Práctica 1 - IP en redes de área local Ethernet

1- Objetivos

Para construir escenarios de redes incluyendo hosts y routers el primer paso es configurar PCs que funcionen con IP en redes de área local. Por ello en esta práctica repasaremos los comandos y ficheros básicos para configurar un interfaz de red Ethernet con IP en Linux y conectarlo a una LAN con un router de acceso. Emplearemos en esta LAN diferentes elementos típicos de redes Ethernet como son los concentradores (hubs) y los conmutadores (switches).

Aprender a configurar un interfaz Ethernet de un PC será también el primer paso para aprender a crear un router IP a partir de un PC, como veremos en otra práctica.

2- Material

Para la realización de esta práctica necesitaremos el siguiente equipamiento de los armarios:

- PCs
- Concentrador Ethernet
- Cables categoría 5
- Cable coaxial fino

3- Avisos generales

En los ordenadores dispuestos para la realización de estas prácticas (PC A, B y C) se ha creado una cuenta de nombre `ar` y password `telemat`. Esta cuenta tiene permisos para ejecutar mediante el comando sudo ciertos comandos restringidos normalmente al superusuario. Igualmente se le han otorgado permisos para modificar el contenido de ciertos ficheros del sistema necesarios para la realización de la práctica. Para más detalle diríjanse a la documentación sobre los armarios.

Si quieren conservar cualquier fichero entre sesiones guárdenlo en un disquete o un pendrive, dado que no se asegura que los ficheros creados o modificados durante una sesión de prácticas se mantengan para la siguiente.

4- Configuración manual de IP sobre el interfaz Ethernet

Los PCs A, B y C disponen cada uno de una tarjeta con cuatro interfaces Ethernet integrados. Analizaremos previamente dichos interfaces (en adelante se tratarán como tarjetas Ethernet independientes).

- Lea la página del manual del comando `ifconfig` (localizado normalmente en el directorio `/sbin`). Este comando permite configurar los interfaces de red de una máquina. Si ejecuta el comando sin opciones podrá ver los interfaces que se encuentran activos. Si no ha configurado ninguna de las tarjetas Ethernet lo normal es que sólo aparezca el interfaz de loopback que suele ser el `lo0`. Este interfaz no corresponde a ninguna tarjeta de red física sino que es parte del software del sistema y puede servir para que programas ejecutándose en la misma máquina se comuniquen empleando protocolos de red.

- Ejecute el comando `ifconfig` con la opción `-a`. Esta opción muestra todos los interfaces de red reconocidos por el kernel. Aquí podremos ver las tarjetas Ethernet, aunque no estén configuradas, siempre que hayan sido detectadas por el sistema operativo.
- Averigüe la dirección MAC (o dirección hardware) de cada una de las tarjetas del PC A

A continuación procederemos a crear una pequeña red con un par de PCs en la misma que se podrán comunicar empleando la familia de protocolos TCP/IP.

- Conecte mediante un cable recto el puerto del panel de parcheo correspondiente al primer interfaz de red (`eth0`) del PC A con uno de los puertos del concentrador que también están en el panel de parcheo
- Haga lo mismo con el primer interfaz del PC B
- Busque en la página del manual del comando ifconfig cómo configurar la dirección IP de un interfaz
- Configure el interfaz `eth0` del PC A para que su dirección IP sea `10.3.armario.1` donde debe substituir armario por el número del armario donde realiza las prácticas. Emplee como máscara de red `255.255.255.0`
- Compruebe que el PC A puede hacer ping a su propia dirección IP
- Configure el interfaz `eth0` del PC B para que su dirección IP sea `10.3.armario.2` donde debe sustituir armario por el número del armario donde realiza las prácticas. Emplee como máscara de red `255.255.255.0`
- Compruebe que el PC B puede hacer ping a su propia dirección IP
- Compruebe que el PC A puede hacer ping a la dirección IP del PC B
- Compruebe que el PC B puede hacer ping a la dirección IP del PC A

Checkpoint 1.1: Muestre al responsable de prácticas que esos pings le funcionan

5.- Viendo el tráfico con tcpdump y con wireshark

Vamos a ver los paquetes IP que los PCs se envían como resultado de la aplicación `ping`. Para ello en primer lugar emplearemos el programa `tcpdump`.

