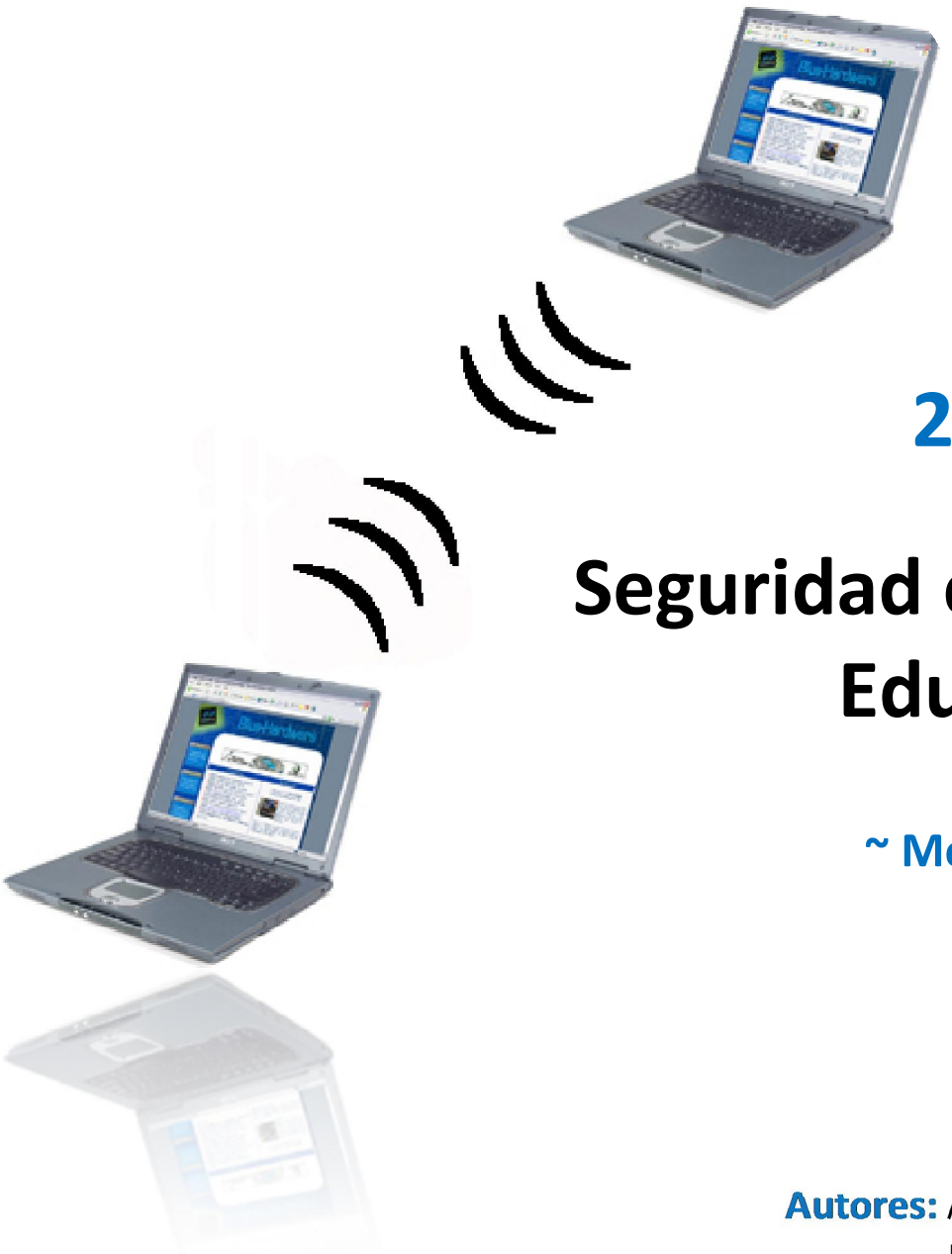
ESCUELA TÉCNICA SUPERIOR DE INGENIEROS

Redes y Servicios de Radio



2010

Seguridad en redes WiFi Eduroam

~ Memoria ~

Autores: Andra FILIP
Estefanía VÁZQUEZ TORRES

Tutor: José Manuel FORNÉS RUMBAO

Índice

Introducción 4
I. Introducción a la seguridad en las redes inalámbricas 5
1. Métodos de autenticación 5
2. Autenticación Abierta 5
3. WEP 5
3.1. Introducción 5
3.2. Autenticación WEP 6
3.3. Formato de Trama 7
4. 802.1x 7
5. WPA/WPA2 8
5.1. Características WPA 9
5.2. Mejoras de WPA con respecto a WEP 9
5.3. Métodos de funcionamiento de WPA 10
5.4. Debilidades de WPA 10
5.5. Características WPA2 y mejoras 10
5.6. Debilidades de WPA2 10
6. WPA empresarial: el protocolo de autenticación EAP 11
6.1. Certificado digital 11
6.2. Autoridad de certificación 12
6.3. Privacidad TLS 12
6.4. Características de WPA-EAP 13
a) EAP-TLS 15
b) EAP-TTLS 16
c) EAP-MD5 17
d) EAP-LEAP 18
e) EAP-FAST 18
f) EAP-PEAP 19
g) EAP-MS-CHAP 19
h) EAP-POTP 20
i) EAP-GTC 20
j) EAP-SIM 20
k) EAP-AKA 21
7. Clave Precompartida o PSK 21
8. Mecanismos de cifrado o encriptación 22
9. El mecanismo RC4 22
9.1. Características de RC4 22
9.2. Ataques al algoritmo RC4 23
9.3. Debilidades del KSA 23
10. WEP 24
10.1. Introducción 24
10.2. Funcionamiento de WEP 24
a) Vector de inicialización (IV) 24
b) Claves WEP 24
c) Fragmentación 25
d) ICV o Integrity Check Value 25
e) Preparación de la MPDU 25
10.3. Debilidades de WEP 26
a) Autenticación 26
b) Integridad de mensajes 27
c) Privacidad 27

c.1) Reutilización de IV 27
c.2) Valores débiles de las claves RC4 28
c.3) Ataques directos de clave 28
11. RSA 29
12. 3DES 30
13. AES 31
14. SHA 34
14.1. Funcionamiento de SHA 34
14.2. Debilidades de SHA 36
14.3. Algoritmo SHA-2 36
14.4. El concurso SHA-3 37
15. MD5 37
II. Proyecto Eduroam 37
1. Eduroam. ¿Qué es? 37
2. Alcance del proyecto a nivel mundial 38
2.1 Breve historia de Eduroam 38
2.2 Organismos reguladores 38
2.2.1 Organismos reguladores en Europa 38
2.2.2 Organismos reguladores en España 39
3. Descripción de las tecnologías usadas en Eduroam 40
3.1 Elementos de la red y su funcionamiento 40
3.2 Aspectos relacionados con la seguridad 43
3.3 Aspectos relacionados con el uso de la red 44
4. Implementación 44
5. Implementación de Eduroam en la Universidad de Sevilla 46
6. Conexión de distintos dispositivos a Eduroam. Pasos teóricos a seguir para conectarlos 47
6.1. Introducción 47
6.2. Características de la conexión a ReInUS 47
a) Configuración ordenador con Windows 7 48
b) Configuración ordenador con Windows Vista 55
c) Configuración ordenador con XP 61
d) Configuración ordenador con Linux 61
e) Configuración ordenador con MacOS 64
e1) Configuración en Mac/OS Panther 64
e2) Configuración en Mac/OS Leopard 65
f) Configuración en iPhone Apple 68
g) Configuración de un PDA con Windows Mobile 71
h) Configuración de un móvil con Symbian 75
i) Configuración de un móvil con Android 79
III. Problemas que presenta la red Eduroam y posibles soluciones 80
1. Dispositivos que utilizan el sistema operativo Symbian 80
2. Dispositivos que utilizan el sistema operativo Android 81
3. Pruebas realizadas con otros dispositivos 82
4. Revuelo en la comunidad Eduroam 82
IV. Conclusiones 83

Glosario 85
Bibliografía 86

Introducción

La necesidad de una red que permita el acceso a internet es una realidad hoy en día para muchas organizaciones. La mayoría de estas organizaciones optan por la instalación de redes inalámbricas, debido a las numerosas ventajas que proporcionan. Entre estas ventajas podemos destacar la reducción de gasto en infraestructura y cableado, así como la comodidad ante la que nos encontramos. Las redes WiFi, sin embargo, también presentan una serie de problemas, que giran casi en su totalidad en torno al aspecto de la seguridad.

En este campo surgen dos problemas principales: el problema de la autenticación y el de la privacidad. Para resolver el primero de ellos, se debe implementar un mecanismo que impida que usuarios no autorizados accedan a nuestra red, permitiendo a aquellos que sí lo están acceder de una forma segura y cómoda. Además al eliminarse el cable, que si bien podía ser interceptado, presentaba más oposición, nos encontramos con que la información se traslada por el aire, y que cualquier persona con los dispositivos adecuados puede acceder a ella. Para evitar que esto ocurra se han desarrollado una serie de mecanismos, que proporcionarán la privacidad y confidencialidad necesarias para la comunicación.

Entre las organizaciones que presentan esta necesidad de conectarse a la red cabe destacar las universidades. En esta organización, a diferencia de lo que puede ocurrir en otras, surge un nuevo elemento a tener en cuenta a la hora de ofrecer este servicio: permitir la posibilidad de que los usuarios (profesores, investigadores, estudiantes y otros miembros del personal universitario) puedan desplazarse entre distintos centros, de distintas universidades del mundo, y seguir teniendo conexión allí donde vayan. Actualmente se está llevando a cabo un proyecto, conocido con el nombre de EDUROAM que responde a esta necesidad.

En la primera parte de este documento vamos a describir algunos de los métodos de autenticación y cifrado existentes. Se va a analizar brevemente su funcionamiento, así como sus principales ventajas y limitaciones.

El objeto de estudio de la segunda parte va a ser la iniciativa EDUROAM. El proyecto EDUROAM ilustra la implementación de los mecanismos de autenticación y cifrado más actuales de entre los descritos en la primera parte en una red real. Se va a realizar una descripción de este proyecto, su puesta en marcha en diversos puntos de la geografía y los pasos necesarios a seguir para poder conectar cualquier dispositivo a esta red de una forma cómoda y segura.

Conectar ciertos dispositivos a una red de este tipo no siempre resulta sencillo. Por ello, en la última parte vamos a mostrar cómo conectar algunos equipos concretos a la red EDUROAM de ciertas organizaciones, los problemas surgidos y sus posibles soluciones.

I. Introducción a la seguridad en las redes inalámbricas

La seguridad en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio no seguro, se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad.

La falta de seguridad involucra las siguientes partes:

- Confidencialidad: evitar que un tercero pueda acceder a la información enviada.
- Integridad: evitar que un tercero pueda modificar la información enviada sin que lo advierta el destinatario.
- No repudio: Permite a cada lado de la comunicación probar que el otro lado ha participado en la comunicación.
- Autenticación: Asegura la veracidad en la identidad de los involucrados en el proceso.

1. Métodos de autenticación

La autenticación es el proceso de verificar y asegurar la identidad de las partes involucradas en una transacción. Si este servicio no se llevara a cabo cabe la posibilidad de que una entidad desconocida asuma una identidad falsa, comprometiendo de esta manera la privacidad y la integridad de la información. En el contexto de las redes LAN, la autenticación es la medida diseñada para establecer la validez de una transmisión entre puntos de acceso y/o estaciones inalámbricas.

2. Autenticación Abierta

En primer lugar tenemos la Autenticación Abierta, en la cual el dispositivo cliente envía un simple mensaje de solicitud de autenticación, al que el punto de acceso (AP) contesta con un mensaje de aprobación.

En principio, al operar en este modo un AP siempre acepta cualquier solicitud. No obstante existe una variante por la cual el AP poseería una lista de direcciones MAC autorizadas en base a la que devolvería un mensaje de éxito o no. Esto nos proporciona un nivel muy leve de protección, ya que la suplantación de MACs es una práctica relativamente simple que desbarataría el sistema.

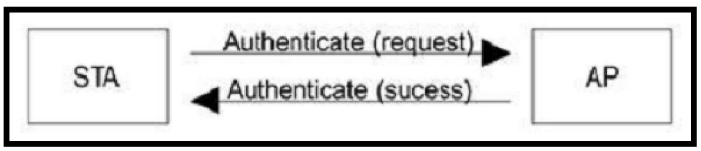


Figura 1: Red abierta

3. WEP

3.1. Introducción:

WEP (Wired Equivalent Privacy) era el método de seguridad original del protocolo 802.11 y el único que hubo durante sus primeros cinco años de vida.

En la publicación de WEP se enunciaron una serie de objetivos que se pretendía que cumpliera:

- Ser razonablemente fuerte. Tiene una clave relativamente larga, y un vector de inicialización que va cambiando la clave efectiva usada en cada paquete.

- Tener la capacidad de que paquete se pueda encriptar y desencriptar por sí solo. Esto es imprescindible en una WLAN, ya que los paquetes perdidos representan un alto porcentaje. Supondría un gran problema que perder un paquete impidiera desencriptar los siguientes.
- Ser eficiente y poderse implementar en hardware o software.
- Ser exportable. Poder utilizarse en todo el mundo.
- Ser opcional.

Se buscaba algo razonablemente fuerte a la vez que una implementación simple y con posibilidad de exportación.

El sistema de seguridad propuesto por el primer estándar tenía dos modos de operación posibles:

- Open Security, que en la práctica no representaba ninguna seguridad. Se corresponde con la autenticación abierta descrita en el apartado anterior.
- Shared Key, que se basa en el conocimiento por parte de ambos extremos de una clave que debe permanecer secreta.

A partir del año 2000 aproximadamente, las redes WIFI se hicieron muy populares, por lo que comenzaron a atraer la atención de la comunidad criptográfica. Rápidamente se descubrieron grietas de seguridad en WEP, de modo que a finales de 2001 ya había en internet herramientas para derrotarlo.

Se ha criticado mucho que el diseño de WEP fuera tan débil. Esto es cuestionable debido a que en el momento de diseño de WEP la comunidad de expertos en seguridad no se implicó demasiado en su diseño, ya que no se pensó que fuera a despertar tanto interés por los hackers como el que finalmente ha tenido.

3.2. Autenticación WEP:

En este tipo de autenticación, existirá una clave secreta, que será empleada sobre un algoritmo para encriptar y desencriptar mensajes. De esta forma para ser capaz de enviar un mensaje hay que saber como encriptarlo y así estamos demostrando que somos un usuario autorizado. La autenticación se basa en la posesión de una clave.

En la Autenticación WEP tenemos un proceso de intercambio de cuatro mensajes. En este protocolo el punto de acceso envía un mensaje al cliente, para que éste efectúe una trasformación sobre él. El mensaje de prueba es un número aleatorio de 128 bits de longitud llamado *challenge text*. Sobre este mensaje se realiza un proceso de encriptado WEP utilizando la clave secreta compartida, y el resultado se compara en el AP con el esperado para obtener la conclusión de este proceso.

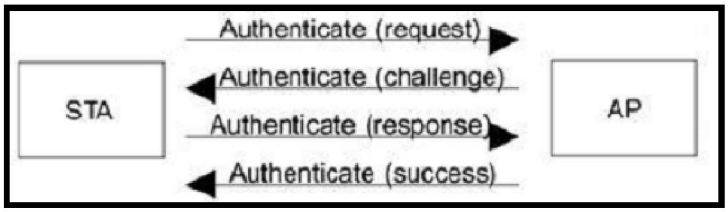


Figura 2: Modelo de autenticación WEP

De esta forma, el cliente está demostrando su conocimiento de una clave secreta sin necesidad de que ésta viaje por el medio, por lo que no peligraría su confidencialidad durante el proceso, aunque hubiera algún dispositivo no deseado realizando alguna escucha o sniffing.

Un inconveniente de este proceso es que en ningún momento el AP se identifica, por lo que la autenticación no es mutua, que sería lo deseable. Otro inconveniente es que aunque la clave no sea

intercambiada en plano, un sniffer sí que puede observar el intercambio entre texto plano y texto cifrado por lo que a través de varias observaciones podría llegar a descubrir la clave.

3.3. Formato de Trama:

Vamos a realizar una breve descripción sobre el esquema de la trama:

- Algorithm Number indica el tipo de autenticación que estamos llevando a cabo (0 = Autenticación Abierta, 1 = Autenticación WEP)
- Transaction Sequence indica cual de los diferentes mensajes de autentificación es, de los diferentes que componen el diálogo.
- Status Code. Su significado cobra importancia en el último mensaje, en el que indica si el proceso ha sido fallido o un éxito.
- Challenge Text. Es el campo usado en Autenticación WEP para trasladar el texto, primero en plano (AP -> STA) y finalmente cifrado (STA -> AP).

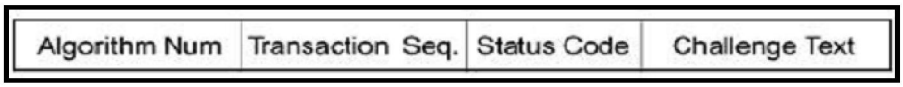


Figura 3: Formato de trama WEP

Se volverá tratar sobre WEP más adelante, cuando se analicen los mecanismos de cifrado. En ese momento se detallarán sus debilidades.

4. 802.1x

Su objetivo es un concepto muy simple. Se trata de conseguir mantener el Control de Acceso en el punto donde el usuario se une a la red, el puerto. En la definición del protocolo se divide la red completa en las tres entidades:

- El servidor de autenticación: Es aquella entidad a la que el autenticador consulta si debe o no, y en qué condiciones, permitir el acceso a los recursos de la red. El servidor de autentificación es el que aporta la inteligencia al proceso ya que es el que realiza la negociación.
- El autenticador: Es aquella entidad que controla el acceso a los recursos de la red. En una red WLAN el punto de acceso es el que proporciona o impide el acceso a los recursos de la red a un determinado cliente. El papel del autenticador se limita a trasladar mensajes desde el suplicante al servidor de autentificación, y finalmente a obedecer el criterio de este último para permitir acceder a la red o no al suplicante.
- El solicitante: Es aquella entidad que pretende tener acceso a los recursos de la red. El software cliente.

Este protocolo añade un nuevo elemento al modelo mencionado hasta ahora. Al punto donde el usuario se conecta a la red se le llama Puerto. PAE significa Port Access Entity y es el nombre completo que un puerto recibe en el texto del estándar. Una red como es lógico tendrá múltiples puertos, cada usuario estará asociado a un puerto en cada momento, y cada puerto tendrá asociado un autenticador que controle su estado. Cada puerto estará desconectado de la red por defecto. Cuando decimos “desconectado”, nos referimos a una desconexión lógica, gracias a la cual la información no atravesaría el puerto hacia la red.
En cada puerto existe un autenticador con el que sí se puede comunicar cualquier solicitante que lo desee. A él se le envía la información relativa a la solicitud de conexión, y él la reenvía hacia el órgano centralizado, el servidor de autenticación, que sí es capaz de discernir entre un

usuario autorizado y uno que no lo está. Esto hace que la decisión sobre permitir o no el acceso se tome en un órgano centralizado, mucho más fácil de controlar para el administrador del sistema.

A continuación podemos mostrar un gráfico extraído directamente del estándar en el que se muestran todas estas relaciones entre las entidades.

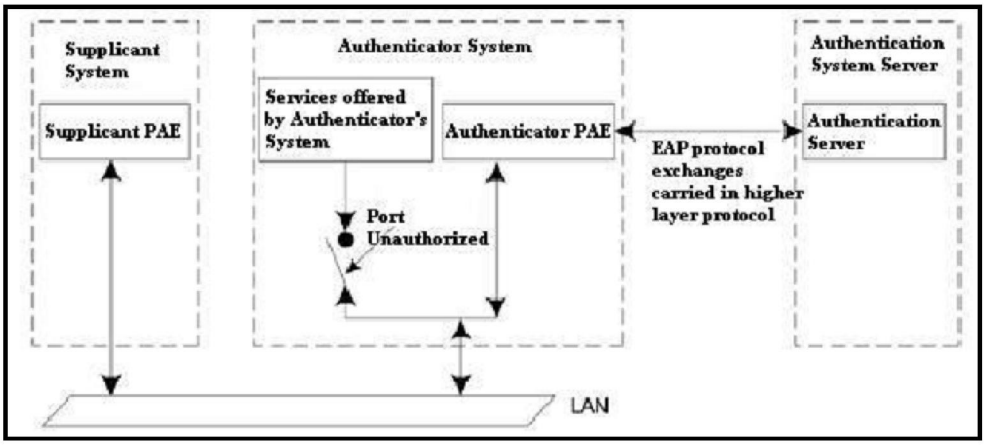


Figura 4: Relaciones entre entidades del estándar 802.1x

Hay que resaltar que 802.1X está relacionado con la parte de control de acceso, sin entrar en cómo se determina si un usuario debe tener acceso o no. Por tanto, su área de influencia en la figura se correspondería con la parte del Sistema Autenticador.

Este protocolo funciona de manera conjunta con otros, que suelen ser EAP y RADIUS. La relación entre ellos se describe brevemente a continuación:

- EAP define una serie de mensajes que soportan el protocolo de alto nivel que verdaderamente lleva a cabo la autenticación. En un sistema como éste, los mensajes que el solicitante envía al autenticador deberán ser reenviados hacia el servidor de autenticación, que será otro sistema remoto.
- RADIUS se usa en la interfaz Autenticador – Servidor de Autenticación. Como el sistema de autenticación está en una localización remota, estos mensajes EAP requieren de un protocolo que les permita alcanzar su destino. El protocolo RADIUS permite que estos mensajes lleguen a su destino.

5. WPA/WPA2

WPA es la abreviatura de *Wifi Protect Access*, y consiste en un mecanismo de control de acceso a una red inalámbrica. También se le conoce con el nombre de TSN (Transition Security Network).

Las múltiples vulnerabilidades de WEP empujaron a Wi-Fi Alliance a desarrollar la alternativa, Wi-Fi Protected Access (WPA), para cerrar la brecha hasta que el nuevo estándar 802.11i pueda ofrecer mecanismos de seguridad más robustos. IEEE tenía casi terminados los trabajos del nuevo estándar para reemplazar a WEP, que se publicó en la norma IEEE 802.11i (nombre comercial de WPA2) a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del nuevo estándar que ya estaban suficientemente maduras y publicar así WPA. WPA es un compromiso entre WEP y el más reciente WPA2.

5.1. Características WPA:

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación. WPA incluye las siguientes tecnologías:

- **IEEE 802.1X**. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos presentado en el apartado anterior.

- **EAP**. EAP, definido en la RFC 2284, es el *protocolo de autentificación extensible* para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (*Point-to-Point Protocol*), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Trataremos más en detalles este protocolo en un apartado siguiente.

- **TKIP** (*Temporal Key Integrity Protocol*). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave dinámica para cada trama, mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización.

- **MIC** (*Message Integrity Code*) o Michael. Código que verifica la integridad de los datos de las tramas.

5.2. Mejoras de WPA con respecto a WEP:

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo de cifrado utilizado por WPA sigue siendo RC4 como en WEP, aunque más tarde se ha demostrado inseguro. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (*replay*). Para la integridad de los mensajes (ICV: *Integrity Check Value*), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP. Para la autentificación, los desarrolladores modificaron los métodos de autenticación y cifrado para proporcionar más seguridad: los clientes utilizan claves previamente compartidas o (en las grandes redes LAN inalámbricas) un servidor RADIUS para asociarse con el punto de acceso.

Después de la autenticación, el cliente y el punto de acceso negocian una clave individual de 128 bits para evitar que otras estaciones en la WLAN rastreen el tráfico de datos. La renegociación periódica de la clave entre el cliente y el punto de acceso añade más seguridad a la WPA estándar, eliminando la posibilidad de que un intruso ponga en marcha un ataque de fuerza. En la figura siguiente podemos ver el formado de una trama WPA.

IV	Datos	MIC	ICV

Figura 5 : Formado de Trama WPA

5.3. Métodos de funcionamiento de WPA:

WPA puede funcionar en dos modos:

- **Enterprise Mode: (modo corporativo) con servidor AAA, RADIUS normalmente**. Éste es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

- **Home Mode: (modo personal) con clave inicial compartida (PSK).** Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

5.4. Debilidades de WPA:

Si se emplea WPA como mecanismo de seguridad los puntos de acceso únicamente aceptan autenticación y cifrado WPA, no permitiendo conectarse a usuarios sin WPA. Por otro lado, un usuario configurado para utilizar WPA no se conecta a puntos de acceso sin WPA. El problema que aún mantiene WPA es que se basa en el algoritmo de cifrado RC4, y como se ha comentado anteriormente ya se le han encontrado vulnerabilidades.

5.5. Características WPA2 y mejoras:

WPA2, que fue presentado en 2004, hace que las WLAN sean aún más seguras. Los desarrolladores abandonaron las características de seguridad heredadas de la infraestructura inalámbrica mediante WPA, por ejemplo, la sustitución del algoritmo inseguro RC4 por el estándar superior AES (Advanced Encryption Standard). Además de esta mejor base, la nueva norma incorpora los métodos de autenticación y el cifrado WPA. Gracias a estas mejoras, los atacantes ya no se benefician del rastreo de una WLAN durante horas o días y ejecutan ataques de fuerza bruta contra los resultados.

Por otro lado, al igual que WPA, WPA2 permite dos modos de llevar a cabo la autenticación según si el ámbito de aplicación es empresarial (IEEE 802.11i/EAP) o personal (PSK). Aunque esta variante ofrece todas las características básicas de seguridad más populares, no es compatible con el beneficio adicional de autenticación a través de un servidor RADIUS. La versión Enterprise WPA2 abarca todo el estándar 802.11i, y por tanto permite la autenticación RADIUS.

		WPA	WPA2
Modo Corporativo	Autenticación	802.1X / EAP	802.1X / EAP
	Cifrado	TKIP/MIC	AES-CCMP
Modo Personal	Autenticación	PSK	PSK
	Cifrado	TKIP/MIC	AES-CCMP

Figura 6: Métodos de autenticación y cifrado en WPA/WPA2

5.6. Debilidades de WPA2:

A partir de este escrito, las redes inalámbricas basadas en WPA2 son consideradas como las más seguras. Teóricamente, la difusión y multidifusión de claves representan otra vulnerabilidad. Todos los nodos de la red necesitan conocerlas, y un atacante que descubra una de las claves puede, al menos, espiar el intercambio de claves entre el punto de acceso y la estación de trabajo.

Gracias al diseño de seguridad del estándar WPA2, las modernas redes inalámbricas disponen ahora de una seguridad bastante eficaz. El mayor factor de incertidumbre es con el usuario. Hoy en día, cuando un intruso obtiene acceso a una moderna infraestructura WLAN y consigue acceder a la red y causar daños, la causa suele ser un punto de acceso configurado de forma negligente. Por tanto, hay que tomar algún tiempo para considerar cuidadosamente cada una de las opciones del router de la red. Si deseamos reducir aún más el riesgo residual, podemos añadir a la WLAN protección basada en software. Si utilizamos un túnel, como una VPN con IPSec, podemos incluso aumentar la barrera para los atacantes experimentados. Como suele ocurrir, el sistema operativo libre Linux, con sus muchos componentes de seguridad incorporados, es una elección perfecta para la eliminación del riesgo residual.

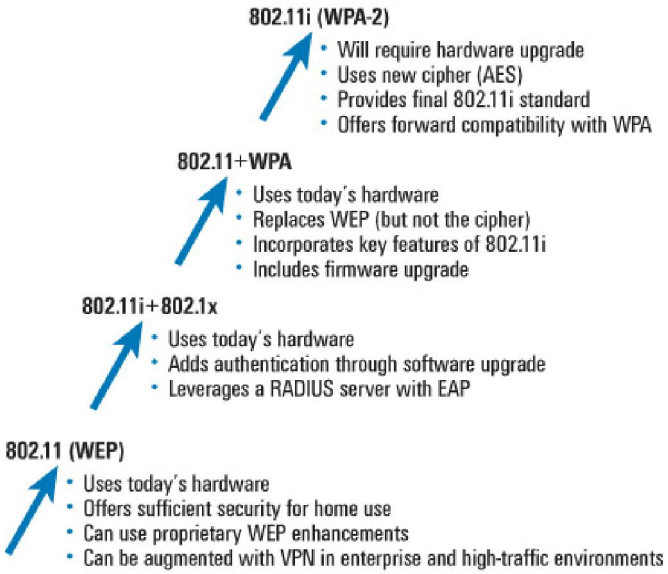


Figura 7: Evolución de los mecanismos de seguridad Wi-Fi

A continuación, detallaremos los mecanismos de autenticación en función de los diferentes modos de funcionamiento de WPA: EAP (empresarial) y PSK (personal).

6. WPA empresarial: el protocolo de autenticación EAP

Hemos visto que 802.1X utiliza un protocolo de autenticación llamado EAP (Extensible Authentication Protocol) que admite distintos métodos de autenticación como certificados, tarjetas inteligentes, Kerberos, ldap, etc. En realidad EAP actúa como intermediario entre un solicitante y un motor de validación permitiendo la comunicación entre ambos. Dentro del 802.1X se define la encapsulación de EAP en tramas Ethernet sobre una LAN, llamado EAPOL (EAP over LAN).

Antes de entrar en detalles sobre el protocolo de autenticación EAP, es necesario introducir algunas nociones importantes como la de certificado digital y la autoridad de certificación, privacidad TLS, nociones que intervienen en el protocolo EAP.

6.1. Certificado digital:

Un **certificado digital** es un documento electrónico mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública. Si bien existen variados formatos para certificados digitales, los más comúnmente empleados se rigen por el estándar UIT-T X.509. El certificado contiene usualmente el nombre de la entidad certificada, número de serie, fecha de expiración, una copia de la clave pública del titular del

certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación. Cualquier individuo o institución puede generar un certificado digital, pero si este emisor no es reconocido por quienes interactúen con el propietario del certificado, el valor del mismo es prácticamente nulo. Por ello los emisores deben acreditarse.

6.2. Autoridad de certificación:

Una autoridad de certificación (CA) es la entidad encargada de dar fe de que el usuario cuyo identificador viaja en el certificado, realmente posee la clave privada que hace pareja con la clave pública que se indica en el certificado. En cierto modo podríamos compararlas con el Gobierno Español cuando éste último certifica que efectivamente un D.N.I. o un pasaporte corresponden a una determinada persona. A la hora de expedir los certificados, las CA se encuentran con el problema de cómo verificar la identidad del solicitante del certificado. Debido a que la credibilidad que los solicitantes exigen para sus certificados varía en función de la aplicación para la que se necesiten las claves, las CA han optado por crear distintos tipos de certificados dependiendo del método que se haya utilizado para autenticar al usuario.

- **B1**. La CA relaciona el nombre que introduce el usuario en su cuestionario con una cuenta de correo válida. Permite la firma y encriptación de correo o la autenticación del usuario ante un servidor. No tienen carácter comercial pues no existe comprobación de la identidad del usuario.
- **B2**. Utiliza como base una verificación documental, por lo que es necesaria la comprobación de la identidad del usuario mediante un documento de identidad válido. Deberá enviarse una fotocopia del documento y abonarse la correspondiente tarifa de la operación. Se conoce como Certificado Personal.
- **B3**. La comprobación del usuario será presencial y documental. El individuo deberá presentarse ante el registrador de la CA con un documento de identidad válido y abonar la correspondiente tarifa. Se le da el nombre de Certificado Personal Presencial.

No hay ni que decir que el certificado que más seguridad aporta es el B3 seguido del B2 y terminando por el B1. Las diferencias entre los tipos de certificados sólo se aprecian en el aspecto judicial y en el de trámites para conseguirlo, ya que desde el punto de vista informático son iguales.

6.3. Privacidad TLS:

El protocolo TLS o *Transport Layer Security* tiene su origen en los comienzos de Internet. En esta época Netscape era el navegador dominante en el mercado, por lo que la mayoría de los avances en aquella época vinieron de él. Apareció la necesidad de realizar transferencias de información de forma segura, así que Netscape implementó una solución a la que se le llamó SSL o *Secure Socket Layer*. SSL se basaba en el uso de Certificados Digitales, y aunque permitía el uso de certificados en cliente y servidor, su uso más común era el de utilizar Usuario/Contraseña en el lado del cliente. Por otra parte, SSL ofrecía la posibilidad de identificar y validar entidades de Internet de forma inmediata, a la par que permitía comunicarse con ellos de forma segura, con control de integridad y privacidad garantizadas. Esto permitía trasladar a otras entidades información muy sensible como podría ser por ejemplo un número de cuenta.

SSL se convirtió rápidamente en el estándar de facto para transacciones Web seguras. Aunque las especificaciones de este protocolo eran conocidas, continuaba siendo una solución propietaria. Esto no es algo que agrade especialmente a los fabricantes por lo que se promovió un protocolo estandarizado, a través del IETF. El resultado de este trabajo vio la luz en 1999 con la aparición de TLS. TLS proporciona más servicios que los que nosotros necesitamos de un Protocolo de

Autenticación de Alto Nivel. TLS proporciona servicios como Autenticación, Cifrado y Compresión de Datos. Nuestro principal interés en TLS será su mecanismo de autenticación, que se adapta muy bien al modelo basado en 802.1X y EAP que vamos a describir a continuación.

TLS se puede dividir en dos capas: TLS Record Protocol y TLS Handshake Protocol. Como primera aproximación se puede indicar que la capa TLS Record Protocol, que es la más baja de las dos, se encarga de trasladar los datos entre los dos extremos de la comunicación utilizando un enlace seguro o túnel cuyas características y parámetros se han negociado a través del TLS Record Protocol. A continuación podemos ver un esquema en el que se representa la situación. Se observa que la conexión segura se apoya sobre una red IP, por lo que podemos decir que este protocolo (TLS) opera en el Nivel de Transporte.

