

*para el*  
*Centro de formación Profesional N° 401 de caseros*

<b>1.1 Concepto de red y clasificaciones .....</b>	<b>1</b>
Clasificación según su tamaño: LAN, MAN y WAN .....	1
Clasificación según su distribución lógica .....	2
<b>1.2 Conmutación de circuitos, de mensajes y de paquetes.....</b>	<b>2</b>
<b>1.3 Comunicación simplex, half-duplex y full-duplex .....</b>	<b>3</b>
<b>1.4 Mecanismos de detección de errores .....</b>	<b>3</b>
Paridad .....	4
CRC .....	4
<b>1.5 Control de flujo .....</b>	<b>5</b>
<b>1.6 Modelo de referencia OSI. Comparación con el modelo TCP/IP ..</b>	<b>5</b>
<b>1.7 Capa física: medios de transmisión .....</b>	<b>9</b>
Cable coaxial .....	10
Cable par trenzado .....	10
Cable de fibra óptica .....	11
<b><i>Capítulo 2 Instalación de cableado .....</i></b>	<b><i>11</i></b>
<b>2.2 Cable par trenzado .....</b>	<b>11</b>
Cable par trenzado directo .....	11
Cable par trenzado cruzado .....	12
<b>2.3 Comparación entre hub y switch.....</b>	<b>12</b>
¿Cómo sabe un switch los ordenadores que tiene en cada rama? .....	13
Dominios de colisión .....	14
¿Qué instalar hubs o switches? .....	14
<b>2.4 Interconexión de hubs .....</b>	<b>14</b>
<b><i>Capítulo 3 Protocolos .....</i></b>	<b><i>15</i></b>
<b>3.1 Protocolos de la capa de acceso al medio .....</b>	<b>15</b>
Token ring (802.5).....	16
Ethernet (802.3) .....	17
Direcciones físicas .....	18
Formato de la trama .....	19
Velocidades .....	19
Tipos de adaptadores .....	20
<b>3.2 Protocolos de las capas de red y transporte .....</b>	<b>20</b>
IPX/SPX .....	20
AppleTalk.....	21
NetBEUI .....	21

TCP/IP.....	22
<b>Capítulo 4 Redes en Windows 98.....</b>	<b>23</b>
<b>4.1 Protocolo NetBIOS.....</b>	<b>23</b>
Cómo deshabilitar NetBIOS en Windows 98 .....	24
<b>4.2 Instalación de una red en Windows 98 .....</b>	<b>25</b>
Contraseña de red Microsoft y contraseña de Windows.....	27
<b>4.3 Cómo acceder a recursos compartidos .....</b>	<b>28</b>
<b>4.4 Cómo compartir carpetas y unidades de disco .....</b>	<b>29</b>
<b>4.5 Unidades de red .....</b>	<b>29</b>
<b>4.6 Cómo instalar una impresora en red .....</b>	<b>30</b>
<b>4.7 Programas de monitorización de la red .....</b>	<b>31</b>
Monitor de red.....	31
Monitor del sistema.....	31
<b>4.8 Resolución de nombres .....</b>	<b>31</b>
Distinción entre nombres NetBIOS y nombres de dominio.....	32
Métodos de resolución de nombres NetBIOS.....	32
Métodos de resolución de nombres de dominio.....	33
<b>4.9 Configuración manual de ICS .....</b>	<b>34</b>
Configuración del servidor proxy: .....	34
Configuración de los clientes:.....	35
<b>Capítulo 5 TCP/IP .....</b>	<b>35</b>
Introducción.....	35
<b>5.1 Capa de red.....</b>	<b>36</b>
Direcciones IP.....	38
Direcciones IP especiales y reservadas.....	40
Máscara de subred .....	42
<b>5.1.1 Protocolo IP .....</b>	<b>46</b>
Formato del datagrama IP .....	46
Fragmentación.....	48
<b>5.1.2 Protocolo ARP .....</b>	<b>49</b>
Tabla ARP (caché ARP) .....	50
<b>5.1.3 Protocolo ICMP .....</b>	<b>51</b>
Encaminamiento.....	56
<b>5.2 Capa de transporte.....</b>	<b>59</b>
Puertos.....	60
<b>5.2.1 Protocolo UDP.....</b>	<b>61</b>
<b>5.2.2 Protocolo TCP.....</b>	<b>62</b>

Nombres de dominio .....	68
--------------------------	----

# Capítulo 1

## Introducción a las redes

### *1.1 Concepto de red y clasificaciones*

Una red es un sistema de transmisión de datos que permite el intercambio de información entre ordenadores. Si bien esta definición es demasiado general, nos sirve como punto de partida. La información que pueden intercambiar los ordenadores de una red puede ser de lo más variada: correos electrónicos, vídeos, imágenes, música en formato MP3, registros de una base de datos, páginas web, etc. La transmisión de estos datos se produce a través de un medio de transmisión o combinación de distintos medios: cables de fibra óptica, tecnología inalámbrica, enlaces vía satélite (el intercambio de información entre ordenadores mediante disquetes no se considera una red).

En la definición anterior hemos indicado el término ordenadores en un intento por simplificar. Sin embargo, los ordenadores son sólo una parte de los distintos dispositivos electrónicos que pueden tener acceso a las redes, en particular a Internet. Otros dispositivos de acceso son los asistentes personales (PDA) y las televisiones (Web TV). Incluso, ya existen frigoríficos capaces de intercambiar información (la lista de la compra) con un supermercado virtual.

Nota: En la práctica el término "red" se suele utilizar con una acepción distinta a la que hemos visto. A partir del siguiente capítulo cada vez que lo usemos nos estaremos refiriendo a un conjunto de máquinas con la misma dirección de red. La dirección de red está relacionada con la configuración lógica que hagamos a las máquinas no con la disposición del cableado. Lo habitual es que las empresas tengan solamente una red, aunque también pueden tener varias con objeto de facilitar su administración o mejorar su seguridad. Las redes se conectan mediante encaminadores (routers). Esto es precisamente lo que queremos significar cuando hablamos de que Internet es la Red de redes.

### **Clasificación según su tamaño: LAN, MAN y WAN**

Las redes LAN (Local Area Network, redes de área local) son las redes que todos conocemos, es decir, aquellas que se utilizan en nuestra empresa. Son redes pequeñas, entendiendo como pequeñas las redes de una oficina, de un edificio... Debido a sus limitadas dimensiones, son redes muy rápidas en las cuales cada estación se puede comunicar con el resto.

Las redes WAN (Wide Area Network, redes de área extensa) son redes punto a punto que interconectan países y continentes. Por ejemplo, un cable submarino entre Europa y América, o bien una red troncal de fibra óptica para interconectar dos países. Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos.

Como vemos, las redes LAN son pequeñas y las redes WAN, muy grandes: debe existir algún término para describir unas redes de tamaño intermedio. Esto es, las redes MAN (Metropolitan Area Network, redes de área metropolitana). Un ejemplo es la red utilizada en una pequeña población de la Comunidad Valenciana, Villena, para interconectar todos sus comercios, hogares y administraciones públicas (proyecto InfoVille).

## Clasificación según su distribución lógica

Todos los ordenadores tienen un lado cliente y otro servidor: una máquina puede ser servidora de un determinado servicio pero cliente de otro servicio.

- **Servidor.** Máquina que ofrece información o servicios al resto de los puestos de la red. La clase de información o servicios que ofrezca determina el tipo de servidor que es: servidor de impresión, de archivos, de páginas web, de correo, de usuarios, de IRC (charlas en Internet), de base de datos...
- **Cliente.** Máquina que accede a la información de los servidores o utiliza sus servicios. Ejemplos: Cada vez que estamos viendo una página web (almacenada en un servidor remoto) nos estamos comportando como clientes. También seremos clientes si utilizamos el servicio de impresión de un ordenador remoto en la red (el servidor que tiene la impresora conectada).

Dependiendo de si existe una función predominante o no para cada puesto de la red, las redes se clasifican en:

- Redes cliente/servidor. Los papeles de cada puesto están bien definidos: uno o más ordenadores actúan como servidores y el resto como clientes. Los servidores suelen coincidir con las máquinas más potentes de la red. No se utilizan como puestos de trabajo. En ocasiones, ni siquiera tienen monitor puesto que se administran de forma remota: toda su potencia está destinada a ofrecer algún servicio a los ordenadores de la red. Internet es una red basada en la arquitectura cliente/servidor.
- Redes entre iguales. No existe una jerarquía en la red: todos los ordenadores pueden actuar como clientes (accediendo a los recursos de otros puestos) o como servidores (ofreciendo recursos). Son las redes que utilizan las pequeñas oficinas, de no más de 10 ordenadores.

## 1.2 Conmutación de circuitos, de mensajes y de paquetes

La comunicación entre un origen y un destino habitualmente pasa por nodos intermedios que se encargan de encauzar el tráfico. Por ejemplo, en las llamadas telefónicas los nodos intermedios son las centralitas telefónicas y en las conexiones a Internet, los routers o encaminadores. Dependiendo de la utilización de estos nodos intermedios, se distingue entre conmutación de circuitos, de mensajes y de paquetes.

- En la conmutación de circuitos se establece un camino físico entre el origen y el destino durante el tiempo que dure la transmisión de datos. Este camino es exclusivo para los dos extremos de la comunicación: no se comparte con otros usuarios (ancho de banda fijo). Si no se transmiten datos o se transmiten pocos se estará infrutilizando el canal. Las comunicaciones a través de líneas telefónicas

analógicas (RTB) o digitales (RDSI) funcionan mediante conmutación de circuitos.

- Un mensaje que se transmite por conmutación de mensajes va pasando desde un nodo al siguiente, liberando el tramo anterior en cada paso para que otros puedan utilizarlo y esperando a que el siguiente tramo esté libre para transmitirlo. Esto implica que el camino origen-destino es utilizado de forma simultánea por distintos mensajes. Sin embargo, éste método no es muy útil en la práctica ya que los nodos intermedios necesitarían una elevada memoria temporal para almacenar los mensajes completos. En la vida real podemos compararlo con el correo postal.

- Finalmente, la conmutación de paquetes es la que realmente se utiliza cuando hablamos de redes. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente desde el origen al destino. De esta manera, los nodos (routers) no necesitan una gran memoria temporal y el tráfico por la red es más fluido. Nos encontramos aquí con una serie de problemas añadidos: la pérdida de un paquete provocará que se descarte el mensaje completo; además, como los paquetes pueden seguir rutas distintas puede darse el caso de que lleguen desordenados al destino. Esta es la forma de transmisión que se utiliza en Internet: los fragmentos de un mensaje van pasando a través de distintas redes hasta llegar al destino.

### ***1.3 Comunicación simplex, half-duplex y full-duplex***

- En una comunicación simplex existe un solo canal unidireccional: el origen puede transmitir al destino pero el destino no puede comunicarse con el origen. Por ejemplo, la radio y la televisión.

- En una comunicación half-duplex existe un solo canal que puede transmitir en los dos sentidos pero no simultáneamente: las estaciones se tienen que turnar. Esto es lo que ocurre con las emisoras de radioaficionados.

- Por último, en una comunicación full-duplex existen dos canales, uno para cada sentido: ambas estaciones pueden transmitir y recibir a la vez. Por ejemplo, el teléfono.

### ***1.4 Mecanismos de detección de errores***

¿Cómo puede saber el receptor que ha recibido el mismo mensaje que envió el emisor? ¿Cómo puede saber que no se ha producido ningún error que haya alterado los datos durante la transmisión? Estas cuestiones son las que vamos a plantear en este apartado: se necesitan mecanismos de detección de errores para garantizar transmisiones libres de errores. Si el receptor detecta algún error, puede actuar de diversas maneras según los protocolos que esté utilizando. La solución más sencilla es enviarle un mensaje al emisor pidiéndole que le reenvíe de nuevo la información que llegó defectuosa.

Los mecanismos de detección se basan en añadir a las transmisiones una serie de bits adicionales, denominados bits de redundancia. La redundancia es aquella parte del mensaje que sería innecesaria en ausencia de errores (es decir, no aporta información nueva: sólo permite detectar errores). Algunos métodos incorporan una redundancia capaz de corregir errores. Estos son los mecanismos de detección y corrección de errores.

Como ejemplos de mecanismos de detección de errores vamos a estudiar a continuación la paridad y los códigos CRC.

## Paridad

Las transmisiones se dividen en palabras de cierto número de bits (por ejemplo, 8 bits) y se envían secuencialmente. A cada una de estas palabras se le añade un único bit de redundancia (bit de paridad) de tal forma que la suma de todos los bits de la palabra sea siempre un número par (paridad par) o impar (paridad impar).

El emisor envía las palabras añadiendo los correspondientes bits de paridad. El receptor comprobará a su llegada que la suma de los bits de la palabra incluyendo la redundancia es un número par (si la codificación convenida entre emisor-receptor es de paridad par) o un número impar (paridad impar). Si el receptor encuentra alguna palabra que no se ajuste a la codificación establecida, le solicitará al emisor que le reenvíe de nuevo la información.

La paridad únicamente permite detectar errores simples, esto es, que varíe un único bit en cada palabra. Si varían 2 bits, este mecanismo no es capaz de detectar el error.

Veamos un ejemplo de paridad par:

Datos (8 bits)	Datos + redundancia (9 bits)	Suma de bits
10110110	10110110 <b>1</b>	6
00101001	00101001 <b>1</b>	4
11001001	11001001 <b>0</b>	4
11111010	11111010 <b>0</b>	6
00010000	00010000 <b>1</b>	2

El receptor realizará la suma de bits a la llegada del mensaje. Si alguna palabra no suma un número par, significará que se ha producido un error durante la transmisión.

## CRC

Los códigos de paridad tienen el inconveniente de que se requiere demasiada redundancia para detectar únicamente errores simples. En el ejemplo que hemos visto, sólo un 8/9 de la información transmitida contenían datos, el resto era redundancia. Los códigos de redundancia cíclica (CRC) son muy utilizados en la práctica para la detección de errores en largas secuencias de datos. Se basan en representar las cadenas de datos como polinomios. El emisor realiza ciertas operaciones matemáticas antes de enviar los datos. El receptor realizará, a la llegada de la transmisión, una división entre un polinomio convenido (polinomio generador). Si el resto es cero, la transmisión ha sido correcta. Si el resto es distinto significará que se han producido errores y solicitará la retransmisión al emisor.

## ***1.5 Control de flujo***

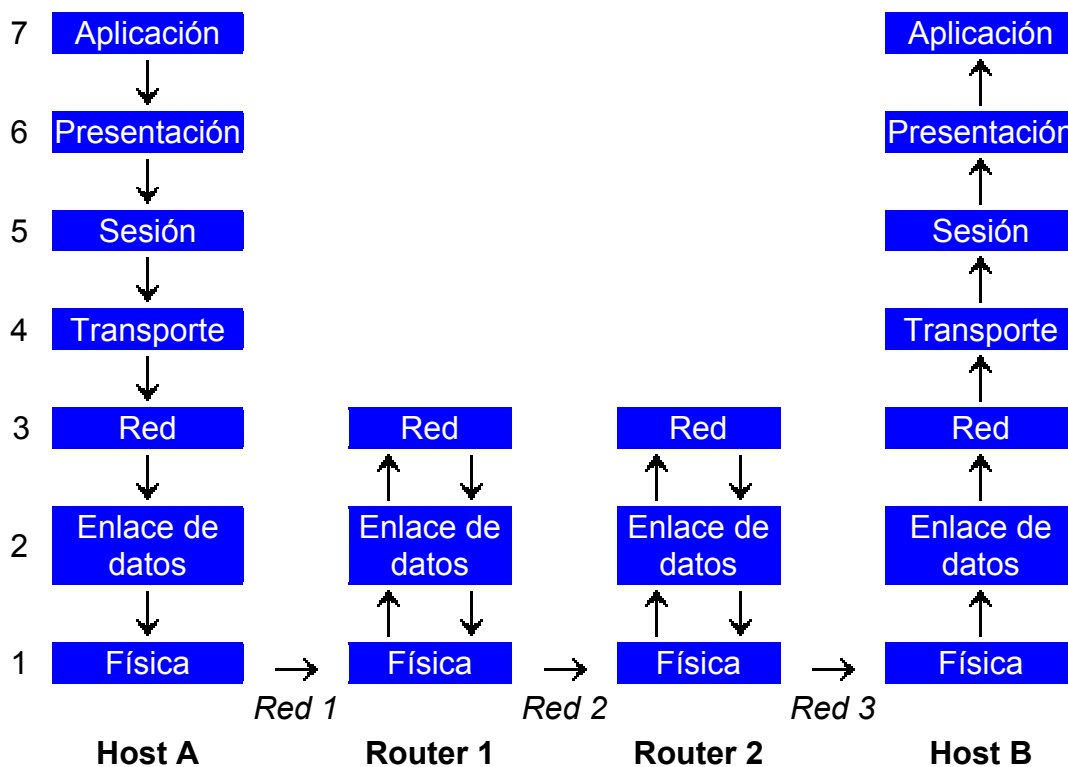
El control de flujo determina cómo enviar la información entre el emisor y el receptor de forma que se vaya recibiendo correctamente sin saturar al receptor. Nótese que puede darse el caso de un emisor rápido y un receptor lento (o un receptor rápido pero que esté realizando otras muchas tareas).

El mecanismo más sencillo de control de flujo se basa en devolver una confirmación o acuse de recibo (ACK) cada vez que el receptor reciba algún dato correcto o una señal de error (NACK) si el dato ha llegado dañado. Cuando el emisor recibe un ACK pasa a enviar el siguiente dato. Si, en cambio, recibe un NACK reenviará el mismo dato.

El procedimiento anterior tiene el gran inconveniente de que el canal se encuentra infrautilizado: hasta que el emisor no reciba un ACK no enviará ningún dato más, estando el canal desaprovechado todo ese tiempo. Una mejora de este método es el envío de una serie de datos numerados, de tal forma que en un sentido siempre se estén enviando datos (dato1, dato2, dato3...) y en el otro sentido se vayan recibiendo las confirmaciones (ACK1, ACK2, ACK3...). La cantidad de datos pendientes de ACK o NACK se establecerá según la memoria temporal del emisor.

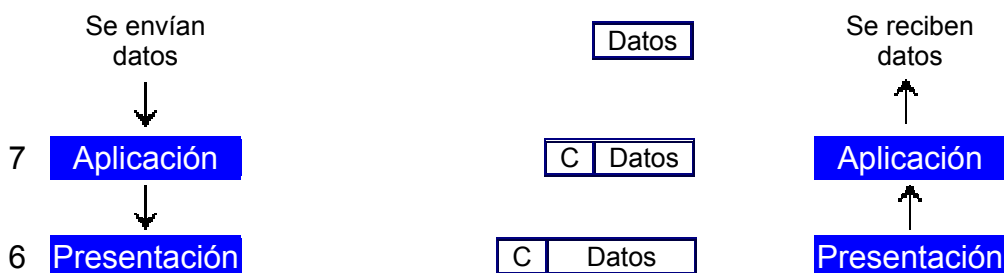
## ***1.6 Modelo de referencia OSI. Comparación con el modelo TCP/IP***

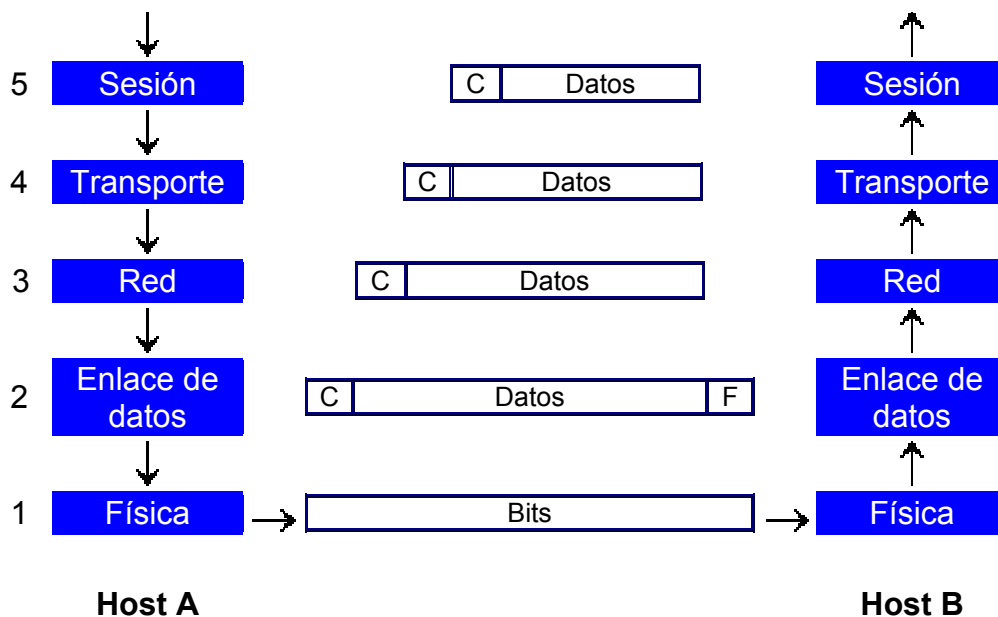
El modelo OSI (Open Systems Interconnection, interconexión de sistemas abiertos) fue un intento de la Organización Internacional de Normas (ISO) para la creación de un estándar que siguieran los diseñadores de nuevas redes. Se trata de un modelo teórico de referencia: únicamente explica lo que debe hacer cada componente de la red sin entrar en los detalles de implementación.



El modelo divide las redes en capas. Cada una de estas capas debe tener una función bien definida y relacionarse con sus capas inmediatas mediante unos interfaces también bien definidos. Esto debe permitir la sustitución de una de las capas sin afectar al resto, siempre y cuando no se varíen los interfaces que la relacionan con sus capas superior e inferior. Los creadores del modelo OSI consideraron que era 7 el número de capas que mejor se ajustaba a sus requisitos.

El gráfico anterior muestra las 7 capas del modelo OSI. Las tres primeras capas se utilizan para enrutar, esto es, mover la información de unas redes a otras. En cambio, las capas superiores son exclusivas de los nodos origen y destino. La capa física está relacionada con el medio de transmisión (cableado concreto que utiliza cada red). En el extremo opuesto se encuentra la capa de aplicación: un programa de mensajería electrónica, por ejemplo. El usuario se situaría por encima de la capa 7. El siguiente gráfico muestra el flujo de información entre capas.





El host A es el nodo origen y el host B, el nodo destino. Nótese que estos papeles se intercambian continuamente en cualquier comunicación. Supongamos que mediante este modelo queremos enviar un mensaje al usuario del host B. El mensaje son los "datos" que se han dibujado por encima de la capa 7. Estos datos van descendiendo de capa en capa hasta llegar a la capa física del host A. Cada capa añade un encabezado (C = cabecera) a los datos que recibe de la capa superior antes de enviárselos a su capa inferior. En la capa de enlace de datos se ha añadido también una serie de códigos al final de la secuencia (F = final) para delimitar no sólo el comienzo sino también el final de un paquete de datos. La capa física no entiende de datos ni de códigos: únicamente envía una secuencia de bits por el medio de transmisión (un cable).

Estos bits llegarán, probablemente pasando por varios encaminadores intermedios, hasta la capa física del host destino. A medida que se van recibiendo secuencias de bits, se van pasando a las capas superiores. Cada capa elimina su encabezado antes de pasarlo a una capa superior. Obsérvese que el mensaje que envía cada capa del host A a su capa inferior es idéntico al que recibe la capa equivalente del host B desde una capa inferior. Finalmente los datos llegarán a la capa de aplicación, serán interpretados y mostrados al usuario del host B.

Los paquetes de datos de cada capa suelen recibir nombres distintos. En la capa de enlace de datos se habla de marcos o tramas; en la capa de red, de paquetes o datagramas. En la capa de transporte, en ocasiones se utiliza el término segmento.

Cada capa se comunica con la capa equivalente de otro host (por ejemplo, la capa de red de un host se entiende con la capa de red de otro host). Sin embargo, como hemos visto, la comunicación realmente se realiza descendiendo capas en el host origen, transmitiendo por el medio físico y aumentando capas en el host destino. Cada capa añade algo nuevo a la comunicación, como vamos a ver ahora:

- **Capa física.** Se encarga de la transmisión de bits por un medio de transmisión, ya sea un medio guiado (un cable) o un medio no guiado (inalámbrico). Esta capa define, entre otros aspectos, lo que transmite cada hilo de un cable, los

tipos de conectores, el voltaje que representa un 1 y el que representa un 0. La capa física será diferente dependiendo del medio de transmisión (cable de fibra óptica, cable par trenzado, enlace vía satélite, etc.) No interpreta la información que está enviando: sólo transmite ceros y unos.

