Práctica 2: Conmutadores LAN, Spanning Tree y VLANs

Autor: Rogelio Montañana

Objetivo y descripción general.

Esta práctica pretende familiarizar al alumno con la configuración y gestión de una red local basada en conmutadores LAN y redes locales virtuales (VLANs). Aunque los detalles concretos de cómo se realizan estas tareas dependen del equipo utilizado, los aspectos básicos son similares en todos los fabricantes.

La práctica simula el establecimiento de una red local que abarca dos edificios denominados Norte y Sur. En cada edificio se dispone de un conmutador, de un conjunto de ordenadores o hosts y de un router (utilizado únicamente en la segunda sesión).

La práctica se divide en dos sesiones, cada una de las cuales consta de 3 partes organizadas de la siguiente forma:

Sesión	Parte	Consiste en:
1	1.1	Conectarse al conmutador por la interfaz de consola, borrar la configuración existente y restaurar la de fábrica.
	1.2	Familiarizarse con el funcionamiento del conmutador y realizar pruebas básicas.
	1.3	Interconexión de ambos conmutadores y hacer pruebas con el Spanning Tree.
2	2.1	Crear dos VLANs y comunicarlas.
	2.2	Configurar un enlace 'trunk'.
	2.3	Interconectar las dos VLANs mediante routers

Para la realización de la práctica los alumnos se organizan en grupos, cada uno de los cuales utiliza una maqueta diferente. Cada maqueta esta formada por dos conmutadores que denominamos Norte y Sur en correspondencia con los edificios a los que supuestamente pertenecen. En las partes 1.1 y 1.2 los alumnos trabajan independientemente con el conmutador Norte o Sur. La parte 1.3 y toda la segunda sesión se desarrollan con los dos conmutadores interconectados. Las maquetas se mantienen independientes durante toda la práctica.

Los conmutadores utilizados son de la marca Cisco modelo Catalyst WS-C1924C-EN (figuras 1 y 2) que es uno de los varios modelos que forman la familia Catalyst 1900 (esta familia de conmutadores, actualmente obsoleta, estuvo a la venta entre 1998 y julio del 2002). Cada conmutador dispone por su parte delantera de 24 interfaces Ethernet de 10 Mb/s (10BASE-T) y dos interfaces Fast Ethernet, una 100BASE-FX y una 100BASE-TX. Además, por la parte trasera dispone de una interfaz Ethernet de 10 Mb/s con conector AUI (Attachment Unit Interface), que puede ser de cobre o fibra según el transceiver que se utilice. Las interfaces AUI y 100BASE-TX no se utilizan en esta práctica

Las interfaces 10BASE-T y 100BASE-FX pueden funcionar en modo half o full dúplex, pero no soportan autonegociación por lo que se han de configurar manualmente. El modo por defecto es half-duplex. Las interfaces de 100 Mb/s (100BASE-TX y 100BASE-FX) soportan autonegociación en el modo duplex (half o full) pero no en la velocidad, solo pueden funcionar a 100 Mb/s.

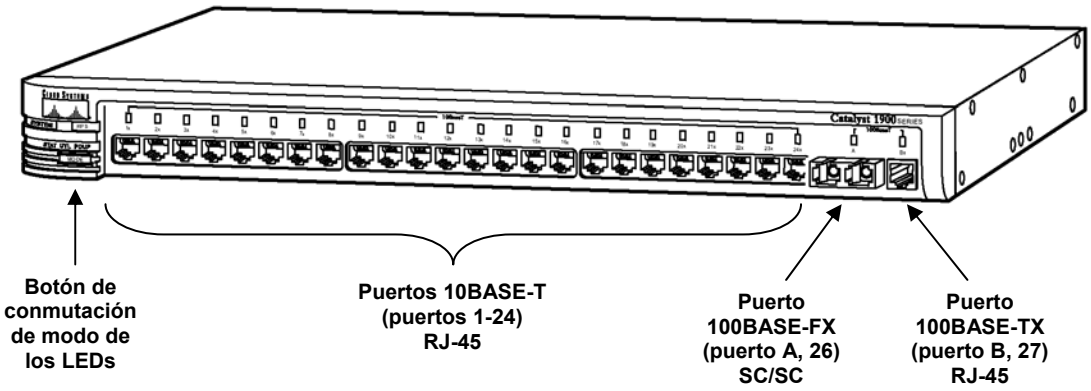

Figura 1: Vista frontal del Catalyst WS-C1924C-EN

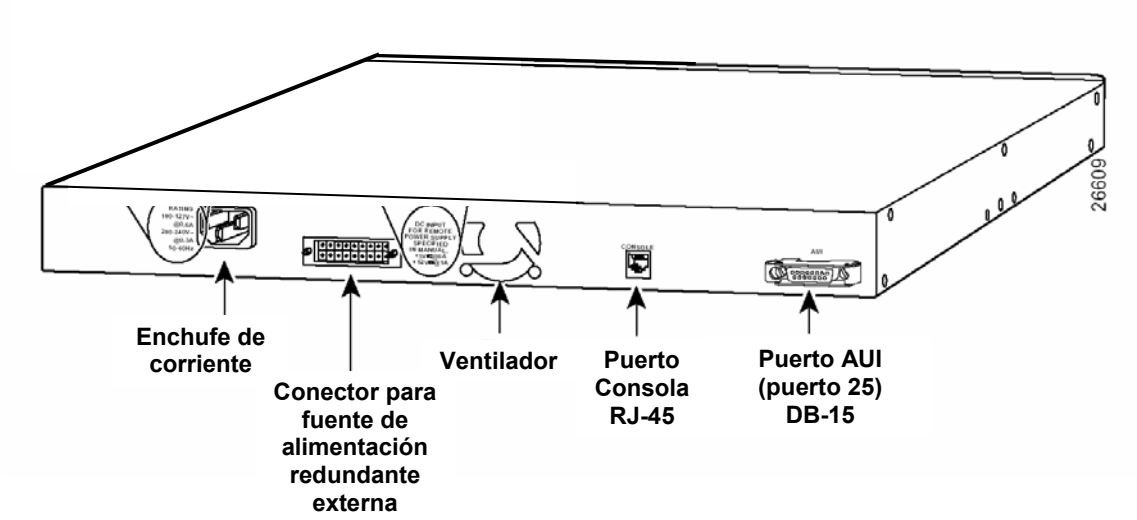

Figura 2: Vista trasera del Catalyst WS-C1924C-EN

Para el desarrollo de la práctica es fundamental conocer el nombre que reciben las interfaces en la configuración del equipo. En la tabla 1 se detallan estas denominaciones y como se corresponden con la etiqueta que aparece en el equipo.

Tipo de interfaz	Posición	Etiqueta exterior	Denominación en configuración
10BASE-T	Frontal	1x a 24x	Ethernet 0/1 a Ethernet 0/24
AUI	Trasera	AUI	Ethernet 0/25
100BASE-FX	Frontal	Ax	FastEthernet 0/26
100BASE-TX	Frontal	Bx	FastEthernet 0/27

Tabla 1. Denominación de interfaces en el Catalyst WS-C1924C-EN

Todas las interfaces con conector RJ-45 (10BASE-T y 100BASE-TX) incorporan internamente la función "crossover", es decir, el cruce de transmisión con recepción (de ahí la ‘x’ que aparece en la etiqueta). Esto permite conectar ordenadores utilizando latiguillos normales, no cruzados. Sin embargo cuando se interconectan entre sí dos conmutadores es preciso utilizar un latiguillo "crossover" para que la comunicación se establezca. En el caso de la interfaz en fibra 100BASE-FX (Ax) el usuario debe realizar el cruce entre transmisión y recepción cuando enchufa los conectores SC/SC para que la comunicación sea posible.

PRIMERA SESIÓN.

Parte 1.1: Conectarse al conmutador por la interfaz de consola, borrar la configuración existente y restaurar la de fábrica.

Interconectar los equipos y ponerlos en marcha

En primer lugar procederemos, con todos los equipos apagados, a realizar las conexiones que aparecen en el esquema de la figura 3 (las direcciones IP que aparecen en la figura se configurarán más adelante):

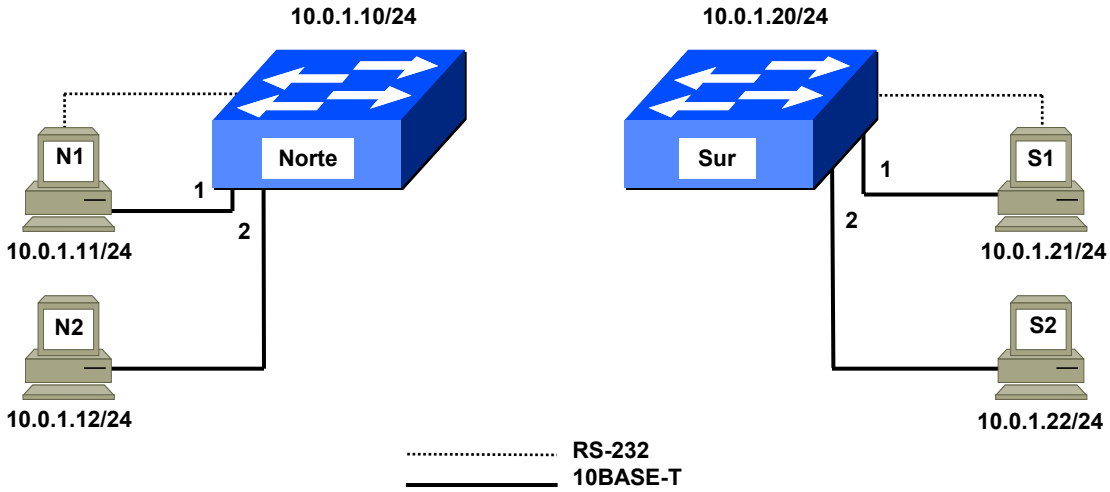

Figura 3: Interconexión de los equipos

Así pues las conexiones a realizar en cada subgrupo son las siguientes:

- Conectar la interfaz de consola del Catalyst 1900 a la interfaz serie (COM1) del ordenador 1 (N1 ó S1). La interfaz de consola del Catalyst es un conector RJ-45 que se encuentra en la parte trasera del equipo (figura 2). Por su parte el ordenador debe tener en el conector COM1 un adaptador de DB-9 a RJ-45, de forma que para la conexión de la interfaz de consola solo necesitamos un cable con dos conectores RJ-45. Este es un cable especial negro plano que nos suministrará el profesor (OJO: para la conexión de consola no puede utilizarse un latiguillo Ethernet pues la interconexión de pines de ese cable no es adecuada para esta conexión).

- Conectar las tarjetas Ethernet de los ordenadores a las interfaces del conmutador. Para esta conexión utilizaremos el latiguillo que conecta el ordenador a la red de la Universidad, que desconectaremos de la roseta de la pared y conectaremos en la toma correspondiente del Catalyst.

Una vez conectados los cables encenderemos los ordenadores. Cuando termina el arranque de la BIOS aparece un menú para elegir el sistema operativo; allí seleccionaremos la opción 'linux redes' que corresponde (a pesar de su nombre) a una instalación de linux capaz de funcionar sin conexión a la red de la Universidad, que es como se desarrolla esta práctica.

Una vez arrancado el sistema nos conectaremos en todos los ordenadores con el usuario `root` y la password que nos indique el profesor.

Ahora en el ordenador 1 (N1 ó S1) abriremos una ventana del intérprete de comandos shell y ejecutaremos el programa de emulación de terminal minicom mediante el comando '`minicom -s`', pulsando a continuación la tecla escape.

Familiarizarse con la interfaz de comandos del conmutador

Con el programa minicom en marcha procedemos a encender el Catalyst 1900 (los 1900 no tienen interruptor por lo que el encendido y apagado se realiza enchufando y desenchufando el cable de corriente). Al encenderlo el 1900 tarda unos 80 segundos en cargar el software y mostrar la pantalla de bienvenida que tiene el siguiente aspecto:

```
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.  1993-1998
All rights reserved.
Enterprise Edition Software
Ethernet Address:      00-50-F0-49-13-C0

PCA Number:            73-3124-01
PCA Serial Number:     FAA03059JPK
Model Number:          WS-C1924C-EN
System Serial Number:  FAA0308J03U
Power Supply S/N:      PHI024800YV
Power Supply P/N:
PCB Serial Number:
-------------------------------------------------

1 user(s) now active on Management Console.

        User Interface Menu

     [M] Menus
     [K] Command Line

Enter Selection:  _
```

Si no aparece dicha pantalla seguramente se debe a que la conexión no funciona o tiene algún problema. En ese caso deberemos comprobar los parámetros de configuración del minicom, para lo cual procedemos de la siguiente forma:

Tecleamos '**CTRL/A'** seguido de '**Z'** para entrar en los comandos del minicom. Tecleamos **'O'** para elegir configuración. De las opciones que aparecen elegimos **'Serial port setup'**. Los parámetros que aparecen deben tener los siguientes valores:

- Dispositivo de entrada: /dev/ttyS0
- Velocidad 9600 bits/s
- 8 bits de datos, un bit de parada, sin paridad (8N1)
- Control de flujo: ninguno

(El uso del dispositivo ttyS0 se debe a que estamos utilizando la interfaz COM1 del ordenador.)

Los Catalyst 1900 pueden configurarse de tres maneras diferentes: por interfaz web, por menús y por comandos. Nosotros utilizaremos la configuración por comandos por ser la más potente y la que más similitud tiene entre todos los equipos de la marca Cisco (conmutadores, routers, etc.). Para ello tecelaremos en la pantalla de bienvenida la letra **'K'**.

Al entrar en la interfaz de línea de comandos veremos aparecer el prompt **'>'**, que indica acceso no privilegiado. Podemos hacer uso del comando **'?'**, que nos muestra la lista de comandos que podemos utilizar en este entorno. Por ejemplo uno de esos comandos es **'show'**[1]; tecleando **'show ?'** nos aparece una lista de los argumentos que admite este comando. Ahora teclearemos el comando **'show**

[1] En este guión hemos seguido el convenio de utilizar **negritas lucida console** para indicar los comandos UNIX, que se deben teclear en una ventana de shell (por ejemplo **'minicom -s'**), mientras que si un comando aparece en **negrita courier** (**'show'** por ejemplo) significa que pertenece a la interfaz de comandos de los Catalyst 1900 y por tanto se debe de teclear en una ventana que esté actuando como consola (minicom o telnet) de un 1900, no en una ventana de shell de UNIX (este es un error muy frecuente en alumnos principiantes).

`version'` que nos muestra una información resumida del conmutador: la versión de software que tiene, el tiempo que lleva encendido, etc.

La interfaz de línea de comandos del conmutador dispone de varios entornos o modos, cada uno de ellos identificado por un prompt diferente. El prompt **`'>'`** identifica el llamado modo Usuario, que es el modo no privilegiado. Mediante el comando **`'enable'`** podemos pasar al modo Privilegiado, con lo que el prompt cambia a **`'#'`**; dependiendo de la configuración que tenga el conmutador es posible que al pasar a modo Privilegiado nos pida una password de acceso, en ese caso deberemos teclear **`'genios'`** (si con esta password no conseguimos entrar consultaremos al profesor). En el modo Privilegiado se pueden usar todos los comandos del modo Usuario más otros solo accesibles en modo Privilegiado. Del modo Privilegiado podemos volver en cualquier momento al modo Usuario con el comando **`'exit'`**. Del modo Privilegiado también podemos pasar a otro modo llamado Configuración Global mediante el comando **`'configure'`** que se caracteriza por el prompt **`'(config)#'`**. Como su nombre indica el modo Configuración Global permite hacer cambios globales en la configuración del equipo, para lo cual dispone de un conjunto de comandos completamente diferente al modo Privilegiado. Se puede volver del modo Configuración Global al modo Privilegiado mediante el comando **`'exit'`**, o también pulsando **`CTRL/Z`**. El último modo que necesitamos conocer para realizar esta práctica es el modo Configuración de Interfaz que también dispone de un conjunto de comandos propio. Se llega a él desde el modo Configuración Global mediante el comando **`'interface int'`** donde **`'int'`** corresponde al nombre de alguna interfaz existente en el equipo según la denominación de la Tabla 1 (por ejemplo Ethernet0/1), como veremos más tarde. El modo Configuración de Interfaz se utiliza para configurar características de una interfaz específica del equipo y se identifica por el prompt **`'(config-if)#'`**. Se puede volver de este al modo Configuración Global mediante el comando **`'exit'`**.

Esquemáticamente la conmutación de modos se desarrolla según la siguiente secuencia:

	`enable`→		**`configure`**→		**`interface int`**→	
Usuario <---------->	Privilegiado	<-------------------->	Configuración	<---------------------->	Configuración	
	←**`exit`**		←**`exit`** o **`CTRL/Z`**	Global	←**`exit`**	de Interfaz

Algunas características interesantes del intérprete de línea de comandos, aplicables a todos los modos, son las siguientes:

- En cualquier modo se puede utilizar el comando **'?'** para solicitar ayuda sobre los comandos permitidos.
- La tecla **CTRL/P** (o flecha hacia arriba ↑) recupera el último comando tecleado.
- Todos los comandos admiten abreviaturas siempre y cuando no haya ambigüedad en su significado. Si se escribe un comando o argumento incompleto y se pulsa la tecla tabulador el sistema termina de escribir el comando o argumento que corresponde. Esto permite al usuario asegurarse de que ha utilizado la abreviatura correcta para el comando que desea utilizar.

Restaurar la configuración de fábrica en los conmutadores

La primera labor que realizaremos es restaurar el conmutador a su configuración de fábrica. Como esta es una acción privilegiada debemos en primer lugar pasar a modo Privilegiado, para lo cual usamos el comando **`'enable'`**; si el equipo no tiene password configurada pasará a modo Privilegiado, inmediatamente, en caso contrario nos pedirá la password y deberemos teclear **`'genios'`** (si con esta password no conseguimos entrar consultaremos al profesor). Podremos reconocer que entramos en modo Privilegiado porque el prompt cambia entonces a **`'#'`**. Una vez en ese modo teclearemos nuevamente el comando **`'?'`** y observaremos que ahora aparece una lista de comandos considerablemente más larga que antes; los nuevos son comandos que solo están disponibles en este modo.

