MECANISMOS DE SEGURIDAD EN REDES WI – FI: WPA2 Y SERVIDORES RADIUS

LUÍS FERNANDO CASTILLA AURELA
JOSÉ MANUEL MARRUGO REDONDO

Monografía presentada como requisito para optar al titulo de Ingeniero Electrónico

ASESOR
DAVID SENIOR ELLES
MAGISTER EN INGENIERIA ELECTRONICA

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
FACULTAD DE INGENIERIA ELECTRONICA Y ELECTRICA
CARTAGENA D.T. Y C.
2006

MECANISMOS DE SEGURIDAD EN REDES WI - FI: WPA2 Y SERVIDORES RADIUS

LUÍS FERNANDO CASTILLA AURELA
JOSÉ MANUEL MARRUGO REDONDO

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
FACULTAD DE INGENIERIA ELECTRONICA Y ELECTRICA
CARTAGENA D.T. Y C.
2006

Cartagena, 15 Junio de 2006

Señores
Comité curricular de Ingeniería Eléctrica y Electrónica.
Universidad Tecnológica de Bolívar
Ciudad

Respetados Señores:

Por medio de la presente me permito informarles que la monografía titulada "MECANISMOS DE SEGURIDAD EN REDES WI – FI: WPA2 Y SERVIDORES RADIUS" ha sido desarrollada de acuerdo a los objetivos establecidos.

Como autores de la monografía consideramos que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

_____ _____

LUIS FERNANDO CASTILLA A. **JOSE MANUEL MARRUGO R.**

Cartagena, 15 Junio de 2006

Señores
Comité curricular de Ingeniería Eléctrica y Electrónica.
Universidad Tecnológica de Bolívar

Respetados Señores:

Cordialmente me permito informarles, que he llevado a cabo la dirección del trabajo de grado de los estudiantes Luís Fernando Castilla Aurela y José Manuel Marrugo Redondo, titulado **MECANISMOS DE SEGURIDAD EN REDES WI – FI: WPA2 Y SERVIDORES RADIUS.**

Atentamente,

_____
DAVID SENIOR ELLES
Ingeniero Electrónico
Magíster en Ingeniería Electrónica.

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Cartagena de Indias D. T. y C. 15 Junio de 2006

DEDICATORIA

A Dios y a la Virgen por la fortaleza y
la voluntad para culminar exitosamente
esta etapa de mi vida.

A mis padres por sus esfuerzos y sacrificios,
por brindarme siempre su apoyo y permitir
materializar mis sueños e ideales.

A mi abuela y mis tías por su apoyo
incondicional, sin ustedes fuese sido más
difícil alcanzar este objetivo.

A mis hermanos Elkin, José Miguel, Migue
y Bertha por su respaldo en todo momento.

A mis amigos por su colaboración y compañía
y por convertirse en los hermanos que escogí tener.

.

A mis profesores por transmisitir sus conocimiento
Y contribuir a mi formación personal.

José Manuel Marrugo Redondo.

DEDICATORIA

A Dios y a los ángeles por darme la gracia y fortaleza

Para vencer todos los obstáculos para

Culminar estés proceso.

A mis padre Jorge Castilla y Norma Aurela por

Apoyarme desde un primero momento

Y ayudarme a no desfallecer y acompañarme hasta

Lograr este triunfo que le da gran sentido a mi vida.

A mis hermanos jorge enrique, Alex, Sandra

Y Maria Claudia por haber estado conmigo en los momentos

Tristes y alegres de mi carrera.

A mi tía Carmen Aurela por ese apoyo incondicional y por

Sus enseñanzas espirituales que son enriquecedoras

Para mi crecimiento personal y profesional.

A mis amigos por estar conmigo y por

Crearme grandes recuerdos.

Luís Fernando Castilla Aurela.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

GLOSARIO

AAA: Autenticación Autorización Accounting
AES: Estándar de Cifrado Avanzado
AP: Punto de Acceso
Beacom Frames: Tramas de Gestión
Bluetooth: Tecnología inalámbrica de corto alcance para redes personales.
BSS: Basic Service Set
CCA: Clear Channell Assesment
CCMP: Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol
DSSS: Direct Sequence Spread Spectrum
EAP: Protocolo de Autentificación Extensible
EAPOL: EAP Over LAN
Eavesdropping: Interceptación
GMK: Group Master Key
Hijacking: Secuestro
IP: Protocolo de Internet
IPSC: Protocolo de Seguridad de Internet
MAC: Control de Acceso al Medio
MIC: Message Integrity Protocol
NIST: National Institute of Standars.
PDA: Personal Digital Assistant
PMK: Pairwise Master Key
PPK: Perpacket Keying
PSK: Preshared Key
PTK: Pairwise Transient Key
RADIUS: Remote Authentication Dial-In User Service
RC4: Cifrado 4 de Rivest
Roaming: Servicio que permite al usuario que viaja y puede operar bajo una red de un operador celular de dicho lugar como si fuera una llamada local
RTP: Protocolo de transporte en tiempo real
Sniffing: Escuhas
Spoofing: Burla
SSID: Identificador de Establecimiento de Servicio
STA: Estación Cliente
Surveillance: Espionaje
TKIP: Temporal Key Integrity Protocol

VPN:	Virtual Private Network
WEP:	Wired Equivalent Privacy
Wi – Fi:	Wireless Fidelity
WISP:	Proveedores de Servicios de Internet Inalámbrico
WPA2:	WI FI Protected Access 2
WPA2/WPS IE:	Wi-Fi Protected Access 2 (WPA2)/Wireless Provisioning Services Information Element (WPS IE)

RESUMEN

Wi-FI, iniciales de Wireless Fidelity, comprende a un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11. Inicialmente Wi-Fi se creó con el objetivo de desarrollar una nueva forma de redes locales, las redes inalámbricas. Actualmente su uso se ha extendido también al acceso a Internet de los equipos integrados en dicha red local.

El uso de redes inalámbricas tiene sus ventajas como la movilidad, la flexibilidad en la instalación, la simplicidad y rapidez en la instalación, el costo de propiedad reducido y la escalabilidad que nos permiten, sin embargo como principal inconveniente tenemos el intrusismo de usuarios no permitidos en dichas redes debido a la vulnerable seguridad que presentan.

Como antes indicamos el organismo que rige el uso de este tipo de redes es el IEEE, mediante su familia de estándares 802.11. Así los estándares más extendidos son el 802.11b y 802.11g debido a que la banda en la que trabajan, la de 2.4 GHz está disponible casi universalmente, teniendo una velocidad de hasta 11 Mbps y 54 Mbps respectivamente. En EEUU y Japón está el estándar 802.11a que opera en la banda de los 5 GHz, aunque este estándar ya se ha incluido en Europa. También hay que mencionar el estándar 802.11n que se espera que alcance la velocidad de 500 Mbps. En Europa también se consideró el uso de otra tecnología inalámbrica llamada HIPERLAN del ETSI.

Los dispositivos inalámbricos son capaces de hacer un rastreo o scan para localizar el canal en que está trabajando la red. El máximo son 14 canales, tomándose como valor por defecto 11 (Cada entidad reguladora ha elegido un valor: 11 en USA, 13 en Europa, 14 en Japón, etc.) que se configura por software (Regulation Domain).

Existes dos tipos de redes inalámbricas. La red mediante ad-hoc, aquella en la cual dos o más dispositivos inalámbricos están conectados sin infraestructura, uno de ellos debe crear la red a la que los demás posteriormente se conectaran. Y la red mediante puntos de acceso, en la que los ordenadores se conectaran a través de estos puntos de acceso.

El hardware Wi Fi que es necesario para una red inalámbrica es: punto de acceso (guardar y repetir los mensajes recibidos), routers (toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados), tarjeta de red inalámbrica y antena.

Para configurar una red Wi Fi mediante puntos de acceso lo primero que tenemos que configurar es el AP, después nuestro equipo, en el que si tenemos activado el DHCP, tendremos que escanear las redes disponibles, seleccionar la nuestra y conectarnos a ella. En cambio si el DHCP lo tenemos desactivado, hay que establecer manualmente la dirección IP de nuestro equipo, la puerta de enlace, la máscara de subred y los servidores DNSs.

El alcance de la señal de nuestra red Wi Fi dependerá de:

- La potencia del Punto de Acceso.
- La potencia del accesorio o dispositivo Wi Fi por el que nos conectamos.
- Los obstáculos que la señal tenga que atravesar (muros o metal).

Cuanto más lejos (linealmente) quieras llegar, más alto deberás colocar el punto de acceso. Si quieres llegar lejos, evita también interferencias como microondas o teléfonos inalámbricos. Si la señal te llega debilitada, utiliza un amplificador de señal

o si es posible, monta una nueva antena de más potencia al AP (los Puntos de Acceso de gama baja NO lo permiten) o una antena exterior al accesorio (normalmente sólo para formatos PCMCIA o PCI).

Los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio. Las ondas de radio, en principio, pueden viajar más allá de las paredes y pueden filtrarse en habitaciones/casas/oficinas contiguas o llegar hasta la calle.

Sin embargo si nuestra instalación está *abierta*, una persona con el equipo adecuado y conocimientos básicos podría no sólo utilizar nuestra conexión a Internet, sino también acceder a nuestra red interna o a nuestro equipo, donde podríamos tener carpetas compartidas, o analizar toda la información que viaja por nuestra red y obtener así datos que podrían comprometer nuestra integridad.

De esta forma la seguridad es un aspecto que cobra especial relevancia cuando hablamos entonces de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red mientras que en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

Por eso el canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

Conscientes de este problema, el IEEE publicó un mecanismo opcional de seguridad, denominado WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cableado), que utiliza una misma clave simétrica y estática en las estaciones y el punto de

acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. El algoritmo de encriptación utilizado es RC4 con claves (seed), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. Sin embargo, el estándar 802.11 no especifica cómo manejar el IV. Queda abierta a los fabricantes la cuestión de cómo variar el IV en sus productos.

La consecuencia de esto es que buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada trama. Por otro lado, el número de IVs diferentes no es demasiado elevado (2^{24}=16 millones aprox.), por lo que terminarán repitiéndose en cuestión de minutos u horas. La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse; existen implementaciones con claves de 128 bits (lo que se conoce como WEP2), sin embargo, en realidad lo único que se aumenta es la clave secreta (104 bits) pero el IV se conserva con 24 bits. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

La forma de aceptar estaciones que vayan a unirse a la red es la siguiente, el punto de acceso envía un texto en claro a la estación y ésta con su contraseña WEP, lo cifra y se lo devuelve. El punto de acceso finalmente descifra el mensaje recibido, comprueba que su ICV es correcto y lo compara con el texto que envió. Este mecanismo de autentificación de secreto compartido tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP.

Otro problema reside también en la ausencia de mecanismos de protección contra mensajes repetidos (replay). Esto permite que se capture un mensaje y se introduzca en la red en un momento posterior.

Por tanto WEP ha sido roto de distintas formas, lo que lo ha convertido en una protección inservible.
WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Las tecnologías de este protocolo WPA son:

- EAP. Es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad. WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN).
- TKIP (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.
- MIC (Message Integrity Code) o Michael. Código que verifica la integridad de los datos de las tramas.
- Servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service). Si la autorización es

positiva, entonces el punto de acceso abre el puerto (el concepto de puerto puede aplicarse a las distintas conexiones de un punto de acceso con las estaciones). El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

WPA puede funcionar en dos modos:

- Con servidor AAA, RADIUS normalmente. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.
- Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

El último apartado referente a la seguridad será el denominado protocolo WPA2, este incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard). Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos, esto significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC.

Otra mejora respecto a WPA es que WPA2 incluye soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

1. SEGURIDAD EN REDES WI – FI

1.1. Introducción

El uso de tecnología de comunicación basada en redes inalámbricas ha proporcionado nuevas expectativas de futuros para el desarrollo de sistemas de comunicación, así como nuevos riesgos.

La flexibilidad y la movilidad que nos proporcionan las nuevas redes inalámbricas han hecho que la utilización de estas se haya incrementado siendo la mejor manera de realizar conectividad de datos en edificios sin necesidad de cablearlos.

Pero como todas las nuevas tecnologías en evolución, presenta unos riesgos debidos al optimismo inicial y en la adopción de la nueva tecnología sin tener en cuenta los riesgos inherentes a la utilización de un medio de transmisión tan "observable" como son las ondas de radio.

El presente trabajo pretende dar una visión global del estado actual de la seguridad en las redes inalámbricas, desde los riesgos existentes en las implementaciones de los estándares actuales, hasta las mejoras propuestas para subsanar dichos riesgos pasando por consideraciones recomendadas en cuanto al diseño de redes inalámbricas.

1.2 Historia de La Seguridad en Redes Wi - Fi

Tras la publicación de los primeros estándares que determinaron el nacimiento de las redes Wireless Ethernet (IEEE 802.11a y b), como podemos ver en la tabla 1, también denominadas WI – Fi por el consorcio que empuja su implantación y la interoperabilidad de los productos, surgió la necesidad inmediata de proporcionar un protocolo que brindara seguridad frente a intrusiones en este tipo de transmisiones de donde surgió WEP (Wired Equivalent Privacy). Este protocolo proporciona tres mecanismos de seguridad (por nombre de la red o SSID, por clave estática compartida y por autentificación de dirección MAC) que se pueden utilizar por separado pero que es más recomendable combinarlos. Sin embargo pronto se descubrió que todos ellos eran fácilmente desbloqueados en corto tiempo (incluso minutos) por expertos, utilizando herramientas de escucha en redes (sniffers).

Wireless Standard	802.11b		802.11a		802.11g	
Popularity		Widely adopted. Readily available everywhere.		New technology. Limited adoption.		New technology. Limited adoption, but rapid growth expected.
Speed	11 Mbps	Up to 11Mbps	54 Mbps	Up to 54Mbps (5X greater than 802.11b)	54 Mbps	Up to 54Mbps (5X greater than 802.11b)
Cost	$	Inexpensive	$$$	Expensive	$$	Moderate
Frequency	2.4 GHz	Crowded 2.4GHz band. May conflict with other 2.4GHz devices like cordless phones, microwave ovens, etc.	5 GHz	Uncrowded 5GHz band.	2.4 GHz	Crowded 2.4GHz band. May conflict with other 2.4GHz devices like cordless phones, microwave ovens, etc.
Range	100-150	Good Range. Typically up to 100-150 feet indoors, depending on construction, building materials, room layout.	25-75	Limited range. Typically no more than 25 to 75 feet indoors.	100-150	Good Range. Typically up to 100-150 feet indoors, depending on construction, building materials, room layout.
Public Access		The number of public "Hot Spots" is growing rapidly, allowing wireless connectivity in many airports, hotels, college campuses, public areas, and restaurants.	X	None at this time.		Compatible with current 802.11b "Hot Spots" (at 11Mbps)
Compatibility	OK 802.11b	Widest adoption Wi Fi	OK 802.11a	Incompatible with 802.11b or 802.11g	OK 802.11b 802.11a	Interoperates with 802.11b networks (at 11Mbps) Incompatible with 802.11a

Tabla 1. Primeros Estándares Para Redes Wi-Fi.[1]

[1] G. Álvarez / P.P. Pérez (CSIC), Seguridad en Wifi. Pag 5

Para inhibir un poco este inconveniente, se han diseñado soluciones no estandarizadas apuntando en diferentes áreas. La primera de ella es sustituir el mecanismo de clave estática por uno de clave dinámica WEP (TKIP), lo que dificulta su identificación, puesto que el tiempo de computación que lleva es mayor que la frecuencia de cambio. Sin embargo debe ser complementada con otras técnicas como sistemas Radius para forzar la identificación de usuario, túneles VPN (Red Privada Virtual) con cifrado IPSC (Protocolo de Seguridad de Internet), o análogo entre el Terminal de usuario y un servidor seguro interno para imposibilitar el análisis de las tramas enviadas por radio.

Los consorcios reguladores, concientes de la gravedad de esta debilidad y su fuerte impacto negativo en el crecimiento de las Wlans, propusieron una recomendación denominada WPA (WI-FI Protected Access) que conjuga todas las técnicas anteriormente expuestas. Fue creado como una solución hasta que se diera la ratificación del IEEE 802.1i, en realidad es un subconjunto de medidas del Standard 802.11i, diseñado para que todos los equipos Wi Fi vendidos puedan ajustarse a sus requerimientos tras una actualización de software o firmware.

Entre sus nuevas funcionalidades se encuentra la implementación de mecanismos de autentificación mutua, la distribución dinámica de claves, la utilización de nuevos algoritmos sobre RC4 que sustituye a WEP, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación con nuevos mecanismos para garantizar la integridad de los mensajes. Aunque WPA es un estándar de encriptación mucho más robusto que WEP tiene ciertas debilidades potenciales en la manera como puede ser configurado por un usuario particular como son: claves muy cortas, claves con cierta cantidad de caracteres pero fácilmente reconocibles, es decir, palabras usuales.

De esta forma nace WPA2 que es una certificación de productos disponible a través de Wi-Fi Alliance que certifica que los equipos inalámbricos son compatibles con el estándar IEEE 802.11i.

El estándar IEEE 802.11i reemplaza formalmente la Privacidad equivalente por cable (WEP, Wired Equivalent Privacy) del estándar IEEE 802.11 original por un modo específico del Estándar de cifrado avanzado (AES, Advanced Encryption Standard), conocido como Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) Protocol (CCMP). CCMP proporciona tanto confidencialidad (cifrado) como integridad a los datos. Aquí se describen los detalles de la implementación de WPA2 para el cifrado, el descifrado y la validación de la integridad de los datos de las tramas inalámbricas 802.11. En la tabla 2 podemos observar los distintos tipos de protocolos que han surgido.

- IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard (1999)
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c - Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e - Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F - Inter-Access Point Protocol (2003)
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i - Enhanced security (2004)
- IEEE 802.11j - Extensions for Japan (2004)
- IEEE 802.11k - Radio resource measurement enhancements
- IEEE 802.11l - (reserved, typologically unsound)
- IEEE 802.11m - Maintenance of the standard; odds and ends.
- IEEE 802.11n - Higher throughput improvements
- IEEE 802.11o - (reserved, typologically unsound)
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
- IEEE 802.11q - (reserved, typologically unsound, can be confused with 802.1q VLAN trunking)
- IEEE 802.11r - Fast roaming
- IEEE 802.11s - ESS Mesh Networking
- IEEE 802.11T - Wireless Performance Prediction (WPP) - test methods and metrics
- IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)
- IEEE 802.11v - Wireless network management
- IEEE 802.11w - Protected Management Frames

Tabla2. Protocolos IEEE 802.11x [2]

[2] G. Álvarez / P.P. Pérez (CSIC), Seguridad en Wifi. Pag 6

2. RIESGOS DE LAS REDES WI – FI

2.1. Vulnerabilidad de las Redes Inalámbricas

Hace algún tiempo se publicó en varios medios de comunicación, de la posibilidad de que exista vulnerabilidad en el protocolo 802.11, y esto lo podemos reflejar en el siguiente caso de la vida cotidiana en el ámbito de la informática

Un ejemplo clave fue cuando, se detectaron vulnerabilidades en las aplicaciones de hardware del protocolo IEE802.11 los cuales habilitan a un usuario que desea atacar, poder hacerlo con un dispositivo de bajo rango y costo. Varias compañías en conjunto han establecido las fallas en las implementaciones de hardware del protocolo inalámbrico IEEE 802.11, estas fallas permiten un ataque trivial, pero efectivo en contra de la disponibilidad de los dispositivos de WLAN.

Un atacante, usando un dispositivo de bajo poder como un PDA electrónico con tarjeta de red inalámbrica, como podemos observar en la figura 1, puede causar una disrupción significativa a todo el rango de tráfico de un WLAN de manera que hace difícil detección o localización del atacante.

Figura 1. Formas Básicas de Penetrar una Red. [3]

[3]. G. Álvarez / P.P. Pérez (CSIC), Seguridad en Wifi. Pag 30.

La falla esta relacionada a la función Médium Acces Control (MAC) del protocolo IEEE 802.11 dentro del procedimiento Clear Channell Assesment (CCA), el cual es usado en todos los dispositivos inalámbricos que cumplen el estándar y que es fundamental para la transmisión simultanea dentro de una WLAN

El protocolo de red inalámbrico IEEE 802.11 usa el algoritmo Clear Channel Assessment (CCA) para determinar si el canal de radio de frecuencia se encuentra libre para que el dispositivo pueda transmitir data. El algoritmo CCA usado en conjunto con la transmisión Direct Sequence Spread Spectrum (DSSS), es vulnerable a un ataque en el cual una señal de radio de frecuencia, especialmente diseñada, causará que el algoritmo concluya que el canal está ocupado haciendo que ningún dispositivo transmita data.

Una persona que ataque y explote dicha vulnerabilidad en la función CCA en la capa física, causará que la transmisión de datos durante el ataque entre los nodos de la WLAN, ya sean clientes o puntos de acceso y, cuando estén siendo atacados los dispositivos, éstos se comportarán como si el canal estuviese siempre ocupado, previniendo la transmisión de cualquier tipo de datos sobre la red inalámbrica.

La particularidad de esta falla es que no se necesitan equipos sofisticados, ni mucho dinero y tampoco muchas habilidades para poderla llevar a cabo. El potencial de daño de esta falla se incrementará en el tiempo a medida que el uso de las redes inalámbricas para infraestructuras críticas.

Los dispositivos de hardware inalámbrico que implementan el protocolo IEEE802.11 usando la capa física DSSS. Incluye también IEEE 802.11, 802.11b y dispositivos inalámbricos 802.11g (debajo de los 20Mbps). Excluye IEEE 802.11ª y dispositivos high-speed 802.11g (por encima de 20Mbps).

Los dispositivos en el rango de dispositivos de ataque estarán afectados. Si un AP está en un rango, todos los dispositivos asociados con ese AP serán denegados del servicio; si un A no está dentro del rango, únicamente esos dispositivos en el rango de ataque tendrán denegación de servicio.

Existen ciertas amenazas en las redes inalámbricas de área local, estas amenazas se caracterizan mínimo por:

- Un atacante puede usar hardware o drivers comodity, no se requiere hardware inalámbrico o dedicado.