El programa `tcpdump` nos permite observar los paquetes de red que son recibidos o transmitidos por un interfaz de red. Para ello lee del interfaz de red y muestra de una forma sencilla de entender el contenido principal de las cabeceras del paquete. Además, si el interfaz está en modo promiscuo (vea `ifconfig`) permite ver también todos aquellos paquetes que circulen por el dominio de colisión al que se esté conectado. Tiene bastantes opciones, entre ellas se pueden especificar filtros para que sólo muestre los paquetes que cumplan ciertas condiciones (por ejemplo ser paquetes TCP dirigidos al puerto 80) o indicar el interfaz por el que leer. Opciones útiles son por ejemplo la combinación `-nl`, la opción `l` hace que los paquetes aparezcan por pantalla nada más recibirse y `n` que las direcciones (o los puertos) no se conviertan en nombres DNS (o en nombres del servicio) (salvo que se indique lo contrario emplee siempre ambas opciones).

Manteniendo la configuración anterior de los PCs A y B siga los siguientes pasos:

- Ejecute en PC A el programa ping enviando paquetes al interfaz del PC B y déjelo ejecutándose.

- En el PC A (en otro terminal) ejecute el programa tcpdump para ver los paquetes que se están enviando y recibiendo. El ping envía paquetes del protocolo ICMP que se transporta dentro de datagramas IP. Para hacer que `tcpdump` nos muestre sólo estos paquetes podemos ejecutar:

```
> tcpdump -nl icmp
```

A continuación emplearemos `wireshark`. Éste es un programa similar a `tcpdump` pero con interfaz gráfico:

- Ejecute en PC A el programa `ping` enviando paquetes al interfaz del PC B y déjelo ejecutándose (o si ya lo tenía corriendo no lo pare).
- Ejecute en el PC B el programa `wireshark` para ver los paquetes que se están enviando. El ping envía paquetes del protocolo ICMP que se transporta dentro de datagramas IP. Puede indicarle al programa `wireshark` que filtre el tráfico que ve de forma que sólo muestre los paquetes ICMP. Para ello en la casilla de texto junto al botón *Filter* escriba `icmp`. En el menú *Capture* escoja la opción *Interfaces...*, y pulse el botón Start del interfaz correcto (`eth0`). Debería ver en una ventana cómo `wireshark` está recogiendo paquetes de diferentes tipos, cuando vea que tiene varios de tipo ICMP pulse el botón *Stop* en el menú de iconos.
- Analice el contenido de esos paquetes ICMP gracias a la decodificación de sus campos ofrecida por `wireshark`

Checkpoint 1.2: Muestre al responsable de prácticas la traza de paquetes ICMP que ha capturado con el programa `wireshark`

Hasta aquí hemos visto los paquetes IP bien en la máquina que envía el ping (y recibe la respuesta) o en la que recibe el ping (y envía la respuesta). Sin embargo, dado que ambas máquinas se encuentran conectadas en el mismo Hub o concentrador Ethernet sabemos que cualquier otra máquina que conectemos al mismo debería ser capaz de ver esos paquetes siempre que configure su tarjeta de red para recibir todo el tráfico. Para ver esto siga los siguientes pasos:

- Conecte mediante un cable recto el puerto del panel de parcheo correspondiente al primer interfaz de red (`eth0`) del PC C con uno de los puertos del mismo concentrador.
- Active dicho interfaz de red del PC C. Para ello no necesita darle una dirección IP (aunque podría hacerlo), basta con que ejecute:

```
> sudo ifconfig eth0 up
```

- Ejecute en PC C el programa `tcpdump` y vea los paquetes IP del ping entre PC A y PC B

Checkpoint 1.3: Muestre al responsable de prácticas que ha realizado esta configuración y puede ver los paquetes en una máquina que no es ni el emisor ni el receptor del ping (o sea, en PC C)

6.- Interconexión de Hubs

A continuación vamos a extender el tamaño de nuestra red en cuestión de número de puertos a los que podemos conectar PCs. Para ello vamos a conectar un segundo hub al primero. Los puertos de un hub están preparados para conectarse a un PC con un cable recto. Si quisiéramos conectar entre sí dos hubs por medio de esos puertos deberemos emplear un cable cruzado. Otra alternativa que nos ofrecen los hubs es que normalmente disponen de un puerto de uplink el cual está listo para conectarse a otro hub con un cable recto. En el caso del segundo hub de que disponen, el puerto 8 tiene dos puertos (sólo se puede emplear uno de los dos a la vez), uno de ellos es para conectar un PC con un cable recto y el otro (el marcado como 8X) para conectar otro hub con un cable recto (no se confundan con los dos puertos que tiene en la parte posterior que son para otra finalidad). Por

supuesto, también podemos conectar un PC en el puerto 8X, pero entonces, ¿Qué tipo de cable deberíamos emplear?

