Unidad de Trabajo 7

Implantación de redes de área local

En esta unidad de trabajo haremos uso de los conceptos abstractos aparecidos anteriormente. Los aplicaremos al diseño de redes de área local reales, construidas a partir de conjuntos de especificaciones sobre necesidades, usos o aplicaciones concretas que puedan darse en organizaciones que necesiten este tipo de tecnología. En este sentido, realizaremos un estudio desde dos puntos de vista: el hardware propio de una red de área local y el software que se debe instalar en los sistemas operativos de los hosts de la red, así como en las máquinas especializadas de red que son necesarias para brindar los diversos servicios requeridos por los distintos usuarios de la red.

1 Conceptos previos

En esta sección definiremos algunos conceptos de utilidad para el resto de la unidad de trabajo. Haremos hincapié en los sistemas operativos de red.

1.1 El sistema operativo de red

El sistema operativo de red o NOS (Network Operating System) es el software que hace que un sistema informático pueda comunicarse con otros equipos constituyendo una red. A veces el software de red viene integrado con el sistema operativo, sin embargo, otros sistemas operativos menos avanzados necesitan una instalación añadida.

1.2 Evolución de los NOS

Los sistemas operativos de red han evolucionado significativamente desde que se crearon las primeras redes de área local. Sintetizaremos esta evolución poniendo como ejemplo equipos con sistema operativo DOS en las siguientes etapas, no necesariamente cronológicas:

- **Etapa inicial**. Antes de que hubiera necesidad de conectar los PC en red para enviar grandes volúmenes de datos, eran posibles las comunicaciones a través de los puertos serie del PC, utilizando software específico para ello. Comercialmente, a estos programas se les llama programas de comunicaciones, que se compraban como productos añadidos que debían instalarse sobre el DOS.

- **Integración de los programas de comunicaciones en el DOS**. En las versiones avanzadas del DOS se integraron los programas de comunicaciones en el propio sistema operativo, de modo que los usuarios podían hacer transferencias de ficheros a través de líneas serie sin necesidad de adquirir productos añadidos. Es el caso de las utilidades «interlink-interserver» del DOS.

- **Software de red añadido**. En esta etapa se requieren productos de red que deben instalarse sobre el DOS o sobre Windows (versión 3.1) para interactuar con otros nodos utilizando un adaptador de red. Es el caso de las redes Novell, Lantastic, etcétera.

- Software de red integrado con el sistema operativo. Esta última etapa se caracteriza por la integración de todo el software en el ámbito del sistema operativo: no es necesaria la instalación de software especial sobre el sistema operativo, pues éste incorpora todo lo necesario. Este es el caso de Windows 9X/NT/2k, MacOS, etc.

1.3 Concepto de grupo de trabajo de red

La mayor parte de los sistemas operativos de red gestionan los recursos formando grupos con ellos, de modo que se facilita su búsqueda a los usuarios. El concepto de grupo de trabajo ha evolucionado mucho, extendiéndose a la idea de trabajo colaborativo, flujo de trabajo (*workflow*), etc. La acepción que a nosotros nos interesa es la de *agrupación de recursos.*

1.4 Concepto de dominio de red

El dominio en una red es una extensión del concepto de grupo de trabajo, pero a este concepto se le añaden otros aspectos, como el de la **centralización de la gestión de red**, **facilidad para la administración de los equipos**, **control de usuarios y contraseñas**, **jerarquización de los recursos**, etc.

Cuando se utiliza el término dominio en comunicaciones, hay que especificar claramente a qué nos referimos, puesto que es un concepto ambiguo: cada tecnología de red tiene un concepto distinto, aunque las características que subyacen son las mencionadas anteriormente.

2 El hardware de las LAN

Vamos a estudiar los elementos de hardware específicos en la construcción de una red de área local. Los sistemas de cableado ya han sido explicados anteriormente y no volveremos a incidir sobre ellos, salvo cuando procedamos a diseñar redes concretas, y siempre en relación con el hardware que veremos en esta parte.

2.1 Los adaptadores de red

Un adaptador o tarjeta de red es el elemento fundamental en la composición de la parte física de una red de área local. Cada adaptador de red es un interface hardware entre la plataforma o sistema informático y el medio de transmisión físico por el que se transporta la información de un lugar a otro.

El adaptador puede venir incorporado o no con la plataforma hardware del sistema. En gran parte de los ordenadores personales hay que añadir una tarjeta separada, independiente del sistema, para realizar la función de adaptador de red. Esta tarjeta se inserta en el bus de comunicaciones del ordenador personal convenientemente configurada. En otros sistemas, el hardware propio del equipo ya incorpora el adaptador de red. No obstante, un equipo puede tener una o más tarjetas de red para permitir distintas configuraciones o poder atacar con el mismo equipo distintas redes.

2.1.1 Descripción y conexión del adaptador

Una tarjeta de red es un dispositivo electrónico que consta de las siguientes partes:

- Interface de conexión al bus del ordenador.
- Interface de conexión al medio de transmisión.
- Componentes electrónicos internos, propios de la tarjeta.
- Elementos de configuración de la tarjeta: puentes, conmutadores, etc.

La conexión de la tarjeta de red al hardware del sistema sobre el que se soporta el host de comunicaciones se realiza a través del interface de conexión. Cada ordenador transfiere internamente la información entre los distintos componentes (CPU, memoria, periféricos) en paralelo a través de un bus interno. Los distintos componentes, especialmente los periféricos y las tarjetas, se unen a este bus a través de una serie de conectores, llamados slots de conexión, que siguen unas especificaciones concretas.

Por tanto, un slot es el conector físico en donde se «pincha» la tarjeta, por ejemplo, el adaptador de red. Es imprescindible que la especificación del slot de conexión coincida con la especificación del interface de la tarjeta.

La velocidad de transmisión del slot, es decir, del bus interno del ordenador, y el número de bits que es capaz de transmitir en paralelo, serán los primeros factores que influirán decisivamente en el rendimiento de la tarjeta en su conexión con el procesador central.

Bus	**Características técnicas**	**Observaciones**
ISA	Bus de 16 bits, 8 Mhz y 8 Mbps	*Industry Standard Architecture*
EISA	Bus de 32 bits, 8,5 Mhz y 33 Mbps	*Extended Industry Estándar Architecture*
MCA	Bus de 32 bits, 10 Mhz y 40 Mbps	*MicroChannel Architecture*. Propio de los PS/2 de IBM
NUBUS	Bus de 32 bits	Propio de algunos ordenadores de Apple
VESA LOCAL BUS	Bus de 32 bits, 33 Mhz y 132 Mbps	En desaparición
PCI	Bus de 32 bits, 40 Mhz y 120 Mbps	*Peripheral Component Interconnect* Este es el estándar que mejor se está implantando en el mercado

La tecnología más consolidada para PC compatibles es ISA, aunque debido a su bajo rendimiento ha sido sustituida por la tecnología PCI, que está implantada en la mayor parte de las plataformas modernas. Las tarjetas ISA son apropiadas si las necesidades de transmisión no son muy elevadas, por ejemplo, para ordenadores que se conecten a través de una Ethernet a 10 Mbps sin demasiadas exigencias de flujo de información. En el caso de que sean necesarias velocidades de transmisión más altas, es recomendable la tecnología PCI. El resto de las tecnologías no están tan extendidas, por lo que no nos detendremos en ellas.

En el mercado existen muchos tipos de tarjetas de red, cada una de las cuales necesita su controlador de software para comunicarse con el sistema operativo del host. Hay firmas comerciales poseedoras de sus propios sistemas operativos de red que tienen muy optimizados estos controladores. Esto hace que muchas tarjetas de red de otros fabricantes construyan sus tarjetas de acuerdo con los estándares de estos fabricantes mayoritarios, de modo que las tarjetas se agrupan por el tipo de controlador que soportan. Por ejemplo, las tarjetas NE2000 de la casa Novell constituyen un estándar de facto seguido por otros muchos fabricantes que utilizan su mismo software.

En general, es conveniente adquirir la tarjeta de red asegurándose de que existirán los controladores apropiados para esa tarjeta y para el sistema operativo del host en el que se vaya a instalar. Además, hay que asegurarse de que se tendrá un soporte técnico para solucionar los posibles problemas de configuración o de actualización de los controladores con el paso del tiempo, tanto de los sistemas operativos de red como de las mismas redes.

Los componentes electrónicos incorporados en la tarjeta de red se encargan de gestionar la transferencia de datos entre el bus del ordenador y el medio de transmisión, así como del proceso de los mismos.

La salida hacia el cable de red requiere un interface de conectores especiales para red, como los que se han visto en la unidad de trabajo anterior: BNC, RJ45, DB 15, etc., dependiendo de la tecnología de la red y del cable que se deba utilizar. Normalmente, la tarjeta de red debe procesar la información que le llega procedente del bus del ordenador para producir una señalización adecuada al medio de transmisión, por ejemplo, una modulación, un empaquetamiento de datos, un análisis de errores, etc.

2.1.2 Configuración de la tarjeta de red

La tarjeta de red debe ponerse de acuerdo con el sistema operativo del host y su hardware en el modo en el que se producirá la comunicación entre ordenador y tarjeta. Esta configuración se rige por una serie de parámetros que deben ser determinados en la tarjeta en función del hardware y software del sistema, de modo que no colisionen con los parámetros de otros periféricos o tarjetas. Los principales parámetros son:

- **IRQ, interrupción**. Es el número de una línea de interrupción con el que se avisan sistema y tarjeta de que se producirá un evento de comunicación entre ellos. Por ejemplo, cuando la tarjeta recibe una trama de datos, ésta es procesada y analizada por la tarjeta, activando su línea IRQ, que le identifica unívocamente, para avisar al procesador central que tiene datos preparados para el sistema. Valores típicos para el IRQ son 3, 5, 7, 9 y 11.

- **Dirección de E/S**. Es una dirección de memoria en la que escriben y leen el procesador central del sistema y la tarjeta, de modo que les sirve de bloque de memoria para el intercambio mutuo de datos. Tamaños típicos de este bloque de memoria (o buffer) son 16 ó 32 Kbytes. Este sistema de intercambio de datos entre el host y la tarjeta es bastante rápido, por lo que es muy utilizado en la actualidad, pero necesita procesadores más eficientes. La dirección de E/S se suele expresar en hexadecimal, por ejemplo, DC000H.

- **DMA, acceso directo a memoria**. Cuando un periférico o tarjeta necesita transmitir datos a la memoria central, un controlador hardware apropiado llamado controlador DMA pone de acuerdo a la memoria y a la tarjeta sobre los parámetros en que se producirá el envío de datos, sin necesidad de que intervenga la CPU en el proceso de transferencia. Cuando un adaptador de red transmite datos al sistema por esta técnica (DMA), debe definir qué canal de DMA va a utilizar, y que no vaya a ser utilizado por otra tarjeta. Este sistema de transferencia se utiliza poco en las tarjetas modernas.

- **Dirección del puerto de E/S**. El puerto de Entrada/Salida es un conjunto de bytes de memoria en los que procesador central y periféricos intercambian datos de Entrada/Salida y del estado en el que se efectúan las operaciones.

- **Tipo de transceptor**. Algunas tarjetas de red incorporan varias salidas con diversos conectores, de modo que se puede escoger entre ellos en función de las necesidades. Algunas de estas salidas necesitan transceptor externo y hay que indicárselo a la tarjeta cuando se configura.

Tradicionalmente, estos parámetros se configuraban en la tarjeta a través de puentes (*jumpers*) y conmutadores (*switches*). Actualmente está muy extendido el modo de configuración por software, que no requiere la manipulación interna del hardware: los parámetros son guardados por el programa configurador que se suministra con la tarjeta en una memoria no volátil que reside en la propia tarjeta.

Algunas tarjetas de red incorporan un zócalo para la inserción de un chip que contiene una memoria ROM (de sólo lectura) con un programa de petición del sistema operativo del host a través de la red. De este modo, el host puede cargar su sistema operativo remotamente.

En la última generación de tarjetas, la configuración se realiza de manera automática: elección del tipo de conector, parámetros de comunicación con el sistema, etc.. aunque requiere hardware especializado en el host. Esta tecnología de autoconfiguración se llama Plug & Play (enchufar y funcionar) aunque hay quién relaciona sus siglas con Plug & Pray (enchufar y rezar).

2.1.3 Características de las tarjetas de red

No todos los adaptadores de red sirven para todas las redes. Existen tarjetas apropiadas para cada tecnología de red: Ethernet, Token Ring, FDDI, etc.

Además, algunas tarjetas que sirven para el mismo tipo de red tienen parámetros de acuerdo con ciertas especificaciones. Por ejemplo, una tarjeta Ethernet puede estar configurada para transmitir a 10 Mbps o a 100 Mbps (Fast Ethernet), dependiendo del tipo de red Ethernet a la que se vaya a conectar. También se puede elegir el tipo de conexión: 10Base2, 10Base5, 10BaseT, 100BaseT, etc.

Algunos adaptadores de red no se conectan directamente al bus de comunicaciones interno del ordenador, sino que lo hacen a través de otros puertos de comunicaciones serie o paralelo. Requieren controladores especiales para su correcto funcionamiento y su rendimiento no es tan alto como en las tarjetas conectadas al bus.

2.2 Las estaciones de trabajo

Las estaciones de trabajo o *workstations* son los nodos de la red desde los que actúan los usuarios de la red. Estos ordenadores no tienen una función específica predeterminada. Su misión fundamental, desde el punto de vista que a nosotros nos ocupa, es la de proporcionar a los usuarios el acceso a los servicios de la red.

En cuanto a las aplicaciones, fundamentalmente actúan como clientes, aunque no se excluye que algunas estaciones puedan proveer algún tipo de servicio. Cada estación es un sistema informático completo al que se le pueden añadir aplicaciones de usuario, sin embargo, el acceso por red completa su funcionalidad.

Todos los ordenadores de propósito general pueden actuar como una estación de trabajo cliente en una red, sin embargo, las cualidades más apreciadas en una estación de trabajo son las siguientes:

- **Potencia de proceso**. La potencia puede ser baja, media o alta. Una estación de baja potencia es un punto de acceso a los servicios de la red en la que no es necesaria la ejecución de aplicaciones de usuario.

- **Subsistema gráfico**. En la mayor parte de las estaciones de trabajo se exige que el subsistema gráfico del ordenador sea potente, ya que está en contacto directo con el usuario. Esto no es imprescindible en el caso de un servidor, ya que éste se caracteriza por el servicio que provee, que no es de gráficos. Por tanto, interesa que las tarjetas gráficas de una estación de trabajo gráfica sean de alto rendimiento en función de las aplicaciones de usuario que se han de ejecutar.

- **Conectividad a red**. No todas las estaciones tienen las mismas necesidades de intercambio de datos con otros ordenadores de la red. Las estaciones de trabajo están pensadas para interactuar en una red, por lo que es frecuente que los adaptadores de red de las estaciones de trabajo sean potentes, especialmente si se prevé que el intercambio de datos sea masivo.

