

# 3

## Unidad

### Instalación y configuración de los equipos de red



#### Y estudiaremos:

- Los sistemas operativos disponibles para la red.
- Los componentes de las pilas de protocolos estandarizados.
- Las órdenes de ejecución asociadas a las utilidades de la red.

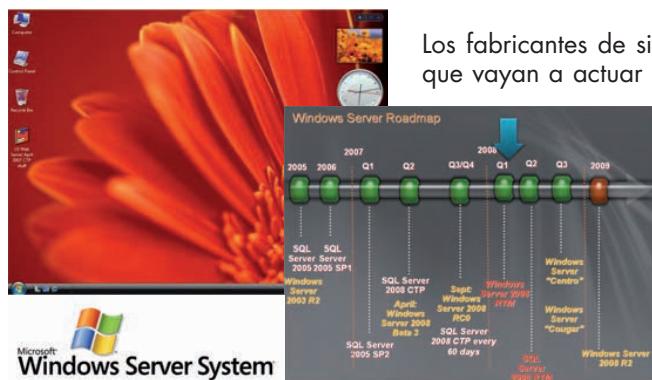
#### En esta unidad aprenderemos a:

- Identificar los protocolos y servicios de red proporcionados por los sistemas operativos.
- Utilizar las herramientas básicas para la gestión de protocolos de red.
- Configurar el sistema de direccionamiento de los equipos de la red.



### Ampliación

Microsoft tiene sistemas operativos cliente y servidor. Cada uno de ellos se comercializa con distintas versiones: domésticas, profesionales, empresariales, etc. Las más actuales son Windows 7 en su versión cliente y Windows Server 2008 R2 para la versión servidor, aunque ya están anunciadas las versiones Windows 8, tanto para cliente como para servidor.



**Fig. 3.1.** Logotipo de una gama de productos de servidor de Microsoft y ejemplo de escritorio de Windows Server 2008 R2 (izquierda). A la derecha, calendario de lanzamientos (roadmap) utilizado para la presentación de productos de Microsoft.



### Vocabulario

**GPL o Licencia Pública General GNU:** es una licencia creada por la Free Software Foundation orientada a proteger la libre distribución, modificación y uso de software.



**Fig. 3.2.** Ejemplo de escritorio gráfico GNOME de la distribución Ubuntu de Linux.

## 1. El sistema operativo de red

Gran parte de la funcionalidad de la red depende del software que se ejecuta en cada uno de sus nodos. Este software se sustenta sobre el sistema operativo y, a su vez, este lo hace en el hardware. De este modo, la red se integra totalmente en el sistema y se hace difícil distinguir lo que es propio de la red de lo que es más específico del sistema operativo. Para ello, los sistemas de red se apoyan en los protocolos, que también serán desarrollados en esta unidad.

El sistema operativo de cualquier sistema conectado a la red es muy importante porque debe interactuar con otros sistemas de la misma o de otra red. Por ejemplo, debe soportar aplicaciones que «hablan» en red, tiene que brindar servicios a otros equipos o servirse de los que otros le proporcionan y, además, tiene que ser interoperable.

### 1.1. Sistemas operativos comerciales

Los fabricantes de sistemas operativos comercializan versiones distintas en función de que vayan a actuar como servidores o como clientes. La máxima interoperabilidad se produce entre sistemas del mismo fabricante, pero la interoperabilidad ha crecido sobre todo porque actualmente todos los sistemas operativos hablan TCP/IP.

#### A. Microsoft Windows

Windows es el nombre genérico de los sistemas operativos de Microsoft. Aunque tradicionalmente NetBeui ha sido el protocolo de red nativo de los sistemas de Microsoft accesible a través de NetBIOS, actualmente el protocolo nativo adoptado por Microsoft es TCP/IP. Sobre él se ha seguido conservando la interfaz NetBIOS por compatibilidad con las aplicaciones de red anteriores.

Microsoft tiene varias gamas de sistemas operativos que van desde los sistemas para dispositivos de mano como teléfonos móviles y PDA hasta sistemas para grandes equipos con muchos procesadores y capaces de gestionar grandes cantidades de memoria central.

#### B. UNIX y distribuciones GNU/Linux

UNIX es el sistema operativo en tiempo real por autonomía y máximamente flexible. Hay muchas marcas de UNIX, lo que conduce a una cierta complicación. Podemos encontrar versiones de UNIX de 32 y de 64 bits; de hecho, UNIX se adelantó a Windows en el soporte de sistemas de 64 bits.

**GNU/Linux** es un sistema operativo que sigue la tecnología de UNIX pero que se distribuye gratuitamente **bajo licencia GPL** (*GNU Public License*). Algunas compañías se dedican a comercializar distribuciones de GNU/Linux, es decir, se dedican a reunir los componentes del sistema junto con muchas aplicaciones y cobran por esta distribución, por el servicio que prestan y por las aplicaciones que no son del sistema y que ellas mismas programan o adquieren a terceros.

Aunque formalmente debe decirse GNU/Linux, habitualmente se le suele llamar simplemente Linux (nombre del kernel o del sistema operativo).

Cada distribución de Linux también tiene sus versiones cliente y sus versiones servidor. Aunque el núcleo de sistema es el mismo para ambas versiones, el número de componentes que lo acompañan varía dependiendo de si se trata de la versión de cliente o la versión de servidor.

Es muy habitual que en las distribuciones de servidor no se incorpore el sistema gráfico del sistema para que este no consuma recursos innecesarios. En cambio, en las versiones cliente la interfaz gráfica es muy importante para hacer más grato el trabajo de los usuarios finales.

La tecnología de red nativa de UNIX y de Linux es TCP/IP; sin embargo, para mejorar la interoperabilidad de estos sistemas, se les incorpora software con las pilas de otros protocolos como los de Microsoft o los de Novell NetWare.

Actualmente hay muchas distribuciones de Linux: **Ubuntu**, **Red Hat**, **SUSE**, **Mandrake**, **Debian**, **Fedora**, etc. Lo más básico y a la vez operativo de estas distribuciones se puede descargar gratuitamente de Internet. En la página [http://es.wikipedia.org/wiki/Anexo:Distribuciones\\_Linux](http://es.wikipedia.org/wiki/Anexo:Distribuciones_Linux) hay una clasificación de muchas de las distribuciones que se pueden encontrar, así como la dependencia de unas con otras.

### Ampliación

UNIX no es lo mismo que Linux, UNIX fue primero. Linux se desarrolló partiendo de cero aunque con la filosofía tecnológica de UNIX. Sobre Linux podemos encontrar muchas aplicaciones GPL. También podemos observar diferencias entre algunas versiones de UNIX y Linux en la página: <http://www.unixguide.net/unixguide.shtml>

## C. Apple Mac OS X

**Mac OS X** es el nombre comercial del sistema operativo de **Apple**. Mac OS X no es más que un sistema UNIX al que se le ha revestido de una interfaz gráfica muy potente y llamativa junto con muchas otras aplicaciones construidas por Apple, que le convierte en un sistema operativo fiable, robusto y eminentemente gráfico. De nuevo, el protocolo de red nativo de Mac OS X es TCP/IP como en cualquier otro sistema UNIX, si bien Apple también ha incorporado por compatibilidad con las versiones anteriores de sus sistemas operativos la pila de protocolos **AppleTalk**. En el caso de Mac OS X, también existe una versión cliente y una versión servidor.



Fig. 3.3. Escritorio típico de Apple Mac OS X.

## D. Novell NetWare

**NetWare** es el nombre del sistema operativo tradicional de **Novell**, aunque esta compañía ha entrado también desde hace unos años en el negocio de UNIX. El avance de Windows y UNIX ha hecho que los servidores NetWare tradicionales sean residuales.

La pila de protocolos nativa de Novell NetWare es SPX/IPX, pero NetWare es muy flexible y admite casi cualquier otra pila de protocolos, lo que le convierte en un sistema operativo de red verdaderamente interoperable.

### Investigación

Es conveniente que los administradores de sistemas estén al corriente de las actualizaciones y nuevas versiones de cada sistema operativo que tengan instalados los equipos de la red. Conéctate a las webs corporativas de las organizaciones que fabrican o distribuyen estos sistemas para que conozcas su estructura de contenidos, especialmente las páginas de novedades y las de descargas de actualizaciones o parches de software.

También puedes encontrar información sobre estos sistemas en Wikipedia buscando: sistema operativo de red, Microsoft Windows, Mac OS X, Linux, Novell NetWare.

### Ampliación

Las redes NetWare determinan muy bien la parte de cliente y la parte de servidor, es decir, no forman redes punto a punto, sino que son auténticas redes cliente-servidor.

El servidor Novell es auténticamente propietario de Novell; sin embargo la parte cliente es una aplicación que puede residir en otros sistemas operativos anfitriones como DOS, cualquier versión de Windows, Apple y UNIX.

### Laboratorio

#### Identificación de los sistemas operativos de cada nodo en la red

Profesionalmente hay que conservar siempre una documentación sencilla pero completa del software que opera en la red. Para desarrollar esta destreza, identifica los sistemas operativos de cada uno de los ordenadores conectados a la red, sean clientes o servidores. Junto con la marca del sistema operativo tendrás que adjuntar la versión del sistema, el idioma, los parches que tenga instalados y cualquier otra información que especifique características comerciales del sistema. Por ejemplo, una estación cliente podría correr un sistema Microsoft Windows 7 en español con Service Pack 1 o una versión Linux con distribución Ubuntu versión 11.04.

Escribe organizadamente toda esta información relativa a los sistemas para crear un inventario de software de sistemas.

A

## Vocabulario

**System crash:** es un fallo irreparable del sistema operativo provocado por un problema importante en el hardware o por un mal funcionamiento del software del sistema. En Windows se puede detectar un *system crash* cuando aparece inesperadamente una pantalla azul llena de mensajes indescifrables que proporcionan alguna información sobre la causa del error a los ingenieros de sistemas. En el argot profesional a esta pantalla se la denomina BSOD (*Blue Screen Of Death*, Pantalla azul de la muerte) en Windows o Kernel panic en Linux (Fig. 3.4). En general, para cualquier sistema operativo se habla de que el sistema se ha «colgado» o se ha «quedado piedra». Un *system crash* solo se puede recuperar arrancando de nuevo el ordenador desde su secuencia inicial.



## Claves y consejos

Conviene visitar frecuentemente la sede web de los fabricantes de dispositivos por si hubieran publicado alguna actualización de los controladores utilizados por el hardware de nuestros equipos.

Actualizar un controlador es una operación que entraña algún riesgo. Para disminuir este riesgo, es importante hacer siempre una copia de seguridad del sistema, aunque muchos sistemas operativos permiten volver a la configuración anterior si algún controlador recién instalado provoca problemas de inestabilidad.

## ● 1.2. Componentes del sistema

El sistema operativo es como el director de orquesta que organiza todos los recursos disponibles tanto de hardware como de software en un sistema informático. Partiendo de esta metáfora, se nos hace evidente la complejidad que globalmente tiene cualquier sistema operativo y, en particular, la mayor parte de sus componentes.

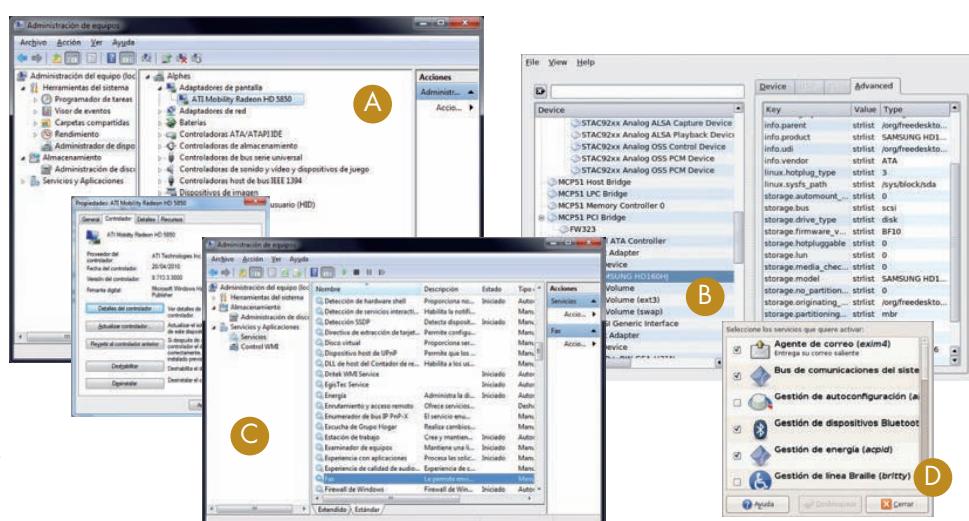
#### **O A. Controlador del adaptador de red**

Es el software que hace que el sistema operativo pueda comunicarse con el hardware de la tarjeta de red. Aunque el sistema operativo suele disponer de muchos controladores, lo habitual es que el fabricante del adaptador lo suministre en un CD o se pueda descargar de Internet.

Es muy importante que el controlador de un dispositivo sea el apropiado. Los fallos de software de un controlador suelen causar situaciones de **system crash**, que ocasionalmente son irrecuperables, especialmente si el controlador problemático es indispensable para el arranque del sistema.

**Fig. 3.4.** Pantallas de kernel panic (abajo, izquierda) y BSOD (arriba, derecha) que son la manifestación de que el sistema ha producido un system crash.

Para evitar este tipo de problemas, algunos sistemas operativos permiten el arranque de los mismos con una configuración mínima. En el caso de Windows, por ejemplo, podemos arrancar el sistema en el modo de prueba de fallos, accesible desde la tecla F8 en el tiempo de arranque del ordenador.



**Fig. 3.5.** A) Administrador de dispositivos en Windows 7 y ficha de propiedades del dispositivo desde el que se puede actualizar el controlador o ser revocado una vez instalado. B) visor de dispositivos en Linux. C) Ventana de administración de equipo en Windows 7 abierto por la ficha de servicios. D) Administrador de arranque y parada de servicios en Ubuntu

## O B. Servicios de red

Un servicio en un sistema operativo es una tarea que se está ejecutando en ese sistema sin necesidad de un terminal (decimos que corre en *background* o, en el mundo Linux, «que es un demonio») y que proporciona una utilidad determinada. Los clientes de ese servicio realizarán sus peticiones al servicio a través de los procedimientos de comunicación soportados por el sistema operativo.

Un servicio de red es aquel que admite que las peticiones vengan a través de la red de área local. Ejemplos de servicios de red en sistemas operativos podrían ser los componentes de software que hacen que un sistema sirva ficheros o sirva impresoras, que hace que unos clientes se sirvan del acceso Internet que tiene otro nodo de la red (servicio proxy) o el elemento encargado de traducir los nombres Internet a direcciones IP equivalentes (servicio DNS).



### Ampliación

En el caso de TCP/IP, a los servicios de red se accede a través de los sockets (elementos de software de comunicaciones) que asocian un número de puerto de comunicaciones y un protocolo a un servicio de red, de modo que toda comunicación de la red con el servicio se lleva a cabo a través del socket.

