Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 8- Configuración de Access Point y cliente WiFi

1- Objetivos

En esta práctica veremos el funcionamiento básico de una red WiFi en la que tenemos un punto de acceso (Access Point, AP) comercial y clientes WiFi PCs con sistema operativo Linux. Configuraremos PCs como clientes de este AP, simultáneamente a PCs en el sistema de distribución cableado. Finalmente, emplearemos las funcionalidades de enrutamiento de los equipos para encaminar el tráfico de la red inalámbrica hacia el laboratorio.

2- Conocimientos previos

- Conocimientos básicos sobre WiFi
- Configuración de IP en PCs Linux

Para la realización de esta práctica necesitará un interfaz 802.11 USB que le prestará el profesor de prácticas. Este interfaz lo puede conectar en cualquiera de los 3 PCs de prácticas, aunque suele tener sentido conectarlo en PCB ya que PCA y PCC ya tienen un interfaz inalámbrico. A diferencia de los interfaces de PCA y PCC, este interfaz USB le permitirá capturar con wireshark el tráfico de las WLANs viendo las tramas completas 802.11 y será el que deba emplear siempre que en la práctica se indique que capture el tráfico de la WLAN.

3- Acceso y configuración de un AP/WirelessRouter comercial

En primer lugar vamos a ver un típico interfaz de configuración de un punto de acceso comercial de bajo coste. En el armario de prácticas dispone de un Cisco Linksys WRT54G. Si ha encontrado el manual de configuración sabrá que dispone de un servidor web interno mediante el cual sirve unas páginas que permiten especificar los parámetros de configuración del equipo. El equipo funciona no solo como un AP sino también como un router (si funcionara solo como AP no necesitaría implementar el nivel IP). Por ello tiene dos interfaces, uno es el llamado interfaz WAN y el otro el interfaz LAN. En el interfaz LAN dispone de un switch de 4 puertos FastEthernet. Por defecto está preconfigurado para ser accesible su servidor web de configuración solo através del interfaz LAN. El manual de configuración del equipo especifica la dirección IP y máscara de subred empleada en él. Configure en el PC B una dirección de la misma red, interconéctelos y acceda mediante un navegador a la página web que sirve el equipo. Si tiene problemas pruebe a resetear la configuración del equipo (debería estar indicado cómo hacerlo en su manual).

Si ignoráramos el interfaz WAN y por lo tanto la capacidad de encaminamiento del equipo nos encontraríamos con un AP con su interfaz inalámbrico y 4 puertos ethernet en el sistema de distribución cableado.

Estudie las opciones de configuración del equipo. Localice el método de configuración de las siguientes funcionalidades:

- Dirección IP del interfaz LAN o local
- Configuración de la dirección IP del interfaz WAN
- Servidor de DHCP interno para la red local

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

- Configuración de la tabla de rutas
- SSID
- Canal WiFi
- Velocidad de transmisión de la WiFi
- Parámetros de QoS

4- Configuración de un cliente WiFi

A continuación configuraremos un cliente de la WiFi de este accesspoint. Comience por dar a su AP un SSID que le permita distinguirlo del de sus comañeros. Para ello, emplee como SSID el nombre de su armario (por ejemplo "armario15").

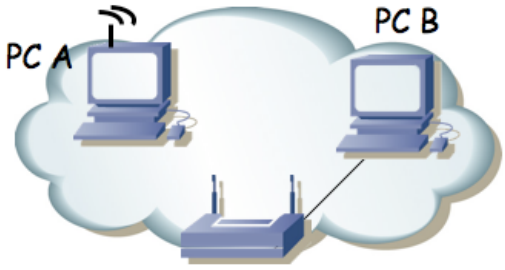

Figura 1.- Accesspoint y cliente

Ahora en PC A configuraremos el intefaz WiFi (`wlan0`). El interfaz puede funcionar en diferentes modos (excluyentes). Los principals son:

- Managed (gestionado): Es el modo en el que se asocia a un punto de acceso.
- Ad-Hoc: Para una WLAN sin punto de acceso (comunicación peer-to-peer entre los terminales inalámbricos).
- Monitor: Permite a aplicaciones (tcpdump, wireshark, tshark, etc) capturar las tramas 802.11. En los otros modos el interfaz y el driver transforman las tramas 802.11 en tramas 802.3 (DIX), además de no entregar al resto del sistema las tramas de gestión de la WLAN.

Para configurar parámetros del protocol IP en el interfaz wlan0 emplearemos *ifconfig* pero para configurar la parte 802.11 usaremos *iwconfig*. Puede ver el estado actual del interfaz con:

```
% iwconfig wlan0
```

Puede ver los canales soportados por su interfaz con:

```
% iwlist wlan0 frequency
```

En primer lugar configure el modo *Managed* si no lo está ya:

```
% sudo iwconfig wlan0 mode managed
```

y active el interfaz (`sudo ifconfig wlan0 up`).