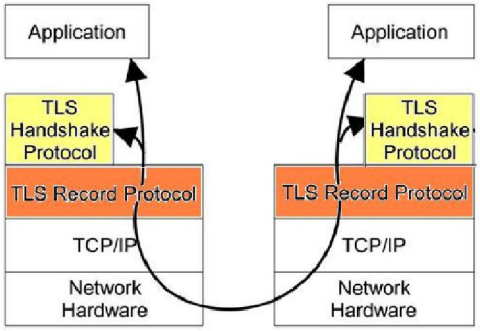


Figura 8: Modelo OSI para TLS

Un último aspecto sobre TLS es que utiliza Certificados Digitales para conseguir la Autenticación y además tiene la flexibilidad suficiente para poder soportar diferentes tipos de certificados.

6.4. Características de WPA-EAP:

En el protocolo EAP, como se muestra en la figura 4, intervienen tres tipos de elementos: el cliente que solicita acceso, el autenticador que sirve de enlace entre el cliente y el servidor de autenticación (que en el caso de redes WIFI es el punto de acceso) y el servidor de autenticación que es el que realiza la comprobación de credenciales que puede ser un servidor RADIUS.

El protocolo funciona de la siguiente forma: el cliente solicita conexión al punto de acceso que filtra todo el tráfico menos el correspondiente al protocolo EAPOL. El punto de acceso se percata de que hay un nuevo cliente pidiendo acceso y le envía una solicitud de identificación. Éste le responde con el identificador, que es directamente reenviado al servidor RADIUS junto con una solicitud de acceso.

El servidor lo utiliza para comenzar la fase de autenticación con el cliente (el punto de acceso hace de mero intermediario), enviándole una solicitud de credenciales, que pueden ser un certificado digital, una pareja nombre/usuario u otros datos.

El cliente le responde con las correspondientes credenciales (dependiendo del tipo de autenticación elegido) y finalmente, el servidor RADIUS las comprueba devolviendo un "accept" o "error" dependiendo de si todo es correcto autorizando el acceso o no, y el punto de acceso en consecuencia abrirá o no la conexión al cliente.

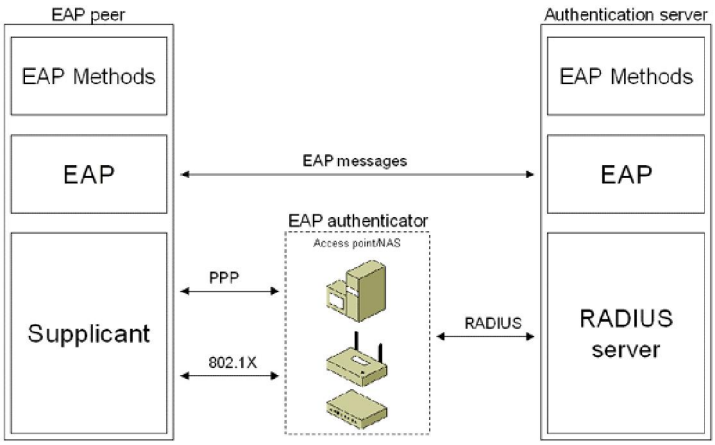


Figura 9: Protocolo de autenticación EAP

Un mensaje EAP, sea cual sea, tendrá la siguiente estructura compuesta por cuatro campos, aunque en ocasiones el de Datos puede no estar presente.

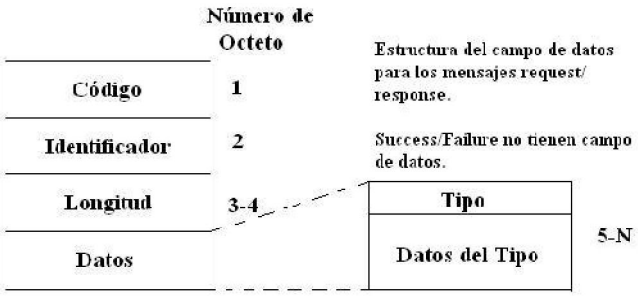


Figura 10: Formato de mensaje EAP

- ***Código***. Indica el tipo de mensaje EAP. En el apartado siguiente los estudiaremos y estudiaremos su función.
- ***Identificador***. Este octeto se utiliza para emparejar peticiones con respuestas, de manera que en todo momento la información de una respuesta se asocie a la petición adecuada. Se entiende que diferencia entre peticiones y respuestas asociadas al mismo puerto lógico. El identificador se mantiene en caso de retransmisión de peticiones fallidas.
- ***Longitud***. Longitud del campo de datos, que por otra parte es el único cuyo tamaño no se conoce a priori. En caso de no haber campo de datos su valor será cero, como es lógico.
- ***Datos***. Su significado dependerá del tipo de mensaje. Sólo aparece en los mensajes request o response.

En la recomendación de EAP se definen cuatro tipos de mensajes.

- ***Request***. Se utiliza para enviar mensajes del autenticador al suplicante.
- ***Response***. Se utiliza para enviar mensajes del suplicante al autenticador.
- ***Success***. Enviado por el autenticador para indicar que el acceso está permitido.
- ***Failure***. Enviado por el autenticador para indicar que el acceso está denegado.

En EAP los mensajes son trasmitidos en claro, además de no requerirse ningún tipo de autenticación por parte del servidor ni del cliente, lo que supone una clara vulnerabilidad a nivel de seguridad, más aún en entornos wireless (inalámbricos). Como mejoras al protocolo, se han incluido variantes que crean canales seguros entre el cliente y el servidor de autenticación algunos siendo estándares y otras soluciones propietarias de empresas: EAP-TLS, EAP-PEAP, EAP-TTLS, etc.

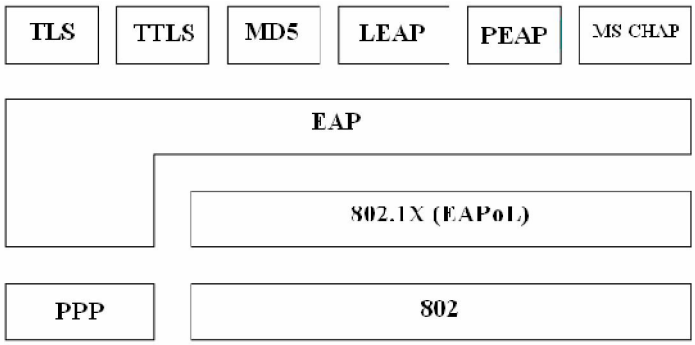


Figura 11: Esquema de ubicación del protocolo EAP

A continuación presentaremos los distintos tipos de EAP, tipos que consisten en las diversas combinaciones que pueden establecerse entre EAP y otro protocolo de alto nivel o Upper-Layer Authentication Protocol.

a) EAP-TLS :

EAP-TLS (*Extensible Authentication Protocol with Transport Layer Security, RFC 2716*) se trata de una variante de EAP en la cual se realiza una negociación SSL con autenticación basada en certificados X.509 para autenticar tanto usuario como servidor. En el caso de TLS, las credenciales corresponden al certificado de cliente, mientras que en otros tipos de EAP la conexión segura se realiza a partir exclusivamente del certificado del servidor. El certificado del usuario se puede almacenar en algún dispositivo hardware como Smart Card o USB para aumentar aún más la seguridad de la red, aunque también hace más difícil la implementación y la gestión de ésta. Además, hay que tener en cuenta que algunos usuarios necesitan extensiones específicas para certificados digitales.

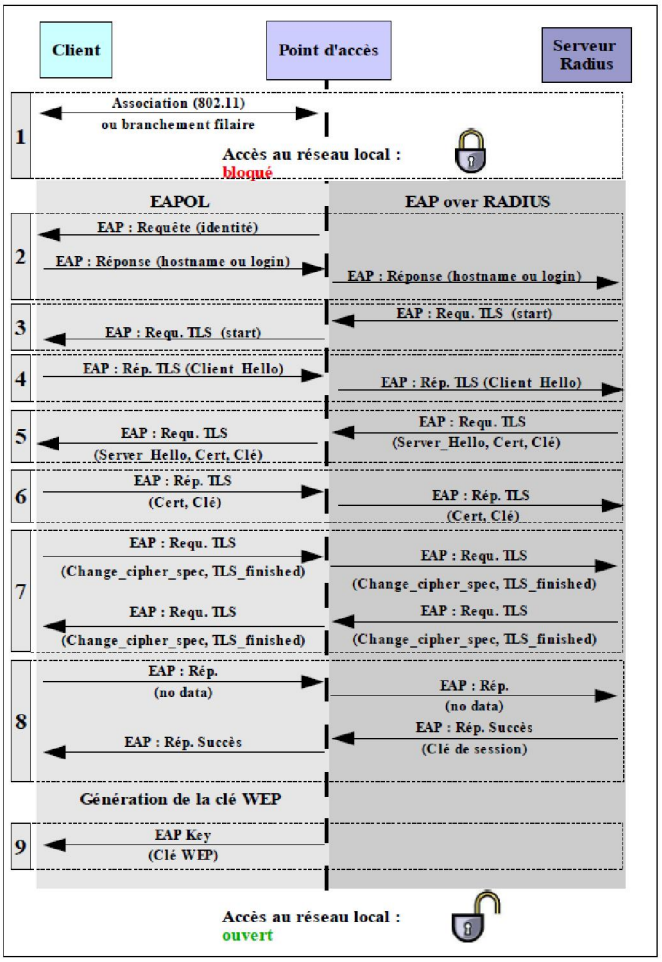


Figura 12: Datagrama de cambios TLS

Las explicaciones siguientes se refieren al número de los pasos en la Figura 6.

1) - El cliente se asocia al punto de acceso físico.

2) - El punto de acceso envía una solicitud de autenticación al cliente. El cliente responde con su ID (nombre de host o login), el mensaje se transmite por el punto de acceso al servidor RADIUS.

3) - El servidor RADIUS inicia el proceso de autenticación TLS con el mensaje *TLS Start*.

4) - El cliente responde con un mensaje *client_hello*, que contiene:

- las especificaciones de cifrado, campos vacíos hasta que se negocian entre el cliente y el servidor;
- la versión TLS del cliente;
- un número aleatorio (reto o desafío);
- un identificador de sesión;
- los tipos de algoritmos de encriptación soportados por el cliente.

5) - El servidor envía una petición que contenga un mensaje *server_hello* seguida por:

- su certificado (x509) y su clave pública;
- la solicitud del certificado de cliente;
- un número aleatorio (reto o desafío);
- un identificador de sesión

El servidor elige un sistema de cifrado entre los que han sido propuestos por el cliente.

6) - El cliente comprueba el certificado del servidor y responde con su propio certificado y la clave pública.

7) - El servidor y el cliente, cada uno a su vez, definen una clave de cifrado principal que se utiliza para la sesión. Esta clave se calcula con los valores aleatorios que han intercambiado el cliente y el servidor. Los mensajes *change_cipher_spec* indican el cambio de clave. El mensaje *TLS_finished* finaliza la fase de autenticación TLS (*TLS handshake*), en el caso de EAP-TLS la clave de sesión no se utiliza para cifrar los siguientes intercambios.

8) - Si el cliente ha verificado la identidad del servidor (con el certificado y la clave pública), devuelve una respuesta EAP sin datos. El servidor devuelve una respuesta *EAP success*.

9) - La clave de sesión generada en (8) se vuelve a utilizar en el punto de acceso para crear una clave WEP que se envía al cliente si se trata de una estación WiFi. La clave de sesión es válida hasta que el cliente se desconecta o su autentificación caduca, en cuyo caso se debe autenticar de nuevo.

El túnel de TLS establecido durante la creación de la clave de sesión no se ha utilizado. Solamente se usa el TLS Handshake, que permite la autenticación mutua de ambas partes. EAP-TLS es un método de autentificación de gran rendimiento. Tan sólo los problemas relacionados con la administración de claves pueden desalentar el uso de este método.

Hablar de ataques *Man In The Middle* en redes con seguridad EAP-TLS no tiene mucho sentido, ya que el usuario comprueba la autenticidad del servidor comparándolo con una lista de servidores autorizados, siendo realmente difícil suplantar la identidad del servidor autorizado.

EAP-TLS sigue manteniendo el problema de exposición de la identidad, puesto que los certificados son enviados por el medio (aire) sin cifrar, por lo que un atacante podría ver la identidad del cliente que está tratando de conectarse. Además, el mensaje de aceptación o denegación de la conexión es enviado sin cifrar, por lo que un atacante podría enviarlo suplantando la identidad del servidor de autenticación.

El uso de certificados tiene sus ventajas y desventajas. A menudo son considerados más seguros que las contraseñas, sin embargo, las operaciones de gestión que generan pueden ser tediosas (creación, supresión, listas de revocación, etc.) y la existencia de una infraestructura de gestión de claves (PKI) es necesaria. La distribución de los certificados a los clientes es una limitación que no debe pasarse por alto.

b) EAP-TTLS :

En la línea de EAP-TLS se encuentran otros métodos que resuelven los problemas de éste. EAP-TTLS (*Extensible Authentication Protocol with Tunneled Transport Layer Security),* desarrollado por Funk Software, está orientado a trabajar con servidores RADIUS. Puede emplear métodos de autenticación EAP adicionales o métodos como PAP y CHAP. Está integrado con una gran variedad de formatos de almacenamiento de contraseñas y sistemas de autenticación basados en contraseñas, así como con múltiples bases de datos de seguridad. Además, en el mercado existen un gran número de usuarios TTLS disponibles.

Hay dos etapas de autenticación:

- Primera fase: identificación del servidor por el cliente mediante un certificado (validado por una autoridad de certificación).
- Segunda fase: identificación del cliente por el servidor mediante usuario y contraseña.

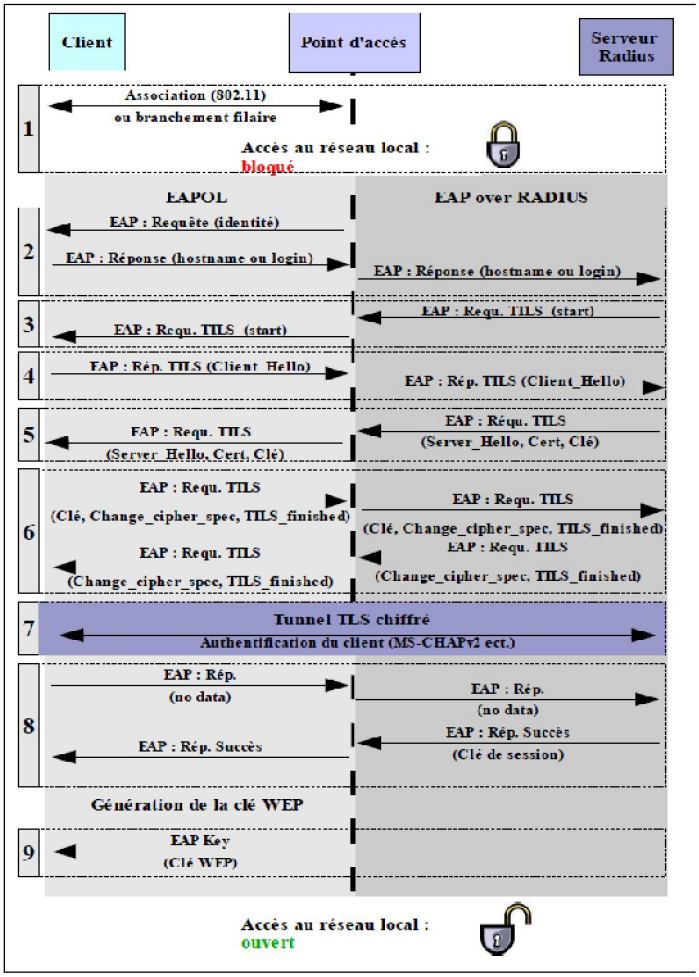


Figura 13: Datagrama de cambios EAP-TTLS o PEAP

Las explicaciones siguientes se refieren al número de los pasos de la Figura 7:

1 a 5) - Los intercambios son similares a EAP-TLS. El cliente autentica el servidor a través de un certificado (Paso 5).

6) - Este paso difiere ligeramente de EAP-TLS porque el cliente no necesita presentar un certificado, la clave utilizada para cifrar el período de sesiones se puede crear directamente. Al final de esta etapa, el *TLS handshake* está completo, los intercambios siguientes serán cifrados por la clave de sesión.

7) - De hecho, el establecimiento de un túnel TLS permite cifrar los intercambios, proporcionando así la identificación del cliente (nombre de usuario y contraseña) al servidor utilizando, por ejemplo MS-CHAPv2.

8 y 9) - Igual que en los métodos EAP-TLS

EAP-TTLS ofrece una fuerte autenticación mutua. EAP-TTLS sólo requiere certificados en el servidor, lo que subsana una desventaja importante respecto a EAP-TLS, cuya gestión es mucho más tediosa y pesada. Con EAP-TTLS se elimina la necesidad de configurar certificados para cada usuario de la red inalámbrica. En un sistema EAP-TTLS se autentica al usuario en el sistema con las credenciales basadas en nombre de usuario y contraseña, y se cifran las credenciales de usuario para garantizar la protección de la comunicación inalámbrica.

c) *EAP-MD5 :*

Este método de autenticación fue el primero en usarse con EAP. EAP-MD5 (EAP Message Digest 5) se basa en el uso del algoritmo de cifrado MD5 (que lo veremos más adelante en el capítulo sobre el cifrado). Su funcionamiento se basa en la generación de claves mediante el algoritmo MD5, que deben ser fijas y configuradas manualmente en el terminal de usuario y no permite que éstas sean asignadas de forma automática, por lo que no es compatible con WPA ni con IEEE 802.11i. Este método de autenticación envía el nombre de usuario sin ningún tipo de protección, lo que hace que sea susceptible de ataques de diccionario o por fuerza bruta.

Éste es el único método EAP que no utiliza ningún mecanismo de seguridad para autenticar el servidor y la estrategia para autenticar al usuario es por medio de contraseñas. Con esta configuración se sigue manteniendo el riesgo de ataques como ataques de diccionario, *Man In The Middle*, secuestro de sesión, y exposición de la identidad, ya que los usuarios no tienen una

certificación seria del servidor con el que se comunican. Debido a su antigüedad fue concebido pensando en que el riesgo de escucha o snooping de las comunicaciones era bajo, como sucedía en las redes cableadas. Esto no es aceptable para redes WLAN por lo que para romper este mecanismo bastaría con interceptar el mensaje con el resumen.

Otro inconveniente que se evidencia en este mecanismo tan simple es que la autenticación no es mutua. La única autenticación que se produce es la del Cliente frente al Sistema, por lo que eso haría posible atacar la red suplantando la identidad del AP y obteniendo los datos de algún cliente legítimo. El último problema es que tampoco resuelve el problema de WEP. En este protocolo no se establece ningún mecanismo que automatice el cambio de las Claves WEP.

EAP-MD5 proporciona el nivel más bajo de seguridad aplicable por lo que no es recomendable como protocolo de autenticación de redes WLAN. Puede ser empleado para llevar a cabo la autenticación en redes WLAN siempre y cuando se emplee adicionalmente un método de tunelado EAP, como EAP-PEAP o EAP-TTLS, para aumentar su eficiencia.

d) EAP-LEAP:

EAP-LEAP (Lightweight EAP) protocolo propietario de Cisco es similar a EAP-MD5. En este caso se utilizan también las contraseñas como método de autenticación del servidor. Cuando se emplea LEAP las credenciales de usuario (nombre de usuario y contraseña) se envían sin cifrar. LEAP no soporta la utilización de One Time Password (OTP) y requiere de infraestructura inalámbrica CISCO para poder ser utilizado. Por lo tanto, esta autenticación, aunque ligera, previene de ataques *Man In The Middle* y de secuestro de la sesión, pero sigue manteniendo el riesgo de exposición de la identidad y de ataques de diccionario.

LEAP no ha sido estandarizado por lo que sus detalles de implementación no eran conocidos. Lo que sucede es que dado lo extendido de su uso, el protocolo fue sometido a un proceso de Ingeniería Inversa que desveló sus secretos y permitió al resto de fabricantes crear dispositivos compatibles con este protocolo. Antes de describir el proceso que sigue es preciso comentar que este mecanismo presenta algunos inconvenientes que han sido solventados en posteriores protocolos.

- El sistema de autenticación mutua se basa en el uso del protocolo MS-CHAP. Este protocolo consiste en un diálogo extremo a extremo entre el Cliente y el Servidor. Esto entraña un riesgo ya que si el Autenticador que se halla entre ambos fuera víctima de un ataque, estaríamos ante una situación *Man-In-The-Middle*. La manera de solucionar esto, que por otra parte no está recogida en este protocolo, sería tener una Autenticación Fuerte entre el AP y el Servidor RADIUS.
- El segundo inconveniente es el típico de cualquier sistema de Usuario/Contraseña en el que el ser humano es el encargado de escoger las contraseñas. Existe un riesgo cuando se utilicen contra el sistema Ataques de Diccionario. La solución a este problema son los certificados.
- El último inconveniente es que LEAP es un protocolo propietario de Cisco. Corremos el riesgo de que otros fabricantes de su nivel se decanten por desarrollar sus propios sistemas propietarios, apareciendo una vez más el fantasma de la incompatibilidad de equipos.

e) EAP-FAST:

Después de LEAP Cisco ha trabajado en la implementación de un nuevo protocolo que lo sustituye llamado EAP-FAST (Flexible Authentication via Secure Tunneling), que no requiere certificados digitales y no es vulnerable a los ataques de diccionario según la opción de la empresa. EAP-FAST, al igual que EAP-TTLS y PEAP, utiliza túneles para proteger el tráfico. La provisión de EAP-FAST es negociada solamente por el cliente como primer intercambio de comunicación, cuando se solicita

EAP-FAST en el servidor. Si el cliente no tiene una Credencial de acceso protegido (PAC) secreta y precompartida, puede iniciar un intercambio de provisión de EAP-FAST para obtener una del servidor de forma dinámica.

f) EAP-PEAP:

EAP-PEAP (Protected EAP) es un protocolo que ha sido desarrollado de forma conjunta entre Microsoft, Cisco y RSA Security como alternativa a EAP-TTLS. Su objetivo original era conseguir un sistema basado en Contraseña pero que a la par fuera más seguro respecto a los Ataques de Diccionario.

Para explicar este protocolo vamos a partir de aquellos defectos que tenía EAP. El mensaje EAP-Identity no estaba protegido, por lo que si en la primera fase del protocolo EAP había alguien observando, la identidad del cliente podría ser descubierta. De la misma forma el EAP-Success y EAP-Reject estaban desprotegidos frente a snooping.

La solución que propone PEAP es proteger el proceso de autenticación completo, incluyendo los mensajes EAP iniciales y finales mediante un túnel TLS. De esa forma PEAP pretende establecer el túnel que proporcione la privacidad del proceso, dejando luego libre toda la flexibilidad de EAP para implementar cualquier método de autenticación, eso sí, implementado desde el primer al último mensaje sobre un canal seguro.

¿Pero cómo establecer un canal seguro si precisamente uno de los propósitos de EAP era ese? La respuesta es simple. Privacidad y Autenticación son independientes, y es posible conseguir privacidad sin tener autenticación. Ese es precisamente nuestro objetivo, utilizar PEAP para proporcionar privacidad, dejando el peso de la autenticación a EAP.

El proceso se puede dividir en dos fases. En la primera de ellos se utiliza EAP del modo convencional para establecer una conexión segura TLS. En la segunda se utiliza el túnel creado para llevar a cabo una nueva negociación EAP, complementada con el protocolo de alto nivel que se desee, en la que se realice una autenticación completa. Hay que resaltar que en la primera fase sí que se produce una autenticación real del servidor, al que se le solicita un Certificado para probar su identidad. Veamos a continuación con algo más de detalle las dos fases.

EAP-TTLS y EAP PEAP son métodos muy similares y el uso de un túnel cifrado TLS les da un buen nivel de Privacidad. La principal diferencia entre EAP-PEAP y EAP-TTLS está en la forma de encapsular los intercambios durante la segunda fase. Para EAP-PEAP, los datos intercambiados entre el cliente y el servidor en el túnel de TLS se encapsulan en paquetes EAP.

g) EAP-MS-CHAP

MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), también conocido como MS-CHAP versión 1 es un protocolo de autenticación de contraseñas de cifrado no reversible. Utiliza una versión de Microsoft del protocolo de desafío y respuesta de RSA Message Digest 4. Éste sólo funciona en sistemas Microsoft y activa la codificación de datos. La selección de este método de autenticación hace que se codifiquen todos los datos.

El proceso de desafío mutuo funciona de la manera siguiente:

- El autenticador (el servidor de acceso remoto) envía al cliente de acceso remoto un desafío formado por un identificador de sesión y una cadena de desafío arbitraria.
- El cliente de acceso remoto envía una respuesta que contiene el nombre de usuario y un cifrado no reversible de la cadena de desafío, el identificador de sesión y la contraseña.

- El autenticador comprueba la respuesta y, si es válida, se autentican las credenciales del usuario.

EAP-MS-CHAP-V2 (Microsoft Challenge-Handshake Authentication Protocol version 2) introduce una función adicional que no está disponible con la autenticación MSCHAPV1 o CHAP estándar, la función de cambio de contraseña. Esta función permite que el cliente cambie la contraseña de su cuenta si el servidor RADIUS informa de que ha vencido la contraseña. La autenticación mutua se proporciona mediante la inclusión de un paquete de autenticador que se devuelve al cliente después de una autenticación de servidor con éxito. EAP-MS-CHAP-V2 es típicamente utilizado en el interior de un túnel TLS creado por TTLS o PEAP.

De forma predeterminada, el protocolo de contraseña EAP-MS-CHAP está disponible para su uso por el Native y los métodos de autenticación de Unix.

h) EAP-POTP

EAP-POTP (Protected One-Time Password), que se describe en el RFC 4793, es un método EAP desarrollado por RSA Laboratories que utiliza fichas one-time password (OTP), como un dispositivo de hardware portátil o el hardware o el módulo de software que se ejecuta en un ordenador personal, para generar claves de autenticación. EAP-POTP se puede utilizar para proporcionar autenticación unilateral o mutua y claves en los protocolos que utilizan EAP.

El método EAP-POTP proporciona dos factores de autenticación de usuario, lo que significa que un usuario necesita tanto el acceso físico y el conocimiento de un número de identificación personal (PIN) para realizar la autenticación.

i) EAP-GTC

EAP-GTC (Generic Token Card), que se describe en el RFC 2284, permite el intercambio de texto sin cifrar las credenciales de autenticación en la red. Sin embargo, como las contraseñas one-time generados por las tarjetas de token no son vulnerables a ataques de repetición, EAP-GTC se puede utilizar por sí mismo. EAP-GTC se suele utilizar dentro de un túnel TLS creado por TTLS o PEAP para proporcionar autenticación de servidor en entornos inalámbricos.

EAP-GTC es típicamente empleado por las empresas que utilizan dos factores de autenticación para evitar las vulnerabilidades de seguridad basadas en contraseñas, tales como la exposición de las contraseñas a terceros.

j) EAP-SIM

EAP-SIM (EAP for GSM Subscriber Identity Module) es un método de autenticación que pueda operar en redes inalámbricas. EAP-SIM se utiliza para una distribución de autenticación y de clave de sesión utilizando la tarjeta SIM GSM. La autenticación estándar de la red móvil GSM se basa en el mecanismo de “challenge-response” (respuesta de desafío). Basada en los algoritmos especificados por los operadores, la tarjeta SIM utiliza el reto de 128-bits y la clave secreta (clave de abonado), Ki, para generar una respuesta de 32-bit y una clave de cifrado de largo de 64-bit, Kc, como salida.

El Ki, que también se conoce como la clave de autenticación, es un valor de 128-bits utilizado para autenticar tarjetas SIM en la red. Cada SIM se asociada con una única Ki, que es asignada por el operador. Por lo tanto, la seguridad del protocolo depende de Kc. Sin embargo, para redes de datos que requieren claves más fuertes y más largas, Kc no es muy seguro. Para mejorar la seguridad, el mecanismo de EAP-SIM combina múltiples desafíos para generar varias claves de cifrado Kc de 64

bits de longitud. La seguridad de EAP-SIM se basa en el mecanismo de GSM. Si las credenciales SIM son utilizadas sólo para EAP-SIM, y no son reutilizados de GSM / GPRS, EAP-SIM es un método más seguro que los mecanismos subyacentes a GSM.

k) EAP-AKA

EAP (EAP Authentication and Key Agreement) es un mecanismo de autenticación y de distribución de claves utilizados en las redes móviles de tercera generación (3G): UMTS y CDMA2000. AKA se basa en el mecanismo de respuesta de desafío y en la criptografía simétrica.

La introducción de AKA dentro EAP permite una gran variedad de nuevas aplicaciones, entre las que se incluyen las siguientes:

- El uso del AKA también como un método seguro de autenticación PPP en dispositivos que ya contienen un módulo de identidad.
- El uso de la infraestructura de autenticación de redes móviles de 3ª generación en el contexto de las redes LAN inalámbricas
- Basándose en AKA y en la infraestructura existente de forma perfecta con cualquier otra tecnología que pueda utilizar EAP.

7. Clave Precompartida o PSK

Como hemos mencionado antes, el segundo modo de funcionamiento de WPA es el Modo Personal. Este modo requiere la configuración manual de una clave precompartida (PSK o PreShared Key) en el punto de acceso y los clientes, es decir, a efectos del cliente basa su seguridad en una contraseña compartida. WPA-PSK usa una clave de acceso de una longitud de entre 8 y 63 caracteres, que es la clave compartida. Al igual que ocurría con WEP, esta clave hay que introducirla en cada una de las estaciones y puntos de acceso de la red inalámbrica. Cualquier estación que se identifique con esta contraseña, tiene acceso a la red. No se necesita servidor de autenticación. Las características de WPA-PSK lo definen como el sistema, actualmente, más adecuado para redes de pequeñas oficinas o domésticas, la configuración es muy simple, la seguridad es aceptable y no necesita ningún componente adicional.

La principal debilidad de WPA-PSK es la clave compartida entre estaciones. Cuando un sistema basa su seguridad en un contraseña siempre es susceptible de sufrir un ataque de fuera bruta, es decir, ir comprobando contraseñas, aunque dada la longitud de la contraseña y si está bien elegida no debería plantear mayores problemas. Hay un momento de debilidad cuando la estación establece el diálogo de autenticación. Este diálogo va cifrado con las claves compartidas, y si se “entienden” entonces se garantiza el acceso y se inicia el uso de claves dinámicas. La debilidad consiste en que conocemos el contenido del paquete de autenticación y conocemos su valor cifrado. Por ello, en una instalación de este tipo es necesario aplicar medidas de seguridad adicionales para aumentar el nivel de seguridad de la red lo máximo posible.

A pesar de su vulnerabilidad, es recomendable emplear WPA-PSK cuando sea la única solución de seguridad implementable para evitar dejar la red WLAN abierta y completamente expuesta a posibles ataques.

8. Mecanismos de cifrado o encriptación

Definimos la confidencialidad en redes inalámbricas como el acto de asegurar que la información transmitida entre los puntos de acceso y los clientes no sea revelada a personas no autorizadas. La confidencialidad debe asegurar que en toda comunicación la información solo puede ser interpretada por el equipo al que va dirigida.

La encriptación es un proceso de combinación entre un mensaje y una clave secreta, a través de un algoritmo de encriptación. El objetivo es lograr que el resultado aparezca a los ojos de un atacante como un flujo binario aleatorio imposible de descifrar o comprender, pero que sea posible descifrarlo por nuestro receptor para recuperar la información gracias al conocimiento de la clave secreta. En ocasiones la gente habla de encriptación refiriéndose a un protocolo de seguridad concreto. Sí es cierto en cambio, que se suelen crear protocolos de seguridad en torno a algoritmos de encriptación.

9. El mecanismo RC4

9.1. Características de RC4:

RC4 es un algoritmo de cifrado en flujo (Ron's Cipher 4), fue desarrollado por Ronald Riverst en 1987 y mantenido en secreto compartido con la empresa RSA Data Security. El problema de los algoritmos de seguridad que se mantienen en secreto se da en el momento que deja de serlo, y con RC4 ocurrió el 9 de Septiembre de 1994, cuando apareció de forma anónima en Internet.

Entrando en las características técnicas del algoritmo, debemos notar que usa claves de longitud variable entre 1 y 256 bytes, generadas con el algoritmo de generación de claves (KSA). Una vez completado, el flujo de bits cifrados se genera usando un algoritmo de generación pseudoaleatoria (PRGA). Si profundizamos un poco más en el algoritmo en sí, RC4 define una tabla interna de estados en el instante t para un valor habitual de n = 8 como:

$$\left(s_t(l)\right)_{l=0}^{2^n-1}$$

y dos punteros de tamaño n, i_t y j_t, generando la salida en el instante t, Z_t.
La evolución de la tabla sería la siguiente:

- $i_0 = j_0 = 0$
- $i_t = i_{t-1} + 1$
- $j_t = j_{t-1} + S_{t-1}(i_t)$
- $S_t(i_t) = S_{t-1}(j_t), S_t(j_t) = S_{t-1}(i_t)$
- $Z_t = S_t(S_t(i_t) + S_t(j_t))$
- Todas estas operaciones realizadas en módulo 2^n

A partir de la clave k se crea por repetición o extensión pseudoaleatoria la cadena clave:

$$K = \left(K_l\right)_{l=0}^{2^n-1}$$

A partir de la cadena clave calculamos la tabla interna inicial S_0 haciendo $j_0=0$ y para cada $l \leq t \leq 2^n$, $j_t=(j_{t-1}+S_{t-1}(t-1)+K_{t-1})$ (mod 2^n), intercambiando en cada instante $S_{t-1}(t-1)$ con $S_{t-1}(j_t)$. En el último resultado el bucle definirá la tabla inicial S_0.

