ANEXO C: **SEGURIDAD WLAN**

***WEP (Wired Equivalent Privacy):*** WEP fue el primer mecanismo de seguridad que se implementó bajo el estándar IEEE 802.11. Es un algoritmo que permite codificar los datos que se transfieren a través de la red inalámbrica y autentica los dispositivos móviles que se conectan al punto de acceso.

Para codificar los paquetes de información, WEP se basa en el algoritmo de encriptación RC4, que utiliza un conjunto de claves de 40 bits, junto con un vector de inicialización (IV) de 24 bits. Actualmente, la mayoría de los fabricantes de puntos de acceso ofrecen algoritmos WEP de 64, 128 o 256 bits, lo cual refuerza el nivel de encriptación.

Cuando una red inalámbrica utiliza WEP se pueden determinar cuatro modos de operación:

- No utilizar WEP.
- Utilizar WEP para codificar datos.
- Utilizar WEP para autenticar dispositivos móviles.
- Utilizar WEP para codificar datos y autenticar dispositivos móviles.

Para realizar la autenticación de dispositivos móviles, WEP establece dos métodos:

• *Libre autenticación*: Permite al dispositivo móvil establecer una conexión con el punto de acceso, sin la necesidad de aplicar ningún mecanismo de autenticación por parte del AP sobre el dispositivo móvil.

Este método se utiliza normalmente en puntos de acceso públicos, como los situados en aeropuertos, cibercafés, salas de conferencias, hoteles, etc.

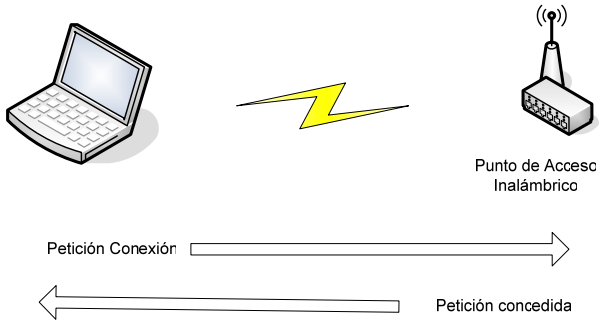


***Figura 1. Libre Autenticación***

• *Utilización de claves compartidas*. En este método existe un conjunto de claves que están en posesión del punto de acceso y del dispositivo móvil. La autenticación se realiza en 4 pasos:

1. El punto de acceso pide al dispositivo móvil que se autentique mediante el envío de una trama de datos.
2. Tras la recepción de ésta, el dispositivo móvil debe encriptar dicha trama y reenviarla al punto de acceso.
3. El punto de acceso decodificará la trama retransmitida por el dispositivo móvil.
4. Si la trama es igual a la original, el punto de acceso permitirá al dispositivo móvil establecer una conexión con el. Por el contrario, si no coincide el dispositivo móvil no se podrá conectar a dicho punto.

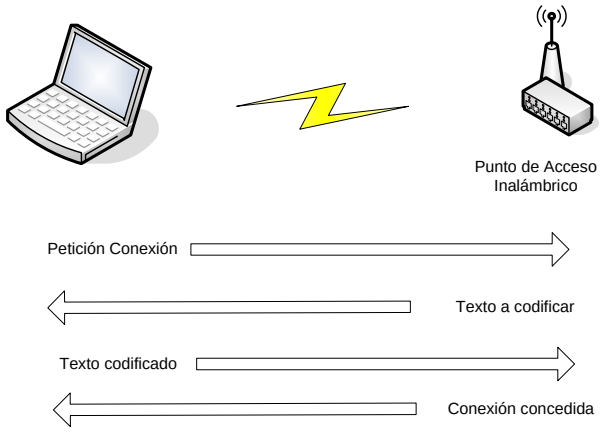


***Figura 2. Utilización de claves compartidas***

WEP, establece dos mecanismos para seleccionar la clave secreta de codificación o decodificación de una trama:

• Primero. Está formado por un conjunto de 4 claves preestablecidas, las cuales se comparten entre los dispositivos móviles y el punto de acceso. La ventaja de este método reside en que una vez obtenido el conjunto de claves, cualquier dispositivo móvil puede comunicarse de forma segura con otro dispositivo de la red inalámbrica. Por otra parte, si el número de dispositivos móviles es elevado, la gestión y mantenimiento de las claves podrá resultar complicada.

