CAPÍTULO 8 – CONTROL DE ACCESO

8.1.- Introducción.

El estándar IEEE 802.1X es una norma del IEEE que define el mecanismo de control de acceso a redes basado en puertos. Mediante él se exige autenticación antes de dar acceso a una red. No se pueden enviar ni recibir tramas en un puerto de conmutación si el proceso de autenticación ha fallado. A pesar de que se diseñó para redes Ethernet fijas, este estándar se ha adaptado para su uso en redes LAN inalámbricas que hagan uso del estándar IEEE 802.11.

En relación con la tecnología de transmisión WLAN, en los últimos años han ido apareciendo una serie de estándares o especificaciones que tratan de cubrir las distintas áreas de esta tecnología. Sin embargo, el uso de un canal compartido y de elementos de acceso a la red cableada directamente accesibles por cualquier persona plantea también ciertos problemas de seguridad que deben ser resueltos.

En general, el mecanismo más utilizado para realizar un control de conexiones ha sido el uso de bases de datos en las que se introducen manualmente los datos de los usuarios autorizados, ya sean sus identificadores de usuario (Access Control Lists, ACLs) o direcciones MAC. Sin embargo, esta solución presenta problemas de escalabilidad cuando las bases de datos crecen demasiado o los usuarios cambian frecuentemente, además del trabajo necesario por parte de los administradores de red para configurar correctamente el control de acceso.

802.1X plantea un escenario con tres entidades básicas como son el cliente (denominado en textos anglosajones Supplicant, suplicante), el elemento que proporciona la conectividad a la red (punto de acceso o conmutador), y el servidor de autenticación encargado de averiguar si un determinado cliente ha sido autorizado a hacer uso de dicha red. En lo que respecta a los protocolos que componen la especificación 802.1X, la propuesta es bastante flexible al no limitar los mecanismos de autenticación a ninguna solución concreta, sino que es posible hacer uso de cualquier tipo de especificación convenientemente adaptada al marco 802.1X. Esta flexibilidad va a permitir hacer uso de protocolos basados en certificados digitales como elementos fundamentales a la hora de constatar la autenticidad de los participantes.

La importancia del uso de certificados digitales radica en su capacidad para aliviar los problemas de escalabilidad asociados a las soluciones fundamentadas en el uso de bases de datos. Estos elementos permiten que un usuario desconocido para el sistema pueda hacer uso de la red con sólo proporcionar el certificado adecuado. Además en este certificado pueden

incluirse ciertos atributos acerca del usuario, como el tiempo máximo que puede utilizar la red, los servicios a los que puede acceder o los recursos que puede utilizar.

8.2.- Relación entre 802.1X y 802.11i.

8.2.1.- WEP (Wired Equivalent Privacy)

WEP es parte del estándar 802.11, fue incluido como estándar de seguridad opcional para redes inalámbricas. Inicialmente los desarrolladores recomendaban usar filtrados de direcciones MAC en lugar de WEP. Aquella solución se vio desbordada en empresas donde tenían que controlar todas y cada una de las direcciones MAC de los distintos equipos en el área de cobertura de la red inalámbrica. Esto junto a herramientas que permitían detectar direcciones MAC aceptadas y hacerse pasar por otros equipos, avivó el interés por WEP.

Inicialmente, WEP fue diseñado para proporcionar un nivel de seguridad equivalente a las redes cableadas, de ahí su nombre. Provee estándares para autenticación entre los clientes de red y los puntos de acceso, además de encriptación de paquetes. Internamente WEP utiliza el algoritmo RC4 para cifrar y descifrar los paquetes 802.11.

WEP presenta 3 puntos principales en la seguridad de las redes WLAN:

- Autenticación, antes de comenzar una comunicación entre el cliente y el punto de acceso existe una fase de autenticación donde la estación cliente envía una petición de autenticación al punto de acceso. Éste responde con un número aleatorio conocido como desafío. El cliente debe responder al desafío, enviando el mismo número al punto de acceso pero cifrado mediante la clave WEP. El punto de acceso verificará que el desafío fue correctamente cifrado. Si todo ha ido satisfactoriamente, el cliente queda autenticado.

- Cifrado, una vez que el cliente es autenticado y asociado al punto de acceso, podrá comunicarse con la red a través del punto de acceso. En esta fase es donde se implementa todo el proceso de cifrado mediante RC4. Inicialmente WEP empleaba claves de 40 bits, que se concatenan a un vector de inicialización (IV, Initialization Vector) de 24 bits, teniendo un total de 64 bits. Más tarde se emplearon claves de 104 y 232 bits, alcanzando respectivamente una protección de 128 y 256 bits.
  De todas formas, el tamaño de la clave no es la principal limitación de seguridad de WEP, para evadirla en clave de mayor longitud basta con capturar un mayor número de paquetes. Incluso hay debilidades en WEP, como colisiones IV o paquetes modificados que no son favorecidas en absoluto empleando claves de mayor longitud.

- Integridad, un campo ICV (Integrity Check Value) acompaña a los datos enviados, el objetivo de esos 32 bits es asegurar que el paquete no es alterado durante la transmisión. Si un solo bit del paquete cambia, el mensaje será descartado por el receptor. El ICV es simplemente un código de redundacia cíclica mejorado, ya que se encripta como parte del paquete.

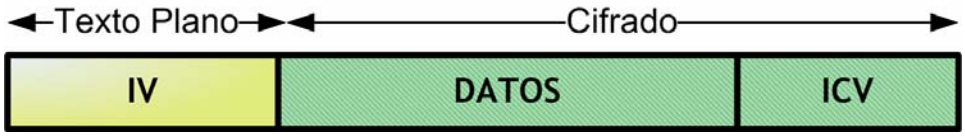

Figura 8.1: Trama 802.11 encriptada mediante WEP.

Sin embargo, a medida que se popularizó el uso de WEP para encriptar las comunicaciones inalámbricas surgieron multitud de deficiencias en su estructura que posibilitaron a los atacantes vulnerar con facilidad la encriptación que lleva a cabo sobre las comunicaciones. La forma principal de ataque consiste en estimular al punto de acceso con determinados tipos de paquetes, para después capturar el tráfico y poder extraer la clave WEP utilizada. Además las claves WEP son engorrosas de cambiar frecuentemente. Con la finalidad de solucionar dicho problema, se recomienda el uso de claves de longitud no inferior a 128 bits así como su continua actualización con el fin de limitar la cantidad de información cifrada con la misma clave.

En respuesta a la falta de seguridad en el uso de WEP, el IEEE diseñó un nuevo estándar de seguridad conocido como 802.11i, donde la especificación 802.1X juega un papel principal.

8.2.2.- El estándar 802.11i

El nuevo estándar de seguridad, 802.11i, que aparece en Junio de 2004, corrige las vulnerabilidades encontradas en WEP. Se divide en 3 grandes categorías:

- TKIP (Temporary Key Integrity Protocol), es el protocolo que soluciona las debilidades de WEP. TKIP puede emplearse con equipos 802.11 mediante una actualización de controladores y/o firmware. Proporciona integridad y confidencialidad.

- CCMP (Counter Mode with CBC-MAC Protocol), es un nuevo protocolo diseñado desde cero que emplea AES (Advanced Encryption Standard) y su algoritmo de encriptación. Requiere más requisitos computacionales que RC4 (empleado en WEP y TKIP), y por tanto una actualización en el hardware 802.11. Algunos controladores de dispositivos son capaces de implementar CCMP en software. CCMP también proporciona integridad y confidencialidad.