- Un atacante consume recursos limitados en un dispositivo atacante, así que no es costoso para montar.

- La vulnerabilidad no será mitigada por capas emergentes MAC en mejoras de seguridad, por ejemplo, IEEE 802.11 TGi.

- Los vendedores independientes han confirmado que actualmente no hay defensa en contra de este tipo de ataques a DSSS basadas en WLANs.

- El rango de alcance del ataque puede crecer si se incrementa el poder de transmisión del dispositivo atacante o se usa una antena de alto aumento.[4]

[4] Canarias Wireless, Vulnerabilidades Inalámbricas. Articulo. Mayo 2003.

2.2. Riesgos de las Redes Inalámbricas

Varios son los riesgos derivables de las vulnerabilidades de las redes inalámbricas. Por ejemplo, se podría perpretar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un punto de acceso ilegal más potente que capte las estaciones cliente en vez del punto de acceso legítimo, interceptando la red inalámbrica. También sería posible crear interferencias y una más que posibilite la denegación de servicio con solo introducir un dispositivo que emita ondas de radio a una frecuencia de 2.4GHz (frecuencia utilizada por las redes inalámbricas).

Los puntos de acceso (AP) están expuestos a un ataque de Fuerza bruta para averiguar los passwords, por lo que una configuración incorrecta de los mismos facilitaría la irrupción de una red inalámbrica por parte de intrusos.

A pesar de los riesgos anteriormente expuestos, existen soluciones y mecanismos de seguridad para impedir que cualquiera con los materiales suficientes pueda introducirse en una red. Unos mecanismos son seguros, otros son fácilmente 'rompibles' por programas distribuidos gratuitamente por Internet.

Si a diario observamos los distintos pensamientos de los hackers que existen en el mundo contemporáneo, podemos deducir que en el ámbito de la seguridad para redes inalámbricas un hacker puede entrar a la WLAN de una compañía a través de un punto de acceso sin protección o a través de una estación de trabajo una vez que esté asociado con la red, va a ser difícil de detectar porque probablemente no sean visibles en o cerca del sitio de la red, además, un hacker inteligente no se arriesga, por ello utilizará los recursos de la compañía silenciosamente, y como resultado, es probable que nunca lo detecten".

Para protegerse, los negocios deben asegurarse que los empleados o los hackers no instalen puntos de acceso que no están autorizados en la red y que los puntos de acceso que sí lo están, estén configurados de manera segura. En ambientes densos, como las áreas urbanas o edificios de oficinas con múltiples locatarios, las compañías tienen que asegurarse de que los usuarios no se conecten a las redes de otras compañías.[5]

2.3. Ataques a Redes Inalámbricas

Los ataques a las redes inalámbricas se basan en las identificaciones estas, este es el método para detectar la existencia de un AP de una red inalámbrica. Para ello, se utiliza una WNIC (tarjeta de red inalámbrica) funcionando en modo promiscuo conjuntamente con un software que permite verificar la existencia de puntos de acceso.

En el momento en que se detecta la existencia de una red abierta, habitualmente se dibuja una marca en el suelo donde se anotan las características de la misma. Esto se conoce Wardriving y, una vez realizado, permite disponer de un autentico mapa donde se anotan todos los puntos de acceso con sus datos (SSID, WEP, direcciones MAC, etc.). Además del Wardriving existen otros ataques y herramientas para la realización de estos como es el caso del WarChalking y el AirSnort respectivamente.

[5] ALAPONT M, Vincent. Seguridad en Redes Inalámbricas: Trabajo Ampliación de Redes. Tesis, Universidad de Valencia España.

2.3.1 WarDriving

Es el método más conocido para detectar las redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como un ordenador portátil o un PDA. El método es realmente simple: el atacante simplemente pasea con el dispositivo móvil y en el momento en que detecta la existencia de la red, se realiza un análisis de la misma.

Para realizar el Wardriving se necesitan realmente pocos recursos, en la figura 2 tenemos los más habituales, como son un ordenador portátil con una tarjeta inalámbrica, un dispositivo GPS para ubicar el AP en un mapa y el software apropiado (AirSnort para Linux o NetStumbler para Windows).[6]

Figura 2 .WarDriving. [7]

[6] Roberto Enrique Sepúlveda y Antonio José Simancas, Seguridad en Redes de Área Local Inalámbrica, Estándar Seguridad IEEE 802.111, 2004.
[7] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág. 7, .Septiembre 2004.

2.3.2 WarChalking.

Este concepto se ha extendido rápidamente por los EEUU, Inglaterra y Dinamarca, aunque nadie, puede saber hasta donde ha llegado, dada la popularidad de los distintos foros en los que se esta promocionando este fenómeno, que ya tiene nombre propio, "Warchalking".

Un fenómeno, que, además, parte de un concepto totalmente colaborativo y en el que sus promotores dan a conocer sus hallazgos a otros interesados, para que estos mismos se beneficien del acceso.

Este ataque básicamente funciona así: Un pequeño ejército de internautas recorre las ciudades y las zonas de oficinas donde se presume que puedan existir redes WIFI. Equipados con portátiles y tarjetas inalámbricas, exploran las redes existentes e intentan encontrar aquellas que puedan ser usadas, por no contar con la protección debida, para el acceso a Internet.[8]

Seguidamente, se toma nota de la dirección (que entrará a formar parte de algunos de los listados que ya empiezan a circular) y se marca la casa con tiza, para advertir a otros "geekies" de las posibilidades de esta red y si esta, o no, protegida.

Como muestra del espíritu del "Warchalking", se adopto la idea de los símbolos de los vagabundos que viven por las calles de las ciudades y su hábito de marcar los domicilios que ofrecen algún tipo de caridad para recordarlos y comunicar al resto de la comunidad de las ventajas que pueden conseguir en esas casas.

[8] Roberto Enrique Sepúlveda y Antonio José Simancas, Seguridad en Redes de Área Local Inalámbrica, Estándar Seguridad IEEE 802.111, 2004.

Por lo que parece, la fiebre esta tomando tal envergadura, que responsables de seguridad informática, temen ver marcada su casa o empresa, lo que significaría un trabajo mal hecho y una puerta abierta para decenas de usuarios que con sus portátiles buscan redes "libres" para navegar por Internet.

Se trata de un lenguaje de símbolos utilizado para marcar sobre el terreno la existencia de las redes inalámbricas, de forma que puedan ser utilizadas por aquellos que 'pasen por allí. El lenguaje como tal es realmente simple:

Por ejemplo, el símbolo mostrado en la figura 3:

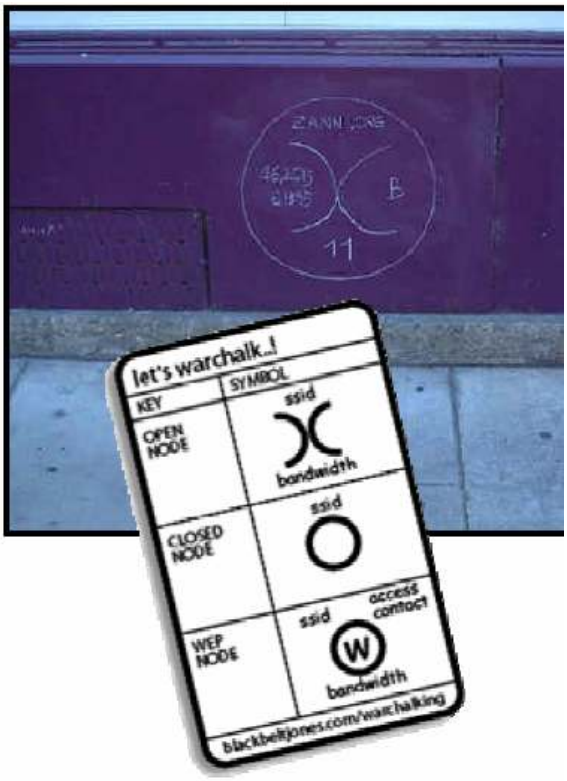

Figura 3. Ejemplo del Uso de Warchalking. [9]

[9] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág. 8, .Septiembre 2004

Esto significa: **“ Prueba)(”** Identifica a un nodo abierto, que utiliza el SSID "Prueba" y dispone de un ancho de banda de 11 Mbps.[10]

2.3.3 Hacking

Con frecuencia la señal Wi-Fi no se queda entre las cuatro paredes de la oficina, sino que puede ser detectada, utilizada y/o explotada por aquellos atacantes conocidos como hackers de redes inalámbricas (War Drivers) y hackers de señales inalámbricas (War Chalkers). Con la ayuda de un equipo sencillo y un software "rastreador" de los puntos de acceso inalámbrico que está listo para su descarga de Internet, estos individuos recorrerán ciudades y pueblos en busca de puntos inseguros de acceso inalámbrico.

Los hackers de redes inalámbricas tienen mucha práctica y han dedicado muchos sitios Web y carteleras de anuncios para mejorar sus actividades y compartir sus ideas. Los hackers de redes inalámbricas dedicados consiguen la ayuda del equipo más sofisticado, como antenas que ayudan a recoger las señales y receptores del Sistema de Posicionamiento Global (GPS), por ejemplo el mapa mostrado en la figura 4, los cuales utilizan para obtener las coordenadas exactas (longitud y latitud) de un punto de acceso inalámbrico detectado con fines de mapeo.[11]

[10] MADRID M, Juan M. Seguridad en redes inalámbricas 802.11. Tesis, Universidad ICESI, Valle del Cauca, Colombia, 2004.
[11] Roberto Enrique Sepúlveda y Antonio José Simancas, Seguridad en Redes de Área Local Inalámbrica, Estándar Seguridad IEEE 802.111, 2004.

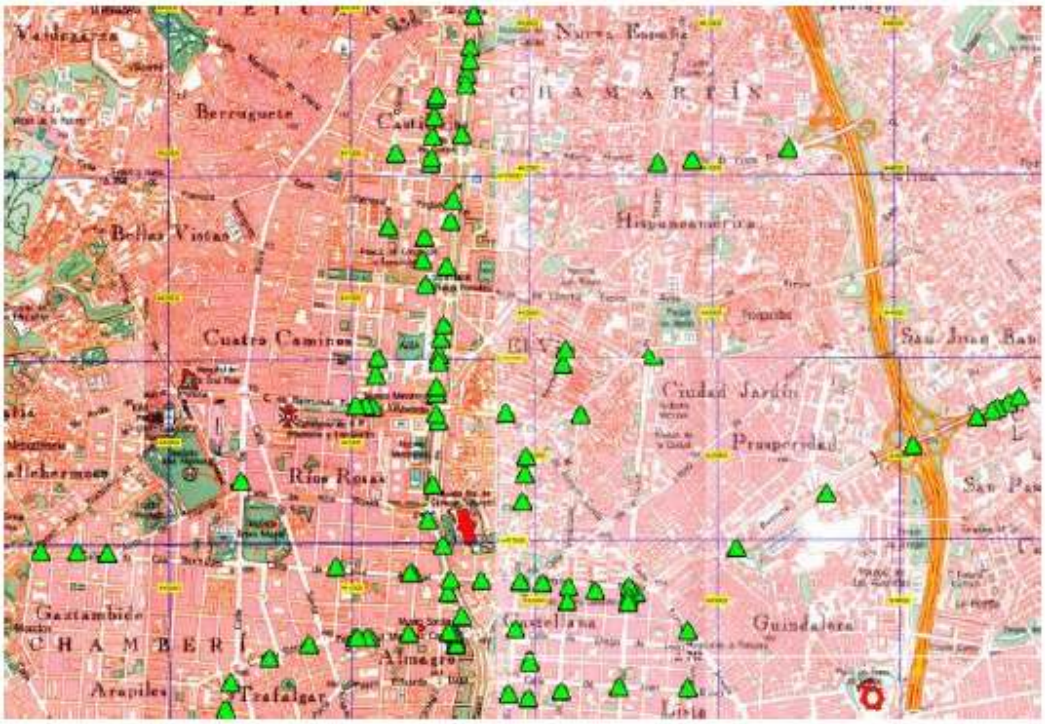

Figura 4. Mapeo por GPS. [12]

2.3.4 Técnicas de Intrusión

Algunas de las técnicas de intrusión mas comunes que afectan a una red de área local inalámbrica son:

2.3.4.1 Spoofing (burla) y Hijacking (secuestro)

El atacante falsifica información, ya sea un identificador de usuario o una contraseña permitidos por el sistema atacado. El funcionamiento de esta técnica, mostrada en la figura 5, se basa en redefinir la dirección física o MAC de nuestra tarjeta inalámbrica por una válida y se le asocia una dirección IP válida del sistema atacado.

[12] G. Álvarez / P.P. Pérez (CSIC), Seguridad en Wifi. Pag 27

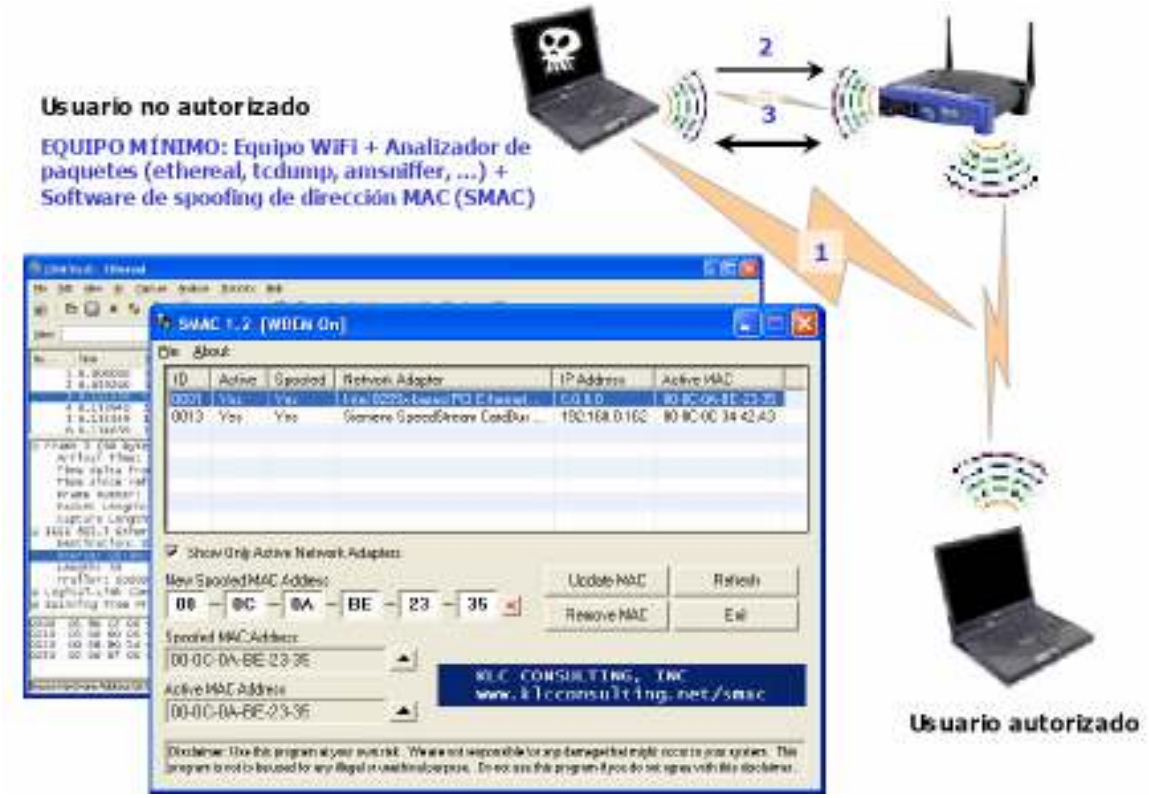

Figura 5. Intrusión tipo Spoofing. [13]

2.3.4.2 Sniffing y Eavesdropping (escuchas - interceptación)

El programa monitoriza los datos y determina hacia donde van, de donde vienen y qué son. Se utiliza una tarjeta de red que actúa en "modo adulterado".

[13] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág.26, .Septiembre 2004

2.3.4.3 Denegación de Servicio (DoS) o Ataques por Inundación

La denegación de servicio sucede cuando un atacante intenta ocupar la mayoría de los recursos disponibles de una red inalámbrica e Impide a los usuarios legítimos de esta, disponer de dichos servicios o recursos.

2.3.5 Otros Ataques

2.3.5.1 Espionaje (Surveillance)

Este ataque consiste simplemente en observar todo el entorno de la red inalámbrica, antenas, puntos de acceso, cables de red y todos los dispositivos conectados a la red, con el fin de recopilar información y combinar con otros tipos de ataques. Para la realización de este ataque no se necesita ningún tipo de “hardware” o “software” especial.

2.3.5.2 Interceptar una Señal

En este ataque el atacante intenta identificar el origen y el destino que posee la información, tras haber interceptado la señal, el atacante intentará recopilar información sensible del sistema.

2.3.5.3 Suplantar una Fuente Real

Esta técnica de ataque se engloba dentro de los ataques activos, donde un intruso pretende ser la fuente real u original.[14]

[14] HUERTAS GRAFIA, José Luís. Tecnologías de Red, “Seguridad en redes inalámbricas”.

2.4 Herramientas para Monitoreo de Redes Inalámbricas

En la Tabla 3. se encuentran citadas las mas comunes herramientas para la identificación y el monitoreo de las redes inalámbricas.

Herramienta	Descripciones
NetStumbler	Identificador de APs, escucha los SSID y manda señales buscando APs
Kismet	Sniffer y monitor de WLANs de forma pasiva monitorea el trafico inalámbrico, orden la información para identificar SSIDs, direcciones MAC, canales y velocidades de conexión.
Wellenreiter	Herramienta para descubrir WLANs, Usa la fuerza bruta para identificar APS de bajo tráfico, oculta su verdadera MAC y se integra con GPS.
THC-RUT	Herramienta para descubrir WLANs, Usa la fuerza bruta para identificar APS de bajo tráfico- Su primera herramienta en una red desconocida.
Ethereal	Analiza WLANs, permite surfear de forma interactiva la información capturada, observando información detallada de todo el tráfico inalámbrico.
WepCrack	Rompe la encriptación. Hace un crack de WEP utilizando las vulnerabilidades en la programación de RC4.
AirSnort	Rompe la encriptación, monitorea de forma pasiva las transmisiones, computando la llave de encriptación cuando se han capturado suficientes paquetes.
HostAP	Convierte una estación WLAN para funcionar como un AP.

Tabla 3. Herramientas Para El Monitoreo de Redes Inalámbricas. [15]

[15] ALAPONT M, Vincent. Seguridad en Redes Inalámbricas.

3. MECANISMOS DE SEGURIDAD

Antes de empezar a hablar de los métodos o mecanismos de seguridad básicos de una red inalámbrica debemos tener claro los componentes que la conforman tratando de establecer cuales pueden ser sus puntos críticos. De esta forma detallaremos cual puede ser el escenario básico de una red hasta los pasos iniciales de una conexión de tal forma que notemos la importancia que estos cumplen con respecto a la seguridad.

3.1 Escenario Básico

En una red inalámbrica podemos encontrar conectados estaciones móviles, como pueden ser Pcs, portátiles, PDAs (todos equipados con una tarjeta inalámbrica), puntos de acceso (AP), extensiones de redes LAN, antenas y cableado como podemos observar en la figura 6.

Los puntos de acceso actúan como un concentrador o hub que reciben y envían información vía radio a los dispositivos de clientes, que pueden ser de cualquier tipo, habitualmente, un PC o PDA con una tarjeta de red inalámbrica, con o sin antena, que se instala en uno de los slots libres o bien se enlazan a los puertos USB de los equipos.
La estructura básica de una red inalámbrica es denominada BSS (Basic Service Set), se puede decir que es la mínima estructura en la cual se pueden organizar un grupo estaciones móviles que se comunican entre si.

Figura 6. Escenario Básico. [16]

En la figura 7 tenemos dos BSS con dos estaciones cada una. Se puede decir que las BSS son el área de cobertura básica de una red.

3.2 Topologías de una WLAN

Se define como topología a la disposición lógica o a la disposición física de una red. Nos centraremos en la lógica, es decir, cómo se comunican los dispositivos.
Existen tres tipos de Topología WLAN:

- Ad-hoc
- Infraestructura
- Mesh

[16] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág.11, .Septiembre 2004

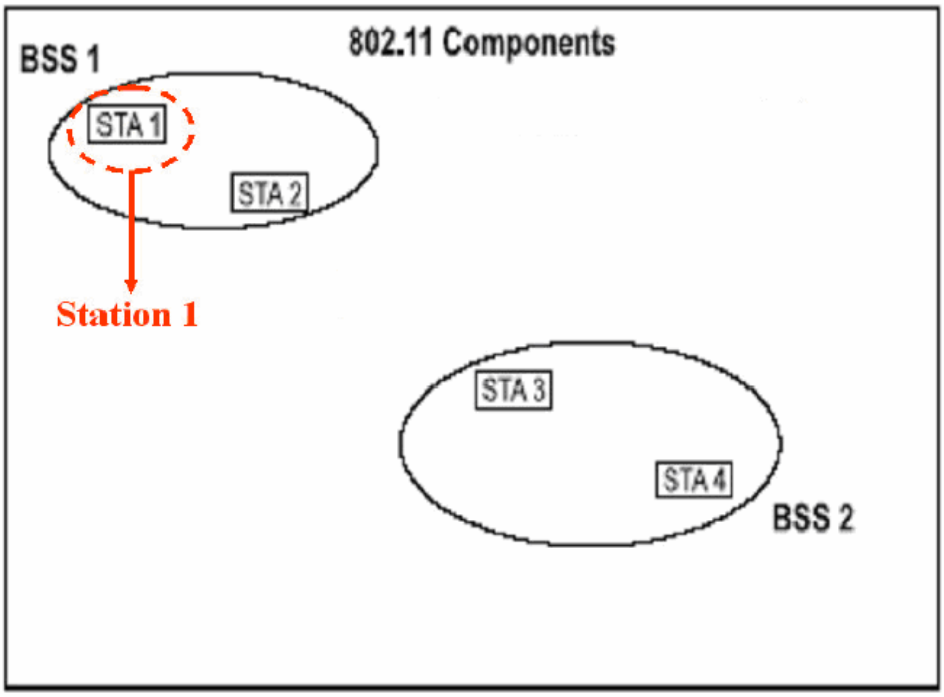

Figura 7. Ejemplo de BSS. [17]

¡3.2.1 Topología tipo Ad - hoc

Son redes formadas por un solo BSS, IBSS (Independent BSS) que no se estructuran alrededor de ninguna estación con funciones particulares, sino que distribuyen las tareas de coordinación entre sí.

