

Configuración de redes WiFi: Sistema de Distribución Inalámbrico (WDS)

1. Objetivos de la práctica

En esta práctica se propone que los alumnos, mediante el uso de dos puntos de acceso, configuren un puente inalámbrico y sean capaces de comunicar dos PCs a través de este. Además, se comprobará que es posible interceptar el tráfico desde un tercer equipo. La figura 1 muestra la topología de red a implementar.



Figura 1: Topología de la red

2. Wireless Distribution System (WDS)

WDS es una parte del estandar IEEE 802.11 concerniente a la interconexión inalámbrica entre puntos de acceso.

WDS permite la creación de una troncal de red inalámbrica de una manera sencilla, evitando el uso de tecnologías cableadas, lo que puede conllevar ciertas desventajas como la dificultad de instalación o un mayor coste económico. A nivel doméstico nos puede permitir extender el rango de cobertura de una red inalámbrica para reforzar la señal en zonas en las que la intensidad recibida es muy debil o nula.

Sin embargo, WDS presenta diversos inconvenientes. En primer lugar, el ancho de banda disponible si se usa el modo híbrido (puente y punto de acceso) disminuye considerablemente. Además, pese a ser un estándar, WDS no está completamente definido, por lo que existen problemas de incompatibilidad entre dispositivos (incluso del mismo fabricante).

Los puntos de acceso de un sistema WDS pueden operar de dos modos: repetidor (*repeater mode*), si aceptan que las estaciones cliente se conecten, y puente (*bridge mode*), si no aceptan conexiones de clientes. En ambos casos los puntos de acceso pueden utilizarse como puente para conectar entre ellos.

3. Inicio de la práctica

En esta práctica se emplearán puntos de acceso domésticos (*Access Point* o AP) del modelo Asus WL-500G Premium v1 con firmware DD-WRT (en realidad serán dispositivos con funcionalidades de router y punto de acceso integradas por lo que emplearemos indistintamente cualquiera de las dos denominaciones dependiendo del contexto).

Al comienzo de la práctica resetearemos los routers a la configuración por defecto. Para ello, enchufar el router y mantener presionado el botón “Restore” (parte trasera del dispositivo), durante unos 20 s, hasta que la luz frontal de “Power” parpadee. Una vez hecho esto desconectar de la corriente eléctrica y volver a conectar para comenzar a trabajar.

4. Configuración WDS

En primer lugar, conectaremos cada PC a un router desconectando el cable amarillo de la roseta de la pared y conectándolo al router. El PC deberá recibir una dirección IP en la red 192.168.1.0/24 por DHCP desde el router. Si no es así, aseguraos de que está activada la conexión “DCLAN eth1-DHCP” en el “Network Manager” (icono en el panel superior).

Accederemos a la interfaz web de configuración de los routers con las siguientes credenciales (la figura 2 muestra el aspecto de la interfaz DD-WRT):

