Práctica 3. Wireless

1. Introducción teórica

Las redes inalámbricas o wireless son un término general aplicado fundamentalmente a redes de ordenadores sin hilos con las mismas funcionalidades que las redes de área local. El diseño de los protocolos de capa de enlace que las soportan se conocen como la familia de protocolos 802.11 y están fundamentadas en la existencia de un elemento gestor central llamado Access Point o AP.

No obstante, la capacidad inalámbrica les confieren la posibilidad de poder ser diseñadas en escenarios mas complejos que traspasan el carácter de red de área local e incluso el de red de ordenadores, pudiendo ser utilizadas como backbones o redes troncales de largo alcance.

La característica inalámbrica hace que la distinción de unas redes y otras que comparten el mismo espacio físico se realice mediante dos parámetros diferentes. El primero es un canal de comunicaciones en el espectro radioeléctrico, y el segundo es un nombre identificador o SSID (Service Set Identifier).

Para saber mas de las redes 802.11, ver el fantástico libro de M. Gas "802.11 Wireless networks: The Definitive Guide" [1]

1.1. Canal de comunicaciones

La tecnología 802.11g dispone de 14 canales de comunicaciones en la banda de los 2,4 Ghz, solapados entre sí. Esto provoca la necesidad de escoger canales alejados en frecuencia en puntos donde pueda existir cierta saturación de canales.

La repartición de canales en la banda libre de 2,4 Ghz tiene la estructura de la figura

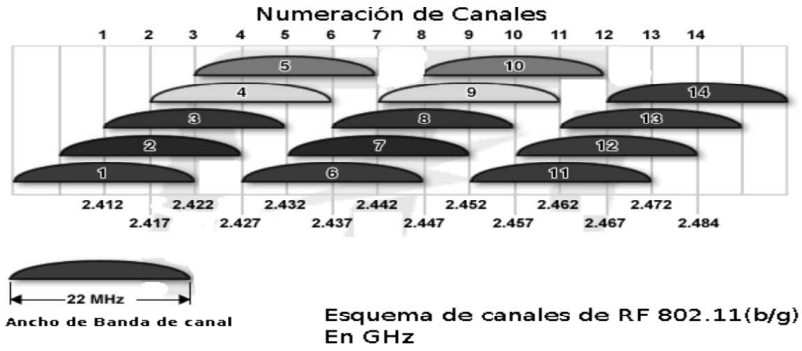

Figura 1: Canales 802.11

1.2. Conjunto de servicios o Service Set (SS) y nombre de red

En redes IEEE 802.11 se definen varios conjuntos de servicios asociados a los diferentes tipos de topologías.

A la topología básica de un punto de acceso AP y varias estaciones cliente conectadas a él se la suele llamar en términos coloquiales "isla wifi". Esta topología utiliza el modo de funcionamiento "Infraestructure" y queda definida como el Basic Service Set (BSS) por tanto cada "isla wifi" es un BSS único. De igual forma, cada "isla wifi" o BSS tiene un identificador único, llamado BSSID que es la dirección MAC del AP que la forma (48 bits asignados al chip de radio del AP). Los dispositivos cliente se "conectan" a ese BSS conociendo su BSSID, pero como este es una dirección MAC, se ha creado el SSID con un formato mas legible. Por tanto, en la topología BSS, el SSID es el nombre de la "isla wifi".

Para la topología Ad-Hoc (modo de funcionamiento Ad-Hoc), donde no se necesita un AP para comunicar equipos entre sí con enlaces 802.11, se define el IBSS (Independent BSS o Conjunto de Servicios

Básicos Independientes). Cada red Ad-Hoc o IBSS queda definida por su IBSSID que es la dirección MAC del chip de radio del primer dispositivo que crea la red Ad-Hoc. El usuario del primer dispositivo que crea la red Ad-Hoc le da un nombre legible: el SSID (o ISSID).

Para topologías formadas por varios BSS interconectados entre sí (es decir, varios APs conectados entre sí) para formar una sola red wifi, conocidas como redes extendidas, se define el Extended Service Set (ESS). En este caso, cada AP tiene su BSSID único, pero la red que forman todos los APs (o BSSs) tiene un sólo SSID, que en este caso se le llama ESSID.

En resumen, una breve descripción de los términos:

BSS – Basic Service Set. También se conoce como Conjunto de Servicios Básicos y es utilizado por el modo de funcionamiento Infraestructure. Se identifica de forma única por el BSSID. Se utiliza el SSID como identificador legible escogido por el administrador.

ISS - Independent Service Set. También se conoce como Conjunto de Servicios Independientes y es utilizado por el modo de funcionamiento Ad-Hoc. Se identifica de forma única por el BSSID o ISSID. Se utiliza el SSID como identificador legible escogido por el administrador.

ESS – Extended Service Set. También se conoce como Conjunto de Servicios Extendidos, y está referido a una topología de varios BSS interconectados entre sí mediante un backbone (habitualmente ethernet cableado) por lo que comparten la misma red física. La forma mas habitual de denominarlo es el modo distribuido o DS (Distribution System). Como no hay un único BSSID, se utiliza el SSID como identificador único de la red formada por todos los BSS, escogido por el administrador. En este caso también se le llama ESSID.

SSID - Service Set Identifier. Este es el que aparece habitualmente como Identificador de Red Wireless. En la perspectiva del usuario o administrador, el identificador de red SSID se parametriza como un nombre de red.

BSSID - Basic Service Set Identifier. Es un identificador único del BSS y coincide con la MAC del AP que forma el BSS.

ISSID - Independent Service Set Identifier. Es igual que el BSSID pero para redes Ad-Hoc. Coincide con la MAC del primer equipo que crea la red Ad-Hoc. Se suele mantener el término BSSID.

ESSID - Extended Service Set Identifier. Es el idenfificador de red wireless extendida ESS. No coincide con ninguna MAC de ningún AP, pues son varios los APs que forman parte del ESS. Es un nombre identificativo puesto por el administrador. También se suele utilizar el término general SSID.

La tabla 1.2 presenta un breve asociación entre topologías y términos.

Cuadro 1: Service Set y Modos

Topología	BSS	IBSS	ESS	BSSID	ISSID	ESSID	SSID
Infraestructure	Unico			MAC		Nombre de red	Nombre de red
Ad-Hoc		Unico			MAC del host creador		Nombre de red
Extendido o Distribuido (DS)	Cada AP es uno.		Unico			Nombre de red	Nombre de red

En la figura 2, se puede ver una topología varíada, donde hay diferentes Servicios.