## O C. Pilas de protocolos

Con este nombre denominamos a las familias de protocolos que instalaremos en el sistema operativo. Algunas pilas de protocolos comunes son TCP/IP, SPX/IPX, NetBeui y AppleTalk.

Las pilas de protocolos se instalan con el software del sistema operativo y proporcionan su funcionalidad a través del núcleo del sistema operativo, especialmente si es la pila nativa del sistema, o a través de los servicios de red.

En otras ocasiones, las necesidades de interoperabilidad con otros sistemas exigirán que añadamos otras pilas de protocolos o servicios de red que se escapan del sistema operativo estándar. Por ejemplo, si un usuario propietario de una Palm desea sincronizarla con su correo electrónico residente en su PC de escritorio, necesitará software de comunicaciones entre la Palm y el PC que permita que se comuniquen entre sí añadiendo la funcionalidad de sincronización de datos de correo: esto se puede llevar a cabo haciendo que los dos dispositivos hablen TCP/IP o instalando en alguno de los dos dispositivos la pila de protocolos nativa del otro.

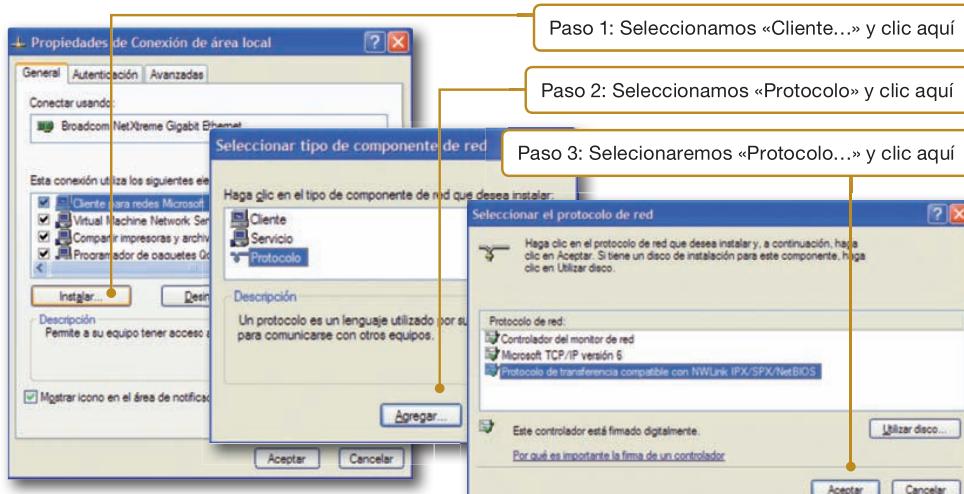


Fig. 3.6. Fichas en Windows XP para añadir la pila SPX/IPX a un sistema que ya tiene la pila TCP/IP.



### CEO

*S M R \_ R L \_ A A b a d \_ 0 3 \_ MantenimientoSistema.docx*

Documento que contiene información sobre:

1. Actualizaciones del sistema.
2. Caso práctico: utilización de *MSINFO* para identificar hardware y software.



### Truco

Ocasionalmente tendremos que instalar algunas pilas de protocolos nuevas que no incorpore el sistema operativo. Por ejemplo, esto es una situación común en algunas impresoras de red que requieren protocolos de comunicación especiales. En estos casos, el fabricante de la impresora nos debería proporcionar tanto el software como los procedimientos de instalación en cada sistema operativo de red.



### Actividades

1. En la tabla siguiente, relaciona el nombre de los sistemas operativos (a la izquierda) con el de las compañías fabricantes o el modelo de licencia (a la derecha).

1. Windows 7	A. GPL, GNU Public License
2. Linux	B. Microsoft
3. Windows Server 2008 R2	C. Apple
4. Mac OS X	D. Novell
5. Windows XP	
6. NetWare	

2. ¿Pueden convivir varias pilas de protocolos sobre la misma tarjeta de red? Razona la respuesta.

3. Cita las razones que conozcas por las que es conveniente actualizar frecuentemente el software de los sistemas operativos.

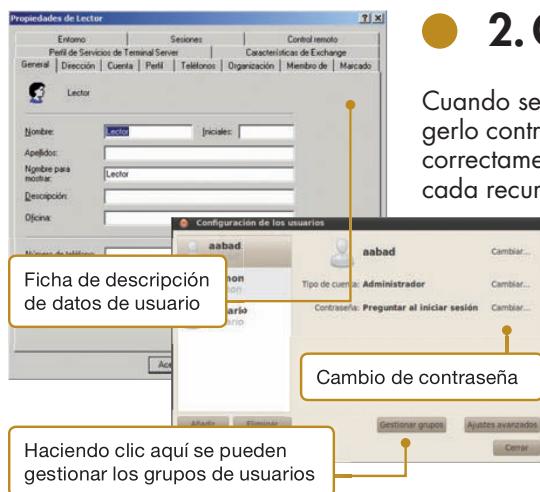


Fig. 3.7. Ficha de creación de un nuevo usuario en un Directorio Activo de Windows, a la izquierda. Gestor de usuarios y grupos en Linux, a la derecha.

## 2. Gestión de usuarios, derechos y accesos

Cuando se comparte un recurso en la red, la norma más básica de seguridad es protegerlo contra accesos indebidos. Para ello, los usuarios de la red deben ser identificados correctamente. Después, a cada usuario se le asignarán sus permisos de acceso sobre cada recurso.

### 2.1. Cuentas de usuario y de grupo

Las cuentas de usuario son el modo habitual de personalizar el acceso a la red. Toda persona que utilice la red con regularidad debe tener una cuenta de acceso. Para que el control de este acceso sea bueno, las cuentas deben ser personales (dos usuarios no deben compartir la misma cuenta).

Una cuenta de grupo es una colección de cuentas de usuario. Al conceder a un usuario la pertenencia a un grupo, se le asignan automáticamente todas las propiedades, derechos, características, permisos y privilegios de ese grupo. Las cuentas de grupo proporcionan una forma sencilla de configurar los servicios de red para un conjunto de usuarios de características similares.

### 2.2. Derechos de acceso y permisos

Una vez que se ha identificado a cada usuario con acceso a la red, se pueden establecer sus derechos de acceso. Corresponde al administrador determinar el uso de cada recurso de la red o las operaciones que cada usuario puede realizar. Ejemplo de estas posibilidades son el derecho de acceso a un servidor o a otro equipo a través de la red, forzar el apagado o reinicio de otro equipo remotamente, cambiar la hora del sistema, etc.

Cada recurso, servicio o utilidad tiene una información asociada que indica quién tiene y quién carece de privilegios sobre ellos.

La asignación de permisos en una red se hace en dos fases:

1. Se determina el permiso de acceso sobre el servicio de red, por ejemplo, se puede asignar el permiso de poderse conectar a un disco de un ordenador remoto. Esto evita que se puedan abrir unidades remotas de red sobre las que después no se tengan privilegios de acceso a los ficheros que contiene, lo que podría sobrecargar al servidor.
2. Deben configurarse los permisos de los ficheros y directorios (o carpetas) que contiene ese servicio de red.

Dependiendo del sistema operativo de red, las marcas asociadas al objeto de red varián, aunque en general podemos encontrar las de lectura, escritura, ejecución, borrado y privilegio de cambio de permisos.

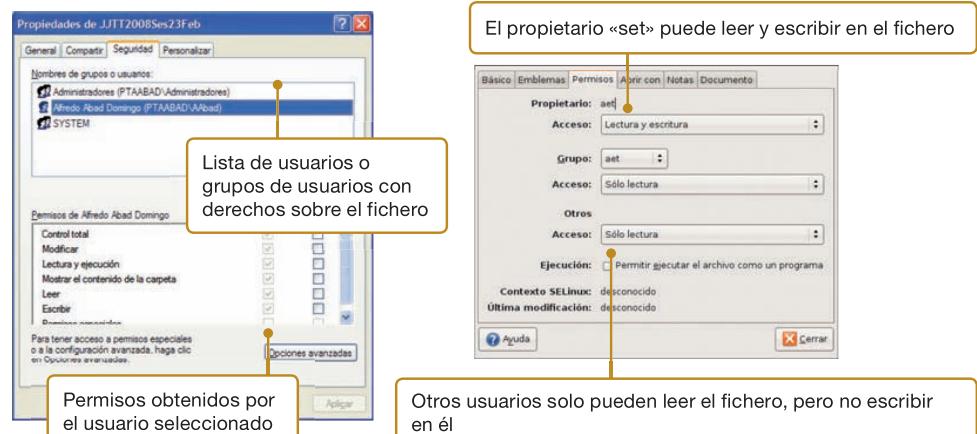


Fig. 3.8. Configuración de privilegios sobre ficheros y carpetas en Windows y en Linux.



#### Ampliación

Los derechos se refieren a operaciones propias del sistema operativo, por ejemplo, el derecho a hacer copias de seguridad. Sin embargo, un permiso se refiere al acceso a los distintos objetos de red, por ejemplo, derecho a leer un fichero concreto. Los derechos prevalecen sobre los permisos, por ejemplo, un operador de consola tiene derecho para hacer una copia de seguridad sobre todo un disco; sin embargo, puede tener restringido el acceso a determinados directorios de usuarios porque se lo niega un permiso sobre esos directorios: podrá hacer la copia de seguridad, puesto que el derecho de backup prevalece a la restricción de los permisos sobre los ficheros y carpetas concretos.



#### CEO

*S M R \_ R L \_ A A b a d \_ 0 3 \_ AdministracionCentralizada.docx*

Documento que contiene información sobre:

1. Administración centralizada de la red.
2. Active Directory de Microsoft.

### 2.3. Notificación de errores

Una vez realizada la instalación y configuración del sistema operativo de red, debemos conducirlo al régimen de explotación, es decir, tenemos que ponerlo a producir.

Tan importante o más que una correcta configuración es el mantenimiento del sistema, que podemos definir como los procedimientos que nos permiten que el sistema operativo funcione correctamente a lo largo del tiempo, tratando de solucionar todos los problemas que surjan. Una parte muy importante del mantenimiento del sistema es la **auditoría del sistema**.

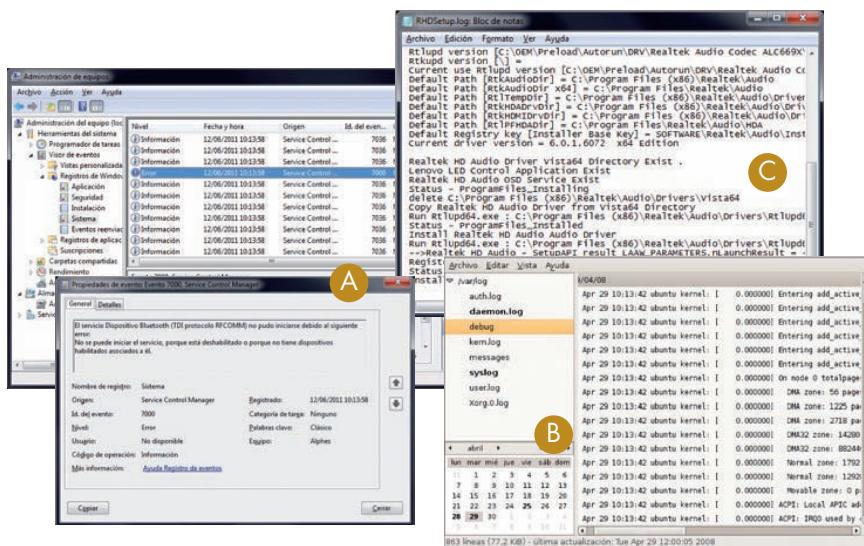


Fig. 3.9. A) Secuencia del visor de sucesos de Windows 7 y ventana descriptora de evento. B) Listado de eventos en Linux. C) Ejemplo de un fichero de log procedente de una instalación y abierto con el bloc de notas.

Algunas aplicaciones más avanzadas son capaces de dejar registros en tablas de bases de datos desde las que posteriormente se pueden realizar consultas o hacer análisis estadísticos y representaciones gráficas.

### A Vocabulario

**Auditoría del sistema:** es la configuración de alarmas que nos advierten del estado del sistema en todo momento. De este modo, el sistema irá dejando registro de cuantos errores o acontecimientos ocurrán en él.

En la Fig. 3.9 se puede ver el visor de sucesos de Windows. Se ha seleccionado un evento que produjo un error en el sistema y este nos informa de que el dispositivo Bluetooth no ha podido iniciarse.

Los sistemas de notificación de los sistemas operativos suelen registrar la información en unos ficheros de texto denominados logs, que normalmente se pueden abrir con cualquier editor de caracteres o procesadores de texto (C).



### Claves y consejos

Es muy importante registrar solo la información significativa. Cualquier sistema puede tomar nota de multitud de sucesos, pero si registramos demasiados, luego no seremos capaces de analizarlos y el registro no nos servirá para nada.

### Actividades

4. ¿Podrías argumentar razones por las que interesa que cada usuario de una red tenga su propia cuenta de acceso identificada por su nombre de usuario?
5. ¿Por qué puede interesar que los usuarios que tengan el mismo perfil laboral pertenezcan a un mismo grupo de usuarios en el sistema operativo servidor?
6. Ensaya los procedimientos de gestión de usuarios creando unos cuantos usuarios en un sistema a los que proporciones propiedades diferentes. Prueba que estas cuentas han sido correctamente creadas iniciando una sesión en el equipo con cada cuenta recién creada. Ahora establece unos cuantos grupos de usuarios y asigna las cuentas anteriormente creadas a estos nuevos grupos.
7. Crea algunas carpetas en el disco duro de una estación de trabajo. Ahora realiza una asignación de permisos sobre esas carpetas a los usuarios y grupos creados en el ejercicio anterior. Comprueba que la asignación de permisos es correcta, es decir, que si a un usuario o a un grupo se le ha asignado solo el permiso de lectura sobre una carpeta, no podrá escribir sobre ella, si bien podrá leer la información contenida en ella.
8. En un sistema Windows, visualiza las distintas páginas del visor de sucesos e identifica los errores que se han producido en el sistema. El código numérico del suceso identifica el evento producido. Puedes investigar en Internet por qué se producen los errores que estás visualizando. Puedes empezar tu investigación buscando este código numérico en la web <http://www.eventid.net>.



### Seguridad

IP es un protocolo sin conexión, por lo tanto, carece de seguridad en la entrega de paquetes. Cuando una comunicación que utiliza el protocolo IP necesita seguridad en la transferencia de paquetes de datos, esta debe ser proporcionada por otro protocolo de capa superior.



### Ampliación

Cada una de estas funciones da origen a una subcapa, la primera función es propia de la subcapa de control de acceso al medio o **MAC** (*Media Access Control*), la segunda lo es de la subcapa de control de enlace lógico **LLC** (*Logical Link Control*), aunque normalmente esta subcapa toma el nombre de la capa OSI que la incluye: enlace de datos o **DLL** (*Data Link Layer*).

