PRÁCTICAS TECNOL. RED AVANZADAS

INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR RADIUS

1. Introducción

En esta práctica vamos a estudiar RADIUS, un protocolo ampliamente empleado para controlar el acceso a servicios en red. En particular instalaremos una solución de código abierto denominada FreeRADIUS, y la configuraremos para un uso concreto: regular el acceso a una red inalámbrica.

Dentro de esta práctica, lo primero que vamos a estudiar es la teoría asociada a este protocolo, viendo también conceptos relacionados con el mismo, como AAA, NAS, y mecanismos de protección de redes inalámbricas (como WEP y WPA).

Posteriormente veremos eduroam, un caso real en el que se utiliza RADIUS como método global de control de acceso a las redes inalámbricas de las principales instituciones académicas de Europa. En este punto configuraremos una máquina del laboratorio para poder acceder a la red eduroam en el entorno de la UPV.

A continuación instalaremos FreeRADIUS en una máquina bajo Linux, y configuraremos el servidor para que dé servicio a un punto de acceso. Lógicamente también tendremos que configurar el punto de acceso para que funcione como cliente del servidor recién instalado. Finalmente probaremos nuestra nueva configuración de la red inalámbrica conectando a dicha red una máquina con Windows XP.

2. Definiciones

En este punto introduciremos diversos conceptos cuyo conocimiento es clave para poder entender qué se está haciendo (qué perseguimos y qué conseguimos) en los apartados posteriores de la práctica.

2.1 RADIUS

RADIUS (*Remote Authentication Dial-In User Server*) es un protocolo que nos permite gestionar la "autenticación, autorización y registro" de usuarios remotos sobre un determinado recurso. La tupla "autenticación, autorización y registro" es más conocida como AAA, al ser éste su acrónimo de su denominación original inglesa "*Authentication, Authorization, and Accounting*". Veamos a continuación a qué se refiere cada uno de estos términos:

- Autenticación (*authentication*) hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y unos credenciales por parte del usuario que demanda acceso.

Un tipo habitual de credencial es el uso de una contraseña (o *password*) que junto al nombre de usuario nos permite acceder a determinados recursos. El nombre de usuario es nuestra identidad, que puede ser públicamente conocida, mientras que la contraseña se mantiene en secreto, y sirve para que nadie suplante nuestra identidad. Otros tipos más avanzados de credenciales son los certificados digitales.

Existen muchos métodos concretos que implementan el proceso de la autenticación. Algunos de ellos, soportados por RADIUS, son:

- autenticación de sistema (*system authentication*), típica en un sistema Unix, normalmente realizada mediante el uso del fichero /etc/passwd;
- los protocolos PAP (*Password Authentication Protocol*), y su versión segura CHAP (*Challenge Handshake Authentication Protocol*), que son métodos de autenticación usados por proveedores de servicios de Internet (ISPs) accesibles vía PPP;
- LDAP (*Lightweight Directory Access Protocol*), un protocolo a nivel de aplicación (sobre TCP/IP) que implementa un servicio de directorio ordenado, y muy empleado como base de datos para contener nombres de usuarios y sus contraseñas;
- Kerberos, el famoso método de autenticación diseñado por el MIT;
- EAP (*Extensible Authentication Protocol*), que no es un método concreto sino un entorno universal de autenticación empleado frecuentemente en redes inalámbricas y conexiones punto a punto;
- por último, también se permite la autenticación basada en ficheros locales de configuración del propio servidor RADIUS.

- Autorización (*authorization*) se refiere a conceder servicios específicos (entre los que se incluye la "negación de servicio") a un determinado usuario, basándose para ello en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema. Es posible configurar restricciones a la autorización de determinados servicios en función de aspectos como, por ejemplo, la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples "*logins*" de un mismo usuario.

  El proceso de autorización determina la naturaleza del servicio que se concede al usuario, como son: la dirección IP que se le asigna, el tipo de calidad de servicio (QoS) que va a recibir, el uso de encriptación, o la utilización obligatoria de túneles para determinadas conexiones.

  Los métodos de autorización soportados habitualmente por un servidor de RADIUS incluyen bases de datos LDAP, bases de datos SQL (como Oracle, MySQL y PostgreSQL), o incluso el uso de ficheros de configuración locales al servidor.

  No se debe confundir los términos autenticación con autorización. Mientras que la autenticación es el proceso de verificar un derecho reclamado por un individuo (persona o incluso ordenador), la autorización es el proceso de verificar que una persona ya autenticada tiene la autoridad para efectuar una determinada operación.