- **Capa de enlace de datos.** Envía tramas de datos entre hosts (o *routers*) de una misma red. Delimita las secuencias de bits que envía a la capa física, escribiendo ciertos códigos al comienzo y al final de cada trama. Esta capa fue diseñada originalmente para *enlaces punto a punto*, en los cuales hay que aplicar un control de flujo para el envío continuo de grandes cantidades de información. Para las *redes de difusión* (redes en las que muchos ordenadores comparten un mismo medio de transmisión) fue necesario diseñar la llamada subcapa de acceso al medio. Esta subcapa determina quién puede acceder al medio en cada momento y cómo sabe cada host que un mensaje es para él, por citar dos problemas que se resuelven a este nivel.
- **Capa de red.** Se encarga del encaminamiento de paquetes entre el origen y el destino, atravesando tantas redes intermedias como sean necesarias. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente. Su misión es unificar redes heterogéneas: todos los hosts tendrán un identificador similar a nivel de la capa de red (en Internet son las direcciones IP) independientemente de las redes que tengan en capas inferiores (Token Ring con cable coaxial, Ethernet con cable de fibra óptica, enlace submarino, enlace por ondas, etc.)
- **Capa de transporte.** Únicamente se preocupa de la transmisión origen-destino. Podemos ver esta capa como una canalización fiable que une un proceso de un host con otro proceso de otro host. Un host puede tener varios procesos ejecutándose: uno para mensajería y otro para transferir archivos, por ejemplo. No se preocupa del camino intermedio que siguen los fragmentos de los mensajes. Integra control de flujo y control de errores, de forma que los datos lleguen correctamente de un extremo a otro.
- **Capa de sesión.** Se encarga de iniciar y finalizar las comunicaciones. Además proporciona servicios mejorados a la capa de transporte como, por ejemplo, la creación de puntos de sincronismo para recuperar transferencias largas fallidas.
- **Capa de presentación.** Codifica los datos que recibe de la capa de aplicación a un sistema convenido entre emisor y receptor, con el propósito de que tanto textos como números sean interpretados correctamente. Una posibilidad es codificar los textos según la *tabla ASCII* y los números en *complemento a dos*.
- **Capa de aplicación.** Aquí se encuentran los protocolos y programas que utiliza el usuario para sus comunicaciones en red. Esta capa tendrá que ser adaptada para cada tipo de ordenador de forma que sea posible el envío de un correo electrónico (u otros servicios) entre sistemas heterogéneos como Macintosh, Linux o Windows.

El modelo OSI, patrocinado por la Comunidad Europea y, más tarde, por el gobierno de los Estados Unidos, nunca llegó a tener la implantación esperada. Entre otros motivos, porque el modelo TCP/IP ya había sido aceptado por aquella época entre investigadores los cuales se resistieron a un cambio que, para la mayoría, era un cambio a peor. Las bases que sustentan Internet son realmente sencillas y quizás esto ha sido la clave de su éxito; el modelo OSI, en cambio, fue tan ambicioso y complejo que terminó arrinconado en las estanterías de los laboratorios.

Sin embargo, la idea de la división por capas del modelo OSI es realmente valiosa. Esta misma idea se aplica a todas las redes actuales, incluyendo Internet.

Como hemos comentado al principio, OSI es un modelo teórico general que da preferencia a un buen diseño en papel, antes que a la implementación de los protocolos. El modelo TCP/IP se hizo justamente al revés: primero vinieron los protocolos y, después, se pensó en sus especificaciones. De tal forma, que el modelo TCP/IP únicamente es aplicable para la pila de protocolos TCP/IP pero no es válido para nuevas redes.

El modelo TCP/IP tiene únicamente 3 capas: capa de red, de transporte y de aplicación. No tiene las capas de sesión ni de presentación que, por otro lado, estaban prácticamente vacías en el modelo OSI. Tampoco dice nada de las capas física y de enlace a datos. Sin embargo, nosotros seguiremos un modelo de referencia fruto de combinar los modelos OSI y TCP/IP. Se trata del modelo real que se está utilizando actualmente en las redes TCP/IP. El siguiente gráfico refleja las 5 capas de nuestro modelo.

<b>Capa de aplicación</b> (HTTP, SMTP, FTP, TELNET...)
<b>Capa de transporte</b> (UDP, TCP)
<b>Capa de red</b> (IP)
<b>Capa de acceso a la red</b> (Ethernet, Token Ring...)
<b>Capa física</b> (cable coaxial, par trenzado...)

## ***1.7 Capa física: medios de transmisión***

La capa física determina el soporte físico o medio de transmisión por el cual se transmiten los datos. Estos medios de transmisión se clasifican en guiados y no guiados. Los primeros son aquellos que utilizan un medio sólido (un cable) para la transmisión. Los medios no guiados utilizan el aire para transportar los datos: son los medios inalámbricos.

Los medios guiados se estudian más abajo.

- **Cable coaxial**
- **Par trenzado**
- **Fibra óptica**

Entre los medios no guiados se encuentran:

- **Ondas de radio.** Son capaces de recorrer grandes distancias, atravesando edificios incluso. Son ondas omnidireccionales: se propagan en todas las direcciones. Su mayor problema son las interferencias entre usuarios.
- **Microondas.** Estas ondas viajan en línea recta, por lo que emisor y receptor deben estar alineados cuidadosamente. Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de unos 80 Kms. de distancia. Es una forma económica para comunicar dos zonas geográficas mediante dos torres suficientemente altas para que sus extremos sean visibles.
- **Infrarrojos.** Son ondas direccionales incapaces de atravesar objetos sólidos (paredes, por ejemplo) que están indicadas para transmisiones de corta distancia. Las tarjetas de red inalámbricas utilizadas en algunas redes locales emplean esta

tecnología: resultan muy cómodas para ordenadores portátiles; sin embargo, su velocidad es inferior a la conseguida mediante un cable par trenzado.

- **Ondas de luz.** Las ondas láser son unidireccionales. Se pueden utilizar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un fotodetector.

## Cable coaxial

El cable coaxial es similar al cable utilizado en las antenas de televisión: un hilo de cobre en la parte central rodeado por una maya y separados ambos elementos conductores por un cilindro de plástico. Las redes que utilizan este cable requieren que los adaptadores tengan un conector apropiado: los ordenadores forman una fila y se coloca un segmento de cable entre cada ordenador y el siguiente. En los extremos hay que colocar un terminador, que no es más que una resistencia de 50 ohmios. La velocidad máxima que se puede alcanzar es de 10Mbps.

## Cable par trenzado

El par trenzado es similar al cable telefónico, sin embargo consta de 4 hilos y utiliza unos conectores un poco más anchos. Dependiendo del número de trenzas por unidad de longitud, los cables de par trenzado se clasifican en categorías. A mayor número de trenzas, se obtiene una mayor velocidad de transferencia.

- Categoría 3, hasta 16 Mbps
- Categoría 4, hasta 20 Mbps
- Categoría 5, hasta 100 Mbps
- Categoría 6, hasta 1Gbps

Los cables par trenzado pueden ser a su vez de dos tipos:

- UTP (Unshielded Twisted Pair, par trenzado no apantallado)
- STP (Shielded Twisted Pair, par trenzado apantallado)

Los cables UTP son los más utilizados debido a su bajo coste y facilidad de instalación. Los cables STP están embutidos en una malla metálica que reduce las interferencias y mejora las características de la transmisión. Sin embargo, tienen un coste elevado y al ser más gruesos son más complicados de instalar.

El cableado que se utiliza en la actualidad es UTP CAT5. El cableado CAT6 es demasiado nuevo y es difícil encontrarlo en el mercado. Los cables STP se utilizan únicamente para instalaciones muy puntuales que requieran una calidad de transmisión muy alta.

Los segmentos de cable van desde cada una de las estaciones hasta un aparato denominado hub o concentrador, formando una topología de estrella.

## Cable de fibra óptica

En los cables de fibra óptica la información se transmite en forma de pulsos de luz. En un extremo del cable se coloca un diodo luminoso (LED) o bien un láser, que puede emitir luz. Y en el otro extremo se sitúa un detector de luz.

Curiosamente y a pesar de este sencillo funcionamiento, mediante los cables de fibra óptica se llegan a alcanzar velocidades de varios Gbps. Sin embargo, su instalación y mantenimiento tiene un coste elevado y solamente son utilizados para redes troncales con mucho tráfico.

Los cables de fibra óptica son el medio de transmisión elegido para las redes de cable que ya están funcionando en algunas zonas de España. Se pretende que este cable pueda transmitir televisión, radio, Internet y teléfono.

## Capítulo 2 Instalación de cableado

### 2.2 Cable par trenzado

#### Cable par trenzado directo

Los conectores de cada extremo siguen el mismo esquema de colores. Una combinación posible es la que se indica a continuación.

En los cables de par trenzado se tienen que respetar siempre los pares formados por los pines 1-2, 3-6, 4-5 y 7-8. Un par son dos cablecitos que van trenzados a lo largo de todo el recorrido del cable (el azul va trenzado con el blanco-azul, el naranja con el blanco-naranja, etc.). Esto significa que podemos cambiar los colores propuestos siempre y cuando se respeten los pares, y se utilice la misma combinación de colores tanto en un extremo como en el otro.

<b>8</b>	N/U
<b>7</b>	N/U
<b>6</b>	Rx-
<b>5</b>	N/U
<b>4</b>	N/U
<b>3</b>	Rx+
<b>2</b>	Tx-
<b>1</b>	Tx+

*Colocar a la izquierda el conector con el clip hacia abajo. A la derecha, sigue el cable.*

Estos cables se utilizan para unir:

- Ordenador con hub.
- 2 hubs (utilizando el puerto *uplink* de uno de ellos y un puerto normal del otro).

Nota: Los puertos uplink y la interconexión de hubs se explica en el apartado Interconexión de hubs.

## Cable par trenzado cruzado

En un extremo del cable se utiliza el esquema propuesto en el apartado anterior. En el otro extremo, se utiliza el siguiente:

Lo que estamos haciendo es cruzar los pines de transmisión (Tx+ y Tx-) de un extremo con los pines de recepción (Rx+ y Rx-) del otro. Los hilos marcados como N/U no se utilizan.

8	N/U (5 = N/U)
7	N/U (4 = N/U)
6	Rx- (2 = Tx-)
5	N/U (8 = N/U)
4	N/U (7 = N/U)
3	Rx+ (1 = Tx+)
2	Tx- (6 = Rx-)
1	Tx+ (3 = Rx+)

*Colocar a la izquierda el conector con el clip hacia abajo. A la derecha, sigue el cable.*

Estos cables se utilizan para unir:

- 2 ordenadores sin necesidad de hub (el cable va de una tarjeta de red a la otra).
- 2 hubs (sin utilizar el puerto *uplink* de ninguno de ellos o utilizando el puerto *uplink* en ambos).

## 2.3 Comparación entre hub y switch

Un hub pertenece a la capa física: se puede considerar como una forma de interconectar unos cables con otros. Un switch, en cambio, trabaja en la capa de acceso a la red (son la versión moderna de los puentes o bridges) pero también puede tratarse como un sistema de interconexión de cables, eso sí, con cierta inteligencia. Los puestos de la red no tienen forma de conocer si las tramas Ethernet que están recibiendo proceden de un hub, switch o han pasado directamente mediante un cable par trenzado cruzado. Estos dispositivos no requieren ninguna configuración software: únicamente con enchufarlos ya comienzan a operar.

Nota: Un router (encaminador) pertenece a la capa de red. Trabaja con direcciones IP. Se utiliza para interconectar redes y requiere una configuración. Podemos averiguar los routers que atraviesan nuestros datagramas IP mediante el comando Tracert.

Un hub o concentrador es el punto central desde el cual parten los cables de par trenzado hasta las distintos puestos de la red, siguiendo una topología de estrella. Se

caracterizan por el número de puertos y las velocidades que soportan. Por ejemplo, son habituales los hubs 10/100 de 8 puertos.

- Los hubs difunden la información que reciben desde un puerto por todos los demás (su comportamiento es similar al de un ladrón eléctrico).
- Todas sus ramas funcionan a la misma velocidad. Esto es, si mezclamos tarjetas de red de 10/100 Mbps y 10 Mbps en un mismo hub, todas las ramas del hub funcionarán a la velocidad menor (10 Mbps).
- Es habitual que contengan un diodo luminoso para indicar si se ha producido una colisión. Además, los concentradores disponen de tantas lucecitas (LED) como puertos para informar de las ramas que tienen señal.

Un switch o conmutador es un hub mejorado: tiene las mismas posibilidades de interconexión que un hub (al igual que un hub, no impone ninguna restricción de acceso entre los ordenadores conectados a sus puertos). Sin embargo se comporta de un modo más eficiente reduciendo el tráfico en las redes y el número de colisiones.

- Un switch no difunde las tramas Ethernet por todos los puertos, sino que las retransmite sólo por los puertos necesarios. Por ejemplo, si tenemos un ordenador A en el puerto 3, un ordenador B en el puerto 5 y otro ordenador C en el 6, y enviamos un mensaje desde A hasta C, el mensaje lo recibirá el switch por el puerto 3 y sólo lo reenviará por el puerto 6 (un hub lo hubiese reenviado por todos sus puertos).
- Cada puerto tiene un buffer o memoria intermedia para almacenar tramas Ethernet.
- Puede trabajar con velocidades distintas en sus ramas (autosensing): unas ramas pueden ir a 10 Mbps y otras a 100 Mbps.
- Suelen contener 3 diodos luminosos para cada puerto: uno indica si hay señal (link), otro la velocidad de la rama (si está encendido es 100 Mbps, apagado es 10 Mbps) y el último se enciende si se ha producido una colisión en esa rama.

## ¿Cómo sabe un switch los ordenadores que tiene en cada rama?

Lo averigua de forma automática mediante aprendizaje. Los conmutadores contienen una tabla dinámica de direcciones físicas y números de puerto. Nada más enchufar el switch esta tabla se encuentra vacía. Un procesador analiza las tramas Ethernet entrantes y busca la dirección física de destino en su tabla. Si la encuentra, únicamente reenviará la trama por el puerto indicado. Si por el contrario no la encuentra, no le quedará más remedio que actuar como un hub y difundirla por todas sus ramas.

Las tramas Ethernet contienen un campo con la dirección física de origen que puede ser utilizado por el switch para agregar una entrada a su tabla basándose en el número de puerto por el que ha recibido la trama. A medida que el tráfico se incrementa en la red, la tabla se va construyendo de forma dinámica. Para evitar que la información quede desactualizada (si se cambia un ordenador de sitio, por ejemplo) las entradas de la tabla desaparecerán cuando agoten su tiempo de vida (TTL), expresado en segundos.

## Dominios de colisión

Un dominio de colisión es un segmento del cableado de la red que comparte las mismas colisiones. Cada vez que se produzca una colisión dentro de un mismo dominio de colisión, afectará a todos los ordenadores conectados a ese segmento pero no a los ordenadores pertenecientes a otros dominios de colisión.

Todas las ramas de un hub forman un mismo dominio de colisión (las colisiones se retransmiten por todos los puertos del hub). Cada rama de un switch constituye un dominio de colisiones distinto (las colisiones no se retransmiten por los puertos del switch). Este es el motivo por el cual la utilización de conmutadores reduce el número de colisiones y mejora la eficiencia de las redes. El ancho de banda disponible se reparte entre todos los ordenadores conectados a un mismo dominio de colisión.

Nota: Podemos indicar un número aproximado de 25-30 como medida máxima de ordenadores que se pueden conectar dentro de un mismo dominio de colisión. Sin embargo, este número dependerá en gran medida del tráfico de la red. En redes con mucho tráfico se debe tratar de reducir el número de ordenadores por dominio de colisión lo más posible mediante la creación de distintos dominios de colisión conectados por switches o mediante la creación de distintas subredes conectadas por routers.

## ¿Qué instalar hubs o switches?

- Siempre que el presupuesto lo permita elegiremos un switch antes que un hub.
- Si nuestra red tiene un elevado número de ordenadores (hay que utilizar varios concentradores enlazados) pero sólo nos podemos permitir un switch, éste lo colocaremos en el lugar de la red con más tráfico (habitualmente será el concentrador situado en el centro de la estrella de estrellas o bien, aquél que contenga a los servidores). En el resto de las posiciones colocaremos hubs. El esquema descrito se utiliza a menudo: un hub en cada departamento y un switch para interconectar los departamentos con los servidores. Desde luego, lo ideal sería colocar switches en todas las posiciones.
- Además de la mejora en eficiencia que supone utilizar un switch frente a un hub, debemos considerar también el aumento de seguridad: si en un ordenador conectado a un switch se instala, con fines nada éticos, un programa para escuchar el tráfico de la red (sniffer), el atacante sólo recibirá las tramas Ethernet que corresponden a ese ordenador pero no las tramas de otros ordenadores que podrían contener contraseñas ajenas.

## 2.4 Interconexión de hubs

Los concentradores incluyen un puerto diferenciado, etiquetado con el nombre "uplink" o "cascade", para facilitar su interconexión con otros hubs. El puerto "uplink" de un hub se conecta mediante un cable par trenzado directo hasta un puerto cualquiera (que no sea el "uplink") del otro hub. Si ninguno de los dos hubs tuviese el puerto "uplink" libre todavía se podrían interconectar utilizando un cable par trenzado cruzado.

Nota: Todo lo que se comenta en este apartado referente a hubs (concentradores) es equivalente para los switches (conmutadores).

¿Dónde se encuentra el puerto "uplink"? Dependiendo de los fabricantes se suele dar una de estas dos situaciones:

- El hub es de  $n$  puertos pero tiene  $n+1$  conectores, uno de ellos tiene una marca especial. Por ejemplo, son habituales los hubs que tienen 9 conectores: 7 puertos normales y un puerto mixto con dos conectores contiguos los cuales no se pueden utilizar simultáneamente. El número máximo de cables que podemos conectar es de 8, quedando un conector vacío (el marcado como "uplink" o el que tiene justo a su lado).
- El hub es de  $n$  puertos y tiene  $n$  conectores, uno de ellos tiene una marca especial. Mediante un botón conmutamos la función del conector diferenciado entre "uplink" y puerto normal. Las prestaciones son las mismas que en el caso anterior. Este diseño es habitual de los hubs del fabricante 3COM.

¿Cómo enlazar unos hubs con otros? Los diseños más habituales son los dos siguientes, aunque se suelen combinar:

- Hubs encadenados. Un hub se va conectando con el siguiente formando una cadena. No es conveniente conectar de esta forma más de 3 hubs puesto que el rendimiento de la red disminuirá considerablemente (las señales tardan en pasar desde el primer hub de la cadena hasta el último).
- Hubs en estrella. Se coloca un hub en el centro y de éste se tiran cables hasta el resto de los hubs. Con esta solución se consiguen velocidades más altas en la red aunque el cableado es más costoso.

## Capítulo 3

### Protocolos

En cada una de las capas de los modelos (excepto en la capa física) se utiliza un protocolo distinto. Estos protocolos se van apilando de forma que los de capas superiores aprovechan los servicios de los protocolos de capas inferiores. Durante una transmisión cada protocolo se comunica con su homónimo del otro extremo sin preocuparse de los protocolos de otras capas.

Una de las decisiones más importantes que debemos tomar a la hora de diseñar una red es elegir un protocolo de la capa de acceso al medio y otro de las capas de red y transporte. A continuación estudiamos los distintos protocolos. Adelantamos, no obstante, que la combinación más interesante para redes locales nuevas es Ethernet + TCP/IP.

#### ***3.1 Protocolos de la capa de acceso al medio***

En la capa de acceso al medio se determina la forma en que los puestos de la red envían y reciben datos sobre el medio físico. Se responden preguntas del tipo: ¿puede un puesto dejar información en el cable siempre que tenga algo que transmitir?, ¿debe esperar algún turno?, ¿cómo sabe un puesto que un mensaje es para él?

Un organismo de normalización conocido como IEEE (Instituto de ingenieros eléctricos y electrónicos) ha definido los principales protocolos de la capa de acceso al medio conocidos en conjunto como estándares 802. Los más importantes son los IEEE 802.3 y IEEE 802.5 que se estudian a continuación.

Otros estándares 802.-- El estándar 802.1 es una introducción al conjunto de estándares y define algunos aspectos comunes. El estándar 802.2 describe la parte superior de la capa de enlace de datos del modelo OSI (entre la capa de acceso al medio y la capa de red) que puede proporcionar control de errores y control de flujo al resto de estándares 802 utilizando el protocolo LLC (Logical Link Control, control lógico de enlace). Las normas 802.3 a 802.5 definen protocolos para redes LAN. El estándar 802.4 que no vamos a estudiar por su escasa implantación se conoce como Token Bus (bus con paso de testigo). Finalmente, 802.6 es un estándar adecuado para utilizarse en redes MAN. Se trata de DQDB (Distributed Queue Dual Bus, bus doble de colas distribuidas).

El protocolo utilizado en esta capa viene determinado por las tarjetas de red que instalemos en los puestos. Esto quiere decir que si adquirimos tarjetas Ethernet sólo podremos instalar redes Ethernet. Y que para instalar redes Token ring necesitaremos tarjetas de red especiales para Token ring. Actualmente en el mercado únicamente se comercializan tarjetas de red Ethernet (de distintas velocidades y para distintos cableados).

### **Token ring (802.5)**

Las redes Token ring (paso de testigo en anillo) fueron utilizadas ampliamente en entornos IBM desde su lanzamiento en el año 1985. En la actualidad es difícil encontrarlas salvo en instalaciones antiguas de grandes empresas.

El cableado se establece según una topología de anillo. En lugar de utilizar difusiones, se utilizan enlaces punto a punto entre cada puesto y el siguiente del anillo. Por el anillo Token ring circula un mensaje conocido como token o ficha. Cuando una estación desea transmitir espera a recibir el token. En ese momento, lo retira de circulación y envía su mensaje. Este mensaje circula por el anillo hasta que lo recibe íntegramente el destinatario. Entonces se genera un token nuevo.

Las redes Token ring utilizan una estación monitor para supervisar el funcionamiento del anillo. Se trata de un protocolo complejo que debe monitorizar en todo momento el buen funcionamiento del token (que exista exactamente uno cuando no se transmiten datos) y sacar del anillo las tramas defectuosas que no tengan destinatario, entre otras funciones.

Las redes Token ring de IBM pueden funcionar a 4 Mbps o a 16 Mbps utilizando cable par trenzado o cable coaxial.

## Ethernet (802.3)

Las redes Ethernet son actualmente las únicas que tienen interés para entornos LAN. El estándar 802.3 fue diseñado originalmente para funcionar a 10 Mbps, aunque posteriormente ha sido perfeccionado para trabajar a 100 Mbps (802.3u) o 1 Gbps.

Una red Ethernet tiene las siguientes características:

- Canal único. Todas las estaciones comparten el mismo canal de comunicación por lo que sólo una puede utilizarlo en cada momento.
- Es de difusión debido a que todas las transmisiones llegan a todas las estaciones (aunque sólo su destinatario aceptará el mensaje, el resto lo descartarán).
- Tiene un control de acceso distribuido porque no existe una autoridad central que garantice los accesos. Es decir, no hay ninguna estación que supervise y asigne los turnos al resto de estaciones. Todas las estaciones tienen la misma prioridad para transmitir.

Comparación de Ethernet y Token ring.-- En Ethernet cualquier estación puede transmitir siempre que el cable se encuentre libre; en Token ring cada estación tiene que esperar su turno. Ethernet utiliza un canal único de difusión; Token ring utiliza enlaces punto a punto entre cada estación y la siguiente. Token ring tiene siempre una estación monitor que supervisa el buen funcionamiento de la red; en Ethernet ninguna estación tiene mayor autoridad que otra. Según esta comparación, la conclusión más evidente es que, a iguales velocidades de transmisión, Token ring se comportará mejor en entornos de alta carga y Ethernet, en redes con poco tráfico.

En las redes Ethernet, cuando una estación envía un mensaje a otra, no recibe ninguna confirmación de que la estación destino haya recibido su mensaje. Una estación puede estar enviando paquetes Ethernet a otra que está desconectada y no advertirá que los paquetes se están perdiendo. Las capas superiores (y más concretamente, TCP) son las encargadas de asegurarse que la transmisión se ha realizado de forma correcta.

El protocolo de comunicación que utilizan estas redes es el CSMA/CD (Carrier Sense Multiple Access / Collision Detect, acceso múltiple con detección de portadora y detección de colisiones). Esta técnica de control de acceso a la red ha sido normalizada constituyendo el estándar IEEE 802.3. Veamos brevemente el funcionamiento de CSMA/CD:

Quando una estación quiere transmitir, primero escucha el canal (detección de portadora). Si está libre, transmite; pero si está ocupado, espera un tiempo y vuelve a intentarlo.

Sin embargo, una vez que una estación ha decidido comenzar la transmisión puede darse el caso de que otra estación haya tomado la misma decisión, basándose en que el canal estaba libre cuando ambas lo comprobaron. Debido a los retardos de propagación en el cable, ambas señales colisionarán y no se podrá completar la transmisión de ninguna de

las dos estaciones. Las estaciones que están transmitiendo lo advertirán (detección de colisiones) e interrumpirán inmediatamente la transmisión. Después esperarán un tiempo aleatorio y volverán a intentarlo. Si se produce una nueva colisión, esperarán el doble del tiempo anterior y lo intentarán de nuevo. De esta manera, se va reduciendo la probabilidad de nuevas colisiones.

Debemos recordar que el canal es único y por lo tanto todas las estaciones tienen que compartirlo. Sólo puede estar una estación transmitiendo en cada momento, sin embargo pueden estar recibiendo el mensaje más de una.