## 3. La familia de protocolos TCP/IP

Por su frecuencia de uso, debemos detenernos especialmente en los protocolos que constituyen esta familia, especialmente en el protocolo IP, en el nivel de red, y el protocolo TCP, en la capa de transporte. Hay muchos más protocolos, pero la importancia de estos dos ha hecho que a toda la arquitectura de protocolos utilizados tanto en sistemas UNIX, como actualmente en muchos otros sistemas, se le llame familia de protocolos TCP/IP.

### 3.1. Los protocolos básicos en TCP/IP

La arquitectura TCP/IP no se fija en el nivel 2 de OSI, lo asume en lo que llama nivel de red, pero las instalaciones habituales de redes TCP/IP utilizan redes Ethernet en el nivel 2 de OSI.

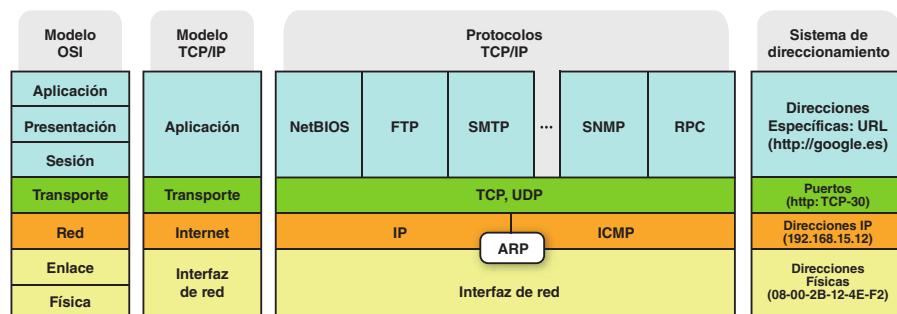
El nivel de enlace asegura una conexión libre de errores entre dos ordenadores de la misma red. Fundamentalmente organiza los bits en forma de tramas y los pasa a la capa física para que sean transmitidos al receptor a través del medio de transmisión.

Cabe distinguir dos funciones en esta capa:

- Como en muchas redes de área local los canales están compartidos por muchos nodos, ¿cómo saber que el canal está libre? Y si lo está, ¿cómo sabe un nodo si puede o no apropiarse de los recursos de la red?
- Puesto que los bits deben ser agrupados en tramas, ¿cómo confeccionar esas tramas? Además, ¿cómo saber si las tramas recibidas son correctas?

Aunque TCP/IP no sigue la arquitectura OSI, se pueden establecer paralelismos como los que aparecen en la Fig. 3.10.

**Fig. 3.10.** Estructura de capas de la arquitectura TCP/IP y su relación con OSI. Se especifican algunos ejemplos de protocolos en cada capa y un ejemplo del sistema de direccionamiento utilizado en cada nivel.



### A. Protocolo IP

IP (*Internet Protocol*) es el protocolo de nivel de red en ARPANET, el sistema de comunicaciones que tradicionalmente han utilizado los sistemas UNIX y que nació a principios de los años 80. Lo más relevante de IP para el administrador de red es que proporciona un sistema de direcciones para que cada nodo de la red quede identificado por una dirección de cuatro números enteros separados por puntos (o 32 bits) denominada dirección IP o de nivel 3, para distinguirla de la dirección MAC (física) o de nivel 2 que se compone de 12 dígitos hexadecimales.

El protocolo IP acepta **bloques de datos** procedentes de la capa de transporte (por ejemplo, desde el protocolo TCP que opera en el nivel de transporte) de hasta 64 Kbytes. Cada bloque de datos, que en este nivel se denominan **segmentos**, debe ser transferido a través de la red (**Internet**) en forma de **datagramas**. Para llevar a cabo este transporte, normalmente la capa de red debe fraccionar los datagramas en un conjunto de **paquetes** IP, que deben ser ensamblados en el destino para que el mensaje sea al final reconstruido con fidelidad. Al ser IP un protocolo sin conexión, cada paquete puede seguir una ruta distinta a través de la internet. El protocolo de capa superior (TCP) será el encargado de la gestión de errores.



### Vocabulario

**Bloque de datos:** conjunto de datos que posee una estructura interior perfectamente definida.

**Segmento:** es el bloque de datos definido en el nivel de transporte (nivel 4 de OSI).

**Paquete:** es el bloque de datos propio del nivel de red (nivel 3 de OSI).

**Datagrama:** es un tipo de paquete (nivel 3) utilizado en servicios de comunicaciones sin conexión.

## O B. Protocolo ICMP

**ICMP** (*Internet Control Message Protocol*, Protocolo de mensajes de control entre redes) es un protocolo que expresa en un único paquete IP algún evento que se produce en la red. Por tanto, se trata de un protocolo de supervisión. Cualquier red TCP/IP debe utilizar el protocolo ICMP.

En la dirección [http://es.wikipedia.org/wiki/Internet\\_Control\\_Message\\_Protocol](http://es.wikipedia.org/wiki/Internet_Control_Message_Protocol) puede encontrarse el formato de los paquetes ICMP así como detalles del funcionamiento orgánico del protocolo.

## O C. Protocolo TCP

**TCP** (*Transmission Control Protocol* o protocolo de control de transmisión) fue especialmente diseñado para realizar conexiones en redes inseguras. TCP es un protocolo de capa de transporte adecuado para proporcionar seguridad a IP.

La seguridad del protocolo TCP le hace idóneo para la transmisión de datos por sesiones, para aplicaciones cliente-servidor y para servicios críticos como el correo electrónico.

La seguridad en TCP tiene un precio que se manifiesta en forma de grandes cabeceras de mensajes, y de la necesidad de confirmaciones de mensajes para asegurar las comunicaciones. Estas confirmaciones generan un tráfico sobreañadido en la red que ralentiza las transmisiones en beneficio de la seguridad.

Los puntos de acceso al servicio (SAP de OSI) en la capa de transporte en TCP/IP se llaman **sockets** o conectores TCP/IP y son extraordinariamente útiles en la programación de aplicaciones de red.

Detrás de cada socket activo se implanta un servicio de red. Cuando alguien en la red requiere de ese servicio, manda mensajes al socket o puerto que identifica a ese servicio. Algunos servicios tienen necesidad de más de un socket para su funcionamiento. Por ejemplo, 80 es el puerto que identifica las peticiones de red hacia un servidor web.

## O D. Protocolo UDP

**UDP** (*User Datagram Protocol* o protocolo de datagrama de usuario) es un protocolo de transporte sin conexión, es decir, permite la transmisión de mensajes sin necesidad de establecer ninguna conexión y, por tanto, sin garantías de entrega. Actúa simplemente como una interfaz entre los procesos de los usuarios de la red y el protocolo IP. Se utiliza en transmisiones rápidas que no necesitan seguridad en la transmisión.

UDP no impone el uso de confirmaciones puesto que su objetivo no es la seguridad y esto hace de él un protocolo de transporte de mucho mayor rendimiento que TCP, y también más inseguro.

En la Tabla 3.1 se pueden observar algunas de las características que diferencian a TCP de UDP, a pesar de que ambos operan en el nivel 4 equivalente del modelo OSI o capa de transporte en el modelo TCP/IP.

TCP	UDP
Es un protocolo confiable	No es confiable
Orientado a la conexión	No establece una conexión inicial
Lleva gestión de las retransmisiones y control de flujo	No gestiona retransmisiones
Secuencia numéricamente los segmentos (paquetes de datos enviados o recibidos)	No gestiona un secuenciamiento de segmentos
Admite segmentos de acuse de recibo	No incorpora acuse de recibo

Tabla 3.1. Diferencias sustanciales entre TCP y UDP.

### Ampliación

En ICMP son posibles, entre otros, mensajes como los siguientes:

- Destino inalcanzable. Se utiliza cuando una subred se da cuenta de que no puede alcanzar otra red solicitada por un datagrama IP, o bien, es alcanzable, pero no en las condiciones especificadas en el paquete IP.
- Tiempo excedido. El campo contador del tiempo de vida de un paquete IP ha descendido hasta 0 y ha sido drenado (retirado) de la red.
- Problemas en parámetros. El valor asignado a un parámetro de una cabecera IP es imposible. Esto suele determinar un error en la transmisión o en las pasarelas de la red.
- Enfriar fuente. Este mensaje se envía a un transmisor para que modere la velocidad de transmisión de paquetes.

### Ampliación

TCP acepta bloques de datos (TPDU, *Transport Protocol Data Unit*) de cualquier longitud, procedentes de las capas superiores o de los procesos de los usuarios, y los convierte en fragmentos de 64 Kbytes como máximo que pasa a la capa de red, quien a su vez puede volver a fraccionarlos para su transmisión efectiva. Cada uno de los bloques de datos –frecuentemente se les denomina **segmentos**– se transmite como si fuera un datagrama separado con entidad propia. TCP es el responsable de ensamblar los datagramas recibidos por el receptor, ya que la red IP puede desordenarlos al utilizar caminos diversos para alcanzar su destino. IP no garantiza que los datagramas lleguen a su destino, por lo que es necesaria una entidad superior (TCP) que se encargue de ello a través de un sistema de temporizadores y retransmisiones en caso de problemas.



### Ampliación

También existe el protocolo RARP (Reverse ARP), que es el protocolo inverso del ARP, es decir, localiza la dirección lógica de un nodo a partir de la dirección física del mismo. Fundamentalmente es utilizado en estaciones de trabajo sin disco, que han conseguido su sistema operativo a través de la red.



### Vocabulario

**Dirección MAC o dirección física:** es la dirección lógica de una interfaz de red en el nivel 2. Se compone de 12 cifras hexadecimales.



### Investigación

En <http://personales.upv.es/rmartin/Tcplp/cap02s01.html> tienes unas descripción de la familia de protocolos TCP/IP y de cómo se relacionan entre sí algunos de ellos. Interesa que leas este documento o alguno similar para que te habitúes a asociar correctamente los niveles de la familia de protocolos TCP/IP con los protocolos concretos que se utilizan en cada nivel. También puedes ayudarte de la página de Wikipedia localizada por la voz «familia de protocolos de Internet».

## E. Protocolo ARP

**ARP** (Address Resolution Protocol o protocolo de resolución de direcciones) no es un protocolo relacionado directamente con el transporte de datos sino que complementa la acción del TCP/IP pasando desapercibido a los ojos de los usuarios y de las aplicaciones de la red.

Como el protocolo IP (equivalente al nivel 3 del modelo OSI) utiliza un sistema de direccionamiento que utiliza el sistema operativo que no tiene nada que ver con las **direcciones MAC** (nivel 2 OSI) que utilizan las tarjetas de las redes de área local, hay que arbitrar un mecanismo de asignación de direcciones IP (cuatro números separados por puntos) a direcciones MAC propias del nivel de enlace. De esto se encarga el protocolo ARP, que funciona del siguiente modo:

Cuando un host quiere transmitir un paquete IP necesita averiguar la dirección MAC del host destinatario cuya dirección es la dirección de destino del campo «dirección de destino» del paquete IP. Para ello genera un paquete de petición ARP que difunde por toda la red. Todos los nodos de la red detectan este paquete y solo aquel host que tiene la dirección IP encapsulada en el paquete ARP contesta con otro paquete ARP de respuesta con su dirección MAC. De este modo el host emisor relaciona dirección IP y dirección MAC, guardando estos datos en una tabla residente en memoria para su uso en transmisiones posteriores.

Puede encontrarse más información detallada sobre este protocolo en la dirección [http://es.wikipedia.org/wiki/Address\\_Resolution\\_Protocol](http://es.wikipedia.org/wiki/Address_Resolution_Protocol).

## 3.2. El direccionamiento de red en TCP/IP

El sistema de direccionamiento IP es muy peculiar y ampliamente aceptado por la comunidad mundial. Cada dirección IP consta de 32 bits agrupados en grupos de 8 bits. Una dirección IP se expresa con cuatro números decimales separados por puntos. Cada uno de estos números varía entre 0 y 255, aunque hay algunas restricciones. Un ejemplo de dirección IP sería 128.100.3.67.

### A. Clases de subredes

Como IP es un protocolo pensado para la interconexión de subredes, cada dirección IP codifica una red y un host dentro de esa red. Atendiendo a los primeros bits de cada dirección se averigua el tipo de subred de que se trata (en cuanto a su volumen) y de su dirección concreta. Los bits restantes codifican el host de que se trata dentro de esa subred. De las cinco clases de subredes, solo tres sirven para el direccionamiento particular de los nodos de la red (Fig. 3.11):

- **Redes de clase A.** Se codifican la subred y los 24 restantes la identificación del host dentro de esa subred. Los valores posibles para la subred varían entre 1 y 126, que coincide con el valor del primer byte de la dirección, es decir, hay 126 subredes posibles de tipo A. Cada una de ellas puede contener 16.777.214 hosts distintos. Este sistema de direccionamiento se utiliza, por tanto, para subredes muy grandes.

- **Redes de clase B.** Se caracterizan porque los dos primeros bits de la dirección son 10. Los 14 bits siguientes codifican la subred, desde 128 a 191 para el primer byte de la dirección, por tanto, son posibles 16.384 subredes de tipo B. Cada una de estas subredes puede contener 65.534 hosts distintos, los codificados por los 16 bits restantes del campo de dirección.



Fig. 3.11. Estructura de los bits para las direcciones IP de las redes de clase A, B, C y D. Las direcciones de clase E están reservadas para aplicaciones futuras o para uso experimental.

- **Redes de clase C.** Se caracterizan por tener sus tres primeros bits con el valor 110. Los 21 bits siguientes codifican la subred y los 8 restantes el host dentro de la subred. El primer byte de la dirección de una subred de clase C tiene un valor comprendido entre 192 y 223. Es posible codificar 2.097.151 subredes distintas de 254 hosts distintos cada una.

Cuando el campo de dirección comienza por la secuencia 1110, se entiende que los 28 bits restantes codifican una dirección de multidifusión, es decir, una dirección especial en donde el destinatario no es único (direcciones de clase D). Las direcciones que comienzan por 1111 se reservan para protocolos especiales como los de administración de grupos de Internet, multitransmisión y otras futuras implementaciones o uso experimental (direcciones de clase E). El valor 127 para el primer byte de una dirección IP está reservado para pruebas de bucle cerrado, es decir, para las comunicaciones entre procesos dentro de la misma máquina.

Al actual protocolo IP se le suele llamar IPv4 para distinguirlo de otra especificación que se empieza ahora a implantar: se trata del protocolo IPv6. Con IPv4 se utilizan direcciones de red de 32 bits, lo que es claramente insuficiente cuando todas las redes se integran entre sí como en el caso de Internet. Aunque tiene muchas más ventajas añadidas en las que aquí no entraremos, IPv6 viene a resolver este asunto, pues su sistema de direccionamiento es de 128 bits. Gran parte de los sistemas operativos modernos así como los dispositivos de red más avanzados ya vienen preparados para la migración de IPv4 a IPv6.

