

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

Autor: Rogelio Montañana

Objetivo y descripción general.

Esta práctica pretende familiarizar al alumno con la configuración, administración y gestión de una red local basada en conmutadores LAN y redes locales virtuales (VLANs). Aunque los detalles concretos dependen de los equipos utilizados, 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 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	Interconectar los equipos, 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	Interconectar los dos 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 han de dividir en equipos de entre tres y cinco personas cada uno (intentando que el número de miembros de cada equipo sea lo más equilibrado posible). Cada equipo utilizará una maqueta formada por dos conmutadores (que denominamos Norte y Sur en correspondencia con los edificios a los que supuestamente pertenecen) y cuatro ordenadores, dos conectados al conmutador (o edificio) Norte y dos al Sur. Los alumnos de cada equipo deben dividirse de la forma más equitativa posible entre el lado norte y sur de la maqueta. Cada 'medio' equipo deberá configurar un conmutador y dos ordenadores. En las partes 1.1. y 1.2 de la práctica cada medio equipo trabaja de forma independiente con su parte de la red, Norte o Sur. Tanto la parte 1.3 como toda la segunda sesión se desarrollan con los dos conmutadores interconectados. Cada maqueta se mantiene independiente del resto durante toda la práctica.

Los conmutadores utilizados son de la marca Cisco modelo Catalyst WS-C1924C-EN (figuras 1 y 2), de la familia Catalyst 1900, que estuvo a la venta entre 1998 y 2002. Este conmutador dispone en 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 el antiguo conector AUI (Attachment Unit Interface), que permite utilizar cable de cobre (UTP o coaxial) o fibra óptica, según el transceiver que se conecte. Las interfaces AUI y 100BASE-TX no se utilizan en esta práctica

Las interfaces 10BASE-T del Catalyst 1924 no soportan autonegociación. Por defecto funcionan en modo half-dúplex, aunque pueden configurarse manualmente en modo full-dúplex. Las interfaces de 100 Mb/s soportan autonegociación en el modo duplex (half o full) pero no en la velocidad (solo pueden funcionar a 100 Mb/s). la interfaz AUI solo puede funcionar a 10 Mb/s en modo half-dúplex.

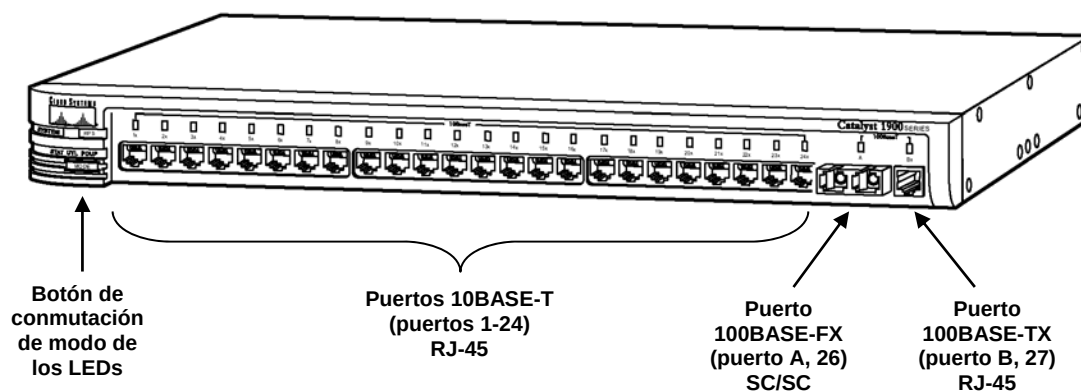


Figura 1: Vista frontal del Catalyst WS-C1924C-EN

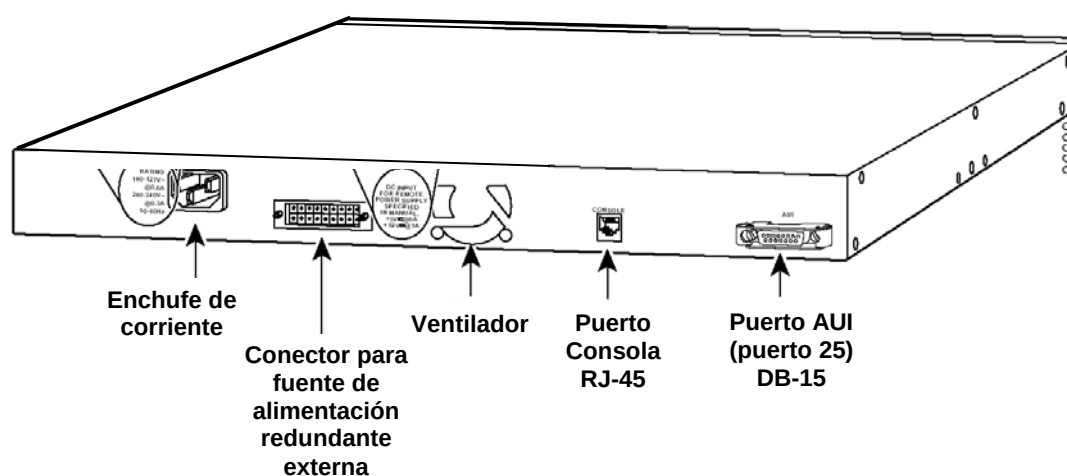


Figura 2: Vista trasera del Catalyst WS-C1924C-EN

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.

Etiqueta identificativa	Denominación en configuración	Tipo de interfaz	Conector	Posición
1x a 24x	Ethernet 0/1 a Ethernet 0/24	10BASE-T	RJ-45	Frontal
AUI	Ethernet 0/25	AUI	AUI	Trasera
Ax	FastEthernet 0/26	100BASE-FX	SC	Frontal
Bx	FastEthernet 0/27	100BASE-TX	RJ-45	Frontal

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 (1x, Ax, etc.). 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 cruce entre transmisión y recepción lo debe realizar el usuario cuando enchufa los conectores SC¹ para que la comunicación sea posible.

¹ SC (Subscriber Connector, Square Connector o Standard Connector) es el conector de fibra óptica utilizado en el Catalyst 1924 y es también el más utilizado en interfaces 100BASE-FX

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):

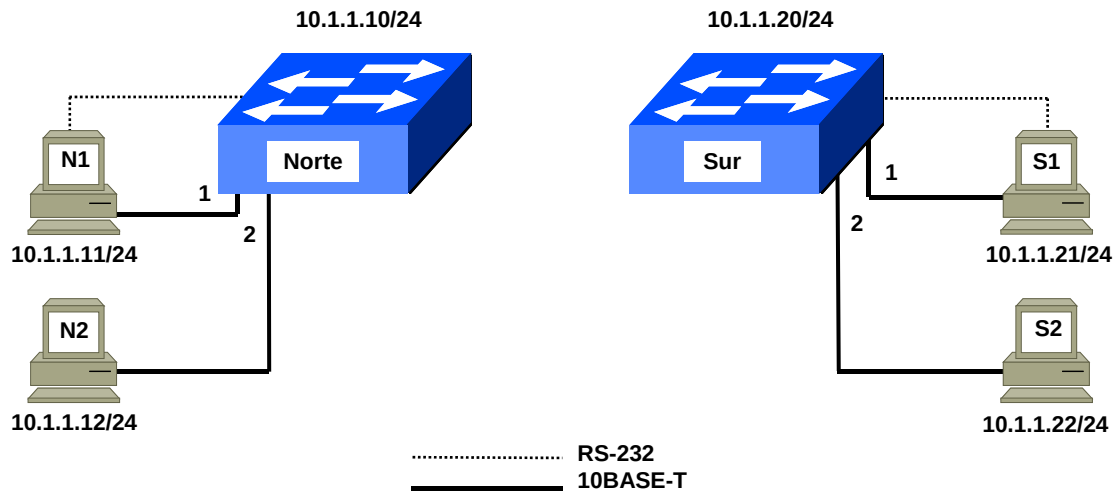


Figura 3: Interconexión de los equipos

Las conexiones a realizar en cada conmutador son las siguientes:

- Conectar la interfaz de consola del Catalyst 1900, que se encuentra en la parte trasera del equipo (ver figura 2) a la interfaz serie (COM1) del ordenador 1 (N1 ó S1). La interfaz de consola del Catalyst es un conector RJ-45 mientras que el puerto COM1 del ordenador será normalmente un conector DB-9.
- Conectar las interfaces Ethernet de los ordenadores 1 y 2 a las interfaces 1 y 2 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 conmutador.

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 contraseña que nos indique el profesor.

Familiarizarse con la interfaz de comandos del conmutador

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**'. Si nos aparece un mensaje que dice:

'Device /dev/modem Access failed: No existe el fichero o el directorio

significa que la configuración por defecto no es correcta, por lo que debemos modificarla. Para ello volveremos a teclear el comando con la opción **-s**, es decir: '**minicom -s**' y en la ventana que

Redes

aparece elegiremos **'Configuración de la puerta serial'** y modificaremos los parámetros A y E poniendo los siguientes valores:

```
A - Dispositivo Serial      : /dev/ttyS0
E - Bps/Paridad/Bits       : 9600 8N1      (opción C)
```

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

Una vez modificados los dos parámetros debemos seleccionar **'Salvar configuración como dfl'** y luego **'Salir'**. Ya debe funcionar la conexión, en caso contrario pediremos ayuda al profesor.

