

CAPITULO III



AUTENTIFICACIÓN DE USUARIOS EN LA RED WLAN

3.1. IEEE 802.1x

3.2. RADIUS

3.3. Configuración del Access Point (AP)

En este capítulo se expondrá las diferentes alternativas de seguridad en entornos inalámbricos adaptadas a una de red de área local disponible en un medio administrativo, de tal forma que se puedan conjugar las redes existentes hasta el momento con la instalación de nuevas redes inalámbricas. Se describen los elementos que participan en la solución, así como los protocolos de red y funcionalidades necesarias para garantizar la seguridad de la red inalámbrica. Los diferentes factores que influyen en la conexión a través de redes inalámbricas son principalmente la Autenticación y la encriptación.

Tener una buena solución de autenticación segura a la hora de conectarse a la red es esencial, tanto en redes de área local cableadas como en de redes inalámbricas, principalmente en estas últimas ya que la posibilidad de intrusión es mayor que en las primeras. La solución elegida para nuestra autenticación es la utilización de 802.1x, estándar de autenticación del IEEE para redes inalámbricas y cableadas. El 802.1x es un estándar que permite el transporte de tramas EAP sobre redes cableadas e inalámbricas

Otro factor importante que influye en la seguridad de las redes inalámbricas es la necesidad de encriptar el contenido de la información que se trasfiere a través de la red inalámbrica. En la actualidad existen principalmente dos métodos de encriptación: WEP y WPA. Tanto WEP como WPA aseguran que las tramas de los usuarios de la red inalámbrica que viajan estén encriptados según un determinado mecanismo y que en caso de ser capturadas por cualquier intruso, estas tramas sean difíciles de descifrar (en la actualidad se han detectado ciertas vulnerabilidades que hacen que determinados mecanismos de encriptación basados en WEP sean vulnerables) [www07].

3.1.- ESTANDAR 802.1x

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x. [www12]

El protocolo 802.1x involucra tres participantes Figura 3.1:

- Suplicante o cliente, que desea conectarse con la red.
- El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red.
- El autenticador, que es el equipo de red (switch, Acces Point) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

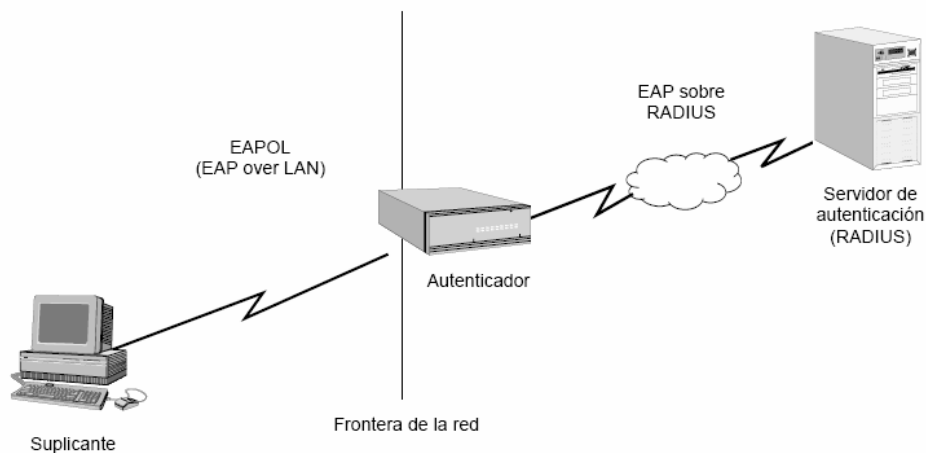


Figura 3.1: Arquitectura del sistema de autenticación 802.1x.

Para entender cómo funciona el protocolo 802.1x sigamos el siguiente esquema.

- 1.- El cliente, que quiere conectarse a la red, envía un mensaje de inicio de EAP que da lugar al proceso de autenticación. Por ejemplo, la persona que quiere acceder al banco pediría acceso al guardia de seguridad de la puerta.
- 2.- El punto de acceso a la red respondería con una solicitud de autenticación EAP. En el ejemplo, el guardia de seguridad respondería solicitando el nombre y el apellido del cliente, así como su huella digital. Además, antes de preguntarle, el guarda de seguridad le diría una contraseña al cliente, para que éste sepa que realmente es un guardia de seguridad.
- 3.- El cliente responde al punto de acceso con un mensaje EAP que contendrá los datos de autenticación. 'Nuestro cliente le daría el nombre y los apellidos al guardia de seguridad además de su huella digital'.
- 4.- El servidor de autenticación verifica los datos suministrados por el cliente mediante algoritmos, y otorga acceso a la red en caso de validarse. En nuestro caso, el sistema del banco verificaría la huella digital, y el guardia validaría que se correspondiese con el cliente.
- 5.- El punto de acceso suministra un mensaje EAP de aceptación o rechazo, dejando que el cliente se conecte o rechazándolo. Nuestro guardia de seguridad le abrirá la puerta o no, en función de la verificación al cliente.
- 6.- Una vez autenticado, el servidor acepta al cliente, por lo que el punto de acceso establecerá el puerto del cliente en un estado autorizado. Nuestro cliente estará dentro del banco. [www13]

La autenticación del cliente se lleva a cabo mediante el protocolo **EAP** (Extensible Authentication Protocol), como veremos en la Figura: 3.2

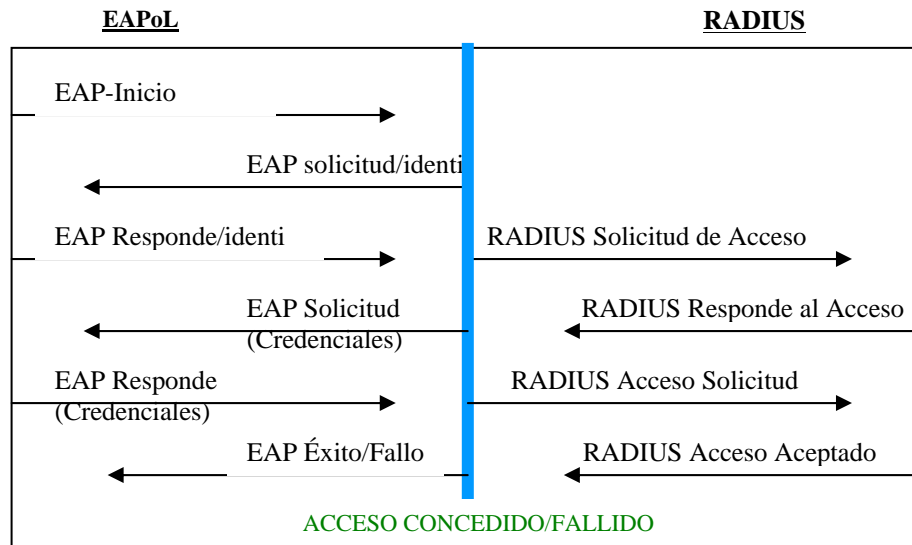
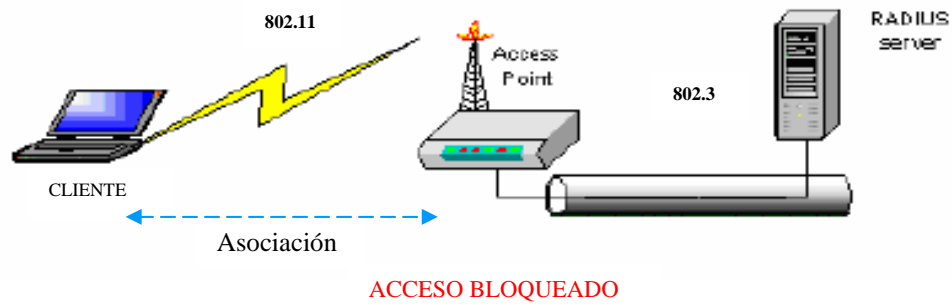


Figura 3.2: Dialogo EAP-RADIUS

3.1.1.- Métodos de autenticación EAP

802.1X utiliza el Protocolo de autenticación extensible (EAP) para el intercambio de mensajes durante el proceso de autenticación y el Protocolo de autenticación extensible utilizado en la LAN (EAPoL, *EAP Over LAN*) usado para transportar EAP. Con EAP se utilizan métodos de autenticación arbitrarios, como contraseñas, tarjetas inteligentes o certificados para autenticar la conexión inalámbrica. La compatibilidad que 802.1x ofrece con los tipos de EAP le permite utilizar cualquiera de los siguientes métodos de autenticación: [www14]

- Método EAP-TLS
- Método EAP-LEAP
- Método MD5

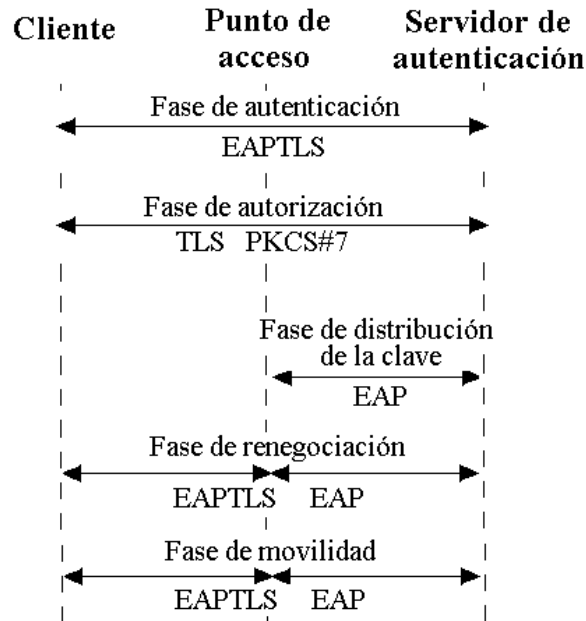


Figura 3.3: Comunicación EAP-TLS

3.1.1.1.- Método EAP-TLS (EAP-Transport Level Security)