Nota: La existencia de colisiones en una red no indica que exista un mal funcionamiento. Las colisiones están definidas dentro del protocolo Ethernet y no deben ser consideradas como una situación anómala. Sin embargo, cuando se produce una colisión el canal se desaprovecha porque ninguna estación logra transmitir en ese momento. Debemos tratar de reducir el número de colisiones que se producen en una red. Esto se consigue separando grupos de ordenadores mediante un [switch](#) o un router. Podemos averiguar las colisiones que se producen en una red observando el correspondiente LED de nuestro [hub](#).

## Direcciones físicas

¿Cómo sabe una estación que un mensaje es para ella? Está claro, que hay que distinguir unas estaciones de otras utilizando algún identificador. Esto es lo que se conoce como direcciones físicas.

Los adaptadores Ethernet tienen asignada una dirección de 48 bits de fábrica que no se puede variar. Los fabricantes nos garantizan que no puede haber dos tarjetas de red con la misma dirección física. Si esto llegase a ocurrir dentro de una misma red la comunicación se volvería imposible. Los tres primeros bytes corresponden al fabricante (no puede haber dos fabricantes con el mismo identificador) y los tres últimos al número de serie (no puede haber dos tarjetas del mismo fabricante con el mismo número de serie). Por ejemplo,

5D:1E:23:10:9F:A3

Los bytes 5D:1E:23 identifican al fabricante y los bytes 10:9F:A3 al número de serie del fabricante 5D:1E:23

Nota: Los comandos `ipconfig / all` |more y `winipcfg` muestran la dirección física de nuestra tarjeta de red Ethernet. Observe que estos comandos pueden recoger también información relativa al adaptador virtual "PPP Adapter" (se corresponde con el módem o adaptador RDSI) además de la referente a la tarjeta de red real.

No todas las direcciones representan a máquinas aisladas, algunas de ellas se utilizan para enviar mensajes de multidifusión. Esto es, enviar un mensaje a varias máquinas a la vez o a todas las máquinas de la red. Ethernet permite que el mismo mensaje pueda ser escuchado por más de una máquina a la vez.

## Formato de la trama

La comunicación entre una estación y otra a través de una red Ethernet se realiza enviando tramas Ethernet. El mensaje que se quiere transmitir se descompone en una o más tramas con el siguiente formato:

8 bytes	6 bytes	6 bytes	2 bytes	64-1500 bytes	4 bytes
Preámbulo	Dirección física destino	Dirección física origen	Tipo de trama	Datos de la trama	CRC

Las direcciones origen y destino son las direcciones físicas de los adaptadores de red de cada ordenador. El campo Tipo de trama indica el formato de los datos que se transfieren en el campo Datos de la trama. Por ejemplo, para un datagrama IP se utiliza el valor hexadecimal de 0800 y para un mensaje ARP el valor 0806. Todos los mensajes (datagramas) que se envíen en la capa siguiente irán encapsulados en una o más tramas Ethernet utilizando el campo Datos de la trama. Y esto mismo es aplicable para cualquier otro tipo de red distinta a Ethernet. Como norma general, cada mensaje que transmite una capa se coloca en el campo datos de la capa anterior. Aunque es muy frecuente que el mensaje no quepa en una sola trama y se utilicen varias.

## Velocidades

Ethernet puede funcionar a tres velocidades: 10 Mbps, 100 Mbps (FastEthernet) y 1 Gbps (1000 Mbps). 10 Mbps es la velocidad para la que se diseñó originalmente el estándar Ethernet. Sin embargo, esta velocidad se ha mejorado para adaptarse a las crecientes exigencias de las redes locales. La velocidad de 100 Mbps es actualmente la más utilizada en la empresa. Las redes a 1 Gbps están comenzando a ver la luz en estos momentos por lo que tardarán un tiempo en implantarse en el mercado (los precios son todavía muy altos).

Para crear una red que trabaje a 10 Mbps es suficiente con utilizar cable coaxial o bien, cable par trenzado de categoría 3 o superior. Sin embargo, es recomendable utilizar cables par trenzado de categoría 5 y concentradores con velocidades mixtas 10/100 Mbps. De esta forma, en un futuro se podrán ir cambiando gradualmente los adaptadores de 10 Mbps por unos de 100 Mbps sin necesidad de instalar nuevo cableado.

La mejor opción actualmente para redes nuevas es FastEthernet. Para conseguir velocidades de 100 Mbps es necesario utilizar cable par trenzado con una categoría mínima de 5, un concentrador que soporte esta velocidad y tarjetas de red de 100 Mbps. Generalmente, los cables UTP cumplen bien con su función pero en situaciones concretas que requieran el máximo rendimiento de la red o existan muchas interferencias, puede ser necesario un cableado STP.

## Tipos de adaptadores

La siguiente tabla resume los principales tipos de adaptadores Ethernet en función del cableado y la velocidad de la red. (T se utiliza para par trenzado, F para fibra óptica y X para FastEthernet).

	10Base5	10Base2	10BaseT	10BaseFP	100BaseTX	100BaseFX
<b>Cableado</b>	Coaxial		Par trenzado	Par de fibra óptica	Par trenzado	2 fibras ópticas
<b>Velocidad</b>	10 Mbps				100 Mbps	
<b>Topología</b>	Bus		Estrella			
<b>Longitud máxima segmento</b>	500 m	185 m	100 m	500 m	100 m	100 m
<b>Nodos por segmento</b>	100	30	2 (un extremo es el hub y el otro el ordenador)			

Los adaptadores pueden ser compatibles con varios de los estándares anteriores dando lugar a numerosas combinaciones. Sin embargo, lo habitual es encontrar en el mercado tarjetas de red de tan sólo estos dos tipos:

- Tarjetas de red combo. Tienen 2 conectores, uno para cable coaxial y otro para RJ45. Su velocidad máxima es de 10 Mbps por lo que soportan 10Base2 y 10BaseT. La tarjeta de red RTL8029 del fabricante Realtek pertenece a este tipo. Este grupo de tarjetas de red tienden a desaparecer (al igual que el cable coaxial).
- Tarjetas de red 10/100. Tienen sólo conector para RJ45. Se adaptan a la velocidad de la red (10 Mbps o 100 Mbps). Son compatibles con 10BaseT y 100BaseT. Como ejemplos de este tipo se encuentran las tarjetas Realtek RTL8139 y 3COM 3C905.

### 3.2 Protocolos de las capas de red y transporte

Los protocolos que vamos a describir a continuación no se preocupan por el medio de transmisión: dan por hecho que existe un protocolo de la capa de acceso al medio que se encarga del envío y recepción de los paquetes a través del medio de transmisión. Para su funcionamiento requieren alguno de los protocolos que hemos estudiado en el apartado anterior.

#### IPX/SPX

La familia de protocolos IPX/SPX (Internetwork Packet Exchange / Sequential Packet Exchange, intercambio de paquetes entre redes / intercambio de paquetes secuenciales) fue desarrollada por Novell a principios de los años 80. Gozó de gran popularidad durante unos 15 años si bien actualmente ha caído en desuso. Estos protocolos fueron creados como parte del sistema operativo de red Novell NetWare. En un principio

fueron protocolos propietarios aunque más adelante se comenzaron a incorporar a otros sistemas operativos: Windows los incluye con los nombres de Protocolo compatible con IPX/SPX o Transporte compatible NWLink IPX/SPX según las versiones.

IPX/SPX es enrutable: hace posible la comunicación entre ordenadores pertenecientes a redes distintas interconectadas por encaminadores (routers). Los principales protocolos de IPX/SPX son, como su nombre indica, IPX y SPX. El primero pertenece a la capa de red y se encarga del envío de los paquetes (fragmentos de mensajes) a través de las redes necesarias para llegar a su destino. SPX pertenece a la capa de transporte: gestiona el envío de mensajes completos entre los dos extremos de la comunicación.

La estructura de protocolos IPX/SPX se corresponde en gran medida con TCP/IP. Su configuración es más sencilla que en TCP/IP aunque admite menos control sobre el direccionamiento de la red. El identificador de cada puesto en la red es un número de 6 bytes, que coincide con la dirección física de su adaptador, seguido de un número de 6 bytes, que representa la dirección de la red. Por ejemplo: 44.45.EA.54.00.00:4C.34.A8.59 (nodo:red).

## AppleTalk

Es el protocolo propietario de Apple utilizado para interconectar ordenadores Macintosh. Es un protocolo enrutable. El identificador de cada puesto es un número de 1 byte y el de cada red, un número de 2 bytes. Por ejemplo, "50.8" representa el ordenador 8 de la red 50. Si el número de puestos en una red es superior a 253 hosts, se utilizan varios números de redes contiguos en lugar de sólo uno. Por ejemplo, la red "100-101" dará cabida a 506 hosts. Un host conectado a la red "100-101" tendrá una dirección de la forma "100.x". En la terminología de Apple, una red se conoce como una zona.

## NetBEUI

NetBEUI (NetBIOS Extended User Interface, interfaz de usuario extendida para NetBIOS) es un protocolo muy sencillo que se utiliza en redes pequeñas de menos de 10 ordenadores que no requieran salida a Internet. Su funcionamiento se basa en el envío de difusiones a todos los ordenadores de su red. Sus difusiones no atraviesan los encaminadores a no ser que estén configurados para dejar pasar este tráfico: es un protocolo no enrutable.

La ventaja de este protocolo es su sencillez de configuración: basta con instalar el protocolo y asignar un nombre a cada ordenador para que comience a funcionar. Su mayor desventaja es su ineficiencia en redes grandes (se envían excesivas difusiones).

Actualmente es un protocolo exclusivo de las redes Microsoft. Fue diseñado para ofrecer una interfaz sencilla para [NetBIOS](#) (este protocolo trabaja en la capa de aplicación, lo estudiaremos cuando veamos las redes en Windows 98).

## TCP/IP

TCP/IP (Transport Control Protocol / Internet Protocol, protocolo de control de transporte / protocolo de Internet) es el estándar en las redes. Fue diseñado por el Departamento de Defensa de los Estados Unidos a finales de los años 70 para utilizarse en una red resistente a bombas: aunque se destruyese alguna línea de comunicación o encaminador, la comunicación podría seguir funcionando por rutas alternativas. Lo sorprendente de TCP/IP es que no fue pensado para resistir el espionaje: los protocolos originales transmiten las contraseñas y datos sin codificación alguna.

TCP/IP es el protocolo de Internet (en realidad, es una familia de protocolos). En la actualidad es la elección recomendada para casi todas las redes, especialmente si la red tiene salida a Internet. En el resto del curso nos centraremos exclusivamente en las redes TCP/IP.

Los dos protocolos principales de TCP/IP son IP, perteneciente a la capa de red, y TCP, perteneciente a la capa de transporte. Estos protocolos se estudian detalladamente en el mas adelante. El identificador de cada puesto es la dirección IP. Una dirección IP es un número de 4 bytes. Por ejemplo: 194.142.78.95. Este número lleva codificado la dirección de red y la dirección de host. Las direcciones IP se clasifican en:

- *Direcciones públicas.* Son visibles desde todo Internet. Se contratan tantas como necesitemos. Son las que se asignan a los servidores de Internet que sirven información 24 horas al día (por ejemplo, un servidor web).
- *Direcciones privadas.* Son visibles sólo desde una red interna pero no desde Internet. Se utilizan para identificar los puestos de trabajo de las empresas. Se pueden utilizar tantas como se necesiten; no es necesario contratarlas.

## Capítulo 4

### Redes en Windows 98

En este apartado vamos a estudiar exclusivamente las redes Microsoft montadas sobre la familia de protocolos TCP/IP. Hasta ahora nos hemos movido en las capas de red y transporte. Sin embargo, Windows va más allá y utiliza un nuevo protocolo en la capa de aplicación, llamado NetBIOS, para encapsular los protocolos de capas inferiores. Las redes Microsoft se caracterizan por la utilización de NetBIOS.

Los equipos Windows 98 pueden funcionar tanto como clientes (accediendo a recursos compartidos) como servidores (ofreciendo recursos). Por tanto, las redes en Windows 98 serán redes entre iguales: no existe una jerarquía de ordenadores, todos pueden desempeñar los papeles de cliente y servidor. En el apartado "Redes en Windows NT" estudiaremos la arquitectura cliente/servidor.

#### 4.1 Protocolo NetBIOS

Es un protocolo de resolución de nombres que puede ser encapsulado sobre TCP/IP. NetBIOS funciona a nivel de la capa de aplicación, dando una apariencia uniforme a todas las redes Windows independientemente de los protocolos que se hayan utilizado para las capas de red y transporte. Permite compartir archivos e impresoras así como ver los recursos disponibles en Entorno de red.

NetBIOS utiliza los puertos 137, 138 y 139. Es un protocolo exclusivo de máquinas Windows. Podemos averiguar si nuestro ordenador tiene NetBIOS activado utilizando el comando `netstat -an`. Este comando nos informará si tenemos los tres puertos anteriores en modo LISTENING.

```
C:\WINDOWS>netstat -an

Conexiones activas

Proto  Dirección local      Dirección remota  Estado
TCP    192.168.0.2:137  0.0.0.0:0         LISTENING
TCP    192.168.0.2:138  0.0.0.0:0         LISTENING
TCP    192.168.0.2:139  0.0.0.0:0         LISTENING
      UDP          192.168.0.2:137  *:*
UDP    192.168.0.2:138  *:*
```

Buena parte de las críticas de seguridad hacia los entornos Windows se centran en el protocolo NetBIOS. Por motivos de seguridad, este protocolo se debe deshabilitar siempre que no sea imprescindible. Veamos 4 ejemplos, ¿quién necesita tener activo el protocolo NetBIOS (puertos 137, 138 y 139 abiertos)? ¿quién debería deshabilitarlo?

1. Un servidor web
2. Un Windows 98 conectado a Internet mediante un módem
3. Un Windows 98 que participa en la red de una empresa

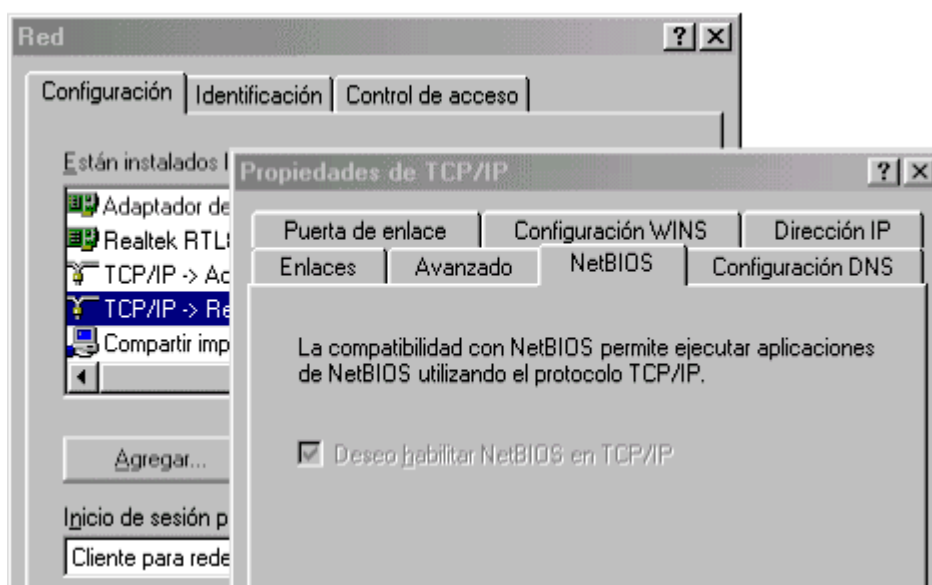
#### 4. Un servidor de usuarios y archivos

En el primer caso, NetBIOS debería estar deshabilitado ya que un servidor web no comparte recursos mediante Entorno de red ni accede a recursos compartidos de otros ordenadores (el servicio de páginas web, HTTP, funciona exclusivamente con TCP/IP). En el segundo caso, NetBIOS tampoco es necesario por las mismas razones anteriores. En el caso número tres las cosas cambian puesto que este ordenador probablemente necesite acceder a recursos compartidos de otros ordenadores así como imprimir en impresoras remotas. El servidor del ejemplo cuatro también requiere NetBIOS. Es necesario para que otros usuarios puedan acceder a sus archivos de una forma cómoda.

Nota: ¿Es posible acceder a archivos de otros ordenadores sin tener NetBIOS habilitado? Sí, desde luego: utilizando los servicios propios de TCP/IP. En concreto, el servicio de transferencia de archivos o FTP. El ordenador que ofrece los recursos se configura como servidor FTP (puerto 21 abierto). El resto de ordenadores utilizarán un cliente FTP para conectarse al servidor. Sin embargo, esto no permite trabajar directamente sobre archivos remotos, sino que es necesario hacer una copia previa de los archivos a nuestro ordenador antes de hacer modificaciones.

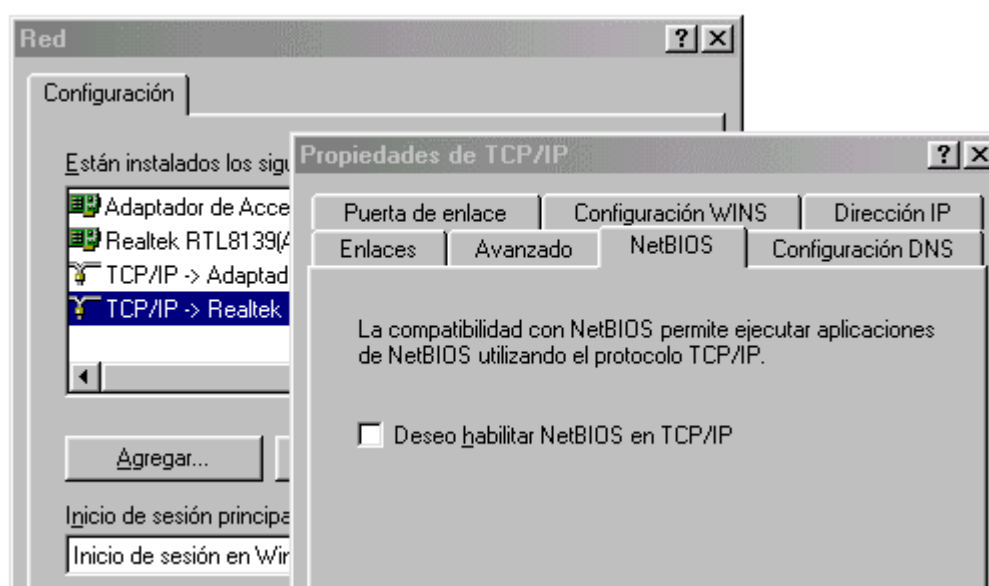
### Cómo deshabilitar NetBIOS en Windows 98

Probablemente hayamos observado que la casilla "Deseo habilitar NetBIOS en TCP/IP" situada en la pestaña NetBIOS de las propiedades de TCP/IP se encuentra marcada y no deja cambiarla. El comando netstat -an nos informará de que tenemos los puertos NetBIOS abiertos. ¿Cómo podemos deshabilitar NetBIOS? La clave se encuentra en el Cliente para redes Microsoft. Este componente de red permite acceder a recursos compartidos de otros ordenadores (es el que abre los puertos 137, 138 y 139). También es requerido, además del servicio Compartir archivos e impresoras para redes Microsoft, para compartir recursos en la red.



Los pasos a seguir son:

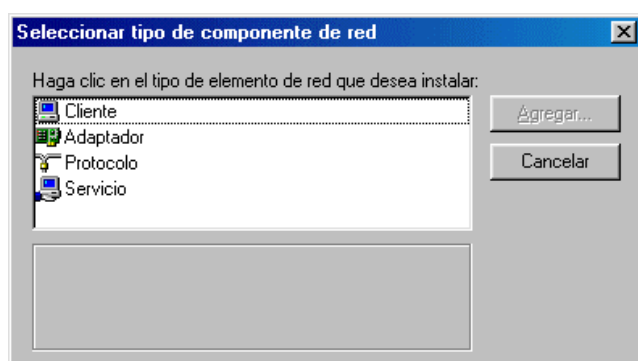
1. En las propiedades de Entorno de red eliminar todos los clientes instalados (ya sea el Cliente para redes Microsoft o el Inicio de sesión en Microsoft Family).
2. En las propiedades de TCP/IP podemos comprobar ya cómo la casilla "Deseo habilitar NetBIOS en TCP/IP" se ha desmarcado automáticamente.
3. Aceptamos la nueva configuración. Windows mostrará el aviso "Su red no está completa. ¿Desea continuar?". Indicamos "Sí" y reiniciamos el ordenador.
4. Al arrancar el ordenador no aparecerá la ventana de Inicio de sesión solicitándonos una contraseña, puesto que ahora no somos cliente de ninguna red Microsoft.
5. Con el comando netstat -an comprobar que no aparecen los puertos NetBIOS abiertos.



Con este procedimiento desaparecerá el icono Entorno de Red del escritorio, así como otros comandos NetBIOS (como el de Buscar PC). El ordenador ya no podrá compartir archivos ni impresoras (no podrá funcionar como servidor NetBIOS) ni podrá acceder a recursos compartidos (no podrá actuar como cliente NetBIOS). Sin embargo, los servicios de Internet (páginas web, FTP, correo...) seguirán funcionando debido a que no requieren NetBIOS para funcionar, sólo TCP/IP.

## 4.2 Instalación de una red en Windows 98

En las propiedades de Entorno de red se definen 4 familias de componentes de red:



1. Cliente. Permite acceder a recursos de otros puestos de la red. Utilizaremos el Cliente para redes Microsoft. Este componente es el responsable de la pantalla de Inicio de sesión que muestra Windows al arrancar

solicitándonos un nombre de usuario y contraseña. En las propiedades de este componente se indica si estamos montando una red entre iguales (casilla "Iniciar sesión en el dominio de Windows NT" deshabilitada) o una red cliente/servidor (casilla habilitada).

2. Adaptador. Es cada tarjeta de red real o virtual que tengamos instalada en nuestro ordenador. Las tarjetas de red reales son aquellas que instalamos físicamente en algún slot libre del ordenador. Las tarjetas virtuales son aquellas que instala Windows para emular a una tarjeta de red, aunque realmente no exista. El caso más común es el Adaptador de Acceso telefónico a redes que se corresponde con los modems o adaptadores RDSI del ordenador.

3. Protocolo. Es el lenguaje que utiliza nuestro ordenador para comunicarse con el resto de puestos de la red. Si bien se pueden definir varios protocolos para un mismo adaptador, no es recomendable con objeto de evitar tráfico innecesario en la red. Utilizaremos el protocolo TCP/IP. En redes pequeñas (menos de 10 ordenadores) y sin salida a Internet podemos considerar el uso del protocolo NetBEUI de TCP/IP.

4. Servicio. Se corresponde con el lado servidor de nuestro ordenador. Utilizaremos el servicio Compartir archivos e impresoras para redes Microsoft. Mediante el botón "Compartir archivos e impresoras" se puede configurar si ofreceremos archivos, impresoras o ambos recursos al resto de equipos de la red. Este servicio necesita que esté instalado el Cliente para redes Microsoft.

La instalación de una red TCP/IP en Windows 98 consiste en seguir los pasos siguientes para cada puesto de la red:

1. Instalar adaptador de red. Como para cualquier otro dispositivo la instalación se divide en:  
 a) Instalación física. Colocar la tarjeta de red en un slot libre. Si tuviésemos problemas con el funcionamiento de la tarjeta, después de haber realizado toda la configuración, probaremos a intercambiar los slots de la tarjeta de red con otra instalada anteriormente (esto fuerza una asignación de IRQs distinta).  
 b) Instalación lógica. Se recomienda instalar los últimos drivers del fabricante. En el caso de tarjetas de red Realtek (se identifican observando el circuito integrado principal de la tarjeta) los drivers están disponibles en [www.realtek.com.tw](http://www.realtek.com.tw).

2. Instalar protocolo TCP/IP y configurarlo.

3. Instalar Cliente para redes Microsoft. En las propiedades de este componente la casilla "Iniciar sesión en el dominio de Windows NT" debe estar desmarcada. El "Inicio de sesión principal" debe indicar "Cliente para redes Microsoft".

4. Configurar identificación NetBIOS. En la pestaña "Identificación" tenemos que dar un nombre al PC (distinto para cada puesto de la red) y un nombre al grupo de trabajo (probablemente sea el mismo para toda la red). Los grupos de trabajo son una forma de organizar los ordenadores dentro de Entorno de red; no imponen

restricciones de acceso.

5. Instalar servicio Compartir archivos e impresoras para redes Microsoft y configurarlo. Sólo lo haremos si queremos que el PC actúe como servidor.

Después de reiniciar el ordenador, Windows (más concretamente el Cliente para redes Microsoft) nos solicitará un nombre de usuario y contraseña. En este momento debemos elegir un nombre de usuario y contraseña que utilizaremos el resto de veces que iniciemos sesión. Si no lo hacemos y entramos pulsando "Cancelar", no podremos acceder a los recursos de la red (Entorno de red no funcionará).

Nota: Podemos tener varios adaptadores de red y para cada uno protocolos distintos. Cada protocolo "se enlaza" con un adaptador de red. Por ejemplo, podemos tener el protocolo NetBEUI enlazado con una tarjeta de red "Realtek RTL8029" y el protocolo TCP/IP enlazado con el "Adaptador de Acceso telefónico a redes". Aquellos enlaces que no sean imprescindibles se deben anular para evitar tráfico innecesario en la red.