- Dirección: 192.168.1.1
- Usuario: admin
- Contraseña: admin

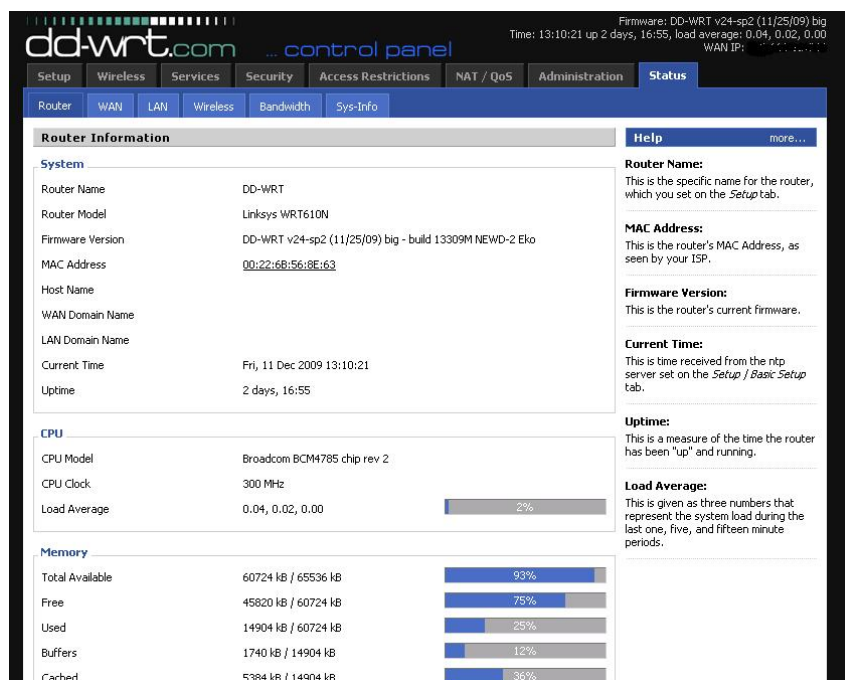


Figure 2: Pantalla de inicio de DD-WRT

4.1. Deshabilitar el servicio DHCP en el router secundario

Solo uno de los routers de la red puede servir direcciones (router primario). Por tanto, deshabilitaremos el servicio DHCP del router secundario. Además, para garantizar el acceso, la dirección IP del router secundario la estableceremos como estática.

Para establecer los parametros adecuados del router secundario nos dirigiremos a la pestaña “Setup” y le asignaremos al router la IP local “192.168.1.2”. Además, cambiaremos “DHCP Type” a “Forwarder” y le asignaremos la dirección correspondiente del router primario (192.168.1.1) que actuará de servidor. Para acabar, guardar cambios (no pulseis “Apply settings” hasta más adelante ya que correis el riesgo de que el PC pierda la IP ya que, en este momento, no tiene acceso a ningun servidor DHCP). La configuración se puede apreciar en la figura 3.

Network Setup				
Router IP				
Local IP Address	192	168	1	2
Subnet Mask	255	255	255	0
Gateway	0	0	0	0
Local DNS	0	0	0	0
Network Address Server Settings (DHCP)				
DHCP Type	DHCP Forwarder			
DHCP Server	192	168	1	1

Figura 3: Desactivar el servicio DHCP

4.2. Configuración del SSID (en ambos puntos de acceso)

WDS no obliga a que los SSID de cada AP del sistema de distribución sean los mismos si operan en modo repetidor, pero es recomendable (ello hará que la movilidad sea más cómoda y sin interrupciones). Sin embargo, en caso de usar un AP en modo puente, el SSID deberá ser el mismo en todos los dispositivos que interconecte. Además, el canal de comunicación tendrá que ser también necesariamente compartido (mismo número) ya que los AP solo disponen de un interfaz.

En la figura 4 se puede observar un ejemplo de configuración. Así, cada grupo de trabajo escogerá un SSID propio, y un número de canal de manera aleatoria. Esta configuración se encuentra en el apartado “Wireless”, donde además se configurará “Wireless Mode” como “AP” y “Wireless Network Mode” en “Mixed”. Tras esto, guardaremos los cambios.

Wireless Physical Interface w10

Physical Interface w10 - SSID [dd-wrt] HWAddr [00:1F:C6:82:21:F3]

Wireless Mode: AP

Wireless Network Mode: Mixed

Wireless Network Name (SSID): dd-wrt

Wireless Channel: 6 - 2.437 GHz

Wireless SSID Broadcast: ☒ Enable ☐ Disable

Sensitivity Range (ACK Timing): 2000 (Default: 2000 meters)

Network Configuration: ☐ Unbridged ☒ Bridged

Figura 4: Configuración inalámbrica

4.3. Configuración del puente WDS (en ambos routers)

En primer lugar se debe averiguar la dirección MAC inalámbrica de cada uno de los AP. Esta se puede averiguar en dos lugares diferentes: en la ventana inicial de DD-WRT (<http://192.168.1.1>), o bien, en la pestaña “WDS” de la sección “Wireless”.

Para conseguir que los APs se conecten mediante WDS hay que introducir la dirección MAC del otro dispositivo en la pestaña “WDS” dentro de “Wireless” y seleccionar LAN en el menú desplegable. Se puede observar un ejemplo en la figura 5. Aseguraos de que todos los parámetros introducidos son correctos y pulsad “Apply settings” para que todos los cambios tengan efecto.

