaciones, y estará situado en el punto de acceso.

El estándar 802.11 define dos periodos de tiempo entre el envío de dos mensajes de señalización de envío de tráfico (DTIM - *Delivery Traffic Indication Message*): el periodo de contienda (CP) y el periodo libre de contienda (CFP). En general, el punto de acceso manda de forma periódica tramas de *beacon*, aunque estas tramas pueden ser retrasadas si el medio está ocupado, y transportan información de red y sincronización. Las tramas de *beacon* (DTIM) son usadas por el PC para indicar el comienzo del CFP. En la Fig. 7 podemos ver como es que se alternan los periodos CFP y CP.

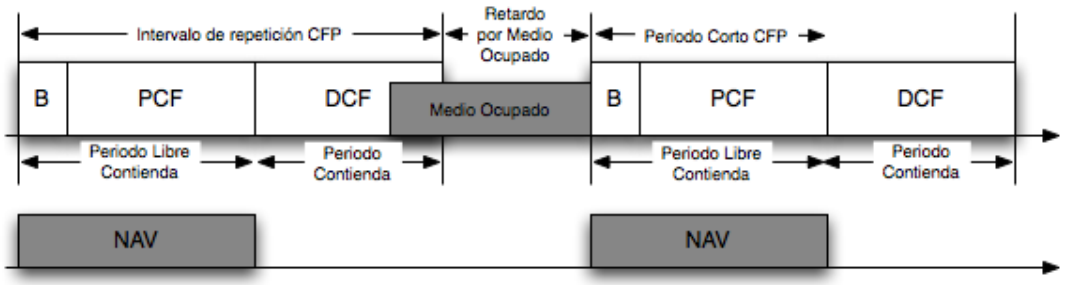


Fig. 7**:** Esquema de Periodos de Contienda.

Durante el CP todas las estaciones compiten por el medio usando el mecanismo DCF. Durante el CFP, el punto de acceso clasifica las transmisiones hacia o desde determinadas estaciones usando un mecanismo de sondeo. No existe contienda entre las estaciones durante el ciclo CFP. Este periodo comienza cuando el AP consigue acceso al medio mediante el uso de un espacio de tiempo PIFS (IFS de función de coordinación centralizada) a la llegada de una trama de *beacon*. El tiempo PIFS es más corto que DIFS, pero mayor que SIFS, y de esta forma PCF logra mayor prioridad que DCF para el acceso, pero no interrumpe ninguna comunicación DCF existente. Una vez que PCF consigue el acceso al medio se utiliza el periodo de tiempo SIFS para el intercambio de tramas durante el ciclo CFP.

El sistema de sondeo comienza cuando el PC envía una trama CF-Poll a una de las posibles estaciones. Si el PC tiene alguna trama pendiente de envío, éste podría utilizar una trama de datos incorporando una trama CF-Poll (*piggy-backing*). La estación sondeada puede responder con datos junto a una trama CF-ACK, o simplemente con una trama CF-ACK si no desea enviar más información. Una vez que el intercambio de tramas con una estación termina, el PC envía el CF-Poll a otra estación que estuviese en la lista de estaciones sondeables. Cuando el PC ha terminado con todas las estaciones de la lista, o una vez que la duración del CFP ha expirado, el PC transmite por difusión una trama Cf-End anunciando el final de ciclo CFP.

Cuando llega una trama de *beacon* el contador NAV de todas las estaciones se inicializa al valor máximo para proteger el ciclo CFP de transmisiones no deseadas. Entonces el punto de acceso transmite por difusión la duración del ciclo CFP en la trama de *beacon*, y el contador NAV se actualiza adecuadamente. Cuando finaliza el ciclo CFP, todas las estaciones inicializan su contador NAV a cero cuando reciben la trama CF-End, o cuando la duración del CFP termina. Desde entonces, hasta la siguiente trama DTIM todas las estaciones compiten por el medio usando DCF.

Este modo de funcionamiento permite que en una misma red coexistan estaciones con soporte PCF y DCF.

1.3.3. IEEE 802.11 MAC - Funciones

A continuación se listan algunas de las principales funciones de la capa MAC que son definidas por el estándar 802.11, para redes inalámbricas de área local (WLANs), en el modo infraestructura.

- **Escaneo**: El estándar 802.11 define dos métodos de escaneo, *pasivo* y *activo*, los cuales una NIC (*Network Interface Card*) puede realizar. El escaneo pasivo es obligatorio para las NICs puesto que hace una búsqueda individual por cada uno de los canales para poder obtener la mejor señal con respecto al punto de acceso. Periódicamente los puntos de acceso emiten los *beacons* en el medio, de modo que las NICs que se encuentren a su alcance mientras escanean el medio toman una referencia de la potencia de la señal emitida por el punto de acceso. Los *beacons* contienen información acerca del punto de acceso, incluyendo el SSID (*Service Set Identifier*), apoyo a la velocidad con que se transmiten los datos, etc. La NIC puede utilizar esta información junto con la potencia de la señal para comparar los puntos de acceso y decidir cuál usar.

  El escaneo activo es similar, con excepción de que la NIC inicia el proceso mediante el envío de una trama de gestión por medio de radiodifusión, de esta forma, todos los puntos de acceso que se encuentren al alcance de la NIC emiten una trama de respuesta. El escaneo activo habilita la NIC para que reciba inmediatamente respuesta de los puntos de acceso, sin esperar los *beacons* emitidos por los puntos de acceso. Sin embargo el escaneo activo sobrecarga la red, ya que para cada trama de gestión corresponde una trama de respuesta.

- **Autenticación**: El proceso de autenticación, como cualquier otro, provee de identidad, el estándar 802.11 especifica dos formas: un sistema abierto (Open System) o la autenticación por medio de una llave compartida (*Shared Key Authentication*).

El sistema de autenticación abierto es obligatorio en la definición del 802.11, y su proceso se compone de dos pasos. Una NIC inicia primero el proceso de envío de una trama de petición de autenticación hacia el punto de acceso. El punto de acceso responde a esta petición por medio de una trama que contiene la aprobación o desaprobación de la autenticación indicado en los campos del cuerpo de las tramas.

El sistema de autenticación por medio de llave compartida es una opción de un proceso de cuatro pasos (*four way handshake*) que se basa en la verificación de una correcta llave WEP (*Wired Equivalent Privacy*). La NIC comienza el proceso de autenticación enviando una trama de petición de autenticación hacia el punto de aceso. Posteriormente el punto de acceso intercambia el texto en la tramas de respuesta y envía esta a la NIC. La NIC hace uso de la llave WEP para cifrar el texto y de esta forma regresa una trama de autenticación al punto de acceso. El punto de acceso descifra el texto cifrado por la NIC y compara éste con el texto inicial. Si los textos son iguales, el punto de acceso asume que la llave es correcta. De esta forma el punto de acceso finaliza el proceso de autenticación envíandole una trama de autenticación donde aprueba o desaprueba la NIC.

- **Asociación**: Una vez autenticada la NIC, debe asociarse con el punto de acceso antes de comenzar el evío de tramas de datos. La asociación es necesaria para la sincronización de la NIC y el punto de acceso con importante información, como puede ser el soporte para la tasa de transferencia de datos. La NIC inicia el proceso, envíando una trama solicitando la asociación, la cual contiene elementos como el SSID y el soporte para las tasas de transferencia de datos. El punto de acceso envía una trama de respuesta de asociación la cuál contiene el identificador de la asociación mas otra información del punto de acceso.

- **WEP**: Con la opción del WEP habilitado, la NIC podría cifrar el contenido (“no las cabeceras”) de cada una de las tramas transmitidas por el medio, haciendo uso de una llave, y la estación receptora podría descifrar las tramas recibidas usando las mismas llaves con que fueron cifradas. El estándar 802.11 especifica una llave

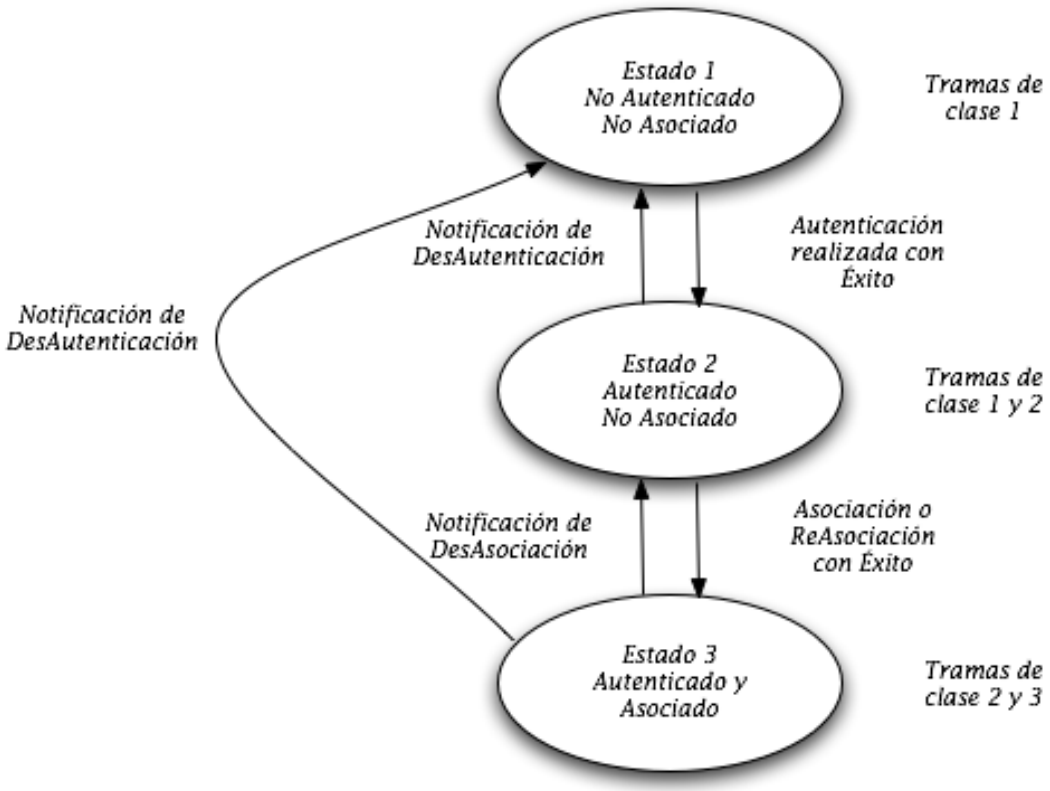


Fig. 8**:** Proceso de Asociación.

de 40-bits pero no un método confiable de distribución de la misma, y por tal motivo hace vulnerable éste método de cifrado para redes inalámbricas. Sin embargo el IEEE desarrolló el estándar **802.11i** el cual incorpora mejoras en las redes inalámbricas y un fuerte algoritmo de cifrado para las comunicaciones por medio del **802.1X**.

- **RTS/CTS**: Las funciones de request-to-send y clear-to-send (RTS/CTS), son funciones que permiten al punto de acceso llevar el control del uso del medio por las estaciones. El uso de RTS/CLS arregla el problema de los "nodos ocultos".

- **Modo en Ahorro de Energía**: La opción que tiene un usuario, para poder ahorrar energía de la batería de la computadora portátil se hace por medio de esta función y es que se puede activar o desactivar en cada una de las NICs. Cuando una NIC quiere entrar en estado de ahorro de energía, ésta envía un bit con el estado de "sleep"

activado en las tramas que son enviadas. El punto de acceso toma nota de cada una de las estaciones o NICs que quieran entrar en “modo de ahorro de energía” y manda a buffers los paquetes correspondientes a la estación que se encuentra en el estado de “ahorro de energía”.

- **Fragmentación**: La fragmentación, al igual que en redes cableadas, funciona de la misma forma, dividiendo tramas grandes en tramas más pequeñas para ser enviadas por el medio. De esta forma se evita el reenviar tramas muy grandes que por el echo de las interferencias o errores hay que retransmitir. Los errores en los bits, resultado de las interferencias de radio frecuencias afectan a una sóla trama, y el hecho de que se envíen tramas más pequeñas influye en que se ocupa menos recursos para enviar una trama más pequeña que una más grande.

Capítulo II

Estándar 802.11i

En Enero de 2001, el grupo de trabajo (*task group*) *i* fue creado en IEEE para mejorar la seguridad en la autenticación y el cifrado de los datos. En Abril de 2003, la Wi-Fi Alliance (una asociación que promueve y certifica redes inalámbricas) realizó una recomendación para responder a las preocupaciones empresariales ante la seguridad inalámbrica. Sin embargo, eran conscientes de que los clientes no querrían cambiar los equipos con los cuales ya contaban.

	WEP	WPA	WPA2
Cifrado	RC4	RC4	AES
Longitud de Llave	40 bits	128 bits enc. - 64 bits auth.	128 bits
Duración de Llave	24-bit IV	48-bit IV	48-bit IV
Integridad de Datos	CRC-32	Michael	CCM
Integridad de Cabecera	Ninguna	Michael	CCM
Cntrol de Llaves	Ninguna	EAP	EAP

Tabla 2.**:** Comparativa entre WEP y WPA

En Junio de 2004, la edición final del estándar 802.11i fue adoptada y recibió el nombre comercial WPA2 por parte de la alianza Wi-Fi. El estándar IEEE 802.11i introdujo varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes de área local como para los grandes entornos de red corporativos. La nueva arquitectura para las redes inalámbricas toma el nombre de Robust Security Network (RSN) y utiliza autenticación 802.1X, distribución de claves

robustas y nuevos mecanismos de integridad y privacidad.

Además de tener una arquitectura más compleja, RSN proporciona soluciones seguras y escalables para las comunicaciones inalámbricas. Una RSN sólo aceptará máquinas con capacidades RSN, pero IEEE 802.11i también define una red transicional de seguridad - *Transitional Security Network* (TSN), arquitectura en la que pueden participar sistemas RSN y WEP, permitiendo a los usuarios actualizar su equipo en el futuro. Si el proceso de autenticación o asociación entre estaciones utiliza *4-Way handshake*, la asociación recibe el nombre de RSNA (*Robust Security Network Association*).

El establecimiento de un contexto seguro de comunicación consta de cuatro fases (ver Fig. 9):

- Acuerdo sobre la política de seguridad.
- Autenticación 802.1X.
- Derivación y distribución de las claves.
- Confidencialidad e integridad de los datos RSNA.

Fase 1: Acuerdo sobre la política de seguridad

La primera fase requiere que los participantes estén de acuerdo sobre la política de seguridad a utilizar. Las políticas de seguridad soportadas por el punto de acceso son mostradas en un mensaje *beacon o Probe Response* (después de un *Probe Request* del cliente). Sigue a esto una autenticación abierta estándar (igual que en las redes TSN, donde la autenticación siempre tiene éxito). La respuesta del cliente se incluye en el mensaje de *Association Request* valido para una *Association Response* del punto de acceso. La información sobre la política de seguridad se envía en el campo RSN IE (*Information Element*) y detalla:

- Los métodos de acceso soportados (802.1X, Pre-Shared Key (PSK)).

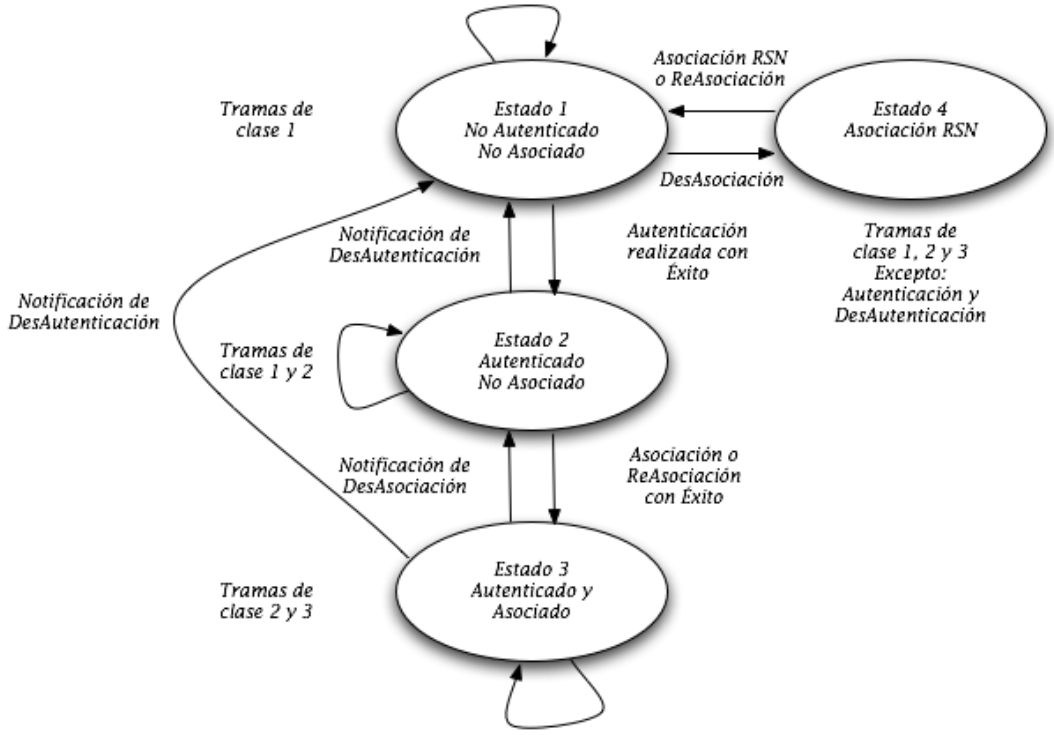


Fig. 9**:** Robust Security Network Association.

- Protocolos de seguridad para el tráfico unicast (CCMP, TKIP, etc.) - la suite criptográfica basada en pares.
- Protocolos de seguridad para el tráfico multicast (CCMP, TKIP, etc.) - la suite criptográfica de grupo.
- Soporte para la pre-autenticación, que permite a los usuarios pre-autenticarse antes de cambiar de punto de acceso en la misma red para un funcionamiento sin retrasos.

La Fig. 10 ilustra esta primera fase.

Fase 2: Autenticación 802.1X

La segunda fase es la autenticación 802.1X basada en EAP y en el método específico de autenticación decidido: EAP/TLS con certificados de cliente y servidor (requiriendo una infraestructura de claves públicas), EAP/TTLS o PEAP para autenticación híbrida

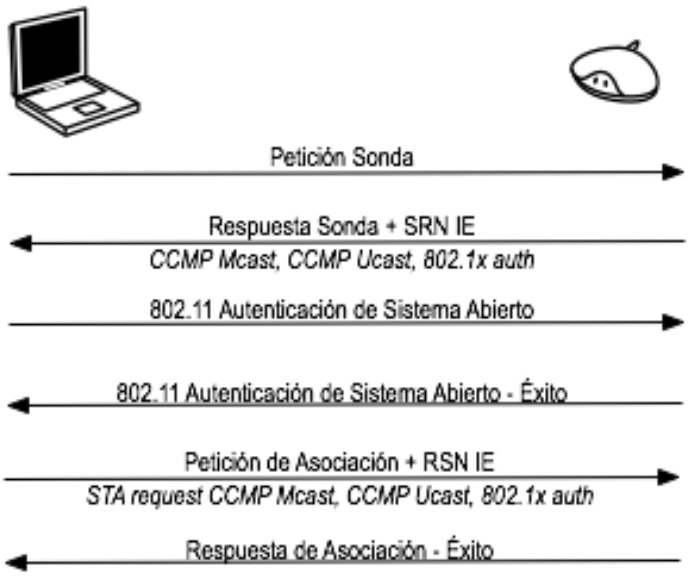


Fig. 10**:** Fase 1. Acuerdo sobre la política de seguridad.

(con certificados sólo requeridos para servidores), etc. La autenticación 802.1X se inicia cuando el punto de acceso pide datos de identidad del cliente, y la respuesta del cliente incluye el método de autenticación preferido. Se intercambian entonces mensajes apropiados entre el cliente y el servidor de autenticación para generar una clave maestra común (MK). Al final del proceso, se envía desde el servidor de autenticación al punto de acceso un mensaje *Radius Accept*, que contiene la MK y un mensaje final *EAP Success* para el cliente. La Fig. 11 ilustra esta segunda fase.

Fase 3: Jerarquía y distribución de claves

La seguridad de la conexión se basa en gran medida en las claves secretas. En RSN, cada clave tiene un tiempo de vida definido y la seguridad global se garantiza utilizando un conjunto de varias claves organizadas según una jerarquía. Cuando se establece un contexto de seguridad tras la autenticación exitosa, se crean claves temporales de sesión y se actualizan regularmente hasta que se cierra el contexto de seguridad. La generación y el intercambio de claves es la meta de la tercera fase. Durante la derivación de la clave, se producen dos handshakes (vease Fig. 12):

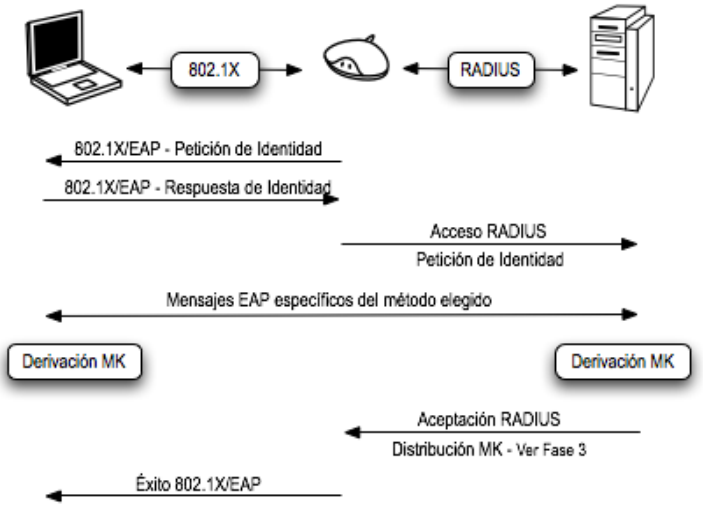


Fig. 11**:** Fase 2: Autenticación 802.1X.

- *4-Way Handshake* para la derivación de la PTK (*Pairwise Transient Key*) y GTK (*Group Transient Key*),
- *Group Key Handshake* para la renovación de GTK.

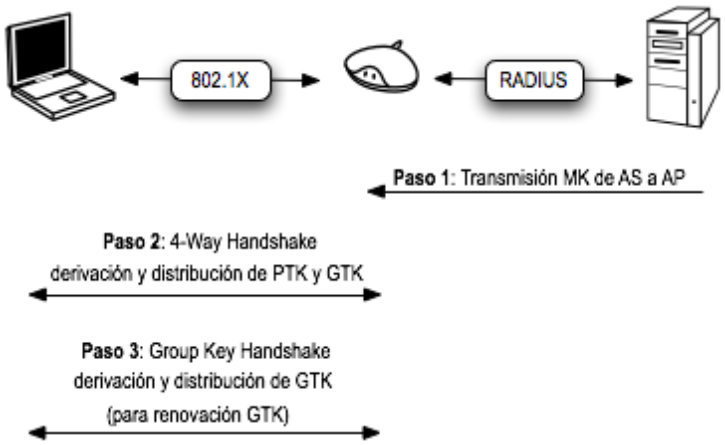


Fig. 12**:** Fase 3: Derivación y distribución de claves.

La derivación de la clave PMK (*Pairwise Master Key*) depende del método de autenticación:

- Si se usa una PSK (*Pre-Shared Key*), PMK = PSK. La PSK es generada desde una *passphrase* (de 8 a 63 caracteres) o una cadena de 256-bits y proporciona una

solución para redes de área local o pequeñas empresas que no tienen servidor de autenticación,

- Si se usa un servidor de autenticación, la PMK es derivada de la MK de autenticación 802.1X.