## Contraseña de red Microsoft y contraseña de Windows

Windows utiliza dos tipos de contraseñas al iniciar sesión:

1. Contraseña de red Microsoft. Es necesaria para tener acceso a los recursos de la red. Nos valida como clientes de la red. Según hayamos configurado la casilla "Iniciar sesión en el dominio de Windows NT" de las propiedades de "Cliente para redes Microsoft" se dan los siguientes casos:

a. Casilla desmarcada. Equivale a una red entre iguales. Podemos escribir cualquier nombre de usuario / contraseña. Como no hay ningún ordenador que valide esta contraseña todas las que se nos ocurran serán válidas. No hay ninguna seguridad: cualquier usuario puede acceder a los recursos en red.

b. Casilla marcada. Equivale a una red cliente/servidor. El nombre de usuario / contraseña que escribamos serán comprobados por el controlador principal del dominio en el que estemos iniciando sesión. Sólo los usuarios correctamente autenticados podrán acceder a los recursos en red.

Nota: En los dos casos anteriores nos podemos "saltar" la ventana de contraseña de red pulsando la tecla "Escape" o el botón "Cancelar". De esta forma tendremos acceso al ordenador local pero no a los recursos en red.

2. Contraseña de Windows. Hace referencia al ordenador local, no a la red. Sin embargo, no impone restricciones de acceso a usuarios, únicamente es la llave que almacena otras contraseñas de Windows, como la clave de "Acceso telefónico a redes". Las contraseñas de Windows se gestionan desde Panel de control / Contraseñas. Solamente se le solicitará al usuario si la contraseña de red Microsoft que había tecleado anteriormente no coincide con una contraseña de Windows

válida. Lo habitual, por tanto, es que ambas contraseñas coincidan para que el usuario sólo tenga que teclearla una vez.

Los usuarios que hayan iniciado sesión en un ordenador con una determinada contraseña deberán introducir la misma las siguientes veces. De lo contrario, el sistema no le permitirá el paso. Sin embargo, se puede dar de alta un nuevo usuario con sólo teclearlo.

Nota: Nos podemos "saltar" la ventana de contraseña de Windows pulsando la tecla "Escape" o el botón "Cancelar". Sin embargo, no nos aparecerá ninguna contraseña guardada en los cuadros de diálogo de Windows (tendremos que teclearlas nuevamente). Además, ciertos programas no serán capaces de almacenar nuestras preferencias personales.

Nota: Las contraseñas de Windows se almacenan en archivos \*.pwl para cada usuario. Podemos eliminar todas las listas de contraseñas de Windows simplemente eliminando los archivos \*.pwl almacenados en el directorio de Windows.

¿Cómo proceder? Lo habitual es escribir únicamente la contraseña de red Microsoft de forma que ésta coincida con la contraseña de Windows. La primera vez se nos solicitará confirmar la contraseña de Windows (el sistema estará creando un nuevo usuario), pero las siguientes veces únicamente tendremos que teclear la contraseña una sola vez (Windows advertirá que ambas contraseñas coinciden). Según las explicaciones anteriores, debemos autenticarnos siempre como usuarios y no entrar con el botón "Cancelar". Este proceso se puede automatizar mediante la herramienta Tweak UI.

### ***4.3 Cómo acceder a recursos compartidos***

Las tres formas más habituales son las siguientes:

1. Entorno de red (doble clic en Entorno de red). No siempre refleja información actualizada de los ordenadores que están en red. Para que esta información sea lo más fiel posible se requiere tener instalado un [servidor de nombres](#).

2. Explorador de Windows (botón secundario en Entorno de Red / Explorar; o bien, Menú Inicio / Programas / Explorador de Windows). Este método equivale al anterior, aunque tiene la ventaja de mostrar los recursos compartidos clasificados en forma de árbol.



3. Buscar PC (botón secundario en Entorno de red / Buscar PC; o bien, Menú Inicio / Buscar / PC). Es el método más eficiente a la hora de localizar ordenadores en la red.

Windows utiliza nombres UNC para indicar la ruta de recursos compartidos en la red. Por ejemplo: \\saturno\recurso1\carpeta2 hace referencia a la carpeta "carpeta2" que se encuentra dentro del recurso compartido "recurso1" perteneciente al ordenador "saturno".

#### ***4.4 Cómo compartir carpetas y unidades de disco***

Para que un ordenador pueda compartir carpetas, unidades de disco o impresoras, tiene que haberse configurado antes como servidor. Esto se consigue agregando el [servicio](#) "Compartir archivos e impresoras".

Los recursos de red son elementos que pueden ofrecerse (compartirse) a otros usuarios de la red. Las carpetas, unidades de disco o impresoras son, por tanto, recursos de red. La forma de compartirlos es similar para todos ellos: botón secundario del ratón sobre el recurso / Compartir.

En el cuadro "Compartir" tenemos que indicar el tipo de acceso (estos tipos de acceso no son aplicables a impresoras):

- Sólo lectura. Otros usuarios de la red sólo podrán ver el contenido del recurso compartido pero no modificarlo.
- Completo. También podrán modificarlo.
- Depende de contraseña. Según la contraseña que escriba el usuario, tendrá un acceso de "Sólo lectura" o "Completo".

Nota: Observe, en el momento de compartir una carpeta, que el nombre del recurso compartido (como lo verán otros usuarios de la red) no tiene por qué coincidir con el nombre de la carpeta (como se verá desde el ordenador local). Es preferible que los nombres de los recursos compartidos no contengan espacios ni caracteres especiales.

#### ***4.5 Unidades de red***

A los usuarios les resulta una tarea incómoda buscar sus archivos dentro de Entorno de red (hay que hacer un elevado número de clics de ratón). Sería interesante que los

recursos compartidos apareciesen dentro de "Mi PC" como si fuesen otras unidades más. Esto es justamente lo que deseamos hacer: crear unidades de red (tendrán asignadas letras de unidad) a partir de recursos compartidos.

Nota: Se utiliza el término "unidades de red" para distinguir estas unidades de las "unidades de disco". Una "unidad" se caracteriza por tener asociada una "letra de unidad". En Mi PC se utilizan iconos distintos para una unidad de disco (perteneciente al ordenador local) y para una unidad de red (recurso compartido de otro ordenador de la red).

1. Hacer clic con el botón secundario del ratón en un recurso compartido y elegir "Conectar a unidad de red".
2. Seleccionar una letra de unidad (habitualmente se eligen las letras altas del alfabeto, como la X:, Y: o Z:)
3. Indicar si queremos que esta unidad de red sea permanente o temporal ("Conectar de nuevo al iniciar sesión").

Para eliminar una unidad de red creada con anterioridad elegimos "Desconectar" del menú contextual de la unidad de red.

## ***4.6 Cómo instalar una impresora en red***

En el servidor de impresión:

1. Instalar la impresora de forma local y comprobar su funcionamiento. En la pestaña "Detalles" de las propiedades de la impresora indicará un puerto físico (LPT1, por ejemplo).
2. Compartir la impresora.

En los clientes:

1. Buscar la impresora compartida en Entorno de red.
2. Hacer doble clic en la impresora y seguir los pasos para la instalación.
3. Comprobar en Panel de control / Impresoras que se ha agregado una nueva impresora. En la pestaña "Detalles" de sus propiedades indicará el nombre del recurso compartido de la impresora en red (por ejemplo, \\servidor\epson).

Nota: Para algunos modelos de impresoras el procedimiento anterior no funciona. En estos casos, hay que instalar los drivers del fabricante en cada uno de los ordenadores cliente (como si la impresora estuviese conectada directamente a cada ordenador) y después, cambiar el puerto "LPT1" por un puerto de red "\\servidor\epson".

Nota: En el servidor se instala una "impresora local". En los clientes se instala la "impresora en red" del servidor.

## 4.7 Programas de monitorización de la red

Los programas Monitor de red y Monitor del sistema se encuentran en Menú Inicio / Programas / Accesorios / Herramientas del sistema. Si no apareciesen, se pueden instalar desde Panel de control / Agregar o quitar programas / Instalación de Windows / Herramientas del sistema.

### Monitor de red

Controla de forma centralizada el lado servidor de nuestro ordenador y muestra los recursos que está sirviendo a otros usuarios de la red. Desde el menú "Ver" se puede cambiar de vista:

- Por conexiones. Indica los usuarios que están conectados a nuestro ordenador.
- Por carpetas compartidas. Enumera las carpetas y unidades de disco que están compartidas. Para cada recurso compartido muestra los usuarios que están conectados en ese momento. Desde el menú "Administrar" se pueden compartir nuevos recursos o dejar de compartir los que ya lo están.
- Por archivos abiertos. Lista los archivos de nuestro ordenador que están siendo utilizados por otros usuarios de la red.

### Monitor del sistema

Muestra estadísticas de forma gráfica. Las gráficas que nos interesan desde el punto de vista de la monitorización de la red son:

- Cliente de Microsoft Network: Bytes leídos/s. Tasa de información que estamos recibiendo desde la red.
- Cliente de Microsoft Network: Bytes escritos/s. Tasa de información que estamos enviando a la red.
- Servidor de redes Microsoft: Bytes leídos/s. Tasa de información que otros usuarios están recibiendo de nuestro ordenador.
- Servidor de redes Microsoft: Bytes escritos/s. Tasa de información que otros usuarios están enviando a nuestro ordenador.

Si disponemos de una conexión a Internet por medio de Acceso telefónico a redes, podemos monitorizar la velocidad que tenemos en cada instante:

- Dial-Up Adapter: Bytes Received/Second. Velocidad entrante de nuestra conexión a Internet medida en bytes por segundo (si la multiplicamos por 8, tendremos bits por segundo = bps)
- Dial-Up Adapter: Bytes Transmitted/Second. Velocidad saliente.

## 4.8 Resolución de nombres

La utilización de nombres para referirnos a los ordenadores de una red resulta habitualmente más cómodo que tratar directamente con direcciones IP. Sin embargo, la

familia de protocolos TCP/IP no es capaz de llegar hasta un ordenador sólo con su nombre: necesita obtener su dirección IP antes. El mecanismo de traducción de nombres a direcciones IP es lo que se conoce como resolución de nombres. Siempre que escribamos un nombre, ya sea en el cuadro de "Buscar PC" de Windows, en un navegador web o en un comando TCP/IP, el ordenador tendrá que dar el paso extra de averiguar su dirección IP antes de poder continuar (será ligeramente más lento que si tecleamos su dirección IP).

## Distinción entre nombres NetBIOS y nombres de dominio

Un ordenador Windows con TCP/IP instalado tiene dos nombres que suelen coincidir:

- Nombre NetBIOS. Es el nombre que se define en el cuadro "Nombre de PC" dentro de la pestaña "Identificación" de las propiedades de Entorno de red. Este nombre es el que utiliza Windows en Entorno de Red.
- Nombre de dominio (o nombre de host). Es el nombre que se define en la pestaña "Configuración DNS" de las propiedades de TCP/IP. El nombre de dominio completo es el nombre de host seguido de un punto y del dominio. Por ejemplo, si el host es "servidor" y el dominio es "mired", el nombre de dominio completo será "servidor.mired". El nombre de dominio se utiliza para identificar un ordenador en Internet (por ejemplo, goliat.sim.ucm.es).

Nota: Un ordenador que no sea Windows (o sea Windows pero con NetBIOS deshabilitado) no tendrá nombre NetBIOS. Por otro lado, un ordenador Windows que no tenga el protocolo TCP/IP instalado no tendrá nombre de dominio. Un servidor web en Linux es un ejemplo del primer caso y un Windows Me que utilice sólo el protocolo NetBEUI es un ejemplo del segundo.

En los siguientes apartados estudiamos los principales mecanismos de resolución de nombres que permiten traducir un nombre NetBIOS o un nombre de dominio a su correspondiente dirección IP.

## Métodos de resolución de nombres NetBIOS

- Caché NetBIOS. Es una tabla dinámica almacenada en cada ordenador que contiene los últimos nombres que se han resuelto por otros métodos. Esta tabla se puede visualizar mediante el comando `nbtstat -c`.
- Broadcasting. Se pregunta el nombre a todos los ordenadores de la red.
- Archivo LMHOSTS. Es un archivo de texto, situado en cada ordenador de la red, que contiene una lista de direcciones IP y nombres NetBIOS.
- Servidor WINS. Es un ordenador que contiene una lista centralizada de direcciones IP y nombres NetBIOS. Esta lista se crea de forma dinámica a medida que se van conectando y desconectando ordenadores en la red. Su configuración se estudia en el apartado [Servidor WINS](#).

El método de resolución que funciona en una red si no se ha configurado otro es broadcasting. Este método resuelve los nombres de forma correcta, sin embargo genera un elevado tráfico en la red. Podemos conocer la cantidad de nombres que se han resuelto mediante broadcasting utilizando el comando `nbtstat -r` (línea "Resolved By Broadcast").

Cada vez que Windows resuelve un nombre lo almacena durante unos segundos en su caché NetBIOS (nbtstat -c). Esta tabla la consultará antes de realizar un broadcasting.

Podemos reducir el número de mensajes de broadcasting en una red sin necesidad de emplear un servidor mediante la creación, en cada máquina, de una lista con todos los nombres NetBIOS de nuestra red y sus correspondientes direcciones IP. Esta lista se debe incluir en un archivo llamado LMHOSTS. Sigue la siguiente sintaxis:

#	Ejemplo	de	archivo	LMHOSTS
192.168.0.1		router		#PRE
192.168.0.5		minerva		#PRE
192.168.0.6	saturno			#PRE

Si utilizamos Windows 98 o Me encontraremos un archivo de ejemplo en C:\WINDOWS\LMHOSTS.SAM. Este archivo debemos renombrarlo para que se llame C:\WINDOWS\LMHOSTS. En Windows NT y 2000, la ubicación de ambos archivos es C:\WINNT\SYSTEM32\DRIVERS\ETC. Después introduciremos los cambios necesarios mediante el Bloc de notas o cualquier otro editor de textos. Para que los cambios comiencen a funcionar debemos escribir el comando nbtstat -R. A continuación podemos comprobar que los nombres se han almacenado correctamente escribiendo nbtstat -c.

Windows comprobará el archivo LMHOSTS antes de hacer un broadcasting a la red. El comando nbtstat -r nos permite comprobar cómo no se generan nuevos mensajes a toda la red para los nombres que hayamos incluido en LMHOSTS. El problema de este método es su difícil mantenimiento ya que cualquier cambio se debe reflejar en todos los ordenadores de la red. Sin embargo, se pueden buscar formas para que el archivo LMHOSTS se actualice automáticamente desde una sola máquina (por ejemplo, mediante un script de inicio de sesión de Windows NT o mediante la cláusula #INCLUDE de los archivos LMHOSTS).

El método más recomendable para redes medianas y grandes es utilizar un servidor de nombres NetBIOS. Este servidor es una máquina Windows NT o 2000 con el Servicio de nombres de Internet para Windows (WINS) configurado. En la pestaña "Configuración WINS" de las propiedades de TCP/IP de cada ordenador cliente tenemos que indicar la dirección IP del servidor WINS que hayamos configurado. Cada vez que escribamos un nombre, nuestro ordenador preguntará al servidor WINS en lugar de hacer un broadcasting a toda la red. Un servidor de nombres asegura, además, que los equipos mostrados en Entorno de red se corresponden con los que realmente están funcionando en la red.

## Métodos de resolución de nombres de dominio

- Local host. Se compara el nombre con el del propio PC. El resto de nombres no es capaz de resolverlos.
- Archivo HOSTS. Es un archivo de texto, situado en cada ordenador de la red, que contiene una lista de direcciones IP y nombres de dominio.
- Servidor DNS. Es un ordenador que contiene una lista centralizada de direcciones IP y nombres de dominio.

Si en una red no configuramos ningún método de resolución de nombres de dominio, el único que funcionará será Local host. Es decir, cada ordenador sólo será capaz de resolver su propio nombre pero no el resto de los nombres de la red ni de Internet.

Para permitir que los ordenadores de la red sean accesibles por su nombre de dominio podemos utilizar archivos HOSTS. En cada puesto de la red tenemos que crear un archivo que incluya al resto de ordenadores, siguiendo la siguiente sintaxis:

#	Ejemplo	de	archivo	HOSTS
192.168.0.1				router.mired
192.168.0.1				router
192.168.0.5				minerva.mired
192.168.0.6	saturno.mired			

Los comentarios que hicimos en la sección anterior sobre la ubicación y uso del archivo LMHOSTS son aplicables al archivo HOSTS (pero no así el comando nbtstat que es exclusivo de nombres NetBIOS). La mejor solución, sin embargo, es configurar un servidor DNS que resuelva no sólo los nombres de nuestra propia red sino también los del resto de Internet (será un [servidor DNS local](#)). En la pestaña "Configuración DNS" de las propiedades de TCP/IP de cada ordenador cliente tenemos que indicar la dirección IP del servidor DNS. Se puede indicar una dirección IP que no sea de nuestra propia red.

## 4.9 Configuración manual de ICS

Windows 98 SE y Windows Me incorporan un servidor proxy doméstico para dar salida a Internet a toda una red privada. Por ejemplo, una red con 5 ordenadores de los cuales sólo uno de ellos tiene módem, podemos configurarla para que todos los puestos tengan Internet compartiendo la conexión del módem. Llamaremos proxy al ordenador que tiene el módem, adaptador RDSI u otra forma de conexión. El proxy compartirá el adaptador virtual de Acceso telefónico a redes a través de su tarjeta de red con el resto de equipos de la red.

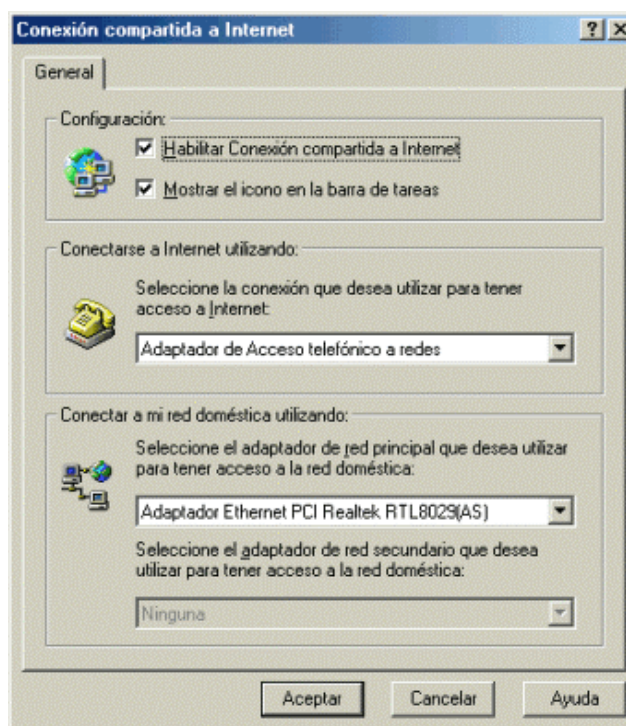
### Configuración del servidor proxy:

1. Comprobar que el proxy tiene conexión a Internet mediante una conexión de Acceso telefónico a redes.
2. Instalar "Conexión compartida a Internet". Se encuentra en Panel de control / Agregar o quitar programas / Instalación de Windows / Herramientas de Internet. Durante la configuración indicaremos que estamos conectados a Internet mediante el "Adaptador de Acceso telefónico a redes" y a nuestra red doméstica mediante la tarjeta de red. No es necesario que creamos el disquete que nos propone el asistente.

Después de los pasos anteriores, Windows habrá asignado al proxy la dirección IP 192.168.0.1 con máscara 255.255.255.0. Con la "Conexión compartida a Internet" instalada, la configuración de red no se debe modificar directamente: toda la configuración la haremos desde Panel de control / Herramientas de Internet / Conexiones / Compartir. Si más adelante necesitamos cambiar la configuración de las propiedades de Entorno de red, tendremos que desinstalar antes "Conexión compartida a Internet".

ICS (Conexión compartida a Internet) convierte al proxy no sólo en puerta de salida (gateway) para Internet sino también en un servidor DNS local. Precisamente estos datos serán los que tengamos que configurar en los ordenadores clientes.

### Configuración de los clientes:



1. Asignar una dirección IP de la red 192.168.0.0 / 255.255.255.0. Por ejemplo: 192.168.0.2 / 255.255.255.0 a un ordenador; 192.168.0.3 / 255.255.255.0 a otro; etc.
2. En "Puerta de enlace" agregar la dirección del proxy (192.168.0.1).
3. En "Configuración DNS" añadir el servidor 192.168.0.1

## Capítulo 5 TCP/IP

### Introducción

Internet no es un nuevo tipo de red física, sino un conjunto de tecnologías que permiten interconectar redes muy distintas entre sí. Internet no es dependiente de la máquina ni del sistema operativo utilizado. De esta manera, podemos transmitir información entre un servidor Unix y un ordenador que utilice Windows 98. O entre plataformas completamente distintas como Macintosh, Alpha o Intel. Es más: entre una máquina y otra generalmente existirán redes distintas: redes Ethernet, redes Token Ring e incluso enlaces vía satélite. Como vemos, está claro que no podemos utilizar ningún protocolo que dependa de una arquitectura en particular. Lo que estamos buscando es un método de interconexión general que sea válido para cualquier plataforma, sistema operativo y tipo de red. La familia de protocolos que se eligieron para permitir que Internet sea una Red de redes es TCP/IP. Nótese aquí que hablamos de familia de protocolos ya que son muchos los protocolos que la

integran, aunque en ocasiones para simplificar hablemos sencillamente del protocolo TCP/IP.

El protocolo TCP/IP tiene que estar a un nivel superior del tipo de red empleado y funcionar de forma transparente en cualquier tipo de red. Y a un nivel inferior de los programas de aplicación (páginas WEB, correo electrónico...) particulares de cada sistema operativo. Todo esto nos sugiere el siguiente modelo de referencia:

<b>Capa de aplicación</b> (HTTP, SMTP, FTP, TELNET...)
<b>Capa de transporte</b> (UDP, TCP)
<b>Capa de red</b> (IP)
<b>Capa de acceso a la red</b> (Ethernet, Token Ring...)
<b>Capa física</b> (cable coaxial, par trenzado...)

El nivel más bajo es la capa física. Aquí nos referimos al medio físico por el cual se transmite la información. Generalmente será un cable aunque no se descarta cualquier otro medio de transmisión como ondas o enlaces vía satélite.

La capa de acceso a la red determina la manera en que las estaciones (ordenadores) envían y reciben la información a través del soporte físico proporcionado por la capa anterior. Es decir, una vez que tenemos un cable, ¿cómo se transmite la información por ese cable? ¿Cuándo puede una estación transmitir? ¿Tiene que esperar algún turno o transmite sin más? ¿Cómo sabe una estación que un mensaje es para ella? Pues bien, son todas estas cuestiones las que resuelve esta capa.

Las dos capas anteriores quedan a un nivel inferior del protocolo TCP/IP, es decir, no forman parte de este protocolo. La capa de red define la forma en que un mensaje se transmite a través de distintos tipos de redes hasta llegar a su destino. El principal protocolo de esta capa es el IP aunque también se encuentran a este nivel los protocolos ARP, ICMP e IGMP. Esta capa proporciona el direccionamiento IP y determina la ruta óptima a través de los encaminadores (routers) que debe seguir un paquete desde el origen al destino.

La capa de transporte (protocolos TCP y UDP) ya no se preocupa de la ruta que siguen los mensajes hasta llegar a su destino. Sencillamente, considera que la comunicación extremo a extremo está establecida y la utiliza. Además añade la noción de puertos, como veremos más adelante.

Una vez que tenemos establecida la comunicación desde el origen al destino nos queda lo más importante, ¿qué podemos transmitir? La capa de aplicación nos proporciona los distintos servicios de Internet: correo electrónico, páginas Web, FTP, TELNET...

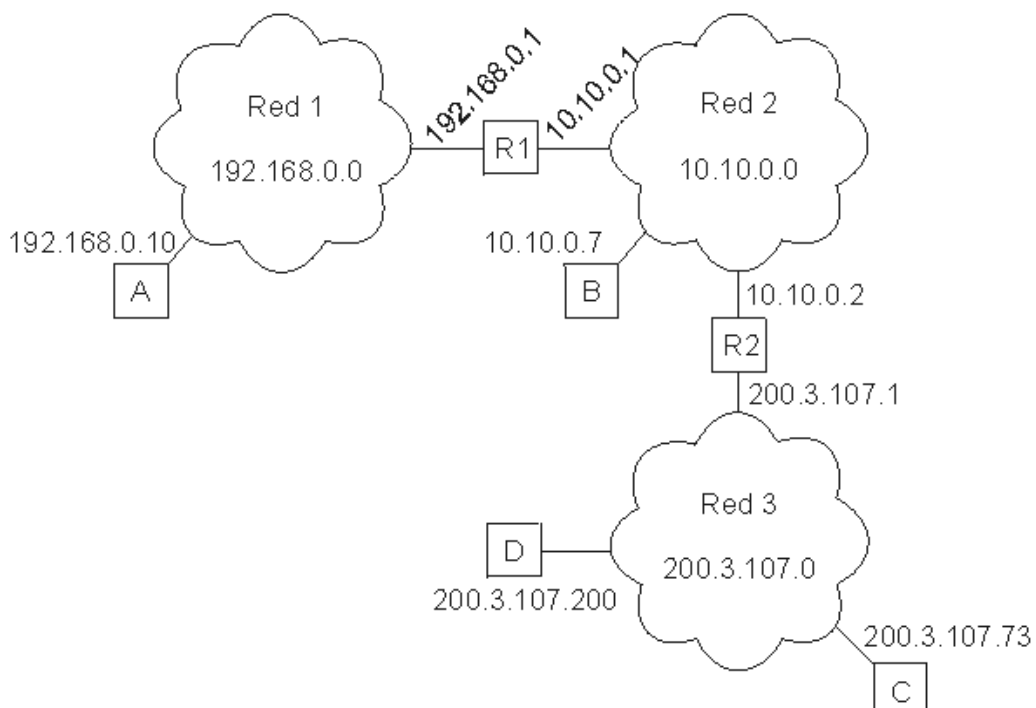
## ***5.1 Capa de red***

La familia de protocolos TCP/IP fue diseñada para permitir la interconexión entre distintas redes. El mejor ejemplo de interconexión de redes es Internet: se trata de un conjunto de redes unidas mediante encaminadores o routers.

