

# 5

## Unidad

### Dispositivos específicos de la red local



En esta unidad aprenderemos a:

- Distinguir las funciones de los dispositivos de interconexión de la red.
- Elegir los dispositivos de red de área local en función de las necesidades.
- Configurar redes locales virtuales y gestionar los bucles de la red.

Y estudiaremos:

- El funcionamiento del módem.
- La funcionalidad de *hubs* y conmutadores.
- El comportamiento de los sistemas operativos en la configuración de redes.



CEO

- S M R \_ R L \_ A A b a d \_ 0 5 \_  
ModemsAnalógicos.docx
1. Elementos del módem analógico.
  2. Normativas estándares para módems y lenguaje Hayes.
  3. Caso práctico de utilización de Hyperterminal.

**Claves y consejos**

En ADSL hay que distinguir el ancho de banda de subida del de bajada, es decir, la velocidad a la que se pueden poner datos en la red y a la que se pueden descargar es diferente, lo que hay que tener en cuenta si hay mucho tráfico de salida hacia Internet ya que la velocidad de subida es mucho menor que la de bajada.

**Truco**

En las instalaciones domésticas en las que se comparten varios supletorios telefónicos sobre la misma línea compartida con el servicio ADSL, debe instalarse en cada teléfono un microfiltro que filtra la señal de voz hacia el teléfono impidiendo que le llegue la señal de modulación de ADSL, que se interpretaría en el teléfono como ruido.



CEO

- S M R \_ R L \_ A A b a d \_ 0 5 \_  
AccesosInternetModem.docx
- Documento sobre:
1. Cómo acceder a Internet mediante módem analógico.
  2. Comprobación y configuración del módem.

**Actividades**

1. Busca los errores técnicos en el siguiente razonamiento:  
«Mi portátil tiene integrado un módem analógico. He contratado un acceso ADSL con mi compañía telefónica y me han comunicado que me lo servirán por mi línea

de teléfono analógica. Para evitar tener que comprar un módem ADSL, utilizaré mi módem que, al ser analógico, es compatible con el servicio ADSL que me envían por mi línea de teléfono analógica.»

## 1. El acceso remoto a la red

Una vez concluido el estudio del nivel físico de la red —cables, conectores e instalación a lo largo de la edificación—, hay que analizar los dispositivos que permiten el intercambio de datos entre los diferentes nodos de la red, incluso aunque estén situados en distintos segmentos de la misma.

Además, nos adentraremos en la creación de redes de área local virtuales, que permiten corregir la inflexibilidad del sistema de cableado, al igual que la conexión de un nodo a un segmento de red con independencia de su ubicación física.

El acceso a los servicios proporcionados por la red de área local se realiza normalmente desde las estaciones conectadas a la misma LAN. Sin embargo, en ocasiones esto no es posible debido a la distancia geográfica que separa al cliente del servidor.

Vamos a estudiar algunas de las tecnologías utilizadas para conseguir un acceso remoto. Tradicionalmente se han utilizado módems analógicos, pero con la llegada de la banda ancha, esto ha sido sustituido por módems ADSL o de cable u otras tecnologías de alta velocidad.

### 1.1. El módem ADSL y el cable-módem

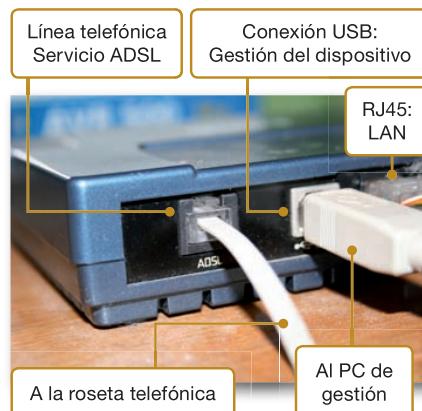
Estrictamente hablando, el módem es un conversor analógico-digital que se utiliza para transmitir información digital por las líneas telefónicas apropiadas para la transmisión de señales analógicas. Sin embargo, también suele aplicarse este término para el caso de los módems ADSL o los módems de cable.

#### A. Tecnología ADSL

DSL son las siglas de *Digital Subscriber Line*. Delante de estas siglas suele ponerse otra letra que identifica la familia específica dentro de DSL, por ello nos referiremos, en general, a tecnologías xDSL.

Con ADSL se trata de aprovechar el mismo cableado del teléfono analógico para la transmisión de datos a Internet a alta velocidad estableciendo dos canales de comunicación sobre la misma línea física.

De todas las modalidades de DSL, nos centraremos básicamente en ADSL por ser la tecnología mayoritariamente implantada por las compañías telefónicas.



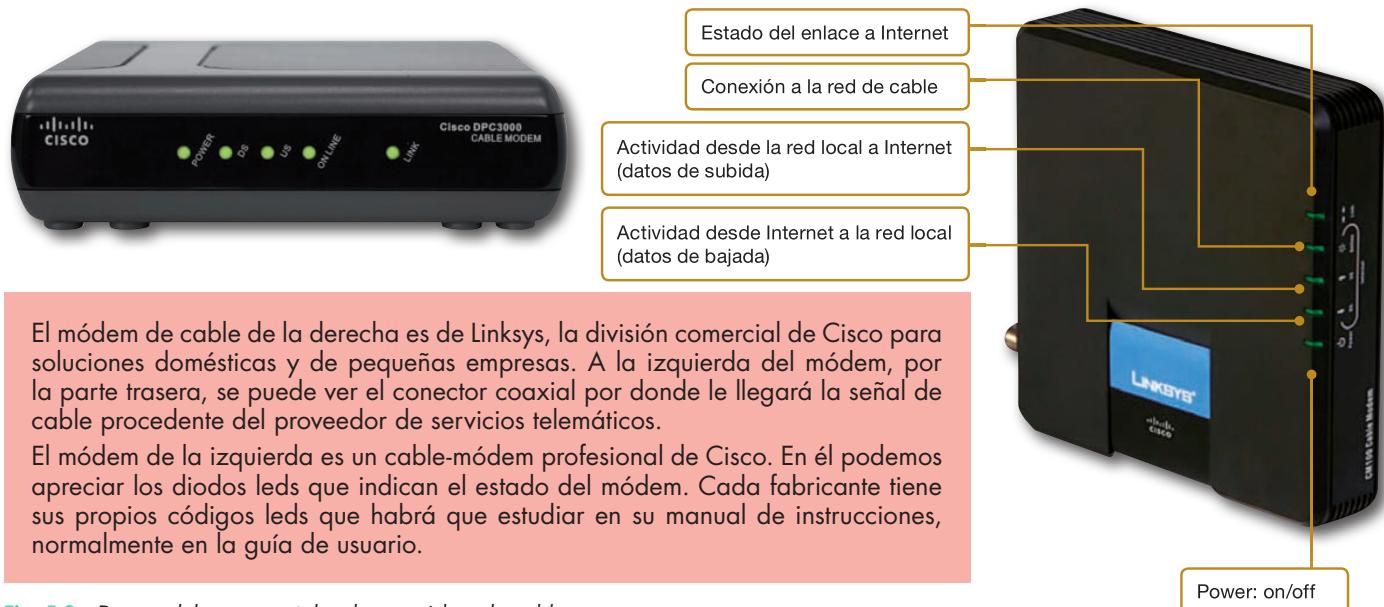
**Fig. 5.1.** Detalle de la vista posterior de un router/módem ADSL en producción.

#### B. Módems de cable

Un módem de cable o cable-módem es un dispositivo que nos permite acceder a Internet a alta velocidad utilizando la infraestructura de las redes de televisión por cable.

Las velocidades de transmisión son muy variables, pero suelen estar entre los 300 Kbps y los 10 Mbps, aunque la tecnología permitiría transmisiones hasta los 40 Mbps.

Los usuarios pueden estar recibiendo sus canales de televisión y simultáneamente estar transmitiendo o recibiendo datos de Internet.



El módem de cable de la derecha es de Linksys, la división comercial de Cisco para soluciones domésticas y de pequeñas empresas. A la izquierda del módem, por la parte trasera, se puede ver el conector coaxial por donde le llegará la señal de cable procedente del proveedor de servicios telemáticos.

El módem de la izquierda es un cable-módem profesional de Cisco. En él podemos apreciar los diodos leds que indican el estado del módem. Cada fabricante tiene sus propios códigos leds que habrá que estudiar en su manual de instrucciones, normalmente en la guía de usuario.

Fig. 5.2. Dos modelos comerciales de un módem de cable.



### Ejemplos

#### Análisis de la configuración de un encaminador ADSL

La configuración de un dispositivo ADSL es muy frecuente en la práctica profesional puesto que cualquier empresa o particular que requiera una conexión a Internet tendrá uno de estos dispositivos.

A veces, el operador del servicio nos lo configurará de modo semiautomático, pero si fuera necesario tener un control exhaustivo de los parámetros de configuración de red, tendríamos que configurarlo nosotros mismos personalmente.

En el caso del router ADSL, se conecta directamente a la red pues estos encaminadores tienen, además de la interfaz telefónica para ADSL, otra interfaz Ethernet para su conexión a la red corporativa. El router que hemos elegido en este ejemplo es gestionable a través del explorador de Internet puesto que incorpora un servidor web a través del cual se puede configurar.

En la Fig. 5.3 podemos ver dos fichas: el resumen de configuración y el resumen de los servicios que proporciona. Podemos observar los parámetros IP de las dos interfaces del módem (el



### Truco

Frecuentemente, los operadores de ADSL proporcionan a sus clientes módems ADSL en vez de routers ADSL. La diferencia más significativa entre ellos reside en el modo en que se conecta a nuestra instalación de red. En el caso del módem ADSL se suele conectar por su puerto USB a un ordenador de la red que hace las funciones de servidor de comunicaciones, comportándose de modo semejante al módem analógico, pero conservando todas las características de la banda ancha.

de ADSL y el de Ethernet), así como parte de la configuración de ATM, la banda ancha en la que termina por desembocar ADSL (parámetro VPI/VCI). Además, podemos ver que el router proporciona a la red corporativa los servicios de DNS y el de NAPT, en el que se profundizará más adelante.

Fig. 5.3. Fichas de resumen de configuración y servicios en un router ADSL.

Continúa...



## Ejemplos

...Continuación

En la Fig. 5.4 se especifican algunos detalles más sobre las configuraciones de las dos interfaces de red. La mayor parte de estos parámetros son proporcionados por el proveedor del servicio ADSL.

Nosotros solo tendremos que configurar la dirección IP del router en su interfaz de conexión a nuestra red corporativa, que en nuestro ejemplo es 10.1.1.1 con máscara 255.255.0.0.

La figura 5.4 muestra dos capturas de pantalla del "SpeedStream 5660 Router Management Interface" en Microsoft Internet Explorer. Ambas capturas muestran tablas de estadísticas para diferentes interfaces.

**Captura 1 (Izquierda): AAL5 Statistics**

	Transmit	Receive
SDUs	232790	272002
Cells	929829	5042011
Octets	34515956	233462833
Errors	0	0
Discards	0	872
SAR Timeouts		0
CRC Errors		773
Oversized SDUs	0	0

**Captura 2 (Derecha): Ethernet Statistics**

	Transmit	Receive
Packets	263396	233219
Octets	234090233	37859444
CRC Errors		167
Long Frames		0
Runt Frames		43
Alignment Errors		0

Fig. 5.4. Detalles de configuración de las interfaces de red de un router ADSL.

Una vez que el router está funcionando, el administrador podrá consultar las estadísticas de conexiones y estudiar su rendimiento. En la Fig. 5.5 tenemos dos detalles de estas estadísticas, la primera de ellas (a la izquierda) para la red ATM (que es la red de transporte utilizada por la tecnología ADSL) y la segunda (a

la derecha) para la interfaz Ethernet que es la utilizada en la conexión a la red corporativa local: el encaminador se encarga de traspasar paquetes entre estas dos redes según unas reglas determinadas por el administrador del router y el servicio prestado por el proveedor telemático.