Wireless Distribution System

WDS Settings

Wireless MAC: 00:1F:C6:82:21:F3

LAN	00	1F	C6	51	33	F4	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	

Extra Options

Lazy WDS: ☐ Enable ☒ Disable (Default: Disable)

WDS Subnet: ☐ Enable ☒ Disable

NAT: Disable

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Figura 5: Añadir direcciones MACs que forman parte del WDS.

Ejercicio 1

¿Por qué crees que ha sido necesario configurar las direcciones MAC entre ambos puntos de acceso?

Una vez hecho esto, ambos APs deberían poder comunicar entre ellos. En la pantalla inicial de DD-WRT encontraremos un gráfico indicando la calidad del enlace WDS que hemos creado (figura 6). Si todo ha ido bien la calidad deberá ser alta¹.

4.4. Prueba de funcionamiento

Se puede comprobar el correcto funcionamiento del puente WDS haciendo un ping desde uno de los PCs al otro y viceversa.

4.5. Monitorización de la comunicación

En este apartado vamos a comprobar el uso de los diferentes campos de la cabecera 802.11 en una conexión WDS.

Para capturar la información del canal inalámbrico se debe configurar el adaptador inalámbrico² en modo “Monitor”. Suponiendo que la interfaz inalámbrica USB sea “wlan0”³, los pasos a seguir son los siguientes:

- `sudo stop network-manager`
- `sudo ifconfig wlan0 down`
- `sudo iwconfig wlan0 mode monitor`
- `sudo ifconfig wlan0 up`
- `sudo iwconfig wlan0 channel <canal empleado>`
- `sudo airmon-ng start wlan0`

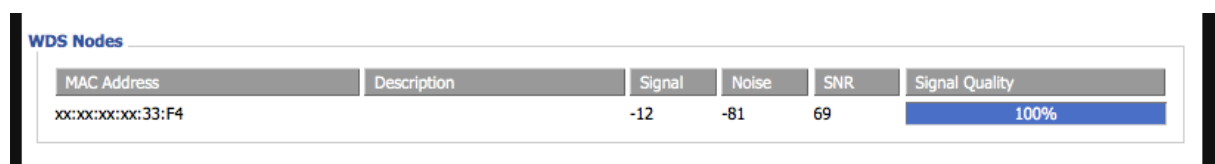
Tras la ejecución de este comando nos aparecerá una tabla con las aplicaciones que pueden interferir en la correcta captura de los paquetes. Si hemos desactivado el network-manager, los procesos restantes no deberían interferir en la captura de paquetes.

Comprobaremos que el sistema ha creado una nueva interfaz de tipo “mon”.

¹Este indicador puede tardar un poco a actualizarse. En cualquier caso debería activarse con el ping de la prueba de funcionamiento que sigue.

²Si no tienes un adaptador WiFi USB pídeselo al profesor.

³Comprueba el nombre de tu tarjeta con el comando “ifconfig -a”.



MAC Address	Description	Signal	Noise	SNR	Signal Quality
xx:xx:xx:xx:33:F4		-12	-81	69	100%

Figura 6: Calidad del enlace WDS (pantalla principal DD-WRT)

```
dcral@ubuntu:~/Desktop$ sudo airmon-ng start wlan0

Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
550      avahi-daemon
551      avahi-daemon
777      NetworkManager
2691     wpa_supplicant

Interface      Chipset      Driver
wlan0          Ralink 2573 USB rt73usb - [phy0]
               (monitor mode enabled on mon0)
```

Figura 7: Ejemplo de salida de la orden `airmon-ng start`.

4.6. Prueba de captura

En primer lugar lanzaremos el ping desde un PC al otro y lo dejaremos en ejecución permanentemente.

A continuación iniciaremos “wireshark”:

- `sudo wireshark`

Comenzaremos una captura seleccionando “Capture -> Interfaces” y haciendo click en “Start” en la línea del dispositivo “monX”. Detendremos la captura pasados unos 20 segundos.