- Registro (a*ccounting*, a menudo traducido también como contabilidad) se refiere a realizar un registro del consumo de recursos que realizan los usuarios. El registro suele incluir aspectos como la identidad del usuario, la naturaleza del servicio prestado, y cuándo empezó y terminó el uso de dicho servicio.

Es interesante el uso del protocolo RADIUS cuando tenemos redes de dimensiones considerables sobre las que queremos proporcionar un servicio de acceso centralizado (aunque posiblemente jerarquizado por medio de diversos servidores RADIUS). Por este motivo, uno de los principales usos de RADIUS se encuentra en empresas que proporcionan acceso a Internet o grandes redes corporativas, en un entorno con diversas de tecnologías de red (incluyendo módems, xDSL, VPNs y redes inalámbricas) no sólo para gestionar el acceso a la propia red, sino también para servicios propios de Internet (como e-mail, Web o incluso dentro del proceso de señalización SIP en VoIP).

Un uso de RADIUS que queremos enfatizar, al ser el que realizaremos en esta práctica, es la autenticación en redes inalámbricas (Wi-Fi), sustituyendo métodos más simples de clave compartida (*pre-shared key, PSK*), que son bastante limitados al gestionar una red cuando ésta alcanza un determinado tamaño.

Aunque RADIUS es el protocolo para AAA más extendido en la actualidad, ya existe un nuevo protocolo que está llamado a sustituir a RADIUS. Su nombre es DIAMETER, y también proporciona manejo de errores y comunicación entre dominios.

2.2 NAS

Un *Network Access Server* (NAS) es un sistema que proporciona acceso a la red. En algunos casos también se conoce como *Remote Access Server* (RAS) o *Terminal Server*. En general, NAS es un elemento que controla el acceso a un recurso protegido, que puede ser desde un sencillo teléfono para VoIP o una impresora, hasta el acceso a una red inalámbrica o a Internet (proporcionado por un ISP).

Cuando un cliente quiere hacer uso de uno de estos servicios se conecta a NAS, quien a su vez se conecta a un servidor de AAA (típicamente RADIUS) preguntando si los credenciales proporcionados por el cliente son válidos. Basándose en su respuesta, NAS le permitirá acceder o no a este recurso protegido. El sistema NAS no contiene ninguna información sobre los usuarios que se pueden conectar ni sus credenciales, sino que utiliza esta información para enviarla a RADIUS, y que éste le informe sobre los permisos del cliente.

Observa que nos encontramos en un escenario en el que hay dos niveles de la arquitectura cliente-servidor. Desde un punto de vista más global, tenemos la típica arquitectura en la que un usuario quiere acceder a un servicio, siendo el usuario el cliente, y el servidor el sistema que proporciona dicho servicio. Sin embargo, si nos centramos en el proceso de AAA, el cliente sería el sistema que proporciona el acceso a la red (por ejemplo NAS), mientras que el servidor es el sistema que autoriza o no dicho acceso (por ejemplo RADIUS). Como esta práctica se centra en este proceso, nosotros hablaremos de servidores RADIUS cuyos clientes son los elementos a proteger (por ejemplo, un punto de acceso para la conexión inalámbrica). Por tanto, desde nuestro punto de vista, los usuarios que quieren acceder al recurso protegido (por ejemplo, la

persona que se desea conectar a la red inalámbrica por medio del punto de acceso), no son clientes de RADIUS sino que se denominan suplicantes.

Una ventaja del uso de RADIUS es que sus clientes tan sólo tienen que implementar el protocolo de comunicación con RADIUS, y no todas las posibilidades de AAA existentes (PAP, CHAP, LDAP, kerberos, mySQL, etc.). En el ejemplo del punto de acceso, tan sólo necesitamos implementar una solución NAS que realice las consultas a RADIUS.

Otra ventaja del protocolo RADIUS es que, en su comunicación con NAS, nunca transmite las contraseñas directamente por la red (lo que se conoce como en *cleartext*), ni siquiera al usar PAP, sino que usa algoritmos para ocultar las contraseñas como MD5. Sin embargo, al no ser considerado MD5 un sistema de protección de credenciales demasiado seguro, es aconsejable utilizar sistemas adicionales de protección para cifrar el tráfico de RADIUS, como puede ser túneles de IPsec.

