Arquitectura de Redes.* *Estudio Experimental Práctica 5
Enrutamiento en internet (RIP). Traducción de direcciones (NAT).

Departamento de Tecnología Electrónica

Estudio experimental

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

(NO ENCIENDA EL PC HASTA QUE SE LO INDIQUEN)

Primera parte: Enrutamiento en Internet (RIP)

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. **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 SWITCH_EUROPA (si está en el PC de la izquierda) o al SWITCH_ASIA (si está en el PC de la derecha).
3. **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 SWITCH_SUDAMÉRICA (si está en el PC de la izquierda) o al SWITCH_NORTEAMÉRICA (si está en el PC de la derecha).
4. Abra una ventana de Símbolo del sistema y ejecute en ella el comando **ipconfig /all**
5. Anote su dirección IP.
6. Inicie el programa Wireshark y empiece a capturar tráfico. En el filtro de visualización, escriba **rip**
7. ¿Se dirige el tráfico RIP a su PC? ¿Por qué puede verlo?
8. ¿Cada cuanto tiempo llega un mensaje RIP?
9. ¿Qué versión de RIP se está utilizando?
10. Entre en alguno de los mensajes RIP
    a. ¿Qué redes vemos en cada mensaje?
    b. ¿Con qué métrica?
    c. ¿Qué significa esto?
    d. ¿Cuál es el TTL de un mensaje RIP? (Obsérvelo en la cabecera IP del mensaje)
    e. ¿Qué puertos se usan?
11. 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?
12. A continuación, se produce un cambio en la topología de la red, ya que se enciende el router África, que había permanecido apagado hasta ahora (Espere a que el profesor lo haga).
    a. ¿Hay algún cambio en el tiempo en el que llegan los mensajes RIP?
    b. ¿Qué está ocurriendo?
13. Observe alguno de los últimos mensajes y busque alguno en el que alguna red tiene métrica 16. ¿Qué significa eso?
14. ¿Cuánto se tarda aproximadamente en llegar a una situación estacionaria?
15. ¿Qué redes ve ahora que antes no podía ver?

Segunda parte: Traducción de direcciones (NAT)

16. En esta segunda parte, la práctica ha de ser realizada por parejas: el alumno que se encuentre en el PC de la izquierda (de los dos que constituyen la pareja), tendrá una dirección IP privada, mientras que el alumno que se encuentre en el PC de la derecha tendrá una dirección IP pública. Es importante que, durante esta segunda parte de la práctica, observe y guarde tanto las capturas de Wireshark que obtenga, como las que obtenga su compañero.
17. Vaya al Centro de Redes y Recursos Compartidos del Panel de Control.
18. Si está en el **PC de la izquierda**, deje su configuración IP de la siguiente manera:
    a. Dirección IP = 10.1.15.X (X es el número que aparece en el frontal de su PC, junto a la palabra RED – G1.31 – o COM – G1.33 -).
    b. Máscara de red = 255.255.255.0.
    c. Puerta de enlace por defecto (Gateway)= 10.1.15.1.