Host	Dirección física	Dirección IP	Red
A	00-60-52-0B-B7-7D	192.168.0.10	Red 1
R1	00-E0-4C-AB-9A-FF	192.168.0.1	
B	A3-BB-05-17-29-D0	10.10.0.1	Red 2
	00-E0-4C-33-79-AF	10.10.0.7	
R2	B2-42-52-12-37-BE	10.10.0.2	
C	00-E0-89-AB-12-92	200.3.107.1	Red 3
	A3-BB-08-10-DA-DB	200.3.107.73	
D	B2-AB-31-07-12-93	200.3.107.200	

A lo largo de este Curso aprenderemos a construir redes privadas que funcionen siguiendo el mismo esquema de Internet. En una red TCP/IP es posible tener, por ejemplo, servidores web y servidores de correo para uso interno. Obsérvese que todos los servicios de Internet se pueden configurar en pequeñas redes internas TCP/IP.

A continuación veremos un ejemplo de interconexión de 3 redes. Cada host (ordenador) tiene una [dirección física](#) que viene determinada por su adaptador de red. Estas direcciones se corresponden con la [capa de acceso al medio](#) y se utilizan para comunicar dos ordenadores que pertenecen a la misma red. Para identificar globalmente un ordenador dentro de un conjunto de redes TCP/IP se utilizan las direcciones IP (capa de red). Observando una dirección IP sabremos si pertenece a nuestra propia red o a una distinta (todas las direcciones IP de la misma red comienzan con los mismos números, según veremos más adelante).



El concepto de red está relacionado con las direcciones IP que se configuren en cada ordenador, no con el cableado. Es decir, si tenemos varias redes dentro del mismo cableado solamente los ordenadores que permanezcan a una misma red podrán comunicarse entre sí. Para que los ordenadores de una red puedan comunicarse con los de otra red es necesario que existan routers que interconecten las redes. Un router o encaminador no es más que un ordenador con varias direcciones IP, una para cada red, que permita el tráfico de paquetes entre sus redes.

La capa de red se encarga de fragmentar cada mensaje en paquetes de datos llamados datagramas IP y de enviarlos de forma independiente a través de la red de redes. Cada datagrama IP incluye un campo con la dirección IP de destino. Esta información se utiliza para enrutar los datagramas a través de las redes necesarias que los hagan llegar hasta su destino.

Nota: Cada vez que visitamos una página web o recibimos un correo electrónico es habitual atravesar un número de redes comprendido entre 10 y 20, dependiendo de la distancia de los hosts. El tiempo que tarda un datagrama en atravesar 20 redes (20 routers) suele ser inferior a 600 milisegundos.

En el ejemplo anterior, supongamos que el ordenador 200.3.107.200 (D) envía un mensaje al ordenador con 200.3.107.73 (C). Como ambas direcciones comienzan con los mismos números, D sabrá que ese ordenador se encuentra dentro de su propia red y el mensaje se entregará de forma directa. Sin embargo, si el ordenador 200.3.107.200 (D) tuviese que comunicarse con 10.10.0.7 (B), D advertiría que el ordenador destino no pertenece a su propia red y enviaría el mensaje al router R2 (es el ordenador que le da salida a otras redes). El router entregaría el mensaje de forma directa porque B se encuentra dentro de una de sus redes (la Red 2).

## Direcciones IP

La dirección IP es el identificador de cada host dentro de su red de redes. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos ordenadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

Las direcciones IP se clasifican en:

- Direcciones IP públicas. Son visibles en todo Internet. Un ordenador con una IP pública es accesible (visible) desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.
- Direcciones IP privadas (reservadas). Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router (o proxy)

que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

- Direcciones IP estáticas (fijas). Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.

- Direcciones IP dinámicas. Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

Las direcciones IP están formadas por 4 bytes (32 bits). Se suelen representar de la forma a.b.c.d donde cada una de estas letras es un número comprendido entre el 0 y el 255. Por ejemplo la dirección IP del servidor de IBM (www.ibm.com) es 129.42.18.99.

Las direcciones IP también se pueden representar en hexadecimal, desde la 00.00.00.00 hasta la FF.FF.FF.FF o en binario, desde la 00000000.00000000.00000000.00000000 hasta la 11111111.11111111.11111111.11111111.

Las tres direcciones siguientes representan a la misma máquina (podemos utilizar la calculadora científica de Windows para realizar las conversiones).

(decimal)	128.10.2.30
(hexadecimal)	80.0A.02.1E
(binario)	10000000.00001010.00000010.00011110

¿Cuántas direcciones IP existen? Si calculamos 2 elevado a 32 obtenemos más de 4000 millones de direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a hosts. Las direcciones IP no se encuentran aisladas en Internet, sino que pertenecen siempre a alguna red. Todas las máquinas conectadas a una misma red se caracterizan en que los primeros bits de sus direcciones son iguales. De esta forma, las direcciones se dividen conceptualmente en dos partes: el identificador de red y el identificador de host.

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las clases primarias A, B y C. La clase D está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de clase E no se pueden utilizar (están reservadas).

	0	1	2	3	4	8	16	24	31	
<b>Clase A</b>	0	red				host				
<b>Clase B</b>	1	0	red				host			

<b>Clase C</b>	110	red	host
<b>Clase D</b>	1110	grupo de multicast (multidifusión)	
<b>Clase E</b>	1111	(direcciones reservadas: no se pueden utilizar)	

Nota: Las direcciones usadas en Internet están definidas en la RFC

Clase	Formato (r=red, h=host)	Número de redes	Número de hosts por red	Rango de direcciones de redes	Máscara de subred
<b>A</b>	r.h.h.h	128	16.777.214	0.0.0.0 - 127.0.0.0	255.0.0.0
<b>B</b>	r.r.h.h	16.384	65.534	128.0.0.0 - 191.255.0.0	255.255.0.0
<b>C</b>	r.r.r.h	2.097.152	254	192.0.0.0 - 223.255.255.0	255.255.255.0
<b>D</b>	grupo	-	-	224.0.0.0 - 239.255.255.255	-
<b>E</b>	no válidas	-	-	240.0.0.0 - 255.255.255.255	-

1166 ([en inglés](#)).

Difusión (broadcast) y multidifusión (multicast).-- El término difusión (broadcast) se refiere a todos los hosts de una red; multidifusión (multicast) se refiere a varios hosts (aquellos que se hayan suscrito dentro de un mismo grupo). Siguiendo esta misma terminología, en ocasiones se utiliza el término unidifusión para referirse a un único host.

## Direcciones IP especiales y reservadas

No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un host: algunas de ellas tienen significados especiales. Las principales direcciones especiales se resumen en la siguiente tabla. Su interpretación depende del host desde el que se utilicen.

Bits de red	Bits de host	Significado	Ejemplo
todos 0		Mi propio host	0.0.0.0
todos 0	host	Host indicado dentro de mi red	0.0.0.10
red	todos 0	Red indicada	192.168.1.0
todos 1		Difusión a mi red	255.255.255.255
red	todos 1	Difusión a la red indicada	192.168.1.255
127	cualquier valor válido de host	Loopback (mi propio host)	127.0.0.1

Difusión o broadcasting es el envío de un mensaje a todos los ordenadores que se encuentran en una red. La dirección de loopback (normalmente 127.0.0.1) se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados en nuestro propio ordenador. Lo veremos más adelante, al estudiar el comando PING.

Las direcciones de redes siguientes se encuentran reservadas para su uso en redes privadas (intranets). Una dirección IP que pertenezca a una de estas redes se dice que es una dirección IP privada.

Clase	Rango de direcciones reservadas de redes
A	10.0.0.0
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0

**Intranet.**-- Red privada que utiliza los protocolos TCP/IP. Puede tener salida a Internet o no. En el caso de tener salida a Internet, el direccionamiento IP permite que los hosts con direcciones IP privadas puedan salir a Internet pero impide el acceso a los hosts internos desde Internet. Dentro de una intranet se pueden configurar todos los servicios típicos de Internet (web, correo, mensajería instantánea, etc.) mediante la instalación de los correspondientes servidores. La idea es que las intranets son como "internets" en miniatura o lo que es lo mismo, Internet es una intranet pública gigantesca.

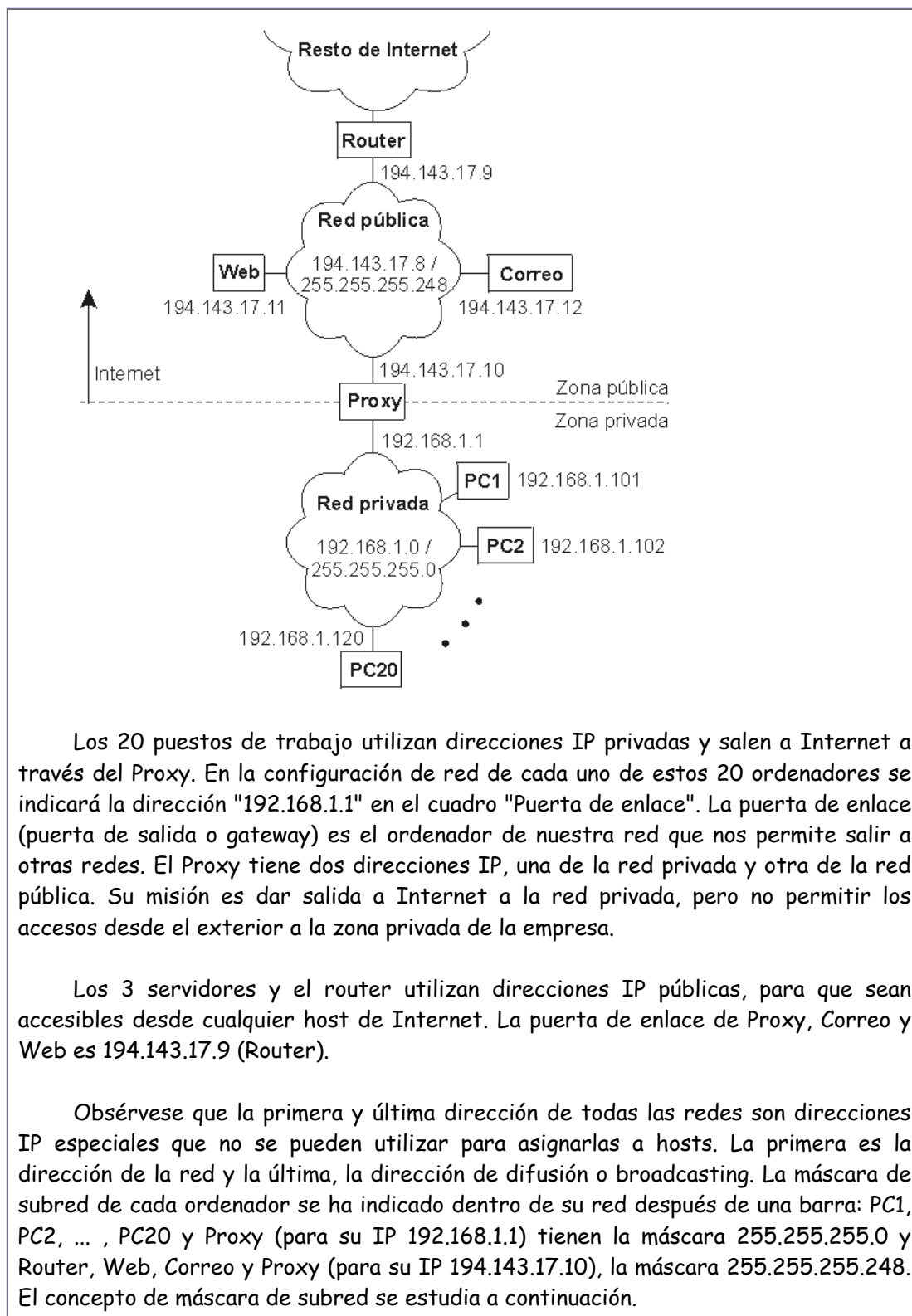
**Extranet.**-- Unión de dos o más intranets. Esta unión puede realizarse mediante líneas dedicadas (RDSI, X.25, frame relay, punto a punto, etc.) o a través de Internet.

**Internet.**-- La mayor red pública de redes TCP/IP.

Por ejemplo, si estamos construyendo una red privada con un número de ordenadores no superior a 254 podemos utilizar una red reservada de clase C. Al primer ordenador le podemos asignar la dirección 192.168.23.1, al segundo 192.168.23.2 y así sucesivamente hasta la 192.168.23.254. Como estamos utilizando direcciones reservadas, tenemos la garantía de que no habrá ninguna máquina conectada directamente a Internet con alguna de nuestras direcciones. De esta manera, no se producirán conflictos y desde cualquiera de nuestros ordenadores podremos acceder a la totalidad de los servidores de Internet (si utilizásemos en un ordenador de nuestra red una dirección de un servidor de Internet, nunca podríamos acceder a ese servidor).

**CASO PRÁCTICO.**-- Una empresa dispone de una línea frame relay con direcciones públicas contratadas desde la 194.143.17.8 hasta la 194.143.17.15 (la dirección de la red es 194.143.17.8, su dirección de broadcasting 194.143.17.15 y su máscara de red 255.255.255.248). La línea frame relay está conectada a un router. Diseñar la red para:

- 3 servidores (de correo, web y proxy)
- 20 puestos de trabajo



## Máscara de subred

Una máscara de subred es aquella dirección que enmascarando nuestra dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no.

La siguiente tabla muestra las máscaras de subred correspondientes a cada clase:

Clase	Máscara de subred
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Si expresamos la máscara de subred de clase A en notación binaria, tenemos:

11111111.00000000.00000000.00000000

Los unos indican los bits de la dirección correspondientes a la red y los ceros, los correspondientes al host. Según la máscara anterior, el primer byte (8 bits) es la red y los tres siguientes (24 bits), el host. Por ejemplo, la dirección de clase A 35.120.73.5 pertenece a la red 35.0.0.0.

Supongamos una subred con máscara 255.255.0.0, en la que tenemos un ordenador con dirección 148.120.33.110. Si expresamos esta dirección y la de la máscara de subred en binario, tenemos:

```

148.120.33.110 10010100.01111000.00100001.01101110 (dirección de una máquina)
255.255.0.0   11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.120.0.0   10010100.01111000.00000000.00000000 (dirección de su subred)
<-----RED-----> <-----HOST----->

```

Al hacer el producto binario de las dos primeras direcciones (donde hay dos 1 en las mismas posiciones ponemos un 1 y en caso contrario, un 0) obtenemos la tercera.

Si hacemos lo mismo con otro ordenador, por ejemplo el 148.120.33.89, obtenemos la misma dirección de subred. Esto significa que ambas máquinas se encuentran en la misma subred (la subred 148.120.0.0).

```

148.120.33.89 10010100.01111000.00100001.01011001 (dirección de una máquina)
255.255.0.0   11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.120.0.0   10010100.01111000.00000000.00000000 (dirección de su subred)

```

En cambio, si tomamos la 148.115.89.3, observamos que no pertenece a la misma subred que las anteriores.

```

148.115.89.3 10010100.01110011.01011001.00000011 (dirección de una máquina)
255.255.0.0   11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.115.0.0   10010100.01110011.00000000.00000000 (dirección de su subred)

```

Cálculo de la dirección de difusión.-- Ya hemos visto que el producto lógico binario (AND) de una IP y su máscara devuelve su dirección de red. Para calcular su dirección de difusión, hay que hacer la suma lógica en binario (OR) de la IP con el inverso (NOT) de su máscara.

En una red de redes TCP/IP no puede haber hosts aislados: todos pertenecen a alguna red y todos tienen una dirección IP y una máscara de subred (si no se especifica se toma la máscara que corresponda a su clase). Mediante esta máscara un ordenador sabe si otro ordenador se encuentra en su misma subred o en otra distinta. Si pertenece a su misma subred, el mensaje se entregará directamente. En cambio, si los hosts están configurados en redes distintas, el mensaje se enviará a la puerta de salida o router de la red del host origen. Este router pasará el mensaje al siguiente de la cadena y así sucesivamente hasta que se alcance la red del host destino y se complete la entrega del mensaje.

Las máscaras 255.0.0.0 (clase A), 255.255.0.0 (clase B) y 255.255.255.0 (clase C) suelen ser suficientes para la mayoría de las redes privadas. Sin embargo, las redes más pequeñas que podemos formar con estas máscaras son de 254 hosts y para el caso de direcciones públicas, su contratación tiene un coste muy alto. Por esta razón suele ser habitual dividir las redes públicas de clase C en subredes más pequeñas. A continuación se muestran las posibles divisiones de una red de clase C. La división de una red en subredes se conoce como subnetting.

Máscara de subred	Binario	Número de subredes	Núm. de hosts por subred	Ejemplos de subredes (x=a.b.c por ejemplo, 192.168.1)
255.255.255.0	00000000	1	254	x.0
255.255.255.128	10000000	2	126	x.0, x.128
255.255.255.192	11000000	4	62	x.0, x.64, x.128, x.192
255.255.255.224	11100000	8	30	x.0, x.32, x.64, x.96, x.128, ...
255.255.255.240	11110000	16	14	x.0, x.16, x.32, x.48, x.64, ...
255.255.255.248	11111000	32	6	x.0, x.8, x.16, x.24, x.32, x.40, ...
255.255.255.252	11111100	64	2	x.0, x.4, x.8, x.12, x.16, x.20, ...
255.255.255.254	11111110	128	0	ninguna posible
255.255.255.255	11111111	256	0	ninguna posible

Obsérvese que en el caso práctico que explicamos un poco más arriba se utilizó la máscara 255.255.255.248 para crear una red pública con 6 direcciones de hosts válidas (la primera y última dirección de todas las redes se excluyen). Las máscaras con bytes distintos a 0 o 255 también se pueden utilizar para particionar redes de clase A o de clase B, sin embargo no suele ser lo más habitual. Por ejemplo, la máscara 255.255.192.0 dividiría una red de clase B en 4 subredes de 16382 hosts ( $2^{14} - 2$ ) cada una.

### EJERCICIOS

1. Calcular la dirección de red y dirección de broadcasting (difusión) de las máquinas con las siguientes direcciones IP y máscaras de subred (si no se especifica, se utiliza la máscara por defecto):

• 18.120.16.250: máscara 255.0.0.0 red 18.0.0.0 broadcasting

18.255.255.255

- 18.120.16.255 / 255.255.0.0: red 18.120.0.0, broadcasting

18.120.255.255

- 155.4.220.39: máscara 255.255.0.0, red 155.4.0.0, broadcasting

155.24.255.255

- 194.209.14.33: máscara 255.255.255.0, red 194.209.14.0, broadcasting

194.209.14.255

- 190.33.109.133 / 255.255.255.0: red 190.33.109.0, broadcasting

190.33.109.255

2. Suponiendo que nuestro ordenador tiene la dirección IP 192.168.5.65 con máscara 255.255.255.0, indicar qué significan las siguientes direcciones especiales:

- 0.0.0.0: nuestro ordenador
- 0.0.0.29: 192.168.5.29
- 192.168.67.0: la red 192.168.67.0
- 255.255.255.255: broadcasting a la red 192.168.5.0 (la nuestra)
- 192.130.10.255: broadcasting a la red 192.130.10.0
- 127.0.0.1: 192.168.5.65 (loopback)

3. Calcular la dirección de red y dirección de broadcasting (difusión) de las máquinas con las siguientes direcciones IP y máscaras de subred:

• 190.33.109.133 / 255.255.255.128: red 190.33.109.128, broadcasting 190.33.109.255

(133=10000101, 128=10000000, 127=01111111)

• 192.168.20.25 / 255.255.255.240: red 192.168.20.16, broadcasting 192.168.20.31

(25=00011001, 240=11110000, 16=00010000, 31=00011111)

• 192.168.20.25 / 255.255.255.224: red 192.168.20.0, broadcasting 192.168.20.31

(25=00011001, 224=11100000, 31=00011111)

• 192.168.20.25 / 255.255.255.192: red 192.168.20.0, broadcasting 192.168.20.63

(25=00011001, 192=11000000, 63=00111111)

• 140.190.20.10 / 255.255.192.0: red 140.190.0.0, broadcasting 140.190.63.255

(020=00010100, 192=11000000, 063=00111111)

• 140.190.130.10 / 255.255.192.0: red 140.190.128.0, broadcasting 140.190.191.255

(130=10000010, 192=11000000, 128=10000000, 063=00111111, 191=10111111)

• 140.190.220.10 / 255.255.192.0: red 140.190.192.0, broadcasting 140.190.255.255

(220=11011100, 192=11000000, 063=00111111, 255=11111111)

4. Viendo las direcciones IP de los hosts públicos de una empresa observamos que todas están comprendidas entre 194.143.17.145 y 194.143.17.158, ¿Cuál es (probablemente) su dirección de red, broadcasting y máscara?

Pasamos a binario las dos direcciones. La primera tiene que estar próxima a la dirección de red y la última, a la dirección de broadcasting:

```
194.143.017.145          11000010.10001111.00010001.10010001
194.143.017.158 11000010.10001111.00010001.10011110
```

Podemos suponer que la dirección de red es 194.143.17.144 y la de broadcasting, 194.143.17.159:

```
194.143.017.144          11000010.10001111.00010001.10010000
194.143.017.159          11000010.10001111.00010001.10011111
<-----RED----->-->HOST
```

Entonces la máscara será:

```
255.255.255.240          11111111.11111111.11111111.11110000
<-----RED----->-->HOST
```

### 5.1.1 Protocolo IP

IP es el principal protocolo de la capa de red. Este protocolo define la unidad básica de transferencia de datos entre el origen y el destino, atravesando toda la red de redes. Además, el software IP es el encargado de elegir la ruta más adecuada por la que los datos serán enviados. Se trata de un sistema de entrega de paquetes (llamados datagramas IP) que tiene las siguientes características:

- Es no orientado a conexión debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino. Entonces pueden llegar duplicados o desordenados.
- Es no fiable porque los paquetes pueden perderse, dañarse o llegar retrasados.

Nota: El protocolo IP está definido en la RFC 791 ([en inglés](#), [en español](#)).

### Formato del datagrama IP

El datagrama IP es la unidad básica de transferencia de datos entre el origen y el destino. Viaja en el campo de datos de las tramas físicas (recuérdese la [trama Ethernet](#)) de las distintas redes que va atravesando. Cada vez que un datagrama tiene que atravesar un router, el datagrama saldrá de la trama física de la red que abandona y se acomodará en el campo de datos de una trama física de la siguiente red. Este mecanismo permite que un mismo datagrama IP pueda atravesar redes distintas: enlaces punto a punto, redes ATM, redes Ethernet, redes Token Ring, etc. El propio datagrama IP tiene también un campo de datos: será aquí donde viajen los paquetes de las capas superiores.

	Encabezado del datagrama	Área de datos del datagrama IP																													
	↓															↓															
Encabezado de la trama	Área de datos de la trama														Final de la trama																
0				10						20						30															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
VERS				HLEN				Tipo de servicio				Longitud total																			
Identificación										Bandrs			Desplazamiento de fragmento																		
TTL				Protocolo				CRC cabecera																							
Dirección IP origen																															
Dirección IP destino																															
Opciones IP (si las hay)																Relleno															
Datos																															
...																															

