Acceso Wifi por WPA y validación RADIUS contra IAS

por Alejandro Moreno
amperisblog[@]gmail.com
http://amperisblog.blogspot.com

14 de junio de 2008

amperisblog

Introducción

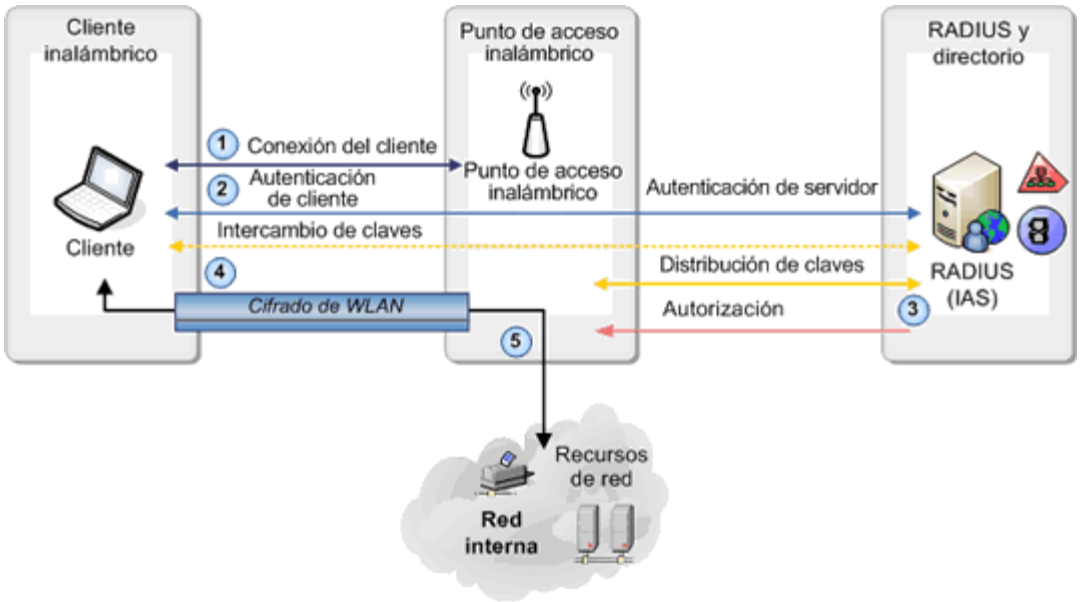
Este manual explica como instalar un punto de acceso Wifi en una empresa y utilizar los recursos que esta posee. He de suponer que en tú empresa hay un servidor de dominio Windows 2003 Server y una infraestructura de red TCP/IP.

Lo que haremos es configurar un router Wifi Zyxel con autentificación WPA y que esta autentificación se valide contra los usuarios de nuestro dominio de Windows. Para ello configuraremos el IAS para que haga de servidor de Radius.
También crearemos una política y un grupo de usuarios de tal forma que todos los usuarios que estén dentro del grupo "Wireless Access" tendrán la posibilidad de acceder por Wifi a la red. También crearemos un usuario genérico para que cualquier consultor que venga a la empresa se pueda conectar por Wifi en un momento dado.

WPA está considerado hasta ahora el protocolo más seguro ya que las claves para el cifrado de la información van cambiando constantemente a diferencia del protocolo WEP en el que solo hay un único intercambio de clave.

Dentro de WPA tenemos dos maneras de autenticarnos. La TKIP o clave temporal (para uso doméstico) y luego tenemos EAP o protocolo de autotentificación extensible (para uso empresarial). Este último será el que utilicemos. EAP se basa el 802.1x el cual valida al usuario en un servidor de Radius (en nuestro caso los usuarios serán usuarios del dominio).

Este es el esquema de funcionamiento de WPA y de la validación contra Radius:



Toda esta documentación sobre 802.1x, EPA, Radius, etc., está disponible en el TechNet de Microsoft.

Prerrequisitos

Antes de comenzar a configurar la infraestructura Wifi necesitaremos tener configurado y funcionando nuestro servidor Windows 2003 Server con nuestro dominio en Active Directory. Necesitaremos también tener instalado el último service pack y la actualizaciones de seguridad necesarias.

Por otro lado también necesitaremos tener instalado el Internet Authentication Service y el Certification Authority. Si no los tenemos instalados tendremos la posibilidad de instalarlos durante el proceso de configuración de la Wifi.

