

Repaso: Configuración de interfaces IP en equipos con sistema operativo GNU/Linux

1- Objetivos

Para probar las configuraciones de redes necesitaremos PCs que colocaremos en las diferentes LANs. Por ello en esta práctica repasaremos los comandos básicos para configurar un interfaz de red Ethernet con IP en Linux y conectarlo a una LAN con un router de acceso. Igualmente, una técnica básica para el *troubleshooting* en redes es la captura y análisis de tráfico, por ello se verá el procedimiento básico para el mismo empleando sniffers en Linux.

2- Material necesario

- 4 cables rectos UTP (cortos)
- Un hub Ethernet
- 3 PCs
- 1 switch con VLANs

3- Conocimientos previos

Es necesario un conocimiento básico sobre IP: direcciones, redes y subredes, máscaras de red, tablas de rutas, ICMP (ping)...

Esta es una prácticas de repaso para todo aquel que haya cursado *Redes de Ordenadores*.

4- Configuración manual de IP sobre el interfaz Ethernet

Los PCs A, B y C disponen cada uno de 4 interfaces Ethernet. Analizaremos previamente dichos interfaces. Para loguearse en estos PCs use el usuario `ftpr` con password `telemat`.

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 solo 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 los interfaces Ethernet aunque no estén configurados, siempre que hayan sido detectadas por el sistema operativo.

Averigüe la dirección MAC (o dirección hardware) de cada uno de los interfaces Ethernet 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 siga el siguiente esquema:
`00001010 . 00000011 . 0000 ABCD . 00000001 /24`

Donde ABCD representa el número de armario en que está realizando prácticas. Es decir `10.3.armario.1`.

- 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.2/24` donde debe substituir “armario” por el número del armario donde realiza las prácticas.
- 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

5- Viendo el tráfico con `tcpdump` y `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 el manual de `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 solo 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 solo 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).
- 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 muestra de forma que solo se vean los paquetes ICMP. Para ello en la casilla de texto junto al botón *Filter* escriba “icmp”. En el menú *Capture* escoja la opción *Start...*, asegúrese de que va a leer del interfaz correcto (probablemente `eth0`) y dele 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 dele al botón “Stop”.

- Analice el contenido de esos paquetes ICMP gracias a la decodificación de sus campos ofrecida por `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 al mismo Hub o concentrador Ethernet cualquier otra máquina que conectemos al mismo debería ser capaz de ver esos paquetes siempre que configure su interfaz 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

6- Acceso al laboratorio

A continuación vamos a configurar uno de los PCs para que pueda acceder a la red del Laboratorio de Telemática (Fig. 1). 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. 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 y conéctenlo al punto C de su puesto de prácticas. Si por ejemplo han escogido el R-9 eso quiere decir que ahora en la primera fila de su panel de parcheo, en el punto 9, 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 tienen un nuevo ordenador conectado (más adelante veremos que este tiempo es debido a la configuración del Spanning Tree Protocol)
- Prueben a hacerle ping a la IP del router (`10.3.16.1`)

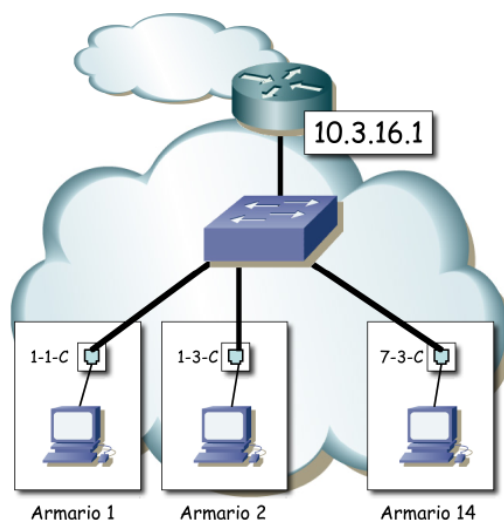


Figura 1: LAN de prácticas

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 comunicarse con otras LANs, como por ejemplo la del laboratorio, hemos de indicarle al PC cuál es el router que debe emplear como intermediario. 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 ahora mismo el PC sabe hacer llegar a su destino es el dirigido a máquinas de su misma red.