La figura 5.5 muestra dos capturas de pantalla del "SpeedStream 5660 Router Management Interface" en Microsoft Internet Explorer. Ambas capturas muestran tablas de estadísticas para diferentes interfaces.

**Captura 1 (Izquierda): AAL5 Statistics**

	Transmit	Receive
SDUs	232790	272002
Cells	929829	5042011
Octets	34515956	233462833
Errors	0	0
Discards	0	872
SAR Timeouts		0
CRC Errors		773
Oversized SDUs	0	0

**Captura 2 (Derecha): Ethernet Statistics**

	Transmit	Receive
Packets	263396	233219
Octets	234090233	37859444
CRC Errors		167
Long Frames		0
Runt Frames		43
Alignment Errors		0

Fig. 5.5. Fichas de estadísticas de transmisión en un router ADSL.



## Caso práctico 1

### Configurando un acceso a Internet por módem

Como ejemplo, vamos a crear un acceso a Internet en el PC utilizando el asistente del acceso telefónico a redes. Aunque en la actualidad la inmensa mayoría de los accesos a Internet son de banda ancha (normalmente ADSL), es interesante conocer cómo se configura una conexión a Internet utilizando un módem analógico.

Es una situación que puntualmente puede resolver el problema de una caída en los dispositivos ADSL de las centrales telefónicas, sustituyendo estas conexiones habituales por un acceso vía módem para comunicaciones críticas o de urgencia mientras el proveedor de Internet soluciona sus problemas.

También puede resolver problemas de conexión en lugares en donde no hay cobertura de banda ancha pero en los que sí llega una línea telefónica analógica. La idea principal es poder tener un acceso a Internet, aunque sea de muy baja calidad, en cualquier sitio en donde haya una roseta de teléfono.

1. En primer lugar, crea una conexión nueva en el panel de control de Conexiones de red (Fig. 5.6, arriba a la izquierda). Windows separa las conexiones de acceso telefónico (arriba) de las conexiones de redes de área local (abajo).
2. Una vez que ejecutas el asistente, aparecerán las fichas que se describen en la Fig. 5.7, en las que vas a informar a Windows de que quieras realizar una conexión a Internet (a la izquierda) y, haciendo clic en *Siguiente*, que vas a establecer la conexión manualmente; de este modo te permitirá agregar la información suministrada por el proveedor de la cuenta de acceso.
3. A continuación, elige la asignación de un módem como medio para realizar la conexión y proporciona un nombre

a la misma (Fig. 5.8) haciendo clic en *Siguiente*. Con este nombre, Windows fabricará un icono que será el que tengas que activar para realizar posteriormente la conexión.

Ya está configurada la parte de la conexión que tiene que ver con el módem, pero aún falta la asignación de los valores que el proveedor nos proporcionó cuando solicitamos la cuenta de acceso.

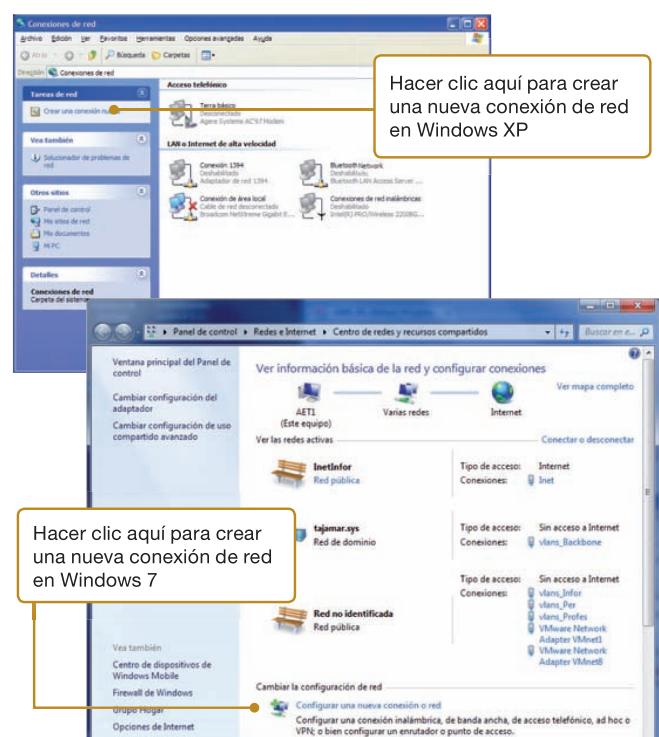


Fig. 5.6. Ventana de conexiones de red de Windows XP y 7.

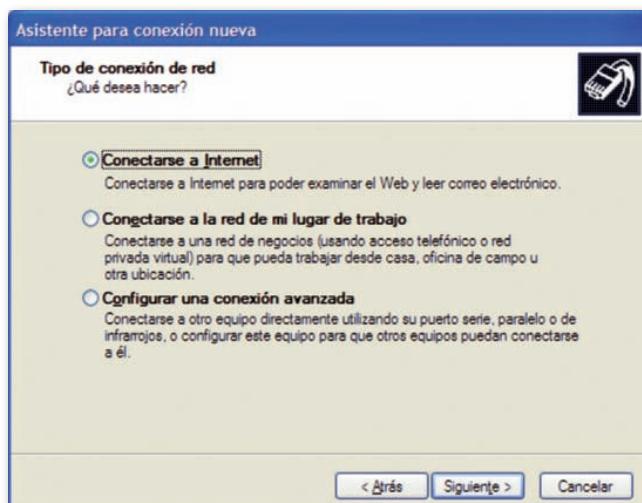
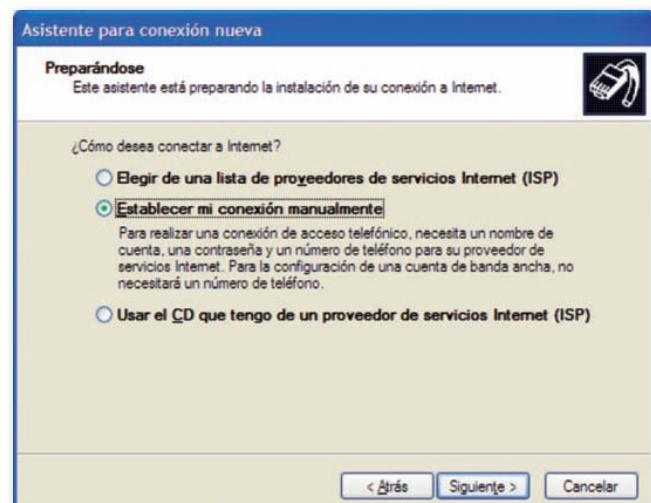


Fig. 5.7. Asistente de creación de una conexión nueva en Windows.



Continúa...



## Caso práctico 1

...Continuación

The figure consists of two side-by-side windows from the Windows New Connection Wizard.

**Left Window (Conexión de Internet):**

- Section:** Conexión de Internet  
¿Cómo desea conectar a Internet?
- Options:**
  - Conectarse usando un módem de acceso telefónico  
Este tipo de conexión usa un módem y una línea telefónica regular ISDN (Red digital de servicios integrados, RDSI).
  - Conectarse usando una conexión de banda ancha que necesita un nombre de usuario y una contraseña  
Esta es una conexión de alta velocidad que usa tanto un módem ADSL como por cable. El ISP puede referirse a este tipo de conexión como de protocolo punto a punto en Ethernet (PPPoE).
  - Conectarse usando una conexión de banda ancha que está siempre activa  
Esta es una conexión de alta velocidad que usa tanto un módem por cable, ADSL o LAN. Está siempre activa y no necesita iniciar sesión.
- Buttons:** < Atrás, Siguiente >, Cancelar

**Right Window (Nombre de conexión):**

- Section:** Asistente para conexión nueva  
Nombre de conexión  
¿Cuál es el nombre del servicio que le proporciona conexión a Internet?
- Text:** Escriba el nombre de su proveedor de servicios Internet (ISP) en el cuadro siguiente.
- Text:** Nombre de ISP
- Text:** El nombre que escriba aquí será el de la conexión que está creando.
- Buttons:** < Atrás, Siguiente >, Cancelar

Fig. 5.8. Asignación del módem y denominación de la conexión.

4. En la Fig. 5.9 asigna el número de teléfono al que tenemos que marcar, el nombre de usuario y la contraseña de acceso. Estos tres datos te los tiene que proporcionar el proveedor de Internet.

Además, podemos hacer que este usuario y contraseña sean utilizados por cualquier usuario del equipo, que esa sea la conexión que se marque por defecto o indicarle al cortafuegos del equipo que se haga cargo de vigilar la conexión.



## Truco

Si vamos a llamar a través de una centralita, tendremos que incorporar los prefijos adecuados para que la centralita pueda conmutar la llamada que hacemos (internal) con una línea externa. Es muy típico de las centralitas tener que marcar un «0», esperar un tono continuo de conexión con el exterior y solo después marcaremos el número de destino.

The figure consists of two side-by-side windows from the Windows New Connection Wizard.

**Left Window (Número de teléfono que desea marcar):**

- Section:** Asistente para conexión nueva  
Número de teléfono que desea marcar  
¿Cuál es el número de su proveedor de servicios Internet?
- Text:** Escriba el número telefónico a continuación.
- Text:** Número de teléfono:
- Text:** Es posible que necesite incluir un "1", el código de área o ambos. Si no está seguro de que necesita números adicionales, marque el número sin más. Si el módem emite un sonido, el número que ha marcado es el correcto.
- Buttons:** < Atrás, Siguiente >, Cancelar

**Right Window (Información de cuenta de Internet):**

- Section:** Asistente para conexión nueva  
Información de cuenta de Internet  
Necesitará un nombre de cuenta y una contraseña para suscribirse a una cuenta de Internet.
- Text:** Escriba un nombre de cuenta ISP y contraseña, a continuación escriba esta información y almacénela en un lugar seguro. (Si ha olvidado un nombre de cuenta existente o contraseña, póngase en contacto con su proveedor de servicios Internet (ISP)).
- Text:** Nombre de usuario:
- Text:** Contraseña:
- Text:** Confirmar contraseña:
- Checkboxes:**
  - Usar el nombre de usuario y contraseña siguientes siempre que un usuario cualquiera se conecte a Internet desde este equipo
  - Establecer esta conexión a Internet como predeterminada
  - Activar el Servidor de seguridad de Internet para esta conexión
- Buttons:** < Atrás, Siguiente >, Cancelar

Fig. 5.9. Asignación del número de teléfono y de la identificación del usuario de la conexión.

5. Llegados a este punto, el asistente crea la conexión con los parámetros que le hemos proporcionado. Ahora solo falta la incorporación de los parámetros de la red

TCP/IP a la que te vas a conectar. Estos parámetros los puedes editar desde las propiedades de la nueva conexión recién creada (Fig. 5.10). *Continúa...*



### Caso práctico 1

...Continuación

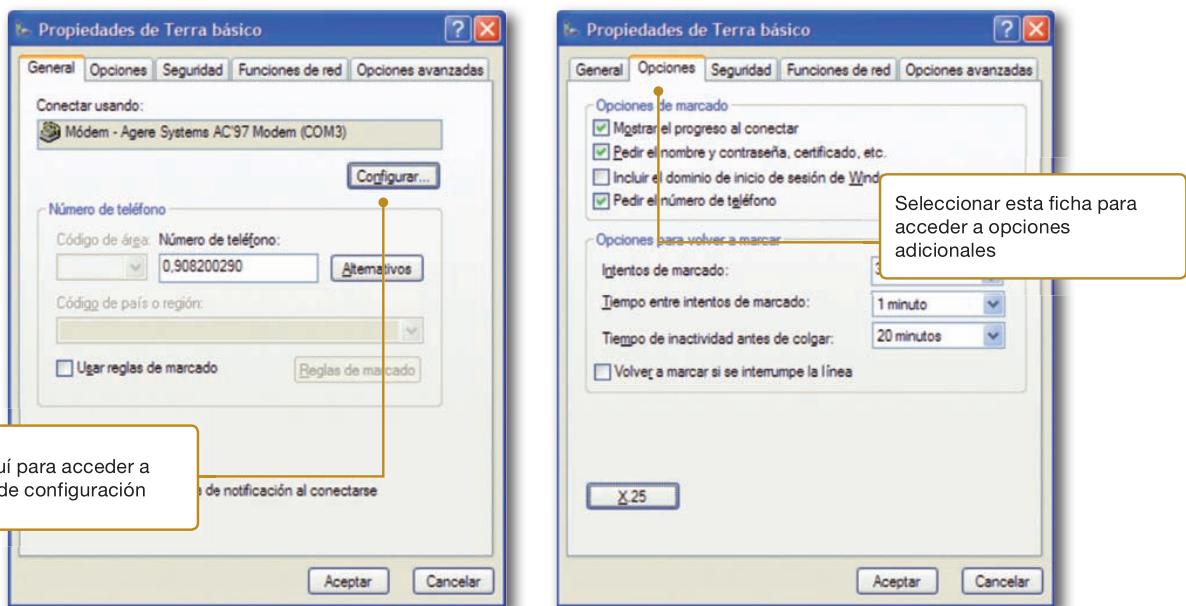


Fig. 5.10. Propiedades de la conexión telefónica: fichas General y Opciones.

