Sistemas de seguridad en redes inalámbricas: WEP, WAP y WAP2

acens
the Cloud hosting company

Calle San Rafael, 14
28108 Alcobendas (Madrid)
902 90 10 20
www.acens.com

Introducción

Actualmente una de las formas más utilizadas para conectarse a Internet es por medio de una conexión WiFi, un sistema que ofrece al usuario importantes ventajas respecto a la conexión mediante cable, como por ejemplo movilidad, facilidad de instalación, amplia cobertura, etc. Pero este sistema tiene también inconvenientes, y uno de ellos hay que tenerlo muy en cuenta: la seguridad de nuestra red.

Entre los principales problemas que nos podemos encontrar con las redes WiFi está el robo del ancho de banda, una situación que se puede dar habitualmente si no se toman medidas. También tenemos que tener en cuenta que si disponemos de una conexión sin cifrar, la información que circula por esa red lo hará de forma pública, por lo que cualquier usuario que se encuentre en el espacio cubierto por la red podría capturar esa información, haciendo uso de unas simples aplicaciones.

Para resolver estos problemas de seguridad que presenta una red inalámbrica, tendremos que usar algún sistema de cifrado que requiera de algún tipo de credencial para poder navegar por esa red. A lo largo de este White Paper analizaremos los distintos sistemas que nos podemos encontrar en la actualidad.

Cifrado WEP (Wired Equivalent Privacy)

El sistema de cifrado WEP fue el primero que apareció para solucionar los problemas generados por las redes abiertas. Se trata de un sistema de cifrado que funciona mediante la autenticación del usuario con contraseña. De esta forma el tráfico viaja cifrado, y aquel usuario que se encuentre escuchando el tráfico sólo leerá caracteres sin sentido alguno, a no ser que tenga la clave de cifrado.

Este sistema de cifrado está basado en el algoritmo de cifrado RC4, utilizando para ello claves de 64 o de 128 bits. Cada clave consta de dos partes, una de ellas la tiene que configurar el usuario en cada uno de los puntos de acceso de la red, mientras que la otra se genera automáticamente y se denomina vector de inicialización, cuyo objetivo es obtener claves distintas para cada trama que se mueve en la red.

Inicialmente se creía que se trataba de un cifrado muy seguro, pero pronto se descubrió que no era así, demostrando que ofrece muchas debilidades.

Entre las principales debilidades de este sistema está que las claves permanecen siempre estáticas, y por otro lado los 24 bits del vector de inicialización son insuficientes, además de transmitirse sin cifrar.

Hoy en día es considerado un sistema poco seguro y no se aconseja su utilización en las redes inalámbricas, ya que se puede llegar a romper su seguridad mediante distintos sistemas como fuerza bruta o el ataque FMS.

Cifrado WPA (Wi-Fi Protected Access)

Este sistema de cifrado surgió para solucionar los problemas de seguridad que ofrecía el sistema WEP. Para ello hace uso de TKIP, un protocolo para gestionar las claves dinámicas, que resuelve muchos de los problemas que tenía WEP tales como la longitud de la clave, el cambio de la clave de estática a dinámica y la multidifusión.

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante una clave precompartida, que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

WPA permite diferentes sistemas de control de acceso incluyendo la validación de usuario, como puede ser contraseña, certificado digital o simplemente hacer uso de una contraseña compartida para identificarse. Algunos sistemas son:

WPA-PSK

Se trata del sistema de control de acceso más simple tras WEP y consiste en un sistema de clave compartida, clave formada entre 8 y 63 caracteres. Es un sistema fácil de utilizar y configurar y el más recomendable **para entornos familiares o pequeñas empresas**. Cualquier equipo que tenga esta clave podrá conectarse a la red.

Este sistema de acceso tiene el problema de que al basarse en el uso de claves, ésta se puede identificar por medio del uso de la fuerza bruta, es decir, ir comprobando distintas claves hasta dar con la correcta, de ahí que sea fundamental utilizar claves complejas alfanuméricas.

WPA Empresarial

Se trata de un sistema más complejo y el que deberían adoptar aquellas empresas que hacen uso de las redes inalámbricas. Funciona mediante el uso de usuario y contraseña o sistemas de certificados. Se suele utilizar con equipos de gran potencia como servidores, para la gestión de usuario o certificados.

Dentro de este tipo de sistemas se puede aumentar más la seguridad haciendo uso de otros mecanismos como EAP-TLS, EAP-TLLs y PEAP.

Es un sistema muy recomendado **para aquellos entornos empresariales donde la seguridad es de vital importancia**.

Cifrado WPA2

WPA2 soluciona los problemas de vulnerabilidad detectados en la primera versión (WPA), e incorpora todas las características del estándar IEEE 802.11i (WAP no lo hacía).