Veamos pues cómo extender nuestra red:

- Mantenga el ping del apartado anterior en ejecución.
- Enchufe el segundo hub en la regleta que tiene en la parte frontal del armario.
- Conecte el puerto 8X del segundo Hub mediante un cable recto a uno de los puertos del Hub del panel de parcheo.
- Desconecte el PC A del panel de parcheo y conéctelo al otro hub.
- Compruebe que sigue funcionando el ping.

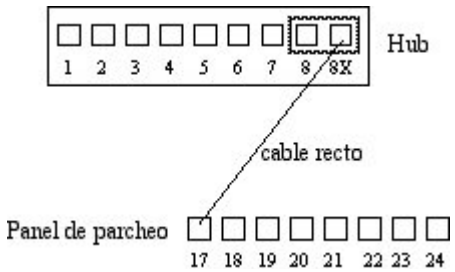

Figura 1.- Conexión de dos hubs

A continuación vamos a comprobar que ambos hubs forman el mismo dominio de colisión:

- Vuelva a conectar el PC A en el hub del panel de parcheo de forma que tanto el PC A como el B se encuentren en dicho hub.
- Conecte el PC C en el segundo hub en vez de en el primero.
- ¿Puede ver desde PC C (en otro hub) los paquetes que se mandan PC A y PC B?

Estos hubs disponen no sólo de puertos RJ45 sino también de un puerto BNC. Estos permiten interconectar los concentradores mediante coaxial para formar una troncal 10Base2. Para comprobarlo:

- Repita el ejercicio anterior, en esta ocasión interconectando los hubs mediante coaxial
- Compruebe que todos los puertos de los dos hubs se encuentran en el mismo dominio de colisión

Checkpoint 1.4: Muestre al responsable de prácticas que ha conectado los dos hubs y que desde un puerto de uno cualquiera de ellos puede ver paquetes que se envían PCs que están conectado al otro hub

7.- Conmutadores Ethernet

Hasta aquí hemos visto el empleo de concentradores para formar una LAN Ethernet. Hemos visto que al interconectarlos extienden el dominio de colisión. Es decir, en todos los hubs de la LAN se ve todo el tráfico que comparte los 10Mbps máximos de la Ethernet convencional (o 100Mbps si es FastEthernet). Podemos mejorar el rendimiento de la LAN empleando puentes o conmutadores (switches). En el armario cuentan con dos conmutadores. A continuación vamos a probar a crear una LAN empleando el switch0.

Manteniendo la configuración IP de los interfaces de red:

- Conecte mediante un cable recto el puerto del panel de parcheo correspondiente al primer interfaz de red (`eth0`) del PC A con uno de los primeros 8 puertos del switch0. Cada 8 puertos de este conmutador están configurados de manera que forman en sí un conmutador independiente.
- Haga lo mismo con el primer interfaz del PC B.
- Compruebe que el PC A puede hacer ping a la dirección IP del PC B.
- Lance tcpdump o wireshark en PC A y PC B y vea los paquetes ICMP del ping.

Llegado este punto volvemos a tener las dos máquinas en la misma LAN y no se aprecia diferencia. Para ver la diferencia con la configuración anterior haga lo siguiente:

- Conecte el PC C en el mismo bloque de 8 puertos que están el PC A y el PC B.
- Asigne al PC C la dirección IP `10.3.armario.3` con máscara `255.255.255.0`
- Compruebe que puede hacer ping dese el PC C al PC B y al PC A.
- Detenga ese ping.
- Lance un ping entre PC A y PC B.
- Lance un `tcpdump` en PC C.
- ¿Puede ver los paquetes IP entre PC A y PC B? ¿Por qué?