6. Despues puedes especificar si el proveedor requiere o no una contraseña segura (o cifrada) o bien si se podrá utilizar una tarjeta inteligente para la identificación de

la conexión. Además, en la ficha de funciones de red puedes ajustar los parámetros del protocolo TCP/IP (Fig. 5.11).

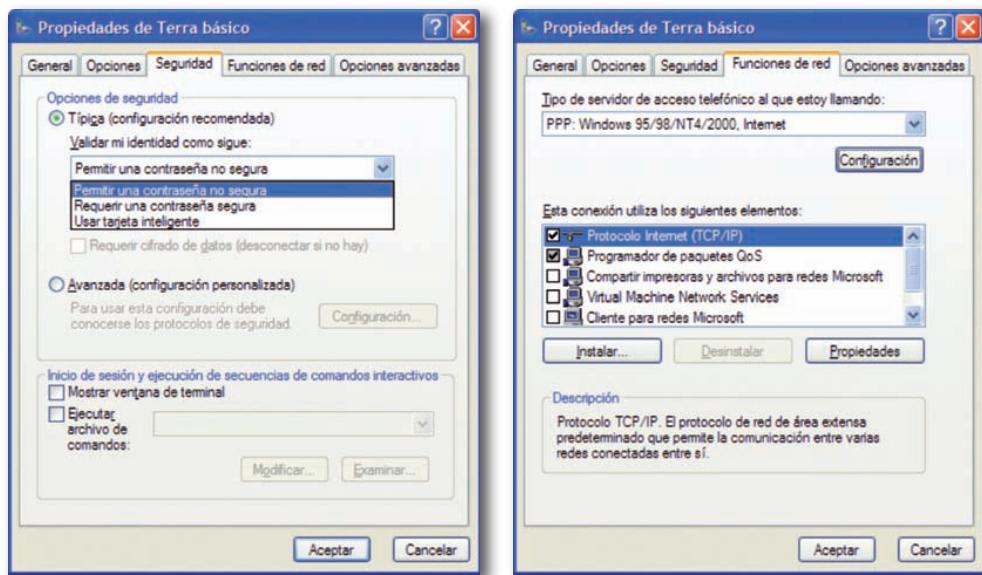


Fig. 5.11. Fichas de identificación del usuario y definición de los elementos de red utilizados en la conexión.

Continúa...



### Caso práctico 1

...Continuación

7. Si seleccionas el protocolo TCP/IP y haces clic en el botón de propiedades, aparecerá algo semejante a la ventana que vemos en la Fig. 5.12. En esta ficha le has dicho a Windows que el proveedor nos asignará la dirección IP automáticamente. Si no fuera así, el proveedor te diría qué valor tienes que escribir aquí.

También has asignado las direcciones de los dos servidores DNS que nos especificó el proveedor. A veces el proveedor también asigna los DNS automáticamente.



### Claves y consejos

Cuando se contrata un servicio de comunicaciones con un operador, este debe especificarnos los parámetros de conexión adecuados que debemos utilizar. En muchos casos, el operador nos asignará estos parámetros automáticamente al identificarnos en el servicio.

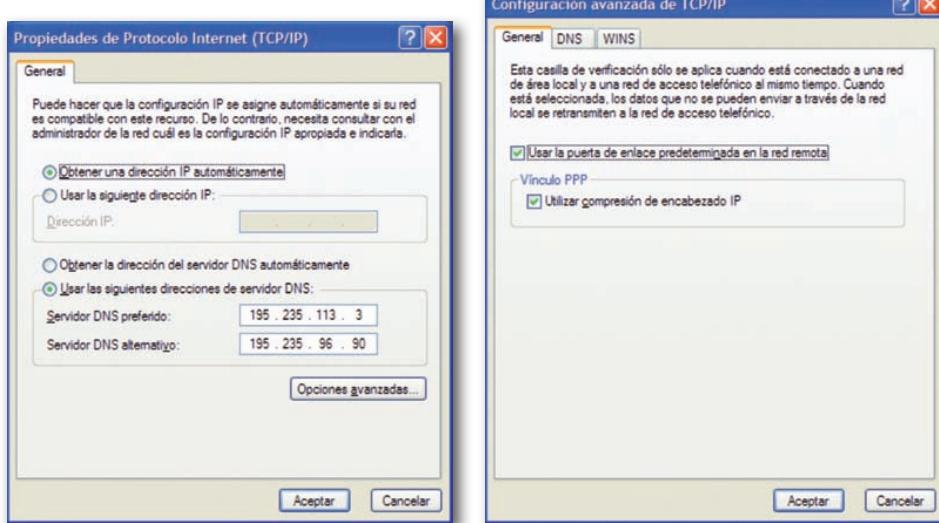


Fig. 5.12. Fichas de configuración del protocolo TCP/IP en una conexión de red por acceso telefónico.

8. En las opciones avanzadas puedes terminar de ajustar el TCP/IP. Habitualmente, salvo que el proveedor diga lo contrario, serán suficientes los valores por defecto que Windows sugiere. Con estas operaciones acaba el procedimiento de configuración del acceso de red.
9. Ahora solo te falta probar la conexión haciendo doble clic en el ícono que Windows habrá creado en las *Conexiones de red*; aparecerá en pantalla la ficha de identificación de usuario y el número de teléfono que se debe marcar (Fig. 5.13).

Podemos validar la información de conexión que Windows nos presenta o modificarla como sea necesario. La conexión se iniciará cuando hagamos clic sobre el botón *Marcar*.

Esto mismo puede hacerse fácilmente en un sistema Linux, aunque el modo concreto de hacerlo dependerá de la distribución de Linux de que se disponga y de la versión. Si el módem analógico es externo, no suele haber dificultades especiales ya que el módem funcionará con solo encenderlo y

únicamente tendremos que ocuparnos de configurar las comunicaciones con él por el puerto serie del PC que ejecute Linux.



Fig. 5.13. Ventana de conexión por acceso telefónico en un sistema Windows.

Continúa...



### Caso práctico 1

...Continuación

En cambio, si el módem es interno la dificultad mayor reside en encontrar los controladores apropiados para el módem, que deberán estar escritos específicamente para el hardware del módem.

Frecuentemente estos controladores se encuentran con mayor dificultad en Linux que en Windows, sobre todo si se trata de módems más modernos.

Una vez que el sistema operativo Linux haya reconocido el módem podremos configurar la conexión en la ficha de *Configuración de la red* (Fig. 5.14-A), a la que se puede acceder desde el submenú de administración del menú de sis-

tema. En ella seleccionaremos la conexión por módem que aparezca.

Hay que fijarse en que la interfaz de comunicaciones que utilizará Linux es *ppp0* (*point to point protocol*), para protocolos de conexión punto a punto.

En las propiedades de la conexión de módem, podremos activar o desactivar la conexión, configurar el número de teléfono, el prefijo de marcado y los datos de identificación de usuario: nombre y contraseña asignados por el proveedor del servicio de conexión (Fig. 5.14-B).

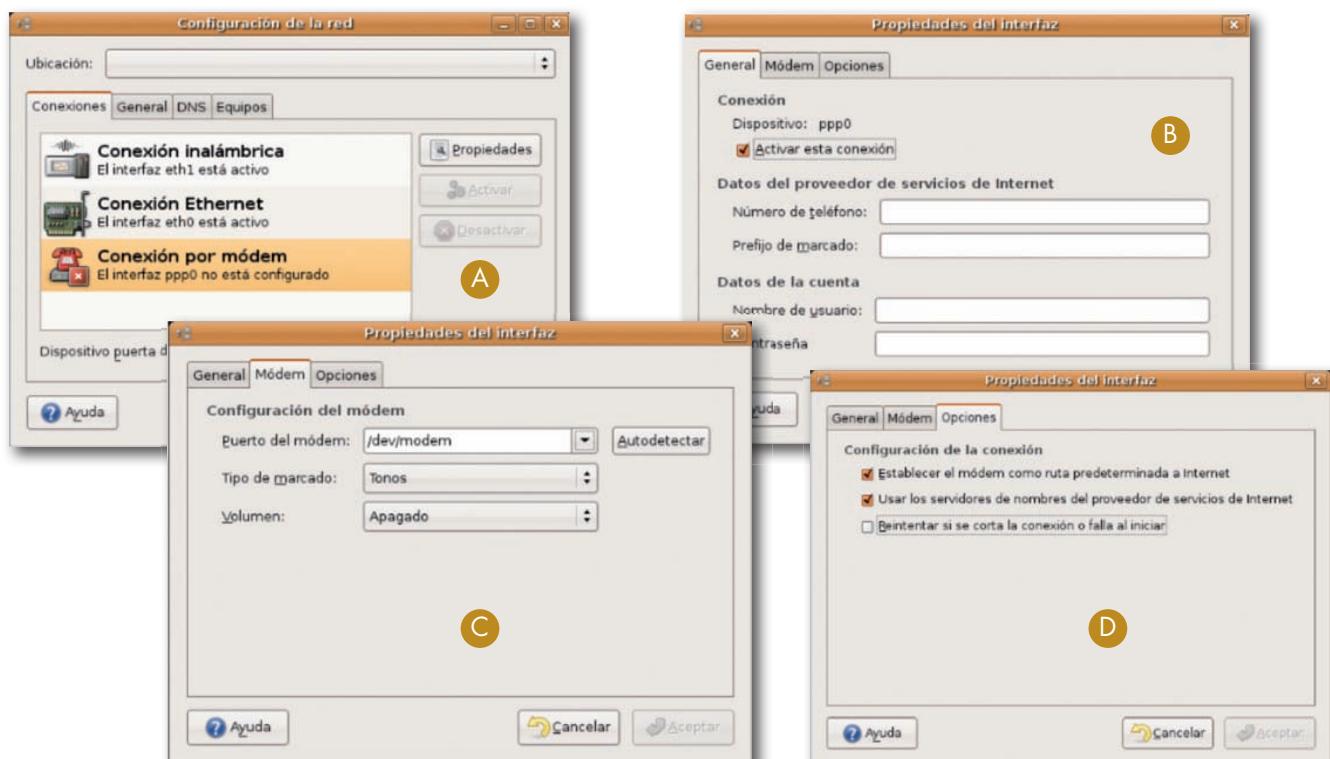


Fig. 5.14. Configuración de un módem en Ubuntu (A). Ficha de configuración general de la conexión (B). Fichas de gestión de módem (C) y opciones de red (D) en la configuración de una conexión por módem en Ubuntu.

En la ficha de la Fig. 5.14-C podremos configurar algunos parámetros de modo automático si Linux es capaz de autodetectar nuestro módem, así como asignar si queremos que este marque por tonos o por pulsos y ajustar el volumen del altavoz. En esta ficha también aparece el nombre del puerto utilizado por el módem para su comunicación con el sistema operativo: en nuestro caso */dev/modem* que se corresponde con un módem interno.