Los dispositivos establecen enlaces punto a punto, como podemos observar en la figura 8, y se comunican a través de esos enlaces con dispositivos que se encuentren en su rango.

.

[17] Dr., Pablo I. Fierens, Introducción a las Redes Wifi, Centro Avanzado de Telecomunicaciones, Instituto Tecnológico de Buenos Aires.

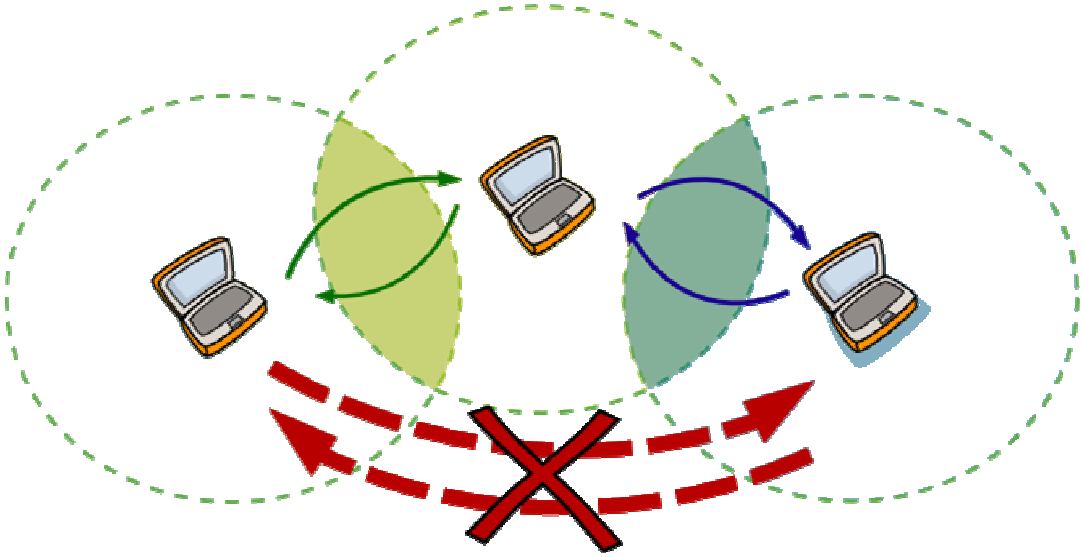

Figura 8. Topología Tipo Ad- hoc. [18]

3.2.2 Topología en Estructura

Un dispositivo se encarga de centralizar las comunicaciones: se denomina Punto de Acceso (AP o Access Point). En este caso, cada BSS está organizada alrededor de una estación (AP) que puede permitir el acceso a una red mayor, por ejemplo a una LAN cableada.

Los dispositivos cliente se conectan a los AP en lo que se denominan células, y pueden intercambiar información con dispositivos conectados a su mismo AP (siempre a través de éste). Por lo tanto, no tienen que encontrase en el rango de alcance para poder comunicarse.
Al ser una comunicación centralizada, si se cae el AP ninguno de los dispositivos podrá comunicarse entre sí. Nótese la figura 9.

[18] Javier de la Villa Regueiro, Estudio, Implantación y Configuración de una Red Inalámbrica Wi-Fi, Pág. 10.

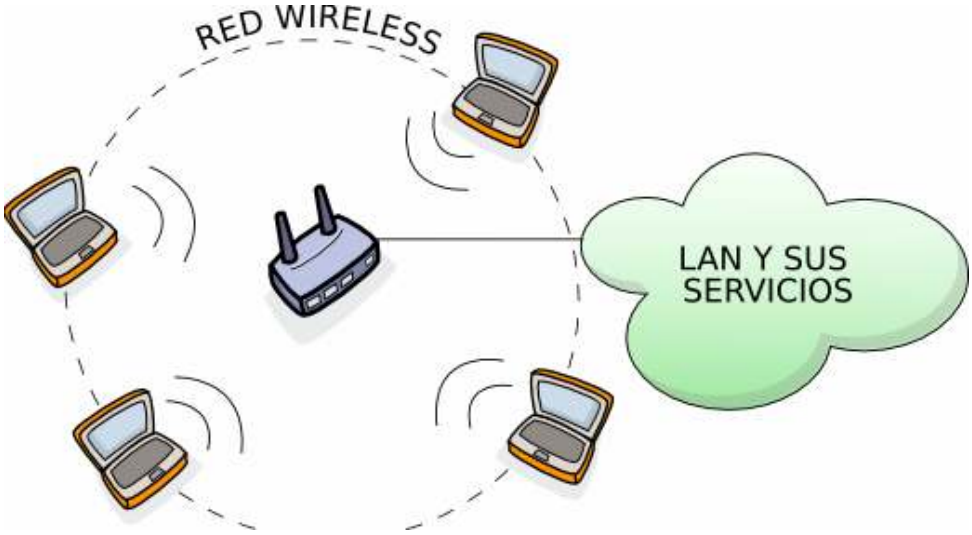

Figura 9. Topología en Estructura. [19]

3.2.3. Topología tipo Mesh

Es el siguiente paso en las topologías inalámbricas. Se descentraliza la comunicación y los dispositivos que intervienen en la comunicación pueden compartir "recursos". Si se cae un nodo, no afecta a toda la red. Ver figura 10.

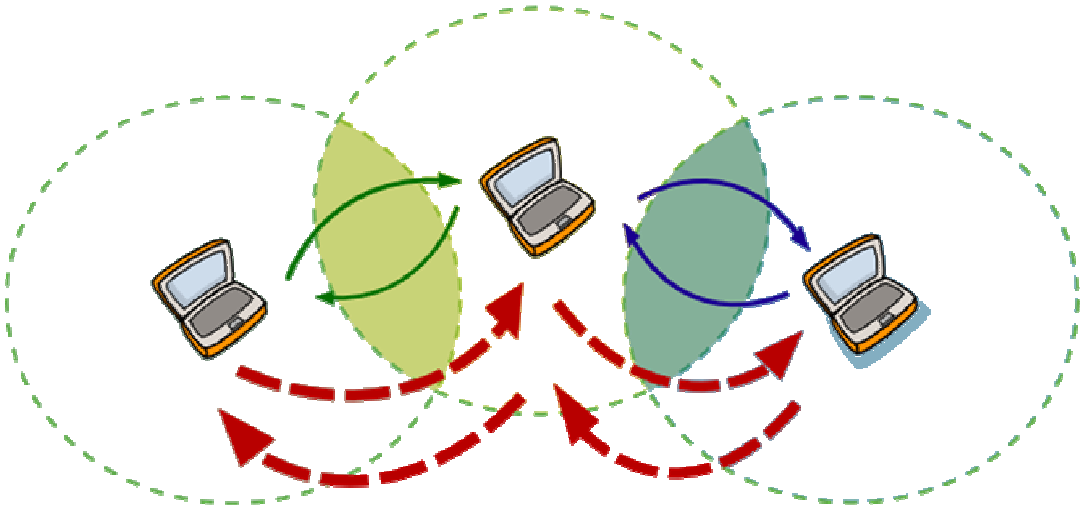

Figura 10. Topología Tipo Mesh. [20]

[19] Javier de la Villa Regueiro, Estudio, Implantación y Configuración de una Red Inalámbrica Wi-Fi, Pág. 11.

3.3 Fases de una Conexión Inalámbrica

Consta de 4 fases básicas que permiten la conexión de una estación cliente (STA) con un punto de acceso (AP):

1. El equipo móvil inalámbrico escanea el espectro en busca de actividad:

- Rastrea automáticamente todos los canales en busca de puntos de acceso disponibles.
- Envía peticiones y espera la recepción de anuncios por parte de los APs.

2. En el equipo móvil se muestra al usuario un resumen con las redes alcanzables por razones de cobertura.

- En cada red aparece, normalmente, solo el AP del que se recibe una mayor intensidad de señal.

3. El equipo móvil realiza una petición de autentificación contra el punto de acceso.

- Si esta fase termina adecuadamente el equipo está autenticado.

4. El equipo realiza la asociación con el punto de acceso.

- En este momento el equipo está asociado con el punto de acceso.
- A partir de ahora el equipo inalámbrico móvil puede comenzar la transferencia de datos:
  - Con otros equipos inalámbricos incluidos en el rango de cobertura del punto de acceso.
  - Con otros equipos incluidos en la parte cableada de la red. [21]

---

[20] Javier de la Villa Regueiro, Estudio, Implantación y Configuración de una Red Inalámbrica Wi-Fi, Pág. 15.
[21] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág.12, .Septiembre 2004

3.3.1. Fases 1 y 2: Rastreo de Frecuencias

Los APs, en su modo de funcionamiento por defecto, generan tramas de gestión (Beacon Frames), en las que envían el SSID (Service Set Identifier) de la red a la que pertenecen.

El equipo móvil escanea el espectro radioeléctrico de cada uno de los canales buscando actividad ya sea periódicamente (AP Beacon Frame) o en respuesta a una petición de los posibles clientes (Probe Request, Probe Response).

El SSID se utiliza para diferenciar entre distintas redes, es decir, bajo la cobertura de APs con el mismo SSID pertenecientes a la misma red (misma dirección IP, misma mascara, misma puerta de enlace, etc.), Wi - Fi soporta la itinerancia de los clientes. Un cliente que se conecte a través de uno de los APs de la red y obtenga por DHCP una dirección podrá desplazarse al rango de cobertura de otro AP de la misma red manteniendo la conectividad.

3.3.2. Proceso de Autentificación del Cliente

El cliente envía una petición de autentificación al AP elegido en la fase anterior. De acuerdo a los métodos implementados por los administradores de red se autenticará al cliente mediante alguno de los siguientes métodos:

- autentificación en base al SSID del cliente: El AP comprueba que el SSID que envía el cliente en sus tramas se corresponda con el suyo propio.
- Autentificación en base a la dirección MAC del cliente: El AP mantiene una lista de direcciones MAC admitidas.
- autentificación basada en retos mediante encriptación.

3.3.3. Asociación y Transferencia de Datos

El cliente inalámbrico, en caso de finalizar correctamente la fase anterior, se asocia con el punto de acceso. Desde este momento puede comenzar la transferencia de datos.

3.4. Medios de Transmisión

Teniendo claro como está conformada una red WI FI y sabiendo los pasos básicos de una conexión, nos damos cuenta que la mayoría de los problemas de seguridad en WLAN son debidos al medio de transmisión utilizado, el aire, que es de fácil acceso para los atacantes.

Por ello, hay que establecer unos medios para asegurar la privacidad de nuestros datos.

- Medios Físicos
- Medios Lógicos (SW)

3.4.1. Medios Físicos

Aunque es difícil delimitar el aire, podemos controlar los límites o el rango de alcance de nuestra red Wireless, aunque no siempre dispondremos de los medios adecuados y pueda ser costoso.

- Mediante el uso de antenas:
  - Forma de la onda (según el tipo de antena).
  - Potencia de emisión.
- Mediante Estructuras:
  - Paredes con materiales aislantes, o de un determinado grosor.

3.4.2. Medios Lógicos

Principalmente son técnicas de cifrado e integridad de la información y técnicas de Autenticación/ Autorización/ Accounting (AAA). Estos dos tipos de técnicas pueden complementarse.

3.4.2.1. Autenticación

La autenticación tiene como objetivo evitar el uso de la red por personas no autorizadas. Se pueden configurar los puntos de acceso de tal manera que utilicen contraseñas, conocidos como SSID (Service Set Identifier). LA autentificación no se lleva a cabo en la capa de aplicación sino en la capa física misma, lo cual significa que usuario que no este autenticado no podrá tener ningún tipo de acceso a la red.

3.4.2.2. Cifrado

Consiste en encriptar las transmisiones a través del canal de radio para evitar la captura de la información. Tiene como objetivo proporcionar a misma seguridad que un medio cableado.

Un cifrado o algoritmo es una formula que se usa para generar un flujo de datos cifrados basados en una clave de cifrado. Esta se pueden medir en términos de longitud y entre mayor sea, más complicado y robusto será.

Para crear un mensaje codificado se combina la clave de cifrado con el mensaje original. También se le puede agregar un vector de inicialización el cual varía constantemente evitando que se descifre la información cuando hallan repeticiones de datos.

3.5. Mecanismos de Seguridad

3.5.1 WEP (Wireless Equivalent Protocol)

El mecanismo de protección WEP es dotar a las comunicaciones inalámbricas del mismo nivel de seguridad de las que tienen las realizadas a través de una LAN Ethernet, es decir solo las personas con un punto de conexión a la red podrían escuchar el intercambio de datos.

Este sistema se basa en el algoritmo RC4 desarrollado por RSA Systems, lo cual se puede ver en la figura 11.; este sistema lo componen dos aspectos claves:

- Algoritmo de clave simétrica.

Las dos partes de la comunicación (emisor y receptor) comparten un secreto, una clave común, con la que encriptan / desencriptan las comunicaciones.

- Versiones con claves de 64 y 128 bits.

Figura 11. Estructura de WEP. [22]

[22] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág.15, .Septiembre 2004

Las características de WEP son:

- La WEP fija el mecanismo mediante el cual se autentica al grupo de usuarios al que se le permite acceder a la red, es decir no autentifica usuarios individuales y no autentifica a los puntos de acceso.
- WEP fija el mecanismo mediante el cual se encriptan/desencriptan los datos transportados en la trama MAC.

- WEP no fija ningún mecanismo de determinación ni distribución de claves, esto se hace manualmente con se ve en la figura 12.

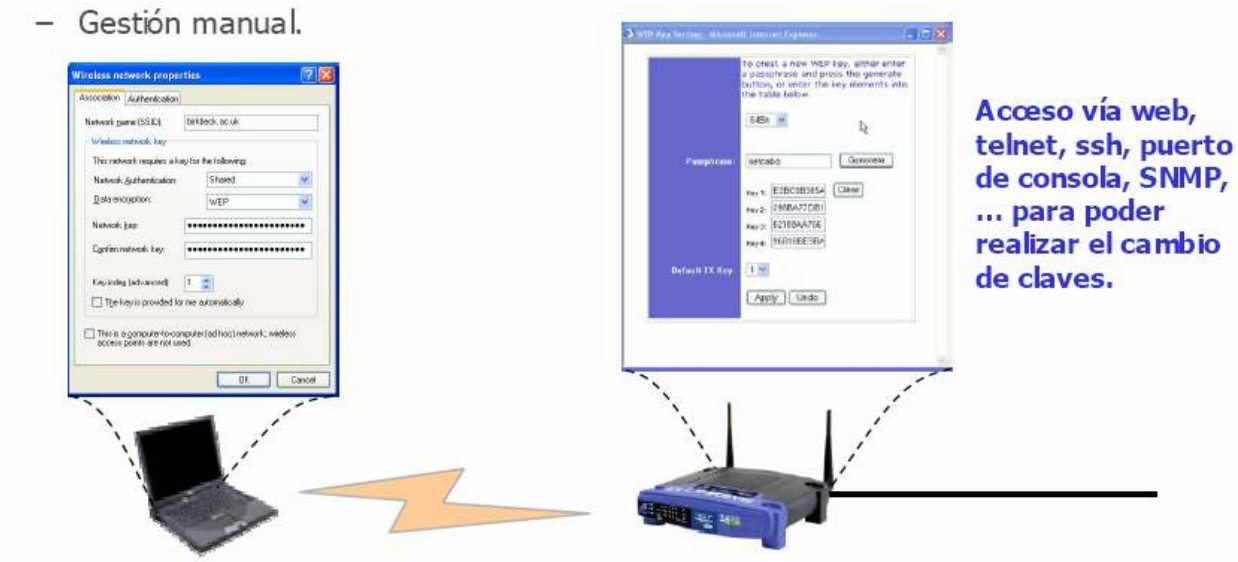

Figura 12. Distribución de Claves Manuales. [23]

[23] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág.16, .Septiembre 2004

3.5.1.1. Encriptación de Datos

1. Se calcula un campo de protección de la integridad del paquete (ICV) y se añade este al final de los datos.

2. Un vector de inicialización (IV) de 24 bits se concatena a la clave WEP.

3. El resultado del paso 2 (IV, clave WEP) se usa como entrada a un generador de números pseudoaleatorio que genera una secuencia de bits (PRNG) que es del mismo tamaño que el resultado del paso 1 (datos, ICV).

4. Se calcula PRNG XOR (datos, ICV) lo que da como resultado los datos encriptación que se van a enviar entre el AP y el cliente inalámbrico.

5. Se introduce en la carga de datos de la trama MAC la concatenación de IV y el encriptación de (datos, ICV).

Todo esto proceso entre el paso 1 y 4 lo podemos encontrar en la figura 13.

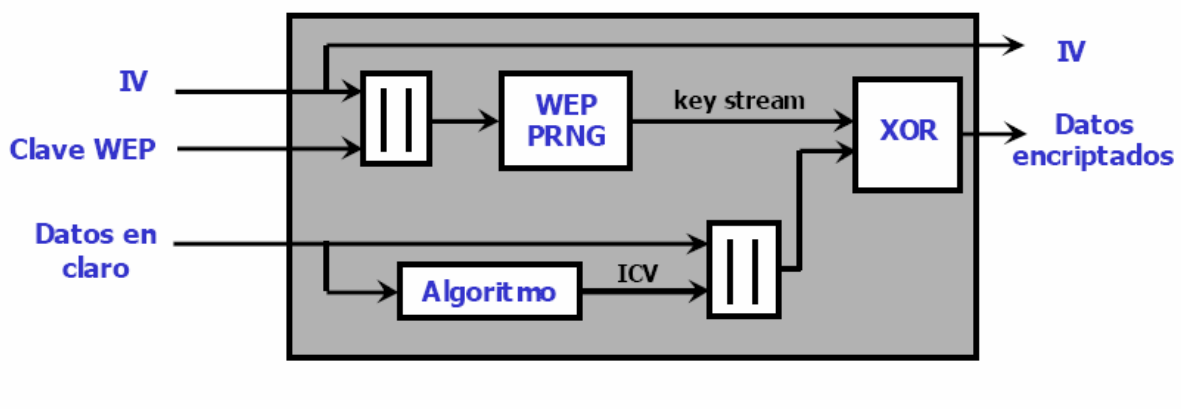

Figura 13. Proceso WEP de Encriptación de Datos. [24]

[24] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág.17, .Septiembre 2004

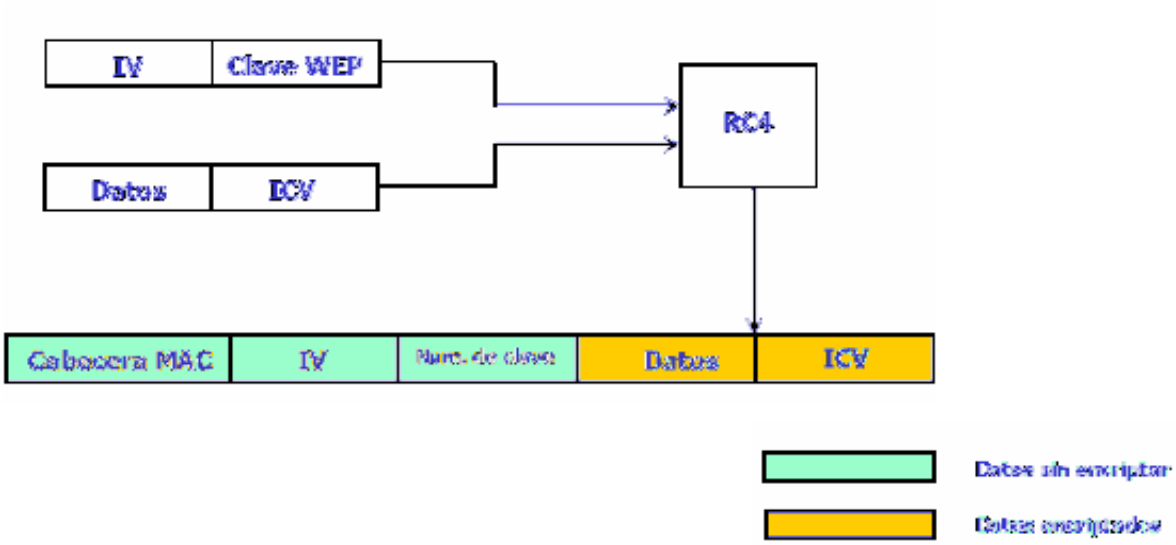

Figura 14. Trama MAC Encriptada con WEP. [25]

Mientras que los pasos 4 y 5 son detallados en la figura 14.

3.5.1.2 Desencriptado de Datos WEP

Como observamos en la figura 15:

1. Se extrae el vector de inicialización (IV) de la trama MAC; viaja en claro.

2. Se concatena este vector con la clave WEP.

3. Se introduce el resultado de la fase 2 en el mismo generador de números pseudoaleatorio que genera la misma secuencia de bits que en el emisor.

4. Se calcula el XOR del resultado de la fase 3 con la parte de la trama MAC en la que viaja la encriptación (datos, ICV). El resultado de esta fase es la concatenación de (datos, ICV) en claro.

[25] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág.18, .Septiembre 2004

5. Se calcula con el mismo algoritmo que en el emisor el campo ICV a partir de los datos y se comprueba se concuerda con el campo ICV que contenía la trama recibida.

