Apéndice H – Actualización de *Firmware* para D-link (DIR-300)

H1. Generalidades

La actualización de *Firmware* es obligatoria si no se cuenta con el soporte de 802.11i en los APs, es decir, no se puede configurar las funcionalidades de cifrado avanzado como AES ni la autenticación 802.1x/EAP. Para sobrepasar esta dificultad y debido a que los APs del mercado que tienen estas características son muy costosos, se decidió que lo mejor era actualizar el *Firmware* de un dispositivo asequible en el mercado colombiano. Para este fin se eligió el *router* D-LINK DIR300 y como *firmware* se eligió el DD-WRT que es libre y brinda las características antes mencionadas. El trabajo fue largo y tedioso ya que para cada marca y referencia de dispositivo hay procesos totalmente específicos, además, luego de tratar con varias versiones del *firmware* algunas deshabilitaban opciones de enrutamiento necesarias o no funcionaban bien. Se debe tener muy presente que la mala instalación y/o actualización de *firmware* puede dejar totalmente inservible el punto de acceso sin posibilidad de recuperar el *firmware* original con toda su funcionalidad.

Luego de realizar diferentes pruebas con varias versiones del *firmware* DD-WRT se optó por dejar instalada la versión de prueba DD-WRTv24 RC4, la cual se ensayo para todos los requerimientos de la parte experimental y funcionó correctamente para todas las pruebas que se realizaron.

H2. Requerimientos

Para una correcta instalación de este *firmware* se necesitan los siguientes archivos [1]:

- *Router* D-LINK DIR 300
- Computador con tarjeta de red 802.3 (Ethernet)
- Cable de red UTP Cat5
- Ap61.ram (*Redboot* temporal)
- Ap61.rom
- Root.fs
- Cualquier servidor TFTP (en este caso se usó PumpKin)
- Un cliente telnet (en este caso se usó Putty)

Se inicia el servidor TFTP y se revisa la lista de archivos de todos los archivos antes mencionados ya que son necesarios a lo largo de los pasos que siguen a continuación.

A continuación se detalla el proceso para la actualización del *firmware.*

H3. Acceso al *Redboot* original

1). Se desconecta el punto de acceso de la red cableada.

2). Se conecta un cable UTP cat 5E en el puerto WAN del punto de acceso D-LINK DIR 300.
3). Se configura el computador con la dirección IP 192.168.20.80/255.255.255.0.

4). Se presiona el botón de *reset* del punto de acceso durante 30 segundos mientras se reinicia.
5). Durante los primeros 5 segundos de conexión[1] se ejecuta un servicio de telnet a la dirección 192.168.20.81 en el puerto 9000:

```
"telnet 192.168.20.81:9000"
```

6). Si las anteriores indicaciones se realizaron con éxito se ingresa al siguiente *prompt*, *RedBoot>*

H4. Instalación del *Bootloader*

Una vez en este *prompt,* se debe cargar *el boot* temporal mediante los siguientes pasos:

```
1. RedBoot> load ap61.ram
           Using default protocol (TFTP)
           Entry point: 0×800410bc, address range: 0×80041000-0×800680d8
2. RedBoot> go
```

En este punto es normal si se desconecta del *prompt*

H5. Instalación del nuevo *Bootloader*

Para conectarse ahora al *boot* temporal, se desconecta el cable de red del puerto WAN del punto de acceso y se conecta a cualquiera de los puertos LAN del mismo, luego se debe cambiar la dirección IP del dispositivo de red del computador a 192.168.1.2; si se realizó correctamente la instalación del nuevo *boot* será posible la conexión al *boot* temporal a través de un telnet a la dirección 192.168.1.1 en el puerto 9000.

```
"telnet 192.168.20.81:9000"
DD-WRT>
```

Una vez en el *prompt* de DD-WRT seguimos los siguientes pasos:

```
DD-WRT> fconfig –i
Initialize non-volatile configuration - continue (y/n)? *Se pulsa la tecla Y
Run script at boot: false
Use BOOTP for network configuration: true
Default server IP address:
Console baud rate: 9600
GDB connection port: 9000
Force console for special debug messages: false
Network debug at boot time: false
Update RedBoot non-volatile configuration - continue (y/n)? *Se pulsa la tecla Y
… Erase from 0xbffe0000-0xbfff0000: .
… Program from 0×80ff0000-0×81000000 at 0xbffe0000: .
DD-WRT> fis init
About to initialize [format] FLASH image system - continue (y/n)? *Se pulsa Y
```

[1] Para saber esto, puede realizar un ping sostenido a la dirección en mención y apenas obtenga respuesta hacer el telnet.

```
*** Initialize FLASH Image System
… Erase from 0xbffe0000-0xbfff0000: .
… Program from 0×807f0000-0×80800000 at 0xbffe0000: .

DD-WRT> ip_address -h 192.168.1.2
Default server: 192.168.1.23

DD-WRT> load -r -b %{FREEMEMLO} ap61.rom
Using default protocol (TFTP)
Raw file loaded 0×80080000-0×800a8717, assumed entry at 0×80080000
DD-WRT> fis create -l 0×30000 -e 0xbfc00000 RedBoot
An image named 'RedBoot' exists - continue (y/n)? *Se pulsa la tecla Y
… Erase from 0xbfc00000-0xbfc30000: …
… Program from 0×80080000-0×800a8718 at 0xbfc00000: …
… Erase from 0xbffe0000-0xbfff0000: .
… Program from 0×807f0000-0×80800000 at 0xbffe0000: .
DD-WRT> reset
```

H6. Instalación del nuevo *Firmware*

En éste proceso es importante no desconectar por ningún motivo el punto de acceso porque el dispositivo puede quedar inservible totalmente, al ejecutar el comando `fis create` en el `prompt` su respuesta puede demorarse un, no se debe interrumpir el proceso por ningún motivo.