Por último, en la ficha de configuración de *Opciones*, podremos indicarle al sistema operativo que para enviar paquetes al exterior del PC utilice los parámetros de red de la conexión por módem en vez de las propias de la red de área local procedentes de otras posibles interfaces de red (Fig. 5.14-D).

En el caso de esta figura se utilizará la ruta predeterminada a Internet (puerto por defecto de la conexión) y los servidores de nombres que proporcione el proveedor (servidores DNS o de nombres NetBIOS).

**Vocabulario**

**Instalación en cascada:** se dice que un conjunto de dispositivos están instalados en cascada o de modo jerárquico cuando unos están conectados a los otros de modo que la salida de uno es la entrada de otro.



**Fig. 5.16.** Distintos modelos de repetidores. Hub doméstico (abajo, a la izquierda). Transceptor 10Base2/10Base5 (abajo, a la derecha). Obsérvese cómo el repetidor tiene en la parte superior una interfaz coaxial y en el frontal varios puertos RJ45 para intercambiar señales entre estos dos distintos tipos de red. El transceptor adecúa la señal de su canal coaxial al de pines.

## 2. Repetidores y concentradores

Las señales eléctricas se degradan al transmitirse. Cuando la longitud del cable de red es grande, la señal puede llegar al otro extremo casi imperceptible, lo que origina problemas graves en las transmisiones. El modo más básico de solucionar estos problemas consiste en la utilización de **repetidores** o concentradores (*hubs*).

El repetidor es un elemento de red que regenera la señal eléctrica que le llega con el fin de restituir su nivel original, y así evitar los problemas que se pudieran producir por una excesiva atenuación.

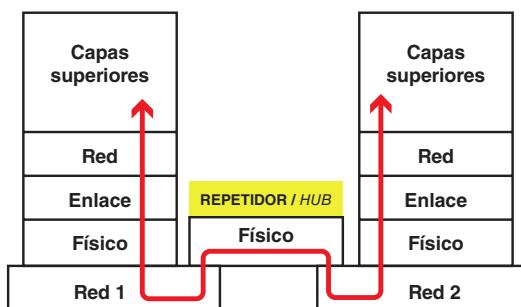
Teóricamente es posible instalar tantos repetidores en una red como sean necesarios, sin embargo, hay serias razones que impiden su **instalación en cascada** en gran número.

Los repetidores operan en el nivel físico, puesto que trabajan con señales. Esto hace que sean rápidos, aunque no puedan procesar los datos que circulan a través de ellos.

En ocasiones, los repetidores se pueden utilizar para convertir la señal de un sistema de cableado en otro. Por ejemplo, un repetidor podría tener una entrada 10Base2 (coaxial) y otra 10BaseT (par trenzado).

Los repetidores operan en el nivel físico, puesto que trabajan con señales. Esto hace que sean rápidos, aunque no puedan procesar los datos que circulan a través de ellos.

En ocasiones, los repetidores se pueden utilizar para convertir la señal de un sistema de cableado en otro. Por ejemplo, un repetidor podría tener una entrada 10Base2 (coaxial) y otra 10BaseT (par trenzado).



**Fig. 5.15.** Modelo de capas para un repetidor o hub. El repetidor opera con señales por eso es un dispositivo que solo contempla la capa física para unir los nodos origen y destino.

La ventaja principal de un *hub* reside en la facilidad de operación: se limita a copiar bits de un segmento de red en otros. No requiere ningún tipo de configuración especial puesto que opera en el nivel físico. No atiende a las direcciones de red, protocolos, servicios, etc. Sencillamente repite la señal de la red a gran velocidad.

La mayor limitación del *hub* consiste en que no aísla de los problemas del tráfico generados en la red en cada uno de los segmentos: si en uno de los segmentos se produce una colisión, esta se propagará por todos los segmentos de la red.

**Actividades**

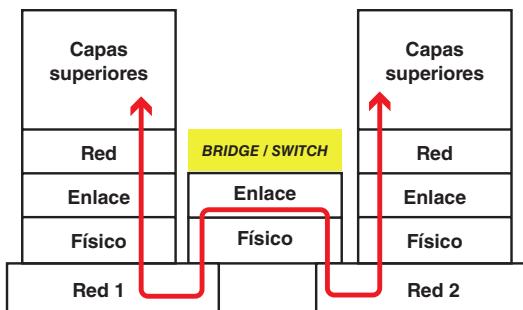
2. Una red local está compuesta por varios segmentos de red. Los segmentos están unidos por medio de un dispositivo de interconexión. Una estación de la red está infectada por un virus de tipo gusano y está generando mucho tráfico Ethernet en el segmento de red en que está la estación. ¿Pasa ese tráfico de un segmento a otro si el dispositivo de interconexión es un concentrador? ¿Y si fuera un repetidor?
3. Seguimos trabajando sobre la configuración de red del ejercicio precedente. Ahora vamos a suponer que el cableado de red es coaxial y lo que ocurre es que se rompe uno de los segmentos de red. Como la red queda abierta, el segmento de red en que se ha producido la rotura deja de funcionar. ¿Funcionarán el resto de los segmentos de red si el dispositivo de interconexión es un repetidor? ¿Y si la red fuera de cable de pares en vez de coaxial y el dispositivo de interconexión fuera un concentrador?

## 3. Puentes

El **punto** o *bridge* es un elemento de cierta capacidad de control. Puede aceptar y reexpedir las tramas que le llegan en función del contenido de las mismas. La instalación de un puente en una red de área local es justificable, por ejemplo, cuando se desea aislar el tráfico en cada segmento de red que conecta el puente.

Los puentes operan en nivel 2 de OSI, es decir, su unidad de operación básica es la trama de red (Fig. 5.17). Cuando un puente debe pasar una trama de un segmento a otro de la red ejecuta las siguientes fases:

- Almacena en memoria la trama recibida por cualquier puerto para su análisis posterior.
- Comprueba el campo de control de errores de la trama con el fin de asegurarse de la integridad de la misma. Si encontrara un error, eliminaría la trama de la red, con lo que tramas incompletas o erróneas no traspasarán la frontera del segmento de red en donde se produjo el fallo.
- Algunos puentes son capaces de retocar de modo sencillo el formato de la trama (añadir o eliminar campos) con el fin de adecuarla al formato del segmento destinatario de la misma.
- El puente reexpide la trama si determina que el destinatario de esta se encuentra en un segmento de red accesible por alguno de sus puertos.



**Fig. 5.17.** Modelo de capas para un puente o un conmutador. El switch opera con tramas por eso es un dispositivo que trabaja en la capa de enlace para unir los nodos origen y destino.

Puesto que los puentes operan en el nivel 2, no pueden tomar decisiones de encaminamiento que afecten a los protocolos o sistemas de direccionamiento del nivel 3: solo pueden operar con direcciones de nivel 2 (direcciones MAC). A este aislamiento de tráfico que se opera en los puentes o en dispositivos de red de nivel superior se le suele denominar «separación de los **dominios de colisión**» ya que dos estaciones situadas en diferentes segmentos no pueden colisionar en su acceso a la red, puesto que las tramas no pueden atravesar la frontera de los segmentos de red salvo que un puente tome la decisión de conmutarlas.



### Actividades

4. Descubre los errores técnicos en el siguiente argumento: «en mi oficina hay dos departamentos claramente diferenciados. En cada uno de ellos se genera mucho tráfico, pero apenas tienen relación entre sí. Se ha pensado en instalar un puente entre las dos redes departamentales, pero no hemos podido puesto que las dos redes están en el mismo edificio y los puentes solo pueden operar remotamente».
5. Una compañía tiene sede en dos ciudades, pero solo poseen una red local compartida entre las dos sedes y conectadas por un puente de red a través de redes públicas. El segmento de red de una de las ciudades es minoritario, pero en la otra sede residen los servidores y en su segmento de red se produce mucho tráfico local. ¿Pasarán ese tráfico al segmento de red minoritario? Un usuario de la sede minoritaria quiere enviar un fichero al servidor que reside en la sede mayoritaria a través del puente. A pesar de que el puente aísla del tráfico local, ¿podrá hacerlo?



### Vocabulario

**Dominio de colisión:** dos nodos de red pertenecen al mismo dominio de colisión si sus tramas pueden interferir entre sí.



### Ampliación

El repetidor, a diferencia del puente, no puede aislar del tráfico broadcast que se genere en la red, ya que difunde cualquier trama que llegue a cualquiera de sus puertos. Esto puede llevar a congestiones serias de la red. Por tanto, un repetidor nunca divide un dominio de colisión y no será capaz de parar las tormentas de tramas de multidifusión.

Tradicionalmente se han clasificado los puentes en transparentes y no transparentes:

- Un puente transparente o de árbol de expansión es un puente que no requiere ninguna configuración para su funcionamiento. Determina la reexpedición de tramas en función de los sucesos que observa por cada uno de sus puertos.
- Un puente no transparente necesita que la trama lleve información sobre el modo en que debe ser reexpedido.

Una segunda clasificación para los puentes se fija en si las dos redes a conectar están o no próximas. Según esto los puentes pueden ser:

- Locales. Un puente local aglutina en sí mismo dos o más segmentos de la misma red.
- Remotos. Un puente remoto está dividido en dos partes. Cada una de estas partes conecta un segmento de red y las dos partes están interconectadas a través de la línea de una red WAN, por ejemplo, una línea de teléfono o RDSI.



### Investigación

Los conmutadores son en la actualidad los dispositivos más utilizados para realizar el despliegue de la red: repetidores y concentradores solo se utilizan en casos muy específicos y siempre minoritarios. Los switches incorporan muchas otras funciones además de la commutación de tramas que es en la que se especializan.

Puedes investigar algunos ejemplos de estas tecnologías en Wikipedia por la voz «switch» y, más en concreto, en la tecnología «spanning tree».



### Ampliación

Aunque el aspecto externo de un hub coincide con el de un switch y, efectivamente, ambos distribuyen señal entre segmentos de red, hay diferencias sustanciales entre ellos. La más significativa es que mientras que en el hub el ancho de banda es compartido por todos los puertos mediante una multiplexación en el tiempo (solo una estación puede transmitir de un puerto a otro en cada instante), en el switch el ancho de banda está por encima del ancho de banda de cada uno de los puertos. De hecho, en los conmutadores de muy alto rendimiento, el ancho de banda del backplane (el bus interno que intercomunica todos los puertos del conmutador) es al menos la suma de los anchos de banda de cada uno de los puertos, con lo que se garantiza que la commutación será de alta velocidad, y que unos segmentos de red no interferirán en los otros. En un switch cada puerto representa un dominio de colisión diferente.

## 4. Conmutadores

El switch o conmutador es un dispositivo que tiene funciones del nivel 2 de OSI y que, por tanto, se parece a un bridge en cuanto a su funcionamiento. Sin embargo, tiene algunas características que lo distinguen:

- El switch es siempre local.
- Son dispositivos multipuerto.
- La velocidad de operación del switch es mayor que la del puente remoto, que introduce mayores tiempos de retardo al tener que utilizar una conexión WAN entre los dos segmentos de la LAN que interconecta.
- En un conmutador se puede repartir el ancho de banda de la red de una manera apropiada en cada segmento de red o en cada nodo, de modo transparente a los usuarios. Esto proporciona facilidades para la construcción de redes virtuales, que trataremos más adelante.
- Gran parte de los modelos comerciales de conmutadores son apilables y, por tanto, fácilmente escalables, lo que les da una flexibilidad semejante a los repetidores, pero con la funcionalidad de los puentes en cuanto a la gestión del tráfico de red se refiere.
- Algunos conmutadores de muy alto rendimiento se conectan en forma modular a un bus de muy alta velocidad (*backplane*) por el que producen su commutación.

Las tecnologías de commutación han avanzado de tal modo que en la actualidad se comercializan también conmutadores de nivel 3 o superior. Un conmutador de nivel 3 incorpora funciones de encaminamiento pero con la velocidad de la commutación.

En la Fig. 5.18 puede verse el modo de funcionamiento de un switch. El conmutador construye una tabla por cada puerto con las direcciones físicas de los dispositivos que ve por cada uno de ellos. Cuando le llega una trama, investiga en estas tablas para averiguar por qué puerto de todos los disponibles alcanza su destino y la transmite por ese puerto y solo por ese, a diferencia del hub que la transmitiría por todos los puertos disponibles salvo por el puerto por donde llegó.

