Departamento de
Tecnología Electrónica
Última actualización: 1/03/2022

Estudio experimental

El estudio experimental de esta práctica consta de dos partes: DNS y HTTP. 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**. En el caso de no completar todas la partes del estudio experimental, antes de abandonar el laboratorio debe realizar el punto 48.

(NO ENCIENDA EL PC HASTA QUE SE LO INDIQUEN)

Pasos previos

1. Asegúrese de que está conectado a la red ETSII.
2. Encienda su PC, restaure (**si así se lo indica el profesor**) y arranque Windows 7. Desactive el firewall tal y como hizo en los pasos 1 al 4 de la primera sesión de laboratorio.
3. Desconecte su PC de la red ETSII y conéctelo a la Intranet del laboratorio, concretamente al **SWITCH_EUROPA** (en G1.31) o al **SWITCH_SUDAMERICA** (en G1.33), de forma similar a como lo hizo en los pasos 40 al 44 de la primera práctica, sólo que ahora se conecta a un SWITCH y no a un HUB. **Si no hubiese puertos libres en el SWITCH adecuado indíqueselo al profesor.**
4. ¿Cómo puede estar seguro de que tiene conectividad a nivel físico entre su PC y el SWITCH?

5. En la intranet del laboratorio, LAB_DTE, los PC conectados a ella requieren de una configuración TCP/IP específica que se obtiene automáticamente de un servidor DHCP. Realice los pasos oportunos para obtener de forma automática la nueva configuración TCP/IP de su PC como hizo en el apartado 46 de la primera práctica. Anote la dirección IP de su PC.
6. Use un comando que le permita comprobar que tiene conectividad a nivel de red (intercambio de R_PDUs) con su router frontera (puerta de enlace predeterminada). Este tipo de comprobaciones aprendió a hacerlas en la primera práctica. No siga adelante hasta que tenga conectividad.

Primera parte: Domain Name System (DNS)

Los sistemas operativos Windows mantienen una caché de DNS donde se van guardando durante un cierto tiempo las resoluciones DNS que se han hecho anteriormente, con idea de no tener que pedirle al servidor DNS que nos resuelva peticiones que le hemos hecho poco tiempo antes.

7. Abra la consola de comandos (es decir, una ventana de "Símbolo del sistema"), y realice una prueba de conectividad (ping) al dispositivo cuyo nombre es *webserver.af.lab.*
8. En el símbolo del sistema ejecute el comando **ipconfig /displaydns** para mostrar todas las entradas que hay en la cache DNS.
9. Averigüe, mirando en la caché, la dirección IP del servidor web *webserver.af.lab*.
10. Borre la caché DNS ejecutando **ipconfig /flushdns** y compruebe con **ipconfig /displaydns** que efectivamente se ha borrado.
11. Haga que Wireshark comience a capturar tráfico.
12. Si el navegador Mozilla Firefox estaba abierto, ciérrelo. Esto es muy importante porque el navegador también guarda una caché propia con las peticiones DNS más recientes, independiente de la caché DNS del Sistema Operativo Windows y podría tener resuelto el nombre que queremos consultar.
13. Abra el navegador Mozilla Firefox y visite la página web http://www.redes.lab/index.html.
14. Detenga la captura de tráfico cuando observe que la carga de la página anterior ha terminado.
15. Con la ayuda de los filtros de visualización debe aislar el tráfico de red del protocolo DNS asociado a la carga de la página. Es decir, el tráfico DNS en el que se observe la pregunta ("query") sobre el nombre www.redes.lab y también la respuesta a la pregunta ("query response"). Use primero un filtro simple como "dns" y fíjese en cuántas tramas le aparecen. Es muy probable que el filtro le muestre más de cuatro tramas con tráfico DNS, así qué será mejor que use un filtro más selectivo que le muestre sólo el tráfico DNS asociado a la carga de la página.
16. Introduzca y aplique el filtro "dns contains redes" y verá como ya sólo le aparecen cuatro tramas con tráfico DNS. Se trata de dos preguntas y sus correspondientes respuestas. La pregunta que nos interesa es aquella que tiene en el campo "Info" un texto muy similar a **"Standard query 0xabcd A www.redes.-**

lab". Note que el número **0xabcd** será otro distinto, pero que detrás de él tiene que aparecer una **"A"** (no nos vale la trama en la que aparezca **"AAAA"**). Haga "clic" con el botón derecho del ratón sobre la trama con la pregunta con la "A" y ejecute la herramienta "Follow UDP Stream". Cierre la ventana "Follow UDP Stream" que se le ha abierto. Sólo debería aparecer ahora en el listado la pregunta DNS que nos interesa junto con su respuesta. El motivo es que se está ejecutando un filtro de visualización que aprovecha el hecho de que una pregunta y su respuesta están identificadas por una pareja de direcciones IP y una pareja de puertos UDP. Otro detalle en el que puede fijarse ahora es que el código numérico similar a **0xabcd** que aparece en la pregunta DNS es el mismo código que aparece en la respuesta DNS asociada.

