Práctica 2 - Comunicación en Ethernet

1. Introducción

El objetivo de esta práctica es ver las tramas Ethernet, familiarizarse un poco con el manejo del programa Wireshark y entender el funcionamiento básico de los conmutadores Ethernet.

La primera parte de esta práctica se puede hacer fuera del laboratorio, instalando Wireshark en cualquier sistema operativo soportado (Windows, macOS y Unix/Linux), incluso si solo tiene un interfaz WiFi[1]. En caso de haber instrucciones concretas en la práctica se supondrá que se está llevando a cabo en el laboratorio, aunque con sencillez se puede entender cómo cambiaría para llevar a cabo algo similar en un ordenador independiente.

[1] Con un "salto de fé" debido a que Wireshark va a mostrarnos Ethernet (802.3) al leer del interfaz WiFi aunque sabemos que ese interfaz envía tramas 802.11. Esto es un cambio que hace en driver. En otras asignaturas veremos cómo impedirlo, para así poder ver las tramas 802.11 originales que circulan por el aire.

2. Usando Wireshark

En el ordenador conectado a la red lance el programa Wireshark desde el menú aplicaciones o con el comando:

```
$ wireshark &
```

El programa se lanzará y abrirá una ventana. Wireshark es un analizador de protocolos. Su función principal es mostrar los paquetes observados (enviados o recibidos) en un interfaz, y ayudar a diseccionarlos identificando cada cabecera de protocolo y los campos con información incluidos en la cabecera. Permite también almacenar en un archivo los paquetes que ha visto en un interfaz, para su posterior análisis. A estos ficheros los llamamos normalmente ficheros de captura o trazas. Wireshark también es capaz de abrir un fichero de traza previamente grabado, aunque sea en otra máquina, y hacer su análisis sobre los paquetes de ese fichero.

La ventana inicial de Wireshark es muy similar a la que se puede ver en la Figura 1. Detalles concretos del interfaz dependen de la versión del programa y del ordenador y sistema operativo donde se esté ejecutando.

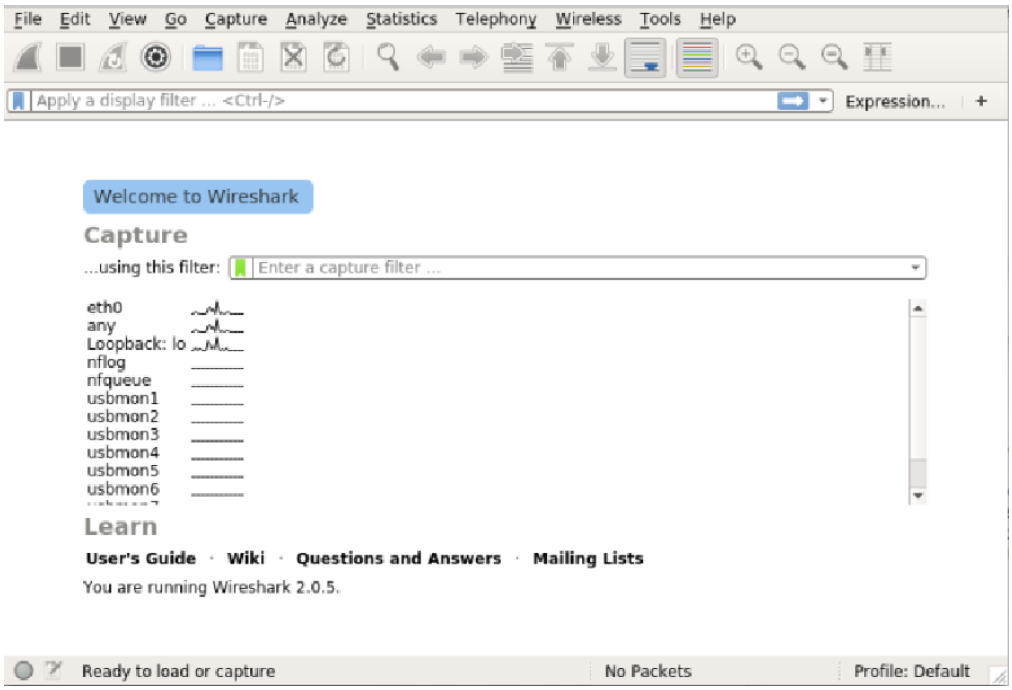

Figura 1 – Ventana inicial de Wireshark

Lo primero que se pide es llevar a cabo una nueva captura del tráfico visto en un interfaz de red. Para ello debe elegir de cuál de los interfaces que unen el ordenador a la red quiere capturar el tráfico. Observe la lista de interfaces disponibles. ¿Su ordenador tiene varios interfaces de red? Aunque es posible tener varias tarjetas de red y estar conectado a varias redes, en el caso del laboratorio la mayoría de los interfaces que ve son virtuales y no representan en realidad una

salida a una red física. En los PCs A, B y C de los armarios sí nos encontraremos con varios interfaces físicos (eth0, eth1, eth2, eth3 y en algunos un interfaz WiFi).