Por ejemplo, si al switch le llega una trama cuya dirección física de destino es MAC4, el conmutador buscará esa dirección entre sus tablas de direcciones, la hallará disponible en el puerto 2 y conmutará la trama para que salga por ese puerto. La trama llegará al hub que está conectado a ese puerto segundo y el hub la transmitirá por todos sus puertos llegando a las estaciones PC4 (su destino) y PC5.

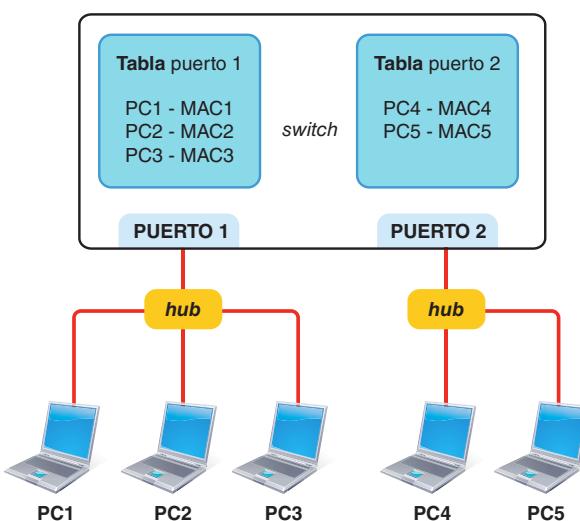


Fig. 5.18. Tablas de direcciones físicas en los puertos de un conmutador.

Los comutadores son gestionables por los protocolos típicos de gestión de red: **SNMP**, **RMON**, etc. Evidentemente, si se hace depender gran parte de la eficacia de la red de unos comutadores, interesaría que la vigilancia de estos sea muy estrecha. La mayoría de los *switches* pueden también gestionarse vía web porque incorporan un servidor web desde donde realizar su configuración, así como a través de conexiones telnet o ssh.

En la Fig. 5.19 podemos ver cómo el *switch* tiene sus parámetros de red TCP/IP como cualquier otro nodo de la red: dirección IP, máscara, puerta por defecto, etc.

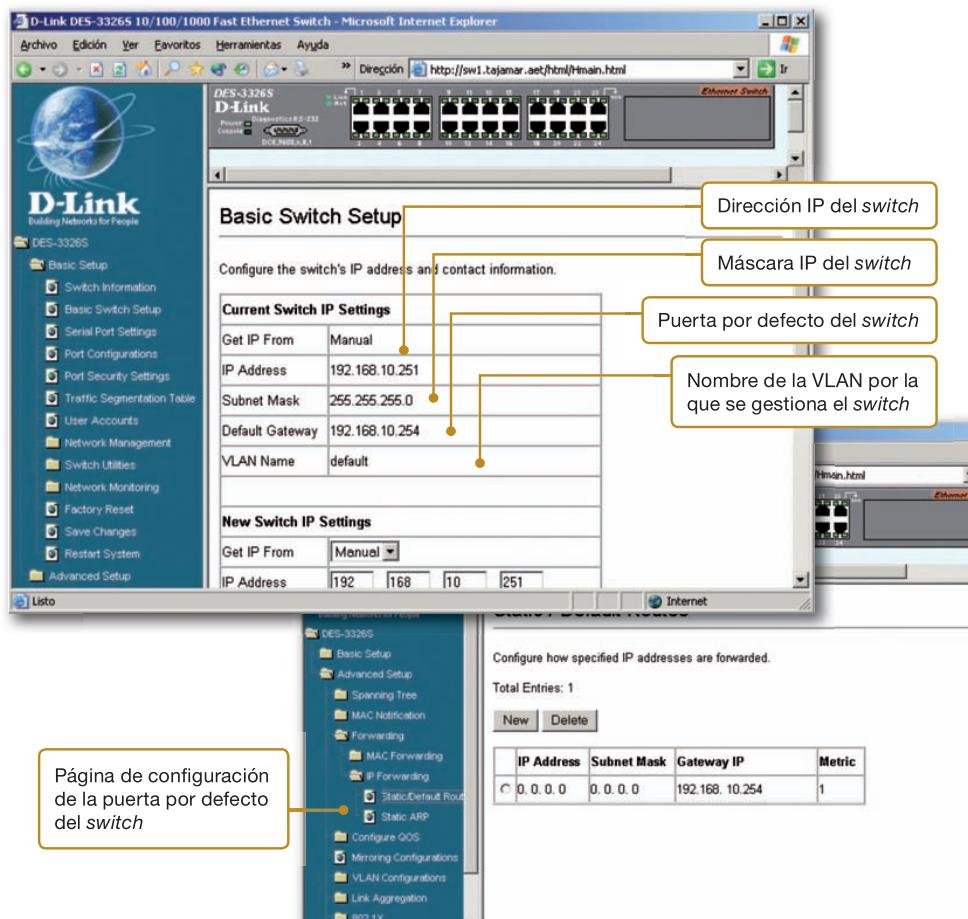


Fig. 5.19. Fichas de configuración web de los parámetros básicos de un comutador gestionable.

Finalmente, hay que centrar la atención en el nivel físico de conexión de los puertos del *switch*. La conexión de las estaciones a los puertos de comutador se hace mediante un cable directo. En cambio, los cables que conectan varios *switches* entre sí requieren cables cruzados. La mayor parte de los *switches* actuales tienen algún puerto especial que hace internamente el cruce de pares de modo que se pueda utilizar también un cable directo para interconectarlo con otro *switch* utilizando este puerto. Estos puertos suelen venir etiquetados con el identificador **MDIX** o **MDI-X** (Interfaz cruzada dependiente del medio, *Medium Dependent Interface Crossover*) para diferenciarlos de los puertos MDI que son los que no hacen crossover (puertos normales para conectar mediante cable directo).

En un estadio más avanzado, el puerto puede tener inteligencia suficiente como para admitir tanto una conexión MDI (cable directo) como MDI-X (cable cruzado): en este caso, el identificador del puerto suele ser **MDI/MDI-X**. En cualquier caso, siempre conviene consultar las especificaciones del fabricante para conocer con exactitud las prestaciones de cada puerto.

### Truco

Cuando el profesional tiene que elegir la solución comercial concreta de un dispositivo de red, no solo debe fijarse en las prestaciones de rendimiento o el precio, hay muchos otros detalles que complementan la funcionalidad básica del dispositivo que frecuentemente lideran la decisión final.

### Actividades

6. Di si son verdaderas o falsas las siguientes afirmaciones:
  - a) Los comutadores son más rápidos que los puentes.
  - b) Un comutador es siempre local.
  - c) El comutador, como el puente, no puede gestionar el ancho de banda.
  - d) Todos los comutadores se pueden escalar.
  - e) La mayor parte de los *switches* se pueden configurar a través de su página web.
7. En la instalación de la red de una oficina se ha propuesto una distribución Ethernet comunitada de los puestos de los usuarios. Inicialmente se han alquilado dos plantas, pero es probable que en un futuro no lejano se tenga que alquilar más espacio para asegurar un crecimiento de la empresa. Esto generará nuevas reconfiguraciones de la red para, sin anular la infraestructura de red inicial, poder ampliar el número de puestos de trabajo con acceso a la red. Teniendo en cuenta que la solución no tiene por qué ser única, ¿qué tipo de *switch* central pondrías en la instalación? Razona la respuesta.



### Claves y consejos

En la red de área local se definen varias VLAN entre las que posteriormente se pueden establecer relaciones de más alto nivel, por ejemplo, se podría organizar una VLAN por cada departamento de una corporación de modo que todos los componentes de ese departamento estén lógicamente aislados de otros departamentos. El servidor que utilizan, si es compartido con otros departamentos, deberá pertenecer a varias redes virtuales simultáneamente. También podría habilitarse el encaminamiento entre las distintas VLAN a través de un enrutador en el que se definirán las políticas de comunicación entre los nodos pertenecientes a las distintas VLAN.

## 5. Tecnologías específicas de los commutadores

Las redes de área local son muy dependientes del cableado. El cambio de posición geográfica de un usuario de una red supone modificar la configuración del cableado de red, lo que casi siempre es imposible. La tecnología VLAN (léase «vilan») permite que los nodos de la red se conecten a redes lógicas en vez de a redes físicas.

### 5.1. Redes de área local virtuales o VLAN

Cada VLAN está formada por un grupo lógico de estaciones físicamente unidas a los puertos de uno o más commutadores que son gestionadas en grupo como si estuvieran en la misma red de área local física.

La pertenencia a una VLAN puede estar asignada manualmente (VLAN estáticas) o hacerse dinámicamente (VLAN dinámicas) mediante un registro automático a través del protocolo GVRP (Generic VLAN Registration Protocol). Cada estación solo puede comunicar con otras estaciones de su grupo, aunque no hay inconveniente en que una estación pueda pertenecer a más de un grupo, si el software de gestión lo permite.

Las principales ventajas que proporciona una VLAN son:

- Mejoras en la velocidad de la red por una mejora en la gestión de los puertos de comunicaciones.
- Incremento del ancho de banda o mejora de la asignación del mismo en función de las necesidades.
- Incremento de la seguridad de la red por segregación de usuarios con necesidades especiales o por aislamiento de conexiones que generen excesivo tráfico y que puedan dañar el rendimiento global de la red.
- Generación de grupos de dispositivos con protocolos obsoletos e incompatibles con el tráfico habitual de la red y que se canalizarán a través de una VLAN específica.

Existen varias formas de establecer una VLAN. Cada uno de estos modos proporciona una funcionalidad distinta. Están basados en la tecnología de commutadores o de encaminadores.

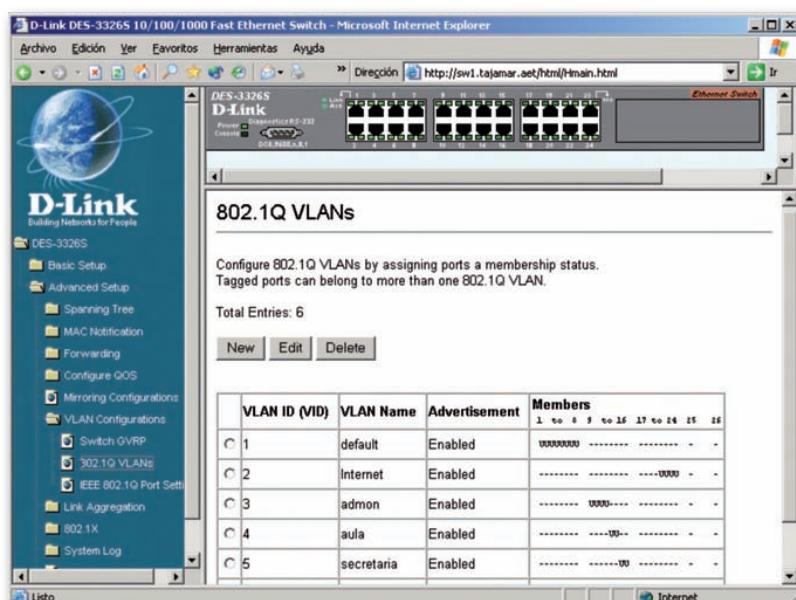


Fig. 5.20. Creación de VLAN 802.1Q en un commutador a través de su página web.

En la Fig. 5.20 podemos observar la página de configuración de VLAN en un commutador compatible con 802.1Q en el que se han dado de alta seis VLAN distintas por el procedimiento de asignaciones de puertos. Por ejemplo, la VLAN denominada «admon» lleva el identificador número 3 y está compuesta por todos los nodos conectados a los puertos 9, 10, 11 y 12 del commutador. La letra «U» en la posición del puerto indica que los nodos destinatarios por ese puerto no entenderán tramas 802.1Q y que, por tanto, será el commutador el encargado de remover la información de tagging a la salida de la trama o de insertarla con el identificador 3 a la entrada de la misma.