## B. Máscaras de subred

Una **máscara** de subred es una secuencia de 32 bits que sirve para distinguir con facilidad qué parte de una dirección codifica la subred (una subdivisión o grupo de la red total) y qué parte el host. Una máscara se construye poniendo a 1 los bits que pertenecen a la subred y a 0 los bits que pertenecen a la identificación del host. Este modo de asignación permite multiplicar extraordinariamente los distintos tipos de subredes. Así una subred de clase A vendría determinada por la máscara 11111111 00000000 00000000 00000000, es decir, 255.0.0.0. Una subred de clase B tendría la máscara 255.255.0.0 (11111111 11111111 00000000 00000000). La subred de clase C tendría la máscara 255.255.255.0. Son posibles combinaciones cualesquiera de los bits para generar subredes y hosts dentro de las subredes siempre que tanto los «1» como los «0» aparezcan consecutivos.

En la Tabla 3.2 se pueden observar los significados de los diferentes códigos **CIDR** y cuántos hosts se pueden identificar en cada subred. La última columna (máscara equivalente) se refiere a la máscara equivalente al CIDR.

Frecuentemente, para facilitar la notación, suele expresarse la dirección IP en formato **CIDR** (*Classless Inter-Domain Routing*, Encaminamiento Inter-Dominios sin Clases), que consiste en escribir la dirección IP en su forma habitual (cuatro números enteros separados por 1) seguida de otro entero cuyo valor es el número de 1 seguidos de la máscara. Estos dos elementos deben ir separados por el símbolo «/». Un ejemplo de notación CIDR sería 128.100.3.67/24, que significaría que el interfaz de red que posee la dirección IP 128.100.3.67 tiene una máscara 255.255.255.0 (24 unos seguidos de otros 8 ceros) y, que por tanto, pertenece a la red 128.100.3.0 o simplemente 128.100.3.



### Laboratorio

#### Identificación de las subredes de la instalación de red

Proseguimos en la investigación de la red de área local que es objeto de nuestro estudio particular para determinar cómo es su sistema de direccionamiento TCP/IP.

Observando las propiedades del protocolo TCP/IP en cada uno de los ordenadores de la red nos daremos cuenta de que las estaciones y servidores que se comunican entre sí comparten el mismo sistema de direccionamiento, permaneciendo ligados a la misma máscara o al menos a máscaras compatibles entre sí.

Identifica todas las subredes de la instalación de red así como los dispositivos que se encargan de comunicar las distintas subredes que hayas localizado.



CEO

S M R \_ R L \_ A A b a d \_ 0 3 \_ RedesIPSocket.docx

Documento que contiene:

1. Ejemplo sobre cómo dos nodos saben que están o no en la misma red IP.
2. Ampliación del concepto de socket.



### Vocabulario

**Dirección IP:** conjunto de cuatro números de ocho bits que identifican únicamente la dirección de nivel 3 de un ordenador en una red TCP/IP.

**Máscara IP:** es una secuencia de unos y ceros, ambos contiguos, que sirve para denotar en las redes TCP/IP qué identifica la red (secuencia inicial de «1») y qué la subred o conjunto de nodos (secuencia final de «0»).

**CIDR:** es una mejora del sistema de direccionamiento IP que permite una mayor flexibilidad a la hora de asignar rangos de direcciones por el método de extender las clases de red.

## 3

## Instalación y configuración de los equipos de red

CIDR	Clases C	Clases B	Clases A	Hosts*	Máscara
/32	1/256			1	255.255.255.255
/31	1/128			2	255.255.255.254
/30	1/64			4	255.255.255.252
/29	1/32			8	255.255.255.248
/28	1/16			16	255.255.255.240
/27	1/8			32	255.255.255.224
/26	1/4			64	255.255.255.192
/25	1/2			128	255.255.255.128
/24	1			256	255.255.255.000
/23	2			512	255.255.254.000
/22	4			1024	255.255.252.000
/21	8			2048	255.255.248.000
/20	16			4096	255.255.240.000
/19	32			8192	255.255.224.000
/18	64			16384	255.255.192.000
/17	128			32768	255.255.128.000
/16	256	1		65536	255.255.000.000
/15	512	2		131072	255.254.000.000
/14	1024	4		262144	255.252.000.000
/13	2048	8		524288	255.248.000.000
/12	4096	16		1048576	255.240.000.000
/11	8192	32		2097152	255.224.000.000
/10	16384	64		4194304	255.192.000.000
/9	32768	128		8388608	255.128.000.000
/8	65536	256	1	16777216	255.000.000.000
/7	131072	512	2	33554432	254.000.000.000
/6	262144	1024	4	67108864	252.000.000.000
/5	524288	2048	8	134217728	248.000.000.000
/4	1048576	4096	16	268435456	240.000.000.000
/3	2097152	8192	32	536870912	224.000.000.000
/2	4194304	16384	64	1073741824	192.000.000.000
/1	8388608	32768	128	2147483648	128.000.000.000

Tabla 3.2. Descripción de los códigos CIDR. Fuente: <http://www.vitessennetworks.com.mx>

### 3.3. Protocolos TCP/IP de nivel superior

En el nivel superior de la arquitectura TCP/IP hay una infinidad de protocolos. Aquí nos vamos a referir a los más comunes, pero existen casi tantos protocolos distintos como tipos de aplicaciones o servicios de nivel de aplicación:

- **FTP.** Es utilizado para la descarga o carga de ficheros en Internet. Define dos canales de comunicación, uno para el gabinete de esta y otro para la transferencia de datos. Pone en marcha el diálogo entre un cliente FTP y un servidor FTP.
- **HTTP.** Es el protocolo utilizado por los navegadores para el acceso a las páginas web.
- **SNMP.** Es uno de los protocolos de la familia TCP/IP utilizados para la gestión de la red. En cada entidad de la red, se habilitan unos agentes que recogen información y que envían a un gestor central desde donde se puede visualizar.
- **RPC.** Es el protocolo de la capa de aplicación en la arquitectura TCP/IP que se encarga de establecer diálogos entre las aplicaciones clientes y sus equivalentes servicios. Se trata de un protocolo básico para la arquitectura de las aplicaciones cliente-servidor.
- **SMTP.** Es el protocolo básico para el intercambio de mensajes de correo electrónico entre servidores de correo o el que usa la aplicación cliente de correo para enviar mensajes al servidor al que se conecta.
- **POP.** Es el protocolo de comunicaciones de alto nivel que se encarga de descargar mensajes de correo electrónico desde el servidor de correo en donde se encuentra el buzón a la bandeja de entrada del cliente de correo. La versión actual del protocolo POP es 3, por ello se denota como POP3.
- **IMAP.** Es un protocolo semejante a POP, pero con algunas funcionalidades añadidas que lo hacen recomendable en situaciones de congestión. Por ejemplo, permite descargar el correo electrónico solo a petición del usuario una vez leída la cabecera del mensaje.

La mayor parte de los protocolos de nivel superior tienen asociado uno o más números de puerto en sus sockets de comunicación, por ejemplo, FTP-21, HTTP-80, SMTP-25, POP-110, etc., aunque esta asociación puede ser alterada por las aplicaciones o por el administrador de la red.



#### Claves y consejos

Las aplicaciones de SNMP son muy útiles a los administradores de la red porque permiten la configuración de los parámetros de la red desde una consola central, además de recoger estadísticas de utilización de los recursos.

#### Ejemplos

##### Acceso desde el explorador a un servidor web

Con este ejemplo vamos a tratar de comprender cómo un explorador de Internet utiliza el sistema de direccionamiento y la tec-

nología de sockets asociados a puertos de comunicaciones para resolver la exploración de una página web.

En la Fig. 3.12 está representado el acceso de un cliente con dirección IP 10.1.1.5 con un explorador a un servidor web que reside en Internet con dirección 225.10.2.150, utilizando como intermediario un servidor que hace la función de encaminador de paquetes entre la red local en la que se encuentra el cliente e Internet en donde se encuentra el servidor. Describamos su funcionamiento.

En el paso 1, el cliente hace una petición con destino 225.10.2.150, dejando abierto el puerto 1345. Este paquete es capturado por el servidor-encaminador y envía en su nombre (dirección 213.97.2.12) el paquete al servidor web dejando abierto otro puerto «x» de su interfaz de red externa (paso 2).

El servidor web procesa la petición y devuelve (paso 3) la página a quien se la pidió que fue 213.97.2.12 por el puerto que le dejó abierto que denominamos «x».

En el cuarto paso, el encaminador pone el paquete en la red interna, enviándolo a quien le solicitó su servicio de encaminamiento por el puerto que le dejó abierto que era el 1345.

Aquí tenemos un ejemplo de un cliente que utiliza un servicio (de encaminamiento) para acceder a otro servicio informativo de páginas web.

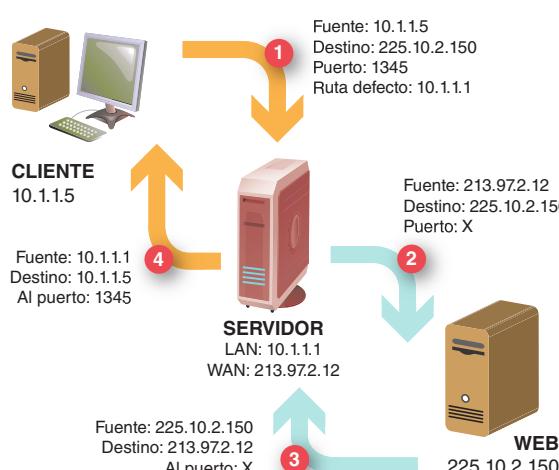
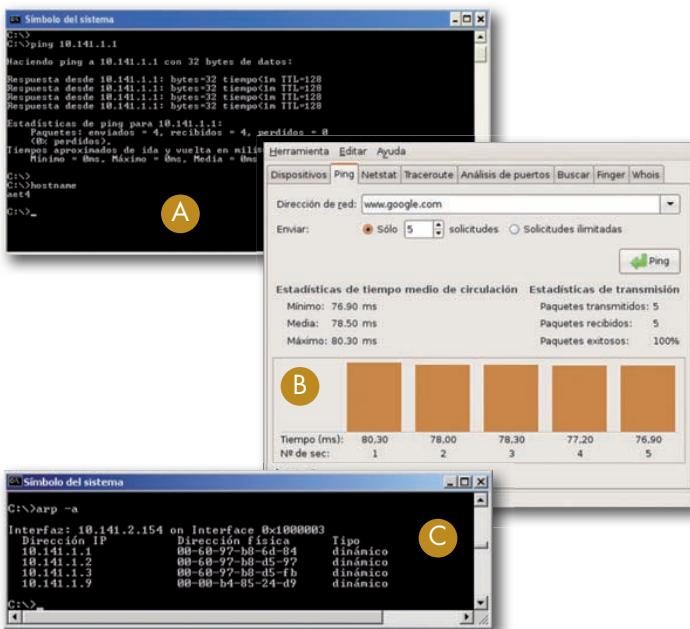


Fig. 3.12. Cliente web que accede a un servidor web a través de un encaminador.



**Fig. 3.13.** A) Ejecución del comando ping sobre el nodo 10.141.1.1, y verificación del nodo local con hostname en una estación Windows. B) Utilidad gráfica de ping en un sistema Linux sobre www.google.com. C) Ejecución del comando ARP.

Hay que tener en cuenta que la utilidad ping varía dependiendo de la versión IP que ejecuta la red. Si no se especifica lo contrario, siempre se supone que se trata de la versión 4 (IPv4).

### 3.4. Utilidades propias de redes TCP/IP

Las siguientes utilidades son comunes en los sistemas UNIX. Otros sistemas operativos las incorporan en alguna medida si llevan instalado TCP/IP. El nombre exacto y los calificadores de las órdenes varían según los sistemas y las versiones. La ayuda del sistema operativo será de gran utilidad para concretar exactamente el formato de cada orden.

#### A. Utilidad ping

Ping (*Packet Internet Groper, Tanteo de paquetes Internet*) es una utilidad que sirve para enviar mensajes a una dirección de red concreta que se especifica como argumento con el fin de realizar un test a la red utilizando el protocolo ICMP. El nodo destinatario nos reenviará el paquete recibido para confirmarnos que se realiza el transporte entre los dos nodos correctamente. Además, proporciona información añadida sobre la red, como se puede ver en la Fig. 3.13, A y B.

Ping puede configurar varios parámetros cuando se ejecuta desde la línea de comandos, por ejemplo, es posible indicarle cuántos paquetes queremos enviar, qué información vamos a enviar con cada paquete, el tamaño de cada paquete enviado, etc. Tendremos que recurrir a la ayuda del comando ping en cada sistema para asegurarnos de la sintaxis exacta de la orden.

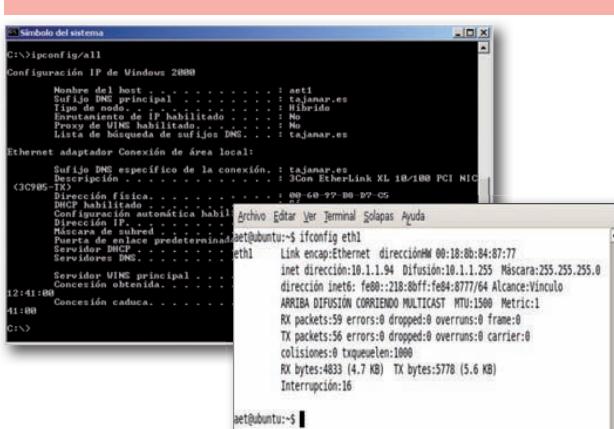
#### B. Utilidad arp

ARP (*Address Resolution Protocol, Protocolo de resolución de direcciones*), es una utilidad sirve para asignar automáticamente direcciones IP a direcciones físicas, es decir, para gestionar el protocolo ARP. En la parte superior de la Fig. 3.13-C se interroga al sistema mediante ARP cuáles son las direcciones IP que tiene resueltas, es decir, de las que conoce su dirección física y cuál fue el tipo de asignación.

#### C. Utilidad ipconfig de Windows e ifconfig/iwconfig de Linux

Configura la dirección del host o bien proporciona información sobre la configuración actual. Por ejemplo, la ejecución del comando siguiente proporciona información sobre la tarjeta Ethernet 3Com EtherLink XL 10/100 PCI (Fig. 3.14, arriba).

La utilidad equivalente en Linux es ifconfig para las redes cableadas e iwconfig para las redes inalámbricas, aunque la mayor parte de las distribuciones ya permiten configurar muchos de los parámetros que admiten a través de la interfaz gráfica. La ejecución del comando «ipconfig help» en Windows e «ifconfig -h» y «iwconfig -h» en Linux nos proporcionarán la ayuda necesaria para la utilización de la orden, ejemplos incluidos. En general, cualquiera de estas órdenes tiene su propia ayuda con el calificador HELP para Windows y -h o --help para Linux.



**Fig. 3.14.** Respuesta del sistema operativo de red al comando ipconfig/all en una estación de trabajo Windows (arriba). Visualización de la configuración de red para la interfaz eth1 en una estación Linux mediante ifconfig (abajo).