El servidor de DHCP también será necesario si queremos que una vez conectado el usuario por Wifi reciba automáticamente su dirección IP.

Necesitaremos también el CD de Windows 2003 por si nos lo pide y conexión a Internet para bajar el software necesario.

Microsoft ha creado unas herramientas llamadas Microsoft WLAN-PEAP Tools disponible en el centro de descarga dedicado a implementar una infraestructura Wifi con validación de Radius.

Comenzamos pues la configuración de infraestructura Wifi.

Instalación de CAPICOM

Lo primero que haremos es instalar en el servidor las librerías de CAPICOM. Estas librerías llamadas CryptoAPI son necesarias para las secuencias de comandos del Certification Autority y para crear secretos entre el servidor de Radius y los puntos de acceso.

Simplemente bajaremos las CAPICOM de Microsoft (capicom_dc_sdk.msi) y las instalaremos. Descargar las CAPICOM según el idioma de nuestro servidor Windows 2003 Server.

Instalación de las MSS WLAN-PEAP Tools

Descargaremos de Microsoft estas Tools (Securing_Wireless_LANs_with_PEAP_and_Passwords_v1.6.zip) desde el centro de descarga de Microsoft.

Una vez descomprimido el Zip instalaremos el .msi que hay dentro. También hay unos archivos PDF con documentación que puede interesarnos.
Por defecto estas Tools se guardarán dentro de C:\Program Files\Microsoft\Microsoft WLAN-PEAP Tools.

Ejecutaremos el archivo *CreateShortcut.cmd* que nos creará un acceso directo en el escritorio para ir trabajando desde allí.

Como veis hay un montón de scripts escritos en Windows Script Host que nos simplificarán el trabajo de configuración de nuestra infraestructura Wifi. Los dos programas que utilizaremos serán el *MSSSetup.cmd* y el *MSSSTools.cmd* que simplemente son archivos batch con llamadas a estos scripts.

Instalación de los miembros y grupos

En este punto crearemos los grupos de Active Directory que tendrán acceso a la Wifi. Una vez creado estos grupos, todos los usuarios que estén dentro del grupo “Wireless Access” tendrán acceso a conectarse a la Wifi.

- Abrimos el Shell del escritorio MSS WLAN Tools
- Ejecutamos el comando *MSSSetup CreateWLANGroups*.

Instalación de la consola de administración de directivas de grupo y las herramientas de soporte técnico de Windows 2003 Server

Instalaremos ahora la GPMC (Group Management Police Console) que será necesario para configurar los objetos de directiva de grupo. Tambien necesitaremos las Windows Support Tools.

- Descargar del centro de descargas de Microsoft el GPMC (gpmc.msi). Seleccionar el idioma correcto según el servidor.
- Instalar el *gpmc.msi*
- Para instalar las Support Tools hay que ir al CD de instalación de Windows 2003 Server y ejecutar *D:\support\tools\supptools.msi*

Importación de la directiva de grupo de la configuración de seguridad

Ahora lo que haremos es importar una nueva política de seguridad a nuestro dominio. Más adelante instalaremos otra. En total son dos: IAS Server Security Policies y IAS Certificate Autoenrrolement Policy.

- Desde las MSS WLAN Tools ejecutaremos *MSSetup ImportSecuriyGPO*
- Abriremos la "Administración de Directivas" de grupos situado en las "Herramientas Administrativas" de Windows.
- En el árbol, abrir "Domains" y seleccionar tú dominio. Botón derecho y seleccionar "Vincular objeto de directiva de grupo existente".
- Seleccionar "Directiva de seguridad del servidor IAS" y pulsar aceptar.
- En el panel de la derecha ("Objetos de directiva de grupo vinculados") seleccionar la política que acabamos de añadir y pulsar el botón Mover hacia arriba para situar esta política al princio de la lista.
- Cerrar la consola y desde una session de dos ejecutar *gpupdate /force*.

Instalación de la entidad emisora de certificado

En prerrequisitos hemos dicho que hay que tener instalado el software de los "Servicios de Certificate Server" y de "Internet Authentication Service". Estos dos software deben instalarse de desde "Agregar/Quitar programas" y con la ayuda del CD de instalación de Windows 2003 Server. Antes de continuar aseguraté de tener esto instalado.

- Abrimos la MSS WLAN Tools y creamos una autoridad de certificación con el comando *MSSetup InstallCA*.
- Nos pedirá que introduzcamos el nombre del la autoridad de certificación. Por ejemplo "Mi empresa CA".
- Verificamos la instalación con *MSSsetup VerifyCAInstall*.