El interfaz `eth0` es el correspondiente, en muchas distribuciones de Linux, a la primera tarjeta Ethernet de tu ordenador (no se extrañe si en una Ubuntu ve algo como `enp0s1` o en macOS un `en0`). En el laboratorio puede observar el cable por detrás que lo une al punto de red de la mesa (directamente del PC en los puestos normales y saliendo del armario en los otros puestos). En el caso del laboratorio de telemática 1, ese punto de red en la mesa es un simple cable hasta el conmutador que se encuentra en la pequeña sala acristalada, en un armario de comunicaciones similar a los que puede ver en el pasillo central del laboratorio.

Del resto de los interfaces que ve, el indicado como `lo` es el llamado interfaz de *loopback,* y sirve para que programas de este ordenador puedan comunicarse entre sí usando protocolos de red, como si lo hicieran por una red física, aunque el ordenador esté desconectado o no posea un interfaz físico; la comunicación es enteramente en software dentro de la máquina y no habrá tiempos de transmisión y de propagación físicos como estamos habituados (o lo estaremos al finalizar esta asignatura). El interfaz `any` no es un interfaz, sino la manera en que Wireshark permite observar todos los interfaces a la vez. En esta práctica queremos observar la red Ethernet del laboratorio, así que elija siempre `eth0`.

Una vez elegido el interfaz a usar, podemos capturar directamente (pulsando el primer icono de la barra de herramientas o doble click sobre el nombre del interfaz) o bien configurar algunas opciones en la captura (cuarto icono, *Capture Options,* Figura 2).

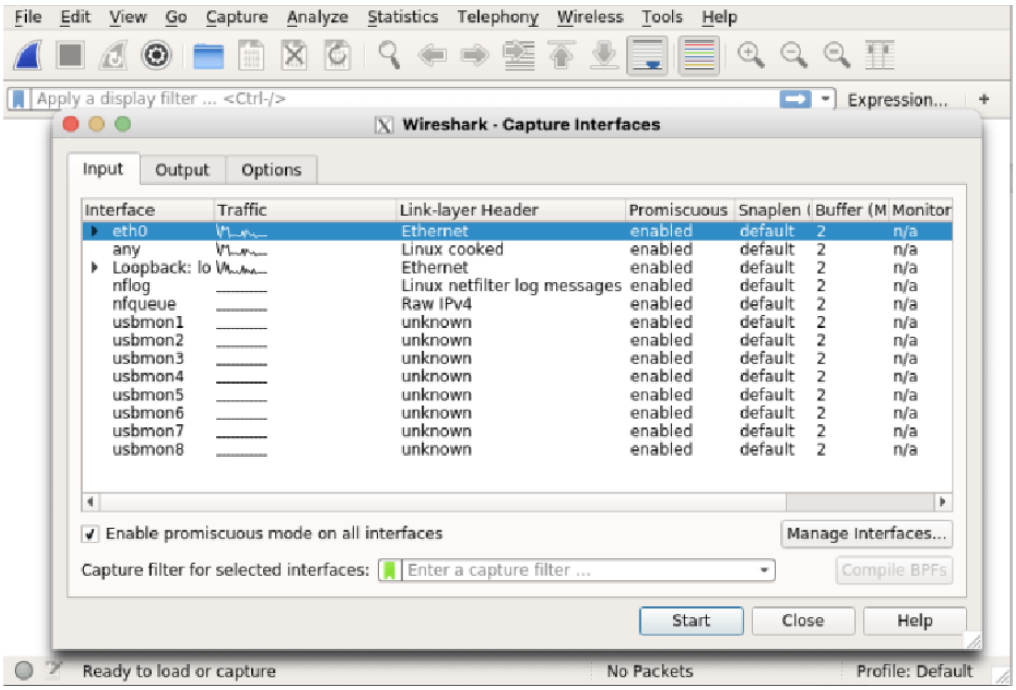

Figura 2 – Ventana de opciones de la captura

La ventana de opciones, en la pestaña de *Input*, muestra:

- *Interface*: permite elegir el interfaz. Disponemos de los mismos que hemos visto anteriormente. Elija `eth0` si no está ya seleccionado.
- *Link-layer header type*: permite elegir el tipo de trama que se envía en ese interfaz. En nuestro caso es *Ethernet.*
- *Capture packets in promiscuous mode*: el modo promiscuo indica si queremos capturar todas las tramas que se vean en ese interfaz o solo las que haya enviado o vayan dirigidas a este ordenador (y de multidifusión). De momento vamos a ver todas las disponibles, con lo que activaremos o dejaremos activada esa opción.
- *Snaplen*: se puede limitar que no se capturen paquetes enteros sino sólo el principio de cada uno para ahorrar memoria y espacio en disco, ya que es posible que lo que queramos ver sean sólo las cabeceras. De momento no capturaremos muchos paquetes así que no indicaremos límite.
- *Capture filter for selected interfaces*: permite decidir de una manera flexible qué paquetes queremos capturar y cuáles no. Es una expresión de texto en un lenguaje de reglas que pone condiciones a todos los paquetes que se reciben, para que los recoja el programa o los ignore. Si un paquete cumple la regla se captura y se muestra o se guarda, y si no la cumple se descarta (el sistema operativo lo sigue procesando siempre con normalidad). En esta primera prueba asegúrese de que el campo está vacío, lo que significa que queremos capturarlos todos.
- Deje el resto de las opciones como están y pulse *Start*

Wireshark empezará a capturar paquetes y a mostrar una lista de los mismos. En cuanto haya unos cuantos detenga la captura pulsando el segundo botón de la barra de herramientas.
Si selecciona ahora un paquete de la lista puede ver detalles sobre ese paquete en los paneles inferiores. Para ver la información un poco más clara, desactive los colores pulsando el botón descrito como *Draw packets using your coloring rules* y que se encuentra justo antes de las lupas de zoom (quinto por la derecha). Si tiene 3 paneles horizontales, en el panel inferior se ve el contenido del paquete completo en hexadecimal y ACSII y en el panel intermedio se ve el análisis que hace Wireshark del contenido del mismo, interpretando cada campo de las cabeceras de protocolos que reconoce. Podemos desplegar cada una de las cabeceras y seleccionar los campos de cada cabecera de modo que en el panel inferior se mostrará dónde está situado ese campo (Figura 3).

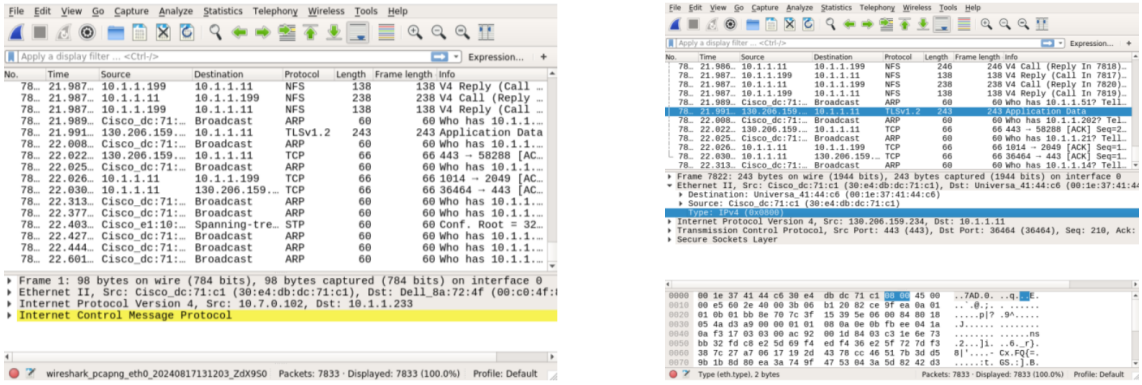

Figura 3 - Captura

En el panel intermedio, la primera línea, que corresponde con el nivel inferior de la pila de protocolos, con nombre *Frame*, muestra los datos de la captura del paquete y no es propiamente una cabecera ni un nivel en la pila, sino metadatos sobre cuándo se capturó el paquete o el tamaño que tenía (podríamos entender que es la información de capa 1). Dentro (a continuación) de *Frame* verá la trama *Ethernet* (su cabecera) y sus datos se interpretarán según el tipo de los mismos (reconocidos por el valor de Ethertype). Dentro de las tramas *Ethernet* verá paquetes IP o ARP, aunque también puede encontrar en el laboratorio tramas con encapsulado 802 LLC. IP a su vez puede transportar paquetes TCP o UDP (y de otros protocolos). Por ejemplo, elija un paquete cualquiera y observe con ayuda del análisis dónde están situadas las direcciones origen y destino de la capa *Ethernet*. Observe también cómo los paquetes de diferentes tipos IP o ARP tienen diferente valor en el campo *Type* (el *Ethertype*).