## O D. Utilidad netstat

Netstat (*Network status*), proporciona información sobre el estado de la red. El comando ejecutado en la Fig. 3.15 sobre Windows obtiene información estadística sobre los paquetes de red enviados y recibidos. Como se ve, sobre Linux, la orden puede proporcionar muchas otras informaciones como el estado de las conexiones, lo que hay al otro lado de cada conexión, etcétera.

## O E. Utilidad route

Sirve para determinar las rutas que deben seguir los paquetes de red. Profundizaremos en el concepto de rutas más adelante. De momento, basta con que entendamos que una ruta indica el camino apropiado por el que un paquete puede alcanzar su destino o, al menos, aproximarse a él.

Para manejar las tablas de rutas, en sistemas Windows suele utilizarse la orden ROUTE, mientras que en sistemas Linux hay una gran diversidad de órdenes y utilidades, aunque la más usual es «ip route», que admite una multitud de parámetros que deberemos consultar en cada versión para utilizarlo con propiedad.

Por ejemplo, si imprimimos las rutas disponibles para un nodo tendremos la siguiente salida (Fig. 3.16-A):

## O F. Utilidad tracert

Se utiliza para controlar los saltos de red que deben seguir los paquetes hasta alcanzar su destino (Fig. 3.16 B y C). Además proporciona información sobre otros parámetros de la internet. Cuando el número de saltos es 1, esto quiere decir que la red es plana, es decir, se trata de una red de área local.

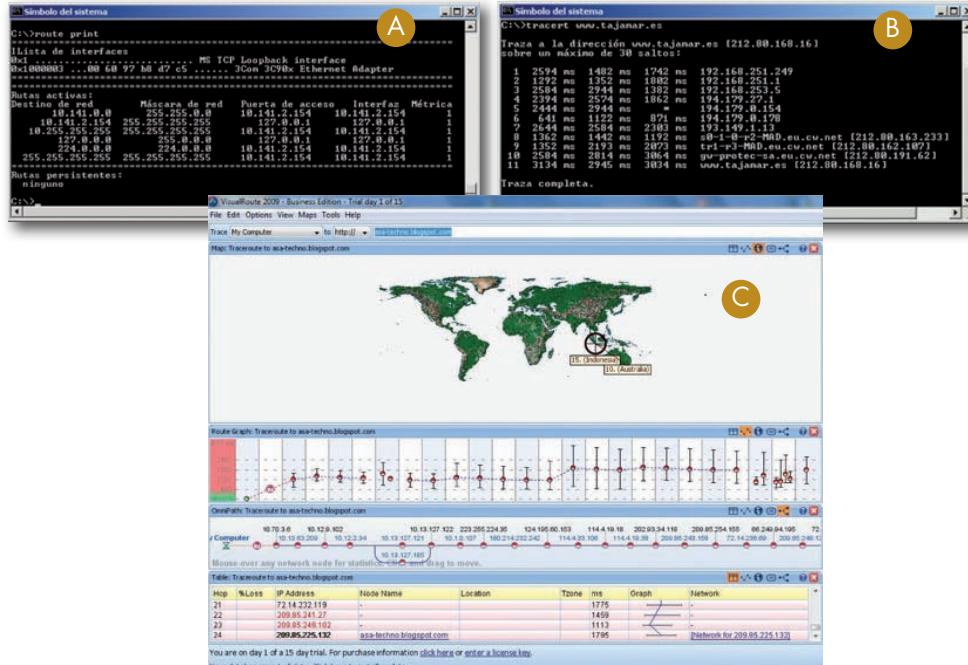


Fig. 3.16. A) Respuesta del sistema al comando route. B) Comando tracert sobre Windows en el que se pueden observar 11 saltos. C) Utilidad gráfica VisualRoute.

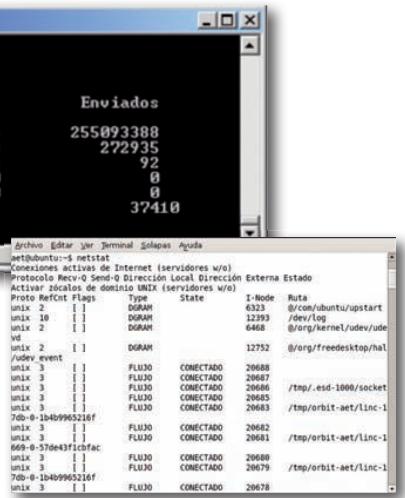


Fig. 3.15. Respuesta del sistema al comando netstat en Windows y en Linux.

En la Fig. 3.16 A podemos apreciar tres secciones. En la primera, se especifican las interfaces de red que posee el nodo en el que se ejecuta route. En la segunda sección se describen las rutas activas en ese momento, núcleo de la tabla de enruteamiento. En la tercera sección se describen, si existen, las rutas persistentes. En Linux es habitual interrogar al sistema sobre las rutas con la orden «ip route».

**Truco**

Para realizar una de estas conexiones anónimas se suele utilizar como nombre de usuario la palabra «anonymous» y como contraseña, suele ser una buena costumbre teclear la dirección de correo electrónico del usuario que pretende beneficiarse del servicio ftp.

**G. Utilidades ftp y tftp**

La utilidad ftp sirve para intercambiar ficheros entre dos nodos de la red utilizando el protocolo FTP. FTP también tiene su parte de cliente y su parte de servidor. Cuando se ejecuta el cliente ftp, aparece el identificador de utilidad «FTP>» sobre la que se ejecutan los comandos ftp: listar, traer (bajar) o dejar (subir) ficheros, etc. Previamente a la utilización del FTP para realizar transferencias, es necesario preparar una conexión segura a través del protocolo TCP. Esto se realiza con el comando open seguido de la dirección IP o el nombre DNS del host remoto. El comando tftp es similar al ftp, más fácil de configurar, pero con menos prestaciones.

La utilización de un servidor ftp exige tener acceso al servidor a través de un nombre de usuario y una contraseña que nos asignará el administrador del sistema remoto. Muchos servidores en Internet tienen información pública a la que se accede sin necesidad de tener cuenta en el equipo, permitiendo conexiones de usuarios anónimos.

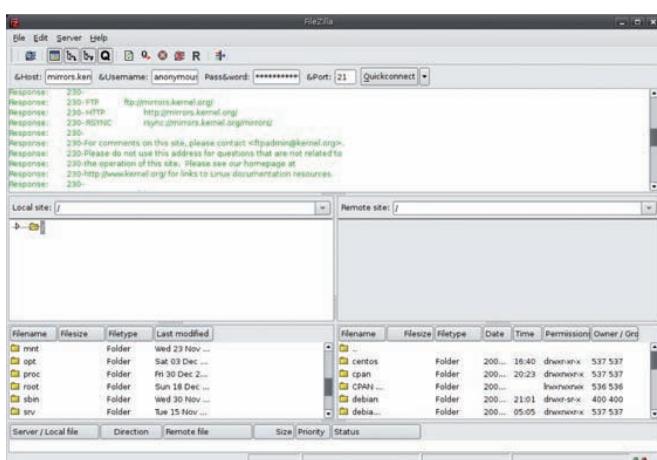


Fig. 3.17. Ejemplo de cliente FTP gráfico.

En la Fig. 3.17 se puede ver un ejemplo de Filezilla, un cliente gráfico típico de ftp, que tiene versiones tanto para Windows como para Linux. En la ventana izquierda aparece el sistema de ficheros local. A la derecha, una vez realizada la conexión aparecerá el sistema de ficheros remoto. Las operaciones de copiado se realizan arrastrando los ficheros o directorios desde un lado hacia el otro.

Filezilla dispone tanto de la versión cliente (la representada en la figura) como versión servidor. Es gratuita y se puede descargar desde <http://filezilla-project.org/>.

**H. Utilidades telnet y ssh**

Sirve para realizar conexiones remotas interactivas en forma de terminal virtual a través del protocolo de alto nivel TELNET. El comando va acompañado de la dirección IP del nodo remoto o de su dirección DNS.

Los servidores Windows implementan un servidor TELNET, que sirve sesiones en forma de ventanas emuladoras DOS a los clientes TELNET que se conectan a ellos desde su red, lo que es muy interesante para ejecutar scripts en máquinas remotas.

En el mundo Linux, la utilidad equivalente más moderna es ssh. Esta es una de las utilidades más versátiles que tiene su parte de cliente y de servidor. Puede ejecutar aplicaciones remotas, copiar ficheros, crear sesiones remotas gráficas, crear túneles de comunicación, etc. Funcionalmente, ssh puede sustituir las conexiones remotas de TELNET, pero la gran ventaja de ssh es que cifra las conexiones, por lo que es mucho más seguro que TELNET.

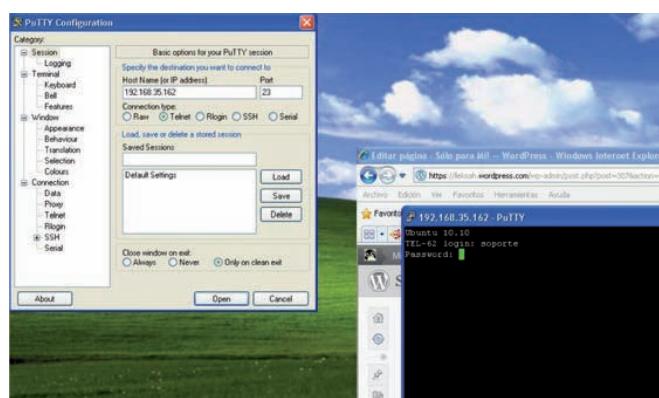


Fig. 3.18. Ejemplo de ejecución de TELNET desde un sistema operativo de Microsoft mediante PuTTY.

**Truco**

Existen aplicaciones gratuitas que se pueden instalar en sistemas operativos de Microsoft que incorporan clientes de conexión remota como telnet, ssh y otros. Por ejemplo, PuTTY (Fig. 3.18).



## Actividades

- 9.** Las siguientes afirmaciones ¿son verdaderas o falsas?
- TCP es un protocolo del nivel de transporte.
  - ARP es un protocolo que sirve para resolver asociaciones de direcciones físicas en direcciones IP.
  - IP es un protocolo que se puede situar en la capa 2 de OSI.
  - Una máscara de red son cuatro números enteros cualesquiera de ocho bits cada uno separados por puntos.
  - Todos los bits puestos a «1» de una máscara de red deben estar contiguos y al principio de la máscara.
  - Dos hosts con idéntica máscara pertenecen a la misma subred.
  - Dos hosts que tienen igual la parte de dirección IP correspondiente a la secuencia de «1» de sus máscaras pertenecen a la misma subred.
  - Dos direcciones IP iguales no pueden convivir en la misma red.
- 10.** Describe las características de las clases A, B y C para redes IP.
- 11.** Identifica qué protocolos de la lista siguiente son específicos de la tecnología TCP/IP:
- |          |          |          |
|----------|----------|----------|
| a) SNMP. | b) IP.   | c) MAPI. |
| d) IMAP. | e) POP.  | f) HDLC. |
| g) ARP.  | h) X.25. |          |
- 12.** Se propone el siguiente ejercicio para practicar la gestión del direccionamiento IP. Primero hay que contar con varios ordenadores en red sobre los que se tengan derechos de administración para poder modificar sus direcciones de red. A continuación, deben seguirse los siguientes pasos:
- Elegir una máscara 255.255.255.0 (clase C) y una dirección 192.168.100.x, donde x será el número que identifique cada PC (si hubiera cinco PC, x valdría 1 en el primer PC, 2 en el segundo, etc.). Después de asignar estas direcciones y máscaras a cada PC, comprobar que todos pueden comunicarse entre sí utilizando la orden «ping destino», donde destino es cualquier PC en red.
  - Seguidamente modificar las máscaras de los PC por 255.255.0.0 (clase B). ¿Pierdes la comunicación? ¿Por qué?
  - Vuelve a la máscara 255.255.255.0 y modifica las direcciones IP de un subgrupo de PC para que sean 192.168.50.x. Comprueba ahora qué PC pueden comunicar con qué otros. Ahora observarás que tienes dos subredes conviviendo en la misma red física, con la misma máscara pero con diferentes direcciones IP: la red 192.168.100 y la 192.168.50.
  - Por último, vuelve a establecer la máscara de todos los PC como 255.255.0.0. En ese momento, has vuelto a tener una única subred (la 192.168) por integración de las dos subredes en una superior. Comprueba que al estar de nuevo todos los PC en una única subred, todos vuelven a tener comunicación entre sí.
- 13.** Busca en Internet una herramienta de escaneo de puertos de libre distribución. Podrás encontrarla buscando «escáner de puertos» o «port scanner». Instálala en una estación de la red y ejecútala para analizar los puertos (sockets) que tiene abiertos un servidor y los servicios asociados a ellos. Si realizas esta operación contra todos los servidores de la red, podrás realizar un mapa de servicios de red.
- 14.** Se propone el siguiente ejercicio para practicar la identificación de parámetros de red. Hemos de partir de un conjunto de PC en red con direcciones IP compatibles de modo que todos puedan responder a la orden ping.
- Elige un PC diana contra el que vas a hacer las pruebas y otro PC cliente desde el que ejecutarás los comandos y en el que operarás tú mismo. Comprueba que la red de ambos PC está operativa.
  - Haz ping desde el PC cliente contra el PC diana. Comprueba que tienes comunicación porque la orden ping obtiene eco del destino.
  - ¿Cuál es la dirección física del PC destino? Con la orden arp -a obtendrás el listado de todas las direcciones físicas con las que el PC cliente se ha comunicado en los últimos minutos. Una de ellas será la dirección física del PC diana: la que corresponda a su dirección IP.
  - Deja pasar algunos minutos sin actividad de red entre el PC cliente y el PC diana y vuelve a ejecutar la orden arp -a. Observarás que la dirección física del PC diana ha desaparecido puesto que la tabla de direcciones arp es dinámica y se reconstruye cada cierto tiempo.
- 15.** Para realizar este ejercicio deberás tener disponible en el laboratorio un servidor ftp básico. Cada servidor ftp admite un conjunto de calificadores para la orden ftp de los clientes que se conectan a él. También existe esta dependencia por parte de los clientes. La ayuda de la orden ftp te puede orientar sobre cómo utilizarlo.
- Identifica en primer lugar la dirección IP del servidor ftp y asigna al cliente que vayas a utilizar una dirección compatible con la del servidor de modo que puedas establecer comunicación entre ellos con la orden ping.
  - Si el servidor ftp requiere autenticación, el administrador del servidor deberá proporcionarte una cuenta de acceso y un directorio sobre el que poder hacer cargas y descargas.
  - Abre el cliente ftp especificando la dirección URL del lugar que te haya asignado el administrador del servidor ftp (Ayuda: comando open).
  - Sube un fichero desde el PC cliente al servidor (Ayuda: comando put).
  - Desde otro cliente, conéctate al servidor ftp y trata de descargar el fichero que subiste en el apartado anterior (Ayuda: comando get).