Las VLAN permiten que los nodos de la red se agrupen según unos criterios lógicos denominados **policies** o políticas de conexión que los independizan de su ubicación haciendo que dos nodos que pertenecen a segmentos distintos de la red pertenezcan de hecho a la misma VLAN y puedan comunicar entre ellos transparentemente como si estuvieran en el mismo segmento.

Podemos hacer una sencilla clasificación de tipos de VLAN:

- **VLAN con asignaciones de direcciones MAC.** Los conmutadores de la red crean grupos lógicos con direcciones MAC de los nodos a los que tienen acceso. Cuando una estación cambia de ubicación, sigue manteniendo su dirección MAC y por tanto sigue perteneciendo al mismo grupo virtual, aunque haya cambiado su situación geográfica.
- **VLAN con asignaciones de puertos.** Es una VLAN semejante a la anterior, pero con la peculiaridad de que las asociaciones se realizan agrupando puertos del conmutador en vez de direcciones MAC de los nodos. Todos los nodos del segmento de red conectado por cada puerto asociado a una VLAN pertenecen a esa VLAN.
- **VLAN por direccionamiento virtual.** Las redes virtuales se constituyen sobre nodos que comparten un sistema de direccionamiento, configurándose a través de máscaras de red. Se trata, por tanto, de una extensión de las VLAN al nivel 3 de OSI.

El estándar más frecuente de creación de VLAN es el **IEEE 802.1Q o VLAN Tagging**. Gracias a él se pueden definir VLAN a través de la red con independencia del fabricante de los conmutadores. En IEEE 802.1Q cada nodo lleva asociado un número de VLAN a la que pertenecerá con independencia de su ubicación en la red y que se registrará en la cabecera de todas las tramas (*tagging*), que serán modificadas. Como la configuración de la VLAN reside en la configuración de la tarjeta de red, es necesario que las tarjetas de red sean compatibles con IEEE 802.1Q.

El puerto del conmutador al que se conecta un nodo configurado con IEEE 802.1Q se marca como «Tag».

Otro modo alternativo posible es dejar las tarjetas de red sin configurar y, sin embargo, configurar el puerto del *switch* al que se conecta el nodo para que sea él quien inserte la modificación en la trama que lleva la información de VLAN. En este caso se dice que el puerto del *switch* está configurado como «Untag».

En la Fig. 5.21, a la izquierda, se puede ver la ficha de configuración de prioridades de VLAN para una interfaz de fibra de D-Link en donde asociaremos el identificador de la VLAN (VLAN ID), que es un número, a una prioridad. A la derecha, tenemos la configuración de VLAN de un interfaz de red de Intel en donde se han definido varias VLAN, asociando el número identificador a un texto. Por ejemplo, la VLAN AG1 tiene el identificador 212, la VLAN Infantil el 205, etc. Abajo, se está definiendo la pertenencia a la VLAN número 3 del nodo poseedor de la tarjeta de red que se está configurando. La mayor parte de las VLAN pueden asociar prioridades a las tramas de las diferentes VLAN de modo que se organice un sistema de calidad de servicio. El protocolo comúnmente utilizado para llevar a cabo esto es **IEEE 802.1P**.

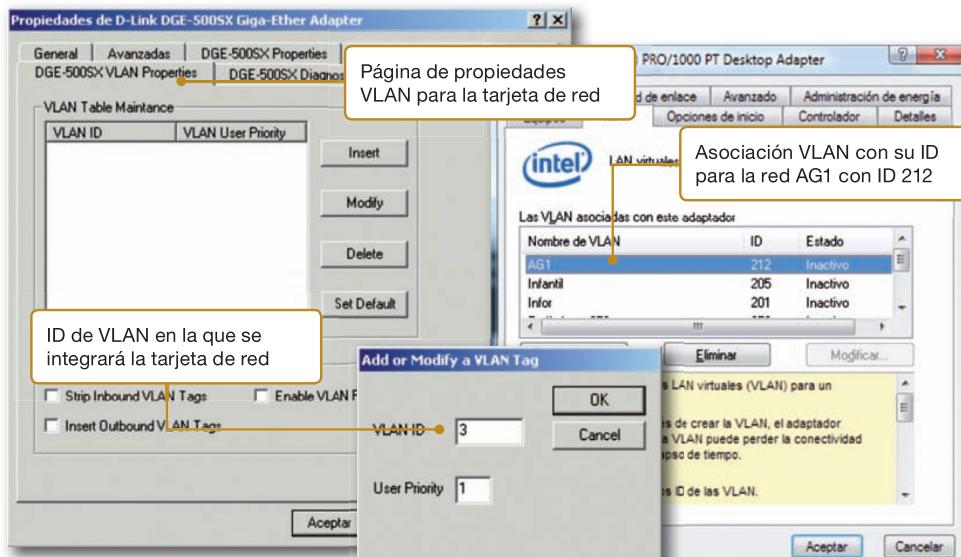


Fig. 5.21. Configuración de la VLAN en una tarjeta de red.

## Actividades

8. En la instalación de red de una oficina bancaria trabajan varias decenas de empleados distribuidos en departamentos. Los oficinistas del departamento financiero tienen acceso a unos datos restringidos a los que no tienen acceso el resto de empleados. Todos deben tener derecho de uso de alguna impresora. El director de la oficina bancaria tiene que poder acceder a todos los datos locales de la sucursal. En el diseño de la red, los datos residen en uno o más servidores. Todos los usuarios se conectan a sus respectivas rosetas y no pueden cambiarse de roseta, ¿puede solucionar el problema de la privacidad una fragmentación de la red de tipo VLAN?, ¿la VLAN que propondrías asociaría las estaciones por puertos o por direcciones MAC? Si instalaras una VLAN por puertos, ¿eres más conveniente una solución Tag o Untag? Razona la respuesta.
9. Sobre la instalación del ejercicio anterior, ¿cómo solucionarías que el director de la oficina bancaria pueda acceder a todos los datos de la red?, ¿cómo tendría que ser configurado el puerto y la tarjeta de red de la impresora para que todos los usuarios pudieran acceder a ella? Por último, debate qué sería mejor: ¿una solución de un único servidor o una solución de varios servidores (uno por cada VLAN)? ¿Podría ser una solución aceptable instalar en el servidor múltiples tarjetas de red, cada una de las cuales estaría configurada en una VLAN?



### Caso práctico 2

#### Construye una VLAN que proteja los segmentos de red

En el ejercicio profesional es muy común tener que hacer un despliegue de la red en donde con los mismos conmutadores se tengan que organizar varias redes locales, cada una de ellas asociada a una VLAN concreta, de modo que solo los dispositivos de red que pertenezcan a la misma VLAN sean alcanzables, pasando el resto inadvertidos.

Un ejemplo podría ser construir una VLAN para el departamento comercial de una empresa de modo que solo el personal de este departamento pueda acceder a la información de su servidor corporativo, que también estaría en la misma VLAN. Además, todo el tráfico generado por los comerciales quedará aislado del tráfico del resto de los departamentos de la empresa.



#### Claves y consejos

Es posible que sea necesario instalar en los switches la configuración de fábrica con objeto de eliminar todas las restricciones procedentes de una anterior instalación.

Para entrenar esta destreza vamos a familiarizarnos con los procedimientos típicos de configuración de VLAN. Para la realización de este ejercicio vamos a necesitar los siguientes materiales:

- Cuatro PC compatibles con IEEE 802.Q en sus tarjetas de red y sistema operativo de red en funcionamiento: dos de ellos simularán estar en la red de los comerciales y los otros dos en el resto de la red corporativa.
- Dos switches que soporten IEEE 801.Q y que simularán distintas ubicaciones en las oficinas de la empresa.

- Latiguillos de red para las conexiones de los PC a los switches.

En primer lugar tendremos que conectar todos los PC a los switches, que deberán estar conectados entre sí, y comprobar que todos los ordenadores pueden comunicarse entre sí. Esto significa que debemos partir de una red local sin restricciones en donde hemos comprobado que la configuración de los sistemas operativos, las direcciones de red y los cables de red funcionan correctamente.

En la Fig. 5.22 puede verse un ejemplo de la topología de conexión que necesitamos.

Una vez que tengas todo el hardware conectado según lo indicado y funcionando, vamos a realizar varias actividades:

1. Configura todas las tarjetas de red de los nodos para que no utilicen IEEE 802.1Q (esto significa que utilizaremos VLAN por puertos). Ahora creamos en el switch A una VLAN por puertos en donde el identificador de VLAN (VLANID) sea «1» y se le asocian los puertos «1» y «2» del switch A en su modalidad *untagged* (red VLAN por puertos), creando la VLAN número «1» con esos dos puertos. Comprueba que los nodos 1 y 2 siguen comunicándose entre sí, pero que no tienen comunicación con el resto de los nodos. Si «1» y «2» son las estaciones de los comerciales, tienen comunicación entre sí, mientras que las demás estaciones no pueden tener acceso a ellos. Esto se mantiene así mientras que los comerciales estén conectados a esos puertos concretos que acabamos de configurar.

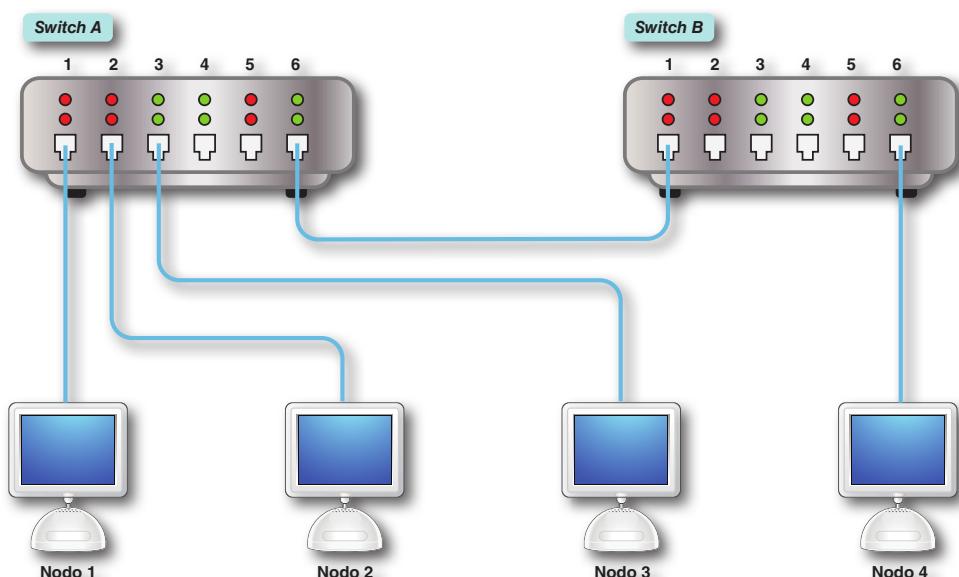


Fig. 5.22. Topología de conexión para pruebas VLAN.

Continúa...



## Caso práctico 2

...Continuación

2. Ahora destruye la configuración anterior y habilita IEEE 801.Q en las tarjetas de red de los tres primeros nodos y en el switch A, es decir, ahora vamos a construir una VLAN no asociada a puertos. Asigna la VLANID 1 a la tarjeta de red del nodo 1, VLANID 2 al nodo 2 y VLANID 3 al nodo 3. Comprueba que, como los tres nodos pertenecen a tres VLAN distintas, no pueden comunicarse entre sí.
3. Seguidamente configura la tarjeta de red del nodo 3 para que tenga la VLANID 1. Ahora el nodo 1 y el nodo 3 pertenecen a la misma VLAN y, por tanto, podrán comunicarse entre sí, pero ninguno de los dos lo podrá hacer con el nodo 2.
- Compruébalo. Este podría ser el caso de la llegada de un nuevo comercial al departamento que tiene la estación «3». El usuario de la estación «2» ha cambiado de departamento y, por tanto, ya no podrá acceder a su antigua VLAN de comerciales.
4. Habilita IEEE 801.Q en el switch B y en el nodo 4 asignándole a su tarjeta de red también el VLANID 1. Ahora los nodos 1, 3 y 4 pertenecen a la VLAN «1» y pueden comunicarse entre sí a pesar de que están

conectados en switches distintos con tal de que el puerto 6 del switch A y el 1 del switch B tengan habilitados también IEEE 802.1Q y estén conectados físicamente con el cable apropiado. Habrá que configurar estos dos puertos para que se transmitan las tramas correspondientes a las VLAN que vayan a comunicarse entre los dos switches, por tanto lo más apropiado es configurar estos dos puertos como Tag y asignarles a los dos todas las VLAN definidas en los switches, es decir, estos puertos de intercomunicación pertenecerán a todas las VLAN. Comprueba que los nodos 1, 3 y 4 pueden comunicarse entre sí y que, sin embargo, ninguno de ellos puede hacerlo con el nodo 2.

