

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/a 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. Desconecte su PC de la red ETSII y conéctelo a LAB_DTE, concretamente al SWITCH_ASIA (en G1.31) o al SWITCH_SUDAMERICA (en G1.33). **Si no hubiera puertos disponibles en el SWITCH adecuado indíquese al profesor para que le diga lo que hacer**. Compruebe que tiene conectividad de nivel físico.
5. Compruebe que la dirección IP de su PC empieza por 193, anótela, y compruebe que tiene conectividad a nivel de red con su router frontera (con un ping).
6. No siga adelante hasta que tenga conectividad.
7. 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: Comando ping avanzado

Como ya sabe de otras prácticas, el comando **ping** sirve para probar que dos equipos tienen conectividad a nivel de red. En clases de teoría ha visto que el programa **ping** usa internamente el protocolo ICMP, protocolo que utiliza los servicios de la capa IP. El proceso utilizado se conoce como **solicitud/respuesta de eco**. El único parámetro obligatorio que hay que pasarle al comando **ping** es la dirección IP del equipo destino o bien el nombre del mismo.

En la ventana de **Símbolo del sistema** ejecute el comando **ping** sin parámetros para mostrar todas las opciones que tiene. Muchas opciones van a ser IP_ICI que el protocolo ICMP le pasará al protocolo IP cuando desee enviar una ICMP_PDU, para así controlar algunos campos de la IP_PDU de la ICMP_PDU que encapsulará a dicha ICMP_PDU.

8. Observe en la ventana de Símbolo del sistema la salida del comando ping sin parámetros y determine:
¿Qué opción permite controlar el número de pruebas de conectividad que se hacen?

¿Qué opción permite limitar el número de saltos que puede dar la IP_PDU que encapsule la ICMP_PDU?

¿Qué opción permite controlar el número de bytes de ICMP_UD de la ICMP_PDU?

¿Qué opción prohíbe que se fragmente la IP_PDU que encapsula a la ICMP_PDU en el camino que le lleva hacia su destino?
9. Ponga a Wireshark a capturar tráfico e introduzca y aplique el filtro de visualización **ip.addr=="IP_PC" and ip.addr=="IP_Router"** para ver sólo las tramas que hagan cierta esa expresión lógica (contienen IP_PDUs cuya dirección IP origen o destino sea la de su PC y cuya dirección IP origen o destino sea la de su **router frontera**). Debe sustituir "**IP_PC**" e "**IP_Router**", respectivamente, por la dirección IP de su PC y por la IP de su puerta de enlace predeterminada, que anotó en el apartado 5.
10. En la ventana de Símbolo del sistema ejecute el comando ping de tal forma que sólo se realice una prueba de conectividad con su router frontera y que el valor del campo TTL de la IP_PDU de la ICMP_PDU sea 1. **Anote** el comando ping completo que ha usado.

11. Una vez finalizada la prueba detenga la captura en Wireshark. ¿Por qué sólo aparecen dos tramas en el listado de tramas de Wireshark? Con la información de detalle de trama determine qué campo TTL de la IP_PCI se controla con la opción -i, ¿el de la IP_PDU enviada por su PC, el de la recibida por éste o el de ambas?
12. La MTU del dominio de broadcast al que está conectado su PC en el laboratorio es de 1500 bytes. Para determinar el número máximo de bytes de ICMP_UD que puede encapsular una ICMP_PDU de forma que la IP_PDU que la encapsule no sea mayor de 1500 bytes, debe restar a 1500 la longitud de la IP_PCI y la ICMP_PCI. Calcule y **anote** ese tamaño de ICMP_UD que da lugar a una IP_PDU de 1500 bytes.
13. Ponga a Wireshark a capturar tráfico con el mismo filtro de visualización que aplicó en el punto 9. En la ventana de Símbolo del sistema ejecute el comando ping de tal forma que sólo se realice una prueba de conectividad con su router frontera, con 1 byte más de ICMP_UD del calculado en el punto anterior y **que NO se permita fragmentar** la IP_PDU que encapsule a la ICMP_PDU. Una vez finalizado el **ping** detenga la captura en Wireshark. No le debería aparecer ninguna trama en el listado de tramas. En el caso de que le aparezca alguna trama en la captura, repita el punto de nuevo porque está haciendo algo mal. **Anote** aquí el comando ping completo que ha usado.

¿Por qué el nivel de red de su PC no envió la IP_PDU?

¿Qué tamaño tenía la IP_PDU que no se ha podido enviar?

Segunda Parte: NIC 802.3 PCs laboratorio

En esta parte se analizará las características de la tarjeta de red Ethernet usada en los ordenadores de los laboratorios G1.31 y G1.33 y cómo se pueden modificar propiedades de la misma.

