REDES DE DATOS

Fuente de información: CD-ROM curso del PNTE.

Adaptación: Fernando Pascual Morales

Tudela 2004/05

LAN, MAN, WAN

Un criterio para clasificar las redes de ordenadores es el que se basa en su extensión geográfica, por eso se habla de redes de área local (**LAN**), redes de área metropolitana (**MAN**) y redes de área extensa (**WAN**).

Aunque este curso se centra en las redes de área local (o simplemente red local), nos dará una mejor perspectiva conocer también los otros dos tipos: MAN y WAN.

Las LAN (***L**ocal **A**rea **N**etwork, red de área local*) son redes de propiedad privada, por ejemplo una oficina, un centro educativo o nuestra propia casa. La longitud de su cableado puede llegar hasta unos cuantos kilómetros de extensión, pero no suelen abandonar el edificio donde se encuentra ubicada (aunque pudieran estar unidos varios edificios próximos, por ejemplo, en un campus universitario o en un complejo hospitalario). Su principal uso reside en la conexión de ordenadores con objeto de compartir recursos e intercambiar información.

Las MAN (***M**etropolitan **A**rea **N**etwork, red de área metropolitana*) son una versión mayor de la LAN y utilizan una tecnología muy similar. Suelen ser también redes privadas. Geográficamente cubren un espacio mayor, pues engloba la conexión entre distintos edificios repartidos por una ciudad. Pongamos, por ejemplo, varios centros de enseñanza, organismos oficiales, sucursales de empresas privadas, etc. Actualmente esta clasificación ha caído en desuso y normalmente sólo distinguiremos entre redes LAN y WAN.

Las WAN (***W**ide **A**rea **N**etwork, red de área extensa*) son redes que se extienden sobre un área geográfica muy grande. Su infraestructura técnica es mucho más compleja que las redes anteriores, pues necesita de una colección de máquinas dedicadas a ejecutar los programas de usuarios (*hosts*) y otros sistemas (routers, líneas de comunicación,...). En realidad suelen ser varias LAN o WAN unidas entre sí formando una red mucho mayor. El mejor ejemplo de una WAN es Internet, donde se interconectan varias redes repartidas por el mundo.

Como puedes suponer, este tipo de redes son ya consideradas como de acceso público (lo cual no está exento de que sea obligado abonarse; es algo así como las líneas telefónicas, las compañías eléctricas o de gas ciudad: todo el mundo puede conectarse, previo pago de la tarifa correspondiente, claro está). También nos podemos encontrar con WAN privadas, tales como la red de cajeros automáticos y oficinas de un grupo bancario, por ejemplo.

Intranet, Extranet e Internet

Podemos definir la intranet como una red privada que ofrece las mismas prestaciones que Internet y que utiliza su misma tecnología y protocolos de comunicación.

Es decir, es una red con capacidad de mostrar páginas web internas, dispone de servidor de e-mail propio, servicio de FTP, foros de discusión, buscador,... y que utiliza un navegador para acceder y moverse por una réplica a escala de un portal de servicios.

Pero mientras que en Internet cualquiera puede conectarse a donde quiera, una intranet es siempre privada y pertenece exclusivamente a la organización a la que sirve. El acceso se da siempre por autorización o invitación.

Una intranet pone a disposición de sus usuarios información de manera interactiva, o sea que no sólo podemos recibir la información sino que también podemos emitirla. Esta socialización de los datos consigue más participación de la colectividad, facilita la consecución de objetivos personales y aumenta la productividad de todos los recursos disponibles, incluidos los humanos.

Ahora bien, cuando a esa misma intranet se pueda acceder desde Internet, se convertirá en una extranet. Así de sencillo. Y es que esto permite que usuarios externos, desde cualquier parte del mundo, a través de Internet, puedan conectarse a la intranet, pero sólo si conocen las claves de acceso, pues no olvidemos el carácter privado de este tipo de redes.

Las extranets están cada día más difundidas entre las entidades privadas, pues esto permite que cualquier trabajador que tenga que desplazarse, pueda estar al día de todo cuanto suceda en la intranet de la empresa;

aunque sólo sea para consultar el correo electrónico interno. Por ejemplo, la compañía Ford tiene una extranet, llamada *Focalpt*, que conecta 15.000 distribuidores a nivel mundial, de manera que cualquiera puede consultar desde la disponibilidad de repuestos, hasta tramitar la compra y seguimiento de un vehículo durante su fabricación, pero su acceso es restringido. Tan sólo las personas habilitadas que disponen de las claves de acceso pueden disfrutar de su contenido.

La verdad es que se suele prescindir de este término y referirse a las extranets como intranets.

Pues bien, expuestas estas primeras cuestiones iniciales, tal vez ahora podamos clarificar aún más las dos intenciones del curso:

- Primeramente aprenderás a montar una red local, en toda su extensión, desde una pequeña red de dos ordenadores hasta una configuración para un centro de enseñanza.
- Y finalmente, te enseñaremos a implementar una auténtica intranet.

Conexión de dos PC

Por ahora no es que ya sepamos mucho de conectividad de redes locales, más bien nada, pero puede ser éste un buen momento para intentar instalar nuestra primera LAN.

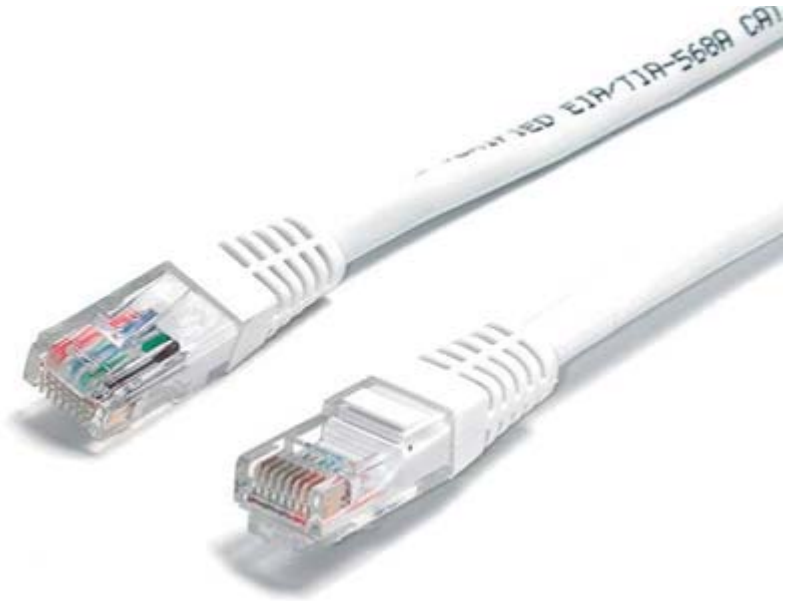
Y no es ninguna locura, es una buena práctica para iniciarse en este nuevo mundo. Sí, ya sabemos que lo normal en estos casos es encontrarse con una retahíla de conceptos teóricos, pero permítenos, por una vez y sin que sirva de precedente, saltarnos lo 'políticamente correcto', coger la caja de herramientas y comenzar el trabajo.

No te dejes sobrecoger por la terminología con la que nos referimos a algunos elementos, simplemente admítela tal y como está escrita y a medida que el curso avance irás descubriendo su significado.

Para implementar una red básica necesitarás:

- Dos ordenadores (por ahora de sobremesa, los portátiles ya se verán más adelante) con el sistema operativo Windows 98, o superior, instalado.
- El CD-ROM de instalación del sistema operativo.
- Dos tarjetas de red PCI Fast Ethernet 10/100 (100-BASE-TX), preferentemente iguales (del mismo modelo y fabricante), con conexión RJ-45 y con sus drivers más actualizados. Los drivers suelen venir en forma de disquete o de CD-ROM, acompañando siempre a la propia tarjeta.

- Cable UTP de par trenzado de categoría 5 o superior (importantísimo respetar esta característica) de cuatro pares de hilos, según la longitud necesaria (pongamos unos 10 metros).



- Dos conectores RJ-45.
- Una herramienta de crimpado.

- Un pelacables o unas simples tijeras de electricista.

- Un comprobador de cables o, en su defecto, un polímetro, para verificar la continuidad del cable.

Las herramientas que mencionamos son indispensables para llevar a buen término cualquier instalación de una LAN y es una inversión casi obligada.

Que duda cabe de que si todo funciona bien nunca se necesitará un comprobador de cables, pero en instalaciones un poco más complejas, no es normal que todo funcione a la primera y en el proceso de solución, las primeras comprobaciones siempre han de ser con respecto al cableado y la conectorización. Los técnicos instaladores tienen una máxima: "*Si todo te funciona bien a la primera, es que algo has hecho mal*".

El cable de conexión

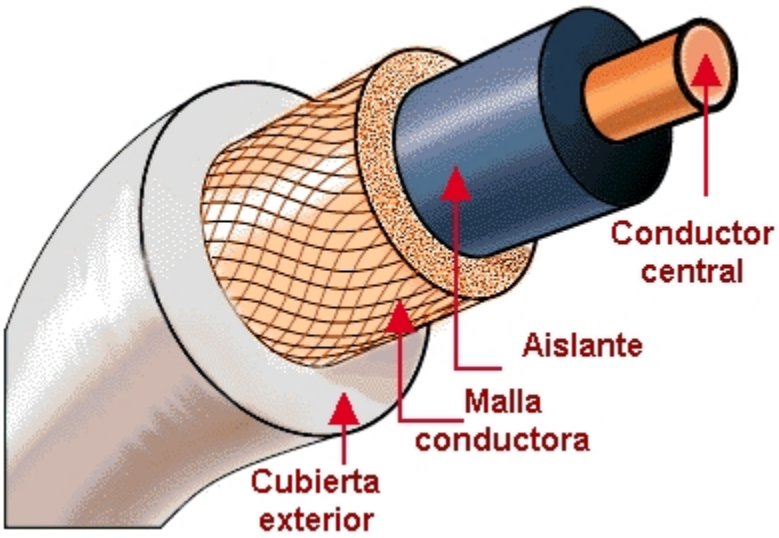
Estamos ante el caso más sencillo de cableado: la unión de dos ordenadores. La verdad es que podríamos comprarlo ya construido en cualquier comercio del ramo, pero no tendría el mismo mérito que si lo construyéramos nosotros mismos. Y eso es lo que vamos a hacer, pues más adelante intentaremos implementar redes mayores y no habrá más remedio que construirse uno mismo toda la conectorización.

Tal y como te dijimos al principio del capítulo, necesitamos **cable de par trenzado UTP** de **categoría 5** (o superior) y de cuatro pares, **dos conectores RJ-45**, el pelacables y la herramienta de crimpado.

¿Qué son todas esas nomenclaturas?. Ya te hemos comentado que en esto de la conectividad por cable en redes locales se utilizan, básicamente, tres tipos: el cable coaxial, el cable de par trenzado y la fibra óptica, de la que no hablaremos por ahora, dado que esta tecnología no se apoya en un cable puramente eléctrico y su alto precio no se justifica en redes locales de pequeña envergadura.

El cable coaxial

¿Cómo es un cable coaxial? ¿Has visto el cable de antena de la TV? Pues eso es un cable coaxial. Consiste en un conductor central rodeado de otro conductor exterior en forma de malla y que se mantiene separado del conductor interno por un material aislante. El conductor exterior se rodea de una cubierta con una funda protectora que da el color característico al cable.

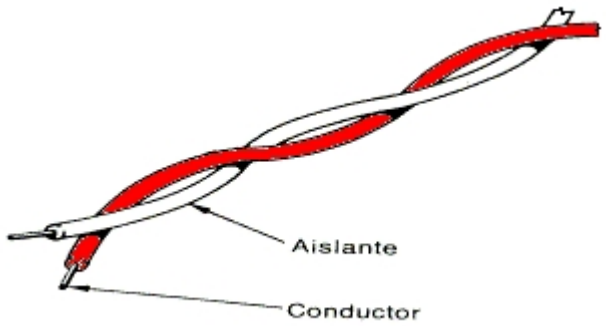


Originalmente fue el cable más usado en las redes locales debido a su alta insensibilidad a las interferencias, pero su grosor, que no lo hace muy adecuado para los conductos eléctricos angulosos, es su mayor defecto.

Tiene a su favor que es capaz de transportar las señales eléctricas a una distancia mayor y con menores pérdidas en la transmisión, gracias a su mejor apantallamiento y menor resistencia eléctrica, por eso suele usarse en tendidos largos. Son tipos característicos el RG-8, RG-11 y RG-58 (el más usado en redes locales).

El cable de par trenzado

Es el que más se utiliza y el más económico. Cada cable de este tipo está compuesto por una serie de pares de cables trenzados en forma helicoidal y sin apantallar (***U**nshielded **T**wisted **P**air* - **UTP**). Los pares se trenzan para reducir las interferencias electromagnéticas o las provocadas entre pares adyacentes (*diafonía*). También se fabrica cable UTP apantallado por una fina lámina de aluminio para aquellas instalaciones que por su alto nivel de interferencia o de ruido eléctrico así lo aconsejen. En este caso se llama cable FTP (***F**oiled **T**wisted **P**air* o ScTP: ***S**creened **UTP***) o cable SSTP (***S**hielded* + ***F**oiled **T**wisted **P**air*): idéntico al anterior, pero además con mejor apantallamiento al incorporar una malla de cobre.



Existen cables con distinto número de pares en su interior, pero nosotros usaremos el que tiene **cuatro pares** de hilos.

Para ayudar en su identificación, los cables de cada par se colorean según un estándar: el llamado **EIA/TIA 568**. Así tendremos los colores:

Par 1: Azul

Par 2: Naranja

Par 3: Verde

Par 4: Marrón

Cada uno con su par trenzado correspondiente formado por un cable de color blanco o con franjas del color de su par.

Para no tener que describir un cable haciendo mención a sus características eléctricas, los cables se han dividido en categorías. La más sencilla es la categoría 1, que se utiliza para comunicaciones telefónicas y no es apropiado para la transmisión de datos. La categoría 2 se emplea para las conexiones telefónicas y datos con velocidades de hasta 4 Mbps. La categoría 3 se usa para la conexión 10-BASE-T (10 Mbps). La categoría 4 se utiliza en redes Token-Ring (de IBM) y llega a los 16 Mbps.

Y, por fin, nuestra **categoría 5** que se usa en conexiones de 100 Mbps (100-BASE-TX).

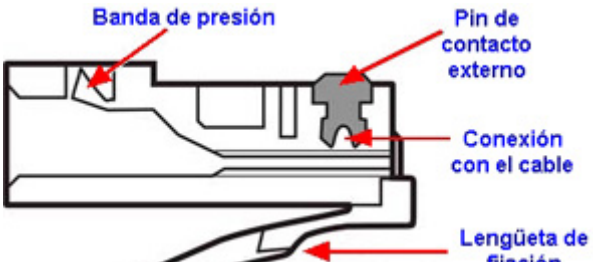
Y esto sigue avanzando, pues ya se está imponiendo la categoría 5e, que no es más que la anterior mejorada al minimizar la atenuación y las interferencias; y las categorías 6 y 7, con mejores prestaciones, pero estos sistemas son mucho más caros y no se justificarían en una red de nuestras características.

Bueno, ya deberías tener claro por qué nuestro cable ha de ser de par trenzado (bien sea UTP ó FTP, no importa) de categoría 5 y de cuatro pares. Ahora hablemos del conector y veamos cómo construir el cable.

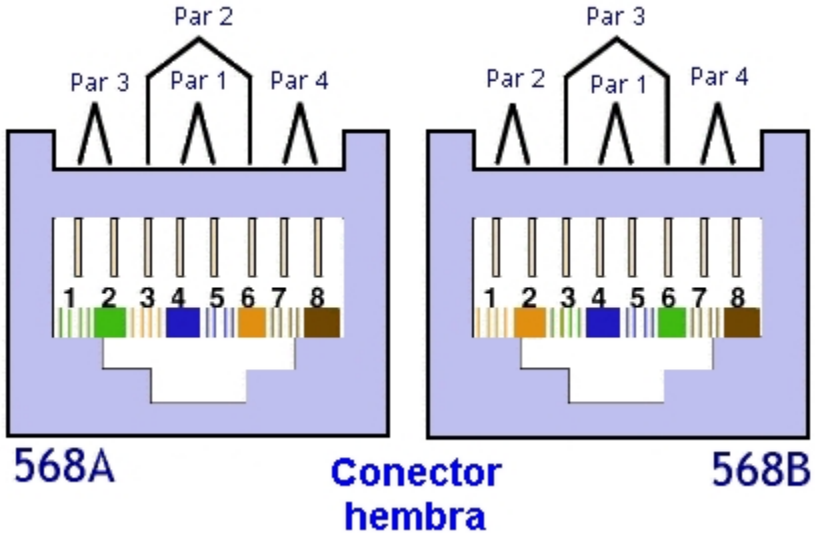
El conector RJ-45 macho

El conector es la interface entre el cable y un dispositivo de la red, en este caso la tarjeta de red o adaptador.

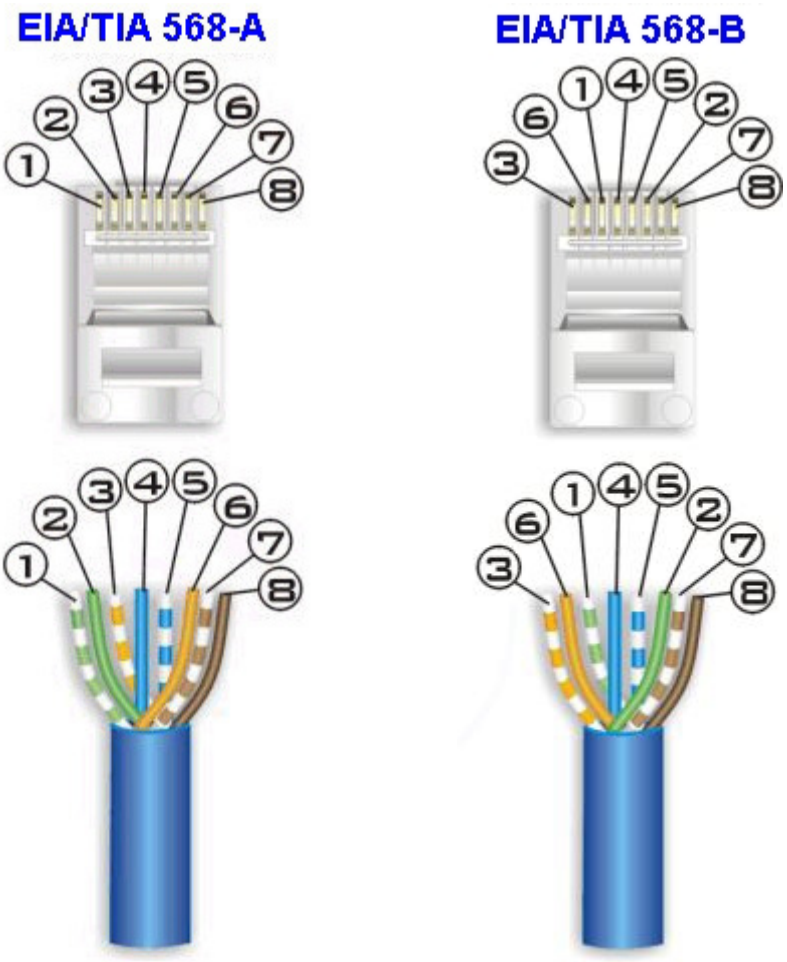
Usaremos un conector **RJ-45** (el término RJ viene de ***R**egistered **J**ack*), que es similar a los utilizados para el teléfono (conocido como RJ-11), salvo que el RJ-45 dispone de conexión para 8 hilos y el telefónico para 4 hilos.



Pero ¿cómo hemos de distribuir los 8 hilos en el conector? Según el estándar EIA/TIA 568, se establecen dos esquemas de conexión: el EIA/TIA **568A** (o *ISDN*) y el EIA/TIA **568B** (o *AT&T*).



Las diferencias básicas entre uno y otro radican en que en el 568A, el par 2 del cable (naranja) termina en los contactos 3 y 6, y el par 3 del cable (verde) en los contactos 1 y 2; mientras que el 568B sólo intercambia estos dos pares.

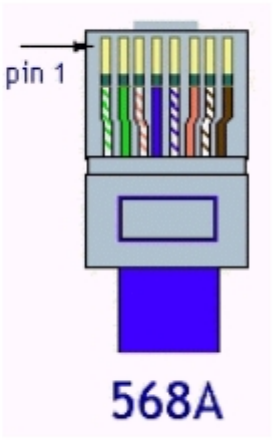


En ambos casos, los pares 1 (azul) y 4 (marrón) no varían de una configuración a otra.

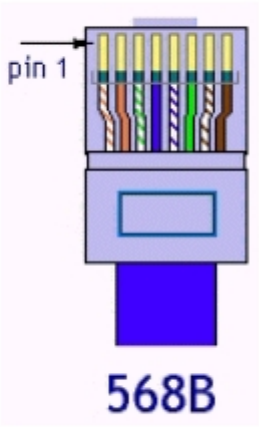
Construir el cable

Así que, para construir cualquier cable de red (técnicamente, *patch cord*), los 8 hilos deben ser colocados en el conector RJ-45 siguiendo cualquiera de estos dos estándares en ambos extremos del cable (es indiferente).

Pin	Par	Función	Color del cable
1	3	TX_D1+	Blanco/Verde
2	3	TX_D1-	Verde
3	2	RX_D2+	Blanco/Naranja
4	1	Bl_D3+	Azul
5	1	Bl_D3-	Blanco/Azul
6	2	RX_D2-	Naranja
7	4	Bl_D4+	Blanco/Marrón
8	4	Bl_D4-	Marrón

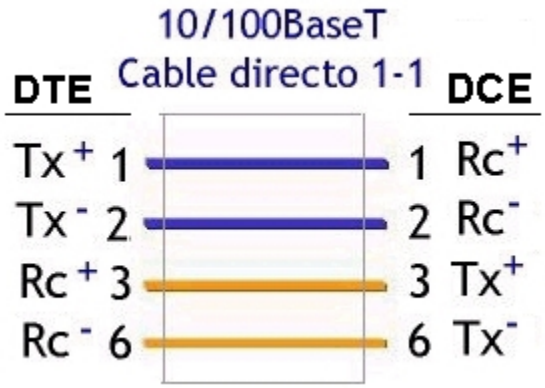


Pin	Par	Función	Color del cable
1	2	RX_D2+	Blanco/Naranja
2	2	RX_D2-	Naranja
3	3	TX_D1+	Blanco/Verde
4	1	Bl_D3+	Azul
5	1	Bl_D3-	Blanco/Azul
6	3	TX_D1-	Verde
7	4	Bl_D4+	Blanco/Marrón
8	4	Bl_D4-	Marrón



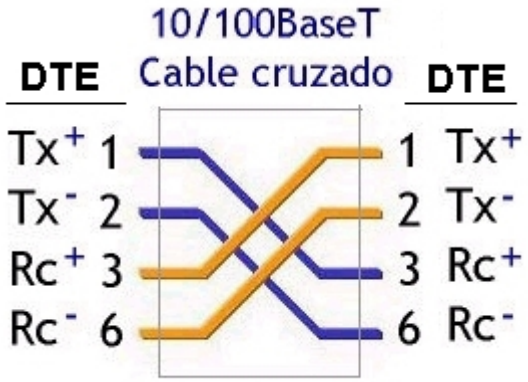
Pero hay aquí una salvedad importante. Se emplean dos tipos de cables: el **cable normal** (o *directo* - *Straight Trough*) y el **cable cruzado** (o *Cross-Over*).

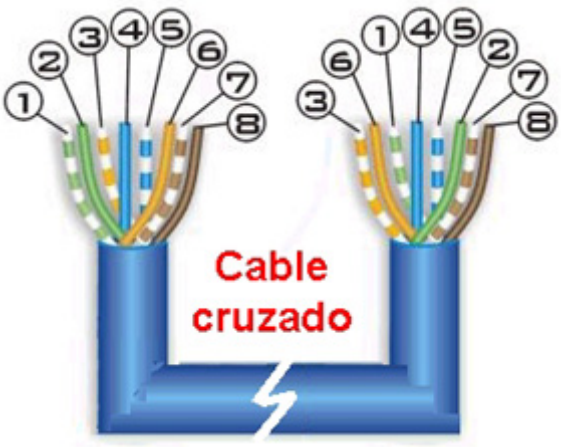
El cable normal es aquel en el que la serie de conexión de los colores de los hilos en cada extremo, bien sea 568A o 568B, son iguales. Es decir, que si en un extremo conectamos los hilos de acuerdo a la especificación EIA/TIA 568A, en el otro extremo ha de ser exactamente igual. Hay una correspondencia directa entre los pines de cada conector: El del pin 1 de un conector está unido al pin 1 del otro conector, y así sucesivamente.



Este tipo de cable se utiliza para unir un **DTE** (*Data Terminal Equipment*), tal como un ordenador, con un **DCE** (*Data Conmunication Equipment*), tal como un hub, switch, etc., equipos que más adelante veremos y que tienen cambiadas las funciones de los pines 1, 2 , 3 y 6. En un equipo transmiten datos y en el otro los reciben.

En cambio, el cable cruzado es aquel en el que por un extremo se coloca el conector según la norma EIA/TIA 568A y en el otro extremo según la norma TIA/EIA 568B. Así se garantiza que un par de transmisión (Tx) de un ordenador llegará a un par de recepción (Rx) del otro. Son los que se utilizarán para unir equipos iguales: DTE con DTE, o DCE con DCE.

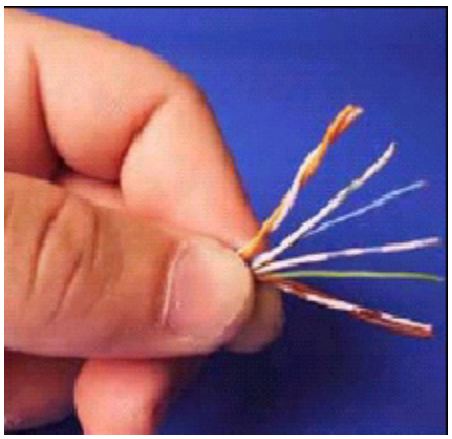




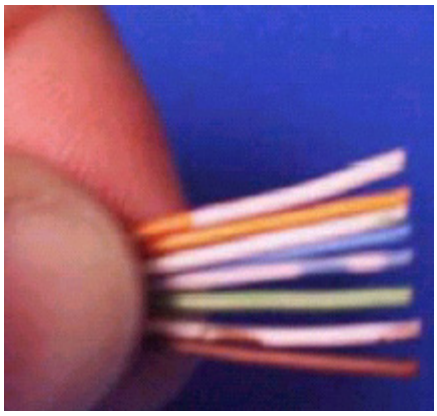
Así pues, para el caso particular de unir dos ordenadores (DTE con DTE) ¡sólo sirve el cable cruzado!