La PMK en si misma no se usa nunca para el cifrado de o la comprobación de integridad. Al contrario, se usa para generar una clave de cifrado temporal, para el tráfico unicast está la PTK (*Parirwise Transient Key*). La longitud de la PTK depende del protocolo de cifrado: 512 bits para TKIP y 384 bits para CCMP. La PTK consiste en varias claves temporales dedicadas:

- KCK (*Key Confirmation Key* - 128 bits): Clave para la autenticación de mensajes (MIC) durante el *4-Way Handshake* y el *Group Key Handshake*,
- TK (*Temporary Key* - 128 bits): Clave para el cifrado de datos (usada por TKIP o CCMP),
- TMK (*Temporary MIC Key* - 2x64 bits): Clave para la autenticación de datos (usada por Michael con TKIP). Se usa una clave dedicada para cada uno de los lados de la comunicación.

Esta jerarquía se resume en la Fig. 13.
El *4-Way Handshake*, iniciado por el punto de acceso, hace posible:

- Confirmar que el cliente conoce la PMK,
- Derivar una PTK nueva,
- Instalar claves de cifrado e integridad,
- Cifrar el transporte de la GTK,
- Confirmar la selección de la suite de cifrado.

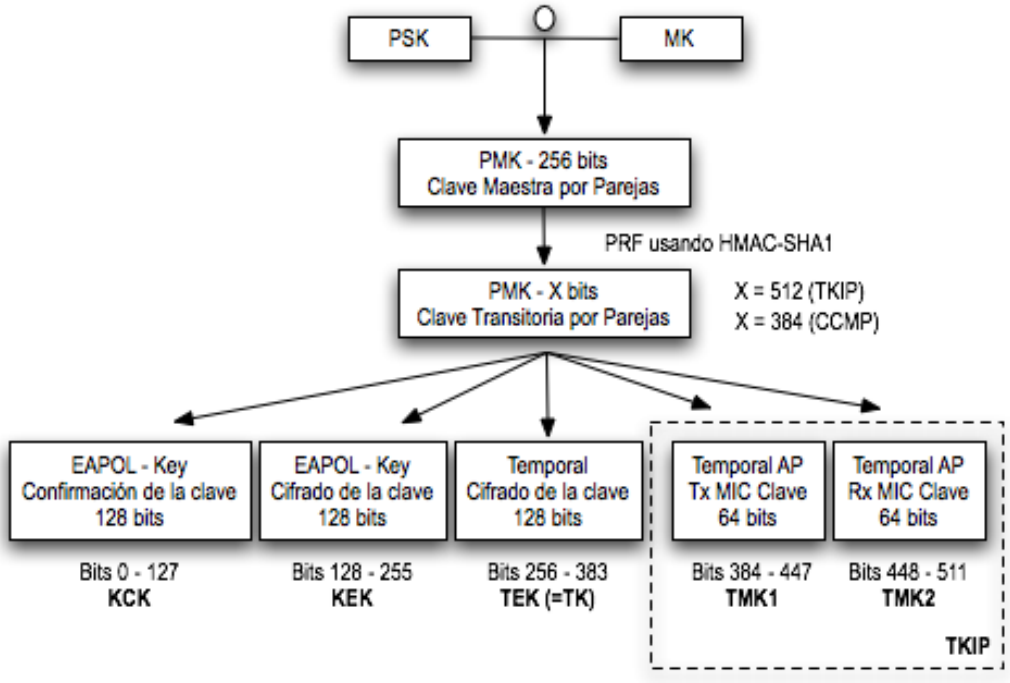


Fig. 13**:** Fase 3: Jerarquía de clave por parejas.

Se intercambian cuatro mensajes EAPOL-Key entre el cliente y el punto de acceso durante el *4-Way Handshake*. Esto se muestra en la Fig. 14.

La PTK se deriva de la PMK, una cadena fija, la dirección MAC del punto de acceso, la dirección MAC del cliente y dos números aleatorios (*ANonce y SNonce*, generados por el autenticador y por el suplicante (usuario), respectivamente). El punto de acceso inicia el primer mensaje seleccionando el número aleatorio *ANonce* y envíandoselo al suplicante, sin cifrar el mensaje o alguna protección. El suplicante genera su propio número aleatorio *SNonce* y ahora puede calcular la PTK y las claves temporales derivadas, así que envía el SNonce y la clave MIC calculada del segundo mensaje usando la clave KCK. Cuando el autenticador recibe el segundo mensaje, puede extraer el SNonce (por que el mensaje no está cifrado) y calcular la PTK y las claves temporales derivadas. Ahora puede verificar el valor de MIC en el segundo mensaje y estar seguro de que el suplicante conoce la PMK y ha calculado correctamente la PTK y las claves temporales derivadas.

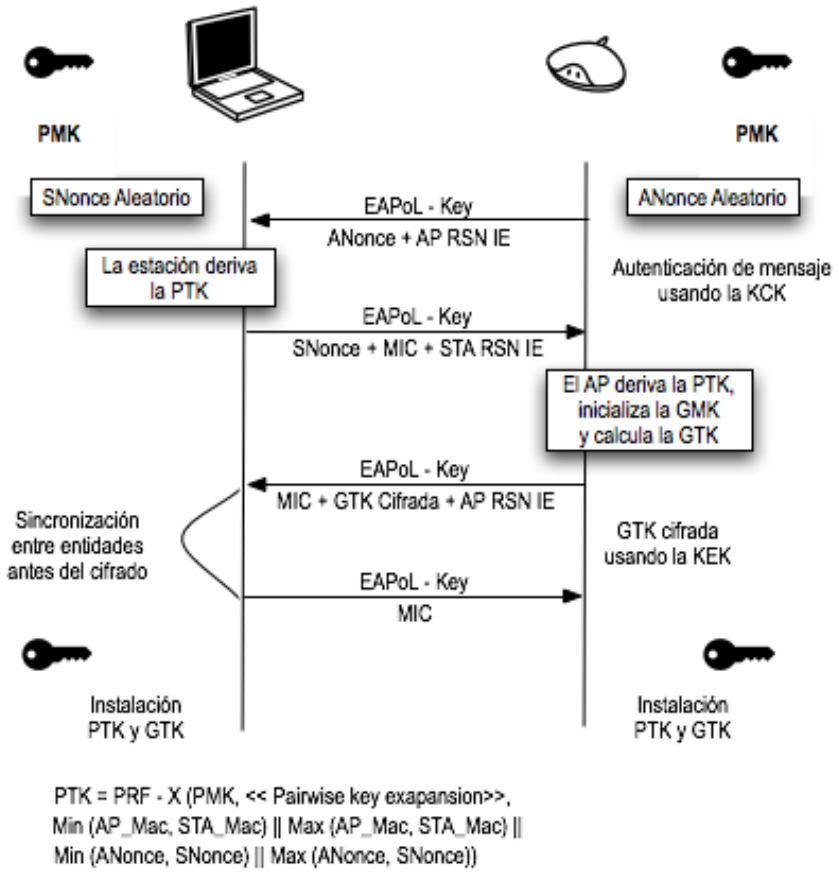


Fig. 14**:** Fase 3: 4 Way Handshake.

El tercer mensaje enviado por el autenticador al suplicante contiene el GTK (cifrada con la clave KEK), derivada de un GMK aleatorio y GNonce (ver Fig. 12), junto con el MIC calculado del tercer mensaje utilizando la clave KCK. Cuando el suplicante recibe este mensaje, el MIC se comprueba para asegurar que el autenticador conoce el PMK y ha calculado correctamente la PTK y derivado claves temporales.

El último mensaje certifica la finalización del hanshake e indica que el suplicante ahora instalará la clave y comenzará el cifrado. Al recibirlo, el autenticador instala sus claves tras verificar el valor MIC, así, el sistema móvil y el punto de acceso han obtenido, calculado e instalado unas claves de integridad y cifrado y ahora pueden comunicarse a través de un canal seguro para tráfico unicast y multicast.

El tráfico multicast se protege con otra clave: GTK (*Group Transient Key*), generada de una clave maestra llamada GMK (*Group Master Key*), una cadena fija, la dirección MAC del punto de acceso y un número aleatorio *GNonce*. La longitud de GTK depende del protocolo de cifrado - 256 bits para TKIP y 128 bits para CCMP. GTK se divide en claves temporales dedicadas:

- GEK (*Group Encryption Key*): Clave para cifrado de datos (usada por CCMP para la autenticación y para el cifrado y por TKIP),
- GIK (*Group Integrity Key*): Clave para la autenticación de los datos (usada solamente por Michael con TKIP).

Esta jerarquía se resume en la Fig. 15.

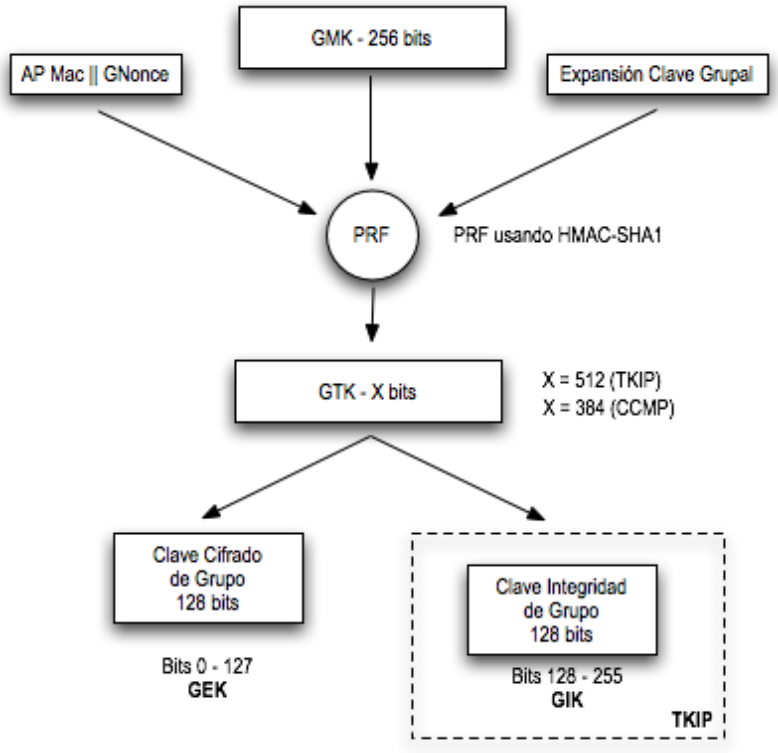


Fig. 15**:** Fase 3: Jerarquía de grupo Key.

Se intercambian dos mensajes EAPOL-Key entre el cliente y el punto de acceso durante el *Group Key Handshake*. Este handshake hace uso de las claves temporales generadas durante el *4-Way Handshake* (KCK y KEK). El proceso se muestra en la Fig. 16.

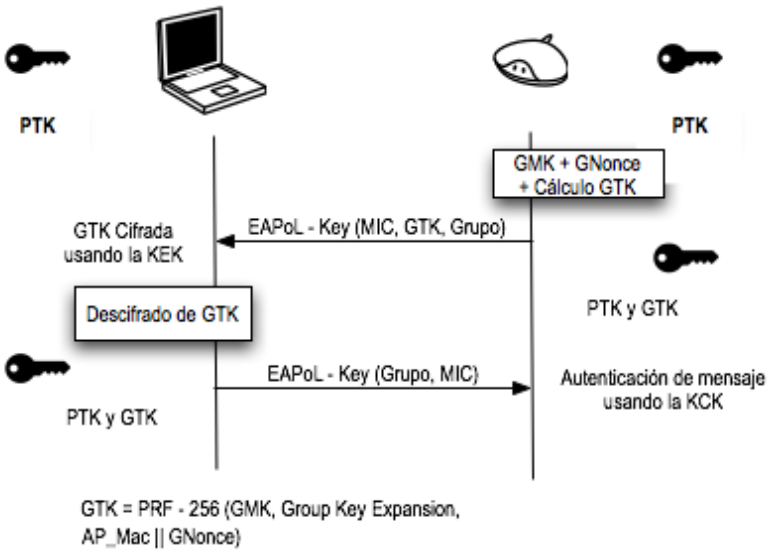


Fig. 16**:** Fase 3: Grupo Key Handshake.

El Group Key Handshake sólo se requiere para la disasociación de una estación o para renovar el GTK, a petición del cliente. El autenticado inicia el primer mensaje escogiendo el número aleatorio *GNonce* y calculando una nueva GTK. Envía la GTK cifrada (usando KEK), el número de secuencia de la GTK y el MIC calculado de este mensaje usando KCK al suplicante. Cuando el mensaje es recibido por el suplicante, se verifica el MIC y la GTK puede ser descifrada.

El segundo mensaje certifica la finalización del *Group Key Handshake* enviando el número de secuencia de GTK y el MIC calculado en este segundo mensaje. Al ser recibido este, el autenticado instala la nueva GTK (tras verificar el valor MIC).

Fase 4: Confidencialidad e integridad de los datos RSNA

Todas las claves generadas anteriormente se usan en protocolos que soportan la confidencialidad e integridad de datos RSNA:

- TKIP (*Temporal Key Hash*),
- CCMP (*Counter-Mode / Cipher Block Chaining Message Autentication Code Protocol*),
- WRAP (*Wireless Robust Authenticated Protocol*).

Hay un concepto importante que debe ser entendido antes de detallar estos protocolos: la diferencia entre MSDU (*MAC Service Data Unit*) y MPDU (*MAC Protocol Data Unit*). Ambos términos se refieren a un sólo paquete de datos, pero MSDU representa a los datos antes de la fragmentación. La diferencia es importante en TKIP y en el protocolo de cifrado CCMP, ya que en TKIP el MIC se calcula desde la MSDU, mientras que en CCMP se calcula desde MPDU.

Al igual que WEP, TKIP está basado en el algoritmo de cifrado RC4, pero esto es así tan sólo por un motivo: permitir a los sistemas WEP la actualización para instalar un protocolo más seguro. TKIP se requiere para la certificación WAP y se incluye como parte de RSN 802.11i como una opción. TKIP añade medidas correctoras para cada una de las vulnerabilidades de WEP:

- Integridad de mensaje: un nuevo MIC (*Message Integrity Code*) basado en el algoritmo Michael puede ser incorporado en el software para microprocesadores lentos,
- IV: nuevas reglas de selección para los valores IV, reutilizando IV como contador de repetición (TSC, o TKIP *Sequence Counter*) e incrementando el valor del IV para evitar la reutilización,
- *Per Packet Key Mixing*: para unir llaves de cifrado aparentemente inconexas,
- Gestión de llaves: nuevos mecanismos para la distribución y modificación de llaves.

TKIP Key-Maxing Scheme se divide en dos fases. La primera se ocupa de los datos estáticos - la llave TEK de sesión secreta, el TA de la dirección MAC del transmisor (incluido para prevenir colisiones IV) y los 32 bits más altos del IV. La fase 2 incluye el resultado de la fase 1 y los 16 bits más bajos del IV, cambiando todos los bits del campo *Per Packet Key* para cada nuevo IV. El valor IV siempre empieza en 0 y es incrementado de uno en uno para cada paquete enviado, y los mensajes cuyo TSC no es mayor que el del último mensaje son rechazados. El resultado de la fase 2 y parte del IV extendido (además de un bit dummy) componen la entrada para RC4, generando un flujo de clave que es XOR-eado con el MPDU de sólo texto, el MIC calculado del MPDU y el viejo ICV de WEP ver Fig. 17.

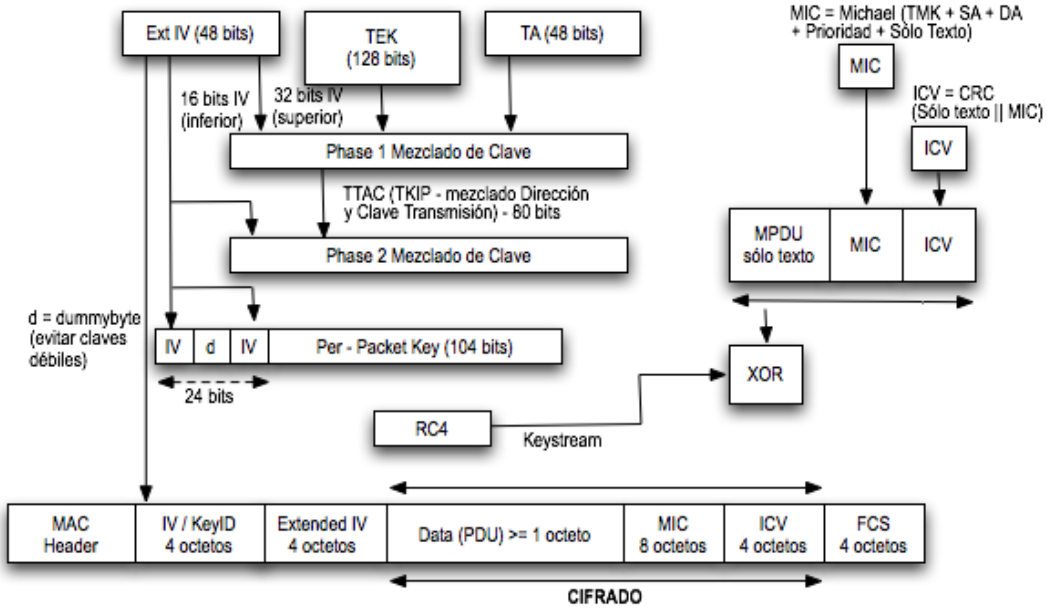


Fig. 17**:** Esquema y cifrado de *TKIP Key-Mixing*.

La computación del MIC utiliza el algoritmo Michael de Niels Ferguson. Se creó para TKIP y tiene un nivel de seguridad de 20 bits (el algoritmo no utiliza multiplicación por razones de rendimiento, porque debe ser soportado por el viejo hardware de red para que pueda ser actualizado a WPA). Por esta limitación, se necesitan contramedidas para evitar la falsificación del MIC. Los fallos de MIC deben ser menores que 2 por minuto, o se producirá una desconexión de 60 segundos y se establecerán nuevas claves GTK y

PTK tras ella. Michael calcula un valor de comprobación de 8 octetos llamado MIC y lo añade a la MSDU antes de la transmisión. El MIC se calcula de la dirección origen (SA), dirección de destino (DA), MSDU de sólo texto y la TMK apropiada (dependiendo del lado de la comunicación, se utilizará una clave diferente para la transmisión y la recepción).

CCMP se basa en la suite de cifrado de bloques AES (Advanced Encryption Standard) en su modo de operación CCM, con la clave y los bloques de 128 bits de longitud. AES es a CCMP lo que RC4 a TKIP, pero al contrario que TKIP, que se diseñó para acomodar al hardware WEP existente, CCMP no es un compromiso, sino un nuevo diseño de protocolo. CCMP utiliza el counter mode junto a un método de autenticación de mensajes llamado *Cipher Block Chaining* (CBC-MAC) para producir un MIC.

Se añadieron algunas características interesantes, como el uso de una clave única para el cifrado y la autenticación (con diferentes vectores de inicialización), el cubrir datos no cifrados por la autenticación. El protocolo CCMP añade 16 bytes al MPDU, 8 para el encabezamiento CCMP y 8 para el MIC. El encabezamiento CCMP es un campo no cifrado incluido entre el encabezamiento MAC y los datos cifrados, incluyendo el PN de 48-bits (*Packet Number* = IV Extendido) y la *Group Key KeyID*. El PN se incrementa de uno en uno para cada MPDU subsiguiente.

La computación de MIC utiliza el algoritmo CBC-MAC que cifra un bloque nonce de inicio (computado desde los campos de Priority, la dirección fuente de MPDU y el PN incrementado) y hace XORs sobre los bloques subsiguientes para obtener un MIC final de 64 bits (el MIC final es un bloque de 128-bits, ya que se descartan los últimos 64 bits). El MIC entonces se añade a los datos de texto para el cifrado AES en modo contador. El contador se construye de un nonce similar al del MIC, pero con un campo de contador extra inicializado a 1 e incrementado para cada bloque.

El último protocolo es WRAP, basado también en AES pero utilizando el esquema de cifrado autenticado OCB (Offset Codebook Mode cifrado y autenticación en la misma operación). OCB fue el primer modo elegido por el grupo de trabajo de IEEE 802.11i,

pero se abandonó por motivos de propiedad intelectual y posibles licencias. Entonces se adoptó CCMP como obligatorio.

Capítulo III

InSeguridad en Redes Inalámbricas WLAN - 802.11 b/g

Conforme han crecido las redes inalámbricas de área local (*WLAN*), la seguridad se ha convertido en una seria preocupación para la mayoría de las empresas. En sí, los pilares de la seguridad para una red inalámbrica incluyen **confidencialidad de los datos, integridad, una autenticación mutua y disponibilidad**.

IEEE 802.11i, un estándar de la IEEE ratificado en Junio del 2004, está diseñado para proporcionar mayor seguridad en el *Medium Access Control* (MAC) de el 802.11. El 802.11i define dos tipos de algoritmos de seguridad: *Robust Security Network Association* (RSNA), y Pre-RSNA. La seguridad del Pre-RSNA consiste de *Wired Equivalent Privacy* (WEP) y una entidad de autenticación del 802.11. RSNA provee dos protocolos de confidencialidad de datos, uno es el *Temporal Key Integrity Protocol* (TKIP) y el *Counter-mode/CBC-MAC Protocol* (CCMP) y el procedimiento establecido por el RSNA, incluyendo autenticación tipo 802.1X y protocolos de administración de llaves.

A continuación vamos a analizar los aspectos de seguridad del 802.11i, considerando confidencialidad de los datos, integridad, mutua autenticación y disponibilidad. Este análisis muestra que el estándar 802.11i es un buen diseño para mantener la confidencialidad, integridad, disponibilidad y aportar una mutua autenticación, en sí, un protocolo comprometido con la seguridad en redes inalámbricas. Aunque vamos a ver que aún en esta tecnología siguen permaneciendo los ataques de denegación de servicios *Denial-of-Service* (DoS). Revisaremos algunos de los ataques de denegación de servicios.

En el procedimiento a través del análisis al 802.11i, encontramos algunas consideraciones o sugerencias de forma que se eviten algunos problemas de seguridad. A continuación se mencionan algunas de las principales recomendaciones: en primer lugar, para la confidencialidad de los datos debe usarse CCMP, ya que TKIP y WEP tienen debilidades inherentes. En segundo lugar, una autenticación mutua debe aplicarse para alcanzar los objetivos de seguridad, según se detalla en el siguiente párrafo. En tercer lugar, varios detalles de aplicación son importantes para abordar la vulnerabilidad en la capa MAC por ataques tipo DoS. Por último, la falta de eficiencia de recuperación puede ser mejorado mediante el uso de algunas políticas.

El objetivo de una mutua autenticación puede lograrse gracias a varios mecanismos puestos en funcionamiento conjuntamente, primero que nada, un método apropiado de autenticación *Extensible Authentication Protocol* (EAP), por ejemplo EAP-TLS el cual impide ataques de Man-in-the-Middle (MitM)[8] . En segundo lugar un servidor RADIUS y la generación de una contraseña *Pre-Shared Key* (PSK), la cual debe ser seleccionada bajo alguna política para evitar ataques de fuerza bruta por medio de diccionarios. En tercer lugar, si los dispositivos permiten correr los dos algoritmos, tanto Pre-RSNA como RSNA al mismo tiempo, el usuario debería tener oportunidad de seleccionar *manualmente* cuál usar en el caso de conexiones con prioridad, y los Puntos de Acceso (APs) deberán tener diferentes políticas de privilegios para cada uno. Esta restricción es sencilla para la infraestructura de redes y el estándar, pero puede tener algunos efectos sobre los posibles usos del 802.11i en combinación con redes ad hoc.