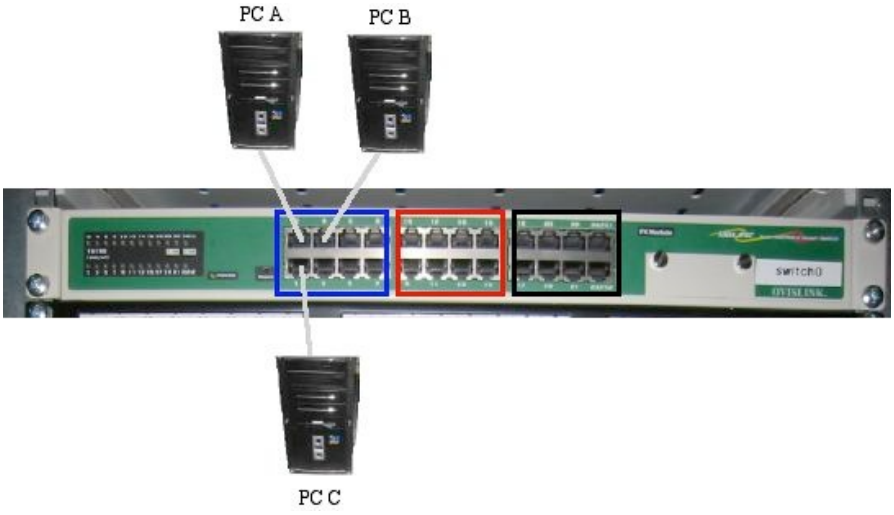

Figura 2.- Conexión de PCs a switch

A continuación vamos a extender nuestra LAN con un hub. Para ello:

- Conecte mediante un cable cruzado uno de los primeros 8 puertos de switch0 a uno de los 8 puertos del hub del panel de parcheo.
- Conecte PC B a otro de los puertos de ese hub.
- Teniendo PC C conectado a switch0 ¿Puede ver con tcpdump los paquetes de ICMP entre PC A y PC B?
- Conecte PC C al hub donde está PC B. ¿Ahora puede ver los paquetes? ¿Por qué?

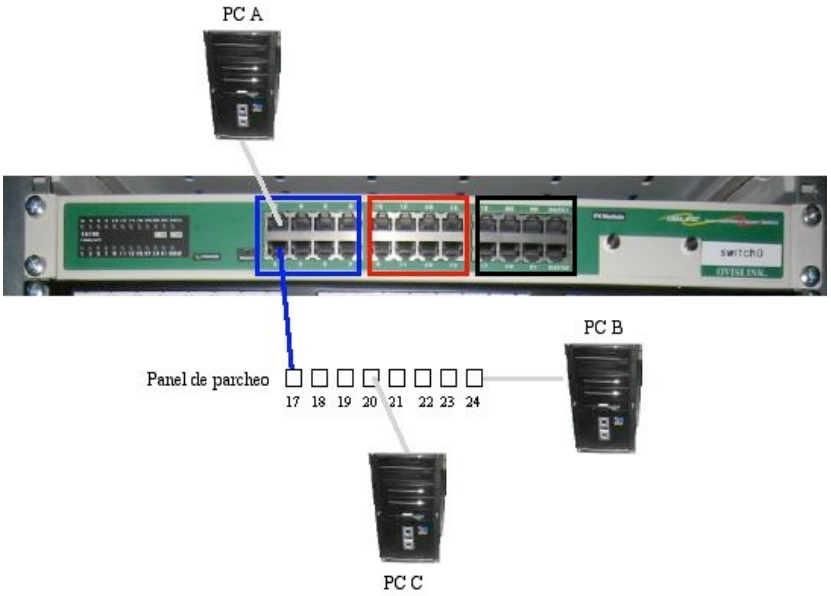

Figura 3.- Conexión de PCs a switch y Hub

Checkpoint 1.5: Muestre al responsable de prácticas esta última configuración.