NOTA: Es importante no confundir la definición de NAS que hemos dado en este apartado con el NAS como "*Network-Attached Storage*", que comunmente se refiere a discos duros conectados directamente a una red.

2.3 Seguridad en tecnologías de red inalámbrica

En redes inalámbricas con infraestructura se utiliza un punto de acceso (*wireless access point*, WAP o simplemente AP) para interconectar todos los dispositivos inalámbricos de la red. Usualmente un AP se conecta también a una red cableada, transmitiendo datos entre los dispositivos conectados a la red por cable y los dispositivos inalámbricos.

La seguridad es un tema importante en las redes inalámbricas porque, al contrario que en una red cableada a la que sólo tienen acceso las personas que físicamente pueden conectarse, cualquier persona de la calle o pisos o edificios vecinos pueden conectarse a una red inalámbrica o ver el contenido de los paquetes que circulan por ella si ésta no está convenientemente protegida.

Algunos de los principales protocolos estándar para proporcionar seguridad en redes inalámbricas IEEE 802.11 son:

- WEP (*Wired Equivalent Privacy*). Fue introducido en 1997 con objeto de proporcionar un nivel de confidencialidad similar al de las redes cableadas. Usa una clave estática de 64 ó 128 bits con el algoritmo RC4. Su uso se desaconseja completamente, ya que aunque es muy fácil de configurar y está muy extendido al ser el primero que surgió, presenta graves fallos de seguridad.

- WPA (*Wi-Fi Protected Access*) fue creado para corregir los múltiples fallos detectados en el protocolo WEP. WPA fue diseñado por el consorcio *Wi-Fi Alliance* basándose en un borrador del estándar 802.11i (es un subconjunto del mismo), y utiliza TKIP (*Temporal Key Integrity Protocol*) como protocolo de cifrado que sustituye a WEP sin necesidad de modificar el hardware existente (podría funcionar actualizando el firmware).

En concreto, WPA sigue usando RC4 como algoritmo de cifrado con claves de 128 bits, pero usa TKIP para cambiar dinámicamente estas claves.

WPA fue diseñado para ser usado junto a un servidor AAA (habitualmente RADIUS), de manera que se asignan claves distintas a cada uno de los posibles usuarios. Sin embargo, para entornos domésticos o pequeñas oficinas también se puede usar, de forma menos segura, con una única clave compartida (*pre-shared key*, PSK). En este caso hablamos de WPA-PSK.

- WPA2 se basa en el nuevo estándar 802.11i, y el cambio más significativo respecto a WPA es que usa el protocolo de cifrado AES en lugar de RC4. Mientras que WAP puede ejecutarse en el hardware que soporte WEP (tras actualizar el firmware), WAP2 necesita un hardware más nuevo (posterior al 2004). Sin embargo, se sabe que WAP también terminará siendo comprometido a medio plazo y por tanto sólo se recomienda como transición a WAP2.

Otro concepto relacionado con la seguridad en redes inalámbricas que merece la pena destacar es EAP (*Extensible Authentication Protocol*). EAP es un marco general de autenticación, y no un mecanismo de autenticación concreto. EAP proporciona algunas funciones comunes y un método para negociar el mecanismo de autenticación a usar. Actualmente hay más de 40 métodos distintos. En esta práctica haremos uso del denominado EAP protegido (PEAP) para la autenticación de nuestro usuario en la red inalámbrica. Como nuestro suplicante es una máquina con WindowsXP, usaremos MSCHAPv2, la versión de PEAP empleada por Microsoft en este S.O.

3. eduroam: una infraestructura de roaming basada en RADIUS

3.1 El proyecto eduroam

Eduroam (EDUcation ROAMing) es un proyecto internacional creado para facilitar el acceso a Internet a los miembros de las instituciones científico-académicas asociadas, desde cualquiera de estas instituciones. Son miembros de este proyecto la mayor parte de centros europeos de investigación (en http://www.eduroam.es/instituciones.es.php se encuentra una lista de los centros españoles), y algunos otros de la zona del Pacífico Asiático.