El tipo de EAP Seguridad del nivel de transporte EAP se utiliza en entornos de seguridad basados en certificados. Si está utilizando tarjetas inteligentes para la autenticación de acceso remoto, debe utilizar el método de autenticación EAP-TLS. El intercambio de mensajes EAP-TLS permite la autenticación mutua, la negociación del método de cifrado y la determinación de claves cifradas entre el cliente de acceso remoto y el autenticador. Proporciona el método de determinación de claves y autenticación más eficaz. Figura 3.4

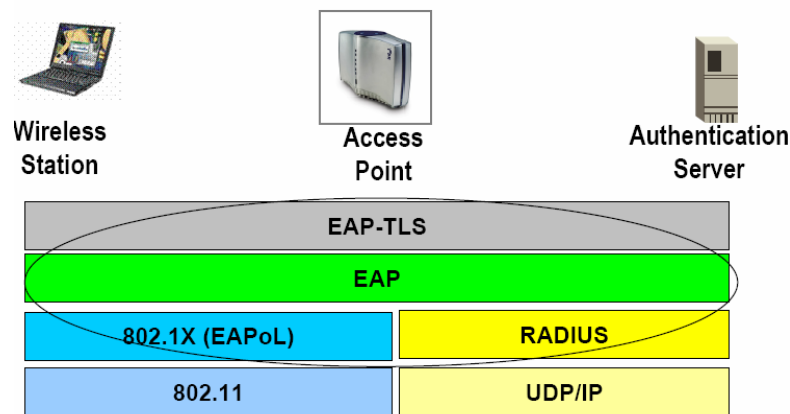


Figura 3.4: Arquitectura EAP-TLS

3.1.1.2.- Método EAP-LEAP

El método (Lightweigth EAP) Implementado por Cisco, emplea contraseñas para autenticar clientes. LEAP. Este método también presenta diversas vulnerabilidades de seguridad tales como propensión a ataques de diccionario sin conexión (que permiten que los atacantes descubran las contraseñas de los usuarios) y los ataques de intermediario. En un entorno de dominio, LEAP sólo puede autenticar al *usuario* en la WLAN, pero no al *equipo*.

3.1.1.3.- Método EAP-PEAP (Protected Extensible Authentication Protocol)

El Protocolo de autenticación extensible protegido (PEAP) proporciona protección a clientes y autenticadores (servidores IAS¹ o RADIUS) que utilizan EAP. La seguridad se la realiza a nivel de transporte (TLS) para crear una comunicación de extremo a extremo entre el cliente y el autenticador una vez comprobada la identidad del autenticador. Esté método emplea certificados para la autenticación de servidores y credencial (nombre de usuarios y contraseña) para la autenticación de usuarios. PEAP proporciona:

- Protección de la negociación del método EAP que se produce entre el cliente y el servidor mediante un canal TLS cifrado. Esto ayuda a impedir que un intruso inserte paquetes entre el cliente y el servidor RADIUS
- Protección contra la implementación de un punto de acceso inalámbrico no autorizado, cuando el cliente EAP autentica el certificado que proporciona el servidor IAS. El secreto principal TLS creado por el autenticador y el cliente PEAP no se comparte con el punto de acceso. Como consecuencia, el punto de acceso no puede descifrar los mensajes protegidos por PEAP.

3.1.1.4.- Método MD5

Suele utilizarse para autenticar las credenciales de los clientes de acceso remoto mediante sistemas de seguridad que usan nombres de usuario y contraseñas. También puede utilizarse para probar la interoperabilidad de EAP.

¹ IAS Servidor de Autenticación de Internet

3.1.2.- Ventajas y Desventajas de 802.11X

Las ventajas y desventajas del estándar 802.1X se resumen en la siguiente tabla.

Ventajas	Desventajas
Nivel de Seguridad alto Se trata de un esquema de autenticación de seguridad elevado porque puede emplear certificados de cliente o nombres de usuarios y contraseñas	interoperabilidad Aunque 802.1x disfruta de una aceptación casi universal, el uso de distintos métodos de EAP implica que la interoperabilidad no siempre está garantizada.
Autenticación de usuarios y de equipos: Permite la autenticación por separado de usuario y de equipo. La autenticación por separado de un equipo permite administrarlo incluso cuando ningún usuario ha iniciado la sesión.	
Transparencia: proporciona una autenticación y una conexión a la WLAN transparentes.	
Cifrado más seguro: permite un cifrado muy seguro de los datos de la red.	Disponibilidad Por ser compleja la configuración en lo que respecta a la seguridad de WLAN, muchas de las empresas no disponen del estándar 802.1x.
Bajo coste: bajo coste del hardware de red.	
Alto rendimiento: dado que el cifrado se lleva a cabo en el hardware de WLAN y no en la CPU del equipo cliente, el cifrado de WLAN no influirá en el nivel de rendimiento del equipo cliente.	

Tabla 3.1: Ventajas y Desventajas del estándar 802.1X

3.1.3.- Certificados

Documento digital que suele utilizarse para la autenticación y para proteger la información en redes abiertas. Un certificado enlaza de forma segura una clave pública con la entidad que contiene la clave privada correspondiente. La entidad emisora de certificados (CA), pueden ser emitidos para un usuario, un equipo o un servicio. [www15]

3.1.3.1.- Certificados Digitales

El certificado digital es un documento electrónico que identifica una persona o entidad y contiene una copia de su llave pública. El certificado garantiza que la clave pública pertenece a la entidad identificada y que la entidad posee la correspondiente clave privada. Para los usuarios proporcionan un mecanismo para verificar la autenticidad de programas y documentos obtenidos a través de la red, el envío de correo encriptado y/o firmado digitalmente, el control de acceso a recursos, etc.

Los *certificados digitales* proporcionan un mecanismo criptográfico para implementar la autenticación, también proporcionan un mecanismo seguro y escalable para distribuir claves públicas en comunidades grandes. La mayor parte de los certificados de uso común se basan en el estándar de certificados **X.509v3**.

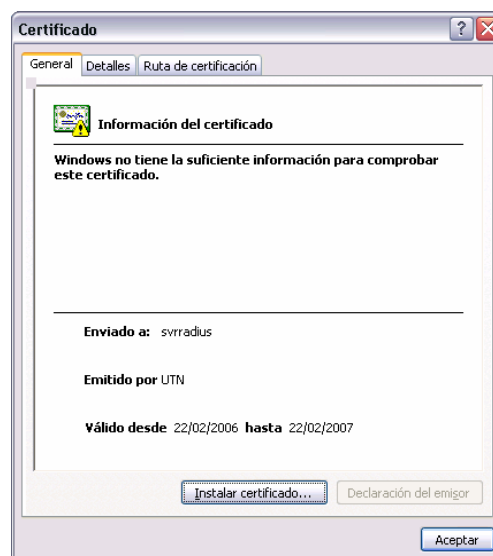


Figura 3.5: Certificado Digital

3.1.3.2.- Certificado X.509 v3

Los certificados X.509 contienen además de la clave pública del interlocutor, información acerca de su identidad, así como información complementaria sobre algoritmos utilizados para la generación de claves, plazos de validez del propio certificado, etc.

Por otra parte, estos certificados contienen una firma digital que garantiza la integridad de sus contenidos, ya sea por la clave privada del mismo interlocutor (certificados autofirmados), o por la clave privada de una tercera parte (**certificado** firmado por una CA). Son los de este último tipo, los firmados por una CA, los necesarios para garantizar la seguridad inicial en las redes WLAN. [www16]:

El contenido de un certificado digital es:

- Identificación del titular del certificado: Nombre, dirección, etc.
- Clave pública del titular del certificado.
- Fecha de validez.
- Número de serie.
- Identificación del emisor del certificado (CA)

3.2.- RADIUS

El Servicio de usuario de acceso telefónico de autenticación remota (RADIUS, *Remote Authentication Dial-In User Service*) Es un protocolo de autenticación de seguridad basado en cliente/servidor, se utiliza para proporcionar servicios de autenticación, autorización y administración (AAA) de cuentas. Un cliente (por lo general, un servidor de acceso telefónico, un servidor VPN o un punto de acceso inalámbrico) envía credenciales de usuario e información de parámetros de conexión en forma de un mensaje a un servidor RADIUS. El servidor autentica y autoriza la petición del cliente y devuelve un mensaje de respuesta. Los clientes también envían mensajes de administración de cuentas a los servidores RADIUS.

Los mensajes se envían como mensajes de Protocolo de datagramas de usuario (UDP, *User Datagram Protocol*). El puerto UDP 1812 se utiliza para los mensajes de autenticación y el 1813 para los mensajes de administración de cuentas. Puede que algunos servidores de acceso a la red utilicen el puerto UDP 1645 para los mensajes de autenticación y el 1646 para los mensajes de administración de cuentas.

Se ha configurado dos servidores RADIUS el uno corriendo bajo la plataforma Linux (SuSe 9.1) y el otro bajo la plataforma Windows (Windows 2003).

