Práctica 3: Funcionamiento de Hubs y Switches (CSMA/CD). ARP. Wireshark

1. Objetivo de la práctica:

Dar a conocer ciertos aspectos relativos a la instalación, funcionamiento y análisis de una sencilla red de área local cableada, conociendo los protocolos más habituales que se utilizan en ella. Concretamente, se probará y estudiará el funcionamiento de:

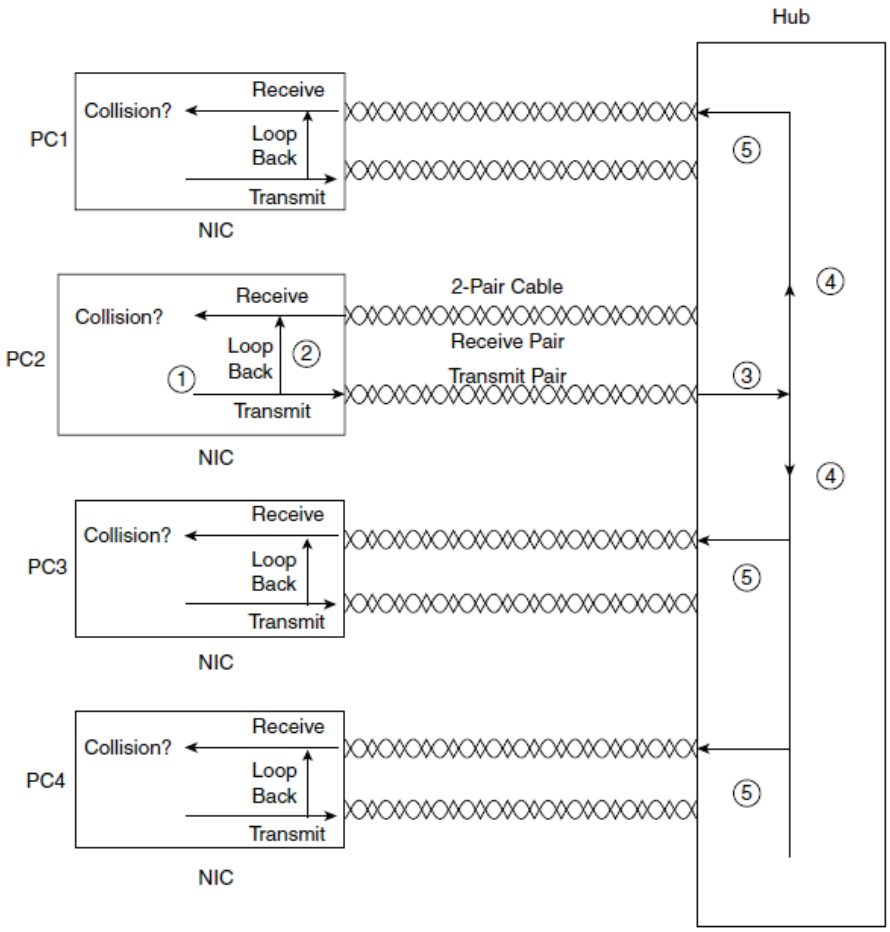
- Funcionamiento de *hubs* y *switches*
- Protocolo ARP
- Análisis de la red mediante el analizador de protocolos Wireshark.
- Telnet

Para realizar esta práctica deberéis dividiros en 5 grupos de 2 o 3 alumnos, colocándose todos los componentes del grupo en la misma mesa.

2. Introducción

2.1. Problemas de rendimiento cuando se utilizan *hubs*

La siguiente figura muestra lo que ocurre cuando un dispositivo envía datos a través de un *hub*.



La figura muestra cómo un *hub* crea un bus eléctrico compartido. Los pasos ilustrados en la figura son los siguientes:

1. La tarjeta de interfaz de red (NIC) envía una trama.
2. La NIC itera la trama enviada hacia su par de recepción internamente en la tarjeta.
3. El *hub* recibe la señal eléctrica, ya la interpreta como bits para poder limpiarla y repetirla.
4. El cableado interno del *hub* repite la señal y la envía a todos los puertos, excepto al puerto por el que se recibió dicha señal.
5. El *hub* repite la señal a todos los pares de recepción de todos los demás dispositivos.

