PRÁCTICA 1

Configuración básica de red en un PC

1 Introducción

Ésta es la primera práctica sobre los armarios de comunicaciones del laboratorio, por lo que servirá inicialmente para familiarizarse con el equipamiento disponible. Se pretende aprender a configurar el interfaz de red de un ordenador sobre Linux para que éste disponga de conectividad en una red de área local.

En esta práctica se revisarán los comandos y ficheros básicos para configurar un interfaz de red Ethernet con IP en Linux. Se emplearán elementos típicos de redes Ethernet como son los concentradores (hubs) y los conmutadores (switches). También se analizará, mediante las aplicaciones tcpdump y wireshark, el tráfico generado entre PCs con el objeto de detectar fallos de configuración o problemas de conectividad.

2 Material

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

- 3x PCs
- 2x Hub Ethernet
- 1x Switch Ethernet
- Cables categoría 5

3 Consideraciones generales sobre los armarios

- Toda la información técnica sobre los armarios se encuentra disponible en la portada de la web de telemática http://www.tlm.unavarra.es donde dice “Información sobre el laboratorio de Telemática”. Por favor, dedique unos minutos a revisarla antes de la sesión de prácticas.

- Cada armario dispone de varios ordenadores con Linux etiquetados como *PC A*, *PC B*, *PC C* y *PC SC*. Se pueden seleccionar mediante el conmutador de teclado y pantalla disponible: pulsando 2 veces la tecla de `BloqueoDesplazamiento` obtendrá el menú del conmutador.

- El *PC SC*, (PC de consola) está conectado a la red del resto de ordenadores del laboratorio y utiliza el sistema de cuentas central de los laboratorios de telemática. A cada estudiante se le habrá asignado una cuenta del tipo *roXX* (*recuerde cambiar la*

contraseña de esa cuenta con el comando passwd) que le permite hacer login en éste ordenador y guardar en su directorio la información que desee de forma privada. Desde este ordenador es posible configurar vía puerto serie los dispositivos de red del armario.

- Los PCs *A*, *B* y *C* se usan en las maquetas de red que se monten en los armarios. Para estos ordenadores hay una cuenta común para la asignatura con nombre de usuario *gro* y contraseña *telemat*. Al ser una cuenta común no puede confiar en que le borren ficheros o accedan a sus datos por lo que se recomienda que no guarde información en dichos equipos y que utilice por ejemplo un pendrive para guardar lo que le interese, por ejemplo, de una sesión de prácticas para la siguiente. 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.

4 Configuración manual de IP sobre el interfaz Ethernet

Los PCs A, B y C disponen cada uno de 4 tarjetas Ethernet. Analizaremos previamente dichos interfaces sobre el PCA.

4.1. Lea la página del manual del comando `ifconfig` con el comando `man ifconfig`. 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.

4.2. 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.

4.3. 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.

4.4. 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

4.5. Haga lo mismo con el primer interfaz del PC B

4.6. Busque en la página del manual del comando `ifconfig` cómo configurar la dirección IP de un interfaz

4.7. 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`

4.8. El comando `ping IPdestino` permite mandar un paquete ICMP Echo Request a esa IP destinio la cual si lo recibe está obligada a contestar con ICMP Echo Reply. Interprete la salida del ping consultando el manual del comando ping. Compruebe que el PC A puede hacer ping a su propia dirección IP. ¿Circulan estos paquetes realmente por la red?

4.9. Configure el interfaz `eth0` del PC B para que su dirección IP sea `10.3.`armario`.2` donde debe substituir armario por el número del armario donde realiza las prácticas. Emplee como máscara de red `255.255.255.0`

4.10. Compruebe que el PC B puede hacer ping a su propia dirección IP

4.11. Compruebe que el PC A puede hacer ping a la dirección IP del PC B

4.12. Compruebe que el PC B puede hacer ping a la dirección IP del PC A ¿Es necesaria esta prueba habiendo hecho la anterior?

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:

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

5.2 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:

5.3 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).

5.4 Para variar, 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 menún *Capture* escoja la opción *Start...*, asegúrese de que va a leer del interfaz correcto (`eth0`) y déle al botón de OK. Debería ver en una ventana cómo `wireshark` está recogiendo paquetes de diferentes tipos, cuando vea que tiene varios de tipo ICMP déle al botón *Stop*.

5.5 Identifique los campos de las cabeceras de protocolos Ethernet e IP de esos paquetes ICMP gracias a la decodificación de sus campos ofrecida por `wireshark`. ¿Es capaz de identificar el número de secuencia IP? ¿Cuál es el tamaño de datos encapsulados por encima de IP?