Construir el cable no requiere ninguna experiencia, sólo algo de destreza y un poco de paciencia la primera vez. Sigue los siguientes pasos:

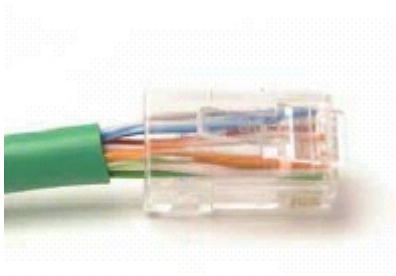
1. Pela el cable trenzado y localiza los cuatro pares con su correspondiente cable trenzado.



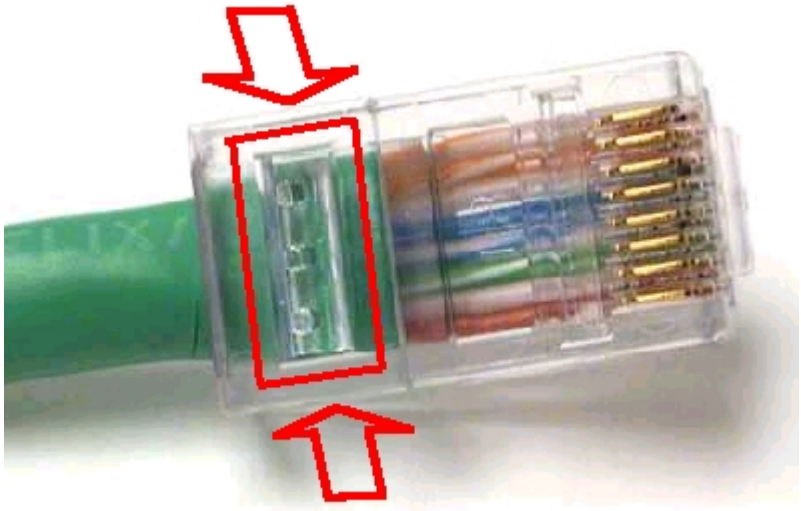
2. Ordena los pares de cables según el estándar EIA/TIA 568A, no hace falta que los peles, sólo asegúrate de que todos están rectos y a la misma longitud (unos 12-15 m/m).



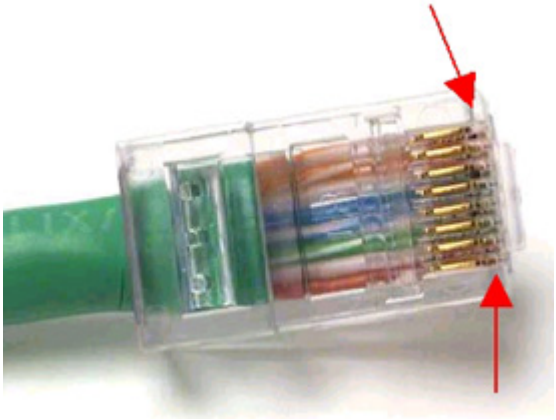
3. Introdúcelos dentro del conector RJ-45 para comprobar si su longitud es la adecuada.



4. Corta de manera que la cubierta del cable quede justo en la banda que lo presiona en el conector. El destrenzado de los pares nunca debe exceder los 13 m/m.



5. Empújalos hasta que lleguen al fondo, todos a la vez. No debe quedar ninguno más retrasado que los demás. Si es así, sácalos de nuevo e iguálalos en longitud.



6. Ahora introdúcelo en la crimpadora y apriétalo lo suficiente hasta que los pines del conector hagan perfecto contacto con los hilos del cable y quede mecánicamente consistente.

7. Repite los pasos anteriores con el otro extremo del cable, pero ahora con la secuencia de colores que marca la especificación EIA/TIA 568B.

8. Finalmente comprueba la continuidad del cable, bien con un comprobador de cables de red o con un polímetro. Ten presente el cruce de los pines en este tipo de cable a la hora de las comprobaciones.

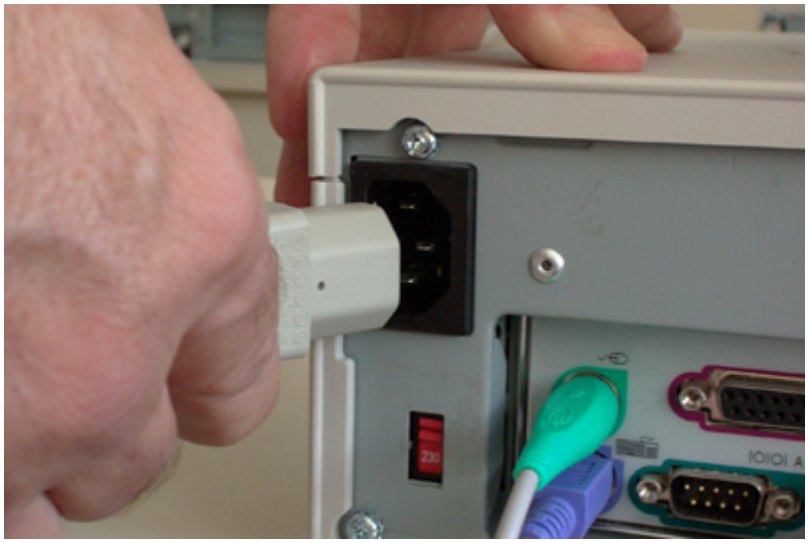
Si algún conector no funciona, no intentes recuperarlo crimpándolo más veces. Lo mejor es cortar el cable y empezar de nuevo, pues puede ser una perpetua fuente de problemas.

No olvides marcarlo de manera inequívoca, no vayas a confundirlo con un cable normal.

Instalar las tarjetas de red

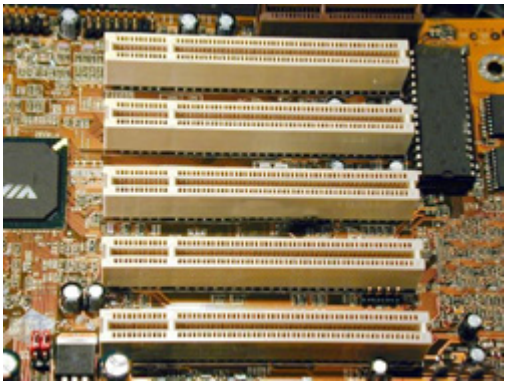
Comenzaremos por instalar las tarjetas de red en cada uno de los ordenadores. Sigue los pasos que se indican a continuación:

1. Cualquier acción dentro del ordenador ha de hacerse con el equipo apagado y totalmente desconectado de la red eléctrica. Así pues: desconecta el cable de alimentación para más seguridad.

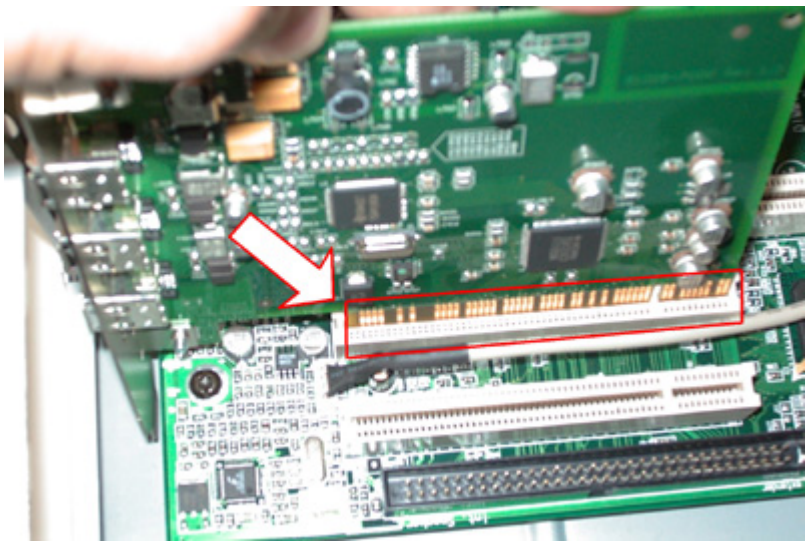


2. Abre la carcasa de la unidad central del ordenador. Según el tipo de caja, tendrás que retirar los tornillos de la parte posterior, o retirar el frontal, y la tapa superior o las laterales.

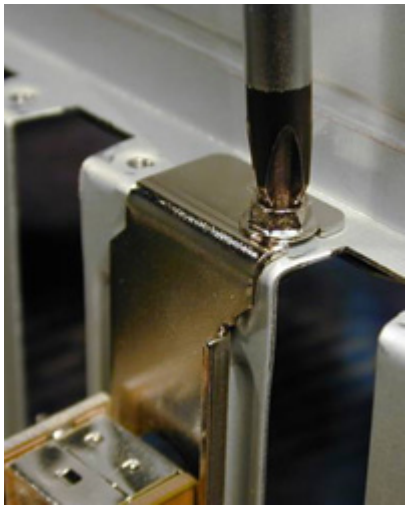
3. Busca una ranura PCI libre en la placa base del ordenador y, si es necesario, retira la plaquita protectora de la parte posterior para que quede libre el conector RJ-45 hembra de la tarjeta donde más tarde se enchufará el conector macho del cable de la red local.



4. Inserta la tarjeta de red en un slot PCI libre. En un principio, procura respetar el orden de inserción no dejando ranuras PCI intermedias. Presta atención a que la tarjeta quede bien conexionada y sus contactos entren perfectamente en el conector PCI.



5. Finalmente, fija la tarjeta al chasis de la caja con un tornillo; esto evitará que se mueva en las operaciones de conexión/desconexión del cable de red externo, pues se corre el peligro de averiar irremisiblemente la placa base. Si el agujero de fijación del tornillo no coincidiera con el del chasis de la caja, tal vez tengas que ajustarlo con un alicate.



Ya puedes cerrar la caja del ordenador.

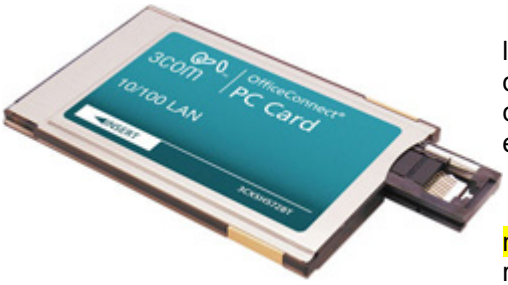
Coloca también la tarjeta en el otro ordenador siguiendo los mismos pasos que has hecho anteriormente.

Ahora, unas observaciones teóricas sin las cuáles no llegaríamos muy lejos.

Hasta este momento, al colocar a cada ordenador una tarjeta de red (técnicamente también se la conoce como *adaptador de red,* o NIC *-Network Interface Card-*) todo lo que has hecho es dotarlo de una circuitería electrónica capaz de permitirle la interconexión con el resto de elementos de la red. O sea, que servirá como interfaz entre el ordenador y el medio físico (técnicamente, *el canal*), en nuestro caso un cable, a través del cual se propagará la sucesión de señales eléctricas que viajarán entre los diferentes equipos que conforman la red.

Fíjate en las características que te indicamos que tuviera: PCI Fast Ethernet 10/100 (100-BASE-TX) y con conector RJ-45. ¿Qué quiere decir todo esto?

Ya te habrás dado cuenta de que se la llama tarjeta porque normalmente es eso: una tarjeta que se coloca en uno de los slot libres del PC (aunque cada vez son más los equipos que la llevan incorporada en la placa base). De ahí lo de indicar que fuera PCI, pues ese es el slot que usaremos en el PC para su conexión.



Si usáramos un ordenador portátil, la cosa cambiaría, pues, de no llevarla ya integrada en el equipo, utilizaríamos el slot PCMCIA que disponen todos los portátiles y la tarjeta tendría otro aspecto: algo así como una tarjeta de crédito. Aunque las prestaciones serían las mismas, el precio sería, como mínimo, el doble.

Lo de Fast Ethernet también tiene su explicación. *Ethernet* es una norma que describe un tipo específico de red. En este mundillo de las redes existen también otras especificaciones, por ejemplo, Token-Ring, ARCNET, FDDI,... pero en más del 90% de los casos se utiliza la tecnología Ethernet. Y no profundizaremos mucho más en ello porque teorizar aquí puede ser muy aburrido. Lo que sí es necesario entender es que todos los elementos que se utilicen en la implementación de la red sean compatibles con una especificación determinada. Así pues, para nosotros, todo cuanto compremos e instalemos ha de ser para una red Ethernet (estándar **IEEE 802.3**).

Desde sus inicios comerciales, la red Ethernet alcanza velocidades de transmisión de 10 Mbps (se lee 10 megabits por segundo), lo que quiere decir que se pueden enviar, aproximadamente, diez millones de bits en cada segundo (algo más de 1 millón de caracteres por segundo).

Para que un ordenador pueda mantener esa tasa de transferencia es preciso instalarle una tarjeta de red que funcione a esa velocidad, y como no podría ser de otra manera, la industria les da un nombre en función del cable que utilicemos para conectarla (ya veremos lo de los cables más adelante). Aunque existen más, aquí te nombramos algunos ejemplos con los que aún podrás encontrarte hoy en día:

- **10-BASE-2**, si se usa cable coaxial.
- **10-BASE-T**, si se usa cable de par trenzado.
- **10-BASE-F**, si se usa fibra óptica.

Para aumentar la velocidad de la red Ethernet se creó un nuevo comité que desarrolló la especificación **IEEE 802.3u**, más conocida como Fast Ethernet (¿lo ves?, ya hemos llegado a ella). Esta versión permite alcanzar velocidades de 100 Mbps que, como podrás suponer, exige que el ordenador disponga de una tarjeta de red específica para esa norma; sólo así se garantizará que alcance esa tasa de transferencia.

Por supuesto, también aquí se les ha dado un nombre a las tarjetas en función del cable que utilicemos para conectarlas:

- **100-BASE-TX**, si se usa cable de par trenzado.
- **100-BASE-FX**, si se usa fibra óptica.

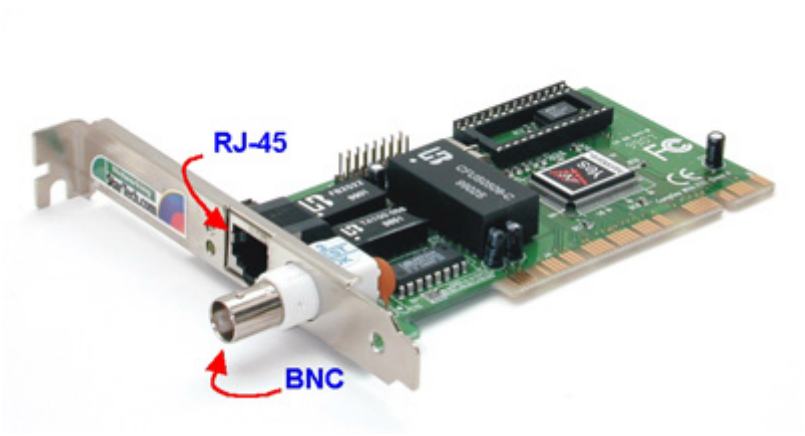
Como puedes comprobar en ambos casos, el primer número indica la velocidad a la que puede trabajar la tarjeta de red: 10:10 Mbps, 100:100 Mbps (aquí ya no se utiliza el cable coaxial). Ten en cuenta que los ordenadores, para poder comunicarse, han de tener instaladas tarjetas de igual velocidad: no se establecerá la comunicación si no se cumple este requisito. (En lugar de la letra 'X' del final podemos encontrarnos con un dígito, pues se refiere al número de hilos que use el cable de conexión: 100-BASE-T4, para cables de 4 hilos: 100-BASE-T8 si tiene 8 hilos -el que usaremos nosotros).

En nuestro caso te proponemos utilizar tarjetas que sean 10/100, lo que viene a decir que pueden funcionar a cualquiera de las dos velocidades. Ellas mismas se configuran, de manera automática, en función de la velocidad del dispositivo con el que quieren comunicarse en cada momento. Esto nos da mucha versatilidad, pues ºººpodríamos conectar cualquiera de estos ordenadores en redes más grandes donde desconociéramos las velocidades de conexión del resto de dispositivos instalados.

¿Y lo de RJ-45? Pues se refiere precisamente a la forma que ha de tener el conector donde se enchufará el cable de la red local que unirá los dos ordenadores. Como luego veremos, en el cableado de una red se utilizan, básicamente, tres tipos de conectores:

- **BNC**, para cable coaxial.
- **RJ45**, para cable de par trenzado.
- Para fibra óptica (varios modelos).

Algunas tarjetas de red pueden venir con los dos primeros tipos de conector (BNC y RJ45). Si sólo traen el BNC son de 10 Mbps; si son de 100 Mbps traerán sólo el conector RJ45, y si son 10/100 pueden traer ambos o sólo el RJ45.



Sea cual sea nuestro modelo de tarjeta, utilizaremos la conexión RJ45.

En el mundo de la conectorización siempre encontrarás dos versiones para cada modelo de conector: el **macho** (el que conecta) y la **hembra** (el que aloja)

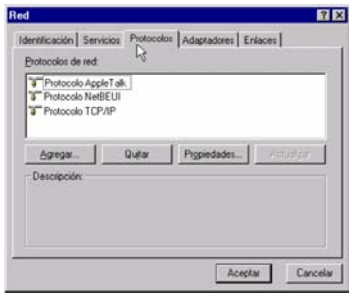
En el caso de la tarjeta, siempre llevan la hembra de cada modelo de conector. El macho es el que está colocado en el propio cable:

Practica 1.- Instalación de una tarjeta NIC -Instalar el driver de la tarjeta de red.

Escribir en el cuaderno de clase cuáles fueron los pasos seguidos para instalar una tarjeta de red. También escribir cuáles fueron las precauciones que se tomaron y la razón por la cual son importantes.

Copia todas las pantallas de configuración que requiere Windows para la instalación y configuración de una tarjeta de red.

Ejemplo:



(descripción de las opciones adoptadas en cada una de las ventanas)

Comprobando la instalación de la tarjeta

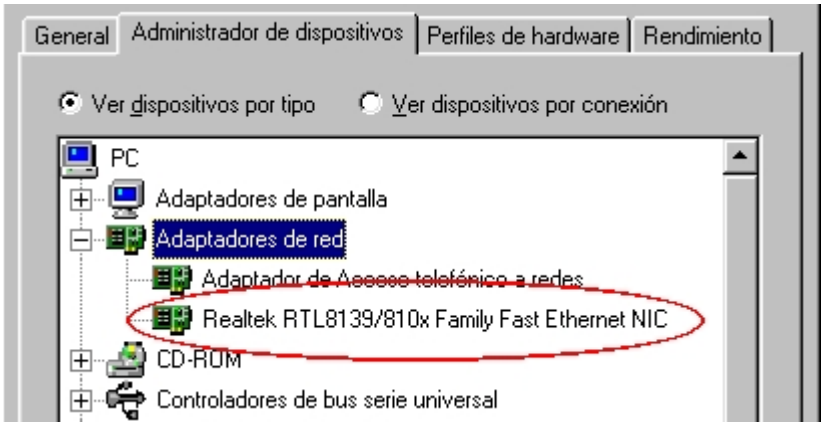
Ahora comprobaremos si la tarjeta está correctamente instalada en Windows. Para ello usaremos el **Administrador de Dispositivos**.

En Windows 95/98/Me, el procedimiento es como sigue:

1. Haz click con el botón derecho sobre el icono **Mi PC** ubicado en el Escritorio.

En el menú contextual que aparece, elige **Propiedades**. Aparecerá el cuadro de diálogo Propiedades de Sistema.

2. Accede a la pestaña Administrador de dispositivos y haz click sobre el símbolo ⊞ de la rama ⊞ Adaptadores de red. Si todo ha ido bien, aparecerá el nombre del adaptador de red instalado:

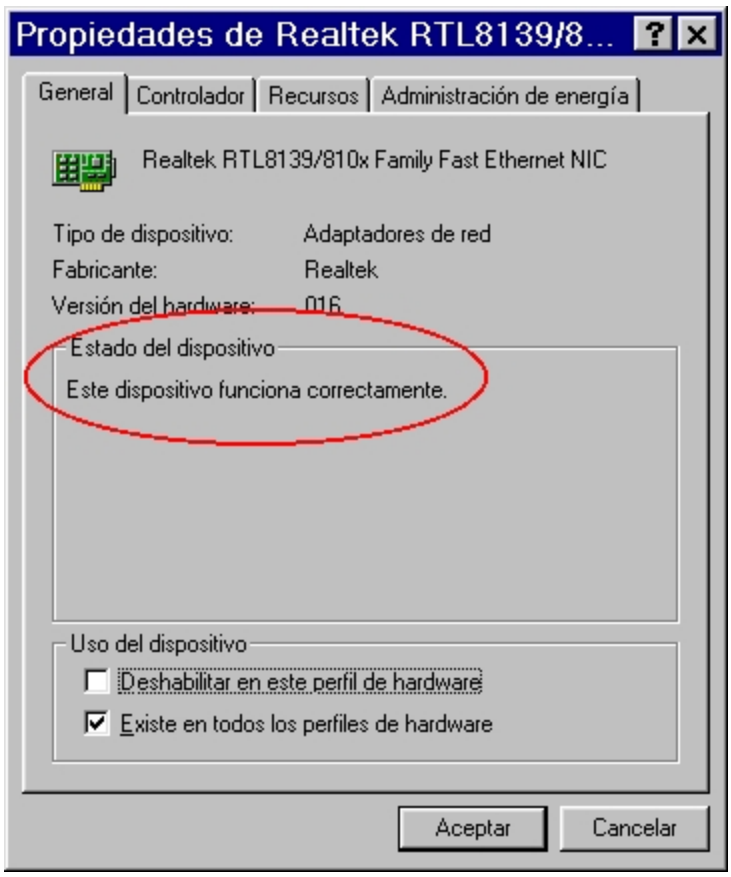


Si también aparece Adaptador de Acceso telefónico a redes es porque seguramente tendrás instalado un módem (como es nuestro caso) en el ordenador.

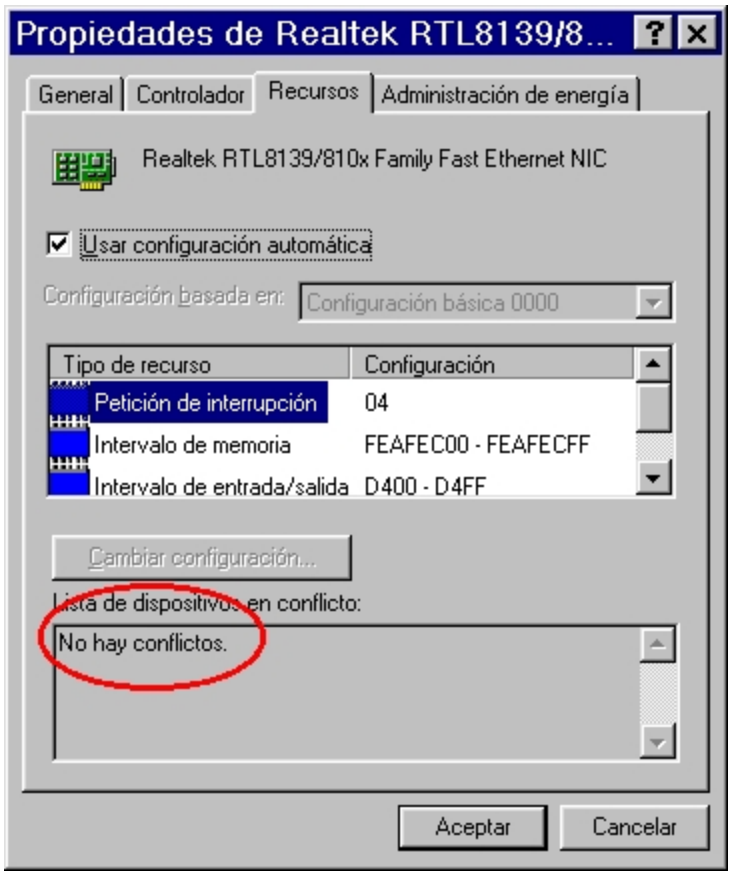
Si ha habido problemas durante la instalación de la tarjeta, puede que aparezca un signo de admiración amarillo al lado del nombre del adaptador si hay un conflicto con otro dispositivo instalado, o que veas una cruz roja sobre el mismo, dándonos a entender que el dispositivo aún no está preparado.

En estos casos, lo más conveniente es desinstalar por completo el driver. Para ello, haces click sobre el nombre de la tarjeta y luego pulsas sobre el botón Quitar. Finalmente, reinicias el ordenador. El sistema operativo volverá a detectar la tarjeta y, de nuevo, comienzas desde el principio la instalación tal y como antes te indicamos.

3. Para comprobar que todo está correcto, puedes hacer doble click sobre el propio nombre del adaptador Realtek RTL8139/810x Family Fast Ethernet NIC, acceder a la pestaña General y comprobar que Este dispositivo funciona correctamente.:



Y, desde la pestaña Recursos comprobar que No hay conflictos.:



Si todo esto es así, será señal inequívoca de que la instalación ha sido plenamente satisfactoria.

Los componentes de la red

Pero es que también ocurren más cosas al instalar las tarjetas de red. En Windows 95/98/Me, se instalan también los **servicios** y **protocolos** más importantes de forma automática. ¿De qué estamos hablando?

Simplificando mucho, diremos que los **servicios** son esas 'pequeñas' cosas que la red puede hacer por nosotros. Por ejemplo: si queremos compartir una impresora o algunas carpetas de las instaladas en el disco duro de cualquier ordenador, entre otros.

La importancia del protocolo

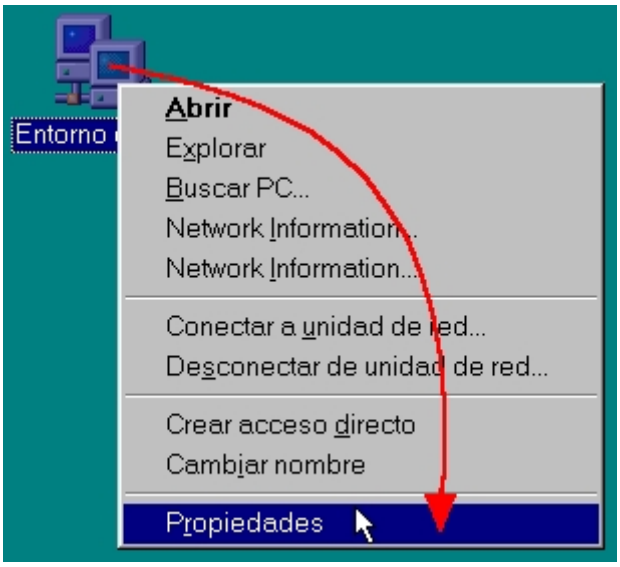
Los **protocolos** son el conjunto de normas que implantaremos en todos y cada uno de los ordenadores de la red para que puedan entenderse entre sí. Es algo así como el idioma que se usará para 'dialogar' con el resto de equipos conectados. Siguiendo con el símil lingüístico, podemos decir que si uno de nuestros ordenadores hablase en alemán y el otro en chino, no sería posible el entendimiento: usan protocolos distintos. De ahí la necesidad de que ambos dispongan o bien del alemán, o bien del chino, o de los dos. En efecto, cada ordenador puede tener instalados varios protocolos y luego, de manera automática, ellos se ponen de acuerdo sobre cuál han de utilizar. En cualquier caso, no es bueno instalar protocolos innecesarios, basta con uno: el adecuado.