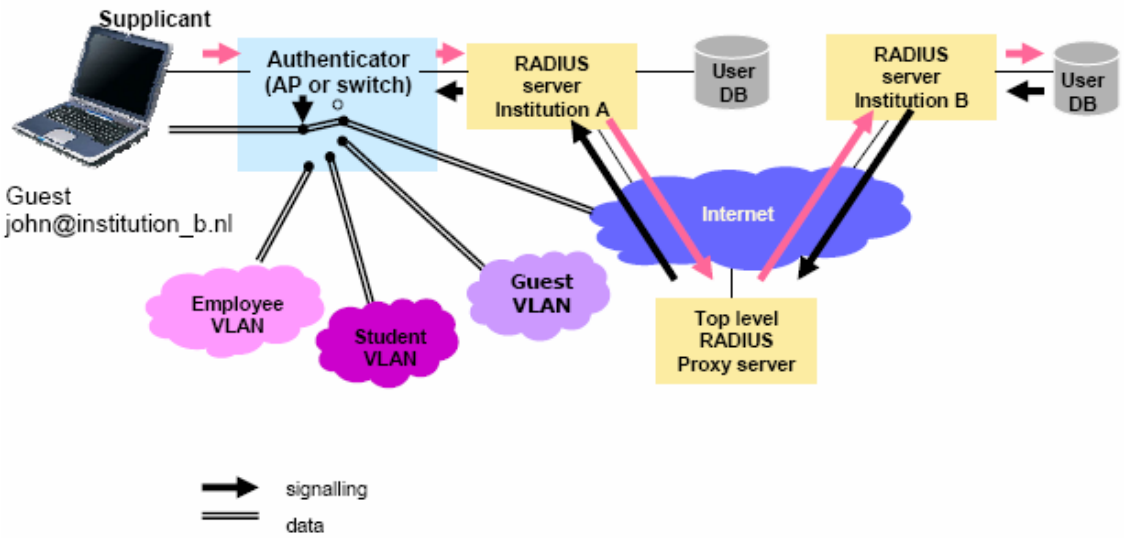
En concreto, en la siguiente figura se puede observar los países europeos pertenecientes al proyecto, y las redes institucionales asociadas (por ejemplo, en España esta red es RedIris).

La ventaja de pertenecer a este proyecto es obvia, a cambio de que los usuarios de otras instituciones se puedan conectar a la red de tu centro, los usuarios de tu centro se pueden conectar a Internet desde cualquier centro asociado al proyecto.

La conexión a Internet se hace habitualmente mediante un punto de acceso inalámbrico (cuyo identificador SSID es “eduroam”) que conecta al usuario directamente a una red IEEE 802.11 local. El proceso de autenticación se hace mediante el protocolo EAP, que como ya hemos visto permite usar varios métodos de autenticación. Esta autenticación la hace siempre el centro al que pertenece el usuario (y no el centro al que se quiere conectar), y para llevar a cabo este proceso de manera segura y escalable se emplea el protocolo RADIUS. Para los usuarios de la UPV se emplea actualmente el modo EAP protegido con autenticación MSCHAPv2.

Una vez que el usuario ha sido autenticado, y se la ha concedido permiso para acceder a la red, la comunicación entre el punto de acceso y el usuario durante la conexión a Internet se hace cifrada mediante claves dinámicas. Esta configuración depende únicamente del centro al que se conecte el usuario, y en el caso de acceder a la UPV se hace actualmente con el protocolo WPA mediante cifrado TKIP.

La arquitectura que se usa para permitir la autenticación en eduroam mediante RADIUS es similar a la que se muestra en la siguiente figura.