19. Si está en el **PC de la derecha**, deje su configuración IP de la siguiente manera:
    a. Dirección IP = 100.100.100.Y (Y es el número que aparece en el frontal de su PC, junto a la palabra RED – G1.31 – o COM – G1.33 -).
    b. Máscara de red = 255.255.255.0.
    c. Puerta de enlace por defecto (Gateway)= 100.100.100.1.
20. Desconecte su PC de la red a la que estaba conectado y conéctelo al SWITCH POLO NORTE (PC de la izquierda), o POLO SUR (PC de la derecha). Podrá ver que ambos switches se encuentran en un bastidor cercano a los routers que forman parte de la intranet del laboratorio. Ambos switches están conectados a un router, cada uno por una interfaz diferente. Los conectados al Switch Polo Norte se encuentran en una red privada, mientras que los conectados al Switch Polo Sur se encuentran en una red pública.
21. Espere unos segundos, y ejecute el comando ipconfig/all, con el fin de comprobar que la configuración de red de su PC es correcta. Compruebe la conectividad de su PC con su puerta de enlace.
22. Inicie una nueva captura de Wireshark y seleccione el filtro de visualización **icmp and not tcp.port==2008**.
23. Compruebe que tiene conectividad con su compañero. ¿Tiene conectividad con su compañero? ¿Y su compañero con usted?
24. Observe las direcciones IP origen y destino que aparecen en su captura y las que aparecen en las de su compañero. ¿Son las mismas? ¿Por qué?
25. A partir de este punto, utilizará el programa nc (netcat). Este programa se basa en un modelo cliente/servidor, en el que, una vez establecida una conexión TCP entre ambos extremos, podrán intercambiarse mensajes de texto entre los hosts. En esta práctica, el PC de la izquierda hará las veces de cliente, mientras que el PC de la derecha hará las veces de servidor. Las conexiones terminan con Ctrl + C de cualquiera de las dos partes. **Muy importante: No olvide que, cada vez que termine una conexión, deberá volver a poner a la escucha el servidor.**
26. Inicie una nueva captura de Wireshark y seleccione el filtro de visualización **tcp and not tcp.port==2008**.
27. Abra una ventana de símbolo de sistema.
28. Si está en el PC de la derecha, ejecute nc –l –p 3000. De esta manera se pondrá a la escucha (-l = listen) en el puerto (-p) 3000.
29. Si está en el PC de la izquierda, espere a que su compañero, ponga en marcha el servidor. Una vez en marcha, ejecute el comando nc 100.100.100.Y 3000 (es decir, conéctese al puerto 3000 de la dirección IP de su compañero).
30. Intercambie impresiones con su compañero (un par de frases o tres) y pulse Ctrl + C, con lo que finalizará la conexión.
31. Seleccione el primer segmento TCP en el PC de la izquierda. ¿Cúal es el número de secuencia empleado? ¿Qué campo de la cabecera indica que se solicita una conexión a la estación 100.100.100.Y? ¿Por qué tiene un valor 0 el campo ACK? ¿Transporta datos de TCP este segmento?
32. Seleccione el primer segmento TCP capturado en por el PC de la izquierda (inside network). Anote los valores de los campos número de secuencia, ack, puerto origen, y puerto destino. ¿Cuáles son las direcciones IP origen y destino de dicho segmento? ¿A qué hosts corresponden dichas IP?
33. Seleccione el primer segmento TCP capturado en el PC de la derecha (outside network). Anote los valores de los campos número de secuencia, ack, puerto origen, puerto destino, dirección IP origen y dirección IP destino. ¿Qué diferencias hay con los valores anotados en el punto anterior? ¿Quién ha modificado los campos cambiados?
34. ¿Qué datos se han almacenado en el router NAT para que todo funcione correctamente? Indique cómo es la tabla NAT (suponiendo que se ha usado NAPT)
35. Observe el cierre de la conexión. ¿Qué flags están activados? ¿Por qué?
36. A continuación, se comprobará cómo actúa un router NAT en el caso de que existan conflictos con un puerto origen. Para ello, si se encuentra en el PC de la izquierda, en esta parte deberá contar con la ayuda de algún otro compañero que se encuentre en su red (es decir, valen todos los que estén delante o detrás de usted). Se usará como puerto destino el puerto 3000 de su compañero. Como puerto origen se empleará en todos los casos el puerto 17000.
37. Reinicien las capturas en ambos PCs (izquierda y derecha).
38. Si está en el PC de la izquierda, ejecute el comando nc 100.100.100.Y 3000 -p 17000 (Si está en el PC de la derecha, recuerde que debe haber vuelto a poner en marcha el servidor). NO CIERRE LA CONEXIÓN.
39. El compañero de la red privada al cual hemos solicitado ayuda debe ejecutar exactamente el mismo comando del punto 38.
40. La segunda conexión será rechazada, pero eso es debido a una limitación del programa nc que se ejecuta en la estación 100.100.100.Y y, en ningún caso tiene que ver con el uso del protocolo NAT. El objetivo de esta parte de la práctica es observar cómo se realiza la traducción de los puertos en caso de conflicto y eso es independiente del hecho de que se rechace la segunda conexión.
41. Paren las capturas de Wireshark.
42. Observe los segmentos de inicio de conexión relacionados con los intentos de conexión realizadas por usted y su ayudante en el PC que se encuentra en la outside network (PC de la derecha). ¿Qué valor poseen los campos

puerto fuente y destino? ¿Qué cambios se han realizado en cada caso? ¿Quién ha realizado dichos cambios? ¿Qué información debe almacenar el router NAT para que todo funcione correctamente?

Tercera parte: Finalización de prácticas

43. Si le ha dado tiempo a terminar esta práctica, y no terminó alguna de las prácticas anteriores, este es el momento de hacerlo. Manos a la obra.
44. 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.