- **Capacidad de almacenamiento en disco**. Hay estaciones de trabajo con disco duro y sin él. Si una estación de trabajo carece de disco, es porque su sistema operativo debe ser descargado desde algún servidor a través de la red, proceso que se estudiará más adelante. No obstante, lo más común es que las estaciones tengan discos duros que contienen su sistema operativo, datos de usuarios y las aplicaciones de éstos. Desde el punto de vista del sistema, es importante que las estaciones tengan disco, especialmente si el sistema utiliza memoria paginada virtual, que requiere intercambios frecuentes y masivos entre disco y memoria. Si el disco sobre el que se pagina está al otro lado de la red, se ralentizarán estos procesos y se sobrecargará el tráfico de red. Las estaciones sin disco se utilizan para aplicaciones muy específicas o para evitar entradas no controladas de datos o programas a la red. Por ejemplo, si ninguna estación de la red tiene discos ni disquetes, es imposible la introducción local de virus informáticos en la red.

Por ejemplo, puede hacer las funciones de estación de trabajo de baja potencia un ordenador personal basado en 80386/486, con poca memoria (1-4 Mbytes), conectado en red con un adaptador de 8/16 bits ISA, para intercambio de datos entre el exterior y algún servidor de la red.

Una estación de potencia media podría estar constituida por un ordenador personal Pentium, 8/16 Mbytes de memoria RAM, conectado en red con un adaptador de 16 bits ISA, para ejecutar aplicaciones de usuario que necesitan intercambio de datos con un servidor, por ejemplo, un paquete ofimático integrado.

Una estación de alta potencia estaría constituida por un procesador Pentium Pro/II/III o PowerPC, con 64-256 Mbytes de memoria RAM, conectada en red a través de un adaptador de alto rendimiento (tarjeta PCI de 32 bits) 100BaseT, especializada en ejecutar aplicaciones sofisticadas de cálculo.

2.3 Servidores de red

Los servidores de red son nodos de la red especializados en brindar servicios al resto de los nodos de la red. Existen muchos tipos posibles de servicios, pero los más comunes son los de discos y ficheros, impresoras y comunicaciones. Un servidor queda definido por el tipo de servicio que provee. No hay que asociar un hardware servidor con un servicio concreto en todos los casos, puesto que el mismo hardware servidor puede ocuparse de distintos tipos de servicios. Así, por ejemplo, un servidor de red puede brindar servicios de discos e impresoras simultáneamente. Además, podría tener un módem que sirviera al resto de los nodos (estaciones clientes) de la red.

Las características fundamentales que deben ser consideradas en el diseño de un servidor son las siguientes:

Potencia de proceso. Los servidores tienen una exigencia alta en cuanto a la velocidad de proceso. Los ordenadores que actúan de servidores tienen procesadores centrales de alto rendimiento, incluso es común que su sistema central esté compuesto de varias CPUs, utilizando sistemas operativos que soporten multiproceso. Entre los procesadores más utilizados en la construcción de servidores de red se encuentran Pentium, Pentium Pro, Pentium II y III, PowerPC, SPARC, PA-8000 y AXP.

Memoria RAM. Un servidor consume mucha memoria RAM, por lo que es recomendable que tenga 64 Mbytes como mínimo, aunque esta cantidad depende de varios factores, por ejemplo, del número de servicios que vaya a proveer, de la cantidad de protocolos de red, del sistema operativo de red que vaya a ejecutar y del número de usuarios que se vayan a conectar a él simultáneamente. Empiezan a ser comunes, en redes para pequeñas oficinas (20 a 30 puestos), servidores con más de 64 Mbytes de RAM. En casos extremos se pueden adquirir servidores con 1 Gbyte de RAM y al menos cuatro procesadores corriendo en multiproceso simétrico; es decir, los cuatro procesadores colaboran en la ejecución del trabajo global.

Capacidad de almacenamiento en disco. Un servidor de discos o ficheros y de impresoras debe tener una gran capacidad de almacenamiento. Puesto que todos los usuarios de la red podrán conectarse a sus servicios, compartiendo sus discos, es necesario que la velocidad de acceso a los discos sea lo más elevada posible, así como el bus al que se conectan. Es normal que este bus sea de tipo SCSI (*Small Computer System Interface*) de alta velocidad. Es conveniente repartir la carga de acceso entre varios discos, de este modo se optimizan las entradas/salidas del sistema servidor. Actualmente también se utiliza el bus USB (*Universal Serial Bus*), que permite la conexión transparente de una gran cantidad de periféricos con unas elevadas velocidades de transferencia. También son necesarios mecanismos de seguridad en los discos, bien por duplicación automática de la información o por un sistema de redundancia basada en la paridad. La tecnología más utilizada para esto es la RAID (*Redundant Arrays of Inexpensive Disk*).

Conexión a la red. El sistema de conexión a la red en un servidor debe ser muy eficaz, puesto que soportará todo el tráfico generado entre él y sus clientes; por tanto, es un candidato ideal a constituirse en cuello de botella de toda la red. Lo habitual es que los adaptadores de red sean PCI (*Peripheral Component Interconnect*) y que la red a la que se conectan sea de alta velocidad, normalmente segmentos de red de 100 Mbps.

2.4 Clasificación de los servidores

Realizaremos aquí una clasificación de los servidores de red atendiendo a tres aspectos fundamentales:

- **En función de los servicios prestados**. En esta primera clasificación los servidores se caracterizan por el tipo de servicio que brindan a los clientes de la red, a estaciones de trabajo o a otros servidores. Así,

tenemos servidores de discos, de ficheros, de impresoras, de gráficos, de comunicaciones, de aplicaciones, de sistemas operativos, etc.

- **En función de la red a la que se conectan**. Un servidor se puede conectar a una red de área local (servidor LAN) o a una red de área extendida (servidor WAN) o a ambas (servidor LAN-WAN). Los tipos de servicios que proveen pueden ser muy distintos. Por ejemplo, un servidor WAN brinda servicios de páginas WEB o WWW (World Wide Web) para Internet, resolución de direcciones (se verá más adelante), de control y seguridad de la red, de transacciones, etc.

- **En función del sistema operativo de red utilizado**. El sistema operativo de red instalado en un servidor o en una estación define gran parte de su funcionalidad.

3 El software de las LAN

3.1 Los controladores de los adaptadores de red

Como cualquier tarjeta, los adaptadores de red necesitan de un software controlador que conduzca sus operaciones desde el sistema operativo. De este modo, las aplicaciones a través del sistema operativo tienen controlado los accesos al hardware del sistema, y en concreto, de la red.

Este software es un programa de muy bajo nivel denominado controlador, que es específico para cada adaptador. Normalmente cada fabricante construye su propio controlador para cada una de las tarjetas que fabrica.

Sobre este controlador pueden establecerse otros programas de más alto nivel y que tienen funciones específicas relacionadas con los protocolos de la red en la que se vaya a instalar el sistema. A estos programas se les llama packet-drivers, porque son los encargados de la confección de los paquetes o tramas que circularán por la red. Estos paquetes están construidos de acuerdo con las especificaciones de los protocolos de capa superior adaptados a las características del medio físico de la red.

Este fraccionamiento del software en capas de programas (no hay que confundir con los niveles OSI) permite que sobre la misma tarjeta de red puedan soportarse distintos protocolos sin interferencias entre ellos. Son las llamadas pilas o stacks de protocolos de distintas familias.

De modo análogo, son posibles los sistemas que tienen una o más pilas de protocolos sobre más de una tarjeta de red.

Hay dos tecnologías básicas para realizar este enlace entre las capas de alto nivel, por ejemplo, las aplicaciones de usuario y el adaptador de red. Se trata de las especificaciones NDIS (*Network Driver Interface Specification*, de Microsoft y 3COM) y ODI (*Open Datalink Interface, de Novell y Apple*). El software de estas especificaciones actúa como interface entre los protocolos de transporte y la tarjeta de red.

Tanto NDIS como ODI se configuran a través de unos ficheros de texto especiales (PROTOCOL.INI) que indican al software cómo utilizar los recursos de la tarjeta, así como los parámetros que definen la red local. Algunos parámetros son el IRQ de la tarjeta, el canal DMA, el tipo de transceptor, el tipo de trama de red que se ha de generar, datos identificativos de la red, etc.

3.2 El acceso de las aplicaciones a los recursos de red

Una vez resuelta la coordinación del hardware con el software de bajo nivel, hay que especificar cómo se benefician las distintas aplicaciones de usuario o del sistema operativo de los recursos de red. Para ello, se establecen unos interfaces construidos en software entre aplicaciones y software de transporte de datos, de modo que las unidades de disco remotas se vean como locales, al igual que las impresoras. El encargado de realizar esta transparencia entre servicios remotos y locales es lo que se denomina REDIRECTOR de la red.

En ocasiones, las aplicaciones deben acceder directamente a la red sin pasar por el interface de usuario del sistema operativo. IBM desarrolló un interface de alto nivel para gestionar las conexiones de las aplicaciones con servicios remotos de red. A este interface IBM le llamó NetBIOS, lo que está construido como una pieza de software que acepta peticiones de las aplicaciones desde arriba y que gestiona los protocolos de transporte de datos por abajo, de modo que independiza a las aplicaciones del tipo de red, tanto en su nivel físico como en los protocolos de transporte.

3.3 Sistemas de redes cliente/servidor

Existen NOS que están especializados en funciones de cliente y otros en funciones de servidor. Esto hace que cada nodo de la red venga definido por su función de cliente o de servidor: el servidor es quien brinda el servicio y el cliente es quien se beneficia de los servicios suministrados por un servidor. Los servidores de una red cliente/servidor suelen estar **dedicados**, es decir, cumplen sólo la función prevista para ellos, la de proporcionar uno o varios servicios, pero ello les incapacita para ejecutar aplicaciones de usuario desde su consola. Un ejemplo de NOS para redes cliente-servidor es Novell Netware.

3.4 Sistemas de red entre iguales o peer to peer

En este caso, el NOS puede actuar como cliente y como servidor simultáneamente. Así, cada nodo de la red puede ser cliente con respecto de un servicio que le provee otro nodo y servidor con respecto de otros clientes de la red que se benefician de sus servicios. Por ejemplo, todas las estaciones de la red podrían servir sus discos a la red si cualquier otra estación los necesitara. Todas las impresoras conectadas a cualquier estación podrían servirse a la red.

En las redes entre iguales se pueden establecer diferencias entre unos nodos y otros en función del número de servicios que se ponen a disposición de la red; así, un servidor brindará más servicios distintos que una estación *no servidora*, que brindará su disco, su impresora y poco más.

Los servidores de las redes entre iguales suelen ser **no dedicados**, es decir, el servidor es un puesto más de la red con posibilidad de ejecutar aplicaciones de usuario desde su consola, aunque lógicamente esto disminuirá el rendimiento del servidor como tal. Un ejemplo de NOS para redes peer to peer es Microsoft Windows NT Workstation.

3.5 Sistemas operativos de red comerciales

En la tabla siguiente se adjuntan algunos sistemas operativos de red comunes con algunas de sus características básicas.

Sistema	Compañía	Hardware	Red	Servidor	Servicios
System 7	Apple	MAC	Entre Iguales	No dedicado	Disco, impresoras
MacOS	Apple	PowerMAC	Entre iguales	No dedicado	Disco, impresoras
Lantastic	Artisoft	PC	Entre iguales	No dedicado	Disco, impresoras
Netware	Novell	PC	Cliente/Servidor	Dedicado/ No dedicado	Disco, impresoras
OS/2	IBM	PC	Entre iguales	No dedicado	Disco, impresoras, otros
Windows 95/98	Microsoft	PC	Entre iguales	No dedicado	Disco, impresoras
Windows NT	Microsoft	PC	Entre iguales	No dedicado	Disco, impresoras, otros
UNIX	Berkeley, otros	Varios	Entre iguales	No dedicado	Disco, impresoras, otros
Open VMS	DEC	VAX, AXP	Entre iguales	No dedicado	Disco, impresoras, otros

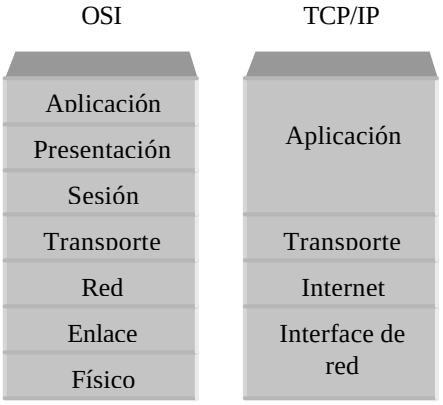
4 Protocolos de redes UNIX

El sistema operativo UNIX está considerado como el sistema abierto por antonomasia. No explicamos con precisión qué significa el término *sistema abierto*, sin embargo, un aspecto que sí nos interesa es su capacidad para interconectarse con otros sistemas. Además, es un sistema operativo que tradicionalmente se ha utilizado en las instituciones educativas, debido a que no es un sistema propietario y a su gran flexibilidad.

UNIX se ha comunicado con el exterior a través de una serie de protocolos cuya utilización se ha extendido mundialmente. De hecho, esta familia de protocolos se ha convertido en un estándar *de facto*. Cualquier otro sistema operativo considera en la actualidad la posibilidad de comunicarse con otras máquinas utilizando esta familia de protocolos, con independencia de su capacidad de emplear protocolos propios.

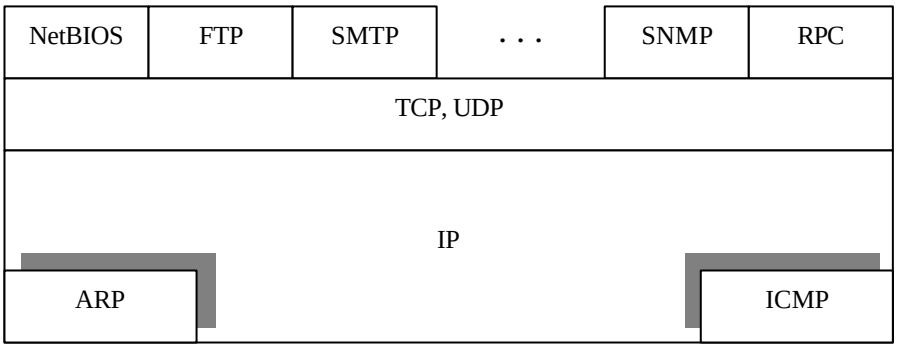
4.1 La familia de protocolos TCP/IP

Las razones anteriormente apuntadas provocan que debamos detenernos especialmente en los protocolos que constituyen esta familia, especialmente en los de tipo IP, en el nivel de red, y el protocolo TCP, en la capa de transporte, que ya se han comentado en unidades didácticas anteriores. 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 en muchos otros, se les llame familia de protocolos TCP/IP. Aunque TCP/IP no es una arquitectura OSI, se pueden establecer algunas comparaciones, como las que aparecen en la siguiente ilustración.



4.1.1 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 ochenta. *IP es un protocolo sin conexión*, por tanto, carece de seguridad en la entrega de paquetes. Cuando una comunicación que utiliza el protocolo IP para transferir los paquetes de datos necesita seguridad, ésta debe ser proporcionada por otro protocolo de capa superior, en nuestro caso el protocolo TCP, que será estudiado más adelante. Los protocolos TCP/IP se relacionan unos con otros del modo que se expresa el siguiente diagrama.