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 encender 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 pasados algo más de 80 segundos no aparece nada en pantalla seguramente se debe a que la comunicación por el puerto serie del ordenador no es correcta. Debemos en ese caso revisar la conexión del cable serie y la configuración del minicom y en caso necesario pedir ayuda al profesor.

Los Catalyst 1900 pueden configurarse de tres maneras diferentes: por interfaz web, por menú y por comandos. Nosotros utilizaremos la configuración por comandos por ser la más potente y la que más similitud tiene con otros equipos de la marca Cisco (conmutadores, routers, etc.). Para ello teclearemos en la pantalla de bienvenida la letra **'K'**²;

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

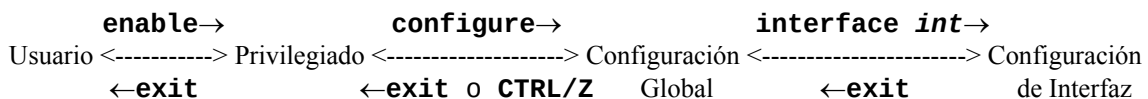
² En este guión hemos seguido el convenio de utilizar **negrita lucida console** para indicar los comandos UNIX, que se deben teclear en una ventana de shell (por ejemplo **'minicom'**), mientras que si un comando aparece en **negrita Courier New** (**'show'** por ejemplo) significa que pertenece a la 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).

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

utilizar en este entorno. Por ejemplo uno de esos comandos es **'show'**, tecleando **'show ?'** nos aparece una lista de los argumentos que admite este comando. Ahora teclearemos el comando **'show 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 contraseña de acceso, en ese caso deberemos teclear **'genios'** (si con esta contraseña 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:



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 y sus argumentos 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 contraseña configurada pasará a modo Privilegiado, inmediatamente, en caso contrario nos pedirá la contraseña y deberemos teclear **'genios'** (si con esta contraseña 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 todas sus interfaces asignadas a la VLAN 1, con el Spanning Tree activado, sin dirección IP y sin contraseña de acceso al modo Privilegiado.

Una vez arrancado el conmutador y restaurada la 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 está detrás) que no tiene LED.

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

En esta parte de la práctica los alumnos del lado Norte y Sur trabajan independientemente, ya que los conmutadores todavía no están conectados (ver figura 3).

Configuración de los ordenadores y prueba básica de conectividad

Los alumnos deberán asignar a cada ordenador una dirección IP y una máscara de acuerdo con lo que se indica en la tabla 2.

Lado Norte		
Ordenador	Dirección IP	Máscara
N1	10.1.1.11	255.255.255.0
N2	10.1.1.12	255.255.255.0
Lado Sur		
Ordenador	Dirección IP	Máscara
S1	10.1.1.21	255.255.255.0
S2	10.1.1.22	255.255.255.0
Tabla 2. Configuración de red de los ordenadores.		

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

COMANDO 'ifconfig'

El comando '**ifconfig**' (interface configure) se utiliza en UNIX para configurar una interfaz de red. Admite multitud de opciones y argumentos, pero nosotros solo veremos los necesarios para asignar una dirección IP y su máscara a una interfaz Ethernet.

Supongamos que queremos configurar el ordenador N2 de nuestra red (dirección 10.1.1.12 y máscara 255.255.255.0). El comando que utilizaremos será:

ifconfig eth0 inet 10.1.1.12 netmask 255.255.255.0

La máscara 255.255.255.0 significa que los primeros tres octetos de la dirección (10.1.1) representan la parte de red y el cuarto (12) la parte host.

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:10.1.1.12  Bcast:10.1.1.255  Mask:255.255.255.0
          inet6 addr: fe80::210:dcff:fedc: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 abrir una ventana de shell en el ordenador y ejecutar el comando:

```
# ifconfig eth0 inet dirección_IP netmask 255.255.255.0
```

donde '**dirección_IP**' será la dirección IP que corresponda al ordenador de acuerdo con la información de la tabla 2. Por ejemplo para el ordenador N2 el comando sería

```
# ifconfig eth0 inet 10.1.1.12 netmask 255.255.255.0
```

Deberemos comprobar que la interfaz se ha configurado correctamente mediante 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 encuentra en prácticamente todas las implementaciones de TCP/IP y se utiliza para comprobar que existe conectividad con una dirección IP determinada. Para utilizarlo hay que teclear **'ping'** seguido de la dirección IP con la que se desea probar la conectividad. Esto provoca el envío de paquetes hacia dicha dirección, que deben ser respondidos inmediatamente. El comando ping nos indica además el tiempo de ida y vuelta midiendo el tiempo transcurrido desde que se efectúa el envío hasta que se recibe la respuesta. Por ejemplo si tecleamos **'ping 10.1.1.22'** obtendremos lo siguiente:

```
[root@lab3inf005 ~]# ping 10.1.1.22
PING 10.1.1.22 (10.1.1.22) 56(84) bytes of data.
64 bytes from 10.1.1.22: icmp_seq=0 ttl=255 time=0.555 ms
64 bytes from 10.1.1.22: icmp_seq=1 ttl=255 time=0.518 ms
64 bytes from 10.1.1.22: icmp_seq=2 ttl=255 time=0.545 ms

--- 10.1.1.22 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 (y recibido) tres paquetes cuyos tiempos de ida y vuelta han sido de 0,555, 0,518 y 0,545 ms, respectivamente.

El ping de UNIX envía por defecto un paquete de prueba por segundo de forma indefinida. En Windows por defecto se envían cuatro paquetes (a razón de uno por segundo) y se para la transmisión.

El comando **'ping'** admite una serie de opciones que en UNIX pueden averiguarse mediante el comando **'man ping'** o **'ping -h'**. Las opciones que nos van a interesar en esta práctica son las siguientes:

Opción	Significado
-f	Indica que se envíen 100 paquetes por segundo (f de 'flood', inundación en inglés) en vez del comportamiento normal, que es enviar uno por segundo.
-c num_paq	Indica que se envíen num_paq paquetes, después de lo cual el ping termina y se devuelve el control a la consola. Si se omite esta opción se envían paquetes de forma indefinida, siendo necesario pulsar CTRL/C para abortar el envío y recuperar el control de la consola.
-R	Indica que se quiere registrar las direcciones IP de todas las interfaces por las 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 servicio de resolución de nombres.
-b	Se utiliza para enviar pings a direcciones broadcast, por ejemplo la 10.1.1.255.

Estas opciones pueden combinarse entre sí, así por ejemplo el comando **'ping -f -c 1000 10.1.1.22'** enviará 1000 paquetes a razón de 100 por segundo (es decir durante 10 segundos) a la dirección 10.1.1.22.

Con el comando **'ping'** podemos comprobar que el conmutador está realizando correctamente su labor, a pesar de que todavía no tiene introducida configuración alguna.

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

Ahora asignaremos una dirección IP al conmutador. Esto lo haremos desde la ventana minicom del ordenador 1 (N1 o S1) que es el que tiene la conexión de consola. Si no hemos cerrado la sesión que abrimos antes esta seguirá mostrando el prompt **'#'**, lo cual indica que sigue en modo Privilegiado, de lo contrario deberemos abrir una nueva sesión, seleccionar la modalidad de línea de comandos (**'K'**) y pasar a modo Privilegiado con el comando **'enable'** (ahora no nos pedirá contraseña ya que la configuración de fábrica no tiene). Una vez en modo Privilegiado tecleamos el comando **'configure'** para pasar al modo Configuración Global, cosa que reconoceremos porque el prompt cambia a

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

'(config)#'. En el modo de Configuración Global utilizaremos el comando '**ip address**' para introducir la configuración IP correspondiente, de acuerdo con los datos que aparecen en la Tabla 3.

Conmutador	Dirección IP	Máscara
Norte	10.1.1.10	255.255.255.0
Sur	10.1.1.20	255.255.255.0

Tabla 3: Configuración de red de los conmutadores.

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 10.1.1.10 255.255.255.0
(config)#CTRL/Z
#
```

