Práctica 3a. Wireless 802.11 WDS

1. Introducción teórica

Leer la introducción teórica de la práctica de wireless. Algunas descripciones se repasan aquí, y se añade una descripción de las posibles topologías, centrándose en la topología WDS.

1.1. Cabecera de enlace 802.11

La cabecera de los protocolos 802.11 dispone básicamente de 4 campos de dirección, y el uso de los mismos depende de dos bits llamados DS que están en el campo Frame Control.

Figura 1: Cabecera 802.11

El modo de uso de esos campos de direccionamiento determinan varios modos de funcionamiento, que básicamente son:

Ad-hoc: interconexión de ordenadores o dispositivos sin la necesidad de un AP. Infraestructure: ordenadores o dispositivos (configuración Managed) conectados a un AP (configuración Master) que gestiona las conexiones. WDS (Wireless Distribution Sistem): interconexión de dos AP que hacen de puente entre dos redes cableadas (o nó) ethernet para formar una misma red local. Monitor: permite capturar paquetes sin asociarse a un AP o red ad-hoc. Este modo no está definido por el estándar y es mas un modo aplicable a capacidades de los drivers de las interfaces de red que se instalan en los ordenadores.

Cuadro 1: Conectividad sugerida

Modo	To DS	From DS	Address 1	Address 2	Address 3	Address 4
Ad-Hoc	0	0	Dest Addr	Source Addr	ISSID	
Master	0	1	Dest Addr	BSSID	Source Addr	
Managed	1	0	BSSID	Source Addr	Dest Addr	
WDS	1	1	Rec Addr	Tran Addr	Dest Addr	Source Addr

Los usos mas comunes estarían representados en la figura siguiente:

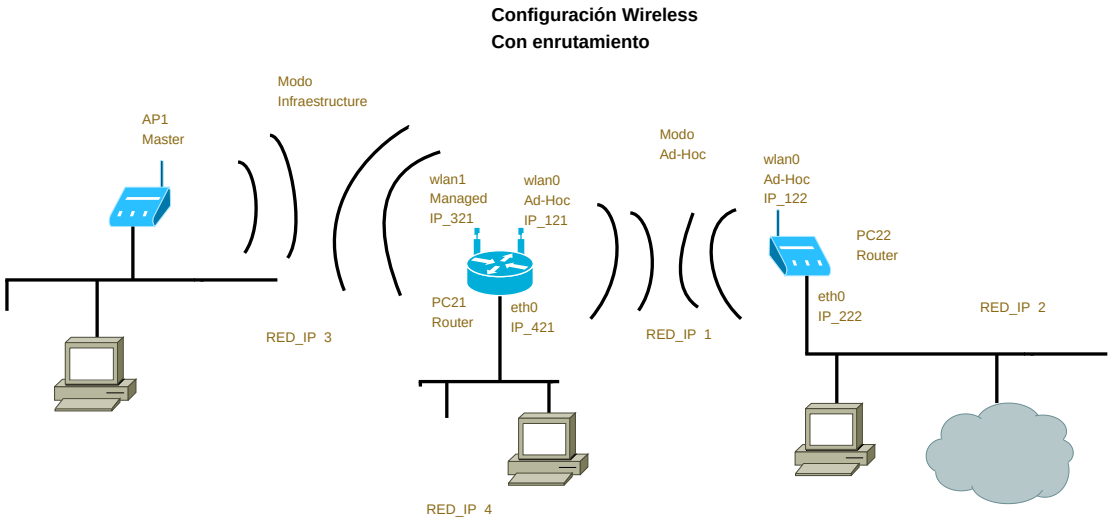
Las diferentes topologías de red no tienen por qué estar ineludiblemente relacionadas con los modos de funcionamiento, de forma que puede haber enlaces punto a punto en modo infraestructure, como redes malladas o en estrella en modo WDS o incluso Ad-Hoc, así como repetidores que dispongan de diferentes modos.