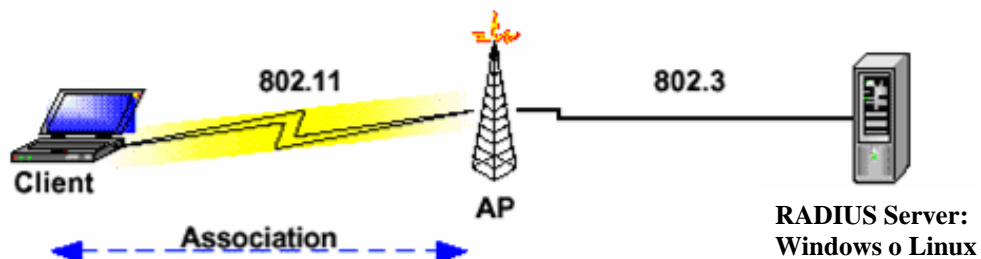


Figura 3.6: Arquitectura RADIUS Server con Windows o Linux

3.2.1.- Servidor Windows

La idea general es la autenticación de usuarios Wireless usando Windows XP contra un servidor IAS como RADIUS.

La instalación con lleva varias etapas, como instalar el servicio de IAS en un servidor Windows 2003 Server (Controlador de dominio), configuración del Access Point (AP) para que interactúe con el servidor RADIUS, y la configuración del cliente Windows XP para que funcione con el protocolo WPA (EAP-PEAP)

El protocolo EAP-TLS funciona con certificado que se debe instalar en el servidor RADIUS (IAS). Por ende necesitamos tener un CA que nos proporcione el certificado.

3.2.1.1.- Requerimientos

Para la instalación y configuración del Servidor RADIUS con Windows 2003 se realiza los siguientes pasos:

- 1.- Instalación, configuración de Active Directory y Servidor DNS²
- 2.- Instalación del Servidor de Aplicaciones
- 3.- Instalación de una entidad emisora de certificados (CA)
- 4.- Instalación y Configuración de RADIUS
- 5.- Configuración de Usuarios
- 6.- Configuración del Access Point
- 7.- Configuración del Cliente XP para WPA (EAP-PEAP)

3.2.1.1.1.- Instalación, configuración de Active Directory y Servidor DNS

Active Directory es el servicio de directorio que almacena información acerca de los objetos de una red y la pone a disposición de los usuarios y administradores de la red. Da a los usuarios de red acceso a los recursos permitidos en cualquier punto de la red mediante un único proceso de inicio de sesión. Proporciona a los administradores una vista jerárquica intuitiva de la red y un punto de administración único para todos sus objetos. Su configuración es la siguiente:

² @stake Servidor de Nombre de dominios

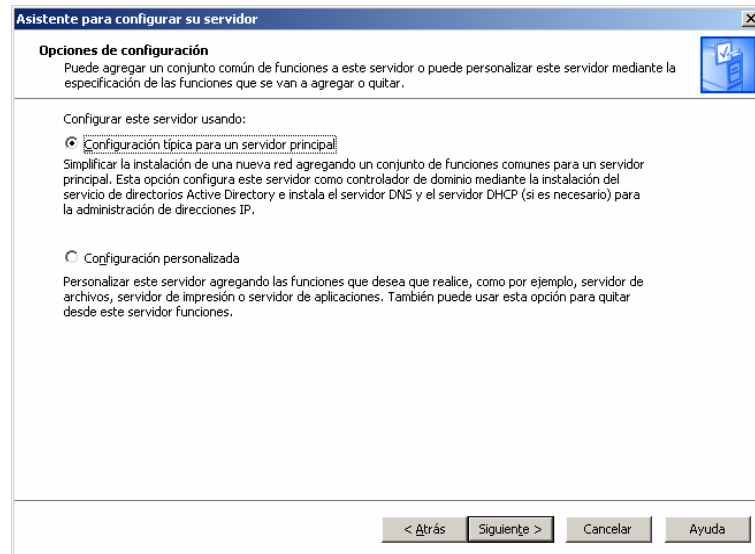


Figura 3.7: Asistente para la configuración del Servidor

3.2.1.1.2.- Instalación del Servidor de Aplicaciones

Función del servidor	Configurado
Servidor de archivos	No
Servidor de impresión	No
Servidor de aplicaciones (IIS, ASP.NET)	No
Servidor de correo (POP3, SMTP)	No
Terminal Server	No
Servidor de acceso remoto/VPN	No
Controlador de dominio (Active Directory)	Sí
Servidor DNS	Sí
Servidor de DHCP	Sí
Servidor de multimedia de transmisión po...	No
Servidor WINS	No

Figura 3.8: Funciones del Servidor

3.2.1.1.3.- Instalación de una entidad emisora de certificados (CA)

Para instalar una entidad emisora de certificados, nos vamos a componentes e instalamos Servicios de Certificate Server. Los servicios de Certificate Server deben ser instalados manualmente de los componentes de Windows.

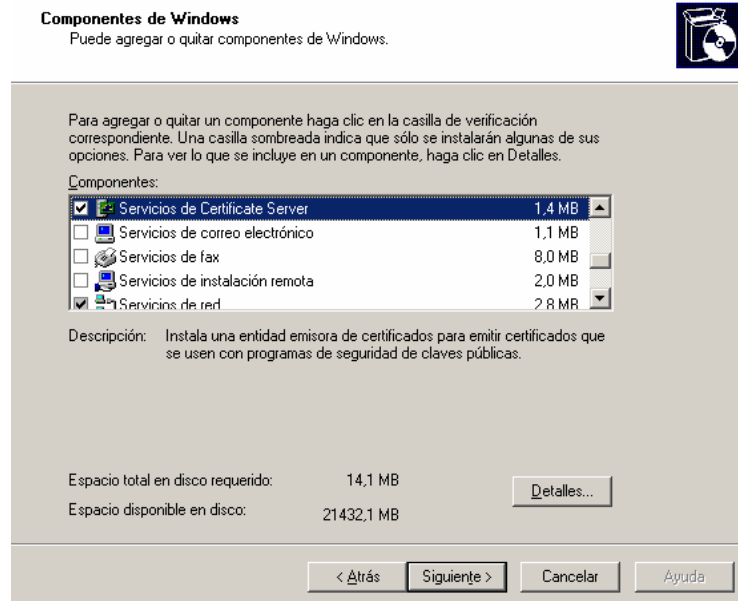


Figura 3.9: Componentes de Windows

Hacemos clic en siguiente y realizamos los siguientes paso seleccionamos el tipo de entidad emisora de certificados que deseamos establecer, en nuestro caso seleccionamos entidad emisora raíz de la empresa.

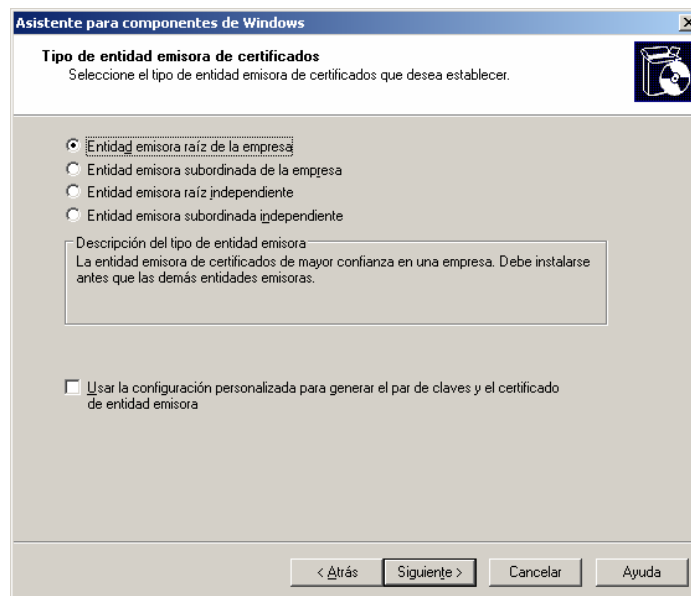


Figura 3.10: Asistente para Componentes de Windows

Damos nombre a nuestra entidad emisora de certificado (CA) y por ultimo ubicamos la base de datos de los certificados.

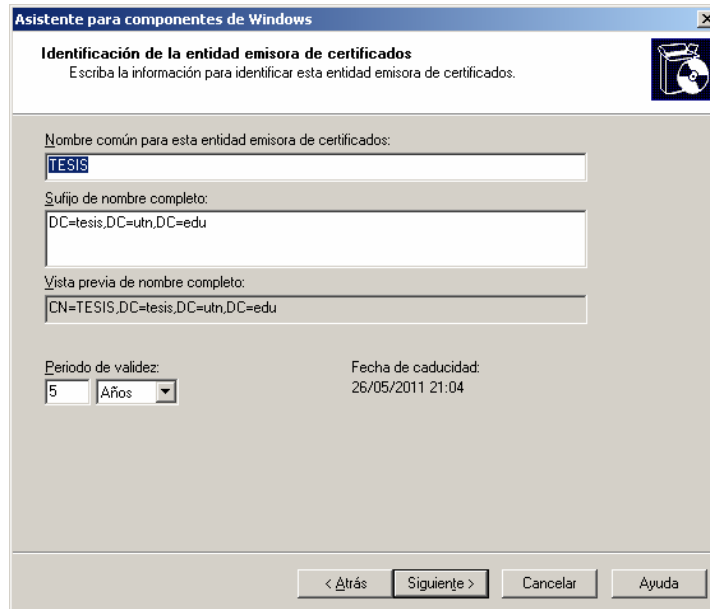


Figura 3.11: Nombre a la Entidad Emisora de Certificado (CA)

3.2.1.1.4.- Instalación del certificado

Para la instalación del certificado hacemos clic en Internet Explorer, escribimos lo siguiente <http://localhost/Certsrv/>, nos aparece la pantalla de bienvenida,