Para restaurar la configuración de fábrica usaremos el comando **`'delete nvram'`**. Se nos pide confirmación y en unos 10 segundos el equipo está nuevamente listo para funcionar:

```
# delete nvram
This command resets the switch with factory defaults.  All system
parameters will revert to their default factory settings.  All static
and dynamic addresses will be removed.
```

```
Reset system with factory defaults, [Y]es or [N]o?  Yes
```

La configuración de fábrica deja el equipo con una sola VLAN, con todas las interfaces asignadas a ella y el Spanning Tree activado en todas. En esta configuración el equipo carece de dirección IP. También se elimina la password que protege el acceso al modo Privilegiado en caso de que hubiera alguna configurada.

Una vez arrancado el conmutador y restaurado a su configuración de fábrica comprobaremos que se encienden los LEDs de 'link' correspondientes a las interfaces que tienen conectados ordenadores. Los LEDs se encuentran en la parte frontal del equipo; hay uno para cada interfaz del conmutador excepto la interfaz AUI, la que esta detrás, que no tiene LED.

Parte 1.2: Familiarizarse con el funcionamiento del conmutador y realizar pruebas básicas.

En esta fase de la práctica cada subgrupo trabaja sobre su conmutador Catalyst 1900 y sus ordenadores para desarrollar una red como la de la figura 3.

Configuración de los ordenadores y prueba básica de conectividad

Cada alumno deberá asignar una dirección IP a su ordenador de acuerdo con lo que se indica en la tabla 2.

Subgrupo Norte	
Ordenador	**Dirección IP**
N1	10.0.1.11
N2	10.0.1.12
Subgrupo Sur	
Ordenador	**Dirección IP**
S1	10.0.1.21
S2	10.0.1.22

Tabla 2. Configuración de red de los ordenadores.

Para ello utilizará el comando **'ifconfig'**.

COMANDO 'ifconfig'

El comando **'ifconfig'** se utiliza en UNIX para configurar la interfaz de red. Admite multitud de opciones y argumentos, pero nosotros solo veremos ahora lo necesario para saber como asignar una dirección IP (y su máscara) a una tarjeta Ethernet.

Supongamos que queremos asignar a un host la dirección 10.0.1.12 con máscara 255.255.255.0, lo cual significa que los primeros tres octetos de la dirección (10.0.1) representan la parte de red y el cuarto (12) la parte de host. El comando que utilizaríamos sería:

```
ifconfig eth0 inet 10.0.1.12 netmask 255.255.255.0
```

Una vez ejecutado el comando podemos comprobar que las definiciones se han realizado correctamente tecleando el comando '**ifconfig eth0'.** Un ejemplo de la respuesta que devuelve el comando **'ifconfig eth0'** es el siguiente:

```
[root@lab3inf005 ~]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:10:DC:CD:89:E7
          inet addr:10.0.1.12  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::210:dcff:fecd:89e7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5603995 errors:325 dropped:0 overruns:0 frame:325
```

```
          TX packets:29009 errors:0 dropped:0 overruns:0 carrier:0
          collisions:3060 txqueuelen:1000
          RX bytes:412078300 (392.9 MiB)  TX bytes:2839718 (2.7 MiB)
```

Para asignar la dirección IP debemos por tanto abrir una ventana de shell en el ordenador y ejecutar el comando UNIX:

`ifconfig eth0 inet` *`dirección_IP`* `netmask 255.255.255.0`

Por ejemplo para el ordenador N2 el comando sería

`ifconfig eth0 inet 10.0.1.12 netmask 255.255.255.0`

Para comprobar que la asignación se ha efectuado correctamente utilizaremos (en la misma ventana de shell) el comando **'ifconfig eth0'**.

Una vez configurada la dirección IP en los ordenadores podemos utilizar el comando **'ping'** para comprobar que existe conectividad.

COMANDO 'ping'

El comando **'ping'** se utiliza para comprobar que existe conectividad con una dirección IP determinada. Se encuentra en prácticamente todas las implementaciones de TCP/IP. Su utilización es muy simple, basta con teclear **'ping'** seguido de la dirección IP contra la que se desea comprobar la conectividad. Esto provoca el envío de paquetes hacia dicha dirección, que deben ser respondidos inmediatamente. Por ejemplo, si tecleamos '**ping 10.0.1.22**' obtendremos una respuesta del host 10.0.1.22. El comando ping nos indica además el tiempo transcurrido desde que se envía el paquete de ida hasta que se recibe el de vuelta, el llamado 'round trip time' o rtt. Un ejemplo de uso del comando ping es el siguiente:

```
[root@lab3inf005 ~]# ping 10.0.1.22
PING 10.0.1.22 (10.0.1.22) 56(84) bytes of data.
64 bytes from 10.0.1.22: icmp_seq=0 ttl=255 time=0.555 ms
64 bytes from 10.0.1.22: icmp_seq=1 ttl=255 time=0.518 ms
64 bytes from 10.0.1.22: icmp_seq=2 ttl=255 time=0.545 ms

--- 10.0.1.22 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.518/0.539/0.555/0.024 ms, pipe 2
[root@lab3inf005 ~]#
```

En este caso se han enviado tres paquetes de 56 bytes de datos más 28 de cabeceras (una de 20 y una de 8 bytes). Cada paquete ha sido respondido por otro de igual tamaño. Los tiempos de ida y vuelta (rtt) han sido de 0,555, 0,518 y 0,545 ms, respectivamente. El rtt mínimo ha sido de 0,518, el medio de 0,539 y el máximo de 0,555 ms. La desviación media ha sido de 0,024 ms.

En algunas implementaciones del ping, como por ejemplo en linux, se envía por defecto un paquete de prueba por segundo de forma indefinida. En Windows por defecto se envían tres paquetes (separados por un segundo) y se para la transmisión.

Como muchos comandos el **'ping'** admite una serie de opciones que modifican su comportamiento. En UNIX esas opciones pueden averiguarse mediante el comando **'man ping'**. Las opciones del ping que nos van a interesar en esta práctica son las siguientes:

Opción	Significado
`-b`	Indica que se quiere realizar un envío broadcast. Cuando se utiliza esta opción la dirección de destino del ping debe ser una dirección broadcast.
`-f`	Indica que se envíen 100 paquetes por segundo (f=flood, inundación) en vez del comportamiento normal, que es uno por segundo.

-c num_paq	Indica que se envíen **num_paq** paquetes, después de lo cual se devuelve el control a la consola. Si se omite esta opción se envían paquetes de forma indefinida, siendo necesario pulsar CTRL/C y abortar el envío para recuperar el control de la consola.
-s tam_paq	Indica que se envíen paquetes de tamaño **tam_paq**, en bytes. El paquete real tiene además 28 bytes de cabeceras (IP e ICMP). Si se omite esta opción se envían paquetes de 84 bytes.
-R	Indica que se quiere que el ping registre las direcciones IP de todos los equipos por los que pasa el paquete, obteniendo así una traza del camino recorrido a la ida y a la vuelta
-n	Se utiliza junto con la opción –R para indicar que no se quiere utilizar el servicio de resolución de nombres. Esta opción es importante en las prácticas del laboratorio ya que la red utilizada no dispone de este servicio

Estas opciones pueden combinarse entre sí, así por ejemplo el comando **'ping –f –c 1000 –s 5912 10.0.1.22'** enviará 1000 paquetes a razón de 100 paquetes por segundo, es decir durante 10 segundos, de 5940 bytes de tamaño a la dirección 10.0.1.22.

Los paquetes recibidos por el ping siempre tienen el mismo tamaño y la misma frecuencia que los paquetes enviados.

Una vez configurada la dirección IP en los ordenadores podemos probar a utilizar en la ventana de shell el comando **'ping'** hacia otro ordenador del mismo subgrupo con lo que comprobaremos que existe comunicación bidireccional entre ellos. Esto demuestra la característica 'plug&play' del conmutador, ya que está realizando la conmutación de tramas sin que le hayamos introducido todavía ningún comando en la configuración.

Configuración IP de los conmutadores, asignación de password y conexión vía telnet

Ahora asignaremos una dirección IP al conmutador. Este paso lo realizaremos desde la ventana minicom del ordenador 1 (N1 o S1) que actúa de consola del conmutador. Si no se ha cerrado la conexión que abrimos antes esta seguirá mostrando el prompt **'#'**, lo cual indica que sigue en modo Privilegiado. Si por alguna razón se hubiera cortado esa conexión deberemos entrar de nuevo en el conmutador, seleccionar la modalidad de línea de comandos (**'K'**) y pasar a modo Privilegiado con el comando **'enable'** (ahora no nos pedirá password ya que la configuración de fábrica no la tiene). Una vez en modo Privilegiado tecleamos el comando **'configure'** para pasar al modo Configuración Global, cosa que reconoceremos porque el prompt cambia ahora a **'(config)#'**. En el modo de Configuración Global teclearemos **'?'** y veremos que aparece en la lista el comando **'ip'**; tecleando **'ip ?'** averiguaremos qué parámetros admite dicho comando. Uno de ellos es **'address'**, que sirve para asignar una dirección IP y máscara al conmutador. Utilizaremos este comando para introducir la configuración IP correspondiente, de acuerdo con la relación que aparece en la Tabla 3 (por ejemplo para el conmutador Norte el comando a teclear será **'ip address 10.0.1.10 255.255.255.0'**. Una vez hecho esto saldremos del modo Configuración Global tecleando **CTRL/Z**. Al salir de este modo volvemos al modo Privilegiado, por lo que el prompt vuelve a ser **'#'**. La secuencia completa de comandos para el conmutador Norte por ejemplo sería la siguiente:

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
(config)#ip address 10.0.1.10 255.255.255.0
(config)#CTRL/Z
#
```

Conmutador	Dirección IP	Máscara
Norte	10.0.1.10	255.255.255.0
Sur	10.0.1.20	255.255.255.0

Tabla 3: Configuración de red de los conmutadores.

Una vez le hemos asignado una dirección IP al conmutador ya podemos comunicarnos con él desde cualquier ordenador conectado a la red, cosa que podremos comprobar ejecutando el comando **ping**

desde alguno de los hosts hacia su dirección IP. En principio esto nos debería permitir configurar el conmutador vía **telnet** desde cualquier ordenador, no solo desde el que tiene conectada la consola (el comando **telnet** nos permite iniciar una sesión en un equipo remoto). Sin embargo, por razones de seguridad el acceso vía telnet no está permitido cuando el equipo no tiene configurada una password de acceso, por lo que lo siguiente que haremos será asignarle una password. La password que utilizaremos es **'genios'** (sin las comillas). Para introducirla teclearemos por consola del conmutador en modo Configuración Global el comando **'enable password level 15 genios'** (como antes entraremos en el modo Configuración Global con el comando **'configure'** y saldremos con **'CTRL/Z'**). La secuencia completa es la siguiente:

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
(config)#enable password level 15 genios
(config)#CTRL/Z
#
```

A partir de este momento podremos acceder vía **telnet** al conmutador desde cualquier ordenador conectado a él. Por ejemplo para acceder al conmutador Sur teclearemos el comando **'telnet 10.0.1.20'**.

Ahora nos conectaremos desde los dos ordenadores al conmutador vía telnet, para acceder como consola remota. Obsérvese que en el ordenador 1 tendremos ahora abiertas dos consolas, la que ya teníamos en la ventana minicom por la interfaz serie (COM1) y la nueva que hemos abierto mediante la conexión telnet; esta última va por la red Ethernet. Para la mayoría de las funciones ambas conexiones son equivalentes y puede utilizarse cualquiera de ellas, pero algunas tareas solo pueden realizarse por la conexión serie (minicom). Por ello en el ordenador 1 mantendremos la ventana de minicom y cerraremos la de telnet.

Uso del comando 'show interface'

En esta parte de la práctica probaremos diversos comandos del conmutador desde las consolas de los ordenadores 1 y 2 (minicom y telnet, respectivamente). En primer lugar pasaremos al modo Privilegiado mediante el comando **'enable'** (password **'genios'**) y tecelaremos el comando **'show interfaces'** para ver las características y forma de numerarse de las diferentes interfaces del equipo. La salida generada por este comando ocupa varias pantallas, quedándose el terminal boqueado cuando se completa la primera, lo cual viene indicado por el texto 'more' al final de la pantalla. Para avanzar a la siguiente pantalla debemos pulsar la barra espaciadora y así sucesivamente hasta agotarlas todas. También puede abortarse la salida por pantalla en cualquier momento pulsando **CTRL/C**. Por cada interfaz aparecen dos pantallas, la primera indica las características físicas de la interfaz y la segunda muestra una serie de contadores de tráfico que luego describiremos. Ahora debemos prestar especial atención a los nombres que reciben las interfaces, que deben corresponderse con los que aparecen en la tabla 1.

El comando **'show interfaces'** puede utilizarse con argumentos, con lo que podemos obtener información sobre una interfaz en particular. Esto resulta útil cuando sólo se quiere obtener información sobre una o unas pocas interfaces, evitando así la farragosa salida por pantalla producida por el comando anterior. Por ejemplo el comando **'show interface Ethernet 0/2'** (que podemos abreviar a **'s in e 0/2'**) nos muestra información sobre la interfaz número 2 únicamente. Ahora haremos un **'show interface'** de la interfaz donde está conectado nuestro ordenador (Ethernet 0/1 ó Ethernet 0/2) y nos fijaremos en la información que aparece. Podemos ver por ejemplo que en la primera línea dice que la interfaz está en estado 'enabled'. Si hacemos un **'show interface'** de una interfaz que no tenga nada conectado (por ejemplo la Ethernet 0/12) veremos que el estado es 'Suspended-no-linkbeat'.El apéndice I explica en detalle el significado de toda la información que devuelve el comando **'show interfaces'**.

Ahora probaremos las posibilidades que nos ofrece el conmutador de contabilizar el tráfico que pasa por él. El conmutador mantiene una serie de contadores de tramas y octetos (bytes) recibidos y transmitidos, así como de una diversidad de situaciones excepcionales y errores (colisiones, múltiples colisiones, colisiones tardías, errores de CRC, etc.). Todos estos contadores nos los muestra cada vez que ejecutamos el comando **'show interfaces'**. El valor mostrado corresponde al acumulado desde la última vez que se encendió el conmutador. Una forma de comprobar que está pasando tráfico en un momento dado

es ejecutar dos veces el comando **'show interfaces'** para una interfaz en particular y comprobar que los contadores de tramas/octetos recibidos y transmitidos se incrementan. Por ejemplo si abrimos una ventana de shell en uno de los ordenadores y ejecutamos el comando ping hacia el otro podremos lanzar periódicamente en la ventana de consola del conmutador el comando **'show interfaces'** y ver como evoluciona el contador de paquetes y bytes transmitidos y recibidos. Podríamos calcular el tráfico en un intervalo de tiempo dado tomando dos lecturas de los contadores y calculando las diferencias en tiempo y en octetos transmitidos/recibidos entre ambas. Esto es lo que hacen programas como el MRTG (ver www.mrtg.org) con la única diferencia de que en vez de utilizar el comando **'show interfaces'** emplean mensajes del protocolo estándar SNMP (Simple Network Management Protocol). Otro comando interesante es el **'clear counters *interfaz*'** (por ejemplo **'clear counters ethernet 0/2'**) que pone a cero los contadores que corresponden a la interfaz indicada; de esta forma sabemos que todo el tráfico contabilizado en los contadores que aparecen en el comando **'show interfaces'** se ha producido desde la última vez que hemos borrado contadores. El comando **'clear counters'** se puede utilizar también sin argumentos, en cuyo caso borra los contadores de todas las interfaces. El comando **'clear counters'** requiere acceso en modo Privilegiado al conmutador. Este comando debería utilizarse con cuidado en un entorno como el de esta práctica donde varias personas están trabajando a la vez en el mismo conmutador y están posiblemente consultando los mismos contadores.

Tráfico de BPDUs y desactivación del protocolo Spanning Tree

Vamos a comprobar ahora que el conmutador genera por sí mismo tráfico, aún en el caso de que los hosts no estén enviando nada. Para evitar interferencias producidas por el tráfico de conexiones telnet haremos este experimento desde la ventana minicom del ordenador 1 (N1 ó S1) y cerraremos la ventana telnet abierta desde el ordenador 2, y la del 1 si la tuviéramos; el tráfico generado por la ventana minicom, al emplear la interfaz de consola, no se refleja en los contadores de las interfaces Ethernet. Ejecutaremos a continuación el coamndo **'clear counters'**, esperaremos 30 segundos y luego ejecutaremos un **'show interface'** (abreviado **'s in'**) de alguna interfaz conectada, por ejemplo **'s in e 0/1'**. Podemos ver que el conmutador envía algo por esa interfaz pues el contador de tramas y octetos transmitidos se incrementa pero no así el de recibidos ya que el host 1 no está enviando nada[2]. Ese tráfico, de caudal reducido pero continuo que genera el conmutador es todo multicast, como puede verse por los contadores, y se debe en su mayor parte a los mensajes 'hello' del protocolo Spanning Tree, que por defecto se envían a razón de uno cada 2 segundos. Para comprobarlo desactivaremos el Spanning Tree en el conmutador. El comando que activa el Spanning Tree es **'spantree'**; como por defecto está activado y lo que queremos ahora es desactivarlo utilizaremos el comando **'no spantree'**. Además debemos indicar en que VLAN queremos aplicarlo; como no hemos configurado todavía ninguna VLAN todos los puertos se encuentran asignados a la VLAN por defecto, que es la 1. Por tanto el comando que debemos teclear es **'no spantree 1'** que ejecutaremos en modo Configuración Global en la consola del conmutador (ventana minicom del ordenador 1). La secuencia es la siguiente:

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
(config)#no spantree 1
(config)# CTRL/Z
#
```

Una vez desactivado el Spanning Tree repetiremos la secuencia anterior (comando **'clear counters'** seguido al cabo de un tiempo de **'s in e 0/1')** para ver si hay algo de tráfico. Podremos observar que el tráfico es ahora mucho menor, pero no nulo (exactamente una trama por minuto). Este tráfico corresponde al CDP (Cisco Discovery Protocol), un protocolo propietario de Cisco que permite que los equipos Cisco presentes en una red se encuentren automáticamente. Si queremos que el conmutador no genere absolutamente ningún tráfico debemos desactivar también este protocolo, cosa que podemos hacer sin ningún problema ya que el CDP no se utiliza en esta práctica. Pero mientras que el Spanning Tree se activa o desactiva de forma global para todo el conmutador el CDP se activa o desactiva a nivel de interfaz, no de forma global. Así pues utilizaremos el comando **'no cdp enable'** en modo Configuración de Interfaz. La secuencia de comandos, por ejemplo para la interfaz 1, es la siguiente:

[2] En el **'show interfaces'** los contadores de tráfico transmitido o recibido siempre se refieren desde el punto de vista del conmutador, es decir transmitido significa saliente, tráfico dirigido desde el conmutador hacia el host.

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
(config)#int eth 0/1
(config-if)#no cdp enable
(config-if)#CTRL/Z
#
```

Una vez desactivado el CDP podremos comprobar que por mucho que esperemos no se genera absolutamente ningún tráfico.