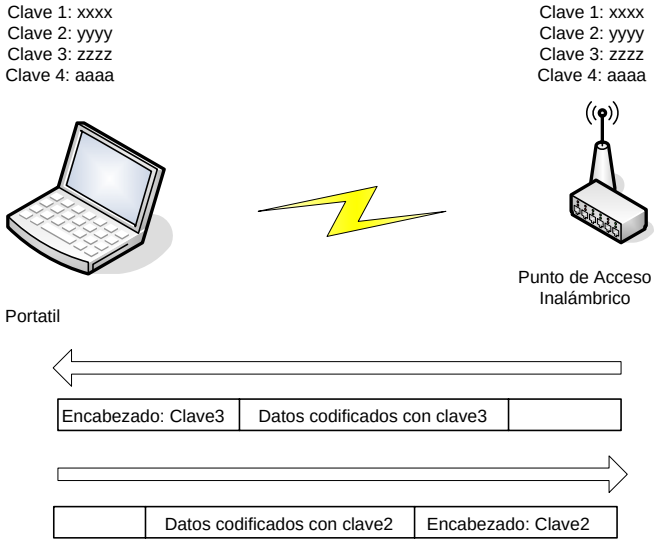


***Figura 3. Conjunto de 4 claves preestablecidas***

• Segundo. Permite a los dispositivos inalámbricos establecer sus propias claves entre ellos. Este mecanismo es mejor frente a un número reducido de dispositivos móviles, pero si el número aumenta, la gestión de las claves es más difícil de administrar.

Para realizar un buen uso de WEP se recomienda seguir las siguientes pautas:

• No utilizar claves obvias. Utilizar números y palabras, código hexadecimal con caracteres no imprimibles, etc.

• Utilizar la mayor longitud de clave posible (64, 128 o 256 bits).

• Cambiar las claves a menudo.

• Utilizar WEP y otros mecanismos de seguridad de forma combinada.

***OSA (Open System Authentication):*** Es un mecanismo de autenticación definido por el estándar 802.11 para autentificar todas las peticiones que recibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aún activando WEP, por lo tanto es un mecanismo poco confiable.

***CNAC (Closed Network Access Control):*** Este mecanismo pretende controlar el acceso a la red inalámbrica permitiendo solamente aquellas estaciones cliente que conozcan el nombre de la red (SSID), actuando este como contraseña.
El SSID (Service Set Identifier) o ESSID (Extended Service Set Identifier) es, básicamente, el nombre que se le asigna a la red inalámbrica, el cual solo es conocido por los dispositivos autorizados.

Este nombre es también utilizado para determinar por parte del dispositivo móvil, a que punto de acceso está conectado y autenticarse en dicho punto de acceso.

***ACL (Access Control List):*** El filtrado de direcciones físicas o filtrado MAC, se utiliza para minimizar el riesgo de conexión de dispositivos no autorizados. Este mecanismo permite configurar en el punto de acceso una lista de direcciones físicas o MAC, de dispositivos inalámbricos. De este modo, solo se permite la conexión de los dispositivos móviles cuya dirección física se encuentra en dicha lista, denegando cualquier servicio que pueda prestar nuestra red inalámbrica a cualquier otro dispositivo móvil que no se encuentre en la lista.

La mayoría de los puntos de acceso hoy en día poseen esta característica y aunque es bastante sencillo de implementar, es recomendable su utilización solamente con un número no muy elevado de dispositivos móviles. Ya que ante un número elevado, la gestión y administración de dicha lista podría resultar costosa.

***Red Privada Virtual:*** Una red privada virtual o VPN (Virtual Private Network), es un sistema para simular una red privada sobre una pública. La idea es que la red pública sea vista desde dentro de la red privada como un “cable lógico” que une dos o más redes que pertenecen a la red privada. Los datos viajan codificados a través de la red pública bajo

una conexión sin codificar, esto se conoce con el nombre de túnel o por el término en ingles “tunnelling”.

La utilización de este sistema tiene varias ventajas como:

- Autenticación
- Confidencialidad de los datos transmitidos.
- Integridad de los datos transmitidos.

Por otra parte, la utilización de VPNs asegura la conexión con el dispositivo móvil de dos formas:

• *Dispositivo móvil – Red.* Basada en la técnica de acceso remoto. El dispositivo móvil se puede conectar a través de una red pública con la red privada. Utilizando VPN el dispositivo móvil formará parte de la red una vez establecida la conexión.

• *Red – Red*. En esta configuración, una subred puede conectarse a otra subred a través de Internet, formando una sola red. De esta forma se elimina el gasto de mantener una red de área extensa (WAN).

Aunque el uso conjunto de WEP y VPN refleja un claro beneficio, deriva un problema debido a dos cosas: por un lado la escasa variedad de clientes VPN para dispositivos móviles (Pocket PC), y por otro lado los requerimientos de procesamiento que se requerirían para utilizar estos métodos en conjunto. El problema tiene su origen en la codificación y decodificación de los datos, ya que esta se realiza dos veces:

• Primero, para WEP.