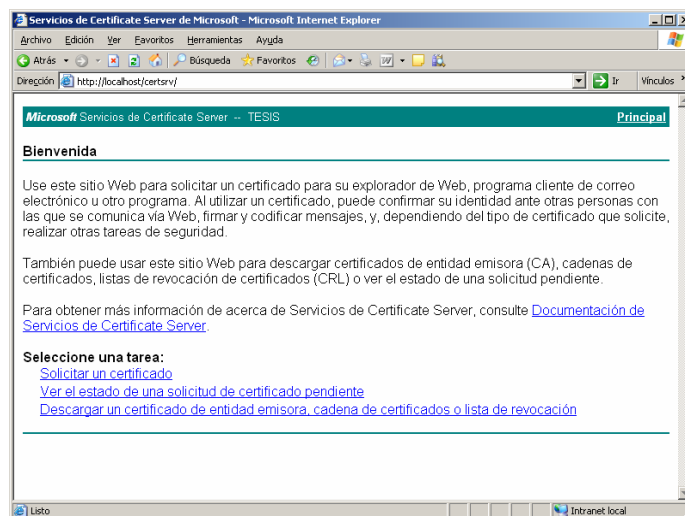


Figura 3.12: Instalación del Certificado

Hacemos click en solicitar un certificado, elegimos el tipo de certificado y escogemos el certificado de usuario o bien una solicitud avanzada de certificado, por ultimo hacemos clic en instalar este certificado y comprobamos escribiendo `\\nombre del servidor\CertEnroll`

3.2.1.1.5.- Instalación y Configuración de RADIUS

Para la instalación del servidor RADIUS nos vamos a componentes agregamos servicios de red y hacemos clic en servicio de autenticación de Internet.

<input checked="" type="checkbox"/>	Protocolo de configuración dinámica de host (DHCP)	0,0 MB
<input type="checkbox"/>	RPC sobre el proxy HTTP	0,0 MB
<input checked="" type="checkbox"/>	Servicio de autenticación de Internet	0,0 MB
<input type="checkbox"/>	Servicio de cuarentena de acceso remoto	0,1 MB
<input type="checkbox"/>	Servicio WINS	1,0 MB
<input type="checkbox"/>	Servicios simples de TCP/IP	0,0 MB
<input checked="" type="checkbox"/>	Sistema de nombres de dominio (DNS)	1,7 MB

Figura 3.13: Instalación del Servicio de autenticación de Internet

Creamos un nuevo cliente RADIUS.

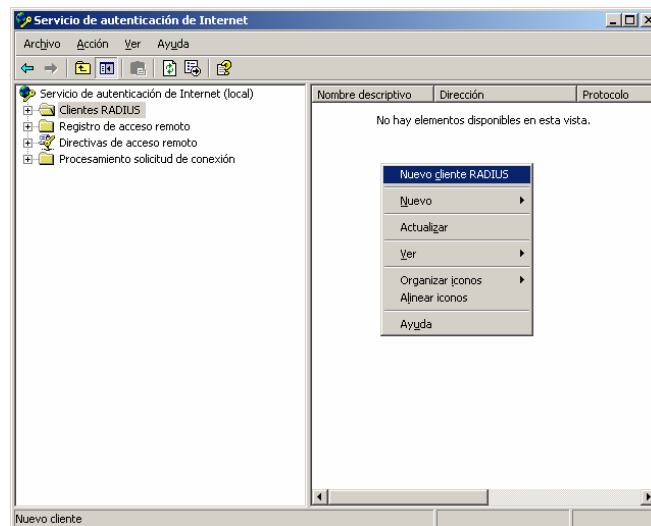
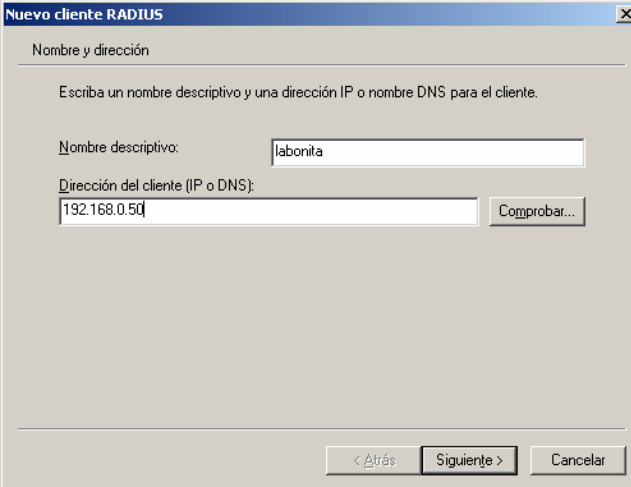


Figura 3.14: Creación del Nuevo cliente RADIUS

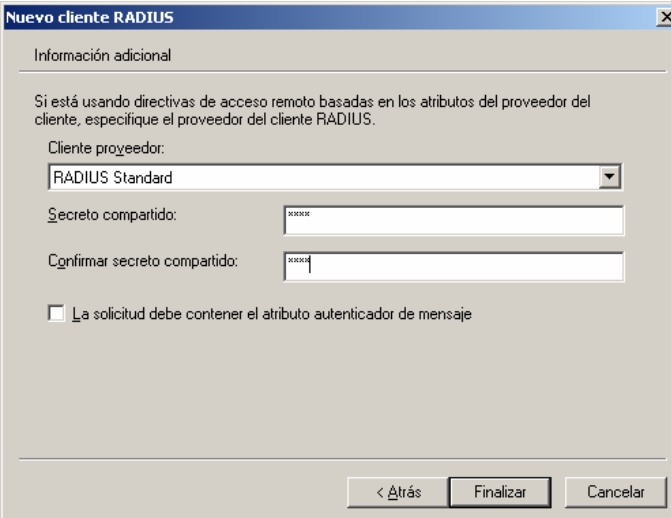
En el siguiente paso escribimos un nombre descriptivo y dirección IP (IP del AP) o nombre DNS para el cliente y comprobamos.



The screenshot shows a dialog box titled "Nuevo cliente RADIUS" with a close button (X) in the top right corner. The main heading is "Nombre y dirección". Below it, there is a text prompt: "Escriba un nombre descriptivo y una dirección IP o nombre DNS para el cliente." There are two input fields: "Nombre descriptivo:" containing the text "labonita" and "Dirección del cliente (IP o DNS):" containing the IP address "192.168.0.50". To the right of the second field is a button labeled "Comprobar...". At the bottom of the dialog, there are three buttons: "< Atrás", "Siguiete >", and "Cancelar".

Figura 3.15: Nombre y Dirección IP del cliente RADIUS

En los siguientes pasos utilizamos directivas de acceso remoto basadas en el atributo del proveedor del cliente y claves de secreto compartido que es la misma clave de secreto compartido del Access Point (AP)



The screenshot shows the same dialog box "Nuevo cliente RADIUS" but with the "Información adicional" tab selected. The text prompt reads: "Si está usando directivas de acceso remoto basadas en los atributos del proveedor del cliente, especifique el proveedor del cliente RADIUS." There is a dropdown menu for "Cliente proveedor:" with "RADIUS Standard" selected. Below it are two input fields for "Secreto compartido:" and "Confirmar secreto compartido:", both containing masked text "xxxx". At the bottom, there is a checkbox labeled "La solicitud debe contener el atributo autenticador de mensaje" which is currently unchecked. The bottom buttons are "< Atrás", "Finalizar", and "Cancelar".

Figura 3.16: Información adicional del cliente RADIUS

Hacemos clic en agregar directivas de acceso remoto y seleccionamos “configurar una directiva personalizada” y ponemos un nombre de directiva

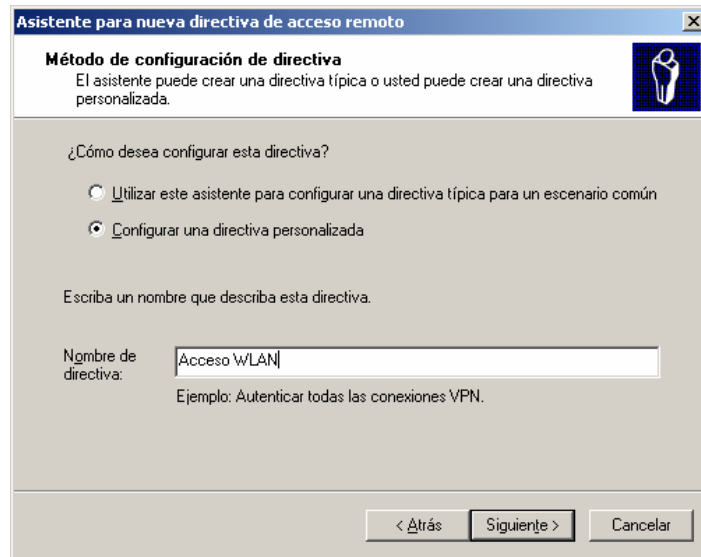


Figura 3.17: Método de configuración de directiva

Click en siguiente y seleccionamos agregar, elegimos “Nas-Port-Type”, click en agregar y elegimos Inalámbrica – IEEE 802.11, por ultimo aceptamos.