Ejercicio 2

- Observad la lista de tramas capturadas. Comprobad que la mayoría de ellas pertenecen a la red de nuestro SSID.
- Seleccionad una trama cualquiera de tipo “Beacon” y examinad el apartado “802.11 Beacon Frame” de la trama ¿Podemos saber el origen de la trama?
- Filtrad aquellas cuyo origen o destino sea uno de nuestros PCs (filtro IEEE 802.11, campo “wlan.addr==MAC_PC_ETH”) y examinad alguna de ellas. ¿Están cifrados los datos que transportan?
- Filtrad por ICMP (escribiendo “ICMP” directamente en la caja de texto del filtro). ¿Cuál es la dirección MAC del origen de la trama? ¿Cuál es la dirección MAC del transmisor de la trama?

Como habéis visto cualquier atacante puede ver los datos que se intercambian entre 2 ordenadores en un enlace WDS. En la siguiente sección vamos a utilizar seguridad WEP para dificultar el acceso a los datos.

Wireless Security w10

Physical Interface w10 SSID [dd-wrt] HWAddr [00:1F:C6:82:21:F3]

Security Mode: WEP

Default Transmit Key: ☒ 1 ☐ 2 ☐ 3 ☐ 4

Encryption: 64 bits 10 hex digits

Passphrase: password

Key 1: F2C7BB35B9

Key 2: 858EDAB02E

Key 3: 27914293E5

Key 4: CE63E8FB8B

Figura 8: Configuración de cifrado.

5. Seguridad en WDS

Hasta ahora la conexión entre ambos routers no disponía de ningún mecanismo de seguridad, por lo que cualquier usuario malintencionado podría interceptar todo el tráfico que circule por ese enlace y tener accesos a los datos transportados. En caso de incorporar seguridad en un sistema de distribución inalámbrico, WDS obliga a utilizar el mismo método de cifrado y contraseña en todos los APs del sistema.

Respecto a los métodos de cifrado disponibles, actualmente WDS no permite el uso de WPA2, sino que solamente es posible configurar la seguridad con WPA y WEP. En esta práctica, y por motivos de sencillez, se empleará un cifrado WEP de 64 bits (pese a ser totalmente inseguro y nada aconsejable su uso en un entorno real).

5.1. Configuración de seguridad (en ambos routers)

Para configurar la seguridad, en ambos routers debemos dirigirnos al apartado “Wireless” y posteriormente a “Wireless Security”. En esta página seleccionaremos “Security mode” “WEP” y “Encryption” “64 bits 10 hex digits”. Además el grupo de prácticas deberá ponerse de acuerdo sobre qué “Passphrase” y “Default Transmit Key” emplear. Un ejemplo se puede observar en la figura 8. Aplicad los cambios.

Una vez se haya decidido y se hayan generado las claves es recomendable apuntar la “Key” empleada, ya que será usada posteriormente.

5.2. Prueba de funcionamiento

Comprueba que la configuración es correcta realizando un ping de un PC a otro.

5.3. Prueba de captura

Ahora vamos a comprobar que partes de las tramas 802.11 son cifradas por WEP. Además veremos como podemos descifrar el contenido usando wireshark.

En primer lugar lanzaremos el ping desde un PC al otro y lo dejaremos en ejecución permanentemente.

A continuación iniciaremos “wireshark”:

- `sudo wireshark`

Comenzaremos una captura seleccionando “Capture -> Interfaces” y haciendo click en “Start” en la línea del dispositivo “monX”. Detendremos la captura pasados unos 20 segundos.

Ejercicio 3

- Observad la lista de tramas capturadas. Comprobad que la mayoría de ellas pertenecen a la red de nuestro SSID.
- Seleccionad una cualquiera de las de tipo “Beacon” y examinad el apartado “802.11 Beacon Frame” de la trama ¿Podemos saber quién la envía? ¿Están cifradas este tipo de tramas?
- Filtrad aquellas cuyo origen o destino sea uno de nuestros PCs (filtro IEEE 802.11, campo “wlan.addr==MAC_PC_ETH”) y examinad alguna de ellas. ¿Cuántas tramas habéis encontrado? ¿Que datos contienen dichas tramas?
- ¿Que tramas estan cifradas? ¿Que tramas no lo están? ¿Que partes de la trama están cifradas? ¿Se filtra toda la trama?