Un *hub* siempre repite la señal eléctrica por todos los puertos, excepto por el que se recibió. Además, la figura anterior no muestra una colisión. Sin embargo, si PC1 y PC2 envían una señal eléctrica al mismo tiempo, en el paso 4 la señal eléctrica se solaparía, las tramas colisionarían y las dos tramas se volverían completamente ininteligibles o repletas de errores. Los hubs implementan un mecanismo denominado CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) que intenta evitar las colisiones y define cómo actuar cuando se produce una colisión.

Sin embargo, presenta problemas de rendimiento. En primer lugar, los dispositivos esperan hasta que Ethernet esté en silencio antes de enviar datos. Este proceso ayuda a evitar colisiones, pero también significa que sólo un dispositivo puede enviar al mismo tiempo. En consecuencia, todos los dispositivos conectados al mismo *hub* comparten la capacidad disponible. El modo de funcionamiento es por tanto *half dúplex*: un dispositivo envía o recibe en un momento dado de tiempo, pero nunca las dos cosas al mismo tiempo.

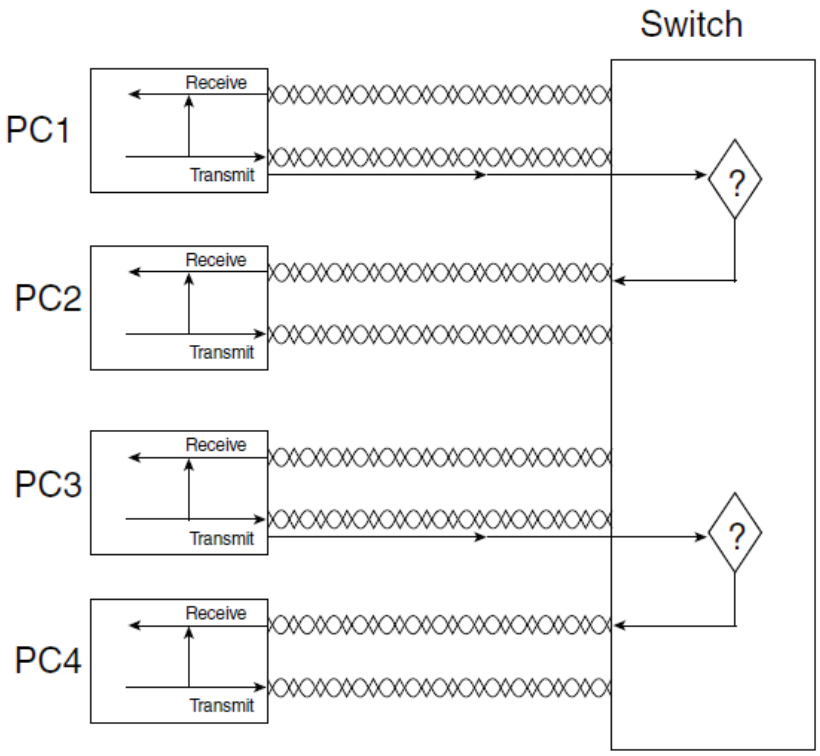
CSMA/CD no evita las colisiones, pero garantiza el correcto funcionamiento de Ehernet incluso cuando estas se producen. Cuando se producen colisiones, los dispositivos que envían las tramas que colisionan esperan un tiempo aleatorio, y después vuelvan a intentarlo. Esto ayuda a que la LAN funcione, pero de nuevo afecta al rendimiento. Durante la colisión ningún dato útil pasa por la LAN. Además, los dispositivos causantes de la colisión tienen que esperar antes de intentar usar la LAN.