• Segundo, para VPN.

Esta doble codificación puede afectar directamente al tiempo de transmisión de un archivo. Pero por otra parte, implementan un buen nivel de seguridad de los datos y la conexión.

***Estándar 802.11i:*** Debido a la necesidad inmediata de mejorar los sistemas de seguridad existentes y la demora de publicación del estándar 802.11i, la Wi-Fi alliance en Noviembre del 2002 aprobó el estándar "Wifi Protectected Access" o WPAv1. Este se basó en los borradors de dicho estándar.

WPAv1 se desarrolló para mejorara el nivel de codificación existente en WEP, y para incorporar un método de autenticación. WPA utiliza el protocolo de integridad de clave temporal (TKIP) para codificar los datos, implementa el estándar 802.1X y el protocolo de autenticación extensible (EAP). El conjunto de estos tres mecanismos forman una fuerte estructura de autenticación que utiliza un servidor de autenticación central, como por ejemplo RADIUS o DIAMETER.

Por otro lado, debido a la liberación de la versión final del estándar 802.11i, se dio a conocer el estándar WPAv2, el cual básicamente es la combinación de CCMP y 802.1X. Simplificando, se tiene:

WPAv1 = TKIP + 802.1X
WPAv2 =CCMP+802.1X

A continuación se explicarán cada uno de estos mecanismos:

- **Estándar 802.1X (Control de acceso a la red basado en puertos):**

802.1X es un estándar que restringe el acceso a la red hasta que el usuario se ha validado. No es en sí un método de autenticación, ya que traduce las tramas enviadas por un algoritmo de autenticación (EAP) en el formato necesario para que estas sean entendidas por el sistema de autenticación que utilice la red (por ejemplo Radius o Diameter).

802.1X utiliza el protocolo de autenticación extensible o EAP, para autenticar al dispositivo móvil y la Entidad de Autenticación de Puertos (Port Authentication Entity, PAE) que controla el proceso de autenticación en la red. Algunos de ellos son EAP-TLS (Windows XP), PEAP (servidor de autenticación), EAP-TTLS (Radius), LEAP (Cisco).

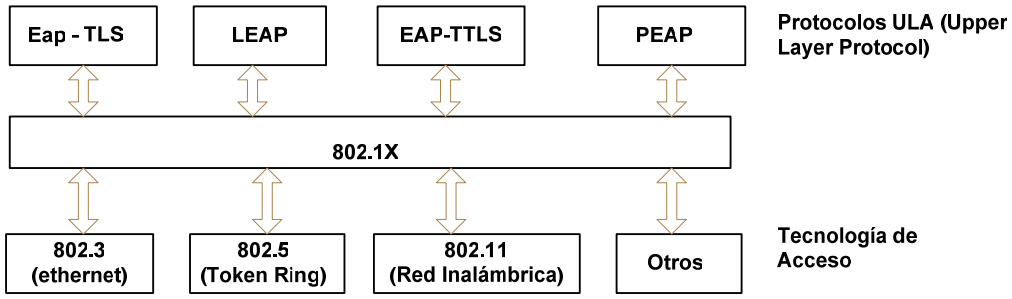


***Figura 4. Protocolo IEEE 802.1X***

El sistema se compone de los siguientes elementos:

- Una estación cliente
- Un punto de acceso
- Un servidor de Autenticación (AS).

En el servidor de autenticación realiza la autenticación real de las credenciales proporcionadas por el cliente. El AS es una entidad separada situada en la zona cableada (red clásica, pero también implementable en un punto de acceso). El tipo de servidor utilizado podría ser el RADIUS, u otro tipo de servidor que se crea conveniente (802.1x no especifica nada al respecto).

El estándar 802.1x introduce un nuevo concepto de puerto habilitado /inhabilitado en el cual hasta que un cliente no se valide en el servidor no tiene acceso a los servicios ofrecidos por la red. El esquema posible de este concepto se puede ver a continuación