- Compruebe que desde PC A no puede hacer ping a la máquina 10.1.1.230 que se encuentra en la red del laboratorio.
- 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 10.1.1.230 que se encuentra en la red del laboratorio.

Para poder acceder a recursos mediante nombres de dominios necesita configurar el servidor DNS del PC. Prueba a hacer ping o acceder mediante el navegador a un nombre de dominio. ¿Puede?

Mire si el fichero `/etc/resolv.conf` tiene una línea especificando el servidor DNS, sino la tiene añada una con `nameserver 10.1.1.193`. Prueba ahora. A continuación borre esa línea para dejar el fichero tal cual estaba.

7- PC como router IP

Vamos a emplear el PC C como router IP. Nuestro primer objetivo es crear una topología como la de la figura 2.

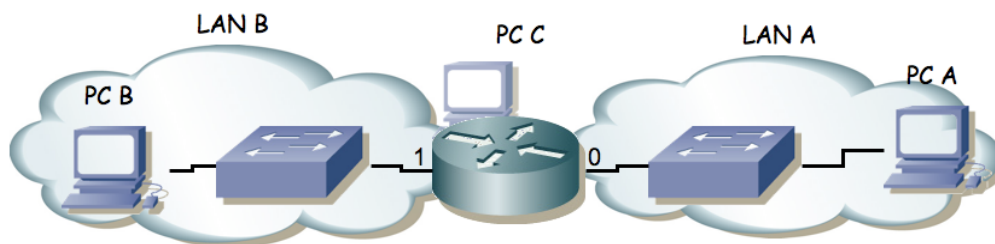


Figura 2.- Router conectado a dos redes

Para ello:

- Dividan su espacio de direcciones (`10.3.armario.0/24`) en al menos dos bloques que no se solapen.
- Configuren las IPs de los dos primeros interfaces ethernet del PC C para que cada uno esté en una de esas redes.
- Configuren un interfaz de PC A para que tenga dirección IP de la Red A y un interfaz del PC B para que la tenga de la Red B.
- Conecten el interfaz del PC C con IP en la Red A en un conmutador (switch0 funciona como 3 conmutadores independientes) y ahí también el PC A.
- Conecten el otro interfaz del PC C en otro conmutador.
- Conecten ahí el PC B.
- Configuren la ruta por defecto de cada PC para que cada uno la tenga haciendo referencia al interfaz del PC C conectado en su misma red.
- Prueben a hacer ping desde el PC C a PC A y PC B.
- Prueben a hacer ping desde PC A a PC C y desde PC B a PC C.
- Prueben a hacer ping desde PC A a PC B. ¿Qué sucede?
- Empleen `wireshark` para averiguar qué es lo que está fallando

El PC C tiene ahora dos interfaces IP en funcionamiento. Tal y como está, se dice que este PC está *multihomed* porque tiene interfaces en redes diferentes. Ahora mismo, si recibe por uno de sus interfaces un paquete que se dirige a una IP destino que no es ninguna de las suyas lo descarta. Para que funcione como un router tenemos que convencerle de que cuando reciba un paquete con esas características no lo tire sino que lo reenvíe aplicando las reglas que tiene en su tabla de rutas. Esta funcionalidad es lo que se conoce como *IP forwarding* o reenvío de paquetes IP. Si el kernel tiene compilada esta funcionalidad (y en nuestro caso la tiene) podemos activarla sin más que escribir un `1` en el fichero `/proc/sys/net/ipv4/ip_forward` (recuerde que en Linux los ficheros en `/proc` en realidad hacen referencias a variables dentro del kernel), o equivalentemente empleando el comando `sysctl` para modificar esa variable del kernel.

Ambas acciones requieren privilegios de superusuario. Para resolver el problemas se les ha dejado un programa muy simple que tan solo ejecuta un comando `sysctl` para activar o desactivar el forwarding según se le indique.

Para activarlo:

```
%> sudo /usr/local/sbin/forwarding si
```

Para desactivarlo:

```
%> sudo /usr/local/sbin/forwarding no
```

Y pueden ver el comando que se está ejecutando porque lo muestra por pantalla.

Con solo activar el forwarding el PC empezará a reenviar paquetes. También se podría activar esta

funcionalidad para que reenviara paquetes solo entre ciertos interfaces, lo cual sería útil si tuviéramos más de dos y no quisiéramos que reenviará entre todos ellos (ficheros `/proc/sys/net/ipv4/conf/*/forwarding`).