1.3. 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.

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.

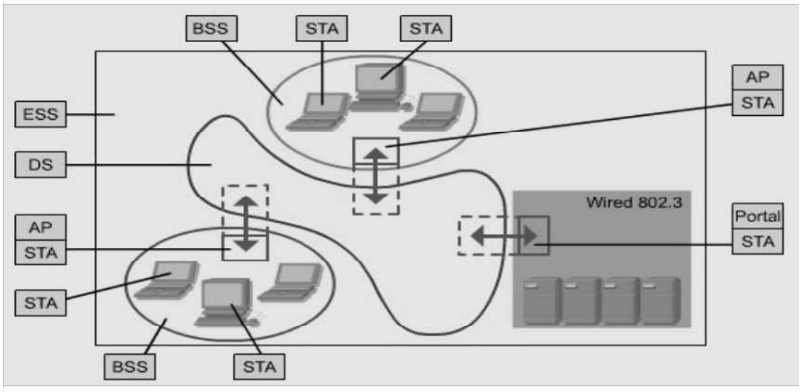

Figura 2: Topología extendida

Figura 3: Cabecera 802.11

- 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 2: 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 4.

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.

1.4. 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.
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.

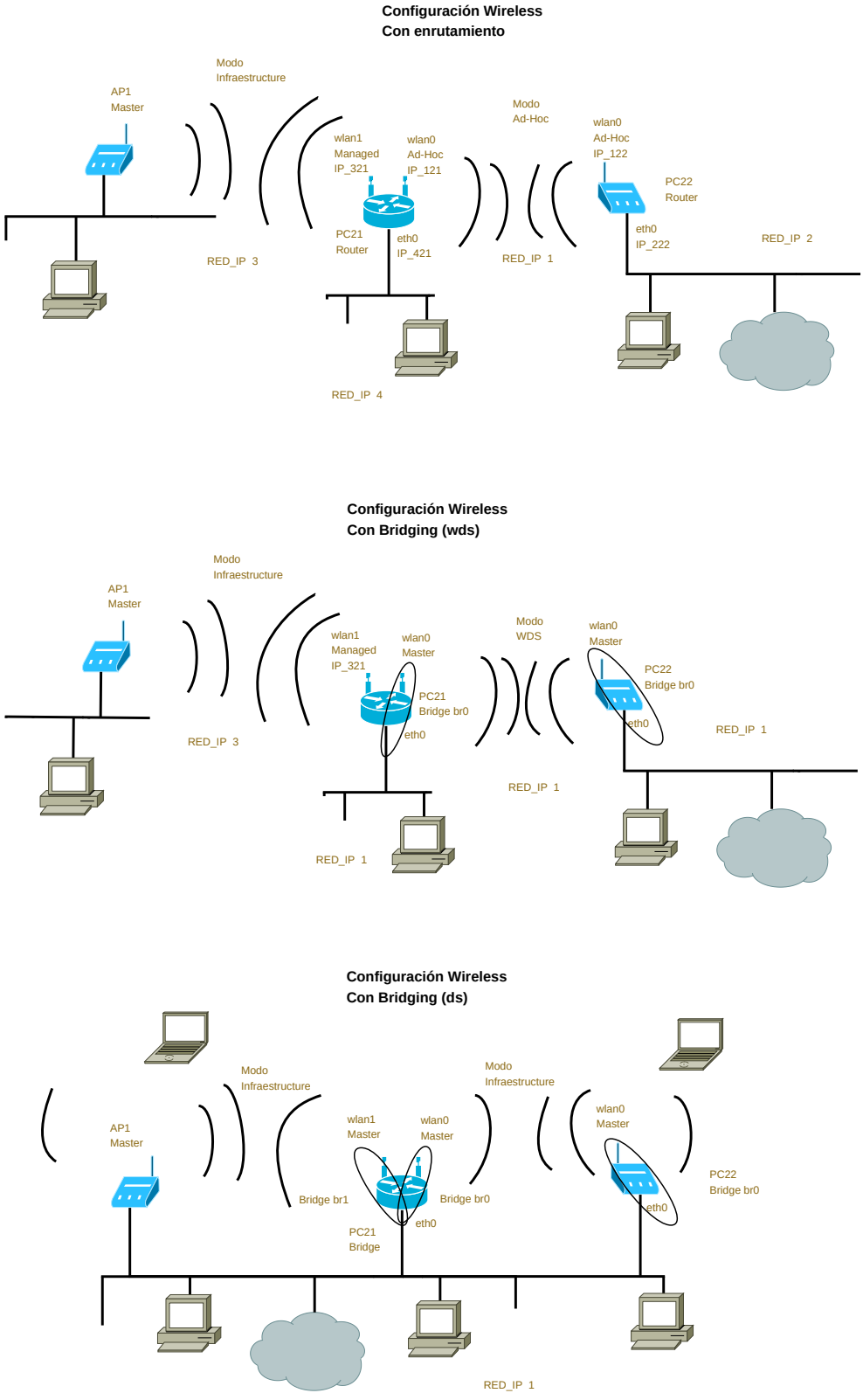

Figura 4: Modos de funcionamiento 802.11

2. Descripción

Esta práctica pretende mostrar la interconexión de equipos a través de enlaces de tecnología ethernet wireless (802.11b/g), tanto en los modos "infraestructure" como "ad-hoc", así como la capacidad de enrutamiento entre redes de diferentes tecnologías. El objetivo final es construir y operar una topología como la mostrada en la figura 5. En este caso, y por disponibilidad se utilizan equipos de sobremesa con sistema operativo Linux, aunque en modos de usuario y como estaciones cliente, pueden utilizarse equipos portátiles con cualquier sistema operativo.

Está diseñada para un grupo de 3 o 4 personas, donde puede trabajar una persona por equipo y la tercera toma notas y/o genera el cuestionario. Entorno de trabajo: LAN plana del laboratorio según el esquema general.

Como infraestructura inicial se dispone de tres equipos PC, de tres modelos de tarjetas wireless USB, y de un Punto de acceso comercial AP Linksys WRT54GL . Todos los adaptadores wireless USB disponen de antena externa sustituible por otras de características mejores.

Toda la infraestructura inicial ya está instalada, por lo que no será necesario realizar los trabajos de carga de módulos o compilaciones. No obstante se describen las tarjetas y su proceso de instalación en el anexo 5.