Utilice en un terminal el comando `ifconfig` (en Windows tiene `ipconfig`) para averiguar la dirección de su interfaz *Ethernet*. Puede ver ahí la dirección MAC (*HWaddr*) y la dirección IP (*inet addr*) si se le ha configurado una (en el laboratorio tienen todos los PCs salvo los PC A, B y C de los armarios).

```
$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:1e:37:41:44:c6
          inet addr:10.1.1.11  Bcast:10.1.255.255  Mask:255.255.0.0
          ...
```

Utilice la dirección MAC para localizar en la traza un paquete enviado por su ordenador. Fíjese en que en la lista de paquetes puede aplicar un filtro para visualizar solo un subconjunto de los mismos. Esto se llama *display filter* y se escribe en un lenguaje de reglas diferente del lenguaje empleado en el *Capture filter*. Puede escribir el filtro directamente o editar reglas y añadirlas pulsando en el botón *Expression* (tendrá que elegir en la lista los protocolos sobre los que aplicar las reglas). Por ejemplo, puede ver solo los paquetes que tengan una dirección MAC concreta eligiendo reglas como las que se muestran a continuación. Note la diferencia entre ellas y pulse *Enter* para aplicar el filtro.

```
eth.addr==00:1e:37:2c:db:b2  # indique su dirección MAC
eth.src==00:1e:37:2c:db:b2   # indique su dirección MAC
ip.src==10.1.1.26            # indique su dirección IP
```

En un paquete resultado del filtro examine la cabecera *Ethernet* para comprobar las direcciones MAC origen y destino de la trama *Ethernet*. Compruebe si la dirección MAC de origen o la de destino coincide con la de su ordenador. Observe que las direcciones IP origen y destino del paquete aparecen en la cabecera IP que va dentro de la trama *Ethernet*. Borre el filtro de *display* con el botón con una X.

Guarde la traza de paquetes capturados en disco para su posterior análisis, use el formato *pcap* o el *pcapng*. Observe (opciones del menú File) que si desea puede guardar solo los paquetes seleccionados o los que cumplan el D*isplay Filter*. Cierre Wireshark y láncelo de nuevo. A continuación, abra con él el fichero de captura para volver a examinar la traza.

Vuelva a iniciar el diálogo de opciones para capturar. Elija el interfaz `eth0` y especifique un filtro de captura. Puede indicar a Wireshark que no capture todos los paquetes que vea sino que sólo elija algunos. Como ya se ha mencionado, esto se llama C*apture Filter*. Consiste en una serie de condiciones en un lenguaje de reglas (BPF, *Berkeley Packet Filter*). Por razones históricas, este lenguaje no es el mismo que el empleado en el D*isplay Filter*. Por ejemplo, las reglas de los ejemplos anteriores, en C*apture Filter* son:

```
ether host 00:1e:37:2c:db:b2
ether src 00:1e:37:2c:db:b2
ip src 10.1.1.26
```

3. Gráficas en Wireshark

El menú *Statistics* ofrece la opción *I/O Graphs,* que permite hacer gráficas con el tráfico capturado (Figura 4). Incluso puede actualizar la gráfica automáticamente a medida que progresa la captura.

Explore las opciones de estas gráficas. Puede cambiar la escala horizontal (el nivel de agregación, con *Interval*). Puede incluir varias secuencias en la misma figura. También puede cambiar el *Display filter* que limita los paquetes en los que se basa una secuencia representada. Vea que en el eje de ordenadas puede representar las cuentas agregadas de bytes o de paquetes en el intervalo de agregación (aunque ponga que son por segundo lo son solo si el intervalo es de 1s).

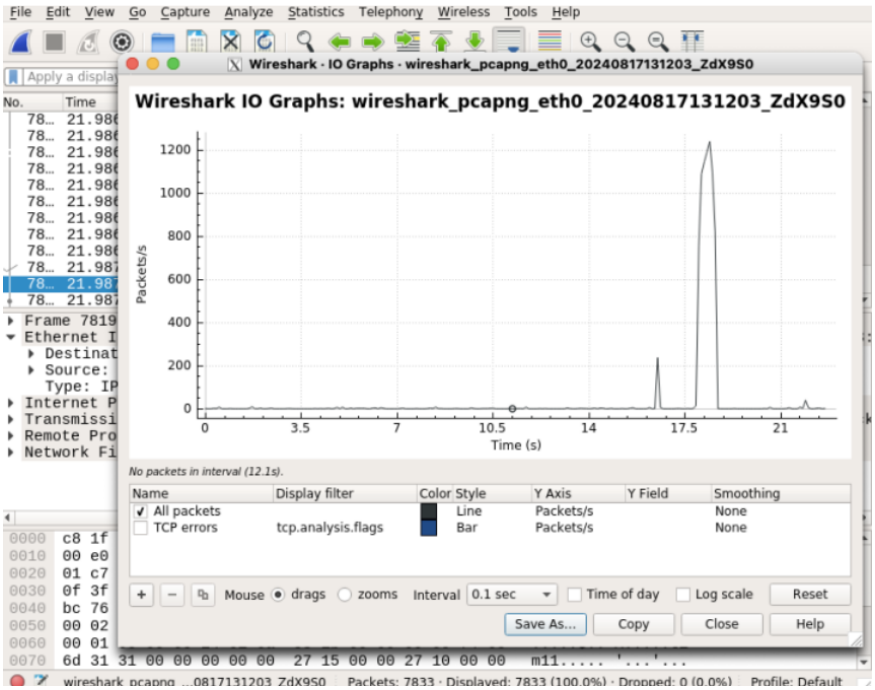

Figura 4 – I/O Graphs

Estas gráficas serán útiles en las prácticas para visualizar la tasa a la que se están enviando paquetes.