Queda clara la importancia de que todos los ordenadores dispongan del mismo protocolo, sino la comunicación sería imposible. Sin embargo, no es necesario que todos tengan los mismos servicios, sólo algunos que son indispensables y del resto, los que quieran disfrutar.

Bueno, pues veamos qué protocolos y servicios se han instalado por defecto en nuestro ordenador.

En Windows 95/98, puedes hacer doble click sobre el icono de **Red** del **Panel de Control**.

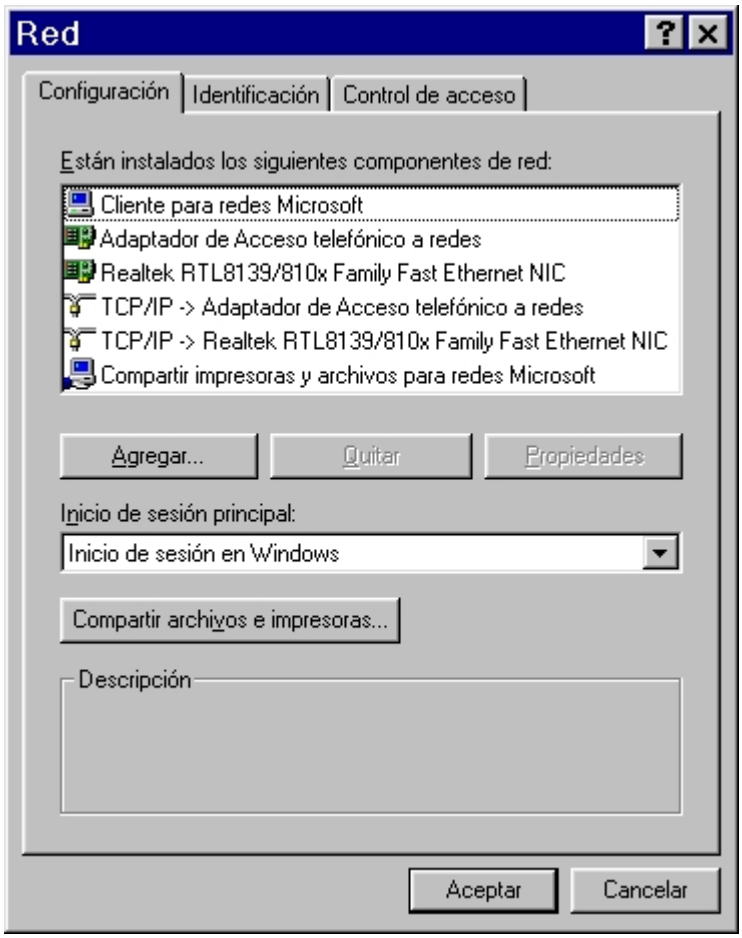
O también, desde el icono **Entorno de red**, del Escritorio, pero haciendo un click con el botón derecho del ratón y eligiendo **Propiedades** en su menú contextual.



Si dispones de Windows *Me*, puedes hacer click con el ratón sobre **Entorno de red** (*Mis sitios de red*) y luego seleccionar **Propiedades** en su menú contextual.

> *En **Windows 2000**, además, debes hacer click con el botón derecho del ratón sobre el icono **Conexión de área local** y luego elegir la opción **Propiedades.***

En cualquier caso aparecerá la ventana Red:



Seguramente, tu ventana Red no será exactamente igual que la nuestra que te mostramos en la figura, pero siempre te encontrarás aquí con la lista de componentes de red instalados en tu ordenador, que siempre se reducen a **Clientes**, **Adaptadores**, **Protocolos** y **Servicios**.

Como mínimo verás:

- Un cliente para redes Microsoft
- Uno o varios protocolos de red
- Una entrada con el modelo de la tarjeta de red (adaptador) instalada.
- Una entrada indicando el uso compartido de archivos e impresoras para redes Microsoft (servicio).

Cada uno de los elementos instalados tiene delante un pequeño icono que indica a qué tipo de componente se refiere:

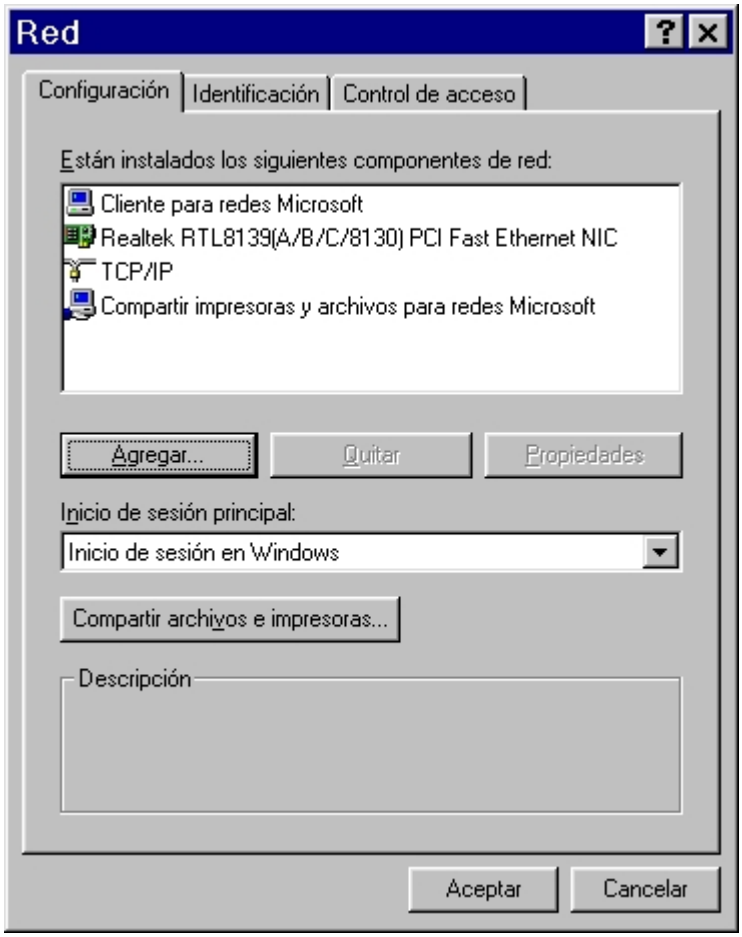
	Es un *Cliente*.
	Es un *Adaptador*.

	Es un *Protocolo*.
	Es un *Servicio*.

Cuidemos al cliente

Ya sabemos qué hace un adaptador, un protocolo y un servicio, pero ¿y un cliente?. Un cliente es un programa que activa el ordenador para que pueda conectarse a otros equipos. De ahí que sea absolutamente necesario disponer de uno instalado. Como nuestra red es para unir ordenadores con sistemas operativos de Microsoft, nos aprovecharemos del que nos da por defecto la instalación:  Cliente para redes Microsoft.

Fíjate en cómo debería quedar una instalación tipo:



Y es así como intentaremos dejar nuestros dos ordenadores. Pero vayamos con calma, pues si estamos trabajando con un equipo que tenga un módem conectado, éste ordenador (y sólo éste) debería tener dos elementos más que no han de tocarse (sino perderías la conexión telefónica y el acceso a Internet a través del módem):

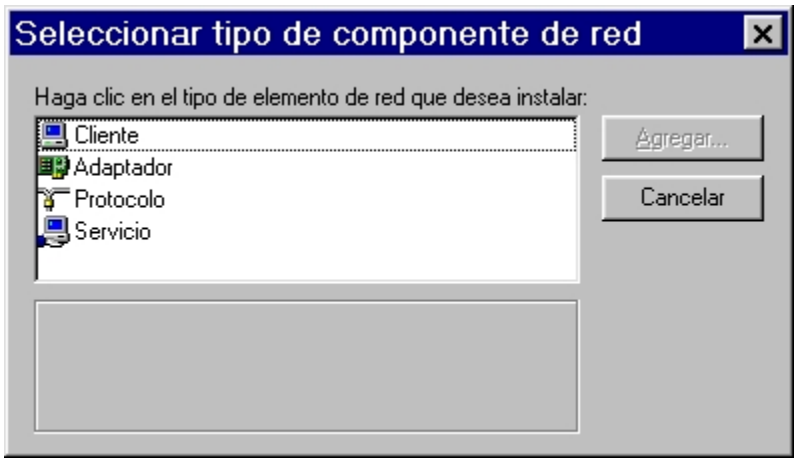
-  Adaptador de Acceso telefónico a redes
-  TCP/IP -> Adaptador de Acceso telefónico a redes

Como ya te podrás imaginar, el servicio  Compartir impresoras y archivos para redes Microsoft instalado te dará la posibilidad de compartir, en cualquier ordenador, desde una impresora hasta cualquier carpeta o archivo que desees.

Cualquier otro componente que exista vamos a eliminarlo, incluso si aparece Inicio de sesión en Microsoft Family, del que ya tendremos ocasión de hablar . ¿Qué cómo eliminarlo? Pues haciendo un click sobre él y luego sobre el botón Quitar de la ventana Red.

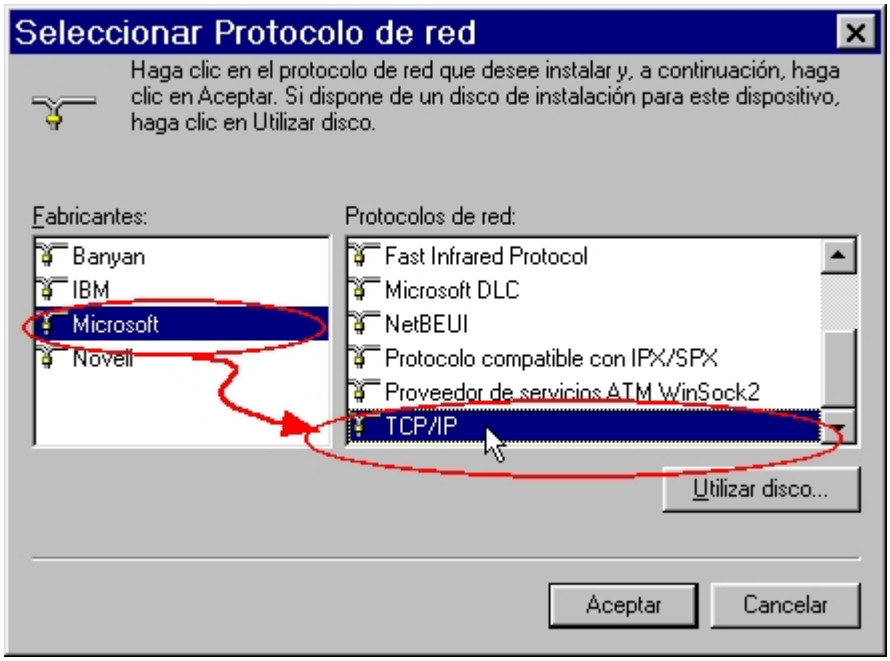
Cómo añadir componentes

¿Y si falta alguna cosa? Pues acudimos al botón Agregar... y, en la nueva ventana que aparece elegimos el tipo de elemento que deseas instalar.



Pongamos un ejemplo. Si no apareciera el protocolo TCP/IP (indispensable para conectarse a Internet) tendrías que seguir los siguientes pasos:

1. Desde Seleccionar tipo de componente de red, haz click sobre Protocolo y el botón Agregar... Se abrirá la ventana Seleccionar Protocolo de red.



2. Desde aquí, en la ventana de la izquierda eliges el fabricante Microsoft y, en la ventana de la derecha, localizas el protocolo TCP/IP. Haces click sobre él y finalmente pulsas el botón Aceptar.

Verás cómo se van incorporando a la ventana Red. Si te pide reiniciar el ordenador, pues dale ese gusto las veces que sean menester.

Entrada sólo para socios

En la pestaña Configuración de esta misma ventana, nos encontramos también con la lista desplegable Inicio de sesión principal:. Aquí se indicará qué cliente se utilizará para entrar en la red (pondremos Inicio de sesión en Windows).

Es el responsable de que, en el momento del arranque, aparezca una ventana pidiéndonos que nos identifiquemos. El mejor consejo es que, por ahora, no coloquemos ninguna contraseña en ningún sitio (pues admitiría cualquiera que introdujeses y no hay ninguna seguridad ni protección), sólo el nombre de usuario (donde se nos pida), y salir siempre pulsando **Intro**; nunca con el botón Cancelar ni con la tecla **Esc**, pues aunque el ordenador arranca sin problemas, los servicios de la red no estarían disponibles en esa sesión.

Es hora de compartir

Finalmente, y en esta misma pestaña Configuración de la ventana Red, aún nos queda la opción Compartir archivos e impresoras....

Si haces click sobre este botón, aparecerá la ventana Compartir impresoras y archivos, desde donde marcaremos las casillas correspondientes para compartir las carpetas, los discos duros, el CD-ROM (luego veremos cómo se comparten, aquí sólo habilitamos esa posibilidad) o la impresora que el ordenador tenga conectada. Ni que decir tiene que los ordenadores sin impresora no necesitan que se marque la segunda de las casillas, aunque si lo haces, no sucederá nada.

¡Identificación y afiliación, por favor!

Otro aspecto importante de la conexión a la red es la identificación del equipo, de modo que hay que darle un **nombre** a cada ordenador. Para ello acudimos a la pestañita Identificación, de la misma ventana Red:

En la ventanita Nombre de PC: le asignamos un nombre, preferiblemente corto y fácil de recordar. Puede tener hasta 15 caracteres. Es mejor no utilizar espacios, caracteres especiales o el signo de subrayado, pues aunque la mayoría están permitidos (teóricamente admite: ¡, @, #, $, %, ^, &, (,), -, _, ', {, }, ., ~), si trabajas con ordenadores bajo W2000 puede causar algún problema.

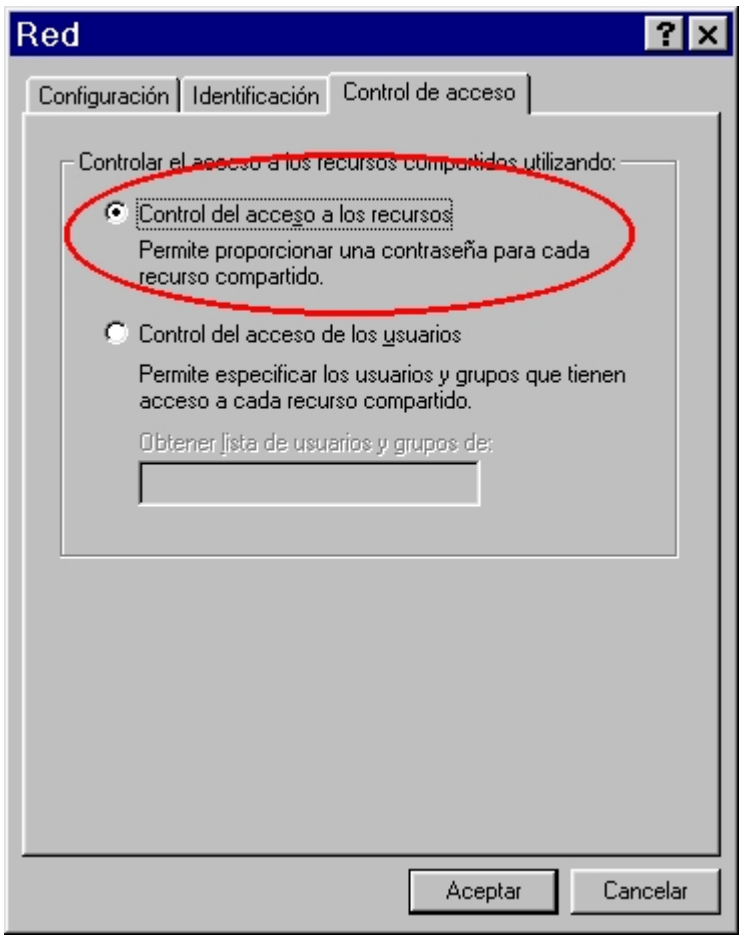
¿Qué tal PC-1, PC-2..., o el nombre del usuario (María, Juan,...) o relacionado con su ubicación (Secretaría, Dirección,...)? En cualquier caso ha de ser un nombre único en la red. Hazlo en los dos ordenadores, a uno llámalo PC-1 y al otro PC-2 (ya sé que somos poco originales; son los efectos de la telebasura).

Luego hay que crear un Grupo de trabajo:. ¿Qué es exactamente esto? Básicamente, el **grupo de trabajo** es una unidad de organización para aglutinar los equipos que queramos, pues facilita el trabajo en equipo. Además es obligatorio que cada ordenador de la red pertenezca a un grupo de trabajo. El nombre que le demos al grupo es indiferente, sólo hay que ceñirse a las mismas convenciones que el nombre del PC, pero todos los que queremos que pertenezcan al mismo grupo, han de llevar el mismo nombre. Así que pónselo a los dos ordenadores.

Ahora mismo, con sólo dos ordenadores, el concepto de grupo de trabajo es un poco difuso, pero cuando nuestra red vaya creciendo y se incorporen nuevas dependencias, el concepto de grupo *Aula-1*, *Aula-2*, *Aula-3*, *Departamentos*,... con varios ordenadores en cada uno de ellos, resultará muy útil y ordenado.

Y aunque es opcional, podemos cumplimentar el campo Descripción de su PC:, donde indicaríamos alguna característica que identifique aún más al ordenador. Esto lo verán el resto de usuarios de la red cuando se conecten a ese ordenador.

Avanzamos a la última pestañita de selección: Control de acceso. Desde aquí sólo haremos una comprobación: que esté marcada la primera de las opciones: Control del acceso a los recursos.



Configurando el protocolo

De entre todos los protocolos posibles hemos elegido **TCP/IP** *(**T**ransmision **C**ontrol **P**rotocol/**I**nternet **P**rotocol)*, ¿por qué? Pues la verdad es que si lo único que quieres es compartir unas cuantas carpetas desde los ordenadores, o el lector de DVD, o la impresora, bastaría con instalar el protocolo NetBEUI o el IPX/SPX. Pero si queremos conectarnos a Internet desde ambos ordenadores, no hay más remedio que instalar el protocolo de la Red de Redes: el TCP/IP.

En realidad no se trata de un solo protocolo, sino de un conjunto de ellos y una serie de características que sirven de base para la creación de redes WAN, e Internet lo es. Además no interfiere en el resto de funcionalidades de la red: compartir archivos, carpetas y dispositivos.

Cierto es que se podrían instalar varios protocolos juntos, dado que posteriormente los propios ordenadores utilizarán el que sea necesario en cada caso. Así, por ejemplo, para las comunicaciones entre los equipos del grupo de trabajo podrían hacerlo a través del NetBEUI, para comunicarse entre distintos grupos de trabajo podrían usar el IPX/SPX y para navegar por Internet usarían el TCP/IP.

En redes cuyos ordenadores sólo tengan Windows 98/Me/2000, la configuración de TCP/IP puede hacerse automática, pero nosotros recurriremos al trabajo manual (genera menos problemas de estabilidad y su funcionamiento es más rápido), dado que esto es un curso de aprendizaje, así que apriétate los machos y termina con el último aspecto de configuración que nos queda.

El protocolo TCP/IP exige que cada ordenador tenga un número único, la llamada **dirección IP**. Ésta es un número de 32 bits, pero escrito de forma decimal y agrupado en cuatro grupos de cifras. Pudiera ser algo así:

192.168.0.2

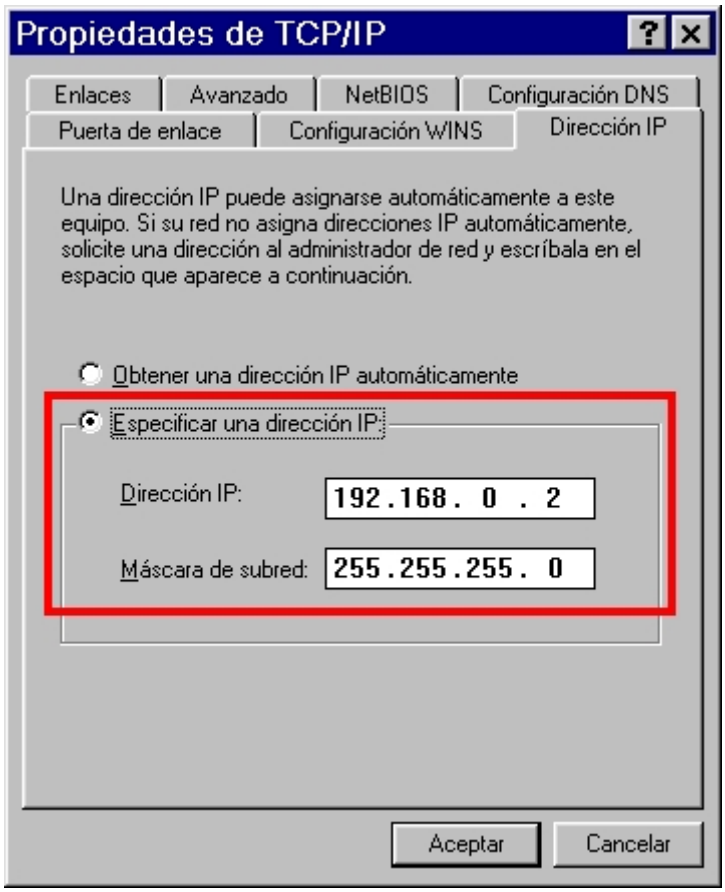
Cada grupo de números está comprendido entre 0 y 255, por lo tanto, teóricamente, son posibles las combinaciones 0.0.0.0 hasta 255.255.255.255. Lo que supone que la red podría tener hasta 4.294.967.296 ordenadores distintos.

Ya tendremos tiempo de profundizar en los aspectos teóricos de este interesante protocolo. Por ahora nuestro interés se centra en poder conectar los dos ordenadores y vamos a ello:

1. Desde la pestaña Configuración de la ventana **Red**, haz doble click sobre el protocolo TCP/IP que esté asociado a la tarjeta de red instalada TCP/IP -> Realtek RTL8139 para acceder a sus propiedades. Si tienes instalado el TCP/IP -> Adaptador de Acceso telefónico a redes , como ves, tendrás dos protocolos TCP/IP. Éste ni lo toques. Si no tienes ninguno más instalado, aparecerá, simplemente como TCP/IP, sin hacer mención al adaptador de red.

   Se abrirá el cuadro de diálogo **Propiedades de TCP/IP**.

2. Desde la pestaña Dirección IP podrás realizar la configuración. Cumplimenta los datos tal y como te los mostramos en la figura:



¿Qué hemos hecho? Pues le hemos asignado a uno de los ordenadores (al PC-1), la dirección 192.168.0.2 con una máscara de subred de 255.255.255.0 (olvídate, por ahora, de este 'palabro' tan raro. Sólo decirte que nada tiene que ver con los carnavales).

Del mismo modo, haz lo propio en el ordenador PC-2, pero ahora cambia la última de las cifras de la dirección IP a 192.168.0.3, y ¡poniendo la misma máscara de subred! (255.255.255.0). En su momento ya comprenderás por qué hemos puesto estos números a la dirección IP y a la máscara de subred.

Y ya está. Configuración de red terminada en los dos ordenadores.

Llegados a este punto, hagamos un nuevo repaso de nuestra actual situación. Si todo ha ido bien hasta ahora, hemos de tener:

- Las tarjetas de red instaladas en los ordenadores.
- Instalados los drivers de manera correcta y sin conflictos de hardware con otros dispositivos del ordenador.
- Instalados correctamente los componentes de red indispensables:
    - Cliente: Cliente para redes Microsoft
    - Adaptador: Realtek RTL8139
    - Protocolo: TCP/IP
    - Servicio: Compartir impresoras y archivos para redes Microsoft
- Cumplimentadas correctamente las propiedades de los componentes de red instalados.
- Configurado adecuadamente el protocolo TCP/IP.

Si es así, ya podrías ir pensando en cómo disfrutar de tu nueva y flamante red local, de no ser porque te falta un elemento importantísimo: el cable de conexión entre los ordenadores.

Comprobar la conexión

La primera prueba a realizar para comprobar el funcionamiento de la red es ejecutar el comando **Ping** con tu dirección IP como parámetro. Una respuesta afirmativa te asegura que tu ordenador (**host**, ese es el nombre que recibe cada ordenador de una red de este tipo) está correctamente configurado. Para ello:

1. Abre una sesión de MS-DOS y teclea el comando **ping** dirección IP del host:

```
C:\>ping 192.168.0.2

Haciendo ping a 192.168.0.2 con 32 bytes de datos:

Respuesta desde 192.168.0.2: bytes=32 tiempo<10ms TDV=128
Respuesta desde 192.168.0.2: bytes=32 tiempo<10ms TDV=128
Respuesta desde 192.168.0.2: bytes=32 tiempo<10ms TDV=128
Respuesta desde 192.168.0.2: bytes=32 tiempo<10ms TDV=128

Estadísticas de ping para 192.168.0.2:
    Paquetes: enviados = 4, Recibidos = 4, perdidos = 0 (0% loss),
Tiempos aproximados de recorrido redondo en milisegundos:
    mínimo = 0ms, máximo =  0ms, promedio =  0ms

C:\>
```

El comando ping es una herramienta de diagnóstico que envía una solicitud de eco a un equipo ubicado en una dirección IP. Nos muestra si se ha recibido una respuesta del destino y cuanto tiempo se ha tardado en recibirla.

Por defecto envía, cuatro veces, una trama o paquete de 32 bytes (una secuencia periódica de caracteres alfabéticos en mayúsculas) a una dirección IP y espera su contestación (pong). En este caso estamos enviando un ping a nuestro propio ordenador, por lo que el tiempo de respuesta del pong será mínimo (*tiempo promedio* = *0ms*) y no debe perderse ninguno de los cuatro paquetes (*0% loss*) enviados.