- Los equipos *PC20*, *PC21* y *PC22* disponen de sistema operativo Linux, con kernel 3.2 de la distribución debian wheezy. ¡¡¡ MUY IMPORTANTE !!! Para todos los equipos será necesario desactivar el software NetworkManager, pues suele interferir con los nuevos adaptadores instalados.
- El equipo *PC20* dispondrá preferentemente de una tarjeta wireless Zydas con chipset zd1211rw descrita anteriormente, y otra tarjeta de cualquiera de los otros tipos descrita, además de la tarjeta de red cableada ethernet integrada en placa base.
- El equipo *PC21* dispondrá preferentemente de una tarjeta wireless Zydas con chipset zd1211rw descrita anteriormente, además de la tarjeta de red cableada ethernet integrada en placa base.
- El equipo *PC22* dispondrá de la tarjeta de red cableada ethernet integrada en placa base.
- El AP Linksys WRT54GL dispone de firmware OpenWRT actualizado a la última versión Backfire 10.3.01. Este AP podrá ser accedido desde el equipo *PC22* al cual está directamente conectado vía Ethernet.

Puede verse la topología básica de la práctica en la figura que representa el esquema general.
La práctica constará de dos partes, referidas a dos configuraciones diferentes que se proponen:

1. Configuración de cada red wireless como redes IP independiente, de forma que se necesitan capacidades de enrutamiento entre ellas para la interconexión de las mismas.
2. Configuración de la red wireless como una única red IP, en cuyo caso, todos los enlaces deben pertenecer al mismo puente o bridge. Esta parte se tendrá que desarrollar de forma libre, inicialmente como trabajo complementario e informativo.

3. Desarrollo

Para la primera parte (conexión por capa 3 IP o enlaces enrutados) , se realizarán distintos modos de funcionamiento en cada enlace, siendo en el enlace *PC20*-*PC21* en modo ad-hoc, y el enlace *AP1*-*PC20* en modo infraestructure con el *AP1* en modo master y *PC20* en modo managed.

Para la segunda parte (conexión por capa 2 bridging o enlace puenteado) se pondrán los dos enlaces en modo infraestructure, siendo los master el *AP1* y *PC20*. En este caso se necesita que los drivers de las tarjetas soporten "wds" y aparentemente lo soporta el driver "hostap". También puede funcionar con la implementación de ProxyARP que es implementada por la utilidad "parprouted". Se intentará realizar el enlace *PC20*-*PC21* con bridging normal con wds, y el enlace *AP1*-*PC22* con ProxyARP.

En esta práctica, se realizará una conexión entre redes wireless mediante la técnica del enrutamiento, siguiendo el esquema de la figura 5

La conectividad entre las redes se realizará en capa 3 IP. Por ello, los equipos *PC20* y *PC21* se configurarán como routers con direccionamiento en sus interfaces según el esquema de la figura 5.

La conectividad entre redes con enrutamiento se realizará en tres partes, la configuración de la conectividad global *PC20*-*PC21*, la de la conectividad global *PC20*-*PC22* y finalmente el enrutamiento entre ambas. En ambas conexiones se configurará primero la capa de enlace y posteriormente la capa de red.

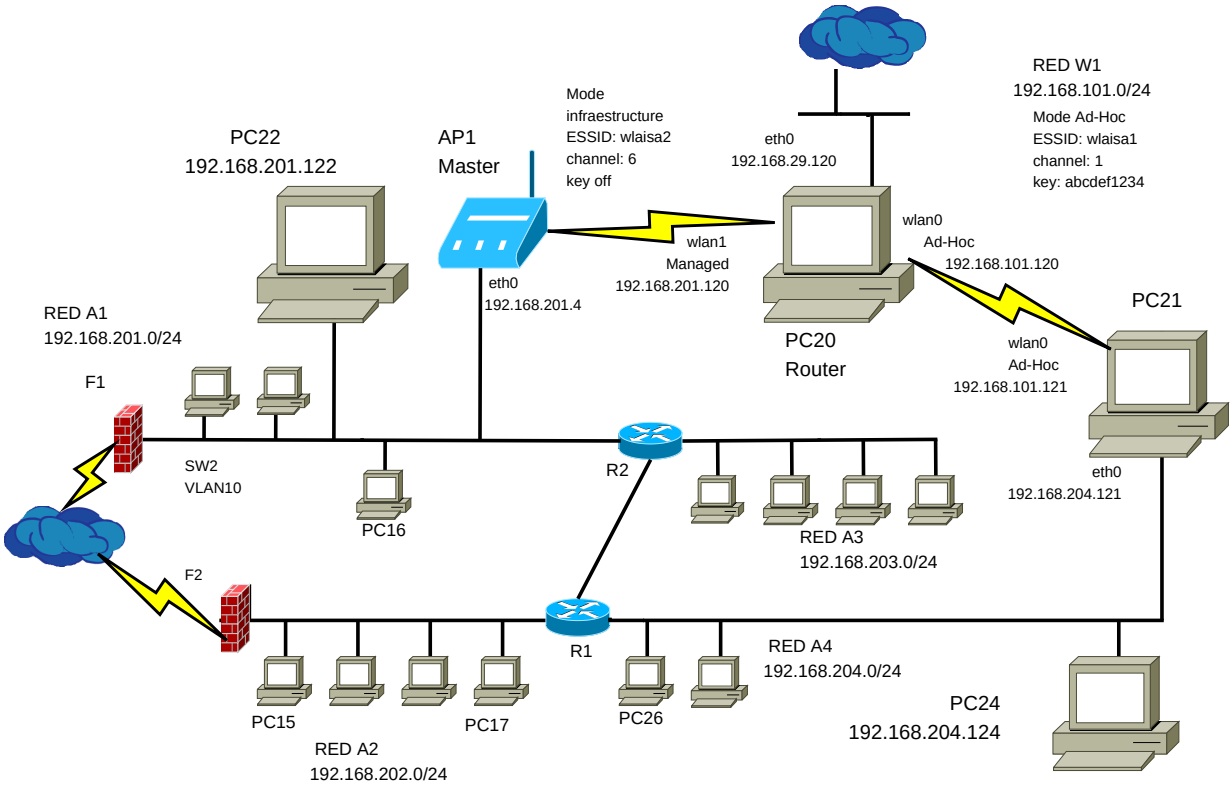

Figura 5: Conexión de redes inalámbricas mediante routing

3.1. Conexión PC20-PC21

3.1.1. Configuración de capa de enlace

Este enlace se hará en modo Ad-Hoc, se pondrá un ESSID "wlaisa1" y utilizará un canal poco saturado o en el caso de varias posibilidades el canal 1. Llevará encriptación WEP de 128 bits con clave en modo hexadecimal "abcdef1234". Llevará además seguridad por filtrado de direcciones MAC.