Ahora puede localizar los puntos de acceso a su alrededor con:

```
% sudo iwlist wlan0 scanning
```

Cada WLAN encontrada ha sido por recibir anuncios del punto de acceso. Dichos anuncios (*beacons*) son paquetes 802.11 enviados por la WLAN correspondiente y por lo tanto vienen por

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

uno de los canales de la banda correspondiente (en este caso la de 2.4GHz).

Revise los puntos de acceso que está encontrando. En el listado podrá ver el canal que están empleando. Puede haber varios empleando el mismo canal, en cuyo caso tendrán que compartir la capacidad del mismo (para eso está el control de acceso al medio). Los anuncios le dirán un "nombre" de la WLAN junto a la etiqueta ESSID. Por ejemplo es común que puedan ver el ESSID "UPNA", que es anunciado por los puntos de acceso del Servicio Informático (SI) para acceso a Internet de alumnos. También puede encontrar el ESSID "eduroam". El ESSID es lo que permite distinguir las tramas de un canal si corresponden a una WLAN o a otra que esté empleando el mismo canal.

Debería encontrar en el listado el anuncio el del AP que ha configurado al principio de la práctica. Compruebe la dirección MAC que anuncia ese AP, que es el auténtico identificador de la WLAN en los paquetes. No se confunda entre su punto de acceso y el de otro grupo (si han puesto bien el ESSID deberían ser fáciles de distinguir). ¿Podría intentar adivinar el fabricante de cada AP que ve? Compruebe que el canal es el que ha configurado en su punto de acceso.

Puede que encuentre varios anuncios del ESSID "UPNA", que vendrán con diferente dirección MAC del AP. Esto corresponde a diferentes APs que están anunciando el mismo nombre de WLAN. Aunque empleen el mismo nombre lo que en realidad distingue los paquetes de una WLAN de los de otra del mismo canal es el ESSID (la dirección MAC del AP), el cual no debe coincidir.

En los *beacons* que se reciben como resultado del scan se obtiene también información del tipo de seguridad empleada en la WLAN así como las velocidades soportadas por el AP.

Para asociar el interfaz inalámbrico del PC a un punto de acceso puede hacerlo indicándole al interfaz el ESSID de la WLAN:

```
% sudo iwconfig wlan0 essid NOMBRE
```

Tenga cuidado de no asociarse al AP de otro grupo de prácticas.

A partir de este punto podrá ver con `iwconfig` a qué AP se ha asociado su interfaz WiFi. Confirme la dirección de dicho AP.

Configure una dirección IP de la red local en el interfaz inalámbrico (con *ifconfig*) y compruebe que puede acceder desde PC A al PC B. Si ha dejado activo en su AP un servidor de DHCP podría emplear un cliente de DHCP en el PC ara obtener la configuración IP (esto no es algo particular de WiFi, ni hace falta que el servidor de DHCP esté en el AP, como ya sabrá de otras asignaturas, pero si tiene dudas consulte con el profesor de prácticas). Si tiene interés investigue el programa *dhclient*. En el resto de la práctica se supondrá que ha hecho una configuración manual con *ifconfig*.

Podríamos repetir la configuración del PC A en el PC C y tener con ello dos terminales inalámbricos. Recuerde que la comunicación entre ellos pasa por el punto de acceso (salvo en modo Ad-hoc) y que por lo tanto los paquetes circulan dos veces por el medio aéreo. Además, el control de acceso al medio (CSMA/CA) se emplea en la comunicación de un PC hacia el AP y después desde el AP hacia el otro PC. Reflexione sobre las implicaciones que esto tiene en el throughput que puede obtener una aplicación que intente transferir un fichero de un PC al otro por el medio inalámbrico (suponiendo que los terminales están junto al AP y no hay problemas de interferencias, atenuación, etc).

El driver de estar tarjetas inalámbricas nos permite ver todas las tramas 802.11. Para ello, en lugar

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

de emplear el modo *Managed* y asociarnos a un punto de acceso debemos emplear el modo *Monitor*. En ese modo, las tramas que el driver entregará serán las tramas 802.11 completas, sin ocultarnos además las tramas de gestión (confirmaciones, *probes,* mensajes de autentificación, asociación, etc). Serán las tramas que se reciban por un canal. El interfaz debe sintonizarse a una frecuencia, la de un canal, así que podremos recibir solo las tramas de las WLANs que empleen ese canal y habrá que reconfigurar el interfaz para recibir las tramas de otras WLANs que estén empleando otro canal. Podremos hacer esto correctamente solo con el interfaz WiFi USB ya que las tarjetas inalámbricas de PC A y PC C no funcionan bien en modo *Managed* con el driver que tienen instalado estos PCs.