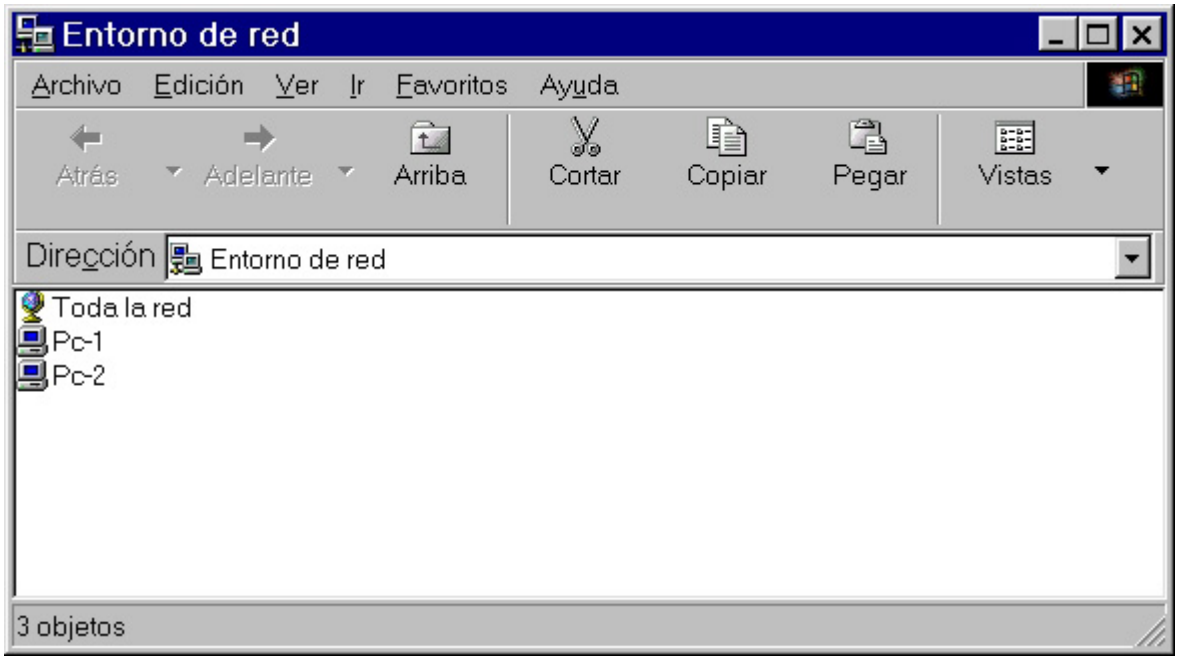
2. Ahora prueba a hacer ping al otro host de la red (ping 192.168.0.3) y comprueba su respuesta:

```
C:\>ping 192.168.0.3

Haciendo ping a 192.168.0.3 con 32 bytes de datos:

Respuesta desde 192.168.0.3: bytes=32 tiempo=1ms TDV=128
Respuesta desde 192.168.0.3: bytes=32 tiempo=1ms TDV=128
Respuesta desde 192.168.0.3: bytes=32 tiempo<10ms TDV=128
Respuesta desde 192.168.0.3: bytes=32 tiempo=1ms TDV=128

Estadísticas de ping para 192.168.0.3:
    Paquetes: enviados = 4, Recibidos = 4, perdidos = 0 (0% loss),
Tiempos aproximados de recorrido redondo en milisegundos:
    mínimo = 0ms, máximo =  1ms, promedio =  0ms
```

Si todo ha ido bien, aumentarán mucho las posibilidades de que puedas disfrutar ya de tu nueva red local.

3. Prueba a hacer doble click sobre el icono **Entorno de Red** en el Escritorio.

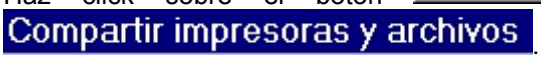
Aparecerá la ventana Entorno de red con los nombres de los ordenadores conectados a la red (Pc-1 y Pc-2).

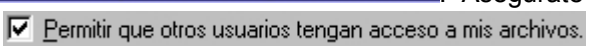


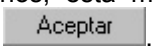
Si el **Entorno de Red** no nos indica ningún equipo conectado, puede que tengamos que activar el servicio de Compartir impresoras y archivos en cada uno de los ordenadores para que sepa que desean compartir algo en la red. Aunque lo retomaremos en el próximo capítulo, no hay más remedio que acudir a él ahora, así que cíñete a los siguientes pasos (en cada ordenador, recuerda):

a. Accede al menú contextual del icono **Entorno de red**, situado en el **Escritorio**, haciendo click con el botón derecho. Selecciona la opción **Propiedades**.

b. Haz click sobre el botón 

. Se abrirá el cuadro de diálogo 

. Asegúrate de que, al menos, está marcada la primera opción: 

y pulsa el botón 

.

Ahora ya deberías ver los ordenadores conectados a la red. Ejecuta los pasos indicados en el punto 3 anterior.

Si aún te encuentras con fallos en estas verificaciones, revisa el cable de conexión y la correcta instalación/configuración del protocolo TCP/IP.

Ahora que tenemos una idea bastante fidedigna de lo que una LAN puede hacer por nosotros, ha llegado el momento de crecer e incorporar más ordenadores a nuestra incipiente red.

Y es que llamar red (aunque lo sea) a un par de ordenadores conectados, resulta un poco peregrino. Planteémonos un reto, por ejemplo: instalar en red un aula dotada de los siguientes equipos:

- 7 ordenadores PC.
- 1 impresora láser.
- 1 impresora de chorro de tinta.
- 1 escáner.
- 1 módem de 56 Kbps.

La idea es que todos estos dispositivos puedan ser accesibles desde cualquier punto de la red, así cualquier ordenador podrá imprimir en cualquiera de las impresoras, compartir o disfrutar de carpetas de otros equipos, y lo que es mejor, acceder a Internet a través del módem.

Pero si estás pensando en utilizar el escáner desde cualquier ordenador, quítatelo de la cabeza. En una red no todo es accesible por el mero hecho de estar conectado, sólo podrás compartir los dispositivos de almacenamiento (disqueteras, discos duros, unidades lectoras/regrabadoras de CD o DVD, unidades de cinta o backup,...), las impresoras y el módem (o cualquier dispositivo similar que utilices para conectarte a otras redes: Router, adaptador RDSI, modem-cable...) y los servicios que estos incluyan (Internet, Correo electrónico, Fax,...). El uso del escáner queda relegado sólo al ordenador donde está instalado. Eso sí, nada impedirá que crees en este equipo una carpeta compartida donde ubicar las imágenes y documentos escaneados para disponer de ellos desde cualquier otro punto de la red.

El Networking

¿Necesitas acudir a una empresa especializada para llevar a cabo este montaje? No. Implementar esta instalación no es más complicado que lo que ya has hecho hasta ahora, sólo más laborioso. Tendrás que seguir familiarizándote con nuevos conceptos y recurrir a una planificación un poco más exhaustiva y previsora, pues esto de cablear una red de

comunicaciones no debería dejarse a capricho del instalador de turno. Y así, casi sin darte cuenta, estarás embarcándote en todo un proceso orientado a la conectividad de equipamiento informático; estarás practicando un nuevo deporte: el **networking**. Así se conoce a toda actividad relacionada con esta tarea.

Para llevar a cabo nuestra red local tendremos que adoptar ciertas determinaciones previas. Una de ellas es decidir cómo vamos a ubicar y distribuir espacialmente los distintos equipos, pues esto influirá en el tipo de red que utilizaremos, del medio o canal de transmisión (cable, fibra óptica, radiofrecuencia) a utilizar, del tipo de conexiones (BNC, RJ-45, ...) y del resto de materiales complementarios a adquirir (rosetas de conexión, hubs, switchs, repetidores, etc…). Hablamos de la *topología de la red*.

Topologías de redes

En esto del networking, la forma de cablear la red en función de la ubicación física que adoptarán los ordenadores, o sea, su distribución espacial, y el tipo de medio de transmisión que se utilizará. Esto define la **topología física** de la red. Y por otro lado la forma en la que los equipos van a conectarse a los medios, o sea, cómo van a comunicarse entre sí. Esto sería la llamada **topología lógica**.

La topología lógica no debe preocuparnos, pues suele ir implícita en la topología física adoptada. De ahí que genéricamente se habla solamente de la topología de una red como el patrón de conexión entre sus nodos, es decir, a la forma en la que están interconectados los distintos equipos que la forman.

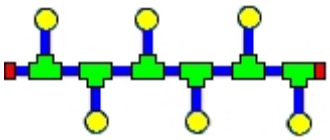
Aunque hay otras, que no son más que variantes de las propuestas aquí, las topologías físicas que se utilizan comúnmente son:

- de **bus**.
- de **anillo**.
- en **estrella**.
- en **estrella extendida**.
- **Jerárquica**.
- de **Malla**.

Veámoslas más de cerca y luego ya elegiremos la que nos parezca más apropiada.

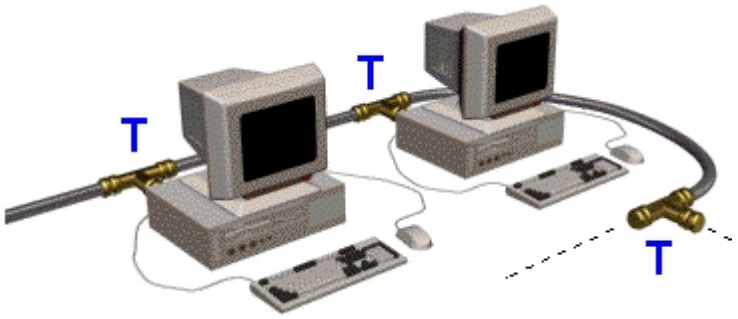
Topología de bus

La *topología de bus* consiste en un cable único al que se conectan todos los nodos de la red. Se dice, por tanto, que es un único *segmento de red*. Este tipo de red resulta muy sencilla y barata de instalar.

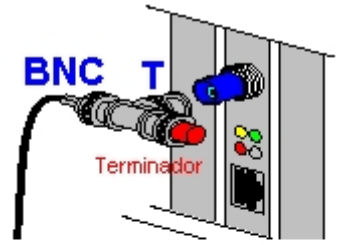


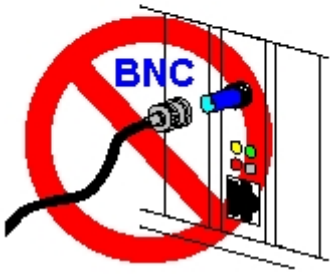
Como medio de transmisión se utiliza el cable coaxial (RG 58), con conectores BNC (***B**ritish **N**aval **C**onnector*), y con una longitud que no debería superar los 185 metros (con cable coaxial fino, *Thinnet*) o los 500 metros, si se usa cable coaxial grueso (*Thicknet*, muy caro y poco manejable) entre nodos.

Para conectar un nodo a la red, se corta el cable, se inserta un conector en forma de **T** y se conecta a la tarjeta de red del ordenador.



Al principio y al final del cable es obligado colocar un elemento terminador (una carga resistiva de la misma impedancia que el cable: 50 ohmios), nunca conectar directamente un host.





Incluso si la red estuviera formada por sólo dos ordenadores, aún así sería obligado el uso de los conectores en T y de los terminadores.

Es importante significar que, en esta topología, si el cable sufre algún corte o deterioro significativo, la red deja de funcionar en su totalidad. Lo mismo sucede si nos olvidamos de colocar cualquiera de los terminadores.

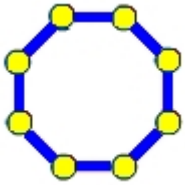
Esta topología hace posible que todos los dispositivos de la red vean todas las señales de todos los demás dispositivos. Esto representa una ventaja cuando se desea que toda la información se dirija a todos los dispositivos, pero es común que se produzcan problemas de tráfico y colisiones.

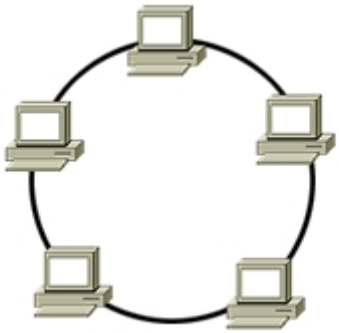
Hay que decir que, tal como vimos en el capítulo anterior, aunque el cable coaxial de 50 ohmios es un tipo de medio para redes reconocido en el estándar **TIA/EIA-568**, su uso no se recomienda para instalaciones nuevas. Es más, se prevé que este tipo de cable coaxial sea eliminado de la lista de medios aceptados para cableado de redes locales durante la próxima revisión del estándar.

Estas son razones suficientes para no apoyarnos en esta topología para la construcción de nuestra red.

Topología de anillo

La *topología de anillo* sólo es un caso especial de la topología de bus, pues cada nodo de la red se conecta con el siguiente y el último con el primero, creando un anillo cerrado donde cada nodo está conectado con sólo sus dos nodos adyacentes.



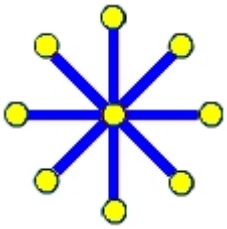


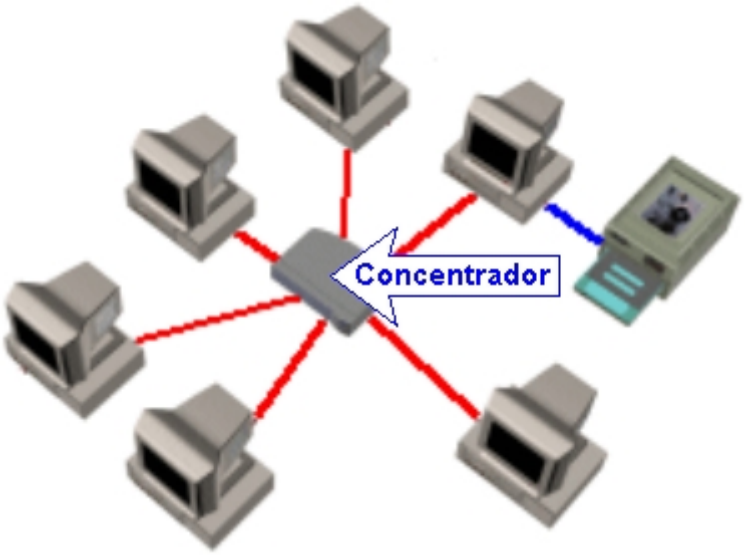
Todo lo expuesto anteriormente, en cuanto al tipo de medio de transmisión empleado, es aquí aplicable a excepción de los terminadores que no son necesarios, pero sí lo son el uso de los conectores en **T**.

Igualmente, sólo existe un único segmento de red. Para que la información pueda circular, cada host conectado debe transferir la información al host siguiente.

Topología en estrella

La *topología en estrella* conecta todos los cables con un punto central de concentración. Por lo general, este punto es un hub o un switch, que se describirán más adelante en éste y en el próximo capítulo.





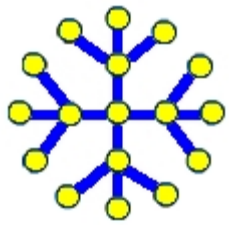
Aquí pueden emplearse todo tipo de medios de conexión: cable coaxial, de par trenzado o fibra óptica. Atendiendo al medio empleado, puede haber unas distancias de entre 185-500 metros si se emplea el cable coaxial, de 100 metros si se emplea cable de par trenzado, o de más de 2000 metros si usamos fibra óptica.

Además, si uno cualquiera de los cables de conexión se deteriorase, sólo afectaría al host conectado con él, mientras que el resto de la red funcionaría sin problemas. Eso sí, al ser una distribución centralizada, cualquier avería en el punto central de concentración supone la caída total de la red. Aquí hay varios segmentos de red, uno por cada equipo conectado.

A la vista de nuestra distribución en el aula y de que no habrá una separación mayor de 90 metros entre los ordenadores, ésta será la topología que adoptaremos. Además dejará el camino abierto para futuras ampliaciones extendiendo las conexiones en estrella.

Topología en estrella extendida

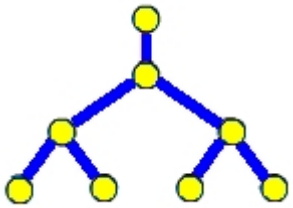
La *topología en estrella extendida* se desarrolla a partir de la topología en estrella, por lo que hereda de ella todas sus características. Esta topología enlaza estrellas individuales conectando entre sí los concentradores.



Esto, como veremos en el próximo capítulo, nos permitirá extender la longitud de la red, de manera que irá creciendo a medida que se vaya necesitando, pues sólo hay que ir incorporando nuevos concentradores que darán lugar a nuevas estrellas.

Topología jerárquica

La *topología jerárquica* o en *árbol* (o *top-down*), se desarrolla de manera muy similar a la topología en estrella extendida. Más que para conectar hosts, suele emplearse para conectar los concentradores o distribuidores entre sí de manera que, partiendo de un punto raíz, se va ramificando para llegar finalmente a los equipos de la red. Aunque más orientada a grandes entornos con exigencias en la seguridad y el control, como veremos más adelante, esta topología puede llegar a sernos útil.



Topología en malla

La *topología en malla* se utiliza cuando no puede existir absolutamente ninguna interrupción en las comunicaciones, por ejemplo, en los sistemas de control de una central nuclear o de un avión. Cada host tiene sus propias conexiones con los demás hosts. Esta es la topología en la que se sustenta la propia Internet, que tiene múltiples rutas hacia cualquier ubicación. Evidentemente, esta topología no es de nuestro interés.

En cuanto a las *topologías lógicas*, los dos tipos más comunes son **broadcast** y **transmisión de tokens**.

Topología broadcast

Por un lado, la *topología broadcast* se basa en que cada host conectado envía sus datos hacia todos los demás hosts de la red. Las estaciones no siguen ningún orden para utilizar la red, el primero que entra es el primero que se sirve. Esta es la forma en que funciona Ethernet y por esa razón será la que adoptará nuestra red, pero no es algo que debamos configurar nosotros de manera expresa, pues al utilizar adptadores de red y drivers específicos para esa tecnología, todo nos viene ya hecho.

Topología transmisión de tokens

Y por otro lado, la *transmisión de tokens* controla el acceso a la red mediante el envío de un token electrónico (algo así como el testigo que se pasan los atletas en una carrera de relevos) a cada host de forma secuencial. Cuando un host recibe el token significa que ya puede enviar datos a la red, si lo desea. Si no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir indefinidamente. Se utiliza mucho en la topología en anillo, así que no profundizaremos más en ello.

Otro aspecto muy importante en la planificación de la red es tener claro cuál será el uso que le daremos, es decir, qué tipo de datos van a circular por la red, pues en estos aspectos relacionados con el tráfico tiene mucho que decir el **ancho de banda** de nuestra instalación.

Ancho de banda

El ancho de banda es un elemento muy importante en el trabajo con redes de transmisión de datos, sin embargo suele ser un concepto bastante abstracto y difícil de entender dado que su interpretación difiere si hablamos de sistemas de transmisión de señales analógicas o de transmisión de flujos digitales.

De manera genérica, el ancho de banda (*Bandwidth*: BW) es el rango de frecuencias que se transmiten por un medio. Se define como:

BW = Frecuencia Máxima - Frecuencia Mínima

Y se expresa en hercios (Hz) o, por ser ya una unidad muy pequeña, en cualquiera de sus múltiplos:

Unidad	Abreviatura	Equivalencia
Hercio, Hertz o Hertzio	Hz	**1 Hz** = unidad fundamental de frecuencia
Kilohercio	KHz	**1 KHz** = 1.000 Hz
Megahercio	MHz	**1 MHz** = 1.000.000 Hz
Gigahercio	GHz	**1 GHz** = 1.000.000.000 Hz

Por ejemplo, el BW telefónico es de algo más de 3 KHz, pues está entre 300 Hz y 3.400 Hz; el BW de audio perceptible por el oído humano es de unos 20 KHz, pues es capaz de oir entre los 20 Hz y 20.000 Hz; y el BW de cualquier canal UHF de TV es de 7 MHz.

En sistemas digitales de transmisión de datos (y una red local lo es) se emplea el término ancho de banda como la cantidad de información que puede fluir de un lugar a otro en un período de tiempo determinado. Esta será la acepción que emplearemos durante el curso, a pesar de que técnicamente no es la más correcta, como te justificamos a continuación.

Dado que en un sistema digital la unidad básica de información es el bit y la unidad básica de tiempo es el segundo, si nos proponemos describir la cantidad de información que fluye por unidad de tiempo, tendremos las unidades *bits por segundo* (**bps**) para describir este flujo. Esta velocidad de transmisión se la denomina también *bit rate*.

Si la comunicación se produjera a la velocidad de 1 bit por 1 segundo, sería demasiado lenta. Imagínate si trataras de enviar el código ASCII correspondiente a tu nombre y dirección: ¡tardarías varios minutos! Afortunadamente, en la actualidad es posible comunicarse de modo más veloz, por lo que se ha tenido que recurrir al uso de unidades mayores:

Unidad	Abreviatura	Equivalencia
Bits por segundo	**bps**	1 **bps** = unidad fundamental del ancho de banda
Killobits por segundo	**Kbps**	1 **Kbps** = 1.000 bps
Megabits por segundo	**Mbps**	1 **Mbps** = 1.000.000 bps
Gigabits por segundo	**Gbps**	1 **Gbps** = 1.000.000.000 bps

Ahora bien, ¿qué será más correcto, expresar el ancho de banda de un canal en **Hz** o en **bps**? Ambos términos son usados para expresar una velocidad potencial de transmisión, pero como apuntábamos antes, difieren sustancialmente en lo que representan.

El *bit rate* viene a expresar la cantidad de bits que se pueden transmitir por un canal, pero para que una transmisión de datos sea fiable se utiliza siempre una codificación y/o una compresión. Esto viene a demostrar que, dado que no todos los bits de una transmisión son datos en estado puro, si utilizamos mejores tipos de codificación y/o compresión podremos obtener mejores *bit rate* efectivos. De este modo se hace posible transmitir más rápido la información sobre un mismo canal cuyo BW no ha variado.

Y por supuesto, cuanto mayor sea el BW de un medio, mayor será el *bit rate* teóricamente alcanzable.

Esta dualidad frecuencia (Hz) - bit rate (bps) hace confuso elegir una unidad para representar el ancho de banda en las transmisiones digitales, por eso podrás encontrarte con clasificaciones o referencias en ambas unidades. Si hemos de ser justos la mejor referencia en cuanto a posibilidades de una más rápida velocidad de transmisión siempre será la frecuencia que soporte el medio.

Precisamente, el concepto de categoría dentro de las normas EIA/TIA, se refiere a las diferentes velocidades que puede soportar el medio en toda su extensión, es decir, incluyendo el cableado y los accesorios de conexión, aunque para nosotros es más cómodo el uso de los bps:

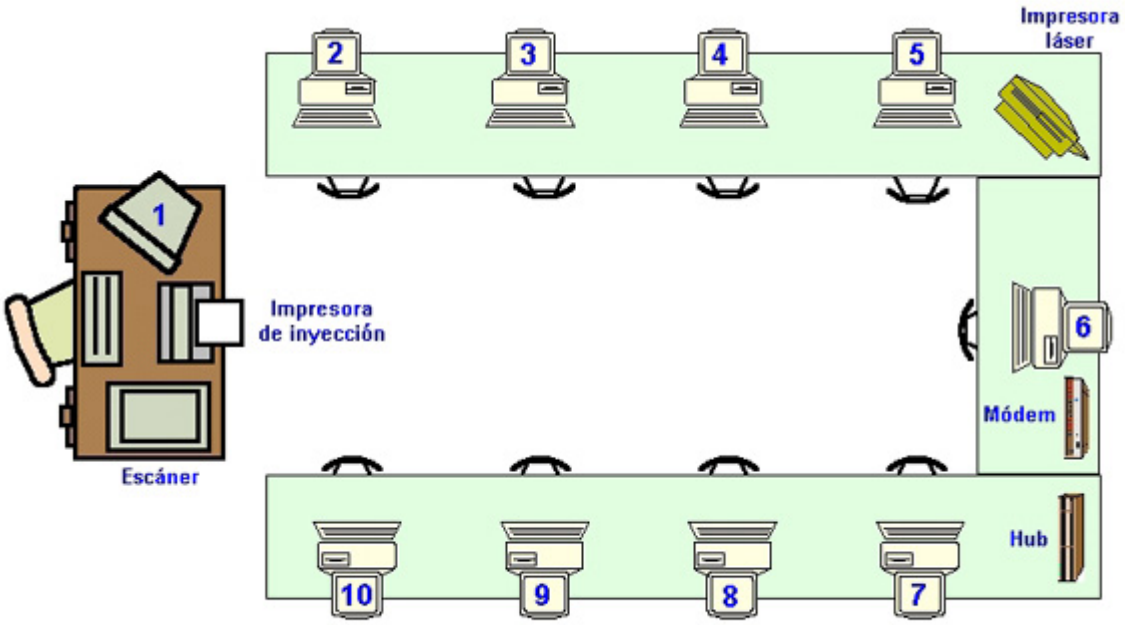
Categoría	Velocidad	
3	16 MHz	4 Mbps
4	20 MHz	16 Mbps
5	100 MHz	100 Mbps
5e	100 MHz	100 Mbps
6	250 MHz	> 100 Mbps *(sin definir)*
7	600 MHz	> 100 Mbps *(sin definir)*

Decir que un cableado es Categoría **5e** equivale a decir que soporta una velocidad de **100 MHz**, o sea que posee cables, conectores y accesorios que soportan esa frecuencia. Pero para nosotros es más significativo utilizar la segunda acepción: decir que es capaz de soportar tráficos de **100 Mbps**.

Toda esta exposición viene al propósito de ayudarnos a comprender y decidir qué categoría de cableado y accesorios es la adecuada para la red de nuestra aula. Como se supone que moveremos archivos de datos, de sonido y vídeo y pretendemos conectar a Internet a todos los equipos, está claro necesitamos el mayor ancho de banda posible y que no vamos a renunciar a nada inferior a la Categoría 5e (que es la que se utiliza hoy mayormente). Así pues, todos los materiales que adquiramos (desde las tarjetas de red hasta el más simple de los conectores) deberán ser aptos para esa categoría. Esto es algo que ya hemos hecho en nuestra primera red, así que no nos pilla de sorpresa.

Planeando la ubicación

Y antes de continuar con la relación de necesidades y sus requerimientos técnicos, hagamos un plano de situación de cómo se distribuirán los equipos de nuestra red en el aula para saber qué materiales necesitamos. Supongamos algo parecido al siguiente planteamiento:



Vemos que la impresora matricial y el escáner estarán conectados al ordenador 1. La impresora láser se conectará, por ejemplo, al ordenador 5 y el módem estará conectado al ordenador 6. En cualquiera de los casos, estos dispositivos se suponen correctamente configurados y funcionando de manera satisfactoria en su ordenador local.

La conexión de cada uno de estos periféricos es irrelevante, pero conviene tener clara su ubicación definitiva para conectarlos a su correspondiente ordenador y facilitar así su posterior configuración en la red. Una vez decidida la ubicación y su conexión no deben cambiarse, sino la configuración de acceso compartido con el resto de ordenadores se perdería.

Un nuevo elemento: el Hub

Cuando uníamos dos ordenadores todo se simplificaba enormemente, pero en el momento en que queremos disfrutar de más de dos equipos en nuestra red hemos de decidirnos por una topología física de conexión. En nuestro caso será de estrella, tal y como justificamos anteriormente.

La topología en estrella requiere utilizar un elemento centralizado que distribuya la información a todos los elementos de la red. Puede ser o bien un **hub** (o concentrador) o bien un **switch** (o conmutador). En este capítulo utilizaremos el primero; del *switch* ya tendremos ocasión de hablar.

Así pues, el hub se encargará de conectar entre sí los equipos de la red, de forma que exista un cable entre la tarjeta de red instalada en cada ordenador y cada una de las conexiones del hub.

Existen infinidad de marcas y modelos de hubs, pero a la hora de adquirir uno sólo tenemos que fijarnos en dos criterios: el **número de conexiones** y la **velocidad** que soportan.

El **número de conexiones** (o **puertos**) del hub marca el límite de dispositivos que se pueden conectar. Los encontraremos de 8, 12, 16, 24, etc...