Una vez hemos asignado dirección IP al conmutador ya podemos comunicarnos con él, cosa que podremos comprobar ejecutando el comando **ping** desde los ordenadores. Ahora probaremos a hacer **telnet** al conmutador desde los ordenadores para ejecutar comandos sin utilizar el puerto de consola. El comando **telnet** (de TELEtype NETwork) nos permite establecer una sesión de terminal remoto a través de la red TCP/IP. Aunque el ping nos ha demostrado que el conmutador está accesible, el conmutador no nos permite, por razones de seguridad, iniciar una sesión telnet mientras no tenga configurada una contraseña de acceso. Por tanto lo siguiente que haremos será configurarle al conmutador la contraseña '**genios**' (sin las comillas) mediante la siguiente secuencia de comandos:

```
#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 ya podremos acceder vía **telnet** al conmutador desde cualquiera de los ordenadores conectados a él.

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

Uso del comando '**show interfaces**'

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

El comando **'show interfaces'** admite argumentos opcionales que permiten especificar una interfaz en particular. Por ejemplo el comando **'show interface Ethernet 0/2'** (que podemos abreviar a **'show int e 0/2'**) nos muestra información sobre la interfaz número 2 únicamente. Ahora haremos un **'show interfaces'** de la interfaz donde está conectado nuestro ordenador (Ethernet 0/1 ó Ethernet 0/2) y nos fijaremos en la información obtenida. El apéndice I explica en detalle el significado de toda la información que devuelve el comando **'show interfaces'**.

Ahora nos fijaremos en las posibilidades que ofrece el conmutador de contabilizar el tráfico que pasa por él. El conmutador mantiene una serie de contadores de tramas y octetos 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 se muestran 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 observar como se incrementan los contadores de tramas/octetos recibidos y transmitidos. Podríamos calcular el tráfico en un intervalo de tiempo dado tomando dos lecturas de los contadores y calculando las diferencias 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 eth 0/2'**) que pone a cero los contadores que corresponden a la interfaz indicada (o todos los contadores del conmutador si no se especifica interfaz); de esta forma sabemos que todo el tráfico contabilizado en el **'show interfaces'** se ha producido desde la última vez que hemos borrado contadores y es más fácil identificar el que se ha producido recientemente. El comando **'clear counters'** requiere acceso en modo Privilegiado al conmutador y debería utilizarse con cuidado en un entorno como el de esta práctica donde varias personas pueden estar trabajando a la vez en el mismo conmutador y posiblemente consultando los mismos contadores.

Tráfico de BPDUs y desactivación del protocolo Spanning Tree

Vamos a comprobar ahora como el conmutador genera por sí mismo tráfico, aún en el caso de que los ordenadores no estén enviando nada. Para evitar interferencias debidas al tráfico de las conexiones telnet que hemos establecido antes las cerraremos todas y haremos este experimento desde la ventana minicom del ordenador 1 (N1 ó S1) ya que el tráfico generado por la ventana minicom, al emplear la interfaz de consola, no se refleja en los contadores de las interfaces Ethernet. Para poder ver el tráfico arrancaremos en los ordenadores el programa Wireshark (pestaña 'Aplicaciones', seleccionar 'Internet' y allí seleccionar 'Wireshark'). Al arrancar el Wireshark seleccionaremos 'captura', 'interfaces' y la interfaz eth0 (Ethernet). El programa nos muestra el tráfico que está llegando al ordenador, que es generado exclusivamente por el conmutador pues no estamos haciendo nada que genere tráfico en la red. Por la captura del Wireshark y por la evolución de los contadores³ podremos ver que se trata de tráfico enviado por el conmutador. Ese tráfico, de caudal reducido pero continuo, se debe en su mayor parte a los mensajes del protocolo Spanning Tree (como podemos comprobar por el Wireshark), que por defecto se envían a razón de uno cada 2 segundos. Ahora vamos a suprimir dicho tráfico desactivando el Spanning Tree, para lo cual utilizaremos el comando **'no spantree'**. Al desactivarlo debemos indicar en que VLAN queremos actuar; como no hemos configurado todavía ninguna VLAN todos los puertos se encuentran asignados a la 1, que es la VLAN por defecto. La secuencia de comandos que debemos utilizar, igual en ambos conmutadores, es la siguiente:

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

³ 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.

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

Una vez desactivado el Spanning Tree seguiremos observando durante algún tiempo la captura del Wireshark para ver si verdaderamente hemos conseguido suprimir todo tipo de tráfico en la red. Veremos ahora mucho menos tráfico, pero sigue apareciendo un paquete de vez en cuando (exactamente uno por minuto) que corresponde al protocolo CDP (Cisco Discovery Protocol), un protocolo propietario de Cisco que consiste en que los equipos Cisco envíen periódicamente mensajes de salutación. Para 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 una VLAN en 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:

```
#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 ya no se genera ningún tráfico.

Una vez terminada esta prueba cerraremos la ventana del Wireshark.

Funcionamiento de los LEDs y cambio de modo

Vamos a describir a continuación el modo de funcionamiento y 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. El modo por defecto es STAT, se puede cambiar a modo UTL pulsando una vez el botón MODE, o a modo FDUP pulsando dos veces dicho botón. Pulsando el botón una tercera vez se vuelve al modo STAT. Si se deja en los modos UTL o FDUP el conmutador revierte automáticamente al cabo de unos instantes al modo STAT, que es el modo por defecto.

En el modo STAT cada LED representa el status de la interfaz correspondiente: una luz verde indica que hay enlace establecido con el equipo conectado a esa interfaz; si además la luz parpadea indica que hay tráfico. 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 conectado está apagado o a que se ha utilizado un cable incorrecto (por ejemplo un cable cruzado). Cuando el LED parpadea en ámbar significa que se están detectando problemas con el tráfico enviado o recibido por esa interfaz, 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 bloqueada por indicación del protocolo Spanning Tree.

En el modo UTL los LEDs de las 24 interfaces 10BASE-T se utilizan conjuntamente a modo de velocímetro para mostrar el ancho de banda agregado que está manejando el conmutador, con la escala más o menos logarítmica que 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 utilizar LEDS parpadeantes para marcar el tráfico instantáneo, el conmutador mantiene encendido fijo el LED que marca el valor máximo alcanzado, como si fuera un termómetro de temperatura máxima.

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 (que es el modo por defecto) el LED no se enciende.

Generación de tráfico masivo

Ahora haremos un experimento consistente en provocar tráfico masivo a través del conmutador. Para ello vamos a utilizar el programa iperf, que realiza una transferencia de datos a la máxima velocidad posible entre dos ordenadores y muestra luego la velocidad de transferencia obtenida. Uno de los ordenadores actuará como cliente y el otro lo hará como servidor. En nuestro caso el ordenador 1 será el cliente y el 2 el servidor. Para ello ejecutamos primeramente en el ordenador 2 el comando:

```
# service iptables stop
```

que desactiva el cortafuegos del equipo, ya que el cortafuegos impide aceptar conexiones entrantes. A continuación arrancamos 'iperf' en modo servidor en ese ordenador con el comando:

```
# iperf -s
```

y después ejecutamos iperf en modo cliente en el ordenador 1 con el comando:

```
# iperf -c dirección_IP
```

donde '*dirección_IP*' debe ser la dirección IP del ordenador 2. En ese momento comienza la prueba, que por defecto dura 10 segundos. Al final aparece, tanto en el cliente como en el servidor, un mensaje informativo similar al siguiente:

```
[root@lab3inf13 ~]# iperf -s
-----
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
-----
[  4] local 10.1.1.12 port 5001 connected with 10.1.1.11 port 39066
[ ID] Interval           Transfer     Bandwidth
[  4]  0.0-10.3 sec    10.4 MBytes  8.46 Mbits/sec
```

donde se indica la cantidad de datos transmitidos (10,4 MBytes en el ejemplo) y la velocidad de transferencia media (8,46 Mb/s). Si la red funciona correctamente el cliente debería dar un valor idéntico al del servidor en la cantidad de datos y uno parecido (pero normalmente no idéntico) en la velocidad. La prueba se puede repetir cuantas veces se quiera ejecutando el comando 'iperf' en el cliente (el servidor debe mantenerse todo el tiempo a la escucha).

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

El comando **iperf** tiene multitud de parámetros opcionales, que se pueden consultar tecleando '**iperf -h**'.

Al hacer la prueba de **iperf** podremos apreciar el tráfico generado observando los LEDs de las interfaces: en el modo STAT veremos que los de las interfaces 1 y 2 parpadean con una frecuencia elevada, proporcional a la cantidad de tráfico. Si pasamos al modo UTL con **iperf** en marcha veremos cómo aumenta el número de LEDs encendidos y como cuando termina se apagan todos, quedando encendido fijo el que corresponde al valor máximo alcanzado. Dado que estamos utilizando una sola interfaz de 10 Mb/s el tráfico generado en el conmutador a nivel global no será muy elevado, aun cuando la interfaz llegue a estar saturada.

Autonegociación

Cuando conectamos un equipo a una red Ethernet, por ejemplo al enchufar un ordenador a un conmutador o dos ordenadores entre sí, se envían antes de establecer el enlace una serie de mensajes en los que se intercambia información sobre la velocidad o velocidades soportadas por cada una de las dos interfaces conectadas (10, 100 ó 1000 Mb/s) así como sobre el modo dúplex soportado (Half o Full). Gracias a estos mensajes las dos interfaces negocian funcionar a la velocidad más alta soportada por ambas, y en modo full dúplex si ambas lo soportan. Esto es lo que se conoce como autonegociación.

En nuestro caso los ordenadores soportan autonegociación de velocidad (10/100/1000) y de modo dúplex (Half/Full), pero los conmutadores solo soportan 10 Mb/s y el modo puede ser Half o Full pero se ha de poner a mano, no se negocia (por defecto es Half). Así pues, gracias a la autonegociación nuestros ordenadores se han adaptado a funcionar en el modo 10/Half, como podemos comprobar mediante el comando '**ethtool**':

COMANDO '**ethtool**'

El comando '**ethtool**' (ethernet tool) se utiliza en UNIX para obtener información sobre la configuración y posibilidades de una interfaz Ethernet. Como es habitual el comando '**man ethtool**' nos permite descubrir todas las opciones y posibilidades del comando, aunque de momento solo nos interesa la información que devuelve el comando sin opciones, como se muestra en el siguiente ejemplo:

```
[root@lab3inf005 ~]# ethtool eth0
Settings for eth0:
    Supported ports: [ TP ]
    Supported link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Supports auto-negotiation: Yes
    Advertised link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Advertised auto-negotiation: Yes
    Speed: 10Mb/s
    Duplex: Half
    Port: Twisted Pair
    PHYAD: 1
    Transceiver: internal
    Auto-negotiation: on
    Supports Wake-on: pumbag
    Wake-on: g
    Current message level: 0x00000001 (1)
    Link detected: yes
[root@lab3inf005 ~]#
```

'Supported link modes' indica las velocidades y modos dúplex que soporta la tarjeta. 'Supports auto-negotiation' indica si la tarjeta soporta autonegociación. Las líneas 12 y 13 ('Speed: 10Mb/s' y 'Duplex: Half') nos indican la velocidad y el modo dúplex que se están utilizando en la interfaz en ese momento. La línea 17 ('Auto-negotiation: on') nos indica que la función de autonegociación está activada (ya que podría estar soportada pero desactivada).