- Control de acceso, ya sea empleando TKIP o CCMP el estándar 802.1X se empleará para los procesos de autenticación.

Además, se presenta un método de cifrado opcional conocido como WRAP (Wireless Robust Authentication Protocol) que puede emplearse en lugar de CCMP. WRAP fue la propuesta inicial al protocolo basado en AES, pero fue reemplazado por CCMP debido a cuestiones de propiedad intelectual en WRAP.

Por otra parte, para asegurar unas determinadas políticas de seguridad empleando algoritmos de cifrado e integridad, es necesario tener un conjunto de claves. El estándar 802.11i especifica el método a seguir para la gestión y obtención de las claves.

8.2.3.- WPA y WPA2

La industria no tuvo tiempo de esperar a que el estándar 802.11i estuviera finalizado, necesitaban corregir los problemas de WEP lo antes posible.

La Wi-Fi Alliance, se anticipó a la norma y tomó las bases del estándar creando WPA (Wi-Fi Protected Access). Una condición fundamental era la compatibilidad con el hardware 802.11 existente, por tanto WPA es en esencia TKIP + 802.1X.

Para pequeñas oficinas, redes ad-hoc o domésticas, es posible emplear lo una clave pre-compartida, PSK (Pre-shared Key), que elude el proceso de autenticación 802.1X. Se conoce como WPA-Personal o WPA-PSK

Dado que WPA no es una solución definitiva a largo plazo, se habla también de la utilización de CCMP + 802.1X bajo el nombre de RSN (Robust Secure Network). Asimismo a WPA se conoce como TSN (Transition Security Network). Para evitar la confusión de nombres en el mercado, RSN es más conocido como WPA2.

En definitiva se tiene lo siguiente:

WPA = TKIP + 802.1X
WPA2 = CCMP + 802.1X

Todos estos nombres han provocado la saturación del uso de siglas para las soluciones de seguridad en los equipos de los fabricantes. No hay que perder de vista que el estándar a seguir para seguridad en redes inalámbricas es el 802.11i, y que 802.1X forma parte de él para proporcionar autenticación y control de acceso.

8.3.- Funcionamiento de la especificación 802.1X.

A pesar de que la especificación 802.1X, como hemos explicado anteriormente, puede aplicarse sobre redes fijas e inalámbricas, nos centraremos un poco más en el funcionamiento sobre redes inalámbricas

debido a que en los últimos años este tipo de redes han ido aumentando en popularidad y aún no presentan un protocolo de autenticación realmente seguro. La especificación 802.1X viene a mejorar la seguridad para este tipo de redes.

El estándar 802.11 describe una arquitectura basada en unidades elementales, o celdas, donde un conjunto de dispositivos intentan acceder al medio haciendo uso de una misma función de coordinación. Estas unidades pueden conectarse entre sí mediante una red o sistema de distribución. El elemento que sirve de puente entre la red inalámbrica y la red cableada es el punto de acceso, el cual jugará también un papel crucial en el proceso de control de conexiones.

Antes de que un equipo que se conecta a un punto de acceso pueda transmitir los datos, éste debe realizar una fase de asociación en la que da a conocer su identificador al punto de acceso para que éste informe al resto de la red de que dicho equipo se encuentra bajo su área de cobertura. Es tras esta fase cuando debe realizarse el proceso de control de acceso para ver si realmente el cliente tiene permiso para hacer uso de la red.

Uno de los mecanismos utilizados por las redes 802.11 para intentar proporcionar un cierto nivel de seguridad es el cifrado de los datos que se transmiten entre el cliente y el punto de acceso. Para ello se utiliza el protocolo WEP. Como hemos visto anteriormente, en los últimos años se han descubierto varias vías de ataque que permiten a un intruso descifrar la comunicación protegida mediante WEP.

De cualquier forma, IEEE 802.1X ofrece la posibilidad de configurarse para la gestión dinámica de claves, es decir, el servidor de autenticación es capaz de proporcionar las claves de sesión al punto de acceso. Éste se las enviará al cliente, que podrá cambiar automáticamente las claves WEP para que no haya tiempo de suficiente de ser descubiertas por un atacante externo.

La especificación IEEE 802.1X permite utilizar diferentes mecanismos de autenticación. Su funcionamiento se basa en el concepto de puerto, visto éste como el punto a través del que se puede acceder a un servicio proporcionado por un dispositivo, que en este caso será el punto de acceso. En principio todos los puertos están desautorizados, excepto uno que el punto de acceso utiliza para comunicarse con el cliente.

Cuando un nuevo cliente entra en su área de cobertura, le pasa al punto de acceso información de autenticación que éste reenvía al servidor de autenticación. Cuando le contesta, si la respuesta es que el cliente puede hacer uso de la red, el punto de acceso autoriza un puerto para que lo utilice el cliente.

La figura siguiente muestra un esquema de la arquitectura 802.1X:

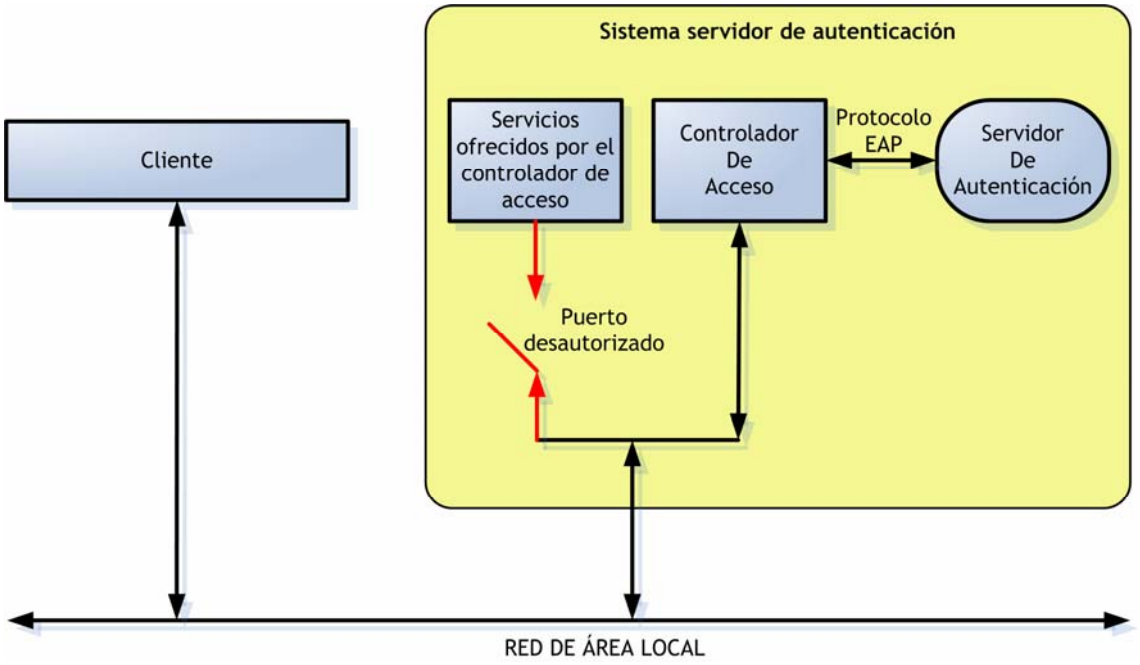

Figura 8.2: Arquitectura 802.1X

En esta arquitectura, la información de autenticación se encapsula en el protocolo EAP (Extensible Authentication Protocol), un mecanismo genérico de transmisión de datos de autenticación que puede ser implementado en distintos subprotocolos entre los que, por ejemplo, se encuentra EAP-MD5, que basa la autenticación del cliente en el uso de login y password, o EAP-TLS, que se basa en el uso del protocolo TLS (Transport Layer Security) y permite autenticación mutua entre los dos extremos. Tratamos aquí el uso de EAP-TLS principalmente por dos motivos: el primero es que durante la fase de establecimiento de la conexión este protocolo hace uso de certificados X.509 para identificar a las partes, lo cual constituye un mecanismo robusto de autenticación; el segundo es que dicha fase genera una clave compartida por los dos extremos que puede utilizarse para derivar claves para el cifrado de las transmisiones inalámbricas, lo cual es uno de los objetivos de la arquitectura.