A continuación se detallan los pasos a seguir:

```
DD-WRT> ip_address -h 192.168.1.2
Default server: 192.168.1.2

DD-WRT> load -r -b 0×80041000 root.fs
Using default protocol (TFTP)
Raw file loaded 0×80041000-0×802effff, assumed entry at 0×80041000
DD-WRT> fis create -b 0×80041000 -f 0xbfc30000 -l 0×002C0000 -e 0×00000000 rootfs
… Erase from 0xbfc30000-0xbfef0000: ……..
… Program from 0×80041000-0×80301000 at 0xbfc30000: ……..
… Erase from 0xbffe0000-0xbfff0000: .
… Program from 0×80ff0000-0×81000000 at 0xbffe0000: .
DD-WRT> load -r -b 0×80041000 vmlinux.bin.l7
Using default protocol (TFTP)
Raw file loaded 0×80041000-0×80100fff, assumed entry at 0×80041000
DD-WRT> fis create -r 0×80041000 -e 0×80041000 -l 0×000E0000 vmlinux.bin.l7
… Erase from 0xbfef0000-0xbffd0000: ……..
… Program from 0×80041000-0×80101000 at 0xbfef0000: ……
… Erase from 0xbffe0000-0xbfff0000: .
… Program from 0×80ff0000-0×81000000 at 0xbffe0000: .
DD-WRT> fis create -f 0xbffD0000 -l 0×00010000 -n nvram
… Erase from 0xbffe0000-0xbfff0000: .
… Program from 0×80ff0000-0×81000000 at 0xbffe0000: .
DD-WRT> fconfig boot_script true
boot_script: Setting to true
Update RedBoot non-volatile configuration - continue (y/n)? y
… Erase from 0xbffe0000-0xbfff0000: .
… Program from 0×80ff0000-0×81000000 at 0xbffe0000: .
DD-WRT> fconfig boot_script_timeout 3
boot_script_timeout: Setting to 3
Update RedBoot non-volatile configuration - continue (y/n)? y
… Erase from 0xbffe0000-0xbfff0000: .
… Program from 0×80ff0000-0×81000000 at 0xbffe0000: .
DD-WRT> fconfig
Run script at boot: true
```

```
Boot script:
Enter script, terminate with empty line
>> fis load -l vmlinux.bin.l7
>> exec
>>
Boot script timeout (1000ms resolution): 3
Use BOOTP for network configuration: false
Gateway IP address:
Local IP address:
Local IP address mask:
Default server IP address:
Console baud rate: 9600
GDB connection port: 9000
Force console for special debug messages: false
Network debug at boot time: false
Update RedBoot non-volatile configuration - continue (y/n)? y
… Erase from 0xbffe0000-0xbfff0000: .
… Program from 0×80ff0000-0×81000000 at 0xbffe0000: .
DD-WRT> fconfig bootp false
DD-WRT> reset
```

Para Finalizar se reinicia y se prueba creando una cuenta inalámbrica y se verifica el correcto transporte de información. A continuación se muestra en las figuras H1 y H2 imágenes de las interfaces tanto original como con el nuevo *firmware* en el dispositivo DIR 300.