Para probar cómo funciona la autonegociación vamos ahora a conectar directamente entre sí los dos ordenadores, sin pasar a través del conmutador. Para ello conectaremos el cable del ordenador 1 en el ordenador 2 directamente. En teoría esto debería hacerse utilizando un cable cruzado, pero las interfaces de estos ordenadores tienen la función de 'cruce inteligente', por lo que cuando una interfaz detecta que no se establece el enlace realiza el cruce internamente a ver si así se establece, por lo que se puede utilizar un cable cruzado o paralelo. Una vez hecha la conexión repetiremos la prueba del iperf para medir el rendimiento real de la conexión y deduciremos, a partir del resultado obtenido, la velocidad de conexión negociada en este caso. A continuación utilizaremos el comando **'ethtool eth0'** para comprobar si la suposición en cuanto a la velocidad es correcta, y para averiguar el modo duplex utilizado.

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 -b 10.1.1.255'**. Esta es la dirección IP broadcast en la red en que nos encontramos (empieza por 10.1.1 y tiene la parte host toda a unos) por lo que a nivel de enlace utiliza la dirección FF:FF:FF:FF:FF:FF, como podemos comprobar fácilmente con el programa Wireshark. El tráfico broadcast se propaga por inundación a todas las interfaces activas del conmutador (las interfaces que no tienen nada conectado están inactivas a nivel físico, por lo que nunca se envía por ellas ningún tráfico).

En teoría al hacer un ping broadcast deberíamos recibir respuesta de todos los dispositivos con dirección IP en la red, en nuestro caso el conmutador y el otro ordenador. Sin embargo dependiendo de la configuración que tengan los Linux es posible que se les haya desactivado la respuesta al ping broadcast, para evitar posibles ataques. En ese caso solo recibiremos respuesta del conmutador.

En esta prueba únicamente utilizaremos el ordenador 1. Primero lanzamos el ping a la dirección 10.1.1.255 desde una ventana de shell y con el ping en marcha abrimos en la ventana minicom 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 la interfaz 2 (en nuestro caso la única interfaz activa que queda) veremos que los contadores que se incrementan son los de la derecha, que corresponden a **'Transmit Statistics'**. Esto significa que el conmutador está transmitiendo por esa interfaz las tramas broadcast que recibe por la interfaz 1. Obsérvese que el conmutador siempre interpreta el sentido de recepción o transmisión desde su punto de vista, es decir como si estuviéramos físicamente situados dentro del conmutador.

Si queremos podemos repetir la prueba con la opción **-f** (**'ping -b -f 10.1.1.255'**) con lo cual conseguiremos el mismo efecto, pero de forma mucho más notoria ya que se envían 100 tramas por segundo.

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 CAM (Content Addressable Memory) que es la tabla de direcciones MAC del conmutador. Para ello utilizaremos en modo Privilegiado el comando:

```
#show mac-address-table
```

que nos muestra la lista completa de las direcciones MAC conocidas y las interfaces por las que están accesibles. También podemos probar el comando

```
#clear mac-address-table
```

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

que borra completamente la tabla CAM, obligando por tanto a que las tramas siguientes sean enviadas por inundación.

Para generar entradas en la tabla CAM vamos a lanzar un ping de un ordenador a otro. Inmediatamente veremos aparecer las entradas correspondientes a los dos ordenadores en la tabla CAM. En dicha tabla no aparecen las direcciones IP, ya que el conmutador solo funciona a nivel de enlace. Para averiguar la equivalencia IP-MAC debemos utilizar en los ordenadores 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 ordenador en un instante determinado. Dicha tabla, conocida como ARP-cache, cambia con el tiempo.

Con la opción **'-h'** podemos ver las opciones disponibles del comando **'arp'**. Nosotros utilizaremos **'-a'** y **'-n'**; la primera indica que queremos obtener la tabla ARP cache, y la segunda que queremos obtener las direcciones IP sin resolución de nombres, ya que en nuestra maqueta no tenemos activado el servicio de resolución de nombres.

Un ejemplo de uso del comando arp es el siguiente:

```
[root@lab3inf005 ~]# arp -a -n
? (10.1.1.12) at 00:0A:5E:3C:81:8C [ether] on eth0
[root@lab3inf005 ~]#
```

Igual que las entradas de la tabla CAM, las de la ARP cache caducan pasados unos minutos, por lo que si están vacías debemos lanzar de nuevo el ping. Obsérvese que en la ARP cache nunca aparece una entrada para el propio ordenador donde se ejecuta el comando, si queremos averiguar la correspondencia MAC-IP para ese caso deberemos utilizar el comando **'ifconfig eth0'**.

Ahora cada alumno deberá rellenar la siguiente tabla de correspondencia entre las direcciones MAC e IP de la maqueta utilizando para ello los comandos **'arp -a -n'** e **'ifconfig eth0'** en un ordenador:

Equipo	MAC	IP
Conmutador		
Ordenador 1		
Ordenador 2		

A continuación utilizará el comando **'show mac-address-table'** en el conmutador para averiguar a que puerto se encuentra asociada cada dirección MAC. En caso de que alguna entrada haya desaparecido por tiempo de alguna de las tablas se puede utilizar el comando **'ping'** para que vuelva a aparecer.

El tiempo de vida de las entradas en la tabla CAM de 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 en modo Configuración Global el comando:

```
(config)#mac-address-table aging-time tiempo
```

Donde '**tiempo**' es el nuevo tiempo de caducidad, en segundos.

Ahora realizaremos un experimento consistente en lo siguiente:

- Reducimos el tiempo de vida a un minuto mediante el comando '**mac-address-table aging-time 60**' (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 en las interfaces 1 y 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 a la interfaz 2 en vez de a la 4 en que se encuentra conectado 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 debería ocurrir justo un minuto después de haber cambiado el cable, como podremos comprobar por el número de pings que fallan (60). Mientras la dirección MAC estaba asociada a la interfaz 2 las tramas se perdían, pues el conmutador seguía empeñado en enviarlas por ella; cuando al cabo de un minuto la dirección del ordenador 2 desaparece de la tabla el siguiente ping se envía por inundación a todas las interfaces y la primera respuesta recibida desde la interfaz 4 hace que la dirección MAC aparezca asociada ahora 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 en el siguiente ping se realice la inundación y se localice la nueva ubicación del ordenador cambiado. Ahora, sin parar el ping, devolveremos el cable del ordenador 2 a su interfaz original (la 2) y a continuación probaremos como mediante este comando la comunicación se restablece de forma inmediata.

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

Ahora, todavía con el ping del ordenador 1 hacia el 2 en marcha, vamos a probar a cambiar la conexión del ordenador 1 a la interfaz 3. ¿Cuánto tarda en este caso en restablecerse el ping? Los alumnos deben encontrar una explicación razonable al comportamiento observado en este caso.

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 ambos por una sola interfaz, con lo que se consigue conectividad. Después se establece un segundo enlace creando un bucle, con lo que el Spanning Tree desactiva uno de los enlaces. Más tarde se realizan diversos experimentos con el fin de alterar las decisiones adoptadas por el Spanning Tree en cuanto a topología.

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 estropeamos nada, lo único que ocurre es que no se establece el enlace). Una vez realizada esta conexión los alumnos deberán comprobar que existe conectividad enviando pings a los ordenadores conectados en el otro conmutador. Mediante el comando '**show interface 0/6**' se puede observar cómo se incrementa el contador de tráfico en la interfaz 6. También puede consultarse la tabla CAM (comando '**show mac-address-table**') y comprobar que en la interfaz 6 aparecen las direcciones MAC correspondientes a los ordenadores del otro

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

conmutador. Para averiguar las direcciones MAC de los ordenadores remotos se puede seguir el procedimiento indicado anteriormente, es decir lanzar '**ping**' a cada uno de ellos seguido del comando '**arp -a**'.