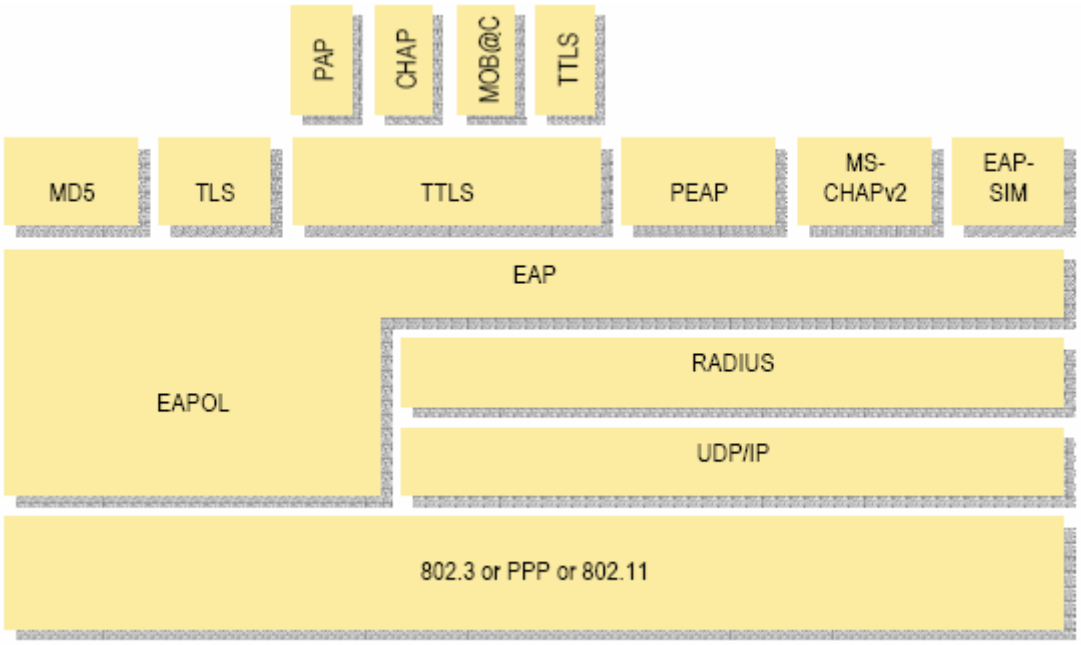
RADIUS se usa habitualmente para permitir *roaming* entre ISPs o redes de distinta propiedad (como en el proyecto eduroam), y para esto se emplea un identificador conocido como **realm**, que identifica a qué servidor RADIUS se debe redirigir el proceso de AAA.

Cuando el usuario externo solicita acceso a la red, éste actúa como suplicante, de forma que el punto de acceso (AP) se conecta al servidor RADIUS para que le indique si los credenciales del suplicante le autorizan a acceder a la red. Los credenciales siempre incluyen un nombre de usuario del tipo "usuario*@realm*", de forma que al incluir un *realm* en el nombre, el servidor RADIUS se da cuenta de que el proceso de AAA lo debe realizar otro servidor RADIUS (siempre y cuando el *realm* no sea el del propio centro). De esta forma, el servidor local se comporta como un *proxy* RADIUS, redirigiendo la consulta al servidor RADIUS que realmente tiene información sobre este usuario. La información sobre los posibles servidores asociados se encuentra en una tabla de *realms* conocidos por el servidor.

Tal y como se observa en la figura anterior, en el caso concreto del proyecto eduroam existe un *proxy* RADIUS de nivel superior, que conoce todos los *realms* asociados al proyecto, y al que se le hacen todas las consultas, para que él las redirija al servidor destino de la consulta.

Observa que este funcionamiento de RADIUS mediante *proxies* es otra de las características fundamentales de este protocolo, que permite una organización jerárquica de todo el proceso, y facilita el *roaming*.

Por último recordar que es importante que tanto el suplicante como el servidor RADIUS destino realicen el proceso de autenticación usando el mismo tipo de EAP. En la siguiente figura se presenta un esquema de algunas de las diversas formas de autenticación que soporta EAP.



3.2 Configuración de un suplicante para eduroam

En este punto vamos a configurar una máquina con Windows XP SP2 y tarjeta de red inalámbrica para que se conecte a la red eduroam en la propia UPV. La idea es que esta configuración nos puede servir como base para cuando queramos conectar nuestro ordenador a cualquier otra red asociada al proyecto eduroam.

La configuración es muy sencilla. Simplemente debemos ir "Inicio→ Conectar a→ Conexiones de red inalámbricas", y allí seleccionar "Cambiar configuración avanzada".

A continuación seleccionar la pestaña "Redes inalámbricas" y seleccionar dentro de la lista de redes disponibles la red "eduroam" y pulsar propiedades (si no estuviera la red en la lista, podemos pulsar directamente el botón agregar).

En este momento vamos a configurar la red eduroam de la UPV.

- En la pestaña "Asociación" configuramos el estándar de seguridad que vamos a usar para la comunicación entre nuestro ordenador y el punto de acceso. El SSID es siempre "eduroam", mientras que los campos "autenticación de red" y "cifrado de datos" dependen de la red en la que estemos conectados. Para la UPV seleccionaremos WPA y TKIP respectivamente. Sin embargo, **en otros centros esta configuración podría ser diferente** y por tanto hay que consultar siempre cuál es la configuración de este apartado en el centro destino.

- En la pestaña "Autenticación" vamos a indicar la forma de autenticarnos dentro de la red. Este apartado depende del centro al que pertenezca el usuario, y para los miembros de la UPV es mediante PEAP. Además vamos a deseleccionar los apartados "Autenticar como equipo cuando la información de equipo esté disponible" y "Autenticar como invitado cuando el usuario o la información de equipo no estén disponibles".

