Configuración manual con DHCP de redes WLAN protegidas con WPA y WPA2 en Debian GNU Linux 7.9

Eugenia Bahit[i]
(LAECI) Laboratorio de Altos Estudios en Ciencias Informáticas

Resumen

Cuando se intenta configurar una red de área local inalámbrica (WLAN) de forma manual con los procedimientos tradicionales más difundidos, se obtiene un fallo crítico que arroja un mensaje *«error for wireless request "set encode" (8b2a)»* si el punto de acceso inalámbrico (WAP) protege la red con sistemas WPA o WPA2. Esto, se debe a que los procedimientos tradicionales basan su método de configuración en redes protegidas con el antiguo sistema de protección WEP declarado obsoleto hace más de una década, a raíz de sus conocidas debilidades criptográficas. Este estudio se concentró en entender el funcionamiento exacto de las redes inalámbricas, sus protocolos, sistemas de protección y mecanismos de transmisión de datos, para obtener así, el procedimiento más adecuado para lograr una configuración propicia cuando se prescinde por completo del entorno gráfico.

Palabras clave:

debian, linux, wlan, wap, dhcp, udp, wpa, wpa2, wep, wifi, wireless, inalámbrica, red, network, 8b2a, aes, tplink, tl-wdr3500, enuwi-g2

Introducción

WLAN *(Wireless Local Area Network)* o Red de Área Local inalámbrica es un sistema de conexión inalámbrico (no cableado) a una red de área local.

En una red local, cada WLAN accede de forma inalámbrica a un mismo **WAP** *(Wireless Access Point* o *punto de acceso inalámbrico*), un dispositivo de red que conecta a estas inalámbricas con el punto de acceso (AP) de la red cableada.

Un WAP contiene una lista de direcciones IP que, si el dispositivo lo soporta, pueden ser asignadas a cada una de las estaciones WLAN de forma dinámica mediante un servidor **DHCP** provisto por el WAP. DHCP es un protocolo de configuración dinámica de *host*, basado en una arquitectura cliente-servidor.

El protocolo de red DHCP permite a los clientes de una misma red obtener parámetros de configuración de forma automática. El servidor DHCP, posee una lista de direcciones IP que van siendo asignadas de forma dinámica a cada dispositivo cliente que se conecta a la red.

Los clientes DHCP transmiten los **datagramas** (paquetes de datos, compuestos de una cabecera de control y sus correspondientes datos asociados) al servidor DHCP, mediante el protocolo **UDP** *(User Datagram Protocol)*. UDP es un protocolo sencillo de bajo coste, que permite la transmisión directa de datagramas en la red, sin mediar conexión previa establecida, ni control del flujo de datos. A diferencia de **TCP**, UDP prioriza la velocidad de transmisión, sobrecargando cada segmento del paquete de datos con solo 8 bytes de información adicional, contra los 20 que emplea TCP, puesto que este último, tiene su máxima prioridad en la fiabilidad de los datos y no en la velocidad.

Por otra parte, los puntos de acceso inalámbricos establecen mecanismos de protección para la red, cifrándola con diferentes algoritmos.

El primero de estos sistemas de cifrado, fue **WEP** *(Wired Equivalent Privacy)* -declarado obsoleto hace más de una década-, quien cifraba la información transmitida a través de las redes inalámbricas empleando claves de 64 y 128 bits. Producto de ciertas debilidades criptográficas, el sistema fue reemplazado por **WPA** *(Wi-FI Protected Access* o *Acceso Wi-Fi Protegido)* y ratificado posteriormente por el estándar final, conocido como **WPA2** que, a diferencia de su versión inicial, emplea el algoritmo de cifrado **AES** *(Advanced Encryption Standard),* el más avanzado para la seguridad inalámbrica, adoptado como estándar por el Gobierno de Estados Unidos.

Materiales y Métodos

Equipo empleado

- *Cablemódem* conectado con un cable de red RJ45 a un *router* «TP-LINK N600 Wireless Dual Band Router», SKU nro. TL-WDR3500 (código fuente del *firmware* disponible bajo licencia GPL v3.0).
- Ordenador portátil antiguo con arquitectura de 32bits y un adaptador genérico, USB 2.0 inalámbrico 802.11g marca ENCORE Electronics, SKU nro. ENUWI-G2.
- Sistema Operativo Live (USB *bootable*), Debian GNU/Linux 7.9 standard (sin entorno gráfico).

Obsérvese que el total de las pruebas se efectuó directamente desde un dispositivo USB, ejecutando la versión Live del sistema operativo estándar, sin instalación previa ni configuraciones automáticas.

Procedimiento

1. Obtención del nombre de interfaz.

Por defecto, no existiendo más de un dispositivo *wireless*, el nombre de la interfaz es wlan0 y dependiendo de la cantidad de dispositivo, se incrementa el entero en el nombre de la interfaz. Para mayor seguridad, se ejecutó el comando *iwconfig*.

> *Obsérvese que al extraer el dispositivo USB inalámbrico, el comando iwconfig no se encontraba disponible.*

2. Puesta en línea de la interfaz

```
ifconfig <interfaz> up
```

3. Obtención del SSID de la red inalámbrica (o redes) disponible/s

```
iwlist <interfaz> scan | grep -i essid
```

4. Creación de archivo de configuración con clave cifrada para la conexión WPA/WPA2

```
wpa_passphrase <ssid> <clave> > /path/to/wpa.conf
```

> *La clave debe indicarse en ASCII o hexadecimal. En la prueba se utilizó solo ASCII.*

5. Establecimiento de la conexión WPA/WPA2

```
wpa_supplicant -B -i <interfaz> -c /path/to/wpa.conf -D <driver>
```

> *Obsérvese que durante las pruebas, se utilizó el driver genérico para Linux wext. Alternativamente, otros dos drivers se encuentran disponibles. Consulte wpa_supplicant man para más información.*

6. Obtención automática de una IP mediante DHCP

```
dhclient <interfaz>
```

Resultados

Tras los pasos descritos, se procedió a verificar la IP asignada y el enrutamiento de la misma mediante la ejecución de los siguientes comandos:

```
ip addr show <interfaz>
ip route show
```

La salida de ambos comandos arrojó resultados favorables habiendo podido comprobarse la asignación de una IP de red local, así como el punto de acceso que originó la misma.

Para comprobar la salida efectiva a Internet, se efectuó un *ping* a diversos sitios Web e IP de acceso público, arrojando todos ellos resultados positivos.

i

Eugenia Bahit – LAECI (Laboratorio de Altos Estudios en Ciencias Informáticas)

483 Green Lanes. London, N13 4BS (UK)