### Caso práctico 1

#### Configurar el sistema de direccionamiento IP de nodos Linux y Windows

Asignar direcciones IP a los ordenadores de la red es la actividad más frecuente del administrador de red puesto que un ordenador no puede funcionar en red sin un correcto sistema de direccionamiento. Vamos a suponer que el administrador de una red tuviera que configurar un servidor y un cliente de la red. El servidor podría ser una máquina destinada a servir sus discos como carpetas compartidas en la red. El cliente podría ser el portátil de un comercial que conecta frecuentemente a la red empresarial, pero que también lo tiene que conectar a las redes de las empresas de los clientes que visita y que, por tanto, debe cambiar su direccionamiento muy a menudo.

Es posible configurar estas direcciones dinámicamente (mediante DHCP) o estáticamente. En el primer caso habrá un servicio de red (servidor DHCP) que asignará automáticamente las direcciones IP a los ordenadores de la red. En el caso segundo, será el administrador de red quien asigne manualmente la dirección a cada ordenador.

Habitualmente, los servidores llevan una dirección estática porque así es más fácil encontrar los servicios de red que provea. En el caso de los clientes, se puede utilizar un sistema dinámico que es más cómodo o el estático.

Vamos a configurar una dirección dinámica (el caso de un cliente) y una dirección estática (el caso de un servidor) tanto para Windows como para Linux.

#### Configurando sobre Linux

Para asignar la dirección IP acudiríamos al panel de red, que está accesible desde el menú de herramientas de sistema (su nombre exacto dependerá de la distribución que utilicemos) y nos aparecerá un panel como el de la Fig. 3.19-A.



Fig. 3.19. Configuración gráfica de la dirección IP en Linux.

Seleccionamos la interfaz de red sobre la que queramos operar, que en la figura es eth1, y hacemos clic sobre el botón de propiedades para que nos aparezca la ventana de la Fig. 3.19-B. Desde allí tenemos dos posibilidades:

a) **Configurar el modo itinerante:** esto activa el direccionamiento automático del nodo y la tarjeta de red esperará a que algún servidor DHCP le asigne automáticamente su dirección. Este sería el caso de querer configurar un cliente con direccionamiento automático.

b) **Configurar una dirección estática (como aparece en la imagen).** En este caso le hemos asignado al nodo la dirección 10.1.1.94, con máscara de red 255.255.255.0 y puerta por defecto 10.1.1.20.

#### Configurando sobre Windows

En este caso la configuración de la red es accesible desde el ícono de «Red» del Panel de control de Windows.

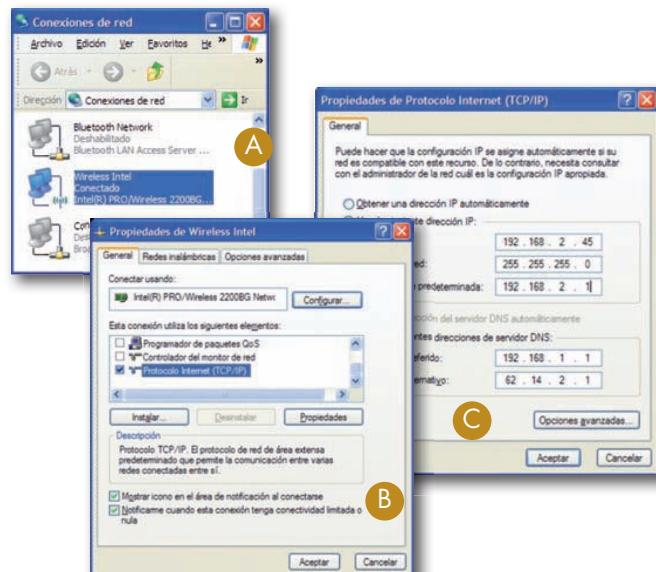


Fig. 3.20. Configuración de la dirección IP en Windows.

Nos aparecerá una ventana con un listado de las interfaces disponibles por el sistema (Fig. 3.20-A). Elegiremos la que nos interese (en nuestro caso es una interfaz inalámbrica denominada «Wireless Intel») y haciendo clic con el botón derecho del ratón elegiremos «Propiedades». Se desplegará la ventana de la Fig. 3.20-B, que nos presenta una lista con las pilas de protocolos y otros servicios disponibles. Seleccionaremos la pila TCP/IP y haciendo clic en propiedades nos presentará la ventana de la Fig. 3.20-C. Desde allí, tenemos dos posibilidades:

- Si seleccionamos «Obtener una dirección IP automáticamente», le indicamos a Windows que solicite para esa tarjeta de red una dirección IP automáticamente. Sería nuestro caso de cliente.
- Si seleccionamos «Usar la siguiente dirección IP», Windows nos iluminará los campos de dirección IP y máscara de red para que los podamos introducir manualmente. De este modo configuraríamos el servidor con dirección IP estática. El resto de los campos no son relevantes de momento. Según esta configuración, el servidor (sea Windows o Linux) siempre tendrá una dirección fija, fácilmente localizable por todos los usuarios de la red. En el caso del portátil del comercial, al tener configurada su dirección IP mediante un procedimiento automático, su dirección variará en función de la red a la que se conecte, pero será transparente para él.

## ● 4. Familia de protocolos en sistemas de Microsoft

Fundamentalmente Microsoft propone los tres siguientes posibles transportes que son compatibles entre sí formando hasta tres pilas de protocolos:

- Protocolo **NetBeui** (*NetBIOS Extended User Interface*, Interfaz de usuario extendida NetBIOS). Da soporte para pequeñas redes y es un protocolo de transporte muy simple y fácil de utilizar. Solo se puede aplicar a redes de área local, es decir, NetBeui es un protocolo incapaz de ser encaminado para saltar de una red de área local a otra.
- Protocolo **IPX/SPX**. Como se ha visto anteriormente, este protocolo ha sido construido por Novell para su sistema NetWare. Da soporte para redes pequeñas y medianas. Con IPX/SPX es posible un sistema básico de encaminamiento. Microsoft ha construido protocolos compatibles con IPX/SPX, que dan servicio de transporte como si se tratara de redes NetWare, por ejemplo, el protocolo NwLink.
- Protocolo **TCP/IP**. Este protocolo ha sido diseñado especialmente para poder ser encaminado entre distintas redes de área local. Es el protocolo ideal cuando en la instalación se halla presente una red de área extendida o se pretenden conectar los ordenadores de la red a Internet.

Con TCP/IP, Microsoft sigue ofreciendo a los usuarios de sus sistemas operativos la misma interfaz que utilizaba con redes NetBeui. Por ejemplo, cuando un usuario necesita acceder a un recurso de la red como una carpeta o una impresora, el nombre del recurso en la red se compone como la suma de dos literales.

El primer literal contiene el nombre del servidor dentro de la red en algún formato permitido por la red, por ejemplo: miservidor.miempresa.com. El segundo literal contiene el nombre del recurso compartido: la carpeta o la impresora. Por ejemplo: ImpresoraPlanta1.

De este modo el acceso a la impresora a través de la red se lleva a cabo con el siguiente nombre compuesto:

**\miservidor.miempresa.com\ImpresoraPlanta1**

Otros sistemas operativos también pueden utilizar los recursos servidos por las redes de sistemas operativos de Microsoft. Samba, por ejemplo, es una tecnología utilizada por sistemas Linux para compartir recursos simulando las redes de Microsoft. Si un sistema Linux, con Samba instalado y configurado, brinda una carpeta a la red, otro sistema Windows en la misma red lo verá como si el servicio residiera en otro sistema Windows en vez de en Linux. De modo semejante, un sistema Linux puede aprovecharse de una carpeta servida por otro sistema Windows utilizando un cliente Samba.

### Ampliación

Microsoft permite además la incorporación de otros protocolos para conexiones específicas como el protocolo DLC (Data Link Control), protocolos AppleTalk para interconexión con redes de Apple, etc. Linux también permite la incorporación de otros protocolos que no le son nativos pero, en general y debido a la filosofía que abandera, es más reacio a integrar protocolos propietarios.

En las últimas versiones de Windows se observa un abandono paulatino del protocolo NetBeui. Esto generaría grandes problemas de compatibilidad con redes anteriores de Microsoft que tradicionalmente utilizaron este protocolo. Para resolver este problema, Microsoft ha incorporado la interfaz NetBIOS, empleada por la mayor parte de las aplicaciones construidas para usar la red con NetBeui, utilizando como transporte TCP/IP en vez de NetBeui. De este modo, las aplicaciones NetBIOS siguen funcionando pero sirviéndose de una red universal como es la red TCP/IP. De hecho, a partir de Windows XP el protocolo NetBeui no está disponible en la instalación típica del sistema operativo.



### Claves y consejos

A la hora de decidir qué protocolo instalar como transporte en el sistema de Microsoft se debe tener en cuenta lo siguiente:

- Si la red es pequeña y no se prevé un crecimiento considerable a corto plazo, bastaría con poner NetBeui, aunque se recomienda TCP/IP.
- Si el servidor o las estaciones con software de Microsoft deben convivir en un entorno de red en que se hayan presentes servidores NetWare, entonces conviene instalar el protocolo IPX/SPX.
- En cambio, si la red de área local debe estar conectada a Internet o debe estar muy segmentada, entonces el protocolo más apropiado es TCP/IP.

En la ventana superior de la Fig. 3.21, denominada «Propiedades de Conexión de área local», tenemos la ventana de configuración de la red en Windows. Se debe observar que tiene algunos elementos instalados. El primero que aparece en la figura, denominado «Compartir impresoras y archivos para redes Microsoft», se encarga de que los recursos locales puedan ser compartidos en la red; se trata, por tanto, de un componente servidor. No consideraremos de momento el segundo elemento de la figura.

El tercer elemento es el protocolo TCP/IP. Desde aquí se pueden configurar todos los parámetros de una red TCP/IP en Windows.

Si decidimos instalar más componentes de la red, lo que se consigue haciendo clic en el botón de instalar, nos aparecerá la ventana superior derecha. En ella vemos que podemos agregar clientes, servicios o protocolos. Un cliente nos permitiría usar los servicios de la red proporcionados por otros servidores que utilizan otras tecnologías de red. De los servicios aún no nos ocuparemos, pero si decidimos añadir nuevos protocolos entonces obtendremos la ventana inferior derecha que permite añadir entre otros protocolos, la pila del protocolo IPX/SPX utilizando NetBIOS sobre él.

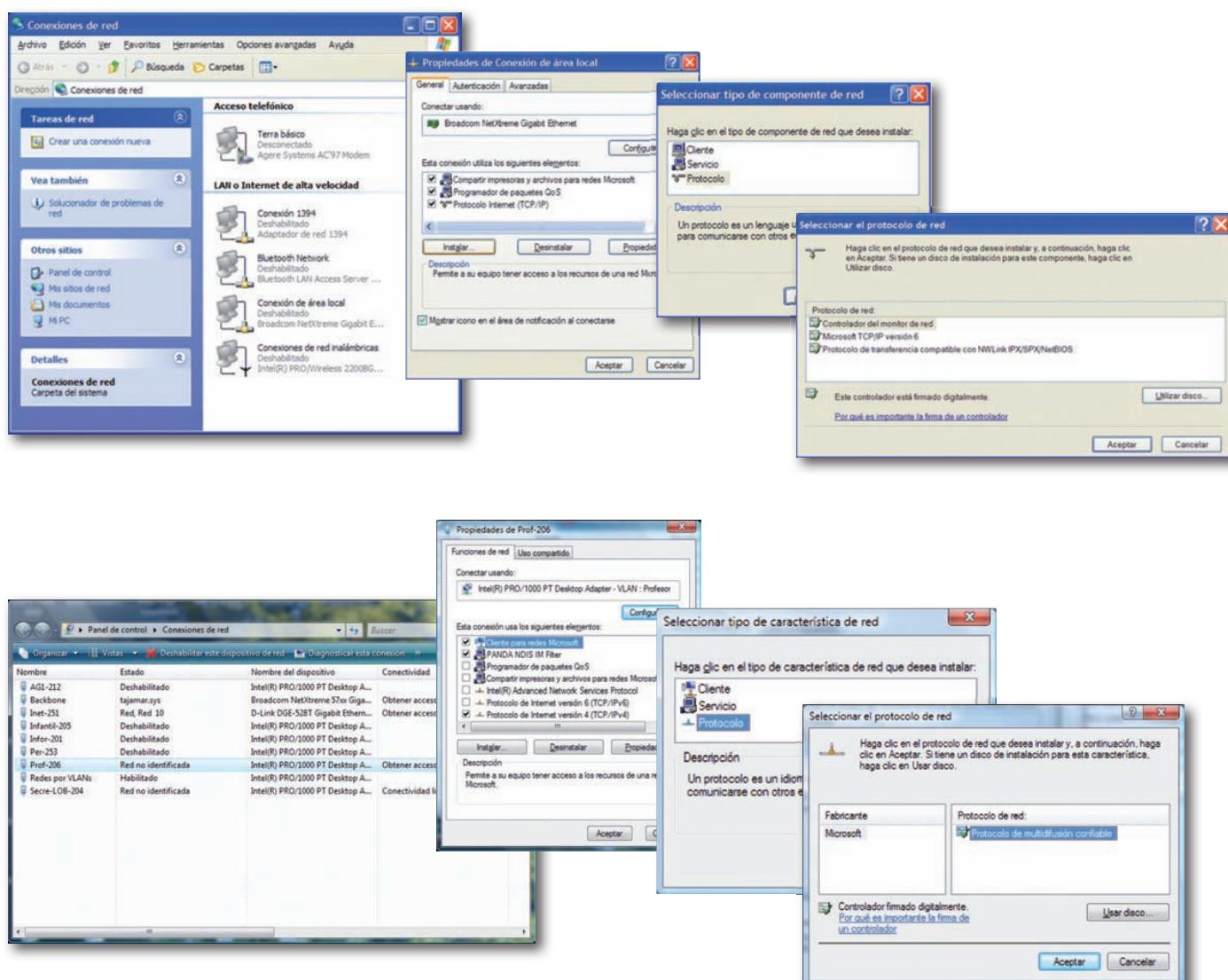


Fig. 3.21. Secuencia de ventanas del asistente de instalación de protocolos en distintos tipos de sistemas Windows.



## Actividades

16. ¿Pueden convivir los protocolos NetBeui y TCP/IP sobre la misma red? ¿Por qué?

¿Pueden convivir los protocolos NetBeui y TCP/IP sobre la misma tarjeta de red? ¿Depende de la tarjeta de red o del sistema operativo?