Y ya está. El PC ya se comporta como un router. Si activáramos más interfaces (Ethernet, PPP, WLAN, etc) podría reenviar tráfico entre todos ellos. De hecho esta es una solución bastante barata para tener un router. Coloque ahora un `wireshark` o `tcpdump` en el servidor y observe que sí reenvía los paquetes ICMP.

Una vez que el PC funciona como un router debemos mirar con más cuidado el contenido de su tabla de rutas dado que ahora no solo la empleará para todos los paquetes que él quiera enviar sino también para todos los que decida reenviar.

Repaso: Configuración básica de routers Cisco

1- Objetivos

En esta práctica veremos los métodos básicos de acceso a un equipo con Cisco IOS, cómo configurar las direcciones IP de interfaces Ethernet y Serie de routers Cisco, su tabla de rutas y el acceso por telnet al mismo.

2- Material necesario

- 2 routers Cisco 1721 (2 interfaces Ethernet e interfaces Serie)
- 3 PCs
- 7 cables rectos
- Un hub Ethernet
- Dos switch Ethernet (o uno con VLANs)

3- Conocimientos previos

Es necesario un conocimiento básico sobre IP: direcciones, redes y subredes, máscaras de red, tablas de rutas, ICMP (ping)...

Esta es una prácticas de repaso para todo aquel que haya cursado *Redes de Ordenadores*.

4- Acceso al router a través del puerto de consola

Cada grupo de prácticas dispone de tres routers Cisco. Consulten la documentación de los armarios. Verán que el servidor de consola tiene un cable desde el puerto serie al puerto de consola de cada uno de ellos (y tiene varios puertos serie). Estos cables tienen por un extremo un conector DB9 y es el conectado al PC. El otro extremo, que pueden ver en los routers, es un conector RJ45 (sigue siendo una conexión serie, NO es Ethernet) (Fig. 1).

- Apaguen el router2 (con el interruptor de alimentación)
- Ejecuten la aplicación `minicom` en el PC-SC para que abra el puerto serie que le comunica con el router2. La comunicación debe ser a 9600 bps, 8 bits de datos, 1 de parada, sin paridad, comprueben que el puerto está bien configurado.
- Ahora enciendan el router. Deberían poder ver el proceso de arranque del mismo.

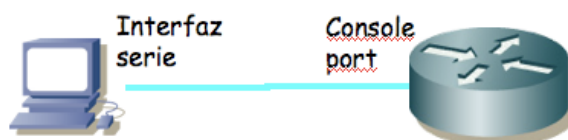


Figura 1.- Conexión al puerto de consola

La primera configuración del router es necesario hacerla a través de este puerto de consola dado que al no tener el router aún una configuración de red no podemos acceder a él por ninguno de sus interfaces de red.

El Cisco IOS CLI ofrece diferentes modos de comandos. Cada modo de comandos ofrece un conjunto de comandos diferentes y con diferente objetivo (configuración, mantenimiento, monitorización...). Los comandos disponibles en cada momento dependen del modo en el cual se encuentre el usuario. En cualquiera de estos modos se puede emplear el interrogante (?) para obtener una lista de los comandos disponibles en ese modo.

Lo mejor es que se acostumbre a la documentación oficial de Cisco. En el siguiente URL tiene una introducción a los diferentes modos existentes:

http://www.cisco.com/en/US/docs/ios/11_0/router/configuration/guide/cui.html

Lea de la sección *Understanding the User Interface* de dicho documento las subsecciones: *Understanding the User Interface*, *User EXEC Mode*, *Privileged EXEC Mode*, *Global Configuration Mode* e *Interface Configuration Mode* (en total unas 5 páginas). Explica las diferencias entre los modos, cómo cambiar de uno a otro y cómo ver la ayuda en línea disponible.

Al finalizar el arranque del router seguramente se encontrarán (a través de minicom) con algo como:

```
Router>
```

Este es el prompt de CLI (en este caso con el nombre del router). En este punto estamos en modo de comandos de usuario (User EXEC Mode) que es el de menos privilegios y con el que no vamos a poder cambiar la configuración del router.