La **velocidad** indica la tasa de transferencia a la que trabajará el concentrador. Es muy importante que coincida con la misma del resto de elementos de la red. Así, si los ordenadores están equipados con tarjetas de red de 100 Mbps, el hub debe ser estrictamente de esa misma velocidad. En el mercado existen hubs que soportan autodetección de la velocidad de cada puerto (los llamados hubs 10/100), de manera que pueden trabajar con hosts que dispongan de tarjetas de red de 10 Mbps o de 100 Mbps, indistintamente. Pero ten en cuenta que si instalas un hub de sólo 100 Mbps, ningún host equipado con tarjeta de 10 Mbps funcionará, y viceversa.

La mejor opción siempre será adquirir hubs 10/100, pues esto garantizará la máxima conectividad. Ni qué decir tiene que la tecnología del hub ha de ser compatible con el estándar Ethernet IEEE/802.3 (hoy día todos lo son).

Una solución rápida

A la vista de todo lo expuesto se desprende que montar una red de ordenadores es tan fácil como:

1. Instalar una tarjeta de red Fast Ethernet en cada ordenador, preferiblemente de 10/100 Mbps, y configurarla adecuadamente.

2. Adquirir e instalar un Hub Ethernet, también de 10/100 Mbps, con un número de puertos suficientes para poder conectar todos los equipos.

3. Construir e instalar los cables UTP Categoría 5e necesarios, con conectores RJ-45 en sus extremos, para unir cada ordenador con un puerto libre del hub. El cable deberá seguir el patrón de conexión EIA/TIA 568 (en cualquiera de sus versiones A ó B) y ha de ser normal, ¡**nunca cruzado**! No ha de superar nunca una longitud de 100 metros.

4. Y configurar los protocolos y servicios adecuados en cada uno de los equipos de la red y compartir los recursos deseados, tal y como hemos visto en el capítulo anterior.

Con estos cuatro pasos tendremos la red funcionando y a nuestra disposición.

Pero esto no es lo más profesional, pues el incremento del número de cables y la incoporación de nuevos elementos (caso del hub), aconseja que extrememos la pulcritud y el orden en esta tarea y no podremos permitir, por ejemplo, que los diez cables que unen el hub con cada ordenador permanezcan tirados por el suelo de la sala donde se implementa la LAN. Piensa que a todo este entramado de cables hay que sumar también los propios de la conexión eléctrica de cada equipo y de sus periféricos, lo que redundaría en un aumento de las posibilidades de avería y dificultaría las tareas de mantenimiento.

Por estas razones no está de más adquirir y mantener unas buenas costumbres en nuestro papel como instaladores. Para eso aparece en esta historia el **cableado estructurado**.

Cableado estructurado

Hace algunos años, cada fabricante de ordenadores, al afrontar la interconexión entre sus equipos, utilizaba sus propios tipos de cables, conectores y una topología específica que en la mayoría de los casos creaba incompatibilidad con el resto de marcas, de manera que cada vez que se precisaba cambiar de ordenador era normal tener que desechar toda la infraestructura de cableado e instalar otra nueva.

De ahí que con el tiempo se vio la necesidad de crear un sistema de cableado estandar, capaz de ser utilizado por todo tipo de ordenadores con los adaptadores precisos, que no quedase obsoleto con el cambio de ordenador, ni de sistema operativo, ni de topología, y que permitiera con facilidad el crecimiento de la red, la reubicación de los equipos y su funcionamiento con velocidades de trabajo cada vez más altas.

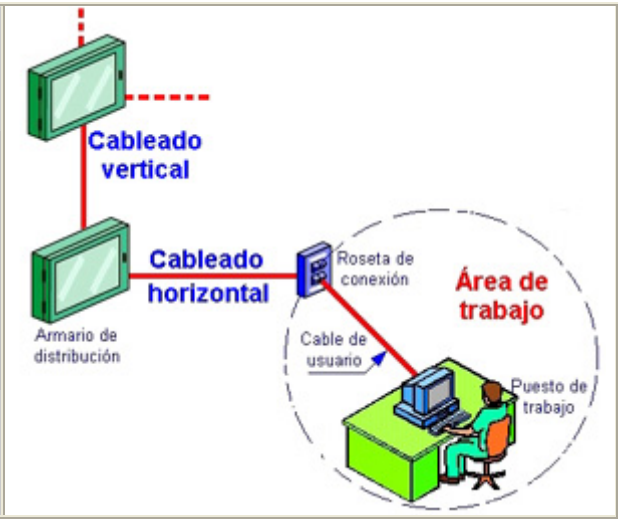
Por eso los organismos *American National Standards Institute*, *Electronics Industries Association* y el *Telecomunications Industries Association* publicaron conjuntamente el estándar **ANSI/EIA/TIA 568-B** en el que se definen un conjunto de sistemas, cables y conectores, tanto en cobre como en fibra óptica, que permite crear un **cableado estructurado** en los edificios.

Entendemos como **cableado estructurado**, al conjunto de elementos y procedimientos orientados a la distribución integral de las comunicaciones de empresa, tanto de voz como de datos o imágenes basado en la normalización y organización de todos los componentes de la instalación. Lo que traducido al idioma del vulgo viene a decir que no sólo se habla de colocar cables, sino también los equipos necesarios para que la instalación sea plenamente operativa y que no conviene hacer las cosas a nuestro buen entender, sino con cierto rigor y ateniéndonos a unas normas establecidas.

Como seguramente habrás observado, uno de los puntos más novedosos es que, en previsión del incremento de los servicios de comunicaciones, la norma contempla la distribución no sólo de datos sino también de servicios de voz (telefonía). Pero en nuestro caso, vamos a simplificarlo todo de manera que se adecue a nuestra realidad, pues en el aula de ejemplo que pretendemos instalar no tenemos que emplazar ningún servicio de voz, sólo conexiones para la red local de datos de los ordenadores. Esto reducirá costes de manera significativa ya que nos ahorrará el cableado correspondiente a los servicios de voz.

Como en nuestro caso nos enfrentamos ya a una instalación con un número considerable de cables, hemos recurrido a los criterios y orientaciones que nos da la normalización ANSI/EIA/TIA para el cableado estructurado. La norma describe los siguientes subsistemas:

- Armarios de distribución.
- Área de trabajo (work area).
- Cableado horizontal.
- Cableado vertical.



Veamos qué pasa con cada uno de ellos.

Armario de distribución

El **armario de distribución** tiene por objeto proveer un entorno controlado y seguro para los equipos de comunicaciones y la electrónica de red.

Deberán estar provistos de cerradura con llave para evitar cualquier acceso indeseado, y han de disponer en su interior de una regleta electrificada con bases *Schuko* de 16 A (amperios) con toma de tierra lateral, además de piloto indicador de la presencia de tensión. Desde aquí alimentaremos toda la electrónica activa instalada (hub, switch, router,...).

Los armarios son siempre metálicos, con guías desplazables normalizadas de 19" (*rack*) sobre las que se montan los distintos tipos de paneles, y de distintas alturas útiles que se expresan en Unidades (**U**). Cada *unidad* de altura útil equivale a 1-3/4", o sea 44, 45 m/m y deben tener un profundidad mínima de 400 m/m.

Armarios de distribución

Tamaños muy usuales son:

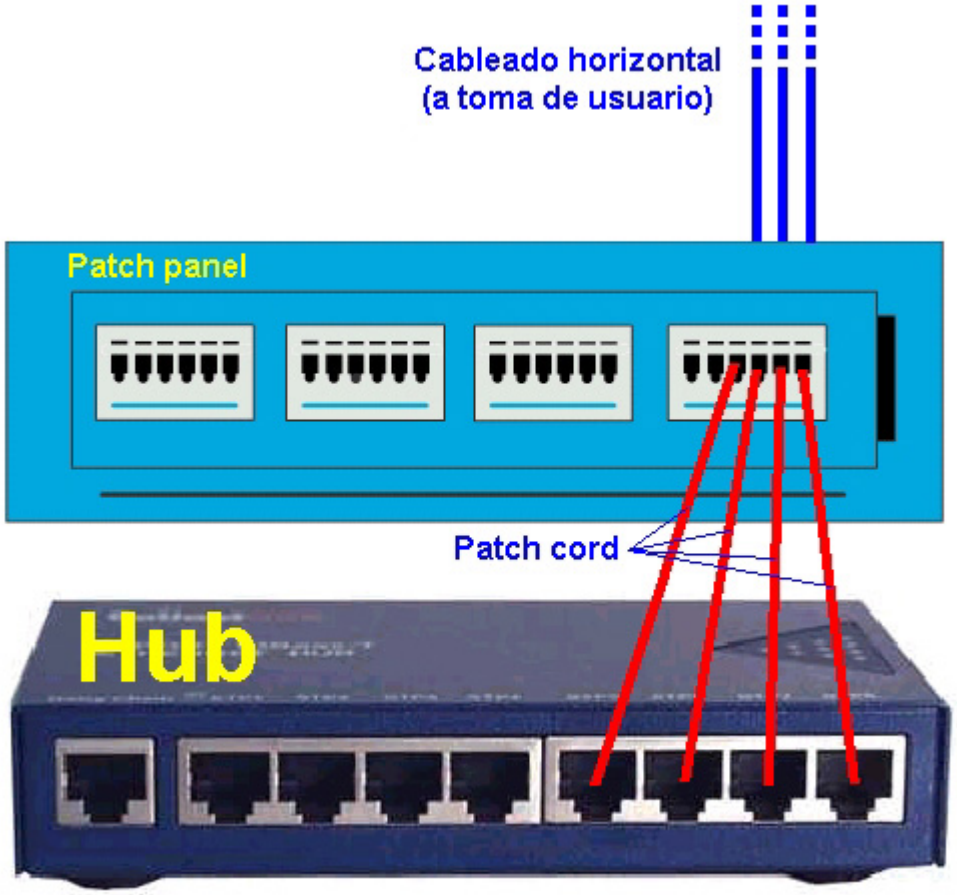
Tipo	Unidades	Altura exterior
Armario mural (o de pared)	**6 U**	400 mm
	11 U	600 mm
	14 U	750 mm
	20 U	1000 mm
Armario de pie (o de suelo)	**40 U**	2000 mm
	45 U	2200 mm

Es recomendable que dispongan de una puerta transparente para poder observar su interior, por ejemplo para controlar la actividad de los equipos electrónicos instalados, a través de sus indicadores luminosos.

¿Para qué usaremos nosotros el armario? Pues para ubicar en él nuestro hub y el panel de parcheo.

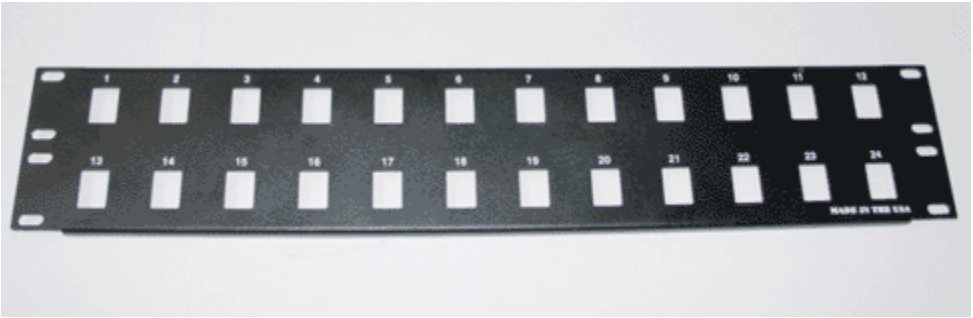
Panel de parcheo

El **panel de parcheo** (*Patch Panel*) es un elemento pasivo desde donde parten, en estrella, los cables que van hacia las tomas de usuario en las áreas de trabajo (el llamado *Cableado horizontal*, que veremos más adelante). Son un medio muy ordenado de facilitar las conexiones con los elementos activos ubicados en el armario.



En el mercado encontrarás varios tipos de paneles:

- **Paneles vacíos**, con capacidad para alojar 16, 24, 32 ó 48 conectores RJ-45 de cualquier tipo (UTP, FTP, SSTP) que se van incorporando a medida que la instalación lo requiera.



- **Paneles modulares**, formados por módulos de 24 ó 48 conectores RJ-45 ya montados sobre circuito impreso. También están disponibles en todas las versiones: UTP, FTP y SSTP.

- **Paneles para fibra óptica**, que permiten la protección, conectorización y sujección mecánica de las fibras ópticas en el rack de 19".

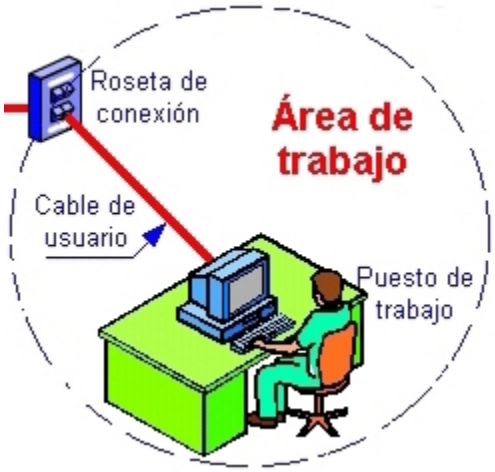
Las conexiones con la electrónica de red incorporada en el armario se realizan con unos cables de pequeña longitud, llamados cables de parcheo (*Patch cord*) o latiguillos de conexión.

Estos cables de parcheo deberán ser de la misma categoría que el resto de la instalación y con el mismo tipo de conectores que el panel de parcheo y los puertos de la electrónica que conectan (RJ-45, RJ-49, F.O.).

Área de trabajo

El **área de trabajo** comprende los elementos que permiten al usuario conectarse con los distintos servicios, desde la roseta de conexión hasta el ordenador.

El área de trabajo abarca el espacio que ha de recorrer la señal de red desde la roseta de conexión hasta la tarjeta de red ubicada en el host. Esta conexión se establece por medio del llamado **cable de usuario**, idéntico a los cables de parcheo, pero en longitudes que no deberían superar los 7 metros.



Como siempre aconsejamos, deben utilizarse cables certificados de acuerdo a la categoría del resto de la instalación. En la medida de lo posible, es preferible no utilizar aquí cables autoconstruidos, pues la mayor parte de las averías vienen por defectos en la construcción y conectorización de estos elementos.

Cableado horizontal

Se denomina **cableado horizontal** al conjunto de cables y conectores que van desde el *armario de distribución* hasta las *rosetas de conexión* (la *toma de usuario*) en el *área de trabajo*.

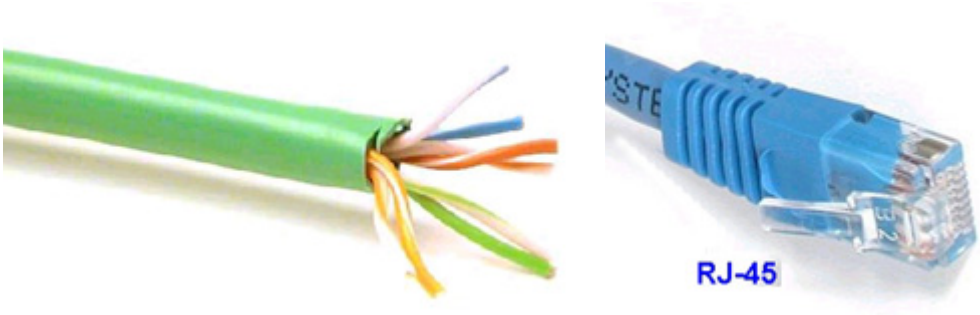
En nuestro caso, por ahora, haría referencia a los diez cables UTP que van desde el hub hasta los equipos y que aun tendríamos tirados por el suelo.

La norma ANSI/EIA/TIA 568-B sostiene que, con independencia del tipo de cable utilizado (a excepción de la fibra óptica, claro está), la distancia máxima del cableado horizontal es de 90 metros. Es decir, que entre la toma de usuario ubicada en el área de trabajo y el armario de distribución, no debe superarse nunca esa distancia.

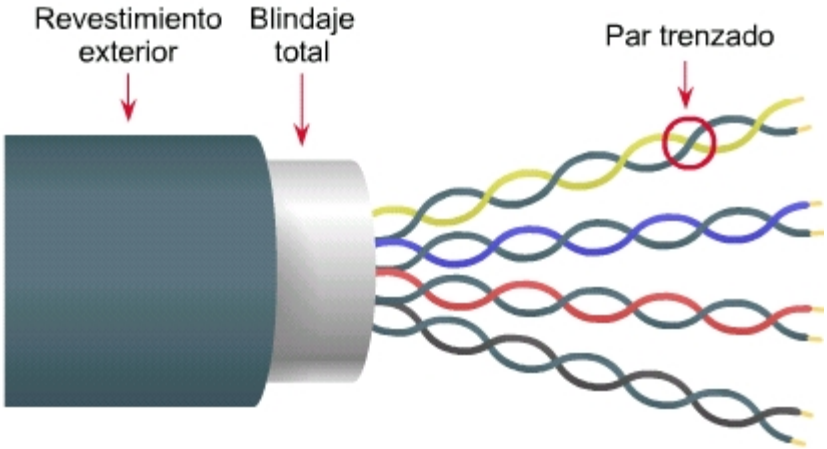
Ahora bien, al establecer la distancia máxima se hace la previsión de 10 metros adicionales para la longitud máxima combinada de cables de parcheo y cables de usuario utilizados para conectar el equipo en el área de trabajo. Así, en total, la distancia máxima desde la electrónica de reparto y distribución ubicada en el armario, y el adaptador de red ubicado en el host puede llegar a alcanzar (pero no superar) los 100 metros.

Aunque ya conocemos los tipos de cable y conectores utilizados en networking, no está de más repasarlos en este punto, dado que la norma define claramente que los medios de transmisión reconocidos para cableado horizontal son:

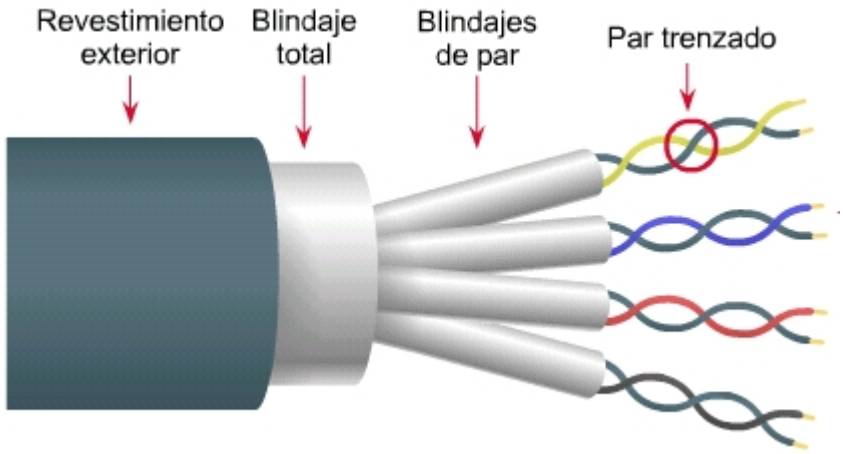
- **Cable UTP** (*Unshielded Twisted Pair*): de cobre, de par trenzado sin blindaje, de 4 pares y 100 Ohms de impedancia, con una galga de AWG 24 (0.51 mm). Es el más usado actualmente. Utiliza conectores RJ-45.



- **Cable FTP** (*Foiled Twisted Pair*): de cobre, de par trenzado apantallado mediante una lámina de aluminio, de 4 pares y 100 Ohms de impedancia, de galga AWG 24. Se está imponiendo ante las exigencias normativas acerca de las emisiones radioeléctricas. Utiliza conectores apantallados RJ-49 FTP (iguales que el RJ-45, pero con un recubrimiento metálico).

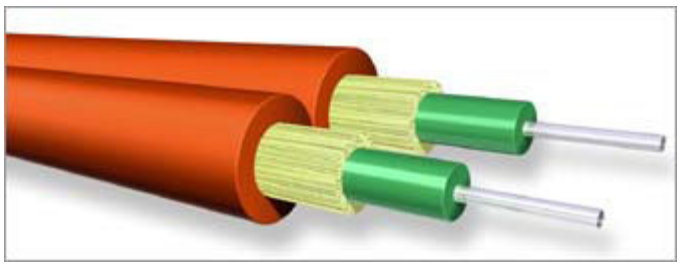


- **Cable SSTP** (*Shielded Foiled Twisted Pair*): de cobre, de 4 pares trenzados apantallados por alumninio de manera individual y apantallado todo el conjunto por una malla de cobre, y de 100 Ohms de impedancia. Su uso está indicado en entornos con fuerte polución electromagnética. Utiliza conexión RJ-49 SSTP, igual al anterior pero con mejor blindaje.

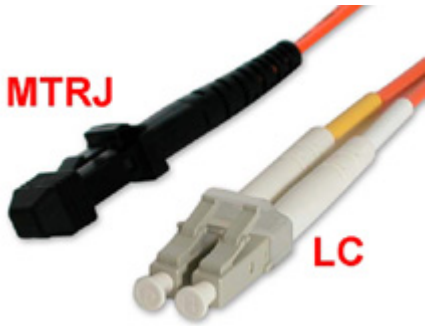


Si queremos llegar a trabajar a 100 Mbps, recuerda que todos los cables de cobre han de ser certificados, como mínimo, de **Categoría 5e** (la Categoría 5 empieza a abandonarse).

Como ves, aquí ya no se habla del cable coaxial, que aunque pueda utilizarse, no se aconseja para las instalaciones nuevas, tal y como ya te comentamos anteriormente.



- **Cable de fibra óptica** multimodo de dos fibras (62,5/125 µm, micras). Se usa en aquellos ambientes donde, por el excesivo ruido eléctrico y/o perturbaciones electromagnéticas, o por que se requiere mayor ancho de banda o porque la distancia ha de superar los 90 metros que marca la norma, hace desaconsejable el cable de cobre. Aquí se pueden utilizar varios tipos de conectores: ST, SC, LC, SMA, MTRJ, ESCOM....

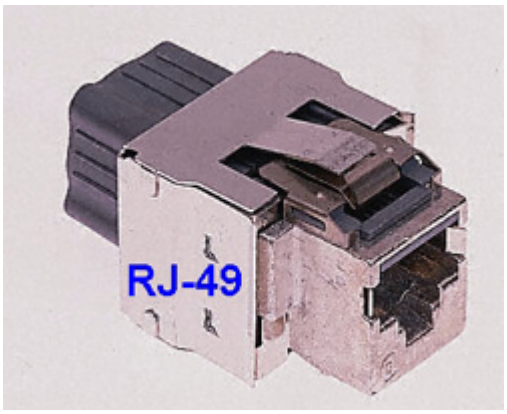


Toma de usuario

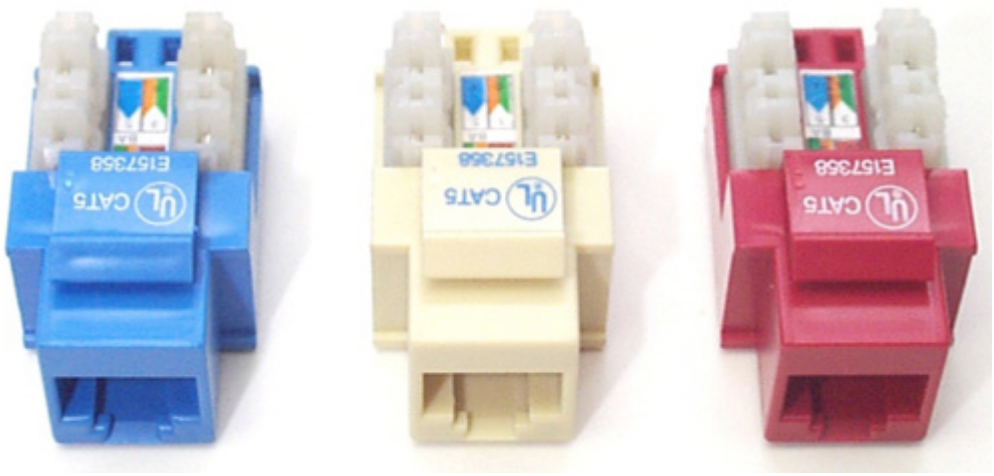
La **toma de usuario** (o **roseta de conexión**) es el punto donde termina el cableado horizontal y comienza el área de trabajo. Por lo tanto es aquí donde se conectará el cable de usuario que unirá el cableado horizontal con el host.

En este punto, la norma dice que cada puesto de trabajo debería de estar equipado, como mínimo, con dos conexiones: una para datos, con cableado UTP, de 4 pares y 100 Ohms de impedancia y conexión RJ-45, y otra para voz. Pero como ya hemos comentado al principio, prescindiremos de esta toma de voz y nos ceñiremos exclusivamente a la conexión de datos.

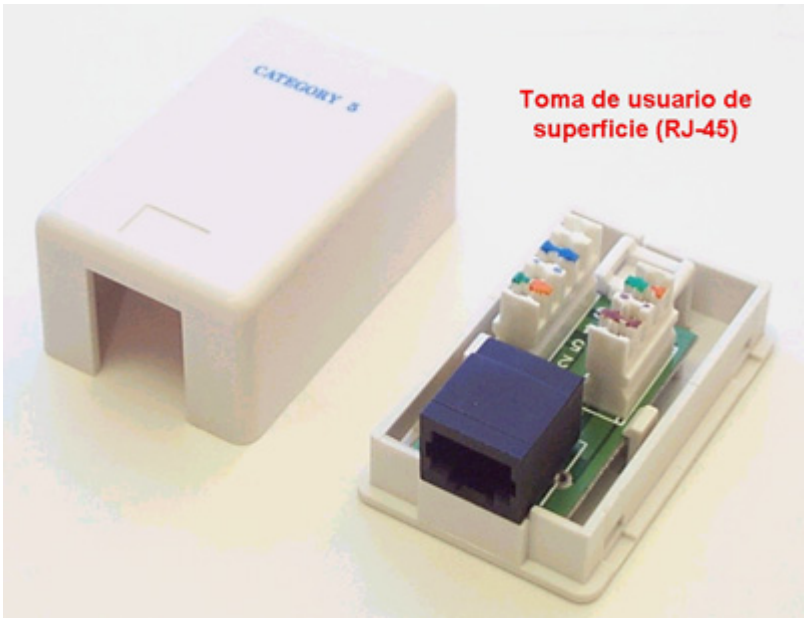
Recuerda que también aquí, estas conexiones deberán estar certificadas de acuerdo a la categoría de la instalación. Físicamente son siempre de tipo hembra y se adaptan a los requerimientos del resto de la instalación. Así podemos encontrarnos con conexiones RJ-45 (para el cable UTP sin apantallar), RJ-49 (en sus versiones FTP y SSTP, según el cable utilizado), e incluso para fibra óptica.



En el mercado encontrarás muchos modelos, colores y accesorios orientados a la instalación de estos conectores, ya sea en cajas de superficie, empotrables, o para colocar en canaletas especialmente diseñadas.



También las hay de uno o de dos conectores; de conexión recta o en ángulo de 45º, etcétera.