Observa cómo, sin cambiar la estructura física de la red, hemos sido capaces de mover a los usuarios en distintos entornos de red.



### Truco

Hay que asegurarse de que ambos switches son compatibles con el protocolo GVRP y que lo tienen habilitado para que las VLAN puedan atravesar las fronteras de cada switch.

## 5.2. Enlaces entre comutadores

En las instalaciones reales es habitual tener que utilizar más de un comutador para dar servicio a todos los usuarios, bien porque el número de usuarios sea muy elevado y supera el número de puertos del switch o bien porque la red se extiende geográficamente por zonas a las que un único comutador no podría llegar.

Los comutadores se enlazan entre sí a través de unos segmentos de red que los unen y que transportan el tráfico entre ellos. Obviamente, como estos segmentos tienen sus dos extremos conectados a sendos comutadores, no admiten estaciones añadidas. Esta es la razón por la que se les llama segmentos des poblados. Técnicamente, a un segmento que une dos comutadores se le denomina **uplink**.

Además, como los comutadores pueden tener configuradas varias VLAN, el uplink tendría que pertenecer a todas ellas, por lo que los puertos de un uplink deben estar configurados como Tag si los comutadores quieren comunicar varias VLAN.

En la Fig. 5.22, el enlace uplink sería el segmento que une el puerto 6 del comutador A con el puerto 1 del comutador B.

Cuando el tráfico de la red entre switches es muy intenso es posible que un único uplink no tenga suficiente capacidad para mover las tramas de un comutador a otro con la suficiente calidad de servicio. El administrador de la red puede agregar varios uplink y configurarlos como si fueran uno solo de mayor capacidad (agregación de enlaces, Fig. 5.23). A este agregado de enlaces se le llama **troncal** o **trunk**.

La agregación de enlaces sigue la normativa **IEEE 802.3ad**. Frecuentemente uplink y troncal se toman como sinónimos obviando si es un agregado de enlaces o solo uno, pero un troncal suele llevar asociado el transporte de VLAN entre comutadores.

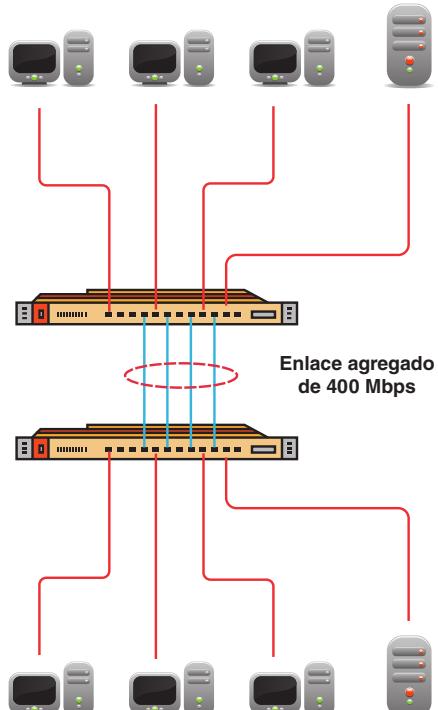


Fig. 5.23. Enlace agregado de conexión entre dos comutadores.



### Ampliación

Cuando un conmutador tiene que averiguar por qué puerto puede alcanzar un destino genera una trama de broadcast contra ese destino que emite por todos sus puertos de modo que a ese nodo de destino le llegue la trama con seguridad (si está activo) y conteste al switch. El conmutador aprenderá por qué puerto le llega la respuesta y utilizará ese puerto para transmitir las tramas con destino en ese nodo.

Las tramas de broadcast se transmiten por todos los puertos y pueden traspasar las fronteras entre switches (no así las de enruteadores, que no generan tramas de broadcast). Si las interconexiones entre switches forman bucles, estos pueden propagar las tramas de broadcast por estos bucles, repitiendo una y otra vez la información que transmiten, consumiendo inútilmente el ancho de banda de la red hasta el punto de que pueden llegar a inutilizarla por un consumo exhaustivo de los recursos disponibles. En este caso, se dice que se ha producido una **tormenta de broadcast**.

## 5.3. Tratamiento de bucles en la red: protocolos de spanning tree

Cuando la topología global de la red se hace compleja es posible que se formen bucles en la red, ya que una trama puede alcanzar su destino por varios caminos. Estas situaciones son muy interesantes porque proveen redundancia de caminos, lo que hace a la red menos sensible frente a averías en el sistema de cableado, pero también son una fuente de problemas puesto que se pueden generar tormentas de broadcast.

Por un lado, hay una necesidad de bucles para que haya redundancia pero, por otro lado, hay que impedir que se produzcan tormentas de broadcast. Para conseguir esto la IEEE ha propuesto un protocolo que impide los bucles en un nivel lógico, evitando las **tormentas de broadcast**, pero que reconfigura la red cuando algún segmento falla para utilizar las ventajas de la redundancia de segmentos físicos. Se trata del protocolo **IEEE 802.1D o STP** (*Spanning Tree Protocol*, Protocolo de árbol de expansión).

### A. Características del protocolo STP

STP es un protocolo de nivel 2 diseñado originalmente para evitar tormentas de broadcast en redes comutadas debido a la creación de bucles entre sus enlaces físicos.

Opera calculando los caminos de red que puedan evitar bucles y para ello bloquea artificialmente los enlaces que formarían un bucle entre cualquier origen y cualquier destino en la red comutada.

STP se adapta dinámicamente a la topología de la red, de modo que si esta cambia, STP recalculará todos los posibles bucles y generará unos nuevos caminos exentos de bucles.

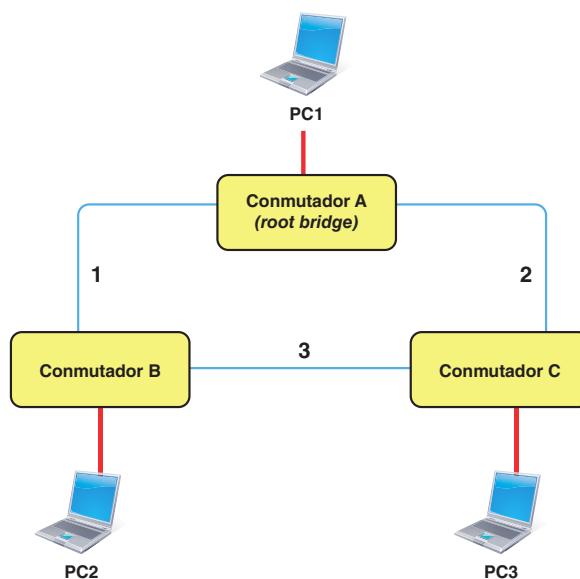
El modo de operación de STP en una red con conmutadores que incorporan esta tecnología y que además la tienen habilitada es el siguiente:

1. Se selecciona un conmutador determinado (*root bridge*, en la terminología de STP) y a partir de él se construye un árbol de caminos a cualquier otro conmutador (*bridge*) de la red.
2. Se bloquean a nivel lógico los caminos que aparecen como redundantes entre cualesquiera origen y destino y se eligen como idóneos los que se calculan como más cortos.
3. Por estos caminos cortos circularán todas las tramas. Los puertos bloqueados no podrán transferir tramas de datos entre las estaciones, solo pueden transmitir las tramas de control del propio protocolo STP.
4. Si uno de los caminos más cortos falla (por ejemplo, se ha deteriorado el cable de red que lo soporta), se recalculará el árbol de caminos para hallar un nuevo camino que obvie el fallo. Este proceso consume un tiempo durante el que la red no estará operativa (tiempo de convergencia de STP). Este tiempo dependerá de la complejidad de la red, pero puede superar el minuto, lo que a veces puede ser inaceptable.

Para mejorar el tiempo de convergencia se han creado protocolos más modernos, derivados del STP que reducen significativamente el tiempo de convergencia a unos pocos segundos. Un ejemplo de estos nuevos protocolos es **RSTP** (*Rapid Spanning Tree Protocol*), que está recogido en la norma **IEEE 802.1w**.

### B. Operación con el protocolo STP

En la Fig. 5.24 se puede ver la representación gráfica de una red comutada con tres switches con caminos redundantes que será útil para estudiar el modo de operación básica de STP. Efectivamente, para que una trama con origen en PC1 llegue a PC3, caben dos caminos: el camino más sencillo consiste en enviar la trama por el camino 2 hacia el conmutador C y él se encargará de conducirla hacia su destino en PC3. El segundo camino tiene un mayor coste y consiste en transmitir la trama por el camino 1 hacia el conmutador B y que este redirija la trama por el camino 3 hacia el conmutador C que es quien tiene la conexión física con el destino PC3.



**Fig. 5.24.** Ejemplo de redundancia de caminos en una red comutada para el estudio del protocolo STP.

La red reúne todos los elementos para que se genere una tormenta de broadcast puesto que tiene bucles. Por ello, es necesario habilitar en los tres conmutadores el protocolo STP o RSTP. Una vez habilitados los conmutadores negociarán quién debe tomar la función de *root bridge*. Supongamos que esta función sea asumida por el conmutador A, como aparece en la figura.

Una vez que haya convergido el proceso de confección del árbol de caminos de STP, el protocolo habrá decidido anular el camino 3. Esto no quiere decir que haya que quitar el latiguillo de conexión de este segmento, sencillamente, STP anulará ese camino impidiendo que por él pasen tramas de datos.

De este modo, PC1 podrá comunicar con PC2 a través del camino 1, PC1 podrá comunicarse con PC3 mediante el camino 2, mientras que PC2 se comunicará con PC3 utilizando los caminos 1 y 2 a través del conmutador A.

Si en un momento dado el camino 1 deja de estar disponible, entonces quedarán incomunicadas todas las estaciones que tienen que utilizar este camino 1 en sus comunicaciones. STP se da cuenta del fallo de red y genera un nuevo árbol anulando el camino 1.

En este caso, STP elegirá los caminos 2 y 3 para asegurar sus comunicaciones y así, PC1 podrá comunicarse con PC3 a través del camino 2, PC2 se comunicará con PC3 por el camino 3 y PC1 lo hará con PC2 a través de los caminos 2 y 3.

Por tanto, STP ha sido capaz de utilizar la redundancia física de la topología de la red, impidiendo que se formen bucles lógicos que causen tormentas de broadcast.



### Actividades

- Sobre el ejemplo de red comutada representada en la Fig. 5.24, ¿cuáles serían los caminos que elegirían los conmutadores para transmitir tramas entre las tres estaciones suponiendo que fallara el *uplink* del camino 2? ¿Y si fallan los caminos 2 y 3?