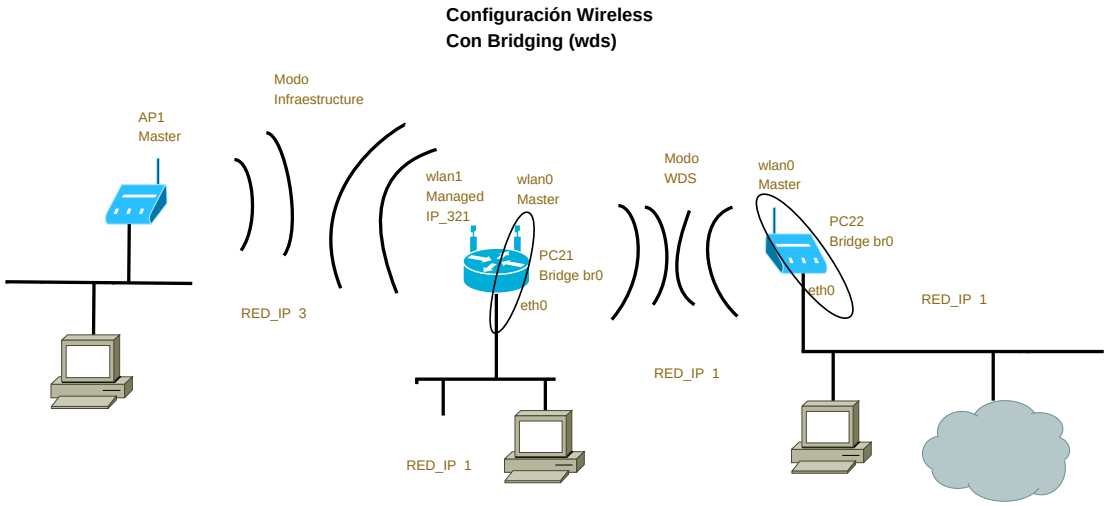
1.2. Seguridad

En las redes inalámbricas, el hecho de estar compartiendo el medio de comunicación de forma abierta obliga al establecimiento de unos parámetros de seguridad. Básicamente existen 3 líneas de seguridad:

1. Encriptación. Consiste en un proceso de encriptación del campo de datos que se transmite por la red. Existen básicamente 2 modelos de encriptación, WEP y WPA.

2. Filtrado de direcciones MAC. Consiste básicamente en permitir el acceso a una red a través de su AP exclusivamente a las interfaces cuya MAC esté en un listado de permitidas.





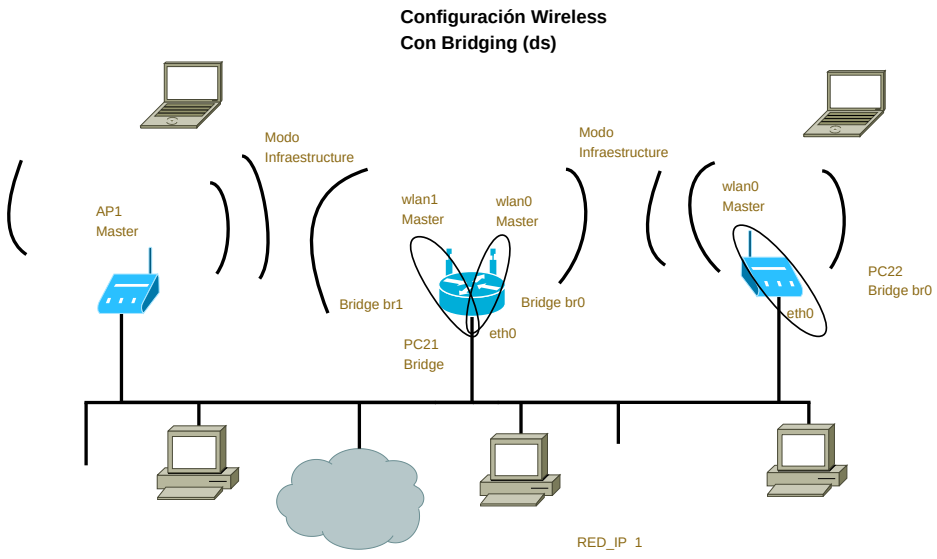


Figura 2: Modos de funcionamiento 802.11

3. Ventana cautiva. Consiste básicamente en permitir el acceso a la red a través de un par nombre de usuario/contraseña presentado en un cuadro de diálogo servido por un servicio de la red.

1.3. Topologías

Los diferentes modos de funcionamiento (Infraestructure, Ad-Hoc, o WDS) permiten generar numerosas situaciones topológicas, algunas de las cuales se describen a continuación.

1.3.1. Islas wifi

El término islas wifi está referido comúnmente al área de cobertura de un punto de acceso AP. Es la topología mas sencilla y mas común, donde varios dispositivos inalámbricos utilizan un AP para interconectarse entre sí. Habitualmente, este AP tiene conectividad cableada a otros segmentos de red, disponiendo por tanto de al menos dos interfaces, una inalámbrica (wlan) y otra cableada (lan). Ambas interfaces suelen estar puenteadas, de forma que el acceso por parte de un dispositivo inalámbrico al AP implica también un acceso al segmento cableado de la red, y viceversa.