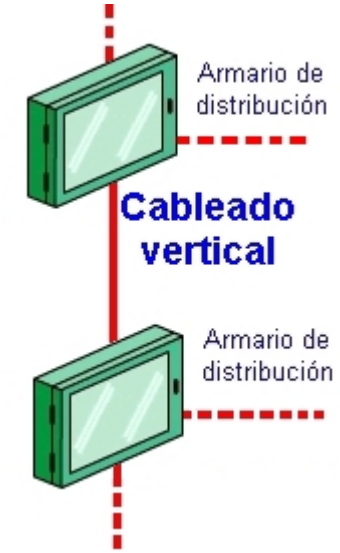


Lo mejor es que acudas a tu proveedor habitual y elijas, dentro de la Categoría 5e, el modelo que mejor se adapte a tus exigencias.

Es normal encontrarse, en muchos de los establecimientos del ramo, la misma referencia a la Categoría 5 que a la Categoría 5e. En nuestro caso, para la implementación de nuestra LAN, no va a influir en su rendimiento sea cual sea la categoría que instalemos (5 ó 5e).

Cableado vertical

Y finalmente, para completar este recorrido sobre los subsistemas del cableado estructurado, al que tendrás que enfrentarte en breve, herramienta en mano, haremos mención al **cableado vertical** (**backbone** o **cableado troncal**).



El cableado vertical se refiere a la infraestructura de cableado necesaria para unir los armarios de distribución, normalmente ubicados en las distintas plantas de un edificio, o entre los distintos edificios de un campus.

Se implementa siempre con una topología en estrella jerárquica, pues siempre se sale de un punto raíz (el armario de entrada de las comunicaciones) y se va ramificando las veces que sea menester. En algunas ocasiones se recurre también a la topología de anillo.

Los medios utilizados para el cableado vertical establecidos en la norma son:

- Cable de par trenzado **UTP**, **FTP** o **SSTP**, 4 pares de 100 Ohms y de categoría 5, siempre que la distancia entre las conexiones, incluyendo los cables de parcheo, no exceda de la distancia máxima permitida para este tipo de cable: 100 metros.
- **Fibra óptica** 62,5/125 µm, **multimodo**, si la distancia no excede de 2.000 metros.
- **Fibra óptica** 9/125 µm, **monomodo**, para distancias de hasta 3.000 metros.

Por ahora esto es todo cuanto hablaremos del cableado vertical, pues se escapa al propósito que nos planteamos de cablear la red dentro del aula. En el próximo capítulo afrontaremos el crecimiento de nuestra red hacia otras plantas del edificio y recurriremos de nuevo a este subsistema del cableado estructurado.

Con todos estos conocimientos acerca del tipo de materiales y equipos que hemos de manejar, ha llegado la hora de afrontar la puesta en práctica, pero ahora ya de un modo profesional y normalizado.

A pesar de toda la teoría que has contemplado desde el principio de este capítulo, verás que todo se hace muy sencillo.

Manos a la obra

En los siguientes apartados aprenderás a utilizar las técnicas más apropiadas y recomendadas para instalar el cableado y los elementos de conexión de nuestra LAN de aula. El cableado es una de las áreas más importantes del diseño y de la implementación de cualquier red de comunicación y hay que hacerlo con los mejores criterios de calidad, pues se espera que el cableado dure entre 10 y 15 años. Ten presente que las cualidades técnicas del cable y de las conexiones son un factor primordial en la reducción de los problemas de la red y el tiempo dedicado al diagnóstico de errores, así que no escatimes nunca aquí en calidad.

Otra lista de la compra

Comenzaremos por fijar los elementos que hay que comprar para llevar a cabo la instalación:

- 10 tarjetas de red Ethernet 10/100. Una para cada ordenador.

- 1 Armario de distribución, rack de 19", para pared y de tamaño apropiado, siempre sobredimensionado para prever posibles ampliaciones.

- 1 Hub Ethernet de 16 puertos y de 10/100 Mbps.

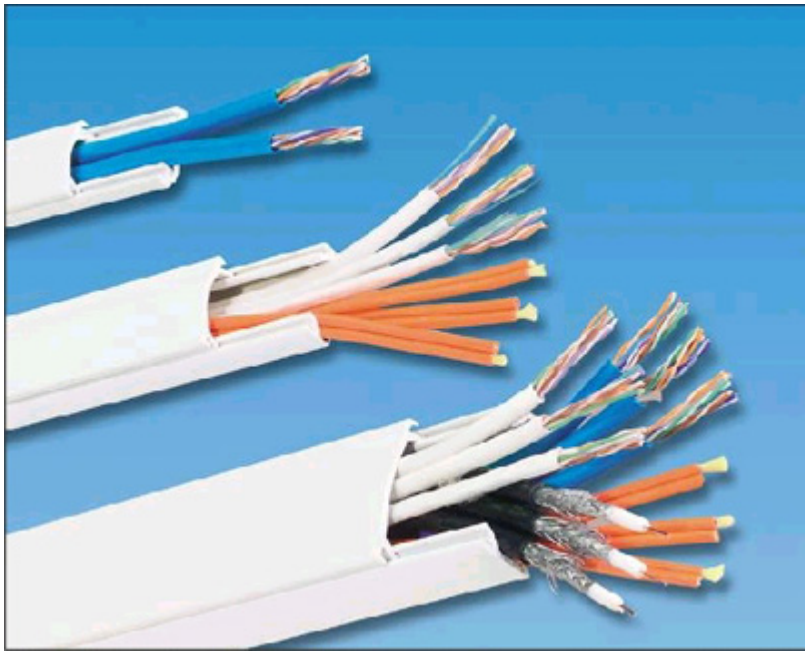
- 1 Panel de parcheo (patch panel) de 19", bien sea vacío o modular, de 16 puertos. Ten presente que si lo compras vacío, hay que adquirir aparte los conectores hembra RJ-45 para insertarlos en el panel y quizás algunos elementos mecánicos de fijación. El modular es más caro, pero viene totalmente equipado y listo para fijar en el rack y cablear.

- 10 cables de parcheo (patch cord).

- 10 rosetas de conexión individuales, de superficie y con conector RJ-45.

- Cable UTP Categoría 5e.

A lo que habrá que incorporar los medios de canalizado de los cables, a modo de canaleta de conexión y de sus elementos accesorios, pues aunque el medio más sencillo sería fijar el cable visto a la pared con algunas grapas de sujeción o similar, la estética y la seguridad de que no sufrirán tirones, desgarros o roces severos aconsejan protegerlos de la mejor manera posible. Utiliza una de anchura suficiente para que los cables no vayan muy apretados y puedas moverlos con comodidad.



Las canaletas disponen de múltiples accesorios que podrás usar para mejorar el acabado final de la instalación: tapas acodadas planas, para esquinas interiores o exteriores, terminadores, etc... Consúltalo con tu proveedor.

Haz acopio de la herramienta general necesaria: taladro eléctrico, destornillador, martillo, alicates, tijeras,... y otros elementos como tacos de sujeción para pared y tornillos. También necesitarás una nueva **herramienta de impacto** específica e indispensable para networking y que luego te explicaremos cómo usarla.

Consejos de seguridad

No descuides este importante apartado de seguridad:

- En el uso de dispositivos eléctricos, nunca trabajes con ellos conectados a la corriente eléctrica.
- Si tienes que hacer la instalación eléctrica para alimentar los ordenadores y otros equipos, hazla antes de las operaciones de cableado de la red.
- En el taladrado de paredes utiliza elementos de seguridad (anteojos, guantes,...) para evitar accidentes y desconecta todas las líneas de corriente que puedan pasar por esa zona de trabajo.

- Mide cuidadosamente antes de taladrar cualquier pared o infraestructura. Aplica la norma del 2x1: "*Medir dos veces, taladra una*".

Si ya lo tienes todo bajo control, ¿a qué esperamos?:

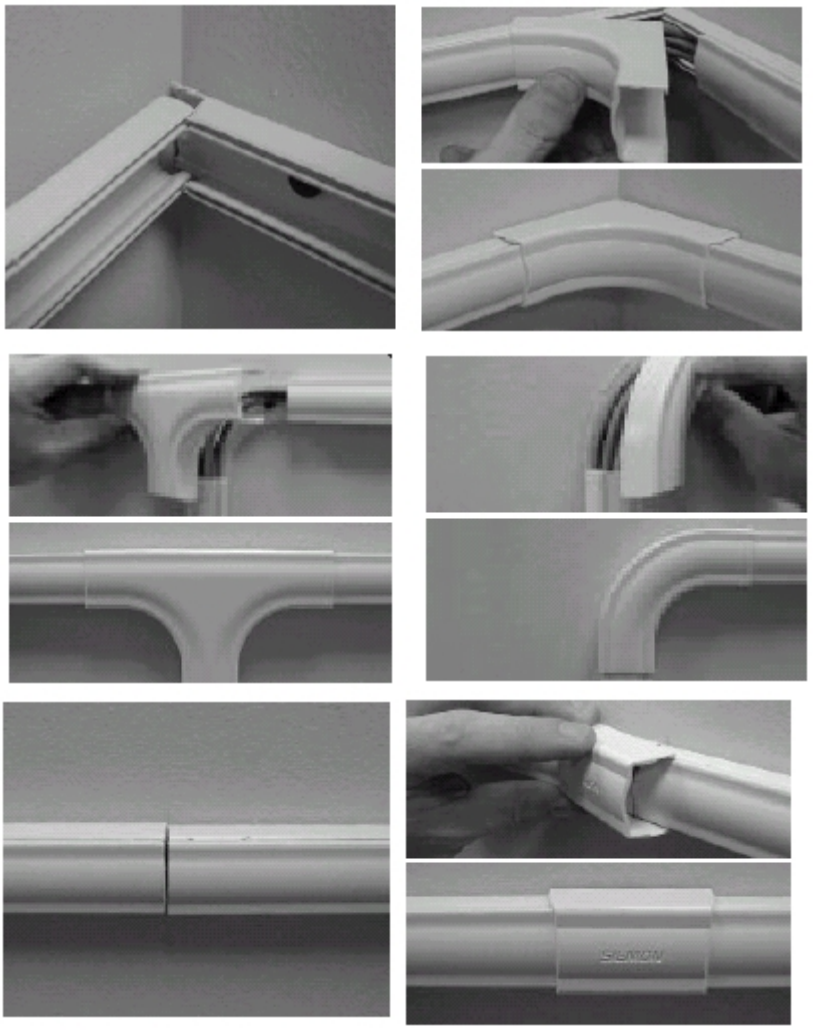
1. El primer paso será fijar a la pared el armario de distribución en el lugar del aula que elijamos. La mejor opción es ubicarlo donde se facilite la distribución en estrella de todo el cableado y las longitudes del cable sean mínimas. En nuestro caso lo ubicaremos en una esquina del aula, en el sitio que previamente habíamos destinado al hub, sobre el plano de distribución.

2. Partiendo del armario, y a una altura que la proteja de los golpes, bien con el mobiliario, equipos o con el pie, colocaremos la canaleta a lo largo de la pared, cortando previamente los tramos a la medida apropiada con una segueta o sierra de metal. En el caso de tener que realizar algún ángulo de 90º, cortaremos los extremos de las canaletas a unir en inglete para conseguir un ajuste perfecto.

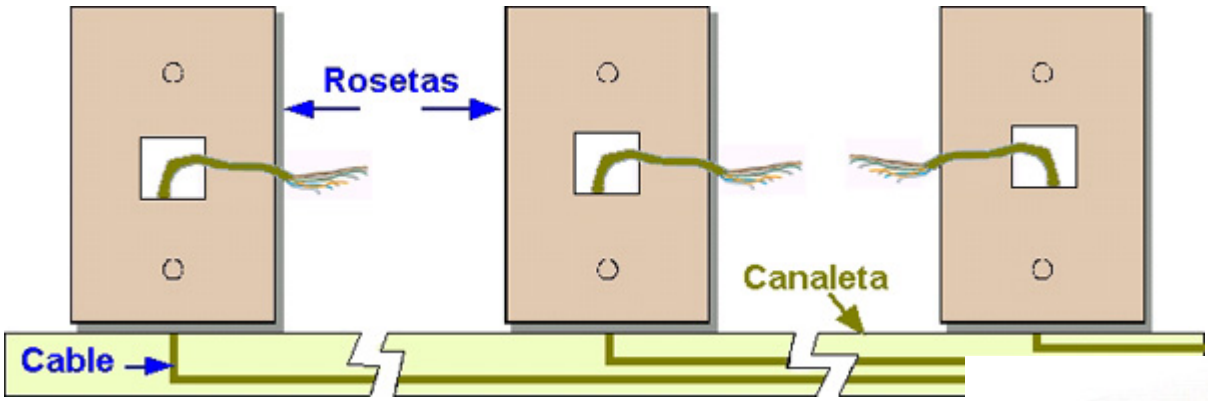
La canaleta siempre has de cortarla con la tapa puesta. De esta manera tendrá más consistencia y te evitas tener que realizar dos cortes por separado, uno para el cuerpo de la canaleta y otro para la tapa.

El uso de canaletas, aunque es muy fácil, lleva una componente artística que no todo el mundo alcanza. Hay que reconocer que no deja de ser un elemento extraño en cualquier pared, así que hay que cuidar la estética en su colocación, sin renunciar a su principal misión, y ocultarla lo suficiente para que no impacte visualmente, de manera que después facilite las tareas de instalación del cableado y su posterior mantenimiento.

Siempre queda la opción de, una vez terminada la instalación, pintarla con el mismo color de la pared. En cualquier caso no renuncies al uso de sus accesorios de terminación en esquinas interiores o exteriores, derivaciones, uniones, etcétera:



3. Fija a la pared las rosetas de conexión cerca de cada ordenador. Más adelante ya colocaremos las tomas RJ-45, por ahora sólo estamos distribuyéndolas adecuadamente. Asegúrate de que quedan bien pegadas al borde de la canaleta, para que cuando coloquemos el cable, no se vea.
4. Introduce los cables en la canaleta. Ya sabes que hay que llevar un cable desde cada roseta de conexión hasta el armario, así que mide cada uno de los tramos, previendo que hay que dejar suficiente cable en los extremos para facilitar su conexionado y ve colocándolos en la canaleta y cerrándola.



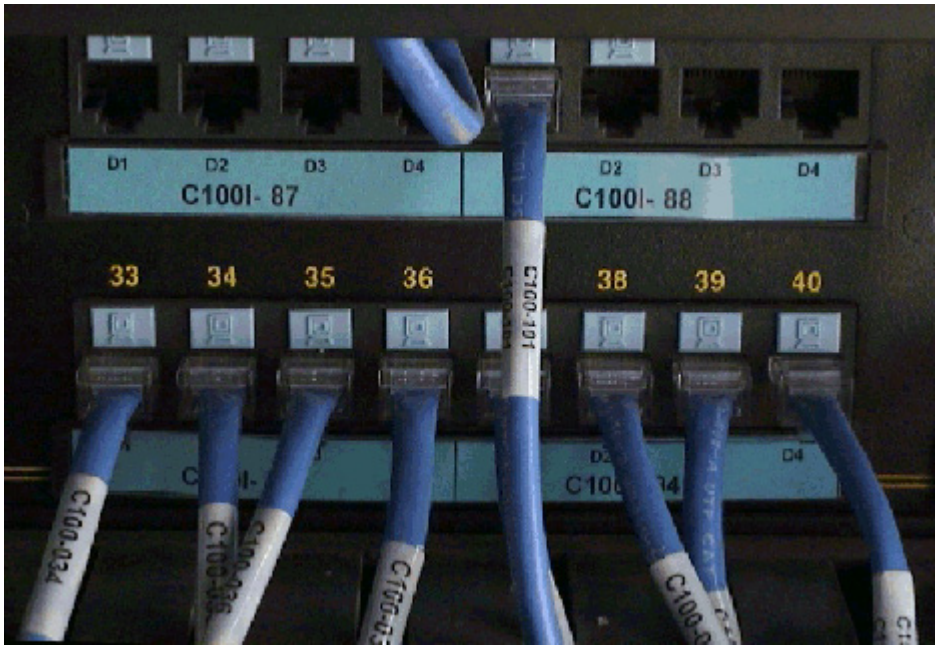
Es muy importante que en la instalación del cableado de la LAN evites acercarlos a fuentes potenciales de radiación electromagnética: motores, aparatos de aire acondicionado, fluorescentes, electrodomésticos. Si no es posible evitarlos, mantén una distancia de seguridad de al menos 1.5 metros.

Los cables UTP no pueden someterse a excesiva torsión ni tracciones fuertes (máximo 11.3 Kg), tampoco deberían doblarse en ángulo menor de

90º. Del mismo modo, evita que vayan en paralelo con los de la corriente eléctrica, pues se producirán acoplamientos que reducirán el rendimiento de la red. Si no es posible, cíñete a las siguientes indicaciones:

- La separación mínima será de 2 cm para recorridos en paralelo menores de 2.5 m.
- La separación mínima será de 4 cm para recorridos en paralelo menores de 10 m.

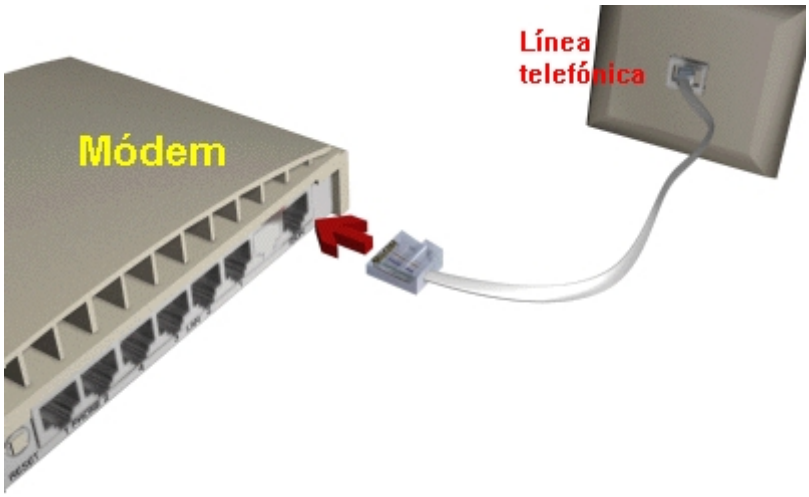
No te olvides de marcar el cable en el extremo del armario, para identificarlo inequívocamente. Piensa en el número de cables que ocuparán el armario de distribución cuando termines y lo dificultoso que sería saber de dónde es cada uno.



De igual modo, coloca la misma marca en la roseta de conexión. Procura no utilizar nombres largos o demasiado personalizados, pues el paso del tiempo puede dificultar las labores de mantenimiento. Piensa que si las llamas como '*Ordenador de Alex*', al paso de unos años es posible que sea destinado a otra persona, con el consiguiente trastorno para el técnico mantenedor.

Lo mejor es emplear números y/o letras: el número de la planta y de aula: "*A0102*", para indicar el Aula 2 de la primera planta, por ejemplo.

5. El siguiente paso será instalar los equipos dentro del armario. Conviene ubicar el panel de parcheo en la parte superior, y debajo el resto de la electrónica de red: hub y módem (en este caso). Pero no atornilles aún el panel de parcheo, pues es mejor tenerlo suelto para conectarle los cables.



Por supuesto, en el armario deberá estar prevista la conexión telefónica del módem, por lo que deberíamos tener una roseta de conexión RJ-11 (la normal de cualquier conexión telefónica), con un latiguillo de conexión.

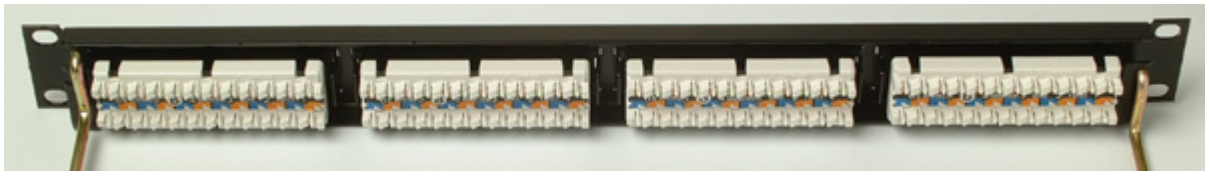
6. Ahora cablearemos las conexiones del panel de parcheo con cada uno de los cables UTP del cableado horizontal que vienen de las rosetas. Para ello:

    - Pela cada cable retirándole el revestimiento externo aproximadamente 2.5 cm, prestando atención a no cortar el aislante de los cablecillos interiores. Ten en cuenta que si pelas más de lo previsto, se reducirá la velocidad de transmisión.

    - Asegúrate de mantener el trenzado en cada par de hilos, lo máximo posible. En Categoría 5 el máximo destrenzado permisible para mantener las condiciones de propagación y apantallamiento es de 13 mm.

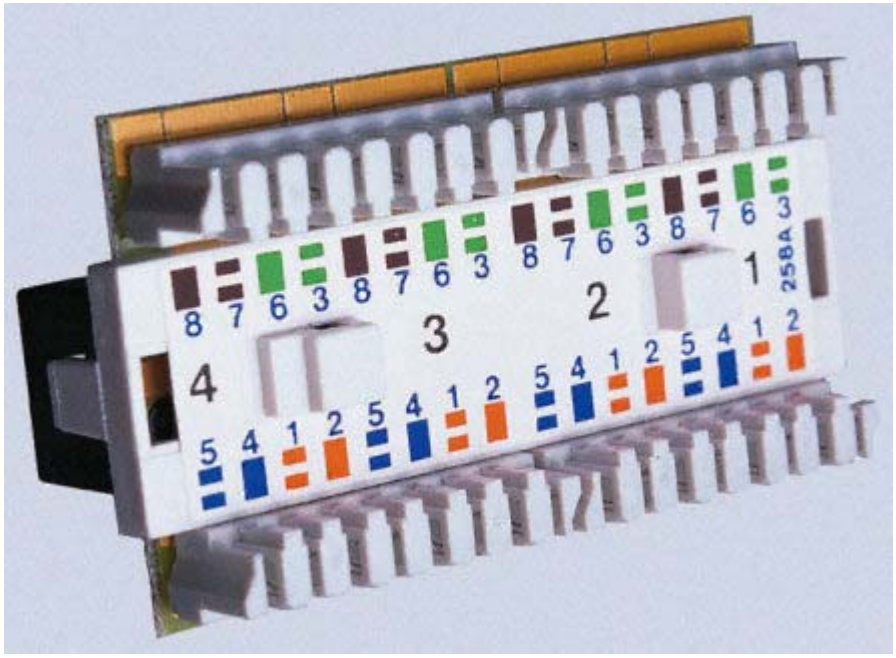
    - Si es necesario doblar el cable para poder dirigirlo, asegúrate de mantener un radio de curvatura no menor de cuatro veces su diámetro.

Dale la vuelta al panel de parcheo y observa cómo aparecen agrupadas las conexiones de los cables para cada jack RJ-45 del frontal:



Cada conexión del panel puede llevar los pines de conexión de manera diferente, pero lo más habitual es que aparezcan a modo de filas, con cada pin de conexión marcado con el color estandarizado correspondiente, listo para recibir su cable del par.

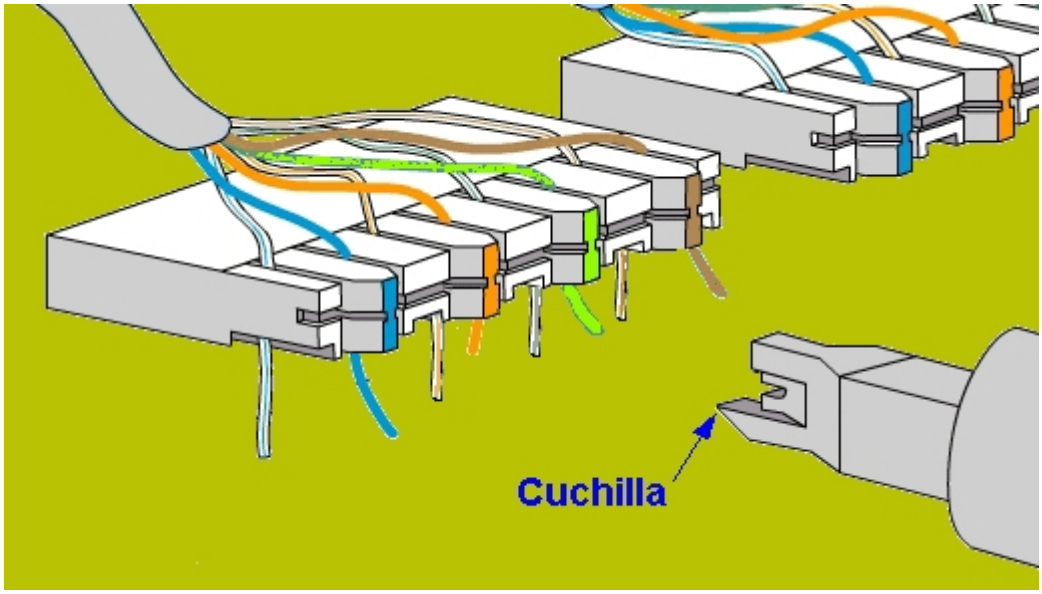
¿Qué secuencia de colores se utiliza? Pues suele usarse la norma EIA/TIA 568-A, pero puedes encontrarte con que los pines vengan marcados con la 568-B o con las dos y que luego el instalador elija la que más le conviene.



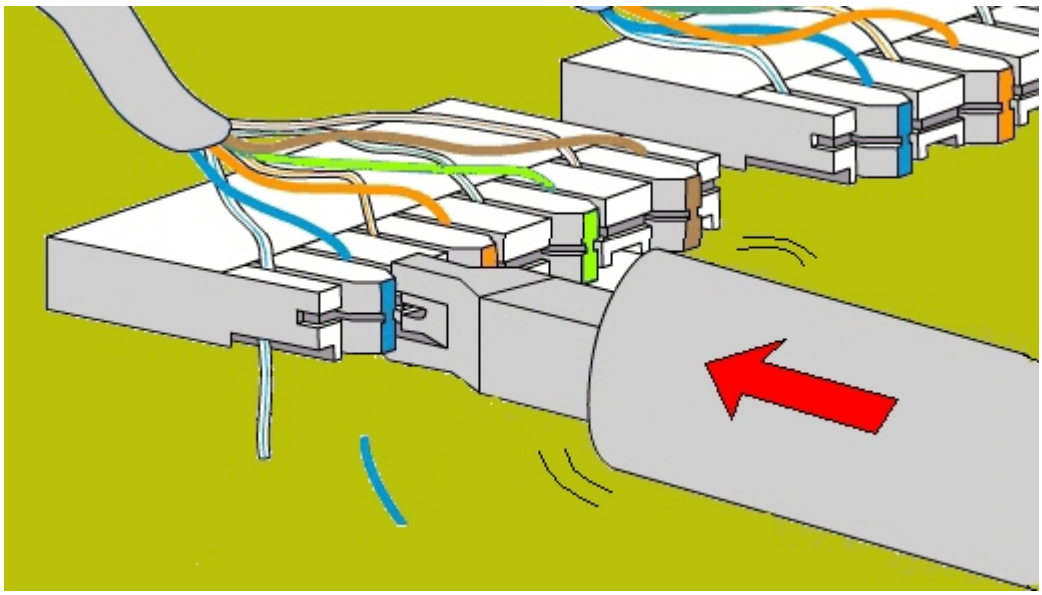
Eso sí, la secuencia de colores elegida aquí ha de coincidir exactamente con la secuencia del otro extremo del cable, es decir, la que pongamos después en el jack RJ45 de la roseta de conexión.