Se presentan los comandos a ejecutar en cada uno de los equipos. El comando siguiente visualiza las redes Wifi captadas por la interfaz de los equipos.

```
PC20/21 # iwlist wlan0 scanning //Visualiza las redes captadas por la interfaz wlan0 y sus ↩
    caracteristicas publicas
```

Si el resultado de este escaneo es *wlan0 Interface doesn't support scanning : Network is down* convendrá activar la interfaz de la forma siguiente y volver a ejecutar el escaneo.

```
PC20/21 # ip link set up dev wlan0  //Visualiza las redes captadas por la interfaz wlan0 y sus ↩
    caracteristicas publicas
```

Se toma nota de los canales mas desocupados de la misma forma que en el enlace anterior. Suponiendo que el canal seleccionado es el 1:

```
PC20/21 # iwconfig  wlan0  essid wlaisa1  mode ad-hoc  channel 1 key abcdef1234     //Pone la ↩
    interfaz wlan0 en modo ad-hoc con identificador de red wlaisa1 y en el canal 1, con clave de ↩
    encriptacion en formato hexadecimal "abcdef1234".
```

Si el resultado de esta configuración es que el dispositivo está ocupado *Resource or device BUSY*, habrá que descativar la interfaz, ejecutar la configuración del *iwconfig* y finalmente acticar la interfaz:

```
PC20/21 # ip link set down dev wlan0
PC20/21 # iwconfig  wlan0  essid wlaisa1  mode ad-hoc  channel 1 key abcdef1234     //Pone la ↩
    interfaz wlan0 en modo ad-hoc con identificador de red wlaisa1 y en el canal 1, con clave de ↩
    encriptacion en formato hexadecimal "abcdef1234".
```

```
PC20/21 # ip link set up dev wlan0
```

La comprobación de que el enlace ya está disponible puede hacerse visualizando el estado de la interfaz, ejecutando simplemente "iwconfig wlan0" en *PC20* o "iwconfig wlan0" en *PC21* y visualizando si dispone de una celda "Cell" uniforme en ambos equipos.

```
wlan0      IEEE 802.11b  ESSID:"wlaisa1"  Nickname:"Prism  I"
           Mode:Ad-Hoc  Frequency:2.422 GHz  Cell: 02:90:31:FC:DC:31
           Bit Rate:11 Mb/s   Sensitivity:1/3
           Retry min limit:8   RTS thr:off   Fragment thr:off
           Encryption key:7072-6F76-6973-696F-6E61-6C00-00   Security mode:open
           Power Management:off
           Link Quality:0  Signal level:0  Noise level:0
           Rx invalid nwid:0  Rx invalid crypt:5  Rx invalid frag:0
           Tx excessive retries:379  Invalid misc:0   Missed beacon:0
```

Los equipos que ejecutan el comando de configuración *iwconfig* en modo ad-hoc, comprobarán la existencia de una red ad-hoc con el mismo nombre, y si no la encuentran, crean una. De esa forma, el primero que ejecuta el comando *iwconfig wlan0 essid wlaisa1 mode ad-hoc channel 1 key abcdef1234* crea la red ad-hoc, y el segundo que lo ejecuta se añade a ella.

Esto puede visualizarse en el parametro "Cell" de la salida *iwconfig* ya comentado, donde la dirección MAC que aparece en ambos equipos será la del equipo que creó la red ad-hoc.

Si alguno de los PCs no tiene asignada ninguna celda "Cell" en el enlace, el enlace no está operativo y habría que comprobar qué pasa. Algunas vias de comprobación y/o solución serían usar el comando *dmesg* y visualizar si da algo de información, reiniciar la interfaz mediante los comandos *ip link set down* y *ip link set up* o proceder a la repetición de todo el proceso. Mientras en la salida del comando *iwconfig* no aparezca una dirección MAC en el campo "Cell" no se continuará la práctica.

3.1.2. Direccionamiento IP

En la conexión *PC20*-*PC21* se trabajará con la red IP *192.168.101.0/24* además de diferentes redes que ya están creadas o forman parte del esquema general de las prácticas. En todo caso, será necesario dotar de las direcciones IP adecuadas a cada interfaz de los equipos de la práctica, quedando finalmente como muestra la figura 5.

Se utilizará el direccionamiento del esquema de la práctica. Para crear las direcciones se utilizará el comando *ip addr* . Se recomienda ejecutar *ip addr help* y *man ip* para conocer las posibilidades y sintaxis del comando. Inicialmente se eliminarán las anteriores direcciones que existiesen en la interfaz con el comando *ip addr flush* como se indica en cada una de las interfaces de los equipos, para partir de una configuración IP limpia.

Nota: los nombres de las interfaces *wlan0* y *wlan1* pueden no corresponderse con los encontrados en los equipos del laboratorio. Consultar al profesor.

- *PC20*:

```
PC20 # ip addr flush dev wlan0      //Elimina las direcciones IP de la interfaz wlan0
PC20 # ip addr flush dev wlan1      //Elimina las direcciones IP de la interfaz wlan1
PC20 # ip addr flush dev eth0       //Elimina las direcciones IP de la interfaz eth0
PC20 # ip addr add 192.168.201.120/24 dev wlan1     //Pone la direccion ip ↩
     192.168.201.120/24 en la interfaz wlan1

PC20 # ip addr add 192.168.101.120/24 dev wlan0     //Pone la direccion ip ↩
     192.168.101.120/24 en la interfaz wlan0

PC20 # ip addr add 192.168.29.120/24 dev eth0       //Pone la direccion ip ↩
     192.168.29.120/24 en la interfaz eth0

PC20 # ip addr      //Visualiza el direccionamiento en todas las interfaces.
```

- *PC21*:

```
PC21 # ip addr flush dev wlan0      //Elimina las direcciones IP de la interfaz wlan0
PC21 # ip addr flush dev eth0       //Elimina las direcciones IP de la interfaz eth0
PC21 # ip addr add 192.168.101.121/24 dev wlan0
PC21 # ip addr add 192.168.204.121/24 dev eth0
PC21 # ip addr
```

3.1.3. Conectividad

Es el momento de comprobar conectividad a nivel de aplicación entre los equipos. Para ello se utilizarán dos procedimientos consecutivos, mediante el envio/recepción de mensajes ICMP, y mediante comprobación del rendimiento con *iperf* .