Ahora configuraremos unos parámetros de la entidad emisora de certificados que deben establecerse una vez instalada.

- Ejecutamos *MSSsetup ConfigureCA* para terminar de configurar el servicio de certificados.
- Ejecutamos *MSSsetup ImportAutoenrollGPO* para crear la política IAS Certificate Autoenrrolement Policy.
- Ahora lo que tenemos que hacer es añadir esta nueva política a nuestro dominio.
- Abriremos la "Administración de Directivas" de grupos situado en las "Herramientas Administrativas" de Windows.
- En el árbol, abrir "Domains" y seleccionar tú dominio. Botón derecho y seleccionar "Vincular objeto de directiva de grupo existente".
- Seleccionar IAS Certificate Autoenrrolement Policy y pulsar aceptar.
- En el panel de la derecha (Objetos de directiva de grupo vinculados) seleccionar la política que acabamos de añadir y pulsar el botón Mover hacia arriba para situar esta política al princio de la lista.
- Cerrar la consola y desde una sesión de dos ejecutar *gpupdate /force*.
- Para finalizar verificaremos la instalación con un *MSSsetup VerifyCAConfig*.

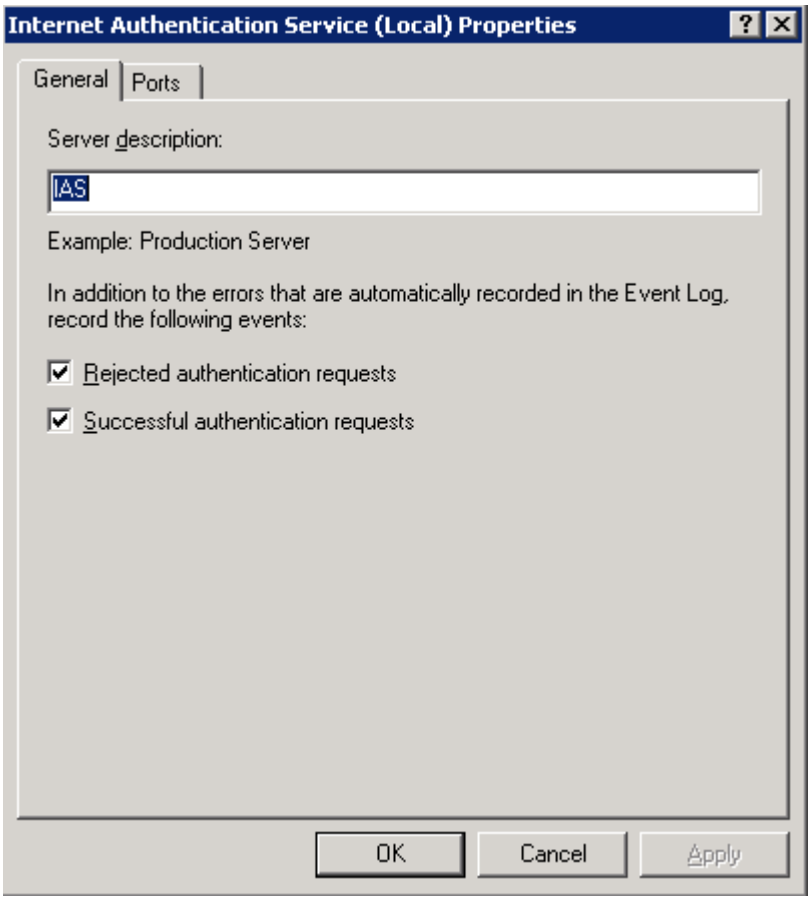
Instalación de IAS

Antes de instalar IAS y configurar el Radius hay que asegurarse que todo lo que hemos estado haciendo es correcto y el entorno esta perfecto para comunicar IAS con nuestro domino.