El modo de funcionamiento wifi de esta topología es el modo infraestructure, esto es, en el AP se configura el modo Master (o AP) y en los dispositivos el modo Client (o Managed).

1.3.2. AP virtual o VAP

Básicamente, es la posibilidad de disponer de varias "islas wifi" con un único AP. Esta topología suele requerir de soluciones específicas para cada AP y de funcionalidades especiales de los drivers, no pudiendo crearse en todos los dispositivos.

1.3.3. Interconexión punto a punto de equipos

Esta topología hace uso del modo de funcionamiento wifi Ad-Hoc. En esta topología se generan conexiones punto a punto entre los dispositivos. Está recomendada para enlaces entre varios hosts sin necesidad de un AP. Suele haber un límite de equipos que se pueden integrar en una red Ad-Hoc, estando recomendado para dos equipos.

1.3.4. Wifi distribuida

Este modo de funcionamiento es el mas común en redes dentro de un edificio, o incluso entre varios de ellos. Básicamente son diferentes islas wifi interconectadas a través de la interfaz cableada de los AP. Dicha interconexión se produce generalmente en un conmutador o entre diferentes conmutadores. El modo de funcionamiento wifi es el Infraestructure, el mismo que en el de las islas wifi, pero cada isla (es decir, cada BSS) deberá tener su propio canal asignado y diferente al resto, para evitar interferencias.

1.3.5. Puente wifi enrutado

La forma mas sencilla de interconectar dos redes mediante un enlace wifi es utilizando enrutamiento. Para ello se necesita crear una isla wifi con un AP en modo Master, y otro AP como cliente en esa isla (es decir, en modo Managed). El AP (u otro dispositivo con una interfaz wlan y otra lan) cliente tiene sus interfaces wlan y lan en diferentes redes IP. En esta topología, el AP cliente es realmente un router IP con dos interfaces, una inalámbrica 802.11 y otra cableada 802.3.

1.3.6. Puente wifi transparente o WDS

Esta topología no está completamente estandarizada, aunque es muy útil y está bastante extendida. WDS (Wireless Distribution System) es una topología de funcionamiento que permite crear un enlace inalámbrico entre dos segmentos de red y mantener una topología lógica única de forma transparente. El hecho de no estar estandarizada, el modo WDS está implementado de forma diferente dependiendo de los fabricantes, de las tarjetas inalámbricas y los drivers, por lo que se recomienda el uso de pares de modelos, en lugar de tener ambos extremos de la conexión de diferentes modelos, lo que podría provocar incompatibilidades.

La mayor ventaja de este modo de funcionamiento es la transparencia a nivel 2, permitiendo puenteado y broadcast, de forma que todos los segmentos conectados forman un solo dominio de broadcast.

La aparición del modo WDS está originada en un problema conocido de puentes wifi cuando quieren unirse dos segmentos que tengan la misma configuración IP. El problema queda representado en la figura 3

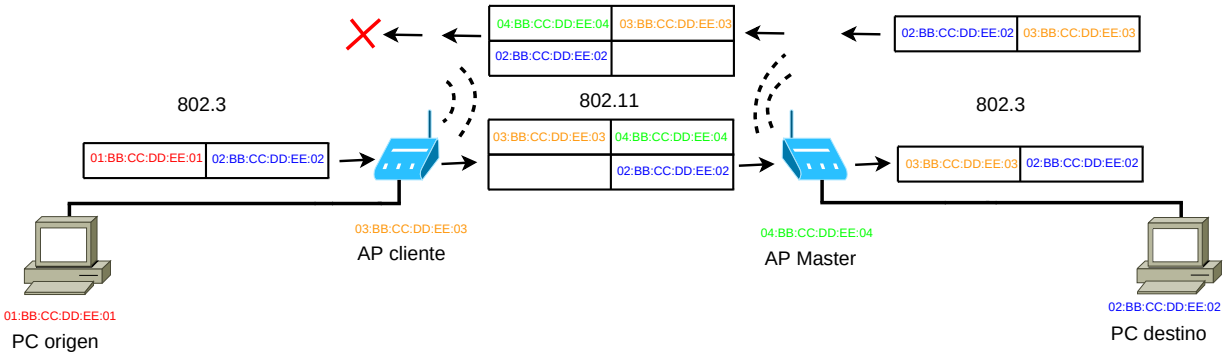


Figura 3: Problema del puente wireless

Y la figura 4 representa la solución WDS, donde se utilizan los 4 campos de direcciones para transmitir la dirección MAC de origen y destino reales.