17. Prepara unos ordenadores en red que tengan como sistema operativo alguna versión de Windows. Después sigue los siguientes pasos:

a) Asegúrate de que cada PC tiene un nombre distinto que le identifique únicamente. Además todos deben pertenecer al mismo grupo o dominio NetBIOS. Tanto el nombre como el grupo al que pertenecen se pueden configurar desde las Propiedades de «Mi PC» (en algunas versiones de Windows, «Mi Equipo»).

b) No es necesario que estos PC ejecuten el protocolo TCP/IP, basta con NetBEUI, pero si tienen TCP/IP ase-

gúrate de que todos comparten el mismo sistema de direccionamiento.

c) Ahora abre el explorador de Windows y abre desde él «Mis sitios de red». Investiga en las subcarpetas de la red y verás todos los servicios compartidos a la red que tienen los PC del grupo a través de NetBIOS. Ten en cuenta que solo verás aquellos servicios para los que tengas derecho desde tu cuenta de acceso a la red.

18. Entérate de los servicios de red provistos por la red de área local que estamos estudiando y prueba a realizar conexiones a estos servicios desde una estación cliente. Ensaya especialmente las conexiones a servicios de ficheros y de impresoras compartidas. Ve familiarizándote con los nombres de los servidores y de los servicios compartidos que proveen.



## Caso práctico 2

### Subnetting

Se hace evidente que la dirección IP de un nodo es el elemento que mejor le define tecnológicamente desde el punto de vista de la red. Es por ello muy importante adquirir una cierta soltura en los cálculos relativos a los sistemas de direccionamiento.

Para el estudio se partirá de un ejemplo sobre el que intentaremos calcular todos los parámetros de red. En concreto, se dispondrá de un nodo con dirección 192.168.15.12 con máscara de red 255.255.255.0 (o lo que es lo mismo 192.168.15.12/24 en notación CIDR) y con puerta por defecto (dirección del encaminador que le conecta a Internet) 192.168.15.254 (Fig. 3.22).

### O A. Cálculo de direcciones IP

#### Cálculo de la máscara de red de clase

La dirección IP del nodo (192.168.15.12) se corresponde con una red de clase C (puesto que el primer octeto está comprendido entre 192 y 233). Su máscara de red de clase es de 24 bits, es decir: 255.255.255.0, lo que en este caso se nos proporciona como dato de partida.

#### Cálculo de la dirección de red

La dirección de red se construye a partir de la dirección del nodo, sustituyendo los bits que codifican el host por ceros y dejando intactos los bits que codifican la red.

En este caso, como la máscara es de 24 bits, habrá que dejar intactos los 24 primeros bits y poner a cero los 8 bits

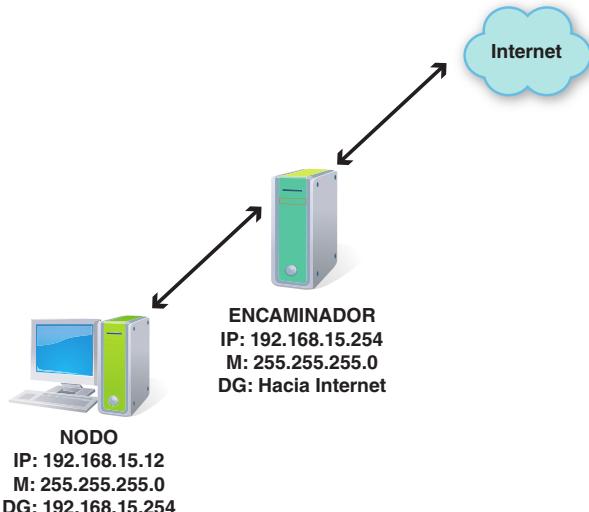


Fig. 3.22. Ejemplo de red para el cálculo de parámetros IP.

restantes (los que aparecen más a la derecha en la máscara).

La dirección de red será, por tanto:  
 $192.168.15.00000000 = 192.168.15.0$

Lo que a veces se especifica simplemente como 192.168.15.0 o más sencillamente como 192.168.15.

Continúa...



## Caso práctico 2

...Continuación

### Cálculo de la dirección de difusión o broadcast de la red

Esta dirección se utiliza cuando un nodo quiere enviar datos a todos los nodos de su red lógica (todos los que comparten su sistema de direccionamiento y con los que él puede comunicarse directamente sin el concurso de dispositivos intermediarios).

La dirección de difusión de red se calcula también a partir de la dirección IP del nodo, dejando intactos los bits que codifican la red y estableciendo a uno los bits que codifican el host dentro de la red.

En el caso que nos ocupa la dirección de difusión será:  $192.168.15.11111111 = 192.168.15.255$ .

Nótese que ni la dirección de red ni la de difusión pueden aplicarse a un nodo, puesto que están reservadas para esas dos funciones especiales: representar a la red (dirección de red) y representar a todos los nodos de la red (dirección de difusión).

### Comprobación de que el nodo se comunica con su puerta por defecto

Al configurar la red en un nodo hay que asegurarse de que, si tiene establecida su puerta por defecto, el nodo está en la misma red lógica que su puerta, de lo contrario no se podrán comunicar entre sí.

¿Cómo saber si están en la misma red dos nodos? Es muy sencillo: calculamos la dirección de red del primer nodo, calculamos la dirección de red del segundo nodo y comprobamos que coinciden.

Si realizamos al cálculo de la dirección de red de la puerta por defecto del nodo (encaminador) siguiendo el procedimiento descrito anteriormente se tendrá lo siguiente:

Dirección de red del encaminador:  
 $192.168.15.00000000 = 192.168.15.0$

Que coincide con la dirección de red de nodo, por tanto, están en la misma red y el nodo podrá comunicarse con su puerta.

### B. Subnetting

A veces interesa que la división que produce una máscara de red entre la parte de nodo y la parte de red no sea tan generosa como la que proporcionan las redes de clases (A, B y C; las direcciones de tipo D y E no intervienen en este estudio).

Por ejemplo, podría darse el caso de una empresa que ha contratado una red con direcciones IP públicas de clase C para repartir entre todos los departamentos de que consta.

Por tanto, el administrador de red de esta empresa tiene que hacer una subdivisión del direccionamiento IP de la red de clase C contratada, confeccionando a partir de esta un conjunto de redes más pequeñas y asignando cada una de ellas a los distintos departamentos. A esta operación de fraccionamiento del sistema de direccionamiento se le llama **subnetting**.

La técnica de subnetting consiste en crear máscaras de mayor número de bits puestos a uno que las que proporcionan las máscaras de clase (8, 16 y 24 bits respectivamente para las clases A, B y C).

Esta división genera un conjunto de subredes, cada una de las cuales tiene su propio sistema de direccionamiento, su nueva máscara, su dirección de red y su dirección de difusión. A partir de aquí se aprenderá a realizar estos cálculos.

Para ilustrarlo se supondrá que disponemos de las direcciones IP de la red de clase C 192.168.15.0 que tendremos que repartir en tres subrangos de red, por ejemplo, porque haya tres departamentos. A cada departamento le asignaremos una de estas subredes.

### Cálculo de tres parámetros: número de bits que desplazaremos en la máscara, nueva máscara de subred (máscara adaptada) y número de subredes que conseguiremos con la división

Como partimos de una red de clase C, tomamos inicialmente una máscara de 24 bits, es decir:

$255.255.255.00000000$

Nos hacemos la siguiente pregunta: ¿Cuántos bits de los 8 que aparecen a la derecha de la máscara anterior tendrían que convertirse en unos para poder codificar tres subredes?

Esta pregunta exige el siguiente cálculo: tomar un número de bits (entre 2 y 6 para una red de clase C), elevar 2 a ese número y restarle 2 al resultado, es decir:

$$\text{Número de subredes válidas} = 2^{\text{Número de bits desplazados}} - 2$$

Para una red de clase B, el número de bits desplazados debe estar comprendido entre 2 y 14, mientras que para una red de clase C entre 2 y 22. La justificación de estos cálculos se comprobará más adelante.

En nuestro ejemplo, si elegimos 3 bits, tendremos que el número de subredes válidas será de  $23 - 2 = 8 - 2 = 6$  subredes válidas.

Con 6 subredes válidas se pueden cubrir los tres departamentos y nos sobran otras tres subredes para usos futuros.

Continúa...



## Caso práctico 2

...Continuación

Nota: Se puede comprobar que con 2 bits no hubiéramos tenido suficiente, puesto que en este caso el número de redes válidas que saldrían serían:  $2^2 - 2 = 4 - 2 = 2$  (un departamento de los tres que tenemos se quedaría sin su propia subred).

Por tanto, el número de bits desplazados que hemos calculado es 3 y el número de subredes válidas en que podremos subdividir la red será de 6.

La nueva máscara de subred o máscara adaptada será 255.255.255.11100000 = **255.255.255.224**.

### Cálculo del número hosts que pueden direccionarse en cada subred

En este caso el cálculo del número de hosts válidos en cada subred es similar al de subredes, pero en vez de tomar el número de bits desplazados se toman los restantes.

Para una red de clase C:  $2^{8-3} - 2 = 2^5 - 2 = 32 - 2 = 30$  hosts/subred.

Para una red de clase B:  $2^{16-3} - 2 = 2^{13} - 2 = 8192 - 2 = 8190$  hosts/subred.

Para una red de clase A:  $2^{24-3} - 2 = 2^{21} - 2 = 2097152 - 2 = 2097150$  hosts/subred.

Por tanto, en nuestro ejemplo, el número de hosts válidos en cada subred será de

Número de hosts válidos en cada subred =  $2^{8-3} - 2 = 2^5 - 2 = 32 - 2 = 30$  hosts/subred.

### Cálculo de las direcciones de red de cada subred válida

Hemos desplazado 3 bits, que ahora codifican la subred, por tanto, tenemos lo siguiente:

- a) Los 24 primeros bits codifican la red: 192.168.15.
- b) Los 3 bits siguientes codifican la subred: desde la 000 hasta la 111 (8 subredes, de las cuales solo 6 serán válidas). Ni la primera subred ni la última son válidas (lo que justificaremos más adelante).
- c) Los 5 bits siguientes (y últimos) codifican el host dentro de la red: desde el 00000 hasta el 11111 (32 hosts en cada subred, de los cuales solo 30 son válidos). Ni el primer host ni el último son válidos (también será justificado más adelante).

¿Cuáles serán las direcciones de red de cada una de las subredes válidas?

Ponemos a cero los cinco bits de host, que aparecerán a la derecha del símbolo «,» que utilizaremos para separar los bits del último octeto:

- 1) Dirección de red de la primera subred:  
192.168.15.000,00000 = 192.168.15.0 (no válida, puesto que coincide con la dirección de red de la red de clase C de la que partimos y si la tomamos no podremos distinguir entre la dirección de red de la clase C y de la primera subred): la descartamos.
- 2) Dirección de red de la segunda subred:  
192.168.15.001,00000 = 192.168.15.32 (dirección de subred del primer departamento).
- 3) Dirección de red de la tercera subred:  
192.168.15.010,00000 = 192.168.15.64 (dirección de red del segundo departamento).
- 4) Dirección de red de la cuarta subred:  
192.168.15.011,00000 = 192.168.15.96 (dirección de red del tercer departamento).
- 5) Dirección de red de la quinta subred:  
192.168.15.100,00000 = 192.168.15.128.
- 6) Dirección de red de la sexta subred:  
192.168.15.101,00000 = 192.168.15.160.
- 7) Dirección de red de la séptima subred:  
192.168.15.110,00000 = 192.168.15.192.
- 8) Dirección de red de la octava subred:  
192.168.15.111,00000 = 192.168.15.224 (esta subred también es inválida, pero la razón se expondrá después).

### Cálculo de las direcciones de difusión de cada subred válida

Hacemos lo mismo que en el apartado anterior, pero poniendo esta vez a uno los bits que codifican el host.

- 1) Dirección de difusión de la primera subred:  
192.168.15.000,11111 = 192.168.15.31 (aunque sabemos que esta subred no sirve porque no es válida su dirección de red).
- 2) Dirección de difusión de la segunda subred:  
192.168.15.001,11111 = 192.168.15.63 (dirección de difusión del primer departamento).
- 3) Dirección de difusión de la tercera subred:  
192.168.15.010,11111 = 192.168.15.95 (dirección de difusión del segundo departamento).
- 4) Dirección de difusión de la cuarta subred:  
192.168.15.011,11111 = 192.168.15.127 (dirección de red del tercer departamento).
- 5) Dirección de difusión de la quinta subred:  
192.168.15.100,11111 = 192.168.15.159.
- 6) Dirección de difusión de la sexta subred:  
192.168.15.101,11111 = 192.168.15.191.

Continúa...



### Caso práctico 2

...Continuación

7) Dirección de difusión de la séptima subred:

$$192.168.15.110,11111 = 192.168.15.223.$$

8) Dirección de difusión de la octava subred:

$192.168.15.111,11111 = 192.168.15.255$  (esta subred también es inválida, porque su dirección de difusión coincide con la dirección de difusión de la red de clase C de la que partimos).

#### Cálculo de las direcciones IP de los nodos de cada una de las subredes válidas

Si tomamos una subred válida, por ejemplo, la primera de todas las válidas, las direcciones IP asignables a los nodos del primer departamento estarán comprendidas entre su dirección de red y la de difusión.

Por tanto, tendremos:

Primera red válida: desde 192.168.15.33 hasta 192.168.15.62 (30 nodos para el primer departamento).

Segunda red válida: desde 192.168.15.65 hasta 192.168.15.94 (30 nodos para el segundo departamento).

Tercera red válida: desde 192.168.15.97 hasta 192.168.15.126 (30 nodos para el tercer departamento).

Cuarta red válida: desde 192.168.15.129 hasta 192.168.15.158.

Quinta red válida: desde 192.168.15.161 hasta 192.168.15.190.

Sexta y última red válida: desde 192.168.15.193 hasta 192.168.15.222.

Como se ve ahora solo podemos aprovechar  $6 \times 30 = 180$  direcciones de las 256 que tenía el rango original de la red de clase C: la pérdida de direcciones IP es el precio que hay que pagar por subdividir la red.

La Fig. 3.23 proporciona un esquema gráfico de la configuración de algunos nodos de cada departamento.