2.2. Incremento de la capacidad disponible usando switches

Los *switches* eliminan las colisiones en una LAN. Los switches no crean un único bus compartido, en su lugar hacen lo siguiente:

1. Interpretan los bits de la trama recibida, por lo que normalmente envían la trama por el puerto al que va destinada, y no por todos los demás puertos.
2. Si un switch tiene que enviar varias tramas por el mismo puerto, las almacena en búferes de memoria y las envía de una en una, evitándose así las colisiones.

La siguiente figura ilustra cómo un switch puede enviar dos tramas al mismo tiempo evitando una colisión.



PC1 y PC3 envían al mismo tiempo. En este caso, PC1 envía una trama de datos con la dirección de PC2 como destino, y PC3 envía una trama de datos con la dirección de PC4 como destino. El switch consulta la dirección Ethernet de destino y envía la trama de PC1 a PC2 en el mismo instante que la trama es enviada por PC3 a PC4. Como el switch no envía las tramas a todos los demás puertos, el switch evita una colisión.

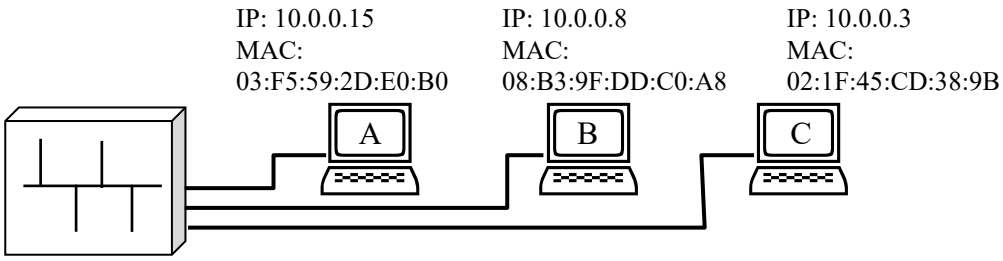
El almacenamiento en búferes también ayuda a evitar las colisiones. Imagine que PC1 y PC3 envían una trama a PC4 al mismo tiempo. El switch, sabiendo que el envío simultáneo de las dos tramas a PC4 provocaría una colisión, almacena en búfer una trama (es decir, la almacena temporalmente en memoria) hasta que la primera se ha enviado completamente a PC4.

Estas características proporcionan una mejora significativa del rendimiento en comparación con el uso de *hubs*:

- Si sólo se cablea un dispositivo a cada puerto de un switch, no habría colisiones.
- Los dispositivos conectados a un puerto del switch no comparten su ancho de banda con los dispositivos conectados a otro puerto del switch. Cada uno tiene su propio ancho de banda separado, de modo que un switch con puertos de 100Mbps tiene 100Mbps de ancho de banda por puerto.

2.3. Protocolo ARP

En una comunicación normalmente se utilizan direcciones IP (nivel de interred, nivel 3 OSI) para identificar a los equipos origen y destino. En nivel 2 (en nuestro caso, Ethernet) es necesario incluir la dirección del destinatario, para que una trama de la red sea aceptada solo por el equipo al que se dirige. Sin embargo, las tramas de nivel 2 no puede utilizar direcciones IP para el direccionamiento: Es independiente del protocolo del nivel 3 que transporte. En su lugar, se utilizan las direcciones *físicas*, o direcciones MAC. De aquí surge un problema: Cuando un equipo A quiere enviar una trama a un equipo B, conocerá su IP (10.0.0.8), pero no la dirección MAC (dirección de nivel de enlace) de B.



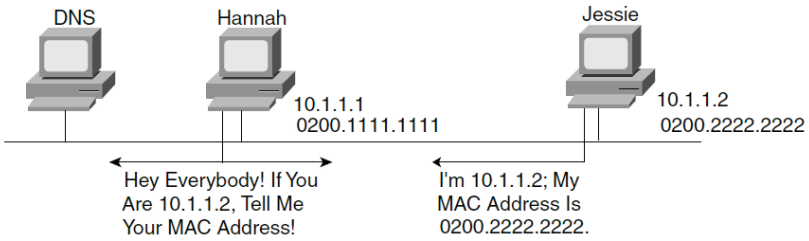
Para resolver este problema, se utiliza el protocolo ARP: *Address Resolution Protocol*. Este protocolo define dos tipos de trama:

1. Solicitud: La envía un equipo, preguntando por la MAC de una IP concreta. En Ethernet es una trama *broadcast,* es decir, que llega a todos los equipos de la red.
2. Respuesta: El equipo que tiene la dirección IP buscada responde al solicitante indicando su dirección MAC. Es una trama *unicast:* se envía a un único destino (el que envió la solicitud original).