Por último, seleccionamos propiedades de PEAP, indicando que no nos vamos a validar usando un certificado, que tampoco queremos habilitar reconexión rápida, y como método de autenticación seleccionaremos EAP-MSCHAPv2, que configuraremos para que no use automáticamente el nombre de inicio de sesión y contraseña de Windows.

- En la pestaña "Conexión" podemos elegir si queremos conectarnos automáticamente cuando se detecte la presencia de esta red.

A continuación, al intentar conectarnos a la red por primera vez, Windows nos mostrará un globo en el que se indica que hagamos clic en él para seleccionar los credenciales. Como nombre de usuario debemos indicar "*usuario*@alumno.upv.es"[1], siendo usuario nuestro *usuario* dentro de la UPV, y como contraseña la que usemos normalmente en nuestra cuenta UPV. El dominio se deja en blanco.

Para más ayuda sobre configurar eduroam, o guías para configuración en otros sistemas operativos, consultar en http://infoacceso.webs.upv.es/accwlan/eduroam.

4. Instalación y configuración del servidor FreeRADIUS

4.1 FreeRADIUS

FreeRADIUS es un paquete de software de código abierto y libre distribución que implementa diversos elementos relacionados con RADIUS, tales como una biblioteca BSD para clientes, módulos para soporte en apache, y lo que más nos interesa en este punto, un servidor de RADIUS.

El servidor FreeRADIUS es modular, para facilitar su extensión, y es muy escalable. Además, tiene casi todas las opciones que un usuario puede necesitar:

- Para realizar las tareas de AAA puede almacenar y acceder a la información por medio de múltiples bases de datos: LDAP (AD, OpenLDAP,…), SQL (MySQL, PostgreSQL, Oracle,…) y ficheros de texto (fichero local de usuarios, mediante acceso a otros Realms, fichero de sistema /etc/passwd,…)

- Soporta prácticamente toda clase de clientes Radius (por ejemplo, ChilliSpot, JRadius, mod_auth_radius, pam_auth_radius, Pyrad, extensiones php de RADIUS, etc)

- Se puede ejecutar en múltiples sistemas operativos: Linux (Debian, Ubuntu, Suse, Mandriva, Fedora Core, etc.), FreeBSD, MacOS, OpenBSD, Solaris, e incluso MS Windows por medio de cygwin.

- Soporta el uso de proxies y la replicación de servidores.

[1] OJO, si somos antiguos alumnos deberemos introducir como nombre de usuario "usuario@aaa.upv.es", y si somos PAS o PDI "usuarios@upv.es".

4.2 Instalación

En esta última parte de la práctica vamos a instalar un servidor de FreeRADIUS sobre una distribución Debian 4.0 de Linux , y lo vamos a configurar para que dé servicio de autenticación a un punto de acceso, que a su vez también deberemos configurar para que sea cliente de RADIUS (actuando como un NAS).

La versión de FreeRADIUS que vamos a instalar es la 2.1.1, que se puede bajar directamente de http://freeradius.org/download.html, y también se encuentra disponible en los recursos de la asignatura. Lo primero que deberemos hacer es descargarnos los fuentes de FreeRADIUS (fichero .tar.gz) localmente en la máquina Debian, y descomprimirlos (usando "tar" con las opciones –xvzf).

Antes de poder compilar e instalar el servidor, necesitaremos una serie de paquetes adicionales de Debian. Estos paquetes son los siguientes: "gcc", "build_essential", "libssl-dev" y "libpq-dev". Para poder instalarlos necesitamos abrir una consola y pasar a ser superusuario (mediante la orden "su"), y usar la orden "apt-get install xxx" (donde xxx es el paquete a instalar). La instalación está configurada para que la descarga se realice automáticamente por medio de ftp.

Una vez preparada la máquina para la compilación, podremos ir al directorio en el que se ha descomprimido ("cd freeradius-server-2.1.1"). El proceso básico de la instalación se encuentra descrito en el fichero de texto INSTALL (lo puedes editar usando gedit). En primer lugar, debemos hacer una operación de configuración. Mediante la orden "./configure --help" podemos ver las opciones disponibles, nosotros usaremos las opciones por defecto.

Una vez configurado el proceso, realizaremos la compilación mediante "make", y posteriormente, si no ha ocurrido ningún error, instalaremos el software en el sistema mediante "make install".