La implementación del algoritmo tanto de generación de clave como el de generación pseudoaleatoria sería la que se muestra en la siguiente figura:

KSA(K)	PRGA(K)
Inicialización: For *i = 0 … N – 1* *S[i] = i* *j = 0* Codificando: For *i = 0 … N – 1* *j = j + S[i] + K[i mod l]* *Swap(S[i], S[j])*	Inicialización: *i = 0* *j= 0* *Bucle de generación* *i = i +1* *j = j +1* *Swap(S[i], S[j])* *Output z = S[S[i] + S[j]]*

Figure 14: Implementación del algoritmo RC4

9.2. Ataques al algoritmo RC4:

Los ataques que ha sufrido el algoritmo RC4 han sido muchos y variados. El hecho de que fuera usado en WEP, y este protocolo, a su vez se usara para la seguridad de redes inalámbricas, le ha convertido en objeto de múltiples ataques. Dichos ataques se han planteado desde dos perspectivas, ataques pasivos y ataques activos. Dentro de los primeros se encuentran los ataques al algoritmo RC4.

Este ataque fue creado por Fluher, Mantin y Shamir. Lo que busca se explicará a continuación, pero su objetivo es conseguir obtener la clave de cifrado a partir de los vectores de inicialización (IV). Y una vez se consigue la clave, se puede proceder a efectuar ataques activos a WEP.

9.3. Debilidades del KSA:

El principal problema que tiene el sistema de generación de claves es la concatenación de la clave secreta con el vector de inicialización (IV). Se considera el caso en que la *session-key* presentada por el KSA está formada por una clave secreta fija concatenada con el vector de inicialización. Si un atacante puede obtener la primera palabra de salida del algoritmo RC4 correspondiente a cada IV, podría reconstruir la clave secreta con poco trabajo.

Como sólo nos interesa la primera palabra de salida para una clave secreta dada y un IV, podemos simplificar el modelo de salida. La primera palabra de salida depende únicamente de tres elementos permutados específicos.

Partimos de que conocemos que el primer byte del *keystream* es S[S[1]+S[S[1]]], ya que se concatena un vector inicial de 3 bytes a la clave. También sabemos que el primer byte de texto en claro que se envía es la cabecera LLC (SNAP) para TCP/IP es 0xAA. Entonces S[S[1]+S[S[1]]] = 0xAA xor C1, siendo C1 el primer byte cifrado.

En este punto abordaremos el ataque FMS clásico. Se puede utilizar para derivar la clave (40, 128 bits) una vez capturados una buena cantidad de paquetes de datos cifrados. Para ello se hará uso de herramientas software creadas con el objeto de conseguir la clave secreta. Dependiendo de la iteración analizada, la cantidad de elementos invariantes hasta el final del algoritmo de cálculo de la tabla inicial, sigue una distribución estadística. Eligiendo candidatos aquellos bytes que más se

asemejan a esa distribución estadística, calculo recursivamente todos los bytes de la clave. Sólo calcularemos K[A] si sabemos los K[i] anteriores.

Podemos mejorar el ataque partiendo del conocimiento de que los tres primeros bytes conocidos a transmitir, que son 0xAA:0xAA:0x03. Y la forma de actuar se guía por los siguientes pasos:

- Apuntar los paquetes resueltos disminuyendo las posibles combinaciones de bytes de la clave.
- Suponer que el usuario introducirá una clave fácil de recordar que estará
- compuesta por caracteres ASCII.
- Comprobar si los bytes de la clave son caracteres ASCII. De ese modo aumentan las posibilidades de adivinar la clave secreta.
- Con suficientes IVs débiles para un valor concreto de un byte de la clave, realizar un análisis estadístico.

10. WEP

10.1. Introducción:

Aunque la privacidad es únicamente una de las partes que componen la seguridad en las WLAN, la búsqueda de ésta es uno de los principales objetivos con los que se definió WEP.

La seguridad WEP se puede descomponer en dos partes. En la primera se lleva a cabo la autenticación, y una vez completada con éxito, la segunda se encarga de la encriptación de los mensajes. Esta encriptación sirve también para continuar autenticando cada mensaje.

Se basa en el algoritmo RC4, analizado anteriormente.

10.2. Funcionamiento de WEP:

a) Vector de inicialización (IV):

En WEP se utiliza un vector de inicialización (IV). Este método se basa en un concepto muy simple. En vez de utilizar solamente la clave secreta para encriptar los paquetes, lo que hacemos es combinar esta clave secreta con un número de 24 bits que va cambiando sus valores. El valor del IV no es secreto, es necesario su envío en plano junto al mensaje para que el destinatario sea capaz de llevar a cabo el proceso inverso.

En teoría los valores iniciales del IV se generan de forma aleatoria, y a partir de ahí se van incrementando de uno en uno para que pase el máximo tiempo posible sin repetirse. En la práctica se basan en mecanismos pseudoaleatorios que partiendo de una misma semilla acaban generando la misma secuencia, y a su vez se apoyan en sistemas que al reiniciarse parten del mismo valor inicial.

b) Claves WEP:

En el estándar se hace mención a dos tipos de claves, Default keys y Key mapping keys. Estas claves tienen dos características:

- Son de longitud fija: 40 0 104 bits.
- Son estáticas, salvo que se reconfiguren los equipos de los clientes y el AP.

Al ser las claves estáticas e idénticas en ambos extremos de la comunicación, cabe la pregunta de cómo se ha llegado a compartir dicha información. Ante esto el estándar se limita a decir: *"La clave*

secreta se presupone que ha sido entregada en ambos dispositivos a través de un canal seguro independiente de IEEE 802.11".

Algunos fabricantes de equipos, como CISCO, han llevado a cabo soluciones relativamente satisfactorias sobre esta cuestión, aunque estos asuntos quedan dentro del ámbito de las soluciones propietarias y por tanto fuera del estándar WEP.

- Default keys: En un sistema WEP el AP utiliza el mismo conjunto de claves secretas, cuatro en total, con todos los dispositivos clientes. En la práctica, bastaría con una clave compartida.
- Key mapping keys: Es un modo de funcionamiento totalmente opcional que consiste en que cada dispositivo cliente tiene su propia clave secreta individual para comunicarse con el AP. Esto es muy útil y deseable para redes grandes en las que mantener una única clave compartida en secreto o cambiar dicha clave sería muy difícil.

Realizamos el siguiente proceso sobre cada una de las MSDU o MAC Service Data Unit (paquetes de datos que se entregan a la capa MAC):

1. Fragmentamos en unidades más pequeñas.
2. Encriptamos con WEP cada uno de estos fragmentos de forma independiente.
3. Le agregamos una cabecera MAC al principio, y un campo Checkword al final.

Tras este proceso obtenemos los MPDUs, que son los paquetes que viajan por la red.

c) *Fragmentación:*

Proceso que se lleva a cabo en la capa MAC del protocolo 802.11. Las MSDUs que llegan a este nivel deben fragmentarse en unidades de tamaño fijo para poder enviar el paquete por el medio de transmisión. El tamaño de los paquetes resultantes del proceso completo depende de las MSDUs iniciales y de las reglas de fragmentación, aunque típicamente oscilan entre 10 y 1500 bytes.

d) *ICV o Integrity Check Value:*

Se trata de un campo de 4 bytes que se añade a continuación del fragmento de datos, antes de realizar el cifrado. El objetivo de este campo es garantizar la integridad del mensaje. Se trata de un resumen o hash que se genera mediante un CRC o Código de Redundancia Cíclica a partir del texto plano. Se caracteriza porque si modificamos el texto, por leve que sea la modificación, el resumen que se derivaría de este nuevo texto sería completamente distinto. Esto permite que no se pueda modificar el texto, salvo que se conozca como descifrar el texto, y como generar un nuevo ICV. Cualquier otra modificación que no se haga así nos llevará a un ICV incoherente, y por tanto, a descartar la trama.

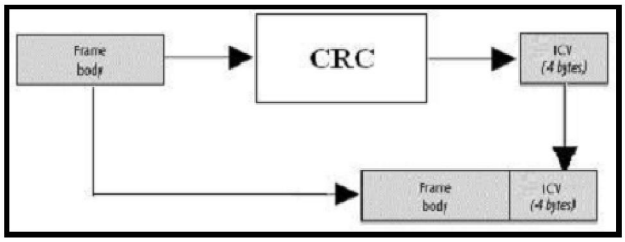


Figura 15: Generación del ICV

e) *Preparación de la MPDU:*

Los dos campos que viajan encriptados son el ICV y los datos. A continuación podemos observar un esquema del proceso, que vamos a describir brevemente:

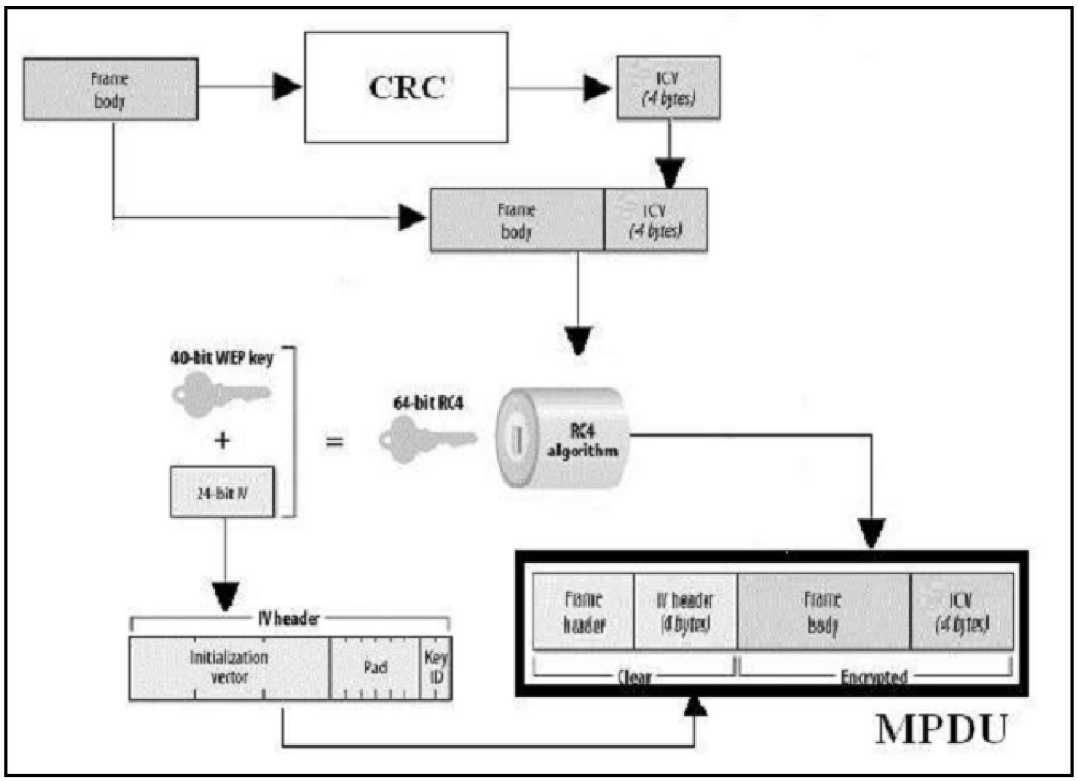


Figura 16: Generación de la MPDU

1. Mediante un generador aleatorio se obtiene un valor para el Vector de Inicialización (IV).
2. Se combina el IV con la clave secreta para generar la clave completa de cifrado.
3. Se hace pasar por el algoritmo al bloque compuesto por los datos más el ICV. Por cada byte de datos introducidos se obtendrá un byte de datos cifrados.
4. Finalmente se añade al texto cifrado resultante un campo llamado IV Header, en el que se transporta el valor del IV en plano, y el Key ID, que identifica la clave secreta utilizada dentro del conjunto de las cuatro Default Keys. Por último se añade la cabecera MAC con las direcciones origen y destino para que el paquete alcance su objetivo.

10.3. Debilidades de WEP:

Aunque el estándar fue aprobado en 1997, no se extendió en uso de las redes 802.11 hasta el año 1999, cuando surgió 802.11b y el sello WiFi. Fue en ese momento cuando los ingenieros comenzaron a señalar algunos problemas de WEP. Entre ellos se observó: autenticación extremadamente débil y una gestión de claves muy complicada, por lo que se promovió un grupo de trabajo para que fuera tratando estos temas.

A continuación veremos como WEP falla en cada una de las áreas que componen un sistema de seguridad, y en qué se basan los mecanismos que explotan estas deficiencias.

a) Autenticación:

La autenticación de WEP se puede romper de la siguiente forma:

- Se observa el medio y se captura una pareja del *Challenge Text* en plano y cifrado.

- Mediante una simple operación de XOR se obtiene el *Keystream* correspondiente a ese mensaje (y por lo tanto a ese IV), ya que el IV viaja en plano como cabecera del mensaje cifrado. Por esto estamos en condiciones de cifrar cualquier mensaje para ese IV dado sin más que hacer un XOR con el *Keystream*, aunque no lo conozcamos la clave secreta de la que proviene.

Recordemos que para cada clave e IV se generaba un *Keystream*, mediante un generador pseudoaleatoria, con el que se hacía el XOR con el texto, siendo el resultado el texto cifrado.

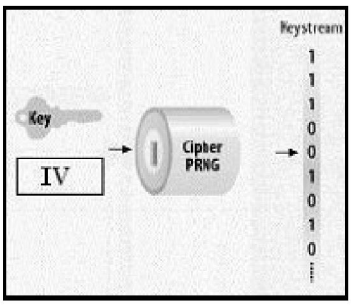


Figura 17: Generación del Keystream

- Finalmente, para romper la autenticación basta con hacer un request, esperar el texto plano, cifrarlo con el *Keystream* incluyendo en la respuesta el IV interceptado. La respuesta al desencriptar será la esperada.

b) *Integridad de mensajes:*

Sería peligroso que alguien pudiera modificar el contenido del mensaje sin que se detectara en el destino. Para evitar este problema, conocido como Modificación o Tampering, se incluye en WEP el campo ICV:

- Se trata de un resumen hash del mensaje, de modo que cualquier modificación en el mensaje por leve que fuera derivaría en otro ICV distinto.
- Se cifra junto al texto, de modo que una modificación del texto, aunque se haga sobre el texto cifrado, derivaría en una incoherencia con su ICV correspondiente.

De esta forma, este ataque sólo tendrá éxito cuando el atacante sea capaz de hacerse con la clave de cifrado para reconstruir correctamente un nuevo datagrama tras modificar el texto.

De nuevo WEP se equivocaba puesto que por una propiedad del CRC usado para calcular el ICV, llamada *Linear Method* se puede determinar qué conjunto de bits del hash cambian cuando cambia un bit del texto. Por el mecanismo de cifrado utilizado (RC4 emplea XOR) esta relación entre bits pervive hasta el texto encriptado y su correspondiente hash encriptado, por lo que de nuevo el objeto de WEP no se consigue.

c) *Privacidad:*

A continuación se comentan tres problemas distintos e independientes que permiten al atacante apoderarse de las claves y quebrar la privacidad:

c.1) Reutilización de IV:

En octubre del año 2000, Jesse Walter, un criptógrafo de Intel remitió una carta al comité 802.11 del IEEE titulada “Inseguro independientemente del tamaño de la clave: un análisis de la encriptación WEP”. Este artículo ponía de manifiesto el problema de la reutilización del IV.

El IV se añadió porque si la única semilla del Generador PseudoAleatorio Numérico (PRNG) que genera el Keystream fuera la clave secreta, que tiene un valor fijo, el Keystream obtenido sería siempre el mismo. Esto quiere decir que averiguando el Keystream, cosa sencilla visto el método de autenticación, estaríamos en condiciones de codificar cualquier mensaje.

La idea del IV es buena, pero tropieza con un inconveniente debido a que sólo puede tomar un conjunto de valores determinados. WEP asume que la reutilización del IV no es problemática, y ahí es donde está la equivocación.

Ataques basados en la reutilización del IV son posibles aunque laboriosos, y por tanto, este aspecto no presenta la mayor debilidad de las muchas que presenta WEP.

c.2) Valores débiles de las claves RC4:

Para ciertos valores de clave, llamados Claves Débiles, un número desproporcionado de bits de los primeros bytes que forman el *Keystream* son determinados por unos pocos bits de la clave.

En teoría, si cambiásemos un solo bit de la clave, cada uno de los bits del Keystream debería tener un 50% de probabilidades de cambiar, pero esto en el caso de las Claves Débiles no sucede, ya que algunos bits tienen mayor efecto modificador que otros.

La solución es sencilla, RSA Labs recomienda descartar los 256 primeros bytes obtenidos del Keystream, que son los que tienen la debilidad, de manera que se elimina el problema y se continúa aprovechando las virtudes de RC4. Por supuesto, WEP no hace caso de esta recomendación, y eso implica que si en los nuevos sistemas se adoptase esto, no podrían ser interoperables con los antiguos.

Tampoco se puede solucionar este problema evitando las claves débiles, ya que la modificación continua del IV tarde o temprano nos llevará a una de ellas.

c.3) Ataques directos de clave:

Estamos ante el ataque más peligroso que se puede hacer a WEP, hasta el punto que los problemas anteriores carecen de importancia al lado de éste.

Se basa en que los primeros bytes del texto encriptado suelen corresponder a una cabecera SNAP por lo que sus valores son conocidos. Lo que se hace es jugar con el texto plano supuesto y su valor encriptado, ya que para el texto plano correspondiente a dicha cabecera, los valores posibles son limitados. Esto permite descifrar el primer byte de la clave con una fiabilidad razonable capturando unos sesenta mensajes.

El método continúa y se pueden ir obteniendo de uno en uno los bytes de la clave a medida que se captura tráfico. La peligrosidad de este ataque radica en lo siguiente:

- A medida que aumenta el tamaño de las claves, el tiempo de quebrar el sistema aumenta linealmente, y no exponencialmente, por lo que una clave más larga lo único que consigue es que el ataque dure un poco más del doble de tiempo.
- Al ser un método mecánico y secuencial es posible crear, como de hecho ha sucedido, una herramienta que obtenga las claves y que convierta a cualquier persona en un atacante potencial.

11. RSA

El algoritmo de clave pública RSA fue creado en 1978 por Ronald Rivest, Adi Shamir y Leonard Adleman. Para ello, se basaron en el artículo de 1976 de Whitfield Diffie y Martin Hellman, titulado "New directions in Crytography" que supuso una revolución en la criptografía, ya que fue el punto de partida de los sistemas de llave pública. Además de este algoritmo fundaron la empresa RSA Data Security Inc., que actualmente es una de las más prestigiosas en el entorno de la protección de datos.

Este algoritmo todavía se usaba en 2002 para proteger los códigos de las armas nucleares de Estados Unidos y Rusia.

Los sistemas de cifrado de clave pública se inventaron con el fin de evitar por completo el problema del intercambio de claves, que es inherente a los sistemas de cifrado simétricos. Los sistemas de cifrado asimétricos usan un par de claves para el envío de los mensajes. Las dos claves pertenecen a la persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona. La otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.

RSA se basa en la dificultad que presenta la factorización de números enteros de gran tamaño para el estado del arte de la tecnología actual.

RSA funciona de la siguiente forma:
En primer lugar es necesario que cada usuario calcule su clave pública y privada:

- Se buscan dos números primos lo suficientemente grandes: p y q (de entre 100 y 300 dígitos).
- Se obtienen los números n = p * q y Ø = (p-1) * (q-1).
- Se busca un número e tal que no tenga múltiplos comunes con Ø, es decir, e y Ø son primos relativos. Existe una propiedad de la aritmética modular que dice que un número a tiene inversa módulo Ø siempre que sean primos relativos.
- Se busca d tal que d * e mod Ø = 1 (es decir, d es el inverso de e en la aritmética mod Ø), con mod = resto de la división de números enteros.

Y ya con estos números obtenidos, n es la clave pública y d es la clave privada. Los números p, q y Ø se destruyen. También se hace público el número e, necesario para alimentar el algoritmo.

Para cifrar m calculamos m^e mod n, siendo m el mensaje. Para descifrarlo se eleva (m^e)^d mod n.

En cuanto a las longitudes de claves, el sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits.

Este algoritmo ha sido roto (con claves de diferentes longitudes), varias veces, aumentando cada vez la longitud de la clave que se consigue romper. La última vez fue el 7 de enero de 2010, y aquella vez la base era de 768 bits.

En los primeros días de Marzo de 2010 (en torno al día 5) Valeria Bertacco, Todd Austin y Andrea Pellegrini alcanzaron un nuevo hito, romper un sistema RSA de 1024 bits. Lo consiguieron variando los niveles de tensión en el equipo del destinario para generar cifrados defectuosos. Obtuvieron la clave privada del sistema combinando una serie de fragmentos que habían obtenido en el proceso. Utilizaron un clúster de 81 chips Pentium 4 trabajando durante 104 horas. El aparto que utilizaron no

dañaba el equipo, por lo que no dejaba huellas.

Aunque a primera vista esto podría generar gran pánico en torno a la seguridad de RSA 1024, no es así. Expertos como Fernando Acero, han explicado, tras la mediática noticia, que la ruptura de este sistema no se ha conseguido mediante un avance en la factorización de números y que este ataque se ha realizado sobre un software y un hardware muy específico, por lo que no se puede decir que cualquier clave RSA de 1024 esté en peligro. Además el ataque ha de realizarse sobre el equipo que contenga la clave privada,

Además Andrea Pellegrini en el *Design, Automation and Test in Europe (DATE)* celebrado en Dresde, Alemania, ofreció una sencilla y muy conocida solución al problema; el *Salting*. Se trata una técnica criptográfica común, que cambia el orden de los dígitos de una forma aleatoria cada vez que se solicita la clave.

12. 3DES

El estándar de encriptación de datos (DES) fue desarrollado por IBM en 1974. Triple DES es una pequeña variación de este estándar, tres veces más lento que su predecesor, pero billones de veces más seguro. Triple DES presenta muchos más usos que DES, ya que DES resulta fácilmente rompible con la tecnología actual. El DES original usa una única clave de 56 bits. En 1998 lo organización Electronic Frontier Foundation, usando un ordenador especialmente diseñado para este propósito, fue capaz de romper DES en menos de tres días. Posteriormente se ha demostrado, que usando un equipo mucho más caro (su precio rondaría el millón de dólares, frente a las 250 mil dólares que costó el ordenador utilizado en 1998), se podría romper DES en un 3 horas y media. Todo esto demuestra que DES no se puede considerar seguro.

Triple DES está basado en el algoritmo DES, por lo que el paso de DES a Triple DES resulta muy sencillo.

Triple DES se estandarizó inicialmente para aplicaciones financieras en el estándar ANSI X9.17 en 1985. El 3DES se incorporó como parte del DES en 1999, con la publicación de FIPS PUB 46-3.El 3DES usa tres claves y tres ejecuciones del algoritmo DES. La función sigue la secuencia cifrar- descifrar-cifrar (EDE: encrypt-decrypt-encrypt):

$$C = E_{K3}[D_{K2}[E_{K1}[P]]]$$

siendo C el texto cifrado, P el texto claro, $E_k[X]$ =cifrado de X usando la clave K, $D_k[Y]$ descifrado de Y usando la clave K. El descifrado consiste en realizar la misma operación, pero con las claves en orden inverso.

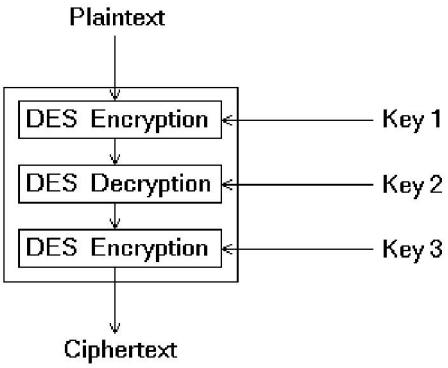


Figura 18: Cifrado 3DES

Con 3 claves diferentes, el 3DES tiene una longitud efectiva de clave de 168 bits. El FIPS 46-3 también permite el uso de dos claves, con K1=K3, lo que proporciona una longitud de clave de 112 bits. Este algoritmo es muy robusto. Con 168 bits de longitud, los ataques de fuerza bruta son imposibles de

realizar con efectividad.
Otro atractivo que presenta 3DES es que usa el mismo algoritmo de cifrado que DEA. Este algoritmo ha estado sujeto a más escrutinios que ningún otro durante un largo período de tiempo, y no se ha encontrado ningún ataque posible salvo la fuerza bruta. Por lo tanto, 3DES presenta una gran seguridad.

Sin embargo, el algoritmo 3DES se considera obsoleto desde 2001, que fue el año en el que el Instituto Nacional de Estándares y Tecnología (NIST) lo sustituyó por AES. Al desarrollar AES, se trató de que fuera al menos tan seguro como Triple DES, pero mucho más rápido, cosa que se consiguió.
AES puede llegar a ser hasta 6 veces más rápido y a la fecha no se ha encontrado ninguna vulnerabilidad.

13.AES

El algoritmo AES usa una longitud de bloque de 128 bits, y la longitud de la clave puede ser de 128, 192 o 256 bits. En la descripción que vamos a hacer a continuación se supone una longitud de la clave de 128 bits, ya que posiblemente sea la más implementada.

En la siguiente figura se muestra la estructura general del algoritmo AES. La entrada a los algoritmos de cifrado y descifrado es un solo bloque de 128 bits. En el FIPS PUB 197, este bloque se representa con una matriz cuadrada de bytes. Este bloque se copia en el vector Estado, que se modifica en cada etapa del cifrado o descifrado. Después de la última etapa, el vector Estado se copia en una matriz de salida. De igual manera, la clave de 128 bits se representa como una matriz cuadrada de bytes. Esta clave luego se expande en un vector de palabra para la generación de claves; cada palabra tiene cuatro bytes, y el número total de palabras para generar claves de 44 para la clave de 128 bits. El orden de los bytes dentro de una matriz se establece por columnas. Así, por ejemplo, los primeros 4 bytes de una entrada de texto plano de 128 bits al cifrador ocupan la primera columna de la matriz **in,** los segundos 4 bytes la segunda columna, y así sucesivamente. De igual forma, los primeros 4 bytes de la clave expandida, que forman una palabra, ocupan la primera palabra de la matriz **w**.

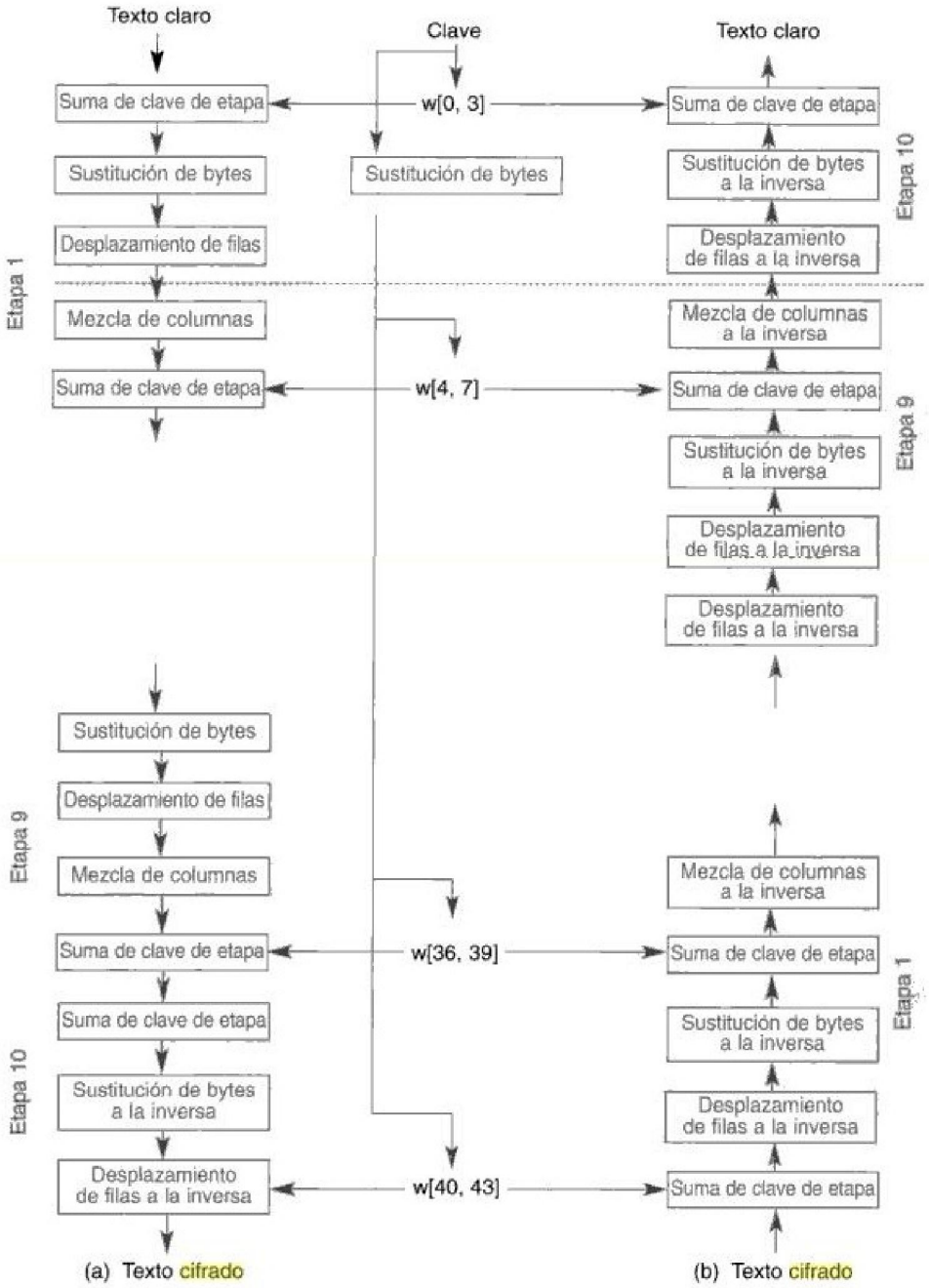


Figura 19: Cifrado y descifrado AES

Algunos aspectos del algoritmo AES:

1.- Una característica notable de su estructura es que no es una estructura Feistel. En la estructura clásica de Feistel, la mitad del bloque de datos se usaba para modificar la otra mitad, y entonces se intercambiaban entre sí. El algoritmo AES procesa todo el bloque de datos en paralelo durante cada etapa, realizando sustituciones y permutaciones.

2.- La clave suministrada como entrada se expande en un vector de 44 palabras de 32 bits, w[i]. Cuatro palabras diferentes (128 bits) sirven como clave de entrada en cada ronda.

3.- Se utilizan cuatro fases diferentes, una de permutación y tres de sustitución:

- Sustitución de bytes: se usa una tabla, denominada caja S, para realizar una sustitución byte a byte del bloque.
- Desplazamiento de filas: una simple permutación realizada fila por fila.
- Mezcla de columnas: una sustitución que altera cada byte de una columna en función de todos los bytes de la columna.
- Suma de la clave de etapa: una simple operación XOR bit a bit del bloque actual con una porción de la clave expandida.

4.- La estructura es muy simple. Tanto para el cifrado como para el descifrado, se comienza con una fase de suma de clave de etapa, seguido de nueve etapas de cuatro fases cada una, y acaba con una décima etapa de tres fases. La siguiente figura muestra la estructura de una etapa completa de cifrado.

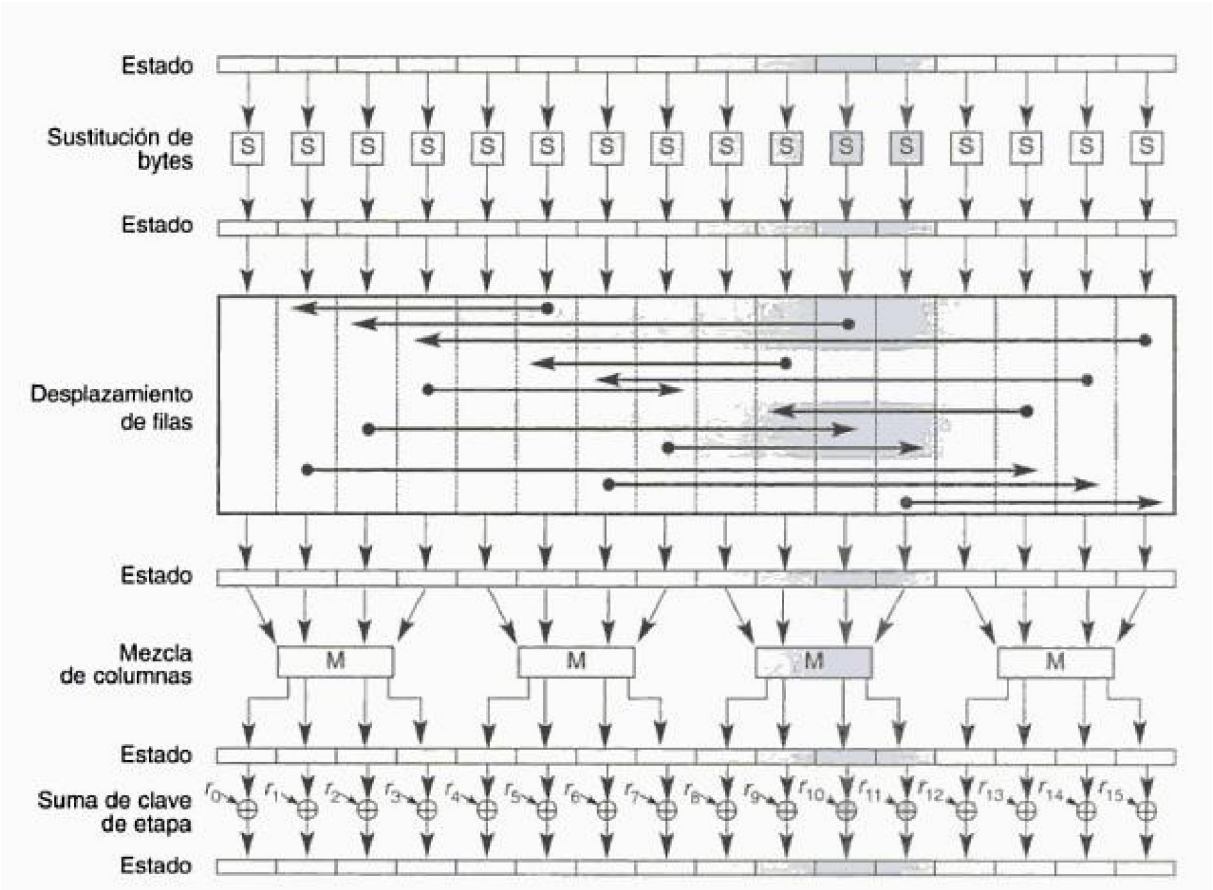


Figura 20: Etapa del cifrado del AES

5.- Solamente la fase de suma de la clave de etapa utiliza la clave. Por esta razón el cifrador comienza y termina con una suma de clave de etapa. Cualquier otra fase, aplicada al comienzo o al final, sería reversible sin conocer la clave y por tanto añadiría inseguridad.