Para poder utilizar este protocolo, es necesario que la red permita enviar tramas *broadcast*. En Ethernet, cada trama lleva las direcciones MAC de origen y destino. Para enviar una trama broadcast, se utiliza la dirección de destino reservada FF:FF:FF:FF:FF:FF (todo 1's), que está predefinida como dirección de broadcast, y que es aceptada por todos los equipos de la red. Si la red no soportase broadcast (por ejemplo, en redes ATM no se pueden enviar tramas broadcast) sería necesario un servidor centralizado que proporcionase la traducción de direcciones (denominado servidor ARP).

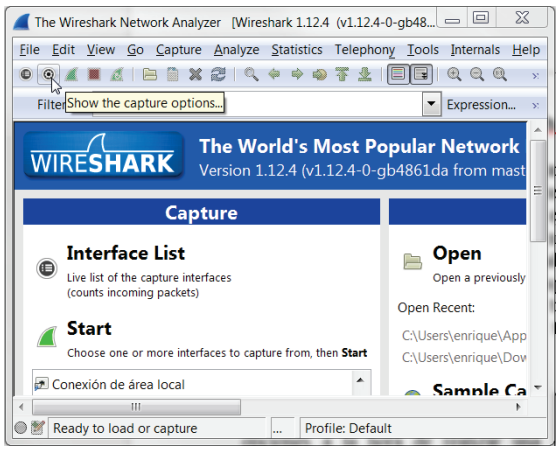
Para evitar tener que hacer uso de solicitudes ARP cada vez que se envía una trama, los equipos guardan en memoria una *tabla ARP*, en la que se guardan las direcciones ya resueltas (el par IP + MAC correspondiente). Se puede acceder al contenido de esta tabla mediante el comando *arp*, como se indica en el apartado 4.4.

La siguiente figura representa todo el proceso:

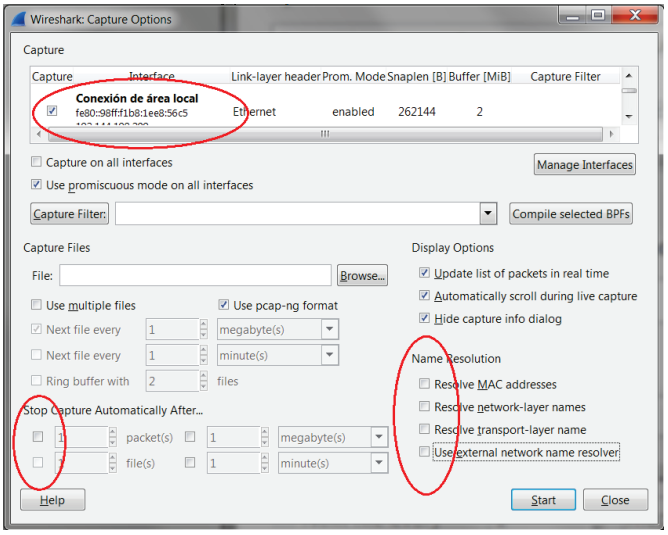


2.4. Introducción al uso de Wireshark

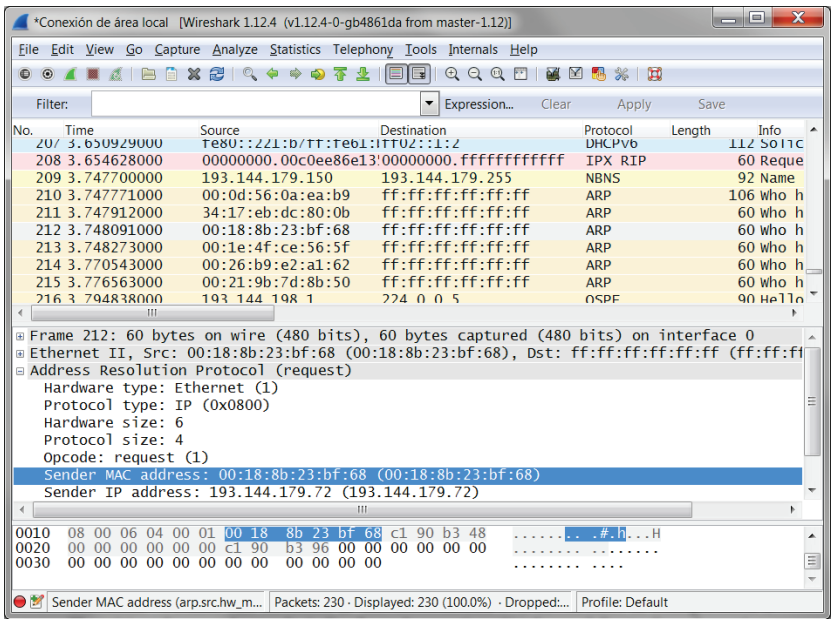
El analizador de protocolos Wireshark permite capturar todo el tráfico que llegue a una interfaz de red, esté o no dirigido al equipo en que se ejecuta. Después de capturar el tráfico, nos muestra todas las tramas, pudiendo analizarlas diseccionando los protocolos que transportan, realizar operaciones de filtrado para trabajar más cómodos, sacar estadísticas del tráfico, etc.



En la barra de herramientas podemos seleccionar, con el segundo botón, las opciones a la hora de realizar una captura. En concreto, tendremos que seleccionar la interfaz de red adecuada (puede que el equipo tenga más de una, o que se muestren interfaces virtuales del sistema operativo). En nuestra practica deshabilitaremos las opciones de resolución de nombres ("*Resolve MAC addresses*" y "*Resolve Transport-layer name*") y, si nos interesa que la captura se restrinja a las primeras tramas, podemos poner un límite de tramas o de cantidad de trafico capturado. Con *Start* comienza la captura.



Cuando finalicemos la captura, la pantalla principal se divide en tres. En la parte superior, se muestra el listado de tramas, pudiendo seleccionar una u otra. Las tramas se colorean automáticamente para simplificar su análisis. En zona central se disecciona la trama seleccionada, por capas: comienza en la parte superior por la capa 1 (Nivel físico) y bajando se muestran las siguientes capas. El analizador descompone cada campo de las cabeceras, mostrándonos su significado y valor. Finalmente, la zona inferior de la pantalla nos muestra los bytes reales que componen el total de la trama.



3. La red del laboratorio

El laboratorio dispone de un rack situado en una de las esquinas, en el que se encuentran varios equipos con los que trabajaremos en esta práctica. Hay que tener en cuenta que en este rack hay un switch "de producción" para el acceso a internet de todos los alumnos de todas las prácticas (no necesariamente de esta asignatura), y varios hubs y switches "de pruebas" para el empleo en esta asignatura de redes.
El laboratorio dispone de cableado estructurado duplicado, de manera que se pueden utilizar dos redes físicamente separadas:
- Las tomas etiquetadas con una "A" son las que se emplean habitualmente en todas las asignaturas. Estas tomas conectan con un panel de parcheo en el rack, que a su vez está conectado el switch "de producción" del rack. Este switch es el que está colocado en la parte superior del rack. En el rack, **NO DEBEMOS CAMBIAR LA CONEXIÓN ENTRE LAS TOMAS DEL PANEL DE PARCHEO "A" Y EL SWITCH SUPERIOR**.
- Las tomas etiquetadas con una "B" son las que emplearemos en esta práctica. Estas tomas conectan con el panel de parcheo colocado a mitad del switch. Desde este panel de parcheo podemos conectar, mediante latiguillos la toma correspondiente a nuestro equipo con el hub o switch que nos interese.