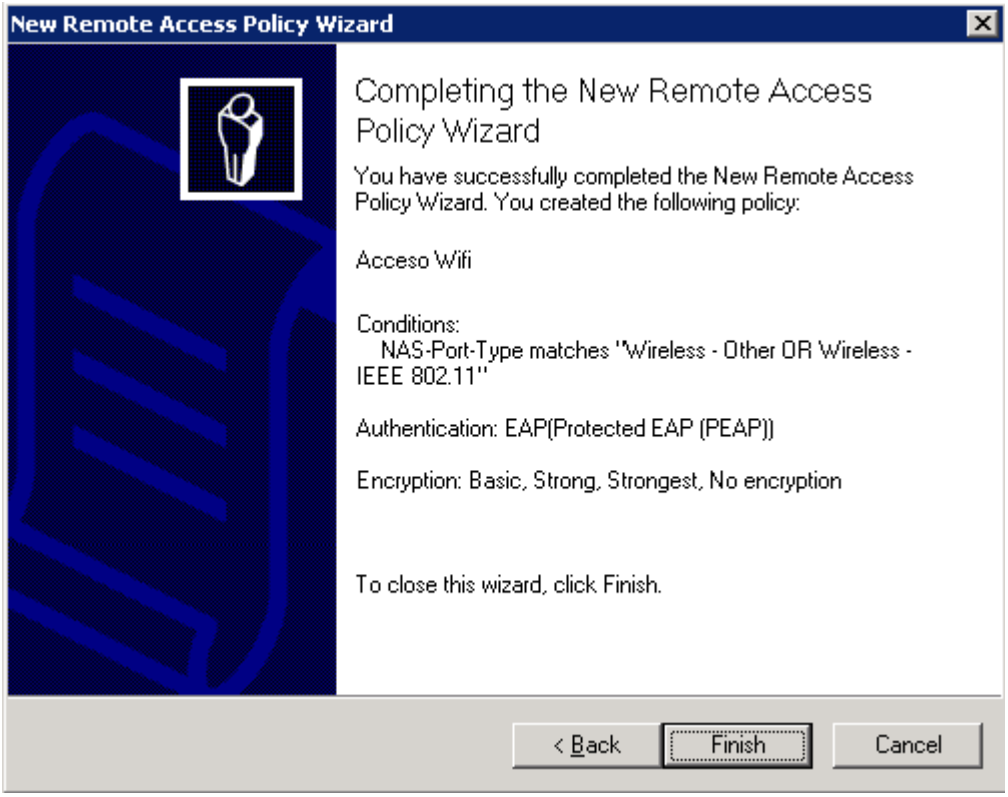
- En las MSS WLAN Tools ejecutamos *MSSsetup CheckIASEnvironment* para verificar el entorno.
- Si no tenemos el IAS instalado puedes utilizar *MSSsetup InstallIAS* para instalarlo. Este paso solo es necesario si no lo tienes instalado. Necesitarás también el CD de instalación de Windows 2003 Server ya que durante el proceso de instalación lo pedirá.
- Para comprobar que está correctamente instalado podemos arrancar el "Servicio de autentificación de Internet" desde las "Herramientas Administrativas".
- El siguiente paso es decirle al IAS que su base de datos de usuario se encuentra dentro del Active Directory. Para ello desde la consola del IAS hacemos "Registrar con Active Directory" dentro del menú Acciones. Este paso lo haremos si no tenemos IAS registrado dentro de AD.

En este punto empieza la parte un poco más complicada pues es la configuración de IAS.

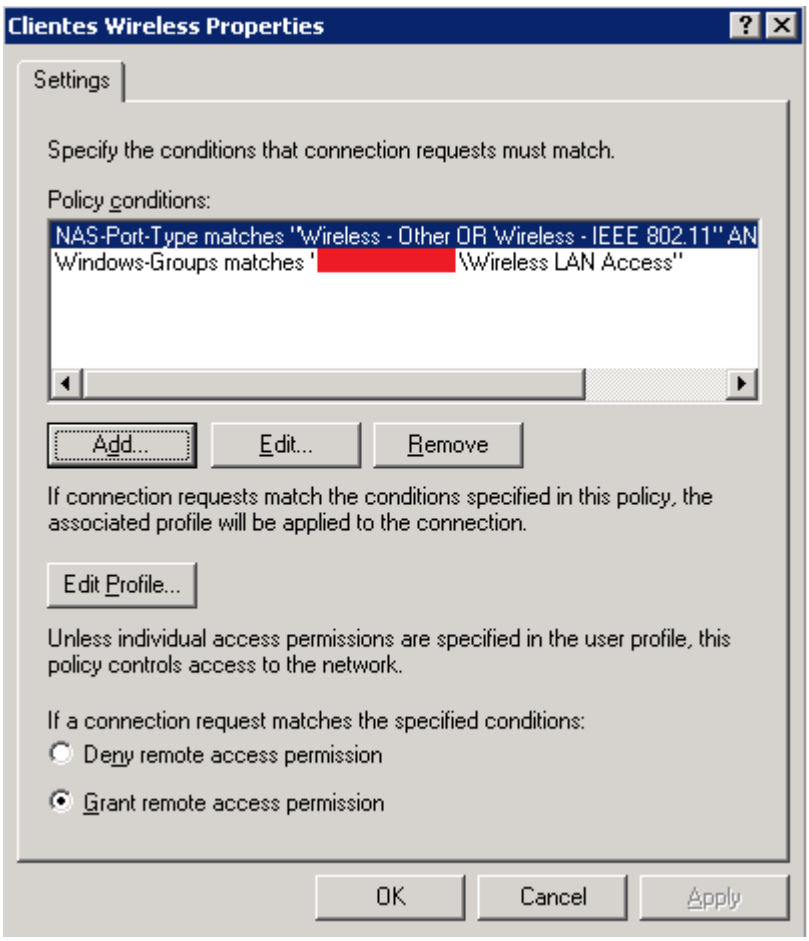
- Arrancamos IAS y seleccionamos Internet Authentication Service (local) y hacemos Action → Properties. Nos aseguramos de tener los dos checkboxs marcados.