### Investigación

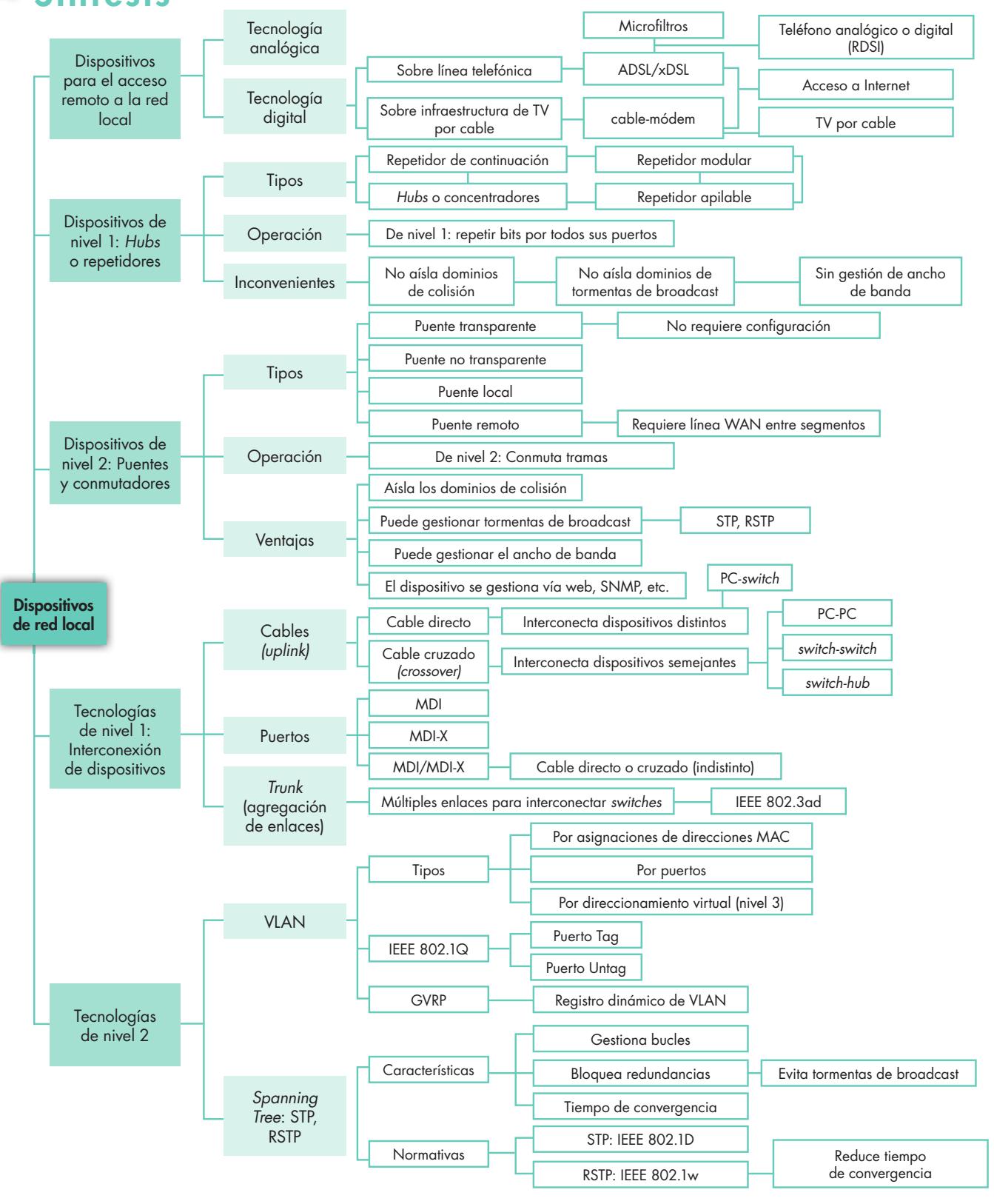
Los conmutadores son en la actualidad los dispositivos más utilizados para realizar el despliegue de la red: repetidores y concentradores solo se utilizan en casos muy específicos y siempre minoritarios. Los switches incorporan muchas otras funciones además de la conmutación de tramas que es en la que se especializan.

Puedes investigar algunos ejemplos de estas tecnologías en Wikipedia por la voz «switch» y, más en concreto, en la tecnología «spanning tree» que se encarga de resolver conflictos de tramas que pueden entrar en un bucle cuando la topología de red es mucho más complicada que una simple estrella y forma bucles

entre sus segmentos. El protocolo original fue STP (*Spanning Tree Protocol*), que producía paradas en el servicio de red durante decenas de segundos cuando se alteraba la topología de la red, aunque actualmente se utiliza mucho más RSTP (*Rapid Spanning Tree Protocol*), que gestiona mucho más rápidamente los cambios topológicos de los segmentos de red.

En las páginas [http://es.wikipedia.org/wiki/Spanning\\_tree](http://es.wikipedia.org/wiki/Spanning_tree) y [http://es.wikipedia.org/wiki/Rapid\\_Spanning\\_Tree\\_Proto](http://es.wikipedia.org/wiki/Rapid_Spanning_Tree_Proto) dispones de una buena información para comenzar el estudio de STP y RSTP respectivamente.

## Síntesis





## Test de repaso

**1.** Enlaza los siguientes elementos característicos de algunas de las tecnologías de bajo nivel, básicas en el acceso remoto a la red:

a) ADSL	1) Cableado telefónico
b) Cable-módem	2) La velocidad de bajada es distinta de la de subida
	3) Televisión por cable
	4) Instalación de microfiltros

**2.** El *hub* o repetidor...

- a) Opera en el nivel 2 de OSI.
- b) Opera en el nivel 3 de OSI.
- c) Opera en el nivel 1 de OSI.
- d) Opera en los niveles 1 o 2, dependiendo de su configuración.

**3.** Asocia las siguientes tecnologías específicas de los conmutadores a sus normativas específicas:

a) VLAN	1) IEEE 802.1D
b) STP	2) IEEE 802.1w
c) RSTP	3) IEEE 802.1Q
d) Trunking	4) IEEE 802.3ad

**4.** Los conmutadores...

- a) Son multipuerto.
- b) Intercambian paquetes entre sus puertos.
- c) Intercambian tramas entre sus puertos.
- d) Fraccionan los dominios de colisión.

**5.** Asocia las características de *hubs* y conmutadores:

a) Hub	1) Puente
b) Switch	2) Repetidor
	3) Nivel 2
	4) Nivel 1
	5) Conmutador
	6) Conmuta tramas
	7) Interpreta las cabeceras de las tramas
	8) No discrimina las tramas

**6.** ¿Qué función de las siguientes no es específica de los conmutadores de nivel 2?

- a) Conmutar tramas entre sus puertos.
- b) Convertir tramas Ethernet en tramas Token ring.
- c) Crear redes locales virtuales.
- d) Encaminar paquetes.

**7.** Un *root bridge* es:

- a) El nodo raíz de una VLAN.
- b) El nodo raíz de un árbol STP.
- c) La estación conectada a un conmutador que tiene habilitado STP.
- d) Un conmutador redundante.

**8.** Enlaza los elementos de las columnas en la tabla siguiente sobre el estado de los puertos de un conmutador que utiliza la tecnología IEEE 802.1Q:

a) Puerto Tag	1) Admite tramas Ethernet no modificadas con la información de VLAN
b) Puerto Untag	2) Admite tramas Ethernet modificadas con la información de VLAN
	3) El conmutador gestiona la modificación de la trama con la información de VLAN
	4) El conmutador conmuta la trama sin modificarla

**9.** Una tormenta de broadcast:

- a) Puede agotar los recursos de la red.
- b) Se genera por la transmisión redundante de paquetes de nivel 3 en la red.
- c) Se genera por la transmisión redundante de tramas de nivel 2 por todos los puertos de la red.
- d) Se puede gestionar mediante el protocolo RSTP.

**10.** Dos conmutadores tienen definidas las dos mismas VLAN en cada uno de ellos. Se desea transmitir tramas de uno a otro a través de enlaces entre ellos. Determina cuál de las siguientes afirmaciones es verdadera.

- a) Basta un enlace (*uplink*) entre dos puertos de sendos conmutadores (uno por cada conmutador) sin ninguna configuración posterior.
- b) Basta un enlace (*uplink*) entre dos puertos de sendos conmutadores (uno por cada conmutador), pero hay que configurar que estos dos puertos pertenezcan a las dos VLAN en cada uno de los dos conmutadores.
- c) Hay que crear un *trunking* con dos puertos en cada conmutador.
- d) El enlace de conexión entre los conmutadores debe ser Tag en un extremo y Untag en el otro.

Solución: 1: a-(1, 2 y 4), b-3, 2: c, 3: a-3, b-1, c-2, d-4, 4: a, b y d; 5: a-(2, 4 y 8), b-(1, 3, 5, 6 y 7); 6: b y d; 7: b, 8: a-(2 y 4), b-(1 y 3); 9: b y d; 10: b.

## Comprueba tu aprendizaje

### I. Distinguir las funciones de los dispositivos de interconexión de red

1. Confirma la veracidad o falsedad de las siguientes afirmaciones:
  - a) Externamente, un *hub* y un *switch* se distinguen con dificultad.
  - b) Un puente remoto consta de dos dispositivos separados por una línea de conexión.
  - c) Los comutadores operan en el nivel 3 y los puentes en el nivel 2.
  - d) Los repetidores se pueden instalar en cascada indefinidamente.
  - e) Los comutadores saben gestionar el ancho de banda de cada puerto.
  - f) Los repetidores y concentradores copian las tramas entre sus puertos.
2. Relaciona la columna de la izquierda (dispositivos) con su tecnología específica (columna de la derecha). Ten en cuenta que la relación es de uno a varios.

Dispositivos	Tecnología o función específica
1. Repetidor	a. Comutar paquetes
2. Transceiver	b. Regenerar la señal eléctrica
3. Concentrador	c. Doble puerto
4. Puente	d. Múltiple puerto
5. Switch	e. Selecciona tramas

3. ¿Es posible crear VLAN utilizando comutadores? ¿Y si utilizamos concentradores? ¿Y si usamos puentes remotos?

### II. Elegir los dispositivos de red de área local en función de las necesidades

4. Busca los errores técnicos en el siguiente comentario:  
 «Una empresa acaba de fusionarse con otra y sus directivos proyectan integrar sus dos redes antiguas en una nueva. Cada red está en la sede de su ciudad original. Se ha propuesto la adquisición de un puente remoto para unir las dos sedes, pero una vez comprobado su escaso rendimiento se ha determinado conectarlas mediante un comutador que es mucho más rápido.»
5. Confirma la veracidad o falsedad de las declaraciones siguientes sobre ADSL:
  - a) La tecnología xDSL siempre es simétrica.
  - b) En ADSL el ancho de banda de bajada suele ser superior al de subida porque es una tecnología asimétrica.

c) Un módem ADSL siempre requiere otro dispositivo intermedio para conectarse a la red local.

d) Al igual que el módem, el router ADSL también requiere un dispositivo intermedio para unirse a la red.

6. Busca en las sedes web de los fabricantes de dispositivos de red información técnica y comercial sobre comutadores.

Compara los distintos modelos de varios fabricantes para familiarizarte con las características básicas de este tipo de dispositivos.

Si consigues listas de precios, podrías realizar comparativas de precios.

Ayuda: Las comparativas de precios no se hacen por comutador, sino por puertos, es decir, se divide el precio total del comutador por el número de puertos que posee.

### III. Configurar redes locales virtuales

7. ¿Qué tipos de redes de área local virtuales conoces? ¿Cómo se llama el estándar IEEE utilizado en la creación de VLAN?
8. Razona en qué condiciones podrían ser verdad las siguientes afirmaciones:
  - a) Dos puertos que se asocian en la misma VLAN en un comutador pueden comunicarse libremente.
  - b) Dos puertos que pertenecen a dos VLAN distintas solo pueden comunicar los protocolos de gestión.
  - c) Las direcciones MAC de los dos nodos se han asociado a la misma VLAN, pero como están conectados en dos comutadores distintos, nunca podrían comunicarse entre sí.
  - d) Dos nodos que pertenecen a la misma VLAN pero que están conectados a distintos comutadores pueden comunicarse entre sí.
9. Toma tres comutadores que contemplen el protocolo STP o RSTP y prepara en el laboratorio un modelo para la red comutada que aparece en la Fig. 5.24.
  - a) Habilita el protocolo STP en los tres comutadores y comprueba que las tres estaciones pueden comunicarse entre sí.
  - b) Rompe ahora el enlace del camino 1 y comprueba que después de un tiempo sigues teniendo conexión entre las estaciones.
  - c) Repite el proceso anterior deshabilitando los caminos 2 y 3.