4. Realización de la práctica.

4.1. Conexionado

4.1.1. Familiarízate con los elementos de la red: cables, hubs, switch, tarjetas de red, puertos RJ-45 y conectores RJ-45

4.1.2. Preparad cada PC como elemento de la red utilizando el cableado estructurado del laboratorio:
Desconectaremos el cable de nuestro PC de la toma "A" y lo conectaremos en la "B". Anotar el número de la roseta.

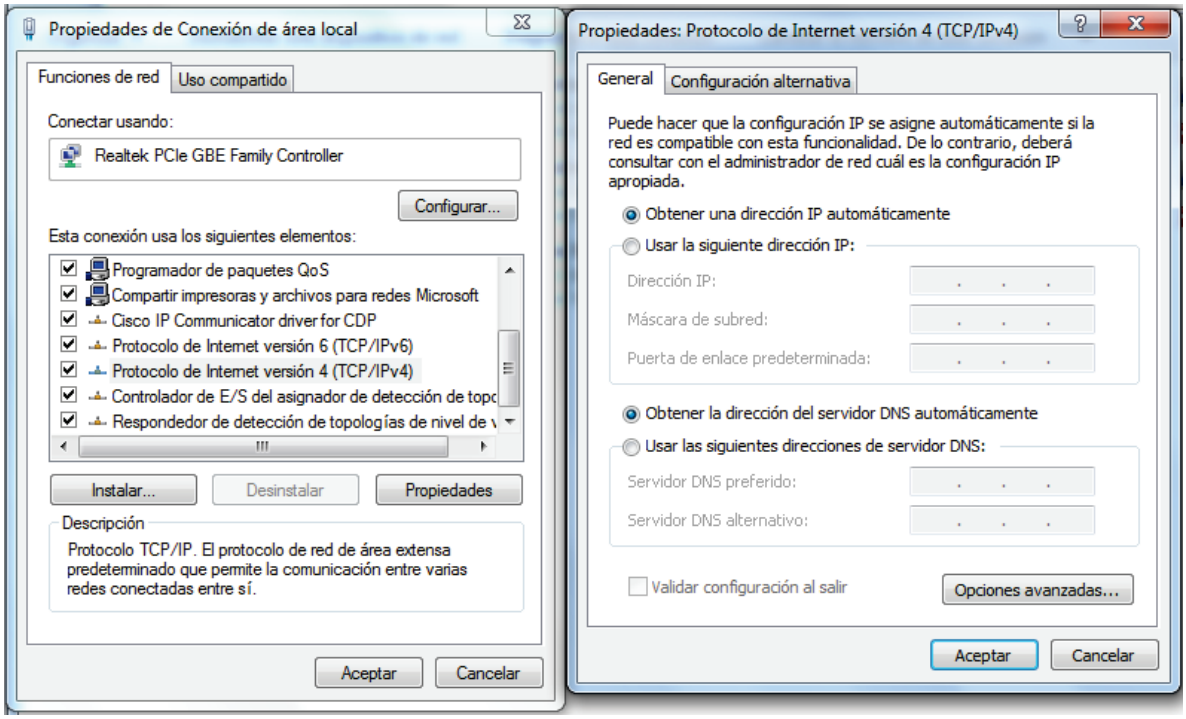
4.1.3. Montad una red de tres PCs sobre el Hub correspondiente a cada grupo (mesa). Por orden, el switch de más arriba es para la mesa más próxima al rack, el siguiente para la siguiente mesa y así sucesivamente.