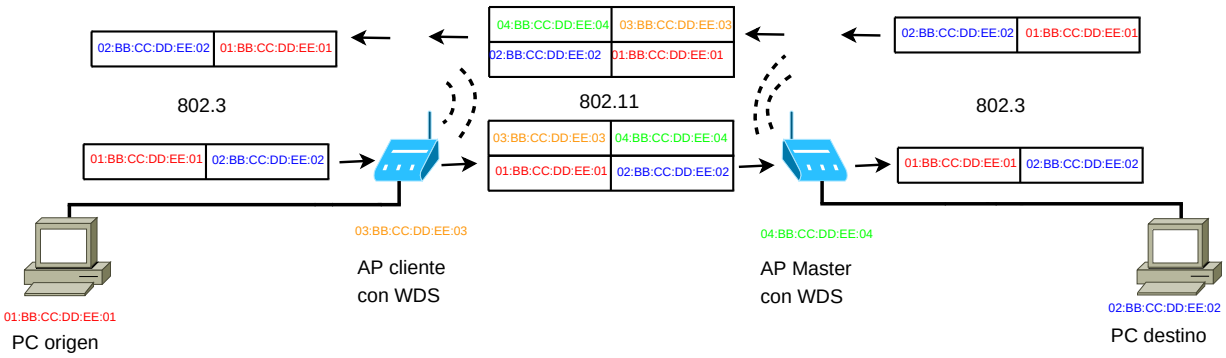


Figura 4: Solución WDS

2. Descripción

Esta práctica pretende mostrar la interconexión de equipos a través de enlaces de tecnología ethernet wireless (802.11b/g). Se trabajará sobre dos modos de operación:

- Modo Distribuido inalámbrico, WDS. Este modo ermitirá interconectar dos segmentos de red diferentes como si fuesen una misma red IP.
- Modo Distribuido (o extendido), DS. Este modo permite crear una sola red wifi con varias islas wifi interconectadas por un backbone Ethernet (ESS).

La práctica se considera dentro del mismo grupo que la práctica de redes inalámbricas 802.11, en la que se muestra la topología de puente wifi enrutado y el modo de interconexión punto a punto entre equipos o modo Ad-Hoc. En esta práctica se utilizarán dos gateways , en una configuración como AP, por lo que se llaman y etiquetan como *AP2* y *AP3*. El sistema operativo que tienen instalado es el OpenWRT , una distribución Linux específica para gateways con interfaz inalámbrica.

Ambos AP tienen instalada la utilidad *iproute2* para facilitar la gestión de las interfaces, aunque OpenWRT dispone de un sistema de configuración de red preinstalado llamado LUCI, bastante sencillo y potente. Se usará parte de este sistema para evitar la necesidad de escribir directamente en la memoria no volatil del sistema (nvram) cuando se modifiquen parámetros de los drivers de las tarjetas.

Está diseñada para un grupo de 2 personas, donde debe trabajar una persona por host y por AP. Entorno de trabajo: LAN plana del laboratorio según el esquema general.

Como infraestructura se dispone de dos equipos PC y de dos AP comerciales Linksys WRT54GL .

- Los equipos *PC26* y *PC28* disponen de sistema operativo Linux, con kernel 2.6.18 de la distribución debian etch.
- Los AP *AP2* y *AP3* tienen instalado el sistema operativo de red OpenWRT , en su versión Backfire 10.03.rc3.

La práctica pretende la configuración de la red wireless como una única red IP, en cuyo caso, todos los enlaces deben pertenecer al mismo puente o bridge. Se considerará la consecución de la práctica cuando *PC26* y *PC28* puedan tener conectividad entre sí y al resto del backbone o incluso a Internet.

3. Desarrollo

Los dos AP tienen la siguiente configuración inicial, donde la interfaz sobre la que se actuará será el puente "br-lan":

```
AP2:

LinkSys WRT54GL v 1.1

OpenWrt Backfire 10.03.1-rc4, r24045) kernel 2.6.32
brcm47xx

root: provisional

br-lan: 192.168.10.2/24
puertos: 1,2,3,5.
mon: 10.11.12.1/24
puertos: 4,5.
wan: deshabilitada
wifi: off.
firewall: off.
```

```
AP3:

LinkSys WRT54GL v 1.1

OpenWrt Backfire 10.03.1-rc4, r24045) kernel 2.6.32
brcm47xx

root: provisional

br-lan: 192.168.10.3/24
puertos: 1,2,3,5.
lan-mon: 10.11.12.1/24
puertos: 4,5.
wan: deshabilitada
wifi: off.
firewall: off.
```

