



Estudio experimental

El estudio experimental de esta práctica consta de 3 partes, en cada una de ellas se describen todos los pasos que el alumno debe realizar, **si tiene cualquier duda consulte con el profesor/la encargado de la sesión práctica**. Como ya sabe, puede ir grabando las capturas realizadas en Wireshark  y llevárselas para futuras consultas o para completar en casa los puntos que no le haya dado tiempo.


(NO ENCIENDA EL PC HASTA QUE SE LO INDIQUEN)

Pasos previos

1. Asegúrese de que está conectado a la red de la ETSII.
2. Encienda su PC, restaure (**si así se lo indica el profesor**) y arranque Windows 7.
3. Desactive el firewall.
4. Haga "clic" en el icono de "Conexión de red" , luego pulse sobre "Abrir Centro de redes y recursos compartidos" > "Conexión de área local" y seleccione "Propiedades" en el menú contextual. En la ventana que le sale, **desactive** "Cliente para redes Microsoft", **desactive** "Compartir impresoras y archivos para redes Microsoft", **desactive** "Programador de paquetes QoS" y **desactive** "Protocolo de Internet versión 6 (TCP/IPv6)". Pulse "Aceptar" para cerrar la ventana y luego "Cerrar".

Primera Parte: Configuración IPv4

En esta parte se analizará la configuración típica de los ordenadores de los laboratorios de la ETSII que sirve para que estos accedan a Internet.

5. Como ya sabe, existen dos mecanismos para configurar el nivel de red de los sistemas finales que se conectan a Internet. Una manera de ver qué mecanismo se utiliza en los PCs del laboratorio es hacer "clic" en el icono de "Conexión de red" , luego pulsar sobre "Abrir Centro de redes y recursos compartidos" > "Conexión de área local" y seleccionar "Propiedades" para abrir la ventana "Propiedades de Conexión de área local". En esa ventana verá un área llamada "Esta conexión utiliza los siguientes elementos" en la que debe seleccionar, al final de la lista, el "Protocolo Internet versión 4 (TCP/IPv4)" y luego pulsar el botón "Propiedades", lo cual le abrirá la ventana "Propiedades de Protocolo Internet versión 4 (TCP/IPv4)". Según lo que ve en la ventana: ¿Cómo obtiene su PC la configuración de nivel de red (configuración IPv4)?
¿Cuál sería el otro mecanismo de configuración?
¿En este otro mecanismo, qué parámetro no hay que configurar obligatoriamente para que el PC pueda comunicarse con cualquier equipo de Internet? ¿Por qué?
6. Cierre las ventanas anteriores y ejecute el comando adecuado en una ventana de Símbolo de Sistema para ver la configuración IPv4 que tiene su PC.
7. ¿Cuál es la dirección IP y máscara asignada a su PC?
¿A qué red está conectado su PC? (anótela en notación barra).
8. ¿Pertenece la dirección IP de su PC a uno de los rangos de direcciones privadas vistos en teoría? ¿Es necesario que haga NAT alguno de los routers del camino entre la red de su PC e Internet?
9. ¿Cuál es la dirección IP de la puerta de enlace predeterminada que usa su PC? (Otros nombres usados comúnmente son router por defecto o router frontera.)
¿Pertenece esa IP a la red de su PC? ¿Cómo lo ha comprobado?
10. ¿Está el servidor DHCP ubicado en el dominio de broadcast de su PC? ¿Cómo lo sabe?
11. Según lo visto en teoría ¿cuál es el contenido mínimo de la tabla de enrutamiento (TE) de su PC?

Segunda Parte: Manipular la tabla de enrutamiento del PC en Windows 7 (comando route)

Para manipular la tabla de enrutamiento (TE) de su PC puede utilizar el comando **route**, disponible en la mayoría de los SO Windows. Este comando le permite ver (**print**) el contenido de la TE y añadir (**add**), modificar (**change**) o borrar (**delete**) una entrada de la TE.

Tanto el comando **route** como otros comandos de administración "**requieren elevación**" para realizar algunas de sus operaciones. Por eso, siempre que ejecutemos ese comando lo haremos dentro de una ventana de Símbolo del sistema abierta en modo administrador.