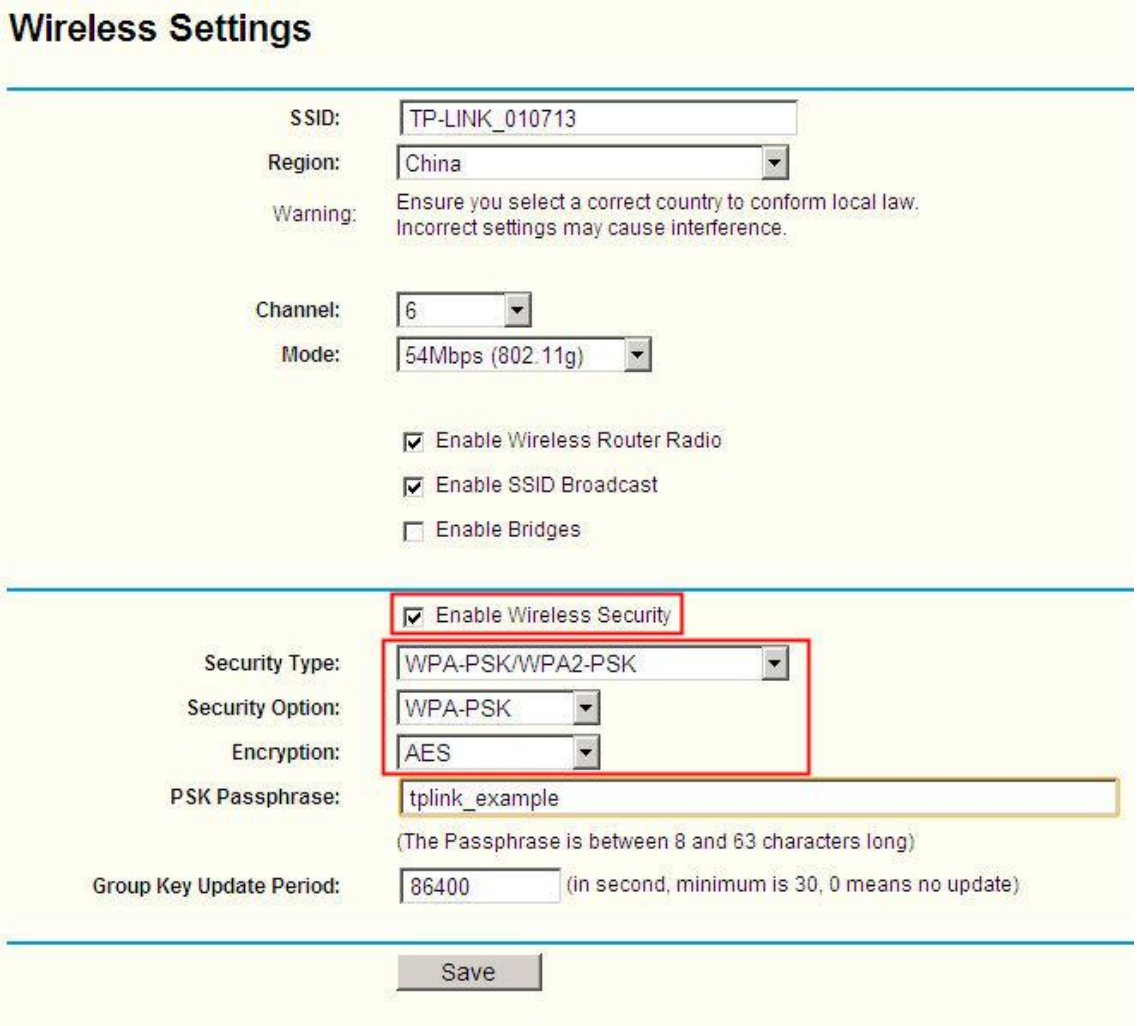
Este sistema presenta dos cambios principales respecto a WPA:

- El reemplazo del algoritmo Michael por un código de autenticación conocido como el protocolo "Counter-Mode/CBC-Mac" que es considerado criptográficamente seguro.
- Reemplazo del algoritmo RC4 por el algoritmo AES, uno de los más seguros actualmente.

Tiene el inconveniente de que **no todos los routers permiten este tipo de cifrado**, además de no ser compatible con el sistema WAP.

Configuración del sistema de seguridad en redes inalámbricas

El proceso de asignación de una clave a nuestra conexión inalámbrica dependerá del tipo de router que tengamos. En menú de configuración del router estará localizada una sección con un nombre del estilo de "Wireless settings" o “Ajustes/preferencias wifi”, y la interfaz de configuración tendrá una apariencia similar a la imagen que os mostramos a continuación.



En ese formulario lo importante es lo resaltado, donde indicamos que queremos activar la seguridad para nuestra red inalámbrica, eligiendo el tipo de sistema de seguridad (en el caso de la imagen el sistema WPA-PSK) y el tipo de encriptación. Además tendremos que indicar la contraseña que utilizaremos. En el ejemplo de arriba, esta clave se mete en el campo llamado “PSK Passphrase”.

También es importante que sepáis que si tenéis un modelo de router antiguo es probable que no permita configurar algunos sistemas de codificación.

Además de lo comentado anteriormente, para disfrutar de una conexión inalámbrica segura es muy recomendable hacer uso de otras medidas de seguridad, como el uso de cortafuegos o indicar qué direcciones IP tendrán acceso al router.