17. Observe que es posible, analizando el tráfico DNS, averiguar la IP del servidor web www.redes.lab. ¿Dónde puede ver, exactamente, esa información?

18. ¿Coincide la IP del apartado anterior con la que anotó en el apartado 9? Nota: Tenga en cuenta que www.redes.lab es un alias de webserver.af.lab, como se explicó en la práctica anterior.

19. Explique qué procedimiento puede seguir para determinar el valor del RTT entre su PC y el servidor DNS y anote el valor de dicho RTT.

20. Explique cómo puede averiguar, usando Wireshark, el protocolo de transporte que usan los clientes y servidores DNS. Avise al profesor para que compruebe sus respuestas.

Segunda parte: HyperText Transfer Protocol (HTTP)

21. La intranet del laboratorio tiene unos enlaces entre routers con un ancho de banda bastante bajo, comparados con los que existen hoy día en Internet. Esto provoca que incluso con poco tráfico de red se produzca congestión en los routers del laboratorio, afectando bastante a los retardos apreciados por los usuarios y las aplicaciones. Concretamente, mientras que en Internet es habitual que un servidor web responda a un intento de conexión por parte de un cliente en un tiempo muy inferior a 250ms, es relativamente normal en el laboratorio que estos tiempos superen los 250ms. Por tanto es conveniente configurar el navegador Mozilla Firefox para que sepa que esos retardos mayores de 250ms son normales y que no debe solicitar una nueva conexión con el servidor web cuando hayan pasado 250ms sin obtener respuesta, sino que debe esperar mucho más, por ejemplo 12000ms (unos 12 segundos).

22. En Mozilla Firefox escriba "about:config" en la barra de direcciones, acepte el "aviso para manazas" y verá una ventana de configuración avanzada. Use como filtro de búsqueda (debajo de la barra de direcciones) la frase "retry-timeout" y haga doble "clic" sobre el resultado de la búsqueda llamado "network.http.connection-retry-timeout". Quite el valor actual, que será de 250, y ponga 12000.

23. Inicie una nueva captura con Wireshark.

24. Cargue la página web **http://www.redes.lab/lab2/tarta.html** en el navegador Mozilla Firefox.

25. Detenga la captura de Wireshark unos segundos después de que termine de cargar la página.

26. En el navegador Mozilla Firefox visualice el código fuente del fichero base HTML. ¿Cuántos objetos referenciados tiene la página HTML? Anote el número. Teniendo en cuenta esto, ¿cuántas peticiones GET debe enviar el navegador?

Averigüe todo lo que se le pregunta a continuación, con ayuda de Wireshark:

27. Localice la trama que encapsula la PDU de petición de la página base. ¿Qué versión de HTTP usa el navegador? ¿En qué idioma(s) ha solicitado ver el contenido del servidor web?

28. Localice la trama que encapsula la PDU de respuesta de la página base (es la primera respuesta que le aparece en el listado de tramas). ¿Qué código de estado ha devuelto el servidor web en la página principal?. Compruebe que la HTTP_PDU de respuesta tiene "cuerpo". Si no tiene "cuerpo" es porque no ha

hecho la captura correctamente "a la primera", por lo que debe avisar a su profesor para que le explique cómo repetir la captura borrando antes la caché de páginas del navegador.

29. ¿Cuántos bytes ocupa el fichero HTML principal (página base)?

30. ¿Se ha establecido una conexión persistente con el servidor?, en caso afirmativo, usando la herramienta "Follow TCP Stream" determine cuántos objetos se han solicitado en esta conexión TCP con el servidor. ¿Se han solicitado todos los objetos de la página base en esta conexión? (anotó el número en el apartado 26), en caso negativo, ¿Cómo habrá solicitado el navegador los objetos que le faltan?. Avise al profesor para que compruebe sus respuestas.