- Las conexiones se realizarán en el rack mediante latiguillos**,** así que pedírselos al profesor.
- Conectar los latiguillos en el rack entre un Hub y las tomas correspondientes del panel de parcheo B, cuyo número coincide con el de las rosetas del paso 4.1.2

4.2. Configuración – Cambio de IP

Los PCs por defecto vienen configurados con IP dinámica (DHCP) lo que Windows denomina "Obtener una dirección IP automáticamente". Cambiaremos la configuración a IP estática, de acuerdo con lo indicado en la pegatina situada en el frente de cada equipo. Pare ello seguiremos los siguientes pasos menús de Windows:
Inicio → Panel de Control → Redes e Internet → Centro de redes y recursos compartidos → Cambiar configuración del adaptador → Conexión de área local
O bien:

Botón derecho sobre el icono de la red (junto al reloj) → *Centro de redes y recursos compartidos* → *Cambiar configuración del adaptador* → *Conexión de área local*



Marcar "Usar la siguiente dirección IP"
En "Dirección IP" y "Máscara de subred" poner las correspondientes a la pegatina, el resto dejarlo por defecto. Finalmente, *Aceptar.*

4.3. Comprobación de conectividad entre todos los PCs

Lo primero que hay que hacer es verificar la configuración IP de cada PC, para ello utilizaremos el comando **ipconfig**. Después se comprobará que hay conectividad IP entre todos los PCs de la red mediante el comando **ping**. Revisar la Práctica 3 si no recordáis cómo utilizar estos comandos.

4.4. Funcionamiento de ARP

En este apartado usaremos dos comandos:

- **ping**: Envía tramas de prueba a un equipo, para ver si hay conectividad con él. La sintaxis más habitual es: ping *ip_destino*. El destino responde a cada *ping* con un ACK; cuando se recibe éste, se muestra en pantalla el tiempo total transcurrido en ms. Si no se recibe, indicará que expiró el plazo para recibir una respuesta. Si todo está bien todos los equipos responderán.
- **arp**: permite mostrar y modificar las tablas ARP del equipo. Se pueden consultar las opciones con arp –h. Nos interesarán:
    - **arp –a:** muestra la tabla de resolución de direcciones
    - **arp –d ***: borra todas las entradas de la tabla. En lugar de todas (*) se podría especificar una entrada concreta.

  Nota: Para utilizar "arp –d" es necesario el modo administrador. Para ello, al abrir el terminal haz click con el botón derecho sobre el icono del escritorio y selecciona "Ejecutar como administrador"

Nuestro objetivo es ver cómo un equipo utiliza ARP para conseguir la dirección MAC del equipo de destino que queremos alcanzar (identificado por su IP).

Las tareas a ejecutar serán las siguientes:

1. Borrar la tabla ARP de un equipo.
2. Arrancar el analizador (Wireshark) en el equipo
3. Comenzar una captura.
4. Realizar un *ping* a otro equipo.
5. Detener la captura.
6. Analizar y comprender la captura. Tenéis que conseguir los siguientes puntos, anotando las respuestas a las preguntas en una hoja:

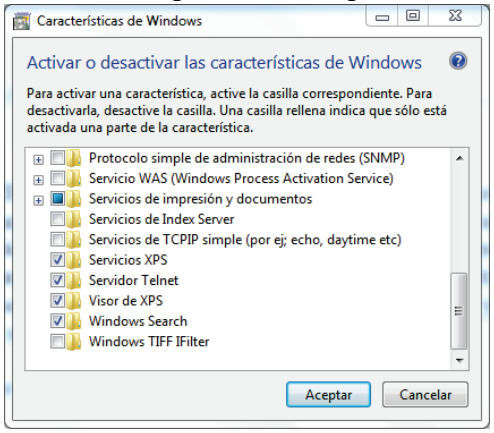
    a. Busca los mensajes del protocolo ARP.
    b. Dibuja la pila de protocolos que se utilizan en ARP (como una pila: nivel físico abajo, y los demás subiendo). Fíjate para ello en las cabeceras utilizadas.
    c. ¿Qué campos contiene la cabecera de Ethernet? Nota: Wireshark no muestra el campo de CRC (aunque marca el paquete si se detecta un error), aunque existe.
    d. ¿En qué momento decide el equipo origen enviar la solicitud ARP de la dirección IP de destino?
    e. ¿Qué MAC de destino tiene la trama de solicitud? ¿Y qué IP de destino? ¿Y en la trama de respuesta? Razona el porqué las respuestas.
    f. ¿Se podría realizar la captura desde el equipo *destino*? ¿Y desde otro equipo, aparte del que pregunta y el que responde? Haced la prueba con una nueva petición.