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, ¿Qué ocurre si intentamos ver el tráfico entre A y B desde otra máquina? Para ver esto siga los siguientes pasos:

5.6 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

5.7 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
```

5.8 Ejecute en PC C el programa `tcpdump` y vea los paquetes IP del ping entre PC A y PC B ¿Por qué C es capaz de ver los paquetes intercambiados entre A y B?

6 Cascada de hubs Ethernet

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:

6.1 Mantenga el ping del apartado anterior en ejecución.

6.2 Enchufe el segundo hub en la regleta que tiene en la parte frontal del armario.

6.3 Conecte el puerto 8X del segundo Hub mediante un cable recto a uno de los puertos del Hub del panel de parcheo.

6.4 Desconecte el PC A del panel de parcheo y conéctelo al otro hub.

6.5 Compruebe que sigue funcionando el ping.

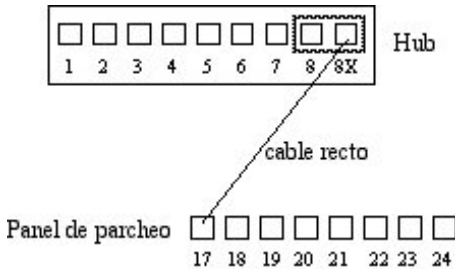

Figura 1.- Conexión de dos hubs

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

6.6 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.

6.7 Conecte el PC C en el segundo hub en vez del primero.

6.8 ¿Puede ver desde PC C (en otro hub) los paquetes que se mandan PC A y PC B?

7 Switches 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 rendimiendo de la LAN empleando puentes o conmutadores (switches). En el armario cuentan con dos conmutadores. A continuación vamos a probar a crear una LAN emplando el switch0.

Manteniendo la configuración IP de los interfaces de red:

7.1 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 si un conmutador independiente.

7.2 Haga lo mismo con el primer interfaz del PC B.

7.3 Compruebe que el PC A puede hacer ping a la dirección IP del PC B.

7.4 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:

7.5 Conecte el PC C en el mismo bloque de 8 puertos que están el PC A y el PC B.

7.6 Asigne al PC C la dirección IP `10.3.armario.3` con máscara `255.255.255.0`

7.7 Compruebe que puede hacer ping dese el PC C al PC B y al PC A.

7.8 Detenga ese ping.

7.9 Lance un ping entre PC A y PC B.

7.10 Lance un `tcpdump` en PC C.

7.11 ¿Puede ver los paquetes IP entre PC A y PC B? ¿Por qué?

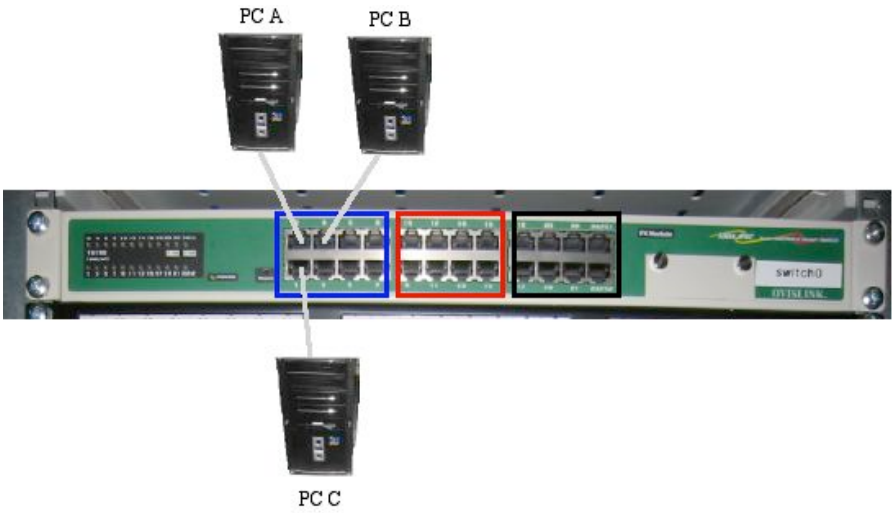

Figura 2.- Conexión de PCs a switch

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

7.12 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.

7.13 Conecte PC B a otro de los puertos de ese hub.

7.14 Teniendo PC C conectado a switch0 ¿puede ver con tcpdump los paquetes de ICMP entre PC A y PC B?

7.15 Conecte PC C al hub donde está PC B. ¿Ahora puede ver los paquetes? ¿Por qué?

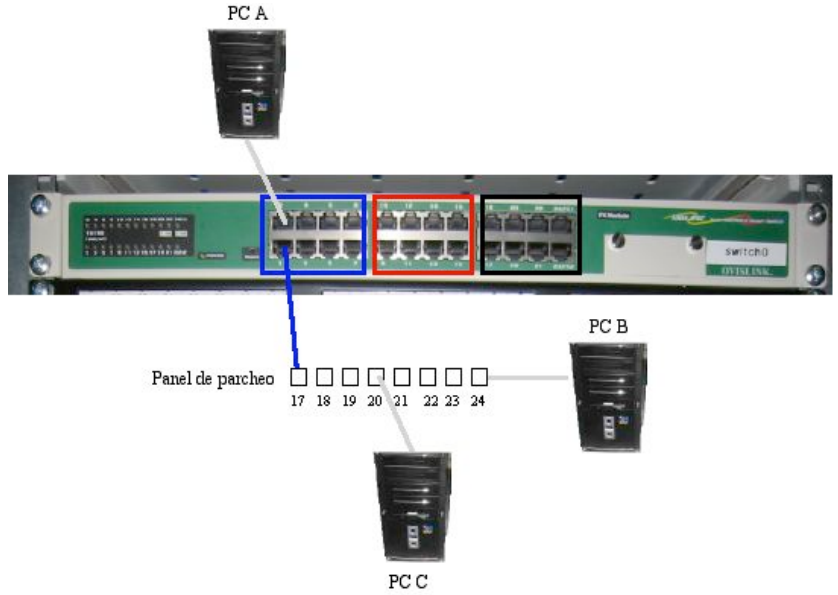

Figura 3.- Conexión de PCs a switch y hub