1. Conectividad ICMP Ejecutar *ping* entre *PC20* y *PC21*.

```
PC20 # ping 192.168.101.121
```

```
PC21 # ping 192.168.101.120
```

Si hay respuesta en ambos casos, se procederá a pruebas de rendimiento:

2. Rendimiento

iperf es una aplicación cliente-servidor para linux, windows y mac. Genera tráfico entre el cliente y el servidor y presenta estadísticas sobre su velocidad, pérdidas y retardos.

Se pondrá *PC20* como servidor y *PC21* como cliente.

```
PC20$ iperf -s
```

```
PC21$ iperf -d -c 192.168.29.120
```

El resultado se presenta tras algunos segundos, donde se puede ver la capacidad de la conexión en ambos sentidos.

3.1.4. Filtrado MAC

En este enlace se realizará filtrado por MAC mediante "iptables"

1. Averiguar la MAC de la interfaz implicada en cada equipo

```
PC20/21 # iwconfig  wlan0
```

El comando anterior presenta la MAC de wlan0, aunque se puede visualizar ejecutando *ip link* " y localizándola visualmente en la salida.

2. Dejar pasar SÓLO los paquetes que tengan esa MAC en el campo "MAC ORIGEN" de la cabecera Ethernet.

```
PC20 # iptables -A INPUT  -i wlan0  -m mac ! --mac-source <MAC_PC21>  -j DROP  //Elimina los ↩
    paquetes que no tengan como MAC origen "MAC_PC21"
PC21 # iptables -A INPUT  -i wlan0  -m mac ! --mac-source <MAC_PC20>  -j DROP  //Elimina los ↩
    paquetes que no tengan como MAC origen "MAC_PC20"
```

3. Depuración

Para conocer las reglas que se están ejecutando en *iptables* y confirmar que se están ejecutando las anteriores, se ejecuta:

```
PC20/21 #  iptables  -L     //Visualiza las reglas de interfaces que se estan ejecutando
```

Para eliminar alguna regla que esté errónea o que ya no haga falta, es necesario fijarse en qué número de línea en que está la regla dentro de la cadena (en este caso la cadena es INPUT). El número de línea puede verse ejecutando *iptables -L* . Para eliminarla se ejecuta

```
PC20/21 # iptables  -D  INPUT  <numerodelinea>  //Elimina la regla iptables de la linea "↩
    numerodelinea"
```

Se pueden realizar las mismas pruebas de conectividad que en 3.1.3.

3.2. Conexión PC20-PC22 (a través de AP1)

PC20 se conectará a *PC22* a través de *AP1* mediante una conexión en modo infraestructura, de forma que esta conexión básicamente consiste en la configuración de *AP1* como master desde *PC22* y la configuración de *PC20* como slave.

3.2.1. Configuración de capa de enlace entre AP1 y PC20

Para la configuración del punto de acceso *AP1* será necesario acceder a él desde el equipo *PC22*. El *AP1* tiene como estado inicial el siguiente:

```
Dir. IP de gestion: 192.168.10.1/24
Canal: 11
ESSID: OpenWRT
KEY OFF
Administracion:
    acceso: a traves del navegador en el puerto 80
    usuario: root
    clave: provisional
```

Toda la configuración podrá realizarse desde el equipo *PC22*, que está directamente conectado al *AP1* a través de la red Ethernet cableada. Al ser la interfaz de configuración en modo web-gráfico, se deja al usuario navegar por las distintas opciones.

Se configurará primero el conjunto *AP1*-*PC22* y posteriormente el otro extremo de la conexión *PC20*

- *AP1*

  Será necesario acceder al dispositivo *AP1* según su configuración inicial desde *PC22*:

  Configuración de la red:

  ```
  PC22 #  ip addr add 192.168.10.122/24  dev  eth0    //Asocia la direccion IP dada a la interfaz↩
      eth0
  ```

  ```
  PC22 #  ping 192.168.10.1              //Comprobacion de conectividad con icmp.
  ```

  En este punto, existe conectividad con el *AP1* Linksys WRT54GL , y se accederá a *AP1* a través de un navegador web en la url *http://192.168.10.1*.

  En el caso de esta práctica y de este modelo de AP, cuando solicite autentificación, se pondrá como usuario "root" y se pondrá como clave "provisinal", tal y como se muestra en las condiciones iniciales del *AP1*. Una vez accedido al entorno de configuración, deberá configurarse la red servida por *AP1* en modo Infraestructure, con el *AP1* en modo Master. Se pondrá un ESSID "wlaisa2" y utilizará un canal poco saturado o en el caso de varias posibilidades el canal 6. No llevará encriptación.

- *PC20*

  PC20 deberá conectarse en modo Managed (o slave) a través de la interfaz wlan1 hacia *AP1*. se partirá del hecho de que ya exista una "celda wifi" operativa creada desde *AP1* con las siguientes características:

  ```
  Dir. IP de operacion: 192.168.10.1/24
  Canal: 6
  ESSID: wlaisa2
  KEY OFF
  Administracion:
      acceso: a traves del navegador en el puerto 80
      usuario: root
      clave: provisional
  ```

Toda la configuración de *AP1* habrá sido realizada desde el equipo *PC22*, que está directamente conectado al *AP1* a través de la red Ethernet cableada.