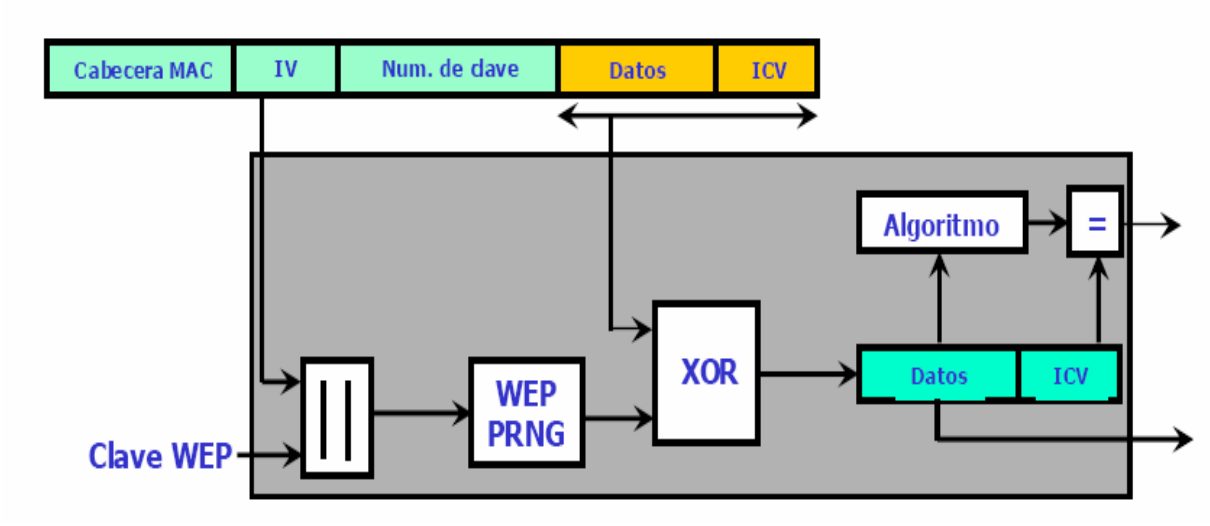

Figura 15. Proceso Desencriptado de Datos WEP. [26]

3.5.1.3. Mecanismo de Autentificación de Usuario WEP

La figura 16 describe el proceso de autentificación de usuario WEP entre un computador y su antena Wi Fi.

[26] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág.19, .Septiembre 2004.

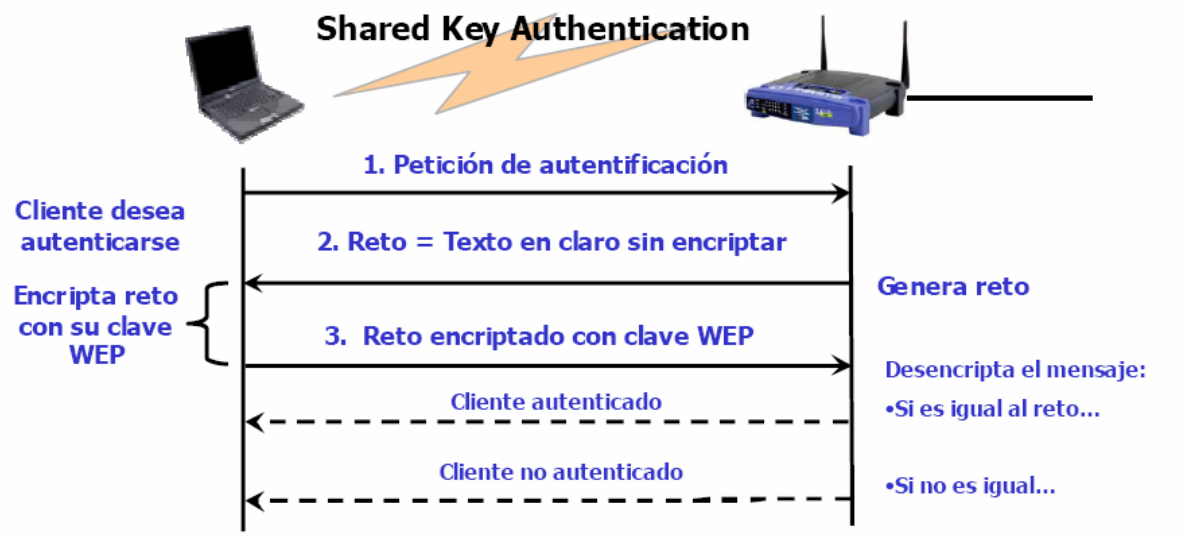

Figura 16. Mecanismo de Autentificación de Usuario WEP. [27]

3.5.2. WPA (WI FI Protected Access)

Es un subconjunto de medidas del estándar 802.11i (No es una solución propietaria con lo que garantizamos la interoperabilidad.) Esta diseñado para que todos los equipos Wi Fi vendidos puedan ajustarse a sus requerimientos tras una actualización de software o de firmware.

Nuevas funcionalidades:

- Implementa mecanismos de autentificación mutua: **IEEE 802.1x**.
- Utiliza nuevos algoritmos sobre **RC4** que sustituyen a WEP: **TKIP** (Temporal Key Integrity Protocol).
- Utiliza nuevos mecanismos para garantizar la integridad de los mensajes: **Michael Message Integrity Check.**

[27] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág. 20, .Septiembre 2004

Define 3 tipos de entidades:

– Solicitante.

– Autentificador.

– Servidor de autentificación.

En la figura 17 se observan los tres tipos de identidades y su función.

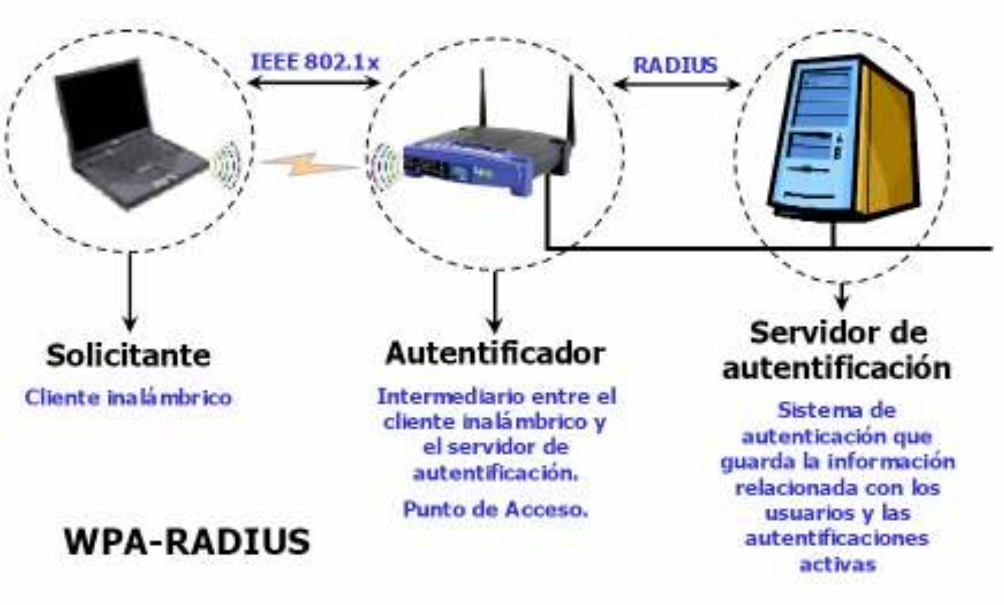

Figura 17. Escenario Básico de WPA. [28]

3.5.2.1. Proceso de Autentificación

1. El solicitante, un cliente inalámbrico que quiere ser autenticado, envía una petición al autentificador.

2. El autentificador, punto de acceso, habilita un puerto para el solicitante:

[28] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág. 32, .Septiembre 2004.

Por este puerto solo pueden viajar mensajes de autentificación en tramas de gestión. El resto del tráfico se filtra **(DHCP, HTTP, FTP, SNMP, POP3).**

3. El autentificador pide la identidad al solicitante mediante el protocolo **EAPOL (EAP encapsulation over LANs).**

4. El solicitante envía su identidad al autentificador.

5. El punto de acceso envía la identidad del cliente al servidor de autentificación mediante **EAP (Extensible Authentication Protocol).**

6. El cliente y el servidor de autentificación establecen un diálogo mediante el protocolo EAP:

Finalizado este diálogo, el solicitante y el servidor de autentificación comparten una clave de sesión que nunca ha viajado por la red.

7. El servidor de autentificación envía la clave de sesión al autentificador mediante el protocolo **RADIUS**.

8. El punto de acceso habilita el puerto para la dirección MAC del dispositivo solicitante y adicionalmente establece una clave de encriptación con el solicitante.

En la figura 18 podemos observar las peticiones para el proceso de autentificación, mientras que en la figura 19 se nota como actúa el camino antes y después de la autentificación.

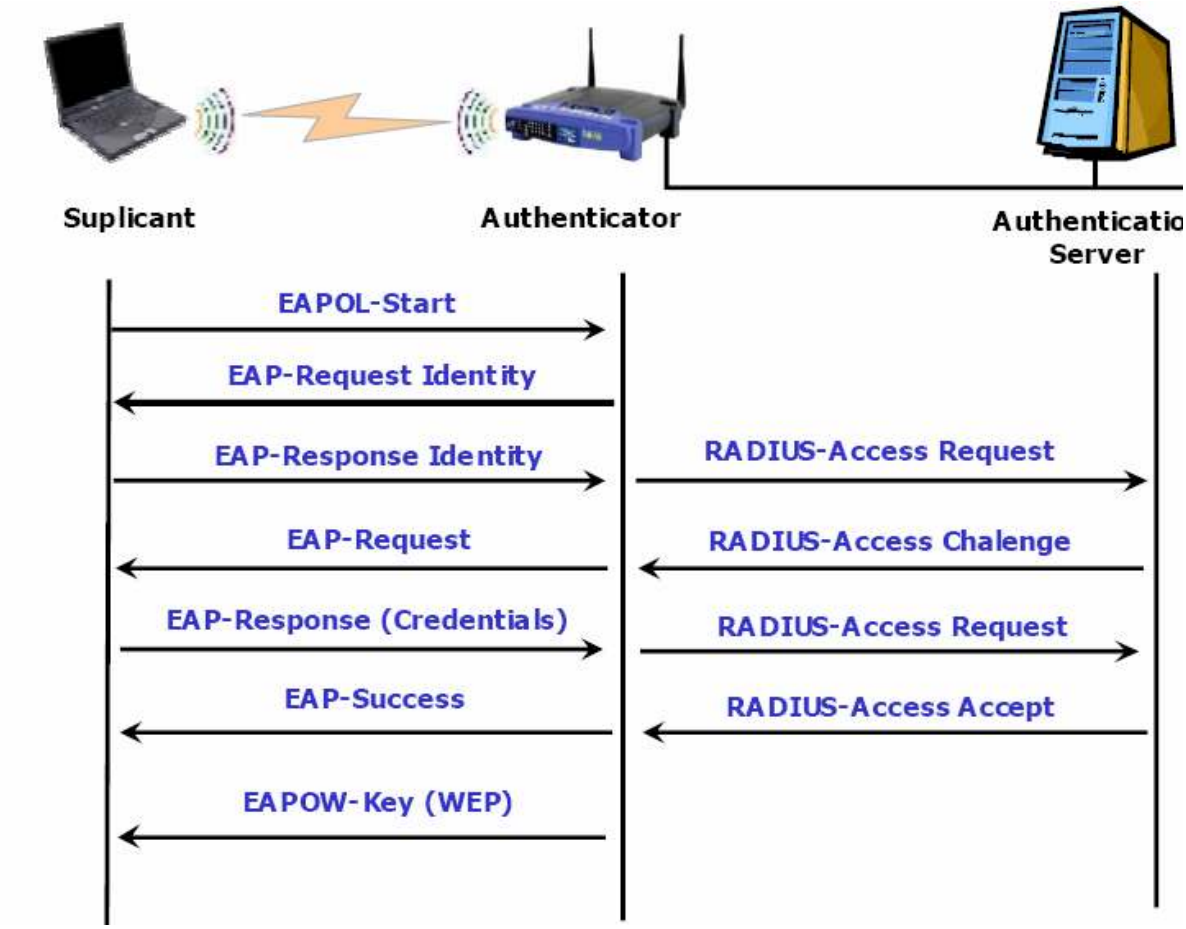

Figura 18. Proceso de Autentificación WPA. [29]

[29] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág. 33, .Septiembre 2004.

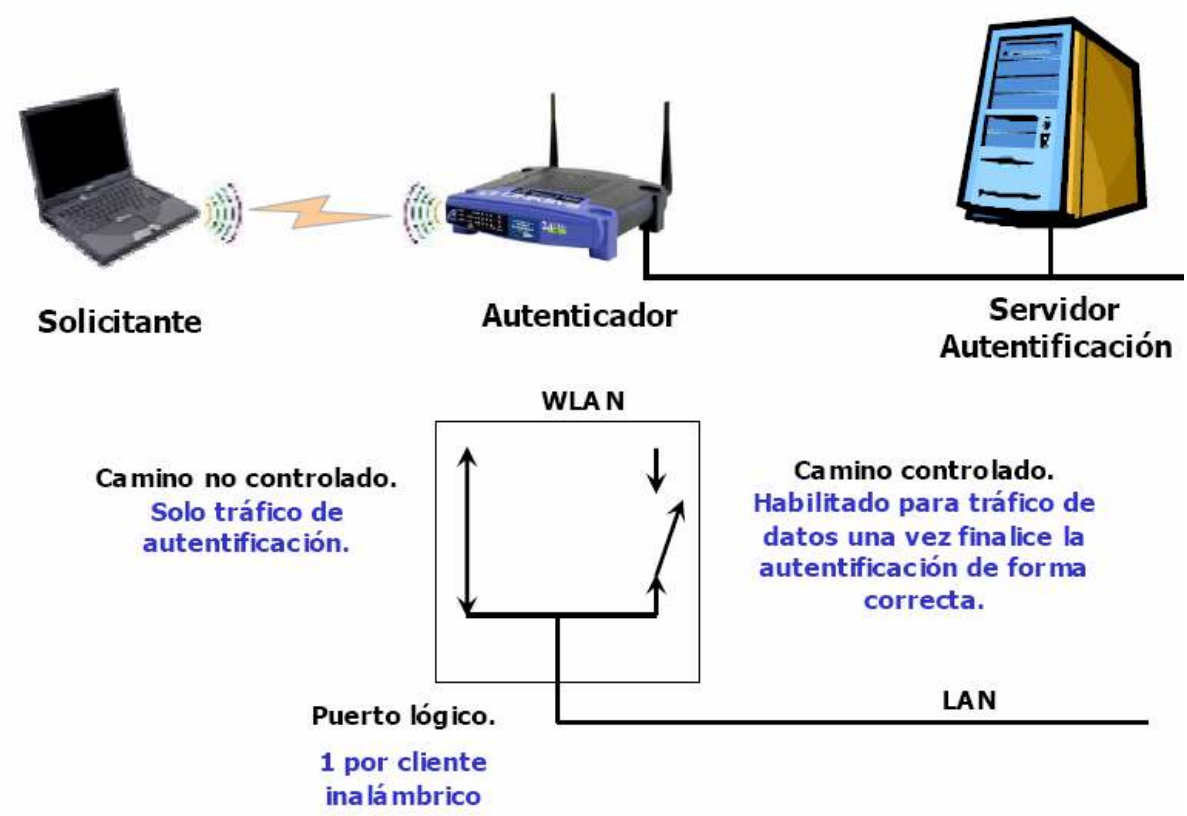

Figura 19. Puertos Controlados y no Controlados. [30]

3.5.3. TKIP (Temporal Key Integrity Protocol)

Se basa en el algoritmo **RC4** pero:

- Con vector de inicialización **(IV)** de 48 bits.
- Claves distintas y dinámicas para cada usuario.
- Una clave diferente para cada paquete enviado.

[30] S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", Agosto de 2001.

Tiene dos tipos de claves:

Unicast:

Pairwise Master Key (PMK):

- Acordada por el solicitante y el servidor.

Pairwise Transient Key (PTK):

- Derivada de la PMK mediante mezclado con las direcciones MAC de solicitante y autentificador.
- **Temporal Key (TK).** Para encriptar los mensajes de datos.

Broadcast:

Groupwise Master Key (GMK):

- Para poder enviar mensajes multidestino.
- Distribuida desde el AP (autentificador) a los clientes (solicitante).
- Cada AP puede tener una diferente.

Tiene una distribución de claves mediante **4-way handshake** y **group key handshake.**[31]

3.5.4. Clave única por paquete (PPK)

La clave se modifica con el envío de cada paquete:

a) La clave inicial, particularizada para cada cliente con su dirección MAC, se mezcla con el vector IV:

- se modifica con cada envío. **(PPK. Perpacket Keying)**
- está relacionado con el número de secuencia del paquete.

[31] S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", agosto de 2001.

b) Para evitar la posibilidad de colisión de dos paquetes, uno desde el AP y otro desde el cliente IV, encriptados con la misma clave y el mismo vector de inicialización como se puede observar en la figura 20:

- Cliente numeración impar.
- AP numeración par.

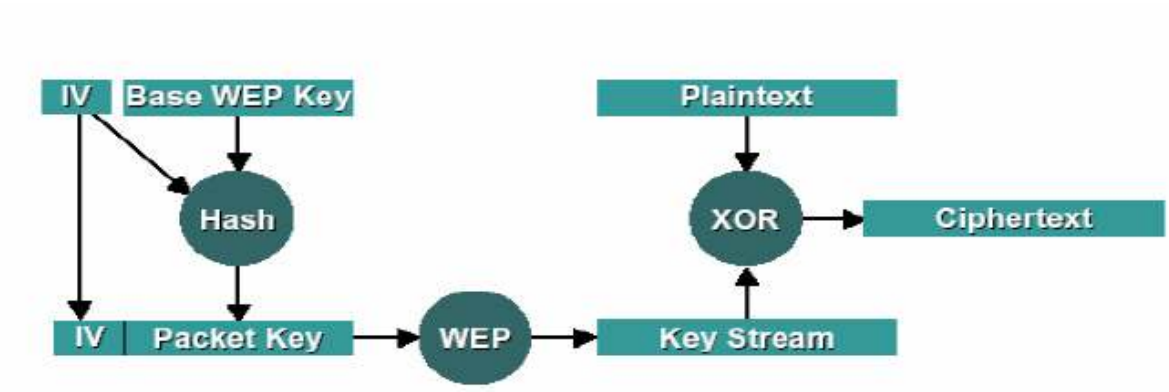

Figura 20. Modelo de Clave Única por Paquete. [32]

3.5.5. WPA-PSK (Pre Shared Key)

Para entornos en los que no hay disponible un servidor de autentificación y en los que no es necesario llegar al mismo nivel de seguridad que en las comunicaciones corporativas:

- accesos en hogares.
- accesos en pequeñas oficinas.

[32] Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi, Pág.37, .Septiembre 2004

Se basa en una clave compartida por todos los equipos involucrados en la comunicación (clientes y APs):

- Pre-shared key, password o master key.
- la gestión de esta clave es manual en todos los equipos.
- no hay un mecanismo estándar para modificar esta clave secreta compartida.
- TKIP + PPK + gestión de claves.

Funcionamiento:

1. Del secreto compartido, mediante un proceso matemático, se deriva una clave primaria **PMK**.

2. A partir de aquí el funcionamiento de TKIP es el mismo.

Pasar de **WEP** a **WPA-PSK** supone simplemente actualizar el firmware, activar **WPA-PSK** e introducir la clave maestra en todos los equipos.

3.5.6. WPA 2 (WI FI Protected Access 2)

-Nuevo estándar de seguridad para redes inalámbricas. Posiblemente no sea compatible con el equipamiento antiguo:

- No es suficiente con una actualización de firmware.
- Investimiento en nuevos equipos:
  - Más potencia de cálculo: requiere coprocesador.
  - Modos duales:
    - **WPA/WEP.**
    - **WPA2/WPA.**

-Soporte para itinerancia rápida:

- Usuario pre-autenticado contra todos los puntos de acceso cercanos no solo con el que esta asociado.

- Encriptación AES (Advanced Encryption System):

- Algoritmo de **Rijndael**.
- Sustituye a **DES** y **3DES**, típicos en la encriptación de VPNs y las comunicaciones bancarias.
- Aprobado por el **NIST (National Institute of Standars).**
- Resistente a todos los ataques de criptoanálisis conocidos.

- Publicado a finales del 2004.

- Primeros equipos ratificados por Wi Fi Alliance 2-9-2004.

De este mecanismo hablaremos detalladamente en el siguiente capitulo.

4. WPA2 (WI-FI PROTECTED ACCESS 2)

El Standard IEEE 802.11i reemplaza formalmente la privacidad equivalente por cable (WEP, Wired Equivalent Privacy) del standard IEEE 802.11 original por un modo específico del Estándar de cifrado avanzado (AES, Advanced Encryption Standard), conocido como Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) Protocol (CCMP). CCMP proporciona confidencialidad (cifrado) e integridad a los datos. En este capítulo se describen los detalles de la implementación de WPA2 de AES CCMP para el cifrado, el descifrado y la validación de la integridad de los datos de las tramas inalámbricas 802.11.

El estándar original **IEEE 802.11** proporcionó el siguiente sistema de características de seguridad para redes LAN Inalámbricas:

- Dos métodos diferentes de autentificación: Sistema abierto (Open System) y llave compartida (Shared Key).
- El algoritmo de encriptación WEP (Privacidad Equivalente al Cableado).
- Un valor de chequeo de integridad (ICV), cifrado con WEP, que proporcionó integridad a los datos.

Con el tiempo, estas características de seguridad demostraron ser escasas para proteger la comunicación de redes LAN Inalámbricas en escenarios comunes. Para tratar las aplicaciones de seguridad del estándar original IEEE 802.11, las siguientes tecnologías adicionales son utilizadas:

- El estándar IEEE 802.1X de control de acceso a la red Port-Based: un método opcional para autenticación clientes inalámbricos 802.11. IEEE 802.1X proporciona por usuario, identificación y autentificación, métodos extendidos de autentificación, y dependiendo del método de autentificación y de la gestión-dinámica del cifrado, determinación de clave por estación o por sesión y recifrado.