Un número de pequeñas modificaciones aparentemente hacen más robusto al estándar 802.11i ante ataques tipo DoS. Una prueba de esto es que puede mitigar ciertos tipos de ataques DoS "conocidos", por ejemplo, eliminando o mejor dicho haciendo caso omiso a ciertos paquetes EAP. En segundo lugar, cuando se adoptó TKIP, el Michael MIC (*Message Integrity Code*) falló, contra esto, debería de aplicarse una mejora al TKIP y se llama *TKIP Sequence Counter* (TSC) y así mitigará un ataque DoS más complicado. En tercer

[8]Para mayor descripción del ataque visitar http://en.wikipedia.org/wiki/Man-in-the-middle_attack

lugar, en el mecanismo de confirmación del RSN IE, la condición de verificación debería estár libre para poder responder a un potencial ataque DoS. Y finalmente en el 4-Way Handshake es mejor que el suplicante reutilice el mismo *nonce* hasta que se complete con éxito la conexión.

3.1. Amenazas en Redes Inalámbricas

Con el fin de analizar el protocolo 802.11i, es importante caracterizar las probables capacidades de cualquier posible intruso. A partir de la capa de enlace en la WLAN, existen tres tipos diferentes de "tramas": tramas de Administración, de Control y de Datos. Cualquier modificación o alteración a estas tramas, potencialmente ponen en peligro la confidencialidad de los datos, la integridad, la autenticación y la disponibilidad, pudiéndose considerar esto, como una amenaza. A continuación se muestran algunos ataques que se pueden consideran en el análisis de este trabajo.

Amenaza 1. Captura pasiva/Análisis de tráfico (*Passive Eavesdropping/Traffic Analysis*)

Debido a las características de las comunicaciones inalámbricas, un intruso puede capturar y guardar todo el tráfico generado en una WLAN. Incluso cuando los mensajes van cifrados, es importante tener en cuenta que un intruso puede leer parcial o completa la información de ciertos mensajes. Esta posibilidad existe si el mensaje común de los campos son predecibles o redundantes; además, los mensajes cifrados pueden ser generados a las peticiones del propio intruso. En el análisis, consideramos que si se registran los paquetes y/o reconoce parte del paquete, este puede ser utilizado para revelar la llave de cifrado, descifrar los paquetes completos, o recoger otro tipo información útil a través de técnicas de análisis del tráfico.

Amenaza 2. Inyección de Tráfico/Captura Activa (*Message Injection/Active Eavesdropping*)

Un intruso es capáz de insertar tráfico en una red inalámbrica, esto, con ciertos dispositivos, por ejemplo con una interfáz de red inalámbrica (NIC) y cierto tipo de aplicaciones. Aunque el firmware de la mayoría de las NICs puede limitarse para determinar el número de paquetes a enviar bajo el estándar 802.11,un intruso es capáz de controlar cualquier campo de un paquete utilizando técnicas conocidas. Por lo tanto, es razonable suponer que un intruso puede dar lugar a cualquier paquete elegido, modificar el contenido de un paquete, y por completo tomar el control de la transmisión del paquete. Si un paquete debe ser autenticado, el intruso puede ser capaz de romper el algoritmo de integridad de los datos para hacer que sea un paquete válido. El intruso también puede **insertar o replicar** paquetes. Por otra parte, mediante la inserción de algunos paquetes, el intruso podría ser capaz de obtener más información de la reacción del sistema a través de una captura activa.

Amenaza 3. Supresión e Intercepción de Mensajes (*Message Deletion and Interception*)

Suponemos que un intruso es capaz de hacer supresión de mensajes, lo que significa que un intruso es capaz de eliminar un paquete de la red antes de que llegue a su destino. Esto podría hacerse por medio de una interferencia en el proceso de recepción de paquetes en la antena del receptor, por ejemplo, causando errores al CRC (Cyclic Redundancy Checksum) de forma que el receptor tire los paquetes. Este proceso es similar al paquete ordinario de error debido al ruido, pero puede ser instigado por el intruso.

Intercepción de mensaje significa que un adversario es capaz de controlar por completo una conexión. En otras palabras, el intruso puede capturar un paquete antes de que el receptor efectivamente lo reciba, y decidir si debe ser eliminado o reenviarlo al receptor. Esto es más peligroso que la captura y la supresión de paquetes. Por otra parte, se diferencia de la captura y la reproducción, porque el receptor no recibe el paquete hasta después de que el intruso se lo reenvíe. La intercepción de mensajes puede parecer difícil en WLANs ya que el receptor legítimo puede detectar un mensaje tan pronto como el

intruso lo haga. Sin embargo, un intruso con conocimientos avanzados tiene algunas posibles formas de lograr la intercepción de mensajes. Por ejemplo, el intruso puede usar una antena direccional para eliminar un paquete en el lado del receptor, mientras que al mismo tiempo utiliza otra antena para poder recibir el paquete.

Amenaza 4. Enmascaramiento y APs Malintencionados (*Masquerading and Malicious AP*)

Debido a que las direcciones MAC de cada dispositivo son trasmitidas en texto plano en cada uno de los paquetes enviados en una sesión inalámbrica, un intruso puede estar capturando el tráfico y de esta forma ver las direcciones MAC válidas que se pueden asociar. El intruso es capaz de cambiar su propia dirección MAC ya que esto es posible con un simple comando, en el caso de sistemas tipo *nix*, si el sistema de seguridad de la red inalámbrica se basa en la autenticación sólo de la dirección MAC, el intruso puede disfrazar (*spoofing*) la dirección MAC por una válida de esta forma asociarse y autenticarse en la red o incluso se puede enmascarar como un punto de acceso (*AP*), esto gracias al desarrollo del software libre, (*HostAP*). Un intruso es también capaz de instalar su propio punto de acceso falsificando su dirección MAC, sin la necesidad de enmascarar a otros, esto es posible, incluso se puede proveer de una señal con más potencia, esperando a que alguna estación se asocie y de esta forma filtrarse en el cliente y así poder ver información privada.

Amenaza 5. Secuestro de Sesión (*Session Hijacking*)

Consideramos que un intruso puede ser capaz de secuestrar una sesión después de que los dispositivos inalámbricos hayan terminado con éxito la autenticación. Enseguida mostramos un posible escenario donde podemos mostrar esto. En primer lugar, el intruso desconecta a un usuario asociado con el punto de acceso, posteriormente el intruso se enmascara como si fuera el usuario o estación asociada para recibir posibles conexiones sin tomar en cuenta al usuario legítimo. En este ataque, el intruso es capaz de recibir todos los paquetes destinados al dispositivo secuestrado y también capaz de enviar paquetes al dispositivo secuestrado. Este ataque podría eludir cualquier mecanismo de autenticación

utilizado. Sin embargo, si se utilizan protocolos que cuiden la integridad y confidencialidad de los datos, el intruso debe romper el algoritmo de cifrado con el fin de enviar paquetes válidos. Por lo tanto, ataques contra la autenticación se puede evitar haciendo uso de mecanismos de integridad.

Amenaza 6. Hombre en Medio (*Man in the Middle*)

Este ataque es diferente desde la intercepción del mensaje por que el intruso debe participar en una comunicación continua. Si ya existe una conexión entre el punto de acceso y una estación, el intruso, primero debe romper esta conexión. Posteriormente el intruso debe enmascararse como estación legítima para poder asociarse con el punto de acceso. Si es AP cuenta con algún mecanismo de autenticación, el intruso es capaz de romper con esta y poder así asociarse. Finalmente el intruso debe hacerse pasar por el verdadero AP y de esta forma, la estación se asociará con este. De igual forma si la estación cuenta con algún mecanismo para poder autenticar al punto de acceso, el intruso presentará sus credenciales y de esta forma quedará autenticado. Otro enfoque posible para lanzar un ataque *MitM* es el envenenamiento de caché ARP, como en una LAN cableada.

Amenaza 7. Denegación de Servicios (*Denial of Service*)

Las WLANs son muy vulnerables a ataques de denegación de servicios. Un intruso es capaz de dejar un *Basic Service Set* (BSS) no disponible, o interrumpir la conexión entre puntos legítimos. Debido a las propias características de las redes inalámbricas un intruso puede lanzar diversos tipos de ataques *DoS*. Por ejemplo, falsificando tramas de administración, (por ejemplo, des autenticación y des asociación), aprovechando algunas debilidades el propio protocolo, o simplemente bloqueando la banda de frecuencias se puede hacer una denegación de servicios. Sólo tomaremos en cuenta ataques DoS donde se ve realmente la función del intruso. Por ejemplo, borrado de todos los paquetes, usando técnicas como las que fueron descritas en la *Amenaza 3*, aunque el uso considerable de los recursos podría considerarse como un ataque de denegación de servicios, pero no lo vamos a tomar en cuenta por que este podría ser generado por medio de una interferencia

de la señal o una señal *jamming*.

Las *Amenazas 1*, *2* y *3*, son ataques a la capa de enlace, posiblemente afectando la confidencialidad y la integridad de la WLAN. Las *Amenazas 4*, *5* y *6*, corrompen la mutua autenticación. La *Amenaza 7*, interfiere con la disponibilidad y podría ser el seguimiento después de haber pasado por las *Amenazas 1*, *2* y *3*, esto en cualquier tipo de trama. En las siguientes secciones analizaremos la efectividad del 802.11i para defenderse de lo antes mencionado, y en caso de no poder eliminar la amenaza se dan algunas sugerencias o modificaciones que habría que tener muy en cuenta.

3.2. Confidencialidad e Integridad de los Datos

El 802.11i de la IEEE define tres protocolos de confidencialidad de los datos: *Wired Equivalent Privacy* (WEP), *Temporal Key Integrity Protocol* (TKIP) y *Counter-mode/CBC-MAC Protocol* (CCMP). En el Apéndice B se trata WEP. En esta parte nos enfocaremos a hablar sobre CCMP. A diferencia de WEP y TKIP que usan **RC4** como algoritmo de cifrado, CCMP está basado en el algoritmo **AES** *Advanced Encryption Standard*, en el caso del 802.11i se eligió el método de operación de AES CCM (*Counter with CBC-MAC*) con una llave de 128 bits y un tamaño de bloques de 128 bits. CCMP usa (CTR) para la confidencialidad de los datos y CBC-MAC (*Cipher Block Chaining Message Authentication Code*) para la integridad de los datos, usando también MIC (*Message Integrity Code*) que es un código de integridad del mensaje, también conocido como “Michael”. Podemos decir que una llave de 128 bits es relativamente “segura” ante ataques de fuerza bruta al algoritmo AES. Con AES, es posible utilizar una sóla llave para cifrar todos los paquetes, eliminando de esta forma los problemas inherentes a los algoritmos asociados con WEP y TKIP. CCMP también provee protección al cuerpo de la trama y casi a toda la cabecera en las tramas MAC por medio de MIC, el cual previene de ataques a las cabeceras de la MAC. En adición CCMP usa un (PN) *Packet Number* para prevenir ataques de “repetición” (*replay attacks*) y construir un nuevo **nonce**, que en si es un número aleatorio para cada paquete del tamaño de 48 bits, haciendo esto casi imposible de adivinar.

Otro posible ataque, es el del pre-cálculo. Mientras una llave de 128 bits es considerada como "segura" ante ataques de fuerza bruta; CCMP usa un incremental PN para construir "nonces", y cada vez que hace esto el PN es inicializado a uno para cada "TK". Esto podría traer consigo un ataque de pre-cálculo. Un intruso desconectado podría generar un tabla para un específico "nonce" y 2^{64} posibles llaves. A continuación el intruso podría comenzar a observar mensajes cifrados con el nonce seleccionado y una llave desconocida. En promedio el intruso podría encontrar una superposición de llaves después de observar 2^{64} mensajes con el nonce específico y diferentes llaves, obteniendo de esta forma el TK de esa sesión. Este ataque de pre-cálculo reduce el espacio de la llave de 2^{128} a 2^{64}, lo cual, la hace prácticamente descifrable por algún algoritmo de cifrado de bloques.

3.3. Autenticación y Administración de Llaves

3.3.1. Análisis de Seguridad al RSNA

Como ya vimos en el Capítulo anterior, el procedimiento del 802.11i RSNA consiste de la autenticación con base en el 802.1X y el conjunto de protocolos para la administración de las llaves. Para este análisis nos basaremos en la secuencia de 6 fases, que definen el procedimiento de autenticación por medio de RSNA, Ver Fig. 18. Donde la primera etapa se lleva a cabo el descubrimiento o reconocimiento de la red, incluso el tipo de seguridad, en la segunda fase se lleva a cabo la autenticación y asociación definida en el 802.11, en la tercera fase se realiza la autenticación bajo *EAP/802.1X/RADIUS*, en la fase 4 se realiza el *4-Way Handshake*, en la fase 5 lleva a cabo el intercambio de la llave de grupo (*GTK*) en caso de haber una comunicación tipo multicast y finalmente en la fase 6 se lleva a cabo el envío de paquetes, pero de forma segura.

Basándonos en el procedimiento establecido por el RSNA (*Robust Security Network Association*), podríamos analizar la seguridad del 802.11i considerando por separado cada una de las amenazas. Desde que las tramas de administración que no son protegidas, un intruso podría interferir en las fases 1 y 2. Específicamente, las fases 1 y 2 son vulnerables a ataques o amenazas del tipo *1, 2, 3* y *4*, (mencionadas anteriormente).

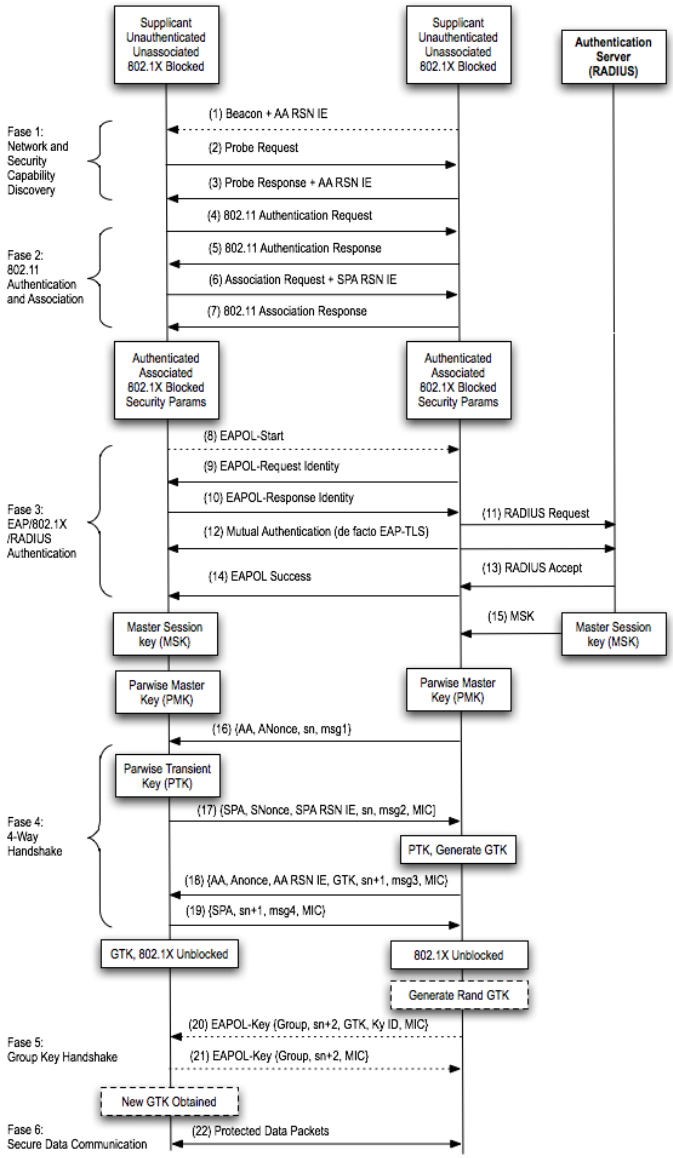


Fig. 18**:** Proceso RSNA (*Robust Security Network Association*).

Un intruso puede enviar paquetes hacia un suplicante suplantando a un autenticador genuino. Una vez que esto ocurra, el suplicante podría ser forzado a usar parámetros inapropiados de seguridad para comunicarse con el autenticador legítimo, o llegar a asociarse con un punto de acceso maligno. Alternativamente, un intruso podría falsificar peticiones de asociación al autenticador con la posibilidad de vulnerar la seguridad. Afortunadamente, estas amenazas son eliminadas en la *Fase 3* si, sólo si, el método de autenticación mutua es robusto. Por ejemplo, haciendo uso de EAP-TLS, se prevé de ataques de falsificado, replicado y modificación de paquetes, eliminando así amenazas del tipo *1, 2* y *3*. Adicionalmente, si se pide la dirección MAC para asociarse, se suprime amenazas del tipo *4*. Después de que los puntos son autenticados y el intercambio de algunos secretos se ha llevado a cabo, después de la *fase 3*, los siguientes intercambios de paquetes son resistentes a esas amenazas. En el caso de que se omita la *fase 3* por que se use una PSK *Pre Shared Key*, cada uno de los puntos se puede autenticar con el otro verificando la posesión de la llave compartida en la *fase 4*. Además la *fase 4* también puede verificar la negociación de la seguridad implementada.

Amenazas del tipo 5 pueden existir aún y cuando se haya implementado un fuerte mecanismo de autenticación. Después de que una estación legítima haya completado con éxito su autenticación, un intruso puede desconectar a la estación por medio del envío de mensajes de de-autenticación y des-asociación, y reanudar la sesión con el AP suplantando la estación legítima. Aquí hay dos puntos que hay que considerar. El primer punto, si la sesión permite al intruso solo aceptar paquetes, esto parecería justamente ser sólo un ataque de escucha de paquetes (*eavesdropping*), el cual es prevenido por medio de algún mecanismo de confidencialidad. El segundo punto es, si la sesión requiere una interacción del intruso, el intruso forzosamente necesita obtener cierta información para poder autenticar a la estación (víctima), esta información es la PTK, esto también para poder generar tráfico supuestamente legítimo. En general, amenazas del tipo *5* no posee más peligro que ataques de captura de tráfico y ataques de denegación de servicios (DoS), esto en la estación.

Las amenazas del tipo *6* se pueden presentar en las WLANs, siempre y cuando no se

haya implementado algún mecanismo de autenticación. Un intruso podría establecer dos conexiones separadas, una hacia el suplicante y otra hacia el autenticador y de esta forma construir un ataque de "Hombre en Medio" (*MitM*). Para llevar a cabo esta técnica, el intruso, primero debe enviar tramas de de-autenticación para desconectar la estación del punto de acceso legítimo. En este momento, depués de varios intentos fallidos, la víctima podría probar con un punto de acceso diferente y eventualmente asociarse con el punto de acceso maligno, tal vez en un canal diferente. Al final el intruso se asocia con el punto de acceso legítimo suplantando la identidad de la estación. Sin embargo cuando el 802.11i es implementado con un fuerte mecanismo de autenticación mutua, usando por ejemplo **EAP-TLS**, tal vez el intruso no pueda autenticar el mismo a la estación ya que no posee las credenciales apropiadas. Por supuesto que el intruso puede reenviar los paquetes de autenticación hacia el punto de acceso; pero los paquetes de autenticación, no pueden ser modificados o reenviados, de forma que el intruso solo puede hacer la función de reenviar paquetes, lo cual causa menos daño que un ataque de captura de paquetes (*eavesdropping*). Sin embargo, si el mecanismo de autenticación mutua no es implementado adecuadamente, un intruso puede ser capaz de lanzar un ataque *MitM* y posteriormente conocer la PMK. Aunque esta vulnerabilidad es considerada una debilidad específica de los protocolos de la mutua autenticación en el 802.11i. Cualquier implementación del 802.11i debería considerar encarecidamente este problema.

En resumen, si lleva a cabo el proceso del RSNA, la autenticación y el proceso de la administración de las llaves podrá decirse que es segura la comunicacón. Sin embargo desde que un intruso puede intervenir en la comunicación, ya sea con una simple captura de tráfico, *Fase 1* y *2*, puede ser capaz de engañar al autenticador o al suplicante, e impedir el proceso completo del RSNA; esto se describe con más detalle en un ataque que vamos a ver un poco más adelante, que es por medio de un ataque de reducción de niveles de seguridad (*Security Level Rollback*). Además algunas malas implementaciones permiten ataques de reflexión en la *Fase 4* del RSNA; aunque hasta este punto se asume que el enlace entre el "autenticador" y el "servidor de autenticación" es seguro, un intruso aún con eso podría descubrir el secreto compartido en el Servidor "RADIUS" por medio de un ataque de fuerza bruta, basado en un diccionario. Cuando una PSK de 256 bits es usada

como PMK, esta PSK podría ser derivada de una frase *passphrase*, lo cual permite que la PSK sea vulnerable a ataques de diccionario. En una buena implementación se debe tomar muy en cuenta el hacer uso de una política para poder generar una buena frase o directamente hacer uso de valor aleatorio de 256 bits para eliminar los problemas de esta vulnerabilidad.

3.3.2. Ataques a la Reducción de Niveles de Seguridad (*Security Level Rollback Attack*)

Cuando en una red inalámbrica se usan los dos algoritmos, tanto el Pre-RSNA y el RSNA, un intruso puede lanzar ataques donde puede disminuir los niveles de seguridad. Existen algunas diferencias de opinión en cuanto a que este ataque no es propiamente una vulnerabilidad, ya que una implementación con RSNA bajo el 802.11i, no acepta una segunda implementación con Pre-RSNA. Además el 802.11i no define el uso de una Transient Security Network (TSN) que soporte ambos algoritmos (Pre-RSNA y RSNA), lo cual es recomendable para implementaciones de redes inalámbricas seguras. En general, nuevas implementaciones de redes inalámbricas deberían contar con equipo que soporte algoritmos Pre-RSNA para posteriormente pensar en una migración completa hacia RSNA. Desde luego que los "suplicantes" también deben de contar con cierto tipo de hardware que soporte estos protocolos. Esta configuración híbrida puede degradar la seguridad del sistema a los niveles más bajos.

La Fig. 19 muestra un ataque de este tipo. En esta figura, las lineas continuas representan la secuencia de los mensajes legítimos y las lineas discontinuas muestran los mensajes enviados por un intruso. En este ataque, el intruso suplanta al autenticador, falsificando los "Beacon" o las tramas de "Probe Response" asi el suplicante, indicando que sólo es soportado el Pre-RSNA (WEP). Del otro lado, el intruso puede suplantar al suplicante, enviando tramas de petición de asociación (*Association Request*). Como resultado de esto, el suplicante y el autenticador podrían establecer una conexión por medio de Pre-RSNA, aunque los dos soporten el algoritmo RSNA. Ya que no existe alguna función de verificación en el algoritmo Pre-RSNA, el suplicante y el autenticador no pueden detectar una falsificación de los paquetes. Aún peor, un intruso es capaz de revelar las

llaves establecidas por defecto por medio de la explotación de la vulnerabilidad de WEP, lo cual disminuye completamente la seguridad. Este ataque es prácticamente factible ya que puede realizar un ataque MitM o falsificar el envío de las tramas de administración oportunamente, esto es, paquetes Beacon o "Probe Response" hacia el suplicante y tramas de petición de asociación (*Asosiciation Request*) hacia el autenticador.