5.4. Decodificación y análisis de la comunicación

Wireshark dispone de una opción para conseguir decodificar la información y saber qué datos contienen las tramas capturadas. Si hacemos click en “Edit -> Preferences” y posteriormente dentro de “Protocols” buscamos “IEEE 802.11”, llegaremos a una ventana similar a la que podeis observar en la figura 9. En esta ventana deberemos introducir en el campo “Key #1” la clave hexadecimal que apuntamos en el punto 4 (Atención: los bytes en hexadecimal deben ir separados mediante “:”).

Tras esto marcaremos “Enable decryption”, pulsaremos sobre “Aplicar” y cerraremos la ventana pulsando en “Aceptar”. Ahora los paquetes ya han sido descifrados y se pueden ver en la ventana principal de Wireshark, donde se pueden examinar las direcciones IP origen/destino, tipo de protocolo empleado, etc., así como los mensajes de aplicacion.

Ejercicio 4

- Observad de nuevo la lista de tramas capturadas. Volved a filtrar por ICMP. ¿Podéis ver el contenido ahora?
- Examinad las cabeceras IP e ICMP de las tramas que contienen los ping. Comprueba que las direcciones IP que figuran son las esperadas ¿Cuál es el tiempo de vida (TTL) de estos paquetes?
- Examinad las cabeceras MAC de las tramas que contienen los ping ¿Cuántas direcciones MAC se emplean en las comunicaciones a través del puente WDS? ¿Para que se usa cada una de ellas?

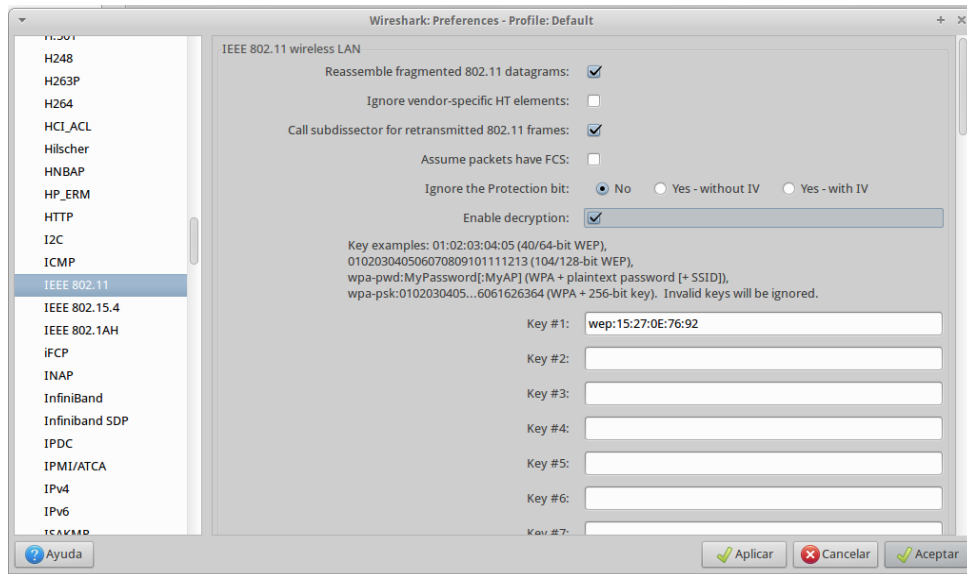


Figura 9: Ventana de opciones de decodificación de las tramas

6. Sobre el firmware

Normalmente los fabricantes de los dispositivos o los proveedores de servicios inalámbricos dotan a sus dispositivos de una funcionalidad y configurabilidad limitada. A raíz de esto, existen multitud de firmwares diferentes y proyectos abiertos, como OpenWRT <https://openwrt.org/> o DD-WRT <http://www.dd-wrt.com/site/index>, que ofrecen nuevos firmwares a un gran número de dispositivos de red, aumentando de una forma exponencial las opciones y posibilidades de configuración de los mismos.

En nuestro caso, aunque el firmware proporcionado por el fabricante cubre las posibilidades de configuración WDS, los routers de prácticas tienen instalado un firmware bien conocido como es DD-WRT.

En cualquier caso, debido a la gran diversidad y heterogeneidad del hardware, es conveniente asegurarse del modelo y número de revisión exacta antes de aventurarse a flashear cualquier dispositivo ya que podríamos inutilizarlo.