- El acceso protegido Wi-Fi (WPA) es un estándar transitorio adoptado por la **Wi-Fi Alliance** para proporcionar una integridad más segura del cifrado y de datos mientras que el estándar de IEEE 802.11i era ratificado. WPA soporta autentificación a través de 802.1X (conocido como WPA Enterprise) o con una clave precompartida (conocida como WPA Personal), un nuevo algoritmo de cifrado conocido como protocolo de integridad de clave temporal (TKIP), y un nuevo algoritmo de integridad conocido como Michael. WPA es un subconjunto de la especificación 802.11i.[33]

El estándar de IEEE 802.11i substituye formalmente la privacidad equivalente al cableado (WEP) y las otras características de seguridad del estándar original IEEE 802.11. WPA2 es una certificación de producto disponible con la alianza Wi-Fi que certifica a los equipos inalámbricos como compatibles con el estándar 802.11i. La meta de la certificación WPA2 es apoyar las características de seguridad obligatorias adicionales del estándar 802.11i que ya no son incluidas para los productos que soportan WPA. Como WPA, WPA2 ofrece ambos modos de operación, Enterprise y Personal.

Microsoft lanzó la actualización de los elementos de información de servicios del aprovisionamiento inalámbrico (WPS IE) / Acceso Protegido W i- Fi 2 (WPA2) para Windows XP con Service Pack 2, una transferencia que pone al día los componentes del cliente inalámbrico en Windows XP con Service Pack 2 para soportar WPA2, el cual describe las características de la seguridad WPA2 y la ayuda para WPA2 incluido con la actualización del WPA2/WPS IE para Windows XP con Service Pack 2. Más adelante comentaremos sobre esta actualización.

[33] Wi-Fi Protected Access 2 (WPA2) Overview, The Cable Guy, Mayo 2005.

4.1. Características de La Seguridad WPA2

Las siguientes características de WPA2 se apoyan en la actualización WPA2/WPS IE para Windows XP con Service Pack 2:

4.1.1. Autentificación de WPA2

Para WPA2 Enterprise, WPA2 requiere la autentificación en dos fases; la primera es una autentificación en sistema abierto y la segunda utiliza 802.1X y un método de autentificación del Protocolo de Autentificación Extensible (EAP). Para ambientes sin una infraestructura RADIUS (Remote Authentication Dial-In User Service) como por ejemplo redes pequeñas de oficina/hogar (SOHO small office/home office), WPA2 personal utiliza una clave inicial compartida (PSK).

4.1.2. Manejo de Clave WPA2

Como WPA, WPA2 requiere la determinación de una clave maestra de par (PMK Mutual Pairwise Master Key) basada en los procesos de autentificación de EAP o de PSK y el cálculo de claves transitorias a través de un proceso de negociación de 4 vías.

4.1.3. Estándar de Cifrado Avanzado

WPA2 requiere la ayuda del estándar de Cifrado Avanzado (AES) que usa el Modo Contador- Encadenamiento de Bloques Cifrados(CBC) - el protocolo de código de autentificación de mensaje (MAC) (CCMP). El Modo Contador de AES es un codificador de bloque que cifra bloques de datos de 128 bits a la vez con una clave de cifrado de 128 bits. El algoritmo CBC-MAC produce un Código de Integridad de Mensaje (MIC) que proporciona la autentificación de origen de datos y la integridad

de datos para tramas inalámbricas. Un campo de número de paquetes incluido en la trama protegida inalámbrica de WPA2 e incorporado en el cifrado y en los cálculos del MIC proporciona una protección contra los replays (mensajes repetidos). El cifrado AES resuelve el requisito del Estándar de Procesamiento de Información Federal (FIPS) 140-2.

4.2. Características Adicionales de WPA2 para Fast Roaming

Cuando un cliente inalámbrico autentica con 802.1X, hay una serie de mensajes enviados entre el cliente y el punto de acceso (AP) para intercambiar identificaciones. Este intercambio del mensaje introduce un retraso en el proceso de conexión. Cuando un cliente inalámbrico hace roaming de un AP a otro, el retraso para realizar la autentificación 802.1X puede causar interrupciones sensibles en la conexión de la red, especialmente para el tráfico time-dependent como es la voz o secuencias de datos video-based. Para reducir al mínimo el retraso asociado con el roaming a otro AP, el equipo WPA2 puede soportar opcionalmente el PMK y la preautenticación.

4.2.1. Captura de PMK

Mientras que un cliente inalámbrico hace roaming de un radio AP a otro, debe realizar una autentificación completa 802.1X con cada AP inalámbrico. WPA2 permite que el cliente inalámbrico y el AP inalámbrico depositen los resultados de una autentificación completa 802.1X de modo que si un cliente escanea de nuevo a un AP inalámbrico con el cual ha autenticado previamente, el cliente inalámbrico solamente necesita realizar el proceso de negociación de 4 vías (4 ways handshake) y determinar nuevas claves transitorias en pares (PMK). En la trama de petición de asociación, el cliente inalámbrico incluye un identificador de PMK que fue determinado durante la autentificación inicial y almacenado con ambos, el cliente inalámbrico y las tablas de PMK de los AP inalámbricos. Las PMK se almacenan por

una cantidad de tiempo, según lo configurado en el cliente inalámbrico y el AP inalámbrico.

Para hacer la transición más rápida para las infraestructuras de redes inalámbricas de una red que utilizan un switch que actúe como el autentificador 802.1X, la actualización de WPA2/WPS IE para Windows XP con Service Pack 2 calcula el valor del identificador de PMK para poder reutilizarlo de acuerdo a lo determinado por la autentificación 802.1X con el switch, cuando se haga roaming entre el APs inalámbricos que se une al mismo switch. Esta práctica se conoce como captura oportuna de PMK. [34]

4.2.2. Preautenticación

Con la preautenticación, un cliente inalámbrico WPA2 puede realizar opcionalmente las autentificaciones 802.1X con el otro APs inalámbricos dentro de su rango, mientras que es conectado a su radio actual AP. El cliente inalámbrico envía tráfico de preautenticación al AP adicional sobre su conexión inalámbrica existente. Después de la preautenticación con un AP inalámbrico y de almacenar el PMK y su información asociada en la cache PMK, un cliente inalámbrico que se conecta con un AP inalámbrico con el cual haya preautenticado necesita realizar solamente el 4 way handsake.

Los clientes WPA2 que soportan la preautenticación pueden solamente preautentificar con el APs sin inalámbricos que anuncia su capacidad de preautenticación en tramas de respuesta de prueba.

[34] Wi-Fi Protected Access 2 (WPA2) Overview, The Cable Guy, Mayo 2005.

4.3. Soporte de una Mezcla Clientes Inalámbricos de WPA2, de WPA, y de WEP

El equipo inalámbrico certificado de WPA2 es también compatible con WPA y WEP. Se puede tener una mezcla o dispositivos inalámbricos de WPA2, de WPA, y de WEP funcionando en el mismo ambiente.

4.4. Cambios Requeridos para Soportar WPA2

WPA2 requiere cambios en los siguientes:

- APs Inalámbricos.
- Adaptadores Inalámbricos de Red.
- Software del Cliente Inalámbrico.

4.4.1. Cambios a Los APs Inalámbricos

Con WPA, los dispositivos de red podrían mejorarse a través de una actualización del firmware ya que las características de seguridad de WPA adquirieron las habilidades de cómputo existentes diseñadas para WEP. Con WPA2, sin embargo, un AP inalámbrico que no tenga estas habilidades de cómputo para realizar los cálculos más complejos para AES CCMP no pueden ser actualizados a través de un los firmware y debe ser sustituido. Estos tipos de APs inalámbricos son típicamente APs viejos fabricados antes de la inclusión de la ayuda para el estándar 802.11g.
Nuevos APs, tales como los que soportan el estándar 802.11g, pueden ser actualizados con un firmware.
Comprobando con tu documentación de venta del AP inalámbrico o a través del Web Site se puede determinar si los APs inalámbrico requieren reemplazo o una actualización del firmware para soportar WPA2. Si solamente necesita una actualización del firmware, se puede obtener la actualización del fabricante del AP inalámbrico e instalarla.

4.4.2. Cambios a Los Adaptadores Inalámbricos de La Red

Como en los APs inalámbricos, su sustitución depende si tienen la capacidad de cómputo necesaria para realizar AES CCMP. Hay que comprobar con la documentación del fabricante del adaptador o con el Web Site para determinar si requieren el reemplazo o un nuevo firmware que soporte WPA2.
Si solamente una actualización del firmware es necesaria, hay que obtener la actualización por parte del fabricante e instalarla en el adaptador inalámbrico de red.
Para los clientes inalámbricos que funcionan con Windows XP con Service Pack 2, deben obtener un driver de adaptador de red actualizado que soporte WPA2. El driver actualizado del adaptador de red debe poder pasar las capacidades del adaptador WPA2 a la autoconfiguración inalámbrica de Windows XP.

4.4.3. Cambios a Los Programas Inalámbricos del Cliente

El software inalámbrico del cliente se debe poner al día para tener en cuenta la configuración de las opciones de la autentificación WPA2. La actualización de WPA2/WPS IE para Windows XP con Service Pack 2 incluye la ayuda para WPA2 y modifica lo siguiente:

- Una caja de diálogo **Escoger una red inalámbrica**.
- La pestaña de Asociación para las propiedades de una red inalámbrica.

Cuando se está conectado a una red inalámbrica de WPA2, el tipo de red es mostrada como WPA2 en una caja de diálogo Escoger una red inalámbrica. La figura 21 muestra un ejemplo.

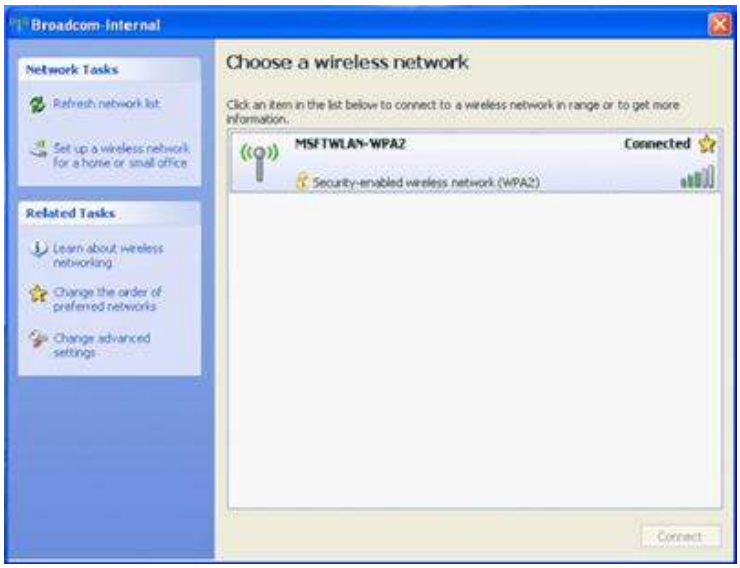

Figura 21. Ventana de Dialogo Escoger una Red Inalámbrica. [35]

En la pestaña de asociación para las propiedades de una red inalámbrica, la caja drop-down de la autentificación de red tiene las opciones adicionales:
WPA2 (para WPA2 Enterprise) y WPA2-PSK (para WPA2 personal). Estas opciones estarán presentes solamente si el adaptador inalámbrico de la red y su driver soporten WPA2. La figura 22 nos muestra un ejemplo:

[35] Wi-Fi Protected Access 2 (WPA2) Overview, The Cable Guy, Mayo 2005.

Figura 22.Ejemplo de como escoger entre WPA2 Personal y WPA2 Enterprise. [36]

Las políticas de red inalámbricas (IEEE 802.11) para Windows Server 2003 con SP1 no soporta la configuración de los ajustes de autentificación WPA2.

4.5. Características Criptográficas de WPA2

La WEP del estándar IEEE 802.11 original tenía puntos débiles criptográficos. La tabla 4 muestra la manera en que WPA2 aborda esos puntos débiles.

Punto débil de WEP	Cómo WPA2 aborda el punto débil
Vector de inicialización (IV) demasiado corto	En AES CCMP, se reemplazó el IV por un campo Número de paquete y se duplicó su tamaño a 48 bits.

[36] Wi-Fi Protected Access 2 (WPA2) Overview, The Cable Guy, Mayo 2005.

Punto débil de WEP	Cómo WPA2 aborda el punto débil
Integridad débil de los datos	El cálculo de suma de comprobación cifrado con WEP se reemplazó por el algoritmo AES CBC-MAC, que está diseñado para proporcionar una sólida integridad de los datos. El algoritmo CBC-MAC calcula un valor de 128 bits y WPA2 utiliza los 64 bits de orden superior como un código de integridad de mensaje (MIC). WPA2 cifra el MIC con el cifrado de modo contador de AES.
Usa la clave principal en lugar de una clave derivada	Al igual que WPA y el Protocolo de integridad de claves temporales (TKIP, Temporal Key Integrity Protocol), AES CCMP usa un conjunto de claves temporales derivadas de una clave principal y otros valores. La clave principal se origina en el proceso de autenticación 802.1X mediante Protocolo de autenticación extensible-Seguridad de la capa de transporte (EAP-TLS) o EAP protegido (PEAP).
No reasigna claves	AES CCMP reasigna claves automáticamente para crear nuevos conjuntos de claves temporales.
No ofrece protección contra la reproducción	AES CCMP usa el campo Número de paquete como contador para ofrecer protección contra la reproducción.

Tabla 4. Como aborda WPA2 los Puntos Débiles de WEP. [37]

[37] Cifrado e integridad de los datos en Wi-Fi Protected Access, The Cable Guy, Agosto 2005.

4.6. Claves Temporales de WPA2

A diferencia de WEP, que utiliza una única clave para el cifrado de datos de difusión única y generalmente una clave separada para el cifrado de datos de difusión y de multidifusión, WPA2 usa un conjunto de cuatro claves diferentes para cada par de clientes inalámbricos-AP inalámbricos (conocidas como las claves temporales de par o "pairwise") y un conjunto de dos claves diferentes para el tráfico de difusión y de multidifusión.

El conjunto de claves de par utilizado para los datos de difusión única y los mensajes de clave EAPOL (EAP sobre LAN) consta de lo siguiente:

- Clave de cifrado de datos: Una clave de 128 bits utilizada para cifrar tramas de difusión única.
- Clave de integridad de datos: Una clave de 128 bits utilizada para calcular el MIC de tramas de difusión única.
- Clave de cifrado de clave EAPOL: Una clave de 128 bits utilizada para cifrar mensajes de clave EAPOL.
- Clave de integridad de clave EAPOL: Una clave de 128 bits utilizada para calcular el MIC de mensajes de clave EAPOL.

4.7. Proceso de Cifrado y Descifrado de WPA2

AES CCMP utiliza CBC-MAC para calcular el MIC y el modo contador de AES para cifrar la carga 802.11 y el MIC. Para calcular un valor de MIC, AES CBC-MAC usa el siguiente proceso:

1. Se cifra un bloque inicial de 128 bits con AES y la clave de integridad de datos. Esto produce un resultado de 128 bits (Result1).

2. Se realiza una operación exclusiva OR (XOR) entre Result1 y los próximos 128 bits de los datos sobre los cuales se calcula el MIC. Esto produce un resultado de 128 bits (XResult1).

3. Se cifra XResult1 con AES y la clave de integridad de datos. Esto genera Result2.

4. Se realiza una XOR entre Result2 y los siguientes 128 bits de los datos. Esto genera XResult2.

Se repiten los pasos 3 y 4 para los bloques adicionales de 128 bits de los datos. Los 64 bits de orden superior del resultado final constituyen el MIC de WPA2. La figura 23 muestra el proceso para calcular el MIC.

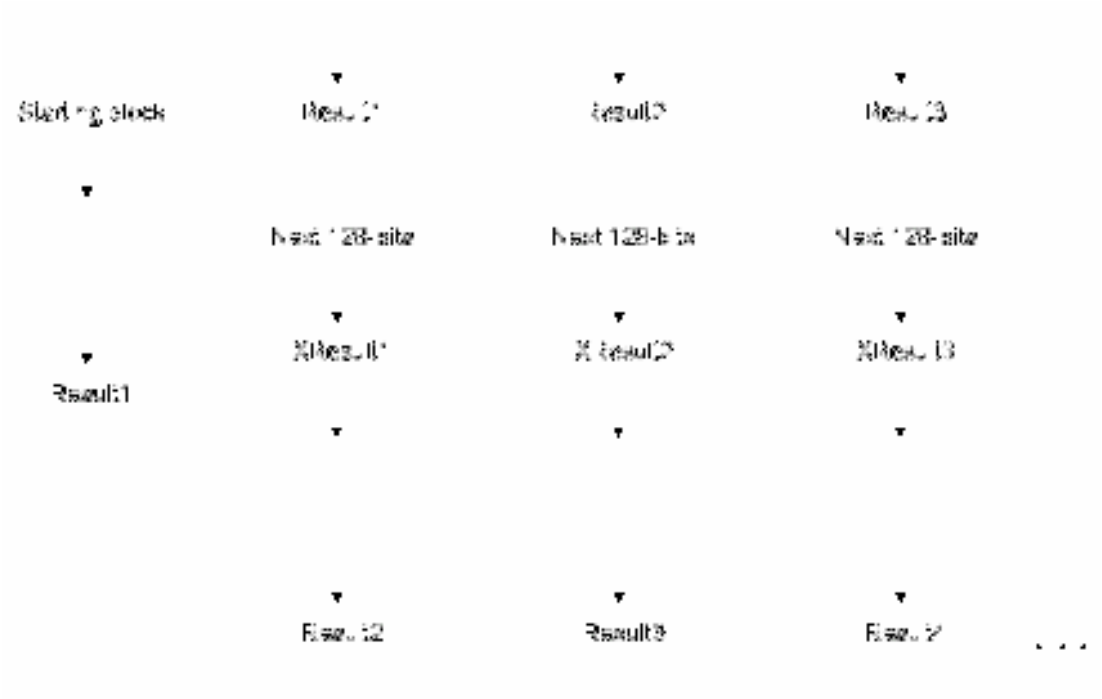

Figura 23. Proceso Para Calcular el MIC. [38]

[38] Cifrado e integridad de los datos en Wi-Fi Protected Access, The Cable Guy, Agosto 2005.

Para calcular el MIC de una trama IEEE 802.11, WPA2 construye lo siguiente:

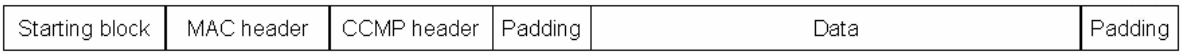

Figura 24. Trama IEEE 802.11 con WPA2. [39]

- El bloque inicial es un bloque de 128 bits que se describirá más adelante en este artículo.
- El encabezado MAC es el encabezado MAC de 802.11 con los valores de los campos que pueden cambiar en tránsito configurados en 0.
- El encabezado CCMP tiene 8 bytes y contiene el campo Número de paquete de 48 bits y campos adicionales.
- Se agregan bytes de relleno (configurados en 0) para garantizar que la parte de todo el bloque de datos que comprende hasta los datos de texto sin formato sea un número entero de bloques de 128 bits.
- Los datos son la parte de texto sin formato (sin cifrado) de la carga 802.11.
- Se agregan bytes de relleno (configurados en 0) para garantizar que la parte del bloque de datos de MIC que incluye datos de texto sin formato sea un número entero de bloques de 128 bits.

A diferencia de la integridad de los datos de WEP y WPA, WPA2 proporciona integridad de los datos tanto para el encabezado 802.11 (con la excepción de los campos variables) como para la carga 802.11.

El bloque inicial, presente en la figura 25, para el cálculo del MIC consta de lo siguiente:

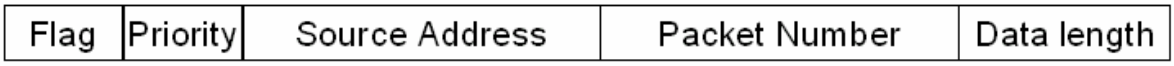

Figura 25. Bloque Inicial para el Cálculo del MIC. [40]

[39] Wi-Fi Protected Access 2 Data Encryption and Integrity, The Cable Guy, Agosto 2005.
[40] Wi-Fi Protected Access 2 Data Encryption and Integrity, The Cable Guy, Agosto 2005.

- El campo Indicador (8 bits) se configura en 01011001 y contiene varios indicadores, por ejemplo, uno que indica que el MIC utilizado en la trama 802.11 tiene una longitud de 64 bits.
- El campo Prioridad (8 bits) está reservado para propósitos futuros y se configura en 0.
- El campo Dirección de origen (48 bits) corresponde al encabezado MAC 802.11.
- El campo Número de paquete (48 bits) corresponde al encabezado CCMP.
- La longitud de los datos de texto sin formato en bytes (16 bits).

El algoritmo de cifrado de modo contador de AES utiliza el siguiente proceso:

1. Se cifra un contador inicial de 128 bits con AES y la clave de cifrado de datos. Esto produce un resultado de 128 bits (Result1).

2. Se realiza una operación exclusiva OR (XOR) entre Result1 y el primer bloque de 128 bits de los datos que se están cifrando. Esto produce el primer bloque cifrado de 128 bits.

3. Se incrementa el contador y se lo cifra con AES y la clave de cifrado de datos. Esto genera Result2.

4. Se realiza una XOR entre Result2 y los siguientes 128 bits de los datos. Esto produce el segundo bloque cifrado de 128 bits.

El modo contador de AES repite los pasos 3 y 4 para los bloques adicionales de 128 bits de los datos hasta el bloque final. Para el bloque final, el modo contador de AES realiza una XOR del contador cifrado con los bits restantes, lo que produce datos cifrados que tienen la misma longitud que el último bloque de datos. La figura 26 muestra el proceso del modo contador de AES.