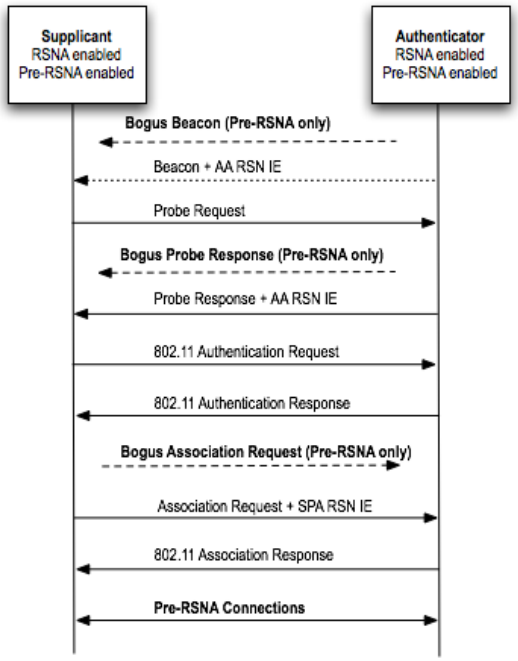


Fig. 19**:** Ataque de Reducción de Niveles de Seguridad.

Lo solución más simple a esta vulnerabilidad, es que tanto el suplicante como el autenticador solo permitan conexiones RSNA. Sin embargo, esto es solo aceptable cuando la seguridad debe ser estricta, por ejemplo a nivel empresarial. En varias implementaciones de redes inalámbricas, TSN podría ser la mejor opción para proveer servicio a más usuarios. Por lo tanto, ambas entidades, el suplicante y el autenticador, deben aceptar conexiones usando Pre-RSNA y RSNA, pero tomando en cuenta una fuerte política en cuanto a seguridad se refiere. Específicamente, el suplicante debería decidir si quiere mayor confidencialidad (RSNA), o quiere mayor disponibilidad de acceso a la red (Pre-RSNA). En cualquier caso, el suplicante debería tener oportunidad a denegar algoritmos Pre-RSNA, antes de iniciar la conexión, ya sea manualmente o por medio de la configuración de

alguna política. Otra forma es que el autenticador limite las conexiones donde se use Pre-RSNA. Mientras que esta política podría causar algunos inconvenientes, esto podría ser un valor agregado a la seguridad. Esto es absolutamente inseguro para que los dispositivos seleccionen un nivel de seguridad transparente, ya que el autenticador y el suplicante no tienen conocimiento de la autenticidad de la *Fase 1* y *2*.

3.3.3. Ataques de Reflexión (*Reflection Attack*)

En la *Fase 4*, el "4-Way Handshake" hace uso de criptografía simétrica para proteger la integridad de los mensajes. Tanto el autenticador y el suplicante conocen la PMK, solo ellos son capaces de calcular los correctos MICs y poder crear mensajes válidos. Éste hecho soporta autenticación. Sin embargo, si un dispositivo es implementado para fungir tanto como autenticador y como suplicante bajo la misma PMK, un intruso puede lanzar un ataque de reflexión a este dispositivo, como se muestra en la Fig. 20. Cuando el dispositivo inicia un "4-Way Handshake" como un autenticador, el intruso podría iniciar otro "4-Way Handshake", con los mismos parámetros pero con el dispositivo víctima actuando como si fuese un suplicante. Una vez que la víctima es engañada, el intruso podría usar esos mensajes como respuestas válidas para el "4-Way Handshake" iniciado por la víctima.

Naturalmente este escenario probablemente no se presente en una infraestructura de red, por que el dispositivo legítimo tal vez nunca tenga las dos tareas, la de suplicante y la de autenticador a la vez. Sin embargo, en redes ad hoc, un posible uso del 802.11i podría permitir a cada dispositivo servir ambos roles para distribuir sus propios GTKs. Esto crearía un posible ataque de reflexión.

3.3.4. Disponibilidad

La disponibilidad, al parecer no es uno de sus principales objetivos en una implementación del 802.11i, dejando varias vulnerabilidades a ataques DoS, incluso si se ocupan fuertes protocolos de autenticación y confidencialidad. Comparando el daño de ataques DoS en la capa física con las vulnerabilidades del 802.11i con respecto a ataques DoS, estos últimos parecen causar más problemas, por varias razones. Primero, un intruso puede

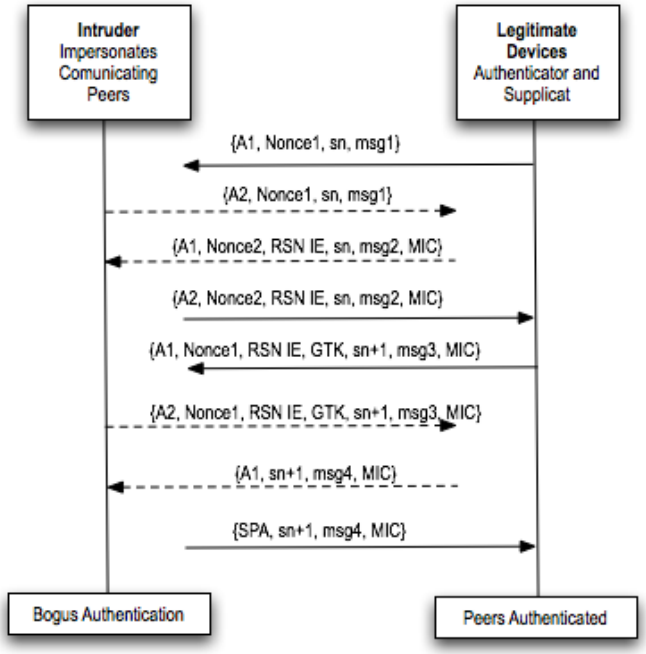


Fig. 20**:** Ataque de Reflexión en el 4-Way Handshake.

lanzar un ataque al 802.11i mucho más fácil que un ataqué a la capa física, con ciertos dispositivos. Segundo, es mucho más complicado para un administrador de redes localizar el punto del ataque. Además, la abstracción del modelo capas es un concepto importante en redes, requiriendo que cada capa tenga funcionalidad independiente. Y esto es apropiado para el 802.11i para resistir ataques DoS. Además un 802.11i más robusto podría ayudar en un futuro a una migración de capa física con otros especificaciones.

3.3.4.1. Ataques DoS

Desde que las tramas de administración y control no son protegidas en una WLAN, un intruso puede fácilmente falsificarlas y lanzar ataques DoS. Entre los ataques a las tramas de administración, el ataque más eficiente es el de falsificar y repetidamente enviar tramas de de-autenticación y des-asociación. Desafortunadamente estos ataques persisten aún y cuando se implementa el 802.11i. Se debería considerar un administrador central para manejar esas tramas específicamente e identificar la falsificación de las tramas por sus comportamientos anormales. Sin embargo, esto requiere funcionalidades extras en

el servidor de autenticación, y el servidor necesitaría mantener los estados de todos los suplicantes. Esto incrementaría la carga de trabajo del servidor y podría ser irrealizable. Otra opción podría ser la de responder a las tramas de deautenticación y des-asociación por medio de la reanudación del proceso del "4-Way Handshake", con un resultado del 4-Way Handshake indicando que algunas tramas han sido falsificadas. Este método podría limitar el impacto de la falsificación de mensajes de des-asociación y deautenticación para el 802.11 en la MAC. Sin embargo, esto no previene el ataque, ya que se forzaría a efectuarse periódicamente el 4-Way Handshake lo cual traería un ataque DoS muy efectivo. Basándonos en estas consideraciones, las tramas de autenticación parecen ser la mejor opción. Por otro lado, el uso de las tramas de control de autenticación podría ser ineficiente y añadir mucha carga, ya que el control de tramas podría ser muy frecuente.

Existen varios ataques DoS que explotan los mensajes EAP sin protección en la autenticación del 802.1X. Específicamente un intruso puede falsificar mensajes de comienzo de EAPOL (*EAPOL-Start*) repetidamente para impedir la completa autenticación del 802.1X, falsificando mensajes EAPOL-Success de forma maliciosa para llegar al puerto del 802.1X en el suplicante sin autenticación, y falsificando EAPOL-Failurey mensajes EAPOL-Logoff para desconectar al suplicante. Afortunadamente, esta vulnerabilidad puede ser eliminada en el 802.11i por el simple hecho de hacer caso omiso a estos mensajes. Esto no afecta en nada la funcionalidad del protocolo. El resultado del siguiente 4-Way Handshake podría tomar el rol de un EAPOL-Success y EAPOL para indicar el resultado de la autenticación; EAPOL-Logoff puede ser reemplazado por una de-autenticación para desconectar al cliente; y EAPOL-Start no sería necesario para el protocolo.

Un intruso puede también lanzar ataques DoS en el AP por medio de la inundación de tramas falsificadas de petición de asociación. Esto podría agotar el espacio del identificador del EAP, el cual es sólo de 8 bits de longitud. Esta vulnerabilidad puede ser mitigada por medio de algunas consideraciones durante la implementación. Ya que un identificador EAP es solo requerido para ser único en una única asociación en el 802.11, esto no es necesario para que el AP deniegue nuevas peticiones de conexiones cuando el espacio del identificador del EAP es agotado. Particularmente el AP puede adoptar un identificador

EAP separado para cada asociación.

3.3.4.2. Contramedidas en el Algoritmo Michael

En adición a los ataques DoS antes mencionados, el algoritmo *Michael* es también vulnerable a este tipo de ataques. TKIP, que es un protocolo que se usa para la confidencialidad de datos, adopta el algoritmo Michael para proveer de protección a los MSDU (*MAC Service Data Unit*). El formato MPDU (*MAC Protocol Data Unit*) de TKIP es mostrado en la Fig. 21. El algoritmo Michael sólo tiene designados para su seguridad 20 bits debido al limitado poder de algunos dispositivos. Esto significa que un intruso, después de 2^{19} intentos falsificados puede llegar a tener éxito su ataque. Sin embargo TKIP implementa una contramedida para limitar una ráfaga de intentos para vulnerar la seguridad. Una vez que se detecta un ataque de este tipo la transmisión y recepción de mensajes se bloquea por 60 segundos. Además el autenticador puede reenviar la llave o de-autenticar al suplicante, el suplicante debería reportar el problema con el algoritmo y posteriormente cerrar la sesión él mismo.

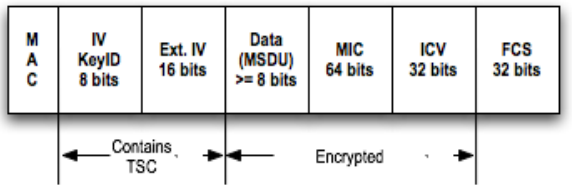


Fig. 21**:** Formato TKIP MPDU.

La contramendida en el algoritmo asegura que la conexión por un intruso haciendo uso de ésta técnica sea casi imposible de conseguir. En una red 802.11b, un intruso puede enviar aproximadamente 2^{12} mensajes por segundo. Por lo tanto, un intruso es capaz de crear un mensaje falsificado que tuviese éxito en aproximadamente 2 minutos, esto si no se implementara alguna defensa para este ataque. Sin embargo si se implementa algún mecanismo para contrarrestar la tasa de transferencia de mensajes falsificados, tal vez serían dos intentos falsificados por minuto, el ataque tendría éxito en aproximadamente 6 meses. Desafortunadamente la protección ante este ataque trae consigo un posible ataque DoS; un intruso puede enviar mensajes falsificados causando fallas al propio algoritmo

Michael MIC y lograr de esta forma tirar la conexión. Para prevenir este tipo de ataques DoS, el protocolo checa el FCS (*Frame Check Sequence*), el ICV (*Integrity Check Value*), el TSC (*TKIP Sequence Control*) y la secuencia del MIC. Una falla en el MIC solo es registrada cuando las tramas del FCS, ICV, TSC son correctas pero las del MIC no lo son. Checando las tramas del FCS e ICV se pueden detectar errores en los paquetes, pero muy posiblemente causados por el "ruido", mientras que checando el TSC se pueden detectar paquetes replicados. Además si el intruso modifica el TSC, modificaría la llave de cada paquete al mismo tiempo, lo cual cusaría una falla al tratar de descifrar cada paquete. Por lo tanto, una revisión completa del FCS, ICV, TSC y el MIC podría causar un ataque DoS.

En la definición de las amenazas del tipo 3, definimos que un intruso puede capturar los paquetes, incluso antes de que llegue a su destino. A través de este enfoque, un intruso puede obtener un TSC válido, manteniendo el campo del TSC sin modificaciones, el intruso puede modificar algunos bits del paquete, actualizando los campos del FSC e ICV, haciendo esto más consistente, debido a la vulnerabilidad en el algoritmo del ICV. Cuando el intruso haya obtenido el paquete deseado, esto, por que el paquete puede pasar la revisión del FCS, ICV, TSC pero con un inválido MIC. Por el envío de este paquete, el intruso puede forzar a fallar al algoritmo Michael MIC del lado del receptor, y eventualmente lanzar un ataque DoS. Aún peor, desde que el 802.11i sugiere actualizar el TSC hasta que el MSDU pase el chequeo del algoritmo, si el destinatario implementa alguna función para reanudar la sesión después de los 60 segundos sin reenvío de la llave, el intruso puede simplemente reenviar mensajes modificados repetidamente por que el TSC es aún válido después de la primer falla. Por otro lado, si el destinatario reenvía la llave, el intruso podría tener suficiente tiempo para construir el próximo paquete y de esta forma bloquear la comunicación. Por supuesto que esto no es tan fácil, ya que se requiere la captura de demasiados paquetes. Sin embargo, esto es muy práctico ya que el tiempo requerido para un reenvió de llaves o re-autenticación es tiempo suficiente para que un intruso pueda construir un paquete.

Este ataque puede ser mitigado tomando en cuenta algunas consideraciones. Primero,

el reingreso y la de-autenticación no son necesarias cuando la disponibilidad es el objetivo. El autenticador y el suplicante deberían esperar los 60 segundos, y entonces si, reanudar la comunicación. Segundo, el TSC debería actualizarse desde que el paquete pasa la revisión del FSC, ICV y TSC, incluso si ocurre alguna falla en el algoritmo Michael MIC. Cabe notar que los paquetes retransmitidos deben usar un nuevo valor de TSC. Y aunque esto no termina completamente con la posibilidad de sufrir un ataque DoS, minimiza el riesgo. Afortunadamente, este ataque desaparece cuando se implementa CCMP para la confidencialidad de los datos.

3.3.4.3. Bloqueo del 4-Way Handshake

Como ya vimos, el 4-Way Handshake es un componente esencial en el RSNA. Su propósito es de confirmar la posesión de la PMK (*Pairwise Master Key*) compartida en el autenticador y en el suplicante, y derivar una nueva PTK (*Pairwise Transient Key*) para los siguientes handshakes. En el handshake para autenticarse, el autenticador y el suplicante generan sus propios nonces y se los envían el uno al otro. La PTK es derivada a partir de la PMK, el nonce y la derección MAC de los dispositivos. El mensaje 1 y 3 portan el nonce generado por el autenticador; el mensaje 2 el nonce generado por el suplicante y el mensaje 4 es el mensaje de aceptación para indicar que todo se ha realizado satisfactoriamente. Mientras que el mensaje 2, 3 y 4 son verificados por la nueva PTK, el mensaje 1 viaja sin protección. En fin, para prevenir ataques a la PTK por medio de mensaje falsificados, el 802.11i adopta una PTK Temporal (*TPTK*) para almacenar la nueva PTK hasta que el mensaje 3 sea verificado. Sin embargo, este enfoque no detiene los ataques DoS en el mensaje no cifrado (mensaje 1).

El suplicante debe aceptar todos los mensajes 1s que recibe con el fin de garantizar el intercambio de mensajes para el inicio de una asociación en caso de pérdida de paquetes o una retransmisión. Esto permite a un intruso generar una PTK inconsistente entre el suplicante y el autenticador por medio de mensaje de tipo 1, donde el nonce tiene un valor diferente entre el mensaje 1 (legítimo) y el mensaje 3. Con el fin de ordenar todos los mensajes 1s, el suplicante almacena todos los nonces generados y las PTKs derivadas. Solo después del mensaje 3 cuando el MIC válido es recibido el suplicante puede instalar

la correcta PTK para una comunicación y así descartar todos los demás. Obviamente un intruso puede lanzar un ataque DoS a la memoria, por medio del envío de una cantidad masiva de mensajes topo 1, como se muestra en la Fig. 22. Este ataque es de suma importancia ya que su implementación es simple y tendrá éxito mientras deniegue el poder autenticarse el suplicante.

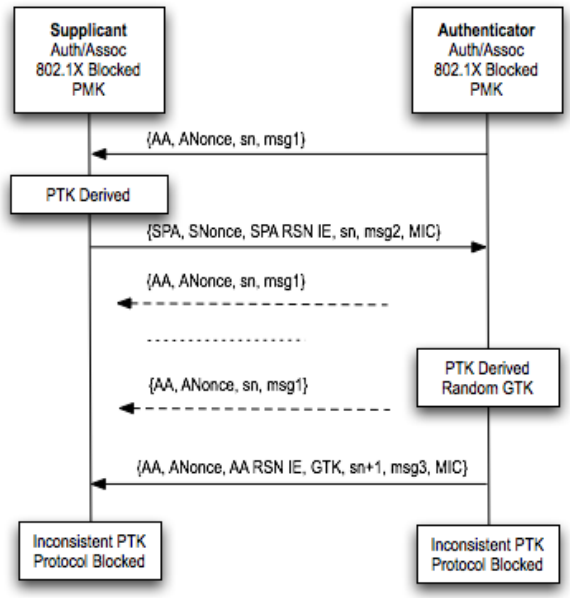


Fig. 22**:** Bloqueo del 4-Way Handshake.

Existen algunos criterios para poder hacer frente a esta vulnerabilidad. Primero, los mensajes 1s, podrían ser autenticados para defenderse de este ataque, puesto que el autenticador y el suplicante ya han logrado intercambiar algunos mensajes e incluso se ha llevado a cabo la autenticación. Sin embargo, esto requiere de algunas modificaciones al formato del mensaje; además el autenticador tendría que añadir un número secuencial en cada mensaje 1, con el fin de prevenir replicación de mensajes. Segundo, el suplicante puede eliminar este tipo de ataques por medio del re-uso del mismo nonce para todos los mensajes 1s recibidos hasta que se complete con éxito el 4-Way Handshake. El suplicante solo guarda un nonce, calcula la PTK por medio de este nonce almacenado y el nonce recibido en el otro mensaje, entonces verifica el MIC. Este enfoque requiere menos

modificaciones al algoritmo del lado del suplicante; el suplicante no necesita almacenar más de una vez un nonce, eliminando de esta forma un posible ataque de desbordamiento de memoria. Sin embargo el suplicante podría requerir mayor procesamiento, puesto que necesitaría calcular la misma PTK dos veces, por los mensajes recibidos (1 y 3), dado que el nonce recibido y derivado de las PTKs no es almacenado. El suplicante tiene que tomar una decisión entre la desventaja del desbordamiento o el mayor consumo de procesamiento. Como una solución combinada, el suplicante puede re-usar el mismo nonce para todos los mensajes 1s para eliminar la vulnerabilidad de un ataque al desbordamiento de la memoria y almacenar l aPTK derivada para un mejor rendimiento.

El diseño del 802.11i parece estar más enfocado en la seguridad que en el preservar la disponibilidad. Una vez que los eventos relacionados con la seguridad o una desconexión ocurre, se sugiere una de-autenticación o una des-asociación. Este proceso reduce fugas de información y previene futuros ataques, pero esto también incrementa la posibilidad de que ocurran ataques DoS. Por lo tanto, se deben especificar ciertos esquemas de recuperación cuando se presente algún ataque DoS significativo. Un esquema de recuperación después de una falla no previene el ataque, sin en cambio, se convierte en un esquema más eficiente, y por lo tanto, los intentos de ataques se vuelven más difíciles de que surjan efecto. Por ejemplo en el Group Key Handshake, un retardo en la conexión, podría causar que el autenticador de-autentique o des-asocie al suplicante. El suplicante tendría entonces que re-asociarse en el mismo AP o "buscar" en otro canal para conectarse a orto AP, lo cual sería tiempo perdido. Además el autenticador primero tiene que crear la GTK y posteriormente cada suplicante; aunado a esto el retraso de reasociación de un suplicante podría afectar a los demás. Alternativamente si el suplicante y el autenticador solo reintentan el Group Key Handshake o el 4-Way Handshake, se podría resumir el proceso de reconexión. Por otro lado si el retraso del Group Key Handshake se debe a la indisponibilidad del suplicante, por ejemplo, si el suplicante se mueve fuera del rango de cobertura, se pierde mucho más tiempo en el reintento del Group Key Handshake o el 4-Way Handshake comparado con que, si solamente se des-asocia del primer AP y se re-asocia con el otro AP. Esto es una desventaja del protocolo y se debe estudiar con mayor detenimiento según el ambiente de la red.

Asumiendo que en algún momento el protocolo está corriendo entre par de estaciones; y en algún momento falla debido a un ataque activo. Si el protocolo se reinicia, podría ser vulnerable a ataques DoS. Lo que significa, que si el intruso puede causar que falle en algún punto el protocolo, podría lanzar un ataque DoS, haciendo repetidamente esta operación. Cada vez que un usuario "legítimo" requiere que se le reenvíe algún paquete perdido o con errores, el intruso tiene más tiempo para poder construir un ataque. Por otro lado, si el protocolo se recupera desde el punto en donde falló, el intruso no tendría tanto tiempo para lanzar tan fácilmente un ataque, y aunque se resuelve un problema, surge otro del mismo tipo (DoS). Donde el intruso capta la atención del usuario antes de que se conecte al AP legítimo.

Específicamente en el 802.11i es razonable pensar que es complicado falsificar una autenticación haciendo uso del 802.1X. Sin embargo, una vez que los handshakes comienzan entre el suplicante y el autenticador y ocurre un error, el punto de recuperación puede ser seleccionado en el punto más cercano para mejorar la eficiencia de los protocolos, ya que las dos entidades "se supone" que pertenecen a una comunicación legítima. Por otro lado si no se llega a concluir la autenticación 802.1X entre el suplicante y el autenticador, podría ser mejor que el protocolo reinicie todo su proceso desde el principio. Desde luego que en un ambiente con mucha movilidad, las fallas se presentarán con más frecuencia ya que una entidad estaría fuera del alcance (no disponible) ; así, si reintenta con el punto más cercano podría perderse más tiempo , sin embargo desde que se hace el escaneo del canal el tiempo ya es relativamente largo, tanto como el que se lleva la ejecución del protocolo completa, de esta forma logramos ver que tal vez el reintento de conexión con el punto más cercano podría no ser tan largo comparándolo con el total del retardo, si se vuelve a hacer una concexión nueva.

3.3.4.4. Proponiendo mejoras al 802.11i

Tomando en cuenta lo anterior, a continuación se propone un esquema para el 802.11i el cual crearía una mayor resistencia a ataques DoS. Debido a que la capa física es vulnerable por naturaleza, los ataques DoS siempre van a existir ya que existen frecuencias *jamming*, redes *jamming* u otro tipo de problemas. En la Fig. 23 se muestra un diagrama un poco más resistente a ataques DoS al 802.11i.

