**Estudio experimental**

El estudio experimental de esta práctica consta de tres partes. En este estudio experimental se describen todos los pasos que el alumno debe realizar**, si tiene cualquier duda consulte con el profesor encargado de la sesión práctica**.

1. Asegúrese de que su PC está conectado a la red ETSII. Encienda su PC y arranque Windows 7. Desactive el firewall de Windows.
2. Descargue el archivo capturawlanp3def.pcap, que se encuentra en EV. Este archivo es imprescindible para la tercera parte de la práctica.

## Primera parte: Configuración dinámica de direcciones. DHCP

3. Ejecute el comando ipconfig/all y haga un ping a su puerta de enlace para comprobar su conectividad.
4. Inicie el programa Wireshark. En el filtro de visualización, introduzca **bootp or arp or icmp and not tcp.port==2008.** Ejecute en el Símbolo del Sistema el comando ipconfig/release. ¿Qué tipo de mensaje DHCP se captura?
5. Haga nuevamente un ping a su puerta de enlace. ¿Qué ocurre? ¿Por qué?
6. Compruebe que Wireshark sigue corriendo y ejecute el comando ipconfig/renew. Posteriormente, vuelva a ejecutar en ella el comando ipconfig /all.
7. ¿Cuál es ahora su dirección IP? ¿Coincide con la que tenía antes? ¿A qué cree que es debido?
8. ¿Cuál es la dirección IP del servidor DHCP? ¿A quién corresponde esa dirección?
9. ¿Cuándo obtuvo su concesión de la dirección IP? ¿Cuándo expira?
10. Observe la captura de Wireshark. Identifique el ciclo básico DHCP (mediante el Transaction Id. verá los mensajes DHCP correspondientes a una misma transacción). Fíjese que es posible que se hayan capturado algunos mensajes DHCP más que los cuatro del ciclo básico de DHCP. Esto es debido a que hay algunos mensajes DHCP en broadcast, por lo que puede que capture mensajes DHCP propiciados por otros hosts de su subred.
    a. ¿Cuántos mensajes tiene el ciclo básico DHCP?
    b. ¿Cuál es el tipo de los mensajes? ¿En qué opción del mensaje DHCP se observa?
    c. ¿Cuál es la dirección IP destino de los mensajes que envía el cliente?
    d. ¿Cuáles son los puertos utilizados?
11. Observe los mensajes DHCP DISCOVER y busque la opción 50 de BootP
    a. ¿Qué dirección IP había pedido el cliente?
    b. ¿Se le ha concedido? ¿Por qué?
12. Puede observar que hay un mensaje ARP denominado ARP gratuito. ¿Cuál es su finalidad? ¿Cuál es el valor en este tipo de mensajes de los campos “sender IP address” y la “target IP address”? ¿Por qué?
13. Abra el mensaje DHCP ACK del ciclo básico.
    a. ¿Cuántas opciones observa en el mensaje DHCP?
    b. ¿En qué opción se nos indica nuestro servidor DNS? Anote la dirección IP de dicho servidor.
14. Ejecute nuevamente ipconfig/renew.
    a. ¿Qué mensajes DHCP observa ahora? ¿Es necesario volver a ejecutar el ciclo básico completo? ¿Por qué?
    b. ¿Cuál es la IP destino del mensaje enviado por el cliente?

## Segunda parte: Enrutamiento en Internet (RIP)

15. **Haga este punto sólo si está en el laboratorio G1.31**. Si es así, desconecte su PC de la red ETSII y conéctelo a la intranet del laboratorio, concretamente al HUB_EUROPA (si está en el PC de la izquierda) o al HUB_ASIA (si está en el PC de la derecha).

16. **Haga este punto sólo si está en el laboratorio G1.33**. Si es así, desconecte su PC de la red ETSII y conéctelo a la intranet del laboratorio, concretamente al HUB_SUDAMÉRICA (si está en el PC de la izquierda) o al HUB_NORTEAMÉRICA (si está en el PC de la derecha).
17. Abra una ventana de Símbolo del sistema y ejecute en ella el comando ipconfig /all. Anote su dirección IP.
18. Inicie el programa Wireshark. En el filtro de visualización, escriba rip
19. ¿Se dirige el tráfico RIP a su PC? ¿Por qué puede verlo?
20. ¿Cada cuánto tiempo llega un mensaje RIP?
21. ¿Qué versión de RIP se está utilizando?
22. Entre en alguno de los mensajes RIP ¿Qué redes vemos en cada mensaje? ¿Con qué métrica? ¿Qué significa esto?
23. Compare las redes que ve en su ordenador y las que ve su compañero.
    a. ¿Son las mismas redes? En caso contrario, ¿a qué cree que es debido?
    b. ¿Es la métrica la misma? ¿Por qué?