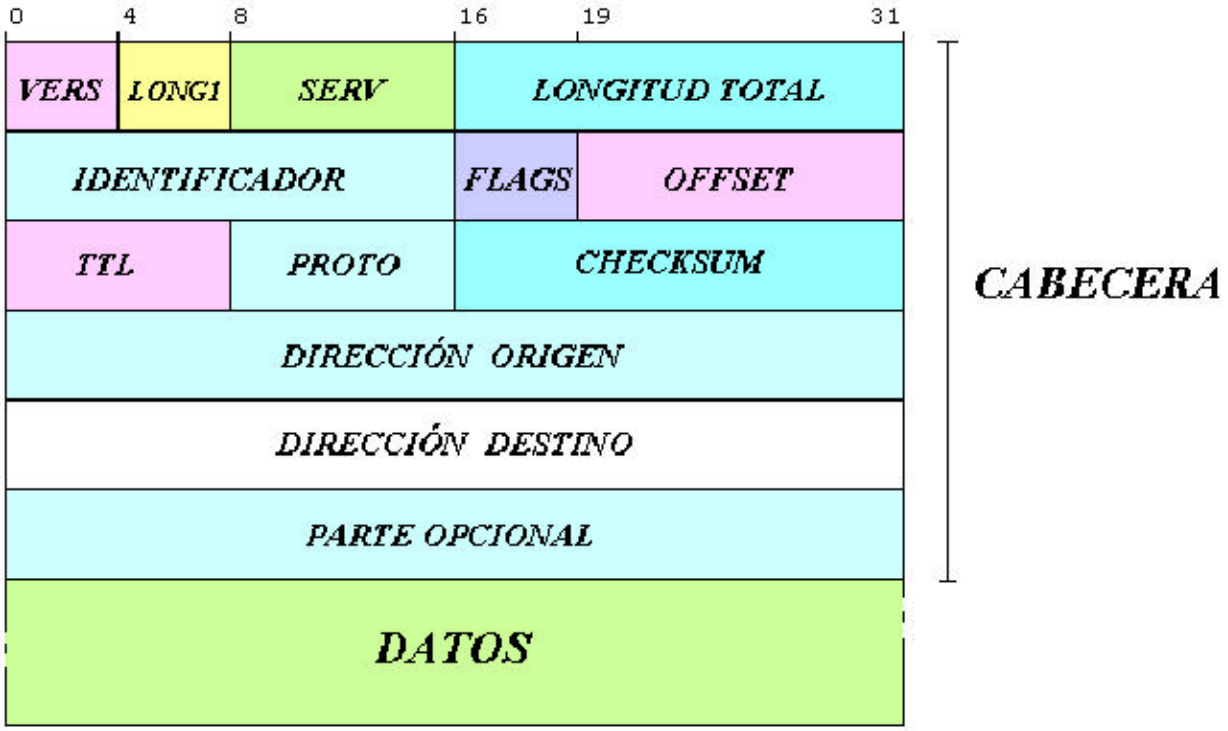


La idea inicial de diseño para IP fue la de confeccionar un protocolo capaz de conducir paquetes a través de distintas redes interconectadas, por tanto, es un protocolo especialmente preparado para que sus paquetes sean encaminados (utilizando routers) entre las distintas subredes que componen una red global. IP es el protocolo base para las transferencias de datos en Internet.

El protocolo IP acepta bloques de datos procedentes de la capa de transporte de hasta 64 Kbytes (por ejemplo, desde el protocolo TCP que opera en el nivel de transporte). Cada bloque de datos 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 bloques en un conjunto de paquetes IP, que tienen que ser ensamblados en el destino para que el mensaje sea 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.

Un paquete IP consta de una cabecera y un campo de datos. La cabecera tiene una longitud variable y se compone de una parte fija de 20 bytes y de un resto variable, lo que convierte a IP en un protocolo muy flexible de cara a nuevos diseños futuros. Los campos de que consta la cabecera son los siguientes:



- **Versión**. Este campo codifica la versión del protocolo IP. De este modo se pueden hacer convivir en la red paquetes de datos de diferentes versiones de protocolos. El receptor, analizando este campo, sabrá cómo interpretar el resto de la cabecera. Tendrá el valor 4 para IPv4 (IP de 4 bytes).

- **IHL**, *Internet Header Length* (Longitud de Cabecera Internet). Como la cabecera de un datagrama IP no es constante, es necesario codificar la longitud de la cabecera en este campo. El valor se expresa en unidades de 32 bits y su valor oscila entre 5 x 32 bits y 15 x 32 bits.

- **Tipo de servicio**. Este campo define el tipo de servicio que se requiere para la transmisión de ese paquete. Por ejemplo, si se le concede más importancia a la corrección de errores o a la velocidad de entrega. En la transmisión de voz o imagen es más importante la velocidad que los errores posibles, sin embargo, en la transmisión de datos financieros, ocurre al contrario.

- **Longitud total**. Este campo contiene la longitud total del datagrama: cabecera más datos. La máxima longitud permitida para un datagrama IP es de 65.536 bytes, es decir, 64 Kbytes, aunque habitualmente son de menor tamaño.

- **Identificación**. Cuando un datagrama se divide, es necesario que todos los fragmentos lleven la misma identificación. De este modo, el destinatario sabrá a qué datagrama pertenece cada parte cuando realiza las tareas de reensamblaje del mensaje original.

- **Flags**
    - **Bit DF**, *Don't Fragment* (bit de no fragmentación). Cuando este bit está puesto a 1, se indica a la red que ese datagrama no debe ser fragmentado, quizá porque el destinatario no será capaz de ensamblarlo.
    - **Bit MF**, More Fragments (bit de «más fragmentos»). Este bit estará siempre puesto a 1 en todos los fragmentos en que haya sido dividido un datagrama, con excepción del último. El bit MF es, por tanto, un indicador de último fragmento.

- **Desplazamiento de fragmento**. Este campo indica el lugar del datagrama en que debe ser insertado un fragmento para que su ensamblaje final sea correcto. Está expresado en número de grupos de 8 bytes comenzando en 0. Se permiten 8.192 fragmentos (13 bits) como máximo por cada datagrama original.

- **Tiempo de vida** (*Time To Life*). Este campo actúa como un contador que determina la vida que le queda a cada paquete en su existencia en la red. Con este campo se trata de evitar que un paquete quede atrapado en la red sin alcanzar su destino. Cuando el contador desciende hasta llegar a cero, cualquier router drena el paquete de la red.

- **Protocolo**. Indica el protocolo de transporte que ha generado el datagrama, por ejemplo, TCP, UDP, etc.

- **CheckSum de la cabecera**. Es un campo CRC que lleva exclusivamente el control de la cabecera del paquete IP.

- **Dirección fuente**. Codifica la dirección de nivel de red del host que produce el paquete.

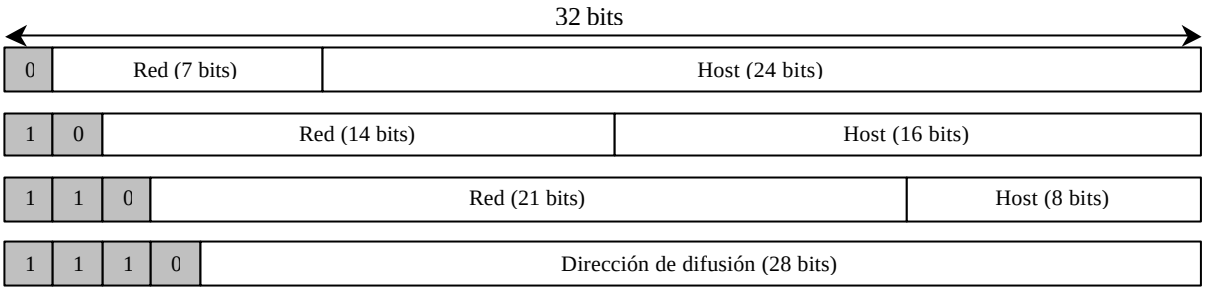
- **Dirección destino**. Codifica la dirección del host destinatario.

- **Parte opcional**. Este campo se utiliza para posibles versiones futuras del IP.

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

Como IP es un protocolo pensado para la interconexión de subredes, cada dirección IP codifica *una red* y *un host* dentro de la misma. 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.

Fundamentalmente hay tres tipos de subredes:



- **Redes de clase A** En ellas el primer bit de bs 32 que tiene cada dirección es un 0. Los siete bits siguientes 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 y cada una de ellas puede contener 16.777.214 hosts distintos. Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta

que sólo puede haber 126 redes de este tamaño. ARPAnet es una de ellas, existiendo además algunas grandes redes comerciales, aunque son pocas las organizaciones que obtienen una dirección de "clase A". Lo normal para las grandes organizaciones es que utilicen una o varias redes de "clase B".

- **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 y de 1 a 254 para el segundo (no es posible utilizar los valores 0 y 255 por tener un significado especial); por tanto, son posibles 16.384 subredes de tipo B. Cada una de estas subredes puede contener 64.516 hosts distintos, los codificados por los 16 bits restantes del campo de dirección.

- **Redes de clase C**. Sus tres primeros bits tienen 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 2.064.512 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 la que no hay un único destinatario. Las direcciones que comienzan por 1111 se reservan para protocolos especiales, como los de administración de grupos de Internet, multitransmisión y otras implementaciones futuras. 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 en la misma máquina.

Tabla de direcciones IP de Internet.

Clase	Primer byte	Identificación de red	Identificación de hosts	Número de redes	Número de hosts
A	1 .. 126	1 byte	3 bytes	126	16.387.064
B	128 .. 191	2 bytes	2 bytes	16.256	64.516
C	192 .. 223	3 bytes	1 bytes	2.064.512	254

En la clasificación de direcciones anterior se puede notar que ciertos números no se usan. Algunos de ellos se encuentran reservados para un posible uso futuro, como es el caso de las direcciones cuyo primer byte sea superior a 223 (clases D y E, que aún no están definidas), mientras que el valor 127 en el primer byte se utiliza en algunos sistemas para propósitos especiales (identificación de la máquina local). También es importante notar que los valores 0 y 255 en cualquier byte de la dirección no pueden usarse normalmente por tener otros propósitos específicos.

El número 0 está reservado para las máquinas que no conocen su dirección, pudiendo utilizarse tanto en la identificación de red para máquinas que aún no conocen el número de red a la que se encuentran conectadas, en la identificación de *host* para máquinas que aún no conocen su número de *host* dentro de la red, o en ambos casos.

El número 255 tiene también un significado especial, puesto que se reserva para el *broadcast (multidifusión)*. El *broadcast* es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo datagrama a un número determinado de sistemas, resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno. Otra situación para el uso de *broadcast* es cuando se quiere convertir el nombre por dominio de un ordenador a su correspondiente número IP y no se conoce la dirección del servidor de nombres de dominio más cercano.

Lo usual es que cuando se quiere hacer uso del *broadcast* se utilice una dirección compuesta por el identificador normal de la red y por el número 255 (todo unos en binario) en cada byte que identifique al *host*. Sin embargo, por conveniencia también se permite el uso del número 255.255.255.255 con la misma finalidad, de forma que resulte más simple referirse a todos los sistemas de la red.

El *broadcast* es una característica que se encuentra implementada de formas diferentes dependiendo del medio utilizado, y por lo tanto, no siempre se encuentra disponible. En ARPAnet y en las líneas punto a punto no es posible enviar *broadcast*, pero sí que es posible hacerlo en las redes *Ethernet*, donde se supone que todos los ordenadores prestarán atención a este tipo de mensajes.

Cuando se quiere construir una red privada utilizando TCP/IP, es conveniente utilizar las direcciones de la tabla siguiente. Estas direcciones son especiales dado que los routers de Internet ignoran cualquier datagrama IP que pertenezca a alguna de estas redes. Cabe recordar que una dirección IP debe ser única en una red y esto se cumple también en Internet, por lo que es conveniente curarse en salud ante fallos de los programas de la red privada que envíen paquetes hacia Internet con IP y utilizar direcciones privadas que no irán más allá de nuestro ISP (*Internet Server Provider*).

Direcciones para redes privadas		
Clase	**Máscara de red**	**Desde - hasta**
A	255.0.0.0	10.0.0.0 -- 10.255.255.255
B	255.255.0.0	172.16.0.0 -- 172.31.255.255
C	255.255.255.0	192.168.0.0 -- 192.168.255.255

4.1.1.1 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 y qué parte el host. Este elemento 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 (255.0.0.0):

11111111 00000000 00000000 00000000

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).

11111111 11111111 11111111 00000000

Son posibles combinaciones cualesquiera de los bits para generar subredes y hosts dentro de las subredes. Parece redundante asignar una máscara a una red sabiendo que con los primeros bits de dirección sabemos a qué tipo de subred pertenece. Esto es cierto, pero **el sistema de máscara permite fraccionar de manera más específica las subredes de distintas organizaciones**.

4.1.1.2 IP (Internet Protocol) versión 6

La nueva versión del protocolo IP recibe el nombre de IPv6, aunque es también conocido comúnmente como IPng (*Internet Protocol Next Generation*). El número de versión de este protocolo es el 6 frente a la versión 4 utilizada hasta entonces, puesto que la versión 5 no pasó de la fase experimental. Los cambios que se introducen en esta nueva versión son muchos y de gran importancia, aunque la transición desde la versión 4 no debería ser problemática gracias a las características de compatibilidad que se han incluido en el protocolo. IPng se ha diseñado para solucionar todos los problemas que surgen con la versión anterior, y además ofrecer soporte a las nuevas redes de alto rendimiento (como ATM, Gigabit Ethernet, etc.)

Una de las características más llamativas es el nuevo sistema de direcciones, en el cual se pasa de los 32 a los 128 bit, eliminando todas las restricciones del sistema actual. Otro de los aspectos mejorados es la seguridad, que en la versión anterior constituía uno de los mayores problemas. Además, el nuevo formato de la cabecera se ha organizado de una manera más efectiva, permitiendo que las opciones se sitúen en extensiones separadas de la cabecera principal.

4.1.2 Protocolo DHCP

La asignación de direcciones IP a todos los nodos de una red de área local puede ser muy laboriosa, sobre todo si el número de nodos es elevado o si tiene que estar conectada a otras redes de área local formando una red de área extendida.

El protocolo DHCP (Protocolo de configuración dinámica de host) junto con los servicios DHCP ayudan al administrador de la red a automatizar estas asignaciones, haciéndolas dinámicas.

El servidor DHCP asigna una dirección IP a cada nodo que lo solicita, a través del protocolo DHCP de modo que no pueda haber colisiones entre dos nodos por concesión de la misma dirección a ambos. Cuando el nodo IP cambia de red o se apaga, su dirección queda liberada y puede ser asignada por el servidor DHCP a otro nodo que lo solicite.

4.1.3 Protocolo TCP

TCP (*Transmisión Control Protocol*; protocolo de control de transmisión) fue especialmente diseñado para realizar conexiones en *redes inseguras* (redes en las que es probable que existan errores en la transmisión). TCP es un protocolo de capa de transporte adecuado para interactuar contra el protocolo IP en el nivel de red que ha sido estudiado anteriormente.

TCP acepta bloques de datos (TPDU) 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 pasan a la capa de red que, a su vez, puede volver a fraccionarlos para su transmisión efectiva. Cada uno de los bloques de datos 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 de retransmisiones en el caso de que haya problemas.