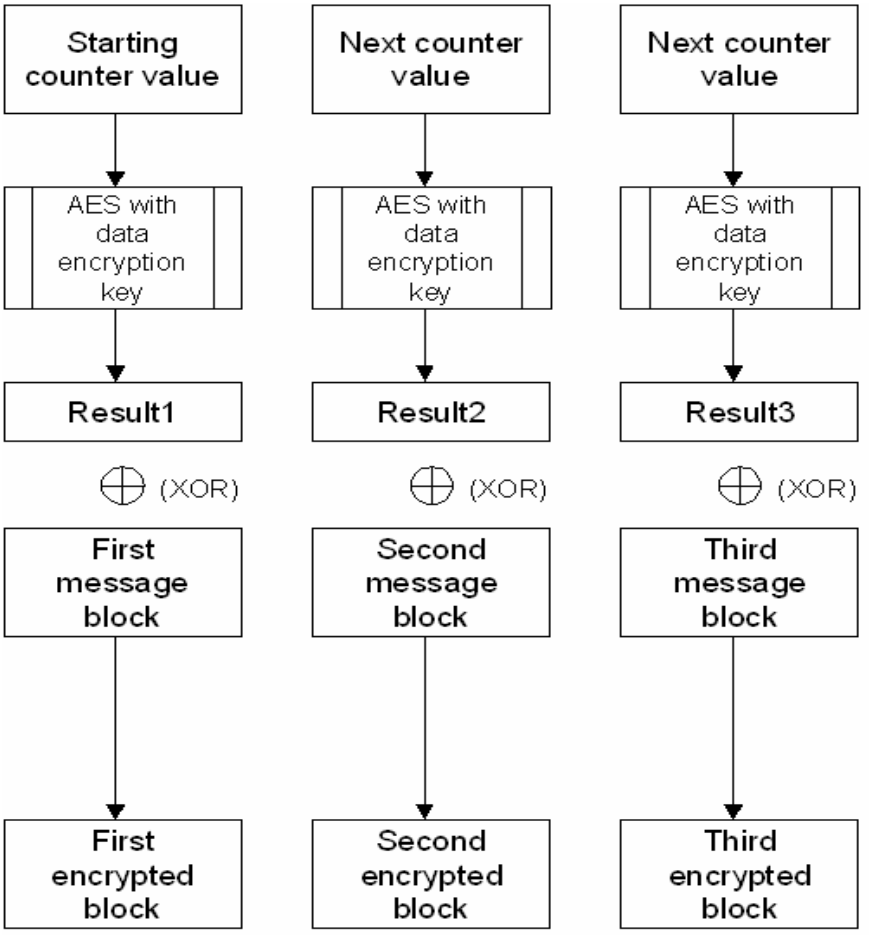

Figura 26. Proceso del Modo Contador de AES.

El valor inicial del contador para el modo contador de AES (ver figura 27) consta de lo siguiente:

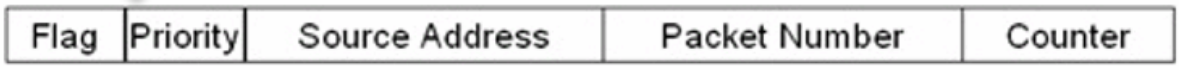

Figura 27. Valor Inicial del Modo Contador de AES. [41]

[41] Wi-Fi Protected Access 2 Data Encryption and Integrity, The Cable Guy, Agosto 2005.

- El campo Indicador (8 bits) se configura en 01011001, que es el mismo valor de Indicador que se usa para el cálculo del MIC.
- El campo Prioridad (8 bits) está reservado para propósitos futuros y se configura en 0.
- El campo Dirección de origen (48 bits) corresponde al encabezado MAC 802.11.
- El campo Número de paquete (48 bits) corresponde al encabezado CCMP.
- El campo Contador (16 bits) se configura en 1 y se incrementa sólo si se fragmenta una carga 802.11 en cargas más pequeñas. Tenga en cuenta que el campo Contador no es el mismo que el valor de contador de 128 bits que se utiliza en el algoritmo de cifrado de modo contador de AES.

Para cifrar una trama de datos de difusión única, WPA2 utiliza el siguiente proceso:
1. Se ingresa el bloque inicial, el encabezado MAC 802.11, el encabezado CCMP, la longitud de los datos y los campos de relleno en el algoritmo CBC-MAC con la clave de integridad de datos para generar el MIC.
2. Se ingresa el valor inicial del contador y la combinación de los datos con el MIC calculado en el algoritmo de cifrado de modo contador de AES con la clave de cifrado de datos para generar el MIC y los datos cifrados.
3. Se agrega el encabezado CCMP que contiene el Número de paquete a la parte cifrada de la carga 802.11, y se encapsula el resultado con el encabezado y el final 802.11.

La figura 28 muestra el proceso de cifrado de WPA2 para una trama de datos de difusión única.

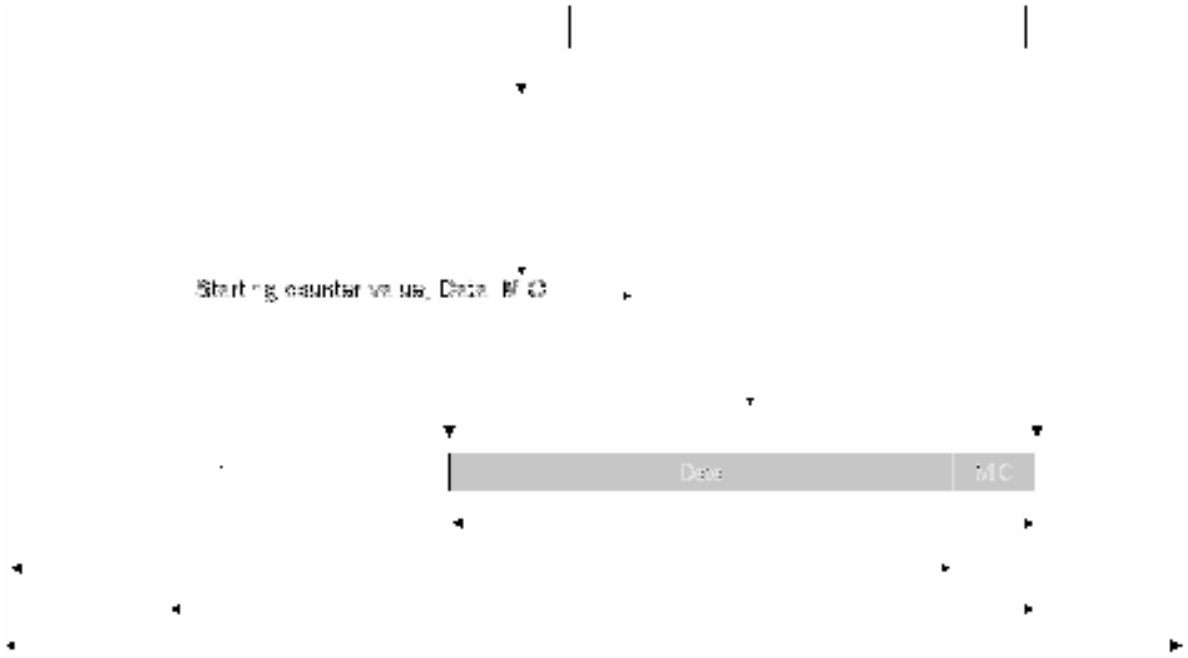

Figura 28. Proceso de Cifrado para Una Trama de Datos de Difusión Única. [42]

Para descifrar una trama de datos de difusión única y examinar la integridad de los datos, WPA2 utiliza el siguiente proceso:

1. Se determina el valor inicial del contador a partir de los valores de los encabezados 802.11 y CCMP.
2. Se ingresa el valor inicial del contador y la parte cifrada de la carga 802.11 en el algoritmo de descifrado de modo contador de AES con la clave de cifrado de datos para generar el MIC y los datos descifrados. Para el descifrado, el modo contador de AES realiza una XOR del valor cifrado del contador con el bloque de datos cifrados, lo que genera el bloque de datos descifrados.

[42] Wi-Fi Alliance, Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise, Marzo 2005.

3. Se ingresa el bloque inicial, el encabezado MAC 802.11, el encabezado CCMP, la longitud de los datos y los campos de relleno en el algoritmo AES CBC-MAC con la clave de integridad de datos para calcular el MIC.
4. Se compara el valor calculado del MIC con el valor del MIC descifrado. Si los valores del MIC no coinciden, WPA2 descarta los datos silenciosamente. Si los valores del MIC coinciden, WPA2 transfiere los datos a las capas superiores de las redes para su procesamiento.

La figura 29 muestra el proceso de descifrado de WPA2 para una trama de datos de difusión única.

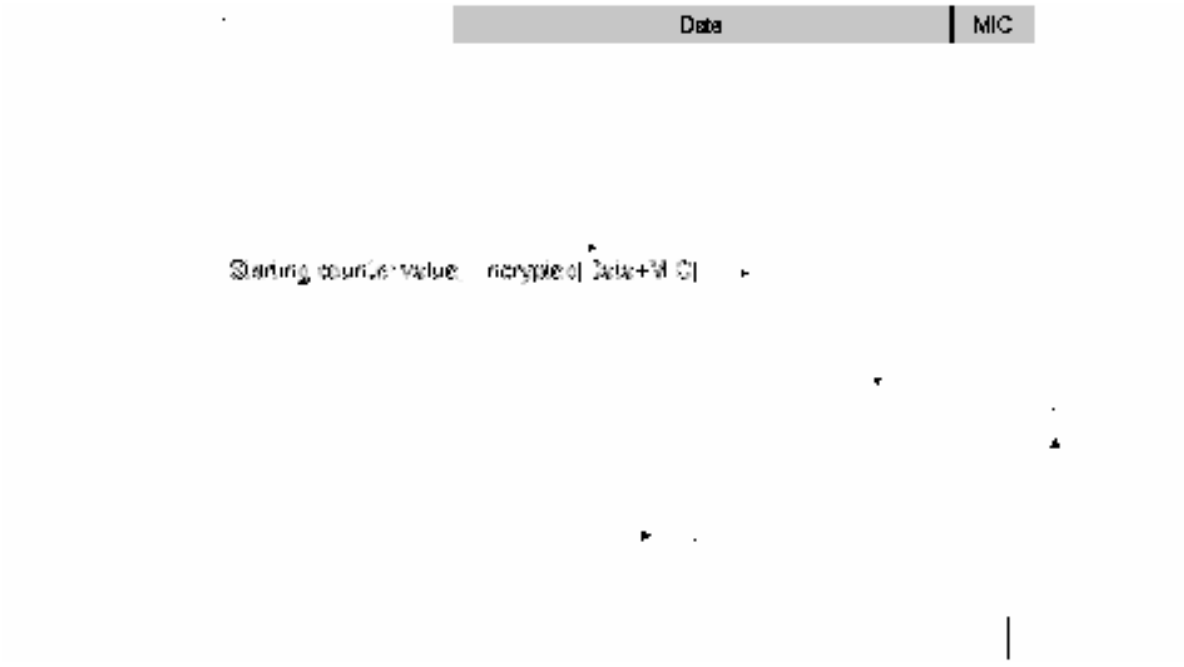

Figura 29. Proceso de Descifrado para una Trama de Datos de Difusión Única.

4.8. Actualización de Wi-Fi Protected Access 2 (WPA2)/Wireless Provisioning Services Information Element (WPS IE) para Windows XP con el Service Pack 2

La actualización admite las funciones de seguridad obligatorias adicionales del estándar IEEE 802 que aún no se incluyen en los productos que admiten WPA. Además, después de instalar la actualización, Windows XP mostrará Identificadores del conjunto de servicios (SSID) que anteriormente habían permanecido ocultos en el cuadro de diálogo Elija una red inalámbrica. Esta funcionalidad facilita la conexión a redes Wi-Fi públicas a las cuales no se haya conectado anteriormente.
Esta actualización mejora el software del cliente inalámbrico de Windows XP para la nueva certificación Wi-Fi Alliance para la seguridad inalámbrica. La actualización también facilita la conexión a espacios públicos seguros que estén equipados con acceso a Internet inalámbrico. Estas ubicaciones se conocen como "zonas activas de fidelidad inalámbrica" (Wi-Fi hotspots).
Se puede descargar del siguiente link:
http://www.microsoft.com/downloads/details.aspx?displaylang=es&FamilyID=662BB74D-E7C1-48D6-95EE-1459234F4483

Requisitos previos

Para instalar esta actualización debe ejecutar Windows XP con SP2. Para obtener más información acerca de cómo obtener el Service Pack más reciente de Windows XP, diríjase al siguiente link:
http://support.microsoft.com/kb/322389/
Para verlo en Microsoft Knowledge Base: **Cómo obtener el Service Pack más reciente para Windows XP.**

Requisito de Reinicio

Una vez aplicada la actualización, se debe reiniciar el equipo.

4.8.1. Información del Archivo

La versión en inglés de la actualización tiene los atributos de archivo (o atributos del archivo más reciente) mostrados en la siguiente tabla. Las fechas y las horas de estos archivos se muestran según el horario universal coordinado (UTC). La información de los archivos se convertirá a la hora local cuando la vea. Para ver la diferencia entre la hora UTC y la hora local, utilice la ficha Zona horaria de la herramienta Fecha y hora del Panel de control.

Fecha	Hora	Versión	Tamaño	Nombre de archivo
19-Abr-2005	23:54	5.1.2600.2658	14.592	Ndisuio.sys
19-Abr-2005	19:21	5.1.2600.2658	1.705.472	Netshell.dll
19-Abr-2005	19:21	5.1.2600.2658	381.440	Wzcdlg.dll
19-Abr-2005	19:21	5.1.2600.2658	52.736	Wzcsapi.dll
19-Abr-2005	19:21	5.1.2600.2658	474.624	Wzcsvc.dll
19-Abr-2005	23:44	5.1.2600.2658	13.824	Xpsp3res.dll

Tabla 5. Horario Universal Coordinado. [43]

La actualización WPA/WPS IE admite las siguientes funciones de la WPA2:

- WPA2 Enterprise, que utiliza la autenticación IEEE 802.1X, y WPA2 Personal, que utiliza una clave compartida (PSK).

[43] Actualización de Wi-Fi Protected Access 2 (WPA2), The Cable Guy, Agosto 2005.

- El estándar de cifrado avanzado (AES), que utiliza el Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP) y proporciona confidencialidad de datos, datos de autenticación e integridad de datos para marcos inalámbricos.
- El uso opcional de la memoria caché de la clave maestra Pairwise (PMK) y de la memoria caché oportunista de la PMK. En el almacenamiento en caché PMK, los clientes inalámbricos y los puntos de acceso inalámbrico almacenan en caché los resultados de las autenticaciones 802.1X. De este modo, el acceso es mucho más rápido cuando un cliente inalámbrico vuelve a un punto de acceso inalámbrico que ya había autenticado.
- El uso opcional de la preautenticación. En la preautenticación, un cliente inalámbrico WPA2 puede realizar una autenticación 802.1X con otros accesos inalámbricos en su intervalo cuando todavía está conectado a su punto de acceso inalámbrico.

Debe usar la actualización WPA2/WPS IE en combinación con lo siguiente:

- Puntos de acceso inalámbricos que admitan WPA2.
- Adaptadores de red inalámbrica que admitan WPA2.
- Controladores de adaptador de red inalámbrica de Windows XP que admitan el paso de las capacidades de WPA2 a la configuración inalámbrica automática de Windows.

La actualización WPA2/WPS IE modifica los siguientes cuadros de diálogo:

- Cuando usted está conectado a una red inalámbrica con capacidades WPA2, el tipo de red se muestra como WPA2 en el cuadro de diálogo Elija una red inalámbrica.

- En la ficha Asociación para las propiedades de una red inalámbrica, la lista Autenticación de red presenta las siguientes opciones adicionales:
  - WPA2 - para WPA2 Enterprise.
  - WPA2-PSK - para WPA2 Personal.

Hay que tener en cuente que estas opciones no existen si el controlador del adaptador de red inalámbrica no admite WPA2.

4.8.2. Valores de Registro que Controlan La Preautenticación y El Almacenamiento en Caché PMK

Las siguientes entradas de Registro en la HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EAPOL\Parameters\General\Global subclave controlan el comportamiento de la preautenticación y el almacenamiento en caché PMK para la actualización WPA2/WPS IE:

- PMKCacheMode
- PMKCacheTTL
- PMKCacheSize
- PreAuthMode
- PreAuthThrottle

PMKCacheMode

Tipo del valor: REG_DWORD - Booleano
Intervalo válido: 0 (habilitado), 1 (deshabilitado)
Valor predeterminado: 1
Presente de forma predeterminada: No

Descripción: especifica si un cliente inalámbrico basado en Windows XP realizará el almacenamiento en caché PMK. De forma predeterminada, se habilita PMKCacheMode.

PMKCacheTTL

Tipo de valor: REG_DWORD
Intervalo válido: 5-1440
Valor predeterminado: 720
Presente de forma predeterminada: No

PMKCacheSize

Tipo de valor: REG_DWORD
Intervalo válido: 1-255
Valor predeterminado: 100
Presente de forma predeterminada: No
Descripción: especifica el número máximo de entradas que pueden almacenarse en la caché PMK. De forma predeterminada, la caché PMK tiene 16 entradas.

PreAuthMode

Tipo de valor: REG_DWORD - Booleano
Intervalo válido: 0 (habilitado), 1 (deshabilitado)
Valor predeterminado: 0
Presente de forma predeterminada: No
Descripción: especifica si un cliente inalámbrico basado en Windows XP intentará llevar a cabo una preautenticación. De manera predeterminada, PreAuthMode es deshabilitado.

PreAuthThrottle

Tipo de valor: REG_DWORD
Intervalo válido: 1-16
Valor predeterminado: 3
Presente de forma predeterminada: No
Descripción: especifica el número máximo de puntos de acceso inalámbrico con el cual el equipo basado en Windows XP tratará de llevar a cabo una preautenticación. El valor está basado en la lista ordenada de los puntos de acceso inalámbrico preferidos, según lo indique el controlador del adaptador de red inalámbrica. De forma predeterminada, PreAuthThrottle tiene un valor igual a 3.
Nota: el cambio de uno o más de estos valores de entrada del Registro no se aplicará hasta la próxima vez que reinicie el servicio inalámbrico o el equipo.
Descripción: especifica la cantidad de minutos que puede existir una entrada en el almacenamiento en caché PMK antes de que se quiten. El valor máximo es 1440 (24 horas). El valor predeterminado es 720 (12 horas).

4.8.3. Wireless Provisioning Services Information Element (WPS IE)

En un principio, los proveedores de servicios de Internet inalámbrica (WISP) ofrecieron acceso inalámbrico a Internet sin seguridad. Esto evitaba que los clientes tuvieran que establecer la configuración de seguridad inalámbrica. Como la seguridad inalámbrica ha ganado más importancia, los WISP desean realizar el paso hacia redes de fidelidad inalámbricas públicas seguras. Durante la migración, los WISP deben ser capaces de admitir tanto el acceso inalámbrico a Internet seguro como el no seguro. Para que este pasaje les resulte rentable, deben ser capaces de ofrecer soporte y anunciar dos redes inalámbricas diferentes que tengan dos nombres de red inalámbrica diferentes y que utilicen una única infraestructura física de red.

Los nombres de red inalámbrica también se conocen como Identificadores del conjunto de servicios (SSID).

Algunos puntos de acceso inalámbrico que están disponibles en la actualidad pueden anunciar múltiples SSID y dar soporte a varias configuraciones de red lógicas al mismo tiempo. Sin embargo, debido a limitaciones del hardware, la amplia mayoría de los puntos de acceso inalámbrico que se implementan hoy en día en las zonas activas de fidelidad inalámbrica sólo permiten la inclusión de un SSID en las tramas de difusión de Beacon y Probe Response. Este comportamiento oculta de manera efectiva los SSID secundarios de los equipos clientes inalámbricos. Por lo tanto, es más difícil descubrir y conectarse a nombres de red de fidelidad inalámbrica a los que nunca se haya conectado. Sin un punto de acceso inalámbrico que permita anunciar múltiples SSID en las tramas de difusión Beacon y Probe Response, las redes inalámbricas adicionales deben implementarse mediante el uso de un conjunto adicional de puntos de acceso inalámbrico físicos, o bien los usuarios deberán establecer la configuración de sus clientes inalámbricos de forma manual mediante el uso de nombres de SSID ocultos. La implementación de un conjunto adicional de puntos de acceso inalámbricos no resulta rentable para los WISP. La configuración manual de los clientes inalámbricos resulta dificultosa para los clientes, y no se adapta a una red WISP de gran magnitud.

La WPS IE es un elemento de información 802.11 recientemente definido que soluciona el problema de los SSID ocultos para los WISP. La WPS IE también proporciona una solución para que los puntos de acceso inalámbrico puedan anunciar SSID adicionales en las tramas de difusión de Beacon y Probe Request La WPS IE incluye SSID y otros detalles, como:

- Si se requiere autenticación IEEE 802.1X.

- Si la red inalámbrica puede proporcionarle al cliente inalámbrico la provisión de información.

La WPS IE debe incluirse en las tramas de difusión de Beacon y Probe Request, y debe ser reconocido y procesado por los equipos cliente inalámbricos. Normalmente, usted puede agregar el soporte WPS IE a puntos de acceso inalámbrico a través de una actualización del firmware. Por lo tanto, usted normalmente no tiene que reemplazar puntos de acceso inalámbrico existentes o que instalar puntos adicionales. Compruebe con la documentación de su proveedor inalámbrico o con el sitio Web del mismo si está disponible una actualización del firmware para su punto de acceso inalámbrico. Para un cliente inalámbrico basado en el SP2 de Windows XP, debe instalar la actualización WPA2/WPS IE.

Cuando usted instala la actualización WPA2/WPS IE en equipos clientes inalámbricos que ejecutan Windows XP con SP2, los componentes inalámbricos de Windows XP reconocen la WPS IE en las tramas de difusión de Beacon o Probe Response. Esta función hace que los SSID que habían permanecido ocultos se vuelvan visibles en el cuadro de diálogo Elija una red inalámbrica. Los equipos cliente inalámbricos basados en Windows XP que no tienen instalada la actualización WPA2/WPS IE no reconocen la WPS IE y no muestran los SSID ocultos.

Para implementar la admisión de la WPS IE correctamente, deberá tener lo siguiente:

- Puntos de acceso inalámbrico que admitan la configuración de SSID adicionales y el anuncio con la WPS IE. Por ejemplo, Cisco ha lanzado actualizaciones de firmware para que sus puntos de acceso inalámbrico admitan la nueva WPS IE. Para obtener información, visite el siguiente sitio Web de Cisco Web:

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin0900aecd801b83b0.html.

- Equipos cliente inalámbricos que ejecutan Windows XP con SP2 y la actualización WPA2/WPS IE.