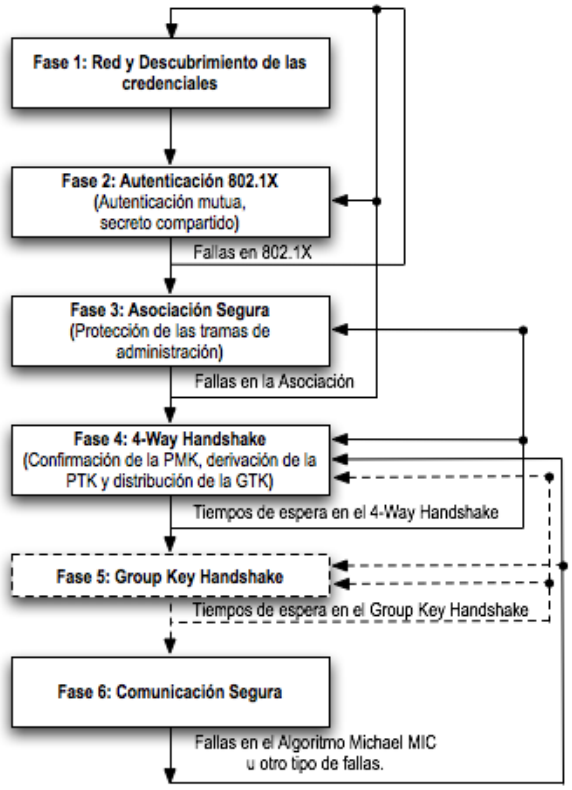


Fig. 23**:** Mejoras al 802.11i.

- Con el fin de eliminar los ataques DoS que se realizan por medio de la inundación de peticiones de asociación, es mejor llevar a cabo la autenticación antes de que se realice la asociación. Específicamente, en el 802.11i es posible reemplazar la entidad de autenticación en el 802.11 con una autenticación haciendo uso del 802.1X.

- El proceso de autenticación y la administración de las llaves debe ser verificado tan pronto como sea posible. De lo contrario, en los siguientes handshakes podría perderse tiempo ya que el conjunto de tramas de negociación podría ser falsificado por un intruso. Específicamente, cuando se adopta una autenticación 802.1X, los puntos pueden verificar sus parámetros de seguridad, durante la autenticación 802.1X; cuando una PSK o una PMK es usada, los puntos pueden verificar la información para una re-asociación segura.

- Las tramas de administración deben ser autenticadas para obtener mayor seguridad, y algunas tramas de control tal vez también, en caso de ser necesario. La autenticación de estas tramas debería llevarse a cabo lo antes posible. Desde que el proceso de autenticación se realiza con éxito, el secreto común debería ser usado para autenticar las siguientes tramas de administración, especialmente las tramas de petición y respuesta de una re-asociación. A través de este enfoque se elimina la vulnerabilidad en las tramas de administración, excepto en los *Beacon*, *Probe Request* y *Probe Response*, las cuales no pueden ser autenticadas.

- Un apropiado esquema de recuperación después de una falla debe ser implementado para mejorar la eficiencia de los protocolos. En una infraestructura de red con poca movilidad, asumiendo que se provee de una fuerte autenticación, el protocolo podría recuperarse desde el punto más cercano si el 802.1X se completó con éxito, mientras que el protocolo podría reiniciarse si no se completó la autenticación en el 802.1X.

Por estas mejoras, se podrían eliminar varias de las vulnerabilidades antes mencionadas, y se tendría una infraestructura más robusta en cuanto a seguridad del sistema se refiere.

Conclusiones

3.4. Caso de Estudio

Con base en un ataque pasivo (*sniffing*), por medio de una técnica llamada "*wardriving*", la cual consiste en rastrear redes inalámbricas desde un automóvil por medio de una computadora portátil, una tarjeta de red inalámbrica y un software especial, se llevó a cabo la captura de las redes inalámbricas de área local en una zona de la ciudad de México con demasiada actividad empresarial, esto con el fin de analizar el número de redes que cuentan con cierto grado o no de seguridad.

Fig. 24**:** Equipo para Wardriving.

Existen una infinidad de herramientas para poder hacer esta taréa y las hay para diferentes Sistemas Operativos. Tomando en cuenta que “Linux” es un sistema operativo estable y que en éste fue donde comenzaron a surgir estas herramientas, hicimos uso de él y de aplicaciones como “Kismet” y la “Suite de Aircrack”. También se usaron algunas antenas para poder obtener un mayor rango de cobertura que el ofrecido por la simple tarjeta inalámbrica, en la Fig. 24 se muestra el equipo utilizado.

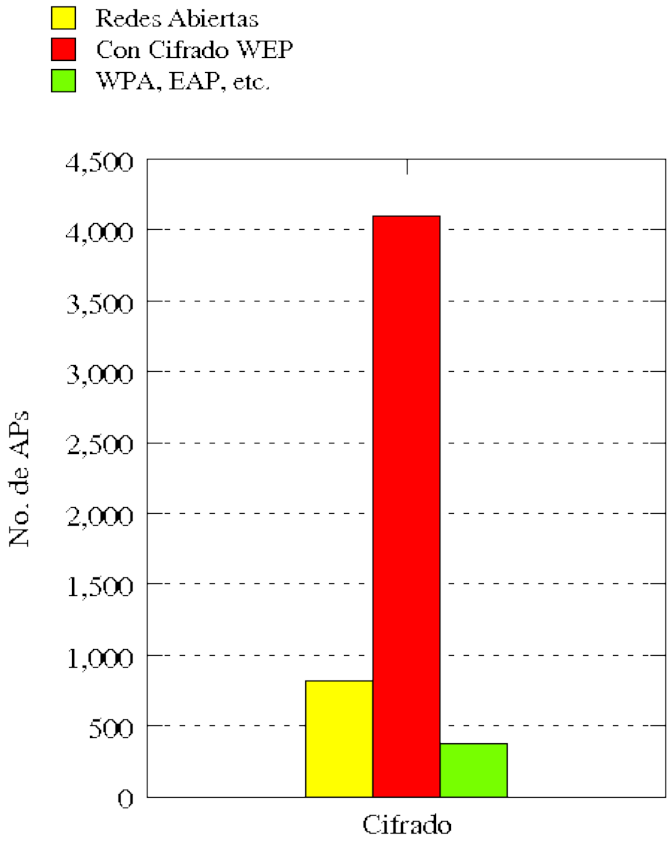


Fig. 25**:** Identificación de Redes por el Sistema de Cifrado.

Como bien sabemos WEP (*Wired Equivalent Privacy*), es el sistema de cifrado más antiguo implementado para mitigar la inseguridad en redes inalámbricas, y por ende el más vulnerable, en el “Apéndice B” se describe el funcionamiento del cifrado WEP. Aún y “a sabiendas de esto”, existen numerosas redes que tienen implementado éste, como

único método de seguridad. En la Fig. 25 se muestra una gráfica que representa la cantidad de redes que implementan de menos algún tipo de seguridad.

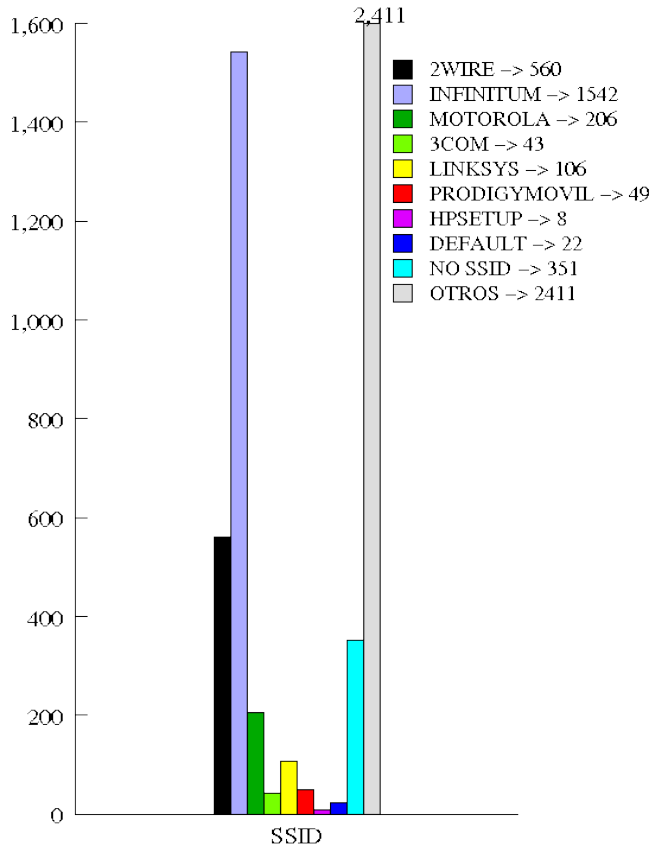


Fig. 26**:** Identificación de Redes por su SSID.

En la Fig. 26 se muestra la cantidad de redes que usan el SSID (*Service Set IDentifier*) que trae por defecto el AP o el Router-AP. A partir de esto podemos identificar, tal vez el tipo de dispositivo y con ello algunas vulnerabilidades de este; ahora bien algo con mayor relevancia, es que diversos dispositivos, sino es que la mayoría se configuran por medio de una interfáz web, aunque esta interfáz en algunos dispositivos te pide un nombre de usuario y una contraseña para poder entrar a la configuración y hacer cambios; si no se cambian estos parámetros se puede entrar a internet y buscar los parámetros por defecto y de esta forma acceder a la configuración y por lo consiguiente, crear una nueva configuración, dejando al propietario tal vez sin servicio, en el peor de los casos !!.

Ahora bien el principal foco de este trabajo de tesis, fue el de la seguridad en redes inalámbricas de área local, y como vimos antes, nos referimos a redes que se encuentran en la frecuencia de los 2.4 GHz., pero dentro de esta rango tenemos varios canales y obviamente los dispositivos inalámbricos de esta tecnología pueden tomar cualquiera de estos canales (11 para esta área geográfica) para poder transmitir, la Fig. 27 muestra una gráfica que representa la cantidad de dispositivos que aparecieron en cada canal.

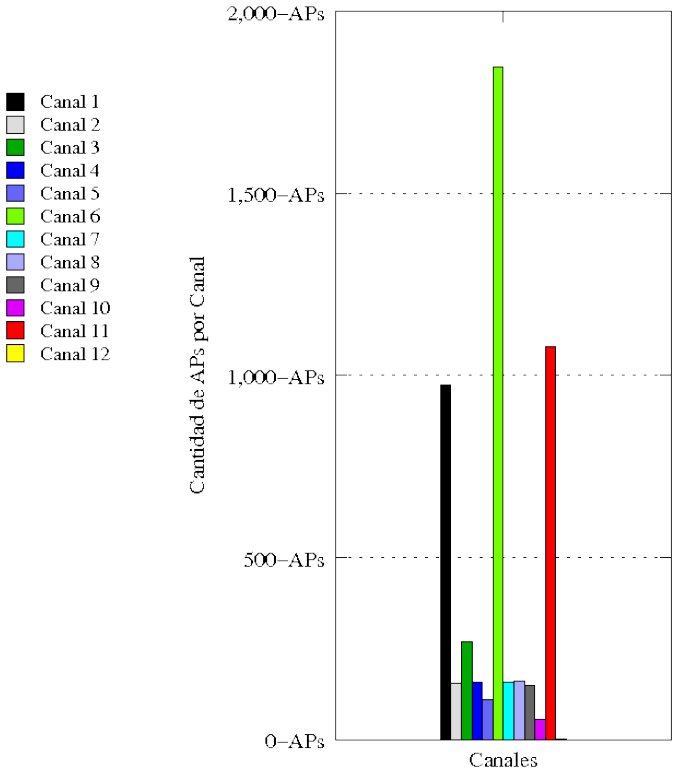
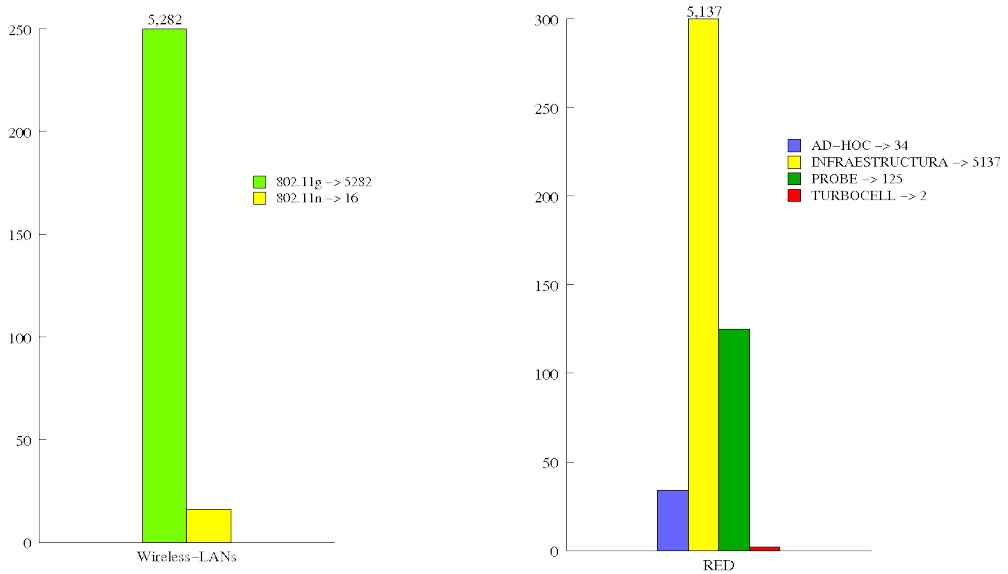


Fig. 27**:** Identificación de Redes por Canal.

Y la Fig. 28a refleja el número de dispositivos que se encuentran en las frecuencias de redes inalámbricas de área local. En la gráfica se muestra la cantidad de redes que usan el nuevo estándar 802.11n el cual puede trabajar tanto en las frecuencias de 2.4 y 5 GHz.. Hace que dispositivos no tan nuevos puedan conectarse a estas redes y los dispositivos hechos para este tipo de tecnología obteniendo un rendimiento mucho mayor y alcanzando



a) b)

Fig. 28**:** Identificación de Redes por: *(a)* Estándar utilizado. *(b)* Topología

velocidades de transferencia de hasta 600 Mbps (en teoría).

Como vimos antes existen distintos tipos de red la Fig. 28b muestra los diferentes tipos de red capturados por *Kismet*.

En el desarrollo de este trabajo se han planteado algunos conceptos básicos sobre redes inalámbricas, algunos de los beneficios que se puede obtener al hacer uso de esta tecnología y en especial algunos factores de inseguridad a los cuales se presentan las redes inalámbricas; en el Apéndice B hacemos referencia al primer mecanismo de cifrado que se ocupó en las redes 802.11 y aunque es demasiado vulnerable aún muchas empresas siguen haciendo uso de el.

En el caso de estudio realizado, se muestra la cantidad de puntos de acceso que pueden llegar a ser vulnerados por un atacante, y es que es realmente sencillo romper la seguridad de aquellos nodos que cuenten simplemente con un mecanismo de cifrado como WEP, existe demasiada información, manuales y hasta videos de cómo poder llevar a cabo esta

tarea. Por ello es que hay que hacer conciencia sobre esto y cambiar los sistemas de cifrado a utilizar por los puntos de acceso.

Y es que a la hora de implementar una red inalámbrica no solo se enfrenta uno a la inseguridad en os sistemas de cifrado o autenticación y es que si nuestra red inalámbrica está conectada a la red cableada de nuestra organización es también afectada por la infinidad de amenazas que hay en estas redes y más aún, si esta está conectada a internet, por ejemplo virus, troyanos e incluso las propias vulnerabilidades del propio hardware del punto de acceso.

La "inseguridad" en redes inalámbricas es inmensa. Existen tantos tipos de ataques que puede sufrir esta tecnología que si se le hace mención de todos ellos al usuario, tal vez tomaría mayor conciencia al conectarse a cualquier tipo de red de esta tecnología. Y es que a pesar de que existen diversos mecanismos, protocolos y buenas prácticas para contrarestar algunas amenazas, aún hay un problema más grande que los descritos en todo este trabajo de tesis y es, **"la ignorancia"**. Y es que en la actualidad cuando un usuario adquiere un dispositivo inalámbrico o se asocia a un punto de acceso lo único por lo que se preocupa es por que funcione (*disponibilidad*), pero no se preocupa si cuenta con los mecanismos necesarios para mantener una comunicación segura, sino hasta que se les presenta algún problema, por ejemplo, pérdida de información, algún tipo de reducción de rendimiento, etc.. Y es que la cultura informática en especial de tópicos relacionados con la seguridad es casi nula.

Hoy en día la seguridad se debe tomar muy en cuenta en cualquier ambiente de redes no sólo de redes inalámbricas y es que debe se parte del diseño y no como algo que se le puede añadir. A partir de este enfoque se pueden tomar diversas medidas para mantener un mejor rendimiento de los recursos y con ello, lograr un nivel óptimo de administración.

Ahora bien aquí solo se hizo mención de algunos mecanismos de seguridad que se pueden tomar en consideración para mantener un nivel razonable de seguridad, pero se

pueden implementar otros, por ejemplo, el uso de *firewalls* como mecanismos de seguridad perimetral, el uso de *VLANs*, IDS (*Intrussion Detection System*) o mejor aún, IPS (Intrussion Prevention System), en fin se puede hacer un sistema tan robusto como sea posible y creado a las necesidades de los usuarios. Y es que en una implementación, por ejemplo casera, no es necesario todo esto, tal vez con tan solo el uso de algún mecanismo de autenticación, por ejemplo usando WPA2, por ejemplo, pero eso si, con una contraseña "fuerte", baste para mantener segura la red.

Todo lo anterior me permite concluir que si de por sí, las redes inalámbricas son sumamente inseguras con una mala configuración o en el peor de los casos, con una nula configuración con respecto a la seguridad de la red lo es aún más. Es por ello que no se debe dejar pasar ya que se vuelve en un punto crítico de nuestra infraestructura, por tal motivo hay que tener muy en cuenta la implantación de mecanismos de autenticidad de los usuarios y mecanismos de privacidad haciendo uso de cifrado de la información por medio de algoritmos robustos.

Uno de los aspectos más importantes y creo yo, el más importante, es el "estar informado" de lo que conlleva hacer la implementación de cualquier tecnolgía en cualqueir ambiente, ya que el tener el conocimiento de lo que se va a realizar pero el verdadero conocimiento, no simplemente el poner el producto y que funcione, sino ver aspectos de disponibilidad, calidad del servicio, seguridad, estándares, etc. hace que se maneje un entorno robusto, estable y seguro y desde luego, esto orienta a ofrecer un mejor servicio, que es realmente lo que se busca.

Por último, pero no menos enfáticamente, agradezco a la Universidad Nacional Autónoma de México por brindarme las herramientas necesarias para la realización de este trabajo de tesis.

Apéndice A

Glosario

802.11 802.11, o IEEE 802.11, es un grupo de trabajo del IEEE que desarrolla distintos estándares para el uso de la tecnología de radiofrecuencia en las redes de área local (LAN).

802.11 se compone de distintas normas que operan a diferentes frecuencias, con distintas velocidades y capacidades.

AES (Advanced Encryption Standard). Algoritmo de cifrado del gobierno de EE.UU, basado en el algoritmo Rijndael, método de cifrado simétrico con clave de 128 bits desarrollada por los belgas Joan Daemen y Vincent Rijmen.

Access Point (AP, Punto de Acceso). Estación base o "base station" que conecta una red cableada con uno o más dispositivos wireless.

Existen muchos tipos de Access Point en el mercado, con diferentes capacidades: bridge, hubs, gateway, router, y las diferencias entre ellos muchas veces no están claras, porque las características de uno se pueden incluir en otro. Por ejemplo, un router puede hacer bridge, y un hub puede hacer switch.

Además, los Access Points pueden mejorar las características de la WLAN, permitiendo a un cliente realizar roaming entre distintos AP de la misma red, o compartiendo una conexión a Internet entre los clientes wireless.

Ad-Hoc, modo. Un tipo de topología de WLAN en la que sólo existen dispositivos clientes, sin la participación de ningún Access Point, de forma que los clientes se comunican de forma independiente punto a punto, peer-to-peer.

Dado que no existe un dispositivo central, las señales pueden ocasionar mayores interferencias reduciendo las prestaciones de la red.

Ancho de banda (Bandwidth). Fragmento del espectro radioeléctrico que ocupa toda señal de información.

Asociación, servicio de. Servicio del protocolo 802.11 que asocia un cliente wireless a un Punto de Acceso.

Autenticación. Proceso de identificación de un equipo o usuario. El estándard 802.11 define dos métodos de autenticación: open system y shared key.

Bluetooth. Tecnología desarrollada para la interconexión de portátiles, PDAs, teléfonos móviles y similares a corta distancia (menos de 10 metros) con una velocidad máxima de 11Mbps a la frecuencia ISM de 2.4 GHz.

Bridge. Dispositivo que conecta dos segmentos de red que emplean el mismo protocolo de red (por ejemplo, IP) pero con distintos medios físicos (por ejemplo, 802.11 y 10baseT).

BSSID, Basic Service Set Identification. Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo Ad-Hoc.

Clave de cifrado. Conjunto de caracteque se utilizan para cifrar y descifrar la información que se quiere mantener en privado. El tipo de clave y la forma de emplearla depende del algoritmo de cifrado que se utilice.

Cliente, o dispositivo cliente. Cualquier equipo conectado a una red y que solicita servicios (archivos, impresión, etc) de otro nodo de la red.

En el caso de las WLAN, se suele emplear para referirse a los adaptadores que proporcionan conectividad a través de la red inalámbrica, como tarjetas PCMCIA, PCI o USB, que permiten al equipo acceder a la red.

Decibelios, dB. Unidad logarítmica empleada habitualmente para la medida de potencias. Se calcula multiplicando por diez el resultado del logaritmo en base 10 de la potencia (en watios): 10 * log10 (W). También puede usarse como medida relativa de ganancia o pérdida de potencia entre dos dispositivos.

Decibelios isotrópicos, dBi. Valor relativo, en decibelios, de la ganancia de una antena respecto a la antena isotrópica. Cuanto mayor sea este valor, más directividad tiene la antena y más cerrado será su ángulo de emisión.

DSSS, Direct Sequence Spread Spectrum. Técnica de transmisión de la señal para minimizar los efectos de las interferencias, que se basa en el uso de bits de redundancia.

Espectro radioeléctrico. El espectro radioeléctrico es toda la escala de frecuencias de las ondas electromagnéticas. Considerado como un dominio de uso público, su división y utilización esta regularizado internacionalmente.

ESSID, Extended Service Set Identification. Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo infraestructura.

Ethernet. Ethernet es el nombre común del estándard IEEE 802.3, que define las redes locales con cable coaxial o par trenzado de cobre.

Existen distintas versiones, desde la original 10Base5 (cable coaxial con 10 Mbps hasta 500 metros), pasando por la 10Base2 (coaxial, 10Mbps, 200m), 10BaseT (par trenzado, 10 Mbps, 100m) y 100BaseT (trenzado, 100Mbps, 100m) conocida como Fast Ethernet, el más utilizado hoy en día en redes locales.

ETSI, European Telecommunications Standard Institute http://www.etsi.org. Organización europea sin ánimo de lucro para el desarrollo de estándares de telecomunicación, agrupa 699 miembros de 55 países.

FCC, Federal Communication Commision http://www.fcc.gov. Agencia gubernamental de los EE.UU. para la regularización de las comunicaciones por radio, televisión, cable y satélite.