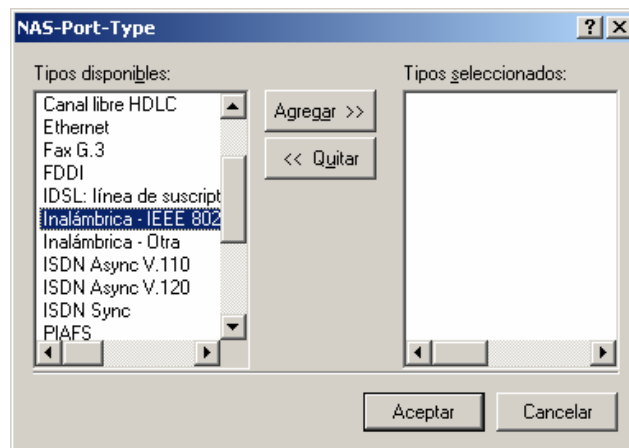


Figura 3.18: Selección del NAS-Port-Type

Una vez agregado y aceptado nos aparece de nuevo el asistente para nueva directiva para acceso remoto, aquí debemos especificar las condiciones que debe cumplir las solicitudes de conexión para poder concederles o denegarles el acceso.

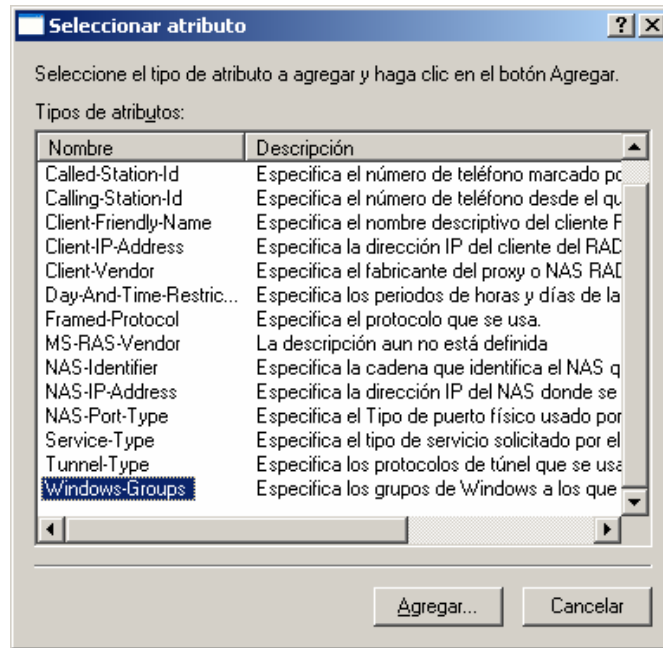


Figura 3.19: Selección del tipo de Atributos

Hacemos clic en agregar y nos aparece una venta de seleccionar nuevos atributos, escogemos el atributo “Windows Grupos” agregamos y clic en avanzadas, seleccionamos el grupo que va a tener acceso a la red.

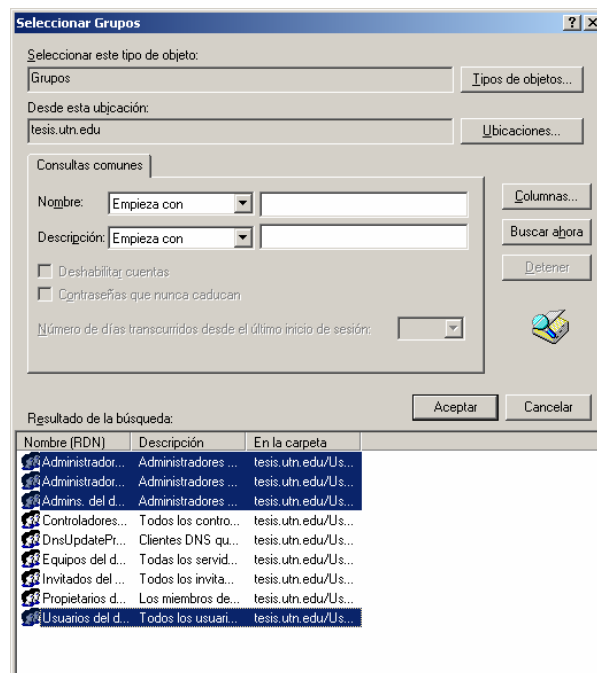


Figura 3.20: Selección de Grupos

Clic en aceptar, otra vez debemos especificar las condiciones que deben cumplir las solicitudes de condición de conexión para poder concederles o denegarles acceso. Clic en agregar y seleccionamos “conceder permiso de acceso remoto”, clic en siguiente, seleccionamos editar perfil, es un conjunto de configuraciones que se aplican a solicitudes de conexión que han sido autenticadas. Clic en autenticación y presionamos el “método de EAP”, presionamos agregar, seleccionamos “EAP protegido PEAP”, por ultimo hacemos clic en modificar ya que nos aparecera contraseña segura (EAP-MSCHAP v2) y escogemos EAP protegido PEAP, aceptamos todo y finalizamos.

3.2.1.1.6.- Configurar de usuarios

En la configuración de usuarios seleccionamos los usuarios que hayamos creado y dado permiso para que tengan acceso a la red, hacemos clic en propiedades de usuarios, clic en marcado y escogemos “permitir el acceso”. Lo mismo para el administrador, clic en propiedades del administrador, en marcado y seleccionamos “permitir el acceso” como veremos en la Figura 3.21

El hecho de que un grupo este dentro de la directiva no significa que el usuario dentro de este puede acceder a la WLAN.

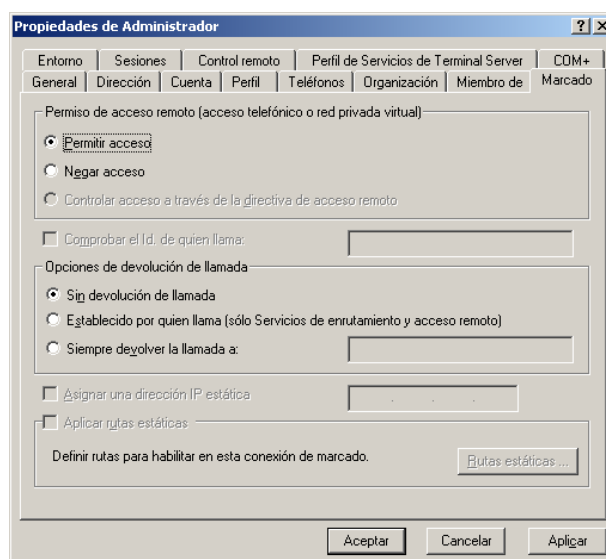


Figura 3.21: Propiedades del Administrador

3.2.1.1.7.- Configuración del cliente XP para WPA (EAP-PEAP)

En la conexión de red segura para los clientes se utilizo la autenticación de red con el mecanismo de seguridad WPA y el sistema de cifrado de datos AES.

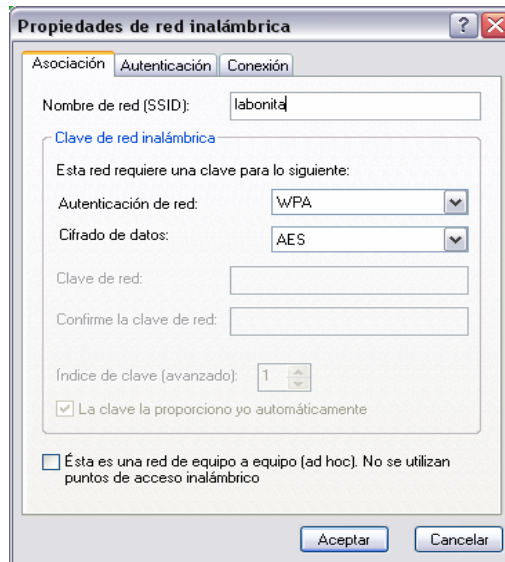


Figura 3.22: Propiedades de Red Inalámbrica

Para la autenticación de usuarios utilizamos el método de “EAP protegido PEAP”, el cual nos proporciona certificados o credenciales para la conexión de la red como veremos en la Figura 3.23.



Figura 3.23: Formato de las Credenciales

3.2.2.- Servidor Linux

El servidor Linux aportan a la fiabilidad en las comunicaciones, autenticación y control de usuarios, en este caso veremos como configurar un servidor RADIUS en Linux con el software **FreeRADIUS** soportando **EAP-TLS** así como configurar 802.1x en un punto de acceso wireless y un ejemplo de configuración en cliente final, utilizando el mecanismo de seguridad **WPA**

3.2.2.1.- Requerimientos

En la instalación y configuración de la red WLAN utilizaremos certificados de cliente y servidor para la autenticación.

Para construir la red necesitamos:

- 1.- Instalación FreeRadius y OpenSSL
- 2.- Archivo Xpextensions
- 3.- Scripts de Generacion de Certificados
- 4.- Creación de Cerificados Digitales.
- 5.- Archivo Clients.conf
- 6.- Archivo radius.conf
- 7.- Archive a los usuarios Users

Como servidor RADIUS vamos a utilizar Linux Suse 9.1 con el sistema de instalación de paquetes apt y como software RADIUS usaremos FreeRADIUS. El AP (Access Point) será un D-link 2000AP+ (802.11b/g) con la última versión de firmware instalada. Como clientes utilizaremos el sistema operativo Windows XP, con soporte de WPA, con la utilización de las tarjetas D-Link

3.2.2.1.1.- Instalación de FreeRadius y OpenSSL

La instalación de estos dos paquetes esta disponible desde el momento mismo de la instalación de Linux, que permite seleccionar el software que deseamos que nuestro servidor disponga, únicamente seleccionamos FreeRadius como OpenSSL de la lista de aplicaciones, el instaladores de Linux añade las dependencias y continuamos con la instalación normal de Linux.