Así que, cualquiera que sea el modelo elegido:

- Coloca los hilos en su correspondiente pin de color. No hace falta que los peles, el propio pin de conexión está diseñado para desplazar el aislante a medida que el cable penetra. Insistimos en que es importantísimo respetar la secuencia de colores. Un error en un hilo supone que la red deje de funcionar:



- Con la **herramienta de impacto** aprieta el cablecillo contra el pin de conexión hasta que salte el resorte de la herramienta. Procura disponer la cuchilla de la herramienta hacia la parte contraria por donde entra el cable, así cortará el sobrante. De hacerlo al revés cortarás el cable directamente y tendrás que volverlo a pelar, reduciendo su longitud. No inclines la herramienta, podrías romper el lateral plástico de la conexión:



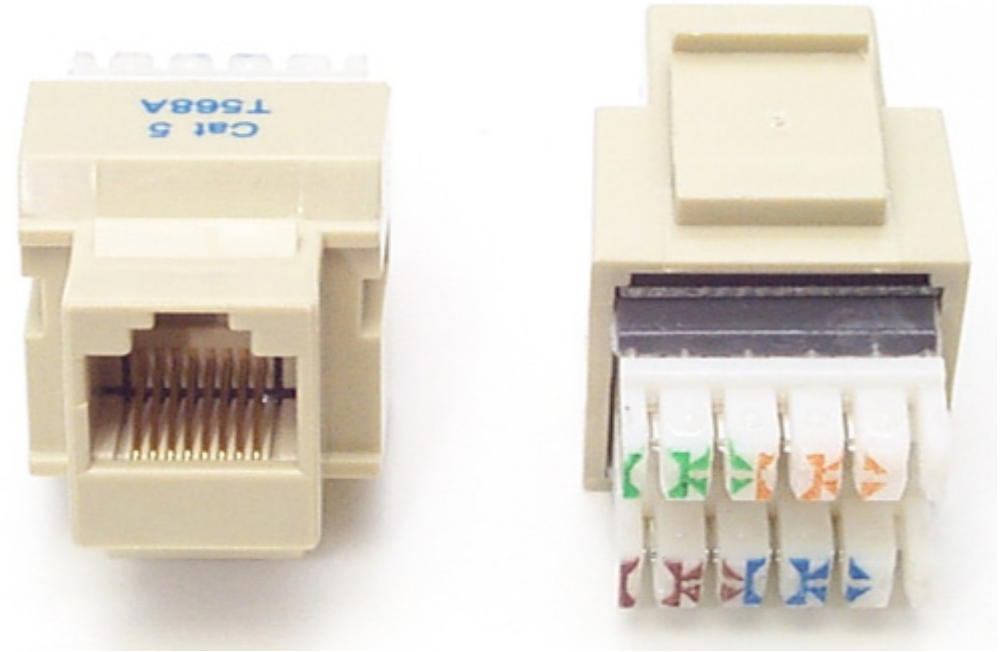
Una vez que hayas colocado todos los cables en su correspondiente conexión, es el momento de cerrar el panel de parcheo y atornillarlo de manera definitiva en el rack, recogiendo los cables de manera ordenada con algún tipo de abrazadera.

7. El siguiente paso será conectar los jacks RJ45 hembra en las rosetas que hemos distribuido por el aula. Pero antes de empezar, examina uno de cerca:

Observa que también posee una codificación de colores estándar (azul, verde, anaranjado y marrón, con su par blanco correspondiente) en sus terminales de conexión, similares a los que ya has visto en el panel de parcheo. No nos cansaremos de repetirte que han de ser estrictamente respetados en su colocación, en la misma secuencia que el panel de parcheo. Recuerda que si en un extremo del cable has usado la secuencia 568-A ó 568-B, en el otro has de utilizar la misma. A fin de cuentas, esta instalación no es más que un cable alargador similar al que ya has aprendido a crear en el Capítulo I. También aquí puedes encontrarte con jacks RJ-45 que ya tienen preimpresos los colores de una secuencia fija: 568-A, 568-B o ambas.

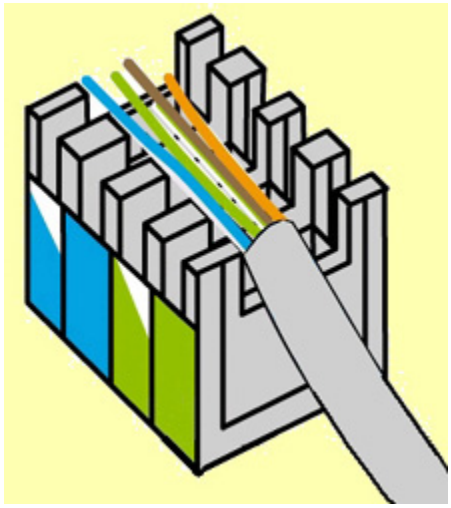
Para realizar el montaje del cable sobre un jack RJ-45 sigue las mismas indicaciones que te aconsejamos en el panel de parcheo, pero, si te es posible, deja un excedente de cable de unos 20-30 cm que quedará recogido dentro de la caja de la roseta:

- Retira el recubrimiento exterior del cable aproximadamente 2.5 cm, con la precaución

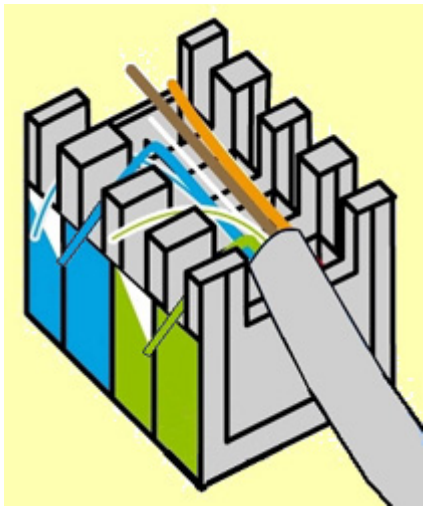


tar a los cablecillos de color internos. Procura no destrenzar los cablecillos de los pares, más de 13 mm.

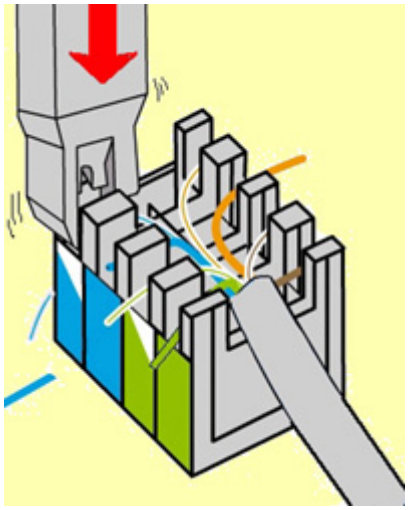
- Lo mejor es que coloques los hilos en el centro del conector para trabajar con más comodidad.



- Separa cada par de hilos trenzados y disponlos en la ranura de su color hasta que los coloques todos.



- Ahora, con la **herramienta de impacto** y al igual que hiciste antes en el panel de parcheo, coloca los hilos por presión dentro de las ranuras del jack. Una vez más, procura no inclinarla para no romper los laterales de plástico de cada pin de conexión.



- Finalmente fija el jack en la roseta, recoge el cable sobrante dentro de la misma y ciérrala para dejarla terminada.

Repite estas operaciones con el resto de rosetas de conexión que has instalado y darás por terminado el cableado horizontal.

Comprobar el cableado

Antes de continuar adelante conectando los dispositivos electrónicos, es preceptivo realizar la comprobación de que el cableado que acabamos de conectar está en perfectas condiciones de uso, pues en las labores de conectividad no basta con emplear cables, conectores, rosetas y paneles de conexión de la mejor calidad: una instalación deficiente puede impedir que la red opere al mejor nivel.

Los profesionales del networking disponen de equipamiento específico y muy caro para certificar que una red cumple con los estándares establecidos. Analizan múltiples factores relacionados con la salud de la red: ruido eléctrico, tasa de errores y colisiones, ancho de banda, reflexiones, protocolos,...

Pero nosotros no podemos ir tan lejos, bastará con disponer de un **comprobador de cables** o en su defecto, de un **polímetro**, para comprobar:

- La continuidad de cada uno de los hilos del par.
- La ausencia de cortocircuitos entre los hilos.
- La correcta asignación de los pares, en función de la norma de conexión elegida: EIA/TIA 568-A ó 568-B, en ambos extremos del cable.

Con un polímetro, la medida es un poco más latosa, pues comprobar la continuidad de los cables exige cortocircuitar los pares en un extremo y realizar la medida desde el otro.

No obstante, el comprobador es de manejo más sencillo y existen modelos muy económicos en el mercado. Nuestro consejo es que, si puedes, te hagas con uno de los que constan de dos unidades: la unidad maestra (*master*) y la unidad remota o esclava (*remote* o *slave*). Esta última puede llevar luces indicadoras o ser solamente un elemento terminador del cable, pero siempre será obligada su conexión.

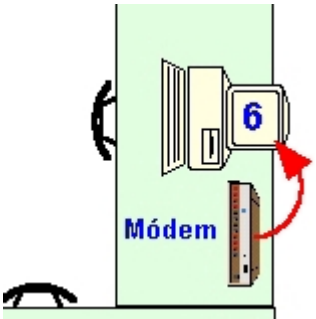
El secreto de la medida consiste en conectar en un extremo del cable la unidad *master*, la cual generará una secuencia de impulsos eléctricos que envía secuencialmente por cada par de hilos, o por cada hilo (según los modelos), de manera que sean vistos por los indicadores luminosos en ambas unidades (*master* y *remote*), o simplemente rebotados por el *terminador* y visionados, si los cables están en perfecto estado, en la unidad *master*.

Si las conexiones son correctas, todos los indicadores luminosos irán encendiéndose secuencialmente. Si por el contrario, los cables están conectados erróneamente, la secuencia de iluminación no será correlativa, o si existe una rotura del hilo la lucecita correspondiente a ese hilo no se iluminará.

Así pues:

- Conecta un latiguillo de conexión (*patch cord*) en uno de los puertos del panel de parcheo y enchúfale la unidad *master* del comprobador.
- Conecta un cable de usuario (o un latiguillo, es indiferente) en la roseta correspondiente al puerto que utilizaste en el panel de parcheo y enchúfale la unidad *remote* (o el *terminador*, según el modelo que dispongas).
- Realiza las comprobaciones según las instrucciones del comprobador de cables.

Y así sucesivamente en cada uno de los puertos y tomas de usuario que hayas instalado. Si detectas cualquier anomalía, no sigas adelante hasta que no la hayas subsanado totalmente. Nunca acumules los problemas, sino que ve resolviéndolos a medida que se presentan y no avances hasta que todo funcione perfectamente.



Conectando los equipos del armario

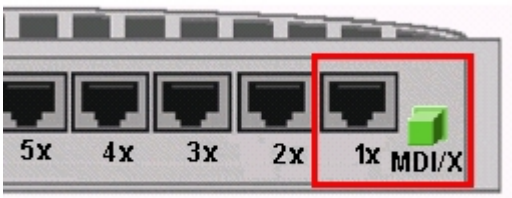
Una vez que todo está comprobado, es hora de conectar la electrónica del armario. Por un lado está la conexión del hub de distribución y por otro, la conexión del módem.

El **módem** no es un elemento relacionado con la propia electrónica de la red, ya que se conecta de manera individual a un ordenador y su uso, como elemento de conexión a la red telefónica para tener acceso a Internet y a todos sus servicios, es un aliciente importante para una LAN, dado que podría compartirse esa conexión para que el resto de ordenadores accedan simultáneamente a la Red de Redes. Sólo lo hemos incluido en el armario por razones de seguridad y limpieza de la instalación. En cualquier caso, damos por supuesto que ya está perfectamente conectado y configurado en uno de los ordenadores. Por razones de seguimiento del curso, vamos a suponer que se encuentra conectado al ordenador número 6 del aula, pues es el más cercano, pero pudiera estar conectado en cualquier otro.

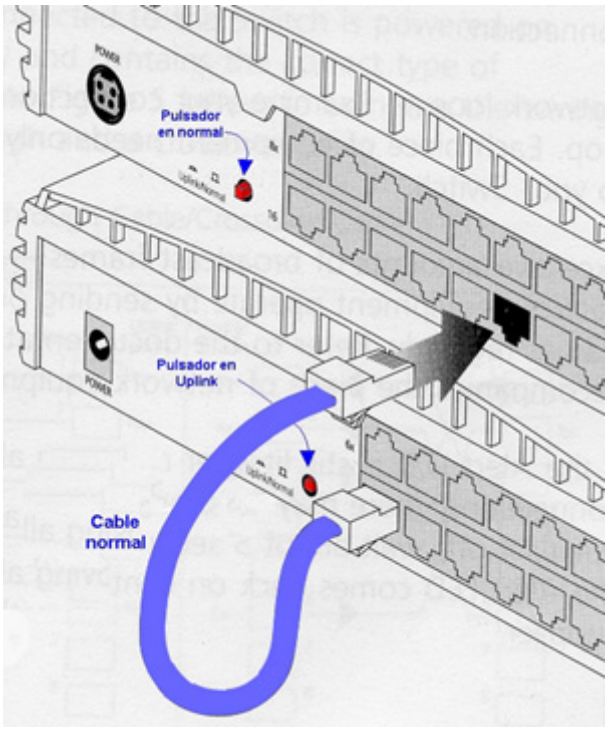
Para la conexión del **hub**, comenzaremos por conectarlo a la corriente eléctrica a través de su alimentador. Luego iremos uniendo cada puerto del mismo con cada una de las tomas del panel de parcheo, usando los latiguillos de conexión. Así de simple.

Y eso es porque los puertos de conexión de un hub, que es un equipo DCE, están preparados para ser conectados directamente a un equipo DTE (un ordenador, por ejemplo) dado que ya tiene los pines de las conexiones cruzados: Rx de DCE con Tx de DTE y viceversa. Por esta razón se utilizan siempre cables normales, y así los hemos construido en nuestro cableado horizontal (recuerda cuánto te insistimos en respetar el mismo estándar de conexión en ambos extremos del cable: EIA/TIA 568-A o EIA/TIA 568-B, indistintamente).

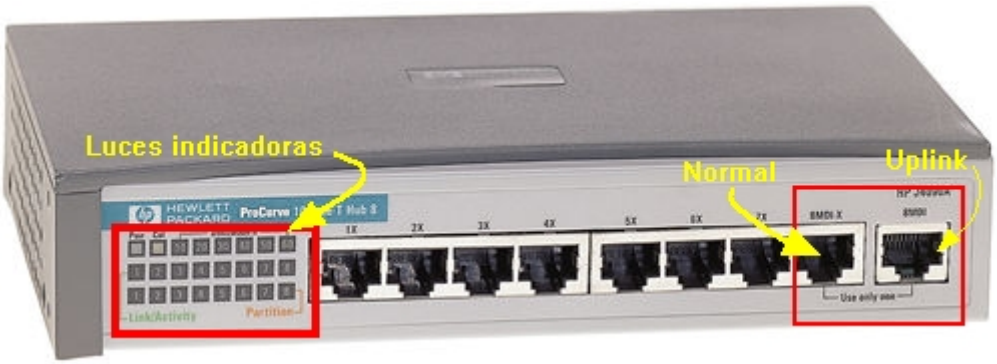
Pero si se quieren conectar en cascada varios hubs, no podríamos utilizar estos mismos cables, ya que al ser equipos del mismo tipo (DCE) habría que acudir a cables cruzados. Por esta razón los hubs disponen siempre de un puerto (normalmente el primero o el último) con capacidad para conmutar por medio de un botón (marcado como MDI/X o *Uplink/Normal*, según modelos) que intercambia el cableado interno del puerto (convirtiéndolo en cruzado) para poder seguir empleando un cable normal.



El puerto 1 puede ser normal o cruzado. Depende del botón MDI/X



Otros modelos de hub no llevan el botón de conmutación, sino que incorporan una conexión secundaria al puerto, de manera que se conecta el cable en una u otra toma, según se desee el tipo de conexión a utilizar (Normal o Uplink), pero nunca se pueden usar las dos conexiones.



Recuerda siempre que cuando conectes un ordenador, el puerto ha de estar en modo normal. Si conectas, por ejemplo, otro hub o un switch, el puerto ha de estar en modo uplink. De no hacerlo así, el equipo conectado no sería reconocido en la red.

Es conveniente hacer coincidir el número del puesto de trabajo con el número del puerto del hub. Así, conectaremos el puesto número 1 con el puerto 1 del hub, el puesto 2 con el puerto 2, etcétera. Esta disposición nos ayudará a identificar mejor cualquier anomalía que se produzca en el futuro, pues interpretando las luces frontales del hub tendremos información instantánea del comportamiento de la red: si un ordenador está o no conectado, si está enviando información, si está conectado a 10 ó 100 Mbps, etc... Todo dependerá del modelo de hub que hayas instalado.

Configura cada host

Ya sólo te queda configurar adecuadamente cada uno de los ordenadores de la red. Recuerda los pasos seguidos en el capítulo 1:

1. Asegúrate de instalar el protocolo TCP/IP.

2. Configura los parámetros de acuerdo a la tabla siguiente:

Equipo	Dirección IP	Máscara de Subred	Nombre del PC	Grupo de trabajo
Ordenador 1	192.168.0.2	255.255.255.0	PC-1	Aula-1
Ordenador 2	192.168.0.3	255.255.255.0	PC-2	Aula-1
Ordenador 3	192.168.0.4	255.255.255.0	PC-3	Aula-1
Ordenador 4	192.168.0.5	255.255.255.0	PC-4	Aula-1
Ordenador 5	192.168.0.6	255.255.255.0	PC-5	Aula-1
Ordenador 6	192.168.0.7	255.255.255.0	PC-6	Aula-1
Ordenador 7	192.168.0.8	255.255.255.0	PC-7	Aula-1
Ordenador 8	192.168.0.9	255.255.255.0	PC-8	Aula-1
Ordenador 9	192.168.0.10	255.255.255.0	PC-9	Aula-1
Ordenador 10	192.168.0.11	255.255.255.0	PC-10	Aula-1

Ya suponemos que te estarás preguntando por qué utilizamos estos números tan raros o por qué no hemos empezado por la dirección IP 192.168.0.1. En el próximo capítulo te lo explicaremos.

3. Comparte algún recurso o carpeta en cada uno de los ordenadores.

4. Instala las impresoras en los ordenadores, tanto en los locales (la impresora láser es local al ordenador 5, y la impresora de chorro de tinta lo es al ordenador 1) como en los del resto de la red. Imprime una hoja de prueba desde cada ordenador que instales.

5. Y acude al **Entorno de red** para comprobar que los equipos se encuentran disponibles y son reconocidos por la red.

¡A ver!: ¡La documentación!

En una instalación de red tan sencilla como la que acabamos de realizar, parece que no es necesario saber más de lo que se ve a simple vista. Anteriormente, en este mismo capítulo, hemos hecho mención a la importancia de nombrar los distintos cables que llegan al panel de parcheo, pero esto no es suficiente, dado que es muy importante dejar bien documentados los pasos que realizamos en la implementación de la red, los inconvenientes encontrados, las soluciones aportadas y sobre todo, los aspectos técnicos y lógicos de toda la instalación:

- Modelos y características técnicas de la electrónica instalada: tarjetas de red, hub, switch,...
- Características físicas y eléctricas de todo el cableado y elementos de conectorización empleados.
- Plano de situación y distribución de los elementos de red, incluyendo plano del edificio con indicación de los recorridos, situación de las tomas de usuario, armario de conexión y todo elemento que influya sobre el funcionamiento de la red.
- Configuraciones de los aspectos lógicos de la red: topologías, protocolos, direcciones IP, restricciones de acceso, etc...
- Establecer una nomenclatura racional para la señalización y etiquetado de los componentes utilizados: cables, paneles, tomas de usuario,...

En definitiva, toda aquella información que facilite las tareas de mantenimiento, tanto al administrador o técnico actual como a los futuros administradores/técnicos que puedan sustituirnos.

Sería interesante que toda esta información estuviera realizada de la forma más clara posible y que estuviera disponible tanto en papel como en formato electrónico.

Guía rápida para la resolución de problemas

Guía rápida para la resolución de problemas		
PROBLEMA	**POSIBLE CAUSA**	**SOLUCIÓN**
No hay conexión de red	**Cableado**	• Hub o Switch averiado. Revisar la alimentación. Sustituir. • Conector mal hecho. Cortar y hacer otro (no reprar). • Algún cable está suelto o defectuoso. Sustituir.
	Tarjeta de red	• Averiada. Sustituir. • Mal instalada o configurada. Revisar conflictos.
	Protocolo de red	• Protocolo no instalado de manera adecuada. • Revisar nombre y/o grupo de trabajo. Posible duplicación de nombre.
	Dirección IP	• Dirección no válida. Rango equivocado. Revisar parámetros de configuración. • Dirección repetida. Ya existe en otro host de la red. Cambiar.
Un equipo no aparece en la red	**No comparte recursos**	• Configuración *Compartir archivos e impresoras*. Revisar • Compartir algún recurso: hardware o software.
No se puede acceder a la red	**Problemas con NetBIOS**	• Desinstalar la tarjeta y reinstalarla de nuevo.

Conclusión

Tras descubrir el mundo del networking y contemplar el abanico de posibilidades para disponer físicamente los equipos de una red local: su topología, has planteado sobre el papel tu primera red de envergadura: un aula completa de diez ordenadores.

Esto te llevó a aprender la disciplina que exige la disposición del cableado y la necesidad de acogerse a los estándares normalizados para afrontar la implementación de redes de comunicación.

Links de interés
http://www.ansi.org/
http://www.tiaonline.org/
http://www.eia.org/
http://www.siemon.com/Literature/product-specsheets/

No nos hemos olvidado de que en el capítulo anterior has configurado unas direcciones IP en los diez ordenadores del aula que empezaban en la dirección 192.168.0.2 con una máscara de subred 255.255.255.0 e iba aumentando la última de estas cifras (192.168.0.3,...) en cada ordenador, y habíamos quedado en explicarte el porqué de estos números. Además aún tenemos pendiente la tarea de conseguir que todos los ordenadores de la red fueran capaces de acceder, de manera simultanea, a Internet, aprovechando que uno de los equipos, el número 6, tenía ya una supuesta conexión activa a través de un módem.

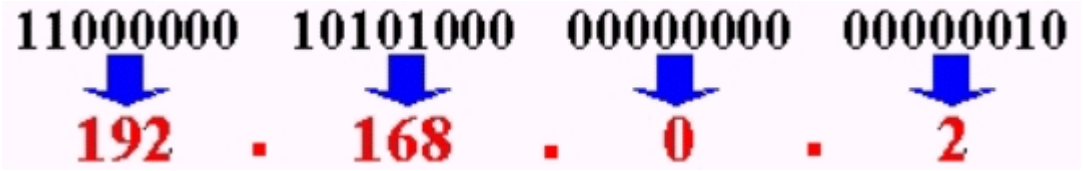
Yendo por partes, vamos a empezar por intentar dejar claro de una vez lo de los números IP, y permítenos que en algunas cosas seamos reiterativos (o pelmas, llámalo como quieras).

El secreto de la IP

En una red que utilice el protocolo TCP/IP, los ordenadores se identifican mediante un número único que se denomina dirección IP, y una dirección IP está formada por 32 bits, que se agrupan en 4 bytes (octetos, grupos de 8 bits). Por ejemplo:

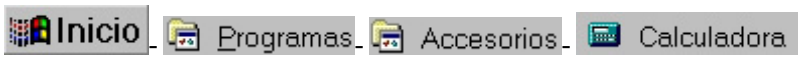
11000000 10101000 00000000 00000010

Ten presente que estamos trabajando con el sistema binario (el preferido por los ordenadores), nada amigable para los humanos, de ahí que, por razones prácticas, y para disminuir la tasa de errores de trascripción, mejor utilizamos las direcciones IP en formato decimal, pasando el valor binario de cada octeto al sistema decimal y separándolo con un punto. Así, la dirección IP anterior sería:

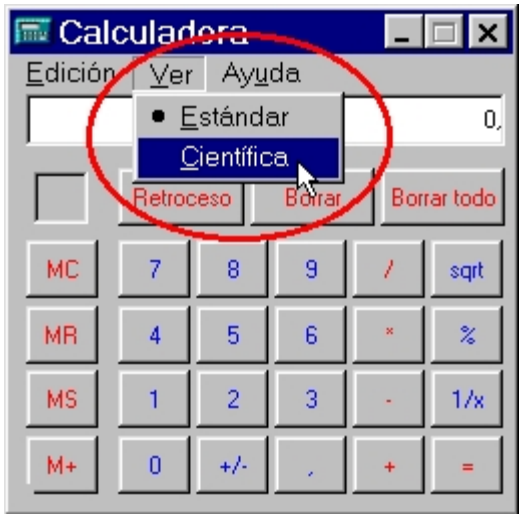


Lo cual nos resulta más fácil de manejar y recordar.

¿Que no sabes cómo pasar una cantidad binaria a decimal y viceversa? Utiliza la **Calculadora** científica que incluye Windows, desde:



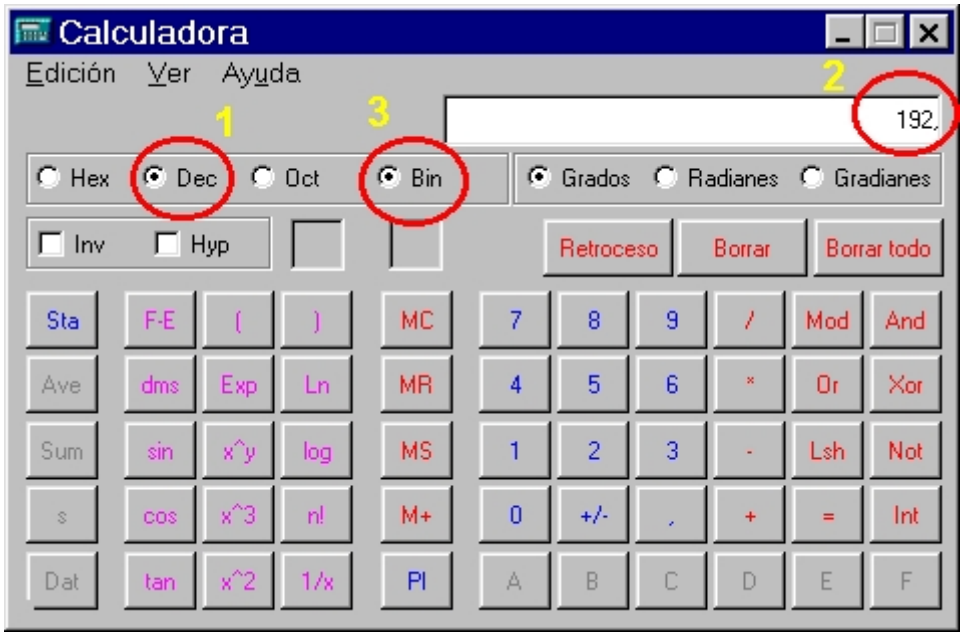
Si la Calculadora apareciera con el interface **Estándar**, acude a la opción de menú **Ver – Científica** y se desplegará con más funciones:



1. Selecciona el modo de trabajo decimal Dec.

2. Escribe el número a convertir.

3. Y haz click sobre Bin. En la pantalla de la calculadora te aparecerá, convertida a binario, la cantidad tecleada inicialmente.