Se recomienda explorar un poco el tráfico que puede encontrar en la red del laboratorio o en la de su hogar. A medida que vayamos pasando por asignaturas sobre redes y aplicaciones iremos entendiendo más sobre los diferentes tipos de tráfico que nos podemos encontrar y los veremos con esta herramienta.

4. Comunicación en Ethernet

A continuación, enviaremos tramas entre hosts (ordenadores) del laboratorio y observaremos el tráfico empleando Wireshark.

Para todas las actividades que requieran configuración de equipos se emplearán los puestos de trabajo del Laboratorio de Telemática 1 que cuentan con armarios rack con equipamiento de red. Cada armario disponible de cuatro ordenadores, así como diverso equipamiento de red. En esta práctica utilizaremos sólo equipos de red Ethernet, en asignaturas posteriores podrá usar el resto (algunos solo en asignaturas optativas). De los cuatro ordenadores disponibles, recuerde que solo el llamado **PC-SC** está unido y configurado para la red normal del laboratorio. En este ordenador puede autentificarse usando su cuenta de prácticas **arssXY** y desde ahí acceder a Internet, por ejemplo, para leer documentación sobre los equipos del armario. Los otros 3 ordenadores **PC-A**, **PC-B** y **PC-C** no tienen configurados los interfaces de red y no están conectados a ningún equipo de red, de forma que pueda practicar con ellos. En estos ordenadores deberá autentificarse con la cuenta común ***arss*** y contraseña ***telemat*** (no modifique la contraseña de esa cuenta).

En primer lugar, familiarícese si no lo ha hecho ya con el control del teclado y pantalla para usar cada ordenador. Pulsando en el teclado dos veces rápidamente la tecla *Bloq-Despl* el monitor presentará un menú con los cuatro ordenadores del armario. En ese menú puede elegir a qué ordenador está asociado el monitor y el teclado. Haga login en PC-SC para tener una sesión con un navegador. Cambie a PC-A y haga login utilizando la cuenta *arss* (no la arssXY). Entre también en PC-B para probar. Observe que puede ir cambiando entre los ordenadores y dar comandos a cada uno manteniendo el login abierto (simplemente está cambiando el teclado, pantalla y ratón de uno a otro). **Recuerde cuando acabe la práctica que debe cerrar todas las sesiones en todos los ordenadores**.

En MiAulario, en el sitio "Área de Ing. Telemática" tiene un enlace "Información sobre los recursos del Laboratorio de Telemática 1" donde puede encontrar información sobre los equipos de los armarios. Es importante que revise especialmente lo relacionado con los PCs y con su cableado. Como no tiene acceso a la trasera de estas máquinas, donde se accede a sus interfaces Ethernet, se han dejado cableados hasta los paneles de parcheo que hay en el armario. Debe localizar qué puerto del panel de parcheo corresponde a cada interfaz de cada equipo.

Recuerde que puede ver el estado y configuración de los interfaces de los ordenadores con el comando `ifconfig`. Si los interfaces están *"apagados"* o `DOWN` no aparecerán en la salida del comando si no incluye la opción `-a`, en cuyo caso verá algo como:

```
$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0d:88:cd:6e:c8
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth1      Link encap:Ethernet  HWaddr 00:0d:88:cd:6e:c9
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth2      Link encap:Ethernet  HWaddr 00:0d:88:cd:6e:ca
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth3      Link encap:Ethernet  HWaddr 00:0d:88:cd:6e:cb
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:388 errors:0 dropped:0 overruns:0 frame:0
          TX packets:388 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:30856 (30.8 KB)  TX bytes:30856 (30.8 KB)

wlan0     Link encap:Ethernet  HWaddr 00:13:f7:83:6c:e4
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Puede activar y desactivar un interfaz empleando el comando `ifconfig` o el comando `ip` (`ifconfig` suele funcionar en cualquier UNIX mientras que `ip` es un comando específico de Linux).

Ciertos comandos o ciertas operaciones con ciertos comandos requieren privilegios extra, normalmente privilegios que tiene solo la cuenta `root` del sistema UNIX.

Por ejemplo, ver la configuración de los interfaces no suele requerir privilegios especiales, pero modificarla sí. En los PCs A, B y C puede ejecutar ciertos comandos que requieren esos privilegios si emplea el comando `sudo`. Este comando permite ejecutar otro comando con los privilegios del usuario `root` (simplemente escriba `sudo` por delante del comando que quiera utilizar). Puede activar y desactivar un interfaz haciendo:

```
# Sustituya eth0 por el interfaz correspondiente
$ sudo ifconfig eth0 up
$ sudo ifconfig eth0 down
```

Puede emplear el comando `ethtool` para obtener información sobre un interfaz Ethernet (el interfaz tendrá que estar activado, "UP"). Se resaltan algunos valores que son de especial interés.