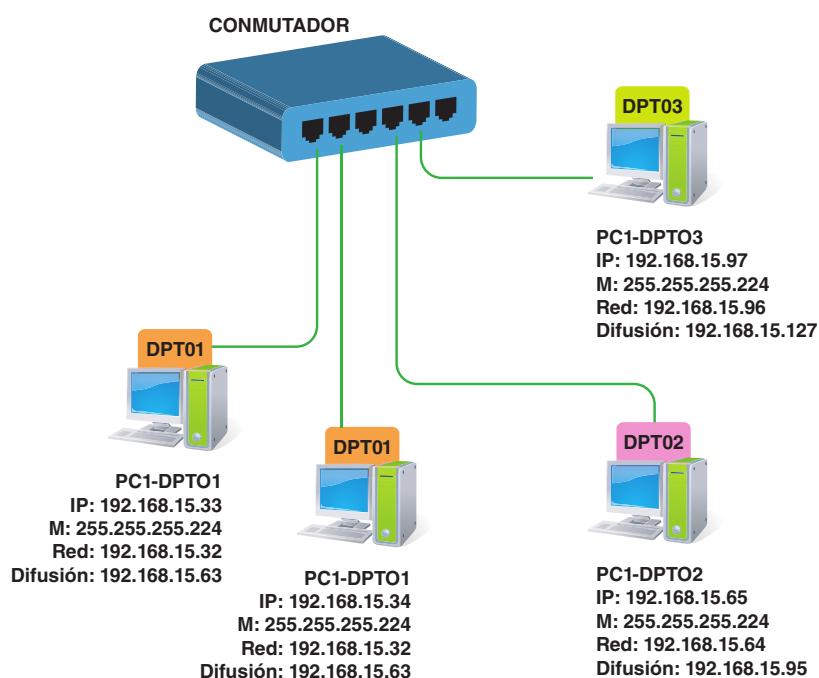
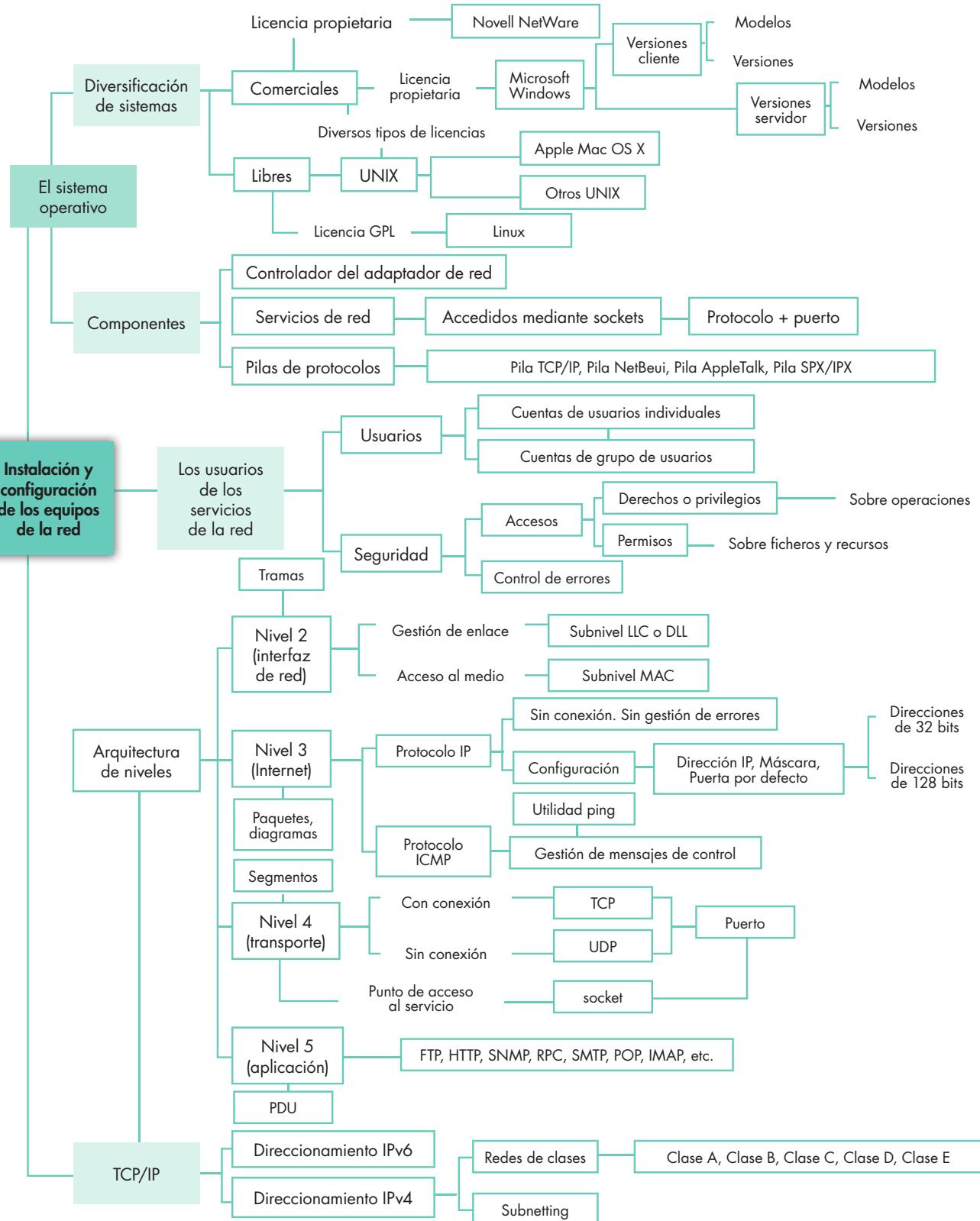


Fig. 3.23. Parámetros de red de los nodos de cada departamento.



## Síntesis





## Test de repaso

**1.** Enlaza los siguientes elementos característicos de distintos tipos de sistemas operativos de red (hay varias posibilidades en las columnas segunda y tercera):

a) Windows 7	1) Apple	i) Sistema propietario
b) Ubuntu	2) Licencia GPL	ii) Sistema gratuito
c) Fedora	3) Microsoft	iii) NetBeui
d) Mac OS X	4) Linux	iv) TCP/IP
e) Netware	5) Novell	v) SPX/IPX

**2.** El controlador de una interfaz de red (tarjeta de red) es:

- a) hardware.
- b) software.
- c) firmware.
- d) netware.

**3.** Asocia los siguientes protocolos a sus equivalentes capas de red en el modelo TCP/IP

a) IP	1) Internet
b) TCP	2) Transporte
c) UDP	3) Aplicación
d) FTP	4) Interfaz de red

**4.** Un socket es la asociación de:

- a) Un protocolo y un número de puerto.
- b) Un protocolo y una interfaz de red.
- c) Un puerto y una interfaz de red.
- d) Dos puertos.

**5.** Asocia las siguientes direcciones IP con sus correspondientes clases:

a) 10.3.1.15	1) Clase C
b) 130.15.1.4	2) Clase B
c) 195.67.100.5	3) Difusión
d) 224.0.0.30	4) Clase A

**6.** El protocolo ARP sirve para:

- a) Averiguar mediante ping si una máquina remota está activa.
- b) Resolver los nombres de las máquinas en sus correspondientes direcciones IP.
- c) Resolver las direcciones IP en sus correspondientes direcciones físicas.

d) Comprobar si la tarjeta de red de un equipo funciona correctamente.

**7.** ¿Cuál es la máscara de red de un nodo cuya red viene especificada por 192.168.15.1/27?

- a) 255.255.255.0.
- b) 255.255.255.224.
- c) 155.155.0.0.
- d) 255.255.240.0.

**8.** Enlaza los siguientes elementos característicos de distintos tipos de protocolos de alto nivel:

a) SMTP	1) Transferencia de ficheros
b) HTTP	2) Diálogo entre aplicaciones
c) FTP	3) Navegación web
d) RPC	4) Intercambio de mensajes de correo

**9.** Enlaza los siguientes elementos característicos sobre las utilidades básicas de red:

a) ping	1) Gestión de la tabla de direcciones físicas
b) arp	2) Configuración de la red en Windows
c) ipconfig	3) Información sobre el estado de la red
d) iwconfig	4) Gestión de rutas
e) netstat	5) Pruebas sobre el estado activo de las máquinas de la red
f) route	6) Visualización de los saltos que un paquete da en la red hasta llegar a su destino
g) tracert	7) Configuración de la red inalámbrica en GNU/Linux

**10.** El protocolo ssh cifra las conexiones que realiza para mejorar la seguridad y sustituye a la utilidad más antigua e insegura siguiente:

- a) rpc.
- b) telnet.
- c) traceroute.
- d) route.

**Solución:** 1: c-3-(i), iii) y iv), b-(2 y 4)-(ii) y iv), d-1-(i) y iv), 2: b, 3: a-1, b-2, c-2, d-3 (no hay ningún protocolo de la capa de interfaz de red). 4: a, 5: a-4, b-2, c-1, d-3. 6: c, 7: b.



## Comprueba tu aprendizaje

### I. Identificar los protocolos y servicios de red disponibles en los sistemas operativos

1. Indica si son verdaderas o falsas las siguientes afirmaciones:
  - a) El Unix con marca comercial Mac OS X puede ejecutar AppleTalk como protocolo nativo.
  - b) AppleTalk no es compatible con TCP/IP en un sistema Mac OS X.
  - c) Microsoft Windows no puede ejecutar TCP/IP.
  - d) Linux solo puede ejecutar TCP/IP.
  - e) Los sistemas Linux y los sistemas Windows pueden comunicarse a través de TCP/IP.

2. En la tabla siguiente, relaciona los elementos de la izquierda (protocolos) con los de la derecha (servicios).

1. POP	a) Sesión de terminal remoto
2. FTP	b) Discos e impresoras
3. IMAP	c) Intercambio de ficheros
4. SMTP	d) Correo electrónico
5. NetBIOS	
6. Telnet	

3. ¿Pueden convivir los protocolos NetBeui y TCP/IP sobre la misma red? ¿Por qué?

¿Pueden convivir los protocolos NetBeui y TCP/IP sobre la misma tarjeta de red? ¿Depende de la tarjeta de red o del sistema operativo?

4. Desde las páginas de ayuda de los sistemas operativos Windows y Linux, investiga si ya pueden incorporar la nueva versión del protocolo IP denominada IPv6. Déjate conducir por sus guías de usuario para instalar —en aquellos casos en que se permita— la ampliación del protocolo IPv4 (el que se ha estudiado en esta unidad) con IPv6. También puedes encontrar información a través de los buscadores de Internet por las voces «instalar ipv6» y en la sede web de los fabricantes de sistemas.

5. Prepara unos ordenadores en red que tengan como sistema operativo alguna versión de Windows. Después sigue los siguientes pasos:

- a) Asegúrate de que cada PC tiene un nombre distinto que le identifique únicamente. Además todos deben pertenecer al mismo grupo o dominio NetBIOS. Tanto el nombre como el grupo al que pertenecen se pueden configurar desde las Propiedades de «Mi PC» (en algunas versiones de Windows, «Mi Equipo»).
- b) No es necesario que estos PC ejecuten el protocolo TCP/IP, basta con que corran NetBeui, pero si tienen TCP/IP asegúrate de que todos comparten el mismo sistema de direccionamiento.

c) Ahora abre el explorador de Windows y vete desde él a «Mis sitios de red». Investiga en las subcarpetas de la red y verás todos los servicios compartidos a la red que tienen los PC del grupo a través de NetBIOS. Ten en cuenta que solo verás aquellos servicios para los que tengas derecho desde tu cuenta de acceso a la red.

### II. Utilizar las herramientas básicas para la gestión de protocolos de red

6. Analiza si son verdaderas o falsas las siguientes afirmaciones:

- a) Una tarjeta de red que tenga instalada la pila TCP/IP no puede instalar la pila SPX/IPX.
- b) Un redirector de red proporciona la interfaz de conexión de servicios a través de varias pilas de protocolos.
- c) NetBIOS no se puede utilizar con TCP/IP, solo puede convivir con protocolos de Microsoft.
- d) Un servicio de disco remoto puede ser alcanzable desde el mismo cliente mediante varios protocolos.
- e) Una impresora remota solo puede admitir conexiones mediante un único protocolo de conexión.

7. Elige un nodo en Internet que tenga respuesta a la orden ping (te puede servir [www.google.com](http://www.google.com)). Ejecuta ping contra ese nodo y fíjate en el tiempo de respuesta de cada ping realizado. Calcula una media entre todos ellos.

Ahora ejecuta el ping con el calificador «-l» que acepta como argumento un número entero entre 0 y 65500 que indica el número de bytes que se enviarán con cada orden ping. La orden tendrá el aspecto siguiente: «ping -l 1000 [www.google.com](http://www.google.com)»

Ejecuta este ping con 1000, 5000, 10000 y 20000. Mide las medias de todas estas ejecuciones y exprésalas en una gráfica. Observarás cómo a medida que la orden ping genera más tráfico, empezarás a notar una congestión en tu línea de acceso a Internet.

8. Selecciona un grupo de servidores web en Internet. Te puede servir cualquier servidor que puedas localizar en Internet. Ahora ejecuta un comando tracert desde tu PC local hacia esos servidores en Internet. Contesta el número de saltos que deben dar los paquetes que envías. Se puede definir una métrica contando el número de saltos hasta alcanzar el destino. Así, por ejemplo, si el tracert a un servidor concreto genera 7 saltos, diremos que el servidor está a una «longitud de red» de 7 saltos del cliente. Ordena ahora los servidores de menor a mayor distancia de red según esa métrica.



## Comprueba tu aprendizaje

### III. Configurar el sistema de direccionamiento de los equipos de la red

9. Analiza si son verdaderas o falsas las siguientes afirmaciones:
- Las direcciones IP son series numéricicas binarias de 32 bits.
  - Todos los ceros y unos de una dirección IP deben estar contiguos.
  - Todos los ceros y unos de una máscara de red deben estar contiguos.
  - Los ceros siempre van antes que los unos en una máscara de red.
  - Hay tres clases de subredes IP.
  - Un CIDR de /24 es lo mismo que una clase C.
  - Un CIDR de /24 admite más nodos que un CIDR de /16.
10. Selecciona dos PC en tu laboratorio: uno con sistema operativo Windows y otro con alguna versión de Linux. Realiza ahora las siguientes actividades:
- Elige una dirección de red para cada uno de ellos y una máscara de modo que los dos puedan comunicarse en la misma red.
  - Prueba que tienen comunicación recíproca mediante ping desde uno y otro PC.
  - ¿Qué utilidades puedes utilizar para comprobar que se comunican entre sí?
  - Ejecuta un tracert desde uno al otro. ¿Cuántos saltos ves en el tracert realizado?

11. Toma dos PC con sistema operativo Linux y Windows respectivamente. Asegúrate de que el PC Linux tiene instalado un servidor Telnet o al menos puede aceptar conexiones interactivas remotas de terminal. Ahora ejecuta las siguientes acciones:

- Examina los dos PC y apunta las direcciones IP de cada uno de ellos. Asegúrate de que están en la misma red IP para que puedan tener comunicación entre ellos.
  - Ejecuta desde el PC Windows un Telnet hacia el PC Linux. Si tienes Windows Vista tendrás que instalar previamente un cliente Telnet equivalente (puede servirte PuTTY). Comprueba que puedes crear sesiones remotas.
  - Crea algunos ficheros en el PC Linux utilizando esa sesión remota y luego comprueba desde la consola local del PC Linux que efectivamente se crearon.
  - Ejecuta el comando de apagado del sistema Linux desde la consola remota en el PC Windows. Observarás que el PC Linux se apaga. ¿Qué ocurre con la conexión Telnet? ¿Por qué? ¿Puedes encender remotamente el PC Linux desde el PC Windows?
12. Una empresa quiere fraccionar su sistema de direccionamiento de red en cinco subredes. La dirección de red de la que se parte es 192.168.3.0/24.
- ¿Cuáles son los parámetros de red que hay que configurar en el tercer PC de la primera subred válida?
  - ¿Cuál es la dirección de difusión de la tercera subred válida?
  - ¿Cuál es la dirección de red de la segunda subred válida?