14. En general, las tarjetas de red Ethernet vienen preparadas para poder utilizar diferentes protocolos de nivel físico. Una manera de ver qué protocolos de nivel físico permite la tarjeta de red de los PCs del laboratorio es la siguiente: en el área de notificación de la barra de tareas pulse con el botón izquierdo sobre el icono , pulse sobre "Abrir Centro de Redes y Recursos Compartidos" > "Conexión de área local", esa ventana le muestra el estado de la Conexión de área local (observe el nombre de la ventana). Anote la velocidad o ancho de banda **R** del enlace que lo conecta a la red del laboratorio. Pulse el botón "Propiedades", en la ventana que le aparece hay un área llamada "Conectar usando:" en la que aparece el nombre de la tarjeta de red del PC, anótelos y pulse el botón "Configurar" para configurarla. Le aparece la ventana "Propiedades Realtek PCIe GBE Family Controller" en la que puede consultar el tipo de dispositivo, el fabricante y la ubicación de la tarjeta. Seleccione la pestaña "Opciones Avanzadas" y le aparecerán una serie de propiedades que se pueden configurar. La propiedad "**Velocidad/Duplex**" es la que permite seleccionar el protocolo de nivel físico que se desea utilizar. Seleccione esta propiedad y comprobará que el valor por defecto es **Negociación automática**, ya que las interfaces de red tienen la capacidad de determinar el mejor protocolo de nivel físico a utilizar (mayor velocidad en bps, es decir mayor **R**, y full-duplex). Despliegue la lista **Valor** y podrá comprobar todos los protocolos de nivel físico que se permiten así como el tipo de uso del medio físico (half-duplex o full-duplex). No cierre esta ventana, ni cambie el valor de la propiedad "**Velocidad/Duplex**". Como sabe de otras prácticas, el medio físico usado en el laboratorio es par trenzado sin apantallar (UTP). Teniendo en cuenta esto y el ancho de banda **R** anotado antes, tras la autonegociación ¿se está utilizando el protocolo de nivel físico 10BaseT de la norma 802.3 para la conexión de su PC a la red del laboratorio? ¿Por qué? ¿Qué protocolo de nivel físico se está usando?, anótelos.
15. En la ventana "Propiedades Realtek PCIe GBE Family Controller" seleccione la propiedad "**Velocidad/Duplex**", modifique el valor de la misma para que el protocolo de nivel físico sea 10BaseT full-duplex y pulse sobre "Aceptar" para que el cambio tenga efecto. Compruebe en la ventana "Estado de conexión de Red de área Local" que ese es el nuevo protocolo de nivel físico. Puede ser necesario esperar unos segundos hasta que le indique que tiene conectividad de nivel físico y que la velocidad es 10Mbps.
16. Vuelva a dejar la propiedad "**Velocidad/Duplex**", al valor **Negociación Automática** y compruebe que el protocolo de nivel físico coincide con el que anotó en el punto 14.

Tercera Parte: Comando arp. Análisis MAC_PDU y ARP_PDU

El comando **arp** sirve para ver el contenido de la caché arp (tabla de mapeo de direcciones) de un PC.