12. Abra ahora una ventana de Símbolo del sistema en modo administrador. Para ello, en lugar de hacer clic en el icono "Símbolo del sistema" con el botón izquierdo del ratón, debe hacer clic en él con el botón derecho y elegir "Ejecutar como administrador".
 13. Ejecute el comando **route print -4** para ver el contenido de la TE de su PC para la versión 4 del protocolo IP y estudie lo que ve. Observará que la TE que ve en pantalla no coincide con la que anotó en el punto 11. Podrá ver que en lugar de la columna "Próximo salto" hay una completamente equivalente que se llama "Puerta de enlace". Las columnas "Destino de red" y "Máscara de red" equivalen a la columna "Red" que hemos visto en teoría. Otro aspecto nuevo es la aparición de la columna "Métrica", que sirve para que, en el caso de que en la TE haya más de una entrada para una misma red, se use la que tenga menor métrica.
 14. Las dos primeras entradas que está viendo de la TE de su PC deben coincidir con las que anotó en el punto 11, aunque con algunos cambios. Recuerde los datos del apartado 7 y responda:
¿Qué se hace para identificar la interfaz en la TE de su PC?
¿Qué se hace para identificar al próximo salto, en la TE de su PC, cuando la red destino está directamente conectada?
 15. Además de las interfaces de red físicas, el protocolo IP usa una interfaz de red virtual, conocida como interfaz de loopback, que se asocia a la red 127.0.0.0/8 (véalo en quinta entrada de la TE) y que se identifica con la dirección IP 127.0.0.1, equivalente al nombre localhost en los PC. La interfaz de loopback sirve para que todo lo que se envíe a ella sea recibido por esa misma interfaz.
¿Cuántas entradas de la TE están asociadas a la interfaz de loopback? ¿Cuántas entradas de la TE están asociadas a una interfaz de red física?
- Tenga presente lo que respondió en el punto 7 a la hora de responder a las siguientes preguntas.
16. Observe la tercera entrada de la TE de su PC y responda:
¿Cuántos bits de ancho tiene el prefijo de red (la parte que identifica a la red) de esa entrada?
¿Cuántas direcciones IP forman parte de la red que aparece en esa tercera entrada? **Anótelas.**
¿Reconoce alguna de esas IPs? ¿Qué interfaz de red está asociada a esta tercera entrada de la TE?
 17. En la entrada cuarta de la TE aparece identificada una red con una única IP.
¿Qué nombre recibe esa IP? ¿A qué red pertenece?
 18. En las entradas 8 y 9 de la TE aparece identificado un bloque CIDR que debería conocer pues se ha visto en el estudio teórico. ¿Qué direcciones IP son?
 19. En las entradas 10 y 11 aparece una red que en realidad es una única IP. ¿Qué nombre recibe esa IP?
 20. Suponga que el nivel de red de su PC tiene que enviar una IP_PDU con dirección IP destino 10.1.15.0.
¿Cuántas entradas de la TE se consultarán en total?
¿Qué dirección IP tendrá el primer nivel de red que recibirá esa IP_PDU?
 21. Suponga que el nivel de red de su PC tiene que enviar una IP_PDU con dirección IP destino 150.214.141.24. ¿Cuántas entradas de la TE se consultarán en total?
¿Qué dirección IP tendrá el primer nivel de red que reciba esta IP_PDU?
 22. Realice una prueba de conectividad con el sistema final 8.8.8.8. ¿Ha sido exitosa?
Si la prueba no tiene éxito consulte con su profesor/a. ¿Qué entrada de la TE habrá utilizado finalmente el nivel de red de su PC para enviar la IP_PDU al 8.8.8.8?
 23. En la ventana Símbolo del sistema ejecute el comando **route delete 0.0.0.0** para borrar la ruta por defecto.
 24. ¿Qué comando puede usar para ver que efectivamente ha desaparecido esa entrada de la TE?
 25. Realice de nuevo una prueba de conectividad con el sistema final 8.8.8.8. ¿Ha sido exitosa?
¿Ahora, cuántas entradas de la TE ha consultado en total el nivel de red de su PC?

Tercera Parte: Análisis de diferentes PDUs. Encapsulación.

26. Desconecte su PC de la red ETSII y conéctelo a LAB_DTE, concretamente al **SWITCH EUROPA** (en G1.31) o al **SWITCH SUDAMERICA** (en G1.33). **Si no hubiera puertos disponibles en el SWITCH adecuado indíquesele al profesor para que le diga lo que hacer.** Compruebe que tiene conectividad de nivel físico.
27. Compruebe que ahora la dirección IP de su PC empieza por 193. **Anote** su configuración IPv4 (dirección IP, máscara, puerta de enlace predeterminada) y también la dirección IP del servidor DNS. Compruebe que tiene conectividad a nivel de red con su router frontera.
28. Compruebe que tiene conectividad a nivel de red con el servidor web **www.redes.lab** y **anote** su IP.
29. Con la finalidad de configurar el comportamiento del navegador Mozilla Firefox para adaptarlo a la Intranet del laboratorio, al igual que en las prácticas tres y cuatro, realice los siguientes pasos: abra Mozilla Firefox 🦊, entre en el URL especial about:config, acepte el "aviso para manazas", busque la frase "retry-timeout", modifique con doble clic el valor de la preferencia "network.http.connection-retry-timeout" para que valga 12000 y cierre Mozilla Firefox 🦊.
30. Entre en Wireshark 🐼 y asegúrese de que las opciones "Resolve network (IP) addresses" y "Resolve transport names" están desactivadas.
31. Abra de nuevo el navegador y antes de comenzar la captura con Wireshark borre la caché DNS del PC y la caché de páginas del navegador.
32. Con Mozilla Firefox acceda a <http://www.redes.lab/lab3/muybreve.html>. A continuación, aplicando un filtro adecuado (puede partir del filtro utilizado en la práctica anterior y adaptarlo a la nueva solicitud) grabe en un fichero llamado "trecetramas" una captura "limpia" conteniendo única y exclusivamente las 13 tramas con las 13 T_PDUs generadas como consecuencia de una descarga normal de dicha página (respuesta HTTP 200 OK) en la cual no deben aparecer retransmisiones.
33. Cargue el fichero "trecetramas" en Wireshark y borre con "Clear" cualquier filtro de visualización. Deberá estar viendo ahora sólo 13 tramas en el listado y los contadores "Packets" y "Displayed" valdrán 13.
34. Aplique el filtro de visualización *ip*. Verá que a pesar del filtro siguen mostrándose trece tramas, porque dentro de cada una de las trece tramas hay encapsulada una IP_PDU.
35. En el listado de tramas, haga clic en la petición DNS que ha enviado el cliente al servidor DNS (trama número uno) y consultando la información de control de UDP (UDP_PCI) conteste: ¿Cuánto mide el segmento UDP (UDP_PDU) que encapsula el mensaje DNS (DNS_PDU) enviado por el cliente?