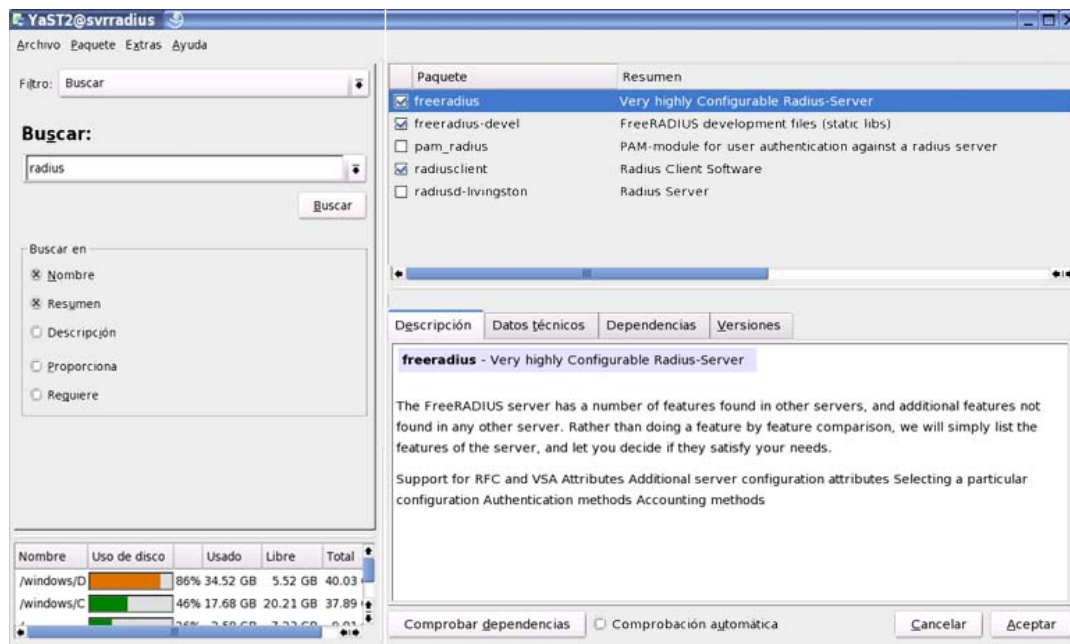


Figura 3.24: Instalación de FreeRadius y OpenSSL con Yast

Si ya tenemos instalado Linux vamos a utilizar la herramienta Yast (Panel de Control de Linux SuSe), a agregar software y de igual forma que la instalación seleccionamos los paquetes y aceptamos.

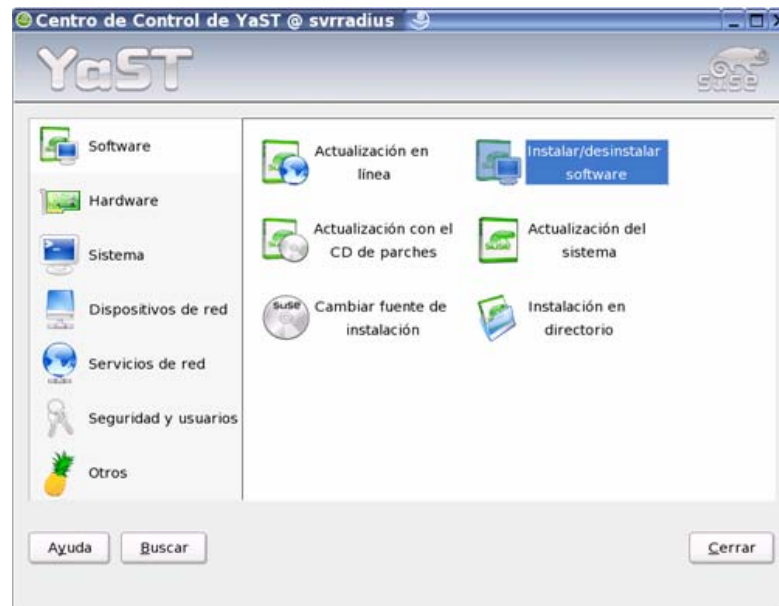


Figura 3.25: Instalar/desinstalar software

Cabe indicar que una vez terminada la instalación se crea la carpeta de configuración de Radius en `/etc/raddb`. Para mejor administración vamos a crear dentro de esta ruta la carpeta `certs`.

3.2.2.1.2.- Archivo Xpextensions

Xpextensions es un archivo que contiene las claves que nuestros certificados van a utilizar. Este archivo no se crea con la instalación por lo que se debe crear manualmente, para esto abrimos kate o kwrite (Editores de Texto) y escribimos las siguientes líneas:

```
[ xpcient_ext ]
extendedKeyUsage = 1.3.6.1.5.5.7.3.2
[ xpserver_ext ]
extendedKeyUsage = 1.3.6.1.5.5.7.3.1
```

Una vez hecho esto guardamos el archivo dentro de la ruta `/etc/raddb/certs` con el nombre `xpextensions`.

3.2.2.1.3.- Scripts de Generacion de Certificados

Para crear la CA y los certificados se pueden usar los scripts que aparecen en la web³, estos están disponibles en raddb.tar.gz

Los scripts que necesitamos son: CA.root, CA.server, CA.client; estos deben igual ser copiados a /etc/raddb/certs.

3.2.2.1.4.- Creación de Cerificados Digitales.

Como se menciona los certificados digitales van a ser creados por los script's CA.root, CA.server, CA.client.

Primero se debe genera el certificado de root para esto ejecutamos el script CA.root.

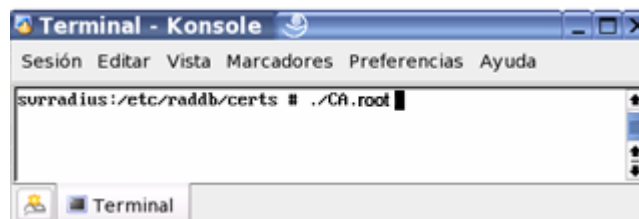


Figura 3.26: Creación del Certificado Digital

Seguimos las instrucciones que nos dice el script y se nos crea el certificado del root o administrador.

³ Web Dirección web para los script de los certificados <http://www.alphacore.net/contrib/nantes-wireless/eap-tls-HOWTO.html>,

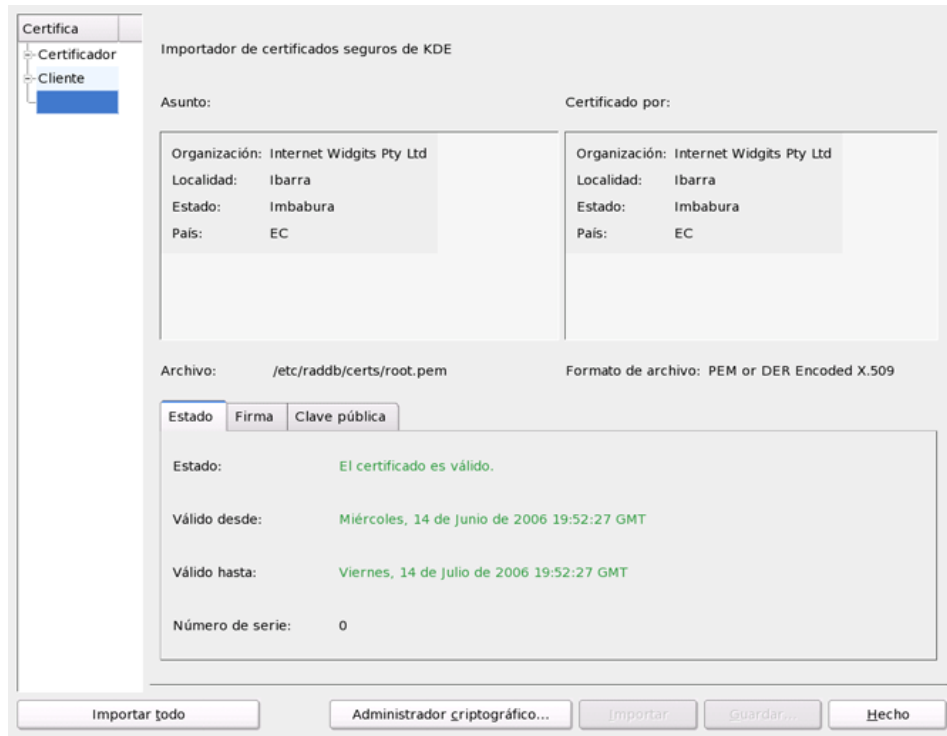


Figura 3.27: Importador de Certificados seguros de KDE

Una vez creado el certificado root procedemos a crear el certificado del servidor. Utilizamos CA.server [nombre de la maquina servidor].

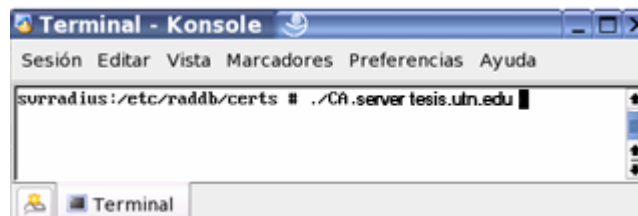


Figura 3.28: Creación del Certificado del Servidor

Seguimos las instrucciones que nos dice el script y se nos crea el certificado del servidor.