Funcionamiento de los LEDs y cambio de modo

Vamos a describir a continuación la información que suministran los LEDs de las interfaces en los Catalyst 1900, ya que para el adecuado desarrollo de la práctica es interesante conocerla. La información de los LEDs es configurable por el usuario, que puede conmutar entre varios posibles modos de funcionamiento pulsando el botón 'MODE', que se encuentra en la parte frontal izquierda del conmutador (ver figura 1). Los posibles modos son: STAT (Status), UTL (Utilization) y FDUP (Full Duplex). Un LED encima del botón MODE indica en que modo se encuentra el conmutador en cada momento. Inicialmente los LEDs se encuentran en modo STAT; se puede cambiar a modo UTL pulsando una vez el botón MODE, o a modo FDUP pulsando dos veces. Pulsando el botón una tercera vez se vuelve al modo STAT. Independientemente del modo en que se encuentre el conmutador revierte al modo STAT al cabo de cierto tiempo.

En el modo STAT cada LED representa el status de la interfaz correspondiente: una luz verde indica que hay enlace con el equipo conectado a esa interfaz; si además la luz parpadea indica que hay tráfico por ella. Si el LED está apagado significa que no hay enlace, lo cual puede deberse a que no hay ningún equipo conectado en esa interfaz, a que el equipo está apagado o a que se ha utilizado un cable incorrecto (por ejemplo un cable cruzado). Cuando un LED parpadea en ámbar significa que se están detectando problemas con el tráfico en esa interfaz, que pueden ser, por ejemplo: excesivas colisiones, errores de CRC, errores de alineamiento (tramas que no tienen un número entero de bytes), etc. Normalmente en estos casos el parpadeo alterna entre verde y ámbar pues no todas las tramas son erróneas. Por último si un LED se enciende en ámbar de forma permanente indica que la interfaz correspondiente se encuentra en estado 'blocked' (o algún otro estado no 'forwarding') por indicación del protocolo Spanning Tree.

En el modo UTL los LEDs de las 24 interfaces 10BASE-T se utilizan de forma conjunta para mostrar el ancho de banda agregado que está manejando el conmutador, con una escala más o menos logarítmica. La escala utilizada se muestra en la tabla 4.

LEDs	Ancho de banda total (Mb/s)
De 1 a 8	De 0,1 a < 6
De 9 a 16	De 6 a < 120
De 17 a 24	De 120 a <280

Tabla 4. Significado de los LEDs en el modo UTL en un Catalyst 1924

Además de marcar el tráfico instantáneo con LEDs parpadeantes el conmutador mantiene encendidos durante breves instantes los LEDs que marcan el valor máximo alcanzado.

Por último el modo FDUP muestra que interfaces están configuradas en modo full dúplex encendiendo en verde el LED correspondiente. En caso de que la interfaz esté configurada half-duplex el LED no se enciende.

Generación de tráfico masivo

Ahora haremos un experimento consistente en provocar tráfico masivo a través del conmutador. Para ello en una ventana de shell ejecutaremos el comando **'ping –f *dirección_IP*'** (donde *dirección_IP* es la dirección IP del ordenador contra el que se ejecuta el ping). La opción –f (flood) envía 100 paquetes por segundo con lo que se genera una cantidad de tráfico fácilmente apreciable en los contadores y en los LEDs. El ordenador 1 ejecutará el ping hacia el 2. Por defecto el comando ping envía paquetes ICMP de

56 octetos de datos, lo cual da lugar a una trama Ethernet de 102 octetos[3]. A razón de 100 paquetes por segundo esto genera un tráfico de 81,6 Kb/s en cada sentido (recordemos que en el ping cada paquete recibido es respondido con otro igual). Mediante el comando **'clear counters *interfaz*'** seguido de **'show interface *interfaz*'** para la interfaz correspondiente (Ethernet 0/1 ó Ethernet 0/2 según se trate del host 1 ó el 2) observaremos el rápido incremento de los contadores de tramas y octetos recibidos y transmitidos. También podemos apreciar el tráfico generado observando los LEDs de las interfaces: en el modo STAT: veremos que los que tienen tráfico parpadean, siendo la frecuencia del parpadeo proporcional a la cantidad de tráfico. Si pasamos al modo UTL veremos como al lanzar el **ping -f** se incrementa el número de LEDs encendidos; si lanzamos varios **ping -f** en paralelo (en varias ventanas) veremos como crece el número de LEDs encendidos en el modo UTL, y permanece encendido el que corresponde al máximo alcanzado.

Prueba de una conexión half-full dúplex (duplex mismatch)

Ahora haremos una prueba de los problemas de rendimiento que se producen cuando se tiene una configuración mixta half-full en una conexión Ethernet (situación conocida como 'duplex mismatch'). Las interfaces 10BASE-T del conmutador no negocian el modo duplex half-full y tienen por defecto configuración half-dúplex. En cambio las tarjetas de los ordenadores sí negocian el modo duplex en el momento de conectarse. Por tanto los ordenadores al conectarse al conmutador se han puesto a trabajar en modo half-duplex.

El experimento que realizaremos a continuación consiste en lo siguiente: en primer lugar mediremos, usando el comando ping, el rendimiento que se obtiene en la comunicación entre los ordenadores 1 y 2 cuando ambos tienen su conexión configurada half en los dos extremos (ordenador y conmutador). Después cambiaremos la interfaz 1 del conmutador a modo full-duplex, con lo que conseguiremos un duplex mismatch en la conexión del ordenador 1 (el ordenador en modo half y el conmutador en modo full). A continuación repetiremos el ping anterior, con lo que podremos comparar el resultado con el obtenido en el primer caso. La figura 6 muestra la situación de forma esquemática.

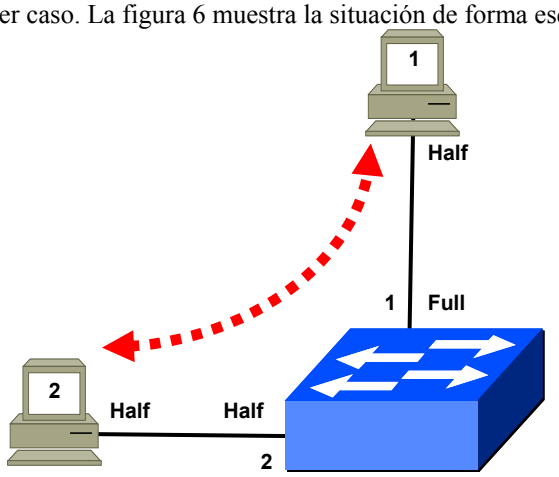

Figura 4. Conexión half-full en un conmutador

Obsérvese que para conseguir una comunicación ineficiente es suficiente tener 'duplex mismatch' en una de las dos conexiones involucradas, en este caso la del ordenador 1 con el conmutador.

Para que la diferencia de rendimiento entre el modo half-half y el half-full sea más evidente provocaremos una situación de congestión en la red. Utilizaremos para ello el comando **'ping -f -c *número* -s 5912 *dirección_IP*'**. Este comando inyecta 100 paquetes por segundo de 5912 bytes en la Ethernet lo cual induce un tráfico de exactamente 9,8432 Mb/s (4,9216 Mb/s de ida y 4,9216 Mb/s de vuelta[4]). La duración de la ráfaga viene determinada por el parámetro 'número' de la opción –c, que inidca el número de paquetes a enviar. Así por ejemplo con **'ping -f -c 1000 -s 5912**

[3] 56 de datos más la cabecera ICMP (8 bytes) la cabecera IP (20 bytes), la cabecera MAC (14 bytes) y el CRC (4 bytes).

[4] Para saber como calcular exactamente el caudal en Mb/s que corresponde a un determinado tamaño de paquete en el comando ping consultar el apéndice II.

dirección_IP' generamos una ráfaga de 10 segundos de duración (1000 paquetes) y con **'ping -f -c 1200 -s 5912** ***dirección_IP***' la ráfaga es de 12 segundos (1200 paquetes).

Para la prueba abriremos en el ordenador 1 (N1 o S1) dos ventanas de shell. En la primera ejecutaremos el comando **'ping -f -c 1200 -s 5912** ***dirección_IP***' poniendo como dirección IP de destino la del ordenador 2 (10.0.1.12 o 10.0.1.22 según se trate de N2 ó S2, respectivamente). Inmediatamente después ejecutaremos en la segunda ventana de shell el comando **'ping -f -c 1000 -s 5912** ***dirección_IP***' hacia la misma dirección IP que el primero. La finalidad del primer ping, cuya duración es de 12 segundos, es actuar de relleno generando un tráfico elevado en la red Ethernet durante los 10 segundos que dura el segundo ping, que es el que utilizaremos para medir el rendimiento. Del segundo ping nos interesa obtener el resumen final sobre paquetes transmitidos y recibidos, del primero lo único que nos interesa es que esté en marcha durante todo el tiempo que dura el segundo, es decir que empiece antes y termine después. Por ello es importante que el ping 'de relleno' (**'ping -f -c 1200'**) se lance antes que el ping de prueba (**'ping -f -c 1000'**), pero no más de dos segundos antes para asegurar que termina después, aunque en caso necesario se puede ampliar la duración del ping de relleno aumentando el número de paquetes. A menudo el ping -f ejecutado en estas condiciones se engancha al final y hay que abortarlo con CTRL/C, pero tanto si termina normalmente como si se aborta con CTRL/C el ping envía todos los paquetes indicados en la opción –c y muestra un resumen final con las estadísticas habituales de tiempo mínimo, medio, máximo, paquetes transmitidos, paquetes recibidos, etc. Si tenemos duda sobre cuando termina el ping podemos controlar el tiempo transcurrido con un reloj o simplemente observar el cambio de actividad en los LEDs del conmutador. De todos los datos que aparecen en el ping de prueba solo nos interesa el número de paquetes transmitidos y recibidos, que deben ser iguales o muy parecidos.

Podemos aprovechar el envío de tráfico masivo que se realiza con el ping –f en esta parte de la práctica para probar el modo UTL de los LEDs, que hemos descrito anteriormente. Pulsando una vez el botón de cambio de modo de los LEDs pasaremos a modo UTL y veremos como mientras está en marcha el **ping -f** se encienden varios LEDs y cuando termina se apagan, quedando encendido entonces el que corresponde al valor máximo alcanzado. Dado que solo estamos generando tráfico en dos interfaces de 10 Mb/s los valores que obtendremos de tráfico a nivel global no serán muy elevados, aun cuando las interfaces utilizadas lleguen a estar completamente saturadas.

Una vez hemos probado y nos hemos familiarizado con el procedimiento descrito para la medida de rendimiento entraremos desde el ordenador 1 (en una ventana minicom) en la consola del conmutador y borraremos los contadores de la interfaz con el comando **'clear counters eth0/1'** en modo Privilegiado. A continuación repetiremos el proceso de los dos **ping -f** y anotaremos los valores de paquetes transmitidos y recibidos de las estadísticas mostradas por el **'ping -f -c 1000'**. Después ejecutaremos en la consola del conmutador el comando **'show interfaces eth0/1'** y anotaremos los valores que allí aparecen de los siguientes contadores:

- Runt frames
- FCS Errors
- Single collisions
- Multiple collisions
- Excessive collisions

Dado que antes de lanzar los dos ping -f hemos borrado contadores los valores que anotamos corresponden únicamente a la ejecución de esos dos pings. Estos valores junto con el número de paquetes transmitidos y recibidos que obtuvimos en la ventana del ping son los que compararemos con la prueba en modo 'half-full' que haremos a continuación. Recordemos que en el apéndice I se encuentra la explicación detallada del significado de todos los contadores que aparecen en el comando **'show interfaces'**.

Ahora debemos cambiar a modo full dúplex la interfaz Ethernet 0/1 en la que se conecta el ordenador 1. Para ello utilizaremos el comando **'duplex full'** en el modo Configuración de Interfaz de la interfaz que queremos cambiar. La secuencia de comandos es la siguiente:

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
(config)#int eth0/1
(config-if)#duplex full
```

```
(config)# CTRL/Z
#
```

Una vez hecho el cambio a full lo comprobaremos de dos maneras. Por un lado utilizaremos el comando **'show interfaces ethernet 0/1'** (o **'s in e 0/1')** y buscaremos el sitio donde ponga 'Duplex setting: Full duplex'. La segunda comprobación la haremos pasando a modo FDUP los LEDs del conmutador mediante el botón MODE (pulsar dos veces para pasar desde modo STAT); en el modo FDUP se encienden únicamente los LEDs correspondientes a las interfaces que están en modo full dúplex, en nuestro caso la interfaz 1.

Comprobaremos a continuación que, aunque hemos modificado la configuración duplex del puerto 1 del conmutador la interfaz Ethernet del ordenador 1 continúa en modo half. Para ello utilizaremos el comando **'ethtool eth0'**.

COMANDO 'ethtool'

El comando '**ethtool'** nos devuelve información sobre la configuración y posibilidades de la tarjeta Ethernet de nuestro ordenador. Como es habitual el comando man ethtool nos muestra todas sus opciones y posibilidades, aunque de momento solo nos interesa la información que devuelve sin opciones, como se muestra en el siguiente ejemplo:

```
[root@lab3inf005 ~]# ethtool eth0
Settings for eth0:
        Supported ports: [ TP MII ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Advertised auto-negotiation: Yes
        Speed: 10Mb/s
        Duplex: Half
        Port: MII
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: g
        Wake-on: g
        Current message level: 0x00000007 (7)
        Link detected: yes
[root@lab3inf005 ~]#
```

La línea 11 ('Duplex: Half') nos indica que el modo duplex actual es Half. También nos indica las posibilidades de la tarjeta, si se encuentra activada la función de autonegociación y la velocidad que se está utilizando actualmente (10 Mb/s).

Una vez cambiada a modo full dúplex la interfaz 1 del conmutador y conseguido por tanto el 'duplex mismatch' repetiremos el proceso anterior consistente en:

1. Borrar contadores de la interfaz 1 con el comando **'clear counters eth 0/1'**

2. Abrir dos ventanas de shell en el ordenador 1 y lanzar el ping de relleno hacia 2 ('**ping -f -c 1200 -s 5912** ***dirección_IP***') seguido inmediatamente del otro (**'ping -f -c 1000 -s 5912** ***dirección_IP***'). Cuando los dos pings hayan terminado (abortar con

CTRL/C en caso necesario) tomaremos nota de los paquetes transmitidos y recibidos en el segundo ping (**'ping -f -c 1000'**).

3. Ejecutar **'show interfaces eth 0/1'** y anotar los valores de los mismos contadores que antes

Antes de ejecutar los dos pings debemos asegurarnos de que los LEDs del conmutador estén en modo STAT. Así podremos observar el parpadeo en los LEDs de las interfaces 1 y 2 durante la ejecución de los '**ping -f'**. Ahora bien, mientras que el LED de la interfaz 2 parpadea siempre en verde el de la 1, que es el que tiene duplex mismatch, alterna el parpadeo verde con el ámbar. Los parpadeos ámbar se producen por tramas incompletas y tramas erróneas que el conmutador está recibiendo del host 1. Esto se debe precisamente al duplex mismatch de la interfaz 1, que no ocurre en la interfaz 2, donde tanto el host como el conmutador están half. El modo half del ordenador 1 provoca que cada vez que detecte una colisión con el conmutador suspenda la transmisión en curso.

Comparando los valores obtenidos en la primera prueba y en la segunda observamos lo siguiente:

- En la primera prueba (conexión half-half) se producen muchas colisiones (sencillas y múltiples) y algunas 'excessive collisions'. Esto es algo normal dado el grado de congestión que hemos provocado, muy superior a lo que la red permite. Sin embargo esas colisiones son resueltas de manera satisfactoria por el retroceso exponencial binario de CSMA/CD y solo las 'excessive collisions' (que son muy pocas) provocan pérdida de tramas. Estas pérdidas se producen en una proporción pequeña, como puede comprobarse por el contador de paquetes del ping.

- En la segunda prueba (conexión half-full) la tasa de pérdidas es mucho mayor como se comprueba por el contador de paquetes del ping y por el elevado valor de los contadores 'FCS errors' y 'Runt frames' en el **'show interfaces ethernet 0/1'**. Los 'runt frames' se deben a envíos del host que éste ha abortado al detectar una colisión antes de haber podido enviar 64 bytes; se trata pues de tramas con una longitud menor que la mínima permitida en Ethernet. Los 'FCS errors' se deben a tramas abortadas por el host antes de terminar pero que ya han pasado del byte 64; por tanto tienen una longitud válida pero un CRC inválido. Es interesante observar que en esta segunda prueba el conmutador no registra ninguna colisión, a pesar de la congestión y del elevado grado de pérdidas de tramas. Esto se debe a que al funcionar la interfaz en modo full se ha desactivado el CSMA/CD con lo que el contador de colisiones del conmutador para esa interfaz es siempre cero.

Envío de tráfico broadcast

Haremos a continuación un experimento que consiste en analizar como evoluciona el contador de tramas broadcast/multicast del conmutador. Para provocar tráfico de este tipo utilizaremos el comando '**ping 10.0.1.100'**. Esta dirección IP no está asignada a ningún equipo, pero al encontrarse en la misma subred (empieza por 10.0.1) nuestro ordenador intentará localizarla enviando mensajes ARP broadcast[5] a razón de uno por segundo, aproximadamente. Los mensajes broadcast (dirección MAC X'FFFF.FFFF.FFFF') se propagan por inundación a todas las interfaces activas del conmutador (las interfaces que no tienen nada conectado no están activas a nivel físico, por lo que nunca se envía por ellas ningún tráfico, ni siquiera el broadcast).

En esta prueba únicamente utilizaremos el ordenador 1. Primero lanzamos el ping a la dirección 10.0.1.100 desde una ventana de shell y con el ping en marcha abrimos en otra ventana la consola del conmutador. A continuación borraremos contadores de todo el conmutador (comando **'clear counters'**) y teclearemos después el comando **'show interfaces'.** Observaremos que en la interfaz 1 (Ethernet 0/1) aumentan paulatinamente los contadores 'Broadcast/multicast frames' y 'Broadcast/multicast octets' en la columna de la izquierda, que corresponde a 'Receive Statistics'. En cambio en el resto de interfaces activas (en nuestro caso solo la 2) veremos que los contadores que se incrementan son los de la derecha, que corresponden a 'Transmit Statistics'. Esto significa que el ordenador conectado a esa interfaz está recibiendo los mensajes

[5] ARP (Address Resolution Protocol) es el protocolo que resuelve la equivalencia de las direcciones IP en las direcciones MAC. ARP se basa en el envío inicial de un paquete broadcast

broadcast que el conmutador recibe por la interfaz 1. (Recordemos que el sentido de recepción o transmisión se interpreta siempre desde el punto de vista del conmutador.)

Tabla de direcciones MAC, tiempo de vida y cambio en marcha de una conexión

En este apartado vamos a analizar la información que contiene la tabla de direcciones MAC del conmutador. Para ello utilizaremos en modo Privilegiado el comando **'show mac-address-table'** que nos muestra una tabla con la relación de todas las direcciones MAC conocidas por el conmutador y las interfaces por las que están accesibles. También podemos probar el comando **'clear mac-address-table'** que, como su nombre indica, borra completamente la tabla de direcciones MAC y obliga a que las tramas siguientes sean enviadas por inundación.

Una manera fácil de llenar la tabla de direcciones MAC del conmutador es lanzar un ping a la dirección IP broadcast de la red, en nuestro caso **'ping –b 10.0.1.255'**[6]. Como esto generamos tráfico hacia y desde todos los dispositivos IP de la red (en nuestro caso el otro ordenador y el conmutador), con lo que rápidamente les veremos aparecer en la tabla de direcciones MAC del conmutador (aunque a veces hay equipos que no responden a los pings broadcast). Sin embargo la tabla del conmutador no nos muestra direcciones IP, ya que este dispositivo solo funciona a nivel 2 y no analiza la información a nivel de red. Si queremos averiguar la equivalencia IP-MAC debemos utilizar en los hosts el comando UNIX **'arp –a –n'** que nos muestra la tabla ARP caché, que sí contiene dicha información.

COMANDO 'arp'

El comando 'arp' (disponible en UNIX y en Windows) permite averiguar la tabla de equivalencia entre direcciones IP y direcciones MAC que tiene un host en un instante determinado. Dicha tabla, conocida como la ARP-cache, es cambiante con el tiempo.

En esta práctica utilizamos el comando 'arp' con las opciones '–a', que indica que queremos obtener la tabla ARP caché, y '–n' que indica que queremos obtener las direcciones IP, no los nombres correspondientes. En la maqueta que estamos manejando en esta práctica no hay servicio de DNS (Domain Name Server o resolución de nombres), por lo que el uso de la opción –n es necesario para que el comando funcione correctamente.

Un ejemplo de uso del comando arp es el siguiente:

```
[root@lab3inf005 ~]# arp -a -n
? (10.0.1.10) at 00:06:5B:B9:A1:94 [ether] on eth0
? (10.0.1.12) at 00:0A:5E:3C:81:8C [ether] on eth0
 [root@lab3inf005 ~]#
```

De manera análoga a lo que ocurre con la tabla de direcciones MAC del conmutador las entradas de la ARP caché también caducan, pero si hemos hecho recientemente el ping broadcast es muy probable que ambas tablas contengan entradas para todos los equipos de la red. La única entrada que nunca aparece en la ARP caché es la que corresponde al propio host donde se ejecuta el comando arp. Para averiguar la dirección MAC (y la IP) del propio host debemos utilizar el comando **'ifconfig eth0'**.

Ahora cada alumno debe realizar desde su ordenador el siguiente proceso:

1. Lanzar un ping broadcast a la red: **'ping –b –c 5 10.0.1.255'**. (enviando cinco paquetes debe ser suficiente para conseguir respuesta de todos los hosts).

2. Ejecutar en una ventana de shell de su ordenador **'arp –a –n'** e **'ifconfig eth0'**. Anotar en una tabla la información obtenida sobre correspondencia entre direcciones IP y direcciones MAC. La tabla debe contener tres entradas, una entrada para cada dispositivo activo en la red (dos hosts y un conmutador).

[6] La dirección broadcast IP en una red se construye poniendo la parte de red de la dirección (en nuestro caso 10.0.1) seguida de una dirección toda unos para el resto.

3. Conectarse como consola al conmutador haciendo telnet a su dirección IP, entrar en modo Privilegiado, ejecutar el comando **'show mac-address-table'** y comprobar que las direcciones MAC que aparecen se encuentran en la interfaz que les corresponde, por ejemplo la dirección MAC del ordenador 10.0.1.12 (N2) debe estar asociada a la interfaz Ethernet 0/2 del Catalyst Norte.

Las entradas en la tabla de direcciones MAC del conmutador caducan al cabo de un tiempo, por lo que en ella solo aparecen los hosts activos (los que están enviando tráfico en ese momento, o que lo han hecho recientemente). El tiempo de vida de las entradas en los Catalyst 1900 es configurable, siendo su valor por defecto de 5 minutos. El comando en modo Privilegiado **'show mac-address-table aging-time'** nos muestra el tiempo de vida que tiene configurado el equipo en un momento dado. Para modificar su valor podemos utilizar el comando **'mac-address-table aging-time'** en modo Configuración Global; por ejemplo mediante el comando **'mac-address-table aging-time 120'** reducimos dicho tiempo a 2 minutos, obligando así a una más frecuente inundación de las tramas.

Ahora realizaremos un experimento consistente en lo siguiente:

- Reducimos el tiempo de vida a 30 segundos mediante el comando **'mac-address-table aging-time 30'** (en modo Configuración Global)

- Ponemos en marcha un **ping** desde el ordenador 1 al 2. En el ordenador 1 abrimos una ventana de consola del conmutador y comprobamos mediante el comando **'show mac-address-table'** (modo Privilegiado) que la tabla contiene las entradas correspondientes a las direcciones MAC correspondientes en las interfaces Ethernet 0/1 y Ethernet 0/2.

- Sin parar el **ping** desenchufamos el ordenador de la interfaz 2 y lo enchufamos en la interfaz 4 del conmutador. Observaremos que el ping empieza a fallar. Entonces repetiremos en la consola del conmutador el comando **'show mac-address-table'** donde podremos comprobar que la dirección MAC del ordenador 2 sigue asociada con la interfaz Ethernet 0/2 en vez de la Ethernet 0/4 en que se encuentra ahora. A continuación repetiremos el comando **'show mac-address-table'** varias veces hasta observar que la dirección MAC se asocia a la nueva interfaz, cosa que ocurre justo 30 segundos después de haber cambiado el cable, como podremos comprobar por el número de pings que fallan. Mientras la dirección MAC estaba asociada a la interfaz Ethernet 0/2 las tramas se perdían pues el conmutador seguía empeñado en enviarlas por él; en cambio una vez la dirección desaparece de la tabla el siguiente ping se envía por inundación a todas las interfaces y la primera respuesta recibida de la interfaz 4 hace que la dirección MAC aparezca enseguida asociada a la nueva interfaz.

Podemos provocar el rápido restablecimiento del ping si después de cambiar el cable tecleamos el comando **'clear mac-address-table'**, ya que de esta forma borramos toda la tabla, forzamos a que se realice la inundación y se localice la nueva ubicación del ordenador cambiado. El alumno devolverá ahora el ordenador 2, sin parar el ping, a su interfaz original; a continuación probará como mediante este comando la comunicación se restablece de forma inmediata.

Obsérvese que si las entradas en la tabla de direcciones MAC no caducaran nunca, entonces sería imposible localizar a un ordenador que se cambiara de interfaz en el conmutador, salvo que se utilizara el comando **'clear mac-address-table'** cada vez.

Parte 1.3: Interconexión de ambos conmutadores y prueba del Spanning Tree.

En esta parte de la práctica se realizan diversas interconexiones entre los dos conmutadores (Norte y Sur) de cada maqueta. Inicialmente se unen por una sola interfaz, con lo que se consigue conectividad entre ambos. Después se establece un segundo enlace creando un bucle, con lo que el Spanning Tree desactiva uno de ellos. A continuación se realizan diversos experimentos con el fin de alterar las decisiones adoptadas por el Spanning Tree.

Interconexión y creación de un bucle 10-100 entre ambos conmutadores

En primer lugar interconectaremos los dos conmutadores por la interfaz 6 (figura 5). Para ello utilizaremos un latiguillo Ethernet "crossover", es decir que cruce la señal de transmisión y recepción de

los dos extremos (si nos equivocamos y utilizamos un latiguillo normal no se estropea nada, lo único que ocurre es que no se establece el enlace). Una vez realizada esta conexión todos los ordenadores Norte y Sur pueden intercambiar tráfico entre sí. Los alumnos deberán comprobar que existe conectividad enviando pings a ordenadores conectados en el otro conmutador. Mediante el comando **'s in e 0/6'** (**'show interface ethernet 0/6'**) pueden observar como se incrementa el contador de tráfico en la interfaz 6. También podrán consultar la tabla de direcciones MAC del conmutador (comando **'show mac-address-table'**) y comprobarán que en la interfaz 6 aparecen las direcciones MAC correspondientes a los ordenadores del otro conmutador. Para averiguar las direcciones MAC de los ordenadores remotos se puede seguir el procedimiento indicado anteriormente, es decir lanzar desde el host un **'ping –b 10.0.1.255'** seguido del comando **'arp –a'**.

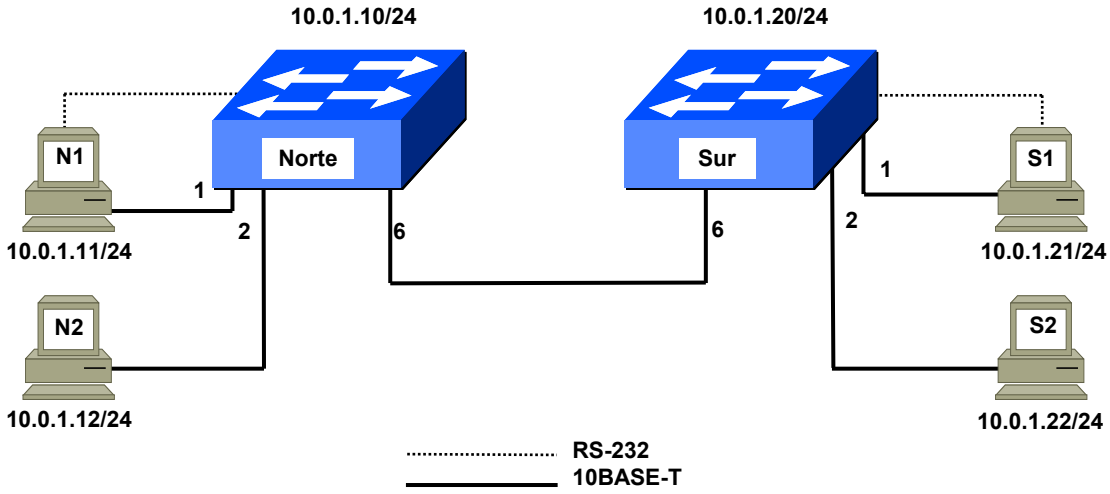

Figura 5. Interconexión de los conmutadores a 10 Mbps

Ahora haremos una prueba del protocolo Spanning Tree. En primer lugar reactivaremos el protocolo, ya que lo habíamos desactivado anteriormente. Para ello entramos en modo Configuración Global y tecleamos el comando **'spantree 1'** (salir con CTRL/Z). A continuación utilizaremos en modo Privilegiado el comando **'show spantree'**. para obtener información de la topología del Spanning Tree. La respuesta que obtendremos por consola será similar a la siguiente:

```
# show spantree 1
VLAN1 is executing the IEEE compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 00e0.1e69.2300
  Configured hell time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0053.4500.0000
  . . .
```

La dirección MAC que aparece en el campo 'Bridge Identifier' (en este ejemplo 00e0.1e69.2300) es el identificador de Spanning Tree de nuestro conmutador (este identificador está escrito además en una etiqueta situada en la parte superior del conmutador). El identificador que aparece en el campo 'Current root' (0053.4500.0000 en este ejemplo) es el identificador del conmutador raíz del árbol de spanning tree. Si ambos coinciden significa que este conmutador ha sido seleccionado como raíz. Si no coinciden significa que el raíz es el otro conmutador. Los alumnos podrán comprobar que en todas las maquetas el Catalyst Norte es elegido como conmutador raíz por tener el identificador más bajo. El comando **'show spantree 1'** muestra una información desglosada por interfaz que ocupa varias pantallas. En dicha información podemos ver que las interfaces Ethernet tienen asociado un costo de 100, mientras que las Fast Ethernet lo tienen de 10. Además podemos comprobar que todas las interfaces se encuentran en estado 'Forwarding' (aunque en este momento muchas de ellas no están operativas a nivel físico pues no tienen nada conectado).

Aunque el conmutador se identifica ediante una dirección MAC, en realidad posee 28 direcciones MAC diferentes consecutivas. La primera de ellas, que denominamos canónica, la utiliza para identificarse en todo lo relacionado con el protocolo Spanning Tree. Las 27 direcciones siguientes se asocian con sus 27 interfaces. Así por ejemplo si la dirección canónica es la **00e0.1e69.2300**, entonces la interfaz 1 (Ethernet 0/1) tendrá asociada la **00e0.1e69.2301**, la 2 la **00e0.1e69.2302** y así sucesivamente

hasta la **`00e0.1e69.231b`** que corresponderá con la interfaz 27 (FastEthernet 0/27). Las direcciones MAC del conmutador nunca figuran como direcciones de origen de las tramas que reenvía, pero sí se utilizan como direcciones de origen de las tramas que él mismo genera, como las del protocolo Spanning Tree, las del CDP (Cisco Discovery Protocol) o las respuestas a los mensajes de ping.

La salida generada en pantalla por el comando **`'show spantree'`** resulta incómoda pues nos muestra la información de todas las interfaces. Para averiguar la situación de Spanning Tree de una interfaz en particular (la 6 por ejemplo) es preferible utilizar el comando **`'s in e 0/6'`** (**`'show interface ethernet 0/6'`**); el estado de Spanning Tree aparece donde pone `'802.1d STP State:'`.

Procederemos ahora a interconectar ambos conmutadores a 100 Mb/s (figura 6) para crear un bucle entre ellos y analizar las decisiones que adopta el Spanning Tree. Antes de realizar la conexión a 100 Mb/s lanzaremos un **ping** entre dos ordenadores conectados a conmutadores diferentes a fin de monitorizar en tiempo real como evoluciona la conectividad entre ellos. A continuación realizaremos la conexión a 100 Mb/s utilizando la interfaz A, es decir la FastEthernet0/26 (100BASE-FX) en el Catalyst Norte y en el Sur. Se deberá utilizar un latiguillo de fibra óptica, que nos suministrará el profesor, cruzando el Transmit con el Receive, es decir el cable que se conecta al transmit en un conmutador debe conectarse al receive en el otro, y viceversa, Como resulta incómodo seguir el latiguillo para averiguar la correspondencia entre extremos lo más sencillo es conectar el latiguillo en ambos conmutadores de cualquier manera, y si no se establece el enlace (cosa que averiguaremos enseguida al ver que no se enciende la luz de link) invertiremos los conectores en uno de los dos lados.

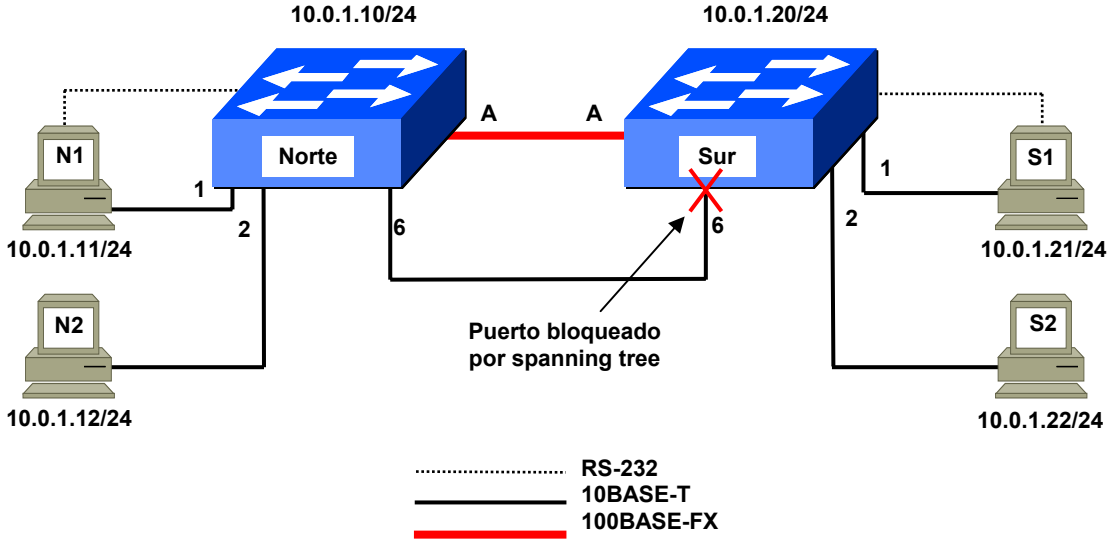

Figura 6. Interconexión de los conmutadores a 100 Mbps y Spanning Tree

Al realizar la conexión por la interfaz A sin desconectar la conexión por la 6 provocamos un bucle en la topología de la red con lo que el Spanning Tree cortará momentáneamente la comunicación entre ambos conmutadores. Al cabo de unos instantes, cuando los conmutadores han intercambiado sus BPDUs y han calculado la nueva topología el bucle se resuelve bloqueando la interfaz 6 en el Catalyst sur (la interfaz de mayor costo al raíz en el conmutador no raíz). Los alumnos deberán medir de forma aproximada el tiempo que dura la desconexión entre ambos conmutadores como consecuencia del cambio de topología utilizando para ello el ping que han dejado en marcha antes de realizar la conexión de 100 Mb/s. Además deberán observar la evolución de los LEDs en las interfaces 6 y A del Catalyst Sur (para esta prueba los LEDs deben estar en modo STAT). Si todo ocurre como es debido deberán observar que inicialmente se bloquean tanto la interfaz 6 como la A en el Catalyst Sur y los LEDs de ambas interfaces se ponen de color ámbar; al cabo de unos instantes, cuando la comunicación se restablece se deberá quedar en ámbar y bloqueada únicamente la interfaz 6 del Catalyst Sur.

Una vez recuperada la conectividad utilizaremos el comando **`'s in f 0/26'`** para comprobar que la interfaz A está en estado 'Forwarding' en ambos conmutadores, mientras que la interfaz 6 se encuentra en 'Forwarding' en el Catalyst Norte y en 'Blocking' en el Sur, impidiendo de este modo la comunicación efectiva a través de ese cable (comprobarlo mediante el comando **`'s in e 0/6'`** en el Catalyst Norte y

en el Sur). Obsérvese que para bloquear la comunicación solo es necesario bloquear la interfaz 6 en el Catalyst Sur, la del Catalyst Norte permanece Forwarding y por tanto ignora la situación. El bloqueo se produce en el conmutador no raíz, es decir en el Catalyst Sur, y se produce en la interfaz 6 (Ethernet) ya que por defecto tiene un costo de 100, mientras que la interfaz 26 (Fast Ethernet) tiene un costo 10. Si ahora generamos tráfico de un conmutador a otro podremos comprobar mediante el comando **'s in f 0/26'** que todo el tráfico discurre a través de la interfaz FastEthernet 0/26. También podremos comprobar con el comando **'show mac-address-table'** que las direcciones MAC del otro conmutador se ven ahora a través de la interfaz FastEthernet 0/26.

Ahora desconectaremos el latiguillo de la interfaz A en uno cualquiera de los dos conmutadores para comprobar como el Spanning Tree restablece, al cabo de unos instantes, la comunicación a través de la interfaz 6. Mediante el ping que tenemos lanzado entre un host del Catalyst Norte y uno del Sur comprobaremos que esto interrumpe la comunicación entre conmutadores hasta que de nuevo el Spanning Tree calcula la nueva topología, que finalmente termina desbloqueando la interfaz 6 del Catalyst Sur. Los cambios de estado que se producen pueden seguirse mediante los comandos **'s in e 0/6'** y **'s in f 0/26'**. Ejecutando repetidas veces el comando **'s in e 0/6'** en el Catalyst Sur, y con algo de suerte, podremos ver como la interfaz 6 evoluciona del estado 'Blocking' al estado 'Forwarding' (los estados intermedios, Learning y Listening no se dan en la configuración por defecto de estas interfaces). El estado de una interfaz también lo podemos ver por el color de su LED: ámbar significa que se encuentra en estado 'Blocking', mientras que verde indica que se encuentra en estado 'Forwarding'.

Una vez terminadas estas pruebas volveremos al estado anterior, es decir volveremos a conectar la interfaz A de ambos conmutadores y dejaremos conectada también la 6. Esto provocará que se rehabilite la conexión Fast Ethernet como vía de enlace entre ambos conmutadores.

Cambio de prioridad de Spanning Tree de un conmutador

Ahora repetiremos el comando **'show spantree 1'** y nos fijaremos en la segunda y cuarta líneas que nos muestran la prioridad de nuestro conmutador y la del conmutador raíz, respectivamente. Ambos tienen una prioridad de 32768, que es el valor por defecto. La prioridad se utiliza para alterar las decisiones que toma el algoritmo de Spanning Tree respecto a que conmutador debe actuar como raíz. A igual prioridad el Spanning Tree elige siempre como raíz al conmutador que tiene un identificador más bajo. En nuestro caso ese era el Catalyst Norte. Lo que haremos ahora es asignarle una prioridad inferior al Catalyst Sur, con lo que independientemente de cual sea su identificador el Spanning Tree lo elegirá a él como raíz. Bastará para ello con asignarle una prioridad una unidad por debajo del valor por defecto, es decir 32767.

Para ello, únicamente en el Catalyst Sur, teclearemos en modo Configuración Global el comando **'spantree-template 1 priority 32767'**. A continuación ambos grupos (Norte y Sur) teclearán de nuevo el comando **'show spantree 1'**, debiendo observar que la raíz del árbol es ahora el Catalyst Sur, es decir que el árbol se ha invertido. Para ver estos cambios de forma más clara los alumnos pueden abrir dos ventanas telnet en cada ordenador, una contra cada Catalyst, de forma que en una sola pantalla puedan tener abiertas las consolas de los dos conmutadores y puedan seguir la evolución del Spanning Tree en ambos equipos.

Aunque hemos cambiado el raíz y le hemos dado la vuelta al árbol el camino elegido sigue siendo el enlace en fibra que une las interfaces A, ya que los costos de las interfaces son iguales en ambos conmutadores, es decir 100 para las Ethernet y 10 para las FastEthernet. Sin embargo, al ser ahora raíz el Catalyst Sur el bloqueo se produce en la interfaz 6 del Catalyst Norte, como se puede comprobar por el cambio de color de los LEDs de la interfaz 6 en ambos conmutadores.

Cambio del costo en una interfaz

Para alterar la decisión en cuanto a caminos hacia el raíz del Spanning Tree vamos a modificar ahora los costos. Lo que haremos es asociar a la interfaz 6 en el Catalyst Norte (que actualmente no es raíz) un costo de 8; de esta forma ese conmutador la elegirá como interfaz raíz, es decir como su camino de menor coste hacia el raíz, bloqueando el puerto A, es decir tomará una decisión que no es óptima debido a que le suministramos información errónea en cuanto a costos. Para cambiar el costo de la interfaz 6 entraremos, solo en el Catalyst Norte, en modo Configuración de Interfaz para la interfaz Ethernet 0/6 y teclearemos el comando **'spantree cost 8'** como se muestra a continuación:

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
(config)#int eth0/6
(config-if)#spantree cost 8
(config-if)#exit
(config)# CTRL/Z
#
```

Una vez modificado el costo veremos que en el Catalyst Norte la interfaz A cambia de color verde a ámbar y la 6 de ámbar a verde. Podemos utilizar también el comando **'show spantree'** para comprobar que la interfaz 6 está ahora 'Forwarding' y que la 26 está 'Blocked'.

Con el costo de la interfaz 6 cambiado en el Catalyst Norte volveremos ahora el árbol a su situación inicial, es decir volveremos a poner el Norte como raíz. Para ello le daremos al Catalyst Norte la misma prioridad que le dimos antes al Sur, es decir 32767. De esta forma vuelve a prevalecer el orden basado únicamente en el identificador. Para cambiar la prioridad procedemos como antes, utilizando en modo Configuración Global el comando **'spantree-template 1 priority 32767'**. Podemos comprobar que el árbol vuelve a su estado original con el comando **'show spantree 1'**. Sin embargo ahora el bloqueo se produce en la interfaz 6 como al principio y no en la A, a pesar del cambio de costos que habíamos efectuado en el Catalyst Norte. En realidad los costos de las interfaces en el conmutador raíz carecen de importancia ya que nunca intervienen en el cálculo de costos. En nuestro caso el Catalyst Sur calculará el costo de sus caminos al raíz en base a sus propios costos únicamente, sin utilizar para nada los costos de las interfaces en el Catalyst Norte. Si ahora volvemos a su valor normal el costo de la interfaz 6 en el Catalyst Norte (comando **'spantree cost 100'**. en modo Configuración de Interfaz) podremos comprobar que esto no tiene ninguna consecuencia en la topología del Spanning Tree.

Desactivación del Spanning Tree en el Catalyst Norte y cambio de la prioridad de una interfaz

Ahora vamos a desactivar el Spanning Tree en el Catalyst Norte (**'no spantree 1'** en modo Configuración Global). Esto provoca que el Catalyst Sur se quede solo ejecutando el Spanning Tree. En esas circunstancias el Catalyst Sur es elegido inmediatamente como raíz de un árbol formado por él únicamente. A efectos del Spanning Tree el Catalyst Norte ahora no existe, se comporta como si fuera un hub (ha dejado de enviar BPDUs propias aunque reenvía las que recibe del Catalyst Sur pues van dirigidas a una dirección multicast que para él es transparente). Al detectar un bucle entre sus interfaces 6 y 26 el Catalyst Sur tiene que desactivar una de las dos. Pero en este caso el costo al raíz es cero, pues él mismo es el raíz. El empate en costos lo resuelve el Spanning Tree bloqueando la interfaz con identificador (o número)más elevado, es decir la A o Fast Ethernet 0/26 en este caso. Paradójicamente se ha tomado la decisión errónea, puesto que la interfaz 26 era precisamente la que nos ofrecía una conexión de mayor velocidad con el Catalyst Norte.

Esta decisión del Spanning Tree no podemos alterarla cambiando los costos como antes, ya que estos son ahora irrelevantes (el costo al raíz siempre será cero). En su lugar debemos actuar sobre el parámetro prioridad de la interfaz, que actúa de forma análoga a la prioridad del conmutador que antes hemos modificado, pero en este caso a nivel de interfaz. Una prioridad más baja prevalece siempre en la elección del camino, independientemente de cual sea el identificador de la interfaz. Así pues, para forzar que la interfaz 26 se elija antes que la 6 simplemente debemos asignarle una prioridad menor. El rango de prioridades posibles en interfaces es de 0 a 255 y el valor por defecto 128, por lo que utilizaremos el valor 127 para situar al puerto 26 por delante del puerto 6. Utilizaremos para hacer el cambio el comando **'spantree priority'** en el modo Configuración de Interfaz, según se indica a continuación:

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
(config)#int f0/26
(config-if)#spantree priority 127
(config-if)#exit
 (config)# CTRL/Z
#
```

Desactivación del Spanning Tree en el Catalyst Sur

Para terminar esta sesión procederemos a realizar una desactivación completa del Spanning Tree. Para evitar interferencias antes desactivaremos el protocolo CDP en los puertos 6 y 26, que son los que interconectan los conmutadores. Para ello ejecutaremos el comando **'no cdp enable'** en el modo Configuración de Interfaz de ambas interfaces, tecleando la siguiente secuencia de comandos:

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
(config)#int eth 0/6
(config-if)#no cdp enable
(config)#int Fast 0/26
(config-if)#no cdp enable
(config-if)#CTRL/Z
#
```

A continuación procederemos de la siguiente forma:

1. Lanzamos un ping desde un ordenador del Catalyst Norte a uno del Catalyst Sur (por ejemplo de N1 a S1). Comprobamos que la comunicación discurre normalmente. Pondremos los LEDs de los dos Catalyst en modo UTL para ver mejor la evolución del tráfico en los conmutadores.

2. Desactivamos el Spanning Tree en el Catalyst Sur mediante el comando **'no spantree 1'** en modo Configuración Global. Al Catalyst Norte ya le habíamos desactivado el Spannng Tree anteriormente, por lo que ahora estamos funcionando con una red en bucle y sin Spanning Tree. Pero el ping sigue funcionando con normalidad ya que, aunque hay un bucle, las direcciones MAC de los ordenadores que están haciendo el ping se encuentran en las tablas de los conmutadores, de forma que las tramas se envían únicamente por las interfaces correspondientes y no hay riesgo de saturar la red. Los LEDs de los conmutadores muestran una actividad normal, de momento.

3. Ahora lanzamos desde cualquier ordenador (del Norte o del Sur) un ping de un solo paquete a una dirección inexistente de nuestra red (**'ping –c 1 10.0.1.100'** por ejemplo). Esto provocará el envío de un paquete broadcast, que se enviará a toda la red y por tanto llegará al otro conmutador dos veces, una por el puerto 6 y otra por el 26. El otro conmutador reenviará ambos paquetes por las interfaces contrarias a las que los recibió, de forma que en unos instantes se saturan todos los enlaces y se bloquea la red.

A partir de ese momento veremos por los LEDs que la actividad del conmutador crece de forma considerable. Si pasamos los LEDs a modo STAT veremos que todos los puertos activos parpadean frenéticamente, y nos resultará muy difícil conectarnos a la consola del conmutador vía telnet. Si no lo conseguimos lo haremos por la interfaz serie (ventana minicom en el host 1) y una vez dentro haremos un **'clear counters'** seguido de **'show interfaces'**, con lo que podremos comprobar que el conmutador está enviando una cantidad de tráfico increíblemente elevada por todos sus puertos. Dicho tráfico se debe exclusivamente a la primera trama broadcast enviada por el ping, que ambos conmutadores han ido propagando y duplicando exponencialmente.

SEGUNDA SESIÓN.

Antes de proceder a realizar las tareas propias de esta sesión debemos repetir algunas de las labores efectuadas en la sesión anterior a fin de crear un entorno adecuado para el desarrollo de la práctica.

En primer lugar procederemos, con todos los equipos apagados, a realizar las conexiones que aparecen en el esquema de la figura 5, como hicimos en la primera sesión. Conectaremos la interfaz de consola del Catalyst 1900 a la interfaz serie (COM1) del ordenador 1 (N1 ó S1) y las tarjetas Ethernet de los ordenadores a las interfaces 1 y 2 (10BASE-T) del Catalyst 1900, utilizando para ello el latiguillo que conecta el ordenador a la red de la Universidad, que desconectaremos de la roseta de la pared para conectar al Catalyst.

Una vez conectados todos los cables encenderemos los ordenadores y seleccionaremos como sistema operativo 'linux redes'. Una vez arrancado el sistema entraremos con el usuario **'root'** y la password utilizada en la sesión anterior, que ya conocemos.

A continuación configuraremos la dirección IP de los hosts como ya hicimos en la primera sesión de esta práctica y utilizando las direcciones, que figuran en la tabla 2. Para introducir la dirección IP utilizaremos el comando **'ifconfig eth0 inet *dirección_IP* netmask 255.255.255.0'** donde *'dirección_IP'* es la dirección IP que corresponde a cada host. Deberemos comprobar mediante el comando **'ifconfig eth0'** que la dirección se ha introducido correctamente.

Ahora en el ordenador 1 abriremos una ventana de shell y entraremos en la consola del conmutador mediante el programa minicom (comando **'minicom –s'** seguido de la tecla escape).

A continuación debemos restaurar la configuración de fábrica del conmutador siguiendo el mismo procedimiento que en la primera sesión. Encendemos el conmutador y entramos por consola tecleando **'K'** para elegir la modalidad de línea de comandos, luego pasamos a modo Privilegiado mediante el comando **'enable'**; si el equipo no tiene password configurada aparecerá enseguida el prompt **'#'**, en caso contrario nos pedirá una password que normalmente será **'genios'** (en caso contrario preguntar al profesor). Para restaurar la configuración de fábrica usaremos el comando **'delete nvram'**. Se pide confirmación y en unos 10 segundos el equipo esta nuevamente operativo.

Como hemos borrado toda la configuración del conmutador tenemos que asignarle una dirección IP. Para ello utilizaremos el comando **'ip address'** en modo Configuración Global y asignaremos la misma dirección y máscara que en la sesión anterior, según figura en la tabla 3.

Una vez realizadas todas las conexiones y configuraciones preliminares comprobaremos mediante el comando ping que tanto los hosts como el conmutador funcionan normalmente.

Parte 2.1: Crear dos VLANs y comunicarlas

En esta parte de la práctica se crearán dos VLANs en cada conmutador y se asignarán los puertos a una u otra. A continuación conectaremos entre sí ambos conmutadores , primero en una VLAN y luego en la otra. Por último comunicaremos ambas VLANs entre sí mediante un latiguillo puente.