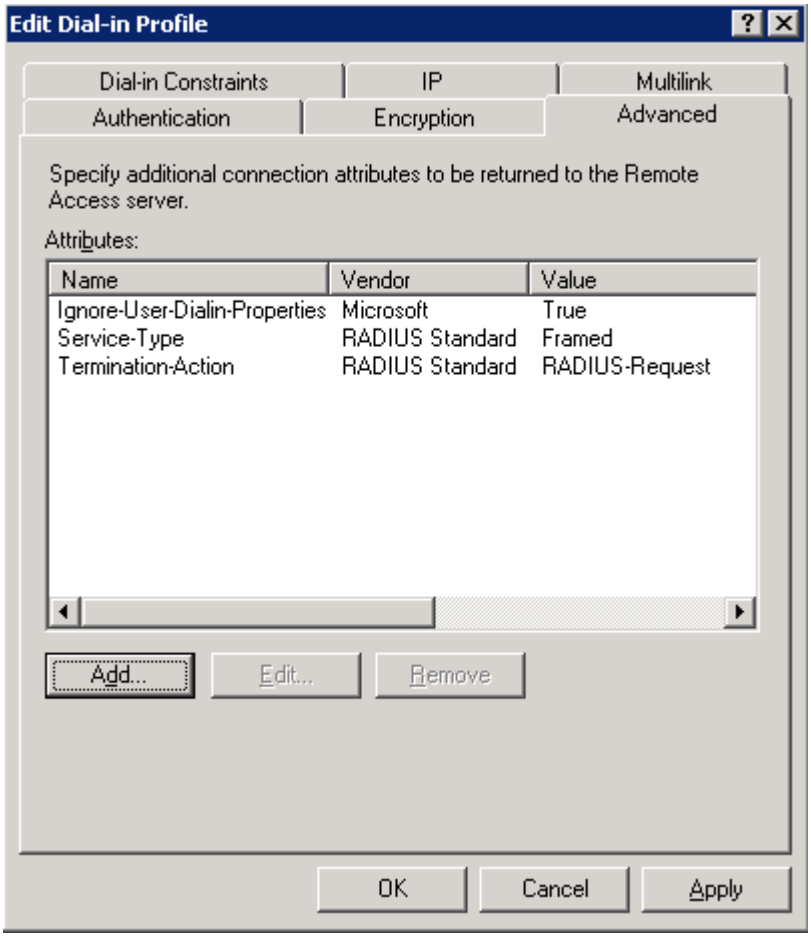
- Nos situamos en "Remote Access Polices" y creamos una nueva política de acceso remoto desde Action → New remote access police. Se nos abrirá un wizard que nos guiará por la política. Le daremos un nombre a la política, por ejemplo "Acceso Wifi". Le diremos que utilice el wizard para crear un política típica.
- Cuando pregunte el método de acceso remoto seleccionaremos Wireless.
- Seleccionar acceso por usuarios.
- Cuando pida el método de autentificación, seleccionar Protect EAP (PEAP). Al finalizar el Wizard tenemos que tener esto:



- Aun nos quedan unas cuantas cosas por configurar en esta política. Hacemos doble clic en la política "Acceso Wifi" y configuramos una nueva condición para la directiva. Para ello pulsamos en el botón Agregar y seleccionamos "Windows-Grupo". En "Windows-Grupo" seleccionaremos al grupo "Wireless LAN Access" de nuestro dominio.