6.- La fase de suma de la clave de etapa no funcionaría por sí misma. Las otras tres fases juntas desordenan los bits, pero no proporcionan seguridad por sí mismos, porque no usan la clave. Se puede ver el cifrador, como una secuencia alternativa de operaciones de cifrado XOR (suma de clave

de etapa) de un bloque, seguida por un desordenamiento del bloque (las otras tres fases), seguida por un cifrado XOR, y así sucesivamente. Este esquema es eficiente y muy seguro.

7.- Cada fase es fácilmente reversible. Para las fases de sustitución de bytes, desplazamiento de filas y mezcla de columnas, se usa una función inversa en el algoritmo de descifrado. Para la fase de suma de clave de etapa, la inversa se consigue con un XOR entre la misma clave de etapa y el bloque, usando la propiedad de que A ⊕A⊕ B = B.

8.- Como la mayoría de los cifradores de bloque, el algoritmo de descifrado hace uso de la clave expandida en orden inverso. De todas formas, como consecuencia de la estructura particular del AES, el algoritmo de descifrado no es idéntico al de cifrado.

9.- Una vez se ha establecido que las cuatro fases de cada etapa son reversibles, es fácil verificar que el de cifrado recupera el texto plano. La primera figura sobre AES muestra el cifrado y el descifrado desplazándose en direcciones verticalmente opuestas. En cada punto horizontal (por ejemplo, la línea discontinua de la figura), el vector estado es el mismo para el cifrado y para el descifrado.

10.- La última etapa de cifrado y descifrado consiste sólo en tres fases. Otra vez, esto es consecuencia de la estructura particular del AES y es necesario que para el cifrador sea reversible.

14. SHA

14.1. Funcionamiento de SHA:

El algoritmo hash seguro (SHA) fue desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) y publicado en 1993 como un estándar federal de procesamiento de la información (FIBS PUB 180); una versión revisada, que se conoce como SHA-1, se publicó en 1995.

Generación del resumen de un mensaje usando SHA-1:

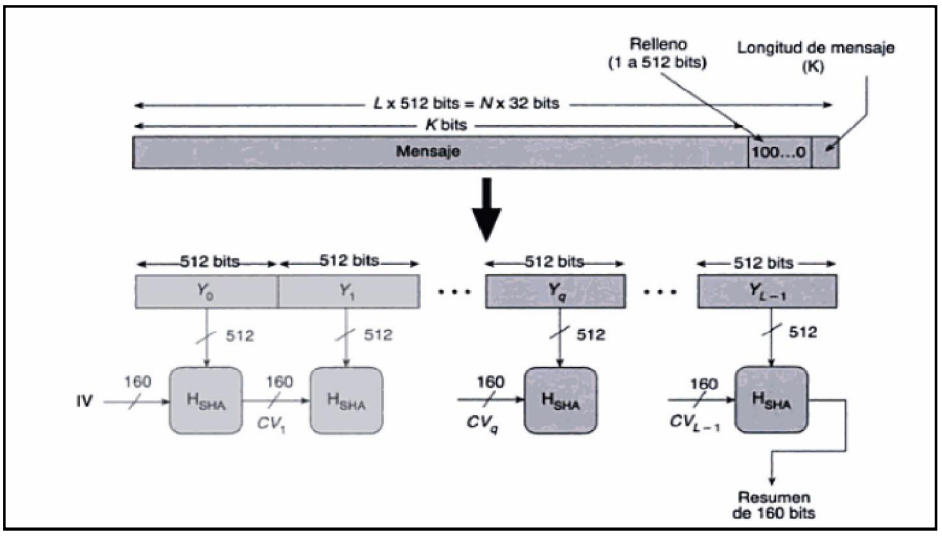


Figura 21: Generación del resumen de un mensaje usando SHA-1

El algoritmo toma como entrada un mensaje con una longitud máxima menor que 2^{64} bits y produce como salida un resumen de mensaje de 160 bits. La entrada se procesa en bloques de 512 bits. La figura anterior muestra el procesamiento general de un mensaje para producir un resumen. El procesamiento consiste en los siguientes pasos:

1.- Añadir bits de relleno: Se añaden entre 1 y 512 bits de relleno (formado por un único bit 1 seguido del número necesario de bits 0), para que la longitud del mensaje sea 448 mod 512, es decir, la longitud del mensaje relleno es 64 bits menor que un múltiplo de 512.

2.- Añadir longitud: Se añade un bloque de 64 bits al mensaje, que contiene la longitud del mensaje original. Con este paso se dificulta un tipo de ataque conocido como ataque de relleno. Ahora la longitud del mensaje es un entero múltiplo de 512 bits.

3.- Inicializar el buffer MD: Para obtener los valores intermedios y finales se utiliza un buffer de 160 bits. Este buffer se representa como cinco registros de 32 bits (A,B,C,D,E) que se inicializan siempre a unos valores predeterminados.

4.- Procesar el mensaje en bloques de 512 bits (16 palabras): El centro del algoritmo es un módulo, conocido como función de compresión, que consiste en cuatro etapas de procesamiento de veinte pasos cada una. La lógica se ilustra en la siguiente figura:

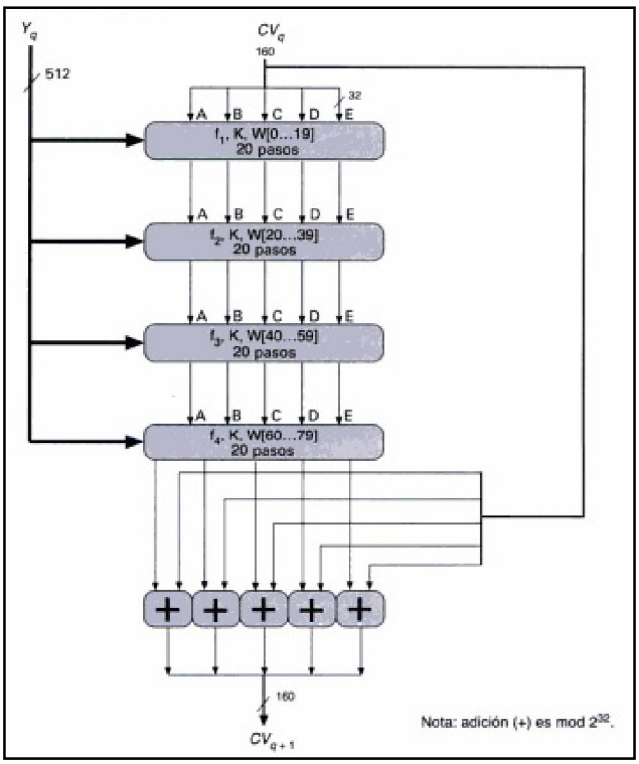


Figura 22: Función de compresión

donde se usan las siguientes constantes:

Número de paso	Hexadecimal	toma parte entera de:
$0 \le t \le 19$	$K_t = 5A827999$	$[2^{30} \times \sqrt{2}]$
$20 \le t \le 39$	$K_t = 6ED9EBA1$	$[2^{30} \times \sqrt{3}]$
$40 \le t \le 59$	$K_t = 8F1BBCDC$	$[2^{30} \times \sqrt{5}]$
$60 \le t \le 79$	$K_t = CA62C1D6$	$[2^{30} \times \sqrt{10}]$

5.-Salida: Después de que todos los bloques L de 512 bits han sido procesados, la salida del L-ésimo estado es el resumen del mensaje de 160 bits. El algoritmo SHA-1 tiene la propiedad por la cual cada bit del código hash es una función de cada bit de la entrada.

14.2. Debilidades de SHA:

En 2005 un equipos de investigadores chinos compuesto por Xiaoyun Wang, Yiqun Lisa Yin y Hongbo Yu (principalmente de la Shandong University en China), demostraron que son capaces de romper SHA-1 en 2005 en unas 2^{69} operaciones, unas 2000 veces más rápido que un ataque de fuerza bruta (que requeriría 2^{80} operaciones).

El NIST (National Institute of Standards and Technology) reconoció la importancia de esta amenaza para algunas aplicaciones que usan firmas digitales, pero también resaltó que muchas de estas aplicaciones incluyen información sobre el contexto, por lo que no es resulta poner en práctica este ataque.

En 2009 el boletín de Hispasec publicó que unos investigadores australianos han logrado reducir el número de operaciones a 2^{52}. A fecha de hoy podemos decir que el algoritmo SHA-1 se ha debilitado en más de un 99% en relación con su fortaleza inicial.

Si ya en el 2004/2005 se aconsejaba abandonar el SHA-1, con este nuevo avance logrado por los australianos, su sustitución por otros algoritmos más resistentes se hace indispensable. Una posible solución, hasta que se publique el SHA-3, es decir, el algoritmo que está llamado a sustituirlo, sería usar dos algoritmos consecutivos, por ejemplo SHA-1 Y RIPEMD-160, puesto que una colisión en SHA-1 es virtualmente imposible que coincida también en RIPEMD-160. Esta solución de la firma múltiple tiene como ventajas que usa algoritmos disponibles en sistemas criptográficos de todo tipo y no implica una excesiva computación.

14.3. Algoritmo SHA-2:

La denominación SHA-2 incluye varias funciones hash con distintos tamaños de salida: SHA-224, SHA-256, SHA-384 y SHA-512, donde el número define el número de bits de salida. SHA-256 y SHA-512 utilizan tamaños de palabra de 32 y 64 bits respectivamente, mientras que SHA-224 y SHA-384 son versiones truncadas de las primeras.

SHA-256 funciona de la siguiente manera:
El mensaje de entrada se divide en bloques de 512 bits, M_i, y se le añade información adicional que incluye la longitud del mensaje original. Para cada uno de estos bloques se ejecuta un *message schedule* que produce 64 variables W_t.

Estas 64 variables son procesadas con la función de compresión mostrada en la figura siguiente, donde las variables A, B, C, D, E, F, G, H se inicializan con valores definidos por el estándar:

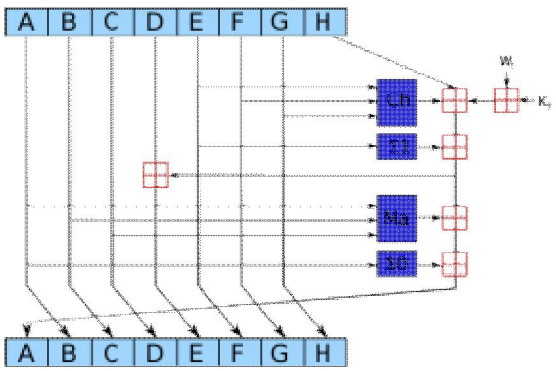


Figura 23: Función de compresión

Tras este procesado, el valor intermedio del hash es obtenido como la suma (módulo 32) de las variables A, B, C, D, E, F, G, H y el valor obtenido en la iteración anterior. Este proceso se ejecuta para cada bloque del mensaje de entrada y al final se obtiene el resumen del mensaje.

14.4. El concurso SHA-3:

En 2009 NIST convocó un concurso para crear un nuevo estándar para funciones hash, SHA-3. La Second SHA-3 Candidate Conference está planificada para Agosto de 2010 y la idea es publicar una revisión del estándar de funciones hash (Hash Function Standard) para 2012.

15. MD5

El algoritmo de resumen de mensaje MD5 (RFC 1321) fue desarrollado por Ron Rivest. Hasta hace unos años MD5 era el algoritmo hash muy usado. Este algoritmo toma como entrada un mensaje de longitud arbitraria y produce como salida un resumen de mensaje de 128 bits. La entrada se procesa en bloques de 512 bits.

Con los años, la velocidad de los procesadores ha aumentado, y la seguridad del código hash se ha puesto en tela de juicio. Se puede demostrar que la dificultad de dar con dos mensajes que tengan el mismo resumen es del orden de 2^{64} operaciones, mientras que la dificultad para encontrar un mensaje a partir de su resumen dado es 2^{128} operaciones. La cifra anterior es demasiado pequeña para garantizar la seguridad.

II. Proyecto Eduroam

1. Eduroam. ¿Qué es?

Eduroam (Educational Roaming) es una iniciativa a nivel internacional que tiene el objetivo de crear un espacio único de movilidad entre las instituciones adscritas al proyecto.

Este espacio único de movilidad consiste en un amplio grupo de organizaciones académicas de ámbito nacional e internacional, que en base a una política de uso y una serie de requerimientos tecnológicos y funcionales, permiten que sus usuarios puedan desplazarse entre ellas, disponiendo en todo momento de servicios móviles que pudieran necesitar.

El objetivo último sería que un usuario al llegar a otra institución dispusiera, de la manera más transparente posible, de un entorno de trabajo virtual con conexión a Internet, acceso a servicios y recursos de su universidad origen, así como de acceso a servicios y recursos de la institución que en ese momento le acoge. Es responsabilidad del usuario móvil respetar las políticas de uso tanto de la institución visitada, como la de su organización origen.

Eduroam es una infraestructura basada en RADIUS que utiliza como tecnología de seguridad 802.1X para permitir la movilidad entre las distintas instituciones que la forman.

Eduroam va a servirnos como escenario para describir la puesta en práctica de algunos de los mecanismos de autenticación y cifrado expuestos anteriormente. Tras describir sus comienzos y la puesta en marcha de este proyecto a nivel mundial, vamos a centrarnos en su implementación en la Universidad de Sevilla.

2. Alcance del proyecto a nivel mundial.

2.1 Breve historia de Eduroam.

La iniciativa Eduroam surgió en 2003 dentro de la *Task Force on Mobility (TF-Mobility)* de Terena (*Trans-European Research and Education Networking Association*). Este departamento creó un banco de pruebas para mostrar la viabilidad de combinar una infraestructura basada en RADIUS con la tecnología del estándar 802.1X para proporcionar movilidad entre las redes educativas y de investigación.

Las pruebas iniciales se llevaron a cabo entre cinco instituciones situadas en Los Países Bajos, Finlandia, Portugal, Croacia y Reino Unido. Más tarde, otras instituciones y organizaciones educativas y de investigación empezaron a unirse a esta infraestructura. Fue en este momento cuando se le dio el nombre de Eduroam (Educational Roaming).

Actualmente Eduroam es una federación de federaciones (confederación); federaciones individuales se dirigen a nivel nacional y todas ellas están conectadas a una confederación regional.

2.2 Organismos reguladores

Tras sus comienzos en Europa Eduroam se ha extendido por gran parte de la comunidad educativa y de investigación de casi todo el mundo.

Actualmente hay tres confederaciones regionales de Eduroam: Europa, Asia-Pacífico y América.

Figura 24: Confederaciones regionales de Eduroam

2.2.1 Organismo regulador en Europa

El servicio Eduroam en Europa es un servicio confederado, proporcionado a través de la colaboración de 36 federaciones de nivel nacional. Aquí se incluyen cientos de organizaciones, la mayoría de las cuales poseen y operan la infraestructura necesaria para ofrecer el servicio. La coordinación nacional e internacional de esta infraestructura la asumen los operadores nacionales de roaming y un centro operativo del equipo Eduroam que está financiado por el proyecto GÉANT (GN3).

A pesar de que Eduroam ha evolucionado mucho en los últimos años sigue en desarrollo. La actividad futura se centrará en lo siguiente:

- Nuevos protocolos de autenticación extensible.
- Apoyo a la internacionalización de nombre de usuarios de Eduroam.
- Privacidad, preservando la identificación frente a estadística y análisis de ataques.

En la Figura se muestra un mapa en el que se han señalado los países europeos que han conectado su servidor RADIUS de mayor nivel al servidor RADIUS europeo de mayor nivel (ETLR).
El ETLR es controlado por la organización nacional de redes para la investigación y la educación en los Países Bajos (SURFNET), y en Dinamarca (UNI-C), con fondos del proyecto GÉANT (GN3).

Figura 25: Países que han conectado su servidor RADIUS Nacional al Europeo

2.2.2 Organismo regulador en España

Eduroam ES es una iniciativa englobada en el proyecto RedIRIS y que se encarga de coordinar a nivel nacional las iniciativas de diversas organizaciones con el fin de conseguir un espacio único de movilidad a nivel nacional.

RedIRIS es la red académica y de investigación española y proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional. Está financiada por el Ministerio de Ciencia e Innovación

RedIRIS cuenta con más de 350 instituciones afiliadas, principalmente universidades y centros públicos de investigación.

El proyecto Eduroam España persigue los siguientes objetivos:

- Coordinar a la puesta en marcha de infraestructuras de movilidad en nuestra comunidad, sirviendo de punto de encuentro de problemas y soluciones.
- Coordinar el desarrollo de una política de uso con el fin de crear un espacio único de movilidad entre nuestras organizaciones y compatible con el desarrollado a nivel europeo.

- Homologar las soluciones tecnológicas a implantar en las diferentes organizaciones con las acordadas a nivel europeo e internacional en este sentido.
- Trabajar en soluciones que ayuden a difundir información sobre tipos de instalaciones e información a nivel de organización sobre: modos de acceso, cobertura, etc.
- Informar de todos los temas relativos a la movilidad: guías de apoyo, estándares, soluciones (tanto propietarias como de libre distribución), etc.
- Promocionar nuevas soluciones e iniciativas originadas en organizaciones de nuestra comunidad tanto dentro de nuestra red, como a nivel internacional.

Figura 26: Organizaciones adscritas al programa Eduroam ES

3. Descripción de las tecnologías usadas en Eduroam

3.1 Elementos de la red y su funcionamiento

802.1X añade funcionalidades a ciertos elementos de la red. Podemos destacar tres componentes fundamentales:

- Un ordenador o portátil con una tarjeta de red, y un sistema operativo que soporte el protocolo 802.1X. Este equipo cumple el papel de solicitante.
- Un puerto, al que el solicitante se conecta, que se encontrará en un switch. Este switch puede denegar o permitir el acceso. Cumple el papel de autenticador. Cuando nos encontramos en una red inalámbrica un dispositivo de control de acceso reemplaza al switch como autenticador.
- El autenticador se dirige a un servidor RADIUS para comprobar si el usuario está autorizado para utilizar un puerto. Este servidor es el tercero componente: el servidor de autenticación.

Resulta irrelevante el tipo de protocolo de transporte que se use (802.11b, 802.11g, 802.11n…).

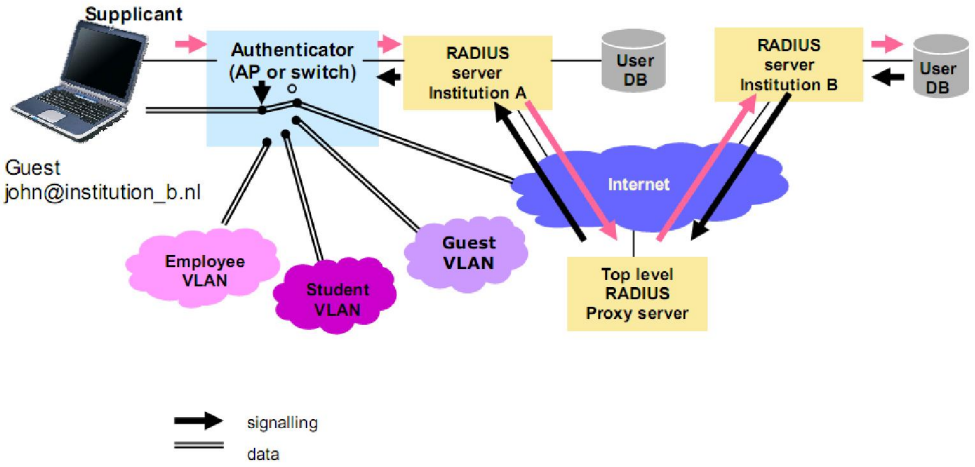


Figura 27: Infraestructura de la Autenticación en 802.1X

Cuando un usuario se conecta a la red, debe proporcionar siempre al autenticador unas credenciales que incluyan un nombre de usuario y un dominio. El autenticador las verifica usando RADIUS.

Si el usuario no pertenece a la institución en la que se encuentra la red a la que intenta conectarse RADIUS detecta que no se trata del dominio local. En ese caso RADIUS envía las credenciales encapsuladas mediante EAP a otro servidor RADIUS de mayor nivel en la jerarquía. Este servidor conoce a todos los servidores RADIUS que existen en la constelación roaming, y envía la petición al servidor que sabe que va a reconocer el dominio. El servidor local RADIUS sólo tiene que conocer a dónde tiene que enviar peticiones de usuarios con un dominio desconocido para él. De esta forma cuando una nueva institución entra a formar parte de Eduroam, no es necesario actualizar todos los servidores RADIUS, sino que es suficiente con hacerlo con los de mayor nivel en la jerarquía.

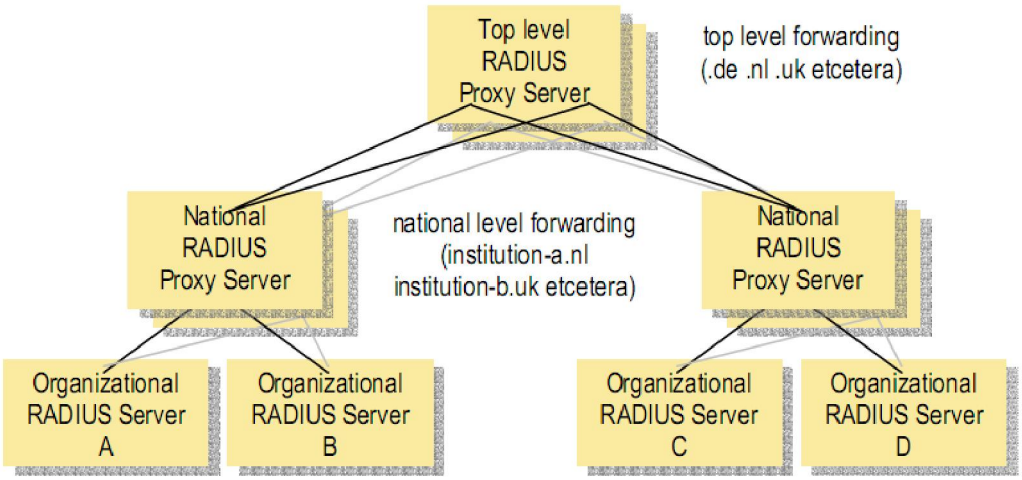


Figura 28: Arquitectura Roaming Internacional

Si un usuario se encuentra en la red de la institución a la que pertenece, el servidor RADIUS le indica al autenticador en que VLAN debe colocarse el tráfico de ese usuario. El cambio de VLAN se basa en

es estándar 802.1Q. Un visitante será asignado a una determinada VLAN para visitantes determinada por el servidor RADIUS de la red de ese visitante.

Una vez que el usuario se ha autenticado con éxito, se lo proporciona conectividad Ethernet, y tiene la posibilidad de utilizar cualquier protocolo de la capa 3.

Cuando el solicitante sale del área de cobertura del dispositivo de control de acceso, éste detecta que la conexión se ha roto y se cierra el puerto.

En la siguiente figura se muestran los distintos mecanismos de autenticación que soporta EAP. En la estructura 802.1X la información de autenticación se transporta sobre EAP (Extensible Authentication Protocol, RFC 2284). Este protocolo permite el uso de cualquier método de autenticación, tales como usuario y contraseña, certificados, OTP (One Time Password, por ejemplo vía SMS) o credenciales que se encuentren en una tarjeta SIM.

Tanto el solicitante como en servidor RADIUS deben usar el mismo tipo de EAP. Al dispositivo de control de acceso no le afecta el tipo de EAP utilizado. Los principales candidatos para la implementación de este sistema son: TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security y PEAP (Protected EAP). Se están haciendo pruebas utilizando una OTP vía SMS.

TLS, TTLS y PEAP establecen una conexión entre el cliente y el dispositivo de control de acceso basada en un certificado del servidor RADIUS. Este mecanismo de autenticación mutua puede prevenir el ataque *Man in The Middle.* TLS usa el certificado del cliente para autenticarlo. TTLS generalmente se utiliza para trasportar un usuario y una contraseña. Como TTLS y PEAP son protocolos que establecen un túnel se puede usar cualquier otro protocolo sobre ellos.

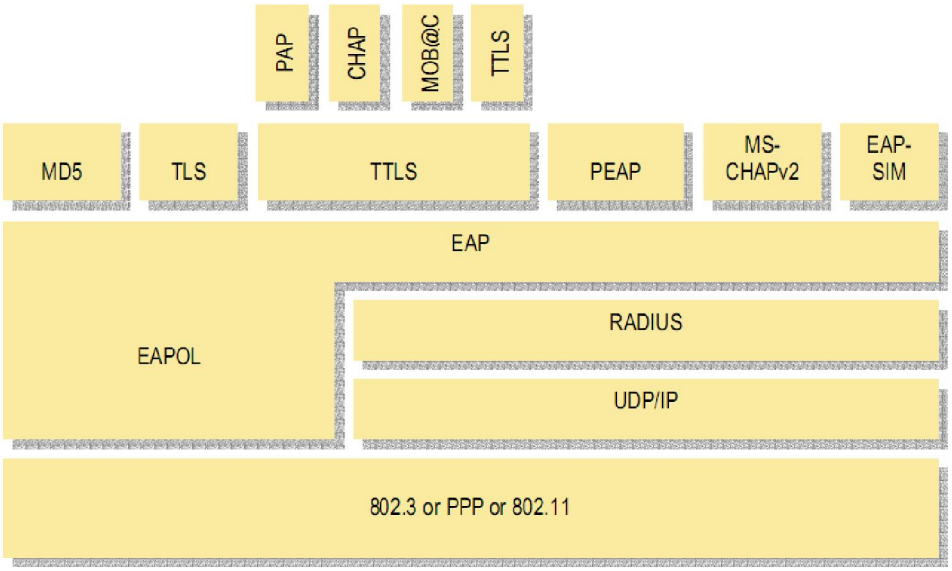


Figura 29: EAP puede soportar varios tipos de Mecanismos de Autenticación

Tras conocer el funcionamiento de estas redes puede resultar interesante detallar algunas características más de los elementos que la componen:

- Cliente/Solicitante: Para la autenticación basada en usuario y contraseña, EAP-TTLS ha sido ampliamente probado. Es fácil de configurar y puede ser usado de forma segura para autenticarnos. Para que un usuario pueda utilizar 802.1X el sistema operativo que utilice debe soportar EAP y el sistema de autenticación de forma nativa o mediante la instalación de un software adicional.

- Dispositivo de control de acceso: La mayoría de los dispositivos de control de acceso actuales soportan la autenticación 802.1X. Se realizaron pruebas con productos de Cisco y Orinoco se resultados satisfactorios.
- Servidor RADIUS: el servidor RADIUS local debe soportar el tipo de EAP utilizado. Los servidores RADIUS intermedio deben ser capaces de reenviar mensajes EAP. La contabilidad es una característica de RADIUS que permite llevar un registro de las peticiones de autenticación. Combinando estas anotaciones con el registro de la asignación de direcciones IP es sencillo rastrear intentos de accesos maliciosos o abusos de red. Los mensajes de contabilidad pueden ser fácilmente reenviados sobre la misma infraestructura.

3.2 Aspectos relacionados con la seguridad

Mientras que se use un protocolo EAP adecuado, como puede ser TLS, 802.1X proporciona una estructura que brinda el suficiente nivel de seguridad. Protocolos que crean túneles tales como PAP o TTLS pueden ser configurados para prevenir algunos tipos de ataques *Man in the Middle* actualmente conocidos. Para proporcionar integridad y privacidad se han propuesto un gran número de extensiones como puede ser WPA, TKIP o 802.11i. Sin embargo, el mecanismo actual que puede ser utilizado para actualizar las claves WEP envía un nivel muy alto de encriptación cuando las claves se actualizan regularmente (típicamente cada veinte minutos o menos cuando se utilizan claves de 64 bits).

La seguridad en la infraestructura RADIUS la proporciona el uso de claves compartidas entre los servidores RADIUS y el hecho de instalar estos servidores en lugares seguros de la red. Sin embargo, algunos mensajes podrían ser alterados por el camino, por lo que además, las rutas entre servidores RADIUS pueden ser protegidas estableciendo túneles IPSEC.

A continuación se van a nombrar una serie de problemas de seguridad y abusos que podrían darse en esta red y los mecanismos que proporciona 802.1X para enfrentarse a ellos:

- Suplantación de identidad: Es difícil detectar abusos en un proceso de autenticación cuando el intruso usa las credenciales de otra persona. RADIUS proporciona registros detallados de la sesiones de usuario, por lo que las quejas de la víctima suplantada pueden ser relacionadas con la sesión actual que ha iniciado el intruso.
- Pérdida de credenciales: Cuando un usuario informa de que ha perdido sus credenciales se puede deshabilitar esa cuenta (tanto en la base de datos de usuarios como el servidor RADIUS de la organización). A partir de ese momento no se puede producir ningún tipo de abuso.
- Abuso del ancho de banda: la detección y la prevención del abuso del ancho de banda en la capa 2 es un problema en cualquier red. Se pueden tomar acciones para modelar el tráfico basado en parámetros VLAN o limitar la capacidad de subida y de bajada en concentradores VPN o pasarelas web, pero esto no previene que los usuarios inunden el aire con una gran cantidad de paquetes en el caso de una red inalámbrica. Si se usa 802.1X el emisor puede ser rechazado en cualquier caso.
- Abuso de contenidos: Este problema se puede solventar mediante un registro que relacione el identificador de un usuario y su IP en una cierta sesión.

Cualquier cuenta sospechosa o incluso un dominio completo se puede bloquear a cualquier nivel de la arquitectura, esto permite prevenir que usuarios u organizaciones sospechosas se conecten a la

red.

3.3 Aspectos relacionados con el uso de la red

Uno de los criterios que más ha influido en el diseño de esta red ha sido proporcionar facilidad de uso a los usuarios finales. Una vez que el usuario instala el cliente 802.1X, el uso de la red es transparente. De hecho, en las pruebas realizadas se observó que los usuarios preferían tener más cantidad de avisos visuales, como la red a la que se están conectando o el nivel de seguridad de la conexión. La única desventaja con la que cuenta 802.1X es su relativa novedad, y el hecho de que actualmente sea necesario un software cliente en la mayoría de las plataformas. Probablemente, la funcionalidad 802.1X se incorporará en los próximos sistemas operativos. Se está trabajando mucho para mejorar la facilidad de uso, sobre todo tratando de integrar la autenticación 802.1X con otros procesos de autenticación.

4. Implementación

Para implementar esta red es necesario contar con una serie de servidores RADIUS, que dependiendo del lugar que ocupen en la jerarquía contarán con las siguientes características y funciones:

- Servidores Proxy RADIUS de las organizaciones (ORPS: Organizational RADIUS Proxy Servers) deben:
    - Resolver las peticiones de su propio dominio.
    - Reenviar las peticiones de otros dominios al servidor RADIUS nacional.
    - Todos los atributos RADIUS se deben reenviar de forma transparente para asegurar la trasparencia EAP.
    - Aceptar peticiones que vengan del servidor RADIUS nacional. Por lo tanto, los servidores RADIUS deben intercambiarse sus direcciones IP y se tiene que determinar un RADIUS Secret que se usará entre cada servidor RADIUS de cada organización y el servidor RADIUS nacional de mayor nivel. El puerto será el 1812.
    - Reenviar mensajes de contabilidad de forma transparente al puerto 1813.
    - Prevenir bucles no reenviando peticiones al servidor del que proceden.
    - Ser implementados en parejas: un primario y un secundario. El secundario se utilizará cuando el primero se caiga. Después de un tiempo se debe intentar alcanzar el primario otra vez. El tiempo de espera y los reintentos deben ser ajustados para que sean óptimos.
    - Registrar, al menos, la hora, la fecha, el nombre de usuario, el dominio y la aceptación o denegación de cada petición.
    - (Opcional) La comunicación con un servidor RADIUS nacional puede ser encriptada con SSL o IPSEC para conseguir seguridad adicional.
    - Pueden eliminarse atributos opcionales de mensajes entrantes que sólo tengan relevancia en el contexto del dominio local del visitante.
    - Se necesita contabilizar las pruebas que se realizar sobre los dominios del ORPS.

Es posible conectar directamente ciertos servidores RADIUS de organizaciones cuando están estrechamente relacionados y van a intercambiar muchas peticiones como puede ser el caso de dos organizaciones que se encuentren en el mismo campus y muchos de los empleados de una

organización visiten las instalaciones de la otra.

- Servidores Proxy RADIUS nacionales (NRPS: The National RADIUS Proxy Servers) deben:
  - Reenviar peticiones basadas en un dominio de segundo nivel
  - Todos los atributos RADIUS se deben reenviar de forma transparente para asegurar la trasparencia EAP.
  - Aceptar peticiones que provengan de servidores RADIUS de confianza de mayor nivel y servidores RADIUS de las organizaciones. Por lo tanto, los servidores RADIUS deben intercambiarse sus direcciones IP y se tiene que determinar un RADIUS Secret que se usará entre cada servidor RADIUS Nacional y el servidor RADIUS Europeo de mayor nivel. El puerto será el 1812.
  - Reenviar mensajes de contabilidad de forma transparente al puerto 1813.
  - Prevenir bucles no reenviando peticiones al servidor del que proceden.
  - Ser implementados en parejas: un primario y un secundario. El secundario se utilizará cuando el primero se caiga. Después de un tiempo se debe intentar alcanzar el primario otra vez. El tiempo de espera y los reintentos deben ser ajustados para que sean óptimos.
  - Registrar, al menos, la hora, la fecha, el nombre de usuario, el dominio y la aceptación o denegación de cada petición.
  - (Opcional) La comunicación con un servidor RADIUS nacional puede ser encriptada con SSL o IPSEC para conseguir seguridad adicional.
  - Se necesita contabilizar las pruebas que se realizar sobre los dominios del NRPS.