FHSS, Frequency Hopping Spread Spectrum. Técnica de transmisión de la señal para minimizar los efectos de las interferencias, que se basa en cambios sincronizados entre emisor y receptor de la frecuencia empleada.

Firewall. Sistema de seguridad que perviene el acceso no autorizado a la red, restringiendo la información que entra o sale de la red. Puede ser un equipo específico o un software instalado en una máquina de uso general.

Hot Spot. También conocidos como lugares de acceso público, un Hot Spot es un lugar donde se puede acceder a una red wireless pública, ya sea gratuita o de pago. Pueden estar en cyber-cafes, aeropuertos, centros de convenciones, hoteles, y otros lugares de encuentro, para proporcionar acceso a su red o a Internet a los visitantes o invitados.

Hub. Dispositivo de red multipuerto para la interconexión de equipos via Eterhnet o wireless. Los concentradores mediante cables alcanzan mayores velocidades que los concentradores wireless (Access Points), pero éstos suelen dar cobertura a un mayor número de clientes que los primeros.

Infraestructura, modo. El modo de infraestructura es una topología de red inalámbrica en la que se requiere un Punto de Acceso. A diferencia del modo Ad-Hoc, toda la información pasa a través del Punto de Acceso, quien puede además proporcionar la conectividad con una red cableada y controlar el acceso a la propia red wireless.

IEEE, Institute of Electrical and Electronics Engineers (http://www.ieee.org). .

Organización formada por ingenieros, científicos y estudiantes involucrados en el desarrollo de estándares para, entre otros campos, las comunicaciones.

Este organismo utiliza los números y letras en una clasificación jerárquica para diferenciar grupo de trabajo y sus normas. Así, el subgrupo 802 se encarga de las redes LAN y WAN, y cuenta con la subsección 802.11 para las redes WLAN.

IP, dirección. Un número de 32 bits que identifica a un equipo a nivel de protocolo de red en el modelo ISO. Se compone de dos partes: la dirección de red, común a todos los equipos de la red, y la direccin del equipo, única en dicha red.

ISM, Industrial, Scientific and Medical band. Bandas de frecuencias reservadas originalmente para uso no comercial con fines industriales, científicos y médicos. Posteriormente, se empezaron a usar para sistemas de comunicación tolerantes a fallos que no necesitaran licencias para la emisión de ondas.

802.11b y 802.11g operan en la ISM de los 2.4 GHz, as como otros dispositivos como teléfonos inalámbricos y hornos de microondas, por ejemplo.

MAC (Media Access Control), dirección. En las redes wireless, el MAC es un protocolo de radiofrecuencia, corresponde al nivel de enlace (nivel 2) en el modelo ISO. Cada dispositivo wireless posee una dirección para este protocolo, denominada dirección MAC, que consiste en un número de 48 bits: los primeros 24 bits identifican al fabricante de la tarjeta, mientras que los restantes 24, a la tarjeta en sí. Este modelo de direccionamiento es común con las redes Ethernet (802.3).

Modulación. Técnicas de tratamiento de la señal que consiste en combinar la señal de información con una señal portadora, para obtener algún beneficio de calidad, eficiencia o aprovechamiento del ancho de banda.

Open System, autentificación. Método de autentificación por defecto del estándard 802.11, en la que no se realiza ningún proceso de comprobación de identidad; simplemente, se declaran, por lo que no ofrece ninguna seguridad ni control de acceso.

PHY. Nombre abreviado del nivel más bajo del modelo ISO, el nivel físico, que describe el medio físico en el que se transmite la información de la red.

En el caso de las redes inalámbricas, las normas 802.11 definen el nivel PHY que utilizan, el aire libre, y los parámetros empleados como la velocidad de transmisión, tipo de modulación, algoritmos de sincronización emisor/receptor, etc.

Roaming. Nombre dado a la acción de moverse del área de cobertura de un Punto de Acceso a otro sin pérdida de conectividad, de forma que el usuario no lo percibe.

Router. Dispositivo de red que traslada los paquetes de una red a otra.

Basándose en las tablas y protocolos de enrutamiento y en el origen y destino, un router decide hacia dónde enviar un paquete de información.

Shared Key, autentificación. Proceso de autentificación por clave secreta. Habitualmente, todos los dispositivos de la red comparten la misma clave.

Spread Spectrum, espectro disperso. Técnica de trasmisión consistente en dispersar la información en una banda de frecuencia mayor de la estrictamente necesaria, con el objetivo de obtener beneficios como una mayor tolerancia a la interferencias.

SSID, Service Set Identification. Conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica. Para que dos dispositivos wireless se puedan comunicar, deber tener configurado el mismo SSID, pero dado que se puede obtener de los paquetes de la red wireless en los que viaja en texto claro, no puede ser tomado como una medida de seguridad.

Dependiendo de si la red wireless funciona en modo Ad-Hoc o en modo Infraestructura, el SSID se denomina ESSID o BSSID.

TKIP, Temporal Key Integrity Protocol. Algoritmo empleado por el protocolo WPA para mejorar el cifrado de los datos en redes wireless. Sus principales características son la renovación automática de la clave de cifrado de los mensajes y un vector de inicialización de 48 bits, lo que elimina el problema del protocolo WEP.

Velocidad de transmisión (Throughput) Capacidad de transmisión de un medio de comunicación en cualquier momento, se suele medir en bits por segundo (bps). Depende de múltiples factores, como la ocupación de la red, los tipos de dispositivos empleados, etc, y en el caso de redes wireless, se añaden los problemas de propagación de microondas a través de la que se transmite la información.

War driving. Localización y posible intrusión en redes wireless de forma no autorizada. Sólo se necesita un equipo portátil, un adaptador wireless, el software adecuado y un medio de transporte.

WEP, Wired Equivalent Privacy. Algoritmo de seguridad, de uso opcional, definido en el estándard 802.11. Basado en el algoritmo criptográfico RC4, utiliza una clave simétrica que debe configurarse en todos los equipos que participan en la red. Emplea claves de 40 y 104 bits, con un vector de inicialización de 24 bits.

Se ha demostrado su vulnerabilidad y que su clave es fácilmente obtenible con software de libre distribución a partir de cierta cantidad de tráfico recogido de la red.

Wi-Fi, Wireless Fidelity. Nombre dado al protocolo 802.11b. Los dispositivos certificados como Wi-Fi son interoperables entre sí, como garantía para el usuario.

Wi-Fi Alliance, también llamada Wireless Ethernet Compability Alliance (WECA). Asociación internacional formada en 1999 para certificar la interoperatibilidad de los dispositivos wireless basados en el estándard 802.11, con el objetivo de promover la utilización de dicha tecnología.

WPA, Wi-Fi Protected Access. Protocolo de seguridad desarrollado por la WECA para mejorar la seguridad de la información en las redes wireless y permitir la autenticación de usuario, cubriendo algunos puntos débiles del WEP.

Apéndice B

WEP

El protocolo WEP nace en 1999 como parte del estándar IEEE 802.11. Su objetivo es cifrar los datos que viajan a través de los nodos de una red inalámbrica para garantizar la privacidad de los mismos. Tomando en cuenta que una red Wi-Fi utiliza el aire como medio de transmisión, es importante que la información que viaje por la misma sea cifrada debido a que las ondas de radio pueden rebasar los límites de donde la red es utilizada.

El protocolo WEP fue concebido con la idea de proporcionar un nivel de seguridad equivalente al de una red cableada; y de ahí tiene origen su nombre: *Wired Equivalent Privacy* o Privacidad Equivalente a una Red Cableada. Pero la realidad es que 4 años antes de su salida ya habían sido descubiertas ciertas vulnerabilidades en el algoritmo RC4, uno de los utilizados en el proceso de cifrado WEP. Más tarde, para el año 2000, aparecía la primera publicación sobre las debilidades descubiertas en WEP y, finalmente en el 2004, se ponía a disposición de los usuarios herramientas gratuitas para vulnerar una red cifrada por WEP. Actualmente WEP es un protocolo que debe considerarse obsoleto y debería evitarse su uso bajo cualquier circunstancia. Es probable que el poco éxito y eficacia proporcionada por WEP se deba a que este no ha sido un protocolo diseñado por expertos en seguridad o criptografía y a que unos de sus pilares, el algoritmo RC4, poseía ya potenciales vulnerabilidades descubiertas años atrás.

Funcionamiento

El protocolo WEP se basa en dos componentes o algoritmos para cifrar los paquetes

que van a circular por la red inalámbrica. El primero de ellos es el CRC o *Código de Redundancia Cíclica* el cual genera una cantidad fija de bits adicionales para añadir al paquete original con el objetivo de ayudar al receptor a comprobar que los datos que recibe sean los mismos que los enviados. Esta secuencia de bits generados por el algoritmo recibe el nombre de cifra CRC. El otro algoritmo es el RC4, y estará encargado de generar una secuencia pseudo aleatoria de bits que se utilizará para combinar con el contenido de un paquete mediante alguna operación lógica, de manera que no sea posible descifrar el contenido de ese paquete sin la posesión de la secuencia generada.

El principio del funcionamiento de WEP está en la operación lógica XOR u o exclusivo. La operación XOR es un tipo de disyunción lógica entre dos operandos que resulta en un valor verdadero o uno si y solo si uno de esos dos operandos vale uno. Esta operación presenta la propiedad que si aplicamos dos veces XOR a un valor, se vuelve a obtener el valor original. Por ejemplo, teniendo un valor A y calculando A XOR B = C, tendremos entonces que A XOR B XOR B será igual a A.

Teniendo en cuenta lo antes dicho, es posible que, si dos nodos de una red inalámbrica conocen un valor B secreto y se quiere transmitir una secuencia de bits A, aplicar la operación A XOR B obteniendo un flujo de datos C cifrado, el cual solo puede ser decodificado por aquellos que conocen el valor de B. En este sentido es posible ver a B como una contraseña secreta que deben conocer y compartir todos los nodos que quieran intercambiar mensajes de manera segura entre sí.

El problema de esta metodología es que al utilizar siempre la misma contraseña B es posible para alguien, que eventualmente pueda interceptar los mensajes, utilizar métodos matemáticos y estadísticos para ir descubriendo los bits que conforman esta secuencia. Una posible solución a esto sería que todos los nodos generen de manera aleatoria una secuencia B para cada paquete a transmitir y que, por supuesto, todos los nodos de la red generen esa misma secuencia en el mismo momento. Existen algoritmos que, al recibir siempre el mismo flujo de bits como entrada, producen un mismo flujo de salida en nodos diferentes de la red, como por ejemplo el algoritmo RC4 anteriormente mencionado.

WEP se basa en todos estos conceptos utilizando el algoritmo RC4 como generador de la clave B. Para generar la misma secuencia B en el nodo emisor y receptor del mensaje, el mecanismo WEP propone el uso de una clave estática conocida por todos las entidades de la red con una longitud de 104 bits (o 40 bits para claves más cortas) definida por el administrador de la red. Esta clave estática se concatenará con una clave dinámica (IV) (*Vector de Inicialización*) elegida pseudo aleatoriamente por el nodo emisor, con una longitud de 24 bits en todos los casos, y enviada en el paquete WEP sin algún cifrado. La secuencia de bits obtenida por la concatenación de la clave estática definida por el usuario en adición a la clave dinámica establecida por el nodo emisor, le servirán al algoritmo RC4 como parámetro de entrada para el cálculo de un flujo de salida utilizado posteriormente en la operación XOR, dando como resultado el cifrado completo del mensaje a transmitir. Este parámetro de entrada utilizado por el RC4 es comúnmente llamado semilla o *seed* en inglés. El emisor por su parte podrá generar la misma salida RC4 o keystream debido a que posee la misma clave estática que el emisor y además puede obtener la clave dinámica del paquete WEP enviado por el emisor pudiendo así generar la misma semilla utilizada para cifrar el mensaje. Al obtener el mismo keystream utilizado para cifrar, será posible finalmente para el receptor, recuperar el mensaje original aplicando la operación XOR entre el keystream y el mensaje recibido, como se explicó anteriormente. La secuencia de pasos utilizados por el mecanismo de encriptación WEP para transformar un flujo de datos en texto cifrado añadiendo cifras CRC se realiza como se describe en el Fig. 30:

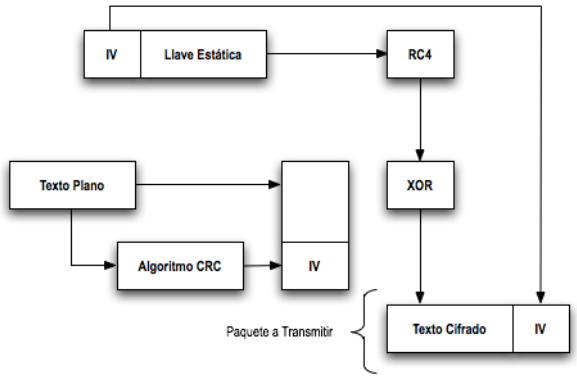


Fig. 29**:** Flujo del Protocolo WEP.

En el cuál el paquete a transmitir desde un nodo emisor hasta un nodo receptor se compondrá, en una vista más detallada, de:

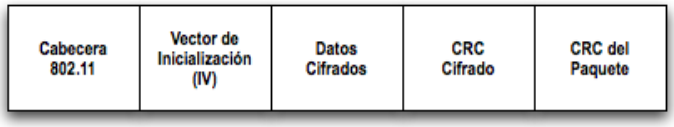


Fig. 30**:** Paquete en el protocolo WEP.

En donde:

- Cabecera 802.11: contendrá información relativa al tipo de paquete, las direcciones MAC del emisor y receptor del mensaje y determinada información de sincronismo.
- Vector de inicialización (IV): es la clave dinámica generada por el emisor y utilizada para concatenar con la clave estática dando origen a la semilla RC4. Como se puede observar esta secuencia de bits crítica para preservar correctamente la privacidad de los datos viaja por la red sin ningún tipo de cifrado.
- Datos cifrados: el mensaje que se desea transmitir de manera segura desde un nodo emisor a un nodo receptor.
- CRC cifrado: código de redundancia cíclica correspondiente al mensaje que se va a transmitir.
- CRC del paquete: código de redundancia cíclica correspondiente al paquete completo.

El Código de Redundancia Cíclica o CRC

Un CRC es un tipo de función que acepta parámetros de cualquier longitud y devuelve siempre una salida de longitud fija. Como se ha mencionado, se utiliza para que el receptor de un paquete pueda detectar una posible alteración accidental del contenido del mismo durante la transmisión. CRC resulta actualmente como el método más eficiente de comunicación digital en materia de detección de errores, aunque el algoritmo no permita

la corrección de un eventual error aparecido durante la transmisión.

Suponiendo que se desea transmitir un paquete M de datos con una longitud de K bits; el objetivo del algoritmo CRC será crear una secuencia de bits F con longitud N para añadir a M para su posterior transmisión. A la unión de las secuencias M y F la llamaremos T y tendrá una longitud de K+N a fines de simplificar este ejemplo. La secuencia de bits F o bits de redundancia se generarán de forma que T sea exactamente divisible por un patrón fijo de bits P llamado polinomio CRC o polinomio generador. Tanto el emisor como el receptor tendrán fijado el valor de P, por lo que el receptor de un mensaje deberá verificar que la secuencia T recibida sea divisible por la secuencia P; en caso que no lo sea significa que ocurrió un error en la transmisión. Tanto el proceso del cálculo de la secuencia F, como la revisión por el receptor, requieren pocos pasos y son muy sencillos de implementar tanto en hardware como en software por lo que prácticamente no le quitan eficiencia al protocolo WEP.

Para calcular F el emisor deberá:

- Obtener la secuencia de bits a transmitir M.
- Añadir a la secuencia M la cantidad de G bits 0 a la derecha, siendo G la cantidad de bits que contiene el polinomio CRC menos 1.
- Dividir lo obtenido en el paso anterior por P.
- El resto de la división binaria será F.
- Añadir F a M y transmitir el paquete.

Por otro lado el receptor al recibir el paquete podrá comprobar su validez realizando las siguientes operaciones:

- Recibir el paquete.
- Dividir la secuencia recibida por el patrón o polinomio P.

- Si el resto de la división anterior es cero, el paquete ha sido correctamente transmitido.

Particularmente, la secuencia de bits P utilizada por el protocolo WEP, es empleada y aprobada por el comité de estándares IEEE 802 y utilizada por el Departamento de Defensa de los Estados Unidos debido a la protección extra que ofrece frente a otro tipo de secuencias. La secuencia dispone de 32 bits siendo estos 11101101101110001000001100100000 en representación binaria o EDB88320 en representación hexadecimal.

Algoritmo RC4

Dentro del campo de la criptografía (ciencia encargada de cifrar y descifrar información mediante técnicas matemáticas de modo que los mensajes que se transmiten solo puedan ser leídos por aquellos a quienes van dirigidos), el algoritmo RC4 es el más utilizado pese a estar actualmente excluido de los estándares de seguridad por los criptógrafos. Diseñado en el año 1987 por Ron Rivest, RC4 fue un secreto registrado hasta 1994, año en el cual una descripción del funcionamiento del algoritmo fue publicada clandestinamente en una lista de correo. Un año más tarde, en 1995, la primera vulnerabilidad potencial era descubierta y a partir de entonces no se recomienda el uso del algoritmo en nuevos sistemas.

La forma de trabajo del algoritmo es muy sencilla y se divide en dos partes bien diferenciadas: en una primera parte, llamada KSA, el algoritmo desordena una secuencia de números consecutivos inicialmente ordenados. En esta fase es donde se utiliza la clave WEP compuesta por el vector de inicialización junto a la clave estática definida por el usuario. Existen en total una gran cantidad de posibilidades de ordenamiento de 256 números diferentes; más precisamente se podrán obtener 256 factorial (256!) combinaciones correspondientes a las permutaciones de los 256 elementos. La clave WEP completa influirá directamente en cómo estos números son ordenados debido a que la posición en la que quedará un número determinado será dependiente de los distintos caracteres de la clave, a los cuales se les aplicarán operaciones MOD (residuo de la división) y sumas para determinar dicha posición.

En la segunda parte, denominada fase PRGA, es donde se genera una secuencia de números pseudo aleatorios a los cuales el protocolo WEP le aplicará la operación XOR con el mensaje que se desea cifrar, como se detallo anteriormente. En esta última fase se utilizará la secuencia de números desordenados en la etapa KSA a los cuales se les aplicarán nuevamente operaciones MOD y sumas para ir calculando los diferentes bytes que compondrán el keystream utilizado para cifrar el mensaje.

Apéndice C

Mejores Prácticas

C.1. Configuración de Un Punto de Acceso para Trabajar con WPA Enterprise (EAP-TLS) usando OpenSSL y FreeRADIUS en Linux.

Instalación de Una Autoridad Certificadora (CA) Usando OpenSSL

OpenSSL es una herramienta que se maneja por medio de la línea de comandos, la cual ofrece varias funciones. OpenSSL puede generar llaves privadas y su correspondiente certificado de llave pública, puede firmar las solicitudes de certificados, publicar listas de revocación de certificados (CRL), convertir entre varios formatos de codificación como DER, PEM, PKCS #12, etc.

A continuación se muestra el cómo instalar una Autoridad Certificadora (CA) usando OpenSSL, cómo generar las llaves privadas, generar los certificados y firmarlos, todo esto en un sistema Linux con Fedora Core 8.

Vamos a instalar todos los paquetes necesarios (todos los comandos van a ser como administrador del sistema):

```
# yum install freeradius
# yum install openssl-devel.i386
# yum install openssl-perl.i386
```

Ya instalados los paquetes vamos a configurar algunos archivos, en este caso el openssl.cnf en /etc/pki/tls/:

```
# vi /etc/pki/tls/openssl.cnf
```

```
[ CA_default ]

dir = /etc/pki/CA # Where everything is kept
certs = $dir/certs # Where the issued certs are kept
crl_dir = $dir/crl # Where the issued crl are kept
database = $dir/index.txt # database index file.
  #unique_subject = no # Set to 'no' to allow creation of
# several ctificates with same subject.
new_certs_dir = $dir/newcerts # default place for new certs.

[ req_distinguished_name ]

countryName                     = Country Name (2 letter code)
countryName_default      = MX
countryName_min              = 2
countryName_max             = 2

stateOrProvinceName       = State or Province Name (full name)
stateOrProvinceName_default = Mexico

localityName                    = Locality Name (eg, city)
localityName_default        = Distrito Federal

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

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

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

commonName                 = Common Name (eg, your name or your server\'s hostname)
```

Quedando todo lo demás sin modificaciones.

Ahora si vamos a crear la Autoridad Certificadora (CA)

En este paso se va a crear la llave privada de la CA y un certificado auto firmado (el certificado de la CA).

El certificado de la CA va a ser almacenado en /etc/pki/CA/cacert.pem, mientras que

la llave privada de la CA puede ser almacenada en /etc/pki/CA/private/cakey.pem:

```
# openssl req -new -x509 -days 365 -newkey rsa:1024 \
-keyout /etc/pki/CA/private/cakey.pem -out /etc/pki/CA/cacert.pem

Generating a 1024 bit RSA private key
...++++++
............++++++
writing new private key to '/etc/pki/CA/private/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [MX]:MX
State or Province Name (full name) [Mexico]:Mexico
Locality Name (eg, city) [Distrito Federal]:Distrito Federal
Organization Name (eg, company) [UNAM]:UNAM
Organizational Unit Name (eg, section) [UNAM]:UNAM
Common Name (eg, your name or your server's hostname) []:FreeRADIUS Server
Email Address []:bautistapedro@gmail.com
```

Por cuestiones de seguridad vamos a cambiarle los permisos a la llave:

```
# chmod 600 /etc/pki/CA/private/cakey.pem
```

Una copia de cada certificado firmado se almacenará en /etc/pki/CA/newcerts, con un número secuencial más la extensión .pem.

```
# mkdir /etc/pki/CA/newcerts
```

El archivo /etc/pki/CA/index.txt lleva un registro de cada certificado firmado.

```
# touch /etc/pki/CA/index.txt
```

El archivo /etc/pki/CA/serial contiene el siguiente número X.509 disponible.

```
# echo 01 > /etc/pki/CA/serial
```

Ahora vamos a generar el certificado y su correspondiente llave privada.

El siguiente comando generará de forma aleatoria, una llave privada RSA de 1024 bits y su correspondiente llave pública dentro de un certificado codificado en PEM. Este certificado aún no está firmado, posteriormente lo firmaremos:

```
   # openssl req -new -days 365 -newkey rsa:1024 -keyout \
   /etc/pki/CA/sslkey.pem -out /etc/pki/CA/sslcert.pem

Generating a 1024 bit RSA private key
............++++++
.........................................++++++
writing new private key to '/etc/pki/CA/sslkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [MX]:MX
State or Province Name (full name) [Mexico]:Mexico
Locality Name (eg, city) [Distrito Federal]:Distrito Federal
Organization Name (eg, company) [UNAM]:UNAM
Organizational Unit Name (eg, section) [UNAM]:UAP
Common Name (eg, your name or your server's hostname) []:FreeRADIUS Server
Email Address []:bautistapedro@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:m@14ki7A
An optional company name []:
```

La llave privada puede ser escrita en /etc/pki/CA/sslkey.pem mientras que la llave pública, está codificada dentro del certificado aún sin firmar en /etc/pki/CA/sslcert.pem.