36. Haga clic en la respuesta DNS enviada por el servidor DNS (trama número 2) y consultando la UDP_PCI: ¿Que tamaño tiene la UDP_PDU enviada por el servidor?

37. ¿Qué tamaño tiene siempre la UDP_PCI? ¿Qué tamaño tienen las DNS_PDUs?

38. A partir de la información de control de IP (IP_PCI) de las tramas uno y dos: ¿Cuánto miden los datagramas IP (IP_PDUs) que encapsulan esas UDP_PDUs? ¿Qué campo ha consultado para averiguarlo? ¿Cuánto mide la IP_PCI? ¿Qué campo ha consultado para averiguarlo?

39. Comprobando la IP_PCI de las tramas uno y dos responda: ¿Qué valor tiene el campo protocolo cuando una IP_PDU encapsula una UDP_PDU?

40. Use Wireshark para responder: ¿Qué IP_PDUs, de las 13 que hay, tienen una IP_PCI con opciones?

41. ¿En qué IP_PDUs, de las 13 que hay, se encuentra encapsulada una TCP_PDU con una TCP_PCI con opciones? ¿Cuántos bytes ocupan las opciones de la TCP_PCI en los casos que ha podido encontrar?

42. En el listado de tramas, haga clic en la petición HTTP que ha realizado el cliente al servidor web (trama número 6) y conteste a las siguientes preguntas usando Wireshark:
¿Cuánto mide la IP_PDU número 6?

¿Cuánto mide la IP_PCI de la IP_PDU número 6?

¿Qué campo de la IP_PCI debe consultar para saber si una IP_PDU encapsula a una TCP_PDU?
¿Qué vale ese campo en la IP_PDU número 6?

¿Qué dos campos de la IP_PCI hay que consultar y qué operación hay que hacer con ellos para calcular el tamaño de la TCP_PDU contenida en una IP_PDU?
¿Qué mide la TCP_PDU contenida en la IP_PDU número 6?

¿Qué campo de la TCP_PCI debe consultar para saber lo que mide la TCP_PCI?
¿Qué mide la TCP_PCI de la TCP_PDU contenida en la IP_PDU número 6?

¿Qué tamaño tiene la HTTP_PDU? ¿Qué operación ha realizado para calcular ese tamaño?

¿Qué campo de la IP_PCI hay que consultar para conocer el destino de una IP_PDU?
¿Cuál es la IP destino de la IP_PDU número 6?

¿Qué campo de la IP_PCI hay que consultar para conocer el origen de una IP_PDU?
¿Cuál es la IP origen de la IP_PDU número 6?

43. En el listado de tramas, haga clic en la respuesta HTTP enviada por el servidor web (trama número 8) y conteste: ¿Cuánto mide la IP_PDU enviada por el servidor? ¿y la TCP_PDU? ¿Cuánto mide la HTTP_PDU? ¿y el objeto (fichero HTML)?

44. Consulte la IP_PCI de las IP_PDUs enviadas por su PC y determine: ¿Qué valor tiene el campo "Time to live" (tiempo de vida) en las IP_PDUs enviadas por el cliente? ¿Cuántos saltos como máximo podrá dar esta IP_PDU para alcanzar al destino? ¿Cuántos routers, como máximo, podrán atravesar esas IP_PDUs antes de llegar a su destino?

45. Avise al profesor/a por si le quisiera hacer alguna pregunta sobre la realización de la práctica.

46. Vuelva a dejar el PC como se lo encontró, es decir, apagado y conectado a la red ETSII.

47. Devuelva a su sitio el latiguillo que ha usado para conectarse a la red LAB_DTE.