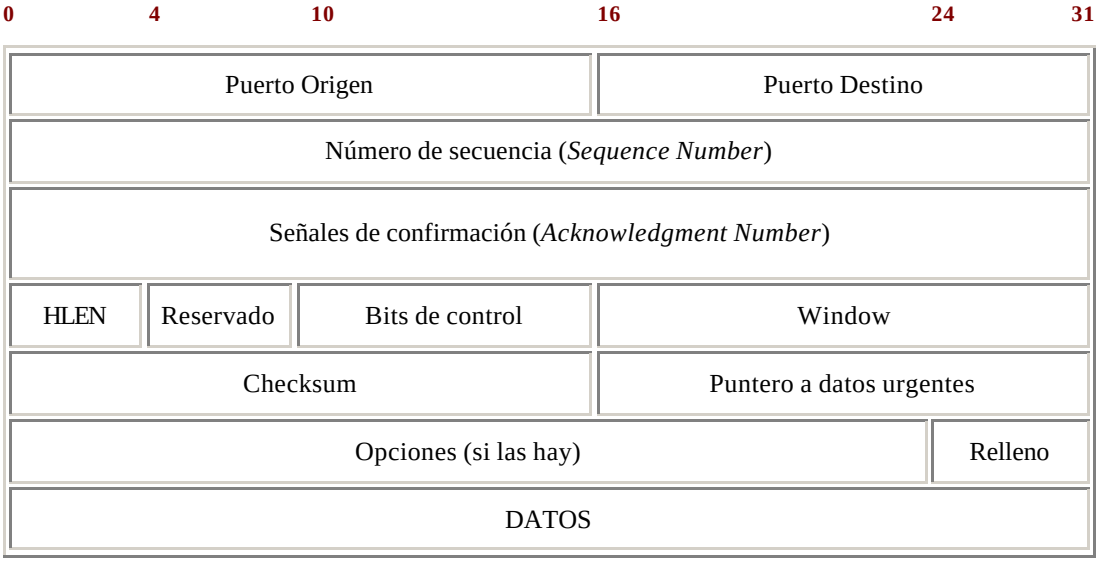
La seguridad del protocolo TCP lo convierte en idóneo para la **transmisión de datos por sesiones**, para aplicaciones cliente-servidor y para **servicios críticos**, como el correo electrónico.

La seguridad en TCP tiene un precio, que se traduce en grandes cabeceras de mensajes y en 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. Las primitivas de la capa de transporte en TCP/IP son mucho menos abstractas que las de OSI y permiten crear sockets, asociar nombres ASCII a sockets previamente creados, establecer y liberar conexiones, enviar y recibir mensajes a través de los sockets, etc.

La cabecera de un datagrama contiene al menos 160 bits que se encuentran repartidos en varios campos con diferente significado. Cuando la información se divide en datagramas para ser enviados, el orden en que éstos lleguen a su destino no tiene que ser el correcto. Cada uno de ellos puede llegar en cualquier momento y con cualquier orden, e incluso puede que algunos no lleguen a su destino o lleguen con información errónea. Para evitar todos estos problemas el TCP numera los datagramas antes de ser enviados, de manera que sea posible volver a unirlos en el orden adecuado. Esto permite también solicitar de nuevo el envío de los datagramas individuales que no hayan llegado o que contengan errores, sin que sea necesario volver a enviar el mensaje completo.

Formato de un segmento TCP



A continuación de la cabecera puede existir información opcional. En cualquier caso el tamaño de la cabecera debe ser múltiplo de 32 bits, por lo que puede ser necesario añadir un campo de tamaño variable y que contenga ceros al final para conseguir este objetivo cuando se incluyen algunas opciones. El campo de tamaño contiene la longitud total de la cabecera TCP expresada en el número de palabras de 32 bits que ocupa. Esto permite determinar el lugar donde comienzan los datos.

Dos campos incluidos en la cabecera y que son de especial importancia son los **números de puerto de origen y puerto de destino**. Los puertos proporcionan una manera de distinguir entre las distintas transferencias, ya que un mismo ordenador puede estar utilizando varios servicios o transferencias simultáneamente, e incluso puede que por medio de usuarios distintos. El puerto de origen contendrá un número cualquiera que sirva para realizar esta distinción. Además, el programa cliente que realiza la petición también debe conocer el número de puerto en el que se encuentra el servidor adecuado. Mientras que el programa del usuario utiliza números prácticamente aleatorios, el servidor deber tener asignado un número estándar para que pueda ser utilizado por el cliente. (Por ejemplo, en el caso de la transferencia de ficheros FTP el número oficial es el 21). Cuando es el servidor el que envía los datos, los números de puertos de origen y destino se intercambian.

En la transmisión de datos a través del protocolo TCP la fiabilidad es un factor muy importante. Para poder detectar los errores y pérdida de información en los datagramas, es necesario que el cliente envíe de nuevo al servidor unas señales de confirmación una vez que se ha recibido y comprobado la información satisfactoriamente. Estas señales se incluyen en el campo apropiado de la cabecera del segmento *(Acknowledgment Number*), que tiene un tamaño de 32 bits. Si el servidor no obtiene la señal de confirmación adecuada transcurrido un período de tiempo razonable, el datagrama completo se volverá a enviar. Por razones de eficiencia los segmentos se envían continuamente sin esperar la confirmación, haciéndose necesaria la numeración de los mismos para que puedan ser ensamblados en el orden correcto.

También puede ocurrir que la información del segmento llegue con errores a su destino. Para poder detectar cuando sucede esto se incluye en la cabecera un campo de 16 bits, el cual contiene un valor calculado a partir de la información del segmento completo (*checksum*). En el otro extremo el receptor vuelve a calcular este valor, comprobando que es el mismo que el suministrado en la cabecera. Si el valor es distinto significaría que el segmento es incorrecto, ya que en la cabecera o en la parte de datos del mismo hay algún error.

La forma en que TCP numera los segmentos es contando los bytes de datos que contiene cada uno de ellos y añadiendo esta información al campo correspondiente de la cabecera del datagrama siguiente. De esta manera el primero empezará por cero, el segundo contendrá un número que será igual al tamaño en bytes de la parte de datos del datagrama anterior, el tercero con la suma de los dos anteriores, y así sucesivamente. Por ejemplo, para un tamaño fijo de 500 bytes de datos en cada datagrama, la numeración sería la siguiente: 0 para el primero, 500 para el segundo, 1000 para el tercero, etc.

Algunos segmentos sólo llevan un acuse de recibo y otros solamente llevan datos. Otros llevan solicitudes para establecer o cerrar una conexión. El software TCP utiliza el campo de 6 bits, etiquetado como bits de control, para determinar el propósito y contenido del segmento. Los seis bits indican cómo interpretar otros campos en el encabezado, de acuerdo con la tabla siguiente:

Bit	Significado si está puesto a 1
URG	El campo de puntero de urgente es válido
ACK	El campo de acuse de recibo es válido
PSH	Este segmento solicita una operación push
RST	Iniciación de la conexión
SYN	Sincronizar números de secuencia
FIN	El emisor ha llegado al final de su flujo de octetos

Existe otro factor más a tener en cuenta durante la transmisión de información, y es la potencia y velocidad con que cada uno de los ordenadores puede procesar los datos que le son enviados. Si esto no se tuviera en cuenta, el ordenador de más potencia podría enviar la información demasiado rápido al receptor, de manera que éste no pueda procesarla. Este inconveniente se soluciona mediante un campo de 16 bit (*Window*) en la cabecera TCP, en el cual se introduce un valor indicando la cantidad de información que el receptor está preparado para procesar. Si el valor llega a cero será necesario que el emisor se detenga. A medida que la información es procesada este valor aumenta indicando disponibilidad para continuar la recepción de datos.

Algunas veces es importante que el programa en un extremo de la conexión envíe datos fuera de banda, sin esperar a que el programa en el otro extremo de la conexión consuma los bytes que ya están en flujo. Por ejemplo, cuando se utiliza TCP para una sesión de acceso remoto, el usuario puede decidir si envía una secuencia de teclado que interrumpa o aborte el programa en el otro extremo. Dichas señales se necesitan aun más cuando una programa en la máquina remota no opera de manera correcta. Las señales se deben enviar sin esperar a que el programa lea los octetos que ya están enviados.

Para incorporar la señalización fuera de banda, el TCP permite que el transmisor especifique los datos como urgentes, dando a entender que se debe notificar su llegada al programa receptor tan pronto como sea posible. El protocolo especifica que, cuando se encuentra con datos urgentes, el TCP receptor debe notificar al programa de aplicación que entre en modalidad urgente. Después de asimilar todos los datos urgentes, el TCP indica al programa de aplicación que regrese a su operación normal.

El mecanismos utilizado para marcar los datos urgentes cuando se transmiten en un segmento consiste en un bit de código URG y en un campo URGENT POINTER (puntero de urgencia). Este indica la posición dentro del segmento en la que terminan los datos urgentes.

4.1.4 Protocolos alternativos a TCP.

TCP es el protocolo más utilizado para el nivel de transporte en Internet, pero además de éste existen otros protocolos que pueden ser más convenientes en determinadas ocasiones. Tal es el caso de UDP e ICMP.

4.1.4.1 UDP (User Datagram Protocol)

El protocolo de datagramas de usuario (UDP) puede ser la alternativa al TCP en algunos casos en los que no sea necesario el gran nivel de complejidad proporcionado por el TCP. Puesto que UDP *no admite numeración de los datagramas*, éste protocolo se utiliza principalmente cuando el orden en que se reciben los mismos no es un factor fundamental, o también cuando se quiere enviar información de poco tamaño que cabe en un único datagrama.

Cuando se utiliza UDP, la garantía de que un paquete llegue a su destino es mucho menor que con TCP debido a que no se utilizan las señales de confirmación. Por todas estas características la cabecera del UDP es bastante menor en tamaño que la de TCP. Esta simplificación resulta en una mayor eficiencia en determinadas ocasiones.

Un ejemplo típico de una situación en la que se utiliza el UDP es cuando se pretende conectar con un ordenador de la red, utilizando para ello el nombre del sistema. Este nombre tendrá que ser convertido a la dirección IP que le corresponde y, por tanto, tendrá que ser enviado a algún servidor que posea la base de datos necesaria para efectuar la conversión. En este caso es mucho más conveniente el uso de UDP.

4.1.4.2 Protocolo ICMP

El protocolo de mensajes de control de Internet (ICMP) es de características similares al UDP, pero con un formato aún más simple. Es un protocolo que encapsula 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. Son posibles, entre otros, mensajes como los siguientes:

- **Destino inalcanzable**. Se utiliza cuando una subred no puede alcanzar otra red solicitada por un datagrama IP, o bien es alcanzable, pero no en las condiciones especificadas en el paquete IP, por ejemplo, porque no se pueda transmitir sin fragmentación previa, estando a 1 el bit DF.

- **Tiempo excedido**. El campo contador del tiempo de vida de un paquete IP ha descendido hasta 0 y ha sido drenado 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.

4.1.5 ARP (Address Resolution Protocol).

El Protocolo de Resolución de Direcciones (ARP) es necesario debido a que las direcciones *Ethernet* y las direcciones IP son dos números distintos y que no guardan ninguna relación. Así, cuando pretendemos dirigirnos a un *host* a través de su dirección de Internet se necesita convertir ésta a la correspondiente dirección *Ethernet*. No es un protocolo relacionado directamente con el transporte de datos, sino que complementa la acción de la conjunción TCP/IP, pasando desapercibido a los ojos de los usuarios y de las aplicaciones de la red.

Como el protocolo IP utiliza un sistema de direccionamiento que no tiene nada que ver con las direcciones MAC de las redes de área local, hay que arbitrar un mecanismo de asignación de direcciones IP a direcciones MAC propias del nivel de enlace. ARP es el protocolo encargado de realizar las conversiones de dirección correspondientes a cada *host*. Para ello cada sistema cuenta con una tabla con la dirección IP y la dirección *Ethernet* de algunos de los otros sistemas de la misma red. Sin embargo, también puede ocurrir que el ordenador de destino no se encuentre en la tabla de direcciones, teniendo entonces que obtenerla por otros medios.

Con la finalidad de obtener una dirección *Ethernet* destino que no se encuentra en la tabla de conversiones se utiliza el mensaje ARP de petición. Este mensaje es enviado como *broadcast*, es decir, que estará disponible para que el resto de los sistemas de la red lo examinen, y el cual contiene una solicitud de la dirección final de un sistema a partir de su dirección IP. Cuando el ordenador con el que se quiere comunicar analiza este mensaje comprueba que la dirección IP corresponde a la suya y envía de regreso el mensaje ARP de respuesta, el cual contendrá la dirección *Ethernet* que se estaba buscando. El ordenador que solicitó la información recibirá entonces el mensaje de respuesta y añadirá la dirección a su propia tabla de conversiones para futuras referencias.

El mensaje de petición ARP contiene las direcciones IP y *Ethernet* del *host* que solicita la información, además de la dirección IP del *host* de destino. Estos mensajes son aprovechados en algunas ocasiones también por otros sistemas de la red para actualizar sus tablas, ya que el mensaje es enviado en forma de *broadcast*. El ordenador

de destino, una vez que ha completado el mensaje inicial con su propia dirección *Ethernet*, envía la respuesta directamente al *host* que solicitó la información.

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.

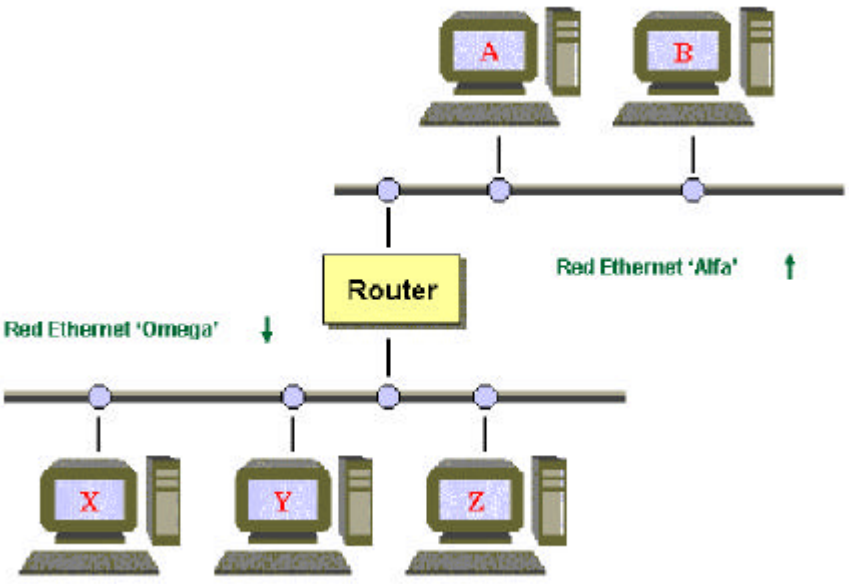
4.2 Routing

Ya se ha expuesto anteriormente la forma en que los datagramas pasan de un ordenador de la red a otro mediante el protocolo IP, sin embargo en esta sección se comenta con más detalle el proceso que permite que la información llegue hasta su destino final. Esto se conoce con el nombre de *routing*.

Para los ejemplos que aparecen a continuación se va a suponer que todas las redes locales en las que se implementan los protocolos de Internet TCP/IP pertenecen a la tecnología *Ethernet*, aunque las redes utilizadas en la práctica pueden ser de muy diversos tipos. También se supondrá que se está utilizando el protocolo IP versión 4, con direcciones de 32 bit.

Las tareas de *routing* son implementadas por el protocolo IP sin que los protocolos de un nivel superior tales como TCP o UDP tengan constancia de ello. Cuando se quiere enviar información por Internet a un ordenador, el protocolo IP comprueba si el ordenador de destino se encuentra en la misma red local que el ordenador origen. Si es así, se enviará el correspondiente datagrama de forma directa: la cabecera IP contendrá el valor de la dirección Internet del ordenador destino, y la cabecera *Ethernet* contendrá el valor de la dirección de la red *Ethernet* que corresponde a este mismo ordenador.