Esto también funciona al revés. Puedes dar una cantidad en binario y transformarla en decimal (o hexadecimal Hex u octal Oct).

Ahora quizás entiendas por qué hemos dicho en capítulos anteriores que los números de una dirección IP no pueden superar el valor 255 (en decimal), que se corresponde con el número 11111111 en binario (compruébalo en la calculadora). Por otra parte, si en la conversión de decimal a binario no se alcanzasen los 8 bits necesarios, se añadirán ceros por la izquierda hasta completar el byte completo. Observa estos ejemplos:

10 en binario debería presentarse como 00000010

1110 en binario debería presentarse como 00001110

101011 en binario debería presentarse como 00101011

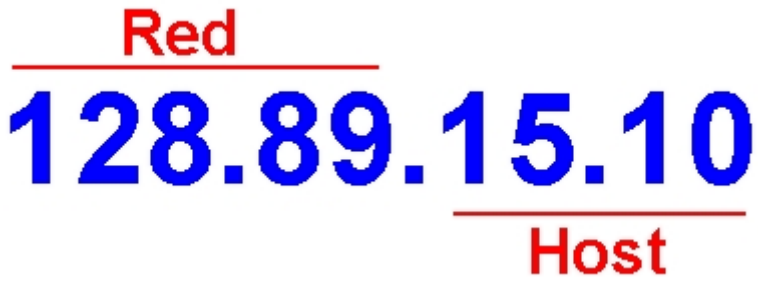
Como podrás imaginar, existen muchas redes en el mundo, cada una de ellas con varios hosts conectados y si utilizan el protocolo TCP/IP para interconectarse entre sí y poder intercambiar información (Internet es una buena muestra de ello), cada ordenador deberá tener asignada una dirección IP única y exclusiva.

Esto ha de ser así, pues para que dos computadoras puedan comunicarse han de estar identificadas con precisión, dado que el mecanismo de transmisión de los datos, al igual que el servicio de correos, exige conocer el destinatario de los mismos y no puede admitir que existan dos direcciones destino idénticas.

Pues bien, no sólo los host tienen un número asignado, sino que también cada una de las redes, de manera individual, han de tener también su propia dirección. Esa es la razón por la que una dirección IP se compone de dos partes:

- **Bits de red**: que son los bits que indican la red a la que pertenece el equipo.
- **Bits de host**: que son los bits que identifican a un equipo particular dentro de una red.

Los bits de red siempre están a la izquierda y los bits de host a la derecha:



Pero ¿cuántos bits se dedican a cada indicador? Según la manera de repartir los bits en una dirección IP, las redes se clasifican en categorías o **clases**:

Aquí hay Clase

Clase A: Destinadas a redes que precisen de una gran cantidad de direcciones IP, debido al número de host que comprenden (organismos gubernamentales, grandes campus hospitalarios o universitarios, etcétera).

Su dirección IP tiene la siguiente estructura:

	RED	NÚMERO DE HOST		
Rango en binario	0xxxxxxx (7 bits)	xxxxxxxx (8 bits)	xxxxxxxx (8 bits)	xxxxxxxx (8 bits)
Rango en decimal	0...127	0...255	0...255	0...255

Donde '**x**' indica cualquier valor binario (**0/1**).

Como ves, el número de la red viene dado por el primer octeto, con la particularidad de que el bit de más peso siempre es un '**0**'. Esto nos deja los **7 bits** restantes para numerar redes, o sea: $2^7 = 128$ redes distintas (desde 00000000 hasta 01111111). Pero como la dirección 0 se utiliza para reconocer la dirección de red propia, y la dirección 127 es la del lazo interno del host, estas direcciones no pueden ser asignadas a ninguna máquina, por lo que se reducen a un total de 126 redes. Así pues, en la clase A las redes posibles van desde **1.0.0.0** a **126.0.0.0** (recuerda que ahora estamos numerando a las redes, no a los hosts).

RANGO	Direcciones de RED - Clase A	
	binario	decimal
	00000001.	1.
	01111110.	126.

Los tres octetos restantes se destinan a asignar direcciones de host, o sea **24 bits** que suponen: $2^{24} = 16.777.216$ teóricos de hosts distintos. Decimos teóricos porque en la práctica no se pueden utilizar las direcciones que tengan todos los bits a 0 (0.0.0. no es válida porque ya sabes que está reservada para la numeración de la red) o a 1 (255.255.255, pues esta dirección se destina a los servicios de broadcast, mediante los cuales pueden enviarse tramas de comprobación y mantenimiento a todos los equipos de la red de manera simultánea). Así pues se quedan en **16.777.214**.

	Direcciones de HOST - Clase A					
	binario			decimal		
RANGO	.00000000	.00000000	.00000001	.0	.0	.1
	.11111111	.11111111	.11111110	.255	.255	.254

O sea, que **el rango de direcciones IP de una red de clase A va desde 1.0.0.1 hasta 126.255.255.254**.

Ejemplo:

*Dada la dirección IP de un ordenador: **12.23.255.0**, averiguar la clase de red a la que pertenece, la dirección de la red, el número que identifica al host y su dirección de broadcast.*

Solución:

- *Red de **clase A**, pues está en el rango 1.0.0.0 a 126.0.0.0*
- *Dirección de la red: **12.0.0.0***
- *Nº de host: **23.255.0***
- *Dirección de broadcast: **12.255.255.255***

Clase B: Destinada a redes que precisan un número de direcciones IP intermedio para conectar todos sus host (grandes empresas, organismos oficiales, campus de tipo medio...). Su dirección IP tiene la siguiente estructura:

	RED		NÚMERO DE HOST	
Rango en binario	10xxxxxx . xxxxxxxx (14 bits)		xxxxxxxx (8 bits)	xxxxxxxx (8 bits)
Rango en decimal	128...191	0...255	0...255	0...255

Donde '**x**' indica cualquier valor binario (**0/1**).

A este tipo de redes se les asigna un rango de direcciones IP identificado por **14 bits** de los dos primeros octetos de la IP, pues los dos bits de mayor peso siempre serán '**10**'. Esto nos permite disponer de 2^{14} **= 16.384** redes distintas y de 2^{16} **= 65.536** host cada una. Teóricamente, en la clase B las redes posibles van desde **128.0.0.0** a **191.255.0.0**.

	Direcciones de RED - Clase B	
	binario	decimal
RANGO	01000000.00000000.	128.0.
	10111111.11111111.	191.255.

Recuerda que, en la práctica, no podrás usar las direcciones X.X.0.0 (dirección de la red) ni X.X.X.255 (dirección para broadcasting), por lo que estas cantidades se verán reducidas. El rango de hosts va desde **x.x.0.1** hasta **x.x.1.254**:

Direcciones de HOST - Clase B			
binario		decimal	
.00000000	.00000001	.0	.1
.11111111	.11111110	.255	.254

Resumiendo, **el rango de direcciones IP de una red de clase B va desde 128.0.0.1 hasta 191.255.255.254**.

Ejemplo:

*Dada la dirección IP **145.233.4.34**, averiguar la clase de red a la que pertenece, la dirección de la red, el número que identifica el host y su dirección de broadcast.*

Solución:

- *Red de **clase B**, pues está en el rango 128.0.0.0 a 191.255.0.0*
- *Dirección de la red: **145.233.0.0***
- *Nº de host: **4.34***
- *Dirección de broadcast: **145.233.255.255***

Clase C: Destinadas a redes pequeñas de no más de 254 hosts (redes locales domésticas, de pequeñas empresas, Centros escolares, pequeños edificios,...)

Su dirección IP tiene la siguiente estructura:

	RED			HOST
Rango en binario	110xxxxx . xxxxxxxx . xxxxxxxx (21 bits)			xxxxxxxx (8 bits)
Rango en decimal	192...223	0...255	0...255	0...255

Donde '**x**' indica cualquier valor binario (**0/1**).

A este tipo de redes se les asigna un rango de direcciones identificado por **21 bits** de los 24 que componen los tres primeros bytes de la IP, pues ahora, los tres bits de mayor peso siempre serán '**110**'. Esto nos permite disponer de 2^{21} **= 2.097.152** redes distintas.

Teóricamente, en la clase C las redes posibles van desde 192.0.0.**0** a 223.255.255.**0**.

	Direcciones de RED - Clase C	
	binario	decimal
RANGO	11000000.00000000.00000000.	192.0.0.
	11011111.11111111.11111111.	223.255.255.

También aquí habría que descontar las direcciones de la red y la de broadcast.

El último byte de la dirección IP se destina a asignar direcciones de hosts, o sea **8 bits** que suponen: 2^8 **= 256** teóricos de máquinas distintas. Eliminando la 0 y la 255, el rango real de hosts va desde **x.x.x.**1 hasta **x.x.x.**254:

Direcciones de HOST - Clase B	
binario	decimal
.00000001	.1
.11111110	.254

Resumiendo, **el rango de direcciones IP de una red de clase C va desde 192.0.0.1 hasta 223.255.255.254**.

Ejemplo:

*Dada la dirección IP **192.168.32.2**, averiguar la clase de red a la que pertenece, la dirección de la red, el número que identifica el host y su dirección de broadcast.*

Solución:

- *Red de **clase C**, pues está en el rango 192.0.0.0 a 223.255.255.0*
- *Dirección de la red: **192.168.32.0***
- *Nº de host: **2***
- *Dirección de broadcast: **192.168.32.255***

Además de las clases A, B y C, existen dos formatos especiales de direcciones, la **clase D** y la **clase E**. Las direcciones de clase D no identifican a un host, sino a un grupo de ellos. Se usan para operaciones de envíos múltiples a grupos (*multidifusión* o *multicast*). Las direcciones de clase E se han reservado para uso experimental y no se pueden utilizar.

Fíjate en la estructura de sus direcciones IP:

Clase D

	RED	HOST		
Rango en binario	1110xxxx	.XXXXXXXX . XXXXXXXX . XXXXXXXX (24 bits)		
Rango en decimal	224...239	0...255	0...255	0...255

Clase E

	RED	HOST		
Rango en binario	1111xxxx	.XXXXXXXX . XXXXXXXX . XXXXXXXX (24 bits)		
Rango en decimal	240...255	0...255	0...255	0...255

Donde '**x**' indica cualquier valor binario (**0/1**).

¿Pública o Privada?

Y todo esto, ¿para qué? Primero matizaremos que las direcciones IP pueden ser de dos tipos:

- **IP Pública**: Aquella que es accesible por cualquier ordenador conectado a Internet.

- **IP Privada**: Aquella que sólo es accesible desde equipos privados conectados en redes locales.

Si tuvieras una red de servidores de páginas web y quisieras conectarlos a Internet para que todo el mundo pudiera contemplar su contenido, habría que asignarles una dirección IP a cada uno, que para poder ser 'alcanzada' por cualquier usuario conectado a Internet, tendría que ser pública. Las direcciones públicas te serán facilitadas por un organismo oficial (el **NIC**, *Network Information Center*) que vigila que no existan duplicados en la asignación de estas direcciones, pues como sabes, técnicamente es inviable que existan dos IP iguales en una misma red. Así que sólo tienes que decirles qué clase de red deseas instalar (A, B o C) y ellos te facilitarán la dirección de la red (15.0.0.0, ó 145.233.0.0, ó 215.168.32.0, por ejemplo), de manera exclusiva para tu empresa. Luego, a tu criterio, completas la IP añadiendo el número de host a medida que los vayas instalando.

Pero si lo que quieres es configurar una red local privada, como es el caso que nos ocupa, las direcciones que coloquemos en cada equipo son aquí irrelevantes, pues no establecerá un conflicto con ningún otro ordenador del mundo, incluso si existieran otras redes locales con las mismas IP configuradas en sus ordenadores en cualquier otra parte del planeta, dado que no hay conexión física entre ellas.

No obstante, se han reservado varios bloques de direcciones para asignarlos en las LAN privadas y que contienen unas direcciones IP que no son utilizadas nunca en Internet, o sea, que nunca serán IP públicas.

Por razones de estandarización es conveniente que las utilicemos, aunque insistimos en que si la LAN es privada se pueden poner los números que se desee. Eso sí, en la numeración hay que respetar siempre el mismo número de red para todos los equipos, sólo iremos variando el número del host. Veamos cuáles son esas IP reservadas para LAN privadas:

- Para **Clase A**: Desde **10.0.0.1** hasta **10.255.255.254**

- Para **Clase B**: Desde **172.16.0.1** hasta **172.31.255.254**

- Para **Clase C**: Desde **192.168.0.1** hasta **192.168.255.254**

Ahora recordemos las IP configuradas en nuestra red:

Equipo	Dirección IP	Máscara de Subred
Ordenador 1	**192.168.0.2**	255.255.255.0
Ordenador 2	**192.168.0.3**	255.255.255.0
Ordenador 3	**192.168.0.4**	255.255.255.0
Ordenador 4	**192.168.0.5**	255.255.255.0
Ordenador 5	**192.168.0.6**	255.255.255.0
Ordenador 6	**192.168.0.7**	255.255.255.0
Ordenador 7	**192.168.0.8**	255.255.255.0
Ordenador 8	**192.168.0.9**	255.255.255.0
Ordenador 9	**192.168.0.10**	255.255.255.0
Ordenador 10	**192.168.0.11**	255.255.255.0

A la vista de lo estudiado en este capítulo, ¿podrías decirnos la dirección de la red y a qué clase pertenece? ...¡!...¿No?... Vale, te echaremos una mano, pero quizás sea mejor que repases de nuevo el capítulo (saltándote el apartado de los mensajes emergentes):

Solución:

Dirección de red: ***192.168.0.0***

Red de Clase ***C.***

¡Por fin! Ahora comprendemos de dónde han venido esos números tan extraños que hemos configurado, en el capítulo anterior, en los diez ordenadores de nuestra red local recién instalada. Fíjate como hemos numerado cada

ordenador, empezamos en la dirección 192.168.0.2 y terminamos en la 192.168.0.11., por lo que hemos respetado las premisas anteriores: utilizar un rango de direcciones IP privadas y mantenemos el número de red (192.168.0.x) en todos los ordenadores, alterando sólo el número de host.

"... Sí, de acuerdo. Nos hemos saltado la dirección 192.168.0.1, pero esa queda reservada para cuando tengamos que conectarnos a Internet. No te impacientes..."

Descubriendo la máscara

¿Y qué hay de la máscara de subred que hemos tenido que configurar? ¿Cómo es posible que sea la misma para todos los equipos de la red?¿Qué significan esos números? ¿Qué es una subred? Demasiadas preguntas para el no iniciado, pero para ti, cuasi profesional del networking, esto será coser y cantar.

Por ahora vamos a acordar que decir red o subred sea decir lo mismo. Y que el concepto de red no se refiere a la disposición física de máquinas conectadas a un cableado común, sino que se refiere a la división lógica que se haga en función del número de red asignado. Es decir, que en nuestra aula de diez ordenadores, que físicamente forma una red local (de eso ya no cabe duda), podemos tener varias redes lógicas distintas, pues nada nos impide asignar las direcciones IP, por ejemplo, tal que así:

Equipo	Dirección IP	Máscara de Subred
Ordenador 1	192.168.0.2	255.255.255.0
Ordenador 2	192.168.0.3	255.255.255.0
Ordenador 3	192.168.0.4	255.255.255.0
Ordenador 4	192.100.80.1	255.255.255.0
Ordenador 5	192.100.80.2	255.255.255.0
Ordenador 6	192.100.80.3	255.255.255.0
Ordenador 7	220.200.10.1	255.255.255.0
Ordenador 8	220.200.10.2	255.255.255.0
Ordenador 9	220.200.10.3	255.255.255.0
Ordenador 10	220.200.10.4	255.255.255.0

A la vista de esta tabla distinguimos que, siendo todas de clase C, existen tres redes distintas:

- **192.168.0.0**
- **192.100.80.0**
- **220.200.10.0**

¿Puede esto llegar a funcionar? Sin ningún problema. La única ¿contrariedad? es que los ordenadores de una red no podrán 'alcanzar' a los de otra red y esto, en ocasiones y por motivos de seguridad, puede ser hasta interesante.

Si el ordenador 1 quiere dialogar con el ordenador 3 ó con el ordenador 7, debería existir un mecanismo que le permitiera averiguar si pertenecen o no a su red. Es aquí donde entra en juego la máscara de red (o de subred, llámalo como quieras).

Una **máscara de red** es un número con el formato de una dirección IP que nos sirve para distinguir si una máquina determinada pertenece a una red dada, con lo que podemos averiguar si dos máquinas están o no en la misma red IP.

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

Clase	Máscara de red
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Ahora ya sabes por qué configuraste a todos los hosts de la red con el valor de subred: 255.255.255.0, pues es la máscara que corresponde a equipos conectados a redes de clase C.

Si expresamos las máscaras de red en notación binaria, tendríamos:

Clase	Red/Host	Máscara de red	Formato binario
A	R.H.H.H	255.0.0.0	11111111.00000000.00000000.00000000
B	R.R.H.H	255.255.0.0	11111111.11111111.00000000.00000000
C	R.R.R.H	255.255.255.0	11111111.11111111.11111111.00000000

(**R**: nº de Red – **H**: nº de Host)

Y podremos comprobar cómo se construyen: los **unos** indican los bits de la dirección correspondientes a la red y los **ceros**, los correspondientes al host, en cada clase. Hay una gran similitud entre los formatos de la máscara y de la IP del host.

Ahora intentaremos explicar cómo funciona esto. Para ello realizaremos un ejercicio retomando el propósito anterior en el que el ordenador 1 deseaba establecer una comunicación con los ordenadores 3 y 7, pero no sabía si podría hacerlo y recurre al mecanismo de la máscara de red para averiguarlo.

Estas son las configuraciones IP de partida:

Host	Dirección IP	Máscara de subred
Ordenador 1	192.168.0.2	255.255.255.0
Ordenador 3	192.168.0.4	255.255.255.0
Ordenador 7	220.200.10.1	255.255.255.0

Paso 1:

El ordenador 1 ha de comprobar a qué red pertenece cada una de las direcciones que intervienen en el proceso. Para ello realizará una operación lógica AND, bit a bit, entre la dirección IP y la máscara de red asociada a esa dirección en cada uno de los ordenadores. El resultado será la dirección de la red.

¿Qué tampoco sabes que es eso de la operación lógica AND entre dos números binarios? Pues nada, para eso estamos aquí.

La operación AND (que se representa por **&**) es la multiplicación lógica y su tabla de verdad es muy sencilla.

A	B	A & B
0	0	0
1	0	0
0	1	0
1	1	1

Se resume en que el resultado de una operación AND será '1' cuando ambos operandos sean también '1'. Basta que uno cualquiera de ellos sea '0' para que el resultado también lo sea. Curiosamente es igual que la multiplicación decimal ordinaria.

Así que si aplicamos estas enseñanzas a cada uno de los 32 bits que forman la dirección IP junto con sus correspondientes 32 bits que forman la máscara de red, en los tres casos, obtendremos:

Paso 2:

Ordenador 1		
Dirección IP:	192.168.0.2	11000000 10101000 00000000 00000010
Máscara de subred:	255.255.255.0	11111111 11111111 11111111 00000000
Dirección de Red:	**192.168.0.0**	**11000000 10101000 00000000 00000000**

Paso 3:

Ordenador 3		
Dirección IP:	192.168.0.4	11000000 10101000 00000000 00000100
Máscara de subred:	255.255.255.0	11111111 11111111 11111111 00000000
Dirección de Red:	**192.168.0.0**	**11000000 10101000 00000000 00000000**

Paso 4:

Ordenador 7		
Dirección IP:	220.200.10.1	11011100 11001000 00001010 00000001
Máscara de subred:	255.255.255.0	11111111 11111111 11111111 00000000
Dirección de Red:	**220.200.10.0**	**11011100 11001000 00001010 00000000**

A la vista de las direcciones de red obtenidas, se comprueba que los ordenadores 1 y 3 pertenecen a la misma red (192.168.0.0), mientras que el ordenador 7 pertenece a otra red (220.200.10.0) y no podrá ponerse en contacto con los primeros (al menos de manera directa).

Ya hemos aprendido algo más acerca de la máscara de subred, pero aún no descubrimos su verdadera potencia. Para ello hay que complicar algo más las cosas. ¿O creías que no era posible?

La subred

Como ya sabemos, una dirección IP se compone de dos partes: la dirección de red y la dirección de host. Hemos adoptado una red de clase C, por las razones que ya se aportaron anteriormente, y también conocemos que las redes de clase C pueden direccionar hasta 256 hosts teóricos. Pues bien, imaginemos que en nuestra red sólo hacen falta 128 equipos. ¿Podríamos dividir la red en dos partes iguales de 128 equipos cada una?. Sí, gracias a la máscara podemos crear dos **subredes** (o más si fuera necesario).

Como regla general, el truco consiste en robarle bits al octeto de mayor peso (el de más a la izquierda) de la máscara de subred que coincida con la dirección del host en la IP. ¿Cuántos bits hay que robar? Dependerá de las subredes que queramos obtener, teniendo en cuenta que: cuantos más bits robemos, más subredes obtendremos, pero con menos host cada una.

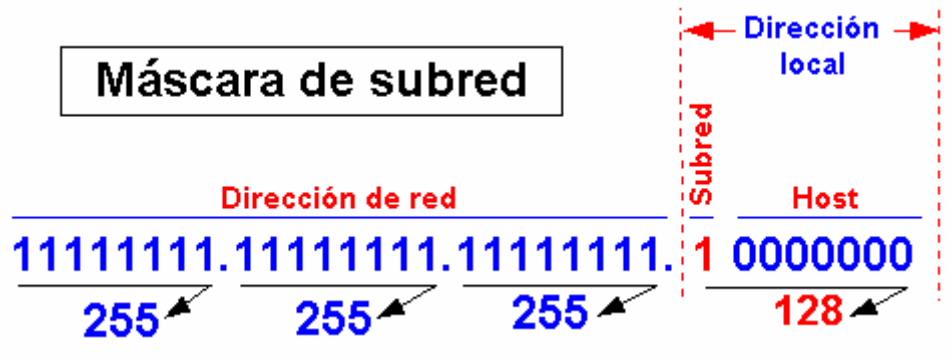
Estamos de acuerdo contigo. "*Esto es un lío*". Pero qué le vamos a hacer. Lo mejor es llevarlo a la práctica. Recuerda la máscara de red de nuestra red de clase C:

Clase	Red/Host	Máscara de red	Formato binario
C	R.R.R.H	255.255.255.0	11111111.11111111.11111111.00000000

Aquí solo hay un octeto para la dirección del host. Ahora le robamos un bit a ese octeto y lo ponemos a '**1**'. La máscara de red se transforma en:

Clase	Red/Host	Máscara de red	Formato binario
C	R.R.R.H	255.255.255.128	11111111.11111111.11111111.10000000

Los bits de host ahora han sido divididos en dos partes, una (el bit robado) para identificar la subred (siempre son bits a '1') y la otra para identificar la máquina (host).



El conjunto formado por la subred y el número de host se conoce como **dirección local** o parte local. Un host remoto verá la dirección local como el número de host.

Si, por ejemplo, la dirección de red que estamos utilizando es la **192.168.0.0**, al poner esta máscara de red crearíamos dos subredes: **192.168.0.0** y **192.168.0.128**, con unos rangos IP definidos:

Red	Rangos IP
192.168.0.0	192.168.0.1 .. .. 192.168.0.127
192.168.0.128	192.168.0.129 .. .. 192.168.0.254

En ambos casos, la máscara de red para las dos subredes sería la 255.255.255.128. Y recuerda que siempre hay que evitar las direcciones IP correspondientes a la propia red y a la dirección de broadcast. Si tienes problemas para obtener las direcciones de red y de broadcast, recuerda esta regla mnemotécnica: la dirección de red es la misma que la IP, salvo que los bits del host se ponen todos a cero. La dirección de broadcast es la misma que la IP, pero con los bits del host puestos a uno.

¿Y si le robamos 2, 3 o más bits a la dirección local? Pues aunque no es habitual dividir las redes privadas de clase C en subredes más pequeñas, nada nos impide hacerlo. En cualquier caso hemos querido explicarte este mecanismo para justificar la existencia de las subredes y de la máscara de subred que ya has empleado en capítulos anteriores.

En la siguiente tabla te mostramos las posibles divisiones de una red de clase C:

Máscara de subred	Binario	Número de subredes	Núm. de hosts por subred
255.255.255.0	00000000	1	254
255.255.255.128	10000000	2	126
255.255.255.192	11000000	4	62
255.255.255.224	11100000	8	30
255.255.255.240	11110000	16	14
255.255.255.248	11111000	32	6
255.255.255.252	11111100	64	2

La primera de estas máscaras de subred es la que se emplea por defecto (255.255.255.0), dado que no existe más que una subred, ¿o es una red? Aunque comenzamos este apartado no distinguiendo entre ambos conceptos, deberíamos de haber aprendido que en este caso es lo mismo; pero sólo en este caso. Las subredes son redes lógicas distintas que comparten una misma dirección IP, pero se diferencian en su máscara de subred.

Si te ves con ganas, intenta plasmar en tablas similares a ésta las posibles divisiones de las redes de clase A y B (es un buen somnífero).

Ejercicio:

Se trata de averiguar la pertenencia de unas direcciones IP a una subred determinada. Supongamos la dirección de red 192.168.114.128, con una máscara de subred 255.255.255.128.

Comprobar si las siguientes direcciones pertenecen a dicha subred:

- *192.168.114.134*
- *192.168.114.192*
- *192.168.114.38*
- *192.168.114.94*

Solución:

Pasamos todo a binario y realizamos la operación AND entre las direcciones y la máscara de subred:

Dirección IP:	**192.168.114.134**	11000000 10101000 01110010 10000110
Máscara de subred:	255.255.255.128	11111111 11111111 11111111 10000000
Dirección de subred:	**192.168.114.128**	**11000000 10101000 01110010 10000000**

Dirección IP:	**192.168.114.192**	11000000 10101000 01110010 11000000
Máscara de subred:	255.255.255.128	11111111 11111111 11111111 10000000
Dirección de subred:	**192.168.114.128**	**11000000 10101000 01110010 10000000**

Dirección IP:	**192.168.114.38**	11000000 10101000 01110010 00100110
Máscara de subred:	255.255.255.128	11111111 11111111 11111111 10000000
Dirección de subred:	**192.168.114.0**	**11000000 10101000 01110010 00000000**

Dirección IP:	**192.168.114.94**	11000000 10101000 01110010 01011110
Máscara de subred:	255.255.255.128	11111111 11111111 11111111 10000000
Dirección de subred:	**192.168.114.0**	**11000000 10101000 01110010 00000000**