Se presentan los comandos a ejecutar en el equipo *PC20*, pues se supone que *AP1* ya está sirviendo una celda Wifi con ESSID "wlaisa2" sin encriptación. El comando siguiente visualiza las redes Wifi captadas por la interfaz de wlan1 de *PC20*.

```
PC20 # iwlist wlan1 scanning    //Visualiza las redes captadas por la interfaz wlan1 y sus ↩
    caracteristicas publicas
```

PC20 se deberá conectar a la red "wlaisa2" de *AP1*, suponiendo que esta está sirviendo en el canal 6.

```
PC20 # iwconfig  wlan1  essid wlaisa2  mode managed channel 6 key off   //Pone la interfaz ↩
    wlan1 en modo managed con identificador de red wlaisa2 y en el canal 6, sin clave de ↩
    encriptacion.
```

La comprobación de que el enlace ya está disponible puede hacerse visualizando el estado de la interfaz, ejecutando simplemente "iwconfig wlan1" en *PC20*.

```
wlan1      IEEE 802.11b  ESSID:"wlaisa2"  Nickname:"Prism  I"
           Mode:managed  Frequency:2.422 GHz  Cell: 02:90:31:FC:DC:31
           Bit Rate:11 Mb/s   Sensitivity:1/3
           Retry min limit:8   RTS thr:off   Fragment thr:off
           Encryption key:off   Security mode:open
           Power Management:off
           Link Quality:0  Signal level:0  Noise level:0
           Rx invalid nwid:0  Rx invalid crypt:5  Rx invalid frag:0
           Tx excessive retries:379  Invalid misc:0   Missed beacon:0
```

Mientras no exista información de "Cell" conectada en la interfaz wlan1 no se procederá a la configuración del direccionamiento IP, debiendo resolverse previamente la conectividad en capa de enlace.

3.2.2. Direccionamiento IP

Será necesario modificar la configuración IP de *AP1* y *PC22* así como crear configuración IP para la interfaz wlan1 de *PC20* para definir la red deseada según el esquema de la práctica. La configuración del *AP1* se realiza por interfaz web, conectándose directamente a la IP *192.168.10.1*.

1. *AP1*-*PC22*

   Para la configuración lógica de red del *AP1*, será recomendable entrar en modo consola a través de `ssh` desde *PC22* e incluir la IP 192.168.201.4/24 según la figura 5.

   ```
   AP1 #  ip addr add 192.168.201.4/24 dev  br-lan     //Asocia la direccion IP dada a la interfaz↩
       puente br-lan
   ```

   Posteriormente se saldrá del entorno SSH desde *PC22* y se configurará *PC22* según la figura 5, con la IP *192.168.201.122/24*.

   ```
   PC22 #  ip addr add 192.168.201.122/24 dev eth0     //Asocia la direccion IP dada a la interfaz↩
       eth0
   PC22 #  ip addr del 192.168.10.122/24 dev eth0  //Elimina la direccion IP dada de la interfaz ↩
       eth0
   ```

   A partir de ese momento, todas las conexiones a *AP1* se realizarán a través de la IP *192.168.201.4*.

2. *PC20*

   El direccionamiento IP de *PC20* se corresponde con el esquema de la figura 5, donde la interfaz wlan1 tiene asignada la IP *192.168.201.120/24*. Por tanto lo único que será necesario hacer será dar de alta esa dirección IP en wlan1:

   ```
   PC20 #  ip addr add 192.168.201.120/24 dev wlan1    //Asocia la direccion IP dada a la interfaz↩
       wlan1
   ```

3.2.3. Conectividad

Se utilizará el mismo procedimiento que para la comprobación de la conectividad entre *PC20*-*PC21* 3.1.3. Las pruebas de conectividad siempre se harán tras el proceso de direccionamiento y enrutamiento.

3.3. Configuración del enrutamiento

El enrutamiento se realizará bajo el principio de conectividad entre todas las redes implicadas en la práctica, la red A1, la red B1 y la red de enlace punto a punto W1. El enrutamiento es una capacidad que no suele venir por defecto en las configuraciones base de los PC's, por lo que será necesario activarla. Esto se realiza mediante la activación de un parámetro del kernel en el sistema de ficheros /proc. En *PC22* y *PC21* se ejecutará:

```
PC20 # echo 1 > /proc/sys/net/ipv4/ip_forward   //Para activar el enrutamiento
PC20 # cat  /proc/sys/net/ipv4/ip_forward       //Para comprobar el enrutamiento
1                       //Enrutamiento activado

PC21 # echo 1 > /proc/sys/net/ipv4/ip_forward
PC21 # cat  /proc/sys/net/ipv4/ip_forward
1
```

Para que esto sea así cada vez que arranque el equipo, será necesario poner la siguiente línea en el fichero */etc/network/options*.

```
ip_forward=yes
```

Para la configuración de las tablas de enrutamiento se utilizará el comando `ip route`. Se recomienda ejecutar `ip route help` para conocer las posibilidades y sintaxis del comando.

- PC20:

```
PC20 # ip route add 192.168.204.0/24 via 192.168.201.1 dev wlan0    // Anhade la ruta a la red ↩
    192.168.204.0/24 a traves de R1 (pasando por AP1) y por la interfaz propia wlan0

PC20 # ip route add default via 192.168.29.1 dev eth0       // Anhade la ruta a cualquier red ↩
    no especificada (Internet) a traves del gateway GW y por la interfaz propia eth0

PC20 # ip route     //Visualiza la tabla de rutas de PC20.
```

- PC21:

```
PC21 # ip route add 192.168.201.0/24 via 192.168.101.120 dev wlan0  // Anhade la ruta a la red ↩
    192.168.201.0/24 a traves de PC20 y por la interfaz propia wlan0

PC21 # ip route add default via 192.168.101.120  dev wlan0  // Anhade la ruta a cualquier red ↩
    no especificada (Internet) a traves de PC20 y por la interfaz propia wlan0

PC21 # ip route     //Visualiza la tabla de rutas de PC21.
```

- PC22:

```
PC22 # ip route add 192.168.204.0/24 via 192.168.201.120 dev eth0   // Anhade la ruta a la red ↩
    192.168.204.0/24 a traves de PC20 y por la interfaz propia eth0

PC22 # ip route add default via 192.168.201.1 dev wlan0     // Anhade la ruta a cualquier red ↩
    no especificada (Internet) a traves de R1 y por la interfaz propia eth0

PC22 # ip route     //Visualiza la tabla de rutas de PC22.
```

De esta forma, se tienen que configurar las interfaces y los enlaces cada vez que se reinician los equipos, pudiéndose editar el fichero /etc/network/interfaces, para que se configure en el arranque. El formato podría ser (en el caso de *PC21*):

```
auto wlan0
```

```
iface wlan0 inet static address 192.168.204.121
netmask 255.255.255.0
network 192.168.204.0
broadcast 192.168.204.255
wireless-mode ad-hoc
wireless-channel 1
wireless-essid wlaisa1
wireless-key s:abcdef1234
```

y tras rearrancar los equipos tendrían la configuración almacenada.

4. Pruebas

La conectividad se comprobará entre *PC21* y *PC22* utilizando el procedimiento descrito en 3.1.3. Si no hubiese conectividad se comprobaría la conectividad en cada una de las conexiones de forma individual.