Finalmente, los paquetes EAP se transmiten mediante el protocolo EAPOL (EAP Over LAN), el cual especifica cómo encapsular los paquetes EAP en una red de área local. En el caso de usar una red inalámbrica 802.11, se emplearía EAPOW (EAP Over Wireless).

8.3.1.- Servidores de autenticación.

Aunque en la especificación 802.1X se habla de los servidores de autenticación en términos genéricos, en la práctica se trata de elementos diseñados según los criterios del marco AAA (Authentication, Authorization and Accounting). Este marco define los elementos básicos necesarios para autenticar usuarios, manejar peticiones de autorización y realizar la contabilidad del sistema. Un servidor AAA debe ser capaz de recibir peticiones, examinar el contenido de dichas peticiones, determinar qué

autorización se está pidiendo, recuperar las políticas que necesite de un repositorio, evaluar la petición y obtener la respuesta a la petición, o bien reenviar la petición a otro servidor AAA.

Para conocer porqué la arquitectura AAA es mejor que otras, es necesario saber qué se usaba anteriormente. Antes de utilizar AAA, equipos individuales, los mismos equipos que hacían las veces de clientes en ciertas ocasiones, tenían que usarse para autenticar a los usuarios. Sin un estándar fijo, cada máquina tenía un método de autenticación: algunas usaban perfiles de usuarios, otros podrían usar protocolos como CHAP (Challenge/Handshake Authentication Protocol), otras una base de datos SQL interna, etc. El mayor problema que presenta este modelo es la escalabilidad, si se quería ampliar la red con otras máquinas cada una debía configurarse de forma distinta y a medida que aumentaba el número de usuarios era casi imposible controlar la autenticación de todos ellos en máquinas distintas. Se escribieron scripts a tal fin, pero no había una forma consistente de controlar el uso, autenticar usuarios automáticamente y proveer eficazmente de varios servicios.

El grupo de trabajo AAA fue formado por el IETF para crear una arquitectura funcional que terminara con las limitaciones de los sistemas antes mencionados. Obviamente, era necesario centrarse en descentralizar los equipos en redes heterogéneas. Los proveedores de acceso a Internet (ISPs) empezaron a ofrecer servicios distintos a la simple conexión telefónica de marcado, incluyendo RDSI, xDSL y acceso por cable y se hacía necesario por tanto un estándar para todos ellos a la hora de verificar, acceder y monitorizar a los usuarios. Así surge la arquitectura AAA.

La arquitectura AAA se centra en 3 aspectos cruciales del control de acceso: autenticación (authentication), autorización (authorization) y contabilidad (accounting). De una forma, simple, se puede decir que el modelo describe cómo unir estos tres elementos fundamentales.

Autenticación

La autenticación consiste en verificar la identidad de una máquina. Inicialmente se usaba el usuario y contraseña para tal fin, pero acabó convirtiéndose en inseguro para ciertas transacciones.

Una de las alternativas para implementar mecanismos de autorización, si no se quiere mantener una base de datos con los permisos de cada usuario, es la utilización de certificados digitales. Un certificado es una estructura que contiene información del usuario en cuanto a identidad o permisos, y que va firmado digitalmente por una entidad de confianza.

La clave de la autenticación es que permite que dos entidades únicas formen una relación de confianza entre ellas. Esa confianza entre sistemas permite funcionar a los equipos como servidores proxy (intermediarios), donde se permite hacer una petición en nombre de otro equipo autorizado para enlazar redes heterogéneas que soportan distintos clientes y servicios.

Autorización

La autorización implica usar un conjunto de reglas u otro tipo de plantillas para decidir lo que un usuario autenticado puede realizar en un sistema. El administrador de red es quien define esas reglas.

Dado que los certificados de clave pública X.509 (los más ampliamente extendidos) se utilizan exclusivamente para propósitos de identidad, se puede optar por el uso de certificados SPKI (Simple Public Key Infrastructure), una especificación que permite plasmar de forma sencilla los privilegios asociados a un usuario individual o a un grupo de usuarios en conjunto. Este tipo de certificados pueden ser utilizados también para representar la pertenencia de un usuario a distintos grupos de privilegios. La especificación SPKI además define un algoritmo para obtener decisiones de autorización en base a un conjunto de certificados presentados como pruebas, una solicitud de acceso y una política de seguridad del sistema. Se puede decir que los certificados SPKI aúnan autenticación y autorización.

Las llamadas "implementaciones inteligentes" de servidores AAA, contienen una lógica que analizará la petición de un equipo y proporcionará lo que pueda, no todo lo que pida. Es decir, si un cliente pide, por ejemplo, un enlace múltiple y sólo tiene permiso para uno punto a punto, el servidor será capaz de interpretar la petición, admitir uno de los enlaces y denegar el resto.

Contabilidad

Sobre el marco AAA existe la contabilidad, que mide los recursos que un usuario utiliza durante su acceso. Se incluyen la cantidad de tiempo de uso, o de datos que el usuario recibe o manda durante una sesión, etc. La contabilidad es llevaba a cabo registrando la estadísticas de una sesión y dicha información se empleará para control de autorización, facturación, análisis de preferencias, utilización de recursos y ampliación de capacidades de los sistemas.

El modelo AAA se apoya en la interacción cliente/servidor, en buenas implementaciones el cliente y el servidor nunca intercambian en general sus papeles. Los entornos clientes/servidor permiten un diseño balanceado. Los servidores pueden estar distribuidos o descentralizados a lo largo de la red, al contrario que en redes punto a punto donde se mezclan las características de clientes y servidores provocando grandes tiempos de espera o largos periodos de fallo del sistema.
Es posible también crear cadenas de servidores AAA, configurando un servidor AAA para que autorice que ciertas peticiones sean reenviadas a través de él hacia otro servidor AAA. Su gran utilidad queda patente al pensar en pequeños proveedores de servicios que pagan un alquiler a un proveedor dominante, si el pequeño proveedor no quiere compartir los datos de sus clientes pero quiere autenticarlos, tan sólo debe emplear una cadena de servidores AAA hasta el servidor del proveedor principal.

8.3.1.1 Servidores RADIUS.

RADIUS (Remote Access Dial-In User Server) es un protocolo encuadrado dentro del marco AAA y utilizado principalmente en entornos donde los clientes son elementos de acceso a la red (como los puntos de acceso). RADIUS usa una arquitectura cliente-servidor e incluye dos componentes: un servidor de autenticación y un protocolo cliente.