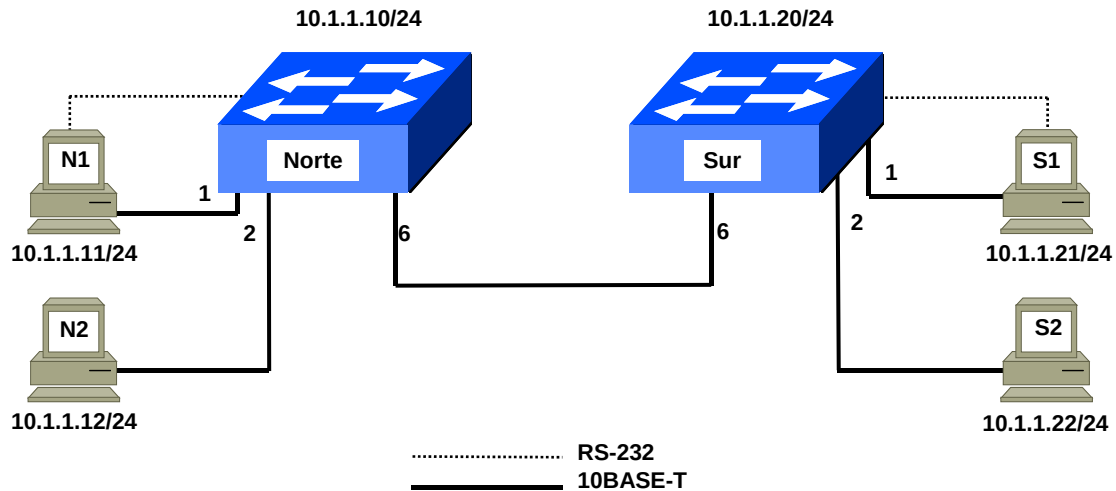


Figura 5. Interconexión de los conmutadores a 10 Mbps

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:

```
(config)#spantree 1
```

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 hello 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 elegido como raíz, de lo contrario habrá sido elegido el otro conmutador. Si los conmutadores están correctamente emparejados el Catalyst Norte debe tener el identificador más bajo y por tanto habrá sido elegido como raíz. El comando '**show spantree 1**' muestra una información desglosada por interfaz que ocupa varias pantallas. En dicha información podemos ver que las interfaces Ethernet (10 Mb/s) tienen asociado un costo de 100, mientras que las Fast Ethernet (100 Mb/s) 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 mediante una dirección MAC, en realidad posee un rango de 28 direcciones consecutivas. La primera de ellas, que denominamos canónica, es la que utiliza para identificarse en 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 tendrá asociada la **00e0.1e69.2301**, la 2 la **00e0.1e69.2302** y así sucesivamente hasta la **00e0.1e69.231b** que corresponderá a la interfaz 27 (FastEthernet 0/27). Las direcciones MAC del conmutador nunca figuran como direcciones de origen de las tramas que éste reenvía, pero sí se utilizan como direcciones de origen de las tramas que él mismo genera. Cuando un conmutador envía mensajes de Spanning Tree o del CDP (Cisco Discovery Protocol) utiliza como MAC de origen la de la interfaz por la que envía la trama; en cambio cuando responde a un ping o a un telnet el conmutador utiliza como MAC de origen la dirección canónica. Por este motivo al interconectar los dos conmutadores por el puerto 6 podemos ver aparecer en la tabla CAM de nuestro conmutador dos direcciones del otro conmutador, la canónica y la del puerto 6.

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 '**show spanning-tree interface 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) sin desconectar el enlace que tenemos entre los puertos 6 de ambos equipos. De este modo provocaremos un bucle entre ellos y analizaremos las decisiones y las acciones que adopta el Spanning Tree. Antes de realizar la conexión a 100 Mb/s lanzaremos un **ping** entre un ordenador norte y uno sur, con el 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 para ello un latiguillo de fibra óptica, que nos suministrará el profesor, cruzando el Transmit con el Receive, es decir el cable que se conecta al puerto Transmit en un conmutador deberá conectarse al Receive en el otro. Como resulta incómodo seguir el latiguillo para averiguar la correspondencia, 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 un lado.

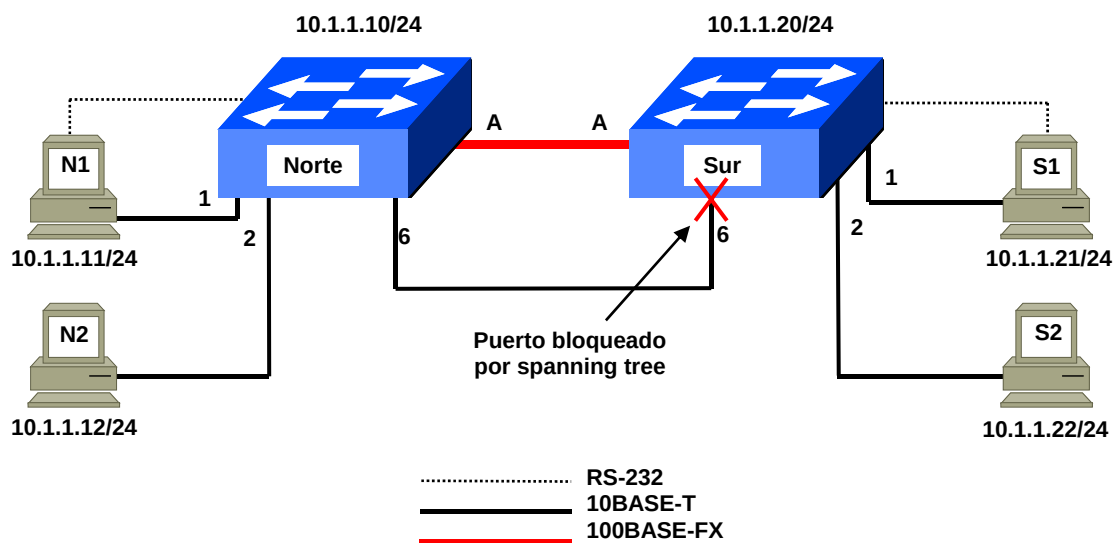


Figura 6. Interconexión de los conmutadores a 100 Mbps y Spanning Tree

Al conectar la interfaz 26 (A) sin desconectar la 6 provocamos un bucle en la red con lo que el Spanning Tree cortará momentáneamente toda comunicación entre ambos conmutadores. Al cabo de unos instantes, cuando los conmutadores ya han intercambiado sus BPDUs y han calculado la nueva topología, el bucle se resuelve bloqueando la interfaz 6 en el conmutador Sur, que es la interfaz de mayor costo al raíz en el conmutador no raíz. Los alumnos deberán medir, utilizando el ping que tienen en marcha, el tiempo aproximado que dura la desconexión entre ambos conmutadores como consecuencia del cambio de topología. Además deberán observar la evolución de los LEDs (en modo STAT) en las interfaces 6 y A de ambos conmutadores. Si todo ocurre como es debido deberán bloquearse inicialmente tanto la interfaz 6 como la A en el conmutador Sur y los LEDs de ambas se pondrán en color ámbar, pero al cabo de unos

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

instantes, cuando la comunicación se restablezca, se deberá quedar en ámbar y bloqueada únicamente la interfaz 6 del conmutador 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 conmutador 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 ambos conmutadores). Obsérvese que para bloquear la comunicación sólo es necesario bloquear la interfaz en el conmutador Sur, la del Norte permanece Forwarding y por tanto ignora la situación. El bloqueo se produce en el conmutador no raíz (el Sur), y se produce en la interfaz 6 ya que tiene un costo de 100, mientras que la 26, Fast Ethernet, tiene un costo 10⁴. Si ahora generamos tráfico de un conmutador a otro podremos comprobar mediante que todo el tráfico discurre a través de la interfaz 26. También podremos comprobar con el comando **'show mac-address-table'** que todas las direcciones MAC del conmutador remoto se conocen a través de la interfaz 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 lado Norte y uno del Sur comprobaremos que el cambio de topología interrumpa la comunicación entre conmutadores hasta que de nuevo el Spanning Tree calcule la nueva, 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'** o simplemente mirando el color de los LEDs correspondientes.

Una vez terminadas estas pruebas volveremos a conectar la interfaz de fibra, manteniendo también el enlace por la interfaz 6. Esto provocará que se vuelva a la situación anterior rehabilitando 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 Spanning Tree respecto a que conmutador debe actuar como raíz. A igual prioridad se elige siempre como raíz la dirección MAC más baja, en nuestro caso el conmutador Norte. Ahora le asignaremos una prioridad 32767 al conmutador Sur, con el fin de que sea elegido como raíz independientemente de cuál sea su dirección MAC. Para ello, únicamente en el Catalyst Sur, teclearemos en modo Configuración Global el comando:

```
(config)#spantree-template 1 priority 32767
```

El efecto puede apreciarse por el cambio de color de los LEDs correspondientes, ya que ahora se bloquea la interfaz 6 del conmutador Norte, no la del Sur. Con el comando **'show spantree 1'** se puede también comprobar que la raíz del árbol es ahora el conmutador Sur, es decir el árbol se ha invertido.

Aunque le hemos dado la vuelta al árbol el camino elegido sigue siendo el mismo, el enlace a través de las interfaces Fast Ethernet, ya que los costos son iguales en ambos conmutadores, 100 para las interfaces Ethernet y 10 para las FastEthernet.