17. Ejecute el comando **arp** en una ventana de **Símbolo del sistema** en modo administrador y averigüe la opción que permite ver la caché arp, la que permite introducir una entrada estática y la que permite borrar una entrada de la caché arp. Necesitará hacer más grande la ventana de Símbolo del sistema para ver todas las opciones del comando arp.
18. ¿Cuántas entradas tiene la caché arp de su estación? En el caso de que su caché arp no esté vacía borre todas las entradas.
19. Ponga a Wireshark a capturar tráfico, e introduzca y aplique el filtro de visualización (**eth.addr==MAC_de_mi_PC and arp**) or (**ip.addr==IP_de_mi_PC and icmp**) para ver sólo las tramas que hagan cierta esa expresión lógica (tramas con dirección MAC origen o destino la MAC_de_mi_PC y que encapsulan una ARP_PDU o tramas que encapsulan una IP_PDU con IP origen o destino igual a la IP_de_mi_PC y que encapsulan un mensaje ICMP). Realice cuatro pruebas de conectividad con su router por defecto (Nota: comando **ping** sin opciones). En el listado de tramas de Wireshark le deben aparecer 10 tramas. En las dos primeras tramas la columna *Protocol* del listado de tramas indica ARP y en las 8 tramas siguientes esa columna muestra ICMP. Si no es así, detenga la captura y repita a partir del punto 18.
20. Detenga la captura de Wireshark. ¿Aparece una entrada en la caché arp asociada a la IP de su router por defecto? ¿Por qué?
21. **Pulse sobre la primera trama** y en detalles de trama pulse sobre el “+” que aparece al lado de **Ethernet II**¹ para ver algunos campos de la cabecera (MAC_PCI) de la trama (MAC_PDU). Wireshark no muestra la cola de la trama, es decir los 4 bytes de CRC. ¿Qué otro campo de la MAC_PCI no muestra? Teniendo en cuenta lo anterior, ¿es correcto el valor que indica Wireshark como tamaño de la MAC_PCI? ¿Cuál sería su tamaño real? ¿Qué campo de la MAC_PCI consulta Wireshark para indicar que la MAC_UD es del protocolo ARP? ¿Coincide el valor de este campo con el que ha indicado en el apartado 2.c del estudio teórico? ¿Qué equipo ha enviado esta trama? Anote la dirección MAC. ¿A qué equipo o equipos iba dirigida? Anote la dirección MAC.
22. En esa misma trama, en detalle de trama pulse sobre el “+” que aparece al lado de **Address Resolution Protocol** para ver los campos de la ARP_PDU. ¿Qué campo de la ARP_PDU consulta Wireshark para indicar que se trata de un ARP_PDU request? ¿Coincide el valor de este campo con el que ha indicado en el apartado 3.a del estudio teórico? Fíjese en el valor del campo **Target MAC address** de la ARP_PDU mostrado por Wireshark. ¿Por qué cree usted que se usa ese valor? ¿Coincide con el valor que ha indicado en el apartado 3.a del estudio teórico? Avisé al profesor/a para que compruebe sus respuestas.
23. **Pulse sobre la segunda trama** y en detalle de trama pulse sobre el “+” que aparece al lado de **Ethernet II** para ver algunos campos de la cabecera (MAC_PCI) de la trama (MAC_PDU). ¿Qué equipo ha enviado esta trama? Anote la dirección MAC. ¿A qué equipo o equipos iba dirigida? Anote la dirección MAC.
24. En esa misma trama, en detalle de trama pulse sobre el “+” que aparece al lado de **Address Resolution Protocol** para ver los campos de la ARP_PDU. ¿Coincide el valor del campo de la ARP_PDU que consulta Wireshark para indicar que se trata de un ARP_PDU reply con el que ha indicado en el apartado 3.b del estudio teórico? ¿Coincide la dirección MAC origen que anotó en el punto 23 con el valor del campo **Sender MAC address** de la ARP_PDU? ¿Por qué? ¿Coincide la dirección destino que anotó en el punto 23 con el valor del campo **Target MAC address** de la ARP_PDU? ¿Por qué? Avisé al profesor/a para que compruebe sus respuestas.

¹ Nombre con el que se conoce a IEEE 802.3 cuando el campo longitud/tipo de la MAC_PCI significa tipo.

25. **Pulse sobre la tercera trama** y usando la información de detalle de trama indique si son coherentes las direcciones IP origen y destino de la IP_PDU con las direcciones MAC origen y destino de la MAC_PDU que encapsula a la IP_PDU, es decir, si los equipos que tienen configuradas esas direcciones IP tienen en sus interfaces de red esas direcciones MAC. Como puede observar la IP_PDU encapsula una ICMP_PDU de petición de eco.
26. **Pulse sobre la cuarta trama** y usando la información de detalle de trama determine si son coherentes las direcciones IP origen y destino de la IP_PDU con las direcciones MAC origen y destino de la MAC_PDU que encapsula a la IP_PDU, es decir, si los equipos que tienen configuradas esas direcciones IP tienen en sus interfaces de red esas direcciones MAC. Como puede observar la IP_PDU encapsula una ICMP_PDU de respuesta de eco.
27. ¿Por qué sólo aparecen 2 tramas que encapsulan ARP_PDUs en el listado de tramas, si se han hecho cuatro pruebas de conectividad entre su PC y el router por defecto?
28. Ponga a Wireshark a capturar tráfico con el mismo filtro de visualización. Borre la caché arp. Realice varias pruebas de conectividad con el servidor web de nombre *webserver.af.lab* hasta que varias de ellas tengan éxito. En el listado de tramas de Wireshark le deben aparecer como mínimo dos tramas (las dos primeras) con la columna *Protocol* indicando ARP y a continuación varias tramas que en esa columna muestran ICMP. Si no es así, detenga la captura y repita este punto.
29. Detenga la captura. ¿Aparece una entrada en la caché arp asociada al servidor web *webserver.af.lab*? ¿Por qué?
30. **Busque en el listado de tramas una trama en la que el campo INFO indique "...echo (ping) request..." y pulse sobre ella.** Usando la información de detalle de trama determine si son coherentes las direcciones IP origen y destino de la IP_PDU con las direcciones MAC origen y destino de la MAC_PDU que encapsula la IP_PDU, es decir, si los equipos que tienen configuradas esas direcciones IP tienen en sus interfaces de red esas direcciones MAC. En caso de no serlo explique el motivo.
31. Avise al profesor/a por si le quisiera hacer alguna pregunta sobre la realización de la práctica.
32. Vuelva a dejar el PC como se lo encontró, es decir, apagado y conectado a la red de la ETSII.
33. Devuelva a su sitio el latiguillo que ha usado para conectarse a la red LAB_DTE.