Los elementos de red mandan información al servidor cuando un nuevo cliente intenta conectarse, tras lo cual el servidor realiza el proceso de autenticación del usuario y devuelve al elemento de acceso la información de configuración necesaria para que éste trate al cliente de la manera adecuada. Toda la comunicación entre el elemento de acceso y RADIUS se encuentra cifrada mediante un secreto compartido que nunca se transmite por la red.

Las especificaciones RFC para el protocolo RADIUS establece las siguientes características:

- Se apoya en UDP y está no orientado a conexión.
- Usa un modelo de seguridad salto a salto.
- Es un protocolo sin estado, es decir, no guarda información de los parámetros de configuración, de transacciones o cualquier otro dato para la próxima sesión.
- Soporta los métodos de autenticación PAP y CHAP a través de PPP.
- Emplea MD5 en sus algoritmos.
- Proporciona unos 50 pares de atributos y valores con la posibilidad de crear parejas especificas para los fabricantes.
- Cumple el modelo AAA.

El uso de UDP en lugar de TCP, viene justificado por ciertas propiedades inherentes a RADIUS que también están presentes en UDP. RADIUS necesita que las peticiones que fallen en un servidor de autenticación primario sean redirigidas a uno secundario, y para conseguir esto, debe existir por encima de la capa de transporte del modelo OSI, una copia de la petición original. En definitiva, implica el uso de temporizadores de retransmisión. TCP consigue un transporte fiable de los paquetes de autenticación a costa de temporizadores que provocan un tiempo excesivo en autenticar, en caso de tener que redirigir peticiones a un servidor secundario de autenticación. Por eso se eligió UDP.

Además UDP tampoco mantiene el estado, al igual que vimos en las características de RADIUS. UDP permite abrir una sesión y mantenerse abierta durante todo el tiempo de una transacción.

La única parte negativa del uso de UDP es que los desarrolladores deben crear y controlar temporizadores de retransmisión, dicha capacidad se encuentra implementada en TCP, pero es un pequeño inconveniente si lo comparamos con la simplicidad que ofrece UDP para realizar el conjunto de operaciones en RADIUS.

EAP sobre RADIUS

EAP (Extensible Authentication Protocol) es una extensión de PPP que permite utilizar una gran variedad de protocolos de autenticación. PPP utiliza como método de autenticación el nombre de usuario/contraseña. Actualmente existe la necesidad de ampliar dicho método a otros, que resulten más seguros o cómodos para el usuario. Así fue diseñado EAP, basado en el protocolo PPP y proporcionando un marco generalizado para diversos métodos de autenticación. EAP sirve como soporte a protocolos propietarios de autenticación, gestiona las contraseñas en mecanismos de desafío-respuesta y es capaz de trabajar con tecnología de clave pública.

Con EAP estandarizado, la interoperabilidad y la compatibilidad de los métodos de la autenticación es más simple. Por ejemplo, si al intentar establecer una conexión se utiliza EAP como protocolo de control de acceso, el RAS (Servidor de Acceso Remoto) no necesitará conocer los detalles del método de autenticación a emplear, solamente el cliente y el servidor de la autenticación tienen que coordinarse. En EAP, un RAS reencamina los datos de autenticación hasta el servidor de autenticación local, el cual sabrá que método utilizar.

EAP aumenta más la seguridad de RADIUS, el conmutador o servidor de acceso se configura para emplear EAP y RADIUS como su proveedor de autenticación. Cuando un cliente intenta conectarse, se negocia el uso de EAP con el controlador RADIUS, de forma que el cliente enviará mensajes EAP al cliente RADIUS, y éste encapsulará el mensaje EAP en un mensaje RADIUS que enviará al servidor RADIUS. El servidor enviará de vuelta un mensaje RADIUS consecuente al cliente RADIUS, que formará un mensaje EAP para mandárselo al cliente.

Radius y LDAP

A la hora de administrar sistemas, existen problemas de eficiencia a la hora de tratar con distintas bases de datos de usuarios a través de múltiples plataformas. Lo ideal sería poder listar, configurar y administrar los usuarios desde un único conjunto de herramientas. Y por tanto el resto de aplicaciones sólo deberían acceder a una única base de datos que contiene a todos los usuarios.

El estándar LDAP (Ligthweight Directory Access Protocol) viene a conseguir precisamente eso. Lo hace mediante una base de datos basada en directorios que contiene los usuarios y su información asociada de una red concreta, y se accede a su información mediante consultas estándar, como puede ser SQL.

Existen implementaciones de RADIUS, tales como FreeRADIUS, que traen soporte para comunicaciones con bases de datos LDAP. De esa forma podremos autenticar los usuarios con bases de datos de otras aplicaciones, como puede ser un servidor de correo o similares.

8.3.2.- Topología de la red.

En la figura 8.3 se puede ver una topología típica donde se hace uso del estándar 802.1X donde existen varios puntos de acceso y un servidor de autenticación conectados mediante un sistema de distribución, y un conjunto de clientes que cuando entran por primera vez en el área de cobertura de un punto de acceso inician el proceso de conexión.

Este proceso consta básicamente de tres fases:

- Autenticación
- Autorización.
- Distribución de la clave de cifrado WEP.

Una vez conectado el cliente, el sistema realizará periódicamente un proceso de renegociación de la clave WEP. Del mismo modo, también gestionará la posibilidad de que el usuario se desplace hacia el área de cobertura de otro punto de acceso, todo ello con el fin de aprovechar la asociación para que el proceso de conexión a través del nuevo punto de acceso se realice de forma eficiente.

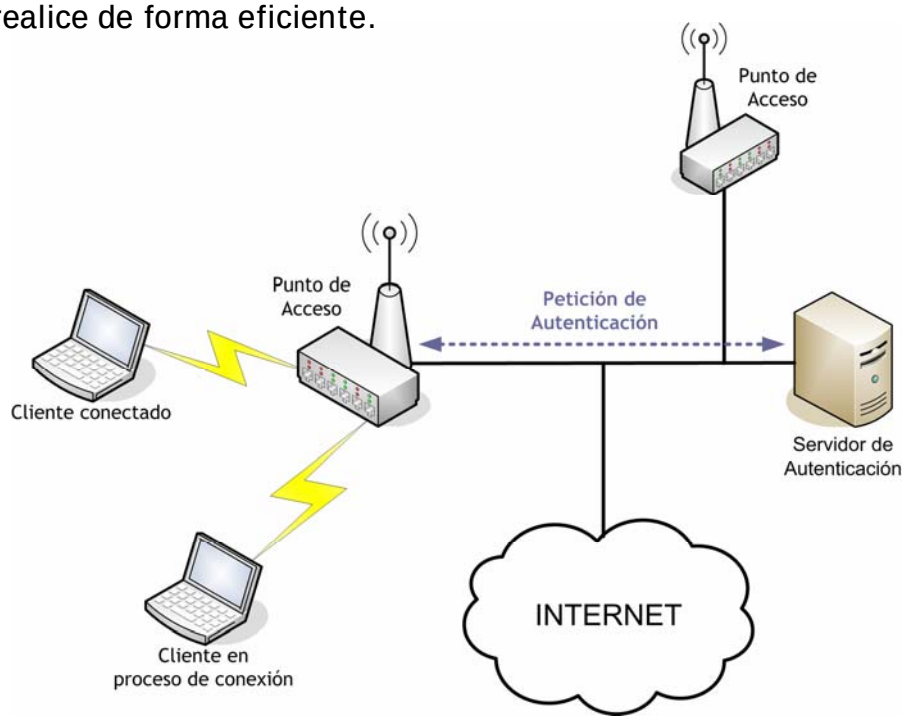

Figura 8.3: Topología de una red que emplea 802.1X.