#### Campos del datagrama IP:

- VERS (4 bits). Indica la versión del protocolo IP que se utilizó para crear el datagrama. Actualmente se utiliza la versión 4 (IPv4) aunque ya se están preparando las especificaciones de la siguiente versión, la 6 (IPv6).
- HLEN (4 bits). Longitud de la cabecera expresada en múltiplos de 32 bits. El valor mínimo es 5, correspondiente a 160 bits = 20 bytes.
- Tipo de servicio (Type Of Service). Los 8 bits de este campo se dividen a su vez en:
  - Prioridad (3 bits). Un valor de 0 indica baja prioridad y un valor de 7, prioridad máxima.
  - Los siguientes tres bits indican cómo se prefiere que se transmita el mensaje, es decir, son sugerencias a los encaminadores que se encuentren a su paso los cuales pueden tenerlas en cuenta o no.
  - Bit D (Delay). Solicita retardos cortos (enviar rápido).
  - Bit T (Throughput). Solicita un alto rendimiento (enviar mucho en el menor tiempo posible).
  - Bit R (Reliability). Solicita que se minimice la probabilidad de que el datagrama se pierda o resulte dañado (enviar bien).
  - Los siguiente dos bits no tienen uso.
- Longitud total (16 bits). Indica la longitud total del datagrama expresada en bytes. Como el campo tiene 16 bits, la máxima longitud posible de un datagrama será de 65535 bytes.
- Identificación (16 bits). Número de secuencia que junto a la dirección origen, dirección destino y el protocolo utilizado identifica de manera única un datagrama en toda la red. Si se trata de un datagrama fragmentado, llevará la misma identificación que el resto de fragmentos.
- Banderas o indicadores (3 bits). Sólo 2 bits de los 3 bits disponibles están actualmente utilizados. El bit de Más fragmentos (MF) indica que no es el último

datagrama. Y el bit de No fragmentar (NF) prohíbe la fragmentación del datagrama. Si este bit está activado y en una determinada red se requiere fragmentar el datagrama, éste no se podrá transmitir y se descartará.

- Desplazamiento de fragmentación (13 bits). Indica el lugar en el cual se insertará el fragmento actual dentro del datagrama completo, medido en unidades de 64 bits. Por esta razón los campos de datos de todos los fragmentos menos el último tienen una longitud múltiplo de 64 bits. Si el paquete no está fragmentado, este campo tiene el valor de cero.

- Tiempo de vida o TTL (8 bits). Número máximo de segundos que puede estar un datagrama en la red de redes. Cada vez que el datagrama atraviesa un router se resta 1 a este número. Cuando llegue a cero, el datagrama se descarta y se devuelve un mensaje ICMP de tipo "tiempo excedido" para informar al origen de la incidencia.

- Protocolo (8 bits). Indica el protocolo utilizado en el campo de datos: 1 para ICMP, 2 para IGMP, 6 para TCP y 17 para UDP.

- CRC cabecera (16 bits). Contiene la suma de comprobación de errores sólo para la cabecera del datagrama. La verificación de errores de los datos corresponde a las capas superiores.

- Dirección origen (32 bits). Contiene la dirección IP del origen.

- Dirección destino (32 bits). Contiene la dirección IP del destino.

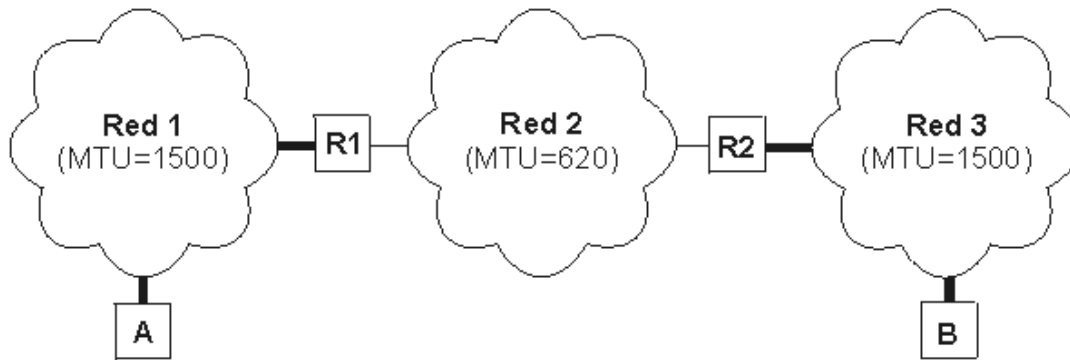
- Opciones IP. Este campo no es obligatorio y especifica las distintas opciones solicitadas por el usuario que envía los datos (generalmente para pruebas de red y depuración).

- Relleno. Si las opciones IP (en caso de existir) no ocupan un múltiplo de 32 bits, se completa con bits adicionales hasta alcanzar el siguiente múltiplo de 32 bits (recuérdese que la longitud de la cabecera tiene que ser múltiplo de 32 bits).

## Fragmentación

Ya hemos visto que las tramas físicas tienen un campo de datos y que es aquí donde se transportan los datagramas IP. Sin embargo, este campo de datos no puede tener una longitud indefinida debido a que está limitado por el diseño de la red. El MTU de una red es la mayor cantidad de datos que puede transportar su trama física. El MTU de las redes Ethernet es 1500 bytes y el de las redes Token-Ring, 8192 bytes. Esto significa que una red Ethernet nunca podrá transportar un datagrama de más de 1500 bytes sin fragmentarlo.

Un encaminador (router) fragmenta un datagrama en varios si el siguiente tramo de la red por el que tiene que viajar el datagrama tiene un MTU inferior a la longitud del datagrama. Veamos con el siguiente ejemplo cómo se produce la fragmentación de un datagrama.



Supongamos que el host A envía un datagrama de 1400 bytes de datos (1420 bytes en total) al host B. El datagrama no tiene ningún problema en atravesar la red 1 ya que  $1420 < 1500$ . Sin embargo, no es capaz de atravesar la red 2 ( $1420 \geq 620$ ). El router R1 fragmenta el datagrama en el menor número de fragmentos posibles que sean capaces de atravesar la red 2. Cada uno de estos fragmentos es un nuevo datagrama con la misma Identificación pero distinta información en el campo de Desplazamiento de fragmentación y el bit de Más fragmentos (MF). Veamos el resultado de la fragmentación:

Fragmento 1: Long. total = 620 bytes; Desp = 0; MF=1 (contiene los primeros 600 bytes de los datos del datagrama original)  
 Fragmento 2: Long. total = 620 bytes; Desp = 600; MF=1 (contiene los siguientes 600 bytes de los datos del datagrama original)  
 Fragmento 3: Long. total = 220 bytes; Desp = 1200; MF=0 (contiene los últimos 200 bytes de los datos del datagrama original)

El router R2 recibirá los 3 datagramas IP (fragmentos) y los enviará a la red 3 sin reensamblarlos. Cuando el host B reciba los fragmentos, recompondrá el datagrama original. Los encaminadores intermedios no reensamblan los fragmentos debido a que esto supondría una carga de trabajo adicional, a parte de memorias temporales. Nótese que el ordenador destino puede recibir los fragmentos cambiados de orden pero esto no supondrá ningún problema para el reensamblado del datagrama original puesto que cada fragmento guarda suficiente información.

Si el datagrama del ejemplo hubiera tenido su bit No fragmentar (NF) a 1, no hubiera conseguido atravesar el router R1 y, por tanto, no tendría forma de llegar hasta el host B. El encaminador R1 descartaría el datagrama.

## 5.1.2 Protocolo ARP

Dentro de una misma red, las máquinas se comunican enviándose tramas físicas. Las [tramas Ethernet](#) contienen campos para las direcciones físicas de origen y destino (6 bytes cada una):

8 bytes	6 bytes	6 bytes	2 bytes	64-1500 bytes	4 bytes
Preámbulo	Dirección física destino	Dirección física origen	Tipo de trama	Datos de la trama	CRC

El problema que se nos plantea es cómo podemos conocer la dirección física de la máquina destino. El único dato que se indica en los datagramas es la dirección IP de destino. ¿Cómo se pueden entregar entonces estos datagramas? Necesitamos obtener la dirección física de un ordenador a partir de su dirección IP. Esta es justamente la misión del protocolo ARP (Address Resolution Protocol, protocolo de resolución de direcciones).

Nota: El protocolo ARP está definido en la RFC 826 ([en inglés](#))

Host	Dirección física	Dirección IP	Red
A	00-60-52-0B-B7-7D	192.168.0.10	Red 1
R1	00-E0-4C-AB-9A-FF	192.168.0.1	
	A3-BB-05-17-29-D0	10.10.0.1	Red 2
B	00-E0-4C-33-79-AF	10.10.0.7	
R2	B2-42-52-12-37-BE	10.10.0.2	
	00-E0-89-AB-12-92	200.3.107.1	Red 3
C	A3-BB-08-10-DA-DB	200.3.107.73	
D	B2-AB-31-07-12-93	200.3.107.200	

Vamos a retomar el ejemplo introductorio de este Capítulo. El host A envía un datagrama con origen 192.168.0.10 y destino 10.10.0.7 (B). Como el host B se encuentra en una red distinta al host A, el datagrama tiene que atravesar el router 192.168.0.1 (R1). Se necesita conocer la dirección física de R1.

Es entonces cuando entra en funcionamiento el protocolo ARP: A envía un mensaje ARP a todas las máquinas de su red preguntando "¿Cuál es la dirección física de la máquina con dirección IP 192.168.0.1?". La máquina con dirección 192.168.0.1 (R1) advierte que la pregunta está dirigida a ella y responde a A con su dirección física (00-E0-4C-AB-9A-FF). Entonces A envía una trama física con origen 00-60-52-0B-B7-7D y destino 00-E0-4C-AB-9A-FF conteniendo el datagrama (origen 192.168.0.10 y destino 10.10.0.7). Al otro lado del router R2 se repite de nuevo el proceso para conocer la dirección física de B y entregar finalmente el datagrama a B. El mismo datagrama ha viajado en dos tramas físicas distintas, una para la red 1 y otra para la red 2.

Observemos que las preguntas ARP son de difusión (se envían a todas las máquinas). Estas preguntas llevan además la dirección IP y dirección física de la máquina que pregunta. La respuesta se envía directamente a la máquina que formuló la pregunta.

### Tabla ARP (caché ARP)

Cada ordenador almacena una tabla de direcciones IP y direcciones físicas. Cada vez que formula una pregunta ARP y le responden, inserta una nueva entrada en su tabla. La primera vez que C envíe un mensaje a D tendrá que difundir previamente una pregunta ARP, tal como hemos visto. Sin embargo, las siguientes veces que C envíe mensajes a D ya no será necesario realizar nuevas preguntas puesto que C habrá almacenado en su tabla la dirección física de D. Sin embargo, para evitar incongruencias en la red debido a posibles cambios de direcciones IP o adaptadores de red, se asigna un tiempo de vida de cierto número de segundos a cada entrada de la tabla. Cuando se agote el tiempo de vida de una entrada, ésta será eliminada de la tabla.

Las tablas ARP reducen el tráfico de la red al evitar preguntas ARP innecesarias. Pensemos ahora en distintas maneras para mejorar el rendimiento de la red. Después de una pregunta ARP, el destino conoce las direcciones IP y física del origen. Por lo tanto, podría insertar la correspondiente entrada en su tabla. Pero no sólo eso, sino que todas las estaciones de la red escuchan la pregunta ARP: podrían insertar también las correspondientes entradas en sus tablas. Como es muy probable que otras máquinas se comuniquen en un futuro con la primera, habremos reducido así el tráfico de la red aumentando su rendimiento.

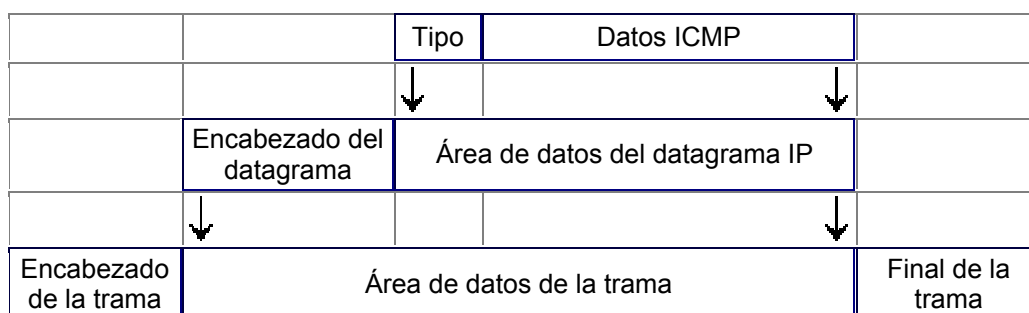
Esto que hemos explicado es para comunicar dos máquinas conectadas a la misma red. Si la otra máquina no estuviese conectada a la misma red, sería necesario atravesar uno o más routers hasta llegar al host destino. La máquina origen, si no la tiene en su tabla, formularía una pregunta ARP solicitando la dirección física del router y le transferiría a éste el mensaje. Estos pasos se van repitiendo para cada red hasta llegar a la máquina destino.

### 5.1.3 Protocolo ICMP

Debido a que el protocolo IP no es fiable, los datagramas pueden perderse o llegar defectuosos a su destino. El protocolo ICMP (Internet Control Message Protocol, protocolo de mensajes de control y error) se encarga de informar al origen si se ha producido algún error durante la entrega de su mensaje. Pero no sólo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.

Nota: El protocolo ICMP está definido en la RFC 792 ([en inglés](#), [en español](#))

El protocolo ICMP únicamente informa de incidencias en la red pero no toma ninguna decisión. Esto será responsabilidad de las capas superiores. Los mensajes ICMP viajan en el campo de datos de un datagrama IP, como se puede apreciar en el siguiente esquema:



Debido a que el protocolo IP no es fiable puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se creará un nuevo mensaje ICMP sino que el primero se descartará sin más.

Los mensajes ICMP comienzan con un campo de 8 bits que contiene el tipo de mensaje, según se muestra en la tabla siguiente. El resto de campos son distintos para cada tipo de mensaje ICMP.

Nota: El formato y significado de cada mensaje ICMP está documentado en la RFC 792 ([en inglés](#), [en español](#)).

<b>Campo de tipo</b>	<b>Tipo de mensaje ICMP</b>
0	Respuesta de eco ( <i>Echo Reply</i> )
3	Destino inaccesible ( <i>Destination Unreachable</i> )
4	Disminución del tráfico desde el origen ( <i>Source Quench</i> )
5	Redireccionar (cambio de ruta) ( <i>Redirect</i> )
8	Solicitud de eco ( <i>Echo</i> )
11	Tiempo excedido para un datagrama ( <i>Time Exceeded</i> )
12	Problema de Parámetros ( <i>Parameter Problem</i> )
13	Solicitud de marca de tiempo ( <i>Timestamp</i> )
14	Respuesta de marca de tiempo ( <i>Timestamp Reply</i> )
15	Solicitud de información (obsoleto) ( <i>Information Request</i> )
16	Respuesta de información (obsoleto) ( <i>Information Reply</i> )
17	Solicitud de máscara ( <i>Addressmask</i> )
18	Respuesta de máscara ( <i>Addressmask Reply</i> )

### Solicitud y respuesta de eco

Los mensajes de solicitud y respuesta de eco, tipos 8 y 0 respectivamente, se utilizan para comprobar si existe comunicación entre 2 hosts a nivel de la capa de red. Estos mensajes comprueban que las capas física (cableado), acceso al medio (tarjetas de red) y red (configuración IP) están correctas. Sin embargo, no dicen nada de las capas de transporte y de aplicación las cuales podrían estar mal configuradas; por ejemplo, la recepción de mensajes de correo electrónico puede fallar aunque exista comunicación IP con el servidor de correo.

La orden PING envía mensajes de solicitud de eco a un host remoto e informa de las respuestas. Veamos su funcionamiento, en caso de no producirse incidencias en el camino.

1. A envía un mensaje ICMP de tipo 8 (Echo) a B
2. B recibe el mensaje y devuelve un mensaje ICMP de tipo 0 (Echo Reply) a A
3. A recibe el mensaje ICMP de B y muestra el resultado en pantalla



```
A>ping 172.20.9.7 -n 1
Haciendo ping a 172.20.9.7 con 32 bytes de datos:
Respuesta desde 172.20.9.7: bytes=32 tiempo<10ms TDV=128
```

En la orden anterior hemos utilizado el parámetro "-n 1" para que el host A únicamente envíe 1 mensaje de solicitud de eco. Si no se especifica este parámetro se enviarían 4 mensajes (y se recibirían 4 respuestas).

Si el host de destino no existiese o no estuviera correctamente configurado recibiríamos un mensaje ICMP de tipo 11 (Time Exceeded).

```
A>ping 192.168.0.6 -n 1
Haciendo ping a 192.168.0.6 con 32 bytes de datos:
Tiempo de espera agotado.
```

Si tratamos de acceder a un host de una red distinta a la nuestra y no existe un camino para llegar hasta él, es decir, los routers no están correctamente configurados o estamos intentando acceder a una red aislada o inexistente, recibiríamos un mensaje ICMP de tipo 3 (Destination Unreachable).

```
A>ping 1.1.1.1 -n 1
Haciendo ping a 1.1.1.1 con 32 bytes de datos:
Respuesta desde 192.168.0.1: Host de destino inaccesible.
```

Utilización de PING para diagnosticar errores en una red aislada



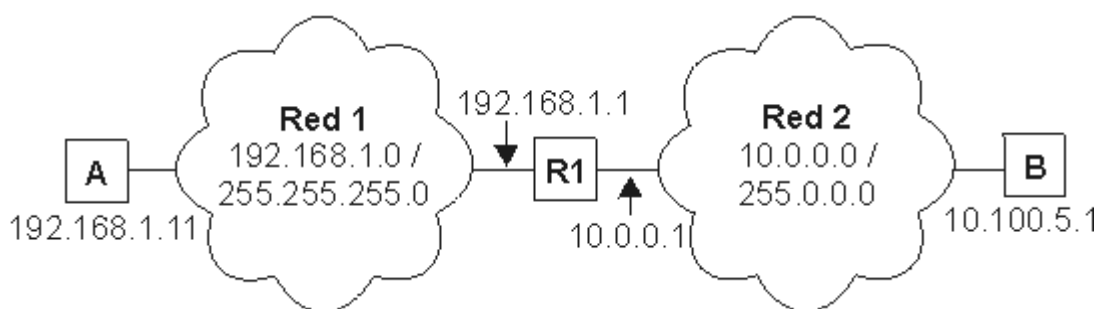
```
A>ping 192.168.1.12
```

- Respuesta. El cableado entre A y B, las tarjetas de red de A y B, y la configuración IP de A y B están correctos.
- Tiempo de espera agotado. Comprobar el host B y el cableado entre A y B.
- Host de destino inaccesible. Comprobar las direcciones IP y máscaras de subred de A y B porque no pertenecen a la misma red.
- Error. Probablemente estén mal instalados los protocolos TCP/IP del host A. Probar `A>ping 127.0.0.1` para asegurarse.

Nota: El comando `ping 127.0.0.1` informa de si están correctamente instalados los protocolos TCP/IP en nuestro host. No informa de si la tarjeta de red de nuestro host está correcta.

### Utilización de PING para diagnosticar errores en una red de redes

A continuación veremos un ejemplo para una red de redes formada por dos redes (1 solo router). La idea es la misma para un mayor número de redes y routers.



`A>ping 10.100.5.1`

- Respuesta. El cableado entre A y B, las tarjetas de red de A, R1 y B, y la configuración IP de A, R1 y B están correctos. El router R1 permite el tráfico de datagramas IP en los dos sentidos.
- Tiempo de espera agotado. Comprobar el host B y el cableado entre R1 y B. Para asegurarnos que el router R1 está funcionando correctamente haremos `A>ping 192.168.1.1`
- Host de destino inaccesible. Comprobar el router R1 y la configuración IP de A (probablemente la puerta de salida no sea 192.168.1.1). Recordemos que la puerta de salida (*gateway*) de una red es un host de su propia red que se utiliza para salir a otras redes.
- Error. Probablemente estén mal instalados los protocolos TCP/IP del host A. Probar `A>ping 127.0.0.1` para asegurarse.

En el caso producirse errores de comunicación en una red de redes con más de un router (Internet es el mejor ejemplo), se suele utilizar el comando PING para ir diagnosticando los distintos routers desde el destino hasta el origen y descubrir así si el fallo es responsabilidad de la red de destino, de una red intermedia o de nuestra red.

Nota: Algunos hosts en Internet tienen deshabilitadas las respuestas de eco (mensajes ICMP tipo 0) como medida de seguridad. En estos casos

hay que utilizar otros mecanismos para detectar si responde (por ejemplo, la apertura de conexión a un puerto, como veremos en el capítulo siguiente).

## Mensajes ICMP de tiempo excedido

Los datagramas IP tienen un [campo TTL](#) (tiempo de vida) que impide que un mensaje esté dando vueltas indefinidamente por la red de redes. El número contenido en este campo disminuye en una unidad cada vez que el datagrama atraviesa un router. Cuando el TTL de un datagrama llega a 0, éste se descarta y se envía un mensaje ICMP de tipo 11 (Time Exceeded) para informar al origen.

Los mensajes ICMP de tipo 11 se pueden utilizar para hacer una traza del camino que siguen los datagramas hasta llegar a su destino. ¿Cómo? Enviando una secuencia de datagramas con TTL=1, TTL=2, TTL=3, TTL=4, etc... hasta alcanzar el host o superar el límite de saltos (30 si no se indica lo contrario). El primer datagrama caducará al atravesar el primer router y se devolverá un mensaje ICMP de tipo 11 informando al origen del router que descartó el datagrama. El segundo datagrama hará lo propio con el segundo router y así sucesivamente. Los mensajes ICMP recibidos permiten definir la traza.

La orden TRACERT (traceroute en entornos Unix) hace una traza a un determinado host. TRACERT funciona enviando mensajes ICMP de solicitud de eco con distintos TTL; traceroute, en cambio, envía mensajes UDP. Si la comunicación extremo a extremo no es posible, la traza nos indicará en qué punto se ha producido la incidencia. Existen algunas utilidades en Internet, como [Visual Route](#), que conocen la localización geográfica de los principales routers de Internet. Esto permite dibujar en un mapamundi el recorrido que siguen los datagramas hasta llegar a un host.

```

A>tracert                                     130.206.1.2

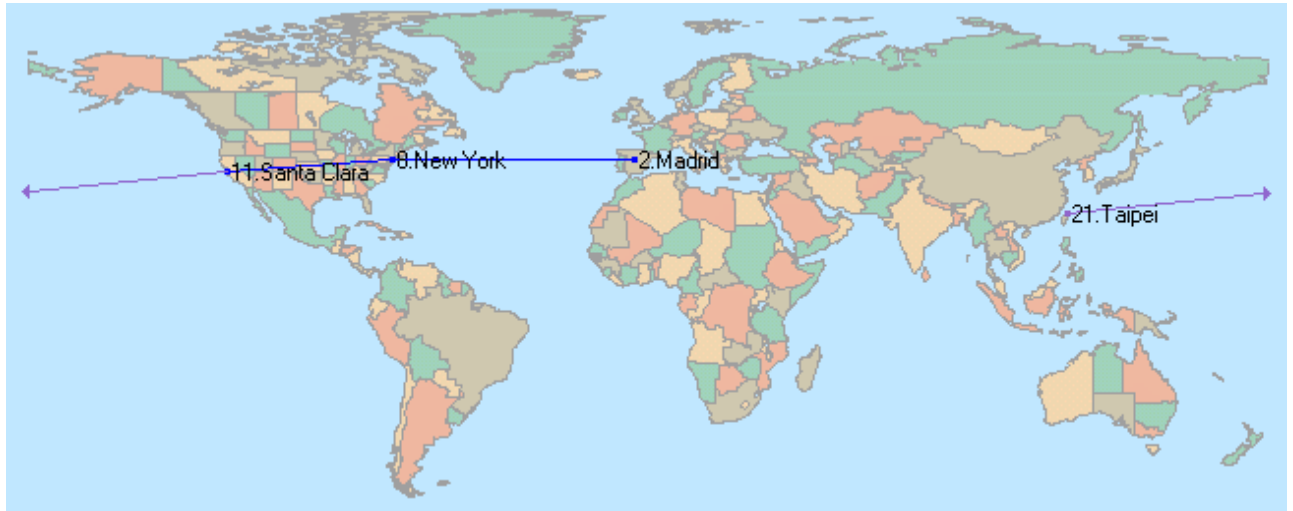
Traza          a          la          dirección          sun.rediris.es          [130.206.1.2]
sobre          un          máximo          de          30          saltos:

 1          1          ms          1          ms          1          ms          PROXY          [192.168.0.1]
 2          122          ms          118          ms          128          ms          MADR-X27.red.retevision.es          [62.81.1.102]
 3          143          ms          232          ms          147          ms          MADR-R2.red.retevision.es          [62.81.1.92]
 4          130          ms          124          ms          246          ms          MADR-R16.red.retevision.es          [62.81.3.8]
 5          590          ms          589          ms          431          ms          MADR-R12.red.retevision.es          [62.81.4.101]
 6          612          ms          640          ms          124          ms          MADR-R10.red.retevision.es          [62.81.8.130]
 7          259          ms          242          ms          309          ms          193.149.1.28
 8          627          ms          752          ms          643          ms          213.0.251.42
 9          137          ms          117          ms          118          ms          213.0.251.142
10          109          ms          105          ms          110          ms          A1-2-1.EB-Madrid00.red.rediris.es          [130.206.224.81]
11          137          ms          119          ms          122          ms          A0-0-0-1.EB-Madrid3.red.rediris.es          [130.206.224.86]
12          109          ms          135          ms          115          ms          sun.rediris.es          [130.206.1.2]

```

Traza completa.

Ejemplo de Visual Route a una dirección IP de Taiwan (203.69.112.12):



## Encaminamiento

Una red de redes está formada por redes interconectadas mediante routers o encaminadores. Cuando enviamos un datagrama desde un ordenador hasta otro, éste tiene que ser capaz de encontrar la ruta más adecuada para llegar a su destino. Esto es lo que se conoce como encaminamiento.