3.1. Modo Distribuido Inalámbrico (WDS)

La solución WDS en los Linksys WRT54GL con el sistema operativo OpenWRT puede tener varias formas de implementación dependiendo del driver de radio utilizado. Según la documentación en la web de OpenWRT el driver mas estable es el driver broadcom (plataforma Broadcom BCM5352) para kernels 2.6, es decir, la distribución backfire 10.03.1 (*https://downloads.openwrt.org/backfire/10.03.1/brcm-2.4/openwrt-brcm-2.4-squashfs.trx*). Básicamente el modo WDS no es un estándar firme, pero el hecho de que haga uso de los 4 campos de dirección en la trama MAC wireless le confiere un caracter estándar de facto.

Para configurar esta topología, inicialmente será necesario cambiar la conexión cableada de los equipos implicados. La figura 5 muestra cómo disponer el cableado para esta práctica. Básicamente, será necesario:

- desconectar el latiguillo rj45 que conecta al equipo *PC26* con la red plana y conectarlo al puerto 2 de *AP2*.
- conectar el latiguillo azul (u otro cualquiera) de *AP3* a *PC26*.
- desconectar el latiguillo rj45 que conecta al equipo *PC28* con la red plana.
- conectar el latiguillo azul (u otro cualquiera) del puerto 2 de *AP3* a *PC28*.

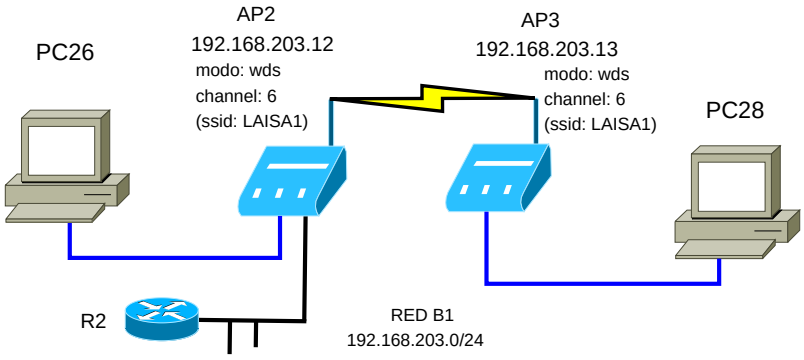


Figura 5: Configuración IP

Se pretende crear la configuración lógica de la figura 5. Los pasos necesarios serán:

1. Acceso al AP. Para ello, habrá que habilitar una dirección IP dentro de la red 192.168.10.0/24 por defecto de cada AP en los PC cliente, y conectarse al AP correspondiente vía ssh. Se usará el comando "ip addr" sobre la interfaz "eth0" de los PC.

2. Cambio de la dirección IP del puente lan-wlan del AP. Se pondrá en cada AP la dirección correspondiente a la mostrada en la figura 5. Se usará el comando "ip addr" sobre la interfaz "br-lan".

3. Localizar las direcciones MAC, de cada dispositivo:

   En *AP2*:

```
root@AP2:/etc/config# ip link show wl0
6: wl0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:18:39:cf:0d:47 brd ff:ff:ff:ff:ff:ff
```

   de donde se vería que la dirección MAC de *AP2* es *00:18:39:cf:0d:47*

   En *AP3*

```
root@AP3:~# ip link show wl0
6: wl0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:18:39:cf:0d:38 brd ff:ff:ff:ff:ff:ff
```

   de donde se vería que la dirección MAC de *AP3* es *00:18:39:cf:0d:38*.

4. Revisar la configuración física de la interfaz en el fichero "/etc/config/wireless". Particularmente los dispositivos enfrentados tienen:

   - Tener habilitado el mismo canal wifi. `option 'channel' '6'`.
   - Que la dirección MAC coincida con la detectada mediante `ip link`, `option 'macaddr' ....`
   - Que tengan la misma tecnología 802.11. `option 'hwmode' '11bg'`

   En *AP2*:

```
config 'wifi-device' 'wl0'
        option 'type' 'broadcom'
        option 'macaddr' '00:18:39:cf:0d:47'
        option 'disable' '0'
        option 'channel' '6'
        option 'txpower' '0'
        option 'hwmode' '11bg'
    ..................
```

   En *AP3*:

```
config 'wifi-device' 'wl0'
        option 'type' 'broadcom'
        option 'macaddr' '00:18:39:cf:0d:38'
        option 'disable' '0'
        option 'channel' '6'
        option 'txpower' '0'
        option 'hwmode' '11bg'
    ...................
```

Ojo, las líneas puestas en *option 'macaddr'* pueden tener direcciones MAC diferentes, y se deben corresponder a las visualizadas anteriormente.