```
$ sudo ethtool eth0
Settings for eth0:
        Supported ports: [ TP MII ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Supported pause frame use: No
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Advertised pause frame use: Symmetric
        Advertised auto-negotiation: Yes
        Speed: 10Mb/s
        Duplex: Half
        Port: MII
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: pg
        Wake-on: d
        Current message level: 0x00000001 (1)
                               drv
        Link detected: no
```

En esta práctica se enviarán tramas Ethernet entre los PCs. Para ello tiene un programa llamado `ethSend` que se ha preparado específicamente para las actividades de esta práctica (no lo encontrará fuera del laboratorio). Puede ver sus opciones lanzándolo con la opción `--help`.

```
$ ethSend --help
```

El programa le permite indicar los valores de la cabecera Ethernet para construir y enviar una o varias tramas, así como puede obtener de un fichero la información necesaria para construirlas y enviarlas.

4.1 Comunicación entre dos hosts en conexión directa

Interconecte dos PCs empleando un cable Ethernet (Figura 5).

Figura 5 – Dos PCs con un enlace Ethernet directo

Tenga en cuenta el tipo de cable que utiliza para la conexión. Elija el correcto (recto o cruzado)[2] para que funcione. En el laboratorio, por lo general, los cables rectos son los que tienen la cubierta de color blanco y los cruzados los que tienen el cable de color azul o el cabezal de color rojo/verde o se le ha añadido una etiqueta en un extremo. No obstante, no debería depender de ello y es mejor comprobar el tipo de cable antes de utilizarlo. Para ello, si alinea los conectores del cable debería poder ver si el orden de los conductores se mantiene o si estos se cruzan (en algunos cables es más sencillo de ver que en otros). Por ejemplo, en la figura 6 puede verse un ejemplo de cable recto, note cómo el orden de los conductores (en base a su color) se mantiene en ambos conectores.

Figura 6 – Cable recto.

Active (up) los interfaces de los PCs que vaya a emplear. Lance Wireshark en uno de ellos y envíe alguna trama Ethernet desde el otro empleando `ethSend` (necesitará usar `sudo`). ¿Debería llegar la trama al otro PC independientemente de la dirección MAC destino que haya indicado? ¿Por qué o por qué no?

[2] https://www.fs.com/es/blog/patch-cable-vs-crossover-cable-what-is-the-difference-4767.html

Si la dirección MAC destino es una dirección unicast que no coincide con la del interfaz que la recibe, éste la descartará. Sin embargo, en este caso al estar el interfaz configurado en modo promiscuo para la captura de Wireshark no la descartará, sino que llegará al programa. En funcionamiento normal (no promiscuo) el sistema operativo no llegaría a ver esas tramas.

Pruebe la funcionalidad de `ethSend` de enviar múltiples tramas consecutivamente para generar un tráfico de cierta intensidad y vea dicho tráfico en el otro PC empleando la utilidad de gráficas de Wireshark.

***Nota importante**: Tenga en cuenta que Wireshark almacena en memoria todos los paquetes que va capturando hasta que usted cierre la captura. Si está capturando muchos paquetes (del orden de varios millones) su ordenador puede empezar a quedarse sin memoria y notará como cada vez "funciona más lento". Si se da el caso, simplemente tiene que cerrar la captura e iniciar una nueva.*

Punto de control 1 (40%): Muestre alguna de estas gráficas al profesor de prácticas mientras se está haciendo el envío, explicando el cálculo de la tasa a la que está viendo tráfico.

4.2 Comunicación a través de un conmutador