Ahora bien, vamos a firmar el certificado:

Para firmar el certificado almacenado en /etc/pki/CA/sslcert.pem, usamos el siguiente comando:

```
   # openssl ca -in /etc/pki/CA/sslcert.pem -out /etc/pki/CA/cert.pem
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
```

```
        Serial Number: 1 (0x1)
        Validity
            Not Before: Jun 17 18:02:28 2008 GMT
            Not After : Jun 17 18:02:28 2009 GMT
        Subject:
            countryName                 = MX
            stateOrProvinceName         = Mexico
            organizationName            = UNAM
            organizationalUnitName      = UNAM
            commonName                  = FreeRADIUS Server
            emailAddress                = bautistapedro@gmail.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                5B:25:EB:EC:A5:11:50:BE:8A:76:07:87:09:54:71:6E:F8:02:3A:E7
            X509v3 Authority Key Identifier:
                keyid:3B:EC:6B:3D:6C:55:93:2C:E5:7A:FE:57:CD:04:40:E8:4A:25:67:83

Certificate is to be certified until Jun 17 18:02:28 2009 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

El resultado de firmar el certificado puede verse en /etc/pki/CA/cert.pem. Una vez que el certificado ya haya sido firmado, el certificado sin firmar puede ser borrado.

Ya instalada nuestra Autoridad Certificadora vamos a proceder con la instalación de los certificados en el servidor RADIUS.

El certificado y su correspondiente llave privada, más el certificado de de la CA deben ser colocados dentro de la rta /etc/raddb/certs para poder hacer uso de EAP-TLS o EAP-TTLS:

Instalamos la llave privada del servidor RADIUS:

```
# mv /etc/pki/CA/sslkey.pem /etc/raddb/certs/RADIUS-key.pem
```

Instalamos el certificado firmado X.509 para el servidor RADIUS:

```
# mv /etc/pki/CA/cert.pem /etc/raddb/certs/RADIUS-cert.pem
```

Instalamos el certificado de la CA:

```
# mv /etc/pki/CA/cacert.pem /etc/raddb/certs/cacert.pem
```

Configuración del Servidor RADIUS (FreeRADIUS).

El autenticador tiene que hacer una petición al servidor de autenticación pero al igual, éste tiene que autenticarse. El autenticador tiene un secreto compartido, una contraseña, con el servidor RADIUS. Este secreto compartido es almacenado en el archivo /etc/raddb/clients.conf.

Editamos en archivo /etc/raddb/clients.conf agregando las siguientes líneas:

```
   client 192.168.10.1/32 {
secret   = p@zzw0r2
shortname = MyWirelessNet
   }
```

La directiva *client* especifíca la IP de la subred de la cual los suplicantes pueden hacer peticiones de autenticación vía 802.1X. La directiva *secret* especifíca el secreto compartido entre el autenticador (Punto de Acceso Inalámbrico) y el servidor RADIUS. La directiva *shortname* es sólo una descripción.

El punto de acceso inalámbrico debe ser configurado para usar WPA Enterprise. Las siguientes parámetros deben ser configurados en el AP:

- Dirección IP del Servidor RADIUS: La dirección IP del servidor RADIUS (que en este caso en particular es:) 192.168.10.30.
- Puerto RADIUS: El puerto del servidor FreeRADIUS (usualmente es 1812-UDP).
- Secreto Compartido (contraseña) de RADIUS: En este caso pusimos p@zzw0r2.

Archivo /etc/raddb/certs/random

FreeRADIUS almacena 1024 bytes de entropía en el archivo /etc/raddb/certs/random, por ser este un archivo de configuración ya viene precargado, pero siempre es mejor volverlo a crear y lo hacemos con el siguiente comando:

```
# dd if=/dev/random of=/etc/raddb/certs/random bs=1 count=1024
```

Archivo /etc/raddb/eap.conf

A cuntinuación se listan las modificaciones que se tiene que hacer a este archivo:

- Se debe de cambiar el método EAP por defecto de EAP-MD5 a EAP-TLS.
- Asegurarse de que el módulo EAP-GTC esté habilitado.
- Habilitar el módulo EAP-TLS.
- Habilitar el módulo EAP-TTLS, el cual depende de EAP-TLS (en caso de usar TTLS).

Donde finalmente el archivo /etc/raddb/eap.conf debe tener la siguiente configuración:

```
    eap {
            default_eap_type = tls
            timer_expire     = 60
            ignore_unknown_eap_types = no
            cisco_accounting_username_bug = no
            md5 {
            }
            leap {
            }
            gtc {
                    auth_type = PAP
            }
            tls {
                    private_key_password = ywtyxc3    #Pass del certificado RADIUS-key.pem
                    private_key_file = ${raddbdir}/certs/RADIUS-key.pem
                    certificate_file = ${raddbdir}/certs/RADIUS-cert.pem
                    CA_file = ${raddbdir}/certs/cacert.pem
                    dh_file = ${raddbdir}/certs/dh
                    random_file = ${raddbdir}/certs/random
                    fragment_size = 1024
                    include_length = yes
                    cipher_list = "DEFAULT"
            }
            ttls {
                    default_eap_type = gtc
                    copy_request_to_tunnel = no
                    use_tunneled_reply = no
            }
             peap {
```

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

Configuración de los los usuarios:

Para poder dar de alta a los usuarios editamos el archivo /etc/raddb/users agregáandolos de la siguiente forma:

```
user Auth-Type := EAP , User-Password == "password"
otro Auth-Type := EAP , User-Password == "newpass"
```

Por último vamos a probar el funcionamiento FreeRADIUS y para poder hacer esto iniciamos el servicio de la siguiente forma:

```
# /usr/sbin/radiusd -X -A
```

Y si FreeRADIUS está trabajando correctamente, el comando anterior debería desplegar algo como lo siguiente:

```
...
Listening on authentication *:1812
Listening on accountin *:1813
Ready to process requests.
```

Fig. 31**:** Configuración del SSID.

Hasta este punto ya tenemos configurado nuestro servidor de autenticación, solo queda por configurar el punto de acceso, que en este caso se utilizó un router Linksys WRT54G V6, pero la configuración en otro router debería ser muy similar, primero que nada definimos el nombre de nuestra red “SSID” Fig. 32:

Y finalmente configuramos los datos del servidor RADIUS Fig. 33:

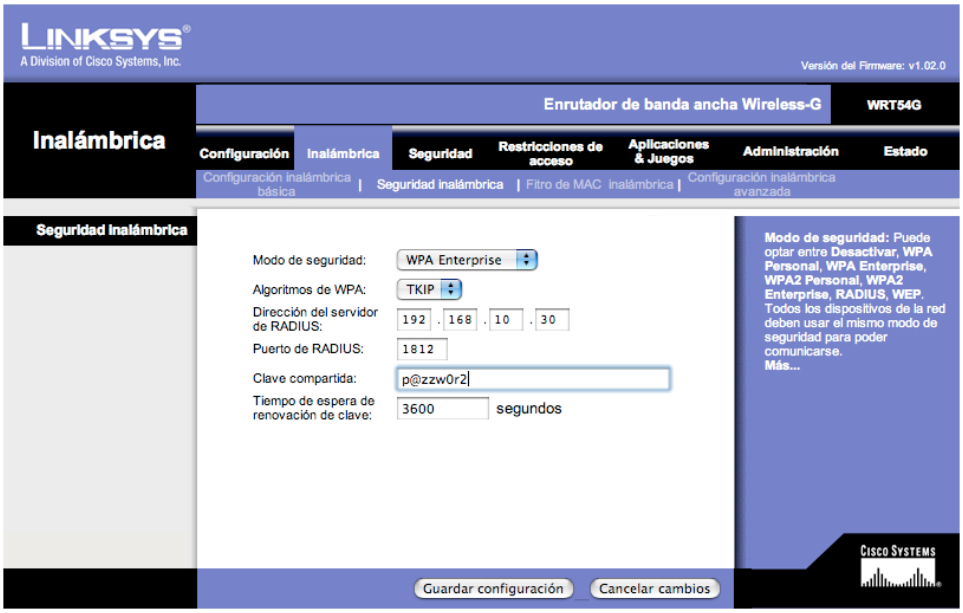


Fig. 32**:** Configuración del Servidor RADIUS.

C.2. Instalación de un Punto de Acceso en Linux con WPA, OpenVPN, OpenSSL, DHCP y SSH.

Introducción

El Acceso protegido Wi-Fi (WPA o WPA2) es una mejora de la seguridad que aumenta considerablemente el nivel de protección de datos y el control del acceso a una red inalámbrica. WPA impone la autenticación y el intercambio de claves de 802.1x y funciona sólo con claves de codificación dinámicas. Para reforzar la codificación de datos, WPA utiliza el Protocolo de integridad de claves (TKIP). TKIP brinda importantes mejoras en la codificación de datos, que incluyen una función de mezcla de claves por paquete, una verificación de integridad de mensajes (MIC) llamada Michael, un vector de inicialización (IV) extendido con reglas de secuencia y un mecanismo de reintroducción de claves. Con estas mejoras, TKIP brinda protección para las flaquezas conocidas de WEP.

WPA-Personal y WPA2-Personal: Provee cierto nivel de seguridad en entornos de redes pequeñas o domésticas. Utiliza una contraseña que también se conoce como clave precompartida (PSK). Cuanto más larga sea la contraseña, más robusta será la seguridad de la red inalámbrica.

Desarrollo

A continuación se describe la instalación de un Punto de Acceso en "Linux" con WPA como sistema de autenticación, OpenVPN como servidor de VPN's, OpenSSL como Autoridad Certificadora, DHCP y Secure Shell para poder crear un túnel aún más seguro.

Antes de comenzar con la instalación, debemos tener en cuenta de que "NO" todo el hardware (tarjetas inalámbricas) soporta el "Modo Master", el cuál hace que la tarjeta se comporte como punto de acceso y pueda recibir mensajes de solicitud. En este caso se utilizó una terjeta Proxim Orinoco Gold 8470-WD con chipset "Atheros", la cual, soporta

el modo Monitor, por supuesto modo Managed y modo Master, éste último siendo el que nos interesa.

Ahora bien, para que este dipositivo funcione correctamente como Punto de Acceso es necesario que se instalen los drivers adecuados y para esta tarjeta son los drivers "Madwifi" (la instalación de estos drivers sale del objetivo de este documento as'i es que no se describe aquí, se puede visitar la página del proyecto madwifi *http://madwifi.org/* para más información).

La instalación de este servidor está en un Debian Etch con un kernel 2.6.26.

En Debian para poder gestionar las tarjetas de red inalámbricas, es necesario contar con el paquete "wireless-tools", en caso de no contar con este, lo podemos instalar de la siguiente forma:

```
# apt-get -y install wireless-tools
```

Ahora para poder ver que está correctamente instalada la tarjeta procedemos a teclear el siguiente comando:

```
# iwconfig
```

Lo cual, nos va a desplegar algo muy similar a lo siguiente:

```
lo        no wireless extensions.

sit0      no wireless extensions.

eth0      no wireless extensions.

wifi0     no wireless extensions.

ath0      IEEE 802.11b  ESSID:""  Nickname:""
          Mode:Managed  Channel:0  Access Point: Not-Associated
 Bit Rate:0 kb/s   Tx-Power:0 dBm   Sensitivity=1/1
 Retry:off   RTS thr:off   Fragment thr:off
 Encryption key:off
 Power Management:off
```

```
Link Quality=0/70  Signal level=-256 dBm  Noise level=-256 dBm
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

donde nos podemos dar cuenta de que la tarjeta es detectada y nombrada como "**ath0**" por el sistema operativo.

A continuación proseguiremos con la instalación del servidor de Secure Shell, DHCP y Hostap, el primero permite conexiones remotas a la máquina, pero de forma segura, el segundo permite asignar direcciones de forma automática a los equipos que se van a conectar al punto de acceso y el tercero es el que va a hacer que funcione el Punto de Acceso. La instalación la hacemos de la misma forma que con el paquete wireless-tools, pero en este caso, los paquetes son "ssh, dhcp y hostapd":

```
# apt-get -y install ssh
# apt-get -y install dhcp
# apt-get -y install hostapd
```

En el caso de OpenSSL y OpenVPN lo vamos a realizar desde los fuentes, ya que de esta forma vamos a contar con la versión más nueva y en todo caso "estable".

Para OpenSSL se puede descargar de la página *http://www.openssl.org/source/*, en el momento de la realización de este documento la versión que se utilizó fue openssl-0.9.8g.tar.gz, ahora procedemos a la instalación.

Primero hay que desempaquetar y descomprimir los fuentes:

```
# tar zxvf openssl-0.9.8g.tar.gz
```

nos cambiamos de directorio:

```
# cd openssl-0.9.8g
```

y tecleamos la siguiente línea de comandos:

```
# ./config && make && make test && make install
```

de esta forma ya tenemos instalado OpenSSL y el binario se encuentra en /usr/local/ssl/bin/openssl.

Ahora continuaremos con la instalación de OpenVPN, y podemos descargar la versión más reciente de *http://openvpn.net/* en el momento de la realización de este documento la versión estable y la que se utilizó fue la openvpn-2.0.9.tar.gz, este paquete requiere de las librerías "lzo", que son usadas para la compresión de datos.

La instalación de las librerías la podemos hacer de la siguiente forma:

```
# apt-get -y install liblzo2-dev
```

ahora si, desempaquetamos y descomprimomos los fuentes:

```
# tar zxvf openvpn-2.0.9.tar.gz
```

nos cambiamos de directorio:

```
# cd openvpn-2.0.9
```

y teclamos lo siguiente para la configuración, compilación y finalmente, la instalación:

```
# ./configure && make && make install
```

Ya teniendo todas las herramientas instaladas, continuaremos con la configuración de nuestra propia Autoridad Certificadora.

Crearemos un directorio en **/etc** llamado openvpn:

```
# mkdir -p /etc/openvpn/keys
```

copiamos la estructura easy-rsa del directorio openvpn-2.0.9 a /etc/openvpn:

```
# cp -r openvpn-2.0.9/easy-rsa /etc/openvpn
```

este directorio cuenta con diversos scripts que facilitan la creación, tanto de la autoridad certificadora como de los certificados de clientes y del propio servidor.

Para mayor seguridad cambiamos algunos permisos:

```
# chown -R root:root /etc/openvpn
# chmod 700 /etc/openvpn/keys
```

nos cambiamos al directorio /etc/openvpn/easy-rsa

```
# cd /etc/openvpn/easy-rsa
```

editamos la variable $PATH, esto para poder agregar la ruta de donde se encuentra el comando “openssl”:

```
# PATH=$PATH:/usr/local/ssl/bin
```

Ahora si, ejecutamos los siguientes comandos:

```
# . ./vars
# ./clean-all
# ./build-ca
# ./build-key-server server_OpenVPN
# ./build-key usuario-01
# ./build-key usuario-02
# ./build-dh
# openvpn --genkey --secret keys/ta.key
# cd keys
# mv ca.crt dh1024.pem server_OpenVPN.crt server_OpenVPN.key ta.key /etc/openvpn/keys
# chmod 644 /etc/openvpn/keys/{ca.crt,dh1024.pem,server_OpenVPN.crt}
# chmod 600 /etc/openvpn/keys/{server_OpenVPN.key.ta.key}
```

Después de esto solo nos queda por distribuir a cada uno de los usuarios lo siguientes archivos: “ca.crt, usuario-XX.crt, usuario-XX.key y ta.key”.

Con esto ahora solo vamos a crear el archivo de configuración de OpenVPN para poder ser iniciado el servicio y lo hacemos de la siguiente forma:

```
# vi /etc/openvpn/serverOpenVPN.conf
```

con el siguiente contenido:

```
port 1194
proto udp
dev tun
ca keys/ca.crt
cert keys/server_OpenVPN.crt
```

```
key keys/server_OpenVPN.key
dh keys/dh1024.pem
server 172.16.10.0 255.255.255.0
ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status-servidorvpn-udp-1194.log
verb 3
```

En la configuración del servidor de Secure Shell no vamos a realizar nada, pero en la configuración del servidor de DHCP si, y vamos a editar el archivo "/etc/dhcpd.conf" agregando las siguientes líneas y comentando todas las demás, simplemente agregando un "#" al principio de la línea:

```
default-lease-time 60;
max-lease-time 72;
authoritative;
subnet 10.0.0.0 netmask 255.255.255.0 {
range 10.0.0.100 10.0.0.254;
option subnet-mask 255.255.255.0;
option broadcast-address 10.0.0.255;
option routers 10.0.0.1;
option domain-name-servers 10.0.0.1;
}
```

Lo siguiente es que vamos a agregar unos módulos al Sistema Operativo para poder hacer que funcione todo, y estos módulos son hostap_cs y tun y lo vamos a hacer de la siguiente forma:

```
# modprobe tun
# modprobe hostap_cs
```

Y comprobamos que se hayan cargado los módulos con el siguiente comando:

```
# lsmod
```

este comando arroja una lista de todos los módulos cargados en el sistema y por ende, en esta lista debe de aparecer "hostap_cs" y "tun", si no aparecen hay que recompilar el kernel y agregarlos.

Ahora vamos a editar el archivo de configuración para “hostapd”, que se encuentra en /etc/hostapd/hostapd.conf quedando de la siguiente forma:

```
interface=ath0
driver=madwifi
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
debug=0
dump_file=/tmp/hostapd.dump
ssid=WirelessNet
wpa=1
wpa_passphrase=k@pul1nayV1Ru7A
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_group_rekey=600
wpa_gmk_rekey=86400
```

En este archivo hay que tener muy en cuenta de que la variable **wpa_passphrase** contiene la clave compartida con la cual los usuarios van a autenticarse con el punto de acceso, por ello esta debe ser una contraña “fuerte”.

Hasta este punto ya todo está listo para poder levantar cada uno de los servicios y lo hacemos de la siguiente forma:

Primero configuramos nuestra tarjeta de red inalámbrica:

```
# wlanconfig ath0 destroy
# wlanconfig ath0 create wlandev wifi0 wlanmode ap
# ifconfig ath0 10.0.0.1
# iwconfig ath0 essid WirelessNet channel 1
# ifconfig ath0 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255
```

Iniciamos el servicio de dhcp:

```
# mkdir /var/state/dhcp
# touch /var/state/dhcp/dhcpd.leases
# dhcpd -cf /etc/dhcpd.conf ath0
```

ahora nuestro punto de acceso por medio de “hostapd”:

```
# hostapd /etc/hostapd/hostapd.conf
```

Ahora iniciamos el servicio de la VPN:

```
# openvpn --config /etc/openvpn/serverOpenVPN.conf
```

y cuando se inicie el servicio va a arrojar una salida como la siguiente:

```
Tue Jul 08 03:37:12 2008 OpenVPN 2.0.9 i686-pc-linux [SSL] [LZO] [EPOLL] built on Jul  3 2008
Tue Jul 08 03:37:12 2008 Diffie-Hellman initialized with 1024 bit key
Tue Jul 08 03:37:12 2008 TLS-Auth MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]
Tue Jul 08 03:37:12 2008 TUN/TAP device tun0 opened
Tue Jul 08 03:37:12 2008 /sbin/ifconfig tun0 172.16.10.1 pointopoint 172.16.10.2 mtu 1500
Tue Jul 08 03:37:12 2008 /sbin/route add -net 172.16.10.0 netmask 255.255.255.0 gw 172.16.10.2
Tue Jul 08 03:37:12 2008 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135 ET:0 EL:0 AF:3/1 ]
Tue Jul 08 03:37:12 2008 UDPv4 link local (bound): [undef]:1194
Tue Jul 08 03:37:12 2008 UDPv4 link remote: [undef]
Tue Jul 08 03:37:12 2008 MULTI: multi_init called, r=256 v=256
Tue Jul 08 03:37:12 2008 IFCONFIG POOL: base=172.16.10.4 size=62
Tue Jul 08 03:37:12 2008 IFCONFIG POOL LIST
Tue Jul 08 03:37:12 2008 usuario-01,172.16.10.4
Tue Jul 08 03:37:12 2008 Initialization Sequence Completed
```

lo cual indica que está iniciado el servicio correctamente.

C.3. Política de Uso y Seguridad de la Red Inalámbrica.

A continuación se describe una posible política que puede implantarse en una institución como la Facultad de Estudios Superiores Aragón.

Introducción

La Facultad de Estudios Superiores Aragón ("FESA") cuenta con una red inalámbrica la cual los estudiantes, empleados y facultad ("usuarios") pueden utilizar para tener acceso desde varios puntos de la Institución al Internet y servicios de la red de la FESA. El acceso a la red inalámbrica es un privilegio, no un derecho. Por tal razón, cada usuario debe registrar su tarjeta inalámbrica para tener acceso a la red inalámbrica en la Centro de Cómputo (CC).

La FESA se reserva el derecho de modificar la Política en cualquier momento, siendo obligatorias dichas modificaciones a partir de la publicación de la Política modificada en la siguiente dirección de Internet:

http://www.fesa.unam.mx/wireless/

Cualquier modificación a esta Política será realizada cuando la FESA considere que es apropiado y es responsabilidad del usuario asegurarse el conocimiento de tales cambios.

Definiciones

- "Access point" (punto de acceso): equipo electrónico que actúa como punto central de conexión para los equipos que van a acceder la red inalámbrica. Utilizan antenas para transmitir y recibir la información que los usuarios soliciten.
- Autenticación: el proceso de verificar la identidad del usuario que solicita el acceso.
- Autorización: el proceso de asignar el permiso al usuario para manejar los objetos que solicita.

- Cobertura: área geográfica donde la señal de la red inalámbrica se puede obtener.
- Infraestructura Inalámbrica: todos los componentes involucrados para conformar una red inalámbrica. Por ejemplo, puntos de acceso, antenas, cableado, etc.
- Interferencia: degradación de la señal causada por la radiación electromagnética de otro dispositivo. La interferencia puede causar que la velocidad de transmisión/recepción de datos sea baja, errores en la transmisión/recepción de datos y/o la pérdida de la señal.
- MAC Address ("MAC"): número de seis octetos que identifica el equipo que va a ser utilizado en la red inalámbrica.
- Privacidad: confidencialidad de la información que se transmite por la red inalámbrica. Estos son discutidos más adelante en la sección de Privacidad.
- Port Scanning: Una tentativa de encontrar las debilidades de una computadora o de una red explorando o sondando puertos abiertos del sistema.
- Red Inalámbrica: una red de comunicaciones que utiliza el aire, minimizando la necesidad de cables, para transmitir y recibir datos.
- Seguridad: medidas para proteger los recursos de comunicación de acceso no autorizado y preservar la disponibilidad e integridad del servicio. Más información en la sección de Seguridad.
- SSID: Identificación que transmiten los puntos de acceso referente al nombre dado a la red inalámbrica para identificar el servicio.
- Spamming: enviar mensajes electrónicos a alguien desconocido que no ha solicitado expresamente la información (habitualmente de tipo comercial).
- Usuario: cualquier persona que solicite y haga uso de los servicios de la red inalámbrica.

Propósito

El manejo efectivo de los recursos de la red inalámbrica es importante para el beneficio de los usuarios de nuestra red y la Institución.

El uso efectivo, ético, moral y legal de los recursos de la red inalámbrica es importante para el beneficio de los usuarios de nuestra red y la Institución.

Este documento describe cómo la tecnología inalámbrica será utilizada, administrada, asegurada y apoyada en la FESA por Centro de Cómputo ("CC"). Además asegura que todos los usuarios de la red inalámbrica reciban un nivel de servicio de calidad en cuanto a confiabilidad, integridad, disponibilidad de servicio y seguridad. Este documento suplementa la Política de Comunicaciones de la FESA y la Política Institucional y Procedimiento para el Uso Ético Legal de las Tecnologías de Información de la FESA incluyendo direcciones y acciones específicas a la red inalámbrica y a la resolución de situaciones que puedan surgir.