Puede ver los comandos disponibles desde este modo con el interrogante:

```
Router> ?
```

```
Exec commands:
```

```
<1-99>          Session number to resume
access-enable    Create a temporary Access-List entry
access-profile   Apply user-profile to interface
clear            Reset functions
connect          Open a terminal connection
disable          Turn off privileged commands
disconnect       Disconnect an existing network connection
enable           Turn on privileged commands
```

...

Podemos obtener ayuda de cada comando e incluso de las opciones del comando terminándolo con un interrogante. Por ejemplo:

```
Router> show ?
```

```
backup          Backup status
clock           Display the system clock
compress        Show compression statistics
dialer          Dialer parameters and statistics
flash:          display information about flash: file system
history         Display the session command history
hosts           IP domain-name, lookup style, nameservers, and host table
location        Display the system location
modemcap        Show Modem Capabilities database
ppp             PPP parameters and statistics
rmon            rmon statistics
rtr             Response Time Reporter (RTR)
sessions        Information about Telnet connections
snmp            snmp statistics
tacacs          Shows tacacs+ server statistics
terminal        Display terminal configuration parameters
traffic-shape   traffic rate shaping configuration
users           Display information about terminal lines
version         System hardware and software status
```

Podemos ver la versión del sistema operativo y el hardware disponible (RAM, interfaces...) mediante el comando `show version`.

- ¿Qué versión del sistema operativo tiene su router?
- ¿Cuánta RAM tiene instalada?
- ¿De cuántos interfaces dispone su router?
- ¿De qué tipo son? Identifíquelos físicamente en el router.

Con el comando `show interfaces` pueden ver los interfaces de red de los que dispone el router y muchas características de estos. Averigüe la dirección MAC de cada uno de sus interfaces Ethernet. Averigüe cómo ver los ficheros que existen en la flash con el comando `show`. Podemos acceder a información referente a IP con las opciones de `show ip` (vea un poco las opciones existentes). Por ejemplo podemos ver información referente a IP de cada interfaz con `show ip interface`, especificar un solo interfaz u obtener información muy resumida de la configuración ip de los interfaces (pruebe `show ip interface brief`). También podemos ver la tabla de rutas con `show ip route`. Lo más probable es que ahora vea que ningún interfaz tiene asignada dirección IP y que no hay ninguna entrada en la tabla de rutas. Podremos remedio a todo esto en breve.

5- Configuración IP básica de un interfaz Ethernet del router

Para hacer cualquier cambio en la configuración del router lo primero que debemos hacer es pasar al modo de comandos privilegiado (*privileged EXEC mode*). Para ello ejecute:

```
Router> enable
```

En este punto el router podría (y debería) solicitar una password. De momento esa password está quitada. Si el comando se ejecuta con éxito el prompt debería cambiar a algo como:

```
Router#
```

para indicarnos que estamos en modo privilegiado.

Si ahora pide de nuevo ayuda (?) podrá ver que hay un nuevo conjunto de comandos disponible. Por ejemplo, pruebe el comando `reload` que sirve para reiniciar el router y aprenda a programar que el router se reinicie dentro de 1 minuto. Aproveche para ver de nuevo los mensajes del arranque del router.

Tras terminar el reinicio vuelva a entrar en modo privilegiado. De ahí pasamos al modo de configuración con el comando:

```
Router# configure terminal
```

Si pide ayuda de nuevo verá otro conjunto de comandos. Lo primero que vamos a hacer es activar que el equipo actúe como un router. Para ello emplearemos el comando `ip`. Vea las opciones de este comando con:

```
Router(config)# ip ?
```

Lo activamos escribiendo:

```
Router(config)# ip routing
```

Nota: Muchos alumnos se acostumbran a escribir este comando (y otros) cada vez que entran en modo configuración. Esto no es en absoluto necesario. Una vez que activemos el reenvío de paquetes se queda activado (salvo que lo desactivemos expresamente o rebotemos y no hayamos guardado la configuración), al igual que con los demás comandos (como por ejemplo activar un interfaz).