Cuando se pretende enviar información a un ordenador remoto que está situado en una red local diferente al ordenador de origen, el proceso resulta más complicado. Esto se conoce como *routing* indirecto, y es el caso que se presenta más frecuentemente cuando se envía información en Internet. La figura muestra un ejemplo en el que dos redes locales que utilizan la tecnología de Internet se enlazan para intercambiar información, creando una red lógica de mayor tamaño gracias a la funcionalidad del protocolo IP.



En Internet existen un elevado número de redes independientes conectadas entre sí mediante el uso de los *routers*. Un ordenador puede actuar como un *router* si se conecta a varias redes al mismo tiempo, disponiendo por lo tanto de más de una interfaz de red así como de varias direcciones IP y *Ethernet* (tantas como redes a las que se encuentre conectado). El *router*, por supuesto, puede enviar y recibir información de los *hosts* de todas las redes a las que está conectado, y siempre será de forma directa. Continuando con el ejemplo anterior, el *host* A puede comunicarse de forma directa con el *host* B, así como los *hosts* A y B pueden enviar o recibir información del *router*. En ambos casos se trata de *routing* directo, pues el ordenador que actúa como *router* está conectado a

la red 'alfa' de la misma manera que los ordenadores A y B, teniendo una dirección IP propia asignada que lo identifica dentro de esta misma red. La situación es la misma para la red 'omega' donde el *router* es identificado a través de una segunda dirección IP que corresponde con esta red.

Si sólo fuésemos a enviar información de manera directa dentro de una misma red no sería necesario el uso del protocolo TCP/IP, siendo el mismo especialmente indicado cuando se desea una comunicación con otras redes. En este caso los datagramas tendrán que ser encaminados a través del *router* para llegar a su destino. La forma de hacer esto es a través del protocolo IP, el cual decide si la información puede enviarse directamente o si por el contrario debe utilizarse el método indirecto a través de un *router*. Tomamos de nuevo el ejemplo de la figura: Suponemos que el *host* B de la red 'alfa' necesita comunicarse con el *host* X situado en la red 'omega'. Una vez que se ha determinado que el destino no se encuentra en la misma red, envía el datagrama IP hacia el *router* correspondiente. Como este *router* y el ordenador que envía la información se encuentran conectados a la misma red, se trata por tanto de *routing* directo, ya comentado anteriormente, y por consiguiente sólo será necesario determinar la dirección *Ethernet* del *router* mediante empleo del protocolo ARP. El paquete enviado incluirá la dirección del *router* como dirección Ethernet de destino, pero sin embargo, la dirección de destino IP corresponderá al ordenador final al que va dirigido el paquete, el *host* X en el ejemplo. El *router* recibe el paquete y a través del protocolo IP comprueba que la dirección de Internet de destino no corresponde con ninguna de las asignadas como suyas, procediendo entonces a determinar la localización de la 'omega', en la que se entrega el paquete al ordenador de destino.

Hasta este punto se ha supuesto que sólo existe un único *router*, pero es bastante probable que una red con conexión a Internet posea múltiples enlaces con otras redes, y por lo tanto más de un *router*. Entonces... ¿cómo determina el protocolo IP el sistema correcto al que debe dirigirse? Para resolver este problema cada ordenador utiliza una tabla donde se relaciona cada una de las redes existentes con el *router* que debe usarse para tener acceso. Debe tenerse en cuenta que los *routers* indicados en estas tablas pueden no estar conectados directamente a las redes con las que están relacionados, sino que lo que se indica es el mejor camino para acceder a cada una de ellas. Por esta razón, cuando un *router* recibe un paquete que debe ser encaminado, busca en su propia tabla de redes la entrada correspondiente a la red para, una vez encontrada, entregarlo al ordenador de destino. Es importante notar que en el caso de que el *router* no tenga conexión directa a la misma red que el ordenador de destino, la búsqueda en su tabla de redes dará como resultado la dirección de un nuevo *router* al que dirigir el paquete, y así continuará el proceso sucesivamente hasta encontrar el destino final.

A causa de la extensión de Internet, es normal que un paquete atraviese numerosas redes (pueden ser decenas) hasta llegar a su destino. La ruta que tiene que recorrer un paquete en su viaje a través de la red no está determinada inicialmente, sino que es el resultado de la consulta en las tablas de direcciones individuales de los ordenadores intermedios.

Ya se ha mencionado anteriormente que todos los *host* de Internet necesitan disponer de una tabla de *routing* con la información de otras redes, pero esto supondría algunos inconvenientes adicionales (como el tamaño y la necesidad de mantenimiento). Con la finalidad de reducir los inconvenientes se utilizan los *routers* (o *gateways*) por defecto. De esta manera cuando un *host* no posee información del camino correcto para un determinado paquete, éste es enviado al *router* que tiene asignado por defecto. Si este *router* es el único del que dispone la red no habrá ningún inconveniente y el paquete continuará su camino. Sin embargo, cuando existen varios *routers* para la misma red puede ocurrir que el utilizado por defecto no sea el más apropiado para el paquete que se quiere enviar, por lo que se necesita algún procedimiento para notificar el error al *host* que envió el paquete. El protocolo ICMP es el utilizado para enviar estos mensajes de notificación que informan al *host* de la ruta correcta, y que en muchos casos éste utiliza para actualizar su propia tabla de *routing* y que los próximos paquetes con el mismo destino sean dirigidos de forma correcta.

La creación y mantenimiento de la tabla de redes para *routing* es un proceso complejo que debe ser realizado por el administrador de la red. Aquí hay que tener en cuenta que la enorme extensión de Internet supone una gran dificultad para conseguir que sean correctas todas las entradas de la tabla, además de que esta tabla puede llegar a tener un tamaño considerable. La utilización de *routers* por defecto mejora la situación al permitir que sean estos los que guarden el registro de la red sin que los ordenadores individuales tengan que ocuparse en ello, pero estos *routers* sí que deberían tener una tabla completa. Para facilitar el mantenimiento de la tabla existen algunos protocolos para *routing* que permiten que un *router* o *gateway* cualquiera pueda encontrar por sí mismo la localización de otros *routers* o *gateways* y guardar la información acerca del mejor camino para acceder a cada red.

Lógicamente el proceso real de *routing* sobre Internet suele ser mucho más complejo que el expuesto aquí, principalmente por el uso de redes y tecnologías muy distintas e incompatibles. Esto obliga a que se realicen conversiones en el formato de los paquetes para que puedan pasar a través de medios diferentes, pero en cualquier caso el protocolo IP proporciona una transmisión transparente para los protocolos de nivel superior y las aplicaciones de red.

4.3 Sistema de nombres por dominio.

El sistema de nombres por dominio (DNS, *Domain Name System*) es una forma alternativa de identificar a una máquina conectada a Internet. La dirección IP resulta difícil de memorizar, siendo su uso más adecuado para los ordenadores. El sistema de nombres por dominio es el utilizado normalmente por las personas para referirse a un ordenador en la red, ya que además puede proporcionar una idea del propósito o la localización del mismo.

El nombre por dominio de un ordenador se representa de forma jerárquica con varios nombres separados por puntos (generalmente 3 ó 4, aunque no hay límite). Típicamente el nombre situado a la izquierda identifica al *host*, el siguiente es el subdominio al que pertenece este *host*, y a la derecha estará el dominio de mayor nivel que contiene a los otros subdominios:

nombre_ordenador.subdominio.dominio_principal

Aunque esta situación es la más común, el nombre por dominio es bastante flexible, permitiendo no sólo la identificación de *hosts* sino que también puede utilizarse para referirse a determinados servicios proporcionados por un ordenador o para identificar a un usuario dentro del mismo sistema. Es el caso de la dirección de correo electrónico, donde el nombre por dominio adquiere gran importancia puesto que el número IP no es suficiente para identificar al usuario dentro de un ordenador.

Para que una máquina pueda establecer conexión con otra es necesario que conozca su número IP, por lo tanto, el nombre por dominio debe ser convertido a su correspondiente dirección a través de la correspondiente base de datos. En los inicios de Internet esta base de datos era pequeña de manera que cada sistema podía tener su propia lista con los nombres y las direcciones de los otros ordenadores de la red, pero actualmente esto sería impensable. Con esta finalidad se utilizan los servidores de nombres por dominio (DNS *servers*).

Los servidores de nombres por dominio son sistemas que contienen bases de datos con el nombre y la dirección de otros sistemas en la red de una forma encadenada o jerárquica.

Para comprender mejor el proceso supongamos que un usuario suministra el nombre por dominio de un sistema en la red a su ordenador local, realizándose el siguiente proceso:

El ordenador local entra en contacto con el servidor de nombres que tiene asignado, esperando obtener la dirección que corresponde al nombre que ha suministrado el usuario.

El servidor de nombres local puede conocer la dirección que se está solicitando, entregándosela al ordenador que realizó la petición.

Si el servidor de nombres local no conoce la dirección, ésta se solicitará al servidor de nombres que esté en el dominio más apropiado. Si éste tampoco tiene la dirección, llamará al siguiente servidor DNS, y así sucesivamente.

Cuando el servidor DNS local ha conseguido la dirección, ésta se entrega al ordenador que realizó la petición.

Si el nombre por dominio no se ha podido obtener, se enviará de regreso el correspondiente mensaje de error.

En sistemas UNIX y en otros existe un fichero de configuración llamado «hosts» (en UNIX suele estar situado en /etc/hosts) que contiene una relación de asignaciones de nombres DNS con direcciones IP para los nodos de la red de área local. Este es un modo de utilizar nombres DNS sin necesidad de tener acceso a un servidor DNS, que exige una conexión WAN hacia un DNS propio de Internet. Obviamente, este fichero sólo puede contener

un número muy limitado de asignaciones que, además, deben ser previamente conocidas para que puedan ser escritas por el administrador de red en el fichero de hosts.

4.3.1.1 Servicios WINS

DNS no es el único sistema de nombres para redes. Existen otros planos, no articulados, que identifican cada nodo de una red por un nombre único. Estos sistemas son especialmente eficaces en pequeñas redes, o en grandes redes combinados con otros sistemas de nombres articulados.

El sistema de nombres planos más extendido actualmente viene determinado por los nombres propios del interface NetBIOS. En ocasiones interesa enlazar los nombres NetBIOS de los equipos de la red con las direcciones IP de los mismos. WINS (Servicio de nombres Internet de Windows) es un servicio propio de redes de Microsoft que viene a resolver inteligentemente este problema, evitando el tráfico de paquetes de difusión en gran medida. La resolución de nombres NetBIOS tiene un archivo semejante al «hosts» de nombres DNS. Se trata del fichero «LMHOSTS», que en Windows NT está situado en:

\raíz_sistema\SYSTEM32\DRIVERS\ETC\LMHOSTS

mientras que en Windows 9X está en el propio directorio del sistema.

4.4 Servicios de Internet: el nivel de aplicación.

Los diferentes servicios a los que podemos tener acceso en Internet son proporcionados por los protocolos que pertenecen al nivel de aplicación. Estos protocolos forman parte del TCP/IP y deben aportar entre otras cosas una forma normalizada para interpretar la información, ya que todas las máquinas no utilizan los mismos juegos de caracteres ni los mismos estándares. Los protocolos de los otros niveles sólo se encargan de la transmisión de información como un bloque de bits, sin definir las normas que indiquen la manera en que tienen que interpretarse esos bits. Los protocolos del nivel de aplicación están destinados a tareas específicas, algunos de los cuales se consideran como tradicionales de Internet por utilizarse desde los inicios de la red, como son por ejemplo:

Transferencia de ficheros (*File Transfer*)

Correo electrónico (*e-mail*)

Conexión remota (*remote login*)

Sistema de ficheros de red (*Network File System)*

4.4.1 Transferencia de ficheros.

El protocolo FTP (*File Transfer Protocol*) se incluye como parte del TCP/IP, siendo éste el protocolo de nivel de aplicación destinado a proporcionar el servicio de transferencia de ficheros en Internet. El FTP depende del protocolo TCP para las funciones de transporte, y guarda alguna relación con TELNET (protocolo para la conexión remota).

El protocolo FTP permite acceder a algún servidor que disponga de este servicio y realizar tareas como moverse a través de su estructura de directorios, ver y descargar ficheros al ordenador local, enviar ficheros al servidor o copiar archivos directamente de un servidor a otro de la red. Lógicamente y por motivos de seguridad se hace necesario contar con el permiso previo para poder realizar todas estas operaciones. El servidor FTP pedirá el nombre de usuario y clave de acceso al iniciar la sesión (*login*), que debe ser suministrado correctamente para utilizar el servicio.

La manera de utilizar FTP es por medio de una serie de comandos, los cuales suelen variar dependiendo del sistema en que se esté ejecutando el programa, pero básicamente con la misma funcionalidad. Existen aplicaciones de FTP para prácticamente todos los sistemas operativos más utilizados, aunque hay que tener en

cuenta que los protocolos TCP/IP están generalmente muy relacionados con sistemas UNIX. Por este motivo y, ya que la forma en que son listados los ficheros de cada directorio depende del sistema operativo del servidor, es muy frecuente que esta información se muestre con el formato propio del UNIX. También hay que mencionar que en algunos sistemas se han desarrollado clientes de FTP que cuentan con un interfaz gráfico de usuario, lo que facilita notablemente su utilización, aunque en algunos casos se pierde algo de funcionalidad.

Existe una forma muy utilizada para acceder a fuentes de archivos de carácter público por medio de FTP. Es el acceso FTP anónimo, mediante el cual se pueden copiar ficheros de los *hosts* que lo permitan, actuando estos *host* como enormes almacenes de información y de todo tipo de ficheros para uso público. Generalmente el acceso anónimo tendrá algunas limitaciones en los permisos, siendo normal en estos casos que no se permita realizar acciones tales como añadir ficheros o modificar los existentes. Para tener acceso anónimo a un servidor de FTP hay que identificarse con la palabra "anonymous" como el nombre de usuario, tras lo cual se pedirá el *password* o clave correspondiente. Normalmente se aceptará cualquier cadena de caracteres como clave de usuario, pero lo usual es que aquí se indique la dirección de correo electrónico propia, o bien la palabra "guest" (invitado). Utilizar la dirección de correo electrónico como clave de acceso es una regla de cortesía que permite a los operadores y administradores hacerse una idea de los usuarios que están interesados en el servicio, aunque en algunos lugares puede que se solicite esta información rechazando el uso de la palabra "guest".

El FTP proporciona dos modos de transferencia de ficheros: ASCII y binario. El modo de transferencia ASCII se utiliza cuando se quiere transmitir archivos de texto, ya que cada sistema puede utilizar un formato distinto para la representación de texto. En este caso se realiza una conversión en el formato del fichero original, de manera que el fichero recibido pueda utilizarse normalmente. El modo de transferencia binario se debe utilizar en cualquier otro caso, es decir, cuando el fichero que vamos a recibir contiene datos que no son texto. Aquí no se debe realizar ninguna conversión porque quedarían inservibles los datos del fichero.

4.4.2 Conexión remota

El protocolo diseñado para proporcionar el servicio de conexión remota (*remote login*) recibe el nombre de TELNET, el cual forma parte del conjunto de protocolos TCP/IP y depende del protocolo TCP para el nivel de transporte.