Privacidad

La red inalámbrica provee acceso a recursos dentro y fuera de la Institución. Tal acceso es un privilegio y no un derecho el cual requiere que los usuarios actúen responsablemente. Los usuarios deben respetar los derechos de otros usuarios, respetar la integridad de los sistemas y los recursos físicos y observar las leyes, regulaciones y políticas a las cuales está sujeto el uso de la red inalámbrica.

La FESA reconoce el derecho a la privacidad de los usuarios y bajo ninguna circunstancia proveerá datos ni información de cualquier usuario sin antes consultarlo con el mismo. En el caso de violaciones a las leyes, regulaciones y políticas a las cuales esta sujeto el uso de la red inalámbrica por el uso indebido de las comunicaciones que se detecte en el monitoreo o auditoria realizada al equipo de la red, se procederá a consultar con el usuario dicha violación y se aplicarán las sanciones requeridas de ser necesario.

Los sistemas inalámbricos utilizan canales de radio para transmitir comunicaciones de

voz y datos en una red. El usuario reconoce que el servicio no es inherentemente seguro, que las comunicaciones inalámbricas pueden ser interceptadas por otros y que usted es el único responsable de tomar las precauciones que usted considere más convenientes para su situación y el propósito del uso del servicio. La FESA no garantiza su privacidad o seguridad en los datos que se transmiten cuando use el servicio de red inalámbrica.

La FESA renuncia a cualquier y a todas las responsabilidades del usuario o de cualquier otra parte por cualquier falta de privacidad, alteración de seguridad (ya sea del usuario o de redes o sistemas a los cuales el usuario se conecte) o pérdida, corrupción o intercepción de datos que el usuario experimente mientras utilice el servicio.

Responsabilidades

La responsabilidad de los recursos para las comunicaciones inalámbricas recae sobre el CC. Estas responsabilidades son y sin limitarse a:

- Toda instalación de equipo inalámbrico que tenga como propósito tener acceso a la red de comunicaciones de la Institución, debe ser aprobada por el CC.
- Proveer asistencia, orientación y recomendaciones sobre el equipo de comunicaciones inalámbricas que se debe utilizar en la Institución a los departamentos y oficinas que deseen proveer acceso a la red inalámbrica a los usuarios.
- Crear, mantener y actualizar la Política de Procedimientos y Seguridad de la red inalámbrica de la FESA.
- Mantener un registro de todas las tarjetas de comunicación inalámbrica y puntos de acceso en la Institución.
- Aprobar la instalación de equipo y programado para la red inalámbrica utilizado en la Institución.
- Informar a los usuarios de la red inalámbrica sobre la seguridad, las políticas y procedimientos relacionados al uso de las comunicaciones inalámbricas en la Institución.

- Monitorear el rendimiento y seguridad de todo el equipo de comunicaciones inalámbricas para prevenir acceso no autorizado a la red.
- Monitorear el desarrollo de las tecnologías de redes inalámbricas, evaluar mejoras a la red inalámbrica y si es apropiado, incorporar nuevas tecnologías para mejorar el rendimiento, capacidad, disponibilidad, seguridad y confiabilidad de la red.
- Resolver cualquier problema relacionado y reportado por los usuarios en relación a la interferencia entre los equipos inalámbricos.

Regulaciones y Estándares

- Todo equipo de cumplir mínimo con el estándar 802.11b de comunicación inalámbrica y con lo estipulado en este documento.
- El equipo de red inalámbrico tiene que cumplir con todas las reglas de las agencias reguladoras de comunicaciones, tales como la Federal Communications Commission (Comisión Federal de Comunicaciones) ("FCC") y las políticas de la FESA.
- Todo equipo de comunicaciones inalámbricas tiene que ser registrado en el CC para su uso.
- Solo se aprobará equipo que cumpla con las especificaciones de los equipos que rigen las comunicaciones de la Institución dispuestas por el CC.

Seguridad

El mantenimiento de la seguridad e integridad de la red inalámbrica de la Institución requiere métodos que aseguren que sólo los usuarios autorizados puedan tener acceso al mismo. De tal manera, el equipo debe tener las seguridades física necesarias para evitar que se vean afectados los servicios de la red inalámbrica.

- Todo departamento u oficina que vaya a comprar puntos de acceso tiene que reunirse con el personal técnico del CC para discutir las necesidades y especificaciones de los equipos que se requieren para la compatibilidad en la red de comunicaciones.

- Todos los puntos de acceso deben cumplir con las especificaciones que requiere el CC.
- Todos los puntos de acceso deben de ser registrados y aprobados por el CC. Para más información ver Registro De Puntos De Acceso.
- La instalación, manejo y uso del equipo de comunicaciones inalámbricas debe ser conforme a las leyes y regulaciones federales, estatales, locales y con las políticas de la FESA.
- El equipo debe ser instalado y configurado por personal técnico del CC.
- El equipo debe ser configurado para modificar los parámetros con los que viene de fábrica, de esta manera asegurar que ningún individuo tenga acceso a los mismos.
- El SSID debe ser configurado de manera que no contenga información que identifique la Institución, el producto, nombres o cualquier otra información que pueda ser utilizada por persona no autorizadas para intentar obtener acceso al servicio.
- Ningún individuo debe conectar ni instalar cualquier equipo de comunicaciones a la red sin la previa autorización del CC.
- El equipo debe ser instalado minimizando la interferencia con otros equipos de radio frecuencia.
- El CC responderá a reportes de equipo que puedan estar causando interferencia y de no resolverse la situación, el uso del equipo sospechoso puede ser restringido.
- El orden de prioridad para resolver asuntos relacionados al equipo de comunicaciones inalámbricas será el siguiente:
    - Vida y seguridad personal
    - Investigaciones
    - Enseñaza
    - Administración

- Acceso público
- Uso personal

- El acceso a la red inalámbrica será limitada a los usuarios registrados por el CC. Más información en la sección Autorización.
- Las comunicaciones inalámbricas no proveen codificación de los datos transmitidos. La protección de los datos es responsabilidad del usuario y de la aplicación que utilice para transmitir los datos.
- No se debe permitir ni fomentar el uso de la red inalámbrica para utilizar los sistemas administrativos de la Institución donde se transmiten o reciben datos confidenciales.
- El equipo debe ser protegido con medidas de seguridad para prevenir el hurto o acceso no autorizado al equipo de la Institución.
- Toda implementación de equipo tiene que proveer una medida de rastreo por MAC y deben proveer una seguridad de acceso interna o externa.
- El equipo está sujeto a monitoreo, pruebas de penetración y auditorías de seguridad.
- Cualquier equipo que represente un riego de seguridad para la red de comunicaciones de la Institución, podrá ser desconectado de la red y la persona que tiene registrados el equipo será notificado.
- Cualquier situación que no se pueda resolver con usuarios o individuos referente al sistema de red inalámbrica mediante el CC, será referido a las Autoridades para tomar la decisión que sea necesaria. La solución debe satisfacer al CC o a la FESA en primer lugar, el departamento u oficina en segundo lugar y por último al usuario.

Procedimiento para la seguridad

Este es el procedimiento para asegurar los recursos de comunicaciones y la seguridad de los servicios y equipos en el caso de detectar el uso indebido de la red inalámbrica:

- Un administrador debe ser contactado lo antes posible para desactivar la cuenta de usuario o desconectar el equipo de la red inalámbrica.
- Notificar al Director(a) de Sistemas de Información.
- Contactar al usuario de ser posible para verificar y discutir el supuesto uso indebido.
- Notificar de los resultados a las oficinas correspondientes para tomar aplicar acciones disciplinarias de ser necesario.

Autorización

Para que un usuario tenga acceso a la red inalámbrica, el equipo debe de estar registrado en el servidor que autoriza la conexión de ese equipo a la red. Se utiliza la seguridad por restricción de direccionamiento MAC. Si la MAC del usuario está registrada en la base de datos, se le da la autorización para aceptar la conexión. Las personas que tienen el privilegio de tener acceso a la red inalámbrica son: los estudiantes activos, los empleados de la FESA, la facultad y cualquier otra persona externa que por razones específicas y discutidas con el(la) Director(a) del CC necesite el acceso.

En el momento que el estudiante ya no esté activo en la Institución, se le revoca el acceso a la red inalámbrica. De la misma manera cuando un empleado o miembro de la facultad no presta servicios para la FESA se le revoca el acceso.

Se permitirá registrar hasta dos equipos para ser utilizado por el usuario.

Procedimientos Para Registrar La Tarjeta Inalámbrica

El usuario que desee tener conexión a la red inalámbrica debe visitar la oficina de Sistemas de Información, en el CC. Se le entregará un documento el cual debe llenar y se le solicitará la siguiente información o documentación:

- MAC Address

- Tira de materias vigente para evidenciar que es un estudiante activo
- Identificación con foto

Se permitirá registrar hasta dos equipos para ser utilizado por el usuario.

Registro De Puntos De Acceso

Las nuevas instalaciones para acceder a la red inalámbrica deben de ser compatibles con las existentes. Por tal razón, se exige que cualquier implementación que se planee hacer en la FESA sea consultada con el CC. De esta manera se asegura que la infraestructura de comunicaciones inalámbricas sea homogénea y uniforme para evitar riesgos de seguridad por incompatibilidad de equipo.

Luego de los puntos de acceso ser aprobados por el CC, cada punto de acceso tiene que ser registrado en para mantener un control de lo que sucede en la red inalámbrica y proveer un servicio de calidad. Para registrar un punto de acceso, tiene que pasar por el CC y llenar el formulario Registro de Puntos de Acceso el cual le requiere la siguiente información:

- Uso y propósito
- Lista de componentes a instalar
- Lugar de instalación
- Área de cobertura proyectada o propuesta
- Plan de cableado
- Plan de electricidad
- Medidas de seguridad física a ser implementadas
- Método de autorización a implementar

- Marca, modelo, numero de serie y dirección MAC del equipo
- Persona contacto

Monitoreo

El uso del equipo de la red inalámbrica es monitoreado por el CC por razones de seguridad y rendimiento. Cualquier equipo conectado a la red inalámbrica, puede ser monitoreado en cualquier momento. De encontrarse alguna falla en el equipo, ya sea por mala utilización, utilización inapropiada o no autorizada, el equipo podrá ser desconectado de la red. En este caso se consultaría a la persona contacto referente al equipo para resolver cualquier punto encontrado que no sea correcto en el monitoreo.

La FESA no monitorea rutinariamente el uso individual de los usuarios, se monitorea el uso del equipo de la red inalámbrica completa para propósitos de mantenimiento y seguridad para proveer un servicio con la mejor disponibilidad, seguridad, confiabilidad y rendimiento. Mediante estos reportes se pueden obtener estadísticas e información del uso que tiene la red de comunicaciones inalámbrica.

En ciertas ocasiones se puede tomar la decisión de monitorear la actividad de un usuario en particular e individual cuando:

- El usuario voluntariamente lo ha solicitado.
- Es necesario para proteger la seguridad, confiabilidad, integridad y disponibilidad del servicio.
- Es necesario para evitar que la FESA pueda estar sujeto a sanciones por violaciones a leyes federales, estatales y/o locales por el uso indebido de las comunicaciones.
- Hay una causa razonable para creer que el usuario ha violado o está violando esta política, leyes federales, estatales y/o locales.
- Hay una acusación o notificación por parte de un usuario que indica que se ha violado o está violando esta política, leyes federales, estatales y/o locales.

- Indicaciones de que el usuario ha estado en una actividad inusual o excesivamente inusual obtenidas de los informes de monitoreo general.
- De ser solicitado por agencias federales, estatales, locales u otra agencia que tenga como responsabilidad aplicar y hacer cumplir las leyes.

Estos monitoreos individuales deben ser autorizados por el Asesor Legal de la FESA, él(la) Rector(a) y él(la) Director(a) del CC. Los privilegios y el derecho a la privacidad del usuario serán considerados y preservados en todo momento y en lo que más se pueda.

Disponibilidad del Servicio

El servicio está disponible mientras estén dentro del rango de cobertura de los puntos de acceso del sistema. Las ubicaciones y los equipos son actualizados o añadidos ocasionalmente y la cobertura actual del servicio, velocidades y calidad podrán variar.

El servicio de conexión a la red inalámbrica está sujeto a la no disponibilidad, incluyendo: emergencias, averías en el servicio, transmisión, equipos, problemas o limitaciones de la red, interferencia, mantenimiento y reparación y, podrá ser interrumpido, denegado, limitado o reducido.

Condiciones de Uso

Para mantener una mejor red inalámbrica se requiere que los usuarios actúen responsablemente. A continuación y sin limitación alguna se mencionan las condiciones de uso para la red inalámbrica.

Los usuarios deben aceptar y cumplir las condiciones de uso que se describirán a continuación. El utilizar el servicio de la red inalámbrica constituye la aceptación de las siguientes Condiciones de Uso y las consecuencias que puedan surgir debido al uso incorrecto de las comunicaciones inalámbricas.

Conexión

- El usuario no debe compartir su conexión a la red inalámbrica con ningún otro individuo.
- No debe acceder a recursos de comunicaciones sin la debida autorización.
- No debe autorizar a ningún otro individuo a usar el servicio.
- A los usuarios que se le provea una cuenta con contraseña, no debe revelar la contraseña ni cederle la cuenta a otro individuo para obtener acceso.
- Nos reservamos el derecho incondicional de suspender o rescindir el uso de la red inalámbrica por cualquier violación a esta Política de Uso, cualquier actividad que interfiera con el uso o disfrute de otros usuarios de Internet o con el funcionamiento de nuestra red o servicios.

Recuerde que el usuario bajo el cual está registrada la cuenta es el responsable de toda actividad que se lleve a cabo bajo esa cuenta.

Licencias y derechos de "copyright"

- Se prohíbe toda transmisión y/o distribución de cualquier material en violación de cualquier ley o regulación aplicable. Esto incluye, sin limitación alguna, todo material protegido por los derechos de autor, marcas, secretos comerciales u otros derechos de propiedad intelectual usados sin la debida autorización.
- Programas y aplicaciones no deben ser copiados o transmitidos, excepto que esté expresamente permitido por su licenciamiento.
- Queda expresamente prohibido el transmitir y/o distribuir archivos de multimedia el cual usted no tenga autoridad, y no limitado a:
    - Música

- Videos
- Fotos

Sistemas

- Queda terminantemente prohibido acceder y utilizar los sistemas administrativos de la FESA.
- No está permitido acceder, alterar o usar áreas no públicas de la red de la FESA, sin limitarse a:
  - El acceso no autorizado o el uso de datos, sistemas o redes, incluyendo cualquier intento de probar, explorar o verificar la vulnerabilidad de un sistema o de la red; o de violar las medidas de seguridad o de autenticación sin la autorización expresa del propietario del sistema o de la red.
  - El monitoreo no autorizado de datos o de tráfico de cualquier red o sistema sin la autorización expresa del propietario del sistema o de la red.
  - La interferencia con el servicio de cualquier usuario, equipo o red incluyendo, sin limitación alguna, intentos intencionales de sobrecargar un sistema y ataques.

Ética y Moral

- Se prohíbe la transmisión y/o distribución de cualquier material discriminatorio, hostil, degradante o intimidatorio para cualquier persona o grupo de personas en razón de su religión, género, orientación sexual, raza, etnia, edad o discapacidad.
- Se prohíbe transmitir información ilegal, abusiva o cuestionable de alguna otra forma, incluyendo, sin limitación a ellas, cualquier transmisión que constituya o anime a una conducta penal delictiva u ocasione una responsabilidad civil según cualquier legislación vigente.
- Se prohíbe transmitir mensaje que revele cuestiones personales o privadas relativas a cualquier persona, entre las que se incluyen, pero sin limitación a ellas, mensajes

o información que pueda infringir los derechos de las personas a su privacidad o publicidad.

- Esta prohibido hacer “spamming” y otro tipo de mensajería en masa a cualquier destinatario.
- No se debe utilizar la identidad de otro usuario si la debida autorización del mismo.
- No se debe actuar de manera que se dé la impresión de que el usuario está representando, dando opiniones o haciendo declaraciones en nombre de la FESA sin la debida autorización.
- No se debe utilizar el nombre la FESA en actividades religiosas ni políticas para implicar el apoyo, representación u oposición a cualquier actividad de esta índole.
- No se debe utilizar la red inalámbrica de la FESA para fines comerciales, excepto que los mismos estén aprobados por las debidas autoridades de la FESA.
- No se debe transmitir anuncios personales, anuncios comerciales o promociones, excepto que los mismos estén aprobados por las debidas autoridades de la FESA.

Equipos de la red inalámbrica

- Los usuarios no deben modificar, dañar o remover el equipo de comunicación inalámbrico de la FESA.
- No deben generar ningún tipo de interferencia que afecte el funcionamiento de los equipos de comunicaciones.

Información y Programas destructivos o no autorizados

- No está permitido la diseminación de información falsa o dañina, por ejemplo:
    - Transmitir mensaje anónimamente o con un nombre o identificación de usuario falsos

- Transmisión y/o distribución de cualquier material que contenga virus de “software” o cualquier otro programa, archivo o código informático diseñado o concebido para perturbar, dañar o limitar el funcionamiento de cualquier “software”, “hardware” o equipo de telecomunicaciones u obtener acceso no autorizado a datos o cualquier otra información.

- No está permitido en utilizar cualquier programa que tenga como fin:
  - Hacer un rastreo de puertos en la red (“port scanning”)
  - Recolectar información que está siendo transmitida
  - Monitorear las comunicaciones
  - Buscar vulnerabilidades en la red, servidores, computadoras, equipo de comunicación, equipo electrónico conectado a la red.
  - Falsificar la identidad de algún usuario
  - Enviar mensajes en masa (“spamming”)
  - Cualquier otro programa que viole alguna de las condiciones anteriormente expuestas

Responsabilidad

Todos los usuario tienen la responsabilidad de notificar al CC de cualquier acción descubierta en relación a la violación de cualquiera de las condiciones descritas anteriormente, el uso inapropiado del las comunicaciones electrónicas o el uso inapropiado del equipo perteneciente a la FESA. El proceso se llevará a cabo en carácter serio, confidencial y seguro.

La FESA no es responsable de los datos, mensajes o páginas perdidas, no entregadas o mal dirigidas, debido a problemas de interrupciones o en el desempeño, asociados con el servicio o redes de comunicaciones de la FESA. La FESA podrá imponer límites de uso, suspender o bloquear ciertos tipos de uso a nuestra única discreción para proteger a los usuarios o a nuestra Institución. El utilizar alguno de los servicios ofrecidos por esta

red inalámbrica implica la aceptación de las presentes condiciones de uso.

No se acepta ningún tipo de responsabilidad, ni civil ni penal, que pudiera derivarse de actividades ilícitas realizadas mediante o con la utilización de los recursos que le hayan sido proporcionados por esta red inalámbrica. Cualquier tipo de responsabilidad recaerá única y exclusivamente en el usuario beneficiario de dicho recurso.

Los servicios se prestan "tal cual" y sin ninguna garantía.

Si el usuario no está de acuerdo con los términos de éste Acuerdo, no debe utilizar el servicio.

Los administradores podrán limitar o denegar el acceso, contenido u otras características de los servicios con el objetivo de preservar el buen funcionamiento de los mismos.

Apoyo Técnico

Los técnicos de la FESA no proveen apoyo técnico a los usuarios en cuanto a "hardware" ni "software" instalados en el equipo. La única intervención de los técnicos de la FESA en el equipo de los usuarios será cuando se deba obtener la MAC Address para poder dar el acceso a la red inalámbrica y/o verificar que el equipo recoja dirección IP del servidor para la conexión a la red. Cuando se determina que el equipo puede recoger la dirección IP del servidor será responsabilidad del usuario el configurar el "software" o sistema operativo para lograr acceso a los servicios de Internet y red, como por ejemplo lo es un "firewall" personal o el "firewall de Windows XP".

Aplicación de las leyes

Violaciones accidentales o menores de estas condiciones serán informadas por el CC al usuario por correo electrónico o en persona para propósitos de discusión y educación.

Violaciones severas (incluyendo violaciones menores en repetidas ocasiones) pueden resultar en una perdida del privilegio de acceso a la red inalámbrica y a posibles sanciones.

Estas violaciones tanto menores como severas pueden ser reportadas a la Dirección y/u otra autoridad para que tomen las acciones correspondientes.

Algunas violaciones constituyen ofensas criminales establecidas en leyes federales, estatales y locales. La FESA reportará tales violaciones a las autoridades correspondientes.

Las violaciones a la seguridad del sistema o de la red están prohibidas, y pueden originar responsabilidad penal o civil. La FESA investigará todos los hechos relacionados con dichas violaciones y cooperará con la aplicación de ley si se sospecha que ha ocurrido una violación de las leyes penales.

Los usuarios en violación de esta Política están sujetos a sanciones, incluyendo la pérdida de los privilegios de acceso a la red inalámbrica, acciones disciplinarias, despido de la Institución, denegación de estudio en la Institución y acciones legales.

Referencias

[1] Jim Geier, *Wireless Networks first-step*, Cisco Press, ISBN: 1-58720-111-9, 2004.

[2] Vijay K. Garg, *Wireless Communications an Networking*, Elsevier, ISBN: 978-0-12-373580-5,2007.

[3] Jim Geier, *Wireless LANs, Second Edition*, SAMS, ISBN: 0-672-32058-4, 2001.

[4] Cyrus Peikari, Seth Fogie, *Maximum Wireless Security*, SAMS, ISBN : 0-672-32488-1, 2002.

[5] Steve Rackley, *Wireless Networking Technology*, Elsevier, ISBN 13: 978-0-7506-6788-3, 2007.

[6] Anand R. Prasad, Neeli R. Prasad, *802.11 WLANs and IP Networking Security, QoS, and Mobility*, ISBN: 1-58053-789-8, 2005

[7] David D. Coleman, David A. Westcott, *CWNA Certified Wireless Network Administratorł Study Guide*, Wiley, ISBN-13: 978-0-471-78952-9, 2006.

[8] John R. Vacca, *Guide to Wireless Network Security*, Springer, ISBN-13: 978-0-387-95425-7, 2006.

[9] Brown, Edwin Lyle, *802.1X Port-Based Authentication*, Auerbanch, ISBN-13: 978-1-4200-4464-5, 2007.

[10] Christian Barnes, Tony Bautts, *Hack Proofing Your Wireless Network*, Syngress, ISBN: 1-928994-59-8, 2002

[11] Chris Hurley, Russ Rogers, *WarDriving and Wireless Penetration Testing*, Syngress, ISBN 13: 978-1-59749-111-2, 2007.

[12] Institute of Electrical and Electronics Engineers, *Wireless LAN Medium Access Control and Physical Layer specifications*, http://easy.intranet.gr/IEEE802.11b.pdf

[13] Institute of Electrical and Electronics Engineers, *802.1X Port-Based Naetwork Access Control*, http://standards.ieee.org/getieee802/download/802.1X-2004.pdf

[14] fluhrer, Scott, *Weaknesses in the Key Scheduling Algoritm of RC4*, http://www.drizzle.com/∼aboba/IEEE/rc4_ksaproc.pdf

[15] Moerschel Grant, Dreger Richard,*CWSP Certified Wireless Security Professional Official Study Guide Exam PW0-200*, ISBN-13: 978-0-07-226320-6