A continuación vamos configurar la dirección IP de uno de los interfaces Ethernet. Para ello hemos de pasar al modo de configuración de ese interfaz. Esto se hace con el comando `interface` especificando a continuación el nombre del interfaz (recuerde que siempre puede usar ? para pedir ayuda). Entre en modo configuración del interfaz FastEthernet de su router. El prompt debería ser ahora:

```
Router(config-if)#
```

Una vez en este modo primero le indicamos al IOS que active el interfaz con:

```
Router(config-if)# no shutdown
```

A continuación especificamos la dirección IP del interfaz empleando el comando `ip`. Investigue las opciones del comando lo suficiente para darle a ese interfaz la dirección IP `10.3.armario.1` con

máscara 255.255.255.0.

Conecte ese interfaz del router al hub (si el interfaz no está conectado a ningún dispositivo entonces el Cisco IOS lo desactiva) (Fig. 2). Vuelva al modo usuario y revise la configuración IP de los interfaces. Debe aparecer *up* tanto en la columna *Status* como en la columna *Protocol* de un interfaz para que este reenvíe paquetes. Revise también la tabla de rutas. Ahora debería ver una ruta a la red a la que está conectado ese interfaz.

Conecte uno de los interfaces Ethernet del PC A al mismo hub y configúrele la dirección 10.3.armario.2 con máscara 255.255.255.0. Ahora debería poder hacer ping a ese interfaz del router desde el PC.

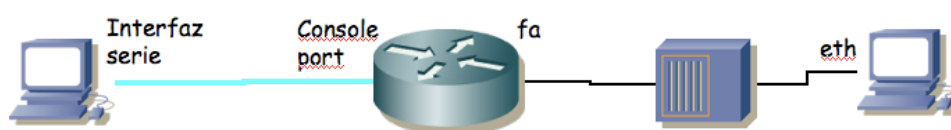


Figura 2.- Conexión a hub

6- Interfaces serie

Los routers se pueden emplear para conectar tanto LANs como WANs, así que suelen tener disponibles interfaces de ambos tipos. A los efectos de nuestros interfaces de red una WAN opera a nivel físico y de enlace y nos permite interconectar LANs.

Generalmente los enlaces WAN utilizan servicios de operadoras (carriers) de comunicaciones, ofreciendo conectividad a nivel de enlace entre los dos extremos. El router (DTE, Data Terminal Equipment) se conecta a la WAN a través de un DCE (Data Communication Equipment) (Fig. 3).

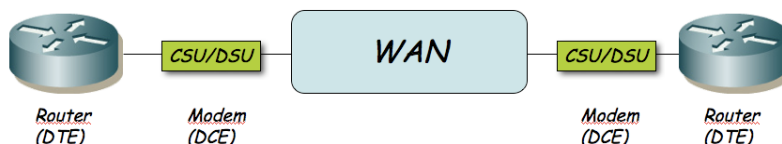


Figura 3.- Routers conectados por un enlace WAN

El DTE se conecta al DCE con un Cable DTE. El conector libre de un cable DTE (en nuestro caso un V.35) normalmente es macho. El DCE ofrece un conector hembra. El router Cisco puede actuar tanto como DTE o como DCE. En las prácticas no vamos a emplear unidades CSU/DSU para conectar los routers entre sí a través de los interfaces WAN serie. Lo que vamos a hacer es conectarlos con un cable tipo *NULL modem*. Para ello juntaremos dos cables, uno un cable DTE y el otro un cable DCE (Fig. 4). El cable DCE tienen un extremo V.35 hembra. Posteriormente, en la configuración de los dos routers, deberemos configurar que uno de ellos actúe como DCE.

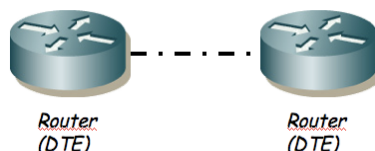


Figura 4.- Routers conectados por cable NULL modem

Las tarjetas WAN de los routers de los que disponen tienen dos puertos serie cada una. Tienen ya conectados cables DTE y DCE.

- Conecten uno de los puertos serie de router2 con uno de router3

Uno de los dos extremos actuará como el DTE y el otro como el DCE, según el cable que le hayamos conectado. La diferencia principal es que normalmente el DCE genera la señal de sincronismo necesaria en el cable.