Después de que se implementa la actualización, el uso de la WPS IE proporciona las siguientes ventajas:

- Permite una migración segura y rentable de zonas activas Wi-Fi de conexión inalámbrica públicas no seguras a zonas activas Wi-Fi de conexión inalámbrica públicas seguras. Las zonas activas de fidelidad inalámbrica públicas seguras deben usar autenticación 802.1X, cifrado, y Wireless Provisioning Services (WPS) para provisionar los valores inalámbricos, utilizando el mismo conjunto de puntos de acceso inalámbrico.
- Permite a los usuarios descubrir y elegir fácilmente si quieren conexiones inalámbricas seguras o no seguras. Además, los usuarios inalámbricos pueden establecer rápidamente la configuración inalámbrica.

4.8.4. Cambios Adicionales en La Actualización WPA2/WPS IE

Los siguientes cambios también se incluyen en la actualización WPA2/WPS IE:

- Ahora, Windows XP le pide que valide si desea crear una red inalámbrica preferida no segura. Se define no segura como una conexión autenticada de sistema abierto que no utiliza cifrado para proteger la información. Además, cuando está conectada a una red inalámbrica no segura, la red muestra la etiqueta No segura. Estos cambios se realizaron para asegurarse de que usted sabe que se está conectando a una red inalámbrica que podría sufrir ataques a la seguridad.

- El cuadro de diálogo Elija una red inalámbrica en Windows XP con SP2 combinaba infraestructura y redes ad-hoc utilizando el mismo nombre de red inalámbrica y sólo una aparecía en la lista de redes disponibles. Este problema se ha corregido. Cuando se instala la actualización, el cuadro de diálogo Elija una red inalámbrica ahora muestra ambos tipos de redes inalámbricas en la lista de redes disponibles como entradas independientes.
- La interfaz de configuración estática API para los Wireless Provisioning Services (WPS) ha sido actualizada para que usted pueda especificar la WPA2 como método de autenticación. Para obtener más información sobre esta API, visite el siguiente sitio Web de Microsoft: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/xpehelp/html/xeconwirelessprovisioningserviceapi.asp
- Anteriormente, había un retardo de un minuto en la conexión cuando iniciaba el equipo si estaba conectado a un sistema de protección inalámbrico WPS. Este problema ya ha sido corregido.

5. SERVIDORES RADIUS

5.1 Características de los Servidores Radius.

RADIUS (***R**emote **A**ccess **D**ial-**I**n **U**ser **S**erver*). Es un protocolo de autentificación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

En el caso de las conexiones inalámbricas, el punto de acceso actúa como autenticador para el acceso a la red y utiliza un servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) para autenticar las credenciales del cliente. La comunicación es posible a través de un "puerto no controlado" lógico o canal en el punto de acceso con el fin de validar las credenciales y obtener claves para obtener acceso a la red a través de un "puerto controlado" lógico. Las claves de que dispone el punto de acceso y el cliente como resultado de este intercambio permiten cifrar los datos del cliente y que el punto de acceso lo identifique. De este modo, se ha agregado un protocolo de administración de claves a la seguridad de 802.11.

Un servidor RADIUS mantiene una base de datos de usuarios, que contiene información de autenticación por usuario como, por ejemplo, el nombre de usuario, la contraseña e información sobre las cuentas. El Servidor RADIUS concederá o denegará el acceso de los Clientes a la red interna, utilizando para la autenticación y autorización la información del Controlador del Dominio.

Un servidor RADIUS puede realizar consultas en una base de datos de autenticación local si ello es adecuado para la situación. O bien, la solicitud puede transmitirse a otro servidor para su validación. Cuando RADIUS decide que se puede autorizar el equipo en esta red, vuelve a enviar el mensaje al punto de acceso y éste permite que el tráfico de datos fluya hacia la misma.

5.2 Funcionamiento de un Servidor Radius.

Los pasos siguientes describen el planteamiento genérico que se utilizaría para autenticar el equipo de un usuario de modo que obtenga acceso inalámbrico a la red.

- Sin una clave de autenticación válida, el punto de acceso prohíbe el paso de todo el flujo de tráfico. Cuando una estación inalámbrica entra en el alcance del punto de acceso, éste envía un desafío a la estación.
- Cuando la estación recibe el desafío, responde con su identidad. El punto de acceso reenvía la identidad de la estación a un servidor RADIUS que realiza los servicios de autenticación.
- Posteriormente, el servidor RADIUS solicita las credenciales de la estación, especificando el tipo de credenciales necesarias para confirmar su identidad. La estación envía sus credenciales al servidor RADIUS (a través del "puerto no controlado" del punto de acceso).
- El servidor RADIUS valida las credenciales de la estación (da por hecho su validez) y transmite una clave de autenticación al punto de acceso. La clave de autenticación se cifra de modo que sólo el punto de acceso pueda interpretarla.
- El punto de acceso utiliza la clave de autenticación para transmitir de manera segura las claves correctas a la estación, incluida una clave de sesión de unidifusión para esa sesión y una clave de sesión global para las multidifusiones.

- Para mantener un nivel de seguridad, se puede pedir a la estación que vuelva a autenticarse periódicamente.

Un ejemplo real podría ser similar al siguiente:

- Un usuario enciende su equipo portátil, con tarjeta 802.11, en un aeropuerto.
- El equipo detecta que existen redes inalámbricas disponibles, elige la óptima y se asocia a ella.
- El equipo envía las credenciales de usuario al punto de acceso para verificar que tiene permiso en esta red.
- El usuario es ErikB@bigco.com. BigCo ha adquirido acceso inalámbrico para todos sus usuarios en todos los aeropuertos del mundo.
- El servidor RADIUS, que recibe la solicitud desde el punto de acceso, comprueba el paquete y descubre que procede de un usuario de BigCo.
- A continuación, el servidor RADIUS pide a un servidor de BigCo que determine si esta persona es un usuario real y si le conceden acceso.
- Si el servidor de BigCo responde afirmativamente, se indica al punto de acceso que permita el flujo del tráfico.

5.3 Estructura de una Red de Servidores Radius

En la figura 30 podemos observar una estructura básica de servidores Radius de donde podemos valorar:

Ventajas

- Fácil de implementar.
- Fácil de gestionar.
- Sensación intuitiva de confianza.

Desventajas

- Claves simétricas.
- Política de afiliación.

- Un solo club.
- Conexión a primer nivel.

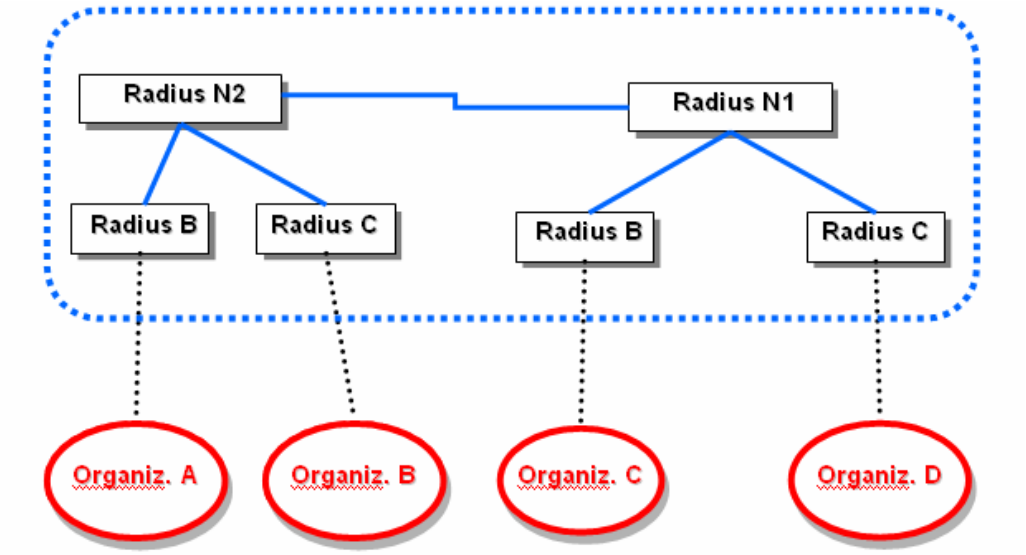

Figura 30. Estructura de Servidores Radius.

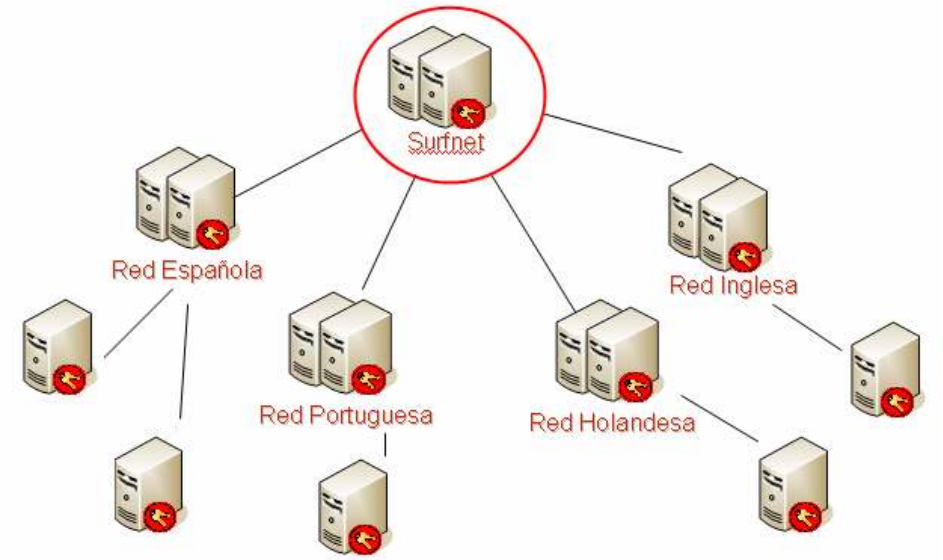

Figura *31. Ejemplo de la Estructura de la Red Europea Radius.* [44]

[44] Red.es , Estructuras de la Red de Servidores Radius.

5.4. Instalacion y Configuración Servidores Radius.

Lo primero será tener configurado el Servidor como Controlador de Dominio, para lo cual ejecutaremos el asistente de instalación de Active Directory; esto es imprescindible para la utilización de Certificados. Opcional será instalar y configurar DHCP y DNS.

El siguiente paso es instalar el “Servicio de Certificados”

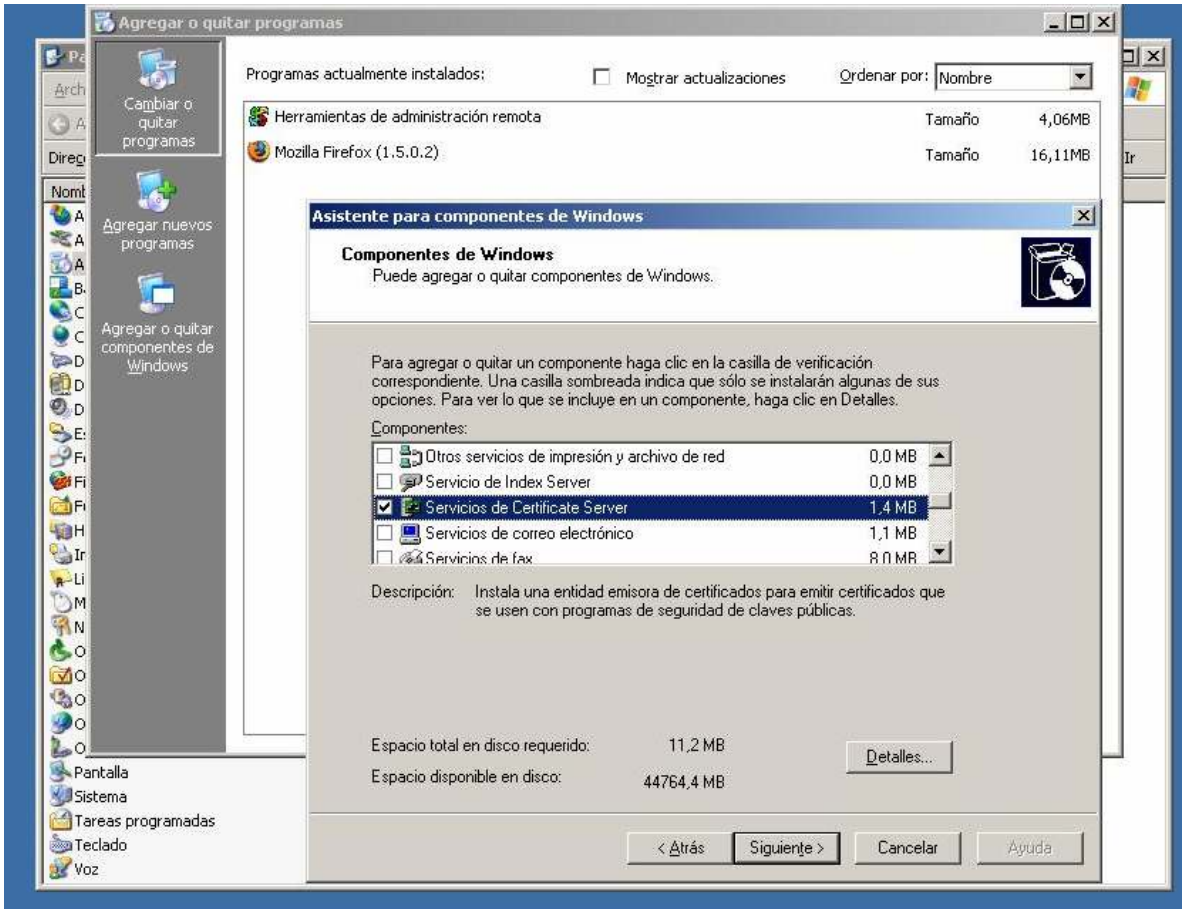

Figura 32. Instalación de Servicios Certificados.

Puesto que es el primer CA (Entidad Emisora de Certificados) en el Dominio, lo instalaremos como “Enterprise root CA”, además habremos de ponerle un nombre y también podemos especificar otras características como el periodo de validez.
Ahora hay que añadir equipos al Dominio y darles acceso Wireless como se observa en la figura 33:

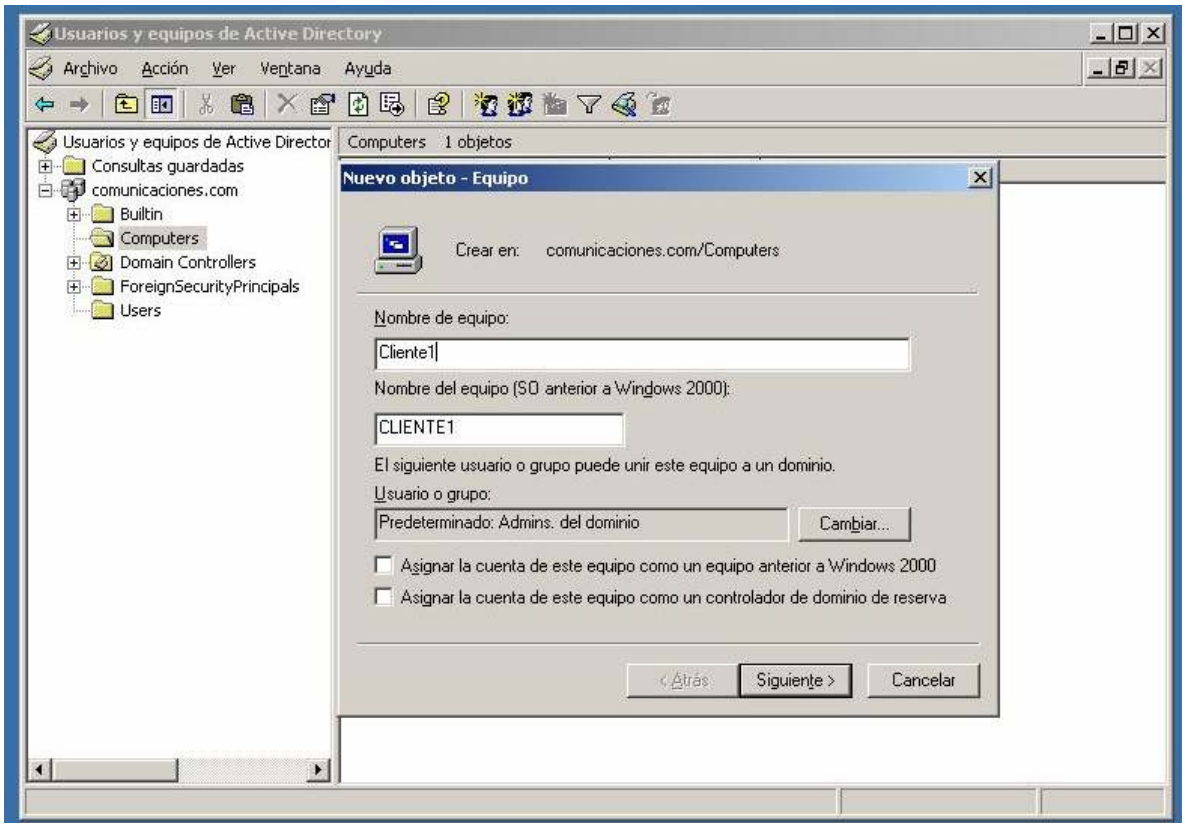

Figura 33. Añadir Equipos al Dominio y darles Acceso al Wireless.

Añadir también usuarios al dominio y darles asimismo acceso Wireless como se puede notar en la figura 34:

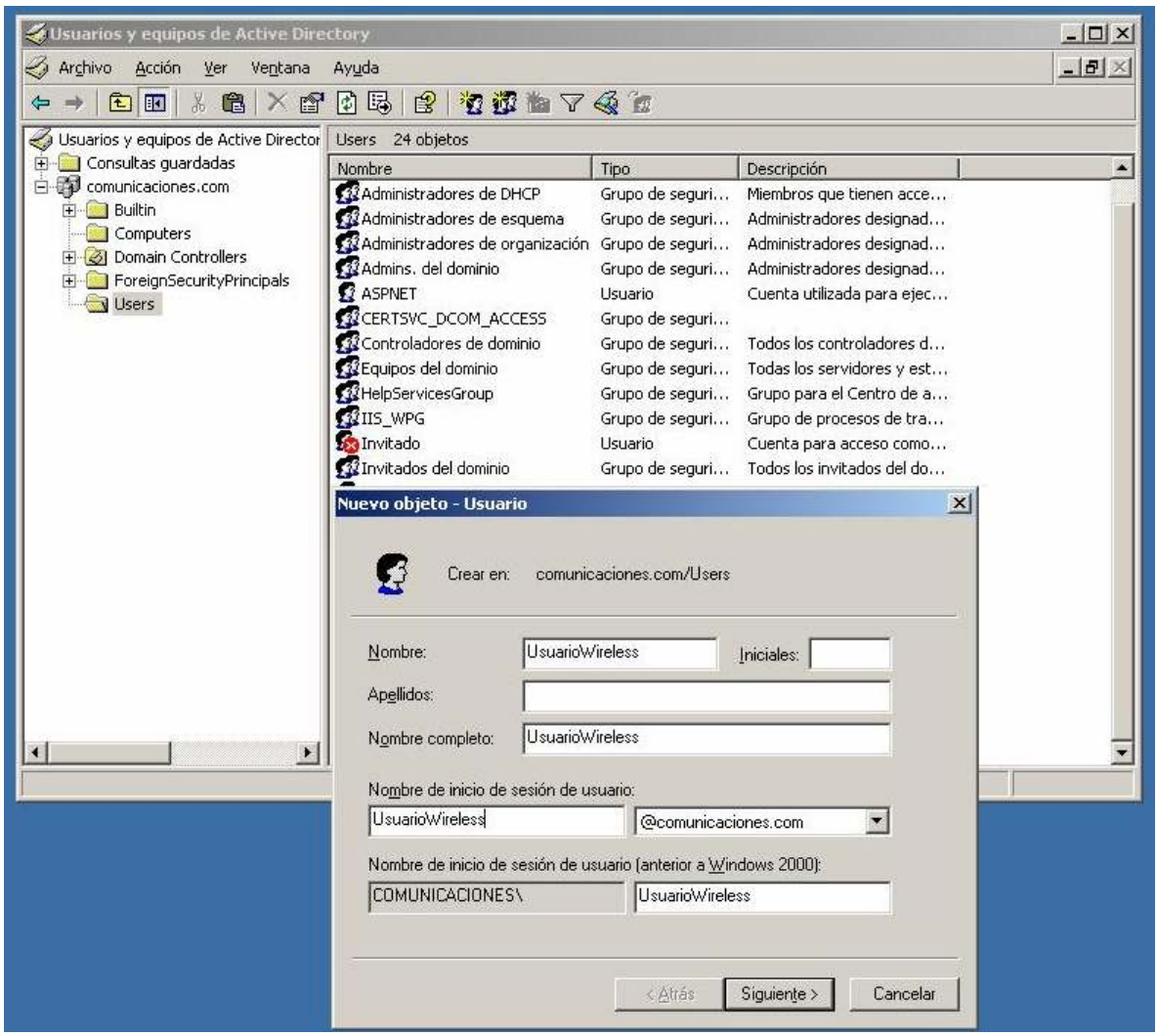

Figura 34. Añadir Usuarios al Dominio y darles Acceso al Wireless.

Añadir un grupo al dominio, y añadir a ese grupo usuarios y equipos:

En la figura 35 se puede observar la creación de un grupo.