Se puede tomar la decisión de permitir que el Servidor Proxy RADIUS Nacional se encargue también de subdominios. También es posible añadir cualquier número de subniveles, con su servidor proxy RADIUS correspondiente, por ejemplo a nivel regional.

- El Servidor Proxy RADIUS de mayor nivel (TRPS: The Top level RADIUS Proxy Server) deben:
  - Reenviar peticiones basadas en el dominio de mayor nivel.
  - Todos los atributos RADIUS se deben reenviar de forma transparente para asegurar la trasparencia EAP.
  - Aceptar peticiones que provengan de los Servidores Proxy RADIUS Nacionales. Por lo tanto, los servidores RADIUS deben intercambiarse sus direcciones IP y se tiene que determinar un RADIUS Secret que se usará entre cada Servidor Proxy RADIUS Nacional y el servidor RADIUS Europeo de mayor nivel. El puerto será el 1812.
  - Reenviar mensajes de contabilidad de forma transparente al puerto 1813.
  - Prevenir bucles no reenviando peticiones al servidor del que proceden.
  - Ser implementados en parejas: un primario y un secundario. El secundario se utilizará cuando el primero se caiga. Después de un tiempo se debe intentar alcanzar el primario otra vez. El tiempo de espera y los reintentos deben ser ajustados para que sean óptimos.
  - Registrar, al menos, la hora, la fecha, el nombre de usuario, el dominio y la aceptación o denegación de cada petición.
  - (Opcional) La comunicación entre un servidor RADIUS nacional y el Servidor Proxy RADIUS Europeo de mayor nivel puede ser encriptada con SSL o IPSEC para conseguir seguridad adicional.

Como se ha podido observar esta red proporciona la suficiente seguridad, una solución sencilla de implementar y sobre todo la una forma de desplegar fácilmente una red que permita el roaming entre instituciones tanto nacionales como internacionales.

5. Implementación de Eduroam en la Universidad de Sevilla

La Universidad de Sevilla (US) forma parte de los miembros del proyecto Eduroam (Educational Roaming), cuyo objetivo es tener conectividad y movilidad entre todas las redes inalámbricas mundiales que estén adheridas a él. De esta forma se logrará que los integrantes de la Comunidad Universitaria puedan acceder a la red y a sus servicios de manera transparente.

Podemos poder como ejemplo la posibilidad de que los estudiantes que llegan a la US con un programa de intercambio académico puedan utilizar la red inalámbrica y sus servicios con su usuario y su contraseña de la universidad origen, independientemente de la institución en la que se encuentren, siempre que ésta pertenezca al proyecto Eduroam.

Para poder implementar Eduroam, la Universidad de Sevilla debe cumplir y respetar ciertas reglas que impone el organismo regulador de este proyecto. Por este motivo, la US se responsabiliza de formar a sus usuarios en el respeto a las políticas de uso y ayudarlos en cualquier aspecto relacionado con el acceso a la red. Además de eso, la US tiene mecanismos para informar a los usuarios visitantes sobre las posibilidades del servicio de movilidad.

Con respecto a los equipos, a parte de los puntos de acceso inalámbrico, que son necesarios en cualquier red inalámbrica, Eduroam requiere que la institución posea un servidor de autenticación (NAS) que pueda, de modo seguro, procesar y transmitir las credenciales de los usuarios de la US solicitadas, y para ellos se usan los paquetes Access-Accept de RADIUS (de acuerdo con lo visto en el aparatado de antes).

El SSID es obligatorio que sea “eduroam”, excepto en aquellos casos en los que exista un solapamiento de puntos de acceso de distintas organizaciones físicamente muy cercanas. Los usuarios deben estar informados de los niveles de seguridad ofrecidos por la US en la transmisión de credenciales.

Las sesiones de autenticación y acceso a la red de cada usuario quedan registradas para evitar un uso fraudulento de la red. Si surgen problemas de este tipo, la Universidad de Sevilla tiene que comunicárselo a los responsables de la iniciativa Eduroam en España, para solucionar los problemas de manera coordinada.

La conexión a Eduroam puede ser distinta de una institución miembro a otra. La Universidad de Sevilla tiene informar al usuario con los métodos de conexión que emplea, y cómo puede conectarse con cualquier entorno que utilice.

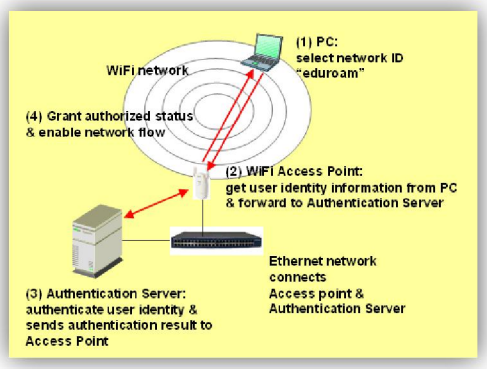


Figura 30: Equipos que intervienen en la conexión a Eduroam

6. Conexión de distintos dispositivos a Eduroam. Pasos teóricos a seguir para conectarlos.

6.1. Introducción:

Para poder conectarse a **Eduroam**, es necesario que tanto la tarjeta inalámbrica de la que se dispone, como su driver, soporten las especificaciones requeridas por la institución de la que se proviene. En general, es necesario que estos elementos cumplan las normas IEEE 802.11a, 802.11b o 802.11g. Además de ser compatible con estas normas, tanto la tarjeta como el sistema operativo del equipo han de ser compatibles con WPA. En el caso de la tarjeta inalámbrica, es posible que sea necesaria la actualización del firmware y/o de los drivers de la misma.

También es necesario ser titular de un usuario virtual de la Universidad de Sevilla (US) o si no pertenece a esta Universidad, tener una cuenta de correo electrónico en cualquiera de las instituciones adheridas a la iniciativa Eduroam. Los usuarios de la Universidad de Sevilla (US) que se desplacen a otras instituciones adheridas a Eduroam, podrán conectarse a la red inalámbrica de dicha institución utilizando las mismas credenciales (usuario virtual y contraseña) que usaban en su universidad de origen. Para la configuración de su conexión deberán comprobar que la institución de destino esté adscrita a la iniciativa Eduroam, qué métodos de conexión están disponibles y como configurarlos.

6.2. Características de la conexión a Eduroam en la US:

SSID	Método de conexión. Requisitos	Seguridad	Configuración y conexión inicial	Siguientes conexiones	Qué se puede hacer
Eduroam	WPA2 802.1X	Seguro	Dependiente del Sistema Operativo	Automáticas	Acceso general a los servicios

El **SSID** (Service Set Identifier) es un código o un nombre que se usa para identificar una determinada red inalámbrica (WiFi). El SSID de la red inalámbrica de la Universidad de Sevilla es “eduroam”. Por razones de seguridad, es recomendable que en el ámbito de la Universidad de Sevilla se acceda a la red ReInUS mediante el uso del SSID Eduroam, rechazando cualquier otro que le pueda aparecer. Una de las tácticas más comúnmente usada para la obtención fraudulenta de los datos de los usuarios es la creación de SSIDs falsos, de tal forma que cuando se utilizan, un intruso o posible atacante puede captar toda la información que aquellos envían a través de la red inalámbrica, incluyendo datos tan sensibles como los de inicio de sesión, números de tarjetas de crédito o contraseñas.
En cuanto a la seguridad de ReInUS podemos indicar que en esta conexión se utilizan los estándares disponibles para las redes WiFi en lo referente a autenticación y cifrado. En concreto se utiliza **WPA2** (*WiFi Protected Access*) en su modalidad *Enterprise* con el método de autenticación **802.1X (EAP-TTLS)** y cifrado **AES,** de los cuales hemos tratado en apartados anteriores de este documento.

Tenemos que mencionar que anteriormente en ReInUS, el SSID eduroam usaba como método de autenticación WPA y como método de cifrado TKIP. Con el descubrimiento de las debilidades que tienen WPA y TKIP, se ha añadido al SSID Eduroam WPA2 y el cifrado AES. Por lo tanto cada dispositivo puede usar tanto WPA2 como WPA y AES o TKIP, en función de la disponibilidad o de las posibilidades que soporta el Sistema Operativo de cada dispositivo.

Configurando estos parámetros en un perfil con SSID eduroam, e instalando el certificado de seguridad de la universidad, ya se estaría en disposición de conectarse a eduroam introduciendo las credenciales. Hay que tener en cuenta que el usuario es la cuenta de correo completa, incluyendo el dominio (@us.es).

Cabe destacar que sólo es necesario configurar el equipo la primera vez que un usuario se conecta desde él, para las posteriores conexiones la configuración quedará guardada y solo deberá indicar el usuario y clave. La conexión será automática y prácticamente no tiene limitaciones, se puede navegar, consultar el correo, chatear, descargar ficheros por FTP, acceder a otros servidores mediante SSH, etc.

A continuación vamos a detallar los pasos teóricos para conectarse a la red inalámbrica de la Universidad de Sevilla utilizando distintos dispositivos (ordenador, móvil, PDA, etc.) con entornos diferentes (Windows, MacOS, Linux, etc.). Estos pasos teóricos sirven de guía para la parte práctica, donde, usando las conexiones de los distintos dispositivos vamos a analizar los debilidades de cada de uno desde el punto de vista de la seguridad, comparándolos entre sí.

a) Configuración de un ordenador con Windows 7:

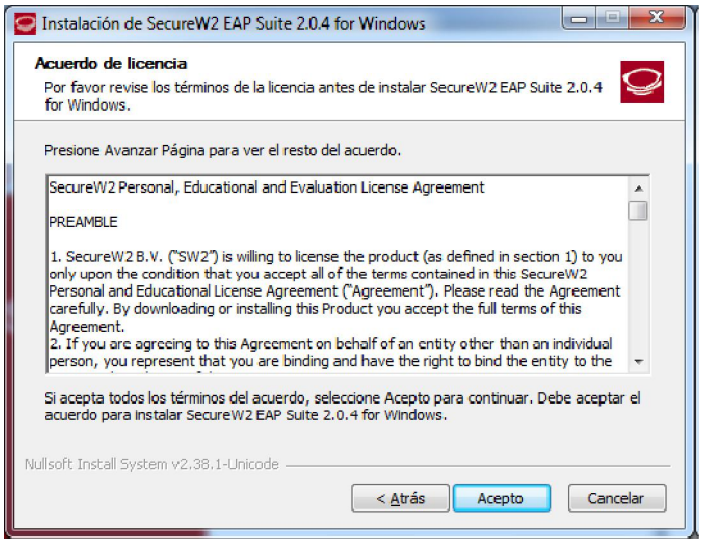
Windows 7 es la versión más reciente de Microsoft Windows. Esta versión está diseñada para su uso en PC, equipos portátiles, tablet PC, netbooks y equipos *media center*. Hoy en día muchos de los ordenadores que hay en el mercado traen instalado este sistema operativo Windows. Por eso, vamos a comenzar describiendo los pasos teóricos de la configuración de Windows 7 para poder acceder a la red inalámbrica Eduroam de la Universidad de Sevilla.

Paso 1: Instalar el cliente de autenticación.

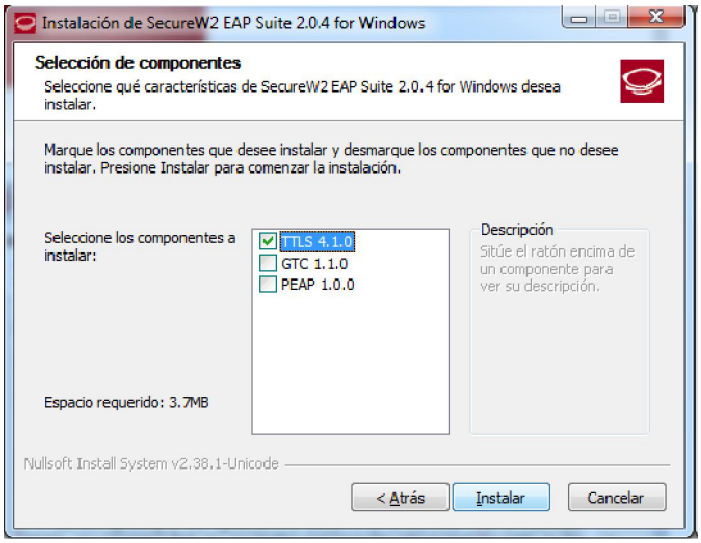
Puesto que la autenticación requiere una interacción con el usuario, es necesario que el dispositivo que desee autenticarse tenga el software para comunicarse con el servidor de autenticación. Debido a que Windows no admite de forma nativa el estándar de protocolo EAP-TTLS, los usuarios deben instalar un software en su ordenador para poder autenticarse mediante 802.1X. Este software, gratuito, llamado SecureW2 (del que podemos encontrar distintas versiones para distintos sistemas operativos en la web del fabricante http://www.securew2.com) permite la gestión de la verificación del certificado proporcionado por el servidor (con los certificados emitidos por la autoridad de certificación), para pedir al usuario que introduzca su nombre de usuario / contraseña. Una vez hecho esto, se encarga de crear el túnel entre el servidor Radius y el ordenador del cliente y enviar la contraseña.

Descargamos e instalamos el programa cliente de autenticación SecureW2 para Windows 7:

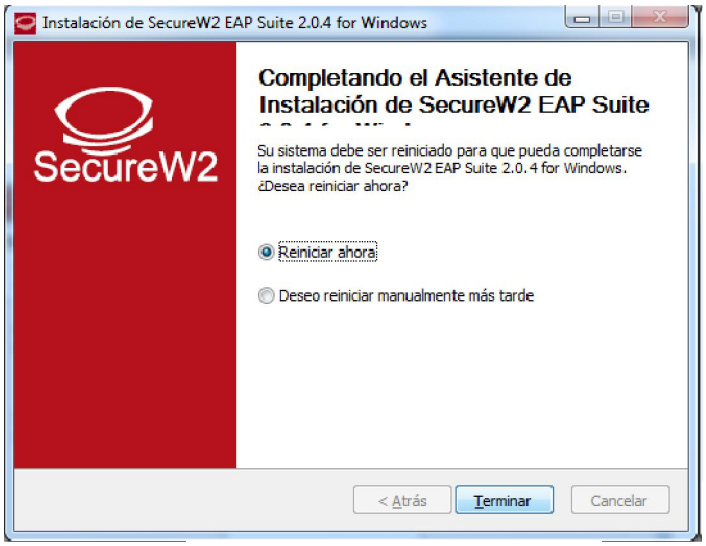
1



2



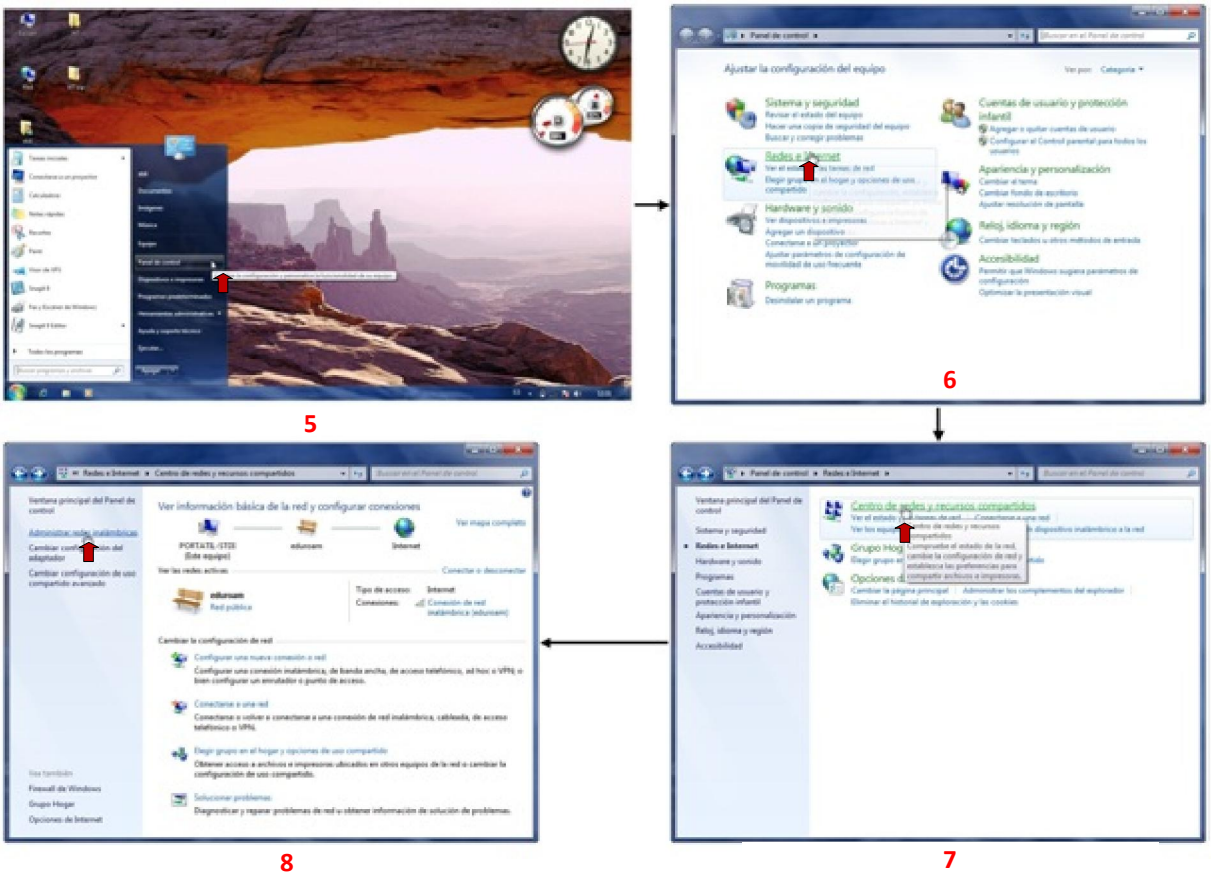
3



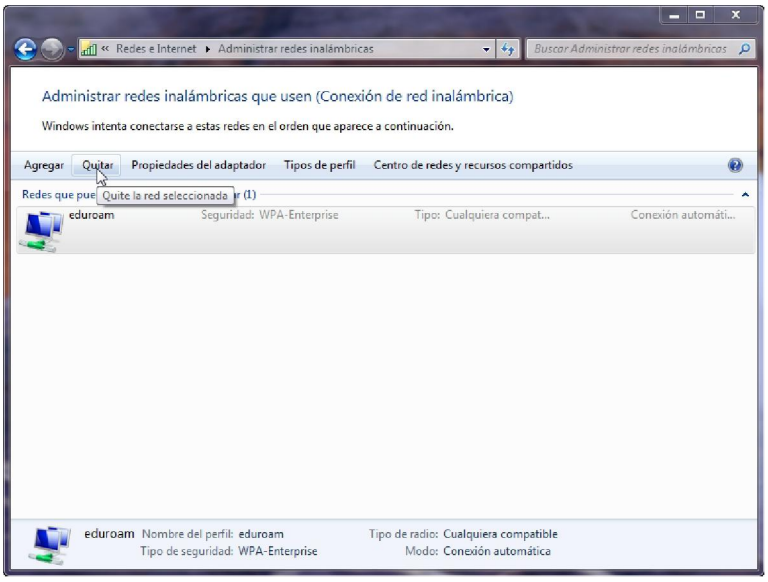
4

Paso 2: Abrir la ventana desde la que se administran las redes inalámbricas.

Tenemos que seguir los siguientes pasos: Inicio→ Panel de control→ Redes e Internet→ Centro de redes y recursos compartidos → (panel izquierdo) Administrar redes inalámbricas.



Paso 3: Eliminar el perfil definido para eduroam en el caso de que exista.



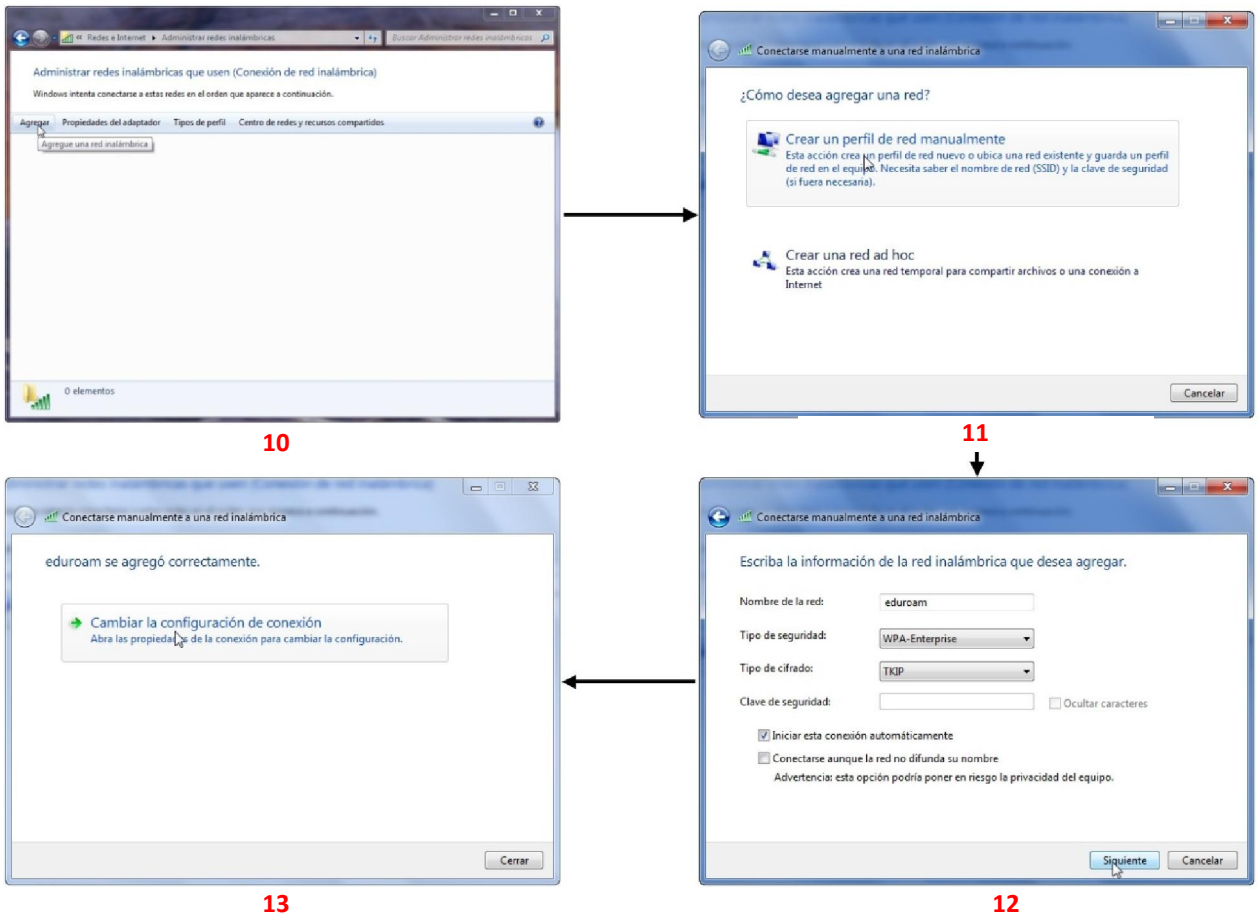
9

Paso 4: Agregar eduroam como una nueva red inalámbrica y editar sus propiedades.

Tenemos que elegir los siguientes parámetros:

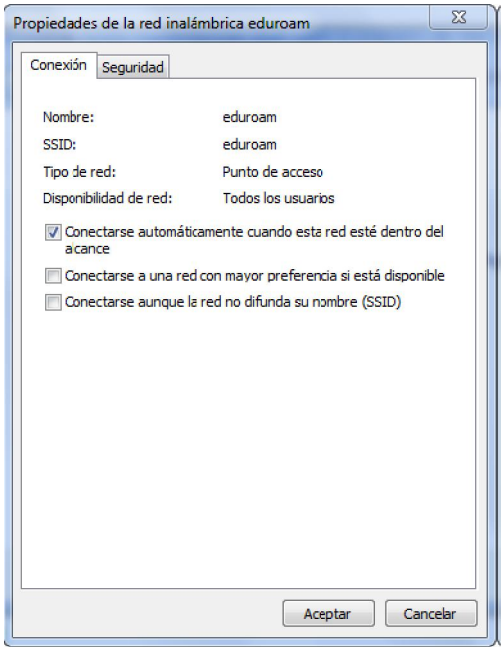
- Nombre de la red: eduroam
- Tipo de seguridad: WPAEnterprise
- Tipo de cifrado: TKIP

- Activar: Iniciar esta conexión automáticamente



Paso 5: Configurar las propiedades de conexión de la red inalámbrica eduroam.

Activar: Conectarse automáticamente cuando esta red esté dentro del alcance.
Desactivar: el resto de opciones.



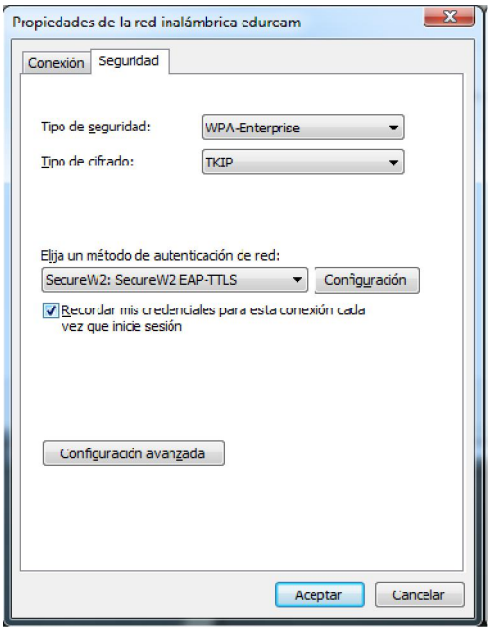
14

Paso 6: Configurar las propiedades de seguridad de la red inalámbrica eduroam.

En la pestaña “Seguridad” de “Propiedades de la red inalámbrica eduroam” seleccionaremos:

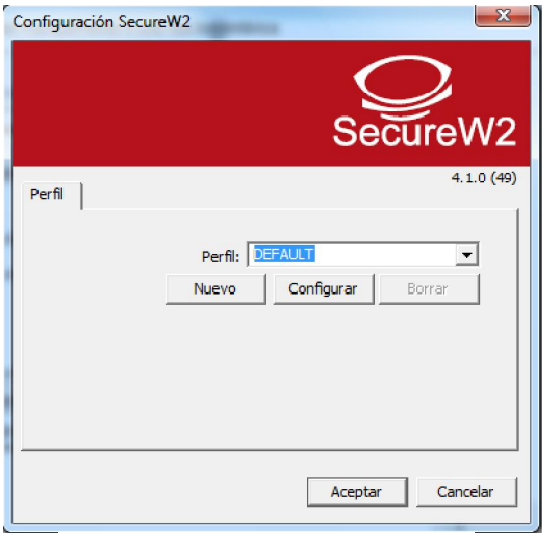
- Tipo de seguridad: WPAEnterprise
- Tipo de cifrado: TKIP
- Método de autenticación: “SecureW2: SecureW2 EAP-TTLS”
- Activar: Recordar mis credenciales para esta conexión cada vez que inicie sesión.

Pulsamos en el botón “Configuración” para configurar el programa SecureW2.



15

Nos aparecerá el cuadro de diálogo de configuración del cliente SecureW2. Podemos crear diferentes perfiles con distintas configuraciones o usar el perfil por omisión DEFAULT. En este caso pulsamos en el botón “Configurar”. En la pestaña Conexión, podemos usar una Identidad Externa “anónima” (Use alternate outer identity).



16

17

En la pestaña “Certificados” nos aseguramos de que NO está marcada la opción “Comprobar certificado de servidor (Verify server certificate)”. En la pestaña “Autenticación (Autentication)”, en la opción Método de Autenticación (Select Authentication Method), seleccionamos la opción PAP.

18

19

En la pestaña Cuenta de Usuario (User Account) tenemos dos opciones:

1. Si activamos la opción “Pedir credenciales de usuario (Prompt user for credentials)”, cada vez que se intente conectar al SSID "eduroam" se solicitará el nombre y la clave de usuario virtual de la Universidad de Sevilla. En el caso de un usuario que no pertenezca a la Universidad de Sevilla, tendrá que introducir las claves de su universidad.
2. Si no activamos la opción “Pedir credenciales de usuario”, escribimos en Usuario y Contraseña (Username y Password) el nombre y clave de usuario. Cuando se conecte a esta red se usará ese nombre de usuario y clave para acceder a ella. De igual forma, si el usuario no pertenece a la Universidad de Sevilla, tendrá que introducir sus claves de la universidad u organización a la que pertenece.

Es conveniente que el nombre de usuario sea el que se utiliza en la Universidad de Sevilla seguido de la especificación del dominio detrás de la arroba “@”: Por ejemplo e12345678x@us.es según proceda, de este modo, no se tendrá que añadir el dominio cuando esté en otra institución adherida al programa EDUROAM.

Por último vamos a comentar en qué consiste la configuración de SecureW2: Tras pulsar el botón Avanzado marcamos la casilla de verificación correspondiente a la opción: “Allow users to setup new connections” para permitir configurar otras conexiones.

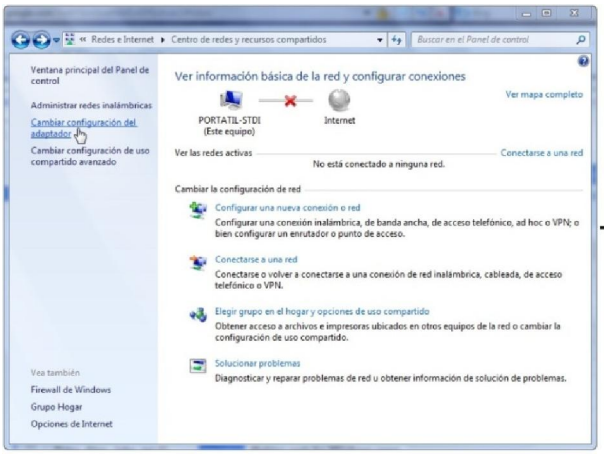
20

21

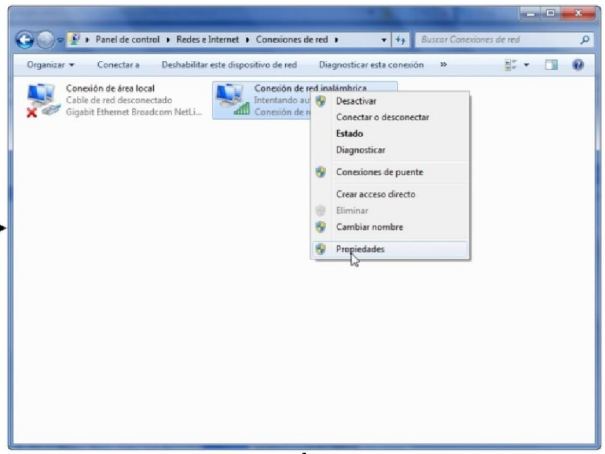
Paso 6: Habilitar la obtención de IP y DNS automáticos para la conexión inalámbrica.

Sobre el icono de la conexión de red inalámbrica pulsamos el botón derecho y seleccionamos "Propiedades". En la pestaña "Funciones de red" de "Propiedades de Conexión de red inalámbrica" seleccionamos "Protocolo de Internet versión 4 (TCP/IPv4)" y editamos sus propiedades.

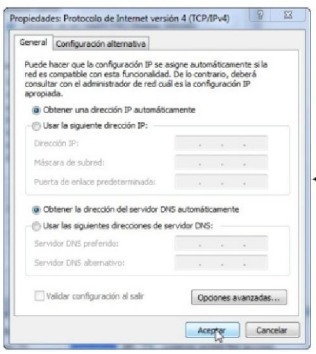
En la pestaña "General" de "Propiedades Protocolo de Internet versión 4 (TCP/IPv4)" activamos "Obtener una dirección IP automáticamente" así como "Obtener la dirección del servidor DNS automáticamente".



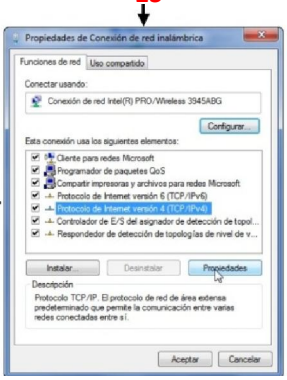
22



23



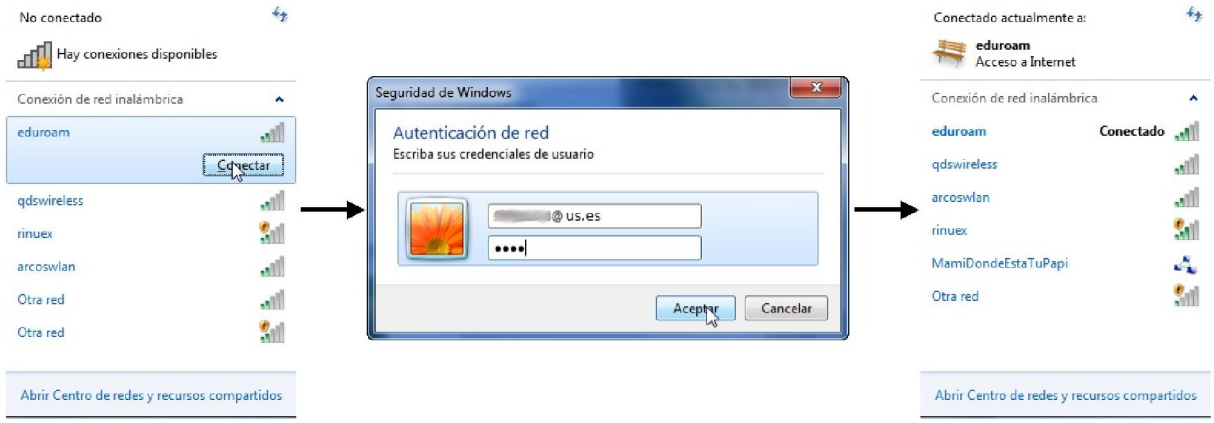
25



24

Paso 8: Conexión a eduroam.