En cada armario tiene un conmutador etiquetado como switch5 de marca Cisco y modelo Catalyst 2950 (preste atención a la etiqueta ya que es posible que su armario tenga dos switches del mismo modelo). Este será el switch que se utilice a lo largo de las distintas prácticas de esta asignatura.

Este conmutador se comporta en realidad como 3 conmutadores independientes. El primero está formado por los puertos del primer bloque (1-8), el segundo por los puertos centrales (9-16) y el tercero por los puertos de la derecha (17-24). A todos los efectos, en estas prácticas puede considerar esos 3 bloques de puertos como 3 conmutadores diferentes. Es decir, si conecta por ejemplo un interfaz de un PC al puerto 1 y otro al puerto 9 no va a haber reenvió de tramas entre ellos pues están conectados a conmutadores independientes. Interconecte 3 PCs empleando el conmutador (Figura 7). Puede usar cualquier puerto siempre que sean del mismo bloque.

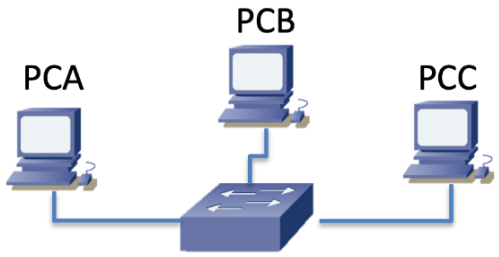

Figura 7 –PCs conectados a un conmutador

El conmutador tiene el comportamiento que se ha visto en clase: aprende en función de la dirección MAC origen de las tramas y reenvía en base a la dirección destino y lo que tiene aprendido. Si no sabe por qué puerto se llega al destino o la dirección destino es de multicast/broadcast hará inundación. Cuando se enciende, el conmutador no conoce por qué puerto debe enviar para llegar a ninguna dirección MAC. Si se desconecta un puerto olvida todo lo aprendido por el mismo. Pasado cierto tiempo sin recibir tramas de una dirección MAC la borrará de su tabla de aprendizaje.

Vamos a emplear 3 PCs para comprobar el comportamiento del conmutador, es decir, en qué situaciones reenvía por todos los puertos y en cuáles no. Con 3 PCs podremos enviar tramas desde uno y comprobar si se reenvían a los otros dos (seguramente por haber hecho inundación), solo a uno de ellos o a ninguno. Según el modelo del conmutador soportará Auto-MDI/MDI-X en todos los puertos o no, así que por si acaso esté atento al tipo de cable (ni las NICs de los PCs A, B y C ni el Catalyst2950 soportan Auto-MDI/MDI-X).

El conmutador no va a aprender las direcciones MAC de los hosts hasta que reciba alguna trama de cada uno de ellos. Aunque usted no envíe ninguna trama es probable que otros programas que estén corriendo en el PC lo hagan en cuanto

detecten un interfaz activo. Esto va a hacer que probablemente sin que hagamos nada el conmutador ya haya aprendido las direcciones MAC de los 3 interfaces (una vez que los active, claro). Sin embargo, recuerde que el conmutador no aprende las direcciones simplemente por conectarle el cable, ni aunque active el interfaz y se encienda la luz del conmutador indicando que detecta el enlace. No hay un mecanismo en capa física para ello (la dirección MAC es un parámetro de capa 2 así que requiere un manejo de tramas). El mecanismo en capa 2 se basa precisamente en enviar alguna trama, pero normalmente la NIC no va a enviar ninguna trama hasta que se lo solicite el sistema operativo. Hasta que el conmutador no vea una trama Ethernet no puede aprender una dirección origen y en cualquier caso no sabe si lo que hay al otro extremo es un host o un conmutador (ni cuando recibe una trama).

Desde el PC SC puede acceder al interfaz de gestión del conmutador y ver la tabla de direcciones MAC que tiene aprendidas. Esto se está haciendo mediante el puerto serie del PC y el puerto "de consola" del switch (probablemente esté por la parte trasera del equipo y no lo ve). Acceda al interfaz de gestión del conmutador como se describe a continuación y compruebe qué direcciones MAC ha aprendido y en qué puerto las tiene identificadas.