31. Para ver las distintas conexiones establecidas entre el navegador y el servidor web puede aplicar un filtro de visualización que muestre sólo las PDU del protocolo HTTP (“http”) y ordenar luego el listado de tramas por la columna SrcPort. ¿Cuántas conexiones distintas ha establecido el cliente? Anótelo ¿Cómo puede identificar cada conexión y diferenciarla de las demás? Avise al profesor para que compruebe sus respuestas.

32. Siga usando el filtro "http" y ordene el listado de tramas por la columna "No." (número de trama, la ordenación normal) para ver las tramas en orden "cronológico", tal y como se han ido capturando.

33. Para cada conexión TCP, determine qué objetos se han solicitado por la misma y el orden en que se han pedido. Haga un diagrama temporal en el que se vea toda esa información.

34. Dentro de cada conexión fíjese en que no se realiza un nuevo GET hasta que ha llegado la respuesta al GET anterior. Observe, sin embargo, que mientras en una determinada conexión un GET aún no ha obtenido respuesta, eso no impide que se envíe un nuevo GET por una conexión diferente. Eso quiere decir que esas dos conexiones están funcionando "en paralelo". Fíjese bien, empezando por el principio de la captura, en los GET que se están realizando por las diferentes conexiones y diga en qué instante encuentra un mayor número de conexiones funcionando en paralelo, es decir, el instante de tiempo en el que hay más peticiones GET pendientes de ser respondidas. Anote el número máximo de conexiones funcionando "en paralelo" que ha podido encontrar y el instante en que se ha producido esa circunstancia.

35. ¿Cuánto tiempo total ha tardado en cargarse la página completa (incluyendo todos los objetos pero excluyendo la resolución DNS)? Anote el valor.

36. Inicie la captura en Wireshark. Ordene a Firefox que haga una recarga de la página actual haciendo clic sobre icono de recarga (la flecha gris enroscada que está a la derecha de la URL de la página). Espere unos segundos hasta que esté seguro de que ha acabado la recarga y detenga la captura.

37. Observe las tramas que encapsulan PDUs del protocolo HTTP y compruebe si los mensajes de respuesta del servidor tienen cuerpo.

38. ¿Qué ha cambiado en los mensajes de solicitud GET para que ahora las respuestas no tengan cuerpo?

39. ¿Cuál es el tiempo total que ha tardado en cargarse la página completa en esta ocasión? Anótelo. ¿Es un tiempo mayor o menor que el anotado en el apartado 35? ¿Por qué?

40. En Mozilla Firefox puede borrar la caché pulsando simultáneamente CTRL+Mayúsculas+Suprimir y luego haciendo clic en el botón "Limpiar ahora". Inicie una captura con Wireshark. Borre la caché de Mozilla Firefox y ordene una recarga de la página. Detenga la captura y compruebe, usando Wireshark, que la recarga después de haber borrado la caché es diferente a la recarga que hizo anteriormente. ¿Tienen cuerpo ahora los mensajes de respuesta HTTP?

41. En Mozilla Firefox se puede cambiar el número de conexiones persistentes en paralelo. Para ello, escriba "about:config" en la barra de direcciones, acepte el "aviso para manazas" y verá una ventana de configuración avanzada. Use como filtro de búsqueda (debajo de la barra de direcciones) la palabra "persistent". Fíjese en la preferencia llamada "network.http.max-persistent-connections-per-server" y anote el valor actual. ¿Coincide ese valor con el anotado en el punto 34?

42. Cambie el valor actual de la preferencia "network.http.max-persistent-connections-per-server" haciendo doble clic en ella e introduciendo como nuevo valor el 1.

43. Ponga en marcha una nueva captura con Wireshark.

44. Borre la caché de Firefox y recargue de nuevo la misma página **http://www.redes.lab/lab2/tarta.html**

45. ¿Cuántas conexiones se han creado con el servidor web? ¿Cuántos objetos se han solicitado en cada una de ellas? ¿Cómo se identifica cada una de las conexiones?

46. ¿Cuánto tiempo ha tardado ahora la carga de la página completa? Compare el resultado con el que anotó en el punto 35 ¿Por qué son distintos?

47. Restaure el valor de las preferencias modificadas usando la ventana "about:config" (apartados 22 y 42), haciendo clic con el botón derecho en cada preferencia y seleccionando "Restablecer".

48. Cierre todas las ventanas abiertas en su PC.
Desconecte su PC de la intranet del laboratorio.
Conecte su PC a la red ETSII.
Apague el PC.
Vuelva a dejar en su sitio el latiguillo que conectó al SWITCH EUROPA o al SWITCH_SUDAMÉRICA.