A las VLANs las llamaremos 'pares' y 'nones' y les asignaremos los números 2 y 3 respectivamente (el número 1 está reservado para la VLAN 'default', que es la que viene por defecto configurada en el equipo). Para crear las VLANs entraremos en consola del conmutador y utilizaremos en modo Configuración Global el comando **'vlan'** según se muestra a continuación:

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
(config)#vlan 2 name pares
(config)#vlan 3 name nones
(config)#CTRL/Z
#
```

Ahora podemos utilizar el comando **'show vlan'** para comprobar que las definiciones se han realizado correctamente. Lo que aparece por pantalla debe ser similar a lo siguiente:

```
#show vlan
VLAN Name             Status     Ports
-------------------------------------
1    default          Enabled    1-24, AUI, A, B
2    pares            Enabled
3    nones            Enabled
1002 fddi-default     Suspended
1003 token-ring-defau Suspended
1004 fddinet-default  Suspended
1005 trnet-default    Suspended
-------------------------------------

VLAN Type           SAID   MTU    Parent RingNo BridgeNo Stp  Trans1 Trans2
------------------------------------------------------------------------------
1    Ethernet       100001 1500   0      0      0        Unkn 1002   1003
2    Ethernet       100002 1500   0      1      1        Unkn 0      0
3    Ethernet       100003 1500   0      1      1        Unkn 0      0
1002 FDDI           101002 1500   0      0      0        Unkn 1      1003
1003 Token-Ring     101003 1500   1005   1      0        Unkn 1      1002
1004 FDDI-Net       101004 1500   0      0      1        IEEE 0      0
1005 Token-Ring-Net 101005 1500   0      0      1        IEEE 0      0
------------------------------------------------------------------------------
#
```

Una vez creadas las VLANs podemos asignar los puertos. Si un puerto no lo asignamos a ninguna quedará en la VLAN 'default' (la 1) que es en la que se encuentran todos inicialmente. Únicamente asignaremos los puertos 1, 2, 5, 6, 7 y 8 en el Catalyst Norte y 1, 2, 5 y 6 en el Sur, los pares a la VLAN 'pares' y los impares a la VLAN 'nones'. Para ello utilizaremos en el modo Configuración de Interfaz, el comando **'vlan-membership'**. Esta configuración debemos realizarla desde una ventana minicom (no telnet) del ordenador 1, ya que de lo contrario la sesión se interrumpirá en el momento asignemos la interfaz por la cual estamos conectados. La secuencia de comandos a utilizar, por ejemplo en el Catalyst Norte, es la siguiente:

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
(config)#i e 0/1
(config-if)#vlan-membership static 3
(config-if)#i e 0/2
(config-if)#vlan-membership static 2
(config-if)#i e 0/5
(config-if)#vlan-membership static 3
(config-if)#i e 0/6
(config-if)#vlan-membership static 2
(config-if)#i e 0/7
(config-if)#vlan-membership static 3
(config-if)#i e 0/8
(config-if)#vlan-membership static 2
(config-if)#exit
(config)#CTRL/Z
#
```

Recordemos que la tecla **CTRL/P** (o flecha arriba) repite el comando anterior, lo cual facilita la introducción repetida de un mismo comando, algo especialmente útil en este caso. Si repetimos ahora el comando **'show vlan'** obtendremos un resultado como el siguiente:

```
#show vlan
VLAN Name             Status     Ports
-------------------------------------
1    default          Enabled    3, 4, 9-24, AUI, A, B
2    pares            Enabled    2, 6, 8
3    nones            Enabled    1, 5, 7
1002 fddi-default     Suspended
1003 token-ring-defau Suspended
1004 fddinet-default  Suspended
1005 trnet-default    Suspended
-------------------------------------

VLAN Type           SAID   MTU    Parent RingNo BridgeNo Stp  Trans1 Trans2
------------------------------------------------------------------------------
1    Ethernet       100001 1500   0      0      0        Unkn 1002   1003
2    Ethernet       100002 1500   0      1      1        Unkn 0      0
```

```
3    Ethernet       100003 1500   0      1      1        Unkn 0      0
1002 FDDI           101002 1500   0      0      0        Unkn 1      1003
1003 Token-Ring     101003 1500   1005   1      0        Unkn 1      1002
1004 FDDI-Net       101004 1500   0      0      1        IEEE 0      0
1005 Token-Ring-Net 101005 1500   0      0      1        IEEE 0      0
--------------------------------------------------------------------------
#
```

Una vez asignadas las interfaces a las VLANs los alumnos comprobarán que los ordenadores conectados a la VLAN nones (N1 y S1) tienen conectividad entre si y los pares (N2 y S2) entre ellos, pero no hay comunicación entre ordenadores de diferente paridad..

La definición de las dos nuevas VLANs equivale a haber creado dos conmutadores 'virtuales', cada uno formado por los puertos que hemos asignado a esa VLAN. Además existe un tercer conmutador 'virtual' que es el formado por los puertos que no hemos asignado a ninguna VLAN y que permanecen en la VLAN default. Como hemos podido comprobar los ordenadores conectados a diferentes VLANs no pueden comunicarse entre sí.

Antes hemos asignado una dirección IP al conmutador. En teoría podríamos hacer ahora telnet o ping hacia esa dirección desde cualquier ordenador conectado. Sin embargo al crear las VLANs hemos perdido la comunicación con él, no podremos acceder desde ninguna de las VLANs que hemos creado. ¿A que se debe esto? Resulta que el conmutador en sí mismo, aunque no está físicamente conectado a ninguna interfaz, también se ha de asignar a alguna VLAN, y si no se asigna a ninguna se encuentra en la VLAN default. Por tanto para acceder al conmutador tendríamos que tener conectado algún ordenador a la VLAN default, pero no tenemos ninguno. Para recuperar el acceso asignaremos el conmutador a la VLAN 3 (nones). De esta forma podremos acceder a él desde los ordenadores nones, pero no desde los pares. Para asignar el conmutador a la VLAN nones utilizaremos en modo Configuración Global el comando **'ip mgmt-vlan'**. Este comando lo debemos ejecutar desde la consola minicom del ordenador 1, ya que en estos momentos no tenemos conexión por telnet con el conmutador. La secuencia de comandos es la siguiente:

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
 (config)#ip mgmt-vlan 2
(config)#CTRL/Z
```

Una vez realizado el cambio de VLAN del conmutador comprobaremos que es posible hacerle ping o telnet desde ordenadores de la VLAN nones.

A continuación realizaremos una conexión entre ambos conmutadores mediante la interfaz 6, tal y como hicimos en la sesión anterior (figura 4). (Recordemos que para esta conexión debe utilizarse un latiguillo curzado o 'crossover'). Pero ahora esa interfaz pertenece a la VLAN pares, por lo que con esa conexión solo podrán comunicarse entre los dos Catalyst los ordenadores de la VLAN pares. Los alumnos deberán comprobar que en efecto la comunicación entre los ordenadores N2 y S2 es posible, pero no entre N1 y S1.

Para conseguir comunicación entre N1 y S1 uniremos la interfaz 5 de ambos conmutadores mediante otro latiguillo crossover (figura 7). Una vez hecho esto comprobaremos que hay comunicación N1-S1. Sin embargo sigue sin haber comunicación pares-nones en ningún caso.

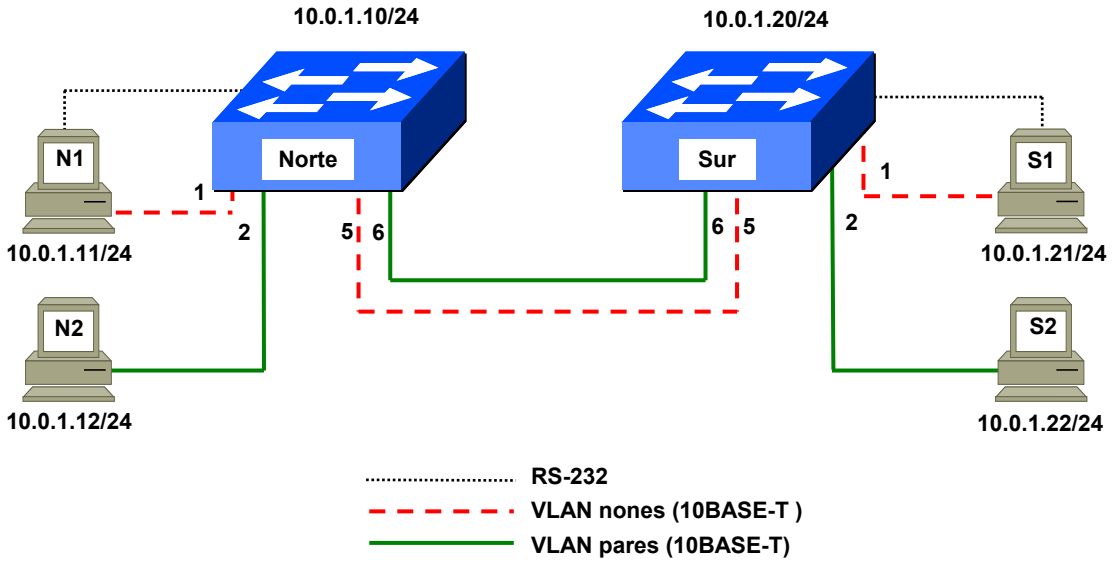

Figura 7. Conexión independiente de las VLANs 'pares' y 'nones'

Obsérvese que en este caso tenemos dos enlaces simultáneamente activos entre ambos conmutadores y ninguno de ellos es desactivado por el Spanning Tree (no hay ningún LED ámbar). Esta aparente paradoja se debe a que el algoritmo Spanning Tree se ejecuta de forma independiente para cada VLAN. Recordemos que a todos los efectos la configuración de VLANs que hemos realizado equivale a partir lógicamente cada conmutador en tres, dos con los puertos asignados a las VLANs pares y nones y uno con el resto (VLAN default). Esto puede comprobarse tecleando el comando **`'show spantree'`** que ahora nos mostrará información relativa a tres Spanning Tree independientes, uno por cada VLAN. Para ver únicamente la información de Spanning Tree relativa a una VLAN debemos indicar el número; por ejemplo el comando **`'show spantree 3'`** nos mostrará únicamente la información relativa a la VLAN 3 (nones).

Conexión directa entre VLANs mediante un latiguillo

Ahora interconectaremos las dos VLANs que hemos creado mediante un latiguillo "crossover" que haga de puente entre ellas. Usaremos para ello las interfaces 7 y 8 del Catalyst Norte, según se indica en la figura 8 (esta es la razón por la que anteriormente hemos asignado esas interfaces a las VLANs nones y pares, respectivamente).

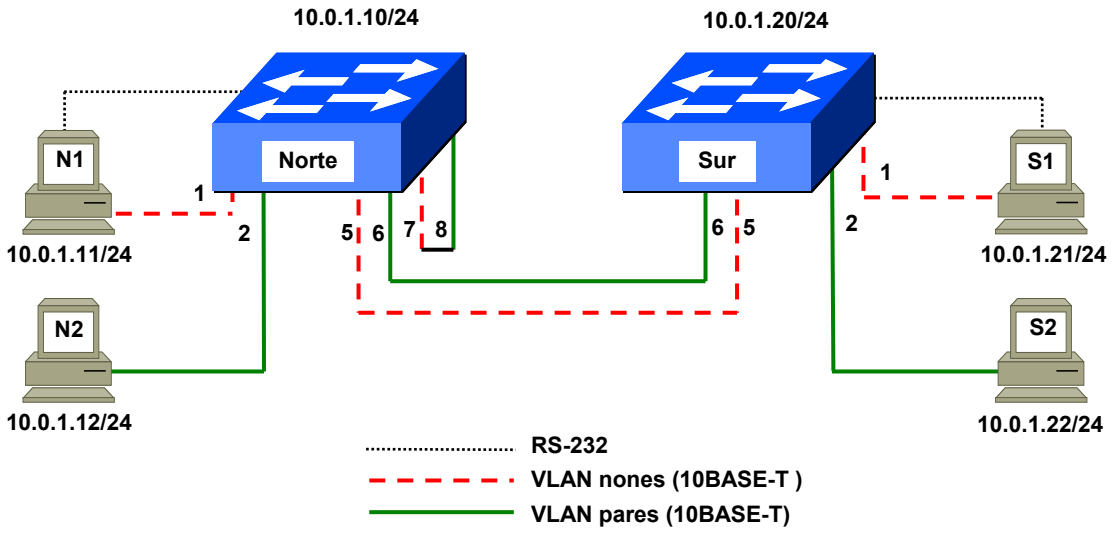

Figura 8. Interconexión de las dos VLANs mediante un latiguillo puente

Una vez realizada la conexión podremos comprobar como se recupera la conectividad entre las dos VLANs en toda la red, uniéndolas como si fueran una.

Una vez terminada esta prueba retiraremos el latiguillo que une los puertos 7 y 8.

Al unir VLANs como lo hemos hecho aquí se recupera la conectividad, pero también se agrega el tráfico broadcast/multicast, cuya separación era precisamente el principal motivo de crear las VLANs. Obviamente si queríamos unir las VLANs de esta forma habría sido más sencillo y eficiente no haberlas creado. Normalmente nunca se unen VLANs de esta forma, aquí lo hemos hecho a modo de demostración con fines pedagógicos. La manera habitual de unir VLANs es mediante un router, que es lo que haremos más adelante en la parte 2.3.

Parte 2.2: Configuración de un enlace 'trunk'.

Vamos a proceder ahora a interconectar de los dos conmutadores a 100 Mb/s. Como disponemos de dos interfaces de este tipo (A y B) bastaría con asignar una a la VLAN pares y otro a la nones y conectar ambas entre los dos conmutadores, como hemos hecho antes. Sin embargo esta solución presenta tres inconvenientes:

- Requiere utilizar dos cables para la conexión de los conmutadores.
- Consume todos los puertos Fast Ethernet de los conmutadores, por lo que ya no sería posible realizar otras conexiones a 100 Mb/s en ellos.
- No se podría utilizar si hubiera más de dos VLANs (salvo que hiciéramos uso de los puertos de 10 Mb/s).

Para evitar esos problemas utilizaremos un enlace trunk, que nos permite enviar por un solo enlace el tráfico de varias VLANs.

Para enviar por un enlace tráfico de varias VLANs sin riesgo de mezclarlas es preciso etiquetar de alguna manera las tramas que se envían. La norma IEEE 802.1Q establece una forma estándar de realizar ese etiquetado (también llamado encapsulado) pero los Catalyst 1900 son anteriores a dicho estándar por lo que no lo soportan. En su lugar utilizan un etiquetado anterior propietario de Cisco que se denomina ISL (Inter. Switch Link). Como en nuestro caso los dos conmutadores son del mismo modelo ambos utilizan el mismo etiquetado y esto no plantea ningún problema de interoperabilidad, pero podría serlo si quisiéramos integrar en la red equipos que no soportaran ISL.

En esta parte de la práctica configuraremos la interfaz A (FastEthernet 0/26) de cada conmutador como enlace trunk (figura 9). De este modo esa interfaz no estará asignada a ninguna VLAN en particular sino a todas a la vez y podrá redirigir tramas pertenecientes a cualquiera de las VLANs existentes en ambos conmutadores. Así un enlace será suficiente para la conexión de los dos conmutadores, independientemente del número de VLANs que se configuren en ellos.

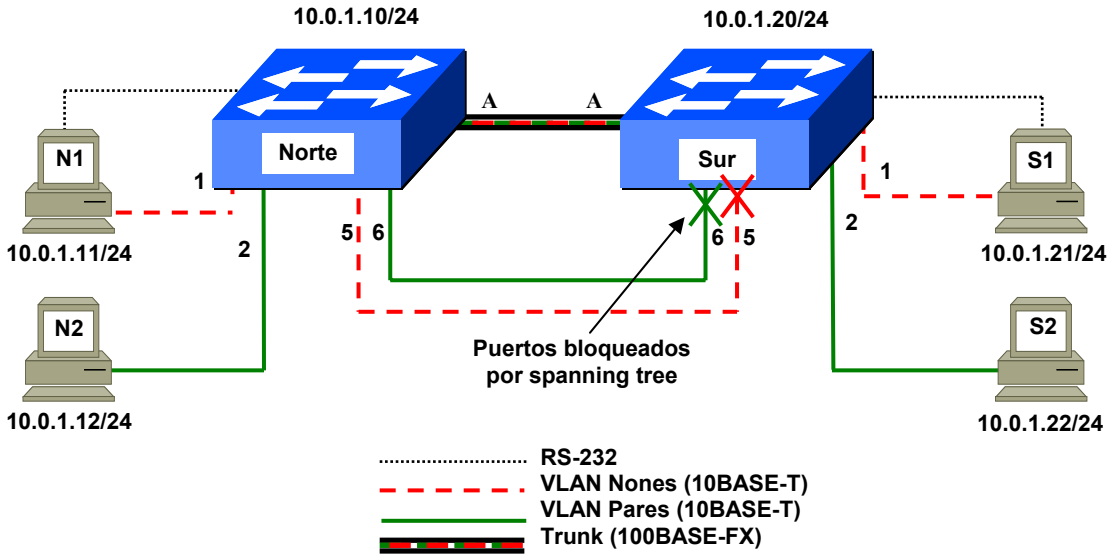

Figura 9. Creación de un enlace 'Trunk'

Para configurar una interfaz en modo trunk utilizamos el comando **'trunk'** dentro del modo Configuración de Interfaz correspondiente a la interfaz que se quiere modificar. La secuencia de comandos en nuestro caso es la siguiente:

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
(config)#i f 0/26
(config-if)#trunk on
(config-if)#exit
(config)#CTRL/Z
#
```

Podemos comprobar que la configuración se ha realizado correctamente tecleando el comando en modo Privilegiado **'show trunk A'**(A corresponde al puerto 26). Una vez hecho el cambio en ambos conmutadores los conectaremos por dicho puerto. Al realizar la conexión producimos un bucle en las VLANs pares y nones, por lo que los puertos 5 y 6 pasarán a estado **'Blocking'** en el Catalyst Sur, como era de esperar pues recordemos que el Catalyst Norte es el raíz. Esto lo podemos comprobar mediante el comando **'s in e 0/5'** y **'s in e 0/6'** en el Catalyst Sur, o más fácilmente mirando como los LEDs correspondientes a estos puertos cambian a color ámbar. En el caso de la interfaz A (FastEthernet 0/26) al estar en modo trunk el comando **'show interface f 0/26'** no nos suministra información de Spanning Tree.

Una vez estabilizada la topología del Spanning Tree comprobaremos que sigue habiendo conectividad entre ordenadores de la misma VLAN, independientemente de que se encuentren en el mismo o en diferentes conmutadores.

Parte 2.3: Interconexión de las VLANs mediante routers

Conexión de las VLANs mediante un router

A continuación interconectaremos las dos VLANs mediante un router, que como ya hemos comentado es la manera normal de hacerlo.