En la figura 8.4 podemos apreciar el intercambio de mensajes que se produce entre el cliente, el punto de acceso y el servidor de autenticación antes de autorizar o desautorizar el acceso al puerto.

El estado del puerto de acceso comienza siendo desautorizado, donde todos los mensajes, salvo los paquetes 802.1X, son descartados.

Si un cliente no soporta el estándar 802.1X al intentar conectar con un puerto 802.1X desautorizado no podrá contestar al punto de acceso, de forma que no podrá acceder a la red.

Por otra parte, cuando un cliente 802.1X se conecta a un puerto que no utiliza el mismo estándar, terminará enviando tramas como si estuviera en estado autorizado. Antes de llegar a ese punto, el cliente enviará tramas de autenticación (EAPOL-Start) un número fijo de veces, cuando no reciba respuesta empezará el envío normal de tramas.

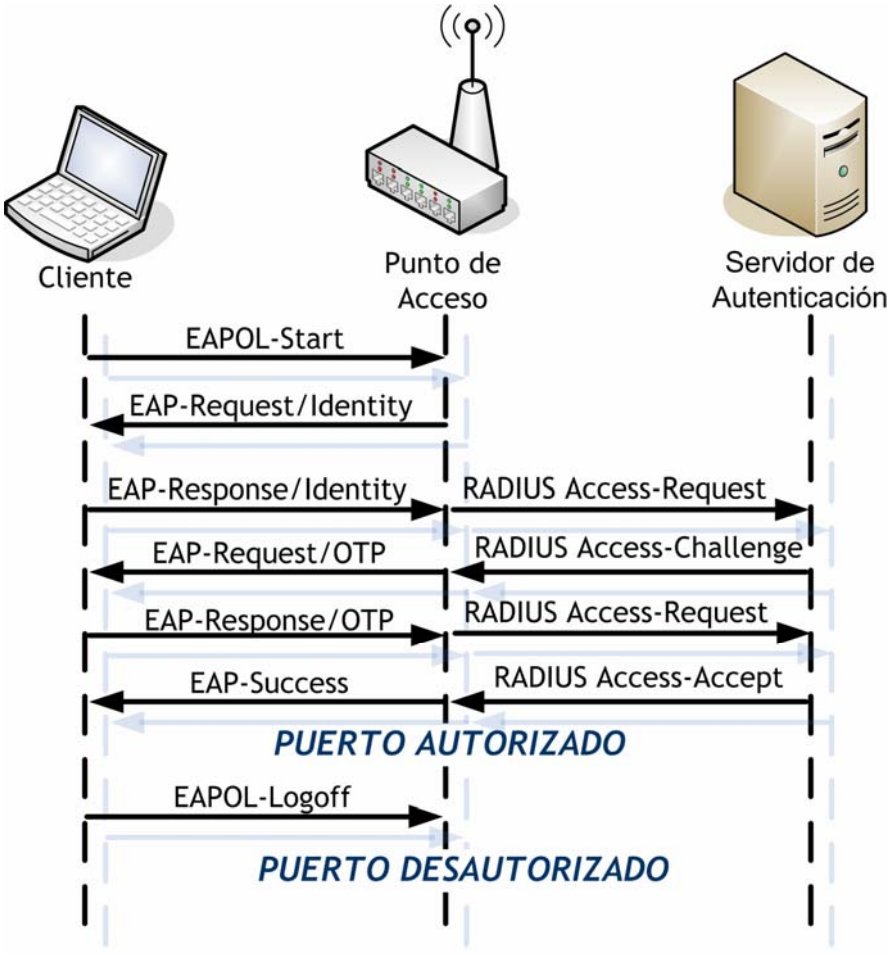

Figura 8.4: Intercambio de mensajes.

8.3.3.- Fases del estándar 802.1X

Comentaremos las distintas fases que se presentan en el siguiente diagrama:

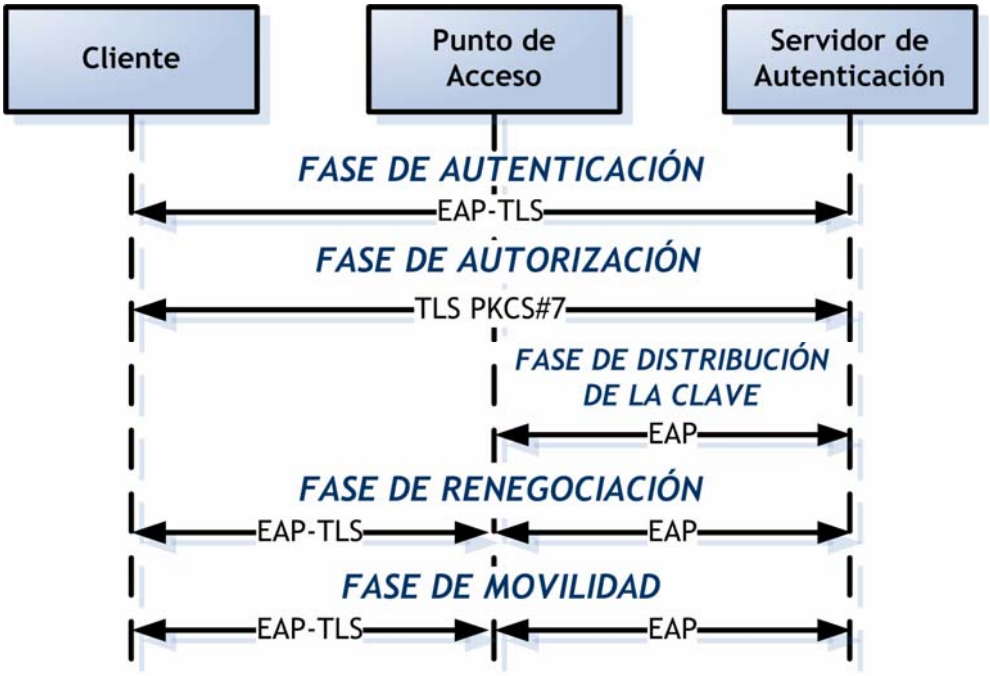

Figura 8.5: Fases protocolo 802.1X.

Fase de autenticación

La primera fase funciona siguiendo el estándar IEEE 802.1X, es decir, cuando el cliente entra en el área de cobertura del punto de acceso, este le pide su identidad, y el cliente se la proporciona.

Tras esta fase inicial se realiza el proceso de establecimiento de conexión TLS entre los extremos, donde según el estándar tanto el cliente como el servidor de autenticación se autentican mutuamente mediante certificados X.509 y negocian los parámetros de configuración necesarios para establecer el canal de comunicación seguro.