5. Habilitar la interfaz inalámbrica del AP. Para ello habrá que editar el fichero "/etc/config/wireless" y poner la línea "option disabled" a "0".

```
config wifi-device radio0
    ...................
        # REMOVE THIS LINE TO ENABLE WIFI:
        option disabled 0
    ...................
```

6. Poner la configuración de los AP en el fichero "/etc/config/wireless".

```
    ..........
config 'wifi-iface'
        option 'device' 'wl0'
        option 'network' 'lan'
        option 'mode' 'wds'
        option 'bssid' '00:18:39:cf:0d:38'
        #option 'encryption' 'none'
    ..................
```

7. Observar que esté habilitado el modo "wds" y que el BSSID coincida con la MAC del dispositivo enfrentado.

```
    ..........
config wifi-iface
    ..................
        option mode wds
        option bssid    <MAC AP CONTRARIO>
    ..................
```

8. Tras ello será necesario reiniciar la interfaz wifi (wlan0) en cada AP y recargar su configuración. Esto se realiza con el comando "wifi"

```
    APx # wifi  //Reinicia la interfaz wifi
```

Se puede ver cómo se encienden los leds de marca de los AP.

9. Comprobar que funciona, mediante pruebas de conectividad ICMP primero entre ambos APs, después entre los PCs y sus respectivos APs enfrentados y finalmente entre ambos PCs.

Como puede verse, la configuración expuesta no incluye encriptación de datos a través del enlace WDS. Para incluir dicha encriptación, del tipo PSK2 (es decir WPA) será necesario ampliar el fichero de configuración creando una isla wifi del tipo infraestructure (modo AP) que disponga de encriptación y habilitarla también en el enlace WDS. Básicamente

1. Añadir una nueva red wifi (isla wifi) enlazada a la interfaz br-lan en el fichero de configuración de redes WIFI donde previamente ya existe la red WDS creada anteriormente. Esto se hará para ambos APs:

```
    ..........
config wifi-iface
    option device       wl0
    option mode         ap
```

```
    option network      lan
    option ssid         LAISA1

config wifi-iface
    <RED WDS>
    ..............
```

2. Habilitar encriptación psk2, con la clave "provisional" sobre la red wifi "LAISA1" creada. Realizarlo en ambos APs.

```
    ..........
config wifi-iface
    ..................
        option ssid  LAISA1
        option encryption psk2
        option key provisional
..................
```

3. Habilitar encriptación psk2, con la clave "provisional" sobre el enlace WDS previo. Realizarlo en ambos APs.

```
    ..........
config 'wifi-iface'
        option 'device' 'wl0'
        option 'network' 'lan'
        option 'mode' 'wds'
        option 'bssid' <MAC AP CONTRARIO>
        option encryption psk2
        option key provisional
    ..................
```

Los ficheros "/etc/config/wireless" en cada AP quedarán de la forma:

- *AP2*:

```
config 'wifi-device' 'wl0'
        option 'type' 'broadcom'
        option 'macaddr' '00:18:39:cf:0d:47'
        option 'disable' '0'
        option 'channel' '6'
        option 'txpower' '0'
        option 'hwmode' '11bg'
        # REMOVE THIS LINE OR SET TO 0 TO ENABLE WIFI:
        option disabled 0

config wifi-iface
        option device       wl0
        option mode         ap
        option network      lan
        option ssid         LAISA1
        option encryption psk2
        option key provisional

config 'wifi-iface'
        option 'device' 'wl0'
        option 'network' 'lan'
        option 'mode' 'wds'
        option 'bssid' '00:18:39:cf:0d:38'
        option encryption psk2
        option key provisional
```

- *AP3*:

```
config 'wifi-device' 'wl0'
        option 'type' 'broadcom'
        option 'macaddr' '00:18:39:cf:0d:38'
        option 'disable' '0'
        option 'channel' '6'
        option 'txpower' '0'
        option 'hwmode' '11bg'
        # REMOVE THIS LINE OR SET TO 0 TO ENABLE WIFI:
        option disabled 0

config wifi-iface
        option device       wl0
```

```
        option mode         ap
        option network      lan
        option ssid         LAISA1
        option encryption psk2
        option key provisional

config 'wifi-iface'
        option 'device' 'wl0'
        option 'network' 'lan'
        option 'mode' 'wds'
        option 'bssid' '00:18:39:cf:0d:47'
        option encryption psk2
        option key provisional
```