Los routers (encaminadores) son los encargados de elegir las mejores rutas. Estas máquinas pueden ser ordenadores con varias direcciones IP o bien, aparatos específicos. Los routers deben conocer, al menos parcialmente, la estructura de la red que les permita encaminar de forma correcta cada mensaje hacia su destino. Esta información se almacena en las llamadas tablas de encaminamiento. Observemos que debido al sistema de direccionamiento IP esta misión no es tan complicada. Lo único que necesitamos almacenar en las tablas son los prefijos de las direcciones (que nos indican la red). Por ejemplo, si el destino es la máquina 149.33.19.4 con máscara 255.255.0.0, nos basta con conocer el encaminamiento de la red 149.33.0.0 ya que todas las que empiecen por 149.33 se enviarán hacia el mismo sitio.

La orden Route muestra y modifica la tabla de encaminamiento de un host. Todos los hosts (y no sólo los routers) tienen tablas de encaminamientos. A continuación se muestra una tabla sencilla para un host con IP 192.168.0.2 / 255.255.255.0 y puerta de salida 192.168.0.1.

Asroute

nnint

Rutas				activas:	
Dirección de red Métrica	Máscara de red	Puerta de enlace		Interfaz	
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.2	1	(7)
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	(6)
192.168.0.0	255.255.255.0	192.168.0.2	192.168.0.2	1	
(5)					
192.168.0.2	255.255.255.255	127.0.0.1	127.0.0.1	1	
(4)					
192.168.0.255	255.255.255.255	192.168.0.2	192.168.0.2		
1					(3)
224.0.0.0	224.0.0.0	192.168.0.2	192.168.0.2	1	(2)
255.255.255.255	255.255.255.255	192.168.0.2	0.0.0.0		
1	(1)				

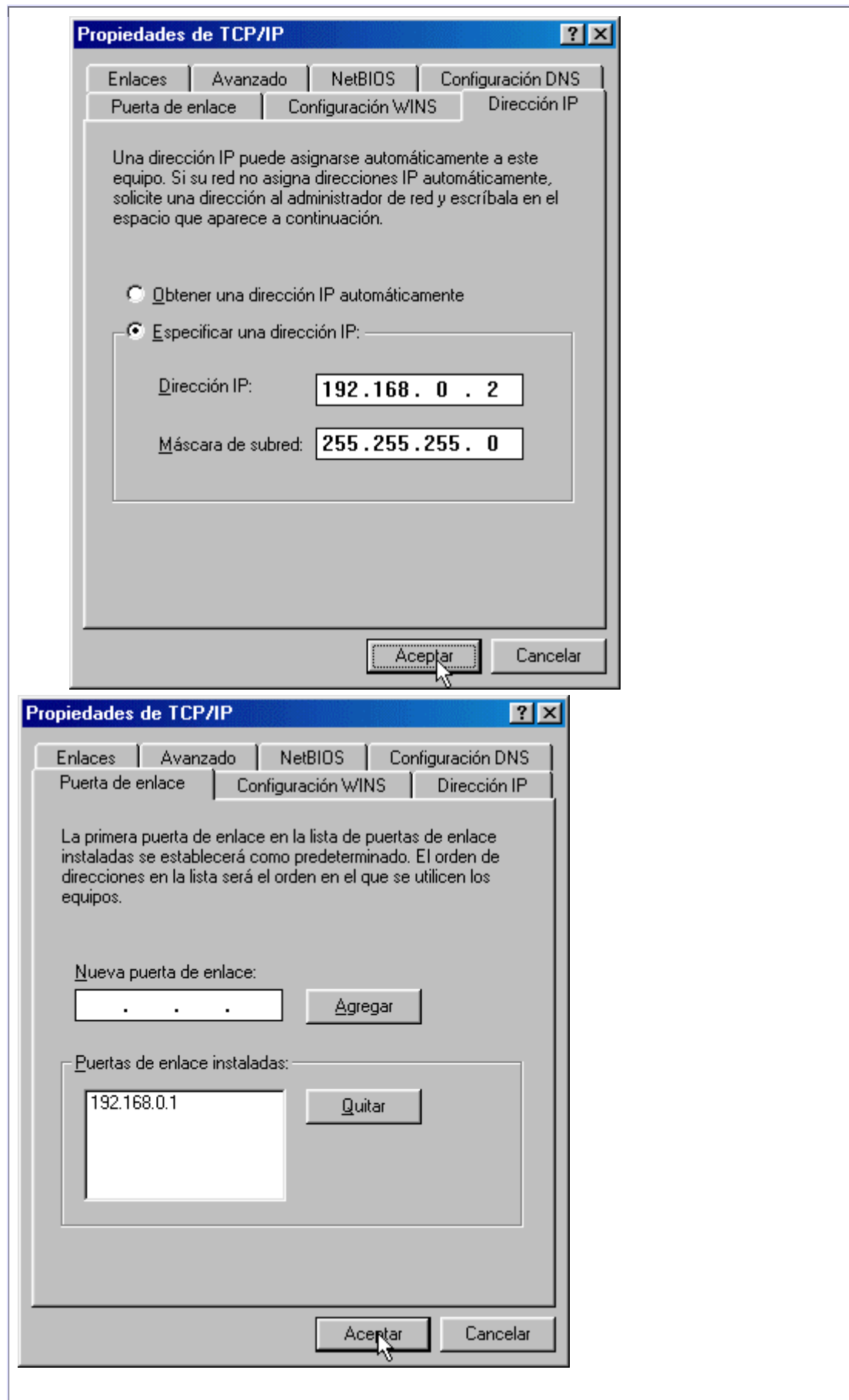
Esta tabla se lee de abajo a arriba. La línea (1) indica que los datagramas con destino "255.255.255.255" (dirección de difusión a la red del host) deben ser aceptados. La línea (2) representa un grupo de multidifusión (multicasting). La dirección "224.0.0.0" es una dirección de clase D que se utiliza para enviar mensajes a una colección de hosts registrados previamente. Estas dos líneas se suelen pasar por alto: aparecen en todas las tablas de rutas.

La línea (3) indica que todos los mensajes cuyo destinatario sea "192.168.0.255" deben ser aceptados (es la dirección de difusión a la red del host). La línea (4) se encarga de aceptar todos los mensajes que vayan destinados a la dirección del host "192.168.0.2".

La línea (5) indica que los mensajes cuyo destinatario sea una dirección de la red del host "192.168.0.0 / 255.255.255.0" deben salir del host por su tarjeta de red para que se entreguen directamente en su subred. La línea (6) es la dirección de loopback: todos los paquetes con destino "127.0.0.0 / 255.0.0.0" serán aceptados por el propio host.

Finalmente, la línea (7) representa a "todas las demás direcciones que no se hayan indicado anteriormente". En concreto son aquellas direcciones remotas que no pertenecen a la red del host. ¿A dónde se enviarán? Se enviarán a la puerta de salida (gateway) de la red "192.168.0.1".

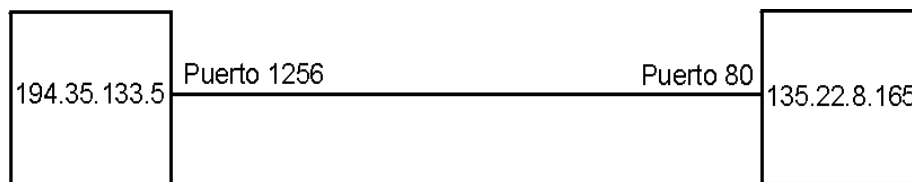
Nótese que la tabla de rutas es la traducción de la configuración IP del host que habitualmente se escribe en las ventanas de Windows:



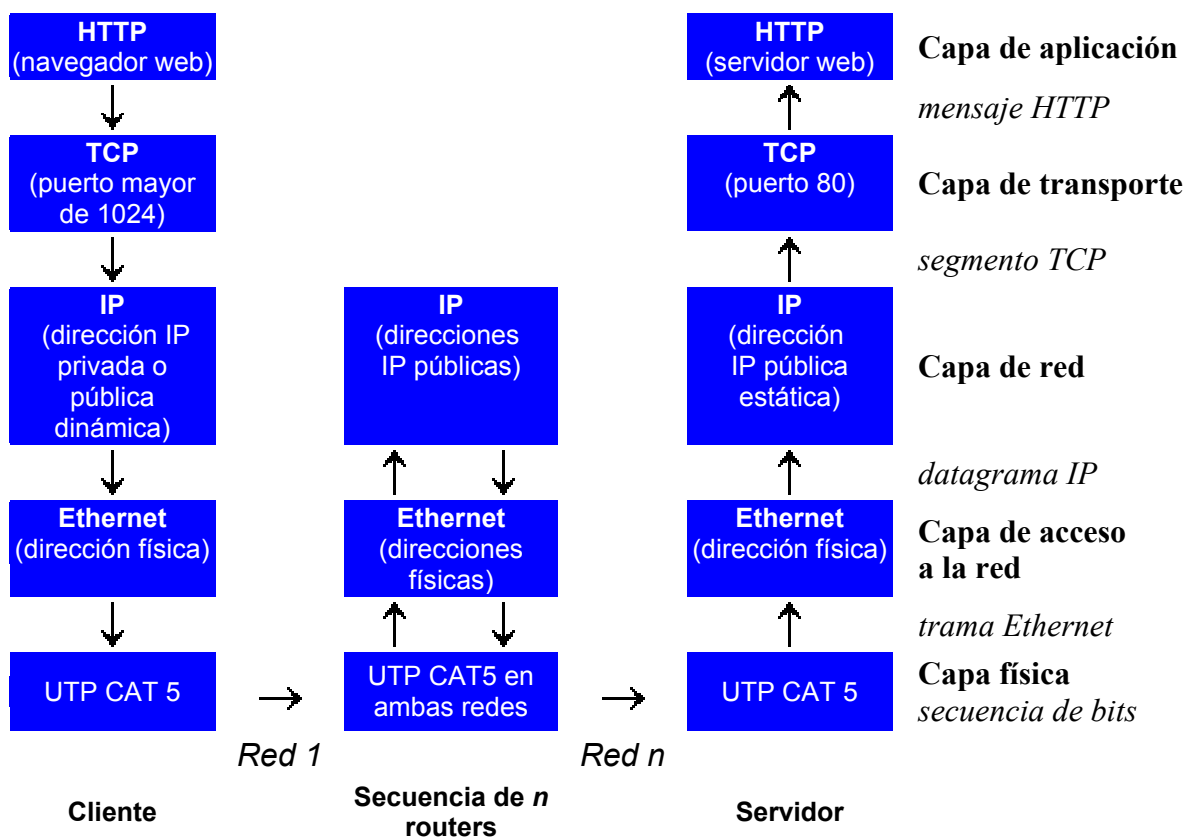
## 5.2 Capa de transporte

La capa de red transfiere datagramas entre dos ordenadores a través de la red utilizando como identificadores las direcciones IP. La capa de transporte añade la noción de puerto para distinguir entre los muchos destinos dentro de un mismo host. No es suficiente con indicar la dirección IP del destino, además hay que especificar la aplicación que recogerá el mensaje. Cada aplicación que esté esperando un mensaje utiliza un número de puerto distinto; más concretamente, la aplicación está a la espera de un mensaje en un puerto determinado (escuchando un puerto).

Pero no sólo se utilizan los puertos para la recepción de mensajes, también para el envío: todos los mensajes que envíe un ordenador debe hacerlo a través de uno de sus puertos. El siguiente diagrama representa una transmisión entre el ordenador 194.35.133.5 y el 135.22.8.165. El primero utiliza su puerto 1256 y el segundo, el 80.



La capa de transporte transmite mensajes entre las aplicaciones de dos ordenadores. Por ejemplo, entre nuestro navegador de páginas web y un servidor de páginas web, o entre nuestro programa de correo electrónico y un servidor de correo.



## Puertos

Un ordenador puede estar conectado con distintos servidores a la vez; por ejemplo, con un servidor de noticias y un servidor de correo. Para distinguir las distintas conexiones dentro de un mismo ordenador se utilizan los puertos.

Un puerto es un número de 16 bits, por lo que existen 65536 puertos en cada ordenador. Las aplicaciones utilizan estos puertos para recibir y transmitir mensajes.

Los números de puerto de las aplicaciones cliente son asignados dinámicamente y generalmente son superiores al 1024. Cuando una aplicación cliente quiere comunicarse con un servidor, busca un número de puerto libre y lo utiliza.

En cambio, las aplicaciones servidoras utilizan unos números de puerto prefijados: son los llamados puertos well-known (bien conocidos). Estos puertos están definidos en la RFC 1700 y se pueden consultar en <http://www.ietf.org/rfc/rfc1700.txt>. A continuación se enumeran los puertos well-known más usuales:

<u>Palabra clave</u>	<u>Puerto</u>	<u>Descripción</u>
	0/tcp	Reserved
	0/udp	Reserved
tcpmux	1/tcp	TCP Port Service Multiplexer
rje	5/tcp	Remote Job Entry
echo	7/tcp/udp	Echo
discard	9/tcp/udp	Discard
systat	11/tcp/udp	Active Users
daytime	13/tcp/udp	Daytime
qotd	17/tcp/udp	Quote of the Day
chargen	19/tcp/udp	Character Generator
ftp-data	20/tcp	File Transfer [Default Data]
<b>ftp</b>	<b>21/tcp</b>	<b>File Transfer [Control]</b>
<b>telnet</b>	<b>23/tcp</b>	<b>Telnet</b>
<b>smtp</b>	<b>25/tcp</b>	<b>Simple Mail Transfer</b>
time	37/tcp/udp	Time
nameserver	42/tcp/udp	Host Name Server
nicname	43/tcp/udp	Who Is
<b>domain</b>	<b>53/tcp/udp</b>	<b>Domain Name Server</b>
bootps	67/udp/udp	Bootstrap Protocol Server
tftp	69/udp	Trivial File Transfer
gopher	70/tcp	Gopher
finger	79/tcp	Finger
<b>www-http</b>	<b>80/tcp</b>	<b>World Wide Web HTTP</b>
dcp	93/tcp	Device Control Protocol
supdup	95/tcp	SUPDUP
hostname	101/tcp	NIC Host Name Server

iso-tsap	102/tcp	ISO-TSAP
gppitnp	103/tcp	Genesis Point-to-Point Trans Net
rtelnet	107/tcp/udp	Remote Telnet Service
pop2	109/tcp	Post Office Protocol - Version 2
<b>pop3</b>	<b>110/tcp</b>	<b>Post Office Protocol - Version 3</b>
sunrpc	111/tcp/udp	SUN Remote Procedure Call
auth	113/tcp	Authentication Service
sftp	115/tcp/udp	Simple File Transfer Protocol
<b>nntp</b>	<b>119/tcp</b>	<b>Network News Transfer Protocol</b>
ntp	123/udp	Network Time Protocol
pwdgen	129/tcp	Password Generator Protocol
netbios-ns	137/tcp/udp	NETBIOS Name Service
netbios-dgm	138/tcp/udp	NETBIOS Datagram Service
<b>netbios-ssn</b>	<b>139/tcp/udp</b>	<b>NETBIOS Session Service</b>
snmp	161/udp	SNMP
snmptrap	162/udp	SNMPTRAP
irc	194/tcp	Internet Relay Chat Protocol

Los puertos tienen una memoria intermedia (buffer) situada entre los programas de aplicación y la red. De tal forma que las aplicaciones transmiten la información a los puertos. Aquí se va almacenando hasta que pueda enviarse por la red. Una vez que pueda transmitirse, la información irá llegando al puerto destino donde se irá guardando hasta que la aplicación esté preparada para recibirla.

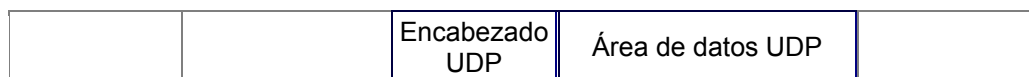
Los dos protocolos principales de la capa de transporte son UDP y TCP. El primero ofrece una transferencia de mensajes no fiable y no orientada a conexión y el segundo, una transferencia fiable y orientada a conexión.

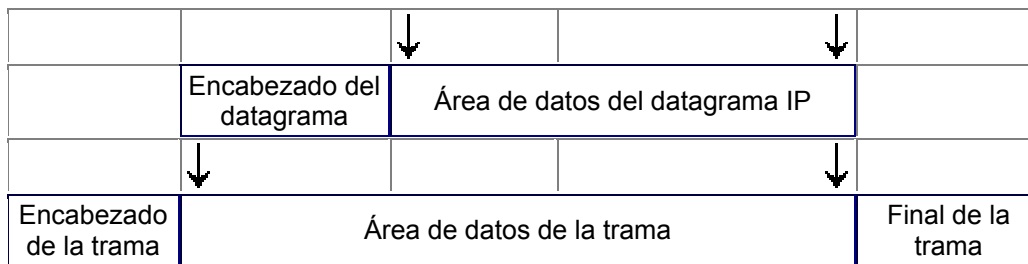
### 5.2.1 Protocolo UDP

El protocolo UDP (User Datagram Protocol, protocolo de datagrama de usuario) proporciona una comunicación muy sencilla entre las aplicaciones de dos ordenadores. Al igual que el protocolo IP, UDP es:

- No orientado a conexión. No se establece una conexión previa con el otro extremo para transmitir un mensaje UDP. Los mensajes se envían sin más y éstos pueden duplicarse o llegar desordenados al destino.
- No fiable. Los mensajes UDP se pueden perder o llegar dañados.

UDP utiliza el protocolo IP para transportar sus mensajes. Como vemos, no añade ninguna mejora en la calidad de la transferencia; aunque sí incorpora los puertos origen y destino en su formato de mensaje. Las aplicaciones (y no el protocolo UDP) deberán programarse teniendo en cuenta que la información puede no llegar de forma correcta.





Formato del mensaje UDP

0																10																20																30															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9																								
Puerto UDP origen																Puerto UDP destino																																															
Longitud mensaje UDP																Suma verificación UDP																																															
Datos																																																															
...																																																															

- Puerto UDP de origen (16 bits, opcional). Número de puerto de la máquina origen.
- Puerto UDP de destino (16 bits). Número de puerto de la máquina destino.
- Longitud del mensaje UDP (16 bits). Especifica la longitud medida en bytes del mensaje UDP incluyendo la cabecera. La longitud mínima es de 8 bytes.
- Suma de verificación UDP (16 bits, opcional). Suma de comprobación de errores del mensaje. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino. Para conocer estos datos, el protocolo UDP debe interactuar con el protocolo IP.
- Datos. Aquí viajan los datos que se envían las aplicaciones. Los mismos datos que envía la aplicación origen son recibidos por la aplicación destino después de atravesar toda la Red de redes.

### 5.2.2 Protocolo TCP

El protocolo TCP (Transmission Control Protocol, protocolo de control de transmisión) está basado en IP que es no fiable y no orientado a conexión, y sin embargo es:

- Orientado a conexión. Es necesario establecer una conexión previa entre las dos máquinas antes de poder transmitir ningún dato. A través de esta conexión los datos llegarán siempre a la aplicación destino de forma ordenada y sin duplicados. Finalmente, es necesario cerrar la conexión.
- Fiable. La información que envía el emisor llega de forma correcta al destino.

El protocolo TCP permite una comunicación fiable entre dos aplicaciones. De esta forma, las aplicaciones que lo utilicen no tienen que preocuparse de la integridad de la información: dan por hecho que todo lo que reciben es correcto.

El flujo de datos entre una aplicación y otra viajan por un circuito virtual. Sabemos que los datagramas IP pueden seguir rutas distintas, dependiendo del estado de los encaminadores intermedios, para llegar a un mismo sitio. Esto significa que los datagramas IP que transportan los mensajes siguen rutas diferentes aunque el protocolo TCP logre la ilusión de que existe un único circuito por el que viajan todos los bytes uno detrás de otro (algo así como una tubería entre el origen y el destino). Para que esta comunicación pueda ser posible es necesario abrir previamente una conexión. Esta conexión garantiza que los todos los datos lleguen correctamente de forma ordenada y sin duplicados. La unidad de datos del protocolo es el byte, de tal forma que la aplicación origen envía bytes y la aplicación destino recibe estos bytes.

Sin embargo, cada byte no se envía inmediatamente después de ser generado por la aplicación, sino que se espera a que haya una cierta cantidad de bytes, se agrupan en un segmento y se envía el segmento completo. Para ello son necesarias unas memorias intermedias o buffers. Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Si el segmento es muy grande será necesario fragmentar el datagrama, con la consiguiente pérdida de rendimiento; y si es muy pequeño, se estarán enviando más cabeceras que datos. Por consiguiente, es importante elegir el mayor tamaño de segmento posible que no provoque fragmentación.

El protocolo TCP envía un flujo de información no estructurado. Esto significa que los datos no tienen ningún formato, son únicamente los bytes que una aplicación envía a otra. Ambas aplicaciones deberán ponerse de acuerdo para comprender la información que se están enviando.

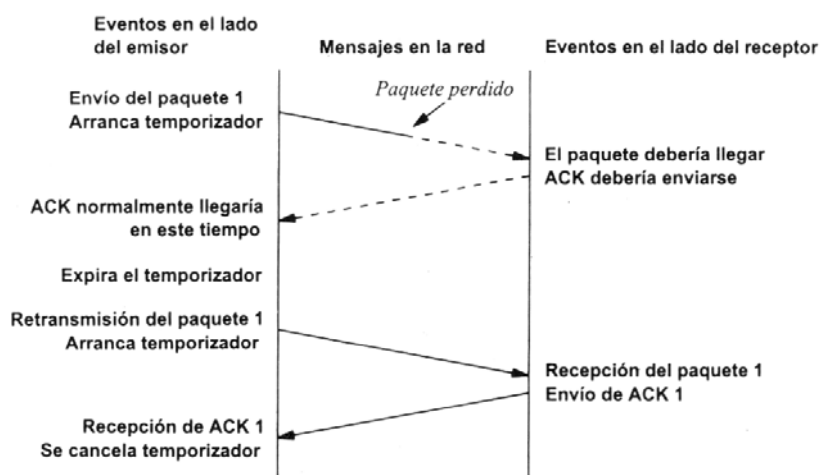
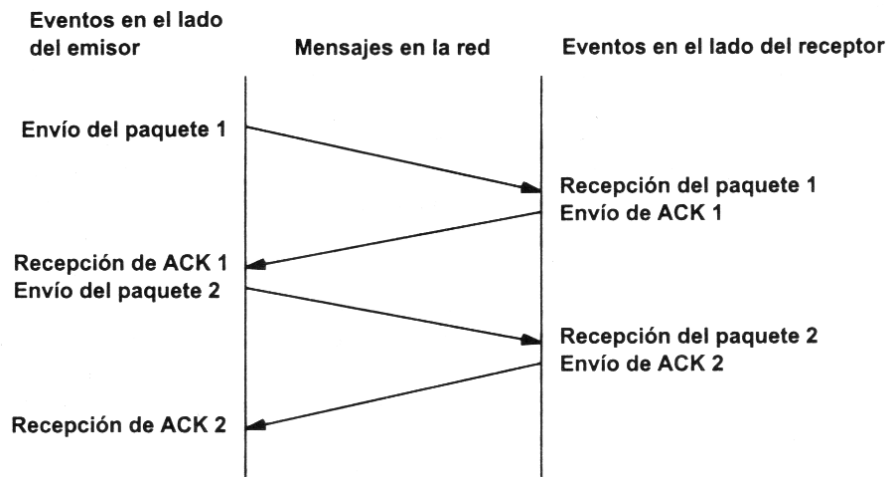
Cada vez que se abre una conexión, se crea un canal de comunicación bidireccional en el que ambas aplicaciones pueden enviar y recibir información, es decir, una conexión es full-dúplex.

## **Fiabilidad**

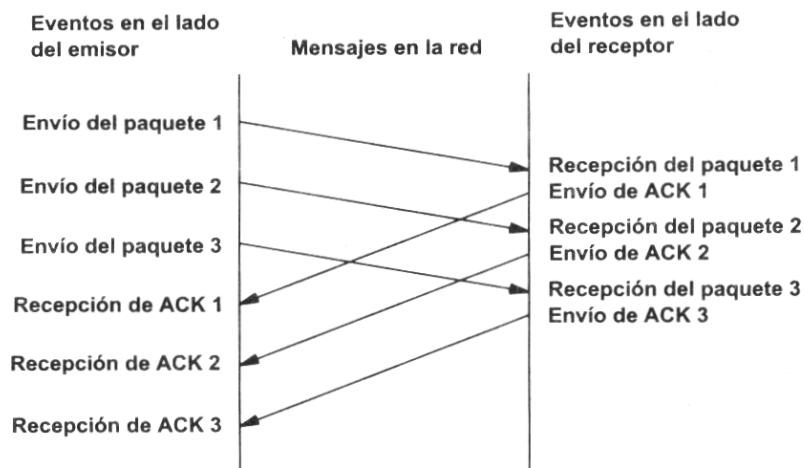
¿Cómo es posible enviar información fiable basándose en un protocolo no fiable? Es decir, si los datagramas que transportan los segmentos TCP se pueden perder, ¿cómo pueden llegar los datos de las aplicaciones de forma correcta al destino?