Para comprobar la conectividad, será necesario el envío y recepción de paquetes ICMP entre todos los equipos de la red wireless. El envío y recepción de paquetes ICMP se realiza con el comando *ping* .

Se recomienda comprobar algunos de los parámetros de enlace mediante el aplicativo *iperf* . Para ello se puede visualizar la práctica dedicada a TCP/IP (práctica 2) y poner al equipo *PC21* como servidor y *PC22* como cliente.

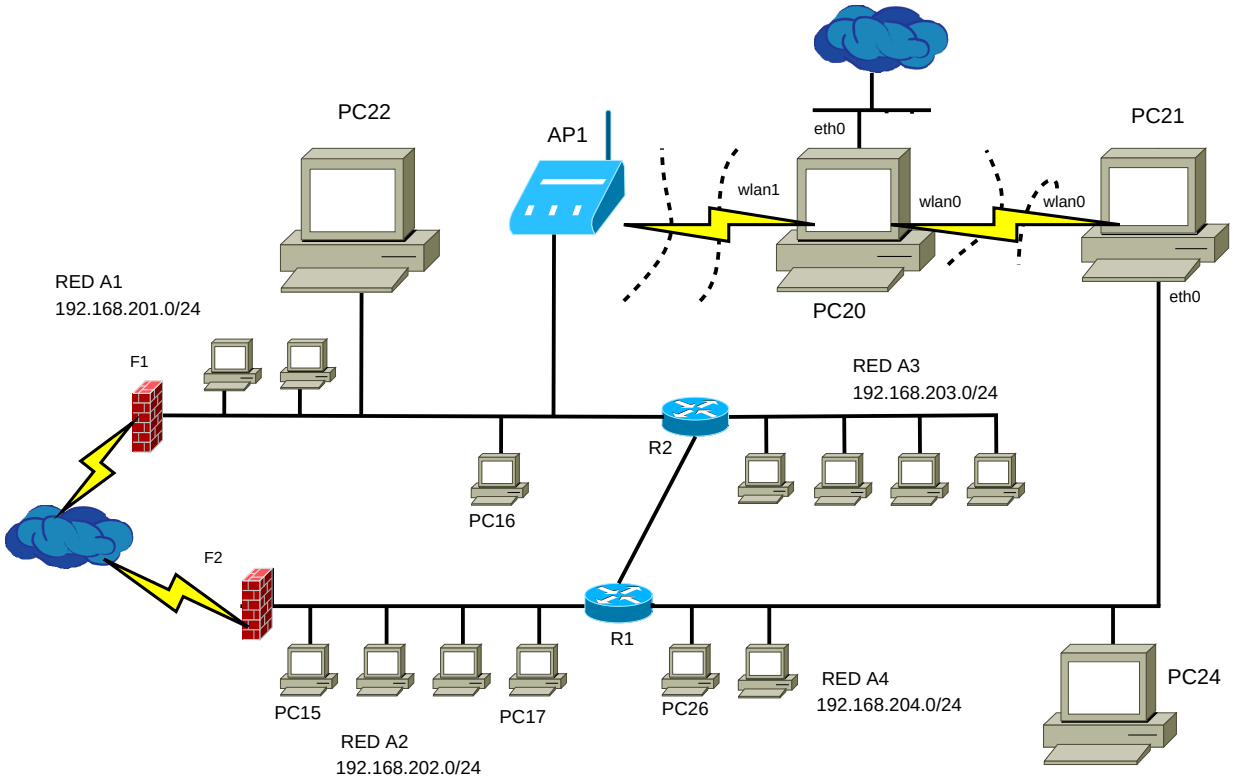

Figura 6: Visión general de la práctica

5. ANEXO. Tarjetas inalámbricas

Los tres tipos de tarjetas inalámbricas con conectividad USB al PC serían:

- Tarjetas Zydas con chipset ZD1211B

```
root@PC20:~# lsusb
.....
Bus 001 Device 004: ID 0ace:1215 ZyDAS ZD1211B 802.11g
......
```

La instalación de estas tarjetas no requiere en kernels 3.2 o superiores de ninguna configuración adicional, salvo que los kernels se hayan compilado para que los módulos no se carguen en el inicio. En ese caso hay que compilar el módulo zd1211rw e insertarlo.

- Tarjetas eRize con chipset Realtek RTL8188SU

  ¡¡¡ IMPORTANTE !!!!. Estas tarjetas requieren que el programa NetworkManager esté deshabilitado. Ver la siguiente sección para ver cómo.

Figura 7: Tarjetas eRize

```
root@PC20:~# lsusb
.....
Bus 001 Device 002: ID 0bda:8171 Realtek Semiconductor Corp. RTL8188SU 802.11n WLAN Adapter
......
```

Las características de las tarjetas:

```
eRize ERZWN150-USB03H400 Adaptador USB Wireless N 150 high power 400 mW Chipset Realtek 8188SU ↩
     antena 5 dbi.

Support advanced 1 x 1 Technology with up to 150Mbps downstream data rate
- Low Noise Amplifier(LNA) support
- Complies with 2.4GHz IEEE802.11n and IEEE802.11b/g standards
- Support 20MHz and 40MHz bandwidth
- Multiple BSSID support
- Wireless security - 64/128bit WEP, WPA and WPA2
- QoS enhancement - WMM
- Link/Activity LED indicator
- USB 2.0 Interface

Specification:
Standard IEEE 802.11b/g/n
Frequency Band 2.412GHz~2.484GHz ISM band
Data Rate
802.11b: 11, 5.5, 2 and 1 Mbps with auto-rate fall back
802.11g: 54, 48, 36, 24, 18, 12, 9 & 6Mbps
802.11n(20MHz): up to 72Mbps
802.11n(40MHz): up to 150Mbps
Working mode Infrastructure
Ad-Hoc
Chipset Realtek 8188SU
Interface USB 2.0 A-Type
Antenna One detachable 5 dBi antenna (SMA connector)
Transmitter Power
802.11b: up to 25 +- 1 dBm
802.11g: up to 20 +- 1 dBm
802.11n: up to 19 +- 1 dBm
```

```
Receive Sensitivity
-95dBm @ 802.11b
-92dBm @ 802.11g
-90dBm @ 802.11n
Media Access Control CSMA/CA
Operation Voltage 5V DC
Security
64/128bit WEP
WPA(TKIP with IEEE 802.1x)
WPA2(AES with IEEE 802.1x)
WPA Mixed
Operating Temperature 0C ~ 60C
Storage Temperature -20C ~ 70C ambient temperature
Storage Humidity 10% ~ 90% (Non-condensing)
Size 49(L) x 26(W) x 10(H) (not including antenna)
Package Contents
WLAN USB Dongle x1
5dBi dipole antenna x1
```

La instalación de estas tarjetas requiere disponer del módulo r8712u. Este módulo está localizado en el área "staging" del kernel, por lo que no está proveido con las imágenes de debian hasta la versión 6. . Podría descargarse el módulo precompilado (r8712u.ko) de algún lugar de la red. El proceso para disponer del módulo sería (disponiendo de las fuentes del kernel).