```
$ minicom switch5
Welcom to minicom 2.7

Options: I18n
Compiled on Feb  7 2016, 13:37:27.
Port /dev/ttyS8,  17:52:25

Pess CTRL-A Z for help on special keys

[Pulse ENTER]
```

Si en este punto le pregunta para abrir la configuración, conteste que no. Posteriormente presione ENTER de nuevo. Una vez conectado al conmutador, puede listar la tabla de direcciones MAC del primer grupo de puertos del conmutador con el siguiente comando:

```
Switch> show mac address-table dynamic vlan 101
Vlan     Mac Address       Type      Ports
----     --------------    -------   -----
 101     000d.88cd.704d    DYNAMIC   Fa0/1
 101     000d.88cd.704e    DYNAMIC   Fa0/2
```

Debería obtener una salida similar a la mostrada (la tabla puede estar vacía si el conmutador no ha aprendido ninguna dirección). También se puede consultar las direcciones MAC de los otros 2 grupos de puertos reemplazando el identificador `101` por `102` o `103` respectivamente. Las columnas que nos resultan de interés son la 1ª, 2ª y 4ª:

- Columna `Vlan`: Nos indica el identificador de la vlan (veremos en asignaturas posteriores qué es esto exactamente). Por el momento podemos entenderlo como a qué bloque de puertos corresponde la regla aprendida. Los identificadores que veremos son el `101`, `102` o `103`, según lo indiquemos al ejecutar el comando.
- Columna `Mac Address`: Nos indica la dirección MAC que el conmutador ha aprendido. Cuando reciba tráfico con esa dirección destino la sacará por el puerto indicado en la 4ª columna. Aquí veremos cómo según generemos tráfico irán apareciendo las direcciones MAC de las interfaces de los PCs.
- Columna `Ports`: Identificador del puerto por el que reenviará el tráfico cuya dirección destino coincida con la indicada. Los nombres de los puertos son `Fa0/x` (de FastEthernet), donde `x` es el número del puerto del conmutador.

Nota: *Puede salir en cualquier momento cerrando la terminal o pulsando `CTRL-A + Z + q`, y contestando que sí a "`Leave without reset?`" pulsando ENTER.*

Habrá visto con la herramienta `ethtool` que las interfaces soportan las velocidades de 10Mb/s y de 100Mb/s, así como la negociación automática de velocidad y duplex. El conmutador también soporta todo eso (aunque puede no soportar Auto-MDI/MDI-X). ¿Qué velocidad ha negociado cada interfaz?

Tenga Wireshark corriendo en los tres PCs, capturando del interfaz conectado al conmutador. Empiece por probar a enviar una trama desde PC A dirigida a la propia dirección MAC de PC A (empleando `ethSend`). ¿En qué Wireshark(s) la ve?

Envíe ahora desde PC A una trama dirigida a la dirección MAC de broadcast (`ff:ff:ff:ff:ff:ff`). ¿En qué Wireshark(s) la ve? Si vuelve a consultar la tabla de direcciones MAC de conmutador, ¿qué diferencias puede ver?

Envíe una trama desde PC A a PC B (misma pregunta) y después una de PC A a PC C (idem).

Envíe un flujo continuo de tramas desde PC A dirigido a la dirección MAC de broadcast. En paralelo, desde otro terminal, envía también desde PC A un flujo continuo dirigido a la dirección MAC de PC B. Finalmente añada un tercer flujo dirigido a una dirección unicast que no corresponda a ninguno de los interfaces de los PCs.

Punto de control 2 (30%): Muestre gráficas con esos flujos en los 3 PCs mientras los va añadiendo y explique lo que está sucediendo. Muestre el contenido de la tabla de MACs del conmutador y explíquelo.

4.3 Comunicación a través de dos conmutadores

Emplee dos conmutadores para crear la LAN que se ve en la Figura 8. En este caso, deberá utilizar dos bloques de puertos distintos en representación de cada conmutador y conectar ambos bloques con un enlace. ¿Qué tipo de cable tendremos que emplear?

En el PC B emplearemos dos de sus interfaces, cada uno conectado a un puerto de uno de los conmutadores (los llamaremos switchI y switchD de Izquierda y Derecha). Lance Wireshark en PC A y PC C escuchando del interfaz correspondiente, y en PC B lance dos instancias del programa, una para escuchar de cada interfaz en uso.

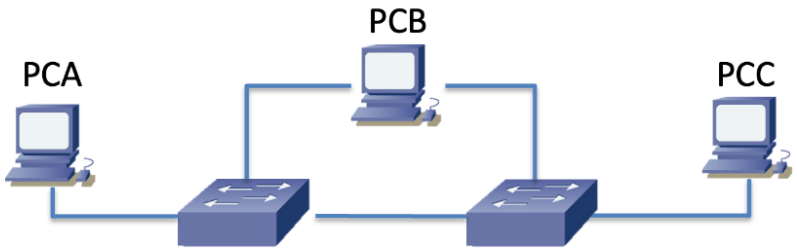

Figura 8 – LAN con 2 conmutadores

Verifique el proceso de reenvío de los conmutadores enviando desde PC A tramas unicast a las direcciones MAC de los diferentes interfaces de los hosts o a la dirección de broadcast y verificando que la trama es reenviada por los interfaces que espera. Puede revisar las tablas de direcciones MAC de los conmutadores para verificar lo que está aprendiendo el conmutador y los saltos que da el tráfico que se envía. Recuerde que para seguir el flujo del tráfico deberá consultar las tablas de todos los grupos de puertos que haya utilizado utilizando el identificador correspondiente.

Recuerde que el conmutador no va a saber por dónde reenviar las tramas a una dirección destino hasta que haya recibido una trama con esa dirección como origen. También recuerde que si pasa suficiente tiempo (del orden de unos pocos minutos) sin que reciba ninguna trama con esa dirección origen va a borrar la entrada en su tabla, al igual que si desconecta el cable de red.

Punto de control 3 (30%): Muestre al profesor un caso de inundación y uno de conmutación en el que solo llegue la trama al destino unicast.