El protocolo TELNET es un emulador de terminal que permite acceder a los recursos y ejecutar los programas de un ordenador remoto en la red, de la misma forma que si se tratara de un terminal real directamente conectado al sistema remoto. Una vez establecida la conexión el usuario podrá iniciar la sesión con su clave de acceso. De la misma manera que ocurre con el protocolo FTP, existen servidores que permiten un acceso libre cuando se especifica "anonymous" como nombre de usuario.

Es posible ejecutar una aplicación diente TELNET desde cualquier sistema operativo, pero hay que tener en cuenta que los servidores suelen ser sistemas VMS o UNIX por lo que, a diferencia del protocolo FTP para transferencia de ficheros donde se utilizan ciertos comandos propios de esta aplicación, los comandos y sintaxis que se utilice en TELNET deben ser los del sistema operativo del servidor. El sistema local que utiliza el usuario se convierte en un terminal "no inteligente" donde todos los caracteres pulsados y las acciones que se realicen se envían al *host* remoto, el cual devuelve el resultado de su trabajo. Para facilitar un poco la tarea a los usuarios, en algunos casos se encuentran desarrollados menús con las distintas opciones que se ofrecen.

Los programas clientes de TELNET deben ser capaces de emular los terminales en modo texto más utilizados para asegurarse la compatibilidad con otros sistemas, lo que incluye una emulación del teclado. El terminal más extendido es el VT100, el cual proporciona compatibilidad con la mayoría de los sistemas, aunque puede ser aconsejable que el programa cliente soporte emulación de otro tipo de terminales.

4.4.3 Correo electrónico.

El servicio de correo electrónico se proporciona a través del protocolo SMTP (*Simple Mail Transfer Protocol*), y permite enviar mensajes a otros usuarios de la red. A través de estos mensajes no sólo se puede intercambiar texto, sino también archivos binarios de cualquier tipo.

Generalmente los mensajes de correo electrónico no se envían directamente a los ordenadores personales de cada usuario, puesto que en estos casos puede ocurrir que esté apagado o que no esté ejecutando la aplicación de correo electrónico. Para evitar este problema se utiliza un ordenador más grande como almacén de los mensajes recibidos, el cual actúa como servidor de correo electrónico permanentemente. Los mensajes permanecerán en este sistema hasta que el usuario los transfiera a su propio ordenador para leerlos de forma local.

4.4.4 Protocolo NFS

NFS (Network File System) es un protocolo basado en TCP/ IP que hace transparente a los usuarios de la red el servicio de discos en una red de nodos UNIX. Así, NFS permite servir discos locales al resto de la red, de modo que a los usuarios remotos les parece que son propietarios del disco al que se conectan. Aunque NFS es un protocolo propietario de SUN, muchas compañías han construido sus protocolos compatibles con él (como RFS, Remote-File System, de AT&T), lo que ha permitido que se puedan brindar servicios de discos entre máquinas de distintos fabricantes a través de NFS.

La familia TCP/IP contiene muchos otros protocolos utilizados en aplicaciones específicas de Internet (HTTP, PPP), correo electrónico (SMTP y POP3), News (SNMP) etc. Algunos de estos protocolos serán explicados al estudiar las redes de área extendida e Internet.

5 Protocolos de redes Netware

Netware ha sido el sistema operativo de red más utilizado a nivel mundial. Su alto rendimiento, su capacidad de crecimiento y, fundamentalmente, la optimización de los recursos requeridos tanto en las estaciones clientes como en las servidoras, han promocionado su utilización masiva. Por ejemplo, se puede utilizar Netware en un Pentium o en un 8086 de Intel con poca memoria RAM.

Los servidores Netware suelen ser dedicados. El resto de las estaciones son exclusivamente clientes de estos servidores. Otro factor que influye en el alto rendimiento de la red es el protocolo propietario desarrollado por Novell, denominado IPX/SPX (Internetwork Packet eXchage/Sequenced Packet eXchange), derivado del XNS (Xerox Network Service) de Xerox.

5.1 La familia de protocolos IPX/SPX

Esta familia de protocolos, como ocurre en las redes TCP/ IP, no tiene un paralelismo exacto con el modelo OSI. Conviene hacer una separación entre lo que son protocolos de comunicaciones y las piezas de software que los gestionan, y los servicios a través de los interfaces adecuados.

5.1.1 Configuración monolítica del IPX

Es la primera configuración utilizada por Novell para la red Netware. En ella se usaba exclusivamente el protocolo IPX. La gestión de este tipo de transporte se realiza mediante dos programas:

- IPX.COM: es un programa compilado para cada adaptador de red a partir de un IPX.OBJ y un fichero objeto propio de cada adaptador, utilizando un programa que suministra Novell denominado SHGEN o WSGEN. «IPX. COM» es un programa configurado para cada tarjeta en el que se ha de especificar cada uno de sus parámetros (IRQ, DMA, etc.). Este protocolo gestiona la interacción con la tarjeta de red y el modo de construcción de la trama en función del tipo de red sobre la que se instale Netware (Ethernet, Token Ring, etc.).

- NETX.EXE: es el redirector de Novell, es decir, la pieza de software que hace transparente el uso de los recursos compartidos. Actúa como un interface entre la red y el shell de usuario.

Para MS-DOS bastan las dos utilidades mencionadas anteriormente, sin embargo, por encima de estos programas se pueden instalar otros controladores que facilitan el establecimiento del diálogo, la apertura y cierre de sesiones, etc. Por ejemplo, es posible la instalación de NetBIOS por encima de IPX.

5.1.2 Configuración con ODI

ODI (*Open Datalink Interface*) es una especificación definida por Novell Corporation y Apple Computer Corporation para simplificar el desarrollo de controladores de red y proporcionar soporte para múltiples protocolos sobre un solo adaptador de red o incluso para hacer convivir varios adaptadores de red sobre el mismo sistema operativo.

ODI proporciona a los protocolos una API (Interface de Programación de Aplicaciones) que permite comunicar con el adaptador de red y la convivencia de distintos protocolos simultáneamente.

La configuración de Netware con ODI está compuesta de los siguientes módulos de software entre otros:

- MLID (Multiple Link Interface Driver). Es el programa que controla al adaptador de red, especialmente preparado para la utilización de la tecnología ODI. Cada tarjeta tiene un módulo MLID distinto, que normalmente recibe el nombre del adaptador y tiene extensión COM. Así, la tarjeta NE2000 tiene un módulo MLID denominado NE20OO.COM.

- LSL.COM (Link Support Layer). Provee la capacidad para la convivencia múltiple de protocolos en una o más tarjetas de red. Sobre este módulo se asientan otras capas de software para habilitar la gestión de red de distintas tecnologías: IPX, TCP/IP, etc. IPXODI.COM. Esta es la versión del IPX/SPX sobre ODI.

- NETX.EXE. Es el redirector de Netware para este modo de configuración.

Por encima de estos módulos se pueden instalar otros de software, como en el caso de la configuración monolítica.

5.2 Sistemas compatibles con IPX

Algunos nuevos sistemas operativos, como Windows NT de Microsoft o Windows 95, incorporan protocolos clónicos del IPX. En concreto, los sistemas de Microsoft lo llaman NWLink.

NWLink no basta para beneficiarse de los servicios proporcionados por un servidor Netware. IPX o NWLink son protocolos equivalentes de la capa de red en OSI. Para conseguir la utilización de los servicios necesitan crear sesiones contra estos servicios, lo que se consigue incorporando un REDIRECTOR (el equivalente al NETX). En estaciones Microsoft, este redirector se denomina «Servicio cliente de Netware».

El módulo NWNBLink se sitúa por encima de las otras capas de software y representa el interface NetBIOS, compatible con el NetBIOS de Novell. Esta configuración optimiza las transferencias de red utilizando la técnica de superposición o piggibacking, a la que ya hemos aludido en unidades anteriores. Del mismo modo, utiliza la técnica de control por ventanas (slide windows) tanto en el receptor como en el emisor.

Los equipos de Apple (Macintosh y PowerMAC) pueden incorporar software compatible con IPX/SPX, pudiéndose configurar desde los paneles de control del sistema operativo de red, tanto en System 7 como en MacOS. A este software se le llama MacIPX.

5.3 Configuración de una red Netware

En la tabla siguiente se describe a modo de ejemplo los pasos que se deben seguir para configurar el servidor de una red Netware. La instalación es muy simple si se efectúa desde un CD-ROM, ya que es totalmente interactiva. Si, además, se elige la configuración simple, apenas hace preguntas, lo que hace que Netware sea una de las redes más sencillas de instalar.

Como en la instalación de cualquier otro sistema operativo, se requiere la preparación de las particiones de disco apropiadas para la instalación de los ficheros. Para conocer con exactitud el modo de instalación debe acudirse al manual de instalación que proporciona el fabricante y que cambia de una versión a otra.

Etapa	*Configuración*	*Observaciones*
Elección del tipo de instalación.	Instalar un servidor. Instalar una estación cliente.	Se puede instalar desde CD-ROM, desde disquetes o desde otro servidor remoto. Elegimos la instalación de un servidor.
Elección del software servidor.	Instalación de un servidor (Netware 4.1). Instalación de un servidor con sistema tolerante a fallos (SFT III).	Elegimos la instalación de un servidor.
Modo de instalación	Instalación simple. Instalación a medida. Actualización del software.	Para usuarios avanzados se aconseja la instalación a medida. La actualización es un modo de instalación en que se conservan los parámetros compatibles de instalaciones de anteriores versiones del software. Elegimos una instalación a medida.
Elección del nombre del servidor.	Ha de proporcionarse una cadena de caracteres única en la red que indentifica al servidor.	Elegimos como nombre de servidor “JIMENA”.
Elección del número interno de red IPX.	Consta de 8 cifras hexadecimales.	El programa instalador genera aleatoriamente una cifra, pero da la opción al usuario de cambiarla. Elegimos “329DDACB”.
Elección del sistema de ficheros que soportará el servidor.	Nombres de ficheros con formato DOS. Nombres de ficheros con formato Netware.	Elegimos la opción recomendada por Novell: formato DOS.
Elección del controlador de discos.	Se elige un controlador de una lista desplegable capaz de acceder a discos y CD: IDE, SCSI, etc. Automáticamente se asignan los parámetros de configuración de la tarjeta controladora de discos (IRQ, Puerto de E/S, etc.).	Elegimos IDE.DSK, controlador de discos IDE. Si hubiera varios controladores hardware de distinta tecnología, habría que elegir varios controladores de software.
Elección del adaptador de red	Se elige un controlador que soporte la tarjeta de red y se configura con los parámetros apropiados.	Elegimos RTL8139.LAN, que es el controlador para una adaptador Realtek 8139 Fast Ethernet. Si hubiera varios adaptadores de red, habría que elegir varios controladores de software.
Elección de los protocolos de red	El protocolo IPX se instala de modo necesario. Son opcionales TCP/IP y AppleTalk.	La configuración de ambos sigue un esquema semejante al explicado en este tipo de redes.
Copia de ficheros de red al servidor.	Deben crearse las particiones Netware apropiadas para albergar los ficheros que componen el NOS.	Seguidamente se copian estos ficheros y se montan los volúmenes automáticamente.
Configuración del NDS.	Debe elegirse la creación de un nuevo árbol NDS o la incorporación a otro ya existente.	NDS (Netware Directory Service) es un sistema jerárquico de gestión de la red, en donde todos los recursos de la red se disponen en forma de árbol.
Creación de los ficheros de configuración de la red.	Una vez finalizada la instalación se crean los ficheros de configuración, que dependen de la versión del software de red.	Un ejemplo de alguno de estos ficheros se pueden ver a continuación, en concreto el fichero AUTOEXEC.NCF.

6 Redes de Macintosh

6.1 La familia de protocolos de Apple

AppleTalk es el nombre de la red entre iguales, diseñada por Apple Computer Corporation, para su utilización en ordenadores Macintosh y, más recientemente, en PowerMAC. El diseño original se pensó para permitir que se compartan ficheros e impresoras entre los usuarios de la red, de modo que su configuración fuera muy sencilla, lo que permitiría beneficiarse a cualquier usuario no experto de los servicios de red.

El primer diseño de AppleTalk fue una sencilla red que resolvía la conexión de un Macintosh a una impresora, sin embargo, con AppleTalk se pueden confeccionar redes muy amplias y complejas, si bien Apple siempre ha tratado de conservar la facilidad de instalación y configuración en sus desarrollos liderando la tecnología Plug & Play. Además, hay importantes sectores empresariales y docentes que han utilizado esta tecnología desde hace mucho tiempo. No hay que olvidar que los sistemas operativos de Apple para Macintosh siempre fueron gráficos y de fácil instalación.

La tabla siguiente esquematiza la arquitectura de protocolos utilizados por AppleTalk y su relación con las capas del modelo OSI.

Aplicación	AppleShare, LaserShare
Presentación	AFP, PostScript
Sesión	ASP, PAP, ZIP
Transporte	ATP, NBP
Red	DDP
Enlace	LLAP, ELAP, TLAP
Física	Cable de pares, coax, fibra ...

Aquí sólo describiremos brevemente algunos de estos protocolos:

- LLAP (LocalTalk Link Access Protocol), ELAP (Ethernet Link Access Protocol) y TLAP (Token Link Access Protocol) son los protocolos de nivel de enlace utilizados por AppleTalk, quien utilizará uno u otro dependiendo de la capa física, que será estudiada más adelante.

- DDP (Datagram Delivery Protocol) es el protocolo AppleTalk en el nivel de red que se encarga de encaminar los datagramas de modo semejante al protocolo IP de las redes UNIX. Las tablas de encaminamiento entre los diferentes encaminadore o routers se mantienen a través de un protocolo denominado RTMP (Routing Table Maintenance Protocol).

- NBP (Name Binding Protocol) es un protocolo situado en la capa de transporte que se encarga de asociar nombres de servicios con direcciones, de modo que los usuarios puedan utilizar nombres mnemotécnicos para solicitar los servicios de la red.

- ATP (AppleTalk Translation Protocol) es el protocolo de transporte encargado de realizar conexiones seguras en AppleTalk. Equivale al TCP de la red UNIX.

- ZIP (Zone Information Protocol) es un protocolo asociado a la capa de sesión que se encarga del gobierno de las zonas AppleTalk. El significado de «zona» será estudiado con el sistema de direccionamiento de la red.

- ASP (AppleTalk Session Protocol) es el protocolo de sesión encargado del gobierno de las sesiones, que elimina paquetes duplicados y los ordena según su número de secuencia.

- PAP (Printer Access Protocol) proporciona en el nivel de sesión los servicios de impresora para toda la red.

En capas superiores aparecen protocolos como **AFP** (AppleTalk Filing Protocol) para el intercambio de ficheros, y **PostScript** como lenguaje descriptor de documentos con que alimentar las impresoras. **AppleShare** y **LaserShare** se encargan de hacer de modo transparente al usuario (nivel de aplicación) del servicio de ficheros y de dispositivos de impresión, de modo que al usuario le parecen locales los discos, carpetas o impresoras que, en realidad, son remotos.

Los sistemas operativos de Apple soportan que en cada máquina, además de AppleTalk, se puedan instalar productos de red añadidos que permitan a los Macintosh comunicarse con nodos de la red con otra arquitectura de protocolos. Por ejemplo, es muy común instalar en un Macintosh la familia de protocolos TCP/IP. De hecho, TCP/ IP está englobado dentro del propio NOS de Apple con el nombre MacTCP.