- Entren en modo de configuración de cada interfaz serie que hayan conectado y asignen una dirección IP y una máscara de red a ese interfaz (empleen a su gusto la red asignada a su armario: 10.3.armario.0/24)
- En el router que vaya a ser el DCE (el del cable de conector V.35 hembra) deben especificar la velocidad a la que se empleará la línea serie (comando `clock rate`). Los interfaces serie de estos routers son de baja velocidad y normalmente estarán limitados en torno a unos 100-120Kbps.
- Y por supuesto activen los interfaces

Con esto deberían poder hacer ping desde un router al otro a través de la línea serie. La línea serie estará empleando como nivel de enlace el encapsulado HDLC. Se puede configurar para que se emplee otro encapsulado como por ejemplo PPP.

- A continuación conecten uno de los interfaces Ethernet de cada router a un conmutador diferente del switch0 (Fig. 5)
- Conecten un PC a cada una de esas LANs
- Configuren 3 redes: una para cada LAN y una tercera para el enlace serie, empleando el espacio de direcciones que tienen asignado
- Configuren en cada PC la dirección IP y el router por defecto. El comando para añadir rutas en el Cisco IOS es (en modo configuración) `ip route`
- Configuren en cada router una ruta por defecto al otro router por el interfaz serie
- Prueben a hacer ping entre los PCs
- Prueben a cambiar la velocidad del enlace serie y vean cómo cambia el retardo indicado por el ping



Figura 5.- Topología en serie

7- Acceso al router a través de telnet

Ahora podemos hacer también un telnet desde el PC al router por el interfaz IP, sin embargo, para poder conectarnos al mismo antes hay que asignar una password para las conexiones que vienen por la red. Para ello, de nuevo desde el minicom entre en modo privilegiado y en modo configuración. Desde ahí pasamos al modo de configuración de líneas por ejemplo con:

```
Router(config)# line vty 0 4
```

Y ahora activamos que se pueda hacer login y asignamos una password:

```
Router(config-line)# login
```

```
Router(config-line)# password invitado
```

Ahora la password que tiene el router para las conexiones del servicio telnet es "invitado". Pruebe ahora a hacer un telnet al router y entrar con esa password (no hay nombre de usuario). Verá que entra en modo usuario, para pasar a modo privilegiado tiene que ejecutar el comando `enable` pero este comando le dará un error porque no hay una password asignada para pasar a modo privilegiado (antes nos permitía cambiar de modo aunque no había password porque estábamos accediendo desde el puerto de consola). No vamos a asignar una password de `enable` para no dificultar la realización de prácticas de otros estudiantes. La password se puede eliminar sin más que anular el `command` que la ha activado con un "no" delante pero por experiencia en ocasiones hay routers que quedan con una contraseña desconocida puesta y no se puede volver a trabajar con ellos sin un

proceso lento de reinicio así que para estas prácticas **no configure una contraseña de enable**.
 ¿Podría conectar su interfaz Ethernet con el del router sin un hub?

8- Topología con 2 routers

A continuación vamos a crear la topología que se ve en la figura 6.

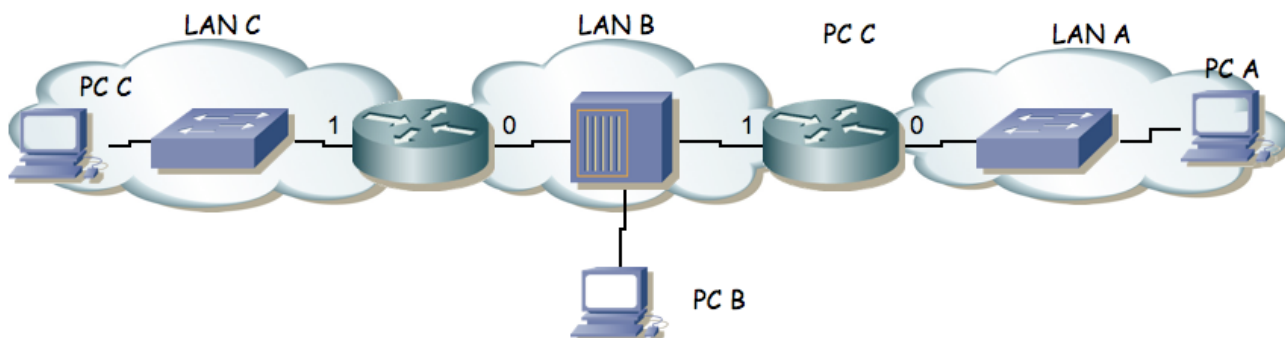


Figura 6.- 2 routers conectando 3 redes

Para ello emplearemos los routers router2 y router3.