- Ahora pulsamos en Editar perfil y en la pestaña Restricciones de marcado ponemos 15 minutos en el tiempo de espera de session (session timeout).
- En la pestaña Advanced añadimos un par de nuevos atributos. Añadiremos el atributo “Service-Type” con el valor “Framed” y también añadiremos el atributo “Termination-Action” con el valor “RADIUS-Request”.



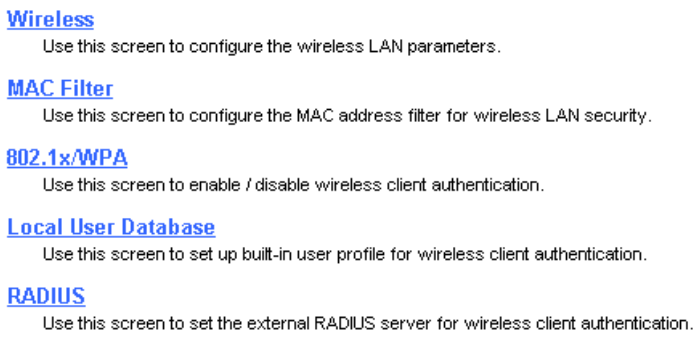
El último paso en IAS es crear un cliente de RADIUS, que en nuestro caso será un punto de acceso Wifi.

- Desde el MSS WLAN Tools ejecutamos *MSSTools AddRadiusClient*. Nos preguntará la dirección IP que le hemos puesto al punto de punto de acceso. También nos proporcionará una contraseña de RADIUS que la tendremos que anotar para configurarla en el punto de acceso y así permitir la comunicación RADIUS-punto de acceso.

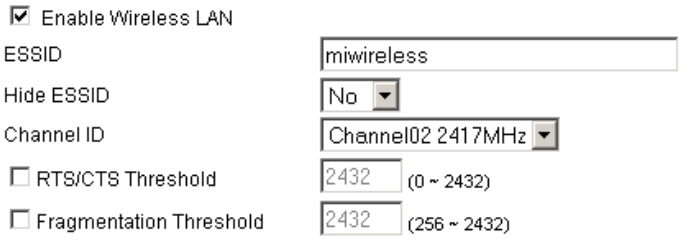
Configuración del punto de acceso Wifi

Es el momento de configurar el punto de acceso. En mi caso configuraré un router Zyxel. Para la configuración estándar le pondremos un password al administrador y le pondremos una dirección IP de nuestra subred.
Comprobaremos que desde el servidor Windows 2003 Server hay conectividad con el punto de acceso haciendo un ping.

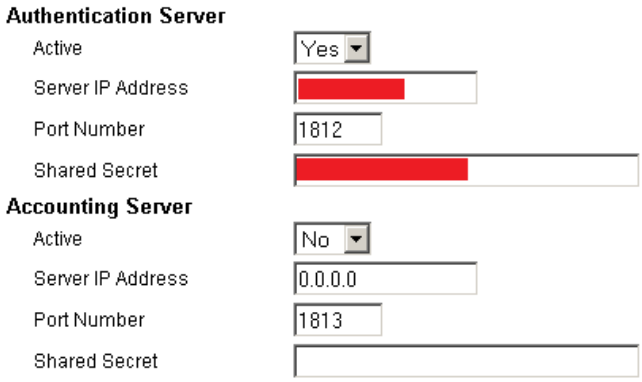
El menú de configuración de la wireless es el siguiente:



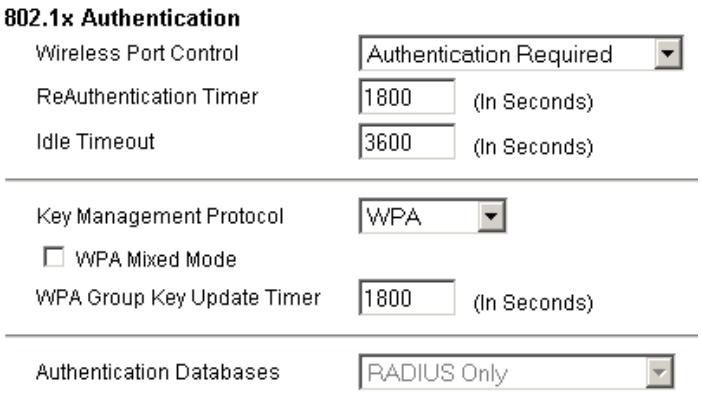
- En el apartado de Wireless configuraremos un SSID.