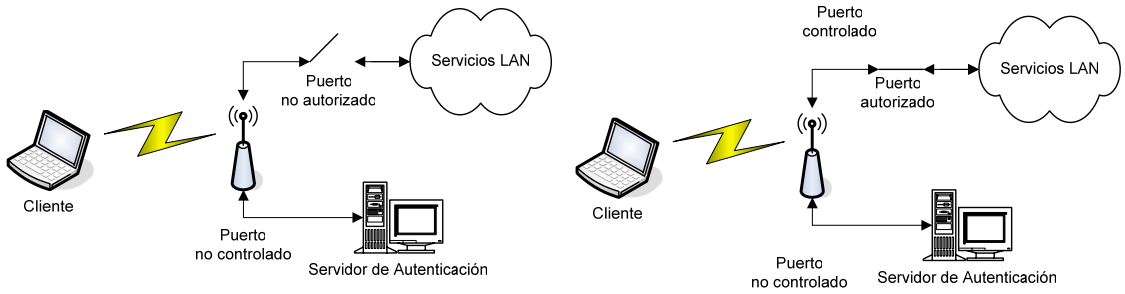


***Figura 5. Esquema puerto inhabilitado/habilitado 802.1x***

En sistemas con 802.1x activado, se generarán 2 llaves, la llave de sesión (pairwise key) y la llave de grupo (groupwise key). Las llaves de grupo se comparten por todas las estaciones cliente conectadas a un mismo punto de acceso y se utilizarán para el tráfico multicast, las llaves de sesión serán únicas para cada asociación entre el cliente y el punto de acceso y se creará un puerto privado virtual entre los dos.

El estándar 802.1x mejora la seguridad proporcionando las siguientes mejoras sobre WEP:

- Modelo de seguridad con administración centralizada
- La llave de encriptación principal es única para cada estación, por lo tanto, el tráfico de esta llave es reducido (no se repite en otros clientes).
- Existe una generación dinámica de llaves por parte del AS (Authentication Server), sin necesidad de administrarlo manualmente.
- Se aplica una autenticación fuerte en la capa superior.

- **TKIP (Temporal Key Integrity Protocol)**

Con este protocolo se pretende resolver las deficiencias del algoritmo WEP y mantener la compatibilidad con el hardware utilizado actualmente mediante una actualización del firmware.

El protocolo TKIP está compuesto por los siguientes elementos:

- Un código de integración de mensajes (MIC) encripta el checksum incluyendo las direcciones físicas (MAC) de origen y destino y los datos en texto claro de la trama 802.11. Esta medida protege contra los ataques por falsificación.
- Contramedidas para reducir la probabilidad de que un atacante pueda aprender o utilizar una determinada llave.
- Utilización de un IV (vector de inicialización) de 48 bits llamado TSC (TKIP Sequence Counter) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden.

La estructura de encriptación TKIP propuesta por 802.11i es la siguiente:

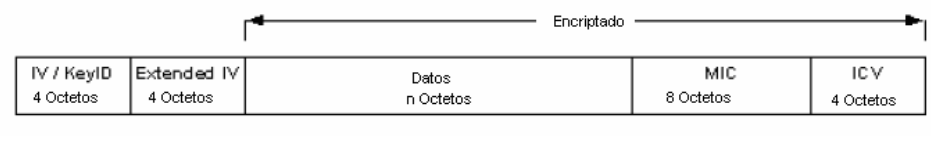


***Figura 6. Estructura de encriptación TKIP***

La utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de redecodificar la llave temporal durante una sola asociación. Pueden intercambiarse $2^{48}$ paquetes utilizando una sola llave temporal antes de ser re-usada. El proceso de encapsulación TKIP se muestra a continuación:

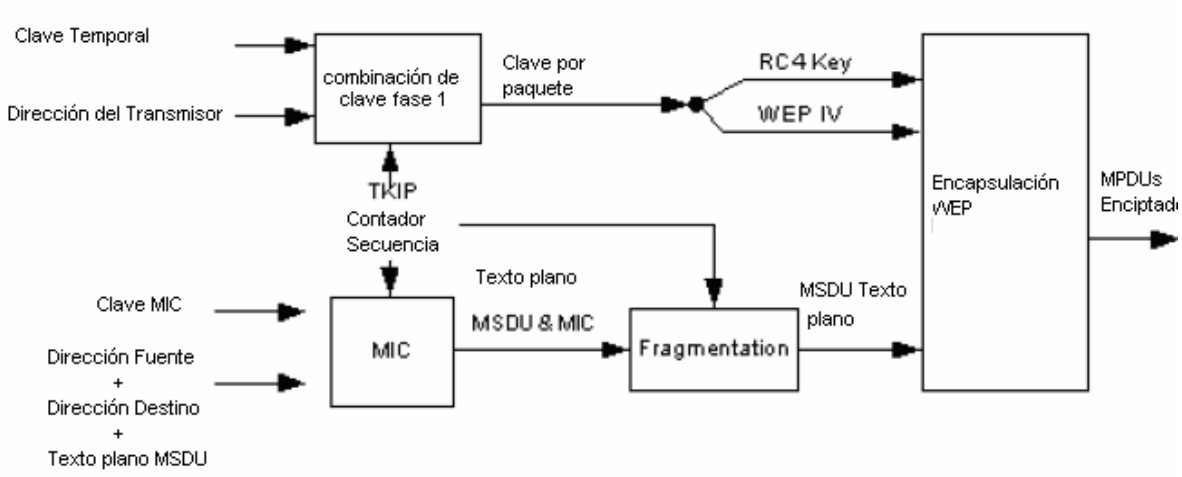


***Figura 7. Proceso de encapsulación TKIP***

Se combinan en dos fases la llave temporal, la dirección del emisor y el TSC para la obtención de una llave de 128 bits por paquete, dividido en una llave RC4 de 104 bits y en una IV de 24 bits para su posterior encapsulación WEP.

El MIC final se calcula sobre la dirección física origen y destino y el MSDU (MAC Service Data Unit o texto plano de los datos en la trama 802.11) después de ser segmentado por la llave MIC y el TSC.

La función MIC utiliza una función *hash* unidireccional, si es necesario, el MSDU se fragmenta incrementando el TSC para cada fragmento antes de la encriptación WEP.
En la desencripción se examina el TSC para asegurar que el paquete recibido tiene el valor TSC mayor que el anterior. Sino, el paquete se descartará para prevenir posibles ataques por repetición. Después de que el valor del MIC sea calculado basado en el MSDU recibido y desencriptado, el valor calculado del MIC se compara con el valor recibido.

- **CCMP (Counter Mode with CBC-MAC Protocol)**

Este protocolo es complementario a TKIP y representa un nuevo método de encripción basado en AES (Advanced Encryption Standards), cifrado simétrico que utiliza bloques de

128 bits, con el algoritmo CBC-MAC. Así como el uso del TKIP es opcional, la utilización del protocolo CCMP es obligatorio si se está utilizado 802.11i (WAPv2). En la figura 8 se puede observar el formato tras la encriptación CCMP:

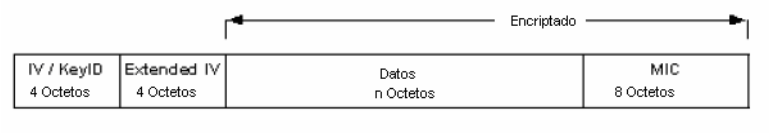


***Figura 8. Estructura de encriptación CCMP***

CCMP utiliza un IV de 48 bits denominado Número de Paquete (PN) utilizado a lo largo del proceso de cifrado, junto con la información para inicializar el cifrado AES para calcular el MIC y la encriptación de la trama.

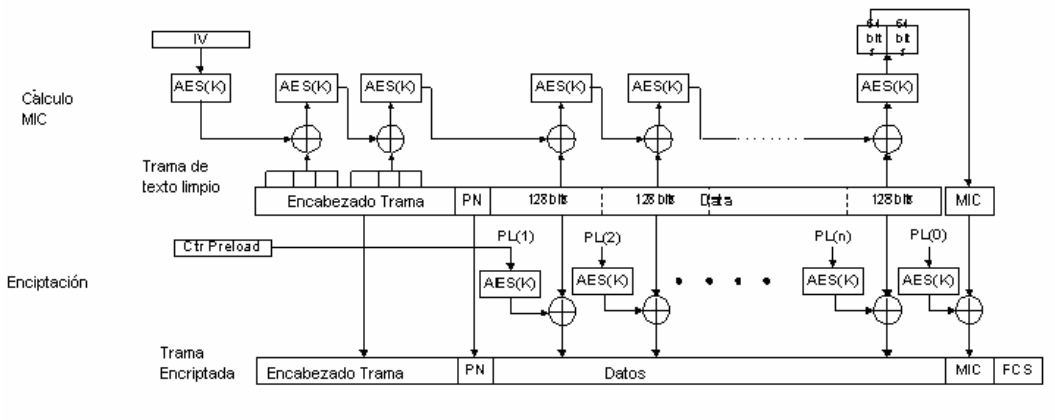


***Figura 9. Proceso de encriptación CCMP***

El proceso de encriptación CCMP, la encriptación de los bloques utiliza la misma llave temporal tanto para el cálculo del MIC como para la encriptación del paquete. Como el TKIP, la llave temporal se deriva de la llave principal obtenida como parte del intercambio en 802.1x. Como se puede observar en la figura 9, el cálculo del MIC y la encriptación se realiza de forma paralela. El MIC se calcula a partir de un IV formado por el PN y datos extraídos del encabezado de la trama. El IV se convierte en un bloque AES y su salida a través de la operación XOR conformará el siguiente bloque AES.