Cambio del costo en una interfaz

Para alterar la decisión en cuanto a caminos hacia el raíz del Spanning Tree vamos ahora a modificar el costo de la interfaz 6 en el conmutador Norte (que actualmente no es raíz) asignándole un costo 8 en vez de 100. De esta forma el conmutador Norte la elegirá como interfaz raíz, bloqueando el puerto Fast Ethernet, es decir tomará una decisión que no es óptima debido a que le estamos suministrando información errónea en cuanto a costos. Para cambiar el costo de la interfaz 6 entraremos, solo en el

⁴ Según los estándares actuales del IEEE el costo de una interfaz de 100 Mb/s ya no es 10 sino 19, pero estos conmutadores utilizan el sistema antiguo en el que el costo era de 10.

conmutador Norte, en modo Configuración de Interfaz para la interfaz Ethernet 0/6 y teclearemos la secuencia de comandos que 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 conmutador Norte la interfaz A cambia de verde a ámbar y la 6 de ámbar a verde. Con el comando **'show spantree'** podemos comprobar que la interfaz 6 está ahora 'Forwarding' y que la 26 está 'Blocked'.

Con el costo de la interfaz 6 cambiado en el conmutador Norte volveremos ahora el árbol a su estado inicial, es decir volveremos a poner el Norte como raíz. Para ello le daremos a este conmutador la prioridad 32767, con lo que vuelve a prevalecer el orden basado únicamente en la dirección MAC. Para cambiar la prioridad procederemos como antes, utilizando en el Conmutador Norte en modo Configuración Global el comando:

```
(config)#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 efectuados en el conmutador Norte. Esto se debe a que los costos de las interfaces en el conmutador raíz carecen de importancia ya que nunca intervienen en los cálculos del Spanning Tree. El conmutador Sur calculará sus caminos al raíz en base a sus propios costos, sin utilizar para nada los costos asignados a las interfaces del conmutador Norte. Ahora volveremos a su valor normal el costo de la interfaz 6 en el conmutador Norte (comando **'spantree cost 100'** en modo Configuración de Interfaz) y comprobaremos 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 solo. A efectos del Spanning Tree el Catalyst Norte ahora no existe, se comporta como si fuera un conmutador sin spanning tree. Ha dejado de enviar BPDUs propias aunque sí reenvía las que recibe del conmutador Sur. Así pues el conmutador Sur detecta un bucle entre sus interfaces 6 y 26 ya que observa que las BPDUs que envía por una las recibe por la otra, y que no recibe BPDUs de ningún otro conmutador. Por consiguiente tiene que desactivar una de las dos interfaces. En este caso el costo al raíz es cero, pues él mismo es el raíz. El empate en costos lo resuelve Spanning Tree bloqueando la interfaz con identificador más elevado, en este caso la 26. Sin embargo se ha tomado la decisión errónea, puesto que se ha activado para la comunicación Norte-Sur el camino más lento (10 Mb/s).

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 la prioridad de la interfaz, que actúa de forma análoga a la prioridad del conmutador pero a nivel de interfaz. El rango de prioridades posibles en interfaces es de 0 a 255 y el valor por defecto 128. Una prioridad más baja prevalece siempre, independientemente de cuál sea el identificador. Así pues, para forzar que la interfaz 26 se elija en primer lugar bastará con asignarle la prioridad 127. Utilizaremos para ello el comando **'spantree priority'** en el conmutador Sur en el modo Configuración de Interfaz, según se indica a continuación:

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

```
#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 en ambos conmutadores, 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 Norte a uno Sur (por ejemplo de N1 a S1). Comprobamos que la comunicación discurre normalmente. Pondremos los LEDs de los conmutadores en modo UTL para ver mejor la evolución del tráfico en los conmutadores.
2. Desactivamos el Spanning Tree en el conmutador Sur (comando **'no spantree 1'** en modo Configuración Global). Al conmutador Norte ya le habíamos desactivado el Spanning 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 CAM, 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 Norte o Sur un ping de un solo paquete a la dirección broadcast de nuestra red con el comando **'ping -b -c 1 10.1.1.255'**. Este paquete se enviará por inundación y por tanto llegará al otro conmutador dos veces, una por el puerto 6 y otra por el 26. El otro conmutador devolverá la copia que recibió por el 6 por el 26 y viceversa, de forma que en unos instantes se saturarán todos los enlaces y se bloqueará la red.

A partir de ese momento podremos apreciar por los LEDs que la actividad del conmutador crece de forma considerable. Si pasamos 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 podemos intentarlo por el puerto de consola (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 enorme cantidad de tráfico por todos sus puertos activos, toda ella originada por el ping broadcast. También podremos ver como el ping que habíamos puesto en marcha antes ya no funciona, o lo hace con muchos fallos.

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

Redes

1. Cerrar ordenadamente el sistema operativo Linux con el comando '**shutdown -h 0**', o pulsando el interruptor de encendido.
2. Apagar los routers y los conmutadores.
3. Devolver 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. Desconectar los demás cables utilizados para conectar equipos y dejarlos en su sitio o entregarlos al profesor. Deberán tener especial cuidado de tapar correctamente las conexiones de fibra óptica, tanto en los conmutadores como en los latiguillos.

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 3, como hicimos en la primera sesión. Conectaremos la interfaz de consola del conmutador 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 conmutador.

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**' seguido de la tecla escape).

A continuación debemos restaurar la configuración de fábrica del conmutador siguiendo el procedimiento descrito 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 '#', de lo 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 indica la tabla 3.

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

Parte 2.1: Crear dos VLANs y comunicarl

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 interconectaremos 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 y a la que están asignadas en principio todas sus interfaces). 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 asignarles interfaces. Si una interfaz no la asignamos a ninguna quedará en la VLAN 'default' (la 1) que es en la que se encuentran todas inicialmente. Únicamente asignaremos las interfaces 1, 2, 5, 6, 7 y 8 en el Catalyst Norte y 1, 2, 5 y 6 en el Sur, las pares a la VLAN 'pares' y las 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:

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

```
#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'** debemos obtener 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 con el comando ping que los dos ordenadores conectados al conmutador han perdido la comunicación entre ellos.

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? La razón es que el conmutador mismo, aunque no está físicamente conectado a ninguna interfaz, también se ha de asignar a alguna VLAN, y si no se asigna a ninguna permanece 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 2 (pares). De esta forma podremos acceder a él desde el ordenador 2, pero no desde el ordenador 1. Para asignar el conmutador a la VLAN pares 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 es nuestra única vía de comunicación 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 comprobaremos que es posible hacerle ping o telnet al conmutador desde el ordenador 2 (N2 ó S2).

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 cruzado o 'crossover'). Pero ahora esa interfaz pertenece a la VLAN pares, por lo que con esa conexión solo podrán comunicarse entre los dos conmutadores los ordenadores de la VLAN pares. Los alumnos deberán comprobar que en efecto ahora la comunicación entre 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 (por ejemplo N1-N2).

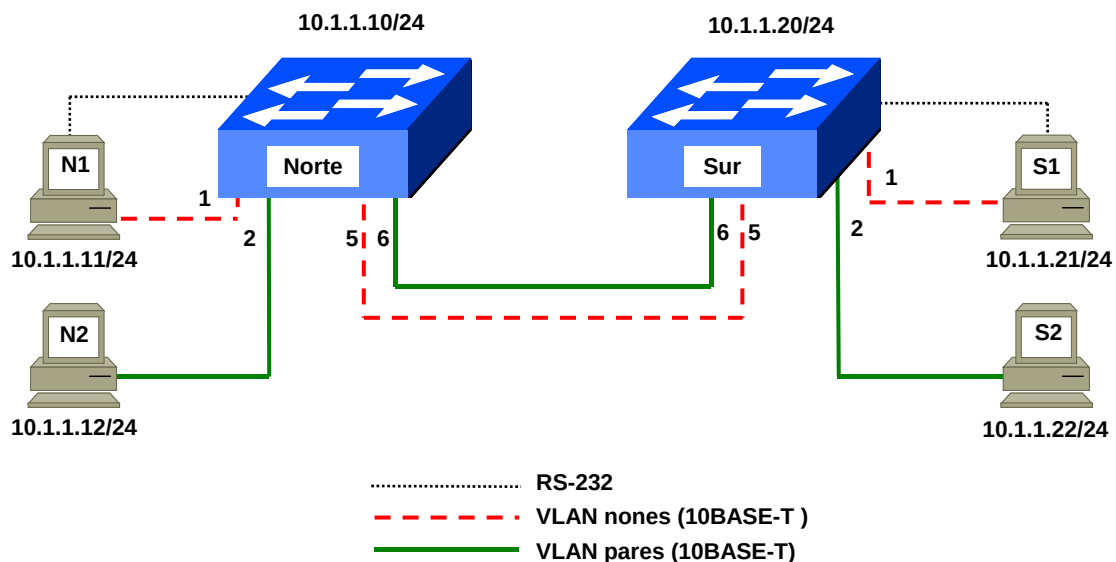


Figura 7. Conexión independiente de las VLANs 'pares' y 'noes'

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 noes y uno con el resto (VLAN default). Analizando cada VLAN por separado no existe ningún bucle. Esto puede comprobarse tecleando el comando **'show spantree'** que ahora nos mostrará información relativa a

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

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

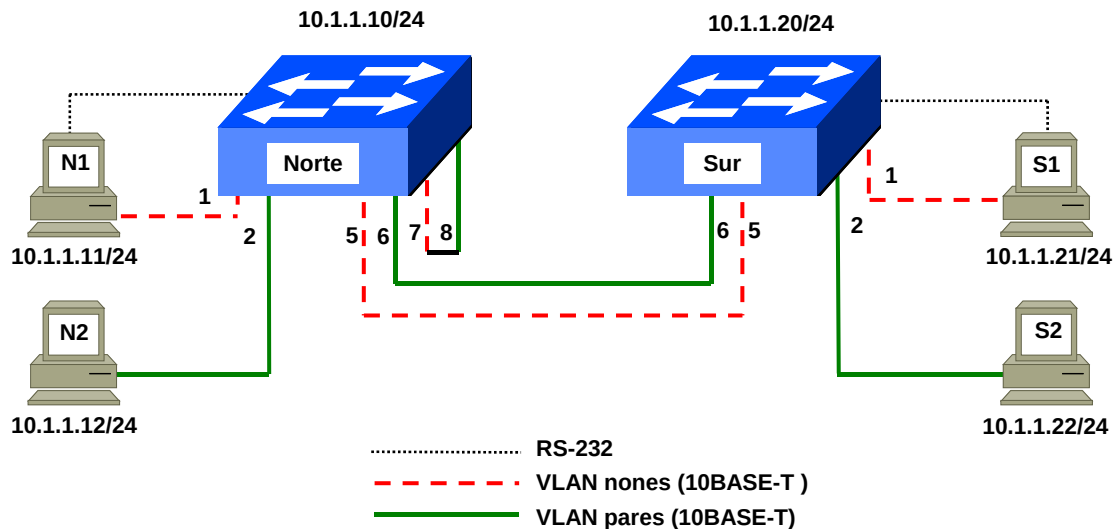


Figura 8. Interconexión de las dos VLANs mediante un latiguillo puente

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 este modo, 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 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 ones 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 disponibles, por lo que ya no sería posible realizar otras conexiones a 100 Mb/s.
- No se puede utilizar si se quiere interconectar 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 las tramas de alguna manera. La norma IEEE 802.1Q establece una forma estándar de realizar ese etiquetado (también llamado encapsulado) pero los conmutadores Catalyst 1900 son anteriores a dicho estándar por lo que no lo soportan. En su lugar utilizan un etiquetado propietario de Cisco que se denomina ISL (Inter. Switch Link). Como los dos conmutadores que utilizamos son del mismo modelo el uso de un sistema propietario no plantea ningún problema de interoperabilidad, pero podría serlo si quisiéramos integrar en esta 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.

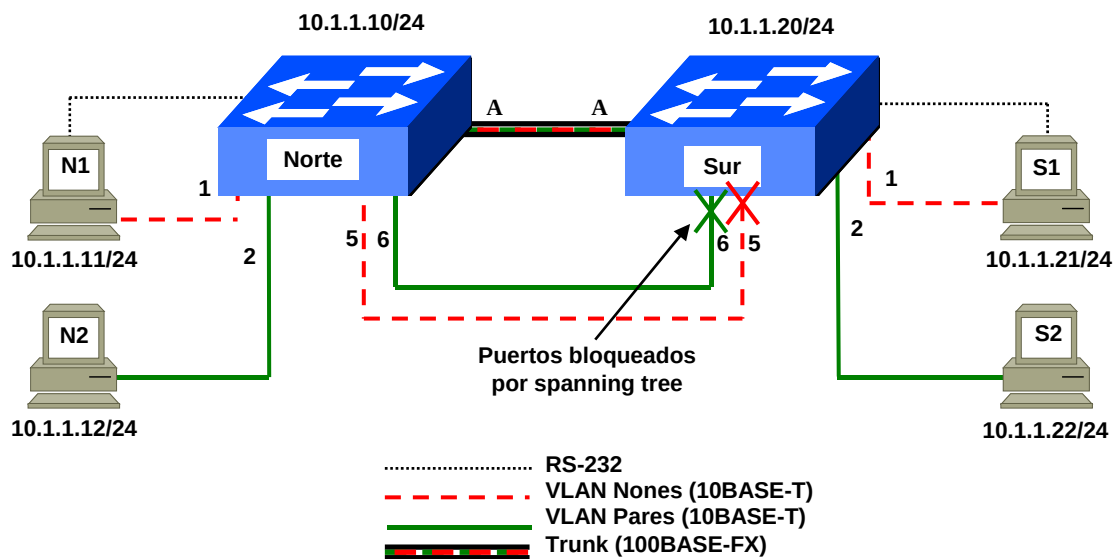


Figura 9. Creación de un enlace 'Trunk'

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 **'show spanning-tree 0/5'** y **'show spanning-tree 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

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

(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 eso 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 10.1.1.0/24 (máscara 255.255.255.0); esta red abarca todas las direcciones que empiezan por 10.1.1, es decir desde la 10.1.1.1 hasta la 10.1.1.254. Esto era lo lógico cuando todos los ordenadores pertenecían a la misma VLAN, y también cuando teniendo en VLANs diferentes las uníamos mediante un latiguillo puente. Pero como ahora queremos que las dos VLANs se comuniquen a través de un router debemos asignarles direcciones de redes diferentes. Usaremos pues la red 10.1.2.0/24 (máscara 255.255.255.0) para la VLAN pares y la 10.1.3.0/24 (máscara 255.255.255.0) para la VLAN nones. Estas redes IP abarcan las direcciones que empiezan por 10.1.2 y por 10.1.3, respectivamente (rangos 10.1.2.1-254 y 10.1.3.1-254). Habrá por tanto una correspondencia biunívoca entre las VLANs y las redes IP. Además debemos asignarle a cada ordenador 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 ordenadores son los que figuran en la tabla 5:

Grupo Norte		
Ordenador	Dirección IP	Router por defecto
N1	10.1.3.11	10.1.3.15
N2	10.1.2.12	10.1.2.15
Grupo Sur		
Ordenador	Dirección IP	Router por defecto
S1	10.1.3.21	10.1.3.15
S2	10.1.2.22	10.1.2.15

Tabla 5. Configuración de red de los ordenadores.

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
```

COMANDO 'route'

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

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

route add default gw direccion_IP_del_router

El router debe pertenecer a la misma red que el ordenador 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 octetos, por lo que si el ordenador tiene una dirección (asignada con **'ifconfig'**) que empieza por 10.1.3 la dirección del router debe necesariamente empezar por 10.1.3.

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

Así por ejemplo en el host S2 teclearemos la secuencia de comandos:

```
# ifconfig eth0 inet 10.1.2.22
# route add default gw 10.1.2.15
```

Para comprobar que los cambios se han realizado correctamente utilizaremos los comandos **'ifconfig eth0'** y **'route -n'**.

Ahora debemos modificar las direcciones IP de los conmutadores y asignarles también un router por defecto. Recordemos que hemos elegido que la VLAN pares actúe como VLAN de gestión de los conmutadores, por lo que les debemos asignar direcciones que pertenezcan a dicha VLAN. Para asignar las direcciones IP utilizamos el comando **'ip address'** que ya conocemos, 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	10.1.2.10	255.255.255.0	10.1.2.15
Catalyst Sur	10.1.2.20	255.255.255.0	10.1.2.15

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 10.1.2.20 255.255.255.0
(config)#ip default-gateway 10.1.2.15
(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 como **'Ethernet 0'** y **'Ethernet 1'**, en otros como **'AUI 0'** y **'AUI 1'** y en otros como **'10BT ETHERNET'** y **'10/100 ETHERNET'**.

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

En todos los casos las interfaces Ethernet presentan conectores RJ45 a los que los alumnos deben conectar latiguillos RJ45 normales (no cruzados).

El router RN está preconfigurado de la siguiente manera:

Etiqueta Interfaz	Nombre interfaz	Dirección IP	Máscara
Ethernet 0, AUI 0 ó 10BT ETHERNET	Ethernet 0	10.1.2.15	255.255.255.0
Ethernet 1, AUI 1 ó 10/100 ETHERNET	Ethernet 1 ó Fastethernet 0	10.1.3.15	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, AUI 0 ó 10BT ETHERNET a la interfaz 6 del Catalyst Norte, y la Ethernet 1, AUI 1 ó 10/100 ETHERNET 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.

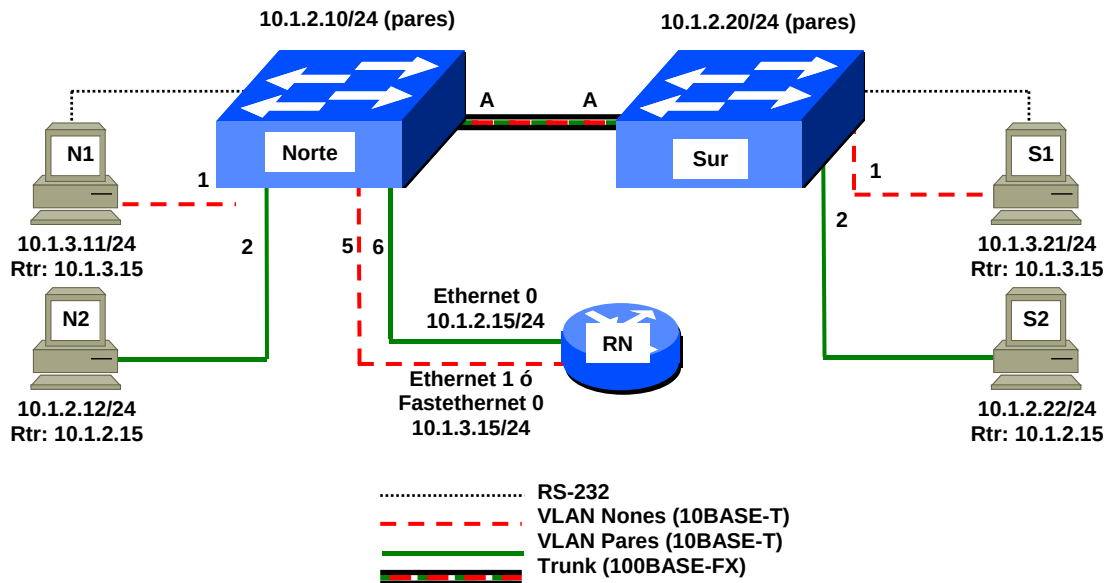


Figura 10. Interconexión física de las dos VLANs mediante un router

Ahora los alumnos deberán comprobar que es posible la comunicación entre cualquier par de ordenadores. 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 nonees haremos ping a 10.1.3.15.