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

Fase de autorización

En esta fase, el cliente indica al servidor de autenticación cual es el tipo de conexión que desea en cuanto al ancho de banda requerido y el tiempo que va a estar conectado, junto con los certificados SPKI que demuestran que dicho usuario está autorizado a realizar el uso de la red que pide. Entonces el servidor evalúa los certificados y comprueba si todo es correcto y si el nivel de privilegios del cliente es el necesario, continuando

con el protocolo si todo va bien y desautorizando al cliente a acceder a la red si hay algún problema. De esta forma no es necesario acceder a ninguna base de datos de usuarios para comprobar los permisos de los mismos, sino que sólo se necesita confiar en las entidades emisoras de dichos certificados de autorización.

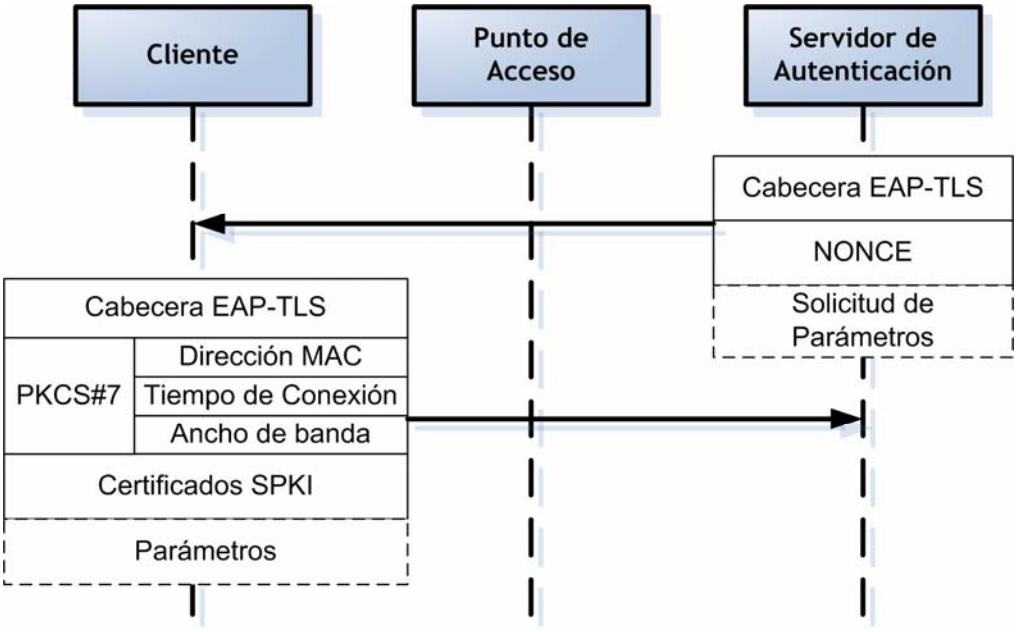

Figura 8.6: Mensajes fase de autorización.

Los parámetros del cliente se mandan en una estructura firmada PKCS#7 (Public-Key Cryptographic Standard #7), de manera que el servidor de autenticación pueda estar seguro de que nadie ha modificado estos parámetros. Además, toda la información relativa a la autorización del cliente, parámetros y certificados, se manda a través del canal TLS establecido anteriormente, de manera que solo pueden haber sido enviados por parte del cliente con el que se ha iniciado el proceso de conexión. Dicha estructura PKCS#7 contiene el certificado del cliente con el que se ha realizado la firma para que el servidor pueda verificar que la firma es correcta.

En el mensaje mediante el cual el servidor le pide al cliente sus parámetros de conexión, se incluye un identificador de 4 octetos aleatorio (llamado nonce), que posteriormente se utilizará para derivar la clave WEP junto con la dirección MAC del punto de acceso y la clave maestra de la conexión TLS anteriormente establecida.

Fase de distribución de clave

En esta fase del protocolo únicamente participan el punto de acceso y el servidor de autenticación, y consiste en que éste último le pase al primero un descriptor de la clave WEP que debe utilizar con el cliente, así como el tipo de servicio que el cliente espera que se le ofrezca. Esta clave WEP la habrá generado el servidor como resultado de una función de resumen digital MD5 aplicada sobre la concatenación de la clave maestra generada por EAP-

TLS, la dirección MAC del punto de acceso, y la carga nonce comentada anteriormente.

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

Tras esto, el proceso de conexión ha terminado, y si todo se ha realizado correctamente, el servidor de autenticación notifica al punto de acceso la autorización por su parte a que el cliente haga uso de la red. El punto de acceso traslada entonces al cliente esta decisión para que inicie la comunicación.

El cliente, que habrá generado la misma clave WEP que obtuvo el punto de acceso, puede comenzar a hacer uso de la red, con la garantía de que sus mensajes son sólo descifrables por el punto de acceso, dado que la clave WEP generada es distinta para cada usuario.

Es posible ver un esquema de los mensajes intercambiados por las distintas entidades durante esta fase en la figura 8.7

Por otra parte, en caso de que una clave WEP de hasta 16 octetos (tamaño del resumen MD5) no proporcione suficiente seguridad, y si la potencia de los equipos lo permite, podría utilizarse el método de extensión de longitud de claves para obtener una clave WEP de mayor tamaño que consiste en el siguiente algoritmo:

WEP0=MD5(clave, MAC, nonce)
WEPn=WEPn-1 || MD5(clave, MAC, nonce,WEPn-1)

donde cuánto más se repita la iteración, mayor será la longitud de la clave generada.

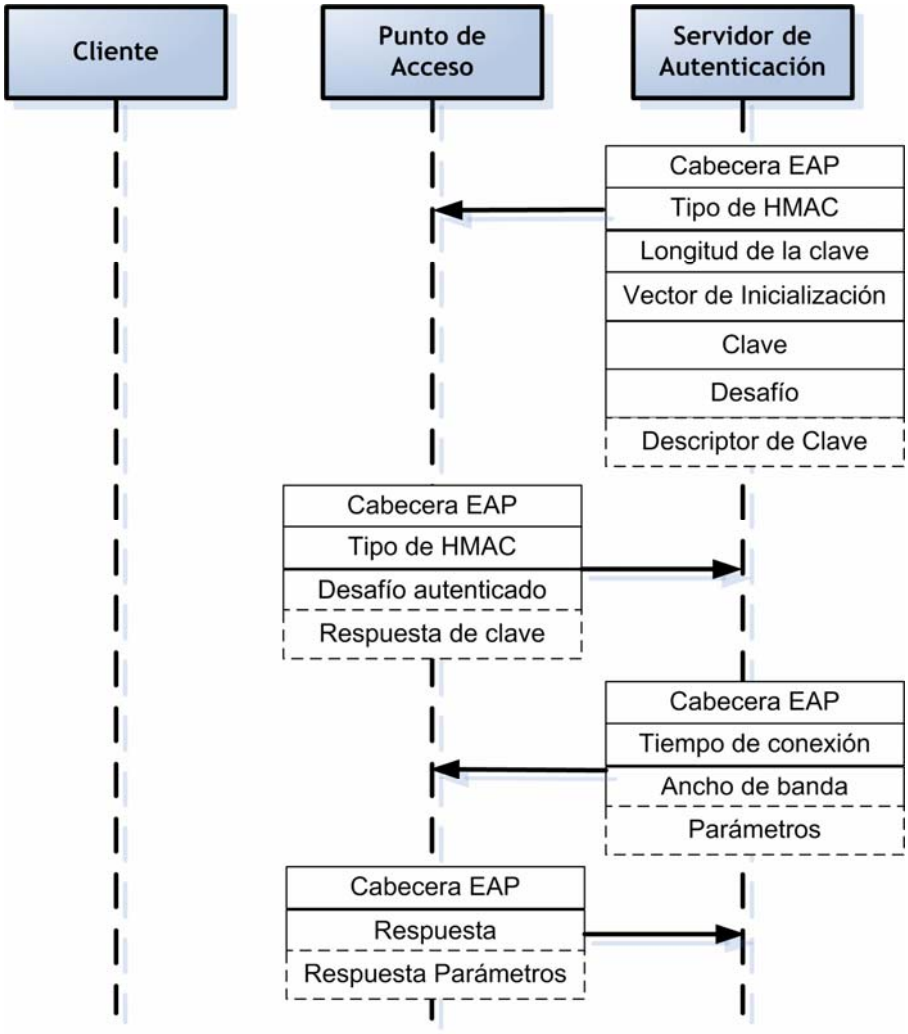

Figura 8.7: Mensajes fase de distribución de clave.