Apple comercializa dos sistemas operativos que tienen el software de red incorporado: System 7 y MacOS.

6.2 Las redes de Macintosh

Los sistemas de red AppleTalk pueden ser clasificados atendiendo a su capa física del modo siguiente:

- **Red LocalTalk**. Es una red AppleTalk sobre cable serie que proporciona unas prestaciones de flujo moderadas, sin embargo, es una red muy barata, incorporada de serie en todos los Macintosh de cualquier gama, así como en las impresoras de Apple y en otros dispositivos. El sistema de cableado consiste en un bus lineal, como en el caso de Ethernet. La velocidad de transferencia es de 230 Kbps. El bus puede medir 300 metros como máximo y sólo permite la conexión de 32 dispositivos. El protocolo de nivel de enlace que gobierna esta capa física es LLAP (LocalTalk Link Access Protocol), aunque en la literatura de Apple también se le llama ALAP.

- **Red EtherTalk**. Cuando AppleTalk tiene una Ethernet en la capa física recibe el nombre de EtherTalk. Es más caro que LocalTalk y exige un adaptador de red conectado en un slot de expansión del ordenador. En los Macintosh de gama media y alta el adaptador de red viene incorporado en la placa madre del ordenador. Se permite cable coaxial fino o grueso y par trenzado. Es posible la conexión de más de 1.000 nodos al bus Ethernet y la velocidad de transferencia es la típica de Ethernet, es decir, 10 Mbps. Obviamente, no se excluye la incorporación de los modernos puertos Fast Ethernet, para conexiones de 100 Mbps. El protocolo de nivel de enlace en una red EtherTalk es ELAP.

- **Red TokenTalk**. Una red TokenTalk es una red AppleTalk en anillo del tipo Token Ring, por tanto, está basada en el estándar IEEE 802.5 y tiene sus mismas prestaciones. El nivel de enlace en TokenTalk está gobernado por el protocolo TLAP.

La evolución de las redes modernas ha permitido la incorporación a la familia AppleTalk de otros niveles físicos, como la posibilidad de AppIeTalk sobre FDDI a 100 Mbps.

6.3 El nivel de enlace en LocalTalk

Ya hemos estudiado en profundidad las tecnologías de red para Ethernet y para Token Ring, por tanto, aquí nos detendremos exclusivamente en el estudio de LocalTalk y de su protocolo LLAP.

LLAP o ALAP (*AppleTalk Link Access Protocol*) es un protocolo que utiliza sobre un bus de cables de pares la tecnología CSMA/CD para gobernar el tráfico de señales en la red. Hasta aquí se parece a Ethernet, sin embargo, el formato de trama es distinto.

Bandera	Dirección destino	Dirección fuente	Tipo de trama	Datos	FCS	Bandera

Veamos el significado de algunos campos. Los flags o banderas son semejantes a los de Ethernet, aunque su tamaño es de 2 bytes. El campo de datos puede tener una longitud máxima de 600 bytes. El campo FCS es el control CRC de trama y tiene una longitud de 2 bytes.

Los campos más característicos de ALAP son el de tipo de trama, cuya longitud es 1 byte, y los de direcciones fuente y destino, también de 1 byte cada uno. El campo de direcciones sólo puede contener 256 valores, de los cuales sólo se usan 254, esta es la razón por la que en una red LocalTalk sólo se puedan conectar 254 dispositivos desde el punto de vista lógico, aunque físicamente está limitado a los 32 a que aludíamos antes.

Cuando la estación de red se enciende, genera un número aleatorio como identificación de nodo y lo pone en un paquete que difunde por la red. Si algún otro nodo de la red tiene ya ese número, generará un paquete que avisará a la estación de que esa dirección ya está siendo utilizada. La estación generará otro número y repetirá la operación hasta que obtenga un número no utilizado por nadie en la red.

El campo de tipo de trama indica el significado de ésta, por ejemplo, existen tramas informativas, de confirmación, de petición de identificación de nodo (dirección), de solicitud de envío de datos (RTS), de concesión de envío de datos (CTS), etc.

LocalTalk utiliza el concepto RTS/CTS que ya hemos estudiado anteriormente, aunque implementa este sistema de control de flujo a través de las tramas que envía por la red y no mediante líneas especiales (líneas RTS y CTS): no debemos olvidar que ALAP es un protocolo orientado a bit. Cuando una estación necesita transmitir datos a otra, le envía previamente una trama RTS para solicitar permiso de transferencia de datos. Si la estación receptora lo considera oportuno, le contesta con una trama CTS que el emisor interpretará como «permiso concedido». Seguidamente se procederá al envío de datos mediante tramas informativas.

6.4 Direccionamiento de la red AppleTalk

6.4.1 Las zonas AppleTalk

Una zona AppleTalk es una agrupación lógica de estaciones que permite a los usuarios de la red visualizar los servicios de la red de modo fraccionado, lo que es especialmente útil cuando la red es grande. Es importante advertir que la zona no exige una delimitación física de los nodos que la componen, es estrictamente lógica.

Así, en la instalación de la única red de una empresa se podría crear una zona por cada departamento. Cuando un usuario visualiza los servicios de la red a través del "Selector" del NOS de Apple, el sistema presentará en el monitor los servicios de red de la zona que ha elegido, por defecto siempre se tomará la zona a la que pertenece el nodo en que está presentado el usuario.

A una zona pueden pertenecer nodos de la misma o de distinta red de área local, es totalmente transparente a los usuarios y cada nodo, en el caso de EtherTalk o TokenTalk, puede estar en una o más zonas. Con LocalTalk cada nodo puede ser asignado exclusivamente a una única zona. También se puede definir una zona por defecto en la que se inscribirán todos los dispositivos de red para los que no se defina una zona determinada.

6.4.1.1 El sistema de numeración de redes en AppleTalk

En AppleTalk cada red tiene asociado un número o un conjunto de números que la identifican, comprendidos entre 1 y 65.279. Una red LocalTalk sólo puede tener un número identificativo, cada uno de los cuales puede soportar hasta 254 nodos, por tanto, desde el punto de vista lógico, una red LocalTalk puede direccionar 254 nodos.

A una red EtherTalk o TokenTalk se le puede asignar un rango de números de red, y cada uno de estos números de red es capaz de direccionar 253 nodos en estos dos tipos de redes. Por ejemplo, si a una red EtherTalk le asignamos el rango 10-19, entonces podría direccionar hasta 10 x 253 = 2.530 nodos. Con este sistema de

identificación de nodos y de redes, AppleTalk puede direccionar redes de hasta 65.279 x 253 nodos, es decir, más de 16 millones de dispositivos de red.

Cuando se diseña una red AppleTalk hay que realizar un estudio previo sobre los equipos existentes y las posibilidades de crecimiento de la red, con el fin de no tener que modificar el sistema de numeración de la red, especialmente si son grandes. Por ejemplo, si realizamos una red con dos zonas A y B, interesa que el rango de números asignado a la red de la zona A esté separado del rango asignado a la red de la zona B. Podríamos asignar el rango 1-10 (2.530 nodos) a la zona A y el rango 21-30 (2.530 nodos) a la zona B, de modo que queda libre el rango 11-20 para posibles ampliaciones futuras, tanto de la zona A como de la B.

Todas estas características que hemos estudiado para las redes AppleTalk pertenecen a la fase 2 de dicha red, que es el tipo de red AppleTalk que Apple suministra en la actualidad con todos sus equipos.

6.4.2 Configuración de la red

La red completa su configuración cuando se definen los usuarios y los servicios que debe prestar. Los servicios Apple son similares a los que proporcionan otras redes.

En primer lugar, hay que definir los derechos de acceso de los usuarios a los ficheros.

Los servicios de ficheros e impresoras de la red utilizan el «selector» de Apple para realizar las conexiones adecuadas. Como estos servicios pueden residir en otros sistemas, los fabricantes suelen proporcionar software añadido para realizar estos accesos.

7 Redes de Microsoft

Microsoft dispone de diversos sistemas operativos para resolver las comunicaciones en las redes de área local. Su sistema operativo servidor se llama Windows NT Advanced Server. Para las estaciones de trabajo posee distintos sistemas: Windows NT workstation, Windows 95/98 y Windows para trabajo en grupo (versión 3.11). Además, sobre otras versiones de Windows, por ejemplo, sobre la versión 3.1, se pueden instalar productos de red, tanto de Microsoft como de otros fabricantes.

7.1 Protocolos utilizados por Microsoft

Las redes de Microsoft suelen utilizar protocolos propuestos por otros fabricantes, especialmente en cuanto a transporte se refiere. Microsoft propone los tres siguientes posibles transportes:

- **Protocolo NetBEUI** (*NetBIOS Extended User Interface*). Da soporte para pequeñas redes y es un protocolo de transporte simple y fácil de utilizar. Sólo 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**. Ha sido construido por Novell para su sistema Netware. Da soporte para redes pequeñas y medianas y con él 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 está presente una red de área extendida.

Microsoft permite además la incorporación de otros protocolos para conexiones específicas, como el DLC, requerido por algunos sistemas, los de AppleTalk para interconexión con redes de Apple, etc.

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

- Si la red es pequeña y no se prevé un crecimiento considerable a corto plazo, es posible poner NetBEUI.
- 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, entonces el protocolo más apropiado es TCP/IP.

Hemos de tener en cuenta que la instalación de cualquiera de estos protocolos no impide la inclusión de cualquier otro, es decir, podemos tener cualquier combinación de todos ellos: la tecnología de redes propuesta por Microsoft, por ejemplo, la especificación NDIS, permite el mantenimiento de diferentes pilas de protocolos sobre la misma o distintas tarjetas de red, lo que hace que sus redes sean extraordinariamente flexibles.

7.1.1 El protocolo NetBEUI

Los sistemas operativos de Microsoft son una base para la construcción de redes entre iguales. Cada sistema operativo de red debe prever el envío y recepción de datos entre los diferentes nodos. NetBEUI es un protocolo, entre los muchos posibles, encargado de realizar esto.

Algunos protocolos se encargan exclusivamente de la manipulación de datos, otros, en cambio, se ocupan del intercambio de mensajes entre las aplicaciones de red. NetBEUI es un protocolo que controla tanto a los datos como a los mensajes entre aplicaciones.

NetBEUI fue desarrollado por IBM en 1985 como un protocolo que utiliza el sistema de ventanas de comunicación, tanto en el receptor como en el emisor, lo que le hace eficaz en las transmisiones de redes de área local, para las que está optimizado. NetBEUI ajusta los parámetros de la ventana de recepción y de emisión automáticamente, dependiendo de las condiciones en que se tenga que producir la transmisión.

Cuando un sistema operativo de red implementa el protocolo NetBEUI, los servicios son alcanzados a través del interface NetBIOS. En las redes de Microsoft, el acceso a las tarjetas de red se suele realizar a través de interface NDIS, aunque no se excluye la tecnología ODI.

7.2 Resolución de nombres en redes de Microsoft

Las redes de Microsoft utilizan distintos sistemas de nombres para establecer las conexiones entre los diferentes nodos y dispositivos remotos. Cada nodo, dispositivo servido en la red, impresora o servicio, debe poseer un nombre que lo identifique. Para ello, es necesario que cada equipo que vaya a realizar una conexión conozca la dirección del nodo que brinda el servicio. Los equipos acceden a la red a través de su adaptador de red, cuyo parámetro fundamental es una dirección física, por ejemplo, la dirección MAC en una red Ethernet.

Resolver nombres en una red significa averiguar la asociación que existe entre ellos en la red y la dirección física o lógica (depende del sistema) con que se asocia. Cada nombre utilizado en una red debe ser único para esa red.

El primer sistema de nombres es el propuesto por el interface NetBIOS, que es un sistema de nombres planos, es decir, no articulados por varias palabras. Cada nombre (palabra) identifica a un ordenador o a un servicio. Por ejemplo, nombres válidos según NetBIOS podrían ser: JIMENA, HAL9000, TALLER, CIC03, TANAKA, etc.

El segundo sistema es DNS y está propuesto según los protocolos TCP/IP, que se han estudiado anteriormente al analizar las redes TCP/IP como un sistema de nombres articulado.

Microsoft permite una asociación entre nombres NetBIOS y nombres DNS. De hecho, en sus sistemas incorpora la posibilidad de que un nombre DNS acabe resolviéndose en un sistema gestor de nombres NetBIOS a través de un servicio WINS.

Por ejemplo, si queremos realizar una conexión remota por medio de una emulación de terminal (terminal virtual) contra un ordenador llamado VENUS como nombre NetBIOS o venus.solar.via_lactea.es como nombre DNS con dirección IP 128.200.5.90, podríamos escribir cualquiera de los siguientes comandos (la aplicación de terminal virtual se llama TELNET):

TELNET VENUS

TELNET venus.solar.via_lactea.es

TELNET 128.200.5.90

El sistema operativo se encargará de resolver estos nombres utilizando los servicios antes indicados, de modo que la conexión se efectúe contra el nodo adecuado que ha sido identificado por cualquiera de estos sistemas de nombres.

Los sistemas operativos de Microsoft pueden resolver nombres con diversas soluciones de software:

- **Servicio WINS o Servicio de Nombres de Internet de Windows**. Gestiona la asociación de nombres NetBIOS con direcciones IP.

- **Servicio DNS o Sistema de Nombres de Dominio**. Se encarga de la asociación de nombres DNS con direcciones IP.

7.3 Otros servicios de las redes de Microsoft

Microsoft Windows NT Advanced Server, la versión de servidor de Windows NT permite otros servicios relacionados con el direccionamiento de las redes. Algunos de ellos ya se han estudiado anteriormente, pues tienen una relación directa e importante con las redes TCP/IP. Algunos de estos servicios son los siguientes:

- **Servicio DHCP**. Es propio de redes UNIX y asigna direcciones IP a los nodos dinámicamente, asegurando que dos nodos no tendrán nunca la misma dirección IP en la misma red.

- **Servicio BOOTP, *Bootstrap Protocol* o protocolo de inicialización**. Permite la configuración del arranque remoto de una estación sin disco. Sólo habría que especificar parámetros como la dirección IP de la estación, la dirección de un gateway y la de un servidor.

- **Servicio SNMP, *Simple Network Management Protocol***. Es un protocolo de gestión de red, que se está extendiendo por todas las plataformas informáticas.

Además de estos servicios, tanto los servidores como los clientes de Microsoft, incorporan protocolos de acceso a Internet, como SLIP, PPP, HTTP, PPTP, etc.

7.4 Configuración de la red

La configuración de la red exige la instalación del sistema operativo, lo que implica acudir a los manuales de instalación que proporciona el fabricante con el software del sistema.

Microsoft tiene integrado el software de red en sus sistemas operativos, de modo que la instalación de la red se puede realizar cuando se instala el sistema. Esto no es obstáculo para poder modificar la configuración de la red en cualquier otro momento.

7.4.1 Configuración del adaptador de red

La primera decisión que hay que tomar es la elección del adaptador, de red. Para ello, Microsoft dispone de controladores de red optimizados para un gran número de tarjetas. En caso de que no existiera el controlador adecuado, Microsoft deja al fabricante la posibilidad de incorporar su propio software a través de un disquete.

Después de elegido el controlador, hay que configurar el adaptador con los parámetros apropiados (IRQ y Dirección base de E/S), según hemos visto anteriormente.