## Tercera parte: Análisis del tráfico inalámbrico

24. En esta parte de la práctica analizaremos tráfico inalámbrico, para lo que debe abrir el fichero capturawlanp3def.pcap, que descargó en el punto 2.
25. Observe la información suministrada por Wireshark. Podrá ver diferentes tramas de gestión 802.11, a saber:
    a. Beacon frame o trama baliza: La envía el AP periódicamente para informar de la existencia de una red inalámbrica.
    b. Probe Request: Sirve para que un cliente rastree un área en busca de redes inalámbricas.
    c. Probe Response: Respuesta de un AP a un Probe Request.
    d. Association Request: Sirve para que un cliente solicite conectarse a una red inalámbrica.
    e. Association Response: Respuesta a un Association Request.
26. Seleccione una de las Beacon frames. Abra la información referente a IEEE 802.11 y observe el campo Tipo/Subtipo. Anote su valor.
27. Seleccione el campo tipo/subtipo. Con el botón derecho del ratón, realice la acción “Apply as filter / Selected”. De esta forma, seleccionará todas las Beacon Frames de la captura.
    a. ¿Cuántos puntos de acceso (AP) han enviado Beacon Frames?
    b. Anote los identificadores del BSS (BSSID)
    c. ¿Cuántos SSID distintos puede ver?
28. Seleccione una de las tramas Probe response. Abra la información referente a IEEE 802.11 y observe el campo Tipo/Subtipo. Anote su valor y repita la operación del punto 5 para ver cuántas Probe Responses hay en la captura.
    a. ¿Cuántos puntos de acceso (AP) han enviado Probe Responses?
    b. Anote los identificadores del BSS (BSSID)
    c. ¿Cuántos SSID distintos puede ver?
29. Seleccione una de las tramas Association response. Abra la información referente a IEEE 802.11 y observe el campo Tipo/Subtipo. Anote su valor y repita la operación del punto 5 para ver cuántas Association Responses hay en la captura.
    a. Verá que solo un punto de acceso (AP) ha enviado Association Responses
    b. Anote el identificador del BSS (BSSID).
    c. ¿Cuántos clientes se han asociado a ese AP? ¿Cuáles son sus direcciones MAC?
    d. ¿Cuál es el SSID de la red? ¿Cómo lo sabe?
30. Quite todos los filtros, de manera que pueda ver también mensajes ICMP, que van en MAC_PDUs de datos y ACKs a estas MAC_PDUs de datos.
31. Observe la trama número 17.
    a. ¿Cuáles son las direcciones IP origen y destino?
    b. Abra la información correspondiente a IEEE 802.11. Verá que hay cuatro direcciones MAC.
        i. Receiver address: es la dirección MAC de quien recibe físicamente la trama.
        ii. Transmitter address: es la dirección MAC de quien envía físicamente la trama.
        iii. Destination address: es la dirección MAC de quien recibe lógicamente la trama de datos (Echo request).
        iv. Source address: es la dirección MAC de quien envía lógicamente la trama de datos (Echo request).

c. Puede ver que, mientras que en Ethernet había dos direcciones MAC (origen y destino), aquí hay tres. Las que corresponden a lo que veríamos en Ethernet son la Receiver address y la Transmitter address. La otra MAC corresponde al otro elemento implicado en la comunicación. Anote estas direcciones MAC y compare con las que ya tiene anotadas de puntos anteriores. ¿Quién emite y recibe físicamente la trama?

32. Observe la trama número 18. ¿Qué tipo de trama es? ¿Quién la envía? ¿Quién la recibe?
33. Observe la trama número 19. Verá que, aparentemente, es la misma trama que la 17. La única diferencia está en las Receiver y Transmitter addresses. Anote las MAC de ambos e indique a quién pertenecen.
34. ¿Por qué se están capturando dos tramas "iguales"? ¿Cuántas de esas tramas procesa el destinatario final?
35. Observe una de las PDUs de datos y busque el campo Tipo/Longitud. ¿En qué cabecera lo ha podido encontrar?
36. Si todo ha ido bien, verá que lo ha encontrado en la cabecera etiquetada como Logical Link Control. Si selecciona dicha cabecera y mira los bytes que ocupa, verá que hay 8 bytes. Realmente, los tres primeros bytes corresponden a la cabecera LLC, mientras que los cinco siguientes corresponden a la cabecera SNAP, que se ocupa de la multiplexión.
37. Cierre Wireshark, desconecte su PC de la Intranet del laboratorio y vuelva a conectarlo a la red de acceso a Internet (red ETSII) en la misma roseta en la que estaba y apague el PC. Vuelva a dejar en su sitio el latiguillo de red.