Fase de renegociación

Periódicamente, y dependiendo del nivel de seguridad que quiera el usuario, es posible renegociar la clave WEP que se está utilizando para cifrar la comunicación entre el cliente y el punto de acceso. Para ello, el cliente inicia un proceso de renegociación de conexión TLS. En esta ocasión, no será necesario que el cliente mande sus parámetros, a no ser que quiera cambiarlos, sino que únicamente se realiza esta fase para indicar al cliente cual es la nueva cadena aleatoria para generar la clave WEP.

De esta manera al terminar el nuevo proceso de conexión, tanto el punto de acceso como el cliente tendrán la nueva clave WEP a utilizar para cifrar sus comunicaciones.

Fase de movilidad

Esta fase se apoya en la anterior, ya que cuando un cliente detecta que está en el área de cobertura de un nuevo punto de acceso, en lugar de iniciar el proceso de conexión descrito desde el principio, inicia un proceso de renegociación de conexión TLS.
Al basarse la nueva conexión en la anterior, la generación del secreto compartido se puede realizar de forma más ligera, y además se evita que el servidor de autenticación tenga que validar de nuevo al usuario.

Una consecuencia directa es también que de forma automática se inicia la fase de renegociación de clave WEP, lo cual implica un cambio de la misma para trabajar con el nuevo punto de acceso.

8.4.- Control de acceso a VPNs usando 802.1X.

Supongamos que un router en un domicilio particular proporciona conectividad a una red corporativa a través de una red privada virtual establecida por medio de Internet. En la red de área local del domicilio, aparte del empleado de la empresa, otros miembros de la casa podrían estar usando el mismo router.

El control de acceso a VPNs usando autenticación 802.1X permite a los empleados de la empresa acceder a la red corporativa desde casa, mientras otros usuarios del domicilio acceden exclusivamente a Internet.
A través del protocolo 802.1X sólo los usuarios autenticados acceden al túnel VPN, y el resto (no autenticados) nunca pueden acceder a la red corporativa.

Este control de acceso extiende el objetivo inicial del protocolo 802.1X hacia la autenticación de dispositivos en lugar de puertos, esto es, varios dispositivos pueden ser autenticados independientemente para un puerto dado. Esta característica permite separar el tráfico de usuarios autenticados de los que no lo están, y por tanto aplicarles diferentes políticas.

8.5.- Soporte de Windows XP para 802.1X.

En Windows XP, la autenticación IEEE 802.1X junto al tipo de autentificación EAP-TLS aparece por defecto en todos los adaptadores de red compatibles con redes LAN.

Para configurar 802.1X en un ordenador que ejecute Windows XP, usaremos la pestaña “Autenticación” que se obtiene al pulsar en las propiedades de la tarjeta de red que queramos emplear y pinchar en “Propiedades” de la pestaña “Redes inalámbricas”. Si se trata de una

conexión fija, la pestaña aparecerá directamente en al pinchar en las propiedades de la tarjeta de red.

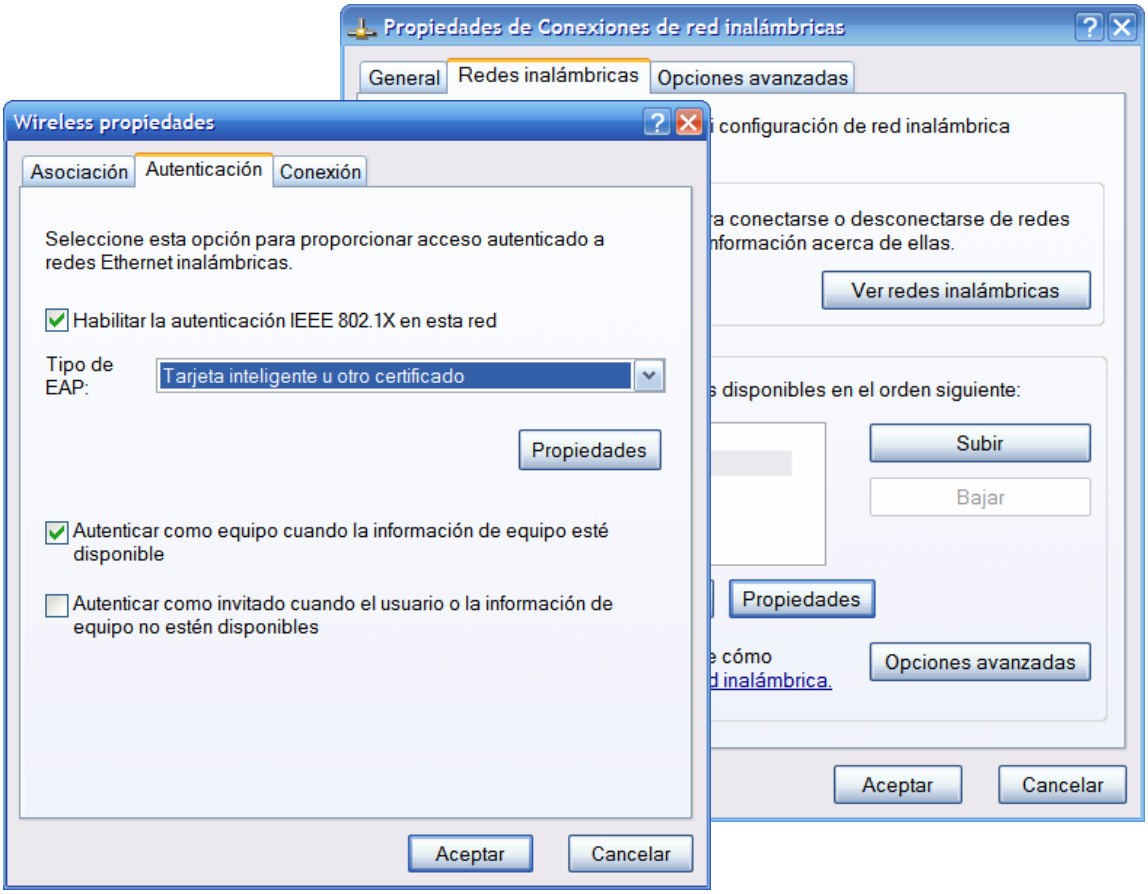

Figura 8.8: Configuración 802.1X en Windows.