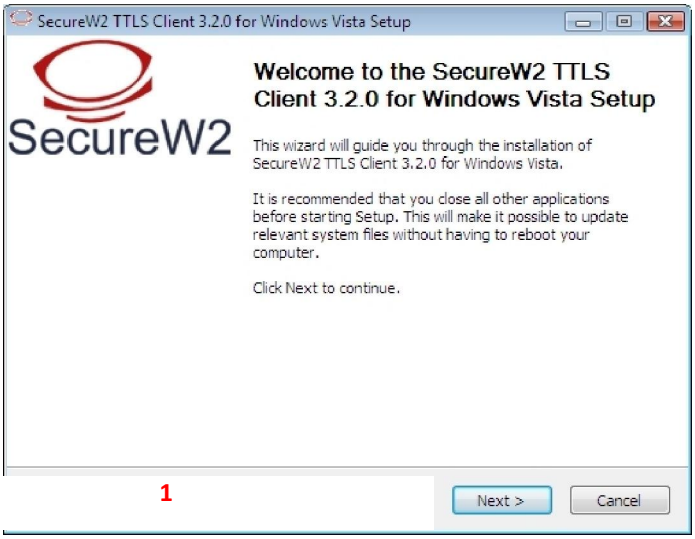
Una vez que hemos configurado la conexión ya podemos conectarnos a eduroam.

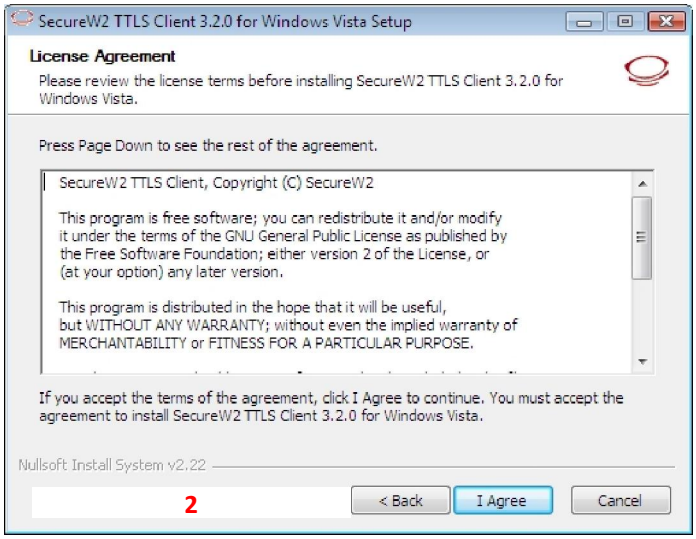


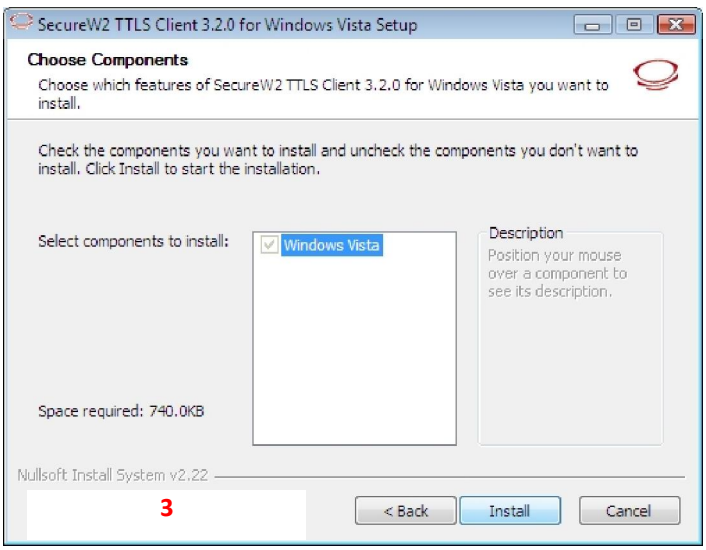
b) Configuración de un ordenador con Windows Vista:

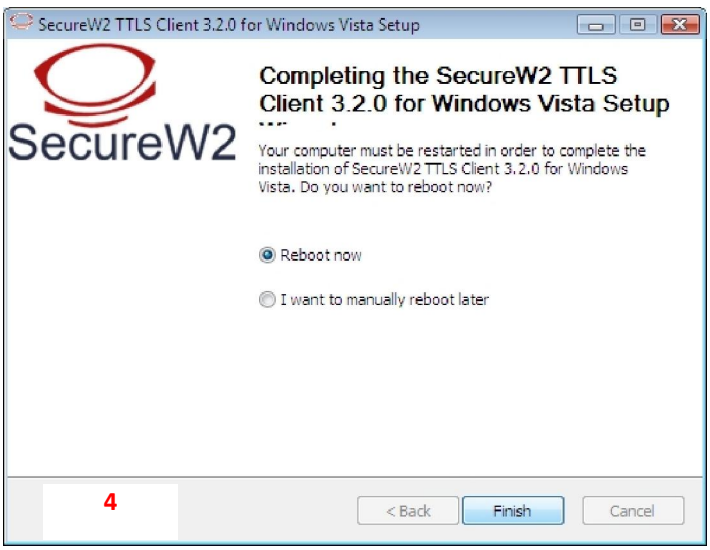
Paso 1: Instalar el cliente de autenticación.

El programa se instala en el ordenador siguiendo los pasos siguientes:



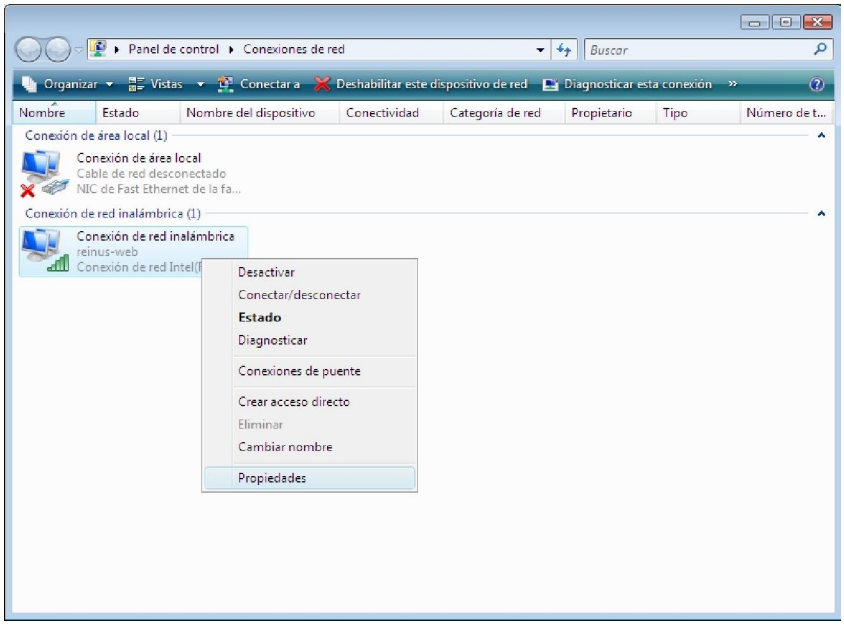




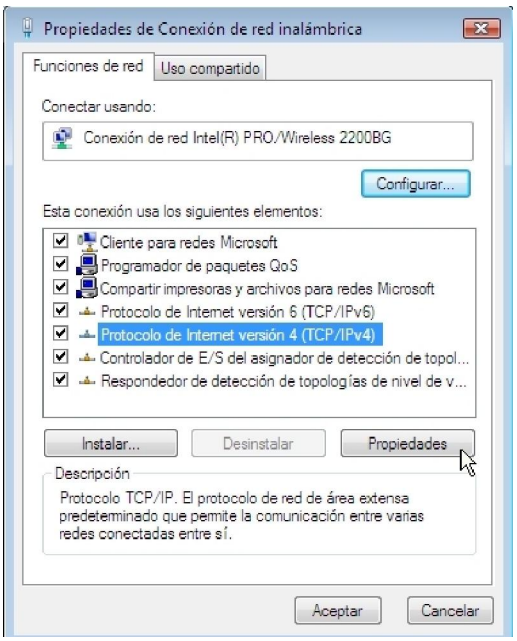


Paso 2: Configuración del protocolo TCP/IP.

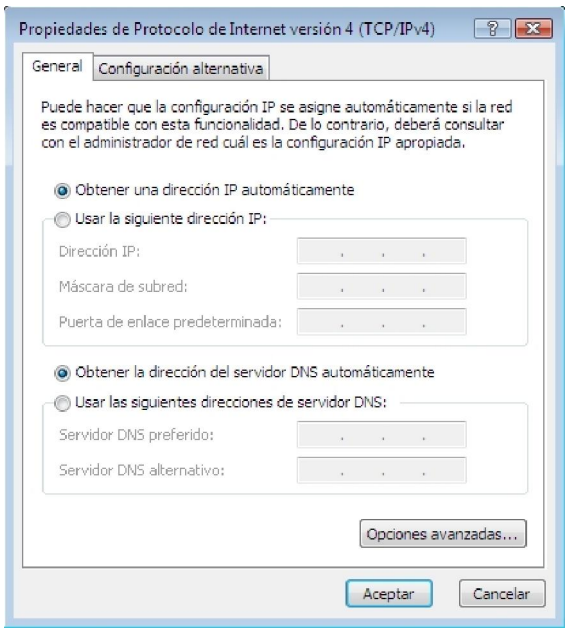
Ahora tenemos que configurar el protocolo TCP/IP. Pulsamos el botón 'Inicio' -> opción 'Panel de Control' -> opción "Administrar conexiones de red" -> pulsamos con el botón derecho del ratón sobre "Conexión de red inalámbrica" y seleccionamos "Propiedades". Debemos asegurarnos de que **NO tiene forzada una dirección IP fija** en la interfaz de red inalámbrica, sino que la IP se obtendrá dinámicamente por *DHCP*. Para ello: En la pestaña "Funciones de red" pulsamos sobre la opción "Protocolo de Internet versión 4 (TCP/IPv4)" y a continuación pulsamos en el botón de "Propiedades". En el nuevo cuadro de diálogo "Propiedades de Protocolo de Internet versión 4 (TCP/IPv4)" en la pestaña "General", nos aseguremos de que están marcadas las opciones "Obtener una dirección IP automáticamente" y "Obtener la dirección del servidor DNS automáticamente" y pulsamos el botón "Aceptar". Ya está terminada la configuración de TCP/IP.



5



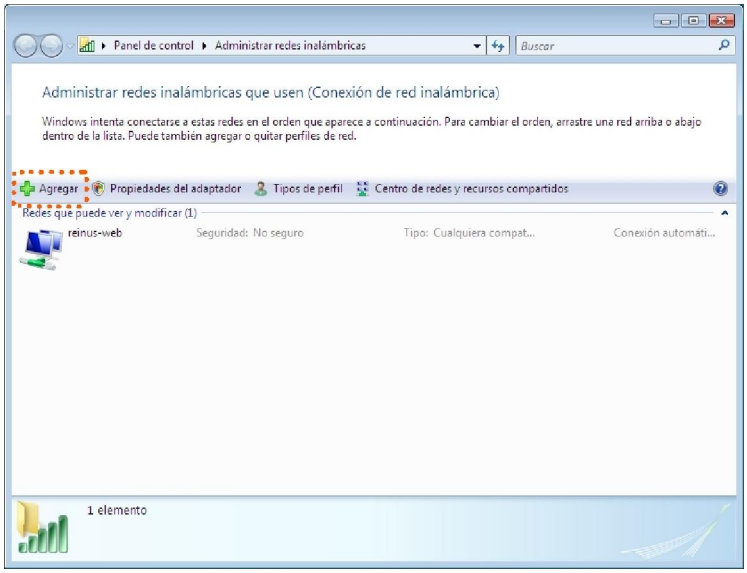
6



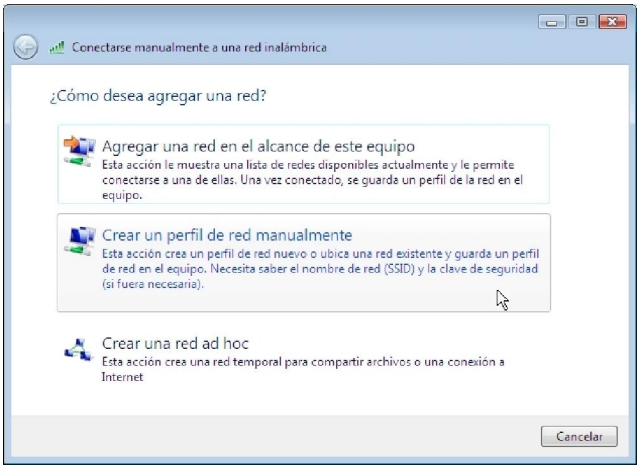
7

Paso 3: Configuración Inalámbrica**.**

Antes de comenzar la configuración inalámbrica tenemos que crear, si no está hecho, una nueva conexión con el nombre de eduroam. Para ello pulsamos el botón 'Inicio' -> opción 'Panel de Control' -> icono "Centro de redes y recursos compartidos", pulsamos en la opción "Administrar redes inalámbricas" y después “Agregar”. Vamos a crear un perfil de red manualmente.

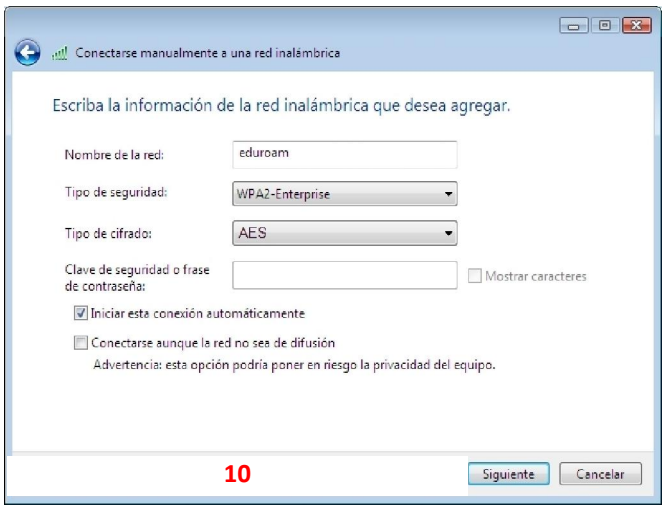


8

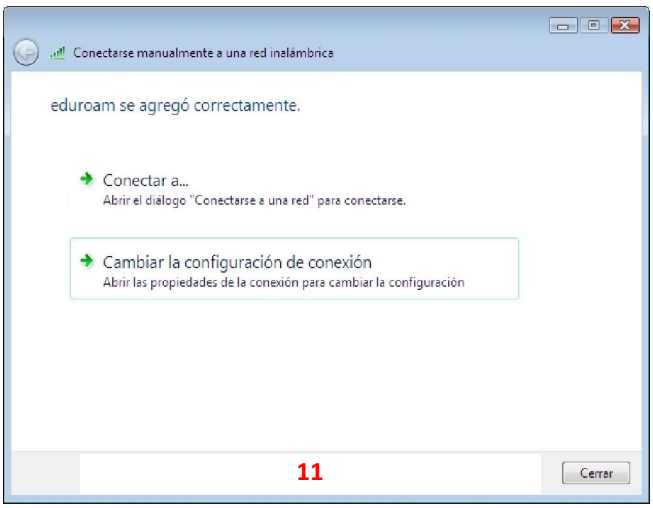


9

En el nuevo cuadro de diálogo "Conectarse manualmente a una red inalámbrica", en el campo "Nombre de la red" escribimos "eduroam". En "Tipo de seguridad" seleccionamos "WPA2-Enterprise" y en "Tipo de cifrado" seleccionamos "AES" y pulsamos el botón "Siguiente". Si no aparece la opción de WPA2 o WPA en "Tipo de seguridad" es porque la tarjeta de red o el driver de la misma no soporta dicho protocolo. Actualizamos si es posible el software de la tarjeta de red. Si no es posible, no podremos utilizar el SSID eduroam y no podremos usar ReInUS. Pulsamos siguiente y en el nuevo cuadro de diálogo, pulsamos en "Cambiar la configuración de conexión".



10

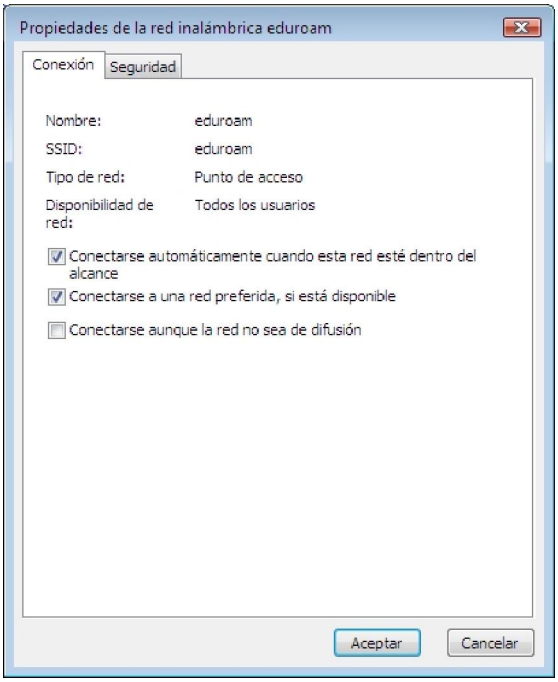


11

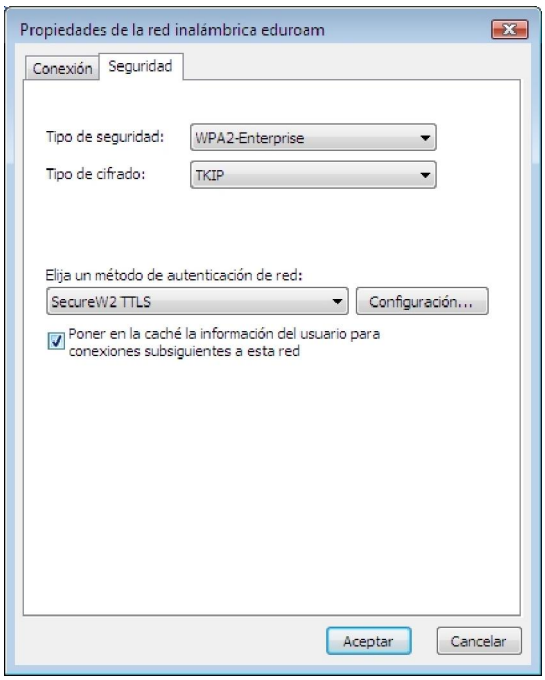
Para configurar el cliente SecureW2, pulsamos en la pestaña 'Seguridad'. En el campo "Elija un método de autenticación de red" seleccionamos "SecureW2 TTLS" y pulsamos en el botón de "Configuración". Podemos crear distintos perfiles (*profiles*) con distintas configuraciones o usar el perfil por omisión (*default*).

En este caso pulsamos en el botón "Configure". Para aumentar la seguridad en el acceso al SSID eduroam, marcamos "Verify Server certificate" y pulsamos el botón "Add CA" y en la ventana que se nos presenta, seleccionamos **"FNMT Clase 2 CA"** y pulsamos el botón "Add". A continuación, marcamos "Verify Server name" e introduzcamos "US.ES" **(en MAYUSCULAS, es IMPORTANTE)**.

De esta forma, cada vez que accedamos a eduroam, se comprobará que los certificados de los servidores de Autentificación están firmados por la Autoridad de Certificación (CA) que indicamos.

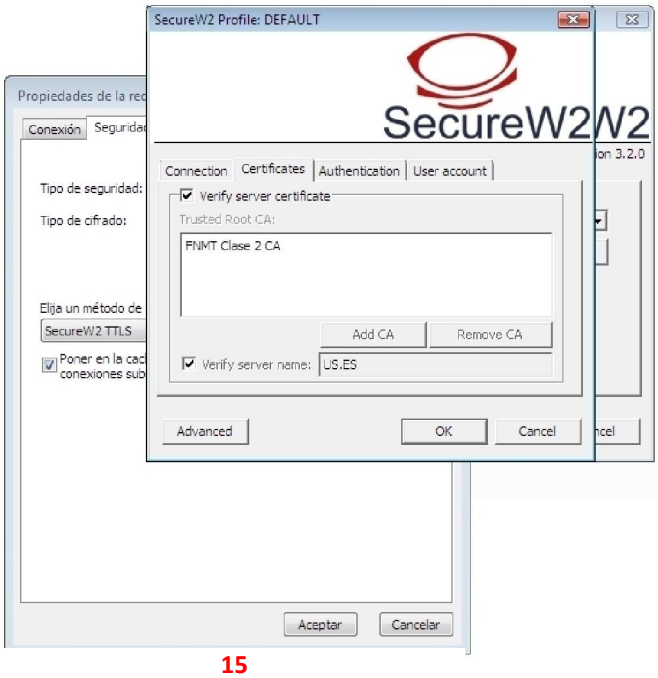


12



13

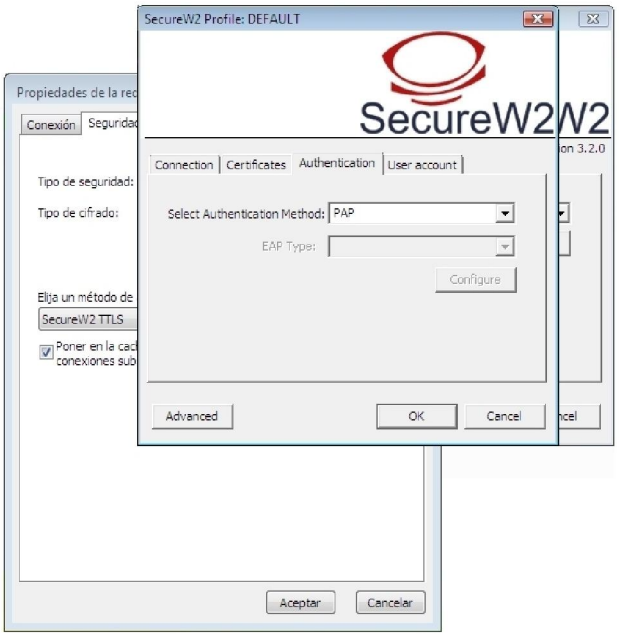
14



15

En la pestaña "Authentication", en la opción "Select Authentication Method", seleccionamos la opción "PAP". En la pestaña "User account" tenemos dos opciones:

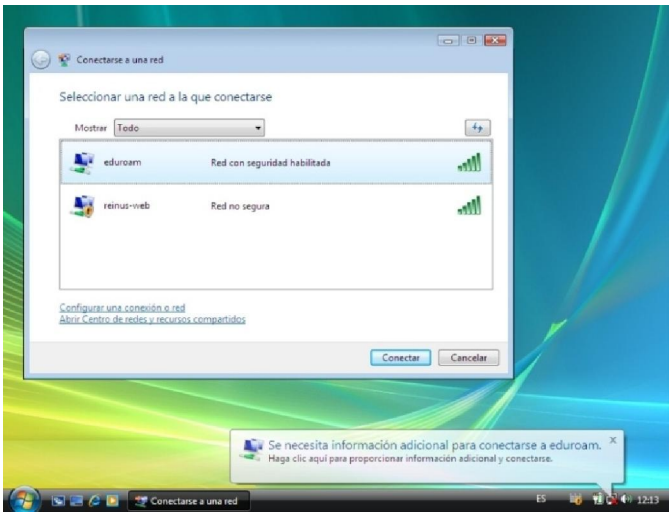
- Si activamos la opción "Prompt user for credentials", cada vez que se intentamos conectarnos al SSID "eduroam" se solicitará el nombre y la clave del usuario virtual de la US (incluyendo @us.es). Si el usuario no pertenece a la Universidad de Sevilla, tendrá que introducir su correo electrónico (incluyendo @ y el dominio de la organización a la que pertenece).
- Si no activamos la opción "Prompt user for credentials", escribimos en "Username" y "Password" el nombre del usuario y la clave del usuario virtual de la US (incluyendo @us.es). Cuando se conecte a esta red se usará este nombre de usuario y clave para acceder a ella.



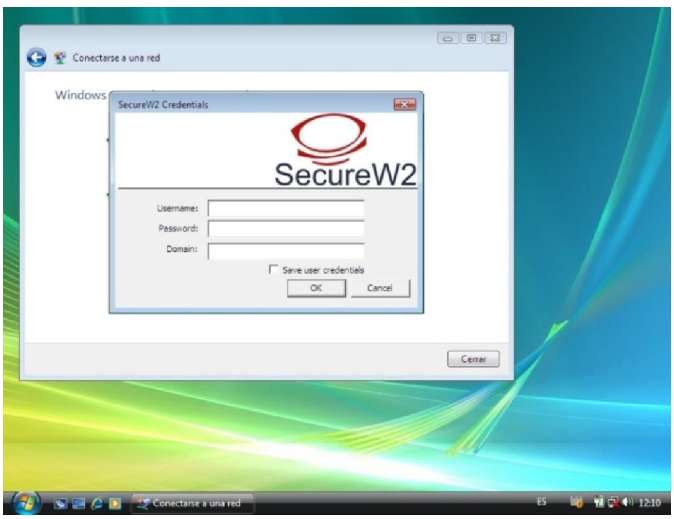
16

17

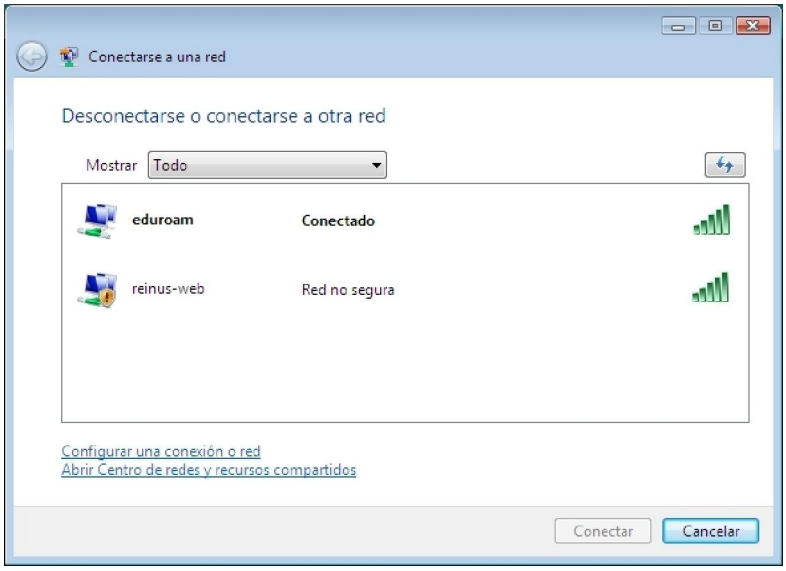
Pulsamos el botón "OK" y habremos terminado de configurar el cliente SecureW2. Ahora, una vez configurada la red inalámbrica, pulsamos en la opción "Conectar a...". Veremos como en la lista de redes aparece la red "eduroam". La marcamos y pulsamos en botón "Conectar". Aparecerá un mensaje en la barra de tareas, indicando que tenemos que proporcionar información adicional para conectarnos a eduroam. Pulsamos en el mensaje e introducimos el nombre y clave del usuario virtual de la US (incluyendo @us.es). Si el usuario no pertenece a la Universidad de Sevilla, tendrá que introducir su correo electrónico (incluyendo @ y el dominio de la organización a la que pertenece).



18



19



20

c) *Configuración de un ordenador con Windows XP:*

Los ordenadores que tienen el sistema operativo Windows XP se configuran de la misma manera que los que utilizan Windows Vista. Lo único que cambia es la versión del programa SecureW2, que tiene que ser una versión que se adapte a este sistema operativo. Los pasos a seguir son los mismos.

d) *Configuración de un ordenador con Linux:*

Paso 1: Comprobar que nuestra tarjeta de red y el driver de la tarjeta de red soportan WPA2 y 802.1X.

Esto depende del fabricante y del modelo. Puede que se necesite actualizar la tarjeta con un programa del fabricante para que soporte dichos protocolos. Si no se dispone de WPA/WPA2 o de 802.1X, no se puede utilizar el SSID eduroam y no se puede usar ReInUS.

Paso 2: Distintas distribuciones de Linux.

El soporte de WPA/WPA2 y 802.1X en Linux se realiza mediante el programa ***wpa_supplicant***. Hay distribuciones que ya llevan incorporado este programa, como por ejemplo, las últimas distribuciones de Suse en la herramienta del sistema Yast. En el buscador *rpmfind* se pueden encontrar paquetes precompilados de *wpa_supplicant* para algunas de las distribuciones más populares. Si no dispone del paquete precompilado wpa_supplicant, se recomienda seguir los pasos que siguen.

Paso 3: Configuración del protocolo TCP/IP.

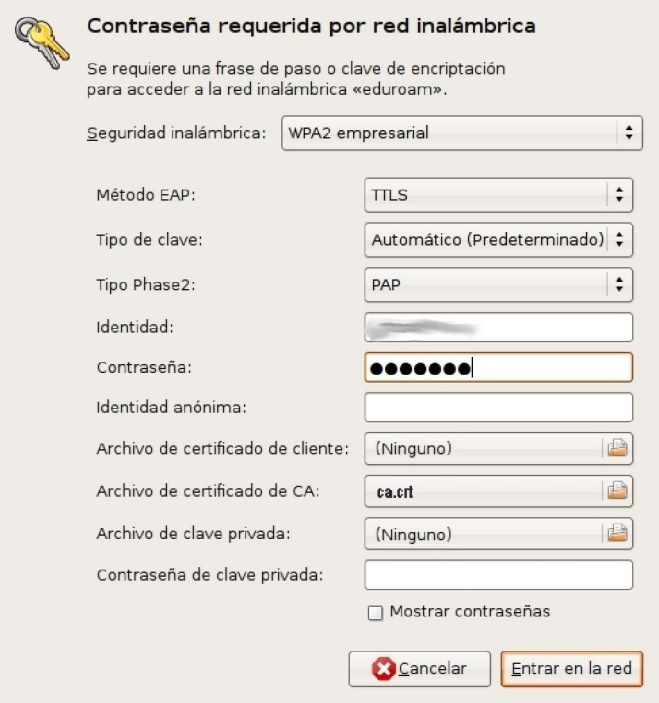
Es importante asegurarse de que no se tiene forzada una dirección IP fija en la interfaz de red inalámbrica, sino que se obtendrá dinámicamente por DHCP.

Paso 4: Configuración Inalámbrica.

Se puede descargar el programa *wpa_supplicant* desde la página oficial http://hostap.epitest.fi/wpa_supplicant/.

Si la distribución dispone del administrador de red Network Manager tenemos que seguir las siguientes instrucciones. Si no dispone de él, pasamos directamente al punto 2 de las siguientes instrucciones.

1. Pulsamos en el icono del administrador de red Network Manager y seleccionamos la red eduroam. Aparecerá la siguiente ventana de configuración:



Completamos lo campos con la siguiente información:

- Seguridad inalámbrica: WPA empresarial.
- Método EAP: TTLS
- Tipo de clave: Automático (predeterminado).
- Tipo de Phase2: PAP
- Identidad: el usuario (que no se olvide @...)
- Contraseña: la contraseña del usuario
- Para aumentar la seguridad en el acceso al SSID eduroam, tenemos que descargar y guardar el *Certificado de la Autoridad de certificación FNMT* que se encuentra en pagina web de la Universidad y seleccionamos el fichero de certificado en el campo "Archivo de certificado de CA". De esta forma, cada vez que accedamos a eduroam, se comprobará que los certificados de los servidores de autentificación están firmados por la Autoridad de Certificación (CA).

Pulsamos el botón "Entrar en la red".

Si de esta forma no consigue conectar a eduroam, puede que *Network Manager* no funcione correctamente con **wpa_supplicant**, por lo que debemos configurarlo manualmente siguiendo los siguientes pasos:

2. Configuramos la tarjeta de red inalámbrica para que use el *wpa_supplicant*. Para ello, añadimos en el fichero de configuración de la tarjeta de red inalámbrica la siguiente línea (el fichero depende de la distribución, por ejemplo en una distribución tipo RedHat sería en `/etc/sysconfig/network-script/[nombre_de_la_interfaz_inalámbrica]` o en una distribución tipo Debian sería en `/etc/network/interfaces`):

```
WIRELESS_WPA_CONF=/etc/wpa_supplicant.conf
```

3. Configuramos el cliente *wpa_supplicant* editando el fichero de configuración. Dependiendo de la distribución, habremos instalado el *wpa_supplicant* como paquete o lo habremos compilado, por lo que la ruta del fichero puede diferir (por ejemplo: `/etc/wpa_supplicant.conf` o `/etc/wpa_supplicant/wpa_supplicant.conf`).