- La red que tiene asignada el grupo de prácticas (10.3.armario.0/24) divídanla en al menos 3 redes que no se solapen.
- Configuren los interfaces de los routers para que tengan la dirección IP en la red que les corresponde.
- Configuren PC A, B y C para que cada uno esté conectado a una de las redes.
- Configuren la ruta por defecto de cada PC. Recuerde que debe apuntar a un router que esté en su misma red. Con el PC B tiene dos para elegir!
- Compruebe que cada PC puede comunicarse con otro que esté a un router de distancia pero los dos de los extremos (PC A y PC C) no pueden comunicarse entre si.
- Para resolver esto introduzcan una ruta por defecto en cada uno de los routers que tenga al otro router como siguiente salto. El comando para añadir rutas en el Cisco IOS es (en modo configuración) `ip route`
- ¿Ahora qué camino siguen los paquetes que van de la Red A a la Red C?
- Coloque un `tcpdump` o `wireshark` en PC B.
- ¿Puede ver los paquetes que van de PC A a PC C? ¿Y los que van de PC C a PC A?
- Si pone un ping entre PC A y PC C y ve los paquetes con wireshark en PC B ¿Qué direcciones IP origen y destino tienen? ¿Qué direcciones MAC tienen? ¿De qué interfaces son?
- ¿Qué camino siguen los paquetes que van de PC B a PC A? ¿Y los que van de PC B a PC C?

Uno de los campos de la cabecera de todos los paquetes IP es el TTL o *Time To Live*. El origen del paquete le da un valor y cada router que reenvía el paquete lo decrementa al menos en una unidad. Si un router va a reenviar un paquete y después de decrementar este campo de la cabecera el resultado es 0 o menos que 0 descarta el paquete sin reenviarlo. Podemos ver el valor de este campo de los paquetes IP con el programa `tcpdump` si le pedimos que saque más información de cada paquete. Pueden emplear para ello la opción `-v`.

- ¿Con qué valor de TTL generan estos PCs los paquetes IP normalmente?
- Vean cómo el TTL se decrementa al ser reenviado por cada uno de los routers

- En esta topología, ¿Qué valor mínimo de TTL se debe emplear para que todos los paquetes puedan llegar a su destino?

Ahora vamos a añadir unas rutas a las tablas de los Cisco. Para ello

- Consulten la ayuda del comando `ip route` en modo configuración con el que pueden añadir rutas estáticas a un router Cisco
- Añadan al router de la izquierda una ruta hacia la red A apuntando al otro router
- Añadan al router de la derecha una ruta hacia la red C apuntando al otro router
- Prueben a hacer ping entre todos los PCs

9- Gestión de configuración

Los cambios que hemos hecho hasta el momento en la configuración del router se perderán en el momento que lo reiniciemos. Para que los cambios sean permanentes lo que se hace es guardar la configuración actual con el nombre del fichero de configuración que lee en el arranque el router y que se encuentra en la NVRAM. En general en estas prácticas NO utilizaremos este commando, para evitar modificar la configuración en el arranque del router, dado que daría problemas al siguiente grupo de prácticas, que esperará una configuración “limpia”. Puede buscar en la documentación de Cisco cómo se haría este paso, si tiene interés. El nombre del fichero que carga en el arranque es “startup.config”.

Para ver la configuración que tiene en el momento actual el router puede ejecutar desde modo privilegiado:

```
Router# show running-config
```

Ahí están todos los comandos que se han ejecutado y están en efecto en este momento. Como se ha comentado, si en algún momento deseamos deshacer un comando lo único que hace falta es ejecutarlo de nuevo poniendo delante `no`. Por ejemplo, para desactivar el routing podríamos desde modo configuración:

```
Router(config)# no ip routing
```

En un escenario real es frecuente que la configuración total sea un fichero bastante grande, por lo que hay formas de visualizar solo partes del mismo. Para el tipo de escenarios que se configuran en estas prácticas es un ejercicio interesante y recomendado acostumbrarse a ver la configuración completa del router (o conmutador), la cual nunca es muy grande.