Pero antes de conectarlas mediante un router debemos separar nuestras dos VLANs en dos redes IP diferentes. Hasta ahora hemos venido utilizando para todos los ordenadores direcciones de una misma red IP, la 10.0.1.0/24 (máscara 255.255.255.0); esta red abarca todas las direcciones que empiezan por 10.0.1, es decir desde la 10.0.1.1 hasta la 10.0.1.254. Esto era normal cuando todos los ordenadores pertenecían a la misma VLAN, y también cuando estando en VLANs diferentes las uníamos mediante un latiguillo puente. Pero como ahora queremos que las dos VLANs se unan mediante un router debemos asignarles

direcciones de redes diferentes. Usaremos pues la red 10.0.2.0/24 (máscara 255.255.255.0) para la VLAN pares y la 10.0.3.0/24 (máscara 255.255.255.0) para la VLAN nones. Estas redes IP abarcan las direcciones que empiezan por 10.0.2 y por 10.0.3 (rangos 10.0.2.1-254 y 10.0.3.1-254, respectivamente). Habrá por tanto una correspondencia biunívoca entre las VLANs y las redes IP. Además debemos asignar a cada host un router por defecto, que será el que utilizará para comunicar con otros que no pertenezcan a su misma red IP (es decir a su misma VLAN). Los valores que debemos asignar ahora a los hosts son los que figuran en la tabla 5:

Grupo Norte		
Ordenador	**Dirección IP**	**Router por defecto**
N1	10.0.3.11	10.0.3.15
N2	10.0.2.12	10.0.2.15
Grupo Sur		
Ordenador	**Dirección IP**	**Router por defecto**
S1	10.0.3.21	10.0.3.15
S2	10.0.2.22	10.0.2.15

Tabla 5. Configuración de red de los ordenadores.

COMANDO 'route'

El comando **'route'** (disponible en UNIX y en Windows) permite definir el router por defecto en un host. También permite definir tablas de rutas complejas, aunque eso no nos interesa ahora.

Para definir el router por defecto se utiliza la siguiente sintaxis del comando route:

```
route add default gw direccion_IP_del_router
```

La dirección del router debe pertenecer a la msima red que la dirección del host donde ejecutamos el comando. En las redes que estamos utilizando en esta práctica (con máscara 255.255.255.0) la red queda especificada por los tres primeros bytes, por lo que si el host tiene una dirección (asignada con '**ifconfig**') que empieza por 10.0.3 la dirección del router debe necesariamente empezar por 10.0.3.

El comando route sin argumentos nos permite comprobar que dirección tenemos configurada para el router por defecto. Para evitar problemas con la resolución de nombres, que no está disponible en la red del laboratorio, debemos utilizar la opción –n, por lo que el comando sería:

```
route -n
```

Para introducir la dirección IP utilizaremos como siempre el comando '**ifconfig eth0 inet *dirección_IP* netmask 255.255.255.0**'. Para introducir el router por defecto usaremos el comando '**route add default gw *dirección_IP***'. Por ejemplo en el host S2 teclearemos los comandos '**ifconfig eth0 inet 10.0.2.22**' y '**route add default gw 10.0.2.15**'.

Para comprobar que el cambio de dirección IP ha sido realizado correctamente utilizaremos el comando '**ifconfig eth0**'. Para comprobar que la definición del router por defecto se ha realizado correctamente utilizaremos el comando '**route –n**'.

Ahora debemos modificar las direcciones IP de los Catalyst, y asignarles también un router por defecto. Recordemos que hemos elegido que la VLAN nones actúe como VLAN de gestión de los Catalyst, por lo que les debemos asignar direcciones que pertenezcan a dicha VLAN. Para asignar las direcciones IP utilizamos el comando '**ip address**', mientras que para asignar el router por defecto emplearemos el

comando **'ip default-gateway'**, ambos en modo Configuración Global. Los datos a introducir son los siguientes:

Conmutador	IP Address	Subnet Mask	Default Gateway
Catalyst Norte	10.0.3.10	255.255.255.0	10.0.3.15
Catalyst Sur	10.0.3.20	255.255.255.0	10.0.3.15

Tabla 6. Configuración de red de los conmutadores.

La secuencia de comandos, por ejemplo para el Catalyst Sur, será la siguiente:

```
#config
Enter configuration commands, one per line.  End with CNTL/Z
(config)#ip address 10.0.3.20 255.255.255.0
(config)#ip default-gateway 10.0.3.15
(config)#CTRL/Z
```

Para la interconexión de los conmutadores se ha suministrado a los alumnos del Catalyst Norte un router (RN) preconfigurado con dos interfaces Ethernet. El router dispone además de interfaces serie que no se utilizan en esta práctica. El modelo de router puede variar en función del material disponible en cada momento. En algunos equipos las interfaces Ethernet se identifican exteriormente como **'Ethernet 0'** y **'Ethernet 1'** (routers antiguos) o bien como **'AUI 0'** y **'AUI 1'** (routers modernos). A nivel de configuración las interfaces se denominan **'Ethernet 0'** y **'Ethernet 1'** respectivamente en todos los modelos.

En todos los casos las interfaces Ethernet de los routers tienen un conector AUI al que se le ha conectado un transceiver 10BASE-T. Por lo tanto los alumnos deberán utilizar para las conexiones latiguillos RJ45 normales (no cruzados).

El router RN está preconfigurado de la siguiente manera:

Interfaz	Dirección IP	Máscara
Ethernet 0	10.0.2.15	255.255.255.0
Ethernet 1	10.0.3.15	255.255.255.0

Tabla 7. Configuración del router RN (edificio Norte)

La configuración del router está preparada para conmutar paquetes entre las dos redes IP

Los alumnos deben ahora conectar el router según se muestra en el esquema de la figura 10, es decir la interfaz Ethernet 0 (o AUI 0) a la interfaz 6 del Catalyst Norte, y la Ethernet 1 (AUI 1) a la interfaz 5. Es importante realizar las conexiones correctamente ya que si se invierten los cables la comunicación a través del router no será posible.

Una vez conectados todos los cables encenderemos el router.

OJO: En uno de los routers antiguos (CGS) si el router se enciende antes de conectar los cables las interfaces Ethernet no funcionan. Si se observan problemas en el funcionamiento de este router y no se está seguro de haber conectado los cables antes de encenderlo se debe apagar y encender el router.

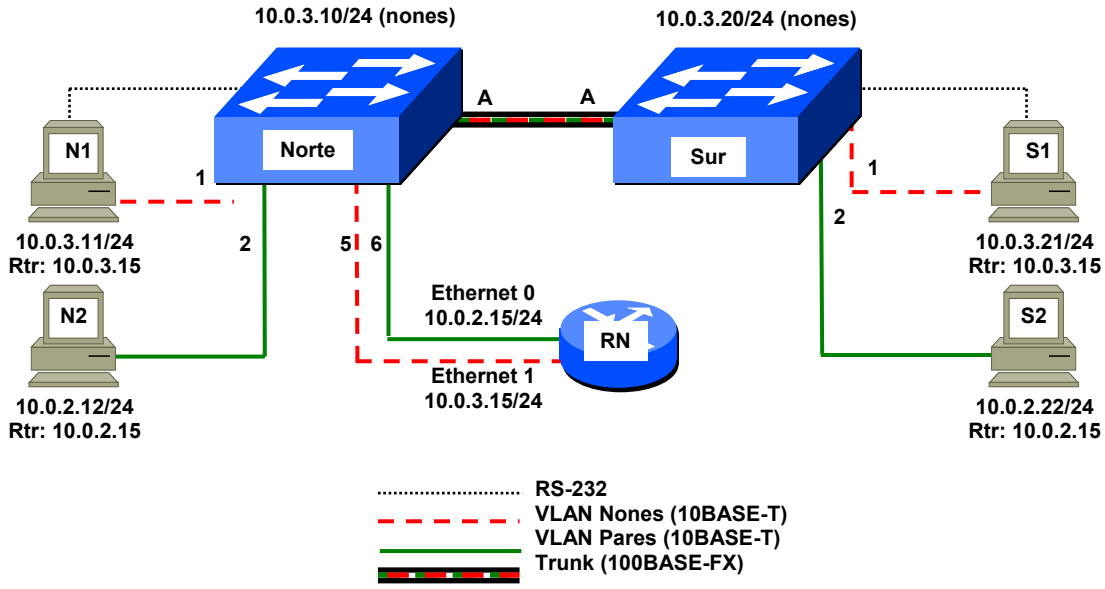

Figura 10. Interconexión física de las dos VLANs mediante un router

Ahora los alumnos deberán comprobar que es posible la comunicación entre cualquier par de hosts. En caso de problemas se puede probar a hacer un ping a la interfaz del router que se encuentra en nuestra misma VLAN, por ejemplo si es un ordenador de la VLAN nones haremos ping a 10.0.3.15.

Los hosts que se encuentran en la misma VLAN se comunican directamente, mientras que los que están en VLANs diferentes lo hacen a través del router. Esto se puede comprobar generando tráfico masivo entre dos ordenadores de diferente VLAN (por ejemplo con **'ping -f'**) y observando el tráfico en las interfaces 5 y 6 del Catalyst Norte (bien por el parpadeo de los LEDs o por los contadores del comando **'s in e 0/5'** y **'s in e 0/6'**). También es posible observar el tráfico haciendo telnet al router por cualquiera de sus dos direcciones IP (la password para entrar es **'genios'**). El router tiene un lenguaje de comandos similar al del Catalyst, por lo que podemos utilizar por ejemplo los comandos **'show interface ethernet 0'** y **'show interface ethernet 1'** con los que nos suministra una serie de contadores de tráfico. Aunque la forma de presentarlos es bastante diferente a la de los 1900, hay dos de esos contadores que son especialmente útiles, ya que nos muestran el tráfico promedio habido durante los últimos cinco minutos en cada sentido (`'5 minute input rate'`.y `'5 minute output rate'`). Si lanzamos un **'ping -f'** que atraviese el router y miramos como evolucionan estos dos contadores veremos que se incrementan de forma notable en poco tiempo.

Otra forma de comprobar que se está haciendo uso del router es utilizar el comando **'ping -R -c 1 -n'**. La opción –R del ping muestra una traza de la ruta seguida por los paquetes a la ida y a la vuelta. La traza solo nos indica las interfaces por las que salen los paquetes, no las interfaces por las que entran (excepto en el caso del host de destino en el que sí se muestra la interfaz de entrada). Así por ejemplo si enviamos un ping -R de N2 a N1 debemos ver aparecer la siguiente secuencia de direcciones:

Ida: 10.0.2.12 (N2)
10.0.3.15 (RN)
10.0.3.11 (N1)

Vuelta: 10.0.3.11 (N1)
10.0.2.15 (RN)
10.0.2.12 (N2)

Si el ping se hace de N1 a N2 la secuencia será:

Ida: 10.0.3.11 (N1)
10.0.2.15 (RN)
10.0.2.12 (N2)

Vuelta: 10.0.2.12 (N2)
10.0.3.15 (RN)
10.0.3.11 (N1)

Como puede verse la ruta es simétrica, aun cuando la forma de presentar la información puede dar inicialmente la impresión de que no lo es.

Conexión de las VLANs mediante dos routers

A continuación vamos a incorporar a la red un segundo router (RS) en el edificio Sur. Este router se suministra preconfigurado a los alumnos del Catalyst Sur. La identificación de las interfaces es igual que antes, es decir exteriormente **'Ethernet 0'** y **'Ethernet 1'** en los routers antiguos, **'AUI 0'** y **'AUI 1'** en los nuevos. En todos los casos la denominación a nivel de configuración es **'Ethernet 0'** y **'Ethernet 1'**. Las interfaces Ethernet tienen conectores AUI a los que se han conectado transceivers RJ45.

Este router pasará a convertirse en el router por defecto del edificio Sur y se suministra a los alumnos preconfigurado de la siguiente forma:

Interfaz	Dirección IP	Máscara
Ethernet 0	10.0.2.25	255.255.255.0
Ethernet 1	10.0.3.25	255.255.255.0

Tabla 8: Configuración del router RS (edificio Sur)

Debemos realizar las conexiones según se muestra en la figura 11, que es lo mismo que hicimos antes para RN, es decir: conectar mediante latiguillos normales la interfaz 6 del Catalyst Sur a la interfaz Ethernet 0 (o AUI 0) del router RS y la interfaz 5 del Catalyst a la interfaz Ethernet 1 o AUI 1. Debemos comprobar que las conexiones se hagan correctamente o de lo contrario no funcionará la comunicación a través del router.

Una vez realizadas todas las conexiones encenderemos el router.

En estos momentos ningún ordenador hace uso todavía del router RS, ya que todos siguen teniendo como 'default gateway' las direcciones 10.0.2.15 ó 10.0.3.15 que pertenecen a RN. Para que los ordenadores utilicen RS debemos asignarles como 'default gateway' las direcciones de RS (10.0.2.25 ó 10.0.3.25, dependiendo de la red en la que se encuentren). También podemos asignar RS a los ordenadores del lado norte, pero lo lógico es hacerlo para los del lado sur únicamente, ya que de esta manera cada router atenderá el tráfico generado por los ordenadores que se encuentran en su mismo lado, la carga se distribuirá entre los dos routers y el tráfico local entre redes diferentes no tendrá que cruzar el enlace trunk para llegar al router.

Para cambiar la asignación de router por defecto utilizaremos en los ordenadores pares del lado Sur los siguientes comandos:

```
route del -net 0.0.0.0 gw 10.0.2.15
route add default gw 10.0.2.25
```

Para los ordenadores nones la secuencia de comandos será:

```
route del -net 0.0.0.0 gw 10.0.3.15
route add default gw 10.0.3.25
```

Obsérvese que antes de añadir la nueva definición de router por defecto borramos la antigua. Esto es muy importante ya que de lo contrario se añadiría detrás de aquella y al quedar detrás esta no se utilizaría. Para comprobar que las definiciones se han realizado correctamente utilizaremos el comando **'route -n'**.

Además hemos de cambiar el router por defecto en el Catalyst Sur mediante el comando en modo Configuración Global **'ip default-gateway 10.0.3.25'** (en este caso no es necesario borrar la definición anterior).

Si todo se ha desarrollado correctamente debemos seguir teniendo comunicación entre los ordenadores de las dos VLANs y los Catalyst, tanto dentro de un mismo edificio como entre edificios diferentes.

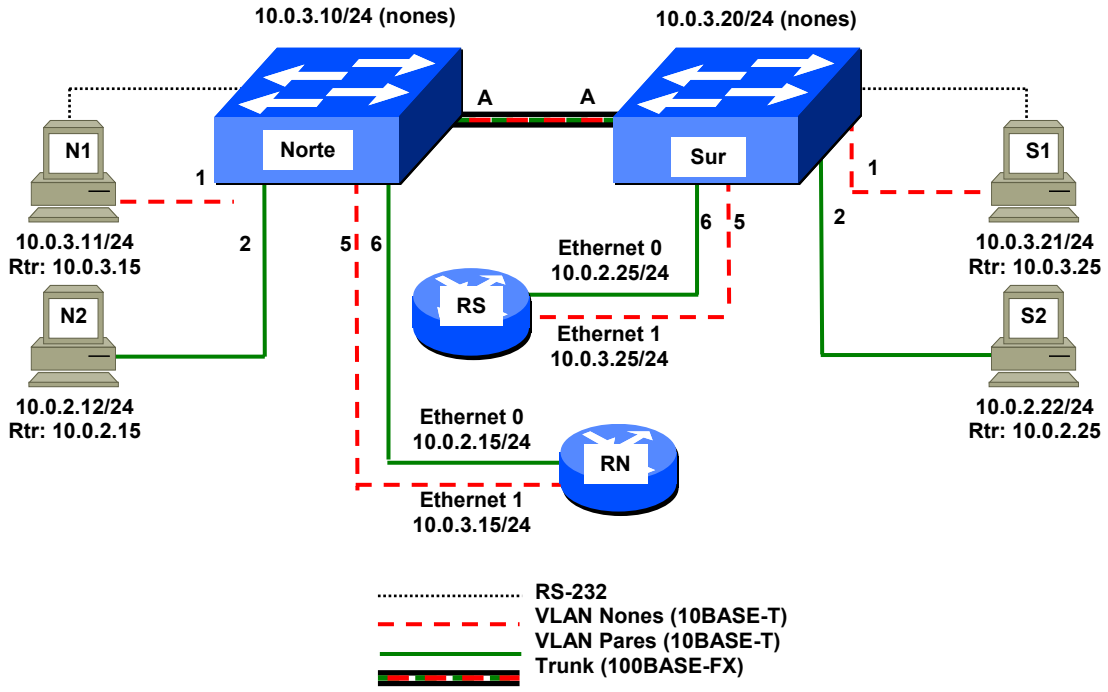

Figura 11. Interconexión de las dos VLANs mediante dos routers y rutas asimétricas

La introducción de un segundo router y su declaración como router por defecto para los equipos del edificio Sur tiene una serie de consecuencias interesantes que merece la pena comentar:

- La comunicación entre ordenadores pares y nones del edificio Sur se realiza ahora sin tener que atravesar el enlace trunk entre los Catalyst. Por tanto dicha comunicación no se vería afectada por problemas que pudieran ocurrir en la comunicación con el edificio Norte o en el conmutador o router de dicho edificio (un fallo de corriente por ejemplo). Esto no ocurría antes, por tanto hemos conseguido una mayor fiabilidad.

- El tráfico Inter.-VLANs se reparte ahora entre ambos routers, con lo que el rendimiento global aumenta. Antes con solo un router en la red la capacidad máxima de tráfico Inter.-VLANs era de 10 Mb/s, mientras que ahora es de 20 Mb/s (10 Mb/s en cada router). Además se reparte entre ambos routers la carga de CPU que supone la conmutación de paquetes, con lo que en este aspecto también hemos doblado el rendimiento.

- Cuando se intercambia tráfico entre hosts de diferentes VLANs en diferentes edificios se producen rutas asimétricas, ya que cada host utiliza para enviar sus paquetes el router que se encuentra en su mismo lado.