- En el apartado de RADIUS, le diremos al punto de acceso que consulte con la IP de nuestro servidor Windows 2003 Server. En "Shared secret" colocaremos la contraseña que habíamos anotado anteriormente.



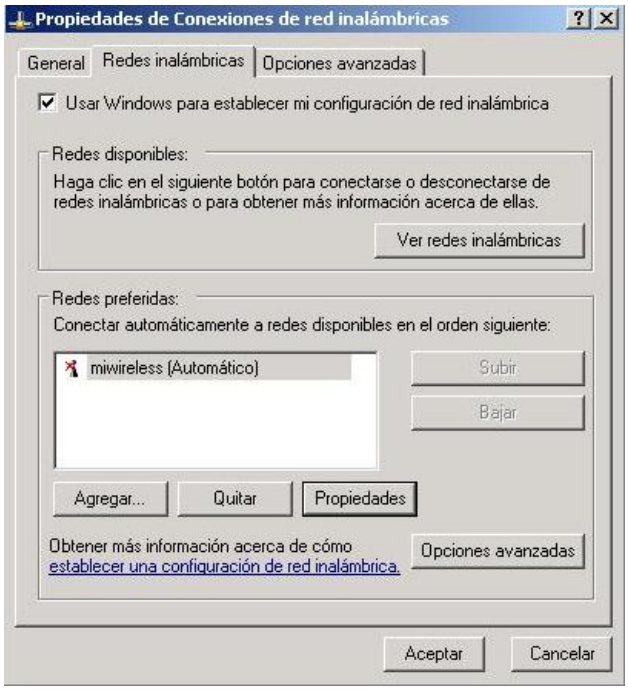
- Por último desde la opción 802.1x/WPA le diremos que utilice la autentificación.

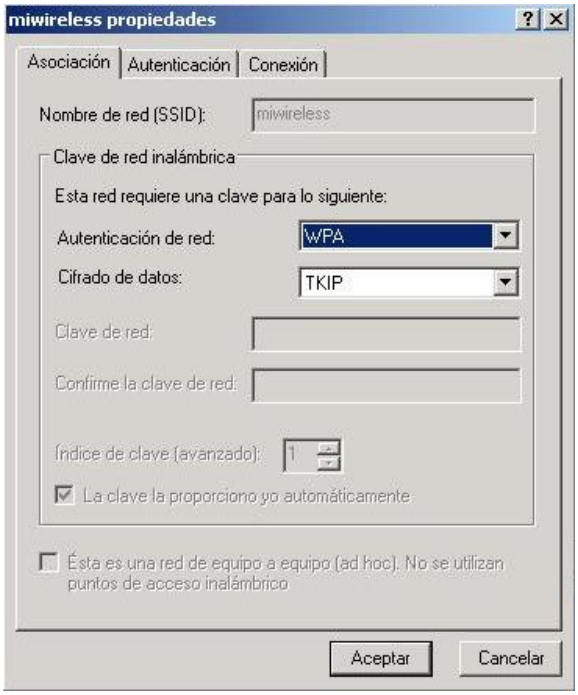


Configuración del cliente de Wifi

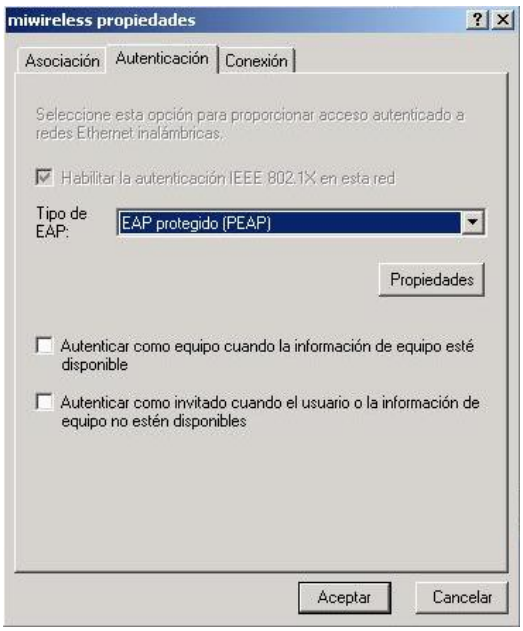
Una vez configurado el punto de acceso ya estamos en disposición de ir por ejemplo a nuestros portátiles Wifi y configurar el sistema operativo para conectarnos a nuestra Wifi de forma correcta. Supondré que el portátil tiene un Windows XP. Una vez arrancado y habilitada la interfaz Wifi le decimos que detecte las redes cercanas. Hemos de detectar nuestra red "miwireless".