1. Disponer de herramientas de compilación

```
$ sudo apt-get install build-essential libncurses5-dev
```

2. Ir al directorio de las fuentes del kernel y entrar en entorno menuconfig:

```
$ cd /usr/src/kernel/linux-3.2.9/
$ sudo make menuconfig
```

3. Entrar en la sección del módulo de la tarjeta y seleccionar el módulo:

```
Device Drivers  --->
   Staging drivers  --->
(M) RealTek RTL8712U (RTL8192SU) Wireless LAN NIC driver
```

4. Compilar el módulo y copiarlo a la carpeta de módulos

```
$ sudo make modules
......
$ sudo cp drivers/staging/rtl8712/r8712u.ko   /lib/modules/3.1.9+/kernel/net/wireless/
```

Tras disponer del módulo será necesario descargarse el firmware realtek:

```
$ sudo apt-get install firmware-realtek
```

Finalmente será necesario insertar el adaptador en un puerto USB disponible. Si este adaptador ya estaba insertado, puede ser necesario cargar el módulo:

```
$ sudo depmod -a
$ sudo modprobe r8712u
$ dmesg

r8712u: module is from the staging directory, the quality is unknown, you have been warned.
usbcore: registered new interface driver r8712u
usb 1-1.2: new high speed USB device number 6 using dwc_otg
usb 1-1.2: New USB device found, idVendor=0bda, idProduct=8172
usb 1-1.2: New USB device strings: Mfr=1, Product=2, SerialNumber=3
usb 1-1.2: Product: RTL8188SU WLAN Adapter
usb 1-1.2: Manufacturer: Manufacturer Realtek
usb 1-1.2: SerialNumber: 00e04c000001
r8712u: DriverVersion: v7_0.20100831
r8712u: register rtl8712_netdev_ops to netdev_ops
r8712u: USB_SPEED_HIGH with 4 endpoints
r8712u: Boot from EFUSE: Autoload OK
r8712u: CustomerID = 0x000a
```

```
r8712u: MAC Address from efuse = 00:aa:bb:cc:dd:ee
r8712u: Loading firmware from "rtlwifi/rtl8712u.bin"
r8712u: 1 RCR=0x153f00e
r8712u: 2 RCR=0x553f00e
```

Se comprobará que se ha instalado correctamente, de forma que aparezca la tarjeta en la salida del comando *iwconfig*.

```
$ lsusb
$ dmesg
$ sudo iwconfig
$ iwconfig

lo        no wireless extensions.
eth0      no wireless extensions.
wlan0     unassociated  Nickname:"rtl_wifi"
          Mode:Auto  Access Point: Not-Associated   Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

- Tarjetas Alfa con chipset Ralink RT2870

```
root@PC20:~# lsusb
.....
Bus 002 Device 004: ID 148f:3070 Ralink Technology, Corp. RT2870/RT3070 Wireless Adapter
......
```

Figura 8: Tarjetas Alfa

Las características baśicas son:

```
eRize ERZWN150-USB03H400 Adaptador USB Wireless N 150 high power 400 mW Chipset Realtek 8188SU ↩
     antena 5 dbi.

Model    AWUS036H V5
Standards    Wireless: IEEE 802.11b/g
USB 2.0 standard
Data Rate    802.11b: UP to 11Mbps
802.11g: 54Mbps
OS Supported     Windows 98SE, Windows ME, Windows 2000, Windows XP, Linux 2.6, Mac 10.4
Interface    USB 2.0 mini USB
Antenna Type     1 x 2.4Ghz SMA connector
Chipset      Realtek 8187L !!!!!!OJO NO DETECTA ESTE CHIPSET!!!!!
One LED      Power/Status, Wireless Act.
Frequency Range      2412~2462 MHz (N.A)
2412~2472 MHz (EU)
2412~2484 MHz (Japan)
Channel      1~11 channels ( North America )
1~13 channels ( General Europe)
1~14 channels (Japan)
Emission Type    DSSS/OFDM
Output Power     24dBm (OFDM), 30dBm(CCK)
Sensitivity for 802.11b      1, 2 Mbps (BPSK, QPSK): - 96dBm
11 Mbps (CCK): -91dBm
(Typically @PER < 8% packet size 1024 and
@25C + 5C)
```

```
Sensitivity for 802.11g      54Mpbs (64QAM): -76dbm
48Mbps (64QAM): -71dbm
36Mpbs (16QAM): -78dbm
24Mbps (16QAM): -80dbm
18Mbps (QPSK): -81dbm
12Mpbs (QPSK): -82dbm
9Mbps (BPSK): -85dbm
6Mbps (BPSK): -91dbm
(typically @PER < 10% packet size 1024 and @25C + 5C)
Frequency Stability      within +25 ppm
Data Modulation Type     BPSK,QPSK, CCK and OFDM
Power    Voltage: 5V+5%
Security     WEP 64/128
802.1X support
Wi-Fi Protected Access (WPA)
WPA-PSK
WPA II
Operating Temp   0C ~ +50C
Storage      -10C ~ +65C
Humidity     5%~98% non-condensing
Dimention    8.5*2.2*6.3cm
Weight   38.5g
```

La instalación del firmware de estas tarjetas requiere símplemente de su descarga desde los repositorios:

```
$ sudo apt-get install firmware-ralink
```

Finalmente se insertará la tarjeta a través del puerto USB y se comprobará su operatividad:

```
$ lsusb
$ dmesg
$ sudo iwconfig
$ iwconfig

lo        no wireless extensions.
eth0      no wireless extensions.
wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
```

Referencias

[1] M. Gast, *802.11 Wireless networks: : The Definitive Guide - Creating and Administering Wireless Networks*. Sebastopol CA, USA: O'Reilly & Associates, Inc., 2002.