7. Conectar los PCs a un switch en lugar de un Hub (Ver paso 4.1.3)
8. Repetid los pasos 1 a 5 y responder a la siguiente pregunta:
   ¿Se puede realizar la captura desde cualquier equipo conectado al switch?
9. Volver a conectar el Hub.

NOTA: Puedes guardar las capturas y llevártelas. El analizador Wireshark es gratuito, y lo puedes instalar en tu equipo personal si quieres hacer pruebas o analizar capturas previas.

4.5. Telnet

La aplicación TCP/IP Telnet permite a un emulador de terminal comunicarse con un dispositivo, de forma parecida a lo que ocurre con un emulador en un PC conectado al puerto serie (Ver Práctica 2). Sin embargo, Telnet utiliza una red IP para enviar y recibir datos, en lugar de usar un cable especial y un puerto físico en el dispositivo. Los protocolos de la aplicación Telnet llaman al emulador de terminal **cliente Telnet** y al dispositivo que escucha comandos y responde a ellos **servidor Telnet.**



4.5.1. Instalar un servidor Telnet en un PC

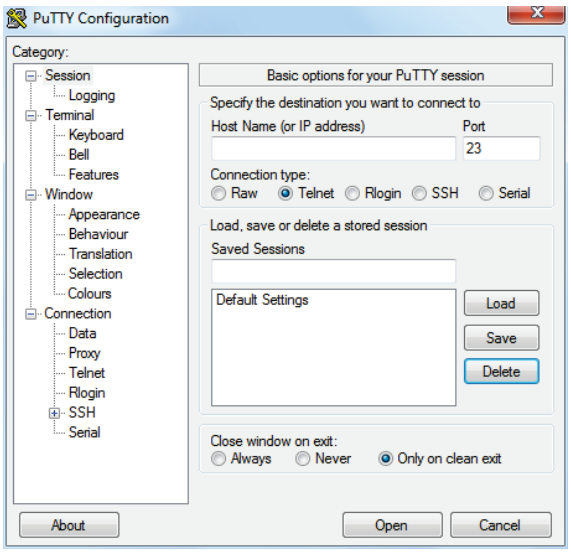
Inicio → Panel de Control → Programas → Activar o desactivar las características de Windows

Marcar “Servidor Telnet” y aceptar.

4.5.2. Arrancar una captura con Wireshark en un segundo PC

4.5.3. Para usar Telnet, el usuario debe instalar un paquete de software de cliente Telnet en el PC. Aquí se utilizará el Putty. En un tercer PC, arrancar el Putty, seleccionar Telnet y en Host Name poner la IP del servidor Telnet.

Puedes ejecutar comandos en la máquina remota (comandos heredados de DOS: dir, cd, etc).



4.5.2. Deten la captura. Localiza la contraseña en las tramas capturadas.

4.6. Recoger el laboratorio

Al finalizar la práctica hay que deshacer las configuraciones realizadas. Para ello se realizarán OBLIGATORIAMENTE las siguientes tareas:

1. Volveremos a conectar los PCs a la toma “A”
2. Desconectar los latiguillos en el rack y devolvérselos al profesor
3. Cambiar la IP a dinámica activando DHCP (ver apartado 4.2)
4. Desactivar el servicio Telnet

4.7. Análisis de tráfico real

En este apartado utilizaremos Wireshark para analizar el tráfico de red mientras navegamos por Internet.

4.7.1. Arrancar una captura con Wireshark en un PC
4.7.2. En ese mismo PC Arrancar el Explorer y navegar por Internet
4.7.3. Observar la captura y localizar las tramas http, ¿cuántas capas aparecen ahora?

Bibliografía

CCENT/CCNA ICND1 Guía Oficial para el examen de Certificación, Wendell Odom, Cisco Press