4. Probar conectividad entre APs y PCs.

5. Puede hacerse algo de auditoria (en el caso en que haya algún problema) utilizando los comandos

```
APx #  wl  wds      //Presenta al MAC del dispositivo enfrentado.
APx #  wl  sta_info    <MAC AP CONTRARIO>    //Muestra informacion del enlace
```

Observaciones:

- Los valores de las direcciones MAC y BSSID pueden cambiar respecto a los presentados.
- Los SSID de las islas wifi tienen que ser iguales en ambos APs, al igual que los modos y claves de encriptación.
- Se podrían crear nuevos enlaces WDS, creando una nueva red (sección "wifi-iface") para cada enlace WDS.
- Al estar utilizándose el mismo canal de radiofrecuencia, los diferentes enlaces creados compartirán ancho de banda y por tanto la capacidad de transmisión será teóricamente la mitad.
- Se recomienda realizar pruebas de rendimiento del canal mediante el comando *iperf* .

Los equipos PC26 y PC28 formarán parte del mismo segmento de red lógico, y podrán acceder a Internet a través de la pasarela de la red (en el bloque1 de prácticas será R2). Se podrá utilizar F0 como pasarela en el caso de que R2 no esté disponible. Para ello bastará mantener el direccionamiento original de los PCs en la red 192.168.29.0/24.

3.2. Modo Distribuido o Extendido (ESS)

Se pretende crear la configuración topológica de la figura 6. En ella los puntos de acceso sirven cada uno una isla wifi, pero con el mismo ESSID (Aula1), de forma que cualquier dispositivo inalámbrico que se conecte a cualquiera de los AP estará conectado a la misma red, y al resto del backbone al que los AP están conectados de forma conmutada (red B1). Para esta configuración no serán necesarias configuraciones especiales, y bastará configurar cada uno de los AP con los mismos parámetros a excepción del canal utilizado.

La configuración se hará en dos pasos, primero sin seguridad y posteriormente con seguridad WPA. El objetivo de realizar estos dos pasos es eliminar posibles confusiones en el caso en que no se consiga poner en funcionamiento el sistema.

Los ficheros de configuración en cada uno de los AP (sin seguridad) son:

- *AP2*:

```
config 'wifi-device' 'wl0'
        option 'type' 'broadcom'
        option 'macaddr' '00:18:39:cf:0d:47'
        option 'disable' '0'
        option 'channel' '1'
        option 'txpower' '0'
        option 'hwmode' '11bg'
        # REMOVE THIS LINE OR SET TO 0 TO ENABLE WIFI:
        option disabled 0

config wifi-iface
```

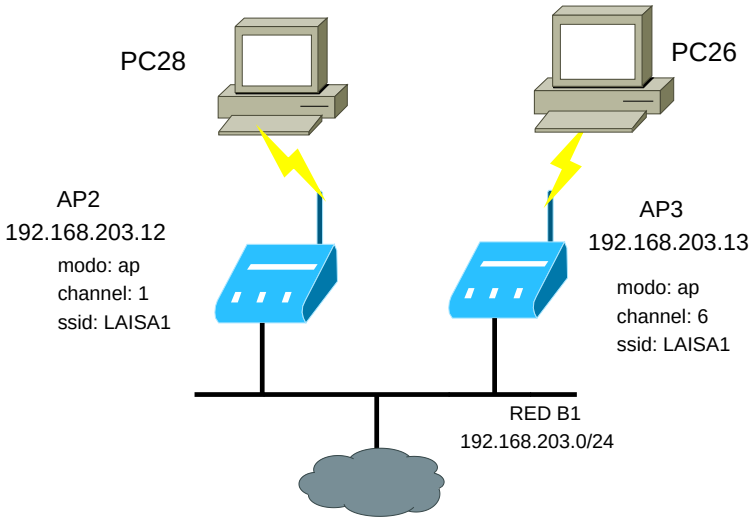


Figura 6: Configuración ESS

```
        option device       wl0
        option mode         ap
        option network      lan
        option ssid         LAISA1
        option encryption none
```

- *AP3*:

```
config 'wifi-device' 'wl0'
        option 'type' 'broadcom'
        option 'macaddr' '00:18:39:cf:0d:38'
        option 'disable' '0'
        option 'channel' '6'
        option 'txpower' '0'
        option 'hwmode' '11bg'
        # REMOVE THIS LINE OR SET TO 0 TO ENABLE WIFI:
        option disabled 0

config wifi-iface
        option device       wl0
        option mode         ap
        option network      lan
        option ssid         LAISA1
        option encryption none
```

Para hacer pruebas de conectividad con PC26 y PC28 será necesario que tengan una tarjeta wifi instalada, habilitada y que establezca la conexión. Se ofrece la posibilidad de que el alumno realice conexiones con su propio dispositivo BYOD y compruebe la conectividad.