Si el proceso es correcto, ya podremos ejecutar el servidor. Sin embargo, como la primera vez que se ejecute el servidor se crearán los certificados necesarios para operar con EAP, antes de esta primera ejecución es conveniente que configuremos estos certificados con los atributos que más se ajusten a nuestra instalación.

En concreto la configuración de los certificados se puede realizar editando los ficheros de configuración que se encuentran en /usr/local/etc/raddb/certs. Aquí podremos editar la configuración de los certificados de la autoridad certificadora (fichero ca.cnf), los usados como servidor (server.cnf), y los de cliente (client.cnf). Los atributos a configurar son el país, provincia, localidad, organización, dirección de correo electrónico y nombre común. Observa que para su correcto funcionamiento, el servidor y la autoridad certificadora deben coincidir en país, estado y organización.

Una vez configurados los certificados, ya podremos ejecutar el servidor, mediante la orden "radiusd –X" (la X se utiliza para funcionar en modo debug, y así recibir información sobre los eventos que se suceden en el servidor). Tal y como hemos dicho previamente, la primera vez que se ejecute el servidor se crearán los certificados necesarios. Si todo va bien, el servidor debe quedarse escuchando en los puertos asociados a los servicios que ofrece.

Para comprobar que el servidor está funcionando correctamente, podremos hacer uso de la herramienta "radtest", de la siguiente manera:

$ radtest usuario contraseña localhost 10 testing123

donde "usuario" y "contraseña" son las credenciales de un usuario local de la máquina. "tesing123" es lo que se denomina un secreto, que permite asociar de manera segura un cliente al servidor. Este cliente ya está configurado en la máquina, tal y como veremos posteriormente, por tanto, y si todo es correcto la respuesta debe ser "Access-Accept". Puedes observar también los mensajes en pantalla que se visualizan en el servidor cuando éste recibe una solicitud. Si quieres ver una solicitud rechazada, puedes volver a realizar una solicitud de servicio, pero cambiando el secreto por otro cualquiera.

4.3 Configuración básica del servidor

La configuración del servidor se hace mediante el fichero "radiusd.conf" del directorio /usr/local/etc/raddb. Aquí podemos seleccionar aspectos relacionados con el servidor (ficheros de log, parámetros de uso máximo, usuarios, grupos, …), bases de datos a utilizar para autenticar y autorizar (ficheros, SQL, LDAP, …), métodos de AAA, etc.

Para evitar una excesiva longitud de este fichero y por cuestiones de organización, "radiusd.conf" se subdivide en varios ficheros mediante la directiva "$INCLUDE":

- eap.conf: Se utiliza para configurar el tipo de EAP a emplear
- clients.conf: Tiene la lista de clientes que están autorizados para usar los servicios de AAA proporcionados.
- proxy.conf: Este fichero configura directivas relacionadas con el funcionamiento en modo proxy y la lista de realms.
- Otros ficheros como sql.conf (para configurar el acceso a bases de datos SQL), policy.conf, etc.

Además, el fichero "users" contiene información sobre la autenticación de suplicantes, de forma que incluso podemos añadir credenciales en forma de usuario y contraseña para permitir una configuración sencilla de usuarios (ten en cuenta que estos usuarios serán realmente clientes del NAS, y no directamente del servidor RADIUS).

Como vamos a trabajar con suplicantes bajo Windows XP, configurados como hemos visto previamente para eduroam en la UPV, vamos a necesitar soporte de PEAP y mschapv2. Para esto editamos el fichero eap.conf, y cambiamos el atributo "default_eap_type" general, de "md5" a "peap" (en minúsculas), y en el apartado de peap asegúrate de que "default_eap_type" esté a "mschapv2". En principio, si usamos la versión 2.1.1 de Radius no deberíamos necesitar cambiar nada más en este fichero, ya que la parte de "peap" está descomentada por defecto.