Los ordenadores 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 conmutador Norte (bien por el parpadeo de los LEDs o por los contadores del comando '**show interface 5**' y '**show interface 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 de los conmutadores, por lo que podemos utilizar el comando '**show interfaces**' para obtener datos del tráfico por sus diferentes interfaces, aunque la forma de presentarlos es bastante diferente a la de los 1900.

Redes

Con el comando '**ping -R**' podemos ver 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 ordenador 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: 10.1.2.12 (N2)
10.1.3.15 (RN)
10.1.3.11 (N1)

Vuelta: 10.1.3.11 (N1)
10.1.2.15 (RN)
10.1.2.12 (N2)

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

Ida: 10.1.3.11 (N1)
10.1.2.15 (RN)
10.1.2.12 (N2)

Vuelta: 10.1.2.12 (N2)
10.1.3.15 (RN)
10.1.3.11 (N1)

Como puede verse la ruta es simétrica, aun cuando la forma de presentar la información puede dar 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 para RN.

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

Etiqueta Interfaz	Nombre interfaz	Dirección IP	Máscara
Ethernet 0, AUI 0 ó 10BT ETHERNET	Ethernet 0	10.1.2.25	255.255.255.0
Ethernet 1, AUI 1 ó 10/100 ETHERNET	Ethernet 1 ó Fastethernet 0	10.1.3.25	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 conmutador Sur a la interfaz Ethernet 0, AUI 0 ó 10BT ETHERNET del router RS y la interfaz 5 del conmutador a la interfaz Ethernet 1, AUI 1 ó 10/100 ETHERNET. 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 10.1.2.15 ó 10.1.3.15 que pertenecen a RN. Para que los ordenadores utilicen RS debemos asignarles como 'default gateway' las direcciones de RS (10.1.2.25 ó 10.1.3.25, 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.

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

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 10.1.2.15
# route add default gw 10.1.2.25
```

Para los ordenadores nones la secuencia de comandos será:

```
# route del -net 0.0.0.0 gw 10.1.3.15
# route add default gw 10.1.3.25
```

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 conmutador Sur mediante el comando en modo Configuración Global **'ip default-gateway 10.1.2.25'** (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 conmutadores, tanto dentro de un mismo edificio como entre edificios diferentes.

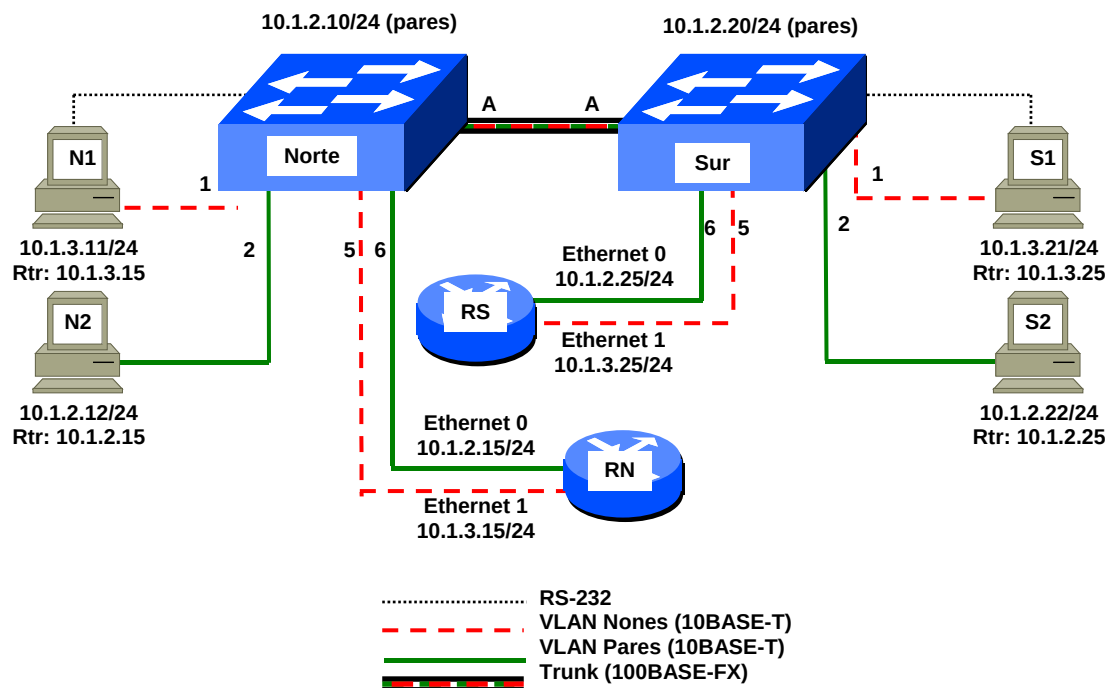


Figura 11. Interconexión de las dos VLANs mediante dos routers y rutas asimétricas

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 conmutadores. 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.

Redes

- 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 nuevamente el comando '**ping -R**' los alumnos deberán comparar el resultado con el obtenido anteriormente y comprobar que cuando el destino se encuentra en el otro conmutador 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 del conmutador es la 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. Obsérvese que esta dirección MAC no tiene nada que ver con la dirección (o direcciones) MAC de los equipos que puedan eventualmente estar conectados a esta interfaz, cuyas direcciones pueden verse con el comando '**show mac-address-table**'. De hecho la interfaz tendrá su dirección MAC propia aún en el caso de que no haya ningún equipo conectado a ella.
4. La MTU (Maximum Transfer Unit) o cantidad máxima de información útil que puede contener una trama en esta interfaz es 1500 bytes (tamaño máximo de la parte de datos en una trama Ethernet). 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.

Redes

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 de recepción (lado izquierdo):

- **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.

Práctica 1: Conmutadores LAN, Spanning Tree y VLANs

Estadísticas de transmisión (lado derecho):

- **Total frames:** tramas enviadas por esa interfaz.
- **Total octets:** bytes contenidos 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. 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 <i>dirección_IP</i> netmask <i>máscara</i>	Asigna la dirección IP indicada con la máscara indicada a la tarjeta Ethernet eth0 del ordenador
iperf -c <i>dirección_IP</i>	Ejecuta el programa iperf en modo cliente con las opciones por defecto hacia la dirección indicada
iperf -s	Pone en marcha el programa iperf en modo servidor
Minicom	Ejecuta el programa de emulación de terminal minicom
ping <i>dirección_IP</i>	Prueba la conectividad a nivel IP con la dirección de destino indicada
ping -b <i>dirección_IP</i>	Envía paquetes de ping a una dirección broadcast
ping -f <i>dirección_IP</i>	Envía paquetes de ping a razón de 100 por segundo
ping -R -n <i>dirección_IP</i>	Envía paquetes solicitando se registre la ruta seguida a la ida y a la vuelta, sin hacer resolución de nombres
route add default gw <i>dirección_IP</i>	Asigna un router por defecto para la comunicación con otras redes
route del -net 0.0.0.0 gw <i>dirección_IP</i>	Elimina el router por defecto asignado con 'route add default gw'
service iptables stop	Desactiva por completo el cortafuegos del host
shutdown -h 0	Termina el sistema ordenadamente sin esperar
telnet <i>dirección_IP</i>	Se conecta como terminal remoto a la dirección IP indicada

Apéndice III. Comandos del intérprete de 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 <i>interfaz</i>	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
ENable	Usuario	Entra en modo Privilegiado
ENable Password Level 15 <i>password</i>	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 <i>interface</i>	Cfg Glb	Entra en modo Configuración de Interfaz para la interfaz indicada
IP Address <i>dirección_IP máscara</i>	Cfg Glb	Asigna la dirección IP y máscara indicadas al conmutador
IP DEfault-gateway <i>dirección_IP</i>	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 <i>números</i>	Cfg Glb	Asocia la dirección IP del conmutador con la VLAN indicada
MAc-address-table Aging-time <i>tiempo</i>	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 <i>interface</i>	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 <i>costo</i>	Cfg Int	Establece para esta interfaz el costo indicado a efectos de Spanning Tree
SPantree Priority <i>prioridad</i>	Cfg Int	Establece para esta interfaz la prioridad indicada a efectos de Spanning Tree
SPANTREE-template VLAN Priority <i>prioridad</i>	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 <i>número</i> Name <i>nombre</i>	Cfg Glb	Crea la VLAN del número indicado y le asocia el nombre indicado
Vlan-membership Static <i>número</i>	Cfg Int	Asocia a la interfaz correspondiente la VLAN indicada.