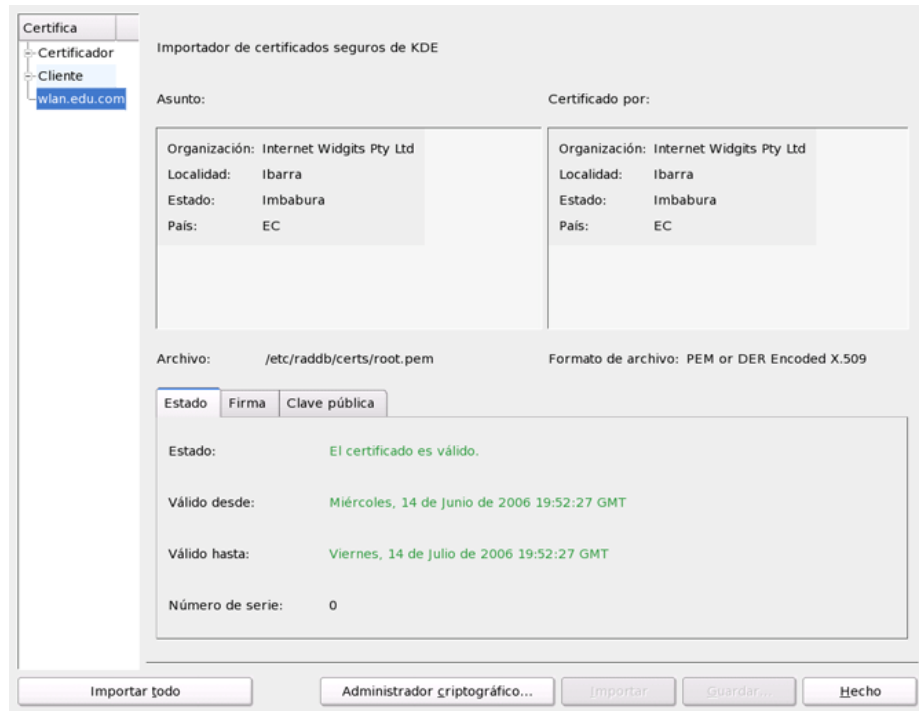


Figura 3.29: Certificado del Servidor

Los certificados de clientes van a ser generados tantos como usuarios tengan que validar el acceso a nuestra WLAN.

Se utiliza CA.client [nombre del cliente]

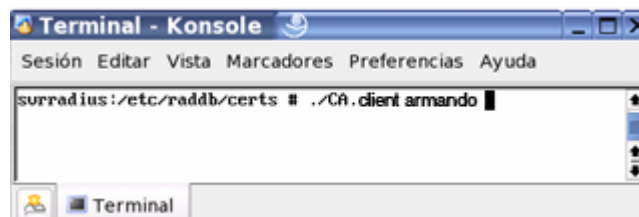
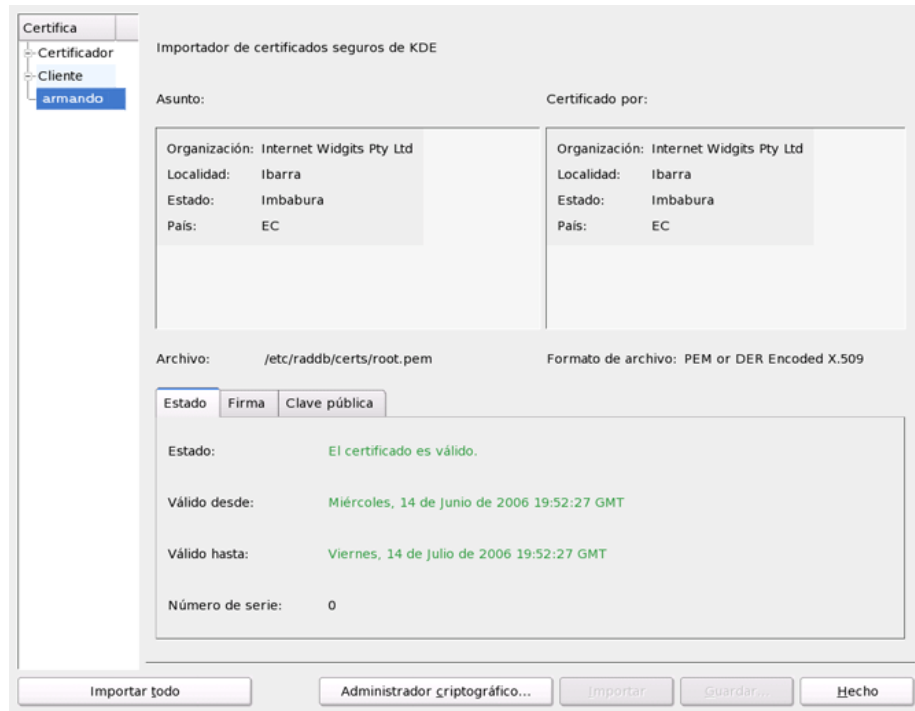


Figura 3.30: Certificado del cliente

Seguimos las instrucciones que nos dice el script y se nos crea el certificado del cliente.



3.2.2.1.5.- Archivo Clients.conf

Una vez creados los certificados vamos a configurar el archivo Clients.conf ; este archivo contiene la información de todos los puntos de acceso(AccessPoint) que van a validar los usuarios en nuestro servidor. Las líneas de configuración son como siguen:

```
client [Direccion ip del AP]{  
    secret      =    [palabra secreta del AP]  
    shortname   =    [nombre del AP]  
}
```

En el caso de nuestra red es:

```
client 192.168.1.50 {  
    secret = tesis  
    shortname = dw2000  
}
```

3.2.2.1.6.- Archivo radius.conf

Uno de los archivos más importantes para que funcione RADIUS en Linux es radius.conf; aquí se van a especificar las rutas de los certificados digitales creados anteriormente además del tipo de autenticación que va a tener.

Las líneas de configuración son las siguientes:

```
eap {
    default_eap_type = [Tipo de Autenticación]
    timer_expire      = 60
    ignore_unknown_eap_types = yes
    cisco_accounting_username_bug = no
}
tls {
    private_key_password = [Palabra Secreta]
    private_key_file = [Ruta del Certificado del servidor]
    certificate_file = [Ruta del Certificado del servidor]
    CA_file = [Ruta del Certificado del root]

    dh_file = ${raddbdir}/certs/dh
    random_file = ${raddbdir}/certs/random
                fragment_size = 1024
    include_length = yes
    check_crl = yes
}
}
```

En caso de nuestra wlan son:

```
eap {
    default_eap_type = tls
    timer_expire      = 60
    ignore_unknown_eap_types = yes
    cisco_accounting_username_bug = no
}
tls {
    private_key_password = tesis
    private_key_file = ${raddbdir}/certs/tesis.utn.edu.pem
    certificate_file = ${raddbdir}/certs/tesis.utn.edu.pem
    CA_file = ${raddbdir}/certs/root.pem
}
```

```
dh_file = ${raddbdir}/certs/dh
random_file = ${raddbdir}/certs/random
fragment_size = 1024
include_length = yes
check_crl = yes
}
}
```

3.2.2.1.7.- Archivo de Usuarios (Users)

La configuración de usuario se la hace en el archivo users. Vale destacar que aquí van las descripciones de los usuarios para los cuales hemos creado los certificados digitales.

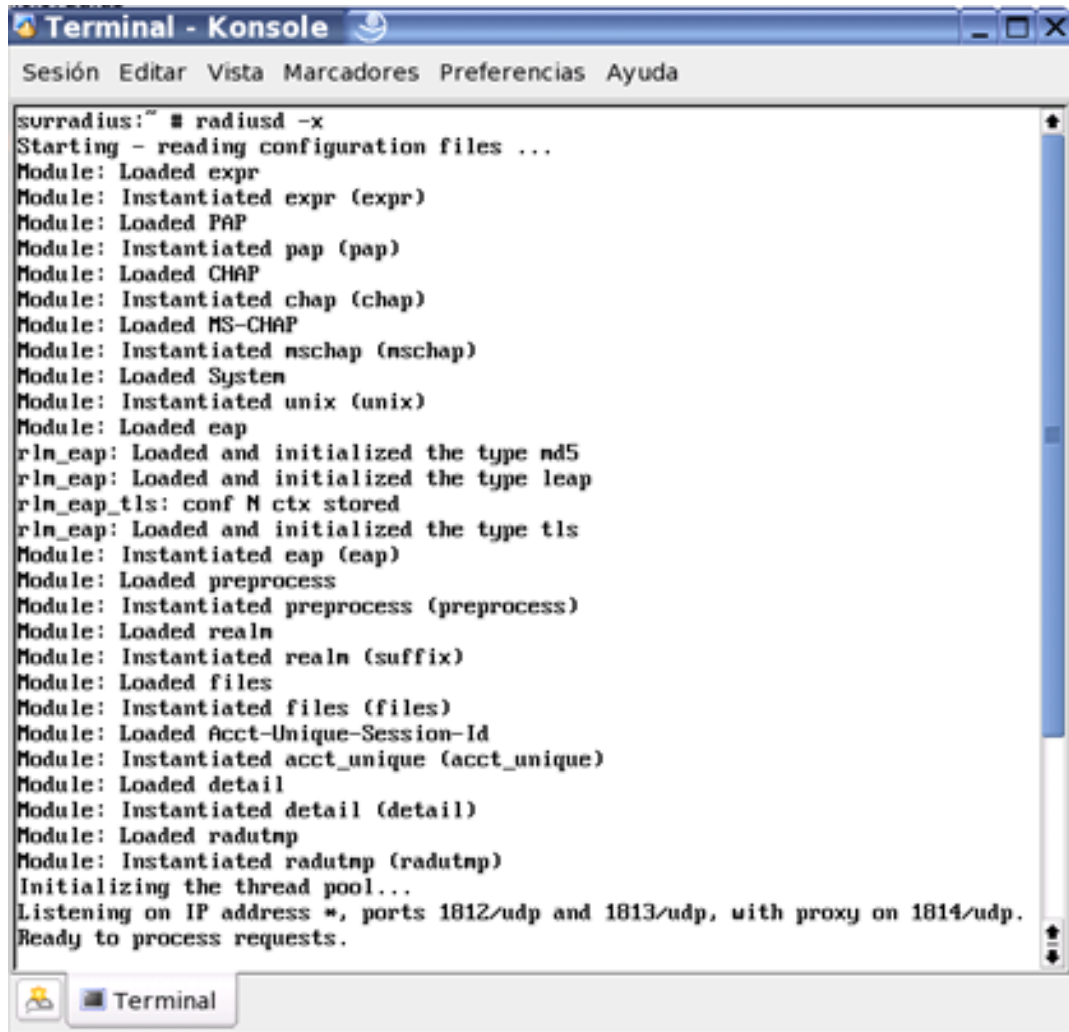
```
[Nombre de Usuario] Auth-Type := EAP
```