A continuación tenemos que informar al servidor RADIUS de que va a tener como cliente un punto de acceso. Para ello, editamos el fichero clients.conf, y añadimos las siguientes líneas:

```
client 192.168.1.1 {
        secret          = secretotra
        shortname       = ap
        nastype         = cisco
}
```

Fíjate que el punto de acceso va a tener como dirección IP por defecto "192.168.1.1", por la configuración del propio punto de acceso que vamos a emplear, y que como secreto para la configuración posterior de NAS en el punto de acceso usaremos "secretotra"

Por último vamos a añadir un usuario que será utilizado por el suplicante cuando solicite acceso a la red inalámbrica. Para esto editamos el fichero users, y añadimos el siguiente usuario y contraseña:

```
"TuNombre"      Cleartext-Password := "passwordtra"
                Reply-Message = "Bienvenido"
```

Para que la nueva configuración del servidor tenga efecto, interrumpiremos su ejecución y lo volveremos a lanzar, tecleando nuevamente "radiusd –X"

4.4 Configuración de un punto de acceso para autenticar con RADIUS

En este punto vamos a configurar el uso de RADIUS en un punto de acceso, que además tendrá funciones de router y asignación de direcciones privadas con NAT, como los típicos routers inalámbricos domésticos.

La configuración del punto de acceso de un routers domésticos suele hacerse mediante interfaz de Web. Además, queremos que el punto de acceso esté en la misma red que el servidor RADIUS, conectados ambos directamente por un cable de red. Por estos dos motivos, el ordenador con Debian está conectado directamente a la red privada del router, en lugar de a la red de la UPV.

A continuación accederemos a la pantalla de configuración del punto de acceso, usando un cliente de Web (en Debian podemos usar el navegador Web "Iceweasel"), y conectándonos a la dirección IP del router (por defecto será 192.168.1.1), usando el usuario y contraseña requeridos para la administración (en muchos casos tanto el usuario como la contraseña son "admin").

En primer lugar, ve al apartado de configuración "wireless" y anota el SSID de tu punto de acceso (para saber el nombre de la red que estás configurando). A continuación vamos a hacer una configuración similar a la empleada en eduroam en la UPV, por lo que como método de autenticación indicaremos WPA (sin PSK) y encriptación TKIP. Por último, para indicar que estamos usando un servidor RADIUS, accede a la parte de configuración RADIUS e introduce la dirección IP de la máquina que ejecuta el servidor y la palabra secreta (en nuestro caso, "secretotra"). Guarda esta configuración y habremos terminado.

Recuerda que para obtener la dirección IP que se le ha asignado a tu máquina puedes usar el comando "ifconfig" en Linux. Además observa que la dirección que hemos

obtenido en este caso ha sido asignada automáticamente por el router, dentro de su red privada, por lo que corremos el peligro de que al rearrancar el servidor se nos asigne una dirección IP distinta, y tengamos que actualizar la configuración del punto de acceso con la nueva IP. Para evitar esto en una configuración definitiva deberíamos asignar al servidor una IP estática dentro de la red privada.

4.5 Configuración del suplicante

Para el suplicante en Windows XP vamos a usar una configuración muy similar a la empleada con eduroam en la UPV (ya hemos configurado el punto de acceso y el servidor RADIUS para que esto sea así). Por lo tanto, la configuración de nuestra máquina con Windows XP para que acceda a nuestra red inalámbrica se hará de la misma forma que realizamos para conectarnos a la red eduroam, pero seleccionando nuestra red (según el SSID que hemos anotado en el aparado anterior), y empleando como usuario y contraseña el que configuramos localmente en el fichero de usuarios de FreeRADIUS (en concreto "TuNombre" y "passwordtra")

5. Ampliaciones opcionales de la práctica

FreeRADIUS es servidor complejo y que tiene muchas funcionalidades y opciones. Para aquellos alumnos que deseen de forma autónoma aprender más sobre el servidor, y todo el paquete FreeRADIUS, pueden encontrar más documentación en las páginas del manual disponibles en http://freeradius.org/radiusd/man/, y también en la zona de documentación Wiki de FreeRadius http://wiki.freeradius.org/. Aquí, entre otras cosas, pueden encontrar más detalles sobre las posibles opciones de configuración.

Otra forma aconsejada por los desarrolladores de FreeRADIUS para obtener más información sobre los ficheros de configuración es leer los propios comentarios que se encuentran en los mismos. Ten en cuenta que la configuración de estos ficheros puede variar de una a otra versión de FreeRADIUS, por lo que es importante que te asegures de que la información que encuentres sobre configuración del servidor freeRADIUS se corresponde con la versión que tienes instalada.

Una posible ampliación de la práctica es configurar el servidor para que la información de usuarios para AAA se encuentre en una base de datos. Para esto habría que instalar la base de datos a emplear (por ejemplo LDAP, MySQL, postgreSQL, etc.), insertar la información de usuarios, y configurar FreeRADIUS para que use la base de datos correspondientes.