La respuesta a esta pregunta es sencilla: cada vez que llega un mensaje se devuelve una confirmación (acknowledgement) para que el emisor sepa que ha llegado correctamente. Si no le llega esta confirmación pasado un cierto tiempo, el emisor reenvía el mensaje.

Veamos a continuación la manera más sencilla (aunque ineficiente) de proporcionar una comunicación fiable. El emisor envía un dato, arranca su temporizador y espera su confirmación (ACK). Si recibe su ACK antes de agotar el temporizador, envía el siguiente dato. Si se agota el temporizador antes de recibir el ACK, reenvía el mensaje. Los siguientes esquemas representan este comportamiento:



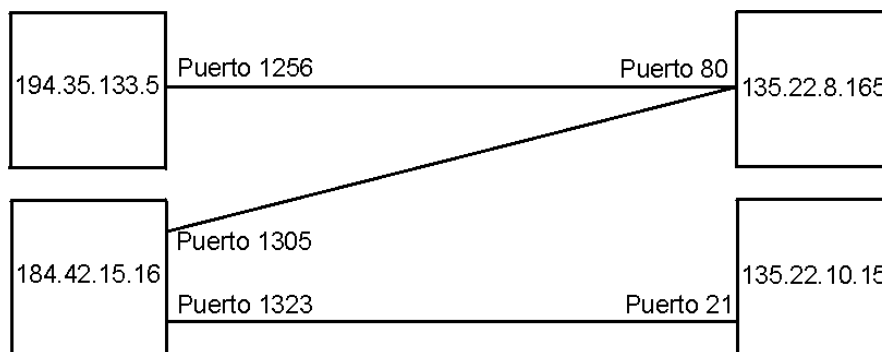
Este esquema es perfectamente válido aunque muy ineficiente debido a que sólo se utiliza un sentido de la comunicación a la vez y el canal está desaprovechado la mayor parte del tiempo. Para solucionar este problema se utiliza un protocolo de ventana deslizante, que se resume en el siguiente esquema. Los mensajes y las confirmaciones van numerados y el emisor puede enviar más de un mensaje antes de haber recibido todas las confirmaciones anteriores.



## Conexiones

Una conexión son dos pares dirección IP:puerto. No puede haber dos conexiones iguales en un mismo instante en toda la Red. Aunque bien es posible que un mismo ordenador tenga dos conexiones distintas y simultáneas utilizando un mismo puerto. El protocolo TCP utiliza el concepto de conexión para identificar las transmisiones. En el siguiente ejemplo se han creado tres conexiones. Las dos primeras son al mismo servidor Web (puerto 80) y la tercera a un servidor de FTP (puerto 21).

Host 1	Host 2
194.35.133.5:1256	135.22.8.165:80
184.42.15.16:1305	135.22.8.165:80
184.42.15.16:1323	135.22.10.15:21



Para que se pueda crear una conexión, el extremo del servidor debe hacer una apertura pasiva del puerto (escuchar su puerto y quedar a la espera de conexiones) y el cliente, una apertura activa en el puerto del servidor (conectarse con el puerto de un determinado servidor).

Nota: El comando NetStat muestra las conexiones abiertas en un ordenador, así como estadísticas de los distintos protocolos de Internet.

## Formato del segmento TCP

Ya hemos comentado que el flujo de bytes que produce una determinada aplicación se divide en uno o más segmentos TCP para su transmisión. Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Para facilitar el control de flujo de la información los bytes de la aplicación se numeran. De esta manera, cada segmento indica en su cabecera el primer byte que transporta. Las confirmaciones o acuses de recibo (ACK) representan el siguiente byte que se espera recibir (y no el número de segmento recibido, ya que éste no existe).

0										10										20										30	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Puerto TCP origen																Puerto TCP destino															
Número de secuencia																															
Número de acuse de recibo																															
HLEN				Reservado						Bits código						Ventana															
Suma de verificación																Puntero de urgencia															
Opciones (si las hay)																								Relleno							
Datos																															
...																															

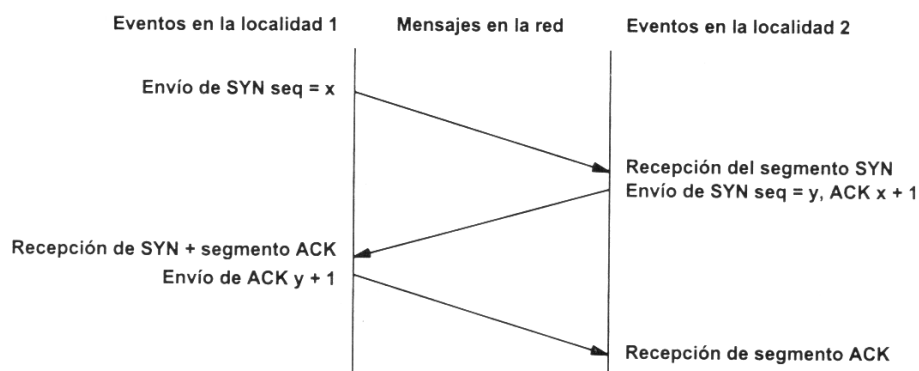
- Puerto fuente (16 bits). Puerto de la máquina origen. Al igual que el puerto destino es necesario para identificar la conexión actual.
- Puerto destino (16 bits). Puerto de la máquina destino.
- Número de secuencia (32 bits). Indica el número de secuencia del primer byte que transporta el segmento.
  - Número de acuse de recibo (32 bits). Indica el número de secuencia del siguiente byte que se espera recibir. Con este campo se indica al otro extremo de la conexión que los bytes anteriores se han recibido correctamente.
  - HLEN (4 bits). Longitud de la cabecera medida en múltiplos de 32 bits (4 bytes). El valor mínimo de este campo es 5, que corresponde a un segmento sin datos (20 bytes).
    - Reservado (6 bits). Bits reservados para un posible uso futuro.
    - Bits de código o indicadores (6 bits). Los bits de código determinan el propósito y contenido del segmento. A continuación se explica el significado de cada uno de estos bits (mostrados de izquierda a derecha) si está a 1.
      - URG. El campo Puntero de urgencia contiene información válida.
      - ACK. El campo Número de acuse de recibo contiene información válida, es decir, el segmento actual lleva un ACK. Observemos que un mismo segmento puede transportar los datos de un sentido y las confirmaciones del otro sentido de la comunicación.
      - PSH. La aplicación ha solicitado una operación push (enviar los datos existentes en la memoria temporal sin esperar a completar el segmento).
      - RST. Interrupción de la conexión actual.
      - SYN. Sincronización de los números de secuencia. Se utiliza al crear una conexión para indicar al otro extremo cual va a ser el primer número de secuencia con el que va a comenzar a transmitir (veremos que no tiene porqué ser el cero).
      - FIN. Indica al otro extremo que la aplicación ya no tiene más datos para enviar. Se utiliza para solicitar el cierre de la conexión actual.
    - Ventana (16 bits). Número de bytes que el emisor del segmento está dispuesto a aceptar por parte del destino.
    - Suma de verificación (24 bits). Suma de comprobación de errores del segmento actual. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino.
    - Puntero de urgencia (8 bits). Se utiliza cuando se están enviando datos urgentes que tienen preferencia sobre todos los demás e indica el siguiente byte

del campo Datos que sigue a los datos urgentes. Esto le permite al destino identificar donde terminan los datos urgentes. Nótese que un mismo segmento puede contener tanto datos urgentes (al principio) como normales (después de los urgentes).

- Opciones (variable). Si está presente únicamente se define una opción: el tamaño máximo de segmento que será aceptado.
- Relleno. Se utiliza para que la longitud de la cabecera sea múltiplo de 32 bits.
- Datos. Información que envía la aplicación.

## Establecimiento de una conexión

Antes de transmitir cualquier información utilizando el protocolo TCP es necesario abrir una conexión. Un extremo hace una apertura pasiva y el otro, una apertura activa. El mecanismo utilizado para establecer una conexión consta de tres vías.



1. La máquina que quiere iniciar la conexión hace una apertura activa enviando al otro extremo un mensaje que tenga el bit SYN activado. Le informa además del primer número de secuencia que utilizará para enviar sus mensajes.

2. La máquina receptora (un servidor generalmente) recibe el segmento con el bit SYN activado y devuelve la correspondiente confirmación. Si desea abrir la conexión, activa el bit SYN del segmento e informa de su primer número de secuencia. Deja abierta la conexión por su extremo.

3. La primera máquina recibe el segmento y envía su confirmación. A partir de este momento puede enviar datos al otro extremo. Abre la conexión por su extremo.

4. La máquina receptora recibe la confirmación y entiende que el otro extremo ha abierto ya su conexión. A partir de este momento puede enviar ella también datos. La conexión ha quedado abierta en los dos sentidos.

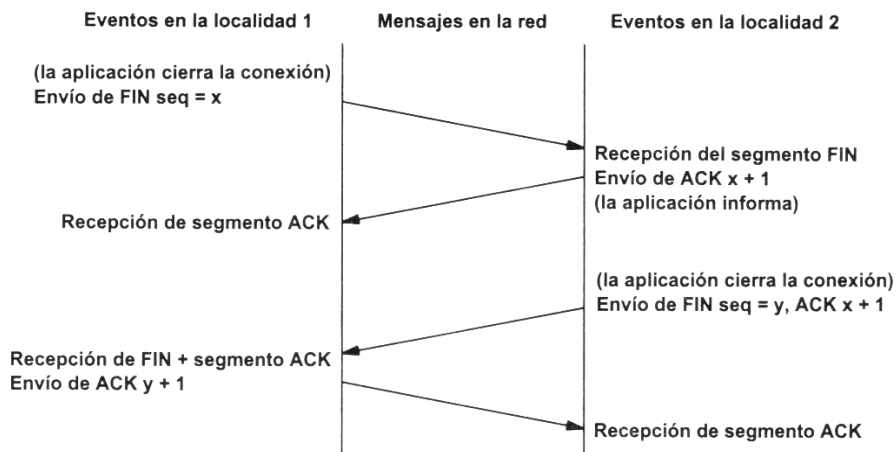
Observamos que son necesarios 3 segmentos para que ambas máquinas abran sus conexiones y sepan que la otra también está preparada.

**Números de secuencia.**— Se utilizan números de secuencia distintos para cada sentido de la comunicación. Como hemos visto el primer número para cada sentido se acuerda al establecer la comunicación. Cada extremo se inventa un número aleatorio y envía éste como inicio de secuencia. Observamos que los números de secuencia no comienzan entonces en el cero. ¿Por qué se procede así? Uno de los motivos es para evitar conflictos: supongamos que la conexión en un ordenador se interrumpe nada más empezar y se crea una nueva. Si

ambas han empezado en el cero es posible que el receptor entienda que la segunda conexión es una continuación de la primera (si utilizan los mismos puertos).

## Cierre de una conexión

Cuando una aplicación ya no tiene más datos que transferir, el procedimiento normal es cerrar la conexión utilizando una variación del mecanismo de 3 vías explicado anteriormente.



El mecanismo de cierre es algo más complicado que el de establecimiento de conexión debido a que las conexiones son full-duplex y es necesario cerrar cada uno de los dos sentidos de forma independiente.

1. La máquina que ya no tiene más datos que transferir, envía un segmento con el bit FIN activado y cierra el sentido de envío. Sin embargo, el sentido de recepción de la conexión sigue todavía abierto.

2. La máquina receptora recibe el segmento con el bit FIN activado y devuelve la correspondiente confirmación. Pero no cierra inmediatamente el otro sentido de la conexión sino que informa a la aplicación de la petición de cierre. Aquí se produce un lapso de tiempo hasta que la aplicación decide cerrar el otro sentido de la conexión.

3. La primera máquina recibe el segmento ACK.

4. Cuando la máquina receptora toma la decisión de cerrar el otro sentido de la comunicación, envía un segmento con el bit FIN activado y cierra la conexión.

5. La primera máquina recibe el segmento FIN y envía el correspondiente ACK. Observemos que aunque haya cerrado su sentido de la conexión sigue devolviendo las confirmaciones.

6. La máquina receptora recibe el segmento ACK.

## Nombres de dominio

Generalmente nosotros no trabajamos con direcciones IP sino con nombres de dominio del estilo de [msnews.microsoft.com](http://msnews.microsoft.com). Para que esto pueda ser posible es necesario un proceso previo de conversión de nombres de dominio a direcciones IP, ya que el protocolo IP requiere direcciones IP al enviar sus datagramas. Este proceso se conoce como resolución de nombres.

## Métodos estándar de resolución de nombres

A continuación se comentan brevemente los distintos métodos de resolución de nombres que utiliza Microsoft Windows para traducir un nombre de dominio a dirección IP. Estos métodos son aplicables a las utilidades TCP/IP que proporciona Windows (Ping, Tracert...) y son distintos a los utilizados desde Entorno de Red.

Método de resolución	Descripción
1. Local host name	Nombre de host configurado para la máquina (Entorno de Red, TCP/IP, configuración DNS)
2. Fichero HOSTS	Fichero de texto situado en el directorio de Windows que contiene una traducción de nombres de dominio en direcciones IP.
3. Servidor DNS	Servidor que mantiene una base de datos de direcciones IP y nombres de dominio
4. Servidor de nombres NetBIOS	Servidor que mantiene una base de datos de direcciones IP y nombres NetBIOS. Los nombres NetBIOS son los que vemos desde Entorno de Red y no tienen porqué coincidir con los nombres de dominio
5. Local Broadcast	Broadcasting a la subred local para la resolución del nombre NetBIOS
6. Fichero LMHOSTS	Fichero de texto situado en el directorio de Windows que contiene una traducción de nombres NetBIOS en direcciones IP

Cada vez que escribimos un nombre de dominio en una utilidad TCP/IP, por ejemplo:

```
C:\>ping www.ibm.com
```

se van utilizando cada uno de los métodos descritos desde el primero al último hasta que se consiga resolver el nombre. Si después de los 6 métodos no se ha encontrado ninguna coincidencia, se producirá un error.

El fichero HOSTS proporciona un ejemplo muy sencillo de resolución de nombres:

```
127.0.0.1 localhost
192.168.0.69 servidor
129.168.0.1 router
```

## Necesidad del DNS

En los orígenes de Internet, cuando sólo había unos cientos de ordenadores conectados, la tabla con los nombres de dominio y direcciones IP se encontraba almacenada en un único ordenador con el nombre de HOSTS.TXT. El resto de ordenadores debían consultarle a éste cada vez que tenían que resolver un nombre. Este fichero contenía una estructura plana de nombres, tal como hemos visto en el ejemplo anterior y funcionaba bien ya que la lista sólo se actualizaba una o dos veces por semana.

Sin embargo, a medida que se fueron conectando más ordenadores a la red comenzaron los problemas: el fichero HOSTS.TXT comenzó a ser demasiado extenso, el mantenimiento se hizo difícil ya que requería más de una actualización diaria y el tráfico de la red hacia este ordenador llegó a saturarla.

Es por ello que fue necesario diseñar un nuevo sistema de resolución de nombres que distribuyese el trabajo entre distintos servidores. Se ideó un sistema jerárquico de resolución conocido como DNS (Domain Name System, sistema de resolución de nombres).

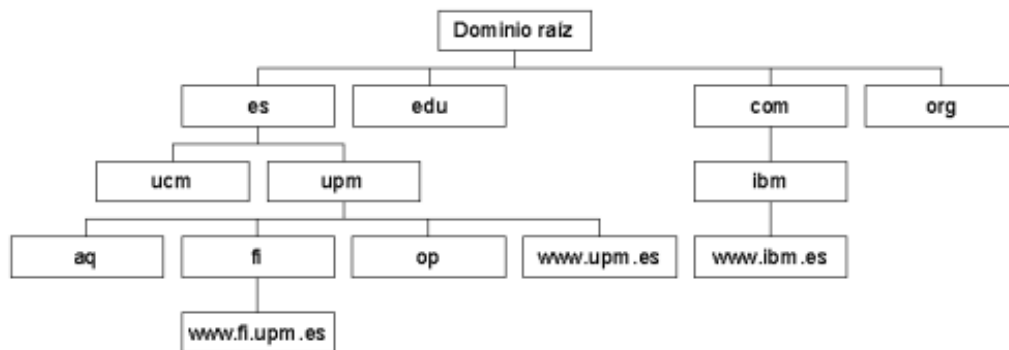
## Componentes del DNS

Para su funcionamiento, el DNS utiliza tres componentes principales:

- Clientes DNS (resolvers). Los clientes DNS envían las peticiones de resolución de nombres a un servidor DNS. Las peticiones de nombres son preguntas de la forma: ¿Qué dirección IP le corresponde al nombre nombre.dominio?
- Servidores DNS (name servers). Los servidores DNS contestan a las peticiones de los clientes consultando su base de datos. Si no disponen de la dirección solicitada pueden reenviar la petición a otro servidor.
- Espacio de nombres de dominio (domain name space). Se trata de una base de datos distribuida entre distintos servidores.

## Espacio de nombres de dominio

El espacio de nombres de dominio es una estructura jerárquica con forma de árbol que clasifica los distintos dominios en niveles. A continuación se muestra una pequeña parte del espacio de nombres de dominio de Internet:



El punto más alto de la jerarquía es el dominio raíz. Los dominios de primer nivel (es, edu, com...) parten del dominio raíz y los dominios de segundo nivel (upm, ucm, microsoft...), de un dominio de primer nivel; y así sucesivamente. Cada uno de los dominios puede contener tanto hosts como más subdominios.

Un nombre de dominio es una secuencia de nombres separados por el carácter delimitador punto. Por ejemplo, www.fi.upm.es. Esta máquina pertenece al dominio fi (Facultad de Informática) que a su vez pertenece al dominio upm (Universidad Politécnica de Madrid) y éste a su vez, al dominio es (España).

Generalmente cada uno de los dominios es gestionado por un servidor distinto; es decir, tendremos un servidor para el dominio aq.upm.es (Arquitectura), otro para op.upm.es (Obras Públicas) y así sucesivamente.

Los dominios de primer nivel (Top-Level Domains) han sido clasificados tanto en función de su estructura organizativa como geográficamente. Ejemplos:

En función de su estructura organizativa:

Nombre de dominio	Significado
com	organizaciones comerciales
net	redes
org	otras organizaciones
edu	instituciones educativas y universidades
gov	organizaciones gubernamentales
mil	organizaciones militares

Geográficamente:

Nombre de dominio	Significado
es	España
tw	Taiwán
fr	Francia
tv	Tuvalu

## Zonas de autoridad

Una zona de autoridad es la porción del espacio de nombres de dominio de la que es responsable un determinado servidor DNS. La zona de autoridad de estos servidores abarca al menos un dominio y también pueden incluir subdominios; aunque generalmente los servidores de un dominio delegan sus subdominios en otros servidores.

## Tipos de servidores DNS

Dependiendo de la configuración del servidor, éste puede desempeñar distintos papeles:

- Servidores primarios (primary name servers). Estos servidores almacenan la información de su zona en una base de datos local. Son los responsables de mantener la información actualizada y cualquier cambio debe ser notificado a este servidor.
- Servidores secundarios (secondary name servers). Son aquellos que obtienen los datos de su zona desde otro servidor que tenga autoridad para esa zona. El proceso de copia de la información se denomina transferencia de zona.

- **Servidores maestros (master name servers).** Los servidores maestros son los que transfieren las zonas a los servidores secundarios. Cuando un servidor secundario arranca busca un servidor maestro y realiza la transferencia de zona. Un servidor maestro para una zona puede ser a la vez un servidor primario o secundario de esa zona. Estos servidores extraen la información desde el servidor primario de la zona. Así se evita que los servidores secundarios sobrecargen al servidor primario con transferencias de zonas.

- **Servidores locales (caching-only servers).** Los servidores locales no tienen autoridad sobre ningún dominio: se limitan a contactar con otros servidores para resolver las peticiones de los clientes DNS. Estos servidores mantienen una memoria caché con las últimas preguntas contestadas. Cada vez que un cliente DNS le formula una pregunta, primero consulta en su memoria caché. Si encuentra la dirección IP solicitada, se la devuelve al cliente; si no, consulta a otros servidores, apunta la respuesta en su memoria caché y le comunica la respuesta al cliente.

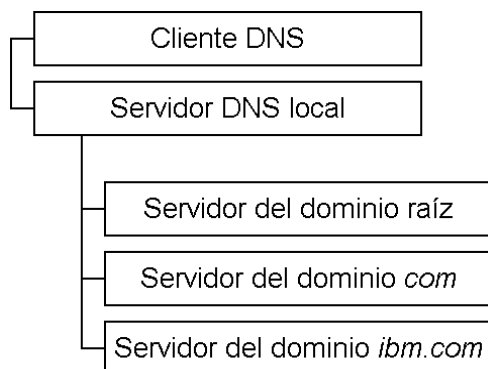
Los servidores secundarios son importantes por varios motivos. En primer lugar, por seguridad debido a que la información se mantiene de forma redundante en varios servidores a la vez. Si un servidor tiene problemas, la información se podrá recuperar desde otro. Y en segundo lugar, por velocidad porque evita la sobrecarga del servidor principal distribuyendo el trabajo entre distintos servidores situados estratégicamente (por zonas geográficas, por ejemplo).

## **Resolución de nombres de dominio**

La resolución de un nombre de dominio es la traducción del nombre a su correspondiente dirección IP. Para este proceso de traducción los resolvers pueden formular dos tipos de preguntas (recursivas e iterativas).

- **Preguntas recursivas.** Si un cliente formula una pregunta recursiva a un servidor DNS, éste debe intentar por todos los medios resolverla aunque para ello tenga que preguntar a otros servidores.
- **Preguntas iterativas.** Si, en cambio, el cliente formula una pregunta iterativa a un servidor DNS, este servidor devolverá o bien la dirección IP si la conoce o si no, la dirección de otro servidor que sea capaz de resolver el nombre.

Veamos un ejemplo: Estamos trabajando con Internet Explorer y escribimos en la barra de dirección: [www.ibm.com](http://www.ibm.com). En primer lugar, el navegador tiene que resolver el nombre de dominio a una dirección IP. Después podrá comunicarse con la correspondiente dirección IP, abrir una conexión TCP con el servidor y mostrar en pantalla la página principal de IBM. La siguiente gráfica muestra el esquema de resolución:



1. Nuestro ordenador (cliente DNS) formula una pregunta recursiva a nuestro servidor DNS local (generalmente el proveedor de Internet).

2. El servidor local es el responsable de resolver la pregunta, aunque para ello tenga que reenviar la pregunta a otros servidores. Suponemos que no conoce la dirección IP asociada a [www.ibm.com](http://www.ibm.com); entonces formulará una pregunta iterativa al servidor del dominio raíz.

3. El servidor del dominio raíz no conoce la dirección IP solicitada, pero devuelve la dirección del servidor del dominio com.

4. El servidor local reenvía la pregunta iterativa al servidor del dominio com.

5. El servidor del dominio com tampoco conoce la dirección IP preguntada, aunque sí conoce la dirección del servidor del dominio ibm.com, por lo que devuelve esta dirección.

6. El servidor local vuelve a reenviar la pregunta iterativa al servidor del dominio ibm.com.

7. El servidor del dominio ibm.com conoce la dirección IP de [www.ibm.com](http://www.ibm.com) y devuelve esta dirección al servidor local.

8. El servidor local por fin ha encontrado la respuesta y se la reenvía a nuestro ordenador.

## Preguntas inversas

Los clientes DNS también pueden formular preguntas inversas, esto es, conocer el nombre de dominio dada una dirección IP. Para evitar una búsqueda exhaustiva por todo el espacio de nombres de dominio, se ha creado un dominio especial llamado in-addr.arpa. Cuando un cliente DNS desea conocer el nombre de dominio asociado a la dirección IP a.b.c.d, formula una pregunta inversa a d.c.b.a.in-addr.arpa. La inversión de los bytes es necesaria debido a que los nombres de dominio son más genéricos por la derecha, al contrario que ocurre con las direcciones.

## Documentación recomendada

### Bibliografía

Comer E., Douglas: Redes globales de información con Internet y TCP/IP, tercera edición. Prentice Hall, 1996. [Protocolos TCP/IP]

Stallings, William: Comunicaciones y redes de computadores, quinta edición. Prentice Hall, 1997. [Principios de redes y comunicaciones]

Tanenbaum, Andrew S.: Redes de computadoras, tercera edición. Pearson, 1997. [Estudio de las redes tomando como ejemplos TCP/IP y ATM]

Yraolagoitia, Jaime de: Windows 98. Paraninfo, 1998. [Redes en Windows 98]

En Internet

Tella Llop, Jose Manuel: Fundamentos del TCP/IP. Publicado originalmente en septiembre de 1999 en los grupos de noticias [microsoft.public.es.windows98](http://microsoft.public.es.windows98). [TCP/IP orientado a Windows]

Request For Comments: <http://www.cis.ohio-state.edu/hypertext/information/rfc.html> [Especificaciones y estándares de Internet]

Categoría de <http://dmoz.org/World/Español/Computadoras/Internet/Protocolos/> de dmoz.org: [Selección de páginas web en castellano que tratan sobre los protocolos de Internet]