Las opciones que aparecen son:

Habilitar la autenticación IEEE 802.1X en esta red: Se puede elegir entre utilizar IEEE 802.1X para autenticar la conexión o no. Esta opción se activa por defecto.
Una conexión LAN en Windows XP envía tres mensajes EAP-Start para hacer que el servidor de autenticación (el router o el punto de acceso inalámbrico) empiece el proceso de autenticación basándose en EAP. Si no se recibe un mensaje EAP de Petición/Identidad significa que el puerto no exige una autenticación IEEE 802.1X y la conexión LAN envía trafico normal para configurar la capacidad de conexión de la red. Si por el contrario se recibe el mensaje esto significa que la autenticación IEEE 802.1X se ha puesto en marcha.
Por lo tanto, si dejamos activada esta configuración para una conexión cuando el router no soporta IEEE 802.1X no perjudicamos la capacidad de conexión de la red.

Tipo de EAP: Muestra los protocolos de autenticación extensible instalados, por defecto EAP Protegido (PEAP) o Tarjeta inteligente u otro certificado. Este último emplea EAP-TLS.

Autenticar como equipo cuando la información de equipo esté disponible: Aquí se especifica si la máquina se intenta autenticar utilizando los credenciales del ordenador (tales como certificados) sin que el usuario introduzca sus datos. Esta opción está activada por defecto.

Autenticar como invitado cuando el usuario o la información de equipo no estén disponibles: Determina si la máquina se intenta autenticar como invitado. Se utiliza cuando los credenciales del usuario o del ordenador no están disponibles. Esta opción está desactivada por defecto.

En el cuadro de diálogo Propiedades de las tarjetas inteligentes y otros certificados, se podrán ver y configurar las siguientes propiedades:

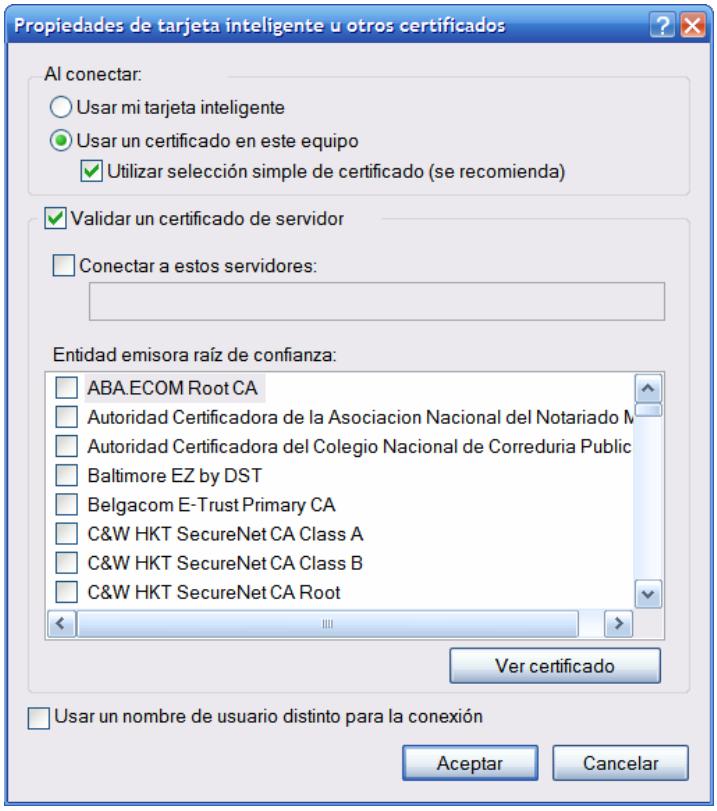

Figura 8.9: Propiedades certificados.

Para poder utilizar para la autenticación un certificado almacenado en el ordenador local o usuario actual se selecciona **Usar un certificado en este equipo**. Cuando hay varios certificados de usuario instalados, el usuario tiene que seleccionar uno en particular para la primera asociación. Ése será el que se utilice en el resto de las asociaciones que tengan lugar hasta que finalice esa sesión de Windows XP.

Validar un certificado de servidor: Aquí se especifica si quiere validar o no el certificado del ordenador del servidor de autenticación (por lo general un servidor RADIUS). Esta opción está activada por defecto.

Entidad emisora raíz de confianza: Gracias a esta opción puede elegir la autoridad de certificación (CA) raíz del certificado del servidor de autenticación. La lista enumera los certificados CA raíz que se encuentran almacenados. Por defecto no se selecciona ninguna CA raíz.

Usar un nombre de usuario distinto para la conexión: Especifica si para la autenticación se quiere utilizar un nombre de usuario diferente al que aparece en el certificado. Esta opción está desactivada por defecto.

Como ya comentamos en el apartado 8.2 de este capítulo, existe una relación entre 802.1X y WPA. Para configurar en Windows XP el uso de WPA, utilizaremos la pestaña "Asociación" que se obtiene al pulsar en las propiedades de la tarjeta de red que queramos emplear y pinchar en "Propiedades" de la pestaña "Redes inalámbricas" (ver figura 8.10)

Una vez ahí podremos configurar nuestra tarjeta de red inalámbrica, para utilizar como autenticación: red abierta, compartida, WPA o WPA-PSK. Para las dos primeras opciones, podemos seleccionar en el apartado "Cifrado de datos" si empleamos WEP o deshabilitamos el cifrado. Mientras que para las opciones WPA y WPA-PSK podremos seleccionar entre TKIP o AES (que se correspondería con CCMP, como ya hemos visto en apartados anteriores)

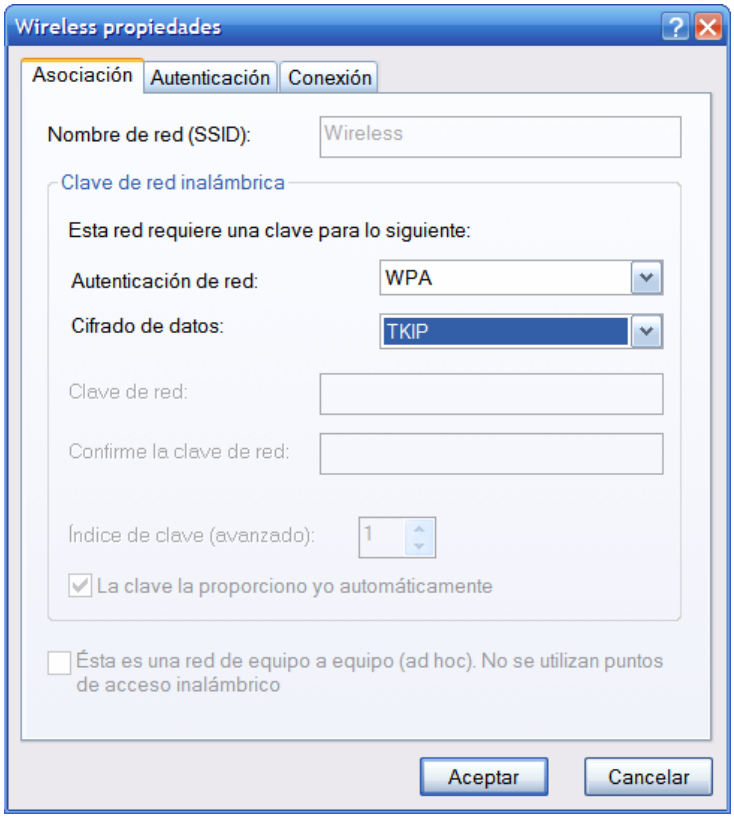

Figura 8.10: Configuración del tipo de red en Windows.