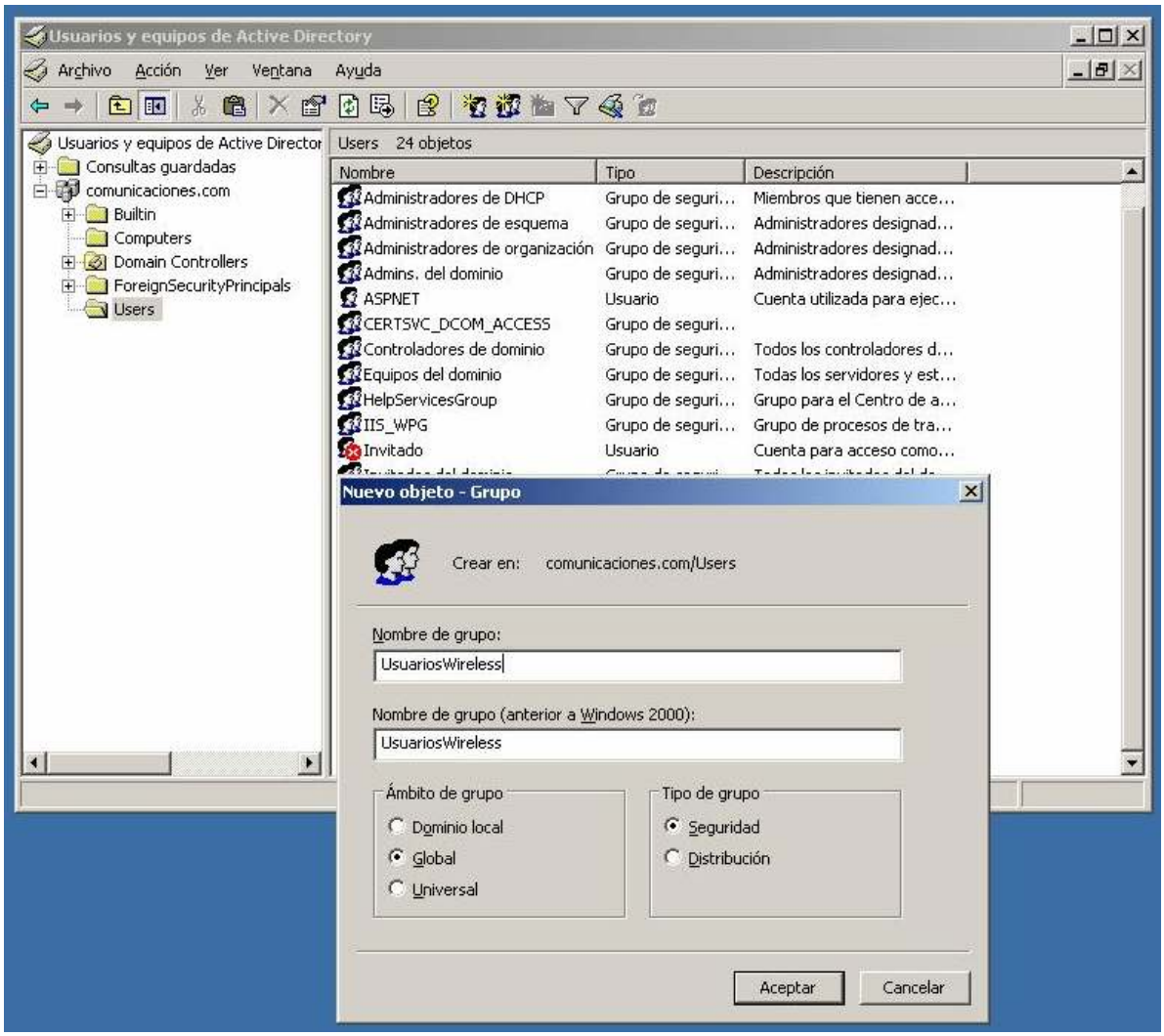

Figura 35. Añadir un Grupo al Dominio.

Mientras que en la figura 36 se observa las propiedades del usuario:

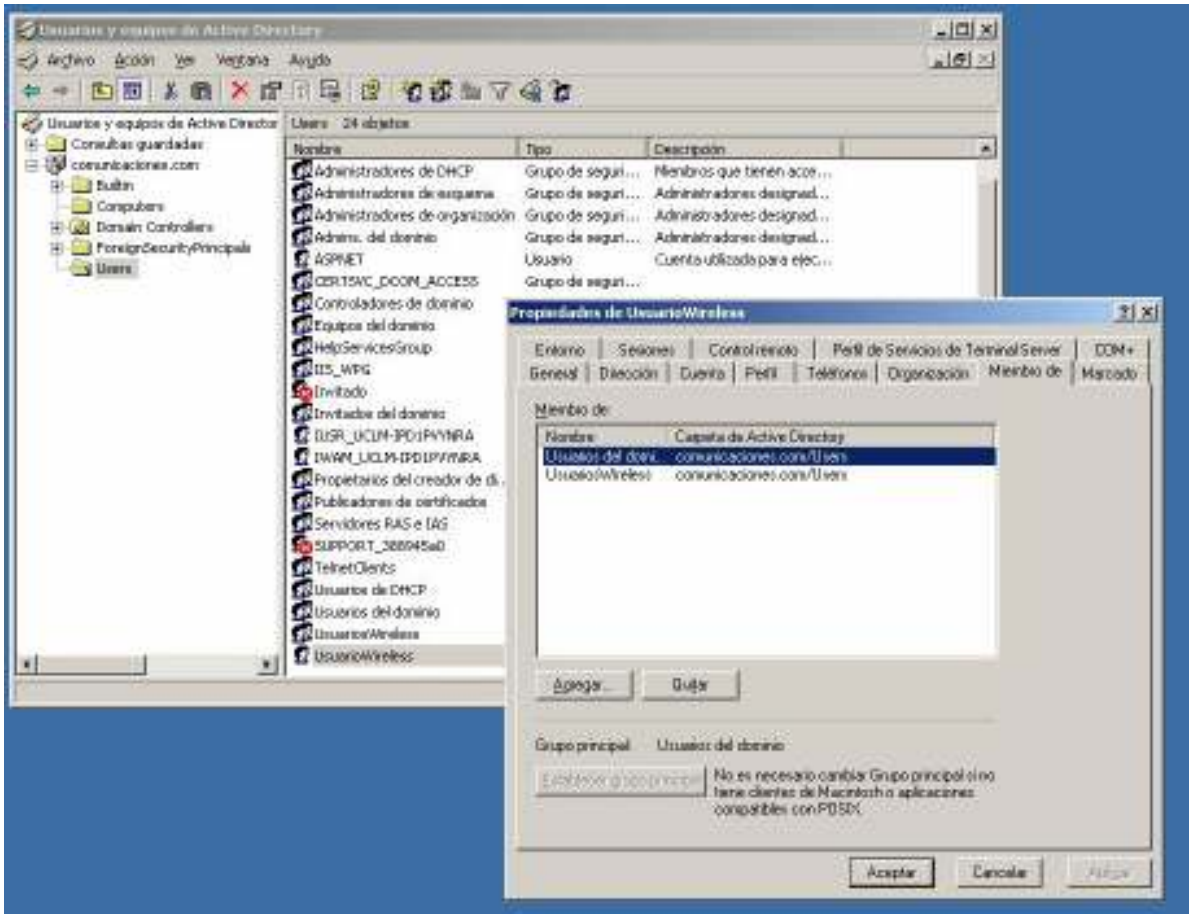

Figura 36. Propiedades de Usuario.

En la figura 37 se puede observar los diferentes clientes que existen en el grupo o que fueron creados:

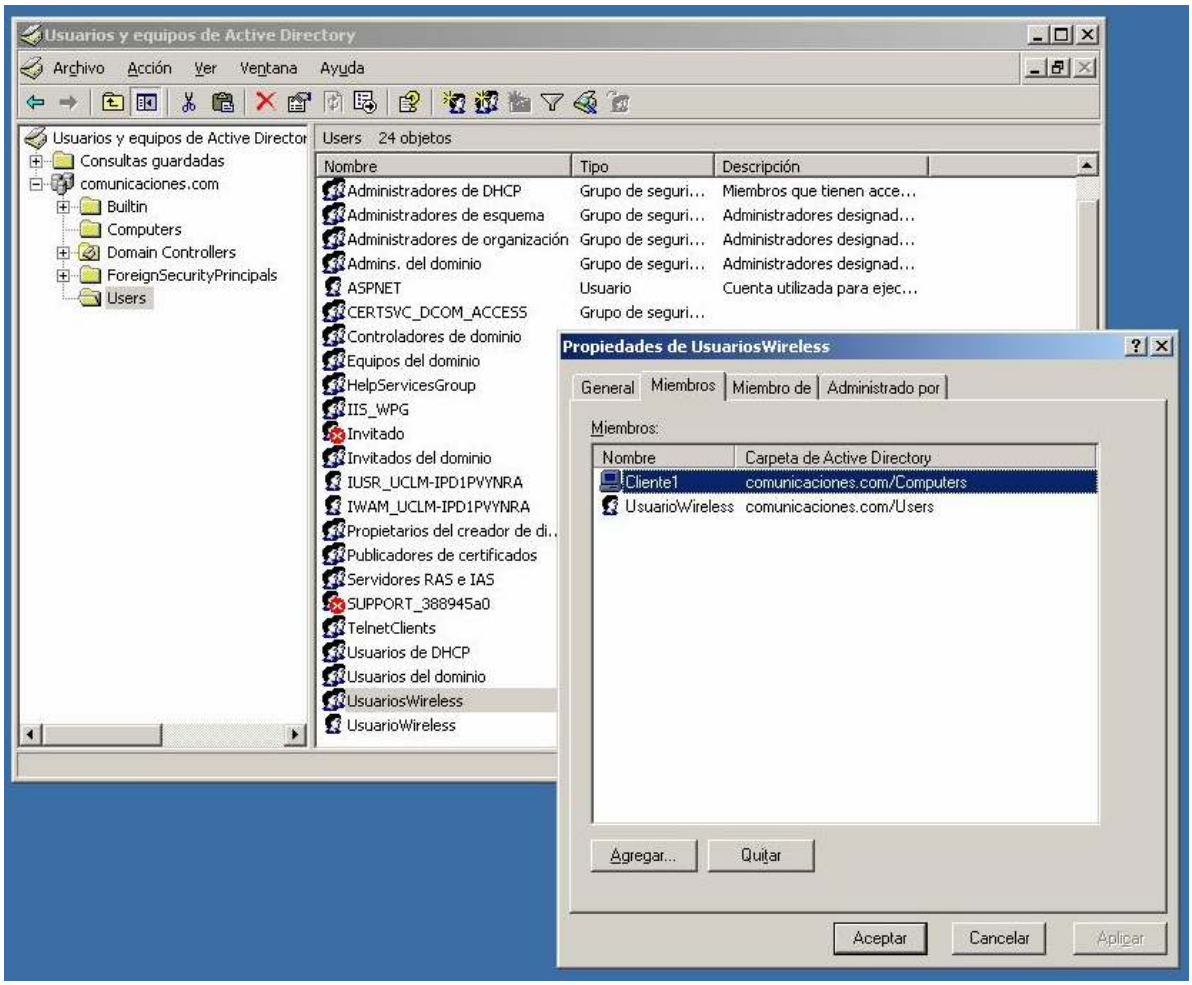

Figura 37. Usuarios y Equipos en el Dominio.

El siguiente paso es instalar el Servicio de Red "**Internet Authentication Service" (IAS)**.

Una vez instalado, hay que configurarlo para que se establezca la conexión con los Puntos de Acceso, pero hay un paso adicional que se debe realizar, y es la solicitud de un Certificado desde el CA (Entidad Emisora de Certificados). Este paso se puede simplificar si se configura el Servidor de CA para que este proceso se realice de forma automática, y así se hará más adelante, pero como todavía no está configurado hay que hacerlo manualmente. De igual forma que se realiza este proceso para el Servidor RADIUS, habrá que hacerlo para los Clientes.

Por ello debemos crear una consola que contenga los certificados, como podemos observar en la figura 38. Una vez que la tengamos iremos a la carpeta de "personal" dentro del certificado y pulsaremos en "solicitar un nuevo certificado"

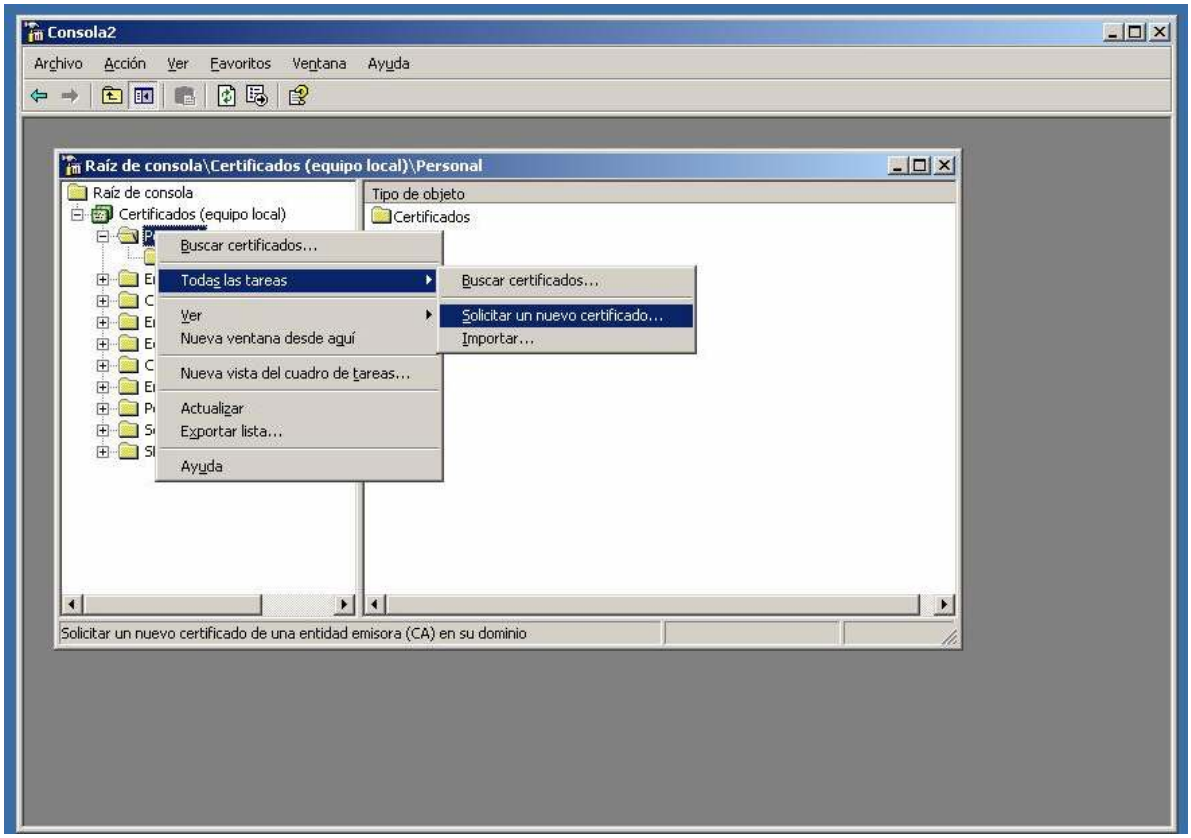

Figura 38. Como Solicitar un Nuevo Certificado.

Seleccionamos como tipo de certificado "**controlador de dominio**" y finalizamos como vemos en la figura 39:

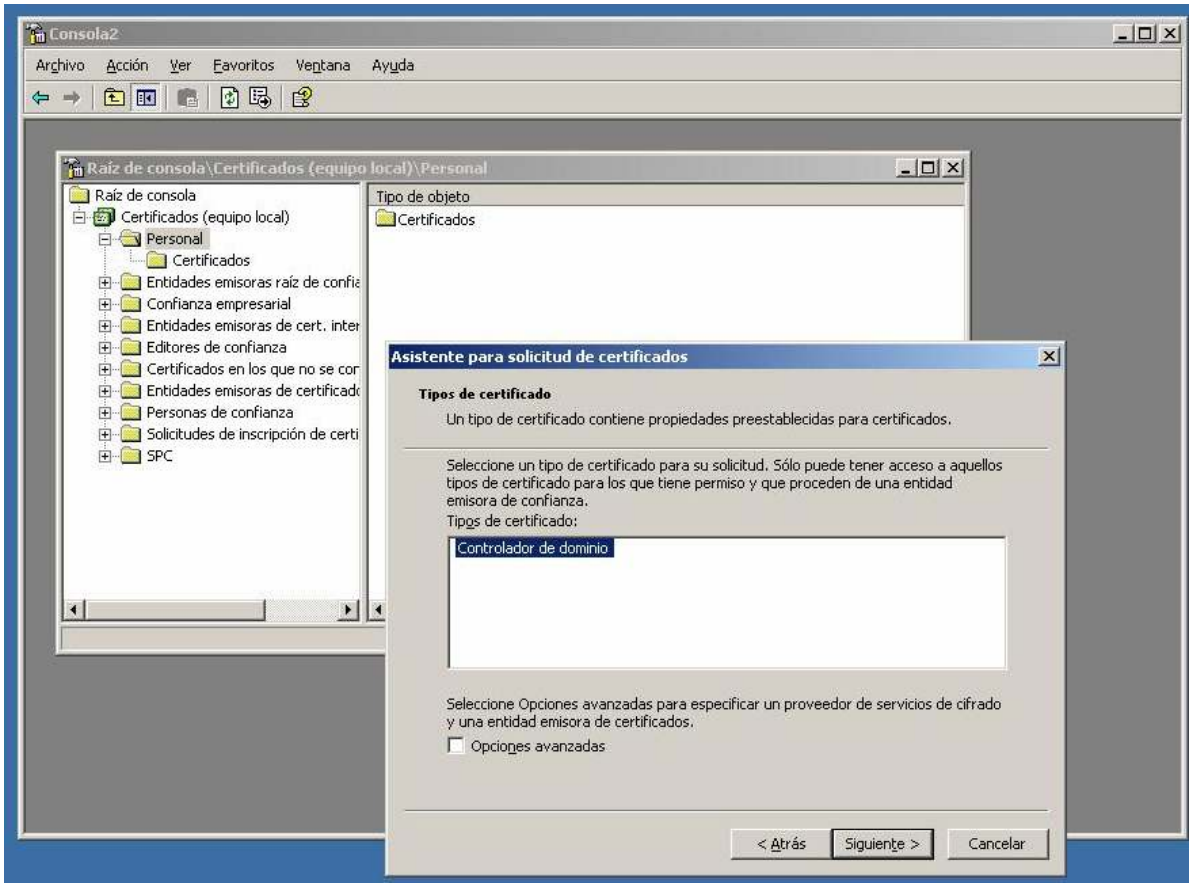

Figura 39. Escoger Controlador de Dominio.

Algo fundamental que debemos realizar es añadir el Punto de Acceso como un Cliente RADIUS, y crear y configurar unas Políticas de Acceso Remoto para los clientes Wireless, que serán todos aquellos Clientes que deseen conectarse a través del Punto de Acceso (AP).[45]

[45] Fernández Díaz Jesús, García Carrión Juan Luís, Añover García Abraham, Instalacion de un Servidor Radius con EAP-TLS, Comunicaciones Móviles.

6. CONCLUSION

Con la tecnología inalámbrica se nos abre todo un mundo de posibilidades de conexión sin la utilización de cableado clásico, proporcionado una flexibilidad y comodidad sin precedentes en la conectividad entre ordenadores.

Esta tecnología tiene como mayor inconveniente la principal de sus ventajas, el acceso al medio compartido de cualquiera con el material y los métodos adecuados, proporcionando un elevado riesgo de seguridad que tendremos que tener presente a la hora de decantarnos por esta opción y que crecerá en igual medida(o más rápido) que las soluciones aportadas para subsanar estos riesgos.

Por lo tanto se recomienda la utilización de una política de seguridad homogénea y sin fisuras, que trate todos los aspectos que comparten riesgo, sin mermar la rapidez y que sepa aprovechar las ventajas de las redes inalámbricas.

La seguridad depende del nivel de la gestión recibida, para hacer segura una tecnología hay que conocerla, una red inalámbrica en su configuración de fábrica se convierte en la puerta trasera perfecta.

Los servidores Radius son un tipo de protocolo de autentificación y autorización para aplicaciones de acceso a la red o movilidad IP.

Los servidores RADIUS se utilizan para reforzar las políticas de seguridad del protocolo WEP. RADIUS es un protocolo de autentificación y autorización para aplicaciones de acceso a la red o movilidad IP, que nos permite autenticar las credenciales del cliente, manteniendo una base de datos de usuarios, que contiene

información de autenticación por usuario como, por ejemplo, el nombre de usuario, la contraseña e información sobre las cuentas.

Para su funcionamiento esto solicita las credenciales de la estación, especificando el tipo de credenciales necesarias para confirmar su identidad. Luego valida las credenciales de la estación (da por hecho su validez) y transmite una clave de autenticación al punto de acceso. La clave de autenticación se cifra de modo que sólo el punto de acceso pueda interpretarla. El Servidor RADIUS concederá o denegará el acceso de los Clientes a la red interna, utilizando para la autenticación y autorización la información del Controlador del Dominio.

En su aplicación se puede comprobar que las características más importantes del servidor RADIUS son su capacidad para manejar sesiones, notificando cuando comienza y termina una conexión.

BIBLIOGRAFIA

- Institute of Electrical and Electronics Engineers: http://www.ieee.org
- "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ANSI/IEEE Std 802.11, 1999 Edition.
- Grupo de trabajo de IEEE 802.11i: http://grouper.ieee.org/groups/802/11/
- Wireless Fidelity Alliance: http://www.wi-fi.org
- Isabel Rodríguez Orviz y Manuel Vilas Paz, Introducción a las Tecnologías inalámbricas WiFi,.Septiembre 2004
- Wi-Fi Protected Access: http://www.wi-fi.org/ opensection/protected_access.asp
- N. Borisov, I. Goldberg, D. Wagner, "Intercepting mobile communications: The insecurity of 802.11", julio de 2001.
- S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", agosto de 2001.
- W. A. Arbaugh, N. Shankar, Y.C. Justin Wan, "Your 802.11 Wireless Network has No Clothes", 2001.
- H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-hashing for message authentication", febrero de 1997.

- “Port-Based Network Access Control”, IEEE Std 802.1X-2001, junio de 2001.

- L. Blunk, J. Vollbrecht, “PPP Extensible Authentication Protocol (EAP)”, RFC 2284, marzo de 1998.

- C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dial In User Service (RADIUS)”, RFC 2865, junio de 2000.

- W. Simpson, “The Point-to-Point Protocol (PPP)”, RFC 1661, julio de 1994.

- Computer Security Resource Center, National Institute of Standards and Technology: http://csrc.nist.gov