Utilizando el comando `'ping -R -c 1 -n'` como hicimos anteriormente los alumnos deberán comparar el resultado con el obtenido anteriormente y comprobar que cuando el destino se encuentra en el otro edificio se producen efectivamente rutas asimétricas.

Una vez finalizada la práctica los alumnos deberán realizar las siguientes tareas:

1. Cerrarán ordenadamente el sistema operativo Linux con el comando `'shutdown -h 0'`.

2. Apagarán los routers y los conmutadores.

3. Devolverán las conexiones de red de los ordenadores a las tomas de la pared en las que se encontraban inicialmente, utilizando para ello los mismos latiguillos que tenían los hosts en un principio.

4. Desconectarán los demás cables utilizados para conectar los equipos (routers y conmutadores) y los entregarán al profesor. Deberán tener especial cuidado de tapar correctamente las conexiones de fibra óptica, tanto en los conmutadores como en los latiguillos.

Apéndice I. Explicación de la salida generada por el comando '**show interfaces**'

La salida generada por el comando '**Show INterface'** en los Catalyst 1900 tiene un aspecto similar al siguiente:

#Show INterfaces Ethernet 0/1

```
1. Ethernet 0/1 is Enabled
2. Hardware is Built-in 10Base-T
3. Address is 0030.9432.0C01
4. MTU 1500 bytes, BW 10000 Kbits
5. 802.1d STP State:  Forwarding     Forward Transitions:  1
6. Port monitoring: Disabled
7. Unknown unicast flooding: Enabled
8. Unregistered multicast flooding: Enabled
9. Description: Ordenador secretaria
10. Duplex setting: Half duplex
11. Back pressure: Disabled


Receive Statistics                        Transmit Statistics
------------------------------------  ------------------------------------
Total good frames                   0  Total frames                        0
Total octets                        0  Total octets                        0
Broadcast/multicast frames          0  Broadcast/multicast frames          0
Broadcast/multicast octets          0  Broadcast/multicast octets          0
Good frames forwarded               0  Deferrals                           0
Frames filtered                     0  Single collisions                   0
Runt frames                         0  Multiple collisions                 0
No buffer discards                  0  Excessive collisions                0
                                       Queue full discards                 0
Errors:                                Errors:
  FCS errors                        0    Late collisions                   0
  Alignment errors                  0    Excessive deferrals               0
  Giant frames                      0    Jabber errors                     0
  Address violations                0    Other transmit errors             0
```

El significado de las 11 líneas de la primera parte es el siguiente:

1. Indica que se trata de la interfaz 1 y que el enlace está operativo.

2. La interfaz es 10BASE-T

3. La dirección MAC de esa interfaz es 0030.9432.0C01. (El conmutador como tal posee como dirección canónica la 0030.9432.0C00, pero asocia una diferente a cada interfaz, desde la 0030.9432.0C01 para la Ethernet 0/1 hasta la 0030.9432.0C1B para la FastEthernet 0/27.)

4. La MTU (Maximum Transfer Unit) o cantidad máxima de información útil que puede contener una trama en esta interfaz es 1500 bytes. El ancho de banda es 10000 Kb/s.

5. El estado Spanning Tree en esta interfaz es 'Forwarding'. Desde el último arranque del equipo la interfaz solo se ha puesto una vez en estado Forwarding.

6. La función de monitorización está desactivada en esta interfaz.

7. La inundación de tramas hacia direcciones unicast desconocidas (no contenidas en la tabla de direcciones MAC del equipo) está habilitada. Este es el comportamiento normal de un puente transparente.

8. La inundación de direcciones MAC multicast no registradas está habilitada. Esto también es normal.

9. El campo 'Description' contiene el texto 'Ordenador secretaria. Este campo sirve para añadir una descripción a efectos puramente documentales.

10. El dúplex está en modo Half. (Este equipo no soporta autonegociación.)

11. El control de flujo ejercido por 'presión hacia atrás' está desactivado. Este control de flujo consiste en transmitir forzando una colisión con el emisor si se está recibiendo una trama y no hay espacio en los buffers de entrada para almacenarla.

El significado de los contadores que aparecen en la segunda parte es el siguiente:

Estadísticas lado izquierdo (de recepción):

- **`Total good frames`**: tramas que se han recibido por esa interfaz que no contenían errores.
- **`Total octets`**: bytes contenidos en las tramas del contador anterior.
- **`Broadcast/multicast frames`**: tramas recibidas por esa interfaz cuya dirección MAC de destino no se encontraba en las tablas del conmutador. Esto incluye todo el tráfico broadcast/multicast pero también las tramas unicast cuya dirección de destino es desconocida (no aparece en la tabla de direcciones MAC del conmutador).
- **`Broadcast/multicast octets`**: bytes contenidos en las tramas del contador anterior.
- **`Good frames forwarded`**: Tramas recibidas por esa interfaz que se han reenviado por alguna otra interfaz (o por todas ellas).
- **`Frames filtered`**: Tramas recibidas por esa interfaz que no se han reenviado a ninguna otra porque en la tabla de direcciones la MAC de destino figuraba asociada a la misma interfaz por la que ha llegado la trama.
- **`Runt Frames`**: tramas recibidas por esa interfaz que tienen una longitud menor de 64 bytes y por tanto son ilegales en Ethernet.
- **`No buffer discards`**: tramas recibidas por esa interfaz que han sido descartadas por falta de espacio en buffer disponible para almacenarlas.

Errores en recepción (lado izquierdo):

- **`FCS errors`**: tramas recibidas que tienen una longitud correcta (entre 64 y 1518 bytes) y un número entero de bytes, pero un valor incorrecto del CRC.
- **`Alignment errors`**: tramas recibidas cuyo número de bytes no es entero, es decir el número de bits no es múltiplo de ocho. Estas tramas son ilegales en Ethernet.
- **`Giant frames`**: tramas recibidas que tienen una longitud mayor de 1518 bytes pero por lo demás son correctas (CRC correcto y número entero de bytes). Estas tramas en principio no deberían ocurrir en Ethernet, aunque podría tratarse de tramas que ya teniendo en origen la longitud máxima (1518 bytes) se les añade posteriormente una etiqueta de VLAN.
- **`Address violations`**: en caso de que se haya activado en el conmutador la función de seguridad, que permite enviar tramas solo desde determinadas direcciones MAC autorizadas, este contador indica el número de veces que se han recibido por esa interfaz tramas con direcciones MAC de origen no autorizadas a utilizar esa interfaz.

Estadísticas lado derecho (de transmisión):

- **`Total frames`**: tramas enviadas por esa interfaz.
- **`Total octets`**: bytes contenídos en las tramas del contador anterior.

- **`Broadcast/multicast frames`**: tramas enviadas por esa interfaz cuya dirección MAC de destino no se encontraba en las tablas del conmutador. Esto incluye todo el tráfico broadcast/multicast pero también las tramas unicast cuya dirección de destino es desconocida (no aparece en la tabla de direcciones MAC del conmutador).

- **`Broadcast/multicast octets`**: bytes contenidos en las tramas del contador anterior.

- **`Deferrals`**: Indica el número de veces que el conmutador ha querido transmitir una trama por esa interfaz y ha tenido que esperar por estar ocupado el medio físico.

- **`Single collisions`**: indica el número de veces que se ha detectado una colisión en esa interfaz mientras se estaba transmitiendo una trama.

- **`Multiple collisions`**: indica el número de veces que se ha detectado una colisión 'reincidente' en esa interfaz, es decir que se ha detectado una colisión en el segundo o posterior intento de enviar la trama.

- **`Excessive collisions`**: indica el número de veces que esa interfaz ha llegado a sufrir 16 colisiones consecutivas al intentar enviar una trama. Cuando ocurre esto el conmutador descarta la trama sin enviarla.

- **`Queue full discards`**: indica el número de veces que se ha descartado una trama debido a no haber sitio libre en la cola de salida.

Errores en transmisión (lado derecho):

- **`Late collisions`**: indica el número de veces que se ha producido una colisión tardía, es decir una colisión cuando ya se habían transmitido los primeros 64 bytes de la trama. Esta es una anomalía que no debería ocurrir nunca en una red bien diseñada. Puede ser debida a longitudes de cable excesivas, número excesivo de hubs o a defectos en el cableado.

- **`Excessive deferrals`**: Es el número de veces que se ha producido un error de transmisión debido a que el medio físico estaba ocupado por otras estaciones durante demasiado tiempo.

- **`Jabber errors`**: tramas recibidas que son demasiado grandes (más de 1518 bytes) y que además tienen un CRC erróneo o un número no entero de bytes. Suele deberse a un problema en el hardware de algún equipo conectado a esa interfaz.

- **`Other transmit errors`**: es el número de veces que han ocurrido errores de transmisión no incluidos en los contadores anteriores.

Apéndice II. Cálculo del caudal generado por el comando ping

Vamos ahora a calcular cual es exactamente el tráfico que genera en una red Ethernet el comando **'ping -f -s 5912 -c 1000'** ejecutado en la práctica.

Con este comando se envían 1000 mensajes ICMP ECHO Request y se reciben 1000 ECHO Reply, a razón de 100 por segundo, es decir la ejecución del comando debería tardar 10 segundos exactamente.

Cada mensaje ECHO contiene 5912 bytes de datos, que unidos a los 8 bytes de la cabecera ICMP y a los 20 de la cabecera IP dan un datagrama de 5940 bytes. Dado que el datagrama se ha de acomodar en tramas Ethernet cuyo tamaño máximo (para la parte de datos) es de 1500 bytes tendremos que fragmentarlo, con lo que resultan los siguientes cuatro datagramas:

Fragmento	Cabecera IP	Cabecera ICMP	Datos	Tamaño datagrama
1	20	8	1472	1500
2	20	0	1480	1500
3	20	0	1480	1500
4	20	0	1480	1500
TOTAL	80	8	5912	6000

Cada fragmento ha de tener su propia cabecera IP, pero no ocurre lo mismo con la cabecera ICMP que solo está presente en el primero.

Estos datagramas se acomodan en tramas Ethernet que contienen, además de los 1500 bytes del datagrama, una cabecera MAC formada por las direcciones de destino y origen (6 bytes cada una), el campo Ethertype (2 bytes) y el CRC al final de la trama (4 bytes); por tanto las tramas MAC tienen una longitud de 1518 bytes cada una. Además a nivel físico las tramas Ethernet tienen un preámbulo de 8 bytes y debe haber un espacio no utilizado entre tramas (el llamado 'interframe gap') equivalente a 12 bytes, como mínimo. Así pues podemos considerar que el tamaño de la trama a nivel físico es de 1538 bytes.

Cada paquete de ping enviado genera ocho tramas Ethernet del tamaño máximo (cuatro de ida y cuatro de vuelta). Y esto ocurre cien veces por segundo (opción -f). Por tanto tenemos un caudal real de:

$$1.538 * 4 * 2 * 8 * 100 = 9.843.200 = 9{,}8432 \text{ Mb/s}$$

Obsérvese que hemos elegido un valor de la opción –s (5912) que produce cuatro fragmentos del tamaño máximo. Como ejercicio curioso calcularemos ahora que sucede cuando se aumenta en un byte (5913) el tamaño del paquete de ping. Dado que los fragmentos en el caso anterior estaban ya completos ahora produciremos un quinto fragmento con su cabecera IP de 20 bytes y un solo byte de datos, es decir:

Fragmento	Cabecera IP	Cabecera ICMP	Datos	Tamaño datagrama
1	20	8	1472	1500
2	20	0	1480	1500
3	20	0	1480	1500
4	20	0	1480	1500
5	20	0	1	21
TOTAL	100	8	5913	6021

Las primeras cinco tramas serán de 1538 bytes como antes, pero la quinta tendrá los 21 del datagrama IP más los 18 de la información a nivel MAC, más 15 bytes de relleno para llegar al mínimo de 64 bytes requerido en Ethernet. A estos 64 bytes se añaden los 20 del nivel físico (8 de preámbulo y 12 de hueco entre tramas) dando un total de 84 bytes. Por tanto por cada paquete de ping se enviarán cuatro tramas de 1538 bytes y una de 84. El tráfico generado será pues ahora de:

$$(1538 * 4 + 84) * 2 * 8 * 100 = 9.977.600 = 9{,}9776 \text{ Mb/s}$$

¿Y que ocurre si aumentamos ahora de forma paulatina el tamaño del ping? Debido a la existencia del relleno los tamaños de paquete entre 5913 y 5928 bytes producen todos exactamente el mismo caudal en

la red, pues se van sustituyendo bytes de relleno por bytes de datos. A partir de 5929 el caudal aumenta de forma paulatina según se muestra en la siguiente tabla:

Paquete de ping –i 0.01	**Caudal (Mb/s)**
5913-5928	9,9776
5929	9,9792
5930	9,9808
5931	9,9824
5932	9,9840
5933	9,9856
5934	9,9872
5935	9,9888
5936	9,9904
5937	9,9920
5938	9,9936
5939	9,9952
5940	9,9968
5941	9,9984
5942	10,0000

Evidentemente estos valores suponen que el host emita exactamente un paquete ICMP cada 0,01 segundos, lo cual solo es cierto de forma aproximada.

Apéndice III. Comandos UNIX utilizados en la práctica

Comando	Función
`arp – a –n`	Muestra la tabla ARP cache del ordenador
`ethtool eth0`	Muestra información sobre la tarjeta ethernet del ordenador
`ifconfig eth0`	Muestra la configuración de red de la tarjeta Ethernet del ordenador
`ifconfig eth0 inet` *dirección_IP* `netmask 255.255.255.0`	Asigna una dirección IP (con máscara de 24 bits) a la tarjeta Ethernet del ordenador
`minicom – s`	Ejecuta el programa de emulación de terminal minicom
`ping` *dirección_IP*	Prueba la conectividad a nivel IP con la dirección de destino indicada
`ping –b` *dirección_IP*	Envía los paquetes a una dirección broadcast
`ping –c` *número dirección_IP*	Envía el número de paquetes indicado
`ping –f` *dirección_IP*	Envía paquetes de ping a razón de 100 por segundo
`ping –R -n` *dirección_IP*	Envía paquetes solicitando se registre la ruta seguida a la ida y a la vuelta, sin hacer resolución de nombres
`ping –s número` *dirección_IP*	Envía paquetes del tamaño indicado
`route add default gw` *dirección_IP*	Asigna un router por defecto para la comunicación con otras redes
`route del –net 0.0.0.0 gw` *dirección_IP*	Elimina el router por defecto asignado con 'route add default gw'
`shutdown –h 0`	Termina el sistema ordenadamente sin esperar
`telnet` *dirección_IP*	Se conecta como terminal remoto a la dirección IP indicada

Apéndice IV. Comandos del Catalyst 1900 utilizados en la práctica

La parte en mayúsculas corresponde a la abreviatura mínima de cada comando.

Comando	**Modo**	**Función**
CDp Enable	Cfg Int	Activa el protocolo CDP (Cisco Discovery Protocol) en la interfaz correspondiente
CLear COunters	Priv.	Borra los contadores de todas las interfaces
CLear COunters ***interfaz***	Priv.	Borra los contadores de la interfaz indicada
CLear Mac-address-table	Priv.	Borra la tabla de direcciones MAC
CONfigure	Priv.	Entra en modo Configuración Global
DElete NVRAM	Priv.	Borra la configuración y restaura la de fábrica
DUplex Full	Cfg Int	Pone la interfaz en modo full dúplex
DUplex Half	Cfg Int	Pone la interfaz en modo half dúplex
ENable	Usuario	Entra en modo Privilegiado
ENAble Password Level 15 ***password***	Cfg Glb	Asigna una password para acceso privilegiado al equipo
Exit	Cfg Glb	Vuelve a modo Privilegiado
EXit	Cfg Int	Vuelve a modo Configuración Global
EXit	Priv.	Vuelve a modo Usuario
Interface ***interface***	Cfg Glb	Entra en modo Configuración de Interfaz para la interfaz indicada
IP Address ***dirección_IP máscara***	Cfg Glb	Asigna la dirección IP y máscara indiciadas al conmutador
IP DEfault-gateway ***dirección_IP***	Cfg Glb	Asigna la dirección IP indicada como router por defecto al conmutador para permitir la comunicación con otras redes a nivel de gestión
IP Mgmt-vlan ***números***	Cfg Glb	Asocia la dirección IP del conmutador con la VLAN indicada
MAc-address-table Aging-time ***tiempo***	Cfg Glb	Fija el tiempo de vida de las direcciones MAC en el valor indicado (en segundos)
Show VErsión	Usuario	Muestra información general del equipo
Show INterfaces	Priv.	Muestra información de todas las interfaces
Show INterfaces ***interface***	Priv.	Muestra información de la interfaz indicada
Show Mac-address-table	Priv.	Muestra la tabla de direcciones MAC del conmutador
Show Mac-address-table AGing-time	Priv.	Muestra el tiempo de vida (en segundos) de las entradas en la tabla de direcciones MAC del conmutador
Show Running-config	Priv.	Muestra la configuración actual del equipo
Show SPantree ***VLAN***	Priv.	Muestra información sobre Spanning Tree para la VLAN indicada
SPantree ***VLAN***	Cfg Glb	Activa el protocolo Spanning Tree en la VLAN indicada
SPantree Cost ***costo***	Cfg Int	Establece para esta interfaz el costo indicado a efectos de Spanning Tree
SPantree Priority ***prioridad***	Cfg Int	Establece para esta interfaz la prioridad indicada a efectos de Spanning Tree
SPANTREE-template ***VLAN*** **Priority** ***prioridad***	Cfg Glb	Establece para este conmutador la prioridad indicada a efectos del Spanning Tree en la VLAN indicada
Trunk ON	Cfg Int	Pone en modo trunk la interfaz correspondiente
VLan ***número*** **Name** ***nombre***	Cfg Glb	Crea la VLAN del número indicado y le asocia el nombre indicado
VLan-membership Static ***número***	Cfg Int	Asocia a la interfaz correspondiente la VLAN indicada.