- Una vez detectada pulsamos en Propiedades para repasar los parámetros de conexión de esta conexión.

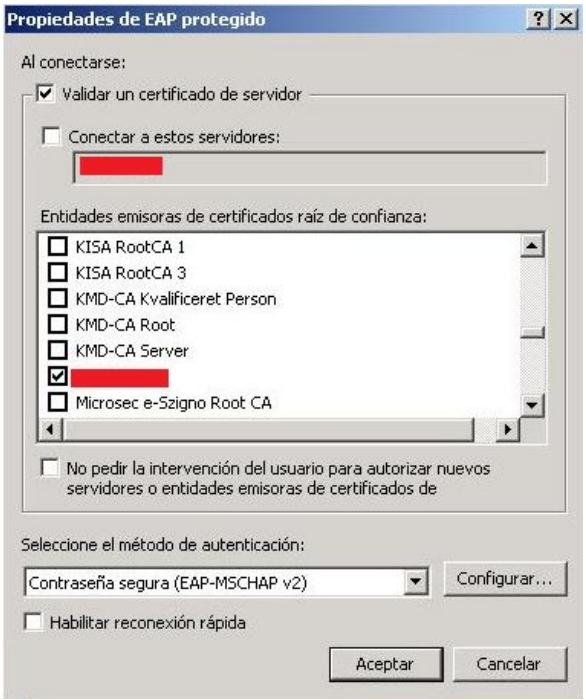




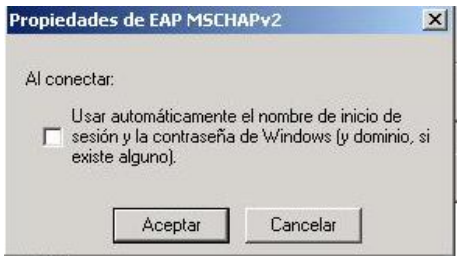
- Tenemos que asegurarnos que tenemos como método de autentificación WPA y como método para el cifrado TKIP.
- En la pestaña de Autentificación tendremos que seleccionar EAP protegido (PEAP) y desmarcar los dos checkbox que hay.



- Luego pulsamos el botón propiedades de EAP protegido y nos aparecerá una ventana como esta. Aquí tenemos dos posibilidades para "Validar un certificado de servidor". Podemos validarlo o no validarlo. Si lo validamos, tendremos que instalar el certificado que hemos generado para la autoridad de certificación CA he instalarlo en todo los portátiles como una "Autoridad de certificación raíz de confianza". Si no queremos instalarlo, le diremos que no valide el certificado. Por ejemplo esto lo haremos cuando vengan portátiles de consultores o de gente externa en la que no podemos instalar nada porque los portátiles no son nuestros.



- Luego seleccionaremos como método de autentificación EAP-MSCHAP v2 y pulsaremos Configurar.



- En propiedades de MSCHAP también tenemos dos posibilidades. Si marcamos el checkbox automáticamente utilizaremos nuestro usuario y contraseña del dominio para validarnos en la Wifi. Si el portátil no esta registrado en el dominio y hemos entrado en el con un usuario local, entonces al entrar en la Wifi nos pedirá un nombre de usuario, una contraseña y un dominio valido.

Crear usuarios para la Wifi

Como he dicho al empezar el manual, los usuarios que tienen acceso a la Wifi son los usuarios que tengamos ya creados dentro del Active Directory. Para que tengan acceso, simplemente basta con editar las propiedades del usuario y decirle que pertenece al grupo "Wireless Access".

Otra cosa que podemos hacer es crear un usuario genérico llamado "wifi" con el mínimo de permisos para poder prestarlo en cualquier momento a alguien externo a la empresa que tenga que conectarse para poder navegar por Internet.

Problemas

Para resolver cualquier problema lo mejor es repasar todos los puntos de este manual y sobre todo la documentación de 802.1x del TechNet de Microsoft.

También recomiendo revisar el visor de sucesos del servidor porque allí encontrarás los errores que puedan haber en el IAS. Otro log que se puede consultar es el visor de sucesos del punto de acceso wifi.