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=wheel
eapol_version=1
ap_scan=1
fast_reauth=1
network={
        ssid="eduroam"
        scan_ssid=1
        key_mgmt=WPA2-EAP
        proto=WPA
        eap=TTLS
        pairwise=CCMP AES
        identity="usuario@us.es"        # <- usuario
        password="xxxxxx"               # <- clave
        priority=2
        phase2="auth=PAP"
        }
```

En las variables '*identity*' y '*password*' debemos introducir el nombre de usuario y la clave del usuario virtual de la US (incluyendo @us.es). Si no pertenecemos a la Universidad de Sevilla, tendremos que introducir nuestro correo electrónico (incluyendo @ y el dominio de la organización a la que pertenecemos).
Configuramos el usuario propietario del fichero y los modos de acceso con los permisos adecuados para que solo sea visible por el usurario, ya que en el mismo aparece su clave. Por ejemplo:

```
chmod 600 /etc/wpa_supplicant.conf
chown root:root /etc/wpa_supplicant.conf
```

4. Iniciamos el *wpa_suplicant* con el comando:

```
wpa_supplicant -i eth1 -D wext -c /etc/wpa_supplicant.conf
```

donde " *-i eth1"* es la interfaz wireless del sistema (en este ejemplo la interfaz eth1), *"-D wext"* es el tipo de *driver* de la tarjeta y *"-c /etc/wpa_supplicant.conf"* es la localización del fichero de configuración del *wpa_supplicant*.

De este modo queda configurada la conexión a la red inalámbrica de la Universidad de Sevilla. En algunos casos, el sistema se conecta a la red inalámbrica eduroam pero no es capaz de obtener una dirección IP por DHCP. En este caso, tenemos que utilizar los siguientes comandos para conectarse y desconectarse a eduroam:

conexión:
```
wpa_supplicant -w -i eth1 -D wext -c /etc/wpa_supplicant.conf -B -w;
ifup eth1
```

desconexión: `ifdown eth1; killall -9 wpa_supplicant`

e) Configuración de un ordenador con Mac OS X:

En este apartado vamos a presentar dos configuraciones para el sistema operativo Mac OS X, en concreto para dos de entre las distintas versiones de este sistema: Mac OS X 10.3 (Panther) y Mac OS X v10.5 (Leopard).

e1) Configuración en Mac OS X Panther:

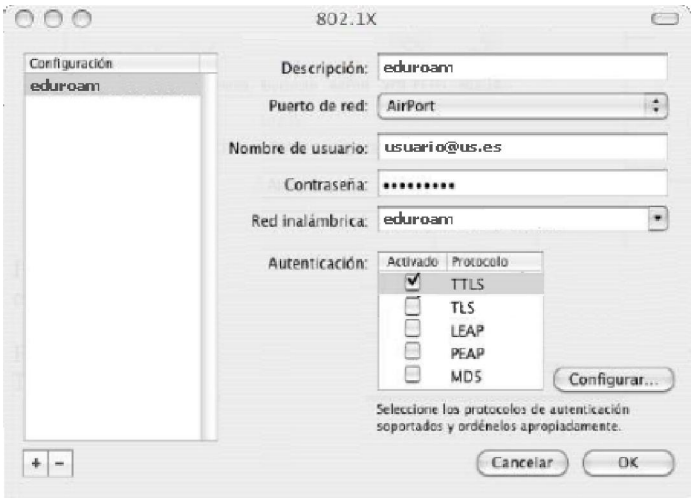
Accedemos a 'Aplicaciones' -> "Conexión a Internet" y pulsamos en el icono '802.1X'. En 'Configuración' pulsamos en "Configuración de 802.1X" y seleccionamos 'Editar configuraciones'.

1

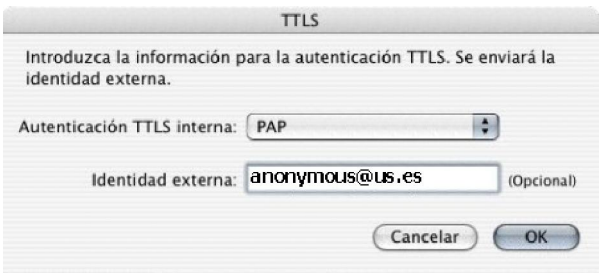
2

Completamos la información que se solicita de la siguiente manera, recordando que como "Nombre de usuario" y "Contraseña" se debe introducir el nombre y la clave del usuario virtual de la US (incluyendo @...). Si el usuario no pertenece a la Universidad de Sevilla pero pertenece a una organización que forma parte del programa eduroam, tendremos que introducir el correo electrónico incluyendo el dominio de esa organización.

En 'Autenticación' seleccionamos el método de autenticación 'TTLS' y pulsamos el botón 'Configurar'. Completamos la información que se solicita de la siguiente manera:

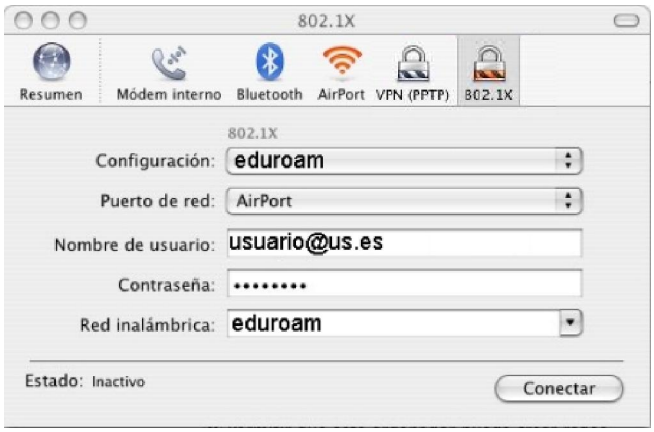


3



4

Una vez que se tenga creada la configuración para el SSID eduroam podemos probarla pulsando en el botón 'Conectar'. Al conectar por primera vez se debe verificar el certificado del servidor RADIUS que es el encargado de comprobar si el nombre de usuario y contraseña son correctos. Para ello, pulsamos el botón "Aceptar todo" en la ventana que aparece.



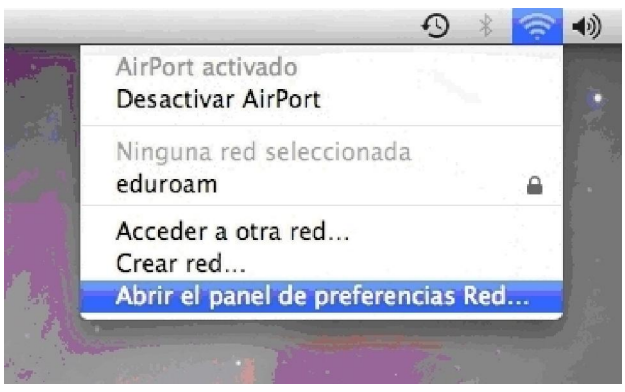
5

6

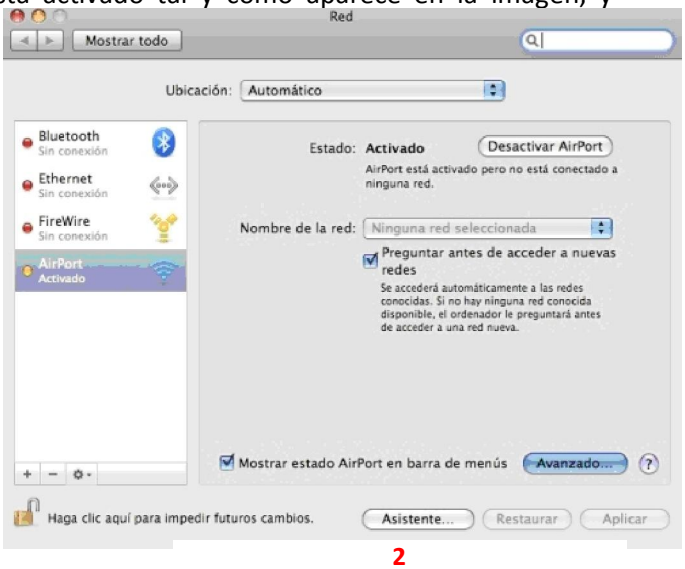
Dado que la Universidad de Sevilla dispone de dos servidores Radius, si el principal no estuviera disponible respondería el secundario "radius2.us.es", por lo que podría aparecer un mensaje similar para el servidor "radius2.us.es".

e2) Configuración en Mac OS X Leopard:

Para configurar eduroam en un Sistema Operativo MacOS Leopard: en primer lugar tenemos que pulsar en el icono AirPort en la esquina superior derecha de la pantalla y seleccionar 'abrir el panel de preferencias Red'. Comprobamos que AirPort está activado tal y como aparece en la imagen, y pulsamos en el botón 'Avanzado'.

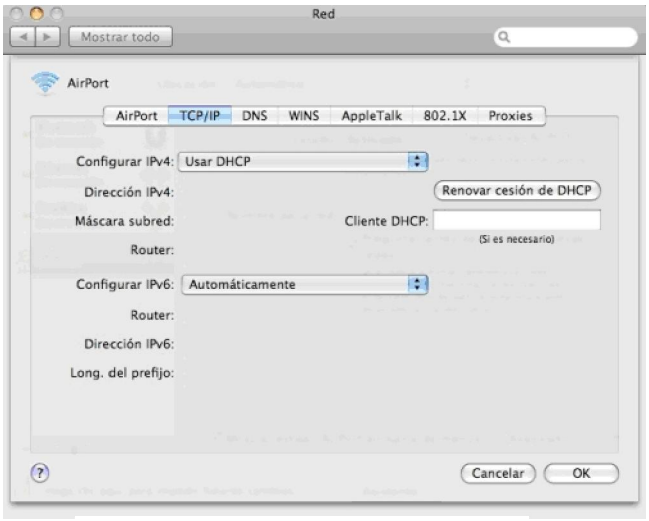


1

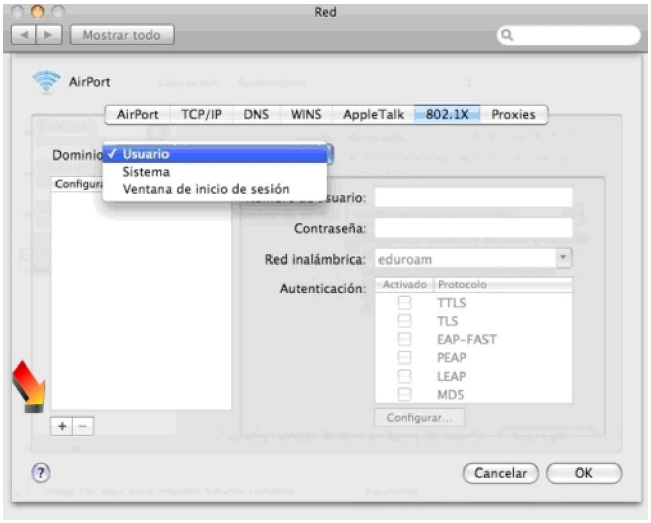


2

Seleccionamos la pestaña 'TCP/IP' y comprobamos que en la opción "configurar IPv4" aparece seleccionado "usar DHCP". Seleccionamos otra vez la pestaña '802.1X' y marcamos en 'Dominio' la opción 'Usuario'. Pulsamos en el botón '+' que aparece en la esquina inferior izquierda de la ventana, y añadimos una nueva configuración con el nombre 'eduroam'. Introducimos el nombre de usuario y contraseña.

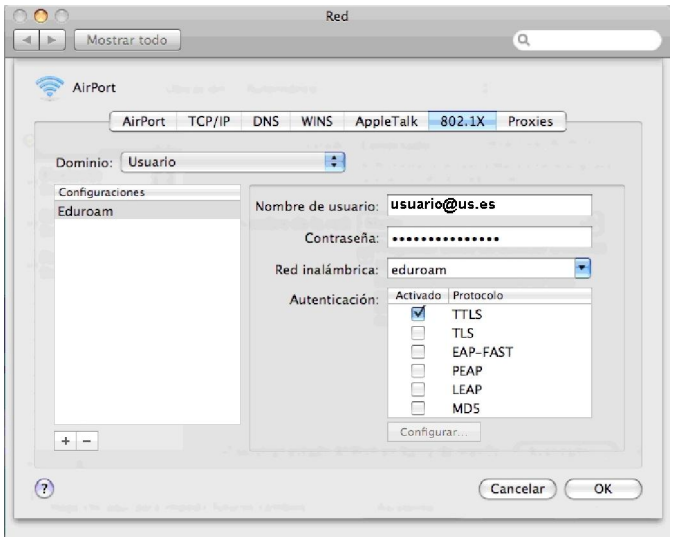


3

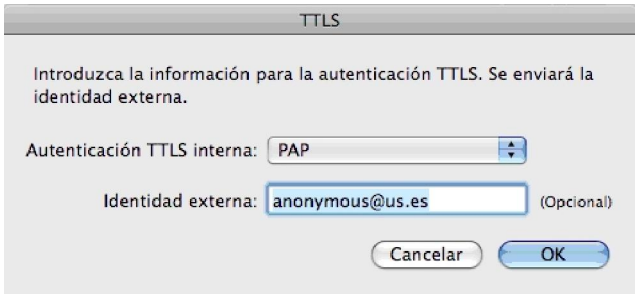


4

En "Red inalámbrica" seleccionamos “eduroam”, en “Autenticación” marcamos exclusivamente 'TTLS' y pulsamos el botón “Configurar...”. En la nueva ventana, seleccionamos como "Autenticación TTLS interna" la opción 'PAP', y si se desea, se puede escribir "anonymous@us.es" en el cuadro "Identidad externa". Confirmamos los cambios pulsando el botón 'OK'.



5

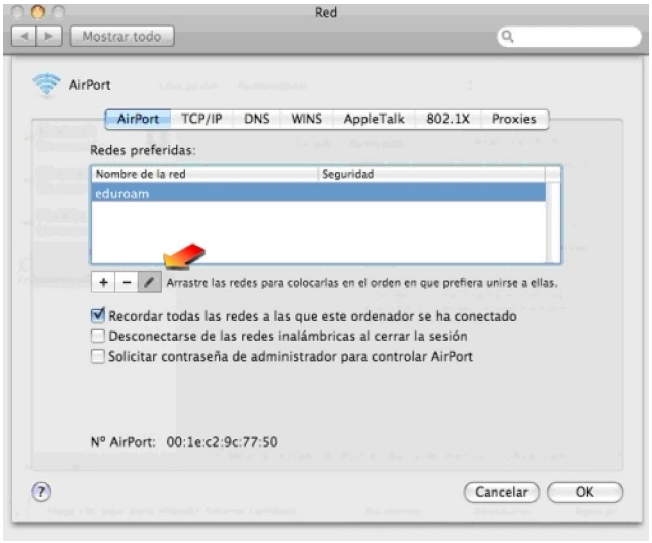


6

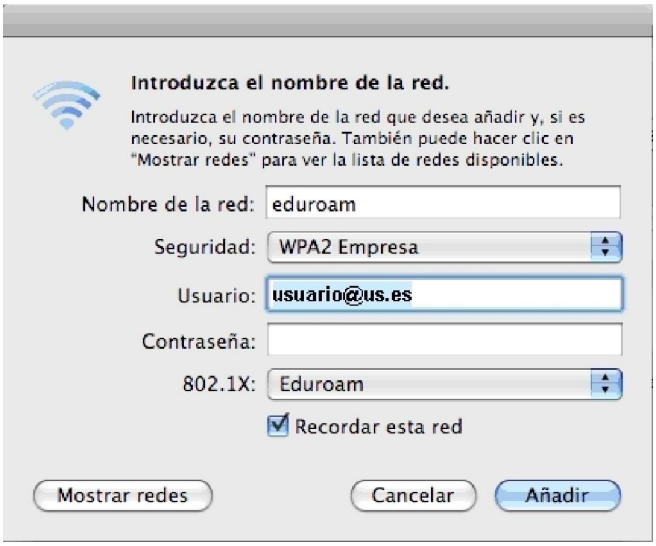
Volvemos a la pestaña 'AirPort', y en el listado de "Redes preferidas", seleccionamos la red 'eduroam' y pulsamos en el botón de edición (el tercero, con el dibujo de un lápiz).

Revisamos la configuración comprobando que el "Nombre de la red" es “eduroam”, “Seguridad” es "WPA2 Empresa" y que “802.1X” es “eduroam”. En los campos “Usuario” y “Contraseña” deberá aparecer el nombre del usuario y contraseña (incluyendo @ y el dominio de la organización que

forma parte del proyecto eduroam). Para confirmar los cambios pulsamos en 'Añadir' y después en 'OK' y en 'Aplicar'.



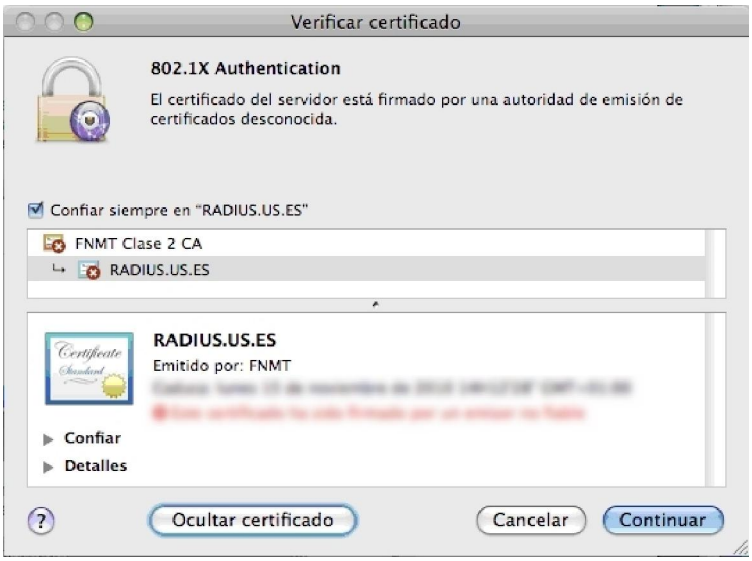
7



8

Al conectar por primera vez al ssid eduroam se debe verificar el certificado del servidor RADIUS que es el encargado de comprobar si su nombre de usuario y contraseña es correcto. Para ello se debe pulsar el botón "Mostrar certificado" en la ventana que aparece, seleccionar el certificado, marcar la opción "Confiar siempre en radius.us.es" y por último pulsar en el botón 'Continuar'.

Dado que la Universidad de Sevilla dispone de dos servidores radius, si el principal no estuviera disponible respondería el secundario "radius2.us.es", por lo que podría aparecer un mensaje similar para el servidor "radius2.us.es".



9

Pulsamos arriba a la derecha en la LUPA y escribimos "LLAVE". Elegimos, de entre los resultados, el que tiene el nombre de "Llaveros" y ordenamos por certificado. Elegimos el certificado de la Autoridad de Certificación (FNMT) y también seleccionamos "confiar siempre". Por último, volvemos a la configuración de AirPort y desactivamos y volvemos a activar el AirPort. Una vez realizado esto, estaremos conectados.

f) *Configuración en iPhone OS:*

Para poder usar el SSID eduroam con un Apple iPhone o iTouch es necesario que el dispositivo tenga al menos la versión 2.0 de firmware. Con esta versión, se habilita una funcionalidad que permite conectarse a redes wifi WPA/WPA2 Enterprise.

1. Para poder configurar la red inalámbrica en el iPhone y en el iPod Touch es necesario estar conectado a internet, por ejemplo reinus-web, que la Universidad de Sevilla pone a disposición de sus usuarios.

1

2. Completamos el siguiente formulario que nos proporcionará un fichero de perfil personalizado para el usuario y para el SSID eduroam en la Universidad de Sevilla.

2

3. Instalamos el fichero de perfil en el dispositivo iPhone o iTouch siguiendo los siguientes pasos y pulsando el botón "Instalar":

3

4

5

6

4. Volvemos a la pantalla principal del iPhone y seleccionamos la opción "Ajustes →Wi-fi". Para evitar problemas durante el uso del SSID eduroam, deshabilitamos el SSID reinus-web pulsando en "reinus-web" y después en el botón "omitir esta red".

7

8

9

5. Seleccionamos "eduroam" e introducimos la clave del usuario virtual de la US. Si el usuario no pertenece a la Universidad de Sevilla, tendrá que introducir la clave de su correo electrónico de la Universidad de origen. Comprobamos el certificado del servidor de autenticación que se nos muestra: el nombre debe ser radius.us.es o radius2.us.es y debe estar firmado por la FNMT. Aceptamos el certificado del servidor.

10

11

12

La pantalla Wi-fi nos indica ahora que estamos conectados con "eduroam".

g) Configuración de una PDA con Windows Mobile:

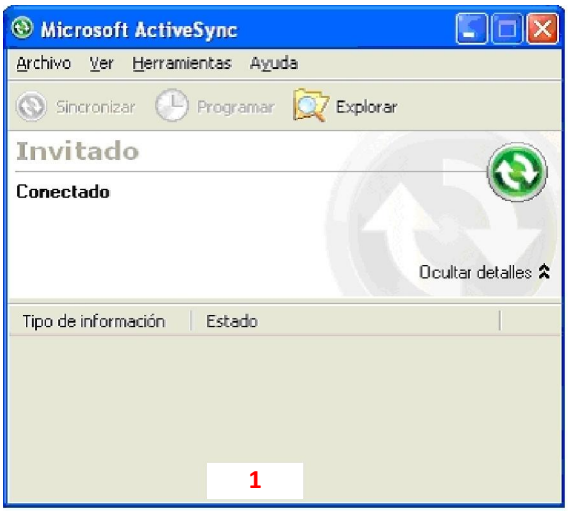
Windows Phone, anteriormente llamado Windows Mobile es un sistema operativo móvil desarrollado por Microsoft, y diseñado para su uso en teléfonos inteligentes (Smartphones) y otros dispositivos móviles. Se basa en el núcleo del sistema operativo Windows CE y cuenta con un conjunto de aplicaciones básicas utilizando las API de Microsoft Windows.

Windows Mobile ha evolucionado y cambiado de nombre varias veces durante su desarrollo, siendo la última versión la llamada Windows Phone 7, anunciada el 15 de febrero del 2010 y sujeta a disponibilidad a finales de 2010.

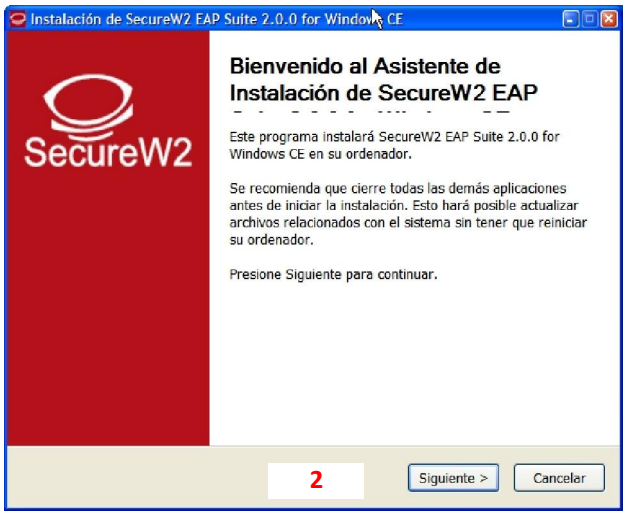
Los pasos a seguir para conectar una PDA con Windows Mobile a la red inalámbrica de la Universidad de Sevilla son los siguientes:

Paso 1: Instalar el cliente de autenticación.

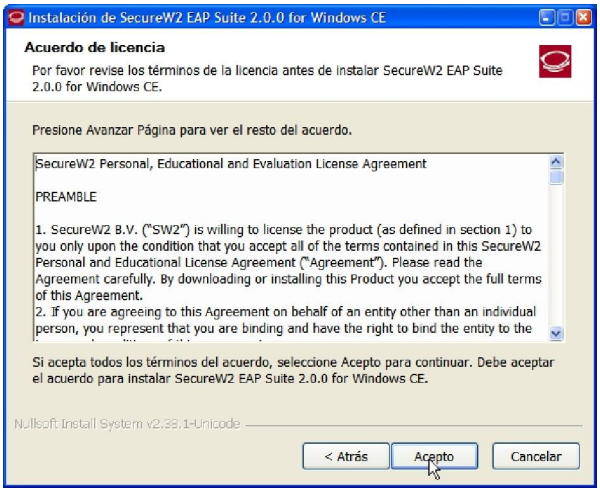
Descargamos e instalamos el programa cliente de autenticación SecureW2 para Pocket PC, como lo hemos hecho en el caso de Windows anteriormente. Teniendo conectada la PDA al ordenador, nos aparecerá la aplicación Microsoft ActiveSync.



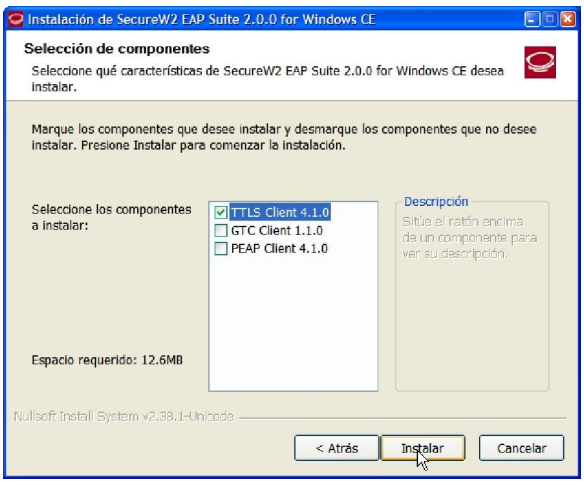
1



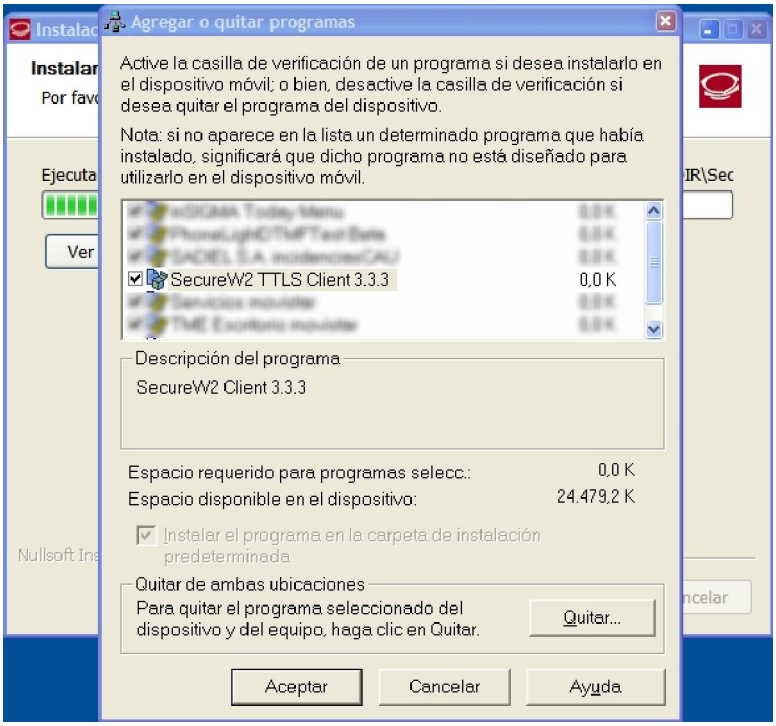
2

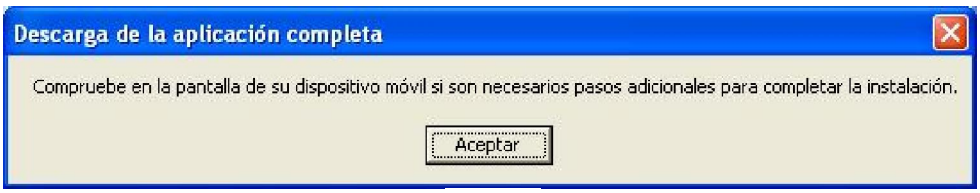


3



4





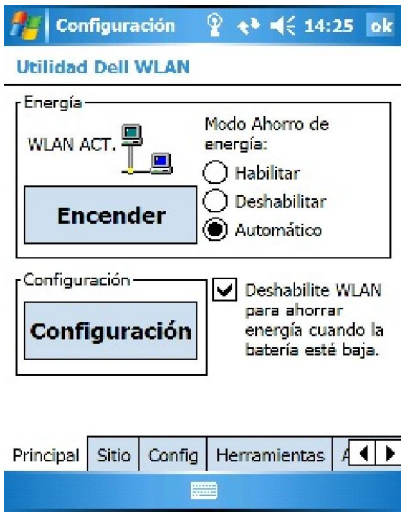
5

Paso 2: Configuración del TCP/IP.

Configuramos el protocolo TCP/IP en el PDA. Debemos asegurarnos de que NO tiene forzada una dirección IP fija en la interfaz de red inalámbrica (al igual que hemos hecho en los casos anteriores), sino que la IP se obtendrá dinámicamente por *DHCP*.

Paso 3: Configuración Inalámbrica.

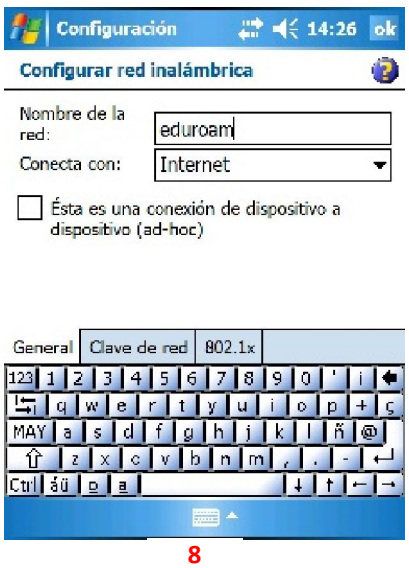
Accedemos a la configuración de redes inalámbricas y pulsamos en el botón de configuración.



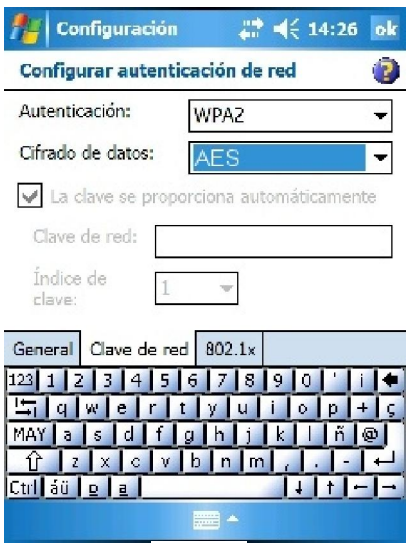
6

7

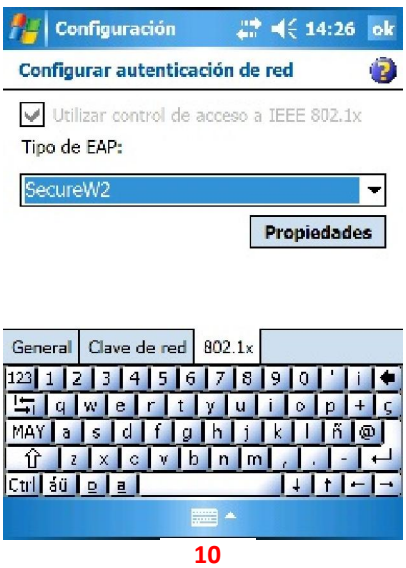
- Pulsamos en la pestaña 'Inalámbrico' y seleccionamos "Agregar nueva...". En la pestaña "General" escribimos eduroam como "Nombre de la red".
- En la pestaña "Clave de red", en 'Autenticación' seleccione WPA2 y en "cifrado de datos" seleccionamos 'AES'.
- En la pestaña '802.1x', nos aseguramos de que está marcada la opción "Utilizar control de acceso a IEEE 802.1x" y seleccionamos como "Tipo de EAP" SecureW2.



8



9

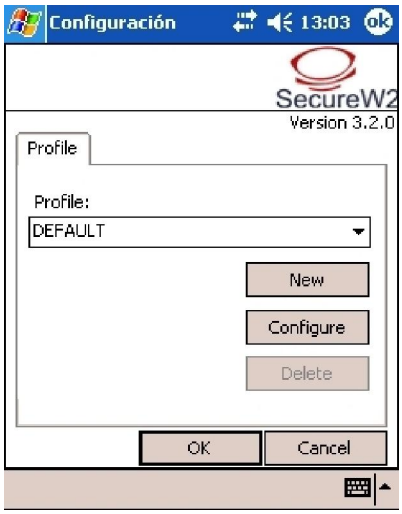


10

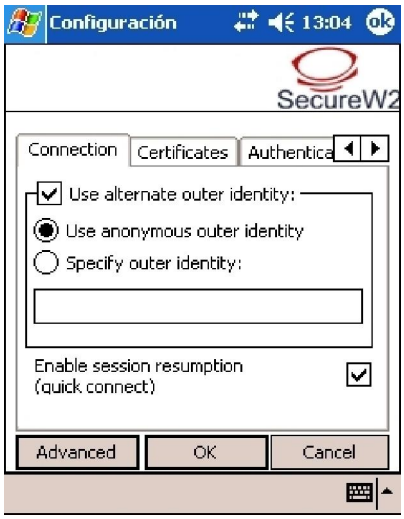
Para configurar el cliente SecureW2, pulsamos en el botón 'Propiedades' y aparecerá el cuadro de diálogo de configuración del software SecureW2. Podemos crear distintos perfiles (profiles) con distintas configuraciones o usar el perfil por omisión (default), igual que en el caso del iPhone. En este caso pulse en el botón 'Configure'.

- En la pestaña 'Connection', nos aseguramos de que están marcadas las opciones "Use alternate outer identity", "Use anonymous outer identity" y "Enable session resumption (quick connect)".

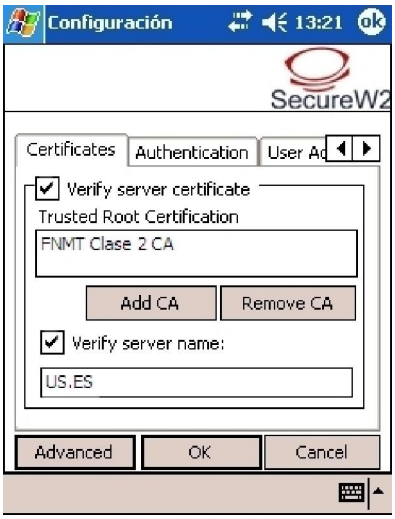
- Para aumentar la seguridad en el acceso al SSID eduroam, marcamos "Verify Server certificate" y pulsamos el botón "Add CA" y en la ventana que se presenta, seleccionamos "FNMT Clase 2 CA" y pulsamos el botón "Add". A continuación, marcamos "Verify Server name" e introducimos "US.ES" (en MAYUSCULAS, es IMPORTANTE).De esta forma, cada vez que accedamos a eduroam, se comprobará que los certificados de los servidores de Autentificación, están firmados por la Autoridad de Certificación (CA) que indicamos.



11

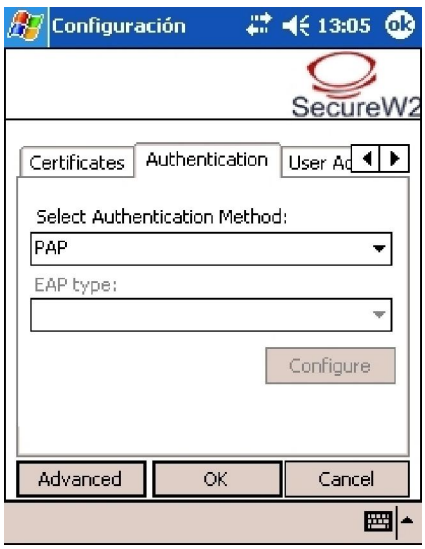


12

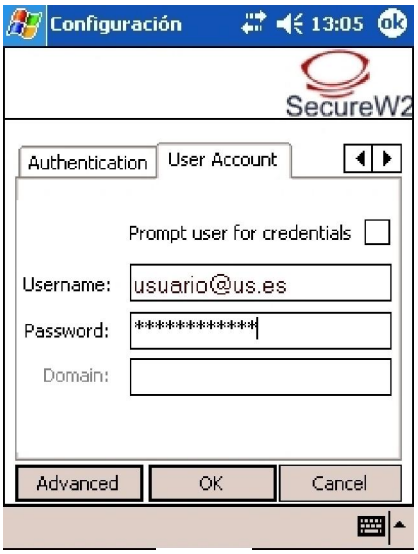


13

- En la pestaña 'Authentication', en la opción "Select Authentication Method", seleccionamos la opción 'PAP'.
- En la pestaña "User account", no activamos la opción "Prompt user for credentials" y escribimos en "Username" y "Password" el nombre y clave de usuario virtual de la US (**incluyendo @us.es**). En el caso de que el usuario no pertenezca a la Universidad de Sevilla, tendrá que introducir su correo electrónico (incluyendo @ y el dominio de la organización a la que pertenece) y su clave.
- Por último, pulsamos en el botón "Advanced" y activamos la casilla "Allow users to setup new connections". Pulsamos OK.



14



15

16

Pulsando el botón 'OK', hemos terminado de configurar el cliente SecureW2 de Windows Mobile. Solo nos queda activar la interfaz inalámbrica de la PDA y seleccionar el SSID eduroam. Tras esto el sistema queda configurado para usar Eduroam.

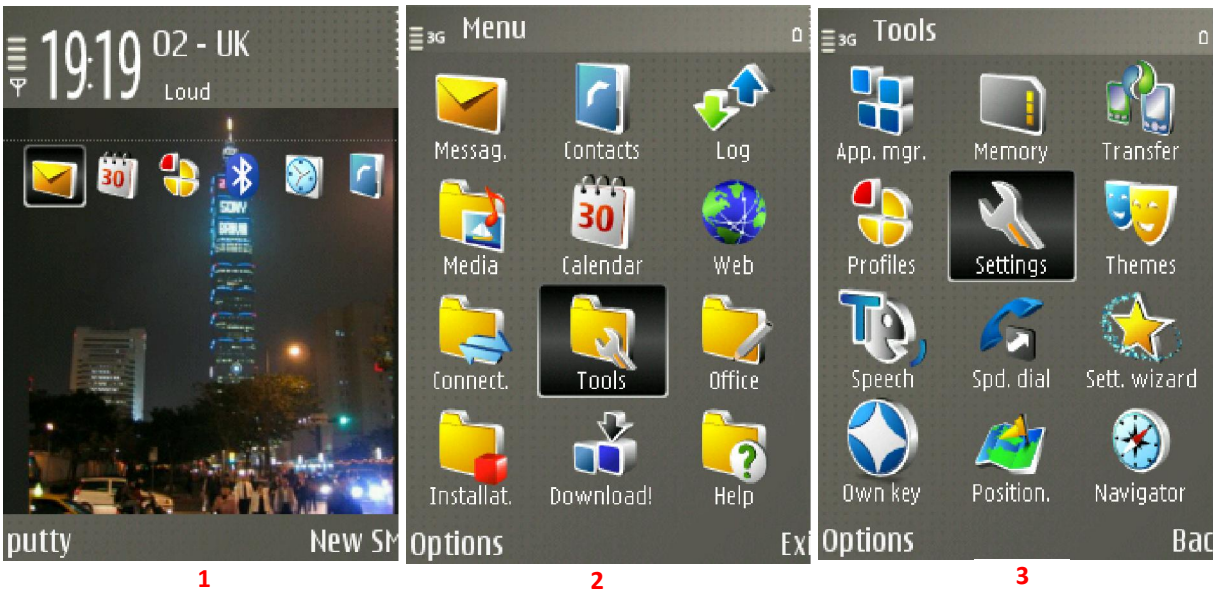
h) *Configuración de un móvil con Symbian:*

Symbian es un sistema operativo que se está incorporado en algunos teléfonos móviles de última generación, y que nos permite realizar conexiones inalámbricas utilizando el cliente 802.1X. Actualmente no hay ningún dispositivo que incorpore el protocolo EAP-TTLS PAP como método de conexión y autenticación. Este protocolo es utilizado por muchas de las organizaciones que forman parte del proyecto Eduroam para conseguir sus objetivos de movilidad. En los foros de Nokia se está debatiendo actualmente cuando va a incorporar Symbian el protocolo EAP-TTLS PAP que permita la conexión a Eduroam.

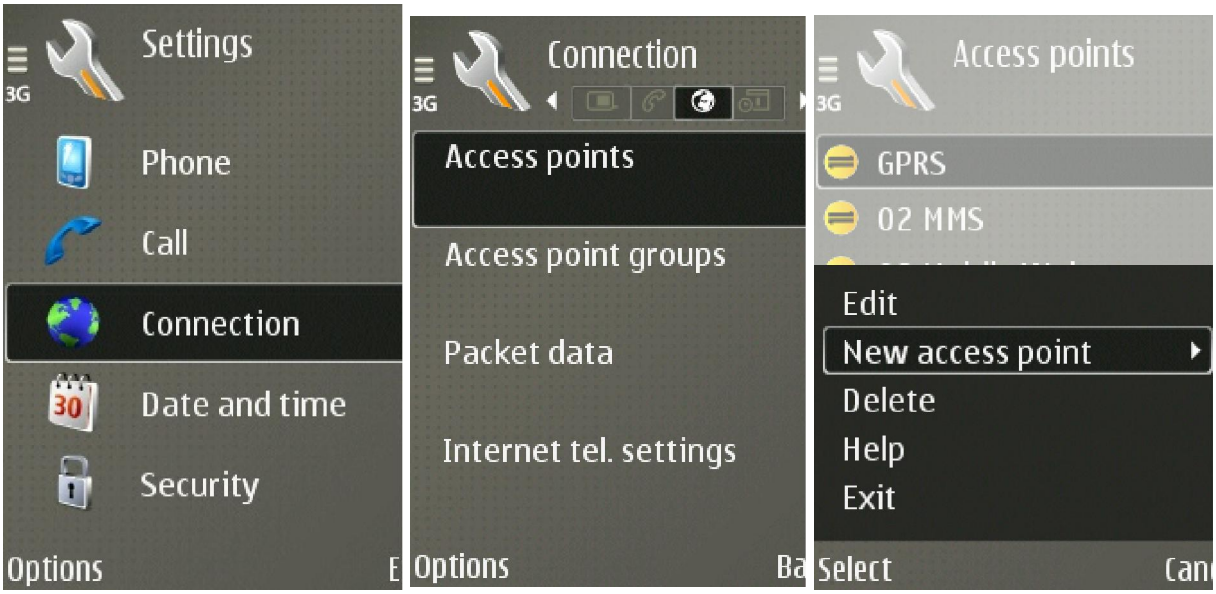
Hasta este momento, los dispositivos Symbian no podían conectarse al SSID eduroam en la Universidad de Sevilla, ya que no son compatibles con WPA/AES/EAP-TTLS/PAP. Para que estos equipos puedan conectarse a ReInUS, se ha modificado el SSID eduroam para que soporte EAP-GTC sobre EAP-TTLS. En este documento se describe como configurar un teléfono Nokia E51 para conectarse al SSID eduroam. La configuración y el acceso a Internet en otros modelos pueden ser ligeramente diferentes.

Paso 1: Definir Eduroam como punto de acceso.

En el menú principal, seleccionamos Conectividad/Gestión de conexiones/WLAN disponibles y marcamos eduroam. Pulsamos en “opciones” y seleccionamos “definir punto de acceso”.



1 2 3



4 5 6

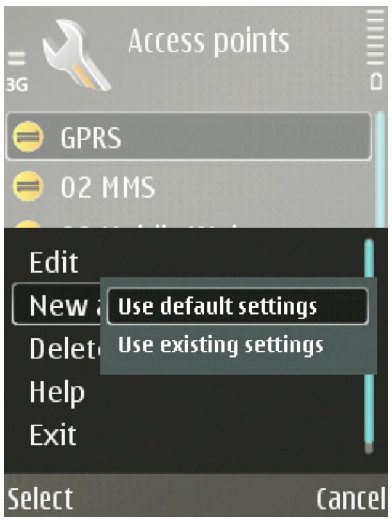
Paso 2: Descargamos el certificado de la Autoridad de Certificación.

Previo al paso 3, necesitaremos tener instalado en el móvil el certificado de la Autoridad de Certificación (CA). Conectándonos a la web de documentación de ReInUS (por ejemplo usando el SSID reinus-web), en el apartado Métodos de conexión|SSID Eduroam|Descargas|Descarga podemos descargar el Certificado de la Autoridad de Certificación FNMT en formato DER (importante).

Paso 3: Configuración del punto de acceso eduroam.

En el menú principal, seleccionamos Herramientas/ Ajustes/ Conexión/ Puntos de acceso y seleccionamos eduroam. En opciones marcamos la opción editar:

- Nombre de conexión: eduroam.
- Portador de datos: LAN inalámbrica.
- Nombre de red WLAN: eduroam.
- Estado de la red: Pública.
- Modo de red WLAN: Infraestructura.
- Modo de seguridad WLAN: WPA/WPA2.



7

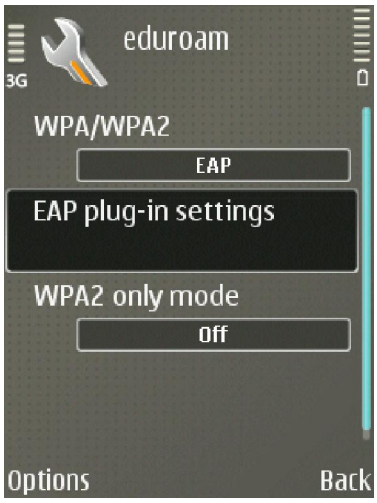
8

9

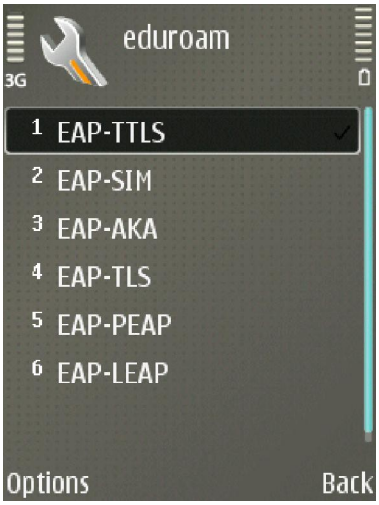
- Ajustes seguridad WLAN:
  - WPA/WPA2: EAP.
  - Ajustes plug-ins EAP:
    - ✓ Desactivamos todas las opciones excepto EAP-TTLS
    - ✓ Seleccione EAP-TTLS (importante de no confundirlo con EAP-TLS) y en opciones pulsamos en editar. Aparecerá una pantalla con 3 pestañas:

      - ❖ Pestaña Ajustes:
        - Certificado personal: No definido.
        - Certificado de autoridad: Seleccionamos FNMT Clase 2 CA que previamente instalamos en el paso 2.
        - Nombre de usuario en...: Definido usuario.
        - Nombre de usuario: Nombre de usuario virtual de la US sin incluir @us.es o correo electrónico sin incluir @ de la universidad a la que pertenece.
        - Área en uso: Definida usuario.
        - Área: Escribimos us.es si el usuario pertenece a la US. Si no, escribimos el Dominio de su Organización.
        - Privacidad TLS: Desactivada (este apartado en algunos teléfonos no aparece).

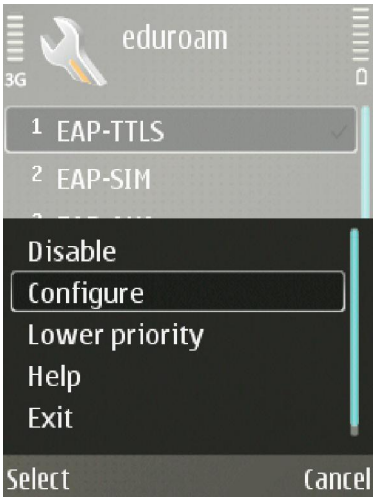
      - ❖ Pestaña EAPs:
        - Desactivamos todas las opciones excepto EAP-GTC.
        - Seleccionamos EAP-GTC y en opciones pulsamos editar:
          - Nombre de usuario: Escribimos el nombre de usuario virtual de la US incluyendo @us.es.
        - Pulsamos Atrás para salir y volver al nivel anterior.



10



11



12

13

14

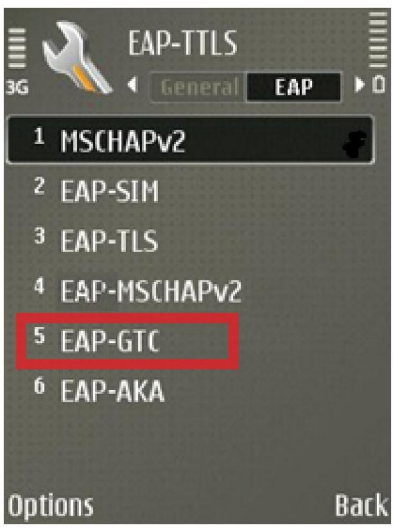
15

❖ Pestaña Cifrado:

- Activamos todas las opciones.
- Pulsamos Atrás dos veces para salir y volver al nivel anterior.

- Modo WPA2 sólo: Desactivado.

➢ Pulsamos Atrás para finalizar.



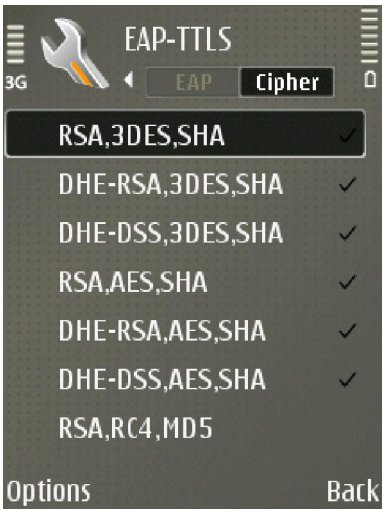
16

17

18

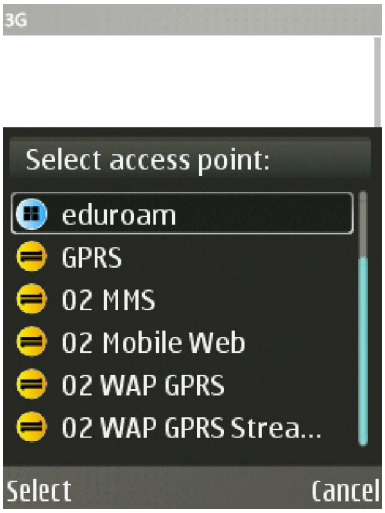
Paso 4: Conexión a Eduroam.

En el menú principal, pulsamos en Conectividad/ Asistente WLAN, seleccionamos eduroam y en opciones seleccionamos Iniciar navegación Web.



19

20



21

Cada vez que una aplicación necesita acceder a Internet aparecerá el menú del "Selección del punto de acceso". Eduroam aparecerá en la lista de redes inalámbricas mientras nos encontremos dentro del alcance de un punto de conexión inalámbrica eduroam. Sólo tenemos que seleccionarlo y el dispositivo se conectará de forma automática.

i) Configuración de un móvil con Android:

Android es un sistema operativo orientado a dispositivos móviles basado en una versión modificada del núcleo Linux. Inicialmente fue desarrollado por Android Inc., compañía que fue comprada después por Google, y en la actualidad lo desarrollan los miembros de la Open Handset Alliance (liderada por Google). Esta plataforma permite el desarrollo de aplicaciones por terceros a través del SDK, proporcionada por el mismo Google, y mediante el lenguaje de programación Java. Una alternativa es el uso del NDK (Native Development Kit) de Google para emplear el lenguaje de programación C.

Hoy en día hay tres versiones principales de Android: 1.5, de nombre en clave Cupcake; 1.6 o Donut y 2.x, Eclair. Por supuesto también existieron versiones anteriores: la 1.0, con la que se lanzó el primer móvil Android del mercado, el HTC Dream o G1, y la 1.1, de febrero de 2009, que solucionaba varios errores y añadía alguna que otra funcionalidad no demasiado importante.

Muchos de los estudiantes de la Universidad de Sevilla tienen dispositivos funcionando con este sistema operativo, en sus distintas versiones, pero la mayoría se queja de que no encuentran la información ni el soporte necesario para conectarse. Este problema de conexión ha sido ampliamente discutido en foros de internet por muchos estudiantes de distintas universidades españolas.

Vamos a intentar averiguar cuáles son los problemas de conexión que surgen en la Universidad de Sevilla, sabiendo que aquí el método de autenticación de Eduroam es EAP-TTLS con cifrado AES, haciendo pruebas prácticas con un dispositivo que funciona con Android.

Suponiendo que los pasos a seguir para la conexión a Eduroam no tienen que ser tan distintos a los del Sistema Operativo Windows Mobile o a los demás presentados anteriormente, intentaremos ofrecer soluciones a los problemas encontrados y dar la oportunidad a los estudiantes de la Universidad de Sevilla de conectarse con sus teléfonos móviles con Android a la red inalámbrica de la Universidad.

III. Problemas que presenta la red Eduroam y posibles soluciones.

1. Dispositivos que utilizan el sistema operativo Symbian

La red Eduroam ya lleva algún tiempo funcionando en los distintos edificios de la Universidad de Sevilla, y durante este tiempo han sido numerosas las quejas por parte de alumnos y profesores sobre la imposibilidad de utilizar este servicio desde sus terminales con Symbian.

Para que un dispositivo de estas características pueda conectarse a la red Eduroam de la Universidad de Sevilla, dicho dispositivo tiene que soportar EAP-TTLS y PAP. Dispositivos bastante actuales como pueden ser el Nokia N95, o el Nokia N81 no soportan PAP. La Universidad de Sevilla, como respuestas a estas quejas, proporcionó el tutorial arriba explicado, que permitía el uso de EAP-GTC en lugar de PAP. Sin embargo, la configuración que propone la Universidad de Sevilla para móviles con Symbian no es válida en muchos de los dispositivos con este sistema operativo. La configuración se realiza de forma correcta, pero al intentar autenticarnos con RADIUS, el sistema operativo entra en un bucle en el que nos pide la contraseña, y sin darnos tiempo a introducirla, vuelve a solicitarla. Se han realizado pruebas con un dispositivo Nokia N95, y con un dispositivo Nokia E65, y en ambos ocurre lo anteriormente expuesto.

Los últimos dispositivos que han aparecido con este sistema operativo sí soportan PAP (actualizando previamente el firmware a la última versión disponible). Los pasos para conectar estos dispositivos, (la Universidad de Sevilla no los facilita), son los siguientes:

1) Descargar de http://reinus.us.es/certificados.es.html , tres certificados con extensión DER. Entrar en Menú – Aplicaciones – Gestor de archivos, y una vez encontrada la carpeta donde los hemos descargado, instalarlos uno a uno, marcando todas las opciones posibles que nos aparecen.

2) En una zona con cobertura Eduroam se siguen los siguiente pasos: Menú - Ajustes - Conectividad - LAN inalámbrica --> Eduroam y seleccionamos conectar. Sale una ventana que permite ajustar los parámetros.

3) Menú - Ajustes - Conectividad - Destinos de red - Internet – Eduroam. Rellenamos con los siguientes datos:

-Nombre conexión: eduroam
-Portador datos: Lan inalámbrica
-Nombre red: eduroam
-Estado: publica
-Modo red: Infraestructura
-Modo seguridad: 802.1x

-Ajustes de seguridad:
WPA/WPA2: EAP

-Ajustes plug-in
Solo marca EAP-TTLS y pincha en ella.

-Certificado personal: No definido
-Certificado de autoridad: FNMT Clase 2 CA (lo añadimos antes, en el paso 1)
-Nombre usuario: tu_nombre@us.es
-Área de uso: Definida por usuario
-Área: (vacio)
-Privacidad TLS: Desactivada

En esta misma pantalla aparece una pequeña flecha arriba a la derecha, la seleccionamos, marcamos sólo PAP y aceptamos.

-Nombre usuario: usuario@us.es
-Contraseña: contraseña_del_usuario

2. Dispositivos que utilizan el sistema operativo Android

La Universidad de Sevilla no proporciona información sobre los pasos a seguir para conectar un dispositivo con Android a su red Eduroam.

Al intentar conectarnos con un dispositivo modelo HTC Tattoo, el terminal nos ofrece la posibilidad de indicarle que utilice EAP-TTLS, y también nos permite introducir nuestro nombre de usuario y contraseña. Sin embargo, no nos permite indicarle que debe usar PAP, por lo que Eduroam no funciona.

La mejor opción para solucionarlo es la siguiente:

Se accede como root al fichero /system/etc/wifi/wpa_supplicant.conf, donde se añade lo siguiente:

```
update_config=1
ctrl_interface=tiwlan0
eapol_version=1
ap_scan=1
fast_reauth=1

network={
    ssid="eduroam"
    key_mgmt=WPA-EAP
    eap=TTLS
    anonymous_identity="anonymous@US.ES"
    identity=”USUARIO@US.ES”
    password="CONTRASEÑA"
    priority=2
    phase2="auth=PAP"
}
```

Debemos asegurarnos de no tener la configuración de IP manual activa.

La diferencia entre este caso y un dispositivo con Symbian, es que Android sí soporta PAP aunque no nos deje configurarlo de forma gráfica.

3. Pruebas realizadas con otros dispositivos

Hemos realizado numerosas pruebas con dispositivos de varios tipos en la Universidad de Sevilla:

- Ordenador con Windows XP/Windows Vista/Windows 7: Siguiendo el tutorial de la Universidad de Sevilla, se conectan sin ninguna dificultad.
- Ordenador con Mac OSX Leopard / Snow Leopard: En Snow Leopard (más actual que Leopard) aparecen pequeñas diferencias con lo expuesto en el tutorial, que sin embargo, un usuario cualquiera podría solventar sin gran dificultad.
- Nokia N95/E65: Sin éxito, por los problemas expuestos anteriormente.
- Hemos probado a utilizar los dispositivos configurados dentro del edificio de la Escuela Superior de Ingenieros en otros edificios de la Universidad de Sevilla, y la conexión funciona sin necesidad de realizar ninguna modificación adicional.
- También hemos intentado autenticarnos en la Universidad de Sevilla con un usuario y un Password de otra universidad (INSA de Lyon) para comprobar que tenía acceso a la red sin problemas. El resultado ha sido positivo.

4. Revuelo en la comunidad de Eduroam

Hasta hace poco tiempo, el cliente utilizado para la autenticación en la red Eduroam de la Universidad de Sevilla, SecureW2, se podía descargar de forma gratuita de la página de dicha universidad. SecureW2 contaba con dos versiones: la 1.x con licencia GPL, y la 2.x con código cerrado o con otras licencias. En 2009 SecureW2 cambio su licencia para la rama 2.x, dejando de permitir la libre distribución de este cliente dentro del espacio académico europeo, retirando la posibilidad de descarga, y pidiendo que no se distribuyera públicamente.

El motivo de este cambio es el alto coste de mantener esta versión: el ancho de banda, el soporte gratis a los usuarios...

Esta situación afecta la comunidad Eduroam, causando un gran revuelo. Todas las instituciones que habían confiado en la gratuidad de esta aplicación ahora tienen dos opciones:

- Pagar para usar la red inalámbrica Eduroam
- Buscar alternativas

¿Qué soluciones se pueden considerar frente a este problema? Una alternativa seria utilizar o desarrollar otros clientes que soporten EAP-TTLS, pero que sean libres. SecureW2 1.x parece funcionar en bastantes plataformas, pero carece de soporte, y otros clientes comerciales existentes, tienen un coste y están pensados para entornos empresariales.

Una posibilidad sería cambiar el método de autenticación EAP-TTLS a EAP-PEAP u otro. Se ha realizado una encuesta cuyos resultados se conocerán en breve sobre el impacto de este cambio. Hasta una decisión final de los organismos reguladores de Eduroam, cada organización toma sus propias decisiones con respecto a este asunto.

Por ejemplo, en la Universidad de Sevilla, para conectar a Eduroam usando el sistema operativo Windows 7 a través del cliente SecureW2, es imprescindible contactar con el administrador de la

Universidad, ya que solamente él dispone de la versión 2.x que desde el año pasado no puede ser distribuida libremente.

IV. Conclusiones

La seguridad en las redes inalámbricas es un aspecto que no se puede descuidar. Debido a que las transmisiones viajan por un medio no seguro, se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad. Por esto, la seguridad se ha convertido en un factor importante en el diseño e implementación de las redes.

El administrador de la red debe estar constantemente implementando medidas de seguridad en la red con el fin de tener una red segura y estable. Las redes inalámbricas están en constante crecimiento y esto representa un reto para los administradores que tendrán que desarrollar medidas eficaces para mantener seguras las redes.

Durante el desarrollo de las redes inalámbricas han aparecido distintos mecanismos, que trataban de garantizar la seguridad en dichas redes. Los equipos informáticos han ido evolucionando paralelamente, permitiendo realizar gran cantidad de cálculos en tiempos cada vez más pequeños. Por este motivo muchos de esos mecanismos han resultado ser menos seguros de lo que inicialmente se pensó.

Gracias al diseño de seguridad del estándar WPA2 y a los últimos métodos de cifrado, las redes inalámbricas más modernas disponen de una seguridad bastante eficaz. El mayor factor de incertidumbre se debe al usuario. Hoy en día, cuando un intruso consigue acceder a una infraestructura WLAN dotada de alguno de los mecanismos de seguridad que actualmente se consideran seguros, la causa suele ser un punto de acceso configurado de forma negligente. Por tanto, es necesario tomarse algún tiempo para considerar cuidadosamente cada una de las opciones de seguridad presentados en este trabajo.

Los métodos para proteger las redes inalámbricas se encuentran en continua evolución. Si bien podemos decir que las técnicas utilizadas hoy en día son bastante seguras, no podemos descartar la aparición de nuevos ataques que hagan que estos mecanismos queden obsoletos.

En la segunda parte de este trabajo, nos hemos centrado en el análisis de un caso concreto de red inalámbrica, la red Eduroam, tanto a nivel mundial, como estudiando su implementación en la Universidad de Sevilla. Eduroam representa un espacio mundial único de movilidad para un amplio grupo de organizaciones, que en base a una política de uso y una serie de requerimientos tecnológicos y funcionales permiten que sus usuarios puedan desplazarse entre ellas, disponiendo en todo momento de los servicios móviles que pudieran necesitar.

Esta red, que tuvo sus orígenes en Europa, se ha extendido rápidamente por todo el mundo, debido a las múltiples ventajas que presenta para todas las organizaciones implicadas en el proyecto, así como para sus usuarios.

Para comprobar su compatibilidad con cualquier dispositivo y entorno, en este trabajo hemos dedicado una parte al estudio teórico y práctico de las distintas formas de conexión a la red inalámbrica Eduroam, analizando en cada caso los problemas que pueden surgir: desde el punto de vista de la seguridad o de la accesibilidad de la conexión.

En la última parte del trabajo hemos analizado y hemos intentado solucionar algunos de los problemas encontrados en el estudio práctico arriba mencionado, lo que nos ha permitido tener un espíritu crítico sobre la implementación de la red Eduroam en la Universidad de Sevilla.

Los principales problemas encontrados se deben a que todavía no todos los dispositivos soportan las modernas técnicas de autenticación y cifrado utilizadas en Eduroam. Este problema será solventado, sin duda, según vayan apareciendo nuevos modelos de dispositivos, que se adapten a las especificaciones requeridas.

En conclusión, este trabajo nos ha permitido, por un lado profundizar en el problema de la falta de seguridad que existe en las redes inalámbricas, y por otro lado conocer las posibilidades de movilidad y conectividad a las que podemos acceder como estudiantes de una organización adherida al proyecto Eduroam, y su funcionamiento.

Glosario

AAA: Authentication Authorization Accounting
AES: Advanced Encryption Standard
AKA: Authentication and Key Agreement
CA: Certification Authority
CHAP: Challenge Handshake Authentication Protocol
CRC: Cyclic Redundancy Check
DATE: Design, Automation and Test in Europe
DES: Data Encryption Standard
EAP: Extensible Authentication Protocol
EAPOL: Extensible Authentication Protocol over LAN (Local Area Network)
Eduroam: Educational Roaming
FAST: Flexible Authentication via Secure Tunneling
FNMT: Fábrica Nacional de Moneda y Timbre
GTC: Generic Token Card
ICV: Integrity Check Value
LEAP: Lightweight EAP
MD5: Message Digest 5
MIC: Message Integrity Code
MS-CHAP: Microsoft Challenge Handshake Authentication Protocol
MSDU: MAC Service Data Unit
NDK: Native Development Kit
PAE: Port Access Entity
PEAP: Protected EAP
POTP: Protected One-Time Password
PPP: Point to Point Protocol
PRNG: Generador PseudoAleatorio Numérico
PSK: Pre Shared Key
RADIUS: Remote Authentication Dial-In User Service
RC4: Ron's Cipher 4
RSA: Rivest Shamir Adleman
SHA: Secure Hash Algorithm
SIM: Subscriber Identity Module
SSID: Service Set Identifier
TKIP: Temporal Key Integrity Protocol
TLS: Transport Layer Security
TTLS: Tunneled Transport Layer Security
WEP: Wired Equivalent Privacy
WPA: Wi-Fi Protected Access

Bibliografía

Libros:

[1] F. Andreu, I. Pellejero, A. Lesta, *"Redes WLAN. Fundamentos y aplicaciones de seguridad"*, equipo gráfico Marcombo, coordinador editorial C. Parcerisas, 2006, Barcelona, España, ISBN 84-267-1405-6.

[2] A. Los Santos Aransay, *"Seguridad en Wi-Fi"*, Universidad de Vigo: Redes Personales y locales, julio 2009.

[3] W. Stallings, *"Fundamentos de seguridad en redes"*, editorial Pearson Educación, 2ª Edición, ISBN 84-205-4002-1.

Artículos:

[4] Kwang-Hyun Baek, Sean W. Smith, David Kotz, *"A Survey of WPA and 802.11i RSN Authentication Protocols"*, Dartmouth College Computer Science Technical Report TR2004-524, noviembre 2004.

[5] Linux-Magazine N° 48, Redes Inalámbricas, "Estrategias de seguridad para redes inalámbricas en el aire", paginas 25-27, marzo 2009.

[6] Alberto Los Santos Aransay, *"Seguridad en Wi-Fi"*, Universidad de Vigo: REDES PERSONALES Y LOCALES, julio 2009.

[7] Rodrigo Castro, *"Avanzando en la seguridad de las redes WIFI"*, Boletín de RedIRIS, nº 73, septiembre 2005.

[8] Jesús Goya Abaurrea, *"Seguridad y Autenticación en Redes Inalámbricas",* Proyecto fin de carrera. Tutor: Juan José Murillo Fuentes. 2005.

[9] José Luís Salazar, *"Criptografía y seguridad en Comunicaciones".* Práctica 1: Criptografía del "Wired Equivalent Protocol" (WEP).

[10] Erik Dobbelsteijn, *"Inventory of 802.1X-based solutions for inter-NRENs roaming"*, Versión 1.2, Mobility Task Force, Terena

Páginas Web:

[11] EAP: http://www.ietf.org/rfc/rfc4017.txt

[12] TLS: http://rfc.sunsite.dk/rfc/rfc2246.html

[13] EAP-MS-CHAPv2: http://tools.ietf.org/id/draft-kamath-pppext-eap-mschapv2-02.txt

[14] EAP: http://docs.hp.com/en/T1428-90071/T1428-90071.pdf

[15] WPA: http://hwagm.elhacker.net/wpa/wpa.htm

[16] RSA:

http://news.techworld.com/security/3214360/rsa-1024-bit-private-key-encryption-cracked/

http://es.kioskea.net/contents/crypto/rsa.php3

http://bitelia.com/2010/03/logran-romper-encriptacion-rsa-de-1024-bits

http://www.kriptopolis.org/supuesta-ruptura-rsa-1024

http://www.hackxcrack.es/blogs/gamarra/26-descubren-punto-debil-en-la-autenticacion-rsa.html

[17] 3DES: http://www.tropsoft.com/strongenc/des3.html

[18]ReInUS: http://www.eduroam.us.es/

[19] Eduroam:

http://www.eduroam.es/politica.es.php

http://www.eduroam.es

http://www.eduroam.org/index.php?p=europe

http://www.eduroam.org

[20] Configuraciones: https://www.unilim.fr/sci/article48.html

[21] Otros:

www.securew2.com

http://www.htcmania.com/showthread.php?t=100426

http://www.lacomunateleco.com/smf/index.php?topic=15720.msg137484#msg137484