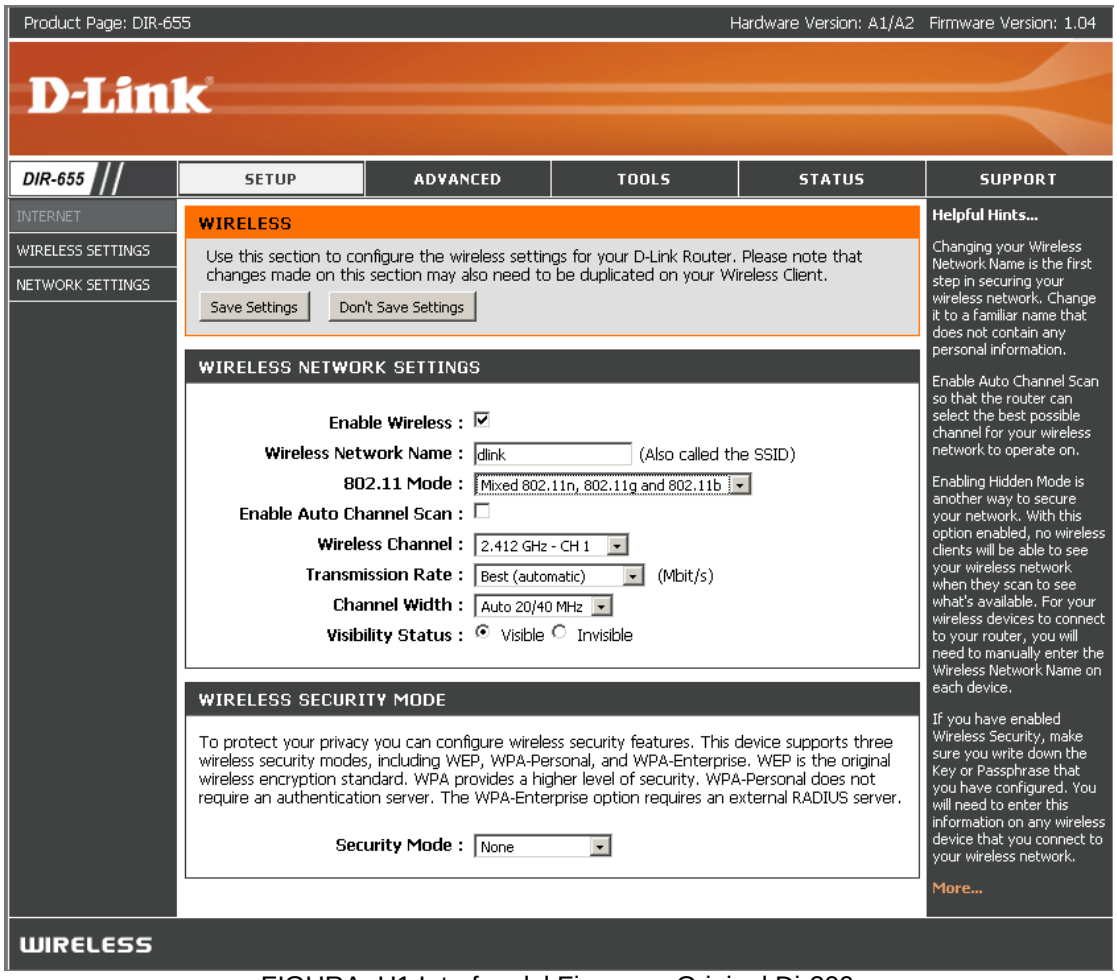

FIGURA H1 Interfaz del Firmware Original Dir300

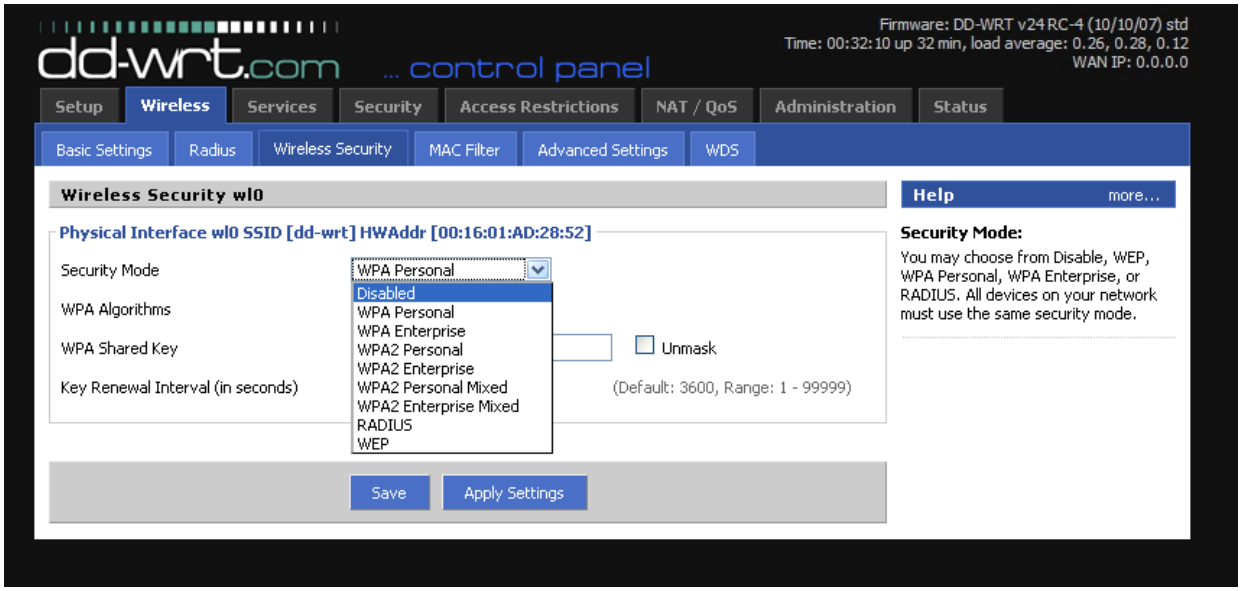

FIGURA H2 Interfaz del Firmware DD-WRT

REFERENCIAS BIBLIOGRÁFICAS

[1] Shadowandy, 2007, Disponible en: <http://www.shadowandy.net/2007/09/mini-flashing-guide-for-dir-300.htm>