Para añadir posteriormente seguridad WPA, será necesario modificar los ficheros de configuración de forma que queden según se muestra a continuación:

- *AP2*:

```
config 'wifi-device' 'wl0'
        option 'type' 'broadcom'
        option 'macaddr' '00:18:39:cf:0d:47'
        option 'disable' '0'
        option 'channel' '1'
        option 'txpower' '0'
        option 'hwmode' '11bg'
        # REMOVE THIS LINE OR SET TO 0 TO ENABLE WIFI:
        option disabled 0

config wifi-iface
        option device       wl0
        option mode         ap
        option network      lan
        option ssid         LAISA1
        option encryption psk2
        option key provisional
```

- *AP3*:

```
config 'wifi-device' 'wl0'
        option 'type' 'broadcom'
        option 'macaddr' '00:18:39:cf:0d:38'
        option 'disable' '0'
        option 'channel' '6'
        option 'txpower' '0'
        option 'hwmode' '11bg'
        # REMOVE THIS LINE OR SET TO 0 TO ENABLE WIFI:
        option disabled 0

config wifi-iface
        option device      wl0
        option mode        ap
        option network     lan
        option ssid        LAISA1
        option encryption psk2
        option key provisional
```

En los equipos inalámbricos será necesario activar las claves WPA. Si estos dispositivos son Linux, será necesario crear un fichero de configuración /etc/wpa_supplicant/LAISA1.conf con el contenido siguiente:

```
ctrl_interface=/var/run/wpa_supplicant
network={
        ssid="LAISA1"
        key_mgmt=WPA-PSK
        psk="provisional"
}
```

y ejecutar como root:

```
PCx# wpa_supplicant -Dwext -q -i wlan0 -c /etc/wpa_supplicant/LAISA1.conf
```

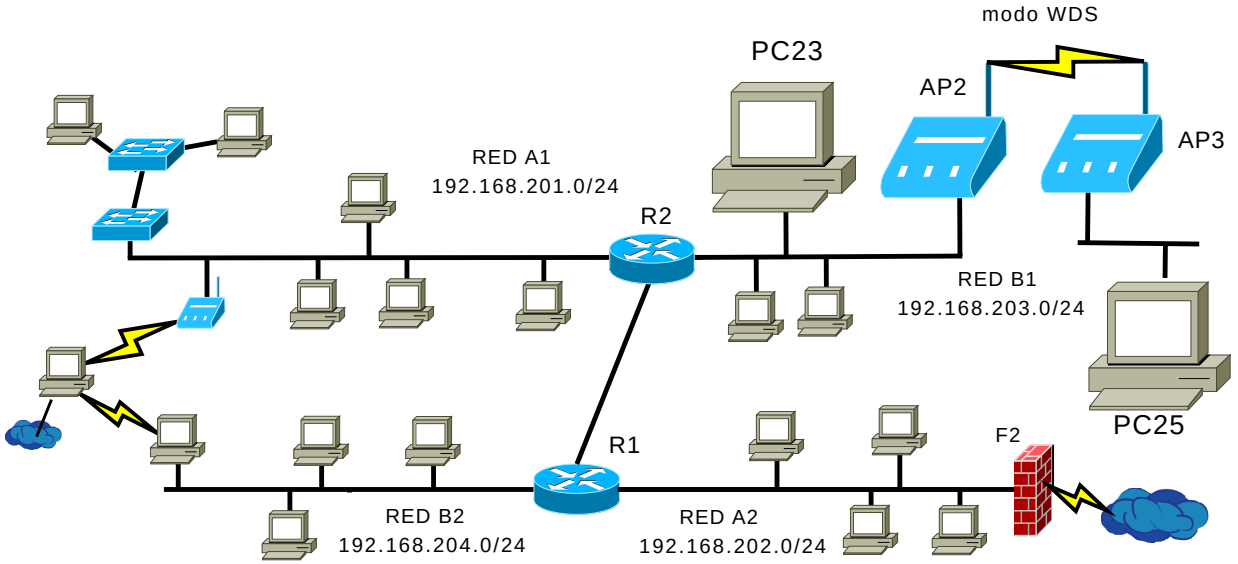


Figura 7: Visión general de la práctica