En nuestro caso

```
"armando" Auth-Type := EAP
```

Activar el servicio RADIUS

Una vez terminada la configuración iniciamos el servidor RADIUS con el comando: **raddiud -x**.



```
Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda

surradius:~ # radiusd -x
Starting - reading configuration files ...
Module: Loaded expr
Module: Instantiated expr (expr)
Module: Loaded PAP
Module: Instantiated pap (pap)
Module: Loaded CHAP
Module: Instantiated chap (chap)
Module: Loaded MS-CHAP
Module: Instantiated nschap (nschap)
Module: Loaded System
Module: Instantiated unix (unix)
Module: Loaded eap
rln_eap: Loaded and initialized the type nd5
rln_eap: Loaded and initialized the type leap
rln_eap_tls: conf N ctx stored
rln_eap: Loaded and initialized the type tls
Module: Instantiated eap (eap)
Module: Loaded preprocess
Module: Instantiated preprocess (preprocess)
Module: Loaded realm
Module: Instantiated realm (suffix)
Module: Loaded files
Module: Instantiated files (files)
Module: Loaded Acct-Unique-Session-Id
Module: Instantiated acct_unique (acct_unique)
Module: Loaded detail
Module: Instantiated detail (detail)
Module: Loaded radutnp
Module: Instantiated radutnp (radutnp)
Initializing the thread pool...
Listening on IP address *, ports 1812/udp and 1813/udp, with proxy on 1814/udp.
Ready to process requests.
```

Figura 3.31: Consola para la activación del Servidor

Con esto, nuestro servidor esta listo a recibir las peticione de los AccessPoint.

3.3.- Configuración del Access Point (AP)

El Access Point es el dispositivo que conecta a toda la red WLAN, para esto la misma instalación y configuración del Access Point funciona tanto para Windows como para Linux, para esto se lo realiza en dos formas de configuración.

- Configuración Básica
- Configuración Avanzada

3.3.1.- Configuración Básica

En esta configuración elegimos: el nombre del AP (AP Name) o por defecto que es DWL-2000AP+, el nombre de la red (SSID) en nuestro caso se llama labonita, el canal (Channel) 6, la IP que viene por defecto que es 192.168.0.50 con la máscara 255.255.255.0, en autenticación (Authentication) se escoge Sistema abierto (Open System) o la llave compartida (Shared Key). En cuanto a seguridad se activa el mecanismo WEP, con encriptación Hexadecimal o ASCII.

3.3.2.- Configuración Avanzada

En la configuración avanzada elegimos Authentication: WPA con el estándar 802.1x y el servidor RADIUS (RADIUS Server 1) con su IP que es 192.168.1.11, puerto (Port) 1812 que sirve para la comunicación y la clave secreta (Shared Secret) como vemos en la figura 3.32. También se puede elegir un segundo servidor (RADIUS Server 2) que nos servirá para respaldos en caso de que se caiga el primer servidor RADIUS.

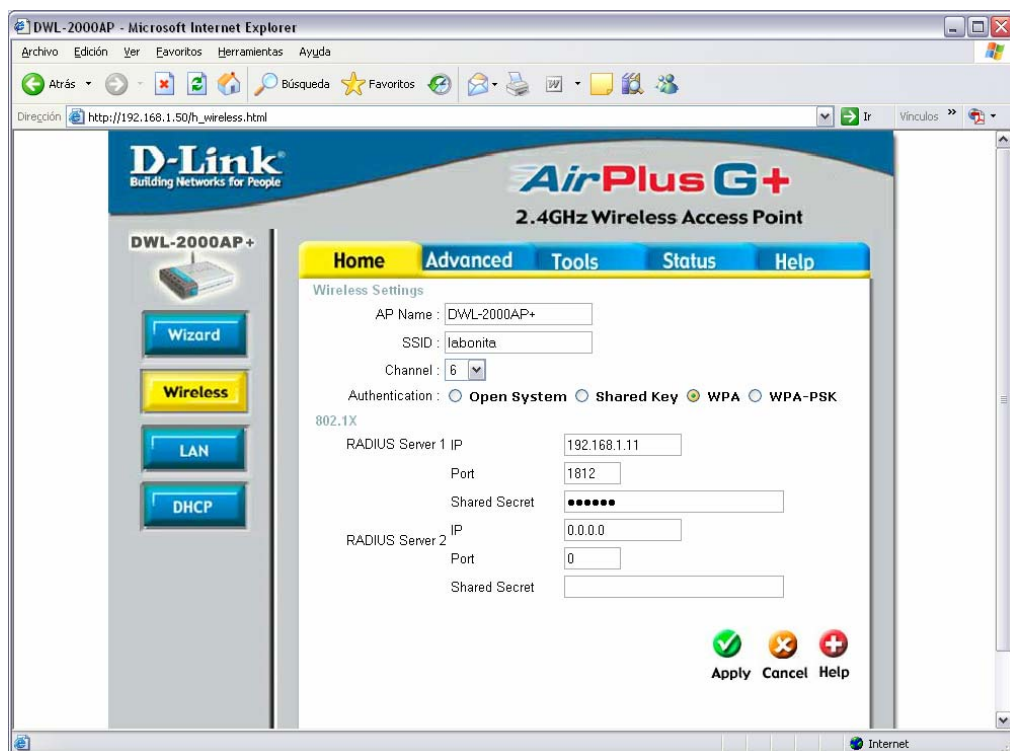


Figura 3.32: Configuración del Access Point AP

En esta Figura 3.33 podemos ver la configuración del Ethernet: con su MAC Address, IP, Mascara, Gateay y Wireless: con su SSID, tipo de encriptación y canal.

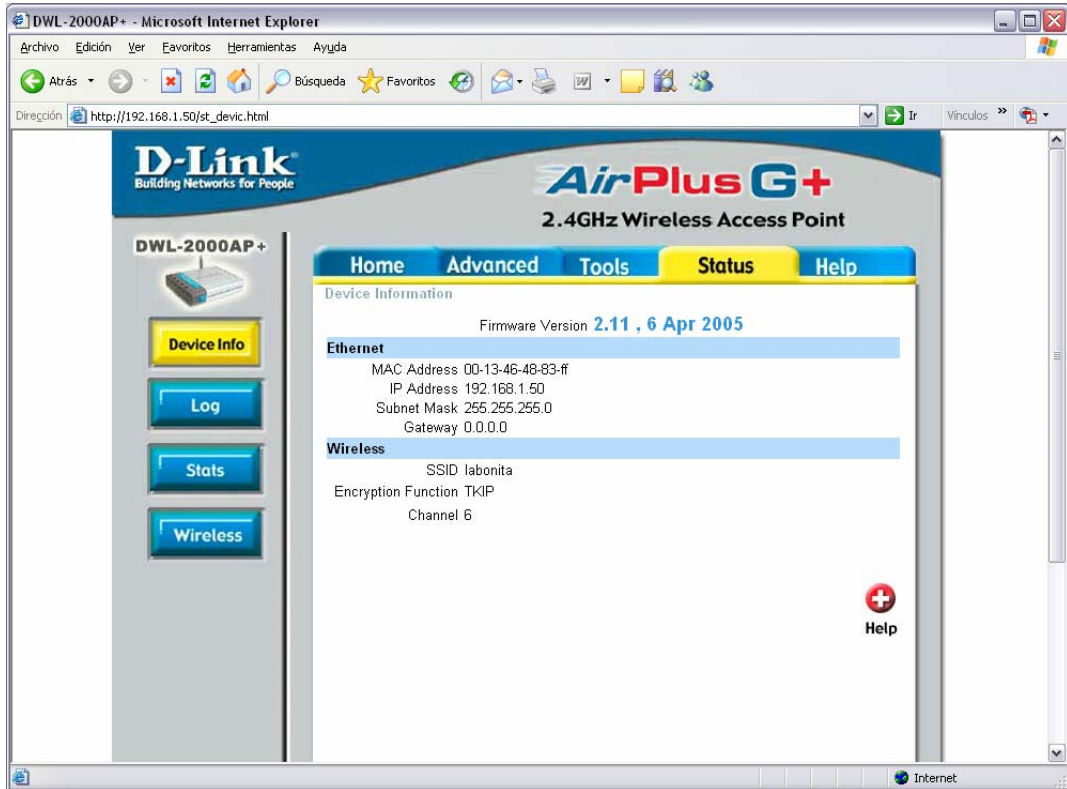


Figura 3.33: Información del Dispositivo