8.- Router de acceso

A continuación vamos a configurar uno de los PCs para que pueda acceder a la red del Laboratorio de Telemática. Para ello se ha dispuesto un router que interconecta una LAN dedicada para las prácticas de esta asignatura con la LAN del laboratorio. Cada puesto de prácticas tiene un punto de red colocado en la LAN de la asignatura, que es el punto C de su mesa. Todos estos puntos C van a un conmutador Ethernet al cual también está conectado un router. Con otro de sus interfaces este router se conecta a la red del laboratorio. En el interfaz conectado a la red de esta asignatura tiene la dirección IP `10.3.16.1`

Procedan de la siguiente forma:

- Escojan uno de los puntos externos del armario, cables etiquetados de R9 a R12, y conéctenlo al punto C de su puesto de prácticas. Si, por ejemplo, han conectado el cable R9 eso quiere decir que ahora en la primera fila de su panel de parcheo, en el punto R9, tienen un punto de red del conmutador de la LAN de prácticas.
- Conecten ese punto con el punto del panel de parcheo correspondiente al interfaz eth0 del PC A. ¿Qué necesitarán, un cable recto o uno cruzado? ¿Por qué?
- Configure en PC A la IP `10.3.17.armario/20`
- Denle un tiempo (aproximadamente 1min) al conmutador para que descubra que tiene un nuevo ordenador conectado.
- Prueben a hacerle ping a la IP del router (`10.3.16.1`).

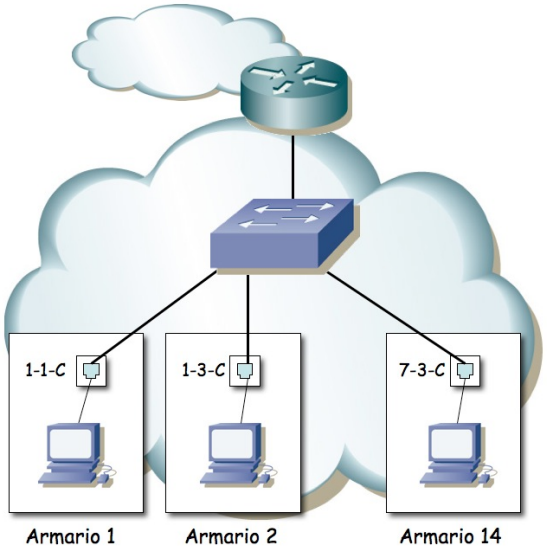

Figura 4.- LAN de prácticas

Ahora ya podemos acceder al router y de hecho debería poder acceder al PC A de cualquiera de sus compañeros de prácticas que hayan alcanzado este punto. Sin embargo, para poder conectarse a otras LANs, como por ejemplo la del laboratorio, hemos de indicarle al PC cuál es el router que debe emplear para salir de ella. Para ello vamos a introducir lo que se llama una ruta por defecto, es decir, una ruta o regla que indica a dónde enviar todo el tráfico IP que no se sabe hacer llegar a su destino de otra forma. En nuestro caso el único tráfico que sabemos hacer llegar a su destino es el dirigido a máquinas de nuestra misma red.

- Compruebe que desde PC A no puede hacer ping a la máquina `10.1.1.193` que se encuentra en la red del laboratorio. También puede probar con su PC SC que tendrá una dirección de tipo `10.1.1.x` o con la dirección IP `8.8.8.8` que es de google
- Consulte el manual del comando route. Averigüe cómo añadir una ruta por defecto (default gateway). La página del manual trae ejemplos.
- Introduzca la ruta por defecto empleando el comando route. Dicha ruta debe tener como gateway a la dirección `10.3.16.1`
- Compruebe que puede hacer ahora ping a la máquina `10.1.1.193` que se encuentra en la red del laboratorio.

Checkpoint 1.6: Muestre al responsable de prácticas que pueden comunicarse con máquinas de la red del laboratorio

9.- Navegando [opcional]

Para finalizar esta práctica vamos a configurar el PC A para que pueda acceder a la Web.

- Compruebe que puede hacer ping al servidor de nombres del laboratorio desde el PC A, que tiene la IP `10.1.1.193` (para esto debe haber completado correctamente el apartado anterior). Si eso le funciona probablemente también sea capaz de enviar paquetes IP con Internet y lo único que le falta es poder resolver nombres DNS.
- Configure la dirección del servidor de nombres (DNS) que va a usar el PC A. Para ello edite el fichero `/etc/resolv.conf` añadiendo una línea que ponga `nameserver 10.1.1.193`.
- Abra el navegador (mozilla).
- Compruebe que ahora puede navegar por Internet

Checkpoint 1.7: Muestre al responsable de prácticas que pueden navegar por Internet desde PC A

Tras completar este checkpoint por favor borren las líneas que han añadido al fichero `/etc/resolv.conf`