7.4.2 Las agrupaciones en la red de Microsoft

Un dominio Microsoft es un grupo de ordenadores que comparten la misma base de datos de cuentas de usuario, privilegios, derechos de acceso, seguridad, etc., dentro de este mismo grupo. A la gestión de todos estos elementos se le llama «servicio de directorio».

Una vez instalado el software básico para el adaptador de red, debemos decidir si el ordenador que estamos instalando pertenecerá o no a un dominio ya existente. En el caso de que estemos instalando un servidor, cabe la posibilidad de que se una a otro dominio como un servidor más o se constituya como base de un nuevo dominio.

También cabe la posibilidad de que el ordenador sea miembro de un grupo de trabajo. En estos casos, cada ordenador del grupo es propietario de sus propias cuentas de usuario. El grupo de trabajo sólo sirve como agrupador de servicios al examinar la red. También se debe especificar el nombre NetBIOS de la computadora, que debe ser definido de modo unívoco en cada red.

7.4.3 Tipos de servidores

Hay tres tipos posibles de instalación para un servidor de Microsoft:

- **Controlador primario**. Un servidor es controlador primario de dominio cuando tiene en posesión la base de datos de los servicios de directorio. Todos los dominios tienen que poseer un controlador primario.

- **Controlador de reserva**. Un servidor es controlador de reserva de un dominio si almacena una copia de seguridad de la base de datos de los servicios de directorio. Cuando el controlador primario de un dominio está fuera de servicio, el de reserva puede tomar sus funciones.

- **Servidor no controlador**. Es el caso de un servidor que pertenece al dominio pero que actúa como una estación normal a la que se añaden los servicios propios del servidor Windows NT, por tanto, no comparte el sistema de cuentas.

8 Utilidades para sistemas con protocolos TCP/IP

Las siguientes utilidades son comunes en los sistemas UNIX. Otros sistemas operativos las incorporan en alguna medida si llevan instalado TCP/IP. Los ejemplos que se exponen a continuación han sido ejecutados sobre Windows NT. Las respuestas del equipo en otros sistemas son análogas.

- Utilidad **ping**.- 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. 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.

- Utilidad **arp**.- Se emplea para asignar direcciones IP a direcciones físicas, es decir, para gestionar el protocolo ARP.

- Utilidad **lpq**.- Se utiliza para preguntar por el estado de impresoras remotas que utilicen protocolo TCP/IP en sus comunicaciones.

- Utilidad **hostname**.- Devuelve el nombre del nodo en el que se ejecuta.

- Utilidad **ipconfig**.- Configura la dirección del host, o bien proporciona información sobre la configuración actual.

- Utilidad **nbtstat**.- Sirve para gestionar los nombres NetBIOS de nodos concretos.

- Utilidad **netstat**.- Proporciona información sobre el estado de la red. Con el comando ejecutado en la Figura 6.19 se obtiene información estadística sobre los paquetes de red enviados y recibidos.

- Utilidad **route**.- Sirve para determinar las rutas que deben seguir los paquetes de red.

- Utilidad **tracert**.- Se emplea para controlar los saltos de red que deben seguir los paquetes hasta alcanzar su destino. Además, proporciona información sobre otros parámetros de la internet.

- Utilidad **finger**.- Sirve para determinar si un usuario está presentado o no en un nodo TCP/IP. Por ejemplo, si necesitamos saber si el usuario «alfredo» está presentado en el nodo 128.100.10 ejecutaremos el comando siguiente:

  finger alfredo @128.100.10.2

- Utilidades **ftp** y **tftp**.- La utilidad ftp sirve para intercambiar ficheros entre dos nodos de la red utilizando el protocolo FTP estudiado anteriormente. Cuando se ejecuta ftp, aparece la marca «FTP>» sobre la que se ejecutan los comandos ftp: listar, traer o dejar ficheros, etc. Previamente a la utilización de FTP es necesario hacer 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, pero más fácil de configurar.

- Utilidad **lpr**.- Se utiliza para enviar trabajos a las impresoras remota que se especifican como argumentos.

- Utilidades **rexec** y **rsh**.- Son utilizadas para ejecutar desde la máquina local comandos UNIX en una máquina remota.

  rexec 128.100.10.2 -1 alfredo ls -las

- Utilidad **telnet**.- 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.

9 Instalación de una red

A continuación estudiaremos los pasos que hay que seguir para instalar una red a partir de unas especificaciones de diseño surgidas como consecuencia de un análisis de las necesidades. Este epígrafe tiene como objeto servir de pauta para llevar a cabo el proyecto de construcción de una red de área local concreta.

Supongamos que queremos implantar una red de área local en el ámbito de las oficinas de una empresa.

9.1 Análisis de necesidades

El primer paso que hay que dar es la realización de un análisis de necesidades. Si en cualquier organización se ha decidido instalar una red de área local, será porque hay una serie de causas que la hacen conveniente. Por tanto,

habrá que investigar cuáles son estas causas y qué tipo de problemas tratan de solucionar con la implantación de la LAN.

Para ello será conveniente fijarse, al menos, en los siguientes aspectos:

- ¿Cómo realiza actualmente el trabajo?
- ¿Con qué volumen de datos trabajan habitualmente?
- ¿Cuáles son los procedimientos de operación más comunes?
- ¿Qué esperan conseguir con la implantación de la red?
- ¿Qué volumen de usuarios trabajarán con la red?

9.2 Instalación existente

En ocasiones en la implantación de una red de área local no se parte de cero, sino que se trata de la ampliación o modificación de una red existente. Es de vital importancia, por tanto, averiguar el tipo de instalación que tienen en uso, qué problemas solucionan con esa red y cuáles son las principales dificultades con que se encuentran.

En el diseño de la red que vayamos a realizar habrá que tener en cuenta el hardware y software que existe para que sean integrados, si es conveniente, con los nuevos elementos de diseño. En ocasiones es imprescindible perder alguna funcionalidad en la nueva red para permitir la integración de elementos tecnológicamente más antiguos, pero que hagan menos traumática la transición.

9.3 Diseño de la red y de los servicios

Una vez determinadas las necesidades, hay que dar una respuesta que intente solventar los problemas de modo asequible. Para ello hay que dar una solución, que llamaremos diseño de la red, y que realizaremos en forma de proyecto de instalación. En el diseño intervendrán distintos elementos: hardware, software, servicios, interconexión con el exterior, tiempo de instalación, etc.

9.3.1 El hardware

Debe hacerse un análisis del hardware necesario para dar respuesta a las necesidades de los usuarios. Esto implica la elección de una plataforma de hardware o una combinación de plataformas (PC, Macintosh, estaciones UNIX, etcétera).

Cabe distinguir varios análisis de hardware en función de si estudiamos los servidores, las estaciones o la red misma. La tabla siguiente trata de describir esquemáticamente los elementos necesarios en cada uno de estos análisis.

Hardware	Configuración	Observaciones
CPU	Un procesador o un sistema de multiprocesadores según la potencia necesitada.	Interesa CPU de altas prestaciones que sean capaces de desarrollar un gran flujo de Entrada/Salida.
Memoria	32 Mbytes o más, dependiendo del sistema operativo.	Si se van a exigir altas prestaciones, interesan configuraciones de muchos más Mbytes de memoria (128 o 256 Mbytes). Para las estaciones de trabajo las necesidades de memoria son menores (8 a 32 Mbytes).

Hardware	Configuración	Observaciones
Discos	Interfaces de conexión rápidos: SCSI o similar. Si se diseña un sistema de seguridad interesan discos RAID. La capacidad debe ser, al menos, un 50 por 100 mayor que la que originalmente se considere necesaria para que el sistema no quede obsoleto en poco tiempo.	La velocidad de acceso debe ser lo más elevada posible. También debe ser rápido el bus de comunicaciones entre CPU y controlador de disco. En el caso de estaciones de trabajo, habrá que decidir si llevarán o no disco. Si llevan disco, hay que definir para qué se utilizará: sólo para paginar (memoria vitual) o si también contendrán datos de usuario y aplicaciones.
Adaptador de red	Si se prevé un gran flujo de datos, es interesanta que el adaptador sea de alta velocidad (100 Mbps). Además, el interface de conexión con la unidad central debe ser rápido (PCI, por ejemplo). Se debe configurar la tarjeta en función del resto del hardware del servidor: IRQ, DMA, etc. En ocasiones habrá que instalar más de un adaptador de red. Si ocurre así, debemos asegurarnos de que el software lo permitirá.	El adaptador dependerá del modelo de red que hayamos elegido: Ethernet, Token Ring, etc., lo que a su vez, dependerá de otros factores: estructura física del edificio, posibilidades de cablear, prestaciones que se desean conseguir, etc. Interesa hacerse un esquema con todas las características de configuración del hardware del servidor.
Topología de la red	Hay que elegir una de las topologías básicas de red, estudiadas en anteriores unidades de trabajo.	La decisión se toma en función de las ventajas e inconvenientes que presentan cada una de ellas.
Cableado de red	Según la topología de la red y su tecnología tendremos que elegir un tipo de cable u otro.	Al diseñar el cableado de red habrá que decidir si se pone o no cableado estructurado, puesto que esto condiciona en gran medida la instalación.

9.3.2 El software

El software de red exige tomar decisiones sobre los sistemas operativos. En ocasiones se elige primero el hardware y después el software, pero otras veces se hace al revés. Una vez elegido el hardware, queda condicionado el software, pues éste debe ser apropiado para aquél. Algunos sistemas operativos modernos, como Windows NT, pueden correr sobre distintas plataformas de hardware, lo que atenúa este problema en gran medida.

Hardware	Configuración	Observaciones
Sistema operativo de red	Se elige en función del hardware. Además, hay que decidir si el sistema será dedicado o no y si necesitamos una red entre iguales o cliente-servidor. Hay que hacer un análisis del volumen ocupado por el sistema operativo y de los protocolos de red que incorpora.	El sistema operativo del servidor no tiene por qué ser igual que el de las estaciones clientes. De hecho, lo normal es que sean diferentes. Si en la red no se parte de cero, habrá que elegir software compatible con las versiones instaladas anteriormente.
Software añadido sobre el sistema	Puede que sea necesaria la incorporación de nuevo software operativo para dar respuesta a todos los servicios requeridos por los usuarios. Por ejemplo, un NOS que tenga que comunicarse con Macintosh requerirá, probablemente, la instalación de un software especial.	Hay que hacer un análisis de compatibilidad entre todas las piezas de software. También hay que asegurarse de que los protocolos añadidos proporcionarán los servicios requeridos.
Aplicaciones de usuario	Hay que asegurarse de la compatibilidad entre el sortware de red y las aplicaciones de los usuarios, especialmente si se deben usar interfaces de aplicaciones como NetBIOS o los sockets del TCP/IP	Además, hay que comprobar que las aplicaciones que habitualmente utilizan los usuarios seguirán corriendo sin problemas, o bien serán actualizadas. Por ejemplo, el correo electrónico.

9.3.3 Los servicios

Seguidamente hay que determinar qué tipo de servicios serán necesarios en la red. La tabla siguiente puede orientarnos en su elección.

Hardware	Configuración	Observaciones
Discos	Deben planificarse los nombres de los discos y su situación en los servidores de la red.	Este tipo de servicio es el más común en las redes de área local. Interesa que los servicios estén distribuidos por todos los discos de la red con el fin de balancear la carga de cada uno de ellos. Es útil la instalación en el servidor de alguna utilidad para realizar copias de seguridad (backup).
Impresoras	Su configuración es análoga a la de los discos; sin embargo, tienen algún matiz distinto relativo al tipo de dispositivo impresor: no todas las impresoras son iguales, ni utilizan los mismos controladores.	Se pueden planificar impresoras de baja, media o alta calidad; de color o blanco y negro; de alta o de baja velocidad; gráficas o alfanuméricas; etc. Las impresoras se pueden distribuir por todas las estaciones para facilitar el acceso a los usuarios, sin necesidad de grandes desplazamientos.
Correo electrónico	Hay que establecer el tipo de correo electrónico que utilizarán los usuarios: si necesitan agentes externos o no (por ejemplo, Internet), si habrá aplicaciones que lo utilicen, etc.	Esto exige la instalación de los clientes de correo, quizá de algún servidor de correo y, por supuesto, los protocolos de acceso a las oficinas de correo.
Interface de aplicaciones	Si las aplicaciones de los usuarios utilizan directamente la red, habrá que asegurarse de que están instalados los interfaces de NetBIOS, sockets o similares.	Los manuales que suministra el fabricante de cada aplicación contienen información sobre el tipo de software de red requerido para el correcto funcionamiento de la aplicaciones.

9.3.4 Conexiones con el exterior

Si la red debe estar conectada con otras hay que prever cómo se realizará esta interconexión: líneas punto a punto o multipunto, conexión RTB o RDSI, así como la velocidad de comunicación, volumen de datos que se van a transferir, etc.

Este tipo de decisiones serán explicadas en profundidad al estudiar las redes de área extendida.

9.4 Ejecución del diseño

Ahora se trata de poner en marcha lo que se diseñó en la fase previa. Para ello, hay que asegurarse de que la instalación de fluido eléctrico es correcta. Un fallo en el suministro eléctrico puede malograr cualquier instalación de red: las líneas de datos son muy sensibles a este tipo de problemas. En general, es conveniente la asistencia de un electricista que supervise la instalación, asegurándose de que las tensiones son correctas, de que la instalación aguantará el flujo de corriente eléctrica y, sobre todo, que las diferentes tierras de las instalaciones eléctricas tienen el mismo nivel.

Posteriormente se tiende el cableado de datos (par trenzado, coaxial, fibra óptica, etc.), según el plan decidido en la fase de diseño. Esto exige la instalación de algún rack, del cableado estructurado, de los conectores apropiados, etcétera. Debe probarse cada uno de los cables antes de la puesta en funcionamiento final.

Después se instalan los equipos, tanto el hardware como el software. Se dan de alta los distintos servicios, se configuran los diversos protocolos, se crean las cuentas y directorios de usuario, se instalan las aplicaciones, etc.

En ocasiones, cuando se trata de una ampliación de red o de la sustitución de un servidor por otro, es necesario salvar los datos de los usuarios para hacer el cambio. Una vez realizado, hay que restituir los datos a la nueva configuración.

9.5 Seguridad

La siguiente fase es la confección de la seguridad de la red: dar los permisos apropiados a los usuarios sobre cada recurso de red, determinar los derechos de acceso a las aplicaciones y, en general, evitar intrusiones (accidentales o no) a lugares de los sistemas de ficheros no autorizados.

9.6 Puesta en marcha y pruebas

Una vez completada la instalación se pasa a la fase de pruebas. Dada la importancia de los servidores de red para todos los clientes de la red, es necesario diseñar un sistema de pruebas para garantizar que los servicios de la red están disponibles y funcionan correctamente para todos los usuarios que deben servirse de ellos.

Una vez realizadas las pruebas de funcionamiento, es posible que haya que retocar el diseño original de la red, ajustándose mejor a las necesidades.

9.7 Régimen de explotación

Una vez probada la red, se puede proceder a su explotación. Existen utilidades que ayudan a los administradores de red a tomar decisiones sobre posibles mejoras en el rendimiento de la red. Estas utilidades ofrecen datos estadísticos que aconsejan la mejora en puntos concretos, que actúan a modo de cuello de botella: mejoras en el rendimiento de la CPU, accesos a los discos, flujo de datos por los distintos segmentos de red, etc.