Emplearemos el PC C o el PC B con la NIC WiFi USB. En general en esta práctica puede ser más interesante conectarla al PC B, de forma que se tiene aún el PC A y el PC C con sus propias NICs WiFi internas. Para colocar el interfaz en modo monitor, en primer lugar debe desactivar el interfaz (*sudo ifconfig wlan0 down*) si estaba activo, para a continuación cambiar el modo (verifique que al conectar la NIC USB aparece el interfaz wlan0 pues si ya tiene un wlan0 porque lo conecte a un PC que ya tiene una NIC WiFi se llamará de otro modo):

```
% sudo iwconfig wlan0 mode monitor
```

Vuelva a levantar el interfaz.

Configure ahora el interfaz para emplear el canal 1 (probablemente sea el que emplee por defecto):

```
% sudo iwconfig wlan0 channel 1
```

Empiece a capturar del interfaz. Debería ver las tramas 802.11 de todas las WLAN que están empleando ese canal. Si por ejemplo configuró su AP en el canal 5 no verá sus tramas y tendrá que reconfigurar el interfaz para que se sintonice en ese canal.

Empleando `tcpdump` o `wireshark` para ver todas las tramas estudie:

- Los beacons enviados por el AP
- El proceso de asociación del PC A (desactive y vuelva a activar su interfaz para verlo)
- El envío de paquetes entre un host en la red inalámbrica y otro en la LAN cableada
- Asocie PC A y PC C con sus NICs internas al AP y envíe tráfico entre ellos. Haga ping de un PC inalámbrico al otro y estudie las tramas 802.11 que viajan y cómo las reenvía el AP emplando el tráfico capturado por la NIC USB.

Emplee las capacidades de filtrado del sniffer para localizar con mayor facilidad las tramas.

Punto de acceso: Muestre a su profesor de prácticas el escenario con el cliente asociado al AP

5- Router WiFi

Ahora emplearemos ambos interfaces enrutados del Linksys WRT54G. En primer lugar en la sección de configuración del mismo *"Setup – Advanced Routing"* asegúrese de que tiene seleccionado el modo de operación *"Router"*. Si tuviera seleccionado *"Gateway"* entonces el equipo actuaría también como un NAT, lo cual en el siguiente escenario no nos interesa. También es recomandable que en la sección *"Security – Firewall"* desactive la protección del Firewall así como desactive la opción *"Block Anonymous Internet Requests"* (averigüe qué hace esa opción).

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

A continuación lleve a cabo la configuración de la figura 2. Tenemos 2 redes. En el lado LAN del WRT54G tenemos conectados a PC A y PC B. En el lado WAN tenemos a PC C. Seleccione las subredes que desee para esta configuración y compruebe que funciona la comunicación entre las máquinas de diferentes redes. Vea las tramas 802.11.

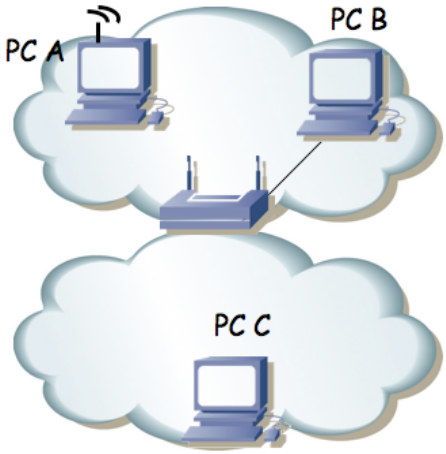

Figura 2.- Router WiFi en funcionamiento

Finalmente lleve a cabo la configuración de la figura 3. En el interfaz LAN empleará una red que depende de su armario de prácticas y será:

`00001010 . 00000011 . 0010 ABCD . XXXXXXXX / 24`

Donde ABCD forma el número de su armario. Por ejemplo en el armario 15 sería: `10.3.47.0/24`.

En el interfaz WAN (conectado al punto C de su puesto de prácticas en la mesa) empleará la configuración IP:

`00001010 . 00000011 . 00010001 . 0000 ABCD / 20`

Donde ABCD forma el número de armario. Por ejemplo en el armario 15 sería: `10.3.17.15/20`. Y el router por defecto en el WRT54G será `10.3.16.1`.

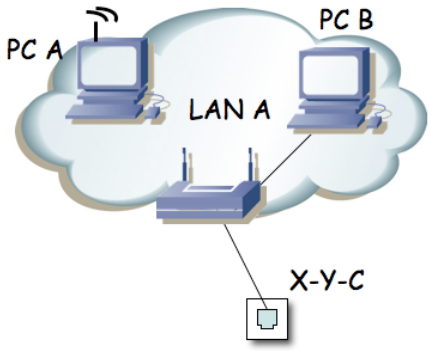

Figura 3.- Acceso de la red WiFi al laboratorio

Punto de control: Muestre el resultado de la configuración anterior